



学电脑从入门到精通



THE SECRETS OF BEING AN EXPERT  
IN COMPUTER FROM A BEGINNER



# 黑客攻防 从入门到精通


## 实战篇

第2版

王叶 李瑞华 孟繁华 编著

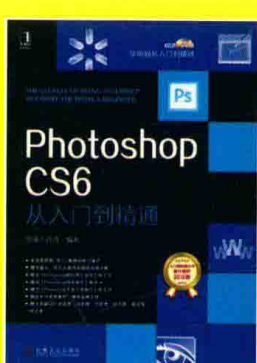
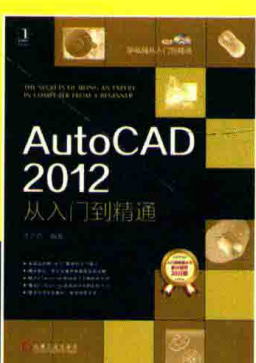
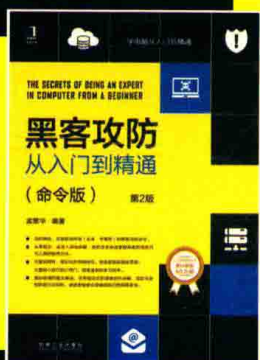
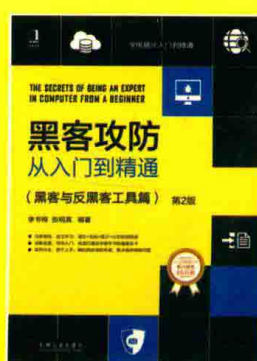
- 简单易学：从易到难、循序渐进，图文并茂、通俗易懂
- 实用性强：网络真实攻防技术、案例+技术的讲解模式
- 技巧与窍门：丰富的攻防技巧与窍门、帮读者答疑解惑，掌握攻防技术



 机械工业出版社  
China Machine Press



# 学电脑从入门到精通



上架指导：计算机/安全

ISBN 978-7-111-65538-1



9 787111 655381 >

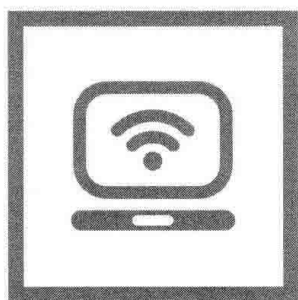
定价：69.00元



投稿热线：(010) 88379604  
读者信箱：hzit@hzbook.com  
客服电话：(010) 88361066 88379833 68326294

华章网站：www.hzbook.com  
网上购书：www.china-pub.com  
数字阅读：www.hzmedia.com.cn

学电脑从入门到精通

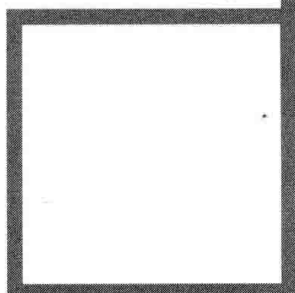
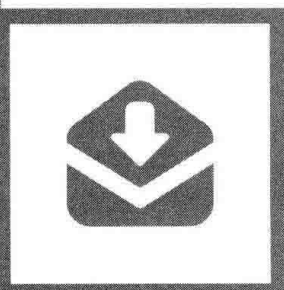
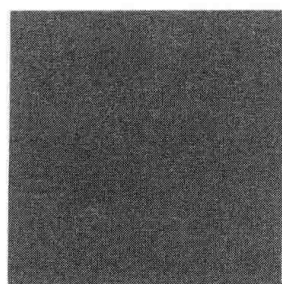


# 黑客攻防

从入门到精通

实战篇 第2版

王叶 李瑞华 孟繁华 编著



 机械工业出版社  
China Machine Press

## 图书在版编目 ( CIP ) 数据

黑客攻防从入门到精通：实战篇 / 王叶, 李瑞华, 孟繁华编著. —2 版. —北京: 机械工业出版社, 2020.5

ISBN 978-7-111-65538-1

I. 黑… II. ①王… ②李… ③孟… III. 黑客 - 网络防御 IV. TP393.081

中国版本图书馆 CIP 数据核字 (2020) 第 081239 号

## 黑客攻防从入门到精通 实战篇 第 2 版

出版发行: 机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码: 100037)

