Windows驱动开发

陈志远　史长亭　白　玉　主编

HEUP 哈尔滨工程大学出版社

Windows 驱动开发

主　编　陈志远　史长亭　白　玉
副主编　郎大鹏　李健利　林　森
主　审　汪家祥　李静梅

HEUP 哈爾濱工程大學出版社

内容简介

本书从一个初级学习者的角度出发，由浅入深、循序渐进地介绍了 Windows 驱动程序的开发方法、注意事项和调试过程。通过一个简单的例子让学习者了解 Windows 驱动程序开发的环境配置与驱动框架，同时重点介绍了开发过程中必须掌握的字符串与内存管理、注册表与文件操作、IRP、Minifilter 等核心技术，最后还对开发设计者所必须了解和掌握的编码规范问题进行了讲解。

本书适合作为 Windows 驱动开发初学者的入门教材。对于学习 Windows 驱动开发的初学者来说，学习与掌握本书是最佳选择。

图书在版编目(CIP)数据

Windows 驱动开发/陈志远，史长亭，白玉主编. —哈尔滨：哈尔滨工程大学出版社，2015.12

ISBN 978-7-5661-1195-1

Ⅰ.①W… Ⅱ.①陈… ②史… ③白… Ⅲ.①Windows 操作系统-程序设计 Ⅳ.①TP316.7

中国版本图书馆 CIP 数据核字(2016)第 000597 号

选题策划 刘凯元
责任编辑 张忠远 马毓聪
封面设计 恒润设计

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 哈尔滨市石桥印务有限公司
开　　本 787mm×1 092mm 1/16
印　　张 16.25
字　　数 415 千字
版　　次 2016 年 3 月第 1 版
印　　次 2016 年 3 月第 1 次印刷
定　　价 45.00 元

http://www.hrbeupress.com
E-mail:heupress@hrbeu.edu.cn

前　言

当我们怀着好奇与热情开始接触 Windows 驱动开发后，信息与系统安全联合实验室的老师和同学们都为此投入了巨大的精力。随着时间的推移，我们从知之甚少到可以用该技术解决实际问题，虽然期间经历了诸多困难与波折，但我们却对 Windows 驱动开发的应用领域产生了浓厚的兴趣。

本书是根据联合实验室全体人员在学习过程中的经验体会而编写的一本具有指导意义的教科书，它可以帮助像我们当初一样的菜鸟一步一步按照章节内容的指引，从最基本的内容开始学习，到后期可以独立完成简单的驱动程序开发设计。

全书共分 6 章，第 1 章介绍进行 Windows 驱动开发时的环境设置及 Windows 驱动开发的框架结构，包括需要的软件、开发环境的设置和调试环境的设置等；第 2 章介绍了 Windows驱动开发时的字符串与内存管理，重点强调了与 C 语言相比在使用时的不同之处；第 3 章针对 Windows 驱动开发时必须涉及的文件操作、注册表及 PE 文件进行了阐述；第 4 章对 IRP 的结构、处理过程、派遣函数、功能、通信及过滤等内容进行了综合分析与解释；第 5 章重点介绍了 Minifilter 的框架形成方式，包括 Minifilter 的具体功能与操作方式；第 6 章介绍了工程项目开发时撰写文档所必须遵循的编码规范及 WinDbg 用法详解。

本书的撰写得到了中天安泰（北京）信息技术有限公司的高级工程师候景山和马刘杰两位老师的亲自指导，他们不仅在学习过程中给予了我们技术方面的悉心指导，更在全书撰写思路上给予了我们正确的指引。在本书的撰写过程中，亦得到了联合实验室诸位同学的支持与帮助，他们是（名字不分先后）：张雷、高申、李明旭、诸邵忆、赵梓渊、李佩瑶、李宇航、张伟、田乔、郑方圆、赵硕、陈晨、贾成罡、廖光宇、王晓昀、翟宇豪、潘媛媛、袁春艳、南瑞涛、王东方。

全书由汪家祥教授主审，李静梅教授对本书进行了内容组织和协调工作。

最后，向所有为完成此书撰写付出努力的人表示深深的感谢！

编　者

2015 年 8 月

目 录

第1章　从一个简单的例子谈起

1.1　Windows 驱动开发简介

驱动程序(device drivers)是一种可以使计算机和设备进行通信的特殊程序,是硬件厂商根据操作系统的功能编写的配置文件。可以说,没有驱动程序,计算机中的硬件就无法工作。通常情况下,操作系统不同,硬件的驱动程序也不同。

Windows 系统中通常需要安装一套完整的驱动程序(包括主板、光驱、显卡、声卡等的驱动程序,CPU 和内存无需驱动程序便可使用,所以并没有 CPU 驱动程序和内存驱动程序)。如果需要外接其他硬件设备,则还要安装相应的驱动程序,例如,插入 U 盘要安装 USB 驱动程序,外接打印机要安装打印机驱动程序,上网或接入局域网要安装网卡驱动程序等。

Windows 驱动开发是针对 Windows 操作系统进行的底层开发。大多数的驱动程序运行在内核模式(kernel mode),程序的错误经常造成系统严重的不稳定,例如蓝屏(blue screen)(如图 1-1 所示),与过去的用户模式(user mode)下的程序设计(例如 Delphi,VB,Java)有明显的差异。

