第四章 中小企业安全路由器带宽管理

近年来，带宽的价格已经不像以前那么昂贵了。一般的中小企业，也能很轻易地使用 ADSL 的宽带服务于企业运作及业务上，以往高不可及的光纤价格也持续在下降。但是由于企业对互联网的依赖性有所增加，不同的对外联络都需要用到宽带服务，再加上更多音频视频应用、大文件交换，如 VoIP、视频会议、设计图传送等等，这些都大量占用带宽，影响日常的工作。

有效优化带宽的应用的工作，我们称为带宽管理。网管追求的是将有限的带宽，应用在对公司有益或重要的应用上，而将效益较小或对企业营运有害的应用，予以限制。好的带宽管理，将使企业中重要的工作可得到足够的带宽，加速完成工作；而恶意占用带宽或员工为个人利益使用带宽的情况降到最少。这样对于企业而言，也是某个层次的安全，因此营运得以持续，企业不会有损失，甚至还可创造利润。

我们把一般中小企业网管常碰到的带宽管理问题列在下面，同时也列出 Qno 侠诺路由器对应可以使用的功能：

项目	问题	侠诺产品功能
1	如何判断整体带宽是否足够？如何进行最简易的带宽管理工作？	系统状态实时监控、动态智能 QoS
2	如何阻挡 MSN，QQ 及实时通等应用?部份重要人士不需要管制如何处理？	单指键阻挡特定服务、排除功能、联机数管控
3	带宽不足情况下，如何予以优化?如何以最简单的方式，完成带宽管理工作?	带宽管理配置、动态智能 QoS
4	如何阻挡大量下载如 BT、点点通?如何有效限制 QQ 视频？如何针对新的网络应用，进行管制配置?	限制特定应用软件、动态智能 QoS

4．1 系统状态即时监控

对于网管来说，带宽管理最重要的工作，就是了解整体带宽是否足够。因为如果对外使用带宽不足，即使做再多配置，可能都无法解决问题。在侠诺路由器的“日志”功能中，有

一个系统状态即时监控的功能，可以提供整体路由器系统运作信息。

在该功能的画面中，有一个显示“上传带宽使用率”及“下载带宽使用率”的信息，即可作为网管判断是否有对外带宽不足现象的依据。若是在正常的状况下，内部没有大量占用带宽的用户或是攻击，所有广域网连接带宽使用率，如果出现上传或下载持续超过 80%的情况，表示企业所使用的对外带宽不足，有升级的必要。如果是多 WAN 的情况，则可经由适当的带宽管理，加以改善。

系统状态

接口位置	局域网接口	广域网1接口	广域网2接口
机器名称	ixp0	ixp1	ixp2
目前端口连线状态	联机	联机	掉线
IP地址	192.168.1.1	60.248.80.100	0.0.0.0
网路实体位置	10-2f-d4-76-14-5d	26-0c-35-3c-74-b4	00-db-78-d2-79-a9
子网掩码	255.255.255.0	255.255.255.0	0.0.0.0
预设网关	---	60.248.80.254	0.0.0.0
域名解析服务地址	192.168.1.1	168.95.1.1 0.0.0.0	0.0.0.0
线路侦测机制	---	测试成功	测试失败
收到的封包数量	5579	0	0
传送的封包数量	5049	0	0
全部的封包数量	10628	0	0
统计收到的封包Byte数量	674266	0	0
统计传送的封包Byte数量	1629421	0	0
统计全部的封包Byte数量	2303687	0	0
接收Bytes/秒	0	0	0
传送Bytes/秒	0	0	0
统计收到的错误封包统计	0	0	0
统计收到的错误封包统计	0	0	0
联机数	---	0	2
新联机数/秒	---	0	0
上传带宽使用率(%)	---	0	0
下载带宽使用率(%)	---	0	0

