WayOS 路由产品
用户手册

尊敬的客户您好！承蒙惠顾 WayOS 产品，谨致谢意！

目　　录

一、设备的安装：

设备接口说明：

LAN 口：用来连接局域网的交换机或者 PC 电脑的网卡。

WAN 口：用以 ADSL、光纤或者以太网的接入。

Reset：复位按钮，用来将设备参数恢复到出厂预设值。

指示灯说明：

Power：电源指示灯。灯亮表示设备通电正常。

System：系统指示灯。系统正常运行时此灯会亮。

WAN：WAN 口工作指示灯。灯亮表示该 WAN 口线路已连通。

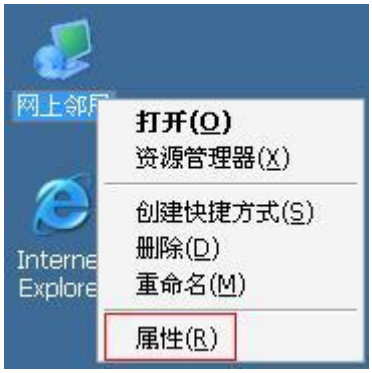
LAN：LAN 口工作指示灯。灯亮表示 LAN 口线路接通。

二、基本上网设置

主要介绍在路由器连接好以后，通过登陆路由的 Web 管理页面，进行路由器的基本信息配置，达到快速上网的目的。

首先需要将您的电脑与路由器的 LAN 口用网线连接起来，并将本机的 IP 地址设置为 192.168.1.X 段。我们以 192.168.1.2 为例来介绍其设置方法：

鼠标右键点击桌面“网上邻居”图标，选择属性，打开‘网络连接’菜单，如图 1 所示，（或者点击“开始-设置-网络连接”也可以打开，如图 2 所示）。



(图 1)

(图 2)

在打开的窗口中找到“本地连接”图标，鼠标右键点击此图标，并选择‘属性’选项，然后在接下来的窗口中选择“Internet 协议(TCP/IP)”并双击（如图 3 所示），进入 IP 地址修改窗口。

(图 3)

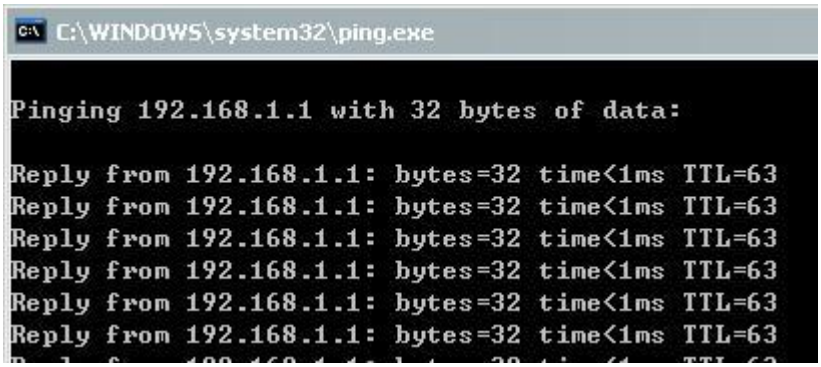
将本机 IP 地址修改为 192.168.1.2，子网掩码为 255.255.255.0，网关为 192.168.1.1，DNS 服务器地址填上网络供应商提供给您的 DNS 地址，若不清楚，可以直接填网关 IP，如图 4 所示：

(图 4)

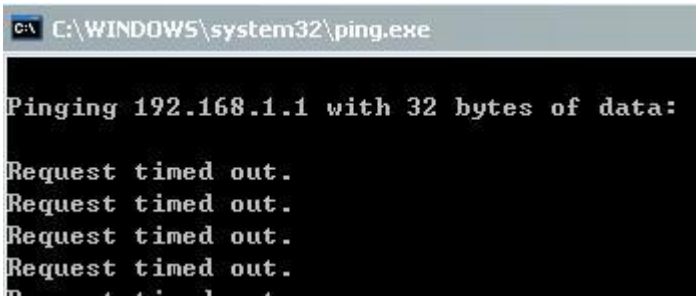
然后我们打开开始菜单，选择“运行”，并输入‘ping 192.168.1.1 -t’看看线路是否通畅。如图 5 所示：

(图 5)

若显示图 6 所示的结果，则表明网络连接正常；若显示图 7 所示的结果，则表明网络连接有问题，请检查网络连接状况。



(图 6)



(图 7)

当您与路由器正常连接以后，您就可以通过 IE，在地址栏输入 192.168.1.1（路由器的默认 IP）进入路由器 WEB 设置界面。会出现图 8 所示的登陆画面：

(图 8)

路由器默认的用户名是“root”密码为“admin”，您可以在‘高级配置-访问设置’里自定义更改登陆的用户名及密码。

温馨提示：为了安全起见，我们强烈建议您在登陆以后更改管理员密码，并牢记此密码。若密码忘记，将无法再登陆到路由器的 Web 管理界面，必须 reset 恢复出厂设定值才能重新登陆。

一、路由向导

设置向导可以协助您快速的配置好您的网络,只要按照步骤操作完成，就可以设置好您的路由器。

1.1 配置向导

进入系统首页点击“配置向导”图标，出现配置向导欢迎界面，如图所示：

点击下一步就开始步骤 1 设置。

步骤 1：路由器局域网口参数，可以修改路由器的 LAN 口 IP 地址，子网掩码及 MAC 地址，如图所示：

如果需要更改局域网口 MAC 地址，可以点击“随机”按钮进行更改；如果想恢复默认 MAC 地址点击“默认”按钮即可。点击“下一步”按钮进行步骤 2 设置。

步骤 2：广域网设置，此处用于对广域网接口参数进行配置。如图所示：

选择您要设置的广域网：可以选择对应的广域网接口来进行设置。

连接类型：即广域网的接入类型选择，有：DHCP 动态获取、PPPOE 拨号、static 静态接入等多种接入方式，一般我们常用的有 DHCP、PPPOE 跟 static 这 3 种。

静态 DNS：填入网络服务商提供给您的 DNS 服务器 IP 地址。(如果是 PPPOE 接入，可以不用设置 DNS 服务器地址，线路会自动获取到)

DNS **解析优先级**：对于多 WAN 口接入时，此值的优先级别决定了 DNS 解析的出口。

MAC **地址**：此选择可以修改路由器对应的广域网的 MAC 地址，可以手动修改，也可以随机选择。点击“克隆”按钮即可将该广域网的 MAC 设置为当前局域网登录的管理员的电脑的 MAC 地址。

参照值：设置广域网出口带宽时的参考数值，可以参考此数值来设置。选择一个参照值之后，下面外网带宽的数值会自动填写上去。

外网带宽：广域网的上下行带宽值，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

运营商：您的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

步骤 3：路由时间更新的设置。您可以自定义修改路由器的时间更新服务器及时区选择。如图所示：

一般建议保持默认设置，如果想手动设置路由器时间，可将模式选择为“手动设置”

步骤 4：配置路由器访问设置。配置路由器的管理员密码，本地及远程访问端口。如图所示：

HTTP 访问端口:局域网访问端口。修改此端口之后访问格式为（http://路由器 IP:HTTP 访问端口），如 http://192.168.1.1:89。

远程访问:是否开启路由器远程访问功能。

远程访问端口:远程访问路由器的端口。远程访问路由器格式为（http://广域网 IP/动态域名:远程访问端口），如 http://wayos.3322.org:8080。 注：访问格式中的冒号为英文状态下输入的符号。

设置好之后，点击完成，路由会显示‘正在操作中，请等待…’等待约十几秒，完成之后，会自动返回到路由向导主界面。

设置好这些之后，您就可以正常连接互联网了。

二、系统状态

系统运行时的一些相关信息，从这些基本信息，我们可以了解到路由器的工作情况。

2.1 网络状态

广域网当前连接时间、连接方式、连接状态。局域网当前的 IP 地址，以及 MAC 地址、子网掩码等信息。

选择您要查看的广域网：显示每个广域网接口的信息。

MAC 地址：显示广域网口对应的 MAC 地址。
如果您的 ISP 提供商绑定了您的 MAC 地址，请在‘网络配置-广域网 mac 地址’中修改广域网 MAC 地址。

连接类型：表示当前广域网口的连接方式。
如果是拨号接入，将显示 pppoe；如果固定 IP 接入，将显示 static；如果是 DHCP 自动获取，将显示 dhcp。

IP 地址：这个地址就是您对应广域网口的外网 IP 地址。

子网掩码/网关：这个就是您相应 WAN 口的外部掩码及网关。

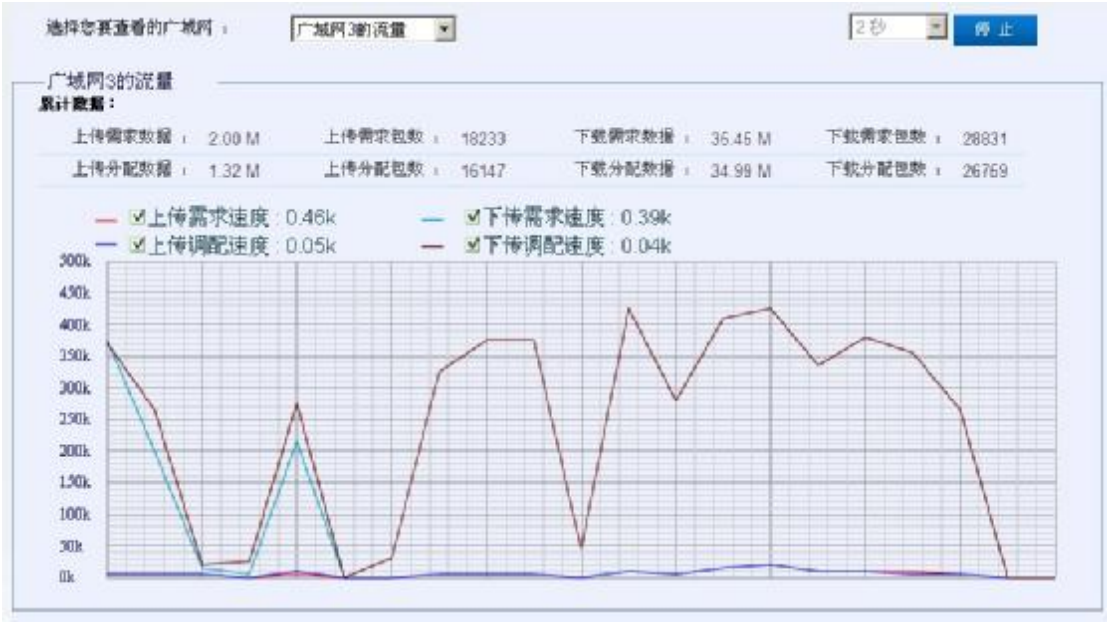
DNS：这里显示 ISP 提供商给您的 DNS 解析服务器 IP。
显示结果将以手动填写为主，若没填写，将自动从上级服务器获取。固定接入方式必须手动指定 DNS。

连接状态：Connected 表示连接成功，Connecting...表示正在连接。

连接时间：表示该广域网口与服务器建立连接的时间，以此时间可以判断 WAN 口是否掉线过。

2.2 流量分析

流量分析可以查看到每一条广域网的流量和总体使用的流量情况。



如上图，显示当前广域网的上传和下载流量分析图，并统计各种数据包类型，

选择查看的广域网：默认显示所有广域网总和的流量，如果需要查看单个广域网流量，请选择相应的广域网口；

上传/下载需求速度：为当前网络中，客户机对外发送请求所需要的流量；

上传/下载调配速度：路由器通过 QoS 规则智能均衡计算之后，分配的速度值。

此处显示的速度单位为 KB，具体换算单位如下：

1.计算光纤传输的真实速度

使用光纤连接网络具有传输速度快、衰减少等特点,因此很多公司的网络出口都使用光纤。比如，网络服务商声称光纤的速度为 5M，那么他的下载真实速度是多少呢？我们来计算一下。一般的情况下，5M 实际上就是 5000Kbit/s(按千进位计算）这就存在一个换算的问题。Byte 和 bit 是不同的。1Byte=8bit.而我们常说的下载速度都指的是 Byte/s 。因此 ISP 所说的“5M”经过还换算后就成为了（5000/8）KByte/s= 625KByte/s 这样我们平时下载速度最高就是 625KByte/s，常常表示 625KB/S。

在实际的情况中，理论值最高为 625KB/S。那么还要排除网络损耗以及线路衰减等原因，因此真正的下载速度可能还不到 600KB/S 不过只要是 550KB/S 以上都算正常。

2.计算 ADSL 的真实速度

ADSL 是大家经常使用的上网方式。那么电信和网通声称的 1 兆 ADSL 下载速度是多少？换算方法为 1Mbit/s=(1000/8)KByte/s=125KByte/s，考虑线路等损耗，实际的下载速度在 100KB/S 以上就算正常了。那么“2MB”呢？大家算算吧，答案是 256KByte/s 。

3.计算内网的传输速度

经常有人抱怨内网的传输的数度慢，那么真实情况下的 10/100Mbps 网卡的速度应该有多快？网卡的 100Mbps 同样是以 bit/s 来定义的，所以 100Mb/S = 100000KByte/s=(100000/8)KByte/s=12500KByte/s 。在理论上 1 秒钟可以传输 12.5MB 的速据，考虑到干扰的因素，每秒传输只要超过 10MB 就是正常了。现在出现了 1Gbps 的网卡，那么速度就是 100MB/S 。

特别提示：

1.关于 bit(比特)/second(秒)与 Byte(字节)/s(秒)的换算说明：线路单位是 bps，表示 bit(比特)/second(秒)，注意是小写字母 b；用户在网上下载时显示的速率单位往往是 Byte(字节)/s(秒)，注意是大写字母 B。字节和比特之间的关系为 1Byte=8Bits；再加上 IP 包头、HTTP 包头等因网络传输协议增加的传输量，显示 1KByte/s 下载速率时，线路实际传输速率约 10kbps。例如：下载显示是 50KByte/s 时，实际已经达到了 500Kbps 的速度。切记注意单位！！！

2.用户申请的宽带业务速率指技术上所能达到的最大理论速率值,用户上网时还受到用户电脑软硬件的配置、所浏览网站的位置、对端网站带宽等情况的影响，故用户上网时的速率通常低于理论速率值。

3.理论上：2M（即 2Mb/s）宽带理论速率是：256KB/s（即 2048Kb/s），实际速率大约为 103-200kB/s；(其原因是受用户计算机性能、网络设备质量、资源使用情况、网络高峰期、网站服务能力、线路衰耗，信号衰减等多因素的影响而造成的)。4M（即 4Mb/s）的宽带理论速率是：512KB/s，实际速率大约为 200-440kB/s。

