电力行业信息化网络流量精细管理
解决方案

一、 综 述

1.1 行业背景

随着电力行业信息化程度的不断提高，电力企业的商业运作，诸如：采购、生产、销售等越来越多地以电子商务的形式得以实现；以提高企业内部管理效率、降低成本的 ERP 系统与 EAM 系统，支持客户信息管理与分析的 CRM 系统，全面提高价值链竞争效率的 SCM 系统等的实现同样基于内联网甚至互联网。网络系统将承载语音、视频、数据各大类多种业务，满足企业公文流转、集团视频会议、基建和生产现场实时监控、生产、计划、财务、人事、档案数据的传输和展现等多种业务。这使得信息化网络的规模越来越大，网络应用也越来越广泛，对网络带宽资源、业务流量、用户访问量等方面都缺乏可见性和可控性。为了更好地了解掌握网络使用情况，管理网络运行状态，提高公司信息化网络的业务管理效率，优化信息化网络的业务服务质量，降低运营成本，需要对信息网络从“流量”这个根本因素出发,进行精细化的监控管理。为整个网络的高效运行维护提供一个高可用性的管理平台，加强信息网络的业务优势，提高全员工使用的满意度，因此需要加强“信息化网络流量精细化监控管理系统”的建设。

对于电力行业来说，如何给自己的信息应用系统提供一个安全的平台，如何充分利用网络资源优化业务流程，节约成本、提高效益，这些都是网络管理建设需要考虑的问题。

主要存在着如下主要问题：

- ◆ 网络资源利用率的问题
  - ●缺乏对全网流量的整体把握
  - ●无法实现对网络流量的精细化分析
- ◆ 资源优化的问题
  - ●如何为优化网络结构、降低网络运行成本提供依据？
  - ●如何更好地利用现有网络资源，提供更优质的服务？
  - ●如何为网络投资升级提供准确的数据依据？
- ◆ 有效监测异常流量的问题
  - ●如何及时发现、诊断和解决网络故障

- 如何预警将要发生的网络拥塞？
- 如何预防异常流量？

◆ 应用管理存在的问题

- 如何保障关键的业务系统应用？如视频、ERP、SG186系统等。
- 业务应用的健康状况和用户满意度如何？
- 如何管理网络的业务服务质量？
- 等等…

1.2 项目意义

有效保护电力信息网络的数据安全、电力调度和办公平台的稳定运行，保证高效的业务运作，保障网络的畅通，从而进一步满足电力服务于民众的社会功能，这不仅是非常必要的，而且具有重要的社会意义。

网络流量管理的完善与否，直接影响网络的顺畅性，更直接影响到企业运作的速度与效率，体认到网络流量管理的重要性，通过网络流量管理的技术，采用先进的系统工具做分析，由宏观面自上而下，掌握网络流量的大方向、由微观面自下而上，追查流量异常的关键因子，藉由主动/自动执行流量异常的抑制，使网络运作顺畅，智能地控制网络流量，并以支持用户未来提供丰富的差异化服务策略和QoS保证机制为目标，期望通过这种梳理和协调来激发更多更好的网络应用。通过面向网络、面向员工和面向核心业务的网络流量监控管理系统，全面掌握网络带宽资源、关键业务应用流量、员工使用网络等信息，优化网络流量的部署，实现电力信息网络系统的流量工程（QoS）、规范遵从性管理，从而改善整体网络的管理水平，提高网络传输效率和网络安全性，降低总体网络的运行维护成本、提升企业的网络业务服务能力。

因此，建立一个全面的、精细化的网络流量监控管理系统十分重要。一方面需要了解网络带宽的具体应用情况，分析网络流量的流向，网络应用的组成，应用流量趋势分析，历史数据流量的对比分析，以及各个分支机构网络带宽的分布。另一方面需要管理网络中的应用优先级、保障关键业务畅通、带宽分配、网络行为过滤、异常流量防范等等。

二、 网络流量管理的挑战

随着技术的发展，业务应用越来越多的依赖于网络来实现，这样就促使了网络规模的扩大，应用的增加，用户的增加。电力企业网络基础设施为支持不同类型的流量和用户而进行扩展，不断增加的网络基础设施使网络管理也变得越来越复杂，流量管理就变

