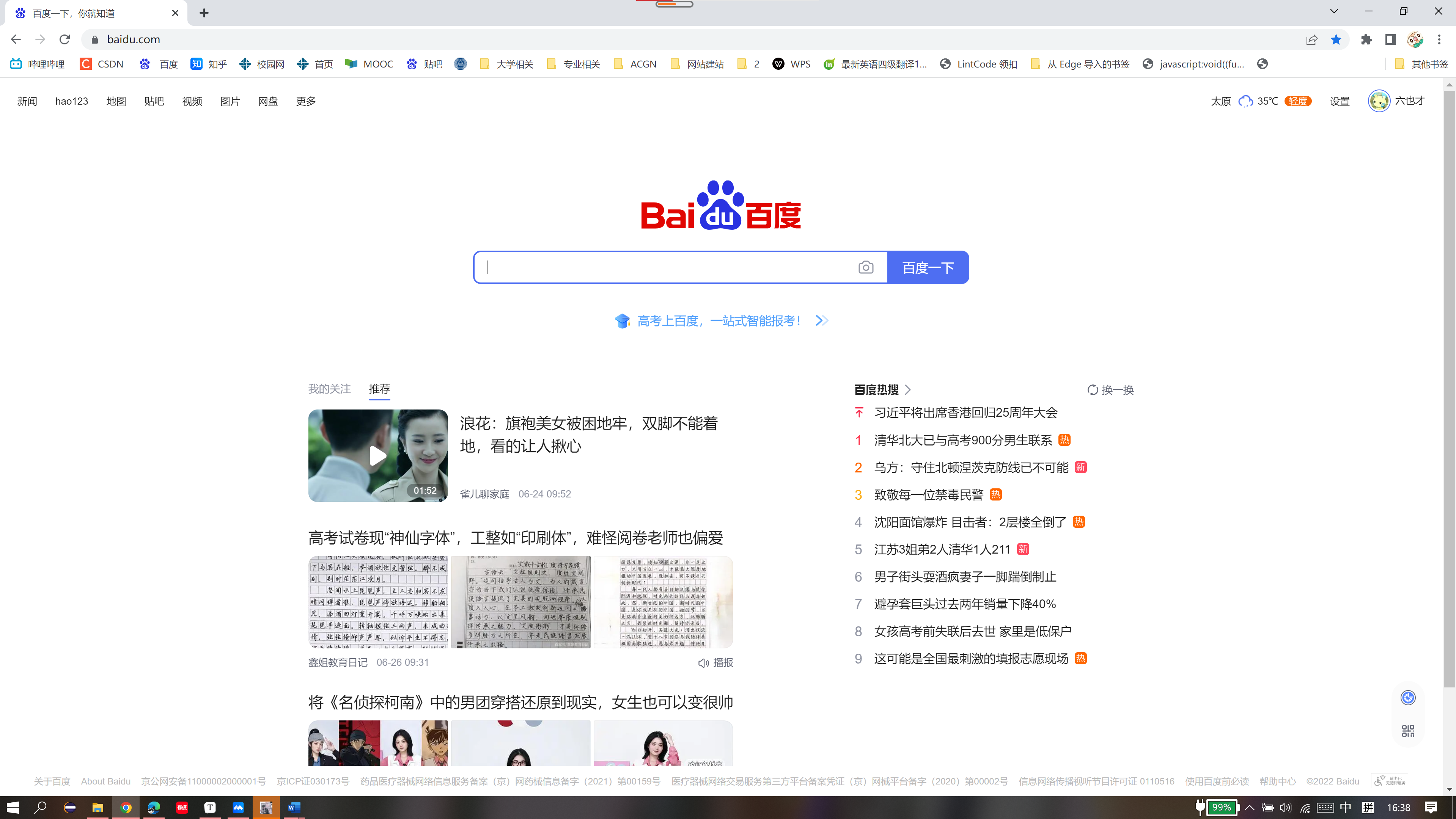
各位同学，由于受到疫情的影响，包括计算机网络在内的大部分课程都无法正常线下授课。在线上授课的过程中，由于缺少教室中零距离的接触，缺少直观的板书，缺少充足的直接互动过程，同学们学习某些课程可能要付出更多的努力，学习效果可能也或多或少地受到了一些影响。但我们觉得计算机网络这门课程反而会因为线上授课而使同学们收获更多。大家在直播授课、线上互动、线上考评、甚至课余时间的线上购物、娱乐中，对计算机网络应该会有更直观深刻的理解。

现在我们进入这门课程的期末考评环节，具体规则和要求如下：

1. 期末考评为开放性考评，各位同学可以查阅课件、教材、参考书籍、网上资料等各种合法获得的资源。
2. 期末考评必须个人独立完成，除查阅资料外不得与其他任何人通过任何方式对考评题目进行讨论。**所有提交内容（包括但不限于文字表述、图表、代码等）均需要有原创性，不得直接拷贝网络现成资源，不得抄袭他人成果。上述情况一经发现，取消这部分相应成绩。**如果参考了已有论文或书籍或网络资源的结论，需作为参考文献在文末列出。
3. 期末考评需要连续完成，中途不应长时间中断。从开始答题计算，建议在八小时内完成本期末考评。所以请各位在开始前预留充足的时间。
4. 各位同学需在**18周周一（6月27日）晚23：59前**按要求将答案提交到BB平台，逾期未提交者取消期末考评成绩，后果自负。
5. 格式要求：所有答案中文部分采用宋体五号字，非中文内容采用Times New Roman字体五号字，图表字号不超过正文字号，单倍行距，图表清晰可读。

下面，我们的考评正式开始，请各位同学认真阅读题目描述，并准确、详细地回答每个问题，每个问题的答案尽量控制在A4纸一页之内。

首先，请打开浏览器，访问百度首页，[www.baidu.com](http://www.baidu.com)，以确保你在考评过程中能正常访问网络。**在整个考评过程中，请勿更换电脑和浏览器！**请将你的包含桌面状态栏和完整浏览器页面（显示百度主页内容）在内的完整桌面截图贴在此处：



