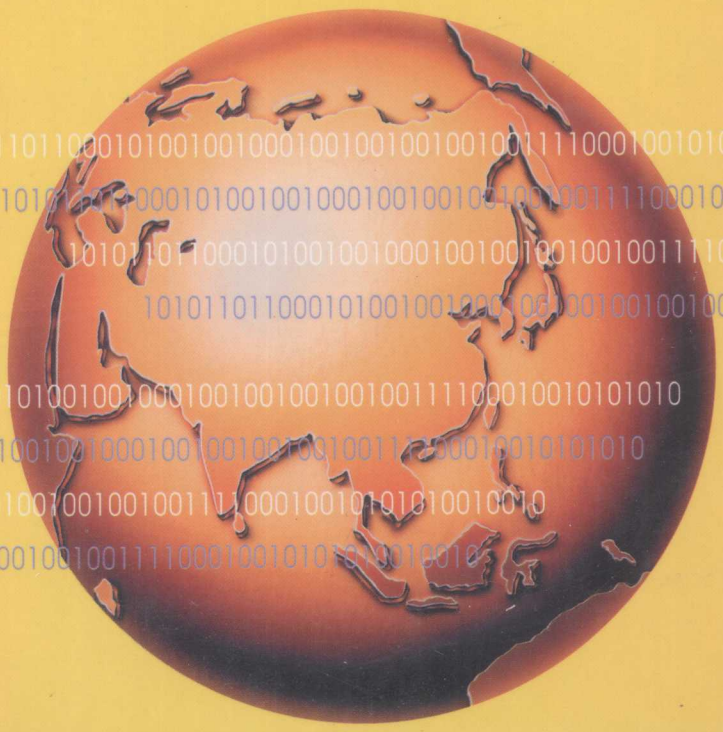
通信网络与信息技术

TONGXIN WANGLUO YU XINXI JISHU

主编 刘恒臣 夏 明



辽宁科学技术出版社
LIAONING SCIENCE AND TECHNOLOGY PUBLISHING HOUSE

前　言

伴随着我国的改革开放，辽宁省通信学会已经走过25个年头。近10年来，辽宁通信事业和其他兄弟省（市）、自治区一样，迎来了发展的最好时期。为了促进辽宁通信科技的繁荣与进步，激励广大会员和通信科技工作者不断攀登科学技术高峰；为了推动辽宁通信事业的大发展，促进通信科技成果向生产力转化，我们编辑了《通信网络与信息技术》一书。

在入选的68篇学术论文当中，我们分别以通信运营管理、交换网管、数据通信、移动通信、无线和卫星通信、传输技术、通信电源、邮政通信等8个方面进行分类，部分学术论文在辽宁省科协和辽宁省通信学会2003年学术年会上获奖，为辽宁通信事业的发展做出了积极的贡献。

由于时间紧和一些客观因素，在编辑工作中如有不妥，恳请批评指正。

编　者

目 录

一、通信运营管理

二、交换网管

三、数据通信

四、移动通信

五、无线与卫星通信

六、传输技术

七、通信电源

八、邮政通信

一、通信运营管理

我省网络安全问题分析及建议

韩殿宽　田　玥

（辽宁省通信管理局网络信息安全处　110013）

摘　要　本文通过分析网络用户通常面临的主要安全威胁，以及我省发生的安全事件，指出了我省目前存在的网络安全问题，并针对具体情况，提出了关于如何加强网络安全工作的几点建设性意见。

关键词　网络安全　分析　建议

当今世界信息技术迅猛发展，人类社会正进入一个信息社会，信息已成为人类宝贵的资源。近年来 Internet 正以惊人的速度在全球发展，Internet 技术已经广泛渗透到各个领域。然而，由 Internet 的发展而带来的网络系统的安全问题，正变得日益突出，网络安全已成为关系国家安全的重大战略问题，网络安全不容轻视。

