网络安全管理与技术防护

姚小兰　主编

姚小兰　李保奎　董　宁　编著

胡昌振　审

北京理工大学出版社

·北 京·

图书在版编目(CIP)数据

网络安全管理与技术防护/姚小兰，李保奎，董宁编著. —北京：北京理工大学出版社，2002.5
ISBN 7－81045－906－6

Ⅰ.网…　Ⅱ.①姚…②李…③董…　Ⅲ.计算机网络－安全技术　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 001702 号

出版发行／北京理工大学出版社
社　　址／北京市海淀区中关村南大街 5 号
邮　　编／100081
电　　话／(010)68914775(办公室)　68459850(传真)　68912824(发行部)
网　　址／http：// www.bitpress.com.cn
电子邮箱／chiefedit@bitpress.com.cn
经　　销／全国各地新华书店
印　　刷／北京房山先锋印刷厂
装　　订／天津高村装订厂
开　　本／787 毫米×1092 毫米　1/16
印　　张／21.75
字　　数／510 千字
版　　次／2002 年 5 月第 1 版　　2002 年 5 月第 1 次印刷
印　　数／1～4000 册　　责任校对／郑兴玉
定　　价／32.00 元　　责任印制／刘京凤

序

网络已成为国家关键的政治、经济、军事资源，成为国民经济建设不可或缺的条件以及国家实力的新象征。随着信息技术的发展，社会对数据通信技术的依赖程度日益增大，越来越多的单位已把网络作为开展业务的基础，网络安全成为生死攸关的大问题。

网络安全涉及法律、管理和技术等诸多因素，是一个人-机-网复杂的系统问题。构筑网络安全防护体系固然离不开技术基础，但是，仅仅凭借技术解决网络安全问题是不现实的，人员的网络安全意识与安全素质是网络安全的核心，比网络安全技术更重要。据 CERT 统计，90％以上的信息网络安全事件都是由于人员误操作和网络与系统的误配置引起的。交通管理及相关设施对保证道路交通安全诚然十分重要，但是，汽车驾驶人员的安全意识和安全素质是基础。信息高速公路也如此，确保网络安全，应该从提高每一个网络操作者的安全意识开始。教育与培训，应该是网络安全领域的一个全员、全过程问题，网络信息安全防护体系也应该以人为本建立。

国防科学技术工业委员会信息网络安全培训以推进国防科技工业网络安全事业、传授最新的安全理念、讲解最新的安全技术进展和介绍我国先进的网络安全自主知识产品为目的，是实施我国国防科技工业系统网络安全的一个十分重要的组成部分。目前网络安全方面的技术书籍数目繁多，大多是国外书籍的翻译本，其内容或深或浅，很难满足培训要求。

本书是受国防科学技术工业委员会委托，由北京理工先河科技发展有限公司策划、胡昌振博士组织北京理工大学的一些多年从事网络安全研究的青年教师编写的。胡昌振博士是北京理工大学优秀的网络安全专家，学风严谨，研究深入，编写的这本书是一部网络安全培训的好教材。该书面向网络管理人员和安全技术管理人员，是一本学习和掌握网络安全知识的综合教材，对初学者、非专业人员以及普通的计算机用户都具有重要的参考与使用价值。

谨作此序，祝愿我国国防科技工业网络安全事业繁荣昌盛！

北京理工大学常务副校长、教授

前　言

网络引发着深刻变化：网络已成为一个国家最为关键的政治、经济、军事资源，成为国家实力的新象征；网络空间变成了“信息获取—信息处理—信息传递”的全方位、实时化和一体化斗争的焦点。通过非授权访问、恶意软件、数据库破坏、电子情报、电子攻击等手段，达到破坏其指挥系统的目的，为战争提供了新的舞台。

孙子曰“不战而屈人之兵，善之善者也”，自古以来，通过谋略与智慧，追求战场信息优势，一直是军事家追求的目标。现代战争中，信息的获取与传递日益迅捷，信息成为十分重要的战略资源，战争的形式也由原来以武力攻击消灭敌人转变为使敌人就范，而运用多种手段，以网络为平台攻击敌方指挥控制系统将是信息战的主要组成部分。要打赢未来的高技术战争，一个十分重要的、带全局性的问题，是要有效地保障自身的信息及信息系统的安全，信息安全已经是战略性的问题。未来战争首先从信息战开始，而网络攻击又是首选的攻击方式。保护网络信息安全，具有战略意义。

