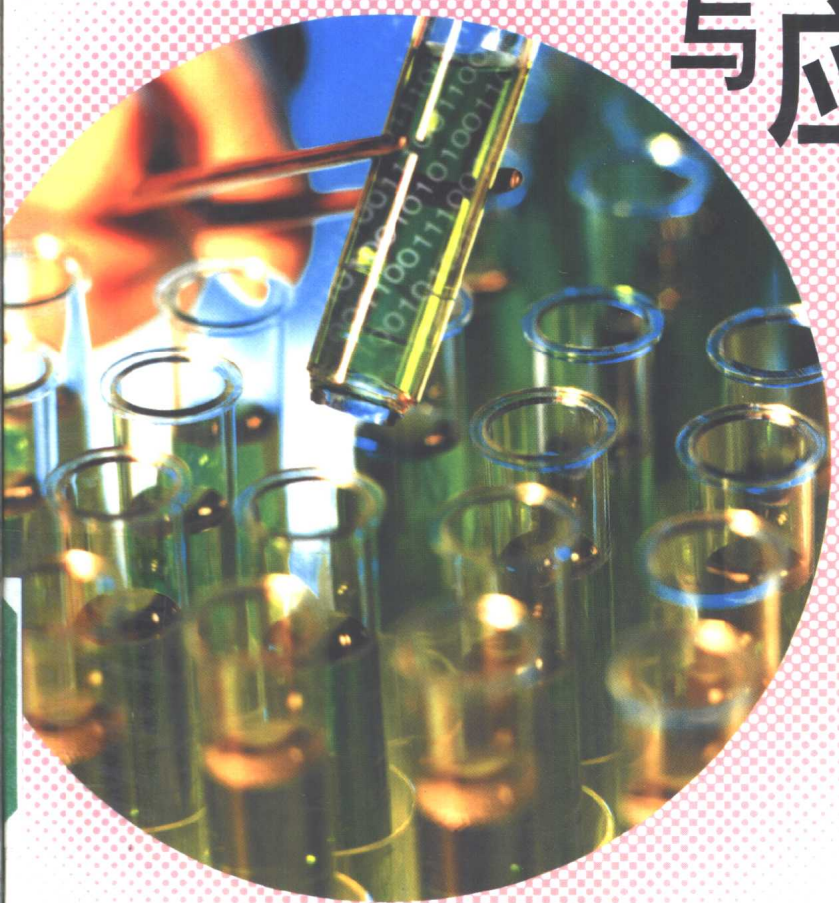
Delphi

网络通信协议分析与应用实现



钟军　汪晓平　等　编著

附光盘
CD-ROM

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

Delphi

网络通信协议分析与应用实现

钟军　汪晓平　等　编著

人民邮电出版社

图书在版编目（CIP）数据

Delphi 网络通信协议分析与应用实现/钟军，汪晓平编著. —北京：人民邮电出版社 2003.1
ISBN 7-115-11003-4

Ⅰ. D... Ⅱ. ①钟... ②汪... Ⅲ. 软件工具—程序设计 Ⅳ. TP311.56

中国版本图书馆 CIP 数据核字（2002）第 105851 号

内容提要

本书介绍如何利用 Delphi 开发网络与通信应用程序，本书主要针对目前流行的 FTP、HTTP、E-mail、Telnet、网络监控、Modem 串口通信编程、拨号网络编程、传真编程等 Internet 协议与网络通信高级编程开发进行详细的讲解，并结合大量的实例使读者能够深入的了解各种网络应用程序的开发技巧。

本书适合中高级 Delphi 程序员阅读、参考。

Delphi 网络通信协议分析与应用实现

◆ 编　　著　钟　军　汪晓平　等
责任编辑　张立科

◆ 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
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：31
字数：755 千字　　2003 年 1 月第 1 版
印数：1-5 000 册　　2003 年 1 月北京第 1 次印刷

ISBN 7-115-11003-4/TP・3303

定价：52.00 元（附光盘）

前　言

随着版本的提高 Delphi 对网络应用程序开发提供了越来越全面的支持。特别是到了 Delphi 6，从基本的网络应用开发控件，到高级的网络应用控件，如提供 SMTP、POP3 控件等，加上 Delphi 开发的简明、灵活，更强的扩展性等特点，成为一种被广泛使用的前端开发平台。

