

**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 | 姜昕阳 | | 院系 | 计算学部 | | |
| 班级 | 2203201 | | 学号 | 2022111742 | | |
| 任课教师 | 詹东阳 | | 指导教师 | 詹东阳 | | |
| 实验地点 | 格物207 | | 实验时间 | 2024.5.15 | | |
| 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：  a) 利用 Wireshark 分析 DNS 协议  b) 利用 Wireshark 分析 UDP 协议  c) 利用 Wireshark 分析 ARP 协议 |
| 实验过程： |
| 1. 学习 Wireshark 的使用   基本介绍：  Wireshark是一种可以运行在Windows，UNIX，Linux 等操作系统上的分组分析器。Wireshark（前称 Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。使用简介：  （1）启动 Wireshark 软件，打开浏览器，选择网络接口 WLAN；  （2）浏览器输入网址http://www.hit.edu.cn，Wireshark 抓包，并筛选 HTTP 协议报文；  （3）详细用户界面：命令菜单、俘获分组列表、分组头部明细、分组内容窗口、筛选俘获分组等信息实验指导书已给出，不再展示。   1. HTTP条件GET/response交互   （1）启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。  （2）启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。  （3）在浏览器的地址栏中http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html  ,在你的浏览器中重新输入相同的 URL 或单击浏览器中的“刷新”按钮。  （4）停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的 HTTP 报文。   1. TCP分析   A. 俘获大量的由本地主机到远程服务器的 TCP 分组  （1） 启动浏览器，打开http://gaia.cs.umass.edu/wireshark-labs/alice.txt网页，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到你的主机上。  （2）打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，如图6-6所示，窗口如下图所示。在Browse按钮旁的文本框中输入保存在你的主机上的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按 “Upload alice.txt file”按钮。  （3）启动Wireshark，开始分组俘获。  （4）在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。  （5）停止俘获。  B. 浏览追踪信息  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。  C. TCP 基础   1. IP分析   通过执行 traceroute 执行捕获数据包  （1） 启动 Wireshark 并开始数据包捕获；  （2） 启动 pingplotter 并“Address to Trace Window”域中输入目的地址。  对捕获的数据包进行分析   1. 抓取 ARP 数据包   （1）利用 MS-DOS 命令：arp查看主机上 ARP 缓存的内容。  （2）在命令行模式下输入：ping 192.20.0.1（或其他 IP 地址）  （3）启动 Wireshark，开始分组俘获。   1. 抓取 UDP 数据包   （1）启动 Wireshark，开始分组捕获；  （2）发送 QQ 消息给你的好友；  （3）停止 Wireshark 组捕获；  （4）在显示筛选规则中输入“udp”并展开数据包的细节。   1. 利用Wireshark进行DNS协议分析   （1）打开浏览器键入:www.baidu.com  （2）打开 Wireshark,启动抓包.  （3）在控制台回车执行完毕后停止抓包 |
| 实验结果： |