刷新

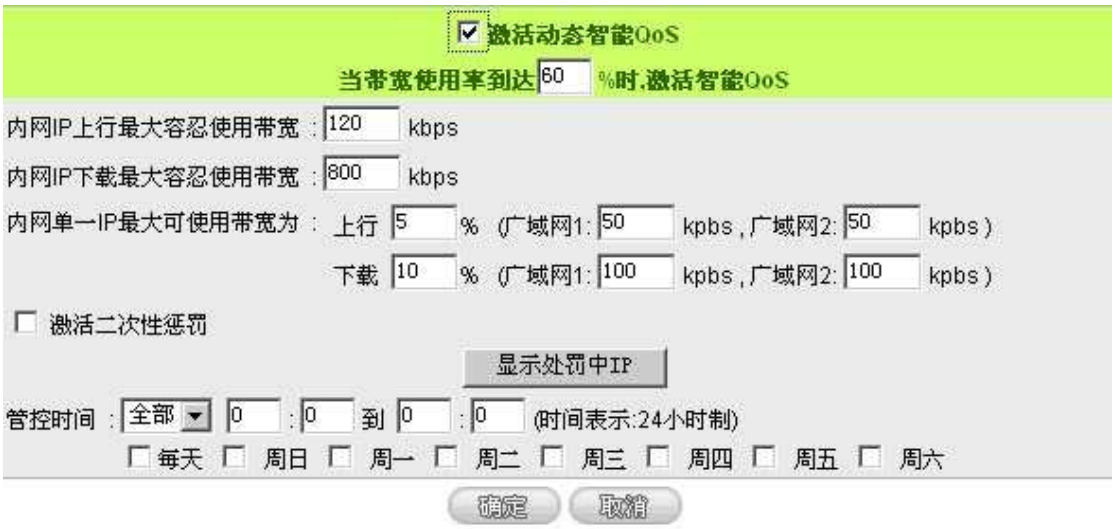
图一：侠诺路由器的“日志”功能中“系统状态即时监控”功能，可显示“上传带宽使用率”及“下载带宽使用率”的信息，即可作为网管判断是否有对外带宽有不足的现象。

4．2 动态智能 QoS

动态智能 QoS 是侠诺为了协助网管解决带宽管理配置，所推出的强大功能。它强调用户可以不管内部各种应用，只要填入基本带宽数字及单一用户的带宽容许比例，路由器即可自行进行依内部带宽使用，进行带宽管理的工作。

动态智能带宽管理强调，自动压抑占用带宽用户，来解决内网 QoS 管理，简化网管的管理工作。当某些用户占用带宽超过网管配置的阀值时，路由器即会限制该用户所使用的带宽一段时间，例如五分钟，以免带宽被少数的用户占用，影响其它用户的使用。对于持续有

意占用带宽的用户，当有持续占用带宽的现象时，路由器即会启动二次惩罚，持续压抑该用户能使用的带宽，这种功能对于中了会持续占用带宽病毒的用户，可起到缩小损害的作用。另外动态智能 QoS 也支持定时的设计，可配置特定时间才启动带宽管理。



图二：无需网管进行配置的智能型带宽管理 Smart QoS 功能。

4．3 阻挡特定服务

侠诺路由器提供一键挡特定的服务功能，可以通过设置将 MSN、Skype、QQ、BT 下载这些服务挡住，以方便用户的管理设置。阻挡特定服务是以勾选的方法,决定限制哪些服务,另外还提供有排除功能,可以排除特定 IP 用户,例如公司老板或是高管等。

图三：本图可以看出内部网络 192.168.1.2~100 的 IP 将不提供 MSN 及时信息服务功能，中小企业可以按照需要对内网 IP 的这几个特定服务做挡定设置。

