



附赠CD

# Windows API

## 开发详解

### ——函数、接口、编程实例

范文庆 周彬彬 安靖 编著

 人民邮电出版社  
POSTS & TELECOM PRESS

# 开发详解

## ——函数、接口、编程实例

范文庆 周彬彬 安靖 编著

人民邮电出版社  
北京

## 图书在版编目 (C I P) 数据

Windows API开发详解：函数、接口、编程实例 /  
范文庆, 周彬彬, 安靖编著. — 北京：人民邮电出版社,  
2011. 3

ISBN 978-7-115-24427-7

I. ①W… II. ①范… ②周… ③安… III. ①窗口软  
件, Windows—软件接口—程序设计 IV. ①TP316.7

中国版本图书馆CIP数据核字(2010)第230248号

## 内 容 提 要

Windows API (Windows Application Program Interface, Windows 应用程序接口) 是一系列函数、宏、数据类型、数据结构的集合, 运行于 Windows 系统的应用程序, 可以使用操作系统提供的接口来实现需要的功能。本书由浅入深、循序渐进地讲解如何使用 Windows API 进行 Windows 应用程序开发。全书共 18 章, 分为 3 个部分, 第 1 部分 (第 1 章~第 3 章) 介绍 Windows 程序设计基础; 第 2 部分 (第 4 章~第 17 章) 按照程序设计的各个方面进行划分, 包括文件系统、内存管理、进程与线程、用户界面、Shell 程序开发、Windows GDI、Socket 网络通信驱动程序开发、安全机制等内容; 第 3 部分 (第 18 章) 作为全书的总结和补充。

本书适合广大的 Windows 应用程序开发人员、VC++ 开发工程师、网络游戏开发人员、软件培训机构学员和高校学生阅读。

### Windows API 开发详解——函数、接口、编程实例

- ◆ 编 著 范文庆 周彬彬 安 靖  
责任编辑 蒋 佳
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号  
邮编 100061 电子函件 315@ptpress.com.cn  
网址 <http://www.ptpress.com.cn>  
北京艺辉印刷有限公司印刷
- ◆ 开本: 800×1000 1/16  
印张: 39.5  
字数: 956 千字 2011 年 3 月第 1 版  
印数: 1 - 3 500 册 2011 年 3 月北京第 1 次印刷

ISBN 978-7-115-24427-7

定价: 79.00 元 (附光盘)

读者服务热线: (010)67132692 印装质量热线: (010)67129223  
反盗版热线: (010)67171154

## 关于 Windows API

Windows API (Windows Application Program Interface) 是一系列接口函数、宏、数据类型、数据结构的集合。运行于 Windows 操作系统的应用程序可以使用其提供的接口来实现应用程序需要的功能。Windows 开发平台是所有程序开发平台中非常重要的一种，是程序设计中一个重要的方面。本书介绍了 Windows 应用程序开发所涉及的各个方面。

## 本书的写作方法

程序设计是一门实践性很强的学科，本书在编写过程中十分注重与实际开发工作相联系，在讲解每一个编程要点时，都以实例为核心进行分析、演示，并把实际工程中开发人员可能遇到的问题以实例的方式向读者讲解。

与此同时，本书同样重视基础知识的讲解，重视原理的说明，对程序所使用的每一个 API 和每一个结构的使用方法都尽量详细说明。本书还在第 18 章详细介绍了 Windows 系统调用的内部过程。

解决开发人员实际编码过程中可能出现的问题也是本书的一个主要目的，因此本书使用了大量篇幅来讲解编译选项等最容易被忽略，但是却是最容易在程序设计中出现问题，也是常常使得程序员不知道如何解决的问题。

## 本书主要内容

本书共分 18 章，涵盖了 Windows 应用程序设计的基本内容。第 1、2、3 章是 Windows 程序设计的基础。第 4 章~第 17 章按程序设计的方面划分，每个方面一章。第 18 章是全书的总结和提高。