责任编辑: 余 洁

责任校对: 李秋荣

印 刷: 三河市宏图印务有限公司

版 次: 2020 年 6 月第 2 版第 1 次印刷

开 本: 185mm×260mm 1/16

印 张: 21.75

书 号: ISBN 978-7-111-65538-1

定 价: 69.00 元

客服电话: (010) 88361066 88379833 68326294

投稿热线: (010) 88379604

华章网站: [www.hzbook.com](http://www.hzbook.com)

读者信箱: [hzit@hzbook.com](mailto:hzit@hzbook.com)

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光 / 邹晓东



## 华章图书

一本打开的书，  
一扇开启的门，  
通向科学殿堂的阶梯，  
托起一流人才的基石。



# 前言

如今，网上消费、投资、娱乐等已占据了我们的生活的一大部分，如何保证网络账户、密码安全已成为广大用户非常关注的问题，尤其是经常听闻身边好友 QQ 被盗、账号丢失等，防御黑客入侵已经成为一个不得不重视的问题，因而作者编写了此书。

## 本书主要内容

本书共分为 14 章，主要内容如下：

第 1 章：认识黑客并介绍学习黑客攻防前首先要了解的基础知识，包括 IP 地址、端口、黑客常见术语及命令，以及曝光黑客在攻击前做的准备工作——创建虚拟测试环境。

第 2 章：介绍黑客攻击前对信息的扫描与嗅探以及网络监控技巧。

第 3 章：介绍系统常见漏洞攻击与防御技巧。

第 4 章：认识病毒并介绍病毒入侵与防御技巧，同时曝光简单病毒的制作过程。

第 5 章：认识木马并介绍木马的伪装与生成、加壳与脱壳以及木马的清除。

第 6 章：介绍通过入侵检测技术自动检测可疑行为，在系统受到危害前发出警告，防患于未然。

第 7 章：介绍代理和日志清除技术，此为黑客入侵常用的隐藏和清除入侵痕迹的手段。

第 8 章：介绍几种常见的远程控制技术，如今该技术在远程教育、远程协助、远程维护等方向应用较多。

第 9 章：介绍 NTFS 文件、多媒体、Word 文件、光盘等的常见加密 / 解密技术，

以及几种常用的加密 / 解密工具。

第 10 章：介绍常见的网络欺骗方式以及防范方法。

第 11 章：介绍 SQL 注入、网络钓鱼等常见网站攻击手法，并给出了预防措施。

第 12 章：介绍系统和数据的备份与恢复，在系统遭受木马病毒攻击而无法使用时，备份与恢复就能够发挥其作用。

第 13 章：介绍间谍软件的清除和系统清理，以保证系统环境更加安全。

第 14 章：介绍常用购物软件、银行 APP 软件的安全防护措施，以及常用手机安全软件的安装。

## 本书特色

- 简单易懂。本书内容从零起步，由浅入深，适用于初次接触黑客攻防技术的读者。
- 实用性强。本书理论和实例相结合，并配以大量插图，步骤解释明晰，让读者能够一目了然，轻松学习。
- 小技巧和小窍门。帮助读者答疑解惑，提高学习效率。

