广州网纵信息技术有限公司

网络优化与管理系统[流控大师]

E 系列产品白皮书

广州网纵信息技术有限公司

Netzone

2013 年 05 月

目录

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

广州网纵信息技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但广州网纵信息技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：广东省广州市天河区天河路 535 号保利中辰广场 A 座 908 室

邮编：510630

电话：020- 85509880

传真：020- 85509883

您可以访问广州网纵网站：www.netzone.com 获得最新技术和产品信息。

1 互联网现状及企业面临的挑战

伴随着中国信息化的普及，互联网的飞速发展及社会的进步给我们的生活带来了巨大的变化，截至2012年12月底，中国网民数量突破6亿。互联网上的应用以及资源从根本上改变了人们生活和工作的方式，人们在工作和生活中对网络的依赖性越来越大，已经成为社会和经济发展的重要推动力和取得经济发展的重要生产要素。

同时，随着社会经济的不断进步，IT产业已渐渐走进人们生活，信息化管理已经成为单位、企业管理的主流趋势，这个趋势是不可扭转的。而且，现在很多企业都以实现信息化管理为荣。各单位也都投入大量资金建成了内部网和互联网。由于缺乏有效的网络流量分析和管理控制手段，网络的发展正面临诸多问题和挑战，由此引发了一系列安全、效率和法律问题。

1.1 网络带宽质量给企业发展带来压力

随着社会的发展，也加快了企业信息化的进程，企业在通过信息化提高工作效率的同时，也为员工提供了自由使用互联网的条件。在网络在单位、企业中的应用，是为了办公的需要和技术的进步，但是很多员工会在办公时间内浏览与工作无关的网站、进行IM/P2P软件使用、流媒体观看或玩游戏、以及其它非工作用途的计算机应用，如娱乐、新闻、IM聊天、游戏、P2P……只要员工有兴趣，他们就能在上班时间尽情享受互联网带来的乐趣。而且，现在的应用软件，为了让用户有畅通无阻和更快速的体验，能争抢带宽就尽量争抢，能逃避监管就尽量逃避。再加上很多使用随机端口，让传统的基于端口来区分应用的管控方式失去了作用。大量应用对带宽的无秩序、无节制的抢占，给所有网络管理者带来了无法回避的巨大压力。这种压力对企业来说已愈发严酷，主要表现在如下几点：

- 网络带宽不断扩容，但是网速问题依然无法解决，新增的带宽不久就被无关的应用占满；同时，即时目前单位、企业出口带宽可以满足需要，也无法说明投入的网络资源是合理的；
- OA、ERP、CRM、SCM等关键业务逐步的部署与使用，这些耗费了企业大

把财力物力同时能给单位、企业带来良好回报的系统却要和诸如P2P、网络电视、网络游戏等无关应用去争夺有限的互联网出口资源。单位、企业关键业务无法得到有效保障成了令管理者是否头疼的问题；

- 员工会在办公时间内浏览与工作无关的网站、进行IM/P2P软件使用、流媒体观看或玩游戏、以及其它非工作用途的计算机应用，如娱乐、新闻、IM聊天、游戏、P2P等。除了给网络带宽带来压力的同时，网络的滥用会给单位、企业带来成本的增加、效益的流失，甚至引来灾难性的后果。

1.2 缺乏了解内网带宽使用情况的手段

对于内网带宽的管理，无法获知企业内部网络各类应用对带宽占用的相对比率，如P2P流量占用了多大的带宽、网站访问流量占用了多大的带宽、视频会议系统占用了多大的带宽、本月与上个月相比哪些应用占用带宽的增长幅度较大、全网哪些应用占用了较多的带宽资源、哪些用户占用了较多的带宽资源等，这些情况网络管理人员都无从了解，无法为制定具体的带宽分配管理策略提供相应的依据。

- **传统网管理念带来误区**

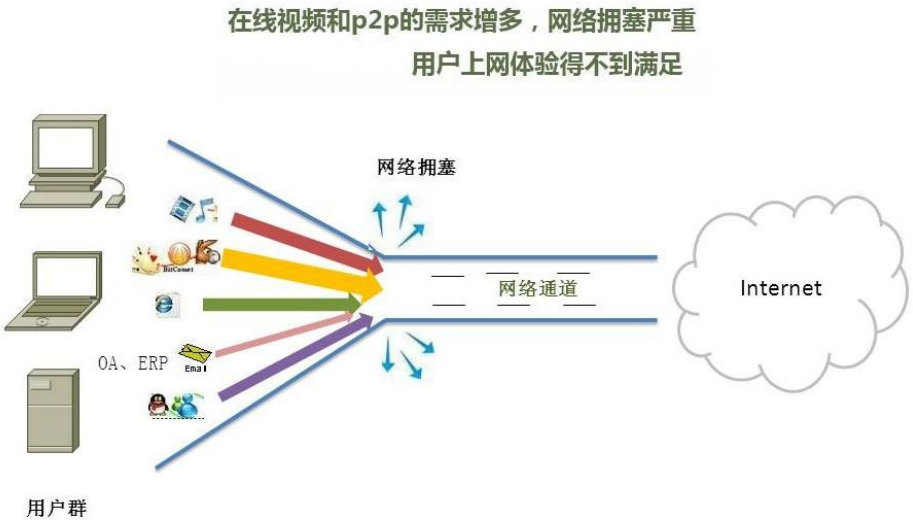
目前，网管人员常对网络管理存在一个误区，通常认为网络管理等于设备管理，而没有从物理层至应用层整体地关注与网络运行的协调性。但网络的管理是不能分散开来看的，网络的计算中心、数据的传输中心、网络的流量信息等各方面元素应该是一个整体，因为网络并不是静态而是在不断发展变化。如果我们过

分强调基于网络的某种服务或者基于网络的某种管理框架，那么很有可能忽视了其发展的根本。在网络中，这些元素是环环相扣的，基础出现了问题，结果很可能是所有服务都出现了问题。

- **网络带宽资源恶性占用现象严重**

不可预知的、突发的性能瓶颈会影响关键应用的运作效率。目前在大部分组织中，用户数量庞大、网络应用环境复杂，各种 P2P 和在线视频应用占用了大量网络带宽(如 FLV、BitTorrent，Kazza，Emule 等)，随之而来的是，由网络链路拥塞引发的应用性能下降问题也日益严重，极大地影响了组织正常业务的开展及用户正常网络应用的服务质量。

- **用户体验得不到满足**



在中国互联网飞速发展的同时 ，P2P 和在线视频应用也迅速普及开来，同时也造成了许多麻烦。据权威部门统计，当前 P2P 与在线视频流量已经占整个互联网流量的约 70%，并且正在以每年 50%的速度增长。在网络中，P2P 与在线视频流量消耗了巨大的网络带宽，提高了网络运营成本，使网络基础设施不堪重负。

P2P 和在线视频流量的暴增，可以通过部署在网络上的流控设备进行有效的控制。但是，普通网络用户的网络使用体验却因此得不到保障。

- **无法有效利用网络资源**

目前大部分管理人员对其网络的带宽使用情况并不了解或无从获知，更不了解他的网络上主要有什么应用在运行，因此也无法采取相应的措施来控制和合理

的使用有限的资源。

当所有的业务应用在网络中进行带宽之争时，由于没有对应用进行优先级的划分，因此非关键型应用总是占据上风。巨大的电子邮件附件或高容量文件传输所消耗的带宽远远超过它们所应享有的，而组织网络中的关键型应用之间又在相互竞争仅有的少量的带宽。最容易的解决方法是不断循环扩大广域网带宽，不断加大广域网资源投资。但是，显然这是一种很大的浪费，不能从根本上解决问题，因为很快扩充的一道路，依旧会被更多的流媒体、网络游戏和 P2P 下载所吞噬。

因此在确保组织正常工作和关键业务的安全、高效运行的同时，如何从根本上解决上述 问题，才能在显著提高企业的生产效率同时保障 IT 投资的回报率（ROI），这是大部分组织目前在网络管理和运维中亟待解决的一大问题。

2 传统的流量管控方案

2.1 传统流控技术

传统的流控产品，大多数手段都是在限制 TCP 并发连接数上做文章。限制 TCP 并发连接数进行流量控制的方法并不科学，很容易影响其他正常流量的通畅，而且，目前很多流量控制类产品所使用的其他技术特点也存在很多问题，如，采取模式匹配的方式，对每个数据包进行模式匹配，并且不考虑数据包之间的逻辑关系，采取这种方式的系统的好处是实现简单，但是它的缺点也是很明显的，就是性能低下，易成为网络的瓶颈。再比如：使用状态识别技术，在现有防火墙技术的状态表的基础上，将连接所产生的所有数据包看作一个整体，如果其中某个或某些数据包符合指定的特征，那么认为这条连接就是符合该特征的连接，需要组装和识别大量的数据包，效率明显偏低。

目前，网管人员一般会直接利用数据链路层、网络层甚至传输层已经比较成熟的技术控制措施来实现性能管理与网络的安全。如 L2 交换机基于 802.1Q 和 VLAN 的控制，对 L3/L4 交换机的访问控制列表进行过滤、通过防火墙进行阻断和控制等等，如下图所示。