第 1 章主要讲解如何配置 Windows 应用程序的开发工具，从最简单的实例入手，使读者对 Windows 应用程序的开发有一个初步的认识。

第 2 章对 Windows API 作了简要的介绍，包括 Windows API 基本的功能分类、数据类型等。

第 3 章介绍了开发工具配置与使用，包括基本的编译链接工具 `cl.exe`、`rc.exe`、`link.exe`，Platform Sdk 的使用，Makefile 的编写以及使用 WinDbg 的调试方法等。

第 4 章文件系统，主要介绍了磁盘和驱动器管理、文件和目录管理、内存映射文件等内容。

第 5 章内存管理，主要介绍了内存管理原理、堆原理、全局和局部内存管理、虚拟内存管理、内存操作与内存消息管理等内容。

第 6 章进程、线程和模块，主要介绍了进程管理，线程、纤程的创建、删除以及获取方法，获取进程状态信息，动态链接库的加载、释放和获取方法等内容。

第 7 章线程同步，主要介绍了线程同步的基本原理、同步对象等内容。

第 8 章服务，主要介绍了基本概念、服务程序的编写、对服务程序的控制和管理等内容。

第 9 章图形用户界面，主要介绍了字符界面程序，窗口、控件、菜单、对话框等界面元素的使用方法。

第 10 章系统信息的管理，主要介绍了系统基本信息、时间信息以及注册表信息的管理。

第 11 章进程间通信，主要介绍了邮箱、管道、剪贴板的创建与使用方法，数据复制消息的使用方法等内容。

第 12 章 Windows Shell 程序设计，主要介绍了 Windows Shell 的目录管理、文件协助、Shell 扩展等内容。

第 13 章 Windows GDI，主要介绍了使用 GDI 指定文字的字体、绘制线条、绘制图形、对位图的操作、坐标变换的方法等内容。

第 14 章网络通信与配置，主要介绍了 Socket 通信的相关内容以及 IP Helper 的使用方法。

第 15 章程序安装与设置，主要介绍了 cab 文件的创建、INF 文件的创建、安装程序 setup.exe 的编写、使用 msi 文件进行安装等内容。

第 16 章设备驱动管理与内核通信，主要介绍了与设备有关的 API 函数、如何对设备驱动进行控制、如何编写设备驱动程序等内容。

第 17 章用户、认证和对象安全，主要介绍了数据认证中的基本概念、安全机制程序示例以及用户的增加、删除、权限更改等内容。

第 18 章 Windows API 的内部原理，主要介绍了 Windows 系统中的对象封装、x86 平台程序函数调用、可执行程序结构与 API 函数接口内部机理等内容。

## 参与本书编写的人员

本书由范文庆、周彬彬、安靖负责编写并统编全书稿，另外感谢以下人员为本书所做的工作：张墨、郭永红、周瑜、王建伟、孙琼、田旭、钟金鑫、王欣、张曦文、尚玉珊、张丛辉、王玮、刘超、张圣亮、李凡、马堃、徐路迎、赵国锋、孙颂武、汪荷君、孙明、林雪梅、黄惠英、刘雯等。

由于时间仓促，加之水平有限，书中不足之处在所难免，敬请读者批评指正。

编者  
2010年12月

第 1 章	Windows 应用程序开发入门	1
1.1	第一个实例程序	1
1.1.1	start.exe	1
1.1.2	Windows API	2
1.1.3	程序入口函数	2
1.1.4	start.c 代码分析	2
1.2	编译代码	3
1.2.1	安装 Visual Studio	4
1.2.2	安装 Microsoft Platform SDK	4
1.2.3	集成 Microsoft Platform SDK 与 Visual C++ 速成版	6
1.2.4	Windows 7 SDK 与 Visual Studio 2010	7
1.2.5	Visual Studio 专业版或团队系统版	7
1.2.6	使用图形化 IDE 建立工程、进行编译	7
1.2.7	“解决方案”与“工程”	9
1.2.8	使用命令行工具编译	9
第 2 章	Windows API 概要	10
2.1	Windows 数据类型	10
2.1.1	Windows 数据类型示例	10
2.1.2	Windows 数据类型与标准 C 数据类型的关系	14
2.1.3	Windows 数据类型与 Windows API	14
2.1.4	Windows 中的数据结构	15
2.2	Windows API 的功能分类	16
2.2.1	系统基本服务	16
2.2.2	系统管理	18
2.2.3	用户界面	18
2.2.4	图像和多媒体	21
2.2.5	网络	21
2.2.6	系统安全	21
2.2.7	其他功能	22
2.3	Windows API 核心 DLL	22
2.3.1	Kernel32.dll	22

