



用户手册

FPX9102H

目 录

关于本指南.....	4
目的.....	6
交叉引用.....	6
反馈.....	6
产品符合声明.....	7
CE 认证.....	7
FCC 认证.....	7
B 类数字设备或周边设备.....	7
操作安全要则.....	8
警告和注意事项.....	9
警告.....	9
注意事项.....	9
第 1 章 产品介绍.....	9
FPX9102H.....	10
指示灯和接口.....	11
LED 指示灯介绍.....	11
接口介绍.....	12
硬件安装.....	13
安装准备.....	13
安装步骤.....	14
第 2 章 基本配置.....	15
Web 页面登录.....	16
Web 界面管理.....	16
关于密码.....	17
网络配置.....	18
配置网络连接.....	18
无线配置.....	19
FXO 口.....	20
第 3 章 Web 界面管理.....	23
Web 页面结构.....	24
Web interface.....	24
状态.....	25
系统信息.....	25
内网主机信息.....	27
系统日志.....	27
网络和安全.....	28
WAN 口设置.....	28
LAN 口设置.....	34
IPv6 设置.....	35
VPN 设置.....	38
端口映射.....	40
DMZ.....	42
QOS.....	42

端口限速.....	44
端口管理.....	44
路由配置.....	45
高级设置.....	46
IPPBX.....	47
基本设置.....	47
无线 2.4G 设置.....	50
基本设置.....	50
无线安全.....	52
Wi-Fi 多媒体(WMM).....	55
无线分布式部署(WDS).....	55
Wi-Fi 保护设置(WPS).....	56
无线客户端(Station Info).....	57
高级设置.....	58
无线 5G 设置.....	59
安全.....	59
MAC/IP/Port/ACL.....	60
内容过滤.....	61
应用.....	63
高级 NAT.....	63
UPnP.....	63
存储.....	65
Disk 管理.....	65
FTP 设置.....	66
管理.....	67
管理.....	67
固件升级.....	70
计划任务.....	71
自动更新 (Provision)	72
SNMP.....	73
TR-069.....	74
诊断.....	75
工作模式.....	78
第 4 章 故障排除.....	79
接通电源后无反应.....	79
无法登录设备的网页.....	79
忘记密码.....	79

关于本指南

感谢您购买我们的无线 VoIP 路由器，我们的设备是一个高集成度的综合接入设备，是一个依据 IEEE802.11ac 标准的高端多合一网关产品。本产品为个体用户，SOHO（小型办公室），小型企业等提供高性能的接入服务。

它提供多方面的管理功能，可以对 DHCP、DMZ 主机、虚拟服务器、防火墙等进行管理；能够组建内部局域网，允许多台计算机共享一条单独宽带线路和 ISP 账号；特有的防火墙功能，可以过滤不良网站；支持禁用 SSID 广播方式，可以防止 AP 广播 SSID 的网络名称，从而可以解决 SSID 广播造成的泄密；支持 64 / 128 位 WEP 无线数据加密，保证数据在无线网络中传输的安全；支持 DHCP 自动分配 IP 地址和动态 / 静态路由；支持访问控制，网络管理员可以通过路由器控制局域网中所有计算机的上网权限；支持虚拟服务器和 DMZ 主机，以满足特殊应用程序的需要；支持远程管理和系统日志，以方便网络管理员对网络的管理和实时监控；支持 UPNP、语音视频传输、在线影音传输、在线游戏等丰富功能。



本指南包含以下内容：

- [第一章：产品介绍](#)
- [第二章：基本配置](#)
- [第三章：Web 界面管理](#)
- [第四章：常见故障排除](#)

联系飞音时代

网站: <http://www.flyingvoice.cn/>

热线: 010-67886296 0755-26099365

北京: 北京市石景山八大处路 49 号点石商务公园 1 号楼 508-509

深圳: 深圳市南山区众创产业园 B52 栋 207-209 室

目的

飞音产品文件旨在指导和协助人员操作，安装、维护以及辅助设备。建议所有参与此类活动的人员接受适当培训。飞音严正声明：所有的责任，包括任何由于客户或可以代表客户的人直接或间接的误操作而导致的设备丢失、损坏或系统性能降低等风险将由您来承担，因此请依照并遵守本文档中的说明，系统参数或建议来配置设备。

交叉引用

对外部出版物的引用以斜体显示。强调的其他交叉引用是引用的活动链接。

本文件分为几个章节，部分章节没有编号，但是在每个页面的顶部单独命名，并列在目录中。

反馈

我们感谢用户对我们文档的反馈，这包括对我们文档的结构，内容，准确性或完整性的反馈。发送反馈给 support@flyingvoice.com。

产品符合声明

CE 认证

本设备符合欧盟的安规指令 2014/35/EU 和电磁兼容指令 2014/30/EU。

FCC 认证

本设备符合 FCC 规则第 15 部分的规定。操作符合以下两个条件：

1. 本设备不会产生有害干扰。
2. 该设备必须接受任何收到的干扰，包括可能导致意外操作的干扰。

B 类数字设备或周边设备

该设备已经过测试，符合 FCC 规则第 15 部分对 B 类数字设备的限制。这些限制旨在提供合理的保护，防止住宅安装中的有害干扰。该设备可以产生，使用和辐射射频能量。如果未按照说明手册进行安装和使用，可能会对无线电通信造成有害干扰。但是不能保证特定安装中不会发生干扰。



注意

未经负责合规方明确批准的变更或修改可能会使用户操作设备的权力失效。

如果该设备产生有害干扰的无线电或电视接收，可以通过打开和关闭设备确定，用户可以尝试纠正干扰，采取以下一项或多项措施：

- 调整接收天线的方向或位置。
- 增加设备和接收器之间的距离。
- 将设备连接到与接收器相连的电路上的插座。
- 咨询经销商或有经验的广播/电视技术人员寻求帮助。

操作安全要则



警告

- 未负荷过重的电源插座或破损的线体及插头均可能引发电击或火灾。应定期检查相关电力线缆，若其外观已有损毁，请立即更换。
 - 请使用为你提供电源适配器。如果使用其他电源适配器，可能会损坏设备或使设备无法正常工作。
 - 本产品应安装在通风且无高温无阳光照射的位置，以避免本产品及相关配件过热而发生故障。
 - 通信设备需注意防潮防湿，严防进水。进水将导致设备工作不正常，更可能因短路造成其他危险。
 - 请勿将本产品放置在不稳固的支撑物上。
-

警告和注意事项

以下说明在本文档中如何使用警告和注意事项。

警告

警告先于包含潜在危险情况的说明。警告用于警告读者可能会导致生命损失或身体伤害的危险。警告具有以下格式：



警告

警告文字和后果如果不符合警告中的说明。

注意事项

注意事项先于指令，并在系统、软件或系统中的各项设备有可能损坏时使用。但是这种损坏对人员没有任何危害。注意格式如下：



注意

如果不遵守说明书中的注意事项，注意后果。

第 1 章 产品介绍

本章包含以下内容：

- [FPX9102H](#)
- [指示灯和接口](#)
- [硬件安装](#)
- [安装准备](#)
- [安装步骤](#)

FPX9102H

功能/型号	FPX9102H
-------	----------

产品图片

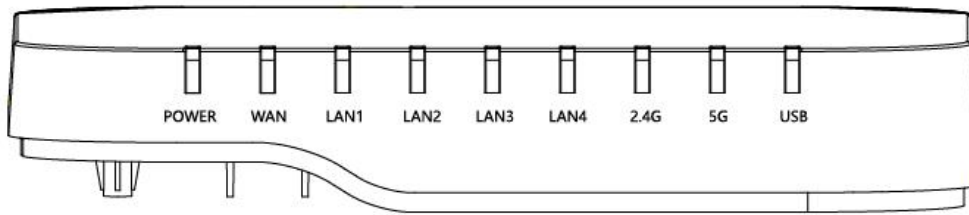


WAN 口	1
LAN 口	4
FXO 口	2
以太网口	5* RJ45 10/100/1000M
USB 接口	Yes
限速 NAT	Yes
传真	T.30, T.38 Fax
WiFi 支持	2.4G 2T2R (300Mbps),5G 2T2R (867Mbps)
Voice 编码	G.711 (A-law/U-law), G.729A/B, G.723,G.726
管理	语音菜单, Web 管理, 自动配置 TFTP/HTTP/HTTPS, TR069, SNMP
Vlan	支持

指示灯和接口

LED 指示灯介绍

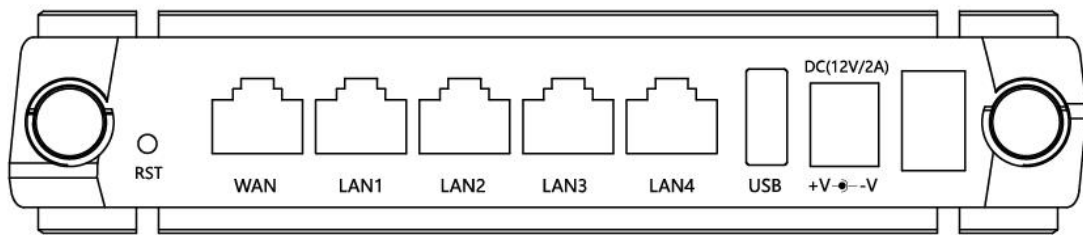
FPX9102H



LED	状态	说明
PHONE1/2	闪烁(绿色)	有业务流传输或者正在注册
	常亮(绿色)	成功注册到软交换机，但无业务流
	熄灭	未注册或注册失败
5G	闪烁(绿色)	有数据传输
	常亮(绿色)	5G 工作
	熄灭	无 5G
2.4G	常亮(绿色)	2.4G 工作
	闪烁(绿色)	有数据传输
	熄灭	无 2.4G
LAN 1/2/3/4	常亮 (绿色)	网口已连接，但无数据传输。
	熄灭	系统未上电或者网口未连接网络设备
	闪烁(绿色)	有数据传输
WAN	常亮 (绿色)	网络连接成功，物理连接已经建立
	熄灭	网络没有连接或者连接失败
	闪烁(绿色)	有数据传输