在网络应用日新月异的今天，对所有的应用流量一视同仁，无法区分延时敏感性和重要性是 TCP/IP 网络的先天不足之处。大量的软件（包括 P2P、在线视频、即时通讯、网络游戏等等）都具备了跳跃端口、随机端口、自定义端口甚至包伪装等等功能，规避 IT 管理员的管理与控制。这些软件的端口随时可变，甚至可以在 web 浏览必须的 80 端口上进行自己的活动。传统的交换机、路由器和防火墙主要是通过对 IP 地址、TCP/UDP 端口号等要素的侦测以实现对网络访问的识别，对此类大量采用动态端口和加密传输技术的应用，则无法识别、形同虚设。

2.2 带宽扩容措施

由于网络流量管理不善，关键应用得不到满足，传统的方法一般都是系统进行扩容，增加网络带宽，这是一种比较消极的、被动的、治标不治本的解决方法，虽能解决一时之需，但随着时间的推移，网络应用慢慢增多，同样的问题还会出现，然后再增加网络带宽，随后同样的问题又会出现……如此往复下去，所带来的成本增加将是巨大的，这也是组织所必须要面对和解决的问题。然而，带宽改善和增加总是有限的，不可能无限制地增加下去，而增加的带宽是否能够得到有效的管理和使用，在这种情况下又如何才能保证 IT 投资的 ROI（投资回报率），都值得商榷。

3 Netzone 专业智能流控方案

Netzone 流控产品是全新的应用层级别的流量控制系统。能为用户提供目前为止性能最好、性价比最高的流量控制解决方案。支持对 IP 流量的应用分类，能做到精准识别、准确评估，实时控制用户组、应用服务流量。通过应用路由、应用分流、应用优先、DNS 管控、行为管理等功能实现各类网络尤其是复杂网络情况下的流量控制目标。

Netzone 的流控解决方案是基于状态和特征的检测，精确识别超过 95%的协议类型，特征库支持超过 900 种应用协议，并创新地自主开发“协议特征描述语言”——PSDL(Protocol Signature Description Language)，使得维护协议特征库更加及时方便快捷。Netzone 的流控解决方案从节点双方的通信过程中寻找特征数据，这些特征数据不限于某条特定的连接，如果特征匹配，那么系统将记录该节点，而不是某条连接。一旦该节点被识别出来，那么后续同该节点通信的数据无须重新验证，因此极大的提高了系统的性能。

Netzone的流控解决方案在基于节点的有状态识别技术的基础上还向智能方面进一步发展，该技术可以从多条连接中自动根据某种统计规律来识别某些特征不明显或者被加密了的通信协议（如SkyPe），在保证性能的同时，提高了系统识别的准确性。这种技术针对P2P应用尤其有效。此外，针对第4代P2P应用软件的变化，采用独有主动探测和服务伪装技术保证对P2P识别的准确性。其独有的服务探测引擎可以识别第四代P2P应用，如emule。对于迅雷这样综合了P2P和HTTP,FTP等传输协议的应用，开发了独有的服务伪装引擎。通过学习的方式，采用连接识别和节点识别相结合的方式，大大减少了连接数，用较少的资源监控更大的P2P应用网络，同时提高了系统的效率。因此，以应用特征识别与控制的技术特点，才是一个真正的应用层流量管控系统。

可以用“智慧带宽”来形容，以最先进的应用识别引擎、精确识别、通道控速、按需调控各种应用占总带宽的比例，通过精确识别将网吧的带宽划分为多个通道，使每一种网络应用分别从不同的通道访问外网。即便某一通道被占满，也不会影响其它任何通道的正常工作。

4 产品技术介绍

4.1 系统架构

Netzone是一款基于网桥构架而实现的流控管理系统，主要由应用特征库、应用识别系统、应用管理系统三大部份组成，并通过系统管理、策略管理、系统维护、监控统计四大人机互动管理功能，对流经的所有应用数据进行实时监控与管理。其结构图如下：

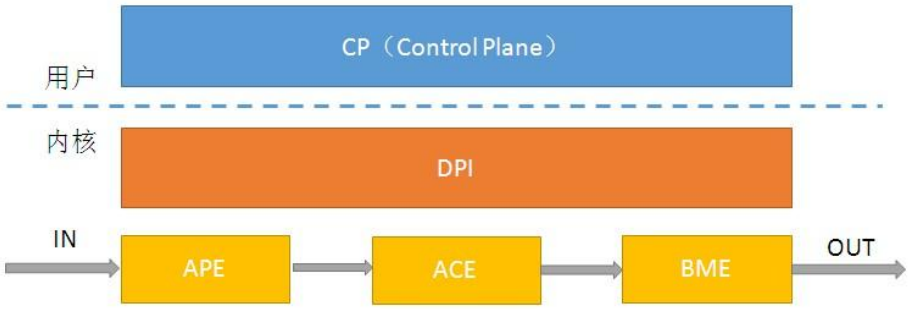
4.2 技术架构

Netzone的流控解决方案具有安全、稳定、可靠的特性。该核心对网络协议栈作了大量的修改和优化，极大提升数据处理速度；修改部分中断处理函数和网卡驱动，优化数据处理优先级。在识别技术方面，在基于会话和特征识别的基础上，采用主动探测技术和智能技术，识别特征模糊和被加密的P2P协议，有效提高识别率；在性能保证方面，利用节点技术和硬件处理特性，如定制硬件驱动，充分发挥硬件性能，从而达到整体的高性能。

整个技术层面分为数据平面（Data Plane）和控制平面（Control Plane）

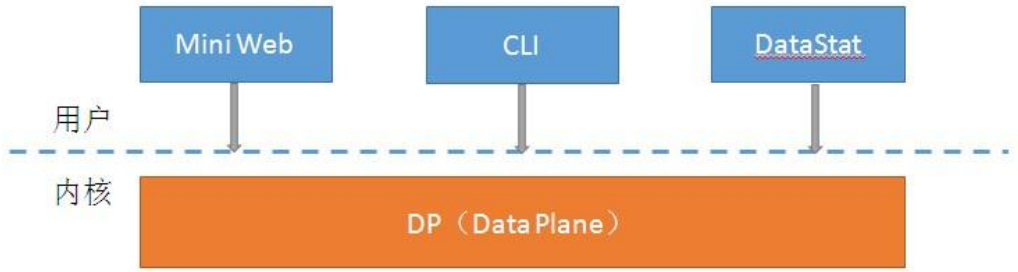
两个部分：

1) 数据平面(Data Plane)：负责数据包处理，同时提供同控制平面的接口。数据层面直接由硬件驱动，这样避免了网络协议栈带来的开销，使得系统能够充分利用硬件的性能而更快处理数据包。数据平面运行在系统的核心层。



数据平面组成

2) 控制平面（Control Plane)：负责系统管理，包括数据平面的维护、Web 管理和命令行管理接口。控制平面运行在系统的应用层。并且数据平面的运行优先级高于控制层面，这样确保数据包即时处理。

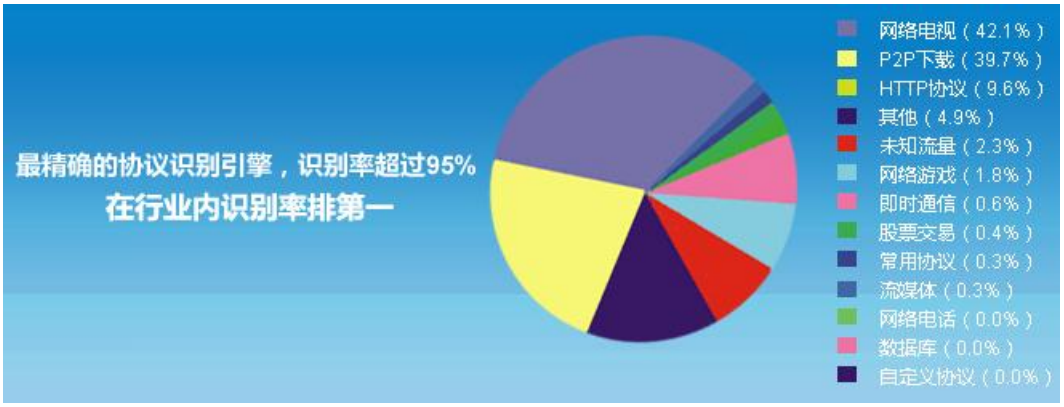


控制平面组成

4.3 技术特点

4.3.1 精确识别

《Netzone》 带有强大的协议识别引擎，不但可以识别各种明文的协议，如Bittorrent，eDonkey，而且其独有的“加密协议深度识别”技术可以识别经过加密的P2P协议，如Skype和eMule。



到目前为止，已经支持9大类超过900种应用协议：

协议类别	应用协议
HTTP 协议	WWW 、Web 音乐、FLASH、HTTP 代理、有道词典等；
HTTP 下载	HTTP 分块传输、伪 IE 下载、网易网盘下载、苹果应用下载、其他下载等；
HTTP 上传	QQ 硬盘上传、其他 HTTP 上传、网易网盘上传、百度云等；
Web 视频	优酷、i 酷、土豆、酷六、六间房、Youtube、HULU 网、Sina 视频、Sohu 视频、网易视频、我乐网、腾讯宽频、凤凰网、波波虎、其他 Web 视频、CCTV 点播、PPLive 视频、芒果 TV、奇异视频、激动网、乐视网、爆米花、优米网，迅雷云点播、搜狐影音、华数、PPStream、东东宽频、风行 Web 视频、天翼视讯、城市联合、第一视频、CC 视频、Viewgood 等；
移动浏览器	Ipad、ipod、iTunes、UCWeb、移动 QQ 浏览器、Android 等；
常用协议	
电子邮件	SMTP、POP3、IMAP、LotusNote、网易闪电邮等；
终端类	VNC、PCAnyWhere 、SSH 、Telnet、远程桌面、Radmin、Dameware、ICA、TeamViewer、向日葵远控、Logmein、网络人、TTVNC、Ctrix 等；
文件传输	FTP 、TFTP、RSync、NFS、CVS、MSDS 等；
网络管理	DNS、DHCP、NNTP、SNMP、NTP、SSDP、UPNP 、NETBIOS、DAYTIME、SYSLOG 、DECRPC、LDAP、NAT 端口映射、ISA 控制协议、STUN、GIOP、WinBox、Radius、万象网管、花生壳、HTTPS 、Socks4/5、SocksOnline 等；
游戏维护	迅闪、网维大师、易游、左轮、强者、i8、MZD、起凡补丁下载、游乐吧、网众快车、QQ 游戏补丁、闪维、方格子、快吧、讯游、迅雷网游加速等；