2.3.2	User32.dll	23
2.3.3	Gdi32.dll	23
2.3.4	标准 C 函数及 CrtDll_dll	23
2.3.5	其他 Dll	23
2.4	Unicode 和多字节	23
2.4.1	W 版本和 A 版本的 API	25
2.4.2	Unicode 与 ASCII 的转换	26
2.5	对 Windows 程序设计规范的建议	26
<b>第 3 章</b>	<b>开发工具配置与使用</b>	<b>28</b>
3.1	使用 Visual C/C++ 编译链接工具	28
3.1.1	编译器 cl.exe	29
3.1.2	资源编译器 rc.exe	34
3.1.3	链接器 link.exe	35
3.1.4	其他工具	41
3.1.5	编译链接工具依赖的环境变量	42
3.1.6	示例: 使用 /D 选项进行条件编译	46
3.2	使用 Platform SDK	47
3.2.1	Platform SDK 的目录结构与功能	47
3.2.2	为编译链接工具设置环境变量	48
3.2.3	Platform SDK 工具集	50
3.2.4	Windows Vista SDK	52
3.3	编写 Makefile	52
3.3.1	使用 nmake.exe 构建工程	52
3.3.2	Makefile 实例	54
3.3.3	注释	55
3.3.4	宏	55
3.3.5	描述块: 目标、依赖项和命令	57
3.3.6	makefile 预处理	60
3.3.7	在 Platform SDK 的基础上使用 nmake	61
3.3	使用 WinDbg 调试	62
3.4.1	安装 WinDbg	63
3.4.2	编译可调试的程序	64



3.4.3	WinDbg 命令	64
3.4.4	调试过程演示	65
3.5	集成开发环境 Visual Studio	68
3.5.1	工程类型选择与配置	68
3.5.2	Visual Studio 快捷方式	70
3.5.3	生成项目	70
3.5.4	调试	71
3.5.5	选项与设置	71
3.6	开发环境配置总结	72
<b>第 4 章</b>	<b>文件系统</b>	<b>73</b>
4.1	概述	73
4.1.1	文件系统的基本概念	73
4.1.2	文件系统主要 API	74
4.2	磁盘和驱动器管理	76
4.2.1	遍历卷并获取属性	76
4.2.2	操作驱动器挂载点	83
4.2.3	判断光驱中是否有光盘	88
4.2.4	获取磁盘分区的总容量、空闲容量、簇、扇区信息	91
4.3	文件和目录管理	94
4.3.1	删除、复制、重命名、移动文件	95
4.3.2	创建、打开、读写文件，获取文件大小	98
4.3.3	创建目录	105
4.3.4	获取程序所在的目录、程序模块路径，获取和设置 当前目录	106
4.3.5	查找文件、遍历指定目录下的文件和子目录	110
4.3.6	递归遍历目录树	113
4.3.7	获取、设置文件属性和时间	115
4.4	内存映射文件	122
4.4.1	使用 Mapping File 提高文件读写的效率	122
4.4.2	通过 Mapping File 在进程间传递和共享数据	127
4.4.3	通过文件句柄获得文件路径	130
4.5	总结	134

