普通高等教育“十一五”国家级规划教材

普通高等学校计算机教育“十三五”规划教材

# 计算机网络安全基础

## （第5版）

## THE BASIS OF COMPUTER NETWORK SECURITY (5th edition)

袁津生 吴砚农 ◆ 主编

中国工信出版集团

人民邮电出版社 POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

普通高等学校计算机教育“十三五”规划教材

# 计算机网络安全基础

## （第5版）

THE BASIS OF COMPUTER NETWORK SECURITY

($5^{th}$ edition)

袁津生 吴砚农 ◆ 主编



人民邮电出版社

北京

**图书在版编目（CIP）数据**

计算机网络安全基础 / 袁津生，吴砚农主编. -- 5版. -- 北京 : 人民邮电出版社，2018.2
普通高等学校计算机教育“十三五”规划教材
ISBN 978-7-115-47621-0

Ⅰ. ①计… Ⅱ. ①袁… ②吴… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第319430号

## 内 容 提 要

计算机网络安全是全社会都关注并亟待解决的一个大问题。本书主要介绍如何保护自己的网络以及网络系统中的数据不被破坏和窃取，如何保证数据在传输过程中的安全，如何避免数据被篡改以及维护数据的真实性等内容。

本书重点讲述与计算机系统安全有关的一些基础知识，如安全级别、访问控制、数据加密、网络安全和数据安全等。

本书可作为高等院校计算机相关专业的教材，也可作为计算机网络的系统管理人员、安全技术人员的相关培训教材或参考书。

◆ 主　　编　袁津生　吴砚农
责任编辑　邹文波
责任印制　沈　蓉　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：22.5　　2018 年 2 月第 5 版
字数：607 千字　　2018 年 2 月河北第 1 次印刷

定价：54.00 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

# 第5版前言 PREFACE

计算机网络技术无疑是当今世界最为激动人心的高新技术之一。它的出现和快速发展，尤其是互联网的迅速成长，正在把一个世界连接成一个整体，“世界”这一概念也正在变小。网络在迅速发展的同时也改变着人们的传统生活方式，给人们带来了新的工作、学习以及娱乐的方式。

但是，在网络技术进步的同时，计算机网络安全也越来越引起世界各国的关注。随着计算机在人类生活各领域中的广泛应用，计算机病毒也被不断地产生和传播，计算机遭到非法入侵，重要资料丢失或被破坏，由此造成网络系统的瘫痪等，已给各个国家以及众多公司造成巨大的经济损失，甚至危及国家和地区的公共安全。可见计算机系统的安全问题关系到人类的生活与生存，我们必须给予充分的重视并设法解决。

编写本书的目的是帮助网络系统管理员在这个千变万化的网络世界中保护自己的网络以及网络系统中的数据，也就是说保护“数据”不被毁坏或窃取；同时本书还着重介绍了计算机安全的一些基础知识，如安全级别、访问控制、病毒、加密等。

目前，大多数高等院校都开设了计算机网络安全方面的课程。为了使本书跟上时代的步伐和更好地适应教师的教学工作和学生的学习，编者经过4年多的实践和教学循环，对第4版的部分内容进行了修订。修正了原书中一些过时的论述，增加了近几年来计算机网络安全领域发展的最新内容，希望对读者学习网络安全的相关知识有所帮助。

本书第3版为普通高等教育“十一五”国家级规划教材，并被教育部评为“普通高等教育精品教材”，受到全国各地许多高校师生的认可。第5版在保证原书结构不变的基础上，对内容进行了修订和扩充，并加强了理论性。具体调整如下。

