|  |
| --- |
| **实验目的：**  研究 IP datagram 中的各个字段，并详细研究 IP fragmentation 的方法  **实验结果：**  1、选择发送的第一个 ICMP Echo Request 消息，然后在 packet details window 中展开数据包的 Internet 协议部分。您的计算器的 IP 地址是多少？  ip地址：192.168.1.102  屏幕截图 2023-04-28 171251  **2、在 IP header 中，上层协议字段的值是多少？**  上层协议为ICMP,上层协议字段的值是1，如下图所示：  屏幕截图 2023-04-28 171416  **3、IP header 有多少 bytes？ IP datagram 的有效负载中有多少 bytes？ 说明如何确定 payload bytes 的数。**  **20types,数据报总长度=ip数据包头部长度+数据长度（有效负载）**  **64=84-20**  **屏幕截图 2023-04-28 171618**  **方法二：直接看报文最底部**  **方法二**  4、此 IP 数据报是否已被分段(fragmented)？  屏幕截图 2023-04-28 172739  More fragments为NOT SET说明未分段   1. **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？**   **标识号Identification、校验和Header checksum、存活时间TTL 一直改变**  **屏幕截图 2023-04-28 173348**  6、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  ****保持不变：****  **显式拥塞通告（ Explicit Congestion Notification，ECN）：允许在不丢弃报文的同时通知对方网络拥塞的发生。**  **全长（Total Length）：占 16 位字段，定义了报文总长，包含首部和数据，单位为字节。这个字段的最小值是 20（0 字节数据），最大值是65535。**  **标识符（Identification）：占16位，这个字段主要被用来唯一地标识一个报文的所有分片，因为分片不一定按序到达，所以在重组时需要知道分片所属的报文。**  **分片偏移 （Fragment Offset）：这个13位字段指明了每个分片相对于原始报文开头的偏移量，以8字节作单位。**  **源地址：报文的发送端；**  **目的地址：报文的接收端；**  **选项：附加的首部字段可能跟在目的地址之后；**  ****必须保持不变：****  **版本（Version）：通信双方使用的版本必须一致，对于 IPv4 字段的值是4；**  **首部长度（Internet Header Length， IHL）：首部长度说明首部有多少 32 位字（4字节）。由于IPv4首部可能包含数目不定的选项，这个字段也用来确定数据的偏移量；**  **区分服务（Differentiated Services，DS）：占 6 bit，只有在使用区分服务时，这个字段才起作用，在一般的情况下都不使用这个字段；**  ****必须更改：****  **标识符（Identification）：占 16 位，主要被用来唯一地标识一个报文的所有分片；**  **存活时间（Time To Live，TTL）：占 8 位，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，最大值是255。这是traceroute的核心原理；**  **首部检验和 （Header Checksum）：占 16 位，检验和字段只对首部查错，在每一跳，路由器都要重新计算出的首部检验和并与此字段进行比对，如果不一致，此报文将会被丢弃；**  **数据：保持不变是这一次的traceroute保持不变，下一次就改变了**   1. **描述您在 IP datagram 的 Identification field 中的值中所看到的？**   **屏幕截图 2023-04-28 174601**  **13130用来唯一标识一个报文，主要被用来唯一地标识**一个报文的所有分片**，对于不同的报文就需要改变这个值，使得报文可以唯一确定。**   1. **ID 字段和 TTL 字段的值是多少？**   **ID:13130 TTL:13**  **屏幕截图 2023-04-28 174601**   1. **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，这些值是否保持不变？为什么？**   **标识字段会更改，因为标识字段是唯一值,TTL字段保持不变，因为第一跳路由器的TTL始终相同**   1. 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？   是的，如下图所示，已碎片化为三个 IP 数据报 363 364 365  屏幕截图 2023-05-05 163302   1. 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 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？   Flag说明已经被分段，根据Offset得到偏移量为0说明是第一个片段，  total length为1500  屏幕截图 2023-05-05 165705   1. 打印出碎片 IP 数据报的第二个片段。 IP 标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？ 你是如何知道的？   Flag中的Offset偏移量为1480说明不是第一个字段，  屏幕截图 2023-05-05 163916  从Echo request的信息中可以看出有三个分段  屏幕截图 2023-05-05 163302  **13、在第一个和第二个片段中，IP 标头中哪些字段发生了变化？**  Flag字段和检验和发生变化  对比如下；  屏幕截图 2023-05-05 163553 屏幕截图 2023-05-05 163916  **14、从原始数据报创建了多少个片段？**  **三个如下图所示：**  屏幕截图 2023-05-05 163302  **15、片段中 IP 标头中的哪些字段发生了变化？**  **标志Flag 检验和headerchecksum 总长度totallength**  ****问题及收获：****  **学会捕获ip数据包，学会分析ip数据包中各个字段和含义，学会判断报文是否被分段。** |

|  |
| --- |
| 实验内容： |