第 5 章 内存管理 .....	135
5.1 Windows 内存管理原理 .....	135
5.1.1 基本概念 .....	135
5.1.2 分页与分段内存管理、内存映射与地址转换 .....	136
5.1.3 进程的内存空间 .....	138
5.1.4 虚拟内存布局、内存的分工、堆与栈 .....	140
5.1.5 内存的保护属性和存取权限 .....	140
5.1.6 本章 API 列表 .....	141
5.2 堆管理 .....	142
5.2.1 获取堆句柄、分配与再分配堆 .....	142
5.2.2 获取堆中内存块的大小信息 .....	147
5.2.3 释放内存、销毁堆 .....	148
5.3 全局 (Global) 和局部 (Local) 内存管理 .....	150
5.3.1 Global 函数 .....	150
5.3.2 Local 函数 .....	152
5.3.3 使用全局和局部函数分配和释放内存、 改变内存块属性 .....	152
5.4 虚拟内存管理 .....	153
5.4.1 虚拟地址空间与内存分页 .....	153
5.4.2 分配和释放可读可写的虚拟内存页面 .....	154
5.4.3 修改内存页面状态和保护属性、 将页面锁定在物理内存中 .....	158
5.4.4 管理其他进程的虚拟内存 .....	159
5.5 内存操作与内存信息管理 .....	159
5.5.1 复制、填充、移动、清零内存块、防止缓冲区溢出 .....	160
5.5.2 获得当前系统内存使用情况 .....	162
5.5.3 判断内存指针的可用性 .....	163
5.6 各种内存分配方式的关系与比较 .....	165
5.6.1 标准 C 内存管理函数与 Windows 内存管理 API 的关系 .....	165
5.6.2 功能性区别 .....	165
5.6.3 效率的区别 .....	166

第 6 章	进程、线程和模块	167
6.1	基本概念	167
6.1.1	应用程序与进程	167
6.1.2	控制台应用程序与图形用户界面应用程序	168
6.1.3	动态链接库、模块	168
6.1.4	线程、纤程与作业	169
6.1.5	权限与优先级	170
6.2	进程管理	170
6.2.1	创建进程、获取进程相关信息、获取启动参数	170
6.2.2	编写控制台程序和图形用户界面应用程序	176
6.2.3	获取和设置环境变量	176
6.3	线程、纤程	180
6.3.1	创建线程、退出线程、获取线程信息	180
6.3.2	挂起、恢复、切换、终止线程	183
6.3.3	创建远程线程、将代码注入其他进程中执行	186
6.3.4	创建纤程、删除纤程、调度纤程	190
6.3.5	纤程与线程的互相转换	191
6.4	进程状态信息	197
6.4.1	PS API 与 Tool help API	197
6.4.2	遍历系统中的进程	199
6.4.3	列举进程的模块、线程	203
6.4.4	进程的堆使用、内存占用、虚拟内存大小， 页面错误情况	205
6.5	动态链接库	207
6.5.1	加载、释放 DLL、通过句柄获取 DLL 相关信息	207
6.5.2	编写动态链接库、导出函数	208
6.5.3	创建动态链接库工程，配置 DLL 编译链接选项	210
6.5.4	运行时动态获取 DLL 导出函数地址并调用	211
6.5.5	声明导出函数、创建 lib 库，为其他模块 提供导入表调用接口	213
6.5.6	通过构建导入表调用 DLL 导出函数	213
第 7 章	线程同步	215
7.1	基本原理	215

7.1.1	线程同步的过程	216
7.1.2	同步对象	216
7.1.3	等待函数	216
7.2	同步对象示例	217
7.2.1	使用事件对象 (Event)	217
7.2.2	使用互斥对象 (Mutex)	223
7.2.3	使用信号量控制访问共享数据的线程数量	227
7.2.4	使用可等待计时器 (Timer)	231
7.3	等待进程和线程的执行完成	235
<b>第 8 章</b>	<b>服务</b>	<b>236</b>
8.1	基本概念	236
8.1.1	服务控制器 (SCM)	237
8.1.2	服务程序	237
8.1.3	服务控制管理程序	237
8.1.4	系统服务管理工具	237
8.1.5	服务的属性	237
8.2	编写服务程序	238
8.2.1	入口函数	238
8.2.2	服务主函数	238
8.2.3	控制处理函数	239
8.3	实现对服务的控制和管理	243
8.3.1	创建、删除服务	243
8.3.2	启动、停止服务, 向服务发送控制请求	246
8.3.3	管理服务状态、配置服务、服务的依赖关系	250
<b>第 9 章</b>	<b>图形用户界面</b>	<b>257</b>
9.1	字符界面程序	257
9.1.1	基本概念	258
9.1.2	控制台读写	259
9.1.3	控制台字体、颜色等属性, 操作屏幕缓存	263
9.1.4	控制台事件	274
9.2	图形用户界面: 基本概念	276

