第3章

电子商务通信过程的安全风险

本章教学目标

- 了解风险及风险分析的相关理论。
- 熟悉 Internet 上存在的风险及其对风险的分析。
- 了解 Internet 上的通信协议。
- 熟悉作为 Internet 上有效传输机制的组成部分，各种协议在通信过程中存在的风险。
- 熟悉 Internet 提供的各种服务，并掌握这些服务在应用过程中存在的风险。

本章关键术语

- Internet 安全与风险
- Internet 通信协议中的安全风险
- Internet 应用风险

3.1 Internet 安全与风险

越来越多的商家、消费者通过 Internet 进行商务活动，电子商务有着良好的发展前景。但随着电子商务活动的深入开展，其安全问题也变得越来越突出。如何充分进行风险分析，建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和消费者都十分关心的话题。

3.1.1 风险分析理论

1. 风险概述

1）风险的概念

人类认识到风险的存在已经有了很长时间，但直到近代才开始了科学、系统的研究。一些学者提出了风险的概念，比如美国学者 Haynes 认为“风险意味着损害的可能性”；DIN VDE 标准（德国工业标准）将风险定义为“如果事故发生，预计损失的程度，预测事故发生的概率”；我国学者杨梅英在其《风险管理与保险原理》中提出“风险是人们对未来行为的决策及客观条件的不确定性而导致的实际结果与预期结果之间偏离的程度”。

总地来说，风险就是指危险发生的意外性和不确定性，包括损失发生与否及损失程度大小的不确定性。近几年来，随着计算机系统的不断普及，上述风险已经极大增加。人们大量利用信息资源，由于访问违背授权的内部资料与通信系统而引发的破坏显著上升。Internet安全事件的数量与破坏发生的概率今后将增加得更快。

2）风险的特征

风险是由于人们没有能力预见未来所产生的，它还能指出那些很重要足以引起注意的不确定性的程度。这个模糊的定义可以通过风险的几个重要的特征，使发生的风险变得更形象化。

首先，风险既是客观的，又是主观的。例如抛硬币是客观的风险，因为它的几率是众所周知的。即使结果是不确定的，客观的风险还是能在理论、试验或尝试的基础上精确描述的，每个人都同意对客观风险的描述。而对于一个网络，下星期一要被攻击几率的描述不是非常清楚的判定，这就表现出主观风险。

其次，决定某事是有风险的需要个人的判断，甚至对于客观的风险也如此。例如，想象一下扔硬币，正面朝上就赢1元，背面朝上就输1元。在1元和－1元的范围内，对于大多数人并不是很重要的。但是如果赌金额是数百万或千万元，大多数人会认为这种情况是相当有风险的。通常，这种发生“风险”的大小，各个行为是不一样的。重要的是，每个行为发生的风险结果都有一定范围。

再次，有风险的行为和因此产生的风险，通常是能选择或避免的。个人在他们能自愿承受风险的量是不同的。例如，两个有相等资本净值的人，对赌注为100万元的抛硬币的赌博的反应是完全不同的，或许一个人可以接受它，而另一个人则会拒绝。他们个人对风险的承受程度是不同的。

2. 风险分析概述

1）风险分析的基本概念

风险分析就是要对风险的辨识、估计和评价做出全面的、综合的分析，其主要组成包括两方面：其一是风险的辨识，也就是哪里有风险，后果如何，参数变化；其二是风险评估，也就是概率大小及分布，后果大小。

2）风险分析的目的

风险分析的最终目的是彻底消除风险，保障风险主体安全。具体包括以下几个方面：

（1）透彻了解风险主体、查明风险客体以及识别和评估风险因素。

（2）根据风险因素的性质，选择、优化风险管理的方法，制定可行的风险管理方案，以备决策。

（3）总结从风险分析实践中得出的经验，丰富风险分析理论。

3）风险分析的原则

风险分析的原则是分析人员在进行风险分析时辨识和评估各种风险因素所持的态度，以及在分析中采用各种技术的原则，它是独立于风险分析的对象（风险主体、风险客体和风险因素等）之外的认知系统遵循的原则。

