计算机网络体系结构实验报告

选课序号 42 专业 网络工程 班级 2班 学号 2220193626 学生姓名 李子毅 课程名称计算机网络体系结构实验 实验时间 2021.7.12

实验名称 web服务器实验 实验成绩

1. 实验内容

1．新建一个 web 站点，局域网内的计算机均可访问该站点；

2．采用虚拟主机技术在同一台服务器上建立多个 Web 站点；

3．在一个站点下建立多个子站点，实现方法：虚拟目录实现；

4．对站点进行安全管理，如设置浏览权限、身份验证、IP 限制等。

二、实验目的

掌握用 Windows 服务器 2003 自带的 IIS 6.0 Web 服务器配置方法；正确理解 Web 服务器

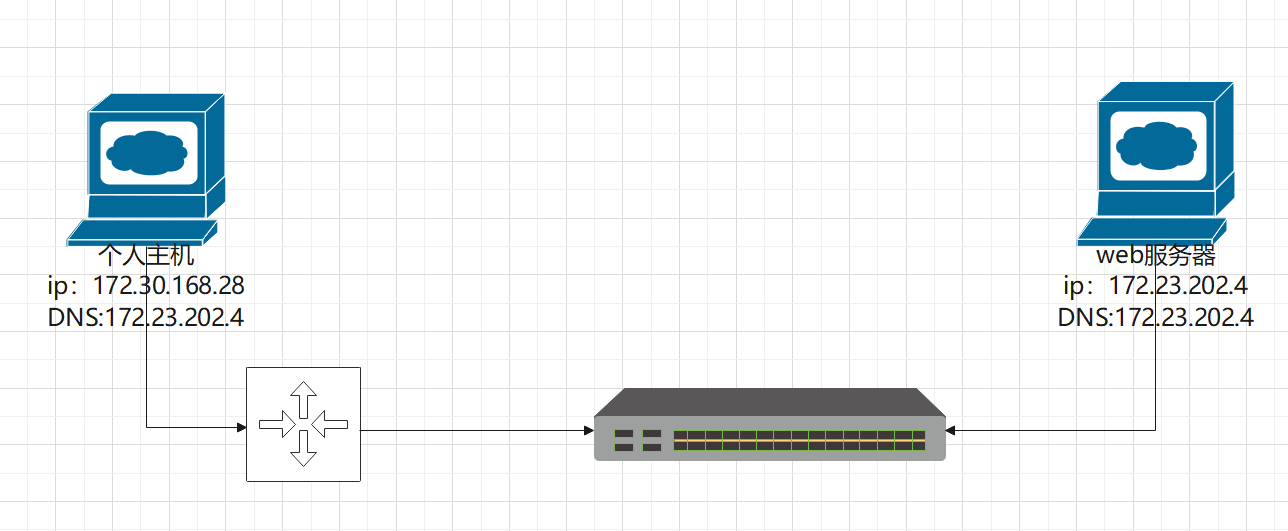
的概念及功能。

三、实验环境

1.实验设备：实验室主机一台，用作web服务器端；个人主机一台，用作客户端。

2.实验工具：windows server2003 、wireshark抓包工具

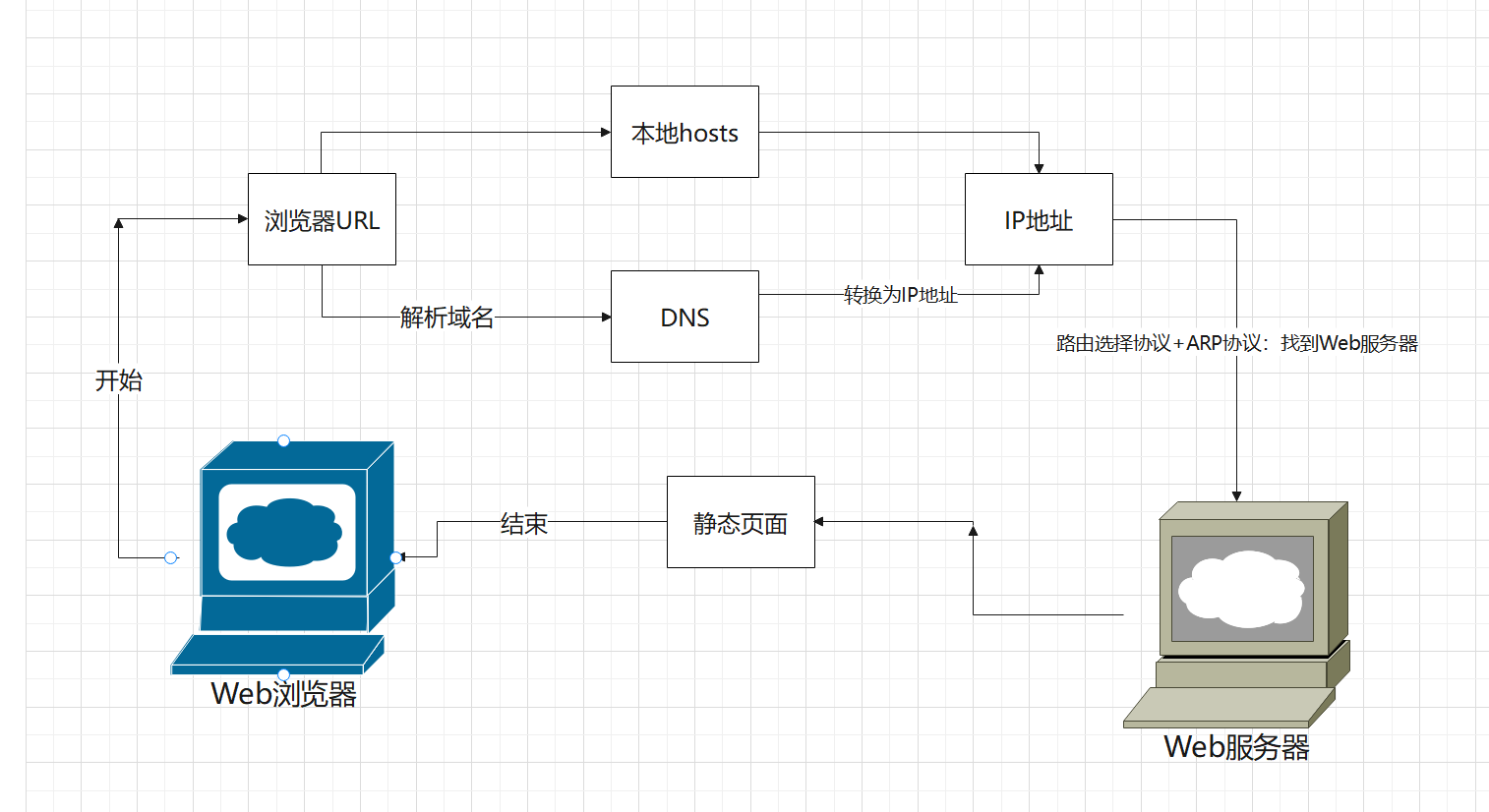
3.实验拓扑：



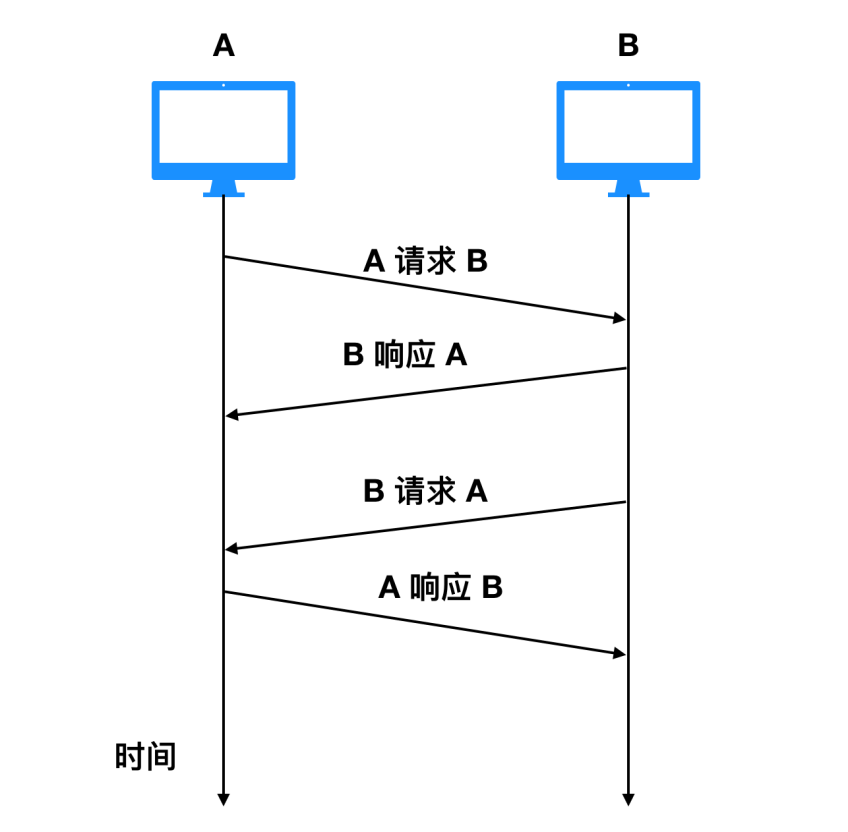
三、实验原理

1.Web站点的访问原理：客户端访问页面的时候是在地址栏上输入一个网然后再通过DNS服务器找到IP地址，返回到客户端然后找到WEB服务器，找到之后建立TCP连接，然后发出http请求，请求的是页面。对于服务器而言，做完网页之后要在这个站点上线，上线就是把网站复制到这个服务器中指定的地方，别人就可以访问了，访问的时候，会把页面的请求到客户端的浏览器中。

**请求静态页面的原理图解如下：**



1. HTTP协议及原理：
   1. HTTP的定义：超文本传输协议，是一个基于请求与响应，无状态的，应用层的协议，常基于TCP/IP协议传输数据，互联网上应用最为广泛的一种网络协议,所有的WWW文件都必须遵守这个标准。设计HTTP的初衷是为了提供一种发布和接收HTML页面的方法。在本次实验中，当web浏览器发送HTTP请求来向web服务器请求一个页面时，就使用到了此协议，在现实中，往往一方既发送请求又得到响应请求，效果如图所示：

