TCP/IP使用详解

(美) Ed Taylor 著

王 虎 邓宏涛 刘志刚 等译

机械工业出版社
China Machine Press

本书是一本全面而详细地讲解TCP/IP的专著，主要内容包括网际协议、传输控制协议、通用TCP和UDP应用程序、设计TCP/IP网络、TCP/IP网络组件、动态主机配置协议等等。

本书既可作为一本用户指南，也可作为学习TCP/IP的理想教材。

本书版权登记号：图字：01-98-2588

图书在版编目(CIP)数据

TCP/IP使用详解/(美)泰勒(Taylor, E.)著；王虎等译. -北京：机械工业出版社，1999.4
书名原文：TCP/IP Complete
ISBN 7-111-07080-1

I.T… Ⅱ.①泰… ②王… Ⅲ.计算机网络－通信协议，TCP/IP Ⅳ.TP393

中国版本图书馆CIP数据核字(1999)第05213号

出 版 人：马九荣(北京市百万庄大街22号 邮政编码 100037)
责任编辑：李云静
北京市昌平环球印刷厂印刷·新华书店北京发行所发行
1999年4月第1版第1次印刷
787mm × 1092mm1/16 · 25.5印张
印 数：0 001- 5000册
定 价：58.00元(附光盘)

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

原作者的话

现在有一种需要，希望将某些信息收集在一起，我的目的即在于此。我已经收集了一些基本的数据通信方面的信息，并用TCP/IP协议组建过一个网络样例。《TCP/IP使用详解》详细叙述了那些一直对我很有好处的东西。可以按以下地址和我取得联系：

Internet: IWIinc@aol.com
IWIinc@ibm.net
IWIinc@msn.com
Edtaylor@aol.com
Zac0002@ibm.net

AOL: IWIinc
Edtaylor

Compuserve: 72714,1417

如何使用本书？你可以将这本书从前至后读完，也可以把它当参考书使用。

参加本书翻译的还有王德福、陈力、高洪波、张小飞、叶剑、王伟、李海辉、高峰、袁玉书、冠小野、丁春玲。

目　录

第1章　传输控制协议/网际协议 (TCP/IP)

传输控制协议网际协议通常是指TCP/IP，它是当今世界上广泛使用的高层网络协议。本章将从历史回顾开始，陈述和TCP/IP 有关的核心部分和内容。

1.1　历史回顾

我们最好从20世纪60年代末说起。美国政府一个高级项目研究代理机构(ARPA)研究的各种技术中，有一项技术需要建立一个基于分组交换技术的网络，以供代理机构的各个成员之间互相交流,这是一种通过电话线将各个地方的科学家和机构工作人员联系起来的途径,可以让他们在网上协同工作。

后来到了1969年，组建ARPA网的各个器件已经准备齐全。在很短的时间内，少数的几个人就建成了一个可以互相交换数据的网络。随着时间的推移，ARPA网上又加了一些东西，也越来越完善了。

1.1.1　20世纪70年代

1971年，国家高级项目研究机构(DARPA)超过了ARPA。结果，ARPA网就归DARPA管辖了。DARPA的专长是卫星、无线电和分组交换技术。

与此同时，由于ARPA网正在使用的网络控制程序(NCP)和其特性密切相关，因此在研究、性能和其他一些要求方面存在很多局限。ARPA网使用协议(即NCP)的明显特点是速度慢，而且周期性地不稳定。既然ARPA网已经正式由DARPA管辖，就需要一个新方法来解决ARPA网的问题，因此采用了一个不同的突破方向。

大约是1974年初，DARPA准备资助研究一套新的协议以取代那时正在使用的协议。这一努力促进了TCP/IP基础协议的研究。最早的TCP/IP出现在1974 ~ 1975年期间。当这些技术正在全面展开时，一个新的情况出现了。

1975年，美国国防部(DoD)将ARPA网划归国防通信机构(DCA)管辖，由DCA负责网络操作方面的工作，也就是在那时侯，ARPA网成了国防数据网(DDN)的基础部分。

随着时间的推移，TCP/IP继续得到完善。有很多网络出现了，它们按TCP/IP协议连到ARPA网上并一同工作。到了1978年，TCP/IP已经很稳定并可以通过卫星在一个连到远地工作站上的可移动终端作公众演示。