基础知识：

在计算机科学中，bit 是表示信息的最小单位，叫做二进制位；一般用 0 和 1 表示。Byte 叫做字节，由 8 个位（8bit）组成一个字节(1Byte)，用于表示计算机中的一个字符。bit 与 Byte 之间可以进行换算，其换算关系为：1Byte=8bit（或简写为：1B=8b）；在实际应用中一般用简称，即 1bit 简写为 1b(注意是小写英文字母 b)，1Byte 简写为 1B（注意是大写英文字母 B）。

在计算机网络或者是网络运营商中，一般，宽带速率的单位用 bps(或 b/s)表示；bps 表

示比特每秒即表示每秒钟传输多少位信息，是 bit per second 的缩写。在实际所说的 1M 带宽的意思是 1Mbps（是兆比特每秒 Mbps 不是兆字节每秒 MBps）。

建议用户记住以下换算公式:

1B= 8b1B/s=8b/s(或 1Bps=8bps)

1KB=1024B　　1KB/s=1024B/s

1MB=1024KB　　1MB/s=1024KB/s

规范提示：实际书写规范中 B 应表示 Byte(字节)，b 应表示 bit(比特)，但在平时的实际书写中有的把 bit 和 Byte 都混写为 b ，如把 Mb/s 和 MB/s 都混写为 Mb/s，导致人们在实际计算中因单位的混淆而出错。切记注意！！！

2.3 运行状态

通过查看路由的运行状态，可以了解路由器目前工作状况，有图表实时显示目前系统 CPU 占用资源率。

此功能可以作为判断网络故障和使用率的依据之一。

2.4 主机监控

2.4.1 主机监控

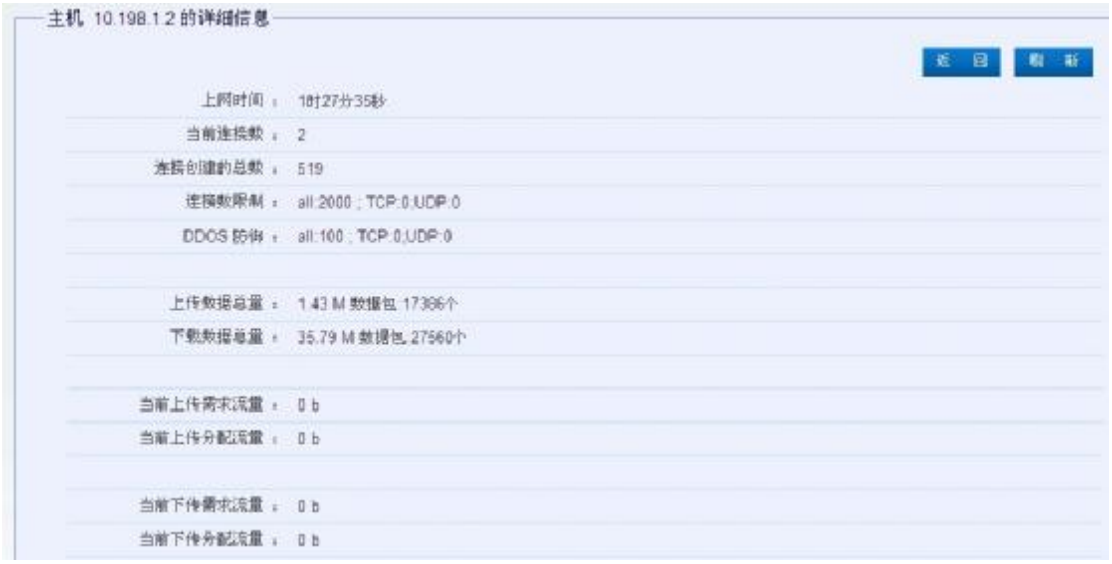
‘主机监控’能显示内网所有用户的网络连接情况。位于"列表"上方的记录数，可以显示当前内网的在线机器数量。

在列表中，可以很直观的看出每台 PC 占用的网络情况，鼠标点击"查看连接"，还能显示该 PC 的网络访问情况，有进程管理的也可以点击查看正在使用的进程。如下图所示：

点击"查看连接"后的效果：

在这个地方可以点击阻止和允许该连接是否使用。默认的是允许使用。如果需要阻止可以点击“阻止”按钮。

点击“详细信息”后的效果：



详细信息页面可以查看当前主机 IP 的规则限制，联机数使用情况及带宽使用情况等。

2.4.2 WEB 用户

用于查看通过 WEB 认证上网的用户信息。如图所示：

2.4.3 PPPoE 用户

该记录是显示通过 PPPOE 拨号到路由器的用户信息。

2.4.4 DHCP 用户

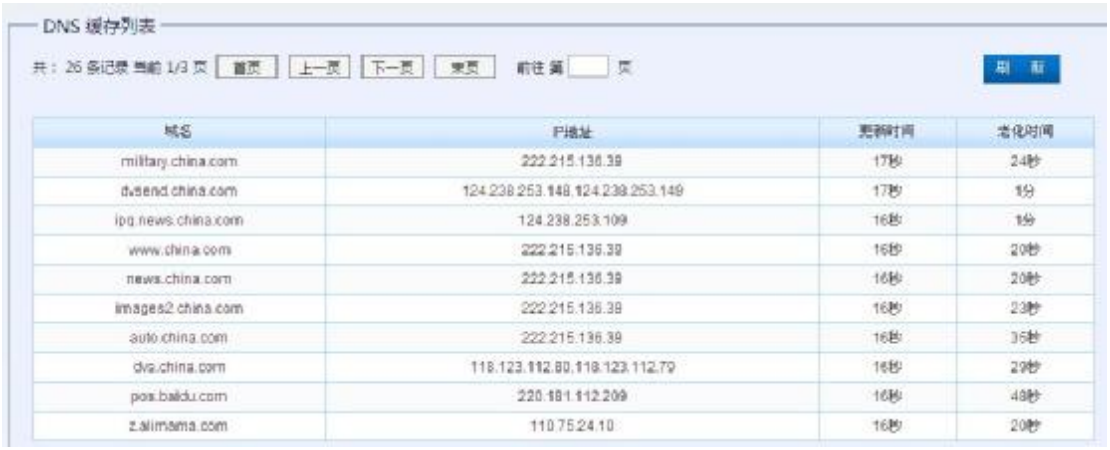
此列表将显示所有 DHCP 自动获取 IP 的用户信息。

2.4.5 聊天账号

列表显示路由器下的用户聊天软件信息，包括有 QQ、MSN、飞信、淘宝旺旺等。

2.5 DNS 缓存

DNS 缓存列表会记录下所有用户近 5 分钟内缓存的域名解析信息，超过时间的缓存信息将会自动老化掉。



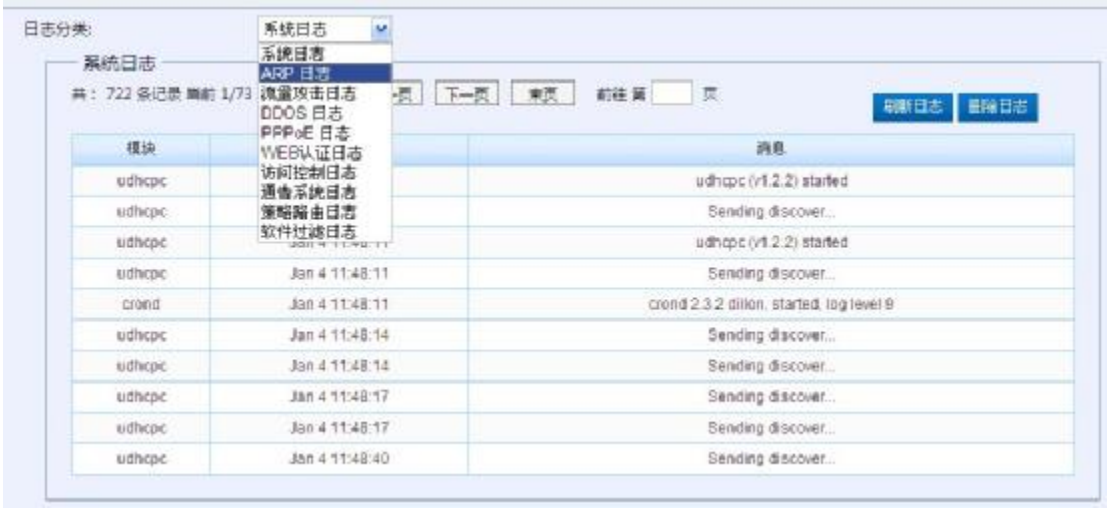
当用户在下次访问列表中的域名时，路由器会有线读取缓存中解析出来的 IP，而不用再经过广域网口的 DNS 去解析，这样便加快了网页的访问速度。

2.6 登陆记录

此列表将显示所有登陆路由器的历史用户。

2.7 日志

在这里可以显示系统日志、ARP 日志、PPPoE 日志、WEB 认证日志、访问控制日志、通告系统日志、策略路由日志、网址日志、URL 重定向日志、软件过滤日志等，所有的日志都可以在这里查看到。



三、网络配置

路由的一些基本功能设置，包括局域网设置、广域网设置、DHCP 配置、及 DDNS 功能的设置。

3.1 局域网

本页面主要用于局域网设置的相关参数，如下图所示：

路由器 LAN 口 IP 地址：设置路由器内网口的 IP 地址，这个地址就是内网计算机的网关地址。该地址出厂时设置为 192.168.1.1，可以根据需要改变它，如果改变了路由器内网 IP 地址，需要重新连接路由器。

子网掩码：根据内网规模设置合适的掩码值。路由器默认使用的子网掩码是 255.255.255.0，可以根据需要更改。

默认网关：当路由器的 WAN 关闭时，如果需要出 LAN 访问外网，则需要设置。此值一般不填。

MAC 地址：根据内网的网络情况，修改 MAC 地址。一般情况下默认的有 MAC 地址，不需要调整。

酒店模式：开启酒店模式之后，路由器下面的电脑设置任意 IP 地址都可以上网，可以设置跟 LAN 口不在同一个网段。（电脑的 IP、掩码、网关、DNS 允许设置任意地址，但必须都设置）开启酒店模式之后，将放弃本地连接的 IP 地址，而使用虚拟的 IP 地址。

多子网段：本路由器内网口允许配置多个 IP 地址，当内部有多于一个子网时可以使用到该功能。其功能与路由器内网地址基本一致，通常作为相应子网的网关使用。此地址不要跟 LAN 口地址设置到同一个子网中，否则可能引起冲突。

多子网段的设置如图所示：

您所添加的 IP 地址相当于是 LAN 口虚拟的另一个网关地址，客户机可以使用您添加的多子网 IP 作为网关地址来上网。此地址不要跟 LAN 口设置到同一个子网，否则可能会引起冲突。

3.2 广域网

本页面主要用于配置 WAN 口相关参数，我们常用的广域网连接方式主要有自动获取 IP、static 静态接入跟 PPPOE 拨号接入 3 种。

1. 自动获取 IP

连接类型：选择自动获取 IP（动态获取地址）。

MTU **设置**：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

MAC **地址**：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整。

静态 DNS：填入网络服务商提供给您的 DNS 服务器 IP 地址，或者上级设备的网关地址。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

DNS 解析优先级：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，动态获取 IP 时，我们一般不用开启。

外网带宽：广域网的上下行带宽值，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

运营商：您的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

2. 静态 IP 接入

连接类型：选择静态 IP 上网方式。

IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，您可以向网络服务商询问获得。

子网掩码：前 IP 所对应的子网掩码，由网络服务商提供。

默认网关：当前 IP 所对应的网关，由网络服务商提供

MTU 设置：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

MAC 地址：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整。

静态 DNS：填入网络服务商提供给您的 DNS 服务器 IP 地址，由网络服务商提供，您可以向网络服务商询问获得。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

DNS 解析优先级：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，静态地址接入时，我们不需要开启此功能。

外网带宽：广域网的上下行带宽值，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

运营商：您的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

3. ADSL 拨号上网（PPPOE 拨号接入）

连接类型：选择 ADSL 拨号上网（PPPOE 拨号接入）。

用户名称：填入网络服务商提供的 PPPOE 线路帐号，可以向网络服务商询问获得。

用户密码：填入网络服务商提供的 PPPOE 线路口令，可以向网络服务商询问获得。

服务名称：一般不填，某些特殊线路可能需要填入服务器名称才可以。

连接检查间隔：用户自行设定重新拨接的时间，默认值为 30 秒。

MTU 设置：即最大传输单元，PPPOE 拨号默认使用 1492 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

MAC 地址：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整。

静态 DNS：PPPOE 拨号接入时可以不用填写 DNS 地址，若您不想使用自动获取的 DNS 地址时，可以填入网络服务商提供给您的其他 DNS 服务器地址。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

DNS **解析优先级**：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，动态获取 IP 时，我们一般不用开启。

外网带宽：广域网的上下行带宽值，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

运营商：您的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

MAC 地址中的 

选项分别有如下定义：

“克隆”表示将该接口的 MAC 地址设置为跟您电脑的 MAC 一样的地址。
“默认”表示使用系统默认的 MAC 地址。
“随机”表示随机分配一个 MAC 地址给该接口。

某些网络服务商将提供给您的线路同某一个固定的 MAC 地址绑定起来，在这种情况下，MAC 地址克隆就非常有用。

4．透明桥接

IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，您可以向网络服务商询问获得。

子网掩码：前 IP 所对应的子网掩码，由网络服务商提供。

默认网关：当前 IP 所对应的网关，由网络服务商提供。

内部主机范围：需要使用到透明模式的内网机器 IP 范围段，此 IP 段必须是跟广域网的 IP 在相同 IP 段才可以。

MTU **设置**：即最大传输单元，系统默认使用 1500 字节。通常情况下这个参数不用设置，保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

MAC **地址**：根据内网的网络情况，随机或克隆 MAC 地址。一般情况下默认的 MAC 地址，不需要调整。

静态 DNS：填入网络服务商提供给您的 DNS 服务器 IP 地址，由网络服务商提供，您可以向网络服务商询问获得。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

DNS **解析优先级**：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，静态地址接入时，我们不需要开启此功能。

外网带宽：广域网的上下行带宽值，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

运营商：您的广域网线路的运营商，例如网通或者电信。如果选择“不设置”，则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

通透模式的使用较少，一般在特殊环境如：不改变现有网络环境，加入一台路由设备到网络中作为管理，这个时候就需要用到透明桥接模式。

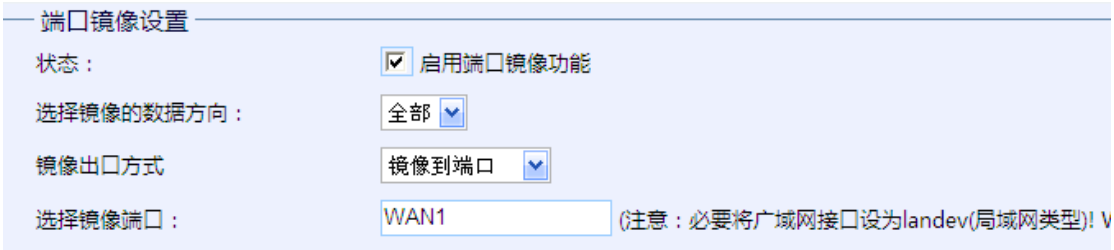
5．局域网

IP 地址：必须设置跟 LAN 口不冲突的 IP 段。此 IP 是作为镜像机器的网关来使用的，镜像机器需要单独接到该广域网口，中间不能接入其他交换机设备。

子网掩码：虚拟子网络的掩码地址。

MTU **设置**：虚拟子网络的 MTU 值大小，一般保持默认即可。

此处的局域网设置是为了配合基于端口的端口镜像来使用的。如在不带交换芯片的硬件路由上开启了基于端口的镜像，那么就需要将镜像的 WAN 口设置为局域网模式，并填写一个与 LAN 口网段不冲突的虚拟子网。