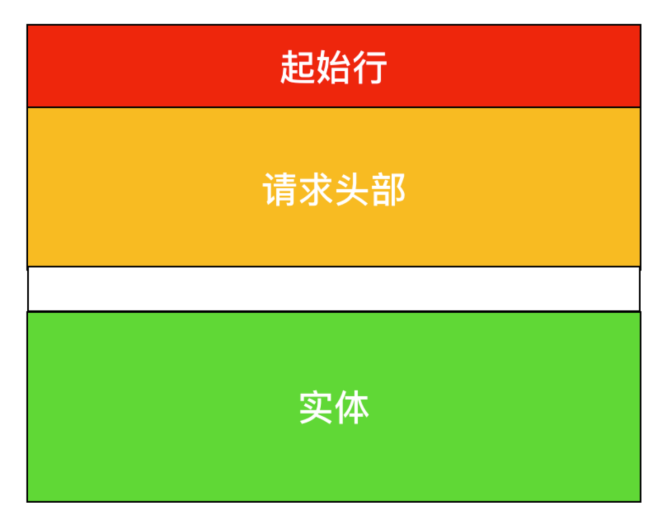


* 1. HTTP报文结构：

HTTP 协议主要由三大部分组成：

* 起始行（start line）：描述请求或响应的基本信息；
* 头部字段（header）：使用 key-value 形式更详细地说明报文；
* 消息正文（entity）：实际传输的数据，它不一定是纯文本，可以是图片、视频等二进制数据。

其中起始行和头部字段并成为 请求头 或者 响应头，统称为 Header；消息正文也叫做实体，称为 body。HTTP 协议规定每次发送的报文必须要有 Header，但是可以没有 body，也就是说头信息是必须的，实体信息可以没有。而且在 header 和 body 之间必须要有一个空行（CRLF），如图所示：



**在接下来的实验步骤中，我将采用wireshark进行抓包验证并详解HTTP报文结构**。

* 1. HTTP工作流程：

本实验中，访问的 URL 地址为 http://www.2220193626.com，当输入网址并点击回车时，浏览器内部会进行如下操作：

DNS服务器会首先进行域名的映射，找到访问http://www.2220193626.com所在的地址，然后HTTP 客户端进程在 80 端口发起一个到服务器 http://www.2220193626.com 的 TCP 连接（80 端口是 HTTP 的默认端口）。在客户和服务器进程中都会有一个套接字与其相连。

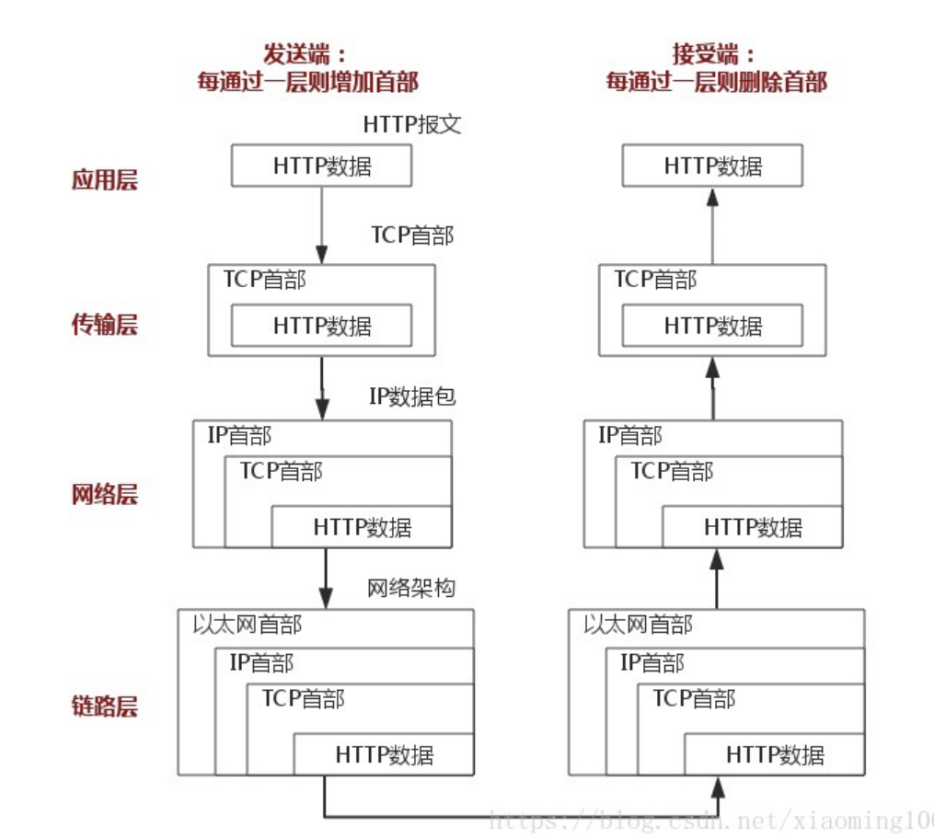
HTTP 客户端通过它的套接字向服务器发送一个 HTTP 请求报文。HTTP 服务器通过它的套接字接受该报文，进行请求的解析工作，并从其存储器(RAM 或磁盘)中检索出对象 http://www.2220193626.com/home.index，然后把检索出来的对象进行封装，封装到 HTTP 响应报文中，并通过套接字向客户进行发送。

HTTP 服务器随即通知 TCP 断开 TCP 连接，实际上是需要等到客户接受完响应报文后才会断开 TCP 连接。

HTTP 客户端接受完响应报文后，TCP 连接会关闭。HTTP 客户端从响应中提取出报文中是一个 HTML 响应文件，并检查该 HTML 文件，然后循环检查报文中其他内部对象。

检查完成后，HTTP 客户端会把对应的资源通过显示器呈现给用户。至此，键入网址再按下回车的全过程就结束了。

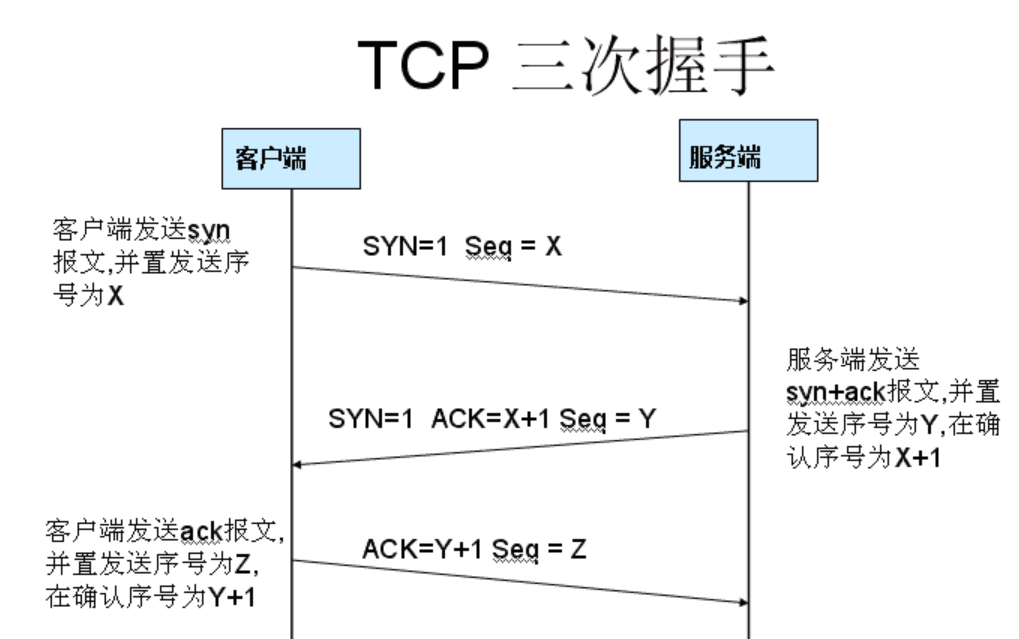
在这一过程中，数据的在各层结构中的传输如下图所示：



**上述过程描述的是一种简单的请求-响应全过程，具体的请求-响应情况可能要比上面描述的过程要复杂。**

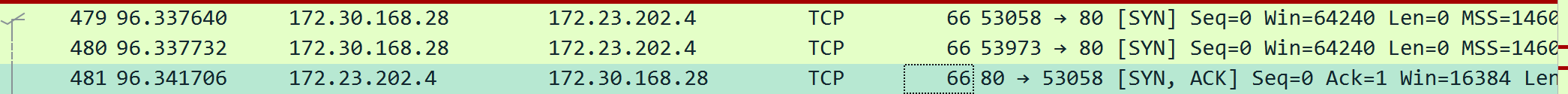
* 1. 三次握手与四次挥手过程：

在这一过程中，运输层通过TCP协议三次握手与服务器建立连接，通过四次挥手释放连接：

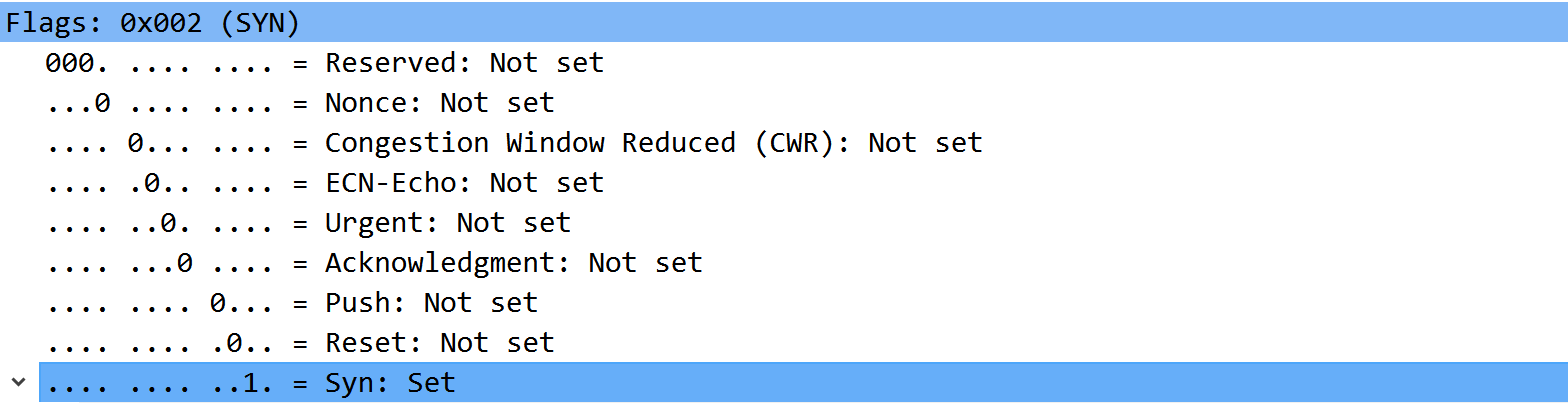


三次挥手的过程是了防止已失效的连接请求报文段突然又传送到了服务端，因而产生错误。比如:客户端发出的第一个连接请求报文段并没有丢失，而是在某个网络结点长时间的滞留了，以致延误到连接释放以后的某个时间才到达服务器。本来这是一个早已失效的报文段，但是服务器收到此失效的连接请求报文段后，就误认为是客户端再次发出的一个新的连接请求，于是就向客户端发出确认报文段，同意建立连接。假设不采用“三次握手”，那么只要服务器发出确认，新的连接就建立了，由于客户端并没有发出建立连接的请求，因此不会理睬服务器的确认，也不会向服务器发送数据，但服务器却以为新的运输连接已经建立，并一直等待客户端发来数据。所以没有采用“三次握手”，这种情况下服务器的很多资源就白白浪费掉了。