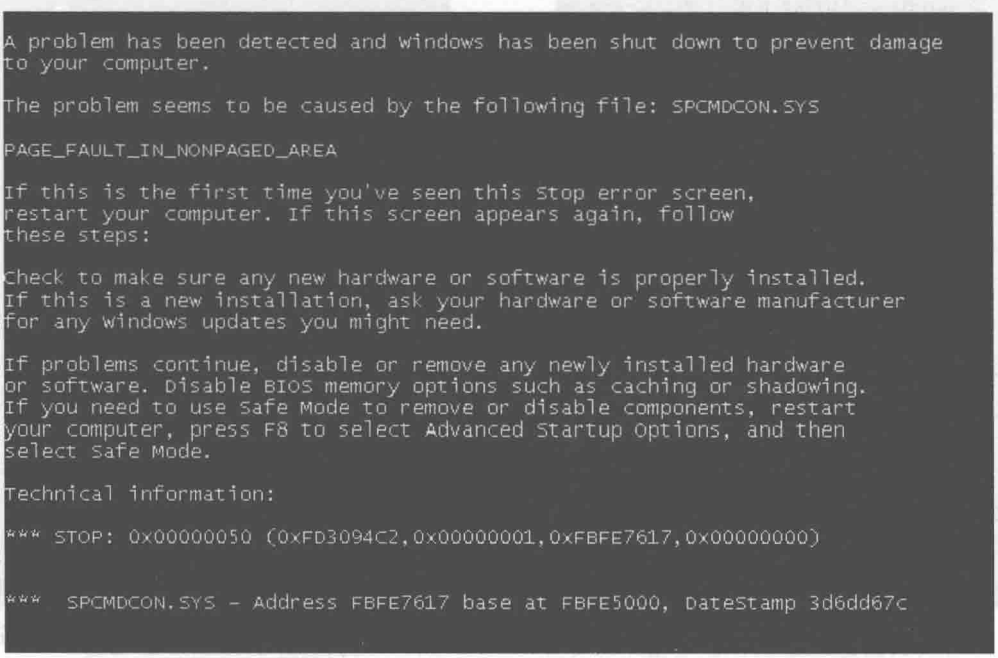

图 1-1　蓝屏

应用范围：

1. 硬件设备的相应驱动；

2. 辅助系统运行；

3. 部分反病毒软件(杀毒软件)可通过在系统添加驱动程序的方式进驻系统，并随操作系统启动。

1.2 环境配置

1.2.1 所需的软件

开发环境：Visual Studio 2013(VS 2013)，Windows Driver Kit 8.1 (WDK 8.1)，Windows Driver Kit 7.1.0.7600 (WDK 7600_1)。

调试环境：VMware，Windows 7 iso，WinDbg，Osrloader，SetDbgPrintFilter，DbgView。

下载地址：

1. VS 2013

https://www.visualstudio.com/downloads/download-visual-studio-vs

2. WDK 8.1

https://msdn.microsoft.com/en-US/windows/hardware/gg454513

3. Windows Driver Kit 7(WDK 7)

http://www.microsoft.com/en-us/download/details.aspx?id=11800

4. Osrloader

http://www.osronline.com/article.cfm?article=157

5. SetDbgPrintFilter

http://www.osronline.com/article.cfm?article=506

6. DbgView

https://technet.microsoft.com/en-us/sysinternals/bb896647

1.2.2 开发环境

本书利用 VS 集成开发环境进行驱动开发。

可以利用 VS 2013 + WDK 8.1 的环境进行 Windows 7 到 Windows 8.1 (包括同样 NT 版本的 Server 版本) 的驱动编译开发。

可以下载免费的 Visual Studio Community 用于开发(当然也可以利用 Profession 以上版本进行开发)。

在 Windows 7 环境中安装 VS 2013，然后再安装 WDK 8.1，即可利用 VS 2013 进行 Windows 7 以上版本的操作系统的驱动开发工作。安装 WDK 7 之后可以进行 Windows XP 到 Windows 7 的驱动开发。

1.2.3　调试环境

由于驱动程序可能会存在问题，因此最好的调式方式是在另外一台机器上进行调试，本书选择的调式方式是在虚拟机中进行调试。

常用虚拟机：

1. VMware Workstation(付费软件)

可在官网下载使用版本并进行安装。

官网地址：http://www.vmware.com/products/workstation/

2. Virtualbox(免费软件)

官网地址：https://www.virtualbox.org/wiki/Downloads

3. Hyper-V(Windows 7 专业版，可以在控制面板中打开)

其中最好的虚拟机环境为 VMware Workstation，因此本书就以 VMware 为例子进行说明。

1.2.4　开发环境配置

注意：安装顺序为 VS 2013，WDK 8.1，WDK 7600_1，必须按此顺序安装。

VS 2013 的安装界面如图 1-2 所示，安装位置不建议选择系统盘 C 盘，体验改善计划选项可选可不选，一般不选。点击“下一步”按钮后会出现如图 1-3 所示的界面。

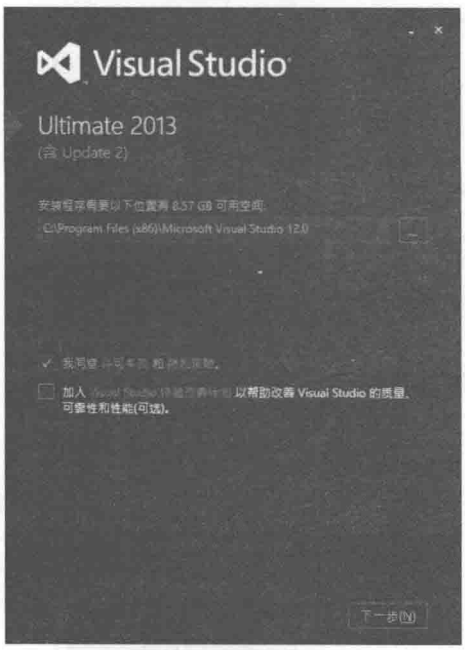

图 1-2　VS 2013 安装(1)