如上图所示，开启了 WAN1 口作为镜像口，那么就需要将 WAN1 口设置为局域网模式，并填入一个跟 LAN 口不冲突的虚拟子网。需要镜像的机器单独接到 WAN1 口，并设置 WAN1 口的 IP 作为镜像机器的网关地址，保证镜像机器 IP 与 WAN1 口处于同一个网段，这样镜像机就可以正常镜像到需要的数据信息。

3.3 DHCP 配置

本界面主要提供DHCP服务器功能。如果内网计算机的TCP/IP协议配置为“自动获得 IP 地址”，并且在内网没有 DHCP 服务器的情况下，可以使用该功能。

DHCP 是 Dynamic Host Configuration Protocol（动态主机配置协议）的缩写，它是 TCP / IP 协议簇中的一种，主要是用来给网络客户机分配 IP 地址。这些被分配的 IP 地址都是 DHCP 服务器预先保留的一个由多个地址组成的地址集，此地址集一般是一段连续的地址。

管理方式：您可以选择普通、高级或者关闭。普通 DHCP 方式只能分配路由器 LAN 口网段的 IP，高级 DHCP 方式可以任意分配 IP 段、掩码及 DNS 服务器地址。

开始地址：DHCP 服务器自动分配的内部 IP 的起始地址。

结束地址：DHCP 服务器自动分配的内部 IP 的结束地址。

释放时间：设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间，默认是 3600 秒。您可以自行设置。

网关地址：DHCP 服务器给客户机分配的默认网关地址。

子网掩码：DHCP 服务器自动分配给客户机的掩码地址。

首选/备用 DNS 服务器地址：DHCP 服务器自动分配给客户机的 DNS 服务器地址。

3.4 动态域名

DDNS 动态域名解析服务主要用于将一个动态的 IP 解析成一个静态的域名，以便于网络来访问。

选择动态域名工作的广域网：选择一个您要绑定域名更新的广域网接口。

动态域名服务：选择一个您要绑定 IP 的域名服务商，后面提供有服务商的官方网址。

用户名称/密码：填写您在域名服务商申请的账号名称及密码。

需要更新的域名：填写您需要绑定此 IP 的一个域名，该域名必须为未被其他 IP 使用过。

设置完毕之后点击“添加”，加入到列表中即可。若域名更新成功，在‘最近响应状态’会显示“Update successful” 的字样，即更新成功的意思。

3.5 路由名称

在这里您可以查看到路由器名称、主机名称以及所在域名信息。

路由名称：默认为 WayOS 多 WAN 高性能路由器，您可以自行修改。
主机名称：默认为 WayOS，您可以自行修改。
所在域名：默认为空，您可以自行修改。

四、智能流控

该页面相关设置可以对您的网络带宽使用进行管理，以保证您的网络使用达到最佳效果。

4.1 带宽限制

在此界面中，您可以对内部机器的带宽使用进行自由控制。

激活：控制规则是否生效。勾上，则表示该规则生效。

描述：对该规则的描述。

主机 IP 地址范围：设置您要控制的主机范围(单个机器 IP 或者是某个 IP 段)，点击空白框，会弹出 IP 添加窗口，如图所示：

首先选择 IP 控制类型，然后填入管控的 IP 范围，并将 IP 添加至列表中，然后点击完成，IP 范围就添加好了。

控制方式：（单独限制）此范围内每个 IP 的速度将被限制在设定的速度内，即对设定范围内的每个 IP 进行单独限速；（共享限制）此范围内所有 IP 的全部速度总和将被限制设定的速度内。

上传/下载速度：上传/下载速度限制，单位为 KB/s，设置为“0”表示不限制速度。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。（每周：您可以设置一周的哪几天生效，如果没有设置，则表示每天都生效；每天：您可以设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。）

4.2 带宽保证

激活：控制规则是否生效。勾上，则表示该规则生效。

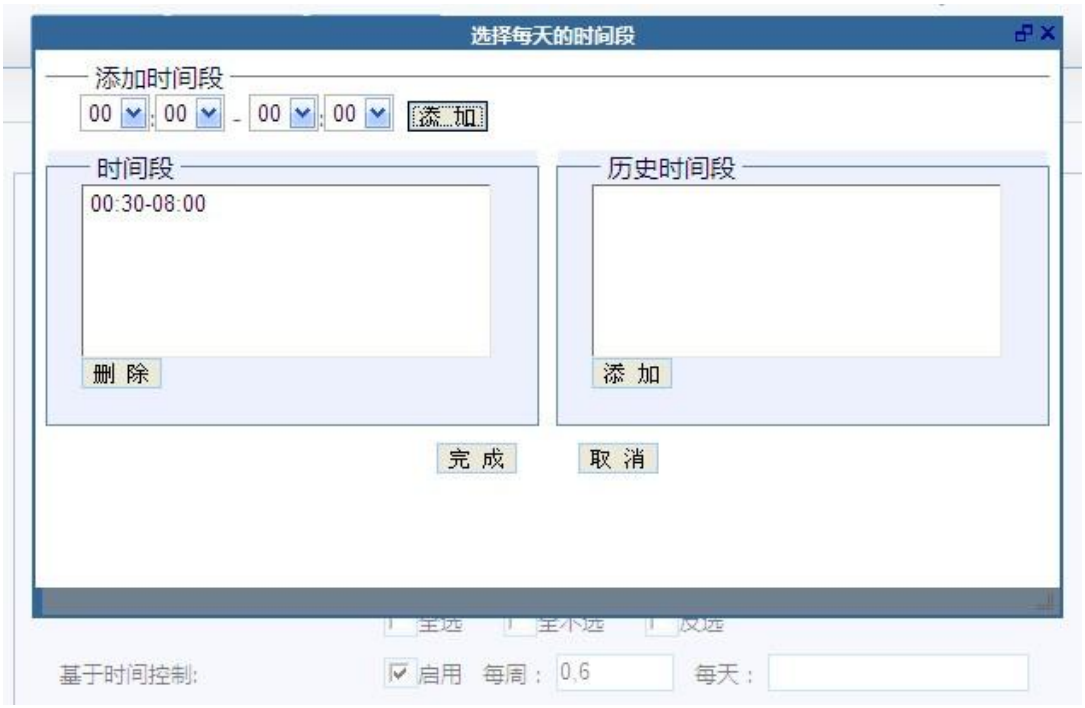
描述：对该规则的描述。

主机 IP 地址范围：设置您要控制的主机范围(单个机器 IP 或者是某个 IP 段)。

控制方式：（独占带宽）此范围内的 IP 将优先占用设置的带宽；（共享带宽）此范围内所有 IP 的全部带宽总和将被限制设定的范围内，即范围内的 IP 将共用所设定的带宽值。

上传/下载速度：上传/下载速度限制，单位为 KB/s，设置为“0”表示不限制。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。如图所示：



（每周：您可以设置一周的哪几天生效，如果没有设置，则表示每天都生效；每天：您可以设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。）

带宽保证的具体设置方法跟速度限制设置相同。其不同之处在于，速度限制是对单个 IP 或者范围 IP 进行的流量限制；而带宽保证则是对单个 IP 或者范围 IP 提供的一个带宽值保障。

4.3 控制例外

该功能可以对外部服务器的访问限制排除在外，不受智能 QOS 的控制。

流量控制例外(基于 IP)：填入您要排除的不受 QOS 控制的广域网 IP 地址。设置之后，您访问到该地址时的流量就不受智能 QOS 规则的限制了。

流量控制例外(基于域名)：填入您要排除的不受 QOS 控制的广域网域名地址（域名格式为：www.qq.com、*.baidu.com、xunlei 等）。设置之后，您访问到该域名时的流量就不受智能 QOS 规则的限制了。

注意：当您设置了 QOS 例外之后，您访问该地址时的流量统计就不会在流量监控显示出来了，包括主机监控也不会显示。

五、无线配置

设置无线部分相关功能，包括无线的开启/关闭、无线加密、MAC 地址过滤以及 WDS、WPS 设置。

5.1 基本设置

对无线功能的开启与关闭，以及基本参数做设置，开启无线之后如下图所示。开启或者关闭无线功能模块时路由都是需要重启的。

加载无线模块：无线模块的功能开关，勾上表示开启无线功能，开启之后路由会重启一次。

网络模式：可以对无线模式进行选择 b/g/n 三种模式进行混合配置，选用 11b/g/n 模式，路由器会根据用户的客户端网卡的速率自动调节。

网络名称 SSID：无线局域网用于身份验证的登录名，只有通过身份验证的用户才可以访问本无线网络。此处的网络名称就是无线设备搜索无线信号时搜索到的无线资源名称。

隐藏：隐藏此 SSID 名称，不广播。其他无线设备将不能直接搜索到此 SSID。

隔离：相当于给此 SSID 下的用户划分了 VLAN，使用户之间不能互相访问。

网络名称 1/2/3/4：您可以给一个无线设备设置多个网络名称（SSID），再通过 AP 外隔离，实现不同的 SSID 内的无线用户无法互相访问，实现无线虚拟局域网。

AP **隔离**：不属于本 AP 的其他客户端不能访问本 AP 下面的客户端。

MAC **地址**：一组无线工作站和一个无线局域网接入点(AP)组成一个基本服务装置(BSS)，BBS 中的每台计算机都必须配置相同的 BSSID，即为 AP 的无线标识。

无线频道：以无线信号作为传输媒体的数据信号传送通道，您可以选择其中的任意一个频道来进行连接。

5.2 无线安全

用于设置无线的各种加密模式，以及对 MAC 地址的过滤。

选择您要设置 SSID：首先选择一个需要设置的 SSID 名称（如果有多个 SSID 的话）。

安全设置：分为开放式、共享式、WEPAUTO、WPA 企业、WPA 个人、WPA2 企业、WPA2 个人、WPAP/WPA2 个人、WPA1/WPA2 企业这 9 类。选择关闭则不采取任何加密方式。

一、开放式：WEP 加密的一种握手方式，是通过 WEP 密钥来进行加密。

可以选择默认密钥为 Key1-Key4，然后分别对 4 个密钥进行定义，4 个密钥都可以满足用户登入无线。

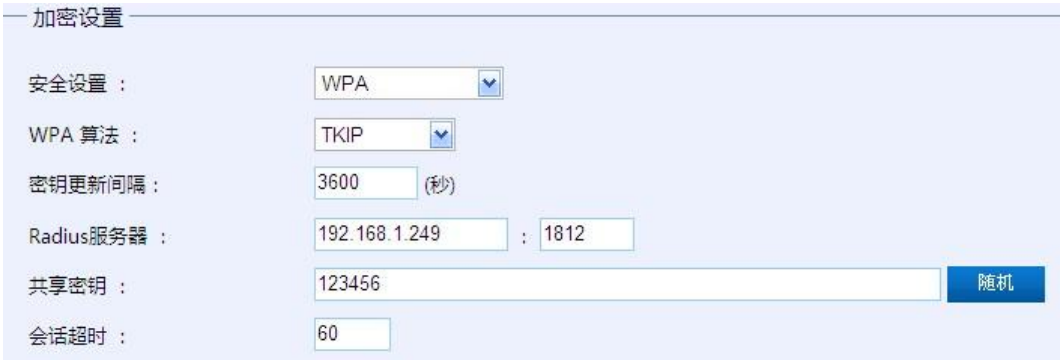
密钥类型说明：密钥的类型分为 Hex(十六进制)和 ASCII(阿斯科码)两种类型；若采用 16 进制，则密钥字符可以为 0-9、ABCDEF；若采用 ASCII 码，则能够用键盘上的所有字符。

二、 共享式：WEP 加密的另外一种握手方式，也是通过 WEP 密钥进行加密，加密类型与开放式加密情况一样。

共享式可以选择不需要 WEP 加密来进行验证，可以在设置上填写加密类型为 None。

三、WEPAUTO：能够自动选择为开放式或者共享式，加密类型方式和前两者一样。

四、WPA：WPA 加密，路由器采用 raius 服务器进行身份认证并得到密钥。



WPA 算法：进行认证过程中所用的算法类型。

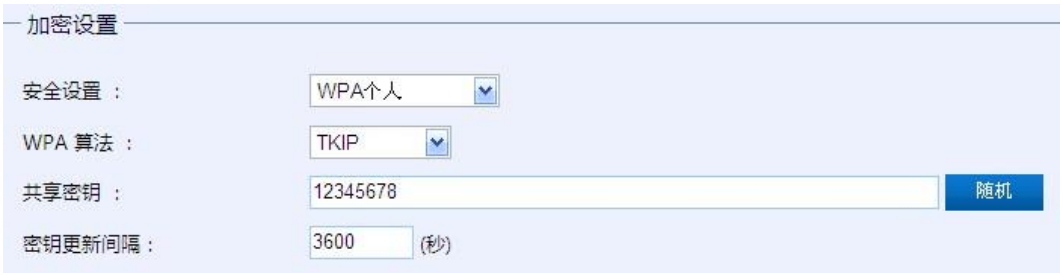
密钥更新间隔：广播和组播密钥的定期更新周期，最大值为 3600 秒，最小为 0，为 0 则不更新。