开始时间：2022-6-26 16:38

假定你需要通过淘宝进行购物，从浏览器地址栏输入URL到显示主页的过程中，计算机网

络主要涉及到下列流程要点：

DNS解析，查找域名对应的IP地址。

与服务器通过三次握手，建立TCP连接

向服务器发送HTTP请求

服务器处理请求，返回网页内容

浏览器解析并渲染页面

TCP四次挥手，连接结束

下面的任务和问题将围绕此场景展开。

**第一题：**通过比较OSI七层模型、TCP/IP四层模型、和课堂上介绍的五层模型比较计算机网络体系结构，请画出三种体系结构的示意图，并分别描述、比较各层的功能和支持的协议。



OSI七层模型是理论上的分层方式，而四层模型是实践过程中的分层模型。



联系与区别：

OSI引入了服务、接口、协议、分层的概念，TCP/IP借鉴了OSI的这些概念建立TCP/IP模型。

OSI先有模型，后有协议，先有标准，后进行实践；而TCP/IP则相反，先有协议和应用再提出了模型，且是参照的OSI模型。

OSI是一种理论下的模型，而TCP/IP已被广泛使用，成为网络互联事实上的标准。

五层协议只是OSI和TCP/IP的综合，实际应用还是TCP/IP的四层结构。



注：以上图表均为本人在Typora绘制，并复制到本文中。

**第二题：**如何理解HTTP协议是无状态的？以登录淘宝购物为例，举例说明有状态的场景、无状态的场景、以及为了解决无状态而引入Cookie之后的场景。

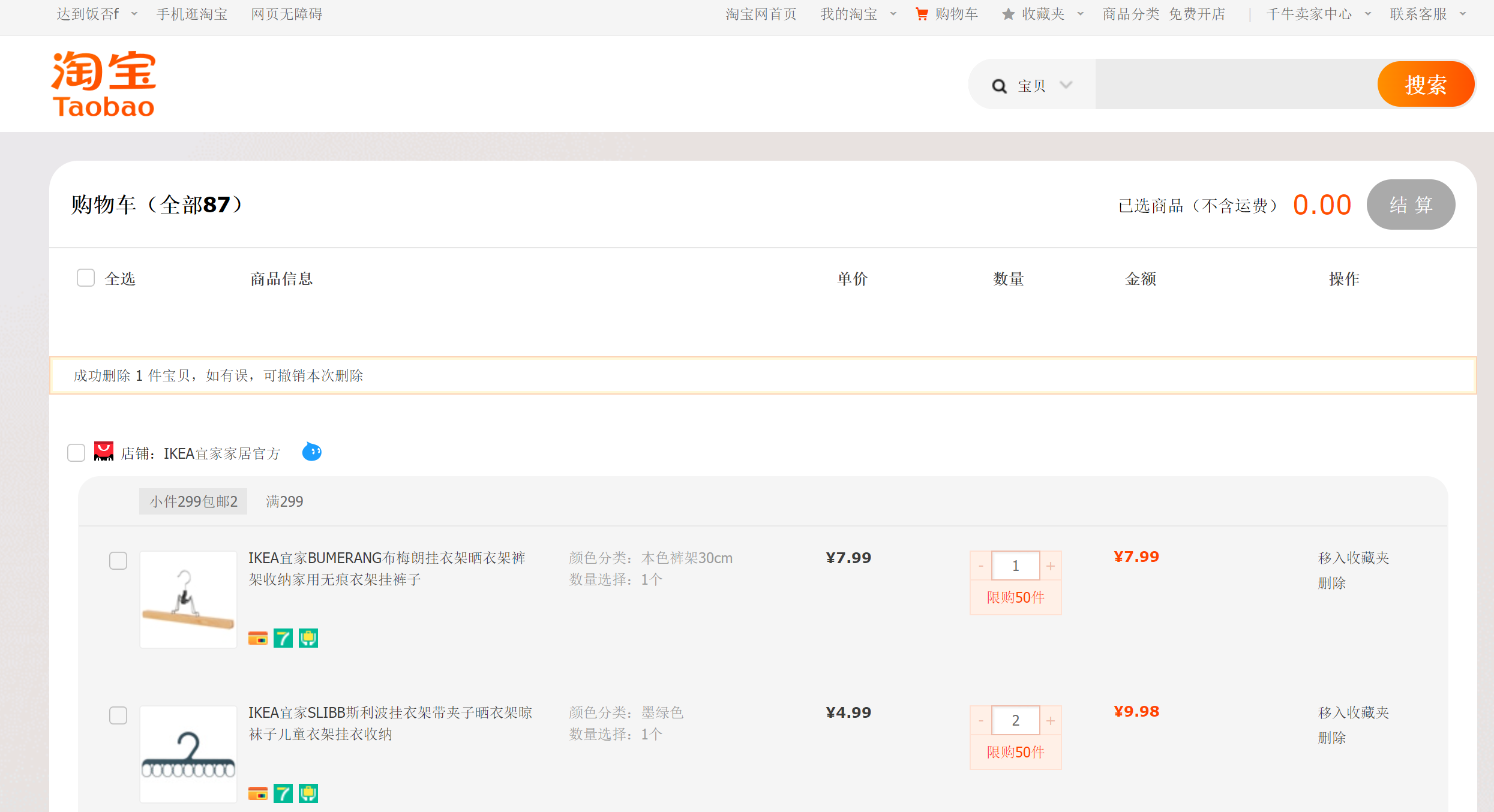
如何理解HTTP协议是无状态的：

HTTP协议是一种超文本传输协议，而为什么说HTTP协议是无状态的呢，是因为当浏览器第一次发送数据给服务器时，服务器响应了；如果同一浏览器，向服务器第二次发送请求时，它还是会响应，但服务器并不知道你就是刚才那个浏览器。简而言之，服务器是不会记住你是谁的，所以是无状态的。

有状态场景：

用户第一次打开淘宝，提示需要登录：

用户在主页面登录成功，跳转到其他页面，比如购物车页面，不需要需要重新登录。



无状态场景：

用户在主页面登录成功，但一旦跳转到其他页面，比如购物车页面；或者是在本页面刷新，页面显示需要重新登录，说明之前的登录状态没有保存。



为解决无状态而引入Cookie之后的场景：

第一次登录淘宝时，输入账号密码并登录成功后服务器会将返回Cookie数据给浏览器，浏览器将Cookie数据保存在本地，当打开淘宝的其他页面，比如购物车，或者刷新本页面时，浏览器会自动把上次请求存储的Cookie数据自动地携带给服务器，这会让浏览器“记住”你的登录状态。同理，当退出浏览器时，如果Cookie不被清除，那么再次打开淘宝首页，也不需要重新登录。**第三题**：什么是DNS？请以访问淘宝网主页www.taobao.com为例说明DNS的解析过程，并借助图表比较迭代查询和递归查询的区别。

**DNS：**

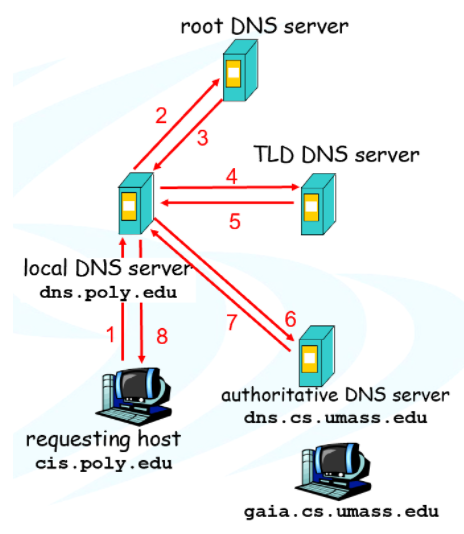
基于UDP；

作用：域名解析

介绍：由解析器和域名服务器组成，是因特网使用的命名系统。作为可以将域名和[IP地址](https://www.jb51.net/network/299890.html)相互映射的一个分布式数据库，用来把便于人们使用的机器名字转换成为IP地址，使人们可以更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

**以访问淘宝网主页www.taobao.com为例说明DNS的解析过程：**

DNS的解析过程一般有两种，一种是迭代查询，一种是递归查询。在实际过程中采用两者的结合，过程如下图：



图源：课程PPT

以访问淘宝为例：当访问淘宝网主页www.taobao.com时，用户的计算机并不知道www.taobao.com的服务器IP地址是多少，此时计算机将发出请求解析域名解析www.taobao.com的报文，实际上相比上图，还多了一个查找本地hosts的过程，总共分为以下几步：

1.先查找本地

当解析器把查询传递给一台本地名字服务器时，该名字服务器在本地的内存缓冲区中搜索最近时间里解析的名称地址。若找到，则将结果返回给客户端。

否则，该名字服务器在本地静态映射表中搜寻，看是否在管理员录入的项中是否有该主机名所对应的IP地址。如果存在相应的表项，则向客户机发送相应的IP地址。

2．若本地查找失败

则表明所要解析的域名为远程域名，于是本地名字服务器向根服务器（Root）查询。

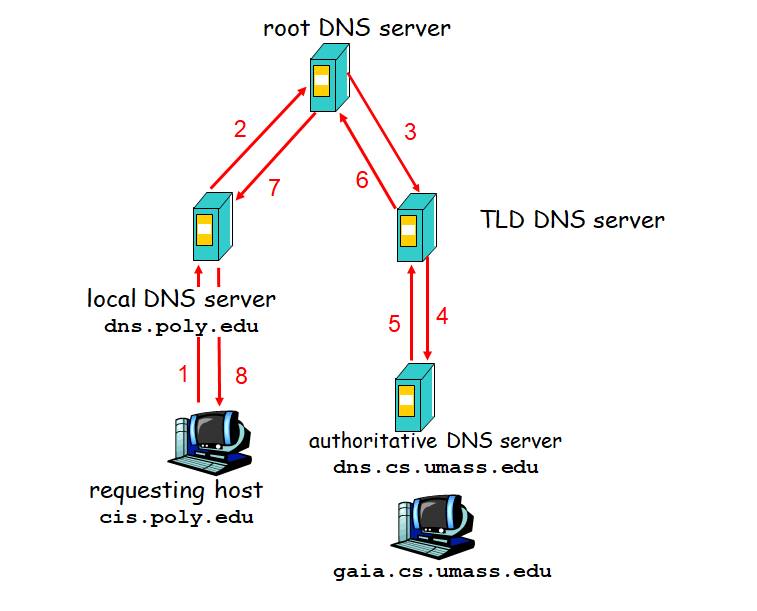
3.根名称服务器根据主机名称中指定的顶层域名进行相应的顶层域名称服务器搜寻，以淘宝www.taobao.com为例，这里找到的是com的顶层服务器，然后，根服务器将相应的顶层域名DNS服务器的IP地址返回给本地DNS服务器。

4.本地DNS服务器再向顶层域DNS服务器查询，顶层域DNS服务器根据主机名称中指定的二层域名进行相应的二级域名称服务器搜寻，并将相应的二级域DNS服务器的IP地址返回给本地DNS服务器。这里找到了taobao.com对应的服务器。

5．和第4步类似，再查询三级域，最终找到 www.taobao.com的IP地址返回给本地服务器。

**迭代查询和递归查询的区别：**

假如完全使用递归查询：



图源：课程PPT

整个查询过程类似一个大环，在实际过程中，本地域名服务器向根域名服务器的查询通常是采用迭代查询，因为大部分的域名解析都可以在本地DNS服务器之前完成。

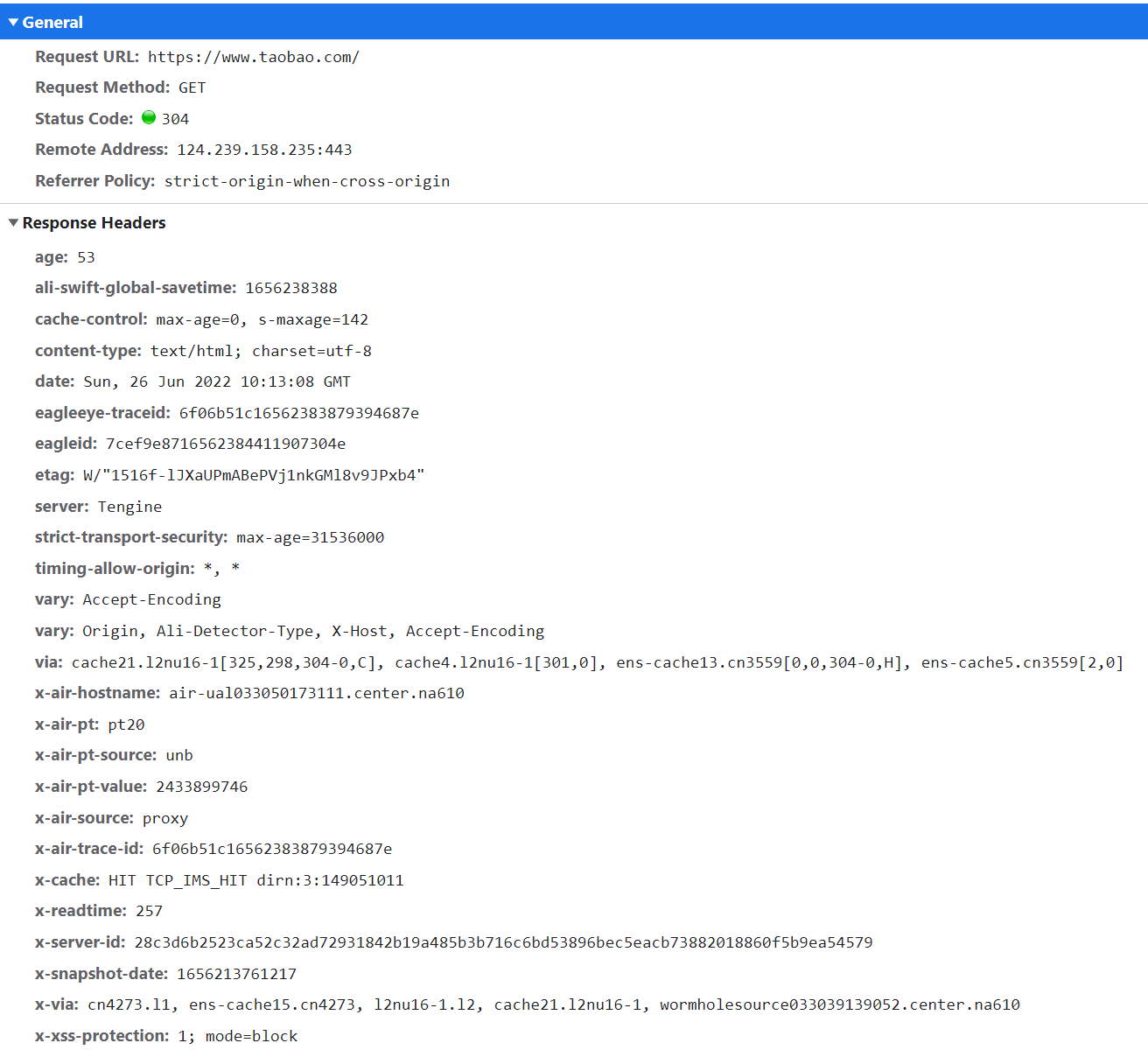
比较：

1、主机向本地域名服务器的查询一般都是采用递归查询。如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。