网络安全不仅是军事研究者所面临的课题，也是所有网络设计者与网络使用者同样关注的问题。网络安全涉及法律、管理和技术三个层次，是一项技术难度高、管理复杂、责任重大的工作，需要所有人员（包括管理者、技术人员、使用者等）共同努力、相互配合、共同完成，因此，与网络安全有关人员的安全意识培训，是网络安全的核心。

目前，网络安全方面的技术参考书，一般都具有相当深度，难以适合初学者或非专业人员的需要。从众多的网络安全技术书籍中找到合适的、综合性的教材，对初学者或非专业人员来说，绝非一件容易的事情。这本网络安全培训教材就是为满足初学者或非专业人员的这一需求，综合网络安全方面的有关知识编写的。

本教材内容包括四部分：第一部分介绍了有关网络及网络安全方面的基础知识，包括OSI安全体系结构和信息安全技术；第二部分介绍了网络安全威胁和风险管理，包括网络安全缺陷、紧急事件处理及风险评估等；第三部分介绍了网络防护技术，包括加密技术、身份识别与验证、防火墙技术、恶意码、虚拟专用网络技术、网络扫描技术、网络攻击检测技术及安全防护体系；第四部分讲述了网络安全实现问题，包括网络安全要素、安全策略、网络系统生命周期、网络安全管理及法律保障等。

本教材面向广大的网络管理人员和安全技术管理人员，对于普通的用户也有很大的参考和使用价值。对于初学者和非专业人员来说，是学习和掌握网络安全方面的综合性教材，是快速达到目标的捷径。

北京理工大学的胡昌振教授对本书的全部书稿进行了认真、细致的审阅，并提出了许多宝贵和重要的修改意见，在此表示诚挚的感谢！

在本书的编写过程中，得到了博士生、硕士生等许多同学的帮助，在此向刘峰、朱金富、林建江、潘志康、牛峰、廖峰、姚金秋、曹传文等人表示感谢。由于时间仓促及编者水平有限，书中许多地方有待进一步改进，欢迎广大读者批评指正。

编　者

2001 年 9 月 8 日

目　录

第一部分　网络安全概论

第二部分　网络安全威胁及风险管理

第三部分 网络安全技术防护

第四部分 网络安全实现

第 1 章　网络的基础知识

1.1　局域网与广域网

计算机网络是连接两台或多台计算机并使之能够相互通信的实体。在构成网络时，计算机与计算机之间是通过电缆和其他网络连接设备连接起来的。计算机网络可分为局域网（LAN）与广域网（WAN）。局域网一般把地理范围小的计算机连接在一起，例如一个建筑物或一个校园的网络，通常规模较小。而广域网是在较大的地理范围内把计算机连接起来，例如大的企业网络将位于不同城市的网络和计算机连接成一个广域网。广域网可将多个局域网连接起来，也可将在全世界不同地方的局域网连接起来。

计算机网络是一个非常复杂的系统，包括一系列的软件、硬件和相关标准。但基本组成不外乎服务器、客户机、网络连接设备和网络操作系统等几个部分。

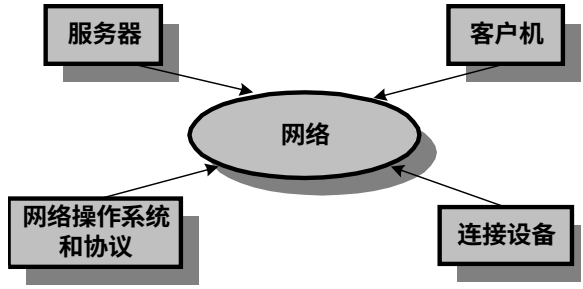

图 1.1　基本网络的组成

1. 服务器

服务器在网络中往往处于中心地位，主要为网络上其他计算机或设备提供各种功能的服务，包括文件服务、打印服务、通信服务，还有一些近期发展很快的应用服务，如 WWW 服务、FTP 服务。根据不同的服务功能，服务器可相应地划分为特定的服务器，如文件服务器、应用程序服务器。应当指出，服务器本身也是一台计算机，只不过比一般计算机功能更强。组建网络时，服务器硬件平台一定要根据网络的应用目的来选择，否则不是大材小用就是不堪重负。