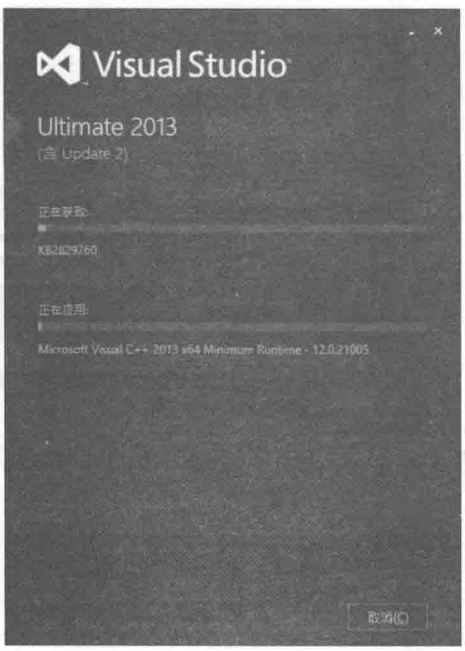

图 1-3　VS 2013 安装(2)

安装完毕后的准备界面如图 1 -4 所示。

图 1 -4　VS 2013 安装(3)

WDK 8.1 的安装界面如图 1 -5 所示(安装路径自选,不建议选择系统盘 C 盘)。

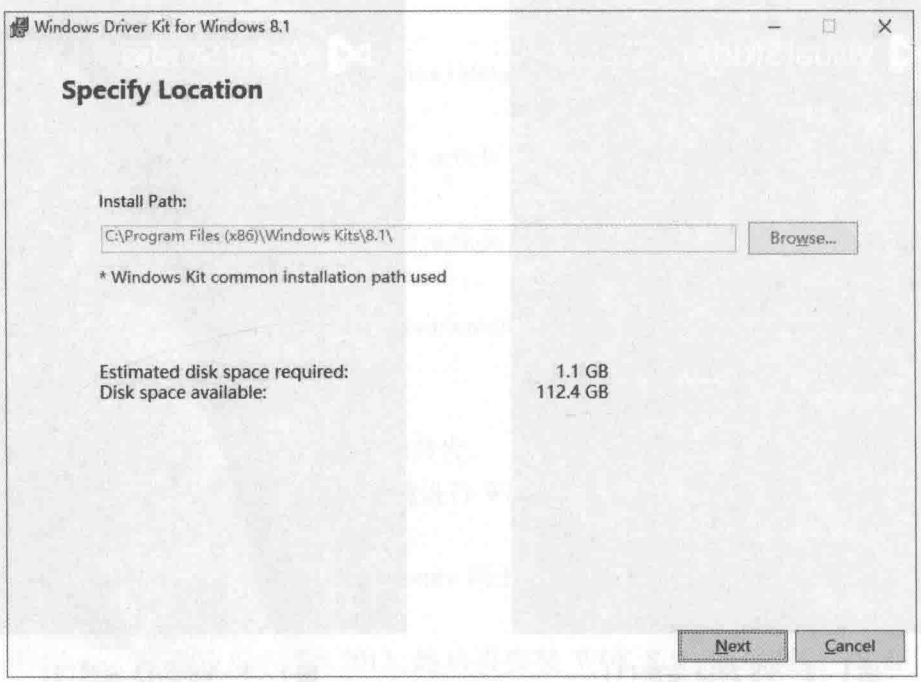

图 1 -5　WDK 8.1 安装

安装好 VS 2013 和 WDK 8.1 之后，WDK 8.1 会合并到 VS 2013 中，此时 VS 2013 界面的菜单栏中会出现“DRIVER”选项，如图 1－6 所示，“新建”项目中会有“Windows Driver”选项（这个就是驱动的项目），如图 1－7 所示。

图 1－6　VS 2013 和 WDK 8.1 安装后效果图（1）

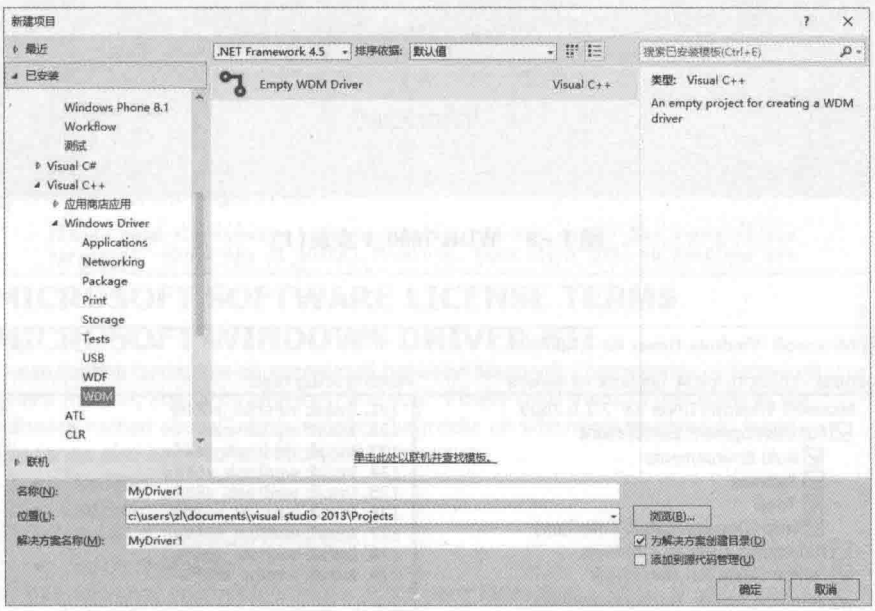

图 1－7　VS 2013 和 WDK 8.1 安装后效果图（2）

WDK 7600_1 的安装步骤如图 1－8 至图 1－12 所示（安装路径自选，不建议选择系统盘 C 盘）。

1.2.5　调试环境配置

1. 安装虚拟机

VMware 的安装步骤如图 1－13 至图 1－15 所示。

安装虚拟机时可能会出现错误提示信息“This product may not be installed on a computer that has Microsoft Hyper-V installed.”，其原因是微软的 Hyper-V 虚拟平台不能和 VMware 的虚拟平台共存，关闭 Hyper-V 即可解决问题。