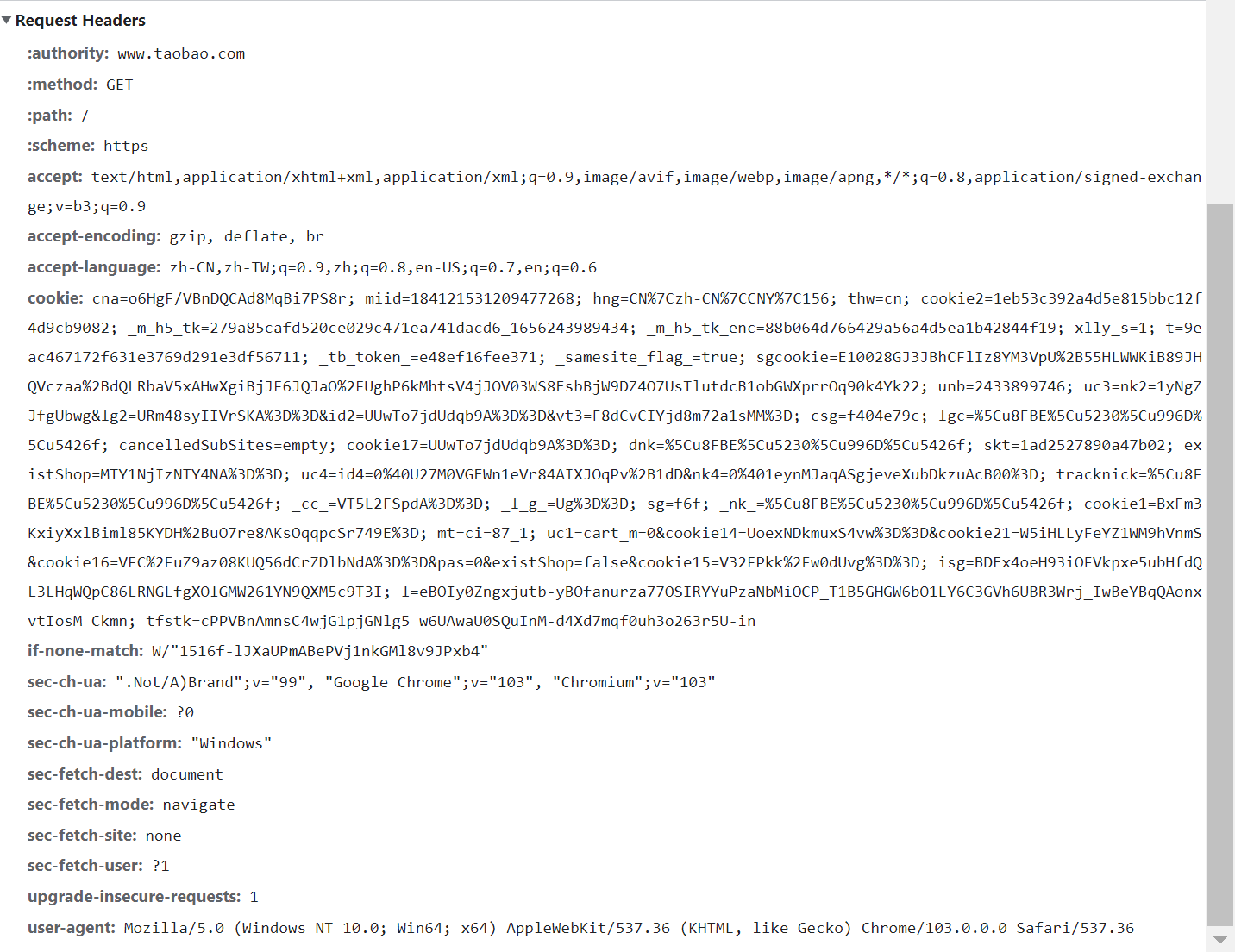
2、本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。

**第四题：**请在浏览器中访问淘宝网首页，并通过浏览器开发者模式获取此访问的HTTP请求和应答报文，将你获取到的完整报文头部信息截图粘贴于此：

请求头：



响应头：



请以访问淘宝网主页为例，用图文解释HTTP请求的过程与原理。HTTP的请求方法有哪些？举例说明各自有哪些使用场景？HTTP哪些常用的状态码？举例说明各自有哪些使用场景。

HTTP请求的过程与原理：

1.浏览器通过三次握手与淘宝网主页服务器建立连接。

2.浏览器发送一个请求给淘宝网主页服务器。

3.淘宝网主页服务器返回相应的响应信息给浏览器。

4.释放连接（四次挥手）。

5.浏览器接收淘宝网主页服务器所返回的信息并进行显示。

HTTP的请求方法以及使用场景：



HTTP常用的状态码及使用场景分别为：



200 表示请求已正常处理

204 请求处理成功，但没有任何资源可以返回给客户端

301 资源的URL已更新，以后应使用现在所指的URL，永久性重定向

302 资源的URL已临时定位到其他位置，临时性重定向（与301类似，但302代表的资源不是永久性移动，只是临时性的）

303 资源的URL已更新（表示由于请求对应的资源存在着另一个URL，应使用GET方法定向获取请求的资源，303和302状态码有着相同的功能，但303状态码明确表示客户端应当采用GET方法获取资源）

304 资源已找到，但未符合条件请求

400 服务器端无法理解客户端发送的请求，请求报文中可能存在语法错误

401 该状态码表示发送的请求需要有通过HTTP认证的认证信息

403 不允许访问资源

404 服务器上没有请求的资源，路径错误等

500 内部资源出错

503 表示服务器暂时处于超负载或正在停机维护，现在无法处理请求

注：以上图表均为本人在Typora绘制，并复制到本文中。

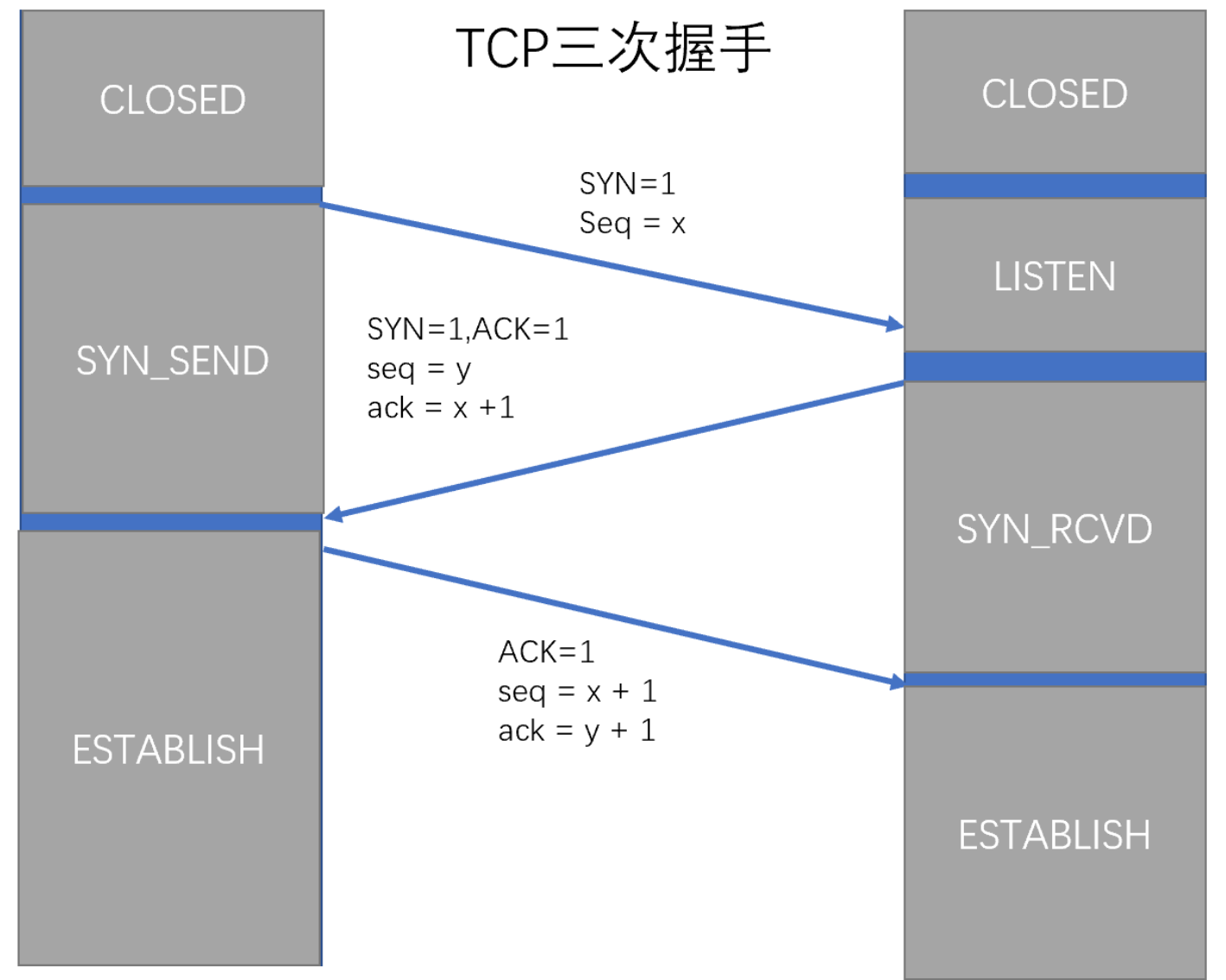
**第五题：**请详细介绍一下TCP的三次握手机制。并通过实例说明TCP握手为什么是三次，为什么不能是两次？不能是四次？

