

Panabit 协议识别与控制引擎 — P2P 控制解决方案



北京三棱镜软件工作室

2007.07

Panabit ?

- ◆ 国内最专业的协议识别与控制引擎
- ◆ 精确协议分析与流量管理
- ◆ 基于应用的分类与控制
- ◆ P2P控制解决方案
- ◆ 带宽保证解决方案
- ◆ 流控设备的最佳OS



Panabit Inside

Panabit Your Net !

基于应用分类的控制需求

- ◆ 传统QOS设备无法对应用进行区分
- ◆ P2P流行，须应用层正确识别区分
- ◆ 带宽限速和带宽保证，基于应用的控制
- ◆ 运营商增值P2P应用
- ◆ 网络流量管理的必要性与益处
- ◆ 应用分类管理，使网络具有可管理性

Panabit Your Net!

- ◆ 出口费用
 - 降低带宽峰值减少出口租费
 - 移峰填谷
- ◆ 网络升级和用户容量
 - 在现有网络中增加承载更多用户
- ◆ 客服中心工作降低
 - 优化网络减少客户投诉
 - 客户流失减少
- ◆ 控制网络资源保证大部分客户的使用体验，增加客户满意度

Panabit Your Net!

流控管理的任务目标

- ◆ 为网络应用和用户提供服务质量(QOS)解决方案
- ◆ 提高网络可用性和应用性能
- ◆ 降低带宽/网络成本
- ◆ 制定服务等级协议(SLA), 并进行积极管理
- ◆ 提供创建和管理高级IP服务的能力

Panabit Your Net!

优化带宽使用？

- ◆ P2P流量过载
- ◆ 对某些用户超额使用没有控制
 - 用户与应用的优先权划分
 - 确保用户之间公平性
 - 处理超额使用
- ◆ 调峰
 - 未使用带宽
 - 未知流量
 - 关键性应用被限制
 - 拥塞与带宽饥荒

Panabit Your Net!

流控效果与影响

- ◆ 100%使用带宽，不再出现“突发行为”，限制未知流量
- ◆ 高优先级经过认证的流量
- ◆ 最佳性能传输
- ◆ 保护关键性应用、紧迫应用
- ◆ 保证VIP用户的带宽使用

Panabit Your Net!

Peer-to-Peer的特点

- ◆ 不需关照的下载方式 – 增加网络峰值带宽和峰值持续时间
- ◆ 流量对称 – 导致上行拥塞
- ◆ 地理不可知 – 增加出口成本
- ◆ P2P 应用使用随即端口 (port-hopping)
 - 不能使用传统技术识别
- ◆ P2P applications are popular – 60% - 80%
 - P2P问题存在并且日益严重

Panabit Your Net!

P2P技术发展

- ◆ 第1代集中式的P2P应用
 - Napster模式，通常使用一个固定的TCP端口；
- ◆ 第2代分布式P2P应用：规避传统网络设备的“技巧”
 - 端口跳跃：随机端口；
 - 盗用常用端口号：如HTTP协议的80端口；
 - HTTP隧道：伪装成HTTP流量；
 - HTTP代理隧道：如Socks代理；
- ◆ 第3代P2P应用：介于集中式和分布式之间的混合折中结构
- ◆ 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. 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。

识别P2P应用软件

- ◆ 深层数据包检测(DPI:Deep Packet Inspection)
- ◆ 基于流量特征的检测技术(Transport Layer Identification)
- ◆ P2P流行，并占宽带流量主导地位
- ◆ 催生了应用层识别的技术与市场需求
- ◆ 精确识别不误判，流控的关键

Panabit Your Net!

技术与市场的驱动

- ◆ P2P流行，P2P应用成为桌面主流
- ◆ P2P技术深刻影响了宽带网络服务的运营模式
- ◆ 影响关键应用，服务无保障
- ◆ 收益降低，冲击其他业务收入
- ◆ P2P应用逃避监管，传统设备无能为力
- ◆ 到应用层识别，基于应用分类管理
- ◆ 疏堵结合，应用可管理，提高网络效率
- ◆ P2P带宽杀手，占据网络出口50—80%的流量

Panabit Your Net!