本书语言简练，内容丰富，并配有大量操作实例，综合作者使用经验和操作心得，可以作为个人学习和了解黑客攻防知识的参考书籍。

最后，感谢广大读者的阅读与支持，鉴于水平有限，书中难免存在疏漏之处，欢迎批评指正。

# 目 录

## 前 言

### 第1章 从零开始认识黑客 / 1

- 1.1 认识黑客 / 2
  - 1.1.1 白帽、灰帽和黑帽黑客 / 2
  - 1.1.2 黑客、红客、蓝客和骇客 / 2
- 1.2 认识 IP 地址 / 2
  - 1.2.1 IP 地址概述 / 2
  - 1.2.2 IP 地址的分类 / 3
- 1.3 认识端口 / 4
  - 1.3.1 端口的分类 / 5
  - 1.3.2 查看端口 / 6
  - 1.3.3 开启和关闭端口 / 7
- 1.4 黑客常用术语与命令 / 11
  - 1.4.1 黑客常用术语 / 11
  - 1.4.2 测试物理网络的 ping 命令 / 13
  - 1.4.3 查看网络连接的 netstat 命令 / 15
  - 1.4.4 工作组和域的 net 命令 / 17
  - 1.4.5 23 端口登录的 telnet 命令 / 20
  - 1.4.6 传输协议 FTP 命令 / 21
  - 1.4.7 查看网络配置的 ipconfig 命令 / 22
- 1.5 在计算机中创建虚拟测试环境 / 22
  - 1.5.1 认识虚拟机 / 23
  - 1.5.2 在 VMware 中新建虚拟机 / 23
  - 1.5.3 在 VMware 中安装操作系统 / 25
  - 1.5.4 安装 VirtualBox / 29

### 第2章 信息的扫描与嗅探 / 31

- 2.1 端口扫描器 / 32
  - 2.1.1 X-Scan / 32
  - 2.1.2 SuperScan / 38
  - 2.1.3 ScanPort / 41

- 2.1.4 网络端口扫描器 / 42
- 2.2 漏洞扫描器 / 43
  - 2.2.1 SSS / 43
  - 2.2.2 Zenmap / 46
- 2.3 常见的嗅探工具 / 49
  - 2.3.1 什么是嗅探器? / 49
  - 2.3.2 捕获网页内容的艾菲网页  
侦探 / 49
  - 2.3.3 SpyNet Sniffer 嗅探器 / 53
  - 2.3.4 网络封包分析软件  
Wireshark / 54
- 2.4 运用工具实现网络监控 / 55
  - 2.4.1 运用长角牛网络监控机实现  
网络监控 / 55
  - 2.4.2 运用 Real Spy Monitor 监控  
网络 / 60

### 第3章

## 系统漏洞入侵与防范 / 65

- 3.1 系统漏洞基础知识 / 66
  - 3.1.1 系统漏洞概述 / 66
  - 3.1.2 Windows 10 系统常见漏洞 / 66
- 3.2 Windows 服务器系统入侵 / 67
  - 3.2.1 入侵 Windows 服务器流程  
曝光 / 67
  - 3.2.2 NetBIOS 漏洞攻防 / 68
- 3.3 DcomRpc 溢出工具 / 73
  - 3.3.1 DcomRpc 漏洞描述 / 73
  - 3.3.2 DcomRpc 入侵 / 75
  - 3.3.3 DcomRpc 漏洞防范方法 / 75
- 3.4 用 MBSA 检测系统漏洞 / 77
  - 3.4.1 MBSA 的安装设置 / 78
  - 3.4.2 检测单台计算机 / 79
  - 3.4.3 检测多台计算机 / 80
- 3.5 手动修复系统漏洞 / 81
  - 3.5.1 使用 Windows Update 修复  
系统漏洞 / 81
  - 3.5.2 使用 360 安全卫士修复  
系统漏洞 / 82

### 第4章

## 病毒入侵与防御 / 84

- 4.1 病毒知识入门 / 85
  - 4.1.1 计算机病毒的特点 / 85
  - 4.1.2 病毒的三个基本结构 / 85
  - 4.1.3 病毒的工作流程 / 86
- 4.2 简单病毒制作过程曝光 / 87
  - 4.2.1 Restart 病毒 / 87
  - 4.2.2 U 盘病毒 / 91
- 4.3 宏病毒与邮件病毒防范 / 93
  - 4.3.1 宏病毒的判断方法 / 93
  - 4.3.2 防范与清除宏病毒 / 94

