

实验4 网络嗅探与伪造

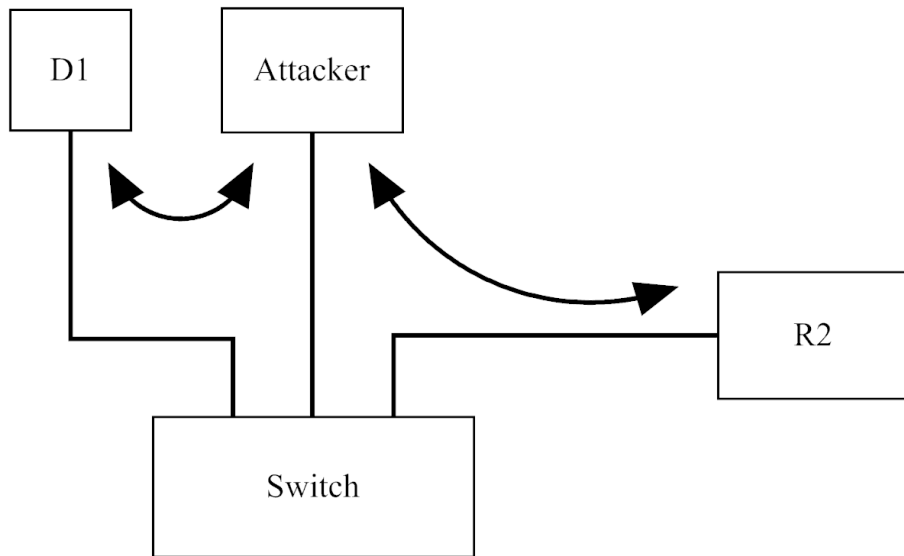
物理网络层安全

基本任务：ARP欺骗

- 链路层数据
 - `socket(PF_PACKET, SOCK_RAW, htons(ETH_P_ARP))`
- 任务：
 - 复习ARP协议
 - 设计软件，实现ARP欺骗
 - 观察ARP缓存更新策略，总结在发送什么报文时，ARP欺骗可以成功

进阶任务：ARP中间人攻击

- 在“数据包嗅探编程”、“数据包伪造编程”和“ARP欺骗”基础上，实现利用ARP完成中间人攻击。



思路

- 1. 对两个目标方同时实施**ARP**欺骗攻击
- 2. 接收双方通信内容，并转发