**北京邮电大学课程设计报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **课程设计**  **名称** | **协议数据的捕获和解析** | | **学 院** | **计算机学院** | **指导教师** | **高占春** |
| **班 级** | **班内序号** | **学 号** | | **学生姓名** | **成绩** | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
| **课**  **程**  **设**  **计**  **内**  **容** | 实验教学目的是加深对IP、ICMP、DHCP、ARP、TCP等协议的格式、作用的理解。基本内容是通过资料等方式来学习IP、ICMP、DHCP、ARP、TCP等协议每个字段的意义、结合具体报文分析其实际内容。实验方式是通过wireshark抓包，用过滤器选出要求的包进行分析。 | | | | | |
| **学生**  **课程设计**  **报告**  （附页） |  | | | | | |
| **课**  **程**  **设**  **计**  **成**  **绩**  **评**  **定** | 遵照实践教学大纲并根据以下四方面综合评定成绩：  1、课程设计目的任务明确，选题符合教学要求，份量及难易程度  2、团队分工是否恰当与合理  3、综合运用所学知识，提高分析问题、解决问题及实践动手能力的效果  4、是否认真、独立完成属于自己的课程设计内容，课程设计报告是否思路清晰、文字通顺、书写规范  **评语**:        **成绩**:  指导教师签名：  年 月 日 | | | | | |

注：评语要体现每个学生的工作情况，可以加页。

|  |
| --- |
| **北 京 邮 电 大 学**  **实 验 报 告**  **课程名称\_\_\_\_计算机网络\_\_\_\_\_\_\_\_\_\_**  **实验名称\_\_\_协议数据的捕获和解析\_\_**  **学院班 姓名**  **教师\_\_ \_\_ 成绩\_\_\_\_\_\_**  **2020年6月6日** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **实验内容和实验步骤描述**   **实验内容和实验目的**  本次实验主要包含下列内容：  1）使用 Wireshark 软件捕获在使用 ping 命令时产生的 ICMP 消息；  2）分析网络层 IP 包头格式，理解各字段的作用，对于分段和校验和进行验证；  3）使用 Wireshark 软件捕获在使用 ARP 消息，分析其消息格式，理解其工作原理；  4）使用 Wireshark 捕获 DHCP 消息，分析其消息序列，理解 DHCP 的功能和操作原理；  5）使用 Wireshark 捕获 TCP 消息，分析 TCP 报文段头格式，理解连接建立和释放的原理，差错控制原理、序号和窗口管理的原理。  **实验环境**  Windows 10 操作系统  Wireshark Version 3.6.5  **实验步骤**  **准备工作**  1. 下载 Wireshark 软件  2. 确保计算机已经连接到网络。  3. 启动 Wireshark，设置捕获接口为WLAN，设置合适的捕获过滤器：  对于 ping 命令，设置捕获过滤器为 icmp  对于 DHCP 消息，设置捕获过滤器为 udp port 67  对于 ARP 消息，设置捕获过滤器为 arp  对于通过网页浏览应用来捕获 TCP 消息，设置捕获过滤器为 tcp port 80  4. 开始捕获。  **数据捕获**  依次捕获 ICMP 协议数据、捕获 DHCP 协议数据、捕获 ARP 协议数据、捕获 TCP 协议数据  **协议分析**  运行 Wireshark 软件，打开所捕获的数据文件，完成下列分析工作：  1. IP 包头分析  2. ICMP 消息分析  3. DHCP 消息分析  4. ARP 消息分析  5. TCP 报头及消息分析  上述分析工作在本实验报告后面的部分进行详细描述。  **撰写实验报告**   1. **IP 协议分析**   **1）对于所捕获并选中的 IP 包，找出包头各字段，参照示例的格式记录在实验报告中**  Ping自己的路由器，用指令“ping -4 -l 8000 192.168.1.1”，得到下面的包    分析之，得到   |  |  |  | | --- | --- | --- | | 字段 | 报文（16进制） | 内容 | | 包头长度 | 45 | 用ipv4，包头长度20字节 | | 服务类型 | 00 | 正常 | | 总长度 | 02 74 | 长628字节 | | 标识 | 19 ac | 标识号6572 | | 标志 | 03 | DF=0、MF=0，允许分片，最后一片 | | 片偏移 | 9d | 偏移量7400 | | 生存周期 | 40 | 每跳生存64秒 | | 协议 | 01 | 使用ICMP协议 | | 头部校验和 | d7 d1 | Checksum计算报头是否正确 | | 源地址 | C0 a8 01 1d | 192.168.1.29 | | 目的地址 | C0 a8 01 01 | 192.168.1.1 |   **2）描述 IP 包头校验和的校验原理，并针对上述 IP 包头进行校验和的验证。**校验原理是头里面所有的十六位（半字）累加起来，再取结果的补码，为0  在这个包当中，把所有的都按照模16的形式加起来  4+0+1+0+4+d+c+0+c+0=f  5+2+9+3+0+7+a+1+a+1=f  0+7+a+9+0+d+0+1+0+1=f  0+4+c+d+1+1+8+d+8+d=f  取补码为全0，符合条件  **3）描述 IP 包分段原理，并通过所捕获到的 IP 包的相关字段进行验证。**标识字段用来让目标主机确定一个新到达的分段属于哪一个数据报。DF表示是否允许切割该数据报，在分段后，这里是0。MF表示这个段的后方还有没有分段，有就1，没有就0。offest表示这个段在当前数据报当中的位置，除了最后一个段，其它的段都必须是8的倍数。这几个字段协同工作实现分段操作。    在这个包当中，一共有6段，前五段每一段都是1480，是8的倍数，offset也依次加1480，由此指明段在包中的位置。同时，除了最后一段MF为0以外，其它各段MF都为1，表明各段是完整的包切割后的分段   1. **ICMP 协议分析**   向北邮官网ping，到wireshark里面去看，得到8个报文，4个为request，4个为reply    **1）理解 ICMP 的功能**  ICMP协议数据包对IP分组在传送时出现的异常情况进行报告，包括主机报告差错与异常使用。它传达IP主机、路由器之间传递网络通不通、主机是否可达、路由是否可用等控制信息。所以说，它是一个“错误侦测与回报机制”，其目的就是让我们能够检测网路的连线状况，也能确保连线的准确性。当路由器在处理一个数据包的过程中发生了意外，可以通过ICMP向数据包的源端报告有关事件。  **2）记录 ICMP 的包格式，自己查找资料总结各字段的功能**  我们找几个报文，来分析ICMP数据。  这是第一个报文      一一对应，可知   |  |  |  | | --- | --- | --- | | 字段 | 报文 | 内容 | | 类型 | 08 | 这是一个request | | 代码 | 00 | 为询问的ICMP报文 | | 校验和 | 4d 3c | 用checksum的方式校验 | | 标识符 | 00 01 | 确定该报文的发送者 | | 序列号 | 00 1f | 序列号 | | 数据 |  | 一串32字节的数据 |   同理，看第二个报文（第一个reply）    可以看到，跟上面的基本一样。   |  |  |  | | --- | --- | --- | | 字段 | 报文 | 内容 | | 类型 | 00 | 这是一个reply | | 代码 | 00 | 匹配类型，为回答的报文 | | 校验和 | 55 3c | 用checksum的方式校验 | | 标识符 | 00 01 | 确定该报文的发送者 | | 序列号 | 00 1f | 序列号 | | 数据 |  | 一串32字节的数据 |  1. **DHCP 协议分析**   **1） 对照讲义和教材理解 DHCP 的功能，观察 DHCP ACK 消息的各字段，自己查找资料理解各字段的功能，总结采用 DHCP 协议可以提供哪些配置参数。**  DHCP是动态主机配置协议，用来解决手动配置主机的问题。它可以对远程主机自动配置，包括IP地址、路由地址、子网掩码等，是一个应用层协议。使用DHCP时，每个网络必须有一个DHCP服务器负责地址配置，计算机在字节网络上广播一个报文，请求IP地址。这个请求报文就是DHCP的discover包，这个包给到DHCP服务器，当服务器受到请求后，就为主机分配IP，并通过DHCP的offer包返回回去。  