



路 由 心 智 未 来

飞鱼星路由器通用型用户手册

VER: 2013

成都飞鱼星科技开发有限公司
VOLANS TECHNOLOGY DEVELOPMENT CO., LTD.

声 明

Copyright © 2002-2014

飞鱼星科技开发有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。



飞鱼星、**VOLANS**、**飞鱼星**、**VOLANS** 均为飞鱼星科技开发有限公司的商标。对于本手册中出现的其他商标，由各自的所有人拥有。

由于产品版本升级或其它原因，本手册内容会不定期进行更新，为获得最新版本的信息，请定时访问公司网站。该手册仅为路由器通用用户操作指导文档，产品实际功能以固件版本本身为准。飞鱼星科技试图在本资料中提供准确的信息，但对于可能出现的疏漏概不负责。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

物品清单

在包装箱完整的情况下，开启包装箱。箱内应包含如下各项：

- 一台路由器主机
- 一条交流电源线
- 一条网线
- 一本快速安装手册
- 无线天线（仅无线设备提供）



注意：

- 如果发现有任何配件损坏或遗漏，请及时与经销商联系。
- 本手册为飞鱼星路由器通用用户操作指导文档，适用于所有飞鱼星 VE、VR 和 VN 系列路由器。
- 部分功能可能会因产品系列不同而有差异，请以产品本身为准。

目录

第一章	网络基础知识	10
1.1	局域网入门.....	10
1.2	IP 地址	10
1.3	子网掩码.....	10
第二章	产品介绍.....	11
第三章	硬件安装.....	12
3.1	安装路由器.....	12
3.1.1	路由器的两种安装方式	12
3.2	认识和连接路由器	13
3.2.1	面板布置	13
3.2.2	设备安装	14
3.2.3	参考以下方式使用路由器为您提供的功能.....	14
第四章	快速安装指南	16
4.1	配置计算机网络设置	16
4.2	配置您的路由器	17
4.2.1	内网设置	18
4.2.2	外网设置	19
4.2.3	重新启动路由器.....	25
第五章	详细安装指南.....	26

5.1 启动和登录.....	26
5.2 系统状态.....	27
5.2.1 系统信息	27
5.2.2 网络接口	28
5.2.3 内网监控	28
5.2.4 流量统计	31
5.2.5 应用分析	32
5.2.6 系统日志	32
5.3 基础设置.....	34
5.3.1 快速配置	34
5.3.2 基本选项	34
5.3.3 内网配置	36
5.3.4 外网配置	37
5.3.5 DHCP 服务器	42
5.3.6 端口管理	46
5.4 无线设置.....	48
5.4.1 基本设置	49
5.4.2 安全设置	50
5.4.3 客人网络	54
5.4.4 高级设置	55
5.4.5 WDS 设置.....	56
5.4.6 客户端状态	58

5.5 上网行为管理.....	59
5.5.1 IP 地址组	59
5.5.2 行为管理策略.....	60
5.5.3 聊天软件高级设置	67
5.5.4 防火墙设置.....	69
5.5.5 WEB 认证	72
5.6 网络安全	75
5.6.1 攻击防御	75
5.6.2 连接限制	77
5.6.3 IP/MAC 绑定	78
5.6.4 MAC 地址过滤	80
5.7 QoS 流量控制	81
5.7.1 智能流控	81
5.7.2 固定流控	82
5.8 高级选项.....	83
5.8.1 端口映射	83
5.8.2 静态路由	86
5.8.3 策略路由	87
5.8.4 地址转换	89
5.8.5 域名转发	93
5.8.6 动态域名	94
5.8.7 UPnP 设置.....	96

5.9 虚拟专网	97
5.9.1 PPTP 客户端	97
5.9.2 PPTP 服务端	99
5.10 系统工具	101
5.10.1 管理选项	101
5.10.2 网络诊断	103
5.10.3 用户管理	104
5.10.4 策略升级	105
5.10.5 固件升级	105
5.10.6 备份恢复配置	106
5.10.7 恢复出厂配置	107
5.10.8 重新启动	108
第六章 特殊功能介绍	108
6.1 时间组（高端产品支持）	108
6.2 WPS 设置（仅带 WPS 按钮的设备支持）	109
6.3 PPPOE 服务器（部分型号支持）	110
6.4 USB 扩展应用（带 USB 接口设备支持）	113
6.4.1 设备状态	113
6.4.2 共享服务	114
6.4.3 3G 上网服务	114
6.5 端口镜像（部分型号支持）	116
6.6 即插即用(部分型号支持)	117

6.7 SNMP 客户端 (3050 平台不支持)	118
6.8 SVPN (仅 V7 平台支持)	118
6.9 IPSec 网对网 (部分型号支持)	122
6.10 IPSec 点对网 (部分型号支持)	124
6.11 L2TP IPSec (部分型号支持)	125
附录 A 路由器选配电缆说明	131
附录 B WindowsXP 环境下的 TCP/IP 配置	132
附录 C 路由器固件升级失败恢复步骤	135
附录 D 常见问题解答	136

第一章 网络基础知识

1.1 局域网入门

路由器是指能将两个网络连接起来的设备，路由器能连接局域网或者一组电脑到互联网，处理并校验在网络中传输的数据。

路由器网络地址转换技术（NAT）保护网络中的电脑，使互联网用户侦测不到，这是保护局域网行之有效的方法。路由器检查互联网端口的数据包，只转发允许通过的数据包到内网，从而增加了局域网的安全性。

1.2 IP 地址

IP 是建立在互联网协议上的。每个基于 IP 的网络设备如计算机，打印服务器和路由器等都需要一个 IP 地址来识别它在网络中的位置。

有两种为网络设备分配 IP 地址的方法：静态地址分配和动态地址分配。

静态地址即手工为网络设备分配的固定 IP 地址，此地址会一直有效到你关闭设备为止。一般将固定地址分配给需要经常访问的网络设备。

动态地址即 DHCP 服务器自动为网络中设备分配的 IP 地址，此地址一般都有生存期，如果超过生存期，DHCP 服务器会再次为其分配新的 IP 地址。

1.3 子网掩码

子网掩码和 IP 地址一样，都是 32 位，它不能单独存在，必须结合 IP 地址一起使用。子网掩码的作用是将某个 IP 地址划分成网络号和主机号两部分。这对于采用 TCP/IP 协议的网络来说非常重要，只有通过子网掩码，才能表明一台主机所在的子网与其他子网的关系，使网络正常工作。

第二章 产品介绍

欢迎您使用飞鱼星路由器！

飞鱼星 VE 系列（上网行为管理路由器）专为中小企业、政府机关、教育及科研机构等用户设计，是具备“上网行为管理”、“多 WAN 路由器”以及“VPN 网关”多重功能的新一代硬件网络接入设备。它能帮助企业对员工使用因特网的情况进行监控、生成报表并进行管理；帮助企业提高员工的生产率、节省网络带宽并且减少法律风险；为您提供完善的上网行为管理、智能带宽管理和多线负载均衡解决方案。

飞鱼星 VR 系列（多 WAN 防火墙路由器）专为中小型网吧、企业、小区、学校等用户设计，支持双线接入和带宽汇聚，智能均衡功能可自动寻找最优的路径和负载模式，不但彻底解决网络互通的瓶颈问题，而且极大减少管理工作量。

飞鱼星 VN 系列（全千兆多 WAN 网吧路由器）是飞鱼星科技为网吧行业量身定制的电信级网吧专用路由器，支持多线接入、智能负载均衡、智能策略路由、智能 QoS、端口镜像、VLAN、VPN 等功能；具备丰富的网吧专用功能和安全特性，能有效防御 ARP 病毒，具备出色的防病毒抗攻击能力；所有接口自动识别网线和交叉线；还提供精细化的内网管理功能，具备电信级的稳定设计，是网吧用户的理想选择。

第三章 硬件安装

3.1 安装路由器

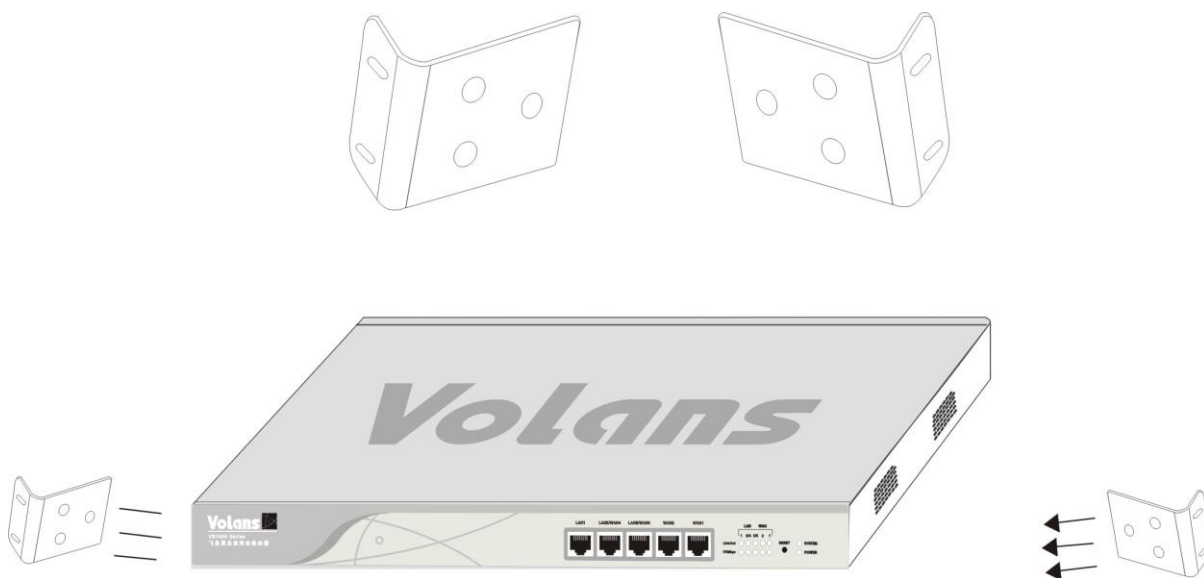
3.1.1 路由器的两种安装方式

1, 安装到工作台上

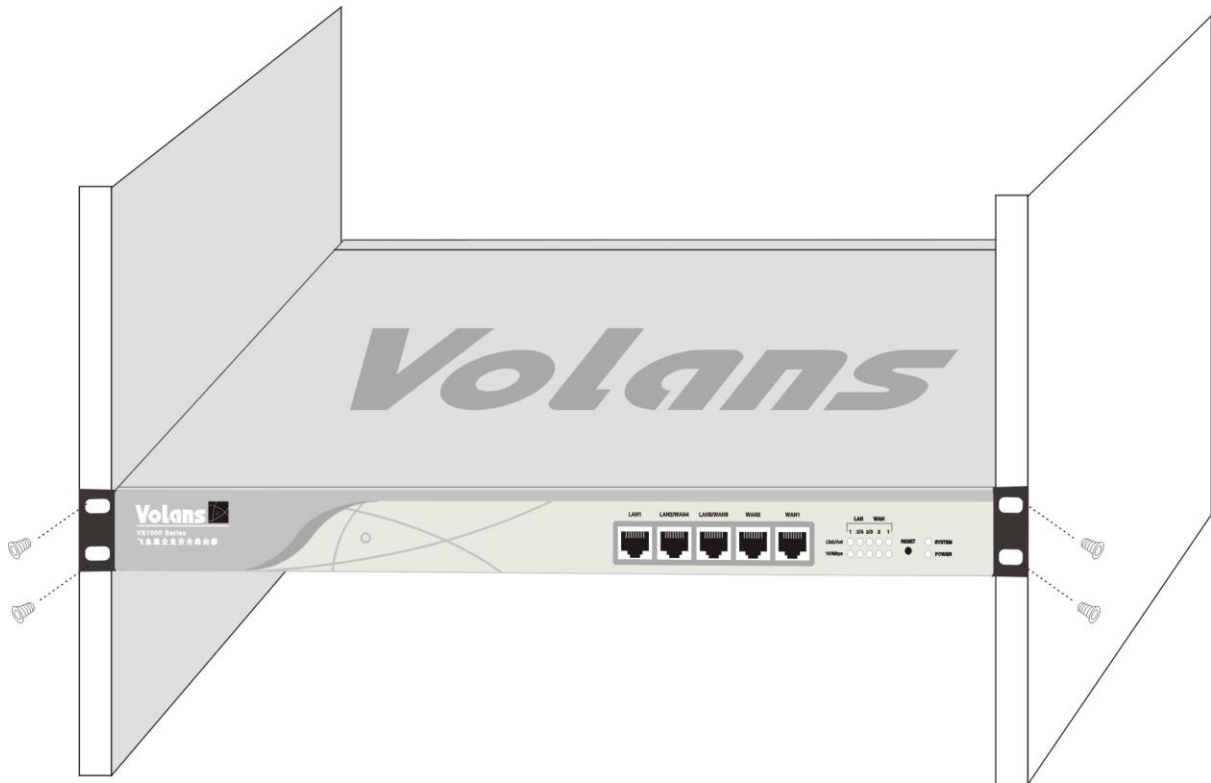
- 确保工作台的平稳性和良好接地，不要在路由器上放置重物或其他电器设备，并在路由器周围留出至少 10 厘米的散热空间。

2, 安装到机架上

- 飞鱼星 13 和 19 英寸路由器按照标准机架尺寸设计，并配置固定附件。请参照下图进行安装。



当您安装完所提供的配件后，可直接将路由器安装在标准机架上，如下图所示：



3.2 认识和连接路由器

3.2.1 面板布置



注意：设备图片为示意图，非实物图。



POWER	电源指示灯，当路由器加电后该灯常亮
System	系统正常运行时，以 1Hz 的速率闪烁。熄灭或常亮时异常
WAN1	路由器外网网络接口 1
WAN2	路由器外网网络接口 2
LAN3/WAN3	路由器内网网络接口 3 或者外网网络接口 3

LAN2/WAN4	路由器内网网络接口 2 或者外网网络接口 4
LAN1	路由器内网网络接口 1
RESET 按钮	按住按钮后松开，路由器恢复出厂设置

后面板

电源插口：接交流 220V，50Hz 电源；

电源开关：打开关闭路由器电源。

3.2.2 设备安装

安装环境要求

请不要将本产品放置在潮湿、粉尘的环境中；

请不要将本产品置于阳光下暴晒或置于其他热源附近。

推荐使用环境

工作温度：0℃到 40℃；

存储温度：-40℃到 70℃；

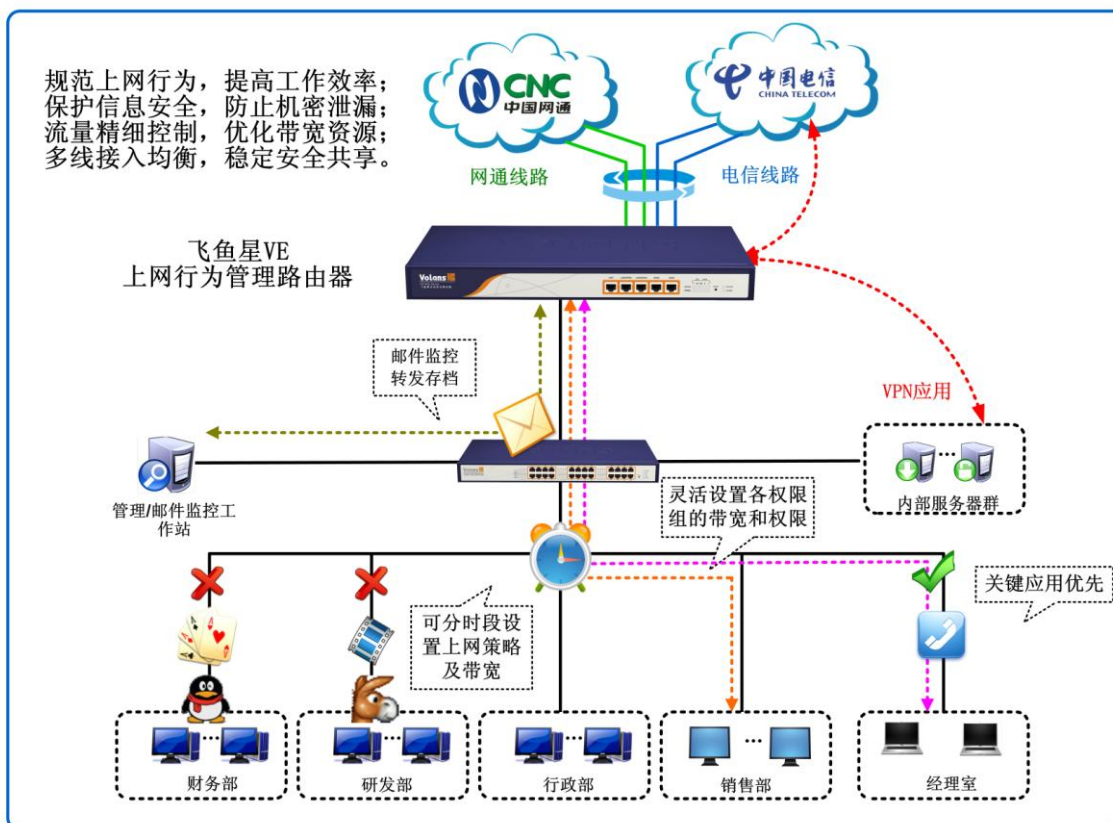
工作湿度：10%到 90%不凝结；

存储湿度：5%到 90%不凝结。

提示：为了您的安全，安装时请关闭电源，拔掉电源插头，保持双手干燥！

3.2.3 参考以下方式使用路由器为您提供的功能

- 多线接入及上网行为管理应用示例



- 支持多线接入，自动实现带宽叠加、线路备份、智能负载均衡，
- 分支机构和出差人员利用 VPN 功能可接入内部网络；
- 网页过滤、关键字过滤、IP 过滤等多种控制功能，禁止员工在上班时间访问与工作无关的网站、聊天、游戏、影视、BT 下载等；
- 灵活的 IP 用户组、时间段设置，为不同级别的用户分配不同的上网权限和带宽；
- 保证关键应用和重要部门的带宽资源和服务优先级；
- 整合多种安全功能，提供一体化的安全机制。

第四章 快速安装指南

4.1 配置计算机网络设置

1、打开路由器电源，等待片刻，当路由器前面板的 system 灯匀速闪烁以后，表示路由器已经进入工作状态，可以接受配置了；

2、请正确配置计算机的网络设置，并加载 TCP/IP 协议；

3、设置计算机的 IP 地址在 192.168.0.2-192.168.0.254 范围内（即与路由器内网地址在同一网段内，比如 192.168.0.2），子网掩码为 255.255.255.0，默认网关为 192.168.0.1，DNS 为 192.168.0.1；

4、依次点击计算机的开始菜单 程序 附件 命令提示符，您现在可以使用下面的命令来检查您的计算机和本产品是否正常连通。在命令提示符下输入：

```
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
```

