

**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 | 姜思琪 | | 院系 | 计算机科学与技术学院 | | |
| 班级 | 1603109 | | 学号 | 1160300814 | | |
| 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 | 2018.11.17周六3、4节 | | |
| 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： |
| 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) 学习 Wireshark 的使用  登陆界面：    2) 利用 Wireshark 分析 HTTP 协议    **思考问题：**  **A.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？**  我的浏览器运行的是HTTP 1.1；服务器：HTTP1.1  **B.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，简体中文  **C.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：192.168.199.183；服务器：219.217.226.25  **D.从服务器向你的浏览器返回的状态代码是多少？**  200  **2）HTTP 条件 GET/response 交互**    **思考问题：**  **A.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？**  没有  **B.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？**  服务器返回了内容。因为在当状态代码为 304 时不明确返回文件；而状态代码为 200 时明确返回文件。  **C.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？**  有，后面带着的是时间。是询问服务器在这个时间后还有没有更新。    **D.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。**  状态代码是304。不会明确返回文件，因为根据之前 HTTP 的 GET 请求中 IF-MODIFIED-SINCE的时间服务器判断结果为 Not Modified，于是客户端会使用本地这个没有过期的缓存文件。    3) 利用 Wireshark 分析 TCP 协议      **思考问题：**  **A.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？**  192.168.199.183  58607  **B.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？**  128.119.245.12  80  **C.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？**  是0。将flags标志位置为1.  **D.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？**  服务器端向客户端发送的报文段序号为 0； 服务器发的 acknowledgment number 字段是根据上一次客户端发给服务器的 seq+1 得到的； 通过Flags标志位中的SYN位和ACK位都是1来确定该报文段是一个SYN ACK 报文段的。    **E.你能从捕获的数据包中分析出 tcp 三次握手过程吗？**  可以看到连续的三个包，第一次有SYN，第二次有SYN ACK，第三次有ACK。    **F.包含 HTTP POST 命令的 TCP 报文段的序号是多少？**  152416    **G.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？**  第六个序列号是6416，在 http post 发送之前，tcp 连接建立之后发送。      对应的 ack 即为服务器返回的第六个 ack。    **H.前六个 TCP 报文段的长度各是多少？**    如图。  **I.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？**  如图，接收端公示的最小的可用缓存空间是 29200，该窗口大小会一直增加， 所以不会出现接收端的缓存是否仍然不够用的情况。    **J.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？**    没有出现重传，因为客户端发送的报文序列号没有出现重复。  **K.TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。**  由图，发送数据总的长度152903B+106\*54=158627B；发送时间间隔约1.673847s；因此吞吐量为158627B/1.673847S=94767.92bps。  4) 利用 Wireshark 分析 IP 协议  （1）在你的捕获窗口中，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。  思考问题：  **A.你主机的IP地址是什么？**  192.168.199.183    **B.在IP数据包头中，上层协议（upper layer）字段的值是什么？**  01    **C.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 头有 20 字节。  IP 包的净载为 Total Length-Header Length=56B-20B=36B    **D.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，分片位移为 0，More fragments 为 0 表示后面无分段。    （2）单击Source列按钮，这样将对捕获的数据包按源IP地址排序。 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。在“listing of captured packets”窗口， 你会看到许多后续的ICMP消息（或许还有你主机上运行的其他协议的数据包）  思考问题：  **A.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 checksun 这三个字段总在变化。  **B.哪些字段必须保持常量？哪些字段必须改变？为什么？