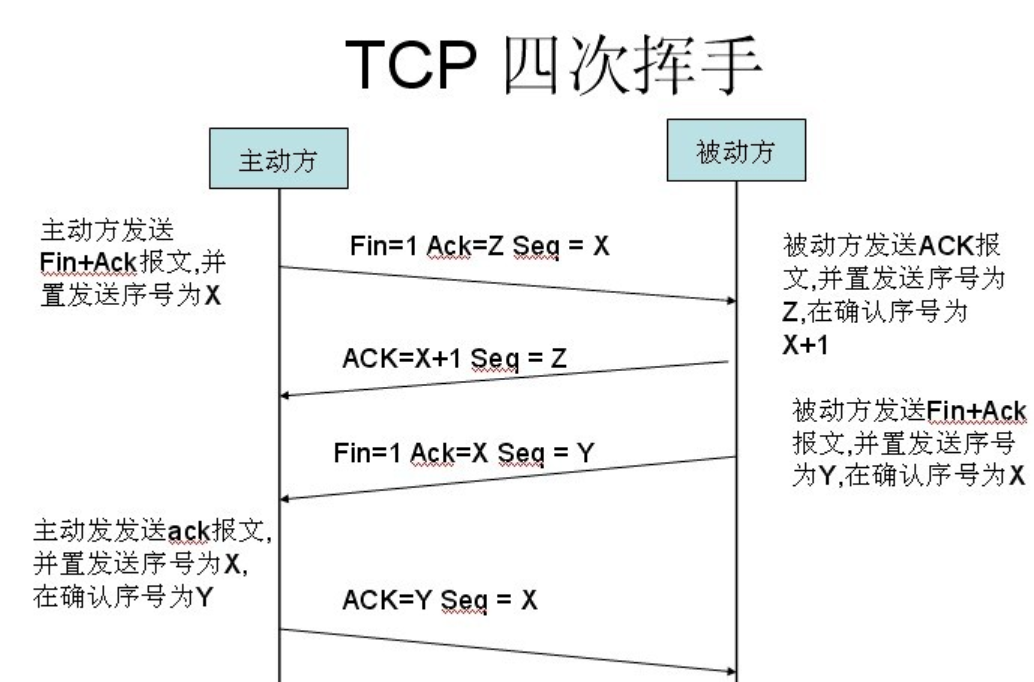
抓取TCP报文验证这一过程：



打开第一个报文，可以通过TCP报文的各个标志位的值得知该报文为三次握手过程中的连接请求报文：

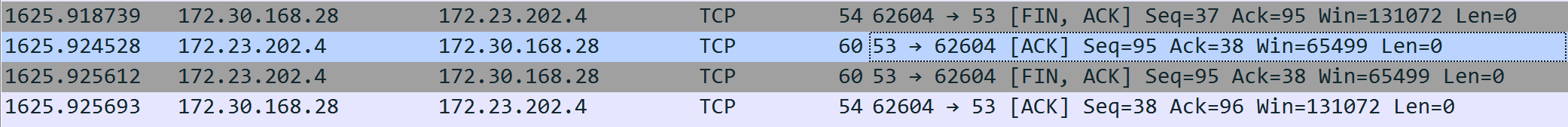


接下来是连接结束时的四次挥手过程：



四次挥手的原因是因为TCP是全双工模式，当客户端发出FIN报文段时，只是表示客户端已经没有数据要发送了，客户端告诉服务器，它的数据已经全部发送完毕了；但是，这个时候客户端还是可以接受来服务器的数据；当服务器返回ACK报文段时，表示它已经知道客户端没有数据发送了，但是服务器还是可以发送数据到客户端的；当服务器也发送了FIN报文段时，这个时候就表示服务器也没有数据要发送了，就会告诉客户端，我也没有数据要发送了，如果收到客户端确认报文段，之后彼此就会中断这次TCP连接。

同样我使用wireshark抓取了这一过程：



3.创建服务器的原理：利用 Window2003 自带的 IIS 6.0 服务功能，可以在 Windows server 2003 系统下建立最常用的 Web 服务器，实现最基本的浏览和文件传输功能。Web 服务器是在网络中实现信息发布、资料查询、数据处理等诸多应用的基本平台。Web 服务器采用的是客户／服务器传输模式，需要静态 IP 地址。服务器端装有提供 Web 服务的软件，并保存了用户所需的信息，但是一般在现实的应用场景中，服务器端一般采用linux系统。

客户端装有 Web 浏览器软件，本次实验中采用了edge浏览器，用于查看web服务器开设的网站。

四、实验过程

**1．建立一个网页文件：t1.htm。**

启动 word 应用程序，新建一个文件，输入字符后，将其存为网页文件，扩展名为 htm；

注意其保存路径。

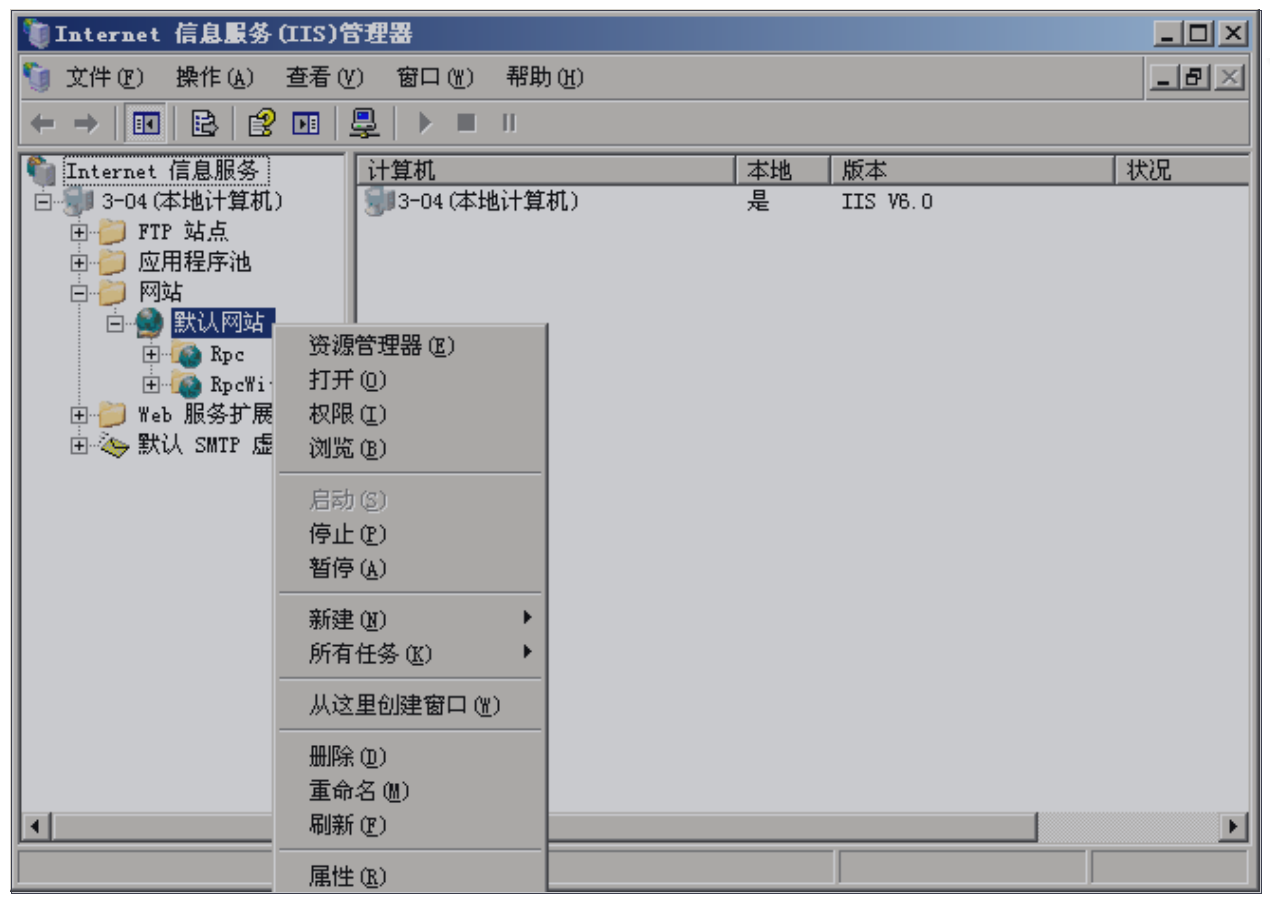
**2．打开 IIS 管理器：选“开始菜单→程序→管理工具→Internet 信息服务。**

