


全国高职高专规划教材

# 实用组网技术

Networking in Practice

李庆风 主 编  
陶剑文 鞠洪尧 副主编



 科学出版社  
[www.sciencep.com](http://www.sciencep.com)

全国高职高专规划教材

# 实用组网技术

李庆风 主 编  
陶剑文 鞠洪尧 副主编

科学出版社

北 京

## 内 容 简 介

本书是一本面向高等职业教育、高等专科教育和成人高等教育的实用组网技术教材。全书共分7章,主要介绍了网络基础知识、PDS技术、网络设备、网络操作系统应用、网络规划、网络管理、网络安全及网络维护等内容。本书在讲解基础知识的同时,尽量以实用为主,强调理论知识与实训相结合,使读者在了解理论的基础上,掌握实用组网技术的操作技能。

本书内容丰富,结构合理,实用性强,不仅适合作为高职高专院校相关专业的教材,而且可供广大的网络爱好者参考。

### 图书在版编目(CIP)数据

---

实用组网技术/李庆风主编. —北京:科学出版社,2003  
(全国高职高专规划教材)  
ISBN 7-03-012083-3

I. 实... II. 李... III. 计算机网络语言—高等学校:技术学校—教材

IV. TP393

中国版本图书馆CIP数据核字(2003)第072967号

---

策划编辑:李振格 /责任编辑:丁波  
责任印制:吕春珉 /封面制作:东方人华平面设计部

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

\*

2003年8月第一版 开本:787×1092 1/16  
2003年8月第一次印刷 印张:14 1/2  
印数:1—5 000 字数:318 000

定价:20.00元

(如有印装质量问题,我社负责调换<长虹>)

# 前 言

近几年, 高等职业教育得到了迅速的发展, 计算机专业成为高等职业教育中的热门专业, 而网络实用组网技术则是计算机专业中非常实用的一门课程。但是实用组网技术教材的出版却严重落后于高等职业教育的发展, 因而编写一本适合高等职业教育的实用组网技术教材迫在眉睫。

本书是一本面向高等职业教育、高等专科学校和成人高等教育的实用组网技术教材。全书在讲解基础知识的同时, 尽量以实用为主, 将组网所牵涉到的 PDS 技术、网络设备、网络操作系统应用、网络安全、网络维护等内容逐一进行讲解。在整本书中强调理论知识与实训相结合, 使学生在了解理论的基础上, 掌握实用组网技术的操作技能。

本书共分 7 章:

第 1 章介绍了网络的基本知识, 包括 TCP/IP 体系结构、IP 地址、子网掩码、访问控制方法、传输介质及 Internet 常见接入方式。

第 2 章讲述了综合布线系统的基本概念、设计标准与规范、体系结构以及详细说明了综合布线系统的设计原理及设计步骤。

第 3 章介绍了网卡、集线器、交换机、路由器以及无线网桥的基本工作原理和它们的主要特点。

第 4 章介绍 Windows 2000 Server 和 Linux 操作系统的优点, 以及在这两个操作系统上构建 DHCP 作用域、DNS 域名解析、Web 站点和 FTP 站点的方法。

第 5 章讲述了网络规划、设计的基本原则, 实施的步骤和方法, 针对当前的网络管理技术, 对目前常用的网络管理软件作出一些介绍。

第 6 章介绍网络安全的含义、网络安全的特征、威胁网络安全的因素、网络安全的关键技术以及网络安全解决的方案、防火墙的原理、防火墙的设备和 VPN 技术, 最后介绍了网络病毒及防治技术。

第 7 章介绍网络文档备案、测试技术以及网络维护、网络故障诊断的方法和步骤, 并针对网络常见的故障进行了举例, 并提出了相应的解决方法。

本书由李庆风任主编, 陶剑文、鞠洪尧任副主编。第 1 章由郭成实编写, 第 2 章由陶剑文编写, 第 3 章由杨鹏、石红波编写, 第 4 章由鞠洪尧、李庆风、杨鹏编写, 第 5 章由黄坤编写, 第 6 章由秦学礼编写, 第 7 章由李庆风编写。