接口介绍

FPX9102H



界面	说明
POWER	连接电源适配器
PHONE1/2	连接电话
LAN(1/2/3/4)	连接本地网络设备 WiFi 开关
WAN	连接访问互联网
RST	恢复出厂设置按钮，长按 5s 后设备恢复出厂设置

硬件安装

安装准备

在安装设备前，请先检查物品是否齐全，安装条件是否具备。打开设备的包装箱，对照物品清单检查箱内物品是否齐全。如果发现包装箱内物品与表中不符，请直接与我公司联系。该设备可安置在桌面上，也可安装在墙壁上。



注意

- 安装地点需具备设备与外部连接的条件（例如：电源线、网线、PC 机等），交流电源插座应采用单相三芯电源插座，并确保地线可靠接地。
- 安装地点的环境要保证足够的空气流动，以利于设备散热（设备适宜的工作温度为-10℃～45℃）。
- 安装地点应具备防水、防潮、防雷等条件（设备适宜的环境湿度为 10%～95%）。

安装步骤

在设置您的路由器之前，您必须正确连接您的设备：

上行以太网连接

- 用 RJ-11 电缆将电话端口连接到固定电话插口；
- 用以太网电缆将设备 wan 口和调制解调器连接起来；
- 将您计算机与设备的 lan 口通过 RJ-45 电缆连接起来；
- 电源线的一端连接到该设备的电源接口，另一端连接到电源插座；
- 启动路由器；
- 检查电源、wan 口和 lan 口的 LED 灯以确保网络连接。

警告



请勿尝试使用不支持的电源适配器，并且在配置或更设备时不要拔掉电源。使用其他电源适配器可能会损坏设备，并将导致制造商保修失效。

第 2 章 基本配置

本章内容包含：

- [Web 页面登录](#)
- [网络配置](#)
- [无线配置](#)
- [FX0 口使用](#)

Web 页面登录

我们的设备支持两级管理：管理员和用户。

(1) 对于管理员模式操作，请在用户名/密码上键入“admin / admin”，然后单击“登录”按钮开始系统配置，该级别可以配置操作设备的所有参数。

(2) 对于用户模式操作，请在用户名/密码上键入“user/user”，然后单击“登录”按钮开始配置，该级别的用户能够浏览以及配置部分的话机参数，SIP 线路中的一些不能被改变的参数，例如服务器地址和端口，该级别用户无法配置。

Web 界面管理

FPX9102H 内置 Web 服务器以响应 HTTP get/post 请求。用户可以使用 Web 浏览器，比如说微软公司的 IE，来登录设备的页面并且配置该设备。

LAN 口登录

确保您的 PC 正确地连接到路由器的 LAN 端口。

登录 Web 页面的 URL 格式为：<http://LAN 端口 IP 地址>，一般默认 LAN 端口 IP 地址为：192.168.1.1，请在地址输入栏输入相应的地址：<http://192.168.1.1>，然后页面会跳转到设备的登录页面，如下图：



WAN口登录

确保您的 PC 正确连接到路由器的 WAN 端口。

获取 WAN 口 IP 地址：您可以使用 IVR 语音提示获取；或可以通过 LAN 端口登录到设备的 Web 管理界面并导航到状态--基本设置页面，可在该页面查看 WAN 端口的 IP 地址。

登录 Web 页面：打开 PC 上的 Web 浏览器，然后输入 [http: // <WAN 端口的 IP 地址>](http://<WAN 端口的 IP 地址>)。将打开以下登录页面，输入用户名和密码，点击登录。



用户名
 密码

关于密码

设备有两种登录的级别，分别是管理员级别和普通用户级别，不同的标准有不同的密码。

默认的管理员级别的登录密码是 admin/admin

默认普通用户级别的登录密码是 user/user

1.修改密码

登录设备 WEB 页面，切换到管理--管理页面，找到“重置密码”标签，选择用户类型，即可设置新用户名和密码，点击“保存”。

管理员设置

重置密码

用户类型	<input type="text" value="超级管理员"/>
新用户名	<input type="text" value="admin"/>
新密码	<input type="password"/> (最大长度是25)
确认密码	<input type="password"/>

2.忘记密码

如果用户更改了 ATA 页面登录的密码，但忘记了，导致用户不能进入 ATA 的配置界面，此时请按住恢复出厂键 5 秒以上，将设备恢复出厂设置，再使用默认密码登陆。

注意

如果出现以下的提示：



上传配置或者恢复出厂设置后，你需要重启以生效！

请**重启**设备确保更改生效。

网络配置

配置网络连接

从网络> WAN 页面，WAN 连接可能被插入或删除。有关 Internet 连接设置的更多信息，请参见下表：

The screenshot shows the WAN configuration page with the following settings:

- INTERNET接入方式: DHCP
- DHCP Server: [Empty text box]
- MAC地址克隆: 禁止
- LAN连接模式: 路由
- DNS模式: 自动
- 主DNS地址: [Empty text box]
- 从DNS地址: [Empty text box]

参数名称	描述
INTERNET 接入方式	INTERNET 接入方式选择：DHCP，静态 IP，PPPoE
DHCP Server	DHCP 服务器 IP 地址
MAC 地址克隆	是否开启 MAC 地址克隆功能
LAN 连接模式	LAN 口的连接方式：路由，桥接
DNS 模式	选择 DNS 模式，选项为自动和指定： 1.当 DNS 模式为自动时，LAN 端口下的设备将自动获取首选 DNS 和备用 DNS 2.当 DNS 模式为“指定”时，用户应手动配置首选 DNS 和备用 DNS
主 DNS	因特网端口的首选 DNS
从 DNS	因特网端口的备选 DNS

无线配置

要设置无线连接，请执行以下步骤：

基本无线设置

无线网络

WIFI开关 1

连接模式 2

网络模式

无线网络名称1 3 开启 4 隐藏 隔离 最大客户端数

无线网络名称2 开启 隐藏 隔离 最大客户端数

广播网络名(SSID) 开启 禁止

AP隔离 开启 禁止

虚拟网络间隔离 开启 禁止

BSSID

飞音企业无绳电话模式 开启 禁止

1. WIFI 开关：请选择“开启”，开启无线网络。
2. 连接模式：默认是“无线接入点”模式。
3. 无线网络名称 1：您可以在这里设置您的无线网络的名称。
4. 请不要忘记同时勾选“开启”选项，否则无线终端设备将无法扫描到该无线

SSID

选择SSID

SSID选择 5

"91020D6CD0"

安全模式 6

WPA

WPA算法 TKIP AES TKIPAES

通行口令 7

私钥更新间隔 秒 (0 ~ 86400)

访问策略

策略

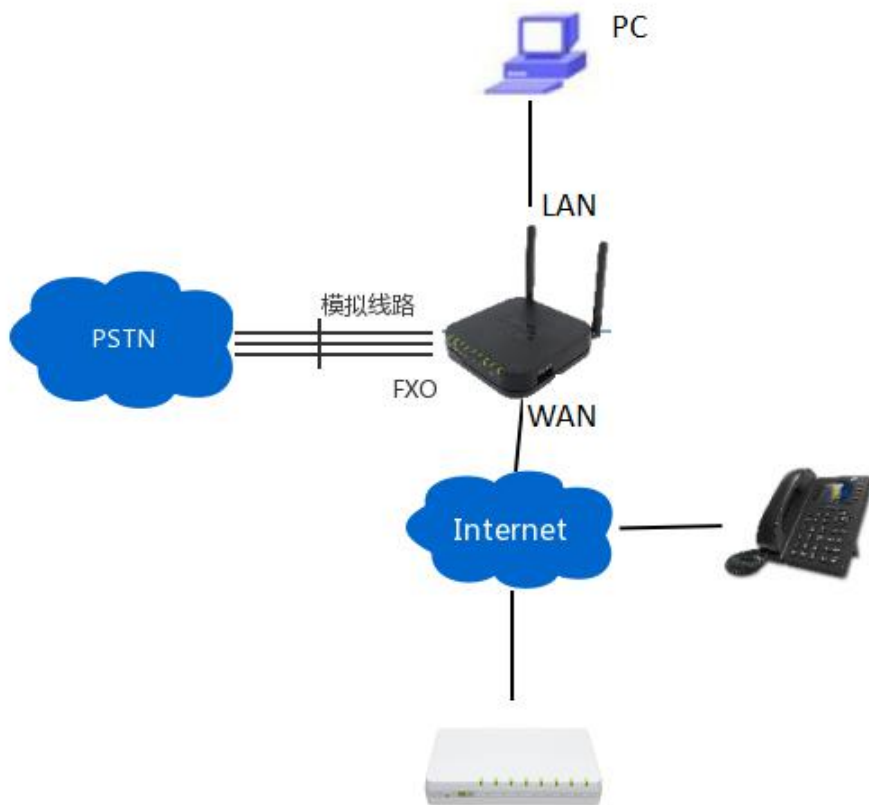
新增： (最大规则数为 64)

5. SSID 选择：选择需要加密的 SSID（无线网络名称）。
6. 安全模式：选择加密的方式。
7. 通行口令：设置无线密码。
8. 全部设置完成后，需要保存设置，并重启设备。之后可以正常使用该无线网络。
9. 5G 的无线和 2.4G 无线设置一样

FXO 口

请按照如下步骤配置使用 FXO 口：

1. 请按图连接 PSTN 线和 FPX9102H。



2. 在 FPX9102H 上有简单的 PBX 功能，默认有 10 个分机号码，您可以在办公室网络中使用这些号码。



分机管理

编号	分机	密码	名字	客户端 MAC
1 <input type="checkbox"/>	600	password600	600	
2 <input type="checkbox"/>	601	password601	601	
3 <input type="checkbox"/>	602	password602	602	
4 <input type="checkbox"/>	603	password603	603	
5 <input type="checkbox"/>	604	password604	604	
6 <input type="checkbox"/>	605	password605	605	
7 <input type="checkbox"/>	606	password606	606	
8 <input type="checkbox"/>	607	password607	607	
9 <input type="checkbox"/>	608	password608	608	
10 <input type="checkbox"/>	609	password609	609	