**TCP三次握手过程：**

第一次握手：开始前两端都处于CLOSED状态，用户端将标志位SYN置为1并生成一个值seq=x，并将报文段发送给服务器端，用户端进入SYN-SENT状态，等待服务器端确认。

第二次握手：服务器端收到报文段后由标志位SYN=1可以知道用户端请求建立连接，然后服务器端将标志位SYN和ACK都置为1、ack=x+1、生成一个值seq=y，并将该报文段发送给C用户端以确认连接请求，然后服务器端进入SYN-RCVD状态，此时操作系统为该TCP连接分配TCP缓存和变量。

第三次握手：用户端收到确认后，检查ack是否为x+1，ACK是否为1，如果正确则将标志位ACK置为1，ack=y+1，并且此时操作系统为该TCP连接分配TCP缓存和变量，并将该报文段发送给服务器端，服务器端检查ack是否为y+1，ACK是否为1，如果正确则连接建立成功，用户端和服务器端都进入ESTABLISHED状态，完成三次握手。



图源：csdn

**为什么是三次：**

首先讨论为什么不是两次：

如果使用两次握手：无法防止历史连接的建立，会造成资源浪费，不能同步双方序列号。

假设我们发送端前面发送了一个序列号为90的syn报文，此时网络中拥塞了，此时发送端可能会连续发起多次请求。但是此时的序列号为90的报文也到了，如果是两次握手的话，接收端接受到就会进入establelisten状态(进入这个状态后就可以发送数据)，然而当发送方判断这是一个历史连接，发送RST报文终止连接，但此时服务端已经进入了establelisten状态，并且可能发送了数据。断开的话，白白造成了服务端的资源浪费。

三次握手的话，客户端发送一个syn报文，服务端接受到后发送syn+ack报文，表示客户端的初始化序列号已经收到。客户端在回复ack报文，表示服务端的初始化序列号也已经收到。这样才能确保双方序列号都被同步了。如果是两次握手，只能保证一方的序列号被成功接收

为什么不是4次

会造成资源浪费

TCP握手必须是三次而不是四次的原因：由于三次握手已经能够正确建立连接，期间服务器有一次确认连接请求的操作就已经足够了，从而没必要再进行多次地确认，所以如果使用四次握手将会会导致对资源的浪费。

总结：2次不够，3次足够，4次多余。**第六题：**请详细介绍TCP四次挥手过程，并通过实例说明TCP挥手为什么需要四次呢？另外，TCP四次挥手过程中，为什么需要等待2MSL,才进入CLOSED关闭状态？

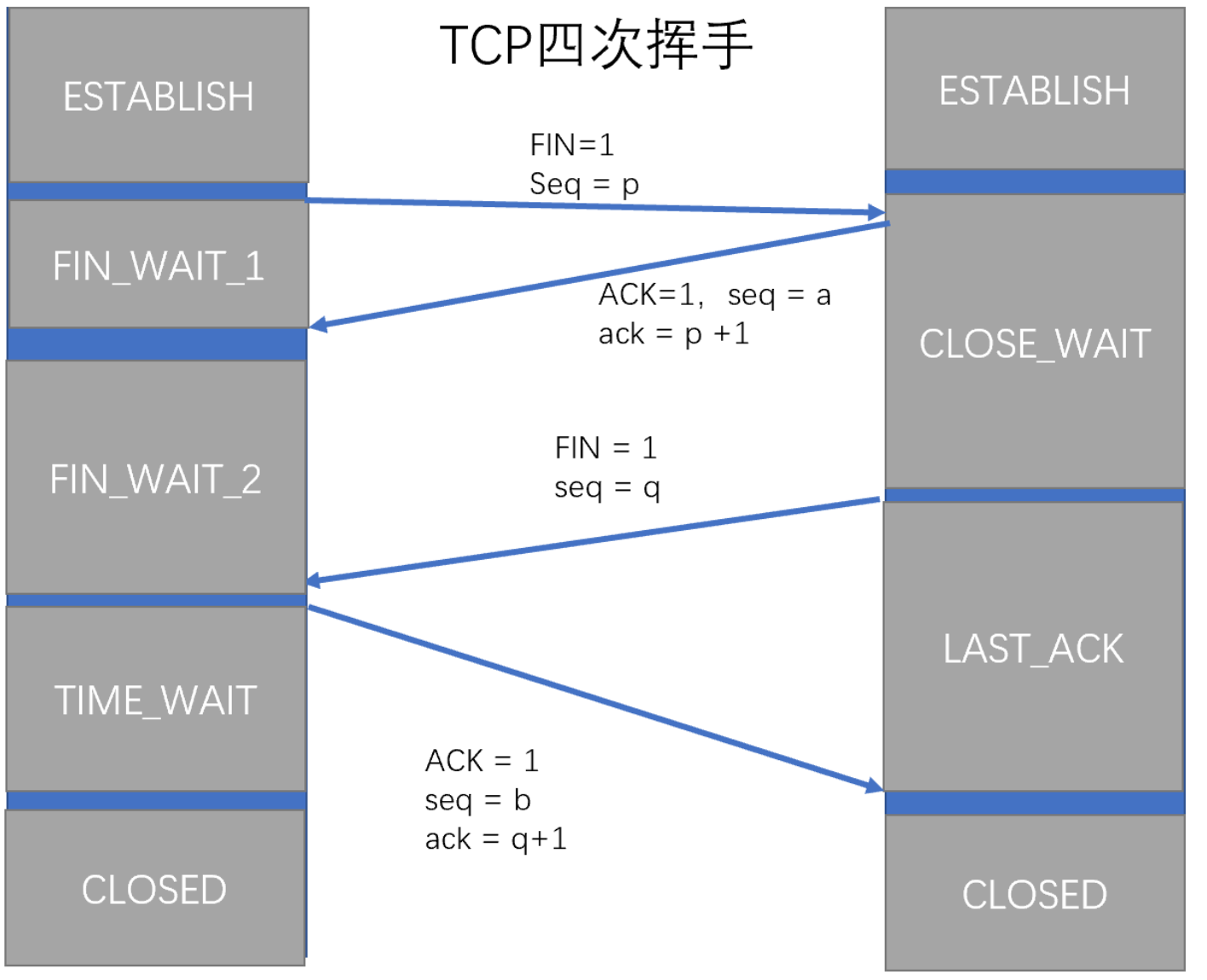
TCP四次挥手机制详细过程如下：

第一次挥手：用户端的应用进程发出连接释放报文段（FIN=1，序号seq=u），并停止再发送数据，主动关闭TCP连接，进入FIN-WAIT-1状态，等待服务器端的确认。

第二次挥手：服务器端收到连接释放报文段后即发出确认报文段，（ACK=1，确认号ack=u+1，序号seq=v），服务器端进入CLOSE-WAIT状态，此时的TCP处于半关闭状态，从用户端到服务器端的连接释放成功。

第三次挥手：用户端收到服务器端的确认后，进入FIN-WAIT-2状态，等待服务器端发出的连接释放报文段。服务器端发出连接释放报文段（FIN=1，ACK=1，序号seq=w，确认号ack=u+1）后进入LAST-ACK状态，等待用户端的确认。

第四次挥手：用户端收到服务器端的连接释放报文段后，发出确认报文段（ACK=1，seq=u+1，ack=w+1），用户端进入TIME-WAIT状态。然而此时TCP还未释放掉，需要经过时间等待计时器设置的时间2MSL后，用户端才会进入CLOSED状态，完成四次挥手。



图源：csdn

**四次挥手的原因：**

“三次握手”的第二次握手发送SYN+ACK回应第一次握手的SYN，但是“四次挥手”的第二次挥手只能发送ACK回应第一次挥手的FIN，因为此时Server可能还有数据传输给Client，所以Server传输数据完成后才能发起第三次挥手发送FIN给Client，等待Client的第四次挥手ACK。

**需要等待2MSL的原因：**

第一：为了保证服务端能收到客户端的确认应答。

若客户端发完确认应答后直接进入CLOSED状态，那么如果该应答丢失，服务端等待超时后就会重新发送连接释放请求，但此时客户端已经关闭了，不会作出任何响应，因此服务端就无法正常关闭。

第二：防止类似与“三次握手”中提到了的“已经失效的连接请求报文段”出现在本连接中。

客户端发送完最后一个确认报文后，在这个2MSL时间中，就可以使本连接持续的时间内所产生的所有报文段都从网络中消失。这样新的连接中不会出现旧连接的请求报文。

**第七题：**与UDP相比，TCP提供了可靠传输、流量控制和拥塞控制等服务。TCP协议是如何保证可靠传输的？谈谈你对停止等待协议、ARQ协议和滑动窗口协议的理解？

**TCP协议保证可靠传输的方法：**

1.确认应答与序列号：

序列号：TCP传输时将每个字节的数据都进行了编号，这就是序列号。

确认应答：TCP传输的过程中，每次接收方收到数据后，都会对传输方进行确认应答。也就是发送ACK报文。这个ACK报文当中带有对应的确认序列号，告诉发送方，接收到了哪些数据，下一次的数据从哪里发。

