华中科技大学网络空间安全学院

《计算机通信与网络》

实验指导手册

（Socket 编程实验分册）

华中科技大学网络空间安全学院

二零二零年十一月

目　录

第一章 实验目标和内容

1.1 实验目的

- ✧ 了解应用层和运输层的基本功能和作用
- ✧ 了解掌握基本的可靠数据传输的原理和机制。
- ✧ 掌握 SOCKET 编程的基本方法。

1.2 实验环境

- ✧ 操作系统：Windows
- ✧ 语言：C
- ✧ 编程开发环境：Visual Studio 2008-2017 皆可

1.3 实验要求

- ✧ 必须基于 Socket 编程，不能直接借用任何现成的组件、封装的库等。
- ✧ 提交实验设计报告和源代码；实验设计报告必须包括程序流程图，源代码必须加详细注释。
- ✧ 实验设计报告需提交纸质档和电子档，源代码、编译说明需提交电子档。
- ✧ 基于自己的实验设计报告，通过实验课的上机试验，将源代码编译成功，运行演示给实验指导教师检查。

1.4 实验内容

完成一个 TFTP 客户端程序。TFTP 是一种简单的文件传输协议。目标是在 UDP 之上上建立一个类似于 FTP 的但仅支持文件上传和下载功能的传输协议

题目：编写实现一个 TFTP 客户端程序，要求如下：

- ✧ 严格按照 TFTP 协议与标准 TFTP 服务器通信；
- ✧ 能够实现两种不同的传输模式 netascii 和 octet；
- ✧ 能够将文件上传到 TFTP 服务器；
- ✧ 能够从 TFTP 服务器下载指定文件；
- ✧ 能够向用户展现文件操作的结果：文件传输成功/传输失败；
- ✧ 针对传输失败的文件，能够提示失败的具体原因；
- ✧ 能够显示文件上传与下载的吞吐量；
- ✧ 能够记录日志，对于用户操作、传输成功，传输失败，超时重传等行为记录日志；
- ✧ 人机交互友好（图形界面/命令行界面均可）；

说明：额外功能的实现，将视具体情况予以一定加分。

第二章　TFTP 协议

2.1 TFTP 协议简介

TFTP（Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务，端口号为 69。

TFTP 通常基于 UDP 协议而实现，但是我们也不能确定有些 TFTP 协议是基于其它传输协议完成的。TFTP 协议的设计目的主要是为了进行小文件传输，因此它不具备通常的 FTP 的许多功能，例如，它只能从文件服务器上获得或写入文件，不能列出目录，不进行认证。

TFTP 代码所占的内存较小，这对于较小的计算机或者某些特殊用途的设备来说是很重要的，这些设备不需要硬盘，只需要固化了 TFTP、UDP 和 IP 的小容量只读存储器即可。因此，随着嵌入式设备在网络设备中所占的比例的不断提升，TFTP 协议被越来越广泛的使用。

2.2 TFTP 的包格式

TFTP 共定义了五种类型的包，包的类型由数据包前两个字节确定，我们称之为 Opcode（操作码）字段。这五种类型的数据包分别是：

- 读文件请求包：Read request，简写为 RRQ，对应 Opcode 字段值为 1
- 写文件请求包：Write requst，简写为 WRQ，对应 Opcode 字段值为 2
- 文件数据包：Data，简写为 DATA，对应 Opcode 字段值为 3
- 回应包：Acknowledgement，简写为 ACK，对应 Opcode 字段值为 4
- 错误信息包：Error，简写为 ERROR，对应 Opcode 字段值为 5

RRQ 和 WRQ 的数据包格式一样，只不过某些值域设置有差别，剩下的三种数据包格式各不相同。

（1）RRQ 和 WRQ 数据包的格式，首先是 2 字节表示操作码，它用来表示当前数据包的类型（取值 1 表示该数据包是个读请求，2 表示该数据包是写请求）；接下来是可变长字段，它用来表示要读取或上传的文件名，它使用 ASCII 码并以 0 表示结尾；第三个字段叫 Mode，也是可变长字段，用来表示传输文件的数据类型，如果传输的是字符串文件，那么它填写字符串''netascii''，如果传输的是二进制文件，那么它填写字符串''octet'',这些字符串都以 0 结尾，其结构如图 2.1 所示：

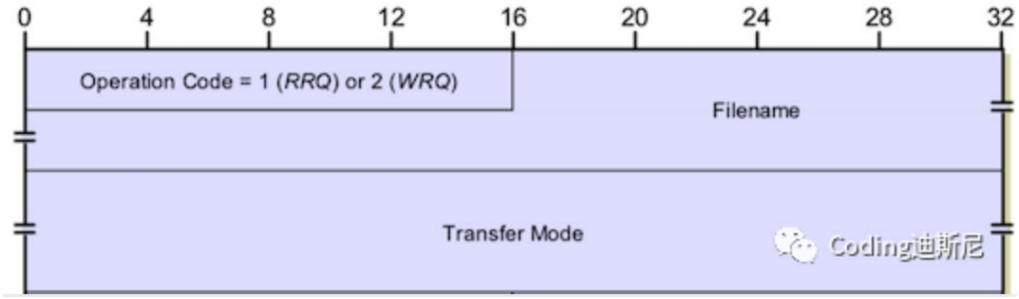

图 2.1 TFTP 协议 RRQ/WRQ 数据报格式

（2）传输数据块的 DATA 数据包，它头 2 字节也是操作码，取值 3 用于表示数据包用于数据块传输，接下来的 2 字节用于表示数据块编号，最后是可变长字段 Data，用于装载数据块，该数据包的格式如图 2.2 所示：

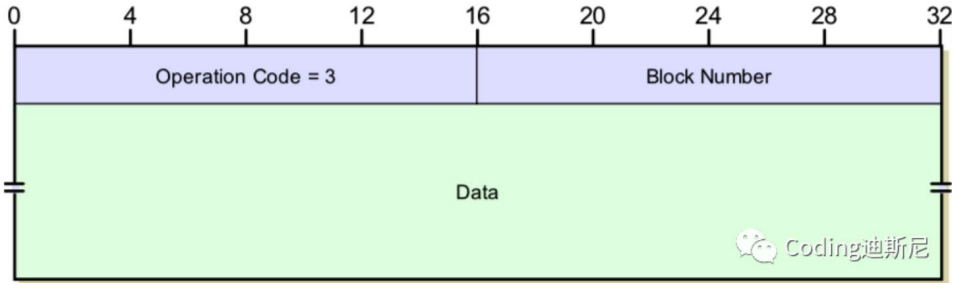

图 2.2 TFTP 协议 DATA 数据包格式

（3）应答 ACK 数据包，它开始的 2 字节也是操作码，取值 4；接下来 2 字节表示接收到的数据块编号，相应结构如图 2.3 所示：

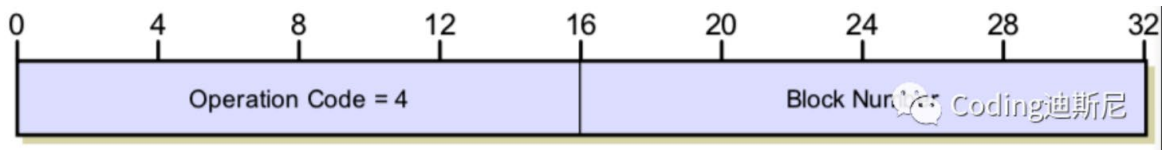

图 2.3 TFTP 协议 ACK 数据包格式

（4）错误 ERROR 数据包，它开始的 2 字节表示操作码，取值 5；接下来 2 字节表示错误码；最后的是可变长字段，它用字符串的形式描述具体错误，该数据包的结构如图 2.4 所示：

