

**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 | 董琦 | | 院系 | 数据科学与大数据 | | |
| 班级 | 2003501 | | 学号 | 120L020701 | | |
| 任课教师 | 刘亚维 | | 指导教师 | 刘亚维 | | |
| 实验地点 | G001 | | 实验时间 | 2022/10/13 | | |
| 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： |
| 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： |
| 1. 学习Wireshark 的使用 2. 利用Wireshark 分析HTTP 协议 3. 利用Wireshark 分析TCP 协议 4. 利用Wireshark 分析IP 协议 5. 利用Wireshark 分析Ethernet 数据帧   选做内容：   * 1. 利用Wireshark 分析DNS 协议   2. 利用Wireshark 分析UDP 协议   3. 利用Wireshark 分析ARP 协议 |
| 实验过程： |
| 1. 开   一．Wireshark使用   1. 打开Wireshark，监听WLAN   我们监听WLAN这个端口。    打开浏览器，访问<http://www.hit.edu.cn>网址。  加载出网页后暂停wireshark抓包。  （学校主页还挺帅的哈）    在wireshark中可以看到发送的http请求：    可以看到链路层、网络层、传输层、应用层的各层协议内容以及报文内容。   1. H 二. HTTP分析 2. Get分析   打开浏览器访问<http://hitgs.hit.edu.cn/news> 开始抓包。  额这个网页挂掉了，换成了主页。    所得到的http分组：    可以看到在加载网页时的一系列GET/response交互。  下面具体分析报文回答问题。  请求报文：    响应报文：     1. 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。   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？      1. 你的计算机的IP 地址是多少？服务器http://hitgs.hit.edu.cn/news的IP 地址是多少？     我：172.20.70.16 服务器：219.217.226.25   1. 从服务器向你的浏览器返回的状态代码是多少？   200，说明正常响应。   1. 条件GET分析   先清除缓存：  重新访问后结束抓包。   1. 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？     如图，没有。   1. 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？   是，通过状态码200，报文体中包含了文件内容。     1. 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，这里我使用自己构建报文访问[www.7k7k.com](http://www.7k7k.com)网站（浏览器访问总是没有）：    抓包到的报文内容：    后面跟着的是上一次收到报文的时间（我自己填的）。   1. 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。    * 1. 表示没有修改。不明确返回文件内容，这样就使用之前缓存报文内容，节省流量。   三．TCP分析   1. 俘获大量的由本地主机到远程服务器的TCP分组     按照指导下载文件并访问网站。  传输完成后停止捕获。     1. 浏览追踪信息   得到如下报文：     1. 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？   172.20.70.16，54280   1. 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.   1. TCP 基础 2. 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？   客户：    序号为840377001。将标记SYN置为1.  服务器：    序号为3755220972。同样将标记SYN置为1.   1. 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？   如1）问第二图，即为SYNACK报文段。序号为3755220972，acknowlegement=1，表示收到SYN报文。  Acknowlegement number=840377002，为客户发送的报文序号加1.将ACK和SYN标记全置为1来表示为SYNACK报文。   1. 你能从捕获的数据包中分析出tcp 三次握手过程吗？   可以，这三个报文即三次握手：    第三个报文中，可以看到发送方和接收方均确认了报文序号和窗口大小。     1. 包含HTTP POST 命令的TCP 报文段的序号是多少？   如图，该报文为包含POST的报文段。    序号为840377002   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？   如图，为此报文段。    序号为840383227，发送时间如timestamps，为第一个TCP帧的5.430216秒后。    上图为对应的ACK报文，这里可以看到是采用滑动窗口协议。  接收时间戳如箭头所指。   1. 前六个TCP 报文段的长度各是多少？     分别为785、1360、1360、1360、1360、1360.   1. 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？     如图，最小时窗口大小为29200.发送报文数量有限，不存在不够用的情况。   1. 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，客户发送的报文序号严格单调递增，没有重复的，   1. TCP 连接的throughput (bytes transferred per unit time)是多少？请写出你的计算过程。   开始发送文件时间为：7.687573s    收到最后一个ACK时间为：8.809907s    共传输153107-1=153106字节，耗时1.122334s。  故吞吐量为：136.418KBPS.  四． IP分析  下载pingPlotter程序并设置packet：    根据指导完成操作后终止抓包。    这里访问的是[www.google.com](http://www.google.com)   1. 你主机的IP地址是什么？   172.20.70.16   1. 在IP数据包头中，上层协议（upper layer）字段的值是什么？   是IPV4协议。     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个字节。净载为500字节，由total length=520，520-20=500可得。   