3. 或者您可以自己手动再添加一些号码，添加号码的步骤：

添加或修改分机：

分机

密码

名字

客户端 MAC

分机：分机号码

密码：注册分机号码时的密码

名字：分机号码显示的名字

客户端 MAC：如果想要用一个分机号码绑定一个特定的设备，可以将设备的 MAC 地址填写在这里。

在配置完成后，请点击“应用”，并重启设备。

设备重启后，就可以正常的使用这些分机号了。

您也可以在“状态”页面检查这些分机号码的状态。

账号状态

账号状态

SIP Trunk 1

SIP Trunk 2

SIP Trunk 3

SIP Trunk 4

SIP Trunk 5

SIP Trunk 6

SIP Trunk 7

SIP Trunk 8

Exten1 600,Unavailable

Exten2 601,Unavailable

Exten3 602,Unavailable

Exten4 603,Unavailable

Exten5 604,Unavailable

Exten6 605,Unavailable

Exten7 606,Unavailable

第 3 章 Web 界面管理

本章指导用户通过管理模式操作执行高级（完整）配置。本章包括：

- Web 界面结构
- 状态
- 网络
- IPPBX
- 无线 2.4GHz
- 无线 5GHz
- 安全
- 应用
- 存储
- 管理

Web 页面结构

Web interface



名称	描述
主导航栏	顶部导航栏单击顶部导航栏（标记为“1”的区域）中的选项。多显示子导航栏中的选项
次导航栏	子导航栏单击子导航栏以选择配置页面（标记的区域）为“2”）
设备信息	参数配置此区域显示配置的当前参数（例如区域标记为“3”）
	对参数进行变更后需要点击此按钮进行保存。点击 保存 后，有重新启动的提示则需要重启设备
	点击 取消 变更
	对参数进行变更后需要点击次按钮进行保存。点击保存后，有像 上传配置或者恢复出厂设置后，你需要重启以生效！ 这样的重新启动的提示，则需要重启设备
	对参数进行变更后需要点击此按钮进行保存和应用，点击 保存并应用 ，修改参数立即生效

状态

该网页显示的产品，网络和系统状态信息，包括产品信息、SIP 帐户状态，FXS 端口状态，网络状态和无线信息。

系统信息

如图所示是状态页面：

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
系统信息	内网主机信息	系统日志						

设备信息

设备信息

设备名称	FPX9102H
网络(WAN) MAC地址	00:21:F2:0D:6C:D1
PC(LAN) MAC地址	00:21:F2:0D:6C:D0
硬件版本	V3.1
Loader版本号	V3.06(Nov 1 2016 17:12:51)
软件版本	V3.11(201611182233)
序列号	FLY69167000116

账号状态

账号状态

SIP Trunk 1	
SIP Trunk 2	
SIP Trunk 3	
SIP Trunk 4	
SIP Trunk 5	
SIP Trunk 6	
SIP Trunk 7	
SIP Trunk 8	
Exten1	600,Unavailable
Exten2	601,Unavailable
Exten3	602,Unavailable

内网主机信息

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
系统信息 内网主机信息 系统日志								
内网主机信息								
MAC地址	IP地址	接口类型	地址类型	租剩时间	主机名	状态		
8E:8F:1D:B6:6D:3F	59.11.128.247	LAN4	DHCP	23:37:1	SKY-20170519RRJ	活跃		
IPv6内网主机信息								
MAC地址	IPv6地址	租剩时间						
描述								

在这里可以查看到设备 LAN 口连接的主机的一些信息

系统日志

在此配置页面，用户可以查看系统记录，系统记录包含了 FPX9102H 的重要的配置信息。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
系统信息 内网主机信息 系统日志								
刷新 清除 保存								
<pre> Manufacturer:FLYINGVOICE ProductClass:FPX9102H SerialNumber:FLY69167000116 BuildTime:201709010452 IP:59.11.128.225:8080 HWVer:V3.1 SWVer:V3.20 <Sun Apr 8 14:30:33 2018> kernel: Wireless: Peer AUTH fail (Status = 1,Maybe MAC is filtered)... <Sun Apr 8 14:39:37 2018> provision[12932]: start to check config file <Sun Apr 8 14:39:37 2018> provision[12932]: HTTP get configuration file failed <Sun Apr 8 14:39:37 2018> provision[12932]: Update configuration fialed, retry 3600 s later <Sun Apr 8 14:44:29 2018> udhcpd[5634]: Sending renew... <Sun Apr 8 14:44:30 2018> udhcpd[5634]: Lease of 192.168.10.245 obtained, lease time 7200 <Sun Apr 8 15:25:27 2018> kernel: Wireless: Send DEAUTH frame to a4:08:ea:82:15:c9 <Sun Apr 8 15:39:37 2018> provision[12932]: start to check config file <Sun Apr 8 15:39:37 2018> provision[12932]: HTTP get configuration file failed <Sun Apr 8 15:39:37 2018> provision[12932]: Update configuration fialed, retry 3600 s later <Sun Apr 8 15:44:31 2018> udhcpd[5634]: Sending renew... <Sun Apr 8 15:44:31 2018> udhcpd[5634]: Lease of 192.168.10.245 obtained, lease time 7200 <Sun Apr 8 16:28:16 2018> kernel: Wireless: Rcv AUTH From a4:08:ea:82:15:c9 <Sun Apr 8 16:28:16 2018> kernel: Wireless: Send AUTH response (SUCCESS)... <Sun Apr 8 16:28:16 2018> kernel: Wireless: Rcv ASSOC From a4:08:ea:82:15:c9 <Sun Apr 8 16:28:16 2018> kernel: Wireless: Send ASSOC response To a4:08:ea:82:15:c9 <Sun Apr 8 16:28:16 2018> kernel: Wireless: a4:08:ea:82:15:c9 ->Encrypt-key exchanged <Sun Apr 8 16:28:16 2018> udhcpd[12398]: Sending OFFER of 59.11.128.252 <Sun Apr 8 16:28:16 2018> udhcpd[12398]: Sending ACK to 59.11.128.252 </pre>								
描述								

在此页面，用户可以通过点击相应的按钮来刷新、清除和保存相关系统信息

网络和安全

在这部分的 Web 管理界面里，您可以配置广域网端口，LAN 端口，DDNS，多 WAN，DMZ，MAC 克隆、端口等参数

WAN 口设置

此页面允许您设置不同模式的 WAN 配置。使用连接类型下拉列表选择一个 WAN 模式，然后显示相应的页面。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理		
WAN	LAN	IPv6高级设置	IPv6 WAN	IPv6 LAN	VPN	端口映射	DMZ	DDNS	QoS	Rate Limit
高级设置	L2TP									

INTERNET

WAN

连接名称	1_MANAGEMENT_VOICE_INTERNET_R_VID ▾	删除此连接
服务模式	MANAGEMENT_VOICE_INTERNET ▾	
IP协议版本	IPv4 ▾	
INTERNET接入方式	DHCP ▾	
DHCP Server	192.168.10.1	
MAC地址克隆	禁止 ▾	
NAT 使能	开启 ▾	
VLAN 模式	禁止 ▾	
VLAN ID	1 (1-4094)	
DNS模式	自动 ▾	
主DNS地址	8.8.8.8	
从DNS地址	192.168.10.1	
DHCP		
DHCP更新	更新	
DHCP 供应商(选项 60)	FLYINGVOICE-FPX9102H	
绑定端口	<input checked="" type="checkbox"/> 端口_1 <input checked="" type="checkbox"/> 端口_2 <input checked="" type="checkbox"/> 端口_3 <input checked="" type="checkbox"/> 端口_4 <input checked="" type="checkbox"/> 无线(SSID) <input checked="" type="checkbox"/> 无线(SSID1) <input checked="" type="checkbox"/> 无线(SSID2) <input checked="" type="checkbox"/> 无线(SSID3)	

注：WAN连接之间不能共享绑定端口，最后绑定端口的WAN连接绑定操作将冲掉之前其它WAN连接对该端口的绑定操作！

参数名称	描述
连接名称	用关键字标明 WAN 口的服务模式-在多 WAN 口设置页面设置相关参数
IP 协议模式	支持 IPv4
INTERNET 接入方式	DHCP、PPoE、静态 IP、桥接

DHCP Server	DHCP 服务器的职责是当工作站登录进来时分配 IP 地址, 并且确保分配给每个工作站的 IP 地址不同
MAC 地址克隆	选择开启或者禁止 MAC 地址克隆
NAT 使能	需要在多 WAN 口页面设置
VLAN 模式	选择 VLAN 模式, 开启/禁止/透传
VLAN ID	注意: 可以使用相同的 VLAN ID 创建多个 WAN 连接
DNS 模式	选择 DNS 模式, 选项为自动和指定: 1.当 DNS 模式为自动时, LAN 端口下的设备将自动获取首选 DNS 和备用 DNS 2.当 DNS 模式为“指定”时, 用户应手动配置首选 DNS 和备用 DNS
主 DNS 地址	因特网端口的首选 DNS
从 DNS 地址	因特网端口的备选 DNS
DHCP	当 WAN IP 模式设置为 DHCP 时显示
DHCP 更新	刷新 DHCP IP
DHCP 供应商 (选项 60)	指定 DHCP 供应商字段显示供应商和产品名称
绑定端口	可以与对应的端口 1~端口 4, SSID1~SSID4 绑定

WAN 口连接类型

本小节主要介绍在基本模式下的 WAN 口网络连接方式

(1) 静态 IP

当用户从互联网提供商接收到固定的公共 IP 地址或公共子网,即多个公共 IP 地址时,可以使用该配置。在大多数情况下,有线服务提供商将提供固定的公共 IP,而 DSL 服务提供商将提供公共子网。如果您有公共子网,可以为 WAN 接口分配一个 IP 地址。

INTERNET

WAN

连接名称	1_MANAGEMENT_VOICE_INTERNET_R_VID ▾	删除此连接
服务模式	MANAGEMENT_VOICE_INTERNET ▾	
IP协议版本	IPv4 ▾	
INTERNET接入方式	静态IP ▾	
MAC地址克隆	禁止 ▾	
NAT 使能	开启 ▾	
VLAN 模式	禁止 ▾	
VLAN ID	1 (1-4094)	
静态IP		
IP地址	192.168.10.223	
子网掩码	255.255.255.0	
默认网关	192.168.10.1	
DNS模式	指定 ▾	
主DNS地址	192.168.10.1	
从DNS地址	192.168.18.1	

