IP协议及网络安全问题的战略思考

作者：陈如明 来源：中国联通网站 发布时间：2007-02-27

摘要 NGN，3G，3G演进及NGBW(下一代宽带无线)是目前通信业界非常关注并在不断探讨的热点话题。人们希望，通过NGN及NGBW来解决目前各类网络中存在的诸多问题。但NGN依然存在不少问题与困惑，对所谓全IP发展NGN的策略是否稳妥，依然有不少怀疑与争议。本文从IP协议的内涵、作用与外延的一系列问题出发，以IP安全性为重点，对IP协议的重要现实作用、存在问题及其进一步的发展策略，提出了一些战略性思考。

关键词 GII NGN 3G/3G演进 安全性 IP-QoS 智能网管 软交换

一、引言

NGN，3G，3G演进及NGBW(下一代宽带无线)是目前通信业界非常关注并在不断探讨的热点话题。人们希望，通过NGN及NGBW来解决目前各类网络中的许多问题，如网络安全问题，QoS问题、智能网管问题，网络的移动性及汇聚与融合问题、前后向兼容平滑演进问题等。2003年下半年至2004年年中，ITU-T SG13研究组进行的标准化工作取得了不少进展，在新研究期中将集中精力，专注NGN的研究。2004年6月的ITU-T第13研究组会议上专门组建了一个新的NGN专题组FGNGN(Focus Group on NGN)，以应对NGN发展的紧迫需要，加强和推进NGN方面的研究工作。目前，已成立七个工作组，分别在业务需求、功能体系架构和移动性，IP-QoS，控制和信令能力、网络安全、网络演进及IP承载能力要求等七个领域进行工作，以满足国际上对全球通用的NGN标准的迫切需求。至今已完成诸多标准建议草案，对NGN的研究方向、通用参考模型、框架体系、业务需求、网络功能、网络安全及IP承载能力要求、互联互通、服务质量、移动性管理、可管理的IP网络、异构网络性能和NGN网络演进融合方式等各个方面提出了总体要求，为世界各国的通信运营商和设备制造商提供了网络发展和产品研发的思路和依据。

但客观地说，NGN依然存在不少问题和困惑，特别是NGN在分阶段务实发展的同时，如何从战略高度确立其目标框架及目标定义及其与分阶段实施的关系至关重要。同时，所谓全IP发展NGN的策略是否稳妥，依然有不少怀疑与争议。本文拟根据IP协议的背景、内涵、作用与外延等一系列问题，重点就进一步发展IP及NGN的理性战略思维问题谈一些个人看法，供分析参考。

二、IP协议及NGN的产生背景与必然性

众所周知，IP或TCP/IP协议是互联网Internet发展的基础。尽管对NGN的概念、定义、结构，NGN的发展是否应以IP为基础，是否采用所谓全IP等这些最基本的问题尚未获得全球性的统一见解，甚至还存在一些较尖锐的分歧，但NGN的背景与必然性，以及IP协议普及应用的基本作用与外延等一系列问题是明显的。

(1)20世纪末期，对无缝隙覆盖全球个人多媒体通信的需求推动了GII建设的热潮。基于TCP/IP协议的Internet技术由

E-mail和VoIP应用切入，使Internet/Intranet和WWW飞速发展，在全球快速普及，广受欢迎，人们普遍认为这可能是未来GII的一个发展方向。

(2)随着数字传输技术、数字信号处理技术及高级软件技术的进展，对一向处于低效率运作状态的三网分立的局面，人们普遍感到不满意，期望IP协议能成为三网融合的基础，再借助一系列新技术逐步实现三网的融合。IP协议有可能成为固定与移动通信融合的粘接剂，这对未来全球个人通信及GII的实施至关重要。

(3)以TCP/IP协议为基础的Internet设计的初衷主要是考虑军事应用及提高抗干扰能力，它是以牺牲网络带宽为代价的。其网络结构及协议也存在一系列问题，是一种非面向连接及尽力而为(BE，Best Efforts)的方式，未顾及移动漫游个性化要求，是一种主要由科研团体和/或政府研究机构松散管理下的一种非商业应用网络。但进入大规模商用后暴露出来的安全性，QoS，网络智能管理、赢利商业模式等多方面问题，使Internet的NGN2/GNI的发展面临严峻挑战。目前尚无法找到一种更好的可进行大规模普及操作的网络结构，因此现实的做法理应是集思广益，博采众长，吸收各种新概念、新思路及新技术，使之尽可能全面改进，以尽快满足市场需求，并创造新的增值效益。从某种意义上讲，这亦是一种不得已而为之的因势利导的现实主义作法。

(4)在“.COM泡沫”的破灭、对“宽带泡沫”的质疑、对3G发展的迷茫及传统电信业务盈利下滑等多种因素的作用下，促使传统运营商与制造商急需寻找出一种能平滑演进、适应市场需求的新一代网络结构与多业务增长途径。20世纪80年代，PC机控制软件与计算硬件分离，形成充分开放的多厂商竞争环境，最终推动整个计算机业的繁荣与发展，促使人们认真思考未来网络的发展是否应走这条道路。

