实验三

IP

**实验目的**

此次实验室中我们将探究IP协议，重点是IP数据报。通过分析traceroute程序执行时发送和接收的IP数据报的捕获跟踪（traceroute程序本身在刚完成的Lab 3 ICMP实验中进行了详细的探索）来实现这一点。我们将分析IP数据报中的各个字段，并详细探究IP分片。

在开始实验之前，请先复习课本中的第1.4.3节和RFC 2151的第3.4节，以熟悉traceroute程序的操作。也请复习课本中的第4.3节，并准备好RFC 791，以讨论IP协议。

**实验步骤**

1. 执行traceroute并捕获其数据包

为了生成这个实验里需要捕获跟踪的IP数据报，我们使用traceroute程序将不同大小的数据报发送到某个目的地，回想一下traceroute的操作方式是首先发送一个或多个数据报，IP报头中的生存时长（TTL）字段设置为1；然后将一系列一个或多个TTL值为2的数据报发送到同一目的地；然后将TTL值为3的一系列数据报发送到同一目的地；依此类推。回想一下，路由器必须将每个接收到的数据报中的TTL递减1（实际上，RFC791表述路由器必须将TTL至少减一）。如果TTL成为0，路由器将向发送主机返回一条ICMP消息（类型11-TTL 超期）。通过这种方式，TTL为1的数据报（由执行traceroute的主机发送）将导致距离发送方一跳的路由器向发送方回送ICMP TTL超期的消息；TTL为2的数据报将导致两跳距离的路由器向发送方回送ICMP消息；TTL为3的数据报将导致三跳距离的路由器地将ICMP消息回送给发送者；依此类推。这样，执行traceroute的主机可以通过查看包含ICMP TTL 超期消息的数据报中的源IP地址来获知其自身和目标X之间路由器的标识。

