http与https:

一.http:

超文本传输协议(HTTP)是一种通信协议，它允许将超文本标记语言(HTML)文档从Web服务器传送到客户端的浏览器

1.结构

- http请求结构：请求行、消息报头、请求正文
- http响应结构：状态行、消息报头、响应正文

2.状态码：http响应结构中状态行由HTTP协议版本号、状态码、状态消息三部分组成，常见状态码有

- 200 – 服务器成功返回网页
- 404 – 请求的网页不存在
- 503 – 服务器超时
- 400-错误的请求，客户端发送的HTTP请求不正确
- 405-服务器不支持客户端的请求方式
- 500-服务器内部错误。

3.Http Request的几种类型

- GET：向特定的资源发出请求。
- POST：向指定资源提交数据进行处理请求，数据被包含在请求体中，POST请求可能会导致新资源的创建或已有资源的修改。
- PUT：向指定资源位置上传其最新内容。
- DELETE：请求服务器删除Request-URI所标识的资源。
- HEAD：请求读取由URL所标志的信息的首部。
- OPTIONS：返回服务器针对特定资源所支持的HTTP请求方法，也可以利用向Web服务器发送的请求来测试服务器的功能性。
- TRACE：回显服务器收到的请求，主要用于测试或诊断。

- CONNECT：HTTP/1.1协议中预留给能够将连接改为管道方式的代理服务器。

4.get与post的区别

- 根据HTTP规范，GET用于信息获取，而且应该是安全的和幂等的。(1).所谓安全的意味着该操作用于获取信息而非修改信息。换句话说，GET请求一般不应产生副作用。就是说，它仅仅是获取资源信息，就像数据库查询一样，不会修改、增加数据、不会影响资源的状态。(2).幂等的意味着对同一URL的多个请求应该返回同样的结果。
- 根据HTTP规范，POST表示可能修改变服务器上的资源的请求。还是新闻以网站为例，读者对新闻发表自己的评论应该通过POST实现，因为在评论提交后站点的资源已经不同了，或者说资源被修改了。
- GET请求的数据会附在URL之后（就是把数据放置在HTTP协议头中），以?分割URL和传输数据，参数之间以&相连.POST把提交的数据则放置在是HTTP报文体中。
- GET安全性较低，POST安全性较高。因为GET在传输过程，数据被放在请求的URL中，而如今现有的很多服务器、代理服务器或者用户代理都会将请求URL记录到日志文件中，然后放在某个地方，这样就可能会有一些隐私的信息被第三方看到。另外，用户也可以在浏览器上直接看到提交的数据，一些系统内部消息将会一同显示在用户面前。
- get传送的数据量较小，不能大于2KB。post传送的数据量较大，一般被默认为不受限制。
- 在FORM（表单）中，Method默认为"GET"

5.如何理解HTTP协议是无状态的

HTTP协议是无状态的，指的是协议对于事务处理没有记忆能力，服务器不知道客户端是什么状态。也就是说，打开一个服务器上的网页和你之前打开这个服务器上的网页之间没有任何联系。HTTP是一个无状态的面向连接的协议，无状态不代表HTTP不能保持TCP连接，更不能代表HTTP使用的是UDP协议（无连接）

6.解释网络ip、tcp、udp、http、socket以及之间的区别

- IP协议：为计算机网络相互连接进行通信而设计的协议。
- TCP：传输控制协议,提供的是面向连接、可靠的字节流服务。当客户和服务器彼此交换数据前，必须先在双方之间建立一个TCP连接，之后才能传输数据。TCP提供超时重发，丢弃重复数据，检验数据，流量控制等功能，保证数据能从一端传到另一端。
- UDP：用户数据报协议，是一个简单的面向数据报的运输层协议。UDP不提供可靠性，它只是把应用程序传给IP层的数据报发送出去，但是并不能保证它们能到达目的地。由于UDP在传输数据报前不用在客户和服务器之间建立一个连接，且没有超时重发等机制，故而传输速度很快
- TCP/IP ：是传输层协议，主要解决数据如何在网络中传输
- HTTP协议：超文本传送协议(Hypertext Transfer Protocol)，HTTP协议是建立在TCP协议之上的一种应用。
- IP协议对应于网络层，TCP协议对应于传输层，而HTTP协议对应于应用层。注意TPC/IP位于传输层，它主要用来解决数据如何在网络中传输，与IP协议要区分开。
- SOCKET：是对TCP/IP协议的封装，Socket本身并不是协议，而是一个调用接口（API），通过Socket，我们才能使用TCP/IP协议，Socket的出现只是使用程序员更方便地使用TCP/IP协议栈而已，是对TCP/IP协议的抽象，从而形成了我们知道的一些最基本的函数接口
-

使用Socket建立网络 网络上两个程序通过双向通信实现数据交换，Socket又叫套接字，每个应用程序开启后，都会在传输层端口上绑定一个socket，不同应用程序之间通过寻找端口找到socket实现数据通信。Socket连接过程分为三个步骤：服务器监听，客户端请求，连接确认。

- 服务器监听：服务器端套接字并不定位具体的客户端套接字，而是处于等待连接的状态，实时监控网络状态，等待客户端的连接请求。
- 客户端请求：指客户端的套接字提出连接请求，要连接的目标是服务器端的套接字。为此，客户端的套接字必须首先描述它要连接的服务器的

套接字，指出服务器端套接字的地址和端口号，然后就向服务器端套接字提出连接请求。

- 连接确认：当服务器端套接字监听到或者说接收到客户端套接字的连接请求时，就响应客户端套接字的请求，建立一个新的线程，把服务器端套接字的描述发给客户端，一旦客户端确认了此描述，双方就正式建立连接。

