面向21世纪 高职高专计算机专业教材

网络安全与维护

费如纯 主编

人民交通出版社

面向21世纪 高职高专计算机专业教材

Wangluo Anquan yu Weihu

网络安全与维护

费如纯 主编

人民交通出版社

内 容 提 要

本书在简要介绍 Internet 中使用的 TCP/IP 协议的基础上，重点讲解了保障信息保密性、完整性、不可否认性的一些典型算法和通信过程中的一些安全协议，全面阐述了防火墙技术、Windows 安全技术、Web 安全技术、电子支付安全、入侵检测技术、网络攻击及预防技术，并讨论了网络安全评估的内容、级别、标准等。通过本课程的学习，读者可以比较全面地掌握网络安全的基本概念，熟悉保障网络安全的基本技术，培养基本的网络安全管理的能力。

本书注重理论与实践相结合，避免过多过深的理论讲解，可读性强，指导性强，可作为高职高专计算机科学与技术类专业的教材，也可供网络安全技术爱好者参考使用。

图书在版编目(CIP)数据

网络安全与维护/费如纯主编. —北京：人民交通出版社，2004.1

ISBN 7-114-04920-X

Ⅰ.网… Ⅱ.费… 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(2003)第121615号

面向21世纪高职高专计算机专业教材

网络安全与维护

费如纯 主编

正文设计：姚亚妮 责任校对：尹 静 责任印制：杨柏力

人民交通出版社出版发行

(100013 北京和平里东街10号 010 64216602)

各地新华书店经销

三河市宝日文龙印务有限公司印刷

开本：787 ×1092 1/16 印张：21.5 字数：534千

2004年1月 第1版

2004年1月 第1版 第1次印刷

印数：0001 — 3000册 定价：34.00元

ISBN 7-114-04920-X

编写人员名单

主　　编：费如纯（本溪冶金高等专科学校）

副 主 编：李华霖（天津交通职业学院）

叶忠杰（浙江交通职业技术学院）

参与编写：董迪晶（天津交通职业学院）

高　洁（天津交通职业学院）

杨国震（天津交通职业学院）

杨志平（浙江交通职业技术学院）

高　军（本溪冶金高等专科学校）

王海波（本溪冶金高等专科学校）

刘丽华（本溪冶金高等专科学校）

律德财（本溪冶金高等专科学校）

刘宏妮（本溪冶金高等专科学校）

本书策划组成员名单

白崤　翁志新　张景　黄景宇

前言 FOREWORD

根据21世纪高等职业教育的新趋势和计算机专业学科建设的要求，结合目前众多高职高专院校的教学计划，人民交通出版社组织全国十几所高职高专院校的多年从事一线教学、实践能力强且具有丰富教材编写经验的教师，编写了这套“面向21世纪高职高专计算机专业教材”，共21本（书目附后），涵盖了高职高专计算机及相关专业的主要课程。在编写过程中认真贯彻了教育部《关于加强高职高专教育人才培养工作的意见》的精神。内容以必需、够用为度，既注重基础知识的讲解，又注意从实际应用出发，满足社会对计算机类专业人才的需求，突出以能力为本位的高等职业教育的特色。

应当说明的是，凡是高等职业教育、高等专科教育和成人高等教育院校的计算机及其相关专业的师生均可使用本套教材。各学校可以根据实际需要，在教学中适当增删一些内容，从而更有针对性地帮助学生掌握计算机专业知识，并形成相关应用能力。

本套教材的出版，将促进高等职业教育的教材建设，对我国高等职业教育的发展产生积极的影响。同时，我们也希望在今后的使用中不断改进、完善此套教材，更好地为高等职业教育服务。

编　者

目 录 CONTENTS

第 1 章　概述

随着计算机网络的不断发展，人与人之间的交流日益便捷，各类信息资源得以充分的共享，但是计算机网络的安全问题也日益突出，网络安全难以得到充分的保障，这已经成为影响计算机网络健康发展重要因素。计算机网络安全是一个非常复杂的问题，它不仅涉及技术问题，还涉及人的心理、社会环境、法律等多方面内容。

在计算机网络中，多个用户都处于一个大的系统之中，系统资源可以被网络用户所共享。随着计算机网络的普及，有更多的军政重要数据、企业的商业机密和个人的隐私等存储在接入网络的计算机中，如果计算机网络安全得不到保障，因系统漏洞以及攻击者的非法侵入，有关方面就可能蒙受巨大损失。

