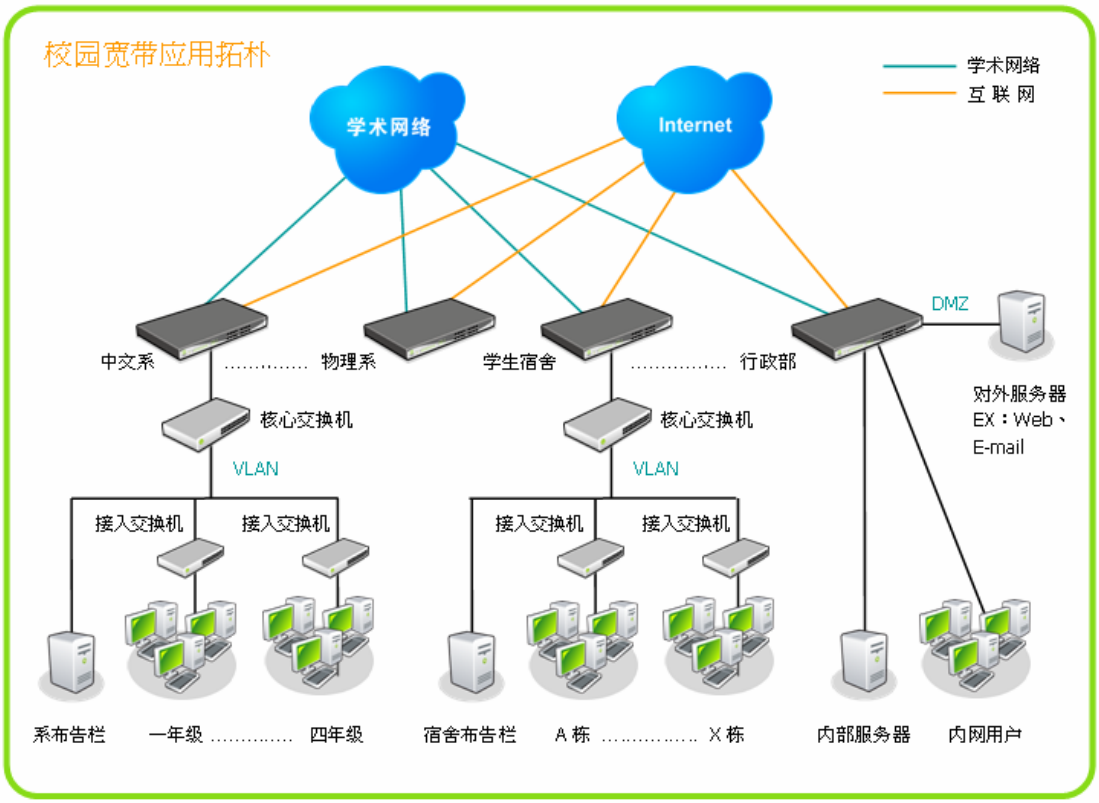
侠诺科技股份有限公司
台湾300新竹市埔顶路25号6F之2
Tel:+886-3-5678100
Fax:+886-3-6686255
http://www.Qno.cn

侠诺工程师经验谈 高校网络建设四个必须

一般而言，校园内都有教育网系统，但因为有限的带宽以及校园网络安全等等问题，各系或是学生宿舍都会在学术网络之外，大多会再自行建置一条或多条 ADSL 网络，以用来应付更大带宽使用的需求。因此在一般校园网络架构系统中，普遍我们可看到包含"教育网"和"公众网络"两种系统并行。

照常理，校园网络比起一般网络应用环境，多出了教育网络系统可以分担上网的流量，因此应该不会有上网速度慢的问题。但根据用户使用经验指出，在校园或宿舍使用网络，不但常常会遭遇到上网慢问题，甚至掉线、病毒攻击等问题也层出不穷。难道带宽还是不够吗？带宽管理没有用吗？究竟学术网络与一般网络应用该如何整合？侠诺科技深圳技术中心主任文浩坚针对校园实际面临到的问题，提出了四个必须的配置建议。



图一：校园宽带应用拓朴图

侠诺科技股份有限公司
台湾300新竹市埔顶路25号6F之2
Tel:+886-3-5678100
Fax:+886-3-6686255
http://www.Qno.cn

