

优化网络，加速应用

- 运用监控、整形、压缩和加速来提高性能

目录

优化网络，加速应用的策略	2
网络及应用性能问题	2
影响	3
通常的解决办法---增加更多带宽	4
我们的整体解决方案	5
部署	6
监控模块提供网络能见度	6
您的网络上有哪些流量？	7
应用的运行情况能否满足所有的期望？	19
什么应用和什么人在占用带宽？	20
在什么时候发生了什么？	21
网络上是否正在发生重要的事情？	22
整形模块控制带宽	23
应用控制功能	24
速率控制技术	25
提高特定网络环境下的性能	26
压缩模块增加容量	29
整形和压缩组合使用	29
压缩功能如何工作？	31
数据包打包	31
压缩的效果	32
压缩效果报告	33
加速模块增强性能	34
Packeteer 的解决方案	37
加速与其他优化工具结合	39
您可以从加速中获益吗？	39
多少流量被加速了？	40
SkyX 与 PacketShaper 兼容性	41
压缩隧道	42
活动隧道	42
隧道监控和配置	42
小结	43
更多信息	44

优化网络，加速应用的策略

对网络的应用性能进行管理可以视为一个极大的挑战。当网络运行缓慢、不一致且无法预测时，生产力就会下降，用户就会出现困惑。您是否会觉得以下这些问题是如此熟悉呢？

- ◇ 不断的带宽升级没有解决性能问题，而且还会明显地增加成本；
- ◇ 数据中心中的网络应用可提供轻松的访问，但性能不高；
- ◇ 员工不论何时将其笔记本电脑与信息服务器同步邮件，分支机构就会出现链路拥塞；
- ◇ 在网络繁忙时，访问者经常会面临网络中断，于是对于VoIP的使用热情就会下降；
- ◇ 娱乐性流量波动和被病毒感染流量波动导致关键应用的互相竞争；
- ◇ 服务器每晚的备份到第二天早上也不能完成。

对于许多企业来说，广域网上应用的性能逐渐下降，甚至不起作用。在一些企业中，单一的一个事件，比如说部署一个新的应用或重新部署服务器都会使性能的下降速度更快。

网络和应用性能的糟糕情况是完全可以解决的，本文描述了通过使用Packeteer网络应用优化解决方案，检测问题，并解决问题来保护应用的运行。

网络及应用性能问题

最近应用及网络环境的改变带来了极大的性能破坏。不断增长的应用、各种不同的性能要求、本地网和广域网间负荷的不匹配，这些问题都使得应用运行速度下降越来越快。

流量的增长来源于应用、网络的发展方向以及用户的不同习惯，包括：

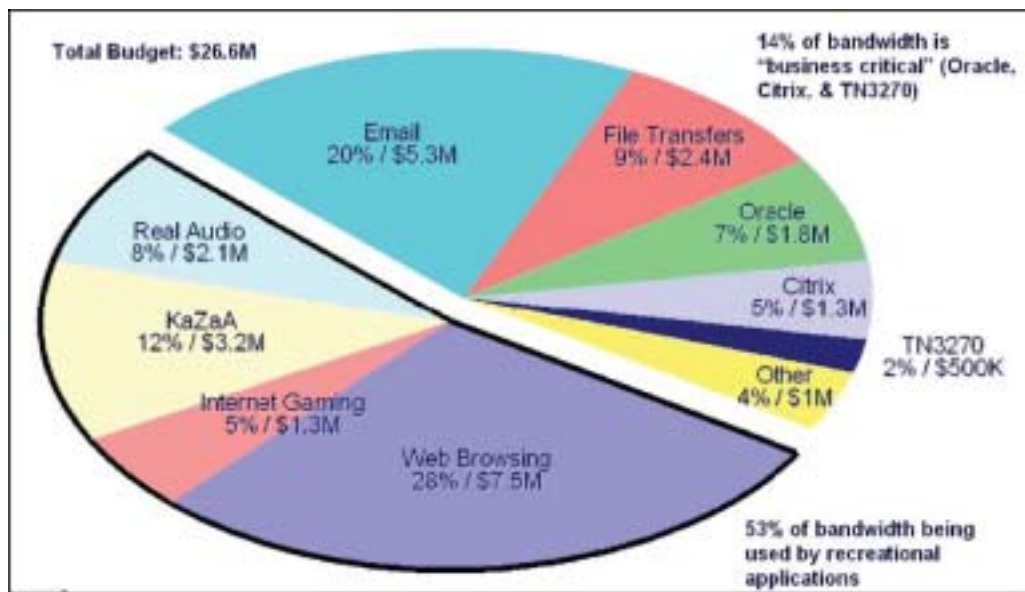
- ◇ 更多的应用流量：应用数据量的激增，用户需求增加以及多媒体的增长；
- ◇ 娱乐性流量：网络中大量的在线视频、MP3下载、即时信息、网页浏览、在线游戏等流量；
- ◇ 基于网页的应用：基于网页的用户界面应用，占用带宽是以前的5-10倍；
- ◇ 分布式应用：在广域网或英特网上的企业应用，并不仅仅局限于一台机器的应用；
- ◇ 服务器整合：数据中心整合，减少服务器数量，预先使本地流量（高带宽，低延时和低成本）穿过广域网或因特网（低带宽，高延时和高成本）。
- ◇ 语音/视频/数据的网络融合：在带宽需求及性能要求上支持多种不同语音、视频和数据的网络；

- ◇ SNA/IP集合：支持TN3270或TN5250上SNA应用的IP网络，没有SNA网络控制，老得应用通常会面临性能的下降；
- ◇ 灾备份：备份数据中心，大数据量镜像；
- ◇ 网络安全：蠕虫、病毒、DoS攻击；
- ◇ 用户的新的网络习惯：用户在网上做更多的事：购物、查找资料、新闻浏览、理财、参与社会活动、疾病诊断等等；

性能问题的出现也会来源于高延时的网络环境，比如卫星链接。延时可使得广域网传输产生极大的破坏，延时的不断增加会延长应用的响应时间，使得文件传输难以进行。

影响

这些问题通常会导致关键应用的性能下降。就算在最好的情况下，运行也会出现不一致或不可预见等问题；而最糟糕的时候，运行会极其缓慢且不时有中断。在财务方面所导致的影响也是非常令人沮丧的。



根据IDC在2003年的报道，美国大企业每年花费在广域网上的金额高达美元26,626,600。上面的图表显示了此类公司在广域网上流量最大的几类应用，以及每一类应用所占带宽的百分比。

正如您所看到的，公司的关键业务应用所用带宽被限制在50%以内；而更令人苦恼的是，公司每年所花的这美元2660多万中，仅有美元370多万是用于关键应用，而用于娱乐性流量的则高达美元1400万。

而此图表所未能显示的还有：这些关键应用（Oracle, Citrix, and TN3270）的性能都非常慢。

其他来源于未经管理的应用流量的影响还包括：

- ◇ 带宽分配的不相等和不公平：公司分支机构、公寓、学生宿舍或用户得到更多的份额；
- ◇ 在时间上非紧急的重要应用，如传输一个重要文件，占用了几乎所有可得到的带宽，影响很多交互式应用的运行；
- ◇ 语音/视频出现抖动，不能正常接收；
- ◇ 恶意流量占据和影响整个网络的运行。

通常的解决办法----增加更多带宽

正如您可以想象，对于网络上流量太多和响应时间太长的解决办法通常就是增加更多的带宽，但实际上带宽扩容并不是最有效的解决方法。为了解决这些性能问题，网络经理将预算的很大一部分都花在了带宽扩容上，但结果却发现这些问题依然继续存在。

而对于这些性能糟糕的应用来说，获得多余容量并不是非常必要。通常这些应用并非紧急应用也非关键应用。所以当企业试图仅用压缩来解决问题，不去对应用进行控制时，情况也同样得不到改善。如果不对应用进行合适、正确的管理，压缩后的带宽所得甚至会被不适当的应用全部占用。

在上图中，关键应用仅占了全部带宽的14%。所以即使在购买了更多带宽后（正如他们平常所做的那样），如果使用模式不改变，那么这些应用所占的百分比还是14%，仍然没占到最好的带宽份额。而网络经理试图增加链路容量的另一个原因是想加速在大型数据中心之间数据备份的速度，改善原来备份缓慢的状况。然而，链路容量可能并不是一个问题，传输速度可能会被其他因素所约束。比如说，假设您数据中心的链路容量是45Mbps，使用大小为16K的Windows 2000操作系统，数据备份有30分钟的来回时间。尽管在这个假设中延时适中，但是因为操作系统的窗口过小，单个流量占到整个带宽不到10%，扩容链路也解决不了问题。这种情况下需要的是对链路上所有可得到带宽的充分利用，而这个问题可以通过网络加速得到解决。

带宽扩容增加了安装成本，在一些地方，特别是在比较偏远的地区，较大的链路要么不能提供要么非常贵。就算是安装成本有所降低，每个月也还需要支出一笔维护费用。Gartner Group公司最近指出：“公司日常的单项最大成本是花费在广域网带宽上的定期成本，甚至比人力成本还要大。”

我们的整体解决方案

在流量不断增长的网路中，广域网和因特网链路上的拥堵导致了应用性能的不断降低和生产力的下降。如果得不到更多的带宽，那么我们可以怎么办呢？答案是：在管理带宽和利用率方面，增加更多的能见度和控制。具体如下：

- ◇ 改善和保护紧急应用和关键应用的性能；
- ◇ 减缓重要但不紧急应用的速度（如邮件中大的附件）；
- ◇ 发现并阻止来自恶意流量的威胁；
- ◇ 限制娱乐性流量，减少它对关键应用的影响；
- ◇ 对视频类应用提供带宽保证，确保接收连续。
- ◇ 压缩流量，从而让更多的数据通过有限的物理链路；
- ◇ 加速流量，使带宽在高延时环境中得到充分利用。

Packeteer的广域网应用优化系统可以做到这些，让IT企业获得如下功能：

- ◆ **网络能见度**：所有型号的PacketShaper都具有此功能，在此监控模式下，您可以准确地知道网络上有哪些应用，这些应用分别所占用的带宽、运行情况，以及延时源自何处。详见第6页“监控模块提供网络能见度”。
- ◆ **控制带宽**：整形模块提供基于策略的带宽分配，管理广域网及因特网上的应用性能。灵活的控制策略可以保护关键应用，减缓带宽占用大的流量，限制娱乐性使用，抑制恶意流量。详见第23页“整形模块控制带宽”。
- ◆ **压缩流量**：压缩模块可使更多的数据通过有限的广域网链路，使关键应用得到更多所需带宽。详见第29页“压缩模块增加带宽容量”。
- ◆ **流量加速**：加速模块可使您的带宽得到最大化的利用，缩短应用响应时间，加速大容量文件的传输速度，减少高延时链路上的基于TCP的应用所面临问题的影响。详见34页“加速模块提高性能”。

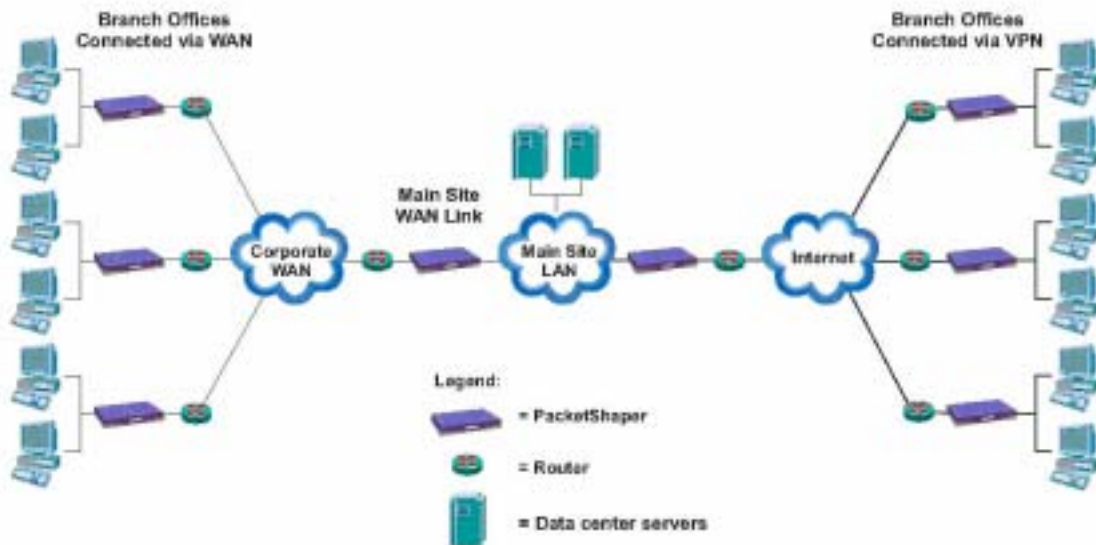
Packeteer的设备部署于全球7000多家企业中，我们的解决方案---网络能见度、控制、压缩和加速等能力均获得专利称号。另外，Packeteer还有PolicyCenter和ReportCenter软件，单独的中心管理，可报告企业内部署的PacketShaper运行情况并对其进行管理。

部署

PacketShaper通常部署在主站点或分支机构的广域网路由器或因特网路由器后面，必须让应用通过设备，这样才能对Inbound和Outbound的流量进行监控。或者也可以将设备旁路放在主要数据通路外面，采用非在线拓扑，这种模式称为“Watch Mode”。在这种模式下，监控模块的所有功能都可以实现，但是其他如整形、压缩和加速等功能却不可以实现。

您可以选择在所有的分支机构都部署PacketShaper，也可以采取阶段性的部署策略，先在主站点或问题较多的几个分支机构部署，然后再一步步扩散到其他分支。而且Packeteer的整形、压缩及加速模式可简单地通过软匙激活。

安装简单，只需插上电缆，在基于网页的安装页面上输入地址、访问密码等安全信息。PacketShaper可集成已有的网络部署，路由器的配置、拓扑、桌面和服务器等无需作任何改变，还可以对其他网络应用进行补充，如防火墙、负载均衡设备、冗余路由器和缓存解决方案等。而对于网络中更多复杂的交换网络，扩展模块可提供更多的灵活性。



多层次的失效处理机制可确保PacketShaper在故障发生的情况下不会阻止流量。基于网页的用户界面可以让您在任何一个地方用网页浏览器访问，并提供适当的安全保护。

监控模块提供网络能见度

对网络和应用行为的能见度是控制应用的首要条件，也是对业务运行进行有效管理的重要条件。您是否拥有其他任何可提供有效能见度的工具来解决出现的问题呢？

- ◇ 您广域网上有哪些流量？哪种流量占用了最多的资源？
- ◇ 娱乐性流量消耗了您多少带宽预算？
- ◇ 您的应用是否满足终端用户的需要？是否能让用户得到所承诺的服务水平？
- ◇ 对于一些特定的应用，哪些用户和分支机构使用最多？
- ◇ 每一个MPLS服务类是如何运行的？性能与服务水平及成本是否匹配？
- ◇ 远程站点是否可获得他们购买的所有带宽？是否全部需要，是否在有效地运用这些带宽呢？