网络安全	L2TP、PPTP、IPSEC、GRE、OpenVPN、深信服 DLAN、ISAKMP、IPSec-NAT-T、天融信 VPN 等；
软件更新	360 更新、Nod32 更新、Windows 更新、卡巴斯基更新、搜狗系列、QQ 管家等；
流媒体协议	RTSP、MMS、QuickTime、Windows、WMPlayer、MediaPlayer、Real Player、BBSee、磊客、新浪奥运视频、网易奥运视频、QQ 奥运视频、CCTV 央视高清、央视高清、RTMP、千千静听、海康威视、ImagineWorld 等；
P2P 下载	Bittorrent、BT 扩展协议、BT 加密协议、eDonkey 、Gnutella、Fasttrack、Kazza、iMesh 、DC、AppleJuice 、Ares、Mute、SoulSeek 、WinMX、Poco 、Napster、Kugoo（酷狗）、迅雷、迅雷资源查询、100Bao（百宝）、BaiduX 、Vagaa、TuoTu（脱兔）、PPGou 屁屁狗）、Maze（妹子）、QQ 旋风、超级旋风、KOOWO、PP 点点通、FlashGet、搜娱、RaySource 、HuntMine 、RealLink、Foxy、P8 、顶阅视听盒、汉魅、131 玩玩、优蛋、米人、游戏罐头、FreeNet、快快游戏、云游戏等；
即时通信	MSN 、雅虎通、QQ、网易泡泡、阿里旺旺、淘宝旺旺、新浪 UC 系列、GoogleTalk TecentMessager(TM)、Lava-Lava 、AIM、IRC、网易 CC、飞信、新浪 UT Game、百度 Hi、51 挂挂、9158 视频聊天、E 话通、iSpeak、呱呱视频聊天、新浪 UC 视频聊天、歪歪语音、盛大语聊、TeamSpeak、移动桌面助理、BigAnt、聊聊语音、嘟嘟、飞秋、齐秀社区、人人桌面、Jabber、诚创网络平台、IMO、飞聊、米聊、微信、RC 语音、新浪微博、移动微博、MSNLite、语酷娱乐、陌陌等；
网络电视	PPS、PPLive、PPStream、Feidian(沸点)、ReCool 乐酷)、QQ 影音、TVants TVKoo、PPMate、MySee、UUSee、CCIPTV、SopCast、VJBase 、Mysee、忽视 TV、JeBoo 、Funshion（风行）、迅雷看看、PPFilm、QVOD、极速酷 6、青娱乐、飞速土豆、BOBO、NetiTV、新浪电视直播、搜狐电视直播、TomLive、iV 影音加速器、乐鱼、暴风影音、DOPOOL、央视电影频道、葫芦网、久久影音、Viewgood、V2 视频会议、VideoSpeed、任子行视频、SVOD、优朋影视、百度影音、完美高清、奇异加速器、乐视客户端、八目电影、飓风电视、PPWeb 等；
网络电话	H.323 、SIP、Skype、UUCall、ET263、MGCP、铁通飞线、铁通 RedVip、VTalk、Sipphone 、Net2Phone、阿里通、KC 网络电话、盛大 ET 语音、Viber、华为语音、Facetime 等；
网络游戏	奇迹世界、卓越之剑、名将三国、巨人、征途、倚天剑和屠龙刀、西游记、新英雄年代、传奇系列、盛大富翁、彩虹岛、龙骑士、风云、冒险岛、热血传奇、超级舞者、鬼吹灯、超级跑跑、X-乒乓、永恒之塔、蜀山系列、千年、乱武天下、热血英豪、英雄连、诸侯、巨星、生死格斗、永恒之塔、泡泡堂、跑跑卡丁车、反恐精英 OL 、蒸汽幻想、露娜、街头篮球、完美世界、武林外传、赤壁、热舞派对、神鬼传奇、梦幻诛仙、纵横时空、机战、魔域、投名状、征服、英雄无敌、91 开心游戏、热血江湖、英雄档案、功夫世界、问道、秦始皇、希望、西游 Q 记、神界、炫舞吧、神泣、数码宝贝、QQ 幻想、QQ 三国、QQ 音速、地下城与勇士、QQ 寻仙、QQ 炫舞、QQ 飞车、QQ 华夏、QQ 自由幻想、QQ 游戏、穿越火线、QQ 对战平台、战地之王、大明龙权、武林群侠传、倚天 2 外传、

	泡泡游戏、大话西游 3、梦幻西游、新飞飞、魔兽世界、大话西游 2、大话西游外传、大唐豪侠、水浒 Q 传、反恐行动 OL、剑侠情缘、剑侠世界、春秋 Q 传、仙履奇缘 2、新浪游戏、天龙八部、突袭、战火红警、凤舞天骄、天地档案、海之乐章、新魔界、生肖传说、武易、伊苏战记、众神之战、劲舞团、仙剑 OL、SD 敢达、宠物森林、超级舞者、风火之旅、梦幻古龙、三国鼎立 梦幻龙族、名将、游戏人生、妖怪 A 梦、刀剑、大话水浒、天龙八部、惊天动地、成吉思汗、特种部队、新破天一剑、飙车世界、盛世 OnLine、三国群英传、精灵乐章、西游天下、秦伤、纳亚外传、梦三国、联众 R2、三国策、联众世界、掌门人、JJ 比赛、面对面、边锋、宽带中国、多多视频、远航游戏中心、GGC 对战平台、VS 对战平台、浩方对战平台、贸易街机、豆客、起凡对战平台、175PT、中国游戏中心、街舞区、星际家园、霸王系列、勇气 OL、真三国无双、预言、炎黄传说、抗战英雄、英雄岛、乱世枭雄、风雷游戏、魔力宝贝、浪漫传说、浪漫庄园、FIFA Online、梦想世界、星尘传说、弹头奇兵、同城游、51 炫舞、赖子山庄、龙 OL 等；
股票证券	大智慧、钱龙系、同花顺、申银万国、指南针、四道立方、证券之星、齐鲁证券投资通、长城证券、大福星、富远行情、大有期货、宏汇软件、国泰君安、东方财付通等；
数据库	MSSQL 、Oracle 、MySQL、PostgreSQL、LotusNotes、FileMaker 等；
其他协议	ICMP 、SYN_ACK 、IP 分片 、文件下载及视频、在线交互式应用、非 IP3 层协议、其他 4 层协议、看天下、OSPF、BGP、ARP、IGMP、PPPOE、IPv6、RSVP、IGRP、IPMobile、IPv6、MPLS、Teredo、未知 80 端口、垃圾包、IPX、无连接 TCP、SYN-FLOODING、VestoreSIS、IPv6-Encap、BMS 等；

精确识别的意义在于评估和掌控。可以简单而又准确的评估网络应用状况，通过精确识别各类应用，随时了解各种应用比例，随时了解带宽利用率及单机应用速度。根据实际需要制订管控策略，控制各种应用的上行和连接数，使应用的瞬间速度接近控制目标并保持速度平稳。同时降低抛弃量，保证总带宽不会瞬间占满，保障各类应用顺畅，彻底掌控整体网络资源的使用情况和效率。

4.3.2 强大的平台性能

在处理吞吐量 20Gbps 以下的网络环境，X86 硬件平台配合多核 CPU 与 ASIC、NP 架构相比，在处理网络应用层流量分析时，X86 硬件平台具有优势，而非 I/O 转发性能决定系统整体性能。20Gbps 吞吐量这个级别以下的网络环境，更需要的是精细化管理，需要精确的识别、快速的更新协议特征库、高效灵活的控制策略，X86 硬件平台配合专用的 OS，能很好的满足这些指标。

Netzone 针对应用层流量管理产品突出强调分析运算能力、快速编程、扩展

等特点，结合 X86 硬件平台优势，专门多核 CPU 重新进行调度，把系统管理 CPU 和数据包处理 CPU 独立运行，充分发挥多核 CPU 的并行处理能力，经大量 ISP 应用案例和实验室的专业评测验证，性能在业界处于领先地位。