Radius 服务器：认证服务器的 IP 地址及认证所采用的端口号，认证服务器可以搭建在内网的某台 PC 上。

共享密钥：访问 RADIUS 服务的密码。

会话超时：当会话超时达到多少时，radius 服务器会自动断开该连接。

五、WPA 个人：路由器将采用基于共享密钥的 WPA 模式。



WPA 算法：进行认证过程中所用的算法类型。

共享密钥：无线用户接入时所需要的口令。

密钥更新间隔：广播和组播密钥的定期更新周期，最大值为 3600 秒，最小为 0，为 0 则不更新。

六、WPA2：与 WPA 模式相类似。

WPA 算法：进行认证过程中所用的算法类型。

密钥更新间隔：广播和组播密钥的定期更新周期，最大值为 3600 秒，最小为 0，为 0 则不更新。

PMK 缓存周期：设定 PMK 缓存周期，当用户断开后的此时间段内连接会加快速度。

预认证：启用可以提高无线接入的速度。

Radius 服务器：Radius 认证服务器的 IP 地址及认证所采用的端口。

共享密钥：访问 RADIUS 服务的密码。

会话超时：当会话超时达到多少时，radius 服务器会自动断开该连接。

七、WPA2 个人：路由器将采用基于共享密钥的 WPA2 模式。

WPA 算法：进行认证过程中所用的算法类型。

共享密钥：无线用户接入时所需要的口令。

密钥更新间隔：广播和组播密钥的定期更新周期，最大值为 3600 秒，最小为 0，为 0 则不更新。

八、WPA/WPA2 个人：与 WPA 个人和 WPA2 个人的设置方式一致。

九、WPA1/WPA2：与 WPA 的设置方法一样。

无线 MAC 地址过滤：提供了对无线访问策略的设置,可以设置允许和拒绝所选的 MAC 地址的接入。如图所示：

过滤方式有 3 种选择模式：禁止使用过滤器、允许如下客户端、阻止如下客户端。

禁止使用过滤器：不使用 MAC 地址过滤功能。

允许如下客户端：只允许列表中添加的 MAC 地址的设备连接无线。

阻止如下客户端：禁止列表中添加的 MAC 地址的设备连接到无线网络。

描述：对添加的 MAC 地址的简单描述，便于管理员识别不同的 MAC 地址。

MAC **地址**：客户端设备的 MAC 地址。

5.3 WDS 设置

WDS（无线分布式系统），是一个在 IEEE 802.11 网络中多个无线访问点通过无线互连的系统。它允许将无线网络通过多个访问点进行扩展。这种可扩展性能，使无线网络具有更大的传输距离和覆盖范围。共分为三种连接方式：自学习模式，桥接模式和中继模式。若选择关闭则不启用 WDS 功能。

1．**自学习模式**：自学习模式不需要填写对方的 BSSID，本设备的 WDS 连接作为被动连接，只需要对方填写了本设备的 BSSID 即可，效果和桥接模式一样。

加密类型：WEP、TKIP 和 AES 三种，WEP 采用 WEP 密钥进行加密，TKIP 采用了暂时密钥集成协议，AES 采用对称分组密码体制。当 WDS 连接的 AP 所设置的加密方式必须一样时，连接才能生效。

密钥：相应的密码，至少为 8 个字符。

PHY **模式**：指物理层。三种模式分别对应三种无线网络标准：

CCK-802.11b;OFDM-802.11g;HTMIX-802.11g/n;一般我们选择 CCK 模式。

2．**桥接模式**：桥接模式需要填写对方设备的 BSSID,本机的 SSID 则被屏蔽，只是作为中继模式的 SSID 的扩展形式。

MAC **地址**：需要连接到的设备的 BSSID 地址。

加密方式：WEP、TKIP 和 AES 三种，WEP 采用 WEP 密钥进行加密，TKIP 采用了暂时密钥集成协议，AES 采用对称分组密码体制。当 WDS 连接的 AP 所设置的加密方式必须一样时，连接才能生效。

密钥：相应的密码，至少为 8 个字符。

PHY **模式**：指物理层。三种模式分别对应三种无线网络标准：

CCK-802.11b;OFDM-802.11g;HTMIX-802.11g/n;一般我们选择 CCK 模式。

3．**中继模式**：中继模式也要填写所需要连接 AP 的 BSSID,本机 AP 作为核心，其他的 AP 只是作为中继的一个扩展形式。

MAC **地址**：即为所需要连接 AP 的 BSSID 地址。

加密方式：WEP、TKIP 和 AES 三种，WEP 采用 WEP 密钥进行加密，TKIP 采用了暂时密钥集成协议，AES 采用对称分组密码体制。当 WDS 连接的 AP 所设置的加密方式必须一样时，连接才能生效。

密钥：相应的密码，至少为 8 个字符。

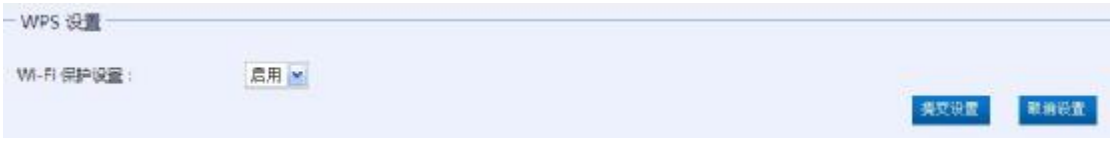
PHY **模式**：指物理层。三种模式分别对应三种无线网络标准：

CCK-802.11b;OFDM-802.11g;HTMIX-802.11g/n;一般我们选择 CCK 模式。

5.4 WPS 设置

WPS 是一种操作简单且加密程度安全的无线连接方式，目前通过 WPS 认证的产品能够为用户提供两种实现方式，即 PBC（按钮）模式和 PIN（个人识别码）模式。

要使用 WPS 功能，首先您需要将 WPS 状态设置为开启状态，如图所示：



在 WPS 信息中将显示当前 WPS 状态的参数信息，您可以在此界面重置 WPS 参数、重新生成新的 PIN 码，如图所示：

在 WPS 模式设置里面，您可以手动去连接已经激活 WPS 的其他无线设备。您可以选择 PIN 模式或者 PBC 模式的客户端。

WPS 状态将显示您当前的 WPS 连接状态信息。

5.5 用户列表

显示当前连接到路由的无线设备信息。

六、行为管理

对内网用户的上网行为进行管控，常用应用软件的封锁限制、网页及关键字的过滤与限制

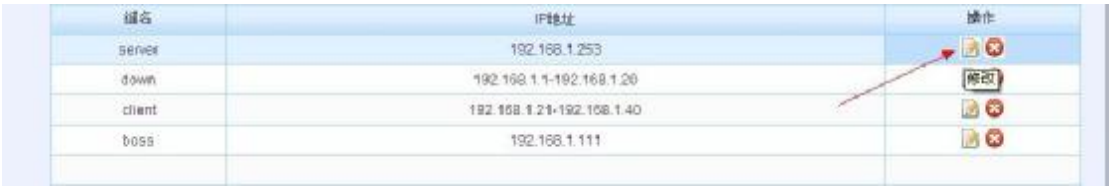
6.1 IP 地址组

此项用于给 IP 地址划分分组，该分组在行为管理中的规则添加时需要用到，也就是添加行为控制规则时的被控制对象

分组名称：对分组的名称描述。

IP 地址：添加一个或者多个 IP 地址。您可以对不同的 IP 划分分组来进行管理。如图所示：

若您要对列表中的规则做修改，只需要点击右边“操作”栏的编辑图标即可对已有的规则进行修改，如图所示：



6.2 娱乐软件

可以有效过滤下载软件、聊天软件、音乐软件、股票软件、代理软件等各类常用娱乐软件。

激活：勾选表示激活此规则。

描述：对此规则的简单描述。

控制方式：设置该规则是允许通过还是禁止通过。

执行顺序：设置一个执行顺序值，值越大的规则越被优先执行。

IP 地址组：选择一个 IP 地址组范围。该组别是在‘行为管理-IP 地址组’里面添加的。

被限制的应用：依据您的需求，勾上要过滤的软件类型。

基于时间管控：是否启用按时间段来控制规则生效。


下载软件
聊天软件
音乐软件
股票软件
代理软件
聊天软件过滤
激活:
激活
日志
描述:
控制方式:
允许通过
执行顺序:
65536
(1-65535)值越大越先被执行。
IP地址组:
全部用户
被限制的应用:
YY语音聊天
QQ
MSN
淘宝旺旺
飞信
WEBQQ
全选
全不选
反选
基于时间控制:
启用
添 加
修 改
取 消


下载软件
聊天软件
音乐软件
股票软件
代理软件
音乐软件过滤
激活:
激活
日志
描述:
控制方式:
允许通过
执行顺序:
65535
(1-65535)值越大越先被执行。
IP地址组:
全部用户
被限制的应用:
酷我音乐
酷狗音乐
QQ音乐
全选
全不选
反选
基于时间控制:
启用


下载软件
聊天软件
音乐软件
股票软件
代理软件
股票软件过滤
激活:
激活
日志
描述:
控制方式:
允许通过
执行顺序:
65535
(1-65535)值越大越先被执行。
IP地址组:
全部用户
被限制的应用:
同花顺股票软件
通达信股票软件
大智慧股票软件
益盟操盘手股票软件
和讯股道股票软件
钱龙股票软件
指南针股票软件
全选
全不选
反选
基于时间控制:
启用

聊天软件、音乐软件、股票软件、代理软件的过滤设置与下载软件设置方法一致，可直接参考下载软件的设置方法。

6.3 网络软件

用于控制网络类的一些软件，包括网络游戏、网页游戏、网络电视、网络电话及一些其他软件。

激活：勾选表示激活此规则。

描述：对此规则的简单描述。

控制方式：设置该规则是允许通过还是禁止通过。

执行顺序：设置一个执行顺序值，值越大的规则越被优先执行。

IP 地址组：选择一个 IP 地址组范围。该组别是在‘行为管理-IP 地址组’里面添加的。

被限制的应用：依据您的需求，勾上要过滤的软件类型。

基于时间管控：是否启用按时间段来控制规则生效。

网页游戏、网络电视、网络电话及其他软件的设置方式与网络游戏设置方式相同。

6.4 邮件管理

邮件管理可用于监控内网所有用户使用邮箱客户端发送的邮件记录。

只需要开启监控功能，并填写您的邮箱地址。系统即可开始监听内网所有基于客户端（foxmail、outlook 等）的邮件信息，在客户机发送邮件的同时，将自动复制相同的邮件内容发送至您填写的邮箱。

6.5 高级管理

6.5.1 聊天软件黑白名单

该功能主要是用于禁止/允许常用的一些聊天软件对网络的访问。

过滤方式：（该处有 3 个选项，分别代表如下含义）

1. 不启用：表示该功能不生效

2. 允许如下号码，禁止其他：表示允许下面规则中聊天软件的账号登陆，禁止同类型的其他号码登陆。

3.阻止如下号码，允许其他：表示阻止下面规则中聊天软件的账号登陆，允许同类型的其他号码登陆。

类型：提供了几种常见的聊天软件选择，有飞信、淘宝旺旺、MSN 及 QQ 等。

号码：填入对应软件的登录 ID 号。

6.5.2 WEB 关键字

该功能是禁止用户在网页中搜索指定的关键字功能，用于屏蔽一些敏感词汇，类似于论坛里的过滤敏感字功能。

控制状态：选择是否启用关键字过滤功能。

日志：是否记录规则执行产生的日志。

状态：是否该条规则生效。

描述：给该规则命名备注，便于识别。

被过滤关键字：要禁止搜索的关键字，支持中文、英文跟数字字符。

如果您在搜索引擎搜索了已经被进制的关键字，那么路由器将会弹出阻止的提示通告，如图所示：

6.5.3 禁止 WEB 提交

该功能是禁止/允许客户机向网络上的服务器的上传行为，比如邮件中的上传附件等。

控制状态：（该处有 3 个选项，分别代表如下含义）

1.不启用：该功能不生效。

2.允许规则之外的通过：除了下面规则中的不能进行 web 提交外，其他不在规则中的用户是可以正常进行 web 提交行为。

3.禁止规则之外的通过：允许下面规则中的用户进行 web 提交，不在规则中的用户不能进行 web 提交行为。

激活：使该规则生效。

描述：给该规则命名的备注信息，便于识别规则。

IP 地址组：表示该规则中对内网哪些用户生效。

基于时间控制：勾上后，可以选择时间段。表示该规则只在指定的时间段内生效，不勾选表示所有时间段都生效。

6.6 后缀名过滤

该功能是禁止/允许客户机访问网络上带有规则中指定的后缀名的文件。

控制状态：（该处有 3 个选项，分别代表如下含义）

不启用：不启用该功能

允许规则之外的通过：除了下面规则中的不能进行 web 提交外，其他不在规则中的用户是可以正常进行 web 提交行为。

禁止规则之外的通过：允许下面规则中的用户进行 web 提交，不在规则中的用户不能进行 web 提交行为。

激活：使该规则生效。

描述：给该规则命名的备注，便于识别。

IP 地址组：表示该规则中对内网哪些用户生效，此 IP 地址组是在“行为管理-IP 地址组”里面添加的。

后缀名：勾上即表示该规则对勾上的后缀名生效

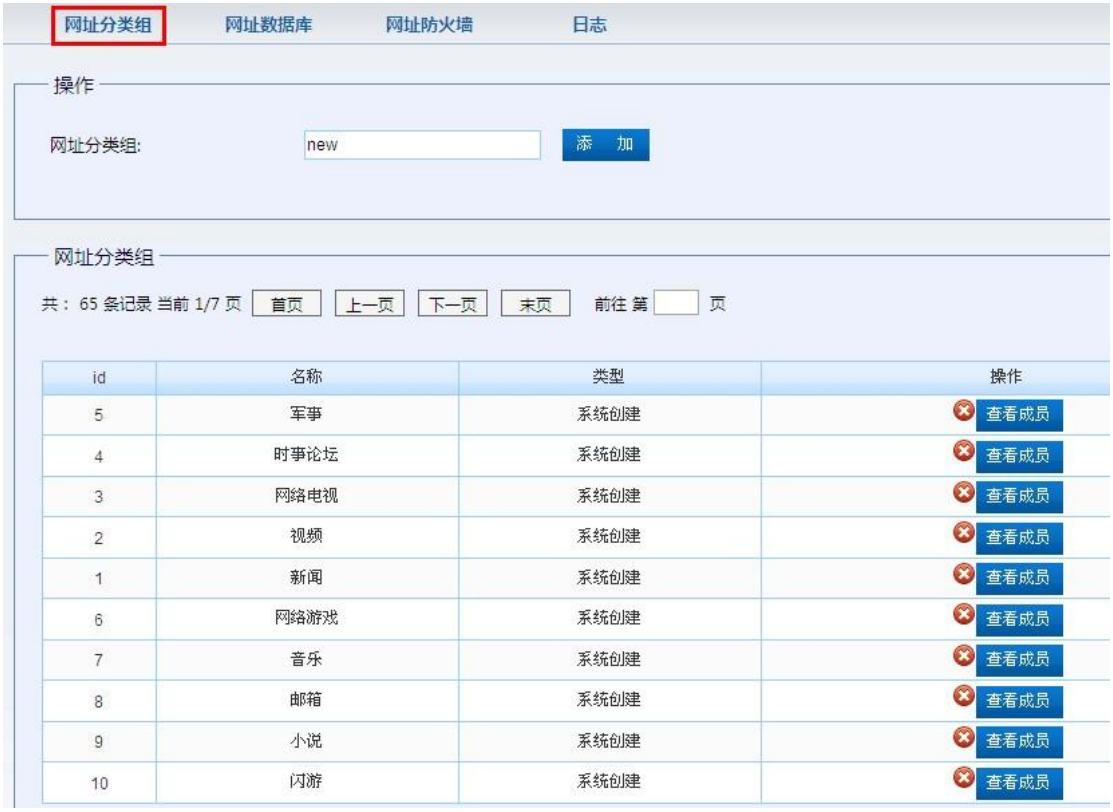
手动输入后缀名：路由器中提供的后缀名没有您需要的后缀名，您可以在这里手动填上，当添加多个后缀名的时候，用‘，’（逗号是英文半角输入法下的符号）分开。

