



校园网络 — 湘潭大學案例

InstantQoS-5000 导入成效



湘潭大學

XIANGTAN
UNIVERSITY

L7 NETWORKS INC.

2008/5/12

校园网络 – 湘潭大学案例

InstantQoS-5000 导入成效

专案背景：

湘潭大学是一所教学研究型的综合性全国重点大学，座落在毛泽东同志的故乡——湖南省湘潭市，是湖南省人民政府、教育部共同重点支持建设高校，是全国首批具有硕士学位授予权的单位，湖南省首批招收留学生和国防生的高校，教育部本科教学工作水平评估优秀学校。

第一部分 湘潭大学网络现状及需求分析

1.1 湘潭大学的网络现状

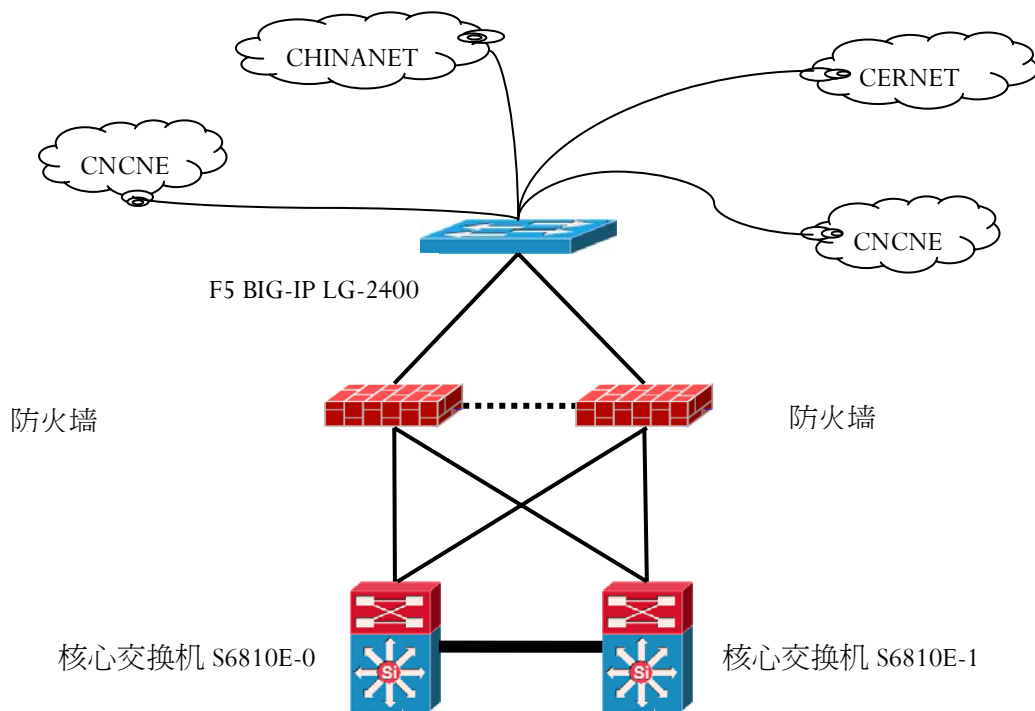
1、网络结构

湘潭大学采用了两台锐捷 S6810E 万兆交换机作为核心交换机，并采用万兆连接将两台设备互联，然后分别以千兆光纤上联至两台博华 YG-FWS-NP 型号防火墙，防火墙之间采用心跳连接。防火墙均采用千兆光纤上联到一台型号为 F5 BIG-IP LG-2400 的负载均衡器，再接入 Internet。

2、网络现状

- 湘潭大学的 Internet 总接入带宽为 400Mb (单向)，其中

CERNET 为 100Mb · 电信 100Mb · 网通 200Mb · 运营商实际提供的带宽是小于 400Mb 的 · 校园网实际可用带宽仅为 330Mb · 与此同时 · 校园网内的用户数在不断增加中 · 不断有新的楼栋接入校园网 · 各二级单位很多都设立了自己的计算机房供学生使用 ·



