应用监控
网络监控
容量规划
问题预防
故障排除
服务水平管理
故障重现
偶发故障诊断和早期排除

NETSCOUT®

统一的网络和应用性能管理解决方案

NetScout Systems, Inc. 在全球网络性能管理解决方案的市场上居于领先地位。NetScout 通过其 CDM™ 技术广泛支持各种数据源，包括探针、MIB/MIBII、Flow 等。建立 CDM 技术之上的 *nGenius*® 网络性能管理系统让用户在单一平台上实现应用监控、网络监控、容量规划、问题预防、故障排除、以及服务水平管理等一系列工作。*nGenius* 解决方案使用户能最大程度地提高网络的性能以保障关键业务系统的高效运行并因而提高企业的整体竞争力。

NetScout 美国总部

NetScout Systems, Inc.
310 Littleton Road
Westford, MA 01886-4105
电话： 978-614-4000
传真： 978-614-4004

NetScout 北京办事处

北京市朝阳区建国路 118 号
招商局大厦 18 楼
邮编：100022
电话：010-5923-3880
传真：010-6566-2632

NetScout 广州办事处

广州市天河区体育东路 118 号财富广场西塔 15 楼 125 室
邮编：510620
电话：020 3886 0668 分机 1253
传真：020 3886 0638

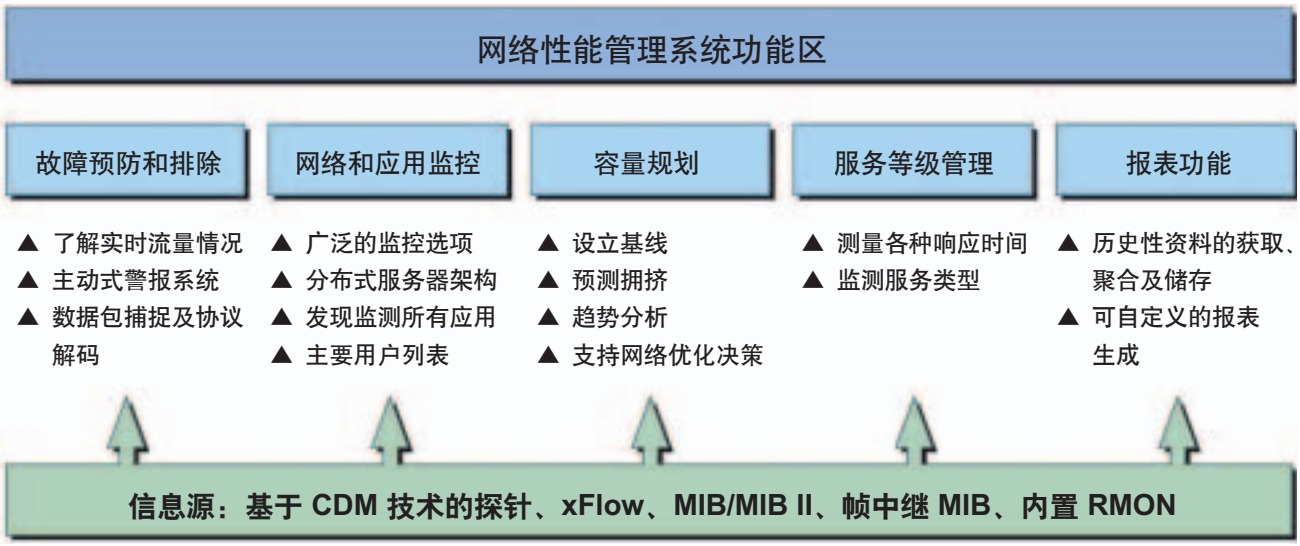
网址： www.netscout.com www.netscout.cn

您有这些网络管理方面的需求吗?

- ▲ 用户投诉网络慢甚至是无法连接
- ▲ 遭遇由于病毒或黑客引起的流量暴涨而导致网络严重拥塞
- ▲ 宝贵的广域网或 Internet 带宽被个别用户或应用占用
- ▲ 需要了解谁是主要用户、他们在干什么以便制定有效的流量管理策略
- ▲ 对于日趋重要的多媒体应用，如 VoIP、视频会议等进行有效的监控和管理以确保服务水平
- ▲ 网络需要优化，但是需要提出具体的统计数据来支持有关决策
- ▲ 每个月都需要花费大量的人力制作各种报表以反映网络使用情况，而且报表中往往缺乏关键数据,如：IP 地址、应用层响应时间及协议种类等

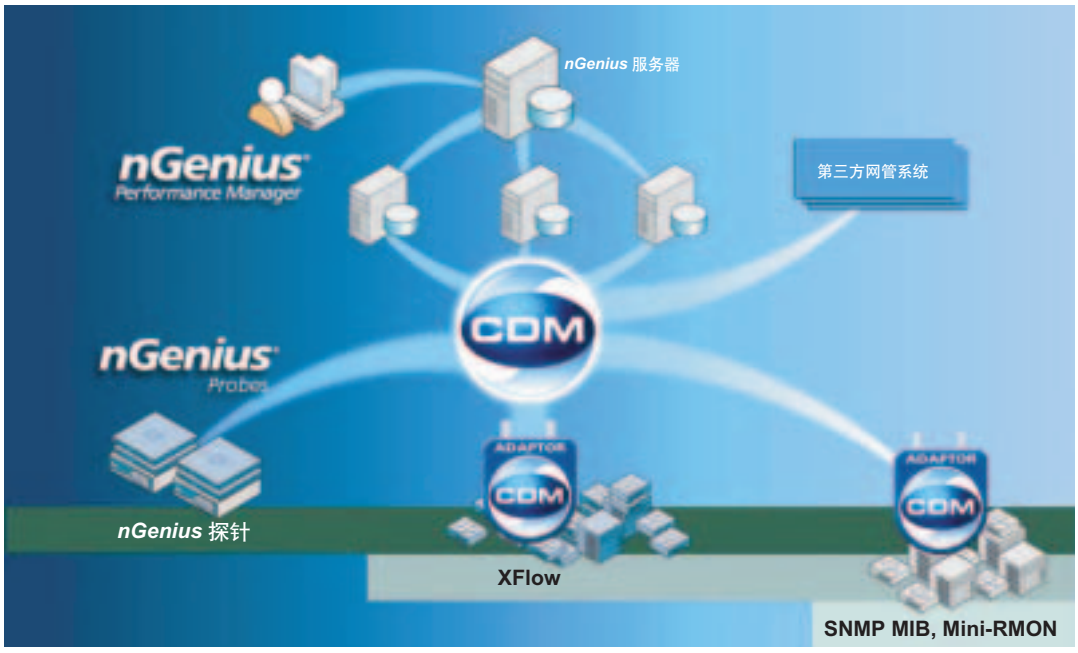
这些需求都可以通过 NetScout 的 *nGenius* 网络性能管理系统得到满足!