1.1.2　20世纪80年代

从1978年到1982年，TCP/IP不断地得到发展和完善。1982年，TCP/IP在很多方面取得了极大的进步。首先，DoD发表了一个政策声明，采纳TCP/IP协议作为连接分布式网络的监督性实体。第二年，也就是到了1983年，DoD正式采纳TCP/IP作为将网络连到ARPA网的协议标准。

1983年早期，DoD正式放弃支持网络控制程序(NCP)而采纳TCP/IP，这标志着因特网的诞

生。术语Internet是Internetworking的延伸，它是用于指网络互连的技术术语。此外，Internet(因特网)的另一个意思是指当今遍布世界的多个网络。

1.1.3 20世纪90年代

今天的因特网由大量互联的网络组成。National Research and Education Network(NREN)是因特网的主体部分。其他部分包括National Science Foundation(NSF)，NASA，The Department of Education，Educational Institutions。

各种组织都加入了因特网，一个因特网的服务产业看来就要出现了。

1.2 有助于TCP/IP协议发展的各种技术力量

前面几部分的历史回顾使得和TCP/IP协议、因特网有关的技术增色不少，但对因特网的某些方面却未加以解释，这些方面有助于理解因特网对TCP/IP协议的技术影响。

1.2.1 技术

美国政府将TCP/IP协议定成了一个标准，因特网就是以TCP/IP协议为基础建成的。现在，因特网已遍布全世界，各种实体都连到了它的上面。这些实体用的都是TCP/IP协议。这就足以解释市场上为什么会有大量的和TCP/IP协议有关的产品了，它还在以当前的速度迅速递增。

80年代是科学技术迅速发展的十年。既然美国政府已经认可TCP/IP协议为因特网的标准，很多公司开始投资生产相关产品以满足这一需要。

TCP/IP协议相关产品的大量注入导致了另外一些产品的需要。例如，在80年代两种技术占了主导地位：PC技术和LAN技术。随着PC和LAN的大量出现，一个完全新型的产业开始形成。这些技术推动了TCP/IP协议的发展，因为完成LAN需要用到TCP/IP协议和PC。在单个基础上实现的TCP/IP协议被称为internet(注意字母i是小写的)。

1.2.2 市场力量

另一个有助于TCP/IP在市场中发展的因素是公司规模的缩小。这听起来有些奇怪，不过在80年代，我目睹了很多这样的例子，即在其他方面收缩的同时基于TCP/IP建立起来的网络却发展了。

举个例子吧，我有过这样一段经历。有一个公司(我不能说出名称)，它的总部在东北部而五十多个分部却遍布全国。该公司需要各个分公司每天独立运作，与此同时与公司数据中心相连。他们之所以如此是因为他们在各个分公司建了一个基于TCP/IP的LAN，然后和数据中心相连。这是我见过的很多例子中的一个。

1.2.3 购买方便

80年代末，TCP/IP产品从很多计算机商店的柜台上都可以买到。这和80年代初相比很能说明问题，那时侯终端用户要买一件产品并不是很容易。

购买TCP/IP产品很方便还有另一方面的原因。DoD不仅鼓励使用TCP/IP协议，他们还成立了一个公司，Bolt,Beranek,and Newman，专门将TCP/IP协议接口到UNIX上去。此外，DoD

还鼓励UC Berkeley将TCP/IP协议包含到他们的BSD UNIX 操作系统中去。因此，用户只要得到了Berkeley UNIX，就能免费得到TCP/IP。其后不久，TCP/IP被加到AT&T的 System V UNIX操作系统中了。

1.2.4 个人的知识

从70年代末到80年代，大多数的大学和其他一些教育协会都讲授TCP/IP协议。因为TCP/IP是购买Berkeley UNIX时免费赠送的，所以到了80年代中期，TCP/IP便在各类学术协会中占据了主导地位。结果，从各地教育协会毕业的一些人中，如果他们的知识背景中包括计算机科学的话，都很可能受过TCP/IP的影响。

这些人进入工作岗位，开始深入到技术和管理部门。当涉及关于网络协议的决定时，TCP/IP在很多情况下就成了极有可能的选择。

在80年代，市场给予了那些掌握TCP/IP协议的人以丰厚的回报。现在，到了90年代中期，市场中有相当数量具有不同程度TCP/IP知识的人。

所有这些因素一起推波助澜，成就了TCP/IP今天的主导地位。TCP/IP协议已经成了世界范围内流行的上层协议。

1.3 层次分析

在因特网早期的日子里，术语网关(gateway)用得相当普遍。它主要是指从一个特定地点连到因特网的一个接口，那时侯这就是它的全部含义。但是现在，这一术语的外延已经发生变化。