- ◆ 普通协议：基于连接的有状态识别
- ◆ P2P应用：基于节点的有状态识别
 - P2P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
 - 节点：IP+服务端口的二元组
 - 通过"识别节点"的方式去识别P2P流量
 - 极大地提高识别性能
 - 特征识别条件(防止误判)
 - 连接建立的过程被监控到
 - 并且特征包能够被监控到
- ◆ 节点识别，高性能技术特色

Panabit Your Net!

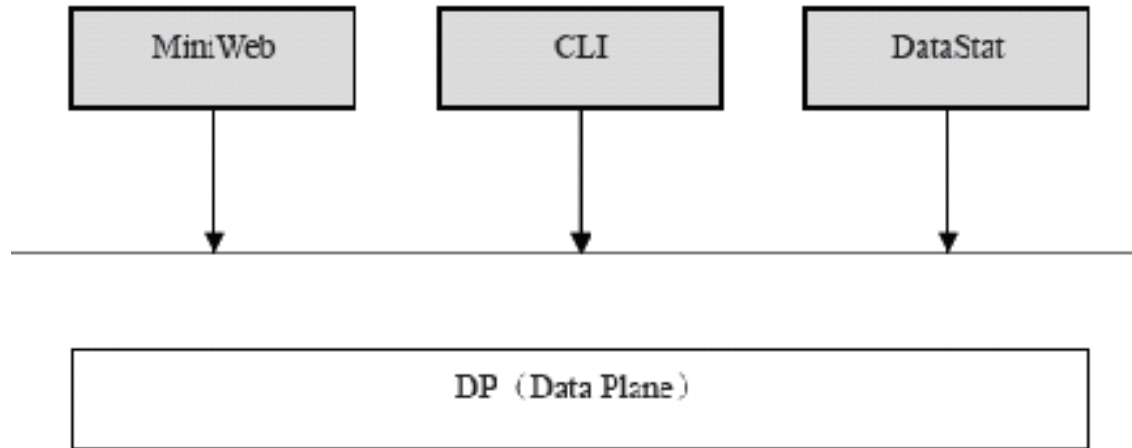
- ◆ 基于节点智能技术
 - 根据连接统计规律，识别特征模糊或被加密的P2P协议
 - 保证性能的同时，提高识别准确性
- ◆ 主动探测技术
 - 独有的服务探测引擎可以识别加密协议，如eMule 0.47c, Skype
- ◆ 服务伪装探测
 - 如探测迅雷综合了P2P和http,ftp等传输协议的应用
- ◆ 独有技术特色

Panabit Your Net!

- ◆ 基于Intel x86 FreeBSD软硬件平台
 - 优化网络协议栈和内核代码，内核直接处理
 - 优化特征库，确保对CPU的Cache使用最大化
 - 修改中断处理函数和网卡驱动，提高效率
 - PCI-E硬件平台，单核志强3.6G，pps达1.2M
 - 数据平面内核运行，确保数据包即时处理
- ◆ 节点识别技术，对于已经识别的节点，不再做应用层分析
- ◆ 良好的系统框架，新增协议特征和模块不损失性能

Panabit Your Net!

PanaOS控制平面(CP, Control Plane)