网络性能管理系统功能结构图



nGenius 性能管理体系结构

nGenius 性能管理解决方案将主要的性能管理工作如应用和网络监测、容量管理、故障排除、问题预防和服务水平管理都整合在一个单一的系统之内，使得 IT 部门能够提供更优化的网络性能。



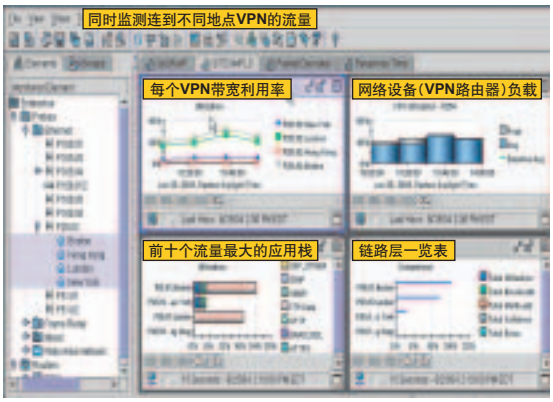
NetScout 建立在其独有的 CDM 架构之上的 *nGenius* 性能管理系统由 *nGenius* 探针、*n*Genius Application Fabric Monitor (AFMon)、*n*Genius Flow Collector 和 *nGenius* Performance Manager 软件等组成。

nGenius® Performance Manager: *减少管理工具混乱，降低整体拥有成本*

随着网络复杂性不断增加，管理工具也变得日趋复杂。每种工具只能应付网管工作的某一部分，不是一个全面的解决方案。*nGenius* Performance Manger 克服当今网络的复杂性，在一个单一的管理应用系统中同时处理多种不同的技术问题。功能强大而又机动灵活的

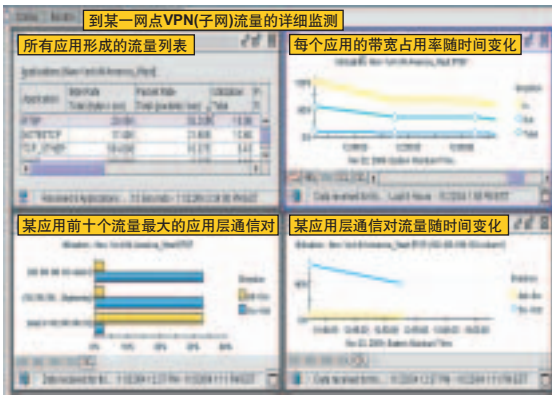
获取与业务相关的信息：

显示企业网络所采用的各种应用和技术的相互关系，是用户充分了解关键的联网商务程序的运作情况。这个统一的方法使用户能将网络作为一个整体来管理，而不是松散地凑合在一起的套件或点解决方案。Performance Manager 使 IT 工作人员能按需定制图像和报表来支持他们各自的工作，帮助他们作出行之有效的决定、迅速解决问题。



统一性能管理：

Performance Manager 将有效的性能管理所要求的主要功能都统一在一个单一的产品里，极大地简化了网络管理的环境。无论是什么任务、应用类型、技术、数据源、指标或时间期限，Performance Manager 都能为用户提供前后一致的图像和导航。所有功能都天衣无缝地整合在一起，为用户更高效率地管理商务服务提供方便。



管理成本，保护投资：

Performance Manager 使用户能有效地管理和优化网络服务。将各种不同的性能管理工具统一成一个单一的产品不仅使用户更好地管理对基础设施的投资，最大限度地减少产品培训和维护的开销，而且还使 IT 工作人员更有效率。另外，Performance Manager 还通过充分利用已经存在于用户网络中的数据源来保存用户现有网络的投资。

nGenius® 硬件探针: *增加对全企业网络的可视性和控制*

NetScout *nGenius* 探针是专用、被动侦听、非侵入式的全网性能探测设备，为整个企业网络提供全面的可视性，从而增强对网络的控制，优化网络性能。

捕捉丰富与商务相关的信息：

nGenius 探针是市面上最全面的数据源，可以用来监控各类应用的运行情况。*nGenius* 探针可以追踪、分析和显示满足各种管理任务所需要的细节，实现从数据包捕捉到测量应用层响应时间等各项功能。

适应网络和应用的复杂性：

以 CDM 技术作为基础，*nGenius* 探针从各种拓扑、虚拟线路、应用和协议采集流量的信息并将其转换成一个共同的格式。通过采集从数据链到应用层的关键统计数据，*nGenius* 探针帮助用户了解聚合应用系统的性能。另外，*nGenius* 探针还通过响应时间的指标综合在一起来保证所有联网的应用能及时得以传输。

有效的监控：

nGenius探针有多种用途，多种选择，可为用户提高效率，节约成本。NetScout 提供单端口探针、多端口以及适用于不同网络链路的探针(如 10M/100M/1G/10G 以太网, ATM, POS 等)。*nGenius* 探针还支持 *nGenius* Flow Director。该可选功能将探针采集自不同网络的原始数据包转发到基于网络的入侵检测系统。

nGenius Application Fabric Monitor (应用结构监控器)

革命性的集实时网络流量监控，故障重现，诊断和排除于一体的解决方案

传统故障诊断解决手段所面临的问题

传统的应用监控虽然可以提供优质的网络、应用、响应时间和趋势的分析，但缺乏数据包层的细节来准确地发现和排除大型网络上运行的复杂应用的性能问题。另外，常见的网络故障诊断解决手段一般采用协议分析仪 (protocol analyzer); 这是一个完全被动式的解决方法。网络管理员用这种方法来捕获网络流量并进行分析以找出问题发生的原因是非常困难的，这主要是因为网络故障具有间歇性和不确定性，当协议分析仪接入到网络中时，网络故障通常已经消失；即使故障仍在持续，但导致故障的原因已失去踪影了。

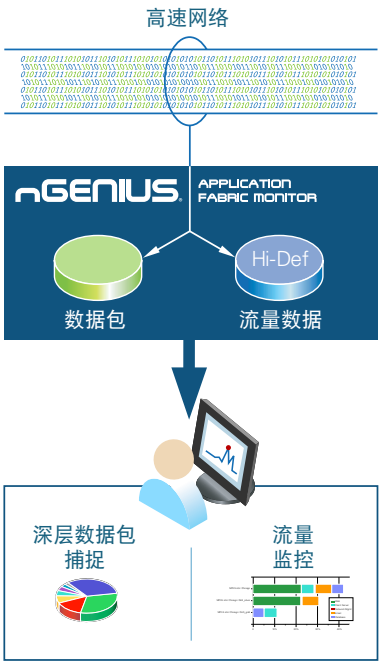
NetScout 解决方案

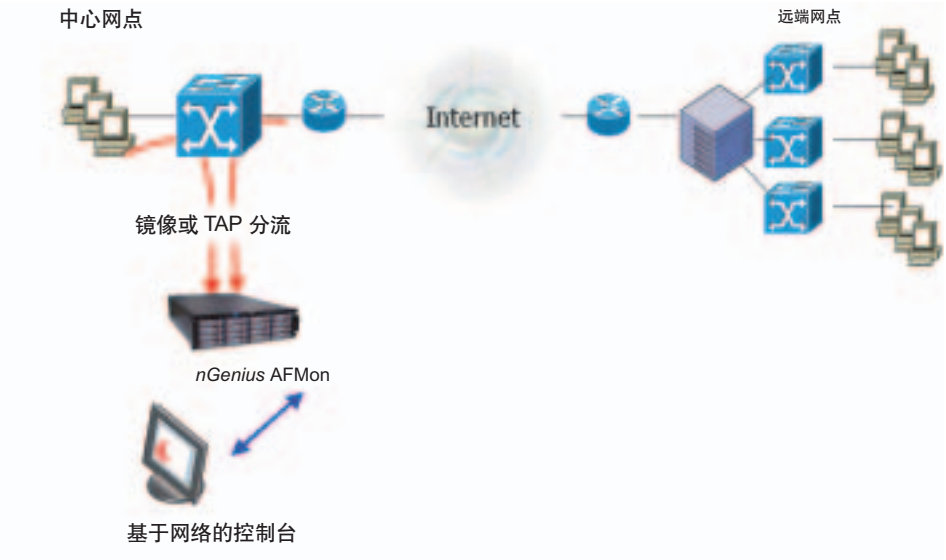
nGenius Application Fabric Monitor (应用结构监控器) 有效地解决了上述所提到的问题。*nGenius* Application Fabric Monitor 是一个高性能的设备。它将网络流量监控和对网络流量进行连续的捕获、存储，重现和分析的功能结合在一起，从而及时发现和排除网络故障。这个革命性的流量监控和网络故障诊断排除解决方案集成了实时和历史流量和应用分析功能、深入细致的数据存储与挖掘、基于规则的异常流量自动检测，应用会话回放和丰富的报表功能，具有极高的性能价格比。IT 工作人员现在可以使用 *nGenius* Application Fabric Monitor在流数据和包数据之间往返（从一分钟到次秒级），同时对基础设施进行监控和对网络故障发生前存储的网络流量进行分析，追踪问题发生的原因。*nGenius* Application Fabric Monitor 及时有效地分析诊断并排除各种间歇性的网络故障可以大大减少网络宕机时间。

