

**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 | 张明远 | | 院系 | 计算机科学与技术 | | |
| 班级 | 2003104 | | 学号 | 120L030501 | | |
| 任课教师 | 聂兰顺 | | 指导教师 | 聂兰顺 | | |
| 实验地点 | 格物207 | | 实验时间 | 2022.10.31 | | |
| 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： |
| 要求撰写实验报告对利用 Wireshark 分析 HTTP、TCP、IP、以太网帧、ARP、DNS 等的抓包分析实验过程、发现的问题、得到的结果、对协议的认识等内容进行总结（可结合每个实验后面的思考题进行分析、总结）。 一、Wireshark简介 Wireshark（前称Ethereal）是一个[网络封包](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B0%81%E5%8C%85?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/Wireshark/_blank)分析软件。[网络封包分析](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B0%81%E5%8C%85%E5%88%86%E6%9E%90/17608901?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/Wireshark/_blank)软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。  在过去，网络封包分析软件是非常昂贵的，或是专门属于盈利用的软件。Ethereal的出现改变了这一切。在GNUGPL通用许可证的保障范围底下，使用者可以以免费的途径取得软件与其[源代码](https://baike.baidu.com/item/%E6%BA%90%E4%BB%A3%E7%A0%81/3969?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/Wireshark/_blank)，并拥有针对其源代码修改及[客制化](https://baike.baidu.com/item/%E5%AE%A2%E5%88%B6%E5%8C%96/9736627?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/Wireshark/_blank)的权利。Ethereal是全世界最广泛的网络封包分析软件之一。wireshark工作流程如下：  （1）确定Wireshark的位置。如果没有一个正确的位置，启动Wireshark后会花费很长的时间捕获一些与自己无关的数据。  （2）选择捕获接口。一般都是选择连接到Internet网络的接口，这样才可以捕获到与网络相关的数据。否则，捕获到的其它数据对自己也没有任何帮助。  （3）使用捕获过滤器。通过设置捕获过滤器，可以避免产生过大的捕获文件。这样用户在分析数据时，也不会受其它数据干扰。而且，还可以为用户节约大量的时间。  （4）使用显示过滤器。通常使用捕获过滤器过滤后的数据，往往还是很复杂。为了使过滤的数据包再更细致，此时使用显示过滤器进行过滤。  （5）使用着色规则。通常使用显示过滤器过滤后的数据，都是有用的数据包。如果想更加突出的显示某个会话，可以使用着色规则高亮显示。  （6）构建图表。如果用户想要更明显的看出一个网络中数据的变化情况，使用图表的形式可以很方便的展现数据分布情况。  （7）重组数据。Wireshark的重组功能，可以重组一个会话中不同数据包的信息，或者是一个重组一个完整的图片或文件。由于传输的文件往往较大，所以信息分布在多个数据包中。为了能够查看到整个图片或文件，这时候就需要使用重组数据的方法来实现。 Wireshark 的使用 （1）启动主机上的 web 浏览器。  （2）启动 Wireshark。只是窗口中没有 任何分组列表。  （3）开始分组俘获：选择“capture”下拉菜单中的“Capture Options”命令，会出现“Wireshark: Capture Options”窗口，可以设置分组俘获的选项。 在实验中，可以使用窗口中显示的默认值。在“Wireshark: Capture Options”窗口的最上面有一个“Interface List”下拉菜单，其中显示计算机所具有的网络接口（即网卡）。当计算机具 有多个活动网卡时，需要选择其中一个用来发送或接收分组的网络接口（如某个有线接口）。随后，单击“Start”开始进行分组俘获，所有由选定网卡发送和接收的分组都将被俘获。  （4）开始分组俘获后，会出现窗口。该窗口统计显示各类已俘获数据包。在该窗口的工具栏中有一个“stop”按钮，可以停止分组的俘获。但此时你最好不要停止俘获分组。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，如：http://www.hit.edu.cn。为显示该网页，浏览器需要连接www.hit.edu.cn 的服务器，并与之交换 HTTP 消息，以下载该网页。包含这些 HTTP 报文的以太网帧将被 Wireshark 俘获。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。Wireshark 主窗口显示已俘获的你的计算机与其他网络实体交换的所有协议报文，其中一部分就是与 www.hit.edu.cn 服务器交换的 HTTP 报文。  （5）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。  （6）选择分组列表窗口中的第一条 http 报文。它应该是计算机发向 www.hit.edu.cn 服务器的 HTTP GET 报文。当选择该报文后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 报文首部信息都将显示在分组首部子窗口中。单击分组首部详细信息子窗口中向右和向下箭头，可以最小化帧、以太网、IP、TCP 信息显示量，可以最大化 HTTP 协议相关信息的显示量。   