（1）设置默认 Web 站点

IIS 安装完成后，系统会自动建立一个“默认网站”。当用户利用“http://IP 地址/”或“http://

域名/”来请求网页时，网站会自动将其“默认网站”中“主目录”中的默认网页传给用户的浏览

器。建立一个网站，“网站描述”中可以输入任何内容来描述所建立的网站。



**配置网站属性**

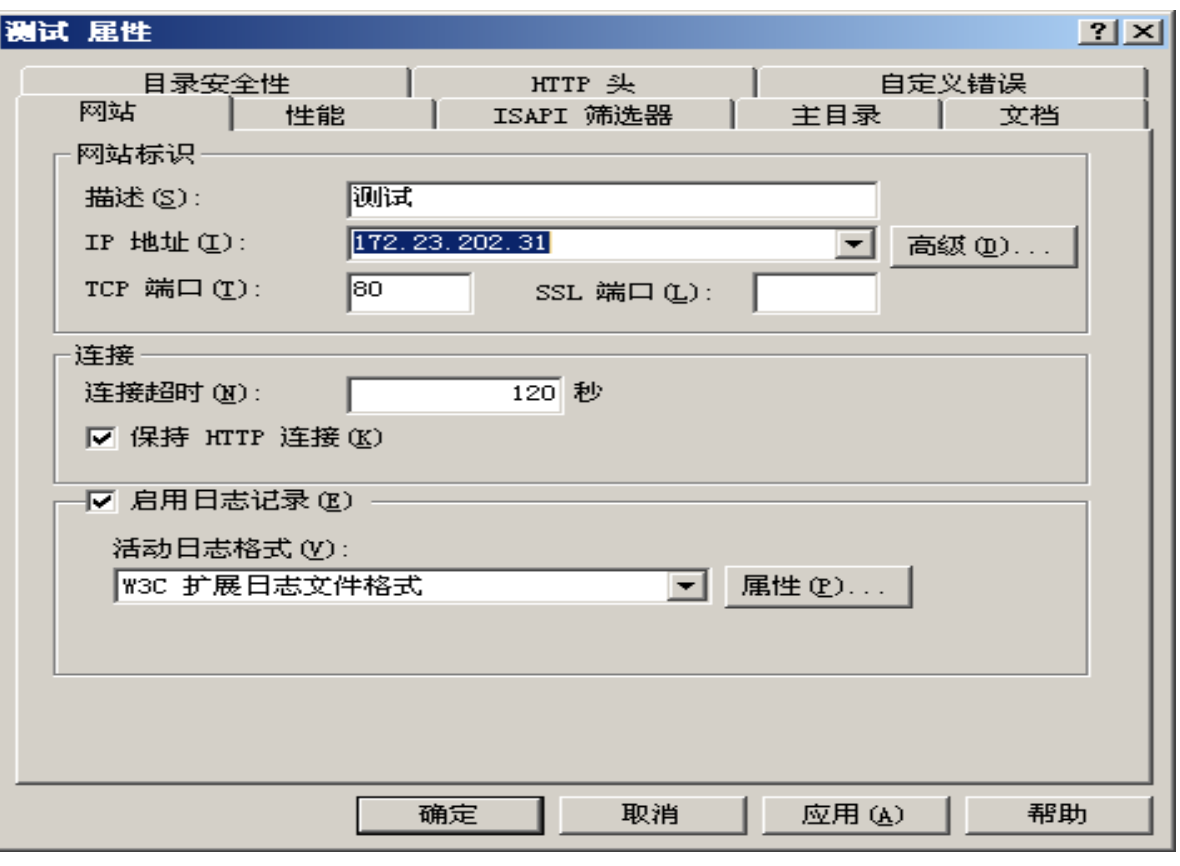
打开默认网站”的属性设置窗口：选“默认”→右键→属性”即可。

选择“网站”选项卡。“描述”中一般填写网站名称，要注意的是这里的网站名称不是指

Web 网站的域名，如本例中的“测试”；“IP 地址”：设置网站的 IP 地址，可以通过点击下拉

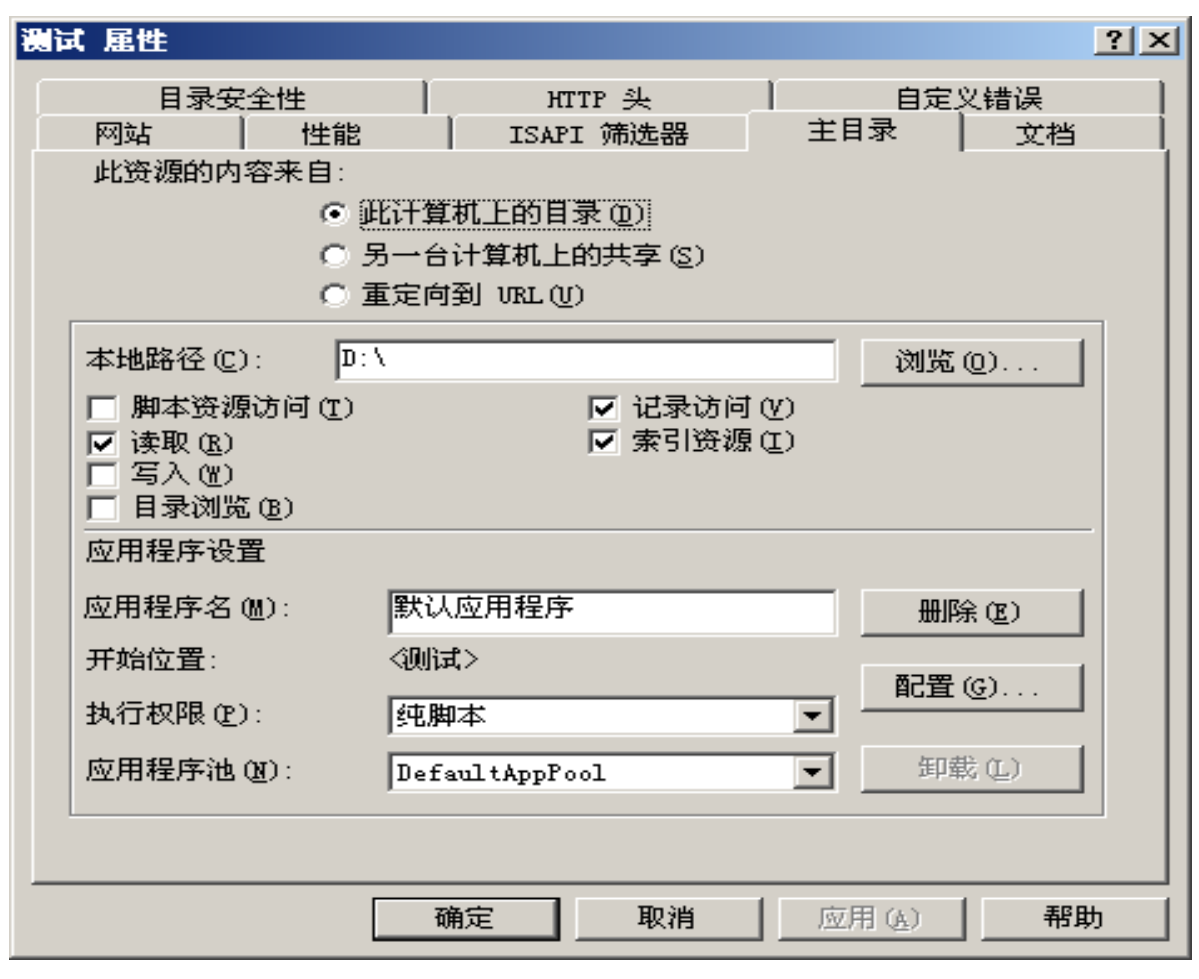
列表选择；“TCP 端口”：确定该 Web 网站所使用的 TCP 端口，默认值为 80，用户可以将该

端口更改为任意唯一的 TCP 端口号，但不要使用标准端口号（小于 1024 的端口号），本例中保持默认值“80”不变。



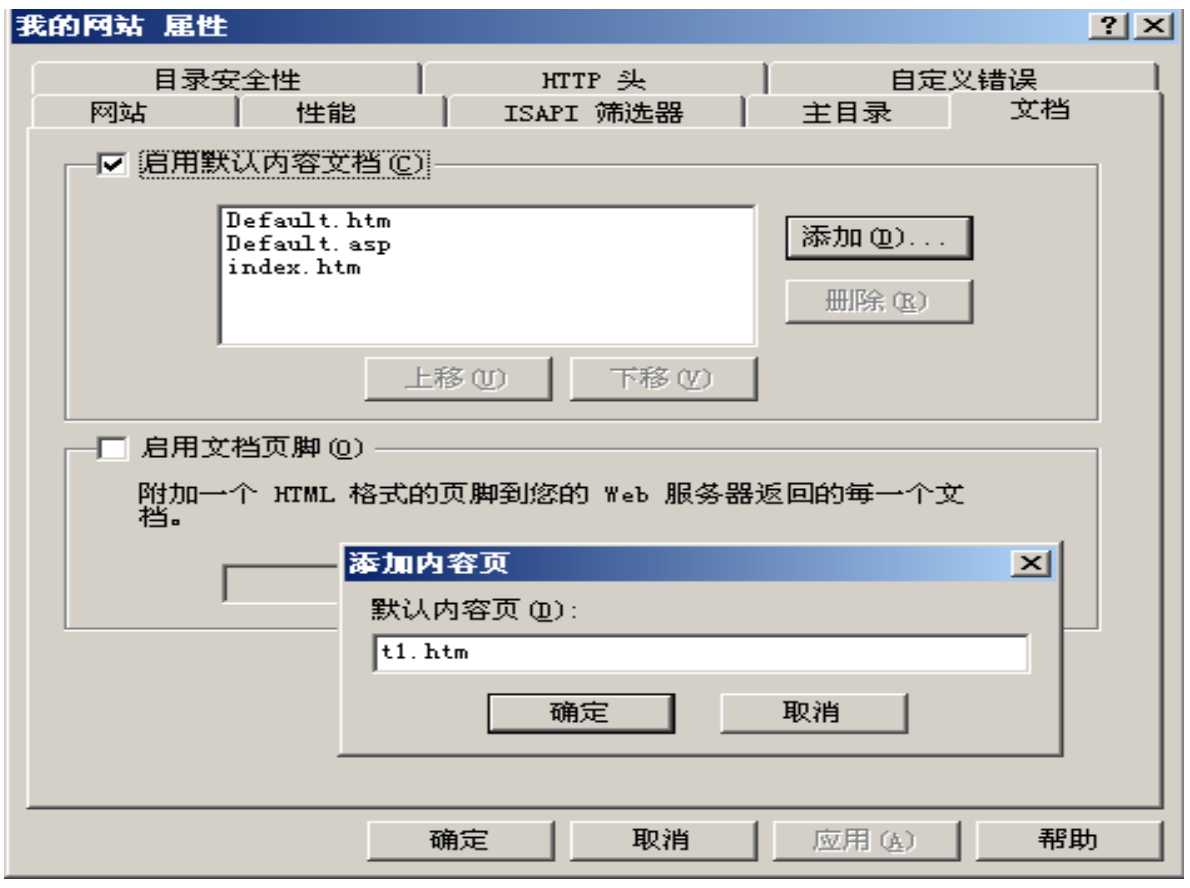
选择“主目录”选项卡。选择此计算机上的目录，在“本地路径”通过“浏览”