1．网络安全问题及网络安全薄弱环节

在网络安全的范畴内，网络并不是物理的网络，它包含数据、关系和能力三个基本要素。即包括在网络上传输的数据与端系统中的数据，网络交流需要建立与维护的通信各方的信赖关系，网络系统的传输能力与端系统的处理能力。一般来说，普通网络用户所面临的安全性威胁主要有以下几个方面。

1.1　计算机病毒

计算机病毒（Computer Virus）是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。目前全球已发现 5 万余种计算机病毒，并且还在以每天 10 余种的速度增长。有资料显示，计算机病毒威胁所造成的损失，占网络经济损失的 76%。仅“爱虫”发作，在全球所造成的经济损失就高达 96 亿美元。

1.2　非法访问和破坏（“黑客”攻击）

目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因此黑客技术逐渐被越来越多的人所掌握并不断发展。黑客活动几乎覆盖了所有操作系统，包括 UNIX、Windows NT、VMS 以及 MVS 等。据统计，全球平均每 20 秒就有一个网站遭到黑客攻击。

1.3　网络的缺陷及软件的漏洞或“后门”

因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议缺乏相应的安全机制，因此它在安全可靠、服务质量、带宽和方便性等方面存

在着不适应性。此外，随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件等等都被发现过存在安全隐患。例如，国际上最早、最有名的 Backdorr. B01.2、B02K 和国产的“冰河”的客户端程序是一个可潜伏在用户机中的后门程序，它可将用户上网后的计算机大开后门，任意进出，可以记录各种口令信息，获取系统信息，限制系统功能，对远程文件、注册表进行操作，这在当时影响极大。

互联网的发展，也使病毒、黑客、后门、漏洞、有害代码等相互结合起来，因此对信息社会造成的威胁将更大。根据 CSI/FBI 2002 计算机犯罪调查结果，92% 的网络用户发现了计算机安全问题，85% 的网络用户发现了计算机病毒，80% 的网络用户承认带来了经济损失，78% 的网络用户发现员工滥用 Internet 网络，40% 的网络用户发现了源自外部的系统渗透入侵，40% 的网络用户发现了遭受拒绝服务攻击，38% 的网络用户遭受示授权访问或非授权使用。调查数据表明，随着互联网应用和服务的不断发展，网络安全形势更加严峻。

目前，我国网络安全问题引起了有关方面的高度关注，但是网络安全方面依然存在着许多薄弱环节。一是网络安全防护能力差，缺乏整体网络安全方案，在网络安全上的投资少。大多数单位把资金都投在了应用系统建设上，而忽视了保障网络安全的投资。同国外对网络安全投资占建设总投资约 20% 来比，国内只有 5%。二是基础信息产业的核心技术和关键部件还严重依靠国外。许多核心部件，如 CPU 等，都是国外制造的。此外，国外厂商几乎垄断了我国计算机软件的基础和核心市场，特别是操作系统。三是网络安全领域在研究开发、产业发展、人才培养、队伍建设等方面和迅速发展的形势极不适应。2002 年 11 月，美国国会批准了耗资 10 亿美元的网络安全研究和发展法案（CSRDA），用于创建安全中心、招募研究生以及支付研究费用。与此相比，我国的网络安全专业人才就显得匮乏，我国的网络安全专业人才数量与迅猛发展的互联网产业是不相适应的。

2. 我省近期发生的网络安全攻击事件

去年以来，在我省发生了几起网络安全攻击事件。

2002 年下半年，锦州某电信运营公司互联网络连续遭到黑客的拒绝服务攻击。此次攻击行为使该公司互联网营业网络瘫痪，并波及到相关电信运营公司的网络，造成了很大的经济损失以及客户的流失。省内其他电信运营公司也曾不同程度的遭到类似的黑客攻击。

