

**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 | 贺宗磊 | | 院系 | 计算机科学与技术 | | |
| 班级 | 1703202 | | 学号 | 1170300421 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 格物214 | | 实验时间 | 2019.11.9 | | |
| 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： |
| （注：实验报告模板中的各项内容仅供参考，可依照实际实验情况进行修改。）  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： 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： |
| 详情见实验结果（包含实验过程） |
| 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   启动主机上的 web 浏览器。 启动 Wireshark。你会看到如图 6-2 所示的窗口，只是窗口中没有任何分组列表。 开始分组俘获：选择“capture”下拉菜单中的“Capture Options”命令，会出现如图 6-3 所示的“Wireshark: Capture Options”窗口，可以设置分组俘获的选项。 在实验中，可以使用窗口中显示的默认值。在“Wireshark: CaptureOptions”窗口的最上面有一个“Interface List”下拉菜单，其中显示计算机所具有的网络接口（即网卡）。当计算机具 有多个活动网卡时，需要选择其中一个用来发送或接收分组的网络接口（如某个有线接口）。随后，单击“Start”开始进行分组俘获，所有由选定网卡发送和接收的分组都将被俘获。通过操作连接<http://www.hit.edu.cn>网站  结果如图：     1. HTTP分析 2. **HTTP GET/response** 交互，输入网址<http://news.hit.edu.cn/>进行捕获   截图如下：      思考题：   1. 浏览器运行的是HTTP1.1,所访问的服务器运行的HTTP协议是HTTP1.1 2. 浏览器向服务器指出它能接收语言版本是zh-CN,zh,即表示中文 3. 我的计算机IP地址为：172.20.21.54   服务器<http://news.hit.edu.cn/>的IP地址为：202.118.254.136   1. 服务器向你、我的浏览器返回的状态代码是200 2. **HTTP** 条件 **GET/response** 交互   清除缓存数据    运行结果如图：      思考题：   1. 通过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，没有一行是： IF-MODIFIED-SINCE 2. 服务器明确回复了文件内容   分析：由结果可知，由如下数据行：    且之后显示状态码为200，所以有传输数据且成功  3.由运行结果可知：    在发出较晚的“HTTP GET”请求后，有一行IF-MODIFIED-SINCE，跟在后面的信息是  缓存最后更新的时间。用于询问服务器该文件在这个时间之后是否发生了修改,如果没有发生修改,浏览器就直接使用缓存,如果发生了修改,则服务器返回更改后的新document   1. 服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是304，服务器没有明确返回文件，有如下截图可知，状态码为304，即服务器判断为Not Modified，表示缓存没有更新，客户端可以直接使用缓存文件。截图如下：      1. TCP分析 2. 向服务器传送文件的客户端主机的 IP 地址：192.168.199.145 TCP 端口号是：60208   截图：     1. Gaia.cs.umass.edu 服务器的 IP 地址是：128.119.245.12   对这一连接，它用来发送和接收 TCP 报文的端口号是：80  截图：    C. TCP 基础 3）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：0  在该报文段中，是用什么来标示该报文段是 SYN 报文段的？  答：通过 Flags 标志位，表示该报文段是 SYN 报文段（将其中的 SYN 位置为 1）  截图如下：  4）服务器向客户端发送的 SYNACK 报文段序号是：0  该报文段中Acknowledgement 字段的值是：1  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？  答：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。  截图如下：  6）你能从捕获的数据包中分析出 **tcp** 三次握手过程吗？  截图如下：  7）包含 HTTP POST 命令的 TCP 报文段的序号是：1  见如图：    8）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：6534  第六个报文段是何时发送的？  答：2.189072  该报文段所对应的 ACK 是何时接收的？  答：2.480555  见如图：        9）前六个 TCP 报文段的长度各是多少？  