



路由器产品用户手册

TG-NET_路由器用户手册 V3.2 (AC 版)

©copyright2011 by Shenzhen TG-NET Botone Technology Co.,Ltd. All rights reserved.

事先未征得深圳市万网博通科技有限公司（以下简称 TG-NET）的书面同意，任何人不得以任何方式拷贝或复制本文档中的任何内容。

TG-NET 不做与本文档相关的任何保证，不做商业性、质量或特定用途适用性的任何隐含保证。本文档中的信息随时可能变更，而不另行通知。TG-NET 保留对本出版物做修订而不通知任何个人或团体此类变更的权利。

深圳市万网博通科技有限公司

总部地址：深圳市南山区中山园路 1001 号国际 E 城 E3 栋

工厂地址：深圳市龙华新区大浪街道华荣路北昱南通科技工业园 2 栋

邮编：518052

服务电话：400-088-7500

网址：<http://www.tg-net.cn>

注明：只有REC、RSC系列产品才有AC功能。

目录

路由器产品用户手册	1
目录	2
一、 设备安装使用向导	10
1.1 安装注意事项.....	10
1.2 设备使用说明.....	10
1.3 上网基本设置.....	11
1.3.1 登陆路由器的 web 管理界面	11
1.3.2 TG-NET 路由器设置上网	18
二、 快速配置向导.....	22
2.1 快速向导.....	22
三、 常用操作	25
3.1 外网配置.....	25
3.1.1 拨号上网	26
3.1.2 固定 ip.....	26
3.1.3 DHCP 上网.....	27
3.2 内网配置.....	27
3.3 端口映射.....	29
3.4 智能流控.....	29
3.5 多线策略.....	29
四、 系统状态	29
4.1 概览	29

4.2 路由	31
4.3 系统日志.....	32
4.4 实时监控.....	33
4.5 主机监控.....	33
4.6 应用统计	35
4.7 QQ 在线列表	36
4.8 接口概览.....	36
4.8.1 硬件接口.....	36
4.8.2 虚拟接口.....	37
4.8.3 历史流量视图.....	38
五、 网络设置.....	38
5.1 接口概览.....	38
5.2 外网配置.....	39
5.3 内网配置.....	39
5.4 DHCP	39
5.4.1 DHCP 设置.....	39
5.4.2 多 LAN 扩展 DHCP	40
5.4.3 DHCP 静态分配.....	40
5.4.4 DHCP 静态批量配置.....	41
5.4.5 DHCP 活动客户端.....	41
5.4.6 DHCP 检测.....	42
5.5 主机名	43
5.5.1 主机别名.....	43
5.5.2 别名批量	43

5.5.3 主机域名	43
5.6 静态路由	44
5.7 动态域名	45
六、 网络安全	46
6.1 ARP 绑定	46
6.2 ARP 安全	48
6.3 端口映射	50
6.4 连接数限制	54
七、 多线设置	56
7.1 多线策略	56
7.1.1 多线设置	56
7.1.2 应用分流	58
7.1.3 策略路由规则	60
7.1.4 线路侦测	61
7.2 单线多拨	61
7.3 WAN 口扩展	63
八、 QOS 流控	64
8.1 智能流控	66
8.1.1 智能流控	66
8.1.2 例外	66
8.1.3 自定义流控策略	67
8.1.4 QOS 高级设置	67
8.1.5 服务器保障带宽	68
8.2 固定流控	69

九、 分组管理	70
9.1 时间组	71
9.2 地址组	72
9.3 端口组	72
9.4 应用组	73
十、 上网行为管理	75
10.1 一键管控	75
10.1.1 一键管控	75
10.1.2 上网行为管理的高级设置	76
10.2 QQ 在线列表	77
10.3 QQ 白名单	78
10.4 URL 重定向	78
10.5 网址过滤	79
10.5.1 网址过滤	79
10.5.2 网址分类库	80
10.5.3 白名单	80
10.6 防火墙规则	81
10.7 WEB 访问记录	83
10.7.1 上网记录配置	83
10.7.2 上网记录查询	83
十一 虚拟专用网	84
11.1 PPTP 服务器	85
11.2 PPTP 客户端	86
11.3 IPsec	87

11.3.1 IPsec 隧道	87
11.3.2 IPsec	88
11.3.3 IPsec 状态	89
11.4 L2TP 服务器	89
11.5 L2TP 客户端	90
十二 认证管理	91
12.1 通用公告	91
12.1.1 通用公告	91
12.1.2 白名单	93
12.1.3 在线用户	93
12.2 PPPoE 服务器	94
12.2.1 服务器设置	94
12.2.2 用户管理	95
12.2.3 账户批量导入	95
12.2.4 在线用户	97
十三 AP 管理	97
13.1 系统管理	97
13.1.1 系统设置	97
13.1.2 AP 升级	98
13.1.3 AP 重启	98
13.1.4 恢复出厂	98
13.2 监控统计	98
13.2.1 AP 信息	98
13.2.2 AP 状态	99

13.2.3 用户信息.....	99
13.3 配置管理.....	99
13.3.1 无线模板.....	99
13.3.2 AP 配置列表.....	100
十四、 无线设置	101
14.1 基本设置.....	101
14.1.1 网络设置.....	101
14.1.2 安全设置.....	102
14.2 客人网络.....	102
14.2.1 网络设置.....	102
14.2.2 安全设置.....	102
14.3 高级设置.....	103
14.3.1 设备设置.....	103
14.4 用户状态.....	103
14.4.1 用户列表.....	103
十五 高级配置	104
15.1 接口高级设置.....	104
15.2 接口模式.....	105
15.3 防二级路由.....	106
15.4 共享破解.....	106
15.5 端口镜像.....	107
15.6 VLAN.....	107
15.7 弹性端口.....	108
十六、 系统管理	110

16.1 系统设置	110
16.1.1 基本设置.....	111
16.1.2 日志	111
16.1.3 Web 界面参数设置.....	112
16.2 路由密码	112
16.3 定时任务	113
16.3.1 线路切换.....	113
16.3.2 定期重启.....	114
16.3.3 定期升级.....	114
16.3.4 定期特征库更新	115
16.3.5 定期运营商路由表更新	115
16.4 诊断工具.....	116
16.5 新系统诊断.....	119
16.5.1 新系统诊断	119
16.5.2 游戏诊断.....	119
16.6 配置导入导出.....	120
16.6.1 配置的导出	120
16.6.2 导入配置文件	121
16.7 恢复出厂设置.....	121
16.8 顺网合作	122
16.9 web 访问管理.....	123
16.10 特征库升级	124
16.11 固件升级	125
16.11.1 在线升级.....	125

16.11.2 本地升级.....	126
16.12 设备认证.....	127
16.13 重启.....	128
十七、AC 管理.....	129
17.1 快速向导.....	130
17.2 监控统计.....	130
17.3 功能管理.....	135
17.4 AP 基本配置.....	135
17.5 认证营销.....	146
17.6 高级策略.....	149
17.7 交换机管理.....	153
17.8 系统管理.....	159
十八、退出.....	167

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，请您按要求接好电源线，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）。

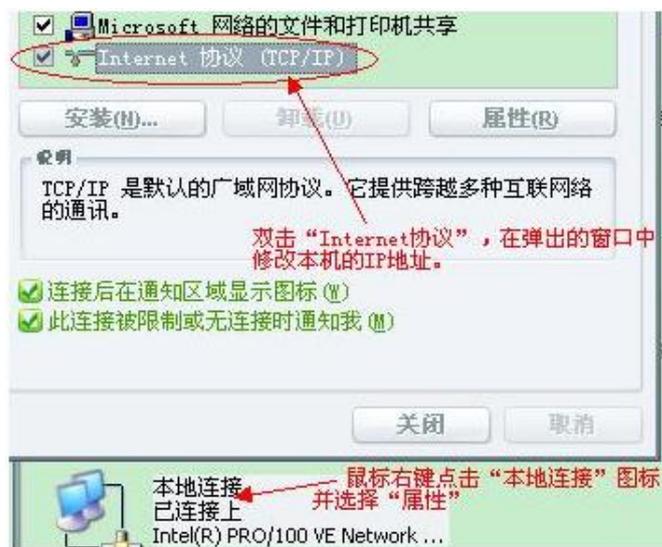


(图 1)



(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 :



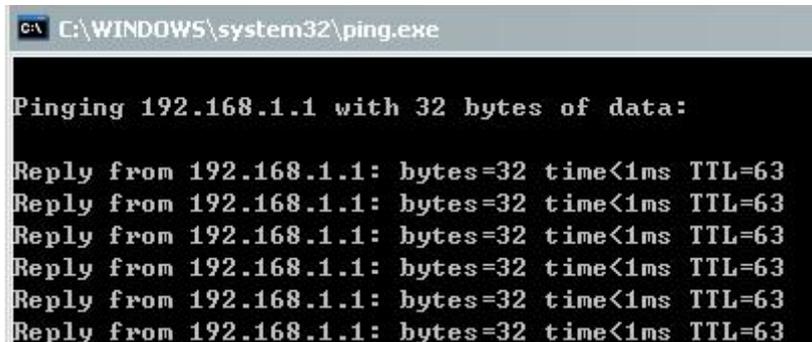
(图 4)