序列号的作用不仅仅是应答的作用，有了序列号能够将接收到的数据根据序列号排序，并且去掉重复序列号的数据。这也是TCP传输可靠性的保证之一。

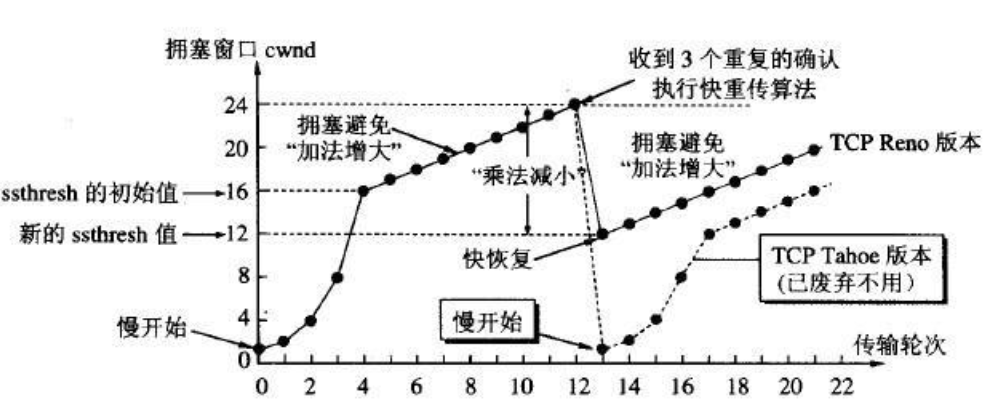
2.超时重传：

发送方在发送完数据后等待一个时间，时间到达却没有接收到ACK报文，则对刚才发送的数据进行重新发送。

3.流量控制：接收端在接收到数据后，对其进行处理。如果发送端的发送速度太快，导致接收端的接收缓冲区很快的填充满了。此时如果发送端仍旧发送数据，那么接下来发送的数据都会丢包，继而导致丢包的一系列连锁反应。而TCP根据接收端对数据的处理能力，决定发送端的发送速度，这个机制就是流量控制。

当接收方来不及处理发送方的数据时，能通过滑动窗口使发送方降低发送的速率，防止包丢失。

4.拥塞控制：防止网络层拥堵造成拥塞，包括慢启动、拥塞避免、快速重传、快速恢复四种机制。



5.合理分片：TCP会按最大传输单元(MTU)合理分片，接收方会缓存未按序到达的数据，重新排序后交给应用层。

6.数据校验：TCP报文头有校验和，用于校验报文是否损坏。

**停止等待协议：**

一次只能发一个帧

是最简单的可靠传输方法，每发完一个分组就停止发送，等待对方的确认，只有在对方在确认后才能再发送下一个分组。如果出现丢失，有两种方法进行确定，一是超时后，发送“未收到”，进行重发；二是规定一个时间没收到就重发。

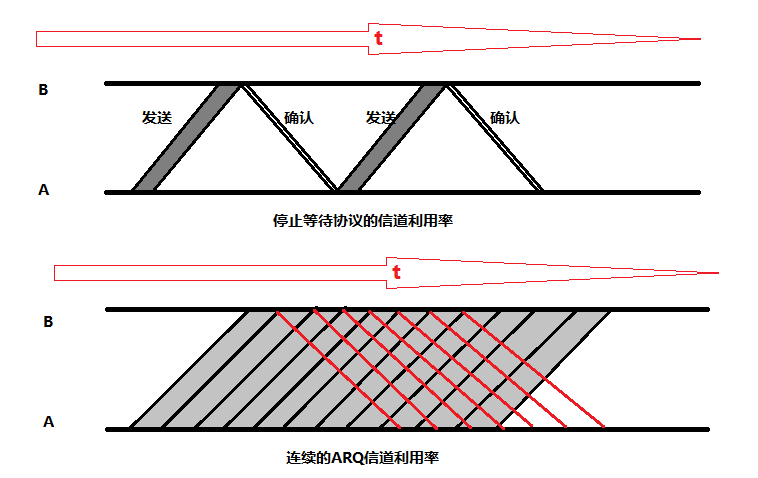
这种方法这种方法效率非常低下，但是可靠性确实是得到了保证。

**ARQ协议：**

一次可发多帧

即自动重传请求协议，包括停止等待ARQ协议和连续ARQ协议。

通过使用确认和重传机制，在不可靠服务的基础上实现可靠的信息传输。如果发送方在发送后一段时间之内没有收到确认帧，则会重新发送数据；且重传的请求是自动进行的，接收方不需要请求发送方重传某个出错的分组。



连续ARQ协议通常是借助滑动窗口协议运行的。

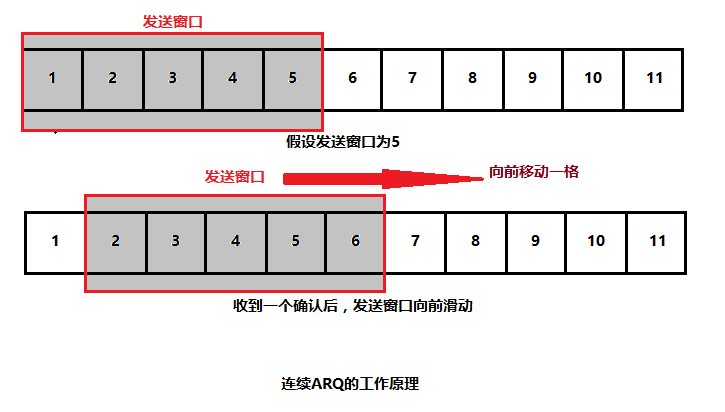
**滑动窗口协议：**

接收方可以接收多帧

发送方：维持一个固定长度的窗口，只有收到一个最左边的确认帧才对窗口进行右移。

接收端：收到数据帧的发送序号落入接收窗口内, 才允许将该数据帧收下，否则一律丢弃。

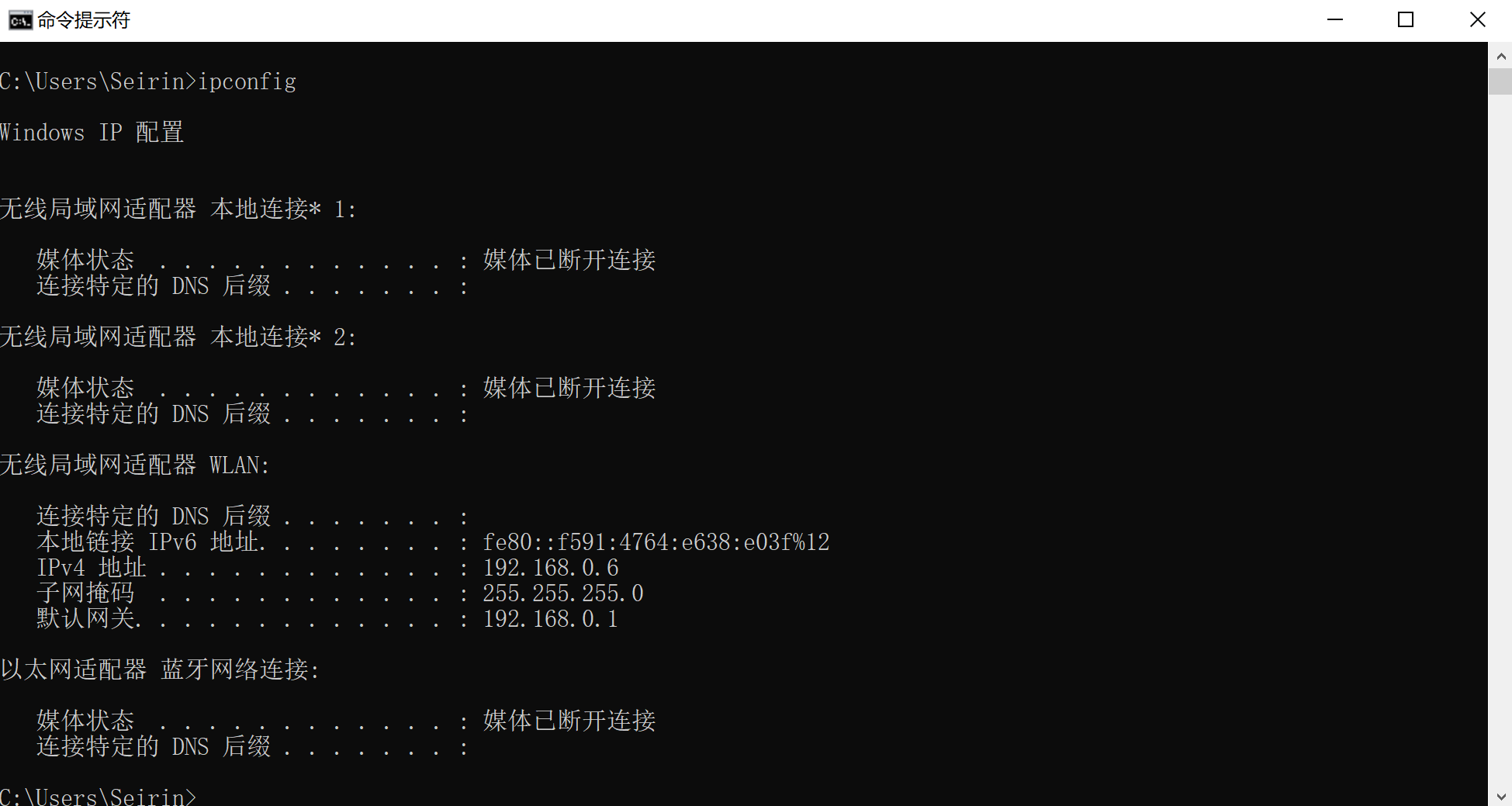
之所以叫滑动窗口协议,是因为窗口是不断向前走的，该协议允许发送方在停止并等待确认前发送多个数据分组。由于发送方不必每发一个分组就停下来等待确认，因此该协议可以加速数据的传输，还可以控制流量的问题。