4）风险分析的步骤

风险分析划分为确定分析的范围、找出风险、评估风险、风险控制等4个阶段。

(1) **确定范围**——划分风险分析所覆盖的区域。由于风险分析复杂,不能在整个数据处理系统上进行,而只能在单个区域内。因此,只能在单个分析区域间确定界面。

(2) **找出风险**——详细地描绘所有现行的风险,并调查风险的影响结果,分析风险采用风险情况分析和模拟研究两种方法。若用风险情况分析,就需将引起安全事件的假设事件集中在一起(处在同一界面上)。通过对主要情况的研究,较快地得到原始结果;若用模拟研究,通过如实反映所分析区域的情况,模拟潜在风险所带来的影响,最后查出风险所在。上述两种分析方法都较昂贵且费时,并且还涉及特殊软件。

(3) **风险评估**——对风险发生的概率及潜在损失的分析和确定基础上进行的基本的风险评估,就是安全事件带来的损失值乘以一年内事件发生的概率。例如,将基本风险评估应用于假设全部数据丢失引起网络崩溃的事件中。

- 数据丢失带来的直接与间接损失值为:25 000 000 元。
- 概率:1/10(10 年一次)。
- 基本的风险评估为:25 000 000×0.1=2 500 000 元/年。

基本的风险评估系统常采用统计表格和范畴分类来帮助确定风险事件。结果表明精确度并没有太偏离现实生活。该项评估主要用在美国,可以利用许多适合的风险分析软件包(比如 BDSS、Bayesian 判决辅助系统,OP&S)。

(4) **风险控制**——根据风险评估的结果,采取一定的措施或方案将风险限定在一个合理的、可接受的水平上,即根据影响风险的因素,经过识别、选择、优化和采用正确的安全和意外事件的控制措施或寻求最佳的风险解决方案,使风险降低到可以接受的等级,最终达到风险与利益的平衡。

常规的风险分析借助于列表和矩阵,首先将信息系统分解为可确定风险的客体。与基本分析方法相反,对风险不做精确计算而是按范畴分类。比如划分为可接受的风险、不可接受的风险、非常小、不可能及非常可能发生的风险等。

3.1.2　Internet 上的安全风险分析

近几年来,随着利用 Internet 从事商业活动的力度加大,犯罪活动与滥用现象日益增多,当企业考虑是否要与 Internet 联网以及如何联网时,需考虑的主要问题就是涉及其中的风险因素。如果没有适当的安全保护措施,一旦与 Internet 相连,将会带来意想不到的风险。

1. DP(数据处理)基础设施中的基本风险

探讨 Internet 安全风险时,常被忽视的事实是,企业的计算机系统面临的严重风险并不仅仅在 Internet 上。事实上,大多数网络安全专家都认为,大部分网络攻击都是由存在漏洞的企业的内部员工所发起的。例如,数据没有备份、由移动存储器设备带进了病毒、出于恶作剧、恶意或者好奇心、误操作等。一旦企业出现上述任何一种情况,其计算机系统不论是否与外部通信网络连接,都会极大地增加被蓄意袭击的机会。

2. Internet 上存在的安全风险

Internet 是一个全球互联网,它包容着众多的异种网络和协议、不同的操作系统、不同

类型和厂商的硬件平台，是一个非常复杂的环境，因而它的安全问题也非常复杂，主要有以下 9 个方面。

- 身份截取：指用户的身份在通信时被他人非法截取。
- 中继攻击：指非法用户截取通信网络中的数据。
- 数据操作：指对通信中的数据进行非法的替换、修改、插入和排序等操作。
- 服务拒绝：指通信被中止或实时操作被延迟。
- 交通分析：指分析通信线路中的信息流向、流量和流速等，从中得到有用的信息。
- 路由攻击：指改变信息的流动路线。
- 非授权存取：指非法使用资源。
- 伪装：指假冒合法用户以获取有用资源的行为。
- 否认：指通信双方有一方事后否认曾参与某次活动的行为。

日益普及的 Internet 给人们提供了方便、快捷的信息获取和沟通渠道，同时，也正是全球互联的 Internet 引发了各种重大安全问题的主要原因。因此，要安全使用 Internet 就需要具备防止信息泄漏以及防止被篡改等网络安全问题的能力。为了预防这些网络上的不正当行为，特别需要了解 Internet 上存在的基本安全风险。