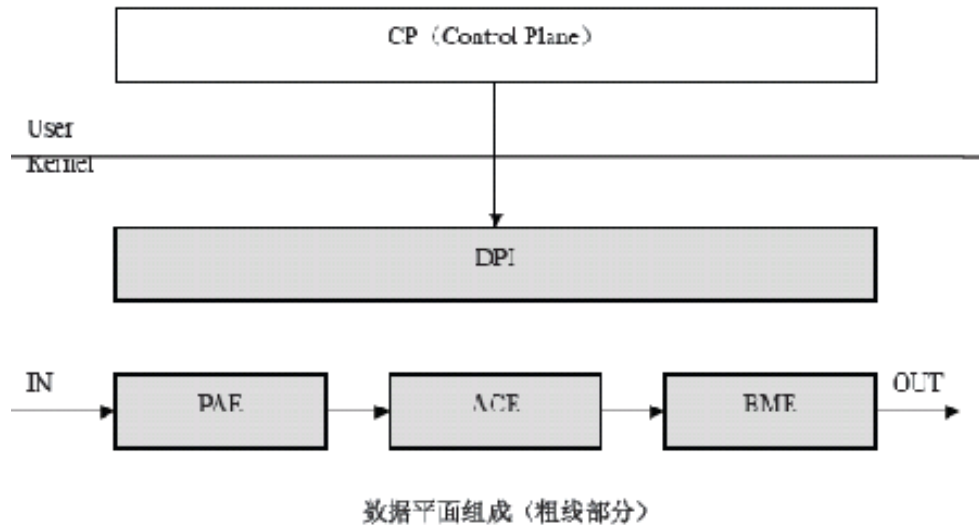


控制平面组成 (粗线部分)

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

Panabit Your Net!

PanaOS数据平面(DP, Data Plane)



- ◆ (1)PAE(Packet Analysis Engine): 负责应用层识别
- ◆ (2)ACE(Access Control Engine): 负责访问控制
- ◆ (3)BME(Bandwidth Management Engine): 负责带宽限制和分配
- ◆ (4)DPI(Data Plane Interface): 为CP提供访问数据平面的数据和相关信息状态的接口
- ◆ 数据平面的运行优先级高于控制平面, 确保数据包即时处理

◆ 协议分析

- 传统协议
- P2P应用的分类，具体到每一个P2P应用的分析
- 网络游戏、股票等应用分析
- 实时监视流量曲线
 - 有用户仅用于流量分析与统计

◆ 策略控制

- 带宽限制
- 带宽保证

◆ 运行报告

Panabit Your Net!

Panabit 已识别协议

- ◆ 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, 热血江湖, 征途, 跑跑卡丁车, QQ幻想, 泡泡游戏, QQ游戏, 中国游戏中心。
- ◆ 8)股票类
 - 大智慧(大智慧Internet经典版、大智慧新一代), 钱龙(经典版、旗舰版), 核新(同花顺2007)

◆ 控制对象

- 基于时间、源IP/目的IP、IP网段、端口、协议、协议组等各条件组合进行访问控制

◆ 流量管理

- 基于应用的流量管理
- 基于IP的流量管理(IP、IP组带宽限制或保证)

◆ 控制策略

- 带宽限制(含支持对"未知协议"速率控制)
- 带宽保证(注册服务, 关键应用, VIP IP或IP组)

Panabit Your Net!

◆ 报表功能

- 1) 日图表、周图表、月图表报表功能
- 2) 连接统计、节点统计、协议统计、PPS统计报表功能
- 3) 总、分流量TOP 30 报表功能
- 4) 自定义报表功能

◆ 日志功能

- 1) 管理员本地操作日志
- 2) 详细日志可导出至日志存储、分析设备

Panabit Your Net!

◆ 高可用性功能

- 支持硬件Lan Bypass功能
- 软件Bypass

◆ 系统管理

- 1)中文https管理界面
- 2)Web界面升级功能
- 3)Web界面License状态查询与更新功能
- 4)Web界面配置文件导入、导出功能
- 5)Web界面链路状态、系统信息、运行时间查询功能
- 6)Web界面核心进程Disable/Enable功能
- 7)Admin操作日志清空功能

Panabit Your Net!