得举足轻重了。因此，全面掌握网络行为不仅越来越重要，而且也越来越具有挑战性。此外，整个网格的问题，如应用性能、带宽利用、网络拥挤及用户与应用流量的适当优先化，通常仍然没有得到解决。

纵观整个互联网的发展，如今的企业电子邮件、端到端下载、Web 浏览、数据库、视频会议、ERP、CRM、SCM 等各种应用越来越多、越来越复杂，而企业 CIO 和网管人员对这些应用的可监视性、可控性、可预测性却越来越低。企业多通过局域网将语音、视频等对延时、抖动、丢包要求苛刻的通信类型和如 ERP、CRM、数据库、电子邮件等对延时并不敏感，但对丢包敏感的通信类型集成在同一数据网络上传输，而且，网络中还混杂着各种与企业核心业务无关的应用，比如音乐、影视下载、聊天工具、网络游戏、垃圾邮件等等。

这些应用需求的差异性要求企业网络管理员合理调配网络流量资源。而从实现方法上看，最简单的方法就是增加网络带宽，但这带来的结果却是，不管交换机的背板带宽有多高，交换机的数据包转发率有多大，数据传输率有多快，网络拥塞隐患都将永远存在于网络中，并有可能造成瞬间崩溃。

由于应用性能低下和网络资源管理失衡已使许多企业在停机期间遭受数十亿美元损失，而且这一数字在不断上升；网络中断及性能下降给一些企业带来的损失，已达到其年度收入的 1%。

面临复杂的异构 IT 环境，网络规模变得越来越大、越来越复杂。虽然已经采取了一些性能优化措施，但仍然存在着很多问题，如：

- 网络应用种类越来越多、应用越来越复杂,网络速度变得越来越慢，网络可控性越来越差；对系统正常的运营投的人力和财力成本越来越大；
- 网络利用率如何？哪些应用在网络中运行？主要用户有哪些？
- 哪些应用、哪些流量占用带宽资源？如何提供端到端的流量管理？
- 网络中存在一些非关键性应用，占用了大量网络带宽，使网络效率大大下降，关键性应用得不到保障，视频会议、财务、ERP 核心业务受到严重影响；分支机构和节点的广域网互联用户更受到网络带宽不足的严重制约；
- 异常流量及病毒大量存在，网络应用存在潜在的危险；如何提高系统对业务处理的稳定性和安全性？
- 当网络中出现异常流量引发网络故障时，如何快速定位问题源？如何尽可能地缩短网络故障排查时间，减少人力投入？
- 如何管理好网络接入带宽，延缓网络扩容周期？
- 如何实时而长期的监测业务应用的情况，提供详细的网络使用情况报告？

- 如何制定合理的管控策略，保障系统的 QoS，提升服务质量（服务品质）？
- 如何更好地利用现有网络资源，提供更优质的服务？

面对这一系列的问题，必须通过对关键业务和关键用户提供有保障的满意服务（QoS）和服务体验(QoE)，保证用户能够平等的使用网络资源和带宽,保障整个网络的稳定运行的同时实现网络性能和效率的最大化。

单纯增加带宽和提高服务器性能并不能解决网络流量本身问题，反而使隐患长期沉积，伺机爆发。企业 CIO 和网络管理员们以前往往忽视了对网络应用流量进行科学、有效的管理，而把重点放在增加网络带宽、提高服务器性能上。即网络资源与应用性能的一致性、适应性管理问题仍然存在。

另外，企业网络还在不断遭受拒绝服务（DoS）袭击、电子邮件滥传、病毒和蠕虫等网络管理问题的影响。

因此，采用应用流量管理手段及设备科学、高效管理企业网络，将是每一位企业 CIO 未来都需关注的重点。

三、 需求分析

电力（或电网）公司计算机信息网络虽然在 IT 基础设施建设方面已经具备了一个网管中心，负责对全网进行管理。但是在业务精细化监控运维管理方面，目前还存在的主要问题是业务应用的可视性和可控性薄弱。

