

**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 |
| 班级 |
| 任课教师 |
| 实验地点 |
| 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  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 |
| **实验过程与实验结果：** |
| 以文字描述、实验结果截图等形式阐述实验过程与结果，必要时可附相应的代码截图或以附件形式提交。 一. Wireshark的使用 （1）启动主机上的 web 浏览器和Wireshark。    （2）在运行分组俘获的同时，在浏览器地址栏中输入某网页的URL：<http://www.hit.edu.cn>。  当完整的页面下载完成后，单击 Wireshark 菜单栏中的 stop 按钮，停止分组俘获。    （3）在显示筛选规则中输入“http”，单击“回车”，分组列表窗口将只显示HTTP协议报文。   二. 分析HTTP协议2.1 HTTP GET/response 交互 开始 Wireshark分组俘获，在打开的Webbrowser窗口中输入一下地址：<http://jwes.hit.edu.cn/>  ，停止分组俘获。     （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？  我的浏览器运行的是HTTP 1.1。我所访问的服务器所运行 HTTP 协议的版本号是HTTP 1.1。   （2）你的浏览器向服务器指出它能接收何种语言版本的对象？  简体中文   （3）你的计算机的 IP 地址是多少？服务器 http://jwes.hit.edu.cn/的IP地址是多少？  计算机的 IP地址是172.20.23.25，服务器的IP地址是219.217.226.139。   （4）从服务器向你的浏览器返回的状态代码是多少？  状态代码是200 2.2 HTTP 条件 GET/response 交互 1. 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”）。   2.启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。   3.在浏览器的地址栏中输入以下 URL: <http://today.hit.edu.cn/>，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。   4.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。    （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   （2）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？    明确返回了文件的内容，因为返回的状态码是200   （3）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，在该首部行后面跟着的信息是缓存最后更新的时间Thu, 07 Nov 2019 09:12:10 GMT   （4）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。    状态码是304，不会明确返回了文件内容，因为服务器判断Not Modified，表示客户端可以使用未过期的缓存内容。 三、 TCP 分析  1. 俘获大量的由本地主机到远程服务器的 TCP 分组      1. 浏览追踪信息 2. 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：172.20.23.25  TCP 端口号：54300   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？   Gaia.cs.umass.edu 服务器的 IP 地址：128.119.245.12，端口号是：80   1. TCP 基础 2. 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？     初始化TCP连接的TCP SYN报文段的序号是0；通过Flags标志位来标示该报文段是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？     服务器端向客户端发送的报文段序号为 0；Acknowledgement字段的值是1，服务器根据上一次客户端发给服务器的序号seq+1 得到Acknowledgement字段的值； 通过Flags标志位中的SYN位和ACK位来确定该报文段是一个SYN ACK报文段的   1. 你能从捕获的数据包中分析出 tcp 三次握手过程吗？     客户端先向服务器发送 seq = 0 的建立连接的请求；然后服务器向客户端返回 seq = 0, ack = 1 的响应；最后客户端向服务器返回 seq = 1, ack = 1的确认报文。   1. 包含 HTTP POST 命令的 TCP 报文段的序号是多少？     序列号是152530   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？         由上图可得，第六个报文段的序号是：7794  第六个报文段的发送时间是在HTTP POST发送之前，所对应的 ACK 是接收的第6个ACK   1. 前六个 TCP 报文段的长度各是多少？     前六个 TCP 报文段的长度依次是693、1460、1460、1460、1460和1460 bytes   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？     接收端公示的最小的可用缓存空间是131328，该窗口大小一直增加，说明限制发送端的传输以后接收端的缓存够用。   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？     没有重传，因为客户端发送的序列号没有重复。   1. TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。     由图可知数据总长度为153012 byte    由上图得时间间隔约是 1.218521 s  吞吐量：153012/1.218521 = 125571.90233078 bps 四、IP 分析 A. 通过执行 traceroute 执行捕获数据包  实验步骤：  1. 启动 Wireshark 并开始数据包捕获  2．启动 pingplotter 并“Address to Trace Window”域中输入目的地址。在“# of times to Trace”域中输入“3”，这样就不过采集过多的数据。Edit->Options->Packet，将 Packet Size(in bytes,default=56)域设为 56，这样将发送一系列大小为 56 字节的包。 然后按下“Trace”按钮。得到的pingplotter 窗口如图所示。    3. Edit->Options->Packet，然后将 Packet Size(in bytes,default=56)域改为 2000，这样将发送一系列大小为 2000 字节的包。然后按下“Resume”按钮。  4. 最后，将 Packet Size(in bytes,default=56)域改为 3500，发送一系列大小为 3500 字节的包。然后按下“Resume”按钮。  5．停止 Wireshark 的分组捕获。  B. 对捕获的数据包进行分析     1. 你主机的IP地址是什么？     172.20.23.25   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（upper layer）字段的值是01   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     IP 头有 20 字节  IP 包的净载为 Total Length-Header Length=56B-20B=46B   1. 该IP数据包的净载大小？   46B   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     没有分片, 因为分片的偏移量为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？     