关闭 Hyper-V 的步骤：①打开“控制面板”，找到“卸载程序”；②点击左边的“启用或关闭 Windows 功能”；③在弹出的对话框里把“Hyper-V”选项的钩去掉，点击“确定”按钮。

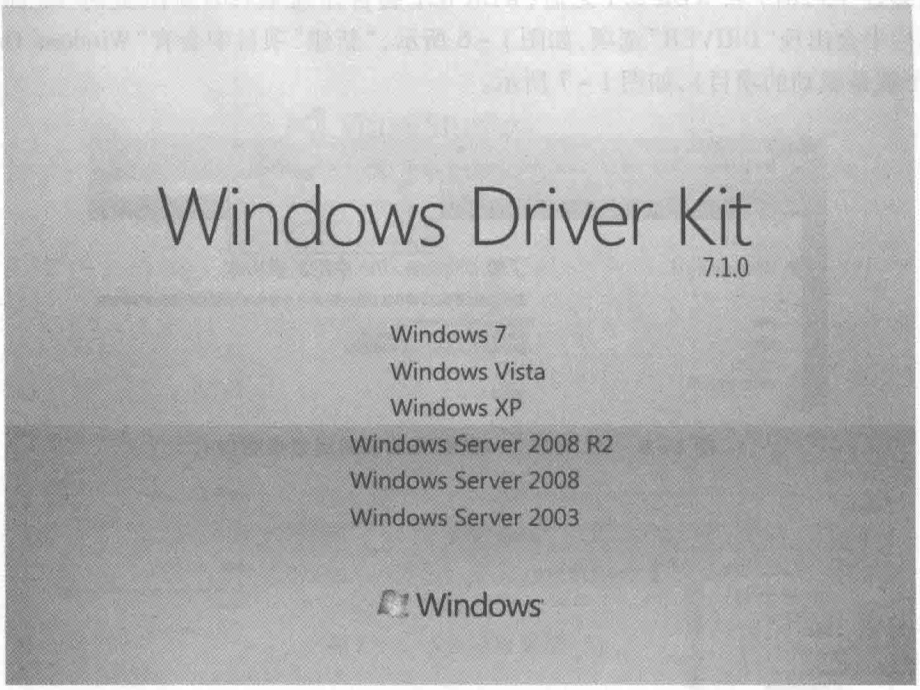

图 1-8 WDK 7600_1 安装(1)

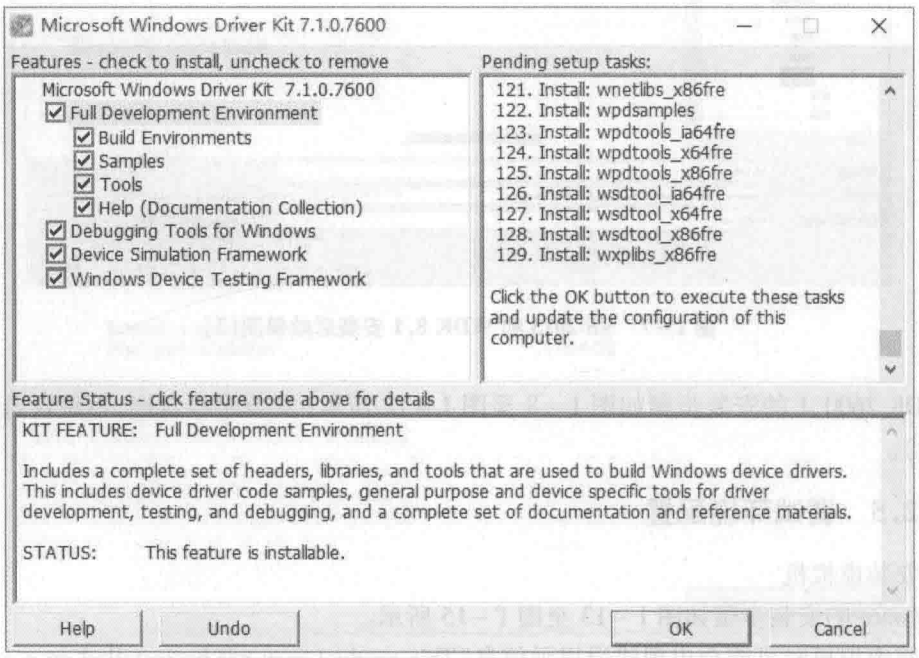

图 1-9 WDK 7600_1 安装(2)