参数名称	描述
Internet 接入方式	选择静态 IP。
LAN 连接模式	LAN 连接模式选择桥接和路由。
IP 地址	因特网端口的 IP 地址。
子网掩码	因特网端口的子网掩码
默认网关	因特网端口的默认网关
DNS 模式	DNS 类型为指定: 用户应手动设置首选 DNS 和备选 DNS。 DNS 类型为自动: IP 电话将从 DHCP 服务器将自动获得的首选 DNS 和备选 DNS。
主 DNS 地址	Internet 端口的首选 DNS 地址
从 DNS 地址	Internet 端口的备选 DNS。

(2) DHCP

路由器有一个内置的 DHCP 服务器，为每个本地客户端分配专用 IP 地址。

DHCP 功能允许 FTA1101 从 DHCP 服务器自动获取 IP 地址。在这种情况下，不需要手动为客户端分配 IP 地址。

INTERNET

WAN

连接名称	1_MANAGEMENT_VOICE_INTERNET_R_VID ▾	删除此连接
服务模式	MANAGEMENT_VOICE_INTERNET ▾	
IP协议版本	IPv4 ▾	
INTERNET接入方式	DHCP ▾	
DHCP Server	192.168.10.1	
MAC地址克隆	禁止 ▾	
NAT 使能	开启 ▾	
VLAN 模式	禁止 ▾	
VLAN ID	1 (1-4094)	
DNS模式	自动 ▾	
主DNS地址	8.8.8.8	
从DNS地址	192.168.10.1	
DHCP		
DHCP更新	更新	
DHCP 供应商(选项 60)	FLYINGVOICE-FPX9102H	

参数名称	描述
Internet 接入方式	选择自动配置 DHCP。
LAN 连接模式	LAN 连接模式选择桥接和路由。
DNS 模式	DNS 类型为指定：用户应手动设置首选 DNS 和备选 DNS。 DNS 类型为自动：IP 电话将从 DHCP 服务器将自动获得的首选 DNS 和备选 DNS。
主 DNS 地址	Internet 端口的首选 DNS 地址。
从 DNS 地址	Internet 端口的备选 DNS。

(3) PPPoE

PPPoE 代表以太网上的点到点协议。它依赖于两个广泛接受的标准：PPP 和以太网，它通过以太网将用户连接到具有普通宽带介质（例如单个 DSL 线路，无线设备或电缆调制解调器）的因特网。以太网上的所有用户都可以共享一个公共连接。

PPPoE 用于大多数 DSL 调制解调器用户，您的服务提供商将提供有关用户名，密码和身份验证模式的信息，所有本地用户都可以共享一个 PPPoE 连接来访问 Internet。

INTERNET

WAN

连接名称	1_MANAGEMENT_VOICE_INTERNET_R_VID ▾	删除此连接
服务模式	MANAGEMENT_VOICE_INTERNET ▾	
IP协议版本	IPv4 ▾	
INTERNET接入方式	PPPoE ▾	
MAC地址克隆	禁止 ▾	
NAT 使能	开启 ▾	
VLAN 模式	禁止 ▾	
VLAN ID	1 (1-4094)	
DNS模式	自动 ▾	
主DNS地址	<input type="text"/>	
从DNS地址	<input type="text"/>	
PPPoE 用户名 <input type="text"/> 密码 <input type="password" value="....."/> 确认密码 <input type="password" value="....."/> 服务名称 <input type="text"/> 空为自动检测		
运行模式	保持活跃 ▾	
重拨时间(0-3600秒)	5	

参数名称	描述
Internet 接入方式	选择 PPPoE。
MAC 地址克隆	是否允许 MAC 克隆
LAN 连接模式	LAN 连接模式选择桥接或路由。
DNS 模式	DNS 类型为指定：用户应手动设置首选 DNS 和备选 DNS。 DNS 类型为自动：IP 电话将从 DHCP 服务器将自动获得的首选 DNS 和备选 DNS。
主 DNS 地址	Internet 端口的首选 DNS 地址。
从 DNS 地址	Internet 端口的备选 DNS。
PPPoE 用户名	填写从 internet 服务提供商获得的 PPPoE 帐号。

密码	填写从 Internet 服务提供商获得 PPPoE 账户的密码。
确定密码	再次输入 PPPOE 账号的密码。
服务名称	填写服务名称，可不填。
运行模式	运行模式，有保持活跃、按需连接和手动设置三种。默认运行模式模式保持活跃。
重播时间	重新拨号的发送时间间隔。

(4) 桥接模式

在管理---工作模式中可设置工作模式，当工作模式为高级时，在网络部分可设置多 WAN 方式。多 WAN 下的桥接模式与传统的桥接设置不同，桥接模式不使用 IP 地址，设备作为 WAN 端口和 LAN 端口之间的桥梁。必须建立路由连接，为设备上的本地服务提供 IP 地址。

INTERNET

WAN

连接名称	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼	删除此连接
服务模式	MANAGEMENT_VOICE_INTERNET ▼	
IP协议版本	IPv4 ▼	
INTERNET接入方式	桥接 ▼	
桥接类型	IP桥接 ▼	
DHCP 服务类型	透传 ▼	
VLAN 模式	禁止 ▼	
VLAN ID	1 (1-4094)	

参数名称	描述
桥接类型	
IP 桥接	允许所有以太网数据包通过， PC 可以直接连接上网
PPPoE 桥接	只允许 PPPoE 包通过， PC 需要 PPPoE 拨号软件
硬件 IP 桥接	数据包通过有线速度的硬件开关，不支持无线端口绑定
DHCP 服务类型	
透传	在 DHCP 服务器和需要获取 IP 的设备不在同一网段的时候，直接连接到客户端设备所在子网的三层设备设置为 DHCP relay，以便将客户端的 DHCP 请求转发至 DHCP 服务
Snooping	DHCP 监听（DHCP Snooping）是一种 DHCP 安全特性。设备支持在每个 VLAN 基础上启用 DHCP 监听特性。通过这种特性，交换机能够拦截第二层 VLAN 域内的所有
本机服务	网关不会在局域网和广域网之间转发 DHCP 报文，还会阻断 WAN 端口的 DHCP 报文。连接到 LAN 端口的客户端可以从在网关中运行的 DHCP 服务器获取 IP
VLAN 模式	
禁止	WAN 接口未标记，LAN 未标记

开启	WAN 接口被标记, LAN 未标记
透传	仅在桥模式下有效, 所有端口 (包括 WAN 和 LAN) 属于此 VLAN ID, 所有端口都标记有该 VLAN ID, 标记的数据包可以通过 WAN 和 LAN
VLAN ID	建立 VLAN ID
绑定端口	可以与对应的端口 1~端口 4, SSID1~SSID4 绑定

**注意**

可以使用相同的 VLAN ID 创建多个 WAN 连接

LAN 口设置

NAT 将数据包从公共 IP 地址转换为本地 IP 地址, 将报文转发到适当的目的地。



LAN口设置

LAN口设置

本地IP地址	<input type="text" value="59.11.128.225"/>
子网掩码	<input type="text" value="255.255.255.224"/>
DHCP服务器	<input type="text" value="开启"/>
地址池开始地址	<input type="text" value="59.11.128.226"/>
地址池结束地址	<input type="text" value="59.11.128.254"/>
DNS模式	<input type="text" value="自动"/>
主DNS	<input type="text" value="192.168.10.1"/>
从DNS	<input type="text" value="192.168.18.1"/>
客户端租约时间(0-86400秒)	<input type="text" value="86400"/>
TFTP服务器地址	<input type="text"/>
启动配置文件	<input type="text"/>
<input type="button" value="DHCP客户列表"/>	

DHCP 静态分配

编号	MAC地址	IP地址
<input type="button" value="删除已选择项"/>	<input type="button" value="添加"/>	<input type="button" value="编辑"/>

参数名称	描述
IP 地址	输入本路由器对局域网的 IP 地址, 局域网中所有计算机的 IP 地址必须与此 IP 地址处于同一网段, 且默认网关必须为此 IP 地址。(默认为 192.168.1.1)
子网掩码	输入子网掩码以确定网络的规模 (默认为 255.255.255.0/24)
DHCP 服务器	是否启用 DHCP 服务器

地址池开始地址	为 IP 地址池输入一个有效的 IP 地址作为 DHCP 服务器向 DHCP 客户端发出的起始 IP 地址，如果路由器 LAN 口 IP 地址是 192.168.168.1，起始 IP 地址可以是 192.168.168.2 或更大，但是小于结束 IP 地址
地址池结束地址	为 IP 地址池输入一个有效的 IP 地址作为 DHCP 服务器向 DHCP 客户端发出的结束 IP 地址
DNS 模式	从自动和指定两种模式中选择 DNS 类型 DNS 类型为自动时，LAN 口下设备将从家庭网关的 DHCP 服务器自动获得首选 DNS 和备选 DNS DNS 类型为指定时，用户应手动配置首选 DNS 和备选 DNS
主 DNS	设备首选 DNS
从 DNS	设备备选 DNS
客户端租约时间	DHCP 服务器给内网计算机分配的 IP 地址的有效使用时间。在该段时间内，服务器不会将该 IP 地址分配给其他计算机。
DNS 代理	选择开启或者禁止；如果开启，转发 LAN 侧网络的 DNS 请求到 WAN 侧网

IPv6 设置

您可以在这里设置 IPv6 的相关信息，开启或禁止 IPv6。

启用 IPv6 功能：

- 1.进入网络> IPv6 高级页面。
- 2.从“IPv6 启用”下拉列表中选择“启用”。
- 3.单击保存并应用。

The screenshot shows a web interface for IPv6 configuration. At the top, there is a navigation bar with tabs: 状态, 网络, IPPBX, 无线2.4GHz, 无线5GHz, 安全, 应用, 存储, 管理. Below this is a sub-menu bar with tabs: WAN, LAN, IPv6高级设置 (selected), IPv6 WAN, IPv6 LAN, VPN, 端口映射, DMZ, DDNS, QoS, Rate Limit. Underneath, there are sub-tabs: 高级设置 and L2TP. The main content area is titled 'IPv6高级设置'. Below the title, there is a section 'IPv6使能' with a dropdown menu currently set to '开启'. At the bottom of the page, there are four buttons: 保存并应用, 保存, 取消, 重启.

