侠诺科技股份有限公司
Qno Technology Inc.
http://www.Qno.cn

Qno 侠诺酒店应用配置案例

Qno 侠诺为新一代宽带接入设备的供货商，主要针对新一代的宽带接入及应用提供解决方案。我们的产品已广泛应用在企业，网吧，小区，酒店等各种行业。谢谢您采用侠诺出品的路由器产品，为了协助您可以更好的利用功能强大的 Qno 侠诺路由器，本文特别针对酒店应用，提供本文件作为进行配置的参考。

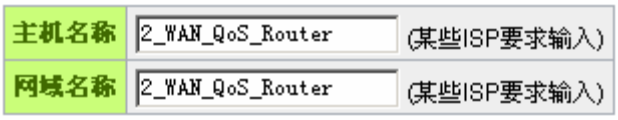
以下针对酒店应用 Qno 侠诺 FVR 系列路由器的五个比较需要注意的项目，加以说明。这四个项目分别为：一、广域网 WAN 口设置；二、线路检测机制；三、DHCP 的设置；四、QoS 带宽管理设置；五、防火墙的设置。

一、WAN 口的设置：

进入路由器设置界面的“网络设置”项目：

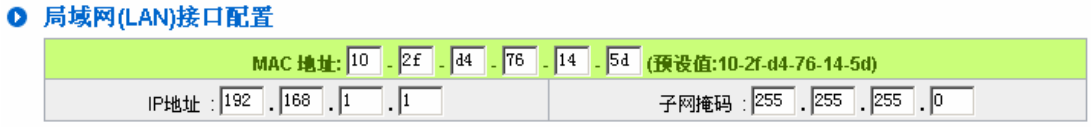
主机名称及网域名称

可输入路由器的名称以及网域名称，于大多数的环境中不需做任何设定即可使用，除非特殊 ISP 需求！

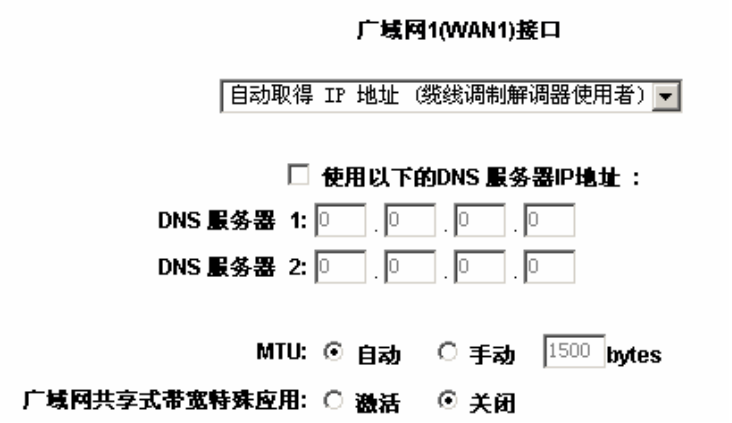


局域网 LAN 接口配置

此为设定路由器的 LAN 端内部网络的 IP 地址，系统默认为 192.168.1.1，子网掩码为 255.255.255.0，现在 FVR360v/420v 可以支持到 Class B，您可以依照实际网络架构做改动！