如果出现以上显示，表示网络连接正确，可以进行下一步操作。如果屏幕提示为：

```
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

说明设备未正确安装，可以按照下面的步骤来检查：

1、设备的物理连接是否正确？

与计算机网卡相连的双绞线的另外一端必须接路由器的内网口(比如 LAN1 口)，并且网线两端的网络接口的指示灯必须正确点亮。

2、计算机的 TCP/IP 协议是否设置正确？

您的计算机 IP 地址必须为 192.168.0.x (x 的范围是 2-254) ,子网掩码为 255.255.255.0(即在同一网段内), 默认网关为 192.168.0.1。

4.2 配置您的路由器

本产品提供基于浏览器的配置界面，打开浏览器，在浏览器的地址栏中输入路由器默认 IP 地址：http://192.168.0.1，如下图所示：



按回车键，下图所示的用户登录界面将会出现在您的面前：



请输入用户名：admin；密码：admin，选择语言类别为 English、简体中文或繁体中文后点击“登录”按钮，您将会看到以下界面：



4.2.1 内网设置

点击“基础设置” “内网配置”选项。

在“内网配置”页面里，可以设置路由器的内网“IP地址”和“子网掩码”。

IP地址：通常是内网计算机指的网关地址。

子网掩码：通常是内网计算机指的子网掩码。

然后点击“保存”按钮，便完成了对路由器内网的设置，如下图所示：

内网配置

内网配置 | 内网扩展配置

IP地址
例如：192.168.0.1

子网掩码
例如：255.255.255.0

接下来我们继续对外网进行设置。

4.2.2 外网设置

点击“基础设置” “外网配置”选项，路由器多个WAN口的配置方法完全相同，都支持三种连接方式：静态地址线路、PPPOE拨号线路、动态获取地址线路。

A. 如果您的第一条线路所用的连接方式是静态地址线路，请用鼠标单击WAN1右边的“编辑”按钮，在“类型”下拉菜单中，选中“静态线路”。配置的参数都是由ISP提供的。

举例如下：

外网配置->WAN1

规则列表

类型	静态线路 ▼		
IP地址	192.168.10.1		
子网掩码	255.255.255.0		
缺省网关	192.168.10.100		
DNS服务器1	61.139.2.69	[电信]	[新联通]
DNS服务器2	202.98.96.68		
网络服务商	<input checked="" type="radio"/> 电信 <input type="radio"/> 新联通 <input type="radio"/> 自动识别 <input type="radio"/> 不指定		
线路带宽	上行: 10	Mbps	下行: 10 Mbps
MTU设置	<input checked="" type="radio"/> 自动 <input type="radio"/> 手动 1500		
工作模式	<input type="radio"/> 启用路由模式		
	<input checked="" type="radio"/> 启用NAT模式		
	<input type="radio"/> 启用桥接模式 (启用后, WAN1和LAN之间实现网桥功能)		
通断检测	<input type="radio"/> 不启用 <input checked="" type="radio"/> 网关检测 <input type="radio"/> DNS检测 <input type="radio"/> 定时切换		
路由器根据WAN网关是否可达来决定线路通断。			

保存

返回

- 1、“IP 地址”，比如填写：192.168.10.1；
- 2、“子网掩码”，比如填写：255.255.255.0；
- 3、“缺省网关”，比如填写：192.168.10.100；

- 4、“DNS 服务器 1”，比如填写：61.139.2.69；
- 5、“DNS 服务器 2”，比如填写：202.98.96.68；
- 6、“网络服务商”，比如申请的是电信的光纤；
- 7、“线路带宽”，比如申请的光纤的带宽是 10M，那么上行填写 10,下行填写 10；
- 8、“MTU 设置”，我们保持默认设置“自动”；
- 9、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改；
- 10、“通断检测”，保持默认设置“网关检测”，或者选择“不启用”，如果选择不启用，则路由器不对此线路的通断作判断。

网关检测：如果 WAN 口到网关这一跳有故障，则选择网关检测效率最高。这个也是默认配置，推荐大多数客户使用。

DNS 检测：用于第 N (N>=1) 跳的故障。使用时必须正确配置静态线路的 DNS 地址，并填写检测域名。

定时切换：某些地区网络服务提供商存在零点断网问题。比如双线接入，WAN1 线路每天凌晨 0:00 断网，早上 7:00 通网，则配置定时切换断线时间为：23:59，上线时间为：7:02。在断线期间，内网所有的上网数据全部由另外一条未断的线路出访，内网不会产生由于零点断网引起的“掉线”问题。

完成后点击下面的“保存”按钮即可。您将会看到如下图所示的界面：

外网配置

外网接口		智能均衡策略	
接口	状态	接口信息	编辑
WAN1	已配置	静态线路 IP:192.168.10.1/255.255.255.0 GW:192.168.10.100	
WAN2	未配置		

B 如果您的第一条线路所用的连接方式是 PPPoE 拨号线路，请用鼠标单击 WAN1 右边的“编辑”按钮，在“类型”下拉菜单中，选中“PPPoE 拨号线路”。配置的参数都是由 ISP 提供的。举例如下：

外网配置->WAN1

规则列表

类型	PPPoE拨号线路 ▾
拨号类型	普通拨号 ▾
PPPoE帐号	88888888
PPPoE口令	●●●●●●
高级设置	
按需拨号	当线路空闲 <input type="text"/> 秒后自动断线 (留空表示永远在线)
网络服务商	<input checked="" type="radio"/> 电信 <input type="radio"/> 新联通 <input type="radio"/> 自动识别 <input type="radio"/> 不指定
线路带宽	上行: <input type="text"/> Mbps 下行: <input type="text"/> Mbps
<input type="radio"/> 启用路由模式	
工作模式	<input checked="" type="radio"/> 启用NAT模式
通断检测	<input checked="" type="radio"/> 不启用 <input type="radio"/> 网关检测 <input type="radio"/> DNS检测 <input type="radio"/> 定时切换



保存

返回

- 1、“PPPoE 账号”，比如填写：88888888；
- 2、“PPPoE 口令”，请正确填写 ISP 给您的密码；
- 3、“按需拨号”，一般在这里保持默认设置，留空；
- 4、“网络服务商”，比如申请的是电信的线路；
- 5、“线路带宽”，比如您申请的线路带宽是 2M，那么请根据 ISP 提供的上行与下行速率的准确数值填写。比如上行填写 1，下行填写 2；
- 6、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改；
- 7、“通断检测”，保持默认设置“网关检测”，或者选择“不启用”，可参考静态线路说明。

完成后点击下面的“保存”按钮即可。您将会看到如下图所示的界面：

外网配置

外网接口		智能均衡策略	
接口	状态	接口信息	编辑
WAN1	已配置	PPPoE拨号线路	
WAN2	未配置		

C. 如果您的第一条线路所用的连接方式是动态获取地址线路，请用鼠标单击 WAN1 右边的“编辑”按钮，在“类型”下拉菜单中，选中“DHCP 线路”。配置的参数都是由 ISP 提供的。举例如下：

外网配置->WAN1

规则列表

类型

DHCP线路

主机名称

某些以太网DHCP线路服务提供商可能需要，通常留空。

网络服务商

☒电信 ☐新联通 ☐自动识别 ☐不指定

线路带宽

上行: Mbps 下行: Mbps

MTU设置

☒自动 ☐手动

工作模式

☐启用路由模式
☒启用NAT模式

通断检测

☐不启用 ☒网关检测 ☐DNS检测 ☐定时切换
路由器根据WAN网关是否可达来决定线路通断。

保存

返回

1、“主机名”，请根据 ISP 的具体需求填写。提示：某些以太网动态获取地址线路服务提供商可能需要，通常留空；

2、“网络服务商”，比如申请的是电信的线路；

- 3、“线路带宽”，比如您申请的线路的带宽是 10M，那么请根据 ISP 提供的上行与下行速率的准确数值填写。比如上行填写 10,下行填写 10；
- 4、“MTU 设置”，保持默认设置“自动”；
- 5、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改；
- 6、“通断检测”，保持默认设置“网关检测”，或者选择“不启用”，可参考静态线路说明。

完成后点击下面的“保存”按钮即可，您将会看到如下图所示的界面：

外网配置

外网接口		智能均衡策略	
接口	状态	接口信息	编辑
WAN1	已配置	DHCP线路	
WAN2	未配置		

以上操作便完成了对 WAN1 的配置。

如果是单 WAN 接入，以上操作便完成了对路由器内网和外网的配置，已可以正常使用。如果是多 WAN 接入，就还需要依次对 WAN2/WAN3/WAN4 进行配置，其具体配置方法请参考 WAN1 配置进行操作即可。

当多 WAN 配置完毕以后，点击“外网配置” “智能均衡策略”，将模式设置为“智能均衡”：

智能均衡是飞鱼星路由器的一大特色，路由器将自动识别线路并调用路由策略，使多条线路工作在最佳状态下。

默认线路类型选项有“电信”和“新联通”。比如 WAN1 和 WAN2 口分别是网通与新联通接入，此时如果内网访问教育网的资源，并且选择默认网络服务商“电信”，则访问教育网的数据从电信线路出访。

自定义策略，通过使用策略路由、静态路由等选项来配置策略路由的高级路由方案。

保存后如下图所示：

外网配置

外网接口

智能均衡策略

☒ 智能均衡

默认线路类型 ☒ 电信 ☐ 新联通
路由器将自动识别线路并调用路由策略

☐ 自定义策略

您可以使用 策略路由, 静态路由 选项来配置策略路由的高级路由方案

保存

4.2.3 重新启动路由器

完成以上操作后，请将路由器重新启动，点击“系统工具” “重新启动”选项，点击“确定”按钮。系统会提示您路由器开始重启，并且有进度显示，大约过 30 秒，system 灯匀速闪烁以后，路由器就进入工作状态了。

恭喜您！您已经完成路由器的配置。可以在浏览器输入 www.adslr.com 来测试路由器。如果您想对路由器有更多的了解，请查看第五章“详细安装指南”。

第五章 详细安装指南

本章节即将为客户提供路由器常用功能介绍和示例，部分特殊功能如端口镜像、即插即用等请参见第六章 [特殊功能介绍](#)。

5.1 启动和登录

本产品默认 IP 地址为：192.168.0.1，子网掩码为：255.255.255.0，管理帐户是：admin，密码是：admin。在启动并登录以后，浏览器会显示本产品的 WEB 管理界面。如下图所示。



左侧菜单栏显示了产品支持的所有功能，点击某个选项即可进行相应的功能配置，下面将详细讲解各个选项的功能。

5.2 系统状态

5.2.1 系统信息

此界面主要通过系统信息、路由器负荷、端口状态、应用分析和流量统计五个部分为用户展示

路由器使用情况：



产品型号：路由器的型号。

版本型号：路由器的当前固件版本。本例是 Beta 1027[2012-09-06 08:48:25]。

默认 MAC：路由器出厂时内网口默认的 MAC 地址。

路由器系统时间：如果时间服务器故障导致不能正常更新路由器系统时间，用户可以在“基本选项”中手动设置，一般情况下时间服务器默认自动更新。

路由器运行时间：路由器的连续工作时间。本例中显示路由器已经工作了 1 天,20 小时 41 分钟。

路由器负荷：路由器运行过程中当前的系统负荷，CPU 使用率在 0% - 40%之间属于正常，在 40%-100%之间属于繁忙。

端口状态：路由器所有端口的连接状态。

应用分析：所有连接客户端的网络应用情况。

流量统计：所有连接端口的流量情况。

5.2.2 网络接口

显示路由器当前网络接口详细信息。具体界面如下图所示：

网络接口

静态线路状态(WAN1)

网卡MAC地址	AA:BA:BB:BB:BB:BB
IP地址/掩码/网关	172.168.1.7 /255.255.255.0 /172.168.1.254
接收/发送数据	4024695497(3838.2MB)/414967862(395.7MB)
线路状态	正常

局域网接口状态

网卡MAC地址	5C:6C:95:03:15:A6
IP地址/子网掩码	192.168.16.16 /255.255.255.0
接收/发送数据	408078804(389.2MB)/4066014711(3877.7MB)

可以通过本界面观察路由器的广域网和局域网的连接状态以及接口信息。其中包括：设备接口的物理地址（MAC地址）、IP地址、子网掩码、网关地址、接受/发送数据量等信息。对于ADSL PPPoE拨号线路，提供手动断开与连接按钮，并显示已连接的时间。

5.2.3 内网监控

内网监控功能采用高速网络流量采集和分析技术，精确统计内网每个IP的累计流量、实时速度、网络连接数等关键指标，并可以按任意指标排名进行分析，实时了解各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。

内网监控的“管控”功能可以一键禁止内网异常活动IP上网。

启用内网分析：将分析服务状态选择为“启用”，并保存。如下图所示：

内网分析

内网分析结果

启用内网分析

禁止列表

分析服务状态

☒ 启用 ☐ 禁止

保存

启用内网分析功能后，就可以通过“内网分析结果”页面来查看当前内网主机连接的具体情况了。其中包括了连入内网的主机 IP 地址、累计下载、累计上传、下载速度、上传速度、连接数等信息。通过查看分析以上各种指标，可以详细掌握内部网络的具体运行情况。

具体界面如下图所示：

内网分析

内网分析结果

启用内网分析

禁止列表

主机	累计下载	累计上传	下载速度	上传速度	连接数	管控
192.168.16.255	0.01MB	0.00MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.162	0.65MB	0.11MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.150	3.25MB	0.99MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.122	161.53MB	7.81MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.50	257.78MB	48.84MB	0.00KB/s	0.00KB/s	10 查看	
192.168.16.152	791.98MB	89.37MB	0.00KB/s	0.00KB/s	5 查看	

共 6 条 << < 1 > >>

自动刷新

排序方式：可以将内网的活动主机按照主机 IP 地址、累计下载、累计上传、下载速度、上传速度、连接数等指标排名，本例是按照主机 IP 地址排名。点击蓝色字体“主机”即可。

管控：当您发现某个 IP 活动异常时，可以使用管控功能，单击管控绿色按钮即可阻断其访问外网。

内网分析

内网分析结果						
启用内网分析						
禁止列表						
主机	累计下载	累计上传	下载速度	上传速度	连接数	管控
192.168.16.255	0.00MB	0.00MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.162	0.10MB	0.04MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.150	0.21MB	0.19MB	0.00KB/s	0.00KB/s	1 查看	
192.168.16.122	103.82MB	4.15MB	0.00KB/s	0.00KB/s	0 查看	
192.168.16.50	145.14MB	28.82MB	0.00KB/s	0.00KB/s	14 查看	
192.168.16.152	575.54MB	39.33MB	0.00KB/s	0.00KB/s	14 查看	

共 6 条 << < 1 > >>

自动刷新

当您阻断某个 IP 地址上网后，您可以在禁止列表中看到该 IP：

内网分析

内网分析结果	
启用内网分析	
禁止列表	
主机	
192.168.16.50	

共 1 条 << < 1 > >>

删除所有规则

当您删除所有规则以后，此 IP 地址又可以正常上网了。

刷新：点击“手动刷新”按钮，路由器每 5 秒刷新一次排序列表；点击“自动刷新”按钮，路由器每 3 秒刷新一次排序列表。

通过点击相应的主机 IP 地址或者该主机的网络连接数，可以查看该主机的 NAT 连接数详情。

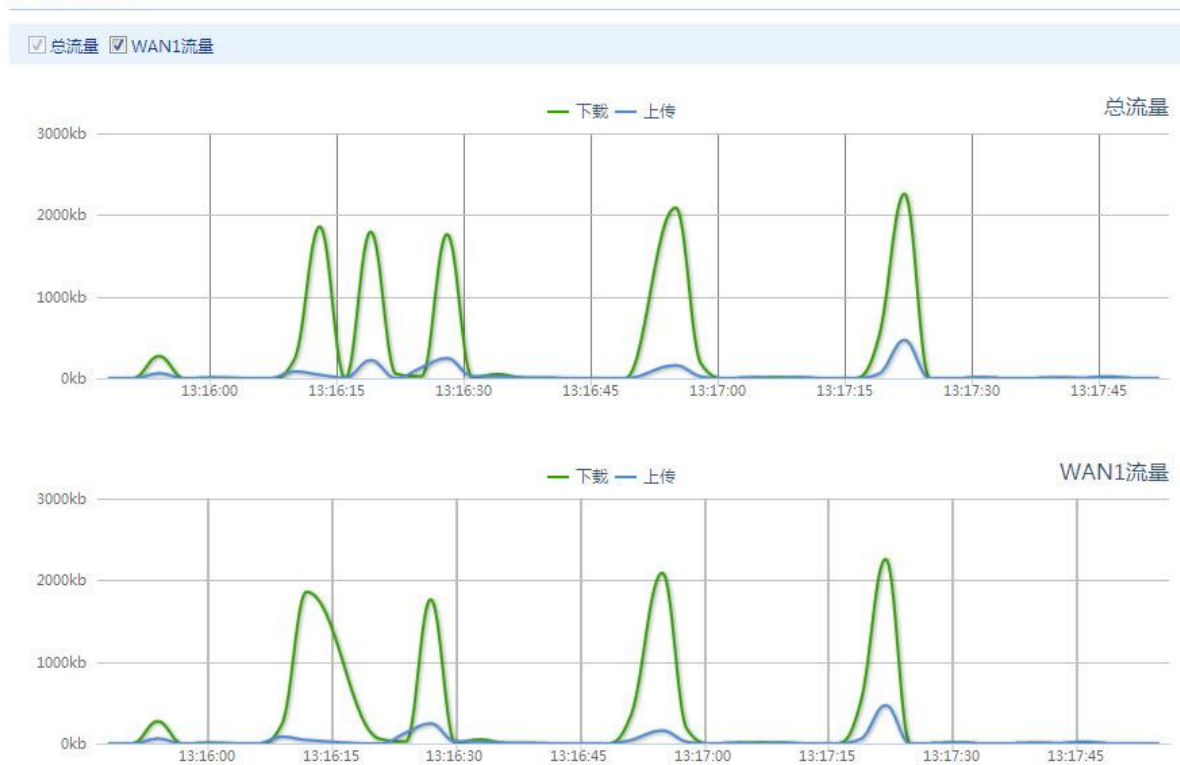
例如要查看 192.168.0.50 的网络连接数，点击“查看”出现如下图所示的界面：

主机分析结果				
协议	源地址	接口	目标地址	连接时间
TCP(unknown)	192.168.16.50:1057	WAN1	192.168.0.140:8000	2012-09-18 08:55:39
TCP(unknown)	192.168.16.50:1915	WAN1	192.168.0.241:30001	2012-09-18 09:58:36
TCP(http)	192.168.16.50:1231	LAN	192.168.16.16:80	2012-09-18 15:56:16
UDP(unknown)	192.168.16.50:138	LAN	192.168.16.255:138	2012-09-18 15:56:14
TCP(http)	192.168.16.50:1232	LAN	192.168.16.16:80	2012-09-18 15:56:16
TCP(http)	192.168.16.50:1090	WAN1	220.181.124.14:80	2012-09-18 15:54:46
TCP(http)	192.168.16.50:1233	LAN	192.168.16.16:80	2012-09-18 15:56:17
TCP(http)	192.168.16.50:1236	LAN	192.168.16.16:80	2012-09-18 15:56:27
TCP(unknown)	192.168.16.50:1911	WAN1	192.168.0.241:1433	2012-09-18 09:58:28
TCP(unknown)	192.168.16.50:1910	WAN1	192.168.0.241:1433	2012-09-18 09:58:28
TCP(http)	192.168.16.50:1235	LAN	192.168.16.16:80	2012-09-18 15:56:17
TCP(http)	192.168.16.50:1218	WAN1	192.168.0.11:80	2012-09-18 15:55:53

5.2.4 流量统计

您可以通过实时的流量统计查看当前路由器各 WAN 口的负载情况。单击图例“上传”/“下载”可以切换单条曲线显示。您还可以在曲线图上单击鼠标左键拖动，对曲线进行缩放查看。

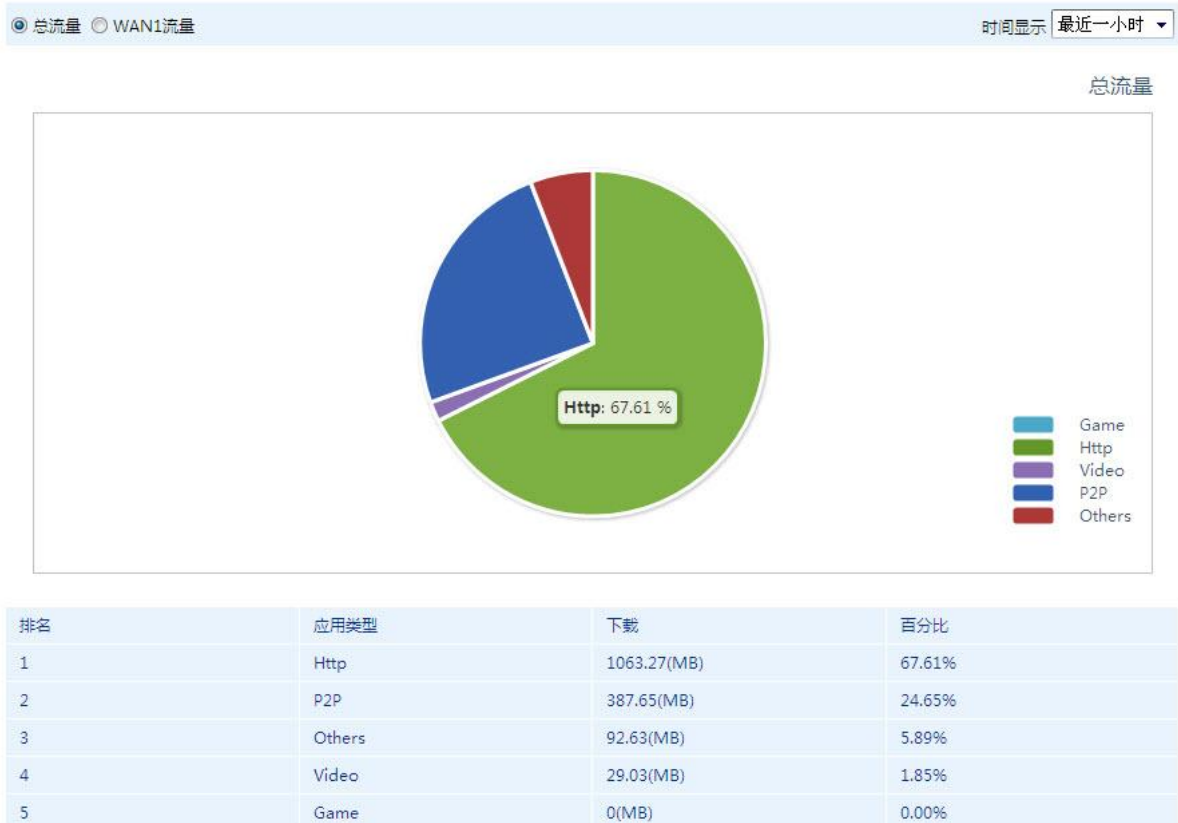
实时数据流量图



5.2.5 应用分析

此界面为您显示了路由器在“最近一小时”内总流量的饼状分析图，用户可以实时查看当前网络中主要应用类型所占流量百分比。

应用流量分析



5.2.6 系统日志

本界面提供的功能是将网络日志和系统日志通过标准协议传输到日志服务器上保存。日志服务器上运行“飞鱼星日志管理服务器软件”接收日志信息。

系统日志

系统日志

参数设置

☒ 启动系统日志服务☒ 启用日志服务器

192.168.0.111

日志服务器地址

在这里指定日志服务器的IP地址，系统将日志通过网络传送。

保存

启用系统日志服务：启用并保存后，重启路由器，将会在本界面中的“系统日志”选项看到系统日志。

启用日志服务器：指定日志服务器的IP地址，在日志服务器上结合“飞鱼星日志管理服务器软件”接收路由器产生的日志信息。请在官方网站下载该软件。

在路由器上查看系统日志信息，点击“系统日志”即可。如下图所示：

系统日志

系统日志

参数设置

时间	事件
2012-06-15 12:08:12	攻击防御：关闭外网端口保护功能
2012-06-15 12:08:12	攻击防御：允许外网UDP请求
2012-06-15 12:08:12	攻击防御：允许外网SYN请求
2012-06-15 12:08:12	攻击防御：启用内网病毒防御
2012-06-15 12:08:12	攻击防御：启用广播风暴抑制
2012-06-15 12:08:12	攻击防御：启用连接限制 1000
2012-06-15 12:08:12	攻击防御：启用内网监控分析功能
2012-06-15 12:08:12	攻击防御：启用内网SYNFLOOD保护 100
2012-06-15 12:08:12	攻击防御：启用内网UDPFLOOD保护 500
2012-06-15 12:08:13	攻击防御：启用内网ICMPFLOOD保护 50

共 61 条 << < 1 2 3 4 5 > >>

5.3 基础设置

5.3.1 快速配置

通过快速配置向导可以轻松地完成上网所需要的基本设置，只需选择您的线路接入类型并正确输入 ISP 提供的参数即可，点击完成后路由器自动重启生效。具体配置界面如下图所示：

快速配置

快速配置

WAN1配置

类型 静态线路

线路带宽 4M

IP地址 172.168.1.7

子网掩码 255.255.255.0

缺省网关 172.168.1.254

DNS服务器1 61.139.2.69

智能流控

流量控制 ☐ 启用智能流控

无线配置

无线密码

完成

5.3.2 基本选项

本界面包含路由器系统的一些基本配置信息，通常情况下，基本选项保持默认配置即可。如下图所示：

基本选项

功能配置

主机名称	<input type="text" value="router"/> 路由器的名称，注意不需要域名部。 例如：router
域名	<input type="text" value="mycorp.com"/> 例如：mycorp.com
时间服务器地址	<input type="text" value="210.72.145.44"/> [立即更新] 系统当前时间 2012-06-27 14:28:48
手动设置时间	<input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 时 <input type="text"/> 分
最大数据分段	<input type="checkbox"/> 启用手动设置最大数据分段，其值为： <input type="text"/>
支持端口回流	<input checked="" type="checkbox"/> 是否支持端口回流
H323穿透	<input checked="" type="checkbox"/> 是否支持H323穿透 该设置重启生效。
快速转发	<input checked="" type="checkbox"/> 启用快速转发 该功能可以大幅提升设备转发性能。

保存

主机名称：路由器的名称。可以在这里给路由器设定一个名称，默认是 router。

域名：路由器作为内网 DHCP 服务器时所使用的名称。

时间服务器地址：路由器通过时间服务器获取准确的系统时间。

手动设置时间：如果时间服务器故障导致不能正常更新路由器系统时间，用户可以自己设置时间。

最大数据分段：对于某些特殊地区的 ISP，用户只有手动设置最大数据分段以后才能更流畅地使用网络。最大数据分段的范围是 536-1460 字节，通常情况下保持默认即可，错误的数据分段会导致您的网络无法正常使用。

支持端口回流：当您访问内网主机对公网提供的服务时，可能出于习惯使用路由器 WAN 口 IP 地址进行访问，此时就需要端口回流功能来支持您的应用，打勾表示启用此功能；如果不启用此功能您只能使用服务器内网 IP 地址访问内网服务器。

H323 穿透：启用 H323 穿透后，一些基于 IP 的语音电话才可以正常使用。

快速转发：启用快速转发后，会提高路由器的转发性能，建议开启该功能。

5.3.3 内网配置

本界面用于配置内网接口参数，如下图所示：



注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。

内网配置

内网配置	
IP地址	<input type="text" value="192.168.0.1"/> 例如：192.168.0.1