IPv6 WAN

如图所示为 IPv6 WAN 相关信息：

参数名称	描述
连接类型	在下拉列表中选择连接类型，包括 DHCPv6/静态 IPv6/PPoE
DHCPv6 获取地址方式	选择获取 IPv6 地址方式的方式，有状态/无状态
前缀分发	开启前缀分发

IPv6 LAN

启用 IPv6 时，G802/G902 的 LAN 客户端可以配置为从本地配置的 IPv6 地址池或外部 DHCPv6 服务器接收 IPv6 地址。连接到 G802/G902 的有线和无线客户端可以根据 LAN 端口配置 DHCPv6 参数的方式获取 IPv6 地址，飞音的由器可以配置为 DHCPv6 服务器，LAN 客户端从配置的地址池中获取 IPv6 地址。启用 LAN DHCPv6 服务，如图所示为 IPv6 LAN 相关信息：

WAN	LAN	IPv6高级设置	IPv6 WAN	IPv6 LAN	VPN	端口映射	DMZ	Vlan	QoS	Rate Limit
高级设置										
IPv6 LAN设置										
IPv6 LAN设置										
IPv6地址	<input type="text" value="fec0::1"/>									
IPv6前缀长度	<input type="text" value="64"/> (0-128)									
DHCPv6服务										
DHCPv6状态	<input type="text" value="禁止"/>									
DHCPv6模式	<input type="text" value="无状态"/>									
域名	<input type="text"/>									
Server首选	<input type="text" value="255"/> (0-255)									
主DNS服务器地址	<input type="text"/>									
次DNS服务器地址	<input type="text"/>									
租约时间	<input type="text" value="86400"/> (0-86400秒)									
IPv6地址池	<input type="text"/> - <input type="text"/> / <input type="text"/>									
路由器通告										
路由器通告	<input type="text" value="禁止"/>									
通告间隔	<input type="text" value="30"/> (10-1800秒)									
RA管理标志	<input type="text" value="禁止"/>									
RA其它标志	<input type="text" value="开启"/>									
前缀	<input type="text"/> / <input type="text"/>									
前缀有效时间	<input type="text" value="3600"/> (0-3600秒)									

参数名称	描述
IPv6 地址	IPv6 地址
IPv6 前缀长度	IPv6 前缀为 0—128 可选，默认为 64
DHCPv6 状态	开启 DHCPv6 状态
DHCPv6 模式	选择 DHCPv6 的模式，有状态/无状态

域名	填入 IPv6 的域名
Server 首选	选择 Server 首选
主 DNS 服务器地址	填入主 DNS 服务器地址
次 DNS 服务器地址	填入次 DNS 服务器地址
租约时间	IPv6 租约时间
IPv6 地址池	填入 IPv6 地址池
路由器通告	开启路由器通告
通告间隔	填入通告间隔
RA 管理标志	开启或禁止 RA 管理标志
RA 其他标志	开启或禁止 RA 其他标志
前缀	填入前缀

VPN 设置

VPN 是在公用网络上建立专用网络的技术。VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，用户数据在逻辑链路中传输。通过 VPN 技术,用户可以在公共网络上的任意两个设备之间建立私有的连接并传输数据,FPX9102H 支持 PPTP、L2TP 和 Open VPN。

PPTP



VPN设置

管理

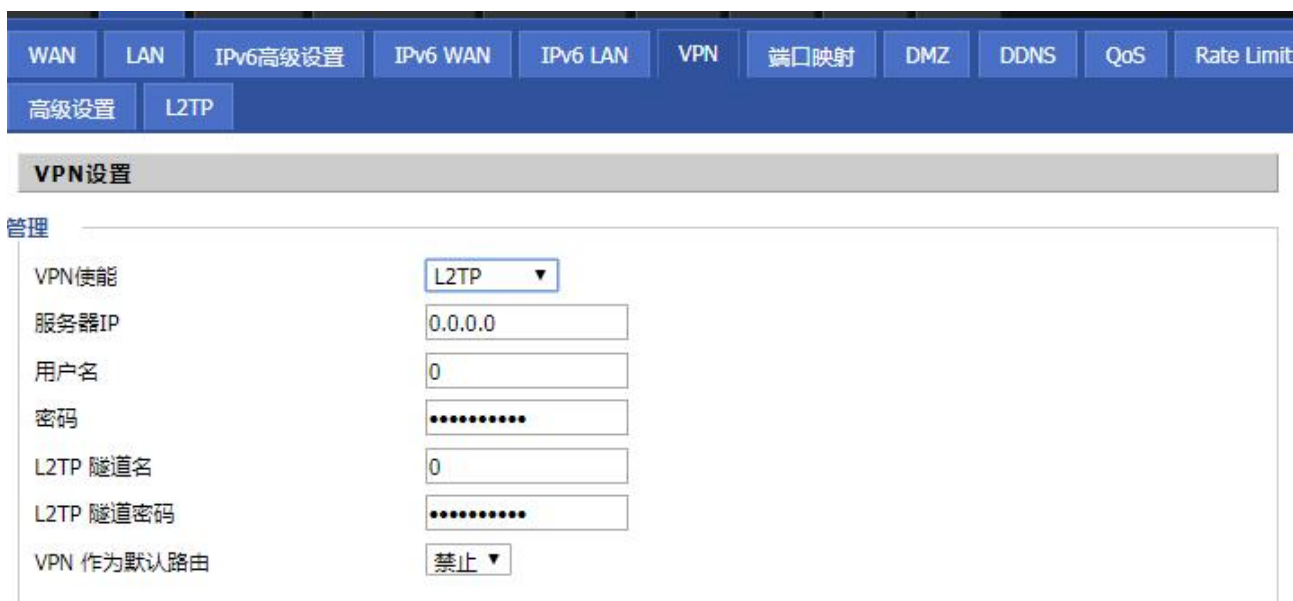
VPN使能	PPTP ▼
服务器IP	0.0.0.0
用户名	0
密码
VPN 作为默认路由	禁止 ▼
有状态MPPE	禁止 ▼
请求MPPE	禁止 ▼

参数名称

描述

VPN 使能	是否使能 VPN。 选择 PPTP 模式。
服务器 IP	VPN 服务器的 IP 地址。
用户名	认证需要的用户名。
密码	认证需要的密码。
VPN 作为默认路由	禁止或开启，默认为禁止。

L2TP



参数名称	描述
VPN 使能	是否使能 VPN。 选择 L2TP 模式。
服务器 IP	VPN 服务器的 IP 地址。
用户名	认证需要的用户名。
密码	认证需要的密码。
L2TP 隧道名	L2TP 隧道的名称
L2TP 隧道密码	L2TP 隧道的密码
VPN 作为默认路由	禁止或开启，默认为禁止。

OpenVPN:



VPN设置

管理

VPN使能	OpenVPN ▼
OpenVPN TLS 认证	禁止 ▼
VPN 作为默认路由	禁止 ▼

参数名称	描述
VPN 使能	是否使能 VPN。 选择 OpenVPN 模式。
OpenVPN TLS 认证	是否开启 OpenVPN TLS 认证
VPN 作为默认路由	禁止或开启，默认为禁止。

端口映射

如图所示是端口映射的相关信息：

状态 **网络** IPPBX 无线2.4GHz 无线5GHz 安全 应用 存储 管理
WAN LAN IPv6高级设置 IPv6 WAN IPv6 LAN VPN 端口映射 DMZ DDNS QoS Rate Limit 端口管理 路由
高级设置 L2TP

端口映射				
编号	注解	IP地址	端口范围	协议

端口映射

注解

IP地址

端口范围 -

协议

(最大规则数为 32)

虚拟服务器					
编号	注解	IP地址	公共端口	私有端口	协议

虚拟服务器

注解

IP地址

公共端口

私有端口

协议

(最大规则数为 32)

参数名称	描述
注解	设置一条端口映射规则的名称或注释
IP 地址	LAN 口下设备的 IP 地址
端口范围	给 LAN 口下设备设置端口范围(1-65535)
协议	可以选择 TCP、UDP、TCP&UDP 三种情况
应用/取消	参数设置完成，点击应用，在 NO.下生成编号；点击取消数据删除
注解	对设置的虚拟服务器的注释
IP 地址	虚拟服务器的 IP 地址
公共端口	虚拟服务器的公共端口
私有端口	虚拟服务器的私有端口
协议	可以选择 TCP、UDP、TCP&UDP 三种情况
应用/取消	参数设置完成，点击应用，在 NO.下生成编号；点击取消数据删除

DMZ

DMZ(Demilitarized zone)是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡，局域网中设置 DMZ 主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。向 DMZ 添加客户机可能会给本地网络带来不安全因素，因此不要轻易使用这一项。



参数名称	描述
DMZ 使能	开启或者禁止 DMZ 设置
DMZ 主机 IP 地址	输入需要的 DMZ 主机 IP 地址

QoS

如图是 QoS 相关信息配置:

状态
网络
IPPBX
无线2.4GHz
无线5GHz
安全
应用
存储
管理

WAN
LAN
IPv6高级设置
IPv6 WAN
IPv6 LAN
VPN
端口映射
DMZ
DDNS
QoS
Rate Limit
端口管理
路由配置

高级设置
L2TP

QoS 配置

QoS 配置

启用QoS 禁止 ▾

上行带宽 0 (0-102400)kbit/s

下行带宽 0 (0-102400)kbit/s

算法 WFQ ▾

注解	条件								动作						
	源IP地址	目的IP地址	协议	源端口范围	目的端口范围	物理接口	DSCP	802.1p	VLAN ID	Remark DSCP	Remark 802.1p	Remark VLAN_ID	优先级	丢弃	速率限制
<input type="button" value="删除已选项"/> <input type="button" value="添加"/>															

参数名称	描述
启用 QoS	禁止/启用 QOS 功能
上行带宽	设置上行带宽
下行带宽	设置下行带宽
删除已选项	在 NO 下，勾选想要删除的项，点击删除已选项
添加	点击添加，添加新的参数