二、HTTP分析2.1 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://jwts.hit.edu.cn/>  停止分组俘获。   2.2 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://jwts.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。    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。   TCP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，将该文件保存到主机上。    （2） 打开http://gaia.cs.umass.edu/Wireshark-labs/TCP-Wireshark-file1.html，，窗口如下图所示。在Browse按钮旁的文本框中输入保存在主机上的文件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，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。   C. TCP 基础 本部分全部在实验结果部分 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。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。  （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。   对捕获的数据包进行分析  1. 在捕获窗口中，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，如图所示。      1. 单击Source列按钮，这样将对捕获的数据包按源IP地址排序。选择第一个自己主机发出的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，会看到许多后续的ICMP消息。      1. 找到由最近的路由器（第一跳）返回给主机的 ICMP Time-to-live exceeded消息。      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字节后主机发送的第一个ICMP Echo Request消息。    找到在将包大小改为3500字节后主机发送的第一个ICMP Echo Request消息。  **Ethernet数据帧分析** 无教学，主要在结果部分分析 **ARP分析** （1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机  上 ARP 缓存的内容，并使用arp -d删除缓存。     1. 在命令行模式下输入：ping 172.20.36.1     （3）启动 Wireshark，开始分组俘获。抓取的数据包大致如下图所示。   **UDP分析**  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   **DNS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 |
| 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。 一、HTTP分析 访问http://jwts.hit.edu.cn/，wireshark抓包结果如下：   1.1 HTTP GET/response 交互 浏览器运行的为https1.1，下图为浏览器发送的http1.1GET请求    访问的服务器亦为http1.1，下图为服务器发送的http1.1 200 ok    浏览器请求语言版本为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    计算机的IP地址为172.20.53.92，服务器为10.160.2.157    服务器返回200 ok，已在上文展示。 1.2 HTTP 条件GET/response 交互 第一个 GTE 请求在请求报文中无 IF-MODIFIED-SINCE。    服务器确实返回了文件内容，可以通过右侧的HTML内容得知    向发出的较晚 GET 请求中，有该行：IF-MODIFIED-SINCE，且该行后的信息是本地缓存文件中 Last-Modified 字段的最后修改时间    服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是304。服务器没有返回文件的内容。这是因为客户端在找到本地缓存之后，经过请求报文向服务器端确定这一份缓存是最新的，那么服务器端就不再向客户端发送这一份数据，客户端直接使用缓存的数据段。 TCP分析俘获大量的由本地主机到远程服务器的 TCP 分组 本部分无讨论 浏览追踪信息 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址是172.20.53.92和TCP 端口号是53214    Gaia.cs.umass.edu 服务器的 IP 地址是128.119.245.12。对这一连接，它用来发送和接收 TCP 报文的端口号是80 TCP基础 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0x42 58 71 c7，在该报文段中，是用SYN标志位是否为1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0xd2 d0 02 db;该报文段Acknowledgement 字段的值是0x4e 58 71 c8;Gaia.cs.umass.edu 服务器是将SYN报文段序号+1确定的这个值。在该报文段中，可以通过 SYN 和 ACK标志位都为1标识该报文段    从捕获的数据包中分析出 tcp 三次握手过程，为下图所示的三个tcp请求    包含 HTTP POST 命令的 TCP 报文段的序号是0x4e 58 71 c8    该 TCP 连接上的第六个报文段的序号是0x4e 58 8c 58;    发送时间：该报文段于 TCP 三次握手之后，四次挥手之前发送的。