（1）在第2章中增加了“网络安全风险管理及评估”的相关内容。

（2）重写了第5章中“计算机病毒的清除”一节的内容。

（3）在第7章中增加了“计算机网络取证技术”的相关内容。

（4）在第8章中增加了“移动互联网安全”和“云计算安全”的相关内容。

经过修订后，书中的内容更加完善，也更便于读者进行自学。同时也满足了目前高速发展的网络和安全技术的需要。

本书是编者基于多年的教学经验，参考若干资料整理而成的。在编写过程中，对基本概念、基础知识的介绍力求作到简明扼要；各章相互配合又自成体系，并附有小结和习题。为配合教学，本书还配有电子课件，可从人邮教育社区（www.ryjiaoyu.com）下载。建议本课程为 40 学时，其中讲课 30 学时，上机和课堂讨论 10 学时。学生应具备系统导论、操作系统、计算机网络和 C 语言的预备知识。

第 5 版的修订工作由袁津生、吴砚农、李群、段利国、王龙、闫俊伢共同完成，最后由袁津生统稿。其中，袁津生编写第 1 章，吴砚农编写第 2 章，李群编写第 3 章，段利国编写第 4 章、第 5 章，王龙编写第 6 章、第 7 章，闫俊伢编写了第 8 章、第 9 章。全书的修订还得到了众多老师的指导和帮助，在此一并表示感谢。

由于编写时间仓促，编者水平有限，书中难免有错误和不当之处，敬请读者批评指正。

袁津生

2018 年 1 月

# 目 录 CONTENTS

# 01 第1章 网络基础知识与因特网

计算机网络技术（Computer Network Technology）是当今世界最为激动人心的高新技术之一，它涉及计算机、通信、电子、自动化、光电子和多媒体等诸多学科。它的出现和快速发展，特别是因特网的迅猛发展正在使世界逐渐成为一个整体。

网络是建设信息高速公路和现代化信息社会的物质及技术基础，它的迅速发展使世界更加绚丽多彩。

本章将介绍网络参考模型、网络互连设备、局域网技术、广域网技术、TCP/IP基础以及因特网提供的主要服务等内容。

# 1.1 网络参考模型

在各种类型计算机之间进行信息传递是比较困难和麻烦的。20世纪80年代初期，国际标准化组织（ISO）认识到，需要一个网络模式来帮助厂商实现网络间的相互操作，于是在1984年发表了著名的开放系统互连（OSI）参考模型。这种模式是学习网络技术的最好的工具。

## 1.1.1 分层通信

在OSI参考模型中，将整个通信功能划分为7个层次。每一层的目的是向相邻的上一层提供服务，并且屏蔽服务实现的细节。模型设计成多层，像是在与另一台计算机对等层通信。实际上，通信是在同一计算机的相邻层之间进行的。7个层次自上到下分布，并具有不同的功能，每一层都按照一组协议来实现某些网络功能。7个层次之间的问题相对独立，而且易于分开解决，也无需过多地依赖于外部信息。

（1）应用层

应用层是OSI参考模型的最高层。它是应用进程访问网络服务的窗口。这一层直接为网络用户或应用程序提供各种各样的网络服务，它是计算机网络与最终用户间的界面。应用层提供的网络服务包括文件服务、打印服务、报文服务、目录服务、网络管理以及数据库服务等。

（2）表示层

表示层保证了通信设备之间的互操作性。该层的功能使得两台内部数据表示结构都不同的计算机（例如，一台设备使用某种编码，而另一台设备却使用另一种编码）能实现通信。它提供了一种对不同控制码、字符集和图形字符等的解释，而这种解释是使两台设备都能以相同方式理解相同的传输内容所必需的。表示层还负责为安全性引入的数据提供加密与解密，以及为提高传输效率提供必需的数据压缩及解压缩等功能。

（3）会话层

会话层是网络对话控制器，它建立、维护和同步通信设备之间的交互操作，保证每次会话都正常关闭而不会突然断开，使用户被挂起在一旁。会话层建立和验证用户之间的连接，包括口令和登录确认；它也控制数据的交换，决定以何种顺序将对话单元传送到传输层，以及在传输过程的哪一点需要接收端的确认。

