

TG-NET 路由器使用手册

感谢您使用 TG-NET 系列路由器，为了更好的使用，请您详细阅读以下文档，如有疑问请咨询当地技术员，或者通过 www.tg-net.cn 获取帮助，我们将竭诚为您服务。

以下条款最终解释权归 TG-NET，如有变更，请谅无法告之。

版权声明

深圳万网博通科技有限公司©2015

版权所有，保留一切权利。

没有经过本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或者全部，并且不得以任何形式传播。

目录

TG-NET 路由器使用手册	1
版权声明	1
目录	2
一、设备安装使用向导	9
1.1 安装注意事项	9
1.2 设备使用说明	9
1.3 上网基本设置	10
1.3.1 登陆路由器的 web 管理界面	10
1.3.2 TG-NET 路由器设置上网	16
二、快速配置向导	19
2.1 快速向导	19
三、常用操作	22
3.1 外网配置	22
3.1.1 拨号上网	23
3.1.2 固定 ip	23
3.1.3 DHCP 上网	24
3.2 内网配置	24
3.3 端口映射	25
3.4 智能流控	25
3.5 多线策略	26
四、系统状态	26

4.1 概览	26
4.2 路由	27
4.3 系统日志.....	29
4.4 实时监控.....	29
4.5 主机监控.....	30
4.6 应用统计.....	31
4.7 QQ 在线列表	32
4.8 接口概览.....	33
4.8.1 硬件接口	33
4.8.2 虚拟接口	33
4.8.3 历史流量视图	34
五、网络设置	35
5.1 接口概览.....	35
5.2 外网配置.....	35
5.3 内网配置.....	35
5.4 DHCP	35
5.4.1 DHCP 设置.....	35
5.4.2 多 LAN 扩展 DHCP	36
5.4.3 DHCP 静态分配	37
5.4.4 DHCP 静态批量配置.....	37
5.4.5 DHCP 活动客户端	38
5.4.6 DHCP 检测.....	38
5.5 主机名.....	39
5.5.1 主机别名	39

5.5.2 别名批量	39
5.5.3 主机域名	40
5.6 静态路由.....	40
5.7 动态域名.....	42
六、 网络安全	42
6.1 ARP 绑定.....	43
6.2 ARP 安全.....	45
6.3 端口映射.....	46
6.4 连接数限制	50
七、 多线设置	51
7.1 多线策略.....	51
7.1.1 多线设置	51
7.1.2 应用分流	53
7.1.3 策略路由规则.....	55
7.1.4 线路侦测	56
7.2 单线多拨.....	57
7.3 WAN 口扩展.....	58
八、 QOS 流控	59
8.1 智能流控.....	61
8.1.1 智能流控	61
8.1.2 例外	61
8.2 固定流控.....	62
8.3 QOS 高级页面	63
九、 分组管理	64

9.1 时间组.....	65
9.2 地址组.....	66
9.3 端口组.....	67
9.4 应用组.....	68
十、上网行为管理.....	70
10.1 一键管控.....	70
10.1.1 一键管控.....	70
10.1.2 上网行为管理的高级设置	70
10.2 QQ 在线列表	72
10.3 QQ 白名单.....	72
10.4 URL 重定向	73
10.5 网址过滤.....	74
10.5.1 网址过滤	74
10.5.2 网址分类库	74
10.5.3 白名单.....	75
10.6 防火墙规则	75
10.7 WEB 访问记录	77
10.7.1 上网记录配置.....	77
10.7.2 上网记录查询.....	77
十一 虚拟专用网.....	78
11.1 PPTP 服务器	79
11.2 PPTP 客户端	80
11.3 IPSec.....	81
11.3.1 IPSec 隧道	81

11.3.2 IPSec	82
11.3.3 IPSec 状态	83
11.4 L2TP 服务器	83
11.5 L2TP 客户端	84
十二 认证管理	85
12.1 通用公告	85
12.1.1 通用公告	85
12.1.2 白名单	87
12.1.3 在线用户	87
12.2 PPPoE 服务器	88
12.2.1 服务器设置	88
12.2.2 用户管理	88
12.2.3 账户批量导入	89
12.2.4 在线用户	91
十三 AP 管理	91
13.1 系统管理	91
13.1.1 系统设置	91
13.1.2 AP 升级	91
13.1.3 AP 重启	92
13.1.4 恢复出厂	92
13.2 监控统计	92
13.2.1 AP 信息	92
13.2.2 AP 状态	92
13.2.3 用户信息	93

13.3 配置管理.....	93
13.3.1 无线模板	93
13.3.2 AP 配置列表.....	94
十四、 无线设置.....	94
14.1 基本设置	94
14.1.1 网络设置.....	94
14.1.2 安全设置	95
14.2 客人网络	95
14.2.1 网络设置	96
14.2.2 安全设置	96
14.3 高级设置	96
14.3.1 设备设置	96
14.4 用户状态	97
14.4.1 用户列表	97
十五 高级配置	97
15.1 接口高级设置	97
15.2 接口模式.....	98
15.3 防二级路由	99
15.4 共享破解.....	100
15.5 端口镜像.....	100
15.6 VLAN	101
15.7 弹性端口	102
十六、 系统管理.....	104
16.1 系统设置.....	104

16.1.1 基本设置	105
16.1.2 日志	105
16.1.3 Web 界面参数设置.....	105
16.2 路由密码.....	106
16.3 定时任务.....	107
16.3.1 线路切换.....	107
16.3.2 定期重启	108
16.3.3 定期升级	108
16.3.4 定期特征库更新.....	108
16.3.5 定期运营商路由表更新	109
16.4 诊断工具.....	109
16.5 新系统诊断	112
16.5.1 新系统诊断	112
16.5.2 游戏诊断	112
16.6 配置导入导出	113
16.6.1 配置的导出	113
16.6.2 导入配置文件.....	114
16.7 恢复出厂设置	114
16.8 顺网合作.....	115
16.9 web 访问管理	116
16.10 特征库升级.....	117
16.11 固件升级	118
16.11.1 在线升级.....	118
16.11.2 本地升级	119

16.12 重启	120
十七、退出	121

一、设备安装使用向导

1.1 安装注意事项

TG-NET 路由器，要求在标准 220v 市电 情况下使用，符合国家规定的网
络设备使用点标准，请接标准的电源。

1.2 设备使用说明

TG-NET 路由器，请您安装要求接好电源线，设备通电会自动启动，启动过程中，
指示灯会闪烁（启动过程中自检，属于正常现象），启动完成后，系统电源指示会呈
现绿色，系统指示灯也是绿色，有较慢的闪烁，说明设备正常启动。

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，用来将设备配置恢复到出厂预设值。

Console：高级配置实用接口。

指示灯示意图：

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亮。

WAN：WAN 口指示灯。灯亮表示该 WAN 口线路已连通。

LAN：LAN 口指示灯。灯亮表示 LAN 口线路接通。

1.3 上网基本设置

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。

路由器的 LAN 口的默认 IP 地址是 192.168.1.1。首先需要将您的电脑与路由器的 LAN 口用网线连接起来，并将电脑网卡的 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：

1.3.1 登陆路由器的 web 管理界面

1.3.1.1 windows xp 设置

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）。

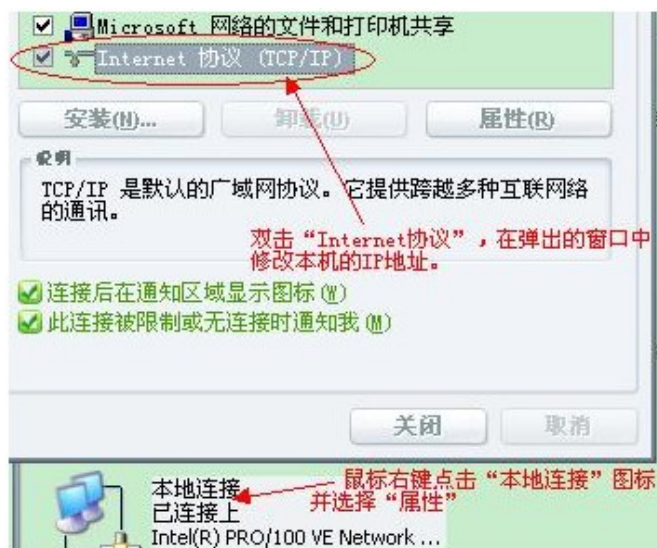


(图 1)



(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：



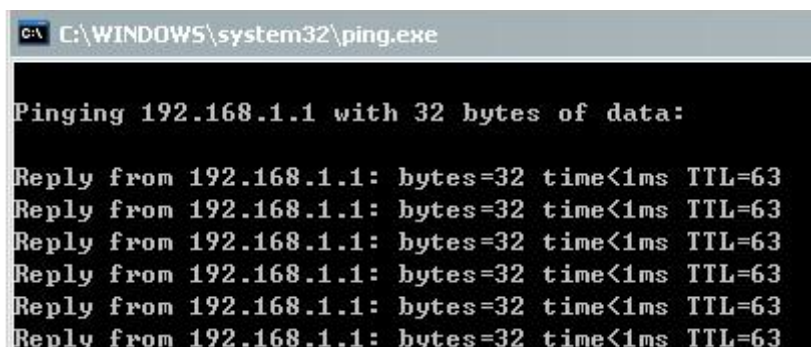
(图 4)

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。

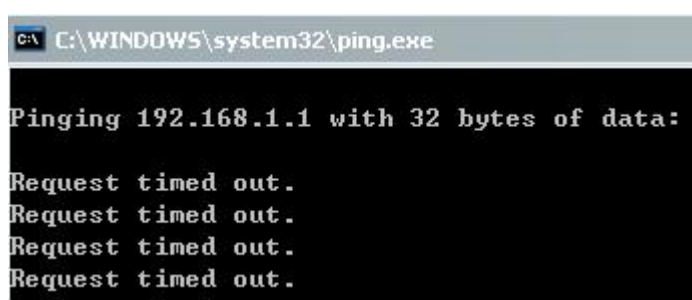


```
C:\WINDOWS\system32\ping.exe

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
```

