

**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 | 傅浩东 | | 院系 | 软件工程 | | |
| 班级 | 1937102 | | 学号 | 1190202105 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 格物207 | | 实验时间 | 2021.11.20 | | |
| 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： |
| 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. 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： |
| 以文字描述、实验结果截图等形式阐述实验过程，必要时可附相应的代码截图或以附件形式提交。   1. **Wireshark的使用**   启用Wireshark，使用无线网络，选择WLAN进入Wireshark界面。   1. **HTTP分析** 2. HTTP GET/response 交互   启动Web browser，然后启动Wireshark分组嗅探器。在窗口的显示过滤说明处输入“http”，分组列表子窗口中将只显示所俘获到的HTTP报文，开始Wireshark分组俘获。在打开的Web browser窗口中输入地址：http://hitgs.hit.edu.cn/news 。停止分组俘获。   1. HTTP 条件 GET/response 交互   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”）。启动Wireshark分组俘获器，开始Wireshark分组俘获。在浏览器的地址栏中输入URL: http://hitgs.hit.edu.cn/,在浏览器中重新输入相同的URL或单击浏览器中的“刷新”按钮。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 2. 俘获大量的由本地主机到远程服务器的 TCP 分组 3. 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，保存文件。 4. 打开<https://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>，在Browse按钮旁的文本框中输入保存的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按 “Upload alice.txt file”按钮。 5. 启动Wireshark，开始分组俘获。 6. 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。 7. 停止俘获。 8. 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，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。   1. IP分析 2. 通过执行 traceroute 执行捕获数据包 3. 启动Wireshark并开始数据包捕获 4. 启动pingplotter并“Address to Trace Window”域中输入目的地址。 5. Edit->Options->Packet，然后将Packet Size(in bytes,default=56)域改为2000，这样将发送一系列大小为2000字节的包。然后按下“Resume”按钮。 6. 将 Packet Size(in bytes,default=56)域改为3500，发送一系列大小为3500字节的包，然后按下“Resume”按钮。 7. 停止 Wireshark 的分组捕获。 8. 对捕获的数据包进行分析   捕获窗口中，应该能看到由你的主机发出的一系列ICMP Echo Request包和中间路由器返回的一系列ICMP TTL-exceeded消息。选择第一个你的主机发出的ICMP Echo Request消息，在packet details窗口展开数据包的Internet Protocol部分。   1. 抓取ARP数据包 2. 利用MS-DOS命令：arp或c:\windows\system32\arp查看主机上ARP缓存的内容。 3. 在命令行模式下输入：ping 192.168.1.82（或其他 IP 地址） 4. 启动 Wireshark，开始分组俘获。 5. 抓取UDP数据包 6. 启动Wireshark，开始分组捕获； 7. 发送QQ消息给你的好友； 8. 停止Wireshark组捕获； 9. 在显示筛选规则中输入“udp”并展开数据包的细节. 10. 利用Wireshark进行DNS协议分析 11. 打开浏览器键入:www.baidu.com 12. 打开Wireshark，启动抓包 13. 在控制台回车执行完毕后停止抓包，查看Wireshark捕获的DNS报文 |
| 实验结果： |
| 采用演示截图、文字说明等方式，给出本次实验的实验结果。   1. Wireshark的使用   双击WLAN，如下图所示：       1. **HTTP分析** 2. HTTP GET/response交互     根据俘获窗口内容，思考以下问题：   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？**浏览器运行的是HTTP1.1，访问的服务器所HTTP协议的版本号是1.1.** 2. 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/zh，zh表示中文整体，可以是方言、文言文、简繁体等混合内容，zh-CN表示中国大陆中文，默认指简体普通话。** 3. 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？**我的计算机IP地址是2001:250:fe01:130:dcc0:eb49:a8af:8d27，服务器的IP地址是2001:da8:b800:253::dbd9:e219。** 4. 从服务器向你的浏览器返回的状态代码是多少？**200** 5. HTTP 条件GET/response交互     根据俘获窗口内容，思考以下问题：   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？**如上图所示，第一个HTTP GET请求报文中，没有一行是：IF-MODIFIED-SINCE。** 2. 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？**服务器明确返回了文件的内容，可以看到返回的状态代码为200。**      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？**如下图所示，请求报文中有一行IF-MODIFIED-SINCE；该首部行后面所跟信息为缓存文件上次修改的时间。**      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。**服务器对于较晚的HTTP GET请求会的的状态代码为304。服务器并未明确返回文件的内容，根据同一文件前后请求的差别，304代表IF-MODIFIED-SINCE首部行后查询的时间点后没有进行过修改，故直接使用本地没有过期的缓存文件。**      1. TCP分析 2. 俘获大量的由本地主机到远程服务器的TCP分组   发送成功界面：     1. 浏览追踪信息      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？