- 网络的应用越来越复杂 · 以 Bit Torrent · eDonkey · 迅雷等为代表的 P2P 类文件共享应用越来越多 · 各种多媒体应用也在逐步向 P2P 协议靠拢 · 近几年出现了 PPLive · PPStream · QQLive 等以 P2P 协议为传输协议的网络视频应用 · 并且随着一些 P2P

协议的开放，有越来越多的 P2P 类多媒体应用在不断出现。另一方面，P2P 的应用的通讯方式已经从早期比较“规范”的单纯 P2P 共享网络模式，慢慢演变为采用一些不文明手段来提高自身共享速率的通讯模式，比如 PPLive 网络电视就采用了类似于 UDP Flood 的方式，即大量发送 UDP 小包的方式来保证自己获得稳定的连接。在这种情况下，校园网的数据流变得异常复杂。

- 随着以太网速率的不断提升，Internet 传输速率的大幅提高，以及联网使用者的不断增多，计算机的安全威胁也在不断的变化。几年前的计算机病毒或特洛伊木马等恶意软件对于网络的利用还仅仅复制自身、窃取信息向特定主机发送等，主要的威胁对象是计算机用户本身，对于网络并不造成直接的威胁，但现今的计算机病毒等恶意软件除了给计算机网络带来传统的威胁外，还越来越多的利用了现代计算机的高性能和网络的高传输速率来向 Internet 上的主机发起拒绝服务式攻击 (DoS)。随着僵尸网络 (BotNet) 的出现，已经有越来越多的局域网计算机在不知不觉的中被人操控成为了 DDoS 的攻击源。在这种新形式的计算机安全威胁中，作为局域网出口的路由器、负载

均衡器等智能设备受到了空前的威胁。

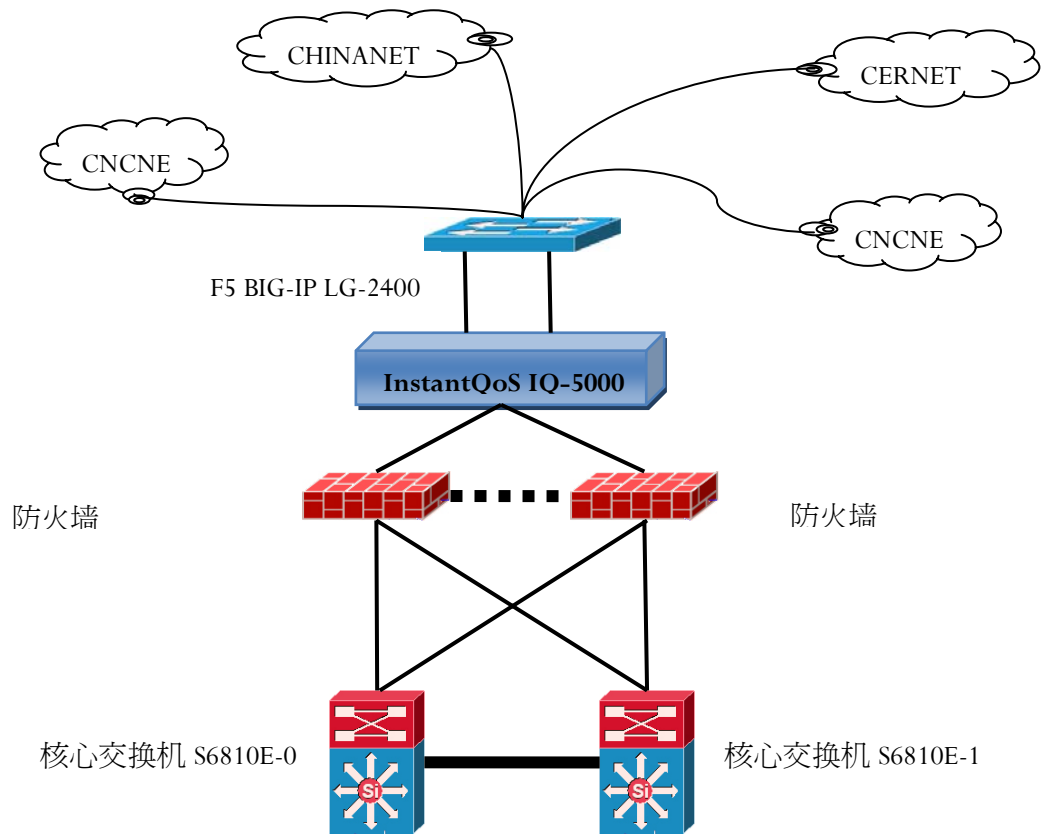
湘潭大学校园网作为一个大型的局域网络，同样遭受着其他所有局域网都遭受着的威胁，其中最为明显的就是内网中毒用户所产生的洪泛流量（UDP Flooding、SYN Flooding 及 ICMP Flooding 等）对出口设备造成的巨大压力。