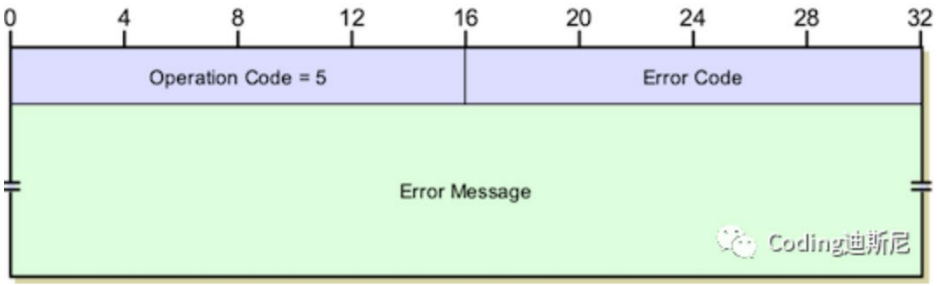

图 2.4 TFTP 协议 ERROR 数据包格式

TFTP 协议目前定义了 8 种错误码，具体的错误码以及对应的错误信息如表 2.1 所示：

表 2.1 TFTP 协议错误码信息

错误码	表示的意思
0	未定义 Not defined, see error message
1	文件未找到 File not found
2	访问被拒绝 Access violation
3	磁盘满或超出可分配空间 Disk full or allocation exceeded
4	非法的 TFTP 操作 Illegal TFTP operation
5	未知的传输 ID Unknown transfer ID
6	文件已经存在 File already exists
7	没有该用户 No such user

2.3 TFTP 的工作流程

TFTP 的工作都是由客户端发起一个 RRQ 或者 WRQ 开始的。这里分别以 WRQ 和 RRQ 为例，讲述读写的工作过程，以及错误处理等内容。

用 S 表示 Server，C 表示 Client，典型的 WRQ 工作流程如图 2.5 所示。

1、WRQ 工作流程

- S 在端口为 69 的 UDP 上等待 C 发出写文件请求包
- C 通过 UDP 发送符合 TFTP 请求格式的 WRQ 包给 S。从 UDP 包角度看，该 UDP 包的源端口由 C 随意选择，而目标端口则是 S 的 69。
- S 收到 C 的这个请求包后，需发送 ACK 给 C。对于写请求包，S 发送的 ACK 包确认号为 0。
- C 发送 DATA 数据给 S，S 接收数据并写文件
  - 当 C 发送的 DATA 数据长度小于 512 字节时，S 认为这次 WRQ 请求完成

这里我们要明确一点，如果有多个 C 同时向 S 发起请求的话，S 如何正确发送包到对应的 C 呢。

在 TFTP 中，一次请求中所有包的源和目标都由 Transfer ID(TID)来标示。TFTP 规定 TID 值就是 UDP 包中的源和目标端口。也就是说，一次请求过程中，S 和 C 通过 UDP 包的源和目标端口来判断这个包是不是发给自己的。

以 WRQ 为例，C 向 S 的 69 端口发送一个文件请求包，这个文件请求包中 UDP 的源端口号为 C 的 TID（假设 C 选择 4845 作为它的 TID），目标端口为 69（这个时候由于请求还未接受，所以这次请求的 UDP 包中目标端口不是 TID）。S 收到这个请求后，将另外采用一个 UDP 端口（应该另启动了一个 UDP Socket）假设为 4849 来回复这个请求的 ACK。这样，这个回复的 UDP 包的源端口就是 S 的 TID（=4849），目标就是 C 的 UDP 端口（TID=4845）。以后，这次请求的后续所有包都在端口为 4845 和 4849 中来往。

上述过程隐含了一定程度上的容错处理。例如，C 收到一个 TID 不是 4849 的包，则认为这个包是错误的。

另外，S 对于每个请求，都要采用一个不重复的新的 UDP 端口号作为它的 TID，也就是说，S 上同时存在的 n 个请求的 TID 都将不同。

这里再介绍下 TFTP 的回复 ACK 机制。虽然 TFTP 中有指定的 ACK 包作为回应，但在普遍意义上，DATA 包和 ERROR 包都可以作为上一次发送包的响应。

一般来说，C 发送了一个非结束 DATA 包给 S，如果在超时时间内，C 未收到 S 发送的 ACK，则 C 继续发送这个 DATA 直到 S 回复 ACK。这种情况是比较好理解的。

但假如 S 回复了上一个非结束 DATA 包 ACK 后，C 在 S 的超时时间内没有发送下一个 DATA 包，则 S 将继续发送这个 ACK。从这个角度看，S 等待的这个新 DATA 包是对上一次 ACK 的确认。