子网掩码	<input type="text" value="255.255.255.0"/> 例如：255.255.255.0
<input type="button" value="保存"/>	

IP 地址：设置路由器内网口的 IP 地址，这个地址就是内网计算机的网关地址。该地址出厂时设置为 192.168.0.1，可以根据需要改变它，如果改变了路由器内网 IP 地址，重新启动路由器后才能生效。重启成功后，必须用新设置的 IP 地址才能登录路由器进行 WEB 界面管理。局域网中所有主机的 IP 地址都需与路由器内网口 IP 地址在同一网段，并且默认网关设置为路由器内网口 IP 地址才能正常上网。

子网掩码：根据内网规模选择，一般填 255.255.255.0 即可。路由器默认使用的子网掩码是 255.255.255.0，可以根据需要更改。

内网扩展配置：当内部有多于一个子网时可能会使用到该功能。可以通过点击“添加新配置”按钮，进入“添加配置”页面，为内网设置多个子网。点击“删除所有配置”按钮，可以删除所有的内网扩展配置。

添加配置界面，如下图所示：

内网配置

规则设置

IP地址	<input type="text" value="10.10.10.0"/>
子网掩码	<input type="text" value="255.255.255.0"/>

保存

返回

IP 地址：其功能与路由器内网地址基本一致，通常作为相应子网的网关使用。

子网掩码：根据子网规模选择，一般填 255.255.255.0 即可。路由器默认使用的子网掩码是 255.255.255.0，可以根据需要更改。

点击保存按钮后，界面如下图所示：

内网配置

内网配置

内网扩展配置

扩展IP地址	子网掩码	编辑	删除
10.10.10.0	255.255.255.0		
共 1 条 << < 1 > >>			

删除所有规则

添加新规则

5.3.4 外网配置

本界面用于配置 WAN 口的接口参数。每个 WAN 口都支持三种连接方式：静态地址线路、PPPOE 拨号线路、动态获取地址线路。



注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。

1. 静态地址线路

外网配置->WAN1

规则列表

类型	静态线路 ▼		
IP地址	172.168.1.7		
子网掩码	255.255.255.0		
缺省网关	172.168.1.254		
DNS服务器1	61.139.2.69	[电信]	[新联通]
DNS服务器2	202.98.96.68		
网络服务商	<input checked="" type="radio"/> 电信 <input type="radio"/> 新联通 <input type="radio"/> 自动识别 <input type="radio"/> 不指定		
线路带宽	上行: 10	Mbps	下行: 10 Mbps
MTU设置	<input checked="" type="radio"/> 自动 <input type="radio"/> 手动 1500		
	<input type="radio"/> 启用路由模式		
工作模式	<input checked="" type="radio"/> 启用NAT模式		
	<input type="radio"/> 启用桥接模式 (启用后, WAN1和LAN之间实现网桥功能)		
通断检测	<input type="radio"/> 不启用 <input checked="" type="radio"/> 网关检测 <input type="radio"/> DNS检测 <input type="radio"/> 定时切换		
	路由器根据WAN网关是否可达来决定线路通断。		

保存

返回

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

子网掩码：当前 IP 所对应的子网掩码，由网络服务商提供，可以向网络服务商询问获得。

缺省网关：当前 IP 所对应的网关，由网络服务商提供，可以向网络服务商询问获得。

DNS 服务器 1/DNS 服务器 2：填入网络服务商提供的 DNS 服务器 IP 地址，可以向网络服务商询问获得。

网络服务商：您申请线路的 ISP，比如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN1 口静态线路的带宽，可以向网络服务商询问获得。

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

工作模式：本路由器对于 WAN1 口提供三种工作模式。

1．路由模式。如果内网的主机全部是合法的公网地址，可以配置路由器工作在路由模式下。路由器工作在路由模式时，内网中出访数据包的源地址将使用本机的合法公网地址，不会被转换为路由器 WAN 口配置的 IP 地址。目前使用这种工作模式的客户比较少。

2．NAT（网络地址转换）模式。如果内网使用了一个私有的网络地址段，比如 10.x.x.x/172.16.x.x/192.168.x.x，并且需要访问互联网，则路由器需要工作在 NAT 模式下。路由器工作在 NAT 模式时，内网中出访数据包的源地址将被转换为路由器 WAN 口配置的合法 IP 地址。目前绝大多数用户使用的是这种工作模式。

3．桥接模式。该模式只针对 WAN1 使用；启用该模式后，路由器的 LAN 口和 WAN1 口实现纯桥功能。LAN 侧 PC 的网关应指到 WAN 侧的真实网关地址，路由器可对 LAN 侧的 PC 进行流控和上网行为管理等控制。

通断检测：如果为不启用，则路由器不对此条线路的通断作判断。

网关检测：如果 WAN 口到网关这一跳有故障，则选择网关检测效率最高。这个也是默认配置，推荐大多数客户使用。

DNS 检测：用于第 N（ $N \geq 1$ ）跳的故障。使用时必须正确配置静态线路的 DNS 地址，并填写检测域名。

定时切换：某些地区 ISP 存在零点断网问题。比如双线接入，WAN1 线路每天凌晨 0:00 断网，早上 7:00 通网，则配置定时切换断线时间为：23:59，上线时间为：7:02。在断线期间，内网所有的上网数据全部由另外一条未断的线路出访，内网不会产生由于零点断网引起的“掉线”问题。

2．PPPOE 拨号线路

外网配置->WAN1

规则列表

类型	PPPoE拨号线路
拨号类型	普通拨号
PPPoE帐号	88888888
PPPoE口令	●●●●●●
高级设置	
按需拨号	当线路空闲 <input type="text"/> 秒后自动断线（留空表示永远在线）
网络服务商	<input checked="" type="radio"/> 电信 <input type="radio"/> 新联通 <input type="radio"/> 自动识别 <input type="radio"/> 不指定
线路带宽	上行: <input type="text"/> Mbps 下行: <input type="text"/> Mbps
工作模式	<input type="radio"/> 启用路由模式
	<input checked="" type="radio"/> 启用NAT模式
通断检测	<input checked="" type="radio"/> 不启用 <input type="radio"/> 网关检测 <input type="radio"/> DNS检测 <input type="radio"/> 定时切换

保存

返回

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

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

按需拨号：当使用计时收费类型的 PPPOE 线路时，可以配置这个功能。配置该功能后，如果内网有上网请求，路由器会自动拨号连接，无需人工干预；PPPOE 线路空闲的时间达到设定的值后，系统自动切断 PPPOE 线路，节省费用。这个值应大于 30 秒，通常设置为 300 秒（5 分钟）。

网络服务商：您申请线路的 ISP，比如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN1 口 PPPOE 线路的带宽，可以向网络服务商询问获得。

工作模式：参考静态线路说明，默认使用“NAT 模式”。

通断检测：参考静态线路说明。

3. 动态获取地址线路

外网配置->WAN1

规则列表

类型	DHCP线路
主机名称	<input type="text"/> 某些以太网DHCP线路服务提供商可能需要，通常留空。
网络服务商	<input checked="" type="radio"/> 电信 <input type="radio"/> 新联通 <input type="radio"/> 自动识别 <input type="radio"/> 不指定
线路带宽	上行: <input type="text" value="10"/> Mbps 下行: <input type="text" value="10"/> Mbps
MTU设置	<input checked="" type="radio"/> 自动 <input type="radio"/> 手动 <input type="text" value="1500"/>
工作模式	<input type="radio"/> 启用路由模式 <input checked="" type="radio"/> 启用NAT模式
通断检测	<input type="radio"/> 不启用 <input checked="" type="radio"/> 网关检测 <input type="radio"/> DNS检测 <input type="radio"/> 定时切换 路由器根据WAN网关是否可达来决定线路通断。
<div>保存 返回</div>	

主机名：某些提供以太网动态获取地址线路的网络服务商可能需要，可以向网络服务商询问获得。

网络服务商：您申请线路的 ISP，比如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN1 口以太网动态获取地址线路的带宽，可以向网络服务商询问获得。

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

工作模式：参考静态线路说明，默认使用“NAT 模式”。

通断检测：参考静态线路说明。

WAN2 线路的参数说明与配置方法与 WAN1 线路的相同。

当多 WAN 配置完毕以后，点击“外网配置” “智能均衡策略”，将模式设置为“智能均衡”：智能均衡是飞鱼星路由器的一大特色，路由器将自动识别线路并调用路由策略，使多条线路工作在最佳状态下。

默认线路类型可选项有电信和新联通。比如 WAN1 和 WAN2 口分别是网通与新联通接入，此时如果内网访问教育网的资源，并且选择默认网络服务商“电信”，则访问教育网的数据从电信线路出访。

自定义策略，通过使用策略路由、静态路由等选项来配置策略路由的高级路由方案。

保存后如下图所示：

外网配置

外网配置

外网接口 智能均衡策略

☒ 智能均衡 默认线路类型 ☒ 电信 ☐ 新联通
路由器将自动识别线路并调用路由策略

☐ 自定义策略 您可以使用 策略路由、静态路由 选项来配置策略路由的高级路由方案

保存

5.3.5 DHCP 服务器

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

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

DHCP服务器

服务器配置	扩展地址池	静态分配	批量添加	DHCP信息	DHCP检测
-------	-------	------	------	--------	--------

☒ 是否在内网上启用DHCP服务器

起始IP地址
例如：192.168.0.30

结束IP地址
例如：192.168.0.100

默认网关

DNS服务器1

DNS服务器2

租期(分钟)
设定DHCP服务器为客户端租用IP地址保留的过期时间。如果留空，默认为60分钟；如果为-1，表明无限期租约。

绑定 ☒ 启动自动绑定IP/MAC功能
启用该功能后，如果有计算机通过DHCP获得IP，那么它的IP/MAC信息将自动绑定。

起始 IP 地址：DHCP 服务器自动分配的内部 IP 的起始地址。

结束 IP 地址：DHCP 服务器自动分配的内部 IP 的结束地址。

默认网关：路由器给 PC 分配的网关地址。通常为路由器的 LAN 口 IP。

DNS 服务器 1/DNS 服务器 2：分配的 DNS 服务器地址。

租期（分钟）：设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间，系统默认留空。如果留空，租期默认为 60 分钟。

绑定：启用自动绑定 IP/MAC 功能后，路由器会自动绑定已分配的 IP 地址与相应主机的 MAC 地址，避免内网由于 ARP 欺骗所带来的掉线问题。

DHCP 检测：当此路由器作为一台 DHCP 服务器时，他会主动探测同一局域网是否也存在其他 DHCP 服务器，如果有则显示其 IP 和 MAC 地址，避免 DHCP 服务冲突。

具体页面如下图所示：

DHCP服务器

服务器配置

扩展地址池

静态分配

批量添加

DHCP信息

DHCP检测

IP地址

MAC地址

扩展地址池：如果需要在多个网段实现动态地址分配，则可以使用此功能通过分别配置不同的地址池来实现。

具体配置如下图所示：

扩展地址池

扩展地址池

起始IP地址

192.168.0.10

例如：192.168.0.30

结束IP地址

192.168.0.40

例如：192.168.0.100

描述

子网地址池

保存

返回

保存后如下图所示：

扩展地址池

服务器配置

扩展地址池

静态分配

批量添加

DHCP信息

DHCP检测

起始IP地址

结束IP地址

描述

编辑

删除

192.168.0.10

192.168.0.40

子网地址池



共 1 条

<<

<

1

>

>>

删除所有规则

添加新规则

静态地址分配：如果希望内网某台主机每次启动以后都会获取 DHCP 服务器分配的同一 IP 地址，可以使用此功能。

比如：内网有台计算机的 MAC 地址是 **00:01:02:03:04:05**，希望它每次启动以后都会获取 IP 地址 **192.168.0.2**。首先，点击“添加新规则”添加一条规则；然后填写相应的 IP 地址与 MAC 地址，并保存。配置的结果如下图所示：

静态分配

服务器配置	扩展地址池	静态分配	批量添加	DHCP信息	DHCP检测
客户MAC	客户IP	描述	编辑	删除	
00:01:02:03:04:05	192.168.0.2	WEB服务器			
共 1 条 << < 1 > >>					
<div>删除所有规则</div> <div>添加新规则</div>					

您也可以批量的添加静态地址，如下图所示：

DHCP服务器

服务器配置	扩展地址池	静态分配	批量添加	DHCP信息	DHCP检测
<div>静态地址分配规则</div> <div>192.168.0.2 00:01:02:03:04:05 WEB服务器 192.168.0.5 00:01:02:03:04:06 张三 192.168.0.7 00:01:02:03:04:07 李四</div> <div>保存</div>					

添加好保存以后如下图显示：

DHCP服务器

服务器配置	扩展地址池	静态分配	批量添加	DHCP信息	DHCP检测
客户MAC	客户IP	描述	编辑	删除	
00:01:02:03:04:05	192.168.0.2	WEB服务器			
00:01:02:03:04:06	192.168.0.5	张三			
00:01:02:03:04:07	192.168.0.7	李四			
共 3 条 << < 1 > >>					
<div>删除所有规则</div> <div>添加新规则</div>					

DHCP 信息：DHCP 信息显示路由器 DHCP 服务当前的状态。可以看到的有：已经分配的 IP 地址、该 IP 所对应的 MAC 地址、获取该 IP 的计算机名称、IP 地址租约到期时间。如下图所示：

DHCP服务器

服务器配置	扩展地址池	静态分配	批量添加	DHCP信息	DHCP检测
ID	IP地址	MAC地址	计算机名	租约到期时间	
1	192.168.16.162	08:00:27:00:00:00	android-7b00f8e34459f91c	2012/7/4 14:54:49	
2	192.168.16.189	08:00:27:00:00:00	IKCLY3BT7TW8SSI	2012/7/4 15:19:32	
共 2 条 << < 1 > >>					

5.3.6 端口管理

本界面提供的功能是调整路由器 WAN 口的工作模式，改变路由器内网口与外网口的 MAC 地址。



注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。

端口管理

接口模式	MAC克隆				
WAN1口配置	自动模式	断开	10M	半双工	数据即时统计
WAN2口配置	自动模式	断开	10M	半双工	数据即时统计

保存

接口模式：可以调整路由器 WAN 口的工作模式。提供四种工作模式供选择：10M 全双工模式、10M 半双工模式、100M 全双工模式、100M 半双工模式。通常情况下网络接口之间自动协商工作模式，用户不需要手动配置，保留“自动模式”即可。也可查看其中某一端口的数据统计：

WAN1数据即时统计	
接收数据包	7368984
接收丢弃包	0
接收错误包	0
发送数据包	4213234
发送丢弃包	0
发送错误包	0

MAC 克隆：可以修改 LAN 口和 WAN 口的 MAC 地址，留空表示使用系统默认的 MAC 地址。某些网络服务商将提供给您的线路同某一个固定的 MAC 地址绑定起来，在这种情况下，MAC 地址克隆就非常有用。

端口管理

接口模式

MAC克隆

LAN口克隆地址

例如：00:0D:98:EF:02:01

WAN1口克隆地址

A4:BA:DB:B7:DD:78

例如：00:0D:98:EF:02:02

WAN2口克隆地址

例如：00:0D:98:EF:02:03

保存



注意：此文档为飞鱼星路由器通用型用户手册，以下功能示例可能会因产品系列不同而有差异，请根据实际产品系列继续查阅功能介绍。

VE 无线系列.....	5.4 无线设置
VE 有线系列.....	5.5 上网行为管理
VR\VN 系列.....	5.6 网络安全

5.4 无线设置

无线局域网 (wlan) 是一个通过无线信号而不是普通网线传输和接收数据的计算机网络。无线局域网越来越多的应用于家庭和办公环境，以及诸如机场，咖啡馆和大学等公共场所。创新的利用 wlan 科技帮助人们更高效的工作和交流。无需电缆连接，拥有更好的移动性已经为许多用户提供了便利。无线功能是本路由器的一项重要功能，利用该功能，可以组建内部无线局域网。组建网络时，内网主机需要一张无线网卡来连接无线网络。

首先请打开无线路由器的无线功能，设定前请先确定您的无线网卡已经正确安装驱动程序，且无线网卡工作正常。

5.4.1 基本设置

进入路由器 WEB 界面，选择菜单“无线设置”→“基本设置”，您可以在下图所示界面中设置无线网络的基本参数。

基本设置

功能配置

无线开关

☒ 启用

SSID

Volans_4FAC

SSID广播

☒ 启用
启用后, 本无线路由器将向无线网络中的主机广播SSID。

无线模式

11b/g/n 混合模式

信道模式

☐ FCC ☐ ETSI ☒ JP

无线信道

自动选取

保存

无线开关：若要使用路由器的无线功能，必须选择该项。选择启用，并保存。

SSID：该项标识无线网络的名称，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该无线网络。

SSID 广播：该项功能用于将路由器的 ssid 号向无线网络内的主机广播，这样，无线网卡将可以扫描到 ssid 号，并可以加入该 ssid 标识的无线网络。此功能默认为启用。

无线模式：该项用于选择路由器的工作模式，可供选择的有 300Mbps 的 802.11n /54Mbps 的 802.11g /11Mbps 的 802.11b 混合模式、802.11g/802.11b 混合模式、 300Mbps 的 802.11n 独立工作模式(此种模式下不兼容支持 802.11g 或 802.11b 的无线网卡)、54Mbps 的 802.11g 独立工作模式(该模式兼容 802.11b, 但不兼容 802.11n)。默认选择第一种，802.11b/802.11g/802.11n 混合模式。

信道模式：支持 FCC、ETSI 以及 JP 三种信道模式，可根据所在地区选择相应信道模式，使用地区范围参见无线信道。

无线信道：该项用于选择无线网络工作的频率段；FCC对应美国、加拿大等地区，可支持11个信道；ETSI对应中国、澳大利亚、委内瑞拉等地区，可支持13个信道；JP对应日本，可支持14个信道。如果选择“自动选取”，设备将根据当前各个信道的信号强度选择干扰较小的信道。默认选择“自动选取”。

5.4.2 安全设置

为了保证你的无线网络更加安全，选择菜单“无线设置”→“安全设置”，您可以在如下图所示界面中设置无线网络安全选项：

安全设置

认证方式设置 **MAC地址列表**

SSID:

MAC地址过滤: ☒ 启用 ☐ 允许 ☒ 禁止
允许：只接受MAC地址列表中的客户端访问网络。
禁止：除了MAC地址列表以外的客户端都可以访问网络。

加密类型:

加密算法:

PSK密码:
输入8-64位字符。

组密钥更新周期:
单位为秒, 最小值为30, 不更新则为0

保存

SSID：该项所显示的 SSID 名称，即为“无线设置”→“基本设置”中所填写的 SSID 内容。

MAC 地址过滤：通过 MAC 地址过滤可以允许或拒绝无线网络中的计算机接入无线局域网，有效控制无线局域网内用户的上网权限。启用此功能，并将开关选择“允许”，表示只接受 MAC 地址

列表中的客户端访问网络；启用此功能，并将开关选择“禁止”，表示除了 MAC 地址列表以外的客户端都可以访问网络。设置此项功能时，请在 MAC 地址列表所示位置添加需要设置的 MAC 地址。

加密类型：在无线网络安全设置页面，可以在此选择加密类型，可供选择的有：WPA-PSK、WPA2-PSK、WPA、WPA2、WEP、不加密方式。

- 1、如果无需开启无线安全功能，请在“加密类型”下拉菜单中选择“不加密”并保存。
- 2、如果要开启无线安全功能，请选择“加密类型”下拉菜单多种安全加密类型中的一种进行无线安全设置。不同的安全类型下，安全设置项不同，下面将进一步介绍：

a、WPA-PSK(或 WPA2-PSK)

选择 WPA-PSK (或 WPA2-PSK)安全类型，路由器将采用基于共享密钥的 WPA 模式，其具体设置如下图所示：

加密类型	WPA-PSK ▼
加密算法	AES ▼
PSK密码	12341234 输入8-64位字符。
组密钥更新周期	3600 单位为秒, 最小值为30, 不更新则为0
<input type="button" value="保存"/>	

加密类型：该项用来选择系统采用的安全方式，即 WPA-PSK(或 WPA2-PSK)、WPA (或 WPA2)、WEP。若选用 WPA-PSK(或 WPA2-PSK)即表示采用 WPA-PSK(或 WPA2-PSK)安全模式。此例中，我们选择 WPA-PSK 加密方式。

加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为 AES。

PSK 密码：该项是 WPA-PSK(WPA2-PSK)的初始设置密钥，设置时，要求最短为 8 个字符，最长为 64 个字符（注：密钥只能由数字和字母组成）。此例中，PSK 密码填入内容“12341234”。

组密钥更新周期：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为 30，若该值为 0，则表示不进行更新。若这里未作过任何改动，则路由器保持填写值为 3600。

b、WPA (或 WPA2)

选择 WPA (或 WPA2) 安全类型，路由器将采用 radius 服务器进行身份认证并得到密钥的 WPA (或 WPA2) 安全模式，其具体设置项如下图示。

加密类型	<input type="text" value="WPA"/>
加密算法	<input type="text" value="AES"/>
Radius服务器IP	<input type="text"/>
Radius端口	<input type="text" value="1812"/> 1-65535, 默认端口: 1812
Radius密码	<input type="text" value="abcdefgh"/> 输入8-64位字符。
组密钥更新周期	<input type="text" value="3600"/> 单位为秒, 最小值为30, 不更新则为0

加密类型：该项用来选择系统采用的安全方式，选择 WPA (或 WPA2)。

