

**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 | 梅智敏 | | 院系 | 计算机院软件工程 | | |
| 班级 | 1837101 | | 学号 | 1183710118 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 格物213 | | 实验时间 | 2020.11.21 | | |
| 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 | | | | | | |
|  | | | | | | |

**计算学部**

|  |
| --- |
| 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： |
| * 学习 Wireshark 的使用 * 利用 Wireshark 分析 HTTP 协议 * 利用 Wireshark 分析 TCP 协议 * 利用 Wireshark 分析 IP 协议 * 利用 Wireshark 分析 Ethernet 数据帧   选做内容：   * 利用 Wireshark 分析 DNS 协议 * 利用 Wireshark 分析 UDP 协议 * 利用 Wireshark 分析 ARP 协议 |
| 实验过程及结果： |
| 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   从官网下载安装之后选择网络接口为WLAN（因为我用的是校园网）    选择之后便开始自动抓取数据包，我们可以从过滤器中筛选数据包类别    利用Wireshark可以对数据报的各个字段进行查看分析     1. HTTP分析 2. HTTP GET/response 交互   首先启动谷歌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。  然后在打开的谷歌浏览器地址栏输入今日哈工大的网址：<http://today.hit.edu.cn/>即可     * 浏览器运行的协议版本为HTTP 1.1      * 所访问的服务器运行的协议版本是HTTP 1.1      * 浏览器向服务器指出它能接收的语言版本为：zh-CN      * 本机IP地址为：172.20.46.136   服务器IP地址为：202.118.254.117     * 服务器向你的浏览器返回的状态代码为：200      1. HTTP 条件 GET/response 交互   首先清空谷歌浏览器的缓存数据    然后再连续访问2次<http://today.hit.edu.cn/>即可   * 浏览器向服务器发出的第一个 HTTP GET 请求的内容中，并无IF-MODIFIED-SINCE      * 分析服务器响应报文的内容，服务器明确返回了文件的内容，通过状态码获知。     通过状态码为200可以获知明确返回了文件内容    而且相应报文中也确实携带了数据   * 浏览器向服务器发出的较晚的“HTTP GET”请求，报文中有IF-MODIFIED-SINCE字段，   且在该首部行后面跟着的信息是本地缓存文件的最新版本（用时间来表示）     * 服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是304，服务器未返回   文件的内容。解释如下：若本地有目的URL的缓存文件，客户端会构造请求报文来确认该报文是否是最新版本；若是，则返回状态码304，并且不携带数据，客户端直接从本地缓存中获取文件内容即可。     1. TCP分析   首先启动浏览器，进入指导书中的URL，得到文本文件如下    然后在给定网站中进行上传该文件即可    下面对我们的追踪信息进行分析     * 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址为：172.20.110.138   TCP 端口号是4219  Gaia.cs.umass.edu 服务器的 IP 地址是183.62.127.13  对这一连接，它用来发送和接收 TCP 报文的端口号是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:3968988941  在该报文段中，用SYN标志位为1来标示该报文段是 SYN 报文段    上图中，各个Flags只有Syn为1，其余皆为0   * 服务器向客户端发送的 SYNACK 报文段序号是：1669533493   该报文段中，Acknowledgement字段的值是：3968988942  Gaia.cs.umass.edu 服务器是如何决定此值的：其值就是客户端的SYN报文段的序列号加一  在该报文段中，是用什么来标示该报文段是SYNACK 报文段的：将ACK和SYN标志位同时置1，其余标志位为0     * 可以从捕获的数据包中分析出TCP的三次握手   可以从它们的标志位明显看出来     1. 包含 HTTP POST 命令的 TCP 报文段的序号是0x360b3afa，即第一个SYN报文段序号+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0x360b542e  发送时间为：三次握手建立TCP连接之后，四次握手断开连接之前  该报文段所对应的 ACK 确认号所对应的报文是：第三次握手时接收的         1. 前六个 TCP 报文段的长度各是多少？      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：29200     限制发送端的传输以后，接收端的缓存是否仍然不够用？：在限制发送方的传输之后，接收端的缓存空间大小开始不断增大，说明空间够用。     1. 在跟踪文件中是否有重传的报文段？：不存在   进行判断的依据是什么？