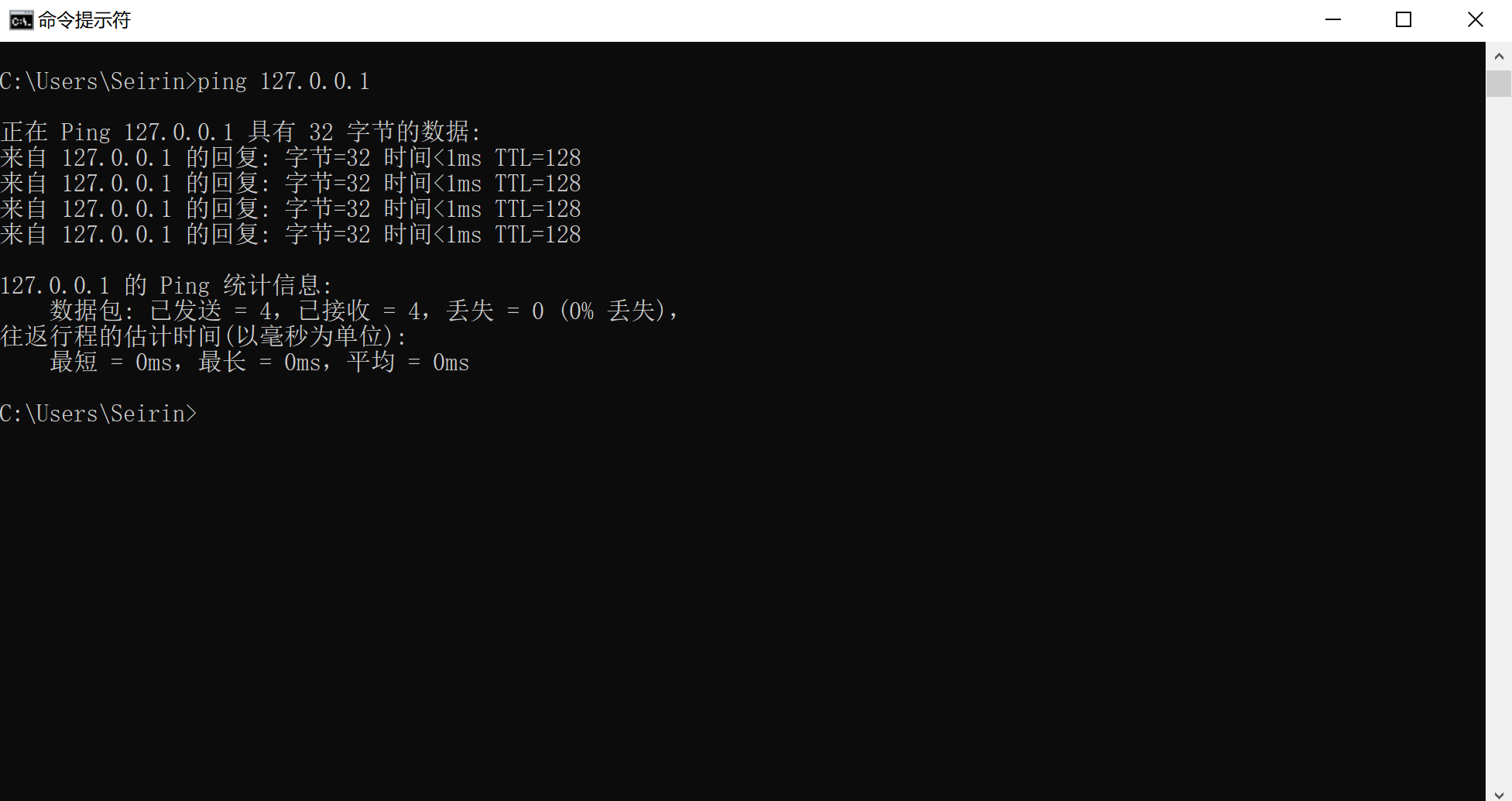
本题图源：PPT与csdn

**第八题：**做到这道题目，你突然发现网络变慢，所以你想通过ICMP协议做一些简单的网络诊断。

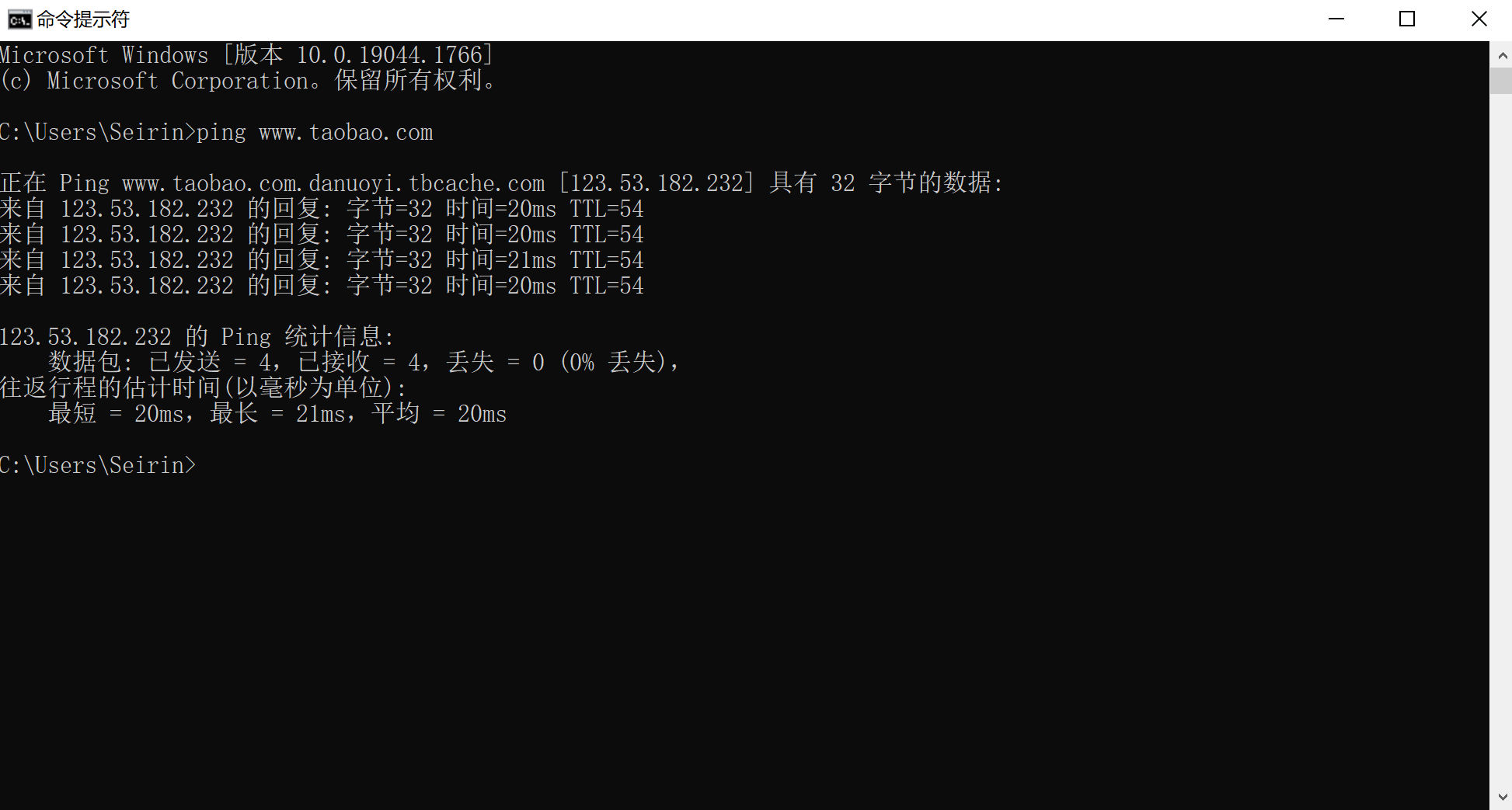
首先你要查看本机网络适配器的全部配置信息，请在console中完成此任务，并将结果截图（需包含完整console边框）粘贴于此：



