



智简路由器 V2

用户基本配置手册

(V2.0)

前言

1. 承蒙惠顾友讯网络产品，谨致谢意！本详细设置手册可协助您完成软件管理方面
的相关配置，硬件安装请参照设备包装里指导书《快速安装指引》，我们将持续以领先
技术为您提供更优质的服务！使用前请仔细阅读本手册，并妥善保管！

2. 此使用说明文档受著作权法、国际著作权条约及有关法律的保护，未经允许请勿
擅自复制本书的一部分或全部内容。本手册为基本用户手册，功能与型号并不是一一对
应，特殊功能模块详情请咨询技术支持。对于此手册的修改、使用以及最终解释权均归
友讯电子设备（上海）有限公司所有。

友讯电子设备（上海）有限公司

全国产品服务热线：400-629-6688

官方主页：www.dlink.com.cn

目 录

1、环境部署	1
1.1 部署线路连通	1
1.2 登录路由器	2
2、配置向导	6
3、系统状态	16
3.1 网络状态	17
3.2 流量分析	18
3.3 主机监控	20
3.4 DNS 缓存	21
3.5 登录记录	22
3.6 系统日志	22
4 网络基本配置	26
4.1 广域网配置	26
4.2 局域网设置	31
4.3 动态域名	33
4.4 接口设置	36
5 智能流控	37
5.1 优先级设置	37
5.2 应用协议分组	38
5.3 带宽限速	40
5.4 带宽保证	42
5.5 控制例外	43
6 行为管理	43
6.1 用户组	44
6.2 行为识别	44
6.3 行为识别	46
6.4 高级管理	47

6.5 邮件监控	51
6.6 网址管理	55
6.7 域名管理	58
6.8 URL 重定向	60
7 认证管理	62
7.1 基本设置	62
7.2 页面管理	64
7.3 PPPOE 设置	65
7.4 用户管理	67
8 防御配置	68
8.1 ARP 管理	68
8.2 访问控制	71
8.3 MAC 地址过滤	73
8.4 连接限制	74
8.5 DDOS 防御	75
8.6 Ping WAN 口	76
8.7 连接数限制	76
9 高级配置	77
9.1 策略路由	78
9.2 DNS 策略	84
9.3 通告系统	87
9.4 端口映射	90
9.5 NAT 转换	94
9.6 端口设置	96
9.7 路由表	97
9.8 DNS 代理	98
9.9 WEB 访问设置	100
9.10 端口镜像	101
9.11 NAT 快速转发	102
9.12 端口 VLAN	102
10.USB 存储	103
10.1 设备状态	103

10.2 共享服务	103
10.3 USB 日志	104
10.4 4G 上网设置	105
11.应用中心	106
11.1 AC 平台服务端	106
11.2 PPTP 配置	137
11.3 IPSEC 网对网	141
11.4 SD-WAN	147
12 系统维护	148
12.1 Ping 检测	148
12.2 网络唤醒	149
12.3 系统控制	149
12.4 系统配置	151
12.5 系统更新	152
12.6 申请控制	152
附录一 无线路由-无线相关设置	154
附录二 SD-WAN 应用相关设置	163

1、环境部署

1.1 部署线路连通

①设备前面板

名称	功能说明
WAN	路由器外网接口（上联接口）
LAN	路由器内网接口（下联接口）
WAN/LAN	角色自定转换接口。可在系统内修改接口为外网或内网口
SPF/SPF+	光纤模块接口。插入光模块后可用于光纤接入
USB	标准 USB 接口，5V 1A。可用于接入储存设备、输入设备以及设备充电
Console	通用型串口（型号不同参数有差异）
RESET	复位按钮。长按 10 秒以后松开，路由器自动恢复默认设置
DC-IN	直流电源插口 12V 1.5A（型号不同参数有差异）

②设备后面板

- 电源插孔：接插交流 100~240V,50~60H 电源
- 无线插孔：固定无线天线接口（仅限无线系列）

③指示灯说明

- PWR：电源指示灯。灯亮表示设备通电正常。
- SYS：系统指示灯。系统正常运行时此灯会亮。
- WAN：WAN 口工作指示灯。左上角为黄灯闪烁表示该 WAN 口线路有数据通过，右上角为绿灯表示 1000M 连接状态，右上角为橙灯表示 100M

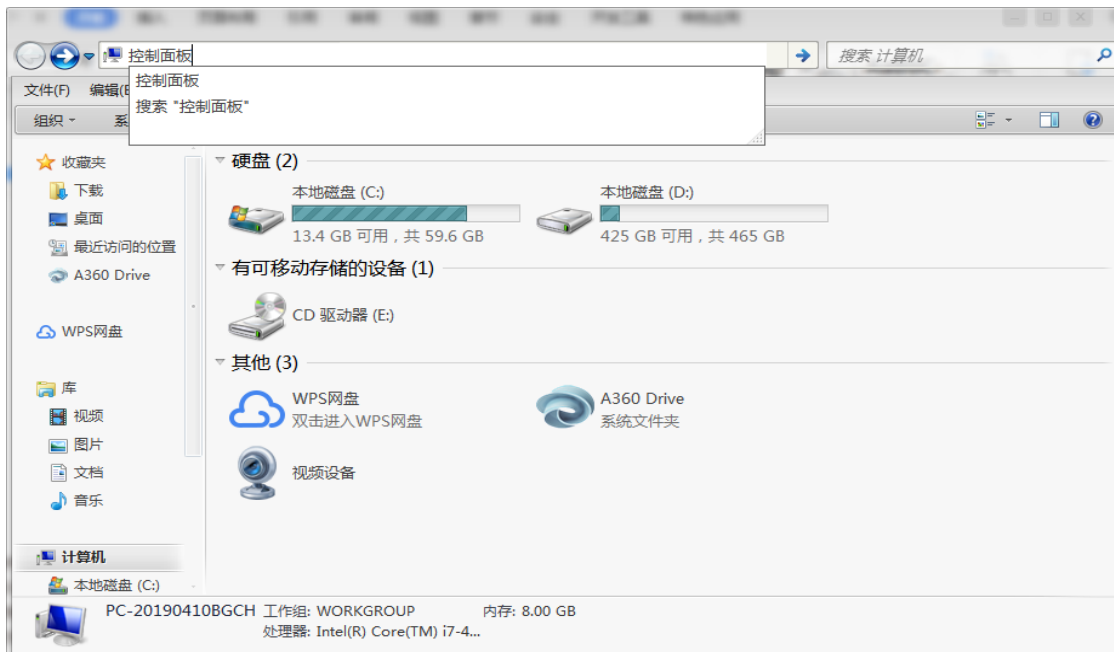
连接状态。

➤ LAN: LAN 口工作指示灯。灯亮表示 LAN 口线路接通。左上角为黄灯闪烁表示该 WAN 口线路有数据通过，右上角为绿灯表示 1000M 连接状态，右上角为橙灯表示 100M 连接状态。

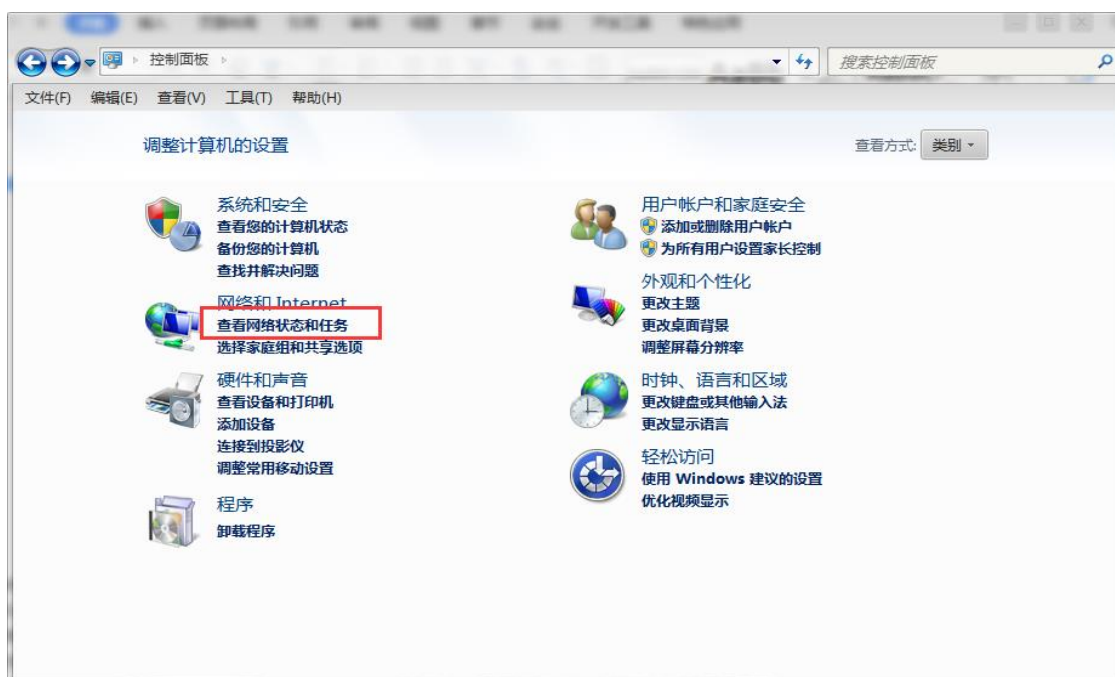
1.2 登录路由器

➤ 第一步：使用网线将电脑与路由器的 LAN1 口相连，并将电脑设置成自动获取 IP 地址。

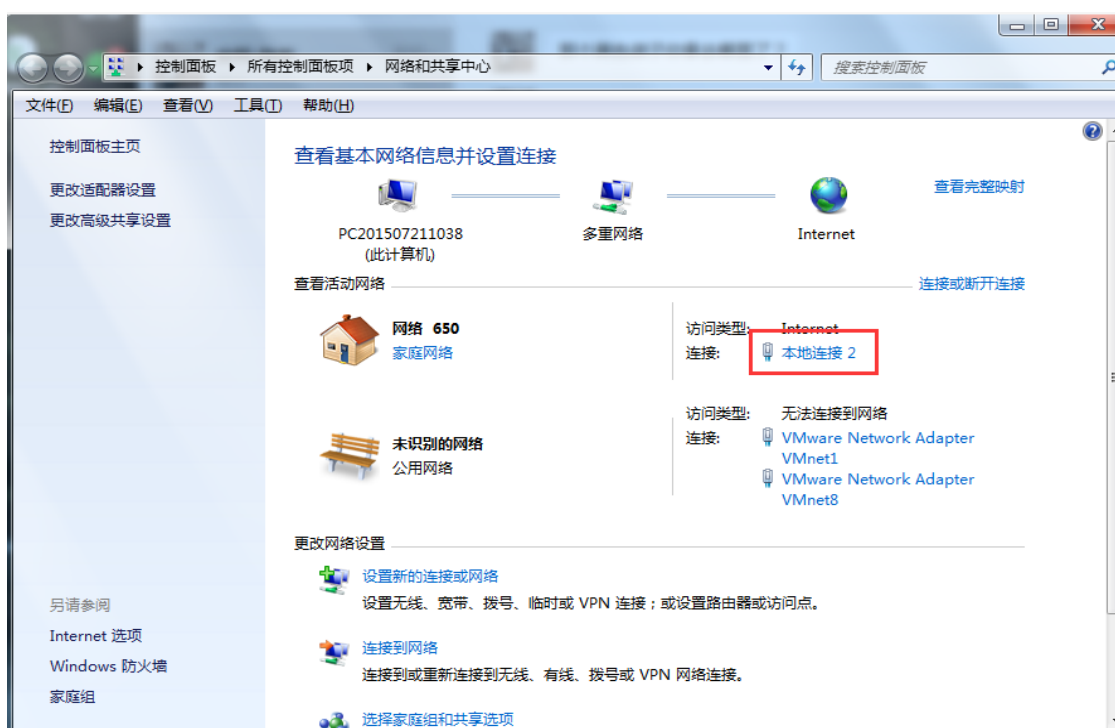
鼠标双击电脑桌面的“我的电脑”或“计算机”，打开后在顶部搜索框输入“控制面板”，然后按键盘的回车键打开：



然后点击控制面板中的“查看网络状态和任务”按钮：



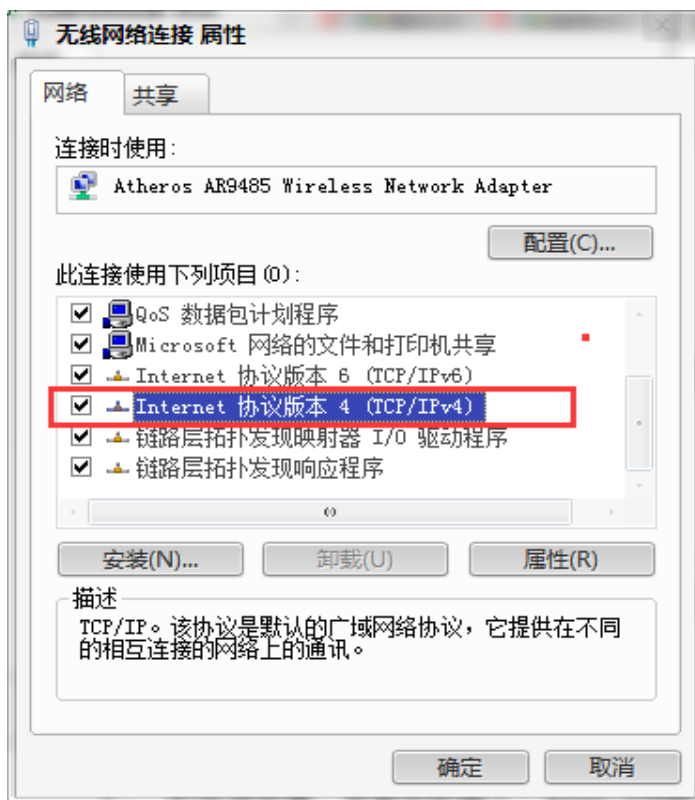
进入网络和共享中心后，点击中间部分显示的“本地连接”按钮：



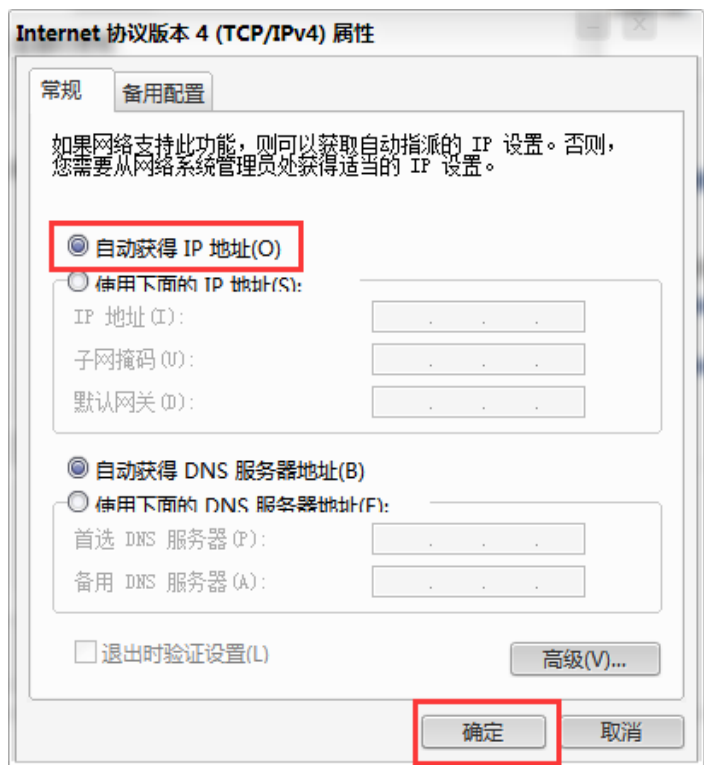
打开状态页面后，再点击左下方的“属性”按钮：



打开属性后，在下方项目中，找到“Internet 协议版本 4 (TCP/IPv4)”并双击打开：



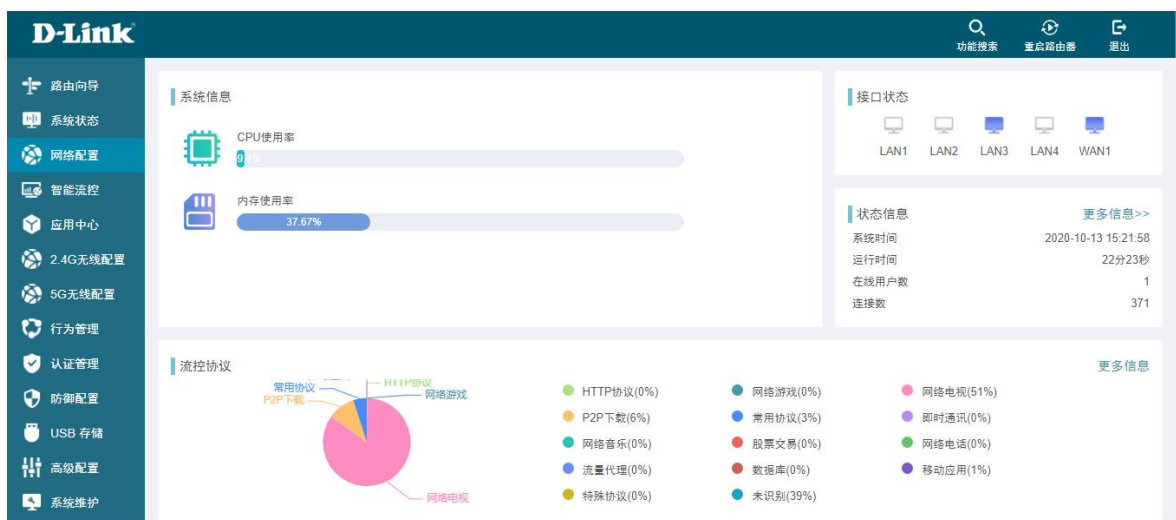
打开后，选择“自动获取 IP 地址”，并持续点击“确定”返回到本地连接界面：



➤ 第二步：打开浏览器，在地址栏输入：<http://192.168.0.1>（路由器默认 IP 地址），然后按键盘的 Enter 键，进入路由器系统登录界面：



输入管理员帐号和密码，点击确定进入路由器。路由器默认管理员帐号 admin 密码 admin。进入管理界面后，画面如下：



✧ **温馨提示：** 为了安全，我们强烈建议您在登录以后更改路由器密码，并牢记新密码。（若密码忘记，将无法再登录至路由器的 web 管理界面，请长按设备面板上的 Reset 按钮 10 秒以上将路由器恢复出厂设置）

2、配置向导

配置向导可以协助您快速配置您的网络。它的目的是让您在最短和最少的设置内能够访问到 Internet 网。进入路由器的配置页面，可以根据您的网络接入方式，选择不同连接类型进行上网。总共有 DHCP 类型线路、PPPOE 拨号线路、静态 IP 地址线路、透明桥和局域网五种。



➤ **第一步：** 点击左侧导航栏中的路由向导-配置向导，出现如下界面：



局域网设置 接口模式 WAN设置 管理设置

IP地址:

子网掩码:

[下一步](#)

➤ **第二步：** 点击下一步，设置内网 LAN 口地址：

IP地址:

子网掩码:

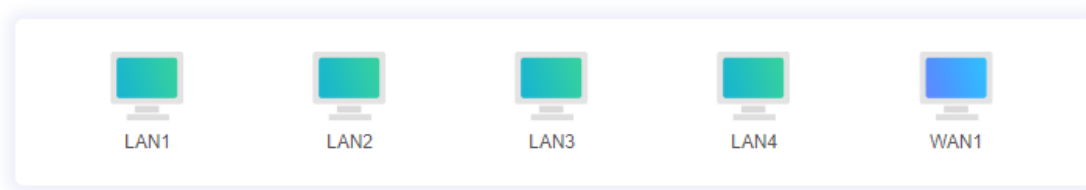
[下一步](#)

路由器 LAN 口 IP 地址： 修改路由器 LAN 口（即内网网关）的 IP 地址。

子网掩码： 填上与 LAN 口对应的掩码地址即可。

➤ **第三步：** 点击下一步，进入广域网口的设置界面。

在这一步中，我们可以先对广域/内网网口所使用的数量进行定义，直接点中图标即可，下一步。



点击图标分配相应LAN / WAN数量,当前LAN口数: 4 个 当前WAN口数: 1 个

上一步

下一步

在 WAN 口设置中可以对其 6 种连接类型（自动获取 IP 线路、PPPOE 拨号线路、静态 IP 地址线路、透明桥、局域网、关闭线路）进行设置，下面我们将一一向大家介绍：

①自动获取 IP 线路：

所谓自动获取 IP 线路，则是自动获取上级网络设备分配的 IP 地址。

WAN口： 广域网1 ▼

连接方式： 自动获取IP ▼

MAC地址： 40:80:00:10:86:D1

克隆 默认 随机

外网带宽： 上行 0 下行 0

KByte (0 表示不设置) 带宽值参考

DNS解析优先级： ☐ 高 ☐ 默认 ☒ 低

选择您要设置的广域网：根据实际接线选择广域网口。如 WAN1 接口对应广域网 1，WAN2 接口对应广域网 2，以此类推。

连接方式：选择自动获取 IP。

MAC 地址：可以填写，也可以不填，填写可以克隆您 PC 或自定义的 MAC 地址，不填则使用设备默认。

DNS 解析优先级：即使用 DNS 服务器来解析域名上网的优先级，如果几个广域网口都接了外线，且填上的 DNS 地址都不同，则可以设置优先级确定首先使用哪个 DNS。如在南方，电信的 DNS 优先级理应高一点，而北方则网通的 DNS 优先级高一点。

外网带宽：可根据出口带宽设定上、下行带宽速率。

②PPPOE 拨号线路（ADSL 拨号线路）：

WAN口：	广域网1	▼
连接方式：	PPPoE拨号上网	▼
用户账号：		
用户密码：		
服务名称：	选填	
连接检查间隔：	30	秒
MAC地址：	40:80:00:10:86:D1	
	克隆	默认
	随机	
外网带宽：	上行 0	下行 0
	KByte (0 表示不设置)	
	带宽值参考	
DNS解析优先级：	<input type="radio"/> 高 <input type="radio"/> 默认 <input checked="" type="radio"/> 低	

选择您要设置的广域网口：选择实际接 adsl 线路相应的广域网口。

连接类型：选择 PPPOE 拨号线路。

用户名称：填上运营商提供给你的帐号。

用户密码：填上运营商提供给你的密码。

服务名称：可以选填写，也可以不填。

连接检查间隔：PPPOE 拨号后根据连接通断情况进行判断是否自动重新连接。

MAC 地址：可以填写，也可以不填，填写可以克隆您 PC 或自定义的 MAC 地址，不填则使用设备默认。

外网带宽：可根据出口带宽设定上、下行带宽速率。

DNS 解析优先级：即使用 DNS 服务器来解析域名上网的优先级，如果几个广域网口都接了外线，且填上的 DNS 地址都不同，则可以设置优先级确定首先使用哪个 DNS。在南方，电信的 DNS 优先级理应高一点，而北方则网通的 DNS 高一点。

③**静态 IP 地址线路**(通常用于光纤接入或需要固定 IP 的情况):

WAN口：	广域网1	▼
连接方式：	静态IP	▼
IP地址：	172.18.170.165	
子网掩码：	255.255.255.0	
默认网关：	172.18.170.224	
静态DNS：	0.0.0.0	?
	0.0.0.0	
	0.0.0.0	
连接检查间隔：	30	秒
MAC地址：	40:80:00:10:86:D1	
	克隆	默认
	随机	
外网带宽：	上行 0	下行 0
	KByte（0 表示不设置）	
	带宽值参考	
DNS解析优先级：	<input type="radio"/> 高 <input type="radio"/> 默认 <input checked="" type="radio"/> 低	