PacketShaper的监控模块可以回答以上所有甚至更多的问题，并不仅仅是进行简单地数据收集。PacketShaper可组织调查的结果，综合得出的结论，并及早地标出问题，进行更有效率地管理。PacketShaper可将数据转变成信息，让您的管理不再被动，并准确地告诉您网络上有哪些应用，他们分别占用多少带宽，运行情况如何，延时源于何处等。在监控模块下，您可以：

- ◇ 自动检测几百个业务应用和娱乐性应用，并对其进行分类；
- ◇ 识别占用带宽最多的应用、用户、服务器、分支机构和访问次数最多的网页。
- ◇ 分析带宽的使用情况、响应时间、配置改变所带来的影响和时延的来源；
- ◇ 跟踪响应时间，区分网络和服务器的响应时间；
- ◇ 设置服务水平的标准，并跟踪其是否达到标准；
- ◇ 监控用户使用网络的状况，超过设定阈值时自动告警，记录或通知问题人；
- ◇ 度量和图表输出100多个参数来描述网络使用情况、可用性、效率、响应时间、错误和诊断结果等。

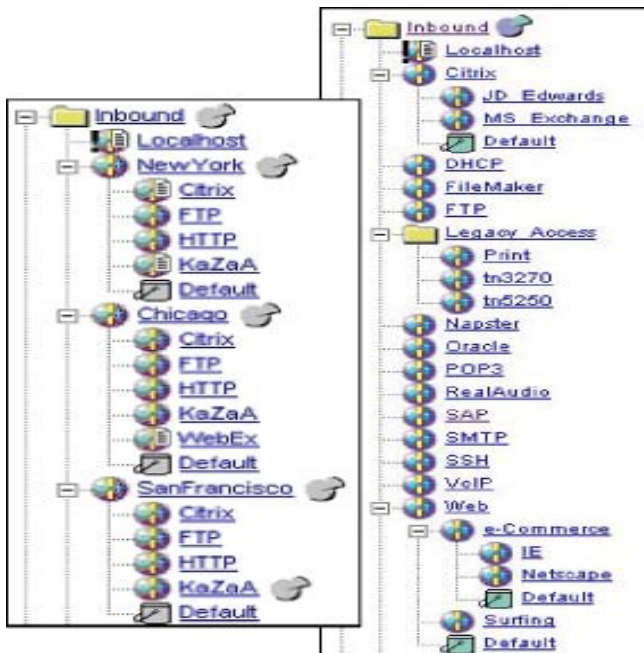
您的网络上有哪些流量？

跟其他类型的网络相比，企业网支持的流量种类通常都很多。您只需将PacketShaper连上网络，并打开“Traffic Discovery”，各种应用便一目了然，PacketShaper会迅速对观察到的不同流量进行识别和组织。每一种流量类型我们称之为流量类（Traffic Class），而网络上流量类型的繁多，通常都会让网络管理者们感到惊讶。

丰富的流量分类是非常重要的，因为如果不能识别流量的种类，就不可能对流量的运行状况进行评估或控制。比如说，如果不能在网页浏览或音乐下载等网页流量中识别出哪些是基于网页的业务应用，那么如何对这些业务应用进行保护呢？

对于网络流量所不断增长的复杂性，我们需要更为先进的分类技术。目前使用简单的IP地址或静态端口的应用已经越来越少，PacketShaper的分类技术可检测到那些使用动态和跳动端口的应用，区分那些使用同样端口的应用，并运用第七层的应用特征来识别不同应用。

使用PacketShaper，您可以将与应用、协议、子网、网页和用户相关的流量隔离。您可以区分ERP流量，如Oracle和JD Edwards、内网应用、Citrix应用和Citrix打印流量、IP语音和视频、从某一特定服务器通过的网页流量、使用给定的浏览器、多种即时消息、游戏、音乐下载等。



对于大部分的应用和协议，PacketShaper都可以进行自动检测、区分和分类，包括：

应用	描述
C/S 结构应用	
CVSpsserver	软件开发中版本控制应用。使用端口：2401/tcp 2401/udp
CVSup	优化 CVS 网络文件分发系统，用于从远程服务器主机上的主 cvs 库分发和更新源码树的应用（软件包）
FIX	金融信息交换协议，常使用于股票交易等
FoldingAtHome	分布式计算屏保，用于蛋白质、RNA 等计算
INFOC-RTMS	Attachmate 公司的 INFOConnect 响应时间监视系统
INT-1	Unisys 交互信息 1 (2200, ClearPath IX)
MATIP	航空流量 IP 服务组(RFC 2351)
MATIP-A	MATIP 类型 A
MATIP-B	MATIP 类型 B
MeetingMaker	Meeting Maker
NetIQ	NetIQ 公司的 AppManager 系统管理软件

OpenConnect-JCP	OpenConnect JCP 的客户端 (基于浏览器的主机访问应用)
PEPGate	Attachmate 的 PEP 网关 (Unisys 2200)
Unisys-TCPA	Unisys TCPA (A Series, ClearPath LX, NX)
内容分发	
Apple-iTunes	Apple 电脑音乐下载
Ariel-419	Infotrieve 公司的文档投递系统 (使用端口 419)
Ariel-422	Infotrieve 公司的文档投递系统 (使用端口 422)
BackWeb	推的技术。Polite BackWeb 在客户端有一个代理, 防止 BackWeb 后台流量妨碍其它 IP 网络应用。
Chaincast	Chaincast 的灵活内容投递系统 (Internet 流服务)
EntryPoint	EntryPoint 的推数据流 (原来的点播)
Kontiki	Kontiki 的内容分发网络
Marimba	Marimba Castanet 的推数据流
Napster2	点对点音乐传输, 类似 BT
Napster2-Data	Napster 音乐文件下载
Napster2-Other	其它的 Napster 数据流
NewsStand	NewsStand-Reader 出版订阅服务
PointCast	同 EntryPoint 应用
Webshots	Webshots Desktop (图片屏保软件), Internet 图片应用软件
数据库和 ERP 软件	
BAAN	Baan 企业管理系统
FileMaker	FileMaker Pro 数据库服务组
FileMaker-DB	FileMaker 数据库访问
FileMaker-R	FileMaker 网络主机响应
JDENet	J. D. Edwards OneWorld JDENet protocol
MSSQL	微软 SQL 服务
MSSQL-Mon	SQL 监视数据流
MSSQL-Server	SQL 服务数据流
Oracle	Oracle 数据库应用, 像联众网络游戏也会使用 Oracle 数据库作后台, 所以有可能也是联众游戏的应用。
Oracle-netv1	Oracle 数据库第一版本, 像早期版 V6, V7
Oracle-netv2	Oracle 数据库第二版本, 包括 Oracle7, 8, 8i, 9i, 10g 等
Oracle-JVM-SSL	Oracle JVM (IIOP) traffic over SSL 基于 SSL 的 Oracle JVM (IIOP) 数据流
Oracle-SSL	基于 SSL 的 Oracle 数据库数据流
OracleClient	Oracle Java 用户端 (Webforms)
OracleEM	Oracle 企业管理
OracleEM1	Oracle 企业管理-1
OracleEM2	Oracle 企业管理-2
PostgreSQL	PostgreSQL 的免费 SQL 数据库
Progress	Progress database traffic

	Progress 数据库数据流
SAP	SAP 的系统分析、开发（数据处理方面的服务、应用和产品）
SAP.MCAST.NET	多播通告协议：224.2.127.254
目录服务	
CRS	Microsoft 内容复制服务
DHCP	动态主机 IP 分配
DHCP-C	DHCP 或 BootP Client
DHCP-S	DHCP 或 BootP Server
DNS	域名服务
Finger	指纹用户信息协议
Ident	Identification Protocol RFC 1413, 鉴定协议, 早期的‘认证服务器协议’, 使用端口 TCP113
Kerberos	Kerberos 安全认证
LDAP	目录访问服务
LDAP-Clear	LDAP 明文
LDAP-Secure	LDAP 加密
mDNS	多播 DNS (Apple 网络使用)
RADIUS	RADIUS 用户认证服务
RADIUS-Acct	RADIUS 帐户服务
RADIUS-Auth	RADIUS 审核服务
RRP	NSI Registry Registrar Protocol NSI 公司的注册登记员服务
Rwho	UNIX 远程“rwho”命令；报告局域网中当前用户
SSDP	简单服务查找协议
TACACS	登入主机协议
WHOIS	WHOIS 服务（标识域中的主机）
WINS	微软 WINS 服务
电子邮件与协作	
Biff	UNIX 新邮件通告
ccMail	Lotus cc:Mail 电子邮件应用
DCOM	Microsoft 部件分发目标模块（即微软的 Exchange 邮件服务器，冲击 波病毒也会使用）
Groupwise	Novell Groupwise 邮件服务
Groupwise-MTA	Novell Groupwise 信息传输代理
Groupwise-POA	Novell Groupwise 电子邮局代理
IMAP	IMAP 邮件协议
LotusNotes	IBM 的 LotusNotes 邮件服务
MSSQ	Microsoft 信息队列服务
OSI	Microsoft 邮件服务 Exchange X.400
POP3	收邮收

SMTP	发邮件
文件服务器	
AFS	Andrew 文件服务组
AFS-FS	AFS 文件服务器
AFS-VL	AFS 卷位置数据库
CIFS-TCP	通用 Internet 文件系统 - 基于 TCP
CU-Dev	富士通设备控制 (基于 TCP/IP)
Lockd	NFS 文件锁守护进程
Microsoft-ds	网上邻居拷贝数据
NetBIOS-IP	网上邻居拷贝数据内容
NetBIOS-IP- DGM	NetBIOS 数据报服务
NetBIOS-IP-NS	NetBIOS 名字服务
NetBIOS-IP-SSN	NetBIOS 会话服务
NFS	UNIX 网络文件系统
NW5-CMD	Netware 5 兼容驱动服务组
NW5-NCP	Netware 5 核心协议
Rsync	UNIX 远程文件同步协议
SunND	Sun 网络磁盘启动协议
游戏	
Asheron's Call	微软的 Asheron's Call 网络游戏
Battle.net	Blizzard 娱乐在线游戏服务, 包括 Diablo II 和 Warcraft III
Doom	Doom 游戏
Everquest	属于 sony 在线
Half-Life	半条命, CS (包括 Opposing Forces, CounterStrike, 和 Team Fortress)
Half-Life-TCP	Half-Life 聊天和服务 (TCP 流)
Half-Life-UDP	Half-Life 请求与玩游戏 (UDP 流)
Kali	Gaming protocol 游戏协议
LucasArts	Jedi Knight II: Jedi Outcast
MSN-Zone	微软网络游戏区, 包括帝国时代
MSN-Zone-TCP	Microsoft Network Gaming Zone — TCP 流
MSN-Zone-UDP	Microsoft Network Gaming Zone — UDP 流
Mythic	Mythic Entertainment games (Dark Age of Camelot)
Quake	Quake 游戏服务组
Quake-A	Quake (端口 26000)
Quake-B	Quake (端口 27500)
Quake-II-TCP	Quake II 基于 TCP
Quake-II-UDP	Quake II 基于 UDP
Quake-III	Quake III Arena
SonyOnline	Sony Online Entertainment 开发的游戏 (例如: EverQuest)

Tribes	Sierra Studios 开发的网络游戏 (包括 Tribes 2)
Unreal	Unreal Tournament 公司的电脑游戏
YahooGames	Yahoo 游戏
医疗	
DICOM	关于医学的数字图像和通信
HL7	健康等级 7
主机访问	
ATSTCP	Galileo 2915 终端和打印机数据流
Attachmate-GW	Attachmate 公司的 INFOConnect-e-Vantage 网关
Persona	Persoft 的 Persona 服务组
Persona-Clear	非加密的 Persoft Persona (使用 1917 端口)
Persona-Secure	使用 SSL 安全的 Persoft Persona
SHARESUDP	基于 UDP 的数据系统共享 (IBM 的 TPF 协议)
SMTBF	Attachmate 的信号网关
tn3270	Telnet 到 IBM 3270 终端及 3270 模拟终端
tn5250	使用 telnet 的 IBM 5250 终端数据流
互联网协议	
ActiveX	微软面向对象编程技术和工具
BITS	Microsoft 后台智能文件传输, windows 自动更新补丁使用的
FTP	FTP 下载和上传文件
Gopher	搜索应用
HTTP	网页浏览
HTTP-Tunnel	HTTP 通道流量, 像 KaZaA, Morpheus 和 ICQ 通过 http-tunnel.com 或 socks2http(totalrc.net)网关的 80 端口来通信。
IP	因特网协议 (不会自动查找)
IPIP	IP 对 IP 的封包协议
IPv6	IP 第 6 版 (IPng)
NNTP	网络新闻传输协议
TCP	所有因特网 TCP 流量(不会自动查找)
TFTP	Trivial 文件传输协议
UDP	所有因特网 UDP 流量(不会自动查找)
UUCP	Unix-to-Unix 拷贝协议
传统 LAN 或非 IP	
AFP	AppleTalk 共享协议 (AppleShare IP)
AppleTalk	Apple 网络协议
DECnet	Digital Equipment Corporation network protocol 数字设备公司 (DEC) 网络协议
FNA	富士通网络架构 (变体的 SNA)
FNAonTCP	在 FNA 上的 TCP 服务
IPX	Novell 网络协议

LAT	DEC 打印机支持 (Local Area Transport)
MOP-DL	维护操作协议 (下载/上传)
MOP-RC	维护操作协议 (远程控制)
NetBEUI	PC 机的 NetBEUI 协议
PPPoE	以太网点对点协议, 像 ADSL 拨号等
SLP	服务定位协议
SNA	IBM 系统网络结构协议
即时通讯	
AOL-AIM-ICQ	AOL 8.0 即实通讯工具及 ICQ
AOL-IM	AOL – 即实通讯或 ICQ 用户-服务
ICQ-2000	ICQ2000 用户到用户协议
AOL-IM-Talk	AOL 即实通讯点对点语音聊天
AOL-IM-IMAGE	AOL 即实通讯点对点聊天
AOL-IM-File	AOL 即实通讯点对点文件传输
AOL-ISP	AOL 8.0 ISP 版 用户端注册
AOL-Default	不了解的 AOL 流量, 可能有一些国产软件基于 AOL 开发。
IRC	Internet 中继聊天服务组
IRC-Chat	IRC 的普通聊天数据流
IRC-DCC	IRC 直接客户端到客户端的数据流
IRC-Secure	基于 SSL 安全的 IRC (端口 994)
IRC-Servers	IRC 服务器到服务器的数据流
IRC-194	基于端口 194 的 IRC
IRC-6665	基于端口 6665 的 IRC (服务器到服务器)
IRC-6667	基于端口 6667 的 IRC (客户端到服务器)
Lotus-IM	基于 Lotus 的即时聊天 注意: 有一些即时聊天数据流会分类到现已有的服务中: 广播服务归到 RTSP, 会议数据归到 T.120 中, 会议更新归到 LotusNotes 中。为了最为有效地追踪和管理 Lotus messaging 信息流, 可以把 Lotus-IM, RTSP, T.120, 和 LotusNotes 归到一个单独的文件夹中。
Lotus-IM-CommC	IBM Lotus 即时聊天 管道通信服务
Lotus-IM-CommS	IBM Lotus 即时聊天 通信服务
Lotus-IM-MtgS	IBM Lotus 即时聊天 会议服务
Lotus-IM-SrvrEx	IBM Lotus 即时聊天 服务器交换
MSN-Messenger	MSN Messenger 聊天服务
Windows-POPUP	Windows 消息投递 (RPC); 划出数据流, 例如 DirectAdvertising 这样的应用所发出的 Windows 系统垃圾消息的弹出窗口。
YahooMsg	Yahoo! 聊天
中间件	
CORBA	Internet 的 CORBA 协议
JavaRMI	Java 1.1.4 TCP 远程调用服务组