nGenius Application Fabric Monitor 可与交换机的镜像端口相连接或直接通过 TAP 设备监听网络流量。

nGenius Application Fabric Monitor 提供四到八个 10/100/1000BaseTX 端口。储存量有 2、5 和 8 太比特 (Terabyte)。

nGenius Application Fabric Monitor (AFMon) 部署方法

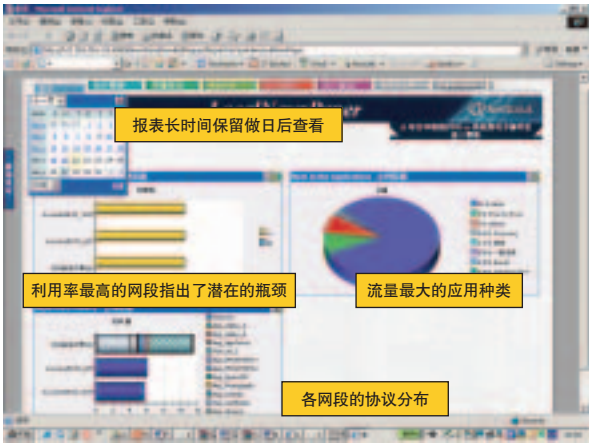




基于 *nGenius* 解决方案的全面可视性

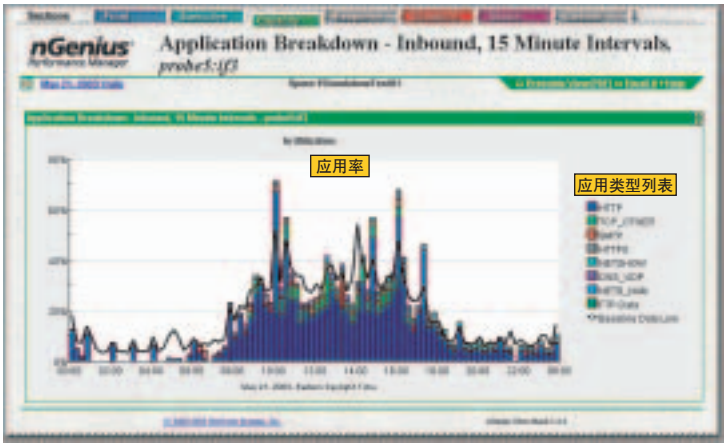
从全网总结深入到个别网段的详细统计，展示和分析。具有对于任意协议，任意应用，任意通信对，任意主机相关的流量的深入可视性。