该报文段所对应的ACK是在下图时间发送    前六个 TCP 报文段的长度都为1414。    接收端公示的最小的可用缓存空间是29200。限制发送端的传输以后，可以发现接收端的可用缓存空间在递增的，最终可用缓存为237184。空间是足够的。    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是：152,138B/(9.284824-2.540395)s = 22.557KBps       IP分析通过执行 traceroute 执行捕获数据包 本部分无讨论 对捕获的数据包进行分析 主机的IP地址是172.20.53.92    在IP数据包头中，上层协议（upper layer）字段的值是1，代表ICMP    IP头有20字节。该IP数据包的净载为36字节。由下图ip length = 20，Total length = 56  56-20 = 36    该IP数据包没有分片。由MF = 0，标志未分片。    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。除了上述四个数据段以外的数据必须保持常值。  标识ID对于每个数据包来说唯一，因此每个数据包都不一样；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，因而IP数据报的数据域也需要不断变化。 Identification字段值的形式：每个报文有一个唯一的固定16字节的数值，且不断递增一。  由最近的路由器（第一跳）返回给主机的 ICMP Time-to-live exceeded消息，可以看到其  Identification字段和是0x0，TTL字段的值是255。  TTL保持255，与第一条TCMP报文一样，而Identification改变。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。    包大小改为2000字节后主机发送的第一个ICMP Echo Request消息，该IP数据包没有分片。由MF = 1，标志分片。由Fragment Offset = 0标志第一个，该分片的长度为1500B   找到在将包大小改为3500字节后主机发送的第一个ICMP Echo Request消息。 原始数据包被分成了3片。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。 Ethernet数据帧分析 访问的网页为http://jwts.hit.edu.cn/  本主机IP：172.20.171.118，目的主机IP：10.160.2.157  本主机发送的第一条HTTP报文的以太网帧结构等装了上层的IP数据，IP封装了上层的TCP数据报，TCP数据报封装了上层的HTTP数据。  Ethernet数据帧结构如下： IMG_256 5)本主机MAC地址：44:ec:ce:d2:ff:c2，目的主机MAC地址：c8:3d:d4:3d:0c:e1；类型是 IPv4  主机MAC地址 6)发送报文的数据域长度范围为46B-1500B，以太网帧MTU为1500B，所以数据域最大为1500B；数据域最小值计算过程：R=10Mbps，RTTmax=512us，Lmin/R=RTTmax，则Lmin=64B，则Datamin=Lmin-18=46B。 ARP分析 下面给出ARP缓存    ARP缓存中第一列是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。  下面给出ping 命令时的数据包    ARP数据包由9 部分组成，分别是：硬件类型 2B、协议类型 2B、硬件地址长度 1B、协议地址长度 1B、OP 2B、源 MAC 地址 6B、源 IP 地址 4B、目的 MAC 地址 6B、目的 IP 地址 4B；    当 OP 值为 1 时是请求包，当 OP 值为 2 时是应答包。    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。 UDP分析 QQ 通讯中捕获到的 UDP 数据包如下：    消息是基于UDP的。  本主机IP：172.20.36.29，目的主机IP：39.156.132.120。  本机端口为4019，服务器端口为8000  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    服务器返回ICQ向客户端反馈收到信息。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。  UDP是无连接的。TCP需要三次握手来建立连接，而UDP没有这个过程。 DNS分析 本主机IP：172.20.36.29，目的主机IP：10.128.1.114  DNS消息包括Transaction ID，flags，questions，Answer RRs ，Authority RRs，Additional RRs和消息体    DNS 的下层协议是 UDP 协议，是不可靠无连接的传输服务    DNS使用Transaction ID来标识一次查询和响应报文，长度是2B，可以发现请求和相应的响应报文的ID是一致的。      请求体内容：Name表示请求域名，Type表示请求类型，Class一般为IN。 |
| 问题讨论： |
| 对实验过程中的思考问题进行讨论或回答。  实验过程中常见ICMP协议相关问题，在这里就其进行介绍。  ICMP（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议簇的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。事实上ICMP是IP的一个组成部分，与 IP 协议、ARP 协议、RARP 协议及 IGMP 协议共同构成 TCP/IP 模型中的网络层。 |
| 心得体会： |
| 对于计算机网络模型有了更加深入的认识。尤其是对于应用层、传输层、网络层、链路层的一些协议有了更加深入的了解。通过对这些协议报文的抓包分析，对于其结构与工作原理的认识更加深刻。 |