1.2 需求分析

根据对湘潭大学网络现状的了解，我们认为存在下面几个方面的需求，针对需求并提出一些建议。

1.2.1 设备数量及对网络拓扑结构的建议

因为 L7 Networks 的 InstantQoS IQ-5000 型号流量控制产品支持多桥并行处理，所以建议采购一台 IQ-5000 型号的流量控制产品，将拓扑图中的两套链路全部经过 IQ-5000 进行连接。这样做可以保证两条链路的在线状态，当一条链路出现问题时，可以由 VRRP 或 OSPF 自动切换到另一条链路，避免管理人员需要到场操作的麻烦。同时通过加接 BYPASS 卡做到容错，以免万一设备故障而造成网络的瘫痪。



1.2.2 处理性能需求

- 由于校园网出口最大可用带宽为 400Mb，同时为保证带宽增加后仍然能够进行处理，所以要求设备至少要提供双向 2Gbps 的处理能力。而且因为校园网核心层采用了双链路冗余设计，故而需要设备能够支持多桥并行处理。
- 能够智慧的识别来自内网的 UDP、SYN、ICMP 洪泛攻击，并自动进行处理，保护出口的负载均衡器不被这些恶意数据流影响。
- 由于校园网的用户庞大且需求各有不同，同时为满足学校管理的需要，所以要求设备应该能够提供针对 IP 地址或 IP 范围(子