**初始化tcp连接的tcp syn报文段的序号为0；该报文段将SYN标志位置为1，表示该报文段为SYN段用于tcp建立连接。**      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？**SYNACK报文段的序号为0；acknowledgement字段值为1，服务器通过SYN请求报文段的seq序号加1确定acknowledgement字段；在该报文段中，使用flags部分的ack和SYN标志位置为1表示，该报文段为SYNACK报文段。** 2. TCP基础 3. 你能从捕获的数据包中分析出 tcp 三次握手过程吗？**客户机向服务器端发送SYN请求报文，服务器向客户机回复SYNACK报文，客户机向服务器回复ack报文，如下：**      1. 包含HTTP POST命令的TCP报文段的序号是多少？**如下，带有POST命令序号是1**      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？**如上图所示，第六个报文段的序号是6456；发送时间是第一帧发送后13.071365000s；ACK接收时间是第一帧发送后13.373590000s。**        1. 前六个TCP报文段的长度各是多少？**前六个TCP报文段的长度各是：第一个报文长615，后面五个均长1460.**      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？**最小的可用缓存空间是30464；窗口大小始终大于发送方发送的分组的容量，限制发送端的传输以后，接收端的缓存够用**。 2. 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，发送端的报文段序号始终在增加，没有出现重复发送。**      1. TCP连接的throughput (bytes transferred per unit time)是多少？请写出你的计算过程。      1. IP分析      1. 你主机的IP地址是什么？ **172.20.220.236** 2. 在IP数据包头中，上层协议（upper layer）字段的值是什么？ **01**      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。**IP头有20字节，该IP数据包的净载为56-20=36字节**      1. 该IP数据包的净载大小的？**36B** 2. 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**      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？**TTL、checksum和sequence number总是发生改变** 2. 哪些字段必须保持常量？哪些字段必须改变？为什么？**保持常量的是版本号、首部长度、区分服务（Differentiated Services Field）以及协议（始终为ICMP）；必须改变的是TTL、checksum和sequence number，TTL为生存时间，每次转发必然改变，由于TTL的改变，checksum也会改变，sequence number是变化的区分不同的ICMP报文。** 3. 描述你看到的IP数据包Identification字段值的形式。**如下所示，两个字节。**      1. Identification字段和TTL字段的值是什么？**如图，Identification是4633和TTL是225** 2. 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？**Identification变化，区分不同的ICMP time-to-live exceeded消息；TTL不变，均为一次转发** 3. 该消息是否被分解成不止一个IP数据报？**在改变包大小前没有变，改为2000后被分解**   以下为对比图：       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。数据包被分片信息：Flags和offset等信息；第一个而不是最后一个分片：more fragment；分片的长度：1500B和520B。**        1. 原始数据包被分成了多少片？ **分为三片** 2. 这些分片中IP数据报头部哪些字段发生了变化？**标志位部分、more fragments和checksum等部分发生了变化** 3. 抓取ARP数据包 4. 利用MS-DOS命令：arp查看主机上ARP缓存的内容。      1. 在命令行模式下输入：ping 192.168.1.82，启动Wireshark开始分组俘获。如下图所示，第一条为ARP请求报文，广播询问172.20.68.220的MAC地址，第二条为回复报文。        1. 利用MS-DOS命令：arp -a，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? 每个IP地址所对应的物理地址及其类型（动态或静态）。** 2. 清除主机上ARP缓存的内容,抓取ping命令时的数据包。 3. 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？**如下图所示，ARP的数据包格式，由九部分构成，分别有：硬件类型2B，协议类型2B，硬件地址长度1B，协议地址长度1B，OP2B，发送端MAC地址6B，发送端IP地址4B，目的MAC地址6B，目的IP地址4B。**      1. 如何判断一个ARP数据是请求包还是应答包？**检测OP字段，当OP为0x0001时为请求包，OP为0x0002时为应答包。**        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？ **ARP查询不知道目的IP地址所对应的MAC地址，需要广播。ARP响应由查询报文知道查询主机的MAC地址，且局域网中的其他主机不需要此次查询的结果。** 2. 抓取UDP数据包      1. 消息是基于UDP的还是TCP的？**UDP** 2. 你的主机ip地址是什么？目的主机ip地址是什么？**主机IP地址是172.20.81.227，目的主机IP地址是111.30.159.72** 3. 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？**发送QQ消息的端口号：4020，QQ服务器的端口号：8000** 4. 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？**如下图所示，UDP数据包的格式，头部包含源端口号、目的端口号、长度和首部校验和checksum组成，各占2个字节。**      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UDP是不可靠的数据传输，需要上层协议实验可靠数据传输，因此每次发送ICQ报文后又回复一个ICQ数据包。UDP是无连接的，可以看到发送数据之前没有连接的建立过程，与TCP不同，因此为无连接数据传输。** 2. 利用WireShark进行DNS协议分析 |
| 问题讨论： |
| 详见实验结果。 |
| 心得体会： |
| 结合实验过程和结果给出实验的体会和收获。  通过Wireshark分析各种网络协议的执行，可以加深对于各种协议交互过程的理解。并且对于协议中各个字段的作用有了更深的了解。Wireshark是个十分强大的工具，不仅仅在本门实验中会利用到他的一些知识，在以后的学习工作生活中还有很大的作用。 |