

**计算机网络**

**课程实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 利用 Wireshark 进行协议分析 | | | | | |
| 姓名 | 汤添凝 | | 院系 | 计算机科学有技术学院 | | |
| 班级 | 1703201 | | 学号 | 1170300728 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 格物214 | | 实验时间 | 11/9 | | |
| 实验课表现 | 出勤、表现得分(10) |  | 实验报告  得分(40) |  | 实验总分 |  |
| 操作结果得分(50) |  |
| 教师评语 | | | | | | |
|  | | | | | | |

****

|  |
| --- |
| 实验目的： |
| （注：实验报告模板中的各项内容仅供参考，可依照实际实验情况进行修改。）  本次实验的主要目的。  熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以及报文交换的情况。 |
| 实验内容： |
| 概述本次实验的主要内容，包含的实验项等。   1. http   HTTP GET/response 交互  你的浏览器运行的是 HTTP1.0，还是 HTTP1.1？你所访问的服务器所运行 HTTP 协议的版本号是多少？  都是HTTP1.1  你的浏览器向服务器指出它能接收何种语言版本的对象？  ZH-CN  你的计算机的 IP 地址是多少？服务器 http://hitgs.hit.edu.cn的 IP 地址是多少？  我的计算机的IP地址：192.168.1.216  服务器的IP地址：219.217.226.25   * 从服务器向你的浏览器返回的状态代码是多少？   200  HTTP 条件 GET/response 交互   * 分析你的浏览器向服务器发出的第一个 HTTP GET 请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？   没有   * 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？   HTTP Status Code 为 200 时返回文件，为304时不返回文件   * 分析你的浏览器向服务器发出的较晚的“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？     有，后面是时间。其意义是在请求消息中，声明所持有版本的日期   * 服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。     说明缓存的内容都是是最新的，同时返回的消息中，不包含任何对象数据。   1. Tcp   在显示筛选规则中输入“tcp”,可以看到在本地主机和服务器之间传输的一系列 tcp 和 http 报文，你应该能看到包含 SYN 报文的三次握手。也可以看到有主机向服务器发送的一个 HTTP POST 报文和一系列的“http continuation”报文。  根据操作思考以下问题：  IMG_256   * 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和TCP 端口号是多少？   IP地址：192.168.1.216  TCP端口号：53862   * Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文的端口号是多少？   128.119.245.12  80   * 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？   IMG_256  客户服务器用于初始化 TCP 连接的 TCP SYN 报文段的序号是0，然后置SYN位为1，标示该报文段是 SYN 报文段   * 服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中，Acknowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器是如何决定此值的？在该报文段中，是用什么来标示该报文段是SYNACK 报文段的？   QQ图片20191118182801  序号为0，ack值为1，是上次客户端发来的序列号加1。即1=0+1  将标志位里的ACK和SYN位，置为1，来标示该报文段是SYNACK 报文段   * 你能从捕获的数据包中分析出 tcp 三次握手过程吗？   IMG_256  这里就是三次握手的过程   * 包含 HTTP POST 命令的 TCP 报文段的序号是多少？   IMG_256  序号是1   * 如果将包含 HTTP POST 命令的 TCP 报文段看作是 TCP 连接上的 第一个报文段，那么该 TCP 连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？   IMG_256  第32帧就是第六个报文段  IMG_256  序列号6322，接受时间如下：  QQ图片20191118183609  下面这条就是对应的ACK，  IMG_256  接收时间：     * 前六个 TCP 报文段的长度各是多少？   IMG_256  长度是567，1506，1506，1506，1506，1506   * 在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？ 限制发送端的传输以后，接收端的缓存是否仍然不够用？     在后续ACK中，这个数字会变大，没有不够用的情况   * 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？   没有重传，依次查询整个过程中的TCP帧，发现没有重复的帧（字节数起点不一样）   * TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。   总共152840长度  时间间隔约为2.8……-1.6……=1.213162‬s  152840/1.213162=125984B/s   1. IP 分析   选择第一个你的主机发出的ICMP Echo Request消息   * 你主机的IP地址是什么？     