2003 年 5 月，我省某政府网站的主页遭到非法篡改。一般来说，主页的篡改对计算机系统本身不会产生直接的破坏，但对电子政务与电子商务等需要与用户通过网站进行沟通的应用来说，就意味着电子政务或电子商务将被迫终止对外服务。对政府网站而言，网页的篡改，尤其是含有政治攻击色彩的篡改，会对政府形象造成严重损害。

2003 年 2～3 月间，我省某信息中心、某市气象局、铁岭某信息中心、某市市委和市政府办公室，都曾不同程度受到网络蠕虫病毒的攻击。网络蠕虫的危害通常有两个方

面：一方面，蠕虫在进入被攻击的系统后，一旦具有控制系统的能力，就可以使得该系统被他人远程操纵，这会导致重要系统失密，或被用来对其他系统进行攻击；另一方面，蠕虫的不断蜕变并在网络上的传播，可能导致网络被阻塞，从而导致网络瘫痪。

上述网络安全事件的发生，充分暴露了一些部门和企事业单位在网络安全方面存在的问题。一些部门和企事业单位的领导对网络安全认识不高、重视不够，从业人员和相关人员的网络安全观念淡薄、意识不强，在贯彻落实相关法律规章和执行各项管理制度方面还不到位，网络安全技术防护配置相对较弱，在网络安全管理方面和技术防范措施方面缺乏经验，应对网络攻击突发事件及主动发现和防御网络攻击的能力不足。

3．对加强网络安全工作的几点建设性意见

为了切实加强我省在网络安全方面的防护能力，保障我省互联网事业健康、快速地发展，针对我省网络安全现状，提出以下几点建设性意见。

3.1 提高对网络安全工作重要性的认识

网络安全关系到国家安全和社会稳定。网络安全是一种状态，是一个过程，是一项长期任务。提高各级领导、网络运营者、各应用单位对网络安全工作重要性的认识，增强网络安全的责任感和紧迫感是当前的一项重要工作。如果认识问题不能很好地解决，还存在轻视网络安全的种种模糊认识，必要的资金投入和人才投入就得不到保证，相关的法律规章和管理制度就很难落到实处。

3.2 层层落实网络安全管理责任制

各部门和企事业单位都要切实加强网络安全管理工作，确定网络安全管理重点，明确哪些资产需要被保护，分析这些资产存在的风险种类、程度和受损时的后果，有针对性地提出有效的解决办法和建立完善的管理制度。网络安全管理工作贯穿到网络规划、网络建设、系统维护和运行使用全过程。要最大限度地消除网络安全隐患，不能随意默认安装操作系统或应用软件，不能使用不安全、不规范的软件，要严格设置密码账号，不进行明文传输，要进行安全备份，限制开放的端口服务，对管理数据的进出地址进行访问控制，进行完整的日志记录。要严格监督检查制度，明确操作规程和责任，避免人为“事故”的发生。要建立网络安全报告制度，对出现的网络安全问题要及时报告，不能隐瞒。

3.3 增强网络安全技术防范能力

各部门和企事业单位不仅要重视网络安全问题，还要增加对网络安全方面的投资，在网络规划建设过程中要同时考虑网络的安全措施。建立一个比较稳固的立体安全防护体系，包括防火墙、防病毒、入侵检测和扫描等一整套安全防护解决方案，提高基础网络和各个应用系统的抗攻击能力，把出现事故的概率降到最低。不仅要充分考虑到服务器自身的安全性、稳定性，而且要保障客户端等其他环节的安全性，增强自身抵抗能力，杜绝一切可能让黑客入侵的渠道，避免造成对系统的威胁。对涉及政治、经济等重要应用，要采取特殊措施加以保护，如安装防火墙、采用数据加密技术等，使不法分子难有可乘之机。基础电信网络运营单位要建立系统软、硬件安全防范体系，阻挡“黑客”的入侵。注意查找设备软、硬件所存在的各种漏洞，及时更新各种软件补丁。建设