2. 客户机

客户机也叫工作站，可享用服务器提供的各种服务。客户机分别运行独立的操作系统，操作系统必须为服务器所认可。有的网络和计算机之间互为服务器和客户机，这样的计算机又称为等机。

3. 网络连接设备

网络连接设备包括网络适配器、网络传输介质和其他的网络设备。网络适配器俗称网卡，

负责完成计算机之间的数据接收和发送。网络传输介质有双绞线、光纤等。其他的网络设备有中继器、网桥、路由器、调制解调器等。网络连接设备直接影响通信的带宽，制约着网络的传输效率。不同功能的网络，对带宽的要求不同，对相应的网络连接设备的要求也就不同。

4. 网络操作系统和协议

像单个计算机的操作系统一样，整个网络的资源和运行也必须由操作系统来管理。目前主流的网络操作系统有 Unix、Windows NT 和 NetWare。协议作为联网的计算机之间或网络之间互相通信和理解的一组规则和标准，也是网络必不可少的组成部分。

1.2 网络拓扑结构

通常将网络中的计算机作为一个节点来对待，网络拓扑指的是这些节点在空间的布局形式，它代表了一个网络的基本结构。由于改变网络拓扑结构的难度较大，因此在组建网络时，选择合适的拓扑结构非常重要。目前最常用的形式有星形、总线形和环形等。

1.2.1 星形拓扑网络

星形拓扑由中心主节点和其他的从节点组成，主节点可直接与从节点通信，而从节点之间必须经过主节点才能通信。通常主节点由一种称为集线器（hub）的设备充当，因此网上的计算机之间都是通过集线器来相互通信的。图 1.2 是星形拓扑网络的示意图。

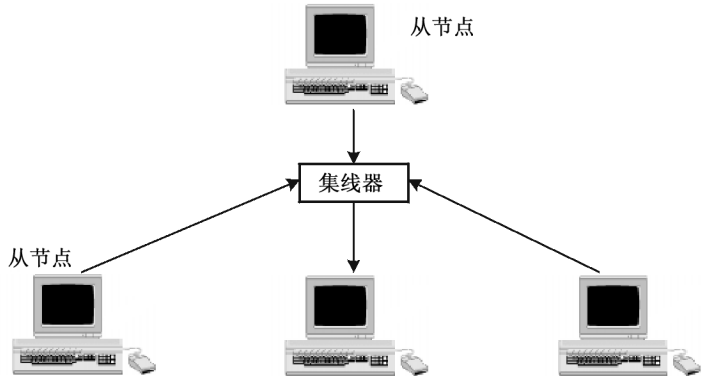

图 1.2 星形拓扑网络

星形拓扑以主节点为中心，集线器是中心主节点，联网的计算机无论是服务器，还是客户机都是从节点，数据从每个从节点传输到主节点，然后由主节点传输到目的节点。联网计算机的数量由集线器的端口数决定，当要连接的计算机比较多时，可以使用多个集线器，将多个集线器连接起来，不过现在的集线器正逐步为交换机所替代。

星形拓扑的优点是故障隔离和容易检测，重新配置灵活，任何节点的计算机的故障不会影响其他节点的计算机，网络运行时增减节点也不会影响正常运行。但是由于过分依赖中心节点集线器，中心节点的故障将导致整个网络的瘫痪。而且每台计算机都要利用单独的电缆与集线器连接，需要的电缆较多。在很多情况下，同星形网络的优势比起来，这些不足和开销是微不足道的，因此星形网络拓扑已成为主流的拓扑结构。

1.2.2　总线形拓扑网络

总线形拓扑是一种比较简单的结构，采用一条称为公共总线的传输介质，各节点与总线连接，信息沿总线介质逐个节点地广播传送。这种结构非常简单，所需的电缆也很少。图 1.3 是总线形拓扑网络的示意图。这种结构安装容易，布线简单，但是由于过分依赖于总线，只要总线某一点发生故障，该点两侧的计算机便无法正常通信。