JavaRMI- Act	Java 1.1.4 TCP 远程调用 激活
JavaRMI - Call	Java 1.1.4 TCP 远程调用 呼叫
JavaRMI-Reg	Java 1.1.4 TCP 远程调用 注册
SmartSockets	Tibco SmartSockets traffic
SunRPC	Sun 远端进程呼叫 (UDP) 服务组
SunRPC-Call	Sun 远端进程呼叫
SunRPC-PortMap	Sun 远端进程呼叫端口映射
多媒体	
Abacast	Abacast 分布式流技术
MPEG-Audio	移动图片专家组 音频流, 使用 Windows MediaPlayer 会产生流量, 像网络收音机等
MPEG-Video	移动图片专家组 视频流, 使用 Windows MediaPlayer 会产生流量, 像网络视频等
QuickTime	基于 HTTP 的 QuickTime 应用, Apple 电脑的媒体播放
RadioNetscape	Radio@Netscape 音乐流应用, 由 Spinner 公司支持
Real	Real 网络音视频流应用服务组, 像使用 Realplayer 或 RealOnePlayer 将会产生此种流量
Real-BackChan	Real 网络多播后台通道流
Real-Encoder	Real 网络基于 HTTP 或 RTSP 的编码流
Real-Multicast	Real 网络实时数据传输的 UDP 多播流
Real-Player	基于 HTTP 或 RTSP 的 Real 网络播放器数据流
Real-RDT-TCP	Real 网络的 Real 数据传输 TCP 数据流
Real-RDT-UDP	Real 网络的 Real 数据传输 UDP 数据流
Real-RTP-TCP	Real 网络的实时数据传输协议 TCP 数据流
Real-RTP-UDP	Real 网络的实时数据传输协议 UDP 数据流
Real-Web	基于 HTTP 或 RTSP 的 Real 网络数据流
RTP-B	实时协议 (广播), 视频会议系统
RTP-I	实时协议 (交互), 电视会议系统
RTSP	实时流协议
Shoutcast	Shoutcast 的音频流
ST2	Internet 流协议, 版本 2
StreamWorks	StreamWorks 的音视频
VideoFrame	Citrix 的 VideoFrame 服务组
VideoFrame-TCP	Citrix 的 VideoFrame 协议 (TCP 流)
VideoFrame-UDP	Citrix 的 VideoFrame 协议 (UDP 流)
WebEx	WebEx 的实时通信平台, 网络会议使用
WinampStream	Winamp 的数据流流量, 听网络 MP3
WinMedia	微软媒体服务组, 使用 Windows MediaPlayer 会产生流量
WinMedia-Mcast	Windows Media 流基于 UDP 多播
WinMedia-MSBD	Windows Media 编码器
WinMedia-TCP	基于 TCP 的微软 Windows Media (Netshow) 数据流

WinMedia-UDP	基于 UDP 的 Windows Media 单播数据流
网络管理	
CiscoDiscovery	Cisco 路由器自动发现协议
Day-Time	Day-Time (端口 13)
Echo	Echo 协议
FlowRecords	Packeteer 的详细流量记录
ICMP	PING、trace route 等使用的协议
IPComp	IP 压缩协议；一种减小 IP 封包大小的技术
NetFlowV5	NetFlow v5
NTP	网络时间同步协议
RSVP	资源预留协议，路由器及交换机会使用
SMS	微软的 SMS2.0 (系统管理服务)，NT 平台发送群组消息
SMS-Auth	SMS 认证
SMS-Chat	SMS 远程聊天
SMS-File	SMS 文件传输
SMS-RC	SMS 远程控制
SNMP	简单网络管理协议
Syslog	UNIX 系统日志
TimeServer	时间服务器 (端口 37)
点对点传输软件	
Aimster	Aimster 文件共享协议
Audiogalaxy	Audiogalaxy 卫星文件共享协议(包括 Rhapsody)
BitTorrent	变态 (BT) 下载
Blubster	Blubster 文件共享协议
DirectConnect	NeoModus 文件共享协议
EarthStationV	EarthStation V p2p
EarthV-Search	EarthStation V 搜索数据流
EarthV-HTTP	基于 HTTP 的 EarthStation V 数据流
EarthV-SSL	EarthStation V 安全数据流
EarthV-PXP	EarthStation V pxp 文件传输
eDonkey	电驴 2000 文件共享应用服务组，像中国的 eMule 将会归在此类中
eDonkey-TCP	电驴 2000 数据流
eDonkey-Ping	电驴 2000 主机位置 ping 请求
FileRogue	FileRogue 文件共享应用
Filetopia	Filetopia 社区数据流
Furthurnet	Furthur 网络端到端文件共享
Gnutella	文件共享分布网络服务组 (多种相像的客户端归类为 Gnutella，如 Mutella, Shareaza, Xolox, Ares, Acquisition, Phex, Qtraxmax, 和 Morpheus)
Gnutella-Cmd	Gnutella 命令和询问数据流
Gnutella-Download	从外到里 Gnutella 文件传输

Gnutella-Init	Gnutella 初始连接
Gnutella-Upload	从里到外 Gnutella 文件传输
Groove	Groove 端到端应用
Hotline	Hotline 文件共享社区服务组
Hotline-TCP	Hotline 文件共享组 TCP 数据流
Hotline-UDP	Hotline 文件共享组 UDP 数据流
iMesh	端到端媒体交换
KaZaA	KaZaA 文件共享应用服务组 注意：MusicCity Morpheus 也归类到 KaZaA
KaZaA-Cmd	KaZaA 命令数据流
KaZaA-Download	KaZaA 文件传输，从外到里
KaZaA-Query	KaZaA 端服务器询问
KaZaA-Upload	KaZaA 文件传输，从里到外
Napster	Napster 音乐社区服务组（多种相像的客户端规类为 Napster，如 Gnapster, AudioGnone, Lopster, 和 Spotlight） 注意：Napster 通过 SOCKS 管道流也规类到 Napster 数据流。
Napster-Cmd	Napster 命令数据流
Napster-Data	Napster 数据流（上传/下载）
Napster-Init	Napster 初始连接到 napster.com 的数据流
Napster-UDP	Napster UDP 数据流（上传/下载）
PeerEnabler	基于 KaZaA (v2.5)的 Altnet 流，和 PeerEnabler 数据流
ScourExchange	ScourExchange 文件共享社区
Scour-Web	ScourExchange 网页数据流
Scour-CSC	ScourExchange CSC 协议
Tripnosis	Tripnosis 文件共享应用
打印流量	
IPP	Internet 打印协议
Printer	UNIX 排队打印（LPR）
tn3287	IBM 3270 打印数据流（TN 3287 的扩展）
tn5250p	基于 Telnet 的 IBM 5250 打印数据流
路由协议	
AURP	AppleTalk 基于更新的路由协议
BGP	Border 网关协议
CBT	内核树（多播路由协议）
DRP	DECnet 路由协议
EGP	外部网关协议（网络路由信息）
EIGRP	增强内部网关路由协议
IGMP	Internet 组管理协议
IGP	内部网关协议
OSPF	开放最短路径优先网络路由信息
PIM	不依赖协议的多播路由协议

RARP	反向地址解析协议
RIP	路由信息协议 (UDP 流)
SpanningTree	IEEE802.1 桥生成树
安全协议	
DLS	基于 TCP 传输的 SNA 链路交换数据流的服务组, 包含读写的端口号
DLS-RPN	数据链路交换读端口号
DLS-WPN	数据链路交换写端口号
DPA	微软分布式口令认证
GRE	通用路由封装
IPMobility	IP 最小封装【RFC 2004】
IPSec	IPSec 封装协议组
IPSec-AH	IPSec 认证头
IPSec-ESP	IPSec 封装安全有效负载
ISAKMP	ISAKMP/IKE 钥匙交换
L2TP	VPN 连接的二层通道协议 (UDP 封装)
PPTP	点到点通道协议
RC5DES	DES (数据加密标准) 加密应用
SOCKS	SOCKSv4 和 SOCKSv5 代理协议
SSH	安全平台远程登录协议, Telnet 加密访问
SSL	安全协议 (网页数据流安全), 像 HTTPS 访问
SSL-Shell	SSL 安全平台远程登录协议
SWIPE	网络层封装加密 IP 协议
会话层	
GoToMyPC	GoToMyPC 软件的 HTTP 数据流
pcAnywhere	远程管理协作工具服务组
pcAnywhere-D	pcAnywhere 数据流
pcAnywhere-OD	pcAnywhere 数据流 (旧端口)
pcAnywhere-OS	pcAnywhere 状态 (旧端口)
pcAnywhere-S	pcAnywhere 状态
Radmin	远程管理员 (远程控制软件)
Rexec	UNIX 远程执行协议
rlogin	远程登录
Rsh	UNIX 远程 shell (平台) 命令
Telnet	Telnet 终端服务组
Telnet-Clear	网络终端协议 (明文)
Telnet-Secure	安全的网络终端协议
Timbuktu	Timbuktu Pro 服务组 (网络远程控制)
Timbuktu-Ctl	Timbuktu 控制通道
Timbuktu-HS	Timbuktu 握手

Timbuktu-Obs	Timbuktu 观察通道
Timbuktu-Snd	Timbuktu 发送通道
Timbuktu-Xch	Timbuktu 交换通道
VNC	虚拟网络计算
XWindows	X11 窗口代理 (UDP 流)
XWindows-DM	Xwindows 显示管理器 (XDMCP)
XWindows-S	Xwindows 服务器
基于瘦客户机的应用	
Citrix	Citrix 连接应用服务组。使得任何客户端通过任意的网络连接都可以访问应用。
Citrix-ICA	Citrix 的独立计算机体系结构 (ICA)
Citrix-SB	Citrix 服务器浏览 (UDP 流)
CitrixIMA	Citrix 集成管理体系服务组
CitrixIMA-CMC	Citrix IMA 管理控制台
CitrixIMA-Svr	Citrix IMA 服务器到服务器
RDP	远程桌面协议 微软 windows 终端服务器
IP 语音 (VOIP)	
CiscoCTI	Cisco 计算机技术接口, Cisco IP 电话
Clarent-CC	Clarent IP 语音呼叫中心
Clarent-Complex	Clarent 复合数据流
Clarent-Mgmt	Clarent 管理数据流
Clarent-Voice-S	Clarent 语音数据流
CUSEeMe	视频聊天服务应用服务组, 网络视频, 有些软件视频会议系统也会使用此协议
CUSEeMe-AV	视频聊天服务 音频/视频
CUSEeMe-CC	视频聊天服务连接控制
CUSEeMe-CE	视频聊天服务连接建立
Dialpad	Dialpad 互联网电话服务组, 网络电话软件
Dialpad-Ctrl	Dialpad 互联网电话 控制流
Dialpad-Stream	Dialpad 互联网电话 RTP 流
H.323	互联网电话标准服务组, 电话会议、语音电话、Netmeeting 等使用
H.323-GKD	H.323 看门人发现
H.323-H.245	H.323 呼叫控制
H.323-Q.931	H.323 呼叫建立
H.323-RAS	H.323 看门人控制 (注册, 允许和状态)
I-Phone	Vocaltec 的互联网电话协议, 网络电话软件
MCK-Signaling	MCK 发信号 (非自动发现)
MCK-Voice	MCK 语音 (非自动发现)
Megaco	媒体网关控制 (H.248)
Megaco-Text	媒体网关控制 (H.248) 文本

Megaco-Bin	媒体网关控制 (H.248) 二进制
MGCP	媒体网关控制协议
MGCP-Gateway	媒体网关控制协议 网关
MGCP-CallAgent	媒体网关控制协议 呼叫代理
MGCP-KpAlive	媒体网关控制协议 保持激活连接
Micom-VIP	Micom 的 IP 语音 (V/P)
Net2Phone	Net2Phone 的通信中心, 网络电话
Net2Phone-TCP	Net2Phone 呼叫建立和控制
Net2Phone-UDP	Net2Phone 互联网电话呼叫
RTCP-B	实时控制协议 (广播), 视频会议的实时控制协议
RTCP-I	实时控制协议 (交互), 视频会议的实时控制协议
SIP	会话初始化协议, 网络电话软件或硬件, SIP Phone
SIP-UDP	会话初始化协议 UDP
SIP-TCP	会话初始化协议 TCP
Skinny	Cisco's Skinny 客户控制协议 (SCCP)。注意: 此服务不能自动发现, 但可以手动建起。
Skype	Skype P2P 技术应用, 网络电话软件
SkypeCommand	Skype 命令
SkypeData	Skype 数据
T.120	协作应用, Netmeeting 和视频会议的白板服务
VDOPhone	互联网电话服务组 (非自动发现), 网络电话
VDOPhone-a	互联网电话服务组 TCP 端口 1 (非自动发现)
VDOPhone-b	互联网电话服务组 TCP 端口 2 (非自动发现)
VDOPhone-UDP	VDOPhone 实时媒体流 (非自动发现)

应用的运行情况能否满足所有的期望?

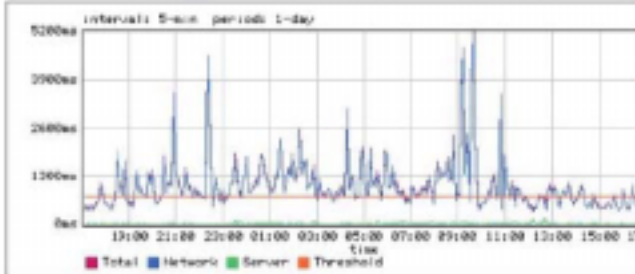
用户的抱怨是否是您度量响应时间的唯一方式? 如没有用户的这些呼叫, 您是否知道网络性能何时运行缓慢? 是否可以比用户更早知道这些情况呢?