答：693B，1460B,1460B,1460B,1460B,1460B  见如图：    10）在整个跟踪过程中，接收端公示的最小的可用缓存空间是：29200B  结果如图：  限制发送端的传输以后，接收端的缓存是否仍然不够用？  答：够用。该窗口大小一直增加， 没有出现接收端的缓存是否仍然不够用的情况。  11）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？  答：没有。判断的依据是如果有相同seq的报文段被发送,表示重传该报文段，经查勘没有相同的seq报文段，所以没有发生重传。  12）TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。  答：在第一个包含post的数据报被传输时,时间是2.188790,其seq是1,在2.7882736s时,找到这个时候的一个数据帧:其seq是42267,其吞吐量大约是70.505KB/s   1. IP分析   下载安装pingplotter软件，按照实验指导书设置  结果如图：    捕捉后截图如下：    思考题   1. 主机的IP地址是：192.168.199.145   2）在IP数据包头中，上层协议字段的值是：ICMP(1)  3）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  答：IP头有20字节，该IP数据包的净载为36字节。由数据包可知Total=56,数据头为20，所以净字节=56-20=36B  截图图下：    4）该IP数据包的净载大小的？  答：IP数据包的净载为36字节  5）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  答：这个数据报没有分片,因为其MF标志位是0,且fragment offset的值是0,表示这个ip分组是最后一个分组,且offset为0,所以一定是没有分组的ipv4数据报。  截图如下：    6）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？  答：ip分组中TTL 字段 header checksum字段 和 identification 字段的值总是在发生改变。  7）哪些字段必须保持常量？哪些字段必须改变？为什么？  答：Version, protocol字段必须保持常量,而和identification和header checksum,以及TTL字段必须改变。version和protocol对于ICMP协议都是固定不变的,而每次的identification 因为是在发送时随机选取,所以一定会不一样,而TTL,因为是要trace router,所以每次发送的ICMP报文的TTL都依次+1,所以一定不一样,而checksum的值与所有字段的 值有关,所以只要有字段的值发生改变,check sum的值一定会发生改变。  identification字段的格式是四个16进制的数字,大小为2字节  8）描述你看到的IP数据包Identification字段值的形式  答：加一递增的16位，同一分片内不变。  找到由最近的路由器（第一跳 ）返回给你主机的 ICMPTime-to-live exceeded消息  9）Identification字段是：0  TTL字段的值是是；254  截图如下：    10）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？  答：是。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都是最大值减一，即254  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  截图如下：    11）该消息是否被分解成不止一个IP数据报？  答：是。因为包的大小为2000字节，而实际包的大小为520字节，所以一定被分解成不止一个IP数据报  12）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：MF=1表明其确实发生了分组, fragment offset的值为0表明这个分组是最后一个分组。  该分片的长度是：1500B，520B  截图如下：    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  截图如下：    11）原始数据包被分成了多少片？  答：3片，  截图：    12）这些分片中IP数据报头部哪些字段发生了变化？  答：前两个分片More fragments=1，后两个分片offest变为了1480和2960   1. 抓取ARP数据包   利用 MS-DOS 命令： arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容    抓取后结果：      思考题：   1. 结果如图：     每个IP地址所对应的物理地址及其类型，动态或是静态  清除主机上 ARP 缓存的内容,抓取 ping 命令时的数据包  结果如图：     1. 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？   答：格式如图：    一共有9部分：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）   1. 如何判断一个ARP数据是请求包还是应答包？   