- 4.3.3 全面防御邮件病毒 / 95
- 4.4 网络蠕虫病毒分析和防范 / 95
  - 4.4.1 网络蠕虫病毒实例分析 / 96
  - 4.4.2 网络蠕虫病毒的全面防范 / 96
- 4.5 预防和查杀病毒 / 98
  - 4.5.1 掌握防范病毒的常用措施 / 98
  - 4.5.2 使用杀毒软件查杀病毒 / 99

## 第5章 木马入侵与防御 / 101

- 5.1 认识木马 / 102
  - 5.1.1 木马的发展历程 / 102
  - 5.1.2 木马的组成 / 102
  - 5.1.3 木马的分类 / 103
- 5.2 木马的伪装与生成 / 104
  - 5.2.1 木马的伪装手段 / 104
  - 5.2.2 使用文件捆绑器 / 105
  - 5.2.3 自解压木马制作流程曝光 / 108
  - 5.2.4 CHM 木马制作流程曝光 / 110
- 5.3 木马的加壳与脱壳 / 113
  - 5.3.1 使用 ASPack 进行加壳 / 113
  - 5.3.2 使用 PE-Scan 检测木马是否加壳 / 115
  - 5.3.3 使用 UnASPack 进行脱壳 / 116
- 5.4 木马清除软件的使用 / 117
  - 5.4.1 用木马清除专家清除木马 / 117
  - 5.4.2 在 Windows 进程管理器中管理进程 / 122

## 第6章 入侵检测技术 / 126

- 6.1 入侵检测概述 / 127
- 6.2 基于网络的入侵检测系统 / 127
  - 6.2.1 包嗅探器和网络监视器 / 128
  - 6.2.2 包嗅探器和混杂模式 / 128
  - 6.2.3 基于网络的入侵检测：  
包嗅探器的发展 / 128
- 6.3 基于主机的入侵检测系统 / 129
- 6.4 基于漏洞的入侵检测系统 / 130
  - 6.4.1 运用流光进行批量主机扫描 / 130
  - 6.4.2 运用流光进行指定漏洞扫描 / 133
- 6.5 萨客嘶入侵检测系统 / 134
  - 6.5.1 萨客嘶入侵检测系统简介 / 134
  - 6.5.2 设置萨客嘶入侵检测系统 / 135
  - 6.5.3 使用萨客嘶入侵检测系统 / 138
- 6.6 利用 WAS 检测网站 / 140
  - 6.6.1 WAS 简介 / 141
  - 6.6.2 检测网站的承受压力 / 141
  - 6.6.3 进行数据分析 / 144

## 第7章 代理与日志清除技术 / 146

- 7.1 代理服务器软件的使用 / 147
  - 7.1.1 利用“代理猎手”找代理 / 147
  - 7.1.2 用 SocksCap32 设置动态代理 / 152
- 7.2 日志文件的清除 / 154
  - 7.2.1 手工清除服务器日志 / 154
  - 7.2.2 使用批处理清除远程主机日志 / 157

## 第8章 远程控制技术 / 159

- 8.1 远程控制概述 / 160
  - 8.1.1 远程控制技术发展历程 / 160
  - 8.1.2 远程控制技术原理 / 160
  - 8.1.3 远程控制的应用 / 160
- 8.2 远程桌面连接与协助 / 161
  - 8.2.1 Windows 系统的远程桌面连接 / 161
  - 8.2.2 Windows 系统远程关机 / 162
- 8.3 利用“任我行”软件进行远程控制 / 164
  - 8.3.1 配置服务器端 / 164
  - 8.3.2 通过服务器端程序进行远程控制 / 165
- 8.4 有效防范远程入侵和远程监控 / 167
  - 8.4.1 防范 IPC\$ 远程入侵 / 167
  - 8.4.2 防范注册表和 Telnet 远程入侵 / 174