◆ 精确的协议识别与控制

- 已支持90多种主流协议，新协议第一时间加入特征库
- 动态协议特征描述语言PSDL(Protocol Signature Description Language)，维护特征库快捷
- 将实现引擎与特征库的分离，类似手机机卡分离模式
- 本地化协议支持优势，响应速度快
- 用户发现新应用，提供客户端或抓包样本，及时更新

◆ 高性能

- 软件与硬件完美配合，性能国内领先水平
- 千兆线速产品，高性价比，得益Intel总线技术发展，使得同级别用ASIC、NP架构的产品优势降低
- 用Intel多颗CPU提高性能，多核是具有竞争力的发展方向

协议识别运行示例

系统概况—>应用协议

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(%)
百度下吧	30	300	0	0	236888438	385363048	38.97
POCO	30	300	11	675	144135573	317596624	28.91
HTTP	30	300	0	0	20873872	213954892	14.71
其它	30	300	0	0	113626304	62738331	11.04
PPStream	30	300	0	0	6248768	20040600	1.65
ReCool	30	300	0	0	545040	20276469	1.30
Kugoo(酷狗)	30	300	0	0	0	18719181	1.17
Bittorrent	30	300	0	22	6614612	7495122	0.88
SMTP	30	300	0	0	13510626	368764	0.87
QQLive	30	300	0	0	588355	3884171	0.28
PPLive	30	300	0	0	691895	481224	0.07
Https	30	300	0	0	102644	596713	0.04
POP3	30	300	0	0	13015	509996	0.03
DNS	30	300	0	4	177743	315578	0.03
NetBIOS	30	300	0	3	121583	148088	0.02
eDonkey	30	1800	0	71	133458	132604	0.02
YahooMessenger	30	300	0	0	0	0	0.00
Thunder	30	300	0	0	0	0	0.00
Telnet	30	300	0	0	0	0	0.00
SSH	30	300	0	0	0	0	0.00
Skype	30	300	0	30	0	0	0.00
RTSP	30	300	0	0	0	0	0.00
MSN	30	300	0	0	0	0	0.00

访问控制示例

流量管理—>策略计划表

一些说明

策略组 数据通道

- (1) 计划表用来描述何时使用什么样的策略组来控制流量
- (2) 没有安排的时段,系统将按照"空策略组"对待.所谓"空策略组"就是不包含任何规则的策略组
- (3) 系统优先按照节假日计划进行调度
- (4) 如果时段重复,系统以最先匹配的时段为准

每周计划

节日计划

日期	起始时刻(时:分:秒)	结束时刻(时:分:秒)	策略组	操作
星期一	08:00:00	18:00:00	上班时间	删除
星期二	08:00:00	18:00:00	上班时间	删除
星期三	08:00:00	18:00:00	上班时间	删除
星期四	08:00:00	18:00:00	上班时间	删除
星期五	08:00:00	18:00:00	上班时间	删除
星期六	00:00:00	23:59:59	周末	删除
星期日	00:00:00	23:59:59	周末	删除
星期一	0	0	空策略组	添加

策略编辑示例

策略组—>编辑“上班时间”