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
```

(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。

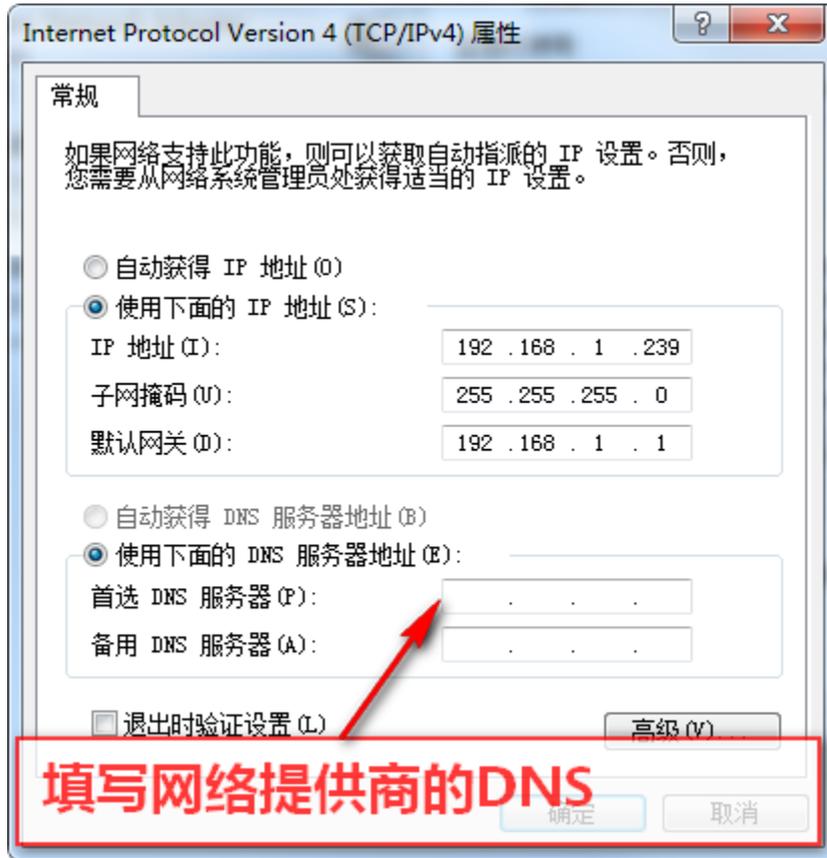
1.3.1.2 windows 7 设置

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)

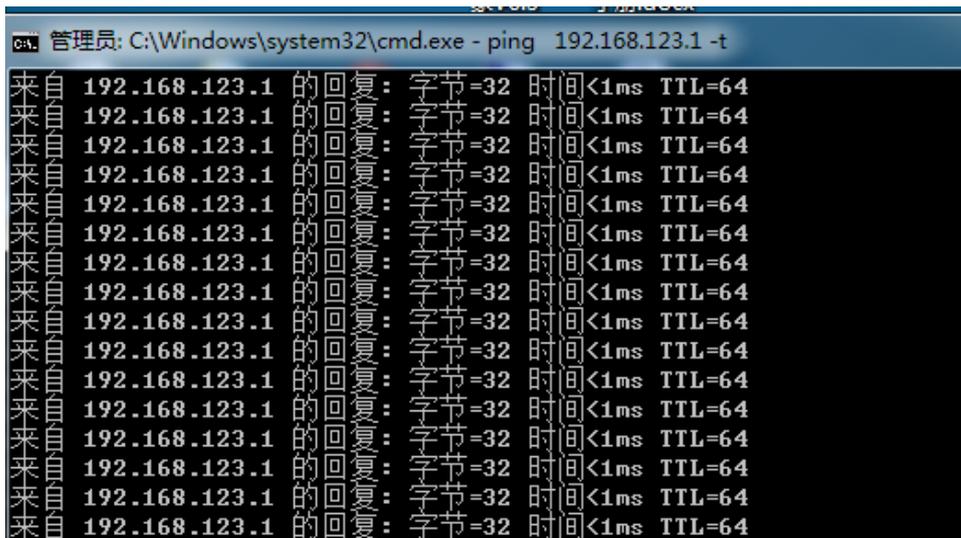
然后在桌面左下角，点击图标，在输入

'ping 192.168.1.1 -t'看看线路是否通畅。如图 11 所示：

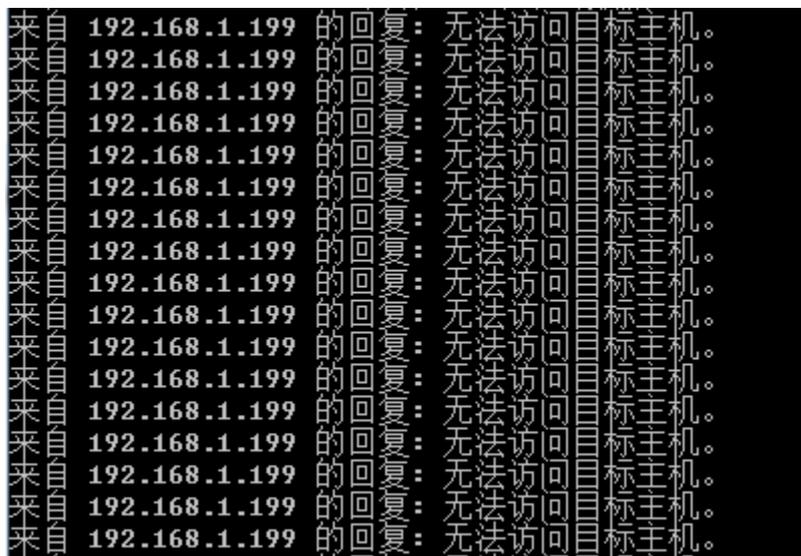


(图 11)

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
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：
密码：
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
此处必须填正确

上网类型及带宽：光纤-10M

参考上行带宽：937.5
上行总带宽单位：KB（千字节每秒）
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

参考下行带宽：937.5
下行总带宽单位：KB（千字节每秒）
勾选此项可以配置wan2，不勾选则跳到内网配置界面

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

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

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

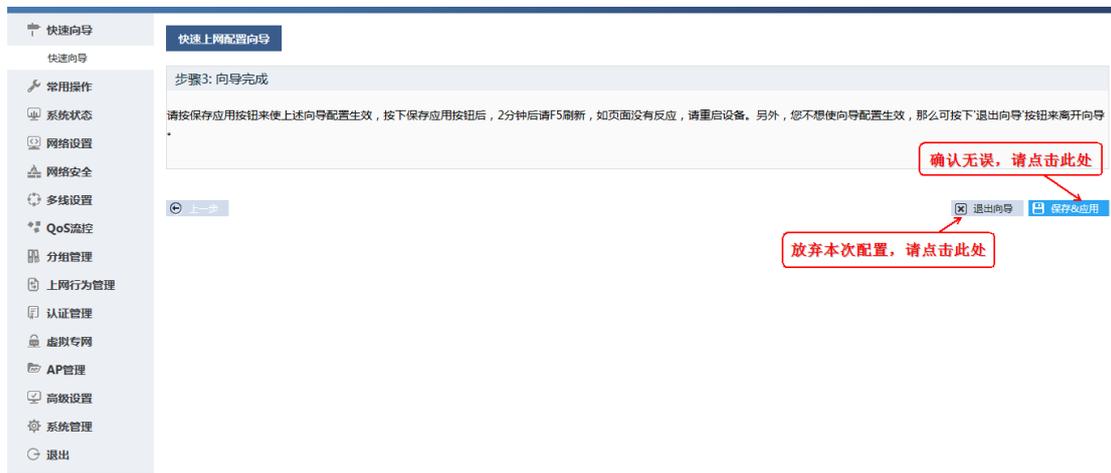
1.3.2.2 配置 LAN 口参数



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



注意事项：

- A). 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；
- B). 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

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

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

线路类型: PPPoE拨号(或ADSL拨号)

用户名: []

密码: []

MAC地址: []

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: 勾选此项可将配置下一个WAN口 (多线路上网用户配置多条上网线路通用)

红色方框中信息由运营商提供

此处必须填写正确

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，可以设置低于 0.9 的值

3.1.2 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: []

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

注意事项：

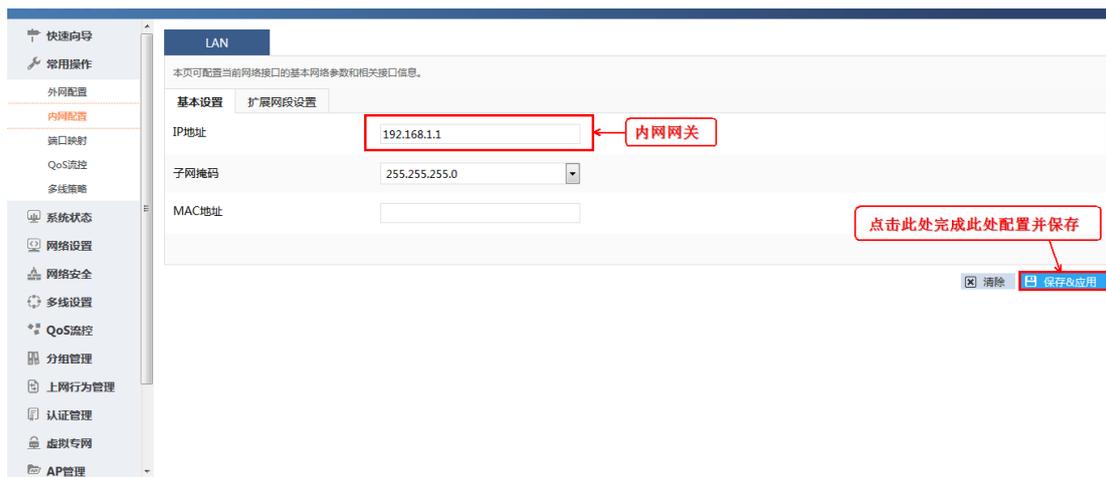
1. 上网服务提供商和带宽信息必须填写准确，如果分类中没有的，勾选其他；（比如长城宽带）
2. 上下行带宽建议设置为总带宽的 0.9 到 0.95，预留部分带宽用于防御突发数据，带宽富裕的地区，可以设置低于 0.9 的值

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。

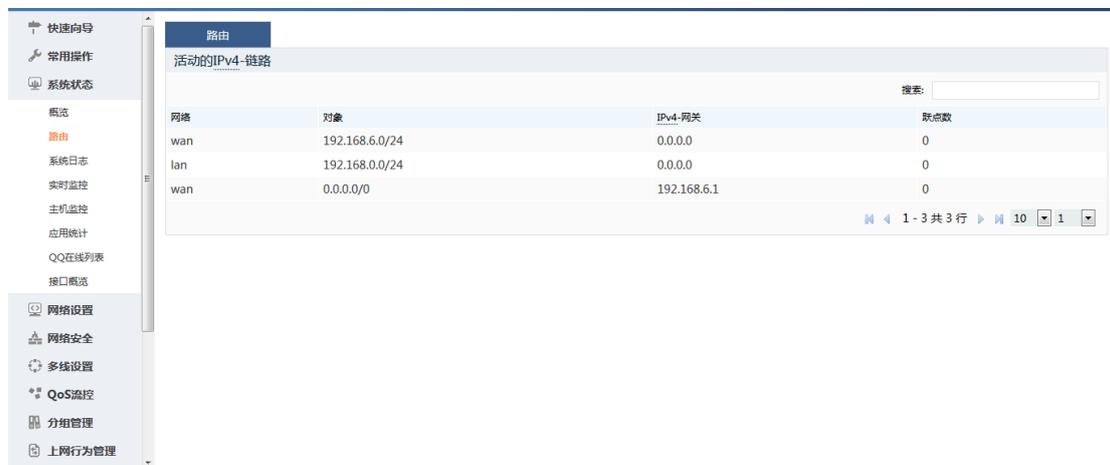
注意事项：

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



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!

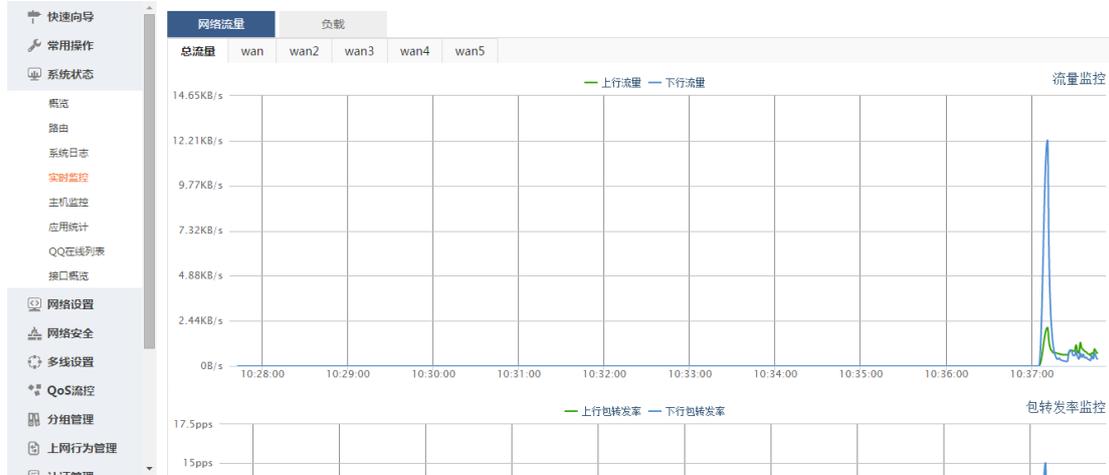
系统日志：显示历史和当前在线主机数

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。

主机	主机别名	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
172.16.21.22	-	37K	5K	2.5G	6.9G	30	172	1天15时15分45秒
172.16.21.42	-	1K	1K	240.8M	2.1G	118	8	1天13时58分37秒
172.16.21.60	-	358	1K	543.4M	7.7G	24	41	1天15时15分38秒
172.16.21.95	-	1K	1K	99.4M	386.3M	23	3	0天22时28分58秒
172.16.21.41	-	180	939	16.8M	60.8M	6	0	1天13时58分35秒
172.16.21.193	-	106	362	784.8M	11.8G	11	6	1天13时58分35秒
172.16.21.108	-	241	322	2.3G	177.3M	82	5	0天4时9分17秒
172.16.21.58	-	85	63	8.1M	79.3M	20	6	1天13时58分40秒
192.168.118.2	-	44	56	1.9M	3.5M	4	1	1天13时58分37秒
172.16.21.50	-	0	26	32.9M	165.5M	11	6	0天4时40分5秒
合计	-	40.02K	9.7K	6.5G	30.25G	352	266	-

基于接口统计：该功能是用来满足用户统计，基于一个或所有接口下主机的实时流量，该功能的使用前提是在系统管理=》系统设置=》web 界面参数设置，基于接口的应用统计处于勾选状态。

点击表格的标题字段可以排序。注意“合计”功能是在 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：

接口	网络协议	本地端口	目的端口	目的地址	上行速率	下行速率	上行字节	下行字节	剩余时间	应用	外网口
172.16.21.60	udp	11020	11001	58.244.48.39	8K	176K	5.5M	111.3M	179	迅雷	wan
192.168.1.1	udp	11020	8835	58.246.189.18	6K	166K	12.6M	289.9M	179	迅雷	wan
172.16.21.60	udp	11020	24608	110.53.98.198	8K	163K	5.8M	117.0M	179	迅雷	wan
172.16.21.60	udp	11020	8727	123.159.178.230	3K	63K	1.7M	32.1M	179	迅雷	wan
172.16.21.60	tcp	50630	11648	112.254.44.205	294	9K	133K	5.2M	3598	迅雷	wan
172.16.21.60	udp	11020	10806	220.200.56.174	437	8K	49K	897K	178	迅雷	wan
172.16.21.60	udp	11020	8000	163.177.79.155	0	142	151K	1.3M	177	迅雷	wan
172.16.21.60	icmp	0	0	112.65.128.201	60	60	2.3M	2.3M	28	ICMP	wan
172.16.21.60	tcp	61294	42707	220.135.0.170	241	51	1K	875	3599	未知流量	wan
172.16.21.60	udp	11020	12042	27.217.80.129	13	19	2K	0	55	迅雷	wan

上下行速率统计：基于连接的速率统计，该功能是在 V3.1.0 以后版本才可出现

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。

应用统计

显示内网各应用程序的流量统计

接口: 所有接口

应用名称	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
网络视频	24K	1.1M	18.6G	301.4G	105.2M	230.4M	4%	26%
常见应用	25K	617K	10.1G	137.7G	73.0M	122.6M	2%	12%
网络游戏	99K	323K	70.1G	194.8G	1.1G	966.0M	17%	17%
即时通信	48K	86K	13.7G	32.9G	94.2M	142.8M	3%	2%
其他应用	20K	37K	105.7G	115.8G	274.5M	251.2M	25%	10%
未知协议	13K	24K	13.4G	9.9G	91.3M	38.9M	3%	0%
P2P下载	710	396	14.4G	92.9G	53.5M	95.1M	3%	8%
文件传输	217	79	5.7G	154.2G	55.2M	108.6M	1%	13%
网络电视	0	0	49.3G	74.7G	83.5M	89.8M	12%	6%
虚拟专用	0	0	512	0	2	0	0%	0%
合计	229K	2.1M	408G	1134G	2G	2G	100%	100%

V3.0版本才支持

V3.0版本才支持，需在【系统设置】【基本设置】【WEB界面参数】里打开‘基于接口的应用统计’后才会显示

点击表头可以排序，默认按下行速率排序

基于接口统计：该功能是用来满足用户统计，基于一个或所有接口下应用的实时流量，该功能的使用前提是在系统管理=》系统设置=》web 界面参数设置，基于接口的应用统计处于勾选状态。

