

# Panabit 技术白皮书



北京三棱镜软件工作室

2007.07

## 目 录

1、前言 .....	3
2、产品背景 .....	4
2.1 P2P应用概况.....	4
2.2 P2P对网络的影响.....	5
2.3 P2P应用技术发展.....	5
3、处理P2P策略 .....	7
4、如何检测网络中的P2P流量 .....	8
5、技术解决方案 .....	9
6、系统架构 .....	11
7、主要功能特色 .....	13
7.1 强大的协议识别引擎 .....	13
7.2 灵活的带宽管理 .....	18
7.3 内网IP统计功能.....	20
7.4 简单易用的单IP限速.....	20
7.5 丰富的报表统计 .....	21
7.6 系统高可用性 .....	22
7.7 全中文化安全的Web管理 .....	22
7.8 灵活方便的部署方案 .....	22
附录一 Panabit部署方案 .....	23
1.1 透明网桥模式 .....	23
1.2 旁路监听模式 .....	23
附录二 典型案例 .....	25

## 1、前言

当前的 IP 网络，基于应用的分类管理，应用可视性和网络可管理性的地位比以前更重要，需求也更加迫切。P2P 应用的广泛流行，已是桌面应用和网络流量的主流。出于技术与市场的驱动，唯有专业的应用层流量管理产品，才能跟踪并分析网络/用户的流量模式，更加有效的管理网络带宽资源，并加强服务特色化，管控结合，提高网络运行效率，提升用户满意度和忠诚度，具有多方面的益处。

P2P(Peer-to-Peer)应用是不需关照的下载方式，增加网络峰值带宽和峰值持续时间，使用随机端口 (port-hopping)，流量普遍占到网络总流量的 60% — 80%，为了让用户更快的体验和畅通无阻，则极力争抢带宽和逃避监管。由于使用随机端口，传统的基于端口来区分应用的方式就失去了作用。

Panabit 是在 P2P 流行时代，诞生的新一代应用层流量管理产品，支持对 IP 流量的应用分类，实时控制用户组、应用服务流量。Panabit 的解决方案是基于状态和特征检测，精确识别 9 大类 80 余种常用协议，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方便快捷。

应用分类中对 P2P 应用的分类是关键，主要是由于 P2P 的特性所决定，BT 等 P2P 应用由于其独特的设计理念，在客户端软件中加入了大量对抗网络封堵、限制的技术手段；识别 P2P，既不能误判也不能漏判，否则就不能达到真正对应用流量的带宽限制或保证。很多非专业产品，通过限制 TCP 并发连接数的方法控制 P2P 并不科学，容易影响其他正常流量的速度。Panabit 经过 3 年的技术积累和实践，以应用特征识别与控制，是一款真正的应用层流量管理产品。

处理应用分类控制，处理 P2P 识别和控制，不但要求识别准确性，而且要求实时性能，Panabit 一般是作为网关类设备部署在网络出口，对时间延迟提出了更高的要求。在识别技术方面，Panabit 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。

Panabit 从基础软件架构上，就充分考虑应用层处理的特性，专为处理应用层识别

与控制设计了 PanaOS，Panabit 使用 Intel x86 硬件平台，相比起同等级用 ASIC、NP 硬件处理的产品，具有成本低、性能高、升级灵活等优势。Panabit 的特色是：专业的协议特征库，并有先进的更新维护机制，同级硬件的整体性能高，处于国内领先水平，Intel x86 单核性能完全满足千兆线速。

使用 Intel 架构硬件系统和 Panabit 软件引擎，满足单台处理 2G 流量的专业性能，得益于 Intel CPU 和 PCI Express 总线技术发展，为发展高端产品带来了良好的硬件平台，硬件不再是瓶颈，关键是软件技术。Panabit 高端产品，通过使用多颗多核 CPU 实现，在成本、性能、产品更新周期方面，具有很强的竞争优势。

## 2、产品背景

### 2.1 P2P 应用概况

P2P 技术，即端到端对等网络技术，是指网络主机在充当客户端获取资源的同时充当服务器向其它对客户端提供服务。

随着计算机网络的广泛应用和多媒体资源的丰富，带宽消耗越来越大。在计算机网络发展史上，恐怕没有任何一种网络应用像 P2P（Peer-to-Peer，端到端对等网络）技术这样深刻的影响了宽带网络服务的运营模式。P2P 使文件下载共享变得简单，动辄 GB 级的电影下载，P2P 应用拉动的带宽消耗增长，据统计，P2P 数据流量占因特网总流量达 80% 以上，并且在用户总数没有显著增长的情况下，P2P 数据流量仍然在快速持续增长，使得宽带运营商的成本增加，收益降低，网络效率和服务质量下降，甚至冲击其他业务收入。

短短几年，P2P 技术迅猛发展，以 P2P 技术为核心的软件产品，雨后春笋般的进入了主流计算机应用，事实已经十分明显。如基于 P2P 协议的文件下载共享软件，典型的应用软件有 BitTorrent、eDonkey、PP 点点通、Gnutella、FastTrack、酷狗(Kugoo)、迅雷、DirectConnect、AppleJuice、百宝、百度下吧、百兆等。这是目前被广泛使用，同时也是头号带宽杀手的应用协议。基于 P2P 的其他应用有：即时信息类，如腾讯 QQ、微软 MSN、YahooMessger 等，网络电话类，如 Skype 等，网络电视类，如 PPStream、PPLive、沸点、Recool、QQLive 等。

运营商网络中 60%—80% 的带宽夜以继日地被这些应用占用。由于传统网络监控

设备无法识别 P2P 应用，处理 P2P，必须是针对 P2P 应用的流量管理系统，才能监测网络并找到正在运行的 P2P 应用以及谁正在使用这些应用，然后设定策略以保证所有用户的公平性，还可以追踪使用情况以便于记帐和微调网络，处理过多的流量并把昂贵的空闲带宽分配给那些能够创造利润的应用。

## 2.2 P2P 对网络的影响

P2P 技术主要提供了分布式交换数据的能力，由于个人用户 PC 的处理能力和硬盘空间逐步增大，资源分布存储已经变为可能。P2P 技术现阶段最大的用途就是提供了在个人用户之间交换数据文件，通过集中资源服务器已经不在是资源存放的唯一途径。