网) 的上下行流量控制、会话数控制，并且能够提供丰富的策略模式以便进行管理。

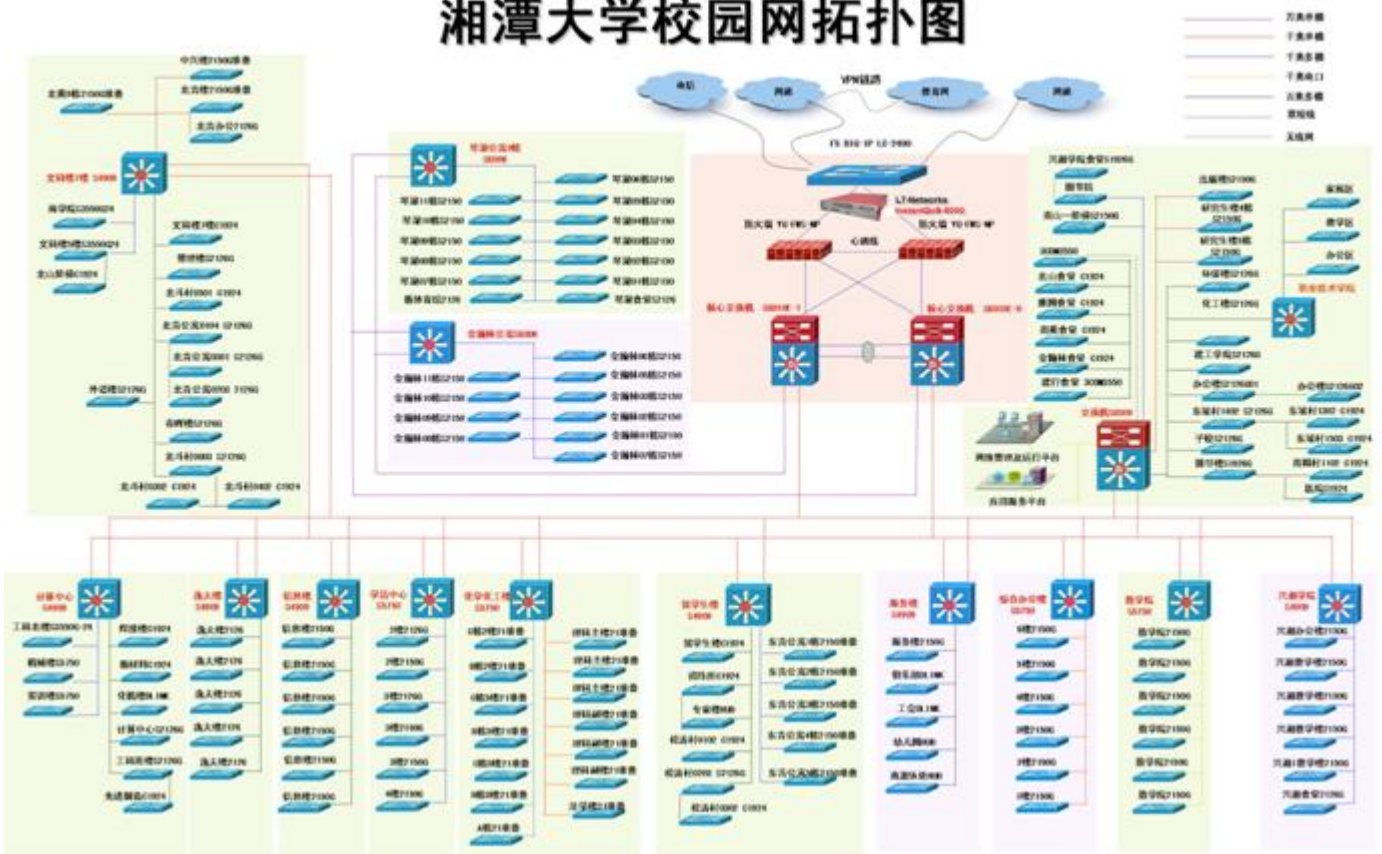
- 能够在不产生网络瓶颈的前提下，依据通讯的内容或行为识别出网络上的各种应用协议，并能够管理这些不同协议的通讯，能够做出粒度比较细的控制策略。
- 为便于管理，需要对网络中流量的历史数据进行记录并生成报表以便查询。