根据American Heritage Dictionary，gateway的定义为："1.在墙壁或篱笆上的一个可以用门关上的开口。2.一个入口方式"。我相信此条目的原始含义为"一个入口方式"。这很好，不过你也许要奇怪为什么提到这个。是的，今天一个完整的产业，internetworking and integration,已经出现了，一些专门的产品也随之产生了。网关就是这样一个器件。

连接器和那些连接不同种类网络的一些器件和网关在定义上是一致的，即在最低程度上将高层协议从一种类型转换为另一种类型的一种器件。它能转换所有的七层协议。

在这里解释这个的目的很简单。这本书从前到后都会出现网关这个词。它在TCP/IP中处于一个很基础性的地位以至于现在还在使用。在TCP/IP和因特网中，网关在很多场合下从技术上讲应该是路由器(router)。

1.4 概览、TCP/IP和OSI的相互关系

TCP/IP是高层协议。尽管某些特定的功能用硬件完成简化的TCP/IP协议，但TCP/IP总体上还是用软件完成的。TCP/IP可以在不同的软硬件平台上操作，支持不止一种的数据链路协议。OSI模型代表了网络中应该出现的各个层次。图1-1给出了TCP/IP和OSI模型的对比。应该注意，TCP/IP有三个层次：网络层，传输层以及由OSI模型最上面的三层组合成为的应用层。涉及到下面两层时，TCP/IP要灵活得多。它可以通过不同的方式实现。

TCP/IP可以和很多数据链路层协作。有一些已经在图1-1列出来了。本章剩下的部分将解释每一层的通用部件。

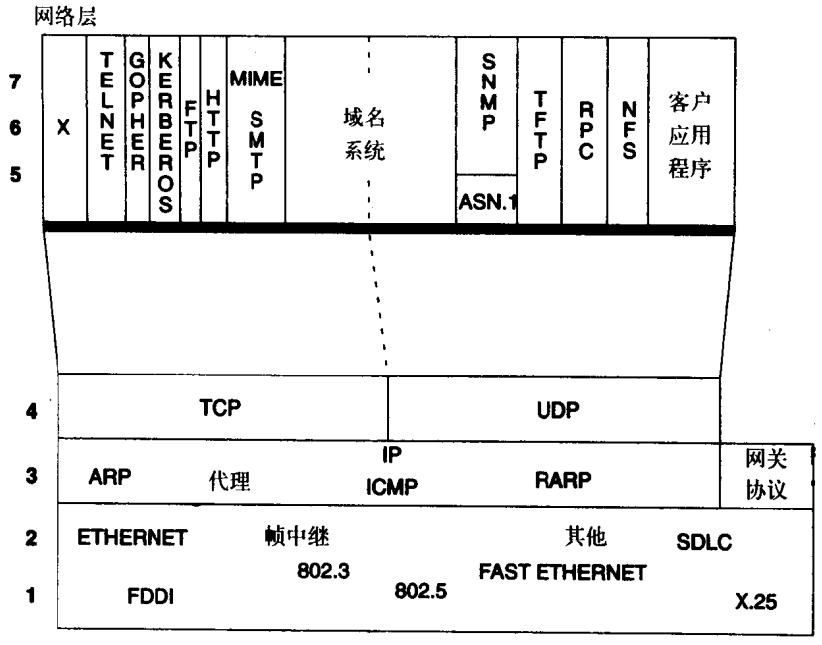

图1-1 TCP/IP与OSI模型的关系

1.5 网络层组件和功能

OSI模型的第三层是网络层。在TCP/IP中它是TCP/IP协议组中的最下层。TCP/IP网络层组件如下:

• 网间协议(IP, internet protocol) IP有一个寻址方案以识别其驻留的主机。IP包括在路由功能中。

• 网间控制报文协议(ICMP, Internet Control Message Protocol) ICMP是实现TCP/IP协议所必须的组件。它负责通过IP头在网络中发送报文 。

• 地址转换协议(ARP, Address Resolution Protocol) ARP动态地将IP地址转换成物理(硬件接口卡)地址。

• 反向地址转换协议(RARP, Reverse Address Resolution Protocol) 通过广播其硬件地址, RARP得到其主机IP地址。典型地, 一个RARP服务器将被指定并发出响应。

• 路由信息协议(RIP, Routing Information Protocol) RIP是在网络层中用到的路由协议。如果实现的话, 它将在它所驻留的主机中执行路由分组。