P2P 技术主要带来了如下一些变化：

(1)Internet 上流量模型的变化：现在 Internet 上 60%—80% 的流量都是 P2P 的流量，而传统的 HTTP 流量已经不是 Internet 上的主要流量。

(2)个人用户的流量模型的变化：以前个人用户的下行流量(从 Internet 到个人用户)远远大于上行流量。而由于 P2P 技术在下载的同时，也需要上传。导致个人用户的下行流量和上行流量都很大。

(3)P2P 应用获取带宽的方式可谓完美：使用“永远在线”的技术日以继夜地在进行贪婪的下载和上传服务，P2P 流量造成网络的极度拥塞。

## 2.3 P2P 应用技术发展

### 第 1 代集中式的 P2P 应用：

Napster 模式，在对等计算机上运行的这类应用通常使用一个固定的 TCP 端口，这种模式从管理员角度来看，第一代的 P2P 应用是比较容易处理的，管理员可以简单地使用可根据协议端口监测网络的防火墙或者路由器限制 P2P 应用的流量。

免费(Free)文件共享理念被保留下来，分布式更易于通信，被用户接受和追捧，在这个模式的驱动下，产生了大量新的、难于控制的 P2P 应用。

### 第 2 代分布式 P2P 应用：

允许计算机能够在任何时间、任何地点连接到其他计算机，而不需要中心服务器的干涉，所有的对等计算机直接对其他的对等体进行响应和文件共享。

第二代 P2P 应用采用的方法中还包括一些用于规避网络安全设备的“技巧”：

(1)端口跳跃：通过这种方法，P2P 应用将不再使用一个固定的端口号，而是采用随机的或者是用户手工设定的协议端口号。

(2)常用端口号：一些 P2P 应用使用 80 端口——官方规定的 HTTP 协议端口，来避开防火墙的限制，获得对 Internet 的访问。这是一种很狡猾的做法，因为企业通常只开通特定的、常用的端口(如 80 端口)访问 Internet；类似地，一些运营商还对 80 端口提供更优化的流量，因为这些流量被认为是来自 HTTP 访问 Web 的。

(3)HTTP 隧道：在很多企业网络中，Internet 的访问是通过 HTTP 带来完成，对于非 HTTP 应用或者未经过 HTTP 的应用将不能访问 Internet。于是很多 P2P 应用将 HTTP 协议作为自己基本协议，这样就避开了这些限制，使得网管设备的限制实效。

(4)HTTP 代理隧道：P2P 客户端将要发给 Web 边缘的对等计算机的流量使用隧道技术进行封装，通过代理(如 Socks 代理)和一些第三方的隧道应用(如 Socks2HTTP)，使 P2P 流量看起来像是标准的代理流量，而这些流量通常是不被限制，从而达到避开限制。

对于这些应用的识别和控制是非常困难的，除非借助应用层可视性检测工具，检查传输协议(如 TCP 协议)的载荷 (Payload) 部分，对不同的应用进行更精确的识别。

### 第 3 代 P2P 应用：

第 3 代 P2P 应用是一种介于集中式和分布式结构之间的混合折中结构。这一类型的网络使用“超级对等体”(超级节点)来充当中心服务器的角色，一方面维护网络的分布式结构，一方面保证良好的搜索点击率、网络速度和可伸缩性。超级对等体是从众多对等体中随机选择，甚至被选择的对等体自身对此也不会有所察觉。超级对等计算机向为数不多的一组对等计算机提供索引服务，同时超级对等体之间也彼此进行通信，文件传输在对等计算机之间直接传输。通过限制处理搜索的对等计算机的数量，同时也消除了使用固定、专用服务器带来的延迟，该类型的网络在提供很高的搜索性能的同时，也继承了分布式网络的特性。某些第三代 P2P 应用使用 SSL 协议(如 HTTPS，是用于加密 Web 流量的协议)对流量进行加密保护。

### 第 4 代 P2P 应用：

P2P 应用最新发展的一个趋势,典型代表有 Skype、eMule 0.47c 和 BitComet 0.80。这一代的 P2P 应用从技术上看,主要有两个特点:

(1) 通过增加无用随机数据和数据进行加密这两个手段使得协议流量特征模糊化,如最新版的 eMule、BitComet 等软件。

(2) 多协议并用(如迅雷, HTTP、FTP、专用协议并存),逃避监管。

日益复杂精巧的设计和开发, P2P 新应用不断涌现,功能更强也更易使用,为了使 P2P 应用运行畅通,新一代 P2P 软件比上一代越来越智能,其中主要是 P2P 应用由于其独特的设计理念,在客户端软件中加入了大量对抗网络封堵、限制的技术手段,使得 P2P 流量管理检测难度水涨船高,同时需要不断升级协议特征库。P2P 应用使人们对使用 Internet 的方式发生着革命性的改变, P2P 应用的潮流不可阻挡,只能顺应潮流,采用有效处理策略。

### 3、处理 P2P 策略

为了能够控制 P2P 应用,企业与网络运营商都各自尝试了不同的解决方案:

#### 扩充带宽:

最简单显而易见的解决办法,就是扩带宽。

优点:增加带宽可以在短时间内缓解网络的拥塞状况,当 P2P 应用觉察到网络中有更多的可用带宽,网络带宽将会再次被 P2P 应用占据。

缺点:增加带宽和增加带宽的费用将是无底洞,这样做只是给 P2P 应用提供了更多可攫取的带宽资源。

#### 禁止 P2P:

全面禁止 P2P 应用将会是拥塞的网络恢复正常状态。

优点:企业可以禁止 P2P 的使用,提高员工的工作效率,而以往员工却花费时间和网络带宽进行娱乐性的网上冲浪。

缺点:ISP 将会失去用户,因为很多用户就是为了不受流量限制才租用了运营商的线路。

#### 限制,而不是禁止 P2P:

使用能够识别第 7 层应用的流量管理解决方案,企业和运营商能够准确判别 P2P

应用并进行限制。

优点：可以通过多种控制策略进行，通过合理调配带宽资源，提高网络运行效率，如发生链路拥塞的情况下，减少分配给 P2P 应用的带宽或者降低 P2P 应用的优先级，保证同一服务级别的用户使用网络的公平性，将会大大改善网络响应速度质量。当对 P2P 应用流量进行限速管理之后，网络中的其他应用将变得很顺畅。