（4）传输层

传输层负责整个消息从信源到信宿（端到端）的传递过程，同时保证整个消息无差错、按顺序地到达目的地，并在信源和信宿的层次上进行差错控制和流量控制。

（5）网络层

网络层负责数据包经过多条链路，由信源到信宿的传递过程，并保证每个数据包能够成功和有效率地从出发点到达目的地。为实现端到端的传递，网络层提供了两种服务：线路交换和路由选择。线路交换是在物理链路之间建立临时的连接，每个数据包都通过这个临时链路进行传输；路由选择是选择数据包传输的最佳路径。在这种情况下，每个数据包都可以通过不同的路由到达目的地，然后在目的地重新按照原始顺序组装起来。

（6）数据链路层

数据链路层从网络层接收数据，并加上有意义的比特位形成报文头和尾部（用来携带地址和其他控制信息）。这些附加信息的数据单元称为帧。数据链路层负责将数据帧无差错地从一个站点送到下一个相邻站点，即通过数据链路层协议在物理链路上实现可靠的数据的传输。

（7）物理层

物理层是 OSI 参考模型的最低层，它建立在物理通信介质的基础上，作为系统和通信介质的接口，用来实现数据链路实体间透明的比特（bit）流传输。为建立、维持和拆除物理连接，物理层规定了传输介质的机械特性、电气特性、功能特性和过程特性。

在上述 7 层中，上 5 层一般由软件实现，而下面的两层是由硬件和软件共同实现的。

### 1.1.2　信息格式

信息在各层间的格式变化如图 1-1 所示。

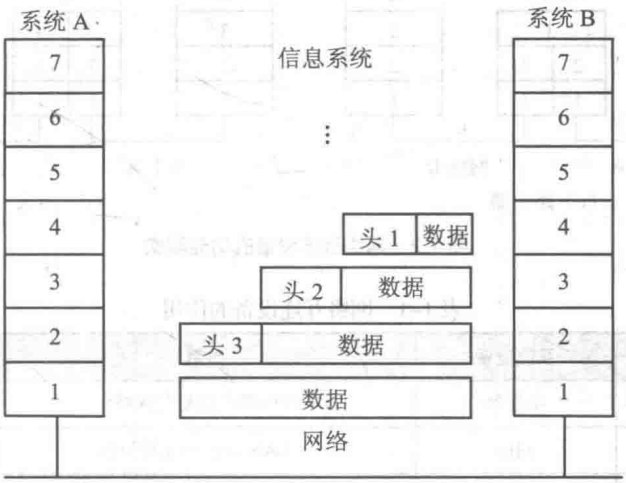


图 1-1　信息在各层之间的传递

在图 1-1 中，系统 B 的第 $n$ 层（$n$<7）是如何知道系统 A 的第 $n$ 层所做的处理呢？第 $n$ 层将其请求作为控制信息，放在传送信息前面、被称为“头”的里面，当对方的第 $n$ 层读到该头时，便可还原信息。

## 1.2　网络互连设备

网络互连设备是实现网络互连的关键，它们有 4 种主要的类型：中继器、网桥、路由器以及网关，这些设备在实现局域网（LAN）与 LAN 的连接中相对于 OSI 参考模型的不同层。中继器在 OSI 参考模型的第一层建立 LAN 对 LAN 的连接，网桥在第二层，路由器在第三层，网关则在第四至第七层。每种网络互连设备提供的功能与 OSI 参考模型规定的相应层的功能一致，但它们都可以使用所有低层提供的功能。