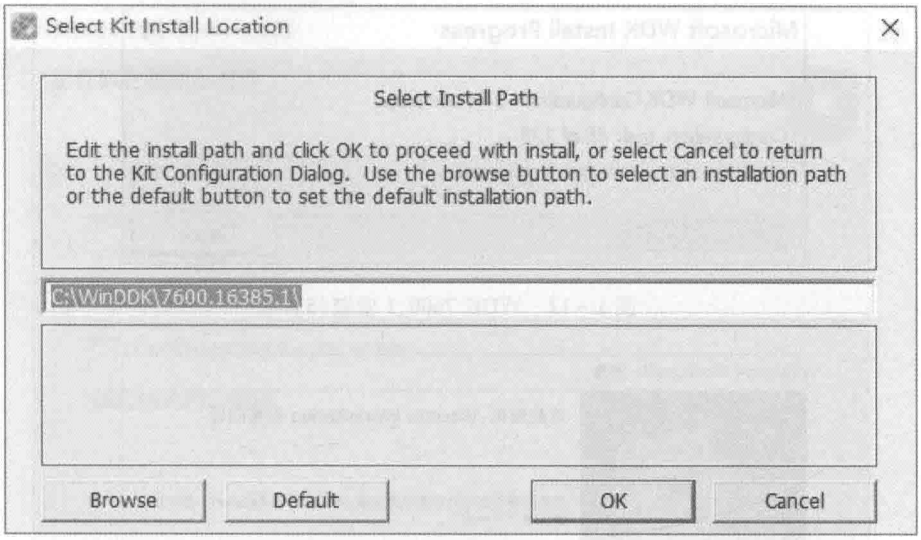

图 1－10　WDK 7600_1 安装(3)

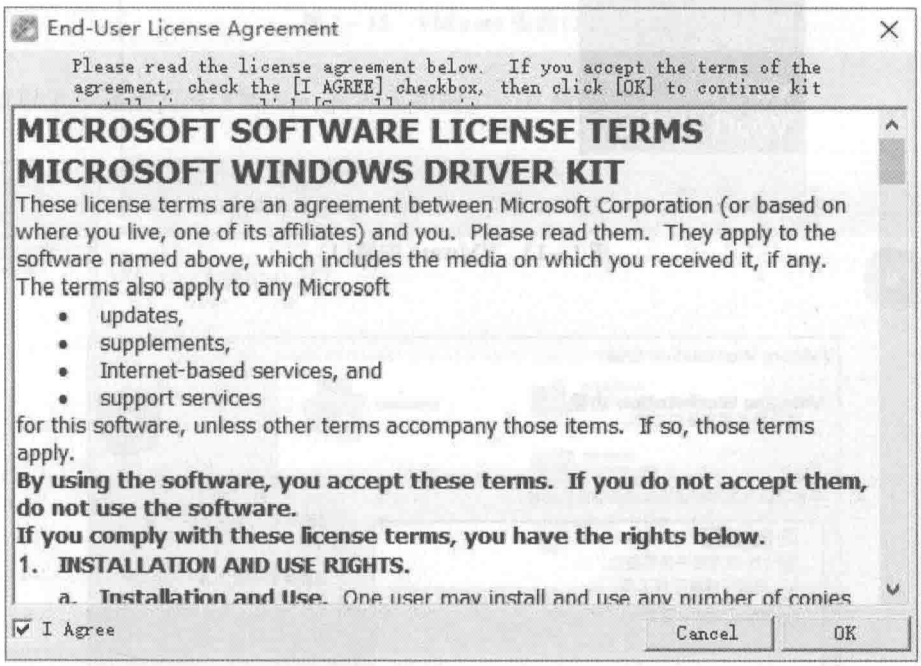

图 1－11　WDK 7600_1 安装(4)

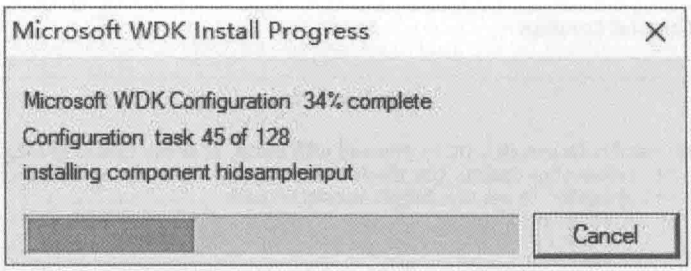

图 1-12 WDK 7600_1 安装(5)

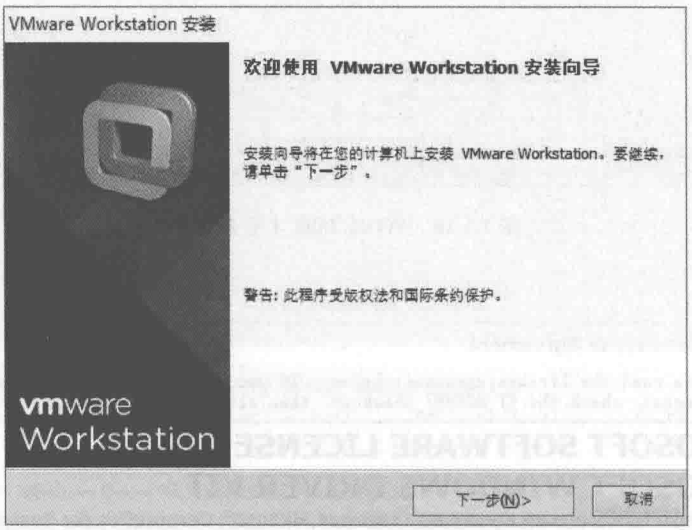

图 1-13 VMware 安装(1)