4．4 联机数管控

另一个阻挡有害服务的控制，是经由联机数管控来进行。联机数管控可以控制内网的计算器最多能同时建立的联机数。这个功能对网管人员在控制内网使用 P2P 软件（如 BT、BT、emule 等会造成大量发出联机数 session 的软件）提供了非常有效的管理。设置恰当的容许联机数可以有效控制 P2P 软件时所能产生的联机数，相对也使带宽使用量达到一定的限制。另外，若计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。

当有内部 IP 对外联机数超过设定的联机数限制值时，路由器即会阻挡该 IP 上网一段时间，以管制带宽不被占用。联机数管控也可设定有效时间,在非生效期间不进行管制。

图四：联机数管控是另一种有效限制大量占用带宽软件的一种方法,联机数管控可配置特定时间管控，也可设定不受限制的服务（公司财务数据的传输，邮件的传输等）或者 IP 不受联机管制。

4．5 带宽管理配置

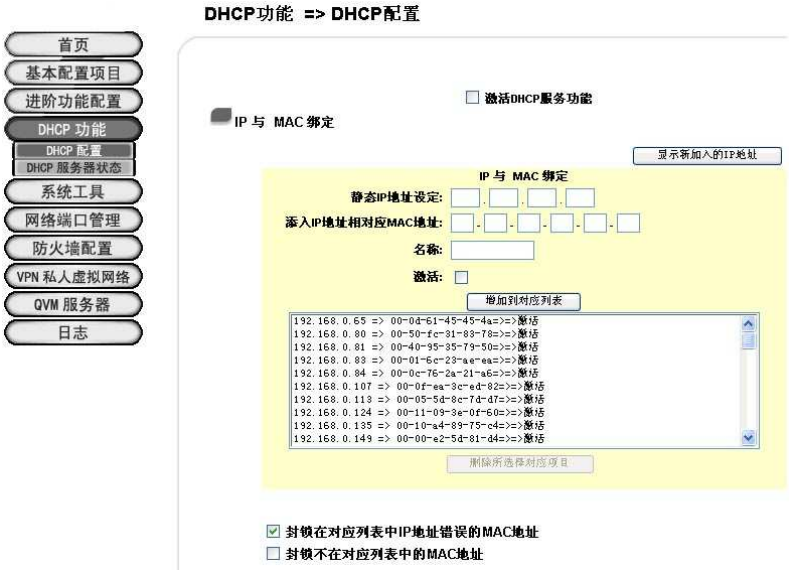
带宽管理可从不同的角度来落实，例如以人为规范进行、以计算机是否可以上网进行，但最方便合理的，还是通过路由器的设定达成。因为路由器往往是局域网对外的网关，通过路由器管制，通常可集中管理效果，不易有遗漏。路由器可检查每个进出的封包，决定优先处理或者不予处理，以将带宽保留给较重要的应用。以下是从路由器的观点，较常见的带宽管理方式：

依使用者或主机加以管制：我们可针对特定局域网或外部的主机，加以进行管制。例如不允

许内部某部计算机上网，或只允许某部计算机上网；或不允许网络用户联机外部某台主机等等。这样的作法，都是通过限制存取某个使用者或主机的方式，进行管制。例如在下图的防火墙配置中，我们看到存取服务规则设定中，可经由设定“来源 IP 地址”及“目的 IP 地址”的方式，限制或允许联机的进行。其中来源地址可能是局域网用户，也可能是外界需要服务的地址；目的 IP 地址也相同。网管可依需要进行配置。

图五：依使用者或主机加以管制是可以采用的方法之一。

对局域网用户而言，以 IP 进行管制也不是完全没有缺点，有些聪明的用户会自行修改 IP，以逃避路由器的管制。有些用户甚至会修改成领导的 IP，以取得更高的权限，进行信息的存取及带宽的利用。对于网管人员，这个问题当然要加以解决。还好，每个网络卡都有一个独一无二的识别号码，一般用户很难更改。因此我们可通过“IP 与 MAC 绑定”的功能，规范在分配 IP 时，某些 MAC 地址，即网络上的网络卡 / 主机取得特定的 IP 地址。若设为其它 IP 时，则无法上网。这个功能对于智能小区业者及高度敏感的单位网管都很重要。