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，如下图所示：

应用统计

显示: 其他应用

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

1 to 10 of 23 rows

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

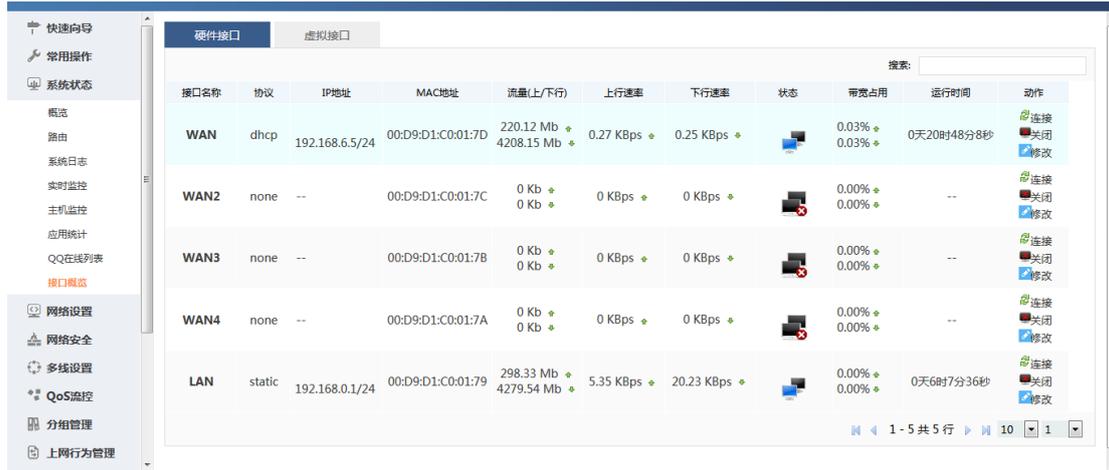


4.8 接口概览

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。



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

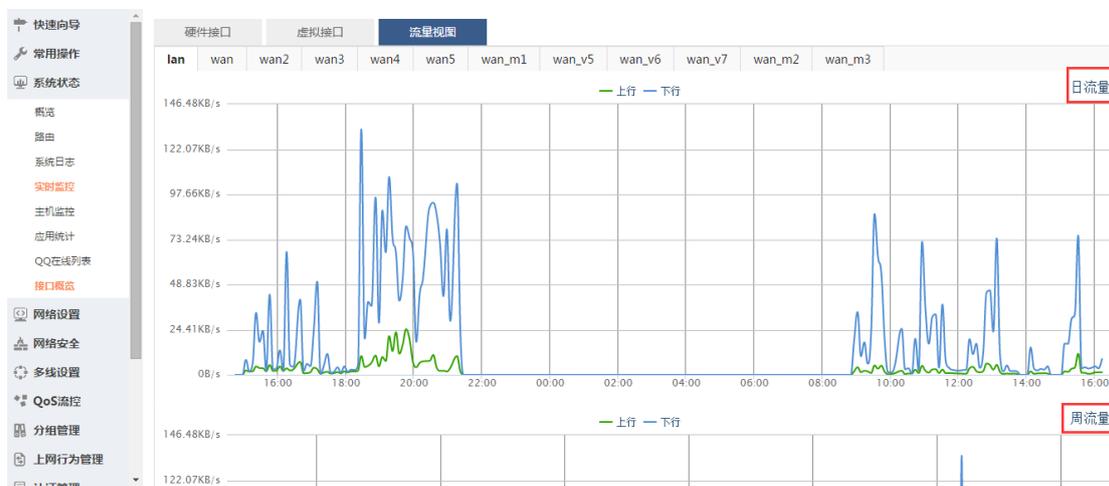
显示设备的虚拟多 wan 接口相关信息



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。

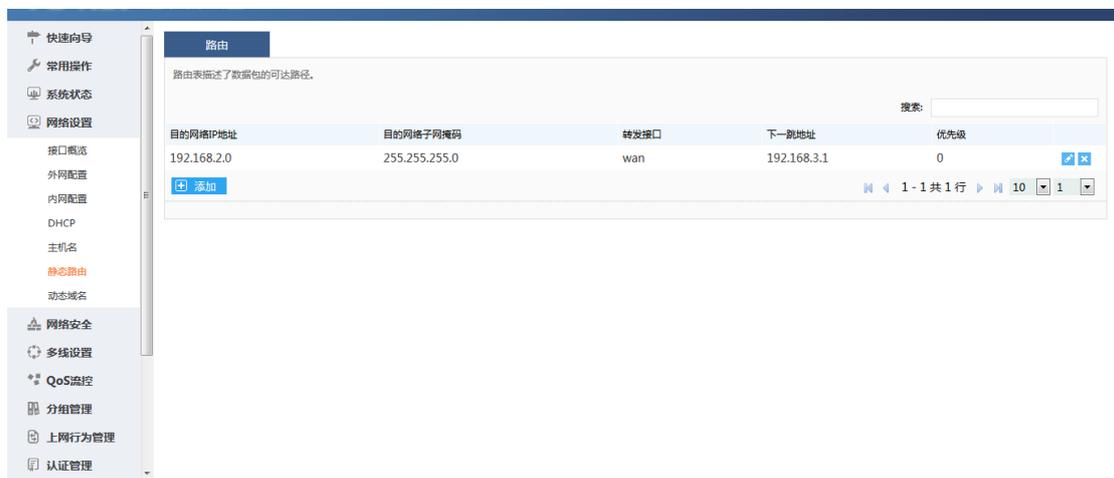


注意：

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，网管员也可以通过对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

字码掩码：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

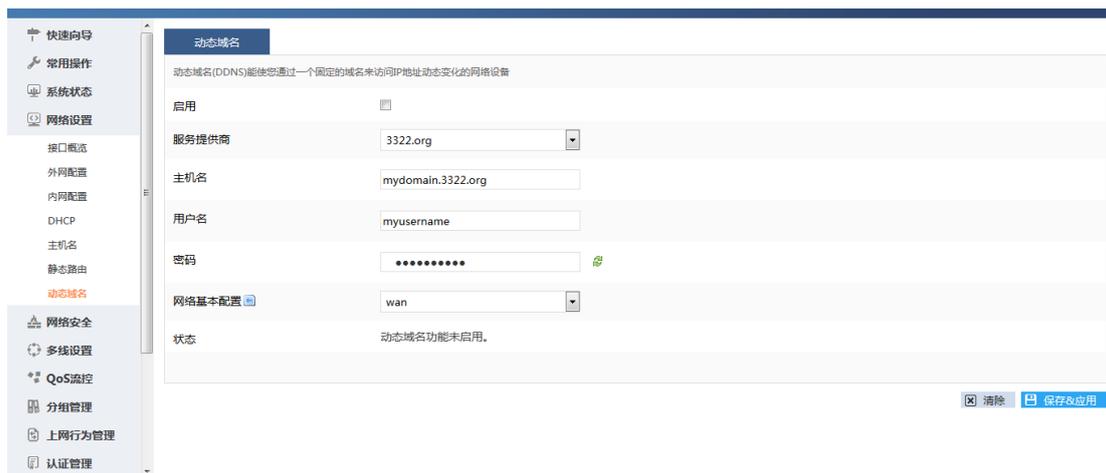
优先级：优先转发等级

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。



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：



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



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

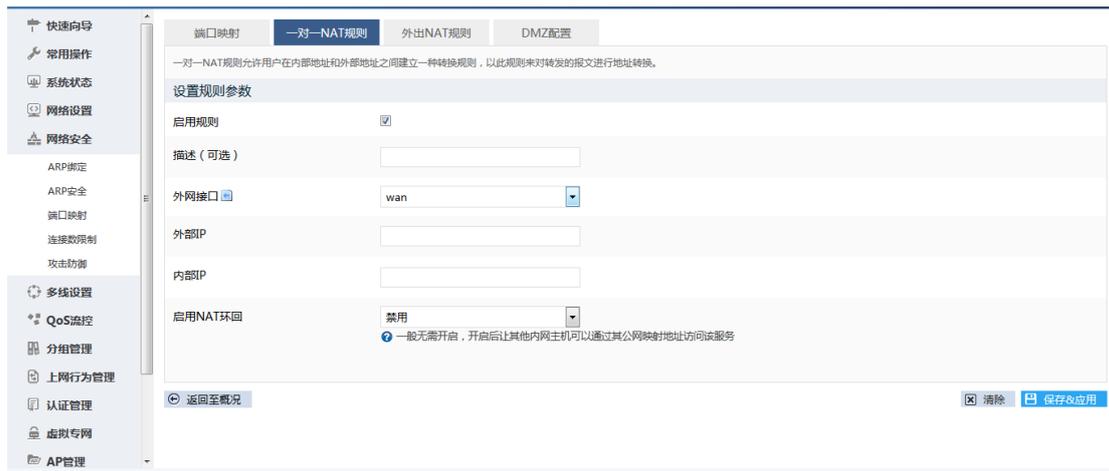
<http://go-cloud.f3322.org:8888> 从内网访问该 WEB 服务器，则在内网电脑上的 IE 地址栏，输入 <http://192.168.1.222/>，192.168.1.222 为 WEB 服务器 ip 地址。

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



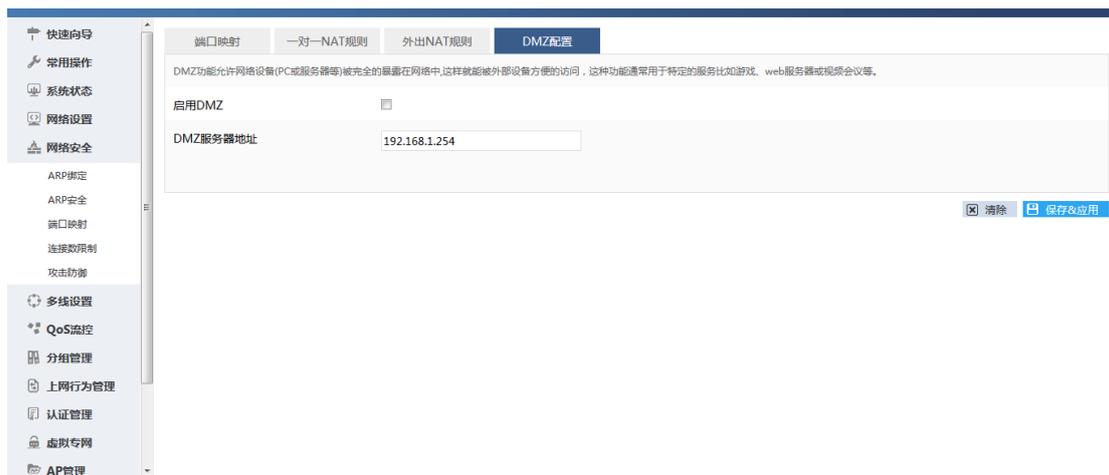
外出 NAT 规则：管理和显示外出 NAT 规则。

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。

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

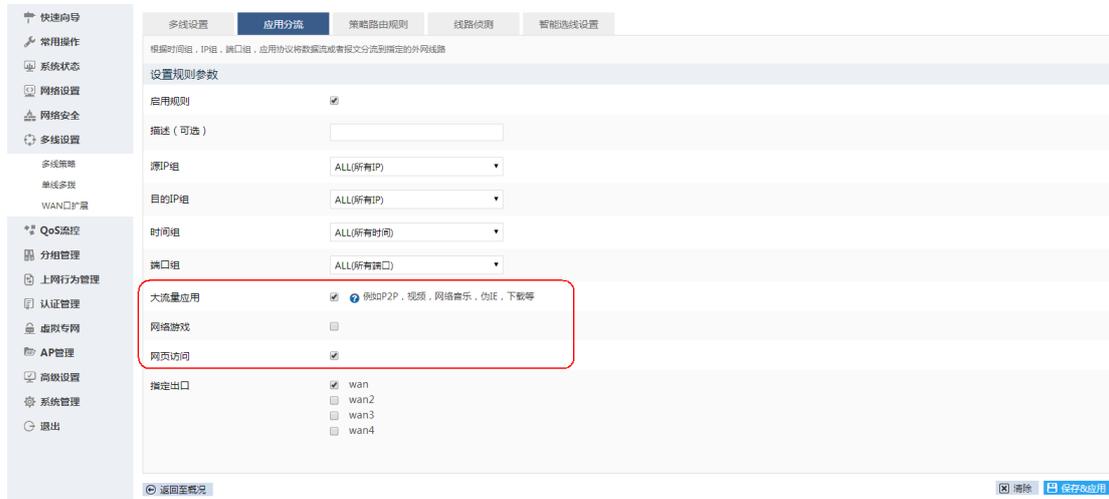
分流界面



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 侦测方式中任意一种。
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。

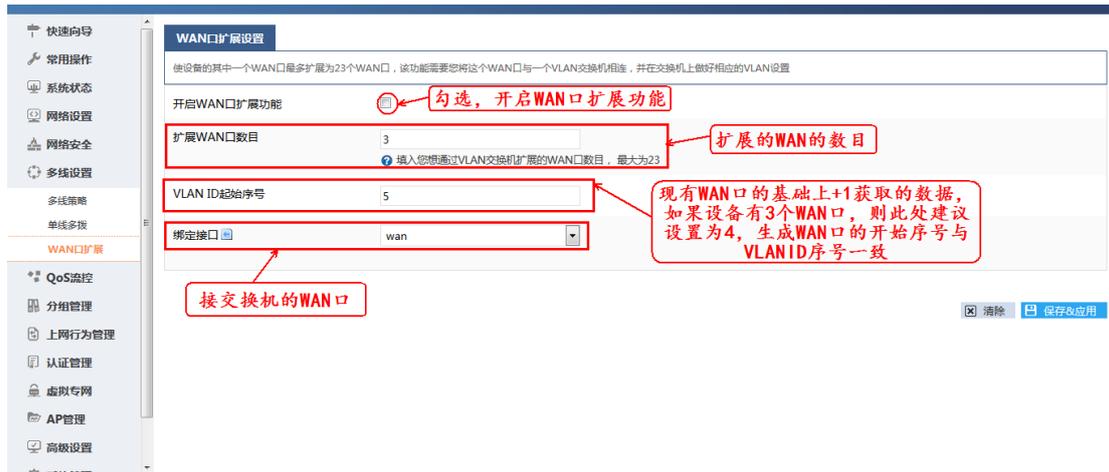
注意：本功能无需外扩 VLAN 交换机，但只有运营商比如电信、联通允许单号多拨的情况下，才能成功单线多拨。



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。
2. 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。
3. 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 口扩张，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。
3. 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

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 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 $(3500 - 2 * 500) = 2500\text{KB/s}$ ）

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

8.1.4 QOS 高级设置

当网络流量需要细化控制时可以打开 QOS 功能高级设置页面进行

该功能在老版本中是隐藏的需要使用 url 才能正常访问,从 3.1.0 开始该功能取消隐藏

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



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

8.15 服务器保障带宽

在网络带宽紧张时，应满足服务器使用正常，设定最低带宽限制，保障客户机正常读取服务器数据。



一般为游戏更新服务器设置一个保障带宽，以防止带宽非常紧张的环境下，游戏更新无速率。保障带宽不会超过接口带宽的三分之一。

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。

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。

The screenshot shows the 'Time Group' (时间组) management page. On the left is a navigation menu with '时间组' (Time Group) highlighted in red. The main content area has a title bar '时间组' and a subtitle '本页显示所有的时间组，系统预定义组不能编辑和删除。' (This page displays all time groups, system predefined groups cannot be edited or deleted). Below the subtitle is a search box labeled '搜索:'. A table lists the time groups:

组名	描述	星期	时间段	
ALL	所有时间	每天		
worktime	-	星期一 星期二 星期三 星期四 星期五	09:00:00-18:00:00	✎ ✕

Below the table is a '+ 添加' (Add) button and pagination controls showing '1 - 2 共 2 行' (1 - 2 of 2 rows) and '10' items per page. At the bottom right are '清除' (Clear) and '保存&应用' (Save & Apply) buttons.

The screenshot shows the '设置规则参数' (Set Rule Parameters) configuration page. The left navigation menu has '时间组' (Time Group) selected. The main content area is titled '设置规则参数' and contains the following fields:

- 组名** (Group Name): Input field with '示例' (Example) and a note '只能是字母和数字!' (Only letters and numbers!).
- 描述 (可选)** (Description (Optional)): Input field with a note '可输入中文!' (Can input Chinese!).
- 星期** (Day of Week): Radio button selection for 星期一 (Monday), 星期二 (Tuesday), 星期三 (Wednesday), 星期四 (Thursday), 星期五 (Friday), 星期六 (Saturday), and 星期日 (Sunday). A note says '日期都不选表示为每天!' (If no date is selected, it represents every day!).
- 时间段** (Time Range): Time selection fields '从 0时 : 0分 到 0时 : 1分' (From 0h:0m to 0h:1m) with a '+' button. A note says '时间填写格式是 hh:mm-hh:mm, 时间留空表示任意时间!' (Time format is hh:mm-hh:mm, empty time represents any time!).

At the bottom left is a '返回至概况' (Return to Overview) button, and at the bottom right are '清除' (Clear) and '保存&应用' (Save & Apply) buttons.

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。

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