二.https协议：

HTTPS(Secure Hypertext Transfer Protocol)安全超文本传输协议： 它是一个安全通信通道，它基于HTTP开发，用于在客户计算机和服务器之间交换信息，它使用安全套接字层(SSL)进行信息交换。

1.https中ssl加密解密流程

对称加密算法：加密和解密使用相同的密钥，典型的有DES、RC5、IDEA、RC4
非对称加密算法（公钥加密算法）：加密解密使用不同密钥（公钥用于加密，私钥用于解密）：RSA、DSA
SSL在握手过程中使用非对称加密算法来握手协商密钥，实际使用对称加密算法来对http内容加密传输

- 客户端的浏览器向服务器端传送客户端SSL协议的版本号，加密算法的种类，产生的随机数以及其他服务器和客户端通讯所需要的各种信息
- 服务器向客户端传送SSL协议版本号，加密算法的种类，随机数以及其他相关信息，同时服务器还向客户端传送自己的证书
- 客户利用服务器传来的信息验证服务器的合法性，合法性包括：证书是否过期，发行服务器证书的CA是否可靠，发行者证书的公钥能否正确解开服务器证书的“发行者的数字签名”，服务器证书上的域名是否和服务器的实际域名相匹配，如果合法性验证没通过，通讯将断开，如果合法性通过，则继续进行
- 客户端随机生成一个用于后面通讯的“对称密码”，然后用服务器的公钥（证书中获得）对其加密，然后传给服务器
- 服务器用私钥解密“对称密码”，然后将其作为服务器端和客户端的“通话密码”加解密通讯。

- 客户端向服务器端发出消息，指明后面的通讯将使用对称密码为对称密钥，同时通知服务器客户端的握手过程结束
- 服务器向客户端发出消息，指明后面的通讯将使用对称密码作为对称密钥，同时通知客户端服务器端的握手过程结束
- SSL握手部分结束，SSL安全通道的数据通讯开始，客户和服务器开始使用相同的对称密钥进行数据通讯

通俗版：

- 当你的浏览器向服务器请求一个安全的网页(通常是 https://)
- 服务器就把它的证书和公匙发回来
- 浏览器检查证书是不是由可以信赖的机构颁发的，确认证书有效和此证书是此网站的。
- 浏览器使用公钥加密了一个随机对称密钥，包括加密的URL一起发送到服务器。
- 服务器用自己的私匙解密了你发送的钥匙。然后用这把对称加密的钥匙给你请求的URL链接解密。
- 服务器用你发的对称钥匙给你请求的网页加密。你也有相同的钥匙就可以解密发回来的网页了

2.http与https的区别：

- https需要到ca申请证书，免费的很少
- http是超文本传输协议，信息是明文传输，https 则是具有安全性的ssl加密传输协议 。
- http和https使用的是完全不同的连接方式用的端口也不一样：前者是80，后者是443。
- http的连接很简单，是无状态的 ，而HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议 ，要比http协议安全 。

三.ARP处理过程：

每个主机都存有一个ARP高速缓存，存放本局域网上各主机和路由器的IP地址到MAC地址的映射表，称为ARP表，使用ARP协议动态维护此表， ARP工作在网络层中。其工作原理是：

- 当主机A欲向本局域网上的某个主机B发送IP数据报时，就先在其ARP高速缓存中查看有无主机B的IP地址。如果有可以查出其对应的硬件地址，再将此硬件地址写入MAC帧，然后通过局域网将该MAC帧发往此硬件地址。
- 如果没有，就通过使用目的MAC地址为本网络的广播地址即32个1的帧来封装并广播ARP请求分组，可以使同一个局域网里的所有主机收到ARP请求。当主机B收到该ARP请求后，就会向主机A发出响应ARP分组，分组中包含主机B的IP与MAC地址的映射关系，主机A在收到后将此映射写入ARP缓存中，然后按查询到的硬件地址发送MAC帧。
- ARP是解决同一个局域网上主机与路由器的IP地址和硬件地址的映射问题。如果所要找的主机和源主机不在同一个局域网上，那么通过ARP协议找到一个位于本局域网上的某个路由器硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。

四.Ping过程：

同一个局域网中：

- Pc1在应用层向PC2发出Ping请求。
- 传输层接到上层请求的数据，将数据分段并加上UDP报头。下传到网络层。
- 网际层接收来处上层的数据后，根据ICMP协议进行封装，添加PC1的IP为源IP为和PC2IP为目标IP后封装成数据包。下传到网络接口层。
- 网络接口层接收数据包后，进行封装，源MAC地址为PC1的MAC地址，目标MAC地址则查询自己的ARP缓存表获取。如果PC1 arp缓存表中没有目标IP对应的MAC地址，则PC1发出一个ARP广播报文。ARP报文中源MAC地址为Pc1mac地址，源IP地址为pc1 IP，所要请求的是PC2的IP对应的mac地址。

- PC2收到ARP广播后，进行解封装，发现所请求的MAC地址是自己的。则PC2将PC1的mac地址写入arp缓存表中。然后向PC1发送一个 ARP 应答单播。该单播消息包括目标IP为PC1ip，目标Mac为pc1mac地址，源IP为PC2的IP，源Mac为pc2的Mac。
- Pc1接收到PC2的arp应答报文后，将Pc2的MAC地址存入arp缓存中，并将Pc2的Mac地址作为目标地址封装到数据帧中。发给下层进行网络传输。
- PC2接收这个帧后，在网络接口层查看目标mac地址是否指向自己。是，PC2则将帧头去掉，向上层传输。
- Pc2网际层接收到这个信息包，查看包头，发现目标IP和自己匹配，则解封装，将数据向上层传输。
- 传输层接收来自下层的Ping请求的UDP报文，则去掉UDP报头，向应用层传送。
- 应用层收到ping请求后，发送一个PIng回应报文给PC1