

**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 | 徐柯炎 | | 院系 | 计算机科学与技术学院 | | |
| 班级 | 2103602 | | 学号 | 2021110683 | | |
| 任课教师 | 刘亚维 | | 指导教师 | 刘亚维 | | |
| 实验地点 | 格物207 | | 实验时间 | 2023.11.4 | | |
| 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，了解网终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   启动Web浏览器，启动Wireshark    开始分组捕获，出现分组捕获窗口：    从上至下分别为命令菜单、俘获分组列表、分组头部明细、分组内容窗口、显示筛选规则。  输入URL（http://www.hit.edu.cn），捕获HTTP GET报文：     1. http分析 2. HTTP GET/response交互   启动Web browser，然后启动Wireshark分组嗅探器。在窗口的显示过滤说明出输入http，分组列表子窗口中将只显示所俘获到的HTTP报文。  开始Wireshark分组俘获。  在打开的Web browser窗口中输入一下地址：http://hitgs.hit.edu.cn/zhxw/list.htm  停止分组俘获，得到如下结果：    根据俘获窗口内容，思考以下问题：   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？     从上图的get报文中看出，我的浏览器运行的是HTTP1.1；  从上图的应答报文看出，我所访问的服务器运行的HTTP协议的版本号是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？     从上图看出，zh-CN表示我的浏览器向服务器指出要接收中文版本的对象，除此之外还有zh、zn、en-GB，en-US，但是zh-CN和zh的权重最高。   1. 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IP地址为上图的Source Address：2001:250:fe01:130:6ca4:1552:39ac:85bb  服务器的IP地址为上图的Destination Address：2001:da8:b800:253::dbd9:e219   1. 从服务器向你的浏览器返回的状态代码是多少？     如上图所示，返回的状态代码为200 OK。   1. HTTP 条件 GET/response交互   启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。  启动Wireshark 分组俘获器。开始Wireshark 分组俘获。  在浏览器的地址栏中输入以下URL: http://hitgs.hit.edu.cn/zhxw/list.htm,在你的浏览器中重新输入相同的URL 或单击浏览器中的“刷新”按钮。  停止Wireshark 分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的HTTP 报文。  清除缓存如下图所示：    根据俘获窗口内容，思考以下问题：   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？     如图所示，并没有IF-MODIFIED-SINCE   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？     如上图所示，服务器响应报文的状态码大部分都是200 OK，说明服务器正确返回了文件的内容，同时返回文件的内容就在报文之中，左下角是报文相关的信息。  但也有小部分报文并没有正确返回文件内容，出现了404 Not Found。如下图所示。    通过报文可以知道是http://hitgs.hit.edu.cn/zhxw/list.htm相关的文件，报文中还返回了哪些内容没有正确收到。   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？     如上图所示，有IF-MODIFIED-SINCE。在该首部行后面跟着的信息是一个时间信息，表示向服务器询问该文件是否在这个时间之后有所更改。   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。     如上图，HTTP状态代码为304 Not Modified，表示信息没有更新。服务器不会明确返回文件，因为根据前面 HTTP 的 GET 请求中 IF-MODIFIED-SINCE 字段内的时间，服务器返回结果为304 Not Modified，这说明客户端会使用本地没有过期的缓存文件。   1. TCP分析 2. 俘获大量的由本地主机到远程服务器的TCP分组 3. 启动浏览器，打开http://gaia.cs.umass.edu/wireshark-labs/alice.txt网页，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到你的主机上。 4. 打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html网页。 5. 启动Wireshark，开始分组俘获。 6. 在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。 7. 停止俘获。   整个操作流程如下图所示。         1. 浏览追踪信息   在显示筛选规则中输⼊“tcp”,可以看到在本地主机和服务器之间传输的⼀系列 tcp 和 http 报⽂，你应该能看到包含 SYN 报⽂的三次握⼿。也可以看到有主机向服务器发送的⼀个 HTTP POST 报⽂和⼀系列的“http continuation”报⽂。  根据操作思考以下问题：   1. 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？     