| 1. Wireshark的使用   1d7fd723e70ca47099e613973526467  选择WLAN接口，打开浏览器。访问网址http://www.hit.edu.cn，在筛选框输入http，就可以获得所有的http请求，示意图如下：  72bfd2ec268ffcb8ec82f06b38521d5  框中的信息包括http协议信息：源地址、目的地址、报文类型以及报文长度和信息等，左下方的界面显示具体数据帧的内容，右下方的界面是数据帧对应的十六进制的信息，右面对应ASCII码转换后的字符。   1. HTTP分析   1）HTTP GET/response交互  打开Wireshark的分组嗅探器，选择HTTP进行过滤，在浏览器输入网址：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html  ，会有如下反应：  d3c7ed450eda46472cbc1fd7f1ddb0c  显然，这里浏览器用的协议是HTTP1.1，访问的服务器运行的也是HTTP1.1  接受的语言是：zh-CN，即中文  本计算机的IP地址为172.20.10.228  服务器的IP地址：129.119.245.12  服务器返回的状态码是200  2）条件get/response交互  首先清除浏览器的缓存文件    此时，访问http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html时，wireshark反应如下：  d3c7ed450eda46472cbc1fd7f1ddb0c  对于第一个请求并没有发现If-Modified-Since 字段，说明浏览器没有缓存，  显示包括http协议信息：源地址、目的地址、报文类型以及报文长度和信息等，左下方的界面显示具体数据帧的内容，右下方的界面是数据帧对应的十六进制的信息，右面对应ASCII码转换后的字符。  服务器明确返回了文件的内容，可以通过状态码200得知（其已成功发送完整的数据报文）。  再次访问的请求中，就包含了询问缓存是否更新字段，在其后跟着的是缓存文件最后修改的时间：If-Unmodified-since：b63e1960d37d0ff2eb2633e430eb972  db94c8b1e62d7b3ca8debb2894f2104  对于该请求，服务器返回304代码，表示缓存未更新，同时报文中也不返回文件内容，让浏览器直接使用缓存内容。   1. TCP分析   对网络上的Alice’s adventure in wonderland下载，存储，  4488f7629acb0fd58d29c21133e8f68  之后在网址http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html点击选择上述存储路径，开启wireShark，之后提交  94f202d37a7c4bbb6a93b669f5bcf2c  获得上述界面后，停止捕获报文  c5a37227db9d75b0a7f851f167145d2  向目标网站http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html传输文件的客户机的IP地址和端口号是：172.20.10.228，端口号是57626服务器的IP地址是128.119.245.12，发送TCP的端口为80，接收TCP的端口为80  查看追踪流  814d260bca3bbba525415f66ae63b57  （1）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？  序号为10和11；在SYN位置1表示该报文段为SYN报文段，seq=0  （2）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SYN-ACK 报⽂段的？  序号为12；acknowledge字段为1，在连接建立后，所有服务器将此位置为1    标志位SYN-ACK：SYN=1且ACK=1，seq=0   1. 捕获3次握手：   bcdf9d0f7611f12cfbb3c329b909fa2  抓包过程中的POST请求  Seq=1  如果将POST请求作为第一条报文，则第六条报文为  a556f48ab1dbb206b043aa6c61047e2  Seq为6100，是ack报文，是在2711.704997发送的，他所回应的是Seq=1的报文段，是在2710.237736发送的。  前6条TCP报文长度是713，1414，1414，1414，1414，1414  a556f48ab1dbb206b043aa6c61047e2  接收端公示的最小缓存为30720，在丢包后限制发送端的传输，接受端的缓存空间达到131840。因此接收端的缓存是足够使用的。  cde9bfeeb7b36eb167e698d70843f91  跟踪文件过程中没有发现有重传的报文段，可以从客户端的分组序号是否有重复出现进行判断，而实际上分组号是递增的。  db79271b8a6fd8f16c4e4c9166bbc2c  第一个HTTP请求的发送时间是2757.439714  8a61f4fb7ef1b0d4d7666f044d5d409  最后一个ACK报文段的发送时间是2760.656855，ACK的对象是153008，所以该TCP连接的Throughout为153008/(2760.656855-2757.439714)=47.56KB/s   1. IP分析   通过pingplotter对jwts.hit.edu.cn发送ping请求后wireshark解析出的界面如下  41517527cb930d2955fc82af849c842  本机的IP地址为172.20.53.104(主机IP动态变化）    IP数据报头的上层协议字段值为ICMP（1）    IP头的长度为20字节    净载荷则为总长度减去头部长度为36字节    Flag全部为0，其中offset与more均置为0，既没有偏移量，同时也是最后一片，所以该数据报没有进行分片  一系列ICMP的IP数据报中的TTL、首部校验和、Identification以及数据域部分每次都会改变。  