在该页面下方有“联线类型配置”功能：



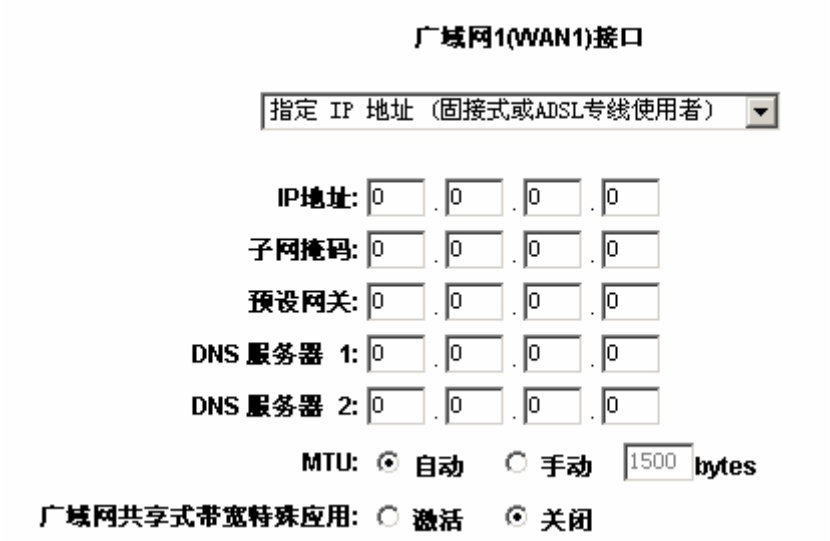
酒店应用依据线路的不同，可采用＂自动取得 IP 地址＂、＂指定 IP 地址＂、＂PPPoE 设定＂等常见的配置。以下分别说明之。

1. **自动取得 IP 地址：**当运营商分配给的是自动获取 IP 的联线方式，可以使用这种方式。

使用以下的 DNS 服务器 IP 地址： 不激活此项目时，则直接采用运营商分配的名称解析服务器 IP 地址。

DNS 服务器： 输入您的 ISP 所提供的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

2. **指定 IP 地址：**当运营商分配固定 IP 时，则使用这种联线方式：



IP 地址： 输入您的 ISP 所核发的可使用固定 IP 位置的其中一个。

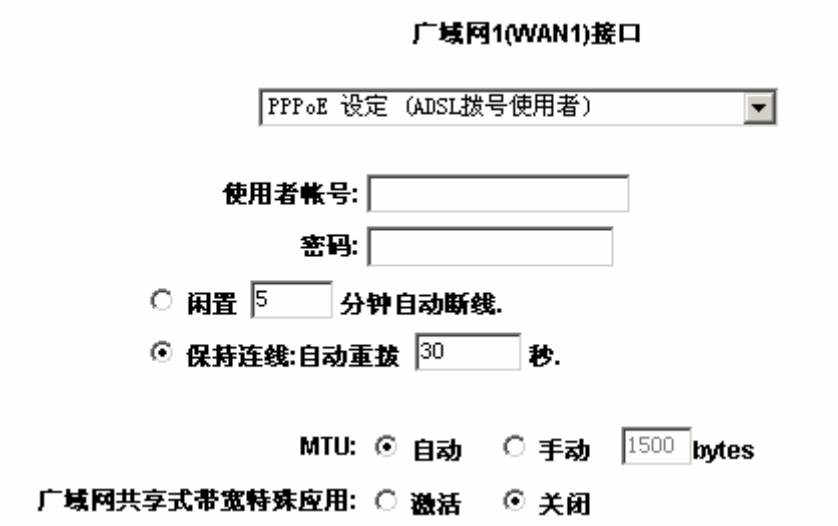
子网掩码： 输入您的 ISP 所核发的可使用固定 IP 位置的子网掩码，如：

发放 8 个固定 IP 位置：255.255.255.248
发放 16 个固定 IP 位置：255.255.255.240

预设网关： 输入您的 ISP 所核发的可使用固定 IP 地址的预设网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

DNS 服务器： 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少可以填入一组，最多可填二组。

3. **PPPoE 设定：**如果您的线路使用 ADSL 等拨号方式上网，则可以使用这种方式。



使用者名称： 输入您的 ISP 所核发的使用者名称。

密码： 输入您的 ISP 所核发的使用密码。

闲置断线： 此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，会自动向预设的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无封包传送的自动离线时间预设为 5 分钟，你可以自行输入所需要的自动离线等待时间。

