

**实验报告**

**课程名称： 计算机网络原理**

**学生姓名： 朱方灏钧 学号： 210111316**

**年级专业： 19级软件工程 班级： 19.11**

**指导教师： 张毅**

**开课学期： 2021 年— 2022 年 1 学期**

**宜宾学院人工智能与大数据学部实验教学中心**

**宜宾学院人工智能与大数据学部**

**实验报告**

**年级：19级**  **专业：软件工程** **上课日期： 2021**年 11月28日

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | **arp协议分组结构** | | | | | |
| **学生姓名** | **朱方灏钧** | **学号** | **210111316** | **实验合作者 姓名** | **无** | |
| **指导教师(签名)** |  | **评 阅 日 期** | |  | **实验报告分** |  |
| **实验报告基本内容：**一、实验目的；二、实验内容；三、实验原理；四、实验步骤及结果；五、实验遇到问题及解决方法；六、实验结论 | | | | | | |
| 1. 实验目的：   掌握arp协议分组结构   1. 实验内容： 2. 在命令提示符中，利用ipconfig /all查看自己主机的ip及MAC地址，查看自己的网关IP地址并记录，方法同实验1。   IMG_256   1. 在命令提示符输入arp，查看arp工具的参数。输入arp –a，查看本地的arp缓存表，并记录下表（不够可添加行）：  |  |  |  | | --- | --- | --- | | Internet地址 | 物理地址 | 类型 | | 192.168.1.1 | 9c-a6-15-f6-5f-4e | 动态 | | 192.168.1.100 | 94-e4-ba-d9-aa-01 | 动态 | | 192.168.1.104 | 20-16-b9-e7-de-84 | 动态 | | 192.168.1.255 | ff-ff-ff-ff-ff-ff | 静态 | | 224.0.0.22 | 01-00-5e-00-00-16 | 静态 | | 224.0.0.251 | 01-00-5e-00-00-fb | 静态 | | 224.0.0.252 | 01-00-5e-00-00-fc | 静态 | | 224.0.0.253 | 01-00-5e-00-00-fd | 静态 | | 238.238.238.238 | 01-00-5e-6e-ee-ee | 静态 | | 239.11.20.1 | 01-00-5e-0b-14-01 | 静态 | | 239.255.255.250 | 01-00-5e-7f-ff-fa | 静态 | | 255.255.255.255 | ff-ff-ff-ff-ff-ff | 静态 |  1. 输入arp –d，删除本地的arp缓存表，使用arp –a再次查看arp缓存表，说明发生了什么变化。输入”ping 网关地址”，再次查看arp缓存表，说明发生了什么变化。通过以上实验的结果，尝试分析arp缓存表的工作模式。   IMG_256  IMG_256  答：输入arp -d时，arp缓存被清空了，ping以后，arp缓存增加了网关的缓存地址，所以arp是工作模式是用来缓存已经与互联网连接的目标地址的，这样就可以减少再次寻找目标地址的时间   1. 运行wireshark抓包分析工具，开始进行捕获，捕获前或者捕获中运行arp –d清除arp缓存表然后在命令提示符输入”ping 网关地址”，过一段时间后停止捕获，观察捕获到的数据包。   IMG_256   1. 在过滤栏中，设置过滤条件过滤从本机mac地址发出的arp数据包，查看捕获数据包的数据链路层帧结构及arp协议分组结构，并记录下表  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 目的MAC地址 | | 源MAC地址 | | | | 类型 | | | 9c-a6-15-f6-5f-4e | | 94-e4-ba-d9-aa-01 | | | | ARP | | | 硬件类型 | 上层协议类型 | | MAC长度 | | IP长度 | | 操作类型 | | Ethernet | IPv4 | | 6 | | 4 | | Request | | 源MAC地址 | | | | 源IP地址 | | | | | 94-e4-ba-d9-aa-01 | | | | 192.168.1.100 | | | | | 目的MAC地址 | | | | 目的IP地址 | | | | | 9c-a6-15-f6-5f-4e | | | | 192.168.1.1 | | | |   根据捕获的数据包信息思考并回答以下问题：   1. 从帧头中的MAC地址来看这个数据帧是谁发给谁的？ 2. arp分组结构中的硬件类型、上层协议类型、操作类型分别是起什么作用的？ 3. arp分组结构中的目的MAC地址是多少？为什么是这个取值？ 4. 试分析这个arp分组是起什么作用的？   IMG_256  答：从本地主机发送到目标主机的  答：硬件类型表示是用什么硬件进行的连接，比如有线网，或者WiFi，上层协议类型表示使用连接的通信是什么应用层协议的，操作类型是指此通信是请求或者回复  答：目的mac地址是94-e4-ba-d9-aa-01，因为这是需要搜索的目标主机的物理地址  答：arp分组是用来记录当前arp数据包的一些基本信息，方便互联网进行解析的   1. 在过滤栏中，设置过滤条件过滤从网关MAC地址发出的arp数据包，查看捕获数据包的数据链路层帧结构及arp协议分组结构，并记录下表  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 目的MAC地址 | | 源MAC地址 | | | | 类型 | | | 94-e4-ba-d9-aa-01 | | 9c-a6-15-f6-5f-4e | | | | ARP | | | 硬件类型 | 上层协议类型 | | MAC长度 | | IP长度 | | 操作类型 | | 以太网 | IPv4 | | 6 | | 4 | | Reply | | 源MAC地址 | | | | 源IP地址 | | | | | 9c-a6-15-f6-5f-4e | | | | 192.168.1.1 | | | | | 目的MAC地址 | | | | 目的IP地址 | | | | | 94-e4-ba-d9-aa-01 | | | | 192.168.1.100 | | | |   根据捕获的数据包信息回答以下问题：   1. 从帧头中的MAC地址来看这个数据帧是谁发给谁的？ 2. arp分组结构中的操作类型字段与步骤5中的对应字段有何变化？ 3. 试分析这个arp分组是起什么作用的？   IMG_256  答：是从目标主机发送到本机主机的  答：从请求变成了回复  答：是回复目标主机的请求，以便于建立一个源头到目标的连接通路   1. 思考：请根据今天实验的所有实验结果 2. 说明arp协议工作的触发条件是什么？ 3. 分析arp协议在主机中工作的完整工作过程是如何进行的？ 4. arp协议可能存在的安全风险是什么？   答：是需要寻找目标主机时，发送arp广播包  答：是当主机需要同目标地址进行连接时，会从主机发送arp请求广播包，当寻找到目标主机以后，发送回复arp广播包，建立连接桥梁，再进行相应的操作  答：如果黑客使用arp欺骗的话，就会让发送端与错误的目标主机建立连接，从而盗取数据   1. 实验原理：   利用wireshark的软件功能实现   1. 实验步骤及结果 2. 实验遇到问题及解决方法   无   1. 实验结论   通过wireshark的使用，把课堂上学到的理论知识用到了实践中，真正理解了什么是arp数据包的知识 | | | | | | |
| **指**  **导**  **教**  **师**  **评**  **语** | | | | | | |