

**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 | 王丙昊 | | 院系 | 计算机科学与技术 | | |
| 班级 | 1603108 | | 学号 | 1160300302 | | |
| 任课教师 | 聂兰顺 | | 指导教师 | 聂兰顺 | | |
| 实验地点 | 格物207 | | 实验时间 | 2018.11.21 | | |
| 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、结果以及思考问题：** |
| 1. **Wireshark的使用** 2. 启动web浏览器 3. 启动Wireshark 4. 开始分组俘获：**Capture -> Options**，采用默认设置，点击**start**开始进行分组俘获，所有由默认网卡发送和接收的分组都将被俘获。        1. 开始俘获后，窗口会显示各类已经俘获的数据包。俘获过程中，可以通过Web浏览器访问网页。通过在显示**筛选**规则中输入不同的协议类型（如”http”）来查看不同类型协议的报文。抓包界面如下所示：      1. **HTTP协议分析** 2. **HTTP GET/response 交互**   启动web浏览器以及Wireshark，访问<http://hitgs.hit.edu.cn>，在筛选处输入http    **思考问题：**   1. **HTTP版本**   我的浏览器HTTP版本：HTTP 1.1  所访问的服务器HTTP版本：HTTP 1.1   1. **浏览器向服务器指出能接收何种语言版本的对象**   Accept-Language: zh-CN，即简体中文   1. **计算机IP地址以及服务器IP地址**   本机IP地址：172.20.112.61  所访问服务器IP地址：219.217.226.25   1. **从服务器向浏览器返回的状态代码**   200   1. **HTTP 条件GET/response交互**   清空浏览器的缓存，启动Wireshark，访问<http://hitgs/hit.edu.cn>，再点击刷新**再次访问**该网页，然后在筛选处输入http：  **思考问题：**   1. **在第一个HTTP GET请求中，请求报文中是否有 IF-MODIFIED-SINCE行？**     可以看到在第一个HTTP请求报文中，没有IF\_MODIFIED-SINCE字段   1. **服务器是否明确返回了文件的内容？如何获知？**       当响应报文状态代码为 **200**时，服务器明确返回了文件的内容  当响应报文状态代码为 **304**时，服务器不明确返回文件的内容  **如何获知**：可以从响应报文中是否有data字段，来确定有没有明确返回文件内容。   1. **较晚的HTTP GET请求中，有没有IF-MODIFIED-SINCE行？有的话，该行后面的信息是什么？**     在较晚的HTTP请求报文中，可以看到**有IF-MODIFIED-SINCE首部行**，后面跟着的信息是**时间**，表示询问服务器在改时间后所请求的内容是否有更新。   1. **服务器对较晚的HTTP GET请求响应的HTTP状态代码是多少？是否明确返回了文件的内容？**     对于较晚的HTTP请求的响应报文，由于请求内容并**没有被修改**，所以响应报文中的**状态代码为304**，从响应报文中没有data字段可以看出，**没有明确返回文件的内容**。   1. **TCP协议分析**   访问实验网址，启动Wireshark，上传文件并开始分组俘获，直到上传完毕，停止俘获。    **思考问题：**   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**   172.20.112.61  52564   1. **Gaia.cs.umass.edu服务器的IP地址是多少？对这一链接，用来发送和接收TCP报文的端口号是多少**   128.119.245.12  80   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？**     上图可以看出，初始化TCP连接的报文段的**seq为0**，通过**将其SYN段置1**来表示这是SYN报文段。   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报文段序号为0  Acknowledgement字段的值为1，是根据上一次客户端发给服务器的SYN段的**seq + 1**得到的  通过**将SYN段置1，将ACK段置1**来标识该报文段是SYNACK报文段。   1. **你能从捕获的数据包中分析出TCP三次握手过程吗？**     上图所示为TCP连接建立的三次握手过程。   1. **包含HTTP POST 命令的TCP报文段的序号是多少？**     包含HTTP POST 命令的TCP报文段的序号为 152933.   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？**     第六个报文段 seq = 7017    由上图可以看出，是在HTTP POST（seq=152933）发送之前发送的，所对应的ACK为服务器返回的第六个ACK   1. **前六个TCP报文段的长度各是多少？**     1460 1460 1176 1460 1460 1176   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？**     接收端公示的最小的可用缓存空间为29200，不会出现仍然不够用的情况，因为该窗口大小一直增加   1. **在跟踪文件中是否有重传的报文段？判断的依据？**   没有，依据：客户端发送的seq没有出现重复   1. **TCP连接的throughput是多少？计算过程？**       传输的数据总量为 153014 + 108 \* 54 = 158846B  传输时间为 3.642515 – 2.703985 = 0.93853s  **Throughput =** 158846B / 0.93853s = 169249.784bps   1. **IP协议分析** 2. **通过pingplotter程序来发送数据包**   启动Wireshark，利用pingplotter发送具有**不同大小的数据包**给目的主机，分析程序发送和接收到的IP数据包。     1. **对捕获的数据包进行分析** 2. 在捕获窗口中，选择主机收到的第一个主机发出的ICMP Echo Request消息，在pachet details窗口展开数据包的Internet Protocol部分。     **思考问题：**   1. **你主机的IP地址是什么？**   172.20.112.61   1. **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？并解释你是怎么确定的**   IP头为20字节，数据包的总长度为56字节，所以净载为36字节。   