保持连线： 此功能能够让您的 PPPoE 拨接连线能够断线自动重拨，而且可以自行设定重新拨接的时间，默认值为 30 秒。

MTU： MTU（最大传输单元），此为 ADSL 线路每笔数据包的最大字节。一般情况下此设置为自动即可。

二、线路检测机制

当酒店接了两条运营商线路时，则请务必设置好此功能，如果您只使用了一条线路，则把线路检测功能关闭，即把“线路侦测机制”前面的复选框的勾去掉。

点击“流量管理”，进入“线路检测机制”：

线路检测的手段是 ping 填入的 IP 地址和解析域名，即 ping 预设网关、ISP 服务器、远程服务器和解析所填入的域名，四者当中只要有一个能 ping 通，路由器则认为该线路是通的，只有全部都不通的时候，路由器才会认为该线路已经不通。所以预设网关、ISP 服务器、远程服务器、域名一定要填入可靠的能 ping 通的地址，避免路由器误判线路的情况发生。

下面就设置参数详细说明下：

重新发起检测次数： 当线路测试不成功时，重试线路检测动作的次数。

响应延迟时间： 每隔多少时间就执行一次线路侦测。

当线路检测失败时： 1.只选择存储到日志记录文件：当线路侦测失败时，不作任何动

	作，系统仍然依照拥有此线路作负载均衡，但会记录至系统日志中。2.删除该线路：当线路侦测失败时，移去此线路不再作负载均衡，并记录至系统日志中，该选项为系统默认。
当上传和/或下载超过2%时：	如果在网络非常繁忙的时候做线路侦测是没有意义的。我们在当下载或者上传的流量超过设定带宽的 2%时，不做线路检测。
预设网关：	连接默认网关做线路检测动作。
ISP 服务器：	连接 ISP 主机做 NSD 动作，在此可填入一个可靠的能 ping 通的 IP 地址。
远程服务器：	指定一个第三方主机连接作线路检测动作，在此可填入一个可靠的能 ping 通的 IP 地址。
使用 DNS 服务器作域名解析：	指定一个被解析的域名做线路检测动作，在此处可使用页面中默认的域名。

三、DHCP 的设置

鉴于酒店的特殊环境，DHCP 自动分配 IP 地址显得尤为重要。点击 DHCP 配置进入设置界面，如下图：

在酒店的实际设置中，我们应该把租约时间改为 120 分，以因应酒店客人频繁的上网及离开，有效 IP 地址的应用。发放的 IP 地址范围应视酒店房间数，应该尽量修改得比较大，如下图：