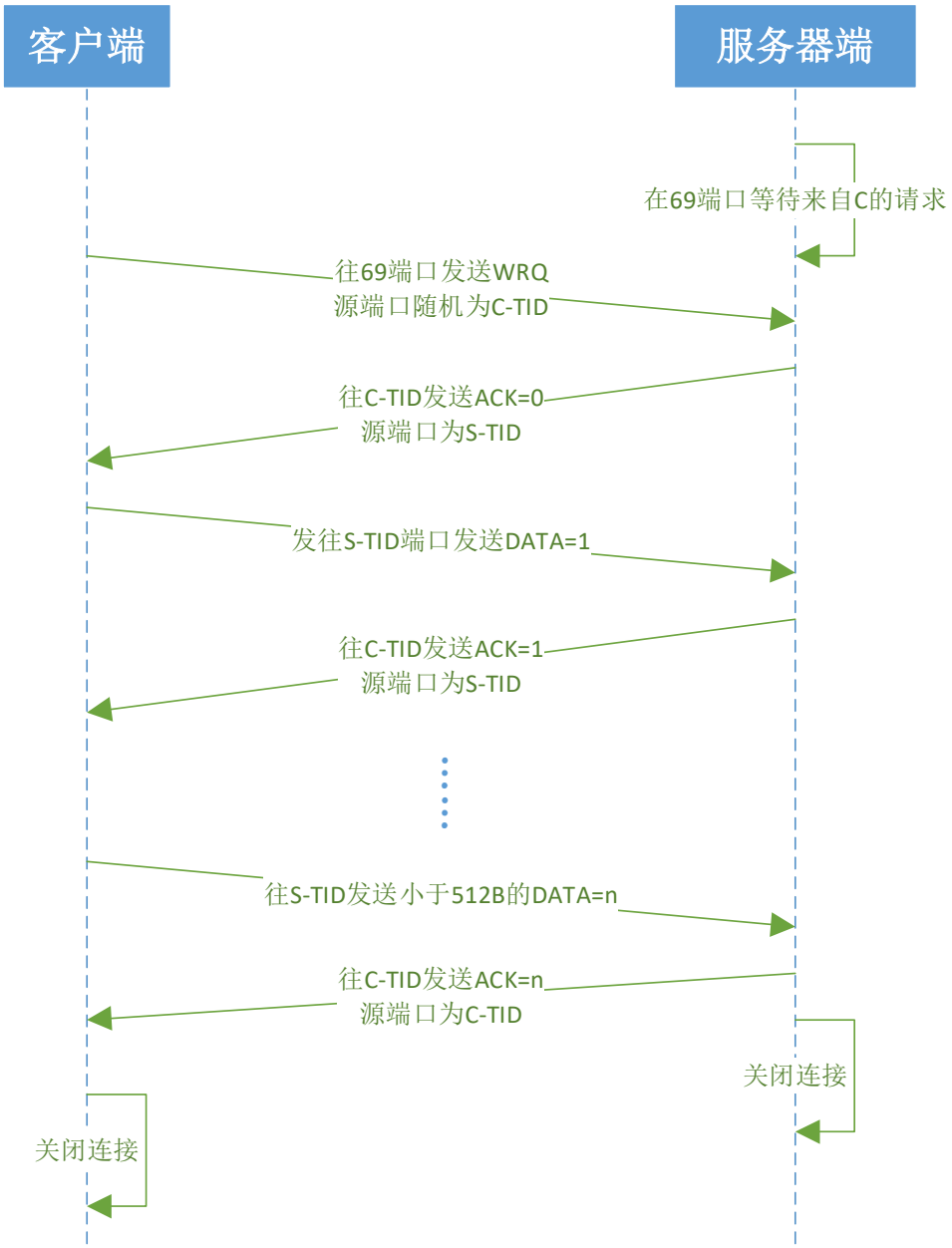

图 2.5 典型的 WRQ 工作流程

2、 RRQ 的工作流程

RRQ 的工作流程和 WRQ 类似，典型的工作流程如图 2.6 所示。

- S 在端口为 69 的 UDP 上等待 C 发出读文件请求包、
- C 通过 UDP 发送符合 TFTP 请求格式的 RRQ 包给 S。
- S 收到 C 的这个请求包后，将直接发送 DATA 包给 C，这个 DATA 包中含 S 选择的 TID 作为 UDP 的源端口和 C 的 TID 作为 UDP 目标端口，起始包号为 1。
- C 接收来自 S 的 DATA 包并回复 ACK。直到请求完成

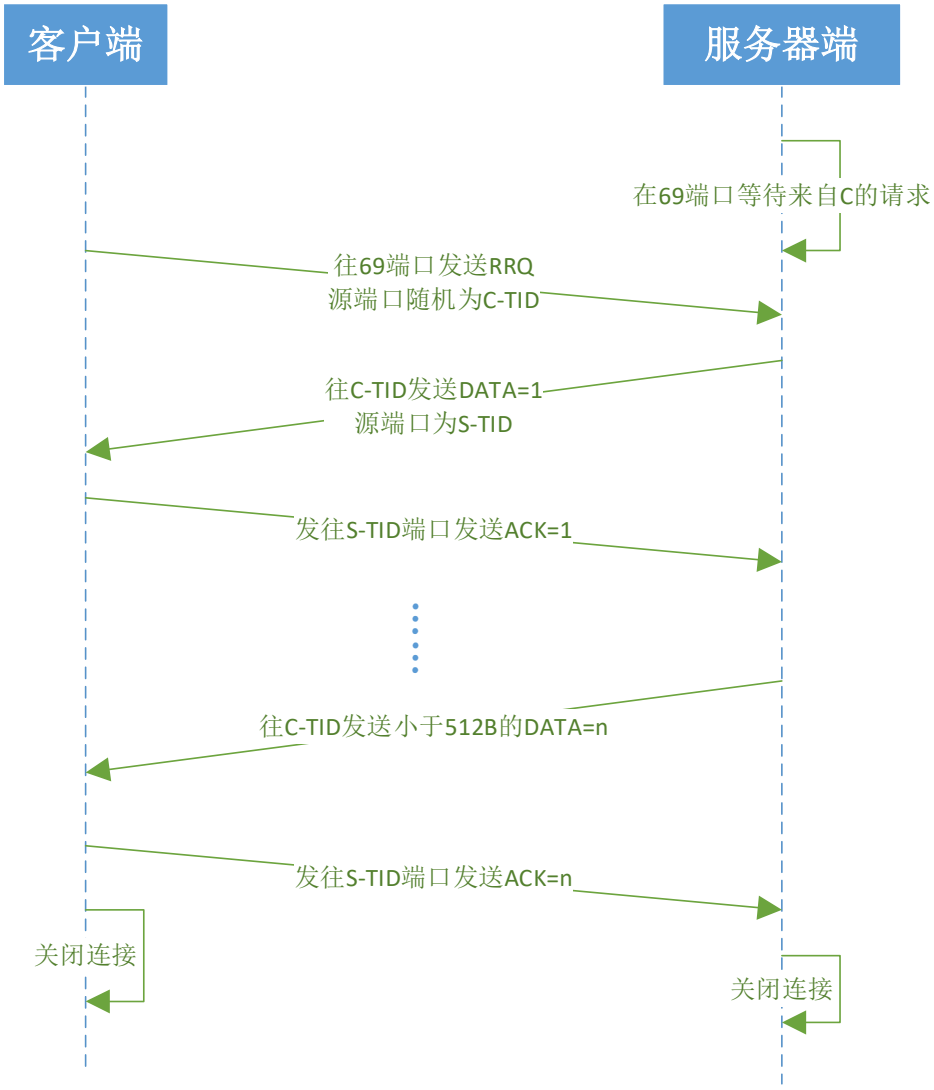

图 2.6 典型的 RRQ 工作流程

3、连接和错误处理

UDP 实际上没有连接的概念。但从上面分析的 RRQ 和 WRQ 看，S 在 69 端口上等待请求，而且 S 总是生成一个新的 UDP 来完成和 C 的交互。这个过程和 TCP 的 listen 以及 Accept 非常类似。所以 TFTP 把这种交互也称作 connection，只不过这种连接是隐含在请求中的。

一般情况下，连接的建立由一次成功的请求来发起，当最后一个 DATA 包发送完毕并且 ACK 回复了后，则连接正常关闭。在传输过程中，如果出现错误，假设 S 向 C 发送了一个 ERROR 包，如果 C 收到 ERROR 包，则连接关闭。如果 C 没有收到 ERROR 包，则需要启动 ERROR 超时检测机制。需要强调的是对于 ERROR 包，S 和 C 都不会重传也不需要 ACK 确认。

TFTP 建议在连接正常关闭的情况下，S 可在发送确认结束 DATA 包的 ACK 后稍等片刻后再关闭连接。例如，当 C 发送结束 DATA 包后，S 回复 ACK 后再等一段时间才关闭。再次等待时间中，如果 ACK 包丢失，C 将再次发送结束 DATA 包或者超时处理。S 如果又收到一次结束 DATA 包后，就知道 ACK 包丢失了。S 可以关闭连接也可以再次发送 ACK 包。

2.4 TFTP 的传输模式

TFTP 传输 8 位数据，传输中有三种模式：

- Netascii：这是 8 位的 ASCII 码形式，一般用来传输字符数据；
- Octet：这是 8 位源数据类型，一般用来传输二进制数据；
- Mail：它将返回的数据直接返回给用户而不是保存为文件，但该模式已经不再支持。

第三章 Windows Socket 编程简介

3.1 Socket 套接字介绍

网络应用程序是由通信进程对组成，每对互相通信的应用程序进程互相发送报文，他们之间的通信必须通过下面的网络来进行。为了将应用程序和底层的网络通信协议屏蔽开来，采用套接字（Socket）这样一个抽象概念来作为应用程序和底层网络之间的应用程序编程接口（API）。

因为网络应用程序是进程之间的通信，为了唯一的标识通信对等方的通信进程，套接字必须包含 2 种信息：(1) 通信对等方的网络地址。(2) 通信对等方的进程号，通常叫端口号。