但是目前市场上与 Delphi 网络与通信开发有关的书籍很少，基本上都是停留在介绍对 Delphi 提供的现有网络控件进行的网络通信编程的阶段，对于一些高级网络的应用开发介绍的很少，相关的理论介绍就更少了。针对这个缺憾，本书着重介绍 Delphi 网络与通信的高级开发，深入剖析网络与通信编程的相关理论，并且在每一章都提供了多个高级开发实例，使得读者在研究实例的过程中更好地掌握和理解这些理论知识。

本书主要面向具有一定 Delphi 网络与通信编程基础并希望学习较高层次编程技术的读者，主要涉及到网络开发与通信两方面的内容，如常用的 Internet 协议开发理论与实例，Modem 串口通信理论与实例，传真开发理论与实例等。本书涉及的理论内容及其实例如下：

第 1 章：Delphi 网络编程基础知识

介绍网络编程的基础知识、以及 Delphi 网络开发的方法、控件等。

第 2 章：基本网络编程实例

介绍一些 Delphi 的基本网络编程，如获取 IP 地址、获取子网掩码、获取网卡信息等应用小实例，读者可以在前面这两章中进行网络编程的热身准备。

第 3 章：FTP 高级编程

FTP 是网络文件传输的最主要方式之一，本章介绍了 FTP 协议以及怎样开发应用 FTP 协议进行网络文件传输，包括 FTP 命令，FTP 会话方式，同时结合了几个强大功能的实例：FTP 客户端与 FTP 服务器。从 FTP 传输的两个方面来理解 FTP 高级编程的理论与内容。

第 4 章：HTTP 高级开发

HTTP 是最常用的协议之一。本章首先介绍了 HTTP 的理论，同时介绍了几个实例，这些实例的功能都很强大。如使用 HTTP 进行网络下载，实现 HTTP Web 服务器、HTTP 代理服务器等。同时介绍了 Netant 网络下载软件的实现方法。

第 5 章：Telnet 高级编程

上过 BBS 的读者也许都想知道怎样才能编写这样的软件。本章介绍了 BBS 客户端使用的协议——Telnet，通过学习这一章，读者可以编写自己的 BBS 程序。

第 6 章：E-mail 协议及高级编程

E-mail 是最常用的网络交流工具。已有的 E-mail 的软件很多，比如 Foxmail，Outlook 等，读者也可以编写自己的 E-mail 程序。本章从 E-mail 通信的基本原理开始，介绍了 SMTP 发送 E-mail、POP3 接收 E-mail 的原理与实现。同时针对于发送附件与解析附件所用的编码解码算法以及乱码的出现，进行了详细的介绍。

第 7 章：网络监控与流量统计与资源搜索

这一章介绍了两个方面的内容：网络监控与流量统计、局域网资源搜索。网络监控对连接到本地机的 TCP/IP 连接进行实时的跟踪，同时能够分析当前的网络数据流量。局域网资源

搜索可以搜索局域网内的资源，包括共享文件、打印机等内容。

第 8 章：Modem 串口通信编程

Modem 编程与串口编程是紧密联系的。本章介绍了 Modem 的常用指令，串口的开发方法。同时介绍了一个商业上使用的一个具有断点续传的 Modem 文件传输软件的实现方法。

第 9 章：拨号网络编程

RAS 拨号是 Windows 提供的一个网络接入服务。本章介绍了 RAS 的编程方法，包括对拨号网络的电话簿、拨号连接、挂断、以及获取拨号网络的动态 IP 等。

第 10 章：传真高级编程

计算机可以通过 Modem 发送与接收传真，这方面的软件并不少见，Delphi 程序员也能够自己编程实现。本章就传真编程所涉及的内容，如传真通信协议、传真的分类以及命令、传真的会话实例描述、传真图像编码等都进行了详细的介绍，最后还给出了一个发送传真的实例。

本书的光盘包括了涉及实例的全部源代码和可执行文件，并且所有实例均在 Delphi 6 环境下调试实现。所有案例的完整程序代码均可在该光盘中找到。

本书由钟军、汪晓平合作编写而成，此外参与编写工作的还有张宏林、肖洪伟、李廷文、张增强、王洪涛、吴继刚、周学明、李闽溟、黄沙、宣小平、但正刚、张文毅、张小磊、胡昱、范国平、陈晓鹏、王凯封、潘邦传、王锐、闫卫东、赵明华、许福、施新刚、郑刚、李现勇、谭思亮、邹超群、郭瑞军、杨枝灵、彭坷珂、赵苏琦、徐建军、胡伟、刘江、王茹、闾海荣、刘理、谭春华、张益贞、刘韬、杨茂林、董晓宇、王三暖、刘星等，在此一并表示感谢。