各种网络互连设备在 OSI 参考模型 7 层中的位置如图 1-2 所示，其作用如表 1-1 所示。

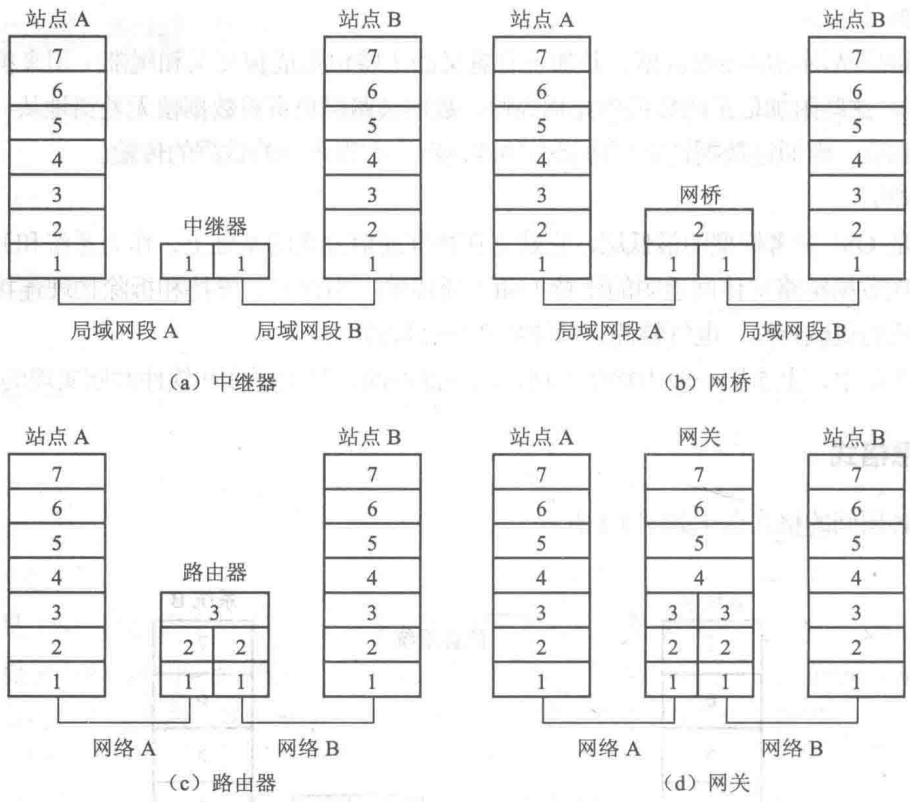


图 1-2　网络互连设备的功能层次

表 1-1　网络互连设备的作用

| OSI 层次 | 互连设备 | 作用 | 寻址功能 |
|---|---|---|---|
| 物理层 | 中继器 | 在电缆段间复制比特 | 无地址 |
| 数据链路层 | 网桥 | 在 LAN 之间存储转发帧 | MAC 地址 |
| 网络层 | 路由器 | 在不同的网络间存储转发分组 | 网络地址 |
| 传输层及以上 | 网关 | 提供不同体系间互连接口 | |

下面分别介绍 4 种主要类型的网络互连设备。

### 1.2.1　中继器和集线器

因特网中最简单的设备是中继器（Repeater），它的作用是放大电信号，提供电流以驱动长距离电缆。它工作在 OSI 参考模型的最低层（物理层），因此只能用来连接具有相同物理层协议的 LAN。对于数据链路层以上的协议来讲，用中继器互连起来的若干段电缆与单根电缆之间并没有差别（除了有一定的时间延迟）。中继器主要用于扩充 LAN 电线段（Segment）的距离限制。如粗线以太网，由于收发器只能提供 500m 的驱动能力，而 MAC（介质访问控制）协议的定时特性允许粗线以太网电缆最长为 2.5km。这样在每隔 500m 的网段之间就要利用中继器来连接。值得注意的是，中继器不具备检查错误和纠正错误的功能，因此错误的数据经中继器后仍被复制到另一电缆段。另外，中继器还会引入时延。使用中继器时应注意以下两点。

① 用中继器连接的以太网不能形成环路。

② 必须遵守 MAC 协议定时特性，即不能用中继器将电缆段无限连起来。例如，一个以太网上最多有 4 个中继器，连接 5 个电缆段。

灵活利用中继器，可以让总线型以太网适用多种布线结构变化。如一幢办公大楼分成多层，如果用逐层电缆绕线，不但浪费电缆，而且出故障时查找也不方便。如果用一根垂直的电缆穿过大楼，每层用中继器引入一水平电缆连起来则十分方便，这种配置一般垂直电缆用粗线，水平电缆用细电缆。