1. **该IP数据包的净载大小？**   36字节   1. **该IP数据包分片了吗？解释你是如何确定的。**     没有分片，由于Flag字段全为0，并且片偏移为0   1. 单机Source列按钮，将捕获的数据包按源IP地址排序。选择第一个主机发出的ICMP Echo Request消息，在pachet details窗口展开数据包的Internet Protocol部分。在“listing of captured packets”窗口，会看到许多后续的ICMP消息。     **思考问题：**   1. **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   1. **哪些字段必须保持常量？哪些字段必须改变？为什么？**     可以看出，除了ID、TTL、Header checksum之外的字段**保持常量，**而ID、TTL、Header checksum必须改变。   1. **描述你看到的IP数据包Identification字段值的形式。**   为4位16进制的数，也就是16位。   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。   **思考问题：**     1. **Identification字段和TTL字段的值是什么？**   Identification：0x0000  TTL：254   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？**   不变。因为都是第一跳路由器返回的数据包，所以TTL字段都是可取的最大值；相同的标识是为了分段后进行重组，给同一个主机返回的标识不代表序号，因此Identification字段也不变。   1. 对捕获的数据包按时间排序。找到在将包大小改为2000字节后主机发送的第一个ICMP Echo Request消息。   下图为改为2000字节后，主机发送的第一个ICMP Echo Request消息：    **思考问题：**   1. **该消息是否被分解成不止一个IP数据报？**   可以看到，该消息被分解成不止一个IP数据报。   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头部的那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？**     发生了分片，找到No.594的报文，由flag中的 **MF=1** 可知，该分片是第一个而不是最后一个分片。由Data字段为1480字节可知，该分片的长度为**1500字节**。   1. 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。   **思考问题：**   1. **原始数据包被分成了多少片？**     被分成了**三片。**   1. **这些分片中IP数据报头部哪些字段发生了变化？**         前两个分片的 **MF段**为1，后两个分片的**片偏移**发生了变化。   1. **Ethernet数据帧分析**   上图为ICMP报文的Ethernet Ⅱ信息。**源MAC地址**：58:59:6c:a5:e2:d3，**目的MAC地址**：74:e5:f9:af:8d:1d，Type : IPv4(0x0800)  对于其他类型的报文Ethernet数据帧分析与上面类似。   1. **DNS协议分析**   实验步骤：   1. 打开Wireshark，启动抓包 2. 打开浏览器键入：[www.baidu.com](http://www.baidu.com) 3. 在控制台回车执行完毕后停止抓包。 4. **DNS查询消息**如下所示：      1. 由上图可以看出，本机的IP地址为172.20.11.183，**本地域名服务器的IP地址为114.114.114.114** 2. DNS查询报文的内容如下所示：      1. DNS回复消息：      1. **UDP协议分析**     **思考问题：**   1. **消息是基于UDP的还是TCP的？**   基于UDP的。   1. **你的主机IP地址是什么？目的主机IP地址是什么？**     主机的IP地址为172.20.11.183，目的主机的IP地址为111.20.159.72   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？**   我的端口：4025  服务器端口：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？**   UDP数据报包括**首部字段和数据字段**，其中首部字段包括：  源端口号：16位  目的端口号：16位  长度：16位  校验和字段：16位   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？这与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？**   因为服务器应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，并不能保证数据一定送达。  可以看出。可以看出在传输开始时，没有连接建立的过程，也就没有初始序列号的交换，因此发送的数据也是乱序的。   1. **ARP协议分析** 2. 利用MS-DOS命令：arp或c:\windows\system32\arp 查看主机上ARP缓存的内容。     **思考问题：**   * 1. **说明ARP缓存中的每一列的含义是什么？**   第一列：IP地址  第二列：物理地址（MAC地址）  第三列：类型，如果是动态类型，过一段时间会被删除。   1. 在命令行模式下输入：ping 192.168.1.82。     **思考问题：**     * 1. **ARP数据包的格式是怎么样的？由几部分构成，各个部分所占的字节数是多少？**   由上图可以看出**ARP数据包的格式**：  硬件格式：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  目标MAC地址：6字节  目标IP地址：4字节   * 1. **如何判断一个ARP数据是请求包还是应答包？**   如果**OP字段**为1(0x0001)，说明为请求包；如果OP字段为2(0x0002)，说明为应答包。   * 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？**   因为进行ARP查询时，并不知道其所在主机的MAC地址，因此采用广播的方式；应答时，主机可以从查询报文中获得查询主机的MAC地址，并且局域网中的其他主机不需要该响应信息，所以在有明确的局域网地址的帧中传送。 |
| **心得体会：** |
| 1. 巩固了本学期所学习的知识，并有了进一步的了解； 2. 掌握了Wireshark工具进行抓包并分析的方法； 3. 了解了各网络协议之间进行报文交换的情况。 |