**中国海洋大学**

**计算机网络 课程实验报告**

实验题目: IP数据报分析实验

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】   在本实验中，我们将研究IP协议，重点关注IP数据报：  • 分析traceroute程序执行发送和接收的IP数据报的跟踪。  • 调查IP数据报中的各个字段，并详细研究IP分段。    【实验环境】实验用的软硬件环境（配置）  • Wireshark  • PingPlotter Pro |
| **实验内容** |
| 【实验方案设计】（思路、步骤和方法，）  **实验任务1：**   1.1 思路/步骤/方法  为了生成一系列 IP 数据报，我们将使用 traceroute 程序向不同的目的地发送不同大小的数据报。traceroute 通过首先发送一个或多个带有生存时间 (TTL) 字段设置为 1 的数据报；然后发送一个或多个带有 TTL 字段设置为 2 的数据报到同一个目的地；然后发送一个或多个带有 TTL 字段设置为 3 的数据报到同一个目的地，以此类推，直到目的地真正收到此数据报为止。路由器必须将每个接收到的数据报中的 TTL 减 1，如果 TTL 达到 0，路由器会向来源主机发送 ICMP 消息。由于这种行为，TTL 为 1 的数据报将导致距发送方一次跳跃的路由器，将 ICMP TTL 超出的消息发送回发送方主机；以TTL 为 2 发送的数据报将导致距离为两次跳跃的路由器，将 ICMP 消息发送回发送方主机等等。以这种方式，执行 traceroute 的主机可以通过查看包含ICMP TTL 超出消息的数据报中的来源 IP 地址来获知其自身与目的地之间的路由器的身份。  我的电脑是Windows操作系统，因此需要使用PingPlotter Pro来改变ICMP Echo请求消息的大小。  下面开始实验：  ①首先使用WireShark对本地WLAN的数据报进行捕获。    ②再使用PingPlotter输入我们要跟踪的域名gaia.cs.umass.edu，进行跟踪。  【注意】PingPlotter的默认数据报大小为56字节    ③我们手动将数据报的大小改为2000字节，并继续跟踪。    继续跟踪：    ④我们手动将数据报的大小改为3500字节，并继续跟踪。    继续跟踪：    1.2 结果及分析  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*数据报大小为56\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  1.Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.  选择计算机发送的第一个 ICMP Echo Request 消息，然后在 packet details window 中展开数据包的 Internet 协议部分。您的计算机的 IP 地址是多少？  答：IP地址为10.169.6.114（如下图）      2. Within the IP packet header, what is the value in the upper layer protocol field?  在IP数据报首部中，上层协议字段的值是多少？  答：由下图我们可以知道在IP数据报首部中，上层协议为ICMP协议，其字段值为1。    3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.  IP数据报首部有多少字节？ IP数据报的有效负载中有多少字节？说明如何确定有效负载的字节数。  答：①IP数据报首部有20个字节（红框）。  ②IP数据报的有效负载为36个字节。  ③我们只需要将该IP数据报的总长度56字节（绿框）减去该IP数据包的首部长度20字节，即可得出该IP数据报的有效负载36字节。（IP数据报总长度 = IP数据报首部长度 + IP数据报的有效负载）    4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.  此IP数据报是否已被分段？解释一下你是如何确定数据报是否已被分段。  答：此IP数据报未被分段。这里给出两种解释：  解释①：在数据报被分段后，经过同一个数据报分段操作之后的数据报中它们的标识字段（这里为Identification）都是相同的。因此我们只需要对比下一个从本地发出去的IP数据报的标识字段的值就可以判断这个IP数据报是否被分段。在下面两张图的对比中我们可以看出这两个IP数据报的标识字段不同，因此这两个IP数据报不是经过分段而来的，而是两个独立的IP数据报。      解释②：在数据报被分段后，经过同一个数据报分段操作之后的数据报中它们的片偏移字段会依次增加，第一个数据报的片偏移字段一定为0，后续的数据报中的片偏移字段一定不为0，且呈现递增趋势。我们截取了从本地发送的第一个与第二个IP数据报，查看他们的片偏移字段，我们发现都为0，因此可以断定IP数据报未被分片。如下图：      5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?  在您的计算器发送的这一系列 ICMP 消息中，IP 数据报中的哪些字段一直在改变？  答：在下面我们对比了三个ICMP消息的所有字段，发现IP数据报中的标识字段(Identification)、TTL(Time to live)、首部校验和字段(Header Checksum)一直在改变。        6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?  哪些字段保持不变？哪个字段必须保持不变？哪些字段必须更改？为什么？  答：**保持不变的字段有：**  ①拥塞通告字段（Explicit Congestion Notification）  ②总长度字段（Total Length）  ③片偏移字段（Fragment Offset）  ④源地址字段（Source Address）  ⑤目的地址字段（Destination Address）  **必须保持不变的字段有：**  ①版本字段（Version）。  原因：要使通信双方的版本要一致，因此这个字段从始至终都不能改变。  ②首部长度字段（Header Length）  原因：因为首部长度说明这个数据报首部有多少个字节，对于相同服务类型的数据报，其首部所占字节数应该相同。  ③区分服务字段（Differentiated Services Codepoint）  原因：在一次通信中，使用到的服务应该是相同的。  **必须更改的字段有：**  ①标识字段（Identification）  原因：标识字段需要用来标识同一个报文的所有分片，这里IP数据报并未分片，因此必须发生改变。  ②存活时间（Time to live）  原因：因为要避免报文在互联网中永远存在。实现为跳数计数器，报文经过的每个路由器都将此字段减1，当此字段等于0时，报文不再向下一跳传送并被丢弃。  ③首部检验和（Header Checksum）  原因：每一个IP数据报在首部字段中必然会有不同的字段出现，因此每一个IP数据报都有相对于自己的首部检验和字段。  下图中，红框内表示必须保持不变的字段；绿框内表示保持不变的字段；紫框内表示必须改变的字段。    7. Describe the pattern you see in the values in the Identification field of the IP datagram.  **描述你在IP数据报中看到的标识字段的值。**  答：IP数据报的标识字段主要是用来唯一标识一个报文段，或者区分由一个报文所分的分片，对于不同的报文，这个值是必然不相同的。这里我给出两个IP数据报的例子，第一个IP数据报的标识字段为0xd5bc；第二个IP数据报的标识字段为0xd5bd。因此这是两个不同的IP数据报，且未分片。      8. What is the value in the Identification field and the TTL field?  ID字段和TTL字段的值是多少？  答：此时查询的是第一跳路由器发送到本主机的回复信息。  ID为542，TTL为255。如下图：    9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?  对于最近（第一跳）路由器发送到您的计算器的所有ICMP TTL超出的回复，哪些值是否保持不变？为什么？  答：其中ID字段（即标识字段）的值发生了变化，而TTL字段的值未发生变化。  因为这是两个不同的IP数据报，因此他们的ID字段必然不同；而ICMP回显应答中TTL的值保持不变，是因为在ICMP回显应答中的TTL字段可以反应操作系统的种类，同一种操作系统的ICMP回显应答中的TTL字段必然是相同的。  如下两图：      \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*数据报大小为2000\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  【说明】因为手误关闭了之前的抓包结果，因此从第10个小问开始使用了新的抓包数据，即数据报的最大长度改为2000之后。  10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?  在将pingplotter中的数据包大小更改为2000后，查找计算机发送的第一个ICMP Echo Request消息。该消息是否已碎片化为多个IP数据报？打印出分段 IP 数据报的第一个片段。IP 报头中的哪些信息表明数据报已分段？IP 标头中的哪些信息指示这是第一个分段还是后一个分段？此 IP 数据报有多长？  答：①已经被分片，分为两个IP数据报。如下图：    ②IP首部中的MF字段表明数据报已分段。  ③结合课上所学：MF为1表明后续还有分段；MF为0说明已经是最后一个分段，后续再无分段。并且片偏移为0，说明是第一个分段。  ④该数据报的长度为1500字节，其中数据部分1480字节，首部部分20字节。  同时给出分段IP数据报的第一个片段，如下图：    11. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?  打印出分段IP数据报的第二个分段。IP 报头中的哪些信息表明这不是第一个数据报片段？是否含有更多片段？你怎么知道？  答：①IP数据包首部中的片偏移字段（Fragment Offset）不为0可以说明这不是第一个数据报片段，因为第一个数据报片段的片偏移应当为0。  ②不含有更多片段了。原因：该数据报首部中的More Fragment字段为not set，说明这个数据报后面没有更多数据报了，因此这是最后一个数据报。  如下图：    12. What fields change in the IP header between the first and second fragment?  第一个片段和第二个片段之间的 IP 标头中有哪些字段发生变化？  答：发生变化的字段有：①数据报总长度字段（Total Length）  ②标志字段（Flags）  ③片偏移字段（Fragment Offset）      \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*数据报大小为3500\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  13. How many fragments were created from the original datagram?  **从原始数据报创建了多少个片段？**  答：创建了3个分段，即原先的数据报被分为了3个分段。如下图：    14. What fields change in the IP header among the fragments?  片段中IP首部中的哪些字段发生了变化？  答：我们拿出三个分段的首部进行比较发现IP首部中发生变化的字段有：  ①数据报总长度字段（Total Length）  ②片偏移字段（Fragment Offset）  ③首部校验和字段（Header Checksum）  下图进行比较： |
| **小结** |
| 在本实验中，我们研究了IP协议，并对IP数据报进行了详细的分析。同时，我们使用PingPlotter可以对数据报的大小进行修改的特性，对片偏移字段也进行了深入研究，巩固复习了课本上的相关内容。  在IP数据报的简单分析方面，我们做了相关分析实验。首先我们分析了IP数据报首部长度字段与IP数据报总长度字段，并对这两种字段的相关计算做了巩固复习。其次我们判断了数据报是否分段的问题，我们既可以通过标识字段对分段问题进行分析，也可以通过片偏移字段对连续的数据报进行分段分析。我们还分析了再一次通信中，首部哪些字段会发生变化，哪些字段不会发生变化，哪些字段一定不会发生变化。  在分段分析方面，我们将重点放在了判断分段的MF字段以及分段之后的片偏移的计算上，MF字段可以有效地帮助我们对一个IP数据报地分段情况进行分析。  通过这次的实验，掌握了IP协议分析的方法，网络分析工具可以帮助我们更加直观地看见数据报的具体信息，也可以筛选出满足我们需要的数据报，让我加深了对IP协议的理解。 |