(图 6)



```
C:\WINDOWS\system32\ping.exe

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

(图 7)

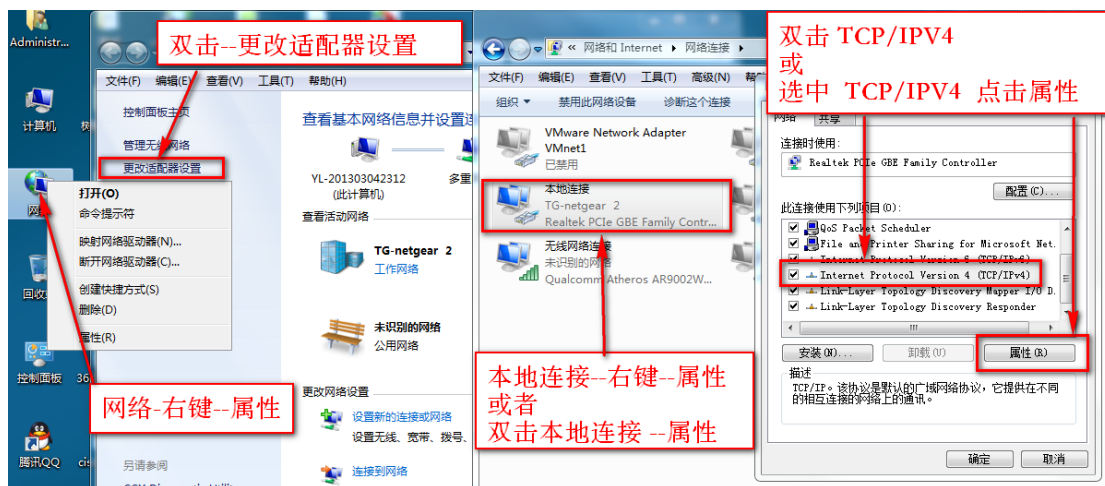
当您与路由器正常连接以后，您就可以通过浏览器（建议是谷歌浏览器或其他浏览器的极速模式），在地址栏输入 192.168.1.1（路由器的默认 IP）进入路由器 WEB 登陆界面

路由器默认的用户名是“**admin**”密码为“**admin**”（您可以在‘系统管理-确认密码’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，通常您必须通过路由器的 **reset** 键恢复默认配置，但本司有些高端型号的路由器没有 **reset** 键，此时必须进入控制台恢复出厂设定值才能重新登陆。

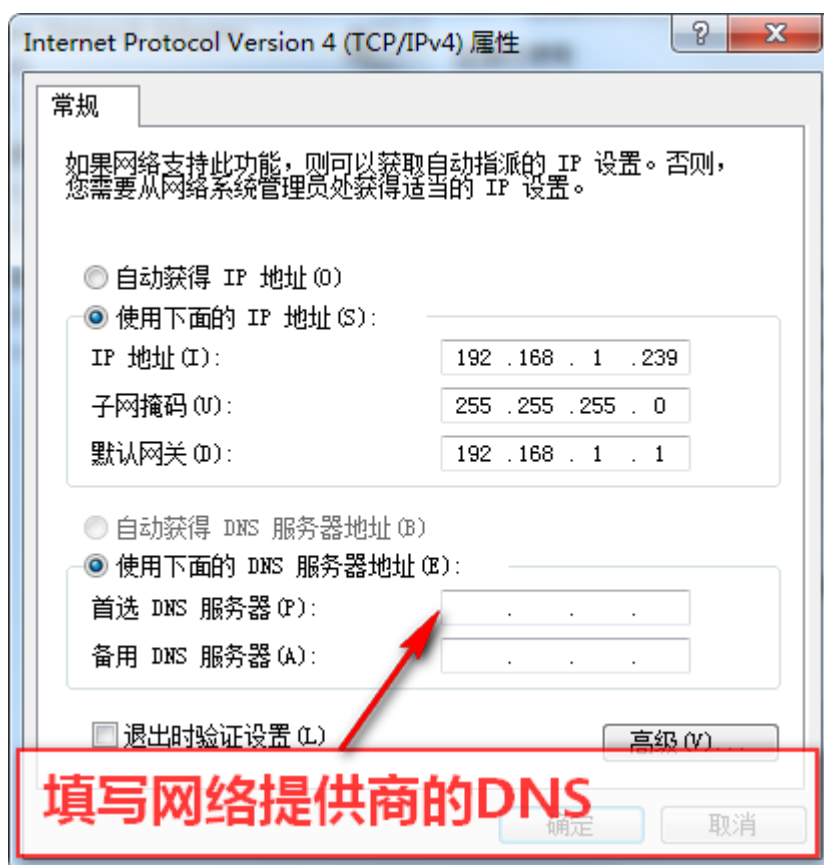
1.3.1.2 windows 7 设置

鼠标右键点击桌面“网络”图标，选择属性，打开‘网络共享中心’菜单，如图 9 所示，（或者点击“开始-控制面板-网络共享中心”也可以打开）。

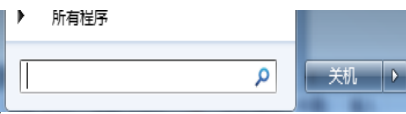


(图 9)

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你的 DNS 地址，若不清楚，可以直接填网关 IP，如图 10 所示：



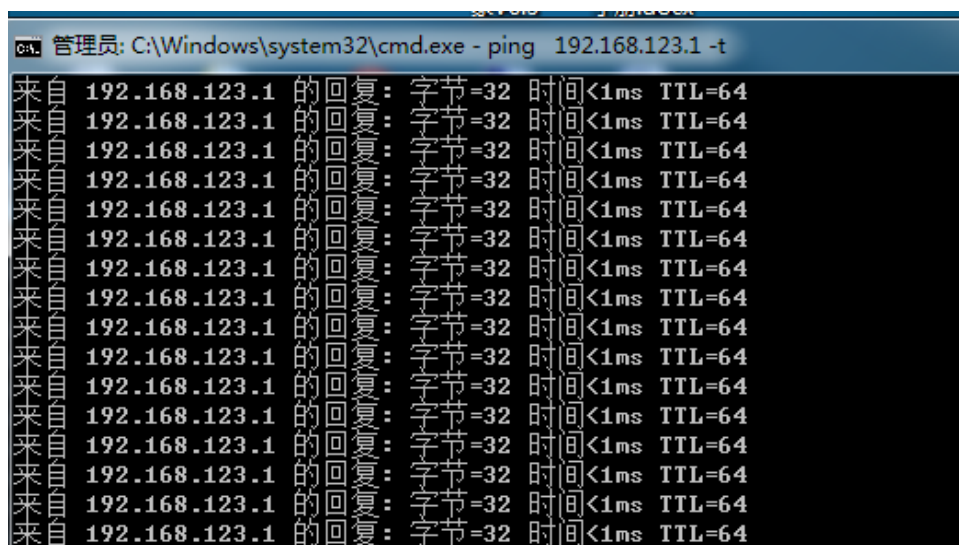
(图 10)

然后在桌面左下角，点击  图标，在  输入 'ping 192.168.1.1 -t' 看看线路是否通畅。如图 11 所示：

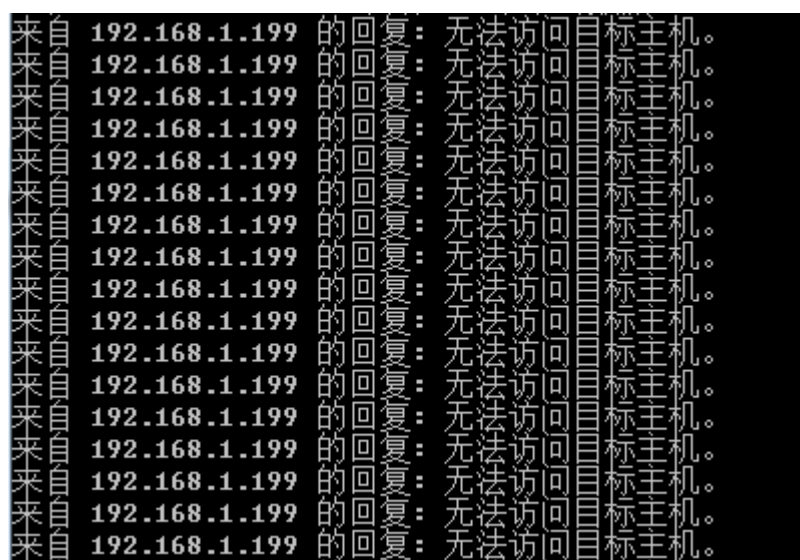


(图 11)

若显示图 12 所示的结果，则表明网络连接正常；若显示图 13 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 12)



(图 13)

当您与路由器正常连接以后，您就可以通过浏览器（建议是谷歌浏览器或其他浏览器的极速模式），在地址栏输入 <http://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 14 所示的登陆画面：



(图 14)

路由器默认的用户名是“**admin**”密码为“**admin**”（您可以在‘系统管理-确认密码’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，通常您必须通过路由器的 **reset** 键恢复默认配置，但本司有些高端型号的路由器没有 **reset** 键，此时必须进入控制台恢复出厂设定值才能重新登陆。

1.3.2 TG-NET 路由器设置上网

登陆路由器以后，我们只需要设置好路由器 WAN 口及 LAN 口相关参数即可正常连接 Internet。我们常见的外网接入方式主要有三种：一种是固定 IP 接入；第二种是自动获取 IP；另一种是 PPPoE 拨号接入。

1.3.2.1 配置 wan 口参数

一般情况下，我们先设置好 wan，让路由器能够上网，网络设置---外网设置

上网的方式，PPPOE 拨号（或 ADSL 拨号），DHCP 上网（自动获取 ip）上网，固定 ip，根据您的情况选择符合您的上网设置即可。

选择运营商提供的上网方式按下图设置即可：

拨号上网

快速向导

常用操作

系统状态

网络设置

网络安全

多线设置

QoS流控

分组管理

上网行为管理

AP管理

认证管理

虚拟专网

高级设置

退出

线路类型: PPPoE拨号(或ADSL拨号)

用户名: [输入框]

密码: [输入框]

MAC地址: [输入框]

选择上网接入服务提供商: 中国电信

上网类型及带宽: 光纤-10M

参考上行带宽: 937.5

参考下行带宽: 937.5

需要配置第2线路: [复选框]

红色方框中信息由运营商提供

此处必须填正确

上下行带宽建议设置为总带宽的0.9~0.95, 预留部分带宽用于防御突发数据

勾选此项可以配置wan2, 不勾选则跳到内网配置界面

注意事项：

1. 上网服务提供商和带宽信息必须填写准确如果分类中没有的，勾选其他；（比如长城宽带）
2. 上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置高于 0.95 的系数。上行、下行总带宽单位为千字节每秒，即 KB/s，一般是标称带宽乘以 100 来计算，比如 10M 光纤，上下行总带宽是 10*100，即 1000KB/s，考虑预留一些带宽，推荐设置 937KB/s。一般而言，选择“上网类型以及带宽”，会自动填充“参考上行带宽”和“参考下行带宽”，系统会自动考虑预留并计算带宽。只有找不到合适的类型时，才需要进行自定义。

固定 ip

快速向导

常用操作

系统状态

网络设置

网络安全

多线设置

QoS流控

分组管理

上网行为管理

AP管理

认证管理

虚拟专网

高级设置

系统管理

退出

线路类型: 固定IP

IP地址: 220.175.104.140

子网掩码: 255.255.255.248

网关: 220.175.104.137

DNS服务器: 202.101.224.68

MAC地址: [输入框]

选择上网接入服务提供商: 中国电信

上网类型及带宽: 光纤-100M

参考上行带宽: 4000

参考下行带宽: 9500

运营商提供

运营商和上网总带宽必须填写正确 上下行带宽建议为总带宽的0.9~0.95, 预留部分带宽用于防御突发数据

注意事项：

1. 上网服务提供商和带宽信息必须填写准确如果分类中没有的，勾选其他；（比如长城宽带）

2. 上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置高于 0.95 的系数。上行、下行总带宽单位为千字节每秒，即 KB/s，一般是标称带宽乘以 100 来计算，比如 10M 光纤，上下行总带宽是 10×100 ，即 1000KB/s，考虑预留一些带宽，推荐设置 937KB/s。一般而言，选择“上网类型以及带宽”，会自动填充“参考上行带宽”和“参考下行带宽”，系统会自动考虑预留并计算带宽。只有找不到合适的类型时，才需要进行自定义。

DHCP 上网



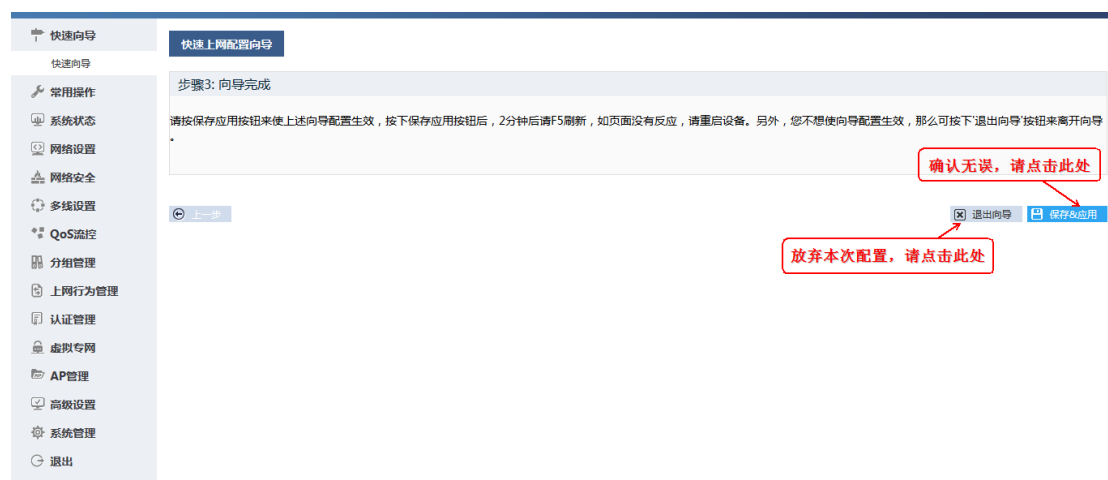
1.3.2.2 配置 LAN 口参数



注意事项：

网吧环境下，一般不建议开启 DHCP 功能，开启 DHCP 可能会与网吧无盘服务器冲突，导致客户机无法启动。

4. 点击保存&应用 即可完成了本次配置，请用你配置的 LAN 口 ip 登陆路由器，注意按照 1.3.1 修改您的 ip 地址。



二、快速配置向导

可以使用快速配置向导，通过引导配置可以快速的配置路由器，快捷方便。

2.1 快速向导

第一步：点击快速向导，请按照提示引导完成路由器配置，如图 19：



第二步，配置外网口（wan 口）参数，此时是配置上网的参数。（在网络设置中将有详细的说明）

常见的外网接入线路类型主要有三种：一种是固定 IP 接入；第二种是自动获取 IP；另一种是 PPPoE 拨号接入。外网接入方式由您的运营商提供。如果运营商提供了用户名、密码，那么就是拨号上网，线路类型您应该选择“PPPoE 拨号（或者 ADSL 拨号）”；如果运营商向您提供静态或者固定 IP，那么就是固定 IP 上网，线路类型您应该选择“固定 IP”；如果运营商说插上网线就能用，那么就是 DHCP 上网，应该选择“自动获取 IP”，下面将分别说明

拨号上网

快速向导

常用操作

系统状态

网络设置

网络安全

多线设置

QoS流控

分组管理

上网行为管理

AP管理

认证管理

虚拟专网

高级设置

线路类型: PPPoE拨号(或ADSL拨号)

用户名: [输入框]

密码: [输入框]

MAC地址: [输入框]

选择上网接入服务提供商: 中国电信

上网类型及带宽: 光纤-10M

参考上行带宽: 937.5

参考下行带宽: 937.5

需要配置第 2 线路: [复选框]

红色方框中信息由运营商提供

此处必须填正确

上下行带宽建议设置为总带宽的0.9~0.95，预留部分带宽用于防御突发数据

勾选此项可以配置wan2，不勾选则跳到内网配置界面

注意事项：

- 上网服务提供商（运营商）有中国电信、中国联通、中国移动、教育网、长城宽带，此项内容必须填写准确，如果分类中没有的，选择其他；
- 上网类型以及带宽可根据上网服务提供商（运营商）给您提供的线路类型和带宽来选择，比如您如果选择了光纤 10M，那么参考上行带宽和参考下行带宽会给出一个线路可用总带宽的参考值，该参考值将会被智能流控和多线策略所使用，所以必须填写准确。如果下拉列表中没有的，请勾选自定义；

由于上行、下行参考值会同步到智能流控的总带宽参数，所以会预留部分带宽用于防御突发数据，总带宽越小，预留越多，总带宽越大，预留越少。

上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置高于 0.95 的系数。上行、下行总带宽单位为千字节每秒，即 KB/s，一般是标称带宽乘以 100 来计算，比如 10M 光纤，上下行总带宽是 10*100，即 1000KB/s，考虑预留一些带宽，推荐设置 937KB/s。一般而言，选择“上网类型

以及带宽”，会自动填充“参考上行带宽”和“参考下行带宽”，系统会自动考虑预留并计算带宽。只有找不到合适的类型时，才需要进行自定义。

固定 ip

线路类型: 固定IP

IP地址: 220.175.104.140

子网掩码: 255.255.255.248

网关: 220.175.104.137

DNS服务器: 202.101.224.68

MAC地址: 留空表示使用默认MAC, 请使用格式如: 00:33:44:55:66:77

选择上网接入服务提供商: 中国电信

上网类型及带宽: 光纤-100M

参考上行带宽: 4000

参考下行带宽: 9500

运营商提供

运营商和上网总带宽必须填写正确
上下行带宽建议为总带宽的0.9~0.95, 预留部分带宽用于
防御突发数据

上网服务提供商以及线路类型、带宽等请参考“拨号上网”的相关说明

DHCP 上网

步骤1: WAN(外网口)设置--WAN

线路类型: 自动获取IP

MAC地址: 留空表示使用默认MAC, 请使用格式如: 00:33:44:55:66:77

选择上网接入服务提供商: 中国电信

上网类型及带宽: ADSL 4M

参考上行带宽: 60

参考下行带宽: 348

需要配置第2线路: ☐ 勾选该项将配置下一个WAN口 (多线路上网用户配置多条上网线路适用)

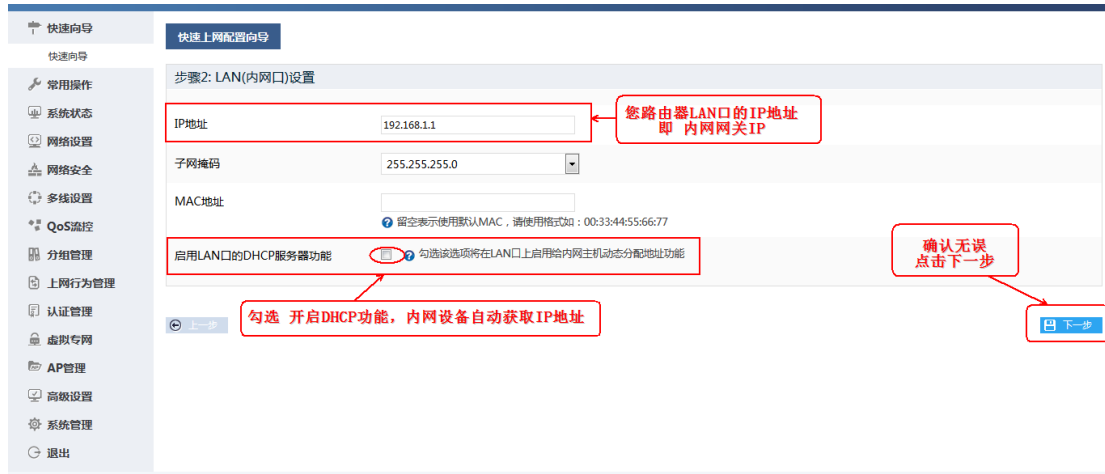
选择好上网方式为 自动获取IP (即DHCP) 后 点击下一步即可

此处需要带宽 需要询问提供者 这个方式较少

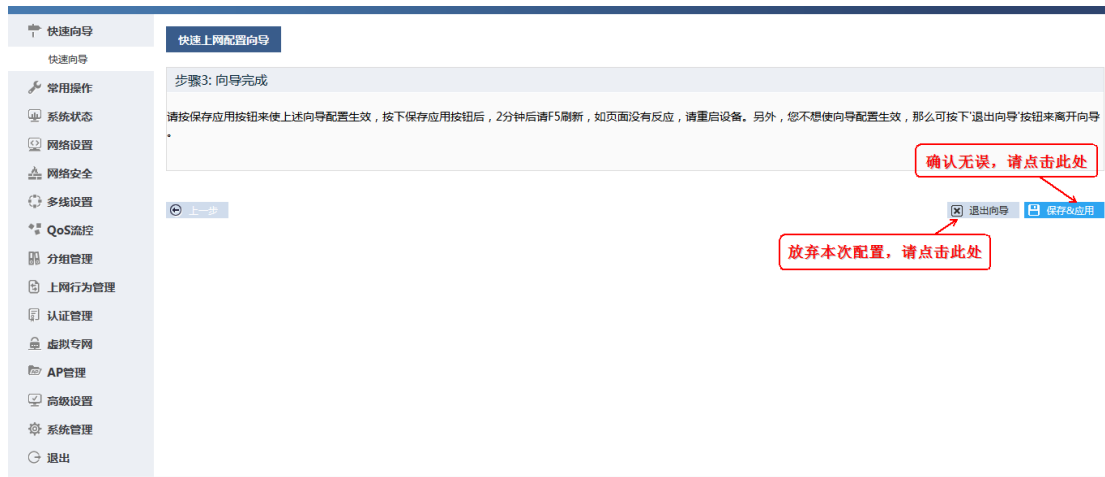
上网服务提供商以及线路类型、带宽等请参考“拨号上网”的相关说明

如果您需要配置第2条外网线路，则勾选“需要配置第二条线路”，然后再重复第二步的相关操作，以此类推。如果您不需要，则进入第三步。

第三步. 配置好 LAN 口设置，即内网网段设置，如下图：



点击保存&应用 即可完成了本次配置，修改后请用您配置的 LAN 口 IP 地址重新登陆路由器



三、常用操作

3.1 外网配置

上网的方式，PPPOE 拨号（或 ADSL 拨号），DHCP 上网（自动获取 ip）上网，固定 ip，根据您的情况选择符合您的上网设置即可。

选择运营商提供的上网方式按下图设置即可：

3.1.1 拨号上网

注意事项：

1. 上网服务提供商和带宽信息必须填写准确，如果分类中没有的，勾选其他；（比如长城宽带）
2. 上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置低于 0.9 的值

3.1.2 固定 ip

注意事项：

1. 上网服务提供商和带宽信息必须填写准确，如果分类中没有的，勾选其他；（比如长城宽带）