3. Internet 上风险等级划分

从上述内容可以看出，Internet 存在风险表现在多个层面，风险的损害程度也有差异。因此，这里采用美国著名网络安全厂商(Internet Security System，ISS)提出的 Internet 风险等级划分标准——AlertCon 对 Internet 上存在风险进行风险程度的划分，以利于防范与管理。

AlertCon 为 ISS 所提供用来判定 Internet 目前存在的风险而产生的威胁状态的一个标准。这个判定标准来自于 ISS Global Threat Operations Center，根据过去 24 小时 Internet 所发生的任何危安事件，进而预测未来 48 小时可能发生的危安事件。经由 ISS Global Threat Operations Center 所发布的判定标准，称为 AlertCon 或 Alert Condition。具体等级及标识见表 3.1。

表 3.1　Internet 风险等级划分

名　称	图　标	等　级
AlertCon 1		一般警戒(Regular Vigilance)：为 AlertCon 的一个基准点，一般状况均定义为 AlertCon 1
AlertCon 2		增进警戒(Increased Vigilance)：发现新的弱点，且确定会影响到主机或网络的隐秘性、完整性、可用性；必须对主机或网络设备进行弱点评估，建议进行修补，ISS 将此状况定义为 AlertCon 2

续表

名　称	图　标	等　级
AlertCon 3		焦点攻击(Focused Attacked)：确定经由特定的弱点或系统内部所存在的弱点，进行攻击时必须立即进行防御措施，ISS 将此状况定义为 AlertCon 3
AlertCon 4		灾难性威胁(Catastrophic Threat)：将或可能发生的严重危害事件，可能发生在某一个区域或蔓延至全球，必须立即进行防御措施；这状况可能是即将发生或已经发生，ISS 将此状况定义为 AlertCon 4

4. Internet 上风险发生的概率分析

经由 Internet 越权侵袭计算机系统的事件逐年增加，基本上与计算机数量的快速增长同步。1988 年，ARPA(高级研究项目署)成立了 Internet 安全组织 CERT(计算机紧急情况处理小组)。根据 CERT 的报道，1989 年仅有 132 起计算机安全事件，到 1995 年安全事件的数量已多达 2412 起，共有 12 000 多个网络受到影响。2004 年，公安部公共信息网络安全监察局与中国计算机学会计算机安全专业委员会共同举办了全国首次信息网络安全状况调查活动。调查时间为 2003 年 5 月至 2004 年 5 月，在 7072 家被调查单位中有 4057 家单位发生过信息网络安全事件，占被调查总数的 58%。其中，发生过 1 次的占总数的 22%，2 次的占 13%，3 次及以上的占 23%，此外，有 7%的调查对象不清楚是否发生过网络安全事件。从发生安全事件的类型分析，遭受计算机病毒、蠕虫和木马程序破坏的情况最为突出，占安全事件总数的 79%，其次是垃圾邮件占 36%，拒绝服务、端口扫描和篡改网页等网络攻击情况也比较突出，共占到总数的 43%。

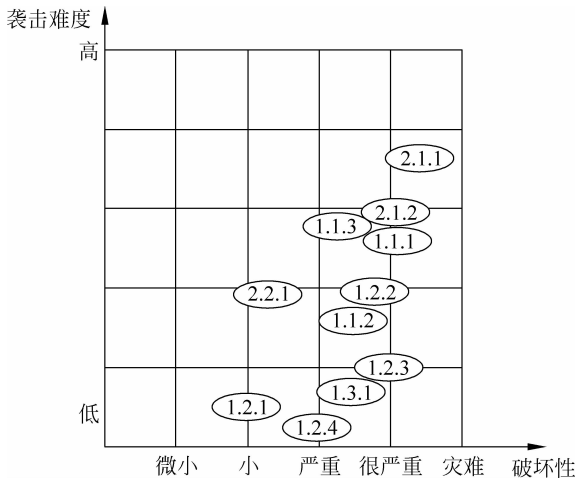
调查结果表明，造成网络安全事件发生的主要原因是安全管理制度不落实和安全防范意识薄弱。其中，由于未修补或防范软件漏洞导致发生安全事件的占安全事件总数的 66%，登录密码过于简单或未修改密码导致发生安全事件的占 19%。