#### 仅对上传进行约束：

对于 ISP 来说，这种约束能力显得更为关键，因为对于那些非线路租户使用其他租户的线路上传(而并不承担相关费用)的情况尤为关注。运营商显然不会考虑这些非线路租户进行线路的升级，这也就是为什么选择限制上传流量的原因。

优点：对上传流量进行限制并不会影响到下载流量。如某运营商对 P2P 应用的出向流量进行了限制，而这个方向的流量主要是由非线路租户产生，由于他们自己的线路租户的 TCP 确认信息并不会受到影响(尽管它们的方向也是向外发送)，就可以继续享受无限制的下载服务。通过这项控制，该运营商用户的流量消耗得到了显著减少，成本大幅度下降，又保证了客户的满意度。

由于流量管理产品具有足够的灵活性，可以在不影响下载的前提下限制上传流量，从而使所有人都能获益：线路租户可以根据自己需要随意下载，运营商也得益于需要支付给骨干网络运营商的成本的大幅度下降。

缺点：无。

## 4、如何检测网络中的 P2P 流量

为了能从应用中把 P2P 应用识别出来，网络可视性（Network Visibility）是至关重要。这种检测能力将了解到在当前的网络中运行着哪些 P2P 应用、哪些 P2P 应用正在吞噬网络中的宝贵资源、哪些用户占据了过多的网络资源从而造成了网络的拥塞。当检测和分离这些流量之后，就可以对 P2P 应用进行限制或者阻止、或者为其他的应用或用户分配和保证所需的带宽，或者把 P2P 应用的流量避开峰值时段，合理调配带宽使用，从而利用现有的带宽资源，最大限度地提高带宽的效率。

#### 深层数据包检测(DPI):识别 P2P 应用的唯一可靠办法：

对 P2P 应用进行判定，需要借助复杂的第 7 层识别技术，使用各种方法来检测这

些难以捉摸的应用。由于多数 P2P 应用软件都使用端口跳动技术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。因此，所有的数据包都必须到应用层面（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代码的样本特征，在很多情况下，对于某一种应用的识别需要检测它是否多个代码样本的特征。

#### 基于会话的应用分类：

标准的协议头部(Header)字段如 TCP/UDP 的端口号字段在每一个数据包中都存在，而第 7 层的协议代码样本通常只能在一次协议会话的前几个数据包中存在，并进行会话标记的请求以标识本次会话中所有的数据包。当网络中产生了一个新的会话，如 P2P 应用会话，那么一个唯一的协议签名(Signature)就必须被找到并能够与已知的协议代码样本相匹配，如当使用第 7 层的分类方法对一个 P2P 应用进行了正确的识别，那么该会话中的后续数据包就能够被正确的判别为该 P2P 应用会话的数据流量。

有些情况下，一个 P2P 应用使用不止一个会话，这就需要流量管理系统能够从两个或多个会话中提取信息并进行关联以找到能够匹配的代码样本。

#### 并非基于端口的分类：

P2P 应用通常使用随机的端口号或者借助一些常用的端口号来进行传输，因此在进行 P2P 应用样本搜寻时，就不能做任何的假设，需要对网络中所有数据流进行第 7 层协议的探测，而不管它们是否使用了某个端口号。

#### 每秒连接数：

不寻常的连接数量可能是在暗示着网络中 P2P 应用的使用，也可暗示着异常流量的存在，如病毒、蠕虫、有害程序等等。P2P 是具有侵略性的应用，它可以在短时间内建立超负荷的连接，异常的连接数量在流量管理设备中可以设定告警机制，帮助网络管理员及时解决问题。

## 5、技术解决方案

针对 P2P 应用的流量管理特点，检测、性能和系统稳定性这三个因素是至关重要。不能正确检测区别 P2P 流量，就不能进行管理控制。性能不能满足要求，没有足够的处理能力，造成网络延迟的增大，同样也是无效。

下面简要介绍一下 Panabit 检测与控制 P2P 系统所使用的独特的应用层识别技术，在此之前，我们先介绍一下目前在其它产品中常用的技术：

**(1)基于数据包的无状态识别技术。**这种技术一般是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。

**(2)基于连接的有状态识别技术。**这种技术是一般的传统防火墙所采取的技术。在防火墙现有的状态表的基础之上，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。所以，如果该特征是 BT 通信，那么这条连接就是两个 BT 客户端或一个 BT 客户端和一个 BT 服务端在通信。

在运营商的网络环境里，由于节点一般都是网络交换节点，因此许许多多的 P2P 节点的通信都会通过运营商的交换网络，这些节点以十万，甚至百万计。如果采取基于连接的有状态识别技术，所能控制的 P2P 通信非常有限，这种技术只适合于小规模的网络，如中小企业网络。

**Panabit 采用“基于节点的有状态识别技术”可以避免上述问题。**

一个典型的 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。基于节点的有状态识别技术的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。P2P 应用中，客户端既是客户，又是服务器，在某端口上监听为其他客户提供服务，根据这一特性，将 IP+服务端口在内存中定义一个二元组，称之为节点。

Panabit 在基于节点的有状态识别技术的基础上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，Panabit 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。Panabit 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，Panabit 开发了独有的服务伪装引擎。

从技术角度看，P2P 应用有如下几个特点：

(1)一个 P2P 节点（客户端程序，比如 BitComet）通常与成百上千个客户端连接，因此节点之间的连接数目巨大。假如一个节点有 200 条连接，那么 10000 个节点就有可能达到 200 万条连接，保守估计也会有 100 万条连接，如此大的连接数将使设备不堪负担。

(2)不像 Web 浏览这样的 HTTP 协议，HTTP 连接一般持续的时间比较短，而 P2P 主要目的是用来共享大的文件，需要传送大量的数据，因此 P2P 客户端之间的连接一般持续的时间比较长，这就意味着系统的资源很长时间不能得到释放，因此大大增加系统被 DOS(Deny Of Service, 拒绝攻击)的机会。

针对上述特点，Panabit 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，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。

## 6、系统架构

Panabit 核心是 PanaOS(Panabit Operating System)，PanaOS 基于 FreeBSD(目前最稳定的操作系统)，但是在原有 FreeBSD 基础上做了如下修改和增强：