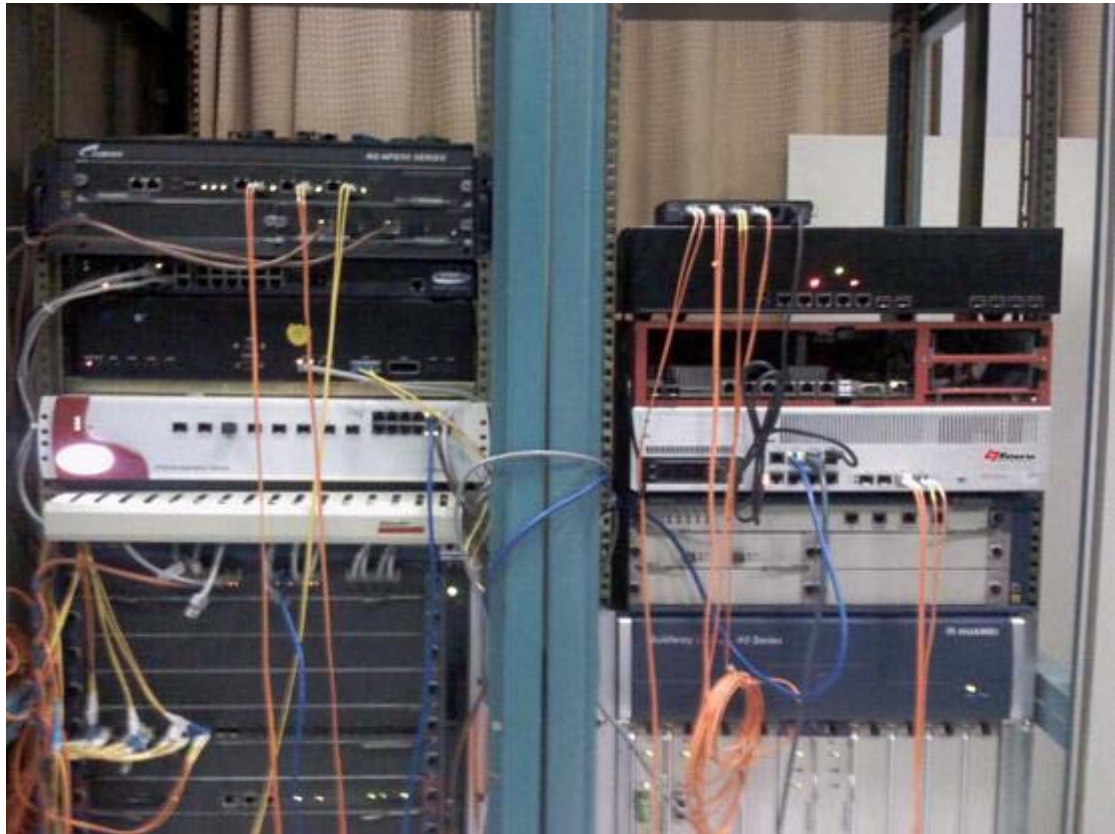
第二部分 湘潭大学网络解决方案

针对湖南湘潭大学校园网络存在的主要问题，L7 Networks 管理推出了相应解决方案：将 L7 Networks InstantQoS 应用优化设备接在网络出口防火墙和核心交换机之间，对于所有经过网络出口的数据报进行了特征码分析，实现 Internet 出口带宽的优化。其具体部署如下图所示。