2. 上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置低于 0.9 的值

3.1.3 DHCP 上网

3.2 内网配置

主要配置 LAN 口即内网的相关信息。

注意：MAC 地址一般不用填，当您填入时，表示您修改了内网接口的 MAC 地址，您可以在您需要时进行填写。

路由器 IP 地址：路由器的内部地址，也就是内网的网关。

子网掩码：相应的子网掩码。



扩展网段设置：填写一个虚拟网段的网关 IP 地址及虚拟网段的子网掩码。为内网模拟出多个独立的网段。（如：要虚拟出一个 192.192.10.X 段的 IP，且其网关为 192.192.10.1，则 ip 地址栏应填入 192.192.10.1，子网掩码栏应填入 255.255.255.0）

3.3 端口映射

此处从略，请参考【网络安全】-->【端口映射】

3.4 智能流控

此处从略，参考【智能流控】相关章节中的说明

3.5 多线策略

参考【多线策略】-->【多线设置】

四、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。

4.1 概览



登陆路由器后，查看此功能，可以了解路由器目前工作状态，作为判断网络故障和使用率的依据之一。

路由器负荷，有图表实时显示目前系统 CPU 占用资源率，内存使用率，当前连接数，可以直观的了解路由器的资源使用情况。

接口状态，直观的显示当前网卡的状态，物理连接是否正常，网络通信是否正常。

系统状态，描述路由器的属性，系统名称，路由器型号，版本号，系统时间，运行时间，负载，活动连接数，是比较全面的介绍路由器本身特点。

系统名称可以在【系统设置】-->【基本设置】中修改‘设备名称’即可。V3.0以后的版本支持了中文名称

V3.0 版本在线主机数支持了最高在线主机数。

注意事项：

1. 系统 CPU 占用资源率正常情况下低于 50%
2. 单台连接数正常情况下低于 500，下载时会高到 2000，这个可以作为判断是否有攻击的一个依据
3. 每台客户机平均连接数正常情况下低于 200，比如，100 台 PC 或者移动终端在线时，总的连接数一般不会超过 2 万条，这个可以作为判断是否有内网攻击的另一个重要依据。

4.2 路由

显示当前路由器的连接的路由路径。

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。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（Routing Table），供路由选择时使用，表中包含的信息决定了数据转发的策略。打个比方，路由表就像我们平时使用的地图一样，标识着各种路线，路由表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路由表可以由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

网络	对象	IPv4-网关	跃点数
wan	192.168.6.0/24	0.0.0.0	0
lan	192.168.0.0/24	0.0.0.0	0
wan	0.0.0.0/0	192.168.6.1	0

网络： 表示路由的出接口

对象： 表示路由的目的网络， 如果出接口为外网拨号接口， 且对象不是 0.0.0.0/0， 那么该对象是局端的 IP 地址（或者说该条线路的运营商网关）。如果对象为 0.0.0.0/0， 表示默认路由

网关： 表示路由的下一跳地址， 如果为 0.0.0.0/0， 通常表示直连路由。当出接口为外网拨号接口， 下一跳地址通常为接口 IP 地址， 如果出接口为外网固定 IP(或者静态 IP) 线路， 那么下一跳地址通常为局端 IP 地址， 也就是运营商网关， 当出接口为 LAN 接口， 且网关非 0.0.0.0/0， 通常为用户自行定义的静态路由下一跳地址。

4.3 系统日志

记录系统的操作日志，安全日志等，方便用户查找操作记录以及故障排除

	系统日志				
	安全日志	系统日志	接口日志	操作日志	模式设置
时间(月/日/时:分:秒)	打印程序	信息			
7/23/08:56:25	kernel	lan 端口连接!			
7/23/08:56:22	kernel	lan 端口断开!			
7/23/08:56:03	kernel	lan 端口连接!			
7/23/08:56:01	kernel	lan 端口断开!			
7/22/21:22:56	kernel	lan 端口连接!			
7/22/21:22:54	kernel	lan 端口断开!			
7/22/15:01:07	kernel	lan 端口连接!			
7/22/14:10:35	kernel	lan 端口断开!			
7/22/13:58:56	kernel	lan 端口连接!			
7/22/13:58:09	kernel	lan 端口断开!			

系统日志：显示历史和当前在线主机数

安全日志：显示历史和当前连接数超出限制、收到攻击等日志信息

接口日志：显示历史和当前 wan 口和 lan 的断开和连接等日志信息

操作日志：显示历史和当前登录的时间、ip、和进行的操作等日志信息

4.4 实时监控



实时监控，显示路由器的实时状态，cpu 的实时负载情况，网络流量情况。

负载：反应了路由器硬件在一段时间内实时的负载情况。

网络流量：反应当前网络的实时流量。

注：1B=1byte=8bit=8b

4.5 主机监控

主机流量监控，显示内网 pc 机实时的网络流量，以及总的上传下载总流量、TCP、UDP 连接数等信息。

点击IP地址，可以看到该主机的详细连接信息

点击表头可以排序
默认按照下行速率排序

主机	主机名称	上行速率	下行速率	上行字节	下行字节	tcp连接数	udp连接数	在线时间
192.168.1.231	-	10K	424K	2.7G	94.2G	213	8	4天17时30分7秒
192.168.1.55	-	7K	306K	305.0M	3.3G	26	10	0天7时21分11秒
192.168.2.99	-	4K	92K	58.3M	395.1M	6	159	0天4时26分35秒
192.168.5.16	-	865	73K	936K	151.2M	6	4	0天0时55分57秒
192.168.1.2	-	1K	46K	44.9M	415.2M	35	53	0天2时54分31秒
192.168.1.56	-	5K	45K	90.4M	382.3M	21	283	0天2时42分56秒
192.168.1.5	-	5K	16K	132.6M	459.6M	12	55	0天6时25分23秒
192.168.3.168	-	3K	13K	15.3M	43.3M	2	1	0天1时57分48秒
192.168.2.131	-	5K	13K	15.5M	31.5M	7	3	0天1时18分53秒
192.168.2.123	-	4K	12K	13.0M	32.7M	7	4	0天1时18分57秒
合计	-	250K	1.3M	125G	145G	1.2K	1.8K	-

V3.0版本才支持合计功能

点击表格的标题字段可以排序。注意“合计”功能是 V3.0 以后的版本才支持。

单击 ip 地址会出现该 ip 的具体连接数、使用的端口、协议和应用的详细信息。如下图：

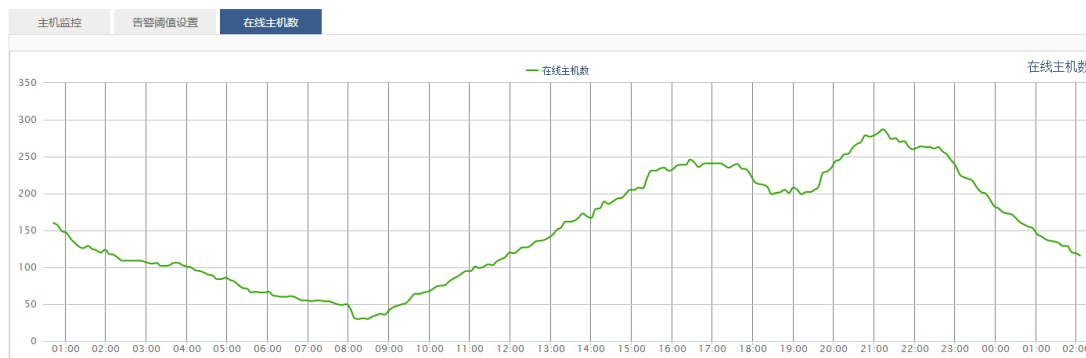
192.168.0.250 的详细连接信息

主机	网络协议	本地端口	目的端口	目的地址	上行字节	下行字节	剩余时间	应用	外网口
192.168.0.250	udp	800	800	255.255.255.255	1.5M	0	59	未知流量	-
192.168.0.250	icmp	0	0	183.56.71.241	1.0M	1.0M	29	ICMP	wan
192.168.0.250	icmp	0	0	192.168.0.1	1.0M	1.0M	29	ICMP	-
192.168.0.250	tcp	63514	49904	113.106.98.104	153K	3.6M	3551	网络大师	wan
192.168.0.250	udp	9818	9720	119.97.175.160	66K	79K	176	其他P2P	wan
192.168.0.250	udp	60488	9818	61.145.71.146	52K	51K	171	UDP小包交互	wan
192.168.0.250	udp	60484	9818	61.142.209.10	52K	51K	171	UDP小包交互	wan
192.168.0.250	udp	60475	9818	58.44.194.83	52K	52K	177	UDP小包交互	wan
192.168.0.250	udp	60476	9818	58.47.159.112	52K	51K	173	UDP小包交互	wan
192.168.0.250	udp	60470	9818	58.20.250.130	52K	51K	171	UDP小包交互	wan

注意，请使用谷歌浏览器、360 极速浏览器（极速模式）等 chrome 内核的浏览器，或者使用 IE9 以上的高版本的 IE 浏览器，否则可能有兼容性问题。

告警阈值设置：设置主机监控的报警阈值和刷新频率。当上行速率、下行速率、TCP 连接数、UDP 连接数其中一个超过它的报警阈值时，在主机监控页面中会以特别的颜色标识出来。

在线主机数：显示过去 24 小时的在线主机数趋势图，如下图所示：



4.6 应用统计

显示内各应用程序大类别的统计，如网络视频，网络游戏等大类的实时网络流量。



点击某大类的超链接，比如点击‘其他应用’可以看到大类里每个应用的详细信息，如下图页面所示：



编号	应用	上行速率	下行速率	上行字节	下行字节	上行包数	下行包数	上行比例	下行比例
37	ICMP	60	60	1.2M	1.2M	21K	21K	5	0
121	UDP小包交互	35	35	1.2M	1.3M	28K	28K	5	0
81	其他P2P	0	0	252K	776K	1K	1K	1	0
183	UDP上传应用	0	0	71K	5K	58	99	0	0
184	UDP下载应用	0	0	2K	55K	39	39	0	0
7	MDNS	0	0	0	0	0	0	0	0
12	BGP	0	0	0	0	0	0	0	0
28	ShoutCast	0	0	0	0	0	0	0	0
32	VRRP	0	0	0	0	0	0	0	0
38	IGMP	0	0	0	0	0	0	0	0

注意，请使用谷歌浏览器、360 极速浏览器（极速模式）等 chrome 内核的浏览器，或者使用 IE9 以上的高版本的 IE 浏览器，否则可能有兼容性问题，比如无法排序，也看不到详细的应用统计信息。

4.7 QQ 在线列表

显示内网的在线 QQ 列表



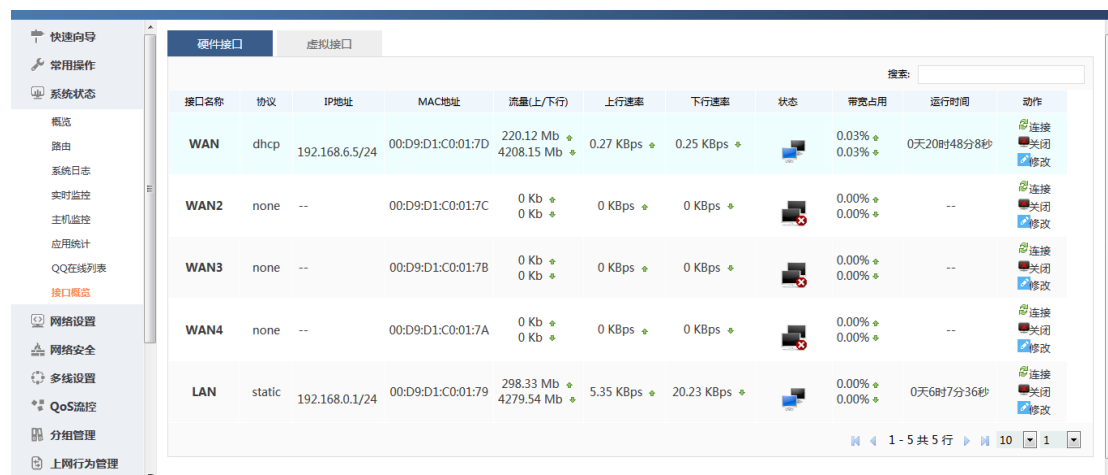
QQ号	IP地址	在线时长	上线时间	是否手机QQ
暂时没有QQ在线。				

4.8 接口概览

显示路由器所有接口的状态，连接方式，带宽，网卡利用率等信息。

4.8.1 硬件接口

显示广域网，局域网等硬件接口相关信息。



接口名称	协议	IP地址	MAC地址	流量(上/下行)	上行速率	下行速率	状态	带宽占用	运行时间	动作
WAN	dhcp	192.168.6.5/24	00:D9:D1:C0:01:7D	220.12 Mb 4208.15 Mb	0.27 KBps	0.25 KBps		0.03% 0.03%	0天20时48分8秒	连接 关闭 修改
WAN2	none	--	00:D9:D1:C0:01:7C	0 Kb 0 Kb	0 KBps	0 KBps		0.00% 0.00%	--	连接 关闭 修改
WAN3	none	--	00:D9:D1:C0:01:7B	0 Kb 0 Kb	0 KBps	0 KBps		0.00% 0.00%	--	连接 关闭 修改
WAN4	none	--	00:D9:D1:C0:01:7A	0 Kb 0 Kb	0 KBps	0 KBps		0.00% 0.00%	--	连接 关闭 修改
LAN	static	192.168.0.1/24	00:D9:D1:C0:01:79	298.33 Mb 4279.54 Mb	5.35 KBps	20.23 KBps		0.00% 0.00%	0天6时7分36秒	连接 关闭 修改

在最右边一列为“动作”，点击编辑，可以对接口参数进行编辑。点击“连接”可以重连接口，比如重新拨号。点击关闭，可以暂时不用某个接口。