本书编写过程中参考了许多文献资料。在写作中力求做到层次清楚, 语言简洁流畅, 便于读者了解当前组网技术的发展形势, 希望本书对读者掌握组网技术有一定的帮助。

限于编者的学术水平, 加之时间仓促, 在本书的选材和内容安排上如有不妥之处, 恳请读者与同仁批评指正。

作 者

2003 年 6 月

## 全国高职高专规划教材编委会名单

主任 俞瑞钊

副主任 陈庆章 蒋联海 周必水 刘加海

委员 (以姓氏笔画为序)

王雷 王筱慧 方 程 方锦明 卢菊洪 代绍庆

吕何新 朱 炜 刘向荣 江爱民 江锦祥 孙光弟

李天真 李永平 李良财 李明钧 李益明 余根墀

汪志达 沈凤池 沈安衢 张 元 张学辉 张锦祥

张德发 陈月波 陈晓燕 邵应珍 范剑波 欧阳江林

周国民 周建阳 赵小明 胡海影 秦学礼 徐文杰

凌 彦 曹哲新 戚海燕 龚祥国 章剑林 蒋黎红

董方武 鲁俊生 谢 川 谢晓飞 楼 丰 楼程伟

鞠洪尧

秘书长 熊盛新

## 本书编写人员名单

主 编 李庆风

副主编 陶剑文 鞠洪尧

撰稿人 李庆风 陶剑文 鞠洪尧 郭成实

杨 鹏 石红波 黄 坤 秦学礼

# 目 录

<b>第 1 章 网络基础知识</b> .....	1
1.1 TCP/IP 体系结构 .....	1
1.1.1 TCP/IP 体系结构简介 .....	1
1.1.2 IP 地址 .....	5
1.1.3 子网掩码 .....	7
1.2 局域网技术 .....	8
1.2.1 IEEE802 LAN 体系结构 .....	8
1.2.2 局域网的拓扑结构 .....	11
1.2.3 局域网介质访问控制方式 .....	15
1.2.4 传输介质 .....	19
1.3 Internet 接入方式 .....	24
习题 .....	26
<b>第 2 章 综合布线系统</b> .....	27
2.1 综合布线系统概述 .....	27
2.1.1 综合布线系统概念 .....	27
2.1.2 综合布线系统的优点 .....	30
2.1.3 综合布线系统的标准与规范 .....	31
2.2 综合布线系统的等级 .....	33
2.2.1 基本型综合布线系统 .....	33
2.2.2 增强型综合布线系统 .....	33
2.2.3 综合型综合布线系统 .....	33
2.3 网络工程的设计与验收 .....	34
2.3.1 综合布线系统的工程设计 .....	34
2.3.2 网络工程的验收 .....	60
习题 .....	63
<b>第 3 章 网络设备</b> .....	64
3.1 网卡 .....	64
3.1.1 网卡的功能及工作原理 .....	64
3.1.2 网卡的选择 .....	65
3.2 集线器 .....	67
3.2.1 集线器的工作原理 .....	67
3.2.2 集线器常用操作 .....	68

3.2.3 集线器的选择 .....	69
3.3 交换机 .....	72
3.3.1 交换机的工作原理 .....	73
3.3.2 交换常用操作 .....	75
3.4 路由器 .....	77
3.4.1 路由器的功能及工作原理 .....	78
3.4.2 局域网接入 Internet 的方案 .....	83
3.5 无线网桥 .....	85
3.5.1 无线局域网络概述 .....	85
3.5.2 无线网桥 .....	89
习题 .....	90
<b>第 4 章 网络应用服务器构建 .....</b>	<b>92</b>
4.1 网络操作系统 .....	92
4.1.1 Windows 2000 操作系统 .....	92
4.1.2 Linux 操作系统 .....	98
4.1.3 常用网络操作系统的比较 .....	100
4.2 DHCP 服务器 .....	103
4.2.1 DHCP 服务器概述 .....	103
4.2.2 用 Windows 2000 平台构建 DHCP 服务器 .....	104
4.2.3 Linux 平台构建 DHCP 服务器 .....	109
4.3 DNS 服务器 .....	111
4.3.1 DNS 概述 .....	111
4.3.2 Windows 2000 平台构建 DNS 服务器 .....	112
4.3.3 Linux 平台构建 DNS 服务器 .....	119
4.4 Web 服务器 .....	121
4.4.1 Web 服务器概述 .....	121
4.4.2 Windows 2000 平台构建 Web 服务器 .....	122
4.4.3 Linux 平台构建 Web 服务器 .....	126
4.5 FTP 服务器 .....	131
4.5.1 FTP 服务器概述 .....	131
4.5.2 Windows 2000 平台构建 FTP 服务器 .....	133
4.5.3 Linux 平台构建 FTP 服务器 .....	139
习题 .....	144
<b>第 5 章 网络规划、设计与管理 .....</b>	<b>145</b>
5.1 网络规划与设计 .....	145
5.1.1 需求分析 .....	146
5.1.2 设计目标 .....	148
5.1.3 设计思想和内容 .....	148