9.2.1	窗口	276
9.2.2	窗口类	277
9.2.3	消息和消息处理函数	277
9.2.4	控件	277
9.2.5	资源	278
9.2.6	对话框	278
9.3	图形用户界面：窗口	278
9.3.1	注册窗口类	280
9.3.2	创建窗口	281
9.3.3	窗口消息处理函数	284
9.3.4	窗口属性、位置和大小	287
9.3.5	窗口显示方式	289
9.3.6	线程消息队列和消息循环	289
9.4	图形用户界面：控件	290
9.4.1	Tree View 控件	290
9.4.2	为 Tree View 控件增加节点	292
9.4.3	Tree View 右键菜单	294
9.4.4	List View 控件	296
9.4.5	为 List View 控件增加分列	298
9.4.6	为 List View 控件增加项	299
9.4.7	文本框控件	300
9.4.8	为文本框控件设置文字	301
9.5	界面资源	302
9.5.1	资源脚本 (.rc)	302
9.5.2	资源 ID 定义和头文件	305
9.5.3	在程序中使用资源	306
9.6	菜单	307
9.6.1	菜单资源和菜单句柄	307
9.6.2	动态增加、删除、设置菜单及菜单项	308
9.6.3	菜单消息处理	308
9.7	对话框	309
9.7.1	创建对话框	309
9.7.2	对话框消息处理函数	310

第 10 章	系统信息的管理	312
10.1	Windows 系统信息	312
10.1.1	获取系统版本	312
10.1.2	获取计算机硬件信息	315
10.1.3	获取系统目录等信息	317
10.1.4	用户名、计算机名、域名	318
10.1.5	处理系统颜色信息、尺度信息等	320
10.1.6	鼠标、键盘等外设信息	320
10.2	时间信息	322
10.2.1	设置、获取系统时间	322
10.2.2	获取开机至现在持续的时间	323
10.2.3	文件时间与系统时间的转换	323
10.3	注册表	324
10.3.1	注册表的作用及组织形式	324
10.3.2	键、子键、键属性及键值的相关操作	325
10.3.3	列举注册表项及键值	328
10.3.4	通过注册表设置一个自启动的程序	330
10.3.5	设置随程序启动而启动的调试器(任何程序)	331
10.3.6	指定程序崩溃实时调试器	331
第 11 章	进程间通信	332
11.1	邮槽(MailSlot)	332
11.1.1	创建邮槽、从邮槽中读取消息	333
11.1.2	通过邮槽发送消息	336
11.2	管道(Pipe)	338
11.2.1	创建命名管道	338
11.2.2	管道监听	340
11.2.3	使用异步 I/O 进行读写	341
11.2.4	关闭管道实例	345
11.2.5	客户端	346
11.3	剪贴板	349
11.3.1	获取、设置剪贴板数据	349
11.3.2	监视剪贴板	356