就像 Unix 操作系统下有一套实现 TCP/IP 网络通信协议的开发接口：BSD Sockets 一样，在 Windows 操作系统下，也提供了一套网络通信协议的开发接口，称为 Windows Sockets 或简称 Winsock。

Winsock 是通过动态链接库的方式提供给软件开发者，而且从 Windows 95 以后已经被集成到了 Windows 操作系统中。

Winsock 主要经历了 2 个版本：Winsock 1.1 和 Winsock 2.0。Winsock 2.0 是 Winsock 1.1 的扩展，它向下完全兼容。

Winsock 同时包括了 16 位和 32 位的编程接口，16 位的 Windows Socket 2 应用程序使用的动态链接库是 WINSOCK.DLL，而 32 位的 Windows Socket 应用程序使用 WSOCK32.DLL（Winsock 1.1 版）和 WS2_32.DLL（Winsock 2.0 版）。另外，使用 Winsock API 时要包含头文件 winsock.h（Winsock 1.1 版）或 winsock2.h（Winsock 2.0 版）。

3.2 Socket 套接字编程原理

3.2.1 Socket 的 2 种类型

Socket 是一个抽象概念，代表了通信双方的端点（Endpoint），通信双方通过 Socket 发送或接收数据。

在 Winsock 里，用数据类型 SOCKET 作为 Windows Sockets 对象的句柄，就好像一个窗口的句柄 HWND、一个打开的文件的文件指针一样。下面我们会看到，在 Winsock API 的许多函数里，都会用到 SOCKET 类型的参数。

Socket 有 2 种类型：

- 流类型（Stream Sockets）。

  流式套接字提供了一种可靠的、面向连接的数据传输方法，使用传输控制协议 TCP。

- 数据报类型（Datagram Sockets）。

数据报套接字提供了一种不可靠的、非连接的数据包传输方式，使用用户数据报协议 UDP。

3.2.2 Socket I/O 的 2 种模式

一个 SOCKET 句柄可以看成代表了一个 I/O 设备。在 Windows Sockets 里，有 2 种 I/O 模式：

- 阻塞式 I/O（blocking I/O）

在阻塞方式下，收发数据的函数在调用后一直要到传送完毕或者出错才能完成，在阻塞期间，除了等待网络操作

的完成不能进行任何操作。阻塞式 I/O 是一个 Winsock API 函数的缺省行为。

- 非阻塞式 I/O（non-blocking I/O）

对于非阻塞方式，Winsock API 函数被调用后立即返回；当网络操作完成后，由 Winsock 给应用程序发送消息（Socket Notifications）通知操作完成，这时应用程序可以根据发送的消息中的参数对消息做出响应。Winsock 提供了 2 种异步接受数据的方法：一种方法是使用 BSD 类型的函数 select（），另外一种方法是使用 Winsock 提供的专用函数WSAAsyncSelect（）。

3.2.3 使用数据报套接字

首先，客户机和服务器都要创建一个数据报套接字。接着，服务器调用 bind（）函数给套接字分配一个公认的端口。一旦服务器将公认的端口分配给了套接字，客户机和服务器都能使用 sendto（）和 revfrom（）来传递数据报。通信完毕调用 closesocket（）来关闭套接字。流程如图 2.1 所示：

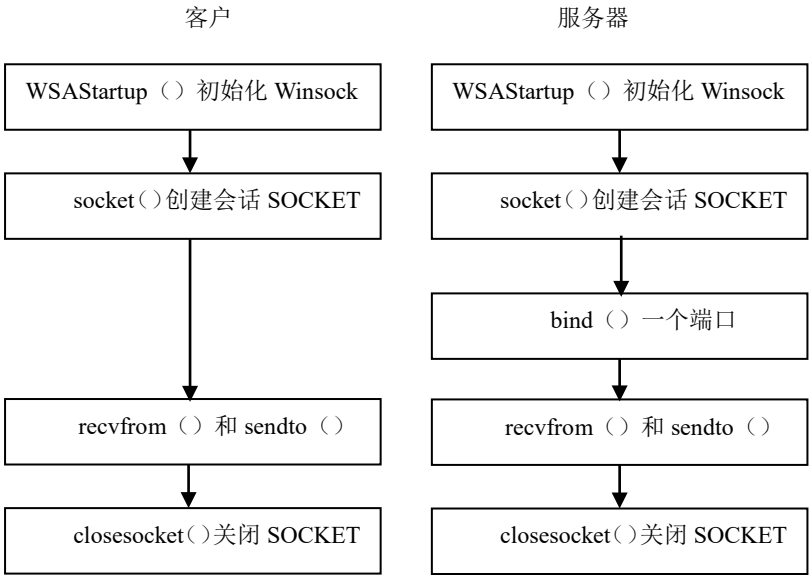

图 3.1 面向无连接的数据报方式过程

3.2.4 使用流式套接字

由于流式套接字使用的是基于连接的协议，所以你必须首先建立连接，而后才能从数据流中读出数据，而不是从一个数据报或一个记录中读出数据，其流程如图 2.2 所示。

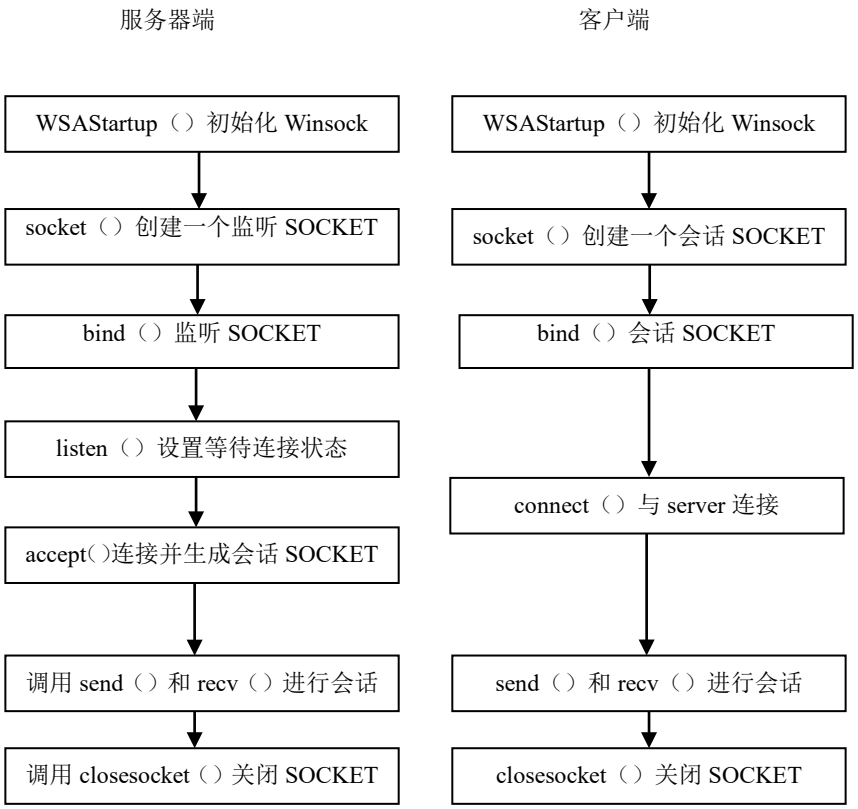

图 3.2 面向连接的流方式过程

第四章 套接字部分库函数列表

4.1 WSAStartup（）

【函数原型】

int WSAStartup (**WORD** wVersionRequested,

LPWSADATA lpWSAData);