全面总结



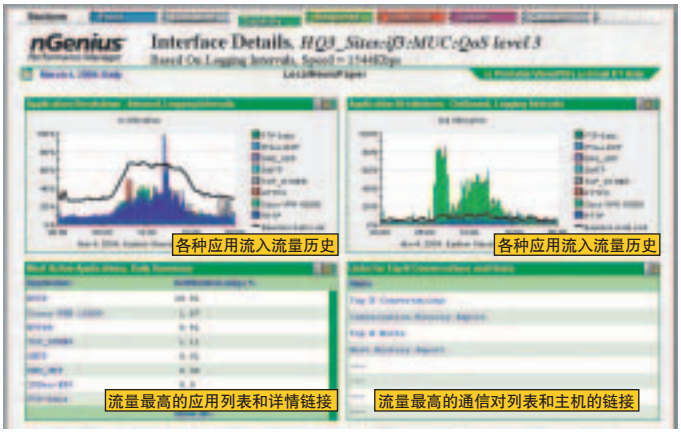
某个网段的详细信息

（进一步了解哪些用户和应用造成了这些流量）

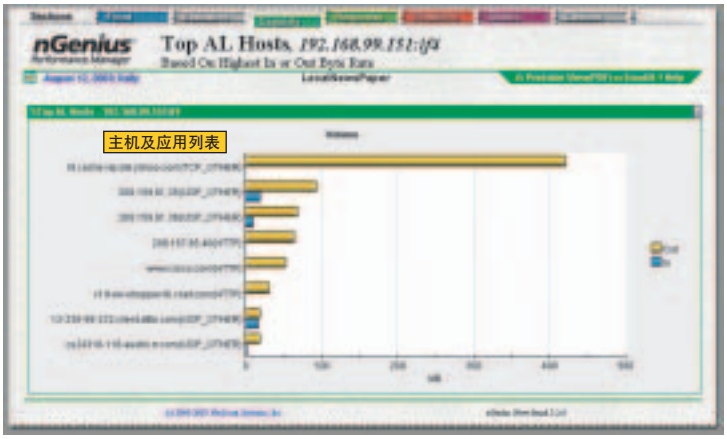


某个网段的全面信息

（进一步了解哪些用户和应用造成了这些流量）

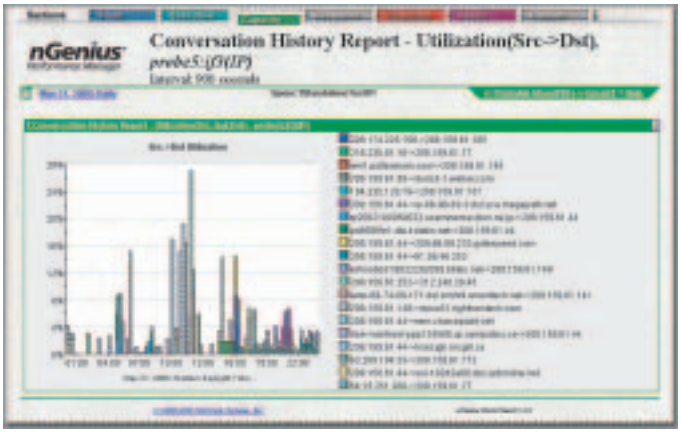


再进一步观察详情：流量最高的主机及应用



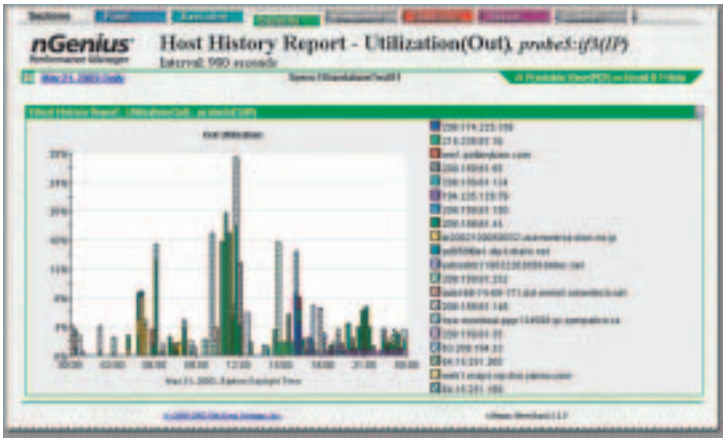
全面的可视性

（流量较大的应用会话列表和随时间变化的流量详情）



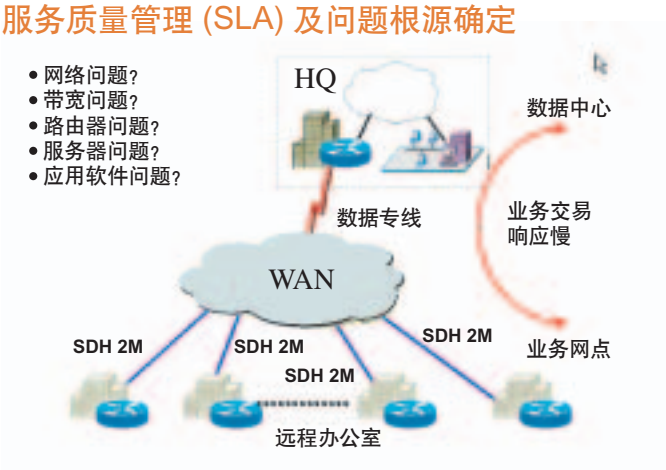
全面的可视性

（流量较大的主机列表和随时间变化的流量详情）

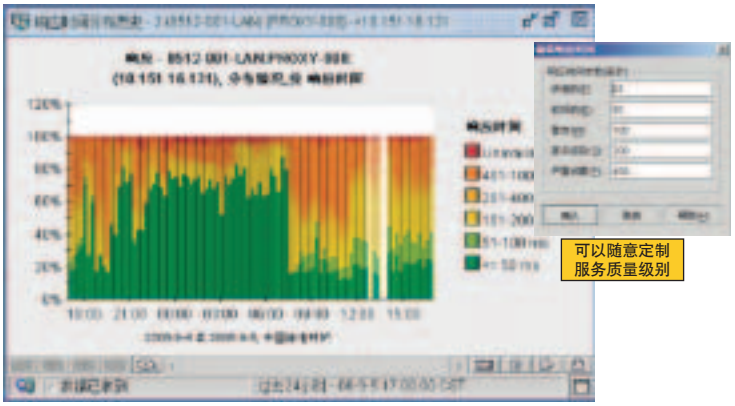


服务质量，应用响应时间的管理及问题根源的确定

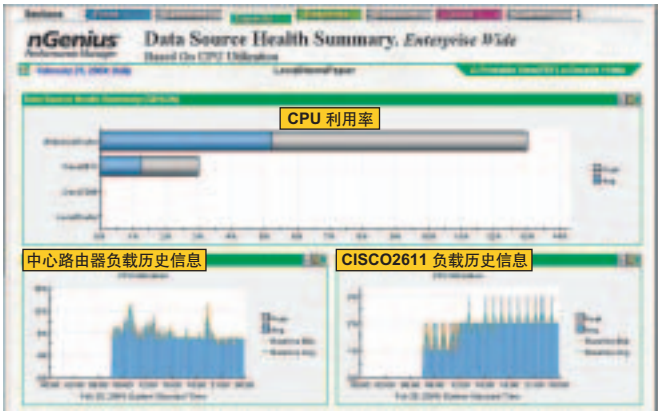
服务质量管理 (SLA) 及问题根源确定



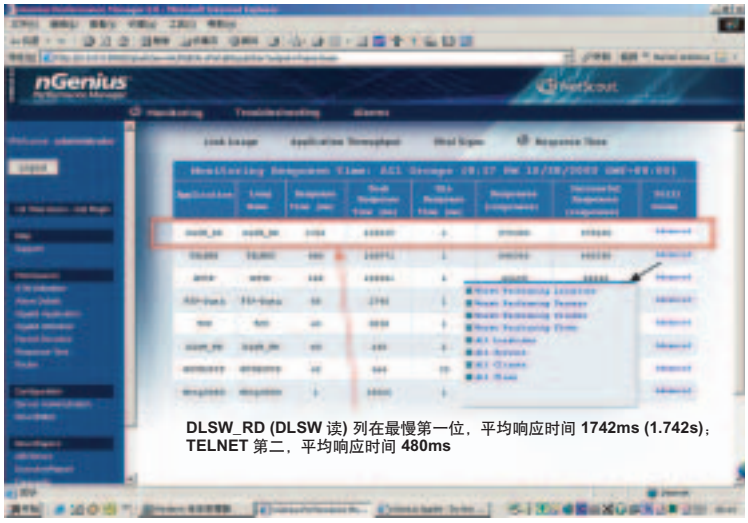
DLSW_RD 响应时间随时间变化分析图



全网数据源健康状态总结

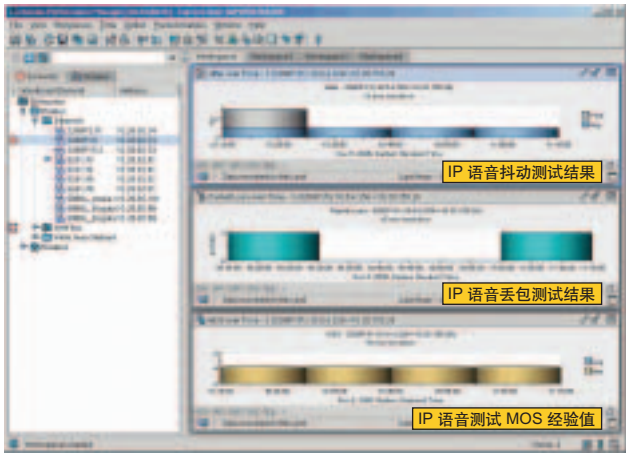


最慢响应时间列表



用户经验质量 (QoE): TCP/HTTP 错误