## 第9章 加密与解密技术 / 177

- 9.1 NTFS 文件系统加密和解密 / 178
  - 9.1.1 加密操作 / 178
  - 9.1.2 解密操作 / 178
  - 9.1.3 复制加密文件 / 179
  - 9.1.4 移动加密文件 / 179
- 9.2 光盘的加密与解密技术 / 179
  - 9.2.1 使用 CD-Protector 软件加密光盘 / 180
  - 9.2.2 加密光盘破解方式曝光 / 181
- 9.3 用“私人磁盘”隐藏大文件 / 181

- 9.3.1 “私人磁盘”的创建 / 182
- 9.3.2 “私人磁盘”的删除 / 183
- 9.4 使用 Private Pix 为多媒体文件加密 / 183
- 9.5 用 ASPack 对 EXE 文件进行加密 / 186
- 9.6 利用“加密精灵”加密 / 187
- 9.7 软件破解实用工具 / 188
  - 9.7.1 十六进制编辑器 HexWorkshop / 188
  - 9.7.2 注册表监视器 RegShot / 191
- 9.8 MD5 加密破解方式曝光 / 192
  - 9.8.1 本地破解 MD5 / 192
  - 9.8.2 在线破解 MD5 / 193
  - 9.8.3 PKmd5 加密 / 194
- 9.9 给系统桌面加把超级锁 / 194
  - 9.9.1 生成后门口令 / 194
  - 9.9.2 设置登录口令 / 196
  - 9.9.3 如何解锁 / 196
- 9.10 压缩文件的加密和解密 / 197
  - 9.10.1 用“好压”加密文件 / 197
  - 9.10.2 RAR Password Recovery / 198
- 9.11 Word 文件的加密和解密 / 199
  - 9.11.1 Word 自身功能加密 / 199
  - 9.11.2 使用 Word Password Recovery 解密 Word 文档 / 202
- 9.12 宏加密和解密技术 / 203

## 第10章

## 网络欺骗与安全防范 / 206

- 10.1 网络欺骗和网络管理 / 207
  - 10.1.1 网络钓鱼——Web 欺骗 / 207
  - 10.1.2 WinArpAttacker——ARP 欺骗 / 212
  - 10.1.3 利用网络守护神保护网络 / 214
- 10.2 邮箱账户欺骗与安全防范 / 218
  - 10.2.1 黑客常用的邮箱账户欺骗手段 / 218
  - 10.2.2 邮箱账户安全防范 / 218
- 10.3 使用蜜罐 KFSensor 诱捕黑客 / 221
  - 10.3.1 蜜罐的概述 / 222
  - 10.3.2 蜜罐设置 / 223
  - 10.3.3 蜜罐诱捕 / 225
- 10.4 网络安全防范 / 225
  - 10.4.1 网络监听的防范 / 225
  - 10.4.2 金山贝壳 ARP 防火墙的使用 / 226

## 第11章 网站攻击与防范 / 228

- 11.1 认识网站攻击 / 229
  - 11.1.1 拒绝服务攻击 / 229
  - 11.1.2 SQL 注入 / 229
  - 11.1.3 网络钓鱼 / 229
  - 11.1.4 社会工程学 / 229
- 11.2 Cookie 注入攻击 / 230
  - 11.2.1 Cookies 欺骗及实例曝光 / 230
  - 11.2.2 Cookies 注入及预防 / 231
- 11.3 跨站脚本攻击 / 232
  - 11.3.1 简单留言本的跨站漏洞 / 233
  - 11.3.2 跨站漏洞的利用 / 236
  - 11.3.3 对跨站漏洞的预防措施 / 242
- 11.4 “啊 D” SQL 注入攻击曝光 / 244