【参数】

wVersionRequested

[in] 表示欲使用的 Windows Sockets API 版本；这是个 WORD 类型的整数，高字节定义的是次版本号，低字节定义的是主版本号。

lpWSAData

[in] 指向 WSAData 资料的指针。WSAData 是结构数据类型，描述了关于 Windows Sockecs 底层实现的相关信息。

【返回值】

函数执行成功返回 0，失败则返回如下错误代码：

WSASYSNOTREADY： 底层网络子系统没有准备好。

WSAVERNOTSUPPORTED：Winsock 版本信息号不支持。**WSAEINPROGRESS**： 阻塞式 Winsock1.1 存在于进程中。

WSAEPROCLIM： 已经达到 Winsock 使用量的上限。

WSAEFAULT： lpWSAData 不是一个有效的指针。

【函数功能】

这个函数是应用程序应该第一个调用的 Winsock API 函数，以完成一系列初始化的工作。

【相关数据结构】

WSADATA 的定义如下：

```
typedef struct WSAData {
    WORD    wVersion;
    WORD    wHighVersion;
    char    szDescription[WSADESCRIPTION_LEN+1];
    char    szSystemStatus[WSASYS_STATUS_LEN+1];
    unsigned short    iMaxSockets;
    unsigned short    iMaxUdpDg;
    char FAR *        lpVendorInfo;
} WSADATA, FAR * LPWSADATA;
```

其中，各结构成员的含义为:

wVersion

应用程序应该使用的 Winsock 版本号。

wHighVersion

DLL 所支持的最高版本号。通常应该等于 wVersion。

szDescription

以 0 结尾的 ASCII 字符串，关于 Winsock 底层实现的描述信息。

szSystemStatus

以 0 结尾的 ASCII 字符串，关于 Winsock 底层状态或者配置信息。

iMaxSockets

一个进程最多可使用的套接字数，仅用于 Winsock1.1，Winsock 2.0 应该忽略该成员。

iMaxUdpDg

最大的 UDP 报文大小，仅用于 Winsock1.1，Winsock 2.0 应该忽略该成员。对于 Winsock 2.0，应该使用 getsockopt 函数取得 SO_MAX_MSG_SIZE。

lpVendorInfo

Winsock 开发厂商信息，，仅用于 Winsock1.1，Winsock 2.0 应该忽略该成员。对于 Winsock 2.0，应该使用 getsockopt 函数取得 PVD_CONFIG。

【示例代码】

```
#include <winsock.h>
//对于 Winsock 2, include <winsock2.h>

WSADATA    wsaData;
int nRc = WSAStartup(0x0101, & wsaData);
if(nRc)
{
  //Winsock 初始化错误
  return;
}
if(wsaData.wVersion != 0x0101)
{
  //版本支持不够
  //报告错误给用户，清除 Winsock，返回
  WSACleanup();
  return;
}
```

4.2 socket（）

【函数原型】

SOCKET socket(int af, **int** type, **int** protocol);

【参数】

af

[in] 指定地址族（address family），一般填 AF_INET（使用 Internet 地址）。

type

[in] 指定 SOCKET 的类型：SOCK_STREAM（流类型），SOCK_DGRAM（数据报类型）。

protocol

[in] 指定 af 参数指定的地址族所使用的具体一个协议。建议设为 0，那么它就会根据地址格式和 SOCKET 类型，自动为你选择一个合适的协议。另外 2 个常用的值为：IPPROTO_UDP 和 IPPROTO_TCP。

【返回值】

函数执行成功返回一个新的 SOCKET，失败则返回 INVALID_SOCKET。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

所有的通信在建立之前都要创建一个 SOCKET。

【示例代码】

```
//创建数据报 socket
SCOKET udpSock = socket(AF_INET,
                        SOCK_DGRAM, IPPROTO_UDP);
//创建流 socket
SCOKET tcpSock = socket(AF_INET,
                        SOCK_STREAM, IPPROTO_TCP);
```

4.3 bind（）

【函数原型】

int bind(SOCKET s, **const struct sockaddr FAR*** name, **int** namelen);

【参数】

s

[in] 一个需要绑定的 SOCKET，例如用 socket 函数创建的 SOCKET。

name

[in] 指向描述通信对象地址信息的结构体 sockaddr 的指针。在该结构体中可以指定地址族（一般为 AF_INET）、主机的地址和端口。通常把主机地址指定为 INADDR_ANY（一个主机可能有多个网卡）。

namelen

[in] name 指针指向的结构体的长度。

【返回值】

函数执行成功返回 0，失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

成功地创建了一个 SOCKET 后，用 bind 函数将 SOCKET 和主机地址绑定。

【相关数据结构】

```
struct sockaddr {
    u_short     sa_family;
    char        sa_data[14];
};
```

sa_family

地址族，比如 AF_INET，2 个字节大小。

sa_data

用来存放地址和端口，14 个字节大小。

sockaddr 结构是一个通用的结构（因为 Winsock 支持的协议族不只是 TCP/IP）。对 TCP/IP 协议，用如下结构来定义地址和端口。

```
struct sockaddr_in {
    short           sin_family;
    u_short         sin_port;
    struct  in_addr sin_addr;
    char            sin_zero[8];
};
```

sin_family

地址族，设为 AF_INET。

sin_port

端口号。如果端口号为 0，Winsock 会自动为应用程序分配一个值在 1024-5000 间的一个端口号，所以客户端一般把 sin_port 设为 0。

sin_addr

为 in_addr 结构类型，用来指定 IP 地址。通常把主机地址指定为 INADDR_ANY（一个主机可能有多个网卡）。结构 in_addr 下面介绍。

sin_zero

8 字节的数组，值全为 0。这个 8 个字节用来填充结构 sockaddr_in，使其大小等于结构 sockaddr（16 字节）。

结构 in_addr 用来指定 IP 地址，其定义为：

```
struct in_addr {
    union {
            struct { u_char s_b1,s_b2,s_b3,s_b4; } S_un_b;
            struct { u_short s_w1,s_w2; } S_un_w;
            u_long S_addr;
    } S_un;
};
```

对于 IP 地址 10.14.25.90，sockaddr_in 结构中的 sin_addr 可以这样赋值：

```
sin_addr. S_un .S_un_b. s_b1 = 10;
sin_addr. S_un .S_un_b. s_b2 = 14;
sin_addr. S_un .S_un_b. s_b3 = 25;
sin_addr. S_un .S_un_b. s_b4 = 90;
```

或者

```
sin_addr. S_un . S_un_w. s_w1 = (14<<8)|10;
sin_addr. S_un . S_un_w. s_w2 = (90<<8)|25;
```

或者

```
sin_addr. S_un . S_addr = (90<<24)|(25<<16)|(14<<8)|10;
```

或者

sin_addr. S_un . S_addr = inet_addr(“10.14.25.90”);

这里的 inet_addr 函数可以将字符串形式的 IP 地址转换为 unsigned long 形式的值。

【示例代码】

```
SOCKET sServSock;
sockaddr_in addr;

//创建 socket
sServSock = socket(AF_INET, SOCK_STREAM, 0);

addr.sin_family = AF_INET;

//htons 和 htonl 函数把主机字节顺序转换为网络字节顺序，分别用于//短整型和长整型数据
addr.sin_port = htons(5050);
addr.sin_addr.S_un.S_addr = htonl(INADDR_ANY);

// LPSOCKADDR 类型转换是必须的
int nRc = bind(sServSock, (LPSOCKADDR)&addr, sizeof(addr) );
```

4.4 listen（）

【函数原型】

int listen (**SOCKET** s, **int** backlog);