一、必须选择多 WAN 的路由器

校园内由于各个系与宿舍，所分配到的学术网络一般有限，因此多半会自行接入公众的宽带网络（例如 ADSL）增加带宽。虽然，校园网络组织架构包含教育网以及公众网络，但是如果分别建置各自的路由器，还必须分别进行配发 IP 与种种管理设定，对于要管理各个系或是学校宿舍的网管人员来说，可以说是非常繁琐的工作。因此，如果能采用多 WAN 口的路由器，即可将学术网络以及一般网络共同建置在一台路由器上，通过策略路由的设定，让教育网与一般网络各种设定分流，达成化繁为简的目的。

图二：策略路由分流学术网络与一般宽带网络

校园各系与学生宿舍在学术网络之外再接入的公众网络，都希望以最低的成本增加最大的带宽，光纤固然是大家脑海中浮现的第一选择，但碍于预算限制，实现起来比较困难。而多 WAN 路由器，不但可接入多条 ADSL，并且凭借其汇聚带宽的作用，不但节省了成本，也能够享受到足够使用的带宽服务。

此外，根据许多学生反应，校园网络仍常常存在网络不稳、掉线等问题，而多 WAN 路由器由于可同时接入多条线路，加上自动备援线路设定，正好可解决此类的问题。

二、必须选用智能带宽管理功能

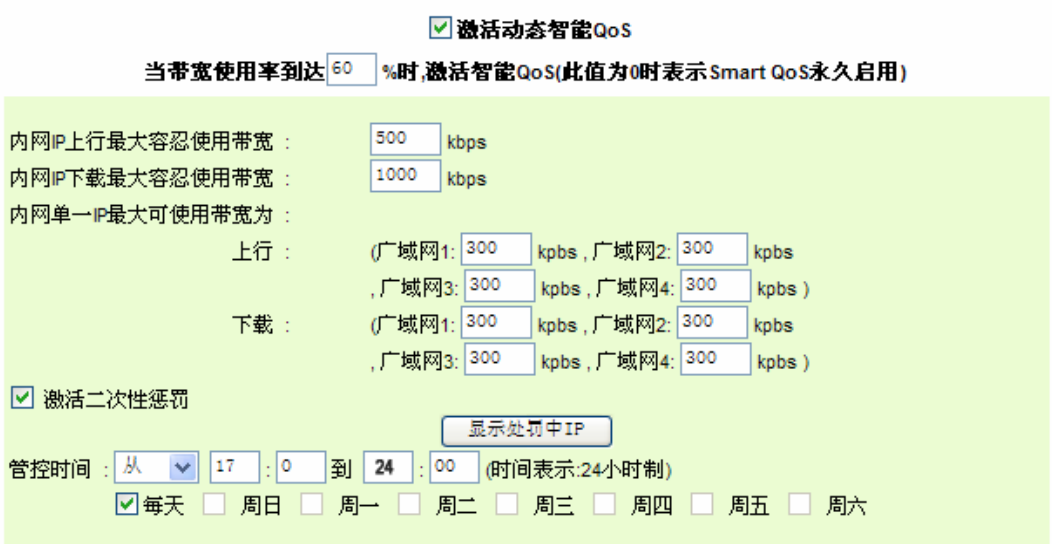
在接触校园的案件中，我们听到学生抱怨最多的便是上网速度慢的问题，对于选课、注册、交作业……等等即时性需求，的确是一个很大的困扰。实际上，当我们技术团队

侠诺科技股份有限公司
台湾300新竹市埔顶路25号6F之2
Tel:+886-3-5678100
Fax:+886-3-6686255
http://www.Qno.cn

深入了解之后，发现经常是因为某些学生正在下载 BT、P2P、或者其它视频影音……，大量占用了整体带宽所导致网络卡的问题，对于这样的情况，增加再多的带宽还是不够用的!