国际标准化组织(ISO)将计算机安全定义为：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然或恶意的原因而遭到破坏、更改或泄露。实际上，还可以再加上一点：保障系统连续正常运行。

1.1　计算机网络的不安全因素

1．环境

造成计算机网络不安全的环境因素包括自然环境和社会环境。对于自然环境，如雷电、自然灾害、强电磁场等，都可能对计算机网络的有线链路、无线链路、网络设备、终端、链路中传输的数据等造成损害。对于社会环境、社会风气、个人的心理健康、法律法规等都对计算机网络安全有重大影响。实际上，目前人们更为关注的是社会环境对计算机网络安全造成的影响，毕竟众多的网络攻击是由人来发动的。

2．资源共享

资源共享是计算机网络的目标，没有资源共享的计算机网络将没有任何价值。但资源共享也为非法用户窃取信息、破坏信息及信息服务带来了可乘之机。非法用户可能通过计算机网络窃取他人的机密和隐私，非法修改他人的文件，或使能够向大众提供有价值信息服务的计算机瘫痪或者提供虚假的信息服务等，给他人或组织带来重大损失。

3．系统的复杂性

操作系统是一个非常复杂的软件，在加上众多的各种各样的其他系统软件和应用软件，单纯对单个计算机的软件系统进行安全确认就相当困难，更不用说包含硬件系统和软件系统的完整的计算机系统和连接大量计算机的网络系统。因此，要确认网络系统是否安全是异常困难的。实际上，绝对安全的系统是不存在的。

4．数据通信

在计算机网络中的信息要通过物理线路、无线电波、网络设备等进行传输和交换，这样，信息在传输和交换的过程中就有可能被窃听或篡改，对信息安全带来威胁。

5. 计算机病毒

计算机病毒一旦侵入接入计算机网络的计算机，不仅危害被侵入计算机的安全，还可能会通过计算机网络不断传播，危害网络中其他结点的安全，甚至会导致网络的瘫痪。

6. 特洛伊木马

特洛伊木马对计算机网络安全的危害也是巨大的。特洛伊木马是指系统在执行任务过程中，所执行的任务不是指定执行的任务，所执行的任务是经过替换或篡改的。这样的任务可能根本不会完成所指定的功能，或者在完成指定功能的基础上附加了其他的功能，为非法用户窃取他人机密或远程控制其它计算机埋下安全隐患。

7. 网络管理

网络系统的安全运行离不开网络管理员对网络系统的管理维护。应该说，计算机网络安全与网络管理员的工作态度、技术水平等是紧密相关的。

8. 设计与编码

不良的设计与编码是造成计算机网络不安全的重要因素。目前已发现的安全漏洞很多是由于网络中的服务软件和客户软件设计与编码不当造成的。

1.2 网络安全的基本概念

1. 物理安全

物理安全是指系统设备及相关设施受到物理保护，免于破坏、丢失等。

2. 信息完整性

信息完整性是指信息不会被非法修改或在传输过程中保持一致，也就是说，防止信息被未授权用户修改，保证信息从真实的信源无失真地传输到真实的信宿。

3. 信息保密性

信息保密性是指高级别信息仅在授权情况下才能流向低级别的客体和主体，保证信息不泄露给未授权用户。

4. 信息可用性

信息可用性是指合法用户的正常请求能够及时、正确、安全地得到服务或响应。

5. 信息的不可否认性

信息的不可否认性是指信息的行为人不能否认自己的行为，包括发送信息的人不能否认他不是信息的发送者、接收信息的人不能否认他已经收到了信息。

6. 信息的可控性

信息的可控性是指信息的所有者或授权用户对信息的传播及内容具有控制能力。

7. 脆弱性

脆弱性是指系统安全保护的弱点，或根本未涉及某种威胁的安全保护。

8. 风险分析

风险分析是指用于估计系统威胁发生的可能性以及估计由于系统脆弱性而引起潜在损失的步骤。风险分析的目的是帮助选择安全保护措施并将风险降低到可接受的程度。

9. 风险管理

风险管理包括物质的、技术的、管理控制及过程的一些活动，通过这些活动来试图得到合算的安全性解决办法，对系统实现最有效的安全保护。风险管理包含了风险分析，风险分析是风险管理的基础。