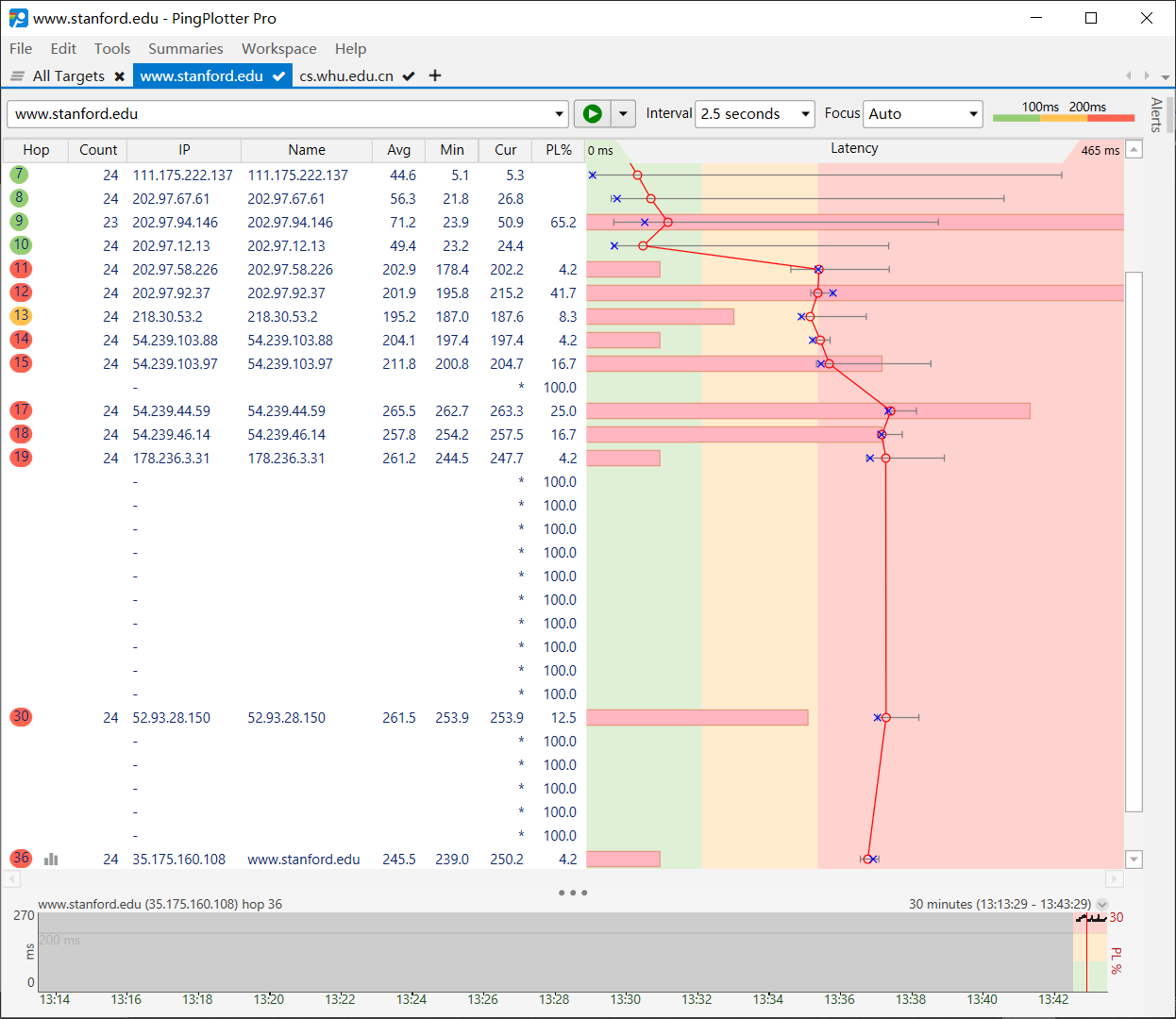
我们运行traceroute并用它发送不同长度的数据报。

* **Windows:** Windows提供的tracert程序（用于前面的Wireshark ICMP实验）不允许更改tracert程序发送的ICMP echo请求（ping）消息的大小。一个更好的Windows traceroute程序是pingplotter，在http://www.pingplotter.com上有免费版本和共享版本。下载并安装pingplotter，执行几个到你喜爱的站点的traceroute来测试一下。选择菜单项“编辑”->“选项”->“默认设置”->“引擎”，然后填写“数据包大小”字段，可以在pingplotter中显式设置ICMP回显请求消息的大小56字节。一旦pingplotter发送了一系列TTL值不断增加的数据包，它将在等待跟踪间隔时间后，以TTL值1重新启动发送过程。跟踪间隔的值可以在pingplotter中显式设置。
* **Linux/Unix/MacOS:** 使用Unix/MacOS traceroute命令，可以通过指示数据报中的字节数来显式地设置发送到目标的UDP数据报的大小；该值在目标名称或地址之后输入traceroute命令行中，要向www.stanford.edu发送2000字节的traceroute数据报，命令如下：

%traceroute www.stanford.edu 2000

执行以下操作：

* 启动Wireshark并开始数据包捕获（捕获->启动），然后在Wireshark数据包捕获选项屏幕上按OK（我们不需要在此处选择任何选项）
* 如果你使用的是Windows平台，启动pingplotter并在“Address to Trace Window”窗口中输入目标目的地的名称。选择菜单项“编辑”->“选项”->“默认设置”->“引擎”，在“数据包大小”字段中输入56的值，然后按“确定”。然后按“跟踪”按钮。您应该会看到一个pingplotter窗口，它看起来像这样地：



接下来，通过选择“编辑”->“选项”->“默认设置”->“引擎”，发送一组长度较长的数据报，并在“数据包大小”字段中输入值2000，然后按“确定”。然后按Resume按钮。

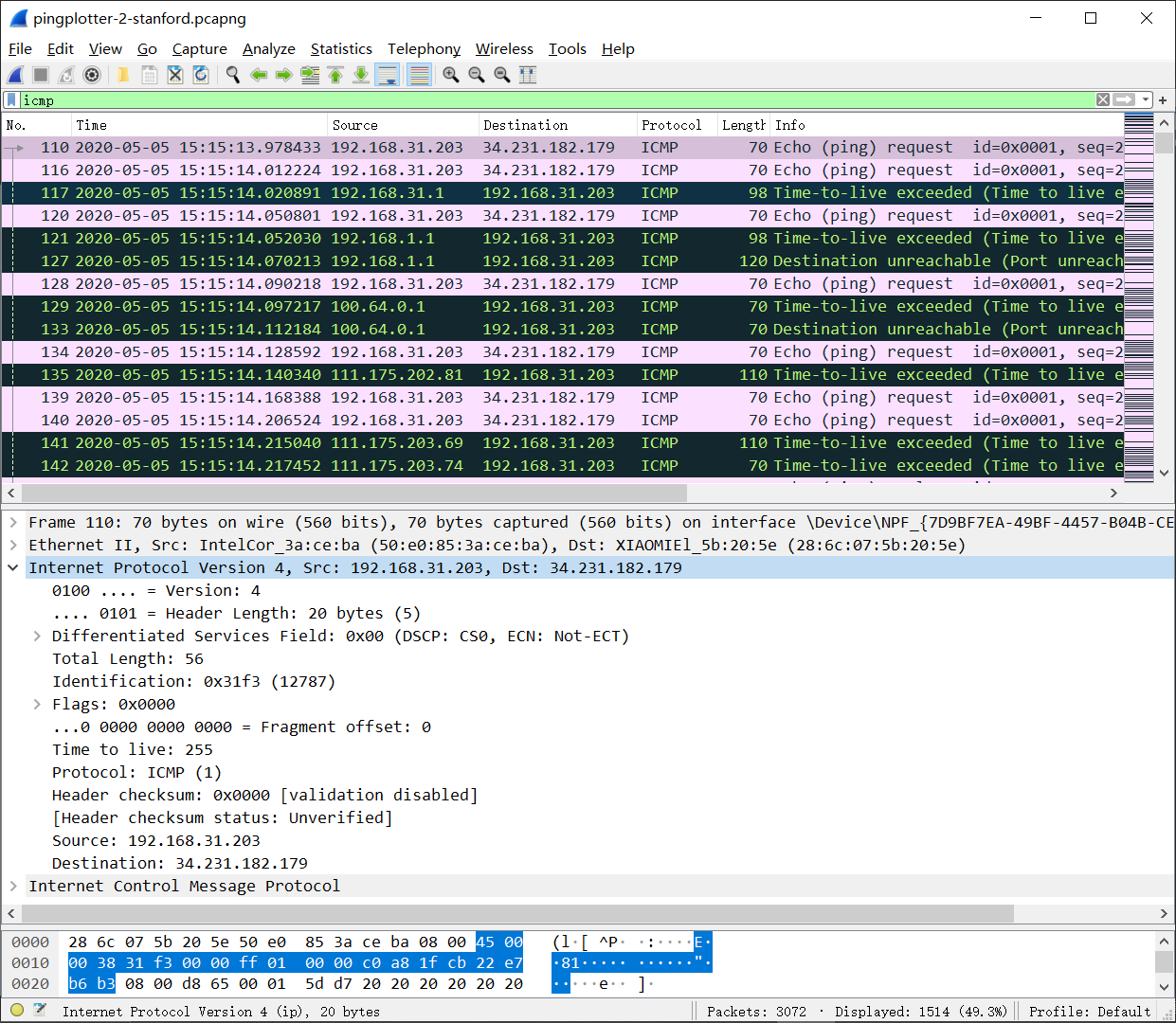
最后，选择“编辑”->“选项”->“默认设置”->“引擎”，在“数据包大小”字段中输入3500的值，然后按“确定”，然后按Resume按钮，发送一组较长的数据报。