我们看下面这个ACK包      对这个DHCP包进行分析   |  |  |  | | --- | --- | --- | | 字段 | 报文 | 内容 | | 报文类型 | 02 | 为响应报文 | | 硬件类型 | 01 | 服务器为以太网 | | 硬件地址长度 | 06 | 以太网地址长度为6字节 | | 跳数 | 00 | DHCP报文经过的中继数量为0，在同一个网内 | | 事务ID | E8 01 11 75 | 客户端发起请求时产生随机数，标记一次请求 | | 时间 | 00 00 | 发送后经过了0秒 | | 标志 | 00 00 | 采用单播 | | 客户IP | C0 a8 01 1d | 192.168.1.29 | | 你的IP | C0 a8 01 1d | 192.168.1.29 | | 下一个服务器IP | 00 00 00 00 | 0.0.0.0 | | 中介代理的IP | 00 00 00 00 | 0.0.0.0 | | 客户MAC地址 | 1c bf c0 a9 19 4f | Chongqin\_a9:19:4f | | DHCP信息类型 | 35 01 05 | 是ACK，长为1 | | DHCP服务器标识 | 36 04 c0 a8 01 01 | 长为4，标识为192.168.1.1 | | IP租赁时间 | 33 04 00 01 51 80 | 长为4，时间86400秒 | | 子网掩码 | 01 04 ff ff ff ff | 长为4，掩码为全1 | | 路由 | 03 04 c0 a8 01 01 | 长为4，路由192.168.1.1 | | 域名服务器 | 06 04 c0 a8 01 01 | 长为4，路由192.168.1.1 |   可见，DHCP向网络主机提供的配置参数包括向网络主机传送配置信息和分配网络地址。配置信息上，这些信息满足了客户得到这些信息后可以连接Internet上其它主机的需要。在网络地址上，则是在地址池中取出一个IP地址，由以太网地址分配给主机，可以用这个IP地址来唯一标记主机。具体来看，这些参数包括了客户IP、你的IP、客户MAC地址、IP租赁时间、子网掩码、路由地址等等。  **2） 根据捕获到消息，画出 DHCP 地址分配过程的消息序列图。注意 DHCP 是采用 Client-Server 模式工作的，你捕获到的消息中，DHCP Server 是否由路由器充当？是否有 DHCP Relay?**  Discover  服务器  用户  Offer  Request  Ack  DCHP由路由器充当，因为是192.168.1.1。  显示的发送到接受之间的时间为0，所以没有DCHP relay   1. **ARP 协议分析**   **1）根据捕获到的消息，对照讲义，理解 ARP 的功能和操作原理。**  ARP用于把IP地址映射成以太网MAC地址，起到地址解析的作用。因为同一局域网通信不用IP而是用MAC地址通信。具体而言，ARP的操作是先通过DNS找到IP，然后发现在自己所在的网络上，就发送一个广播包到以太网网络上，每个听到这个信息的主机都比对自身，如果拥有这个IP，就回答自己的以太网地址，这样就建立了连接。这个过程就是ARP所做的事情。  **2） 记录 ARP 的包格式，自己查找资料总结各字段的功能。**  看这个ARP协议，分析如下   |  |  |  | | --- | --- | --- | | 字段 | 报文 | 内容 | | 硬件类型 | 00 01 | 以太网 | | 协议类型 | 08 00 | Ipv4 | | 硬件规模 | 06 | 大小为6字节 | | 协议规模 | 04 | 大小4字节 | | Op码 | 00 01 | 是Request | | 发送方MAC地址 | 1c bf c0 a9 19 4f | Chongqin\_a9:19:4f | | 发送方IP地址 | 00 00 00 00 | 0.0.0.0 | | 目标MAC地址 | 00 00 00 00 00 00 | 00:00:00:00:00:00 | | 目标IP地址 | A9 fe dc 9a | 169.254.220.154 |  1. **TCP 协议分析**   **1）对照讲义和教材理解TCP报文段的首部各字段的功能，以表格的方式总结每个字段的名字、长度和功能。