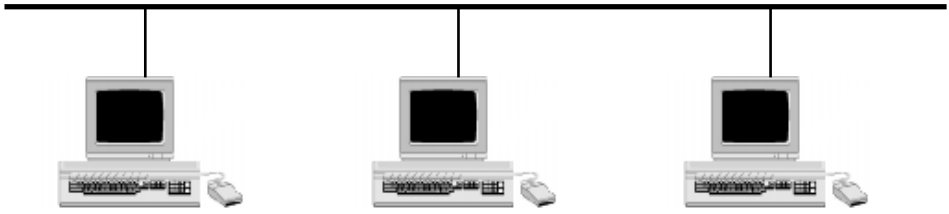

图 1.3　总线形拓扑网络

1.2.3　环形拓扑网络

环形网络拓扑是一个闭环，各节点连到环上，信息沿环路逐个节点传递信息。图 1.4 是环形拓扑网络的示意图。

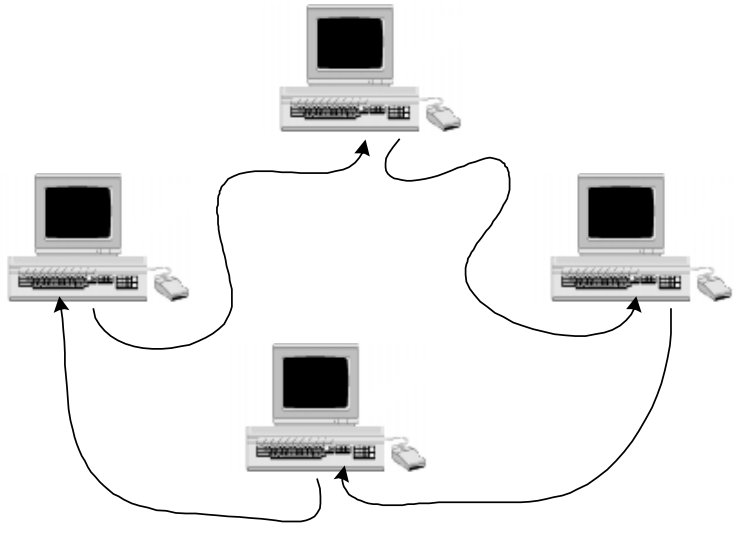

图 1.4　环形拓扑网络

环形拓扑网络是单向传输信息的点到点连接的结构，非常适合光纤介质。不过环上任何一点的故障都会导致整个网络的瘫痪。环形拓扑支持的计算机数据量比总线形和星形多，往往用来设计覆盖地理范围较大的网络，如校园的主干网络。

网络拓扑结构是网络的基本要素，处于基础的地位，选择合适的网络拓扑很重要。

确定拓扑结构，要考虑连网的计算机数量、地理覆盖范围、网络节点变动的情况，以及今后的升级或扩展等因素。三种拓扑结构各有千秋，选择时应综合考虑、全面衡量。

简单的网络是单一的结构，复杂的网络则将几种拓扑结构组合起来，如大型的校园网往往三种结构都包括。总的说来，星形拓扑的使用最广泛，虽然初次安装费用可能高一些，但是它作为一种可靠的网络拓扑，可以集中管理网络，还可以方便地变动网络节点和扩展网络，特别是双绞线介质的大量使用和交换技术的发展，更奠定了它的主导地位。

1.3 以太网

以太网和 TCP/IP 都有一段发展的历史。以太网由 Xerox Palo Alto 研究中心 （Xerox PARC）的 Robert Metcalf、Daniel Boggs 和他们的同事设计。当美国为 ARPANET 开发 TCP/IP 时，以太网已经相当成熟了。自从 TCP/IP 产生后，两者就紧密地结合在一起。大多数 TCP/IP 在实现中都可看到以太网 II 的设计思想。

以太网有两代。第一代以太网出现于 1980 年，由 Digital、Intel 和 Xerox 共同开发。第一代以太网通常称为 Ethernet I（或 DIX 1.0）。新版以太网于 1982 年出现，称为 Ethernet II（或 DIX 2.0）。如今 Ethernet I 已经很少用了，但我们还会在老的硬件里遇到它。与之形成对比的是，Ethernet II 在 TCP/IP 网络中普遍使用。