由于作者水平有限，书中难免有不足和疏忽之处，恳请读者朋友和各位同仁批评指正，联系方法：zhanglike@ptpress.com.cn。

编者

2002 年 12 月

目 录

第 1 章　Delphi 网络编程基础知识

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）是发展至今最成功的通信协议之一，它起源于 20 世纪 60 年代末美国政府资助的一个分组交换网络研究项目，它允许分布在各地的装着完全不同操作系统的计算机互相通信。随着计算机的普及，TCP/IP 以其开放性的特点，成为了 Internet 的基础，并通过 Internet 把全世界数以千万的计算机连接在了一起。

千里之行，始于足下，一个程序员要想自如地进行网络编程，对 TCP/IP 底层协议的结构、基本概念有个充分的了解是必不可少的。本章力求通过简明的论述，使读者对 TCP/IP 有个整体的把握，为后续章节的学习作好准备。

1.1　TCP/IP

1.1.1　TCP/IP 结构

每一层负责的功能介绍如下：

- 链路层：有时被称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡，它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。该层包含的协议有 ARP（地址转换协议）和 RARP（反向地址转换协议）。
- 网络层：有时也被称为互联网层，负责分组在网络中的活动，包括 IP（网际协议）、ICMP（Internet 互联网控制报文协议）以及 IGMP 协议（Internet 组管理协议）。
- 传输层：该层主要为两台主机上的应用程序提供端到端的数据通信，它分为两个不同的协议，即 TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 提供端到端的质量保证的数据传输，该层负责数据的分组、质量控制和超时重发等，对于应用层来说，就可以忽略这些工作。UDP 则只提供简单的把数据报从一端发送到另一端，至于数据是否到达或按时到达、数据是否损坏都必须由应用层来做。这两种协议各有各自的用途，前者可用于面向连接的应用，而后者则在及时性服务中起着重要的作用，如网络多媒体通信等。
- 应用层：该层负责处理实际的应用程序细节，包括大家都十分熟悉的 Telnet（电子公告板）、HTTP（超文本传输协议）、SMTP（简单邮件传输协议）、FTP（文件传输协议）和 SNMP（简单网络管理协议）等著名协议。

为了更好地理解 TCP/IP 的四层结构，下面通过一个具体的示例对其进行说明，示例的网络结构如图 1-1 所示。

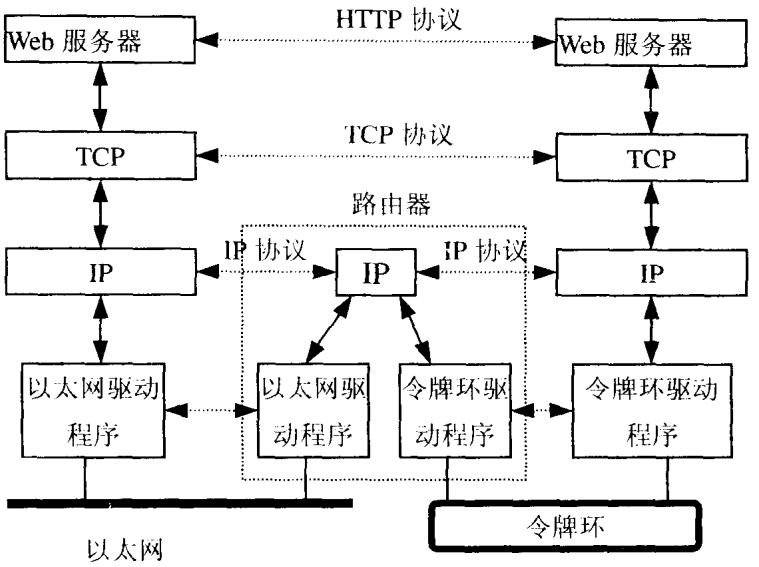


图 1-1 通过 TCP/IP 和路由器连接的两个网络

在图 1-1 所示的系统中，两个网络通过路由器互相连接。路由器可以用来把以太网、令牌环、点对点链接和 FDDI（光纤分布式数据接口）等不同的网络连接到一起。

协议的各个层对上一层是透明的，也就是说，应用层只负责应用程序之间的通信规则，完全不必理会数据是怎样在网络中传输，也不必理会它怎样接入网络。而对于链路层来说，它完全不需要知道正在传送的是什么数据，只需要负责传输就行了。