基于时间控制：勾上后，可以选择时间段。表示该规则在指定的时间段内生效。

6.7 网址管理

6.7.1 网址分类组

此界面可以对用户访问的网页做管理控制，系统默认收集了 62 个分类，约 7 千多个网站，除此之外，您还可以自定义添加更多的相关网站并对其进行控制。如图所示



该页面用于添加网址的分组，每个组里面可以添加多个成员（即网站域名）。点击列表中的操作栏可以查看每个分组里的详细域名信息。

6.7.2 网址数据库

该页面可以往指定的分组里添加域名信息，用于完善已有的分组或者新添加的分组。如图所示：

同时您还可以将已有的网址分类信息导入路由或者导出备份，如图所示：

6.7.3 网址防火墙

网址过滤功能可以自定义设置规则用来控制用户对网页的访问，如下图所示：

网址过滤方式：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式。

不启用，就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过，列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过，规则之外的所有都不允许通过，规则之内的受规则管控。

状态：是否启用该规则。

日志：是否在日志中记录该规则的发生情况。

动作：该规则为允许通过还是禁止通过。

描述：对规则的一个描述。

主机 IP 地址范围：所受限制的 IP

执行顺序：规则的执行优先等级。

网站地址组：选择您要控制的网址分类组。如下图所示：

基于时间管控：是否启用按时间段来控制规则生效。

6.7.4 日志

记录网址防火墙控制时候产生的日志信息，根据日志可以查看有那些规则是被禁止或者允许的。

6.8 域名解析

6.8.1 域名解析

域名特殊解析主要是用来将一些特定的域名绑定到指定的线路上去解析。如图所示:

DNS **域名**：需要绑定到线路上的域名或者域名关键字。

出口选择：选择一个广域网的接口用来解析指定的域名。

6.8.2 域名过滤

DNS **过滤方式**：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式。

不启用，就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过，列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过，规则之外的所有都不允许通过，规则之内的受规则管控。

DNS **域名**：添加所需过滤的域名或者域名关键字。

6.8.3 域名重定向

DNS 域名：填入被转向的域名。支持通配符 * （例如：*.qq.com 即表示所有带 qq.com 的网站，象 news.qq.com，qzone.qq.com，mail.qq.com 等等）。

重定向到：填入您需要转向到的一个域名或者 IP。（此域名必须是服务器解析之后只有单一地址的。象 www.baidu.com 解析出来就有多个 IP，这样的就不行。）

若需要将域名转向到一个解析后有多个地址的域名，可以使用“行为管理-URL 重定向”来实现。

6.9 URL 重定向

6.9.1 URL 重定向

URL 重定向是对域名重定向功能的补充跟完善，一些用域名重定向无法转向的域名，通过 URL 重定向就可以实现。

状态：选择是否激活应用此规则；

日志：是否需要在日志中显示记录。

描述：对该条规则的简单描述。

URL 的主机名称：填入您需要被转向的域名地址。

目录网页（URL）：填入被转向域名的目录网页，若没有，则可不填。

网页的参数：填入被转向域名的网页参数，若没有，则可以不填。

重定向到：需要被转向到的域名地址。

主机 IP 地址范围：内部需要被重定向的主机 IP 地址。

基于时间控制：启用则规则只在设定的时间段内生效。

6.9.2 日志

该功能是用来记录 URL 重定向中勾选日志的规则的匹配记录。

6.10 软件过滤日志

用于记录 WEB 关键字过滤时的规则日志信息记录。

七、进程客户端

维盟公司独家研发的进程客户端功能，能对客户机进程或者目录进行带宽、策略等控制

7.1 基本设置

7.1.1 基本设置

打开应用程序基本设置界面，可以选择是否启用 WayOS 客户端功能，如图所示：

控制方式可以用来选择是否开启 WayOS 客户端功能。

不启用 WayOS 客户端：不启用应用程序控制功能。

启用 WayOS 客户端，但不强制安装客户端：开启应用程序策略功能。PC 客户机可以选择安装 WayOS 客户端，也可以不安装 WayOS 客户端。

启用 WayOS 客户端，并强制安装客户端：开启应用程序策略功能。PC 客户机在开启网页的时候弹出下载确认，要求客户机必须下载安装 WayOS 客户端。

允许不安装客户端例外 IP 地址范围：添加的 IP 将被排除在外，不强制安装 WayOS 客户端。

选择相应的控制方式，然后点击下方的‘提交设置’按钮提交更改。

7.1.2 提示管理

用于修改默认的客户端下载提示界面，您可以将默认的下载界面先下载到本地电脑上，然后使用网页编辑软件进行美化或者修改，然后再重新导入到路由。

在修改提示界面时，默认客户端下载地址请不要修改，否则可能引起客户端下载出错。

7.2 进程列表

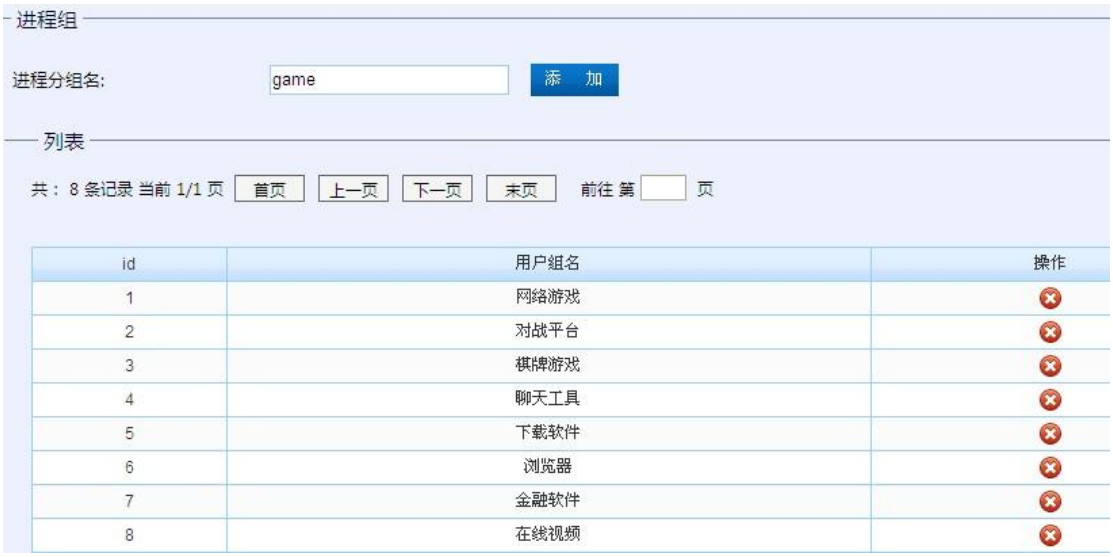
应用程序列表可以用来查看当前应用程序的带宽使用状况。

点击“查看”按钮可以显示当前进程对网络带宽的占用情况。

点击“添加到组”按钮可以将选定的进程添加到任意一个分组里面。

7.3 进程组

分组管理主要是用于为应用程序进行归类，以便进行管理。



进程组可以用于策略路由的规则添加，还可以用于访问控制的规则添加应用。

7.4 进程管理

程序管理可以针对程序的进程名、程序的目录/路径进行分类，结合策略路由的控制，以达到让指定的程序或者指定路径的程序按照设定的线路出去。以达到让游戏与下载分开走，互不干扰的效果。

进程名：添加您需要管控的应用程序进程名或是应用程序的路径目录。（可以是进程名，也可以是程序路径目录，还可以是程序的路径目录+进程名）

所属组：选择所属的组别。组的类别是在“进程客户端-进程组”里进行添加的。

标识：用来区分不同应用程序的信息描述。

类型：程序的匹配类型。

仅匹配进程名：只匹配添加的程序进程名。

匹配路径目录和进程名：匹配程序路径目录跟进程名。

仅匹配路径目录：只匹配程序的路径目录。

添加应用程序之后，我们还需要在策略路由里面设置程序的出口线路，才能达到让指定程序从设定的线路走。

位于列表下方的导入导出功能，可以将您的进程分组信息及进程的配置导出到本地电脑，或者从本地电脑导入到路由器中。如图所示：

下面，我们以设置迅雷软件走 WAN1、所有网络游戏走 WAN2 来举例说明：

首先，我们需要在分组管理里添加新的分组信息，为了便于好记，我们就添加‘下载软件’跟‘网络游戏’两个分组。如图 1 所示:

(图 1)

然后再来添加迅雷的进程名。因为迅雷的进程名是 thunder.exe，所以我们只需要添加进程名就可以了。如图 2 所示:

（图 2）

接下来，添加网络游戏的路径目录。（因为我的网络游戏全部都是安装在“d:\game\网络游戏”目录下，所以直接添加游戏路径更为方便一些。也可以单独添加每个游戏的进程名。）如图 3 所示:

（图 3）

之后我们需要在策略路由中设置迅雷走 WAN1 的规则，如图 4 所示:

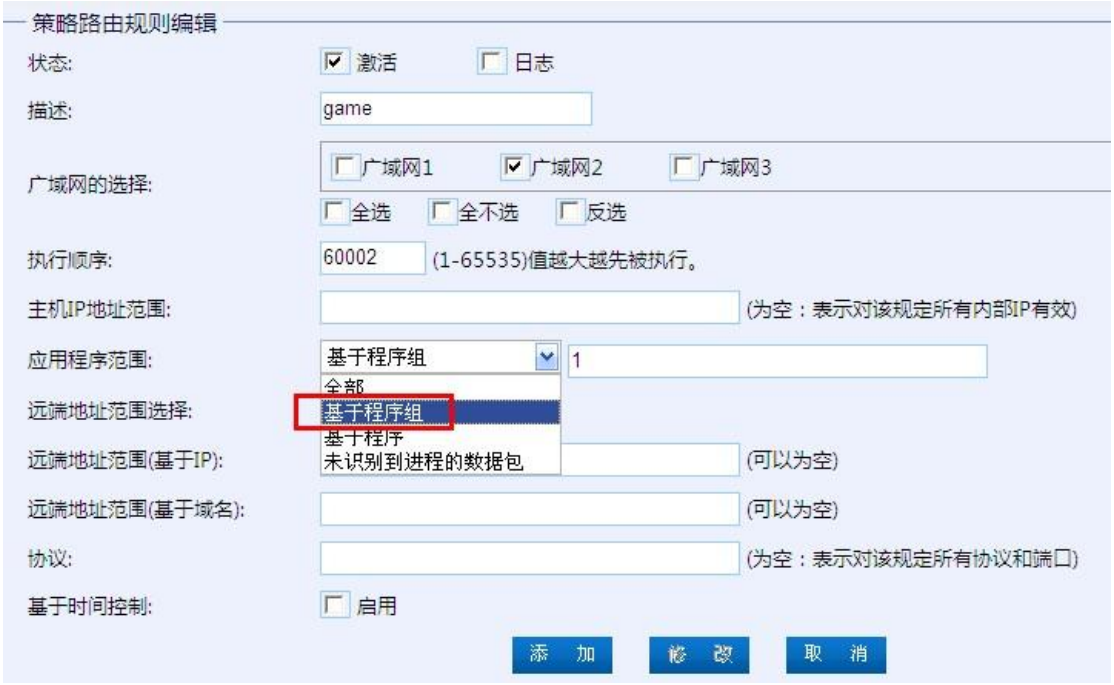
(图 4)

(图 5)

(图 6)

在应用程序范围中选择‘基于程序’，然后点击内容框，在弹出的窗口中勾选上‘迅雷’并确定，如图 5、图 6 所示。最后将此条规则添加到策略规则列表中。

接下来设置网络游戏走 WAN2 的规则，如图 7、图 8 所示:



（图 7）

（图 8）

在应用程序范围中选择‘基于程序’，然后点击内容框，在弹出的窗口中勾选上‘网络游戏’并确定，如图 8 所示。最后将此条规则添加到策略规则列表中。

这样，设置迅雷软件走 WAN1、所有网络游戏走 WAN2 的规则就设置完了，如图 9 所示：

八、认证管理

对 WEB 用户、PPPOE 用户进行管理，并设置用户上网的认证方式，以及对上网通告的管理

8.1 基本设置

用户上网控制主要用于对用户上网的方式做控制，允许 3 种上网认证方式，如图所示：

在“用户上网方式控制”中，默认是不需要认证，即路由器下的所有用户不需要经过任何认证，直接填写正确的 IP 就可以直接上网，跟普通路由器共享上网原理一样。若选择“需要认证”即可激活下面的菜单，出现上图的相关的认证方式选项界面。

允许上网的方式： 选择允许用户上网的认证方式。

ARP 绑定用户直接上网：IP 与 MAC 地址进行绑定过的用户可以直接上网；

PPPoE 用户直接上网：利用 PPPOE 协议拨号到路由器端的用户验证通过之后才可以上网；

允许 Web 认证上网：通过网页认证信息登陆过的用户才可以上网。

关闭 WEB 认证页面时：勾选上，表示在关闭 IE 认证的页面就退出 WEB 认证；若不勾选，即表示，只有在网络被重置或者电脑重启的情况下认证才退出。此功能仅对 WEB 认证有效，不使用 WEB 认证时，此选项无效。

用户账号到期提前通知：账号到期之前提醒用户的通知时间。默认为提醒时间内每天第一次开启网页时出现，直到账号到期（或者延长期限）为止。

用户帐号到期查询间隔：此功能用于检测帐号到期但仍持续在线的用户，在帐号到期以后，达到设置的时间之后，在线用户将被强制踢下线，避免了因为到期用户长期不下线导致的带宽资源浪费。此值可以尽量设置大一点，效果更佳。

用户账号到期提前通知的消息：用户到期的提前通告内容，由用户自行定义，不支持加入 html 网页代码。此通知消息是对快到期的 Web 认证用户才有效的；pppoe 用户的提前通知消息是在“认证页面管理”里面进行修改的。如图所示：

不需要认证的内部主机(基于 IP)：所添加的 IP 用户将不受任何一种认证方式的管制，可以直接上网，即认证排除的内网 IP。

允许访问的外网范围(基于 IP)：没有进行认证的用户也能访问的外网 IP 地址范围。

允许访问的外网范围(基于域名)：没有进行认证的用户也能访问的外网域名。

8.2 认证页面管理

认证页面管理用于对认证用户或者未经认证的用户所弹出的提示页面进行管理，该通告内容允许用户自定义其中的内容或者替换新的通告文件。

管理员联系信息：填入管理员的相关联系信息，通告文件在弹出时会显示出管理员的联系信息资料，方便用户随时联系到管理员。WEB 认证用户在认证之后会提示该信息，如图所示：