连接类型：选择静态 IP 地址线路

IP 地址：填写运营商提供给你的 IP 地址。

子网掩码：填写运营商提供的子网掩码。

默认网关：填写运营商提供的网关。

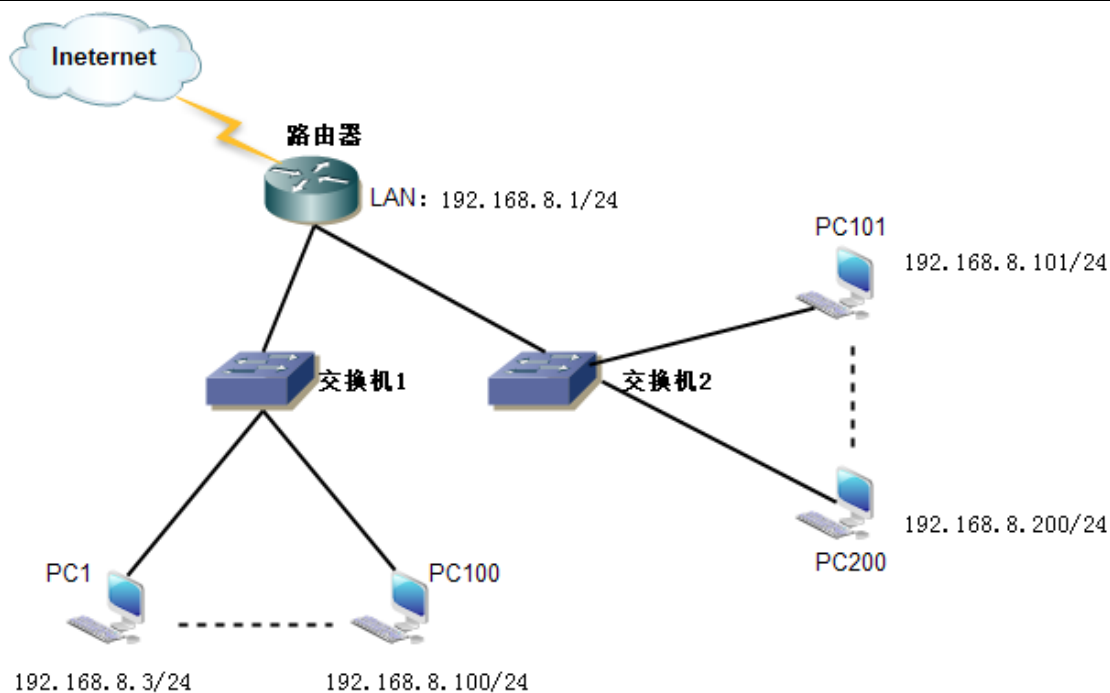
静态 DNS：必须填写，如不填写可能会造成无法访问网页。一般由运营商提供。

DNS 解析优先级：即使用 DNS 服务器来解析域名上网的优先级，如果几个广域网口都接了外线，且填上的 DNS 地址都不同，则可以设置优先级确定首先使用哪个 DNS。在南方，电信的 DNS 优先级理应高一点，而北方则网通的 DNS 高一点。

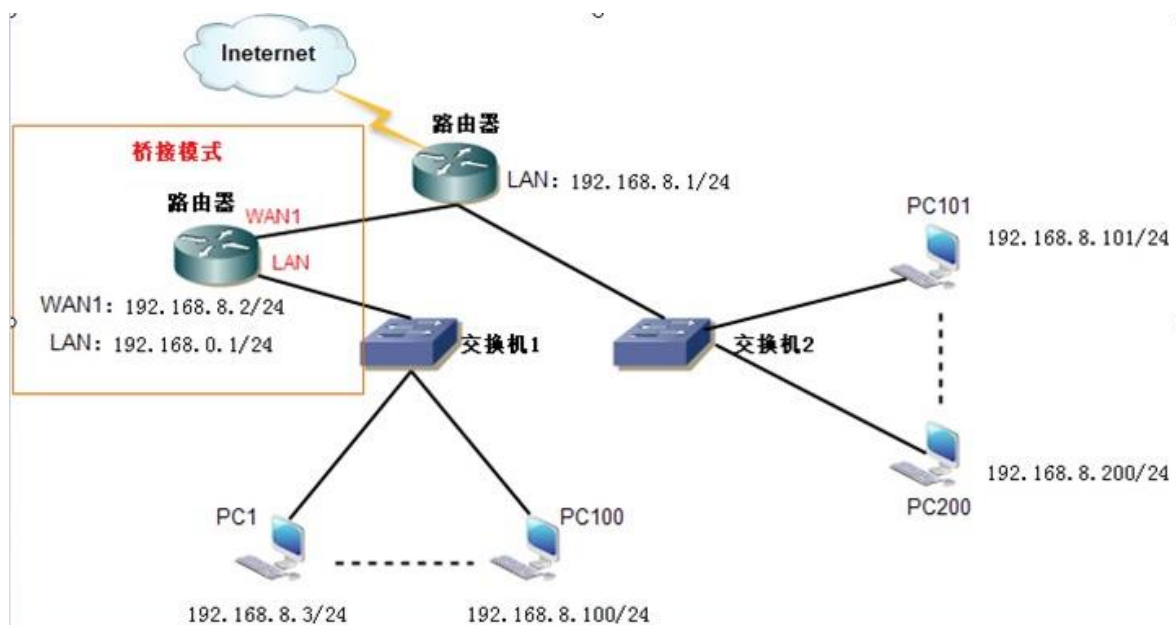
④透明桥：

透明桥顾名思义就是透明的意思，作了该设置后，路由器在网络拓扑中就相当于一根网线，对网络不会有结构上的影响，但其流控与行为管理功能还在。这种模式常用在主路由器不具备流控或行为管理功能，在想加入这些功能又不想换掉主路由器以及不想大范围改变内网用户电脑设置的情况。可加入此路由器作为二级路由，然后设置成透明桥模式。

以下面拓扑图为例：



上图的结构中,该网络所使用的网段为 192.168.8.0/24.现在把路由接到“交换机 1”的前面,WAN1 接入上层设备.如下图所示:



路由器设置如下图所示:

WAN口：	广域网1	▼
连接方式：	透明桥接	▼
IP地址：	192.168.8.2	
子网掩码：	255.255.255.0	
默认网关：	192.168.8.1	
连接检查间隔：	30	秒
内部主机范围：	必填	?
MAC地址：	40:80:00:10:86:D1	
	克隆	默认
	随机	
外网带宽：	上行 0	下行 0
	KByte (0 表示不设置)	
	带宽值参考	
DNS解析优先级：	<input type="radio"/> 高 <input type="radio"/> 默认 <input checked="" type="radio"/> 低	

透明桥可以用于测试路由的性能，也可以用在不改变网络结构情况下，加入一台路由做智能 QoS，行为管理等。

⑤局域网：

此功能是将一个广域网口设置成另一个 LAN 口来使用，从而实现设置多个局域网并端口隔离，局域网间不能互相通信。

WAN口：	广域网1	▼
连接方式：	局域网	▼
IP地址：	192.168.8.2	
子网掩码：	255.255.255.0	
连接检查间隔：	30	秒

我们的路由器默认有一个局域网是 192.168.0.x，通过选择**局域网**，可以把**广域网 1** 设置成另一个 LAN 口，且 IP 地址为 192.168.8.2，掩码为 255.255.255.0，这样就多了一个局域网 192.168.8.x，由于这两个局域网是端口隔离开的，所以不能相互通行。

⑥关闭线路：

当某个广域网口没被使用时，为了避免影响路由器性能，可以选择关闭线路来关闭该端口。如下图所示：

WAN口：	广域网1	▼
连接方式：	关闭	▼
连接检查间隔：	30	秒

- 第五步：点击下一步，将弹出远程访问以及登录路由器的帐号和密码设置界面，如下图所示：

远程访问：

远程访问端口：

8080

管理员：

admin

管理员密码：

管理员密码确认：

远程访问：如果您有需要对路由器进行远程访问，则可以开启此功能。只需要勾选远程访问选项即可。

远程访问端口：从外网访问路由器设置页面的端口号。可以修改为任意值，只要您设置的端口未被占用，且在 0~65535 范围内即可。外网访问路由器格式为“IP 地址：远程访问端口号”或“域名：远程访问端口号”。如“3322net.com:1234”。

管理员：登录并管理路由器的帐号。

管理员密码：登录并管理路由器的密码。

最后点击完成，则路由器及上网所需的基本设置已完成，可以上网了。

3、系统状态

打开左侧导航栏里的系统状态，可以查看路由器当前的工作状态和相关参数，如下图：



3.1 网络状态

网络状态：显示路由器局域网、广域网等基本配置信息。

首页 / 系统状态 / 网络状态

局域网信息										
MAC 地址: 40:80:00:10:86:D0			IP 地址: 192.168.2.1			子网掩码: 255.255.255.0				
广域网信息 刷新										
广域网口	MAC地址	连接类型	IP地址	子网掩码	网关	DNS	MTU	连接状态	连接时间	操作
WAN1	40:80:00:10:86:D1	DHCP	172.18.170.165	255.255.255.0	172.18.170.224	172.18.170.224, 202.106.0.20	1500	Connected	3 days, 04:01:26	刷新 重置

广域网信息：当前查看的广域网口全部信息。

MAC 地址：WAN 端口的 MAC 地址，设备出厂时由厂家所分配，可变换。

连接方式：该广域网口的连接方式为 DHCP 类型。

IP 地址：您接入 Internet 的 IP 地址。当前端口 **DHCP 成功**后，网络运营商会**分配 IP 地址**。

子网掩码：网络运营商提供的子网掩码。

网关：网络运营商提供的网关地址，即当地网络主机的 IP 地址。

DNS：用于对访问网站时所需要的域名进行解析，根据地区不同分配最优的 DNS 地址。

MTU：路由器所允许通过的最大数据单元。

连接状态：当前显示 Connected，表示已连接；若 Connecting 为正在建立连接；Disconnected 表示无连接。

连接时间：接入 Internet 后运行的时间长短

操作：左数第一个蓝色按钮为链接此线路；第二个红色叉按钮为断开此线路。

局域网信息

MAC 地址: 40:80:00:10:86:D0

IP 地址: 192.168.2.1

子网掩码: 255.255.255.0

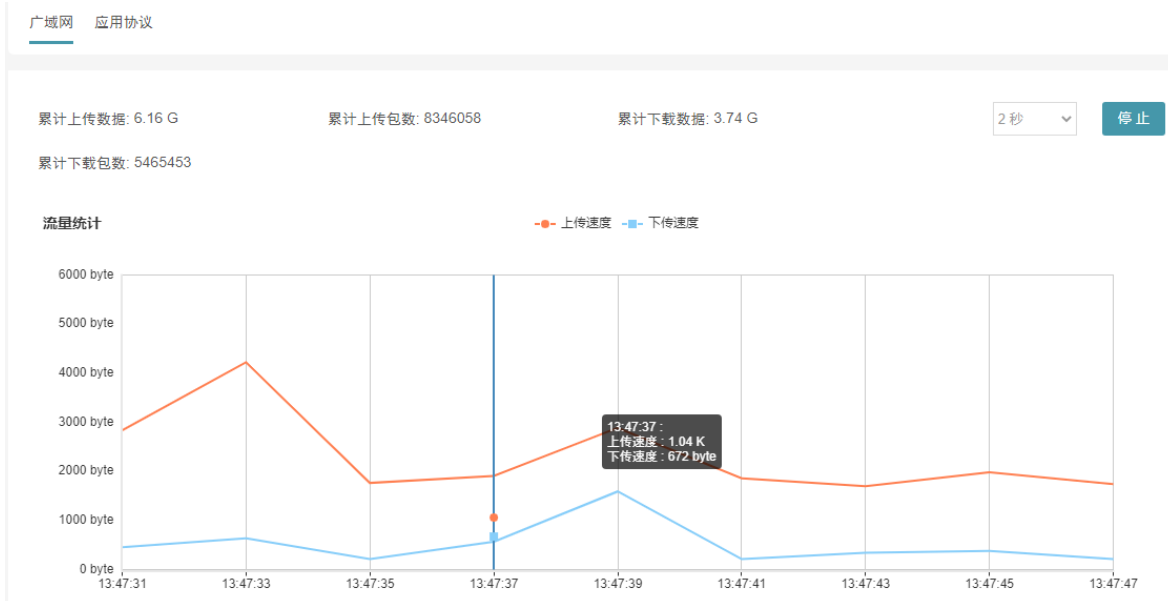
IP 地址：局域网口的 IP 地址，可以在内网配置中修改

子网掩码：与局域网口 IP 地址对应的掩码，可以在内网配置中修改

MAC 地址：局域网口的 MAC 地址出场时由厂家所分配，固定且唯一

3.2 流量分析

广域网



实时显示出口进出流量示意图，可根据自己需求的刷新时间进行刷新设置，如手动刷新，或 1 秒~30 秒的自动刷新设置。

应用协议

广域网 应用协议

上传总速度: 1.46 K 下载总速度: 383 b 上传总数据: 275.09 G 下载总数据: 278.82 G 刷新

应用协议	上传速度	下载速度	上传数据	下载数据	详情
HTTP协议	0 b 0%	0 b 0%	16.24 G 5.91%	40.32 G 14.46%	查看详情
网络游戏	0 b 0%	0 b 0%	133.66 M 0.05%	5.08 G 1.82%	查看详情
网络电视	866 b 57.69%	0 b 0%	197.88 G 71.93%	46.11 G 16.54%	查看详情
P2P下载	0 b 0%	0 b 0%	28.05 G 10.2%	9.95 G 3.57%	查看详情
常用协议	635 b 42.31%	383 b 100%	18.31 G 6.66%	68.98 G 24.74%	查看详情
即时通讯	0 b 0%	0 b 0%	562.16 M 0.2%	4.90 G 1.76%	查看详情
网络音乐	0 b 0%	0 b 0%	26.81 M 0.01%	338.67 M 0.12%	查看详情
股票交易	0 b 0%	0 b 0%	719.98 K 0%	2.16 M 0%	查看详情
网络电话	0 b 0%	0 b 0%	4.56 M 0%	106.41 M 0.04%	查看详情
流量代理	0 b 0%	0 b 0%	38.17 K 0%	29.33 K 0%	查看详情
数据库	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
移动应用	0 b 0%	0 b 0%	4.96 G 1.8%	81.69 G 29.3%	查看详情
特殊协议	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
未识别	0 b 0%	0 b 0%	8.91 G 3.24%	21.32 G 7.65%	查看详情

根据知名应用协议，以其上下行流量数据进行统计，同时显示相关协议实时速率情况，并可点击查看详情，根据大类查看具体应用。

上传总速度: 700 b

下载总速度: 0 b

上传总数据: 197.88 G

下载总数据: 46.11 G

[返回上一级](#) [返回顶部](#) [刷新](#)

应用协议	上传速度	下载速度	上传数据	下载数据	详情
PPTV	0 b 0%	0 b 0%	1.21 M 0%	22.70 M 0.05%	查看详情
PP加速器	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
PPS	700 b 100%	0 b 0%	7.42 G 3.75%	7.30 G 15.84%	查看详情
暴风影音	0 b 0%	0 b 0%	9.10 K 0%	3.55 K 0%	查看详情
风行	0 b 0%	0 b 0%	405.31 K 0%	10.66 M 0.02%	查看详情
uusee	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
百度影音	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
皮皮	0 b 0%	0 b 0%	188.20 K 0%	4.06 M 0.01%	查看详情
快播	0 b 0%	0 b 0%	1.96 G 0.98%	1.70 G 3.7%	查看详情
清点	0 b 0%	0 b 0%	333.04 K 0%	417.56 K 0%	查看详情
QQ直播	0 b 0%	0 b 0%	668.00 K 0%	141.87 K 0%	查看详情
极速播6	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
SopCast	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
VJBase/西瓜影视	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
搜狐电视直播	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
CNTV直播	0 b 0%	0 b 0%	44.66 K 0%	777.68 K 0%	查看详情
VideoSpeed	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
优酷影视	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
奇艺加速器	0 b 0%	0 b 0%	0 b 0%	0 b 0%	查看详情
迅雷看看	0 b 0%	0 b 0%	240 b 0%	96 b 0%	查看详情

3.3 主机监控

监控内网主机相关的信息，精确统计内网每个 IP 的上网时间、累计流量、实时速度、网络连接数等关键指标，并可以按任意指标排名分析；实时分析各 IP 的网络连接详情，轻松掌握网络资源分配情况，定位问题易如反掌。

[主机监控](#) [PPPoE用户](#) [DHCP用户](#) [聊天账号](#)

用户信息

IP地址

MAC地址

组名

请选择上网状态

查询

手动刷新

刷新

用户信息	姓名	组名	IP地址	MAC	上网时间	连接数	上传数据	下载数据	上传速度	下载速度	上网状态	操作
DESKTOP-4JBJO36			192.168.2.122	18:03:73:83:74:9C	4时31分38秒	ALL:264,TCP:25 UDP:239,ICMP:0	246.99 M	582.06 M	353 b	245 b	允许	<div></div>

另外，还可以针对某个 IP 点击[查看连接](#)和[详细信息](#)以更详细地了解当前用户的上网情况



➤ **查看连接：**用于查看当前用户网络使用协议情况。

协议	本地端口	远端IP	远端端口	运行时间	优先级	上传总数据	下载总数据	类型	接口	域名	控制	操作	
TCP	4566	172.217.160.78	443	11秒	中 中	264 b	0 b		WAN1		允许	允许	阻止
TCP	4565	172.217.160.78	443	11秒	中 中	264 b	0 b		WAN1		允许	允许	阻止
TCP	4564	172.217.160.74	443	16秒	中 中	330 b	0 b	HTTPS	WAN1		允许	允许	阻止
TCP	4563	192.168.2.1	80	17秒	中 中	0 b	0 b	普通网页	LAN		允许	允许	阻止
TCP	4562	192.168.2.1	80	17秒	中 中	0 b	0 b	普通网页	LAN		允许	允许	阻止
TCP	4561	192.168.2.1	80	17秒	中 中	0 b	0 b	普通网页	LAN		允许	允许	阻止
TCP	4560	192.168.2.1	80	17秒	中 中	0 b	0 b	普通网页	LAN		允许	允许	阻止
TCP	4557	216.58.200.234	443	21秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4556	172.217.27.138	443	21秒	中 中	330 b	0 b	HTTPS	WAN1		允许	允许	阻止
TCP	4555	216.58.200.234	443	21秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4554	192.168.2.1	80	33秒	中 中	0 b	0 b	普通网页	LAN		允许	允许	阻止
TCP	4553	172.217.160.74	443	40秒	中 中	330 b	0 b	HTTPS	WAN1		允许	允许	阻止
TCP	4552	172.217.160.74	443	42秒	中 中	330 b	0 b	HTTPS	WAN1		允许	允许	阻止
TCP	4551	216.58.200.234	443	1分1秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4549	216.58.200.234	443	1分3秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4547	216.58.200.234	443	1分12秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4546	216.58.200.234	443	1分12秒	中 中	330 b	0 b		WAN1		允许	允许	阻止
TCP	4519	111.206.25.157	443	3分42秒	中 中	50.77 K	34.42 K	HTTPS	WAN1		允许	允许	阻止
TCP	4518	40.100.2.114	443	3分47秒	中 中	9.66 K	8.19 K	HTTPS	WAN1		允许	允许	阻止
TCP	4228	108.177.125.188	443	32分13秒	中 中	3.82 K	6.91 K	HTTPS	WAN1		允许	允许	阻止

共: 268 条记录 当前: 1/14 页

上页123...14下页

➤ **详细信息：**用于查看当前用户的上网统计信息和防御信息等。

主机 192.168.2.122 的详细信息

上网时间:	4时33分4秒
当前连接数:	276
连接创建的总数:	7122
连接数限制:	all:3000 ; TCP:0;UDP:0;ICMP:0;OTHER:0
DDOS 防御:	all:500 ; TCP:0;UDP:0;ICMP:50;OTHER:50
上传数据总量:	247.11 M 数据包:633178个
下载数据总量:	582.08 M 数据包:620198个
当前上传需求流量:	2.02 K
当前上传分配流量:	2.02 K
当前下载需求流量:	375 b
当前下载分配流量:	375 b

3.4 DNS 缓存

DNS 缓存列表会记录下所有用户 DNS 最大老化时间内缓存的域名解析信息，超过时间的缓存信息将会自动老化掉。对某域名做过规则或该域名正被连续使用，将会加长老化时间。

域名	IP地址	查询				刷新
域名	IP地址	DNS组ID	DNS出口组ID	更新时间	老化时间	
wup.imtt.qq.com	111.206.25.146,123.126.122.26,111.206.25.147	未配置	未配置	6秒	7分8秒	
content-autofill.googleapis.com	172.217.160.74	国外应用	未配置	1分20秒	4分19秒	
wup.browser.qq.com	111.161.111.57,111.206.25.157	网页	未配置	1分21秒	8分43秒	
safebrowsing.googleapis.com	203.208.50.161	国外应用	未配置	1分55秒	1分56秒	
msg.qq.net	123.126.131.1,123.126.131.2,111.206.23.98	未配置	未配置	2分35秒	4分2秒	
android.clients.google.com	172.217.160.78,216.58.200.238,172.217.24.14	国外应用	未配置	2分52秒	4分54秒	
www.googleapis.com	172.217.160.74,172.217.27.138	国外应用	未配置	3分	4分33秒	
flux.hcdn.ppsstream.com	122.190.66.112,124.64.199.237	未配置	未配置	3分32秒	7分6秒	
flux.hcdn.qq.com	124.64.199.237,122.190.66.112	视频	未配置	3分32秒	6分25秒	
homeab2.secnr.com	205.159.223.111	未配置	未配置	5分28秒	10分	
homeab1.secnr.com	205.159.223.111	未配置	未配置	7分46秒	10分	
nj.lbcsp2p.baidu.com	112.80.255.122	网页	未配置	9分28秒	2分31秒	
pan.baidu.com	111.206.37.70	网页	未配置	12分35秒	4分45秒	
dns.weixin.qq.com	109.244.169.50,109.244.169.236,220.194.91.159	网页	未配置	16分2秒	1分53秒	
data6.video.qq.com	123.126.128.12,123.126.128.9,123.126.128.31	视频	未配置	27分33秒	9分47秒	
live.net.video.qq.com	111.202.75.22	视频	未配置	27分35秒	9分40秒	
liveheart.video.qq.com	111.206.13.22	视频	未配置	27分35秒	7分50秒	
policy.video.qq.com	111.202.74.191,111.202.74.192	视频	未配置	27分35秒	9分	
fp-vs-nocache.azureedge.net	117.18.232.200	未配置	未配置	28分19秒	10分	
update.pan.baidu.com	123.125.114.235	网页	未配置	29分30秒	2分1秒	

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

3.5 登录记录

显示管理登录路由器的记录，包括登录IP及登录时间，如下图所示：

登录IP	登录时间	登录用户
192.168.2.122	2020-09-30 13:09:37	管理员
192.168.2.122	2020-09-30 09:30:07	管理员
192.168.2.188	2020-09-27 18:56:59	管理员
192.168.2.188	2020-09-22 18:43:58	管理员
192.168.2.188	2020-09-15 14:21:00	管理员
192.168.2.188	2020-09-15 11:17:06	管理员
192.168.2.3	2020-09-14 13:49:24	管理员
192.168.2.180	2020-09-09 15:15:20	管理员
192.168.2.180	2020-09-08 17:08:13	管理员
192.168.2.170	2020-09-04 09:43:11	管理员
192.168.2.145	2020-08-31 10:17:48	管理员
192.168.2.133	2020-08-28 16:05:20	管理员

3.6 系统日志

系统日志

本界面显示系统日志、ARP 日志、流量攻击日志、DDOS 日志、PPPoE 日志、访问控制日志、策略路由日志、网址日志、URL 重定向日志、行为管理日志。如图：

日志分类：
☒ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

①系统日志：

日志分类：
☒ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

删除日志 导出日志 刷新

模块	时间	消息
syslog	Sep 30 02:39:51	Time Updated: Wed, 30 Sep 2020 02:39:49 +0800 [+1s]
syslog	Sep 30 03:39:52	Time Updated: Wed, 30 Sep 2020 03:39:51 +0800 [-1s]
syslog	Sep 30 05:40:04	Time Updated: Wed, 30 Sep 2020 05:40:02 +0800 [+1s]
syslog	Sep 30 06:39:58	Time Updated: Wed, 30 Sep 2020 06:39:57 +0800 [-1s]
syslog	Sep 30 07:39:59	Time Updated: Wed, 30 Sep 2020 07:39:57 +0800 [+1s]
syslog	Sep 30 08:40:00	Time Updated: Wed, 30 Sep 2020 08:39:59 +0800 [-1s]
syslog	Sep 30 09:38:11	dns_more_check start.

上图我们可以看到系统自动对时，更新时间信息；

②ARP 日志：

日志分类：
☐ 系统日志 ☒ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
0	08-31 11:20:21	主机192.168.2.138 的MAC地址从08-31-8B-56-DA-DC变成DA-A1-19-F4-15-A0
1	08-31 11:20:41	主机192.168.2.138 的MAC地址从DA-A1-19-F4-15-A0变成08-31-8B-56-DA-DC
2	09-07 09:26:56	主机192.168.2.107 的MAC地址从F8-9A-78-7B-2D-0B变成DA-A1-19-A7-20-05
3	09-07 09:27:07	主机192.168.2.107 的MAC地址从DA-A1-19-A7-20-05变成F8-9A-78-7B-2D-0B

上图显示的是 ARP 日志，管理员可通过该日志查看当前是否存在 IP 冲突、ARP 攻击记录等。

③流量攻击日志：

显示某时间段哪个 IP 地址流量暴增，主要针对内网用户进行监控；

日志分类:

☐ 系统日志 ☐ ARP 日志 ☒ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
0	09-22 10:10:45	广域网1: 在2秒中内收到102 KByte的数据包攻击!
1	09-22 10:10:47	广域网1: 在2秒中内收到211 KByte的数据包攻击!
2	09-22 10:10:49	广域网1: 在2秒中内收到161 KByte的数据包攻击!
3	09-22 10:10:52	广域网1: 在2秒中内收到110 KByte的数据包攻击!
4	09-22 10:10:54	广域网1: 在2秒中内收到270 KByte的数据包攻击!