• 开放最短路径优先(OSPF, Open Shortest Path First) OSPF是在网络层实现的RIP路由协议, 不过它要用到网络拓扑知识来得到最快路径的路由信息。

1.6 传输层组件和功能

OSI模型的第四层是传输层。在TCP/IP协议中也处于中层。传输层组件如下:

• TCP 该传输层协议是很可靠的, 在必要的时候执行再发送的操作。

• UDP 该传输层协议是不太可靠的, 并不执行再发送的操作。相反地, 这由享受其服务的应用程序来完成。

1.7 通用应用层服务

TCP/IP协议中传输层的上面，有一些通用的应用程序:

• X 这是一个在多售主环境下实现的窗口化系统。

• TELNET 该应用程序提供远程登录服务。

• 文件传输协议(FTP, File Transfer Protocol) 该应用程序提供异型系统之间的文件传输能力。

• 简单邮件传送协议(SMTP, Simple Mail Transfer Protocol) 该应用程序提供基于TCP/IP协议用户的电子邮件服务。

• 域名服务(DNS, Domain Name Service) 该应用程序用于解决TCP/IP网络中的目的地址。它可以自动提供网络地址而不需要手工的更新主机路由表。

• 普通文件传送协议(TFTP, Trivial File Transfer Protocol) 这个UDP应用程序最好用于将软件下载到设备时的网络设备初始化。因为TFTP是一个普通文件传送协议，它可以很好的满足这一需要。

• 简单网络管理协议(SNMP, Simple Network Management Protocol) 这是大多数TCP/IP网络管理的方法。SNMP是基于主体、管理者的设计方案的。主体收集关于主机的信息，而管理者则维护主机参与主体的状态信息。

• 网络文件服务(NFS, Network File Servicer) NFS这个应用程序可以使得远端目录看上去象是用户主机目录系统的一个部分。

• 远端进程调用(RPC, Remote Procedure Call) 该应用程序协议可以调用一个进程并在服务器上执行。

• 用户应用程序(Custom Application) 用户应用程序可以按传输层协议UDP编写。如果这样做的话，可以在应用程序之间进行同层次的通信。

1.8 TCP/IP网络要求

在深入研究TCP/IP协议的细节之前，有必要知道TCP/IP网络运作的基本要求。例如,

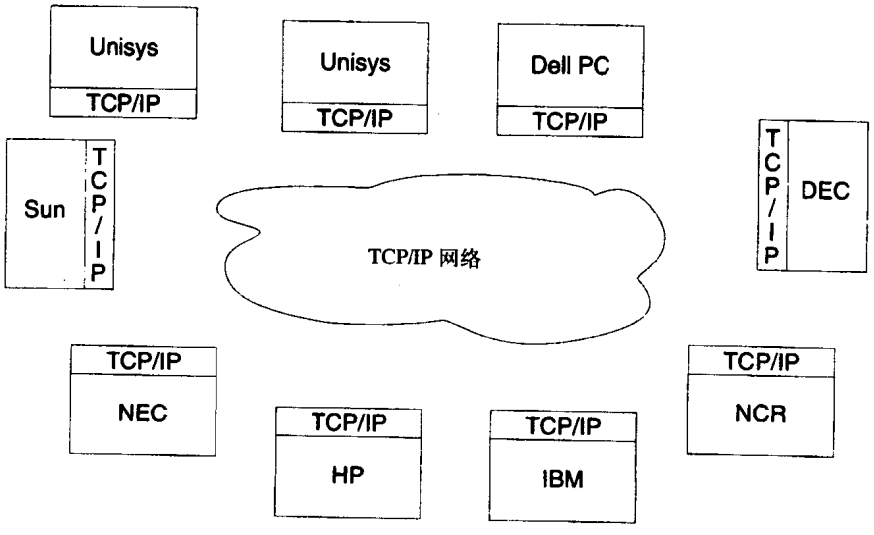

图1-2 主机使用TCP/IP协议作为他们的网络标准

TCP/IP网络要求所有接入的主机按TCP/IP协议运作，并且直接或间接的接到一个共同的连接上。对有些系统，这可能需要有网关功能，图1-2就是一个带有不同售主计算机的典型TCP/IP网络系统的例子。