---

5.1.4	网络设计方案 .....	151
5.1.5	设计实例 .....	154
5.2	网络管理 .....	156
5.2.1	网络管理功能 .....	156
5.2.2	网络管理协议 .....	159
5.2.3	网络管理系统 .....	161
	习题 .....	165
<b>第 6 章</b>	<b>网络安全 .....</b>	<b>166</b>
6.1	网络安全重要性 .....	166
6.1.1	网络安全的含义 .....	166
6.1.2	网络安全的特征 .....	167
6.1.3	网络安全的威胁 .....	167
6.1.4	网络安全的关键技术和策略 .....	171
6.1.5	网络安全的解决方案 .....	172
6.2	防火墙技术 .....	180
6.2.1	防火墙的功能 .....	181
6.2.2	防火墙的主要工作 .....	182
6.2.3	防火墙类型 .....	183
6.2.4	防火墙技术 .....	184
6.2.5	防火墙设备介绍 .....	185
6.3	VPN 技术 .....	188
6.3.1	VPN 技术原理 .....	189
6.3.2	VPN 设备 .....	194
6.3.3	VPN 产品 .....	196
6.4	网络杀毒软件介绍 .....	196
6.4.1	互联网下的病毒新特点 .....	196
6.4.2	网络版杀毒软件新趋势 .....	197
6.4.3	几种常见的网络杀毒软件 .....	199
	习题 .....	202
<b>第 7 章</b>	<b>网络维护与故障诊断 .....</b>	<b>203</b>
7.1	网络故障预防 .....	203
7.1.1	文档备案 .....	203
7.1.2	网络测试 .....	204
7.2	网络维护战略 .....	209
7.2.1	预防性网络维护 .....	209
7.2.2	网络维护的关键要素 .....	210
7.3	网络故障诊断 .....	211
7.3.1	故障诊断步骤 .....	211

---

7.3.2 网络故障排除工具 .....	213
7.3.3 常见故障现象及解决方法.....	216
7.3.4 网络常见故障举例 .....	218
习题.....	220
<b>主要参考文献.....</b>	<b>221</b>

# 第 1 章 网络基础知识

## 本章要点

本章主要介绍网络的基本知识：TCP/IP 体系结构、IP 地址、子网掩码、子网划分、局域网的体系结构、拓扑结构、访问控制方法、传输介质及 Internet 常见接入方式。

## 本章难点

TCP/IP 体系结构、子网划分及媒体访问控制方法。

## 1.1 TCP/IP 体系结构

### 1.1.1 TCP/IP 体系结构简介

#### 1. TCP/IP 协议

TCP/IP (Transmission Control Protocol/Internet Protocol) 协议，即传输控制协议 / 网间协议，事实上是国际互联网的工业标准和目前使用最为广泛的通信协议，拥有完整的体系结构和协议标准。Linux、Windows 2000、Netware 等一些著名的网络操作系统都将 TCP/IP 纳入其体系中。

TCP/IP 协议遵从四层概念模型：应用层、传输层、互联层及网络接口层。ARPANET 最初设计的 TCP 称为网络控制程序 NCP，在上面传送的数据单位是报文 (Message)，实际上就是现在的 TPDU。随着 ARPANET 逐渐变成了 Internet，子网的可靠性也就下降了，于是 NCP 就演变成了今天的 TCP。与 TCP 协议配合使用的网络层协议是 IP 协议。图 1.1 所示为 TCP/IP 与相应的国际标准化组织开放式系统互连参考模型 (ISO/OSI RM, International Standards Organization/Open System Interconnect Reference Model) 的简单对比。