集线器（Hub）的工作原理与中继器类似，只是它能对更多的设备进行中继。注意，绝大多数集线器只能以双绞线介质连接，而中继器主要用同轴电缆进行连接。有些集线器只是集中连接的简单硬件设备（称作被动集线器）；有些则是复杂的电子部件，它们对到达各个物理位置的信息流进行监视和控制（称作主动集线器）。

### 1.2.2　网桥

网桥（Bridge）是一种在数据链路层实现互连的存储转发设备，它独立于高层设备，或者说与高层协议无关。它在两个局域网段之间对链路层帧进行接收、存储与转发，它把两个物理网络（段）连接成一个逻辑网络，使这个逻辑网络的行为看起来就像一个单独的物理网络一样。网桥通过数据链路层的逻辑链路控制子层（LLC）来选择子网路径。它接受完整的链路层帧，并对帧进行校验，然后查看介质存取控制层（MAC）的源地址和目的地址以决定该帧的去向。网桥在转发一帧前可以对其作一些修改，如在帧头加入或删除一些字段。由于网桥与高层协议无关，原则上网桥可以互连，如 DEC 网、TCP/IP 网或 XNS 网络。不过在实际应用中，网桥只有连接协议一致才能使用，如两个 802.X 网络，只有当它们都采用相同的网络操作系统才有价值；如果高层协议不一样，即便用网桥连接起来，应用程序也不能交换信息。

与上面介绍的中继器相比，网桥具有以下特点。

① 可以实现不同类型的 LAN 互连，而中继器只能实现以太网段间的相连。例如，用网桥可以把以太网和令牌环网（Token Ring）连起来。

② 利用网桥可以实现大范围局域网的互连。由于中继器受 MAC 定时特性的限制，一般只能将 5 段以太网连接起来，且不能超过一定的距离。但网桥工作在数据的链路层，不受 MAC 定时特性的限制，可以连接的网络跨度（距离）几乎是无限制的。

③ 利用网桥可以隔离错误帧，提高网络性能，而用中继器互连的以太网区段，随着用户数的增加，总线冲突加大，必将大大降低网络的性能。其原因在于：中继器只是简单地将信号从这一段电缆复制到另一段电缆，并不管这些信号的错与对，也不管有没有复制的必要。但网桥则不同，它收到一个帧后，先读取地址信息，以决定是将其复制转发还是丢弃，如果网桥连接的是以太网的话，网桥将判断收到的帧的目的地址是在发送帧的同一段还是在另一段。如果目的地址在本段网络，就不需要复制和转发，从而减轻了网络的压力，保证了多网络性能的稳定。此外，当以太网上的某一个工作站出现问题时，不会使整个网络的运行停顿。可见，网桥在此起到隔离故障的作用。

④ 网桥的引入可进一步提高网络的安全性，尤其是对局域网。因为局域网采用的是广播式通信方式，当一个工作站发送信息时，网络上的各个工作站点都可以收到。这对于银行或财务部门的网络来说是极不安全的，保密问题在此时就显得十分突出。因此，可采用网桥将一些重要部门的网络电缆与其他不相关部门的网络隔离开来，这将有助于加强网络的安全保密性能。

### 1.2.3 路由器

路由器（Router）是局域网和广域网之间进行互连的关键设备，通常的路由器都具有负载平衡、阻止广播风暴、控制网络流量以及提高系统容错能力等功能。一般来说，路由器多数都可支持多种协议，提供多种不同的物理接口，从而使不同厂家、不同规格的网络产品之间，以及不同协议的网络之间可以进行非常有效的网络互连。

路由器与网桥的最大差别在于网桥实现网络互连是在数据链路层，而路由器实现网络互连是在网络层。在网络层上实现网络互连需要相对复杂的功能，例如，路由选择，多路重发以及出错检测等均在这一层上用不同的方法来实现。与网桥相比，路由器的异构互连能力、阻塞控制能力和网段的隔离能力等都更强。此外，由于路由器能够隔离广播信息，从而可以将广播风暴隔离在局部的网段之内。