(5)随着软交换技术及软件无线电技术的诞生与改进，无论是有线网还是无线网，均可采用分层、分面及全开放模式，基于独立的模块化结构，实施业务驱动，使业务、呼叫控制及承载完全分离，从而以优良的性能价格比、前后向兼容的过渡方式，平滑地向新的以IP为基础的网络演进。这些技术可望成为较现实的新一代网络，即所谓NGN的核心支撑技术。尽快统一全球标准，与原先提出的GII这一目标进行协调与融合，已成为相关组织(如ITU-T/R，ETSI，IETF，3GPP，3GPP2，ISC/IPCC，TINA/TIMNA，MSF，OMA等)的共同愿望。

尽管在IP协议及NGN问题上，人们在概念、定义和结构等方面均明显存在含混不清及不同理解之处，依然成为全球各大标准组织、运营商、制造商、研究开发及政府相关部门共同关注的热点，并在加紧探索各种务实发展途径。这无论对固定或移动，对公网/共网及专网，对地面或空间，均是如此。

三、IP化是大势所趋

目前，IP化已是大势所趋，故NGN应以IP为主要考虑前提。

1.NGN发展的目标战略

NGN应是能提供各种多媒体业务的综合网络，支持固定和移动的融合及传统电信业务和广播业务的融合，是有线/无线网络元素、计算机系统、家庭外围设备、智能工具等组成的综合融合环境。NGN必须能折衷满足不同业务质量及物理接口的要求，在业务管理、网络管理、智能化、个性化服务等方面均可提供完备的机制。

纵观全球，尽管尚未对NGN给出一个统一清晰的定义，但在一些基本点上已达成共识，即NGN是基于分组交换的网络，分组交换一般是基于IP协议；以市场与业务驱动为导向，将呼叫控制与网络传送层及业务层完全分离；网络结构分层，各

层间有开放的标准接口；业务承载网与业务网应能有效地彼此分离；核心传送网为高带宽光传送网；网络具有满意的服务质量保证和合理的安全保证；网络是可维护、可运营的，并且是可赢利的多业务网络；网络应支持包括终端移动性和用户移动性在内的广泛移动性。

从广义角度看，应该说，NGN是一种目标网络，而不是下一代Internet网，亦不是下一代PSTN电话网及下一代电信网与下一代有线电视网及广播电视网，而是由新的分组交换传送及以IP协议为基础的融语音、视象、数据于一体的一种全新的网络。它将真正使网络设施不受时间、空间和带宽的限制，充分实现网络的个性化与个体化，使基于网络的虚拟世界与现实世界完美地融合起来，具有所谓接近于零的网络时延与优良的网络端到端QoS性能，令人满意的网络与系统的可靠性与可用性，以及足以信赖的网络安全性。网络管理可达到全局智能化，既有利于可赢利商业模式运作的集中智能网管，又可将网络智能分布化，保持与发扬Internet终端智能化的长处，摒弃其整体网管弱智与缺乏可赢利商业模式运作的严重缺憾。网络接入可达到普遍灵活、多样化、个性化的5W(5A)方式的无缝隙宽带接入，有跨协议、跨标准国际漫游能力，以市场与业务驱动为导向，将呼叫控制与网络传送层及业务层完全分离，可进行服务的快速布设与移植，可充分利用平台的分布性、开放性与标准性，积极调动运营商及第三方的创造性。它是具有快速丰富业务种类与市场应用等特征的一种理想化的网络，可充分满足社会与个人愈来愈高的综合性全球通信要求，具有多业务、高质量、宽带化、分组化、智能化、移动性、分组性、安全性、开放性、分布性、兼容性及可管理性与可赢利性等一系列全业务综合运作的基本特征。这是目前Internet网、电信网、移动网、广播电视网及专用通信网等均不能全面具备的基本特征，亦是它们按NGN定义与框架目标要求进一步演进、集成、协同、汇聚与融合所期望达到的目标要求的基本特征。因此，各类在NGN概念导引下前向演进产生的新一代网络均为NGN集合的子集。

显然，按上述框架目标实施的NGN决不可能轻而易举地一步到位，必然是一个积极稳妥、科学务实地分阶段向GII逐步演进发展的漫漫征途。因此，从定义和实施策略看，制定明确、科学、稳健的长远性及各阶段性的NGN务实发展步骤依然十分必要。应该说，从现在至今后五到十五年左右，NGN依然处在其初始发展阶段。在此阶段，应较好地解决启动问题，坚定地迈出成功的第一步。这一方面需要较满意地完成NGN的确切定义、基本框架目标、阶段实施途径等基本标准化工作，另一方面NGN的三大组成部分，即下一代因特网(GNI)、下一代电信网(NGTN)、下一代移动网(NGMN)均应根据自身发展基础，积极按NGN的基本概念、定义、目标要求等制订与实施务实发展策略，从技术层面、系统结构与市场模式彼此渗透，并一步步汇聚与有机融合。例如，GNI应以引入IPv6以及网格技术与业务为中心，同时改进TCP/UDP等一系列相关协议，使GNI在未来宽带多媒体、多业务时代首先实现可管理、可赢利。

NGTN以软交换技术为核心，试验探索及启动实施则基于TDM的电路型PSTN语音网络和ATM/IP分组型网络向初级NGN网络的融合演进，使所期望的NGN低建设成本、低运营花费、多业务高创收、有效的前后向兼容平滑演进及充分发挥用户积极性和创造性等优点有所体现。NGMN以3G及3G演进为中心，并有机融合802.xy，包括终端、业务与应用在内，制订与2.5G有差异化的务实发展策略与商业模式。