在 DHCP 设置页面中还有：IP 和 MAC 地址绑定，DNS 域名解析，WINS 解析功能。

DNS 域名解析： 在此处填入 ISP 提供的 DNS 地址，则内网 PC 的 DNS 地址设置为自动获取时，可获取该 DNS 地址。

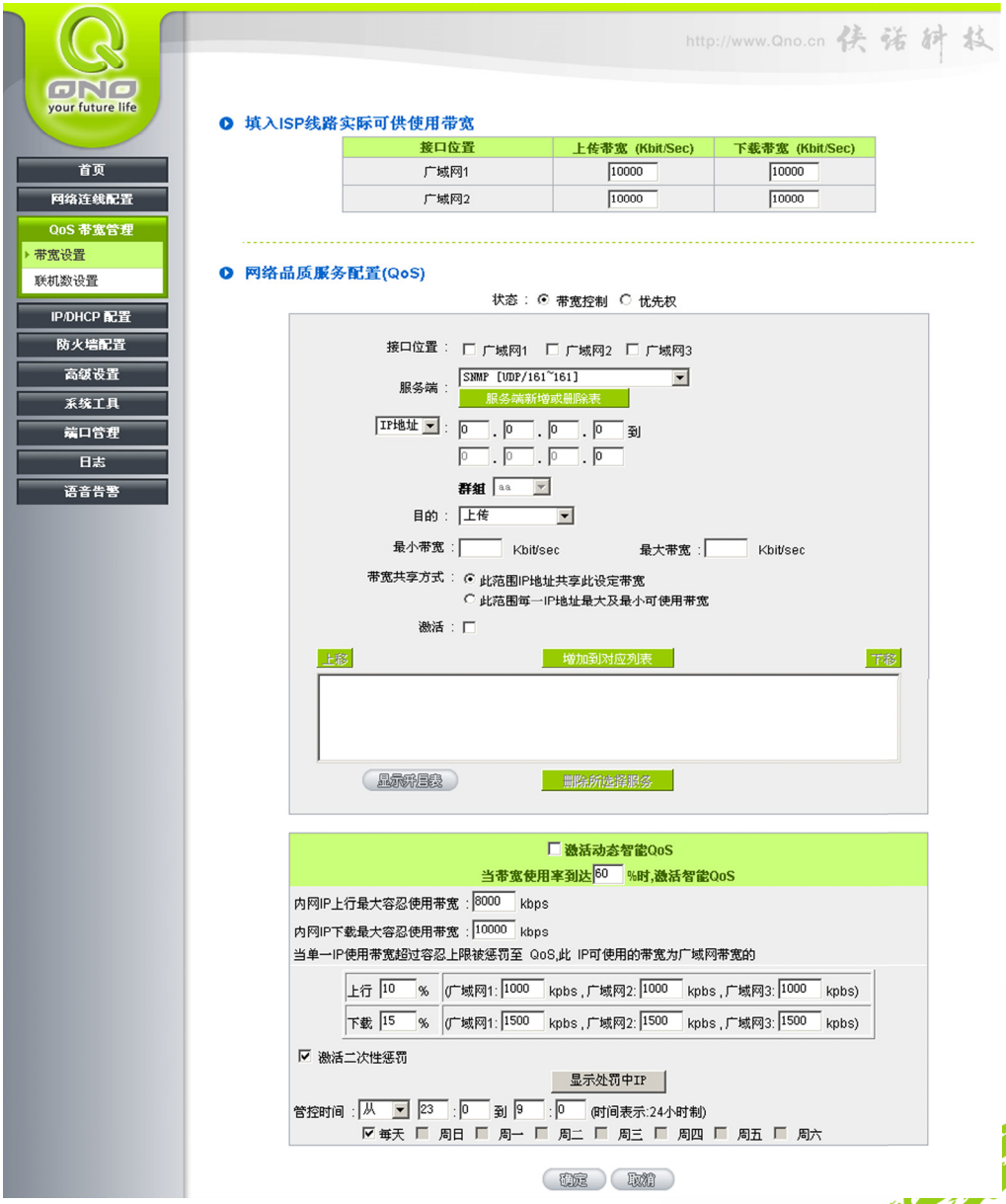
WINS 解析： 在此处填入 WINS 地址，则内网 PC 可以自动获取 WINS 地址。

四、QoS 带宽管理设置

带宽管理意指 QoS(Quality of Service)，其功能为用来满足各种应用程序各种不同网络环境应用的带宽管理管理需求，以提供稳定，可靠的数据传输服务。按照应用程序以及网络管理人员对酒店的实际需求来设置使用 QoS，让网络带宽在特定的网络环境更有效率的使用。

在酒店的环境中，为防止房客使用 BT 或者迅雷软件占用大量带宽从而造成其它正常上网的房客网速非常慢，我们可以把带宽平均分配给每个 IP 地址，让每个上网的客人都能享用到带宽。在少数人上网时，每个人分配的带宽就多，否则就较少，但都可保证可以上网。

点击 “QoS 带宽管理”，进入“带宽设置”就可以打开 QOS 的设置界面了。



填入ISP线路实际可供使用带宽

接口位置	上传带宽 (Kbit/Sec)	下载带宽 (Kbit/Sec)
广域网1	10000	10000
广域网2	10000	10000

填入 ISP 线路实际可供使用频宽　此广域网 1，广域网 2 的带宽请填入您所申请的带宽。

网络品质服务配置（QoS）：

接口位置：　选择 QOS 功能在哪条广域网口执行，可以 2 个广域网口都选择，也可以选择其中一个。

服务端： 选择要设置带宽的服务端口，如果是所有的服务请选择“所有服务[TCP&UDP/1-65535]”。

IP 地址： 填入需要管理的带宽用户，例如：192.168.0.1 To 254 是指从 192.168.0.1 到 192.168.0.254 的所有 IP 地址。