数据报中的version与protocol 字段会一直保持常量，而Identification 和首部校验和以及TTL字段是必须进行改变的。由于对ICMP协议来说，version与protocol都是固定不变的,而每次的identification在发送时都相较于上一个报文的对应位置+1，所以一定不一样，而TTL因为是要进行路由探测，所以每次发送的ICMP报文相应的TTL都依次+1，所以一定不一样；首部校验和则是随其他字段的改变而改变，所以一定是不一样的。      最近路由器返回的消息中TTL为252，Identification是0x4c02  其中TTL保持不变，而Identification会发生变化，这是因为TTL字段是被第一跳路由器设置好的，不会改变，而Identification则随报文变化而生成不同的值  将分组大小改为2000B后    从more fragments=1标志可知主机发送的ICMP消息出现了分片，且不是最后一片，offset=0则说明这是第一片，该分片的长度为1500B，包含20B的头部。  将分组大小改为3500B后，再进行分析    发现被分成了三片，并且这三个分片的offset以及MF标志会发生变化：偏移量三者各不相同，而最后一片的MF为0，表示没有更多的分片了。    这是刚刚在ICMP分析中的报文截取到的以太网帧，可以看到帧的头部由目的mac地址、源mac地址以及类型组成。目的MAC地址即是数据链路层的接口地址，源MAC地址是发送端适配器MAC地址。Type表示该报文的协议类型，这里指的是IPv4报文。当目的适配器的MAC地址与目的MAC地址相匹配时，这个帧就会被接受并转交给上一层。   1. 抓取ARP数据包--ARP分析   9afb1d4477a4607a039e18002ea6682  本机的ARP缓存表如图，第一列是缓存的IP地址，第二列是对应的MAC地址，第三列是类型，表示是动态还是静态  dd3c7ed944244ba9eb1f46de3d35a5b  Ping 172.20.0.1,结果如下：  a06917d1e67e5023b5c7f383c099da5  ARP数据包的格式如下图    由九部分组成，分别为硬件类型，占2B，协议类型，占2B，硬件地址长度，占2B，协议地址长度，占2B，OP码，占2B，发送端的MAC地址，占6B，发送端的IP址，占4B，目标MAC地址，占6B，目标IP地址，占4B  判断ARP数据包是请求包还是应答包可以由OP值判断，OP=1：请求包，OP=2：应答包    ARP查询要在广播帧传送的原因是：查询ARP时如果不知道目的IP相应的的MAC地址，就需要在同一广播域进行广播（或不同广播域--交给路由器处理，路由器去别的子网再广播）；ARP响应在明确目的地址的帧中传送的原因是：ARP响应时已经通过送来的查询ARP知道源MAC地址了，所以响应时要明确目的地址，单播发送。   1. 抓取UDP数据包--UDP解析   发送QQ消息后，抓包如下：  a2e7e2076276d8306fb6d46f7682238  QQ发消息过程基于UDP协议，本主机IP地址172.20.53.104，目的主机IP地址39.156.125.82。  f836573534e4bec9965a3ea7d33dfa0  本机端口4020，对方8000  数据报格式为：源端口号 4B，目的端口号 4B，段长度2B，校验和2B，之后是数据部分  服务器返回ICQ数据包的目的是用于确认，表示服务器已收到消息。因为UDP是不可靠数据传输，而QQ需要保障即时通讯的数据传输正确性，所以QQ需要在UDP基础上实现应用层的可靠数据传输，所以要返回ICQ数据包作为确认。UDP是无连接的，与有连接的TCP进行对比，UDP不需要进行三次握手才能进行数据传输，同时中断传输也不需要TCP的四次挥手，因此UDP是无连接的。   1. 利用Wireshark进行DNS协议分析--DNS分析   打开Wireshark，开始捕获，打开网址，得到下面结果  329de99afb280ce20c8d808ee0c26c6  本机IP为172.20.53.104，目的主机IP为10.128.1.114  DNS由UDP实现，可以递归查询、迭代查询  522f84605d47d697afff680b7d273bc  Do query recursively：采用递归查询  详情如下：  **8200a4b641c498909c384234c3200a8** |
| 问题讨论： |
| 所有内容全部完成，报告中的问题均在上述实验结果中回答。 |
| 心得体会： |
| 初步了解了Wireshark捕获数据包的过程，复习了HTTP、TCP、IP、UDP、ARP、DNS等协议以及Ethernet的802.3帧、结构等内容。  对于计算机网络模型有了更加深入的认识。 |