(1)对网络协议栈作了大量的修改和优化，使得数据平面(Data Plane，见下图)能够以最快速度执行。

(2)去掉内核部分代码，使得核心更小。

(3)针对特定的硬件进行优化，使得在特定的硬件上更快运行。

(4)修改部分中断处理函数和网卡驱动，使得数据平面(Data Plane)以较高优先级运行。

PanaOS 分为数据平面（Data Plane）和控制平面（Control Plane）两个部分：

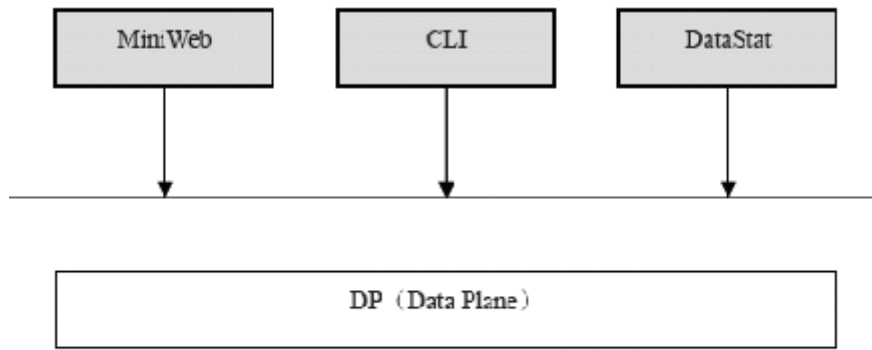
**(1)数据平面(Data Plane):** 负责数据包处理，同时提供同控制平面的接口。数据层面直接由硬件驱动，这样避免了传统 OS（包括 FreeBSD）的网络协议栈带来的开销，使得 PanaOS 能够充分利用硬件的性能而更快处理数据包。数据平面在 PanaOS 内核内运行。

**(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 PanaOS 的应用层。

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(CP, Control Plane)

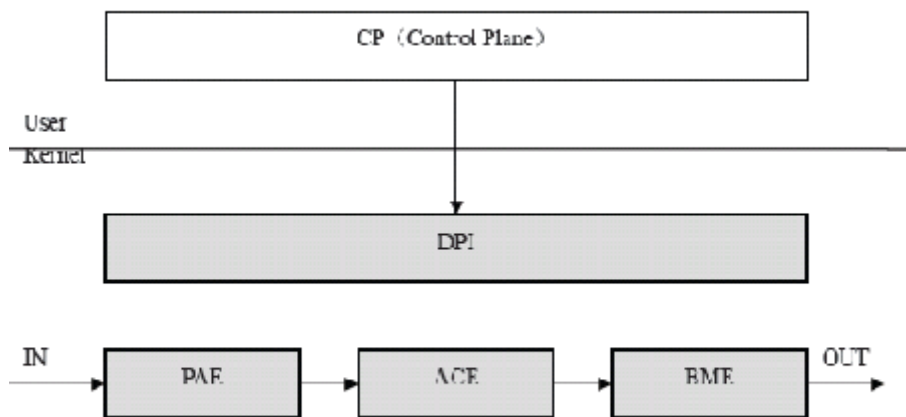


控制平面组成 (粗线部分)

其中:

- (1)MiniWeb: 一个轻量级的 Web 服务器，并提供 Web 管理接口。
- (2)CLI: 命令行接口进程。
- (3)DataStat: 负责数据的收集和统计分析。

### 数据平面(DP, Data Plane)



数据平面组成 (粗线部分)

其中：

(1)PAE(Packet Analysis Engine): 数据包分析引擎，负责应用层识别。

(2)ACE(Access Control Engine): 访问控制引擎，负责访问控制。

(3)BME(Bandwidth Management Engine): 带宽管理引擎，负责带宽限制和分配。

(4)DPI(Data Plane Interface): 数据平面接口为 CP 提供访问数据平面的数据和相关状态信息的接口。

## 7、主要功能特色

Panabit 主要功能模块有：

- (1) 强大的协议识别引擎
- (2) 灵活的带宽管理
- (3) 内网 IP 统计功能
- (4) 简单易用的单 IP 限速
- (5) 丰富的报表统计
- (6) 系统高可用性
- (7) 全中文化安全的 Web 管理
- (8) 灵活方便的部署方案

下面分别详细介绍上述模块：

### 7.1 强大的协议识别引擎

Panabit 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 0.47c。到目前为止，Panabit 已经支持如下协议：

1)传统协议: HTTP, HTTPS, FTP, Telnet, SSH, DNS, SMTP, POP3, NetBIOS, CVS, DHCP, NTP, NFS, NNTP, SNMP, TFTP, BGP, HTTP 分块传输, 伪 IE 下载, Microsoft-DS, Remote-sync。

2)流媒体协议: RTSP, MMS。

3)P2P 下载: BitTorrent, eMule, Gnutella, Kazaa, iMesh, DC, AppleJuice, Ares, Mute, SoulSeek, POCO, 酷狗, 迅雷(含 Web 迅雷), 百宝, 百度下吧, Vagaa, 脱兔, PPGou。

4)即时通信: MSN, MSN 视频, YahooMessger, QQ, QQ 视频, QQ 文件传输, 网易泡泡, 淘宝旺旺, 新浪 UC。

5)网络电话: Skype。

6)网络电视: PPStream, PPLive, 沸点, Recool, QQLive, TVAnts, TVKoo, PPMate, MySee, UUSee, CCIPTV, SopCast, VJBase, JeBoo。

7)网络游戏: 魔兽世界, 奇迹世界, 征途, 热血江湖, 跑跑卡丁车, QQ 幻想, 泡泡游戏, QQ 游戏, , 中国游戏中心。

8)股票证券: 大智慧(经典版、新一代)、钱龙(经典版、旗舰版)、核新(同花顺 2007)

注: 应用协议的支持更新, 请参考 [www.panabit.com](http://www.panabit.com) 首页支持协议更新列表。

系统运行效果图:

#### 网络统计—>协议统计

请选择协议或协议组		P2P下载		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
eDonkey	120	900	16394	5801	1324389738573	728578949053	30.96		
脱兔	120	600	4474	0	839086979859	792922578468	24.61		
Bittorrent	120	600	63836	2	820816531948	485818728016	19.71		
Vagaa	120	600	935	0	626051825794	361849167559	14.90		
迅雷	100	600	1382	0	293115690485	279577509557	8.64		
酷狗	120	600	71	0	11311804336	25864398119	0.56		
PPGou	120	600	0	0	5093126267	13182085517	0.28		
Poco	120	300	102	0	7217966719	8468489019	0.24		
Gnutella	120	600	5	0	742127879	2147910936	0.04		
百度下吧	120	600	0	0	830333821	1299691796	0.03		
百宝	120	600	0	0	621112781	1320429106	0.03		
SoulSeek	120	600	0	0	1194768	6919232	0.00		
Napster	120	600	0	0	0	0	0.00		
Mute	120	600	0	0	0	0	0.00		
iMesh	120	600	0	0	638904	974332	0.00		
Fasttrack	120	600	0	0	317	60	0.00		
DirectConnect	120	600	0	0	0	0	0.00		
Ares	120	600	11	0	34508268	84733971	0.00		
AppleJuice	120	600	0	0	0	0	0.00		

流量统计

连接统计

节点统计

## 网络统计—&gt;协议统计

请选择协议或协议组		网络电视		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
PPLive	120	600	78032	4371	1348097712516	838592195282	48.67		
QQ直播	120	600	1742	0	743636307729	306683252691	23.38		
PPStream	120	600	1281	0	712599295282	297808617590	22.49		
悠视TV	120	600	27	0	73195787531	63911999070	3.05		
沸点	120	600	14	25	18502460099	19623023521	0.85		
TVKoo	120	600	166	0	20858095746	12619985192	0.75		
PPMate	120	600	0	0	13011345700	5954442984	0.42		
SopCast	60	600	0	0	8980254412	2822062916	0.26		
TVAnts	120	600	0	0	2268701068	2183161761	0.10		
CCIPTV	120	600	0	0	211659554	885427949	0.02		
Jeboo网络电视	120	3600	0	0	233701976	338970130	0.01		
VJBase	60	600	0	0	0	0	0.00		
乐酷	120	600	0	0	0	0	0.00		
MySee	120	600	0	0	61108	94055	0.00		

流量统计    连接统计    节点统计

## 网络统计—&gt;协议统计

请选择协议或协议组		传统协议		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
HTTP	120	600	2237	0	655464220840	3967088125264	72.86		
HTTP分块传输	120	600	28	0	59672764034	1050799602448	17.50		
FTP	120	600	27	5	24037808019	221259013734	3.87		
伪IE下载	120	600	4	0	16056086915	212863504407	3.61		
HTTPS	120	600	113	0	28359839465	55612797856	1.32		
SMTP	120	600	5	0	16549671045	3505187316	0.32		
DNS	120	600	457	0	4814700430	8276085188	0.21		
POP3	120	600	1	0	553470643	10850439642	0.18		
NFS	120	600	6	0	845569454	2124931567	0.05		
SSH	120	600	1	0	1727404241	956059151	0.04		
Telnet	120	600	2	0	496726389	937085294	0.02		
SNMP	120	600	237	0	315395241	1026290517	0.02		
TFTP	120	600	0	0	1122960	622077	0.00		
Remote-Sync	120	600	0	0	702	1442	0.00		
NTP	120	600	44	0	39759599	49810713	0.00		
NNTP	120	600	0	0	3676550	43921264	0.00		
NETBIOS	120	600	0	0	13133719	46048	0.00		
Microsoft-DS	120	600	0	0	0	0	0.00		
DHCP	120	600	10	0	6761728	85855004	0.00		
CVS	120	600	0	0	38008	133221	0.00		

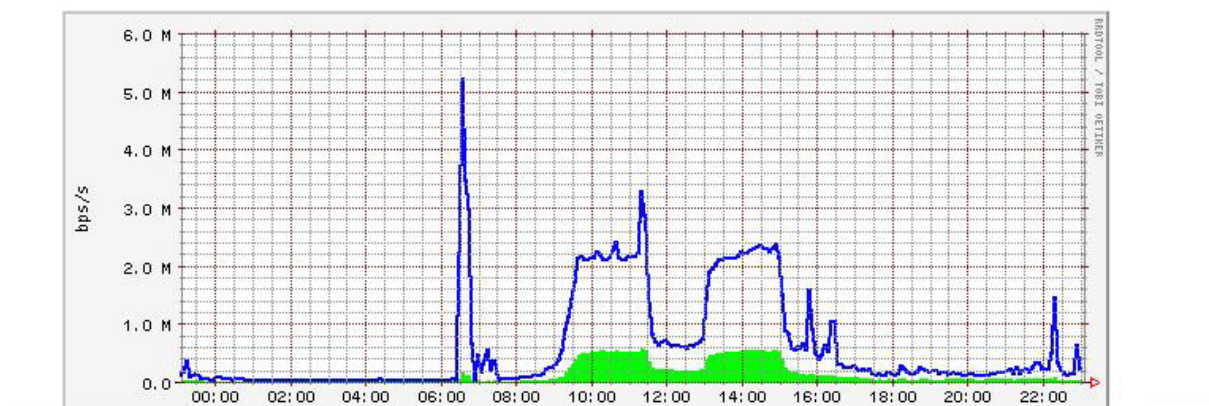
## 网络统计—&gt;协议统计

请选择协议或协议组		股票交易		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
同花顺	300	36000	106	582	8681547828	32673211054	55.49		
大智慧	120	600	20	5	2476594584	15220849280	23.75		
钱龙系	120	600	6	1	7330171315	8140662879	20.76		

流量统计 | 连接统计 | 节点统计

更新时间 2007-07-31 23:04:46

## 最近一天趋势图



## 网络统计—&gt;协议统计

请选择协议或协议组		即时信息		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
QQ	120	36000	1779	408	177342563299	29185039853	55.88		
QQ视频聊天	120	600	10	0	50573407771	65468431748	31.40		
QQ文件传输	120	600	5	0	17781724735	12726765517	8.25		
MSN	120	600	141	0	4006474721	10535372774	3.93		
新浪UC	120	600	21	0	220561043	615237671	0.23		
淘宝旺旺	120	600	56	4	259575702	388506352	0.18		
MSN视频聊天	120	600	4	0	65779241	143936550	0.06		
网易泡泡	120	600	7	0	46556754	154380827	0.05		
阿里旺旺	120	7200	0	0	12033484	65885323	0.02		
雅虎通	120	600	3	0	6474856	5405635	0.00		