将 L7 Networks InstantQoS 应用优化设备部署在湘潭大学的网络出口，可以为湖南湘潭大学信息化网络实现如下功能和效果：

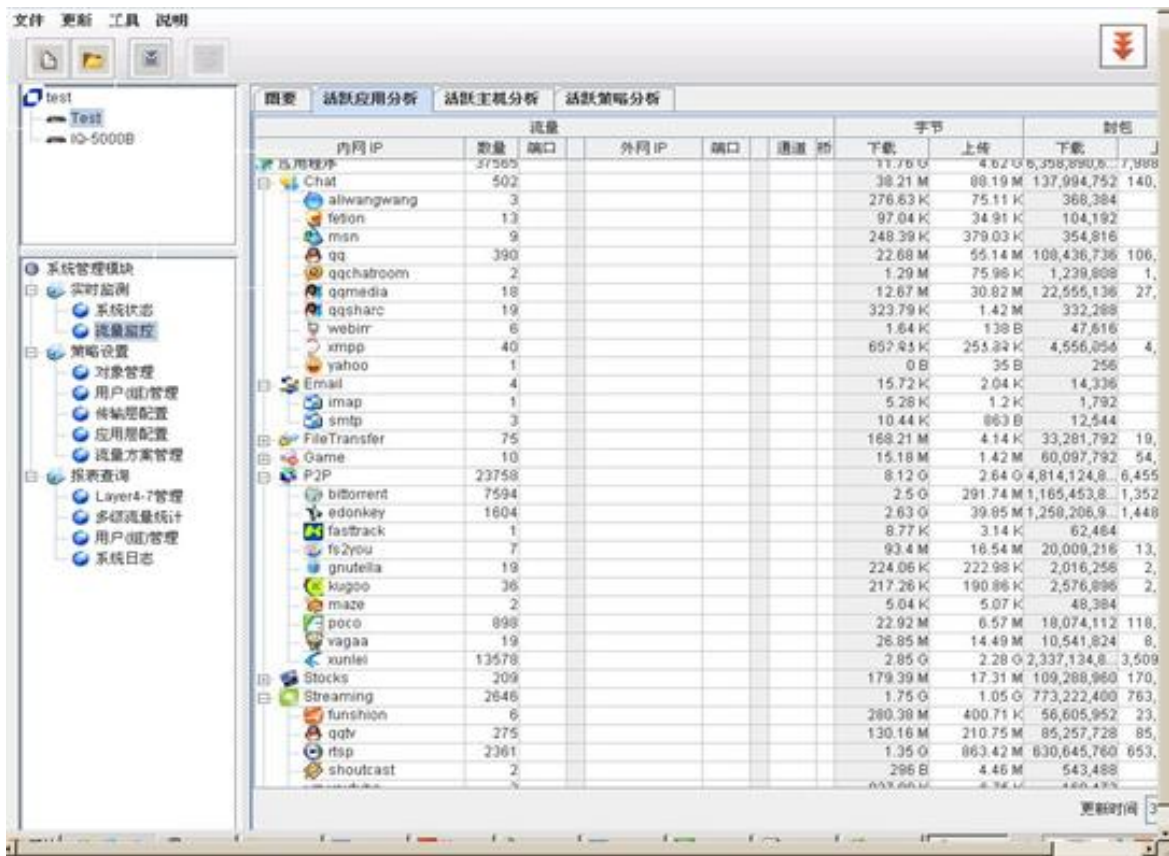
湘潭大学校园网拓扑图





方案一、可视化显示网络流量

将 L7 Networks InstantQoS 部署在网络出口，自动侦测湖南湘潭大学校园网络中异常的流量，使得网管人员可以详细了解校园网络中运行着哪些应用和流量。它以数据化和图形化直观的了解网络应用程序运行的性能，网络负载以及网络带宽使用情况，提供多样化的查询方式。



方案二、限制非关键应用

限制没有经过校方管理部门允许的通过校园网络的上网行为，如 P2P 下载、聊天、网络游戏等严重影响学生学习和生活的各类网络应用。

方案三、优化网络流量

L7 Networks InstantQoS 应用内容交换器设备的网络流量优化功能可以有效地进行校园网络带宽资源管理和分配，实现分级服务分配，对于动态端口应用如 P2P,迅雷等 Layer7 应用全部都可以进行管理和控制，对于没有经过授权的未知网络流量进行阻断，从而保证带宽资源的有效利用，提高网络性能保障系统服务质量。

方案四、保障关键应用和用户的带宽

利用分级带宽管理功能，指定校园网络为 WEB 应用和办公网段保留带宽，同时限制学生应用带宽。固定每个子网的带宽，不会因为个别用户的疯狂下载而导致某个网段内部甚至整个校园网络重大问题。在不同的时间段进行自动的策略分配，满足不同时间段内不同用户不同应用的带宽资源分配。灵活、高效、可靠。

方案五、实现网络的安全稳定化

无论在什么时候，网络的安全总是头等大事。L7 Networks InstantQoS 应用优化设备虽然不是一个专门的安全类型产品，但是它利用智能识别技术可以识别并阻断端口扫描、DoS 攻击等黑客行为，提高网络系统的整体安全性。因而被誉为“应用层的防火墙”。

综上所述：L7 Networks InstantQoS 应用内容交换器设备秉持“保障核心业务和关键用户的网络带宽服务质量”的理念，使得湖南湘潭大学的网管人员能轻松管理、控制和优化自己的网络应用，达到可见、可测、

可控、可优化的主动式、智能化的应用优化和带宽管理，达到“效率和安全性最大化，实施和威胁最小化”的效果。

用户获得的投资收益：

部署了 L7 Networks InstantQoS 应用内容交换器设备对湖南湘潭大学的网络进行规范化管理后，节省了大量宝贵的网络带宽资源。L7 Networks InstantQoS 应用内容交换器设备运行稳定可靠，性能表现相当出色。能够为湖南湘潭大学用户带来如下的收益：实现湖南湘潭大学信息出口的网络应用与网络流量的可视化；保障 湖南湘潭大学校园网到 internet 的畅通无阻；提高了湖南湘潭大学的带宽使用效率，降低 IT 投资成本；降低湖南湘潭大学信息中心的网络运维管理成本；提高整个湖南湘潭大学网络运行的可见性、可测性、可控性和可优化性。