|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级： 2020 | 班级： 网三 |
| 分组： | | 实验室：402 | 指导教师：郭念 | 实验日期：2023-02-24 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验一 ARP地址解析协议 | | |
| **实验目的** | 1) 掌握ARP协议的作用和格式。 | | |
| **实验内容** | 1) ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。用于解析MAC地址以实现链路层操作。IP数据包常通过以太网传输，在以太网中是以48位的物理地址传输数据包而不是32位的IP地址。因此当我们知道IP地址不知道MAC地址时，就要用到ARP协议。ARP协议的功能是将网络层的IP地址转换为数据链路层的MAC地址。ARP协议的请求包是以广播方式发送的，网段中的所有主机都会接收到这个包。如果一个主机的IP地址与ARP请求中的目的IP地址相同，该主机会对这个请求数据包作出ARP应答，将其MAC地址发送给请求端。  2) ARP请求或应答的分组格式:  图片.png  **硬件类型**：表示硬件类型，1表示以太网。  **协议类型**：表示要映射的协议类型，0x0800表示IP地址。  **硬件长度**：指明硬件地址长度，单位是字节，MAC是48位，6个字节。  **协议长度**：高层协议地址的长度，对于IP地址，长度是4个字节。  **操作码**：共有二种操作类型，1表示ARP请求，2表示ARP应答。  **发送方MAC**：6个字节的发送方MAC地址。  **发送方IP**：4个字节的发送方IP地址。  **目的MAC**：6个字节的目的物理地址。  **目的IP**：4个字节的目的IP地址。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 ☑设计性 □综合性 | | |
| **实验的重点、难点** | ARP工作流程和报文格式 | | |
| **实验环境** | 绘图1  本次实验根据虚拟机的真实MAC地址进行实验. | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、查看主机信息**  1.1 在主机A上,单击”开始”->”运行”-〉输入“cmd”->”ipconfig /all”,显示主机A的IP设置。**实验截图如下:**    1.2 输入命令“arp -a”查看ARP缓存表，输入“arp -d”清空缓存表。  **实验截图如下:**    **二、分析ARP协议**  2.1 打开主机B上的“网络协议分析软件，单击工具栏”过滤器“-〉”添加“-〉”类型过滤器“->”arp协议“->”接受”->”设置参数”-〉”确定“，然后单击”开始“按钮，捕捉arp数据包。然后单击菜单栏中的”开始”按钮,开始抓包。**实验截图如下:**    2.2 在主机A输入命令“arp -a”查看ARP缓存表，输入“arp -d”清空缓存表。**实验截图如下:**    2.3 在主机A命令行窗口输入“ping 192.168.1.3”。**实验截图如下:**    2.4 查看主机B上的网络协议分析软件，捕获到ARP请求报文,写出各个字段的值和含义。**实验截图如下:򁹸**    l  **硬件类型：** 0001  l  **协议类型**： 0800  l  **硬件长度**： 6  l  **协议长度**： 4  l  **操作码**： 1  l  **源物理地址**：B2-0B-16-15-13-13  l  **源IP地址**： 192.168.1.3  l  **目标物理地址**：00-00-00-00-00-00  l  **目标IP地址**： 192.168.1.2  2.5 查看主机B上的网络协议分析软件，捕获到主机B发送的ARP应答报文。,写出各个字段的值和含义。**实验截图如下:**    l  **硬件类型：** 0001  l  **协议类型**： 0800  l  **硬件长度**： 6  l  **协议长度**： 4  l  **操作码**： 2  l  **源物理地址**：44-9D-84-3B-C5-5F  l  **源IP地址**： 192.168.1.2  l  **目标物理地址**：B2-0B-16-15-13-13  l  **目标IP地址**： 192.168.1.3  **三、数据包发送器发送ARP数据包**  3.1 在主机A上打开”数据包发送器”，单击工具栏“添加”按钮，选择“ARP协议模板”，单击“确认”按钮，建立一个ARP数据包。**实验截图如下:**  3.2 在数据包编辑区，设置ARP数据包的各项数值。设置源物理地址为主机A的MAC地址00-22-22-22-22-22，目的物理地址为“FF-FF-FF-FF-FF-FF”,即广播地址。**实验截图如下:**  **Ethernet封装：**  l  **目的物理地址**：FF-FF-FF-FF-FF-FF，ARP请求为广播报文，目的地址为广播地址；  l  **源物理地址**：00-22-22-22-22-22，发送端物理地址；  l  **类型**：0806，上层协议是ARP协议；  l  **硬件类型**：0001，表示硬件类型为以太网；  l  **协议类型**：0800，表示上层协议是IP地址；  l  **硬件长度**：6，表示硬件地址长度为6字节；  l  **协议长度**：4，表示协议地址长度为4字节；  l  **操作码**：1，表示此ARP报文为ARP请求报文。  **ARP封装：**  l  **发送物理地址**：00-22-22-22-22-22，为发送ARP请求报文主机的物理地址；  l  **发送IP地址**：192.168.1.2，为发送ARP请求报文主机的IP地址；  l  **目标物理地址**：FF-FF-FF-FF-FF-FF，ARP请求为广播报文，目的地址为广播地址；  l  **目标IP地址**：192.168.1.3，目标主机IP地址。  3.3 在主机B上,单击”开始”->”运行”-〉输入“cmd”->” arp -d”, 清空ARP高速缓存，然后输入” arp -a”查看主机B的缓存。**实验截图如下:**    3.4 在A的数据包发送器上单击工具栏中“发送”按钮，选中“循环发送”->”5”-〉“开始”，发送5个ARP请求报文（先打开主机B上的网络协议分析软件，并单击菜单栏“开始”按钮，开始抓包）。**实验截图如下:**    3.5 主机B收到主机A的第一个数据包为arp请求数据包，目的MAC地址为广播地址，操作码值为1（表示arp请求数据包）。**实验截图如下:**    3.6 在数据包分类列表中，单击第二个数据包。目的MAC地址为主机A的MAC地址，操作码值为2（表示为ARP应答数据包），主机B发送一个ARP单播帧给主机A，告诉主机A主机B的MAC地址。**实验截图如下:**    3.7 在主机B用命令arp -a可以查看ARP缓存中主机B的ARP记录，当主机A编辑ARP请求报文发送给主机B，主机B收到主机A的ARP请求报文，首先把主机A的IP和MAC对应关系更新到主机B的ARP的缓存中（arp缓存有时间限制，超过规定时间，arp缓存表清空）。**实验截图如下:**    3.8 在主机A打开“网络协议分析软件”，抓取主机B发送给主机A得ARP应答包。当主机B发送ARP应答报文发送给主机A，主机A收到主机B的ARP应答报文，把主机B的IP和MAC对应关系更新到主机A的ARP的缓存中。**实验截图如下:** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**  1． arp数据包可以请求不同网段的主机MAC地址？  不可以，ARP协议适用于获取同一物理网络的主机的马车地址的协议，因此ARP数据包只能用于请求同一网络上的主机mac地址。  如果想请求不同网络上的主机的MAC地址，需要使用另一个协议，如IPv6的Neighbor Discovery Protocol (NDP)或IPv4的Proxy ARP。 NDP允许IPv6主机查询其连接的网络上的另一个IPv6主机的MAC地址。Proxy ARP允许一个网络上的主机充当另一个网络上的主机的代理，响应其他网络上的主机的ARP请求，从而允许不同网络上的主机之间通信 | | |

**注意：**

1. **实验关键步骤和结果需要截图后粘贴到相应位置，截图要注明学号和姓名。**
2. **提交实验报告时，文档名改为：学号-姓名-实验名称.docx。**