作为NGN启动发展的有效步骤，以软交换为中心，或以IPv6及网格技术与业务为中心，务实推进是十分必要的。与此同时，必须站在目标NGN角度，进行更全面与更长远的规划与思考。以软交换为例，用软交换机改造现有PSTN网络及其“硬”交换机时，切忌将其理解为只是由“硬”到“软”的设备与技术的更替。这样，很容易回归到PSTN的封闭性理念与框架的怪圈之中，从而违背NGN目标的初衷。就NGTN而言，它不仅仅是由TDM技术转化为IP分组技术。从应用与多业务层面看，更重要的是应按NGN目标框架，将原有僵化的端到端连接型控制机制转变为灵活、丰富、多样化的会话型控制机制，将原有的由个体网元集中控制的管理模式转变为资源自适应均衡调配的分布式网络控制管理模式，将原有缺乏前向扩展能力的单一业务垄断经营模式转变为多业务/综合业务的共赢价值链经营模式，并充分发挥第三方的天才与创造性。在具体规划和实施各类NGN起步工作时，应时刻牢记、并有效贯彻这些总目标。

2.NGN应以IP为主要考虑前提

如上所述，NGN以分组交换传送为基础及多(全)业务网络的分组化在IP，MPLS，ATM和Ethernet方面已获得共识。很明显，MPLS及Ethernet与IP是完全可以协调发展的，主要分歧仅在于IP与ATM谁更适合。这依然是一个重要问题，因为它对确定NGN的发展基础与前提至关紧要。

在确立NGN的基本发展策略时，应根据其基本技术特征与长期的市场检验和选择的结果，明确NGN以分组交换为基础，以IP为主要考虑前提，否则将无益于推进以IP为基础的NGN的创新与发展。当然，并不排斥在NGN的阶段发展过程中充分合理地利用ATM在一定阶段上尚存在的可能作用与价值，以及吸取ATM的某些有益理念，使NGN以IP为基础的QoS控制及VPN的发展获得强有力的支撑。退一步说，如果ATM果真出现奇迹般的长进，比起更新演进后的IP来，全局含义上更为合适，也可由市场作出最后抉择。但归根结蒂，在这一点上至今并未发现有任何可能的迹象，因此认定NGN以分组交换为基础，以IP为主要考虑前提，应该是一种明智的现实选择。

事实上，ATM的兴衰亦与数据交换的发展紧密相关。应该说，ATM是后来者，它比Ethernet及Internet晚了近20年，比个人电脑亦晚了近15年。上世纪90年代初，在语音/数据集成及端到端QoS控制方面，ATM深受青睐，当时人们甚至认为，以太网交换技术仅仅是延长其陈旧技术生命的一种权宜之计而已。因为从最佳系统设计的负荷平衡理论观点看，以太网速率低，集线器采用共享式的CSMA/CD(载波侦听多址连接/冲突检测)模式运作，当用户上网增多时，就会导致传送瓶颈，更谈不上QoS保证。因此，千兆比第三层交换机出现之前，ATM被视为更新核心网交换的惟一合适途径。然而，始料不及的是，市场驱动的魔力使以太网经受住了严峻的挑战，七年内将网络速度提高了两个量级。而ATM的所谓端到端连接忽视了至关重要的台式机用户，需要在终端用户处附加许多软硬件设备。从节省成本角度看，快速以太网显然占上风。而且，ATM/以太网的混合环境使网络分割与重组开销很大，在图像处理等计算密集场合无法容忍，ATM的很多应用便显得缺乏实用性。ATM的结构严谨，但缺乏灵活性，且价格昂贵。以太网的GB/10GB高速交换的进展及由LAN向MAN/WAN的扩展，Internet及IP的爆炸性增长与IP QoS的逐步进展，终于使人们认定，ATM只能退居市场中的过渡地位，逐步走下坡路，这是市场选择的结果。与此同时，人们对IP QoS的信心与决心日益增加。由于传输资源的紧缺与昂贵，本来可利用提高节点设备ATM交换机的复杂度和提供QoS控制能力以换取传输资源带宽能力的不足，这是一种有效的互补性选择。但历史的发展证明，不用说核心层面，甚至接入层面，带宽资源已愈来愈显得不那么稀缺昂贵。同时，IP技术带来的多业务的增值灵活性、价位的吸引力以及日益完善的IP-QoS技术的安全性，使移动、固定及卫星通信等原本资源最受限的无线传输与接入手段亦均无例外地选择ATM作为一种过渡的权宜之计，而将长远目标均锁定在以IP为基础上。3G及3G演进的全IP NGWB选择即为其明显示例，且未引起过多的质疑。因此，围绕ATM与IP选择的争论实际上是没有必要的。认为NGN以分组交换为基础，以IP为主要考虑前提，应该是一种明智有益且较现实的选择。

