上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

实验报告

LAB REPORT

数据通信

Winsock ex6

姓 名: 裘炜程

学 号: 516030910287

班 级: F1603602

一、实验要求

Write a program to test the reachability of an Internet interface identified by an IP address or name. (The basic function of “ping” command)

Hints: Send an ICMP “echo request” to the destination, an ICMP “echo reply” will be sent back if the destination is reachable. (refer to RFC 792 for more information about ICMP)

1. Create a raw socket: socktype=SOCK_RAW, protocol=IPPROTO_ICMP;
2. Construct an ICMP message;
3. Use “sendto” to send the ICMP message to the remote machine;
4. Use “recvfrom” to receive any response.

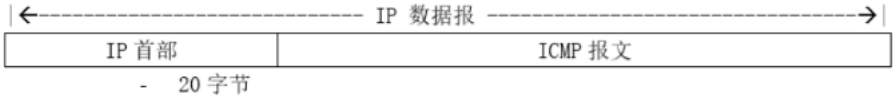
二、实验原理

1、ICMP 协议及 Ping 的原理

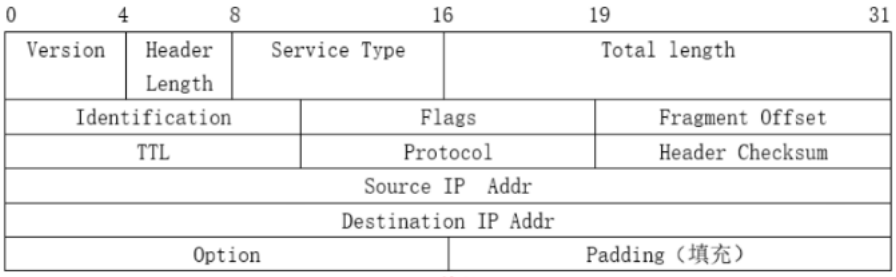
ping 是一种计算机网络工具,用来测试数据包能否透过 IP 协议到达特定主机。ping 的运作原理是向目标主机传出一个 ICMP echo@要求数据包，并等待接收 echo 回应数据包。程序会按时间和成功响应的次数估算丢失数据包率(丢包率)和数据包往返时间(网络时延，Round-trip delay time)。

互联网控制消息协议（英语：Internet Control Message Protocol，缩写：ICMP）是互联网协议族的核心协议之一。它用于 TCP/IP 网络中发送控制消息，提供可能发生在通信环境中的各种问题反馈,通过这些信息,使管理者可以对所发生的问题作出诊断,然后采取适当的措施解决。一个应用就是 Ping,Ping 就是主动请求,获取到主动应答。但是 Ping 是在原生的 ICMP 中添加了自定义格式区域。例如 Ping 中放了发送的请求时间，以此计算出路程。所以，其实在 Ping 的报文中会加入序号，以用来区分数据包，从而提高计算时间或者路程的准确性。

2、ICMP 包和 IP 包格式



ICMP 封装在 IP 数据报内部



IP 首部

ICMP 报文

在程序中，依照 ICMP 报文中的内容要求，设置 type、code、checksum、ID、sequence 构成头部。Ping 时返回的 ICMP 包会显示 TTL，因此需要查到 TTL，即第 9 个字节。此外 version 即 IPv4 还是 IPv6 从第一个字节前半段读出，但是我的程序只能接收 IPv4 的包。关于包的填充，通过抓包一次正常的 Ping，发现 ICMP 包应填充 "abcdefghijklmnopqrstuvwabcdefghi"，共 32bit 数据，这在计算校验和之前就填充上去。

3、计算校验和

1) 将校验和字段置为 0,然后将 IP 包头按 16 比特分成多个。

2) 对各个单元采用反码加法运算(即高位溢出位会加到低位,通常的补码运算是直接丢掉溢出的高位),将得到的和的反码填入校验和字段。

3) 当接收到 IP 对其进行检测：对各个单元采用反码加法运算，检查得到的和是否符合是全 1(有的实现可能对得到的和会取反码，然后判断最终值是不是全 0)

4、程序基本步骤

1) 创建一个 ICMP 头部结构体，以便对每个包的头部进行分析，之后进入 main 函数；

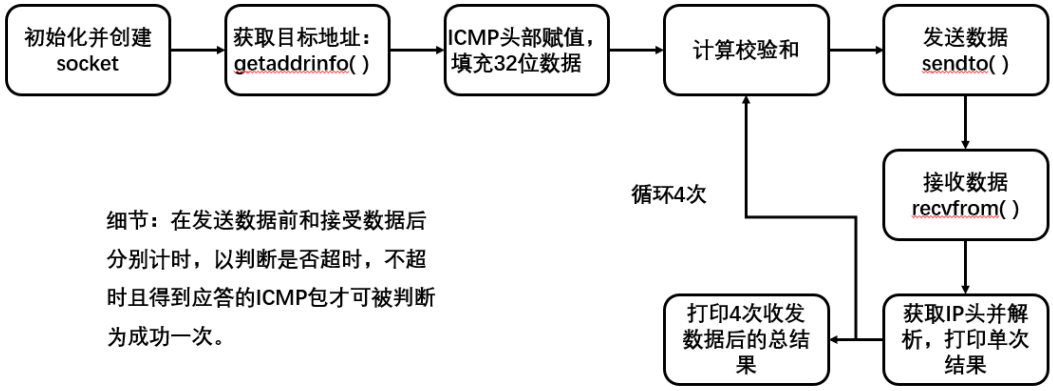
2) 创建 socket，从输入的参数中得到域名或 IP 地址进行得知目的端 IP，使用 getaddrinfo( )函数；

3) 构造 ICMP 包并填充数据；

4) 开始循环，处理每一次的发送和接受消息；

5) 计算校验和，填充后发送数据；

6) 接受数据，获得 IP 信息，并根据回复的 ICMP 头部判断是否 Ping 成功，并将结果输出。



三、实验结果

1、myping 和 ping

```
C:\windows\system32\cmd.exe

C:\Users\hp>cd C:\Users\hp\Desktop\数据通信\winsock_ex6\myping\Debug

C:\Users\hp\Desktop\数据通信\winsock_ex6\myping\Debug>myping www.baidu.com

正在 Ping www.baidu.com 具有 32 字节的数据:
来自 115.239.211.112 的回复: 字节=32 时间=15ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=15ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=16ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=15ms TTL=54

www.baidu.com 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 15ms, 最长 = 16ms, 平均 = 15ms

C:\Users\hp\Desktop\数据通信\winsock_ex6\myping\Debug>ping www.baidu.com

正在 Ping www.a.shifen.com [115.239.211.112] 具有 32 字节的数据:
来自 115.239.211.112 的回复: 字节=32 时间=14ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=14ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=14ms TTL=54
来自 115.239.211.112 的回复: 字节=32 时间=14ms TTL=54

115.239.211.112 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 14ms, 最长 = 14ms, 平均 = 14ms
```

四、实验思考

这次实验中，我学习了ping的原理和ICMP包的格式和内容，对计算校验和等细节有了更深的理解，也学到了IP包中的格式处理。现在myping还有一个问题，就是无法处理ping不到的情况，因为是判断sendto和recvfrom之间的时间，但一旦没有收到消息，就会阻塞住。正确的方法可能是不断在每个毫秒判断是否接受到信息，但我不知道怎么和系统的计时函数结合起来。