



Qno 俠諾中小企业宽带接入解决方案

● 背景介绍

今日互联网的发展带动了企业信息化的发展。现代企业透过互联网宽带的接入,支持信息的收集、传送、加工和汇总等等工作。企业宽带接入必须满足企业对网络的几个重要的需求,包括 Web 服务、邮件服务、远程接入、远程的办公自动化系统及文件和打印服务共享等。同时,还得保证网络服务的不断与稳定的需求。由于外在攻击的存在,宽带接入也必须避免病毒的危害及不受攻击等网络安全的需要。最后则为对内网的管理,对不同上网用户需要做一定的限制,分配不同权限的设置,以优化带宽的利用。

对于中小型企业而言,利用互联网无疑是一个可以发挥以小对大、以慢打快的竞争利器。但对于资源相较有限的中小企业,如何能对宽带接入作较好的规划,可以满足现有的使用及经费需求,又能因应未来成长的空间,是一个值得思考的问题。本方案以带机量在 120 以下的中小企业,需要稳定的带宽接入方便员工连接互联网,整体对外带宽在 200Mbps 的情况下进行规划时需要注意要点的说明。

● 应用特性

对于一般的中小企业用户,对于宽带接入希望能达到以下的要求特性:

- 访问互联网,实现局域网 Web 服务、邮件等服务的要求;
- 广域网带宽利用优化;
- 提供高性能高稳定的网络环境;
- 网络不受攻击以及病毒的防制;
- 对不同部门或者个人对上网服务有不同的要求的人设定不同上网权限;
- 限制少部份用户占用带宽影响一般用户上网;
- 无需太多网络技术能力即能管理,不占用网管太多时间;
- 需要的投资费用能控制在一定的水平之下。

而较为特别的需求则为:

- 不同地点局域网络能透过互联网安全的互相连通;
- 考虑企业的网络对不同部门实现静态 IP 分配与动态 IP 分配的方式相结合方便管理;
- 可随着企业成长因应未来的发展。

简而言之，中小企业用户相对数量较少，对于宽带的要求较简单，但相对的对于管理、建置费用、及未来网络的成长性较为注重。

● 组网方案特性

中小企业信息点一般在 120 个以下，接入信息点（各部门 PC 机的接入）虽然不是很多，但是相对地对于建置费用及管理简易度的要求较高。也就是说，要保证整个网络高效，稳定，同时中小企业在构建信息化网络方案应根据预算限制、网管能力、及网络发展扩充需求等打造符合自身需求的解决方案。

根据以上的要求，我们可以选择使用 Qno 侠诺科技的 QVM100、QVM330 以及 QVM660 VPN 防火墙网络带宽管理路由器作为宽带接入的路由器，建置宽带接入的方案。中小企业可依预算需求选择适当的机型，这些机型在管理上都十分简易，而且可以满足企业未来成长的需要。



图：QVM100 是侠诺面向中小型企业或分支机构网路宽带接入及 VPN 联机双功设计，入门级 VPN 闸道产品。可提供企业需要的多 WAN 接入、VPN、防火墙、负载均衡、线路备援、QoS 带宽管理及路由功能。采用高效网路专用处理器，封包处理稳定性佳。



图：QVM330 是侠诺面向中型企业或企业分支机构网路宽带接入及 VPN 联机双功设计，多功能 VPN 闸道产品。可提供企业需要的多 WAN 接入、VPN、防火墙、负载均衡、线路备援、QoS 带宽管理及路由功能。采用高效 Intel IXP 266 主频处理器，双向转发速率 100Mbps，可支持 10,000 个联机数，封包处理快速稳定。



图:QVM660 是侠诺面向中小型企业或大企业分支机构网路宽带接入及 VPN 联机双功设计, 高阶多功能 VPN 闸道产品。可提供企业需要的多 WAN 接入、VPN、防火墙、负载均衡、线路备援、QoS 带宽管理及路由功能。采用高效 Intel IXP 533 主频处理器、搭配侠诺历经验证的智能软件, 双向转发速率 200Mbps, 可支持 100,000 个联机数, 最大带机量 500 台, 封包处理快速稳定。内建高规格 64MB 大容量内存, 长时间高负载运作稳定可靠。

以上三个产品特性对比表如下:

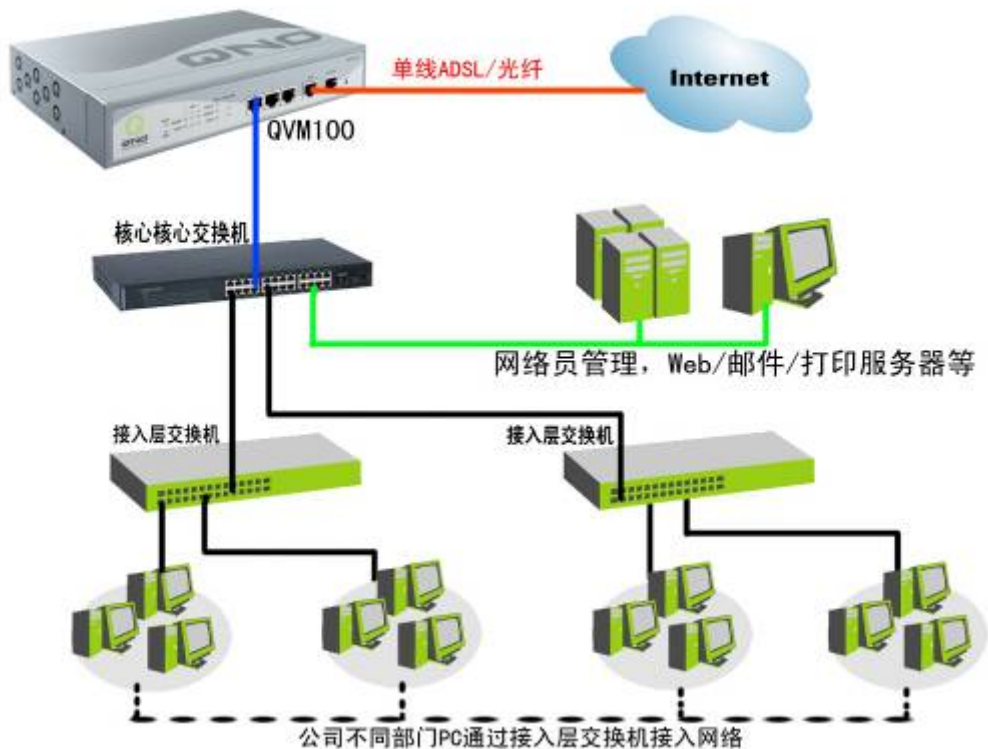
产品型号	QVM100	QVM330	QVM660
CPU 处理器	网络专用处理器	Intel IXP425 266MHz RISC	Intel IXP425 533MHz RISC
Flash 快闪	8MB(64Mbit)	8MB(64Mbit)	16MB(128Mbit)
DRAM 内存	32MB(256Mbit)	32MB(256Mbit)	64MB(512Mbit)
广域网 WAN 端口	1~2	1~2	2~4
可 设 定 的 DMZ/WAN 端口	-1 (WAN4/DMZ)	-1 (WAN4/DMZ)	-
局域网 LAN 端口	11~13	11~13	7~13
非军事区 DMZ 端口	1	1	1
联机数 Sessions	5,000	10,000	100,000
防火墙效能	双向转发 200Mbps	双向转发 200Mbps	双向转发 200Mbps

- 网络带宽接入方式:

1. 采用单线上网, 单独通过运营商 (电信, 网通等) 的 ADSL 或者光纤接入互联网

本方案较为简单, 一般适合企业上网人数不太多, 对上网服务要求不太高的情况下使用, QVM100 接单条广域网线路, 下接核心交换机, 核心交换机下接接入层交换机连接不同部门 PC 机, 对内通过路由器管理设置联机限制或者 QoS 带宽管理 (限制用户最大带宽), 避免少数用户 Bt 下载以及其它大量下载占用带宽, 还可以设定上网时间以及规则, 更加有效利用带宽。将来带宽需要扩充, 则可启用第二个 WAN 口, 增加带宽。Web 服务器、邮件服务器等连接到主交换机上提供相关服务, QVM100 还支持多方式的 IPSec VPN 连接, 同时还拥有 Qno 特有的 SmartLink VPN 客户端功能, 相比其它路由器可以方便快捷的建立安全的 VPN 连接, 方便用户以后需要实现 VPN 连接升级应用。

具体拓扑结构如下图。



如上图：QVM100 单线 ADSL/光纤，下接交换机，服务器连接交换机以提供相关服务，各 PC 机连接交换机再通过 QVM100 实现数据转发连接互联网。

2. 采用双线上网，通过相同的运营商（电信，网通等）ADSL 或者光纤接入互联网

本方案一般适合企业上网人数相对较多，对上网服务要求较高的情况下使用，QVM330 对外接两条广域网线路，下接核心交换机，核心交换机下接接入层交换机连接不同部门 PC 机，对内通过路由器管理设置联机限制或者 QoS 带宽管理（限制用户最大带宽），避免少数用户 Bt 下载以及其它大量下载占用带宽，还可以设定上网时间以及规则，防止不正当的带宽使用。对外通过路由器管理设置 IP 均衡模式，将内部不同用户依 IP 分配到不同 WAN 端口，实现负载均衡的优化转发功能。Web 服务器、邮件服务器等连接到主交换机上提供相关服务。