如上图所示，客户端主机IP地址为Source Address：172.20.156.105  TCP端口号为Src Port：62816   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？   如上图所示，服务器主机IP地址为Destination Address：128.119.245.12  TCP端口号为Dst Port：80   1. TCP 基础   根据操作思考以下问题：   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？     如图，序号（sequence number）为0。    如图，客户服务器之间用于初始化TCP连接的TCP SYN报文段序号是0，报文段中利用一个SYN标志位，该标志位置1时，标识该报文段是SYN报文段。   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？     如图所示，服务器向客户端发送的 SYNACK 报⽂段序号为0。  如上图所示，该报⽂段中，Acknowledgement 字段的值是1。  Gaia.cs.umass.edu 服务器通过将客户端发送过来的报文段的 seq+1 得到的ACK的值。    如上图所示，在该报⽂段中，是通过将 ACK 标志位和 SYN 标志位同时置 1 来标识该报文段是 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？         如图在红色方框中的报文为三次握手的过程。  第一次握手：客户端会向服务器发送一个TCP SYN报文段，其中SYN标志位置1，初始序列号Seq为0，请求与服务器建立TCP连接。  第二次握手：服务器收到SYN报文段，同意建立连接，同时向客户端发送一个SYNACK报文段，其中SYN和ACK标志位都置1，初始序列号Seq为0，Ack为1，以此响应客户端请求。  第三次握手：客户端收到服务器的SYNACK报文段，回复ACK报文段，其中SYN标志位置0，ACK标志为1，Seq=1，Ack=1，可以携带数据。   1. 包含 HTTP POST 命令的 TCP 报⽂段的序号是多少？     如上图所示，序号为152220。   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？       如上图所示，序号为6188。    发送时间如上图所示。    接收时间如上图所示。   1. 前六个 TCP 报⽂段的⻓度各是多少？     如图所示，第一个报文为747个字节，后面五个报文的长度为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？     如图所示，接收端公示的最小的可用缓存空间是131840字节。      从上图可以看出，接收端的缓存会不断增大，因此接收端的缓存不会不够用。   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？   有重传的报文段。因为有重传的报文段的话就会有retransmission提示，如下图所示。     1. TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。         如上图所示，发送的报文的总长度为153066个字节；  发送第一个报文的时间为4.255s  发送最后一个报文的时间为5.203s  发送时间为：5.203-4.225≈1s  所以吞吐率为：153006\*8/1 ≈ 1Mbps   1. IP分析 2. 通过执行 traceroute 执行捕获数据包      1. 对捕获的数据包进行分析   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出的ICMP Echo Request消息，在packet details窗⼝展开数据包的Internet Protocol部分。  思考下列问题：   1. 你主机的IP地址是什么？     如图所示，主机IP地址为172.20.156.105   1. 在IP数据包头中，上层协议（upper layer）字段的值是什么？     如图所示，上层协议字段的值为1，也就是ICMP协议。   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？     如图所示，IP头的字节数为20，  左侧Total Length 为56，所以IP数据包的净字节数为56-20=36   1. 该IP数据包分⽚了吗？解释你是如何确定该IP数据包是否进⾏了分⽚     如图所示，该IP数据包没有分片，因为标志位为0，表示允许分片但没分片。   1. 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）   思考下列问题：   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？     如图，IP数据报中标识位和TTL位一直在变。   1. 哪些字段必须保持常量？哪些字段必须改变？为什么？   版本号、服务类型和上层协议必须保持常量，而标识和TTL是必须改变的。  因为版本号是不能变的，不然数据的传输会出问题；服务类型和上层协议字段也是如此。  但由于标识位是唯一的，所以必须改变，TTL是在不断变化的，因为是ICMP的ping探测。   1. 描述你看到的IP数据包Identification字段值的形式。     如图，IP数据包Identification字段值的形式为16进制的两字节的数。   1. 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。     由图可知，第一跳的IP为10.0.3.0  所以第一跳返回的信息为下图：    思考下列问题：   1. Identification字段和TTL字段的值是什么？     如图所示，Identification字段的值为0x57b1，TTL字段的值为1   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变化，因为是唯一标识一个数据报的内容。而TTL不变。因为一开始设置的TTL不变，到第一跳的TTL也不会改变。   