【参数】

s

[in] 一个已经绑定但未连接的 SOCKET。

backlog

[in] 等待连接的队列的长度，可取 SOMAXCONN。如果某个客户程序要求连接的时候，服务器已经与其他客户程序连接，则后来的连接请求会放在等待队列中，等待服务器空闲时再与之连接。当等待队列达到最大长度（backlog 指定的值）时，再来的连接请求都将被拒绝。

【返回值】

函数执行成功返回 0，失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

对于服务器的程序，当申请到 SOCKET,并将通信对象指定为 INADDR_ANY 之后，就应该等待一个客户机的程序来要求连接，listen 函数就是把一个 SOCKET 设置为这个状态。

4.5 accept（）

【函数原型】

SOCKET accept (SOCKET s, **struct sockaddr FAR*** addr,
int FAR* addrlen);

【参数】

s

[in] 一个已经处于 listen 状态的 SOCKET。

addr

[out] 指向 sockaddr 结构体的指针，里面包含了客户端的地址和端口。

addrlen

[out] int 型指针，指向的内容为 addr 指针指向的结构体的长度。

【返回值】

如果函数执行成功，会建立并返回一个新的 SOCKET 来与对方通信，新建的 SOCKET 与原来的 SOCKET（函数的第一个参数 s）有相同的特性，包括端口号。原来的 SOCKET 继续等待其他的连接请求。而新生成的 SOCKET 才是与客户端通信的实际 SOCKET。所以一般将参数中的 SOCKET 称作“监听”SOCKET，它只负责接受连接，不负责通话；而对于函数返回的 SOCKET，把它称作“会话”SOCKET，它负责与客户端通话。

如果失败则返回 INVALID_SOCKET。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

accept 函数从等待连接的队列中取第一个连接请求，并且创建一个新的 SOCKET 来负责与客户端会话。

【示例代码】

```
SOCKET sServSock;    //服务器监听 socket
sockaddr_in addr;
int nSockErr;
int nNumConns = 0;     //当前请求连接数
SOCKET sConns[5];    //会话 SOCKET 数组
sockaddr ConnAddrs[5];//请求连接的客户端地址
int nAddrLen;

//创建服务器监听 socket
sServSock = socket(AF_INET, SOCK_STREAM, 0);

addr.sin_family = AF_INET;
addr.sin_port = htons(5050);
addr.sin_addr.S_un.S_addr = htonl(INADDR_ANY);

if( bind(sServSock,(LPSOCKADDR)&addr,sizeof(addr)) ==
                    SOCKET_ERROR )
{
    nSockErr = WSAGetLastError();
    //绑定出错处理
}
```

```
//监听客户端请求连接
if( listen(sServSock, 2)  ==  SOCKET_ERROR)
{
    nSockErr = WSAGetLastError();
    //出错处理
}

while( nNumConns < 5){
    //每当收到客户端连接请求，创建新的会话 SOCKET，保存在/  //sConns 数组中
    //客户端地址保存在 ConnAddrs 数组中
    sConns[nNumConns] = accept(sServSock,
                        ConnAddrs[nNumConns], &nAddrLen);
    if(sConns[nNumConns] == INVALID_SOCKET)
    {
        nSockErr = WSAGetLastError();
        //创建会话 SOCKET 出错处理
    }
    else
    {
        //创建会话 SOCKET 成功，启动新的线程与客户端会话
        StartNewHandlerThread(sConns[nNumConns]);
        //当前请求连接数+1
        nNumConns ++;
    }
  }
```

4.6 connect（）

【函数原型】

int connect (**SOCKET** s, **const struct sockaddr FAR*** name,
int namelen);

【参数】

s

[in] 一个未连接 SOCKET，一般是由 socket 函数建立的。

name

[in] 同 bind 函数。

namelen

[in] 同 bind 函数。

【返回值】

函数执行成功返回 0，失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

向对方主动提出连接请求。

4.7 send（）

【函数原型】

int send (**SOCKET** s, **char *** buf, **int** len ,**int** flags);

【参数】

s

[in] 一个已经连接的 SOCKET。

buf

[in] 指向要传输的数据的缓冲区的指针。

len

[in] buf 的长度。

flags

[in]指定函数调用的方式。一般取 0。

【返回值】

函数执行成功返回发送的字节数（可能小于 len），失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

通过已经连接的 SOCKET 发送数据。

4.8 recv（）

【函数原型】

int recv (**SOCKET** s, **char *** buf, **int** len ,**int** flags);

【参数】

s

[in] 一个已经连接的 SOCKET。

buf

[out] 指向接收数据的缓冲区的指针。

len

[in] buf 的长度。

flags

[in]指定函数调用的方式。一般取 0。

【返回值】

函数执行成功返回接收到数据的字节数。如果失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取

得具体的错误代码。

【函数功能】

通过已经连接的 SOCKET 接收数据。当读到的数据字节少于规定接受的数目（len）时，就把数据全部接收，并返回实际接收到的字节数；当读到的数据多于规定的值时，在流方式下剩余的数据由下个 recv 读出，在数据报方式下多余的数据被丢弃。

4.9 sendto（）

【函数原型】

int sendto (**SOCKET** s, **char *** buf, **int** len ,**int** flags,

struct sockaddr_in * to, **int** tolen);

【参数】

s

[in] 一个 SOCKET(可能已连接)。

buf

[in] 指向要传输的数据的缓冲区的指针。

len

[in] buf 的长度。

flags

[in] 指定函数调用的方式。一般取 0。

to

[in] 指向目标地址结构体的指针。

tolen

[in] 目标地址结构体的长度。

【返回值】

函数执行成功返回发送的字节数（可能小于 len），失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

该函数一般用于通过无连接的 SOCKET 发送数据报文，报文的接受者由 to 参数指定。

4.10 recvfrom（）

【函数原型】

int recvfrom (**SOCKET** s, **char *** buf, **int** len ,**int** flags,

struct sockaddr_in * from, **int *** fromlen);

【参数】

s

[in] 一个已经绑定的 SOCKET。

buf

[out] 指向接收数据的缓冲区的指针。

len

[in] buf 的长度。

flags

[in] 指定函数调用的方式。一般取 0。

from

[out] 指向源地址结构体的指针。

fromlen

[in/out] 源地址结构体的长度。

【返回值】

函数执行成功返回发送的字节数（可能小于 len），失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

该函数一般用于通过无连接的 SOCKET 接收数据报文，报文的发送者由 from 参数指定。

4.11 closesocket（）

【函数原型】

int closesocket (SOCKET s,);

【参数】

s

[in] 要关闭的 SOCKET。

【返回值】

函数执行成功返回 0，失败则返回 SOCKET_ERROR。这时可以调用 WSAGetLastError 函数取得具体的错误代码。

【函数功能】

关闭指定的 SOCKET。

第五章 Windows Socket 编程示例

本章给出了流式 Socket 和数据报 Socket 编程简单示例，供各位同学参考。示例代码说明如下：

1、流式 Socket 示例代码是一个用 Win32 控制台程序实现的一个简单聊天室的例子。客户端在一个控制台窗口输入的聊天信息发送到服务器端，服务器将该条消息转发到所有当前和服务器保持连接的客户端上。