一些说明

策略组 策略计划表

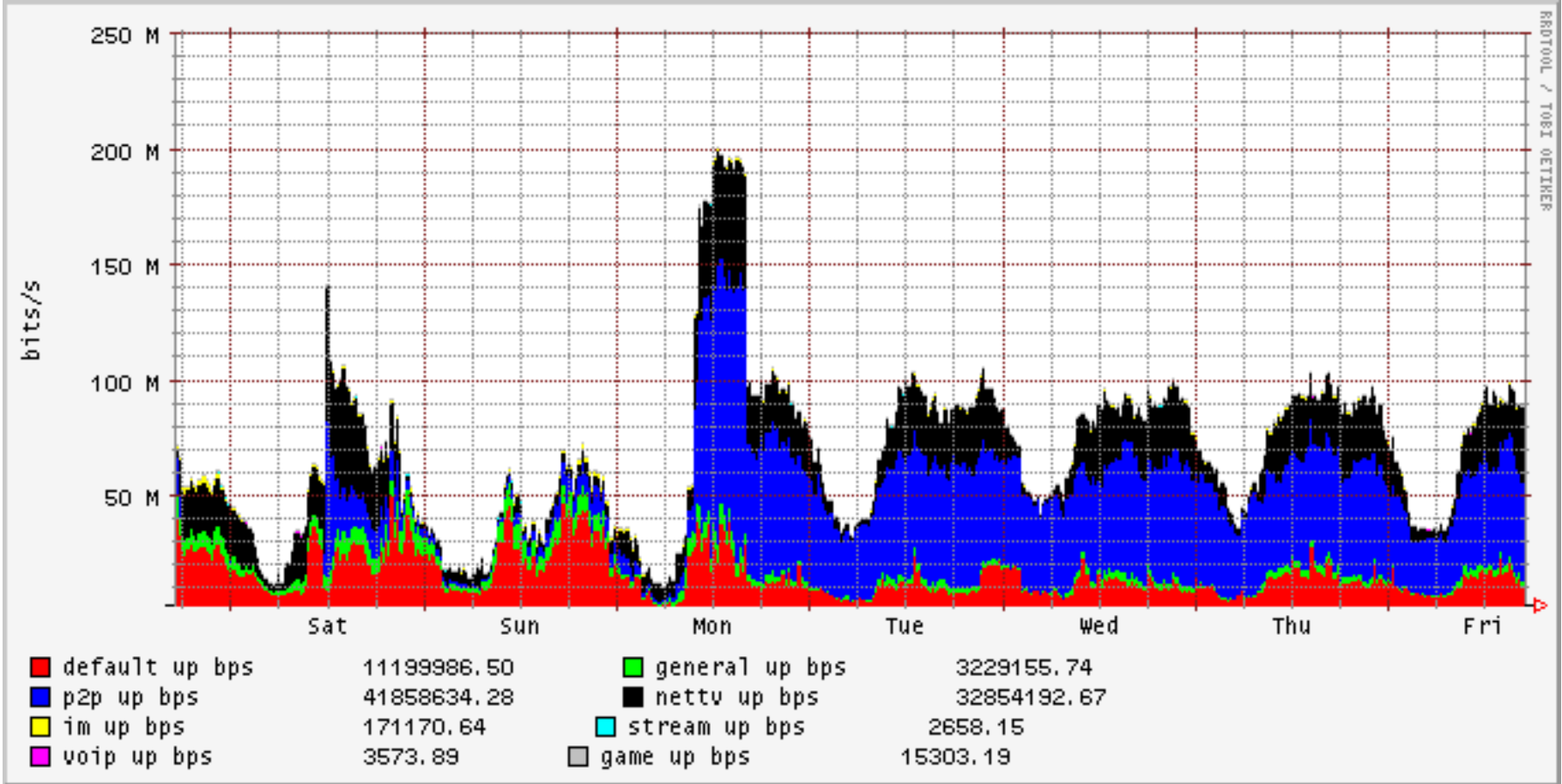
- (1) 系统优先按照协议规则匹配，如果没有任何一条基于协议的规则匹配，系统按照“基于规则”匹配
- (2) 基于规则的策略匹配的原则是：序列号小的规则优先匹配。
- (3) 这是当前正在起作用的策略组

按照协议

按照规则

协议名称	上行通道	下行通道	操作
百兆	100zhao_up	100zhao_down	删除
HTTP	允许	允许	删除
Bittorrent	阻断	阻断	删除
PPLive	阻断	阻断	删除
Thunder	thunder_up	thunder_down	删除
HTTP	阻断	阻断	添加