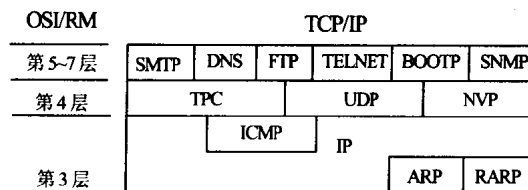


图 1.1 TCP/IP 与相应 ISO/OSI RM 层次对比

对应于 OSI 的第 3 层，TCP/IP 体系结构协议主要有 4 个，其中 Internet 控制报文协议 (ICMP, Internet Control Message Protocol) 可以看作是 Internet 协议 IP 的一部分，

在互联网中，网关或主机用 ICMP 向源站发送关于所发数据报的有关问题的报告，如某个目的站或端口不可到达，或网络中的某处出现拥塞现象。地址转换协议（ARP，Address Resolution Protocol）用来将 IP 地址转换成物理地址（MAC 地址）。反向地址转换协议（RARP，Reverse Address Resolution Protocol）则使一个新接入网络的只有物理地址的站点通过 RARP 发出广播请求，得到 RARP 服务器给它分配的 IP 地址。

对应于 OSI 第 4 层的协议有 3 个，如下所示。

- ① 运输控制协议 TCP：这是最主要的一个面向连接的协议。
- ② 用户数据报协议（UDP，User Datagram Protocol）：这是主机和主机之间无连接的数据报协议，UDP 使用 IP 提供的数据报服务，但对 IP 进行了扩充，如增加了端口编号等。
- ③ 网络话音协议（NVP，Network Voice Protocol）：即分组话音通信协议。在军事通信领域中比较有用。

对应于 ISO/OSI RM 第 5~7 层的高层协议如下所示。

- ① 远程登录协议 TELNET：使用户的终端可以很方便地接入远程的主机系统。
- ② 文件传输协议（FTP，File Transfer Protocol）：用于主机之间文件的交换。
- ③ 简单电子邮件传送协议（SMTP，Simple Mail Transfer Protocol）。
- ④ 域名服务（DNS，Domain Name Service）：提供名字到 Internet 地址的转换。
- ⑤ 引导协议 BOOTP：提供类似于 Windows 2000 和 Netware 客户端的无盘站远程引导。
- ⑥ 简单网络管理协议（SNMP，Simple Network Management Protocol）：提供网络的配置管理、故障管理、性能管理、安全管理和计费管理等功能。

## 2. TCP 报文段格式

TCP 在两台计算机之间传输的协议数据单元 TPDU 称为报文段（Segment）。由于网络层不能保证数据报的正确传送，因此 TCP 不仅承担超时和重传的责任，还要将收到的数据报按顺序再装成报文上交给用户。每个报文分为两部分，前面是 TCP 首部，后面是数据。图 1.2 所示是 TCP 的 TPDU 首部的格式，其首部的最小长度为 5 个 32 位，即 20 个字节。下面介绍各字段的意义。

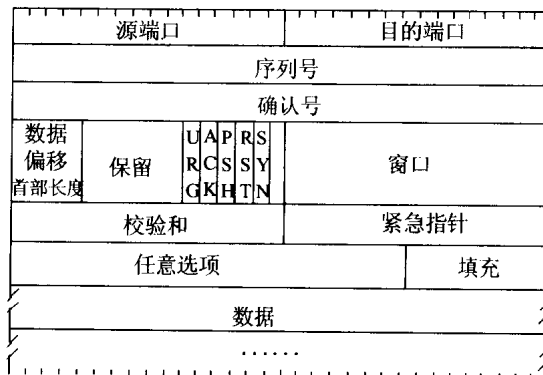


图 1.2 TCP 报文段格式

① 源端口 (Source Port) 字段和目的端口 (Destination Port) 字段: 都各占 16 位, 分别是源站和目的站中传输层与高层的服务接口。

② 序列号 (Sequence Number) 字段: 占 32 位, 它不是为每一个 TPDU 编号, 而是为所传数据的每一个报文编上序号。序号字段就是指该 TPDU 所传的最大序号。

