

**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 | 林燕燕 | | 院系 | 人工智能 | | |
| 班级 | 1903601 | | 学号 | 1190200501 | | |
| 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 | 2020.11.20 | | |
| 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： |
| 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： |
| 1. Wireshark 的使用   选择无线网卡进行分组捕获，并访问<http://www.hit.edu.cn>。在完整的页面加载完成后，结束分组捕获。在这一段时间Wireshark捕获了本机所有利用该无线网卡与其他网络实体进行交换的报文。   1. HTTP分析 2. HTTP GET/response交互   在Wireshark显示过滤部分输入“HTTP”即仅显示捕获的HTTP报文，开始捕获后访问 <http://news.hit.edu.cn>，在加载完全部页面后停止分组捕获。   1. HTTP 条件 GET/response交互   将浏览器内的所有缓存清空，启动Wireshark分组捕获，访问<http://news.hit.edu.cn>，在加载完全部页面后，重新刷新页面；在刷新页面后，停止Wireshark分组捕获。   1. TCP分析 2. 访问<http://gaia.cs.umass.edu/wireshark-labs/alice.txt>，获得alice.txt文件。再打开<https://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>，选择好本地alice.txt文件的位置，开始Wireshark分组捕获后，点击”Upload alice.txt file”按钮；在文件上传完毕后，停止Wireshark分组捕获。 3. 在筛选规则中选择“tcp”部分，进行分析。 4. IP分析   使用pingplotter进行实验，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。   1. 抓取ARP数据包 2. 利用arp查看本机的ARP缓存表 3. 开始Wireshark分组捕获，在命令行中输入：ping 172.20.45.95 4. ping通之后停止Wireshark捕获 5. 抓取UDP数据包   启动Wireshark分组捕获，利用QQ给好友发送消息，消息发送结束后，停止分组捕获。   1. 利用Wireshark进行DNS协议分析   首先清空dns缓存，在浏览器中访问[https://www.baidu.com](http://www.baidu.com)，进行Wireshark抓包。 |
| 实验结果： |
| 1. Wireshark 的使用   访问<http://www.hit.edu.cn>。在完整的页面加载完成后，结束分组捕获。    在显示筛选规则中输入“http”：    筛选后可看到第一条HTTP报文为计算机发向 www.hit.edu.cn 服务器的 HTTP GET 报文。   1. HTTP分析 2. HTTP GET/response交互   在Wireshark显示过滤部分输入“HTTP”即仅显示捕获的HTTP报文，开始捕获后访问<http://news.hit.edu.cn>，在加载完全部页面后停止分组捕获。     1. 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？   本地浏览器运行的协议是HTTP1.1，服务器运行的协议是HTTP1.1     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？   可接收的语言版本为zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2     1. 你的计算机的 IP 地址是多少？服务器 <http://news.hit.edu.cn>的 IP 地址是多少？   计算机IP地址为 172.20.78.109，服务器的IP地址为202.118.254.136     1. 从服务器向你的浏览器返回的状态代码是多少？   返回的状态码为200     1. HTTP 条件 GET/response交互   将浏览器内的所有缓存清空，启动Wireshark分组捕获，访问<http://news.hit.edu.cn>，在加载完全部页面后，重新刷新页面；在刷新页面后，停止Wireshark分组捕获。   1. 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IF-MODIFIED-SINCE头部     1. 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？   服务器明确返回了文件的内容，在服务器响应报文中多了Line-based text data字段。     1. 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IF-MODIFIED-SINCE字段，后面跟着的信息是上一次缓存文件的修改时间。     1. 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。   状态码为304，服务器没有明确返回文件的内容，消息长度只有313bytes，缓存的内容没有更新，直接使用缓存中的储存的信息。     1. TCP分析 2. 访问<http://gaia.cs.umass.edu/wireshark-labs/alice.txt>，获得alice.txt文件。再打开<https://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>，选择好本地alice.txt文件的位置，开始Wireshark分组捕获后，点击”Upload alice.txt file”按钮；在文件上传完毕后，停止Wireshark分组捕获。 3. 在筛选规则中选择“tcp”部分，进行分析。 4. 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？   客户端主机的 IP 地址是172.20.53.162，TCP 端口号是63190     1. 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？   服务器的 IP 地址是128.119.245.12，用来发送和接收 TCP 报文的端口号都是80     1. 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？   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标志位置为1来标示该报文段是 SYN 报文段的     1. 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？   服务器向客户端发送的 SYNACK 报文段序号是0，Acknowledgement 字段的值是1，服务器通过SYN请求报文段的seq序号加1确定acknowledgement字段，在该报文段中，是用flags部分的ack和SYN标志位置为1表示该报文段为SYNACK报文段。     1. 你能从捕获的数据包中分析出 tcp 三次握手过程吗？   以上两图反映了tcp连接的三次握手中的前两次，分别是客户机向服务器端发送SYN请求报文，以及服务器向客户机回复SYNACK报文；下图为客户机向服务器回复ack报文段：    可以根据回复的ack报文段中，ack端的内容为1（恰好为SYNACK报文段序号0加1所得），可知这是对SYN ACK报文段的回复，即第三次握手   1. 