4.8.2 虚拟接口

显示设备的虚拟多 wan 接口相关信息



主要显示 WAN 口扩展的虚拟接口以及单线多拨虚拟接口，此处为虚拟接口参数配置的唯一入口。

4.8.3 历史流量视图

历史网络流量：反映设备所有网络接口的历史流量趋势。



上行：接口此时的上传流量情况。

下行：接口此时的下载流量情况。

日、周、月流量：根据范围来统计此时的流量数据。

五、网络设置

路由器的主要网络参数的设置，外网口设置，内网口设置，DHCP 设置等。

5.1 接口概览

显示路由器所有接口的状态，连接方式，带宽，网卡利用率等信息。可参考【系统状态】--》【接口概览】，是同一个内容的多个链接，不再多做说明。

5.2 外网配置

(详细配置请参考【常用操作】--》外网配置)

5.3 内网配置

(详细配置请参考【常用操作】--》【内网配置】)

5.4 DHCP

DHCP 服务用来动态分配 IP 地址、网关、域名服务器等信息给工作站客户机，省去了客户机手工设置的繁琐性。当客户机较多时，使用 DHCP 来配置网络可以大大减少管理员的工作！

5.4.1 DHCP 设置

关闭 dhcp 服务：关闭 lan 口的 dhcp 服务，即我们常说的内网自动获取 ip 的功能，关闭就无法自动获取 ip，只能手动填写。

起始 ip 地址：开始分配 ip 的的第一个地址，以后是逐一添加。如：



注意：

1. 如果上网人数较多，那么建议减少租用时间到 30 到 45 分钟，避免耗尽地址池。
2. 如果是网吧环境下，建议关闭 DHCP 配置，
3. 内网有接入无线 AP 的，建议通过配置独立多 LAN，将 AP 接入到另一个 LAN 口，从而在物理上隔离无线网络

5.4.2 多 LAN 扩展 DHCP

为独立的多 LAN 配置扩展 DHCP，必须要做两个步骤。首先，点击【创建】按钮创建 DHCP 配置。然后编辑保存应用它



注意：

注意：多 LAN 扩展 DHCP 建立前提是必须拥有独立的多 LAN 即，【高级设置】-->【弹性端口】，从中生成独立多 LAN，请参考【弹性端口】相关说明

5.4.3 DHCP 静态分配

静态租约用于给 DHCP 客户端分配固定的 IP 地址和主机标识。只有合法主机才能连接，并且接口须为非动态配置。

使用添加按键来增加新的租约条目。MAC-地址鉴别主机，IPv4-地址分配地址，主机名分配标识。

简而言之：为固定的 mac[固定电脑]（电脑的 mac 地址唯一固话，如果人为修改），分配指定的 ip 地址。



5.4.4 DHCP 静态批量配置

DHCP 静态分配条目的批量增加。每行的格式是：IP MAC，IP 地址和 MAC 地址用空格隔开，每行请回车。如：192.168.1.111 00:0e:0f:1d:1c:eb



5.4.5 DHCP 活动客户端

显示自动获取 ip 的客户端



5.4.6 DHCP 检测

点击【检测】按钮来检测局域网内是否有其他的 DHCP 服务器。这需要一点时间。



5.5 主机名

5.5.1 主机别名

主机名和 MAC 地址进行一对一关联。



主机别名将会在主机监控里显示在主机别名一列。

5.5.2 别名批量

主机别名批量增加。每行的格式是: MAC 地址 别名, MAC 地址和别名用空格隔开, 每行请回车。



5.5.3 主机域名

主机域名配置。默认的域后缀是 lan。

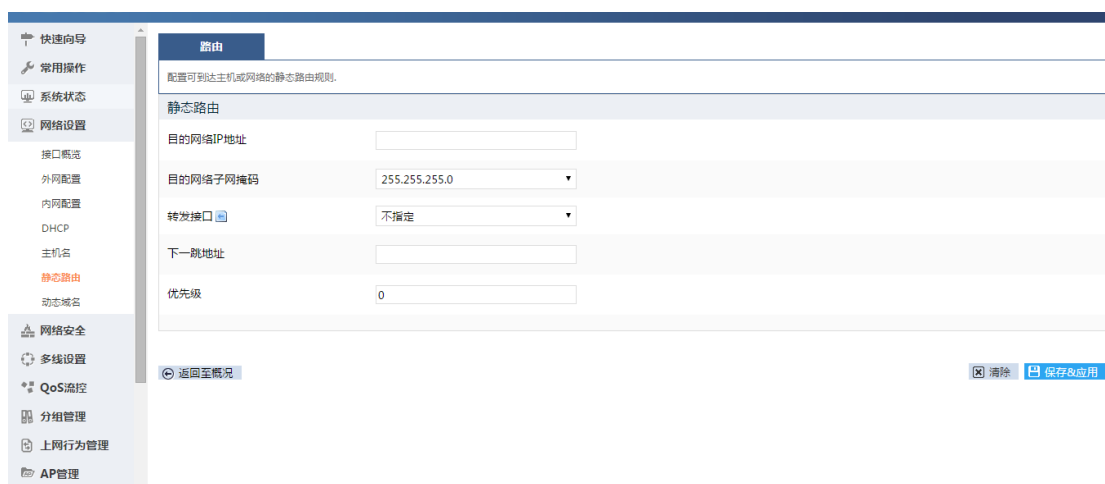
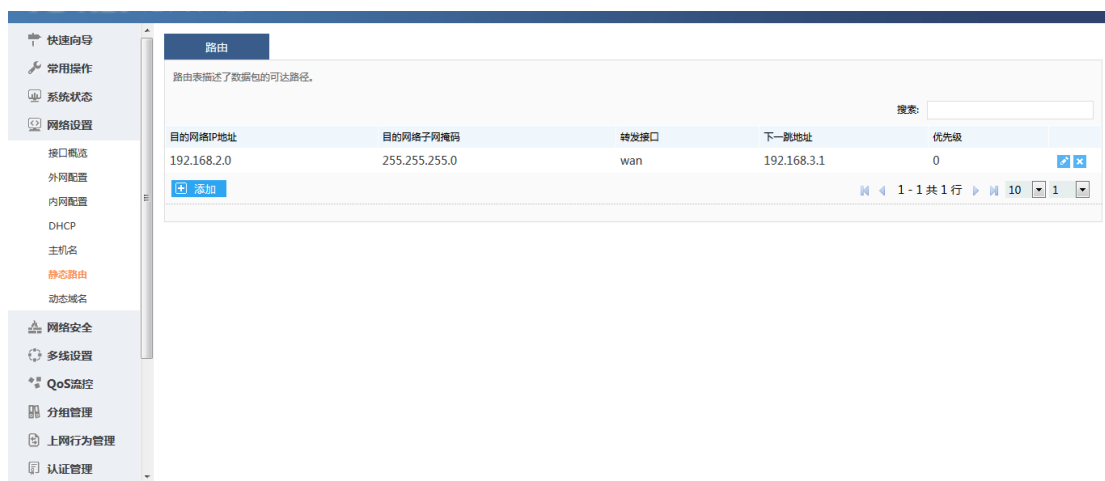


注意：

主机域名有效的前提是，内网主机使用路由器的内网 IP 作为 DNS 代理。

5.6 静态路由

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。



目的网络 ip 地址：目的地，所有访问的网段或者主机

子网掩码：子网的掩码

转发接口：指定从路由器某个接口转发，一般可不填

下一跳地址：可填路由器 wan 口地址，也可填与之相连的对端接口的地址

优先级：优先转发等级

一般用在内网有三层交换机的场景下。或者二级路由使用路由模式，或者在使用 VPN 的场景下。

5.7 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。打开“DDNS 设置”可以看到如下界面：

由于运营商的 ip 的地址有限，采取的是动态分配 ip 地址的方式，普通拨号用户的 ip 是随机分配，且每次拨号，获取相同 ip 的可能性很低。

动态域名

动态域名(DDNS)能使您通过一个固定的域名来访问IP地址动态变化的网络设备

启用 ☐

服务提供商

主机名

用户名

密码

网络基本配置

状态 动态域名功能未启用。

服务商：网络上提供动态 ip 转换成唯一的域名（需要你申请）的服务的提供商。

主机名：你在动态域名服务商那里申请的域名。

用户名：你在服务商网站上，申请动态域名时注册的那个用户名。

密码：申请注册用户名，对应的登陆密码

接口：通过那个 wan 口来维持这个 ip 域名更新。

状态：可以看到动态域名的更新状态。

六、网络安全

保护内网安全，防范攻击。

6.1 ARP 绑定

为了更好的对网络中的计算机进行管理，您可以通过 ARP 绑定功能来控制网络中计算机间的访问(IP 绑定)。使得局域网中计算机的 mac 和 ip 绑定在一起，而别的计算机不能使用该 IP。

可以通过 ARP 扫描内网 IP 选定所需绑定的主机进行绑定，也可以手动批量或单个绑定。操作界面如下图：

绑定列表图示



ARP 扫描图示



注意：一次扫描只能扫描一个 C 网段，由此避免扫描大网段导致大量消耗路由器资源。如果您内网有多个 C 网段（也就是掩码不是 255.255.255.0），或者内网口上配置有扩展网段，那么您必须多次扫描。

高级设置图示



请谨慎使用“只允许绑定的 IP/MAC 通过”

批量绑定图示



小技巧：此处也可以用作“批量导出”，Ctrl+A, 选中编辑框中所有条目，然后 CTRL+C 可以完整导出到任意文本文件。

6.2 ARP 安全

针对 ARP 欺骗，RE 路由器网络安全设置下有 ARP 绑定，ARP 安全设置，在 ARP 安全设置下勾选免费 arp 发送，ARP 攻击防御，ARP 欺骗检测功能。

在 web 管理界面下可以直接设置，如下图所示：



安全设置		欺骗列表	
ARP安全防护。包括arp速率限制（arp攻击防御）、免费arp发送和arp欺骗检测			
ARP攻击防御		☒	
速率限制		1000	
		5~50000包/秒	
免费ARP发送		☒	
发送时间间隔		5	
		1~60秒	
ARP欺骗检测		☒	

提示：此处的速率限制是内网所有 ARP 包速率限制；如果您内网 PC 或者移动终端较多，速率限制应保证单台终端 10 包/秒，避免误杀；如果您内网终端数目为 200 台，那么速率限制以 2000 包/秒为宜。



欺骗检测只是提示欺骗的可能性，等级越高，那么欺骗的可能性越大；为安全起见，路由器并不会对欺骗者丢包；ARP 欺骗相关信息，不但会在此处显示，也会在系统安全日志里告警，请参考【系统状态】--》安全日志

6.3 端口映射

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，通过外网访问内部的 PC



添加新的规则，基本设置，高级设置，基本设置 设置一般的映射规则。

名称：映射的规则名称，最好根据目的起名。

选择网络区域或接口：选择映射的端口，一般选择 wan 口。

协议：映射基于的协议 TCP、UDP、TCP+UDP，根据服务类型选择。如果不知，请选择 TCP+UDP。如果确切知道是 TCP 或者 UDP，应避免选择“TCP+UDP”，可以有效降低资源消耗。

外部端口：通过外部访问的端口

内部端口：内部电脑提供此服务的端口，不填写，则和外部端口保持一致 注明：外部端口和内部端口可以不一致。

启用规则：启用这条规则

快速向导
常用操作
系统状态
网络设置
网络安全
ARP绑定
ARP安全
端口映射
连接数限制
攻击防御
多线设置
QoS流控
分租管理
上网行为管理
认证管理
虚拟专网
AP管理
高级设置
系统管理
退出

端口映射 一对一NAT规则 外出NAT规则 DMZ配置

您可设置您刚才添加或者编辑的这条规则

设置规则参数

启用规则 ☒ 勾选为启用此规则，不勾选则为禁用此规则

描述（可选） 对此规则的一个描述，便于管理

外网接口 所有外网接口 默认所有外网接口

协议 TCP+UDP 协议，UDP、TCP或TCP+UDP，一般选择TCP+UDP

外部端口 0-65535
在这个主机上，匹配输入的信息指向给定的端口或者范围

内部IP 重定向匹配到的入站流量至选定的内部主机

内部端口 0-65535
重定向匹配到的入站流量至内部主机的指定端口

启用NAT环回 禁用
一般无需开启，开启后让其他内网主机可以通过其公网映射地址访问该服务

返回至概况 清除 保存&应用

NAT 环回，又称“端口回流”（3.0 版本已改成“端口回流”），开启后，在内网客户机或者终端可以用路由的外网接口的公网 IP 地址访问内网的服务器。一般情况下，如无必要，请勿启用，避免无谓消耗路由器的资源



举例：

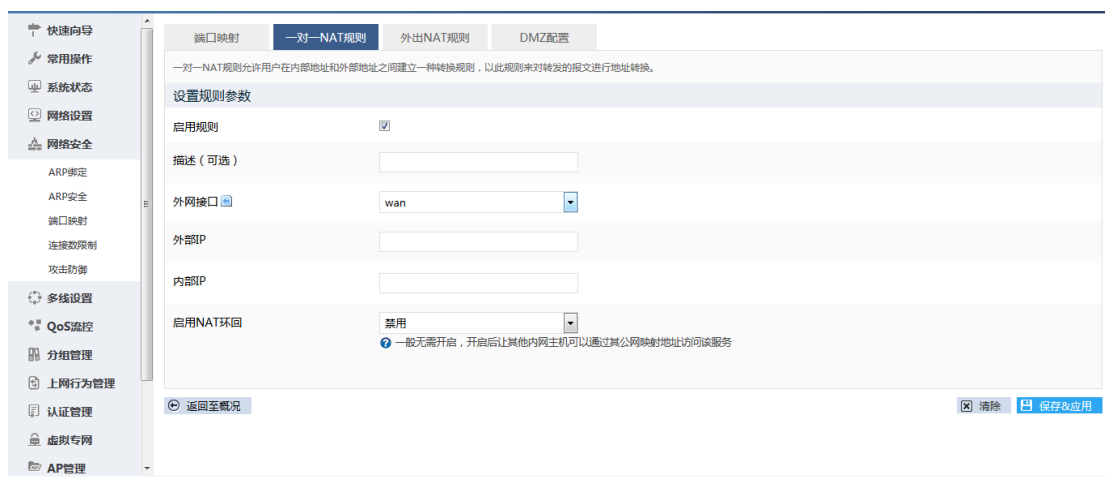
假设外网配置有动态 DNS 解析，比如为 go-cloud.f3322.org，同时外部端口设为 8888，内部端口为 80（WEB 服务器端口为 80，IP 地址为 192.168.1.222），从外网访问该内部的 web 服务器，则在 ie 地址栏应该输入

<http://go-cloud.f3322.org:8888> 从内网访问该 WEB 服务器，则在内网电脑上的 IE 地址栏，输入 <http://192.168.1.222/>，192.168.1.222 为 WEB 服务器 ip 地址。

如果开启了“端口回流”（又称 NAT 回环），则从内网电脑也可以通过 <http://go-cloud.f3322.org:8888> 访问内网的 WEB 服务器。

一对一 NAT 规则：允许用户在内部地址和外部地址之间建立一种转换规则，以此规则来对转发的报文进行地址转换,一个外网 ip 完全映射一个内网 pc，此种方式使用较少。

设置如下图：添加规则



外出 NAT 规则：管理和显示外出 NAT 规则。

通过此功能可以将内网的某些 IP 或者网段翻译成指定的外网 IP。比如有些外网线路，运营商提供了两个公网 IP 地址 A/B，其中一个公网 IP 配置为外网接口 IP A，另一个外网 IP 则可以使用外出 NAT 规则来将某些内网 IP 翻译成 IP B；可以用在多个网吧内网或者相对独立的局域网合并的场景下。



DMZ 配置：DMZ 功能允许网络设备(PC 或服务器等)被完全的暴露在网络中,这样就能被外部设备方便的访问，这种功能通常用于特定的服务比如游戏、web 服务器或视频会议等。



6.4 连接数限制

连接数设置可以控制整个网络对外的连接数量。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连接请求时，也可以达到抑制作用。

列外：就是在此规则之外，不受此规则控制。

攻击防御：DDOS 攻击的原理大量发包消耗资源，导致路由系统拒绝服务，从而严重影响正常上网。比如，SYN 攻击就是利用 TCP 的三次握手协商的特点，每次只发送第一个 SYN 报文，让路由器收到 SYN 报文以后应答 SYN ACK 报文，而攻击者不理睬 SYN ACK 报文，让连接无法创建，这样路由器就要消耗系统资源不断重传报文。大量的 SYN 报文，将使路由器的系统资源被消耗尽，最后就导致掉线现象的出现。DDOS 攻击的源头不仅可以来源于内网，也可以来源于外网。

攻击防御 web 配置界面如下，可勾选如图选项所示



禁止内网间转发 主要目的是隔离内网多个子网，禁止内网多个子网之间通过路由器跨网段转发来实现互通。

提示：UDP 攻击防御的阈值一般不要高于 2000。

七、多线设置

多条线路接入好处在于：互联互通，应用分流，叠加带宽，冗余备份；多 wan 或者多线接入是解决中国多个运营商之间通而不畅、综合资源节省费用的一种通行的方式。

注意事项：

优先级：策略路由》应用分流》多线模式设置

7.1 多线策略