3.以用户新业务需求为驱动力IP化已成全球发展现实

如上所述，以IP为基础的Internet的普及商用成功已造就一张覆盖全球的Internet大网。在此大网上，尽管有大量的麻烦与问题不断产生，但也已有大量IP业务在运行和使用，亦有大量支持IP的业务开发人员、运行维护人员在运作，并正在投入大量人力、物力与财力，针对IP商用暴露出来的弊端对IP技术进行改进，大力开发各类IP新业务与新应用，努力推进IPv6，GNI，100×100项目及美国国防网格网，向目标NGN迈进，这已是不争的事实。

实践证明，业务与承载可分离的充分开放的IP平台为业务与应用创新提供了广阔的发展空间，门户网站、搜索引擎，P2P(Peer to Peer)等应用无一不是其开放性的创新硕果。随着IP QoS的一步步改进，VoIP不仅在专线专网，而且在长途/本地市话方面，包括VoIP的O/P-WLAN运用在内，均已经或正在逐步走向成熟，逐步达到电信级运营要求。IP平台上的宽带数据业务，包括(准)实时流媒体及视频业务IPTV等均已显露出其芒锋与潜力。即便对ATM而言，亦未历经大规模、大范围视

频业务的传送检验。如果要投入巨大的人力、财力、物力去尝试E-mail/WWW/FTP/TelNet乃至(准)实时流媒体、双向视频over TDM/ATM等，简直不堪设想。因此，目前逐步由IP over Everything转移至Everything over IP绝非偶然，这是市场需求导向检验与选择的结果。虽然在这一进程中并非一切尽善尽美，但以用户新业务需求为驱动力的IP化，确实成了大势所趋，已在全球成为无可否认的现实。

四、IP协议存在的问题与发展的战略思考

1.IP协议的问题所在

如上所述，根据以TCP/IP协议为基础的Internet的发展历程可知，IP协议最可取的内涵与作用在于其充分的开放透明性与灵活有效的多业务增值能力。然而，在开放透明的同时，也往往更容易“充分暴露”，自然也容易受到攻击。在Internet商用化后暴露出来的一系列问题中，最棘手、解决难度最大的问题就是安全性问题。

对IP协议的安全性问题，最尖锐的观点来自TINA/TIMNA。TINA/TIMNA的观点很明确，认为NGN不应该是“全IP化的网络”，而应该是一种以“中间件(Middleware)为基础的网络。TINA支持ITU-T建议Y.130的ICA(信息通信结构，Information Communication Architecture)，认为Internet及其IP网的三大缺陷是安全失控，QoS无保障及网管弱智。全IP化即使使用IPv6也不能有本质性的变化，必须从中间件层入手，才能真正取得隔离功能及解决安全问题。IP协议结构象“明信片”，源/目的地和内容三者关联，全局暴露，是其易受攻击与无法解决好安全性问题的根本所在。“IP决定一切”违背分层网设计“应用决定一切”的公认理念，造成事实上的本末倒置。有结构的进化，才能有功能的突破。“未来网技术IP不是惟一的选择”。TINA支持以ICA为基础向NGN演进。

应该说，TINA/TIMNA提出的看法是有价值的，尤其是它一针见血地指出了IP协议安全失控的本质所在。实际上，仔细分析PSTN，ATM及IP网络结构可更充分理解IP网易受攻击的原委。

一般情况下，安全攻击多半在终端发起。PSTN的终端本质上是傻瓜型，兼之PSTN的收费模式，若想在终端入手发起大规模攻击，成本很高，难以操作。在PSTN的用户端与网络端，UNI与NNI彼此分离，业务的提供及控制权均在运营商手中。没有运营商的参与，用户难于在终端玩新花样、播发病毒及发动攻击。就算客户想做手脚，追查亦较方便。因为PSTN对所有终端均按E.164码号规则赋予全球惟一的公开编号。此外，当PSTN提供IP网接入服务时，PSTN仅作为IP网的链路层接入，IP数据只是在PSTN上透传，故无法在PSTN接入IP之际从IP网攻击PSTN。由此可以看出，PSTN的网络与终端安全性较好，而其丧失的则是灵活有效的宽带多业务增值能力。

ATM虽然同属分组型技术，但ATM并无直接的终端业务与用户。对用户而言，只是提供一个逻辑“专网”。用户只能在自己的“专网”中运作，无能力亦无可能发送ATM网络可识别或要识别的信令与业务数据。同样，ATM的UNI与NNI是分离的，网络只是为用户提供透传功能，其信令、业务数据等对用户而言是不可见的，用户无法产生恶意数据对ATM进行攻击。相应地，ATM网络与网络间的安全性则是靠运营规则与运营商间的信任关系和协同合作予以保证。而且，由于用户只能在自己所在的网络中运作，即便能发动攻击，亦只能攻击自己网络内的有限用户，故很容易追查。因此，ATM网络虽有较好的安全性保证，但却带来了宽带多业务增值的不灵活、不方便与不经济等缺点。

IP网络如同信息的明信片传送，没有UNI与NNI的分离问题，运营商设备、协议乃至网络拓朴对用户均是开放可见的。用户端产生的IP信息，无论在用户端或在网络中均可传送。通过用户端与运营商网络交换非法的恶意路由信息，即可对运营商网络的路由器、接入服务器等设备及三层以上设备实施攻击。与此同时，位于IP网络边际的用户侧的网络与业务/应用，一般均使用TCP/UDP/IP这一基础技术。这导致用户间在IP层及应用层等各层面彼此透明可见，从而为恶意用户攻击对