QVM330 还支持 IPSec VPN 连接以及 PPTP 拨号连接，同时还拥有 Qno 特有的 SmartLink VPN 客户端功能，相比其它路由器可以方便快捷的建立安全的 VPN 连接，方便用户以后需要实现 VPN 连接升级应用。

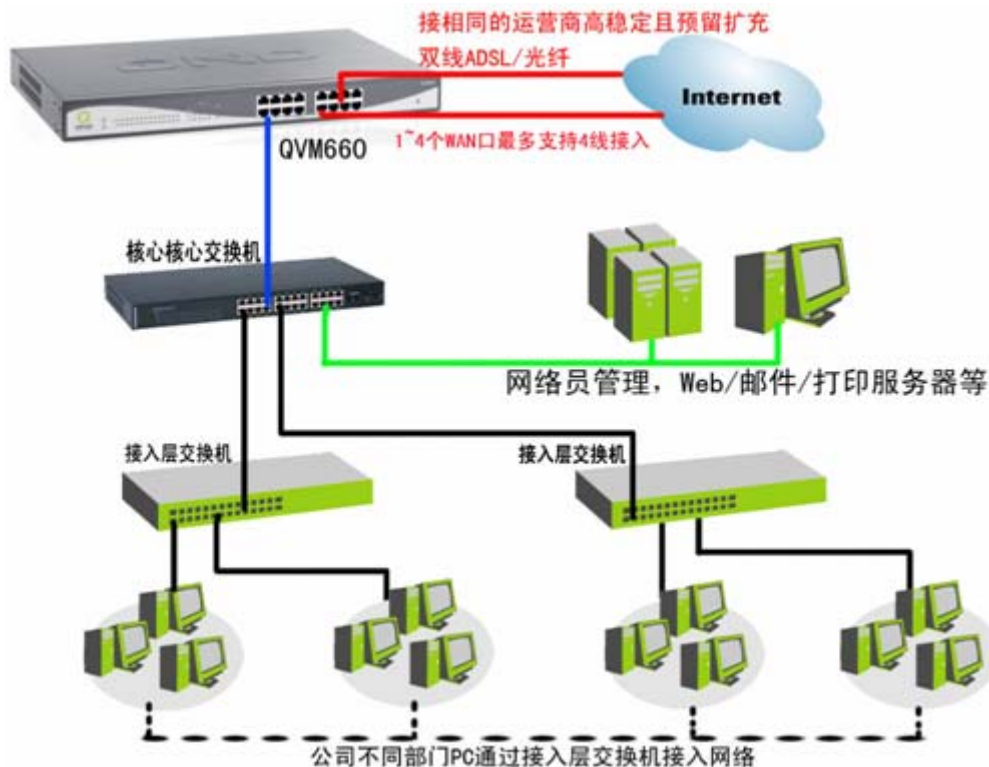
具体拓扑结构如图。



如上图：QVM330 双线接相同运营商 ADSL/光纤，下接交换机，服务器连接交换机以提供相关服务，各 PC 机连接交换机再通过 QVM330 的 IP 均衡模式功能实现数据转发连接互联网。

在企业成本投入比较大的情况下，而且对稳定要求比较高的情况下采用 QVM660，此路由器共有 4 个 WAN 口和支持更多的上网联机数，方便企业以后发展要求，预留 WAN 口将来企业规模扩充的时使用，增加带宽和添加机器。QVM660 对外接两条广域网线路，下接核心交换机，核心交换机下接接入层交换机连接不同部门 PC 机，对内通过路由器管理设置联机限制或者 QoS 带宽管理（限制用户最大带宽），避免少数用户 Bt 下载及其它大量下载占用带宽，还可以设定上网时间以及规则，防止不正当的带宽使用。对外通过路由器管理设置 IP 均衡模式，将内部不同用户依 IP 分配到不同 WAN 端口，实现负载均衡的优化转发功能。Web 服务器、邮件服务器等连接到主交换机上提供相关服务。

QVM660 还支持 IPSec VPN 连接以及 PPTP 拨号连接，同时还拥有 Qno 特有的 SmartLink VPN 客户端与服务端功能，相比其它路由器可以方便快捷的建立安全的 VPN 连接，方便用户以后需要实现 VPN 连接升级应用。