- **网络透明度降低:**
  - 网络状况日趋复杂，大量新兴应用涌现
  - 缺乏对全网流量的整体把握
  - 无法实现对网络流量的精细化分析
- **大量未知流量挤占网络资源:**
  - P2P 流量吞噬网络带宽
  - 非关键应用无法得到管理
  - 异常流量威胁网络安全
- **网络稳定性、安全性下降:**
  - 网络拥塞时有发生
  - 关键应用无法得到保障
  - 病毒、网络攻击导致网络瘫痪

◆ **对员工的网络行为缺乏有效的监管机制：**

- 上班时间上网聊天、看电影、玩游戏、浏览非法网站，严重影响工作效率；
- 缺乏员工上网行为的记录，无法根据用户上网行为日志进行追溯；
- 即时通讯软件可能会导致保密信息的泄露。

鉴于上述网络现状和问题的分析，为了提高电力公司 IT 网络的管理效率，降低企业的 IT 经营成本，为整个网络的高效维护提供一个高可用性的网络平台，成为公司迅速发展的重要基石。在面对复杂的异构网络环境，需要对网络中各种业务应用所占用的带宽资源有清晰的了解。对当前网络应用情况进行实时、长期的监控，实现网络的透明化管理。通过相应优化策略，对关键性应用给予高带宽、高优先级进行保障，对非关键性应用进行限制，对一些恶意的网络攻击行为进行抵御。优化系统布置以根据业务应用需要对出/入网的流量进行控制，对每种应用占用带宽进行合理分配，从而保障整个网络的稳定运行，缓解网络扩容压力，同时实现网络性能和效率的最大化。从而需要：

- **确保客户关键应用的QoS：**
  - 对客户关键应用，平滑QoS
  - 阻止娱乐性和带宽占用大的应用竞争有限带宽
- **避免网络拥塞**
  - 克服拥塞，队列延时和在应用响应上的低效
  - 减少远程分支机构的时延
- **阻止娱乐和恶意流量**
  - 阻止不受控制的娱乐性和恶意流量

通过对电力公司的网络现状和问题的调研，我们主要总结出以下重点需求：

(1) 应具有高可靠性、高安全性、高效率、易维护、高可扩展性

- 对于流量管理设备而言，首先要避免自身成为用户链路的故障点，因此只有保证高可靠性、高效率、易维护和高扩展性，才能在用户的关键链路中发挥作用。

(2) 提供网络运维新手段—高级网络使用分析

- 流量管理设备必须具备强大的“应用感知”能力，能够基于应用层感知到网络中每种应用类型，利用各种监控手段及时准确地对各种应用，用户，端口，流量。
- 怎样就算具备强大的流量感知能力是个大问题。从目前的技术市场的发展来看，通过硬件平台组成的高性能 Layer2-Layer7 的应用流量分析技术即 DPI

技术。（深度数据包检查）是流行的趋势和方向。这类技术可以实时地通过基于 7 层的数据包检查，同预先识别的代码库相互比对。从而确认流量的特征。这类技术需要几个重要的技术支持。一是不断更新的特征库。人力、物力的投入。二是强大的硬件平台运行。强大的性能保证。

- 能够进行实时的网络中的各种应用进行监控。这在应用感知网络中是个重要的话题。管理者对网络流量的事态感知能力应该是实时、及时的。可以通过这些实时的信息，及时的处理网络突发情况。及时处置、改变策略或者设置更好的策略等。
- 能够对网络中的各种应用进行长期监视和统计报告。

(3) 网络资源控制和流量优化

- 采用什么样的 Qos 或者流量技术对网络资源管理有帮助呢？从目前的情况来看，队列或者经过改良的队列技术即符合标准性，又能够便于网络芯片执行提供强大的性能处理能力。相比较于 TCP 整形技术（滑动窗口）技术来看，具有性能强大、配置方便。不改变 TCP 连接内在固有的性状以及连接特性。对运营网络来说，提供“绿色”的管理技术。
- 能够通过策略实施实现对重要业务（等）的稳定质量,；
- 重点对大量耗费带宽的应用进行一定程度的监测和限速,防止带宽资源的浪费。
- 能够在全局、单个用户或单个流量水平层次上,对网络应用流量进行带宽管理，使 能够对网络资源进行自由的分配，改善用户体验（QoE）。