按钮来选择你的网页文件所在的目录，本例是“D：\”。其它保持默认值。



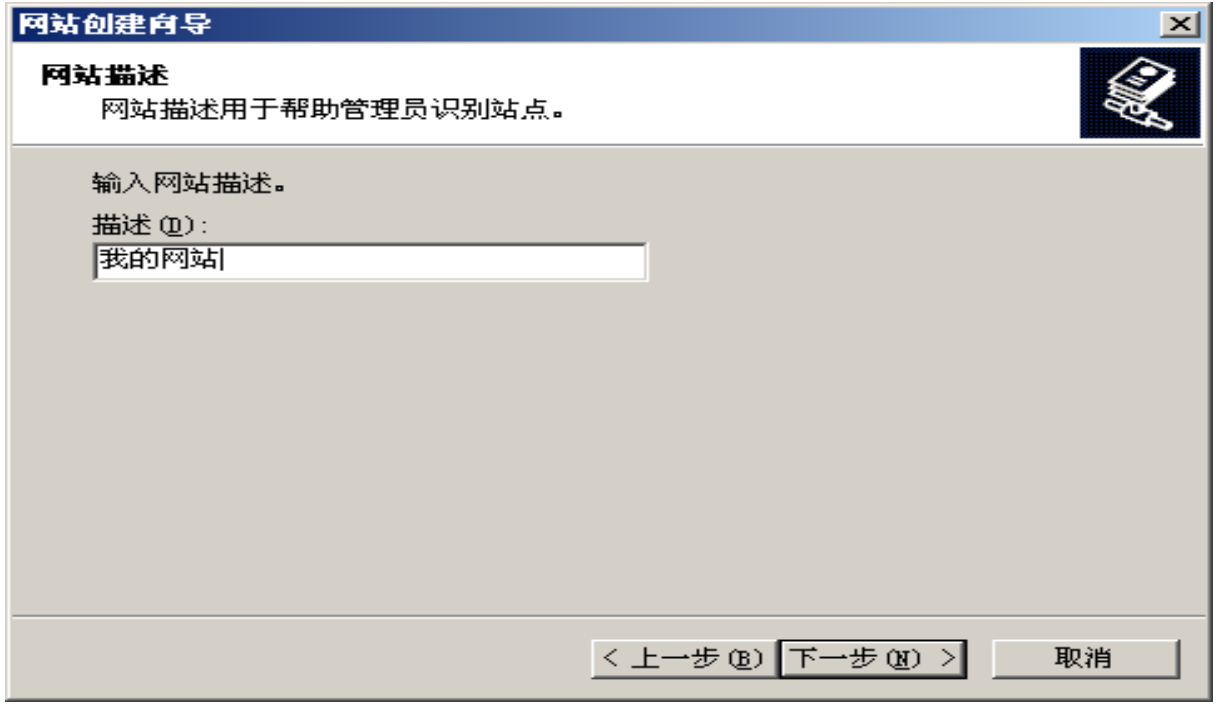
选择“文档”选项卡。选择“启用默认内容文档”，点击“添加”按钮，出现“添加内容页”的

对话框，在对话框中输入所建网页文件的名称（包括扩展名）。



（2）新建一个 Web 站点

选择“网站” →右键→新建→网站，“网站描述”中可以填写任何内容。



指定网站的 IP 地址。网站 TCP 端口和主机头均保持默认值。输入第一步中所建网页文件的路径。

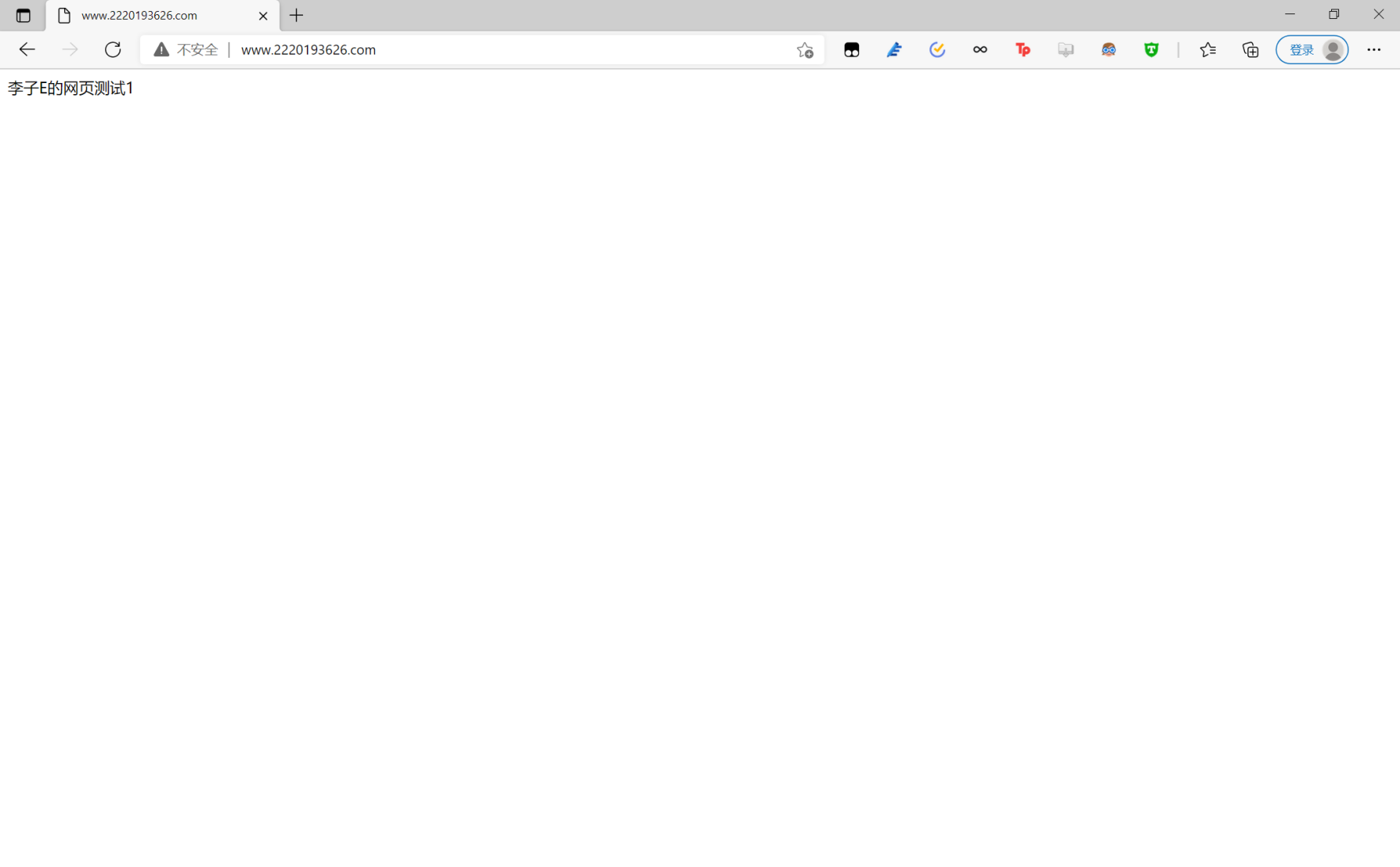
其它选项保持默认值。最后对新建的 Web 站点进行属性配置，操作步骤同默认 Web 站

点属性配置。

**3．实验结果验证**

在客户端edge浏览器写入URL，然后回车。

**成功结果为**：



[www.2220193626.com,可以看到已经成功。](http://www.2220193626.com。可以看到默认页面已经出现。)

[2.](http://www.2220193626.com。可以看到默认页面已经出现。)**[建立多个网站](http://www.2220193626.com。可以看到默认页面已经出现。)**

[虚拟主机是使用特殊的软件技术，将一台运行在 Internet 上的服务器主机划分成若干台](http://www.2220193626.com。可以看到默认页面已经出现。)

[虚拟的主机，每一台虚拟主机都具有独立的域名，具有完整的 Web 服务器功能，虚拟主机](http://www.2220193626.com。可以看到默认页面已经出现。)

[之间完全独立，并可由用户自行管理。在外界看来，每一台虚拟主机和一台独立的主机完全](http://www.2220193626.com。可以看到默认页面已经出现。)

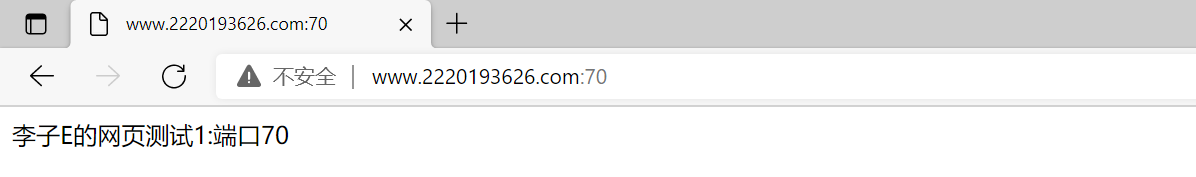
[一样。](http://www.2220193626.com。可以看到默认页面已经出现。)

[IIS 6.0 通过分配 TCP 端口、IP 地址和主机头名来运行多个网站。每个 Web 网站都具有](http://www.2220193626.com。可以看到默认页面已经出现。)

[唯一的：由 TCP 端口号、IP 地址和主机头等三部分组成的网站标识。通过更改其中的任何](http://www.2220193626.com。可以看到默认页面已经出现。)

[一个标识，就可以在一台计算机上维护多个网站。](http://www.2220193626.com。可以看到默认页面已经出现。)