端口限速

状态
网络
IPPBX
无线2.4GHz
无线5GHz
安全
应用
存储
管理

WAN
LAN
IPv6高级设置
IPv6 WAN
IPv6 LAN
VPN
端口映射
DMZ
DDNS
QoS
Rate Limit

高级设置
L2TP

端口限速设置

Rate Limit Enable

Rate Limit Enable 开启 ▾

端口	入口速率	出口速率
WAN	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN1	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN2	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN3	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN4	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s

端口	ARP, 广播风暴抑制速率
WAN	<input type="text" value="255"/> (0-255)*64 packets/s
LAN1	<input type="text" value="255"/> (0-255)*64 packets/s
LAN2	<input type="text" value="255"/> (0-255)*64 packets/s
LAN3	<input type="text" value="255"/> (0-255)*64 packets/s
LAN4	<input type="text" value="255"/> (0-255)*64 packets/s

描述

设置 WAN 口和 LAN 口的端口速率，选择开启或者禁止

端口管理

如图是端口相关信息配置:

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理		
WAN	LAN	IPv6高级设置	IPv6 WAN	IPv6 LAN	VPN	端口映射	DMZ	DDNS	QoS	Rate Limit
高级设置	L2TP									

端口管理

端口管理

WAN 速率设置	自动侦测 ▼
LAN1 速率设置	自动侦测 ▼
LAN2 速率设置	自动侦测 ▼
LAN3 速率设置	自动侦测 ▼
LAN4 速率设置	自动侦测 ▼

参数名称	描述
WAN 口速率设置	从自动协商，100M 全双工，100M 半双工，10M 全双工和 10M 半双工中选择端口所支持的速度协商方法
LAN1-LAN3 速率设置	从自动协商，100M 全双工，100M 半双工，10M 全双工和 10M 半双工中选择端口所支持的速度协商方法

路由配置

如图是路由相关信息配置:

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理		
WAN	LAN	IPv6高级设置	IPv6 WAN	IPv6 LAN	VPN	端口映射	DMZ	DDNS	QoS	Rate Limit
高级设置	L2TP									

静态策略路由配置

添加一条路由规则

目的地址	<input type="text"/>
主机/掩码	主机 ▼
网关	<input type="text"/>
网络接口	LAN ▼
注解	<input type="text"/>

参数名称	描述
目的地址	路由目的地址
主机/掩码	在下拉列表中选择主机/掩码
网关	网关 IP 地址

网络接口 在下拉列表中选择 LAN/VOICE/INTERNET/TR069/VPN

注解 注解

高级设置

如图是高级设置相关信息配置:



Nat最大连接数(512-8192)	4096
Mss模式	<input type="radio"/> 指定 <input checked="" type="radio"/> 自动
Mss值(1260-1460)	1260
防Dos攻击	<input checked="" type="radio"/> 开启 <input type="radio"/> 禁止
IP地址冲突检测	<input checked="" type="radio"/> 开启 <input type="radio"/> 禁止
IP地址冲突检测间隔(0-3600s)	600

参数名称	描述
Nat 最大连接数	Nat 最大连接数为 4096
Mss 模式	有 Manual 和 Auto 两种选择
Mss 值	设置 TCP 的值
防 Dos 攻击	可以选择使能或者禁止
IP 地址冲突检测	选择使能或者禁止；如果使能，发生 IP 冲突话机会有提示
IP 地址冲突检测间隔	检测 IP 地址冲突的时间间隔

IPPBX

点击进入 IPPBX 的配置页面，IPPBX 配置文件的上传和下载，IPPBX 的 IVR 上传和下载，IVR 支持的音频为 GSM 格式

基本设置

如图是无线的基本设置相关信息配置：

状态 网络 **IPPBX** 无线2.4GHz 无线5GHz 安全 应用 存储 管理

基本设置 用户

PBX配置界面

Asterisk-gui

使用 Asterisk-gui配置PBX

[点击此处去配置PBX](#)

Asterisk Config File

配置文件上传与下载

本地文件

[选择文件](#)

未选择任何文件

[上传](#)

[下载](#)

Welcome IVR 文件

Welcome IVR 上传与下载

文件

IVR1 ▾

本地文件

[选择文件](#)

未选择任何文件

(仅支持上传 *.wav)

[上传](#)

[下载](#)

允许接入IP列表

允许接入IP设置

编号	IP地址	编号	IP地址
1 <input type="checkbox"/>	host = dynamic	2 <input type="checkbox"/>	sip_trunk_server_2
3 <input type="checkbox"/>	sip_trunk_server_3	4 <input type="checkbox"/>	sip_trunk_server_2
5 <input type="checkbox"/>	sip_trunk_server_1		

[删除已选择项](#)

[添加](#)

添加允许接入的IP、网段或者域名

允许接入的IP/网段/域名

[应用](#)

[取消](#)

参数名称	描述
PBX 配置界面	
使用 Asterisk-gui 配置 PBX	点击  此按钮，会进入 PBX 配置界面
Asterisk Cofig File	
配置文件上传和下载	在此上传或者下载配置文件
Welcome IVR 文件	
文件	在 IVR1~IVR5 里面选择一个文件，然后点击本地文件去上传或者下载 IVR，注意，仅支持上传*.wav 格式
允许接入 IP 列表	
添加允许接入的 IP、网段或者此项不可选 域名	
允许接入的 IP/网段/域名	填写客户端允许介入的 IP/网段/域名等

无线 2.4G 设置

基本设置

如图是无线的基本设置相关信息配置:

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置		

基本无线设置	
无线网络	
WIFI开关	开启 ▾
连接模式	无线接入点 ▾
网络模式	仅11n(2.4G) ▾
无线网络名称	flytest_2.4g 开启 <input checked="" type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 <input type="checkbox"/> 最大客户端数 32
无线网络名称1	开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 <input type="checkbox"/> 最大客户端数 16
无线网络名称2	开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 <input type="checkbox"/> 最大客户端数 16
无线网络名称3	开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 <input type="checkbox"/> 最大客户端数 0
广播网络名(SSID)	<input type="radio"/> 开启 <input type="radio"/> 禁止
AP隔离	<input type="radio"/> 开启 <input checked="" type="radio"/> 禁止
虚拟网络间隔离	<input type="radio"/> 开启 <input checked="" type="radio"/> 禁止
BSSID	00:21:F2:0D:6C:D0
频率(频道)	2477MHz (Channel 14) ▾
高吞吐量物理模式	
工作模式	<input checked="" type="radio"/> 混合模式 <input type="radio"/> 节电模式
频道带宽	<input checked="" type="radio"/> 20 <input type="radio"/> 20/40
保护间隔	<input type="radio"/> 长 <input checked="" type="radio"/> 短
反转方向权限(RDG)	<input type="radio"/> 禁止 <input checked="" type="radio"/> 开启
STBC	<input type="radio"/> 禁止 <input checked="" type="radio"/> 开启
聚合MAC业务数据单元(A-MSDU)	<input checked="" type="radio"/> 禁止 <input type="radio"/> 开启
自动单一区块确认	<input type="radio"/> 禁止 <input checked="" type="radio"/> 开启
拒绝单一区块确认要求	<input checked="" type="radio"/> 禁止 <input type="radio"/> 开启
HT Disallow TKIP	<input type="radio"/> 禁止 <input checked="" type="radio"/> 开启
20/40 Coexistence	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

参数名称	描述
WIFI 开关	选择开启或关闭来启用或禁用无线连接
网络模式	根据无线客户端类型选择其中一种模式。默认为 11b/g/n 混合模式
SSID	它是无线局域网的基本标识。SSID 可以是任何文字数字或各种特殊字符的组合。它将显示在无线网卡搜索到的无线网络列表中
多 SSID1~SSID3	可以实现一个 AP 拥有多个 SSID
隐藏	勾选上该项后, 相应的 SSID 不再显示在无线网卡搜索到的无线网络列表中
广播网络名称(SSID)	初始状态开启, 用于将路由器的 SSID 向无线网络内广播

AP 隔离	本 AP 内隔离，启用后本 AP 内的客户端不能互相访问
MBSSID AP 隔离	本 AP 外隔离，不属于本 AP 的其他客户不能访问本 AP 下的客户端
BSSID	一组无线工作站和一个无线局域网接入点(AP)组成一个基本访问装置(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
频率(频道)	可以在 AutoSelect/1/2/3/4/5/6/7/8/9/10/11/12/13 中选择
工作模式 0	1. Mixed Mode: 在这一模式下，以前的无线网卡可以识别并连接到 Pre-N AP，但吞吐量会受到一定影响 2. Green Field: 能够达到高吞吐量，但是会影响向后兼容，以及系统的安全性
频道带宽	请选择为默认设置，分为 20MHz 和 20/40MHz 两种
保护间隔	默认为自动，为了达到优良的误码率性能，必须设定合适的保护间隔
反转方向权限(RDG)	可以选择启用或者禁止此权限
STBC	可以选择启用或者禁止此权限
聚合 MAC 业务数据单元	把多个 Ethernet 报文通过一定的方式聚合成一个较大的载荷
自动单一区确认	启用：使用单个块确认多个帧。 禁止：设备不使用自动闭塞确认——当移动设备遇到低吞吐量/连接问题时，使用此配置
拒绝自动单一区确认要求	启用：禁止来自设备的块确认请求 禁用：允许来自设备的块确认请求
HT Disallow TKIP	启用：不允许对连接的设备使用时间密钥完整性协议 禁用：允许对连接的设备使用时间密钥完整性协议
HT LDPC	启用：启用低密度奇偶校验机制，以提高在具有挑战性的无线环境中成功交付的机会 禁用：禁用低密度奇偶校验机制

无线安全

如图是无线安全相关信息配置：

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置		

SSID

选择SSID

SSID选择 flytest_2.4g ▼

"flytest_2.4g"

安全模式 WPA2PSK ▼

WPA

WPA算法 TKIP AES TKIPAES

通行口令 *****

私钥更新间隔 3600 秒 (0 ~ 86400)

访问策略

策略 白名单 ▼

新增 : (最大规则数为 64)

参数名称	描述
SSID 选择	从 SSID、多 SSID1、多 SSID2 和多 SSID3 中选择一个 SSID
安全模式	选择一种合适的加密模式以提高无线数据包的安全和隐私功能

用户可以配置相应的参数。 以下是一些常见的加密方法：

(1) WPA-PSK，路由器将采用基于共享密钥的 WPA 模式：

基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置

SSID

选择SSID

SSID选择 flytest_2.4g ▼

"flytest_2.4g"

安全模式 WPA-PSK ▼

WPA

WPA算法 TKIP AES TKIPAES

通行口令 *****

私钥更新间隔 3600 秒 (0 ~ 86400)

访问策略

策略 白名单 ▼

新增 : (最大规则数为 64)

参数名称	描述
WPA 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 TKIP、AES 两种
通行口令	设置 WPA-PSK 安全密码
私钥更新间距	设置密钥定时更新周期，默认为 3600s

(2) WPA2-PSK，路由器将采用基于共享密钥的 WPA2 模式：

The screenshot shows the configuration interface for wireless security. The 'Wireless Security' tab is active. Under the 'SSID' section, 'flytest_2.4g' is selected. The 'Security Mode' is set to 'WPA2-PSK'. Under the 'WPA' section, 'AES' is selected as the algorithm, and the key update interval is set to 3600 seconds. The 'Access Policy' section shows 'Whitelist' as the strategy.