多路由的物理网络，提高网络在各种情况下的自愈容灾和抗打击能力。

3.4 健全网络安全保障体系

按照检测预警、指导协调和应急响应的架构，努力构筑一个技术先进、管理高效、反应迅速、安全可靠的网络安全保障体系。一是，根据有关部门对网络安全事件苗头的检测，提供对网络安全事件的预警信息，及时通过媒体进行预警。二是，建立网络安全事件协调机制，指导、协调处理所发生的网络安全事件。三是，充分依托基础电信网络运营单位，建立网络应急响应机制，及时应对网络安全事件。

3.5 加强网络安全教育和人才培养

网络是否安全，不仅是单一的物理防范问题，还受人的素质等其他“软”因素的影响。因此，有必要根据各类人员的具体工作进行有针对性的安全教育和技能培训，尤其是“网管”人员和其他涉及网络安全的相关人员。定期聘请国内外著名的网络安全专家和学者进行培训，聘请有关行业主管部门讲授网络安全法律法规，使其了解我国网络安全现状，有的放矢地做好本职工作。同时，要特别加强网络安全方面的人才培养和使用，加强网络安全技术的研究工作。

4. 结束语

网络安全是一项长期、复杂的工作，安全的网络是网络应用和发展的前提。相信，通过各部门和企事业单位的共同努力，营造出一个安全的网络环境，来推动我省互联网事业持续、健康地向前发展。

参考文献

1 张立涛，钱省三．信息安全策略的原则和方法．网络安全技术与应用，2003，6：11～14

2 冯运波，夏光升．信息安全技术发展现状．计算机安全，2002，11：11～15

3 科飞管理咨询公司．信息安全管理概论．北京：机械工业出版社，2002

4 江苏，老诚．网络攻击技术新趋势．网络安全技术与应用，2003，2：76～77

5 蒋建春，马恒太，任党恩，卿斯汉．网络安全入侵检测．研究综述，软件学报，2001，11：1460～1466

论宽带运营中的定价策略

王凌云

（中国网通集团辽宁省通信公司市场经营部　110003）

摘　要　在宽带的运营策略中，最重要的有两点：一是定价策略，二是用户拓展策略。其中电信运营商通常都要先制定价格策略，然后再根据价格策略制定相应的用户拓展计划。本文从一个主导电信运营商角度，从用户群的划分、计费方式的选择、与窄带业务的关系、不同的建设方式以及竞争因素五个方面，对于宽带运营中的定价策略进行论述，着重说明了这五个方面对于宽带价格的制定的影响，以及如何从这五方面入手制定合理的宽带业务资费。

关键词　宽带　定价策略　主导运营商

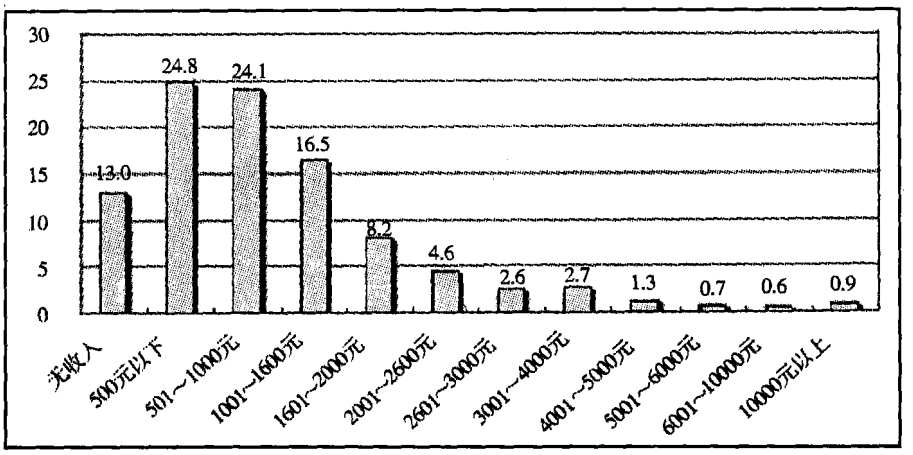
在宽带的运营策略中，最重要的有两点：一是定价策略，二是用户拓展策略。其中电信运营商通常都要先制定价格策略，然后再根据价格策略制定相应的用户拓展计划。本文从一个主导电信运营商角度，着重论述宽带运营中的定价策略。