如果您的外网只有一条外线，除了线路侦测外，多线策略的所有设置您都无需关心。

7.1.1 多线设置



智能选线：根据运营商智能进行选路，在有多家运营商多根线的情况下，选用此模式可实现对应游戏和应用电信走电信，联通走联通，从而解决电信、联通之间通而不畅的问题，如果电信流量和联通线路流量不均衡，建议配合开启应用分流来进行均衡，如果您有多条电信线路和多条联通线路，路由默认会选择带宽最大或者权重最大的那条联通线路和带宽最大或者权重最大的电信线路分别作为电信、联通的主线，从而实现电信流量走带宽最大的电信线路；同时联通流量走带宽最大或者权重最大的联通线路，（接口权重可以在【高级设置】--》【接口高级设置】里进行设置，默认带宽大的线路的权重也大）；此时其余的线路需要通过应用分流来调度分配流量。

主辅模式：推荐一条商用或者专用光纤加 1 条或者多条 ADSL（或者拨号线路）的情形下使用，需要配合开启应用分流。

提示 1：在不配置【应用分流】的情况下，辅助线路默认将不会有任何流量，也就是说此时所有流量只会走主线。

提示 2：在商用光纤线路带宽十分紧张，比如只够玩游戏时，那么应该选择某条 ADSL 或者拨号线路作为主线，同时将网络游戏通过【应用分流】规则分流到光纤，该 ADSL 线路或者拨号线路的运营商最好与光纤线路的运营商一致，比如光纤是电信光纤，而 AD 也是电信 AD。

负载均衡：多根同运营商，同样大小的同种类型的根据带宽的比重在各条线中均衡选路，同时实现带宽叠加（比如所有外网线路都是电信 20M ADSL），**各外网线路流量分配多少，取决于接口权重大小，权重大的，分流多，反之则少，在【高级设置】--》【接口高级设置】可以调整权重大小，系统默认带宽越大，权重越大。**

主备模式：只有主线 down 掉的情况下才会走其他线路

注意事项：

1. 主线和默认线路一般南方选电信，北方选联通或网通，光纤优于 adsl，但以具体情况为准
2. 国内一般以智能选线和主辅模式为多，负载均衡和主备模式适用在一些特殊情景下
3. 模式选定后，如果不另外进行应用分流或者策略路由配置，都会按照选路模式所定义的方式分配流量到各条线路。
4. 多线模式修改后，不影响老的连接的选线方式，只有新的连接才会按照新的配置分配流量到各条线路。所以，配置修改不会拆除老连接，不会引起现在正在玩的游戏、QQ 等掉线，也会因此产生一个错觉：配置貌似没有立即生效。

7.1.2 应用分流

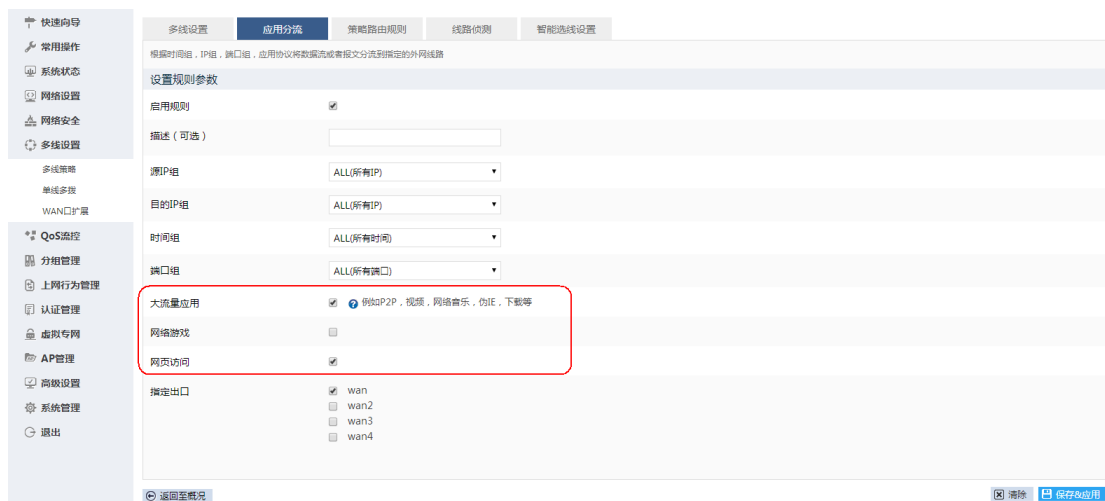
分流界面



配置分流界面



V2.1 以后的版本支持了分流规则的快捷方式，增加了大流量应用、网页、游戏三大类的应用预定义，大大简化了规则配置的复杂性。



当大流量应用、网络游戏、网页访问都不选择是，会出现应用协议编辑框，点击编辑框，则会出现协议选择对话框，如下图：

添加协议和应用界面



注意事项:

1. 小流量协议和应用不建议参与分流，比如 DNS、ICMP 等
2. 大流量协议和应用主要有其他 P2P 下载（在其他应用中）、P2P 下载、网络视频、网络电视、伪 IE（常见应用中），软件更新、文件传输，您可视带宽充裕程度决定分流的多少，带宽紧张就多分一些，带宽比较充裕就少分流一些。大流量应用分流规则可以指定多个出接口，各出接口流量分配多少，取决于接口权重大小，权重大的，分流多，反之则少，在【高级设置】--》【接口高级设置】可以调整权重大小，系统默认带宽越大，权重越大。
3. 在智能选线和主辅模式下，如果主线带宽充裕，游戏一般不需要另行配置分流规则，且，网络游戏在配置分流时，外网出口只能指定一个，不能多选
4. 应用分流配置修改后，不影响老的连接的选线方式，只有新的连接才会按照新的配置分流到指定线路。所以，配置修改不会拆除老连接，不会引起现在正在玩的游戏、QQ 等掉线，也会因此产生一个错觉：配置貌似没有立即生效。

7.1.3 策略路由规则

源 ip 地址：发送者的 ip 地址

目的 ip 地址：接收者的 ip 地址，目的地址

协议类型：所使用的协议，TCP,UDP,ICMP,ALL

端口：端口号使用的端口号 指目的端口。

指定出口：数据的出口，通过那个网卡发出数据到目的 ip。



注意：

策略路由配置修改后，不影响老的连接的选线方式，只有新的连接才会按照新的配置分配流量到指定线路。所以，配置修改不会拆除老连接，不会引起现在正在玩的游戏、QQ等掉线，也会因此产生一个错觉：配置貌似没有立即生效。

7.1.4 线路侦测

线路侦测，防止虚连接，保证外线的连通，自动切换到其他可用线路。



注意：

1. 只有固定 IP 线路或者 DHCP 自动获取 IP 的线路需要进行线路侦测，拨号方式的线路不会出现在此配置页面中。
2. 单线的情况下，建议禁用
3. 多线情况下，当某条线路侦测到断开，会自动切换将流量到其他线路

4. 默认为 Arp 侦测，建议在在外网允许 PING 的情况下，使用 PING 侦测方式中任何一种。
5. 较新的版本才支持 ping 指定 IP 和线路侦测状态显示。

7.2 单线多拨

配置单线多拨，通过一个 WAN 口生成多条 ADSL 拨号线路



点击添加，填上运营商提供的用户名和密码即可，应用后将生成 wan_m1/wan_m2 类似名字的接口，您可以在【网络设置】--》【接口概览】--》【虚拟接口】里进行更多参数设置。

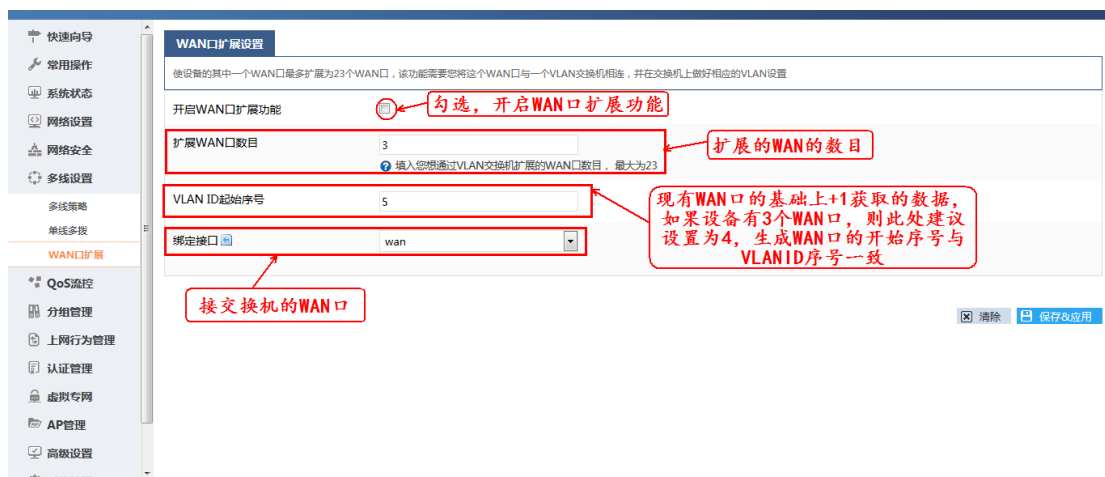
注意：本功能无需外扩 VLAN 交换机，但只有运营商比如电信、联通允许单号多拨的情况下，才能成功单线多拨。



7.3 WAN 口扩展

路由器通过 VLAN 的技术，虚拟出多个网卡，通过虚拟的网卡实现多条物理拨号。

您能使设备的其中一个 WAN 口扩展为 23 个 WAN 口，只要您将这个 WAN 口与一个 24 口的 VLAN 交换机相连，并在交换机上做好相应的 VLAN 设置。



注意事项：

1. 绑定的物理接口本身不要使用。

- 部分低端型号不支持 WAN 口扩展。如果您的设备里没有【WAN 口扩展】菜单，则表示该设备不支持该功能。
- 按照上述界面配置好之后，外网配置中会出现对应的外网虚拟接口，比如在 wan 口扩展，就会出现 wan_v1/wan_v2 等，您可以在【网络设置】--》【接口概览】--》【虚拟接口】里进行更多上网参数设置。
- V3.0.0.5955 以后的版本支持指定非连续 VLAN ID，如下图：



VLAN ID 分配方式默认为连续 VLAN ID，建议使用 V3.0.2.6192 以后的版本，配置可与之之前配置兼容。使用连续 VLAN ID 分配的方式见下图：



八、QOS 流控

随着 p2p 下载、p2p 视频大行其道，导致大量政府、企业、学校等带宽严重拥塞，同时对优先级高的应用优先保障带宽的需求也日益增长，因此对各种应用流量进行优先级控制的 QoS 流控功能显得异常关键。

QOS 流控的设计目标是：

QOS 流控采用 PHQ 智能算法，在全局统筹的高度将内网全部流量按照优先级高低依次分为游戏、聊天、网页、常用、视频、下载 6 个业务通道，经过精巧设计，反复打磨，QOS 流控算法具有如下特点：优先有序、各行其道、公平共享、通道借用

1. 优先有序

任何情况下，优先保障游戏、聊天、网页等优先级高的业务通道的带宽，保证不卡不掉，流畅如行云流水

2. 各行其道

单机在下载、看视频的同时，玩游戏流畅，打开网页不卡。

3. 公平共享

PHQ 算法保证了每一个业务通道中每台主机都有公平的机会，防止某台主机长时间的独占带宽；并且根据使用者人数自动均分带宽，假设下载通道当前有 10M 带宽可用，而下载的主机有 2 个，那么这两台主机每台可获得 5M 带宽，当有 3 台在下载，每台主机可获得 3.3M 带宽，依此类推；因此最显著的效果是：迅雷下载每台主机自动均分带宽，下载的人少，则快，下载的人多，则会自动降低每台下载主机的下载速度

4. 通道借用

当高优先级通道没有流量，则带宽将自动借用给低优先级业务通道。

所以综合来看，PHQ 智能流控算法在实际网吧测试中，表现非常抢眼，真正做到了优先有序、各行其道、公平共享、通道借用四大目标，总体效果是不管大带宽、小带宽、不管单线、多线，游戏不卡不掉，网页流畅，下载有速度，带宽利用率高。

8.1 智能流控

8.1.1 智能流控



注意事项:

1. 务必勾选上图中的“启用智能流控”，否则后续的配置均不生效
2. 此处下行带宽为外网线路的上传总带宽，建议设置为上网带宽的 0.9-0.95 之间，预留足够的带宽（视带宽是否充裕和具体应用设定）
3. 开启智能流控后、默认游戏优先级最高、其次为聊天，再次为网页。

8.1.2 例外



注意事项:

1. 例外规则中的 IP 或者 IP 组不受智能流控的控制，使用时务必谨慎小心
2. 需要配置固定流控策略来控制其最大速率，但 仍然有可能失控。
3. 配置了固定流控后，智能流控中建议减去固定流控的值，同时两者相加不能大于总的上网带宽（假设例外规则设置了一个 IP 组，该组中有两个 IP，每个 IP 固定限速 500KB/s，假设下行总带宽设置为 3500KB/s，现在固定流控设置了 500KB/s，那么智能流控建议设置为 $(3500 - 2 \times 500) = 2500\text{KB/s}$ ）

8.1.3 自定义流控策略

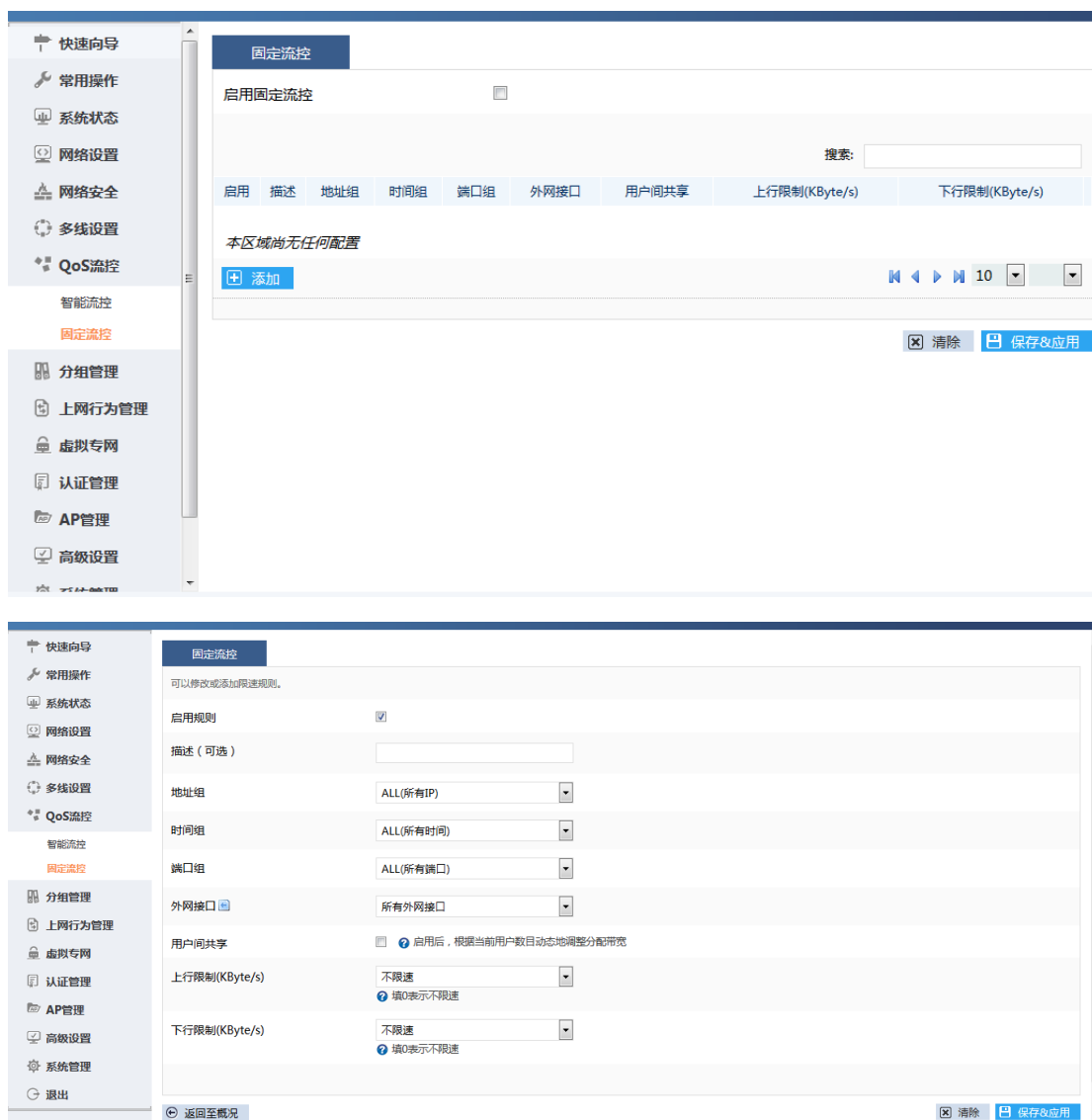


注意事项:

1. 这里你可以自定义流控规则，如果要使规则生效，必须关闭接口上的智能流控功能，也就意味着勾选此项后所有默认的优先级全部失效，同时与智能流控不能共存
2. 此功能不是很建议使用，技术牛人可以试试

8.2 固定流控

既可以在智能流控的基础进行带宽管控，也可以独立的进行带宽管理，和 qos 智能流控相互独立。在智能流控开启的情况下，固定流控仍然有效，相当于对内网 IP 进行了最高限速。由于智能流控极为有效，绝大多数情况下都无需像有些友商那样进行单 IP 固定限速-:)



注意：这里的上行限制和下行限制都是可以针对单台 pc 的，也可以针对 IP 组内的 PC 进行用户间共享。

8.3 QOS 高级页面

当网络流量需要细化控制时可以打开 QOS 功能高级隐藏页面进行

http://路由器管理地址/cgi-bin/webui/admin/flowqos/qos/qos_advopt

在浏览器输入以上地址即可进入 QOS 隐藏页面



禁止上行 QOS：可禁止接口的上行智能流控 QOS，一般不建议禁止

禁止下行 QOS：可禁止接口的下行智能流控，一般在带宽特别大，而路由器负荷很大的情况下可以尝试，减轻路由器的硬件资源消耗

抑制因子：通过抑制上行来控制下行，数值越大，则抑制效果越好，一般 70 到 80 就非常严厉了。20M 以内的小带宽的情况下出现流控失控的，可以设置 70 到 80

动态因子：可控制每个通道内带宽共享程度，动态因子越小，对共享的控制越严厉，一般 20 就表示非常严厉了。20M 以内的小带宽的情况下出现流控失控的，可以设置 15 到 20

游戏通道上行、游戏通道下行：针对所有游戏的流量上下行做限制，只有在极为罕见的情况下才可能需要设置

聊天通道上行、聊天通道下行：针对所有聊天程序的流量上下行做限制，只有在极为罕见的情况下才可能需要设置

网页通道上行、网页通道下行：针对所有网页浏览的流量上下行做限制，只有在极为罕见的情况下才可能需要设置

九、分组管理

进入路由器一级菜单“分组管理”，设置基于时间、地址、端口、应用的分组，方便用户设置相关的规则。



9.1 时间组

本页显示所有的时间组，系统预定义组-“ALL”不能编辑和删除，点击“添加”或“修改”可进行相关时间组设置。



快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

上网行为管理

AP管理

虚拟专网

设置规则参数

组名

示例

只能是字母和数字！

描述（可选）

可输入中文！

星期

☐ 星期一
 ☐ 星期二
 ☐ 星期三
 ☐ 星期四
 ☐ 星期五
 ☐ 星期六
 ☐ 星期日

日期都不选表示为每天！

时间段

从 0时 0分 到 0时 1分

时间填写格式是 hh:mm-hh:mm。时间留空表示任意时间！

返回至概况

清除

保存&应用

9.2 地址组

本页显示所有的地址组，系统预定义组-“ALL”不能编辑和删除,点击“添加”或“修改”进行地址组相应设置。

快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

地址组

本页显示所有的地址组，系统预定义组不能编辑和删除。