以太网的消亡已经被预言了多次，因为专家们预测以太网会让步于令牌环、FDDI 以及 ATM 的发展。但是以太网仍然生存了下来，其原因是多方面的。10Mbit/s 以太网提供的服务能胜任除了那些极其苛刻的要求之外的所有局域网应用的要求。只要使用桥接器、路由器或者交换机把网络分段，就可以把本地通信量保持在一定程度上，提供令人满意的性能。除了基本的稳固性，以太网也已经证明了它的扩展能力。同轴以太网已经向使用非屏蔽双绞线的方向转变。现在人们已经开发出了的 100Mbit/s 的以太网，它的成本比 FDDI 和 ATM 都要低得多。局域网管理员不必离开已熟悉的以太网环境就能享受高速率。现在千兆以太网正在形成，它可使以太网充分利用光缆提供的网络带宽。尽管有一天像 ATM 这样的技术可能使以太网黯然失色，但在未来几年内，以太网仍将是最流行的局域网布线方式。

1.3.1 以太网是怎样运作的

大多数局域网使用基带介质，在每个时刻都只有一台计算机在发送信息。因此网络设计者必须用一种方法，让多个计算机共享介质。有一种机制称为“ 访问控制方法 ”，它决定计算机如何共享一个介质。

以太网使用的访问控制方法很基本，如果节点需要在以太网上传输消息，在发送信息之前它要做的仅仅是监听网络。如果网络上没有信息在传输，那节点就开始发送自己的消息。这种访问控制方法的正式名称叫做“ 载波侦听多路访问 ”（CSMA）。所谓载波侦听不过意味着节点在交谈以前先倾听网络的动静。

如果这就是全部内容，那以太网确实是够简单的。不幸的是，电波信号通过线路传输需要时间，因而产生的延迟会给网络带来一些问题。两个节点可能会同时发现网络上没有消息在传输，于是它们立即开始传送消息，在网络上产生两个信号，这种情况称为“ 冲突 ”。网上发生冲突时，传输的数据无效。此时，节点在发送消息时继续侦听网络，很快，它便察觉到发生了冲突（冲突很容易检测，因为冲突发生时，两个信号的叠加会产生超过正常水平的电位）。当传输数据的节点侦测到了冲突时，它便发送一个干扰信号，使刚发送的帧无效，并通

知其他所有节点网络上发生了冲突。然后发送消息的节点暂时停止发送。在重新发送消息之前节点等待的时间是随机确定的。随机延时减小了再次发生冲突的可能性。检测冲突的机制称为“冲突检测”(CD)。以太网开发的访问控制方法全称为“带有冲突检测的载波侦听多路访问”。由于这种称呼有点拗口，因此通常简称为 CSMA/CD。

冲突检测机制有一个问题，即在极短的帧之间发生的冲突可能检测不到。节点只在传输时监听网络冲突。如果消息传送完毕后发生冲突，冲突就不会被发现。为了保证能够检测到所有的冲突，必须指定一个最小帧长度。最小帧长确保节点在发送完成之前所有的帧都能到达网络上的节点。因此传输节点在停止发送以前总能检测到冲突。

以太网 CSMA/CD 是一个有效的协议，在一个负荷适中的网络上，用于以太网操作的网络带宽极少。如果冲突相对较少，它就不会严重损害网络性能。

然而如果发生很多冲突，那问题就比较严重了。CSMA 网络通常称为“基于竞争的网络”。当竞相访问网络的节点过多时，冲突开始主导网络，网络性能严重下降，最终会因为大部分传送尝试都产生冲突而使传输变得很困难。从理论上说，冲突可以使得网络上所有节点都无法访问网络。因为不保证节点能得到传输消息的机会（换句话说，节点是不是能发送消息只是存在可能性，不保证一定能发送），所以以太网有时也称为“或然网络”。

无论如何，以太网（指 EthernetII 和 IEEE 802.3）仍然是最流行的网络标准。在大多数情况下它都工作得很好。另外它也很简单，所需的网络部件相对也比较便宜。

1.3.2　以太网介质

以太网最初使用的介质是粗同轴电缆，因此以太网也被称为“粗缆以太网”，或简称为“ThickNet”。电缆连接的网段最长可达 500m。电缆可支持多达 100 个节点，以 10Mbit/s 的速率传输。然而，以太网用的这种粗缆（以及它所要求的网络硬件）的价格却相当贵，因此，在一定程度上限制了网络的发展。