4.3.3 灵活的带宽管理

在传统的 IP 网络中，所有的报文都被无区别的等同对待。每个路由器都对所有报文采取先进先出（FIFO，First In First Out）的策略进行处理，它尽最大的努力（Best—Effort）将报文送到目的地，但对报文传送的可靠性、传输延迟等不做任何保证。在一个网络中，不同的人员对带宽的使用是不均衡的，有人使用得多，那么留给别人的带宽就少，如果某些人员使用 BT、迅雷下载文件或者使用 PPStream、PPLive 在线收看网络电视，那么这些人员就会占用大量带宽，并将持续占用甚至耗尽出口带宽资源，造成网络速度和性能明显下降，使其他用户的正常网络应用比如 Web 访问、收发 E-mail、MSN 聊天、股票查询、视频会议出现延迟、停顿、掉线等现象。与类似产品单纯通过对 P2P 及其他特定流量进行带宽控制来变相“保障”正常应用的方式不同，《Netzone》同时提供基于应用或基于 IP 的“带宽控制”、“带宽预留”、“带宽保证”三种机制，为用户灵活调控网络带宽资源提供更方便的功能。

1) 带宽限制：根据策略对特定 IP/IP 组、应用协议进行带宽限制，避免这些 IP/IP 组、应用协议过度使用带宽而影响他人和整个网络。特别地，《Netzone》 支持针对“未知协议”的带宽限制功能，可将未识别或尚未支持的协议流量或异常流量控制在一定的范围内。下图为某用户设定的策略：每天 8 点到 24 点将 P2P 和 NetTV 的上下行带宽限制为 10M，其它时间不限，并使用自定义的图表定制的实际效果图。

2) 带宽预留：预留出一定的带宽给特定的 IP/IP 组或应用协议使用。比如：假设网络出口的总带宽为 100M，如果为某些 IP、IP 网段、应用协议预留了 10M 带宽，那么其他所有 IP、应用协议可使用的总带宽即为 90M。预留出的 10M 带宽始终属于规定的 IP、IP 网段、应用协议所有，其他任何 IP、应用协议无论如何都不能占用。

3) 带宽保证：带宽保证与带宽预留类似。所不同的是，带宽保证在其保证的带宽不能满足要求的时候，会从剩余的总带宽里借用所需带宽。以上面 b 中提到例子为例，如果做一条带宽保证策略，分配 10M 带宽给某 IP 组，那么当某个时刻该 IP 组所需要的带宽大于 10M，比如 15M，那么《Netzone》就会从其余的 90M 带宽中借出 5M 给该 IP 组以满足其使用。

对于企业，是否可以以及如何优先保障关键业务、关键科室、关键 IP 的带宽使用是他们首要关注的功能点，而精细的统计分析报表对于网络管理人员更具有策略上的指导意义；

应用优先可对应用进行压制，通过桥带宽减少指定应用的带宽使用量，使总带宽不会被完全占满，保证重要应用不会出现网络拥堵；也可对应用实行借用机制，让不同的应用享有不同的优先等级，优先等级高的应用对带宽资源的利用享有优先权，重点保证主流应用的速度。具备优先等级的应用能在有带宽有剩余时相互借用。

《Netzone》的带宽管理灵活性在具体使用中体现在两个方面：

1) 数据通道：定义带宽管理和调度方式。上面所说的带宽限制、带宽预留和带宽保证就是三种不同类型的带宽对象。系统根据带宽类型和带宽的大小系统地对带宽进行分配和调度。

2) 策略：策略是用来将流量进行分类的机制。《Netzone》里所定义的每一条策略可以包含源地址、目标地址、数据流向（上行还是下行）、应用协议等因素。当匹配这些因素后，就会执行某个动作，如阻断、放行或将其注入某个数据通道。通过将符合这些条件的数据注入通道，实际上就已经对符合上述条件的数据包实施了流量管理。

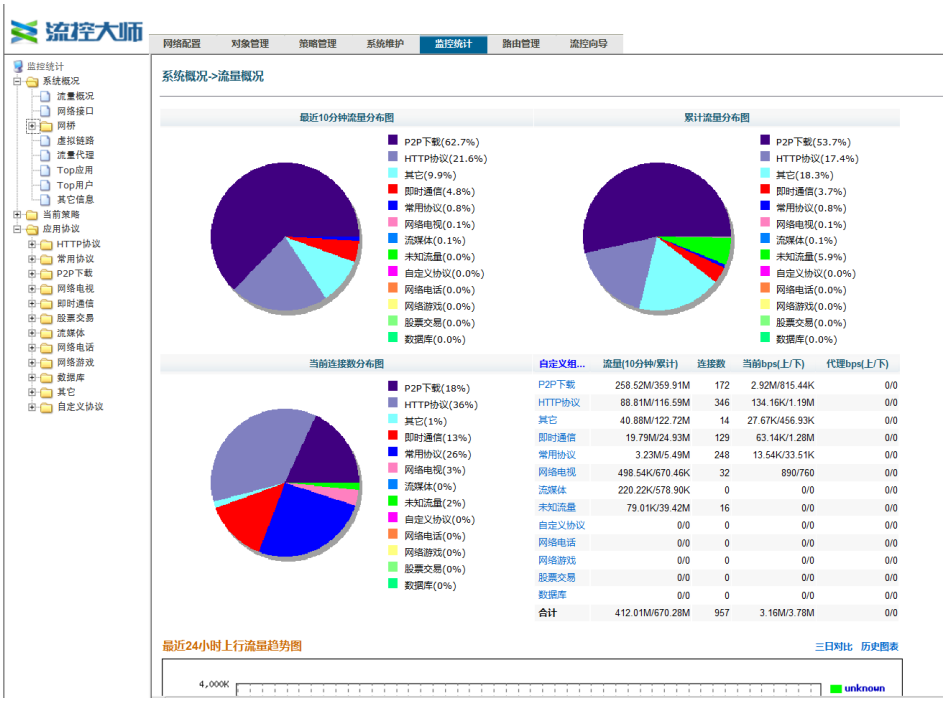
4.3.4 内网 IP 统计功能

用户可在 Web 界面中选择是否打开内网 IP 统计功能。用户可选择 TOP 10、20、30、所有 IP 的统计排名，并可选择以下三种方式：

a、按照累计流量进行排名

b、按照当前速率进行排名

c、按照在线时间进行排名



用户可以看到单个 IP 的应用流量、连接明细，可直观的列出某个 IP 具体的历史应用　明细，以及目前与该 IP 相关的连接情况，包括每条连接中对方的 IP 地址及端口。

4.3.5 丰富的报表统计

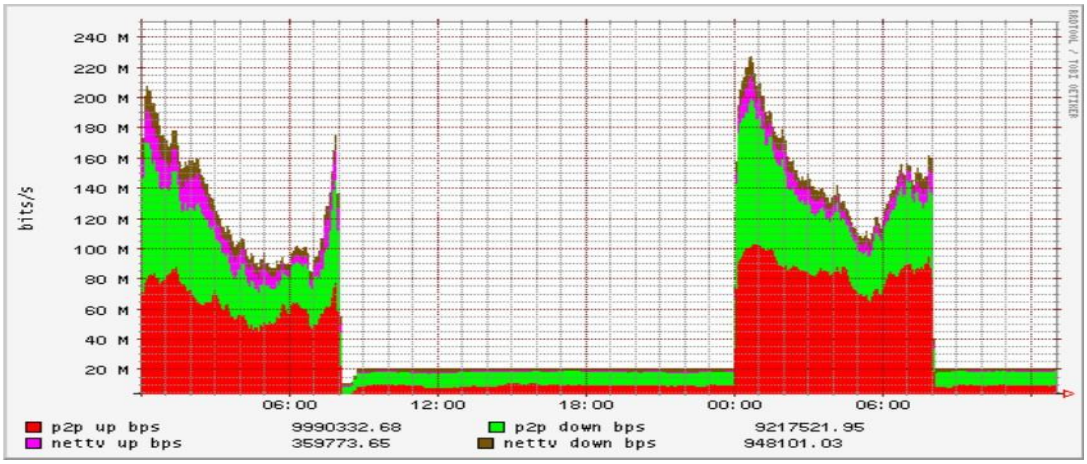
1) 网卡流量、各应用协议/协议组的日图表、周图表、月图表

2) 连接统计、节点统计、协议统计、PPS 统计

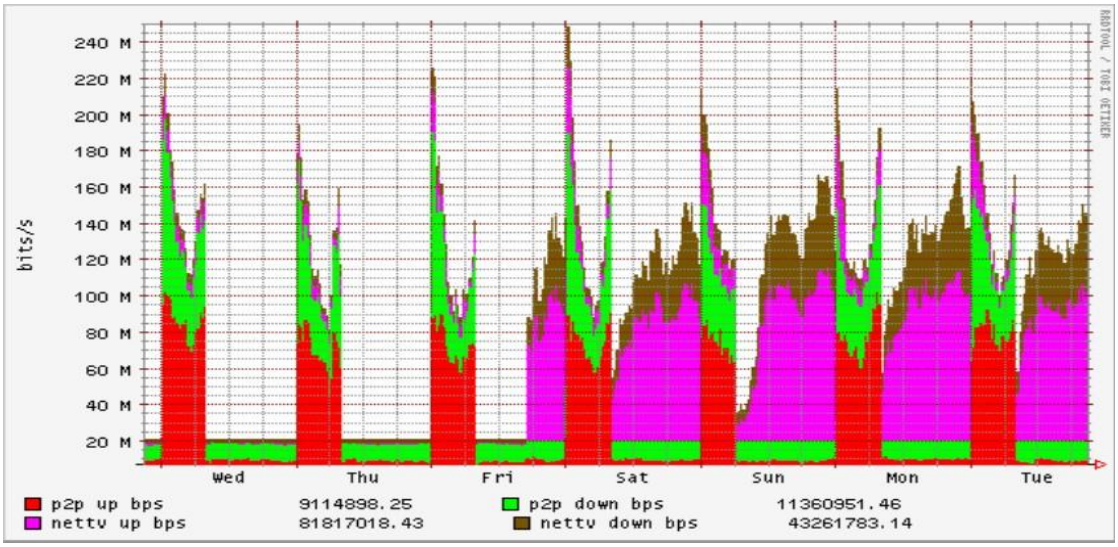
3) 自定义报表功能 用户可针对自己关心的 IP/IP 组、应用协议/协议组等不同的对象自定义一个报表，将针对多个对象的统计结果集中显示在一个图表中，减少日常监控的工作量。统计数据可以指定不同的线形和颜