(4) 分级与访问控制

- 能够对根据业务应用的级别进行差异化服务，制定差异化的带宽策略。
- 能够根据不同的部门或用户，区分服务等级
- 能够根据不同的业务类型，能够按等级区分用户，如提供金、银、铜等级别用户区分，或根据带宽需求大小来分类。提供分级/区分服务、有流量优先级的多类服务、有保证带宽的 SLA，以及基于使用方法的统计。

(5) 服务安全

- 服务的安全，首先是提供设备自身的安全。运行得是否稳定？关键部件有无冗余性？是否提供硬件的旁路单元？设备自身是否收到 DoS 攻击等的影响？

- 设备能够对网络中流行的攻击、病毒等不安全流量进行防御，保证重要服务的安全性。
- 设备是否能够提供告警功能？能否及时、甚至是预先报告设备的流量异常等情况？

四、 建设目标

电力行业 IT 网络流量管理的目标是实现：

- **关键业务保障**
- **差异化 分级管理**
- **应用行为内容控制**
- **流量实时监控**
- **量化、可视、动态**
- **适应性、一致性管理**
- **基于策略的管理**
- **诊断和预警**

➢ 网络应用的一致性
  ✓并发连接数的平滑
  ✓应用流量带宽整形
➢ 网络应用保护
  ✓属性和特征的识别
  ✓基于策略的分类及控制
➢ 网络状态的报告
  ✓ 统计和分析
  ✓ 诊断和预警

针对电力公司具体项目的建设目标是：

1）外网 Internet 访问的流量管理；

- 上网行为管理（即网络行为审计）

对外网 Internet 的访问流量进行策略管理，限制 P2P 下载、网络游戏、聊天等无关的网络应用，减少对办公网的带宽影响；

2）内网广域网的流量管理。

- 根据关键应用合理分配流量带宽，进行资源整合
- 实现层次化分级管理模式，规范网络资源使用
- 监控阻断网络异常流量，加强网络信息安全

对内网广域网的流量进行策略管理，保障视频会议、财务、ERP 等关键业务应用的带宽；

对内网流量进行广域网应用加速，提升应用响应速度，保障其传输质量，减少重传次数，节省网络带宽资源。

从长远来看，基于策略智能化地控制网络流量,并以支持未来网络运维提供丰富的差异化服务策略和 QoS 保证机制为目标，期望通过这种梳理和协调来激发更多更好的网络应用。

五、 解决方案

针对电力公司IT网络的流量管理解决方案，采用东华流量管理平台构架，包括全面的网络流量监测分析（FlowAnalyzer系统）和网络应用流量控制（FlowShaper系统）两部分。

- **流量监控技术：**
  - 自动识别网络上的应用
  - 准确了解带宽利用率
  - 准确了解网络效率
  - 准确了解关键应用响应时间
  - 定位、隔离性能问题
- **监控与分析：**
  - 网络利用率
  - 网络效率
  - 应用响应
  - 问题定位（监控和报警 WAN 问题）

- **流量管理方案目标：**
  - 自动识别应用并分类
  - 监控利用率和网络效率
    - 识别网络问题，包括：娱乐性流量和延时
  - 度量用户体验
    - 监控 SLA
    - 度量应用响应时延
  - 访问性能定位

- **流量管理的价值：**
  - 网络带宽及性能管理由被动管理变成主动管理
  - 应用业务规则匹配到广域网流量
  - 分配带宽
    - 使用具有应用智能的 QoS 到客户关键应用，达到保障单路会话

