

**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 | 瞿久尧 | | 院系 | 计算学部 | | |
| 班级 | 2037101 | | 学号 | 120L022314 | | |
| 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 | 2022.10.28 | | |
| 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： |
| * 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： |
| 1. **wireshark的使用**          1. **HTTP 分析**   访问http://www.hit.edu.cn   1. HTTP GET/response 交互  * 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？   我的浏览器：HTTP1.1  服务器：HTTP1.1     * 你的浏览器向服务器指出它能接收何种语言版本的对象？   中文     * 你的计算机的 IP 地址是多少？服务器http://www.hit.edu.cn的 IP 地址是多少？   我的计算机：172.20.157.186  服务器：61.167.60.70   * 从服务器向你的浏览器返回的状态代码是多少？   200ok     1. HTTP 条件 GET/response 交互  * 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？   否     * 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，由content-length可知。     * 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？   否，但如果有，跟的信息应该是最近一次修改时间。  IMG_256   * 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。   304not modified，服务器没有明确返回文件的内容，但是给出了ETag，浏览 器可以在此缓存中查找文件，其值与第一次返回的报文的ETag一致。   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  B.浏览追踪信息   * 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？   IP地址：172.20.157.186  端口号：50448     * 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？   IP地址：128.119.245.12  端口号：80    C. TCP 基础   * 客户服务器之间用于初始化TCP连接的TCPSYN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seq为0  通过设置tcp头部flags字段的syn标志位来标示该报文段是 SYN 报文段。       * 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？   序列号：0  Acknowledgement 字段：1  服务器收到客户端发来的syn报文，此报文消耗一个序列号（0），因此服务器回 复期望收到的下一个序列号的值为1  通过设置tcp头部flags字段的syn标志位来标示该报文段是SYNACK报文段     * 你能从捕获的数据包中分析出 **tcp** 三次握手过程吗？          * 包含 HTTP POST 命令的 TCP 报文段的序号是多少？   152741     * 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？   序号：6187  在http post发送之前发送  对应的ack是服务器发送的第6个ack       * 前六个 TCP 报文段的长度各是多少？   747，1360，1360，1360，1360，1360     * 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239，够用，因为该窗口大小会一直增加     * 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？   否，应为客户端发送的seq并不重复   * TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。   头部为54B，共106个包，106\*54 = 5724B  总传送数据为152982 +　5724 = 158706B  时间间隔：5.073677 – 4.329848 = 0.743829s  throughput = 158706B/0.743829s = 213363.555Bps |
| 实验结果： |
| 1. **IP分析** 2. 通过执行 traceroute 执行捕获数据包 3. 对捕获的数据包进行分析  * 你主机的IP地址是什么？   172.20.157.186     * 在IP数据包头中，上层协议（ upper layer）字段的值是什么？   01     * 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头部有20字节  净载为36字节（净载= total length - 头部大小）     * 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，因为Don’t fragment 为1，More segments 为0.     * 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   * 哪些字段必须保持常量？哪些字段必须改变？为什么？   ID必须改变，因为其为鉴别吗，用以区分不同的数据包  TTL必须改变，来自traceroute的要求，用来测试路径上的路由信息  Header checksum 必须改变，这是首部校验和，前面的字段改变该值会随之改变。   * 描述你看到的IP数据包Identification字段值的形式。   16bit，在某一范围内递增。   * Identification字段和TTL字段的值是什么？   Identification：50196  TTL：124     * 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。   * 该消息是否被分解成不止一个IP数据报？   是，分解为了2个     * 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?   more segment为1，表明被分片了，且当前不是最后一片，该分片长度为 1500Byte。  C.   * 原始数据包被分成了多少片？   3     * 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 more segment 为1， 最后一个为0。  第一个分片偏移为0，第二个为1480，第三个为2960。   1. **抓取 ARP 数据包**  * 说明 ARP 缓存中每一列的含义是什么?   第一列：IP地址  第二列：MAC地址  第三列：类型（静态不变，动态超过一定时间，记录会被删除）     * 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？   查看arp解析即可知格式，查看每一部分所占位数即可知所占字节数  hardware type:16bit  protocol type:16bit  hardware size:8bit  protocol size:8bit  opcode:16bit  sender mac address:48bit  sender ip address:32bit  target mac address:48bit  target ip address:32bit     * 如何判断一个ARP数据是请求包还是应答包？   根据opcode值：  请求：opcode = 1  应答：opcode = 2       * 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？   查询时没有相应的mac地址，即无法在链路层装配该ip地址的mac帧，因而采用广 播的方式；应答时，主机可以从arp请求中知道源主机的mac地址，因此对特定主 机应答，从而减少网络流量的耗费。   1. **抓取 UDP 数据包**  * 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?   我的：172.20.157.186  目的：61.149.23.29     * 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：4007  目的：8000     * 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？     source port:16bit  destination port:16bit  length:16bit  checksum:16bit   * 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？   因为服务器应返回接受的结果给客户端。  可以看出udp的不可靠数据传输，因为只提供了一次返回的ack，没有保证数据一 定送达。  还可以看出udp数据包没有序列号，因此不能像tcp协议一样先握手再发送数据， 因此发送的数据是乱序的。   1. **利用 WireShark 进行 DNS 协议分析** |
| 问题讨论： |
| 无。 |
| 心得体会： |
| 通过本次实验，我对http, tcp, udp, ip, arp, dns等报文的结构有了全面的了解，并对tcp连接的建立过程和数据传输过程有了更为清晰的认识。 |