这里顺便介绍一下网桥、路由器和网关的差别。网桥是一种在链路层将不同类型的局域网连接成一个更大的局域网的网络设备，路由器则是在网络层实现该功能，而网关是指连接不同协议族的进程（例如 TCP/IP、IBM 公司的 SNA），它为某个特定的应用程序（常常是电子邮件或文件传输）服务。

1.1.2 应用层协议

应用层的协议是平时使用最广泛的协议，这层的每个协议都由两部分组成：客户程序和服务程序。程序通过服务器与客户机的交互来工作。

1. Telnet 协议

Telnet 是网络虚拟终端协议的一个典型例子，该协议允许用户通过 Internet 登录到远程计算机中。客户程序需要自己实现 Telnet 协议，同时在某些键以及显示的特性上，不同的终端类型定义是不一样的，目前的大多数终端支持 DEC 的 VT100 终端类型。在进行 Telnet 协议的实现时，工作量最大的还在于使自己的客户程序适应不同的终端类型上。

2. FTP

FTP 的全称是 File Transfer Protocol，即文件传输协议。该协议，要求使用者是经过授权的用户，从而使文件的访问具有一定的安全限制。由于 FTP 口令在网络上传输的是明文的，因此一旦被监听泄密就会威胁到系统安全。许多站点也提供匿名 FTP 服务（Anonymous FTP），

在这类站点上，通常的登录用户名为 anonymous，口令按照惯例是 guest，也有可能为用户的 E-mail 地址，当然提供一个假的地址也可以通过审查。

使用 FTP 可以在提供 FTP 功能的服务器上进行文件检索与传送等操作。经常使用的 FTP 客户端软件包括 CuteFtp，LeapFtp 等。

3. HTTP

HTTP 的全称是 Hypertext Transfer Protocol，超文本传输协议，是 WWW 服务程序所用的协议。也是目前在 Internet 中使用最广泛的协议。著名的 HTTP 客户端包括 IE（Internet Explorer），以及 Netscape 公司的 Netscape Communicator 和 Netscape Nevigator 等，还有众多的如 Opera 这类出色而小巧的 WWW 浏览器。

4. SMTP 与 POP3

SMTP（Simple Mail Transfer Protocol），即简单邮件传送协议。POP3（Post Office Protocol 3），即邮局协议。通过这两个协议就可以实现 E-mail 的收发功能。

目前国内使用最广泛的电子邮件客户端中，Foxmail 就是由个人开发的，使用的开发工具是 Delphi。

5. DNS

DNS（Domain Name Serivce），即域名服务。它实现了由主机名到 IP 地址的映射功能。

1.1.3 传输层协议

传输层协议的功能是建立并且维护连接，这些协议主要是保证主机间的数据传输的安全性。在这个层中定义了两个协议：TCP 和 UDP。

1. TCP

TCP 的全称是 Transmission Control Protocal，即传输控制协议。在网络通信传输机制中，它属于“面向连接，可靠传输”的类型。这一点如果和 UDP 进行比较就会看得比较清楚。面向连接的传输意味着在进行通信以前，需要在两个系统之间建立逻辑连接，在每个数据传输的过程中都需要进行应答以保证数据包的完整。这种方法需要的网络开销较大，但可以保证数据传输的可靠性。

在常见的上层协议中，Telnet、FTP、SMTP、HTTP 等都是使用 TCP 作为基础的，而一些简单的协议如 Echo（一种简单的回显服务，即客户端会从服务器端接受到自己的发送包的拷贝），则可以使用 TCP 也可以使用 UDP。

2. UDP

UDP 的全称是 User Datagram Protocol，即用户数据报协议。它属于“面向无连接，不可靠传输“的类型。该协议只负责接受和传送由上层协议传递的消息，它本身不做任何检测、修改和应答，上层协议需要自己处理这些事务。

UDP 中，每个数据包成为“数据报”，它的包头只包括 4 个域，主要是地址信息与包的长度和校验信息。与此对应，TCP 包的头信息有十多个域。因此它的网络开销一般要小于 TCP。