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

时间组
地址组
端口组
应用组

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

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

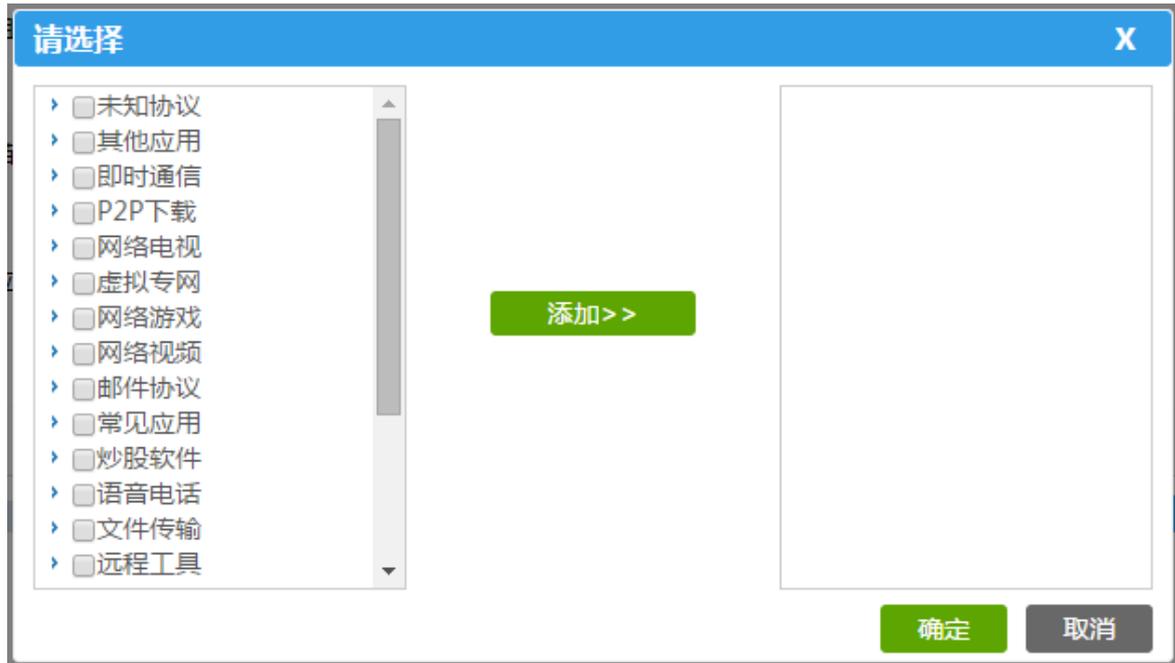
返回至概况 清除 保存&应用

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。



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。

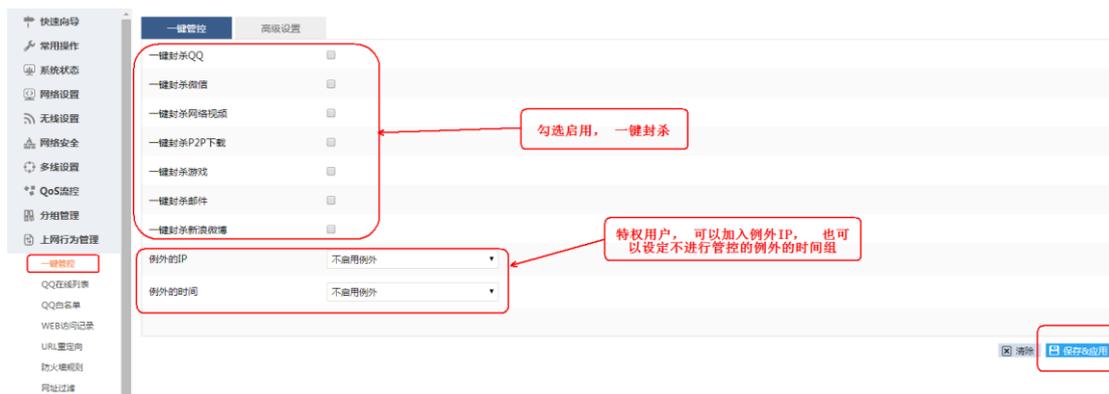
十、上网行为管理

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：

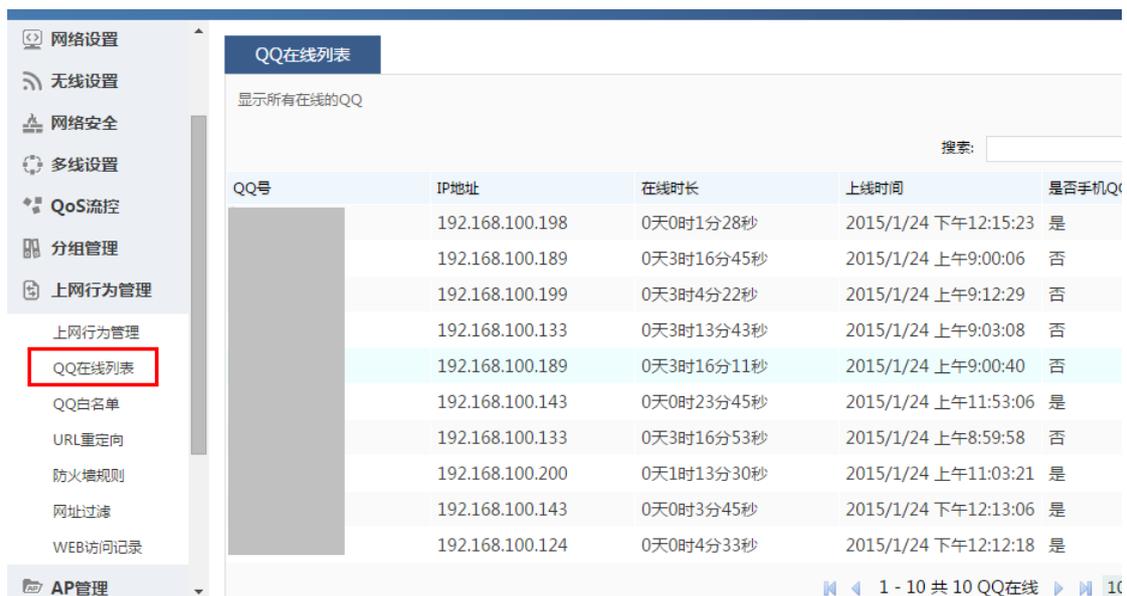


保存应用后，会回到规则列表，如下图所示



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。



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。



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。





10.5 网址过滤

10.5.1 网址过滤



10.5.2 网址分类库

网址过滤 网址分类库 白名单

显示网址分类库

搜索:

网址组名称	类型
休闲娱乐	系统默认
新闻资讯	系统默认
网页游戏	系统默认
在线购物	系统默认
社交网址	系统默认
博客论坛	系统默认
财经证券	系统默认
电子邮件	系统默认
不良网址	系统默认

添加 1-9 共 9 行 10 1

清除 保存&应用

点击此处添加自定义网址组

点击此处保存配置

网址过滤 网址分类库 白名单

本页面你可以修改网址分类库。

网址组名称

URL地址

返回至概况 清除 保存&应用

点击+, 添加URL地址, 创建新的网址组

点击此处保存配置

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

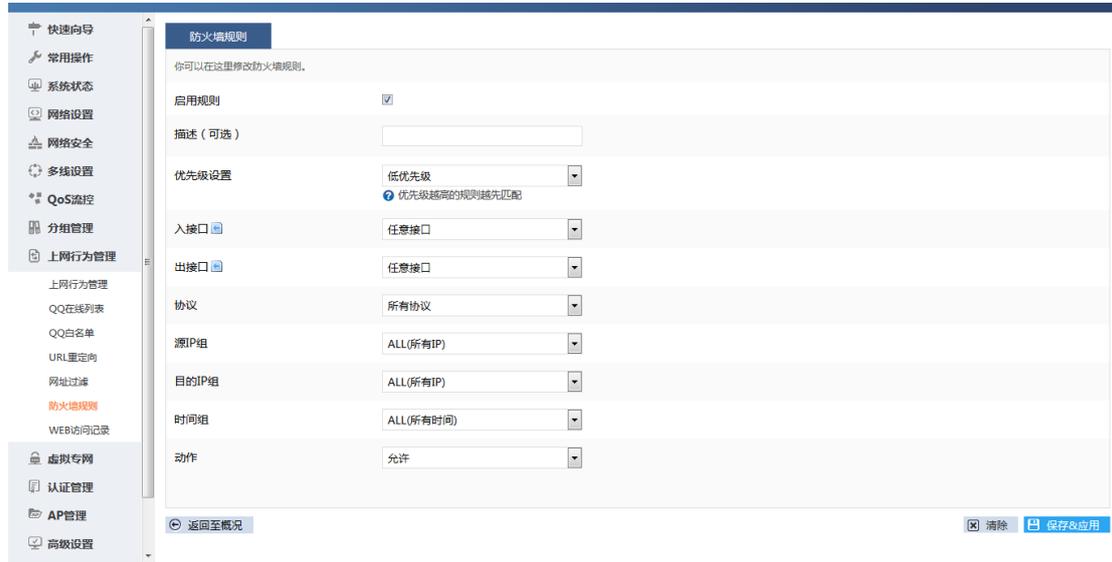
协议：基于那条协议 TCP,UDP,ICMP ,ALL 等

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 客户端和服务器之间建立

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设备上。

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。



借线选项：除了“其他借线模式”外，其他借线模式默认都不开启 NAT，服务端需要配置静态路由，在【高级设置】【接口高级设置】里开启了 nat 模式后，则不再需要在服务器端设置静态回程路由。

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

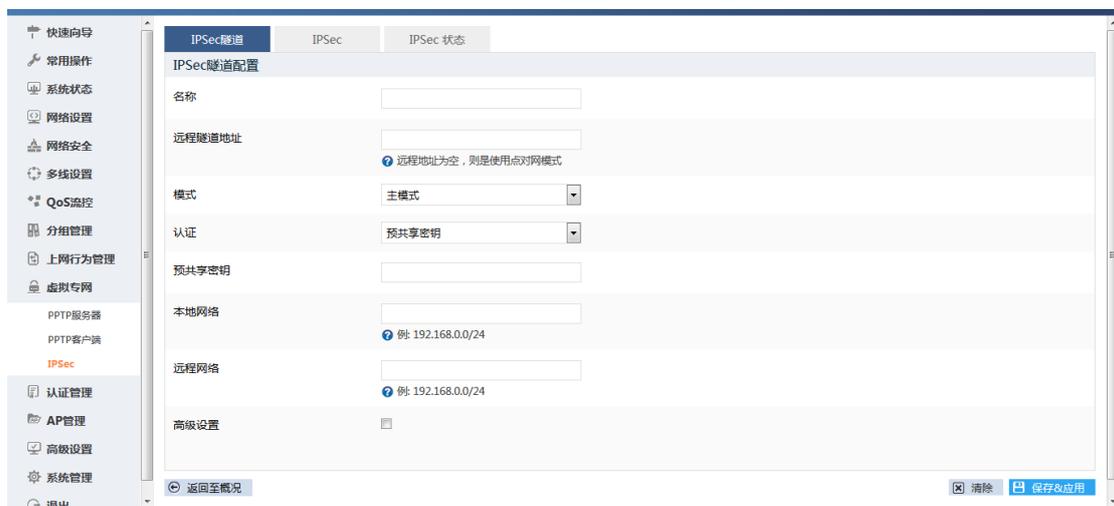
11.3 IPsec

11.3.1 IPsec 隧道

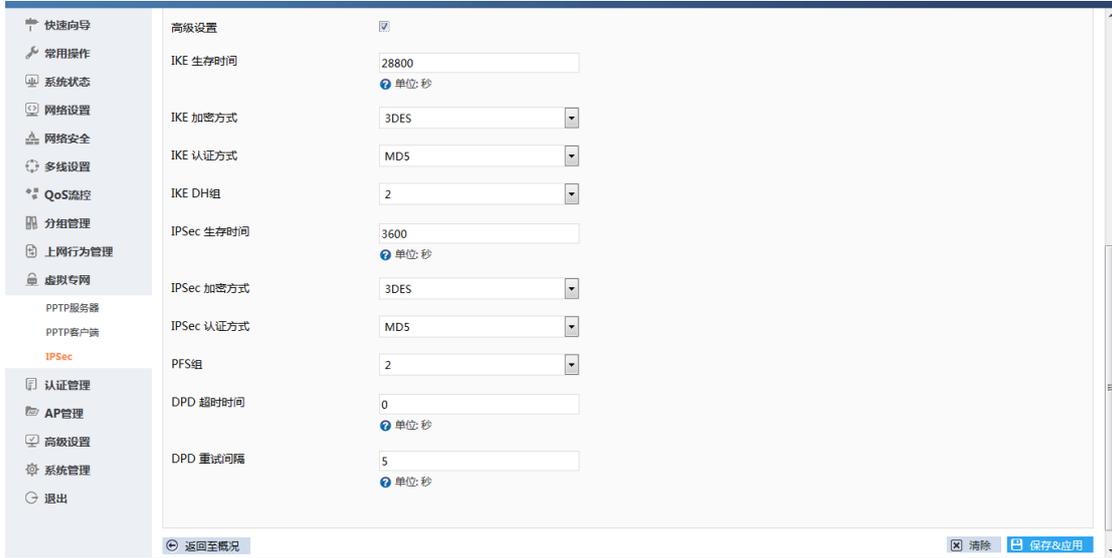
对 IPsec 隧道的参数进行配置，在 IPsec 隧道点添加



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。

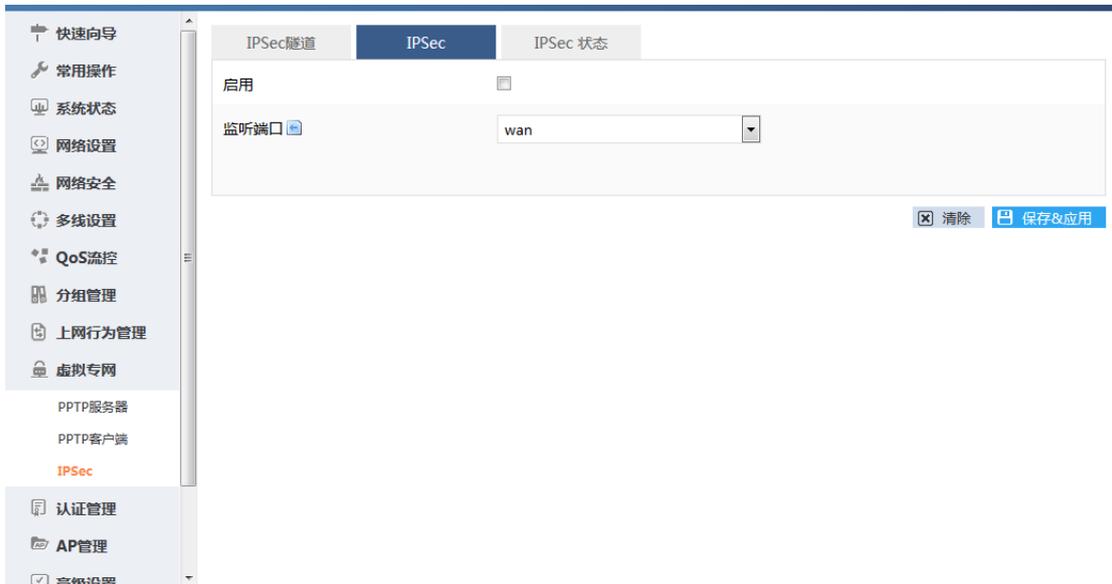


然后勾选高级设置，在里面设定密钥交换过程的加密、认证方式，IPSec 预共享密钥的加密、认证方式。PFS 组与 IKE DH 组可以不一致，并且数字越大 VPN 性能会越低。其他的内容按照默认值就可以了。



11.3.2 IPsec

打勾启用 IPsec



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”



十二 认证管理

12.1 通用公告

12.1.1 通用公告



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 TG-NET 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。



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。

PPPOE 帐号新增加备注功能，在此可以为帐号添加备注以便区分，此处支持中文

“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。

服务器设置
帐号编辑
帐号批量导入
在线用户

用于增加 / 删除用户帐号，设置用户帐号的权限。请注意绑定IP必须在PPPoE服务器中设置的IP地址池之外，比如，IP地址池的起始地址为10.67.7.1，最大拨号用户数为64，那么绑定IP不能在10.67.7.1到10.67.7.64的范围内。

激活

备注 (可选) 可输入中文！

用户名 由字母和数字组成，不能有空格

密码

绑定IP (可选) 请注意绑定IP必须在PPPoE服务器中设置的IP地址池之外。

绑定MAC (可选)

到期时间 (可选) 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

PPPoE帐号新增加备注功能，在此可以为帐号添加备注以便区分，此处支持中文

服务器设置
帐号管理
帐号批量导入
在线用户

显示并设置PPPoE用户的帐号信息

激活	备注	用户名	密码	绑定IP	绑定MAC	到期时间	
<input checked="" type="checkbox"/>	*	test	test	10.67.7.200	00:11:22:33:44:55	2011-08-25 18:00:00	✕ ✕
<input checked="" type="checkbox"/>	测试	111	111	10.1.0.2	*	2018-08-08 18:18:18	✕ ✕

+ 添加
1 - 2 共 2 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



13.2.3 用户信息

显示 AP 当前连接的无线终端信息

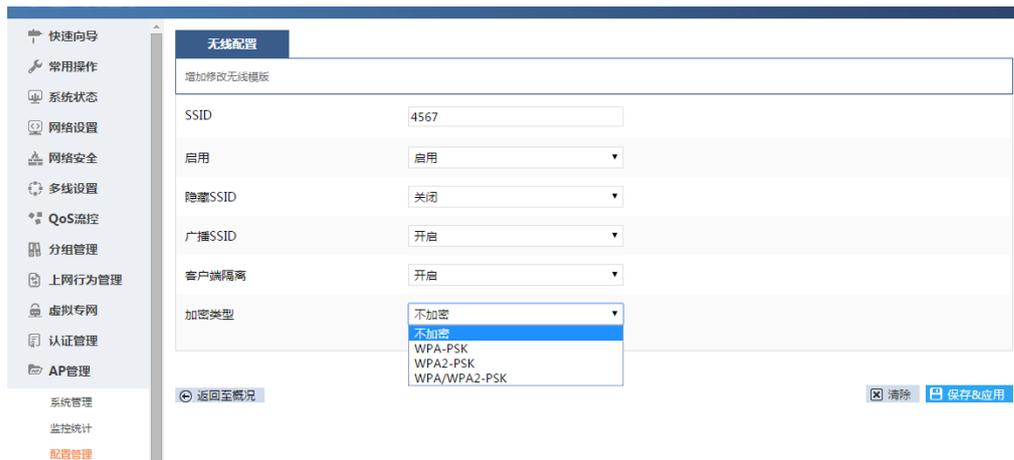


13.3 配置管理

13.3.1 无线模板

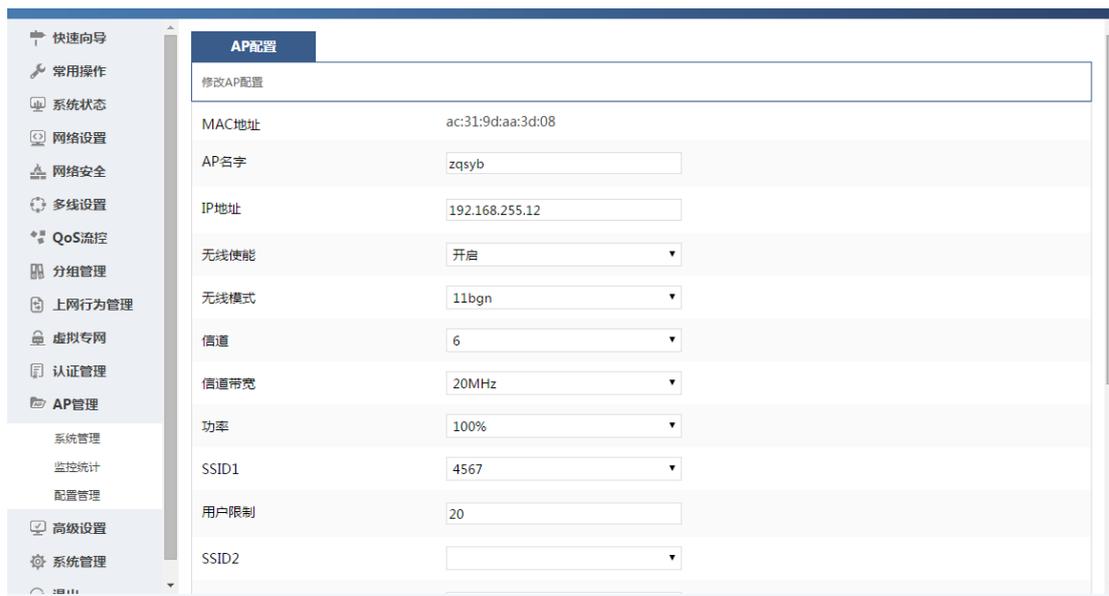
此页面用来创建 SSID 无线模板，路由器通过下发配置可将模板中的 SSID 参数应用于 AP。





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。



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



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。



14.3 高级设置

14.3.1 设备设置

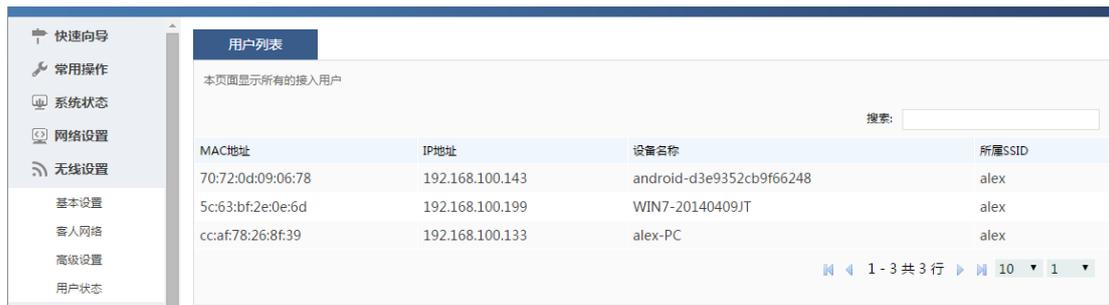
本页面用来设置无线模式、信道、发送功率等相关参数。



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，否则将无法正常上网

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。



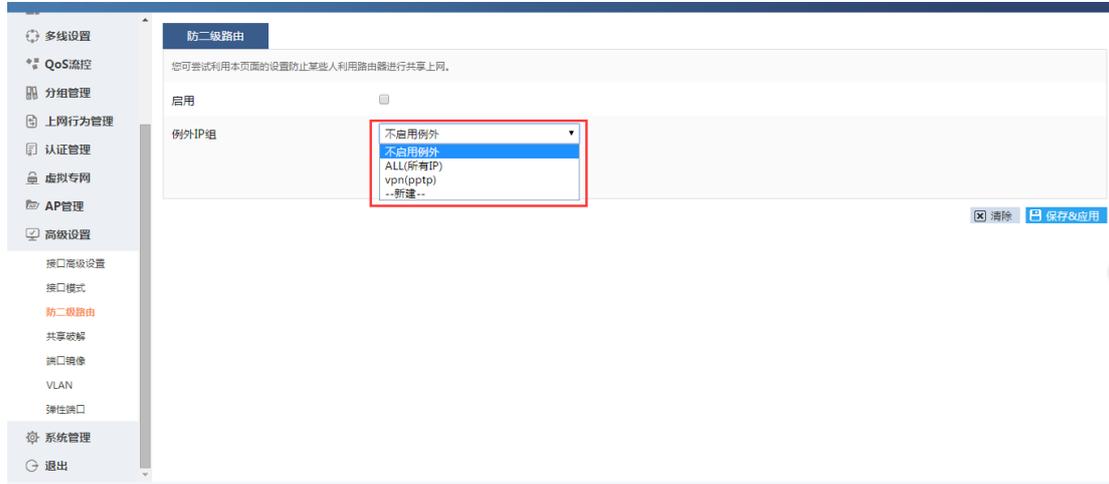
请注意：软路由此处会显示网口的网卡芯片类型，如下图：



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。



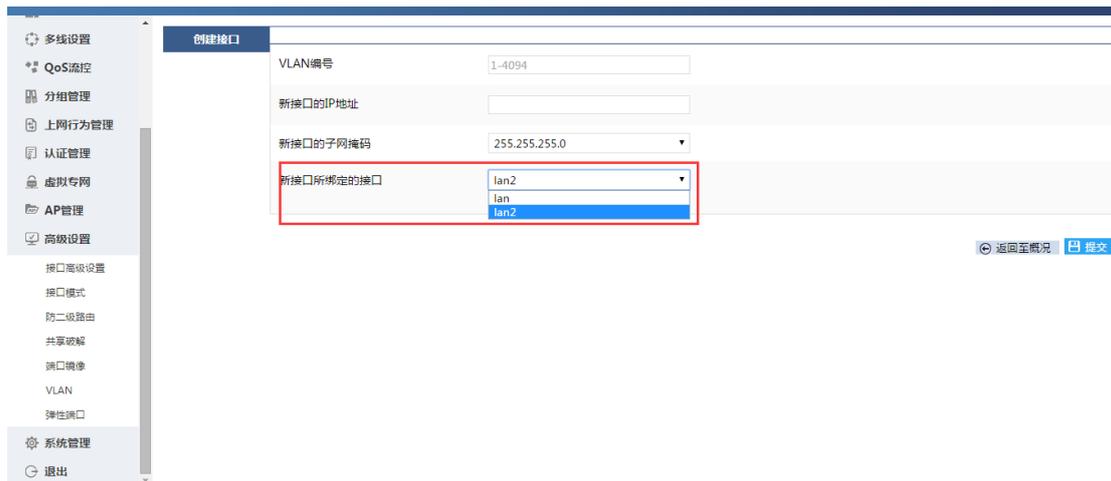
15.5 端口镜像

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



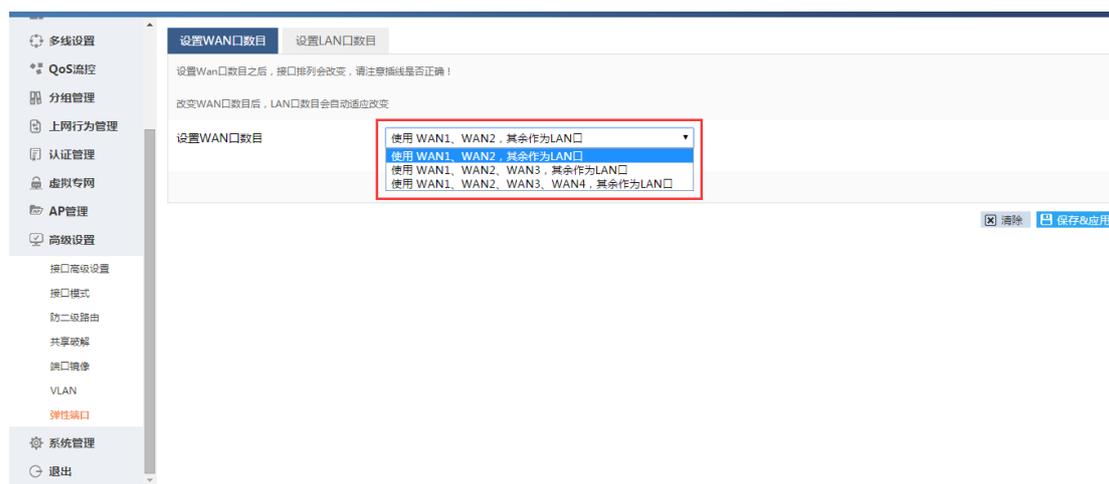
填写该接口 IP 地址、掩码和该接口所绑定的 LAN 口。绑定的物理接口可根据需要设定。



点击编辑按钮可对接口地址进行修改

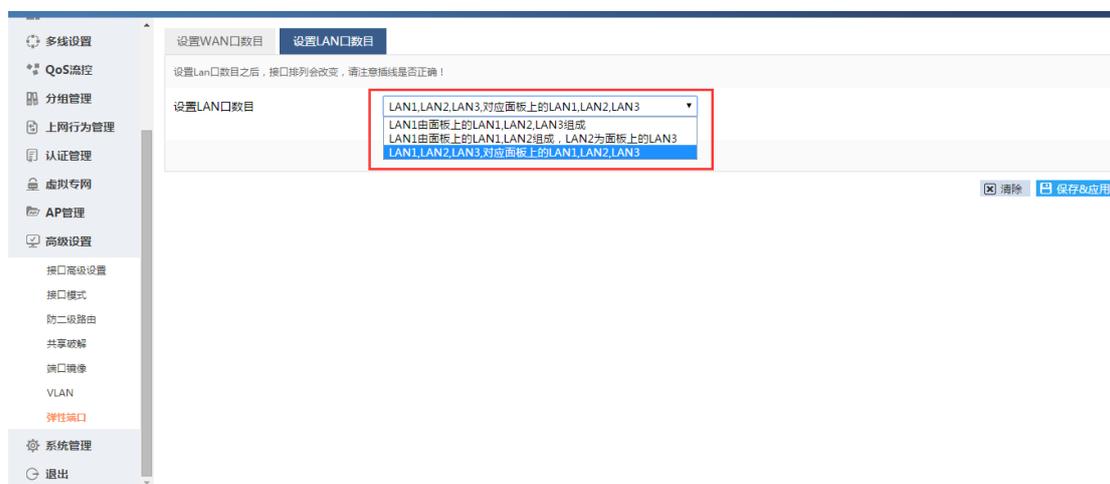
15.7 弹性端口

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

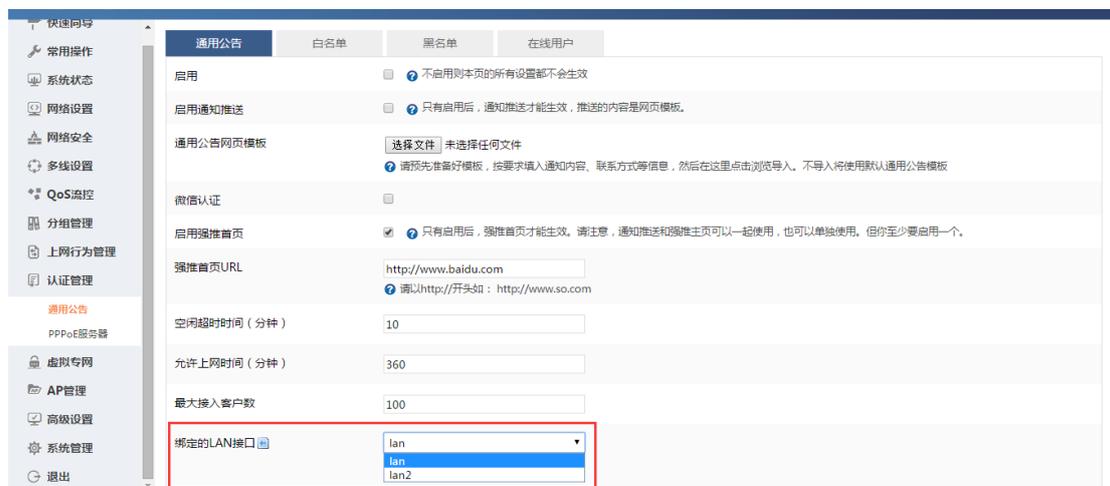
口数下设置“LAN1、LAN2 为对应面板上的 LAN1、LAN2”。也可以不用设置 LAN 口数，但此时路由器 WEB 界面就显示为 LAN 口，即该 LAN 口为 LAN1、LAN2 组成。如下图：



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

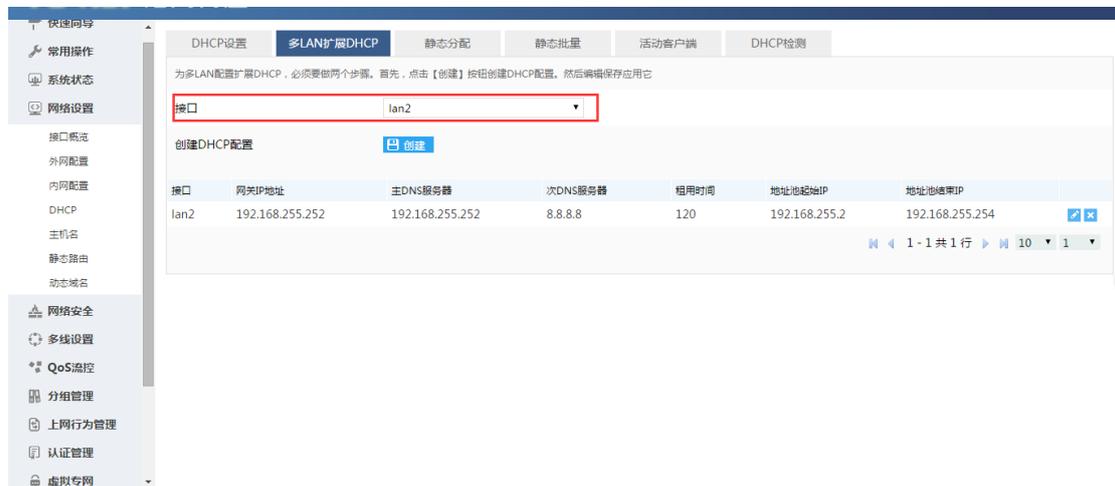


可根据需求选定绑定 LAN 口

PPPOE 拨号



DHCP



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。

外网抓包：选择外网出接口，抓取 5 秒内从该接口通过的流量



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。

Ping诊断
Nslookup诊断
Traceroute诊断
外网抓包

主机名

包的大小
单位：字节

包的个数

接口

Ping

结果输出