方网络及相应的业务/应用大开了方便之门。IP网络的终端高度智能化及多业务能力，使终端用户发动攻击变得容易，又增加了识别与防范各类花样繁多的安全攻击的难度。由于多种业务综合承载在同一网络上，难以分辩与确定用户间的信任关系，导致恶意用户很容易找准对象，发动攻击。而被攻击的用户实际上难以分清哪些是合法用户的正常访问，哪些是非法用户侵入或恶意攻击。

鉴于IP网络及技术发展快速，在协议设计及软件开发中难以避免的缺陷与漏洞在大规模应用之前来不及测试，故难于发现并将其彻底排除，这亦给恶意攻击造成了各种可乘之机。此外，IP用户身份难以识别，导致很难跟踪及遏止攻击者。而且，IP高度智能的终端及其宽带化，加上其有利的计费模式，更有利于恶意用户方便且低成本地有效实施大规模攻击。制造这类攻击的技术难度变得愈来愈容易，从而使得这类非法入侵及恶意攻击有增无减，肆意蔓延，防不胜防，令人担忧。当然，IP协议的开放透明性所导致的安全性弊端，亦带来了其灵活有效的宽带多业务增值能力，便于互联互通及有效降低成本等明显的市场应用优势与吸引力。

目前，黑客、病毒似乎愈杀愈烈，泛滥成灾，已成为安全计算及IP网络安全运作的头等隐患。例如，2004年新病毒增加了52%。瑞星报告指出，其中有十大病毒对用户造成的破坏最大：网络天空(Worm.Netsky，占总病毒数的39.9%)、爱情后门(Worm.Lovgate，21.3%)、SCO炸弹(Worm.Novarg，7.7%)、小邮差(Worm.Mimail，1.5%)、垃圾桶(Worm.Lentin.M，0.9%)、恶鹰(Worm.BBeagle，0.8%)，求职信(Worm.Klez，0.5%)、高波(Worm.Agobot.3，0.5%)、震荡波(Worm.Sasser，0.4%)及瑞波(Backdoor.Rbot，0.4%)。而且，黑客和病毒威胁呈现四大发展趋势：变种病毒数量翻番剧增，防不胜防。从漏洞被发现到攻击病毒出现的时间间隔越来越短，国产型木马病毒及后门程序成为主流，目标直指网民真实财产以及“网络钓鱼”(Phishing)形式的诈骗病毒活动明显增加等。显然，在这十大病毒中，有九种为蠕虫病毒。就对用户的危害性而言，蠕虫病毒依然是最为严重的。病毒变种之所以快速增长蔓延，一个重要原因是很多病毒源代码借助于网络被病毒作者公开并提供下载，甚至有些代码还包括完整的说明文档及相应工具和示例，易于普及传播，毋需特别技能，仅需修改配置文件和部分源代码便可编译生成一个新的变种病毒。这是对公开性(包括源代码公开在内)造成的负面影响的一种直接讽刺，亦说明如何正确认识与控制一种事物的正反两个方面是何等重要。

由这些分析可充分看出IP网络安全问题的本质之所在。就象SARS情况一样，只有控制其病源，才能控制其蔓延。因此，寻找IP网络的有效安全对策，尤为紧要。

其实，IP和Internet研究的权威机构——IETF，对现有Internet及IP协议的缺陷与不足亦有足够的认识，列举出Internet下一步发展面临的十大技术问题：身份识别技术、保护IPR技术、保护个人隐私技术、新一代Internet通信协议IPv6技术、下一代Internet结构的网格(Grid)技术、无线Internet技术、传统电话网与Internet融合的技术、更有效地在网上传输的视频技术、防止垃圾邮件的过滤技术及网络安全技术。如果无法在网络安全、个人隐私及IPR保护方面取得突破，Internet将无法成为一种真正可信的商业工具。当然，IETF相信，在采取一系列有效措施后，如改进IP协议，改进TCP/UDP协议，缩短路由及传输时延，提高传输效率及质量，实施有效的全球大容量移动扩展，访问与漫游，提高网络安全性及改进网络管理能力等，新的IP网是能够担当起NGN重任的。而此十大技术问题中有一半以上与安全性有关，可见IP安全性的实际严重性。可以说，IP问题的最大难点是其安全性，其次是IP QoS。

2.IP发展的战略思考

(1)解决IP及NGN发展问题的总体策略思考

无论是IP(包括“后IP”创新)还是NGN的发展，不定因素与风险很多，仍应遵循“积极、稳妥、科学、求实”这一总方针行事。任何“过热”炒作，“过冷”悲观均不适当。既要尽可能避免“泡沫”的发生，又应博采众长，大胆努力创新。