1. 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：   1. 该消息是否被分解成不⽌⼀个IP数据报？     如图所示，分解成了不止一个IP数据报。   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？该分⽚的⻓度是多少     如图，标识、标志和片偏移这几个位表明数据包进行了分片，IP头部的片偏移字段为0表明了数据报是第⼀个⽽不是最后⼀个分⽚，该分片的长度为1500-20=1480字节。   1. 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。   思考下列问题：   1. 原始数据包被分成了多少⽚？     如图，原始数据包被分成了三片。   1. 这些分⽚中IP数据报头部哪些字段发⽣了变化？     如上图，总长度、标志位、DF、MF、片偏移发生了变化。   1. Ethernet数据帧分析   首先我们访问计算学部官网http://cs.hit.edu.cn 进行抓包，具体如下图所示：    Ethernet数据帧结构如下图所示：  IMG_256、  接下来，我们在Wireshark中寻找对应的以太网帧的内容；    从图中可以看到，我主机的mac地址是48:51:c5:28:20:17  目的主机的mac地址是44:ec:ce:d2:ff:c2  网络层使用的协议是IPv4。   1. 抓取ARP数据包 2. 利用MS-DOS命令查看主机APR缓存的内容      1. 在命令行模式下输入：ping 192.168.1.82（或其他IP地址）      1. 启动Wireshark，开始分组俘获 2. 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?   每一列分别表示 IP 地址以及所对应的物理地址和类型（动态配置或静态配置）。   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： 2. 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？     如上图所示，ARP数据报的格式由9部分构成，分别为   * 硬件类型：2字节，值为1表示以太网地址； * 协议类型：2字节，0x0800表示IP地址； * 硬件地址长度：1字节， * 协议地址长度：1字节，数值为4； * 操作代码：2字节，1表示请求报文，2表示应答报文； * 源MAC地址：6字节； * 源IP地址：4节字； * 目的MAC地址：6字节； * 目的IP地址：4节字。  1. 如何判断⼀个ARP数据是请求包还是应答包？   如果操作代码（OP）为1则为请求报文，为2则为应答报文。   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？   因为进行ARP时不知道目标主机IP地址对应的MAC地址，所以要进行广播查询；  而进行ARP响应时是知道目的主机的MAC地址的（通过查询主机发出的查询报文获得），所以ARP响应要在一个有着明确目的局域网地址的帧中传送。   1. 抓取UDP数据包 2. 启动Wireshark，开始分组捕获； 3. 发送QQ消息给你的好友； 4. 停止Wireshark组捕获 5. 在显示筛选规则中输入“udp”并展开数据包的细节，如图所示。     分析QQ通讯中捕获到的UDP数据包。根据操作思考以下问题：   1. 消息是基于UDP的还是TCP的？   UDP   1. 你的主机ip地址是什么？目的主机ip地址是什么？     如图所示，我的主机ip地址为172.20.156.105  目标主机ip地址为39.156.132.120   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？     如图所示，源端口号为4015，目的端口号为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？     如图，数据报首部包含源端口号，占两个字节；目的端口号，占两个字节；数据报长度，占两个字节；校验和，占两个字节。数据报还包含数据部分，占155个字节。  首部8个字节。源端口号2字节；目的端口号2字节；长度2字节；校验和2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？   因为服务器要把返回的结果返回给客户机。  客户端只发送给服务器要发送的消息，而服务器也只是应答一下接收到了消息，可以看出是尽力而为传输数据的服务，也就是不可靠的数据传输；  前面的TCP有三次握手建立连接的过程，而这里UDP没有建立连接，所以UDP是无连接的。   1. 利用WireShark进行DNS分析   打开浏览器键入:www.baidu.com，并打开Wireshark进行抓包。    查询的目的地址均为10.128.1.114；  通过所学知识可知，此IP地址为DNS服务器。  DNS查询报文：    DNS应答报文： |
| 问题讨论： |
| 1. 默认使用IPV6的情况：   由于电脑系统的版本问题，windows10默认使用IPv6协议，为了在实验中采用IPv4协议，我进行了如下调整：   1. 打开网络和共享中心界面 2. 点击左侧“更改适配器选项” 3. 在更改适配器设置中我们可以看到所有的连接，连接你连接网络的连接，如果 4. 使用的是网线就是“以太网”，无线则选择“无线连接”，右键点击，选择属性。 5. 然后在服务列表中我们就可以看到“Internet 协议 6（TCP/IPV6）”了，取消勾选复选框，然后确定。   这样就解决了问题。   1. 在TCP分析中没有建立连接的过程：   刚开始做的时候由于开着代理服务器，会出现报文中没有建立连接的过程。  解决方法：不使用代理服务器就可以了。 |
| 心得体会： |
| 1. 对HTTP协议、TCP协议、UDP协议、IP协议、DNS协议等等的报文格式有了更深入的了解，明白了每一个标志位的含义与作用，深入地了解了协议交互的过程以及工作方式； 2. 学会了wireshark和pingplotter的简单使用，熟悉了网络协议实体间进行交互及报文交换的大致流程与情形。 |