图1-2包括操作系统各不相同的多个供应商，他们的硬件平台也各不相同。不过，只要连接是建立到TCP/IP网络之上的，不同的计算机之间可以进行有效的通信。

1.9 小结

TCP/IP协议已经发展了好几十年，它起源于开发、教育和研究机构。80年代出现的一些技术和市场力量使TCP/IP获得了市场动力。

TCP/IP在技术上是一个四层协议，可以和OSI模型相比较。TCP/IP可以和许多低层的协议协同运作，就像本章所揭示的那样。现在，很多在TCP和UDP之上操作的应用程序已变得通用化。在合并了这些应用程序的一些软件包中，他们的功能已经一样了。

TCP/IP的流行有很多原因。其中的一个就是协议提供者的一致性因素。现在在市场上每一种主要的操作系统都可以使用TCP/IP协议。

第2章　网际协议(IP)

IP是网络的第三层。IP将分组(数据单元)从源地址经特定的路由送到目的地址。有的人将IP意义上的分组看成是数据报。IP数据报是TCP/IP网络的基本数据单元。

IP是无连接的。它实现两个基本的功能：分段和寻址。分段(再装配)由IP报头的一个域来完成。在一个面向分组的小网络中，当需要流过网络的数据报更小一些时就需要分段。

2.1　IP报头格式

寻址功能也要在IP报头里实现。报头里面包括源地址和目的地址，还有一些其他的信息。图2-1是一个IP报头的例子。

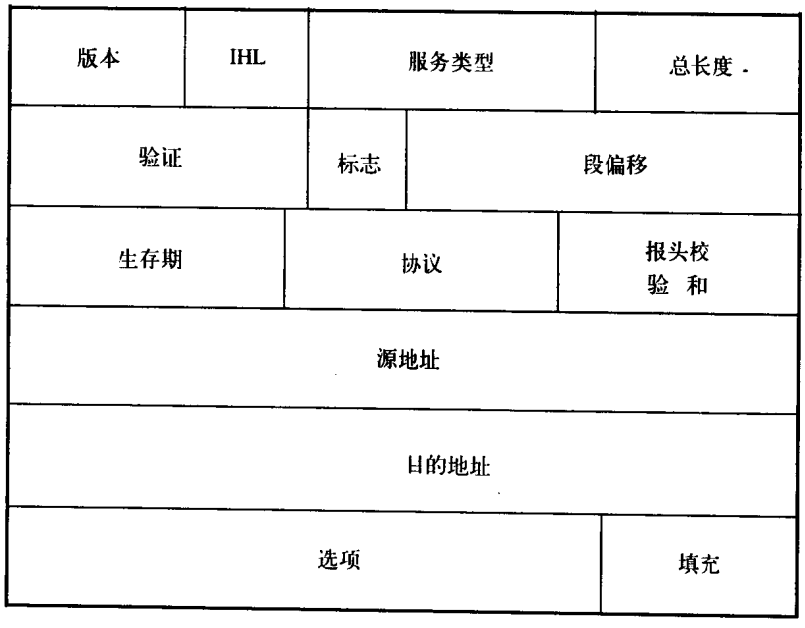

图2-1　一个IP报头的内容

IP报头组件及其功能如下：

• 版本(VERSION)　版本域用于显示IP报头的格式信息。

• IHL　IHL代表了网间网报头长度。它是网间网报头以32位字计算的长度，并指向数据的开始位置。

• 服务类型(TYPE OF SERVICE)　服务类型域指明数据报在网络里发送时是如何被处理的。

• 总长度(TOTAL LENGTH)　该域指示数据报的总长度；包括IP报头和数据。

• 标志(FLAGS)　标志域有三个比特。如果支持分段的话，他们用于指示不用分段、更多的段和最后的段。

• 段偏移(FRAGMENT OFFSET) 如果分段的话，该域指示分段在数据报的什么位置。

• 生存期(TIME TO LIVE) 该域指示一个数据报允许在网络中停留的最长时间(无论是本地网还是因特网)。当该值为零时，数据报被丢弃。时间以秒为单位计算，每一个处理数据报的实体都要将该值减一，即使处理的时间不到一秒。

• 协议(PROTOCOL) 该域决定在网络的下一层数据将被送到TCP还是UDP。

• 报头校验和(HEADER CHECKSUM) 这是一个报头校验和域。每一次报头被处理，如果报头域改变了，该报头校验和就要被重新计算和校验。

• 源地址(SOURCE ADDRESS) 这是数据报的发送地。它由32个比特组成。

• 目的地址(DESTINATION ADDRESS) 这是报头和数据的目的地。和源地址一样，它也是由32个比特组成。

• 选项(OPTIONS) 选项部分在数据报中可有可无。选项必须按IP 模式实现；不过在发送过程中不一定使用。

在选项域中有多个变量。下面列出了这些变量，包括一些简短的说明:

