计算机网络课程设计

实验4： ICMP协议分析

1.实验目标

本实验的目的是使用Wireshark软件捕获Ping和Traceroute命令会话过程中的数据包，并通过分析数据包来了解ICMP协议的原理和应用，以及Ping和Traceroute的设计原理。

2.实验平台

Windows 11（任何平台均可以完成）；

3.实验工具

Wireshark;

实验4： ICMP协议分析

4.实验步骤

- 第一步：Ping数据包捕获及原理分析；
  - 1）打开Wireshark软件，启动分组捕获器；
  - 2）在命令行中输入“ping -n 5 www.scu.edu.cn”（如果想了解ping命令的参数说明，可以在命令行中输入“ping /?”，其中，-n 参数是用来指定要发送的回显请求数）后回车；
  - 3）停止分组捕获；
  - 4）在过滤器中输入“icmp”，只显示与ICMP相关的数据包，如图7-11所示。从图中可以看到，共有10个ICMP数据包，这是因为实验中设置了ping程序发送5次请求，每次请求都会收到一个ICMP应答数据包，所以总共有10个数据包。在Info域中，可以区分哪些是请求包，哪些是应答包。

实验4： ICMP协议分析

- 根据捕获的数据报回答问题，实验报告中必须附抓包的截图：
  - 1）Ping命令利用了ICMP的哪种类型报文，从哪里可以看出来?
  - 2）Ping包发送的ICMP报文的数据部分内容是什么?
  - 3）第一个Ping报返回的准确时间是多少?
  - 4）IP数据报头部已经有checksum字段，为什么ICMP还有checksum字段?

实验4： ICMP协议分析

4.实验步骤

- 第二步：Traceroute数据包捕获及原理分析。
  - 1）打开Wireshark，启动Wireshark分组俘获器；
  - 2）在命令行中输入“tracert /d www.scu.edu.cn”，回车，结果如7-12 所示。
  - 3）停止分组俘获；

实验4： ICMP协议分析

- 根据捕获的数据报回答问题，实验报告中必须附抓包的截图：

1）Traceroute应用发送的是ICMP的什么类型数据报?

2）Traceroute发送的回显请求数据包和ping发送的数据包数据部分有什么差异?

3）发送的报文，出现了什么错误，错误原因是什么?

4）第一个TTL超时报文时由谁发出的?

5）在Traceroute的过程中，发送方一共发送了多少个不同TTL的报文，相同的TTL算一个?

6）这五种不同TTL的数据包TTL字段的特点是什么?

7）Traceroute到达目的地的判断方法是什么?

8）从捕获的数据包中分析，源主机收到了哪些不同IP发送的ICMP报文?