由于 UDP 在传送数据过程中没有建立连接，而且不进行检查，因此在优良的网络环境中，其工作的效率较 TCP 要高。目前使用 UDP 工作的软件主要是 OICQ。由于 UDP 自身的特点，也同时成为了网络广播的首选协议。传统的 NFS（Net File System，网络文件系统）使用 UDP，当然从 NFS v30 版本开始同时支持 TCP 与 UDP。

1.1.4 网络层协议

网络层协议的主要功能是负责数据的传输、在不同网络和系统间寻找路由、分段和重组数据报文，其次就是进行设备寻址。

这一层中的协议包括 IP、ICMP、ARP 还有 RARP，这些协议的功能见后讨论。

1. IP

IP 全称为 Internet Protocol，即 Internet 协议。它负责在 TCP/IP 主机之间提供数据报服务，进行数据封装、产生协议头。该协议是 TCP 与 UDP 的基础。

由于在以太网中帧大小是有限制的，因此 IP 需要将较大的数据报文分割，在目的主机则负责将这些打散的包重新组合。由于不同的包段可能是由不同的网络路径传送的，因此 IP 还需要负责将这些包按正确的顺序重新组合。注意一点，IP 不负责包的校验，它也是一种无连接不可靠传输。不可靠（Unreliable）的意思是它不能保证 IP 数据报能成功地到达目的地。如果发生某种错误，IP 有一个简单的错误处理方法，丢弃该数据报，然后发送 ICMP 消息报给信源端。数据包的检测校验是由上层协议如 TCP 等负责的。无连接（Connectionless）这个术语的意思是 IP 并不维护任何关于后续数据报的状态。每一个数据包都是独立的。

IP 还需要负责寻找路由，因此它还需要配套一个确定的 IP 地址。在 IP 报文的包头中包含了源与目的的 IP 地址。

一般来说不会有应用程序直接访问 IP。

2. ICMP

ICMP 全称为 Internet Control Message Protocol，即 Internet 控制报文协议。ICMP 其实是 IP 的附属协议，IP 用它来与其他主机或路由器交换错误报文和其他的一些网络情况。在 ICMP 包中携带了控制信息和故障恢复信息，这些信息可以用于：

- 源抑制：这是一个流控制信息，通过由接收方向源主机发送来请求源主机停止发送数据。在接收主机的缓冲区快满时发送。
- 路径重定向：由网关向请求其提供服务的主机发送，用于通知该主机在网络中还有其他的距离目的主机跟近的网关。
- 主机不可到达：在网络状况不佳的网络中传送数据报时，发生故障（如链路失效、链路堵塞、主机失效等）的网关或者系统会发出此消息。在 ICMP 报文中通常包括失效的原因。
- 应答请求与回复：用 ping 指令来检测目标主机是否可以到达。ping 指令调用 ICMP 消息的应答请求功能发送数据报，如果远程主机是可以到达的，则该系统会用应答回复功能来响应。

ICMP 的主要职责就是用于路由器或者主机向其他的路由器或者主机发送出错报文和控制信息。

尽管 ICMP 主要被 IP 使用，但应用程序也有可能访问它，在 Windows 系统中有专门的 DLL 接口可以使用。除去前面所说的 ping，Traceroute 是另外一个流行的诊断工具，它们都使用了 ICMP。

3. ARP

ARP 的全称为 Address Resolution Protocol，即地址解析协议。每一块网卡（NIC，Network Interface Card）都有一个唯一的硬件地址（由网卡的生产厂商设置的，需要使用特殊的方式才可以修改）。这个硬件地址称为 MAC（Medium Access Layer）。一块网卡依据数据帧的包头信息中是否写有它的 MAC 地址来决定是否接受并上传该帧。

分配给主机使用的 IP 地址和它固有的 MAC 地址是互不相干的。IP 地址只对 TCP/IP 有效，MAC 地址只对网络访问层有意义。在物理网络上的数据帧交换依赖于 MAC 地址，ARP 实现了从 IP 地址到 MAC 地址的映射。

4. RARP

RARP 的全称为 Reverse Address Resolution Protocol，即逆向地址解析协议。它负责根据 NIC 硬件地址去查询对应的 IP 地址。