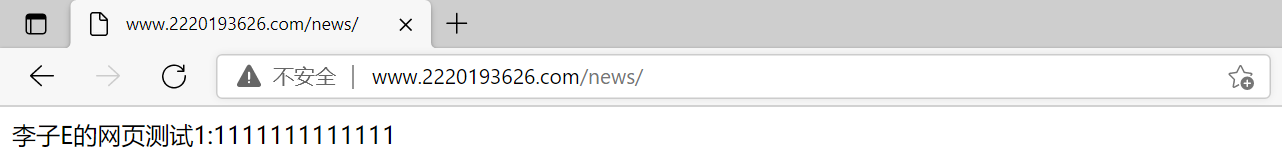
[这里我采用多个端口的技术:](http://www.2220193626.com。可以看到默认页面已经出现。)

[](http://www.2220193626.com。可以看到默认页面已经出现。)

[可以看到已经建立成功](http://www.2220193626.com。可以看到默认页面已经出现。)

**[3](http://www.2220193626.com。可以看到默认页面已经出现。)**[.](http://www.2220193626.com。可以看到默认页面已经出现。)**[虚拟目录](http://www.2220193626.com。可以看到默认页面已经出现。)**[技术实现一个web站点多个子站，子站为/news：](http://www.2220193626.com。可以看到默认页面已经出现。)

[要在“默认 Web 站点”下建立虚拟目录，选“默 认 Web 站点→右键→新建→虚拟目录”，然后在“别名”处输入“news”，在“目录”处选择它的实际路径即可。](http://www.2220193626.com。可以看到默认页面已经出现。)

[](http://www.2220193626.com。可以看到默认页面已经出现。)

**[4.安全机制](http://www.2220193626.com。可以看到默认页面已经出现。)**

[IIS 6.0 本身提供的是一种应用级的安全机制，它以 Windows Server 2003 操作系统和](http://www.2220193626.com。可以看到默认页面已经出现。)

[NTFS 文件系统的安全性为基础，提供了强大的安全管理和控制功能。](http://www.2220193626.com。可以看到默认页面已经出现。)

[身份验证和访问控制是 IIS 安全机制中最为主要的内容，它从用户和资源（网站、目录和文件）两个方面来限制访问。](http://www.2220193626.com。可以看到默认页面已经出现。)

[用户可以通过“目录安全性”选项卡来设置 IIS 的安全机制，如下图。通过该对话框，用](http://www.2220193626.com。可以看到默认页面已经出现。)

[户可以设置身份验证和访问控制这两方面的基本安全机制。](http://www.2220193626.com。可以看到默认页面已经出现。)

[我将自己主机的ip地址设置为禁止访问，查看结果：](http://www.2220193626.com。可以看到默认页面已经出现。)

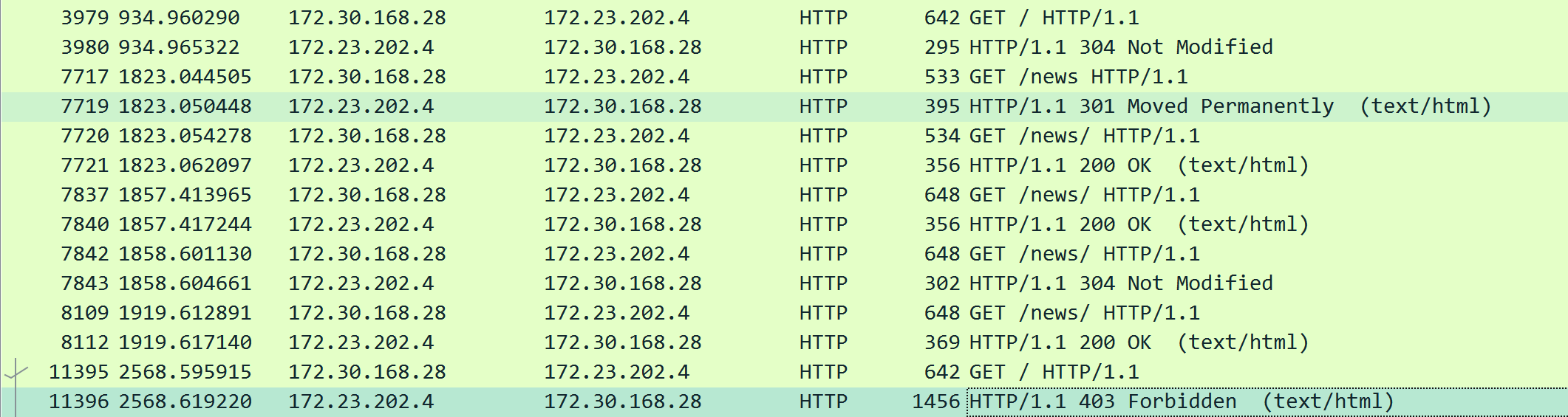
[](http://www.2220193626.com。可以看到默认页面已经出现。)

[如上，发现已经被禁止访问，由于new为目录下的站点，所以也是无法访问的。](http://www.2220193626.com。可以看到默认页面已经出现。)

**接下来我对各个步骤的结果进行逐一的分析**

五、实验结果、实验分析

1. 抓取HTTP请求报文进行分析：打开wireshark抓取的http报文



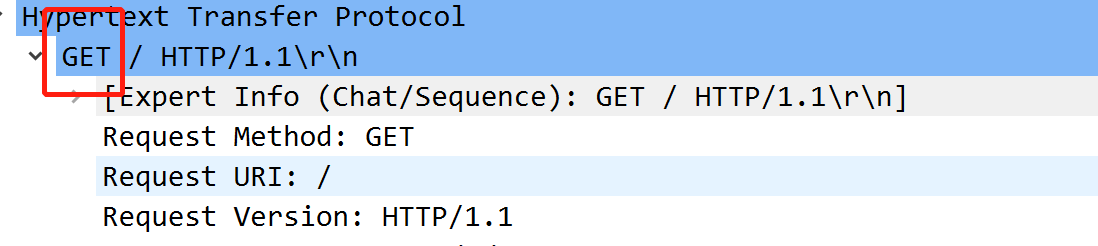
**首先对第一个报文及其响应报文进行分析**

(1)**首先打开http应用层部分进行分析**：

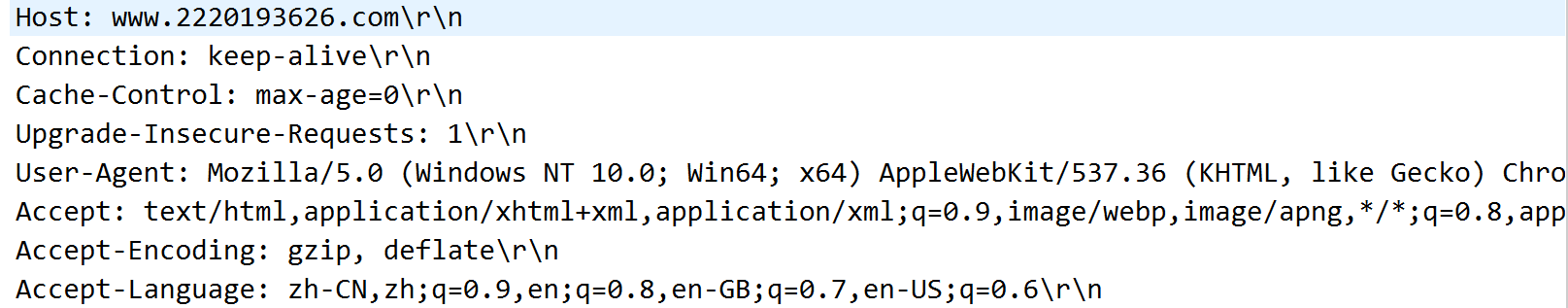


根据前面的分析，现在来验证一下，第一行是请求行，由三部分组成，分别为：请求方法，URL，以及协议版本，采用空格分隔

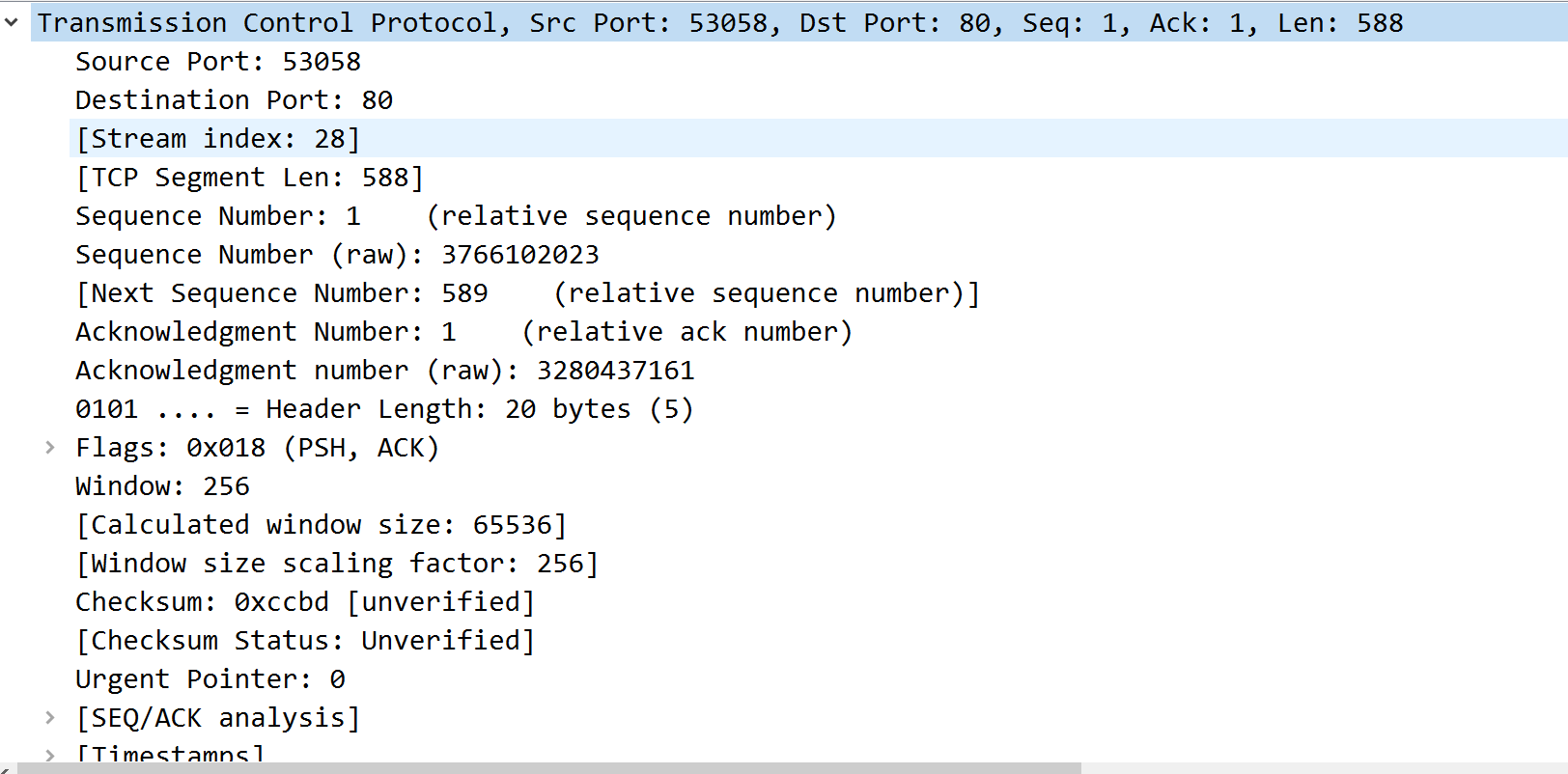
首先，可以看到第一行请求的方式为GET报文：



这里一般有GET和POST两种，GET一般用于获取信息，是没有副作用的，可以缓存，但POST往往不能缓存，且有副作用。请求行由于较简单，不再解释过多，接下来看请求头部：