④DDOS 日志：

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☒ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
0	07-03 14:37:16	局域网: 192.168.2.100 在5秒内发起1个数据包攻击, 成功拦截。
1	07-03 14:59:27	局域网: 192.168.2.100 在5秒内发起2个数据包攻击, 成功拦截。
2	07-09 11:42:02	局域网: 192.168.2.100 在5秒内发起1个数据包攻击, 成功拦截。
3	07-17 16:44:01	192.168.2.100 在2秒内发起579个连接攻击, 被禁止掉79个连接!
4	07-31 09:35:22	192.168.2.103 在2秒内发起734个连接攻击, 被禁止掉234个连接!
5	08-18 12:07:59	局域网: 192.168.2.110 在5秒内发起1个数据包攻击, 成功拦截。
6	08-26 17:32:10	局域网: 192.168.2.120 在5秒内发起1个数据包攻击, 成功拦截。

上图所显示的为当 2 秒内用户连接超过 100 个或 300 个时, 就禁止掉超出的, 并保留到下 2 秒执行;

⑤PPPOE 日志：

记录 PPPOE 用户的登录和下线时间。

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☒ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL 重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
----	----	----

⑥访问控制日志：

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☒ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
----	----	----

⑦策略路由日志：

记录策略路由里的策略规则执行的相关信息。

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☒ 策略路由日志 ☐ 网址日志 ☐ URL重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
0	07-07 10:46:00	广域网1: 侦测断网!
1	07-07 11:32:26	广域网1: 侦测断网!
2	07-21 10:53:40	广域网1: 侦测断网!
3	08-19 17:19:24	广域网1: 侦测断网!

⑧网址日志：

记录网址防火墙规则执行的相关信息。

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☒ 网址日志 ☐ URL重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
----	----	----

⑨URL 重定向日志：

记录网址转向规则执行的相关信息。

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☒ URL重定向日志 ☐ 行为管理日志

删除日志

编号	时间	事件
----	----	----

⑩行为管理日志：

记录软件过滤规则执行的相关信息。

日志分类:

☐ 系统日志 ☐ ARP 日志 ☐ 流量攻击日志 ☐ DDOS 日志 ☐ PPPoE 日志 ☐ 访问控制日志 ☐ 策略路由日志 ☐ 网址日志 ☐ URL重定向日志 ☒ 行为管理日志

删除日志

编号

时间

事件

4 网络基本配置

4.1 广域网配置

本界面用于配置 WAN 口的接口参数。四个 WAN 口都支持 5 种连接方式，包括 DHCP、静态地址线路，PPPOE 拨号线路，PPTP 设定、透明网桥。

连接类型:	<div> <div>自动获取IP</div> <div>自动获取IP</div> <div>PPPoE拨号上网</div> <div>河南网通 PPPoE</div> <div>静态IP</div> <div>透明桥接</div> <div>局域网</div> <div>关闭</div> </div>	批量导入PPPoE登录账号
MAC地址:		克隆 默认 随机
外网带宽:		带宽值参考
静态DNS:	<input type="text" value="0.0.0.0"/> <input type="text" value="0.0.0.0"/> <input type="text" value="0.0.0.0"/>	
线路侦测:	<input type="checkbox"/> 详细配置	
高级参数	<input checked="" type="checkbox"/>	
802.1X:	<input type="checkbox"/>	
MTU设置:	<div>默认参数</div> <input type="text" value="1500"/>	
工作模式:	<input checked="" type="radio"/> 网关模式 <input type="radio"/> 路由模式	
DNS解析优先级:	<input type="radio"/> 高 <input checked="" type="radio"/> 默认 <input type="radio"/> 低	
防御信息检测:	<div>不启用</div>	
运营商:	<input checked="" type="radio"/> 不设置 <input type="radio"/> 电信 <input type="radio"/> 网通 <input type="radio"/> 移动 <input type="radio"/> 教育网 <input type="radio"/> 长城宽带	
基于时间控制:	<input type="checkbox"/>	

以下着重介绍三种连接类型，其余类型可参考[配置向导](#)中关于六大类型的介绍。

➤ 静态 IP 地址接入的上网设定

连接类型:	<div>静态IP</div>	批量导入PPPoE登录账号
IP地址:	<div>172.18.170.165</div>	
子网掩码:	<div>255.255.255.0</div>	
默认网关:	<div>172.18.170.224</div>	
MAC地址:	<div>40:80:00:10:86:D1</div>	<div>克隆</div> <div>默认</div> <div>随机</div>
外网带宽:	<div>0</div> KByte(千字节)	<div>带宽值参考</div> ?
	<div>0</div> KByte(千字节)	
静态DNS:	<div>0.0.0.0</div>	?
	<div>0.0.0.0</div>	
	<div>0.0.0.0</div>	
线路侦测:	<div></div> <div>详细配置</div> ?	
高级参数	<div>▼</div>	
802.1X:	<div></div>	
MTU设置:	<div>默认参数</div>	<div>1500</div>
工作模式:	<div><input checked="" type="radio"/> 网关模式</div> <div><input type="radio"/> 路由模式</div>	?
DNS解析优先级:	<div><input type="radio"/> 高</div> <div><input checked="" type="radio"/> 默认</div> <div><input type="radio"/> 低</div>	?
防御信息检测:	<div>不启用</div>	?
运营商:	<div><input checked="" type="radio"/> 不设置</div> <div><input type="radio"/> 电信</div> <div><input type="radio"/> 网通</div> <div><input type="radio"/> 移动</div> <div><input type="radio"/> 教育网</div> <div><input type="radio"/> 长城宽带</div>	
基于时间控制:	<div></div>	

连接类型： 请选择“静态 IP 地址线路”；

IP 地址： 填入网络提供商提供给您固定 IP 地址；

子网掩码： 填入网络运营商提供给您相应子网掩码；

默认网关： 网络运营商提供给您外网网关；

DNS 服务器：填入网络供应商给您的 DNS 服务器地址（此地址由网络供应商提供，若不清楚，可以咨询当地网络供应商，索取 DNS 服务器地址）；

线路侦测：根据配线路侦测功能，在多 WAN 口线路使用时，会根据线路状态切换。

MTU 设置：选择默认参数；

工作模式：默认网关模式；（路由模式无法上网，需做 NAT 解析）

DNS 解析优先级：设置 DNS 解析的优先级。

运营商：选择该外线的网络提供方。

➤ **PPPoE 拨号接入的上网设定**

连接类型:	PPPoE拨号上网	批量导入PPPoE登录账号
用户名称:	<input type="text"/>	
用户密码:	<input type="password"/>	
MAC地址:	40:80:00:10:86:D1	克隆 默认 随机
外网带宽:	0 KByte(千字节)	带宽值参考 ?
	0 KByte(千字节)	
静态DNS:	0.0.0.0	?
	0.0.0.0	
	0.0.0.0	
线路侦测:	<input type="checkbox"/> 详细配置 ?	
高级参数	✓	
服务名称:	<input type="text"/>	
使用ISP指定的IP地址:	<input type="checkbox"/>	
获取指定的网关地址:	<input type="checkbox"/> 启用 <input type="text"/> <input type="checkbox"/> 更换MAC	
连接模式:	保持连接	
连接检查间隔:	30	秒
MTU设置:	默认参数	1480
工作模式:	<input checked="" type="radio"/> 网关模式 <input type="radio"/> 路由模式 ?	
DNS解析优先级:	<input type="radio"/> 高 <input checked="" type="radio"/> 默认 <input type="radio"/> 低 ?	
防御信息检测:	不启用 ?	
运营商:	<input checked="" type="radio"/> 不设置 <input type="radio"/> 电信 <input type="radio"/> 网通 <input type="radio"/> 移动 <input type="radio"/> 教育网 <input type="radio"/> 长城宽带	
基于时间控制:	<input type="checkbox"/>	

接入类型：使用 PPPoE 拨号接入网络，请选择“PPPoE 设定（ADSL 拨号用户）”；

用户名称：填入网络供应商提供给您的宽带账号；

用户密码：填入网络提供商提供给您的账号相应的密码；

服务名（可选）：用户可以自定义服务的名称，也可以不填；

工作方式：选择网关模式；（路由模式无法上网，需做 NAT 解析）

设置完成后点击“**提交设置**”。

➤ 透明网桥接入上网设定

连接类型:	<input type="text" value="透明桥接"/>	批量导入PPPoE登录账号
IP地址:	<input type="text" value="172.18.170.165"/>	
子网掩码:	<input type="text" value="255.255.255.0"/>	
默认网关:	<input type="text" value="172.18.170.224"/>	
内部主机范围:	<input type="text"/> ?	
MAC地址:	<input type="text" value="40:80:00:10:86:D1"/>	<input type="button" value="克隆"/> <input type="button" value="默认"/> <input type="button" value="随机"/>
外网带宽:	<input type="text" value="0"/> KByte(千字节)	<input type="button" value="带宽值参考"/> ?
	<input type="text" value="0"/> KByte(千字节)	
静态DNS:	<input type="text" value="0.0.0.0"/> ? <input type="text" value="0.0.0.0"/> <input type="text" value="0.0.0.0"/>	
线路侦测:	<input type="checkbox"/> 详细配置 ?	
高级参数	<input checked="" type="checkbox"/> 网关模式 <input type="checkbox"/> 路由模式 ?	
MTU设置:	<input type="text" value="默认参数"/> 1500	
DNS解析优先级:	<input type="radio"/> 高 <input checked="" type="radio"/> 默认 <input type="radio"/> 低 ?	
防御信息检测:	<input type="text" value="不启用"/> ?	
运营商:	<input checked="" type="radio"/> 不设置 <input type="radio"/> 电信 <input type="radio"/> 网通 <input type="radio"/> 移动 <input type="radio"/> 教育网 <input type="radio"/> 长城宽带	
基于时间控制:	<input type="checkbox"/>	

IP 地址：接入路由器 WAN 口的 IP 地址

默认网关：主干网网关

内部 IP 地址 1/2：接入路由器 LAN 口的 IP 地址组，与主干网相同网段

工作方式：选择网关模式（路由模式无法上网，需做 NAT 解析）

DNS:可填可不填，不填则使用默认 DNS

提示：设置完成后点击“提交设置”。

4.2 局域网设置

点击**网络配置—局域网设置**，将进入局域网设置的界面，可设置当前内网 LAN 口的 IP 地址(路由器登录 IP 地址)，如下图所示：

是否开启多LAN设置: ☐ 获取DHCP成功后自动绑定IP/MAC: ☐

LAN设置

IP地址:

子网掩码:

当前主机范围: 192.168.2.1-192.168.2.254

MAC地址:

DHCP管理方式: ☐ 关闭 ☒ 普通设置 ☐ 高级设置

开始地址:

结束地址:

释放时间: 秒

多子网段: ☐

注意：只有**全千兆路由器**才支持**多 LAN 多 DHCP 功能**

➤ 多 LAN 功能。启用后，如下图，选择不同的 LAN 口，填写不同的 LAN 内网信息

是否开启多LAN设置: ☒

获取DHCP成功后自动绑定IP/MAC: ☐

LAN设置

选择LAN口:

LAN1 LAN2 LAN3 LAN4 SSID1 5G_SSID1

IP地址:

192.168.2.1

子网掩码:

255.255.255.0

当前主机范围: 192.168.2.1-192.168.2.254

MAC地址:

40:80:00:10:86:D0

默认

随机

DHCP管理方式:

☐ 关闭 ☒ 普通设置 ☐ 高级设置

开始地址:

192.168.2.100

结束地址:

192.168.2.200

释放时间:

3600

秒

同时，多 LAN 还有划分 VLAN 功能

选择LAN口:

LAN1 LAN2 LAN3 LAN4 SSID1 5G_SSID1

IP地址:

192.168.2.1

子网掩码:

255.255.255.0

当前主机范围: 192.168.2.1-192.168.2.254

MAC地址:

40:80:00:10:86:D0

默认

随机

DHCP管理方式:

☐ 关闭 ☒ 普通设置 ☐ 高级设置

开始地址:

192.168.2.100

结束地址:

192.168.2.200

释放时间:

3600

秒

多子网段:

☐

VLAN设置

+

描述:

VLAN ID:

?

VLAN IP地址:

VLAN子网掩码:

255.255.255.0

填写相应的 VLAN ID、IP 地址、子网掩码、MAC（选择随机）、DHCP 地址池，完成全，添加，然后点击[页面右下角提交设置按钮](#)，重启后生效

- 获取 DHCP 地址后自动绑定 IP/MAC，启用后，客户获取的 IP 地址将全部绑定为静态 IP 地址

4.3 动态域名

Internet 上的域名解析一般是静态的，即一个域名所对应的 IP 地址是静态的，长期不变的。动态域名的功能，就是实现固定域名到动态 IP 地址之间的解析。因为 ADSL PPPoE 用户上网的时候分配到的 IP 地址都是动态的（每次重新拨号所获取的 IP 地址不同），用传统的静态域名解析方法，ADSL 用户想把自己上网的计算机做成一个有固定域名的网站，而有了动态域名就可以实现。用户可以申请一个域名，利用动态域名解析服务，把域名与自己上网的计算机联系在一起，这样就可以在很方便地搭建自己的网站。

智能路由器广域网口都提供动态 DNS 配置，其配置方法完全相同。动态域名客户端支持多种服务类型，可以参看“动态域名服务”中的列表数据。动态域名服务目前很多机构都有提供，某些还是免费的。

注意：动态域名功能的前提是路由器 WAN 口获取的 IP 地址为公网 IP，若获取的为私网 IP 或保留 IP，则功能不能生效。

那么，我们如何申请和设置动态域名呢？下面以**每步**动态域名为例，向大家详细地介绍：

第一步：点击**网络配置—动态域名**。



第二步：进入**动态域名**的设置界面后，点+号新增，申请**每步**动态域名。

首页 / 网络配置 / 动态域名

1

动态域名服务:

花生壳

3322 - 动态地址

3322 - 静态地址

DynDNS - 动态地址

DynDNS - 静态地址

DynDNS - 自定义

每步

确定

取消

用户名称:

用户密码:

编号

服务器名称

域名

第三步：点击 <http://www.meibu.com/>，申请每步动态域名。

每步科技

Meibu.com

塑造最贴心的互联网服务品牌

免费域名注册 公司资质 老版

服务热线: 0532-88862636

首页

免费二级域名

顶级域名注册

顶级域名转入

技术文章

软件下载

疑难解答

虚拟空间

汇款方式

用户登陆

类别: 请选择

忘记密码? PASSWORD?

用户名:

登陆密码:

☒ 登陆
 ☐ 注册

动态域名解析

Meibu二级域名动态域名解析永久免费使用！多台服务器同时工作，任何一台服务器的损坏不会影响用户的使用。是最稳定快速的服务。支持建立WEB服务、FTP服务、VPN远程控制、Email服务、游戏服务器、视频服务、硬盘录像机、网络摄像机、网上电台、数据动态传输、3G无线上网，支持泛域名解析，可转入其他公司国际域名。LINUX用户可用路由器登陆方式使用我们的服务。

异网端口映射：如果你用ADSL上网,你可以把这个电脑的端口映射到其它地方任何一个内网电脑的端口,你访问这台电脑就等于访问到其它地方的内网电脑,如果你其它地方的电脑在网通或有线宽带这样的网络,也可以实现外网访问了.利用异网端口映射可以访问任何内网的电脑而不需要去用别的服务器中转。

最新公告

- 1 异网端口映射不同内网映射
- 2 如何远程控制电脑远程桌面
- 3 支持网通或小区无公网IP用户
- 4 远程协助用户解决各种问题
- 5 设置ddwrt动态域名
- 6 免费域名升级为高级用户
- 7 如何检测公网和内网
- 8 用ADSL上网如何设置端口映射
- 9 如何提高alexa排名

在用户登录中，点击注册；

1、 每步网服务条款确认与接受
本协议是用户和每步网之间达成的整个动态域名服务条款。用户接受每步网提供的动态域名服务时，请在仔细阅读本章程后，按下“我同意”按钮，即表示用户与每步网达成协议并接受所有的服务条款。

2、 服务项目说明
每步网动态域名服务提供各种基于域名服务的别名映射和主机查找服务。
用户必须
(1)提供所有必须的网络连接设备，包括计算机和调制解调器；
(2)自己提供上网存取权限和相关上网费用。
用户应同意提供和维持本服务所要求的用户的完整、准确、最新资料。所有填写的信息将做为注册数据。
另外，每步网有权公开有关法律或合法处理所要求的用户注册信息和服务信息。
如果用户所供信息不真实，每步网有权中止会员资格和使用服务的权利。

3、 协议修改
每步网有权在必要时改变本协议的有关条款。每步网希望用户积极地确保对最新许可协议的认可，修改版及修改日期将被放在显著位置，此时本协议即告生效。用户对本服务的继续使用意味着对本协议和所修改的内容的认可。

4、 服务修改
每步网有权对免费用户修改或停止有关服务，可以通知或不通知用户。每步网在行使权利

监控用户：请购买磊科NR215P路由器(价格便宜)，内嵌最新每步动态域名协议，已有该路由器的用户请在我们的网站下载最新固件升级
磊科NR205+、NR215P路由器，可以支持解析网通、移动、广电有线宽带等网络的IP地址，可以帮助这类用户使用动态域名服务，新版本则支持解析电信、网通等用户。本站均提供升级下载

注意：如果你的路由器里没有内嵌我们的服务，申请完域名一定要下载客户端软件运行，下载软件登陆后即可生效，不需要另外做设置
每步科技动态域名解析独特技术使该服务永不掉线，如果你的设备或软件需要嵌入该服务，联系我们，我们可无偿协助你解决

有磊科下列型号路由器的交费用户，在使用申请的域名登陆的时候，可以同时得到 meibu.org 为后缀的二级域名的同步解析
NR205+、NR215P、NR235W、NR286 其它型号在陆续更新协议，有磊科路由器的用户请关注我们网站，会第一时间提供新固件的下载

威百仕网络提供免费的远程开机服务，无论内网外网电脑都能远程控制开机启动，甚至用手机也可以控制。点此访问

* 申请域名 .

* 密码

* Email

* 输入附加码 47394 图片看不清？点击重新得到

公司或姓名

固定电话

QQ或MSN

地址

注意：顶级域名转入点这里(可自由转入国际国内各种域名，即开即通) [申请顶级域名] 顶级域名注册费：**60元/年**，。顶级域名静态解析永久免费，顶级域名动态解析费180元/年。一次交三年送一年，一次交五年，永久免费动态解析(可50元购买一台NR215P路由器，汇款前请联系我们确认)
密码可使用任何英文字母及阿拉伯数字组合，不得少于4个字符，并区分英文字母大小写。例如：**JohN123DoLe**。
此处输入您的有效电子邮箱地址，否则无法提供有效服务。



机票预订
www.xbqclub.com
☎ 13585619903

填写必要的信息，填好后点击**提交设置**；

VBScript

恭喜您注册成功！您的域名是 yyzhong123.meibu.com 在您的主机上运行客户端输入完整域名后即可访问。在线QQ： 304045641 290377866

点击**提交**后，出现此对话框，说明域名申请成功。

第四步：在路由器上设置动态域名，依次填写内容完毕后，然后点击**添加**按钮；

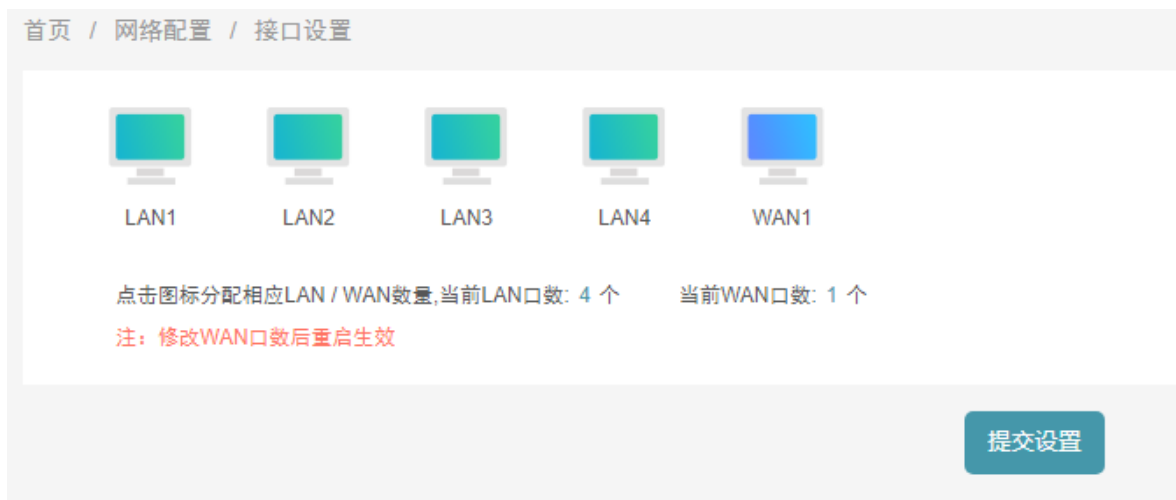
4.4 接口设置

点击**网络配置—接口设置**，我们可以对路由器端口进行、WAN/LAN 口数量设置修改：

路由器的 WAN 口为弹性端口，可以通过设置使网络接口在 WAN 口和 LAN 口中互相转换（顺序由左至右）该设置在设备重启后生效。

提示：路由器固有的 LAN 口不能修改为 WAN 口。

第一步：直接点击端口图标切换 **LAN/WAN 口数设置**选项卡，并设置对应端口的 LAN\WAN 口定义；



第二步：重启设备，设置生效。

①点击左边导航条的**系统维护-系统控制-重启路由器**；



②点击**重启路由器**按钮，重启完后，设置生效。



5 智能流控

5.1 优先级设置

优先级设置是以协议为前提，根据内网用户实时的带宽需求动态智能地为每个用户分配足够的带宽，满足其上网需求的同时，保证内网用户自定义协议的优先级顺序浏览网页不卡、视频以及游戏畅顺，从而提高上网质量。

具体设置如下所示：

第一步：点击**智能流控**—点击+号添加规则；



第二步：配置相关内网用户组及自定义应用协议。

状态: ☒

描述:

执行顺序: ?

应用协议: 取消选择

自定义IP协议: 取消选择

包含关系: ☒ 全部 ☐ 部分

高级参数: ☒

全局优先级: ☐ 高 ☒ 中 ☐ 低 ?

局部优先级: ☐ 高 ☒ 中 ☐ 低

用户组: ? 查看用户组

广域网的选择: ?

基于时间控制: ☐

5.2 应用协议分组

本次更新了 QOS 版本, 采用更加灵活直观的方式, 鼠标点击应用协议分类, 选取相应协议应用即可。(如可以点击协议大类或选择下一级找到指定的知名应用)

协议导航:全部协议

协议导航:全部协议>移动应用>手机APP|返回上一级

请输入名称查询

查询

请输入名称查询

查询

选中	协议	下一级
<input type="checkbox"/>	HTTP协议	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	网络游戏	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	网络电视	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	P2P下载	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	常用协议	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	即时通讯	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	网络音乐	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	股票交易	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	网络电话	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	流量代理	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	数据库	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	移动应用	<input checked="" type="radio"/> 下一级

<input type="checkbox"/>	嘀嗒拼车	
<input type="checkbox"/>	百度翻译	
<input type="checkbox"/>	汽车报价大全	
<input type="checkbox"/>	中关村在线	
<input type="checkbox"/>	WIFI分享	<input checked="" type="radio"/> 下一级
<input type="checkbox"/>	韵达快递	
<input type="checkbox"/>	顺丰速运	
<input type="checkbox"/>	EMS	
<input type="checkbox"/>	360搜索	
<input type="checkbox"/>	it007	
<input checked="" type="checkbox"/>	抖音	
<input checked="" type="checkbox"/>	快手	
<input checked="" type="checkbox"/>	火山小视频	

自定义 IP 应用协议：根据应用所使用的 IP/TCP/UDP 相关协议端口自行定义特征

自定义IP协议

远端地址范围选择

不选择

远端地址范围[基于IP]

-

添加

(可以为空)

删除

协议

TCP

内部端口:

 -

外部端口:

 -

添加

(为空表示所有协议和端口)

5.3 带宽限速

带宽限速主要针对于需要单独限制内网中一台或多台主机以及不同协议的上传和下载速度，是最常用的限速功能。

状态: ☒

描述:

控制方式: ☒ 单独限制 ☐ 共享限制 ?

应用协议:

自定义IP协议:

包含关系: ☒ 全部 ☐ 部分 ?

上传速度: KB ?

下载速度: KB ?

高级参数: ☒

用户组: ?

广域网的选择: ?