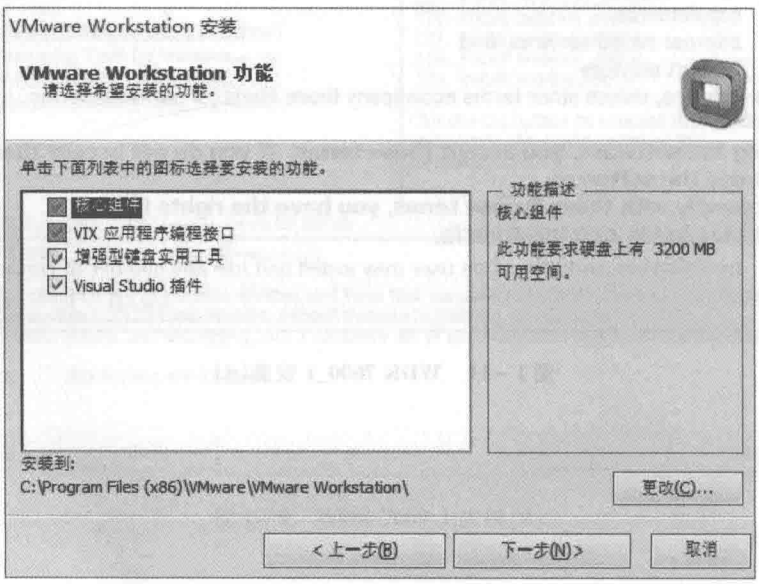

图 1-14 VMware 安装(2)

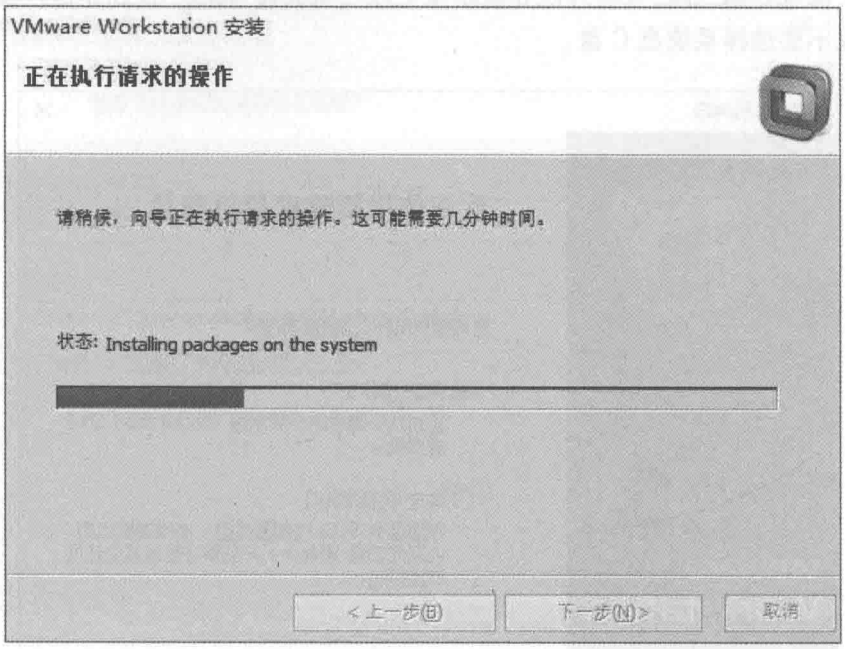

图 1－15　VMware 安装(3)

完成以上步骤后打开 VMware,其界面如图 1－16 所示。

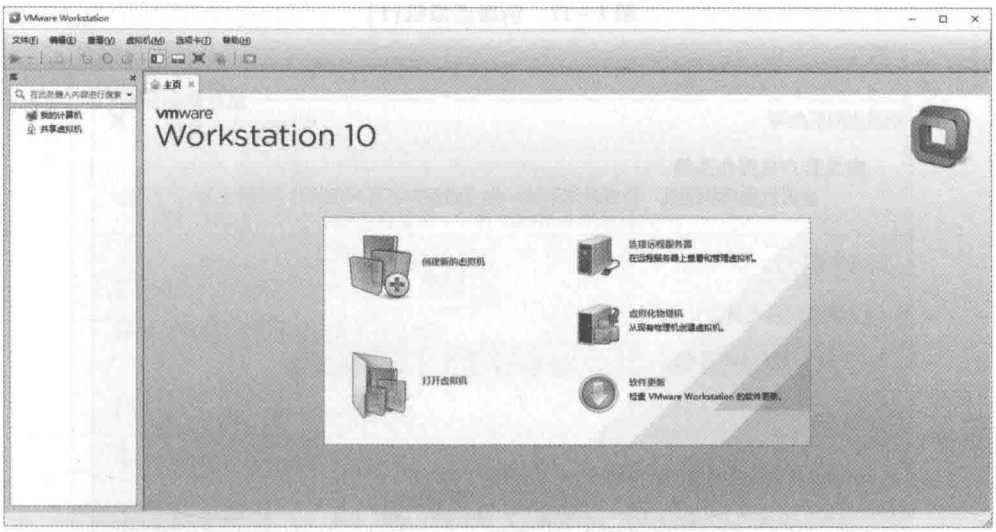

图 1－16　正确安装 VMware 后的效果图

2. 创建虚拟机

VMware 安装完毕之后,在 VMware 的界面点击菜单栏的“文件”→“新建虚拟机”,配置类型选择“典型”即可,然后按照说明选择 Windows 7 (32 位) iso 或者光盘进行安装,如图 1－17至图 1－21 所示。