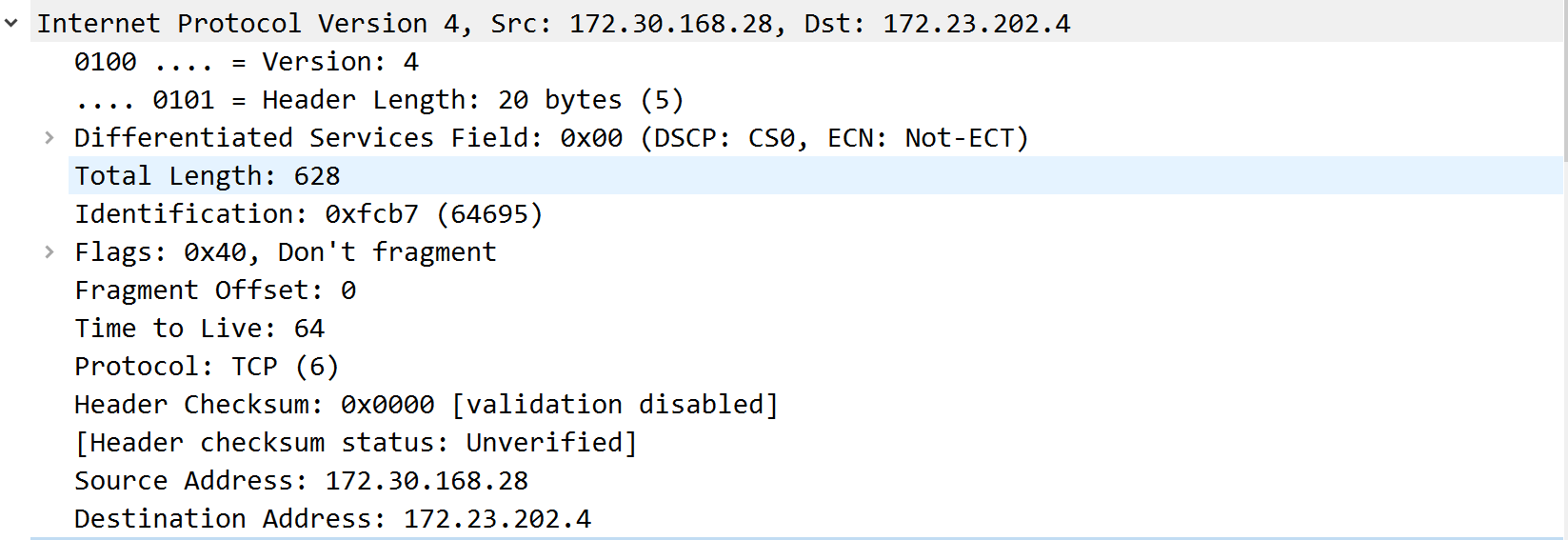


* Host为请求的主机名，是我自己申请的域名。
* Connection为客户端与服务端指定的请求，这里为keep-alive，意为保持连接
* User-Agent为发送请求的浏览器信息，如果知道了这些信息，理论上可以实现自动化登录等操作。
* Accpet为用户可以识别的内容类型列表
* 其中的Encoding部分代表了数据的编码方式
* Language代表了支持的语言类型，这里为中文。

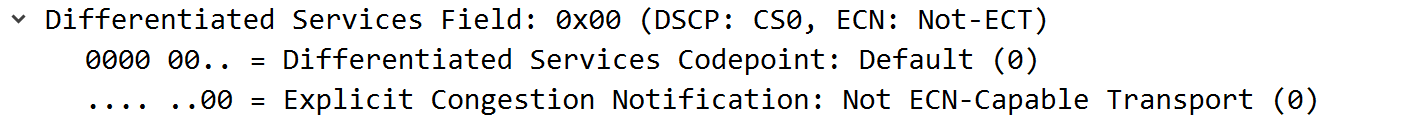
**(2)接着对运输层部分进行分析：**

首先可以看到，运输层采用的协议为TCP协议，这符合理论课所学，HTTP协议的运输层协议一定是TCP协议，只支持点到点的通信。接着对其他部分进行分析：

* 源端口号：53058，目的端口号为80，目的端口号在建立网站是默认为80
* 序列号为1，下一个序列号为589，这可以说明此报文一共588字节长，根据segment len部分可以看出推断是合理的
* 确认号为1，头部长度为20字节，说明没有额外的可变长度部分
* 标记字段Flags为PSH和ACK，PSH说明这是一个要求紧急发送到应用层的报文，因为此报文是HTTP连接请求报文，所以符合常理，ACK为1说明此报文也有确认功能。
* 窗口值为256，这个窗口值用于流量控制，用于调节另一方的发送窗口
* 校验和字段为0xccbd

**(3)接下来对网络层IP数据报进行分析：**  


* 首先是版本，可以看到是ipv4
* 然后头部检验和共20字节，IP数据包长度628字节，标志字段为64695。
* Differentiated Services Field（下面简称为DS Field）的意思是区分服务领域，这是以前在理论课学习中不太熟悉的部分，这里我展开DS Field部分

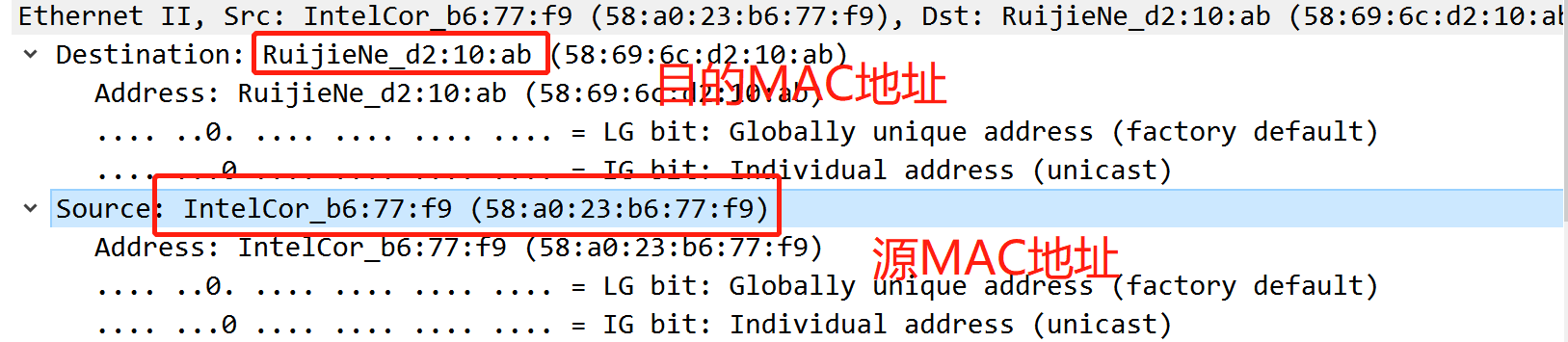


通过查阅资料得知，DSCP：区分服务代码点，即DS标记值，在iPV4中为0x00,ECN为显示拥塞通知，使得系统能够前瞻性地向同类设备发出调度路由器将超载的信号，以便它们能够采取避退措施，这里为00，显示为Not-ECT，也就是没有拥塞，不需要使用这一部分的功能。

综上可以得知，**DS Field的两个部分DSCP和CU组合成一个可扩展性相对较强的方法以此来保证IP的服务质量**。

* 接着打开Flags部分，这里显示不允许分片，一共三个字节RB,DF,MF，按照理论课的叙述，只有后两个部分有意义，由于没有采用分片功能，可以看到DF为1，MF为0，显示不允许分片，后续没有分片，是符合理论课的学习的。
* TTL为报文的生存时间，首部检验和为0x0000，源ip和目的ip均正确