价格在任何商品的销售过程中都是一个关系到其成败的敏感因素，一味的价格战通常会降低整个行业的利润水平，并不是可取的营销策略，然而多家运营商的相互竞争，又必然要在定价策略上做足文章，因此考虑多方面因素，制定切实可行、又能够给企业带来足够效益的市场价格十分必要。从宽带的运营角度来讲，制定宽带业务的价格要从以下几方面考虑。

1．用户群的划分

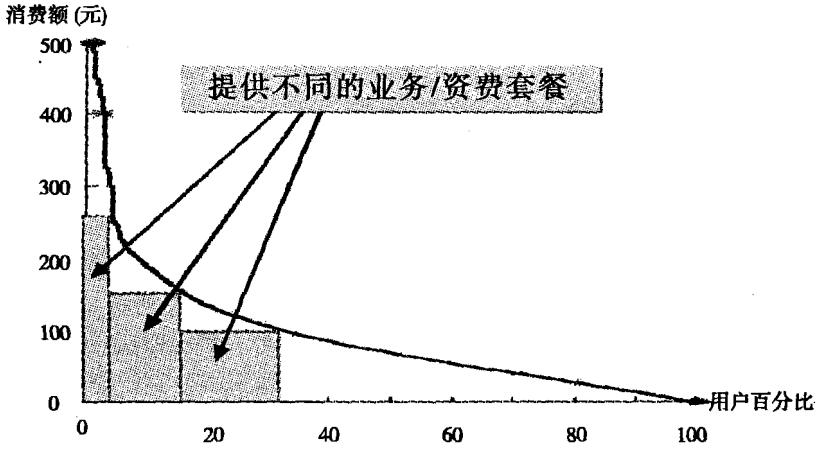
针对不同的用户群实行差异化的价格，能够很好地兼顾运营商的收益和不同用户群的不同承受能力。CNNIC 第 10 次互联网调查结果显示，目前 77.1% 的网民采用自费上网方式，是上网费用的主要来源，而网民个人月收入情况却有很大的差异性，如图 1 所示，这种收入上的差异使得即便宽带业务市场上存在一个利润最大化的单一价格，也会有数量极为庞大的用户群，因为这个价格超过他们的承受能力而无法成为宽带业务用户，从而使运营商丧失一部分市场空间和利润来源。而针对多个用户群制定不同的资费会解决这个问题。如图 2 所示，这是一条宽带业务的用户需求曲线，如果执行 150 元/月的统一价格，会有 15% 的用户选择宽带业务，但是运营商无法收到愿意支付 250 元/月的 5% 用户的额外收益和只能承受 100 元/月的另外 20% 用户的费用支出，而区分不同用户群进行定价就可以做到这一点。