基于时间控制: ☐

状态：规则的开启或关闭

描述：对这条规则的备注

控制方式：单独表示对单个 IP，共享限制表示对整体 IP

应用协议：针对应用分组上面的分组限速

自定义 IP 协议：针对自定义应用分组上面的分组限速

包含关系：针对协议的全部或部分，默认使用全部，针对部分限速不准确

上传速度：需要限制的最大上传速度

下载速度：需要限制的最大下载速度

用户组：可以设置单个 IP 或一段 IP 段等自定义 IP 地址组

广域网选择：选择相应的外网端口，不选择表示全部

基于时间控制：设置规则的使用时间段

选择上诉所需要控制的条目并填写需求，如果某一条目留空则表示限制该条目下所属的所有的因素。注：描述不可以为空。

5.4 带宽保证

带宽保证可以实现保障内网中一台或多台主机使用一定量的带宽的功能。实现进一步细致优化网络。

状态: ☒

描述:

控制方式: ☒ 独占带宽 ☐ 共享带宽 ?

应用协议: 取消选择

自定义IP协议: 取消选择

包含关系: ☒ 全部 ☐ 部分 ?

上传速度: KB ?

下载速度: KB ?

高级参数:

用户组: ? 查看用户组

广域网的选择: ?

基于时间控制: ☐

确认 取消

状态：规则的开启或关闭

描述：对这条规则的备注信息或名称

控制方式：独占带宽表示为每个主机单独保证填写的带宽速度；共享带宽表示为填写的所有主机共享所使用的带宽速度。

应用协议：针对应用分组上面的分组限速

自定义 IP 协议：规则对外的 IP、域名或端口等

包含关系：针对协议的全部或部分，默认使用全部，针对部分限速不准确

上传速度：需要保证可使用的最大上传速度

下载速度：需要保证可使用的最大下载速度

用户组：可以设置单个 IP 或一段 IP 段等自定 IP 地址组

广域网选择：选择相应的外网端口，不选择留空表示全部

基于时间控制：设置规则的使用时间段

选择上诉所需要控制的条目并填写需求，如果某一条目留空则表示限制该条目下所属的所有的因素。注：描述不可以为空。

5.5 控制例外

该功能可以对外部服务器的访问限制排除在外，不受智能 QOS 的控制。访问该服务器的流量将不会在主机监控、流量分析里显示出来。

控制例外

流量控制例外(基于外部IP): ?

流量控制例外(基于协议): ?

流量控制例外(基于内部IP): ?

如果有些外部服务器或者内部主机，访问他的流量不受接入带宽的限制，那么就需要设置这样的例外
该功能一般用于局域网中个别特殊主机或对某些特殊协议或目的地址等;没有特殊情况不建议使用该功能

提交设置

取消设置

6 行为管理

对内网用户的上网行为进行管理控制，常用应用程序的封锁限制、网页及

关键字的过滤与限制，以及对域名的重定向。

6.1 用户组

首页 / 行为管理 / 用户组

—

名称:

IP地址范围:

确定

取消

ID	名称

浏览

导入用户组信息

导出用户组

删除所有用户组

名称：添加用户名称，用于管理员区分。

IP 地址范围：用户对应的单个 IP 地址或是一端 IP 地址。

6.2 行为识别

用于对指定范围的内部主机进行应用协议上的管控，允许或者禁止指定协议的通过。

点击**行为管理**—行为识别，即可进入设置界面：



为了方便对内网不同类型用户做行为管理，我们可以在用户组里添加 IP 组，如下图所示：



- ①创建 IP 组名；
- ②网该 IP 组添加 IP 地址；
- ③点击添加按钮，即可创建 IP 组，新建组将会添加在下面栏目里。

—

名称:

IP地址范围:

确定

取消

ID

名称

6.3 行为识别

用于对指定范围的内部主机进行应用协议上的管控, 允许或者禁止指定协议的通过。

访问控制的方式: ☐ 关闭 ☒ 允许规则之外的通过 ☐ 禁止规则之外的通过 ?

规则编辑

—

状态:

描述:

控制方式:

☒ 允许 ☐ 阻止

执行顺序:

30000

?

用户组:

查看用户组 ?

应用协议:

取消选择

自定义IP协议:

取消选择

日志:

基于时间控制:

确定

取消

访问控制的方式: 对设定规则的启用与否的按钮。

关闭: 即设置的规则不启用。

允许规则之外的通过：即除了设置的规则内的，其余的都能通过。

禁止规则外的通过：即除了设置的规则内的，其余的不能通过。

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：对该条规则的简单描述。

控制方式：允许和禁止。对该条规则的控制方式，选择允许或者禁止规则的协议通过。

执行顺序：规则与规则之间的执行顺序值，值越大的越被优先读取执行。

用户组：填入您需要管控的内部主机地址范围。

应用协议：选择您需要管控的协议类型。

自定义协议：选择自定义您需要管控的协议类型。

日志：对于匹配上的数据包，进行日志记录。

基于时间控制：是否启动按时间段管控功能。（若启用，规则将只会在您自定义的管控时间段内生效，默认不启用，表示所有时间段都生效。您可以设置一周的哪几天生效，也可以设置一天的哪些时段生效。）

6.4 高级管理

本界面主要用于对 WEB 页面认证相关参数的设定。

6.4.1 关键字过滤

该功能是禁止用户在网页中搜索指定的关键字功能，用于屏蔽一些敏感词汇，类似于论坛里的过滤敏感字功能。（注意：该功能仅对非 Https 访问的搜索引擎生效）

WEB关键字过滤 禁止WEB提交 后缀名过滤

控制状态: ☒ 日志: ☐ 弹出警告提示: ☒

一

状态: ☒

描述:

被过滤关键字:

状态	描述

控制状态：选择是否启用关键字过滤功能。

日志：是否记录规则执行产生的日志。

弹出警告提示：选择开启，表示在访问被过滤的关键字时，会弹出“您访问的内容被管理员阻止”的警告提示。

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：给该规则命名备注，便于识别。

被过滤关键字：要禁止搜索的关键字，支持中文、英文跟数字字符。

6.4.2 禁止 WEB 提交

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

WEB关键字过滤

禁止WEB提交

后缀名过滤

控制状态:

☒ 关闭 ☐ 允许规则之外的通过 ☐ 禁止规则之外的通过

提交

—

状态:

☒

描述:

主机IP地址范围:

日志

☒

基于时间控制:

☐

确认

取消

控制状态：分别有关闭、允许规则之外的通过、禁止规则之外的通过三种状态。

关闭：该功能不生效。

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

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

状态：使该规则生效。

描述：给该规则命名的备注信息，便于识别规则。

主机 IP 地址范围：表示该规则中对内网哪些用户生效。

日志：选择是否开启记录日志，开启后设定将记录在日志中，便于查看。

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

6.4.3 后缀名过滤

该功能是禁止/允许客户机访问网络上带有规则中指定的后缀名的文件。

WEB关键字过滤
禁止WEB提交
后缀名过滤

控制状态:
☒ 关闭
☐ 允许规则之外的通过
☐ 禁止规则之外的通过

弹出警告提示:
☒

提交

-

状态:
☒

描述:

主机IP地址范围:

后缀名:

☐ exe
☐ bat
☐ rar
☐ zip
☐ arj
☐ txt
☐ doc
☐ docx
☐ dot
☐ xls
☐ xlsx
☐ ppt
☐ pptx
☐ wps
☐ rtf
☐ pdf
☐ wav
☐ mp3
☐ ram
☐ rm
☐ avi
☐ mpg
☐ swf
☐ fla
☐ gz

☐ 全选
☐ 全不选
☐ 反选

手动输入后缀名:

日志
☒

基于时间控制:
☐

控制状态：分别有关闭、允许规则之外的通过、禁止规则之外的通过三种状态。

关闭：不启用该功能。

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

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

弹出警告提示：选择开启，表示在访问过滤的后缀名时，会弹出“您访问的内容被管理员阻止”的警告提示。

状态：是否选择设定规则生效。

描述：给该规则命名的备注，便于识别。

主机 IP 地址范围：填入需要管控的 IP。

后缀名：勾上即表示该规则对勾上的后缀名生效。

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

日志：选择是否开启记录日志，开启后设定将记录在日志中，便于查看。

基于时间控制：您可以设置自定义时间段，让规则在指定的时间段内才生效。默认不设置表示所有时间段都生效。（每周：您可以设置一周的哪几天生效； 每天：您可以设置一天的哪些时段生效）

6.5 邮件监控

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

6.5.1 邮件监控

首页 / 行为管理 / 邮件监控

邮件监控 邮箱白名单 WEB邮箱过滤 WEB邮箱白名单

状态: ☒ 接收邮箱:

确认

开启：开启邮件监控功能。

接收邮箱：填入监听邮箱地址。

6.5.2 邮箱白名单

对于白名单内的邮箱，将不会受到邮件监控功能的监管。（也就是白名单内的邮箱在发送邮件时，将不会抄送邮件至您填写的接收邮箱）。

首页 / 行为管理 / 邮件监控

邮件监控 邮箱白名单 WEB邮箱过滤 WEB邮箱白名单

监控状态:



接收邮箱:

白名单状态:



提 交



描述:

邮箱地址:

确 认

取 消

状态：选择是否启用邮件白名单功能。

描述：对本规则进行简单描述备注。

邮箱地址：填入不受邮件监控功能监管的邮箱地址。

6.5.3 WEB 邮箱过滤

此功能即网址防火墙，默认添加了邮箱过滤功能，您在此处添加的规则将会同步在网址防火墙里面显示出来，管控效果也是一样的。

邮件监控 邮箱白名单 WEB邮箱过滤 WEB邮箱白名单

过滤方式: ☒ 关闭 ☐ 允许规则之外的通过 ☐ 禁止规则之外的通过

弹出警告提示: ☒

提 交

—

状态: ☒

描述: mail

动作: ☒

执行顺序: 30000 ?

主机IP地址范围: 全部用户 ?

日志 ☐

基于时间控制: ☐

确 认

取 消

网址过滤方式：过滤方式有三种。

关闭：关闭访问控制功能，列表中的所有规则将都不生效。

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

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

填出警告提示：选择开启，表示在打开被禁止的页面时，会弹出“您访问的内容被管理员阻止”的警告提示。

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：对该条规则的简单描述。

动作：规则的管控方式，该规则为允许通过还是禁止通过。

执行顺序：规则与规则之间的执行优先等级，值越大的越被优先执行。

主机 IP 地址范围：您需要管控的内部主机地址范围。

日志：对于匹配上的数据包，进行日志记录

基于时间控制：是否启动按时间段管控功能（若启用，规则将只在设置的时间范围内生效。默认为空，表示所有时间段都生效）。

6.5.4 WEB 邮箱黑白名单

添加到白名单里面的邮箱将不会受到网址防火墙（WEB 邮箱过滤）的限制。

首页 / 行为管理 / 邮件监控

邮件监控 邮箱白名单 WEB邮箱过滤 WEB邮箱白名单

—

描述:

邮箱地址: ?

确 认 取 消

描述：对该条规则的简单描述。

邮箱地址：填入您需要排除限制的 WEB 邮箱地址。

6.6 网址管理

6.6.1 网址分类组

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

id	名称	类型	操作
5	军事	系统创建	+ -
4	时事论坛	系统创建	+ -
3	网络电视	系统创建	+ -
2	视频	系统创建	+ -
1	新闻	系统创建	+ -
6	网络游戏	系统创建	+ -
7	音乐	系统创建	+ -
9	小说	系统创建	+ -
10	网游	系统创建	+ -
12	财经	系统创建	+ -
13	交友	系统创建	+ -
15	银行	系统创建	+ -
16	体育	系统创建	+ -
18	手机	系统创建	+ -
19	汽车	系统创建	+ -
20	男性	系统创建	+ -
21	女性	系统创建	+ -
23	彩票	系统创建	+ -
24	实用查询大全	系统创建	+ -
25	天气	系统创建	+ -

共: 63 条记录 当前 1/4 页 [上页](#) [1](#) [2](#) [3](#) [4](#) [下页](#)

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

6.6.2 网址数据库

该页面可以往指定的分组里添加域名信息，用于完善已有的分组或者新添加的分组。

首页 / 行为管理 / 网址管理

网址分类组 网址数据库 网址防火墙 日志

标识:

所属组:

网址地址:

标识 所属组 网址地址

同时您还可以将已有的网址分类信息导入路由或者导出备份，如图所示：

6.6.3 网址防火墙

网址过滤功能可以自定义设置规则用来控制用户对网页的访问，如下图所示：

[网址分类组](#)
[网址数据库](#)
[网址防火墙](#)
[日志](#)

过滤方式:
 ☒ 关闭
 ☐ 允许规则之外的通过
 ☐ 禁止规则之外的通过

弹出警告提示:
 ☒

提交

—

状态:
 ☒

描述:

动作:
 ☒

执行顺序:

?

主机IP地址范围:

?

网站地址组:

?

日志
 ☐

基于时间控制:
 ☐

确认
 取消

网址过滤方式：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式。

不启用：就是对列表中的规则不做任何控制，规则不会生效。

允许规则之外的通过：列表之外的规则允许通过，列表之中的规则受规则控制。

禁止规则之外的通过：规则之外的所有都不允许通过，规则之内的受规则管控。

弹出警告提示：选择开启，表示在打开被禁止的页面时，会弹出“您访问的内容被管理员阻止”的警告提示。

状态：是否启用该规则。

描述：对规则的一个描述。

动作：该规则为允许通过还是禁止通过。

执行顺序：规则的执行优先等级。

主机 IP 地址范围：所受限制的 IP

网站地址组：选择您要控制的网址分类组。

日志：是否在日志中记录该规则的发生情况。

基于时间控制：是否启用按时间段来控制规则生效。

6.5.4 日志

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



6.7 域名管理

主要是对域名解析、过滤、重定向。

6.7.1 域名解析

域名特殊解析主要是用来将一些特定的域名绑定到指定的线路上去解析。如图所

示:



DNS 域名：需要绑定到线路上的域名或者域名关键字。

出口选择：选择一个广域网的接口用来解析指定的域名。

6.7.2 域名过滤

域名过滤主要是用于对一些域名或者域名关键字进行阻止。



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

关闭：就是对列表中的规则不做任何控制，规则不会生效。

允许规则之外的通过：列表之外的规则允许通过，列表之中的规则受规则控制。

禁止规则之外的通过：规则之外的所有都不允许通过，规则之内的受规则管控。

DNS 域名：添加所需过滤的域名或者域名关键字。

6.7.3 域名重定向



域名解析 域名过滤 域名重定向

—

DNS 域名:

重定向到:

添加 取消

DNS 域名：填入被转向的域名，不支持通配符 *。

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

6.8 URL 重定向

6.8.1 URL 重定向

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

URL重定向 日志

—

状态：

描述：

default

URL的主机名称：

相同

?

目录网页(URL)：

全部

?

网页的参数：

全部

?

重定向到：

?

主机IP地址范围：

?

被重定向置尾：

?

日志

基于时间控制：

确 认

取 消

状态：选择是否激活应用此规则。

描述：对该条规则的简单描述。

URL 的主机名称：填入您需要被转向的域名地址。

目录网页（URL）：填入被转向域名的目录网页，若没有，则可不填。

网页的参数：填入被转向域名的网页参数，若没有，则可以不填。

重定向到：需要被转向到的域名地址。

主机 IP 地址范围：内部需要被重定向的主机 IP 地址。

日志：是否需要在日志中显示记录。

基于时间控制：启用则规则只在设定的时间段内生效。

6.8.2 日志

该功能是用来记录 URL 重定向中勾选日志的规则匹配记录。



7 认证管理

7.1 基本设置

用户上网控制主要用于对用户上网的方式做控制，如图所示：

首页 / 认证管理 / 基本设置

用户上网方式控制:	<input checked="" type="checkbox"/>
允许上网的方式:	<input type="checkbox"/> ARP绑定用户直接上网 <input type="checkbox"/> PPPoE用户直接上网 ?
高级参数	▼
用户帐号到期提前通知:	<input type="text" value="7"/> 天
用户帐号到期查询间隔:	<input type="text" value="0"/> 分 ?
不需要认证的内部主机:	<input type="text" value="基于IP"/> ?
不需要认证的内部主机:	<input type="text" value="基于MAC"/> ?
允许访问的外网范围:	<input type="text" value="基于IP"/> ?
允许访问的外网范围:	<input type="text" value="基于域名"/> ?
会话存活超时时间:	<input type="text" value="0"/> 分钟 ?
MAC自动认证老化时间:	<input type="text" value="48"/> 小时 ?
接口免认证:	<input type="checkbox"/>
保存本地认证日志到U盘:	<input type="checkbox"/> ?
包时用户定时重设时长:	<input type="checkbox"/>

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

允许上网的方式： 选择允许用户上网的认证方式。

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

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

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

用户帐号到期查询间隔： 此功能用于检测帐号到期但仍持续在线的用户，

在帐号到期以后，达到设置的时间之后，在线用户将被强制踢下线，避免了因为到期用户长期不下线导致的带宽资源浪费。此值可以尽量设置大一点，效果更佳。

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

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

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

允许访问的外网范围(基于域名)：没有进行认证的用户也能访问的外网域名。

接口免认证：可对指定接口免认证，如有线、无线接口

7.2 页面管理

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

首页 / 认证管理 / 页面管理

帐户到期提前通知页面

查看当前“帐户到期提前通知页面”

使用默认“帐户到期提前通知页面”

下载“帐户到期提前通知页面”模板

重新提交通告文件“帐户到期提前通知页面”:

浏览

提交

阻止上网的通告页面

查看当前“阻止上网的通告页面”

使用默认“阻止上网的通告页面”

下载“阻止上网的通告页面”模板

重新提交通告文件“阻止上网的通告页面”:

浏览

提交

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

阻止上网的通告页面：在开启了认证后，没有认证的用户将会收到此通告文件的提醒；开启了 web 认证则弹出 web 认证页面。

7.3 PPPoE 设置

PPPoE 全称 Point to Point Protocol over Ethernet，意思是基于以太网的点对点协议。实质是以太网和拨号网络之间的一个中继协议，所以在网络中，它的物理结构与原来的 LAN 接入方式没有任何变化，只是用户需要在保持原接入方式的基础上，安装一个 PPPoE 客户端（这个是通用的）。之所以采用该方式给小区计时/计流量用户，是方便计算时长和流量。此类用户在使用上比包月用户增加了 PPPoE 虚拟拨号的过程。电信的 ADSL 接入也是需要安装使用 PPPoE。

以下介绍如何设置 PPPoE 服务，如下图所示：

PPPoE Server状态:	<input type="checkbox"/>	
允许任意服务器名接入:	<input type="checkbox"/>	
PPPoE 服务器名字:	<input type="text" value="dlink-PPPoE"/>	?
PPPoE 服务器的地址:	<input type="text" value="10.0.0.1"/>	
PPPoE 服务器的子网掩码:	<input type="text" value="255.255.255.0"/>	
高级参数:	<input checked="" type="checkbox"/>	
只允许使用PPPoE接入:	<input type="checkbox"/>	?
首选 DNS 服务器:	<input type="text" value="0.0.0.0"/>	?
备份 DNS 服务器:	<input type="text" value="0.0.0.0"/>	?
空闲检测时间:	<input type="text" value="3"/> 秒	?
多少个检测请求未应答则断开连接:	<input type="text" value="3"/>	?
认证方式:	<input checked="" type="checkbox"/> 不用加密的密码(PAP) <input type="checkbox"/> 质询握手身份验证协议(CHAP) <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2	
任意账号登录:	<input type="checkbox"/>	?
<input type="button" value="提交设置"/> <input type="button" value="取消设置"/>		

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

PPPoE 服务器名字：拨号服务器的名称，用户可以自定义更改。

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

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

首选 DNS 服务器：PPPOE 服务器分配给客户机的 DNS 服务器地址。

备份 DNS 服务器：PPPOE 服务器分配给客户机的 DNS 服务器地址。

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

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

认证方式：对于不同应用环境，可以采取不同的认证方式类型。对于一

般 PC 电脑，都是采用的 PAP 模式。如果是采用下级路由进行拨号，可以把所有的认证方式都勾选上。

7.4 用户管理

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

定时删除未锁定的用户: ☐ 每周: 每天:

用户状态: ☒ 锁定

用户名:

密码:

MAC地址:

到期:

登录用户数:

起始IP地址:

结束IP地址:

速度设置: [参考速度设置](#)

姓名:

电话:

备注:

身份证:

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

用户名/密码：为用户创建一个登录的登陆用户名及密码。

MAC 地址：有不绑定、自动绑定、手动绑定 3 种形式可供选择。

到期：可以对用户的上网期限进行限定。有按日期、包时、包流量。

IP 地址:用于手动给用户指定 IP 地址。PPPoE 用户手动绑定的 IP 为 PPPoE 拨号服务器 IP，Web 认证可以选择自动绑定 IP 和手动绑定 IP。

上传速度：限制账户网页上传速度，0 为无限制。

下载速度：限制账户下载视频资料等速度，0 为无限制。

登录用户数：对登录数量进行设置。

备注：对此用户的简单描述，方便管理员进行查看管理。

用户信息备注：以便对用户信息的记录。

8 防御配置

8.1 ARP 管理

8.1.1 ARP 列表

ARP 列表显示当前局域网连接用户的 IP 及 MAC 信息。

ARP列表

ARP防御

日志

+?

描述

IP地址

MAC地址

接口

类型

状态

查询

刷新

描述	IP地址	MAC地址	接口	类型	状态	提示	操作
	192.168.0.60	F8:9A:78:B2:D0:B	局域网	动态	正常		静态 唯一 免认证
	192.168.0.54	A0:C9:A0:90:06:B7	局域网	动态	正常		静态 唯一 免认证
	192.168.0.59	DC:37:14:6D:CC:9F	局域网	动态	正常		静态 唯一 免认证
未知	192.168.0.58	DC:F0:90:B1:F7:DB	局域网	动态	正常		静态 唯一 免认证
DESKTOP-4JBJO36	192.168.0.51	C0:D9:62:FA:B5:C5	局域网	动态	正常		静态 唯一 免认证

唯一：指只有 IP 和 MAC 地址对应才能连接网络。

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

描述：对该条绑定信息的简单文字描述，便于管理员区分。

IP 地址：填写需要绑定的 IP 地址。

MAC 地址：输入您要进行 ARP 绑定的 MAC 地址，可以通过“查询 MAC”来设置 MAC。如果用户不在线则需要手动输入。

8.1.2 ARP 防御

用于设定 ARP 主动防御的相关参数。

防御“LAN 口伪网关攻击”：防御常用的 ARP 攻击软件！如“网络执法官”、“P2P 终结者”、等 ARP 攻击软件，对其他电脑的网关攻击，将记录在“ARP 日志”。默认时间间隔是 200ms。

启用：是否选择启用 LAN 口为网关 ARP 攻击。

误差时间：发送 ARP 探测报文的间隔时间，该时间可自行设定。

探测 LAN 口非法网关：检查内网是否有 IP 和路由器的 LAN 的 IP 相同，如果有，将记录在“ARP 日志”。默认检测时间是 10s。

处理级别：ARP 防御系统智能防御系统的处理级别，级别越高，越安全。您可以根据网络环境做相应调节。

8.1.3 日志

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



8.2 访问控制

8.2.1 访问控制

首页 / 防御配置 / 访问控制

访问控制 日志

访问控制的方式: ☒ 关闭 ☐ 允许规则之外的通过 ☐ 禁止规则之外的通过



状态: ☐

描述:

控制方式: ☒ 允许 ☐ 阻止

执行顺序: 

用户组: [查看用户组](#)

自定义IP协议: [取消选择](#) 

日志: ☐

基于时间控制: ☐

访问控制的方式：设置访问控制的方式，有如下三种选择：

关闭：关闭访问控制功能，列表中的所有规则将都不生效。

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

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

通过。

状态:对规则的控制开关，选择启用表示激活该条规则。

描述：对此规则的简单描述。

控制方式：控制访问规则是允许通过或是禁止通过。

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

用户组：选择该条规则需要控制的用户组。（用户组建立请前往“高级配置”-“DNS策略”——“用户组”）

自定义 IP 协议：您可以自行定义远端 IP、域名及端口协议，并以此作为管控对象。

日志：对设置的规则记录日志，可以方便观察规则是否生效。

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

8.2.2 日志

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




8.3 MAC 地址过滤

对 MAC 地址进行管理，允许或者禁止该 MAC 地址的用户通过。

首页 / 防御配置 / MAC过滤

过滤方式: ☒ 关闭 ☐ 允许规则之外的通过 ☐ 禁止规则之外的通过 ?

 -

状态: ☒

描述:

控制方式: ☒ 允许 ☐ 阻止

MAC地址:

基于时间控制: ☐

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

关闭：对列表中添加的所有规则将不做任何控制。

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

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

状态：选择是否激活此规则。

描述：对此规则的简单描述。

控制方式：分为“允许”和“阻止”两类，用户可以选择此规则是否允许通过。

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

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

8.4 连接限制

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

The screenshot shows the 'Connection Limit' (连接限制) configuration page. At the top, there is a breadcrumb: '首页 / 防御配置 / 连接限制'. Below this, there is a row of input fields for 'Host Connection Limit' (主机连接数限制): 'ALL' (set to 3000), 'TCP' (0), 'UDP' (0), 'ICMP' (0), and 'OTHER' (0). A '提交' (Submit) button and a help icon are to the right. Below this row is a minus sign icon. The 'Status' (状态) section has a toggle switch that is currently off. The 'Description' (描述) section has an empty text box. The 'User Group' (用户组) section has a dropdown menu set to 'All Users' (全部用户) and a '查看用户组' (View User Groups) button. The 'Connection Limit' (连接数限制) section has radio buttons for 'ALL' (selected), 'TCP', and 'UDP', followed by an empty input box and a help icon. The 'Based on Time Control' (基于时间控制) section has a toggle switch that is currently off.