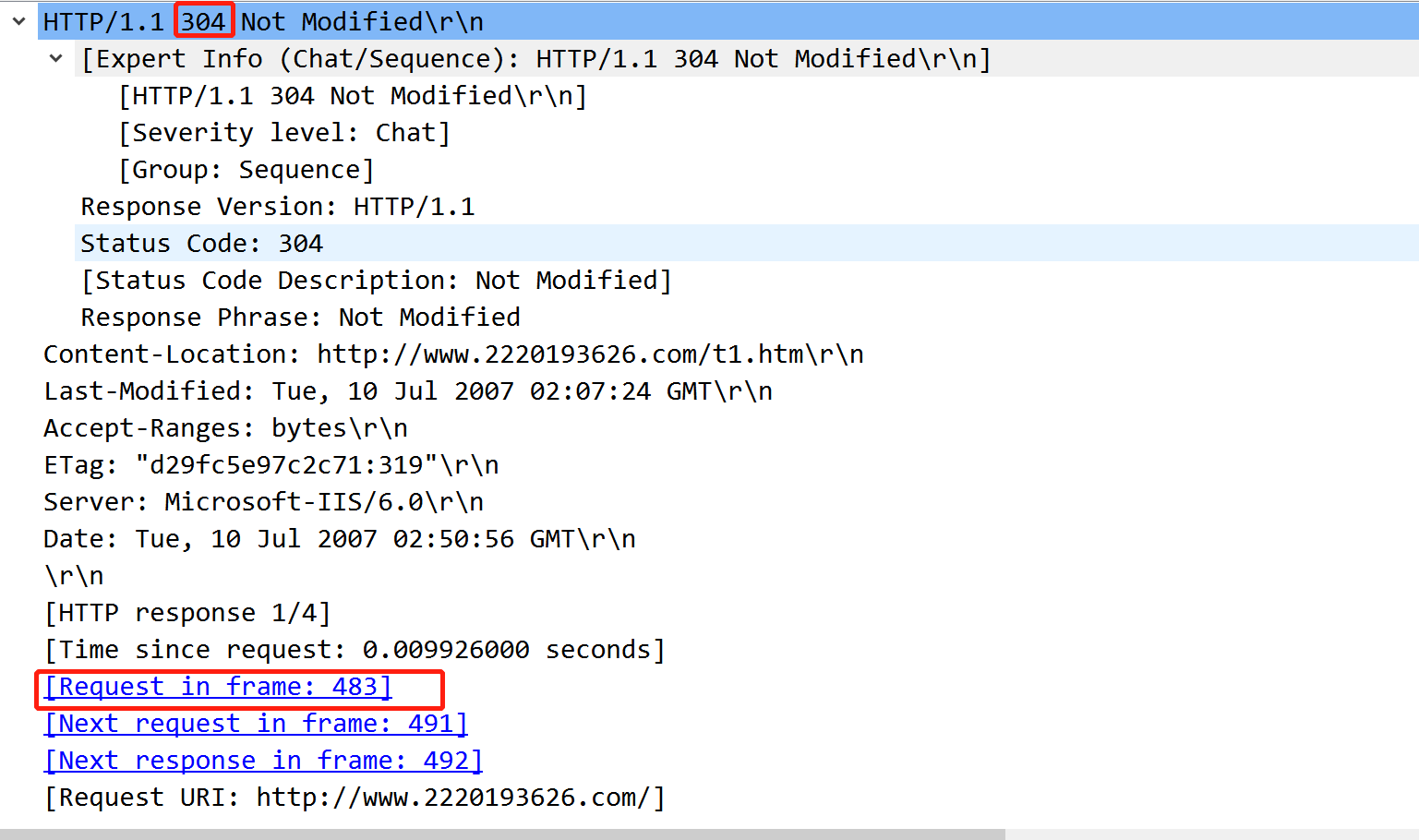
(4)**对数据链路层以太网帧进行简单分析**：



(5)最后对物理层数据帧进行简单的分析如下：

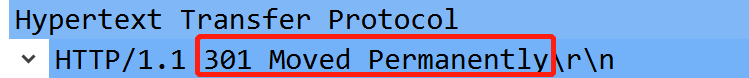


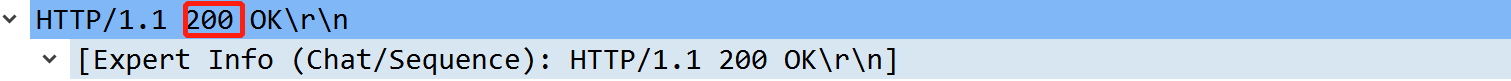
为了验证整个过程的正确性，我打开HTTP响应报文并查看和请求报文有关的项目：



可以看到响应报文的第一行状态码为304，这代表本地缓存已经有了这个网站的缓存，所以服务器提示可以直接从缓存获取，这是因为我之前已经尝试用客户端登录过服务器端建立的网站，所以本地缓存中已经有相关的不变的静态页面信息，不占用带宽。

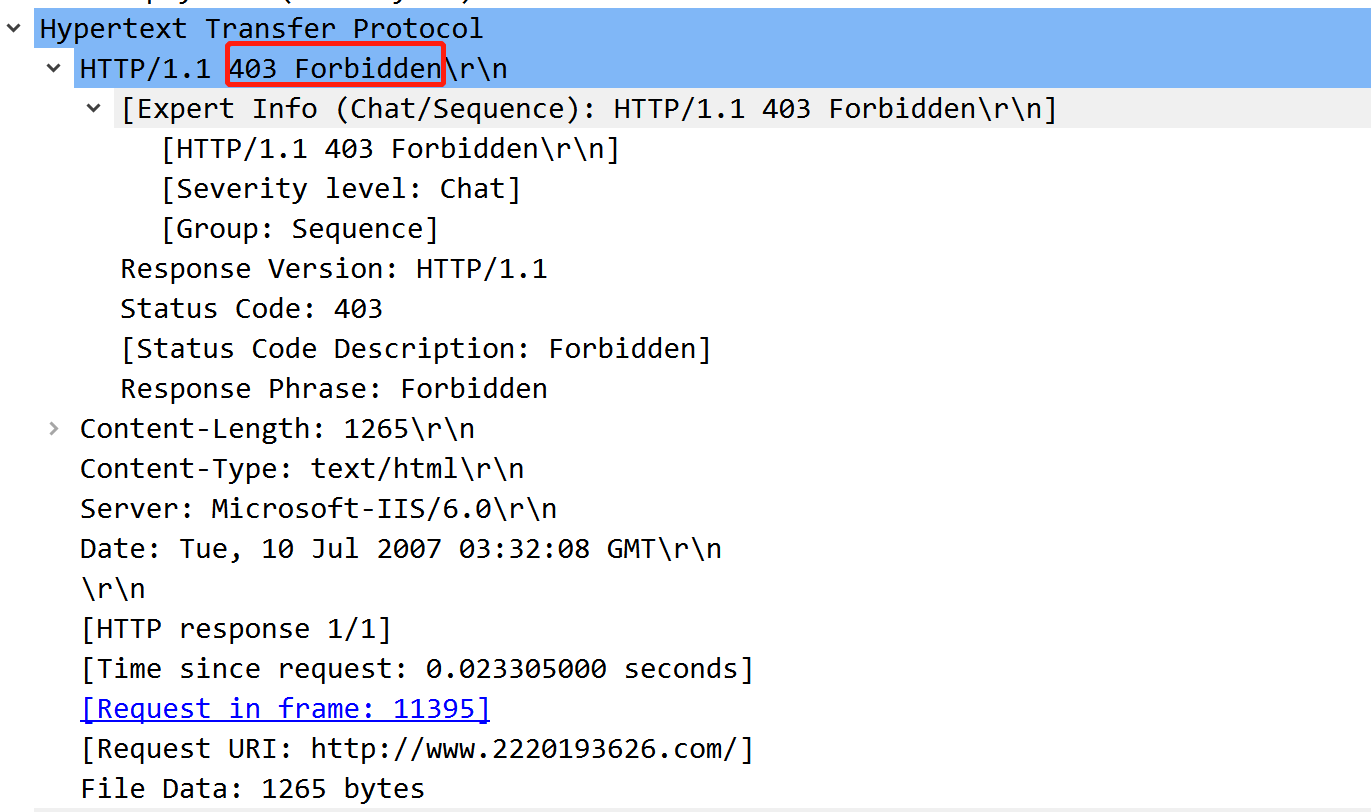
1. 在我建立子网站，把资源放入子网站对应的文件地址时，再抓取HTTP应答报文，可以看到：

  
应答报文的状态码维301，并提示该资源已经被迁移到了别的地方，是正确的。这时候查看下一个HTTP请求报文的状态码：



为200，这是一个比较普通的状态码，属于回答了请求报文，并把HTML文件发给了客户端。

1. 为了验证浏览器的安全机制，我将自己的地址设置为被禁止的ip地址，然后试图访问该网站，通过前面可以得知，我的访问被禁止，然后我抓取HTTP响应报文：



可以看到响应的状态码为403，我的这次访问被拒绝。

1. 实验总结

1.错误和解决：

(1)客户端主机无法通过域名www.2220193626.com访问到web服务器端的网站，解决方式：错误来自于客户端的DNS服务器并没有存储这个域名-ip对，所以需要将DNS服务器的ip地址由自动获取改为一个存有该web服务器地址的，我采用实验室的服务器建立了一个DNS服务器，并将客户端的DNS服务器地址替换，解决了问题

(2)利用服务器创建网站时，显示未启用，解决方式：这个问题出现的原因是建立了其它网站，而主页和路径设置都相同，ip地址也相同，无法区分，所以服务器不允许这样的网站被使用，解决方式为删除默认的网站，并重新设置路径。

(3)如何区别各个网站，每个网站都有唯一的ip地址，tcp端口号和主机头，通过不同的端口号/ip地址，就可以实现在一台服务器上建立多个虚拟主机。但是通过后者的方法，必须要对本地连接的属性的ip地址进行改变。

(4)首次抓取HTTP报文时，打开响应报文，发现状态码为不是200 OK而是304解决方法：经过查阅资料，了解到之前我的本地主机之前访问过服务器，所以本地缓存中有需要的文件，所以服务器端的响应报文为304，这样可以节约带宽，非常合理。

2实验的感悟：

(1)对于c/s模式与p2p模式的优缺点的个人理解：C/S架构的界面和操作可以很丰富。

安全性能可以很容易保证，而且只有两个端，因此响应速度较快，但是维修成本较高，每次更新，客户端的所有程序都需要更新。相比而言，p2p模式的网络中节点的可扩展性高，节点可以随意的添加和删除，并且不存在客户端与服务器这样的严格区分，每个节点可以又充当着客户端和服务器，但会经常出现冗余和堵塞。

1. web服务器提供一个动态文档时，需要先在另一个服务器上运行，再传给web服务器，再传给客户端，不同于简单的HTML静态页面的架构。
2. 网站安全性的实现途径：可以通过身份验证、ip地址和域名限制等方式实现，但仍具有很大奉献，很多网站都是不安全的，所以我们绝不能对网络法律法规发起挑战，而应该尽力发挥自己所长帮助实现网络的进一步安全化。
3. 总结：通过本次实验，我深刻体会到了web页面的请求原理，通过wireshark抓包验证了课上所学的网络中的各个著名过程，并且对于HTTP协议有了更深一步的理解，对于网站页面的编写和页面的美化也越来越感兴趣，深刻理解了C/S模式下的计算机的运作原理，感谢老师的指导与和我一起对问题的探讨！