细分用户群首先要考虑能够将用户按照某种典型的特征划分开，避免界定不清的用



资料来源：CNNIC，2002 年 7 月

图 1　网民个人月收入分布（%）



资料来源：CNNIC，2001 年 7 月

图 2

户向低资费的用户群倾斜，也就是说各个用户群要有自己鲜明的特征，其划分才具有可操作性。目前传统的语音业务通常是按照住宅用户和商业用户进行划分的，宽带业务也完全可以借鉴这种划分方式。随着业务的发展，用户的逐渐增多，还应该进一步细分用户群，来制定与之相符的价格。如高等院校学生用户，根据人民邮电报调研结果，目前平均每个学生每月的宽带上网费用在 40～60 元左右，一个拥有 10000 学生的高等院校每月会有 40 万～60 万元/月的潜在收益。然而，学生市场与普通的住宅用户有着不同的消费特征。首先，大家很难达成协议去共同承担初装费。其次，学生内部结算非常成问题，而且后付费形式可能会带来收费上的麻烦。因此应将其划分出来制定有针对性的资费。再如酒店和写字楼用户，同样属于流动性比较大的用户群，但通常用户消费水平较高，同时运营商还要考虑酒店、写字楼物业作为中间商的二次运营问题，因此，与二次运营的中间商共同制定这部分用户的宽带资费十分必要。

细分用户群还要考虑不同用户对于宽带业务的不同需求，只有从不同的角度满足了他们的需求，用户才会愿意支付宽带上网费用，这就涉及到价格策略中的计费衡量标准问题。如网吧用户，他最关心的是上网的速率，只有高速率才能赢得用户的青睐，因此应采用基于宽带的灵活资费策略来吸引他；再如普通住宅用户，由于窄带业务一直是以时长为计费的衡量标准，而用户的消费是有惯性的，所以采用基于时长的资费策略有利于更好的拓展用户市场。除此之外，细分用户群后还要实时的跟踪不同类别用户的消费行为，从而及时调整资费策略。

2．计费方式

宽带接入业务的计费方式无非三种：包月、限时包月和计时制。其中许多省市都曾采用了一包到底的包月制（如100元/月），这种包月制在宽带业务发展初期是一种很好的计费形式，资费形式简单明了，收入有保证，而且有一定的进入门槛（如按照上述包月标准，上网时间较短，消费远低于100元的用户通常无法选择宽带），但它毕竟是一种比较粗放的资费形式，不易于对于用户进行管理，无法满足用户个性化需求，而且用户的使用量与费用支出不匹配。

限时包月（如表1所示）是对一包到底的包月制的一种改进，避免用户无度的使用网络资源，同时细化了收费层次，降低了使用门槛。收益上也会随着用户群的扩大而增加。这种方式应与计时制相结合，才显得更加完整、合理。在制定限时包月费时，要诱导用户尽量往其以往消费水平的上一档选择，鼓励用户多消费。

表1　　资料来源：北京市通信公司信息港

月使用费	限制使用时间	超出部分
99元	40小时	0.05元/分钟
199元	100小时	0.05元/分钟
380元	200小时	0.05元/分钟

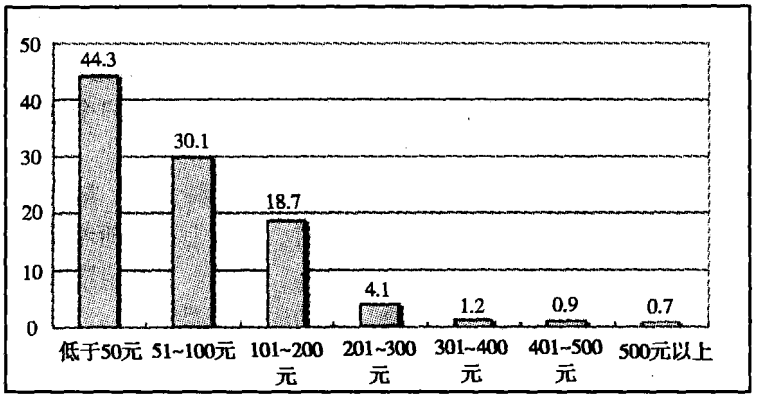
计时制（即＊＊元/小时）是宽带业务进一步发展后的计费模式，但对于普通用户来说，它往往会导致用户长时间地占用端口却不能产生足够的消费。尤其在目前各宽带接入运营商都在努力抢占市场，接入能力没有过剩的情况下，这种方式会导致一方面有需求的用户得不到满足，另一方面，已有用户消费不足，甚至产生大量零次户，因此它属于未来宽带计费方式，不宜过早采用。但对于校园用户来讲，它可以解决学生间的内部结算问题，如采用卡付费方式还可以解决收费问题，这部分用户群可以率先考虑使用计时制进行计费。