如上图：QVM660 双线接相同运营商 ADSL/光纤，下接交换机，服务器连接交换机以提供相关服务，各 PC 机连接交换机再通过 QVM660 的 IP 均衡模式功能实现数据转发连接互联网。

3. 采用多线上网，通过不同的运营商（电信，网通等）ADSL 或者光纤接入互联网,下接交换机

本方案一般适合企业上网人数相对较多，对上网服务要求较高的情况下使用，QVM330 对外接多条广域网线路，下接核心交换机，核心交换机下接接入层交换机连接不同部门 PC 机，对内通过路由器管理设置联机限制或者 QoS 带宽管理（限制用户最大带宽），避免少数用户 Bt 下载以及其它大量下载占用带宽，还可以设定上网时间以及规则，防止不正当的带宽使用。对外通过路由器管理设置策略路由模式，路由器可依网络包目的判断适当的 WAN 端口，保证电信走电信、网通走网通，确保联机反应快速，实现数据的优化转发功能。Web 服务器、邮件服务器等连接到主交换机上提供相关服务。

QVM330 还支持 IPSec VPN 连接以及 PPTP 拨号连接，同时还拥有 Qno 特有的 SmartLink VPN 客户端功能，相比其它路由器可以方便快捷的建立安全的 VPN 连接，方便用户以后需要实现 VPN 连接升级应用。

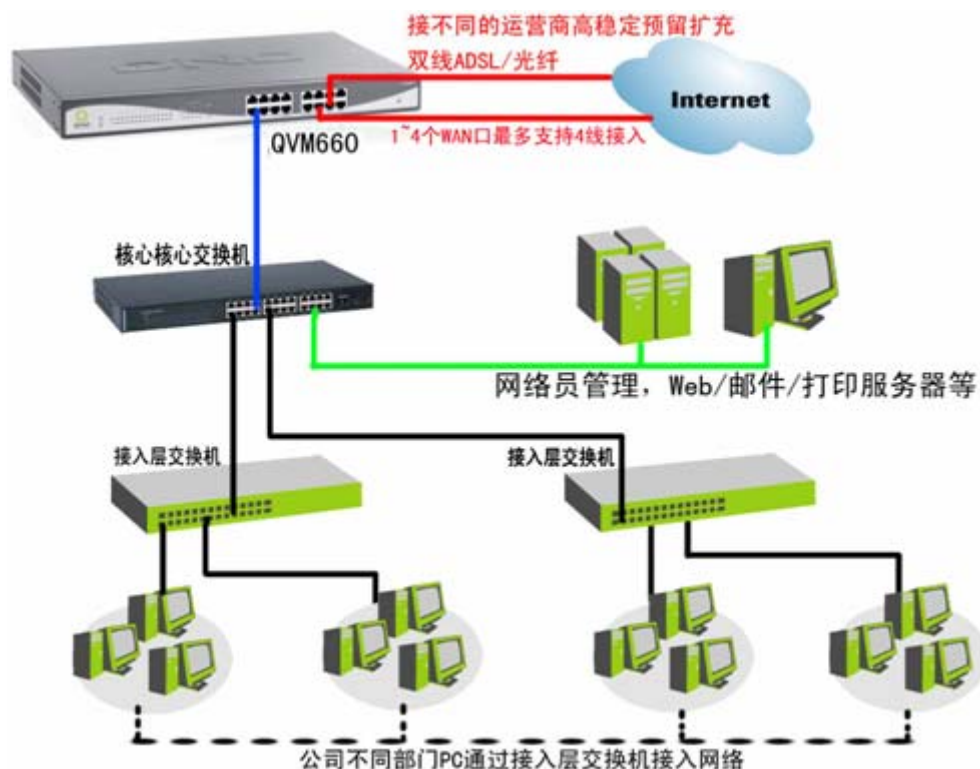
具体拓扑结构如图。



如上图：QVM330 双线接不同运营商 ADSL/光纤，下接交换机，服务器连接交换机以提供相关服务，各 PC 机连接交换机再通过 QVM330 的策略路由模式功能实现数据转发连接互联网。