色以绝对值或叠加的方式显示。报表统计的时间跨度可以是当天、本周和当月。

以下两张截图是某用户自定义的只统计“P2P 协议组”和“网络电视协议组”上、下行流量的图表。



说明：当前策略为 08:00—24:00 之间将 P2P 与网络电视两类流量双方向控制为 20M； 00:00—08:00 不做限制。可以看到在策略生效的时间点，流量呈现明显的瞬间下降情况。



说明：一周内应用限速策略时 P2P 与网络电视两种协议组的流量曲线图。周五将

策略修改为全天放开网络电视流量，只在 08:00—24:00 之间限制 P2P 流量双向为 20M，可以看到每天在策略生效的时间段，被限速的流量始终被严格控制在 20M 以内。

Netzone 的六大类系统报表如下：

设备性能报表	CPU 利用率报表
	内存利用率报表
功能类报表	吞吐量报表
	在线 IP 数报表
	在线会话数报表
功能类报表	Pipe 通道报表
	VC 通道报表
	共享 Pipe 报表
	共享 VC 报表
用户报表	用户报表
	用户组报表
功能类报表	接口信息报表
	接口利用率报表
	接口包大小分布报表
	接口包类型分布报表
链路层报表	链路层主机报表
	链路层主机对报表（可展现主机对集群报表）
功能类报表	网络层主机报表
	网络层主机对报表
	网络层网段报表

4.3.6 具备应用路由、DNS 管控、行为管理等功能。

面对各类用户的多样化需求，流量控制的灵活多样，能更好的满足用户需求。

4.4 核心技术

4.4.1 DPI

传统的IP包流量识别和QoS控制技术，仅对IP包头中的“5Tuples”,即“五元组”信息进行分析，来确定当前流量的基本信息，传统IP路由器也正是通过这一系列信息来实现一定程度的流量识别和QoS保障的，但其仅仅分析IP包的四层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型，随着网上应用类型的不断丰富，仅通过第四层端口信息已经不能真正判断流量中的应用类型，更不能应对基于开放端口、随机端口甚至采用加密方式进行传输的应用类型。

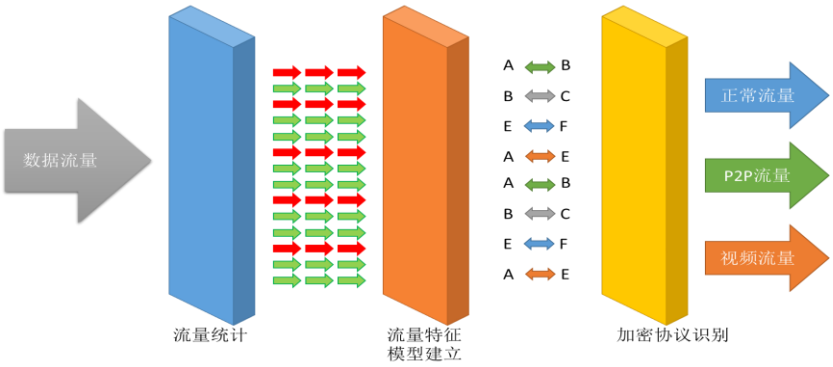
要准确识别网络应用，需要借助复杂的第7层识别技术。现在大量的网络应用包括P2P、即时通讯、网络游戏等等，都具备了跳跃端口、随机端口、自定义端口，甚至伪装或者盗用一些常用服务的协议端口进行通信传输，所以通过对端口对它们进行识别显然是远远不够，传统的流量限速设备无能为力。所以，网络数据包必须在应用层面（Application Layer）上进行检查，即对传输协议如TCP协议的载荷（Payload）部分进行检查，以判断它们是否符合代表某种应用的特征签名。

Dpi——Deep Packet Inspection，深度包检测技术，DPI将网络上的数据报文根据五元组分为若干个的应用流，并通过识别技术对应用流中的特定的数据报文进行探测，从而确定应用流对应的应用或者用户动作。

Netzone的DPI引擎，将传统DPI技术中的基于“特征字”的识别技术、应用层网关识别技术、行为模式识别技术有机的整合起来，有效的灵活的识别网络上的各类应用，目前，产品支持900多种协议和应用的自动识别，从而为用户提供全面的、有效的、灵活的控制和计费。

4.4.2 DFI

DFI——Dynamic Flow Inspection，动态流检测技术，DFI 采用的是一种基于流量行为的应用识别技术，即不同的应用类型体现在会话连接或数据流上的状态各有不同。例如，网上 IP 语音流量体现在流状态上的特征就非常明显：RTP 流的包长相对固定，一般在 130～220byte，连接速率较低，为 20～84kbit/s，同时会话持续时间也相对较长；而基于 P2P 下载应用的流量模型的特点为平均包长都在 450byte 以上、下载时间长、连接速率高、首选传输层协议为 TCP 等。DFI 技术正是基于这一系列流量的行为特征，建立流量特征模型，通过分析会话连接流的包长、连接速率、传输字节量、包与包之间的间隔等信息来与流量模型对比，从而实现鉴别应用类型。DFI 技术通过行为特征鉴定一个基于会话的应用，比较适合用户检测加密应用协议。



4.4.3 PSDL

PSDL ——Protocol Signature Description Language，协议特征描述语言，使得维护协议特征库更加及时方便快捷，通过微编译器和引擎，确保协议数量的可扩展性和灵活性。

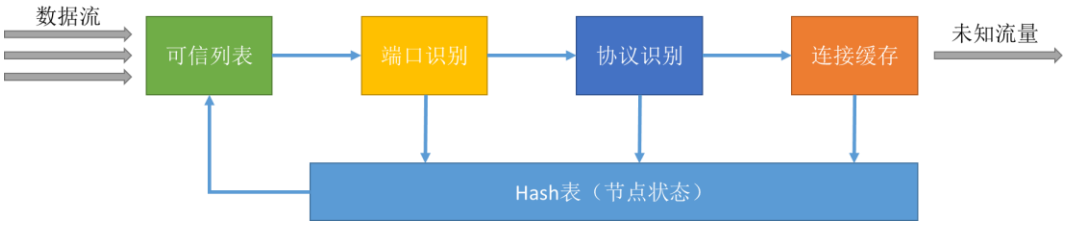
4.4.4 DSCP

DSCP——Differentiated Services Code Point，差分服务代码点。通过在每个数据包 IP 头部的服务类别 TOS 标识字节中，通过编码值来区分优先级。在

Netzone 流控设备中，系统首先识别不同的应用协议类型，之后将不同的应用协议标识以不同的 DSCP，以便对不同的应用协议赋予不同的优先级以及带宽，保证在固定带宽下的应用协议带宽保障与带宽压制。

4.4.5 节点跟踪技术

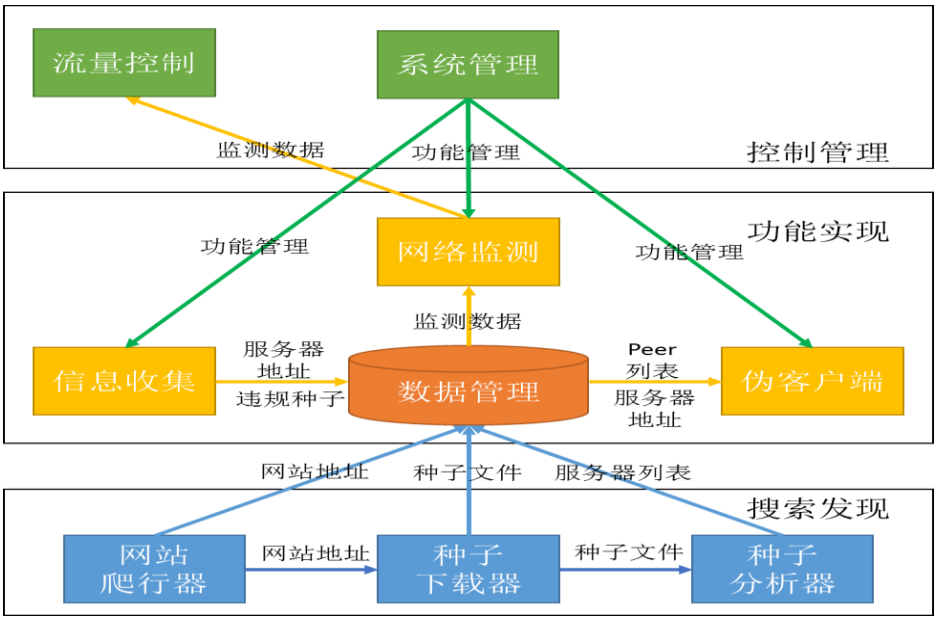
众多的新型网络应用如 P2P，是由许多节点构成的，每个节点都是一个服务器，这个节点可以同时为其它节点提供服务。基于节点的跟踪技术通过多级检测模块,综合基于流量特征、深度包检测等多种检测方法,将获取的节点状态信息存入 Hash 表,并映射形成可信列表反馈到检测端。其基本思想是从节点双方的通信过程中寻找特征数据，这些特征数据不限于某条特定的连接，如果特征匹配，那么系统将记录该节点，而不是某条连接。一旦该接点被识别出来，那么后续同该节点通信的数据无须重新验证，因此极大的提高了系统的性能。