Packeteer具有响应时间管理 (RTM) 的特性, 可以提供的信息包括: 运行中的数据统计、阈值监控、高层问题指示器和运行情况的图表。这些重要信息可以让网络管理者做到以下几点:

- ✧ 跟踪各个灵活分类流量的时延统计数据, 度量单个应用、主机、子网的响应时间, 以及面向交易的TCP流量分类的响应时间;
- ✧ 响应时间度量可分为网络延时 (传输时间) 和服务器延时 (服务器处理用户需求的时间);
- ✧ 识别出运行最慢的用户和服务器;

- ◇ 设置可接受的标准，并跟踪性能是否一直符合这些标准；
- ◇ 自动检测功能以及可选的自动纠正功能，改善关键应用糟糕的运行状况。

Transaction Delay

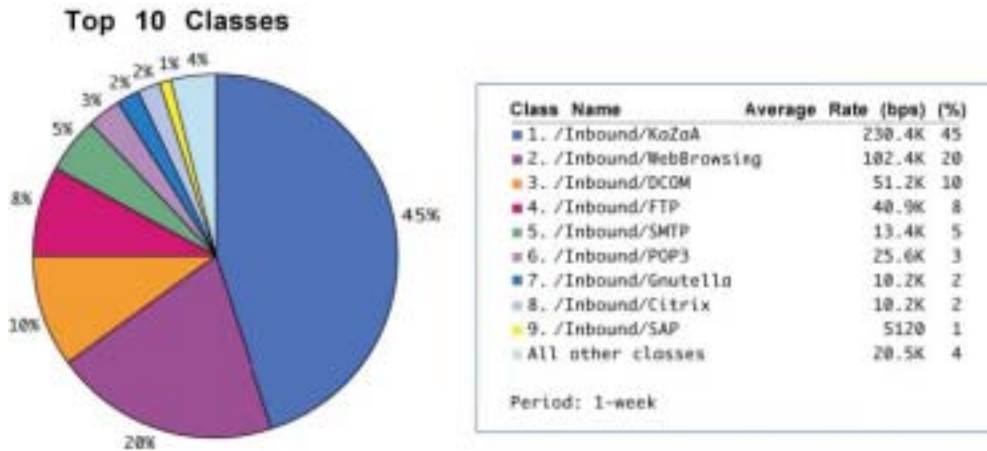


此图表显示了网络及服务器等各种交易延时，以及突发时产生响应时间的缓慢。我们可以看到导致此问题的并不是服务器，而是网络。如果发生这种状况的是关键应用，那么此应用的性能肯定是需要改善的，而整形模式在这种情况下便可以充分发挥其作用。

通过MIB库或XML API，您可以直观地查看当前以及历史的数据报表，并可以与第三方SNMP和报告工具无缝集成。

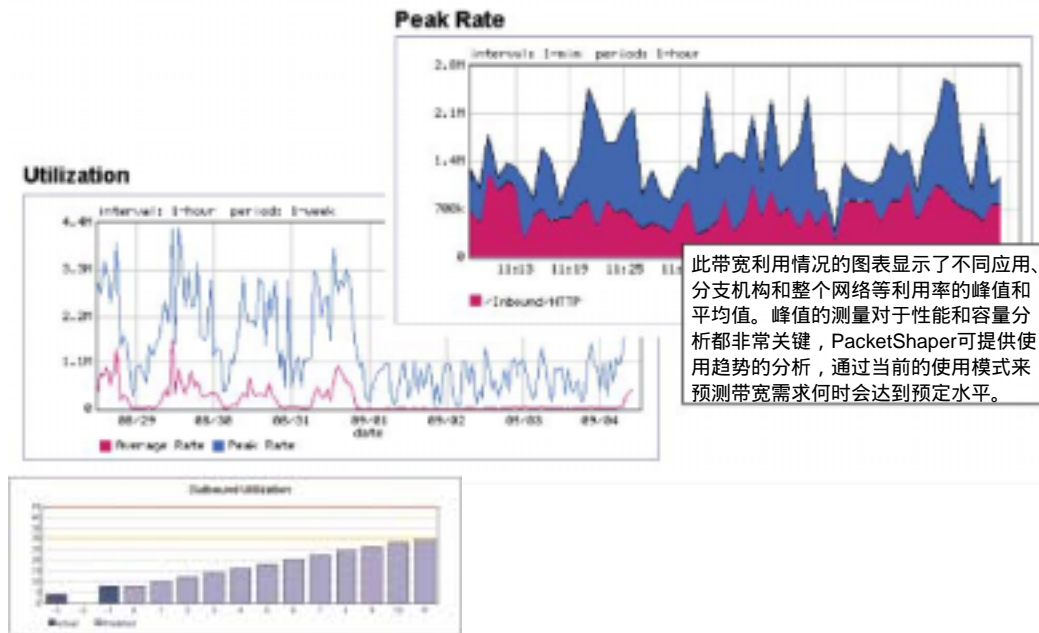
什么应用和什么人在占用带宽？

带宽是宝贵的资源，英特网及广域的链路更是昂贵却又总是面临拥塞。PacketShaper可以决定什么应用占用多少带宽，什么应用、协议和服务器可以被使用。



PacketShaper可以识别出占用最多带宽的用户、应用和网站，跟踪平均流量级别及峰值流量级别，评估网络效率，提供大量的度量数据，某种程度上可以替代探针和Sniffer。

PacketShaper还可以自动对单个流量分类数据进行更详细的展现；甚至如果您需要，也可以对单个用户和单个应用流的数据进行更细致的展现。



在什么时候发生了什么？

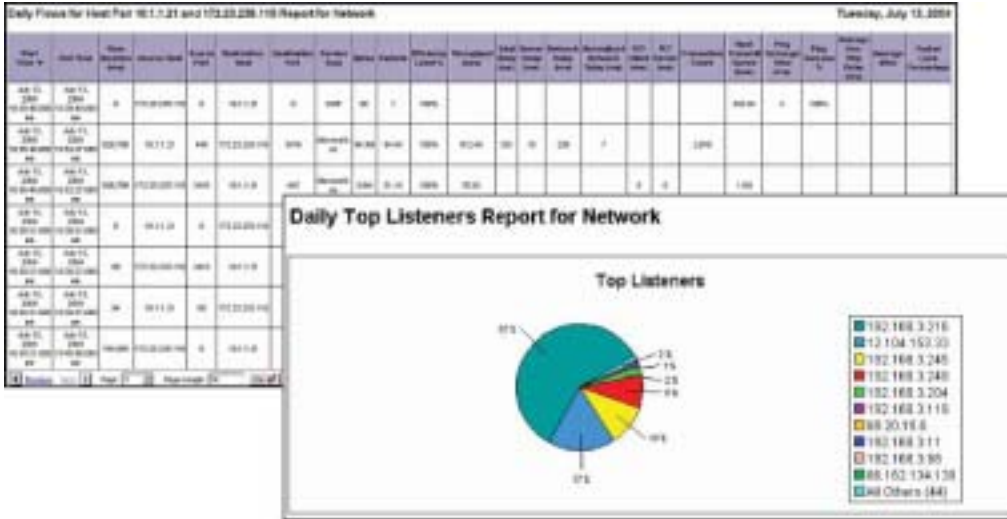
PacketShaper的综合报告可对于应用的性能、负载、网络效率、TCP健康和链接等提供清晰的视图。这些报告可以帮助您确认配置的改变，证明购买行为，评估服务水平是否符合之前的承诺，查找应用的历史趋势，对运行情况进行持续的评估。

您可以查看任何一个PacketShaper的预置报告，也可以运用存储的参数和几十个图表来定义和创建自己的报告，所有的报告均可以在网页上访问。Packeteer的ReportCenter还可为多种不同应用提供集中的报告功能，如对企业不同区域的分支机构的行为进行比较、相互关联和总结。用户可以在ReportCenter、SNMP管理平台、NetFlow v5 collectors、和第三方报告工具的报告中获得Packeteer大量的度量数据。Packeteer的度量数据可存储长达两个月，并且会不定期发到ReportCenter服务器上。PacketShaper也可以基于每个应用流来提供参数，包括流量的来源和目的地、流量的大小（以数据包或字节计算）、发送时间、流量的应用或服务、流量的第4层协议及IP ToS/Diff Serv Bit、流量所应用的控制种类、响应时间等等。

这个精细的细节分析可提高故障检测的能力，例如：

- ◇ 将一个分支机构的流量分离成不同的应用、协议或DSCP种类，即使在流量经过时您没有明确定义其子分类。
- ◇ 从一些特别的应用、地点或结合方式来检查交互式最多的主机IP对；
- ◇ 列出最繁忙的端口号，看一些特定的应用或主机在使用哪些端口，一些特定的端口又在使用哪些应用，发现潜在的端口扫描；

- ◇ 计费，对客户或部门基于不同应用的使用情况进行计费；如果需要，也可根据不同的应用类型来计费（如P2P、VoIP、邮件和网页浏览等）；
- ◇ 列出最近或历史上流量最高的贡献者、接收者和应用类别，甚至当出现问题您并没有运用这些特性时，Packeteer也会做这些检查；



网络上是否正在发生重要的事情？

报告对于很多的目标都颇有价值，但是当问题发生时，报告也并不是发现和响应问题的最好选择。报告要求有人为的干预----需要有人来检查、解释所发现的东西，并根据决定做出反应。

PacketShaper的自适应响应特性可自动监测用户的使用偏好，察觉潜在的问题并予以通报，并作出正确的反应。而您需要决定的是：

- ◇ 什么组成问题；
- ◇ 如果您要对问题进行报告，需决定采取何种方式获取通报信息（邮件、SNMP捕获还是Syslog信息）；
- ◇ 如果需要做出相应的反应，则哪种反应是比较恰当的；

PacketShaper可以提供很多预置的条件，或者您也可以自己定义，PacketShaper已自动包含了一些决定监控条件和响应的方法举例，如：

- ◇ 当重传占网络流量的15%时，则给HP OpenView发出告警；
- ◇ 不论何时，只要有10%的交易在两秒钟内得不到响应，则给SAP分配更多带宽或提高SAP的MPLS服务等级；

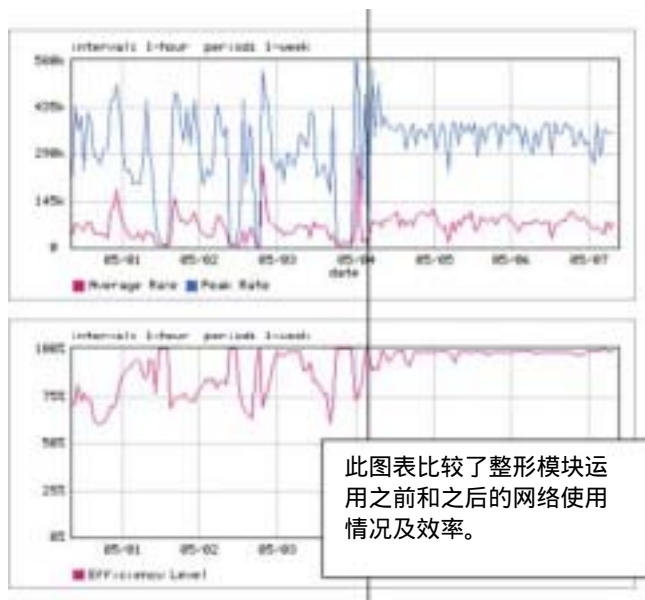
- ◇ 不论新的应用何时出现在网络上，当这些应用占据了总容量的8%或更多时，以邮件通知您；
- ◇ 当用户占用过多的带宽时，暂时遏制和隔离这些用户。

整形模块控制带宽

在拥塞的广域网和英特网接入链路中，对于带宽的争抢时时发生，占用大量带宽的应用（如大文件的下载和邮件中的大附件）占据了所有带宽，破坏关键应用的运行。丰富数据、网络中无处不在的协议、网络瓶颈、新的应用、流行应用和占用带宽极大的应用，所有这些似乎形成一个组合，共同破坏了关键应用的运行。

识别性能问题只是第一步，PacketShaper还可以解决性能问题：运用灵活的策略来保护关键应用，控制带宽分配，调整带宽占用大的流量，限制娱乐性应用和阻止恶意流量。

可控制每个应用、会话、用户或地点的最小和最大带宽，为每种流量设置特定的带宽分配策略，确保每个应用获得适当的带宽。



运用整形模块，您可以：

- ◇ 保护重要应用的性能，如SAP和Oracle；
- ◇ 限制未批准的流量和娱乐性流量，如KaZaA和AudioGalaxy；
- ◇ 保证语音和视频流量的稳定、流畅；

- ◇ 阻止应用或用户独占链路；
- ◇ 可为应用设置一个明确的速率、占用带宽的百分比和优先级；
- ◇ 使带宽分配策略能够适合实时应用的运行和适应突发故障；
- ◇ 检测病毒、蠕虫或攻击，减少对网络的影响；
- ◇ 平衡应用的连续访问和应用的带宽限制，这些应用如Microsoft Exchange，非常重要，但也需要大量带宽；
- ◇ 允许对延时敏感的小的流量快速通过，如Telnet；
- ◇ 在多个地点、小组和用户之间平等分配带宽；

应用控制功能

Packeteer提供丰富且灵活的机制来控制带宽分配，如“分区（Partition）”的特性，此特性可以用来保护或抑制某一应用。以下是整形模块的一些控制特性：

控制特性	具体描述	举例
分区（Partition）	运用分区可保护或限制某一分类中所有的应用，规定预留虚拟链路的大小，并选择是否可以超出这个大小或限制它的增长。分区的功能类似PVC，只是成本更小，并且可与其他流量共享那些未使用的带宽。	将音乐下载限制在T1广域网链路中的128Kpbs，为Microsoft Exchange保存至少20%的广域网链路，可超过此额度，但最高不得超过链路的60%。
动态的每用户分区（Dynamic Per-User Partitions）	为用户公平地分配带宽。当指定分类中的用户起始流量需要时，创建每用户的动态子分区。同样，未使用的带宽可分配给其他人。	学生宿舍的每个学生可以获得最少20Kbps，最多60Kbps的带宽，这些带宽的使用方式可由他们自己决定。
速率策略（Rate Policies）	确保关键应用和流媒体应用每会话的带宽。保护延时敏感的会话，用速率策略控制带宽占用大的流量会话。为流量的单个会话分配一个最小速率（此速率有可能为零），允许有优先权的会话使用额外带宽，并为其设置一个可使用带宽的最大额度	为每个VoIP会话预留刚好24Kbps，避免其抖动或停滞，同时FTP下载最高不超过56Kbps
优先权策略（Priority Policies）	优先权策略可基于应用的优先权来分配带宽，优先等级可从0级-7级。此策略特别适用于小的、非突发以及延时敏感的应用。	保护Telnet，优先级别为6级，占用带宽少但对延时敏感。对业务网上的游戏类应用，如Doom、Quake，设定优先级别为0级，只有在网络不繁忙时才可以使用的。
删除策略（Discard Policies）	此策略用来阻止流量，只是简单地将数据包扔掉，不会给发送者任何反馈信息。	将网站上有问题内容的流量删除，阻止Telnet到您的站点，阻止到您内部FTP服务器的外部请求。
禁止策略（Never-	此策略与删除策略相似，除了它会	对音乐网页重新定位，规定语音

Admit Policies)	将通知发送者。	流只可在22:00-6:00之间使用。
忽略策略 (Ignore Policies)	此策略可允许某些流量通过，不对其应用进行带宽管理。	如果流量的终点不是管理下的广域网接入链路，在其通过时都可不进行管理。

