

利用Wireshark观察网络报文 (2)

网络层

1.实验内容

实验步骤

利用 wireshark 和 PingPlotter 观察网络层数据包

- (1) 下载并安装wireshark以及PingPlotter
- (2) 配置PingPlotter发包大小为3000Bytes
- (3) 启动wireshark
- (4) 启动PingPlotter追踪 gaia.cs.umass.edu，大约count值为3-4次时停止

1. 实验内容

实验要求

- (1) 保存抓包结果, 文件名为”学号+姓名+wireshark_ip_cap.pcapng” 。 5%
- (2) 结合抓包结果分析:
 - 使用显示过滤器, 过滤出本机到目的主机的所有IP和ICMP数据包。 10%
 - 查找本机发送的第一个 TTL等于1 的 ICMP Echo Request 消息, 请问此IP数据报是否被分片 (fragmented) ? 10%
 - 打印出碎片IP数据报的第一个片段。IP 头中的哪些信息表明数据报已碎片化? IP报头中的哪些信息表明这是第一个片段还是后一个片段? 这个IP 数据报header有多少个字节? 有效负载有多少个字节? 20%
 - 打印出碎片 IP 数据报的第二个片段。IP 报头中的哪些信息表明这不是第一个数据报片段? 是否还有更多的片段? 20%
 - 从原始数据报创建了多少个片段? 如何判断是最后一个片段? 最后一个IP数据报负载有多少个字节? TTL的值? 下层协议字段? 20%

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_ip_report.pdf”，应包含

- 使用到的显示过滤器以及应用显示过滤器后的截图
- 抓包分析结果需要有推理过程，以及截图佐证

注意：

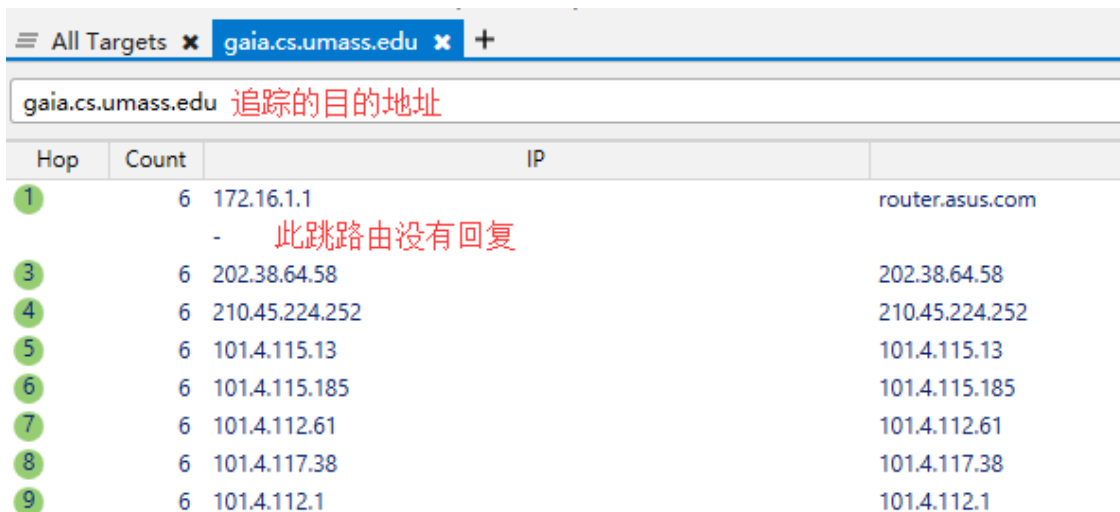
wireshark抓包实验包含多个部分, 本次为第二部分. 各项后的百分比为该项占本部分实验的分值的百分比.

将抓包文件和pdf文档放在一个目录下，目录名为“学号+姓名+实验4.2”，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/>.

PingPlotter

(1) 简介

PingPlotter通过ICMP协议发送不同TTL值的PING包，计算和获取访问网站所经过的路由。TTL是存活时间，每经过一次路由器，存活时间就会减一，当其为0时候，路由会丢掉这个包并且发出TTL超时给原始的发出者。然后每次PingPlotter都会发送从TTL=1起始的数据包，然后逐渐增大TTL，用来获取所访问网站经过的路由。有些路由会因为安全不回应这些包，所以会看到有些请求并没有回复。



The screenshot shows the PingPlotter application window. At the top, there's a tab labeled 'All Targets' with a sub-tab for 'gaia.cs.umass.edu'. Below the tab, the target address 'gaia.cs.umass.edu' is entered, followed by the red text '追踪的目的地址'. The main area displays a table of network hops. The table has three columns: 'Hop', 'Count', and 'IP'. The first row shows Hop 1 with Count 6 and IP 172.16.1.1, with a red note '- 此跳路由没有回复' (This hop router did not respond). The subsequent rows show hops 3 through 9 with their respective counts and IP addresses. The IP address for the final hop is 'router.asus.com'.

Hop	Count	IP
1	6	172.16.1.1
	-	- 此跳路由没有回复
3	6	202.38.64.58
4	6	210.45.224.252
5	6	101.4.115.13
6	6	101.4.115.185
7	6	101.4.112.61
8	6	101.4.117.38
9	6	101.4.112.1

PingPlotter

(2) 下载（注：专业版只有14天试用时间）

<http://222.195.68.57/011144/>

(3) 配置发包大小