目的： 指定要设置带宽的类型。这里有 4 种选择：“下载带宽” **“**上传带宽” “ 内网对服务器的上传带宽**”**这是从内网的电脑对内网服务器上传的带宽； **“**局域网内的下载带宽**”**这是从内网服务器下载文件到电脑的带宽；

最小频宽：控制的最小带宽，单位为 Kbit/sec。

最大频宽：控制的最小带宽，单位为 Kbit/sec。

频宽共享方式： 带宽共享方式。这里有两种可以选择：“此范围 IP 地址共享此设定频宽： ”选择此项表示您设定的 IP 范围内的所有 PC 共享这一设定的带宽。“此范围每一 IP 地址最大及最小可使用频宽”选择此项表示您设定的 IP 范围内的每一台 PC 独享这一设定的带宽。

激活： 激活设置。

上移和下移： 由于 QOS 的每条规则执行的优先级为由列表的最下面那条 QOS 规则往上执行，也就是越后面的规则越优先执行，所以就可以自行调整每条规则的优先顺序。

更新特殊应用软件： 您可以修改所设定的规则后，点击此按钮即可。

删除所选择服务： 删除您所设定的规则。

新增： 您可以增加新的设定规则。

显示开启表： 显示所有的设置。

下面我们通过一个实例来设置 FVR360v/420v 路由器的 QoS 功能。现在一个酒店需要限定每个 IP 为下载流量不能超过 100kbytes，上传不能超过 15kbytes。则我们可以如下设置：（注：1kbytes=8kbits，这里设置的单位是以 kbits 来计算的。并且在填入来源 IP 地址的时候不要把路由器的 LAN IP 地址填进去，例如本例当中假设路由器的 LAN IP 为 192.168.1.1，那么该 IP 地址不要被包含在来源 IP 地址的范围内。）

- **联机数管控**

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、迅雷、emule 等会造成大量发出联机数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，也可以达到抑制做用。

1. 联机管制设定以及时间管制：

关闭： 不使用此联机数管控功能。

每一内网 IP 最大对外联机数限制不可超过： 此选项为限制每一台内网的计算机最大可建立的对外联机数，当用户计算机使用联机数到达此限制值时，要建立新的联机必须等到之前的联机结束后才能再建立。例如，当用户使用 BT 或 P2P 等下载时且联机数超过此设定值后，当用户又要再开其它服务时会无法使用，除非将使用中的 BT 或 P2P 软件关闭。

当单一个 IP 联机数到达：

阻挡此 IP 新联机 5 **分钟：**此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户在 5 分钟之内将不能再增加新联机，就算旧联机已经结束，也必须等到设定时间过后才能再建立新的联机。

封锁此 IP 所有联机 5 **分钟：**此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户正在使用的所有联机都将被清除，且在 5 分钟之内将不能建立任何联机(不能上网)，必须等到设定时间过后才能再建立新的联机。

时间管制设定： 选择“**全部**”，此 QoS 设定在所有时间都有效果，如果选择“**从___:___到___:___**”填入时间段（24 小时记时制，例如 19：00 到 24：00），以及勾选“**每天/周日/周一/周二/周三/周四/周五/周六**”的某一天或者几天，其 QoS 设定在勾选的那几天的设定的特定时间段有效。

确定： 按下此按钮“**确认**”即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，但是必须于确认储存动作之前才会有效。

