利用Wireshark观察网络报文(3)

ARP协议

1.实验内容

利用wireshark观察arp数据包.

(1) 指定显示过滤器, 只显示”请求指定IP的MAC地址”的arp数据包. (20%)

(2) 指定显示过滤器, 只显示**指定主机**发送的”请求指定IP的MAC地址”的arp数据包. (25%)

(3)删除本地缓存的某个主机的arp条目, 然后ping该主机, 定义过滤器, 只显示**重建该arp条目**的数据包. (30%)

删除arp缓存的方式:

Windows: 以管理员打开cmd, 运行 arp -d 即可清空缓存

Linux: 以root身份运行arp -d ip/host 即可删除指定项

2. 提交

(1) 文档(15%), 描述实验过程和结果, 文件名为

”学号+姓名+wireshark_arp_report.pdf”, 应包含:

- 使用到的显示过滤器.
- 应用每个显示过滤器后的截图.
- 内容(3)操作前后arp缓存的变化(截图).

(2) 导出抓取的所有数据包为pcap文件,

文件名为”学号+姓名+wireshark_arp_cap.pcapng”. (10%)

注意:

如果观察不到arp包, 可以尝试ping其他主机.

wireshark抓包实验包含多个部分, 本次为第四部分. 各项后的百分比为该项占本部分实验的分值的百分比.

将抓包文件和word文档放在一个目录下, 目录名为”学号+姓名+实验4.3”, 将此目录压缩为zip再提交. 请在2018年12月11日之前(不包含12月11日)提交到 ftp://222.195.68.57/