

**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 | 李世轩 | | 院系 | 软件工程 | | |
| 班级 | 2037102 | | 学号 | 120L022109 | | |
| 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 | 2022年10月28日 | | |
| 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： |
| 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： |
| 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。  （一）HTTP 分析  1）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处输入“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/news （因为该网页已不存在，这里使用http://today.hit.edu.cn/）。    停止分组俘获。        （二）TCP 分析  注：访问以下网址需要设置代理服务器。如无法访问可与实验 TA联系，下载 tcp-Wireshark-trace 文件，利用该文件进行 TCP 协议分析。  A. 俘获大量的由本地主机到远程服务器的 TCP 分组  （1） 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。  （2） 打开http://gaia.cs.umass.edu/Wireshark-labs/TCP-Wireshark-file1.html，如图6-6所示，窗口如下图所示。在Browse按钮旁的文本框中输入保存在你的主机上的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按 “Upload alice.txt file”按钮。  （3） 启动Wireshark，开始分组俘获。  （4） 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。  （5） 停止俘获。  B. 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。    （四）IP 分析  通过分析执行 traceroute 程序发送和接收到的 IP 数据包，我们将研究 IP 数据包的各个字段，并详细研究 IP 分片。  A. 通过执行 traceroute 执行捕获数据包为了产生一系列 IP 数据报，我们利用 traceroute 程序发送具有不同大小的数据包给目的主机 X。回顾之前 ICMP 实验中使用的 traceroute 程序，源主机发送的第一个数据包的 TTL 设位 1，第二个为 2，第三个为 3，等等。每当路由器收到一个包，都会将其 TTL 值减 1。这样，当第n个数据包到达了第n个路由器时，第 n 个路由器发现该数据包的 TTL 已经过期了。根据 IP 协议的规则，路由器将该数据包丢弃并将一个 ICMP 警告消息送回源主机。  在 Windows 自带的 tracert 命令不允许用户改变由 tracert 命令发送的ICMP echo 请求消息（ping 消息）的大小。一个更优秀的 traceroute 程序是 pingplotter，下载并安装 pingplotter。ICMP echo 请求消息的大小可以通过下面方法在 pingplotter 中进行设置。Edit->Options->Packet，然后填写 Packet Size(in bytes，default=56)域。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。  （1） 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。  （2） 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。  （3） 停止 Wireshark 的分组捕获。  B. 对捕获的数据包进行分析  （1）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发出的ICMP Echo Request消息，在packet details窗口展开数据包的Internet Protocol部分，    （2）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）  （3）找到由最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded消息。    （4）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。    C. 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。    （五）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。  从 Wireshark 的第一栏中，我们看到这是个 ARP 解析的广播包，如上图。由于这个版本的 Wireshark 使用的是 Ethernet II 来解码的，我们先看看 Ethernet II 的封装格式。    从 Ethernet II 知道了是 ARP 解析以后，我们来看看 Wireshark 是如何判断是 ARP 请求呢还是应答的。  以太网的 ARP 请求和应答的分组格式，如图 6-11 所示。    从上图中我们了解到判断一个 ARP 分组是 ARP 请求还是应答的字段是“OP”，当其值为 0×0001 时是请求，为 0×0002 时是应答。      （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 6-14所示。    （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 |
| 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。  实验结果已详细体现在实验过程中，这里不再赘述。 |
| 问题讨论： |
| （一）HTTP 分析  1）HTTP GET/response 交互    根据俘获窗口内容，思考以下问题：   * 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HTTP请求报文中可知，浏览器运行的是HTTP1.1，    从HTTP应答报文中可知，服务器运行的是HTTP1.1，   * 你的浏览器向服务器指出它能接收何种语言版本的对象？     浏览器向服务器指出它能接收中文版本的对象   * 你的计算机的 IP 地址是多少？服务器 http://today.hit.edu.cn/的 IP 地址是多少？     这里使用IPv6地址  计算机的 IP 地址是2406:280:1005:e19:88dc:38d8:9134:51d0  服务器 http://today.hit.edu.cn/的 IP 地址是2001:da8:b800:253::aa0:fb2e   * 从服务器向你的浏览器返回的状态代码是多少？     从服务器向浏览器返回的状态代码是200  2）HTTP 条件 GET/response  根据俘获窗口内容，思考以下问题：   * 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？     在该请求报文中，没有IF-MODIFIED-SINCE   * 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？     服务器已经明确返回了文件的内容，  从Line-based text data: text/html(10782 lines)可知，且在报文中可以明确找到对应html文件的内容   * 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？     在该请求报文中没有一行是：IF-MODIFIED-SINCE。   * 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。     