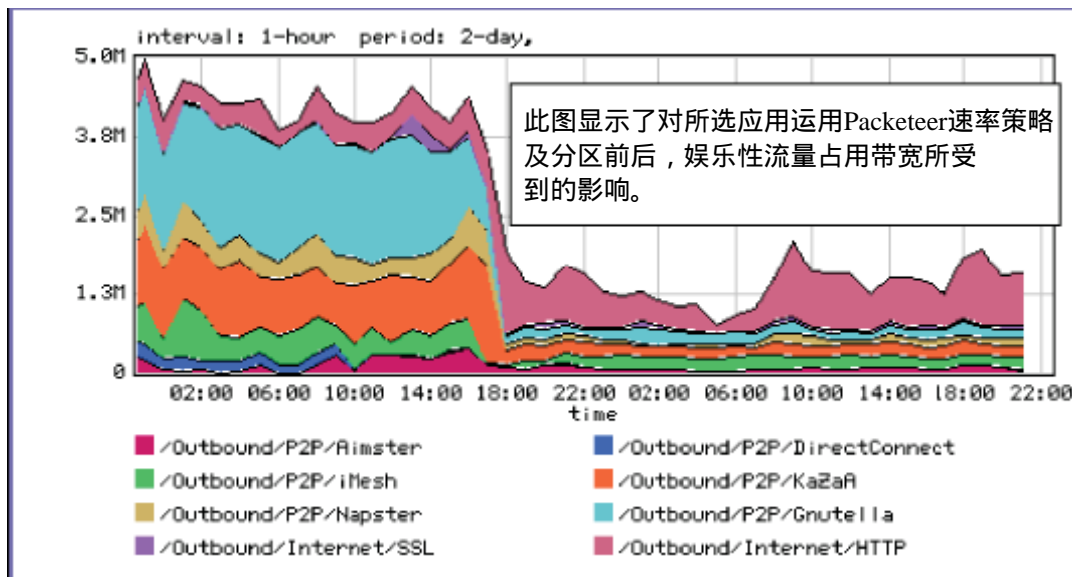
您可以将PacketShaper任一个控制特性明确地运用到某个特别的流量类型中，如某一应用或分支机构，您也可以将任一个自动响应的控制特性运用到实时的环境中。比如说，假设您为一个重要的销售应用保留了10%的带宽，在两种情况下您可以让这个份额自动提高到20%，1) 在每月末，2) 响应时间超过3秒（当您想要定义一个不可接受的性能时除外）。正如您所见，控制功能不仅灵活和强大，而且当这些功能被激活时，您有权选择。

速率控制技术

PacketShaper拥有多种控制技术，可对流入和流出广域网或英特网链路的流量速率进行控制。Packeteer的速率控制技术 - TCP速率控制、UDP速率控制和高级列队技术 - 共同创造并形成了一个平滑、均匀的流动速率，从而最大化吞吐率，并避免了网络的拥塞。

TCP速率控制

Packeteer的TCP速率控制技术运行在所有采用速率策略控制的流量后面，优化容量有限的链路。TCP速率控制克服了TCP的缺点，阻止了Inbound和Outbound的拥塞。TCP速率控制可计算流量速率，并通知流量的发送端减速或加速。但是如果数据包只有使用特定发送速率到达时才可接收，那么就没有必要加快传输速度。并且TCP速率控制是通过检测、计算数据包的发送及传输来避免拥塞，而不是在拥塞的队列中不断丢包。



不像TCP速率控制，列队方法需等待队列形成、拥塞发生后，重新将数据包排序然后再丢弃其中的一些。而且对于单独基于列队的解决方案，当流量在广域网的另一边进入时，此方案不能预先控制速率。更重要的是，基于列队的解决方案不是双向的，在流量从广域网流入局域网时也不能够控制速率，因为此处并没有队列。

TCP速率控制可检测实时流的速度，预先告知数据包到达的时间，计算确认信息的返回时间，并适当修改确认信息窗口的大小。正如路由器通过控制数据包的标题信息来控制包的方向，PacketShaper通过标题信息来控制包的速率。想象一下，当细微的沙粒通过一根麦秆或小小的管子时，沙粒平滑且迅速地通过了；而当大块的砂砾通过同样一根麦秆时，砂砾被陷住了。PacketShaper可调整流量，使流量更像是微小的沙粒，而不是大块的砂砾。在这种顺利控制的链接中，丢包几乎是不可能的现象，更重要的是，可以让最终用户享受到持续的可靠服务。

UDP速率控制

UDP不需要建立连接便可将数据发送给接收者，也不会检验到达的数据是否完好无损，由于UDP不管理端到端连接，因此不会获得有关实时连接的反馈，而且它无法阻止或适应拥塞。因此，UDP对过多的流量束手无策，从而会影响所有协议，包括UDP和TCP。此外，像VoIP这样对延时敏感流量会受到延迟而无法使用。

PacketShaper可以识别UDP数据流，并在UDP数据包穿过拥塞链路前调整其流量。整形模块的很多控制机制可帮助您管理UDP流量，如：

- ◇ 优先策略，对于面向交易的UDP流量来说是最好的；
- ◇ 速率策略，对于持久稳固的UDP流量来说也是最好的，因为其保证的Bps选项可确保实现每个UDP流量的最小速率。例如，您可以为每个VoIP流分配24Kbps。

UDP Delay Bound定义了数据包最大等待多长时间就需要放弃的时间，例如，语音流传输能够容忍的延迟限制为200ms。

提高特定网络环境下的性能

PacketShaper的控制特性可帮助作出适用性评估、进行日常管理事务、分析性能收益，以及较大网络环境中其它的支持，其中部分介绍如下：

数据包标记 (CoS/ToS/Diff serv/MPLS)

数据包标记是一种可确保在WAN与不同网络设备中进行快速处理的一种增长趋势，这种标准随着时间的推移已经得到了不断的发展。首先，IP中集成了CoS/ToS。接着，Diff serv成

为了针对一致服务质量的较新标记协议，它在本质上与ToS位相同，只是它们位数比较多。最近，MPLS已经作为最新的标准出现，它将指定网络路径的能力与服务分类进行了完美集成，从而实现了一致的QoS。

Packeteer可基于IP COS/TOS位、Diff serv 设置和MPLS标签进行分类、标记和重新标记流量，因此通过不同WAN中的多厂商设备可使各种流量类型得到统一的端到端处理。在致力于标记和重新标记方面，PacketShaper作为一种通用转换器，可检测一种协议的多个意图，并可在PacketShaper转发数据包时将这些意图与不同协议维系在一起。

增强MPLS性能

多协议标记交换（MPLS）已经成为企业连接各个分支机构的领先技术。大部分企业采用MPLS来获得服务分类所带来的好处，确保应用的良好运行。

但是，MPLS一旦执行，商业企业就会经常发现：给关键应用使用Premium Service Class并没有获得期望的利益，为什么？这是因为当MPLS解决方案在面对以下三种主要情况时，其功能就会下降：

- ◇ 流量没有恰当的分类到相应得MPLS服务等级中。当Premium Class采用冗长的非紧急流量处理时，就只能获得次优化的效果，重要的应用被不恰当地分配到Only Best-Effort分类中。
- ◇ 在流量进入服务供应商的MPLS网络入口处，拥塞的瓶颈造成流量就会被挂起。此外，未经管理的流量流入局域网时也会很难控制，流量速率会变得非常高；
- ◇ 企业需要掌握在MPLS网络上运行的每个应用和服务分类的运行情况的详细性能信息。简单的说，对于服务水平的评估，具体的、量化的指标非常少。

PacketShaper可以补充MPLS的部署，克服上述的局限：

- ◇ 检测、区分不同的应用并对其进行分类，同时分配不同的QoS标记。PacketShaper可以用MPLS标签直接作流量标识，或者用Diff Serv标记来作标识，将流量中继到MPLS云图内的第一个路由器。
- ◇ 确保特定MPLS服务分类中的流量是合适的流量。强大的、精细的应用分类可确保准确的、恰当的分配MPLS服务分类。
- ◇ 通过控制特性和速率控制，减缓MPLS网络入口点的瓶颈压力；
- ◇ 扩展MPLS的好处到网络边缘和用户处；
- ◇ 度量每个应用的性能和每个MPLS分类的性能，并用图表展现，评估是否满足服务水平协议（SLA）；

帮助语音/数据网络融合

在语音部署前后，PacketShaper都可帮助网络融合；在准备VoIP部署时，PacketShaper可以帮助企业来决定语音流量需要的带宽，通过模拟最大呼叫量，来评估对已有应用及性能所产生的影响，从而决定是否需要带宽进行扩容。

一旦VoIP和数据在同一网络上使用，PacketShaper可以：

- ◇ 区分多种语音流量，包括VDO Phone Vonage, Skype, CU See Me, Net-2Phone, Dialpad, RTCP, SIP, Megaco, MGCP, Skinny, MCK-Signaling, RTP, Micom VIP, MCK Voice 等；
- ◇ 作为一个整体，保护VoIP所需带宽；
- ◇ 为VoIP的部署清理网络流量并进行控制；
- ◇ 为每个语音流分配稳定的速率，保证其良好性能；
- ◇ 管理过度突发需求（如：公司的每个员工突然要同时使用电话）；
- ◇ 根据Diff serv、ToS和MPLS标记来分配适当QoS标签；
- ◇ 为相互竞争的应用，恰当的分配带宽；

检测和避免攻击

PacketShaper 不是防火墙，但它能够帮助检测病毒、蠕虫和 DoS 攻击，并且限制它们的影响。而且，PacketShaper 在临界点（企业释放补丁或解决方案来处理新出现的攻击之前）时尤其有用。PacketShaper 可运用多种方法和途径来帮您处理攻击：

- ◇ 识别异常情况的出现；
- ◇ 准确查明受感染的主机；
- ◇ 抑制那些由于受感染主机所导致的恶意流量；
- ◇ 任何时候都确保关键应用的性能，在异常情况出现时保证不会受到任何影响；
- ◇ 限制任何主机的连接数；
- ◇ 检测没有请求的 ICMP 回复，限制 ICMP 流量（ICMP 是一个频繁的攻击手段）；
- ◇ 检测来自未批准服务器的流量；
- ◇ 限制来自于一个应用、客户、服务器或任何种类流量分类的流量数量；
- ◇ 检测并阻止蠕虫，这些蠕虫有一些显著的嵌入字符串；
- ◇ 阻止那些假装来源可信任的流量；
- ◇ 揭露哪些流量在尝试使用流行的 80 端口，或其他任何端口；

压缩模块增加容量

PacketShaper 不仅仅提供对应用和网络行为的能见度和对带宽分配的控制，还可以对网络上的流量进行压缩。压缩可提高应用性能，创造更大的吞吐率，更快的性能以及更大的网络容量。

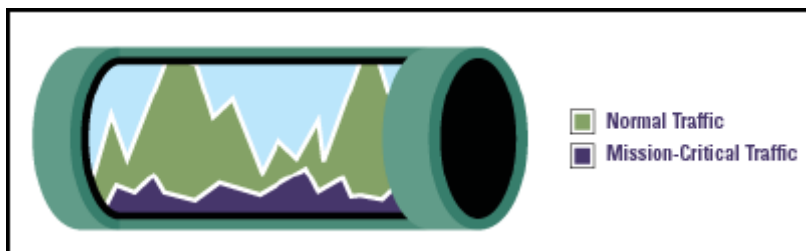
PacketShaper 的压缩模块采用已获得专利的压缩技术，可更快地传输数据，让更多的流量通过有限的广域网链路。当获得更多的带宽时，最关键业务应用的性能便可得到大大的提高。

通过压缩模块，您可以：

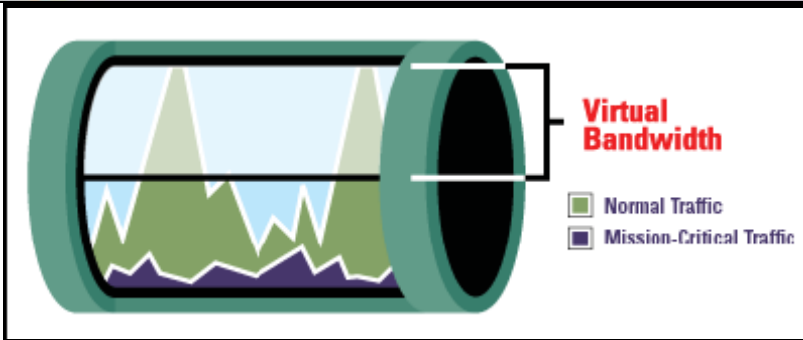
- ◇ 享受到压缩所得的最大 10 倍的容量，而且数据不会丢失；
- ◇ 容量增长，为关键应用增加直接带宽；
- ◇ 减缓饱和和广域网链路的拥塞；
- ◇ 延迟或避免带宽的扩容；
- ◇ 降低定义和保持压缩隧道，以及减少、传输和恢复流量的机制的压力；
- ◇ 为单个应用自适应选择压缩技术；
- ◇ 精简重复数据，缩小传输流量，以及减少数据包的数量。

整形和压缩组合使用

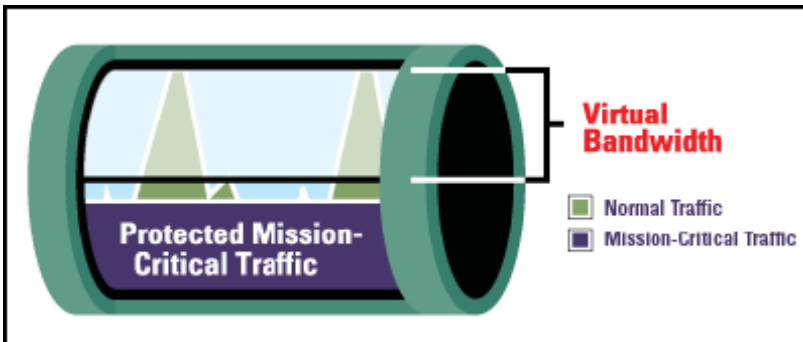
如果您使用 500Kbps 便可以传输 1.5Mbps 的 T1/E1 的流量，将会是什么情况呢？这将为其他的应用留出 1Mbps 的容量。那么谁可以获得这额外的带宽？是某一重要的交互式应用还是非紧急文件的传输？而后者很有可能最终赢得额外的带宽，除非由 PacketShaper 介入，来确保您的带宽分配，并控制整个链路的使用。



上图显示了未经管理的链路中，非紧急流量对于关键应用的影响。

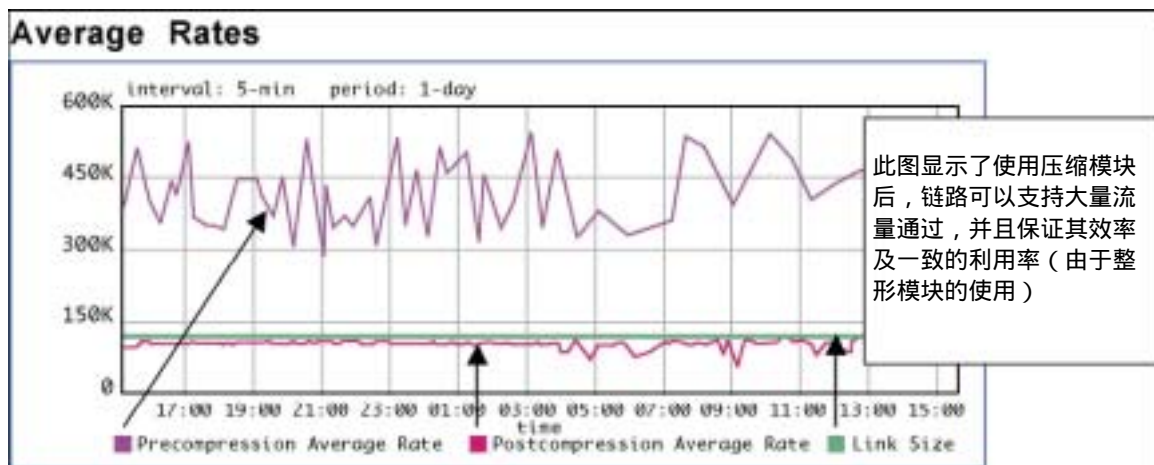


通过此图，我们可以知道压缩和带宽扩容还不能决定哪种流量可获得额外的容量。通过链路的流量越来越多，紧急任务的流量所需带宽得不到保证，如SAP和Oracle等都不能获得充足的带宽和持续的性能，反而那些非紧急的流量消耗了增长的容量部分。而PacketShaper除了可释放更多的带宽外，还提供对这些带宽有效运用及分配的能力，这样便可确保所有网络资源的分配，包括增加部分的带宽分配，都可以优先给最紧急和重要的应用。