有关“泡沫”问题，应辩证思维，盲目“跟风”应绝对避免。至于所谓泡沫，往往与不科学、不切实际及不务实有关，应尽量根据科学求实的原则，避免“泡沫”的产生。但有些“泡沫”的产生是有其前因后果的，生成原因极为复杂。一方面，要分析其原因并充分汲取教训，尽量避免泡沫的发生。但另一方面，应尽快将消极因素转化为积极因素，创造新的现实价值和长期价值。“.Com”高科技泡沫就是一个典型实例。其实，IP及Internet本身就是一个具有长期潜价值的令全球瞩目的伟大创新。尽管人们往往有“一朝被蛇咬，十年怕井绳”的心理，但对IP及NGN的发展，不能因为害怕“泡沫”的可能发生而影响积极创新与推进。对此，2002年诺贝尔经济学奖得主弗农史密斯(Vernon Smith)有一句名言，即“每个泡沫都因伟大的技术创新而引起，这些技术为人类创造了大量的长期价值”。笔者以为，在推进IP及NGN发展时，应从V.Smith的名言中吸取一定营养，尽量避免“泡沫”的发生。新技术、新系统及新事物的发展多多少少均遵循描述可行性与成熟性关系的所谓超级循环(HyPer Cycle)曲线，亦是类似的道理。

(2)IP安全性发展战略思考

如上所述，TINA/TIMNA提出的有关IP安全失控的结构缺陷的论述是有道理的。IP包结构兼含“内容”加“地址”(源地址及目的地址)，在网内传送时，来龙去脉清楚，自我暴露性强。借助地址引导，有利于黑客通过“地址过滤”技术按选定地址窃取网上信息及实施攻击。于是，提出了以“中间件”层的ICA结构解决这一难题的方案。尽管其具体操作方法尚需探讨，但指明其“中间件”层的突出作用是正确的。在目前推进以IP为基础的NGN的发展过程中，不只是应用层面，对安全性，IP-QoS，智能网管等目标，均应在多维层面大量发挥各类“中间件”的重要作用。从战略观点看，在推进NGN的发展过程中，应鼓励创新，集思广益，博采众长。提出“未来网技术IP不是惟一的选择”说法，应该说没有坏处，只有好处。目前之所以强调，在IP基础上下功夫，首先是基于其在全球大规模普及的基础与事实，并具备多业务增值的基本吸引力。更重要的是，目前尚未找到或比较一致地认同比IP协议更适合操作的其它途径。

事实上，全球为IP的安全性已花费大量人力、物力和财力，而且取得了不少进展与成绩。从解决安全性的源头角度考虑，一般认为终端是要害。对终端应用，其中包括OMA及NGOSS而言，已充分注意到中间件及CORBA(公共对象请求代理体系结构)软总线技术，并发挥了重要作用。但“中间件”的含义与定义有一定松散性、广泛性与含混性，需进一步严格规范定义与改进协调，否则将可能严重影响实际应用的互联互通等多厂商环境下的互操作性。

信息安全有更广义的内涵，营造一个防止黄色不良信息危害青少年身心健康的安全信息环境，规则/政策监管与技术措施双管齐下才能奏效。信息对策的“老三样”——“堵漏洞、筑高墙、防外攻”等属于消极防御措施，尤其当它们单独实施时，已愈来愈不能凑效。为此，一方面要想出更积极的对抗措施，包括对其源头跟踪堵截；另一方面，即使对单个用户而言，也需要防黑防毒，修复漏洞，拯救数据。这些措施应融为一体，形成综合对抗能力更强的整体安全系统，转被动/消极防御为主动/积极防御。应注意，解决安全性问题是需要付出代价的。信息安全对策应根据用户不同安全类别的实际要求提供不同的解决方案。如果用户只需要BE类业务，则应提供简单、经济、实惠的解决方案。

目前，有关IP安全性对策方面的重要进展值得一提。一是信息产业部正在制订“互联网IP地址管理办法”及建立“ICP/IP地址信息备案管理系统”。这对查处有害信息的快速定位、搜索非法网站及有效提高信息查询与安全性管理效率有重大意义。二是认定终端为安全重点及中间件的隔离作用是非常重要的。在终端芯片嵌入密码型安全子系统，对全部自主研发场合来说很容易处理，即以一个独立于每个系统的平台作为中间件，分别与系统及应用程序连接，以解决应用程序对系统层的访问及控制。当然，此时依然要解决好系统层接口的安全性问题，而这往往是个难题。三是为确保高级保密用户的安全，采取网络彻底隔离断开。在保证安全前提下，支持自动文件和应用数据的交换，这就是所谓网闸(GAP)的概念。众所周知，内/外网是采取物理隔离断开方式，人工文件可安全复制转移，这是手动实施的一种最简单原型。显然，如何实

施网络断开以进行有效的文件交换，特别是各种应用数据的交换，是网闸技术的关键所在。总体来看，网闸技术包含三大要素，即网络隔离断开、模拟拷盘或单向传输工作机制及应用数据交换支持。由于网络断开即可消除黑客对网闸本身的入侵，使其无法从网闸外部主机侵入到内部主机，也不会从外网侵入内网，从而消除了基于通信连接的攻击和基于TCP/IP协议的攻击及漏洞扫描和入侵攻击。至于网闸对应用的支持，通常是通过对应用协议的剥离来获得应用数据。交换应用数据后，再对应用协议进行重建恢复。目前的网闸技术已可对大部分应用数据进行剥离与重建。当然，这些运作均要以资源消耗、高速运作及硬件补偿等为代价。三是国内两大防毒软件商——北京瑞星科技股份有限公司和北京金山软件有限公司宣布，正式加入思科公司所倡导的网络准入控制(NAC)计划，以研发集成化的安全解决方案，全面提高安全级别和防御威胁的能力。这是国内信息安全知名企业与国际领先技术有机合作与良性互动的新契机，将对中国信息安全事业起到巨大的推动和促进作用。NAC合作计划最早由思科公司于2003年11月提出，其主旨是授权合作伙伴公开技术信息，以支持合作伙伴开发和销售支持NAC网络基础设施的第三方服务器及客户端应用。NAC计划分三步实施。第一步，在2004年中期，思科的接入路由器和中档路由器已可支持NAC计划。第二步，NAC将扩展至多种思科产品，如交换机、无线接入设备和安全设备。第三步，将PC和服务器端点与网络的安全互操作能力扩展上升为自我防御能力。显然，专业信息安全厂商与硬件设备提供商进行深层次技术合作，既是企业用户的普遍安全需求，也是整个信息安全行业的重要发展趋势。思科、瑞星、金山等联手打造全局防御的信息网络安全体系，既有明显的现实价值，亦有重要的战略意义。