Netzone 节点跟踪技术可以从多条连接中自动根据某种统计规律来识别某些特征不明显或者被加密了的通信协议（如 SkyPe），在保证性能的同时，提高了系统识别的准确性。还通过学习的方式，采用连接识别和节点识别相结合的方式，大大减少连接数，这样可以用较少的资源监控更大的 P2P 应用网络，同时提高了系统的效率。

4.4.6 主动探测技术

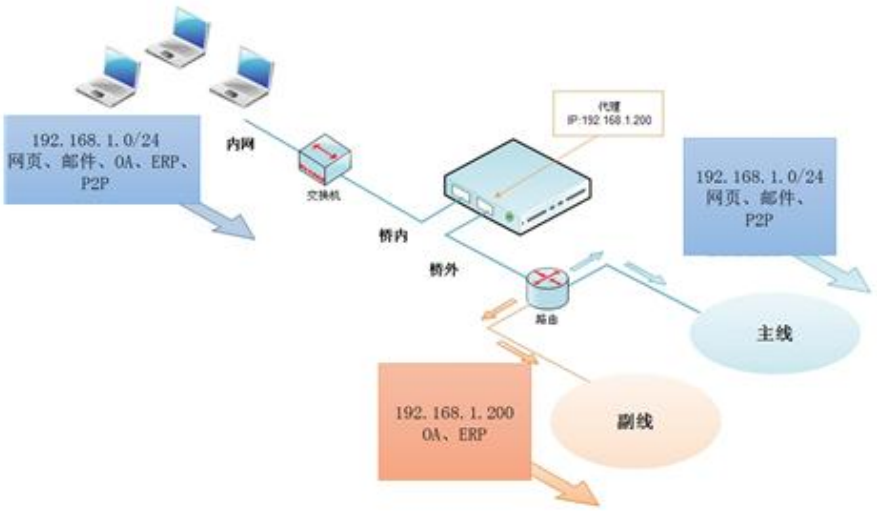
目前，BT 和 eMule 是使用最广泛的 P2P 文件共享软件，分别使用公开的 BitTorrent 协议和 eDonkey（电驴）协议，在因特网的 P2P 应用中流量占用率最大。对 BT 和 eMule 网络进行监控技术研究，即具有典型性，也具有重要的现实意义。Netzone 流控设备在协议分析的基础上，研究主动探测技术，开发了 P2P 网络信息主动探测技术，实现了对 BT 和 eMule 网络中文件传播的资源探测和节点定位，能有效解决 P2P 网络中信息传输不易发现和不易定位的问题，在实际应用中达到了实用效果。



此外，Netzone 流控设备针对第 4 代 P2P 应用软件的变化采用独有主动探测和服务伪装技术保证对 P2P 识别的准确性。流控设备采用独有的服务探测引擎可以识别第四代 P2P 应用　如 emule 0.47c。服务伪装对于迅雷这样综合了 P2P 和 HTTP,FTP 等传输协议的应用流控设备开发了独有的服务伪装引擎。

4.4.7 应用分流技术

应用分流可对应用进行疏导，把指定应用分流到多条线路上，降低主线路压力，间接增加带宽基数、提高带宽利用率、降低带宽使用成本；也可对应用进行管制，根据实际情况强制指定应用走哪条线路，满足特殊应用需求，尤其适合有备用线路的企业。



如上图所示，在启用应用分流策略后，网页、邮件、P2P 等流量全部从原有主线链路访问 Internet，OA、ERP 因为对带宽响应时间的要求较高，被流控通过应用分流代理机制旁路到副线访问 Internet，保证了企业实际业务的需要。同时，在副线链路出现故障时，数据还会被自动路由回到主线链路，保障了关键业务可靠性的要求。

5 产品功能与应用

5.1 产品功能

➢ 可视化的实时分析

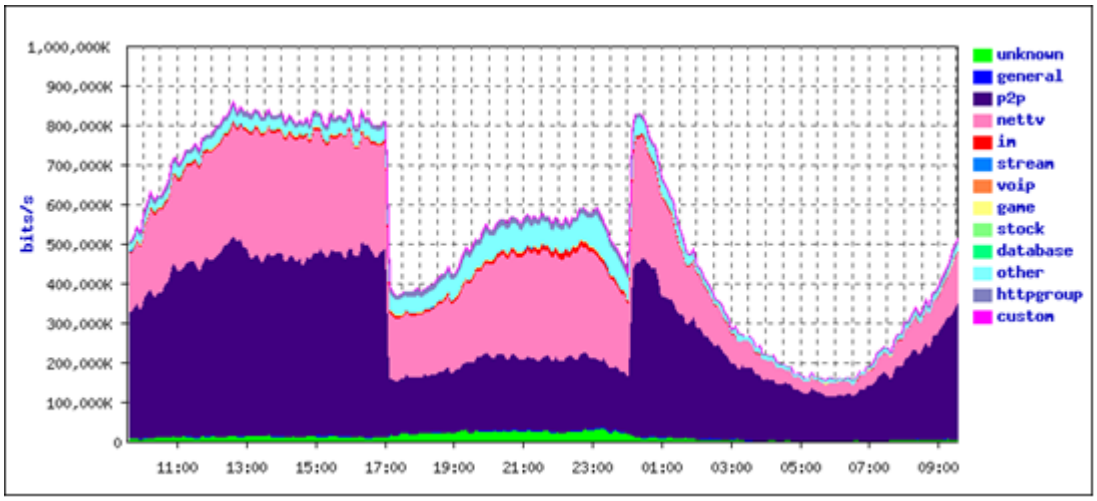
Netzone 接入网络中，缺省即加载所有特征库，并立即开始自动分析网络中流量构成和显示统计数据。Netzone ISP 根据应用类别缺省分为 11 大类，每一类别又可分为若干子类别。在一个千兆链路网络环境中，通常只需 6-8 小时的分析，即可提供全面的统计报表，如饼图百分比和应用实时数据方式，为下一步制定管理策略提供了决策支持。

➢ 灵活简洁的策略配置

策略配置管理对象和动作选项，基于参数化的驱动配置方案，扩展新功能仅需要增加参数项，保持策略管理配置的一致性，非常简洁易用；支持策略嵌套，即在同一条管理策略里，既可以针对特定对象(IP 或应用)进行总体的数据通道控制，也可以单个 IP 限速，同时可并列匹配“DSCP 标记”、“对端抑制”、“应用优先级”、“流量代理”等参数，实现策略的高度灵活性、简洁性和高效。

➢ **流量管理**

支持基于应用协议/协议组和 IP/IP 群组的速率控制； 支持阻断、限速、带宽保证和带宽预留；Netzone 以精确的协议识别、精细的控制效果著称，通过配置流量管理策略，匹配时间段和在线 IP 数等参数启用相应策略，达到削峰填谷、保证关键应用、网络安全畅通高效的运行。Netzone 产品管理带宽最小控制粒度为 1kbps。



实例：上图为出口带宽为 1G 的网络环境中，下行方向的 24 小时流量趋势图；17：00-24：00 上网高峰时段，仅对 P2P 下载（紫色）和网络电视（粉色）自动匹配控制策略，其余非高峰时段全部放开的效果；

➢ **基于 Web 的身份认证**

基于动态过滤 http 协议通信。它可授权对网络中某一个具体安全域进行访问。用户在进行 HTTP 通讯之前不需要主动的登陆进行认证，当用户进行通讯时，Netzone 流控设备收到 HTTP 请求，会主动返回一个 web 页面要求用户进行认证，认证通过后，通讯过程才能继续。

➢ **连接数管理**

支持针对应用协议的 TCP、UDP 和总并发数控制； 支持到外网特定 IP 地址的 TCP、UDP 和总的应用并发连接数控制；支持根据数据链路、外网 IP、内网 IP、IP 群组和应用协议、协议组等参数制定连接数控制策略；可根据时间和在线 IP 数等参数启用相应策略。

连接数管理更多适用于防火墙连接并发数不够成为网络瓶颈时，Netzone ISP 启用连接数控制，对防火墙起到很好的保护效果。

➢ **HTTP 管控**

支持 URL 访问控制，如阻断非法站点； 支持 URL 重定向和 Web 信息提示；可根据内网 IP、文件类型、访问方法(GET 或 POST)和目标 URL 等参数设置控制策略；可根据时间和在线 IP 数等参数启用相应策略。

➢ **监控统计**

可提供整个系统、各链路的流量和连接数统计图表、最近 10 分钟流量、累计流量、并发连接数统计图表、实时显示协议和协议组当前速率、三日对比以及最近一天、最近一周和最近一月的流量趋势图表、实时显示某个 IP 流量速率和当前各个应用的速率明细、实时显示某个 IP 的当前连接明细，以便于异常流量诊断、可根据应用速率、流量和连接数等条件进行排序、可实时显示某个应用下的 Top 用户、可提供在线并发连接、连接创建和删除速率等数据的趋势图表、可提供在线 IP 和共享用户趋势图表、可选中多个协议进行趋势图分析对比等。