**  必须改变：  ID鉴别码，用于区分不同数据包；  TTL来自于traceroute的要求，用来测试路径上的路由信息；  Header Checksum首部校验和，前面的字段改变，该值也必须跟着改变；  必须保持常量：  除以上(ID,TTL,Header Checksum) 外的字段保持常量。  **C.描述你看到的IP数据包Identification字段值的形式。**  16位，在某一范围内是+1递增的。        （3）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：  **A.Identification字段和TTL字段的值是什么？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，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 ICMP，标识不代表序号， TTL 消息是相同的，因此 Identification 不变;因为是第⼀跳路由器发回的数据报，故 TTL 是最⼤值减1，总是等于 254。  （4）单击Time列按钮，这样将对捕获的数据包按时间排序。找到在 将包大小改为2000字节后你的主机发送的第一个ICMP Echo Request消息。  思考下列问题：  **A.该消息是否被分解成不止一个IP数据报？**  是的，该消息被分解成了 2 片    **B.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 fragments=1 表⽰分⽚了且不是最后⼀⽚，该分⽚的长度是 1500B    C. 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。  **A.原始数据包被分成了多少片？**  三片    **B.这些分片中IP数据报头部哪些字段发生了变化？**  前 2 个分⽚More fragments=1，后两个分⽚offset 变为 1480 和 2960  选做内容：  **a) 利用 Wireshark 分析 DNS 协议**  打开浏览器输入[www.baidu.com](http://www.baidu.com)，DNS查询消息如下：    我的电脑IP地址：192.168.199.183，本地域名服务器IP地址：192.168.199.1 如图：    UDP 报文的源端口号 54953，目的端口号 53    DNS 查询报文内容如下图，表示查询主机域名为 sp0.baidu.com 的主机的 IP 地址    DNS回复信息：    主机域名为 sp0.baidu.com 的主机 IP 地址为：119.75.217.109  **b) 利用 Wireshark 分析 UDP 协议**  分析 QQ 通讯中捕获到的 UDP 数据包。根据操作思考以下问题：  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？  我的主机 IP 地址：192.168.199.183 ;目的主机 IP 地址：182.254.33.150    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 消息端口号：4019; QQ 服务器端口号：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？  格式类似下表：   |  |  |  |  | | --- | --- | --- | --- | | 来源端口 | 目的端口 | 长度域 | 校验和 |   UDP 数据报格式有首部和数据两个部分。首部很简单，共 8 字节。包括：  源端口号： 2 字节  目的端口号： 2 字节  长度： 2 字节， UDP 用户数据报的总长度，以字节为单位。  校验和： 2 字节，用于校验 UDP 数据报的数字段和包含 UDP 数据报首部的“伪首部”。 其校验方法同 IP 分组首部中的首部校验和。  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？  因为服务器需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，所以不保证数据一定送达。 可以看出。 UDP 数据包没有序列号，因此不能像 TCP 协议那样先握手再发送数据，因为每次只发送一个数据报，然后等待服务器响应。  **c) 利用 Wireshark 分析 ARP 协议**  **（1）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?**  输入 apr –a 查看主机上 ARP 缓存的内容，结果如下图所示：    ARP 缓存中的每一列分别表示 IP 地址所对应的物理地址和类型（动态配置或静态配置）  **（2）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,回答下面的问题：**  **A.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？**  格式如图：      由 9 部分构成，分别是硬件类型（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），目的 MAC 地址（6 字节），目的 IP 地址（4字节）。  **B.如何判断一个ARP数据是请求包还是应答包？**  通过 OP 字段。当 OP 字段值为 0x0001 时是请求包，当 OP 字段值为 0x0002时是应答包。  下图是请求包：    下图是应答包：    **C.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 查询时并不知道目的 IP 地址对应的 MAC 地址，所以需要广播查询；而 ARP 响应报文知道查询主机的 MAC 地址（通过查询主机发出的查询报文获得），且局域网中的其他主机不需要此次查询的结果，因此 ARP 响应要在一个有着明确目的局域网地址的帧中传送。 |
| 实验结果： |
| 本次实验是利用Wireshark来分析各种协议。所以实验结果截图均在实验过程中给出，同时给出了分析结果。实验过程是结合每个实验后面的思考题进行分析和总结的。 |
| 问题讨论： |
| 本次实验过程是结合每个实验后面的思考题进行分析和总结的，在这个过程中中，我发现需要注意以下问题：  在安装Wireshark时，不可以在中文目录下安装，容易出现编码错误；  抓包会抓到很多不知名的包，是因为电脑后台有很多程序再运行，所以也会抓到它们的包。 |
| 心得体会： |
| 通过本次实验，我学会了使用Wireshark 工具进行抓包，然后看到具体的包进行协议的分析；对各个协议的报文格式以及工作过程都有了进一步的认识与掌握，从以前的了解到深刻的学习；了解了网络之间如何通信，了解了网络协议实体间进行交互及报文交换的情况。 |