10. 敏感信息

敏感信息是指那些一旦丢失、滥用、被窃取或篡改，就有可能损害个人利益、公司利益甚至国家利益的信息。

11. 后门/陷阱

后门是进入系统的一种方法，通常它是由设计者故意建立的。陷阱是后门的一种形式。后门/陷阱是一般用户所不知道的。

12. 拒绝服务

拒绝服务是指提供服务的系统无法继续向合法用户连续正常地提供信息服务的情况。目前 Internet 上的网络攻击中，拒绝服务攻击占了很大比例。攻击者利用拒绝服务攻击使受害系统崩溃，或大量消耗系统资源使系统无法在规定时间内向合法用户提供信息。

13. 认证

认证是指通信参与方的身份及数据来源真实可靠。确保通信参与方身份真实性的认证称为实体认证，确保某条消息来自某个特定的数据源的认证称为数据源认证。

14. 访问控制

访问控制是指只有经过授权的用户才能访问受保护的资源。访问控制的目的在于限制主体对各对象的访问，并且限制主体在访问对象时所做的具体操作。

1.3　安全服务与安全威胁

ISO 定义了以下几种基本的安全服务：认证、访问控制、保密性、完整性、不可否认性。

如果没有安全服务，系统就会暴露在各种不同的安全威胁或攻击的目标范围内。对系统的安全威胁主要有以下几种：

1. 中断

通信被非法中断，从而使信息变得无用或无法使用。中断是对信息可用性的威胁。

2. 篡改

未经授权的人不但访问了信息资源，而且篡改了信息，例如篡改数据文件、篡改程序甚至拦截并篡改网络上尚未到达目的的报文。篡改是对信息完整性的威胁。

3. 窃取

未经授权的人访问了原本无权访问的信息资源，如对网络通信数据的监听。窃取是对信息保密性的威胁。

4. 假冒

一个实体通过欺骗等手段伪装成另外一个实体，从而了通过对被假冒实体的认证。另外的假冒情况是信源或信宿的假冒，通过假冒信源，信息的接收方会误认为它所收到的信息是来自于它所信任的信源；通过假冒信宿，原本是发送给某个信宿的信息会错误地被发送给假冒者。

5. 重放

攻击者将另一方参与者以前发送过的消息重新放到网络上传输到特定的接收者，从而获得另一方参与者的特权。重放实际上可归入假冒这一种情况。

6. 渗透

攻击者滥用某合法参与方的特权，以非法获得信息资源的访问权，或者运行恶意的程序等。

1.4 安全机制

1. 数据加密机制

进行数据加密是保密通信的基本手段，也是其它安全方法的基础。数据加密可以有效防止未经授权的用户访问敏感信息。一般的保密通信模型可以这样描述：在发送端，明文用加密算法和加密密钥，经过加密变换，得到密文，然后将密文发送给接收端；在接收端收到密文以后，用相应的解密算法和解密密钥经过解密变换恢复原始的明文。这样，偷听者窃取到的是加密后的密文，由于他不知道解密密钥，则他就无法获得对他有价值的明文。

在上述模型中，如果加密密钥和解密密钥是相同的，则我们将这种加密体制称为对称钥体制，否则称为非对称钥体制。典型的对称钥体制有 DES、AES 等，典型的非对称钥体制有 RSA、ElGamal 等。

2. 认证机制

防止主动攻击的重要措施是使用认证机制。通过认证，可以识别通信双方的身份，防止假冒，也可以验证消息在传输过程中是否被篡改。要达到认证的目的，可以在实体认证中使用名字/口令验证方法，当然更好的选择是使用数字签名和消息摘要方法。

3. 不可否认机制

数字签名是一种非常有效的防止否认的方法。同手写签名的作用类似，数字签名系统向通信双方提供服务，使得发送方 A 向接收方 B 发送签名的消息之后，接收方 B 可以验证消息的确来源与预定的发送方 A，同时 A 也不能否认他确实对该消息进行过签名，但包括接收方 B 在内的其它任何实体都不能假冒 A 伪造出 A 签过名的另一条消息或篡改 A 已经签名的消息。这是对数字签名最基本的要求。当然，很多数字签名体制或协议还满足其它一些更为严格的要求，例如，接收方在收到经过数字签名的消息后不能否认他确实接收了该消息。