特别为以太网开发的其他介质包括一种比较细的同轴电缆。用这种电缆的以太网被称为细缆以太网或简单 ThinNet。细缆以太网网段长限于 185m 以内，最多支持 30 个节点。细缆以太网的传输速率与粗缆以太网一样，都是 10Mbit/s。对于网络硬件的要求，细缆以太网要比粗缆以太网简单得多，所以细缆以太网的造价要比粗缆以太网低很多。

这两种以太网介质（粗缆和细缆）都被作为 IEEE 的 CSMA/CD 网络工业标准。

1.3.3　以太网帧格式

以太网 II 帧格式与 TCP/IP 有密切的关系，因此两者完全相互适应。而把 TCP/IP 用于其他类型的网络还必须多做一些工作。

一般而言，帧格式的第一位都显示在帧图的左边，所以应该从左向右看，从帧格式的开头读到结尾。表 1.1 中给出了以太网 II 帧的域。许多协议标准都用到了一个术语，即 octet（八位组），它表示八比特组（由于八位组与字节是同一回事，所以新的标准都使用字节）。

将所有域的长度加起来，就可发现以太网帧的最大长度为 1518bytes（6+6+2+1500+4=1518），最小帧长度为 64bytes（6+6+2+46+4=64）。64bytes 的最小长度再加上 8bytes 前导就构成了最小帧长 576bits，这一长度足以保证所有冲突都能检测到。

表 1.1 以太网 II 帧格式的域

前导	长度为 8bytes（64bits），标识以太网帧的开始。前 7 个字节的位模式为 10101010，最后一个字节的位模式为 10101011。这种特殊模式标志帧的开始，但是前导不属于帧，也不计入帧的长度
目的地址	6bytes（48bits），指出帧要去往的节点物理地址。接收节点检查该域，确定自己是不是帧的目的地
源地址	6bytes（48bits）指帧起源的节点物理地址，接收节点用这个地址定位响应帧返回的地址
类型	2bytes（16bits），描述帧携带数据的类型。这个域的信息一般指以太类型
数据	这个域包含从上层接收到的协议数据单元。域的最小长度为 46bytes，最大长度为 1500bytes。如果数据长度小于 46bytes，上层协议必须使用全 0 字节补足最小长度
帧校验序列（FCS）	4bytes（32bits）码，检测传输中产生的差错。校验码由一种叫做“循环冗余校验”（CRC）的算法推出。接收端重新计算 CRC，将计算结果与帧校验序列进行对比。如果两者匹配，说明帧没有崩溃

1.3.4 以太网寻址

以太网使用一种非常简单的寻址机制在网络上传输帧。发送节点将目的节点地址插入帧的目的地址域。然后将帧发送到网络上，所有节点都要检查帧。如果某节点在目的地址域发现是自己的地址，那么该节点接收帧。

为了使这种模式动作起来，网络中的每个节点都必须有惟一的编号，以太网的设计者创建了一种模式，它可以保证全世界的以太网设备都有惟一的编号。

以太网地址的格式包括三个域，共 48bits。比特位的编码从 bit 0（低位比特）到 bit 47（高位比特）。地址左边的第一位比特是高位比特，地址的排列如同传统的二进制数——从高位比特到低位比特，从左读到右：

物理／多播比特　生产厂商代码（23bits）全球管理地址（24bits）

典型的以太网地址都以六个两位的十六进制数表示。这种表达法比较简单，因为每个八位组映射为两位十六进制数。十六进制表示法使得人们浏览地址更方便。十六进制非常容易使用，所以很少有必要考虑以太网的二进制地址。

比特 47（高位比特）是物理／多播（P/M）比特。这个位为 0 时，帧指定网络上节点的物理地址。P/M 设置为 0 用于单播消息。如果位值为 1，地址是一个广播地址。

以太网地址的前三个八位组构成厂商码。生产以太网设备的每家制造商都由注册中心分配一个或多个 24bits 的身份码（所有厂家的身份码都以 P/M 位为 0 开始）。注册最初由 Xerox 公司执行，但是后来这个任务委派给了 IEEE。表 1.2 列出了一些典型的厂商码，它们都已写入 RFC1700，冠名为“已分配码”。