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

状态：是否启用规则，启用之后规则才会生效。

描述：对规则的简单描述。

用户组：选择该条规则需要控制的用户组。（用户组建立请前往“高级配置”-“DNS 策略”——“用户组”）

连接数限制：可以单独对 TCP/UDP 连接限制或者做全部的限制。

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

8.5 DDOS 防御

对用户的并发连接进行限制。并发连接指一定时间内用户发起的连接的总数。

并发连接数:	ALL 500	TCP 0	UDP 0	ICMP 50	OTHER 50
并发间隔时间:	ALL 2秒	TCP 2秒	UDP 2秒	ICMP 2秒	OTHER 2秒
信任的MAC列表:	<div></div>				
被攻击自动重拨:	<input type="checkbox"/> 阈值: 20 KB				
过滤广播包:	<input type="checkbox"/>				
<div>提交</div>					
<div>一</div>					
状态:	<input type="checkbox"/>				
描述:	<div></div>				
用户组:	全部用户				<div>查看用户组</div>
并发类型:	<input checked="" type="radio"/> ALL <input type="radio"/> TCP <input type="radio"/> UDP				
并发连接数:	<div></div>				
并发连接间隔时间:	3600 秒				
基于时间控制:	<input type="checkbox"/>				

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

默认并发连接间隔时间：并发连接单位时间。

信任的 MAC 列表：设置可信任的、无需受上述规则限制的 MAC 地址。

状态：是否启用规则。

描述：对规则的简单描述。

用户组：选择该条规则需要控制的用户组。（用户组建立请前往“高级配置”-“DNS

策略”——“用户组”)

并发连接类型：可以单独选择 TCP，UDP 或者所有。

并发连接数：单机所允许的最大并发连接数条目。

并发连接间隔时间：相应的间隔时间，单位为秒。

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

8.6 Ping WAN 口

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



8.7 连接数限制

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

首页 / 防御配置 / 连接数设置

路由器连接数容量: 100000

高级参数: 

TCP超时设置

None: 600 ?

Established: 1800 ?

SYN Sent: 60 ?

SYN Received: 60 ?

FIN Wait: 10 ?

Time Wait: 12 ?

Close: 2 ?

Close Wait: 10 ?

Last ACK: 3 ?

Listen: 120 ?

UDP超时设置

Unreplied: 120 ?

Assured: 300 ?

9 高级配置

设备高级功能的相关参数设置，包括端口镜像、交换机联动、NAT 转换、DNS

代理、通告系统及 WEB 访问设置等

9.1 策略路由

9.1.1 负载均衡

负载均衡功能用于设置线路的均衡模式及侦测方式、均衡权值等。

[首页](#) / [高级配置](#) / [策略路由](#)

[负载均衡](#)
[地址范围](#)
[策略路由](#)
[日志](#)

当前只有一个广域网出口，策略路由相关功能仅在开启了VPN借线功能后才有意义！

均衡模式

智能负载均衡模式：☐ IP地址 ☒ 会话数 ☐ 流量 ☐ 流量和会话数

身份绑定功能：☒ 只对网银有效: ☒ ?

在主机连接信息中显示策略规则描述：☐

线路配置

该线路参与默认均衡策略：☒

线路侦测：☐

高级参数 ☒

均衡的权值：☒ 自动 ☐ 自定义

侦测间隔： 秒 ?

侦测次数： ?

当线路连接失败时：☐ 仅记录到日志 ☒ 移除该线路并记录日志

下载流量超过： KByte 时不进行线路侦测 ?

侦测默认网关：☒

侦测远程服务器：☒

智能型负载均衡模式分为 IP 地址均衡、会话数均衡、流量均衡、流量和会话数均衡。

- (1) IP 地址均衡：依据内部用户的 IP 地址来决定线路的负载均衡。
- (2) 会话数均衡：依据用户的对外联机数来决定线路的负载均衡。
- (3) 流量均衡：依据用户的网络使用流量来决定线路的负载均衡。
- (4) 流量和会话数：依据用户流量使用和对外联机数来决定线路均衡。

①IP 均衡的作用，每条线路上的 IP 用户数目是等同的。

②会话数均衡的作用，每条线路上的对外联机数目是等同的。当使用会话数均衡的时候，就是将外网的几根线路都叠加起来，相当于是合并了总带宽。

③流量均衡的作用，每条线路上流量是等同的。

④流量和会话数均衡的作用，每条线路上流量和对外联机数目是等同。

身份绑定功能：如果配置了多线路，要使 QQ、网银等正常使用，请启用只对网银有效功能。

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

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

线路侦测：启用线路侦测功能。激活时下面的选项才起作用，否则无效。线路侦测主要用于检测线路的通畅与否，对于多线路环境，若其中一根线路侦测失败，系统

默认会将该线路移除，线路上的所有会话将会自动转移到另外侦测成功且参与均衡的线路上去。

侦测间隔：线路自动侦测的中间间隔时间。

侦测次数：线路侦测的次数。

当线路连接失败时：当线路检测失败时，对该线路的处理方式。

(1) 仅记录到日志：仅在日志中记录下此次掉线日志，不删除该线路。

(2) 移除该线路并记录日志：将此线路删除，并记录到日志中，该线路上的所有联机将自动转移到其他线路上。

下载流量超过：下行流量超过设置值的时不进行线路侦测。

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

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

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

9.1.2 地址范围

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

查询 IP 所在范围:查询该 IP 属于以下已经启用的地址范围列表中的哪一类。

您可以在此界面自行更新电信/网通等的地址范围，或者自定义添加新的地址范围

段。

查询IP所在范围:

查询

地址自动更新:



更新时间:

地址范围列表

电信

启用 ☒

[下载电信地址范围](#)

使用默认“电信地址范围”

提交新的电信地址范围:

浏览

提交

网通

启用 ☒

[下载网通地址范围](#)

使用默认“网通地址范围”

提交新的网通地址范围:

浏览

提交

移动

启用 ☒

[下载移动地址范围](#)

使用默认“移动地址范围”

提交新的移动地址范围:

浏览

提交

教育网

启用 ☒

[下载教育网地址范围](#)

使用默认“教育网地址范围”

提交新的教育网地址范围:

浏览

提交

9.1.3 策略路由

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

[负载均衡](#)
[地址范围](#)
[策略路由](#)
[日志](#)

当前只有一个广域网出口，策略路由相关功能仅在开启了VPN借线功能后才有意义！

—

状态：☒

描述：

执行顺序： ?

用户组： ? [查看用户组](#)

应用协议： [取消选择](#)

自定义IP协议： [取消选择](#)

广域网的选择： ?

自动切换线路：☒

日志：☒

基于时间控制：☐

状态：对规则的控制开关，选择开启表示激活该条规则。

描述：对该条规则的简单文字描述，该描述必须是唯一的。

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

用户组：对需要管控的用户组进行选择设定。

应用协议：选择您需要管控的单个或者多个协议。

自定义 IP 协议：您可以自行定义远端 IP、域名及端口协议，并以此作为管控对象。

广域网的选择：当数据匹配上时，匹配的数据直接从选择接口出去，不再进行后面规则的匹配。

广域网断网自动切换路线：选择是否开启断网自动切换功能。

日志：对于匹配上的数据包，进行日志记录。

基于时间控制：如果启用了“基于时间控制”，那么该规则，将在指定的时间段内生效。（每周：您可以设置一周的哪几天生效；每天：您可以设置一天的哪些时段生效）

在列表下方，您可以选择将设置的策略路由规则导入导出，如图所示：



9.1.4 日志

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



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

9.2 DNS 策略

9.2.1 DNS 组

用于添加 DNS 组，查询域名所在分组。

DNS组 DNS出口组 规则

— ?

DNS分类组:

查询域名所在分类组:

ID	名称	类型	操作
1	视频	系统创建	
2	P2P	系统创建	
3	网页	系统创建	
4	QQ网吧特权	系统创建	
5	网络游戏	系统创建	
6	国外应用	系统创建	

DNS 分类组：建立新的 DNS 分组。

查询域名所在分组：输入需要查询域名，点击查询即可查找分组情况。

9.2.2 DNS 出口组

DNS组 DNS出口组 规则

— ?

当前只有一个广域网出口，DNS策略相关功能仅在开启了VPN借钱功能后才有意义！

名称:

DNS服务器:

出口选择:

ID	名称	DNS服务器	出口接口	操作
----	----	--------	------	----

名称：添加出口名称。

DNS 服务器：填入需要出口的 DNS 服务器地址。

出口选择：选择出口外网线路。

9.2.3 规则

对 DNS 策略规则的设定功能版。

DNS组
DNS出口组
规则

默认DNS出口组:

▼

提交

—

状态:

名称:

执行顺序:

30000

?

用户组:

全部用户
▼

查看用户组

DNS组:

全部DNS
▼

查看DNS组

DNS出口组:

▼

查看DNS出口组

确定

取消

状态
名称
执行顺序
用户组

默认 DNS 出口组：选择 DNS 出口组，选择以后成为默认出口组。

名称：填写名称，便于管理员区分。

执行顺序：规则与规则之间的执行顺序值，值越大的越被优先读取执行。

用户组：选择规则管控的用户组。

DNS 组：选择规则管控的 DNS 组。

DNS 出口组：选择规则管控的 DNS 出口组。

9.3 通告系统

9.3.1 文件编辑

首页 / 高级配置 / 通告系统

文件编辑 规则管理 日志

下载通告模板

查看通告模板

通告板1

还没有通告文件信息。

浏览

提交新的通告文件

通告板2

还没有通告文件信息。

浏览

提交新的通告文件

通告板3

还没有通告文件信息。

浏览

提交新的通告文件

通告板4

还没有通告文件信息。

浏览

提交新的通告文件

如果需要更改原通告文件，请先下载通告模板，更改后再上传提交。导入的通告文件必须是“.htm”格式的，且大小不能超过 8K，新的通告文件导入之后将会自动替换掉旧的通告文件。通告文件最多可以导入四条。

9.3.2 规则管理

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

文件编辑 规则管理 日志

优先级：☒ 认证优先通告 ☐ 通告优先认证 ?

触发方式：☒ 根路径请求 ☐ 所有请求 ?

通告板显示确认按钮：☐

提交

—

状态：☒

描述：

间隔时间： 分钟

通告时长： 秒

用户类型：

用户IP范围： ?

目的域名范围： ?

通告内容： 查看通告

日志：☐

基于时间控制：☐

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：对此规则的简单描述。

间隔时间：通告文件弹出的间隔时间，单位为分钟。

注意：通告文件默认不会像弹窗广告那样自动弹出，只有在开启网页的时候才会将网页强行转向到指定的通告页面。

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

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

日志：是否记录到日志。

基于时间控制：启用之后设定的规则将只会在指定的时间段内生效。

设定完毕之后点击“确定”按钮，将规则加入列表之中。

9.3.3 日志

记录通告管理系统产生的一些日志信息。



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

9.4 端口映射

9.4.1 端口映射

使外网可以通过 IP 地址或域名访问到内网机器映射出去的端口。

端口映射 DMZ设置 UPnP设置

映射模式: ☒ 模式1 ☐ 模式2 ?

提交



状态: ☒

描述: default

协议: ☒ TCP ☐ UDP ☐ TCP/UDP

源地址限制: 选填，可为空

外部端口: - ?

内部端口: - ?

内部主机地址: 必填

广域网接口: 全部广域网 ?

状态：对规则的控制开关，选择启用表示激活该条规则

描述：对规则的简单描述。

协议：分为 TCP、UDP、TCP 和 UDP。

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

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

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

内部主机地址：内网需要映射的机器 IP 地址。

广域网接口：选择您要映射的广域网接口，默认为所有接口 ALL。

例如：

将内部机器 192.168.1.2 的 TCP-2000 端口映射为外网的 TCP-1000 端口，那么只需要按照上图这样设置就可以了。

内部机器访问 192.168.1.2 机器时使用 192.168.1.2:2000 这样的方式；外部广域网网络访问映射机器时就需要使用 WAN 口 IP:1000 这样的方式来访问映射机器了。

9.4.2 DMZ 设置

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

端口映射 DMZ设置 UPnP设置

启用DMZ: ☒

目的地址: 192.168.0

源地址限制:

确认 取消

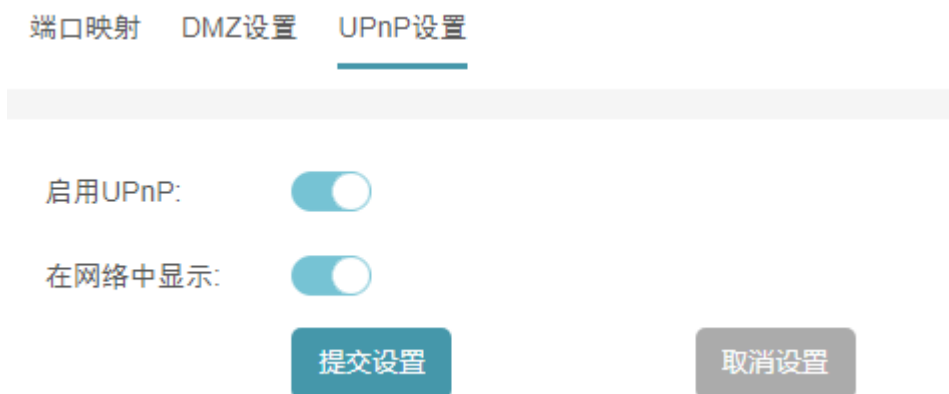
启用 DMZ：选择开启即表示启用此功能。

目的地址：需要设为 DMZ 的内部机器 IP 地址。

源地址限制：是可选项（可以不用填写），允许外部广域网口访问的地址或地址段。允许输入“202.103.24.68”、“202.103.24.68-202.103.44.150”、“202.103.24.0/24”这三种格式。

9.4.3 UPnP 设置

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



The image shows a screenshot of the UPnP settings page in a web interface. At the top, there are three tabs: '端口映射' (Port Mapping), 'DMZ设置' (DMZ Settings), and 'UPnP设置' (UPnP Settings), with the latter being the active tab. Below the tabs is a horizontal separator line. The main content area contains two toggle switches. The first is labeled '启用UPnP:' (Enable UPnP:) and is currently turned on (blue). The second is labeled '在网络中显示:' (Show in network:) and is also turned on (blue). At the bottom of the settings area, there are two buttons: '提交设置' (Submit Settings) in blue and '取消设置' (Cancel Settings) in grey.

启用 UPNP：选择开启即表示启用此功能。

在网络中显示：选择开启之后需要自动映射端口的应用类型软件就会在列表中显示，便于管理员查看使用的软件类型。

9.5 NAT 转换

9.5.1 NAT 一对一规则

NAT一对一规则

NAT多对多规则

—

状态:

描述:

default

?

内部地址:

?

外部地址:

?

开放协议:

TCP

▼

开放端口:

?

内部端口:

?

接口:

WAN1

▼

状态：打勾表示启用本条规则，规则被激活才能正常使用。

描述：可以在这里简单备注一下本条规则。

内部地址：填写主机的内部 IP 地址。

外部地址：填写一个外网 IP 地址用来作一对一的映射。

注意：填写的外网地址必须是网络服务商已经提供的合法的静态地址，否则 NAT 一对一功能无法实现。

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

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

接口：规则作用于哪个 WAN 口。

9.5.2 NAT 多对多规则

NAT一对一规则
NAT多对多规则

—

状态：☐

描述： ?

源地址

设为内网扩展地址：☐

IP地址：

子网掩码：

目的地址

类型： ▼

IP地址：

子网掩码：

接口： ▼

转换地址： ?

状态：开启本条规则，规则被激活才能正常使用。

描述：可以在这里简单备注一下本条规则。

源地址：内网扩展地址已经在内网设置里面配置，所以不需要将“设为内网扩展地址”打勾。IP 地址和掩码请填写需要 NAT 转换的计算机的网段和掩码，本例是 192.168.5.1/24。

目的地址：需要访问的外网目的地址。“类型”可以选择“任意”或者“子网”。如果选择“任意”，表示源地址出访到任意目标地址的数据包都需要通过转换地址做 NAT 出访。如果选择“子网”，则表示源地址出访到指定目标地址段的数据包才需要转换地址做 NAT 出访。建议通常情况下这里保持默认配置。

接口：选择“不指定”，只能是单出口上网模式才能应用；多线路模式上网时，需选择一个使用的 WAN 接口。当用户使用 PPPoE 上网时，如果指定了相应的 WAN 口，则转换地址自动为当前 WAN 口的 IP 地址，本例选择“WAN1”。

转换地址：NAT 以后，源地址使用填写的转换地址访问外网。这里可以填写一个地址或一个地址段，设置地址段时，最大长度为 16 个地址。

9.6 端口设置

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

端口名称: WAN1

端口模式: 自动

修改

取消

刷新

端口名称	端口模式	当前连接状态	操作
LAN1	自动	断开	
LAN2	自动	断开	
LAN3	自动	断开	
LAN4	自动	断开	
WAN1	自动	1000M/全双工	

9.7 路由表

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

9.7.1 当前路由

用于查看当前路由情况

当前路由表 静态路由表

目的地址	网关	子网掩码	Metric	网络接口
10.255.0.2	10.255.0.1	255.255.255.255	0	wvpn1
127.0.0.0	*	255.0.0.0	0	lo
192.168.0.0	*	255.255.255.0	0	LAN

9.7.2 静态路由

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

例如：指定内网的主机访问 222.12.12.0/24 这个网络的资源从 WAN1 出去，WAN1 的网关地址是 61.121.13.1，可以按此操作。点击添加新规则，做如下的配置：

当前路由表 静态路由表



描述:

default

目的地址:

222.12.12.0

子网掩码:

255.255.255.0

网关:

61.121.13.1

Metric:

0



网络接口:

WAN1

确定

取消

9.8 DNS 代理

9.8.1 DNS 代理

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

DNS代理 DNS缓存

DNS 代理:



DNS的最小老化时间:

60

秒



DNS的最大老化时间:

600

秒



主机连接信息中显示远端IP域名:



提交设置

取消设置

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

老化时间：域名解析的 IP 对应关系在 DNS 列表中缓存的最大时间

9.8.2 DNS 缓存

DNS 缓存列表会记录下所有用户 DNS 最大老化时间内缓存的域名解析信息，超过时间的缓存信息将会自动老化掉。对某域名做过规则或该域名正被连续使用，将会加长大化时间。

DNS代理 DNS缓存

域名	IP地址	查询				
域名	IP地址	DNS组ID	DNS出口组ID	更新时间	老化时间	刷新
browser.360.cn	60.214.111.204	未配置	undefined	27秒	1分	
cloud.browser.360.cn	180.163.237.176	未配置	undefined	7分28秒	1分	
gateway.icloud.com.cn	17.248.161.41	未配置	undefined	9分8秒	1分	
report.uri.cn	116.128.163.211	未配置	undefined	8分15秒	1分	
mmbiz.qpic.cn	123.6.1.55	QQ网吧特权	undefined	4分52秒	1分	
sdkapiv2.bizport.cn	101.37.191.173	未配置	undefined	3分27秒	1分	
grs.dbankcloud.cn	49.4.17.190	未配置	undefined	9分44秒	1分	
ovv4.allook.tv	0.0.0.0	未配置	undefined	9分37秒	1分	
vweixinthumb.tc.qq.com	119.188.150.114	未配置	undefined	7分19秒	1分	

9.9 WEB 访问设置

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

首页 / 高级配置 / WEB访问设置

HTTP 访问端口:	<input type="text" value="80"/>	
认证通告端口:	<input type="text" value="0"/>	
远程访问:	<input type="checkbox"/>	
远程访问端口:	<input type="text" value="8080"/>	
管理员:	<input type="text" value="admin"/>	
管理员密码:	<input type="password"/>	
管理员密码确认:	<input type="password"/>	
启用guest用户:	<input type="checkbox"/>	
guest用户:	<input type="text" value="guest"/>	
guest用户密码:	<input type="password"/>	
guest用户密码确认:	<input type="password"/>	

HTTP 访问端口：本地局域网访问路由器时的端口。默认为 80。

认证通告端口：认证页面、通告页面等页面的弹出时使用的端口，如果为 0，表示和管理端口相同。

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

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

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

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

guest 用户/密码：自定义您的 guest 用户名及密码。

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

9.10 端口镜像

端口镜像功能主要用于监控端口数据流量，以方便管理人员对网络数据进行分析。

首页 / 高级配置 / 端口镜像

状态:

☐

选择镜像的数据方向:

☐ 出口 ☐ 入口 ☒ 全部

镜像出口方式:

☒ 镜像到主机IP ☐ 镜像到端口

将数据包镜像到内部主机的IP:

192.168.0.2

状态：选择是否启用端口镜像功能。

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

镜像出口方式：选择是镜像到主机 IP 或者镜像到端口。

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

9.11 NAT 快速转发

开启 NAT 快速转发功能后，可提升设备的吞吐性能，为了提高处理能力，对行为管理及邮件监控、过滤等功能会失效。

首页 / 高级配置 / NAT快速转发

开启NAT快速转发：

☐

注意：开启NAT快速转发后WEB关键字过滤、邮件监控，酒店模式，3G/4G上网等功能可能会失效

状态：

未启用

提交设置

9.12 端口 VLAN

根据需要可通过端口 VLAN 将 LAN 端口进行端口 VLAN 的化分，可实际端口隔离目的。

首页 / 高级配置 / 端口VLAN

LAN1: ☒ VLAN1 ☐ VLAN2 ☐ VLAN3 ☐ VLAN4

LAN2: ☒ VLAN1 ☐ VLAN2 ☐ VLAN3 ☐ VLAN4

LAN3: ☒ VLAN1 ☐ VLAN2 ☐ VLAN3 ☐ VLAN4

LAN4: ☒ VLAN1 ☐ VLAN2 ☐ VLAN3 ☐ VLAN4

提交设置

10.USB 存储

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

10.1 设备状态

可以查看到当前已连接的 USB 设备信息，在 USB 不使用时，请将 USB 设备移除。



10.2 共享服务

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

存储设备状态:

未连接

刷新

USB共享服务:

☒ 允许外网用户访问

?

☐ 开启WEB认证访问

设备标识:

用户名:

login

密码:

123456

超级用户名:

hlogin

超级密码:

123456

?

外网访问URL发送到邮箱:

☒ 发送共享用户名
 ☐ 发送共享密码

高级参数

▼

允许访问USB共享的内部主机:

基于IP

允许访问USB共享的内部主机:

基于MAC

?

您只需要在地址栏输入共享地址即可访问到 USB 共享数据，私有目录地址需要登录才可以进行访问，您可以手动修改登录密码。

10.3 USB 日志

使用这个功能的前提是需要 USB 存储设备已连接的状态；USB 日志的功能为路由当中所记录的使用日志，由于路由重启后日志都会清空，如果加上 USB 日志记录到 USB 中，日志便于查询。

启用USB日志功能

☒

?