总起来说，IP安全性的进展实际上与上述ICA思想的安全保证是有所协同与汇聚的，比起防火墙等措施来已更上一层楼。因此，基于IP协议的安全计算问题应以科学求实、积极创新的原则而努力推进，决不能不求创新，甚至悲观失望。

(3)IPv6发展的冷思维

随着中国下一代互联网示范工程CGNI的启动及中国五大运营商全面加入IPv6规模部署阵营，并拟在2005年底建成世界上最大规模的IPv6网络，起到引领全球IPv6推广与应用的作用，IPv6热正在中国快速升温。诚如全球IPv6论坛主席Ladif Ladid所说：“中国需要IPv6，IPv6更需要中国”。由此亦不难理解，IPv6为何在国内日渐升温，有些人甚至认为NGN就是IPv6，IPv6一上，NGN的所有问题基本上就都可以解决了!这种不适当的升温不利于IPv6在中国稳妥、健康的发展，并有碍中国引领全球IPv6的推广应用、成为真正IPv6大赢家这一宏伟目标的实现。因而，对IPv6进行理性思维，甚至冷思维，看来很有必要。

首先，应充分理解IPv6对IP协议的重大改进与战略价值。IPv6协议已约有十年历史。其在地址容量、安全性，QoS控制、地址资源管理的合理性方面均有较大幅度改进，包括对新一代全球移动业务的支持。尽管如此，亦不能说明它已十全十美，可全盘包揽、永世长存。从IPv4至IPv6的不兼容性即可看出其阶段性设计的局限性与巨大弊端。其实，应该说，地址匮乏是ICT业界对IPv6研究与建设应用的最主要驱动力，对其它一些功能不应寄以过份的期待，更不应不切实际地炒作与夸大。赋予IPv6太多的期望，将导致IPv6走向反面，甚至重蹈3G由神话向理性转变的覆辙。

由以下几方面对IPv6在中国的发展进行冷思维是有益的：

●安全性问题。IPv6在其协议栈中强制执行IPSec，确比IPv4时的安全性有所改善。但安全性问题很复杂，需有不同层次、不同方位的可靠保障。首先，IPSec仅是一个网络层协议，负责其下层的网络安全，并不负责其上层应用，如Web，E-mail及文件传送之类的安全。对确保安全而言，IPSec决非惟一手段，还需与多种手段，诸如认证体系、加密体系、密钥分发体系等全面配合。

●QoS问题。如上所述，IPv6 QoS改进的一个重要手段是“流标签”。但已有十年历史的IPv6至今还未制定出流标签应用的有关标准，一些基于流转发的产品仅是基于厂家特定环境的产品，并非基于流标签协议，从而大大限制了它的推广与

应用。何况，IP-QoS问题与IP安全性问题类似，涉及QoS的体系结构。因此，首先要完善低层承载层面的综合有效的IP-QoS实施途径，其次要解决高层与低层间的快速控制运作，实现包括低层运作在内的业务、应用等高层层面改进IP-QoS潜在作用的高层智能路由/交换能力，使得纵向、横向各层面能有效运作，最大限度地调动网络资源，才能实现愈来愈令人满意的IP-QoS保证。

●IPv6的所谓移动通信杀手锏应用问题。确实，MIPv6对3G及3G演进等新一代移动通信应用可提供有力支撑，不过IPv6在新一代移动通信终端上的有效应用还有很长的路要走。目前的PDA手机，内置仅为IPv4协议栈，并不支持其移动特性，而借助GRPS，CDMA 1x上网的手机使用的均为专网地址。从后向兼容演进角度看，期望IPv6成为3G的杀手锏应用决非轻而易举之事。

●IPv6的应用奇迹问题。应该说，IPv6利用其海量地址优势发挥其端到端个性化/个体化及大面积消费电子类应用确有其巨大威力与潜力，但也必须应对诸多难题。首当其冲的依然是安全性问题。防火墙入口认证模式及保险柜式连接对象认证模式均不能令人满意，产品内嵌安全功能亦相当困难，如何有效交换密钥亦非易事。因此，探索价廉物美而有效的IPv6安全应用途径，依然面临严峻的挑战。

●IPv6的实际部署问题。目前，全球已拥有2亿多IPv4用户。IPv4与IPv6的非无缝兼容特征将成为其业务快速有效演进的障碍与阻力，并意味着在时间、金钱、资源方面的巨大投入。而且，大有作为的第三方应用软件的编译亦很少在目标操作系统的最新版本上实施。因此，对IPv6的装备实施不宜持过份乐观的期望。