11.3.3	剪贴板数据格式	366
11.4	数据复制消息 (WM_COPYDATA)	368
11.4.1	数据发送端	368
11.4.2	数据接收端	371
11.5	其他进程间通信方式	373
11.5.1	动态数据交换 (DDE) 和网络动态数据交换 (NDDE)	373
11.5.2	通过 File Mapping 在进程间共享数据	374
11.5.3	Windows Socket	374
<b>第 12 章</b>	<b>Windows Shell 程序设计</b>	<b>375</b>
12.1	Windows Shell 目录管理	376
12.1.1	Shell 对目录和文件的管理形式	376
12.1.2	“我的文档”等特殊目录相关操作	376
12.1.3	接口绑定、目录遍历以及文件对象属性获取	378
12.1.4	浏览文件对话框	380
12.2	文件协助 (File Associations)	382
12.2.1	文件类型相关注册表键值	382
12.2.2	为文件指定默认打开程序	383
12.2.3	定制文件类型的图标	384
12.3	Shell 扩展	384
12.3.1	对象及概念	385
12.3.2	CLSID, 处理例程的 GUID	386
12.3.3	注册 Shell 扩展	387
12.3.4	COM 程序开发基础	388
12.3.5	编写 Handler 程序	388
12.3.6	Shell 扩展程序的调试	406
12.3.7	总结	406
12.4	任务栏通知区域 (Tray) 图标	407
12.4.1	创建图标窗口	408
12.4.2	创建图标和图标菜单	412
12.4.3	最小化主窗口到通知区域	414
12.4.4	弹出气泡通知	417
12.4.5	动态图标	418

12.4.6	其他功能	421
<b>第 13 章</b>	<b>Windows GDI</b>	<b>424</b>
13.1	GDI 编程接口概述	424
13.1.1	Windows GDI 的功能	424
13.1.2	链接库与头文件	424
13.2	设备上下文 (DC)、输出操作与图形对象	425
13.2.1	设备上下文类型与关联设备	425
13.2.2	图形对象的作用及与 DC 的关系	425
13.2.3	各类图形对象的具体属性与作用	428
13.2.4	绘制、填充、写入等图形输出操作	429
13.2.5	修剪与坐标变换	430
13.2.6	设备上下文的图形模式	430
13.3	一个最简单的 GDI 程序	431
13.3.1	示例	431
13.3.2	DC 的操作	433
13.3.3	颜色的表示	434
13.3.4	图形对象: 画刷和画笔	435
13.3.5	输出操作: 绘制图形和线条	436
13.4	文字和字体	437
13.4.1	选择、设置字体	439
13.4.2	选择字体图形对象	441
13.4.3	文字的颜色	441
13.4.4	输出文字	441
13.4.5	DC 图形模式设置	442
13.4.6	遍历已安装字体	443
13.4.7	为系统安装、删除字体文件	446
13.5	绘制线条	446
13.5.1	选择画笔对象	446
13.5.2	直线	446
13.5.3	绘制任意曲线	446
13.5.4	跟踪鼠标轨迹	447
13.5.5	弧线	453



13.6	绘制图形	454
13.6.1	填充颜色与边缘勾勒	454
13.6.2	绘制矩形、椭圆、圆角矩形	454
13.6.3	椭圆弓形和椭圆扇形	460
13.6.4	多边形	461
13.6.5	RECT 结构及对 RECT 的操作	462
13.7	位图操作	463
13.7.1	截取屏幕、保存位图文件	464
13.7.2	将位图显示在界面上	469
13.8	区域 (Regions)、路径 (Paths) 与修剪 (Clip) 操作	473
13.8.1	区域的创建及形状、位置等属性	473
13.8.2	区域边沿、区域填充、反转与勾勒操作	474
13.8.3	组合、比较、移动等操作	477
13.8.4	点击测试 (Hit Testing)	478
13.8.5	路径的创建与操作	483
13.8.6	路径转换为区域	484
13.8.7	使用区域和路径进行修剪操作, 限制输出	484
13.9	坐标变换	491
13.9.1	缩放	492
13.9.2	旋转	492
13.10	调色板	493
<b>第 14 章</b>	<b>网络通信与配置</b>	<b>496</b>
14.1	Socket 通信	497
14.1.1	客户端	497
14.1.2	服务端	503
14.1.3	处理并发的客户端连接	510
14.1.4	网络通信的异步 I/O 模式	510
14.2	IP Helper	511
<b>第 15 章</b>	<b>程序安装与设置</b>	<b>519</b>
15.1	创建 cab 文件	519
15.1.1	makecab.exe	519