## 第12章 系统和数据的备份与恢复 / 251

- 12.1 备份与还原操作系统 / 252
  - 12.1.1 使用还原点备份与还原系统 / 252
  - 12.1.2 使用 GHOST 备份与还原系统 / 254
- 12.2 使用恢复工具来恢复误删除的数据 / 262
  - 12.2.1 使用 Recuva 来恢复数据 / 262
  - 12.2.2 使用 FinalData 来恢复数据 / 266
  - 12.2.3 使用 FinalRecovery 来恢复数据 / 270
- 12.3 备份与还原用户数据 / 273
  - 12.3.1 使用驱动精灵备份和还原驱动程序 / 273
  - 12.3.2 备份和还原 IE 浏览器的收藏夹 / 277
  - 12.3.3 备份和还原 QQ 聊天记录 / 280
  - 12.3.4 备份和还原 QQ 自定义表情 / 282
  - 12.3.5 备份和还原微信聊天记录 / 285

## 第13章 间谍软件的清除和系统清理 / 290

- 13.1 认识流氓软件与间谍软件 / 291
  - 13.1.1 认识流氓软件 / 291
  - 13.1.2 认识间谍软件 / 291
- 13.2 流氓软件防护实战 / 291
  - 13.2.1 清理浏览器插件 / 291
  - 13.2.2 流氓软件的防范 / 294
  - 13.2.3 金山清理专家清除恶意软件 / 297
- 13.3 间谍软件防护实战 / 298
  - 13.3.1 间谍软件防护概述 / 298
  - 13.3.2 用 Spy Sweeper 清除间谍软件 / 299
  - 13.3.3 通过事件查看器抓住“间谍” / 303
  - 13.3.4 使用 360 安全卫士对计算机进行防护 / 307
- 13.4 清除与防范流氓软件 / 311
  - 13.4.1 使用 360 安全卫士清理流氓软件 / 311
  - 13.4.2 使用金山卫士清理流氓软件 / 314
  - 13.4.3 使用 Windows 流氓软件清理大师清理流氓软件 / 317
  - 13.4.4 清除与防范流氓软件的常见措施 / 318
- 13.5 常见的网络安全防护工具 / 319
  - 13.5.1 AD-Aware 让间谍程序消失无踪 / 319
  - 13.5.2 浏览器绑架克星 HijackThis / 321

## 第14章 如何保护手机财产安全 / 326

- 14.1 账号安全从设置密码开始 / 327
  - 14.1.1 了解弱密码 / 327
  - 14.1.2 弱密码的危害 / 327
  - 14.1.3 如何合理进行密码设置 / 327
- 14.2 常用购物软件的安全防护措施 / 328
  - 14.2.1 天猫账号的安全设置 / 328
  - 14.2.2 支付宝账号的安全设置 / 330
- 14.3 常用银行 APP 软件的安全防护措施 / 332
  - 14.3.1 建设银行账号的安全设置 / 332
  - 14.3.2 工商银行账号的安全设置 / 333
- 14.4 常用手机安全软件 / 335
  - 14.4.1 360 手机卫士常用安全设置 / 335
  - 14.4.2 腾讯手机管家常用安全设置 / 335

# 第 1 章

## 从零开始认识黑客

主要内容:

- 认识黑客
- 认识 IP 地址
- 认识端口
- 黑客常见术语与命令
- 在计算机中创建虚拟测试环境

## 1.1 认识黑客

### 1.1.1 白帽、灰帽和黑帽黑客

自 1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面与网络的结合也越来越紧密，网络也由此逐渐成为人们生活的一部分。可以说，信息时代已经到来，信息作为物质和能量以外维持人类社会运转的第三资源，正体现出越来越重要的作用，它是未来生活中的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现。