• 无选项(NO OPTION) 该选项用于相邻两选项之间以保证第二个选项在32比特边界处开始。

• 安全措施(SECURITY) 安全措施是DoD采用的一个机制。它通过分割、处理限制和传输控制代码(TCC)给主机提供了一种采用安全机制的方法。当传输的信息未加以分割时就使用该分割值。处理限制由Defense Intelligence Agency定义。TCC允许数据通信的分离。

• 稀疏信源和记录路由(LOOSE SOURCE AND RECORD ROUTE) 该域提供了一个方法，使得数据报的源端可以提供路由信息以帮助向前发送数据报。它还可以帮助记录路由信息。

• 严格信源和记录路由(STRICT SOURCE AND RECORD ROUTE) 该选项可以让数据报的源端提供供路由器使用的信息，也可以记录路由信息。

• 记录路由(RECORD ROUTE) 这是一个记录数据报遍历网络路由的简单方法。

• 流标志符(STREAM IDENTIFIER) 对于不支持流这一概念的网络，它提供了一种在网络中携载流标志符的方法。

• TIMESTAMP 该选项包括一个指针域、溢出域、标志域和因特网地址。简而言之，它提供了路由器处理处理数据报的时间和日期。

• 填充项(PADDING) 使用该填充项是为了保证报头在32比特边界处结束。

2.2 IP版本6：远景

IP版本6(IPv6)是网际协议的一个新版本，该版本是IP版本4(IPv4)[RFC-791]的后继版本。从IPv4到IPv6，其变化主要有以下几类:

• 扩展的寻址能力 IPv6将IP地址大小从32位变到了128位以支持更多级的寻址层次，更多的可寻址结点，更简单的自动地址配置。通过将广播地址中加入“范围(scope)”域，改进了广播地址的可缩放性。还定义了一个称作“any-cast address”的新型地址，用于将分组送到任何一个结点组中去。

• 报头格式简化(Header Format Simplification) IPv4报头的有些域被减小或成了可选项，这样减小了分组处理中一些通常(common-case) 情况下的处理代价，并限制了IPv6报头的带宽代价。

• 对扩充和选项的进一步支持 IP报头选项编码方式的改变使得前向效率更高，对选项的长度没有那么多严格的限制，将来在加入新的选项时有了更多的余地。

• 流标号能力(Flow Lablling Capability) 这个能力的加入可以使分组的标号属于一个特定的发送者要求专门处理的通信流，比如服务的非缺省质量，实时服务。

• 鉴别和保密能力(Authentication and Privacy Capabilities) IPv6指定了支持鉴别、数据完整性和数据保密性的功能。该文件指定了基本的IPv6报头和最初定义的IPv6扩展报头和选项。它还讨论了分组问题，流标号和优先权的语义，还有IPv6高层协议的效果问题。IPv6地址的格式和语义单独在[RFC-1884]里说明。实现IPv6所要包括的ICMP的IPv6版本在[RFC-1885]里说明。

2.3 网络控制报文协议(ICMP)

ICMP和IP一起工作，它和IP一样在第三层。因为IP 是无连接的，它无法将报文和错误信

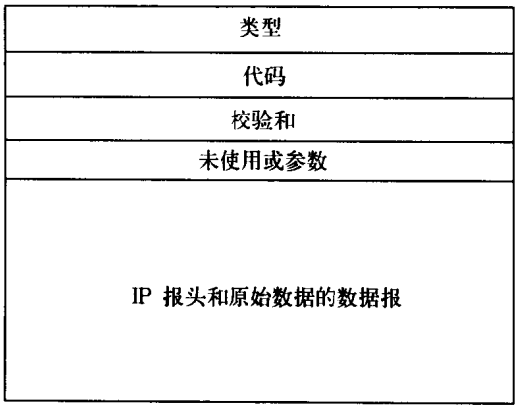

图2-2 ICMP报文格式

Type	报文含义
0	Echo 应答
3	目的地不可到达
4	源中断
5	重定向
8	Echo 请求
11	数据报超时
12	数据报参数有问题
13	时间戳请求
14	时间戳响应
17	地址屏蔽请求
18	地址屏蔽响应

图2-3 ICMP报文类型及其含义