

得“新”应手：构建和谐的互联网

— 浅析 DPI 技术和应用

北京畅讯信通科技有限公司

2008 年 2 月 24 日

“互联网”已为家喻户晓，而且不仅是当代高科技的产物也不可或缺地成为社会发展的动力和经济变革的杠杆。什么是互联网？我们不妨参考美国国家计算、信息和通讯科技顾问委员会（CCIC）下属的联邦网络通信顾问理事会（FNC）在 1995 年 10 月 24 日公布的关于定义互联网的决议（http://www.nitrd.gov/fnc/Internet_res.html）：

“互联网”指的是全球性的信息系统：

- 1、通过全球性的唯一的地址逻辑地链接在一起。这个地址是建立在‘互联网协议’（IP）或今后其它协议基础之上的。*
- 2、可以通过‘传输控制协议’和‘互联网协议’（TCP/IP），或者今后其它接替的协议或与‘互联网协议’（IP）兼容的协议来进行通信。*
- 3、可以让公共用户或者私人用户得到层次化和高水平的服务，这种服务是建立在上述通信及相关的基础设施之上的。*

这个定义看似物理的（或网络技术性的），但至少揭示了三个方面的基本内容：首先，互联网是全球性的；其次，互联网是由物理网络和网络协议支撑的；最后，互联网用户和应用所得到相应的服务来自于开放和完备的环境保障。

时至今日，这个定义也许不得不做点补充。从应用的角度，互联网是个能够相互交流，相互沟通，相互参与的互动平台，也正是因为成为“风云人物”的互联网用户和创意者们彻底改变了互联网发展的轨迹，使得互联网的应用从单调型的“一统天下”到自主式的“百花齐放”，迫使传统的工业和产业在新的服务需求下面临转型和重构的挑战压力。换言之，“厅堂”里定义的标准和“厨房”里开发的应用在互联网的持续发展中互补和共

存已成为不可逆转的潮流和趋势。因此，在广义上我们或许可以这样补充修正互联网的定义：

作为全球性的信息系统，互联网在逻辑上是由两个平台组成，即应用互动平台虚拟地叠加在物理传输平台上。其中，“虚拟”指的是在应用互动平台上的每个用户都可以认为公平地拥有随时获取信息和与他人交互的通讯通道而无需关注通道是如何建立的；“物理”指的是网络的基础设施和管理。

即使如此，FNC对“互联网”的定义仍不失为互联网发展的基石。

另一方面，随着借助于各种自主自发（非标准）的交互工具（如P2P）的使用，网络流媒体成为互联网应用的主流，从而导致对网络的带宽需求大幅度增加，体现在网络上传输流量与日俱增。同时，由于直觉的用户体验（QoE）逐渐成为衡量抽象的服务品质（QoS）尺度，也使得应用和服务难以调合的矛盾日益突出，其中一个直接负效应结果是动摇了互联网发展的基石和环境。

不可避免的是，互联网的服务基本停滞在原始水平（技术上，40年前诞生的TCP/IP协议以及不断扩展的外围辅助兼容协议并不具备对网络应用的管理能力），事实证明没有管理的简单网络基础设施扩容不仅远不能满足互联网应用的快速增长而且扩容投资也无法得到相应的回报。作为一个例子，美国最大的有线电视运营商Comcast对网络实施新的应用管理，并在日前向美国联邦通讯委员会（FCC）提交的报告中强调：

“尽管对网络容量不断进行升级和投入，但事实是网络容量不会一而且是永远不会无限扩大”。因此，“没有一定的、负责任的管理，所有用户的体验都将恶化到让人无法接受的地步”。结论是“简而言之，没有管理，网络就没有‘中性’可言。”

事实上，通信网络（互联网）的流量管理与电力网络、交通网络、民航票务管理是建立在相同的理论基础、模型和应用目标上，例如：

- 电力网络在用电高峰期实施对部分区域或用户拉闸限电；从每个用户或家庭到各级电力传输变压器所安装的保险丝限制了各种使用负荷的上限。
- 交通网络的定时信号灯管制；不同地段的车速限制；交叉路段的停车（Stop）和礼让（Yield）规则。
- 民航票务的超强比（Overbooking）售票；头等舱和公务舱旅客的优先绿色通道。

诸如这些管理的技术、措施、规则、策略等都是为了保障一个安全有序的环境以在有限的基础设施能力上最大限度提高服务的质量和被服务者的体验。不失一般性，管理完完全全与“服务”有关，而与“控制”无关，限制仅仅是管理的一种手段但绝不是封堵。毫无疑问，只有在有序的环境里才有可能构建和谐，任何通信网络也不例外。

畅讯科技从 2001 年开始对网络流量进行研究和分析，在算法、集成电路设计和系统设备上持续研发。2005 年在国内市场率先推出基于 DPI（深度包检测）技术的高性能电信级产品 QQSG，在应用开拓中 QQSG 得到完善并形成产品的系列化和相关配套解决方案和技术服务平台。根据我们的认识和理解，本文对 DPI 的技术和应用抒一管之见。