安装来源选择第二项“安装程序光盘映像文件”,可通过“浏览”找到光盘映像文件。安装位置建议不要选择系统盘 C 盘。

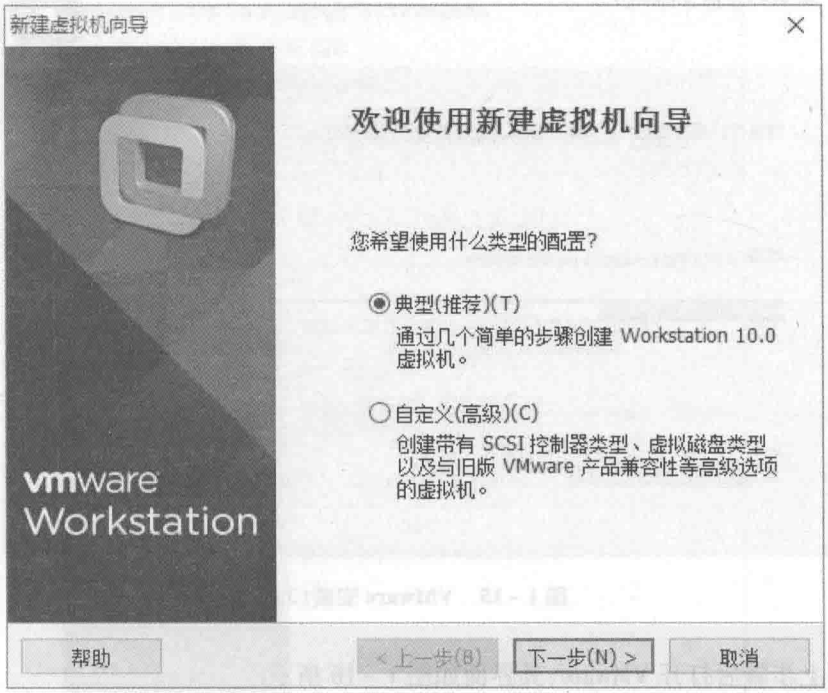

图 1-17　创建虚拟机(1)

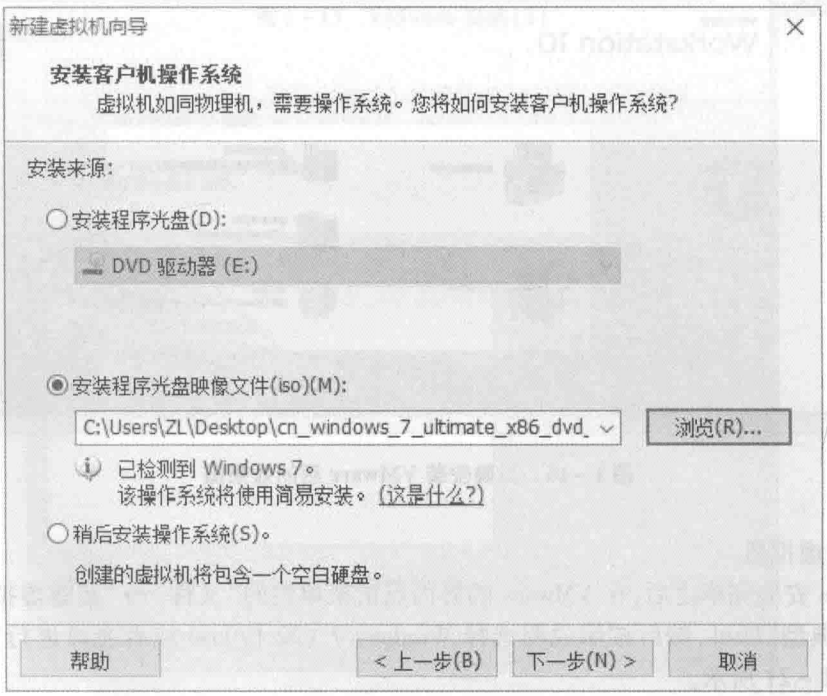

图 1-18　创建虚拟机(2)

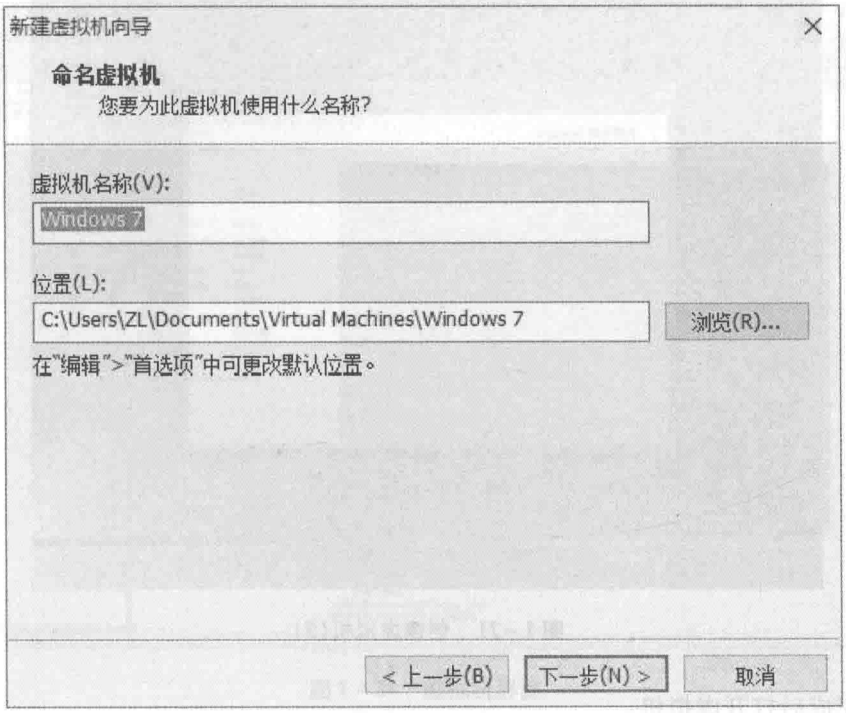

图 1－19　创建虚拟机(3)