```

PING baidu.com (123.125.114.144): 56 data bytes
64 bytes from 123.125.114.144: seq=0 ttl=53 time=28.069 ms
64 bytes from 123.125.114.144: seq=1 ttl=53 time=28.170 ms
64 bytes from 123.125.114.144: seq=2 ttl=53 time=28.080 ms
64 bytes from 123.125.114.144: seq=3 ttl=53 time=28.108 ms
64 bytes from 123.125.114.144: seq=4 ttl=53 time=28.058 ms

--- baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 28.058/28.097/28.170 ms
                    
```

Nslookup：域名解析查询，一般多用邮件排障。

Ping诊断
Nslookup诊断
Traceroute诊断
外网抓包

主机名

nslookup

结果输出

```

Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: baidu.com
Address 1: 220.181.57.217
Address 2: 111.13.101.208
Address 3: 180.149.132.47
Address 4: 123.125.114.144
                    
```

Traceroute：查找路径，定位故障点。

Ping诊断
Nslookup诊断
Traceroute诊断
外网抓包

主机名

Traceroute

结果输出

```

traceroute to baidu.com (123.125.114.144), 30 hops max, 38 byte packets
 1  172.16.21.1  0.382 ms
 2  192.168.118.1  0.641 ms
 3  112.65.128.201  3.154 ms
 4  112.64.252.85  3.732 ms
 5  *
 6  139.226.201.65  7.114 ms
 7  219.158.12.149  25.432 ms
 8  123.126.0.62  29.648 ms
 9  202.106.34.84  28.287 ms
10  61.49.168.62  28.918 ms
11  *
                    