接下来，在console内继续进行本机回路测试，请将结果截图（需包含完整console边框）粘贴于此：



在确定本机回路畅通后，你又使用相同的命令对淘宝网主页进行了连通性测试，请将结果截图（需包含完整console边框）粘贴于此：

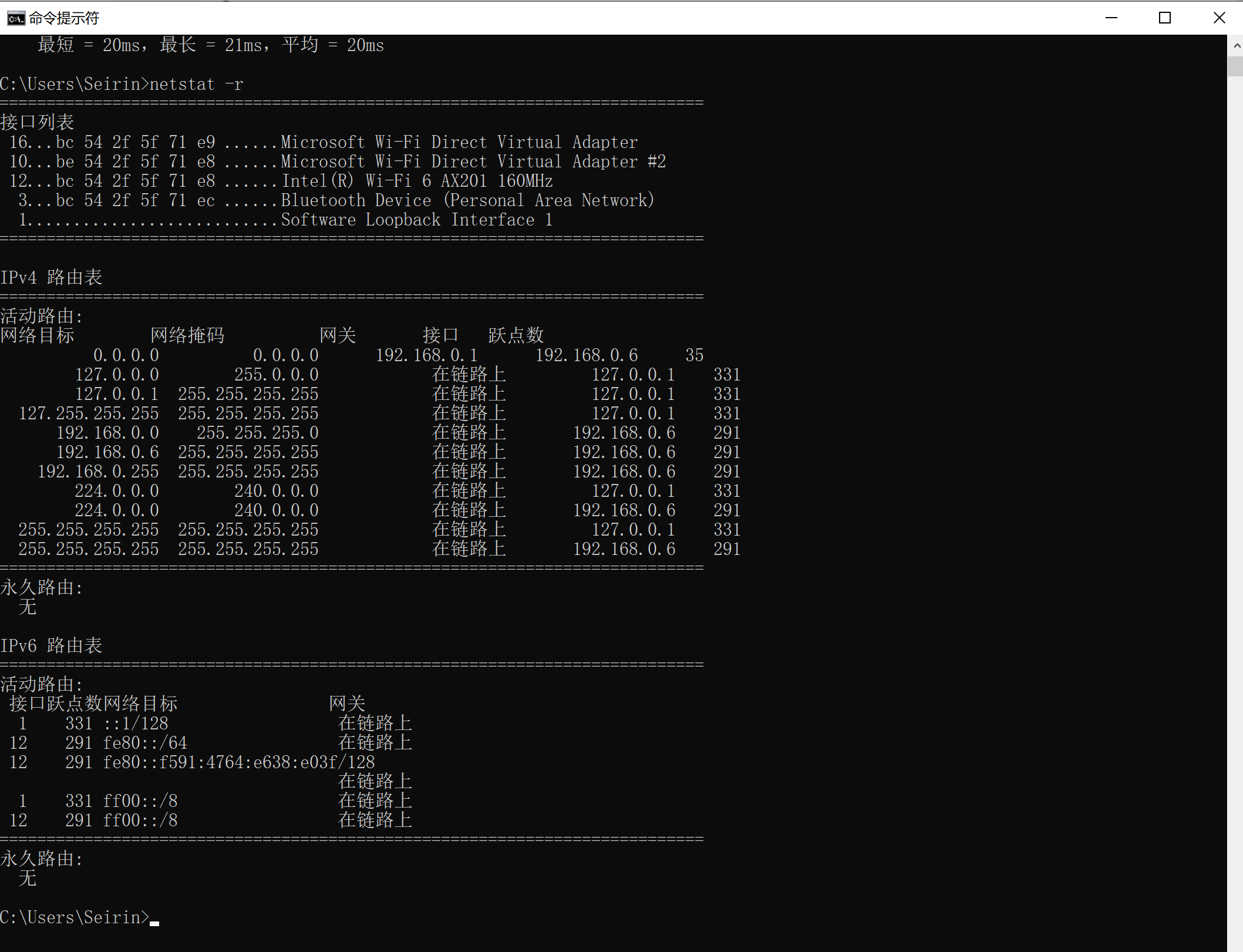


比较本机回路测试和远程主机连通性测试的结果，你都有哪些发现？

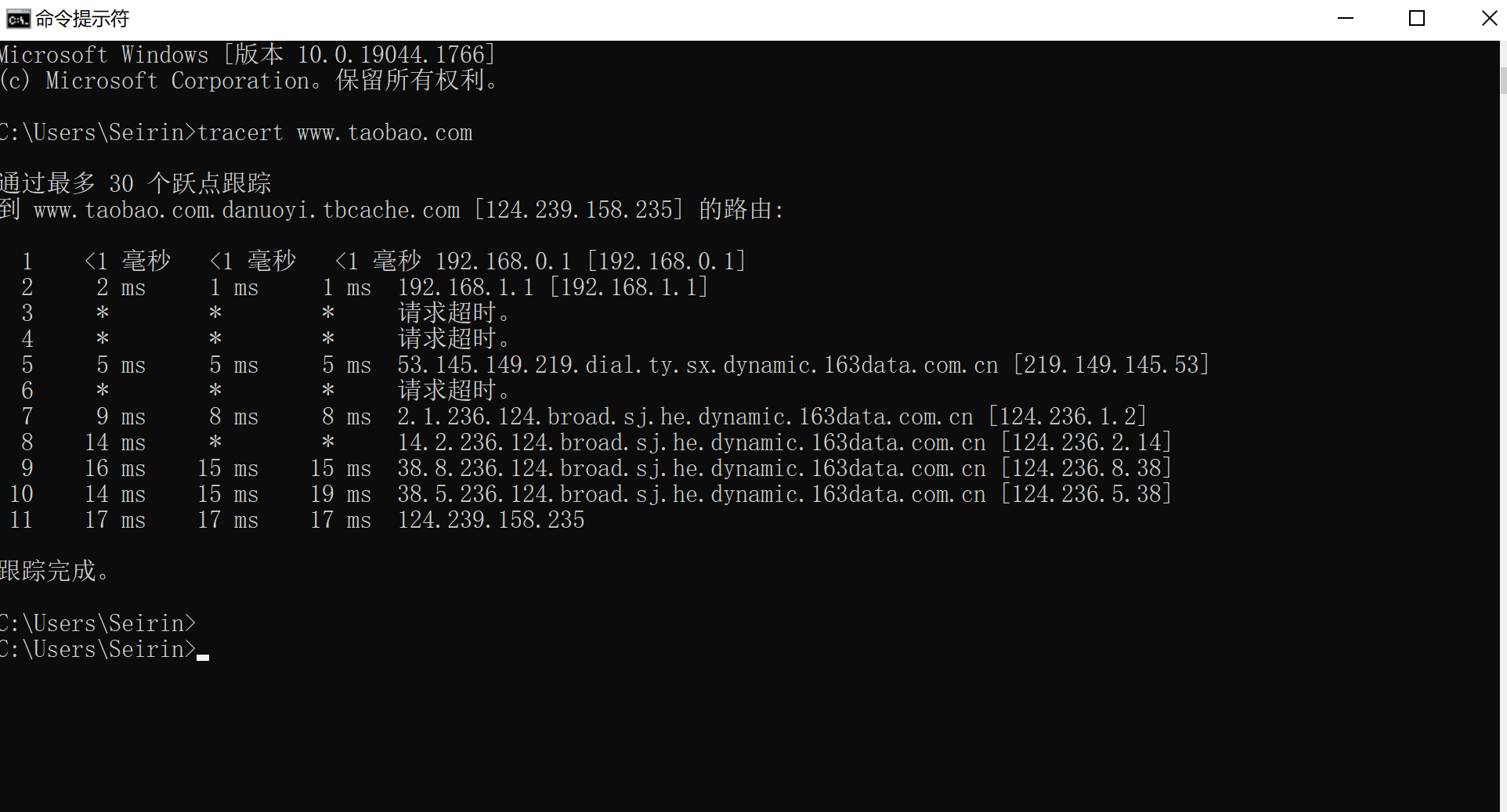
本机回路测试和远程主机连通性测试中数据包的发送和接收数量都是4个，丢包率为0，说明回路畅通；而远程主机连通性测试往返时间明显多于本机回路测试往返时间，说明本机访问速度快于远程访问速度。

**第九题：**确定链路连通正常后，你猜测网络卡顿可能是由于路由延迟产生的，那么接下来你将通过console命令对路由信息进行测试。

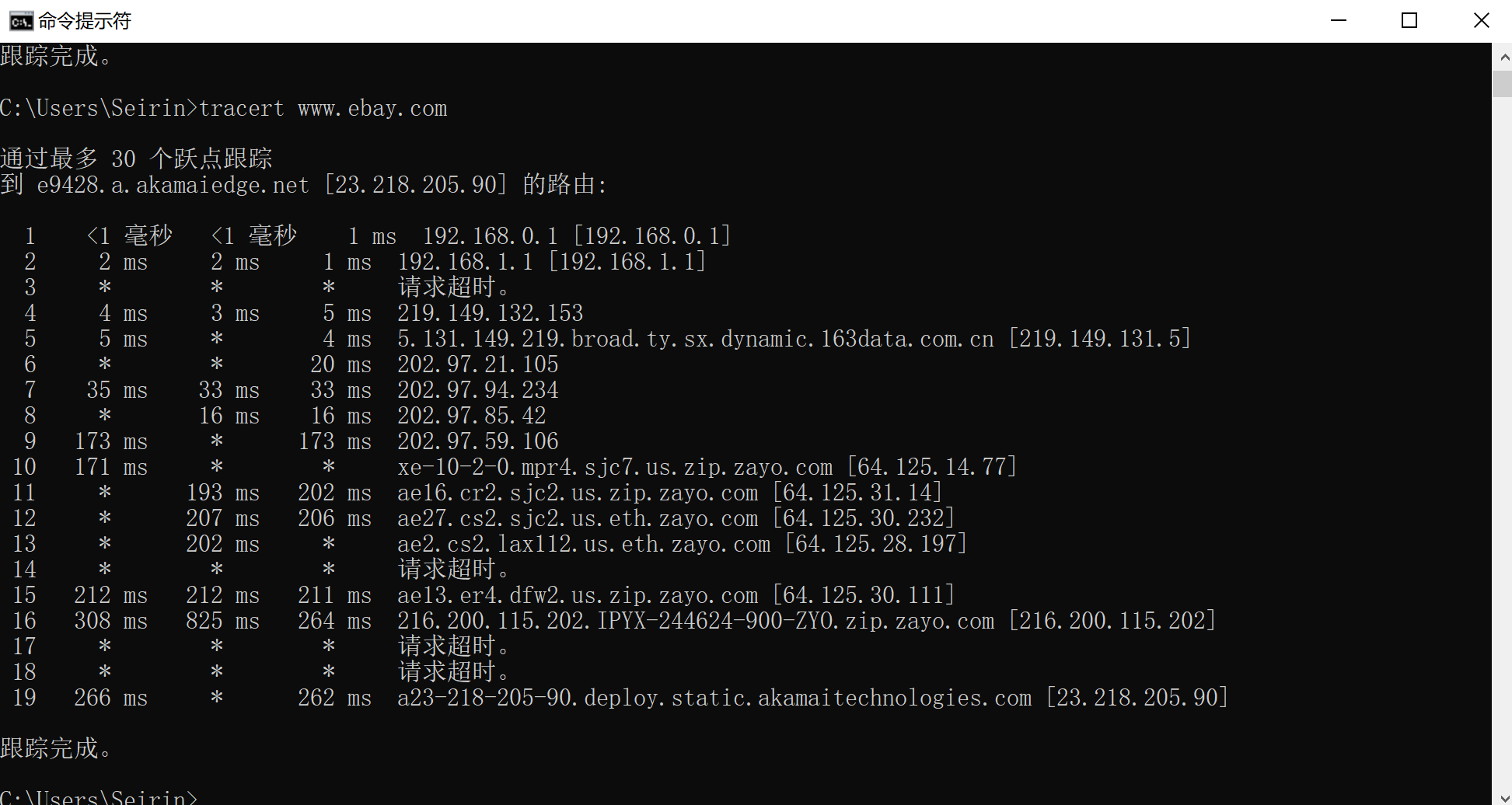
首先，请显示本机路由表信息，将结果截图（需包含完整console边框）粘贴于此：



接下来，你要探测从本机到淘宝网服务器的路由信息，请将结果截图（需包含完整console边框）粘贴于此：



这时，你发现淘宝网上没有找到你想找的东西，想要再去ebay（www.ebay.com）逛一逛，请探测本机到ebay服务器的路由信息，并将结果截图（需包含完整console边框）粘贴于此：