认证页面及通告内容用于对认证用户到期发出提醒通告。

WEB **认证页面：**使用 WEB 认证上网时，弹出的用户登录认证的界面。您可以根据需要自行修改登录页面文件，但文件大小不要超过 4K。否则无法导入进去、

账户到期通知：认证用户帐号到期之前的通知提醒页面，用户帐号快到期时，打开网页的时候会自动弹出此通告内容。

阻止上网通告：在开启了认证方式时，没有认证的用户将会收到此通告文件的提醒。

8.3 PPPOE 设置

提供对 PPPOE 拨号服务端的一些参数设置。

PPPoE Server 状态：是否启用 PPPoE 拨号服务端功能。默认为启用状态，若您关闭了此功能，客户机将无法通过 PPPoE 拨号到路由器。

只允许使用 PPPoE 接入：激活之后将只有通过 PPPoE 拨号的用户才能访问到路由器跟上网。（且只能使用下方的‘PPPoE 服务器地址’才能访问路由器 WEB 界面，若使用 LAN 口 IP 将无法访问到路由器 WEB 界面）

PPPoE 服务器名字：拨号服务器的名称，用户可以自定义更改。

PPPoE 服务器的地址：即 PPPoE 拨号用户的网关地址。（PPPoE 用户可以通过此地址来访问路由器配置页面）

PPPoE 服务器的子网掩码：即 PPPoE 服务器的掩码地址，您可以根据环境需求来修改此地址。

DNS 服务器：PPPOE 服务器分配给客户机的 DNS 服务器地址。

空闲检测时间：在达到设定的时间之后，若客户机与服务器之间还没有数据通信，则开始检测客户端是否掉线。默认值为 3 秒。

多少个检测请求未应答则断开连接： 在设定的请求个数之后，客户机若无数据通信应答，则断开其连接。默认值为 3 个。

认证方式：对于不同应用环境，可以采取不同的认证方式类型。对于一般 PC 电脑，都是采用的 PAP 模式。如果是采用下级路由进行拨号，可以把所有的认证方式都勾选上。

8.4 用户管理

针对 PPPoE 用户及 Web 认证上网的用户进行添加、修改或删除的操作，如用户账号的建立、认证方式、到期时间、MAC 地址的绑定、备注信息等设置。

用户状态：勾上即表示禁用此用户，禁用后此用户将不能进行拨号上网（用户当前连接断开以后才生效）。

登陆方式：有 PPPoE 拨号和 Web 认证两种，您可以对不同的用户设定不同的登陆方式。

用户名/密码：为用户创建一个登录的登陆用户名及密码。

MAC **地址**：有不绑定、自动绑定、手动绑定 3 种形式可供选择。

到期时间：可以对用户的上网期限进行限定。点击右边的“…”进行添加。如图所示：

IP **地址**：用于手动给用户指定 IP 地址。默认情况下系统会依照 IP 地址池自动为用户分配一个 IP。

上传/下载速度：对该帐号的带宽使用做以限制，只允许使用指定的带宽速度值。默认为 0，表示不做限制。

速度控制方式：可以选择单独限制或者共享限制。

单独限制：对帐号做单独限制，用户使用的最大速度不超多限制的速度值。

共享限制：对一号多拨的用户有效，可以限制一个帐号在多人共享使用时，多人共享限制的速度值。

允许登陆的用户数：设定该账号可以允许被多少个用户同时登陆使用，即一号多拨功能。（当允许登陆的用户数设置大于 1 时，绑定的 MAC 地址将只会对第一个拨号的用户有效）

备注：对此用户的简单描述，方便管理员进行查看管理。

点击用户列表中的操作栏，可以对账户进行修改、删除及断开等操作，如图所示：

用户列表下方有用户数据导入导出功能按钮，可以将所有的用户数据导出到本地电脑上，或者将本地电脑的用户数据导入到用户列表中，如图所示:

九、VPN 应用

提供点对点、点对网的 VPN 应用设置，包括 PPTP/L2TP、OpenVPN、IPSec 管理、VPN 借线等

9.1 VPN 管理

提供 VPN 借线及 PPTP 连接相关服务。

9.1.1 PPTP 服务

用于管理 PPTP 的 VPN 服务及借线相关。

PPTP 服务：控制 PPTP 服务端功能的开启与关闭。做服务端来使用的时候必须先开启服务，做客户端使用的时候不用开启。

端口：PPTP 连接默认使用的端口，尽量不用去修改，否则可能造成 PPTP 连接失败。

地址范围：服务端分配给客户端的 IP 地址范围。此 IP 是连接 VPN 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障。因 VPN 连接之后会从中分配一个 IP 作为 VPN 网关地址，所以，此地址范围请设置至少 2 个以上的 IP 范围。

分配给客户的 DNS：服务端分配给客户端的 DNS 地址。只有在用到借线或者客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

9.1.2 PPTP 用户

管理 PPTP 的帐号，包括帐号的创建、修改与删除以及帐号类型的设置。

用户状态：勾选上表示禁用此账号。

用户名/密码：为客户端分配的账号及密码。可以由英文字母或数字组成。

指定 IP：如果不想用服务端自动分配的 IP，就可以在此处手动指定一个 IP。（指定的 IP 必须与 VPN 服务端分配的 IP 处于同一个网段内。）

类型：有‘VPN 隧道’和‘VPN 借线’两种模式可以选择。

VPN 隧道：用来连接服务端，与服务端的网络组建一个虚拟的局域网环境，可以共享服务端内部资源。

VPN 借线：借用服务端的线路出口作为网络接口来上网，共享服务端的网络出口。

内网网段：仅隧道模式有用。填入连接 VPN 的客户端的内网网段地址，格式：192.168.1.0/24 （例如：客户端使用的网段是 192.168.10.X，那么就应该填入:192.168.10.0/24）

备注：对添加的用户账户的简单信息描述，由用户自定义。

9.1.3 PPTP 状态

此状态显示目前已经连接上的 PPTP 用户信息及网络流量情况。

9.1.4 VPN 借线

使用路由器作为 VPN 客户端的时候需要用到 VPN 借线功能，可以实现路由对路由的 VPN 连接或者 VPN 借线功能。

选择您要设置的 VPN 接口：选择路由使用的 VPN 接口，最多允许同时连接 4 个 VPN 网络，默认使用 VPN1 接口。

连接类型：选择 PPTP 表示启用 VPN 客户端功能，默认是关闭状态。

出口接口：可以选择用哪个广域网作为 VPN 的出口，请尽量选择带宽大且稳定的线路做出口，以保证 VPN 连接的稳定性。默认是 ALL（表示全部）。

用户名称/密码：填入 VPN 服务端创建的 PPTP 用户名及密码。

服务器地址：VPN 服务端的广域网接口 IP 地址或者动态域名。

MTU 设置：VPN 连接所使用的 MTU 值，默认是 1400。此值一般不做改动，使用默认值即可。

工作模式：有隧道模式与借线模式两种。默认是隧道模式。

隧道模式下，路由只作为 VPN 连接使用，可以共享虚拟网段的内部资源，但不能访问服务端的外部资源（也就是不能使用借线功能）；

借线模式下，路由器客户端可以借用服务端的网络，通过服务端的网络来访问外部资源，但不能访问服务端内部资源。

路由网段：只有在选择隧道模式时此项才生效。这里填写服务端所在的网段（比如，服务器现在是 192.168.2.X 段的 IP，那么这里就填 192.168.2.0/24）。

外网带宽：设置 VPN 线路所占用服务端的带宽值。0 表示不设置，即不限制 VPN 接口的带宽。VPN 接口的出口带宽仍需占用客户端实际的网络带宽资源，能使用的最大带宽取决于客户端的网络出口带宽值大小。

带宽参考值：您可以选择一个参考的带宽来自动填入上下行带宽值。

9.1.5 VPN 状态

用于查看 VPN 客户端与 VPN 服务端之间的 VPN 连接状态。只有当路由作为客户端并与服务端连接以后，才会显示连接状态。

9.2 IPSec 配置

9.2.1 IPSec 网对网

用于管理 IPSec 网对网服务的建立与连接，如果需要使用此功能，需要连接的两边路由器都开启 IPSec 功能。

状态：开启 IPSec 网对网配置。

查看高级配置：显示 IPSec 服务的参数配置。

名称：填写此规则的名称，由英文字母或数字组成。

主动连接：启用 IPSec 网对网的主动连接。

本地隧道接口：选择使用哪个广域网口来进行隧道连接。

本地网络：填写本地的内网的网段。（比如，本地网络现在是 192.168.2.X 段的 IP，那么这里就填 192.168.2.0）。

远程隧道地址：填写对端的路由器的广域网网 IP 地址或者动态域名。

远程网络：填写对端路由器的内网网段。

IKE 验证模式：默认的加密类型。

PSK 密钥：设置密钥的密码。由数字和字母组成。连接隧道的两边路由器必须设置相同的密钥，否则连接不会成功。

9.2.2 IPSec 点对网

状态：启用 IPSec 点对网服务。

本地网络：填写本地内网的网段。（比如，本地网络现在是 192.168.2.X 段的 IP，那么这里就填 192.168.2.0）。

IKE **验证模式**：默认加密类型。

PSK **密钥**：设置密钥的密码。由数字和字母组成。客户端在连接时，必须输入与此相同的密钥。

查看高级设置：显示 IPSec 服务的参数配置。

IPSec 点对网客户端连接需要使用到专门的 VPN 连接软件，推荐使用 ”vpn-client-2.1.7-release.exe “。

9.2.3 L2TP IPSec

状态：启用 L2TP Over IPSec 服务。

L2TP **最大连接数**：允许接入 L2TP 客户端的连接数。（注意：在“L2TP 客户端地址范围”必需与“L2TP 最大连接数”处的值要相对应，且不能和所有级连的路由器内网在同一个网段，否则连接不成功）。

PSK **密钥**：设置密钥的密码。由数字和字母组成，L2TP 客户端连接时需要填入与此相同的密钥。

端口：L2TP IPSec 服务的端口号。默认是 1701。L2TP 连接默认使用的端口，尽量不用去修改，否则可能造成 PPTP 连接失败。

L2TP **客户端地址范围**：服务端分配给客户端的 IP 地址范围。此 IP 是连接 L2TP 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障。

分配给客户的 DNS：服务端分配给客户端的 DNS 地址。只有在用到借线或者客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

L2TP 客户端连接 VPN 时，需要使用系统自带的虚拟专用网络来创建 L2TP 连接。

9.2.4 L2TP 用户

用来创建 L2TP 客户端连接 VPN 时拨号的用户。

用户状态：是否禁用此账号。

用户名/密码：创建 L2TP 连接使用的账号及密码。可以由英文字母或数字组成。

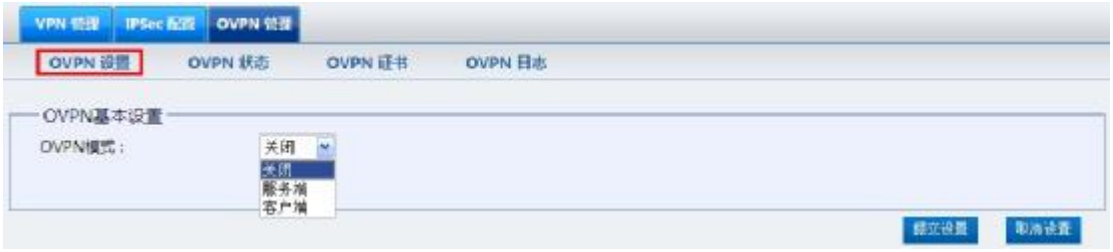
备注：对添加的用户账户的简单信息描述，由用户自定义。

9.2.5 L2TP 状态

主要用于查看客户端与服务端之间的连接状态。只有当路由作为客户端并与服务端连接以后，才会显示连接状态。

9.3 OVPN 管理

9.3.1 OVPN 设置



OVPM 连接模式： 关闭，不启用 VPN 服务； 服务端，将此路由作为 OVPN 连接的服务器端； 客户端，也就是 OVPN 路由客户端。

路由器的 VPN 连接方式分为路由与路由的连接和路由对 PC 机的连接两种：

路由对路由 即网关对网关的连接方式。也就是将其中一端的路由设置为服务端，另一端路的由设置为客户端。在这种连接模式下，两端的路由若外网连接都正常，两者将会自动进行 VPN 连接，VPN 连接成功之后，服务端下面的所有用户与客户端下面的所有用户就组成了一个虚拟的局域网。

路由对 PC 客户机 即路由对客户机的连接方式。就是把路由器作为 OVPN 服务端，然后客户机利用 OVPN 连接软件来与服务端进行连接。在这种连接模式下，客户机必须利用 OVPN 软件手动去连接服务端，VPN 连接成功之后，该客户机就与服务端下面的所有用户组成了一个虚拟的局域网，即加入到服务端的局域网内。

VPN 服务端是提供给客户端做 VPN 连接而用，我们需要在服务端上建立不同的用户，分配给客户端用来连接 VPN。其中分为 PC 客户端的用户建立与路由器客户端的账号建立两种。

在 OVPN 模式中选择‘服务端’，如下图所示：

然后，填写相关数据参数。

协议类型：自定义 OVPN 服务所走的协议。默认为 TCP 协议。

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时。

MTU **设置：**定义 VPN 传送数据的 MTU 值，用于特殊环境中使用，一般保持默认即可。

端口：自定义一个 OVPN 服务使用的端口。默认为 4443，您可以修改为其他未被占用的端口。

VPN **虚拟网段地址/掩码：**自定义一个用来连接 VPN 的虚拟网段地址及子网掩码。（请避开您正在使用的网段。如您正在使用的是 192.168.X.X，请使用 10.X 或者 172.X 的 IP 段）

用户之间互通：即 VPN 客户端与 VPN 客户端之间相互通信的功能。默认允许。

以上已完成了服务端的基本参数设置，接下来我们需要为客户端建立 VPN 连接的账号及密码以供客户端与服务端来进行 VPN 连接。

状态：选中表示激活此账号。

用户类型：请根据用户类型来建立相应的帐号。

客户端是 PC：建立的帐号只能用于 PC 电脑作为客户端使用 OVPN 客户端软件来连接 VPN 时使用。

客户端是路由器：建立的帐号只能用于路由器作为客户端时连接 VPN 使用。

用户名/密码：新建一个客户端用来连接 VPN 的账号及密码。（此账号是客户端路由用来连接服务端而使用的，用户账号可以由用户自行定义，请使用英文或者数字作为用户名/密码）

内部网段 IP/掩码：此项仅对客户端是路由器时适用 。填入您客户端连接 VPN 所用的内部 IP 地址及子网掩码。（此处 IP 不能与服务端内网处于同一网段。如，服务端路由 IP 为 192.168.1.X 段，客户端路由 IP 为 192.168.100.X 段，那么此处就需要填 192.168.100.0）