```

外网抓包：选择外网出接口，抓取 5 秒内从该接口通过的流量

结果输出					
SRC=172.16.21.106	DST=172.16.21.108	LEN=40	PROTO=TCP	SPT=62252	DPT=80
SRC=172.16.21.106	DST=172.16.21.108	LEN=40	PROTO=TCP	SPT=62252	DPT=80
SRC=172.16.21.106	DST=172.16.21.108	LEN=40	PROTO=TCP	SPT=62252	DPT=80
SRC=172.16.21.106	DST=172.16.21.108	LEN=40	PROTO=TCP	SPT=62252	DPT=80
SRC=192.168.199.22	DST=255.255.255.255	LEN=36	PROTO=UDP	SPT=52928	DPT=22313
SRC=172.16.21.106	DST=172.16.21.108	LEN=40	PROTO=TCP	SPT=62252	DPT=80

外网抓包,指定一个外网出接口,单击开始抓包,系统默认抓取 5 秒内从该接口通过的流量,如上图

结果输出
5秒内该端口无下行数据

外网抓包,若是五秒中内该接口无流量通过将提示“5 秒内该端口无下行数据”

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	<input type="text" value="172.16.21.106"/>
接口	<input type="text" value="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。

The screenshot shows the TG-NET software interface. The top navigation bar includes '游戏管理', '分组管理', '客户机管理', '监控中心', and '其他功能'. The main content area displays 'RouterOS (详情)' with a status '智能流控已开启 (关闭)'. A large green checkmark and text '智能流控已开启' are prominent. Below this, a table shows a log entry: '2014-05-29 11:12:13 BarView [40791][本地登陆:63766] 登陆成功'. A red box highlights the '智能流控' option in the left sidebar, with a red arrow pointing to it and the text '打开网维大师 选择 智能流控'. Another red box highlights the '连接设置' link in the top right corner.

The second screenshot shows the '智能流控' configuration window. It has a title bar '智能流控' and a navigation bar similar to the first. The main content area shows '未连接路由器' and a red box with the text '暂时填写ros 5.x, 后续会有我们自己的TG-NET'. Below this, there are three steps for configuration:

- 1 请选择您的路由器: RouterOS, 5.x, 没有我的路由器型号
- 2 请输入路由器IP地址: IP地址: 192 . 168 . 0 . 1 (highlighted with a red oval and labeled '路由器地址')
- 3 请输入单条WAN口中最大的上行带宽: 上行带宽: 联通, 2 Mbps (*请务必与路由器保持一致)

 A '确定' button is at the bottom. A table at the bottom shows log entries: '2014-05-29 11:12:13 BarView [40791][本地登陆:63766] 登陆成功' and '2014-05-29 11:13:29 客户机[TGNET13] 下线'.

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 设备认证

设备认证		认证导入
设备认证		已认证
产品序列号	M5HK52EPFEGH3XRC79QX9XC7H	
许可证用户名	玄武网络	
最大主机数目	9999	
许可证有效期至	2020-01-01 00:00:00 UTCTime	
本次认证时间	2015-09-30 15:27:32	

系统管理=》设备认证，序列号认证成功在此处可以看到该序列号的具体信息

设备认证	认证导入
本页面用于认证信息的导入。	
接口逆向排列:	<input type="checkbox"/> 如果勾选，则LAN在最右侧，WAN在最左侧
认证文件:	<input type="button" value="选择文件"/> 未选择任何文件 <input type="button" value="导入"/>

接口逆向排序：导入注册码勾选接口逆向排列，则 wan 从最左边开始 lan 在最右；不勾选为默认。导入完成恢复出厂，立即生效。

16.13 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、AC 管理

AC 管理模块主要用于管理内网中的 AP 以及交换机，对 AP 与交换机进行集中管理，统一配置下发，并且实现认证、广告推送业务、AP 监控统计、终端监控统计等。

登录路由器后，点击“AC 管理”，即可进入 AC 管理模块功能配置页面。



AC 管理主要包括快速向导、监控统计、功能管理、AP 基本配置、AP 高级配置、认证营销、高级策略、交换机管理、系统管理、审计配置等 10 个功能模块，下面将逐个介绍。



注意：AC 管理配置修改后，页面上方会有“配置已更改，请点击 保存”提示，请您根据提示，注意及时保存配置。有多个配置操作时，可以在最后一次配置操作后，保存配置。

配置已变更，请点击 **保存**

17.1 快速向导

快速向导功能，按照提示轻松完成 AC 配置。您也可以直接到菜单项中选择您需要修改的设置项进行设置。

(1) 点击“下一步”，使用快速向导配置；

快速配置向导

使用配置向导，按照提示轻松的完成AC配置。您也可以直接到菜单项中选择您需要修改的设置项进行设置。要继续配置，请单击“下一步”按钮。

下一步

(2) 配置 AP 管理密钥，该配置与 AP 的管理密钥相一致，才能管理 AP；

快速向导-功能管理

AP管理密钥: admin

温馨提示：请确保AP上的管理密钥和此处设置一致。

上一步 下一步

(4) 修改无线管理的默认模板；

默认 SSID 个数为 2 个，可手动添加；

快速向导-AP模板

选择	序号	SSID名	广播SSID	客户端隔离	安全模式	加密方式	密钥	用户数
*	1	Wanbroad_2G	开启	开启	不加密	不加密		30
*	2	Wanbroad_5G	开启	开启	不加密	不加密		30

添加 删除

温馨提示：双频AP使用模板配置时，SSID 1/3/5/...是2.4G频段，SSID 2/4/6/...是5G频段！

上一步 应用

17.2 监控统计

监控统计菜单项，包括 AP 列表、AP 信息、用户列表三个子菜单。下面将分别介绍。

AP列表										
编号	名称	SN码	MAC地址	型号	最大速率	硬件版本	软件版本	在线状态	管理密钥	配置同步
1	BK-AP-X1	D00tion007654321	EC:D9:C2:05:00:61	BK-AP300-X1	300M	V1.0.0	V1.0.0-R1	在线	匹配	已同步
2	BK-AP	D207031101660072	EC:D9:D1:C4:D1:90	BK-AP300-M1	300M	V1.0.0	V1.0.0-R1	在线	匹配	已同步

17.2.1 AP 列表

AP 列表页面，可查看局域网内 AP 的基本信息。

首次加入 AC 管理的 AP，路由 AC 将自动为其推送默认模板“Defaults”的配置信息。已加入过 AC 管理的 AP，如信息未同步，可通过单击“同步”按钮，将 AC 管理的配置同步到 AP，或单击“一键同步”按钮进行批量配置同步。

注意：AP 接入与路由器同一个局域网网络，密钥匹配，即接受路由器的管理，AP 信息页面就会存在已接入 AP 的信息。

AP列表										
编号	名称	SN码	MAC地址	型号	最大速率	硬件版本	软件版本	在线状态	管理密钥	配置同步
1	BK-AP-X1	D00tion007654321	EC:D9:C2:05:00:61	BK-AP300-X1	300M	V1.0.0	V1.0.0-R1	在线	匹配	已同步
2	BK-AP	D207031101660072	EC:D9:D1:C4:D1:90	BK-AP300-M1	300M	V1.0.0	V1.0.0-R1	在线	匹配	已同步

AP 列表页面，显示局域网内所有 AP 设备信息（无论管理密钥匹配与否，都能显示），包括 AP 对应的名称、SN 码、MAC 地址、型号、最大速率、硬件版本、软件版本、在线状态、管理密钥是否匹配、配置同步等信息。右上角还有可按 MAC 地址过滤 AP 的搜索功能。

AP 列表中灰色底纹条目，表示该 AP 当前为离线状态。

AP 列表页面显示的主要信息说明：

名称：显示 AP 名，可以在【AP 基本设置-AP 配置】页面更改（注意请使用英文字符或数字）；

SN 码、MAC 地址、型号、最大速率、硬件版本、软件版本：分别显示 AP 当前基本信息；

在线状态：显示对应的 AP 是否在线，如果 AP 重启或断电则显示断开；

管理密钥：显示 AP 与 AC 的管理密钥是否匹配，只有密钥匹配的 AP 才能接受 AC 管理，否则，只能被发现而无法管理完成配置更改下发；

配置同步：显示 AP 的配置是否与 AC 上的配置相同，若相同则显示已同步，不同则显示“同步”，单击“同步”按钮，配置将下发到 AP，同步 AC 的配置；

MAC 地址搜索：输入需要定位的 MAC 地址，可在输入框内输入需要搜索的 AP 的 MAC 地址进行准确搜索。

17.2.2 AP 信息

AP 信息页面，显示局域网内的所有 AP 的状态信息。



编号	名称	IP地址	MAC地址	网络模式 (2.4G/5G)	信道 (2.4G/5G)	功率 (2.4G/5G)	用户数	上线时长	上/下行流量(KB)	SSID1	SSID2	SSID3	SSID4	无线邻居
1	BK-AP-...	192.168.0.123	EC:D9:C2:05:00:61	11bgn/无	11/无	25%/无	0	00:38:15	0/0	test1	test2			扫描
2	BK-AP	192.168.0.31	EC:D9:D1:C4:D1:90	11bgn/无	1/无	25%/无	0	01:36:44	11/0	test1	test2			扫描

AP 信息表主要包括 AP 对应的名称、IP 地址、MAC 地址、网络模式、信道、功率、用户数、上线时长、上/下行流量、SSID1、SSID2、SSID3、SSID4、无线邻居信息。页面右上角会显示当前 AP 总数、在线 AP 数、离线 AP 数。（无线网络模式、信道带宽、功率这三项，针对双频 AP 区分 2.4G 频段和 5G 频段，左侧显示的为 2.4G 频段的配置信息，右侧显示的为 5G 频段的配置信息）

AP 信息页面主要字段信息显示说明：

名称：显示 AP 名，可以在【AP 基本配置-AP 配置】页面更改（注意请使用英文字符或数字）；

IP 地址：显示 AP 的 IP 地址，可以在【AP 基本配置-AP 配置】中更改；

MAC 地址：显示 AP 的 MAC 地址；

网络模式 显示 AP 所使用的无线网络模式，2.4G 频段有 11bgn、11g、11bg、11b 四种模式；5G 频段有 11a、11n、11an、11ac/a/n 四种模式。

信道：显示 AP 发射无线信号信道，2.4G 频段分为 1~13 共 13 个信道，5G 频段分为 149~165 共 5 个信道，并都支持 auto 信道选择；

功率：显示 AP 的发射功率，百分比形式显示，可配 25%、50%、75%、100%及 auto。可以在【AP 基本配置-AP 配置】中更改；

用户数：显示已接入 AP 的无线终端数；

上线时长：显示 AP 接受 AC 管理的运行时长；

上/下行流量：显示关联 AP 的无线终端发往外部网络/接收外部网络的总流量数据；

SSID1、2、3、4：各个 SSID 的名称显示；

无线邻居：单击“扫描”按钮，可以扫描该 AP 周围的 SSID 信号，数据会 5 秒钟自动刷新。如下图所示。

编号: 4 AP无线邻居信息

SSID	MAC	信道	信号强度
123haha	AC:31:9D:11:11:10	6	-44dBm
3601_2G	EC:D9:D1:C2:A7:4F	6	-69dBm
TG-NET	00:11:22:33:44:11	6	-74dBm
TG-NET-ceshibu	EC:D9:D1:C2:A8:12	6	-40dBm
tgtest	EC:D9:D1:C2:A7:AF	6	-35dBm
xuwj_3333	EE:D9:D1:C1:B3:D9	8	-65dBm
111111	58:69:6C:2C:E5:28	6	-46dBm
aa	AC:31:9D:AA:74:70	13	-35dBm
Tenda_10D6A0	C8:3A:35:10:D6:A1	10	-69dBm
xuwj_1111	EC:D9:D1:C0:B3:D9	8	-64dBm
xuwj_jiz	EE:D9:D1:C0:B3:D9	8	-64dBm
M1-R4ceshi	78:A3:51:02:2F:64	8	-60dBm
yxcs11	EC:D9:D1:C0:B3:E9	10	-56dBm
Tenda 888888	00:90:4C:88:88:89	10	-62dBm

17.2.3 用户列表

用户列表页面，如下图所示，显示所有无线终端用户的状态信息。

选择	编号	用户名	IP地址	终端MAC地址	接入SSID	接入AP MAC	上行/下行流量(KB)	在线时间	认证类型	黑白名单
<input type="checkbox"/>	统计	总用户数:1	认证用户数:0	未认证用户数:1	黑名单数:0	白名单数:0			选择	
<input type="checkbox"/>	1		192.168.1.128	DC:2B:2A:B0:88:52	test1	EC:D9:C2:05:00:61	4/1	00:00:12	未认证	

Page 1 of 1

用户列表页面主要字段信息显示说明：

选择：可以选中对应的终端用户，可对选中的用户进行终端下线操作；

用户名：显示已认证终端的认证方式账号，如短信认证显示为手机号，Radius认证、身份证认证显示身份证号码、外置WEB认证显示认证账号，微信认证、一键认证、密钥认证、未认证时终端用户名显示为空；

IP地址：显示终端设备的IP地址信息；

MAC地址：显示终端设备的MAC地址信息；

接入SSID：显示终端所连接的SSID名称；

接入AP：显示终端所连接的AP的MAC信息；

上行/下行流量：显示终端设备的上、下行流量数据。

在线时间：显示终端设备的在线时间；

认证类型：显示终端设备的认证方式，显示值为未认证或对应的认证方式；

黑白名单：一键配置终端用户的黑白名单属性，用户默认未配置黑白名单属性。这里会关联【高级策略—黑白名单】功能，请参考 1.6.1 黑白名单功能介绍。

17.3 功能管理



功能管理主要进行 AP 管理密钥的设置、无线漫游功能的开启、AP 本地认证功能的开启、AP 广播控制的开启。

AP 管理密钥：AC 和 AP 之间通信的认证机制，一个 AP 只能由与它管理密钥匹配的 AC 管理，密钥不匹配的 AP 将不受 AC 管理。默认管理密钥均为 admin。

无线漫游：实现 AP 的主动漫游，漫游检测周期默认开启。

AP 广播控制，即 AP 广播抑制功能，可通过设定，对经过 AP 的广播包进行抑制，避免广播包过多，影响无线终端使用。默认开启抑制功能，且默认广播包数抑制 10 pps。

17.4 AP 基本配置

该选项用于对 AP 进行维护及管理配置下发。

快速向导	AP模板
快速向导	请输入模板名称 <input type="text"/> Go!
监控统计	
功能管理	
AP基本设置	
AP模板	
AP配置	
AP升级	
AP系统维护	
AP定时重启	
AP高级设置	
认证营销	
高级策略	
交换机管理	
系统管理	
审计配置	

序号	选择	默认	模板名称	2.4G使能	5G使能	2.4G网络模式	5G网络模式	2.4G带宽	5G带宽	SSID/加密方式	操作
1	<input type="checkbox"/>	<input checked="" type="radio"/>	Defaults	开启	开启	11bgn	11an	20M/40M	20M/40M	Wanbroad_2G/未加密 <small>详情>></small>	详细信息
2	<input type="checkbox"/>	<input type="radio"/>	test	开启	开启	11bgn	11an	20M/40M	40M+	test1/未加密 <small>详情>></small>	详细信息
3	<input type="checkbox"/>	<input type="radio"/>	a	开启	开启	11bgn	11an	20M/40M	40M+	sad/未加密 <small>详情>></small>	详细信息
4	<input type="checkbox"/>	<input type="radio"/>	213	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息
5	<input type="checkbox"/>	<input type="radio"/>	1231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息
6	<input type="checkbox"/>	<input type="radio"/>	2131	开启	开启	11bg	11ac/a/n	20M	80M	123/未加密 <small>详情>></small>	详细信息
7	<input type="checkbox"/>	<input type="radio"/>	231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息

100 ▾ | Page 1 of 1 | [go](#) | [▶](#) | [○](#)

[添加](#) [删除](#) [刷新](#)

17.4.1 AP 模板

此页面用于建立、删除、修改 AP 模板，最多支持 512 个无线模板。

注意：AP 与 AC 密钥匹配时，接入 AP 后，AC 会自动给 AP 下发默认模板的配置，默认模板 Defaults 不可以删除，只支持修改无线配置信息。

快速向导	AP模板
快速向导	请输入模板名称 <input type="text"/> Go!
监控统计	
功能管理	
AP基本设置	
AP模板	
AP配置	
AP升级	
AP系统维护	
AP定时重启	
AP高级设置	
认证营销	
高级策略	

序号	选择	默认	模板名称	2.4G使能	5G使能	2.4G网络模式	5G网络模式	2.4G带宽	5G带宽	SSID/加密方式	操作
1	<input type="checkbox"/>	<input checked="" type="radio"/>	Defaults	开启	开启	11bgn	11an	20M/40M	20M/40M	Wanbroad_2G/未加密 <small>详情>></small>	详细信息
2	<input type="checkbox"/>	<input type="radio"/>	test	开启	开启	11bgn	11an	20M/40M	40M+	test1/未加密 <small>详情>></small>	详细信息
3	<input type="checkbox"/>	<input type="radio"/>	a	开启	开启	11bgn	11an	20M/40M	40M+	sad/未加密 <small>详情>></small>	详细信息
4	<input type="checkbox"/>	<input type="radio"/>	213	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息
5	<input type="checkbox"/>	<input type="radio"/>	1231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息
6	<input type="checkbox"/>	<input type="radio"/>	2131	开启	开启	11bg	11ac/a/n	20M	80M	123/未加密 <small>详情>></small>	详细信息
7	<input type="checkbox"/>	<input type="radio"/>	231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <small>详情>></small>	详细信息