3．与窄带业务的关系

本文是从一个电信主导运营商的角度来论证宽带运营的定价策略问题。所谓电信主导运营商，是指经营本地固定电话业务，并占本地网范围内同类业务市场份额50%以上的电信业务经营者，并对其他电信业务经营者进入电信业务市场能构成实质性的影响

的电信运营商。宽带业务的迅猛发展使得窄带的高端用户群向宽带转移，而目前许多地区宽带资费普遍低于窄带的现象很可能导致运营商的互联网接入收入不升反降，因此，无论从资源的有效利用和效益最大化的角度来讲，主导运营商都应该在制定宽带价格策略时考虑与窄带业务的关系，即给窄带业务留有一定的发展空间。

首先从收入上看，第 10 次 CNNIC 调查结果显示，网民每月花费的上网费用主要集中在 100 元以下，低于 50 元的网民最多，达到 44.3%（如图 3 所示），可以考虑将消费低于 50 元的用户群留给窄带。例如，将限时包月的最低消费门槛定在 50 元，这样，部分月消费不足 50 元的窄带用户不会向宽带转移。各地市也可以根据本地的窄带用户消费情况制定自己的最低消费门槛。



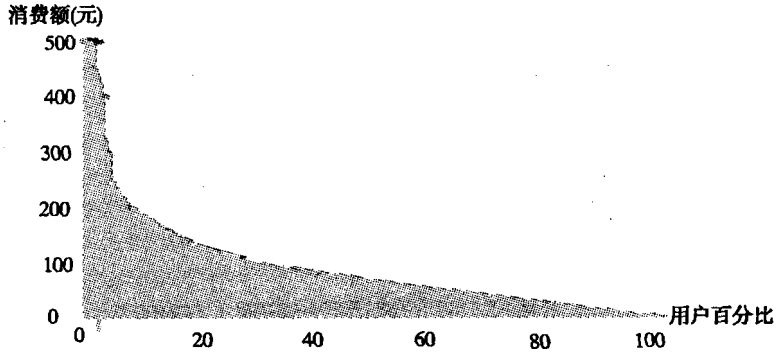
资料来源：CNNIC，2002 年 7 月

图 3　网民每月实际花费的上网费用分布（%）

其次，从上网时长来看，第 10 次 CNNIC 调查结果显示，网民平均每周上网 8.3 个小时，即每月不到 35 小时。在制定限时包月制资费时，就可以考虑将宽带消费的起始时长设为 30～35 小时，这样就将上网时间较少的一部分用户留给了窄带。

4. 建设方式

不同的宽带接入方式会有不同的建设成本，其特点决定了它要有不同的定价策略。例如，DSL 宽带接入与 LAN 方式就有很大的区别，DSL 方式随着接入用户数的增加，其边际成本在递减，但不会等于零。也就是说，它存在一个极限的单位用户成本，提供低于这个成本的接入价格对于运营商来说是没有效益的。而 LAN 方式不同，一旦某个 LAN 小区建设完成，小区的网络成本就已经固定了，其边际成本为零，也就是说，此时新发展一个用户不会新增一份成本，那么每发展一个用户都是有益的。所以制定一个能够使每个用户都能按照自己的承受能力购买宽带服务的价格策略会使整个小区的收益最大化。其最完美收益情况如图 4 所示，尽管有些理想化，但至少应该考虑为价格承受能力较低的低端用户群提供宽带业务，如出售小面值的宽带上网卡等。