下面是 Internet 上风险袭击难度与破坏程度的概率分析，如图 3.1 所示。

5. 风险的详细分析

利用风险矩阵可以进行详细的风险分析，这使得具体评估安全风险给企业带来损害的程度成为可能。潜在的安全事故可看作是损害程度和所发生事故的概率的函数。每种闯入事件的概率都与所用的计算机和网络系统、现有的基础设施(外部数据线、联网情况、拨号网等)以及现有的安全保护措施(防火墙、拨号应答等)有关。影响基本安全风险的其他因素有：

- 企业的运作情况是潜在指标(产品、竞争者等)。
- 企业所处的位置。
- 企业规模和员工数量。



1. 内部袭击
   - 1.1 未授权访问企业数据(插入、删除、破坏数据等)
     - 1.1.1 通过认证系统破坏
     - 1.1.2 NFS 袭击
     - 1.1.3 X-windows 袭击
     - 1.1.4 ……
   - 1.2 网络基础结构的破坏
     - 1.2.1 网络过载的发生
     - 1.2.2 对网络部件的袭击
     - 1.2.3 对物理网络基础结构的破坏
     - 1.2.4 病毒感染
   - 1.3 机密信息的丢失
     - 1.3.1 网络嗅探器
2. 外部袭击
   - 2.1 未授权访问企业数据
     - 2.1.1 TCP 序号袭击
     - 2.1.2 路由袭击
   - 2.2 网络基础结构破坏
     - 2.2.1 网络过载的发生

图 3.1 数据网络的风险概率分析

风险分析的第一步就是将所有不同的潜在威胁(通过 DP 基础设施)进行列表,然后测算每种威胁发生的概率。

利用上面确定的风险因素,可根据风险矩阵中各种潜在威胁及风险发生的概率,推导出安全事故的公式。面对潜在的袭击者,措施越全面,被侵袭的可能性就越小。对所有潜在的威胁,基本安全风险值越高,就意味着通过操纵台的风险权限越大。借助于图 3.2,就可以对结果进行分析,并利用这些结果,决定应采取的措施。

潜在袭击的损失值					
很高	2	2	1	1	1
高	2	2	2	1	1
中等	3	2	2	2	1
小	3	3	3	2	2
很小	3	3	3	2	2
	很小	小	中等	高	很高
					袭击的可能性

注：1、2、3 由高到低分别为操纵台的优先权或风险权

图 3.2　潜在袭击的概率与损失价值关系

3.1.3　Internet 中最容易受到侵袭的薄弱环节

1. Internet 中潜在的安全隐患——固有的风险

Internet 由大量的硬件和软件构成，体系结构极其复杂，整个网络系统基本上充满了各种各样的编程和误操作。例如要编译 1 万条语句的程序，并保证在所有情况下都工作正常，没有一定的规则是无法实现的，这也意味着任何商用软件都会碰上潜在的安全故障。有些故障是人为利用编程错误制造的，一旦有关部件通过网络接入到大量用户系统上，那么薄弱环节的风险将大大提高。

2. Internet 的隐患——不完善的软件设计

Internet 中存在如此多的安全问题的原因之一在于 TCP/IP 协议和 UDP 协议的基本体系结构。这几种协议在开始制定时都没有重点考虑路径的安全性，例如，当用 TCP/IP 协议通过 Internet 传送数据时，无法知道传输了哪些节点，如果攻击者成功地在一个或多个节点上装上了嗅探器，那么以原文传送的口令就会泄漏，信息就会被截获。

被成功侵袭的另一个原因是计算机系统配置的安全性很薄弱。Internet 访问系统都很少或根本没有配置安全保护。从纯技术角度上来看，存在着 5 个领域的薄弱性，即缺乏安全防护设备(没有安全防火墙)、不足的安全配置与管理系统、通信协议上的基本安全问题、基于 WWW 和 FTP 上的应用软件问题及不完善的服务程序。

3. 侵袭的命中率清单

根据 CERT(计算机紧急事故处理小组)协调中心在匹兹堡 Carnegie Mellon 大学所列出的侵袭法的命中率清单中，嗅探器袭击是最能成功侵袭网络的方法，列在第一位。袭击者采用“看不见”的微型程序，偷偷连到 Internet 主机上，监控数据流并捕获口令和系统 ID(标识符)。