搜索:

组名	描述	IP地址段
ALL	所有IP	所有的IP地址

添加

1 - 1 共 1 行

10

1

清除

保存&应用

快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

地址组

本页用于添加和修改IP 组的配置。

设置规则参数

组名

只能是字母和数字！

描述（可选）

可输入中文！

IP地址段

IP地址范围的填写格式是：A.B.C.D-E.F.G.H！

返回至概况

清除

保存&应用

9.3 端口组

本页显示所有的端口组，系统预定义组-“ALL”不能编辑和删除,点击“添加”或“修改”进行端口组相应设置。

快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

端口组

本页显示所有的端口组，系统预定义组不能编辑和删除。

搜索:

组名	描述	网络协议	端口段
ALL	所有端口		

添加

1 - 1 共 1 行

10

1

清除

保存&应用

快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

端口组

本页用于添加和修改端口组的配置。

设置规则参数

组名

只能是字母和数字！

描述（可选）

网络协议

TCP

端口段

0-65535

+

端口范围的填写格式是：xxxxx-xxxxx！端口值的范围是[0-65535]！

返回至概况

清除

保存&应用

9.4 应用组

本页显示所有的应用组，系统预定义组-“ALL”不能编辑和删除,点击“添加”或“修改”进行应用组相应设置。在“应用名称”里提供多种应用可选。

快速向导

常用操作

系统状态

网络设置

无线设置

网络安全

多线设置

QoS流控

分组管理

时间组

地址组

端口组

应用组

应用组

本页显示所有的应用组，系统预定义组不能编辑和删除。

搜索:

组名	描述	应用名称	
ALL	所有应用		
P2PVIDEO	P2P/视频	P2P下载 网络电视 网络视频	✎ ✕
P2PVIDEODL	P2P/视频/下载	P2P下载 网络电视 网络视频	✎ ✕

添加

1 - 3 共 3 行

10

1

清除

保存&应用

鼠标点击应用名称对应的编辑框，则会出现下图所示：

选中相关协议，添加到右边，然后点击【确定】即可

注意，应用组只能用于上网行为管理相关配置中。

十、上网行为管理

对上网的行为进行监控管控，维护网络的监控规范。一级菜单“上网行为管理”下提供“一键管控”、“QQ在线列表”、“QQ白名单”、“URL重定向”、“防火墙规则”、“网址过滤”、“WEB访问记录”。

10.1 一键管控

10.1.1 一键管控

根据需求选择封杀特定的应用一键封杀选项进行操作即可，如有特权用户则加入例外即可。如果需要在某个时间段，不进行任何管控，那么设置例外的时间组



注意，上述功能在 V2.3 以后的版本才有。原来的上网行为管理规则配置移入到了【一键管控】-->【高级设置】，请见 10.1.2 相关说明

10.1.2 上网行为管理的高级设置

进入【一键管控】-->【高级设置】，点击“添加”或“修改”可进行相应上网行为管理设置，主要针对不同的分组分优先级进行允许或禁止动作，提高网络的管理手段。



点击上图中的添加后，会看到如下页面：



保存应用后，会回到规则列表，如下图所示



10.2 QQ 在线列表

统计所有在线的 qq，登陆 qq 的 pc 的 ip 地址，在线数时长，登陆时间，是否是手机登陆。

QQ在线列表

显示所有在线的QQ

搜索:

QQ号	IP地址	在线时长	上线时间	是否手机Q
	192.168.100.198	0天0时1分28秒	2015/1/24 下午12:15:23	是
	192.168.100.189	0天3时16分45秒	2015/1/24 上午9:00:06	否
	192.168.100.199	0天3时4分22秒	2015/1/24 上午9:12:29	否
	192.168.100.133	0天3时13分43秒	2015/1/24 上午9:03:08	否
	192.168.100.189	0天3时16分11秒	2015/1/24 上午9:00:40	否
	192.168.100.143	0天0时23分45秒	2015/1/24 上午11:53:06	是
	192.168.100.133	0天3时16分53秒	2015/1/24 上午8:59:58	否
	192.168.100.200	0天1时13分30秒	2015/1/24 上午11:03:21	是
	192.168.100.143	0天0时3分45秒	2015/1/24 下午12:13:06	是
	192.168.100.124	0天0时4分33秒	2015/1/24 下午12:12:18	是

1 - 10 共 10 QQ在线

10.3 QQ 白名单

“QQ 白名单”可添加 QQ，在白名单内的 QQ 不受上网行为管理 QQ 应用的控制，白名单支持单个添加和批量添加。

QQ白名单

QQ白名单批量添加

在本页中您可以添加QQ号，可以使它不受上网行为管理禁用QQ的控制。

启用QQ白名单功能 ☐

搜索:

QQ号	描述
本区域尚无任何配置	

[+ 添加](#)

清除 保存&应用

10.4 URL 重定向

URL 重定向可以实现，如果主机访问某个网址时，将其导向另一个网址。

The image displays two screenshots of the TG-NET router's web management interface, specifically the 'URL 重定向' (URL Redirection) section.

Top Screenshot: URL 重定向配置页面

- URL 重定向功能:** 勾选，启用URL重定向功能。
- 例外IP组:** 不启用例外。在例外IP组中的IP，不受URL重定向的管控。
- URL 重定向规则列表:** 本区域尚无任何配置。
- 添加URL重定向规则:** 点击“添加”按钮。

Bottom Screenshot: 添加URL重定向规则对话框

- 启用规则:** 勾选，启用URL规则。
- 原URL地址:** 例如：www.google.com。
- 重定向URL地址:** 例如：www.google.com。
- 说明:** 如果访问 原URL地址 时，页面会自动跳转到 重定向URL地址。

10.5 网址过滤

10.5.1 网址过滤



10.5.2 网址分类库





10.5.3 白名单

本页面你可以配置内网主机，服务器 IP 地址以及网址白名单，使他们不受网址过滤的影响



10.6 防火墙规则

显示并管理防火墙的访问列表规则

访问列表列出了 已经添加的规则，点击添加，就可以添加新规则如图：



描述：您对新建规则的描述，请您安装你需要的目的描述。

源区域：选择的作用网卡，是 lan 还是 wan 口，wan1，wan2 等，一般选择 wan 口

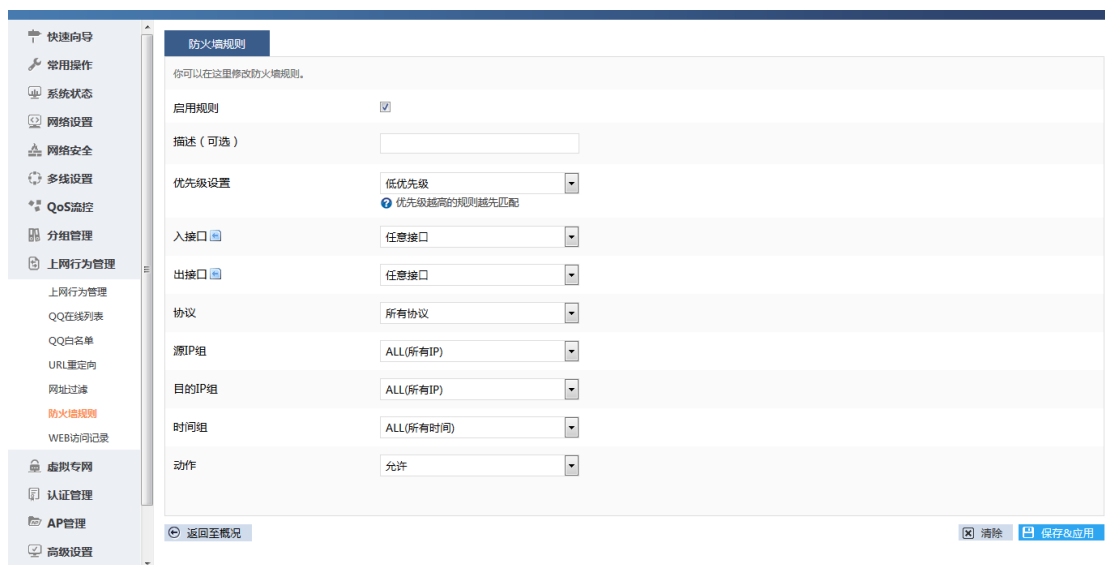
协议：基于那条协议 TCP,UDP,ICMP ,ALL 等

源 IP 组：在选择 wan 口的情况下，指明内部的 pc 的 ip 地址

目的 IP 组：在选择 wan 口情况下，指外网的 ip 地址等。

动作：允许，禁止

设置完成后，点击保存&应用即可生效。





注意：协议选择了 UDP 时，才会出现两个选择源端口和目的端口的下拉列表。

10.7 WEB 访问记录

10.7.1 上网记录配置

配置 WEB 访问记录的相关参数



10.7.2 上网记录查询

可对上网记录进行查询



十一 虚拟专用网

通过虚拟专线（VPN），使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网。达到远程无碍办公，提供了接入的安全性。

PPTP（Point-to-Point Tunneling Protocol），点到点隧道协议：PPTP 是一种虚拟专用网络

协议，属于第二层的协议。PPTP 将 PPP（Point-to-Point Protocol）帧封装在 IP 数据报中，

通过 IP 网络如 Internet 或企业专用 Intranet 等发送。

PPTP 协议的基本功能是在 IP 网络中传送采用 PPP 封装的用户数据包。PPTP 客户端负责

接收用户的原始数据，并将之封装到 PPP 数据包，然后在 PPTP 客户端和服务端之间建立

PPTP 隧道传送该 PPP 数据包。

典型的应用通常是 PPTP 客户端部署在远程分支机构或移动办公用户的个人电脑软件中，

他们用来发起 PPTP 隧道。PPTP 服务器部署在企业中心或办公室，用来接收来自 PPTP

客户端的呼叫，当建立起 PPTP 隧道连接后，PPTP 服务器接收来自 PPTP 客户端的 PPP

数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑上。

11.1 PPTP 服务器

远程用户接入的服务器，用户通过客户端接入到 pptp 服务器接入内网。这里服务器 IP 可随便填写，只要不和内网在同一个网段就行。下面两个则填写客户端接入后自动获取的 IP 的范围。



点击添加按钮来添加 VPN 账号和密码



拨入用户可以显示当前已经通过 PPTP 拨入的用户账号



11.2 PPTP 客户端

路由器以客户端直接接入到 PPTP 服务器的网络，相当于子网到子网的虚拟网络连接。既可以使 PPTP 客户端所在设备的内网的主机和 PPTP 服务器内网的主机互访互通，也可以只作为客户端接入 PPTP 服务器实现 VPN 借线。



请注意：V3.0.2 以后的版本才支持 VPN 借线选项，通过该选项，可以使得 PPTP 客户端拨号形成的虚拟线路成为一条具备特定运营商属性的线路，可以参与多线设置中的智能选线，无需再到策略路由或者应用分流里配置规则

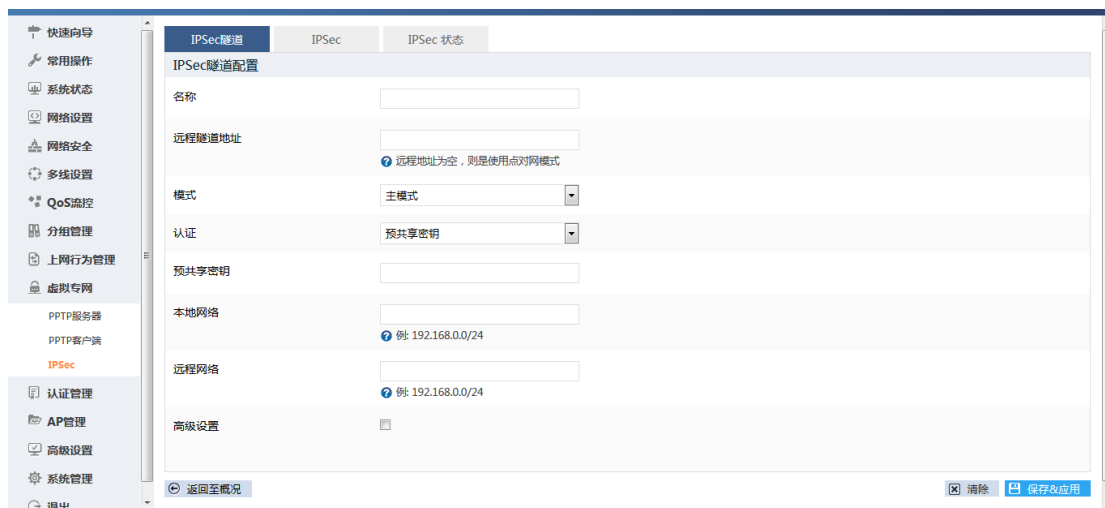
11.3 IPSec

11.3.1 IPSec 隧道

对 IPSec 隧道的参数进行配置，在 IPSec 隧道点添加



远程隧道地址填写公网 IP，本地和远程网络填写网段，并且不能一样。



然后勾选高级设置，在里面设定密钥交换过程的加密、认证方式，IPSec 预共享密钥的加密、认证方式。PFS 组与 IKE DH 组可以不一致，并且数字越大 VPN 性能会越低。其他的内容按照默认值就可以了。

高级设置 ☒

IKE 生存时间 28800 单位: 秒

IKE 加密方式 3DES

IKE 认证方式 MD5

IKE DH组 2

IPSec 生存时间 3600 单位: 秒

IPSec 加密方式 3DES

IPSec 认证方式 MD5

PFS组 2

DPD 超时时间 0 单位: 秒

DPD 重试间隔 5 单位: 秒

返回至概况 清除 保存&应用

11.3.2 IPSec

打勾启用 IPSec

IPSec隧道 IPSec IPSec 状态

启用 ☒

监听端口 wan

清除 保存&应用

11.3.3 IPSec 状态



11.4 L2TP 服务器

L2TP (Layer 2 Tunneling Protocol , 二层隧道协议) 是 VPDN (Virtual Private Dial-up Network , 虚拟私有拨号网) 隧道协议的一种。



点击添加按钮来添加 VPN 账号和密码



拨入用户可以显示当前已经通过 L2TP 拨入的用户账号



11.5 L2TP 客户端

根据具体信息填写数据，

借线选项的作用是，使得 vpn 线路模拟某个运营商线路，也参与“智能选线”。如通过 vpn 模拟电信线路，则应选择“借电信线”，如模拟联通线路，则应选择“借联通线”

网络设置

网络安全

多线设置

QoS流控

分组管理

上网行为管理

认证管理

虚拟专网

PPTP服务器

PPTP客户端

L2TP服务器

L2TP客户端

IPSec

AP管理

高级设置

客户端设置

启动L2TP客户端

服务器地址

用户名

密码

借线选项

服务器内网网段

服务器内网掩码

刷新状态

状态

远端服务器的IP地址或者域名

可选，如果需要和服务内网的主机通信必须要设置

可选，如果需要和服务内网的主机通信必须要设置

巴 刷新

未连接

十二 认证管理

12.1 通用公告