加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为 AES。

Radius 服务器 IP：radius 服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的 ip 地址。

Radius 端口：radius 服务器用来对无线网络内的主机进行身份认证，此项用来设置该 radius 认证服务采用的端口号，默认端口：1812。

Radius 密码：该项用来设置访问 radius 服务的密码。

组密钥更新周期：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为 30，若该值为 0，则表示不进行更新。若这里未作过任何改动，则路由器默认为 3600。

c、WEP

选择 wep 安全类型，路由器将使用 802.11 基本的 wep 安全模式。其具体设置项如下图示。

加密类型	<input type="text" value="WEP"/>	
预设密钥	<input type="text" value="密钥1"/>	
密钥1	<input type="text" value="aaabbbcccd"/>	<input type="text" value="16进制"/>
16进制：输入10或26位 (0-9, a-f, A-F 范围内的) 字符。 ASCII码：输入5或13位 (0-9, a-z, A-Z 范围内的) 字符。		
密钥2	<input type="text"/>	<input type="text" value="16进制"/>
密钥3	<input type="text"/>	<input type="text" value="16进制"/>
密钥4	<input type="text"/>	<input type="text" value="16进制"/>
<input type="button" value="保存"/>		

加密类型：该项用来选择系统采用的安全方式，即 WEP 加密。

预设密钥：该项提供四组密钥，即密钥一、密钥二、密钥三、密钥四，你可以任意选择其中一项密钥进行设置。

密钥 1：该项用来设置 WEP 加密密码。提供两种密钥类型，即 16 进制以及 ASCII 码。16 进制：输入 10 或 26 位十六进制字符；ASCII 码：输入 5 或 13 位 ASCII 码字符。

密钥 2、3、4：设置与密钥 1 相同。

MAC 地址列表：在此实现 MAC 地址过滤功能。

添加新规则：该项用于添加需要设置的 MAC 地址以及描述。

删除：该项用于删除不需要的规则。

编辑：该项用于对设置的 MAC 地址以及描述进行修改。

删除所有规则：该项用于当所有规则不需要时，一次性快捷删除。

安全设置

认证方式设置

MAC地址列表

MAC地址	描述	编辑	删除
00:01:02:03:04:05	123		

共 1 条 << < 1 > >>

删除所有规则

添加新规则

5.4.3 客人网络

当你的无线局域网有不同权限和不同级别要求的时候，开启此功能进行设置，即可以实现。选择菜单“无线设置”→“客人网络”，您可以在如下图所示界面中进行设置：

客人网络

客人网络设置

客人网络开关

☒ 启用

MAC地址过滤

☒ 启用 ☐ 允许 ☒ 禁止
允许：只接受MAC地址列表中的客户端访问网络。
禁止：除了MAC地址列表以外的客户端都可以访问网络。

SSID

密码

输入8-64位字符，留空表示不加密。

保存

客人网络开关：该项用于设置是否开启此功能，打勾表示开启。

MAC 地址过滤：允许或限制 MAC 地址列表中的客户端访问网络。

SSID：该项与基础设置中的 SSID 一样，用于标识无线网络的网络名称，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该无线网络。（注：与基础设置中的 SSID 有一

区别，客人网络中的 SSID，默认是不向外广播的，即无线网卡扫描不到客人网络的 SSID，需手动添加）

密码：该项用于设置密钥，设置时，要求最短为 8 个字符，最长为 64 个字符；也可以留空，留空表示不加密。（注：密钥只能由数字和字母组成）

5.4.4 高级设置

需要对路由器无线信号的强度和收发性能进行调节和修改，可以在无线设置功能的高级设置中进行设置，选择菜单“无线设置”→“高级设置”，如下图所示：

高级设置

功能配置

频段带宽	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
AP独立	<input type="checkbox"/> 启用 启用后, 接入的无线客户端之间将不能通信。
无线访问控制	<input checked="" type="checkbox"/> 启用 启用后, 接入的无线客户端不能与内网的有线客户端通信。
Beacon时槽	<input type="text" value="100"/> (20-1000, 默认值:100)
RTS阈值	<input type="text" value="2346"/> (1-2346, 默认值:2346)
分片阈值	<input type="text" value="2346"/> (256-2346, 默认值:2346)
DTIM阈值	<input type="text" value="1"/> (1-255, 默认值:1)
发送功率	<input type="text" value="100"/> (1-100, 默认值:100)
Wi-Fi多媒体	<input type="checkbox"/> 启用

保存

频段带宽：该项用于设置无线数据传输时所占用的信道宽度，可选项为：20、20/40。默认配置为 20/40。

AP 独立：该项用于控制通过无线信号接入的 PC 与 PC 之间的通信，启用，不能通信；不启用，可以相互通信。默认不启用。

无线访问控制：该项用于控制通过无线信号接入的 PC 与有线 PC 之间的通信，启用，不能通信；不启用，可以相互通信。默认启用。

Beacon 时槽：该项表示路由器通过发送 beacon 广播进行无线网络连接的同步。beacon 时槽表示路由器发送 beacon 广播的频率。beacon 广播的取值范围是 20 - 1000 毫秒，默认值为 100 毫秒。

RTS 阈值：该项用于设置数据包指定 RTS (request to send , 发送请求) 阈值。当数据包长度超过 RTS 阈值时，路由器就会发送 RTS 到目的站点来进行协商。接收到 RTS 帧后，无线站点会回应一个 RTS (clear to send , 清除发送) 帧来回应路由器，表示两者之间可以进行无线通信了。取值范围为 1-2346，默认值为 2346。

分片阈值：为数据包指定分段阈值。当数据包的长度超过分段阈值时，会被自动分成多个数据包。过多的数据包将会造成网络性能降低，所以分段阈值不应设置过低。默认值为 2346。

DTIM 阈值：该值在 1 至 255 毫秒之间，默认值为 1。用于设置传输指示消息(DTIM)的间隔。DTIM 是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它就会传送夹带有下一个 DTIM 时槽的 DTIM；当客户端听到 beacon 讯号时，就会接收该广播和组播信息。

发送功率：该项表示无线路由器广播 SSID 的功率的大小，数值越大信号越强，该值在 1 至 100 之间，默认值为 100。

Wi-Fi 多媒体：该项启用后，无线路由器可根据网络资料类型进行传输分类，以便提升效能的 Wi-Fi 多媒体 (WMM) 技术，可提升使用无线网络时的声音、影像、以及语音应用的体验。

5.4.5 WDS 设置

WDS (无线分布式系统)，是一个在 IEEE802.11 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，而不像以前一样无线访问点要通过有线进行连接，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。所以使用该功能时，至少要有两台同功能的无线路由器，选择菜单“无线设置”→“WDS 设置”，如下图所示：

WDS设置

WDS设置

WDS模式

加密类型

密钥

16进制：输入10或26位 (0-9, a-f, A-F 范围内的) 字符。
ASCII码：输入5或13位 (0-9, a-z, A-Z 范围内的) 字符。

扫描无线AP

MAC地址1 例如：00:01:02:03:04:05

MAC地址2

MAC地址3

MAC地址4

WDS 模式：该项支持三个选项：禁用、桥接模式和中继模式。

加密类型：该项设置 WDS 连接时双方通信的加密密钥，支持不加密、WEP、TKIP、AES。例如，我们此时选择其中一种 WEP 加密类型。

密钥：该项用于设置要加密的密码，例如，此时我们填入密码 0123456789。

扫描无线 AP：该项用于无线路由器桥接时，清楚记得对方无线路由器的 MAC 地址，这时候可点按“开始扫描”功能进行自动扫描。选择你需要桥接的路由器，点按选择，相对应的此台设备的 MAC 将会出现在“WDS 设置”页面的“MAC 地址 1”位置处，然后保存，在对方设备上同样如此操作，桥接设置完成。扫描后界面如下图所示：

WDS设置

无线AP列表

SSID	MAC地址	信道	强度	选择
Volans_8586	ec:6c:9f:07:8f:02	1	100	<input type="radio"/>
Volans_1B5C	ec:6c:9f:04:1b:5c	1	100	<input type="radio"/>
Volans_5288	00:00:84:00:00:11	1	50	<input type="radio"/>
Volans_8586	ec:6c:9f:08:97:0f	3	100	<input type="radio"/>
Volans_8259	ec:6c:9f:0a:82:59	10	100	<input type="radio"/>
Volans_1B4A	ec:6c:9f:04:1b:4a	7	15	<input type="radio"/>
Volans_8198_Guest_1	ec:6c:9f:07:8f:08	7	24	<input type="radio"/>
facemeeting_882	ec:6c:9f:04:1b:00	12	20	<input type="radio"/>
facemeeting_Guest	ec:6c:9f:04:1b:0b	12	29	<input type="radio"/>
PC_041M_5288	00:0c:43:30:52:08	12	86	<input type="radio"/>

返回

共 12 条

<<

<

1

2

>

>>

MAC 地址 1：该项用于显示桥接后的路由器 MAC 地址，支持与四个访问点同时进行桥接。

注：桥接后，有线网络之间被无线桥接起来，但无线路由器信号被屏蔽，不能支持其他 PC 通过无线信号接入网络。

5.4.6 客户端状态

无线客户端正常接入后，在路由器上查看主机状态，选择菜单“无线设置”→“客户端状态”，您可以看到如下图所示的界面：

客户端状态

客户端列表

ID	MAC	IP	SSID
1	74:DE:2B:44:8A:9F	192.168.16.122	Volans_1FAC
2	1C:65:9D:3E:ED:68	192.168.16.152	Volans_1FAC
3	A0:0B:BA:6A:F8:3C	192.168.16.162	Volans_1FAC

共 3 条

<<

<

1

>

>>

5.5 上网行为管理

5.5.1 IP 地址组

我们建议您通过 IP 地址组设置来规划局域网的组织结构,对于某些不属于特定部门的人群,如:来访人员、新入职的员工、兼职人员等,您可以另外建组。好的规划对后续的管理是非常有帮助的,会使整个网络架构井然有序。

IP 地址组:用于设置一个包含某些 IP 地址范围的 IP 组。这个 IP 组可以是内网的 IP 段,也可以是公网的某些 IP 段。设置好的 IP 组将与上网行为管理的各个子功能配合使用,可用于定义源 IP 或者目的 IP。比如企业研发部的 IP 段:192.168.0.20-192.168.0.50,研发部配置为一个 IP 组的方法是,点击“添加新规则”。

- 1、组名称:yanfabu;
- 2、IP 段:192.168.0.20-192.168.0.50,点击“添加”按钮;
- 3、描述:添加注释“研发部”;
- 4、点击“保存”后出现如下的界面。

类似地,可以添加企业行政部、市场部,或者添加一组外网的不安全 IP 段 221.50.50.0-221.50.50.254。

IP地址组

IP地址组列表				
组名称	IP地址	描述	编辑	删除
yanfabu	192.168.0.20-192.168.0.50	研发部		
xingzhengbu	192.168.0.60-192.168.0.65	行政部		
shichangbu	192.168.0.90-192.168.0.120	市场部		
virus	221.50.50.0-221.50.50.254	禁止访问的IP段		

共 4 条 << < 1 > >>

删除所有规则 添加新规则

5.5.2 行为管理策略

行为管理策略可以根据用户需要配置同时基于 IP 地址组和时间组的上网行为管理策略。主要通过“策略对象”、“应用软件过滤”、“网址分类”、“WEB 安全”、“电子公告”等五部分来实现。

策略对象：每个策略规则都需要启动策略后才能生效。可以从“所有地址组”列表中选取需要进行上网行为管理的对象，被选取的 IP 地址组将显示在“IP 组添加”列表中。再从“所有时间组”列表中选取对该对象进行上网行为管理的时间，被选取的时间组将显示在“时间组添加”列表中。

比如：在工作时间，需要对研发部和行政部实行上网行为管理。可以通过如下配置方式实现：

- 1、选择“启用策略”；
- 2、根据需要配置优先级；
- 3、从“所有地址组”中选择 yanfabu 和 xingzhengbu 添加到“IP 组添加”列表；
- 4、从“所有时间组”中选择 shangwu 和 xiaowu 添加到“时间组添加”列表；
- 5、对此次行为管理进行简单描述；
- 6、点击“保存”按钮，策略对象设置生效。

具体设置界面如下图所示：

行为管理策略

策略对象	应用软件过滤	网址分类	WEB安全	电子公告
------	--------	------	-------	------

☒ 启用策略

优先级设置

0

优先级0为高优先级。
优先级1为中优先级。
优先级2为低优先级。
同级别的优先级，防火墙高于行为管理策略。

IP组

IP组添加

yanfabu
xingzhengbu

所有地址组

yanfabu
xingzhengbu
shichangbu
virus

时间组

时间组添加

shangwu
xiawu

所有时间组

shangwu
wuxiu
xiawu
zhoumo

描述

研发部和行政部在上班时间不能使用应用软件

保存 返回

应用软件过滤：应用软件过滤采用深度协议分析技术，可以有效限制内网用户使用聊天软件、股票软件、P2P 软件、网络游戏（开心网、QQ 农场）等。对于最热门的聊天软件 QQ 的封锁，除了可以封锁通过代理登陆 QQ 外，还可以针对 QQ 号码实行封锁，允许例外的 QQ 号码登陆，同时记录 QQ 的登录日志。比如：规定周一至周五上班时间禁止公司内网所有用户使用聊天软件、禁止炒股、禁止做 P2P 下载、禁止播放在线视频、禁止玩网络游戏，可做如下的配置。



注意：由于应用软件的版本随时会升级，过滤功能可能会对新版本的软件失效，飞鱼星科技会不定期更新软件特征库，确保过滤功能对绝大多数的软件版本有效。

行为管理策略

策略对象
应用软件过滤
网址分类
WEB安全
电子公告

☒ 启用功能

聊天软件过滤

<input checked="" type="checkbox"/> QQ过滤	<input checked="" type="checkbox"/> WebQQ	<input checked="" type="checkbox"/> 邮箱QQ
<input checked="" type="checkbox"/> MSN过滤	<input checked="" type="checkbox"/> 飞信过滤	<input checked="" type="checkbox"/> 阿里旺旺过滤
更多应用	全选	反选

股票软件过滤

<input checked="" type="checkbox"/> 大智慧	<input checked="" type="checkbox"/> 钱龙	<input checked="" type="checkbox"/> 同花顺
<input checked="" type="checkbox"/> 证券之星	<input checked="" type="checkbox"/> 指南针	
	全选	反选

P2P软件过滤

<input checked="" type="checkbox"/> 迅雷过滤	<input checked="" type="checkbox"/> BT过滤	<input checked="" type="checkbox"/> 电驴过滤*
<input checked="" type="checkbox"/> FlashGet	<input checked="" type="checkbox"/> HTTP多线程下载	<input checked="" type="checkbox"/> 暴风影音
更多应用	全选	反选

游戏过滤

<input checked="" type="checkbox"/> QQ游戏	<input checked="" type="checkbox"/> 联众世界	<input checked="" type="checkbox"/> 浩方
<input checked="" type="checkbox"/> 梦幻西游	<input checked="" type="checkbox"/> 魔兽世界	<input checked="" type="checkbox"/> 跑跑卡丁车
更多应用	全选	反选

网页游戏过滤

<input checked="" type="checkbox"/> 开心网	<input checked="" type="checkbox"/> QQ农场	
	全选	反选

代理过滤

<input checked="" type="checkbox"/> HTTP代理	<input checked="" type="checkbox"/> SOCKS4代理	<input checked="" type="checkbox"/> SOCKS5代理
	全选	反选

保存

返回

网址分类：网址分类管理功能将大多数热门网站进行分类，用于对外网网站的访问进行管控，杜绝员工访问与工作无关网站。比如：规定公司内网所有用户在工作时间只能访问公司网站 www.kmds.com 和合作伙伴网站 www.abc.com，不允许访问其他网站。配置如下：

- 1、选择“启用功能”；
- 2、在白名单中添加 www.kmds.com 和 www.abc.com；
- 3、将从“休闲娱乐”到“其他网址”的所有分类全部“阻断”，在跳转地址栏处填入公司地址 www.kmds.com。当员工访问公司规定之外的网站时，页面将自动跳转到公司网站页面；
- 4、点击“保存”按钮。

阻断：启用后，禁止用户访问“被阻断网站”，并将网址自动跳转到指定页面。

记录：启用后，日志会记录某个 IP 什么时候访问过哪些网站。

警告：启用后，当用户访问“被警告网站”时，浏览器会显示警告信息。

禁止 IP 访问网站：有些网站通过在浏览器输入 IP 地址就可以直接访问，启用该功能后，路由器将禁止内网用户使用这种方式访问网站。本例只允许内网访问 IP 为 61.122.123.6 的网站。

行为管理策略

策略对象
应用软件过滤
网址分类
WEB安全
电子公告

☒ 启用功能
☐ 禁止IP访问网站

IP白名单
61.122.123.6

白名单
www.kmds.com
www.abc.com

黑名单
☐ 记录
☐ 警告

请填入需要例外的远程网站服务器IP。

示例网址：
example.com 包括此域名下所有子域名中的网页如img.example.com
example.com.cn 包括此域名下所有子域名中的网页如www.example.com.cn
test.example.com.cn 仅指“test.example.com.cn”子域名中的网页

网址分类管理

休闲娱乐	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
新闻资讯	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
聊天交友	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
网络游戏	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
电子购物	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
论坛博客	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
证券基金	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
电子邮件	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
网上银行	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
不良网址	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告
其他网址	<input checked="" type="checkbox"/> 阻断	<input type="checkbox"/> 记录	<input type="checkbox"/> 警告

警告页面管理

预览

警告标题
警告内容
警告链接
例如：www.google.cn
警告链接文字

阻断页面管理

显示方式
☒ 链接地址
☐ 静态页面

跳转地址设置
www.kmds.com
例如：www.google.com

保存
返回

WEB 安全：可以实现禁止内网用户在论坛发帖、禁止用户下载指定扩展名（比如 exe、torrent 等）的文件、禁止用户访问 URL 中包含指定关键字的网站等功能。

比如：禁止公司内网所有用户在工作时间到论坛发帖、下载扩展文件名为 exe、.torrent 的文件、访问 URL 包含 bbs、org 的网站。配置方法如下：

- 1、选择“启用功能”；
- 2、过滤文件扩展类型填写：torrent,exe（用英文的逗号分隔）；
- 3、过滤的 URL 关键字填写：bbs,org（用英文的逗号分隔）；
- 4、将“禁用 WEB 页面提交”打勾；
- 5、点击“保存”按钮。

具体配置界面如下图所示：

行为管理策略

策略对象	应用软件过滤	网址分类	WEB安全	电子公告
<input checked="" type="checkbox"/> 启用功能				
过滤文件扩展类型	<input type="text" value="exe,torrent"/> 已设置2种文件类型 最多只能过滤20种文件扩展类型。不同的文件类型用“,”隔开。例如： rar,exe,torrent			
过滤的url关键字	<input type="text" value="bbs,org"/> 已设置2个url关键字 <input type="checkbox"/> 精确匹配域名 最多只能过滤10个url关键字。不同的url关键字用“,”隔开。例如：img,bt,bbs			
WEB安全高级设置				
<input checked="" type="checkbox"/> 禁用WEB页面提交				
<input type="button" value="保存"/>		<input type="button" value="返回"/>		

电子公告：此系列产品的电子公告功能，支持“公告”、“链接地址”、“静态页面”等三种显示方式。

第一种：普通的公告显示方式

公告功能将按照管理员设置的公告周期定时向网内用户发送设置的公告内容，用户可以通过浏览器查看到公告内容。

比如：以 720 分钟为周期，定时向研发部和行政部员工发送题为“禁止应用软件”的电子公告，可做如下设置：

- 1、选择“启用功能”；

- 2、公告周期，单位为分钟，填写 720；
- 3、公告标题，填写“禁止应用软件”；
- 4、公告内容，填写具体的公告内容；
- 5、点击“保存”按钮，设置生效。

具体的配置界面如下图所示：

行为管理策略

策略对象	应用软件过滤	网址分类	WEB安全	电子公告
<input checked="" type="checkbox"/> 启用功能				
公告周期	<input type="text" value="720"/> 分			
显示方式	<input checked="" type="radio"/> 公告 <input type="radio"/> 链接地址 <input type="radio"/> 静态页面			