③ 确认号字段: 占 32 位, 它捎带在本站发送的 TPDU 中, 指出期望收到对方的数据字节中的最小序号, 因而隐含地告诉对方, 比确认号少一个号的数据字节已经正确收到。

④ 数据偏移字段: 它是必要的, 因为在首部的 20 个字节以后有一个长度不定的选项, 用来在连接建立时指出允许的最大报文段长度, 指出数据部分从 TPDU 中的多少个 32 位以后才开始的。偏移字段之后有 6 位的保留字段, 供以后使用。

⑤ 控制字段: 占 6 位。下面分别说明其中每一个比特的意义。

- 紧急指针段 URG (Urgent): 当 URG 置“1”时, 表明此 TPDU 相当于紧急数据, 应尽快传送。例如, 键盘的中断信号就属于紧急数据, 此时要与第 5 个 32 比特字中的后半“紧急指针” (Urgent Pointer) 配合使用。紧急指针指出紧急数据的最后一个字节的序号 (因为可能后面接着发送的几个 TPDU 都是紧急数据)。
- 确认号段有效标志 ACK (Acknowledge): 当 ACK 置“1”时, 确认号段有效, 否则无意义。
- 急迫推动标志 PSH (Push): 当 PSH 置“1”时, 表明请求将本 TPDU 紧急投递。
- 重置连接标志 RST (ReSe): 当 RST 置“1”时, 表明要重建传输连接。
- 同步序列号标志 SYN (Synchronization): 当 SYN 置“1”而 ACK 置“0”时, 表明这是一个连接请求 TPDU。对方若同意建立连接, 则应在发回的 TPDU 中将 SYN 和 ACK 均置为“1”。
- 终止标志 FIN (Final): 当 FIN 置“1”时, 表明发送方要发送的数据已经发完, 并要求释放传输连接。

⑥ 检验和字段: 检验的范围包括 TPDU 的首部和数据部分。

TPDU 长度的选择也很不容易。当 TPDU 长度变小时, 网络的利用率就降低; 但若 TPDU 太长, 那么在 IP 层传输时就要分段, 到达目的站后再将收到的各个段装成原来的 TPDU, 一旦传输出错还要重传出错的数据报, 这些都使网络开销增大。

### 3. IP 分组格式

IP 分组也称 IP 数据报, 它是以无连接方式通过网络传输的, 在源发主机和目的主机以及经过的每个路由器中, 网络层都使用始终如一的 IP 协议和不变的 IP 分组格式。要注意的是, IP 是基于数据报服务的。IP 分组作为 Internet 的基本传送单元, 分为分组头和数据信息, 在分组头中包含源站和目的站地址。IP 分组头的长度为 4 个字节的整数倍, 如图 1.3 所示。

下面分别说明其中每一个字段的意义。

① 版本号: 该 4 位字段标识当前协议支持的 IP 版本号, 在处理 IP 分组之前, 所有的 IP 软件都要检查分组的版本号字段, 以保证分组格式与软件期待的格式一样。如

果标准不同，机器将拒绝与其协议版本不同的 IP 分组。本小节给出的是对版本为 4 的 IP 的描述，版本 1~3 几乎已经过时不用。

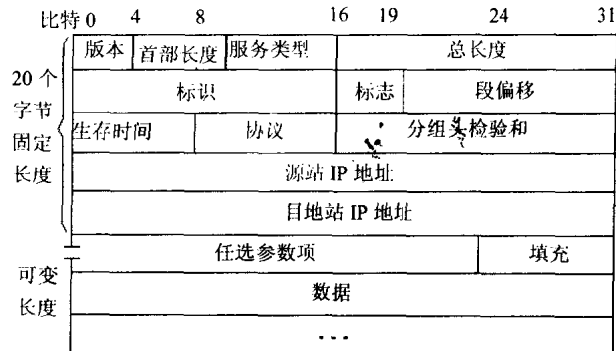


图 1.3 IP 分组头格式

② IP 分组头首部长度：该 4 位字段表示 IP 分组头的长度，取值的范围是 5~15。由于 IP 分组头格式的长度单位是 4 字节，因此首部长度的最大值是  $15 \times 4 = 60$  字节。当 IP 分组头长度不是 4 字节的整数倍时，必须利用最后一个填充字段加以填充。这样，数据部分永远在 4 字节的整数倍时开始，实现起来比较方便。首部长度限制为 60 字节的缺点是有时不够用（如长的源路由），但这样做的用意是要用户尽量减少额外开销。