在企业成本投入比较大的情况下，而且对稳定要求比较高的情况下采用 QVM660，此路由器共有 4 个 WAN 口和支持更多的上网联机数，方便企业以后发展要求，预留 WAN 口将来企业规模扩充的时使用，增加带宽和添加机器。QVM660 对外接多条广域网线路，下接核心交换机，核心交换机下接接入层交换机连接不同部门 PC 机，对内通过路由器管理设置联机限制或者 QoS 带宽管理（限制用户最大带宽），避免少数用户 Bt 下载以及其它大量下载占用带宽，还可以设定上网时间以及规则，防止不正当的带宽使用。对外通过路由器管理设置策略路由模式，路由器可依网络包目的判断适当的 WAN 端口，保证电信走电信、网通走网通，确保联机反应快速，实现数据的优化转发功能。Web 服务器、邮件服务器等连接到主交换机上提供相关服务，QVM660 还支持 IPSec VPN 连接以及 PPTP 拨号连接，同时还拥有 Qno 特有的 SmartLink VPN 客户端与服务端功能，相比其它路由器可以方便快捷的建立安全的 VPN 连接，方便用户以后需要实现 VPN 连接升级应用。

具体拓扑结构如图。



如上图：QVM660 双线接相同运营商 ADSL/光纤，下接交换机，服务器连接交换机以提供相关服务，各 PC 机连接交换机再通过 QVM660 的 IP 均衡模式功能实现数据转发连接互联网。

● 其它设置

1、 设定访问存取规则

对于有些企业而言，不是所有的电脑连入了网络都需要提供上网服务的，比如一个公司，有一台电脑专门只做文字处理，根本不需要提供上网服务，还有销售部门的几台电脑在上班时间 08:00~17:30 不提供上网服务，以免影响工作，对于这种情况我们可以在防火墙配置里的访问存取规则设定来阻挡这几台电脑的在特定要求的情况下不可以上网，管理人员可以通过类似的设定达到对局域网内的电脑实施阻挡的目的，首先添加新的管制存取规则，具体设置如下，拥有 192.168.1.4 的这个电脑设置在任何时间是禁止上网的，同样可以把销售部门的 4 台电脑的 IP 192.168.1.5~8 地址通过类似的方法再设定时间的管制使这 4 台电脑在星期一到星期五的 08:00~17:30 这段时间不可以上网。

存取服务规则设定

管制动作:

服务端口:

日志:

来源接口:

来源IP地址:

目的IP地址:

时间管制设定

此存取规则 : 到 : (时间表示:24小时制)

每天 周日 周一 周二 周三 周四 周五 周六

图：添加存取规则画面

添加了这 5 个规则之后就可以看到网络存取规则表里显示这几项规则，这样就达到了网管人员预期的目的。

跳到 / 2 页 每页显示的字段 下一页 >>

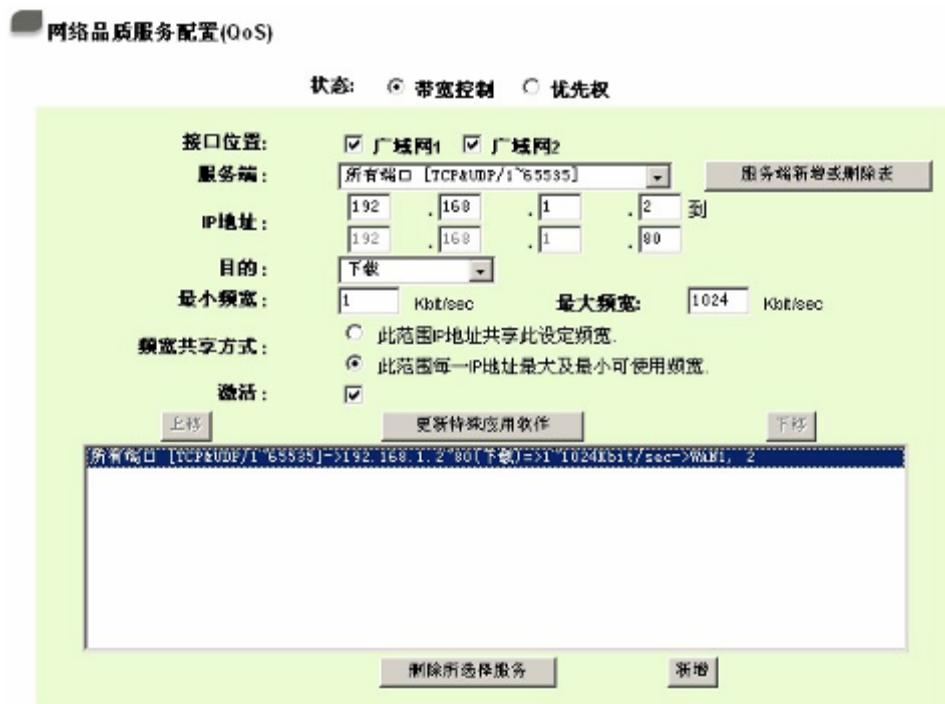
优先级	激活	管制动作	服务端口	未通端口	来源位置	目的位置	管制时间	日	删除
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	*	192.168.1.8 ~ 192.168.1.8	任何的	8:0 ~ 17:30	周一, 周二, 周三, 周四, 周五,	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	*	192.168.1.7 ~ 192.168.1.7	任何的	8:0 ~ 17:30	周一, 周二, 周三, 周四, 周五,	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="text" value="3"/>	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	*	192.168.1.6 ~ 192.168.1.6	任何的	8:0 ~ 17:30	周一, 周二, 周三, 周四, 周五,	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="text" value="4"/>	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	*	192.168.1.6 ~ 192.168.1.6	任何的	8:0 ~ 17:30	周一, 周二, 周三, 周四, 周五,	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="text" value="5"/>	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	*	192.168.1.4 ~ 192.168.1.4	任何的	所有时间		<input type="button" value="编辑"/> <input type="button" value="删除"/>