- 解决任何地点的应用性能问题

• 保护网络，不受 DoS 攻击

- 控制娱乐性或恶意流量

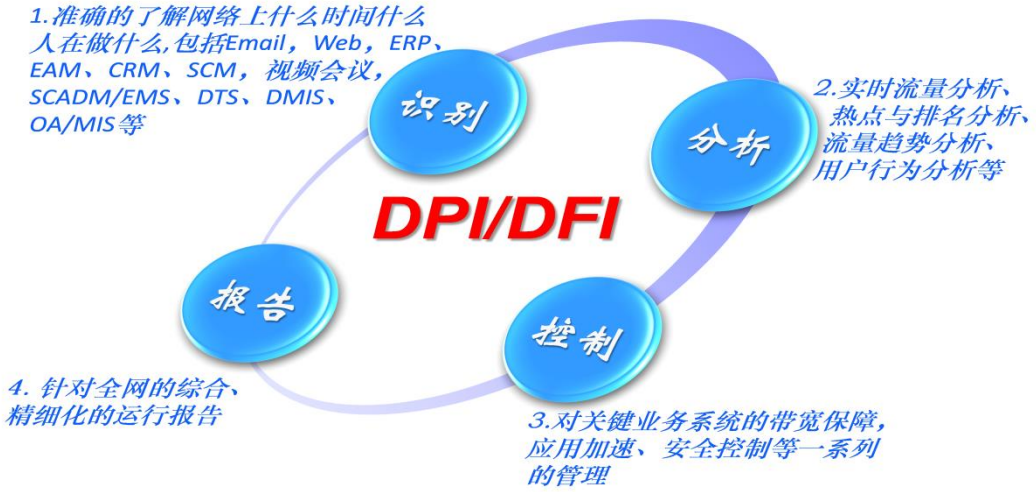
• 聪明的处理拥塞

- 针对特定应用，最小化时延和低效

5.1 方案概述

FlowShaper是基于DPI/DFI技术和HTB（多层令牌桶队列控制）技术，对业务流量进行全面的2-7层分析和实时带宽精细规划管理，能够帮助用户全面了解网络应用的情况，帮助您的营造一个透明化的、可视化的、可控化的，并且更规范，更健康，更安全网络应用环境，从而实现企业用户降低运营成本和网络收益最大化的最终目标。

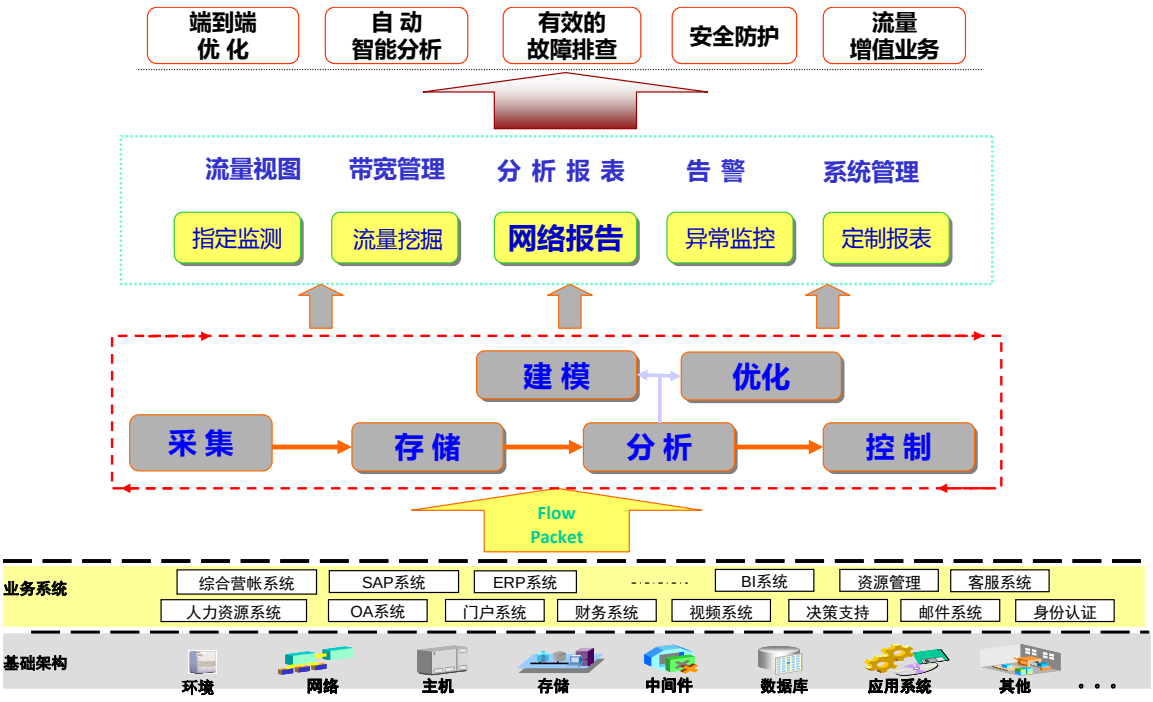
FlowShaper为优化网络流速、保障网络健康运行，围绕新一代网络宽带应用和服务进行拓展性开发和提供整体解决方案。包括网络应用和服务管理、网络应用属性和行为分析，提供关键业务和应用的QoS保证，能够有效地缓解带宽资源紧张问题，定制和确保应用层传输质量，丰富和提升业务增值手段。采用透明桥接的方式串接在网络关键点，能够对流量进行全面的企业流量7层应用分析和实时带宽精细规划管理，使您的网络从“无序”到“有序”，从“可视”到“可控”。