排在第二位的是 IP 欺骗，即袭击者输入自己的数据地址。这一地址属于目标网络的地址范围，因此看起来像是由哪个网络上的用户产生的，所以称为欺骗。该侵袭方式主要能突破信息包过滤器和防火墙系统，因为这种信息包过滤器或防火墙的认证机理是基于 Internet 地址的。

第三位是发送邮件，它利用邮件服务器应用软件中的不完善来袭击网络。

第四位和第五位分别是 NFS(网络文件系统)和 NIS(网络信息服务器)的侵袭。

3.2 Internet 通信协议中的安全风险

作为 Internet 上有效传输机制的组成部分，通信协议 IP(网际协议)、TCP(传输控制协议)和 UDP(用户数据报文协议)，都明显成为了潜在攻击者的袭击目标。利用协议或系统中的安全隐患来侵袭的手段多种多样，这些安全隐患有的是协议本身固有的，有的是由于系统的配置不合理造成的。

3.2.1 Internet 通信协议简介

1. 网际协议(Internet Protocol，IP)

1) IP 协议的体系结构

所谓“协议”是关于通信过程的规则或条约，它规定了如何传输信号，如何在宿主计算机上将数据包重新组成计算机信息等。IP 协议的结构模型与 ISO 的 OSI 模型略有不同，IP 对 OSI 模型进行了更进一步的简化，它采用 4 层结构模型，如图 3.3 所示。图 3.3 中也画出了对应的 OSI 层次，这里需说明的是，IP 协议分层并不严格对应 OSI 模型的相关协议层次。最上面第四层为应用层，它支持用户，提供通信工具和相关服务(如 FTP、E-mail 等)；往下第三层为传输层，负责传输控制，保证端对端数据传输的完整性(TCP)；第二层为网络层，负责数据传输，将数据发往目的地；最底层为网络接口层，负责访问具体网络(如以太网、令牌网等)。

<table>
<tr><td>应用层</td><td rowspan="3">应用层</td><td colspan="6" rowspan="3">FTP　HTTP　Telnet　SMTP　POP3　SNMP　DNS</td></tr>
<tr><td>表示层</td></tr>
<tr><td>会话层</td></tr>
<tr><td>传输层</td><td>传输层</td><td colspan="6">TCP　UDP</td></tr>
<tr><td>网络层</td><td>网络层</td><td colspan="6">IP　ICMP　ARP　IGMP</td></tr>
<tr><td>数据链路层</td><td rowspan="2">网络接口层</td><td>以太网</td><td>FDDI</td><td>ATM</td><td>FR</td><td>X.25</td><td>ISDN</td></tr>
<tr><td>物理层</td></tr>
</table>

图 3.3　TCP/IP 和 OSI 网络体系结构

2) IP 协议

IP 协议对应于 OSI 模型的第三层，即网络层，提供了一种不可靠、无连接的投递机制。IP 提供了 3 个重要的定义：第一，IP 定义了在整个计算机网络上数据传输所用的基本单元，它规定了 Internet 上传输数据的确切格式；第二，IP 完成路由选择的功能，选择一个数据发送的路径；第三，除了数据格式和路由选择的精确而正式的定义外，IP 还包括了一组嵌入了不可靠分组投递思想的规则，这些规则指明了主机和路由器应该如何处理分组，何时、如何发出错误信息以及在什么情况下可以放弃数据包。