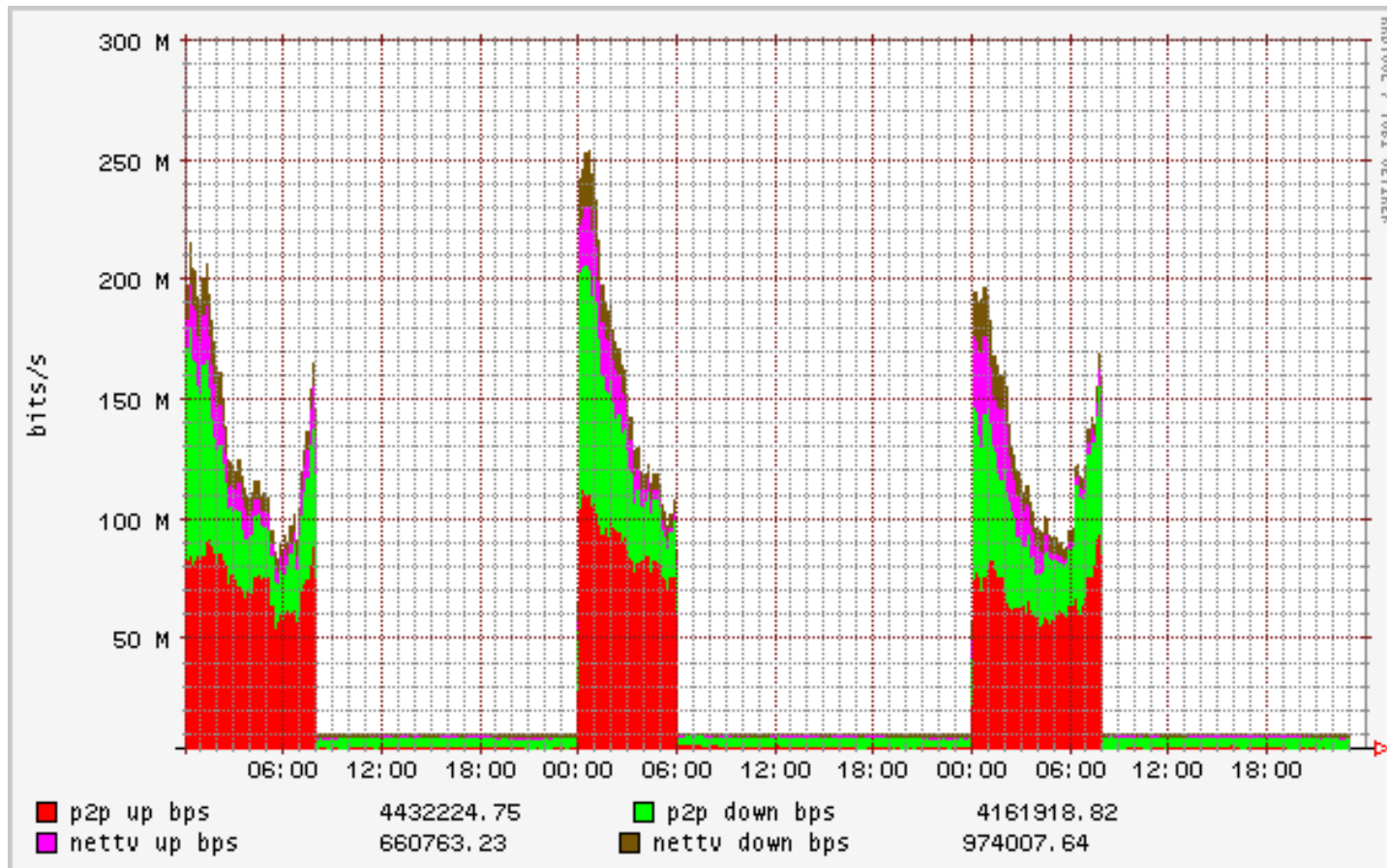
监控波形图



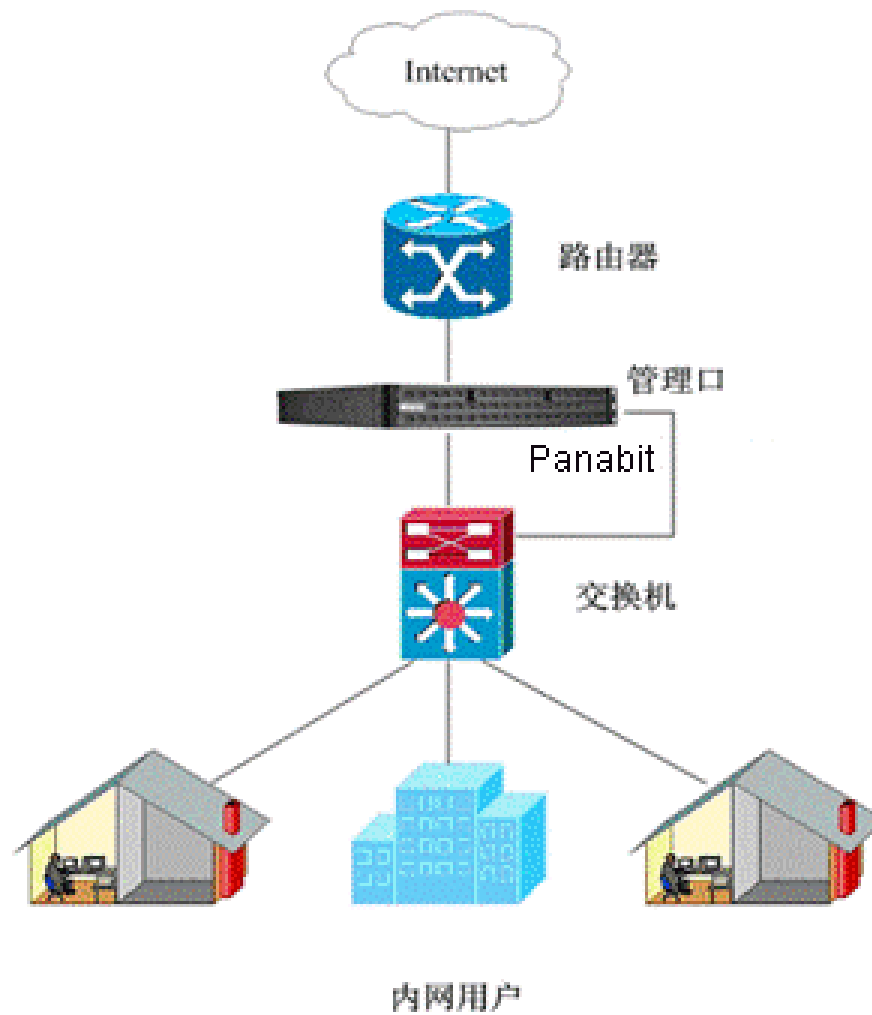
Panabit Your Network

某用户实际控制效果

- ◆ 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，自定义的图表

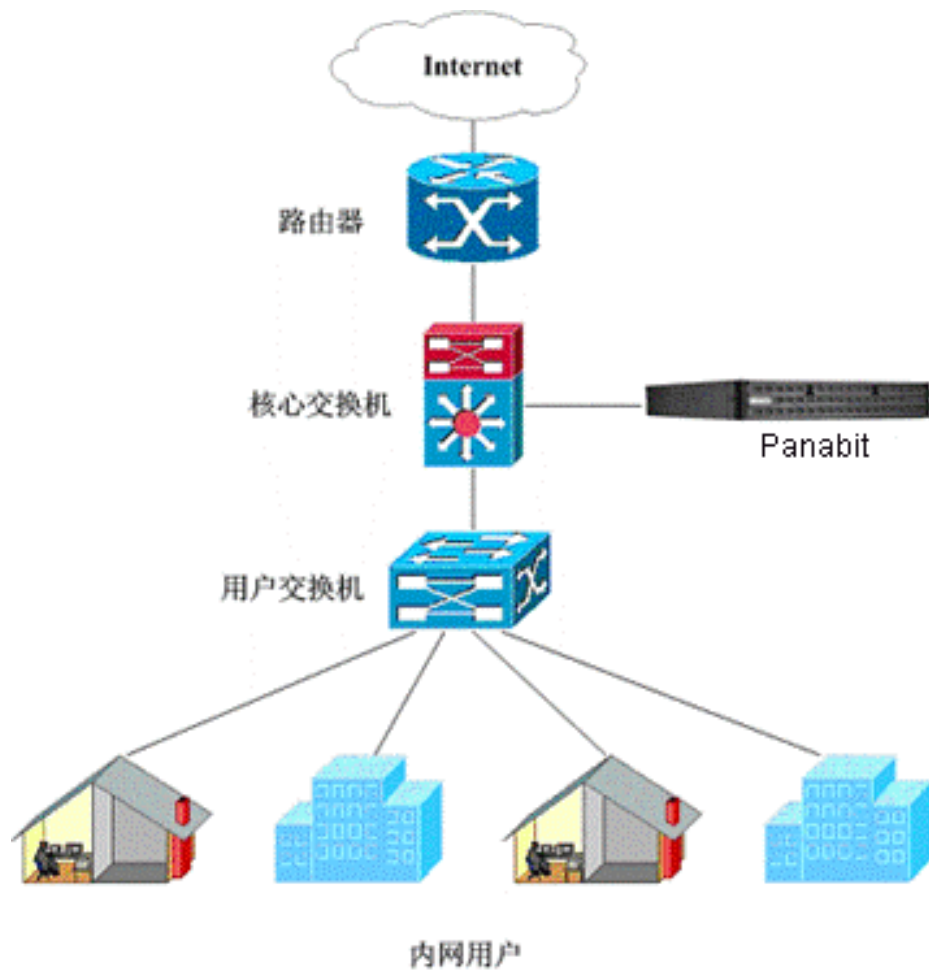


网桥部署方式



Your Net!

监听部署方式



Panabit: Your Net!

◆ 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；

◆ 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；

◆ 保障网络稳定运行

- 监测、分析网络数据，优化网络传输效率；

◆ 提高网络服务质量

- 通过对带宽的合理规划，错开峰值，保障网络畅通。

Panabit Your Net!

运营商案例

- ◆ 某城域网出口，千兆链路，实际双向流量**1.8G**左右