- 厂商需要使用多播地址时，常常使用厂商代码，把 P/M 位改一下。

地址的剩余部分是一个 24 位码，惟一标识厂家制造的每一种设备。惟一厂商码与每个硬件设备的惟一码合并，构成每个硬件设备惟一的以太网地址。这个地址固化到硬件里，通常称为物理地址。由于地址基于全球范围登记，因此它也称为“全球管理地址”。

表 1.2　以太网厂商举例

厂商代码	厂　　商
00 80 C2	IEE 802.1 委员会
00 AA 00	Intel 公司
08 00 09	惠普公司
08 00 14	Novell 公司
08 00 2B	DEC 公司
08 00 56	斯坦福大学
08 00 69	IBM 公司

- 可以替换以太网适配器的物理地址，修改网络驱动器里的参数即可。本地创建的地址称为本地管理地址。

另外还有一个以太网地址。全由 1 组成的地址是标准的以太网广播地址，用十六进制表示为 FF FF FF FF FF FF。用广播地址发送的消息路由取决于网络层。广播消息不允许通过路由器，只能在本地网络中传播。

下面对以太网地址作一概括，以太网地址可分为三类：

- 全球管理地址（固化到硬件里的物理地址），物理/多播位（高位）的值为 0；
- 多播地址，物理/多播位（高位）的值为 1；
- 广播地址，全由 1 组成。

1.3.5　以太类型

在与 TCP/IP 的关系中，类型域（或以太类型）扮演着重要的角色。这个域标识数据域传送的数据类型。以太类型用于协议复用，确保数据传到正确的上层协议栈。已分配码 RFC（RFC 1700）列出了已经分配给特定协议和组织的以太类型码。表 1.3 给出了 RFC 1700 中常用的以太类型值。

表 1.3　以太类型数字举例

以太类型	以太类型	数据类型
2048	0800	以太网 IP（Ipv4）
2053	0805	X.25Level3
205	0806	ARP
33023	80FF-8103	Wellfleet Communications
32873	8069	AT&T

在 IEEE 802.3 版的以太网中，类型域被长度域取代，长度域的最大值限为 1500，所有以太类型值都为 1501（5DDh）或者更大。因此系统通过检查类型或长度域的值，可以区分 IEEE 802.3 帧和以太网 II 帧。

1.4 IEEE 局域网标准

制定国际局域网标准的主要组织是国际电气电子工程师协会（IEEE），它是世界上最大的专业性组织。网络标准由 802 委员会处理，委员会之所以称 802 是因为该委员会于 1980 年 2 月举行第一次会议。国际标准化组织（ISO）建立了国际局域网标准，在 ISO 8802 标准中采用了 IEEE 802 标准（基于 IEEE 802.3 的 ISO 标准称为 ISO 88023）。

OSI 的数据链路层细分为两个子层。这种划分让 IEEE 能够在所有局域网协议上指派一个公共层。数据链路层在两个子层间的职责如下：

① 逻辑链路控制（LLC）子层提供 IEEE 底层协议与网络层之间的公共接口。LLC 在同一个网段的各个节点之间传送数据。

② 介质访问控制（MAC）子层是一种能够使网络节点共享公共网络的机制。

下面介绍三个 802.x 标准：

- 802.2，定义 LLC 子层。
- 802.3，定义 MAC 子层和源于以太网 II 的 CSMA/CD 网络物理层。
- 802.5，定义 MAC 子层和源于 IBM 令牌环网的物理层。

注意：802.2 LLC 协议充当 802.3 和 802.5 网络之上的通用协议。这一设计简化了网络层对不同类型局域网的适应过程。下面分别讨论这些协议中的每一个协议。首先让我们看一看 802 网络的寻址模式。

1.4.1 IEEE 802 寻址

节点物理地址用于数据帧的本地传输。开发物理地址格式的时候，IEEE 要求格式能够用于所有 802 协议。最终选择的地址格式与以太网 II 的地址格式非常相似。在 IEEE 模型中，物理地址是 MAC 协议子层的功能，所以物理地址经常称作 MAC 地址。IEEE 定义了 16 位和 48 位地址格式，16 位地址很少使用。

网络上的所有节点都必须配置为同样的地址格式。下面举例说明 48 位地址格式。这种地址格式已经被 IEEE 802、ISO 8802 以及其他像帧中继这样的网络标准（比）所采用。虽然格式类似于以太网 II 的地址格式，但它们之间还是存在一些差别。