答：arp request的数据包:    由9部分组成  Hardware type 表示使用的链路层硬件类型 2bytes  Protocol 表示协议的类型 2bytes  Hardware size 为6 与 mac地址的大小6字节对应 1bytes  op用来标识是request 类型的arp还是 response类型的arp 2bytes  之后是source mac address 6bytes 和source IP address 4bytes  以及 destination mac address 6bytes 和 destination IP address 4bytes  在OP字段中,0×0001 时是请求，为0×0002 时是应答请求。  4）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？  答：Request 使用的是广播地址,是因为它不知道ip对应的mac地址是多少,所以只能通过广播的形式发出,但是如果对应ip的主机收到了这个广播帧,则必须针对性的告知request主机自己的mac是多少,没有必要再广播地址。   1. 抓取UDP数据包   登录qq，给一位好友发消息，同时捕捉，得出结果  结果如图：    思考题：   1. 消息是基于UDP的还是TCP的？   答：UDP  结果如图：     1. 你的主机ip地址是：192.168.199.145   目的主机ip地址是：111.30.159.76  结果如图：     1. 主机发送QQ消息的端口号：4012   和QQ服务器的端口号是：8000  结果如图：     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？   答：数据报的格式是:  Source port 源端口号 占2bytes  Destination port 目的端口号 占2bytes  Udp长度 指udp数据报的整个长度 占2bytes  Udp校验和 占2bytes  之后是数据字段   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？   答：在客户端发送了一个UDP给QQ服务器之后,QQ也会给客户端发送一个UDP数据报,表示服务器已经收到消息  因为UDP是不可靠数据传输,但是QQ作为一个及时通讯软件,所以必须要在UDP的基础上(在应用层)自己实现一个可靠的数据传输,所以出现了服务器会立即给客户端发送UDP确认数据报的情况  通过与TCP协议的对比,可以发现UDP是没有连接的建立过程的,可以直接从源IP地址的源端口发送数据报给目的IP的目的端口,且如果没有数据发送,可以直接停止传输;而TCP如果想要发送数据,则必须要先通过三次握手建立连接,双方才可以互相发送数据报,同时,如果TCP链接想要中断,则必须要通过四次数据交换才能中断连接,由此可以看出,UDP协议是无连接协议,而TCP是有连接的协议。   1. 利用 **WireShark** 进行 **DNS** 协议分析 2. 打开浏览器键入:www.baidu.com 3. 打开浏览器键入:www.baidu.com 4. 打开 Wireshark,启动抓包   结果如图：      DNS报文格式分为五大部分。分别为： 报文头Header， 问题区段（Question），回答区段（Answer），权威区段（Authority）， 额外信息区段（Additional）。但是不是五个段必须存在，只有Header必须存在，别的段在不同情况下不存在。  结构如图：    DNS ID号（DNS ID Number）： 用来对应DNS查询和DNS响应  查询/响应（Query/Response， QR）： 用来指明这个报文是DNS查询还是响应，占1个比特位。为1代表响应，0代表查询  操作代码（OpCode）：用来定义消息中请求的类型  权威应答（Authoritative Answer， AA）：这个比特位在响应的时候才有意义。则说明这个响应是由域内权威域名服务器发出的  截断（Truncation， TC）：用来指出报文比允许的长度还要长，导致被截断  期望递归（Recursion Desired, RD）：如果设置了RD，就建议域名服务器进行递归解析，递归查询的支持是可选的。  在这个DNS数据报中使用了递归查询的方式  保留（Z）： 未使用，用0表示  问题计数（Question Count）： 问题区段中的问题记录数  回答计数（Answer Count）：回答区段中的回答记录数  域名服务计数（Name Server Count）：权威区段中的记录数  额外记录数（Additional  Records Count）：在额外信息区段中的记录数 |
| 问题讨论： |
| 1. ARP删除缓存时删除不成功   解决方法：通过看控制台提示，得知是权限不够，所以以管理员身份运行，在输入arp -d \*，删除掉主机内部arp全部缓存   1. IP分析中寻找最近的路由器（第一跳）不知如何寻找   解决方法：按Source排序后，先找到传输到主机的第一个，观察到TTL=254，因为TTL有8字节，所以最大值为255，所以可知每次从该路由器到达主机是只需要一跳即可到达，所以可知便是最近的路由器。   1. 在寻找对应报文段对应的ACK时未找到对应ACK   解决方法：本以为是未接收到ACK，后发现是GBN传送，即累积确认，找到其后面下一报文段的ACK即可确认收到ACK，其对应时间即为接收到ACK的时间 |
| 心得体会： |
| 结合实验过程和结果给出实验的体会和收获。  通过本次实验首先熟悉并掌握使用了wireshark这个用来抓包的的工具，也同时学习使用了pingplotter，并通过练习抓包过程进一步加深了对HTTP,TCP,IPV4,DNS,UDP等不同协议的了解，也了解在实际网络运行中不同协议间的相同合作，对TCP和IP分析印象深刻，也同时对其的协议的报文结构，传输过程中的变化加深了了解，收获很多。 |