虽然数字签名和手写签名在作用上有很多相似之处，但在安全强度上，数字签名比传统的手写签名强健得多，而且，手写签名明显不适合于网络。

典型的数字签名体制有 RSA、ElGamal、DSA 等。

4. 完整性机制

一般使用数字签名和消息摘要算法相结合来保障数据的完整性，其中消息摘要可以用于加速数字签名算法。

消息摘要方案是针对消息本身，计算一个固定长度的认证码，附加在消息后面进行发送；接收方收到之后，用同样的方法计算一个认证码，如果计算得到的认证码与消息后面附

加的认证码不一致，则说明消息在传输过程中被篡改了。

以不定长的消息作为输入、以定长的认证码作为输出的计算函数被称为哈希函数，当然，这个函数最起码应该满足单向性，即已知函数的输出难以计算函数的输入是什么。典型的单向哈希函数另外应该满足的要求有：(1)根据某个输入消息所计算得到的认证码 C，很难找到另外一条不同的消息使计算得到的认证码也等于 C；(2)很难找到两个不同的随机消息使它们的哈希函数值(认证码)相同。

目前比较典型的消息摘要算法有 MD4、MD5、SHA 等。

我们可以分析出，仅仅依靠消息摘要算法还不足以保障消息的完整性。假如攻击者截获了附带有认证码的消息，他可以篡改消息，然后用相同的消息摘要算法计算新的认证码，这样被篡改的消息也可以通过接收方的验证。解决这个问题的一般方案是将消息摘要算法与数字签名算法相结合。对整个消息进行数字签名的效率太低，而对相对短小且定长的消息摘要进行数字签名则要高效得多。

1.5　我国网络安全的现状

1. 与网络安全有关的法律法规还很不完善

目前我国在网络安全方面的法律方面存在很大缺陷，对危害网络安全的行为在取证、量刑、定罪以及有关程序方面都没有系统、周密的条款，这必将导致对利用网络进行涉及信息安全的犯罪行为的打击力度受到很大影响。以电子签名(数字签名)法为例，电子签名法涉及网络社会的信用安全问题，应该是与网络安全有关的法律中非常重要的一个方面，但我国目前还没有开展电子签名的立法，而我国周边的一些国家已经颁布了电子签名法。当然，网络安全的立法及其不断完善的问题也是全世界各个国家共同存在的一个问题。

2. 基础信息产业严重依靠国外

我国目前信息产品(包括软件和硬件)的研发、生产能力比较弱，关键软硬件受制于人，国外厂商几乎垄断了我国软硬件的基础和核心市场，特别是操作系统和处理机。如果这种现状不得到扭转，整个国家的安全都可能在未来受到重大影响。

3. 网络的安全防护能力比较弱

目前我国计算机网络的发展速度是前所未有的，但很多应用系统都处于一种不设防的状态。政府、企事业单位对网络安全的关注程度还很不够，对网络安全的人力、物力、财力的投入微乎其微。

4. 信息安全管理机构的权威性不够

目前，我国有比较多的民间信息安全管理机构，但这些机构往往各自为战、相互隔离、缺乏协调，互相之间缺乏信任，各类网络安全产品之间也缺乏互操作性。民间信息安全管理机构与国家信息化领导机构之间也没有充分的沟通协调。各安全管理机构的权威性不够，导致网络用户对网络安全管理机构的信任程度不高。

5. 专门从事网络安全工作的专业技术人才队伍现状与网络的发展形势极不相称

我国的高等教育在近几年才密切关注网络安全技术人才的培养，但在培养数量、层次上还很不够。目前，我国有非常少的高校开设网络安全方面的专业，未来更多的从事网络安全

工作的人才可能没有经过系统的网络安全方面的理论学习和实践训练。这与目前我国网络化的发展形势极不相称。

6. 用户的网络安全意识淡薄

广大网络用户的安全意识淡薄，很多的用户认为网络安全是网络中各类服务器管理人员的事，网络安全问题离自己的生活相距甚远，而实际上网络安全与生活在网络社会中的每一个人都息息相关，网络安全都关系到每一个人的切身利益。网络安全与每一个人的关系在未来的网络社会将会更加密切，甚至每时每刻都伴随在身边。

练习题

1. 以实例说明几种安全威胁的危害。
2. 以实例说明几种安全机制的重要价值。

第 2 章　TCP/IP 协议

TCP/IP 协议(Transfer Control Protocol/Internet Protocol)叫做传输控制/网际协议,这个协议是 Internet 国际互联网络的基础。