FlowAnalyzer是基于NetFlow数据流和SNMP网络数据实时监控与分析的产品。采用软硬件结合的产品体系架构，应用xFlow技术(NetFlow/NetStream/ sFlow/ cFlow等)，实时而长期的监控网络系统业务流量数据，对全网络流量实施监测并以图像化展现，以加强网络的可视性与可控性，实现带宽成本分析、用户流量日志、流量基线、DOS/DDoS攻击检测、蠕虫病毒监测、异常流量检测、网络带宽优化等。系统采用Web的界面，方便管理人员随时随

地分析处理并生成报表，帮助用户更清晰地掌握流量流向和流量成分的分布，它通过统计流经网络的数据业务类型、用户来源、流量流向、区域分布等信息，掌握流量基线，网站访问量和应用排名、路由负载分析、以及业务带宽成本分析、网络带宽成本分析，从而对行业业务的成本和发展情况做出判断，最终为网络优化以及业务发展策略的制定提供科学的决策数据依据。并实时侦测异常流量（如蠕虫、DoS/DDoS攻击等），更好的发现网络异常流量、有效监控用户上网行为，能够快速提升网络的服务品质。管理员可根据报表分析出用户访问了哪里或被哪个IP地址访问过，用了什么服务，传了多少信息量以及用了多少时间等。用户可利用这一报表系统，研究企业的上网行为以及企业网站被外部访问的情况。以便问题产生时，为管理人员提供备查数据。提供网络的数据业务类型、用户来源、流量流向、区域分布等信息，掌握流量基线，网站访问量和应用排名、路由负载分析、以及业务带宽成本分析、网络带宽成本分析，从而对行业业务的成本和发展情况做出判断，最终为网络优化以及业务发展策略的制定提供科学的决策数据依据。