2. 不受限制的服务或 IP 地址

当有的用户以及 IP（比如公司管理层等），或者是特定需要不受限制的服务（公司财务数据的传输，邮件的传输等），管理人员可以设定这些服务或者 IP 不受联机管制。

服务端： 选择不受限制的服务端口。

来源 IP 地址： 输入不受限制的 IP 地址范围，或者选择不受限制的 IP 群组。

激活： 启用此规则。

增加到对应列表： 将添加的规则增加到列表中。

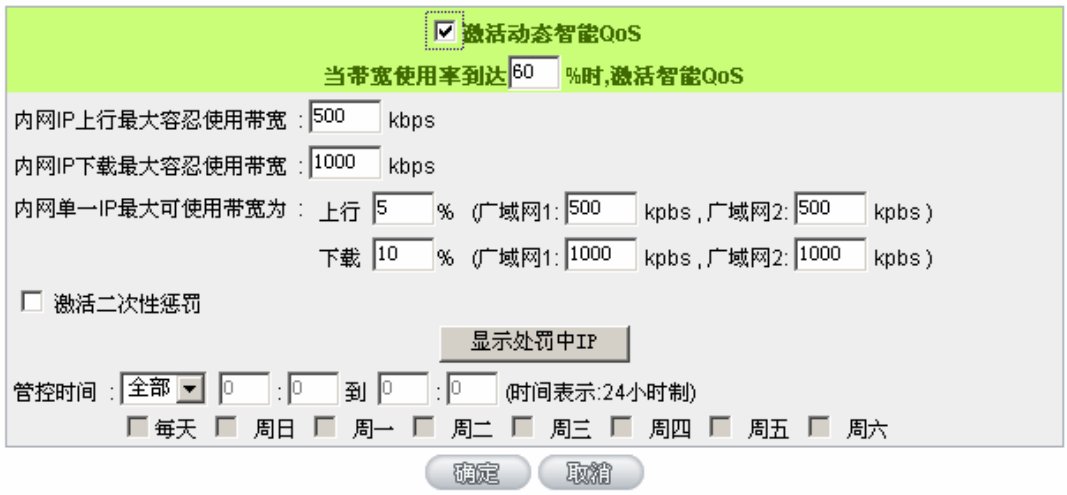
删除所选服务： 选择列表中中的规则，删除选中的规则。

确定： 按下此按钮“**确认**”即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，但是必须于确认储存动作之前才会有效。

- **智能带宽管理**

无需网管进行配置的智能型带宽管理 Smart QoS 功能，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。



激活动态智能 QoS: 勾选激活动态智能 QoS。

当带宽使用率到达 60 %时，激活智能 QoS 当带宽使用率到达实际带宽的一个%比时，将启动活智能 QoS，您可输入需要的数值，系统默认是 60%。

内网 IP 上行最大容忍使用带宽 ： 填入内网 IP 上行最大容忍使用带宽。

内网 IP 下载最大容忍使用带宽 ： 填入内网 IP 下载最大容忍使用带宽。

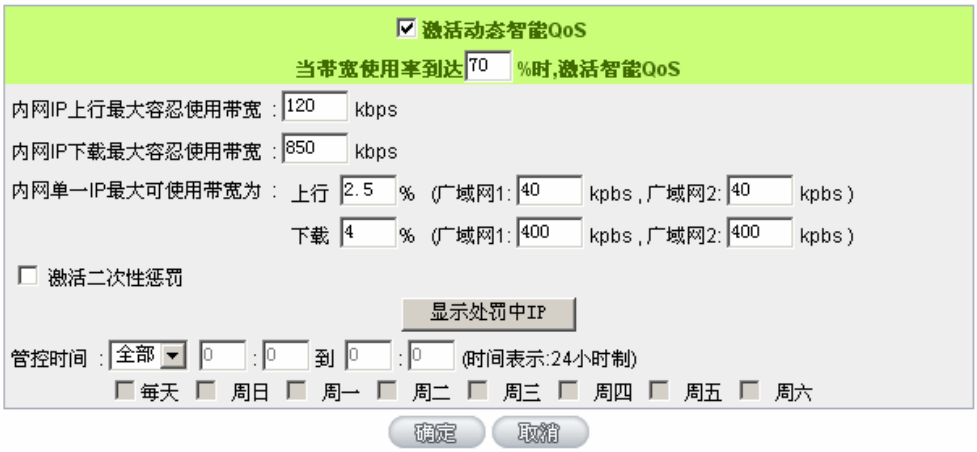
内网单一 IP 使用带宽超过容忍上限被惩罚至 QoS,此 IP 可使用的带宽为广域网带宽的上行 10 %，下载 10 %： 填入内网单一 IP 上传和下载超过容忍上限，就实行惩罚措施，限制这单一 IP 地址上行和下载值在总带宽的%几，范围在 1%~90%