2、数据报 Socket 示例代码将一个长度小于 512 字节的字符串传输给服务器。

5.1 流式 Socket 服务器端代码

```
// socksrv.cpp : Defines the entry point for the console application.
#include "stdafx.h"
#include <stdio.h>
#include <winsock2.h>
#include <list>
#include <algorithm>
#include <string.h>

#define MAXCONN 5
#define BUFLEN 255

using namespace std;

typedef list<SOCKET> ListCONN;
typedef list<SOCKET> ListConErr;

void main(int argc, char* argv[])
{
  WSADATA wsaData;
  int nRC;
  sockaddr_in srvAddr,clientAddr;
  SOCKET srvSock;
  int nAddrLen = sizeof(sockaddr);
  char sendBuf[BUFLEN],recvBuf[BUFLEN];
  ListCONN conList;          //保存所有有效的会话 SOCKET
  ListCONN::iterator itor;
  ListConErr conErrList;     //保存所有失效的会话 SOCKET
  ListConErr::iterator itor1;
  FD_SET rfds,wfds;
  u_long uNonBlock;

  //初始化 winsock
  nRC = WSAStartup(0x0101,&wsaData);
  if(nRC)
  {
    printf("Server initialize winsock error!\n");
    return;
```

```
}
if(wsaData.wVersion != 0x0101)
{
   printf("Server's winsock version error!\n");
   WSACleanup();
   return;
}
printf("Server's winsock initialized !\n");

//创建  TCP socket
srvSock = socket(AF_INET,SOCK_STREAM,0);
if(srvSock == INVALID_SOCKET)
{
   printf("Server create socket error!\n");
   WSACleanup();
   return;
}
printf("Server TCP socket create OK!\n");

//绑定  socket to Server's IP and port 5050
srvAddr.sin_family = AF_INET;
srvAddr.sin_port = htons(5050);
srvAddr.sin_addr.S_un.S_addr = INADDR_ANY;
nRC=bind(srvSock,(LPSOCKADDR)&srvAddr,sizeof(srvAddr));
 if(nRC == SOCKET_ERROR)
{
   printf("Server socket bind error!\n");
   closesocket(srvSock);
   WSACleanup();
   return;
}
printf("Server socket bind OK!\n");

//开始监听过程，等待客户的连接
nRC = listen(srvSock,MAXCONN);
if(nRC == SOCKET_ERROR)
{
   printf("Server socket listen error!\n");
   closesocket(srvSock);
   WSACleanup();
   return;
}

//将 srvSock 设为非阻塞模式以监听客户连接请求
uNonBlock = 1;
ioctlsocket(srvSock,FIONBIO,&uNonBlock);

while(1)
```

```
{
  //从 conList 中删除已经产生错误的会话 SOCKET
  for(itor1 = conErrList.begin();itor1 != conErrList.end();itor1++)
  {
   itor = find(conList.begin(),conList.end(),*itor1);
   if(itor != conList.end()) conList.erase(itor);
  }

  //清空 read,write 套接字集合
  FD_ZERO(&rfds);
  FD_ZERO(&wfds);

  //设置等待客户连接请求
  FD_SET(srvSock,&rfds);

  for(itor = conList.begin();itor != conList.end();itor++)
  {
   //把所有会话 SOCKET 设为非阻塞模式
   uNonBlock = 1;
   ioctlsocket(*itor,FIONBIO,&uNonBlock);
   //设置等待会话 SOKCET 可接受数据或可发送数据
   FD_SET(*itor,&rfds);
   FD_SET(*itor,&wfds);
  }
  //开始等待
  int nTotal = select(0, &rfds, &wfds, NULL, NULL);

  //如果 srvSock 收到连接请求，接受客户连接请求
  if(FD_ISSET(srvSock,&rfds))
  {
   nTotal --;
   //产生会话 SOCKET
   SOCKET connSock = accept(srvSock,
                            (LPSOCKADDR)&clientAddr,
                            &nAddrLen);
   if(connSock == INVALID_SOCKET)
   {
        printf("Server accept connection request error!\n");
        closesocket(srvSock);
        WSACleanup();
        return;
   }
   sprintf(sendBuf,"来自%s 的游客进入聊天室!\n",
                        inet_ntoa(clientAddr.sin_addr));
   printf("%s",sendBuf);

   //将产生的会话 SOCKET 保存在 conList 中
```

```
 conList.insert(conList.end(),connSock);
}
if(nTotal > 0)
{
 //检查所有有效的会话 SOCKET 是否有数据到来
      //或是否可以发送数据
 for(itor = conList.begin();itor != conList.end();itor++)
 {
       //如果会话 SOCKET 可以发送数据，
            //则向客户发送消息
       if(FD_ISSET(*itor,&wfds))
       {
            //如果发送缓冲区有内容，则发送
            if(strlen(sendBuf) > 0)
            {
                 nRC = send(*itor,sendBuf,strlen(sendBuf),0);
                 if(nRC == SOCKET_ERROR)
                 {
                      //发送数据错误，
                           //记录下产生错误的会话 SOCKET
                      conErrList.insert(conErrList.end(),*itor);
                 }
                 else//发送数据成功，清空发送缓冲区
                      memset(sendBuf,'\0',BUFLEN);
            }
       }

       //如果会话 SOCKET 有数据到来，则接受客户的数据
       if(FD_ISSET(*itor,&rfds))
       {
            nRC = recv(*itor,recvBuf,BUFLEN,0);
            if(nRC == SOCKET_ERROR)
            {
                 //接受数据错误，
                      //记录下产生错误的会话 SOCKET
                      conErrList.insert(conErrList.end(),*itor);
            }
            else
            {
                 //接收数据成功，保存在发送缓冲区中，
                      //以发送到所有客户去
                 recvBuf[nRC] = '\0';
                 sprintf(sendBuf,"\n 游客说:%s\n",recvBuf);
                 printf("%s",sendBuf);
            }
       }
```

```
            }
        }
    }
    closesocket(srvSock);
    WSACleanup();
}
```