(1) IPv4。

现在所用的以及所指的IP协议版本为1981年定义的第四版，即IPv4，其数据报文格式如图3.4所示。在传输过程中从左到右，从上到下，图3.4中各字段的说明如下：

图3.4　IP数据报文格式

- 版本号——4位，指出当前使用的IP版本。
- 报头长度——4位，用来给出以32位字长为单位的报头长度。
- 服务类型——8位，指出上层协议对处理当前数据报文所期望的服务质量，并对数据报文按照重要性级别进行分配。这些8位字段用于分配优先级、延迟、吞吐量以及可靠性。
- 总长度——16位，指定整个IP数据报文以8位分组为单位的总长度，IP数据报文的最大长度为2^{16}即65 535个8位组。
- 标识符——16位，包含一个整数，用于识别当前的数据报文。该字段由发送端分配帮助接收端集中数据报文分片。
- 标志——3位，其中低2位(最不重要)控制分片。低位指出数据报文是否可进行分片。中间位指出在一系列分片数据包中数据包是否是最后的分片。第三位即最高位不使用。
- 字段偏移量——13位，指出与源数据报文的起始端相关的分片数据位置，支持目标IP适当重建源数据报文。
- 生存期(TTL)——8位，用来设置该数据在Internet中允许存在的以秒为单位的时间，其目的是避免数据报文在网络中出现无限循环。
- 协议——8位，类似于网络帧中的类型字段，它说明数据报文的数据字段中的数据是用哪种高层协议产生的。
- 报头校验和——16位，帮助确保IP协议头的完整性。由于某些协议头字段的改变，如生存期(Time to Live)，这就需要对每个点重新计算和检验。
- 源地址和目的地址——均为32位，用来标明数据报文的源地址和目的地址，在IPv4中将地址分为4类地址。
- IP选项——字段是任选的，主要用于网络测试或调试。
- 填充位——为使报头长度是4个字节(32比特)的整数倍，而调整添加的0的字段。
- 数据——用来传送需要传送的数据，可以为0～65 535个字节。

(2) IPv6。

现在的 IPv4 的地址长度是 32 位,理论上可以支持多达 1600 万个网络,容纳 40 多亿台主机($2^{32}=4\ 294\ 967\ 296$),但由于 IP 对地址进行了分类,分成 A、B、C 等类地址,实际可用的网络数和地址数远小于这个数目。随着 IP 业务的爆炸式增长,Internet 上的 IP 地址已经不能满足实际的需要,此外现有 IP 网络协议还存在安全等问题,随着 IP 在下一代通信网络中标准地位的确立,迫切需要有新的 IP 协议来代替现有的 IP 协议。RFC 1883 定义的 IPv6 就是在这种情况下产生的下一代 IP 协议。

① IPv6 的特点。

与现有的 IPv4 相比,IPv6 具有以下特点:

第一,扩大了地址空间。这是 IPv6 的最大特点,IPv6 将地址长度从 IPv4 的 32 位扩展到 128 位,可以提供约 3.4×10^{38} 个地址,IPv6 的地址是由 8 组 16 位组成。其表示方法与 IPv4 不同,IPv4 是十进制数加".",IPv6 是十六进制数加":"。IPv4 的地址可以在 IPv6 中表示,采用 X:X:X:X:X:X:d.d.d.d 格式,其中 X 是十六进制数,d 是十进制数。例如,IPv4 的地址"202.13.181.100",表示成 IPv6 的地址为"0:0:0:0:0:0:202.13.181.100",称为 IPv4 兼容 IPv6 地址;表示成 IPv6 的地址为"0:0:0:0:0:FFFF:202.13.181.100",则称为 IPv4 映射 IPv6 地址。IPv6 支持多级地址,IPv6 的地址中有单级地址(Unicast Address)、多级地址(Multicast Address)。

第二,简化了数据报头格式。IPv6 的数据报头由标准报头和扩张报头两部分组成。IPv6 的标准数据报头从 IPv4 的数据报头中去除了不需要的域(field),标准数据报头的前 4 位是版本号"域",IPv6 的"6"就在此域表示,该域处于与 IPv4 相同的位置,所以可区别 IPv4 和 IPv6。这样,在同一网络中,IPv4 和 IPv6 可以通用。

第三,易于扩充。由于 IPv6 包含扩展数据报头,增加了选择设定的灵活性,能很好地适应新增功能。

第四,内置安全特性。IPv6 通过对数据报头认证和安全包头封装,提高了信息传输的安全和保密性。

此外,IPv6 的特点还包括 IPv6 采用名为"可聚集全球统一计算地址"的构造,使地址构造与网络拓扑相一致,因而能使 Internet 的路由表缩小,高效地决定路由;互联网地址的自动分配和设置是 IPv6 的默认标准功能,极大地减少了网络管理的负担。IPv6 的具体细节可参阅 RFC1883。

