Lab 8：链路层观察

一、实验任务一：Ethernet帧观察

捕获以太网帧

- step1：清空浏览器缓存
- step2：wireshark抓包
- step3：访问http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

选中包含HTTP GET消息的以太网帧，回答以下问题：

- 你的电脑的mac地址是多少？
- 以太网帧的目标mac地址是多少？这个地址是gaia.cs.umass.edu的mac地址吗？
- 以太网帧EtherType字段值是多少，对应着什么协议？
- 从以太网帧的开始到”GET”中的’G’出现，有多少字节？

选中第一个包含HTTP响应消息的以太网帧，回答以下问题：

- 这个以太网帧中，源mac地址是多少？拥有这个以太网地址的设备是什么？
- 这个以太网帧中，目的mac地址是多少？拥有这个以太网地址的设备是什么？
- 以太网帧EtherType字段值是多少，对应着什么协议？
- 从以太网帧的开始到”OK”中的’O’出现，有多少字节？

二、实验任务二：ARP

查看计算机上ARP缓存：　　MS-DOS: arp -a；　　Linux/Unix/MacOS：arp

回答以下问题：

- 列出ARP缓存的内容(截图)，每列表示什么意思？

清除计算机上ARP缓存：　　MS-DOS: arp -d；　　Linux/Unix/MacOS：arp -ad

抓取ARP包：

- step1：清空ARP缓存
- step2：清空浏览器缓存
- step3：wireshark抓包
- step4：访问http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

抓取并观察ARP包，回答以下问题：

- 第一个包含ARP请求信息的以太网帧中，源和目的mac地址为？

参考ARP规范，回答以下问题：

- ARP操作字段在以太网帧的第几个字节？
- 进行ARP请求的以太网帧中，ARP负载部分操作字段值是多少？
- ARP消息是否包含发送方的IP地址？
- 在ARP请求中从哪里看出我们想查询相应IP的mac地址？

找到ARP请求对应的回应包，回答以下问题：

- ARP操作字段在以太网帧的第几个字节？
- 进行ARP响应的以太网帧中，ARP负载部分操作字段值是多少？
- ARP回应之前请求信息的内容？
- 包含ARP回应信息的以太网帧中，源和目的mac地址为？

按照实验要求完成实验，提交实验报告，并提供回答的依据及必要的截图。

Previous

Lab 7：网络层控制平面流表下发

Next
附录A：Wireshark 教程

Last updated 8 minutes ago