192.168.1.6档案 系统已连续运行0天18小时43分35秒（系统正常）

TTL(秒)	在线时间(秒)	流出流量	流入流量	流出bps	流入bps
596	9526	3.27M	18.92M	148.28K	1.74M
MAC地址		连接数	被拒绝的连接数(TCP/UDP)		
00.1c.25.1a.3c.18		425	0/0		

流量概况 | 连接信息 | 相关身份 | 共享用户

序号	协议	流入速率(bps)	流出速率(bps)	总速率(bps)
1	迅雷	1.03M	103.37K	1.13M
2	伪IE下载	603.48K	26.47K	629.95K
3	迅雷看看	59.56K	3.54K	63.10K
4	WWW	23.77K	1.50K	25.27K
5	其它HTTP上传	8.55K	1.06K	9.62K
6	QQ直播	5.81K	2.42K	8.23K
7	QQ聊天	3.70K	4.31K	8.02K
8	QQ音乐	2.62K	192	2.81K
9	SYN_ACK	1.20K	3.73K	4.93K
10	DNS	920	640	1.56K

➢ **基于应用协议优先级调度**

率先实现支持基于应用协议的优先级调度机制；同时支持网络层基于 IP 的优先级调度机制；支持 0-6 七个优先级别。

➢ **应用路由，内容路由**

实现基于应用、内容级路由，首要前提是协议识别率高、精准、误识别率低；Netzone ISP 的优秀识别能力，为实现应用层流量的终极管理奠定了坚实的基础。

基于应用协议的策略路由功能，简称应用路由。对于多出口链路，可实现将不同类型的应用协议导向不同的网络出口，变控制为疏导。

内容路由：支持将 www、web 视频、http 传输等 HTTP 类应用访问请求多链路路由选择或重定向到网络中的缓存服务器 Cache，实现 HTTP 类应用流量的网内传输。

- **共享检测，身份信息**

检测网关后面的私有 IP 地址(1 拖 N)；非 IP ID 检测，基于应用层检测，不仅能检测到共享用户数量，也能检测到具体的 IP 地址，先进的检测手段能应对所有的共享机制。可对内网 IP 下的 QQ 账号、MSN 账号和 POP3 账号进行跟踪。

- **海量日志存储**

支持 Netzone 专用的日志系统，也支持以 SYSLOG 或者 NETFLOW 格式向第三方设备输出会话日志；支持以 SYSLOG 格式向第三方设备输出单独的：URL 访问日志、QQ 登陆登出日志、MSN 登陆日志、POP3 登陆日志、DNS 查询事件等日志。

1) **QQ 事件日志：**当内网用户登陆 QQ 时，系统将对该行为自动识别并自动记录该 QQ 号码与 IP、时间的对应关系。之后可根据时间段、IP 地址进行 QQ 登陆事件的查询； 并可对指定 QQ 号码进行 IP 和时间等登陆信息的反查功能，

2) **MSN 事件日志：**当内网用户登陆 MSN 时，系统将对该行为自动识别并自

动记录该 MSN 帐号与 IP、时间的对应关系。之后可根据时间段、IP 地址 MSN 登陆事件的查询； 并可对指定 MSN 帐号进行 IP 和时间等登陆信息的反查功能

3) **POP3 事件日志：**当内网用户登陆 POP3 时，系统将对该行为自动识别并自动记录该 POP3 帐号与 IP、时间的对应关系。之后可根据时间段、IP 地址进行对 POP3 登陆事件的查询； 并可对指定 POP3 帐号进行 IP 和时间等登陆信息的反查功能

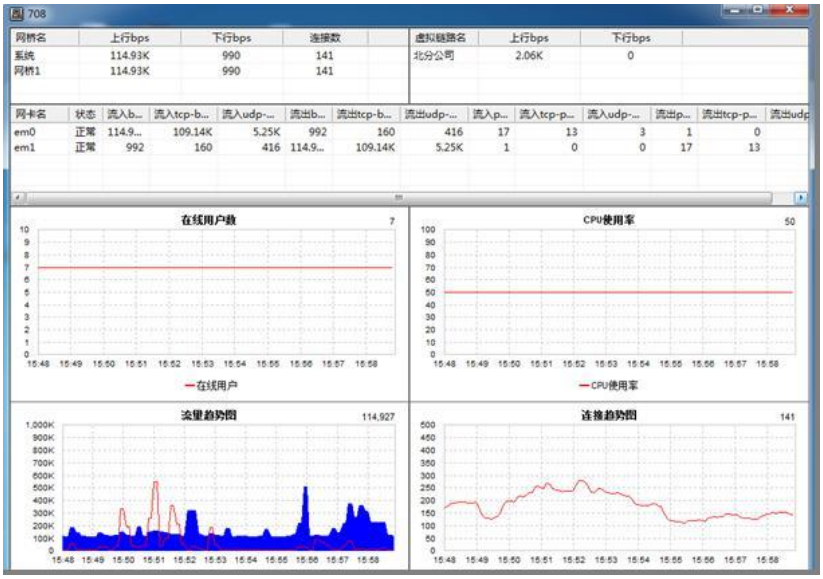
4) **URL 访问事件日志：**当内网用户进行网页访问时，系统将对该行为自动识别并自动记录该 URL 访问记录。可根据浏览网页或上传(发帖)为条件进行针对性查询；可针对指定 URL 进行访问者的事件反查；可查询指定 IP 的 URL 访问记录

5) **域名统计：**根据访问次数，对指定时间段以内网络用户所访问过的域名进行排名统计；点击排序中的各个域名，可提供该域名的 IP 访问者统计列表

6) **会话日志：**当内网用户发起每一次网络访问时，系统都将对其进行日志记录。记录信息包括：源 IP、源端口、目的 IP、目的端口、应用协议名称、URL、持续事件、上传/下载的字节数等

➢ **集中监控管理**

实时监控客户端，最大可管理 16 台 Netzone 流控设备。

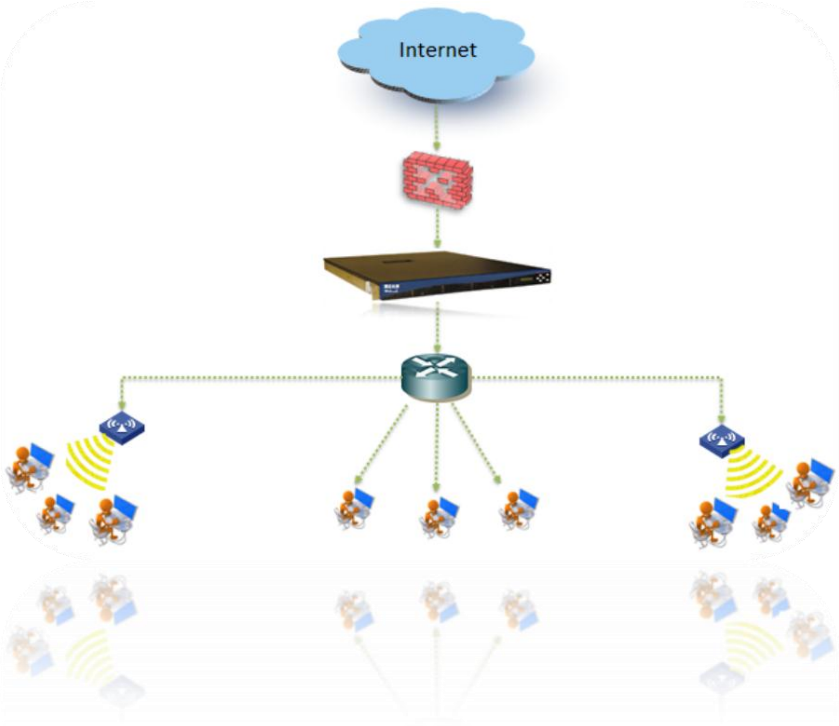


5.2 典型应用

5.2.1 透明网桥部署

以透明网桥方式部署在出口链路上时，可对出口链路上的双向流量进行协议分析、统计，同时根据所设定的规则对流量进行灵活的限制和分配。为避免设备受扫描、攻击，网桥上无需配置 IP 地址，用户可通过专门的管理端口对《Netzone》进行配置管理，使用透明网桥模式接入，用户既可以统计流量，又可以做访问控制和带宽管理。