TTL、ID鉴别码、头部校验和   1. 哪些字段必须保持常量？哪些字段必须改变？为什么？   保持常量：IP版本等  必须改变：TTL、ID鉴别码、头部校验和   1. 描述你看到的IP数据包Identification字段值的形式。   用16进制表示的4位字段（如0x1a08）   1. Identification字段和TTL字段的值是什么？     Identification字段：0  TTL字段的值：253   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？   不变，因为是第一跳路由器发回的报文，TTL不变；IP是无连接服务，标识不是序列号，相同的标识是为了分段后重组，给同一个主机发送的ICMP报文，TTL不变，则Identification字段不变。  C.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？     该消息被分解成两个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？该分片的长度是多少     IP头部的信息Don’t fragments、More fragments和Fragments offset表明数据包被进行了分片。若IP头部的More fragment= 1表明数据包是第一个而不是最后一个分片，否则表明数据包是最后一个分片。第一个分片长度是1480B，第二个分片长度是500B。  D. 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。   1. 原始数据包被分成了多少片？     分为3片   1. 这些分片中IP数据报头部哪些字段发生了变化？   前两片More fragments均为1，最后一片为0。且第二片的分片offest为1480，最后一片为2960。 五、Ethernet数据帧  1. Ethernet\_II 帧     Ethernet\_II 的帧中各字段说明如下：  DMAC（Destination MAC）是目的MAC地址。DMAC字段长度为6个字节，标识帧的接收者。  SMAC（Source MAC）是源MAC地址。SMAC字段长度为6个字节，标识帧的发送者。  类型字段（Type）用于标识数据字段中包含的高层协议，该字段长度为2个字节。类型字段取值为 0x0800的帧代表IP协议帧；类型字段取值为0806的帧代表ARP协议帧。  数据字段(Data)是网络层数据，最小长度必须为46字节以保证帧长至少为64字节，数据字段的最大长度为1500字节。  循环冗余校验字段（FCS）提供了一种错误检测机制。该字段长度为4个字节。   1. IEEE802.3帧     格式类似于Ethernet\_II帧，只是Ethernet\_II帧的Type域被802.3帧的Length域取代，并且占用了Data字段的8个字节作为LLC和SNAP字段。  Length字段定义了Data字段包含的字节数。  逻辑链路控制LLC（Logical Link Control）由目的服务访问点DSAP（Destination Service Access Point）、源服务访问点SSAP（Source Service Access Point）和Control字段组成。 逻辑链路控制LLC（Logical Link Control）由目的服务访问点DSAP（Destination Service Access Point）、源服务访问点SSAP（Source Service Access Point）和Control字段组成。  SNAP（Sub-network Access Protocol）由机构代码（Org Code）和类型（Type）字段组成。Org Code三个字节都为0。  Type字段的含义与Ethernet\_II帧中的Type字段相同。 六、抓取 ARP 数据包 1.利用 MS-DOS 命令： arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。  2.在命令行模式下输入： ping 192.168.1.82（或其他 IP 地址）  3.启动 Wireshark，开始分组俘获。抓取的数据包大致如下图所示    4. 思考下面问题：   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?     从左到右，每一列依次是：每一个IP对应的Internet地址、物理地址和类型（动态地址）   1. 使用arp -d命令清除主机上ARP 缓存的内容,抓取 ping 命令时的数据包。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？   数据报格式：    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？   检测OP字段，当OP为0x0001时为请求包，OP为0x0002时为应答包。  请求包：    应答包：     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ARP表中没有目的IP地址，不知道目的IP地址对应的MAC地址，所以ARP查询要在广播帧中传送。ARP响应时已经知道目的IP地址对应的MAC地址，并且局域网中的其他主机不需要此次查询的结果，所以在一个有着明确目的局域网地址的帧中传送。 六、抓取 UDP 数据包 （1）启动 Wireshark，开始分组捕获；  （2）发送 QQ 消息给你的好友；  （3）停止 Wireshark 组捕获；  （4）在显示筛选规则中输入“udp”并展开数据包的细节，如图所示     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？     主机ip地址:172.20.23.25  目的主机ip地址:223.166.151.93   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？     发送QQ消息的端口号:54733  QQ服务器的端口号: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数据报格式包括首部和数据，其中数据存放具体内容。首部只有4个字段，包括源端口号（2个字节）、目的端口号（2个字节）、数据报长度（2个字节）、校验和（2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？   原因：UDP收到请求后将响应报文发送给客户端。  原因：UDP提供不可靠数据传输，尽力而为地将报文段发送给客户端，而无需保证数据传输成功  可以看出UDP是无连接的。UDP没有接收和发送缓存、序列号与确认号等参数，无需执行发送方与接收方之间的握手，不维护连接状态， 七、利用 WireShark 进行 DNS 协议分析 （1）打开浏览器键入:www.baidu.com  （2）打开 Wireshark,启动抓包.  （3）在控制台回车执行完毕后停止抓包.Wireshark 捕获的 DNS 报文如图所示。 |
| 问题讨论： |
| 1. 实验指导书中给出的网址，访问后使用wireshark分析后发现ipv6地址，造成难以按照实验步骤进行分析  解决方案：更改访问网站为IPv4网站（http://jwes.hit.edu.cn/或http://today.hit.edu.cn/等）  2. 进行HTTP分析时 HTTP POST找不到，没有POST记录。  原因：因为下载文档访问国外网站使用了代理服务器，使用wireshark分析时忘记退出代理服务器。  解决方案：退出代理服务器后重新执行程序。  3. 实验过程中发现QQ是使用udp协议，为什么不使用TCP协议？  因为：QQ是实时聊天应用，通常要求最小发送速率，不希望过分地延迟报文段的传送，可以容忍一定的数据丢失。UDP协议不需要建立连接和握手过程，文件传输代价较小，但不保证文件数据不会丢失，符合QQ的要求。 |
| 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，我学会了wireshark和PingPlotter 5软件的使用。使用wireshark对HTTP，TCP,UDP,IP，DNS和ARP等协议，结合课本上各协议的数据报结构图，我更加具体地了解了各协议数据报的封装结构。通过TCP与UDP的对比，我了解了TCP（有连接）和UDP（无连接）在传输过程的区别。在IP分析过程中，我了解了IP数据报以及分片等。在ARP分析过程中，我更加直观地看到ARP表的结构。实验过程有些繁琐，但我感觉受益良多。 |