图六：IP 与 MAC 绑定可确保管控的有效性。

依应用加以管制：我们也可以利用网络应用的端口号，加以进行管制。这就好比军事上针对特定频道加以干扰，破坏通讯的例子一样。由于常见的应用，往往都有特定的端口号，因此我们只要找出对应的端口号，在存取规则设定中，进行允许或限制的执行即可。依应用的端口加以管制。以下的画面，就显示出常用的应用端口号，只要进行设定允许或禁止，即可管制不同应用封包的进出。

除了常见的应用端口号外，面对日新月异的应用，网管也可自行设定应用及对应端口号，以简化日后设定的过程。

图七： 应用的管制是利用网络应用的端口数，加以进行管制。

依内容：最直接的作法，就是针对传送内容进行管制。也就是不想传送什么内容，就通过关键词或文件名管制。在以下的管制设定页面中，我们可以看到网页内容管制设定，是依网页内容所包含的字符串进行管制。而网页字符串，则是通过传送网页的名称或文件名，加以管制。通过这二者的设定，网管可阻绝特定内容的网页，或者是特定文件格式的网页、服务或文件。

图八：针对传送内容进行管制是通过关键词或文件名进行管制。

依 WAN 口：对于多 WAN 路由器而言，也可通过不同 WAN 口的分配模式，将带宽分配到不同的 WAN 口。Qno 的产品可支持三种不同带宽分配模式。IP 群组是将特定 IP 使用者，指定到某个 WAN 口，它的好处是可将不同群组使用带宽分隔来开，部份群组使用带宽的情况不会影响其它的使用者。IP 负载均衡则是路由器会依局域网 IP，依次分派到不同 WAN 口，以平衡带宽的使用，它的好处是同一个 IP 存取流向都经由同一个 WAN 口，能适应不同应用的通讯特性，不易出错。智能型负载均衡则是路由器会综合考虑应用、使用带宽、WAN 流量、及 IP 分布，自动进行带宽的分布。通过 WAN 口的限制，也能有效进行带宽的管理。

图九： 多 WAN 路由器而言，也可通过不同 WAN 口的分配模式，将带宽分配到不同的 WAN 口。

以下显示不同 WAN 口还可以设定各种管制方式，交叉应用进行管制。

图十：实际的应用往往需要组合不同的管制方法。

除了以上的管制方式外，还有其它的方式可以进行管理。例如在防火墙配置的访问存取规则设定中，每个规则都可设定作用的时间，可按星期或一天的时间进行设定。网管可设定上班时间启动管制，在下班及休息时间不作管制。

以上我们了解了带宽管理的一些技巧后，相信大家对如何作带宽管理有一个基本的了解。

4．6 如何针对新应用进行带宽管理

在我们了解可使用的带宽管理工具后，网管必须针对面临的问题，进行分析诊断，再适当组合不同的工具，以达到限制或管理的目的。虽然不同网管面临的问题不同，寻求的解决程度也不相同，但是整体来说，要通过路由器进行带宽管理，是方式可以遵循的。以下我们简单介绍这个程序，并以几个例子说明如何实际针对问题，加以解决。

一般来说，在进行带宽管理或管制时，有以下的步骤可依循：

定义问题：首先网管必须先了解问题出在什么地方，才能针对问题谋求解决方式。有些问题是因为带宽不足造成，有些问题是因为 ISP 服务质量不足，而有些则是特定使用者大量下载文件造成。为了定义问题，网管必须从路由器或其它网络监看软件，了解带宽的使用，才能真正定义问题。定义问题对于寻求解决之道提供良好的参考。

决定解决策略：当了解问题所在后，接下来就是要决定解决策略了。其实要进行带宽管理不一定全通过路由器的配置进行。对于需要管理的应用或使用者，是限制还是禁止？进行限制的时间是何时？是否一体应用于所有的使用者，还是特别的使用者。网管必需考虑实际情况，决定整体解决策略。