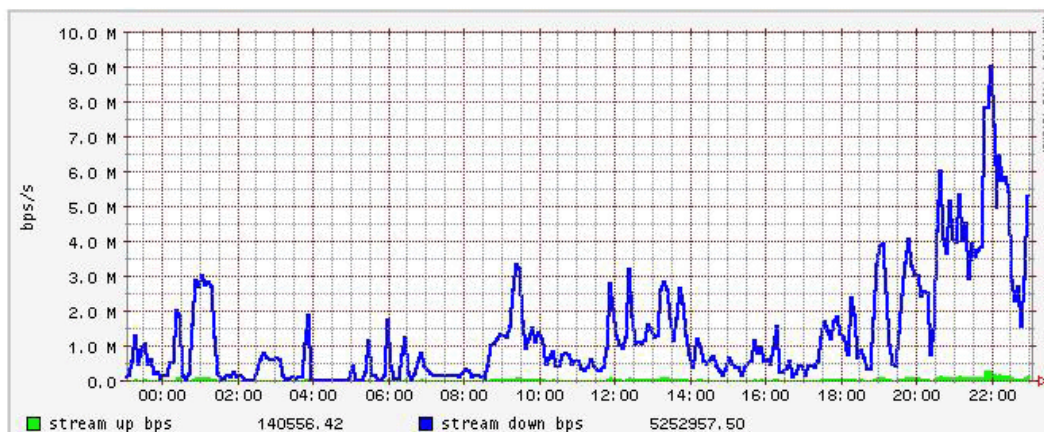
流量统计 | 连接统计 | 节点统计

## 网络统计—&gt;协议统计

请选择协议或协议组		流媒体		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
RTSP	120	600	3	0	4134380074	146313074383	76.81		
MMS	120	600	14	0	1145806948	44276260844	23.19		

更新时间 2007-07-31 23:03:04

## 最近一天趋势图

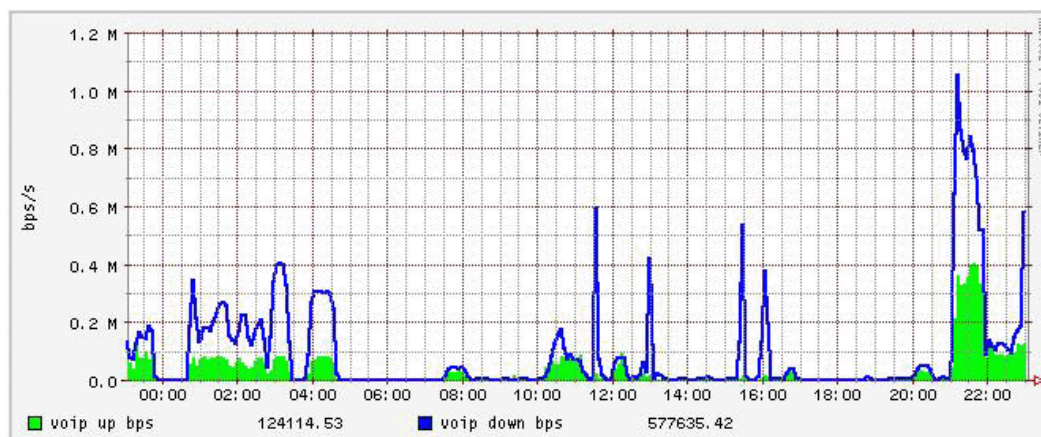


## 网络统计—&gt;协议统计

请选择协议或协议组		网络电话		请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)		
Skype	120	1200	61	735	4283598070	7723532779	100.00		

更新时间 2007-07-31 23:03:46

## 最近一天趋势图



## 网络统计—&gt;协议统计

请选择协议或协议组		网络游戏			请选择刷新频率(秒)		不刷新		提交	
协议	会话TTL	节点TTL	会话数	节点数	上行流量	下行流量	百分比(%)			
QQ游戏	120	600	4	0	1313143308	21331752762	46.87			
征途	120	600	11	2	2035646754	7970078953	20.71			
魔兽世界	60	600	7	0	1871158932	7904106436	20.23			
热血江湖	120	600	1	0	368704809	2397596173	5.73			
跑跑卡丁车	120	36000	2	0	261158200	1604555854	3.86			
中国游戏中心	120	600	1	0	63907267	953825575	2.11			
泡泡游戏	120	600	0	0	59455747	78831703	0.29			
QQ幻想	120	36000	0	0	27780108	69960016	0.20			
奇迹世界	120	600	0	0	28242	30354	0.00			

流量统计    连接统计    节点统计

## 7.2 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。

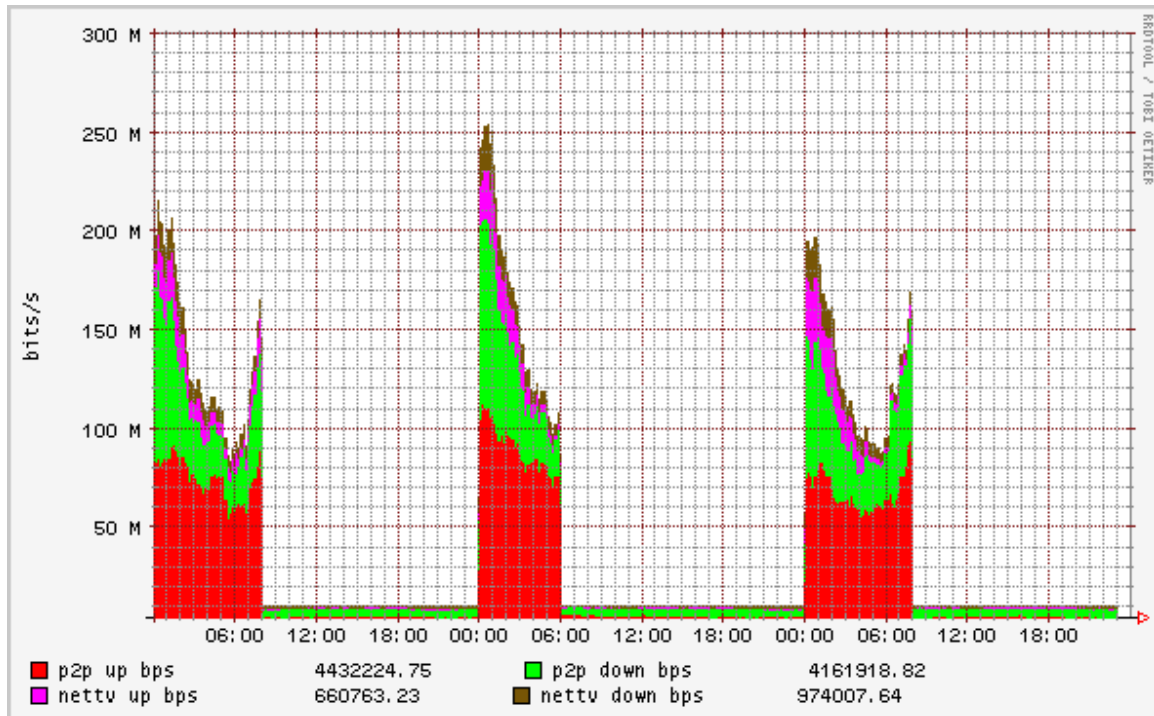
与类似产品单纯通过对 P2P 及其他特定流量进行带宽控制来变相“保障”正常应用的方式不同，Panabit 同时提供基于应用或基于 IP 的“带宽控制”、“带宽预留”、“带宽保证”三种机制，为用户灵活调控网络带宽资源提供更方便的功能。