路由器设置自动保存时间:

18 : 0

设置

刷新

名称	路径	文件大小	操作
----	----	------	----

启用 USB 日志功能，设置自动保存时间。提交设置后，路由器将会在您设置的

时间自动将日志保存在 USB 设备中。并且在日志信息列表中会有相关信息。

日志记录的文件夹会存储在 USB 设备中，打开之后里面所有的格式都是 log，使用记事本打开就可以查看到。

10.4 4G 上网设置

10.4.1

该功能的可以使路由器多一个使用 4G 网络的广域网。该局域网内的用户可以共享该 4G 网络。



状态： 选择启用表示开启 4G 功能。

支持列表： 可以看到路由可以支持的 4G 设备列表，您也可以根据这个支持列表来进行选选择 4G 卡。

ISP： 可以自行选择 ISP 供应商或者让路由去自行查找，如果选择了 ISP 供应商，那么需要填写正确用户名和密码。

连接模式： 自动连接：如果 3G 断开了或者才接上 3G 卡路由自动去进行连接；

手动连接：断开之后需要手动去点击连接。

10.4.2



点击连接刷新，可以查看到 4G 连接状态。

连接状态：Connected：连接成功。

提示：是否连接成功您可以在策略路由-线路状态中查看到是否有多一条广域网。

（如果您的路由是 4 个 WAN 口，那么添加的 4G 卡就会显示为广域网 5；两个 wan 口的路由 4G 卡显示的广域网为广域网 3）

11.应用中心

11.1 AC 平台服务端

AC: Wireless Access Point Controller, 无线控制器。AC 统一管理是 AC+AP 的覆盖的管理平台。无线网络中一个 AC（无线控制器），多个瘦 AP（收发信号），此模式适用大中型企业、酒店、小区等，有利于无线网络的集中管理，多个无线发射器能统一发射一个信号（SSID）、下发配置、修改相关配置参数、

射频智能管理等。

状态:	<input checked="" type="checkbox"/>	?
旁路模式:	<input type="checkbox"/>	?
LAN口IP:	<input type="text" value="192.168.0.1"/>	
默认网关:	<input type="text" value="0.0.0.0"/>	
DNS:	<input type="text"/>	
服务器地址:	<input type="text" value="http://192.168.0.1:800"/>	
	默认用户名:admin 密码:admin	
	(注意1: 开启旁路模式之前, 请先将所有广域网口的接入类型设置为关闭状态, 同时关闭DHCP服务器, 修改LAN口IP地址)	
申请控制:	<input type="button" value="申请控制"/>	<input type="button" value="关闭控制"/>
	<input type="button" value="刷新状态"/>	
	未开启此功能 <input type="button" value="Copy"/>	

11.1.1 系统登录

①在首行的状态点击“启用”，旁路模式、默认网关、DNS 参数保持默认即可，然后点击右下角的“提交设置”

状态:	<input checked="" type="checkbox"/>	?
旁路模式:	<input type="checkbox"/>	?
LAN口IP:	<input type="text" value="192.168.0.1"/>	
默认网关:	<input type="text" value="0.0.0.0"/>	
DNS:	<input type="text"/>	?
服务器地址:	http://192.168.0.1:800	
	默认用户名:admin 密码:admin	
	(注意1: 开启旁路模式之前, 请先将所有广域网口的接入类型设置为关闭状态, 同时关闭DHCP服务器, 修改LAN口IP地址)	
申请控制:	<input type="button" value="申请控制"/>	<input type="button" value="关闭控制"/>
	<input type="button" value="刷新状态"/>	
	未开启此功能 <input type="button" value="Copy"/>	

②点击页面第四行的服务器地址，即“http://192.168.0.1:800”，进入智能 AC 管理系统登录界面，如下图所示：

状态:	<input checked="" type="checkbox"/>	?
旁路模式:	<input type="checkbox"/>	?
LAN口IP:	<input type="text" value="192.168.0.1"/>	
默认网关:	<input type="text" value="0.0.0.0"/>	
DNS:	<input type="text"/>	?
服务器地址:	http://192.168.0.1:800	
	默认用户名:admin 密码:admin	
	(注意1: 开启旁路模式之前, 请先将所有广域网口的接入类型设置为关闭状态, 同时关闭DHCP服务器, 修改LAN口IP地址)	
申请控制:	<input type="button" value="申请控制"/>	<input type="button" value="关闭控制"/>
	<input type="button" value="刷新状态"/>	
	未开启此功能 <input type="button" value="Copy"/>	



③输入默认用户名和密码“admin”，点击密码后的箭头登录进入 AC 管理系统。

11.1.2 系统界面

登录系统以后，将显示系统的主界面，如下图所示。系统主界面主要分为三个部分：标题栏、菜单导航区、功能操作区。

D-Link

AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

云控管理

系统配置

当前位置: 系统信息 > 2.4G AP设备

共: 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往 第 页

刷新

组名	设备名	SSID名称	网络模式	BSSID	AP隔离	IP地址/掩码位	用户信息	操作
门口AP	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:45:40	禁用	172.18.170.197 / 22[D]	详细信息	扫描附近AP
DI-810WO	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP
S桌	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP

友讯电子设备（上海）有限公司版权所有 全国客服电话:400-629-6688 技术支持

- 标题栏：显示当前版本信息、登录信息和注销登录；
- 菜单导航区：该功能导航栏显示目前系统所有功能目录；
- 功能操作区：该区包含各菜单功能的具体操作；

11.1.3 系统信息

该功能用于展示所连接的 2.4G 无线 AP 和 5G 无线 AP 设备的组名、设备名、SSID 名称、网络模式、BSSID、AP 隔离、IP 地址/掩码位数、用户信息、扫描操作等功能。

当前位置: 系统信息 > 2.4G AP设备

共: 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往 第 页

刷新

组名	设备名	SSID名称	网络模式	BSSID	AP隔离	IP地址/掩码位	用户信息	操作
	门口AP	DLINK 详细信息	11b/g/n混合	0C:73:EB:DB:45:40	禁用	172.18.170.197 / 22[D]	详细信息	扫描附近AP
	DI-810WO	DLINK 详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP
	S桌	DLINK 详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP

操作说明:

① 2.4G AP 设备

SSID 名称: 查看设备的 SSID 名称及加密类型, 密码等信息。如图:



用户信息: 查阅当前设备所连接的用户数量, 并显示连接的用户信息。包括用户 IP 地址, MAC 地址, SSID 号, 信号强度, 上行/下载数据, 上传/下载速度等参数信息。如图:

D-Link

AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G AP设备

5G AP设备

分组管理

2.4G设备管理

5G设备管理

用户管理

云控管理

系统配置

当前位置: 系统信息 > 2.4G AP设备

共: 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往第 页

刷新

组名	设备名	SSID名称	网络模式	BSSID	AP隔离	IP地址/掩码位	用户信息	操作
门口AP	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:45:40	禁用	172.18.170.197 / 22[D]	详细信息	扫描附近AP
DI-810WO	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP
S桌	DLINK	详细信息	11b/g/n混合	0C:73:EB:DB:42:80	禁用	172.18.170.174 / 24[D]	详细信息	扫描附近AP

扫描附近 AP: 对 AP 无线覆盖内的其他所有 AP 进行信号扫描, 查找附近所有 AP。

2 5G AP 设备

具体的功能和操作方式与 2.4G AP 设备目录下一致, 请参考上述内容。

11.1.4 2.4G 设备管理

该功能模块为管理员提供 2.4G 无线设备的设备管理, 对设备进行批量配置 2.4G 无线 wifi 名称和加密方式、信道、组名、频率等模块, 对设备进行中继配置和实现 MAC 地址过滤, 以及查看运行状态的功能。

①设备管理

此功能展示了当前与 AC 统一管理系统的 2.4G 频段的 AP 无线设备信息, 包括组名、设备名称、AP 获取到的 IP 地址和掩码、MAC 地址、当前连接用户数、频道、创建时间、状态、旁路认证、备注以及对设备的查找、修改和删除等信息。

D-Link

AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

设备管理

中继配置

MAC地址过滤

运行状态

5G设备管理

用户管理

当前位置: 2.4G设备管理 > 设备管理

组名:

设备名:

IP地址:

BSSID:

在线:

AP隔离:

查询

取消

共: 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往第 页

批量修改 刷新

组名	设备名	IP地址/掩码位	BSSID	当前用户数	频道	创建时间	状态	AP隔离	旁路认证	配置状态	无线网络	操作
	门口AP	172.18.170.197 / 22 [D]	0C:73:EB:DB:45:40	0	1	4天18时30分27秒	在线	禁用	禁用		打开	修改 删除
	DI-810W O	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时17分28秒	离线	禁用	禁用		打开	修改 删除
	S桌	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时9分16秒	在线	禁用	禁用	下发成功	打开	修改 删除

选择文件

未选择任何文件

导入设备信息

导出设备信息

➤ 修改单个 AP 参数。在对应的设备后方点击操作栏目下的“修改”按钮；

配置向导

系统信息

2.4G设备管理

设备管理

中继配置

MAC地址过滤

运行状态

5G设备管理

用户管理

云控管理

系统配置

当前位置: 2.4G设备管理 > 设备管理

组名:

设备名:

无线网络:

获取IP方式:

IP地址:

子网掩码:

默认网关:

BSSID:

备注:

最大用户数:

LAN口VLAN ID:

LAN口2VLAN ID:

关闭WiFi指示灯:

快速漫游切换:

频道:

运行模式:

带宽:

扩展频道:

频道模式:

AP隔离:

主动断开阈值:

发送功率:

旁路认证上网:

WEB管理端口:

WEB管理用户名:

WEB管理密码:

DHCP服务器防御:

DHCP管理方式:

网络模式:

SSID:

SSID 1:

组名：可将多个 AP 设置到同一分组内

设备名：修改此设备的识别名称

获取 IP 方式：DHCP 动态获取地址和静态手动为 AP 配置地址

IP 地址、子网掩码、默认网关：可通过 DHCP 自动获取或手动配置

BSSID：随 AP 出厂的 MAC 地址

备注：可为设备添加备注信息

最大用户数：依据当前 AP 型号进行设置

LAN 口 VLAN ID：可设置范围为 5-4095，默认 0 为不设置

关闭 WIFI 指示灯：可选开启或禁用

组播：可选择组播转组播或组播转单播，默认为关闭状态

频道：WIFI 的信道，可选自动选择或手动选择特定频道

运行模式：AP 的运行模式，可选择普通模式和增强模式

带宽：可选 20MHZ 或 20/40MHZ 频率

扩展频道：可选 2 或 10 个扩展频道数量

频道模式：可选择单频或双频的频道模式

AP 隔离：可将同一局域网中的 AP 相互隔离，默认为禁用

主动断开阈值：当连接 WIFI 的设备达到最远距离阈值时，会自动断开当前 WIFI 连接，可设范围为 0-127，0 为不启用此功能

发送功率：可设置范围为 0-100，默认为最大功率 100

旁路认证上网：本地 AC 的组网方式为旁路（见第三章智慧 wifi 中的旁路布网示意图），用户上网时，认证信息通过本地 AC 发送到公网服务器中进行认证，最终返回到 AP 中，AP 按照返回的命令执行是否允许用户上网操作

WEB 管理端口：默认为 80，可设置范围 1-65535

WEB 管理用户名、密码：使用 WEB 管理时登录的用户名和密码

DHCP 服务器防御：可防御非法的 DHCP 服务器对 AP 下发 IP 地址

DHCP 管理方式：将 AP 作为 DHCP 服务器对连接的设备自动分发 IP 地址

网络模式：支持 802.1b、802.1g、802.1n 单种或多种混合的网络模式

SSID：设置含有的参数：SSID 名称，隐藏（隐藏让设备无法通过扫描发现此 SSID），隔离（SSID 之间隔离），均衡模式和安全设置。均衡模式分为：用户数均衡、信号强度均衡、流量均衡；加密类型分为：开放式、共享式、WEPAUTO、WPA、WPA 个人、WPA2、WPA2 个人、WPA/WPA2 个人、WPA1WPA2；WPA 算法类型分为：TKIP、AES；共享密钥支持除特殊符号外的字母与数字任意组合。

为了提高安全性和兼容性，建议加密设置选择“**WPA/WPA2 个人**”，WPA 算法选择“**TKIP/AES**”。

➤ 批量修改 AP 设备。在设备管理界面的右上角，点击“批量修改”按钮，如图所示：

D-Link

AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

设备管理

中继配置

MAC地址过滤

运行状态

5G设备管理

用户管理

当前位置: 2.4G设备管理 > 设备管理

组名:

设备名:

IP地址:

BSSID:

在线: 全部

AP隔离: 全部

查询

取消

共: 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往 第 页

批量修改

刷新

组名	设备名	IP地址/掩码位	BSSID	当前用户数	频道	创建时间	状态	AP隔离	旁路认证	配置状态	无线网络	操作
门口AP	172.18.170.197 / 22 [D]	0C:73:EB:DB:45:40	0	1	4天18时32分3秒	在线	禁用	禁用		打开	修改 删除	
DI-810W O	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时19分4秒	离线	禁用	禁用		打开	修改 删除	
S桌	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时10分52秒	在线	禁用	禁用	下发成功	打开	修改 删除	

选择文件

未选择任何文件

导入设备信息

导出设备信息

配置向导

系统信息

2.4G设备管理

设备管理

中继配置

MAC地址过滤

运行状态

5G设备管理

用户管理

云控管理

系统配置

当前位置: 2.4G设备管理 > 设备管理

设备选择:

无线网络:

关闭无线网络 打开无线网络

获取IP方式:

DHCP

最大用户数:

32

LAN口VLAN ID:

0 (0-4080)

LAN2口VLAN ID:

0 (0-4080)

关闭WiFi指示灯:

启用

快速漫游切换:

禁用 (注意: 只支持WPA2企业和WPA2个人/AES加密方式, 并且保证AP之间能互通)

频道:

2447MHz (频道 8)

运行模式:

普通

带宽:

20MHz

扩展频道:

4

频道模式:

双频

AP隔离:

禁用

主动断开阈值:

0 (为0表示不启用, 范围是0到-127; 当客户端连接信号低于设定阈值时主动断开连接)

发送功率:

100 (1-100)

旁路认证上网:

启用

WEB管理端口:

80 (1-65535)

WEB管理用户名:

root

WEB管理密码:

admin

DHCP服务防蹭:

禁用 白名单: (MAC格式: 11:22:33:44:55:66 多个MAC之间用';'分隔)

DHCP管理方式:

关闭 普通设置 高级设置

网络模式:

11b/g/n混合

SSID:

WoYaoWiFi * 隐藏 隔离 编码: GB2312 均衡模式: 关闭

安全设置: 关闭 VLAN ID: 0 (0-4080)

SSID 1:

隐藏 隔离 编码: GB2312 均衡模式: 关闭

安全设置: 关闭 VLAN ID: (0-4080)

SSID 2:

隐藏 隔离 编码: GB2312 均衡模式: 关闭

安全设置: 关闭 VLAN ID: (0-4080)

SSID 3:

隐藏 隔离 编码: GB2312 均衡模式: 关闭

安全设置: 关闭 VLAN ID: (0-4080)

设备选择：首先选择需要更改的设备，选择后点击确定。并在下列需要修改的选

项参数前打钩。

组名：可将多个 AP 设置到同一分组内。

获取 IP 方式：DHCP 动态获取地址和静态手动为 AP 配置地址。

最大用户数：对选中的每个设备设置最大的连接上的人数，依据当前 AP 型号进行设置。

LAN 口 VLAN ID：可设置范围为 5-4095，默认 0 为不设置。

关闭 WIFI 指示灯：可选开启或禁用。

组播：可选择组播转组播或组播转单播，默认为关闭状态。

频道：WIFI 的信道，可选自动选择或手动选择特定频道。

运行模式：AP 的运行模式，可选择普通模式和增强模式

带宽：可选 20MHZ 或 20/40MHZ 频率

扩展频道：可选 2 或 10 个扩展频道数量

频道模式：可选择单频或双频的频道模式

AP 隔离：可将同一局域网中的 AP 相互隔离，默认为禁用

主动断开阈值：当连接 WIFI 的设备达到最远距离阈值时，会自动断开当前 WIFI 连接，可设范围为 0-127，0 为不启用此功能

发送功率：可设置范围为 0-100，默认为最大功率 100

旁路认证上网：本地 AC 的组网方式为旁路（见第三章智慧 wifi 中的旁路布网示意图），用户上网时，认证信息通过本地 AC 发送到公网服务器中进行认证，最终返回到 AP 中，AP 按照返回的命令执行是否允许用户上网操作

WEB 管理端口：默认为 80，可设置范围 1-65535

WEB 管理用户名、密码：使用 WEB 管理时登录的用户名和密码

DHCP 服务器防御：可防御非法的 DHCP 服务器对 AP 下发 IP 地址

DHCP 管理方式：将 AP 作为 DHCP 服务器对连接的设备自动分发 IP 地址

网络模式：支持 802.1b、802.1g、802.1n 单种或多种混合的网络模式

SSID：设置含有的参数：SSID 名称，隐藏（隐藏让设备无法通过扫描发现此 SSID），隔离（SSID 之间隔离），均衡模式和安全设置。均衡模式分为：用户数均衡、信号强度均衡、流量均衡；加密类型分为：开放式、共享式、WEPAUTO、WPA、WPA 个人、WPA2、WPA2 个人、WPA/WPA2 个人、WPA1WPA2；WPA 算法类型分为：TKIP、AES；共享密钥支持除特殊符号外的字母与数字任意组合。

为了提高安全性和稳定性，建议加密设置选择“WPA/WPA2 个人”，WPA 算法选择“TKIP/AES”。

查找与删除设备。在设备列表上方设有查找和筛选工具，可对某个或一类特定 ap 进行筛选和查找，可选条件有组名、设备名称、IP 地址、BSSID、是否在线、AP 是否隔离。如图：

当前位置: 2.4G设备管理 > 设备管理

组名: 设备名: IP地址: BSSID: 在线: AP隔离:

共: 3 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往 页 [批量修改](#)

组名	设备名	IP地址/掩码	BSSID	当前用户数	频道	创建时间	状态	AP隔离	旁路认证	配置状态	无线网络	操作
	门口AP	172.18.170.197 / 22 [D]	0C:73:EB:DB:45:40	0	1	4天18时33分26秒	在线	禁用	禁用		打开	修改 删除
	DI-810W O	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时20分27秒	离线	禁用	禁用		打开	修改 删除
	S桌	172.18.170.174 / 24 [D]	0C:73:EB:DB:42:80	0	1	2天17时12分15秒	在线	禁用	禁用	下发成功	打开	修改 删除

未选择任何文件 [导出设备信息](#)

查找到对应的 AP 后，可对其进行对应的修改和删除操作。

②中继配置

AC 集中管理平台中的中继配置，同 WDS 设置。即无线网络中把多个 AP 通过中继或桥接起来。

➤ 操作步骤

例如 S 桌 和 门口 AP 设备连接中继模式，配置方式如下图：

中继设备：选中所有需要连接的 AP 设备

WDS 模式：选中中继或者桥接模式。中继模式即继承设备继承了被继承设备的

所有参数，桥接模式继承设备只继承了被继承设备的网络连通性相关参数。

填写完成后，点击“下一步”

当前位置：2.4G设备管理 > 中继配置

中继设备： 请选择中继设备进行参数配置。

目标中继设备1： 加密类型： 密钥：

目标中继设备2： 加密类型：

目标中继设备3： 加密类型：

目标中继设备4： 加密类型：

注意：请依次设置目标中继设备，如果中间预留空，后面的目标中继设备将自动前移。

当前位置：2.4G设备管理 > 中继配置

中继设备： 请选择中继设备进行参数配置。

目标中继设备1： 加密类型： 密钥：

目标中继设备2： 加密类型：

目标中继设备3： 加密类型：

目标中继设备4： 加密类型：

注意：请依次设置目标中继设备，如果中间预留空，后面的目标中继设备将自动前移。

规则完成之后，点击“全部下发”。此规则就下发到 AP 设备中。桥接模式连接与中继连接的方法一致。桥接设备和被桥接设备都需要设置目标设备和密钥，同中继设备和被中继设备都需设置目标设备和密钥。

注：1、同一个 AP 设备，不能做多个中继或桥接规则。如果规则相冲突的话，AP 设备的参数只会同步最后的一个规则信息。

2、连接中继配置需要相同的 SSID 及加密方式、频道。

③AC 地址过滤

通过过滤 MAC 地址来阻止或允许 AP 设备中的终端用户上网。过滤的方式为：允许如下客户端、阻止如下客户端。如图：

当前位置: 2.4G设备管理 > MAC地址过滤

过滤方式: 关闭

提交

规则编辑

描述:

MAC地址:

设备:

添加

取消

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往第 页

刷新

描述	MAC地址	设备	操作

全部下发

➤ 操作步骤

首先在过滤方式中选择“允许如下客户端”或“禁止如下客户端”，点击提交

当前位置: 2.4G设备管理 > MAC地址过滤

过滤方式: 关闭

提交

规则编辑

描述:

MAC地址:

设备:

添加

取消

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往第 页

刷新

描述	MAC地址	设备	操作

全部下发

然后在下面编辑具体规则，描述一栏按自己意愿随意填写，MAC 地址填写需要做控制或允许的设备的 MAC 地址，最后在设备一栏中选择要做规则的设备 SSID，点击添加。在添加后会在下图规则表中显示已添加的规则：

当前位置: 2.4G设备管理 > MAC地址过滤

过滤方式: 阻止如下客户端 ▾ 提交

规则编辑

描述:

MAC地址:

设备:

添加 取消

点击右下角“全部下发”按钮，则所有规则将会下发到对应的 AP 设备中。

④运行状态

此功能模块主要用于展示当前连接 AP 设备的运行时间、CPU 使用率、总内存、剩余内存、连接数容量、当前连接数，可以使用左边的搜索栏对特定的 AP 进行查找。

D-Link
AC管理控制器

1.02.040
admin 安全退出

当前位置: 2.4G设备管理 > 运行状态

刷新

配置向导

系统信息

2.4G设备管理

设备管理

中继配置

MAC地址过滤

运行状态

5G设备管理

用户管理

云控管理

系统配置

设备列表

键入关键字查询，双击查看

DI-810WO

S桌

门口AP

当前为: DI-810WO 的运行状态

运行时间:	3分26秒
CPU 使用率:	1.00 %
总内存:	230.73 M
剩余内存:	141.27 M
连接数容量:	16384
当前连接数:	80

11.1.5 5G 设备管理

该模块为管理员提供 5G 无线设备的设备管理，对设备进行批量配置 5G 无线 wifi 名称和加密方式、信道、组名、频率等模块，对设备进行中继配置和实现 MAC 地址过滤，以及查看运行状态的功能。

➤ 显示当前与 AC 统一管理系统的 5G 频段的 AP 无线设备信息，包括组名、设备名称、AP 获取到的 IP 地址和掩码、MAC 地址、当前连接用户数、频道、创建时间、状态、旁路认证、备注以及对设备的查找、修改和删除等信息。

D-Link AC管理控制器 1.02.040 admin 安全退出

当前位置: 5G设备管理 > 设备管理

组名: 设备名: IP地址: BSSID: 在线: AP隔离: 查询 取消

共 3 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往第 页 5G批量修改 刷新

组名	设备名	IP地址掩码位	BSSID	当前用户数	频道	创建时间	状态	AP隔离	旁路认证	配置状态	操作
门口AP		172.18.170.197 / 22[D]	0C:73:EB:DB:46:48	0	149	4天20时22分40秒	在线	禁用	禁用		修改 删除
DI-810WO		172.18.170.174 / 24[D]	0C:73:EB:DB:42:88	0	149	2天19时9分50秒	离线	禁用	禁用		修改 删除
S桌		172.18.170.174 / 24[D]	0C:73:EB:DB:42:88	1	149	2天19时1分38秒	在线	禁用	禁用		修改 删除

选择文件 未选择任何文件 导入设备信息 导出设备信息

友讯电子设备（上海）有限公司版权所有 全国客服电话:400-629-6688 技术支持

➤ 修改 AP 参数

在对应的设备下点击操作下的“修改”按钮，对 AP 设备各项参数进行修改

配置向导

系统信息

2.4G设备管理

5G设备管理

设备管理

用户管理

云控管理

系统配置

当前位置: 5G设备管理 > 设备管理

5G 参数配置

组名:

设备名:

门口AP

BSSID:

0C:73:EB:DB:45:48

最大用户数:

255

频道:

频道 149

运行模式:

普通

带宽:

20/40MHz

VHT BandWidth:

20/40MHz

扩展频道:

自动

频道模式:

双频

AP隔离:

禁用

主动断开阈值:

0

(为0表示不启用, 范围是0到-127; 当客户端连接信号低于设定阈值时主动断开连接)

发送功率:

100

(1-100)

网络模式:

11AC/AN/A

SSID:

DLINK

☐ 隐藏

隔离 编码: GB2312

均衡模式: 关闭

安全设置: 关闭

VLAN ID: 0

(0-4080)

SSID 1:

☐ 隐藏

隔离 编码: GB2312

均衡模式: 关闭

安全设置: 关闭

VLAN ID:

(0-4080)

SSID 2:

☐ 隐藏

隔离 编码: GB2312

均衡模式: 关闭

安全设置: 关闭

VLAN ID:

(0-4080)

SSID 3:

☐ 隐藏

隔离 编码: GB2312

均衡模式: 关闭

安全设置: 关闭

VLAN ID:

(0-4080)

SSID 4:

☐ 隐藏

隔离 编码: GB2312

均衡模式: 关闭

安全设置: 关闭

VLAN ID:

(0-4080)

下发

取消

刷新

组名: 可将多个 AP 设置到同一分组内

设备名: 修改此设备的识别名称

BSSID: 随 AP 出厂的 MAC 地址

最大用户数: 依据当前 AP 型号进行设置

LAN 口 VLAN ID: 可设置范围为 5-4095, 默认 0 为不设置

关闭 WIFI 指示灯: 可选开启或禁用

组播: 可选择组播转组播或组播转单播, 默认为关闭状态

频道: WIFI 的信道, 可选自动选择或手动选择特定频道

运行模式: AP 的运行模式, 可选择普通模式和增强模式

带宽: 可选 20MHZ 或 20/40MHZ 频率

扩展频道：可选 2 或 10 个扩展频道数量

频道模式：可选择单频或双频的频道模式

AP 隔离：可将同一局域网中的 AP 相互隔离，默认为禁用

主动断开阈值：当连接 WIFI 的设备达到最远距离阈值时，会自动断开当前 WIFI 连接，可设范围为 0-127，0 为不启用此功能

发送功率：可设置范围为 0-100，默认为最大功率 100

网络模式：支持 11a、11a/n 单种或多种混合的网络模式

SSID：设置含有的参数：SSID 名称，隐藏，隔离，均衡模式和安全设置。均衡模式分为：用户数均衡、信号强度均衡、流量均衡；加密类型分为：开放式、共享式、WEP AUTO、WPA、WPA 个人、WPA2、WPA2 个人、WPA/WPA2 个人、WPA1WPA2；WPA 算法类型分为：TKIP、AES；共享密钥支持除特殊符号外的字母与数字任意组合。