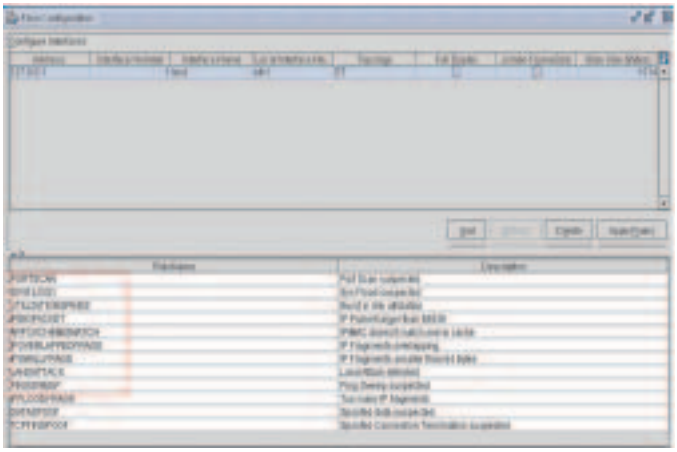
IP SLA 语音电话测试结果



异常流量，网络攻击的侦测及源头确认

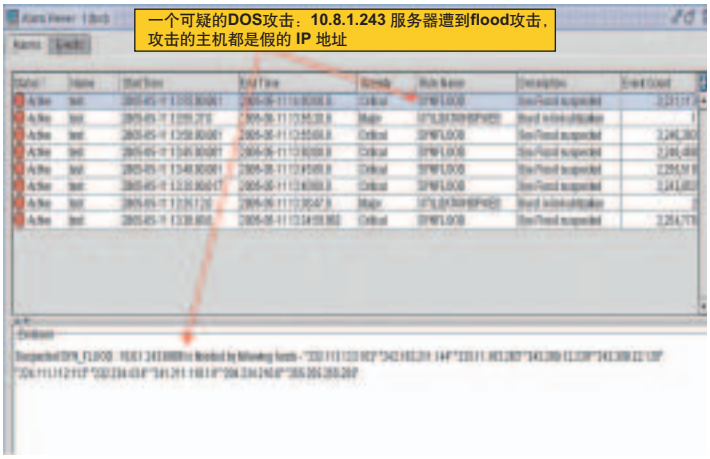
侦测异常流量实例 1 (基于规则)：

检测 **DOS** 攻击：利用系统内置或用户自定义的规则来实时监测流量



侦测异常流量实例 1 (基于规则)：

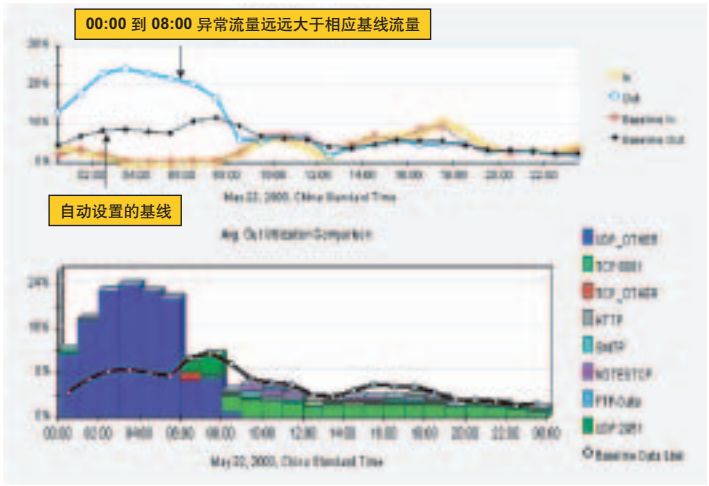
检测 **DOS** 攻击：探测到符合规则的流量，发出告警，包含有证据信息



侦测异常流量实例 1 (基于规则)：

检测 **DOS** 攻击：存储的流数据用于细节行为分析

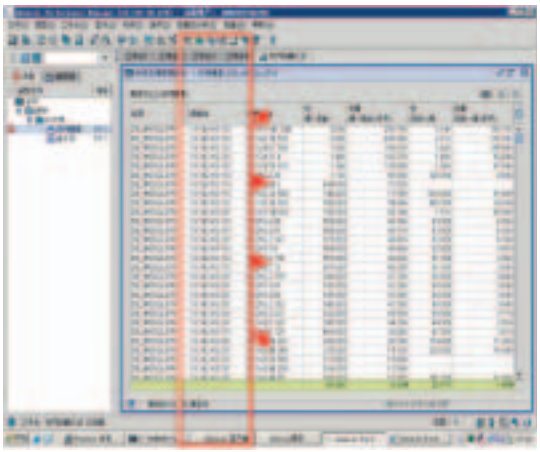
侦测异常流量实例 2 (基于行为)：



进一步看到 **00:00** 到 **08:00** 间，**UDP_OTHER** 协议流量导致了异常流量

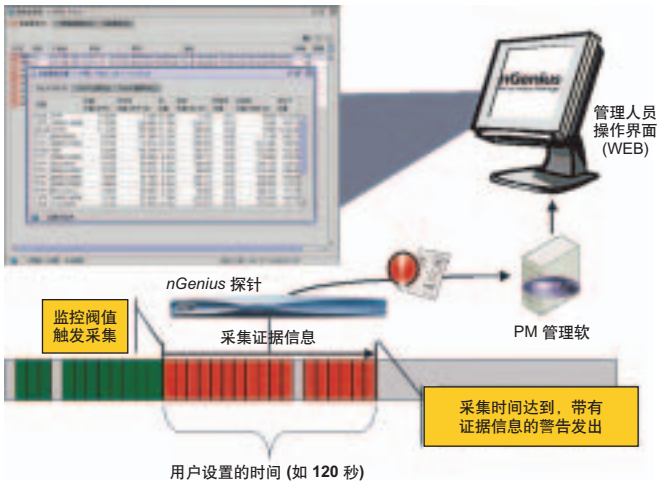
侦测异常流量实例 2 (基于行为)：

进一步看这些 **UDP_OTHER** 流量中的应用层通信对，发再大量从单一源地址发出的 **UDP1434** 数据包。随后，可以启动数据包捕获，从而得到数据联络层的信息，如 **(MAC** 地址，**VLAN ID,PVC** 号等)，准确找到攻击源头。