1、DPI 技术的一般表述

DPI（Deep Packet Inspection）是一种技术用来实现识别数据包内容的工具。必须明确的是，这里所指的“数据包内容”并不是用户交互的内容数据信息，而是指封装传送用户内容数据信息的第 2 层到第 7 层的协议信息（即 OSI 的 7 层网络结构）。传统的网络设备基本上都是基于标准的网络协议在技术和工程上实现不同层次的功能（如 2/3 层交换机，3 层路由器，4 层防火墙），在第 4 层以上的应用协议是层次化地被封装在网络协议（TCP/IP）内，而传统的网络传输设备遵循着“尽力而为：Best Effort”的原则既无必要也无法知道所处理的交换或路由的网络数据流里是由那些应用（协议）组成。DPI 填补了这一技术空白，并且在与其它技术组合后实现从对网络流的粗旷型管理到对应用和用户颗粒化（Granularity）的精细管理之补充或转变以及对进一步应用服务需求的必要扩展。

2、DPI 技术应用的必要性

“按需服务：service-on-demand 或 bandwidth-on-demand”曾经在过去的网络基础设施规划和网络流量管理（Traffic Management）中就一直是个优化目标，不尽如人意的主要障碍包括缺少支配性的市场应用驱动力和服务的增长点以及相关实现的技术手段和能力。从 2005 年开始 P2P（peer-to-peer）工具在国内互联网上呈爆炸性的应用，问题首先引起 2 级运营商（或驻地运营商、接入运营商）的关注和重视并开始部署基于 DPI 技术的网络设备，主要目的是为了缓解 P2P 应用占用了高达 90% 所租赁的有限出口带宽而对运营服务和运营成本造成的巨大压力。

P2P 从其技术体系结构上应该说是一个开创性的成功应用，从文件共享下载和上传到 VoIP 无疑颠覆了某些传统的技术应用。但是在应用的背后存在鲜为人知或易于被忽略对网络安全（注：关于网络安全在下一节讨论）的巨大的杀伤力和为此要付出的高昂代价，主要表现在：

- 带宽 – P2P 的有效应用基础是“对等性”，共享使得参与 P2P 的用户既是内容使用者（下载：Client）也是内容提供者（上

传：Server），所不同的是 P2P 的用户们往往可能是在不知情的状态下不自觉地成为了内容提供者（未必是同一下载内容）。由于 P2P 的用户是动态和随机地构成交互连接，P2P 的机制要保证下载和上传的完整性和一致性就必须连续不断地发出请求搜索和发现新的用户或新的内容源。同时，由于 P2P 的下载可以是在后台批处理运行（无需人机交互），在这种 P2P 多用户集中大并发情况下，传输网络的带宽会被很快占用殆尽而造成堵塞或网速降低。

- 对话 – 又称链接或 **Session** 是 TCP 协议的属性。不仅 P2P 应用而且目前大多数音视频服务站点在建立一个点到点的交互连接后隐含着十数个乃至数十个并发对话（**Concurrent Sessions**）。在千兆带宽中存在数百万个并发对话是目前网络中常见的（在传统的网络和网络标准应用中并不会出现这样大量并发对话），对网络安全所带来的直接冲击所导致的结果或现象是导致一类拒绝服务（**DOS-like**）而并非完全由于传输带宽的因素（换言之，网络流量由两维信息量所组成：传输用户信息所需的带宽，和用户交互连接所需的对话数/带宽。本文以下所涉及的“网络流量”都是在这个定义上）：

- ❖ 现有典型高档服务器处理并发对话数的最大能力一般在 2000-3000 个，饱和时服务器整体性能会急剧下降。
- ❖ 并发对话的传输一般是以 64 字节（Bytes）短信息包为主，现有的网络设备（如路由器）在处理大量并发短信息包时性能（即吞吐量、丢包率、延时、抖动）会大大下降。

通过 DPI 技术和以及相应的网络产品和解决方案对 P2P 应用的管理能避免网络的基础设施资源被无序的滥用，也使 P2P 应用得以健康发展，进而保证对互联网绝大多数用户的服务。尽管如此，DPI 技术的应用决不仅仅是在网络流量管理上，事实证明 DPI 技术在网络安全、服务整合和管理等方面也有显著功效，其应用领域也随之增加。此外，需要 DPI 技术的已经不仅仅是有线电信运营商了。速度更快、日益普及的移动网络数据服务提供商对 DPI 技术越来越感兴趣。因为如果他们不能对网络流量进行有效管理以保持盈利的模式，无疑也会重蹈覆辙。美国“泛读：Lightreading Insider”在她公开发表的一个市场权威调查分析报告中指出：