公告标题	<input type="text" value="禁止应用软件"/>			
公告内容	<div><div>上班时间，研发部和行政部员工禁止使用各种应用软件</div><div></div></div> <div>预览</div>			
<div>保存 返回</div>				

第二种：链接地址的显示方式

此方式可直接在路由器电子公告的配置界面中填写相应的链接地址，当内网计算机打开网页时，便会弹出所填链接地址对应的网页。具体配置界面如下图：

行为管理策略

策略对象	应用软件过滤	网址分类	WEB安全	电子公告
------	--------	------	-------	------

☒ 启用功能

公告周期 分

显示方式 ☐ 公告 ☒ 链接地址 ☐ 静态页面

链接地址
例如：www.google.cn

第三种：静态页面

选择显示方式为 html 文件格式的静态页面，在内网计算机打开网页时，便会弹出自定义的静态页面，具体如下图所示配置界面：

行为管理策略

策略对象	应用软件过滤	网址分类	WEB安全	电子公告
------	--------	------	-------	------

☒ 启用功能

公告周期 分

显示方式 ☐ 公告 ☐ 链接地址 ☒ 静态页面

网址库设置：通过网址库设置可将指定网址添加进系统默认分类中，并可添加自定义网址分类及其网址。例如添加“休闲娱乐”中某个网址为自定义网址，保存生效后可通过行为管理策略的网址分类功能对自定义分类网址进行阻断、记录和警告操作。

行为管理策略

规则设置

组名称

休闲娱乐

网址

www.abc.com

编辑格式为一条域名占一行，支持完整格式域名，不可用通配符，例如：www.example.com

保存

返回

5.5.3 聊天软件高级设置

QQ 登陆日志记录：该功能可允许例外的 QQ 号码（如：工作 QQ）和 MSN 用户登陆，若要记录 QQ 和 MSN 的登录日志，分别启用“QQ 登陆日志记录”、“MSN 登陆日志”即可。启用该功能后若内网有用户尝试登陆私人 QQ 和 MSN，路由器就会记录对应 IP 所登陆的 QQ 号码和 MSN 账号，同时禁止使用该 QQ。

具体配置界面如下图所示：

聊天软件高级设置

QQ登陆日志记录

例外的QQ号

例外的MSN账户

批量添加

☒ 启用QQ登陆日志记录☒ 启用MSN登陆日志记录

保存

例外的 QQ 号：启用该功能，可以允许部分有工作需求的 QQ 号登陆。比如：需要实现允许 32475698 和 56128745 两个工作 QQ 号登陆。

具体配置效果界面如下图所示：

聊天软件高级设置

QQ登陆日志记录 例外的QQ号 例外的MSN账户 批量添加

QQ号	描述	编辑	删除
32475698	允许登录工作QQ1		
56128745	允许登录工作QQ2		

共 2 条 << < 1 > >>

添加新规则

例外的 MSN 账户：启用该功能，可以允许部分 MSN 账户登陆。比如：需要实现允
xx123@msn.com 和 YY456@ hotmail.com 两个 MSN 账户登陆。

具体配置效果界面如下图所示：

聊天软件高级设置

QQ登陆日志记录 例外的QQ号 例外的MSN账户 批量添加

MSN账户	描述	编辑	删除
xx123@msn.com	允许xx123账户登陆		
YY456@hotmail.co m	允许YY456账户登陆		

共 2 条 << < 1 > >>

添加新规则

批量添加：你也可以批量添加例外 QQ 号和 MSN 账号。具体配置界面如下图所示：

聊天软件高级设置

QQ登陆日志记录	例外的QQ号	例外的MSN账户	批量添加
<div>批量添加QQ号</div> <div>32475698 允许登录工作QQ1 56128745 允许登录工作QQ2 45821682 允许登录工作QQ3 78942132 允许登录工作QQ4</div>			
<div>批量添加MSN账户</div> <div></div>			
<div>保存</div>			

5.5.4 防火墙设置

本界面提供了飞鱼星路由器内置的高性能防火墙的配置。防火墙访问控制规则一旦设置后，路由器将运用所配置的规则来匹配报文中的相关信息，决定允许或者拒绝报文通过。

比如禁止所有计算机在任何时刻上网。可在防火墙设置里做如下操作，点击“添加新规则”，在出现的界面中做如下配置：

- 1、不使用：保持默认，不勾选。若勾选，则本条规则配置后不生效；
- 2、动作：禁止；
- 3、优先级：中优先级；
- 4、接口：LAN；

- 5、协议：ALL[ALL/1-65535]；
- 6、目的端口范围：当协议为 ALL 时，目的端口范围默认为所有端口；
- 7、目的地址组：选择下拉菜单“任意”；
- 8、源地址组：选择下拉菜单“任意”；
- 9、时间组：任意；
- 10、描述：进制所有计算机上网；
- 11、点击“保存”按钮，设置生效。

具体配置界面下图所示：

防火墙设置

规则设置

一键添加

不使用

☐ 不使用这条规则
 设置不使用这条规则，您以下的配置将只会被保存，不生效！

动作

允许

选择包过滤方式

留意：允许和不允许处理方式的不同

优先级

中优先级

同级别的优先级，防火墙高于行为管理策略。

接口

入接口

LAN

出接口

LAN

选择匹配的包接口

协议

ALL[ALL/1~65535]

选择哪一种IP协议将被匹配

留意：大多数情况下您应该选择TCP

端口范围

到

目的地址组

任意

☐ 取反

源地址组

任意

☐ 取反

时间组

任意

描述

禁止所有计算机上网

保存

返回

配置保存后，具体显示界面如下图所示：

防火墙设置								
规则列表								
优先级	动作	目的地址组	源地址组	详情	状态	移动	编辑	删除
中优先级	允许	*	*					
共 1 条 << < 1 > >>								
<div>删除所有规则</div> <div>添加新规则</div>								



注意：规则的匹配顺序是从上到下，一旦匹配了一条规则就会马上执行，下面的规则不再进行匹配。因此一般将比较细化的规则放在上面，可以使用“上下移动”键来调整规则顺序。

一键添加：防火墙的一键添加按钮可以很方便地实现一些网络访问控制功能。比如配置所有的计算机只能浏览网页和收发邮件，禁止其他互联网应用，具体配置界面如下图所示：

防火墙设置

<div>规则设置</div> <div>一键添加</div>	
不使用	<input type="checkbox"/> 不使用这条规则 设置不使用这条规则，您以下的配置将只会被保存，不生效！
优先级	中优先级 同级别的优先级，防火墙高于行为管理策略。
	仅能收发邮件，禁止其他互联网应用 <input type="radio"/> 启用
规则	仅能浏览网页，禁止其他互联网应用 <input type="radio"/> 启用
	仅能浏览网页和收发邮件，禁止其他互联网应用 <input checked="" type="radio"/> 启用
源地址组	任意 <input type="checkbox"/> 取反
时间组	任意
描述	只能浏览网页和收发邮件
<div>保存</div> <div>返回</div>	

5.5.5 WEB 认证

WEB 认证功能只允许通过认证的内网用户上网，禁止未授权用户访问互联网。认证方式可分为身份认证（用户名+密码）、MAC 地址认证、IP 地址认证等方式。

启用 WEB 认证：即打开该功能的总开关。

WEB认证

认证设置 用户登记 批量添加 例外MAC 例外IP 用户信息

☒ 启用WEB认证

窗口标题

窗口标题

窗口提示文字

窗口提示文字

[预览](#)

保存

导入背景图片

浏览...

背景图片为不超过200KB的jpg文件。

导入

用户登记：启用用户登记时，需在路由器上配置合法用户的用户名以及密码。打开 WEB 认证总开关后，内网用户用浏览器尝试访问 www.163.com 时，会弹出认证界面，此时需输入登记的用户名和密码，通过认证，该用户才可以上网。

WEB认证

认证设置 用户登记 批量添加 例外MAC 例外IP 用户信息

用户名	备注	编辑	注销
test			

共 1 条 << < 1 > >>

登记

可通过批量添加用户输入框，复制→粘贴多个用户。

WEB认证

认证设置 用户登记 批量添加 例外MAC 例外IP 用户信息

批量添加

test 1234
test1 1111
test2 2222

保存

例外 MAC:启用 MAC 认证后,内网用户的 MAC 地址若与列表内的 MAC 地址相同,则该用户可直接通过路由器上网。

WEB认证

认证设置 用户登记 批量添加 例外MAC 例外IP 用户信息

MAC地址	描述	编辑	删除
00:01:02:03:04:05	test		

共 1 条 << < 1 > >>

删除所有规则 添加新规则

例外 IP:启用 WEB 认证中的例外 IP 后,IP 地址组中的用户可直接通过路由器上网。例如,只允许行政部上网。

WEB认证

认证设置

用户登记

批量添加

例外MAC

例外IP

用户信息

IP地址组

所有地址组

IP认证地址组

xingzhengbu

<<>>

yanfabu

xingzhengbu

保存

通过 Web 认证的用户，就可以在“用户信息”里查看目前认证成功用户的相应信息

WEB认证

认证设置

用户登记

批量添加

例外MAC

例外IP

用户信息

用户名	IP地址	MAC地址
共 0 条 << < 1 > >>		

5.6 网络安全

VR\VN 系列上网行为功能请参照 [5.5 上网行为管理](#)

5.6.1 攻击防御

本界面提供全新网络自防御体系配置。飞鱼星网络自防御机制能够侦测及阻挡 ARP 欺骗，源路由攻击，IP 端口扫描，DoS 等网络攻击，可以有效防止多种病毒攻击。即使内网存在恶意流量，飞鱼星独有的“网络自防御”技术也可以杜绝整个网络的瘫痪，以保证其他主机浏览网页、聊天、游戏等的正常应用，确保网络整体的正常运营。

网络攻击防御

内网防御		外网防御	
ARP欺骗防御保护	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止	设置arp发包频率 <input type="text" value="10"/> 个/秒	
广播风暴抑制	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止		
内网病毒防御	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止		
过滤未知协议	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止		
syn-flood 攻击防御	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止	每秒最多允许通过 <input type="text" value="100"/> 个包	
udp-flood 攻击防御	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止	每秒最多允许通过 <input type="text" value="500"/> 个包	
icmp-flood 攻击防御	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止	每秒最多允许通过 <input type="text" value="50"/> 个包	
禁用内网诊断	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁止		
<input type="button" value="保存"/> <input type="button" value="恢复默认设置"/>			

ARP 欺骗防御保护：内网 ARP 欺骗保护功能，请使用默认配置。

广播风暴抑制：在一个布局不合理的局域网中或者局域网有某些病毒时，内网会有很大比例的广播包，大量广播包会导致内网速度变慢，运行不稳定。此功能通过拦截内网的大量广播包来保证内网的稳定运行。

内网病毒防御：此功能可以阻断来自内网中毒计算机对路由器的攻击。在一个比较复杂的内网环境中，使用飞鱼星路由器，可以在“系统信息”页面看到路由器一天拦截到几百万个数据包，内网运行状况稳定；在同样环境下，如果使用其他路由器，内网几乎无法运行。

过滤未知协议：如果“启用”，路由器可以阻止来自 LAN 口的特殊类型的乱包攻击。

Syn-flood 攻击防御/ udp-flood 攻击防御/ icmp-flood 攻击防御：飞鱼星独有的防御来自内网的针对路由器的 DoS 攻击。后面的参数都是飞鱼星根据当前攻击类型的特点做的优化设计，请保持默认配置。

禁用内网诊断：默认启用。可在路由器负荷比较高的环境下启用该功能对路由器进行调试。

网络攻击防御

内网防御

外网防御

响应外网ping请求

☐ 启用 ☒ 禁止

阻断外网请求

☐ 启用 ☒ 禁止

外网开放端口保护

☐ 启用 ☒ 禁止

保护阈值

外网ARP公告

☐ 启用 ☒ 禁止

设置arp发包频率 分钟

保存

恢复默认设置

响应外网 ping 请求：出于安全考虑，请保持默认“禁止”。如果选择“启用”，外网用户将可以 ping 通路由器的 WAN 口地址，这样以来会增加风险。

阻断外网请求：默认选择“禁止”。如果“启用”，外网用户将不能访问内网的虚拟服务器。

外部开放端口保护：保护内网的虚拟服务器。使内网虚拟服务器在受到来自外网的恶意攻击的情况下，不至于瘫痪，确保网络整体的正常运营。

5.6.2 连接限制

通过网络连接数限制功能，可以设置内网每台计算机能够使用的最大连接数，每台主机 1000 条连接数为全局默认的最大连接数，其中 UDP 连接数最大不能超过 300 条。您可以通过规则列表来针对特殊 IP 主机设置不同的连接限制数量，但需注意规则设置中配置的连接数优先于全局默认的连接数限制。

具体配置界面如下图所示：

连接数限制

功能配置

规则列表

☒ 启用连接数限制最大不超过 条网络连接☒ 启用UDP连接数限制最大不超过 条网络连接

保存

连接限制功能既可以统一对内网的所有计算机进行最大 NAT 连接数限制，也可以单独限制某些特殊功能计算机（比如服务器）的最大连接数；还可以启用高级连接数限制，以保证某些游戏更加快速地连接到服务器。该功能可根据网络的实际应用情况，更加合理地分配连接数资源，有效的保证内网整体的可用性与可靠性。

比如配置内网每台计算机的连接数为 600 条，并且启用高级连接数限制，内网 DMZ 主机 192.168.0.99 连接数为 2000 条，UDP 连接限制为 300 条；内网段 192.168.0.22-192.168.0.24 的几台 web 服务器的连接数为 1000 条，UDP 连接限制为 50 条。具体配置结果如下图所示：

连接数限制

功能配置

规则列表

地址	总条数	UDP条数	描述	状态	编辑	删除
192.168.0.22-192.168.0.24	1000	50	WEB服务器			
192.168.0.99	2000	300	DMZ主机			

共 2 条 << < 1 > >>

删除所有规则

添加新规则

5.6.3 IP/MAC 绑定

本功能用于实现内网计算机的 IP 地址与 MAC 地址之间的绑定。路由器的 ARP 映射表如果被更改，整个网络将陷于瘫痪。使用飞鱼星集成的 IP-MAC 扫描工具，一键绑定内网计算机的 IP 地址和 MAC 地址，可以极大的降低因 ARP 欺骗造成的“掉线”故障。

网络管理人员总是希望网络秩序良好、运行稳定，但事实往往不尽如人意：IP 地址被随意改动导致 IP 地址冲突而使合法的主机不能上网；无法限制某些 IP 地址的主机访问互联网等，飞鱼星提供的地址绑定功能可以很好的解决这些问题。

地址绑定一旦配置完成后，指定的 IP 地址就只能被指定的计算机使用，解决了局域网中因 IP 地址被随意改动而导致的 IP 地址冲突问题。另外也可以通过选中“禁止未绑定 ARP 信息的主机通过”选项来禁止所有未被绑定的计算机出访互联网。

点击“动态列表” “扫描 MAC”，可以扫描出内网活动主机的 IP/MAC 地址，具体扫描结果如下图所示：



在该扫描结果列表中可通过点击每条结果后的“绑定”选项，对单台主机进行 IP/MAC 绑定；也可以通过点击“绑定所有 IP/MAC 项”对所有扫描出来的主机进行 IP/MAC 绑定。

批量绑定：可在此手动添加内网主机的 IP/MAC 项，IP 和 MAC 之间用一个空格隔开。点击“保存”按钮，可以将绑定内容添加到绑定列表。

具体配置界面如下图所示：

IP/MAC绑定

绑定列表

动态列表

批量绑定

批量添加

10.10.10.104 XX:XX:XX:XX:XX:XX

10.10.10.15 XX:XX:XX:XX:XX:XX

保存

绑定列表：该列表中显示了目前已被绑定的内网主机的 IP/MAC 信息。可以通过点击“编辑”图标为每条 IP/MAC 添加描述内容。

具体界面如下图所示：

IP/MAC绑定

绑定列表

动态列表

批量绑定

IP地址	MAC地址	描述	编辑	删除
192.168.0.2	00:01:02:03:04:05			
192.168.0.10	00:11:22:33:44:55			

共 2 条 << < 1 > >>

☐ 禁止未绑定IP/MAC的主机通过

保存

删除所有绑定

添加新规则

如果将“禁止未绑定 IP/MAC 的主机通过”打勾，则内网未被路由器绑定 IP/MAC 的计算机就不能通过该路由器上网。

5.6.4 MAC 地址过滤

本界面提供的 MAC 地址过滤功能可以禁止内网计算机上网。有时候可能需要禁止内网某些计算机上网，只要找到该计算机的 MAC 地址，在 MAC 地址过滤里添加一条规则，便可以实现。

比如：想禁止 MAC 地址是 00:01:02:03:04:05 的计算机上网。首先，点击“添加新规则”并填写计算机 MAC 地址，可对该项进行简单描述，然后点击“保存”按钮，规则生效。

具体配置结果如下图所示：

MAC地址过滤

规则列表			
MAC地址	描述	编辑	删除
00:01:02:03:04:05	文控主机		
共 1 条 << < 1 > >>			
<div>删除所有规则</div> <div>添加新规则</div>			

5.7 QoS 流量控制

5.7.1 智能流控

飞鱼星智能流控技术只需一键开启，路由器自动对各类应用的深度感知、分类管理、分级处理，始终让企业关键业务走优先通道，其余流量都给他们让路，保证关键应用如：视频会议、OA 系统等！同时还能把剩余带宽分配给其他用户或应用（例如文件下载、在线视频），真正做到人少多用、人多好用！

智能流控：智能流控功能总开关。启用智能流控后，路由器将自动根据网络中活动主机的各种应用（包括游戏、P2P、网页及其他应用）的带宽使用变化情况，对网络带宽的分配进行优化调整。如下图所示：

智能流控

智能流控			
<input checked="" type="checkbox"/> 启用智能流控			
接口	接口类型	下行带宽	上行带宽
WAN1	10M 光纤	10000 Kbps	10000 Kbps
WAN2	10M 光纤	10000 Kbps	10000 Kbps
<div>保存</div>			

5.7.2 固定流控

启用固定流控并保存生效后，路由器可对配置列表中主机进行指定的流量控制，主机的网络带宽被控制在该范围内。“上行限制”和“下行限制”分别限制主机上行和下行最大带宽。“上行保证”和“下行保证”分别保证主机上行和下行最小带宽。点击“流控规则” “添加新规则”，即可对指定的IP 或 IP 段进行限制，如下图所示：

固定流控

规则设置

☐ 不使用
设置不使用这条规则，您以下的配置将只会被保存，不生效！

IP地址
IP地址 到
例如：192.168.0.2 到 192.168.0.254

上行限制
 KBps
请输入一个整数，如果您想限制到1.6Mbps，可输入200KBps，为实时智能流控。(参考公式：
1MBps=8Mbps=1024KBps≈1000KBps)

下行限制
 KBps

上行保证
 KBps

下行保证
 KBps

接口
 请选择您要用的接口。

时间
 时 分 到 时 分 留意：时间留空为任意时间

工作日期
☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六 ☐ 周日
留意：工作日期留空为每天

描述

不使用：打勾表示不使用本条规则，但该规则并不被删除。

IP 地址：需要做流量控制的计算机的 IP 地址。

上行\下行限制：限制主机上行和下行最大带宽，默认单位为 KB。

上行\下行保证：保证主机上行和下行最小带宽，默认单位为 KB。

接口：是否需要配置分接口流控。如果选择任意，则为不分接口流控，此时使用非弹性流控，则单

机下载最大速度约等于所设定的值(若 WAN 口数为 2，则单机下载最大速度为 2*设定值)；如果选择 WAN1，则为对 WAN1 进行流控，此时使用非弹性流控，则单机使用 WAN1 带宽下载速度约等于所设定的值，但是单机下载总带宽可能会大于所设定的值。

时间\工作日期：设置固定流控的时间和日期，流控表示任意时间、任意每天。

描述：添加对于本条规则的注释。

点击“保存”按钮后，路由器将对配置列表中主机进行指定的流量控制，主机的网络带宽被控制在该范围内，出现如下图所示的界面：



5.8 高级选项

5.8.1 端口映射

本界面提供端口映射的配置。端口映射又称虚拟服务器，当内网使用私有地址时（比如 10.x.x.x/172.16.x.x/192.168.x.x）外部网络无法直接访问内网中的服务器，可通过在路由器上做端口映射，配置内网服务器的 IP 地址与端口，如此一来外部网络便可以访问内网服务器，从而使用内网提供的服务了。

比如：内网有 100 台计算机，已经配置好一台 FTP 服务器，它的 IP 地址是 192.168.0.5，如果想让外网用户也可以访问此服务器，可以点击“添加新规则”，在出现的界面做如下图所示的配置操作：

端口映射

规则列表

不使用

☐ 不使用这条规则

设置不使用这条规则，您以下的配置将只会被保存，不生效！

外部IP

例如：8.8.8.8

外部端口

 到

您可以指定一个外部端口映射到内部主机开放的端口上。如果留空，则外部端口同内部端口相同。填写范围在1 - 65535之间。

内部IP

内部网络中对外提供服务的主机IP。
例如：192.168.0.50

内部端口

 到

内部网络中对外提供服务的主机所开放的端口。填写范围在1 - 65535之间。

协议

端口映射使用的协议，可以是TCP、UDP或者二者兼有。

映射线路

端口映射时可以使用的线路可以是单WAN或者多WAN。

描述

您可以在这里填写简单的提示表示这条端口映射规则的意义。
例如：市场部的WEB服务器

保存

返回

不使用：打勾表示不使用本条规则，但该规则并不被删除。

外部 IP：外网用户 IP 地址。

外部端口：指定一个对外开放的端口，映射到内部服务器开放的端口上，外部端口可以指定为一个连续的端口范围，但是需与内部开放端口相对应。如果不指定，则外部端口与内部端口相同。填写范围 1 - 65535。

内部 IP：内网的服务器的 IP 地址。

内部端口：内网服务器提供的服务所使用的端口。内部端口可以指定为一个连续的端口范围，但是需与外部开放端口相对应。详情请参考“常见的端口和服务对照表”。

协议：服务器提供的服务所使用的协议，如不清楚是哪种协议，可以选择“TCP/UDP”。详情请参考“常见的端口和服务对照表”。

映射线路：如果是双 WAN 接入，在这里选择外网用户通过哪条线路进来访问内网的服务器，系统默认选择“WAN1/WAN2”。若外网用户从 WAN1 访问，就用 WAN1 口的 IP 地址；从 WAN2 访问，用 WAN2 口的 IP 地址。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，显示界面如下图所示：

端口映射

规则列表						
外部端口	内部IP	内部端口	描述	状态	编辑	删除
21	192.168.0.5	21	FTP服务器			
共 1 条 << < 1 > >>						
<div>删除所有规则</div> <div>添加新规则</div>						

网络服务		使用协议	端口
ftp	文件传输	TCP	21
Ssh	安全远程管理	TCP	22
telnet	远程登录	TCP	23
Smtp	简单邮件传输	TCP	25
Time	时间同步	TCP	37
DNS	域名解析	UDP	53
www	网页浏览	TCP	80
POP3	邮局协议 3	TCP	110
Snmp	简单网络管理协议	UDP	161
CS server	CS 网络游戏	TCP	27015

常见的端口和服务对照表

5.8.2 静态路由

静态路由就是静态的路由表信息。在某些网络环境下，需要通过修改静态路由表，指定静态路由信息来实现正常通信。

比如：指定内网的主机访问 221.12.12.0/24 这个网络的资源从 WAN1 出去，WAN1 的网关地址是 61.121.13.1，可点击“添加新规则”，具体配置界面如下图所示：

静态路由：编辑

规则设置