为了提高安全性和稳定性，建议加密设置选择“**WPA/WPA2 个人**”，WPA 算法选择“**TKIP/AES**”。

4. 查找与删除设备

在设备列表上方设有查找和筛选工具，可对某个或一类特定 ap 进行筛选和查找，可选条件有组名、设备名称、IP 地址、BSSID、是否在线、AP 是否隔离。如图：

当前位置: 5G设备管理 > 设备管理

组名:	设备名:	IP地址:	BSSID:	在线:	AP隔离:	查询 取消
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	全部 ▼	全部 ▼	

查找到对应的 AP 后，可对其进行对应的修改和删除操作。

11.1.6 用户管理

该模块提供了已连接上 AP 的用户管理功能，该模块主要分为四个目录：2.4G 用户管理、5G 用户管理、用户连接 AP 管理、上网黑白名单管理。

① 2.4G 用户列表

可通过此列表查看 2.4GAP 设备连接上无线网络的所有移动设备的具体信息，包括所属设备、用户名称、用户设备 MAC 地址、IP 地址、连接信号强度、SSID、在线时间、上传数据量、下载数据量、上网方式、认证状态。

D-Link AC管理控制器 1.02.040 admin 安全退出

当前位置: 用户管理 > 2.4G用户列表

所属组: 所属设备: IP地址: MAC地址: 信号强度: SSID: 查询 取消

共: 条记录 当前 1/1 页 首页 上一页 下一页 尾页 前往第 页 手动刷新 刷新

所属组	所属设备	用户名称	MAC地址	IP地址	信号强度	SSID	在线时间	上传数据	下载数据	上传速度	下载速度	上网方式	认证状态
-----	------	------	-------	------	------	------	------	------	------	------	------	------	------

首先使用顶部的查找筛选工具对特定用户的进行查找，可选填写项有:所属设备、IP 地址、信号强度、SSID，填写任意一项或多项后，点击“查询”，在下方的列表会显示当前查询结果

当前位置: 首页 > 用户管理 > 2.4G用户列表

所属设备: IP地址: 信号强度: (dbm) SSID: 查询

查询到相应的设备后，在设备信息最后的操作一栏有三个选项按钮，分别代表 A—组织连接所有 AP、X—阻止连接当前 AP、S—阻止连接当前 AP 的当前 SSID，点

击对应按钮即可实现对应功能：

当前位置：用户管理 > 2.4G用户列表

所属组： 所属设备： IP地址： MAC地址： 信号强度： SSID：

② 5G 用户列表

可通过此功能查看 5GAP 设备连接上无线网络的所有移动设备的具体信息，包括所属设备、用户名称、用户设备 MAC 地址、IP 地址、连接信号强度、SSID、在线时间、上传数据量、下载数据量、上网方式、认证状态。

D-Link
AC管理控制器

1.02.040
admin 安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

2.4G用户列表

5G用户列表

上网黑白名单

云控管理

系统配置

当前位置：用户管理 > 5G用户列表

所属组： 所属设备： IP地址： MAC地址： 信号强度： SSID：

共 1 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往第 页

所属组	所属设备	用户名称	MAC地址	IP地址	信号强度	SSID	在线时间	上传数据	下载数据	上传速度	下载速度	上网方式	认证状态
	S桌		AC:BC:32:7F:26:B9	172.18.170.73	-75 dbm	DLINK	3分54秒	0 M	0 M	0 b	2.00 K	未初始化	

首先使用顶部的查找筛选工具对特定用户的进行查找，可选填写项有：所属设备、IP 地址、信号强度、SSID，填写任意一项或多项后，点击“查询”，在下方的列表会显示当前查询结果。

当前位置：用户管理 > 5G用户列表

所属组： 所属设备： IP地址： MAC地址： 信号强度： SSID：

查询到相应的设备后，在设备信息最后的操作一栏有三个选项按钮，分别代表 A—组织连接所有 AP、X—阻止连接当前 AP、S—阻止连接当前 AP 的当前 SSID，点击

对应按钮即可实现对应功能：

所属组	所属设备	用户名	MAC地址	IP地址	信号强度	SSID	在线时间	上传数据	下载数据	上传速度	下载速度	上网方式	认证状态
	S桌		AC:BC:32:7F:26:B9	172.18.170.73	-75 dbm	DLINK	3分54秒	0 M	0 M	0 b	2.00 K	未初始化	

③ 上网黑白名单

功能描述：通过过滤 MAC 地址来阻止或允许 AP 设备中的终端用户上网。过滤的方式为：允许如下客户端、阻止如下客户端。

操作说明：选择需要做控制的 SSID，然后选择过滤方式：允许或阻止如下客户端，添加需要控制的设备 MAC 地址，点击保存。设置成功。

当前位置：用户管理 > 上网黑白名单

选择网络名称 (SSID):

SSID ▼

过滤方式:

关闭 ▼
 关闭
 允许如下客户端
 阻止如下客户端

D-Link

AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

2.4G用户列表

5G用户列表

上网黑白名单

云控管理

系统配置

当前位置: 用户管理 > 上网黑白名单

选择网络名称 (SSID):

SSID

过滤方式:

关闭

MAC列表:

每行一个MAC地址,格式: "MAC;描述", 以英文分号分隔

保存

取消

11.1.7 云控管理

该模块为用户提供将 AP 设备连接第三方服务器进行统一管理、认证上网、信息备份、审计监控等功能，用户可选择使用旁路认证或与我公司自带的服务器网址进行对接。

① 旁路认证设置

该功能为用户提供了除本地认证（PPPOE 等）方式上网的第三方服务器在线认证功能，可与第三方认证平台进行对接。

首先需要与第三方后台服务网站协商是否可以申请开启旁路认证服务，然后填写认证服务器地址和认证服务器端口，然后打钩选中需要管理的 SSID，点击保存生效

第129页

D-Link

AC管理控制器

1.02.040

admin安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

云控管理

旁路认证设置

云控管理

系统配置

当前位置: 云控管理 > 旁路认证设置

认证服务器地址:

client.dlinkwifi.com.cn

认证服务器端口:

5500

设备序列号:

RTAC_CFLV1V20101000010C

SSID

状态:

☐ 启用

SSID 1

状态:

☐ 启用

SSID 2

状态:

☐ 启用

SSID 3

状态:

☐ 启用

SSID 4

状态:

☐ 启用

SSID 5

状态:

☐ 启用

保存

重新连接

刷新状态

② 云控管理

该功能由内部提供的云平台对 AP 实现线上集中管控，可以实现认证上网等功能。

向云平台请求授权并得到授权后，在状态一栏点击启用，最后提交设置

当前位置: 云控管理 > 云控管理

设备管理设置

状态:

☐ 启用

提交设置

重新连接

刷新状态

当前状态信息

功能没开启!

11.1.8 系统配置

提供了 AC 统一管理系统的各项系统参数的设置，包括 AP 系统管理、DHCP 服务器防御、访问端口、登录用户名和密码等参数的设置以及查看 AC 系统的用户接入日志和系统日志。

① AP 系统管理

该功能提供了 AP 的查找筛选功能，并展示了当前在网 AP 的各项系统参数，包括 AP 设备的名称、IP 地址、型号、固件版本号、定时重启时间、定时开启 WIFI 时间。

首先输入需要进行操作的 AP 设备的名称，IP 地址，型号或版本号，点击查询：

当前位置：系统配置 > AP系统管理

组名： 设备名： 型号： 版本号： [查询](#)

共: 3 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往 第 页 [刷新](#)

找到对应的 AP 后，可对 AP 进行如下操作：

D-Link
AC管理控制器

1.02.040
admin 安全退出

当前位置：系统配置 > AP系统管理

组名： 设备名： 型号： 版本号： [查询](#)

共: 3 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往 第 页 [刷新](#)

<input type="checkbox"/> 全选 <input type="checkbox"/> 反选	组名	设备名	型号	版本号	定时重启状态	定时重启时间
<input type="checkbox"/>		门口AP(172.18.170.197)	DI-810WO-2020-10	14 R(65278)	关闭	每周[] 每天[]
<input type="checkbox"/>		DI-810WO(172.18.170.174)	DI-810WO-2019-11	28 R(65278)	关闭	每周[] 每天[]
<input type="checkbox"/>		S桌(172.18.170.174)	DI-810WO-2020-10	14 R(65278)	关闭	每周[] 每天[]

[选中设备恢复默认设置](#) [重启选中的设备](#)
 定时重启: ☐ 激活 每周: 每天: [定时重启选中的设备](#)
 所选版本: 未选择 [重新选择](#) [升级选中的设备](#)

AP固件升级: [选择文件](#) 未选择任何文件 [上传](#) [查看或删除版本](#)

系统可使用内存: 23.94 M (大概值, 内存可能被全部作为缓存)

选中设备恢复默认设置：恢复出厂时的默认设置

重启选中的设备：重新启动设备的系统

定时重启：勾选“激活”按钮，在每周按钮中勾选需要重启的天数和选择每天重启的时段，点击“定时重启选中的设备”，设置生效

定时开启 wifi：勾选“激活”按钮，在每周按钮中勾选需要开启 wifi 的天数和选择每天开启 wifi 的时段，点击“定时开启 WIF 选中的设备”，设置生效

AP 固件升级：点击“选择文件”按钮，在电脑文件夹中选择升级文件，点击“上传”上传到 AC 服务器。上传完成后在所选版本后点击“重新选择”，最后点击“升级选中的设备”按钮。稍等片刻点击“刷新”，会看到 AP 版本号处已经变更，说明 AP 升级成功

所选版本：未选择 [重新选择](#) [升级选中的设备](#)

AP固件升级： [选择文件](#) 未选择任何文件 [上传](#) [查看或删除版本](#)

<input type="checkbox"/> 全选 <input type="checkbox"/> 反选 组名	设备名	型号	版本号	定时重启状态	定时重启时间
<input type="checkbox"/>	门口AP(172.18.170.197)	DI-810WO-2020-10	14 R(65278)	关闭	每周[] 每天[]
<input type="checkbox"/>	DI-810WO(172.18.170.174)	DI-810WO-2019-11	28 R(65278)	关闭	每周[] 每天[]
<input type="checkbox"/>	S桌(172.18.170.174)	DI-810WO-2020-10	14 R(65278)	关闭	每周[] 每天[]

② DHCP 服务器防御

该功能可以防止在内网中存在多个 DHCP 服务器时，AP 误获取到非对应的 DHCP 服务器地址下发的 IP 地址。可以保证 AP 获取到的地址段准确性和稳定性。

操作步骤

首先需要在 DHCP 服务器防御选项里选择“启用”，然后在本设备 DHCP 服务器选项选择“加入”。若只要 AP 获取本 AC 系统下发的地址，则“其他信任 DHCP 服务器列表”一项可不填，点击“保存”后可自动默认添加本 AC 系统的 MAC 地址；若需要添加额外的 DHCP 服务器，则需要在“其他信任 DHCP 服务器列表”后添加服务器的 MAC 地址。如图：

当前位置：系统配置 > DHCP服务器防御

③ WEB 访问设置

提供了修改 AC 统一系统的设备名称、访问端口、管理员用账户和密码、guest 账户和密码功能。

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

云控管理

系统配置

AP系统管理

DHCP服务器防御

WEB访问设置

用户接入日志

系统日志

当前位置: 系统配置 > WEB访问设置

设备名称:

HTTP访问端口:

800

远程访问端口:

800

(为0表示关闭远程访问)

管理员:

admin

管理员密码:

管理员密码确认:

启用guest用户:

☐ 开启 ☒ 关闭

guest用户:

guest

guest用户密码:

guest用户密码确认:

保存

取消

操作步骤

- 修改设备名称：AC 管理平台的名称。

当前位置: 系统配置 > WEB访问设置

设备名称:

- 修改访问端口：HTTP 访问端口即本地内网访问端口，远程访问端口即从外网访问 AC 管理平台的端口。

HTTP访问端口:

远程访问端口: (为0表示关闭远程访问)

- 修改管理员账号和密码

管理员:

管理员密码:

管理员密码确认:

➤ 启用和修改 guest 账号密码:guest 账户即仅有访问权限的游客账户，此账户没有配置 AC 管理器权限，只能查看当 AC 控制器的配置信息。

启用guest用户: ☐ 开启 ☒ 关闭

guest用户:

guest用户密码:

guest用户密码确认:

修改完成后，点击“保存”

④ 用户接入日志

显示了当前所有用户的连接状态，包括连接时间、MAC 地址、设备名称。

操作说明：

在“记录用户接入日志”一项选择“启用”此功能，然后点击“保存”按钮，使能此功能

当前位置: 系统配置 > 用户接入日志

记录用户接入日志:

设备名称: MAC地址:

开启功能后，便会逐渐看到列表记录了用户登录信息

D-Link
AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

云控管理

系统配置

AP系统管理

DHCP服务器防御

WEB访问设置

用户接入日志

系统日志

当前位置: 系统配置 > 用户接入日志

记录用户接入日志: ☐ 启用

设备名称: MAC地址:

共: 73 条记录 当前 1/8 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往第 页

编号	时间	MAC地址	设备名称	状态
0	10-16 18:50:51	82:59:A6:40:61:DB	门口AP	undefined
1	10-16 18:51:19	82:59:A6:40:61:DB	门口AP	undefined
2	10-16 18:55:17	EA:85:C0:DE:B3:91	门口AP	undefined
3	10-16 18:56:13	EA:85:C0:DE:B3:91	门口AP	undefined
4	10-17 08:47:55	88:40:3B:1F:D9:E5	门口AP	undefined
5	10-17 08:48:51	88:40:3B:1F:D9:E5	门口AP	undefined
6	10-17 09:33:54	14:A5:1A:02:62:56	门口AP	undefined
7	10-17 09:34:08	14:A5:1A:02:62:56	门口AP	undefined
8	10-17 11:50:36	E6:5F:2D:82:27:9C	门口AP	undefined
9	10-17 11:51:18	E6:5F:2D:82:27:9C	门口AP	undefined

[导出用户接入信息](#)

⑤ 系统日志

显示了当前 AC 统一管理系统的启动、上线、登录、错误等日志

D-Link
AC管理控制器

1.02.040

admin 安全退出

配置向导

系统信息

2.4G设备管理

5G设备管理

用户管理

云控管理

系统配置

AP系统管理

DHCP服务器防御

WEB访问设置

用户接入日志

系统日志

当前位置: 系统配置 > 系统日志

共: 8 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [尾页](#) 前往第 页

编号	时间	事件
0	10-14 16:10:21	系统启动成功
1	10-14 16:13:55	设备[DI-810WO]IP[172.18.170.197]上线
2	10-15 11:52:56	设备[DI-810WO]IP[172.18.170.197]重新上线
3	10-16 17:26:57	设备[DI-810WO]IP[172.18.170.174]上线
4	10-16 17:35:09	设备[DI-810WO]IP[172.18.170.174]上线
5	10-19 10:35:08	设备管理 向设备[赵鑫桌]IP[172.18.170.174]下发参数
6	10-19 10:35:08	设备[赵鑫桌]接收SSID VLAN ID参数成功
7	10-19 10:35:08	设备[赵鑫桌]接收配置参数成功1

11.2 PPTP 配置

PPTP 服务端支持从计算机连接到 VPN 路由器，也支持路由器连接路由器的“网对网”连接模式。

网对点连接模式主要用于在外单独的电脑访问公司内部场景。比如：企业员工出差在外，需要每天晚上将出差报告发送到主管的企业内部邮箱，同时收取企业内部邮箱里面的邮件，这时候就需要用到 PPTP VPN，出差员工通过 VPN 拨号进入企业内网来完成上述操作。

网对网连接模式主要用于当存在总公司和子公司建立内网隧道连接的情况。当 VPN 隧道建立后，总公司的服务端和子公司的客户端内所有的设备可以互相访问。

11.2.1 PPTP 服务

打开左侧“PPTP 配置—PPTP 服务”，设置如图所示：

➤ PPTP 服务端设置

PPTP服务 PPTP用户 PPTP客户端

状态: ☒

端口:

起始地址:

结束地址:

分配给客户的DNS:

高级选项: ☒ 支持MPPE加密 ☐ 支持CCP压缩

分配给VPN用户的IP地址

提交设置 取消设置

状态：关闭服务，打开服务；

端口：默认 1723。不推荐修改。

地址范围：分配给 VPN 用户的 IP 地址；

分配给用户的 DNS：可根据服务器所在城市的 DNS 进行分配；

提交设置：点击提交，服务器配置生效。

11.2.2 PPTP 用户（PPTP 客户端设置）

此界面用户创建 PPTP 客户端账号及密码，具体设置如下图所示：

PPTP服务 PPTP用户 PPTP客户端

—

用户状态: ☒

用户名:

密码:

指定IP: ?

类型: ☒ VPN 隧道 ☐ VPN 借线 ?

客户端内网网段: ?

备注:

确定 取消

分公司只需要在其路由器上点击 **VPN 设置—PPTP 客户端**，开启 PPTP VPN 客户端，并设置上该账号及密码、PPTP 服务器的 IP 地址、**工作模式**处选择**隧道模式**、路由网段处按要求填写 VPN 服务器端内网的网段，然后点击**保存生**

效。路由器将自动拨通 VPN，实现总公司与分公司两个局域网间直接相互通信。

如果在类型处选择的是网对点，则适用于出差员工。出差人员通过在自己的笔记本电脑上启动 VPN 客户端程序，使用 PPTP 服务端当前 WAN 口 IP 或路由器的动态域名和相应的用户名、密码配置客户端，就可以通过拨入公司内网。

➤ 用户状态

显示启用 VPN 客户端进入局域网的用户信息，包括用户名、连接时间、虚拟接口、IP 地址、数据包个数等。

刷新

状态	登录名	密码	指定IP	类型	连接时间	虚拟接口	分配IP	拨入IP	接收数据	接收数据包	发送数据	发送数据包	备注	操作
----	-----	----	------	----	------	------	------	------	------	-------	------	-------	----	----

11.2.3 PPTP 客户端

➤ PPPTP 客户端

打开左侧“vpn 服务器—PPTP 客户端”，连接类型选择 PPTP，然后分别填入 PPTP 服务器已设置好的参数，设置如图所示：

选择您要设置的VPN: **VPN1** VPN2 VPN3 VPN4

VPN1设置

PPTP状态: ☒

出口接口: ?

用户名称:

用户密码:

服务器地址: ?

服务器端口:

高级选项: ☐ 支持MPPE加密 ☐ 支持CCP压缩

MTU设置:

工作模式: ☒ 隧道模式 ☐ 借线模式 ?

路由网段: ?

外网带宽: KByte(千字节) **带宽值参考**

KByte(千字节)

确定

取消

外网接口：可选择默认，默认接口为 ALL；

用户名称：PPTP 服务器端中 VPN 用户管理设置的用户名；

用户密码：PPTP 服务器端中 VPN 用户管理设置的密码；

服务器地址：外部域名或者外部 IP；

工作模式：根据 PPTP 服务器—VPN 用户管理中用户选择的工作模式选择，这里我们选择隧道模式；

路由网段：服务器端内网网段。

保存生效：以上设置完后保存生效即可。

➤ PPTP 客户端状态

当用户连接 PPTP 时，客户端状态可显示登录用户的信息，如下图所示：

VPN1状态

连接类型： off

连接状态：

出口广域网：

设备名：

本地IP地址：

对端IP地址：

DNS：

MTU：

连接时间：

连 接

断 开

11.3 IPSEC 网对网

11.3.1 IPSEC 网对网

采用 IPSec 协议来实现远程接入的一种 VPN 技术，IPSec 全称为 Internet Protocol Security，是由 Internet Engineering Task Force (IETF) 定义的安全标准框架。

IPSec 网对网 IPSec 隧道状态 IPSec 点对网 L2TP IPSec

IPSec 网对网配置:



名称:

IPSec 网对网主动连接:



保持连接:

☒ 用ping保持连接

本地隧道接口:

广域网1

模式:

☒ 主模式 ☐ 野蛮模式 ?

本地网络:



子网掩码:

255.255.255.0

远程隧道地址:



远程网络:



子网掩码:

255.255.255.0

IKE验证模式:

IKE-PSK

PSK 密钥:

高级参数



IKE DH Group:

☐ group1 ☒ group2 ☐ group5

IKE加密:

☒ 3DES ☐ DES ☐ AES128 ☐ AES192 ☐ AES256

IKE认证:

☒ MD5 ☐ SHA1

IKE有效时间:

3600 秒

PFS:

☒ 启用 ☐ 禁用

PFS Group:

☐ group1 ☒ group2 ☐ group5

IPSEC数据加密:

☒ ESP-3DES ☐ ESP-DES ☐ ESP-AES128 ☐ ESP-AES192 ☐ ESP-AES256

IPSEC数据认证:

☒ MD5 ☐ SHA1

数据传输SA有效时间:

3600 秒

IP压缩:

☒ 启用 ☐ 禁用

状态： 启用

最大连接数： VPN 最大接入隧道数量。具体数量会根据设备型号有所差异

名称： 类似备注，自己定义即可

主动连接： 保持打钩即可

保持连接： 保持打钩即可

本地隧道接口： 选择作为 VPN 连接的外网接口

模式：

主模式：正常情况下使用的模式，如果服务端和客户端的外网 IP 都是固定的公网 IP，则选择此模式即可。

野蛮模式：当使用正常模式无法成功连接或客户端的外网 IP 不是公网 IP 时，使用野蛮模式。

本地网络： 本地内网 IP 网段

子网掩码： 本地内网的子网掩码

本地身份 ID 类型： 若上方模式选择了主模式，则选择 NONE 即可；若选择了野蛮模式，且本端为**客户端**时，请选择 **FQDN** 类型

远程隧道类型： 填写**对端**的外网实际线路类型。选择静态地址时，必须填写对端的公网 IP 地址

远程网络： 填写对端的内网网段

子网掩码： 填写对端的内网子网掩码

远端身份 ID 类型： 当上述远程隧道类型选择静态时，保持 NONE 即可；当上述远程隧道类型为动态地址，则必须要选择 FQDN 类型。

IEK 验证模式： 加密类型。保持 IKE-PSK 默认

PSK 密钥：添加用于 VPN 相互建立的密码（数字或者字母都可），服务端和客户端必须保持一致

11.3.2 IPSEC 点对点网

IPSec 网对网 IPSec 隧道状态 IPSec 点对点网 L2TP IPSec

IPSec点对点网服务：☐

本地网络：

子网掩码：

IKE验证模式：

IKE-PSK ▼

PSK 密钥：

高级参数 ▼

IKE DH Group：

☐ group1 ☒ group2 ☐ group5

IKE加密：

☒ 3DES ☐ DES ☐ AES128 ☐ AES192 ☐ AES256

IKE认证：

☒ MD5 ☐ SHA1

IKE有效时间：

3600 秒

PFS：

☒ 启用 ☐ 禁用

PFS Group：

☐ group1 ☒ group2 ☐ group5

IPSEC数据加密：

☒ ESP-3DES ☐ ESP-DES ☐ ESP-AES128 ☐ ESP-AES192 ☐ ESP-AES256

IPSEC数据认证：

☒ MD5 ☐ SHA1

数据传输SA有效时间：

3600 秒

IP压缩：

☒ 启用 ☐ 禁用

提交设置

状态：勾选启用

本地网络：本地内网的网段

子网掩码：内网的子网掩码

IKE 验证模式：IKE-PSK 默认

PSK 密钥：即 VPN 相互建立连接的密码

11.3.3 IPSEC 状态

配置 IPSEC VPN 后，可在此查看当前 VPN 链接的具体信息和当前状态等。



11.3.4 L2TP IPSec

为解决苹果设备的 VPN 连接兼容性问题，使用 L2TP 协议建立 VPN 连接。

IPSec 网对网 IPSec 隧道状态 IPSec 点对网 L2TP IPSec

L2TP IPSec 服务: ☐ 最大支持 16 个客户端

PSK 密钥:

端口: ?

客户端地址: ?

客户的DNS: ?