：序列号一直在严格递增     1. TCP 连接的 throughput (bytes transferred per unit time)是多少？：109730.9Bps   请写出你的计算过程：总字节数/总时间=152935/（4.814917-3.421189）=109730.9Bps         1. IP分析  * 选择第一个主机发出的ICMP Echo Request消息     你主机的IP地址是什么：172.20.57.89    在IP数据包头中，上层协议（upper layer）字段的值是什么：1    IP头有多少字节：20 该IP数据包的净载为多少字节：36  并解释你是怎样确定该IP数据包的净载大小的：总长度-头部长度    该IP数据包分片了吗：未  解释你是如何确定该P数据包是否进行了分片：标志位全0     * 分析源主机发出的一系列报文     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：标志ID、TTL、checksum、数据域  哪些字段必须保持常量？哪些字段必须改变？为什么？  答：除了上述4个字段之外，其他字段必须保持常量。原因是：表示ID唯一、随之checksum也不同、TTL在变大（由于ICMP的ping检测），而且数据域中封装有ICMP的报文，故数据域也在变化  描述你看到的IP数据包Identification字段值的形式。    答：16b数据，线性递增   * 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：1109 TTL字段的值是：58    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，但是TTL不变。因为：第一跳路由器设置TTL字段为REC指定的值，故不变；但是ID唯一标识一个IP数据报，故变化。   * 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：被分解为2片  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  答：第一个分片中的标志位MF被置为1，说明后面还有分片该分片数据长度为1480B，IP总长度为1500B       * 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？  答：MF变化，片偏移变化，第一个和第二个分片的标志位MF=1，第一个分片的片偏移为0，第二个是185，第三个是370       1. Ethernet数据帧分析   你的主机IP和目的主机IP是什么？    我的主机发送的第一跳的HTTP请求报文的帧结构是什么？封装了上层哪些数据？  答：以太网帧封装了上层的IP数据报，IP封装了上层的TCP数据报，TCP数据包封装了上层的HTTP数据。  我的主机mac地址为和目的主机mac地址如下：    发送数据域长度范围：46B-1500B  计算过程：  MTU=1500B，故数据域最长为1500B     1. 抓取ARP数据报  * 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?     第一列是ARP协议缓存的IP地址，第二列是对应的MAC地址，第三列是类型   * 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       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：    如何判断一个ARP数据是请求包还是应答包？  通过“OP”字段的值来判断：当其值为 0×0001 时是请求，为 0×0002 时是应答。  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ARP查询不知道目的MAC地址，故需要广播；ARP在接收到的ARP查询中知道了源MAC地址，故在有明确目的局域网地址的帧中传输。   1. 抓取UDP数据报      * 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？      * 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？      * 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？      * 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？  答：服务器返回ICQ数据包是为了确认收到，因为UDP是不可靠无连接传输，客户端无法确认服务器是否已经收到了数据，所以需要服务器返回ICQ报文  可以看出UDP是无连接的，因为UDP首部无标志位，也无序列号   1. DNS协议分析      * 主机IP和目的IP      * DNS下层协议为：UDP      * DNS的一对查询与响应报文的ID相同          * 请求内容如下，包含“Name”“Type”“Class”等字段      * 响应报文同样包含上述字段 |
| 问题讨论： |
| 全部的思考问题已经在前面的实验过程中给出答案，故此处不再赘述。 |
| 心得体会： |
| 1. 掌握了Wireshark的基本使用方法，知道如何利用它来进行抓包分析 2. 通过对各层数据报文的结构分析，我对计算机网络的分层协议有了更深入的理解   其实就是通过各层协议将上层的数据分组加上本协议的头部字段和尾部字段，从而转入下一层进行传输，当接受方收到相应的数据报时，按照协议进行解析即可。   * 应用层：支持各种网络应用 * 传输层：TCP、UDP等进程间通信协议 * 网络层：通过路由存储转发将数据分组从源主机送到目的主机，如IP协议 * 链路层：进行相邻网络设备之间的数据传输，如：Ethernet |