目标网络地址	<input type="text" value="221.12.12.0"/> 请输入目标网络地址。
掩码	<input type="text" value="255.255.255.0"/> 请输入您的子网掩码。 例如：255.255.255.0
网关	<input type="text" value="61.121.13.1"/> 请输入您的网关地址。
接口	<input type="text" value="WAN1"/> 请选择您要用的接口。
描述	<input type="text" value="静态路由 1"/>

保存

返回

目标网络地址：输入目标网络的网络地址。

掩码：目标网络地址的子网掩码，可以根据实际情况选择。

网关：输入与目标网络匹配的数据交付的网关地址，本例是 WAN1 口的网关。

接口：指定数据交付的接口，本例选择 WAN1 口。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下图所示的界面：

静态路由：编辑

规则列表

批量添加

目标网络地址	掩码	网关	接口	描述	编辑	删除
221.12.12.0	255.255.255.0	61.121.13.1	WAN1	静态路由 1		

共 1 条

<<

<

1

>

>>

删除所有规则

添加新规则

静态路由的批量添加功能可以快速地一次性添加多条静态路由规则。使用批量添加时请注意书写格式,例如 233.233.233.0 255.255.255.0 233.233.233.254 WAN1 每个条目之间用一个空格隔开,注意 IP 地址一定要填写正确,否则错误的静态路由规则会导致您的网络不流畅,甚至无法使用。配置如下图所示：

静态路由

规则列表		批量添加	
<div>233.233.233.0 255.255.255.0 233.233.233.254 WAN1</div> <div>批量添加路由规则</div> <div>保存</div>			

5.8.3 策略路由

策略路由可以使数据包按照用户指定的策略进行转发。源地址路由就是指定具体的主机从具体的 WAN 口访问外网。此功能可以根据实际情况灵活调度多 WAN 的使用,实现负载均衡。比如：指定内网 IP 地址为 192.168.0.3 - 192.168.0.100 这个段的主机访问外网从 WAN1 出去。可以按此操作,点击“添加新规则”,做如下图所示的配置：

策略路由

规则设置

不使用

☒ 不使用这条规则

设置不使用这条规则，您以下的配置将只会被保存，不生效！

目标网络地址

221.12.12.0

请输入目标网络地址。

掩码

255.255.255.0

请输入您的子网掩码。

例如：255.255.255.0

目标域名

编辑格式为一条域名占一行，支持完整格式域名，不可用通配符，例如：www.example.com

协议

HTTP[TCP/80~80]

端口

80

到

源地址

192.168.0.3

到

192.168.0.100

例如：192.168.0.2 到 192.168.0.128

接口

☒ WAN1 ☐ WAN2

请选择您要用的接口。

描述

从WAN1口访问外网

保存

返回

不使用：打勾表示不使用本条规则，但该规则并不被删除。

目标网络地址：输入目标网络的网络地址

掩码：目标网络地址的子网掩码，可以根据实际情况选择。

目标域名：目标域名"不可与"目标网络地址"、"协议"和"端口"同时设置。

协议：应用程序所使用的协议，请根据实际情况选择。可以是 TCP、UDP 或者二者兼有，这种情况下需要指定端口的范围；也可以是具体的应用协议，比如 HTTP、POP3，这种情况下不需要指定端口的范围。

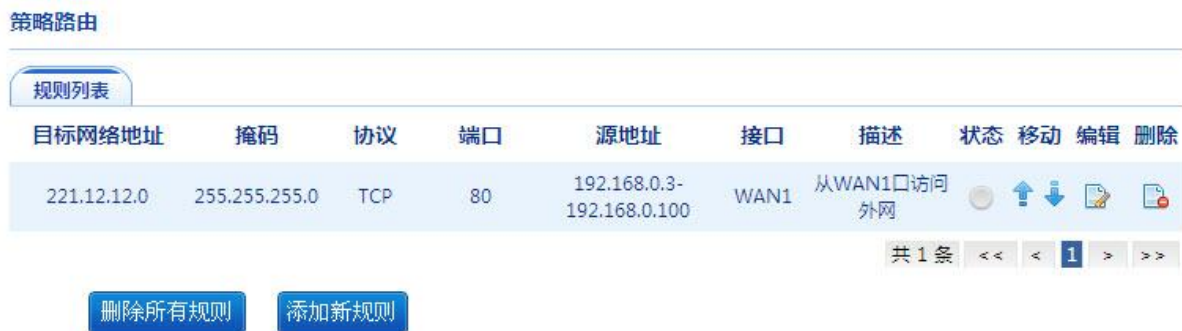
端口：当协议选择 TCP、UDP 或者 TCP/UDP 的情况下，指定端口的范围。

源地址：指定内网的一个地址段，或者一个 IP 地址。

接口：选择该地址（段）访问外网从哪个接口出去。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下图所示的界面：



5.8.4 地址转换

随着 Internet 网络爆炸性的膨胀，IP 地址短缺及路由规模越来越大已成为一个相当严重的问题。为了解决这个日益严重的问题，出现了多种方案。目前在应用中最行之有效的解决方案是网络地址转换(NAT)。

一个组织网络内部可以自定义其 IP 地址（不需要经过申请，即私有的 IP 地址，如 10.x.x.x/172.16.x.x/192.168.x.x），在本组织内部，各计算机之间可以通过私有 IP 地址进行通讯。但当组织内部的计算机需要与外部 Internet 网络进行通讯时，就需要为内网计算机配备一个公网的合法 IP 地址才能实现。而具有 NAT 功能的设备就负责将私有的 IP 地址转换为公网 IP 地址（即申请的合法 IP 地址），使内网计算机能够在公网上正常通信。简单地说，NAT 就是一种将私有 IP 地址转换为公网合法 IP 地址的技术。

本界面的地址转换功能提供多对一转换和一对一转换两种模式。

1. NAT 外出规则

比如：内网主网段 192.168.0.0/24，有一个扩展网段 192.168.1.0/24（已经在“内网配置”“内网扩展配置”里配置实现）。外网单 WAN 接入，WAN 口光纤有 2 个 IP 地址，218.6.90.34 和 218.6.90.35，WAN1 口已经配置了一个 IP 地址 218.6.90.34，默认情况下主网段和扩展网段的

计算机 NAT 以后都将从 218.6.90.34 出访。但是，如果想让扩展网段的计算机 NAT 以后用 IP 地址 218.6.90.35 出访，可做如下操作：

点击“添加新规则”，在“规则设置”界面做如下图所示的配置：

NAT外出规则：编辑

规则设置

不使用

☒ 不使用这条规则
设置不使用这条规则，您以下的配置将只会被保存，不生效！

源地址

IP地址

子网掩码

目标地址

类型:

任意 ▾

IP地址

子网掩码

接口

不指定 ▾

请选择您要用的接口。

转换地址

218.6.90.35

在这里您可以设置一个IP地址作为转换地址，也可以设置一个地址段做为转换地址。设置地址段时，最大长度为16个地址，例如：221.18.10.6-221.18.10.21。

描述

地址转换

为了方便识别，您可以在这里简单描述设定的规则。

保存

返回

不使用：打勾表示不使用本条规则，但该规则并不被删除。

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 192.168.1.1/24。

目标地址：需要访问的目的地址。“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：如果选择“不指定”，则必须填写转换地址，该地址应是 ISP 提供的合法 IP 地址；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（仅用于 WAN 口是 PPPoE 情况）。本例选择“不指定”。

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。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，本条规则生效，出现如下图所示的界面：

NAT（网络地址转换）：外出规则

NAT : 外出规则

NAT : 一对一

扩展	源地址	接口	描述	状态	编辑	删除
非扩展	192.168.1.1/255.255.255.0	不指定	地址转换	<div></div>	<div></div>	<div></div>

共 1 条

<<

<

1

>

>>

删除所有规则

添加新规则

2. NAT 一对一

本路由器可通过 NAT 一对一的方式支持 DMZ 功能。这个功能可以使内网某台特定计算机完全向互联网开放，从而支持更多的网络应用。本路由器支持 DMZ 主机的数量只取决于您所拥有的合法 IP 地址的数量。一台 PC 设置成 DMZ 主机后，就完全暴露在公网上，这时候这台 PC 就失去了 NAT 防火墙的保护，所以请谨慎使用。

比如：内网有网段 192.168.0.0/24，外网单 WAN 接入，WAN 口光纤有 2 个公网 IP 地址，分别是：218.6.90.34 和 218.6.90.35。WAN1 口已经配置了一个 IP 地址 218.6.90.34，如果此时需要对内网中 IP 地址为 192.168.0.4 的计算机作 NAT 一对一转换，外部地址选择 218.6.90.35，那么可以通过如下操作来实现：

将标签切换到“NAT 一对一”页面，点击“添加新规则”，在出现的“规则设置”页面做如下图所示的配置：

NAT（网络地址转换）：一对一规则

规则设置

不使用

☐ 不使用这条规则
设置不使用这条规则，您以下的配置将只会被保存，不生效！

内部地址

写入内部地址用于做一对一的网络地址转换。
例如：192.168.0.50

外部地址

写入外部地址用于做一对一的网络地址转换。
例如：218.35.97.7

接口

WAN1

▼

请选择您要用的接口。

规则描述

为了方便识别，您可以在这里简单描述设定的规则。

保存

返回

不使用：打勾表示不使用本条规则，但该规则并不被删除。

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。请注意：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。

接口：规则作用于哪个 WAN 口。

规则描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下图所示的界面：

NAT（网络地址转换）：一对一规则

NAT：外出规则		NAT：一对一					
内部IP	外部IP	接口	描述	状态	编辑	删除	
192.168.0.4	218.6.90.35	WAN1	DMZ1				
共 1 条 << < 1 > >>							
删除所有规则		添加新规则					

5.8.5 域名转发

本界面提供域名服务功能，路由器直接向内网的计算机转发其域名缓存列表中的域名地址。域名转发工作的前提是“启用 DNS 缓存转发”功能。通过域名转发规则，可以将指定的域名同指定的 IP 地址绑定起来，在内网中生效，这个设置与外部网络的 DNS 解析没有关系。

域名服务器转发配置

规则列表

功能配置

☒ 启用DNS缓存转发

☒ 强制域名转换

保存

比如：内网有台 WEB 服务器，IP 地址为 192.168.0.3，设定域名为 www.myweb.com。设置内网所有的计算机的 DNS 值和内网网关相同。

在“规则列表”页面，点击“添加新规则”，做如下图所示的配置：

域名服务器转发配置：编辑

规则设置

名称	<input type="text" value="web_server"/> 主机名称，没有域名部分。 例如：web_server
域名	<input type="text" value="www.myweb.com"/> 主机的域名 例如：www.webs.com
IP地址	<input type="text" value="192.168.0.3"/> 主机的IP地址 例如：192.168.0.100
描述	<input type="text" value="web服务器"/> 为了方便识别，您可以在这里简单描述设定的规则。

保存

返回

名称：填写内部主机的名称。

域名：指定内部主机的域名，注意：这个域名仅在局域网内网生效，并且需要开启 DNS 缓存转发功能。

IP 地址：填写内部主机的 IP 地址。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下图所示的界面：

域名服务器转发配置：编辑

规则列表

功能配置

名称	域名	IP地址	描述	编辑	删除
web_server	www.myweb.com	192.168.0.3	web服务器		

共 1 条

<<

<

1

>

>>

删除所有规则

添加新规则

重启路由器使域名转发功能生效，之后您就可以通过在内网计算机的浏览器上输入 www.myweb.com 来访问内网的 WEB 服务器了。

5.8.6 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 地址都不同），如果采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具有固定域名的网站，是不可能的。而有了动态域名，这个美梦就可以成真了。首先用户可以申请一个域名，再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，这样就可以很方便地搭建自己的网站了。

飞鱼星路由器为每个 WAN 口都提供了动态 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“服务类型”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。

比如在 www.3322.org 上申请了一个动态域名 xxxx.3322.org，用户名 xxxx，密码 1234。其具体的配置方法如下：

点击“编辑”按钮添加一条新规则，按照如下图所示的方法配置：

动态域名

动态域名信息

WAN1 ☒ 启用动态DNS客户端

服务类型 3322.org

主机名称 xxxx.3322.org

用户名 xxxx

密码 ●●●●

保存 返回

WAN1：启用动态 DNS 客户端后，本条规则才生效。

服务类型：选择提供动态域名服务的服务商类型，在本例是 3322.org。

主机名称：申请的主机名称。

用户名：申请动态域名时使用的用户名称。

密码：申请动态域名时使用的密码。

点击“保存”按钮，规则生效，出现如下图所示的界面：

动态域名

动态域名信息			
接口	状态	动态域名配置信息	编辑
WAN1	已配置	xxxx.3322.org	

5.8.7 UPnP 设置

UPnP(Universal Plug and Play) ,通用即插即用 ,是一组协议的统称 ,不能简单理解为 UPnP=“自动端口映射”。在 BitComet 下载中 , UPnP 包含了 2 层意思 :

1、对于一台内网电脑 , BitComet 的 UPnP 功能可以使网关或路由器的 NAT 模块做自动端口映射 , 将 BitComet 监听的端口从网关或路由器映射到内网电脑上。

2、网关或路由器的网络防火墙模块开始对 Internet 上其他电脑开放这个端口。

通过使用 UPnP , BitComet 等 P2P 软件可以获得更快的下载速度。

UPnP 的配置方法如下 , 点击 “UPnP 设置” , 将 “使用 UPnP” 打勾 , 并保存。具体界面如下图所示 :



UPnP设置

UPnP使用信息 **UPnP设置** 允许IP列表

☒ 使用UPnP

保存

点击 “允许 IP 列表” , 并 “添加新规则” , 在这里设置使用 UPnP 的计算机 IP 地址范围。例如设置 192.168.0.1-192.168.0.254 范围的计算机使用 UPnP 功能。

具体的配置结果如下图所示 :



UPnP设置

规则设置

源地址 192.168.0.1 / 24 ▾
例如 : 192.168.0.2 / 24

描述 整个内网使用UPnP

保存 返回

点击 “UPnP 使用信息” , 可以查看当前的 UPnP 服务状态 , 如下图所示 :

UPnP设置

UPnP使用信息 UPnP设置 允许IP列表

IP地址	内部端口	外部端口	协议	包/字节	应用描述
共 0 条 << < 1 > >>					

删除所有规则

5.9 虚拟专网

VPN (Virtual Private Network) ,即虚拟专用网络。它是通过一个公用网络 (通常是因特网) 在两个局域网或者工作站之间建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道。通常,VPN 是对企业内部网的扩展,通过它可以帮助远程用户、公司分支机构、商业伙伴以及供应商同公司的内部网建立起可信的安全连接,并保证数据的安全传输。

有两种建立 VPN 连接的方法:第一种是从计算机到 VPN 路由器、第二种是从 VPN 路由器到 VPN 路由器。

飞鱼星路由器支持这两种建立 VPN 连接的方法。

5.9.1 PPTP 客户端

PPTP 客户端支持从 VPN 路由器客户端连接到 VPN 路由器服务端。比如:企业分支机构 A 与企业总部之间需要实现简单安全的信息互访,可以在分支机构的路由器中配置 PPTP 客户端来实现上述功能。

具体的配置方法如下图所示:

PPTP客户端

PPTP客户端配置

☒ 启用PPTP客户端

PPTP服务器地址 221.237.88.88

用户名 user2

密码 ●●●●

PPTP服务器网段 192.168.3.0

PPTP服务器掩码 255.255.255.0

PPTP客户端高级设置

是否启用加密 ☒ 启用加密

状态

未连接

重拨

刷新

保存

启用 PPTP 客户端：打勾表示启用 PPTP 客户端功能。

PPTP 服务器地址：需要拨入的 PPTP 服务端地址。

用户名：使用的 PPTP 用户名，由服务端分配。

密码：用户名所对应的密码，由服务端分配。

PPTP 服务器网段：通过 PPTP 隧道访问的网段，一般配置为 PPTP 服务端内网地址段。

PPTP 服务器掩码：PPTP 服务端内网地址段掩码。

是否启用加密：根据服务端配置选择是否启用加密，保证服务器和客户端配置相同才可以正常通信。

做好上述配置之后，还需要在 PPTP 服务端配置“PPTP 用户”，客户端内网主机才可以通过 PPTP 隧道来访问服务端内网主机，从而实现内网互访。

5.9.2 PPTP 服务端

如果 PPTP 客户端要拨入服务端内网，则必须配置 PPTP 服务端。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。

具体的配置方法如下图所示：

PPTP服务端

PPTP服务端设置 PPTP用户 拨入列表

☒ 启用PPTP服务

PPTP服务端地址 192.168.16.16

PPTP客户端地址范围 192.168.0.151 到 192.168.0.158
例如： 192.168.0.151---192.168.0.158

保存

启用 PPTP 服务：打勾表示启用 PPTP VPN 服务端。

PPTP 服务端地址：服务端 LAN 口的 IP 地址。

PPTP 客户端地址范围：客户通过 VPN 拨进来以后，服务端随机给它分配内网 IP 地址的范围。此地址段设置应当与服务端内网地址在同一网段并且不要与内网产生地址冲突。

启用 128-bit 数据加密：支持 128-bit 数据加密功能，此配置必须服务端同客户端保持一致才能正常通信。打勾表示两端的通信会以 128-bit 密钥加密的方式进行。

以上配置完成后，还需要在服务端新建 PPTP 用户。方法是点击“PPTP 用户”，在该页面通过点击“添加用户”来设置一个新用户。

比如：用户名为 user1、密码为 1234。具体配置界面如下图所示：

编辑用户

编辑用户

用户名

user1

密码

••••

•••• (确认密码)

描述

用户1

保存

返回

点击“保存”按钮，出现如下图所示的界面：

PPTP服务端

PPTP服务端设置

PPTP用户

拨入列表

用户名	类型	网络	描述	编辑	删除
user1	主机		用户1		

共 1 条 << < 1 > >>

添加用户

PPTP 用户配置完成后，出差员工通过在自己的电脑上启动 VPN 客户端程序，使用 PPTP 服务端当前 WAN 口 IP 和相应的用户名、密码配置客户端，就可以拨入公司内网了。

若企业分支机构 A 需要通过 VPN 拨入公司总部局域网，实现分支机构 A 内的所有计算机都可以访问公司总部内网资源。可以通过如下的配置来实现：

在服务端配置用户名为 user2、密码为 1234 的新用户，勾选“用户所在客户端为一个网络”，客户端网段与客户端掩码分别填写分支机构 A 的内网网段和掩码。

具体配置如下图所示：

编辑用户

编辑用户

用户名

user2

密码

•••••

•••••

(确认密码)

描述

用户2

保存

返回

通过对 PPTP 服务端、PPTP 用户以及 PPTP 客户端的设置，用户就可以通过服务端分配的用户名和密码拨入公司内网，建立 VPN 连接了。并且可以从“拨入列表”中查看到拨入 VPN 用户的具体情况。

拨入列表：您将在这里看到哪些用户拨入了 VPN，以及为其分配到的 IP 地址和他的拨入地址。

5.10 系统工具

5.10.1 管理选项

本界面提供修改路由器的 WEB 管理密码和 WEB 管理端口功能。

修改路由器 WEB 管理密码界面如下图所示：

管理选项

用户密码管理

WEB管理

用户名

admin

管理密码

••••••

••••••

(确认密码)

如果您想改变WEB管理部分的访问密码，请在上面设置并确认。

保存

点击“保存”后，所做的修改立即生效。

WEB 管理选项提供 WEB 管理端口的修改，WEB 管理 IP 的添加等功能。

具体界面如下图所示：

管理选项

用户密码管理 WEB管理

WEB管理端口 如果您想改变WEB管理部分的访问端口，请在上面键入新的端口号，缺省系统使用80端口。

允许外部使用WEB管理 ☒ 是否允许外部主机使用WEB管理？
打勾表示允许，如果允许，外部主机将能够使用本机进行管理配置。

外部端口

登陆保留时间 分钟
登陆保留时间设置为0时表示不限制。

显示行数设置 行

保存

WEB 管理端口：修改路由器的 WEB 管理端口（在路由器重新启动后生效）。系统默认使用 80 端口，如果要修改 WEB 管理端口，请注意不要用系统中已经使用的标准端口，比如 53 等，建议使用 8000 - 60000 之间的端口号。更改 WEB 管理端口后请牢记端口号。

允许外部使用 WEB 管理：如果希望外网可以通过 WEB 管理路由器，将“是否允许外部主机使用 WEB 管理”打勾，保存即可。请注意：开放路由器的外网 WEB 管理存在一定风险，请谨慎使用。系统默认不允许对外部主机开放 WEB 管理功能。

外部端口：修改管理端口不要用系统中已经使用的标准端口，比如 53 等，建议使用 8000 - 60000 之间的端口号。更改 WEB 管理端口后请妥善保管。


登陆保留时间：若设置时间为 5 分钟，使用 admin 打开路由器的 WEB 界面，5 分钟内不做任何操作，则再次访问路由器 WEB 时，系统要求重新认证。

显示行数设置：可以通过配置显示行数来修改系统日志、防火墙等列表每一页的显示行数。

5.10.2 网络诊断

网络诊断：启用诊断模式会关闭路由器所有的上网行为管理，防火墙规则和防御模块，通常用于调试设备才启用网络诊断。默认情况下该开关保持禁止状态。页面如下图所示：

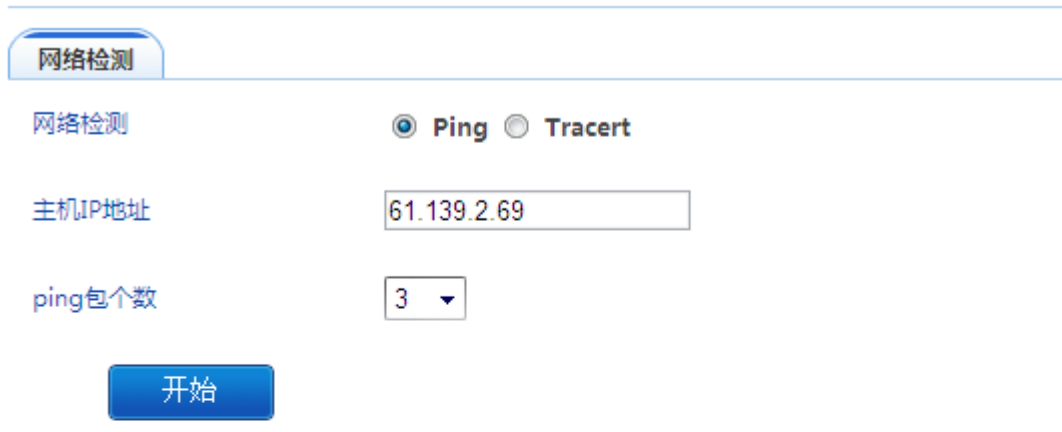
网络诊断



The screenshot shows the 'Network Diagnosis' configuration page. It has two tabs: 'Network Diagnosis' (selected) and 'Network Detection'. Under the 'Network Diagnosis' tab, there is a checkbox labeled 'Enable Diagnostic Mode' which is currently unchecked. To the right of the checkbox is a button labeled 'Enable'. At the bottom of the page is a blue button labeled 'Save'.

网络检测：本界面提供两个使用频率最高的网络命令，ping 和 tracert，命令的发起端都是路由器。使用 ping 可以检测目标地址是否可以到达。比如，ping 61.139.2.69 的结果如上图所示：
(ping 包个数选择 3 个)

网络检测



The screenshot shows the 'Network Detection' configuration page. It has a single tab labeled 'Network Detection'. Below the tab, there are two radio buttons: 'Ping' (selected) and 'Tracert'. Below these is a text input field for 'Host IP Address' containing '61.139.2.69'. Below that is a dropdown menu for 'Ping packet count' with '3' selected. At the bottom is a blue button labeled 'Start'.

ping输出结果：