③ 服务类型：该 8 位字段说明分组所希望得到的服务质量，它允许主机制定网络上传输分组的服务种类及高层协议希望处理的当前数据报的方式，并设置数据报的重要性级别，允许选择分组的优先级，以及希望得到的可靠性和资源消耗。

④ 总长度：该 16 位字段给出 IP 分组的字节总数，包括分组头和数据长度。由于总长度字段有 16 位，所以最大 IP 分组允许有 65536 字节，这对某些子网来说是太长了，这时应将其划分成较短的分组报文段，每一段加上首部后构成一个完整的数据报。IP 的总长度并不是指未分段前的 IP 报文总长度，而是指分段后形成的 IP 分组的首部长度与数据长度的总和。

⑤ 标识符：该 16 位字段包含一个整数，用来使源站唯一地标识一个未分段的 IP 分组，该分组的标识符、源站和目的站地址都相同，且“协议”字段也相同。该字段可以帮助数据报重新组合在一起。IP 分组在传输时，期间可能会通过一些子网，这些子网允许的最大协议数据单元 PDU 的长度可能小于该 IP 分组长度，为处理这种情况，IP 为以数据报方式传送的 IP 分组提供了分段和重组功能。当一个路由器分割一个 IP 分组时，要把 IP 分组头中的大多数段值拷贝到每个分组片段中，这里的标识符段必须拷贝。它的主要目的是使目的站地址知道到达的哪些分组片断属于哪个 IP 分组。源站点计算机必须为发送的每个 IP 分组产生一个唯一的标识符字段值。为此，IP 软件在计算机存储中保持一个全局计数器，每建立一个 IP 分组就加 1，再把结果放到 IP 分组标识符字段中。

⑥ 标志段：3 位的标志段含有控制标志，如图 1.4 所示。不可分段位（DF, Don't Fragment）的意思是不许将数据报进行分段处理，因为有时目的站并不具备将收到的各段组装成原来数据报的能力。DF 置“1”，禁止分段；DF 置“0”，允许分段。当一

一个分组片到达时，分组头中的总长度是指该分组的长短，而不是原始报文的长短，这样就无法判断该报文的所有分组段是否已收集齐全。当“还有分组段位”置“0”时，就说明这个分组段的数据为原始报文分组的尾部，置“1”时，表明不是最后的分组段。未定义段，必须是“0”。

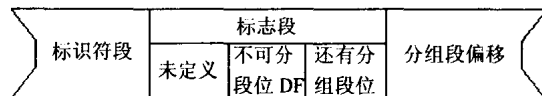


图 1.4 标志段的含义

⑦ 段偏移：13 位的段偏移（Fragment Offset）字段表明当前分组段在原始 IP 数据分组报文中数据起点的位置，以便目的地站点能够正确地重组原始数据报。

⑧ 生存时间：8 位的生存时间字段指定 IP 分组能在 Internet 互联网中停留的最长时间，记为 TTL（Time To Live）。当该值降为 0 时，IP 就被放弃。该段的值在 IP 分组每通过一个路由器时都减去 1。该段决定了源发 IP 分组在网上存活时间的最大值，它保证 IP 分组不会在一个互联网中无休止地循环往返传输，即使在路由表出现混乱，造成路由器为 IP 分组循环选择路由时也不会产生严重的后果。

⑨ 协议：8 位的协议字段表示哪一个高层协议将用于接收 IP 分组中的数据。高层协议的号码由 TCP/IP 中央权威管理机构予以分配。例如，该段值的十进制值表示对应于互联网控制报文协议 ICMP 是 1，对应于传输控制协议 TCP 是 6，对应于外部网关协议 EGP 是 8，对应于用户数据报协议 UDP 是 17，对应于 ISO/OSI RM 第 4 类传输层协议 TP4 是 29。