图 1.5 IEEE 802 标准的网络功能分层模型

高位比特（比特 47）指定地址为单一地址或组地址，所以这个比特位也称为 I/G 比特。如果 I/G 比特值为 0，那么地址为单一地址（单一地址可比作以太网 II 的物理地址）。如果 I/G 比特值为 1，那么地址为组地址（组地址可比作以太网 II 的多播地址）。换句话说，除了术语不一样以外，I/G 比特的用途和功能都与以太网 II P/M 比特相同。

IEEE 802 的地址格式：

组织惟一标识符（22bits）、组织管理地址（24bits）、U/L 比特（0＝全局管理地址/1＝本地管理地址）、I/G 比特（0＝单一地址/1＝组地址）。

比特 46 把地址分配为全局或本地管理地址。因此比特 46 称为 U/L 比特。如果 U/L 比特

的值为 0，则地址为全局管理。全局管理地址基于一个 22 位标识符和一个 24 位地址。22 位标识符惟一分配给某个组织。24 位地址由组织分配给它制造的每件设备。全局地址可以通过配置网络适配器驱动器的参数覆盖。如果 U/L 比特的值为 1，则地址为本地管理。

分配的惟一标识符与分配的惟一地址组合，这样，每个网络设备都可以分配一个全球惟一的 IEEE 802 地址。现在由 IEEE 为组织分配惟一标识符，这种责任已经从 Xerox 转移到了 IEEE。总体而言，全局管理地址更好一些，因为它们避免了地址冲突的发生。

1.4.2　IEEE 802.2 逻辑链路控制

LLC 子层执行两个基本功能：帧传递、协议复用和解复用。LLC 子层的许多服务都是可选的，而且可以由上层协议代替执行。

1. 协议复用和解复用

LLC 子层的复用能力能够支持多个上层协议栈。这种功能通过以太网 II 帧的以太类型域完成。802.2 LLC 使用了一种不同的机制，叫做“链路服务访问点”（LASP）。每个上层协议都分配有一个 LSAP，执行逻辑地址的功能。LSAP 标识与每个帧对应的协议栈，使得 LLC 能够将帧传送给正确的协议栈。

IEEE 协议与以太网 II 之间最显著的区别就是 LSAP 和以太类型机制之间的区别。要支持 TCP/IP，必须使用“子网访问协议”（SNAP），它是 LLC 协议的扩展。

2. 传送服务

LLC 负责在计算机之间传送数据。数据传送服务有两个功能：流量控制和差错恢复。LLC 提供三种水平的传送服务，保证不同程度的通信完整性。

（1）流量控制

通信设备都设有接收缓冲区——数据等待设备处理时能够存储数据的内存。如果数据到达的速度比设备从接收缓冲区读取数据的速度快，那么就可能丢失一些数据。LLC 的责任之一就是防止缓冲区溢出。

主要有两种机制用于控制通信流：

- “停止等待”机制。这种方法不复杂，它要求接收设备对接收到的每个帧进行确认。确认消息表示接收端有能力接收更多数据。发送端在送出更多数据以前先等待确认消息。这一技术很有效，但有时效率不高，因为确认过程使数据传输的速度慢了下来。而且，由于每个数据帧都产生一个确认帧，这项技术实际使网络流量增加了一倍。
- “滑动窗口”机制。这种方法可使接收端一次确认多个帧。所谓窗口就是在给定时间内能够传送的帧数。两个设备为交换数据建立连接时，它们协商好适当的窗口大小。发送设备最多能传送窗口规定的帧数。达到这个数目后，发送设备必须暂停。接收设备可以一次确认一条消息的多个帧。帧经确认后，窗口向前滑动，这样发送者能够发送更多的帧。在全双工对话中，发送端可同时发送数据和接收确认消息，滑动窗口机制可产生更规则的数据流。由于一条消息可确认多个帧，因此网络流量的增加并不像停止等待机制那么明显。

（2）差错恢复

差错恢复可由 LLC 执行，这取决于所选的设备。MAC 子层检测差错但不执行差错恢复。LLC 差错恢复采用一种“ARQ（自动重复请求）”技术。就 ARQ 而言，接收节点必须确