通过 TCP/IP 协议可以把不同的网络连接在一起以便共享网络资源。网络不仅解决了共享资源的问题,更重要的是通过网络互联,可以充分地保护宝贵的信息资源。

TCP/IP 协议是网络中使用的基本的通信协议。虽然从名字上看 TCP/IP 包括两个协议,传输控制协议(TCP)和网际协议(IP),但 TCP/IP 实际上是一组协议,它包括上百个各种功能的协议,如:远程登录(Telnet)、文件传输(FTP)和电子邮件(SMTP、POP3)协议等,而 TCP 协议和 IP 协议是保证数据完整传输的两个基本的重要协议。通常说 TCP/IP 是 Internet 协议族,而不单单是 TCP 和 IP。

本章简要介绍 TCP/IP 协议发展、TCP/IP 协议分层结构及工作过程,重点讲解 TCP/IP 各层主要协议的基本概念和基本原理,为后面的学习打下基础。

2.1　TCP/IP 协议的发展

TCP/IP 协议的产生与发展与 Internet 的发展密不可分。第二次世界大战期间,美国国防部为了保证美国本土防卫力量和海外防御武装在受到前苏联第一次核打击后仍具有一定的生存和反击能力,认为有必要设计出一种分散的指挥系统:它由一个个分散的指挥点组成,当部分指挥点被摧毁后,其它点仍能正常工作,并且这些点之间,能够绕过那些已被摧毁的指挥点而继续保持联系。为了对这一构思进行验证,1969 年,美国国防部国防高级研究计划署(DoD/DARPA)资助建立了一个名为 ARPANET(即“阿帕网”)的网络,这个网络把位于洛杉矶的加利福尼亚大学、位于圣芭芭拉的加利福尼亚大学、斯坦福大学,以及位于盐湖城的犹它州州立大学的计算机主机联接起来,位于各个结点的大型计算机采用分组交换技术,通过专门的通信交换机(IMP)和专门的通信线路相互连接。这个 ARPANET 就是 Internet 最早的雏形。

1972 年,全世界电脑业和通讯业的专家学者在美国华盛顿举行了第一届国际计算机通信会议,就在不同的计算机网络之间进行通信达成协议。会议决定成立 Internet 工作组,负责建立一种能保证计算机之间进行通信的标准规范(即“通信协议”)。1973 年,美国国防部也开始研究如何实现各种不同网络之间的互联问题。

1977 至 1979 年,IP(Internet 协议)和 TCP(传输控制协议)问世,合称 TCP/IP 协议。这两个协议定义了一种在电脑网络间传送报文(文件或命令)的方法。随后,美国国防部决定向全世界无条件地免费提供 TCP/IP,即向全世界公布解决电脑网络之间通信的核心技术,TCP/IP 协议核心技术的公开最终导致了 Internet 的大发展。

到 1980 年,世界上既有使用 TCP/IP 协议的美国军方的 ARPANET,也有很多使用

其它通信协议的各种网络。为了将这些网络连接起来，美国人温顿·瑟夫(Vinton Cerf)提出一个想法：在每个网络内部使用自己的通讯协议，在和其它网络通信时使用 TCP/IP 协议。这个设想确立了 TCP/IP 协议在网络互联方面不可动摇的地位。

今天，TCP/IP 协议已经变成互联网的同义词，许多网络系统、应用系统甚至 PC 机系统都有相应的 TCP/IP 工业产品，如 NOVELL 公司的 Netware TCP/IP、FTP 公司的 TCP/IP、PC-NFS 等等。Microsoft 公司的 Windows NT、Windows 95、IBM 的 OS/2 等等都内置了 TCP/IP。

2.2 TCP/IP 协议的分层结构与工作过程

TCP/IP 协议的基本传输单位是数据包，TCP 协议负责把数据分成若干个数据包，并给每个数据包加上包头(就像给一封信加上信封)，包头上有相应的编号，以保证在数据接收端能将数据还原为原来的格式，IP 协议在每个包头上再加上接收端主机地址，这样数据找到自己要去的地方(就像信封上要写明地址一样)，如果传输过程中出现数据丢失、数据失真等情况，TCP 协议会自动要求数据重新传输，并重新组包。总之，IP 协议保证数据的传输，TCP 协议保证数据传输的质量。