图：网络存取规则表画面

2、防止 BT 及电影等大量下载占用带宽 (QoS)

限制大量占用带宽：现在企业的环境中，BT，kugoo，电驴，迅雷等软件的使用，更是线路带宽的杀手，因此，如何保证企业的带宽得到有效的利用，成了各网管人员的当务之急。而使用 Qno 的路由器，可以针对每个区用 QoS（带宽管理）功能，来限制内网每个 IP 或者服务端口的流量，可以把 P2P，迅雷等软件的使用带宽限制到非常小，再也不会因为内网的某台电脑

大量下载而占用比较多的线路带宽。例如我要限制内网 192.168.1.x 段
(192.168.1.2~192.168.1.80) 的每台电脑最大只能使用 2M 的带宽，只需如下设置即可：



图：限制内网 192.168.1.x 段的每台电脑最大只能使用 2M 的带宽的配置。

3、 IP 与 MAC 绑定

有些企业,对不同部门或个人设定了不同的上网权限,可能有的部门以及个人工作比较特殊,没有联入互联网的上网权限,为了避免这些用户去修改 IP 地址逃脱规则的设定而达到上网的目的,我们可以通过 IP/MAC 的绑定功能使得这些用户即使修改了 IP 地址也无法达到上网目的。比如公司有一台专门做文件处理的电脑和销售部门的 4 台电脑是不可以上网的,他们的 IP 地址分别是 192.168.1.4~8 (分别对这 5 个 IP 地址做存取规则的设定,阻止联入互联网),我们通过对 IP/MAC 的绑定后,无任用户改变什么 IP 地址,都是不可以上网的。

具体设定如下。

IP 与 MAC 绑定

显示新加入的IP地址

IP 与 MAC 绑定

静态IP地址设定: 192 . 168 . 1 . 4

添加IP地址相对应MAC地址: 00 - 01 - 0f - 0a - 4e - 5d

名称: 文件处理

激活:

更新区块

192.168.1.4 => 00-01-0f-0a-4e-5d => 文件处理 => 激活
192.168.1.5 => 00-01-02-0f-2e-00 => 销售部门 => 激活
192.168.1.6 => 01-00-0e-05-0d-2e => 销售部门 => 激活
192.168.1.7 => 00-01-05-06-2f-2f => 销售部门 => 激活
192.168.1.8 => 00-05-3e-3d-2a-0a => 销售部门 => 激活

删除所选项对应项目 新增

封锁在对应列表中IP地址错误的MAC地址

封锁不在对应列表中的MAC地址

图：IP/MAC 绑定画面

4、防止攻击

ARP 攻击, DOS 攻击是同样可以影响到企业网络的正常运行, 前者可以让内网电脑不定时的掉线, 后者可以使网络瘫痪。而 Qno 路由器的防火墙功能则可以很好的解决此问题, 提供侦测、阻文件及配置的功能。

防火墙功能:	<input checked="" type="radio"/> 激活	<input type="radio"/> 关闭	
SPI封包主动检测检验功能:	<input checked="" type="radio"/> 激活	<input type="radio"/> 关闭	
DoS检测功能:	<input checked="" type="radio"/> 激活	<input type="radio"/> 关闭	
关闭对外的封包回应:	<input type="radio"/> 激活	<input checked="" type="radio"/> 关闭	
远程配置管理功能:	<input type="radio"/> 激活	<input checked="" type="radio"/> 关闭	Port: <input style="width: 50px;" type="text" value="80"/>
允许Multicast封包穿透格式:	<input type="radio"/> 激活	<input checked="" type="radio"/> 关闭	
防止ARP病毒攻击:	<input type="radio"/> 激活	<input checked="" type="radio"/> 关闭	
MTU:	<input checked="" type="radio"/> 自动	<input type="radio"/> 手动	<input style="width: 50px;" type="text" value="1500"/> bytes