提 交

L2TP IPSec 服务: 点击开启

L2TP 最大连接数: L2TP 服务支持的 VPN 隧道数量。(不同型号设备数量有所差异)

PSK 密码: VPN 隧道互相建立的密码，必须和用户端保持一致

端口: VPN 本地连接端口，保持默认即可。

L2TP 客户端地址范围: 给连接成功后的 VPN 客户端分配范围中的地址

分配给客户的 DNS: 分配给客户端的 DNS

填写好后，点击“提交”生效

11.3.5 L2TP 用户



The image shows a web-based configuration form for an L2TP user. At the top left is a blue circular icon with a minus sign. Below it, the label '用户状态:' (User Status) is followed by a toggle switch that is currently turned on. Below this, there are three input fields: '用户名:' (Username), '密码:' (Password), and '备注:' (Remarks). At the bottom of the form are two buttons: a blue '确定' (Confirm) button and a grey '取消' (Cancel) button.

用户状态：默认为启用，勾选则禁用

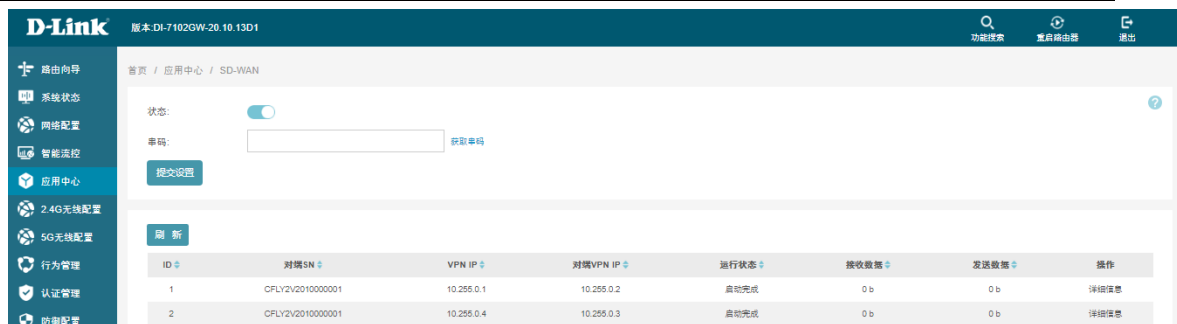
用户名：VPN 连接用户的账号

密码：VPN 连接用户的密

备注：根据需要自行填写，可以为空

11.4 SD-WAN

SD-WAN 应用目前代表了 SDN 技术最为关注的应用，它旨在帮助用户降低广域网（WAN）的开支和提高网络连接灵活性。用户只要关心 WAN 口的连接，SD-WAN 方案，为企业总部、分支机构、跨广域网的连接提供高效的基于 SDN 的解决方案。



状态：启用，提交设置，即可。（请参阅附录二 SD-WAN 配置指南）

12 系统维护

管理路由相关参数设置，包括 ping 检测、网络唤醒、固件升级等。

12.1 Ping 检测

用于方便管理者了解网络对外联机的实际状况，可以借由此功能判断网络的状态。



输入地址：填写您需要检测的 IP 或者域名。

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

Ping 包计数：ping 数据包的检测个数。

Ping 包大小：每个 ping 数据包的大小限制。

12.2 网络唤醒

此功能主要用于远程开启计算机而用（被唤醒的计算机必须先开启远程唤醒设置）。

首页 / 系统维护 / 网络唤醒

IP地址	MAC地址	接口	类型	状态	操作
192.168.0.110	F8:9A:7B:2D:0B	局域网	动态	正常	唤醒
192.168.0.111	7C:D6:51:F4:F7:F9	局域网	动态	正常	唤醒
192.168.0.110	B4:0B:44:EB:E8:1D	局域网	动态	正常	唤醒
192.168.0.120	7E:A9:FC:AC:51:58	局域网	动态	正常	唤醒

将需要远程唤醒的机器 MAC 地址填入“MAC 地址列表”栏，然后点击“唤醒”按钮。

如果您的计算机支持远程唤醒，而且已经开启了远程唤醒功能，那么远程的计算机将会被唤醒。

12.3 系统控制

用于将路由参数导入导出，恢复默认参数以及对路由执行重启操作。

恢复系统参数

选择需要恢复的系统参数文件:

浏览

恢复

恢复默认设置

恢复默认设置

重启路由器

重启路由器

系统参数备份

发送参数备份到邮箱:



保存参数到本地

确定

定时重启路由器

状态:



确定

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

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

恢复默认设置：选择“恢复路由默认设置”，并点击确定。恢复之后路由器会自动

重启，重启完之后请使用默认 IP 及用户名/密码登录路由。路由器默认 IP 为 192.168.0.1，默认用户名为 admin 密码为 admin。

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

定时重启路由器：激活，启用之后设定的规则将只会在指定的时间段内生效。（每周：您可以设置一周的哪几天生效；每天，您可以设置一天的哪些时段生效。）

12.4 系统配置

此功能可对设备系统名称和时间进行设定。

首页 / 系统维护 / 系统配置

路由名称:	<input type="text" value="DLINK"/>
主机名称:	<input type="text" value="DLINK"/>
所在域名:	<input type="text"/>
系统内网域名:	<input type="text"/> ?
路由时间:	2020-10-19 12:23:54
模式:	<input type="text" value="自动"/> ▼
时区选择:	<input type="text" value="UTC+08:00 中国, 香港, 澳大利亚西部, 新"/> ▼
自动夏时制时间:	<input checked="" type="checkbox"/>
高级参数	▼
自动更新:	<input type="text" value="每4小时"/> ▼
在需要时触发连接:	<input type="checkbox"/>
NTP时间服务器:	<input type="text" value="默认设置"/> ▼
指定接口:	<input type="text"/> ?

12.5 系统更新

该界面可以对路由器进行固件升级和应用特征库更新操作。



固件升级：升级前请先确认好路由器的当前版本，看是否需要进行升级操作。点击“浏览”按钮，选择新版本的存放路径之后，按下“升级”按钮开始升级操作。升级时间一般会在二分钟左右完成，各型号升级时间也不一致。

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

设定特征库更新模式，其中包含手动更新模式和自动更新模式。

手动更新即自行点击“立即更新”按钮，并不勾选“自动更新”启用功能。

自动更新，即选择“启用”按钮，设定时间。在预设时间里，系统将自动更新特征库。

12.6 申请控制

申请控制是用于外网访问设备的功能配置。点击申请控制，刷新状态，当前信息显示连接成功后，外网用户使用固定的云平台 WiFi 服务器地址加上这里提供的代理端口号，即可实现对设备的控制。

首页 / 系统维护 / 申请控制

云平台认证:



云平台地址:

http://cloud.dlinkwifi.com.cn

开启此功能表示您接受[免责声明](#)（请点开阅读）

提交设置

立即申请

关闭控制

未开启此功能

刷新

Copy

重启后自动申请控制:



描述:

远程访问URL发送到邮箱:



定时发送模式:



提交设置

附录一 无线路由-无线相关设置

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

1. 基本设置

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

首页 / 2.4G无线配置 / 基本设置

无线模块:	<input checked="" type="checkbox"/>	?
发射无线信号:	<input checked="" type="checkbox"/>	
网络模式:	11b/g/n 混合	?
选择SSID:	SSID1 +	
网络名称1:	D-Link_BJinn	?
编码:	GB2312	?
安全设置:	WPA/WPA2个人	?
WPA 算法:	TKIP / AES	?
共享密钥:	20200102	? 随机
密钥更新间隔:	3600 秒	
高级参数	>	

MAC地址:	60:80:82:10:00:30	
无线频道:	2422MHz (频道 3)	?
	频道3	扫描附近AP所使用的频道
高级参数	∨	
带宽:	20MHz (抗干扰模式)	?
运行模式:	<input checked="" type="radio"/> 普通 <input type="radio"/> 增强	
无线发射功率:	100	?
主动断开客户端阈值:	基于信号强度: 0 dBm	?
	基于接收速率: 0 Mbits	?
组播:	关闭	

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

发射无线信号：打开/关闭无线网络

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

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

网络名称 1/2/3/4：您可以给一个无线设备设置多个网络名称（SSID），再通过 AP 外隔离，实现不同的 SSID 内的无线用户无法互相访问，实现无线虚拟局域网。设置含有的参数：SSID 名称，隐藏，隔离，均衡模式和安全设置。均衡模式分为：用户数均衡、信号强度均衡、流量均衡；加密类型分为：开放式、共享式、WEP AUTO、WPA、WPA 个人、WPA2、WPA2 个人、WPA/WPA2 个人、WPA1WPA2；WPA 算法类型分为：TKIP、AES；共享密钥支持除特殊符号外的字母与数字任意组合。

安全设置：为了提高安全性和稳定性，建议加密设置选择“WPA/WPA2 个人”，WPA 算法选择“TKIP/AES”。

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

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

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

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

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

网络名称1:	<input type="text" value="D-Link_BJinn"/>	?
编码:	<input type="text" value="GB2312"/>	?
安全设置:	<input type="text" value="WPA企业"/>	?
WPA 算法:	<input type="text" value="AES"/>	?
密钥更新间隔:	<input type="text" value="3600"/> 秒	
Radius服务器:	<input type="text" value="0"/> : <input type="text" value="1812"/>	
通信密钥:	<input type="text" value="DLINK"/>	<input type="button" value="随机"/>
会话超时:	<input type="text" value="0"/>	
高级参数	>	

WPA 算法：进行认证过程中所用的算法类型。

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

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

共享密钥：访问 RADIUS 服务的密码。

会话超时：当会话超时达到多少时，radius 服务器会自动断开该连接。

五、WPA 个人：路由器将采用基于共享密钥的 WPA 模式。

网络名称1:	<input type="text" value="D-Link_BJinn"/>	?
编码:	<input type="text" value="GB2312"/>	?
安全设置:	<input type="text" value="WPA个人"/>	?
WPA 算法:	<input type="text" value="AES"/>	?
共享密钥:	<input type="text" value="20200102"/>	<input type="button" value="随机"/>
密钥更新间隔:	<input type="text" value="3600"/> 秒	
高级参数	>	

WPA 算法：进行认证过程中所用的算法类型。

共享密钥：无线用户接入时所需要的口令。

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

六、WPA2：与 WPA 模式相类似。

WPA 算法：进行认证过程中所用的算法类型。

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

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

预认证：启用可以提高无线接入的速度。

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

共享密钥：访问 RADIUS 服务的密码。

会话超时：当会话超时达到多少时，radius 服务器会自动断开该连接。

七、WPA2 个人：路由器将采用基于共享密钥的 WPA2 模式。

WPA 算法：进行认证过程中所用的算法类型。

共享密钥：无线用户接入时所需要的口令。

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

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

九、WPA1 企业/WPA2 企业：与 WPA 企业的设置方法一样。

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

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

无线发射功率：设置无线发射功率大小。

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



— 无线MAC地址过滤 —

过滤方式：☐ 禁止使用过滤器 ☐ 允许如下客户端 ☒ 阻止如下客户端

描述：

MAC地址：

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

禁止使用过滤器：不使用 MAC 地址过滤功能。

允许如下客户端：只允许列表中添加的 MAC 地址的设备连接无线。

阻止如下客户端：禁止列表中添加的 MAC 地址的设备连接到无线网络。

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

MAC 地址：客户端设备的 MAC 地址。

2.WDS 设置

WDS（无线分布式系统），是一个在 IEEE 802.11 网络中多个无线访问点通过无线互连的系统。它允许将无线网络通过多个访问点进行扩展。这种可扩展性能，使无

线网络具有更大的传输距离和覆盖范围。共分为三种连接方式：自学习模式，桥接模式和中继模式。若选择关闭则不启用 WDS 功能。

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

首页 / 2.4G无线配置 / WDS 设置

WDS 模式: 桥接模式 ▼ BSSID:

扫描无线AP 扫描

SSID:

MAC地址:

加密类型: NONE ▼

频道: 3 ?

MAC 地址：需要连接到的设备的 BSSID 地址。

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

密钥：相应的密码，至少为 8 个字符。

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

WDS 模式: 中继模式 ▼ BSSID:

扫描无线AP

SSID:

MAC地址:

加密类型: WPA-PSK/WPA2-PSK ▼

密钥:

频道: 3 

MAC 地址：即为所需要连接 AP 的 BSSID 地址。

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

密钥：相应的密码，至少为 8 个字符。

3 用户列表

显示当前连接到路由的无线设备信息。

首页 / 2.4G无线配置 / 用户列表 

IP地址	MAC 地址	信号强度	发送速率	接收速率
192.168.0.51	C0:D6:62:FA:B5:C5	-61 dBm	139.7 Mbps	115.9 Mbps
192.168.0.120	7E:A9:FC:AC:61:B8	-69 dBm	123.8 Mbps	20.8 Mbps

4 终端过滤：

可通过无线 MAC 地址对无线接入端做允许或阻止的设置

选择网络名称 (SSID):

D-Link_BJinn

无线MAC地址过滤

过滤方式:

☒ 禁止使用过滤器

☐ 允许如下客户端

☐ 阻止如下客户端

+

描述	MAC地址	操作
----	-------	----

—

描述:

MAC地址:

确认

取消

附录二 SD-WAN 应用相关设置

如何通过 SDWAN 让公司 A 和公司 B 内部互连

一、云平台注册流程如下：

1、注册用户自助管理平台 <http://cloud.dlinkwifi.com.cn>



2、注册成功后登录平台(注册可通过手机注册帐号，首次登录须先绑定路由器)

Ps:使用平台注册好的帐号，在路由器登录页面选择"帐号登录"即可绑定设备。

账号

密码

联系人

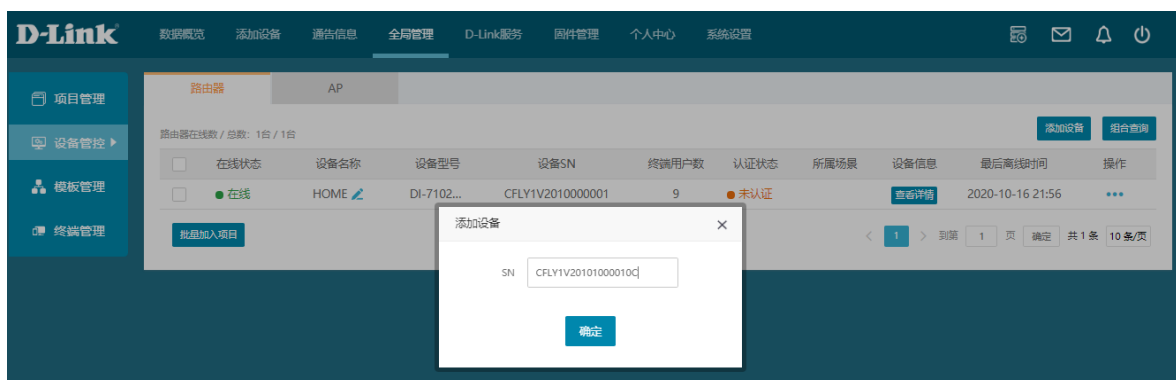
手机号

验证码

地址

[已有账号? 去登录](#)

绑定须注意，一定要填写路由器的型号和 SN 才可以完成绑定。



设备绑定成功后，回到自助平台即可看到设备在线。(对设备进行管理以及远程等操作)



3、登录 D-Link 云平台(可通过自助平台“D-Link 服务” 点击进入 SD-WAN 设置页面



二、SD-WAN 配置流程如下：

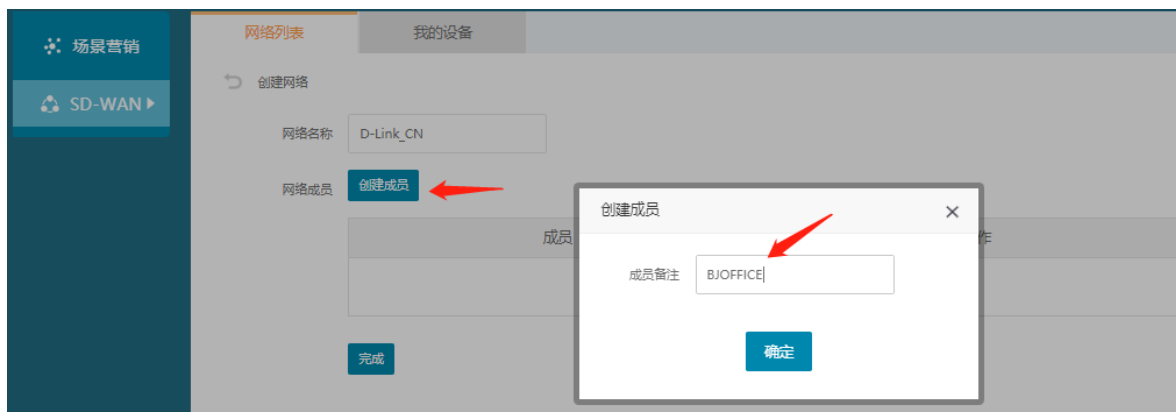
1、点击创建网络



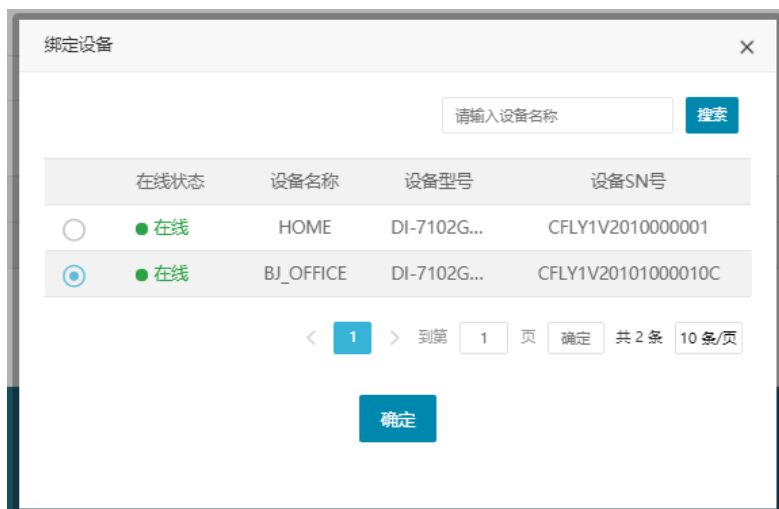
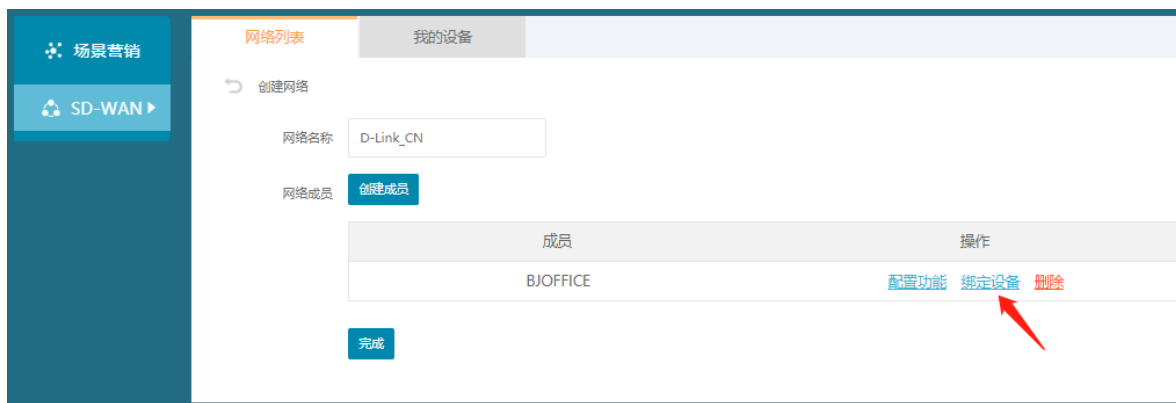
添加网络成员及此 SD-WAN 组名称



设置成员备注信息



通过点击绑定设备，在弹出的列表选中需要绑定的设备



设备绑定成功后，点击配置功能，来配置相应参数

两种配置类型：一种是网对网模式，一种是网对点借线模式。



2、网对网模式配置如下：

开启内网 （两端设备自行添加本地路由网段）

公司 A 内网如下：

配置功能

×

开放内网

☒

内网网段

格式:192.168.1.0/24 多个网段用";"隔开

允许访问此内网的成员

☒ 全部成员 ☐ 指定成员

借线上网

☐

确定

公司 B 内网如下：

配置功能

×

开放内网

☒

内网网段

格式:192.168.1.0/24 多个网段用";"隔开

允许访问此内网的成员

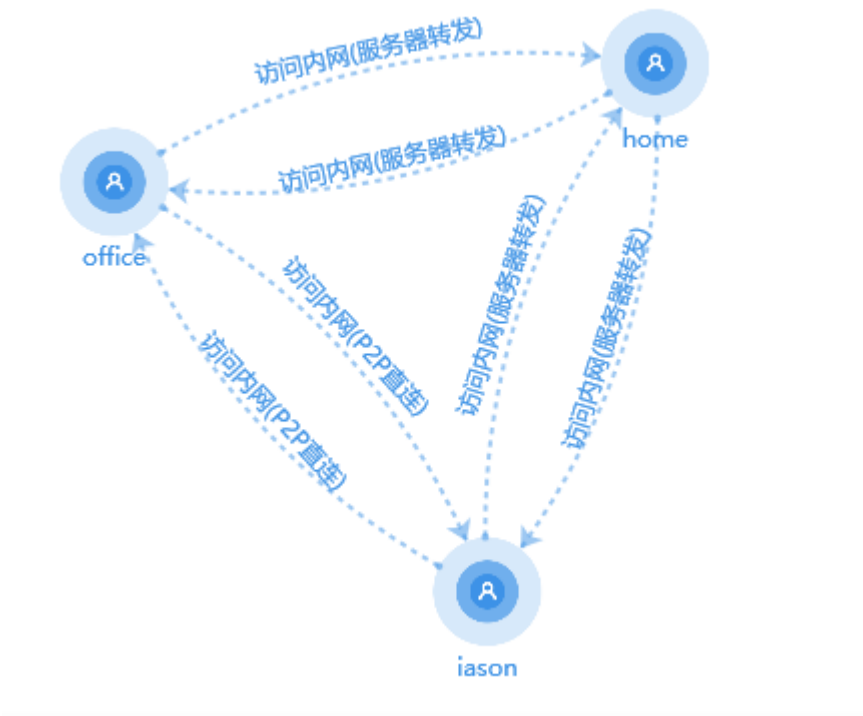
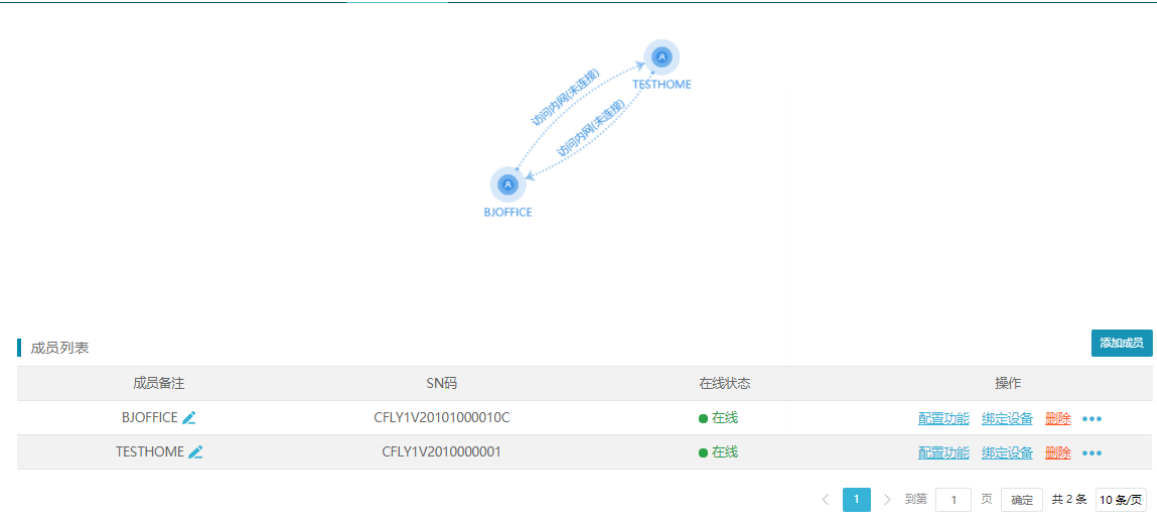
☒ 全部成员 ☐ 指定成员

借线上网

☐

确定

参数配置成功后，可通过两端内部电脑互 ping 对端网关来检测是否成功。（当然也可以进入路由器 SDWAN 中来查看连接状态）



路由器连接状态如下：

首页 / 应用中心 / SD-WAN

状态: ☒

串码: [获取串码](#)

[提交设置](#)

[刷新](#)

ID	对端SN	VPN IP	对端VPN IP	运行状态	接收数据	发送数据	操作
1	CFLY1V2010000001	10.255.0.2	10.255.0.1	启动完成	0 b	0 b	详细信息
2	CFLY1V2010000001	10.255.0.3	10.255.0.4	启动完成	0 b	0 b	详细信息

3、借线模式（仅需要一端开启借线模式）



谁想借线，就选这个节点，选择成功后点击确定，这时借线客户端会自动搜索指定的节点来进行连接。

此时在借线端电脑浏览器上输入 ip138.com 来查询外网 ip。如果显示对端外网 ip，此时说明借线模式连接成功。