在路由器 OVN 设置中选择客户端可以使用路由作为客户端来连接 OVPN，其设置方法比较简单，只需要填写几项关键参数就可以了，如图所示：

协议类型：选择 VPN 连接所使用的协议类型，必须与服务端的协议类型一致，否则无法正常连接 VPN。

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时。

MTU **设置**：VPN 连接的 MTU 值大小，可由用户自定义，一般使用默认值即可。

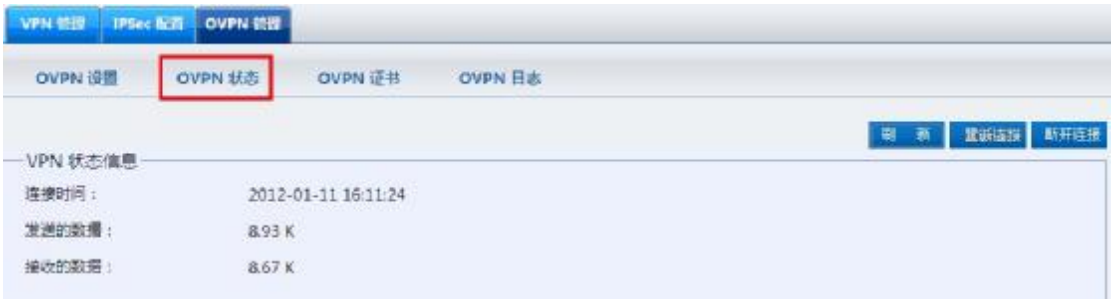
用户名/密码：请填入您在服务端建立的路由客户端用户名及密码，并再次确认密码。

服务器地址：填写您服务端的 WAN 口 IP（外网 IP）地址或者动态域名。冒号后面填入与您服务端相同的协议端口号。

服务器地址备份：当您有多条 WAN 接入时，您可以分别填入其他 WAN 口的 IP 地址或者动态域名，当其中一条线路不通时，另外的线路可以继续保持 VPN 连接，使其不会意外中断；如果您只使用了一个 WAN 口接入，可以不用填写备用地址。

9.3.2 OVPN 状态

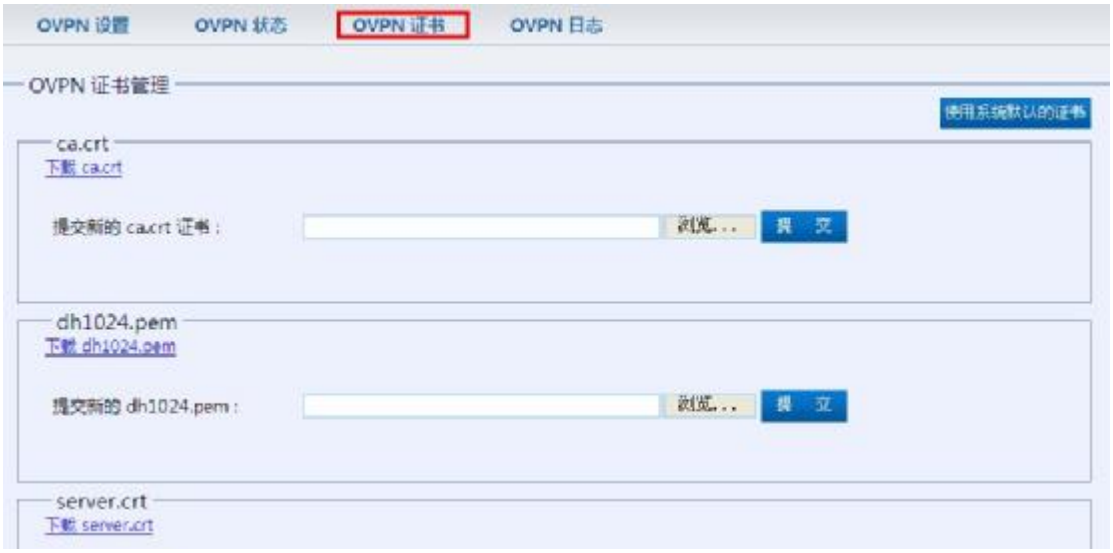
记录 VPN 相关连接的状态，管理员可以由此了解到 VPN 线路的运行状态，以便进行管理。



9.3.3 OVPN 证书

主要用于用户下载原有的证书文件，或者自行导入新的证书。其中，ca.crt 证书文件是 PC 客户端连接 VPN 必须的文件，您可以将其下载下来保存好，以提供给 PC 客户端连接 VPN 时使用。

鉴于稳定性，建议用户使用默认的证书，以免使用自行导入的证书时出现问题。若您自定导入的证书在使用时出现问题，请点击右下方按钮将证书恢复到默认值。



9.3.4 OVPN 日志

主要用于记录 VPN 连接时出现的日志信息。只有在勾选上相应选项之后，才会在日志中记录。


OVPN 设置
OVPN 状态
OVPN 证书
OVPN 日志
OVPN日志
共：244 条记录 当前 24/25 页
首页
上一页
下一页
末页
前往 第 页
刷新日志
删除日志
时间
消息
2012-01-11 16:10:26
SENT CONTROL [UNDEF]: PUSH_REQUEST (status=1)
2012-01-11 16:10:27
PUSH: Received control message: PUSH_REPLY,route 192.168.10.0 255.255.255.0,route 10.98.0.0 255.255.255.0,topology net30,ping 10,ping-restart 60,ifconfig 10.98.0.6 10.98.0.5
2012-01-11 16:10:27
OPTIONS IMPORT: timers and/or timeouts modified
2012-01-11 16:10:27
OPTIONS IMPORT: --ifconfig/up options modified

十、防御配置

设置路由器安全防御信息，包括 ARP 管理与防御、联机数设置、DDOS 防御、访问控制、网址管理等

10.1 ARP 管理

10.1.1 ARP 列表

ARP 列表显示当前局域网连接用户的 IP 及 MAC 信息。

将 LAN 所有未绑定的设为唯一: 将局域网未绑定过的用户一键绑定为唯一类型。

将 LAN 口所有为绑定的设为静态：将局域网为绑定过的用户一键绑定为静态类型。

唯一：指只有 IP 和 MAC 地址对应才能连接网络。

静态：将该 IP 地址指定为只能在该 MAC 地址上使用，但是该 MAC 地址还可使用其他 IP 地址连接网络。

10.1.2 ARP 绑定

ARP 绑定允许用户对局域网 IP 或者广域网 IP 进行手动绑定。

描述：对该条绑定信息的简单文字描述，便于管理员区分。

IP 地址：将要绑定的 IP 地址。

查询 MAC：如果该 IP 地址在线则可以点击该按钮查询到其使用的 MAC 地址。

MAC 地址：需要绑定的 IP 的 MAC 地址。如果用户不在线则需要手动输入。

类型：选择绑定的类型有静态和唯一可选。

接口：如果绑定的 IP 地址属于局域网请选择“局域网”，如果将要绑定的 IP 属于广域网请选择“广域网”。

在列表下方，您可以对所有绑定的 MAC 地址进行导入导出操作，如图所示：

10.1.3 ARP 防御

ARP 用于设定 ARP 主动防御的相关参数。

LAN 口伪网关攻击：限制内部机器伪造路由器 IP 发起的攻击，默认时间间隔是 200ms。

探测 LAN 口非法网关：检测局域网口出现的非法网关（与路由器相同 IP 的设备），默认检测时间是 10s。

处理级别：默认防御级别为中级，您可以根据网络环境做相应调节。

10.1.4 ARP 日志

ARP 日志：当网络出现广播回路，ARP 绑定错误或者 ARP 攻击时，路由器会在日志里面记录相关信息。

10.2 访问控制

10.2.1 访问控制

访问控制方式：设置访问控制的方式，有三种选择：

不启用访问控制：关闭访问控制功能，列表中的所有规则将都不生效；

允许规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则不受控制，直接允许通过；

禁止规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则受到控制，禁止被通过。要单独设置允许通过的，请在规则中添加相应规则来运行其通过。

激活：选择是否激活此规则。

日志：对设置的规则记录日志，可以方便观察规则是否生效。

描述：对此规则的简单描述。

控制方式：控制访问规则是允许通过还是禁止通过。

执行顺序：用来比较多条规则的优先级，值越大越优先执行。当出现有相互冲突的两条规则时，会优先执行数值大的那一条规则。

主机 IP 地址范围：需要进行控制的内部主机 IP 地址范围。

远程地址范围：有基于 IP 和基于域名之分，可以直接填写需要被管控的远端地址 IP 或者域名。

协议：需要控制的协议和端口，可以选择 TCP，UDP 和 ICMP，也可以是内部端口和外网端口。

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

举例说明：

限制 IP 为 192.168.1.10-192.168.1.20 之间的机器只能上 QQ 跟浏览网页，其他机器不做限定，可以做如下设定：

1.选择访问控制的方式为‘允许规则之外的通过’，并点击提交按钮。如图所示：

2.先添加一条禁止 192.168.1.10-192.168.1.20 之间的 IP 访问任何地址的规则，如图所示：

3.再添加一条允许192.168.1.10-192.168.1.20之间的IP访问网页跟QQ的规则。如图所示:

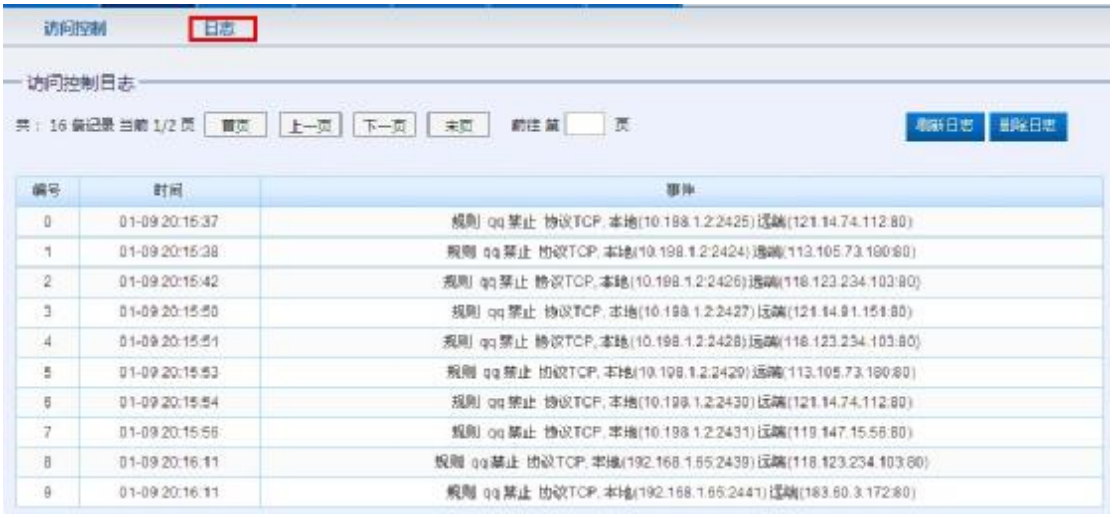
此规则优先级必须高于被禁止的规则，否则此规则设置将无效。

由于大多数网页都是走的TCP协议的80跟443端口，QQ程序一般都是使用UDP协议的8000-8004端口，所以我们将以此为例做限制。需要注意的是，设置协议端口时，我们一般使用的是外部端口，如图所示:

设定完毕之后请点击添加按钮，将规则添加进列表中即可.规则会在添加之后立即生效，不需要重启路由器。所以在做禁止的规则时，请先考虑好是否有正在使用的协议等在控制范围之内，否则一旦设置了禁止的规则，就会对现有的协议使用受到影响。

10.2.2 日志

记录访问控制规则产生的日志记录，需要在添加规则的时候先勾选上日志选项才会记录。



10.3 MAC 过滤

对 MAC 地址进行管理，允许或者禁止该 MAC 地址的用户通过。

MAC 地址过滤的方式：有‘不启用 MAC 地址过滤’、‘允许规则之外的通过’和‘禁止规则之外的通过’3 种选择，请根据需要来进行选择。

不启用 MAC 地址过滤，对列表中添加的所有规则将不做任何控制；

允许规则之外的通过，列表中添加的规则按照控制方式来执行，列表之外的不受限制，直接通过；

禁止规则之外的通过，列表之中的规则按照控制方式来执行，列表之外的所有地址将都被禁止通过。

状态：选择是否激活此规则。

描述：对此规则的简单描述。

控制方式：分为‘允许通过’和‘禁止通过’两类。用户可以选择此规则是否允许通过。

MAC 地址：填入您要管控的 MAC 地址。格式为：00:0A:0B:0C:0D:0E

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

10.4 连接限制

连接数限制可以控制整个网络对外的连机数量。若对单个 IP 的连接数进行管控可以控制内网的计算机最多能同时建立的连接数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出连接数的软件提供了非常有效的管理。设置恰当的允许连接数可以有效控制 P2P 软件下载时所能产生的连接数，相对也使带宽使用量达到一定的限制。另外，若内网有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。

默认主机连接数限制：所有用户默认主机的连接数限制。当客户机连接数满了之后，由于新的连接出不去，就形同断网，所以请谨慎设置。

激活：是否启用规则，激活之后规则才会生效。

描述：对规则的简单描述。

主机 IP 地址范围：对指定的 IP 地址范围单独设置连接数规则，那么这些 IP 地址将只受规则限制，不受默认主机连接限制。

连接数限制：可以单独对 TCP/UDP 连接限制或者做全部的限制。

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

10.5 DDOS 防御

对用户的并发连接进行限制。并发连接指一定时间内用户发起的连接的总数。

默认并发连接数：单位时间内可以发起的连接总数。规则之中的用户不受默认并发连接影响。

默认并发连接间隔时间：并发连接单位时间。

激活：是否启用规则。

描述：对规则的简单描述。

主机 IP 地址范围：需要单独控制并发连接的主机对象。

并发连接类型：可以单独选择 TCP，UDP 或者所有。

并发连接数：单机所允许的最大并发连接数条目。

并发连接间隔时间：相应的间隔时间，单位为秒。

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

10.6 Ping WAN 口

路由器默认在外网是不可以 Ping 通 WAN 口的，如果需要在外网能够 Ping 通 WAN 口，请勾选此选项并提交设置。

10.7 联线数设置

主要用于设置路由器最大对外联机数目，默认连接数是根据机器内存自动获取的，默认情况下不需要做修改。

十一、USB 存储

在路由上插入 USB 设备，实现文件、资料的共享，无需单独建立文件共享服务器。

11.1 设置状态

设备状态可以查看到当前已连接的 USB 设备信息，在 USB 不使用时，请将 USB 设备弹出。

11.2 共享服务

USB 设备连接之后，存储状态将显示连接信息。路由器默认已经将 USB 设备的共享开启。

您只需要在地址栏输入共享地址即可访问到 USB 共享数据，私有目录地址需要登录才可以进程访问，默认用户名为：login 默认密码为：123465，您可以手动修改登录密码。

十二、高级配置

设备高级功能的相关参数设置，包括端口映射、端口镜像、远程访问、静态路由、DNS 代理、通告系统及域名重定向等

12.1 策略路由

12.1.1 负载均衡

负载均衡：用于设置线路的均衡模式及侦测方式、均衡权值等。

负载均衡模式分为 IP 地址均衡跟联机数均衡两种。

依 IP 地址均衡：依据内部用户的 IP 地址来决定线路的负载均衡。

依会话数均衡：依据用户的对外联机数来决定线路的负载均衡。

IP 均衡的作用，每条线路上的 IP 用户数目是等同的；会话数均衡的作用，每条线路上的对外联机数目是等同的。当使用会话数均衡的时候，就是将外网的几根线路都叠加起来，相当于是合并了总带宽。