服务器已经明确返回了文件的内容，  从Line-based text data: text/html(10782 lines)可知，且在报文中可以明确找到对应html文件的内容  （二）TCP 分析  根据操作思考以下问题：   * 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 地址和TCP 端口号是172.17.115.166:50052   * 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？   ip地址为128.119.245.12，端口为80  C. TCP 基础  根据操作思考以下问题：   * 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？       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0，在该报文段中，是用0x002来标示该报文段是 SYN 报文段的   * 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,该报文段中，Acknowledgement 字段的值是1.Gaia.cs.umass.edu 服务器是根据客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号来确定这个序号的。在该报文段中，是用0x012来标示该报文段是SYNACK 报文段的。   * 你能从捕获的数据包中分析出 tcp 三次握手过程吗？      * 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。   * 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6508。Time为5.978612发送。该报文段所对应的 ACK 是6.253080接受的   * 前六个 TCP 报文段的长度各是多少？      * 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240    限制发送端的传输以后，接收端的缓存不断增大，其缓存够用了。   * 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？   在跟踪文件中没有重传的报文段，进行判断的依据是通过观察客户端的分组序号，可以发现分组序号是一直在增长，没有出现过重复的序号的，因此可以判断没有重传的报文段。   * TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。       TCP 连接的 throughput 是138418.87Bps  请写出你的计算过程如下：  共计用时7.083360-5.978489=1.104871  152935B/1.104871=138418.87Bps  （四）IP 分析  思考下列问题：     * 你主机的IP地址是什么？   主机的IP地址是172.20.207.206   * 在IP数据包头中，上层协议（upper layer）字段的值是什么？   ICMP（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？   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    IP头有20个字节，该IP数据包的净载为36个字节（total length - header length）  该数据包没有分片，片偏移为0且more flag为0  思考下列问题：   * 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？       本主机发出的一系列ICMP消息中IP数据报中以下字段总在发生改变：标识ID，TTL，首部校验和，数据域。   * 哪些字段必须保持常量？哪些字段必须改变？为什么？   除了上述四个数据段以外的数据必须保持常值。上述四个字段总要发生改变的原因：标识ID对于每个数据包来说唯一，因此每个数据包的这个字段都不一样；由于是ICMP的ping探测，因此TTL在不断变大；由于上述两个字段不断变化，因此首部校验和也需要变化；由于数据域中封装有ICMP的报文，而ICMP的头部信息不断变化，因此IP数据报的数据域也需要不断变化。   * 描述你看到的IP数据包Identification字段值的形式。   IP数据包Identification字段值的形式：每个报文有一个唯一的16字节的数值，且不断+1递增。  （3）找到由最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded消息。  思考下列问题：   * Identification字段和TTL字段的值是什么？     Identification字段值为0x0000，TTL字段为255   * 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？   TTL保持不点，ID字段不断改变，原因是：第一跳路由器设置TTL字段为RFC指定的值，因此始终保持不变；而ID值标识每一个IP字段，是唯一的，因此不断改变。  思考下列问题：     * 该消息是否被分解成不止一个IP数据报？   该消息被分为两个数据报   * 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   More Fragment = set表明数据包被进行了分片，IP头部的Offset=0和More Fragment = set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1514  C. 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：     * 原始数据包被分成了多少片？   原始数据包被分成了3片   * 这些分片中IP数据报头部哪些字段发生了变化？   这些分片中IP数据报头部标志位MF变化、片偏移变化。第一个和第二个分片标志位MF为1标识后面还有分片，第一个分片的片偏移为0，第二个为185，第三个是370。  （五）抓取 ARP 数据包  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?     ARP缓存中第一列指的是ARP协议的缓存的IP地址，第二列是MAC地址，第三列是类型，即表示是动态类型还是静态类型。   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？        * 如何判断一个ARP数据是请求包还是应答包？   判断一个 ARP 分组是 ARP 请求还是应答的字段是“OP”，当其值为 0×0001 时是请求，为 0×0002 时是应答。       * 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？   查询ARP不知道目的IP对应的MAC地址，因此需要广播查询；ARP响应的时候已经从查询ARP中找到了源MAC地址，因此ARP响应可以有一个明确的目的地址。  （六）抓取 UDP 数据包  分析 QQ 通讯中捕获到的 UDP 数据包。根据操作思考以下问题：     * 消息是基于UDP的还是TCP的？     消息是基于UDP的   * 你的主机ip地址是什么？目的主机ip地址是什么？   主机ip地址是172.17.122.202目的主机ip地址是39.156.132.108   * 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？   主机发送QQ消息的端口号是4009和QQ服务器的端口号是8000   * 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？   数据报格式：源端口号2B，目的端口号2B，UDP 段长度2B，校验和2B   * 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？   服务器返回ICQ用于确认。这是由于UDP提供的是不可靠的无连接的传输服务，客户端无法确认服务器是否接收到信息，因此需要一个ICQ报文表示收到。可以看出UDP是无连接的。这是因为TCP需要三次握手来建立连接，而UDP没有这个过程。同时UDP首部也没有标志位用于客户端与服务器端之间互相确认传输情况。 |
| 心得体会： |
| 熟悉并掌握 Wireshark的基本操作，了解各层网络协议实体间进行交互以及报文交换的情况（HTTP 协议、TCP协议、IP协议、Ethernet数据帧、DNS协议、UDP协议、ARP协议）。 |