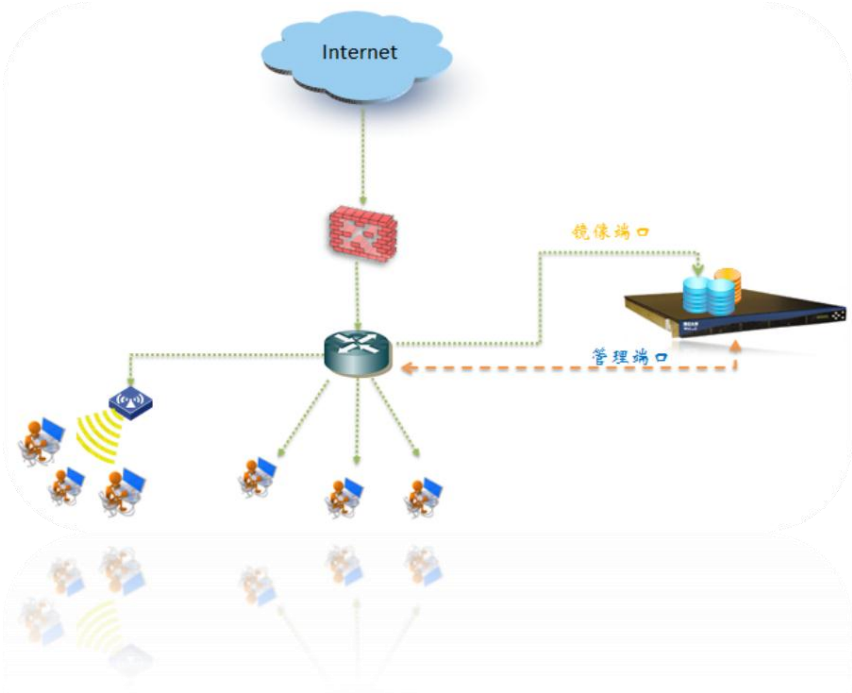
典型的部署方式如下图所示：



5.2.2 旁路监听部署

以旁路监听方式部署时需要核心交换机支持端口镜像功能，设备在交换机或路由器旁，通过交换机或路由器的“Port Mirror”（端口镜像）技术对经过交换机和路由器的上下行端口的流量进行协议分析、统计。在旁路监听模式下，《Netzone》只能对流量做分析统计，而不能做控制。不会对现有网络造成任何影响，典型的使用方式是用户先采取旁路监听模式采集网络的各种流量信息，然

后根据网络实际情况制定相关访问控制和带宽管理策略，最后以透明网桥《Netzone》接入到网络中对整个网络的流量进行管控。



6 成效及案例

6.1 应用成效

- **宽带运营商**

1) 告别普遍困扰各级 ISP 的两大难题：少数用户 P2P 滥用导致其他用户针对网速缓慢的频繁投诉、游戏用户对于网游速度得不到保证的频繁投诉；
2) 提升用户满意度：通过合理调控高峰期 P2P 类应用的带宽滥用，提升常规应用的网络体验，减少用户投诉，更加有利于市场竞争；
3) 提高带宽利用率：通过区分应用协议的精细化带宽管理，提升当前链路的用户承载能力，提高链路的收益能力；
4) 网络运营从此“可视”和“可控”：实时掌握网络运行状态，随时根据网络变化情况在最短时间内实施有效的技术应对策略；

5) 解决用户共享上网，即俗称的“一拖N”检测问题：基于应用协议的检测手段，能应对所有的共享、代理行为，精确度大大高于传统设备基于IP ID的检测机制，为宽带运营商的合法收益提供技术保障；

6) 拓展企业盈利模式：提供层次化网络服务质量，支撑增值业务服务平台。

➢ **政企事业单位**

1) 网络可视化管理能力提升：通过实时详尽的统计报表，掌控员工的网络应用情况，并具备行之有效的策略管理机制；

2) 规范员工网络应用，提升企业生产力：上班时间与工作无关的应用如开心农场、QQ、股票、土豆网、迅雷等通通不再是困扰企业管理者的问题；

3) 必要的安全防范机制：利用自身强大的性能优势，实时监控网络运行，识别阻断网络攻击，根据并发连接个数可以确定并阻断DOS攻击等异常行为,为企业提供专门应对伪IP类木马攻击、IP碎片攻击等检测和防护机制保护网络设备安全；

4) 优化网络运行管理：通过检测分析带宽使用状况，合理分配带宽资源；

5) 强化网络行为管理：根据各种应用业务的流量，制定相关策略限制非主流业务(例如可以对即时通讯、P2P 下载、网络游戏、网络电视等)在峰值时段进行限速、阻断，进一步规范员工上网行为，为人性化科学化管理提供基础保障；

6) 保障关键网络应用：根据企业需求保障关键应用(例如 ERP、CRM、视频会议等)，限制非主流业务占用过多的带宽，监测、阻断异常流量；

7) 必要的日志和审计功能：专用的日志系统，除提供详尽的全应用日志存储和细致的统计分析功能外，甚至可提供单独的QQ登陆/登出、MSN登陆/登出、URL访问、DNS查询日志，以满足相关部门对特定应用特定事件的审计要求。

8) 让企业已经配备的系统，如：病毒墙、IPS/IDS、UTM、邮件病毒墙、网络杀毒系统等等，具备良好数据传输条件。

➢ **教育行业**

1) 网络可视化管理能力提升：通过实时详尽的统计报表，掌控校园网的网络应用情况，并具备行之有效的策略管理机制；

2) 保障教学、科研、招生和远程教育等关键的网络应用，合理管控P2P类应用；

3) 提高学生宿舍使用校园网的管理水平。

➢ **酒店行业**

1) 高峰期采取“通道和单IP限速结合的策略模式，既满足客人P2P下载应用的适度需要， 也避免少数人的下载导致其他客人无法正常发送e-mail或浏览网页的商务需求;非高峰期采取针对应用协议做级别差异化的优先级调度策略模式，完美解决了有限的出口带宽下两类客户不同应用需求之间的矛盾，显著降低酒店关于网络的投诉率；

2) 详尽的日志功能，满足相关部门对特定应用或特定事件的查询和审计要求，如配合公安部门通过QQ号码、POP3账号等信息对特定目标进行反查或相关取证。

➢ **ISP运营商**

1) 强化网络行为管理：根据各种应用业务的流量，制定相关策略限制非主流业务(例如可以对即时通讯、P2P 下载、网络游戏、网络电视等)在峰值时段进行限速、阻断，进一步规范用户上网行为，为人性化科学化管理提供基础保障。

2) 必要的安全防范机制：利用自身强大的性能优势，实时监控网络运行，识别阻断网络攻击，根据并发连接个数可以确定并阻断DOS攻击等异常行为,为小区ISP提供专门应对伪IP类木马攻击、IP碎片攻击等检测和防护机制保护网络设备安全；

3) 优化网络运行管理：通过检测分析带宽使用状况，合理分配带宽资源；

4) 提升用户满意度：通过合理调控高峰期P2P类应用的带宽滥用，提升常规应用的网络体验，减少用户投诉，更加有利于市场竞争；

5) 精确识别用户的网络应用，分析网络的流量走势、应用分布、用户分布，为网络的流量优化提供依据；

6.2 案例

网纵公司在政府政府、企业、教育、能源、运营商、网吧、酒店等行业积累了大量的客户，以下是部分客户列表：

政府	能源
交通部	
天津广电	佛山绿电能源
福州广电	广东燃气集团
广东中科院	贵州永贵能源集团
北京海淀区法院	缅甸镍冶炼有限公司
云南楚雄州政府	三一重工股份有限公司
四川内江市财政局	赞比亚谦比希铜冶炼有限公司
中国国际问题研究所	
运营商、ISP	**网吧、酒店**
中国电信	辽宁 21 世纪
中国移动	广东爱心网盟
中国联通	四川时空引擎
广州滢通网络	广东星空网盟
神州物联网络	山东鼎立网城
中国铁通集团有限公司	香格里拉酒店
北京光泽时代通信技术有限公司	格林豪泰酒店
浙江华数广电网络股份有限公司	陕西红树林连锁
吉林省网宽,沈阳创亿鑫数据网络	海南三亚商务酒店
四川艾普信息传播股份有限公司	四川云南今朝网苑
北京北大方正宽带网络科技有限公司	天津市西青区中北镇梦缘网吧
教育：	**企业**
福州大学	以岭药业
西安交通大学	中粮集团
华中师范大学	中通速递
福建师范大学	广东宽联集团
福建农林大学	北新建材集团
福建工程学院	珠海宣传易集团
福建中医药大学	珠海宣传易集团
昆明玉溪师范学院	正元国际包装集团
长沙交通职业学院	成都广视通有限公司
长沙机电职业学院	中国国际招标服务公司
湖南司法警官学院	桂林福达集团有限公司
解放军信息工程大学	四川安宁铁钛股份有限公司
丽江师范高等专科学校	广州维动网络科技有限公司
福建教育科研网络服务有限公司	方正宽带网络服务股务有限公司江门分公司

7 公司简介

广州网纵(Netzone)信息技术有限公司[简称：广州网纵]是业界领先的网络带宽优化与管理整体解决方案提供商，集研发、生产、销售于一体。 致力于为用户提供先进、可靠、最具性价比的网络应用层设备与解决方案。

公司总部位于广州天河 IT 中心，拥有北京、广州两大研发中心；生产基地位于深圳，在北京、上海、成都等多个城市设立分公司或办事处；现有员工 200 多人，公司有一批资深技术和项目管理专家，建立了规模化的产品研发、咨询、营销和服务体系，产品行销海内外 20 多个国家与地区，为客户提供最优质的产品和服务。

网纵拥有 35000 多家国内外用户，范围涉及政府、企业、教育、运营商、金融、能源、ISP、网吧、酒店等多个行业。

网纵人秉承“专业创新、诚信共赢”的理念，与全球合作伙伴携手共进，致力于帮助用户优化与管理好网络，提升网络应用价值。朝着成为国际领先网络应用层设备供应商和打造民族品牌的目标而奋进！

使命：提升网络应用价值

愿景：成为全球领先的网络应用层设备供应商

价值观：专业 创新 诚信 共赢 企业灵魂：

军队：是，保证完成任务；学校：学习无处不在；家庭：你的事就是我的事

广州网纵信息技术有限公司 Netzone.Inc

广州市天河区天河路 535 号保利中辰广场 A 座 908 室

电话：020-85509880 传真： 020-8550 9883

邮编：510630 网址： www.netzone.com

BBS ： bbs.netzone.com 企业 QQ： 4008-3311-23