上图中，PacketShaper运用整形模式，使关键应用获得所需带宽，确保其运行的持续和快速。剩下的带宽则提供给其它剩余流量，通过这个步骤，所有应用的性能均可得到明显改善。

当整形模块基于策略进行带宽分配和平滑突发流量时，压缩模块可帮助获得更大的网络吞吐率和更快的传播时间。



压缩功能如何工作？

实现Packeteer的压缩功能需要最少两台PacketShaper设备，部署在连接的两个端点。每个设备压缩Outbound流量，接收终点的设备解压缩Inbound流量，将流量恢复至原始状态。大部分的企业都会在其各个分支机构分别部署一台PacketShaper，这样各分支机构之间以及与主站点之间都可以交换流量。这种部署方案可充分利用整个企业的所有带宽。

两台PacketShaper设备之间的连接被称为压缩隧道（Xpress Tunnel），压缩数据便是由此隧道发送，而两台设备便是我们所说的“隧道伙伴”，详见42页的“压缩隧道”。

PacketShaper对通过的每个数据包都会自动进行监控，根据数据包流量的种类来决定压缩是否合适。之前已压缩的流量（如流媒体）和加密数据（如HTTPS和SSH）不会再次进行压缩。PacketShaper只对可能产生效果的流量进行压缩。

Packeteer可提供压缩算法的多种选择。通常来说，应用从某一种压缩方法所获效果会比其他方法要多，如P2P和即时通信通过CNA算法获益最多，邮件和HTTP可通过ICNA取得最好的效果，VoIP会自动使用UDPRT算法（此算法仅对UDP包头进行压缩）。另外，PacketShaper还提供创建规则的选择，用来决定哪种流量使用何种压缩算法，或者根据用户的使用偏好，避免这个选择这个算法，保持最好的效果。

数据包打包

压缩模块中的另一种能力是“数据包打包”。启动此功能后，若干数据包在发送到压缩隧道之前会组合成一个单独的“超级数据包”，减少了发送数据包的数量，节省了由数据包头引起的额外开销。对于特定的隧道或基于每个分类或每种服务类型，您可以启动或关闭此打包功能。

超级数据包的最大尺寸由MTU决定。MTU是最大的数据包，可以通过IP接口传输，无需分解成更小的单元。因为数据包尺寸可增加至MTU的最大限度，所以打包可改善链路的利用情况。MTU可以全局设置也可以为单一隧道而设置。

因为不同的流量类型可以容忍不同的延时量，所以可为每个服务类型分配其适当的*pack holding time*（数据包等待保持时间）——指超级数据包等待其他数据包被打包进来的时间。例如，对延时敏感的服务分配到1毫秒的等待时间，Telnet和Skype便属于这种典型的服务类型。打包的默认设置可适用于大多数情况，但如果您需要，也可通过CLI命令来对这些设置进行细微的调整。

由于数据包在组合过程中所固有的延时现象，打包会加剧网络延时的情况。但是在繁忙的链路中，打包并不会引起太多延时，这时因为数据包已被捆在一起并被迅速地发送出去，而

在不太活跃的链路中，Xpress可能需要等待将足够的数据包捆在一起，因此可能会导致某些应用的性能问题。所以如果您怀疑打包已引起延时，您可以降低数据包的等待保持时间或者停止打包。总的来说，在处理小数据包时或者数据包可以被减少时，打包是高效的、效果显著的方法。

压缩的效果

在标准术语中，压缩比例、压缩百分比和其他的术语等通常都被用来描述所取得的效果。如100byte的数据被压缩成33byte，则压缩比例是3：1，压缩百分比是67%。

某些厂商承诺10：1的压缩比例，但是这些数据是基于测试的最好结果，实际上，PacketShaper在测试中也可以达到90%的压缩百分比或10：1的比例。但不论是Packeteer还是其他的厂商做出如此陈述，都不能够代表实际使用中可取得的长期效果。所以当实际执行时，压缩比例的期望值范围应该是在2：1到3：1之间。

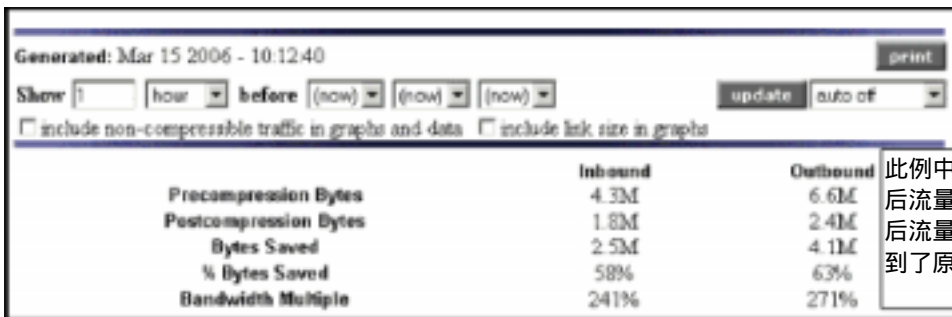
压缩比率表		
应用	平均压缩比	最大压缩比
Baan	80%	90%
Citrix	50%	75%
Compressed Citrix	15%	35%
FTP	50%	95%
General Internet	45%	75%
ICMP (ping)	50%	95%
JD Edwards	80%	90%
Mail	55%	90%
Microsoft-DS	65%	90%
NetBIOS	65%	90%
Oracle	75%	95%
PeopleSoft	80%	90%
SAP	75%	90%
Secure Applications (SSL, IPsec, SSH)	0%	0%
SQL Server	75%	95%
Sybase	75%	95%
Telnet	60%	85%
VoIP*	10%	25%
Web-Based Applications (Intranet)	75%	95%

*尽管VoIP数据在传到网络时已被IP电话应用压缩到了极致，但是PacketShaper的压缩模块仍然可以通过包头压缩功能和打包技术来对VoIP流量进行压缩。Packeteer收集了多种不同应用的压

缩结果，包括内部的测试和客户在他们的网络上对自己的应用使用Packeteer压缩功能的测试。当检查压缩效果时，需注意压缩的效果会根据网络负载水平、时间间隔和网络环境的不同而不断变化，有时候甚至相差很远。

压缩效果报告

PacketShaper可以提供大量的报告，来帮助判断流量压缩所取得的效果。以下为三个简单的例子：



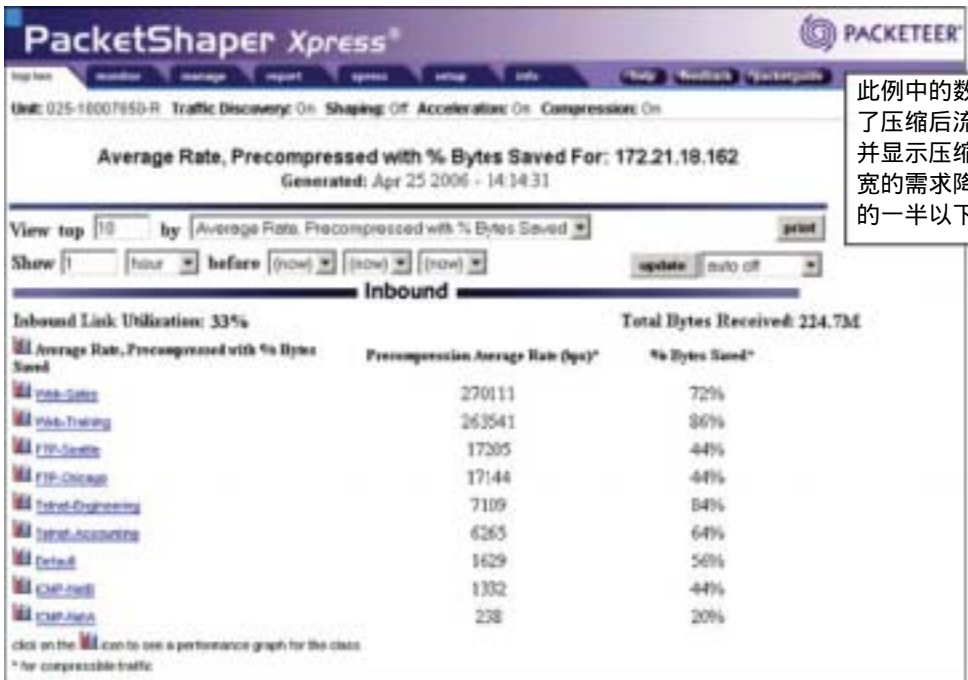
Generated: Mar 15 2006 - 10:12:40

Show 1 hour before (now) (now) (now) update auto off

include non-compressible traffic in graphs and data include link size in graphs

	Inbound	Outbound
Precompression Bytes	4.3M	6.6M
Postcompression Bytes	1.8M	2.4M
Bytes Saved	2.5M	4.1M
% Bytes Saved	58%	63%
Bandwidth Multiple	241%	271%

此例中的数据概括了压缩后流量的状况，显示压缩后流量对带宽的需求降低到了原来的一半以下。



PacketShaper Xpress

Unit: 025-10007650-R Traffic Discovery: On Shaping: Off Accelerator: On Compression: On

Average Rate, Precompressed with % Bytes Saved For: 172.21.18.162
Generated: Apr 25 2006 - 14:14:31


View top 10 by Average Rate, Precompressed with % Bytes Saved print

Show 1 hour before (now) (now) (now) update auto off

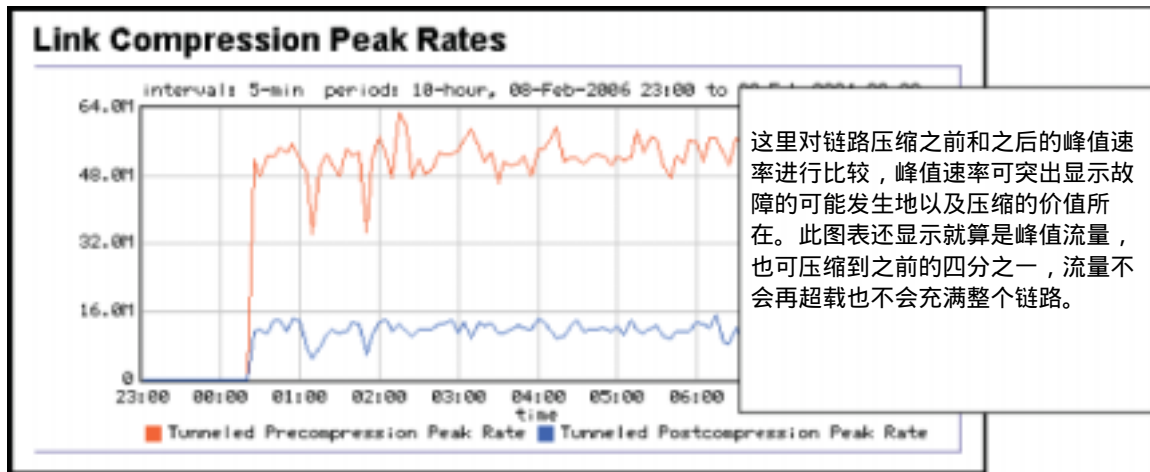
Inbound

Inbound Link Utilization: 33% Total Bytes Received: 214.7M

Average Rate, Precompressed with % Bytes Saved	Precompression Average Rate (bps)*	% Bytes Saved*
web Sites	270111	72%
web Training	263541	86%
ftp-Savite	17205	44%
ftp-Chicago	17144	44%
Telnet-Engineering	7109	84%
Telnet-Accounting	6265	64%
Default	1629	50%
cslr.net	1332	44%
cslr.net	238	20%

click on the  can to see a performance graph for the data.
* for compressible traffic

此例中的数据同样概括了压缩后流量的状况，并显示压缩后流量对带宽的需求降低到了原来的一半以下。



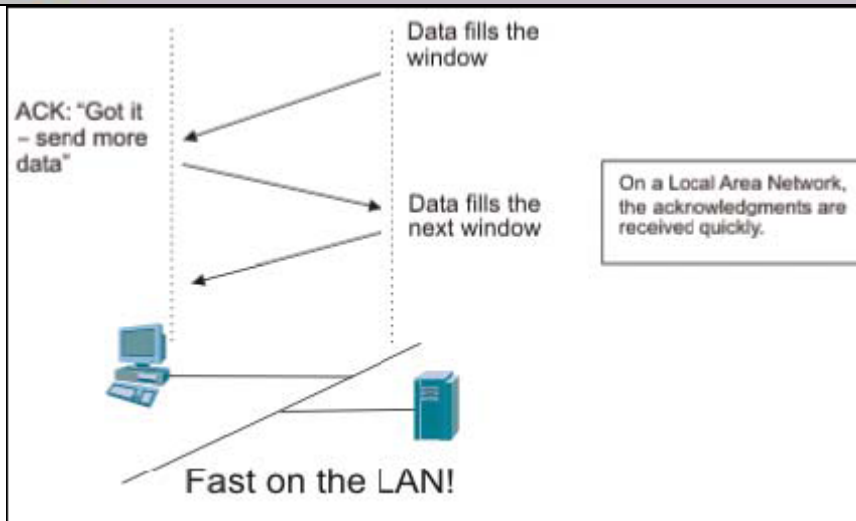
加速模块增强性能

重要文件传输缓慢；早上到达办公室时，服务器的夜间备份仍然没有结束；客户数据库中糟糕的响应时间使得最有耐心的人也会放弃；以上的这些仅仅是部分性能问题的举例。最初您可能想要通过带宽扩容来解决这些问题，但是马上就会发现增加带宽也不是解决方案。这是因为带宽消耗大的应用——并不完全是客户的关键应用——吞噬了所有新增加的带宽，而且已有的协议限制也使得应用不能完成利用所有可用带宽。

如果增加带宽不能解决问题，那么什么方法可以呢？加速模块，Packeteer的广域网应用优化套装软件的可选功能，可以帮助改善下列网络环境中的应用性能，如大带宽链路、大文件传输、高时延、相当大的网络交易等。在我们深入了解加速模块的具体技术之前，让我们来检查一下这些问题会导致的后果。

TCP：有问题的协议

TCP是在IP网络进行数据传输的可靠协议，但是传统的TCP协议会带来更高时延的连接，TCP利用滑动窗口机制来对传输的数据数量进行限制。当这个窗口被充满时，发送者就停止发送，直到收到新的确认信息（ACK）。在长距离的网络中，确认信息返回速度缓慢，TCP窗口尺寸通常会限制最大的发送速率。每个操作系统都预先设定了最大窗口尺寸，例如，Windows 2000窗口尺寸为16KB；Windows XP可达64KB。