100 ▾ | Page 1 of 1 | [go](#) | [▶](#) | [○](#)

[添加](#) [删除](#) [刷新](#)

AP 模板列表下方的功能按钮说明：

添加 按钮：添加一个模板。

删除 按钮：勾选一个模板，删除一个模板。

刷新 按钮：刷新模板配置信息。

点击“操作”栏中的“详细信息”按钮，可查看并修改模板详细信息。点击“添加”按钮，可以新增一个 AP 模板。

AP模板											
模板名称		2.4G网络模式	2.4G信道带宽	5G网络模式	5G信道带宽	登录名	登录密码				
Defaults		11bgn	20M/40M	11an	20M/40M	admin	admin				
选择	序号	SSID名	广播SSID	客户端隔离	安全模式	加密方式	密钥	VLAN ID	用户数	上行带宽(KB/s)	下行带宽(KB/s)
*	1	Wanbroad_	开启	开启	不加密	不加密		0	30	0	0
*	2	Wanbroad_	开启	开启	不加密	不加密		0	30	0	0

温馨提示：双频AP使用模板配置时，SSID 1/3/5/...是2.4G频段，SSID 2/4/6/...是5G频段！

模板名称：设置 AP 模式的名称，可设置为数字、字母；

网络模式 配置无线的网络模式，2.4G 网络模式有 11b、11g、11b/g、11b/g/n 可选；5G 网络模式有 11a、11n、11an、11ac/a/n 可选；

信道带宽 配置 AP 的信道带宽，2.4G/5G 信道带宽有 20M、20/40M、40M+、40M-可选；5G 的 11ac/a/n 网络模式下，信道带宽还支持 80+；

登录名/登录密码：AP 界面的登录用户名、密码；

SSID 名：配置 SSID，输入 SSID 名称（支持 8 个中文）；

广播 SSID：设置开启，终端才能扫描到该 SSID，默认开启；

设置关闭，终端将不能搜索到该 SSID；

客户端隔离：默认关闭，开启后同一个 AP 下客户端之间将无法进行通讯；

安全模式：对无线进行加密。加密方式可选用 WPA-PSK、WPA2-PSK、WPA/WPA2-PSK 三种模式；

加密方式：选择加密算法方式，分别可选 AES、TKIP、AES/TKIP 算法。如需加密，设置安全模式、加密方式、密钥（8~31 位）即可；

VLAN ID：设置 SSID 的 VLAN ID，即接入用户将会带上该 tag 标签，0 为不配置；

用户数：设置每个 SSID 连接终端的最大用户数目；

上/下行带宽：对该 SSID 的每一个用户的上/下行带宽限制，默认不限制。

添加 按钮：添加一个 SSID，默认使用 2 个 SSID；

删除 按钮：勾选一个 SSID，删除一个 SSID，SSID1/2 不可删除；

刷新 按钮：刷新模板配置信息；

应用：应用并保存该模板；

返回：取消对模板的修改，返回 AP 模板页面。

【示例】添加一个 AP 默认模板步骤

1. AP 模板页面，点“添加”按钮，进入 AP 模板配置页面，如下图 3-1-20 所示。可以清楚看到模板默认配置项及空缺配置项。每一项的配置都需要结合实际应用场景按需选配。

AP模板											
模板名称		2.4G网络模式	2.4G信道带宽	5G网络模式	5G信道带宽	登录名	登录密码				
<input type="text"/>		11bgn	20M/40M	11an	40M+	<input type="text"/>	<input type="text"/>				
选择	序号	SSID名	广播SSID	客户端隔离	安全模式	加密方式	密钥	VLAN ID	用户数	上行带宽(KB/s)	下行带宽(KB/s)
*	1	<input type="text"/>	开启	开启	不加密	不加密		0	0	0	0
*	2	<input type="text"/>	开启	开启	不加密	不加密		0	0	0	0
<input type="button" value="添加"/> <input type="button" value="删除"/> <input type="button" value="应用"/> <input type="button" value="返回"/>											
<small>温馨提示：双频AP使用模板配置时，SSID 1/3/5/...是2.4G频段，SSID 2/4/6/...是5G频段！</small>											

2.配置无线模板名称

为区分模板，添加模板时，需要输入新添加模板名称。

注意：模板名称不能与已有模板相同、不可留空配置，不支持中文；模板配置保存后，模板名称不可编辑修改。

3.配置无线网络模式

2.4G 频段 AP 的无线网络模式 默认为 11bgn 模式，可选模式有 11bg、11b、11g、11bgn。如无特殊需要，建议使用默认 11bgn 模式，兼容性好，速率高；

5G 频段 AP 的无线网络模式，默认为 11an 模式，可选模式有 11an、11a、11n、11ac/a/n，建议使用默认值；

4.配置无线的信道带宽

2.4G 频段 AP 的信道带宽 默认为 20/40M，可选项有 20M、20/40M、40M+、40M-，建议使用默认值；

5G 频段 AP 的信道带宽，默认为 40M+，可选项有 20M、20/40M、40M+、40M-，11ac/a/n 网络模式下，可选项还有 80M，建议使用默认值；

5.配置登录 AP 的用户名/密码

注意，这里用户名密码是 web 方式登录 AP 时的用户名密码，用户名密码合法字符为 3~32 位的英文或数字组合；

6.配置 SSID 信息（无线使能需要开启）

（1）配置 SSID1 的名称，即无线信号的名称，合法字符包括汉字、字母、数字、下划线、连字符，最多支持 8 个汉字，含汉字时，最大字符数为 8 个，不含汉字时，最大字符数为 31 个；

（2）配置广播 SSID，开启广播 SSID，无线终端才能扫描到该 SSID，默认开启，若关闭，无线终端无法扫描到该 SSID；

（3）配置客户端隔离，默认关闭，功能开启后，客户端之间不能在二层通信；

支持单个 SSID 下客户端隔离配置；不同 SSID 下客户端默认为隔离状态，不可配。

(4) 配置 SSID1 的安全模式及加密方式，除默认“不加密”外，安全模式可选项有 WPA-PSK、WPA2-PSK、WPA/WPA2-PSK 三种模式，加密方式可选项有 AES、TKIP、AES/TKIP 三种算法，三种安全模式与三种加密算法可任意组合；

提示：建议使用 WPA/WPA2-PSK 安全模式与 AES/TKIP 加密算法组合，加密安全程度高，终端兼容性好。

(5) 配置 SSID1 的密钥，安全模式选择加密方式后，才可配置 SSID 密钥，密钥为无线终端连接 SSID 后，接入无线网络时的密码，密钥合法字符由 8~31 位的英文或数字组成；

(6) 配置 SSID1 的 VLAN ID，即为该 SSID 下的用户打上 tag 标签；

(7) 配置 SSID1 的用户数，即 SSID1 可接入多少个无线终端。接入 SSID 终端数的限制，可根据 AP 的实际使用场景及业务需求情况进行合理配置；

注意：新增模板，默认只使用 SSID1、SSID2，可配的最大的用户数为 128 个，若需要开启多个 SSID，可点击下方的添加按钮进行添加；

(8) 配置 SSID1 的上下行带宽，即对 SSID1 的接入用户进行带宽限制；

8. 单击“应用”按钮，保存模板的配置信息，保存后，新模板添加成功。

若不想保存，单击“返回”按钮即可；

AP模板											请输入模板名称	Go!
序号	选择	默认	模板名称	2.4G使能	5G使能	2.4G网络模式	5G网络模式	2.4G带宽	5G带宽	SSID/加密方式	操作	
1	<input type="checkbox"/>	<input checked="" type="radio"/>	Defaults	开启	开启	11bgn	11an	20M/40M	20M/40M	Wanbroad_2G/未加密 >>	详细信息	
2	<input type="checkbox"/>	<input type="radio"/>	test	开启	开启	11bgn	11an	20M/40M	40M+	test1/未加密 >>	详细信息	
3	<input type="checkbox"/>	<input type="radio"/>	a	开启	开启	11bgn	11an	20M/40M	40M+	sad/未加密 >>	详细信息	
4	<input type="checkbox"/>	<input type="radio"/>	213	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 >>	详细信息	
5	<input type="checkbox"/>	<input type="radio"/>	1231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 >>	详细信息	
6	<input type="checkbox"/>	<input type="radio"/>	2131	开启	开启	11bg	11ac/a/n	20M	80M	123/未加密 1321/未加密 345/未加密 3423/未加密	详细信息	
7	<input type="checkbox"/>	<input type="radio"/>	231	开启	开启	11bgn	11an	20M/40M	40M+		详细信息	

100 Page 1 of 1 go

配置完成后 ,AP 模板页面 SSID/加密方式 ,显示 SSID1 的名称和加密方式 ;
未配置该 SSID 时 , SSID 显示未启用 , SSID3、 SSID4 可不配置 ;

提示 : 将鼠标放于 SSID 区域中的 “MORE” , 可以预览所有 SSID 的名称及加密方式信息。

9. 选配默认模板

已配置多个 AP 模板 , 通过 “默认” 列可以完成选配默认模板。如 : 需配置名称为 test 的 AP 模板为默认模板 , 勾选 test 模板默认选项 , 即配置成功。

首次接入的 AP 将按照配置的默认模板自动推送 AP 模板配置信息 ;

注意 : 配为默认模板后 , 该模板不能删除 , 要删除需先选择其他 AP 模板为默认模板。

AP模板											请输入模板名称	Go!
序号	选择	默认	模板名称	2.4G使能	5G使能	2.4G网络模式	5G网络模式	2.4G带宽	5G 带宽	SSID/加密方式	操作	
1	<input type="checkbox"/>	<input type="radio"/>	Defaults	开启	开启	11bgn	11an	20M/40M	20M/40M	Wanbroad_2G/未加密 <more >>	详细信息	
2	<input type="checkbox"/>	<input checked="" type="radio"/>	test	开启	开启	11bgn	11an	20M/40M	40M+	test1/未加密 <more >>	详细信息	
3	<input type="checkbox"/>	<input type="radio"/>	a	开启	开启	11bgn	11an	20M/40M	40M+	sad/未加密 <more >>	详细信息	
4	<input type="checkbox"/>	<input type="radio"/>	213	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <more >>	详细信息	
5	<input type="checkbox"/>	<input type="radio"/>	1231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <more >>	详细信息	
6	<input type="checkbox"/>	<input type="radio"/>	2131	开启	开启	11bg	11ac/a/n	20M	80M	123/未加密 <more >>	详细信息	
7	<input type="checkbox"/>	<input type="radio"/>	231	开启	开启	11bgn	11an	20M/40M	40M+	123/未加密 <more >>	详细信息	

100 | Page 1 of 1 | go

10. 配置保存 , 保存 AP 模板配置信息 , AC 重启后配置不会丢失 , 若不保存配置 , AC 重启后配置信息将丢失。

17.4.2 AP 配置

AP 配置页面 , 可对接受 AC 管理的 AP 名称、 IP、掩码、无线功率、信道及 AP 模板进行选择配置 , 同时可以对 AP 进行配置下发及统一配置下发。

快速向导	AP配置表 请输入AP的MAC地址											
监控统计	序号	选择	AP名称	AP MAC	IP地址	IP掩码	2.4G功率(%)	5G功率(%)	2.4G信道	5G信道	AP模板	AP基础信息
功能管理	*	<input type="checkbox"/>	<input type="text"/>	*	<input type="text"/>	<input type="text"/>	选择	选择	选择	选择	选择	*
AP基本设置	1	<input type="checkbox"/>	BK-AP-X1	EC:D9:C2:05:00:61	192.168.0.123	255.255.255.0	25	auto	11	auto	test	基础信息
AP模板	2	<input type="checkbox"/>	BK-AP	EC:D9:D1:C4:D1:90	192.168.0.31	255.255.255.0	25	auto	1	auto	test	基础信息
AP配置	Page 1 of 1 go											
AP升级	应用 删除											
AP系统维护												
AP定时重启												

AP名称：配置AP的名称，在“编号”为“*”一行的输入框，可对AP的名称进行批量更改，AP名称可由英文、数字或连字符组成，最大支持31个字符，批量配置时，名称尾数会进行自动“加1”递增；

AP MAC：显示AP的MAC地址信息；

IP地址：配置AP的IP地址，在“编号”为“*”一行的输入框，下面的IP地址将“加1”递增，方便批量配置AP IP地址；

IP掩码：配置AP的IP地址的掩码，在“编号”为“*”一行的输入框，可以批量地配置IP掩码；

2.4G功率：配置双频AP 2.4G频段的无线发射功率；

5G功率：配置双频AP 5G频段的无线发射功率；

2.4G信道：配置AP 2.4G频段的信道，可选项1~13、Auto信道，建议临近AP使用1/6/11信道进行循环错开配置；

5G信道：配置AP 5G频段的信道，可选项149~165、Auto信道，建议临近AP的信道错开配置；

注意：双频AP的信道配置受信道带宽的影响，将有不同的信道配置，如下表所示：（双频AP模板、默认的信道带宽为20M/40M）

信道带宽	20M	20/40M	40M_PLUS	40M_MINUS
频段信道				
2.4G 频段	Auto、1~13	Auto、1~13	Auto、1~9	Auto、5~13
5G 频段	Auto、 149~165	Auto、149、157	Auto、149、157	Auto、153、161

AP 模板：配置指定 AP 需要的 AP 模板，应用后 AP 模板信息将下发到 AP，同时可以勾选多个 AP，配置多个 AP 的模板，应用后，可实现批量配置下发；

删除：“选择”勾选需要删除的 AP 信息，单击“删除”按钮，将删除该 AP 在 AC 上的信息，AP 重新加入后则会再次显示；

注意：AP 配置页面的所有配置操作，都需要通过单击“应用”后，配置才会下发，下发时，AP 将自动重启，在下发过程中，请勿进行其它配置更改操作。

17.4.3 AP 升级

AP 升级页面，可以查看 AP 的名称、设备型号、MAC 地址、SN 码、当前版本 AP 密钥状态等信息，可以对在线 AP 进行批量升级。

快速向导	AP升级表
监控统计	
功能管理	
AP基本设置	
AP模板	
AP配置	
AP升级	
AP系统维护	
AP定时重启	

选择	名称	设备型号	MAC地址	SN码	当前版本	AP密钥状态
<input type="checkbox"/>	-	-	-	-	-	-
<input type="checkbox"/>	BK-AP-X1	BK-AP300-X1	EC:D9:C2:05:00:61	D001ion007654321	V1.0.0-R1	匹配/正常
<input type="checkbox"/>	BK-AP	BK-AP300-M1	EC:D9:D1:C4:D1:90	D207031101660072	V1.0.0-R1	匹配/正常

浏览

100 Page 1 of 1

温馨提示:升级设备时请保持型号一致!

AP 密钥状态：可以查看 AP 的密钥匹配状态，密钥不匹配则不能对该 AP 进行升级，若当前有 AP 正在升级，则状态会由正常显示为升级中，需等待该 AP 升级完成后，才能对其他 AP 进行升级。

MAC 地址：AP 唯一的标识，可通过 MAC 地址对 AP 进行区分。

当前版本：可以查看 AP 当前的软件版本号。

若需要为在线 AP 进行升级操作，可在选择项中对需升级的 AP 进行勾选，通过浏览进行版本加载，再单击“升级”执行版本升级操作。

勾选单个、多个相同型号及版本的 AP，可实现多个同型号 AP 批量升级，请务必保证升级软件与设备型号匹配。

AP 版本升级过程约需要 3 分钟，升级完成后可在“当前版本”查看升级后的版本信息，升级过程中请注意，防止设备断电或断开网线连接。

17.4.4 AP 系统维护

AP 系统维护页面，可对接受 AC 管理的 AP 进行重启或恢复出厂配置操作。



选择	名称	设备型号	MAC地址	SN码	当前版本	AP密钥状态
<input type="checkbox"/>	-	-	-	-	-	-
<input type="checkbox"/>	BK-AP-X1	BK-AP300-X1	EC:D9:C2:05:00:61	D008m007654321	V1.0.0-R1	匹配正常
<input type="checkbox"/>	BK-AP	BK-AP300-M1	EC:D9:D1:C4:D1:90	D207031101660072	V1.0.0-R1	匹配正常

支持单个或多个在线状态 AP 批量重启。通过 AP 密钥状态可以查看 AP 的密钥匹配状态，密钥不匹配的 AP，重启操作无效。

注意：单击重启后，连接到对应 AP 上的终端将会断开 WiFi 连接，AP 启动后会重新加入 AC 并接受管理。

支持单个或多个在线状态 AP 批量恢复出厂配置。处于断开状态的 AP，配置复位操作无效。

17.4.5 AP 定时重启

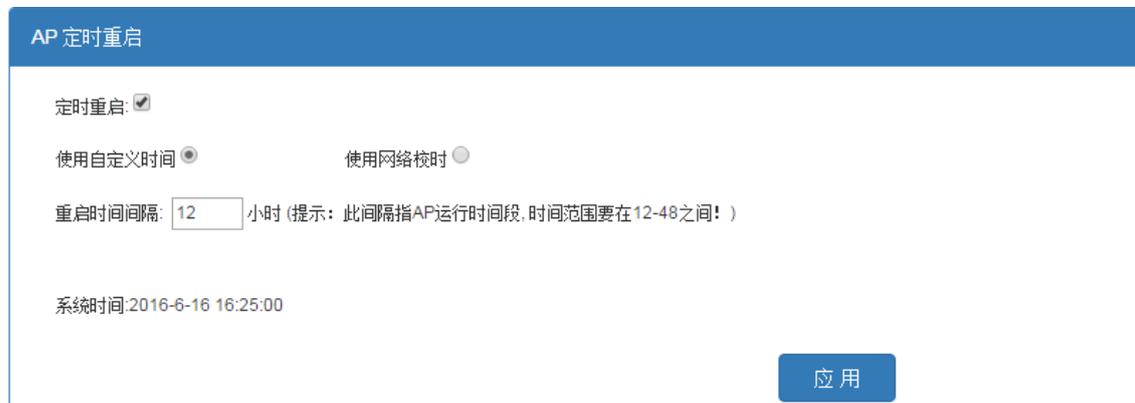
AP 定时重启页面，定时重启功能默认未启用，会显示当前系统时间（路由器可上网，获取网络时间）。



勾选定时重启功能选框，可以看到 AP 定时重启功能分为：自定义时间重启和网络校时重启两种模式。

自定义时间重启：需要设置 AP 重启时间间隔，即从应用该功能后，AP 的运行时间大于等于该设置时间时，会自动重启，有效时间范围为 12~48 小时，且为整数。

例如：若当前 AP 运行时间为 8 小时，设置 AP 定时重启，重启时间间隔为 12，则在 4 小时之后，AP 运行到 12 小时时，自动重启 AP。若当前 AP 运行时间为 15 小时，我们填写自定义重启时间为 12，那么设置后，点击应用，AP 会立即重启。



网络校时：勾选使用网络校时，配置页面如下图，需要配置重启时间点和重启的日期（选择一周内日期方式），即实现在一周内的指定日期、指定时间点，对 AP 自动重启。配置完成后并点击应用，将同步网络系统时间。



关于重启时间点，可选择 0~23 点的整点重启，建议选择配置凌晨 2:00、3:00、4:00 这样的业务闲时，进行定时重启操作。还可以选择一周内的指定日期进行重启（不勾选的日期默认为不重启），默认星期一到星期日未勾选。

17.5 认证营销

17.5.1 认证方式

•认证选择

用户认证页面，可实现用户上网认证方式配置，AC 管理支持 7 种主流认证方式，分别是：一键认证、微信认证（微信连 WiFi）、短信认证、密钥认证、Radius 认证、身份证认证、外置服务器认证，满足用户不同认证方式需求，还支持免认证。



AC 管理认证页面，勾选需要开启的认证方式（一键认证、微信认证（微信连 WiFi）、短信认证、密钥认证、Radius 认证、身份证认证、外置服务器认证），按页面提示配置相应信息，单击“应用”保存，即可完成认证配置操作。

还支持组合认证，支持 Radius 认证、短信认证、微信认证（微信连 WiFi）、一键认证、密钥认证组合，支持任意组合，可全选。

• 倒计时认证

可设置用户浏览页面 X 秒后，允许其无需认证上网 Y 分钟。

• 用户时限

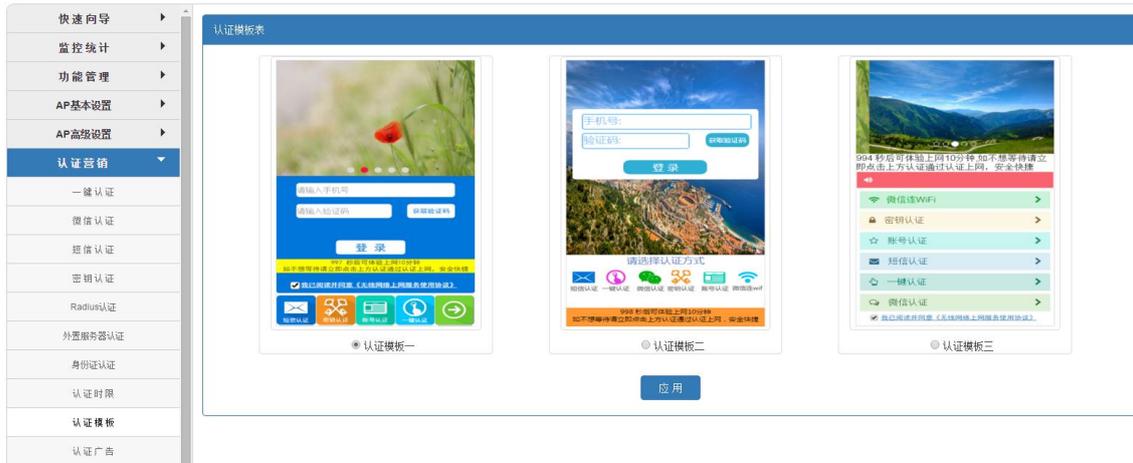
用户时限：提供两种上网时间限制，一是用户离开 X 分钟后下线，即 X 分钟内，用户无任何数据网络流量；二是强制给用户设定上网时限 Y，即用户上线 Y 分钟后，强制下线。

配置认证功能后，终端接入网络后，无法直接进行上网，需要在浏览器弹出的认证页面，输入正确的账号密码或单击指定按钮后，才能实现上网。

17.5.2 认证模板

可设置认证页面所使用的模板，有两种认证模板供选择。

勾选模板下方的圆圈，点击应用即生效，默认启用认证模板一。



17.5.3 认证广告