选择广域网：选择您要设置的广域网接口。

是否参与默认均衡策略：勾上即表示参与，若不需要让此线路参与均衡，去掉勾即可。不参与均衡的线路将只接受策略路由里绑定的规则数据走向，若策略路由里也没有绑定数据走该线路，那么该线路将不会有数据流量。

均衡的权值：此值主要用于跟其他线路的均衡做比较，系统会根据值的大小来决定线路的负载大小，默认值是依靠带宽值的大小来自动判定，需填写出口带宽值才有效。若改为自定义，请根据线路的权衡比例来设置此参数，参数越大，通过的数据/用户就会越多。

线路侦测：启用线路侦测功能。激活时下面的选项才起作用，否则无效。线路侦测主要用于检测线路的通畅与否，对于多线路环境，若其中一根线路侦测失败，系统默认会将该线路移除，线路上的所有会话将会自动转移到另外侦测成功且参与均衡的线路上去。

侦测间隔：线路自动侦测的中间间隔时间。

侦测次数：线路侦测的次数。

当线路连接失败时：当线路检测失败时，对该线路的处理方式。

移除该线路并记录日志：将此线路删除，并记录到日志中，该线路上的所有连机将自动转移到其他线路上；仅记录到日志：仅在日志中记录下此次掉线日志，不删除该线路。

下载流量超过*时不进行线路侦测：下行流量超过设置值的时候才进行线路侦测。

侦测默认网关：勾选上即表示侦测此线路的外网网关。内容为空，表示侦测默认的网关。有些 ISP 的默认网关可能不允许 ping，那么可以自己手动指定一个其他的广域网地址来测试。

侦测远程服务器：填入一个稳定的域名或者广域网 IP 地址用于检测线路的通断与否。

注意：线路侦测默认是以 ping 来判断线路的通与断，所以，在填写侦测 IP 或者服务器地址的时候，请尽量选择一个长期稳定在线的地址。

12.1.2 地址范围

用于多条运营商线路的环境中，使用策略路由。只要选择好相应的线路，并设置好策略方式即可实现电信网通分开走，互不干扰。

您可以在此界面自行更新电信/网通等的地址范围，或者自定义添加新的地址范围段。

12.1.3 策略路由

策略主要用于设置您内网用户对不同线路的走向。对于单线路用户，则无需对此功能进行设置。

状态：勾选表示激活此条规则。

日志：是否将产生的信息记录到日志中。

描述：对此规则的信息描述。

广域网的选择：选择您需要设置的广域网接口。

执行顺序：以 1-65535 之间的数字来表示规则的执行顺序，数值大的规则优先执行。

主机 IP 地址范围：选择您需要设置的 IP 地址范围。（若为空，表示对内网所有用户都有效）

远端地址范围选择：选择您需要设置的远程地址范围。

远端地址范围（基于 IP）：填入您要设置的远程地址 IP 范围。

远端地址范围（基于域名）：填入您要设置的远程地址域名。

协议：添加您需要设置的协议类型。

基于时间控制：是否启用按时间段来控制规则生效。

在列表下方，您可以选择将设置的策略路由规则导入导出，如图所示：

12.1.4 线路状态

显示每根线路的在线状态及主机数、会话数信息。

主机数信息只有在均衡方式为 IP 均衡时才会显示，会话数信息是会实时显示的。

12.1.5 日志

用于记录广域网口线路的工作状态，如果线路有掉线等情况，将会在此日志里显示出来。

如果在策略路由中添加规则的时候，勾选了日志，那么策略规则产生的日志信息将会在这里记录下来。

12.2 通告系统

12.2.1 文件编辑

用于用户对现有的通告文件做修改、添加、删除等操作。

导入的通告文件必须是‘.htm’格式的，且大小不能超过 4K，新的通告文件导入之后将会自动替换掉旧的通告文件。通告文件最多可以导入四条。

12.2.2 规则管理

通告系统是以 Web 页面的形式弹出的，设置的弹出窗口将只在用户开启浏览器访问英特网的时候将页面自动转向到您设置的通告页面。

描述：对此规则的简单描述。

激活：勾上表示启用此规则，不启用则规则设置无效。

日志：是否记录到日志。

间隔时间：通告文件弹出的间隔时间，单位为分钟。（注：通告文件默认不会象弹窗广告那样自动弹出，只有在开启网页的时候才会将网页强行转向到指定的通告页面。）

用户类型/范围：选择通告文件的适用对象。有“基于 IP 地址”（针对指定 IP 用户弹出通告）、“基于 MAC 地址”（对绑定/未绑定用户弹出通告）、“基于接入类型”（对拨号用户/非拨号用户弹出通告）三种选择方案。

通告内容：选择您导入的通告文件或者直接使用外部 URL 地址。（建议使用本地导入的通告文件，因为外部 URL 地址开启速度会受到网络影响。若外部地址访问超时，用户会误以为网络不正常。）

基于时间控制：启用之后设定的规则将只会在指定的时间段内生效。

设定完毕之后点击‘添加’按钮，将规则加入列表之中。

12.2.3 日志

记录通告管理系统产生的一些日志信息。

只有在勾选了通告规则中的日志选项时，这里才会显示出通告的日志信息，否则不会显示。

12.3 端口映射

12.3.1 端口映射

使外网可以通过 IP 地址或域名访问到内网机器映射出去的端口。

激活：启用此规则。

描述：对规则的简单描述。

协议：分为 TCP、UDP、TCP 和 UDP。

源地址限制：限制只有处于填入的 IP 或者域名所在的网络才可以访问路由映射出去的端口。不填即表示所有广域网的 IP 都能访问到映射出去的端口。

外部端口：来自外部广域网的 IP 访问映射机器时的端口，可以自定义，但不能跟其他规则的端口相冲突。

内部端口：内部局域网络访问映射机器时使用的端口，一般由软件本身决定。若需要映射的内部端口跟外部端口一样，则可以不用填写内部端口。

内部地址：内网需要映射的机器 IP 地址。

网口设置：选择您要映射的广域网接口，默认为所有接口 ALL。

举例：将内部机器 192.168.1.251 的 TCP-3389 端口映射为外网的 TCP-63890 端口，那么只需要按照上图这样设置就可以了。

内部机器访问 192.168.1.251 机器时使用 192.168.1.251:3389 这样的方式；外部广域网网络访问映射机器时就需要使用 WAN 口 IP:63890 这样的方式来访问映射机器了。

12.3.2 DMZ 设置

当您将内部的某台机器 IP 填入到此 DMZ 选项时，路由器 WAN 口的合法 IP 地址会直接对应给此台机器使用，也就是说从 WAN 端进来的封包，若是不属于内部的任何一台机器，都会传送到这台机器上（也就是把此机器完全的映射出去）。

启用 DMZ：勾上即表示启用此功能。
目的地址：需要设为 DMZ 的内部机器 IP 地址。
源地址限制：是可选项，允许外部广域网口访问的地址或地址段。

12.3.3 端口触发

触发端口是初次 LAN 连接至 WAN 的“触发”。如果触发启用,WAN 至 LAN 的映射端口将被打开，这些端口将在不使用时几分钟后被自动关闭。

启用：启用此规则。
描述：对规则的简单描述。
协议：分为 TCP、UDP、TCP 和 UDP。
触发端口：内部访问触发条件的端口。
映射端口：触发之后在广域网口对其开放的端口，WAN 可见。

12.3.4 UPNP 设置

UPnP(Universal Plug and Play)是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的计算机有支持 UPnP 机制的话，而且您的计算机 UPnP 功能有开启，您可以将路由器的 UPnP 功能启动。开启 UPNP 之后，对 P2P 类的下载软件有一定加速作用，但同时对您的网络也会产生更大的负荷，过多的 P2P 下载将会影响到您的网络正常使用，请酌情使用此功能。

启用 UPNP：启用此功能。
广域网接口：选择需要设置的网络接口
在网络中显示：勾上之后需要自动映射端口的应用类型软件就会在列表中显示，便于管理员查看使用的软件类型。

12.4 端口设置

用于强行修改路由接口的工作模式，一般情况下不需要修改工作模式，否则可能引起接口工作不正常。

点击列表中操作栏对应的网络接口，可以修改端口的工作模式。

提供四种工作模式供选择：10M/全双工、10M/半双工、100M/全双工、100M/半双工。

通常情况下网络接口之间自动协商工作模式，用户不需要手动配置，保留“自动”即可。

12.5 WAN 口数

该功能可以把不需要用到的 WAN 口变换成 LAN 口来使用，允许设置的最大广域网数量不超多默认广域网数量。

设置需要的广域网之后提交设置，在重启路由之后设置才会生效。

12.6 路由表

所谓路由表，指的是路由器或者其他互联网网络设备上存储的表，该表中存有到达特定网络终端的路径，在某些情况下，还有一些与这些路径相关的度量。路由器的主要工作就是为经过路由器的每个数据报寻找一条最佳传输路径，并将该数据有效地传送到目的站点。

12.6.1 当前路由表

当前路由表是路由器当前自动生成的静态路由表：

此路由表是系统自动生成的，提供给用户查看，不可以修改。

12.6.2 静态路由表

在一些特殊环境中，我们也需要手动去指定静态路由表的走向，此时，我们需要手动去添加静态路由表，如图所示：

举例：如 wayos 路由下层挂接有一台三层交换机，交换机的 IP 为 192.168.1.244，该三层交换机下发的有一个 172.15.2.1/24 的网段，三层交换机下的主机使用 172.15.2.X 网段的 IP 上网，并使用 172.15.2.1 作为网关地址，那么，我们就需要添加如上图所示的静态路由，才可以使三层交换机下的主机正常上网。

12.7 DNS 代理

12.7.1 DNS 代理

DNS 代理功能可以缓存最近一段时间之内路由解析的域名与 IP 对应关系表，当用户下次访问“DNS 缓存列表”中的域名时，路由会优先读取缓存列表里的对应 IP 地址，这样便加快了网页访问的速度。

DNS 代理：勾上表示启用此功能，默认为开启。有些特殊环境可能解析方式不一样，若有网页不能解析的情况，我们可以尝试关闭此功能。

老化时间：域名解析的 IP 对应关系在 DNS 列表中缓存的最大时间。

12.7.2 DNS 缓存

记录下所有用户访问的站点信息，但只显示 DNS 设置的老化时间之内所访问的域名，超过时间的将自动老化掉。

12.8 访问设置

对路由器 WEB 界面的访问权限设置，包括用户名/密码的修改、管理员用户及普通用户的修改及远程访问功能的开启与关闭。

HTTP 访问端口：本地局域网访问路由器时的端口。默认为 80.

远程访问：勾上表示激活远程访问。激活之后，在广域网也能访问到您的路由器 WEB 控制界面，方便管理员进行远程维护。默认为不启用。

远程访问端口：广域网远程访问路由 WEB 控制界面时的端口。默认为 8080.

管理员/密码：自定义您的管理员账户与密码。管理员具有对路由器的最高管理权限。

启用 guest 用户：是否启用 guest 用户。Guest 用户只能查看路由设置，不能对路由设置做任何更改。默认不启用。

guest 用户/密码：自定义您的 guest 用户名及密码。

管理员用户可以修改路由器任何设置，guest 用户只能查看设置，不能修改设置。忘记管理员用户/密码之后只能通过按下 reset 按钮来恢复到出厂默认值，请牢记您的管理员用户名及密码。默认管理员用户名是 root 密码是 admin;guest 用户名与密码都是 guest。

12.9 端口镜像

端口镜像功能主要用于监控端口数据流量，以方便管理人员对网络数据进行分析。

状态：选择是否启用端口镜像功能。

选择镜像的数据方向：选择监控的数据包走向，出去的数据或者进来的数据，或是所有的数据。

镜像出口方式：选择是镜像到主机 ip 或者镜像到端口。

将数据包镜像到内部主机的 IP：设置一个您需要用来作为监控的主机 IP 地址，选择“镜像到主机 IP”时有效。

选择镜像的端口：选择镜像的端口，选择“镜像到端口”时有效。

十三、系统维护

管理路由相关参数设置，包括 ping 检测、网络唤醒、固件升级、系统参数管理

13.1 Ping 检测

用于方便管理者了解网络对外联机的实际状况，可以借由此功能判断网络的状况。

输入地址：填写您需要检测的 IP 或者域名。

网络接口：指定您需要检测的网络接口，如果留空，表示从默认的路由出口进行检测。

Ping 包计数：ping 数据包的检测个数。

Ping 包大小：每个 ping 数据包的大小限制。

13.2 网络唤醒

此功能主要用于远程开启计算机而用（被唤醒的计算机必须先开启远程唤醒设置）。

将需要远程唤醒的机器 MAC 地址填入“MAC 地址列表”栏，然后点击“立即唤醒”按钮。如果您的计算机支持远程唤醒，而且已经开启了远程唤醒功能，那么远程的计算机将会被唤醒。

13.3 系统控制

用于将路由参数导入导出，恢复默认参数以及对路由执行重启操作。

保存参数：保存您的路由器配置参数数据。以备路由器调试后出现问题时能及时恢复到以前的状态。

恢复系统参数：将您预先保存的系统配置文件导入到路由器（配置文件为.cfg 格式的）。请不要将其他路由器的配置文件导入到本路由器，否则将导致路由器不能工作。

恢复默认设置：选择“恢复路由默认设置“，并点击确定。恢复之后路由器会自动重启，重启完之后请使用默认 IP 及用户名/密码登录路由。路由器默认 IP：192.168.1.1，默认用户名为 root 密码为 admin。

重启路由器：点击“重启路由器”按钮，在弹出的对话框中选择“是“，路由将会重新启动一次

13.4 固件升级

该界面可以对路由器进行固件升级操作及软恢复操作。如图所示：

固件升级：升级前请先确认好路由器的当前版本，看是否需要进行升级操作。点击‘浏览’按钮，选择新版本的存放路径之后，按下‘升级’按钮开始升级操作。升级时间一般会在一分钟左右完成，各型号升级时间也不一致。

？ 温馨提示:

升级路由器的时候，请不要刷新页面，并且保证机器在不断电的情况完成升级操作，否则将造成路由器升级失败！请尽量选择本地升级路由器，远程升级路由器受到网络影响容易导致升级失败！

13.5 授权激活

在此界面，您可以导入您所购买的授权文件。在未导入授权的情况下，您只能接入 4 台客户机，如果需要接入更多的机器，请购买正式授权。

联系我们：

更多有关 WayOS 产品技术信息可以登录 WayOS 官方网站，或者联系 WayOS 售后技术部。

官方网站：http://www.wayos.cn

官方论坛：http://bbs.wayos.cn

服务热线： 400-6313766

技术支持：028-86962416、84191922

资料共享：ftp://www.wayos.cn