**实验5 arp协议分组结构**

**实验目的：**

掌握arp协议分组结构。

**实验内容：**

1. 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。
2. 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 |
|  |  |  |

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。
2. 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。
3. 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 | |
|  | |  | | | |  | |
| 硬件类型 | 上层协议类型 | | MAC长度 | | IP长度 | | 操作类型 |
|  |  | |  | |  | |  |
| 源MAC地址 | | | | 源IP地址 | | | |
|  | | | |  | | | |
| 目的MAC地址 | | | | 目的IP地址 | | | |
|  | | | |  | | | |

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？
5. 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 | |
|  | |  | | | |  | |
| 硬件类型 | 上层协议类型 | | MAC长度 | | IP长度 | | 操作类型 |
|  |  | |  | |  | |  |
| 源MAC地址 | | | | 源IP地址 | | | |
|  | | | |  | | | |
| 目的MAC地址 | | | | 目的IP地址 | | | |
|  | | | |  | | | |

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？
4. 思考：请根据今天实验的所有实验结果
5. 说明arp协议工作的触发条件是什么？
6. 分析arp协议在主机中工作的完整工作过程是如何进行的？
7. arp协议可能存在的安全风险是什么？