② IPv4 向 IPv6 的过渡。

从 IPv4 向 IPv6 的过渡将逐渐进行,两者会有一定的共存期。把 IPv4 的地址纳入到 IPv6 地址,作为 IPv6 的一部分来使用,有两种方法:一是映射 IPv4 而得到的 IPv6 地址(IPv4-mapped IPv6 Address);另一种是与 IPv4 兼容的 IPv6 地址(IPv4-compatible IPv6 Address)。前者只用于支持 IPv4 的节点,后者是用于支持 IPv6 的节点。实现 IPv4 向 IPv6 转移的技术包括双堆栈系统(Dual Stack System)、隧道技术(Tunneling)和数据报头翻译(Header Translation)。

③ IPv6 的应用。

作为下一代 Internet 基础的 IPv6 经过多年的开发,已经开始从试验阶段向实用阶段过渡。在 1995 年决定主要规格后,IPv6 便成为决定在 Internet 上传输的数据地址及格式的

下一代 IP 的规范。在有关标准化的讨论告一段落后，便开始作为通信用的软件安装于路由器和 UNIX 工作站上。1996 年 2 月美国新罕布什尔大学的 IOL(相互操作性实验室)进行了第一个相互连接实验，随后美国和日本的一些厂商也参加了这类实验。1997 年，以验证 IPv6 为主要目的的实验网络 6-Bone 的规模从 1996 年 7 月的 3 个国家(丹麦、芬兰和日本)迅速扩大到 29 个国家。包括 IBM、HP、Sun、DEC、SGI、富士通、日立等在内的 20 多家厂商参加了对应于 IPv6 的操作系统和路由器的开发。在美国，IPv6 也已经开始在 vBNS(超高带宽网络服务)上运行。目前多数核心路由器均支持 IPv6。

2. 传输控制协议(Transfer Control Protocol，TCP)

由于在最底层的计算机通信网络提供的服务是不可靠的分组传送，当传送过程中出现错误时，在网络硬件失效或网络负载太重时，数据报文可能丢失，数据可能被破坏。TCP 协议的目的是提供可靠的传输服务，TCP 是 Internet 上的第二个最重要的协议，也可以说是基于 IP 上的 TCP。TCP 与 IP 之间的主要差别是 TCP 通过虚拟连接能“保证”数据传输质量，提高传输的可靠性，也就是 TCP 增加了检测分组是否真正到达目标节点的机制。如果数据分组丢失，系统将发出请求，发送端再重新发送所丢失的数据分组。TCP 报文的格式如图 3.5 所示。

<table>
<tr><td colspan="5">位 0　　4　　10　　16　　24　　31</td></tr>
<tr><td colspan="3">源端口</td><td colspan="2">目的端口</td></tr>
<tr><td colspan="5">发送序号</td></tr>
<tr><td colspan="5">确认序号</td></tr>
<tr><td>报头长度</td><td>保留域</td><td>代码位</td><td colspan="2"></td></tr>
<tr><td colspan="3">校验和</td><td colspan="2">窗口长度</td></tr>
<tr><td colspan="3">TCP 选项</td><td colspan="2">填充位</td></tr>
<tr><td colspan="5">数据</td></tr>
<tr><td colspan="5">数据</td></tr>
</table>

图 3.5　TCP 数据报文格式

- 源端口和目的端口——均为 16 位，包含了连接两端对应用程序进行标识的 TCP 端口号。其中源端口识别上层源处理器接收 TCP 服务的点，目的端口识别上层目标处理器接收 TCP 服务的点。
- 发送序号——32 位，通常指定分配到当前信息中的数据首字节的序号。在连接建立阶段，该字段用于设置传输中的初始序列号。
- 确认序号——32 位，包含数据报文发送端期望接收的数据下一字节的序列号，一旦连接成功，该值会一直被发送。
- 报头长度——4 位，TCP 协议头中的 32 位字序号表示数据开始位置。
- 保留域——6 位，是为将来的应用而保留的，必须设置为 0。
- 代码位——6 位，用来指出报文段的目的和内容。
- 窗口长度——16 位，指定发送端接收窗口的大小，也就是数据可用的 8 位缓存区大小。
- TCP 选项——指定各种 TCP 选项。可选项有两种可能形式：单个 8 位可选类型和