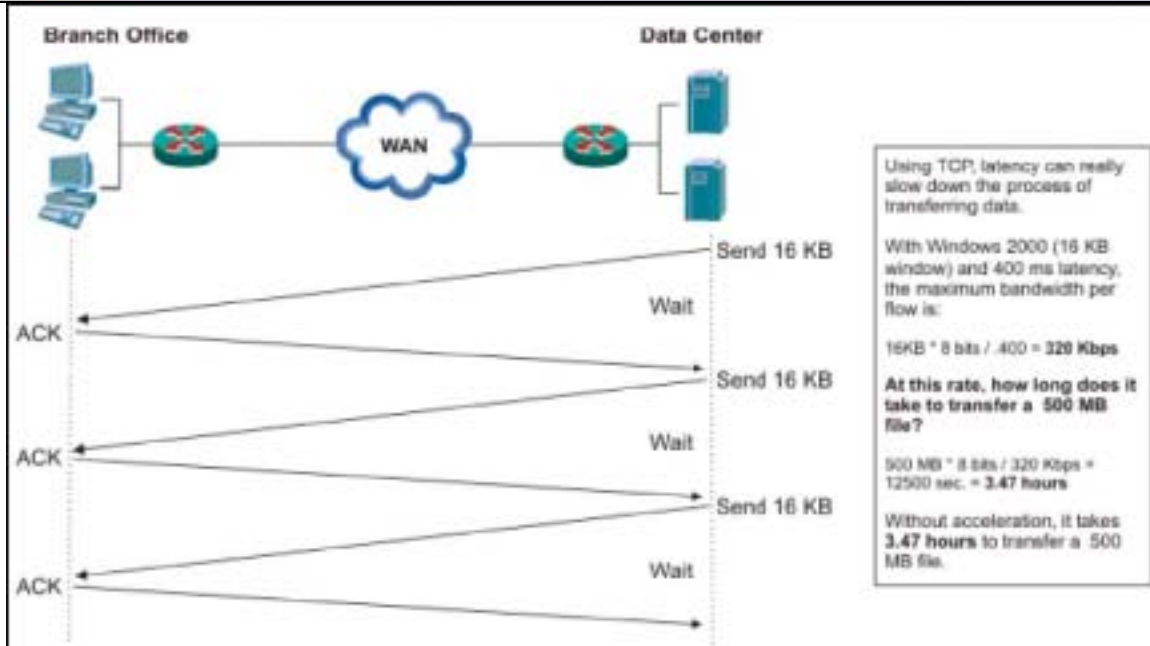


根据链路的距离远近，收到ACK的时间可在15毫秒到600毫秒之间。

WAN链路平均时延

同城 15 ms
地区 30 ms
省内 100 ms
跨省 200 ms
卫星 600 ms

当距离增大时，ACK的等待时间也同样增加。假设使用的操作系统为Windows 2000（窗口尺寸为16KB），一旦收到ACK，下一个16KB的数据就会被发送出去，这对于每个16KB的窗口都是一样的。当延时增加时，大链路的利用率就会越来越低，因为宝贵的时间都用来等待确认信息了。结果是数据不能迅速地发送，无法利用可用带宽，大量的链路带宽被浪费。从用户的角度来说，网络上的所有事情都变慢了，包括文件传输、网页浏览、邮件同步和对基于网页的应用的使用。



一个典型的例子是连接数据中心的广域网链路，这些数据中心之间较大的连接链路（DS3，45 Mbps，OC-3/STM-1/155 Mbps）本来能承担越来越多的流量。目前，使用较大连接链路来加速灾难备份的速度、加快服务器同步、分布式存储等，都是很好的办法。但是大部分的服务器镜像和灾难备份的解决方案是使用TCP协议来进行文件传输。

链路大小	潜在的，Windows XP浪费的带宽	潜在的，Windows 2000浪费的带宽
512Kbps	0	0
2Mbps	0	720Kbps (36%)
10Mbps	4.8Mbps (48%)	8.7Mbps (87%)
45Mbps	39.8Mbps (88%)	43.7Mbps (97%)
155Mbps	149.8Mbps (96%)	153.7Mbps (99%)

假设有一个业务应用运行在Windows XP操作系统上，并通过100毫秒时延的洲际链路，则单个流量最大值是5.1Mbps。在45Mbps的链路上，大约88%的带宽都会由于TCP和窗口尺寸的限制而被浪费。而且用户期望通过更大的链路来进行更有效的备份和同步，当用户的这个期望不能满足时，便会希望通过增加更多带宽来解决这个问题，因此将网络链路扩到155Mbps上，然而这仅仅是制造了更多的浪费，大约有96%的带宽仍然没有被利用。当可用带宽由于TCP和延时限制造而没有充分利用时，其结果就造成了带宽的浪费，满足不了性能指标。当大文件的传输及交互式应用都非常缓慢时，生产效率会受到消极影响，于是对这些传输和应用的加速便是解决问题的关键。

Packeteer 的解决方案

要消除网络上的延时几乎是不可能的，但这并不意味着我们只能无奈地忍受，而没有办法来减轻它的影响。Packeteer的加速模块便可最大化地减少高时延带来的消极影响，减轻以下问题：

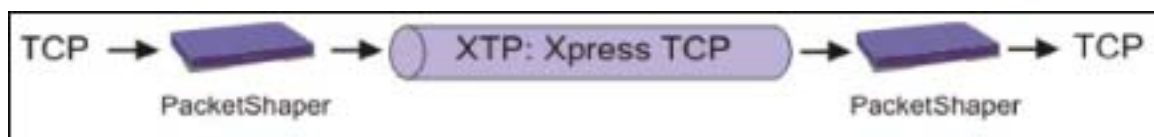
- ◇ 占用带宽大的流量的糟糕性能，如大文件传输、灾后备份、数据库同步等等；
- ◇ 丢包和重传所造成的影响；
- ◇ 广域网带宽的浪费和链路的未充分利用；
- ◇ 基于大量交易的用户关键应用；
- ◇ 未响应的HTTP会话；

Packeteer可同时为交易和文件传输提供加速，提高网络性能。在正常情况下，对于高延时的链路，加速可显著改善其性能-----使网页浏览速度增加8倍，文件下载加快50倍。

Xpress TCP

由于TCP对于高时延网络来说并不是一个合适的传输协议，所以PacketShaper提供了另外一种技术，来解决高时延环境中使用TCP时所产生的问题，这种技术称为“Xpress TCP”。

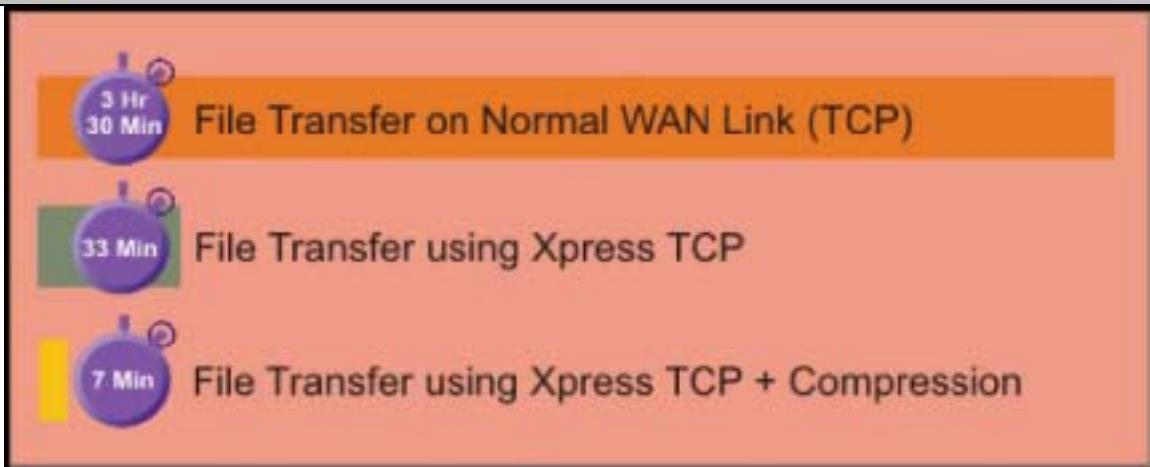
在Xpress TCP作为加速流量的传输协议时，PacketShaper就从客户处截取TCP连接，将数据转变成XTP，然后再通过压缩隧道，而在隧道另一端的PacketShaper设备在收到数据后会将XTP再转变成TCP。



Xpress TCP同时也具有标准TCP的优点。首先，Xpress TCP是高性能的协议，不会受到正常TCP操作的窗口限制，从而使广域网链路的带宽得到充分利用。然后，Xpress TCP使用基于速率的拥塞控制，能够确保连接使用可用带宽。最后，运用Xpress TCP技术，ACK被发回到当地站点，使得客户和服务器的之间的数据交换速度相当于局域网内的响应速度。

当出现丢包时，有选择的ACK会在客户反应前重发。这种技术通过汇总应用于TCP的FEC（Forward Error Correction）避免了带宽**开销（TAX）**。

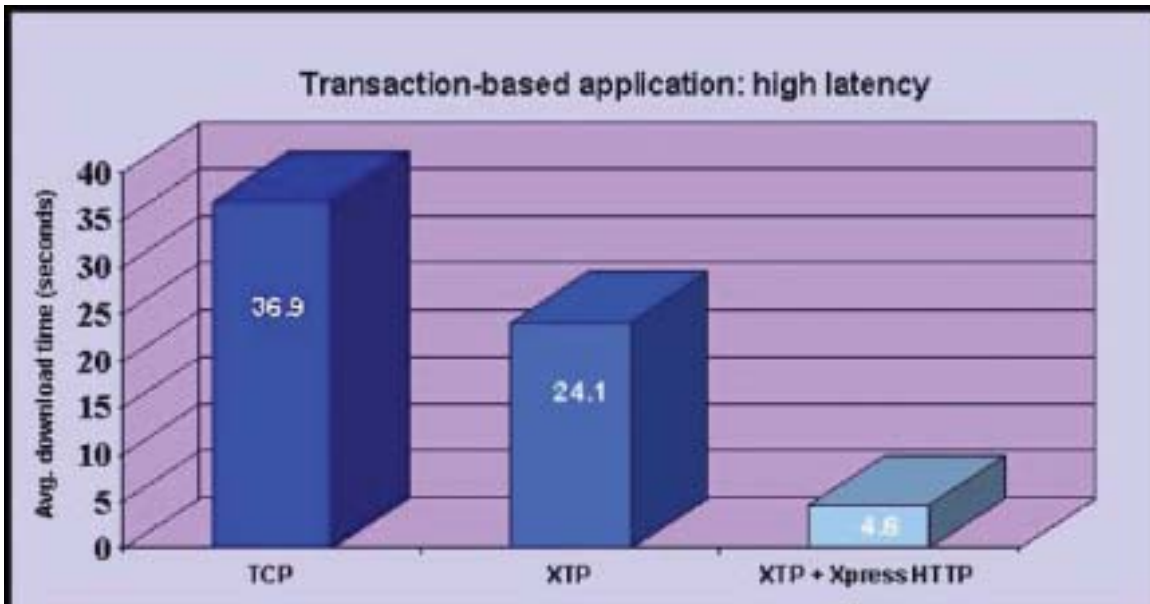
让我们回到之前的举例，500MB的文件传输大约需要3.5小时，通过使用Xpress TCP来代替标准的TCP，2M的链路全部可用，相同的文件传输只需33分钟（加快了7倍），如果您结合使用压缩模块和加速模块，则500MB的文件传输只需不到7分钟的时间（加快了30倍）。



Xpress HTTP

加速模块可以显著改善高时延链路上的基于网页和XML的应用的性能，这项技术称为“Xpress HTTP”。当加速功能启用时，网页的显示速度可提高8倍。以下两种特性可以让您加快HTTP流量：FastStart和Prefetch。

FastStart特性是通过减少建立每个HTTP新连接的时间，来加快网页下载的速度。使用FastStart，PacketShaper无需等待建立网络服务器连接的时间，便可立即确认TCP连接，这个迅速的确认信息使得浏览器可立即发送它的HTTP GET需求，而PacketShaper接下来会组合HTTP GET需求和XTP连接需求，这个过程可将HTTP需求传递到网络服务器的来回时间减少一圈。而对于包含大量对象和主题的网页来说，FastStart极大地提高了显示的响应速度。



Prefetch特性也可减少网页下载及显示的时间，服务器端的PacketShaper设备可拦截那些网络服务器所送回的HTML网页，并开始检索这个页面上的嵌入图表和其他对象。然后，这台设备将这些对象送到链路的另一端，也就是放置另一台PacketShaper设备的客户端，当浏览器

提出需求时，这台客户端设备就为立刻提供服务，由此避免了网络延时。但在多种情况下，这些对象通常在浏览器提出需求之前就会到达客户端。

加速与其他优化工具结合

当需要最大化地对应用性能进行改善时，各种优化技术的组合使用便成为关键。

Packeteer的各种技术 - 监控、整形、压缩和加速---可工作在一起，用以改善网络上的应用性能。为了获得最大利益，这些技术应该同时应用。当用户正在为性能问题而苦恼时，Packeteer的多种软件模块便可以结合在一起使用，解决出现的问题：

- ◇ **监控**是第一步，可识别网络上的各种应用并进行分类，此模块对其他优化工具是必需的；
- ◇ **整形**可抑制娱乐性流量，保证关键应用的带宽，为用户确保应得的服务质量；
- ◇ **压缩**可有效地扩大物理链路尺寸，使应用增加额外带宽；
- ◇ **加速**允许流量充满整条链路，不会浪费带宽，而加速的结果是应用性能获得改善、响应时间也在可以接受的范围。通过使用PacketShaper，提供应用智能化的能见度、控制和压缩，客户可以决定：什么应用可以占用带宽，可占用多少带宽等。此外，加速可以减少时延和克服文件传输、数据备份及远程站点同步等应用的TCP协议限制。

您可以从加速中获益吗？

正如之前所解释的，大带宽的链路并不能保证其带宽都可以被充分利用，操作系统的窗口尺寸和链路时延都是链路容量是否可以充满的因素。通过评估链路利用率来帮您决定：您的网络是否可以从加速模块中获益。

Packeteer开发了一个在线的“链路利用率计算器”，您只需：选择您的操作系统；以毫秒为单位输入时延；输入链路大小；估计压缩所节省带宽（如果您正在使用或计划使用压缩模块），那么这个计算器就会告诉您：单个流量可以占用链路的多少；从而确定，加速是否对您的网络环境有帮助等等。



PACKETEER® Fast WAN. Fast Apps. Fast Business.

Link Utilization Calculator

How much wasted bandwidth can you reclaim? Although a lot will depend on your application, estimating your link's percent utilization can take you some way toward determining how much you can benefit from Xpress TCP acceleration. Your operating system's window size, latency, and link size are factors that go into calculating how much of the link can be utilized per flow. Because PacketShaper compression effectively increases your bandwidth, you'll need to indicate the expected compression savings if you are planning on using compression; this allows the virtual link size to be calculated.