黑客的原本含义是指拥有熟练计算机技术的人，但现今大部分的媒体提到的“黑客”指计算机侵入者。其中黑客又可分为白帽黑客、灰帽黑客和黑帽黑客。

白帽黑客是指有能力破坏计算机安全但不具恶意目的的黑客。白帽子一般有清楚定义的道德规范，并常常试图同企业合作来改善被发现的安全弱点。

灰帽黑客是指对于伦理和法律暧昧不清的黑客。

黑帽黑客这个词自 1983 年开始流行，采用了 safe cracker 的解释，并且理论化为一个犯罪和黑客的混合语。

### 1.1.2 黑客、红客、蓝客和骇客

黑客：最早源自英文 hacker，他们都是水平高超的计算机专家，尤其指程序设计人员，是一个统称。

红客：维护国家利益的黑客，他们热爱自己的祖国、民族、和平，极力维护国家安全与尊严。

蓝客：信仰自由、提倡爱国主义的黑客，用自己的力量来维护网络的和平。

骇客：是“Cracker”的音译，就是“破解者”的意思，从事恶意破解商业软件、恶意入侵别人的网站等活动。

## 1.2 认识 IP 地址

在网络中，每一台主机也有一个“地址”，这就是 IP 地址。因此，如果想要攻击某个网络主机，就要先确定该目标主机的域名或 IP 地址。

### 1.2.1 IP 地址概述

所谓 IP 地址就是一种主机编址方式，给每个连接在 Internet 上的主机分配一个 32bit(位)

地址，也称为网际协议地址。

按照 TCP/IP (Transport Control Protocol/Internet Protocol, 传输控制协议 / 网际协议) 的规定, IP 地址用二进制来表示, 每个 IP 地址长 32bit, 换算成字节就是 4 字节。例如一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”, 这么长的地址人们处理起来很费劲。为了方便使用, IP 地址经常被写成十进制的形式, 中间使用符号“.”来分为不同的字节, 即用 XXX.XXX.XXX.XXX 的形式来表现, 每组 XXX 代表小于或等于 255 的十进制数, 例如 192.168.38.6, 这显然比二进制的 1 或 0 容易记忆多了。

一条完整的 IP 地址信息, 通常应包括 IP 地址、子网掩码、默认网关和 DNS 等 4 部分内容。只有四者协同工作时, 用户才可以访问 Internet 并被 Internet 中的计算机所访问(采用静态 IP 地址接入 Internet 时, ISP 应当为用户提供全部 IP 地址信息)。

### 1. IP 地址

企业网络使用的合法 IP 地址由提供 Internet 接入的服务商 (ISP) 分配, 私有 IP 地址则可以由网络管理员自由分配。但网络内部所有计算机的 IP 地址都不能相同, 否则会发生 IP 地址冲突, 导致网络连接失败。

### 2. 子网掩码

子网掩码要与 IP 地址结合使用, 其主要作用有两个, 一是用于确定地址中的网络号和主机号, 二是用于将一个大 IP 网络划分为若干个小的子网络。

### 3. 默认网关

一台主机如果找不到可用的网关, 就把数据包发送给默认指定的网关, 由这个网关来处理数据包。从一个网络向另一个网络发送信息, 也必须经过一道“关口”, 这道关口就是网关。

### 4. DNS

DNS 服务用于将用户的域名请求转换为 IP 地址。如果企业网络没有提供 DNS 服务, 则 DNS 服务器的 IP 地址应当指向 ISP 的 DNS 服务器。如果企业网络自己提供了 DNS 服务, 则 DNS 服务器的 IP 地址就是内部 DNS 服务器的 IP 地址。

## 1.2.2 IP 地址的分类

互联网中的每个接口有一个唯一的 IP 地址与其对应, 该地址具有一定的结构, 一般情况下, IP 地址可以分为 5 大类, 即 A 类、B 类、C 类、D 类以及 E 类。

这些 32 位的地址通常写成 4 个十进制的数, 其中每个整数对应一字节。这种表示方法称为“点分十进制表示法”(dotted decimal notation)。

### 1. A 类 IP 地址

A 类 IP 地址由 1 字节的网络地址和 3 字节的主机地址组成, 网络地址的最高位必须是“0”。可用的 A 类网络有 126 个, 每个网络能容纳 1 亿多个主机(网络号不能为 127, 因为该网络号被保留用作回路及诊断功能), 地址范围为 1.0.0.1 ~ 126.155.255.254。