路由器有以下几个主要功能。

① 在网络间截获发送到远地网络段的网络层数据报文，并转发出去。

② 为不同网络之间的用户提供最佳的通信路径。为了实现这项功能，路由器要按照某种路由信息协议查找路由表。路由表中列出了整个因特网中包含的各个节点，以及节点间的路径情况和与它们相关的传输开销。如果到指定的节点有一条以上的路径，则基于预先确定的规则，使用最小时间算法或最优路径算法调节信息传输路径。如果某一网络路径发生了故障或堵塞，路由器可以为其选择另一条冗余路径，以保证网络的畅通。

③ 隔离子网，抑制广播风暴。任何子网中的广播包都将截止于路由器，因为路由器并不转发广播信息包。

④ 维护路由表，并与其他路由器交换路由信息，这是网络层数据报文转发的基础。

⑤ 数据报的差错处理，拥挤控制（网络流量控制）。

⑥ 利用网际协议，可以为网络管理员提供整个网络的有关信息和工作情况，以便于对网络进行有效管理。

⑦ 可进行数据包格式的转换，实现不同协议、不同体系结构网络的互连。例如，路由器可以用TCP/IP把以太网连到X.25网络上。一般来说，局域网和广域网的互连必须通过路由器才能实现。

路由器与网桥相比，它们之间最重要的一个区别就是：网桥独立于高层协议，它把几个物理网络连起来后提供给用户的仍然是一个逻辑网络，用户根本不知道有网桥存在；路由器则利用IP将网络分成几个逻辑子网，每个子网仍有各自独立的网络地址，是完全独立的自治域。

对于不同规模的网络，路由器所起的作用有所不同。

在主干网上，路由器的主要作用是路由选择。主干网上的路由器必须知道到达所有下层网络的路径。这需要维护庞大的路由表，并对连接状态的变化做尽可能迅速的反应。路由器的故障将会导致严重的信息传输问题。

在地区网中，路由器的主要作用是网络连接和路由选择，即连接下层各个基层网络单位——园区网，同时负责下层网络之间的数据转发。

在园区网内部，路由器的主要作用是分隔子网。早期的因特网基层单位是局域网，其中所有主机处于同一个逻辑网络中。随着网络规模的不断扩大，局域网演变成以高速主干和路由器连接的多个子网所组成的园区网。其中，各个子网在逻辑上独立，而路由器是唯一能够分隔它们的设备，它

负责子网间的报文转发和广播隔离，在边界上的路由器则负责与上层网络的连接。

### 1.2.4　网关

网关（Gateway）实现的网络互连发生在网络层之上，它是网络层以上的互连设备的总称。对于网络体系结构差异比较大的两个网络，从原理上来讲，在网络层以上实现网络互连是比较方便的。

对于局域网和广域网而言，下面三层的结构差异比较大，它们之间的耦合是十分复杂甚至是不可能实现的，因而习惯上多数情况都采用网关进行网络互连。

网络互连的层次越高，代价就会越大，效率也越低，但是能够互连差别更大的异构网。目前，典型的网络结构通常是由一个主干网和若干段子网组成，主干网与子网之间通常选用路由器进行连接，子网内部往往有若干个局域网，这些局域网之间采用中继器或网桥来进行连接。校园网、公用交换网、卫生网络和综合业务数字网络等，一般都采用网关进行互连。

网关通常由软件来实现，网关软件运行在服务器上或一台计算机上，以实现不同体系结构的网络之间或局域网与主机之间的连接。

网关连接的是不同体系的网络结构，它只可能针对某一特定应用而言，不可能有通用网关，所以有用于电子邮件的网关，用于远程终端仿真的网关等各种用途的网关。不管哪一种网关，都是在网络层以上进行协议转换的。

## 1.3　局域网技术

目前，流行的局域网主要有 3 种：以太网、令牌环网和 FDDI（光纤分布式数据接口）。本节对这 3 种局域网技术作简单介绍。

### 1.3.1　以太网和 IEEE 802.3

以太网是由施乐公司于 20 世纪 70 年代开发的，IEEE 802.3 发表于 1980 年，它是以以太网作为技术基础的。如今以太网和 IEEE 802.3 占据了局域网市场的最大份额，而以太网通常指所有采用载波监听多路访问/冲突检测（CSMA/CD）的局域网，包括 IEEE 802.3。