Fill in the fields below:

*Operating System	<input type="text" value="*****"/>
*Latency (in milliseconds)	<input type="text"/> ms
*Link size (in Mbps)	<input type="text"/> Mbps
Expected Compression Savings	<input type="text"/> %

Calculate Utilization

* indicates a required field

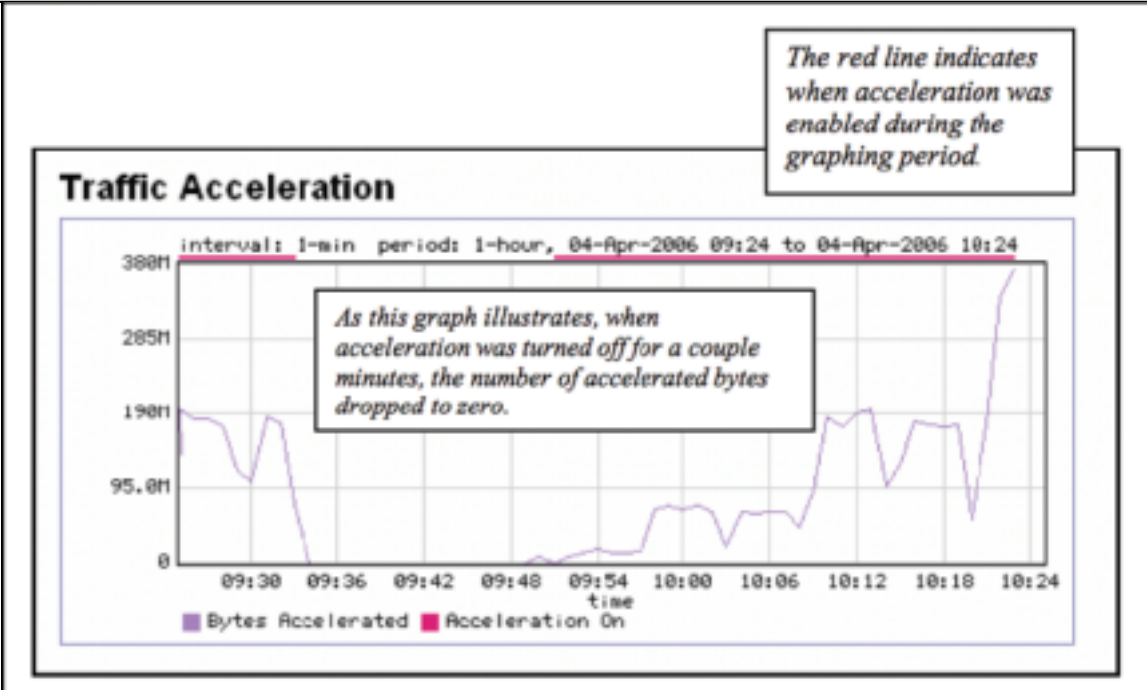
如果链路利用率计算器表明加速可以提供帮助，则接下来的一步就是查看您网络中应用的类型，加速对以下的流量类型是最有用的：

- ◇ 大文件传输（CAD、X-rays、法律文件、多媒体文件、印刷文件）；
- ◇ 数据库同步；
- ◇ 服务器备份；
- ◇ 存储镜像；
- ◇ 网络门户；
- ◇ 基于网页的应用；
- ◇ 基于XML的Web服务；

对于大交易应用，如客户从ERP或CRM发出的请求，同样可以通过加速来获得显著帮助。对于基于交易但包很小的应用，Xpress TCP可能没有帮助。这种类型的流量更适合的解决方案是Packeteer的拥塞管理技术，在整形和压缩模块中所含。

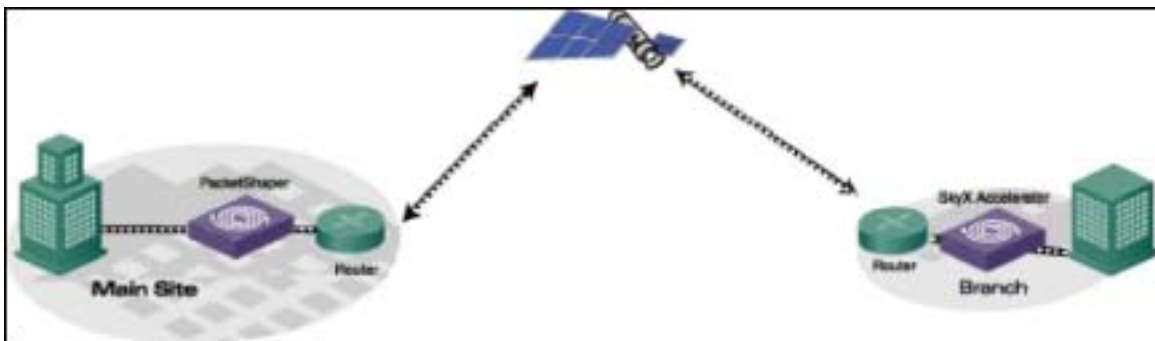
多少流量被加速了？

关于加速模块如何运行在链路上，“流量加速总结报告”可以帮助看到表述。两个图表来表示，分别代表流量的Inbound方向和Outbound方向。每个图表表示了通过加速隧道中已加速字节的带宽利用。如果在图表中所表示时期中的任何一点运用加速，图表上方就会显示一条红色的水平线。



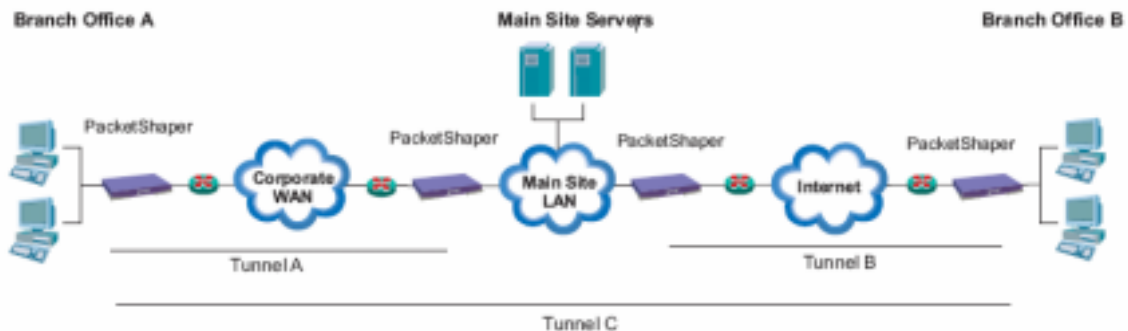
SkyX 与 PacketShaper 兼容性

除了与其它PacketShaper设备建立通道，加速模块还可以与SkyX加速器，Packeteer专门的加速硬件设备，建立通道。SkyX提供的功能与加速模块相似：它可以加速高时延链路中的TCP。使用SkyX通道，您可以对通过PacketShaper这边的主机和SkyX加速器那边的主机之间的流量进行加速。



压缩隧道

压缩隧道是两台PacketShaper设备之间的通信通道，它的功能是传输已经被压缩、打包和加速的数据。下图显示了三条压缩隧道，隧道A设置在分支机构A和主站点间；隧道B在另一个分支机构B和主站点间；隧道C在这两个分支机构之间。

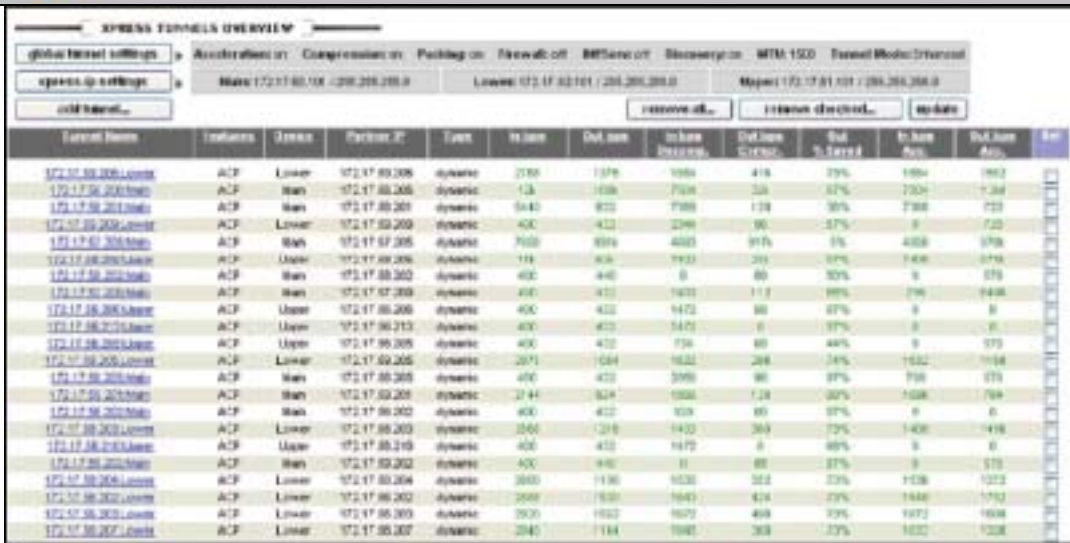


活动隧道

Packeteer活动隧道的特性对网络上的PacketShaper设备进行自动检测，并在他们之间建立Xpress隧道，这种隧道称为动态隧道；相应的，您也可手动定义隧道的端点，这种隧道称为静态隧道。PacketShaper可对隧道中传输的流量不断进行监控，当发现隧道对资源的要求过度而资源有限时，PacketShaper就会自动决定：对于那些效果最好的隧道，保证他们继续活动；同时，释放低利用率的隧道，来支持更活跃、更有价值的隧道。尽管Packeteer最大支持300条活动隧道（具体数量由型号和内存决定），但是它仍然可以产生更多潜在的隧道，并坚持最有效的隧道为活动隧道，而临时释放低效隧道。活动隧道这种产生大量隧道的能力，以及保持高效隧道能力，可使网络边缘的每台PacketShaper设备都无缝连接到网状环境中。在网状环境中，只要在每个端点部署了一台PacketShaper设备，则每个连接都可以拥有一条隧道。在PacketShaper看来，隧道的数量问题就不再是问题。

隧道监控和配置

尽管活动隧道特性可对所有隧道进行自动管理，仍然需要：查看有多少隧道是活动的、这些隧道的伙伴分别是谁、压缩和加速在每个隧道中运行的如何、哪些隧道出现了故障等等。如下所示“加速隧道概述”提供了这方面信息的实时写照，列出了所有与PacketShaper设备建立的隧道及每一隧道统计数据。



Tunnel Name	Features	Usage	Partner IP	Type	In Use	Out Use	In Use Bytes	Out Use Bytes	In Use Comp.	In Use Acc.	Out Use Acc.	Out Use Comp.
172.17.0.201.com	ACF	Lower	172.17.0.201	dynamic	278	1376	1086	416	33%	1804	1802	
172.17.0.202.com	ACF	Web	172.17.0.202	dynamic	126	108	704	28	37%	704	704	
172.17.0.203.com	ACF	Web	172.17.0.203	dynamic	540	822	788	128	36%	788	722	
172.17.0.204.com	ACF	Lower	172.17.0.204	dynamic	408	422	234	80	37%	0	722	
172.17.0.205.com	ACF	Web	172.17.0.205	dynamic	702	836	422	976	37%	422	278	
172.17.0.206.com	ACF	Upper	172.17.0.206	dynamic	716	824	1922	20	37%	1922	1976	
172.17.0.207.com	ACF	Web	172.17.0.207	dynamic	408	440	0	80	32%	0	0	
172.17.0.208.com	ACF	Web	172.17.0.208	dynamic	408	422	1422	112	36%	796	1428	
172.17.0.209.com	ACF	Upper	172.17.0.209	dynamic	408	422	1422	80	37%	0	0	
172.17.0.210.com	ACF	Upper	172.17.0.210	dynamic	408	422	1422	0	37%	0	0	
172.17.0.211.com	ACF	Upper	172.17.0.211	dynamic	408	422	736	80	44%	0	0	
172.17.0.212.com	ACF	Lower	172.17.0.212	dynamic	2071	104	1622	288	74%	1622	1618	
172.17.0.213.com	ACF	Web	172.17.0.213	dynamic	408	422	308	80	37%	796	0	
172.17.0.214.com	ACF	Web	172.17.0.214	dynamic	2144	624	1086	128	36%	1086	796	
172.17.0.215.com	ACF	Web	172.17.0.215	dynamic	408	422	308	80	37%	0	0	
172.17.0.216.com	ACF	Lower	172.17.0.216	dynamic	2064	1216	1422	368	72%	1422	1418	
172.17.0.217.com	ACF	Upper	172.17.0.217	dynamic	408	422	1422	0	48%	0	0	
172.17.0.218.com	ACF	Web	172.17.0.218	dynamic	408	440	0	80	37%	0	0	
172.17.0.219.com	ACF	Lower	172.17.0.219	dynamic	2060	1180	1622	322	73%	1622	1572	
172.17.0.220.com	ACF	Lower	172.17.0.220	dynamic	2060	1180	1622	428	73%	1622	1572	
172.17.0.221.com	ACF	Lower	172.17.0.221	dynamic	2070	1182	1622	428	73%	1622	1628	
172.17.0.222.com	ACF	Lower	172.17.0.222	dynamic	2040	1184	1622	368	73%	1622	1528	

概括了每条隧道的配置信息，包括隧道名、功能（压缩、打包、加速）、隧道伙伴的IP地址、隧道是动态还是静态。另外，还显示了每条隧道的下列统计数据：Inbound和Outbound的速度；已解压数据的Inbound速度；已压缩数据的Outbound速度；压缩节省的带宽百分比；已加速数据的Inbound和Outbound速度。如果有隧道出现问题，那么此隧道名旁就会出现一个告警符号。除了进行隧道监控外，您还可以：

- ◇ 对隧道设置进行全局配置（如启动压缩和防火墙支持）；
- ◇ 定义Xpress IP地址（如果您想要在压缩隧道中使用内嵌装置或LEM装置，就必须为每个装置分配一个唯一的IP地址）；
- ◇ 删除隧道；
- ◇ 创建静态隧道，并定制设置。

小结

Packeteer的广域网应用优化解决方案可使企业中部署的所有重要应用都获得最佳的性能，同时，最大限度地减轻娱乐性流量和恶意性流量的影响。监控、整形、压缩和加速----广域网应用优化的四座基石----可以让企业：

- ◇ 确保网络资源满足业务目标；
- ◇ 从已有的广域网、因特网和应用投资中获取最大的性能和价值；
- ◇ 识别网络上的应用，分析他们的带宽需求和历史性能；
- ◇ 加快关键应用性能的速度；
- ◇ 限制娱乐性流量，保护网络不被攻击；

◇ 通过压缩，增加带宽容量达10倍，并且可把这些增加的带宽直接分配给关键应用。
今天的企业要求网络及应用具有良好的性能、风险预知性及连续性，而这恰恰是 PacketShaper可以提供的。

更多信息

如果您想要获得更多关于Packeteer产品的信息，请登陆网址：www.packeteer.com.cn

或拨打电话：

408-873-4400（美国）

800-697-2253（全球）

010-65391051（中国）