**在精确识别应用协议的前提下，Panabit 提供以下三种带宽调控机制：**

(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，Panabit 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(2)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 Panabit 就会从其余的 90M 带宽中借出 5M 给该 IP 组以满足其使用。

对于运营商，在 P2P 应用已成潮流的现实背景下，运营商已不单纯着眼于如何控制 P2P 流量来控制带宽成本和运营压力，而是逐步寻求通过 P2P 增值运营来实现收益。在很多地方，运营商自主开办的 IPTV 同样也是依赖于 P2P 技术，那么对于运营商来说，能对该 IPTV 进行带宽预留或带宽保证就更具现实意义；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；对于特殊行业（比如网吧），盈利主要来自于网络游戏与 QQ 视频聊天等消遣娱乐型应用，对这些盈利性的应

用进行带宽保证，同时对大量占用带宽的 P2P 下载进行带宽限制，限制与保证结合，可大幅度提升网络的整体性能和用户满意度。

Panabit 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分配和调度。

(2)**策略**：策略是用来将流量进行分类的机制。Panabit 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。

### 7.3 内网 IP 统计功能

(1) 用户可在 Web 界面中选择是否打开内网 IP 统计功能。

(2) TOP N 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

(3) 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。

### 7.4 简单易用的单 IP 限速

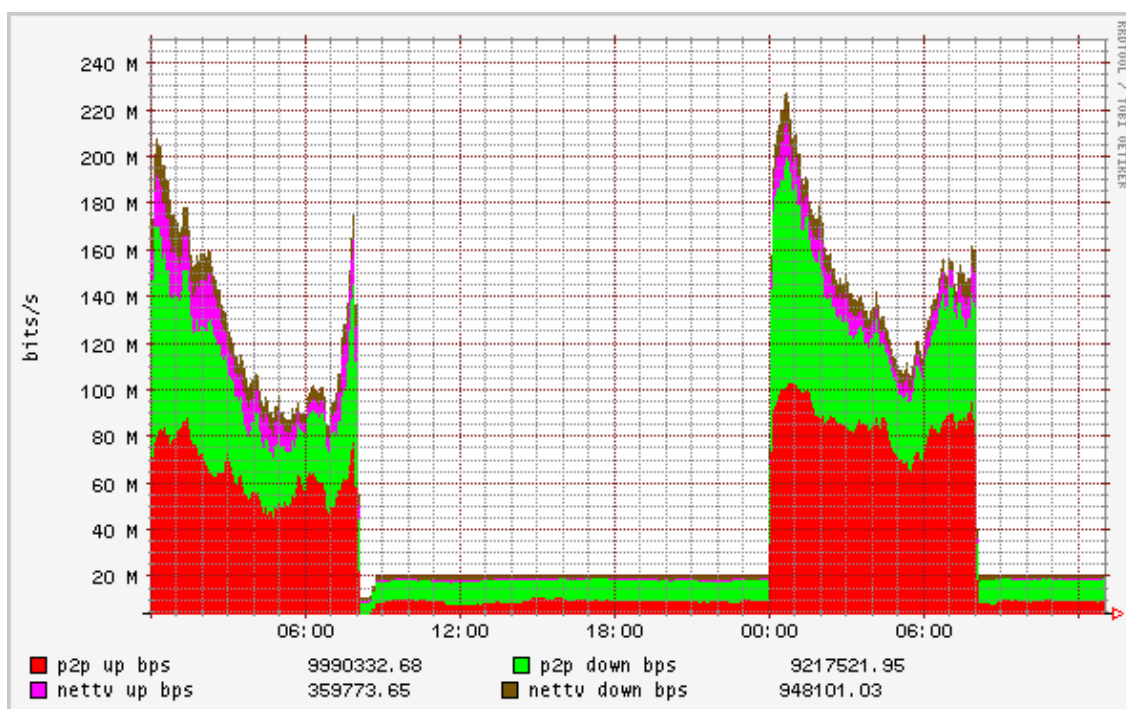
得益于其灵活的策略管理功能和带宽管理能力，Panabit 可以对内网 IP 进行单独限速。在 Panabit 中，只需要一条规则就可以实现控制某个网段内的每个 IP 最大可使用带宽和该网段的总带宽。