参数名称	描述
WPA 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 TKIP、AES、TKIP/AES11N 模式不支持 TKIP 算法
通行口令	设置 WPA-PSK/WPA2-PSK 安全密码
私钥更新间距	置密钥定时更新周期，默认为 3600s

(3) WPAPSKWPA2PSK 方式与 WPA2-PSK 设置一致：WPA-PSK/WPA2-PSK 安全类型其实是 WPA/WPA2 的一种简化版本，它是基于共享密钥的 WPA 模式，安全性较高，设置也比较简单，适合普通家庭用户和小型企业使用。

基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置
SSID						
选择SSID						
SSID选择	flytest_2.4g ▼					
"flytest_2.4g"						
安全模式	WPAPSKWPA2PSK ▼					
WPA						
WPA算法	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES					
通行口令	*****					
私钥更新间隔	3600	秒	(0 ~ 86400)			

参数名称	描述
WPA 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 TKIP、AES、TKIP/AES。11N 模式不支持 TKIP 算法
通行口令	设置 WPAPSKWPA2PSK 安全密码
私钥更新间隔	置密钥定时更新周期，默认为 3600s

(5) 无线访问策略:

访问策略	
策略	禁止 ▼
新增 :	<input type="text"/> (最大规则数为 64)
<input type="button" value="保存并应用"/> <input type="button" value="保存"/> <input type="button" value="取消"/> <input type="button" value="重启"/>	

参数名称	描述
访问策略	无线访问控制功能是以 MAC 地址为条件允许或禁止指定的客户端接入到无线网络
策略	禁止：表示不使能无线访问控制策略；允许：表示仅允许列表中客户端接入，拒绝：表示仅禁止列表中客户端接入
新增	输入您要允许或禁止无线客户端的 MAC 地址
例子：	禁止无线网卡 MAC 地址为 00:1F:D0:62:BA:FF 的计算机访问无线网络，而其他计算机可以访问此网络
实现方法：	如图所示，选择策略为拒绝，在新增处填入 00:1F:D0:62:BA:FF，设置完成后，点击保存并重启设备以使设置生效

Wi-Fi 多媒体(WMM)

WMM(Wi-Fi 多媒体)全面定义了四种连接内容，其中包括语音、视频、best effort 以及 background，以此优化网络通信的质量，以保障这些应用与网络资源建立稳定连接。同时，WMM 优化了 Wi-Fi 原始终端用户的通信体验，在一个更为广泛、更为庞杂的网络环境和通信环境中，提供高质量的数据、语音、音乐、视频应用的网络连接性能。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置		

WMM参数						
	仲裁帧间隙数	最小竞争窗口	最大竞争窗口	传输机会	强制接入控制	响应规则
尽力而为流	3	15 ▼	63 ▼	0	<input type="checkbox"/>	<input type="checkbox"/>
背景流	7	15 ▼	1023 ▼	0	<input type="checkbox"/>	<input type="checkbox"/>
视频流	1	7 ▼	15 ▼	94	<input type="checkbox"/>	<input type="checkbox"/>
语音流	1	3 ▼	7 ▼	47	<input type="checkbox"/>	<input type="checkbox"/>

描述

WMM(Wi-Fi MultiMedia)是 Wi-Fi Alliance(WFA)的 QoS 证书。提供了对无线多媒体参数的设置，WMM 允许无线通信根据数据类型定义一个优先级范围。为了使 WMM 功能工作，无线客户端必须也支持

无线分布式部署(WDS)

FPX9102H 有四种选择模式，禁止/懒人模式/桥接模式/中继模式，您可以根据自己的需要选择对应的模式。

WDS 设置

WDS模式

- 禁止
- 懒人模式
- 桥接模式
- 中继模式

保存并应用 保存 启动

描述

WDS 代表无线分配系统，使 WDS 接入点互连，扩展无线网络

Wi-Fi 保护设置(WPS)

WPS 是由 Wi-Fi 联盟所推出的全新 Wi-Fi 安全防护设定(Wi-Fi Protected Setup)标准，该标准推出的主要原因是为了解决长久以来无线网路加密认证的步骤过于繁杂艰难之弊病。通过无线路由器上的 WPS 键可以让我们轻松快速的加密无线网路传输数据，阻止非法用户的入侵。一方面既保证了无线网络的安全，另一方面又让我们设置加密轻轻松松。

WPS设置

WPS 开启

应用

WPS概要

WPS当前状态	空闲
WPS设置	Yes
WPS服务集合标识符	flytest_2.4g

Wi-Fi保护设置的进度

WPS模式 PIN PBC

应用

WPS状态

WSC:Idle

参数名称	描述
------	----

WPS 设置	开启和关闭 WPS 功能
WPS 概要	显示当前 WPS 的情况，包括当前状态、SSID 名称、认证方式、加密类型，以及本 AP 的 PIN 码
Generate	生成新的 PIN 码
Reset OOB	系统采用默认的安全策略让其他的非 WPS 用户接入使用
WPS 模式	<p>PIN: 在下面的 PIN 选项中，填入需要接入的客户端(无线网卡等)的 PIN 码，然后点击应用。WPS 开始发送信号，此时，在客户端上也开启 PIN 接入方式，则客户端可以自动连接无线 AP</p> <p>PBC: PBC 模式有两种方法启动，可以在硬件上直接按下 PBC 按钮，或者从软件上选择到 PBC 模式，然后点击应用。两种方式都可以激活 PBC 模式的 WPS 连接，此时只需要在客户端选择到 PBC 接入方式，则客户端可以自动连接到无线 AP</p>
WPS 状态	<p>当前的 WPS 状态有三种：WSC:</p> <p>Idle 状态为空闲</p> <p>WSC: Start WSC Process 状态为开始发送信息</p> <p>WSC: Success 状态为已经有客户接入 AP，WPS 连接成功</p>

无线客户端(Station Info)

状态
网络
IPPBX
无线2.4GHz
无线5GHz
安全
应用
存储
管理

基本设置
无线安全
Wi-Fi多媒体
无线分布式部署
Wi-Fi保护设置
无线客户端
高级设置

无线状态

无线状态

当前频道	频道 14
flytest_2.4g	00:21:F2:0D:6C:D0

无线网络

无线网络

MAC地址	序号	省电管理	MimoPS	速率参数	带宽	短保护间隔	空时编码
-------	----	------	--------	------	----	-------	------

描述

此页面显示有关当前注册的客户端连接的信息，包括操作 MAC 地址和操作统计信息

高级设置

基本设置	无线安全	Wi-Fi多媒体	无线分布式部署	Wi-Fi保护设置	无线客户端	高级设置
高级无线						
高级无线						
BG保护模式			自动侦测 ▾			
信标间隔	100	毫秒(范围20-999, 默认100)				
数据信标比例 (传输量指示讯息)	3	(范围1-255, 默认3)				
分割界限	2346	(范围256-2346, 默认2346)				
传输请求界限	2347	(范围1-2347, 默认2347)				
发射功率	100	% (范围1-100, 默认100)				
短前导码	<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
短碰撞槽	<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
传输突发	<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
数据包聚合	<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
国家代码	NONE ▾					
支持的频道	Ch1~14 ▾					
Tx Beamforming	Disable ▾					
Wi-Fi多媒体 (WMM)						
Wi-Fi多媒体能力	<input checked="" type="checkbox"/>					
无线网络名称	<input checked="" type="checkbox"/>					
无线网络名称1	<input type="checkbox"/>					
无线网络名称2	<input type="checkbox"/>					
无线网络名称3	<input type="checkbox"/>					
自动省电模式能力	<input type="radio"/> 开启		<input checked="" type="radio"/> 禁止			
多播到单播转换器	<input type="radio"/> 开启		<input checked="" type="radio"/> 禁止			
多播到单播	<input type="radio"/> 开启		<input checked="" type="radio"/> 禁止			

参数名称	描述
BG 保护模式	选择开、关或者自动，来确定 BG 保护模式的状态
信标间隔	发送无线信标帧的间隔时间，在此时间范围内，会发送一次信标帧获取周围无线网络接入信息
数据信标比	指定传输指示消息的间隔，是一种倒计时作业，用以告知下一个要接收广播和多播的客户端窗口
分割界限	为数据包指定分片阈值，当数据包的长度超过分片阈值时，会被自动自动分成多个数据包
传输请求界限	为数据包指定 RTS 阈值，当数据包超过此值时，路由器会发送 RTS 到目的站点协商
发射功率	定义当前的无线 AP 对于 SSID 的发射功率大小，越大信号越强
短前导码	默认开启，系统不兼容传统 IEEE802.11，系统操作速率 1、2Mbps
短碰撞槽	默认开启，开启可以提高无线通信的传输速率
传输突发	属于 MAC 地址层的特性，能提高网络 TCP 传输公平性

数据包聚合	增强局域网确保数据包正确到达目的地的机制
支持 IEEE802.11H	默认禁止，可以开启
国家代码	有 CN、US、JP、FR、TW、IE、HK、NONE 可选
Wi-Fi 多媒体(WMM)	
Wi-Fi 多媒体能力	开启 WMM 功能，开启后才生效
自动省电模式	开启后会降低无线性能，但是能够起到节能省电的作用
WMM Parameters	点击 WMM Configuration 可以直接跳出 Wi-Fi 多媒体参数配置页面
多播到单播转换	默认禁止，可以选择开启