TCP/IP 协议数据的传输基于 TCP/IP 协议的四层结构：应用层、TCP 层(传输层)、IP 层(互联网层)、网络接口层(图 2-1)，数据在传输时每通过一层就要在数据上加个包头，其中的数据供接收端同一层协议使用。而在接收端，每经过一层要把用过的包头去掉，这样来保证传输数据的格式完全一致。

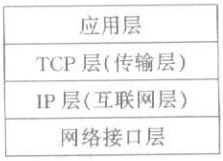

图 2-1 TCP/IP 参考模型

2.2.1 网络接口层

从图 2-1 中可以看出，网络接口层是 TCP/IP 模型的最低层，它主要负责接收从互联网层交来的 IP 数据报并将 IP 数据报通过底层物理网络发送出去，或者从底层物理网络上接收物理帧，抽出 IP 数据报，交给互联网层。

2.2.2 IP 层(互联网层)

IP 层的主要功能是负责传送相邻结点之间的数据。它的主要功能包括三个方面。(1)处理来自传输层的数据发送请求：将数据装 AIP 数据报，填充报头，选择去往目的结点的路径，然后将数据报发往适当的网络接口。(2)处理输入数据报：首先检查数据是否合法，然后进行路由选择，假如该数据报已到达目的结点(本机)，则去掉报头，将 IP 报文的数据部分交给相应的传输层协议；假如该数据报尚未到达目的结点，则转发该数据报。(3)处理 ICMP 报文：即处理网络的路由选择、流量控制和拥塞控制等问题。

IP 层由多个协议组成，主要是 IP 协议，还有三个辅助协议，即控制报文协议 ICMP，用于在网际层进行差错控制等；地址转换协议 ARP(Address Resolution Protocol)和反向地址解析协议 RARP(Reverse Address Resolution Protocol)用于互联网地址与结点物理地址

的转换。

2.2.3 TCP 层(传输层)

传输层的作用是在源结点和目的结点的两个进程实体之间提供可靠的端到端的数据通信,是端到端的协议。为保证数据传输的可靠性,传输层协议规定接收端必须发回确认,并且当数据有错或丢失时,发送方必须重传。

传输层还要解决不同应用程序的标识问题,因为在一般的通用计算机中,常常是多个应用程序同时访问互联网。为区别各个应用程序,传输层在每一个分组中增加识别信源和信宿应用程序的标记。另外,传输层的每一个分组均附带校验和,以便接收结点检查接收到的分组的正确性。

这一层有两个协议,一个是传输控制协议 TCP,是面向连接的报文分组传输协议,可以提供端到端可靠的传输。另一个用户数据报协议 UDP,是无连接的数据报传输协议。

2.2.4 应用层

TCP 层的上一层是应用层,应用层包括所有的高层协议。应用层有远程登录协议(Telnet),远程登录协议允许用户登录到远程系统并访问远程系统的资源;文件传输协议(File Transfer Protocol, FTP)提供在两台机器之间进行有效的文件传送的手段;简单邮件传输协议(Simple Mail Transfer Protocol, SMTP)最初只是文件传输的一种类型,后来慢慢发展成为一种特定的应用协议。最近几年出现了一些新的应用层协议:如用于将网络中的主机的名字地址映射成网络地址的域名服务(Domain Name Service, DNS)和用于从万维网上读取页面信息的超文本传输协议(Hyper Text Transfer Protocol, HTTP)。

2.3 IP 协议与 IP 路由

2.3.1 IP 协议

1. IP 地址

1)物理地址与逻辑地址

互联网通过路由器把各个通信子网互联,通信子网又称为物理网络,网络内的每个结点都存在一个物理地址,这是各结点的唯一标识,还有一些地址是有层次的地址,如 ARPANET 中,地址形如(P.N),其中 P 代表分组交换结点号,N 代表与该交换结点相连的主机号,这样的层次地址可以提高路由效率。

在互联网中,不同物理地址连成虚拟网后必须有一个统一的地址,以便在整个网上有一个唯一的结点标识,这就是我们所说的逻辑地址 IP 地址。IP 地址对各个物理网络地址的统一是通过上层软件进行的,这种软件没有改变任何物理地址,而是屏蔽了它们,建立了一种 IP 地址与它们之间的映射关系。这样,在互联网络层使用 IP 地址,到了底层,通过映射得到的物理地址也是层次型的。

2)IP 地址种类

IP 地址是一个 32 位的地址,理论上,可以表示 232 个地址。从实际出发,IP 协议把 IP