●中国IPv4/IPv6地址资源匮乏的严重性

如上所说，IPv6的地址数是如此巨大，约为IPv4地址量的8万兆兆平方倍。有人甚至声称它可赋予地球上每一颗沙子及每一滴水以相应的地址。即便如此，包括GNI及NGXiYiJi在内的NGN与GII是瞄准全球个人化、个性化及个体化目标的，而后两者的需求与数量将远远超越直接意义上的全球“个人”数量，哪怕是只要覆盖最重要的那些“沙子”与那些“水滴”，IPv6地址能力的真正充裕性便值得怀疑，更何况遍及每一颗沙子及每一滴水!说穿了，在IPv4地址分配上吃了大亏的中国人，最关心的是中国应该且必须及时拿到中国应该得到的IPv6或将来更长远IPvX地址资源。“兵马未发，粮草先行”，这是千古常理。发展3G/3.5G/4G之类3G演进与宽带无线，首先要解决的是全球与中国自身需求的频率/轨道/码号资源，同样发展好中国的GNI及NGXiYiJi在内的NGN必须首先解决好中国的IPvX地址资源。目前，绝不应对IPv6地址总量感到盲目乐观，而应切实思考如何解决好我国IPv4/IPv6地址资源匮乏的严重问题。

IPv4地址分配极不合理，其分布极不均衡。美国3亿人口，1.65亿互联网用户，拥有75个A类地址，占全球IP地址的70%。中国13亿人口，互联网用户数约达9000万户，估计到2007年将达3亿户，却仅拥有4100万IPv4地址，相当于不到3个A类地址，仅相当于美国IPv4地址数的1/38。拿足了地址者留着不用，而急需地址者又一筹莫展，可见地址分配达到了何等惊人的不公平、不合理地步，地址的管理是何等地令人遗憾与可悲。在这一点上，中国目前及未来几年内很可能依然大吃苦头。因为全球IPv6论坛于2004年3月公布的预测资料表明，对IP地址需求最多的15个国家即需附加298个A类地址，超过目前剩余IPv4地址库地址量的3倍。其中，仅中国一国即需附加105个A类地址，约占其1/3强。依然在先到先占和按需分配原则指导下的IPv6地址资源争夺大战的序幕已经拉开，而中国在此第一回合中已处于很不利的地位。截止到2004年6月，我国分配到的IPv6地址块仅为11块，占全部已分地址块(606块)的1.8%，且均为/32类别的缺省型，未得到任何更大的IPv6地址块，捷足先登的一些国家仍占大头。例如，至2003年底，美国、日本、德国、荷兰、英国等五个国家所分配到的IPv6地址占全球总数的48%。在亚太地区，我国分到的IPv6地址仅占11%，约为韩国的1/2.5、日本的1/6，比中国的台湾省(14%)还少。何况在新一轮IPv6地址争夺战中，美国国防部DoD不仅针对今后两年的需求在积极申请获取/16类别的巨大IPv6地址块，甚至已对其10年以内地址需求作出了规划申请。因此，在缺乏IP地址前提下，奢谈什么“中国需要IPv6，IPv6更需要

中国”以及希望“中国引领全球IPv6推广应用，成为真正IPv6大赢家”之类口号实在没有意义。尽快从NGN-I，NGXiYiZi及NGN发展总目标入手，通信、计算机、广播电视、教育科研、商务政务、国防军事、企业家庭、网格运行、个体物流，制造运营等，全面考虑，联手规划，申请获得应有的IPv6地址已成我国当务之急。在IPv6地址的新一轮资源争夺大战中，力争取得好战绩，才是确保IPv6及NGN务实发展所需资源的前提。同时，应积极响应ITU-T对IPv6地址分配的有益战略观点，摒弃“杞人忧天、犯不上着急，IPv6地址取之不尽，眼下没有必要去争抢”之类的短视想法，力促从分配机制上进行改革，使IPv6地址的分配不致重蹈IPv4地址分配的覆辙，使之向更合理、更健康的分配轨道发展。事实上，IPv6地址分配工作本身，确有不少有待改进之处。从上述第一轮分配结果可以看出，先入为主、先到先满足的原则对后来者有失公允。发达国家和一些占风气之先的国家抢占地址的现象依然普遍，现在的游戏规则实质上沿用了IPv4的套路，很难做到公平合理，这些都是亟待解决的问题。在国际上建立一种权威的公平合理的IPv6地址分配管理机制是国际社会努力的目标，也是当务之急。

五、结束语

应该承认，IP协议及Internet是人类全球通信的最伟大创举之一，它创造了无可估量的长期价值。同时，鉴于TCP/IP协议及Internet的发展历史与背景，随着其商用化暴露出的一系列问题，诸如安全性，IP-QoS，智能网管、可赢利商业模式等必须切实重视，并科学务实、博采众长、积极创新、脚踏实地、一步一步地予以解决，包括战略上引入更优秀的结构理念与系统解决方案在内。本文以IP安全性为重点，对IP协议的重要现实作用、存在问题及其进一步发展策略，提出了一些战略思考，期望IP/NGN获得积极、稳妥、健康、有序的可持续成功发展。
