**中国海洋大学**

**计算机网络 课程实验报告**

实验题目: ICMP实验

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】   在本实验中，我们将探讨 ICMP 协议的几个方面：  • Ping 程序生成的 ICMP 消息;  • Traceroute 程序生成的 ICMP 消息;  • ICMP 消息的格式和内容。  【实验环境】实验用的软硬件环境（配置）  • Wireshark  • Best Trace |
| **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  执行ping -n 10 www.ntu.edu.sg命令，向www.ntu.edu.sg发送10个数据报并接收应答从而检测网络连通性与速度。结果如下：    在Wireshark中只捕获协议为ICMP的数据包，ping程序结束后同时终止Wireshark的捕获，结果如下：    1.2 结果及分析  1. Q: What is the IP address of your host? What is the IP address of the destination host?  Q: 主机的 IP 地址是什么？目标主机的 IP 地址是什么？  A: 我的主机IP地址为：10.149.1.21 目标主机IP地址为：104.16.4.14    2. Q: Why is it that an ICMP packet does not have source and destination port numbers?  Q: 为什么ICMP报文没有源端口号和目的端口号？  A: 因为ICMP报文实质上是一个IP数据报，而不是TCP或UDP数据报，因此不需要源端口与目的端口。  3. Q: Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?  Q: 检查主机发送的 ping 请求数据包之一。ICMP 类型和代码是什么？此 ICMP 数据包还具有哪些其他字段？校验和、序列号和标识符字段有多少个字节？  A: ICMP类型为8，代表ICMP请求；代码为0。  此 ICMP 数据包还具有Checksum（校验和字段）、Checksum Status（校验和状态字段）、Identifier(BE)（大端标识符字段）、Identifier(LE)（小端标识符字段）、Sequence Number(BE)（大端序列号字段）、Sequence Number(LE)（小端序列号字段）。其中：  校验和字段（Checksum）：2字节  序列号字段（Seuence Number）：2字节  标识符字段（Identifier）：2字节    4. Q: Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?  Q: 检查相应的 ping 应答数据包。ICMP 类型和代码是什么？此 ICMP 数据包还具有哪些其他字段？校验和、序列号和标识符字段有多少个字节？    **实验任务2：**   2.1 思路/步骤/方法  执行tracert [www.inria.fr](http://www.inria.fr)命令对[www.inria.fr](http://www.inria.fr)进行路由跟踪，本次测试有20个跃点跟踪。跟踪结果如下：    同样在Wireshark中只捕获ICMP协议数据包，在tracert程序终止时，停止在Wireshark中的捕获。结果如下：            2.2 结果及分析  5. Q: What is the IP address of your host? What is the IP address of the target destination host?  Q: 主机的 IP 地址是什么？目标主机的 IP 地址是什么？  A: 主机IP地址为10.149.1.21 目标主机IP地址为128.93.62.83    6. Q: If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?  Q: 如果 ICMP 发送的是 UDP 数据包（如在 Unix/Linux 中），探测数据包的 IP 协议编号是否仍为 01？如果不是，那会是什么？  A: ICMP本身是一个基于IP协议的协议，用于在IP网络中传递控制消息。它本身并不发送UDP数据包，而是发送ICMP数据包。在Unix/Linux系统中，ICMP消息是作为IP数据报进行传输的，IP协议编号为01。  UDP是另一种基于IP的传输层协议，与ICMP是两种不同的协议。用于传输用户数据，而非用于传输控制消息。因此，如果ICMP发送的是UDP数据包，那么它不是纯粹的ICMP消息，而是一个UDP数据包。在这种情况下，IP协议编号不是01。  7. Q: Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?  Q: 检查屏幕截图中的 ICMP 回显数据包。这与本练习前半部分的 ICMP ping 查询数据包不同吗？如果是，怎么会这样？  A: 与ICMP ping 查询数据包不同。