

**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 | 姚舜宇 | | 院系 | 计算学部 | | |
| 班级 | 1903602 | | 学号 | 1190202107 | | |
| 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 | 2021.11.20 | | |
| 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： |
| 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 6. 利用wireshark分析DNS协议 7. 利用wireshark分析UDP协议 8. 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。  首先需要知道本机的IPv4地址。地址：172.20.78.35     1. wireshark的使用   双击WLAN2，wireshark就自动开始分组捕获，可以在应用显示过滤器一栏中输入协议进行筛选。可以将捕获记录保存到本地。     1. HTTP分析   （1）.HTTP GET/response交互  在应用显示过滤器中输入http进行筛选，然后开始捕获。打开浏览器，访问hitgs.hit.edu.cn，然后停止捕获。将结果保存在http1.pcapng中。  （2）.HTTP 条件GET/response交互  启动浏览器，清楚缓存，在应用显示过滤器中输入http进行筛选，然后开始捕获，访问hitgs.hit.edu.cn，然后刷新网页，停止分组捕获。将结果保存在http2.pcapng中。   1. TCP分析   首先访问http://gaia.cs.umass.edu/wireshark-labs/alice.txt，获得alice.txt文件。然后打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，选择好本地alice.txt文件的 位置。然后启动Wireshark开始分组捕获，在浏览器中点击“Upload alice.txt file”按钮上传文件，在文件上传完毕后停止Wireshark分组捕获。在筛选规则中选择“tcp”部分，进行分析即可，将所有分组保存在文件tcp.pcapng中。   1. IP分析   使用pingplotter进行实验，待发送IP分组的网站为hit.edu.cn，启动Wireshark开始分组捕获，首先发送一系列56字节的包；再发送一系列2000字节的包；再发送一系列3500字节的包，然后停止Wireshark捕获。将所有分组保存在ip.pcapng中。   1. 抓取ARP数据包   在命令行输入arp –a命令，查看主机上ARP缓存的内容。在命令行模式下输入：ping 192.168.1.82。然后启动Wireshark进行捕获。将所有分组保存在arp.pcapng中。   1. 抓取UDP数据包   先启动Wireshark分组捕获，然后用QQ给好友发送消息，消息发送结束后，停止分组捕获。将所有分组保存在udp.pcapng中。   1. 利用wireshark进行DNS协议分析   打开浏览器输入[www.baidu.com](http://www.baidu.com)，打开wireshark启动抓包，在控制台回车执行完毕后停止抓包。将所有分组保存在dns.pcapng中。 |
| 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. HTTP GET/response交互   打开http1.pcapng，输入http进行分组过滤，点击第一条HTTP报文，信息如下。    思考题：  (1).浏览器运行的协议为HTTP/1.1，访问的服务器运行的HTTP版本号是HTTP/1.1。  (2).浏览器向服务器指出的接收的语言版本对象为：Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n。  (3).本机IP地址为172.20.78.35，服务器的IP地址为219.217.226.25。  (4).服务器向浏览器返回的状态码为200。     1. HTTP 条件GET/response交互   打开http2.pcapng，输入http进行分组过滤，点击第一条HTTP报文，信息如下。    思考题：  (1).第一个HTTP GET请求没有IF-MODIFIED-SINCE头部  (2).服务器在第一个GET中返回了文件的内容如下。可以看出服务器返回的文件内容是用来构成主页HTML的其他元素。    (3).对于浏览器向服务器发出较晚的HTTP GET请求，报文中有一行IF-MODIFIED-SINCE。在该首部行后跟着的信息是缓存文件上次修改的时间。  (4).服务器对较晚的HTTP GET请求的响应中的HTTP状态代码是304，服务器不会明确返回文件的内容，因为会从浏览器中读取内容。   1. TCP分析   下载alice.txt之后，进入网站上传。    思考题：  (1).客户端主机的IP地址和TCP端口号分别为172.20.78.35和60891。    (2).服务器IP地址为128.119.245.12，它用来发送和接收TCP报文的端口号是80。  (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。在该报文段中将SYN置为1，表示该报文段用于tcp建立连接。      (4).服务器向客户端发送的SYNACK报文段序号为0。该报文段中Acknowledgement字段的值是1。Gaia.cs.umass.edu服务器通过SYN请求报文段的seq序号加1来决定此值。在该报文段中，是使用flag部分的ack以及SYN标记为1来标示该报文段是SYNACK报文段的。    (5).