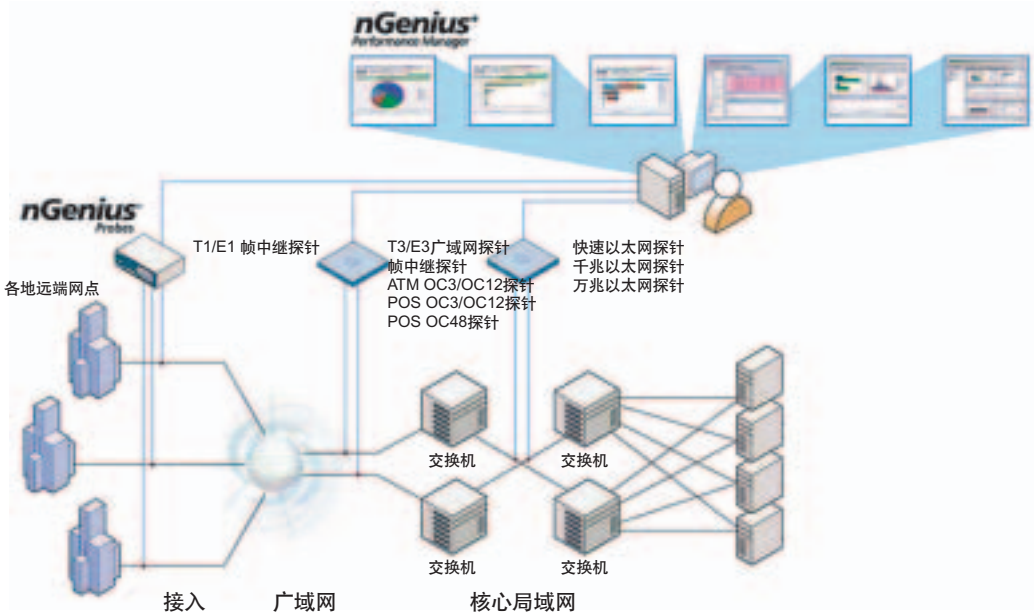


NetScout 的 **Power Alarms** 系统

- 选择用户设置阀值和自动报警
- 选择相对于智能基线的比例阀值设置和报警
- 在发出报警的同时提供相关细节采集证据信息，有助于快速故障排除



nGenius 硬件探针: 对网络的骨干层、分布层、接入层和存储区域网提供全面的网络可视性

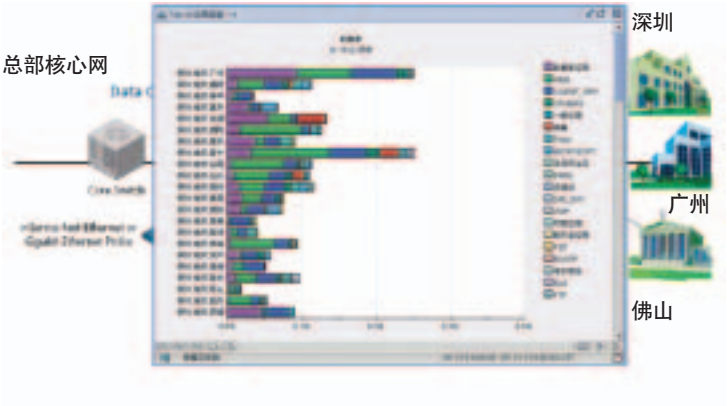


探针部署：可以无处不在

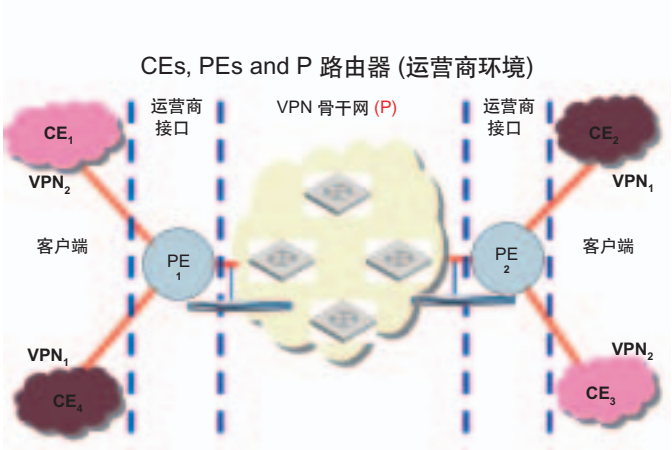
关键应用和网络性能管理解决方案

容量规划及流量趋势预测

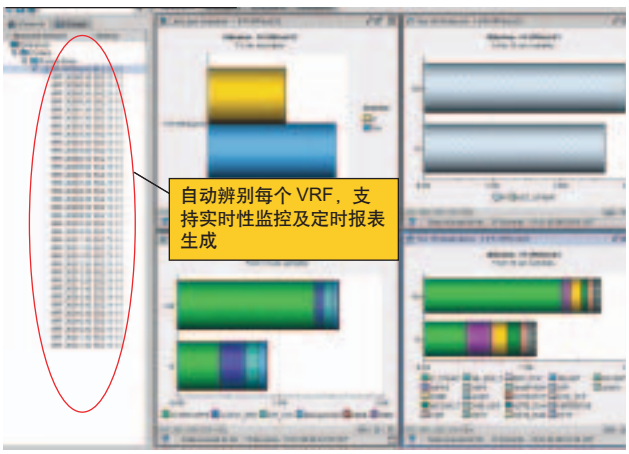
监控远程各地的流量



MPLS 监控



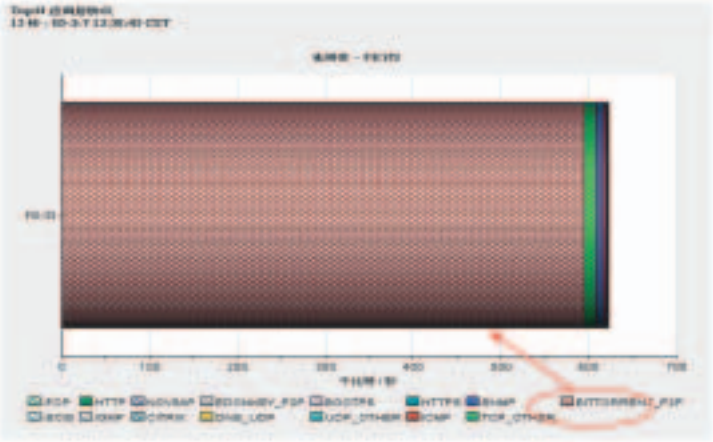
MPLS/VPN 监控



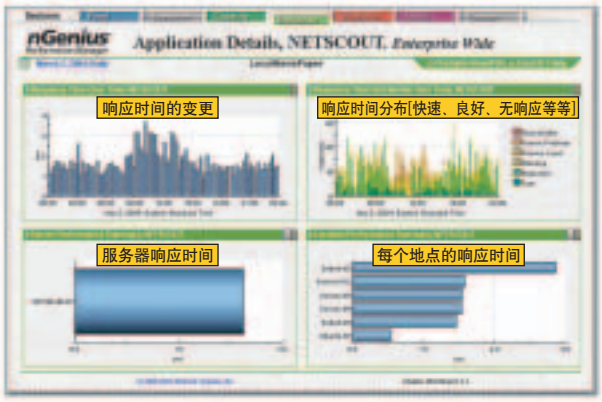
关键应用和网络性能管理解决方案

监测“P2P”应用流量

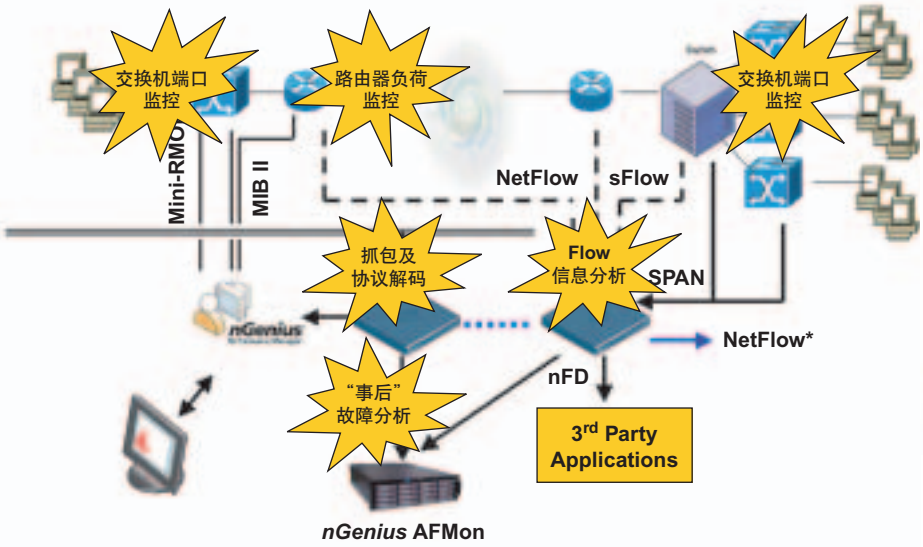
流量最高的 N 个应用，可以看出 P2P 应用“BT”导致了绝大部分流量，利用探针可以监测各种不同类型的 P2P 流量。



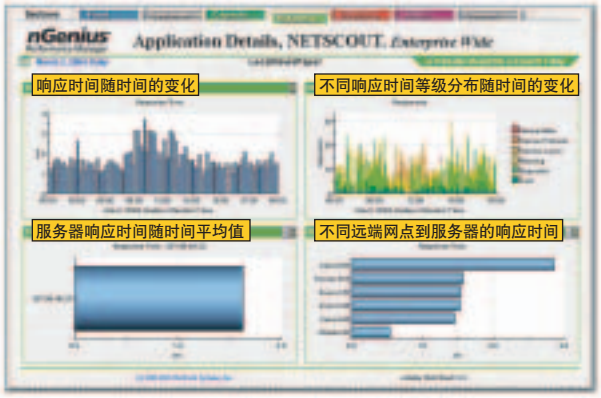
应用的 Qos 和服务质量 (SLA) 管理



故障排除 (利用 CDM 专利技术/网络的全面可视性)