资料来源：CNNIC，2001年7月

图4 LAN小区理想消费情况

5．竞争因素

竞争因素是宽带定价策略中应该最先考虑的因素。不仅要考虑竞争者的定价情况，还要考虑它们对于本企业价格变动的可能反应。在与竞争对手接入能力、服务水平相当的区域，以及从战略上讲必须占领的用户地区，应该采取适当的低资费策略，争取抢先进入市场。因为用户的消费是有惯性的，决不会因为竞争对手的再次降低资费就轻易转网（除非对手的资费水平过于低廉）；对于竞争对手还没有能力进入的地区，或者服务水平、产品质量与我们有差距的地区，应该考虑前面的四点因素，制定一个能够体现本企业宽带产品质量的价格，率先给宽带做一个比较准确的市场定位。其他运营商通常会采用竞争导向定价法，即比照主导运营商的价格，来制定自己的宽带业务价格，因此主导电信运营商制定的宽带价格至关重要，直接关系到整个宽带业务市场的利润空间。

以上是制定宽带价格策略时应着重考虑的几个方面，随着竞争的加剧，宽带业务的不断发展，宽带运营的价格策略会越来越重要，相信合适的价格策略会给运营商在宽带接入市场上带来更大的收益。

论接入网维护管理

徐北鸥

（辽宁省通信公司网络运行维护部　110002）

摘　要　本文首先论述厂接入网维护管理目标和基本任务，以此为基础进一步阐述了接入网障碍处理的流程，关键环节的控制，障碍统计分析的作用，以及接入网日常维护的项目和管理方式，维护质量考核与评价的根本目的和相关思路。

关键词　接入网　维护　管理

接入网（Access Network）是指交换局到用户终端之间的所有机线设备。ITU－T 规定，接入网是由业务节点接口（SNI）和相关用户网络接口（UNI）之间的一系列传送实体组成。通常包括用户线路传输系统、复用设备、用户网络/网端设备，能为电信业务提供所需传送承载能力的实施系统，并可用网络管理接口（Q3）进行配置和管理。本文论述的接入网维护管理是指交换 V5 接口出去以后的所有通信设备，包括光纤线路终端（以下简称 OLT），相应的 SDH 传输设备，光纤网络单元（以下简称 ONU），光缆、电缆线路，以及相应的配套设备（如图 1 所示）

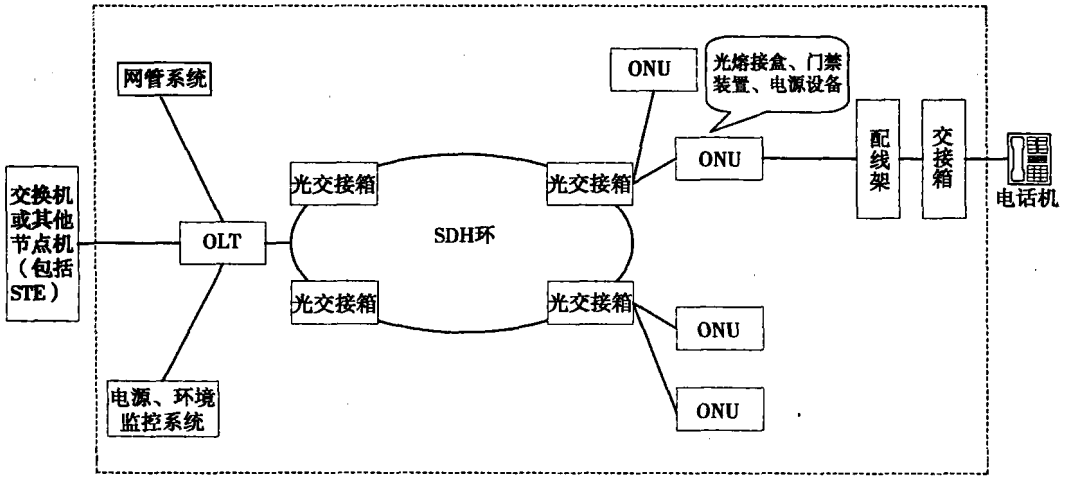


图 1　接入网维护管理对象图