## 7.5 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

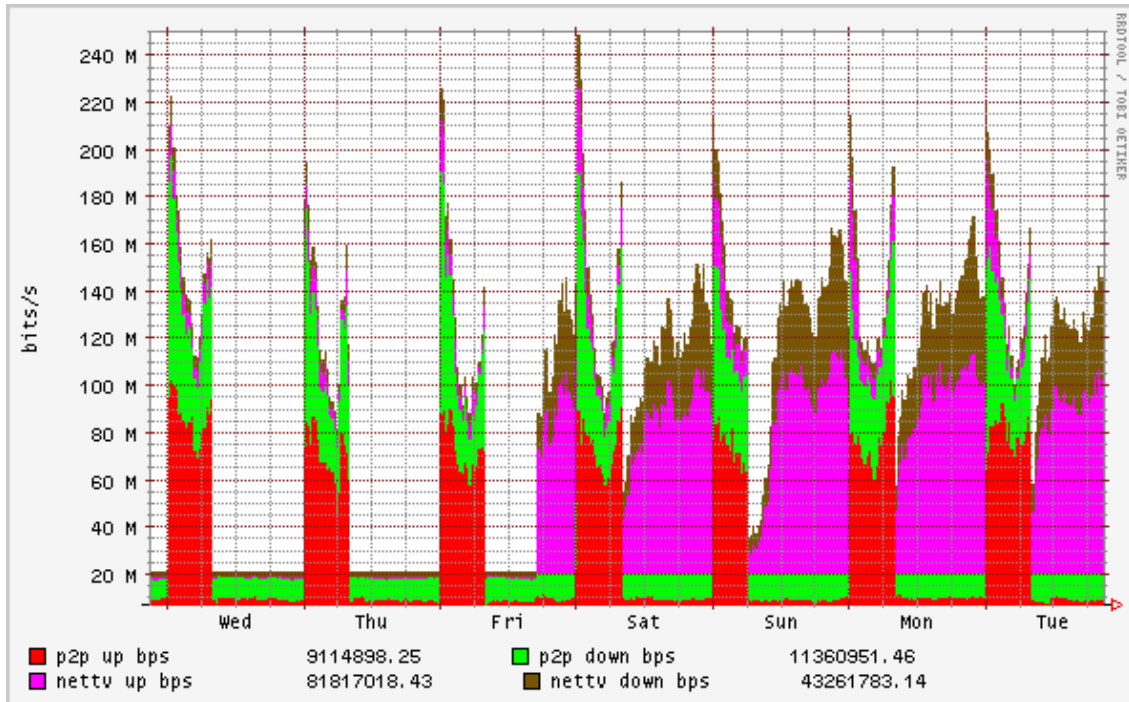
用户可针对自己关心的 IP/IP 组、应用协议/协议组等不同的对象自定义一个报表，将针对多个对象的统计结果集中显示在一个图表中，减少日常监控的工作量。统计数据可以指定不同的线形和颜色以绝对值或叠加的方式显示。报表统计的时间跨度可以是当天、本周和当月。

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。



P2P 与 NetTV(网络电视)流量的日图表

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。



P2P 与 NetTV(网络电视)流量的周图表

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)，同样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。

## 7.6 系统高可用性

支持硬件 Lan Bypass 功能，当断电、硬件故障、系统死机等，系统自动切换到 Lan Bypass 状态，保持网络连通。

## 7.7 全中文化安全的 Web 管理

所有配置管理都通过 HTTPS 方式的 Web 界面进行，使得管理员可以随时随地安全的管理系统。

## 7.8 灵活方便的部署方案

Panabit 支持两种接入和部署方案：

(1)旁路监听；(2)透明网桥。

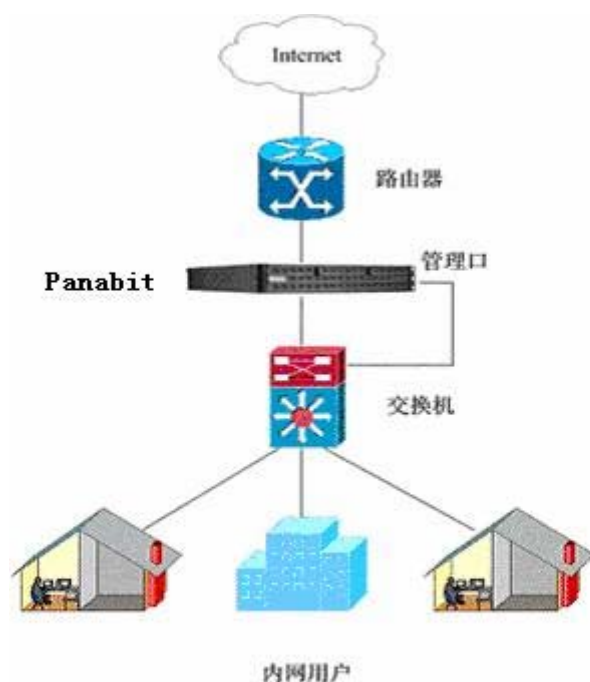
## 附录一 Panabit 部署方案

### 1.1 透明网桥模式

Panabit 以透明网桥方式部署在出口链路上，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 Panabit 遭受扫描、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 Panabit 进行配置管理。

典型的部署方式如下图所示：

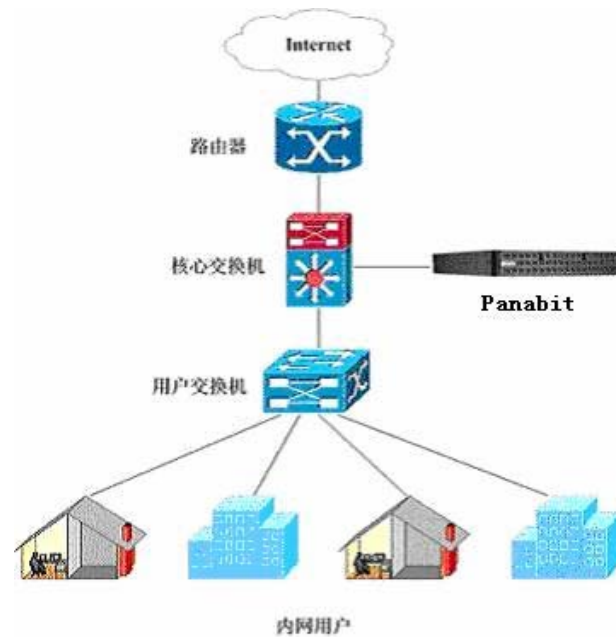


使用透明网桥模式接入，用户既可以统计流量，又可以做访问控制和带宽管理。

### 1.2 旁路监听模式

Panabit 设备以旁路方式部署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。（注：旁路监听模式下，Panabit 只能对流量做分析统计，而不能做控制。）

典型的部署方式如下图所示：



采用监听模式接入，Panabit 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，最后以透明网桥或透明网关模式将 Panabit 接入到网络中。

## 附录二 典型案例

### 宽带网络运营商：

- 1) 控制网络运营成本：选择性限制高耗带宽流量，确保正常业务的带宽资源；
- 2) 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；
- 3) 保障网络稳定运行：监测、分析网络数据，优化网络传输效率；
- 4) 提高网络服务质量：通过对带宽的合理规划，错峰峰值，保障网络畅通。

### 企业网和校园网：

- 1) 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；
- 2) 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，规范员工或师生的上网行为；
- 3) 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；
- 4) 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，保护网络设备安全。