请观察两次路由探测的结果，分析其中的异同点：

两次路由探测过程中均出现了请求超时；探测从本机到淘宝网服务器的路由信息所需要经过的节点数少于探测从本机到ebay服务器的路由信息所需要的节点数，且前者消耗的总时间明显少于后者所消耗的时间。

**第十题：**这时，细心的你可能会发现，访问淘宝网的URL协议并不是我们常见的HTTP，而是HTTPS。那么，什么是HTTPS？HTTPS与HTTP的区别何在？请用借助图表描述HTTPS的实现流程。

　HTTPS(全称：Hyper Text Transfer Protocol over Secure Socket Layer)，是以安全为目标的HTTP通道，简单讲是HTTP的安全版。HTTPS相当于在HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。 它是一个URI scheme(抽象标识符体系)，句法类同http:体系。用于安全的HTTP数据传输。

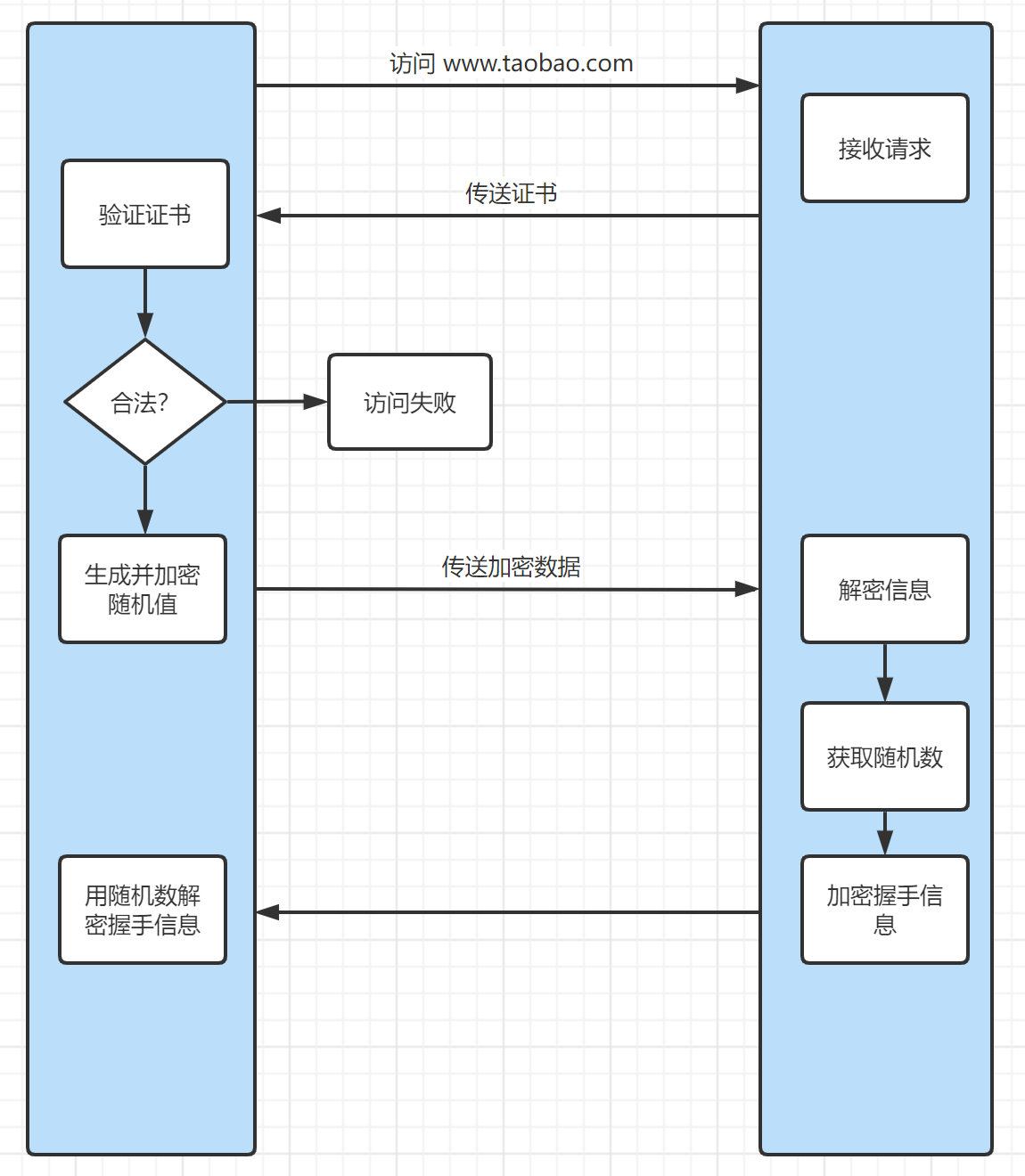
HTTPS与HTTP的区别如下：

1、"HTTP"和"HTTPS"都是超文本传输协议，但不同的是"HTTPS"是加安全协议，所以跟多用于敏感的通信，比如交易场景。

2、HTTPS主要由两部分组成：HTTP+ SSL / TLS，也就是在 HTTP上又加了一层处理加密信息的模块。

3、HTTPS协议是由SSL+ HTTP构建的可进行加密传输、身份认证的网络协议，要比 HTTP安全，可防止数据在传输过程中被窃取、改变，确保数据的完整性。

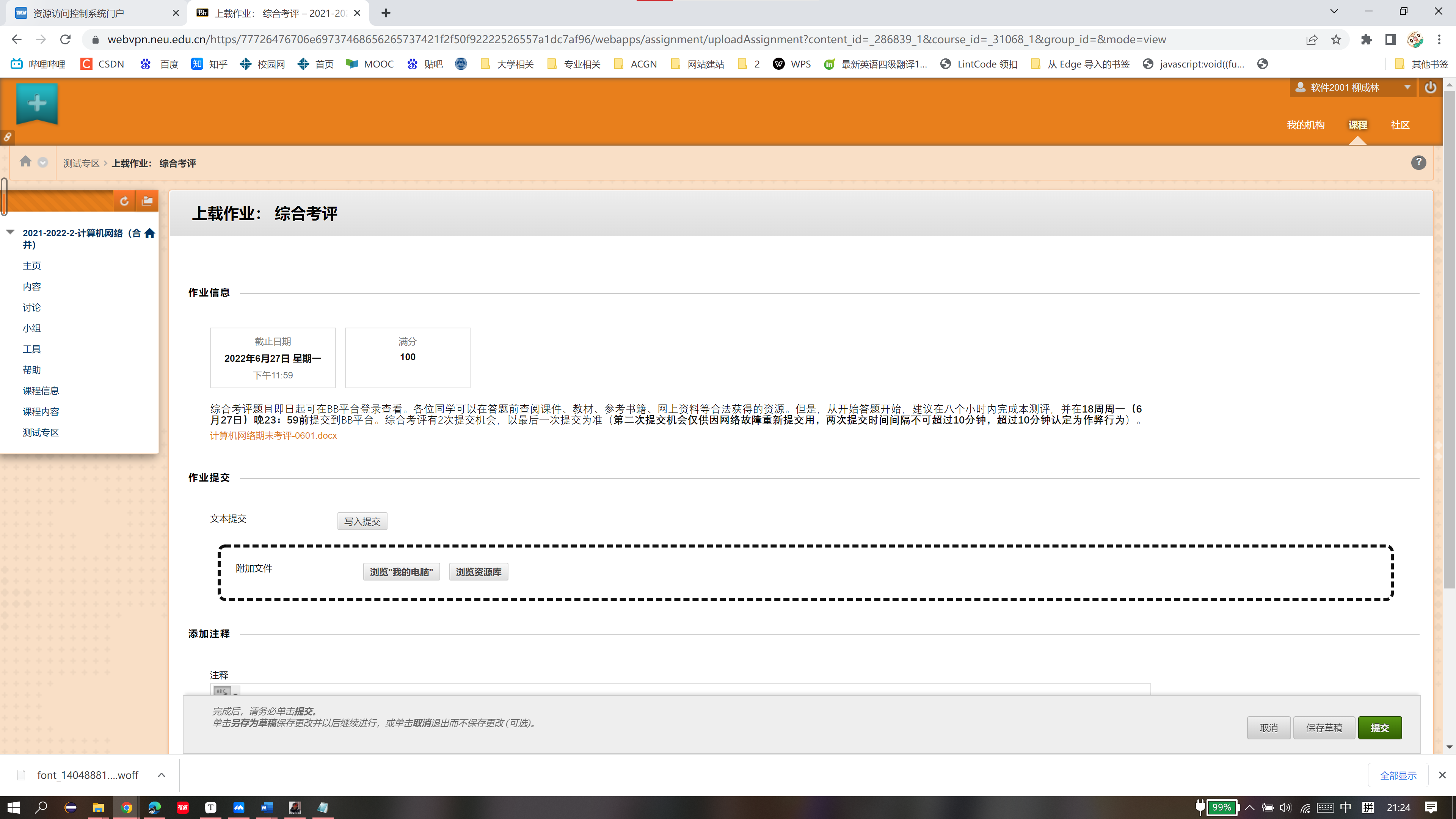
HTTPS访问淘宝的实现流程如下：（流程图为本人绘制）



用户端发起HTTPS请求：访问服务器端的https://www.taobao.com地址。

服务器端一般具有自己的公钥和私钥，当服务器端收到请求后给用户端发送证书，其中包含公钥等信息。然后用户端验证公钥的有效性，如果发现异常则会进行警告提醒，如果证书没有问题则生成一个随机值，然后公钥对该随机值进行加密，并将加密后的随机值传递给服务器端。之后服务器端用私钥解密得到用户端传过来的随机值，然后使用该随机数对握手信息进行对称加密，并将数据传递给用户端，在用户端接收之后可以用之前生成的随机数解密该数据。以上过程中，由于数据一直是加密的，所以即使第三方获取到数据也无法知道其详细内容。

至此，你已经完成了本次期末考评的全部任务。为了确保你能够正常提交本文档，请使用浏览器登录BlackBoard平台，进入计算机网络（合并）课程，点击“测试专区”，确保你能看到本次任务的提交入口，请将你的包含桌面状态栏和完整浏览器页面在内的完整桌面截图贴在此处：



完成时间：2022-6-26 21:24