包含 HTTP POST 命令的 TCP 报文段的序号是多少？   包含HTTP POST命令的 TCP 报文段的序号是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多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？   该 TCP 连接上的第六个报文段的序号是6801；是第一帧发送后0.331851s发送的；该报文段所对应的 ACK 是第一帧发送后0.664942s接收的       1. 前六个 TCP 报文段的长度各是多少？   前六个 TCP 报文段的长度都是1360     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？限制发送端的传输以后，接收端的缓存是否仍然不够用？   在整个的跟踪过程中，接收端公示最小可用的缓存空间为131840，并且始终为131840。所以始终没有出现限制发送端发送的情况。     1. 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？   没有重传的片段，依据为发送端的报文段序号始终在增加，没有出现重复发送某一个序号的报文段的情况，故没有重传的。报文段序号变化如下：     1. TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程   第一个TCP段及最后一个TCP段如下：      吞吐量计算如下：   1. IP分析   使用pingplotter进行实验，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。   1. 你主机的IP地址是什么？   本机地址为172.20.2.22     1. 在IP数据包头中，上层协议（upper layer）字段的值是什么？   上层协议字段的值是ICMP(1)     1. 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数据包大小为56，则净载为36字节     1. 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   该IP数据包未分片，观察flag段，没有其余帧且帧偏移为0     1. 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？   IP数据报中TTL、checksum和sequence number总是发生改变。     1. 哪些字段必须保持常量？哪些字段必须改变？为什么？   必须保持常量的是版本号、首部长度、区分服务（Differentiated Services Field）以及协议（始终为ICMP）；  必须改变的是TTL、checksum和sequence number，TTL为生存时间，每次转发必然改变，由于TTL的改变，checksum也会改变，sequence number是变化的区分不同的ICMP报文。   1. 描述你看到的IP数据包Identification字段值的形式。   Identification字段值，一字节一字节逐渐递增：     1. Identification字段和TTL字段的值是什么？   Identification字段的值是0xcd00，TTL字段的值是252     1. 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？   Identification段变化，为了区分不同的ICMP time-to-live exceeded消息，  但TTL保持不变，均为一次转发。   1. 当包的大小变为2000字节后，找到第一个ICMP echo request消息，该消息是否被分解成不止一个IP数据报？   当包的大小变为2000字节后，第一个ICMP echo request消息形式如下，可以看到确实被分解成了不止一个数据包。     1. 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   flag域中，More fragments位被置为1且长度非1500，表示发生分片；，More fragments位被置为1且offset为0，表示发生分片且该分片不为最后一片；且长度为1500字节     1. 当包的大小变为3500字节后，找到第一个ICMP echo request消息，原始数据包被分成了多少片？   原始数据包被分成3片     1. 这些分片中IP数据报头部哪些字段发生了变化？   IP数据报头部flag字段和checksum字段发生了变化。         1. 抓取ARP数据包 2. 利用arp查看本机的ARP缓存表 3. 开始Wireshark分组捕获，在命令行中输入：ping 172.20.45.95 4. ping通之后停止Wireshark捕获 5. 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?   ARP 缓存中每一列均由其表头决定，如地址等；每一行为某地址对应的硬件地址：     1. 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：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？   ARP数据包格式如下：       1. 如何判断一个ARP数据是请求包还是应答包？   只需要判断opcode部分，当其值为0x0001时为请求，0x0002时为应答       1. 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？   因为不知道具体的ip地址对应的mac地址，需要通过ARP查询得到ip地址对应的mac地址；而由于响应报文能从ARP查询的ip数据包中，拆分出发送查询的主机的ip地址和mac地址，所以不需要再利用广播帧发送信息   1. 抓取UDP数据包   启动Wireshark分组捕获，利用QQ给好友发送消息，消息发送结束后，停止分组捕获。   1. 消息是基于UDP的还是TCP的？   消息是基于UDP的     1. 你的主机ip地址是什么？目的主机ip地址是什么？   主机IP地址为172.20.160.92，目的主机ip地址为111.30.159.62     1. 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？   本人的主机发送QQ消息的端口号是4008；QQ服务器的端口号是8000     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？   UDP数据包的格式如下，头部包含源端口号、目的端口号、长度和checksum。各占1个字节     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？   因为UDP是不可靠的数据传输，需要上层协议实验可靠数据传输，因此每次发送ICQ报文后又回复一个ICQ数据包。  UDP是无连接的，可以看到发送数据之前没有连接的建立过程，与TCP不同，因此为无连接数据传输。   1. 利用Wireshark进行DNS协议分析   首先清空dns缓存，在浏览器中访问<https://www.baidu.com>，进行Wireshark抓包。    查询的目的地址均为相同的202.118.224.100，可以推测这是哈工大的dns服务器，经过ip地址查询确实这是一个来自哈尔滨市南岗区的教务网ip地址。 |
| 问题讨论： |
| 见上面实验结果 |
| 心得体会： |
| 在本次的实验中，通过Wireshark分析各种网络协议的执行，可以加深对于各种协议交互过程的理解。并且对于协议中各个字段的作用有了更深的了解。  Wireshark是个十分强大的工具，不仅仅在本门实验中会利用到他的一些知识，在以后的学习工作生活中还有很大的作用。 |