**     |  |  |  |  | | --- | --- | --- | --- | | 字段 | 报文 | 长度（位） | 功能 | | 来源端口 | E8 94 | 16 | 标记链接的来源端 | | 目的端口 | 01 bb | 16 | 标记链接的另一端 | | 序列号 | 69 94 42 79 | 32 | 给字段编号 | | 确认号 | 51 87 c7 bf | 32 | 返回确认 | | 头长度 | 5 | 4 | 指明TCP头包括多少32位的字 | | CWR | 0 | 1 | 拥塞 | | ECE | 0 | 1 | 拥塞 | | URG | 0 | 1 | 有没有紧急指针 | | ACK | 1 | 1 | 确认段是否有效 | | PSH | 1 | 1 | 是否是push的数据 | | RST | 0 | 1 | 重置一个混乱的连接 | | SYN | 0 | 1 | 用来同时表示request和accepted | | FIN | 0 | 1 | 释放连接 | | 窗口 | 02 00 | 16 | 标记窗口大小 | | 校验和 | Eb d7 | 16 | 校验传输是否正确 | | 紧急指针 | 00 00 | 16 | 指示紧急数据，方便中断 |   **2） 针对连接建立消息和连接释放消息，分析相应标志位和序号的作用，参照讲义中的示例画出连接建立和连接释放过程的消息序列图，在图上标出对应的标志位和序号。**  建立连接时  SYN(SEQ=x)  主机2  主机1  SYN(SEQ=Y,ACK=x+1)  (SEQ=x+1,ACK=y+1)  采用三次握手建立连接。第一次是发送syn包给主机2，到达接受方以后，那里的TCP实体就检查是否有一个进程已经在目标端口字段指定的端口，如果有在监听的，就移交给这个进程。如果它接受，就返回一个确认段，自己发送一个SYN包回去，这是第二次握手。第三次是主机1收到主机2发的SYN+ACK包，向主机2返回确认，这时两个主机完成三次握手，均进入了established状态，可以传输数据了。  释放连接时  SYN(SEQ=x),ACK=1,FIN=1  主机2  主机1  SYN(SEQ=Y,ACK=x+1),ACK=1  SYN(SEQ=y+1),ACK=1,FIN=1  SEQ=x+1,ACK=y+2  第一次是主机1发送一个FIN来关闭1对2的数据发送。第二次是主机2发回一个ACK，确认序号加1，其FIN将占用一个位。第三次是主机2传一个FIN给主机1，关闭数据发送。第四次是主机1接收到，发回ACK报文，双方断开连接。  **3） 针对 TCP 的数据传输过程中的数据报文段和应答报文段，分析发送序号、应答序号、应答标志位、窗口大小、数据长度、MSS 等字段的作用，参照讲义中的示例画出数据传输过程的消息序列图，其中应包括数据校验错和数据丢失导致的数据重传情形，在图上应标出对应的序号、标志位**  **和窗口大小。**发送字号帮助接受有一个顺序，保证数据有序。应答序号表明了哪些序号的已成功接受，而这个之后的可以开始传了。应答标志位指示了拥塞等，进行流量控制保证发送效率。窗口大小保证了多久才会发现问题，以及提升传输效率。数据长度指示了数据包的大小。MSS标识TCP能够承载的最大的应用数据段长度。  窗口大小：2  主机2  主机1  SEQ:501-600,ACK:x  SEQ:601-700,ACK:x  ACK:701  SEQ:701-800,ACK:x  lost  SEQ:701-800,ack:x  Ack:701  Seq:701-800,ack:x  Ack:901   1. **实验结论和实验心得**   **问题和解决方案**  **问题1**  我的是IPV6，直接ping的话得到的是一个IPV6的报文，格式与我们需要的IPV4的很不一样，实验无法进行。  **解决**  通过查找资料，我了解到用“ping -4”就能强制性传输IPV4的报文，从而得到合法的材料，实验得以进行  **问题2**  Ping -l 8000时，尝试了很多个网站，总是提示“请求超时”，均无法ping通  **解决**  改为ping路由器192.168.1.1，这样可以ping通  **问题3**  做DHCP时，用udp port 67过滤器过滤得不到任何结果  **解决**  改为用DHCP过滤，可以得到很多DHCP的包，经比对，就是我们实验要用的那些包  **实验心得**  通过实验，我更进一步掌握了IP、ICMP、DHCP、ARP、TCP等协议，对它们有了比较直观的认识，感觉自己花的时间和精力没有白费，还是学到很多东西的。  用Wireshark做抓包真的非常简单而方便，门槛非常低，让我能够一开始就沉浸在实验当中，而不会像其它学科的很多实验一样要花很多时间搭环境、做准备工作。从这一点上来说，我非常喜欢这个实验。  此外，这个实验看上去条理清晰、操作简便，但其实是一个力气活。我从早上做到晚饭，一直做了7-8个小时，才做完这个实验。因为要填写的数据非常多，IP、ICMP、DHCP、ARP、TCP每一个都要仔细分析它的组成，还是要下功夫，花费很多时间的。而且在这个过程中，我深刻地发现自己对有关知识的掌握还是有欠缺，这个实验很好地帮我增长了这方面的知识。  最后，在实验中，我遇到了一些问题。通过查阅资料、请教同学等方式解决了它，增长了自己的自学能力。 |