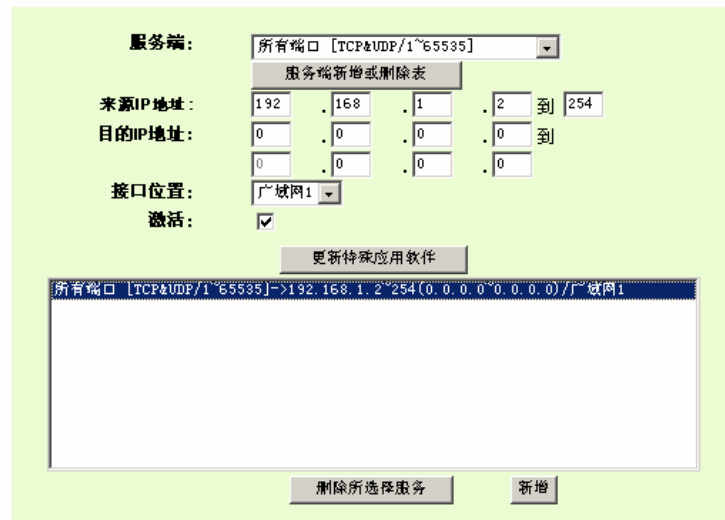
图：FVR420 的防火墙配置画面。

5、路由器线路侦测机制

企业有时候由于 ISP 线路不稳定等原因路由器连接广域网的 ADSL 或光千可能容易出现断线的情况 (路由器多线路连接互联网), 这个时候我们可以通过路由器的线路侦测功能来实现当

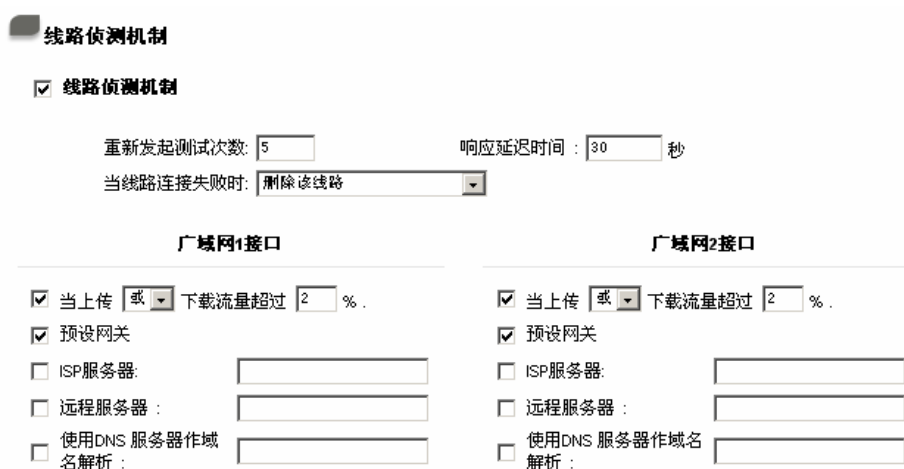
主光纤断网后，路由器侦测到此线路不通，然后连接另外的一条线路来继续提供上网服务，具体配置如下。

首先在双广域网设置栏目选择好负载均衡模式，再到下面设置添加一个规则，保证在光纤运行正常的情况下所有的流量（192.168.1.2~192.168.1.254）都走 WAN1 口，当然，如果有特殊的要求，只对特定的 IP 的做类似的设置，也可以只添加特定的 IP 地址，如下图。



图：添加相应规则画面

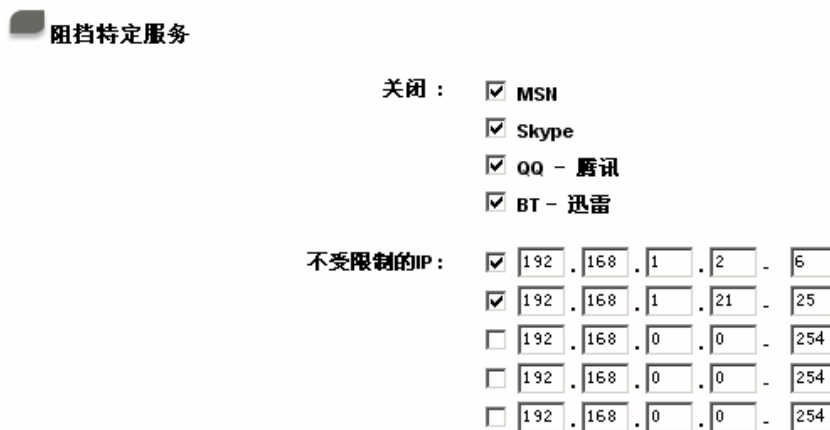
然后通过勾选线路侦测机制，填入相关数据点击确认按钮就可以做到光纤断线由 ADSL 继续运营备份的功能，如下图。