⑩ 分组头校验和：16 位的分组头校验和字段保证了 IP 分组头值的完整性，当 IP 分组头通过路由器时，分组头发生变化（如 TTL 生存时间段值减 1），校验和必须重新计算。校验和的计算非常简单，首先，在计算前将校验和字段的所有 16 位均赋值 0，然后 IP 分组头从头开始每两个字节为一个单位相加，若相加的结构有进位，则将和加 1。如此反复，直至所有分组头的信息都相加完为止，将最后的和值对 1 求补，即得出 16 位的校验和。

### 1.1.2 IP 地址

TCP/IP 协议是目前网络操作系统的默认协议，是目前最重要的网络协议。Internet 支持 TCP/IP 协议，它可以让不同网络结构、不同操作系统的计算机之间相互沟通。

在 TCP/IP 的网络上，每台连接在网络上的计算机与设备都被称为是一台“主机”，而主机与主机之间的沟通需要通过以下三个桥梁：IP 地址、子网掩码和 IP 路由器。

在以 TCP/IP 为通信协议的网络上，每台主机都必须拥有惟一的 IP 地址，该 IP 地址不但可以用来标识每一台主机，其中也隐含着网络的信息。

#### 1. 公用 IP 地址

IP 地址共占用 32 个二进制位，一般是由 4 个十进制数来表示 (W.X.Y.Z)，每个数字占一个字节 (1 个字节=8 位二进制)，字节与字节之间用点隔开，例如，202.197.147.80，

这个 32 位的 IP 地址包含了 Network ID 与 Host ID 两部分数据。

① Network ID 网络标识码。每个网络区域都有惟一的网络标识码。

② Host ID 主机标识码。同一个网络区域内的每一台主机都必须有惟一的主机标识码。

如果网络要与外界沟通, 为了避免网络内的主机所使用的 IP 地址与外界其他网络内的主机所使用的 IP 地址相同, 必须为网络申请一个 Network ID, 也就是整个网络区域内的主机都使用一个相同的 Network ID, 然后给网络内的每台主机分配惟一的主机 ID, 因此, 网络上的每台主机就都有惟一的 IP 地址 (Network ID 与 Host ID 的组合)。

为了适合各种不同大小规模的网络需求, IP 地址被分为 A、B、C、D、E 五大类, 其中 A、B、C 类是可供 Internet 网络上的主机使用的 IP 地址, 而 D、E 类是供特殊用途的 IP 地址。可以根据单位的网络规模来申请适合的 Network ID 类别。

① A 类: A 类的 IP 地址适合于超大型的网络, 其 Network ID 占用一个字节 (W), 但 W 的可用范围是 1 到 126, 因此, 总共有 126 个 A 类 Network ID。Host ID 共占用 X、Y、Z 三个字节, 它提供  $(2^{24}) - 2 = 16777214$  个 IP 地址。减二是因为 Host ID 全为 0 或 1 的地址被保留, 有特殊用途。

② B 类: B 类的 IP 地址适合于大、中型网络, 其 Network ID 占用两个字节 (W、X), 但 W 值的可用范围为 128~191, 它可提供  $(191 - 128 + 1) * 256 = 16384$  个 B 类的网络。Host ID 共占用 Y、Z 两个字节, 因此, 每个网络可以支持  $(2^{16}) - 2 = 65534$  台主机。

③ C 类: C 类的 IP 地址适合于小型网络, 其 Network ID 占用三个字节 (W、X、Y), 但 W 的值为 192~223, 它可提供  $(223 - 192 + 1) * 256 * 256 = 2097152$  个 C 类的网络。Host ID 只占用一个字节 (Z), 因此, 每个网络可支持  $(2^8) - 2 = 254$  台主机。

④ D 类: D 类的 Network ID 用于多点播送, 其 W 的范围为 224~239。

⑤ E 类: 这是一个用于将来扩展用的 Network ID。其 W 的范围为, 240~54。

这 5 大类的 IP 地址中, 只有 A、B、C 类可以供 Internet 网络上的主机使用, 但是在使用时, 还需排除以下几种特殊的 IP 地址。

① Network ID 不可以为 127: 127 是用来本机循环测试的, 不可以做其他用途。可以利用 ping 127.0.0.1 命令作为循环测试, 以便检查网卡与驱动程序是否正常运行。