了解关注应用的网络运作：接下来需针对需要进行管理的题目，了解其网络运作情况，例如应用程序名称、通讯端口、服务主机 IP、传输文件扩展名等。常见的应用，很容易在网络上或论坛中找到详细的工作原理，及对应的管制之道。如果是不常见的应用，则必须使用路由器的监控功能或网络监控软件，了解相关的信息。

决定管制方式：当了解需要管制对象的运作原理后，即可很容易地决定管制的方式。常见的以 IP、通讯端口、内容、文件名、时间、及 WAN 端指定的方式，都可应用，或者混合使用。网络论坛上也可找到相关的信息，有些管理方法比其它的方式更为简单有效，最好作些研究再进行处理。

寻找路由器上相关配置：最后就是落实在路由器的配置上。网管必须仔细阅读路由器的产品说明书，并找出需要的设定实际在配置画面上进行设定。

进行测试：做完配置后，记得要进行实际的测试，观察相关设定是否生效。许多情况下，往往因为忘记存储或是应用的 IP 或通讯端口可以改变，导致预期的管制或管理效果并没有作用。所以做完配置后，务必要进行测试，确定达到预期的效果。否则仍需要再找寻其它解决之道。

接着，我们下面以二个案例，说明几种常见的带宽管理及管制设定：

案例一 限定时间上网

有一所学校，在上计算机课程时，不希望学生因上网分心，所以希望在上课时间禁止学生上网，而下课及其它时间则不加限制。因为主要的限制为时间，而希望阻绝所有的上网行为，因此我们可通过禁止所有通讯端口服务来达到这个目的。因此，设定重点为：

管制动作：禁止

服务端口：所有端口[TCP&UDP/1~65535]

来源接口：局域网

来源端口：任何的

目的 IP 地址：任何的

时间管制：从周一到周五的早上 8 点到下午 6 点。

作完设定后，按存储，就可达到上课时间管制学生上网的目的了。

案例二 网页以外的服务都禁止

某间公司由于工作需要，上班时间只允许员工访问网页，其它的上网动作都不允许。由于网页的传送是通过 TCP/80 端口传送，因此我们可以通过只允许 TCP/80 端口传送来达到这个功能。设定的方式如下：

首先比照前例，新增加一条规则禁止所有的封包通过防火墙，也就是说禁止上网，就是

管制动作： 禁止

服务埠： 所有端口[TCP&UDP/1~65535]

来源接口： 局域网

来源埠： 任何的

目的 IP 地址： 任何的

时间管制： 从周一到周五的早上 9 点到下午 6 点

然后再新增加一条：允许 TCP/80 埠的封包通过。也就是说：

管制动作：允许

服务埠：HTTP[TCP/80]

来源界面：任何的

来源 IP 地址：任何的

目的 IP 地址：任何的

管制时间：从早上 9 点到下午 6 点

最后点击确定完成此设置。

这样就可以实现只能访问网页的这个功能了。设定完后，在“规则”页面要注意的是：由

于规则是从上向下执行的，所以要把禁止连接网络的规则放在上，再把打开 TCP/80 端口规则放到下面，才能达到预期的效果。当然我们也可以通过相同的设定，通过开放电子邮件发送及收信相关的端口，来允许电子邮件服务的通过。

小结

由于面临的情况不一,因此带宽管理的工作相对显得较为困难,需要网管对于网络技术有较深的了解及经验。有经验的网管可以简单地以一个配置,就达到一个没有经验的网管以多重配置的效果。侠诺路由器也一直朝着简化配置,又能达到强大的效果的方向,积累各式的带宽管理功能;侠诺的讨论区及技术支持也乐意提供针对不同问题的建议给用户。带宽管理是现代网管一门值得深入的课题!