图：线路侦测机制功能设置画面

6、 阻挡特定服务

QVM660 还提供了阻挡特定服务的功能，通过简单的设置就可以阻挡 MSN、Skype、QQ、BT-迅雷这几个特定的服务，减少管理人员通过封锁这些服务的服务器公网 IP，达阻挡的效果的工作量和出错几率，如果你运用了这两款机器的话，需要对内网特定的服务做阻挡设置，可以如下图所示方法来完成你的设定需要。



图：QVM660 挡了 MSN、Skype、QQ、BT-迅雷的服务，但 192.168.1.2~6 和 192.168.21~25 这 10 台机器不受此阻挡，用户可以按照需要做类似的设置，

7、 远程管理

路由器提供了远程管理功能，我们只要开激活路由器的远程管理功能，管理人员不论在任何地点只要有电脑连入互联网，都可以通过路由器的广域网 IP 地址远程登陆路由器对路由器做相关设置，方便了管理人员同时提高了工作效率和减少了工作时间，如图。



图：远程管理激活



● Qno 侠诺方案特点

QVM100/ QVM330/ QVM660 提供强大的路由功能，他们分别同时可支持 5,000/10,000/100,000 个联机(session)数，在中小企业（带机量在 120 台电脑以下的企业）路由器运行处理数据轻松自如。QVM100/ QVM330 提供了 2 个 WAN 口以及 QVM660 提供了 2~4 个 WAN 口，可以提供多线通过相同或者不同的运营商连接互联网实现多需求的接入方式，多 WAN 口支持线路备援功能，在线路不稳定的时候仍然保证网络联机的不间断

QVM100/ QVM330/ QVM660 的高可管理可维护性，环境适应性，长期运行性能稳定可靠的特点可用为中小型企业提供一个可靠，放心的网络环境。提供多种带宽均衡模式方便用户在不同的接入方式情况先选择不同的数据转发机制保证网络的畅通和稳定。侠诺三代电信网通策略路由，可会聚同运营商的线路宽带，做负载均衡控制，让电信走电信、网通走网通，确保联机反应快速，解决中国“南电信北网通”跨网带宽受限的问题，大大提升网络资源运用的灵活性。

存取规则的设定以及 IP/MAC 绑定功能方便对内网电脑设定不同规则达到限制一些电脑的上网情况，有时候一些客户通过修改 IP 地址达到上网目的的，网管人员可以通过对这些电脑的 IP 地址与电脑的物理地址（MAC）绑定在一起防止用户修改 IP 地址来逃脱规则的限制。

对于局域网用户行为监控力度不足，员工有意无意的的行为，比如网络视屏下载，恶意病毒的传播，非常途径上网都有可能给企业带来不可估计的损失，路由器支持固定 分配 IP 地址和动态分配 IP 结合的方法方便用户管理，同时对用户的上网权限做严格限制保证网络正常的运行，同时路由器还提供了日志功能方便管理人员随时查阅日志可以及时发现问题并解决问题来减少内部网络用户的不正当行为。

QoS 管理可限制特定应用或用户的带宽，例如 BT 多绪下载软件，以免影响其它用户的带宽。这可减少企业员工的抱怨，同时保证网络能够正常的运行。

侠诺 QVM 系列产品支持 VPN 功能，对于未来企业建置 VPN 可直接升级，不需要进行额外的投资。

● Qno 侠诺方案的效果

QVM100/ QVM330/ QVM660 的解决方案既能保证安全又容易实施，它能够帮助企业以更稳定的网络模式开展业务，确保了各分部门间通讯畅通。在性能方面，以上方案以及相关型号路由器的内部硬件配置的性能都能满足相关要求。



俠諾科技股份有限公司
Qno Technology Inc.
URL: <http://www.qno.com.tw>

QVM 系列产品强调配置的简易及智能，可解决中小型网管不足的问题，弹性的功能可以针对不同环境来配置，可以达到用户的预期的效果。

以上方案经过 Qno 的多个技术人员和工程师的讨论以及实际应用，无论从架构成本以及企业所需要的功能、目的以及管理上所要达到的要求都能够满足中小型企业客户的需要。