12.1.1 通用公告

快速向导

常用操作

系统状态

网络设置

网络安全

多线设置

QoS流控

分组管理

上网行为管理

虚拟专网

认证管理

通用公告

PPPoE服务器

AP管理

高级设置

系统管理

通用公告

白名单

在线用户

启用

启用通知推送

通用公告网页模板

微信认证

启用强推首页

强推首页URL

空闲超时时间（分钟）

允许上网时间（分钟）

最大接入客户端数

不启用则本页的所有设置都不会生效

只有启用后，通知推送才能生效，推送的内容是网页模板。

浏览... 未选择文件。
请预先准备好模板，按要求填入通知内容、联系方式等信息，然后在这里点击浏览导入。不导入将使用默认通用公告模板

只有启用后，强推首页才能生效。请注意，通知推送和强推主页可以一起使用，也可以单独使用，但你至少要启用一个。

http://www.so.com
请以http://开头如：http://www.so.com

10

360

100

清除 保存 & 应用

本页用来设置路由器通知推送、强推首页、微信认证等相关功能。

“通知推送”是指当内网用户用浏览器试图访问网络资源时，路由器以网页的形式强制向用户推送通知。用户只有点击该通知页面才能继续访问网络。路由器内置默认通知页面如下图，可以通过修改推送模板文件来改变通知推送的页面内容。通用公告模板和模板修改方法的资料可以到国云官方 FTP 服务器中下载获取。



“强推首页”是指当用户点击通知推送页面后，路由器强制推送的一个网站页面，该网站页面可以通过设置“强推首页 URL”来定制。

“微信认证”是指用户需要关注公众微信号，才能接入网络。

具体设置项说明如下：

“空闲超时时间（分钟）”：设置本参数后，当内网 PC 没数据发送即空闲时间超过设定的时间后，路由器会再次推送通知。

“允许上网时间（分钟）”：当内网 PC 接入网络的时间超过设定的时间后，路由器会再次推送通知。

“最大接入客户数”：绑定的 LAN 口能允许接入的最大 PC 数。

“绑定的 LAN 接口”：指定通用公告功能所应用的 LAN 口。

12.1.2 白名单



通过设置“内网主机白名单”，可以让内网某些 PC 不受通用公告规则的影响；而通过设置“URL 白名单”可以让内网 PC 访问某些特定的网页时不受通用公告规则的影响。

12.1.3 在线用户



“在线用户”页面可以显示受通用公告规则影响的主机信息。包括 IP 地址、MAC 地址、认证状态、在线时间。

12.2 PPPoE 服务器

可以将路由器配置为一台 PPPOE 服务器，使内网用户只有通过 PPPoE 拨号才能上网，并可以自由控制其上网期限，网络使用到期后自动停网。省去了管理员单独对每个用户进行管理的难度。

请注意本功能的菜单位置：【认证管理】-->【PPPoE 服务器】

12.2.1 服务器设置

设置 PPPOE 服务器的相关参数。

“DNS 服务器”、“备用 DNS 服务器”两项，请填入路由器所接外线所属运营商提供的 DNS 服务器 IP 地址。

The screenshot displays the 'PPPoE 服务器' (PPPoE Server) configuration page. The left sidebar contains navigation options like '快速向导', '常用操作', '系统状态', '网络设置', '网络安全', '多线设置', 'QoS流控', '分组管理', '上网行为管理', '虚拟专网', '认证管理', '通用公告', 'PPPoE服务器', 'AP管理', '高级设置', '系统管理', and '退出'. The main content area is titled '服务器设置' and includes tabs for '用户管理', '账号批量导入', and '在线用户'. Under '配置PPPoE拨号服务器相关信息', the '启动PPPoE服务器' checkbox is checked. The '本地IP地址' (Local IP Address) is set to 10.0.0.1. The '最大拨号用户数' (Maximum number of users) is 64. The '分配给内网拨号用户的IP网段和掩码' (IP address range for internal users) is 10.67.7.0/24. The 'DNS服务器' (DNS server) is 8.8.8.8, and the '备用DNS服务器' (Backup DNS server) is 208.67.222.222. The '只允许PPPoE拨号上网' (Allow only PPPoE dial-up) checkbox is unchecked. The '禁止单号多拨' (Prohibit single number multi-dial) checkbox is unchecked. The '绑定的LAN接口' (Bound LAN port) is set to 'lan'. Red annotations explain that the local IP is for the server, the IP range is for internal PCs, the DNS servers are for local users, and the LAN port is the interface where users can dial up.

12.2.2 用户管理

在本页面可以创建账户密码，供内网用户 PPPOE 拨号使用。

“绑定 IP”一项可以不填，如果绑定 IP，那么所填的 ip 必须在 PPPOE 服务器设置的“分配给内网拨号用户的 IP 网段”中，而且绑定 ip 后，与此 ip 绑定的帐号只能同时在一台 PC 上使用。

“到期时间”的格式为：年-月-日 时-分-秒，日与时之间有空格。如果不做时间限制，请留空，不填写。

快速向导
常用操作
系统状态
网络设置
网络安全
多线设置
QoS流控
分组管理
上网行为管理
虚拟专网
认证管理
通用公告
PPPoe服务器
AP管理
高级设置
系统管理
退出

服务器设置 用户管理 账号批量导入 在线用户

用于增加 / 删除用户帐号，设置用户帐号的权限。请注意您给用户绑定的IP地址必须在PPPoe服务器中设置的拨号用户网段范围内，比如，PPPoe服务器中网段如设置为10.67.7.0/24,那么绑定IP必须在10.67.7.1到10.67.7.254之间。

PPPoe用户参数设置

回到上一级

激活 ☒

用户帐号名称
由字母和数字组成，不能有空格

密码

确认密码

绑定IP
可不填，如果您选择要绑定IP，那么此IP必须与PPPoe服务器中设置的网段一致，比如，PPPoe服务器中网段如设置为10.67.7.0/24,那么绑定IP必须在10.67.7.1到10.67.7.254之间，绑定IP后，同一个帐号只能同时拨号一次

到期时间
请用YYYY-MM-DD HH:MM:SS时间格式，如2018-08-08 18:18:18，如不作时间限制，那么请留空

返回至概况 清除 保存&应用

显示并设置PPPoe用户的账号信息

搜索:

激活	用户帐号名称	绑定IP	到期时间
☒	test	10.67.7.2	2015-10-10 23:59:59

添加 1-1 共1行 10 1

清除 保存&应用

12.2.3 账户批量导入

“帐号批量导入功能”可以一次性导入多个帐号密码信息，批量增加帐号的格式为：

用户名 密码 激活状态 绑定 IP 到期时间，每个参数中间有一个空格。

注意：

- 1、在“批量增加或编辑账号”的方框中增加帐号时，不能清除已经存在的帐号，而只能追加帐号，否则清除的帐号将会被自动删除，在“用户管理”中将不存在。
- 2、批量添加帐号时，除了用户名，其他参数都是可选的，比如可以只填用户名，密码将会自动生成，并自动激活帐号。
- 3、可以将“批量增加或编辑账号”方框中的帐号信息选中，并复制到外部文件中，从而实现导出帐号信息的功能。



注意：

1. 账号批量导入界面中，全部选中后，可以批量拷贝出来，从而实现账号批量导出
2. 账号批量导入界面中，当您只提供了用户名，点击保存&应用，那么密码会自动创建并激活，可以大幅减少您批量创建账号的工作量。



点击保存应用后，将看到自动生成了密码并且激活，如下图



12.2.4 在线用户

显示当前拨号用户的账号，ip 信息。



十三 AP 管理

13.1 系统管理

13.1.1 系统设置

开启或关闭 AC 功能



13.1.2 AP 升级

可以针对不同型号的 AP 批量升级。



13.1.3 AP 重启

可以指定 AP 批量重启



13.1.4 恢复出厂

可以指定 AP 批量恢复出厂值



13.2 监控统计

13.2.1 AP 信息

显示路由器发现的 AP 的相关信息，需要将 AP 加入，路由器才能管理 AP。



13.2.2 AP 状态

显示 AP 的相关状态

快速向导

常用操作

系统状态

网络设置

网络安全

AP信息

AP状态

用户信息

搜索:

AP名字	IP地址	MAC地址	无线模式	信道	功率	用户数量	在线时间	SSID1	SSID2	SSID3	SSID4
zqsyb	192.168.255.12	ac:31:9d:aa:3d:08	11bgn	6	100%	0	04:54:14	4567			

13.2.3 用户信息

显示 AP 当前连接的无线终端信息

快速向导 常用操作 系统状态 网络设置 网络安全	AP信息 AP状态 用户信息			
	搜索:			
	MAC地址	AP名字	SSID	在线时间
	5c:63:bf:2e:0e:6d	zqsyb	4567	00:00:18

13.3 配置管理

13.3.1 无线模板

此页面用来创建 SSID 无线模板，路由器通过下发配置可将模板中的 SSID 参数应用于 AP。

快速向导 常用操作 系统状态 网络设置 网络安全 多线设置 QoS流控	无线模板 AP配置列表							
	无线模板应用于AP配置，作为AP配置的一部分							
	搜索:							
	SSID	启用	隐藏SSID	广播SSID	客户端隔离	加密类型	算法	密码
	4567	启用	关闭	开启	开启	不加密	无	

快速向导 常用操作 系统状态 网络设置 网络安全 多线设置 QoS流控 分组管理 上网行为管理 虚拟专网 认证管理 AP管理	无线配置	
	增加修改无线模板	
	SSID	4567
	启用	启用
	隐藏SSID	关闭
	广播SSID	开启
	客户端隔离	开启
	加密类型	不加密
	不加密 WPA-PSK WPA2-PSK WPA/WPA2-PSK	
	返回至概况 清除 保存&应用	

13.3.2 AP 配置列表

此页面用来配置 AP 的名称、IP 地址、用户限制数、信道、功率等其他参数。点击“下发到 AP”按钮将配置下发到 AP。

选择	AP名字	MAC地址	无线使能	IP地址	无线模式	信道	信道带宽	功率	SSID1	用户限制	操作
☐	zqsyb	ac:31:9d:aa:3d:08	开启	192.168.255.12	11bgn	6	20MHz	100%	4567	20	

十四、无线设置

只有带无线的部分型号的路由器才有无线相关设置。

14.1 基本设置

14.1.1 网络设置

本页面可设置无线禁用、SSID、加密类型、加密算法、密码等参数。



注意:

1. 支持 Windows 的中文 SSID 只有 V3.0 以后的版本才支持。
2. 绑定 LAN 接口是指无线绑定到特定的 LAN 接口，与该 LAN 接口共用 IP 地址、DHCP 服务、Portal 认证等设置和策略，有助于多个 SSID 存在的情况下随同其绑定的 LAN 接口使用不同的配置策略，比如使用不同的 Portal 认证策略：无线主网络不使用 Portal 认证，而无线客人网络则使用 Portal 认证。只有多个独立 LAN 存在的情况才能做上述配置，多个独立 LAN 口相关设置请参考【高级设置】-->【弹性端口】相关说明。

14.1.2 安全设置

本页面可设置无线安全相关参数



14.2 客人网络

路由器可以启用第二个 SSID 来供客人使用，并可以针对这个 SSID 作相应安全设置。

14.2.1 网络设置

本页面用来启用和设置客人网络的 SSID 参数

网络设置 安全设置

禁用 ☒ 启用客人SSID

SSID alex-Guest