1. 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   分片了，由标志位可得，而且前面还有俩个同一分组的包。     1. 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、Header checksum这三个字段总在变化。   1. 哪些字段必须保持常量？哪些字段必须改变？为什么？   ID、TTL、Header checksum这三个字段总在变化。ID用来标识不同的数据，TTL每次路过一个路由器会减1，由于前两个发生改变，头部校验和Header checksum也会发生改变。MF，数据包长度，源和目的IP地址可能会变。除以上的三个字段其他正常情况下，不发生改变。   1. 描述你看到的IP数据包Identification字段值的形式。   单调递增。     1. Identification字段和TTL字段的值是什么？   0，255.   1. 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？   保持不变。原因：IP是无连接服务，相同的标识是为了分段后组装成同一段， 给同一个主机返回的标识不代表序号，因此Identification字段不变；又因为 是第一跳路由器发回的数据报，所以TTL字段是最大值-1（254）     1. 该消息是否被分解成不止一个IP数据报？   是，分成俩个。   1. 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？     Don’t fragments为0表示被进行分片，More fragments为1表示不是最后一个分片。长度为1480B     1. 原始数据包被分成了多少片？   3片。   1. 这些分片中IP数据报头部哪些字段发生了变化？   Fragment offset,还有more fragments标志位。  五． 抓取ARP数据包   1. 查看ARP缓存（部分）      1. Ping我的手机：      1. 抓取ARP分组：      1. 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?   是每一个IP地址与MAC物理地址的转换映射条目。   1. 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： 2. 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？   如上图所示。   1. 如何判断一个ARP数据是请求包还是应答包？   查看OP字段。OP为1为查询，为2为响应。     1. 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？   因为你询问的时候不清楚哪个节点有对应IP的条目，所以需要广播。而响应时知道是哪个节点发出了询问，故可以明确目的地址。  六．抓取UDP数据包  抓取到数据包如下：（查询可知QQ使用端口为4000）     1. 消息是基于UDP的还是TCP的？   UDP。。。。。。   1. 你的主机ip地址是什么？目的主机ip地址是什么？   我的：172.20.70.16 目的：39.156.132.122   1. 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？   我的：54476 目的：8000   1. 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？   格式如图：俩字节的源端口，俩字节的目的端口，俩字节的长度，俩字节的首部检验和，余下的为内容。  1   1. 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？这UDP的不可靠数据传输有什么联系？对比前面的TCP协议分析，你能看出UDP是无连接的吗？   因为服务器需返回接收的结果给客户端。因为服务器只提供了一次返回的ACK，所以不保证数据一定送达。可以看出UDP是无连接的。UDP数据包没有序列号，因此不能像TCP协议那样先握手再发送数据，因为每次只发送一个数据报，然后等待服务器响应。  七． DNS分析  抓到包如下：（这里访问的是www.youtube.com）    打开看一下：    这个是返回的报文：    可以看到返回了四个条目，其中一个为CNAME类型，为规范主机名，三个为A类型，为规范主机名的IP地址。 |
| 实验结果：  这次实验成功完成了实验内容的七个任务，并且针对实验中问题做了思考和解答。 |
| 问题讨论： |
| **协议总结**   1. HTTP协议 2. HTTP 协议支持客户/服务器模式； 3. 简单快速：客户向服务器请求服务时，只需传送请求方法和路径；请求方法常用 GET、HEAD、POST 等，每种方法规定了客户与服务器联系的不同类型；HTTP 协议简单，服务器程序规模小，通信速度较快； 4. 灵活性：HTTP 允许传输任意类型数据对象；正在传输数据类型由Content-Type 标记； 5. 无连接：无连接是指每次连接只处理一个请求；服务器处理完客户请求，并收到客户应答后，即断开连接，节省传输时间； 6. 无状态：指协议对于事务处理无记忆能力；应答快，但传输数据量较大。 7. TCP协议 8. 提供面向连接的、可靠的、基于流的数据传输服务，传输单位是报文段； 9. 使用超时重发、数据确认等方式确保数据被正确发送至目的地。 10. IP 协议 11. 任务: 负责对数据包进行路由选择和存储转发； 12. 负责为分组交换网上的不同主机提供通信服务。在发送数据时，网络层把运输层产生的报文段和用户数据报封装成分组（IP 数据报）或包进行传送； 13. IP 协议:逐跳发送模式；根据数据包的目的地 IP 地址决定数据如何发送；如果数据包不能直接发送至目的地，IP 协议负责寻找一个合适的下一跳路由器，并将数据包交付给该路由器转发； 14. ICMP 协议：因特网控制报文协议，用于检测网络连接 15. ARP协议   地址解析协议 ARP（Address Resolution Protocol），负责完成逻辑地址向物理地址的动态映射，将 32 位逻辑地址（IP 地址）转换为 48 位的物理地址（MAC地址）   1. UDP协议 2. 为了在给定的主机上能识别多个目的地址，同时允许多个应用程序在同一台主机上工作并能独立地进行数据包的发送和接收，设计用户数据报协议 UDP。 3. UDP 使用底层的互联网协议来传送报文，同 IP 一样提供不可靠的无连接数据包传输服务。它不提供报文到达确认、排序、及流量控制等功能。 4. DNS协议 5. DNS 是一种可以将域名和 IP 地址相互映射的以层次结构分布的数据库系统。 6. DNS 系统采用递归查询请求的方式来响应用户的查询，为互联网的运行提供关键性的基础服务。   目前绝大多数的防火墙和网络都会开放 DNS 服务，DNS 数据包不会被拦截，因此可以基于 DNS 协议建立隐蔽信道，从而顺利穿过防火墙，在客户端和服务器之间传输数据。 |
| 心得体会： |
| 这次实验首先是学会了抓包软件wireshark的使用，然后在七个不同的任务中对于互联网的应用层、运输层、网络层、链路层的各层协议有了深入的认识，更加深了对于计算机网络体系结构的认识，收益匪浅。 |