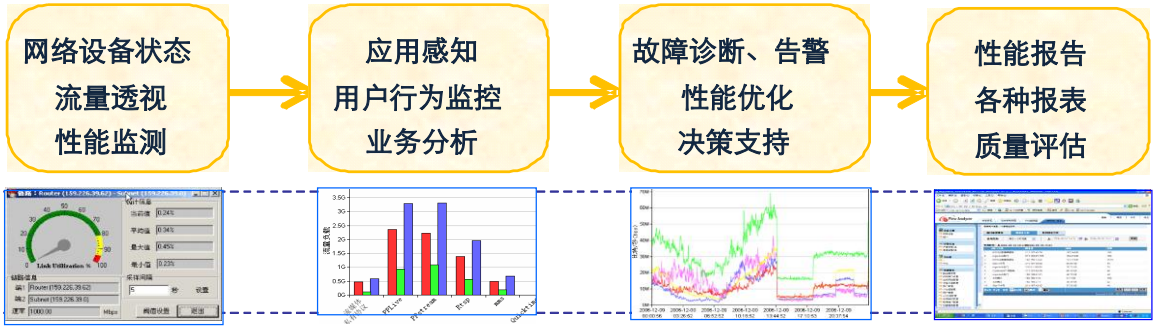
5.2 方案架构



感知你所思，优化您所想，控制您所需，保护您所虑

- 透视网络传输，全面的用户应用感知
- 深入的业务分析，详尽的网络运行报告
- 精细化网络服务管理，提高 IT 业务质量

- 简化管理，规范管理，提升网络安全性



透明：能够全面了解网络运行状况；

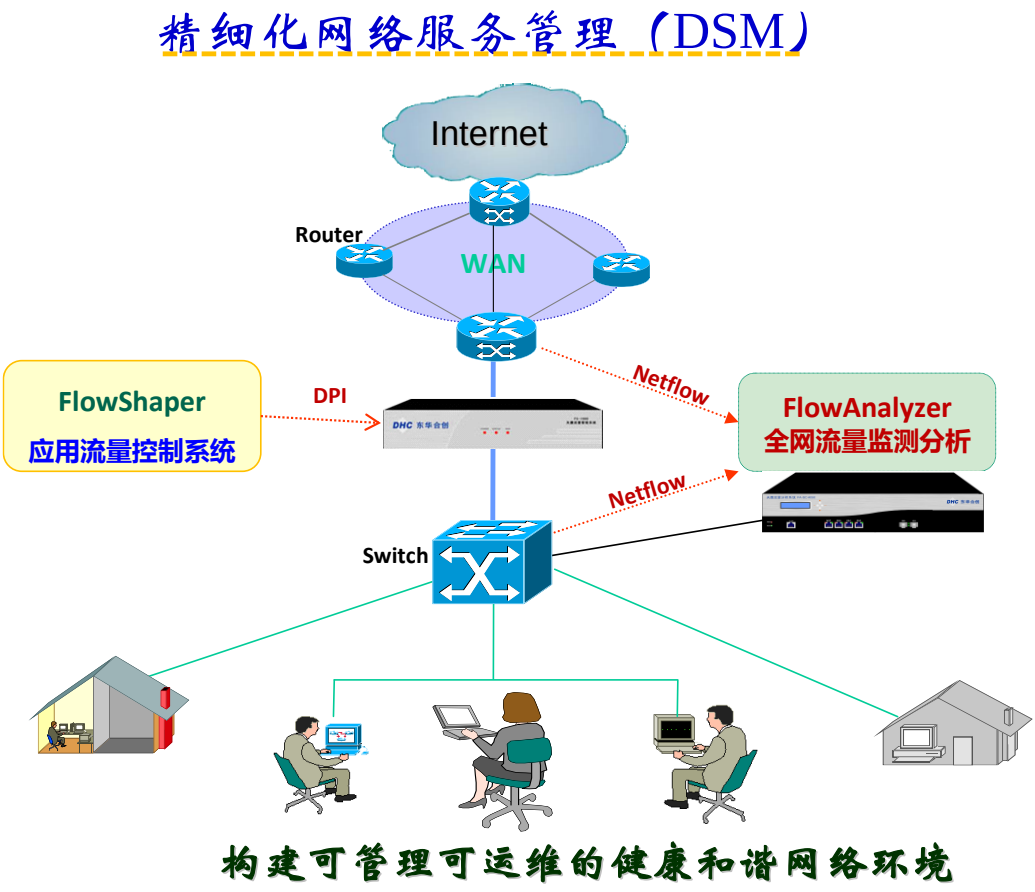
可控：能够控制网络流量带宽，保证网络服务质量；

自动：能够自动发现上报网络异常；

规范：能够规范网络的应用和用户；

易用：能够使用简单友好的统一界面进行管理。

5.3 方案部署



在本部核心部署FlowAnalyzer流量监测分析系统，在本部核心部署FlowShaper流量控制管理系统，在各个分支机构部署Flowshaper流量控制管理与加速系统。监控内网的各类应用，进行识别、分析，对用户应用进行宽带分配、优先级控制、允许或阻断等管理，保障核心业务系统的网络效能。

其主要项目建设内容功能点包括：

- ***保障视频会议的网络带宽；***
- ***保障ERP、EAM、CRM、SCM系统的网络带宽；***
- ***保障SCADM/EMS、DTS、DMIS等电力调度系统的网络带宽；***
- ***保障SG186系统及其各关键业务子系统等网络带宽；***
- ***保障OA/MIS等企业内部管理系统的网络带宽。***