分析TCP三次握手过程  第一次握手，客户端向服务器发送SYN请求报文，第二次握手，服务器向客户端回复SYNACK报文，然后第三次握手就是客户端向服务器回复ack报文段，此时回复的ack报文段中，ack的内容为为1（为SYNACK报文段序号加1），说明是第三次握手。    (6).包含HTTP POST命令的TCP报文段的序号是1。    (7).向下查询到第六个报文段信息如下：    是在第一帧发送后3.593秒之后发送的报文段。该报文段对应的ACK报文接收如下：    (8).      长度分别为：749，13140，1460，8760，14600，2920字节。  (9).接收端公示的最小的可用缓存空间为64240字节。在整个过程中接收端并没有对发送端的传输进行限制    (10).得到序列号随时间的变化，可以看出整个过程中序列号随时间一直增长，为1，750，13890，15350，24110，38710。而若有重传的报文段会出现序列号变小的情况。说明没有发生重传。  (11).总共传输的字节数为149474-1=149473字节，所用时间为4.449935-3.03036（第一次握手）=1.419575秒。吞吐量throughput=149473字节/1.419575秒=1.053MB/s。     1. IP分析   使用pingplotter向hit.edu.cn发送一系列大小为56字节，2000字节和3500字节的IP分组，然后用Wireshark进行捕获结果如下。      思考题：  (1).我的主机IP地址为172.20.78.35。  (2).对主机第一个发送的ICMP报文进行查看，IP数据包头中，上层协议为ICMP（1）。  (3).IP头为20字节，该IP数据包的净载为36字节（IP数据包总大小为56字节，头部有20字节，所以净载为56-20=36字节）。  (4).没有分片。通过观察flag区域可以推断得出。可以看到没有其余的帧且帧的偏移为0，MF=0，则说明该IP数据包没有分片。    (5).通过比较几个分组可以发现，这些IP数据包的Identification、TTL和checknum字段总是发生改变。        (6).保持常量的字段有：版本号、上层协议、源IP地址和目的IP地址。因为要使该数据包成功发送到目的地址，这些字段必须保持该值。必须改变的字段有：Identification，TTL，checknum。Identification是IP数据包的序号，每个包的序号都不同。且根据traceroute的工作原理，每次主机发送的IP数据包的TTL都加一。校验和为头部数据求和得出，这两者的变化都会使校验和发生改变。  (7).Idenfification字段由两个字节组成，每次加1。  (8).找到最近的路由器返回给主机的ICMP Time-to-lice exceeded消息。查看该报文如下：    Identification字段为0x0000，TTL字段为255。  (9).Identification会改变，TTL不变。因为在同一跳，Identification用于区分不同的IP数据包，TTL字段相同。  (10).可以发现包大小改为2000字节后我的主机发送的第一个ICMP Echo Request消息被分成了两片，分别为1514字节和534字节。    (11).观察第一个报文段，此时DF=0，MF=1，说明了该数据包进行了分片，并且不是最后一个分片。并且该数据包的片偏移为0，说明该包是第一个数据包。该分片的长度为1500字节    (12).从下图中可以看到将包大小改为3500字节后，第一个ICMP Echo Request消息被分成了三片，分别为1514字节，1514字节和534字节。    (13).这三个IP分片的数据头部Total length，片偏移量，标志位，checksum字段发生了变化。如下图所示。         1. 抓取ARP数据包     思考题：  (1).ARP缓存中第一列为借口的IP地址，第二列为借口的MAC地址，第三列为地址的类型，包括静态和动态。  (2).清除主机ARP缓存的内容，抓取ping命令时的数据包，如下图：    数据包格式如下：    构成部分有：  硬件类型：2字节  协议类型：2字节  硬件地址长度：6字节  协议长度：4字节  操作类型：用来表示这个报文的类型，ARP请求为1，2字节  发送方MAC地址：6字节  发送方IP地址：4字节  目标MAC地址：6字节  目标IP地址：4字节。  (3).可以根据操作类型字段判断。若为1则为请求包，若为2则为应答包。  (4).因为查询MAC时主机不知道目的IP的MAC地址是多少，所以需要在局域网中广播查询。而ARP响应只需要发给提出查询的主机即可，所以ARP查询需要在广播帧中传送，而ARP响应要在一个有明确目的局域网地址的帧中传送。   1. 抓取UDP数据包   启动wireshark开始分组捕获，发送QQ消息，停止捕获。筛选中UDP数据包如下。    思考题：  (1).消息是基于UDP的。  (2).主机IP地址：172.20.78.35，目的主机的IP地址为111.30.159.59。  (3).主机发送QQ消息的端口号为4005，QQ服务器的端口号为8000。  (4).数据包格式如下。    字段有：  源端口号：2字节  目的端口号：2字节  报文长度：2字节  校验和：2字节  (5).由于UDP是不可靠数据传输，所以每次发送一个ICQ数据包后服务器都会返回一个ICQ数据包进行确认。和TCP相比，UDP在发送数据之前没有握手，这里能够推断出UDP是无连接的。   1. 利用wireshark进行DNS协议分析   访问[www.baidu.com](http://www.baidu.com)的抓包结果如下。    数据包格式如下： |
| 问题讨论： |
| 在实验结果中已经进行了论述。 |
| 心得体会： |
| 1. 学会了使用wireshark进行抓包的操作 2. 通过使用软件进行协议的分析，加深了对各种协议以及数据包格式的理解。 |