- ◆ 测试数据表明，**P2P**流量占**50%**，总流量需控制在**1.4G**左右
- ◆ 简单一条策略，把**P2P**上下行控制到**500M**，也可以仅限上行
- ◆ **P2P**限速，**http**等流量将放大
- ◆ 用户体验，网页、邮件等变快，**P2P**下载体验不明显改变，还可以通过时间段调节
- ◆ 运营商自主运营的**IPTV**，可以做带宽保证，保证增值服务的质量

Panabit Your Net!

◆ 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；

◆ 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；

◆ 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；

◆ 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。

Panabit Your Net!

企业案例

- ◆ 现状：上班时间，边工作边开着P2P下载等工作无关的应用，正常浏览、收发邮件变慢，影响工作效率
- ◆ 上班时间可以设定一些限制策略
- ◆ 有些员工工作需要P2P下载找资料，不做限制
- ◆ VIP用户，带宽保障，如基于IP或IP组
- ◆ 非应用层控制设备，控制效果微弱，应用软件会逃避监管

Panabit Your Net!

产品特色小结

- ◆ 基于应用层的识别与控制
- ◆ 新一代的流控设备
- ◆ 科学完善的完全控制方案
 - 非限制连接数
 - 对Skype、eMule、迅雷准确识别与控制
 - 如迅雷，先断迅雷自身P2P协议，第二限制http分块传输，第三控制伪IE下载(包括FlashGet等)
- ◆ 带宽限速和带宽保证
 - 基于协议和IP
 - 传统设备无法对P2P协议限速和保证
- ◆ 区分应用，是网络可管理性的基本要求

Panabit Your Net!

The End

- ◆ 创新 诚信 务实!
- ◆ 专业执着，精益求精
- ◆ 领先技术，持续竞争力
- ◆ 客户第一，质量是生命
- ◆ 您的成功，是Panabit团队最大的心愿
- ◆ 欢迎访问: www.panabit.com
- ◆ 欢迎参与: forum.panabit.com

Panabit Your Net!