1.1.5 RFC 和标准简单服务

所有关于 Internet 的正式标准都以 RFC（Request for Comment）文档出版。另外，大量的 RFC 并不是正式的标准，出版的目的只是为了提供信息。RFC 的篇幅从 1 页到 200 页不等。每一项都用一个数字来标识，如 RFC112；数字越大说明 RFC 的内容越新。

所有的 RFC 都可以通过电子邮件或用 FTP 从 Internet 上免费获取。如果发送下面这份电子邮件，就会收到一份获取 RFC 的方法清单：

```
To: rfc-info@ISI.EDU
Subject: getting rfcs
help: ways_to_get_rfcs
```

最新的 RFC 索引总是搜索信息的起点。这个索引列出了 RFC 被替换或局部更新的时间。下面是一些重要的 RFC 文档：

- 赋值 RFC（Assigned Numbers RFC）列出了所有 Internet 协议中使用的数字和常数。所有 Internet 端口号都列在这里。
- Internet 正式协议标准，这个 RFC 描述了各种 Internet 协议的标准化现状。
- 主机需求 RFC，该 RFC 包括大量的协议资料。
- 路由器需求 RFC，它与主机需求 RFC 类似，但是只单独描述了路由器的需求。

本书附录 1 分类列出了一些常用 RFC 文档的索引。

表 1-1 列出一些常用的标准简单服务，它们的服务类型一般是 Telnet。

表 1-1　　比较普遍的标准简单服务

名字	TCP 端口号	UDP 端口号	描述
Echo	7	7	服务器返回客户发送的所有内容

续表

名字	TCP 端口号	UDP 端口号	描述
Discard	9	9	服务器丢弃客户发送的所有内容
Daytime	13	13	服务器以可读形式返回时间和日期
Chargen	19	19	当客户发送一个数据报时，TCP 服务器发送一串连续的字符流，直到客户中断连接。UDP 服务器发送一个随机长度的数据报
Time	37	37	服务器返回一个二进制形式的 32bit 数，表示从 UTC 时间 1900 年 1 月 1 日午夜至今的秒数

1.2 TCP/IP 基本概念

通过上节的学习，想必读者对 TCP/IP 已经有了一个整体的了解，但这只是认识 TCP/IP 的第一步。作为一个整体的结构体系，TCP/IP 必然要涉及到一系列基本但非常重要的概念，它们同样也是读者学习的起点。本节主要对 IP 地址、地址解析、IP 数据报、UDP 数据报、TCP 数据报及端口号进行简明扼要的介绍。

1.2.1 IP 地址

网络互联的目的是提供一个无缝的通信系统，为此，互联网协议必须屏蔽物理网络的具体细节，并提供一个虚拟网络的功能，使设计者可以在不考虑物理硬件细节的情况下自由地选择地址。在 TCP/IP 中，编址由 IP 规定，IP 标准分配给每台主机一个 32 位的二进制数作为该主机的 IP 地址。在最新出台的 IPv6 中 IP 地址升至 128 位，这样 IP 资源就变得更加丰富。目前支持 IPv6 协议的软件已经有很多，但是离实用化还有一段距离，有兴趣的读者可以参考其他资料。

每个 32 位 IP 地址被分割成两部份：前缀和后缀。前缀用于确定计算机从属的物理网络，后缀则用于确定网络上一台单独的计算机。互联网中每一个物理网络都有一个惟一的值作为网络号（Network Number）。IP 地址的层次性保证了以下两个重要性质：

- 每台计算机分配一个唯一的地址。
- 虽然网络号分配必须全球一致，但后缀可本地分配，不须全球一致。

IP 地址共分 5 类：A 类、B 类、C 类、D 类和 E 类。其中 A 类、B 类和 C 类为基本类，D 类用于多播传送，E 类属于保留类，现在不用。它们的格式如下（其中，*代表网络号位数）：

A 类：0******* xxxxxxxx xxxxxxxx xxxxxxxx

B 类：10****** *******x xxxxxxxx xxxxxxxx

C 类：110***** ******** ******** xxxxxxxx

D 类：1110xxxx xxxxxxxx xxxxxxxx xxxxxxxx

E 类：1111xxxx xxxxxxxx xxxxxxxx xxxxxxxx

IP 地址一般采用点分十进制的表示方法，例如：

100000001 00110100 00000110 00000000 → 129.52.6.0

采用点分十进制表示方法后的地址分类如表 1-2 所示。