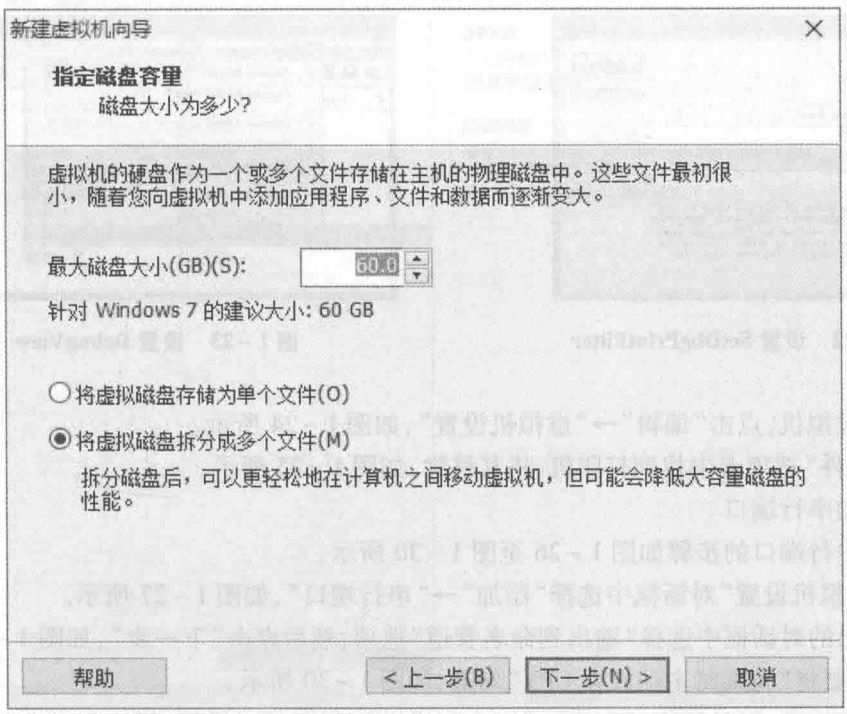

图 1－20　创建虚拟机(4)

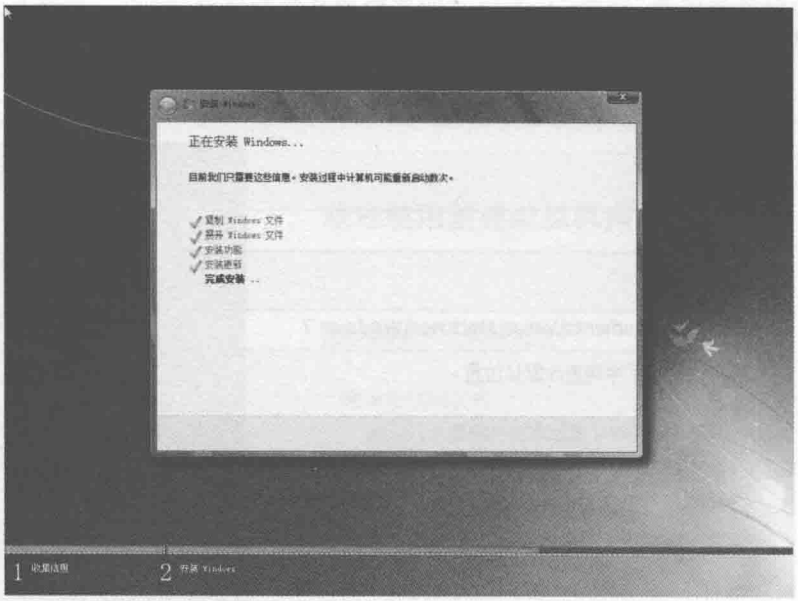

图 1-21　创建虚拟机(5)

安装完成后打开虚拟机。

首先打开 SetDbgPrintFilter,将其值改为 15(十六进制的 F),如图 1-22 所示。

然后打开 DebugView,按照如图 1-23 所示的方式进行设置,将可勾选部分全部勾选。

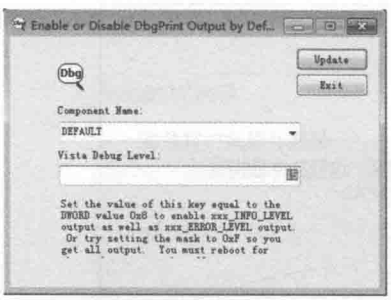

图 1-22　设置 SetDbgPrintFilter

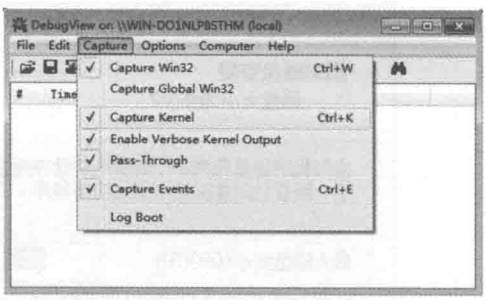

图 1-23　设置 DebugView

关闭虚拟机,点击“编辑”→“虚拟机设置”,如图 1-24 所示。

在“硬件”选项卡中找到打印机,将其移除,如图 1-25 所示。

3. 添加串行端口

添加串行端口的步骤如图 1-26 至图 1-30 所示。

在“虚拟机设置”对话框中选择“添加”→“串行端口”,如图 1-27 所示。

在弹出的对话框中选择“输出到命名管道”选项,然后点击“下一步”,如图 1-28 所示。

注意:要将“轮询时主动放弃 CPV”勾选,如图 1-30 所示。

打开虚拟机,同时按住“Windows”键和“R”键打开运行对话框,键入“msconfig”并点击“确定”按钮,如图 1-31 所示。

选择“引导”→“高级选项”,如图 1-32 所示。勾选“调试”,如图 1-33 所示。