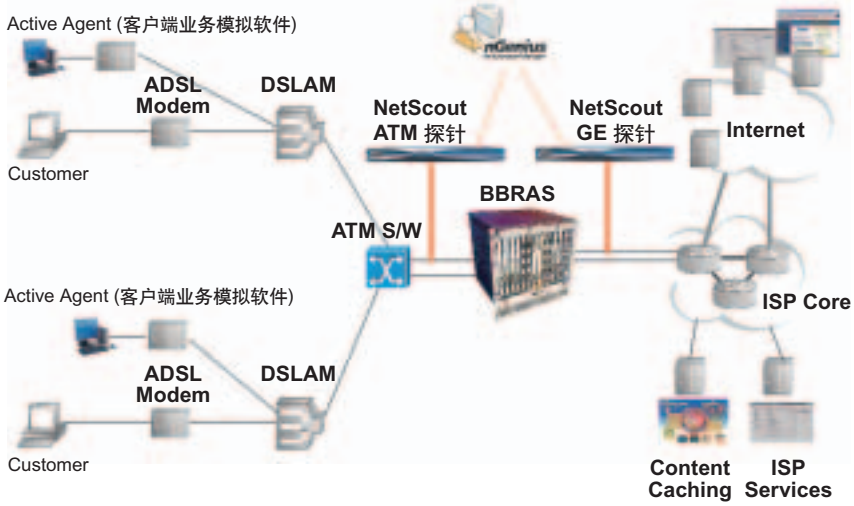


应用响应时间中央监测



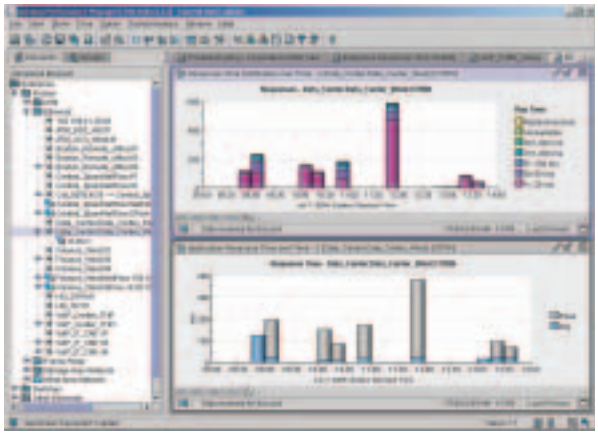
PPPoE 监控与分析

可以监视和分析每一个用户的各种应用流量和行为



应用 (Citrix) 性能监测

监测某一应用 (如 Citrix) 的响应时间和服务质量

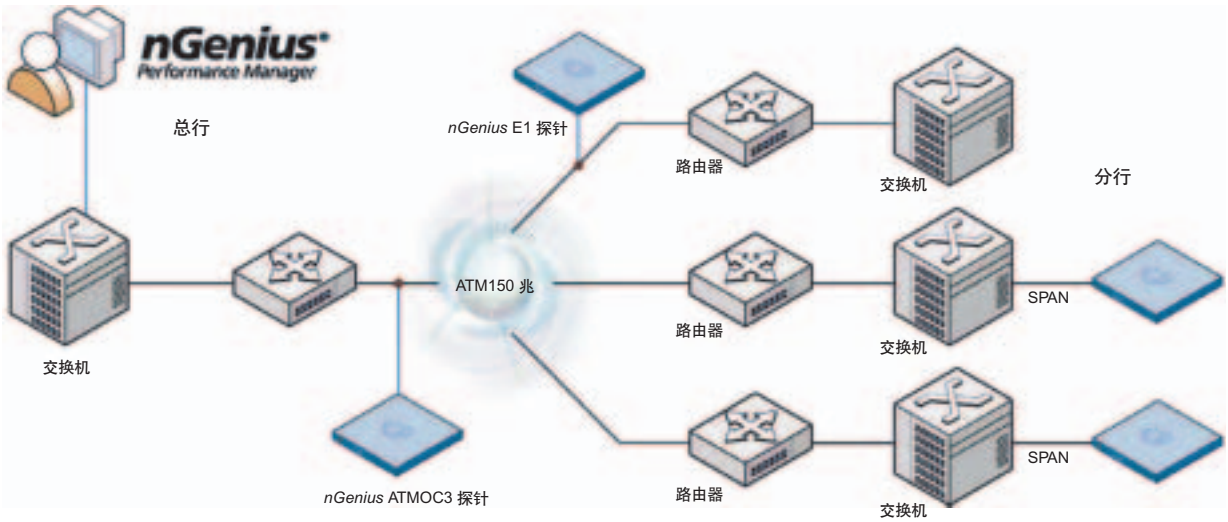


NetScout 产品应用案例

金融银行

目前国内银行在业务数据管理，皆采取集中式的管理政策。所有关于业务的应用系统都必须透过网络与总行的数据中心进行处理。如何确保网路的正常运行，通过远程监控、集中管理全国的网络，优化其分布广泛的广域网性能，为关键的银行应用系统提供全网络范围的可视性和控制，提高 IT 人员的工作效率，成为目前最重要的课题。

NetScout 的 *nGenius*® 解决方案在任何时间、任何地点都可以通过 Web 灵活安全地获得关键的网络性能信息。可以通过远程存取的方法获取实时的网络应用层流量信息，实时监控异常流量、故障检修，其历史报表可作为扩容政策及网优的依据。增加现有工作人员的效率，减少在各地分行所需新增的资源。



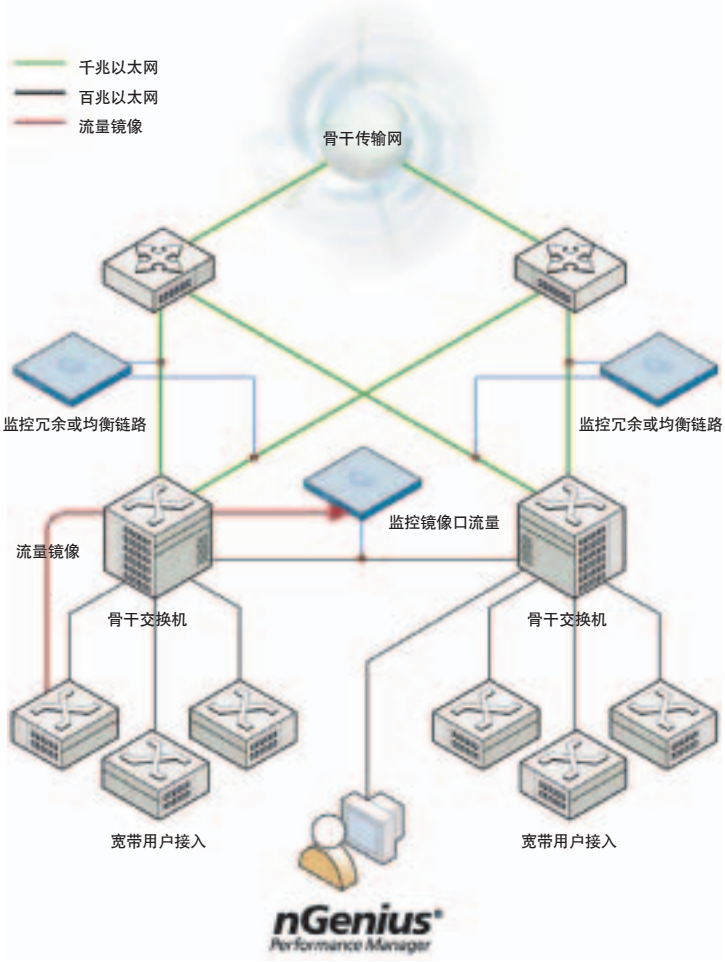
通过选用 NetScout 的 *nGenius* 性能管理系统：

- 拥有了可以通过远程存取的方法获取实时信息的中央化的性能管理解决方案
- 获得了对网络流量(包括联网的应用系统)的可视性和控制
- 能够充分利用数目有限的网管员来预防性地管理网络性能
- 24 小时不停监视网络异常，并发出实时告警
- 可以迅速解决网络性能问题
- 为各类读者提供内容丰富、可自定义、每天自动生成的各类报表
- 保证了新的应用系统、服务项目的启动和系统升级顺利进行
- 部署在总行广域网的 ATM155 兆探针，可监控每一个 PVC 上的流量,应用，进行网优和排障
- 部署在分行广域网的 2 兆探针，可监控分行连接到总行或区域中心带宽利用率和所有应用的双向会话
- 部署在分行交换器的局域网探针，可利用镜像 (SPAN) 方式将重要端口的流量镜像到探针，进行网络监测和故障排除