激活二次性惩罚： 点击勾选“激活二次性惩罚：”后，路由器内部设置好二次惩罚条件，当内部网络上网用户上网过程中的上传与下载达到内部条件将执行二次惩罚。

显示处罚中的 IP： 点击后，在弹出的对话框中将会显示路由器罚中的 IP，上行限制中，下载限制中以及二次惩罚信息。

管制时间： 选择“**全部**”，此 QoS 设定在所有时间都有效果，如果选择“**从___:___到___:___**”填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选“**每天/周日/周一/周二/周三/周四/周五/周六**”的某一天或者几天，其 QoS 设定在勾选的那几天的设定的特定时间段有效。

例如：



当总带宽是使用率到达 70%（该数值如果设置为 0%，那么表示无论什么情况都激活智能 QoS 功能）后，智能 QoS 生效：如果内网的任意一个 IP 地址上行带宽超过 120kbps 或者下载带宽超过 850kbps，那么这个 IP 将被限制为：上行带宽 2.5%(即两条线路加起来 80kbps)，下载带宽 4%（即两条线路加起来 800kbps），这个限制的数据是根据 QoS 设置页面的上端“填入 ISP 线路实际可供使用带宽”所填写的带宽数来计算，所以正确填入您的线路实际带宽情况是很重要的。

五、防火墙设置

在防火墙功能当中，有一键管制 QQ，MSN，BT，迅雷等软件的功能，结合酒店的环境，管制 BT 软件是有必要的。

点击“防火墙配置”进入“基本设置”。

由上图的设置，可以实现：管制 BT-迅雷的使用，但是 192.168.0.180~200 这些 IP 地址不受管制。

在木马、病毒肆虐的今天，防止其在内网之间传播是有效的遏制手段。把 TCP/135~139、UDP/135~138、TCP/445 端口封掉，则可挡住蠕虫等病毒在内网的传播。

请依照如下设置：

1. 点击“防火墙配置”，进入“访问规则设置”，并点击“添加新的管制规则”。

2. 在添加规则的页面中，点击“服务端口新增或删除表”，在弹出的窗口中增加 TCP/135~139，UDP/135~139，TCP/445 端口。我们先来示例增加 TCP/135~139 端口：

首先输入端口名字，例如：蠕虫端口。然后在通讯协议处选择：TCP；端口范围输入：135~139；然后点增加到对应列表，这样就完成了 TCP/135~139 的端口增加。再依次增加完 UDP/135~139，TCP/445 端口，最后点确定即可。如下图：

3. 增加完端口后，我们就可以添加管制规则了，先示例增加一条阻挡 TCP/135~139 端口的管制规则：

- 管制规则：禁止
- 服务端口：蠕虫端口 1[TCP/135~139]
- 来源接口：局域网
- 来源 IP 地址：任何的
- 目的 IP 地址：任何的

最后点确定即可完成。如下图：

最后依次增加阻挡 UDP/135~139，TCP/445 端口的管制条例。如果增加完成，“访问存取界面”应该是如下图所示：

经过以上程序，FVR 系列产品在酒店环境的基本设置已经完成。对于内网用户可以防止少数人占用大量带宽，也可防止蠕虫病毒的攻击，对于酒店日常的运营将会起到简化的作用。