支持中文，长度小于32

加密类型 WPA2-PSK

加密算法 AES

密码 12345690
由字母和数字组成，长度是8到63个字符

清除 保存&应用

14.2.2 安全设置

本页面用来设置客人网络的相关安全参数。

网络设置 安全设置

隐藏SSID ☐

孤立客人网络 ☒ 禁止客人网络的用户和主网络、有线网络通信
勾选后，客人SSID下的终端无法与路由器其他网络下用户通信，一般勾选此项。

隔离接入用户 ☒ 禁止接入无线用户之间的通信
勾选后，同在客人SSID下的终端也无法通信

最大接入用户 20
0表示不受限

MAC过滤
☒ 禁用
☐ 仅允许列表内
☐ 仅允许列表外

MAC列表

清除 保存&应用

14.3 高级设置

14.3.1 设备设置

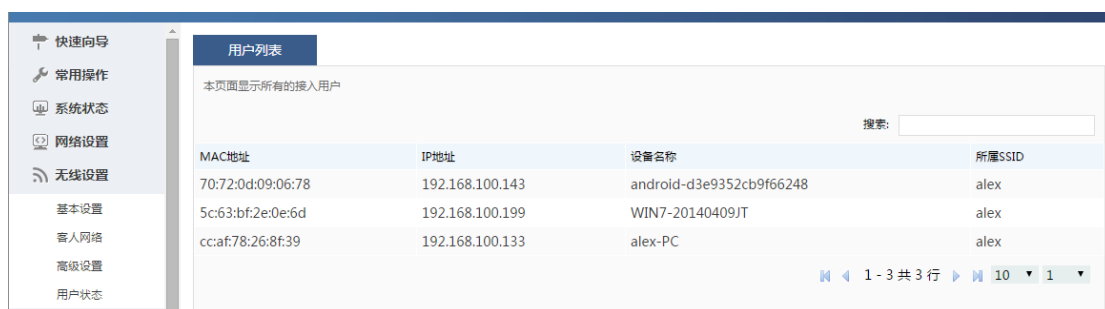
本页面用来设置无线模式、信道、发送功率等相关参数。



14.4 用户状态

14.4.1 用户列表

本页面显示所有 SSID 下连接的用户终端的相关信息



十五 高级配置

15.1 接口高级设置

该页面可设置 WAN 口的权重（越大越优）和工作模式（一般默认为 NAT 模式）。



注意：

1. 当您选择路由模式时，上一级路由必须配置回程路由，否则将无法上网
2. 接口权重默认将根据线路带宽来确定。多线智能选线模式下，会优先从同一个运营商线路中选择权重最大的线路来参与智能选线；当一条应用分流规则中，当有多条线路参与分流时，会根据权重来分配流量比例；当一条策略路由规则中，当有多条线参与时，也会根据权重来分配流量比例

15.2 接口模式

在本页面中，您可以对以太网接口的工作模式进行设置。



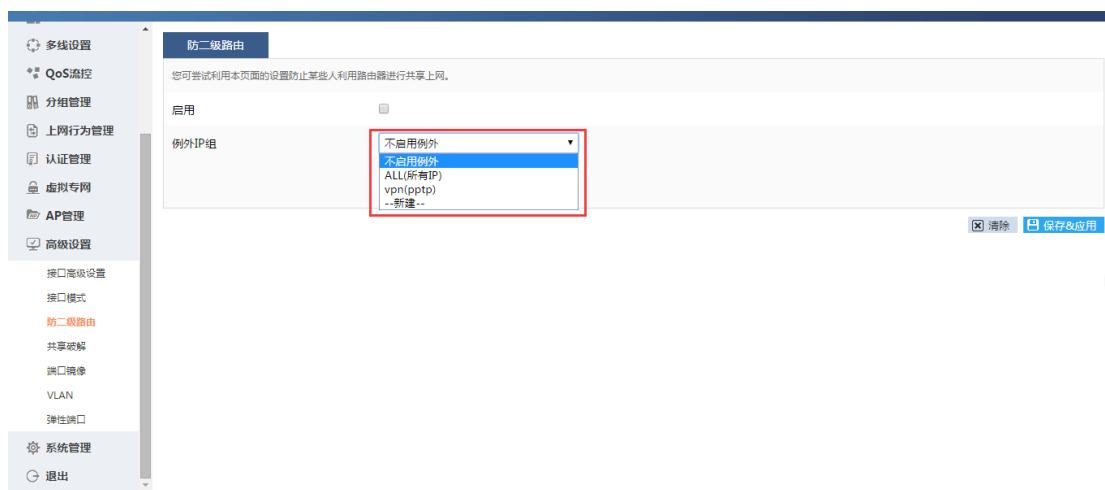
请注意：软路由此处会显示网口的网卡芯片类型，如下图：



可以帮助您判断外网接口通用名称 WAN*所对应的网口。

15.3 防二级路由

您可尝试利用本页面的设置防止某些人利用路由器进行共享上网。



可启用例外，使例外分组不受防二级路由约束

15.4 共享破解

中国有些地区的运营商利用网络尖兵等工具对网络共享进行限制，您可尝试利用本页面的设置进行破解。



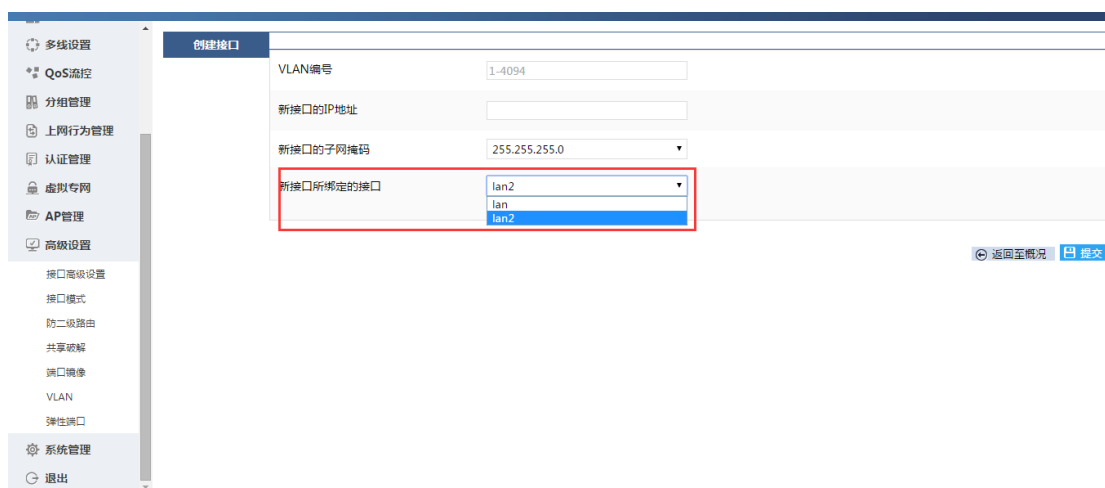
15.5 端口镜像

此页面的 LAN1、LAN2、WAN1 等，是路由器面板上标注的接口，并非网络配置中的 LAN1、LAN2 等。



15.6 VLAN

此页面可以添加虚拟子接口，可虚拟一个内网 LAN 口。点击添加创建虚拟接口



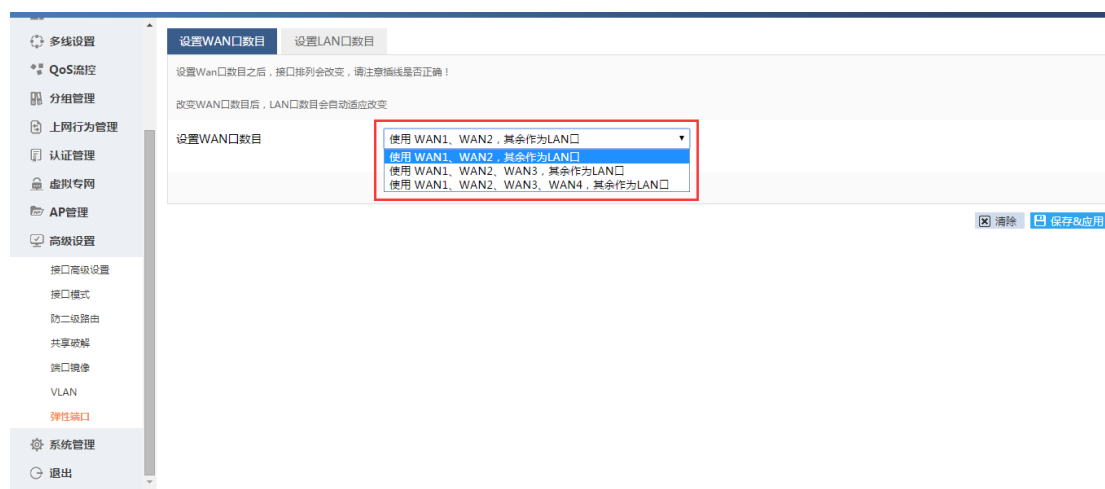
填写该接口 IP 地址、掩码和该接口所绑定的 LAN 口。绑定的物理接口可根据需要设定。



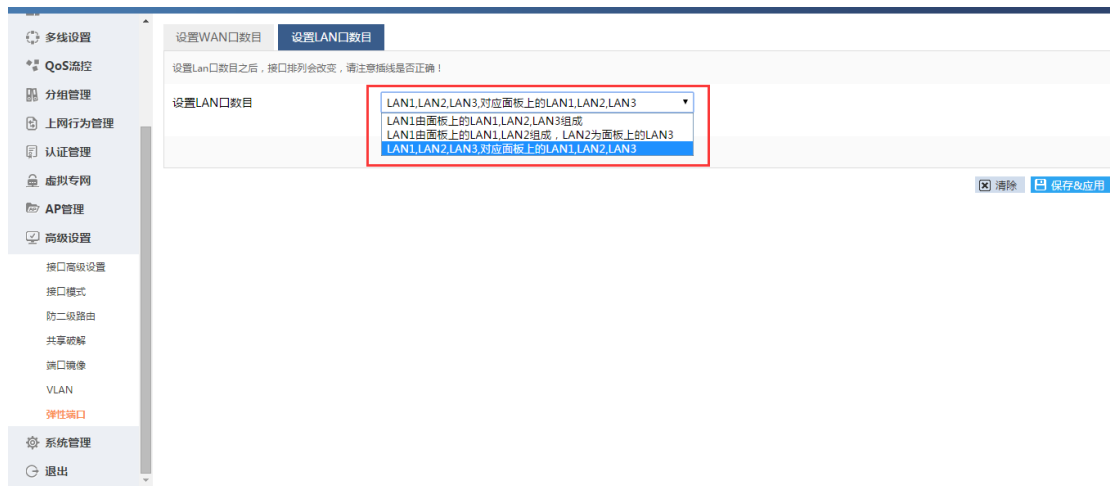
点击编辑按钮可对接口地址进行修改

15.7 弹性端口

当您有多条连接 internet 的线路，然而在外网设置下只有两个 WAN 口，这时可以在【高级设置】--》【弹性端口】中设置 WAN 口数，满足多条线路上网的需求。例：当有 3 条线路上网时，可设置为“使用 WAN1、WAN2、WAN3，其余为 LAN 口”此时 WAN1、WAN2、WAN3 对应路由器面板上的 WAN1、WAN2、WAN3



同理在该菜单下可设置路由器 LAN 口数目，可将面板上的 LAN1、LAN2、LAN3 口设置为单独的 LAN 口。上例已经设置了 3 个 WAN 口，剩下 2 个 LAN 口，此时可在设置 LAN 口数下设置“LAN1、LAN2 为对应面板上的 LAN1、LAN2”。也可以不用设置 LAN 口数，但此时路由器 WEB 界面就显示为 LAN 口，即该 LAN 口为 LAN1、LAN2 组成。如下图：



注意：

- 1、 RN1000/RN2000/RN4000/RN2200/RE1500/RE3500/RE4500 在设置好弹性端口后设备都要重启，且恢复出厂值后该配置依然生效。
- 2、 在设置 LAN 口数时，内网会短暂断网
- 3、 设置好 LAN 口数后，通用公告（网吧 WiFi 认证）、DHCP、PPPoE 服务器、内网设置页面都会相应变化，会给出 LAN 口选择
- 4、 当您内网需要将无线网和有线网进行物理隔离时，建议使用两个独立的 LAN 口分别有线局域网和无线局域网

通用公告



可根据需求选定绑定 LAN 口

PPPOE 拨号

DHCP

接口	网关IP地址	主DNS服务器	次DNS服务器	租约时间	地址池起始IP	地址池结束IP
lan2	192.168.255.252	192.168.255.252	8.8.8.8	120	192.168.255.2	192.168.255.254

可根据需求添加扩展 DHCP

十六、 系统管理

设置路由器本身相关的一些参数，路由器自身参数设置。

16.1 系统设置

这里可以配置路由器的部分基本信息，比如主机名和时区。

16.1.1 基本设置

设备名修改后，会显示在首页（系统状态--》概览）的右上角

16.1.2 日志

日志有利我们查看路由器的工作状态的历史记录，了解路由器的健康状态。

16.1.3 Web 界面参数设置

此功能 V2.1 以后的版本才支持



勾选启用了“基于接口的应用统计”后，在【系统状态】-->【应用统计】会出现接口选项，如下图：



16.2 路由密码

供您修改路由器登陆密码



密码修改成功后，会自动跳转到登陆页面。

提示：RN5000、RN6000、RN8000 等带有两个 USB 接口的路由器，以及基于 X86 平台的软路由，可以通过 U 盘来恢复密码，具体步骤：

1. 准备一个 U 盘，并且将 U 盘格式化为 fat 格式，然后 U 盘根目录里放入一个文件名为 reset_passwd.txt 的空文件
2. 在路由器处于运行状态时，插入 U 盘，1 分钟后拔掉 U 盘，即可恢复密码

注意，通过 U 盘恢复密码时，不会重启路由器，也不会影响路由器的正常运行。

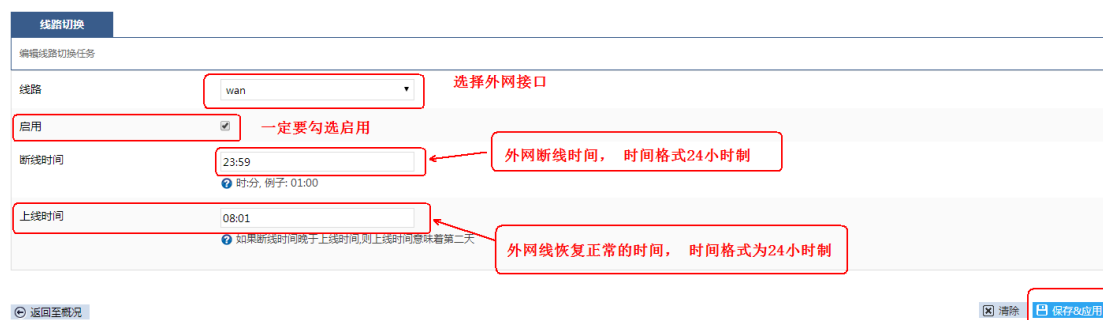
16.3 定时任务

16.3.1 线路切换

一些地区光纤专线晚上 24 点左右断线，早上 8 点左右恢复，通过线路切换可平滑切换到备用线，从而有效避免大面积掉线



点击添加后可见到如下页面



上图中假设外网口（WAN 口）在晚上 24 点断线，早上 8 点恢复正常，一般我们在设置时建议断线时间提前一分钟，而恢复时间则延后一分钟。

注意，使用定时任务实现平滑切换的前提条件：有可用的备用线路

16.3.2 定期重启

可定时重启设备，即可按天、周、月周期性执行，也可以只执行一次

16.3.3 定期升级

可实现定时自动在线升级，即可按天、周、月周期性执行，也可以只执行一次

启用后，将自动到云端检查新版本，有新版本则在设定时间自动升级到新版本

16.3.4 定期特征库更新

可实现定时自动在线升级特征库，既可按天、周、月周期性执行，也可以只执行一次

启用后，将自动到云端检查是否有特征库新版本，如有新版本则在设定时间自动升级到特征库最新版本

16.3.5 定期运营商路由表更新

可实现定时自动在线升级运营商路由表，既可按天、周、月周期性执行，也可以只执行一次

启用后，将自动到云端检查是否有运营商路由表更新，如有新版本则在设定时间自动升级到最新的运营商路由表

16.4 诊断工具

方便您维护您的网络，快捷的查找网络故障点。

Ping 工具：诊断连通性。

Traceroute：查找路径，定位故障点。

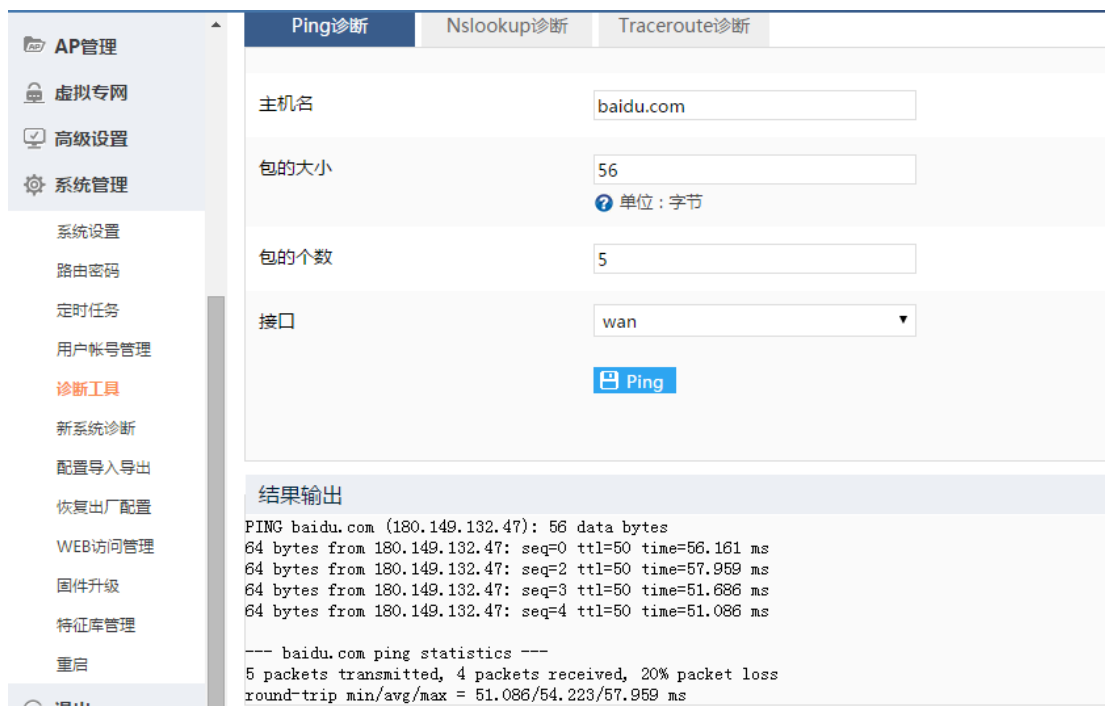
Lookup：域名解析查询，一般多用邮件排障。



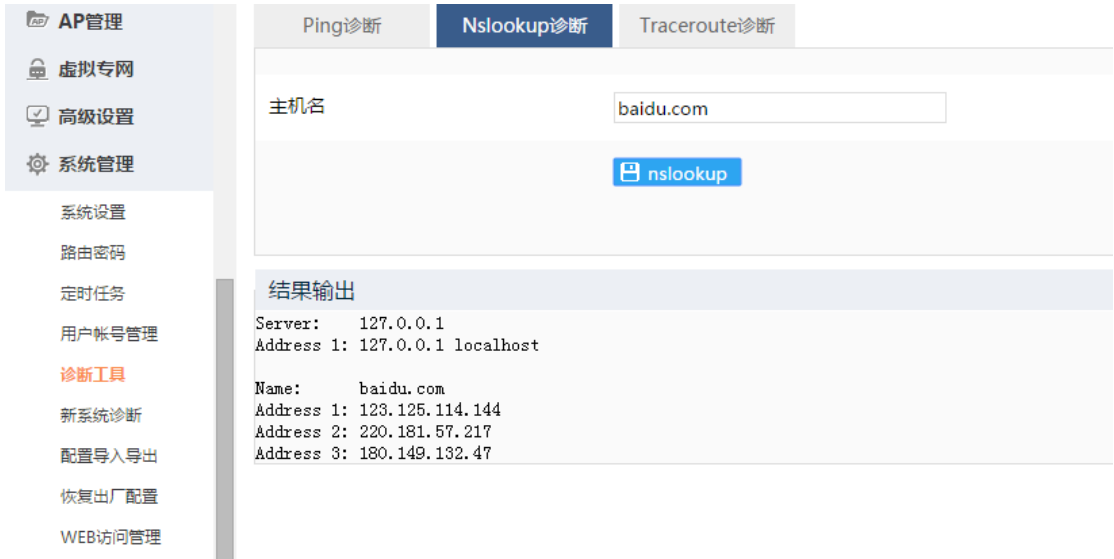
V3.0 最新版本有所修改，请参考如下说明

方便您维护您的网络，快捷的查找网络故障点。

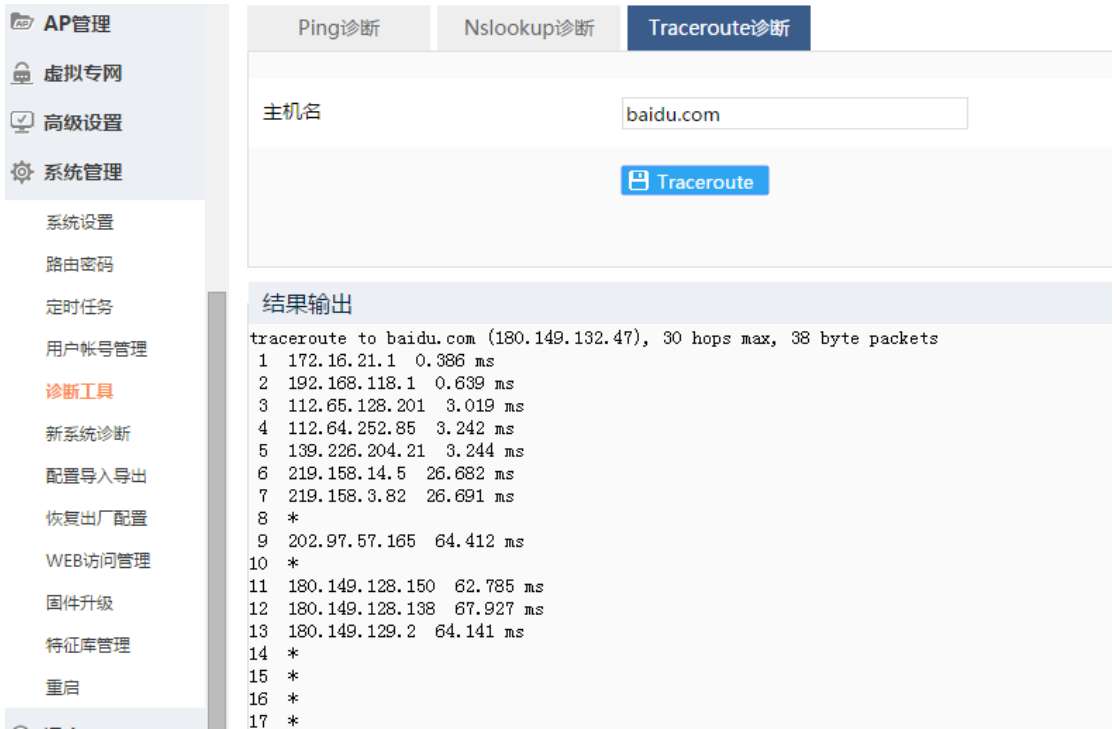
Ping 工具：诊断连通性。



NSLookup：域名解析查询，一般多用邮件排障。



Traceroute：查找路径，定位故障点。



16.5 新系统诊断

16.5.1 新系统诊断



16.5.2 游戏诊断



注意：V3.0 版本将不再需要选择游戏进行诊断，只要选择 IP 和接口即可，如下图所示：

新系统诊断		游戏诊断	
主机IP	172.16.21.106		
接口	wan		
检查			
检测结果	炫舞时代 天龙八部 延时时间(最小值/平均值/最大值)是29.453/29.646/29.831毫秒		

此时显示的 172.16.21.106 上正在玩炫舞时代和天空八部，这两个游戏服务器的平均延时为 29 毫秒左右。

16.6 配置导入导出

16.6.1 配置的导出

导入导出路由器配置。方便用户管理快捷配置路由器。



16.6.2 导入配置文件

把保存好的用户配置文件导入，方便用户快速配置路由器，或者恢复某个时间段的配置。



请注意，

1. 导入配置后，设备会自动重启。
2. 不同机型之间请勿进行配置导入

16.7 恢复出厂设置

通过恢复出厂设置，路由器会清空所有的用户的配置文件，恢复设备出厂的设置。



提示：

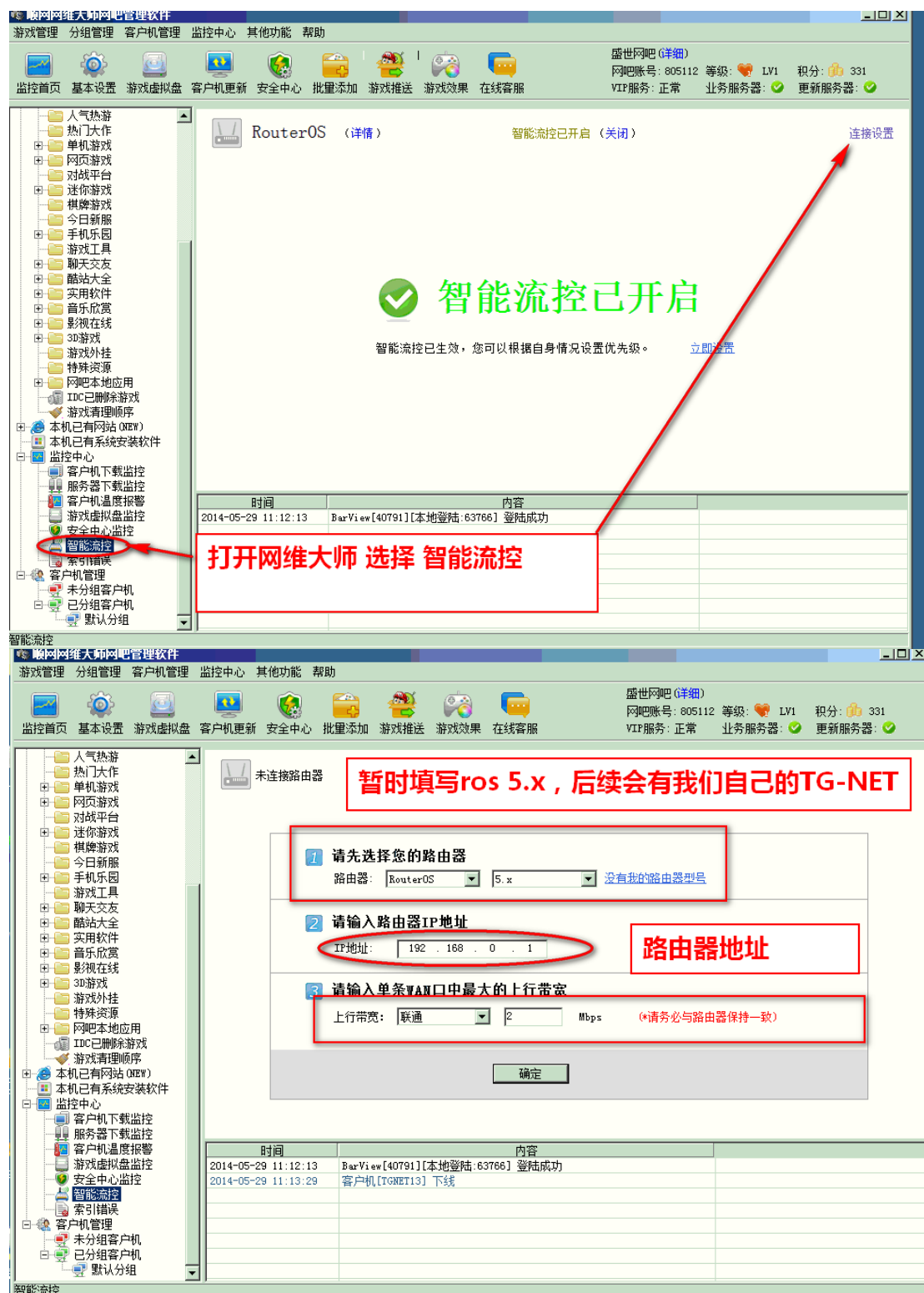
提示：RN5000、RN6000、RN8000 等带有两个 USB 接口的路由器，以及基于 X86 平台的软路由，可以通过 U 盘来恢复出厂配置，具体步骤：

1. 准备一个 U 盘，并且将 U 盘格式化为 fat 格式，然后 U 盘根目录里放入一个文件名为 reset_factory.txt 的空文件
2. 在路由器处于运行状态时，插入 U 盘，1 分钟后拔掉 U 盘，即可恢复出厂状态，恢复出厂后，路由器将自动重启。

注意：如果系统本身奔溃了，通过 U 盘是无法恢复出厂的

16.8 顺网合作

基于顺网的网维大师 8200 以上版本（包括 8200），根据顺网的网维大师对各种进程进行识别，我们的路由器进行智能流控。



16.9 web 访问管理

设置访问界面的端口。



16.10 特征库升级

特征库(又称 DPI 特征库)是流控和分流的核心基础，DPI 识别数据的升级，可提高对应用程序的识别率。



当您真正开始执行升级后，会显示一个升级进度条，此进度条会在几十秒钟内展示完毕，然后跳转到首页。此处请注意，当您使用 IE6、IE8 浏览器或者相应的兼容模式

时，进度条可能不会正常工作。推荐您使用谷歌浏览器、360 浏览器极速模式等 chrome 内核的浏览器进行操作。

注意：请不要在高峰期升级特征库。

当您需要在某个适当的时候在线升级到最新特征库版本，那么可到【系统管理】--》【定时任务】--》【特征库升级】进行操作。

16.11 固件升级

固件升级，即路由器软件系统升级，一般升级都会重启，在升级过程中，请勿断电，点击固件升级后，固件文件先会验证一下，请等待一会儿

16.11.1 在线升级

通过网络实现自动升级到最新版本。



当您真正开始执行升级后，会显示一个升级进度条，此进度条会在几分钟内展示完毕，然后跳转到首页。此处请注意，当您使用 IE6、IE8 浏览器或者相应的兼容模式时，进度条可能不会正常工作。推荐您使用谷歌浏览器、360 浏览器极速模式等 chrome 内核的浏览器进行操作。

升级完毕，设备会自动重启。

当您需要在某个适当的时候在线升级到最新版本，那么可到【系统管理】-->【定时任务】-->【定时升级】进行操作。

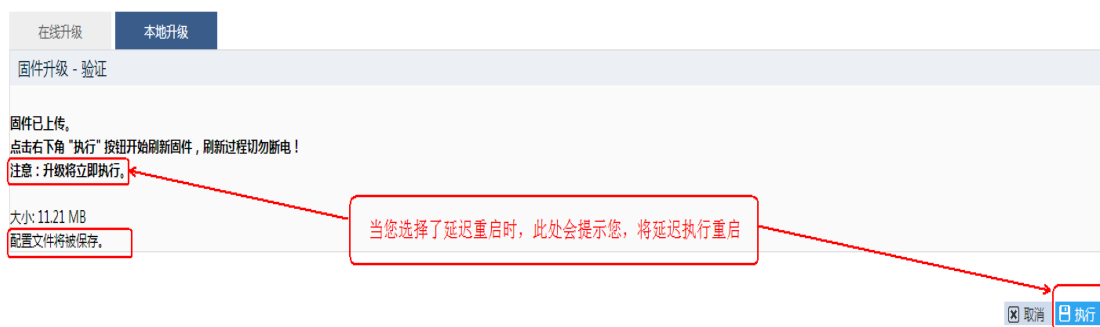
16.11.2 本地升级



固件上传后，将跳转到如下界面：



注意，3.0 以后的固件版本自动进行校验，所以上图中的校验相关信息不会显示。



当您点击了上图中的执行后，会显示一个升级进度条，此进度条会在几分钟内展示完毕，然后跳转到首页。此处请注意，当您使用 IE6、IE8 浏览器或者相应的兼容模式时，进度条可能不会正常工作。推荐您使用谷歌浏览器、360 浏览器极速模式等 chrome 内核的浏览器进行操作。

16.12 重启

通过 web 路由器界面重启路由器





此处请注意，当您使用 IE6、IE8 浏览器或者相应的兼容模式时，进度条可能不会正常工作。推荐您使用谷歌浏览器、360 浏览器极速模式等 chrome 内核的浏览器进行操作。

十七、退出

退出本次登陆，返回到登陆界面。