5.2 流式 Socket 客户端代码

```
// sockclient.cpp : Defines the entry point for the console application.
//
#include "stdafx.h"
#include <stdio.h>
#include <winsock2.h>
#include <string.h>
#include <windows.h>
#include <process.h>
#include <winbase.h>
#define BUFLEN 255

//全局的临界区保护变量，以保护主线程和子线程都要访问的 sendBuf
CRITICAL_SECTION gCriticalSection;

//子线程运行的函数，获取客户从键盘输入的信息
unsigned __stdcall GetInputs(void *arg);

void main(int argc, char* argv[])
{
    WSADATA wsaData;
    int nRC;
    sockaddr_in srvAddr,clientAddr;
    SOCKET clientSock;
    char sendBuf[BUFLEN],recvBuf[BUFLEN];
    FD_SET rfds,wfds;
    u_long uNonBlock;
    HANDLE hThread;
    unsigned dwThreadID;

    if(argc != 2)
    {
        printf("Usage:%s ClientIPAddress name\n",argv[0]);
        return;
    }

    InitializeCriticalSection(&gCriticalSection);
    //初始化 winsock
    nRC = WSAStartup(0x0101,&wsaData);
```

```
if(nRC)
{
	printf("Client initialize winsock error!\n");
	return;
}
if(wsaData.wVersion != 0x0101)
{
	printf("Client's winsock version error!\n");
	WSACleanup();
	return;
}
printf("Client's winsock initialized !\n");

//创建  client socket
clientSock = socket(AF_INET,SOCK_STREAM,0);
if(clientSock == INVALID_SOCKET)
{
	printf("Client create socket error!\n");
	WSACleanup();
	return;
}
printf("Client    socket create OK!\n");

clientAddr.sin_family = AF_INET;
clientAddr.sin_port = htons(0);
clientAddr.sin_addr.S_un.S_addr = inet_addr(argv[1]);
nRC = bind(clientSock,
	(LPSOCKADDR)&clientAddr,sizeof(clientAddr));
if(nRC == SOCKET_ERROR)
{
	printf("Client socket bind error!\n");
	closesocket(clientSock);
	WSACleanup();
	return;
}
printf("Client socket bind OK!\n");


//准备服务器的信息，这里需要指定服务器的地址
srvAddr.sin_family = AF_INET;
srvAddr.sin_port = htons(5050);
srvAddr.sin_addr.S_un.S_addr = inet_addr("192.168.0.3");

//连接服务器
nRC = connect(clientSock,
	(LPSOCKADDR)&srvAddr,sizeof(srvAddr));
if(nRC == SOCKET_ERROR)
{
```

```
        printf("连接服务器失败!\n");
        closesocket(clientSock);
        WSACleanup();
        return;
    }

    //启动一个子线程，获取客户从键盘输入的信息
    hThread = (HANDLE)_beginthreadex(NULL,
                                     0,
                                     GetInputs,
                                     sendBuf,
                                     0,
                                     &dwThreadID);


    //向服务器发送数据和从服务器接受数据
    while(1)
    {
        //清空发送和接收缓冲区
        memset(sendBuf,'\0',BUFLEN);
        memset(recvBuf,'\0',BUFLEN);

        //将 SOCKET 设为非阻塞模式，
        //并且等待有数据到来或者可以发送数据
        FD_ZERO(&rfds);
        FD_ZERO(&wfds);
        FD_SET(clientSock,&rfds);
        FD_SET(clientSock,&wfds);
        uNonBlock = 1;
        ioctlsocket(clientSock,FIONBIO,&uNonBlock);
        select(0,&rfds,&wfds,NULL,NULL);

        //如果有数据到来
        if(FD_ISSET(clientSock,&rfds))
        {
            //接受服务器发来的数据并且显示
            nRC = recv(clientSock,recvBuf,BUFLEN,0);
            if(nRC == SOCKET_ERROR)
            {
                printf("接收数据失败!\n");
                DeleteCriticalSection(&gCriticalSection);
                closesocket(clientSock);
                WSACleanup();
                return;
            }
            else if(nRC > 0)
            {
```

```
                recvBuf[nRC] = '\0';
                printf("\n%s\n",recvBuf);
            }
        }
        //如果可以发送数据
        if(FD_ISSET(clientSock,&wfds))
        {
            //如果用户在键盘输入了信息，则发送
            if(strlen(sendBuf) > 0)
            {
                nRC = send(clientSock,sendBuf,strlen(sendBuf),0);
                if(nRC == SOCKET_ERROR)
                {
                    printf("发送数据失败!\n");
                    DeleteCriticalSection(&gCriticalSection);
                    closesocket(clientSock);
                    WSACleanup();
                    return;
                }
                else
                {
                    EnterCriticalSection(&gCriticalSection);
                    sendBuf[0] = '\0';
                    LeaveCriticalSection(&gCriticalSection);
                }
            }
        }
        if(strcmp(sendBuf,"exit") == 0) break;
    }
    DeleteCriticalSection(&gCriticalSection);
    closesocket(clientSock);
    WSACleanup();
}
//子线程运行的函数，获取客户从键盘输入的信息
unsigned __stdcall GetInputs(void *arg)
{
    char *inputs = (char *)arg;
    while(1)
    {
        printf("\n 我要发言:");
        EnterCriticalSection(&gCriticalSection);
        gets(inputs);
        LeaveCriticalSection(&gCriticalSection);
        if(strcmp(inputs,"exit") == 0)
            return EXIT_SUCCESS;
    }
}
```

5.3 数据报 Socket 服务器端代码

```
#define SERVER_PORT 8000
#define BUFFER_SIZE 1024
#define FILE_NAME_MAX_SIZE 512

int main()
{
 /* 创建 UDP 套接口 */
 struct sockaddr_in server_addr;
 bzero(&server_addr, sizeof(server_addr));
 server_addr.sin_family = AF_INET;
 server_addr.sin_addr.s_addr = htonl(INADDR_ANY);
 server_addr.sin_port = htons(SERVER_PORT);

 /* 创建 socket */
 int server_socket_fd = socket(AF_INET, SOCK_DGRAM, 0);
 if(server_socket_fd == -1)
 {
  perror("Create Socket Failed:");
  exit(1);
 }

 /* 绑定套接口 */
 if(-1 == (bind(server_socket_fd,(struct sockaddr*)&server_addr,sizeof(server_addr))))
 {
  perror("Server Bind Failed:");
  exit(1);
 }

 /* 数据传输 */
 while(1)
 {
  /* 定义一个地址，用于捕获客户端地址 */
  struct sockaddr_in client_addr;
  socklen_t client_addr_length = sizeof(client_addr);

  /* 接收数据 */
  char buffer[BUFFER_SIZE];
  bzero(buffer, BUFFER_SIZE);
  if(recvfrom(server_socket_fd, buffer, BUFFER_SIZE,0,(struct sockaddr*)&client_addr, &client_addr_length) == -1)
  {
   perror("Receive Data Failed:");
   exit(1);
  }

  /* 从 buffer 中拷贝出 file_name */
```

```
 char file_name[FILE_NAME_MAX_SIZE+1];
 bzero(file_name,FILE_NAME_MAX_SIZE+1);
 strncpy(file_name, buffer, strlen(buffer)>FILE_NAME_MAX_SIZE?FILE_NAME_MAX_SIZE:strlen(buffer));
 printf("%s\n", file_name);
 }
 close(server_socket_fd);
 return 0;
}
```

5.4 数据报 Socket 客户端代码

```
#define SERVER_PORT 8000
#define BUFFER_SIZE 1024
#define FILE_NAME_MAX_SIZE 512

int main()
{
 /* 服务端地址 */
 struct sockaddr_in server_addr;
 bzero(&server_addr, sizeof(server_addr));
 server_addr.sin_family = AF_INET;
 server_addr.sin_addr.s_addr = inet_addr("127.0.0.1");
 server_addr.sin_port = htons(SERVER_PORT);

 /* 创建 socket */
 int client_socket_fd = socket(AF_INET, SOCK_DGRAM, 0);
 if(client_socket_fd < 0)
 {
  perror("Create Socket Failed:");
  exit(1);
 }

 /* 输入文件名到缓冲区 */
 char file_name[FILE_NAME_MAX_SIZE+1];
 bzero(file_name, FILE_NAME_MAX_SIZE+1);
 printf("Please Input File Name On Server:\t");
 scanf("%s", file_name);

 char buffer[BUFFER_SIZE];
 bzero(buffer, BUFFER_SIZE);
 strncpy(buffer, file_name, strlen(file_name)>BUFFER_SIZE?BUFFER_SIZE:strlen(file_name));

 /* 发送文件名 */
 if(sendto(client_socket_fd, buffer, BUFFER_SIZE,0,(struct sockaddr*)&server_addr,sizeof(server_addr)) < 0)
 {
  perror("Send File Name Failed:");
```

```
 exit(1);
}

close(client_socket_fd);
return 0;
}
```

5.5 工程配置

服务器端和客户端程序都为 Win32 Console Application。

对于服务器和客户端工程，都必须打开工程设置（Project->Settings…），然后选中 Link 选项卡，在 Object/library modules 栏目中添加 ws2_32.lib。

对于客户端工程，还必须打开工程设置（Project->Settings…），然后选中 C/C++选项卡，Category 选择 Code generation ,Use run-time library 选择 Debug Multithreaded。