```
PING 61.139.2.69 (61.139.2.69): 56 data bytes
64 bytes from 61.139.2.69: seq=0 ttl=250 time=8.185 ms
64 bytes from 61.139.2.69: seq=1 ttl=250 time=7.978 ms
64 bytes from 61.139.2.69: seq=2 ttl=250 time=8.022 ms
--- 61.139.2.69 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.978/8.061/8.185 ms
```

由于 61.139.2.69 是一个外网地址，根据使用 ping 命令的结果得出的结论是：从路由器发出的数据包可以到达外网，并且路由器可以收到外网回应的数据包，说明外网是通的；只要路由器没有配置任何限制规则，内网的用户就可以通过路由器上网。

再举个例子来说明 tracert 的使用情况，tracert 61.139.2.69 的结果如下图所示：

网络检测

网络检测

网络检测

☐ Ping ☒ Tracert

主机IP地址

61.139.2.69

开始

Tracert输出结果：

1 8ms 8ms 8ms 222.212.68.1
2 * * * request time out.
3 12ms 12ms 11ms 182.151.194.198
4 * * * * * request time out.
5 338ms 810ms 1718ms 61.139.2.69

根据使用 tracert 命令的结果，得出的结论是：从路由器发出的数据包在到达 61.139.2.69 (电信地址) 之前经过了 4 个网关的转发。通常我们只关心到达的第一个网关，在这里是 222.212.68.1，它是 WAN 口线路的网关，本例是在使用电信和网通双线接入的情况下测试 tracert，输出结果验证了访问电信的资源从电信的线路出访，实现了策略路由。

5.10.3 用户管理

本界面提供的功能是添加 user 组，以便对路由器的访问权限实行分级管理。路由器将管理用户划分为 admin 组与 user 组。admin 组对路由器的配置有修改的权限，user 组则只能查看路由器在运行过程中的重要参数，不能修改路由器的配置。这样设计大大提高了路由管理的安全性，减少了由于配置不当而引起的网络故障。

配置方法是，首先点击“添加用户”，填写用户名，密码，并可以对该用户进行简单的描述，然后点击“保存”按钮，如下图所示，添加了一个用户名为 user1 的用户。通过使用 user1 用户与相应的密码登陆路由器的 WEB 管理界面，就可以查看路由器在运行过程中的一些参数。

用户管理

用户列表			
用户名	描述	编辑	删除
user1	用户1		
共 1 条 << < 1 > >>			
<button>添加用户</button>			

5.10.4 策略升级

本界面提供升级路由器策略库的功能，如策略路由引擎库、聊天软件特征库、P2P 软件特征库、网址分类信息库等，确保路由器对于聊天软件，P2P 软件的较新版本达到最佳封锁效果。建议配置为自动更新，并设置自动更新时间。

比如设置自动更新时间为每月的 1 号上午 10 时，可以做如下图所示的配置：

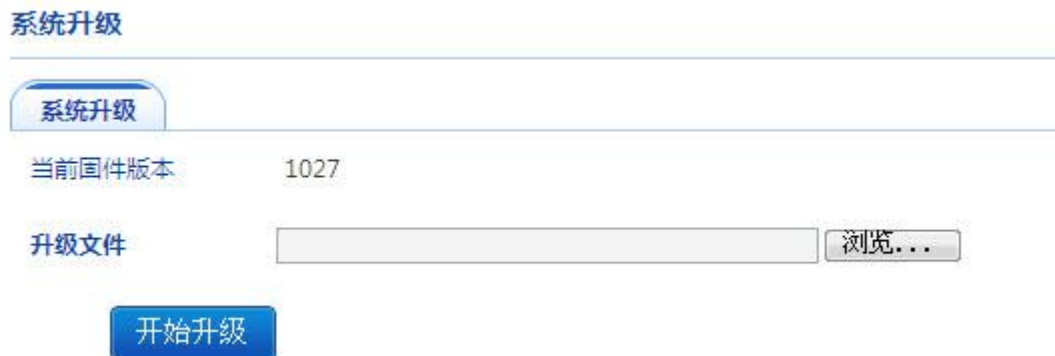
策略升级

策略升级配置		策略本地升级
策略库版本	120731	<button>立即更新</button>
	<input checked="" type="checkbox"/> 启用自动更新	
自动更新时间	每月 1 日 0 时	
<button>保存</button>		

5.10.5 固件升级

本界面提供路由器的固件升级功能。路由器需要相应的软件才能提供丰富的功能。在厂家发布路由器的升级固件后，会提供一个固件升级包。通常情况下，使用新的固件升级包都可以得到更多

的功能和更好的性能。在厂家的官方网站下载得到最新的固件升级包后，就可以使用“固件升级”功能给路由器升级固件。升级成功并自动重启后，就可以看到“当前固件版本”已经发生了变化。具体界面如下图所示：



当前固件版本：显示路由器的当前固件版本号。

升级文件：点击“浏览”按钮，指定路由器固件升级包在本地电脑中的位置。确定后，点击“开始升级”按钮。在升级的过程中系统有提示，大概 2 分钟完成升级，升级成功后路由器会自动重启。

注意事项：

- 1、固件升级之前请确认固件升级包与设备之间是否匹配，不同型号的设备使用不同的固件升级包；
- 2、升级过程请不要断开电源，否则升级无法完成；
- 3、升级之前请重新启动路由器，启动正常后，断开外网连线。内网仅连接一台 PC 机，使用 IE 正常打开路由器 WEB 升级界面，选择正确的升级包操作。
- 4、若在升级过程中出现固件升级失败，请参照附录 C 的操作步骤恢复固件。

5.10.6 备份恢复配置

本界面提供的功能是将路由器的所有配置保存为文件，如果因为操作不当导致配置出现错误时，可以使用原先保存的配置文件恢复配置。界面如下图所示：

备份恢复设置

备份恢复设置

点击按钮下载系统配置文件

保存配置

保存配置

打开配置文件用于恢复配置

恢复配置

注意：
恢复配置后重启生效

浏览...

恢复配置

保存配置：点击“保存配置”按钮，将路由器的所有配置保存为文件。

恢复配置：点击“浏览”按钮，指定原先保存的配置文件在本地电脑中的位置，确定后，点击“恢复配置”按钮开始恢复配置，恢复成功后路由器自动重启。

5.10.7 恢复出厂配置

本界面提供将路由器的所有配置清空，恢复到出厂配置的功能。它的效果和按一下路由器前面板上的“RST”键（复位按钮）相同。界面如下图所示：

恢复出厂设置

恢复出厂设置

重要提示：

路由器恢复出厂设置后，所有用户的配置都将删除。如必要，请使用“备份配置”功能保留当前路由器配置。恢复出厂设置后，您可以通过<http://192.168.0.1>来重新配置路由器，登录用户名和口令都是admin。确定恢复出厂设置吗？

确定

提示：路由器恢复出厂配置后，所有的配置都将被清空。可以通过<http://192.168.0.1>来重新配置路由器，登录用户名和密码都是 admin

5.10.8 重新启动

本界面提供的功能是从软件上重启路由器，它的效果和使用路由器后面板的电源开关相同。通过的 WEB 管理界面重启路由器在某些时候可能非常方便，比如路由器放置在一个无法触及到的地方时。路由器的重启过程大概需要 40 秒。界面如下图所示：

重新启动路由器

重新启动路由器 自动重启设置

重要提示：

路由器重新启动会中断网络很短一段时间，确定吗？

确定

本路由器设计了自动重启功能，开启该功能后，路由器将会在设定的启动时间自动重启。界面如下图所示：

重新启动路由器

重新启动路由器 自动重启设置

☐ 开启自动重启功能

定时启动时间 0 时 0 分

定时启动日期 ☐周一 ☐周二 ☐周三 ☐周四 ☐周五 ☐周六 ☐周日

保存

第六章 特殊功能介绍

6.1 时间组 (高端产品支持)

时间组：基于时间的分组管理可使上网行为管理策略更加精细、配置更加灵活。

添加时间组 shangwu，时间 9:00-12:00，工作日期周一至周五，描述“工作日（上午）”。类似地可根据需要添加“工作日（午休）”，“工作日（下午）”，“周末”等时间组。

时间组

时间组				
组名称	时间	描述	编辑	删除
shagnwu	9:0-12:0 周一 周二 周三 周四 周五	工作日（上午）		
wuxiu	12:0-13:0 周一 周二 周三 周四 周五	工作日（午休）		
xiawu	13:0-18:0 周一 周二 周三 周四 周五	工作日（下午）		
zhoumo	0:1-23:59 周六 周日	周末		

共 4 条 << < 1 > >>

删除所有规则 添加新规则

6.2 WPS 设置（仅带 WPS 按钮的设备支持）

WPS（Wi-Fi 保护设置）能够简单、快捷地在无线网络客户端和无线 AP 之间建立加密连接。您不必设置繁琐的加密方式和密钥，只需输入正确无线客户端的 PIN 码或者选择 PBC（或按路由器面板上的 WPS 按钮）即可实现无线网络的连接。如下图所示：

WPS设置

功能配置

WPS功能 ☒ 启用

添加无线设备

PIN模式

连接

PBC模式

虚拟按钮

6.3 PPPOE 服务器（部分型号支持）

PPPoE 服务器提供了认证上网的功能。内网计算机使用正确的用户名和密码，通过 PPPoE 拨号到路由器进行认证，从而获取上网权限。注意，聊天软件过滤功能可能会对 PPPoE 拨号用户失效。

PPPoE服务器

服务器配置

用户配置

批量导入

用户状态

账号到期通告

☒ 启用PPPoE服务器

☒ 禁止非PPPoE拨号用户上网

例外IP地址组

例外IP地址组

yanfabu

所有地址组

所有地址组

yanfabu

xingzhengbu

☒ 每用户最多拨入一个连接

起始IP地址

192.168.0.20

系统最大会话数

30

主DNS服务器

8.8.8.8

备DNS服务器

保存

启用 PPPoE 服务器：开启 PPPoE 服务器功能的总开关。

禁止非 PPPoE 拨号用户上网：只允许通过 PPPoE 认证的计算机上网，其他配置静态 IP 地址的计算机不能上网。

每用户最多拨入一个连接：当一个账户拨号在线时，其他电脑不能再次使用该账户拨号。

起始 IP 地址：认证成功后，PPPoE 服务器自动分配的起始 IP 地址，该地址设置为与路由器的内网 IP 在同一个网段。

系统最大会话数：PPPoE 服务器最多允许同时拨入的计算机数量。

主 DNS 服务器/备 DNS 服务器：认证成功后，PPPoE 服务器给客户机分配的 DNS。

启用 PPPoE 服务器，必须添加 PPPoE 用户。

PPPoE服务器

用户配置

用户名	<input type="text" value="test"/>		
密码	<input type="password" value="••"/>	<input type="password" value="••"/>	(确认密码)
客户IP	<input type="text" value="192.168.0.2"/>		高级设置
	例如：192.168.0.2		
客户MAC	<input type="text" value="00:01:02:03:04:05"/>		
	例如：00:01:02:03:04:05		
带宽	上行: <input type="text" value="50"/>	KBps	下行: <input type="text" value="100"/>
	KBps		
有效日期:	<input type="text" value="2012-07-01"/>	到	<input type="text" value="2012-07-31"/>
描述	<input type="text"/>		
<input type="button" value="保存"/> <input type="button" value="返回"/>			

内网用户通过 PPPoE 认证成功后，可以查看当前 PPPoE 用户状态。

PPPoE服务器

服务器配置	用户配置	批量导入	用户状态	账号到期通告
用户名	客户IP	客户MAC	描述	详情 编辑 删除
test	192.168.0.2	00:01:02:03:04:05		<input type="button" value="详情"/> <input type="button" value="编辑"/> <input type="button" value="删除"/>
共 1 条 << < 1 > >>				
<input type="button" value="添加新规则"/>				

可通过批量导入功能一次添加多个用户，添加的格式必须与 pppoes.cfg 文件格式一致。

PPPoE服务器

服务器配置

用户配置

批量导入

用户状态

通告配置

导出配置文件

 **pppoe.cfg**(单击右键，选择“目标另存为”)

导入配置文件

D:\pppoe.cfg

浏览...

导入

PPPoE 用户状态显示当前已拨入的 PPPoE 用户信息。

PPPoE服务器

服务器配置	用户配置	批量导入	用户状态	账号到期通告
用户名	客户IP	上行/下行(KBps)	有效日期	状态
共 0 条 << < 1 > >>				

根据 PPPoE 账户的到期剩余时间开始，按照设置的通告周期定时向客户发送您所设置的公告内容，用户可以通过不同的显示方式查看到公告内容。

PPPoE服务器

服务器配置
用户配置
批量导入
用户状态
账号到期通告

☒ 启用功能

通告开始时间 时
提示:帐号到期剩余时间

通告周期 分

显示方式 ☒ 公告 ☐ 链接地址 ☐ 静态页面

通告标题

通告内容

您的账号在2012年8月1日23:59分到期, 请及时续费, 谢谢。

预览

保存

6.4 USB 扩展应用 (带 USB 接口设备支持)

6.4.1 设备状态

当正确接入 USB 移动存储设备时, 本界面会显示存储设备的状态信息。在断开 USB 移动存储设备之前, 建议先点击“移除”按钮, 可更安全地卸载 USB 设备。

设备状态

USB设备状态

连接状态	 已连接		
安全移除设备	<div>移除</div> <div>点击移除按钮后将停止所有和USB设备有关的读写操作, 以便安全的卸载USB设备</div>		

分区名	总容量	已使用	未使用
part1	3.7G	4.0k	3.7G

刷新

6.4.2 共享服务

本路由器支持接入 USB 设备。启用 USB 共享可以使局域网用户共享 USB 设备上指定目录中的资源。具体配置界面如下图所示：

USB共享设置

服务设置	
存储设备状态	 已连接 刷新
USB共享服务	<input checked="" type="checkbox"/> 启用
密码	<input type="text" value="123456"/> 登录私有目录时需要输入该密码, 预设值为123456。
共享目录	\\192.168.0.1\share
私有目录	\\192.168.0.1\private 默认用户名: login
保存	

目录类型：系统根据用户使用权限，分别设置了“共享目录”和“私有目录”。直接将 USB 移动设备插到路由器上后，路由器会在 USB 设备上自动建立目录。

共享目录：用户可直接登录，可对共享目录中的资源进行访问、添加和删除操作。

私有目录：用户登录时需要输入设置的用户名和密码，默认用户名为 login。登录私有目录后，可对私有目录中的资源进行访问、添加和删除操作。

6.4.3 3G 上网服务

飞鱼星无线上网行为管理路由器支持多种上网模式：

只使用 WAN 口：只能通过 WAN 口上网，表示不启用 3G 模式上网。

3G上网服务

3G服务设置

3G流量统计

上网模式

☒只使用WAN口 ☐WAN口优先, 3G候补 ☐只使用3G [\[支持列表\]](#)

保存

WAN 口优先, 3G 候补 : 在 WAN 口全部掉线后, 路由器将自动切换到 3G 链路。配置界面如下图所示 :

3G上网服务

3G服务设置

3G流量统计

上网模式

☐只使用WAN口 ☒WAN口优先, 3G候补 ☐只使用3G [\[支持列表\]](#)

ISP

中国联通

接入点

UNINET

拨号

*99#

用户名

wcdma

密码

●●●●

连接模式

自动连接

设置自动断线等待时间: (60-3600)秒

保存

只使用 3G : 只能通过 3G 上网, 3G 链路支持自动连接、手动连接和按需连接三种模式, 可以选择任意一种模式连接。

自动连接 : 路由器在上电或掉线后会自动连接。

手动连接 : 需要进入 3G 流量统计页面中手动点击连接按钮进行拨号, 路由器不会自动进行拨号。

按需连接 : 在有访问数据的时候路由器会自动拨号连接, 若无数据, 则会在设定的时间内自动断开网络连接。

3G上网服务

3G服务设置

3G流量统计

上网模式

☐只使用WAN口 ☐WAN口优先，3G候补 ☒只使用3G [\[支持列表\]](#)

ISP

中国联通 ▼

接入点

UNINET

拨号

*99#

用户名

wcdma

密码

●●●●

连接模式

自动连接 ▼
设置自动断线等待时间: (60-3600)秒

保存

6.5 端口镜像 (部分型号支持)

端口镜像就是通过配置交换端口来把经过一个或多个端口的数据同步复制到某一个端口来实现对网络的监听。

目前我国的文化部和公安部要求网络服务场所等安装监控软件，他们通过该软件采集相关数据，分析用户使用网络的情况。飞鱼星提供的端口镜像功能可以与监控软件完美结合，在降低网络服务场所业主投资成本的情况下满足文化部和公安部的需求。其配置方法十分简单。

比如安装监控软件的计算机接到路由器的 LAN2 口，路由器 LAN1 口与 LAN3 口接主交换机，
需要实现 LAN2 口监听内网数据，具体的配置方法如下图所示：

端口镜像

端口镜像

启用

☒ 允许端口镜像功能
打勾表示下面提供的配置功能将能够被启用。

选择监听端口

☐ LAN1 ☒ LAN2 ☐ LAN3
请选择一个交换端口作为监听端口。作为监听的交换端口依旧可以正常交换使用

选择被监听端口

☒ LAN1 ☐ LAN2 ☒ LAN3
请选择您需要监听的端口，被监听端口的数据将会被发送到监听端口上。

保存

启用：打勾表示启用该功能。

选择监听端口：安装监控软件的计算机所使用的端口，本例是 LAN2（注意监听端口下一定不能连接交换机）。

选择被监听端口：主交换机所使用的端口，本例是 LAN1、LAN3。

6.6 即插即用(部分型号支持)

在路由器上启用“即插即用”功能后，系统默认开启 ARP 代理，DHCP 服务器和 DNS 代理，在主机上设置任意 IP，网关，DNS 都可以上网。若想让内网 2 台主机可互相访问，必须互相绑定对方的 IP 和 MAC。该功能通常用于酒店等环境。

即插即用

即插即用

例外IP

批量添加

☒ 启用即插即用
主机设置任意IP,网关,DNS都可以上网。该设置重启生效。

保存

批量添加：即插即用的批量添加功能可以快速地一次性添加多个 IP 地址，实现内网中的互访。

即插即用

即插即用

例外IP

批量添加

批量添加 IP