解决这个问题，就需要进行带宽管理。但由于网络普及以及日趋繁杂应用，一般的带宽管理 QoS 功能突显了两大弊病。第一，无法有效抑制大量占带者：网管人员必须进行手动的一一查找，才可找出大量占带者的 IP，但是网络却已经瘫痪好时间了。接下来再花费一番功夫给予警告或封锁 IP，恶意占带者经常是再换个 IP 继续下载，网管人员又得一一重来，可以说是防不胜防；第二，大弊病在于带宽利用率很低的问题：一般 QoS 带宽管理，必须一次配置好每个 IP 容许的最大带宽使用量，但是网络使用有高峰与低峰的时间，如果都采用同一个配置带宽使用限制，会造成整体环境只有 1 人上网与有 100 人上网时，每个人可使用的带宽都一样，导致整体带宽利用率很低的现象。当然，网管人员也可时时自行调整带宽使用限制，但是会在无形中增加繁重的工作量。

因此，建议校园网要进行有效的带宽管理，可采用配备智能 QoS 带宽管理的路由器，可同时解决恶意大量占带者以及带宽使用率不佳的两大问题。由于智能 QoS 可自动将大量占带者的 IP 自动列入黑名单列表进行观察，针对持续占带者再加以二次惩罚，将该 IP 可使用的带宽减半等等，即可轻松有效的抑制恶意占带者，保障正常使用者的带宽，快速恢复正常网络速度。另外在带宽利用率上，智能 QoS 提供可自由设定某一天某一个时段，整体带宽流量门坎达多少以上（例如现有带宽使用达 60%），才会开始执行带宽控管，轻松实现高峰与低峰时间享受不同大小的带宽服务，达成弹性的带宽管理，也成就了带宽使用率最佳化的表现。



图三：智能 QoS 自动弹性控管带宽

三、必须具备有防火墙的功能

校园网络由于学生人数众多，因此更要防止各式黑客、蠕虫病毒等攻击，以确保内网以及外网的安全。目前来说，最多的攻击形式仍以 ARP 攻击居多，因此建议校园选择的路由器设备中，最好能够拥有内建的防制 ARP 功能，藉由自动检视封包的机制，侦测过滤可疑的封包，做为防制 ARP 攻击的第一道防线。当然如果网管人员可搭配 IP /MAC 双向绑定，在路由器端以及各个系或是宿舍内的 PC 端进行 IP/MAC 绑定，即可达到防堵 ARP 无漏洞的效果。

另外一方面，由于网络信息包罗万象，有许多例如 BT 下载、色情网站等不当应用或网站，对于校园风气造成不良的影响，应通过防火墙设定予以封锁。

图四：防火墙设定接口图

四、必须有基础 VLAN 隔离

虽然强效防火墙可防止一般的攻击，但目前许多病毒与攻击层出不穷，校园网络又如此庞大，因此万一不幸中毒，也希望可以尽量缩小感染的范围，不致扩散到整体网络。因此各个系及学生宿舍都必须建置基础的 VLAN 隔离，才不会导致某层宿舍里某个学生中毒，造成整个学生宿舍网络全面感染中毒的状况。

侠诺科技股份有限公司
台湾300新竹市埔顶路25号6F之2
Tel:+886-3-5678100
Fax:+886-3-6686255
http://www.Qno.cn

VLAN 的概念是让网管依据不同网段，划分出不同的局域网，比如宿舍区可区分为一楼、二楼、三楼等不同 VLAN，再使用 VLAN 功能将一楼、二楼、三楼不同局域网区分为 VLAN1、VLAN2、VLAN3 作为隔离。如此一来，不同 VLAN 的局域网便不能互相访问，进而可限制病毒与无用信息流通。也就是说，当一个 VLAN 中(例如：一楼)有人不幸中毒，只会影响同一个 VLAN(一楼)内的 VLAN，不会扩散到整个学生宿舍，可有效避免广播及病毒封包迅速扩散全网，大大降低感染区域。

图五：VLAN 避免广播及病毒封包迅速扩散全网

最后，侠诺科技深圳技术中心主任文浩坚建议，校园在建置网络同时，若能将多 WAN、智能带宽管理、防火墙、基础 VLAN 四个必须，结合再同一台路由器上，并同步进行各项控管，才能真正实现化繁为简的强大功能，进一步帮助校园轻松建立全面、安全、快速、稳定的网络系统。