电信行业

随着宽带用户数量的快速增长，运营商的数据业务部门无论在网络优化还是在日常运行维护方面都面临着巨大的挑战：一方面要制定出既符合经济效益又能够满足实际需要的网络扩容和优化方案；另一方面要努力提高服务质量，具体表现在提供畅通的网络连接、最大程度地降低网络宕机时间。NetScout *nGenius* 性能管理系统完善的数据采集、自动化的报表生成、实时流量监控及故障排除等功能使它成为数据业务部门的网管利器。

在一个实际实施的案例当中，数据网络管理人员通过 *nGenius* 清楚了解整个网络的运行情况，实时察觉异常现象并加以排除，起到防微杜渐的效果。而详细的、个性化的报表准确预测网络瓶颈，为网络优化的决策提供坚实依据。

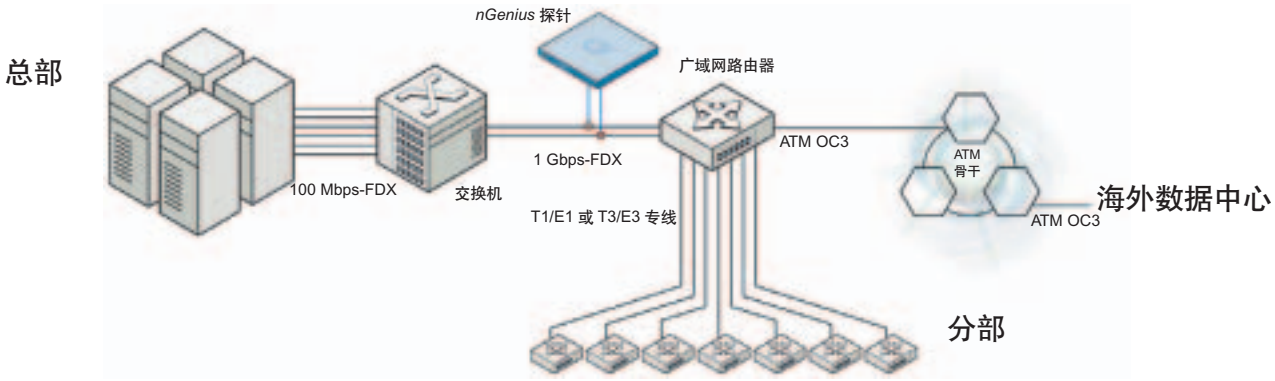


NetScout *nGenius* 性能管理系统给电信行业带来的效益包括：

- 使用探针监控关键网段，信息涵盖 OSI 七层
- 通过交换机内置 RMON 功能实现网络整体监控
- 拥有了可以通过远程存取的方法获取实时信息的中央化的性能管理解决方案
- 能够充分利用数目有限的网管员来预防性地管理网络性能
- 可以迅速发现和解决网络性能问题
- 利用收集得到的大量数据，及开放式的 SQL 数据库，自定义电信级报告
- 对于与电信业务有冲突的应用，马上收集证据
- 成为电信对客户的增值服务

企业用户

在全球化的趋势下，企业间的竞怎争越来越激烈。无论在欧美或中国大型企业均已导入 ERP 系统以降低营运成本，如何确保 ERP 系统在其遍布全球的网络中正常运行，实时监控 ERP 应用系统的响应时间，当 ERP 应用系统的响应时间产生延迟时，立即产生报警并分析其原因，迅速解决问题，成为致胜的关键。同时监控广域网带宽利用率进行趋势分析,作为网优及扩容计划的依据。



通过选用 NetScout *nGenius* 性能管理系统给企业用户带来的效益包括：

- 拥有了可以通过远程存取的方法获取实时信息的中央化的性能管理解决方案
- 获得了对总部千兆以太骨干网的可视性
- 在 ERP 应用系统响应时间缓慢时能迅速判断是服务器，网络设备，还是主要数据中心和各分部的链接有问题并及时进行故障排除
- 数目有限的网管员能够预防性地管理整个网络的性能
- 可以迅速发现和解决网络性能问题

NetScout *nGenius*: 完整的网络性能管理解决方案

▲ 广泛数据源支持：通过 **CDM** 技术支持探针、**MIB/MIBII**、**Flow**、**Mini RMON** 及仿真软件等
▲ 高度的可扩充性：管理分布式的企业网络
▲ 自动化：分析、展示和分发性能信息来简化管理
▲ 促进企业内部的信息交流：增进 **IT** 工作人员之间的合作
▲ 一体化性能管理: 结合实时性监控分析、自动化历史报表生成
▲ 应用层可视性: 提供量化信息支持有关 **IT** 资源运用策略的制定
▲ 预防性: 让网管员赢取时间防微杜渐
▲ 从上至下式网络监控模式: 从概括性全网监控到个别网段的深入分析
▲ 个性化: 制定个性化的报表格式
▲ 高性价比: 一个系统、多种功能

产品系列

NetScout 网络性能管理软件: ***nGenius* Performance Manager**
NetScout *nGenius* 硬件探针

广域网

T1/E1	单端口、双端口、四端口和八端口广域网探针。可选购 1G 内存和/或 *nGenius* FlowDirector。
T3/E3	单端口、双端口广域网探针。支持透明通道，FRAME RELAY，ATM，可选购 1G 内存和/或 *nGenius* FlowDirector。
Packet-over-SONET(POS)	单端口、双端口 OC3，OC12POS 广域网探针，单端口 OC48 探针。
ATM OC3/OC12	单端口、双端口ATM广域网探针。可选购 1G 内存。

局域网

以太网/快速以太网	单端口双端口、四端口、八端口以太网/快速以太网探针。可选购1G内存。
千兆以太网	双端口、四端口、八端口探针。可选购1G内存。
千兆以太网聚集	支持四个或八个千兆以太网链接。可选购1G内存
万兆以太网	双端口探针

nGenius AFMon (应用结构监控器) 提供四到八个 10/100/1000M 以太网端口, 多达 8T 的硬盘存储

中国用户列表：

金融，证券，保险：	**电讯业，服务提供商：**	**企业：**	**政府，教育，研究单位：**
中国银行 中国建设银行 中国农业开发银行 民生银行 福建兴业银行 中国人寿 上海期货交易所 花旗银行上海分行	甘肃电信 上海电信长途局 浙江移动 江苏移动 上海联通 深圳电信 广州电信数据局 北京首信集团	克拉玛依油田(新疆油田) 兰州石化 仪征石化 GM 中国公司 索尼中国公司 Juniper 网络公司中国公司 CA 中国公司 中国远洋运输总公司 江森自控公司 阿里巴巴公司 罗氏(Roche)产品责任有限公司 NV 科技公司 Budweiser 有限公司 Veritas 中国公司 Eli Lily 中国公司 Seagate 中国公司	公安部 国家发展改革委员会 国家安全信息中心 615 研究所 浙江传媒大学 上海浦东教育局 深圳公安局