```
192.168.0.2 test1
192.168.0.3 test2
192.168.0.4 test3
```

保存

6.7 SNMP 客户端 (3050 平台不支持)

启用 SNMP 服务之后，就可以在远程使用 SNMP 软件管理和监视设备。具体配置界面如下图所示：

远程管理

远程管理配置

远程管理

☒ 启用

中心端地址

192.168.16.160

用户ID

EC6C9F021FAC

高级配置

保存

6.8 SVPN (仅 V7 平台支持)

SVPN 支持从 VPN 路由器连接到 VPN 路由器。比如：某网络服务场所业主拥有 A 和 B 两个营业点，各使用一台飞鱼星具备 SVPN 功能的路由器，A 路由器采用双线接入（网通 + 电信），B 路

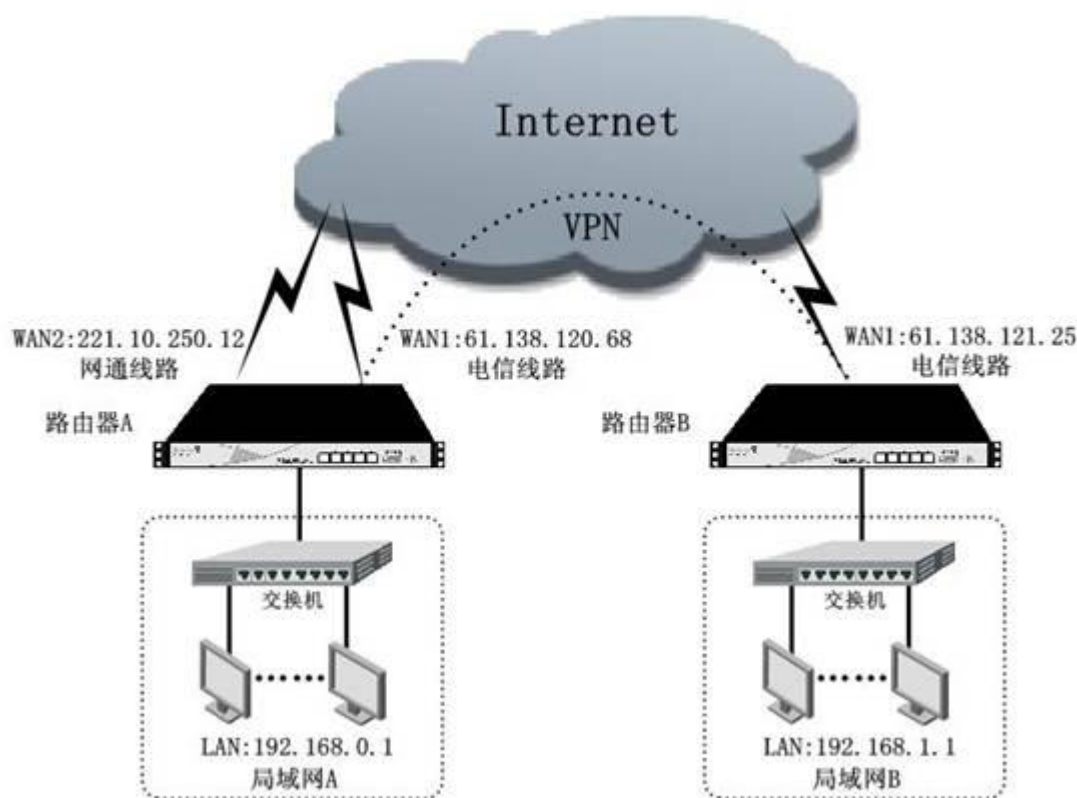
由器只是电信单线接入，他想让 B 营业点的用户访问网通时借用 A 营业点的网通线路出访，这个需求通过飞鱼星的 SVPN 功能可以实现。



注意：此功能配置以后需要重新启动路由器才生效。

首先 将 A 路由器配置为 SVPN 服务端 假设它的当前网络接口参数为 内网网关 192.168.0.1，子网掩码 255.255.255.0，WAN1 电信 IP 61.138.120.68，WAN2 网通 IP 221.10.250.12，隧道地址为 192.168.0.2。B 路由器配置为 SVPN 客户端，假设它的当前网络接口参数为，内网网关 192.168.1.1，子网掩码 255.255.255.0，WAN1 电信 IP 61.138.121.25。

网络拓扑图如下所示：



A 路由器的配置方法是：首先，将“启用隧道服务”打勾，隧道类型选择“服务端”，并保存。

添加一条规则，具体的参数如图所示：

隧道配置

隧道配置

☒ 启用隧道服务

隧道类型

☒ 服务端 ☐ 客户端

保存

点击保存后可以对服务端进行配置：

服务端配置

服务端配置

不使用

☒ 不使用这条规则

服务端地址

61.130.120.68

请输入服务端地址，例如WAN1口外网地址。

客户端地址

61.138.121.25

客户端的隧道地址

192.168.0.2

隧道带宽

256

KBps

请输入您的隧道带宽，不限制则留空。

备注

服务端配置

保存

返回

不使用：打勾表示不使用本条规则，规则并不被删除。**服务端地址：**作为 SVPN 服务端的 WAN 口 IP 地址，因为本例中的客户端使用电信线路，在这里服务端地址就选择电信 IP，即 WAN1 口 IP。**客户端地址：**作为 SVPN 客户端的 WAN 口的 IP 地址。**客户端隧道地址：**由服务端给客户端分配的隧道地址，此地址不是服务端内网网关且必须与服务端内网网关在同一网段。本例分配的是 192.168.0.2。

隧道带宽：服务端为客户端分配的隧道带宽。本例的意思是服务端给客户端分配 256KB(即 2Mbps) 的网通带宽。

备注：可以在这里简单备注一下本条规则。

点击“保存”按钮，并重新启动路由器，重启成功后，规则生效。

B 路由器的配置方法是：首先，将“启用隧道服务”打勾，隧道类型选择“客户端”，并保存。
然后在新出现的界面中作如下图所示的配置：

隧道配置

隧道配置	服务端配置
<input checked="" type="checkbox"/> 启用隧道服务	
隧道类型	<input type="radio"/> 服务端 <input checked="" type="radio"/> 客户端
服务端地址	<input type="text" value="61.138.120.68"/> 请输入服务端地址
客户端的隧道地址	<input type="text" value="192.168.0.2"/> 请输入隧道地址，具体值请咨询服务方。
服务端的隧道地址	<input type="text" value="192.168.0.1"/> 请输入服务端内网网关地址。
隧道带宽	<input type="text" value="256"/> KBps 请输入您的隧道带宽，不限制则留空。
隧道策略	新联通 ▼
隧道通断检测	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁止
隧道通断检测地址	<input type="text"/> 请输入隧道通断检测地址，为空时缺省是服务端网关地址。
<input type="button" value="保存"/>	

服务端地址：作为 SVPN 服务端的 WAN 口 IP 地址，应该与服务端当前配置的 IP 一致。本例为 61.138.120.68。

客户端隧道地址：由服务端给客户端分配的隧道地址，此地址不是服务端内网网关且必须与服务端内网网关在同一网段。本例分配的是 192.168.0.2。

服务端隧道地址：服务端内网网关地址。

隧道带宽：服务端为客户端分配的隧道带宽。本例的意思是服务端给客户端分配 256KB(即 2Mbps) 的网通带宽。

隧道策略：可选项为新联通、电信和教育网。本例选择新联通。

隧道状态检测：客户端探测隧道是否正常。请保持默认选择“禁用”。

备注：可以在这里简单备注一下本条规则。

保存以后，重新启动 B 路由器使配置生效。然后可以在 B 营业点的计算机上运行 tracert 命令跟踪一个新联通的 IP，可以看出，数据是从 A 路由器的联通线路出访的。

6.9 IPsec 网对网（部分型号支持）

IPsec 协议是网络层协议，是为保障 IP 通信安全而提供的一系列协议族。IPsec 针对数据在通过公共网络时的数据完整性、安全性和合法性等问题设计了一整套隧道、加密和认证方案。IPsec 能为 IPv4 网络提供能共同使用的、高品质的、基于加密的安全机制。提供包括存取控制、无连接数据的完整性、数据源认证、防止重发攻击、基于加密的数据机密性和受限数据流的机密性服务。

IPSEC Net-To-Net 的配置方法如下：

启用 IPSEC Net-To-Net，并保存，具体配置界面如下图所示：



点击“IPSEC Net-To-Net 列表”，并添加新规则，具体配置界面如下图所示：

IPSEC Net-To-Net隧道配置

规则设置

名称	<input type="text" value="test"/>	
主动连接	<input checked="" type="checkbox"/> 启用IPSEC Net-To-Net主动连接	
保持连接	<input checked="" type="checkbox"/> 用ping保持连接	
本地隧道接口	<input type="text" value="WAN1"/>	
本地网络	<input type="text" value="192.168.5.0"/>	掩码： <input type="text" value="255.255.255.0"/>
远程隧道地址	<input type="text" value="221.237.74.180"/>	
远程网络	<input type="text" value="192.168.0.0"/>	掩码： <input type="text" value="255.255.255.0"/>
备份链路	<input type="checkbox"/> 启用	
IKE验证模式	<input type="text" value="IKE-PSK"/>	
PSK密钥	<input type="text" value="123456"/>	

IPSEC高级设置

保存

返回

名称：IPSec 隧道名，请用英文字母开头。

主动连接：若两个路由器之间建立 IPSEC Net-To-Net 隧道，只需在其中一个路由器上启用主动连接即可。

本地隧道接口：选择使用哪个 WAN 口进行 IPSEC Net-To-Net 连接。

本地网络/掩码：与该路由器的内网网段/掩码一致。

远程隧道地址：对端 WAN 口的当前 IP 地址，也可以填写域名。

远程网络/掩码：与对端路由器的内网网段/掩码一致。

IKE 验证模式：默认为 IKE-PSK，两端的验证模式必须相同。

PSK 密钥：密钥由数字和英文字母组成，两端的 PSK 密钥必须相同。

保存后界面如下图所示：

IPSEC Net-To-Net

IPSEC Net-To-Net列表					
名称	本地隧道接口	远程隧道地址	远程网络	编辑	删除
a1	WAN1	2.2.2.2	3.3.3.3/255.255.255.0		
共 1 条 << < 1 > >>					
<div>删除所有规则</div> <div>添加新规则</div>					

在两端都配置完毕并保存后，IPSEC Net-To-Net 会自动拨号。可以通过“IPSEC VPN 隧道状态”查看连接情况，具体界面如下图所示：

IPSEC Net-To-Net

IPSEC Net-To-Net列表			
名称	远程隧道地址	状态	操作
conn_a1	0.0.0.0	断开	连接
共 1 条 << < 1 > >>			

6.10 IPSec 点对点网（部分型号支持）

IPSEC 点对点网功能，可以实现本地网络与远程 PC 之间的安全加密互访。

点击选择“是否启用 IPSEC Road Warrior 服务”启用该服务。在“本地网络/掩码”处填入与该路由内网地址/掩码一致的信息；选择“IKE 验证模式”，默认为“IKE-PSK”；设置“PSK 密钥”。

完成以上设置，具体配置情况如下图所示：

IPSEC Road Warrior隧道配置

IPSEC Road Warrior设置

☒ 是否启用IPSEC Road Warrior服务

本地网络

192.168.5.0

掩码：255.255.255.0

IKE验证模式

IKE-PSK ▼

PSK密钥

123456

IPSEC高级设置

保存

6.11 L2TP IPsec (部分型号支持)

飞鱼星路由器支持 L2TP IPSEC VPN，这种方式的 VPN 与 PPTP VPN 相比，安全性更高。具体配置方法与拨号方法如下所示：

启用该功能，设置 PSK 密钥为 123456，客户端地址段为 192.168.0.100-192.168.0.105，与路由器的 LAN 口在同一个网段。

具体配置界面如下图所示：

L2TP Over IPSEC

L2TP IPSEC设置

L2TP用户

拨入列表

☒ 启用L2TP Over IPSEC服务

最大L2TP连接数

16

PSK密钥

123456

L2TP客户端地址范围。

192.168.0.100

到

192.168.0.105

例如：192.168.0.151---192.168.0.158

保存

L2TP IPSEC 设置完成后，点击“L2TP 用户”，选择“添加用户”，进入“编辑用户”页面。

比如：添加一个用户名为“test”，密码为“1234”的用户。

具体配置页面如下图所示：

编辑用户

L2TP用户

用户名

密码 (确认密码)

描述

点击“保存”后，页面如下图所示：

编辑用户

L2TP IPSEC设置 L2TP用户 拨入列表

用户名	描述	编辑	删除
test	test		

共 1 条 << < 1 > >>

下面介绍在 PC 上的配置方法，注意“网络”标签下的“VPN 的类型”必须选择为“L2TP IPSec VPN”。“安全”标签下的 IPSec 设置，密钥设置为 123456，与路由器上的设置保持一致。





“常规” 标签下的目的地址设置为路由器的 WAN1 口 IP 地址。



填写用户名和密码，开始拨号。



拨号成功后，就可以在拨入列表中看到用户名，拨入 IP 等信息。

附录 A 路由器选配电缆说明

1, 以太网接口电缆

路由器的以太网接口电缆为 8 芯非屏蔽双绞线, 1、2 脚为发送端, 3、6 脚为接收端; 和计算机网卡的 10BASE-T 接口相同, 可以与 HUB 直接相连。

RJ-45 管脚号	信号	信号描述
1	TxData+	发送数据
2	TxData-	发送数据
3	RxData+	接收数据
4	---	电话接头
5	---	电话接头
6	RxData-	接收数据
7	---	网络测试
8	---	网络测试

附录 B WindowsXP 环境下的 TCP/IP 配置

本章介绍如何为您的个人计算机配置 TCP/IP 协议。首先请您确认在计算机中已经正确安装了网卡。以下步骤将指导您正确设置计算机与路由器连接时的 TCP/IP 配置。

- 1、依次点击：开始 控制面板 网络连接。

LAN 或高速 Internet



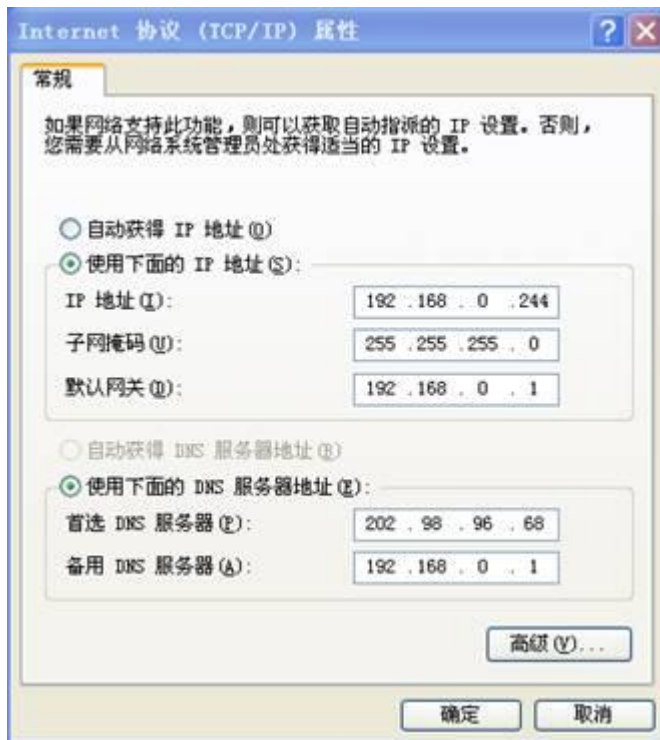
- 2、双击“网络连接”，选中“本地连接”击右键选择“属性”。

- 3、双击 Internet 协议 (TCP/IP) 。

- 4、现在，您有两种设置方法：

第一种，手工设置 IP 地址

- 1) 选中“使用下面的 IP 地址”，在 IP 地址栏中填写 IP 地址：192.168.0.244，子网掩码：255.255.255.0，缺省网关：192.168.0.1（因为路由器的默认 IP 地址为 192.168.0.1）。
- 2) 选中“使用下面的 DNS 服务器地址”，在 DNS 设置栏中，首选 DNS 服务器填写 ISP 为您提供的 DNS 服务器地址，备用 DNS 服务器填写路由器的默认 IP 地址。
- 3) 单击“确定”即可。配置结果如下图所示：



第二种，通过 DHCP 服务器设置 IP 地址

- 1) 选中“自动获得 IP 地址”；
- 2) 选中“自动获得 DNS 服务器地址”，
- 3) 单击“确定”即可。配置结果如下图所示：



附录 C 路由器固件升级失败恢复步骤

当您在升级固件的过程中意外断电，路由器的主系统会被损坏（其表现为 sys 灯不是以每秒 1 次的频率闪烁，它或者长亮或者不亮或者快速闪烁），这时候您可以使用路由器的备份系统恢复固件，具体的操作步骤如下：

第一步：固件升级失败以后，路由器的内网口默认 IP 会变为 192.168.0.1，LAN 口直接连一台 PC，ping 通 192.168.0.1 以后，在浏览器上输入 <http://192.168.0.1/>，回车以后会出现以下的界面：



以上就是路由器的智能备份系统界面。

第二步：点击“浏览”，选择正确的升级固件，点击“开始恢复”按钮，路由器就重新恢复主系统。注意固件恢复的过程中不要断电，否则无法完成固件恢复。固件恢复的过程中浏览器会有进度提示。

第三步，固件恢复完毕，路由器会自动重启。重启成功后 sys 以每秒 1 次的频率正常闪烁。此时您用路由器之前配置的内口 IP 就可以登录 WEB 管理界面，您会发现之前的配置没有丢失。

附录 D 常见问题解答

1. 路由器不能上网，不能进入登录界面？

- 1) 路由器工作指示灯是否正常。正常情况下，路由器 system 指示灯以 1Hz 的频率闪烁。
- 2) IP 地址是否正确。计算机 ip 地址与路由器内网接口地址应当在同一个网段内，并且不与路由器内口地址相同，可以用 ping 工具检查是否连通。
- 3) WEB 管理端口是否正确。可能更改了路由器 WEB 管理系统的管理端口，因此登录时必须使用正确的端口匹配。
- 4) 密码是否正确。出现登录窗口后，输入密码依然不能登录，可以确定密码错。
- 5) 如果不能确定路由器的内网接口地址、WEB 管理端口和密码，请将路由器恢复到出厂设置，使用默认参数登录。

2. 忘记路由器的管理密码怎么办？

当您忘记了登录路由器的密码或是因为其它人为因素使用不当时，可能希望设备能够恢复到出厂设置。路由器通电正常启动后，按一下前面板上的 RST 键（复位键）后释放，路由器将重新启动并恢复出厂设置。这个操作会清空用户的全部设置，请慎用。

3. 除了 Windows 系统，使用其它操作系统（如 Unix、OS/2、Linux 等）的计算机能否使用本宽带路由器？

能，本宽带路由器支持所有符合 TCP/IP 通信协议的操作系统。

4. 路由器设置正确，部分客户端上不了网？

首先请检查您的客户端网线连接是否正确，如正确请检查客户端的 TCP/IP 协议配置是否正确、网关配置是否正确。注意：网关一定要设置为本路由器 LAN 口的 IP 地址。

5. 为什么我的计算机出现 IP 冲突画面？

当您的局域网内有手动设定 IP 时，请不要与本路由器 DHCP 服务器（如启动）IP 范围发生冲突。

6. 如何知道计算机的 IP 地址及网卡 MAC 地址？

在 Windows XP/2000/NT 系统中，在命令提示符模式下运行 ipconfig/all

在 Windows 95/98 系统中，在命令提示符模式下运行 winipcfg

7. 我的计算机如何释放或重新分配动态 IP 地址？

在 Windows 系统中，在命令提示符模式下运行 “ipconfig/release” 即可释放已经分配到的 IP 地址，运行 “ipconfig/renew” 即可重新分配 IP 地址。

8. 路由器的 WEB 配置页面没有正确显示我刚才设定的值？

本地 PC 可能没有从路由器上取得新的 WEB 页面，您看到的可能是本地 PC 浏览器中缓存的 WEB 页面。请重新启动一个浏览器后刷新即可。

9. 路由器可支持多少客户端同时上网？

路由器可支持的同时上网的客户端数量受很多条件影响，如广域网接入的带宽限制，局域网内部的数据流量，用户对上网速度的要求等等，请依出口带宽合理配置客户端计算机上网的数量。

10. 什么是 DMZ？飞鱼星宽带路由器支持 DMZ 吗？最多支持多少台 DMZ 主机呢？

DMZ(Demilitarized Zone 非军事区)这一功能可以使某台特定计算机向互联网完全开放，支持更多的网络应用。DMZ 允许一个计算机完全暴露在外网上，用户配置为 DMZ 主机的计算机必须使用静态 IP。

飞鱼星路由器通过一对一的网络地址转换方式支持 DMZ 功能。

飞鱼星路由器支持 DMZ 主机的数量只取决于您拥有的合法 IP 地址的数量，路由器本身没有限制。请注意：当一台 PC 设置成 DMZ 主机后。这台 PC 就失去了 NAT 防火墙的保护，所以请谨慎使用。

如有更多问题敬请访问飞鱼星科技网站 <http://www.adslr.com>



飞鱼星产品咨询热线: **400-8115-315**

飞鱼星科技开发有限公司

地址：四川省成都市高新区益州大道中段 1800 号天府软件园 G 区 4 栋 7-8F

邮编：610041 电话：028-85336711 85336722 85336733

传真：028-85336799