截图对比如下：          ICMP ping查询数据包是发送到目标主机以检查其可达性，并且用于诊断网络连接。目的是检查主机是否可访问以及确认网络是否可用。这些数据包带有特定类型、代码与序列号，以及由发送主机计算得出的校验和。  ICMP回显数据包是目标主机对发送到它的ICMP ping查询数据包做出的响应。它携带有关原始查询的数据，并且用于确认通信双方之间的连通性。回显数据包包含与原始查询相同的标识符和序列号，使发送方可以确定这是对本次查询的响应。  8. Q: Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?  Q: 检查屏幕截图中的 ICMP 错误数据包。它比 ICMP 回显数据包具有更多的字段。这些字段包含哪些内容？      A：通过屏幕截图对比可以看出，这个数据包含：类型(Type)字段（表示特定类型的错误，不可达、超时…）、代码(Code)字段（更为具体的错误信息）、校验和(Checksum)字段（校验ICMP消息的完整性，确保传输过程中没有变化与损坏）、不可用(Unused)字段（有些字段被标记为“未使用”，未来预留）。  9. Q: Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?  Q: 检查源主机接收的最后三个 ICMP 数据包。这些数据包与ICMP错误数据包有何不同？为什么它们不同？  A: 不同：  ①类型字段：ICMP错误数据包和普通的ICMP数据包在类型字段上有不同的值。ICMP错误数据包的类型字段指示了具体的错误类型。  ②代码字段：ICMP错误数据包中的代码字段提供了更具体的错误信息，明确错误的具体类型和原因。  ③可变信息：ICMP错误数据包通常会携带与原始IP报文相关的一些字段，提供关于导致错误的更多细节。而普通的ICMP数据包包含用于标识和跟踪消息的标识符和序列号数据字段。  原因如下：  最后一组 3 个数据报可以到达目的主机，因为被目的主机接收，目的主机不会丢弃，而是收到的这个探测的数据报并进行了响应。    10. Q: Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link？  Q: 在tracert测量中，是否存在延迟明显长于其他链接的链接？参考图 4 中的屏幕截图，是否有延迟明显长于其他链接的链接？根据路由器名称，你能猜出这个链接末尾两个路由器的位置吗？  A: 本次实验在tracert测量中，存在延迟明显长于其他链接的链接，即第11个请求到第12个请求。我们使用可视化路由跟踪工具BestTrace来进行可视化路由跟踪。    Best Trace跟踪结果如下：    在图中发现当IP地址变为62.40.125.101时延迟出现了剧增，正好对应tracert程序执行过程中的第11个请求到第12个请求。  出现这一延迟剧增的原因是此次转发的起点为***中国北京***，终点为***英国伦敦***，IP所在地跨度大，因此出现较大延迟。 |
| **小结** |
| 本次实验使用ping程序向指定域名发送10个数据报并接收应答从而检测网络连通性与速度，使用tracert程序向指定域名发送数据包并进行路由跟踪。了解了ping程序与tracert程序的执行过程。  ping 程序允许我们验证某主机是否存在，通过将数据包发送到目标IP地址，如果目标主机在线则目标主机中的ping程序将会发送响应数据包进行响应。  tracert 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。  实验中复习巩固了ICMP协议，ICMP报文在主机和路由器之间起到沟通网络层信息的作用。差错报告允许主机或路由器报告查错情况和提交有关异常情况的报告。例如主机是否可达、路由是否可用等网络消息，这些消息对于数据的传递起着重要的作用。ICMP报文作为IP有效载荷承载的，因此虽然 ICMP是IP的一部分，但在体系结构上 ICMP 位于 IP 之上。当主机接收到指明上层协议为ICMP的IP数据报时，该数据报分解的内容应当交给ICMP。  同时再一次熟悉了ICMP的报文格式，通过Wireshark抓包的结果我们可以查看到ICMP报文所含有的字段结构：  类型字段（Type）  代码字段（Code）  校验和字段（Checksum）  校验和状态字段（Checksum Status）  大端序列号字段（Seuence Number(BE)）  小端序列号字段（Seuence Number(LE)）  大端标识符字段（Identifier(BE)）  小端标识符字段（Identifier(LE)）  ICMP ping查询数据包是发送到目标主机以检查其可达性，并且用于诊断网络连接。目的是检查主机是否可访问以及确认网络是否可用。这些数据包带有特定类型、代码与序列号，以及由发送主机计算得出的校验和。  ICMP回显数据包是目标主机对发送到它的ICMP ping查询数据包做出的响应。它携带有关原始查询的数据，并且用于确认通信双方之间的连通性。回显数据包包含与原始查询相同的标识符和序列号，使发送方可以确定这是对本次查询的响应。  同时使用了Best Trace这款路由跟踪工具，使报文转发可视化，能够更加清晰地理解延迟剧增的原因。 |