“如今全球都在投资 DPI。随着网络运营商不断升级网络，使用消耗大量带宽应用（如网络视频服务）的用户越来越多，对 DPI 的需求也会随之扩大。因此未来几年，DPI 技术以及 DPI 应用将会飞速发展。”

3、DPI 技术应用的充分性

在实际应用中，“网络安全”往往多为涉及防火墙、防病毒、防攻击、防垃圾邮件等。从网络运营的角度，网络安全更多的是关注基础设施的可靠性（Reliability）、稳定性（Stability）以保证相应的服务能够可推送（Deliverability）和可使用（Availability）。客观地说，如果网络的运营安全没有保障，网络的应用安全也就无从谈起了。

感谢国际标准化组织、网络运营商、设备制造商的共同多年努力，网络的基础设施的使用和运营对于标准化的网络应用已是相当成熟和完善的。如果今天互联网的应用仍然是基于标准的（如 TELNET, FTP, HTTP, SNMP），网络的运营安全应该是有保障的。但是这个假设不成立，而且可能永远不会成立，因为驱动互联网发展的应用不再仅仅是标准化的。上述 P2P 应用只是一个范例，但可见它所造成的影响已足以动摇网络基础设施可靠性和稳定性的根基；同时没有相应管理能力的服务也只是形同虚设，最终不仅殃及池鱼的是最终用户而且运营商自身也深受其害。

基于 DPI 技术的电信级网络设备可以透明地串接在网络中的任何一个节点，实时地提供网络的运营安全的规范支持，如同电力网中的保险丝和交通网中的信号灯；同时在线地提供各种运营服务策略执行的支持，如同民航票务系统中的服务绿色通道；进一步地通过统计分析为网络基础设施的规划和决策以及提高服务能力和水准提供定量的参考依据。

另一方面，DPI 技术也是对现有网络应用安全技术的补充。作为一个例子，目前穿透标准防火墙是已知绝大部分互联网应用所必须具备的缺省功能。DPI 技术与其它技术组合可有效地具备识别和过滤能力，实现与防火墙在网络应用安全保障的互补。

4、DPI 技术应用的约束

综上所述，DPI 技术的发展动力和主要应用目标是互联网上各种非标准的应用。尽管 DPI 技术可以有不同的实现方法，但是存在不可逾越的约束：

- 标准与非标准的网络应用本质上的区别主要在于前者是通用型的而后者是地区或地域型的（包括如文化背景，政策法规等影响因素），同时非标准的网络应用发展速度可谓日新月异。因此，不可能有一种如同交换机或路由器的通用型基于 DPI 技术的设备，既能满足“西”又能适应“东”。事实上，某些知名品牌的 DPI 设备在国内市场上难以应付被称为“水土不服”的问题。如果研

发和市场不能持续地紧密结合，DPI 技术对使用者和开发者都不会产生实际和真正的价值，而且可能会成为包袱或负担。

- 基于 DPI 技术的网络设备与传统网络设备的主要本质区别在于前者必须具备可编程以及周期性的升级和扩展的能力，同样这是由于非标准的市场应用环境所决定的；后者是网络基础设施的组成之一，并不可能轻易变更（包括各种配置）。在现实中，往往大多数网络设备直到被淘汰都保留着原始的状况。这个特性决定了 DPI 技术“一站式集成：All-in-One”在应用环境缺乏实际意义。这并不是一个技术问题，有个形象地表述：一个手里握了三个球投出去，结果一个目标都不可能击中。不仅如此，还有可能导致不可预测的灾难性结果，在网络通信史上有不少切肤之痛的教训可引以为鉴。
- 网络应用以及相应的网络流量的一个特点是高速和具有动态、随机的时效性。不管是粗旷型的传统流量管理还是基于 DPI 技术的精细化流量管理，如果不能做出实时地反应无疑将会是事倍功半（甚至可能“弄巧成拙”）。这是以软件型的或离线型实现 DPI 技术的方案所无法跨越的一个“门槛”或存在的“制肘”。

5、归纳

DPI 技术是在互联网快速发展的新环境中应运而生并正在得到广泛的应用。DPI 技术同时也是一个概念，实现可实用的设备和方案是需要与其他技术有机结合的一个系统工程。DPI 技术的真正价值在于由市场（或用户）需求导向下不断地提供新的、精而细的功能和可定向的技术服务和支持。

运用 DPI 技术实现网络运营的精细化管理不是控制更不是封堵，而是从网络安全的角度优化网络资源和网络服务，提高网络的使用率，保障网络应用的有序和谐，推动互联网良性发展。

DPI 技术具有通用性，但不具备标准性，因为应用的环境确定了研发路线；应用的特点制约了实现方法；应用的目的决定了使用门槛。

广义下的互联网是由“应用互动平台”和“物理传输平台”所组成的全球性信息系统。作为网络基础设施，物理传输平台支撑着应用互动平台，“皮之不存，毛将焉附”的关系是显而易见的。因此，网络的精细化管理是个“纲”，纲举目张。