以太网和 IEEE 802.3 是两项较为相似的网络技术，它们都隶属于 CSMA/CD LAN，也都隶属于广播网络，换句话说，网络上所有的站点都能监听到网络上的所有数据帧，而不管它们自己是否是数据帧的目标站点；每个站点都必须通过检查接收到的数据帧来判断它自身是否为数据帧的目标站点，如果是，则将数据帧传至当前站点的更高协议层做进一步的处理。

从某种意义上说，以太网和 IEEE 802.3 之间也存在着细微的差别，以太网提供的服务与 OSI 参考模型的物理层和数据链路层一致，而 IEEE 802.3 仅仅规定了物理层和数据链路层的信道访问部分，并没有定义逻辑链路控制协议，这些协议的物理实现可以是主机内的接口卡或者是主机内的主电路板上的电路。

1. 物理连接

IEEE 802.3 规定了几种不同类型的物理层，而以太网仅仅定义了一种物理层，每一种 IEEE 802.3 物理层协议都有一个概括它们自身特点的名称。

以太网和 IEEE 802.3 10Base 5 的各个方面都极为相似，这两个协议所采用的拓扑结构都是总线型的，用连接电缆将末端网络站点和实际的网络传输媒介连接起来。在以太网中，这种连接电缆叫作收发器电缆，它与直接连接在物理网络媒介上的收发器设备连接。IEEE 802.3 的配置与以太网基本类似，仅仅在一些名称上稍有差别，如收发器被称作介质连接单元（MAU），连接电缆被称作连接单元接口（AUI）。在这两种情况下，连接电缆连接在末端网络站点接口板（或接口电路）上。

2. 数据帧格式

以太网和 IEEE 802.3 的帧格式如图 1-3 所示。

以太网和 IEEE 802.3 的帧格式的开始是一个 7 字节字段，被称为前同步码。它的作用是通知接收端站点有数据帧到达。前同步码中的内容为互相交替的“0”和“1”。

图 1-3 所示的数据帧格式中的 SOF 为数据帧开始的定界标志，其长度为 1 个字节。目标地址和源地址字段的长度均为 6 个字节，它们通常包含在以太网和 IEEE 802.3 接口卡的硬件中。源地址通常是单节点的地址，而目标地址则可以是单节点组成节点的地址，也可以是具有广播性质的全部节点的地址。


图 1-3 以太网和 IEEE 802.3 的帧格式

在以太网的数据帧中，类型字段具有两个字节，在物理层和数据链路层对数据帧所作的处理结束之后，该字段指明应该接收数据的上层协议；在 IEEE 802.3 的数据帧中，源地址字段之后是两个字节长的长度字段，它指明在该字段和数据帧检查顺序（FCS）字段之间所包含的数据的字节数。

在类型/长度字段之后是数据帧中的实际数据，在物理层和数据链路层对数据帧所作的处理结束之后，这些数据才被传送给上层协议。对于以太网而言，接收数据的上层协议用类型字段指定；对于 IEEE 802.3 来说，接收数据的上层协议必须在数据帧的数据部分内部加以定义，如果数据帧中包含的数据不足 64 个字节，就需插入相应的默认填补字节以使数据帧的大小达到 64 个字节。

数据帧检查顺序（FCS）字段中包含有循环冗余校验（CRC）值。CRC 值开始时是由发送数据帧的设备来确定的，然后通过接收数据帧设备的重新计算确定数据帧在传输过程中是否发生损坏。

## 1.3.2 令牌环网和 IEEE 802.5

令牌环网由 IBM 公司于 20 世纪 70 年代开发，至今仍是 IBM 的主要局域网技术。IEEE 802.5 规范几乎完全等同于或兼容于令牌环网。

1. 令牌的传递

令牌环网的介质接入控制机制采用的是分布式控制模式的循环方法。令牌环网传递网络的主要