停止wireshark追踪。

1. 查看捕获的跟踪

在你的跟踪中，应该能够看到你的计算机发送的一系列ICMP echo请求（对于Windows计算机）或UDP报文段（对于Unix计算机），以及中间路由器返回给你的计算机的ICMP TTL超期的消息；对于Unix机器的情形，相应的问题应该是简单的。在回答下面的问题时尽可能在用来回答问题的实验报告上附一份打印出来的数据包。当你交实验报告时，对输出进行注释，这样就可以清楚地知道你在输出中从哪里得到你的答案的信息。要打印数据包，使用“文件”->“打印到pdf文件”，选择“仅选定数据包”，选择“数据包摘要行”，然后选择需要回答问题的数据包最小详细信息量。

1. 选择计算机发送的第一条ICMP echo请求消息（示例数据中的编号110），并在“数据包详细信息”窗口中展开数据包的IP协议部分



你电脑的IP地址是多少？

1. 在IP数据包头中，上层协议字段的值是多少？
2. IP头中有多少字节？IP数据报的有效负载中有多少字节？解释如何确定有效负载字节数。
3. 此IP数据报是否已分段？解释如何确定数据报是否已被分割。

下一步，通过单击Source column header，根据IP源地址对跟踪的数据包进行排序；单词Source旁边应该出现一个向下的小箭头。如果箭头指向上，请再次单击Source column header。选择计算机发送的第一条ICMP echo请求消息，并在“details of selected packet header”窗口中展开“IP协议”部分。在“listing of captured packets”窗口中，应该在第一个ICMP下面看到所有后续的ICMP消息（可能还有其它在你计算机上运行的协议发送的数据包）。使用向下箭头在你计算机发送的ICMP消息中移动

1. 在你的计算机发送的这一系列ICMP消息中，这个与下个的IP数据报中的哪些字段总在变动？
2. 哪些字段保持不变？哪些字段必须保持不变？哪些字段必须更改？为什么？
3. 描述在IP数据报的标识字段的值中看到的模式

下一步（数据包仍按源地址排序）查找最近（第一跳）路由器发送到你计算机的ICMP TTL超期应答序列。

1. 标识字段和TTL字段中的值各是多少？
2. 对于最近的（第一跳）路由器发送到你计算机的所有ICMP TTL超期应答，这些值是否保持不变？为什么？

**分片**

通过单击time列，回到最初根据time对数据包列表进行排序。

1. 在pingplotter中将数据包大小更改为2000（示例数据中的编号为10271026）后，查找计算机发送的第一条ICMP echo请求消息。该消息是否被分段在多个IP数据报中？如果你的计算机具有以太网接口，则数据包大小为2000将导致分片。[[1]](#footnote-1)
2. 打印出分片IP数据报的第一个分片。IP报头中的哪些信息表示数据报已被分片？IP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数据报有多长？
3. 打印出分片IP数据报的第二个片段。IP头中的哪些信息表明这不是第一个数据报片段？有更多的分片吗？你怎么知道的？
4. 第一个片段和第二个片段之间的IP头中的哪些字段发生了变化？

现在查找在pingplotter中将数据包大小更改为3500（示例数据中的编号为210821072106）之后计算机发送的第一条ICMP echo请求消息。

1. 从原始数据报创建了多少个片段？
2. 在这些片段中，IP头中的哪些字段发生了变化？

1. 这是因为以太网卡最大IP数据包的长度限制为1500字节（40字节的TCP/IP头数据和1460字节的上层协议有效负载）。这个1500字节的值是以太网允许的标准最大长度。 [↑](#footnote-ref-1)