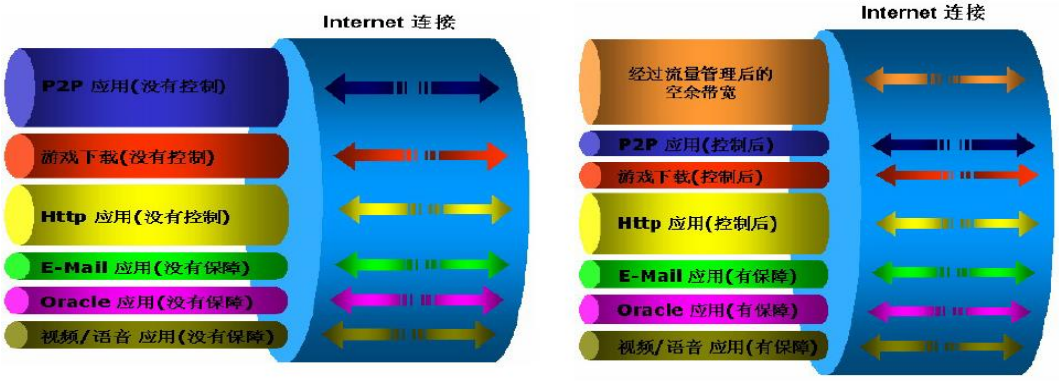
方案目标：

- 根据关键应用合理分配流量带宽，进行资源整合；
- 实现层次化分级管理模式，规范网络资源使用；
- 监控阻断网络异常流量，提升网络服务安全性；
- 全面监控网络使用情况，提供详尽的网络报告；
- 掌握网络流量的特性、了解用户的网络行为。
- 透视网络流量状态，量化网络承载能力
- 为网络服务优化提供辅助决策依据。

六、 预期效果

- ◆ 掌握网络流量的特性、了解用户的网络行为。
- ◆ 透视网络流量状态，分析用户行为。
- ◆ 量化网络承载能力，为网络服务优化提供辅助决策依据。
- ◆ 检测分析异常流量，提升网络服务安全性。

通过流量管理的技术平台，对网络中各种业务应用所占用的带宽资源有清晰的了解。对当前网络应用情况进行实时、长期的监控，实现网络的透明化管理。通过相应优化策略，对关键性应用给予高带宽、高优先级进行保障，对非关键性应用进行限制，对一些恶意的网络攻击行为进行抵御。优化系统布置以根据业务应用需要对出/入网的流量进行控制，对每种应用占用带宽进行合理分配，从而保障整个网络的稳定运行，缓解网络扩容压力，同时实现网络性能和效率的最大化。



在电力公司IT网络中部署东华流量管理系统后，帮助用户轻松实现：

- ◆ 清晰了解企业网络用户及业务对于网络资源的使用状况；
- ◆ 精确评估企业网络资源状况，为网络扩容提供定量依据；
- ◆ 针对不同部门和被管用户特点制定不同的流量管控策略；
- ◆ 针对不同业务质量要求调控网络资源，提升业务应用质量；
- ◆ 保障关键业务流量，限制非关键业务流量，提高企业网络带宽价值，提高工作效率；
- ◆ 评估网络使用状况，优化网络带宽资源；
- ◆ 提供分等级、差异化业务服务，提升用户SLA；
- ◆ 保障用户合理公平性，提高用户QoE。
- ◆ 网络异常流量发现和管理，提升企业网安全等级。

总体来说，通过使用流量监控管理系统，可以实现基于业务的流量流向和流量成分的分析性能，分析总体业务发展趋势和访问行为，为网络瓶颈排除和性能优化提供依据；可以对网络资源的使用情况进行精细化管理，避免因为资源使用过度或使用状况不明所导致

的网络服务质量下降；可以实现性能统计和性能趋势分析，提供灵活的报表功能，提高网络运行维护水平；可以提供多样的历史资料条件查询和统计分析，便于指导网络的规划和资源优化，为网络业务发展提供数据依据；实现网络的统一调配。可以加强网络的流量安全防范，建立系统化的流量管理体系，提高网络访问质量，增强用户的自御能力。

- 建立可视化、量化、可管理的系统网络；
- 构筑和谐健康、稳定高效的网络系统；
- 提高用户满意度，提升企业竞争力。