② Network ID 与 Host ID: 以二进制位来看不可以全部是 1, 也不可以全部是 0 (以十进制来看不可以是 255 与 0)。例如, 不可以将某一台主机的 IP 设为 255.255.255.255。255 代表广播信息, 如果给出 255.255.255.255 这个地址送信息, 则表示是将信息广播给每一台主机。又如, 如果给出 202.197.147.255 这个地址发送信息: 则表示将信息广播给 Network ID 为 202.197.147 的网络内的每一台主机。

## 2. 专用 IP 的使用

如果单位所申请的 IP 地址数不够使用, 那么如何让公司内部网络所有的计算机都能够使用 TCP/IP 协议来沟通, 并连接到 Internet 并访问 Internet 上的资源呢? 或者因为安全性的考虑, 不让某些主机直接与外界沟通。利用专用 IP 地址是一个较好的办法。

在前面所介绍的 IP 属于公用 IP 地址, 这些地址可以直接用来连接 Internet, 但是专用 IP (参见表 1.1 所示) 是不能直接对外的 IP 地址, 只能够在公司内部 Intranet (企



业内部网)中使用。虽然专用 IP 无法直接连接到 Internet。但是却可以通过防火墙、NAT (Network Address Translation) 等设备间接地连接到 Internet, 这些设备介于 Internet 与公司内部 Intranet 之间, 利用 NAT 设备的公用 IP 来连接 Internet, 而公司内部的主机则使用专用 IP 即可, 他们可通过 NAT 来连接到 Internet, 访问 Internet 的资源, 接收邮件, 浏览网页等。从外界的 Internet 上只能看到使用公用 IP 地址的 NAT 设备, 但是看不到公司内部使用专用 IP 地址的主机。

表 1.1 专用 IP

专用 IP 地址	子网掩码
10.0.0.0~10.255.255.255	255.0.0.0
169.254.0.0~169.254.255.255	255.255.0.0
172.16.0.0~172.31.255.255	255.255.0.0
192.168.0.0~192.168.255.255	255.255.255.0

如果 Windows 计算机的 IP 地址设置为自动向 DHCP 服务器索取, 但是当计算机在索取 IP 地址时, 经过多次尝试后, 仍然无法索取到 IP 地址, 这时, Windows 计算机自动产生一个为 169.254.X.Y 的专用 IP 地址, 并暂时使用这个 IP 地址。

### 1.1.3 子网掩码

子网掩码也占用 32 位, 它可以用来从 IP 地址内得到 Network ID 和 Host ID, 也可以用来将网络切割为若干个子网。

#### 1. 利用子网掩码获得 IP 地址的 Network ID 和 Host ID

当 TCP/IP 网络上的主机相互通信时, 可以利用子网掩码得知这些主机是否处在相同的网络区段内, 即 Network ID 是否相同。

A 类 IP 地址的子网掩码为: 255.0.0.0; B 类 IP 地址的子网掩码为: 255.255.0.0; C 类 IP 地址的子网掩码为: 255.255.255.0 (255 为二进制的 8 位 1, 0 为二进制的 8 位 0)。其中为 1 的位用来定出 Network ID, 为 0 的位用来定出 Host ID。

例如, 某 A 主机的 IP 地址为 202.197.147.3, 则计算其 Network ID 的方法是将 IP 地址与子网掩码 (子网掩码为 255.255.255.0, 因该 IP 地址是 C 类地址) 两个值中相对应的二进制位做 AND 的逻辑运算。取得子网掩码为 1 的 IP 地址的位, 即为 Network ID。在 IP 地址中扣除 Network ID 后, 其余的部分就是 Host ID。

```

202.197.144.3 —— 11001010 11000101 10010011 00000011
255.255.255.0 —— 11111111 11111111 11111111 00000000
AND 后的结果 11001010 11000101 10010011 00000000
                (202)   (197)   (147)

```

因此, IP 地址 202.197.147.3 的 Network ID 就是 202.197.147, 而 Host ID 为 3。

若 B 主机的 IP 地址为 202.197.147.18 (子网掩码为 255.255.255.0)。当 A 主机要和 B 主机通信时, A 主机和 B 主机都会将自己的 IP 地址分别与子网掩码做 AND 运算, 得知这两台主机的 Network ID 都是 202.197.147, 因此, 判断这两台主机是在同一个网络区域内, 可以直接通信。但是, 如果两台主机不在同一个网络区域内 (Network ID