实验4 网络诊断工具 Traceroute

实验背景：网络层错误处理

网络层的错误处理难题：

- 网络层的错误报告发送给哪个模块？

网络层的端到端错误报告：

- ICMP协议

ICMP能干什么？

- 路由器缓冲区满/快满了
- 目标不存在
- 参数问题不能识别
- 跳数超长（TTL到零）

实验背景：设计机会

错误管理机制带来的设计机会

利用已有设计	获得额外收益
询问包	进行主机存活判断
跳数超限错误	探测途径点的地址（traceroute）
询问包的时延	进行网络拥塞判断
询问包的大小	发现MTU

实验背景：Ping与Traceroute工具

1. Ping用于探测网络上主机的可达性。
2. Ping是Mike Muuss在1983年于美国弹道研究实验室工作时在BSD4.3上编写的。"ping"即声呐定位的拟声词，也有人说它是“Packet InterNet Groper”的首字母缩写。第一版作为公共域软件(PD)发布，之后则以BSD协议发布。在其他平台上的Ping工具，有的是作者以MIT协议、GPL协议发布的，也有商用软件。
3. 安全问题：早期有人使用畸形或过大的ICMP echo request包来进行网络攻击，也有使用它进行DDoS，致使有些服务器关闭了ICMP echo request包的回应服务。

实验背景：Ping与Traceroute工具

1. Traceroute是在类UNIX系统上广泛应用的网络诊断工具，用于确定数据包在网络中传输的路径和延迟。Windows上通常会提供类似的Tracert工具。
2. 最早的traceroute程序是由Van Jacobson于1987年在LBL工作时编写。据Muuss声称使用了他开发ping时为了使用原始ICMP套接字编写的内核ICMP支持。
3. 在UNIX上的实现通常发送udp数据包，在Windows上通常发送icmp数据包，在MacOS上有时会发送TCP SYN数据包。
4. Van Jacobson设计了TCP/IP拥塞控制的Jacobson/Karels算法，目前在UCLA从事NDN方面的研究

实验目的

1. 学习Ping和Traceroute工具的使用，能够在网络开发和维护中熟练使用该工具获取网络状态和进行错误排查。

2. 巩固课堂学习的因特网分层设计实现知识，理解因特网的分组转发网络的特性，通过分析互联网数据包因转发而产生的时延，加深理解尽力而为的因特网设计思想。

3. 通过分析ICMP协议，学习在分层设计中进行跨层通信的设计实现方法，思考因特网网络层在错误处理上的折中设计和处理技巧。

4. 通过Traceroute工具基于错误处理包进行路径探测功能的设计，体会在实践中体会设计方案在解决问题的同时是如何带来新的设计机会的。

Ping与Traceroute的工作原理

- RFC 1122规定，主机都应以echo reply回应ICMP的echo request包。
- IPv4数据包中具有TTL字段，该字段发出时进行初始化（如128或64），路由器转发时会将TTL减1，当TTL为0时，路由器将丢弃数据包并发送一个ICMP时间超时消息给源主机。该机制可以减轻网络路由回路的影响，并可及时提醒沿途路由器回路的存在。
- Ping使用echo request包判断目标主机的可达性。
- Traceroute可能向目标主机发送任何协议类型的数据包，每个数据包具有不同的TTL值。通过这种方式，Traceroute可以逐个路由器地确定数据包的传输路径，并显示每个路由器的IP地址、延迟和跃点数（跳数）。通过收到的数据，可以诊断网络连接问题，找出网络中存在的瓶颈和故障点，查找网络故障、分析网络延迟等。

实验环境

1. 软件环境：Linux操作系统，多核处理器

- 用户名: stu01-stu130　　服务器: 10.140.32.159
- 端
- 用

如果报错：　WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

执行：　ssh-keygen -R "[10.140.32.159]:分配的服务器端口号"

清除原有信息后即可成功连接

2. 要求：

① 请大家拿到后先修改登录口令，不能使用其他人的账号登录，也不得替他人登录练习，严禁使用账号进行与学习无关或攻击他人及恶意消耗系统资源等行为，一旦发现，按违规处理，后果严重；

② 大家认真进行练习，练习量将作为实验课达标的依据之一（不评优劣，达到基本练习量即可）

实验安排

知识介绍与环境配置		15分钟
实验内容 1		25分钟
实验内容 2		30分钟
实验内容 3		25分钟
布置课下实验		5分钟

实验内容1 Ping应用

原理

- 通过使用互联网控制消息协议（ICMP）向主机发送echo request消息。支持ICMP并接受该消息的主机将发送echo reply消息给发送者。

操作

1. 使用man命令简单了解ping命令的作用，认真阅读descirption的内容，并用不超过200字进行简要概括。
2. 使用ping，对www.sdu.edu.cn发送10个长度为56字节的数据包。
3. 使用ping，对www.ouc.edu.cn发送长度为56字节的50个数据包。

- 记录结果。（注意命令参数）

实验内容1 Ping应用

问题：

1. 用不超过200字简要概括ping命令；
2. 说明实验现象背后的原因；
3. 通过查询资料，画出所使用的ICMP数据包的结构。

实验内容2 Traceroute应用

操作

1. 使用man命令简单了解traceroute命令的作用。
2. 使用traceroute www.baidu.com,尝试确定并说明从源计算机到www.baidu.com的路径，并思考输出结果每个字段的意义。
3. 记录输出结果。

实验内容2 Traceroute应用

问题

4. 用不超过200字简要概括traceroute命令；

5. 确定并说明从源计算机到 www.baidu.com的路径；

6. 说明输出结果每个字段的意义。

实验内容3 traceroute探索

操作

1. 在命令提示符下，输入:traceroute 18.31.0.200
   - 描述观察到的输出有什么特殊性，思考为什么traceroute会给出这样的输出。查阅traceroute手册获得帮助。
2. 使用traceroute分析从源地址到www.baidu.com和到cn.bing.com的网络路径差异。

实验内容3 traceroute探索

问题

7. 解释traceroute 18.31.0.200的输出。
8. 说明从源地址到www.baidu.com和到cn.bing.com的网络路径差异。
9. 如果在IPv6上实现路径探测，应该使用包头的哪个字段?

课后实验内容及思考

拓展学习

- Traceroute在网络故障排查中有哪些应用场景?
- 在Traceroute中如何通过修改参数来优化网络诊断的效果?
- Traceroute交换源节点/目的节点，在同一时刻探测到的两条路径应该是相同的吗?