广告配置功能，为用户提供设置认证登录页面的广告图片。该功能需结合认证功能使用。

认证登录页面广告图片支持 5 张，上传广告图片需注意：广告图片图片大小限制为不超过 128KB，否则上传不成功（您可通过 Windows 自带的画图工具，将高清图片等比缩放或使用专业图形处理工具处理图片），为保证体验效果，建议您配置 16:9 尺寸的图片；

图片上传：浏览路径，选择需要上传的图片，单击提交即可；

广告信息：配置的广告信息将在 portal 页面进行滚动播放，广告信息长度支持 50 位字符。

认证后推送网址：结合认证功能使用，为用户提供认证后跳转页面的 URL 链接配置，URL 连接最大支持 255 个字符。

认证后推送网址的 URL 配置方法：输入有效的 URL 的连接，单击“应用”保存 终端接入认证 通过认证后 会自动跳转到推送的 URL 页面 默认为 TG-NET 的官网链接。

认证后推送网址

URL:

17.6 高级策略

高级策略主要是配置用户的一些业务需求。高级策略二级菜单包括 2 个三级菜单，依次是黑白名单、ACL 配置。

17.6.1 黑白名单

黑白名单功能开启认证功能后生效，可实现限制指定用户的上网行为，配置为黑名单的用户，无论是否已认证，都将被禁止上网，配置为白名单的用户，无需认证，可直接上网。

注意：黑白名单功能生效的前提是 AC 开启了认证功能，最大支持 128 条黑白名单条目。

黑白名单页面。可实现添加、删除黑白名单条目。



【示例 1】添加一个白名单条目

单击“添加”按钮，填写白名单用户名称、终端 MAC 地址、业务行为“通过”，应用，配置完成。

【示例 2】添加一个黑名单条目

单击“添加”按钮，填写黑名单用户名称、终端 MAC 地址、业务行为“丢弃”，应用，配置完成。

【示例 3】删除黑名单条目

选中指定的一个、多个或全部黑名单用户名称，单击“删除”，即完成删除黑名单条目操作。

黑白名单条目名称为对该用户进行简单的描述，以便区分，名称支持字母、数字或连字符组成。

业务行为：指添加的用户的上网行为是通过还是禁止，可选“通过”或“丢弃”，通过即配置终端为白名单用户，丢弃则配置终端为黑名单用户；

同时，认证用户可在【监控统计—用户列表】页面，单击黑白名单图标，进行快捷添加，单击后会提示填写黑白名单用户名，填写后确认，即添加成功。



在黑白名单页面可以看到黑白名单用户信息。

黑白名单				
选择	序号	名称	MAC地址	业务行为
<input type="checkbox"/>	*	*	格式: XX:XX:XX:XX:XX:XX	请选择
<input type="checkbox"/>	1	123	DC:2B:2A:B0:88:52	通过

温馨提示: 请不要重复输入相同的MAC地址!

配置完成后，请根据页面右上角保存配置提示，及时保存当前配置。

17.6.2 ACL 配置

开启认证功能后，ACL 配置功能生效。通过配置 ACL 规则，可实现限制局域网内终端设备的接入访问控制。

注意 :ACL 功能生效的前提是 AC 管理开启了认证功能，最大支持 16 条 ACL 配置条目。

ACL配置表									
选择	ACL名称	过滤方式	用户网络	源端口	目的网络	目的端口	作用时期	业务行为	配置帮助
<input type="checkbox"/>	*	请选择	*	*	*	*	请选择	请选择	

如果有需要，请点击右上角的配置帮助，参考配置指导

添加：实现添加一条 ACL 条目。

删除：选中指定 ACL 条目，实现删除操作。

应用：保存配置的规则，并使其生效。

选择：可实现勾选对应的 ACL 条目，进行“删除”操作。

ACL 名称：ACL 配置名称，名称需唯一。可对该条目进行简单的描述，以便区分，名称可由英文、数字或连字符组成。

协议规则：分为 IP、ICMP、TCP、UDP、URL 五种协议，可设置对应的协议规则，通过协议过滤，达到访问控制的效果。

用户网络 需要过滤的用户 IP 地址和掩码 格式为 IP/掩码位 如 1.1.1.1/24 , 表示需要过滤的 IP 地址段为 1.1.1.1~1.1.1.255 填 0.0.0.0/0 即表示所有用户。

源端口：需要过滤的源端口，若不确定可配置为 0，填 0 为缺省。

目的网络 需要过滤的目的 IP 地址和掩码 格式为 IP/掩码位 如 2.2.2.2/24 , 表示需要过滤的 IP 地址段为 2.2.2.1~2.2.2.255 填 0.0.0.0/0 即表示所有用户。

目的端口：需要过滤的目的端口，若不确定可配置为 0，填 0 为缺省。

作用时期：与用户认证有联系，分为三种时期，“所有”、“认证前”、“认证后”。“所有”表示认证前、后都对用户的上网行为进行过滤；“认证前”表示对用户认证前的上网行为进行过滤；“认证后”表示对用户认证后的上网行为进行过滤。

业务行为：可选项为“丢弃”、“通过”，选择“丢弃”时对所有匹配的报文全部丢弃；选择“通过”时对所有匹配的报文正常转发。

【示例 1】添加一条 IP 协议规则的 ACL 条目

单击“添加”按钮，填写 ACL 用户名称，选择协议号，填写用户网络、目的网络、源端口、目的端口信息，然后配置作用时期及业务行为，单击“应用”，即配置完成。

ACL 配置表 配置帮助								
选择	ACL 名称	过滤方式	用户网络	源端口	目的网络	目的端口	作用时期	业务行为
<input type="checkbox"/>	*	请选择	*	*	*	*	请选择	请选择
<input type="checkbox"/>	123	ICMP	192.168.1.0/24	0	192.168.1.254/32	0	所有	丢弃

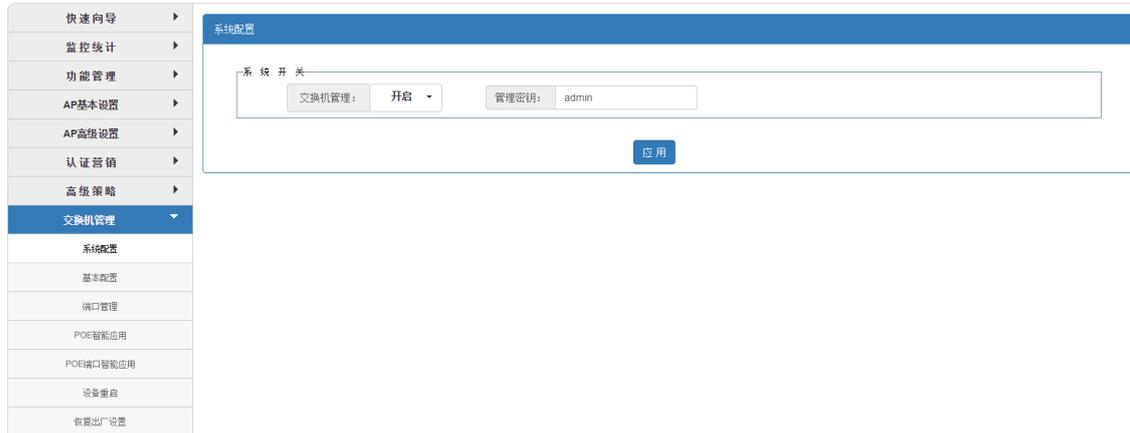
如果有需要，请点击右上角的配置帮助，参考配置指导

【示例 2】删除 ACL 条目

选中指定的一个、多个或全部 ACL 条目，单击“删除”，即完成删除 ACL 条目的操作。

17.7 交换机管理

交换机管理主要用于管理交换机，可对内网中云管理 key 与 AC 管理密钥相同的交换机进行管理。



17.7.1 系统配置

系统配置页面。系统开关功能，可配置交换机管理开启、禁用，修改 AC 的交换机管理密钥。交换机管理默认开启，管理密钥默认为：admin，最大可配 8 位字符，支持数字+英文。

注意：交换机的云管理 KEY 必须与 AC 管理的管理密钥相同，否则 AC 管理将不能对交换机进行管理。



交换机管理设置为开启，则 AC 管理可以管理交换机；交换机管理设置为关闭，则 AC 管理无法管理交换机。

管理密钥匹配，AC 管理密钥与交换机的云管理 key 相同时，AC 可以对交换机的配置进行修改操作；管理密钥不匹配，AC 不能对交换机的配置进行修改操作。

17.7.2 基本配置

基本配置：可查看交换机的设备 ID、SN、MAC 等信息，可配置交换机的基本信息，如交换机的设备别名、IP 地址、IP 掩码、用户密码等，如下图所示。

设备ID	设备型号	MAC地址	序列号	设备类型	设备别名	IP地址	IP掩码	用户密码
3	BK-S1000-24POE	AC:31:9D:0C:99:99	12345678999	POE交换机	BK-S1000-24POE[3]	192.168.1.5	255.255.248.0
4	BK-S1000-8POE	AC:31:9D:0D:60:99	A2020135668777	POE交换机	BK-S1000-8POE[5]	192.168.1.4	255.255.248.0
5	BK-S1000-26G	AC:31:9D:AC:31:9F	A1236456789	交换机	BK-S1000-26G[2]	192.168.1.2	255.255.248.0
6	BK-S1000-24POE	AC:31:9D:07:A7:55	A2020135668799	POE交换机	BK-S1000-24POE[4]	192.168.1.3	255.255.248.0

温馨提示：如果将交换机和路由器配置成同一网段，可以点击【设备型号】下的链接，登录交换机管理页面。

在*行 还可批量配置设备基本信息 其中 IP 地址批量配置为加 1 递增方式，设备别名会在配置名称后加数字区分设备。

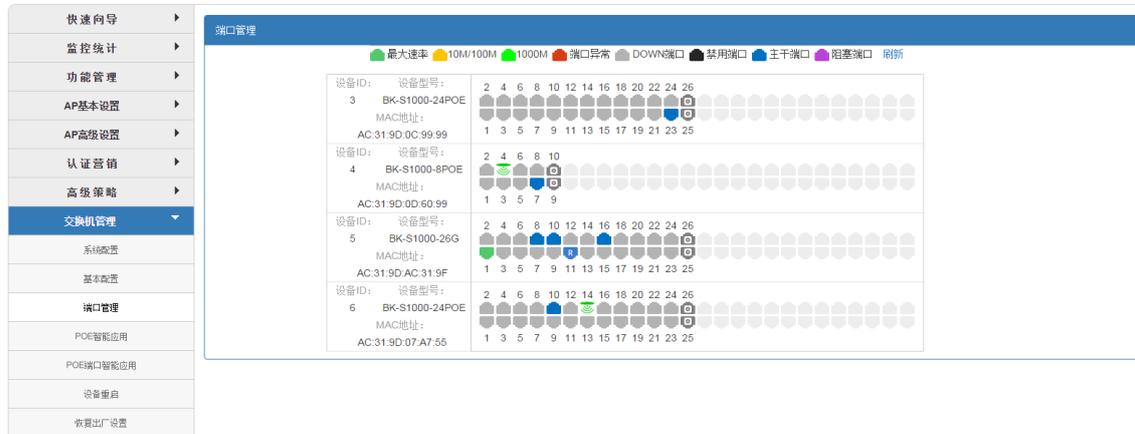
设备ID	设备型号	MAC地址	序列号	设备类型	设备别名	IP地址	IP掩码	用户密码
*	*	*	*	*	BK-SW	192.18.1.100	255.255.255.0	admin
3	BK-S1000-24POE	AC:31:9D:0C:99:99	12345678999	POE交换机	BK-SW1	192.18.1.101	255.255.255.0
4	BK-S1000-8POE	AC:31:9D:0D:60:99	A2020135668777	POE交换机	BK-SW2	192.18.1.102	255.255.255.0
5	BK-S1000-26G	AC:31:9D:AC:31:9F	A1236456789	交换机	BK-SW3	192.18.1.103	255.255.255.0
6	BK-S1000-24POE	AC:31:9D:07:A7:55	A2020135668799	POE交换机	BK-SW4	192.18.1.104	255.255.255.0

温馨提示：如果将交换机和路由器配置成同一网段，可以点击【设备型号】下的链接，登录交换机管理页面。

注意：若将交换机和路由器配置成同一网段，可以点击【设备型号】下的链接，登录交换机管理页面。

17.7.3 端口管理

端口管理页面，可查看、设置交换机端口。



端口管理页面顶部，展示了交换机端口显示的颜色状态对应的含义。设备每个端口的状态都会有对应的状态显示，并且会显示出内网交换机中所有端口，并标明路由器端口、AP 端口、服务器端口。

 为连接路由器的端口；

 为连接 AP 的端口；

 为服务器端口，该端口需要用户手动设置后才会显示，用户点击连接服务器的端口，勾选“服务器端口”项，确定保存后即可。

端口管理页面，点击任一设备的任一端口，可以查看端口基本信息、接入终端的 IP、MAC 信息，可设置端口状态，如下图。

端口基本信息

✕

请选择端口状态 ▾ 服务器端口 设置

AP端口、路由器端口均不能设置为服务器端口!

端口类型:	电口
连接状态:	连接
双工模式:	全双工
最大速率:	100M
终端IP:	192.168.0.31
终端MAC:	EC:D9:D1:C4:D1:90

提示: BK-AP下有0个终端在线

使能端口: 开启端口状态;

禁用端口: 关闭端口状态;

端口自协商: 设置端口的速率模式修改为自动协商;

强制 1000M: 设置端口的速率模式为强制 1000M;

端口重启: 重启端口;

注: POE 交换机, 只能重启供电端口, 非供电端口不会重启; 非 POE 交换机, 可重启所有端口, 请勿重启连接路由器的端口。

服务器端口: 可设置接服务器的交换机端口设置为服务器端口。

17.7.4 POE 智能应用

此功能可以定时的对 POE 交换机进行设备重启、所有供电端口的端口供电开启/关闭操作。

设备智能应用					
设备	行为	时间	重复	使能	删除
BK-S1000-24POE[3],BK-S1000-8POE[5],BK-	设备重启	03:00	周一-周四	<input checked="" type="checkbox"/> ON	<input type="button" value="删除"/>
<input type="button" value="添加"/> <input type="button" value="保存"/>					

设备：选择需要进行定时操作的设备

行为：选择需要进行的的行为操作

设备重启：设置此行为，所选择的设备将会重启

端口供电开启：设置此行为，所选择的设备的所有供电端口的供电功能将会开启，即端口将能为终端设备供电

端口供电关闭：设置此行为，所选择的设备的所有供电端口的供电功能将会关闭，即端口将不能为终端设备供电

时间：设置此定时任务的执行时间

重复：设置此定时任务规律性执行的时间

使能：定时任务的开关，使能开启，定时任务生效，使能关闭，定时任务无效。

删除：可删除定时任务

17.7.5 POE 端口智能应用

此功能可以定时的对 POE 交换机的端口进行定时重启、供电端口的端口供电开启/关闭、端口的使能/禁用、智能重启操作。

端口智能应用						
设备	端口	行为	时间	重复	使能	删除
BK-S1000-24POE[3]	1,2,3,4,5,6,7,8,9,10,11,12,13,14	智能重启			<input checked="" type="checkbox"/> ON	<input type="button" value="删除"/>
BK-S1000-8POE[5]	1,2,3,4,5,6,7,8,9,10	智能重启			<input checked="" type="checkbox"/> ON	<input type="button" value="删除"/>
BK-S1000-24POE[4]	1,2,3,4,5,6,7,8,9,10,11,12,13,14	智能重启			<input checked="" type="checkbox"/> ON	<input type="button" value="删除"/>
<input type="button" value="添加"/> <input type="button" value="保存"/>						

定时重启：设置此行为，所选择的设备的端口，将会重启，只对供电端口生效

端口供电开启：设置此行为，所选择的设备的供电端口的供电功能将会开启，即端口将能为终端设备供电

端口供电关闭：设置此行为，所选择的设备的供电端口的供电功能将会关闭，即端口将不能为终端设备供电

端口使能：设置此行为，所选择的设备的端口将处于数据转发和供电状态。

端口禁用：设置此行为，所选择的设备的端口将无法转发数据、供电。

智能重启：此行为只对连接 AP 的端口生效，若 AP 连续 10 分钟不响应 AC 的报文，则会重启该接口，1 天内只重启一次

17.7.6 设备重启

如下图，系统重启页面，可对接受 AC 管理的交换机进行重启操作。

支持单台或多台交换机的批量重启。

选择	名称	设备型号	MAC地址	当前软件版本
<input type="checkbox"/>	*	*	*	*
<input type="checkbox"/>	BK-S1000-24POE[3]	BK-S1000-24POE	AC:31:9D:0C:99:99	V3.1.1-R2
<input type="checkbox"/>	BK-S1000-8POE[5]	BK-S1000-8POE	AC:31:9D:0D:60:99	V3.1.1-R2
<input type="checkbox"/>	BK-S1000-26G[2]	BK-S1000-26G	AC:31:9D:AC:31:9F	V3.1.1-R1
<input type="checkbox"/>	BK-S1000-24POE[4]	BK-S1000-24POE	AC:31:9D:07:A7:55	V3.1.1-R1

17.7.7 恢复出厂设置

恢复出厂设置页面，可对接入 AC 的交换机进行恢复出厂配置操作。

恢复出厂设置				
选择	名称	设备型号	MAC地址	当前软件版本
<input type="checkbox"/>	*	*	*	*
<input type="checkbox"/>	BK-S1000-24POE[3]	BK-S1000-24POE	AC:31:9D:0C:99:99	V3.1.1-R2
<input type="checkbox"/>	BK-S1000-8POE[5]	BK-S1000-8POE	AC:31:9D:0D:60:99	V3.1.1-R2
<input type="checkbox"/>	BK-S1000-26G[2]	BK-S1000-26G	AC:31:9D:AC:31:9F	V3.1.1-R1
<input type="checkbox"/>	BK-S1000-24POE[4]	BK-S1000-24POE	AC:31:9D:07:A7:55	V3.1.1-R1

温馨提示：恢复出厂后交换机会重启，除IP以外的所有配置均丢失！

支持单台或多台交换机的批量恢复出厂设置。

注意：交换机恢复出厂后，除管理 IP 地址配置不变外，其他配置均会恢复为系统默认配置。恢复出厂设置功能生效时，交换机将会自动重启。

17.8 系统管理

17.8.1 加入云端

云端管理，通过虚拟化技术，可让每个客户远程管理自己分布在各地的路由器，路由器加入云端后，就可以实现真正意义上的集中智能化管理，就像独享一个云端一样。

加入云端的条件：路由器可访问公网。

加入云端主要步骤：注册账号——加入云端——云端管理。下面将详细介绍。

17.8.1.1 注册云端账号

在 AC 管理页面，在“加入云端”菜单。在登录页面，可以看到这里需要填写加入云端的用户名、密码。



点击“欢迎访问万网博科云端管理系统”链接，访问云端网站。



点击立即注册，进行账号注册，进入云端用户注册页面，请按照提示信息，按实际情况填写注册信息，填写完成后，提交即完成云端账号注册。



注意：请填写真实信息，特别要注意及时保存、备份用户名、密码、手机号/邮箱（如果忘记用户名、密码，可通过手机号或邮箱方式找回密码）信息，以方便在您的网络出现问题时，网络运维商能及时联系并解决您的问题。

17.8.1.2 加入云端

注册云端账号成功后，在“加入云端”页面，用已注册的用户名、密码，登录，会弹出的“加入云端”信息页面，远程管理和上传告警建议均勾选。项目名称可按需设置中文、数字、字母等，联系人、联系电话、联系地址请填写真实信息，便于您对项目及管理、维护。

填写完成后，点击确定，会提示保存成功，再确定即加入云端。

云端信息

远程管理 上传告警

项目名称: BK-RC-2 (深圳) 联系人: XXX

联系电话: XXX 授权ID:

联系地址: XX省XX市XX区XX街道XX号

该设备已被管理员注册, 接受万网博科云端远程管理!

用户ID: huangfeng1 【maple】

E_MAIL: 2312174291@qq.com

[欢迎访问万网博科云端管理系统](#) [解除绑定](#)

加入云端

注意：普通用户授权 ID 可为空，非必填项。

加入云端后，加入云端按钮会更改为退出云端。

云端信息

远程管理 上传告警

项目名称: BK-RC-2 (深圳) 联系人: XXX

联系电话: 授权ID:

联系地址: 广东省深圳市南山区

该设备已被管理员注册, 接受万网博科云端远程管理!

用户ID: huangfeng1 【maple】

E_MAIL: 2312174291@qq.com

[欢迎访问万网博科云端管理系统](#) [解除绑定](#)

退出云端

此时，点击退出云端图标，确认后，路由器即退出云端。再点击加入，可以重新加入云端。

17.8.1.3 云端管理

路由器成功加入云端后，可以从外网，访问 <http://cloud.wanbroad.com/>，进入云端管理系统登录页面，如下图，填写云端登录用户名（或手机号/邮箱）、密码（即注册的用户名/手机号/邮箱、密码），登录。若用户忘记云端用户名、密码，可通过注册时使用的手机号/邮箱方式找回。



登录云端管理系统后，在商家列表中点击自己对应项目名称的“远程管理”，即可对该名称的路由器进行远程访问管理。



17.8.1.4 找回密码

在云端管理登录页面，点击忘记密码按钮，进入云端找回密码页面，输入注册时的用户名或邮箱，输入验证码，点击下一步；

点击获取验证码，输入获取的验证码，点击下一步；

设置您的新密码，即可使用该密码登录。

17.8.2 配置管理

配置管理页面，可进行 AC 管理配置的导入/导出。

单击“导出”按钮选择保存文件即可保存当前配置文件。如需导入配置文件，单击浏览按钮选择需要导入的正确的配置文件，单击“导入”按钮执行导入操作，导入配置文件后，需手动重启路由器，使其配置生效，路由器启动后，导入配置成功。



注：交换机管理中的 POE 智能应用与 POE 端口智能应用的配置，暂不支持导入/导出。

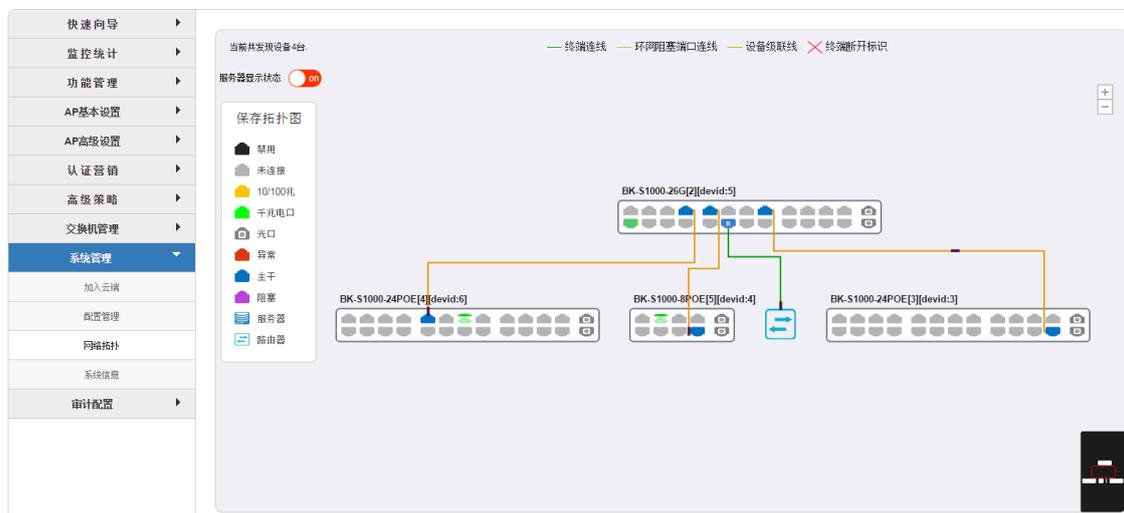
17.8.3 网络拓扑

通过自动侦测网络拓扑的方式，并以图形化方式显示出网络所有交换机实际连接结构；自动生成网络实际拓扑图，直观方便的管理界面使人对网络运行状况一目了然；丰富的图示信息，简单明了的显示了交换机端口的各种工作状态。

该拓扑简单明了的展示了各设备的接入关系，界面默认为最小缩略图，如下图：

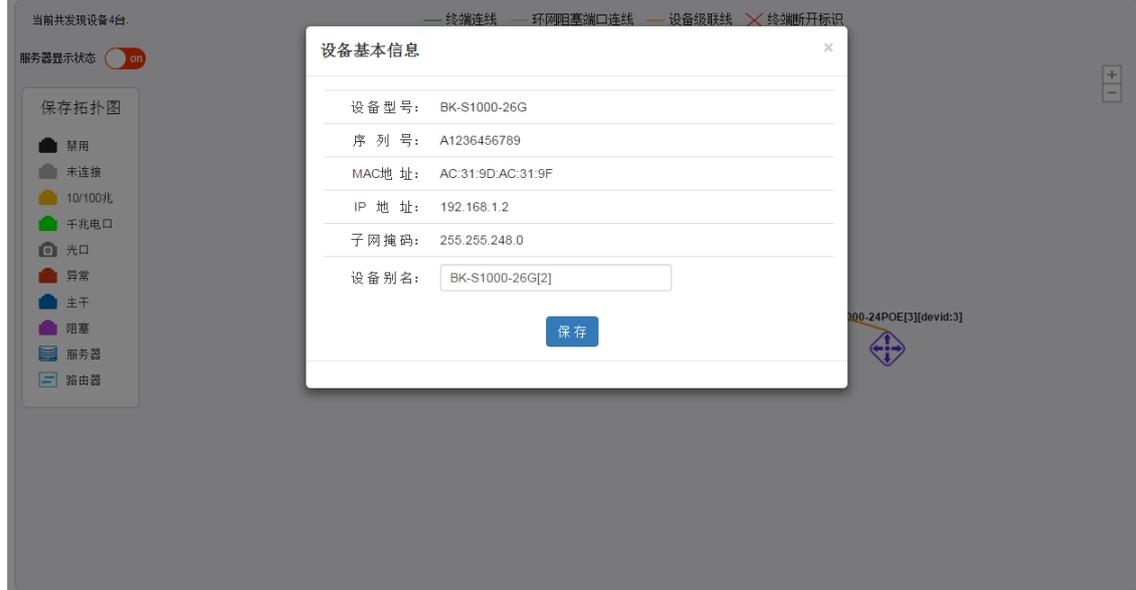


滚动鼠标，或者点击右上角“+”可以逐步放大拓扑图，查看详细拓扑，如下图所示：



放大拓扑图后，若拓扑图超出界面显示范围，可长按鼠标拖动拓扑图，且界面右下角会显示缩略图图标。

单击交换机设备名称或者图片，可以查看设备基本信息，修改设备名称，如下图所示：



在放大的拓扑图中，点击端口，可查看端口基本信息，并设置端口状态、服务器端口，如下图：



保存拓扑与重置拓扑

保存拓扑：可以保存当前拓扑图中的设备，保存成功后，AC 将不会再学习新接入的设备；

重置拓扑：可以取消当前的保存拓扑功能，让 AC 重新学习并生成拓扑图；

17.8.4 系统信息

可查看 AC 管理支持的 AP 数，以及 AC 管理的版本信息。

快速向导	▶
监控统计	▶
功能管理	▶
AP基本设置	▶
AP高级设置	▶
认证营销	▶
高级策略	▶
交换机管理	▶
系统管理	▼
加入云端	
配置管理	
网络拓扑	
系统信息	

系统信息	
AP授权数	128
软件版本	V1.0.1-R4

十八、退出

退出本次登陆，返回到登陆界面。