主机的IP地址是192.168.1.52   * 在IP数据包头中，上层协议（upper layer）字段的值是什么？   值为1   * IP头有多少字节？该IP数据包的净载为多少字节？并解释你是怎样确定该IP数据包的净载大小的？   IP 头有 20 字节，TOTAL length=56字节  净载56-20=36字节  单击Source列按钮，这样将对捕获的数据包按源IP地址排序。选择第一个你的主机发出的ICMP Echo Request消息   * 该IP数据包分片了吗？解释你是如何确定该P数据包是否进行了分片没有   Df=mf=0，偏移量为0，说明允许分片但未分片   * 你主机发出的一系列ICMP消息中IP数据报中哪些字段总是发生改变？   id,ttl,checksum   * 哪些字段必须保持常量？哪些字段必须改变？为什么？   ID必须改变：鉴别码，⽤于区分数据包；  TTL必须改变：保留和获取路径上的路由信息；  Header Checksum必须改变：⾸部校验和，前⾯的字段改变，checksum也改变；  除以上外的字段保持常量。   * 描述你看到的IP数据包Identification字段值的形式。   大小为2字节，相邻数据包，该字段，作差，结果为1  找到由最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded消息。   * Identification字段和TTL字段的值是什么？     Id: 0x3345  ttl: 64   * 最近的路由器（第一跳）返回给你主机的ICMP Time-to-live exceeded消息中这些值是否保持不变？为什么？   ID变化，不同ICMP数据包ID不同  因为是第一跳的路由器返回的Time-to-live exceeded消息，每次只有一跳，TTL值不变  找到在将包大小改为2000字节后你的主机发送的第一个ICMP Echo Request消息。   * 该消息是否被分解成不止一个IP数据报？   是，分成两个  IMG_256   * 观察第一个IP分片，IP头部的哪些信息表明数据包被进行了分片？IP头部的哪些信息表明数据包是第一个而不是最后一个分片？该分片的长度是多少   第一片：  IMG_256  Mf=1，有分片，非最后一片。且OFFset为0，那一定是第一片，长度1500  找到在将包大小改为3500字节后你的主机发送的第一个ICMP Echo Request消息。  找到在将包大小改为3500字节后你的主机发送的第一个ICMP Echo Request消息。   * 原始数据包被分成了多少片？     3片   * 这些分片中IP数据报头部哪些字段发生了变化？   前两片MF为1，最后一片MF为0  第一片OFFSET为0，第二片OFFSET为1480，第三片OFFSET为2960   1. 抓取 ARP 数据包  * 利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。说明 ARP 缓存中每一列的含义是什么?   IMG_256  分别表示，IP地址，所对应的物理地址，类型（动态配置或静态配置）  清除主机上 ARP 缓存的内容,抓取 ping 命令时的数据包。分析数据包,回答下面的问题：   * ARP数据包的格式是怎样的？由几部分构成，各个部分所占的字节数是多少？   2  由9部分构成，分别是硬件类型（2字节），协议类型（2字节），硬件地址长度（1字节），协议地址长度（1字节），OP（2字节)，发送端MAC地址（6字节），发送端IP地址（4字节），目的MAC地址（6字节），目的IP地址（4字节）。  IMG_256   * 如何判断一个ARP数据是请求包还是应答包？   看OP字段。当OP字段值为0x0001时是请求包，当值为0x0002时是应答包。   * 为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？   查询时并不知道目的地址，所以需要在广播帧中传送。  查询帧，有写清SOURCE地址，响应帧把该地址作为目的地址，询问主机就能成功接受响应报文。至于其他主机，没有发查询帧，自然也不用给他们发响应，所以响应帧不用在广播帧中传送   1. 抓取 UDP 数据包   分析 QQ 通讯中捕获到的 UDP 数据包。根据操作思考以下问题：  IMG_256   * 消息是基于UDP的还是TCP的？   Udp   * 你的主机ip地址是什么？目的主机ip地址是什么？   主机IP：192.168.1.216  目的主机IP：125.39.45.59   * 你的主机发送QQ消息的端口号和QQ服务器的端口号分别是多少？   4010  8000   * 数据报的格式是什么样的？都包含哪些字段，分别占多少字节？   1  源端口号（4字节），目的端口号（4字节），长度（4字节），校验和（4字节）和应用层数据。   * 为什么你发送一个ICQ数据包后，服务器又返回给你的主机一个ICQ数据包？   返回包作为确认信息   * 这UDP的不可靠数据传输有什么联系？   因为UDP是不可靠数据传输，如果不做任何改良的话，这一点是不能接受的，  所以，“返回一个包作为确认”，是QQ这个软件实现可靠数据传输的一种方案   * 对比前面的TCP协议分析，你能看出UDP是无连接的吗？   没有利用SYN位的握手，无法确认连接是否建立。  此外也没有序列号等等   1. 利用 WireShark 进行 DNS 协议分析   QQ图片20191118192237  我的主机IP 172.20.34.141  IMG_256  UDP，源端口号57692，目的端口号53  内容如下，即请求百度IP  QQ图片20191118192426  DNS回复信息如下，带有百度IP  IMG_256 |
| 心得体会： |
| 本次实验内容充实紧凑，且有一定难度与复杂度，但在老师、助教、同学以及个人自学的多重努力下成功完成了实验。  本次实验为“利用 Wireshark 进行协议分析”，以设计代理服务器的形式逐步教会我们HTTP协议的含义细节，协议信息构造，缓存设计实现，效果出众。在此前，我从来没有考虑过诸如“TCP究竟是如何工作的？”、“为什么要设计ARP”这类问题，经过了这次实验后，我对这些HTTP协议设计细节有了更深入的了解，在逐渐完成实验任务的同时，开拓了计算思维。我想这大概就是身为“计算机科学有技术学院”的学生相比其他专业学生对于计算机认识更深入的地方之一了。 |