无线 5G 设置

请参考[无线 2.4G 设置](#)。

安全

在该页面可以进行过滤设置、内容过滤

MAC/IP/Port/ACL

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理	
MAC/IP/PORT ACL									
内容过滤									
基本设置									
<p>基本设置</p> <p>使能过滤 <input type="button" value="禁止"/> ▾</p> <p>默认策略 <input type="button" value="白名单"/> ▾</p> <p>不匹配任何规则的数据包将被 丢弃</p> <p><input type="button" value="保存"/> <input type="button" value="取消"/></p>									
MAC/IP/Port 过滤设置									
<p>网络接口 <input type="button" value="LAN"/> ▾</p> <p>Mac 地址 <input type="text"/></p> <p>目的 IP 地址 <input type="text"/></p> <p>源 IP 地址 <input type="text"/></p> <p>协议 <input type="button" value="无"/> ▾</p> <p>目的 Port 区间 <input type="text"/> - <input type="text"/></p> <p>源 Port 区间 <input type="text"/> - <input type="text"/></p> <p>行为 <input type="button" value="接收"/> ▾</p> <p>注解 <input type="text"/></p> <p>(最大规则数为 32)</p> <p><input type="button" value="保存"/> <input type="button" value="取消"/></p>									
MAC/IP/Port 过滤列表									
编号	网络接口	Mac 地址	目的 IP 地址	源 IP 地址	协议	目的 Port 区间	源 Port 区间	行为	注解
<p>WAN: 其他的会被丢弃.</p> <p>LAN: 其他的会被丢弃.</p> <p><input type="button" value="删除"/> <input type="button" value="取消"/></p>									

参数名称	描述
使能过滤	开启/禁止过滤功能
默认策略	默认策略是接受或禁止过滤规则
不匹配的数据包	列出已经存在的 URL 过滤规则（黑名单）
保存/取消	您可以选择删除或取消现有的过滤规则
默认策略	可选择放弃或者接受
Mac 地址	添加需要过滤的 Mac 地址
目的 IP 地址	目的 IP 地址
源 IP 地址	源 IP 地址
协议	选择协议名称，支持 TCP、UDP 和 TCP&UDP
目的 Port 区间	目的端口的范围
源 Port 区间	源端口的范围
行为	可以选择接收或者放弃

注释	对添加内容的标注
删除	删除选中项
取消	取消设置

内容过滤

MAC/IP/PORT ACL
内容过滤

基本设置

基本设置

使能过滤 禁止 ▼

默认策略 黑名单 ▼

过滤列表上传与下载

本地文件 未选择任何文件

Webs URL过滤

当前系统的URL过滤列表

编号	URL
[]	[]

URL过滤

URL

(最大规则数为 16)

关键字过滤

当前系统的关键字过滤列表

编号	关键字
[]	[]

关键字过滤

关键字

(最大规则数为 16)

参数名称
描述

基本设置	描述
使能过滤	是否使能 content 过滤
默认策略	默认策略是接受或者禁止过滤规则
Webs URL 过滤	描述
连接 URL	已经存在的 URL 过滤规则（黑名单）
删除/取消	对已存在的过滤规则可以选择删除或取消
添加一个 URL	添加 URL 过滤规则
添加/取消	点击添加或取消
Web 过滤设置	描述
当前 ULR 过滤列表	已经存在的关键字（黑名单）
删除/取消	对已存在的关键字可以选择删除或取消
关键字过滤	添加关键字
添加/取消	点击添加或取消
基本设置	描述
使能过滤	是否使能 content 过滤

应用

在该页面可以对高级 Nat、UPnP、IGMP、日常应用、DMS、MLD、设备命名 WIFI 分享、DDNS 进行设置。

高级 NAT

状态
网络
IPPBX
无线2.4GHz
无线5GHz
安全
应用
存储
管理

高级Nat
UPnP
IGMP

ALG

ALG 配置

FTP	开启 ▼
SIP	禁止 ▼
H323	禁止 ▼
PPTP	禁止 ▼
L2TP	禁止 ▼
IPSec	禁止 ▼

参数名称	描述
FTP	开启/禁止 FTP
SIP	开启/禁止 SIP
H323	开启/禁止 H323
PPTP	开启/禁止 PPTP
L2TP	开启/禁止 L2TP
IPSec	开启/禁止 IPSec

UPnP

UPnP（Universal Plug and Play）支持零设置连网，并能自动发现多种连网设备。启用 UPnP 时，允许支持 UPnP 功能的设备动态的接入网络，获得 IP 地址，传送其性能信息。如果在网络上有 DHCP 和 DNS 服务器，可以自动获取 DHCP 和 DNS 服务。

支持 UPnP 的设备可自动脱离网络，对该设备或网络上的其他设备无影响。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
<div style="display: flex; justify-content: space-between;"> 高级Nat UPnP IGMP </div>								
<div style="border: 1px solid #ccc; padding: 5px;"> <p>UPnP</p> <p>UPnP 配置</p> <p>UPnP <input type="button" value="开启"/></p> </div>								
参数名称		描述						
UPnP		开启/禁止 UPnP						

IGMP

组播具有同一个数据发送到多个设备的功能。

IP 主机使用 IGMP（Internet Group Management Protocol）报告组播组成员资格给相邻路由器发送数据，同时组播路由器使用 IGMP 发现哪些主机属于同一组播组。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
<div style="display: flex; justify-content: space-between;"> 高级Nat UPnP IGMP </div>								
<div style="border: 1px solid #ccc; padding: 5px;"> <p>IGMP</p> <p>IGMP 配置</p> <p>IGMP 代理 <input type="button" value="开启"/></p> <p>IGMP Snooping enable <input type="button" value="开启"/></p> </div>								
参数名称		描述						
IGMP 代理		是否开启 IGMP 功能						

存储

在该页面用户可以管理其路由器设备，用户能够设置设备 Disk 管理、FTP 设置、SMB 等相关配置。

Disk 管理

该页面用于管理 USB 存储设备。

参数名称	描述
删除	删除 USB 存储设备文件
RemoveDisk	在 USB 存储设备中传输文件
Fomat	格式化 USB 存储设备
Re-allowcate	重置 USB 存储设备

FTP 设置

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
Disk 管理		FTP 设置						
FTP 设置								
FTP服务器配置								
FTP Server			<input type="radio"/> 开启		<input checked="" type="radio"/> 禁止			
FTP Server Name	FTP							
Anonymous Login			<input type="radio"/> 开启		<input checked="" type="radio"/> 禁止			
FTP Port	21							
Max. Sessions	10							
Create Directory			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Rename File/Directory			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Remove File/Directory			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Read File			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Write File			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Download Capability			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			
Upload Capability			<input checked="" type="radio"/> 开启		<input type="radio"/> 禁止			

参数名称	描述
FTP Server	开启 FTP server
FTP Server Name	设置 FTP server name
Anonymous Login	是否支持匿名登录
FTP Port	设置 FTP server 端口
Max. Sessions	最大连接数
Create Directory	开启创建目录
Rename File/Directory	开启/禁用重命名文件/目录
Remove File/Directory	启用/禁用文件/目录的传输
Read File	启用/禁用读文件
Write File	启用/禁用写入文件
Download Capability	启用/禁用下载功能。
Upload Capability	启用/禁用上载功能函数

管理

在该页面用户可以管理其路由器设备，用户能够设置设备的时间/日期、密码、web 登录、系统日志以及 TR069 的相关配置等。

管理

1) 保存配置文件

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式

保存配置文件

配置文件上传与下载

本地文件 未选择任何文件

参数名称	描述
配置文件上传与下载	上传：点击浏览，在本地选择文件，按上传按钮开始上传文件
载	下载：点击下载，然后选择存放路径开始下载配置文件

2) 管理员设置

管理员设置

重置密码

用户类型	<input type="text" value="超级管理员"/>
新用户名	<input type="text" value="admin"/>
新密码	<input type="text"/> (最大长度是25)
确认密码	<input type="text"/>

语言

语言	<input type="text" value="中文"/>
----	---------------------------------

VPN 使用

管理使用VPN	<input type="text" value="禁止"/>
---------	---------------------------------

管理员设置	
重置密码	
用户类型	超级管理员 ▼
新用户名	admin
新密码	(最大长度是25)
确认密码	
语言	
语言	中文 ▼
VPN 使用	
管理使用VPN	禁止 ▼
网页设置	
远程Web登录	开启 ▼
本地Web端口	80
Web端口	8080
Web SSL端口	443
Web闲置超时(0 - 60分钟)	5
允许的远程IP地址(IP1;IP2;...)	0.0.0.0
Telnet 使用	
远程 Telnet	开启 ▼
Telnet 端口	23
允许的远程IP地址(IP1;IP2;...)	0.0.0.0
主机名	Mediatek

参数名称	描述
用户类型	有管理员、普通用户二个级别
新用户名	可以修改用户名，设置新的用户名
新密码	添加新用户名的密码
确认密码	再次添加新密码
语言	有中文、英语、俄语、芬兰语、西班牙语可以选择，Web 页面会发生对应的变化
远程 Web 登录	是否启用远程 Web 登录
Web 端口	设置用于通过 Internet 端口和 PC 端口进行登录的端口，默认值 80
Web 闲置超时	设置网络空闲超时时间，若网络空闲超时没有任何操作，网页自动注销
允许远程的 IP 地址	设置用户可以远程登录设备的 IP
Telnet 端口	设置用于 telnet 到设备的端口值

**注意**

默认情况下禁用 telnet 访问。

3)NTP 设置**时间/日期设置****NTP设置**

NTP开关	开启 ▾
Option 42	禁止 ▾
当前时间	2017 - 09 - 25 . 16 : 03 : 16
与主机同步	与主机同步
NTP设置	(GMT+08:00) 中国海岸,香港 ▾
主NTP服务器	pool.ntp.org
从NTP服务器	cn.pool.ntp.org
NTP同步(1 - 1440分钟)	60

参数名称	描述
NTP 开关	是否启用 NTP
当前时间	显示当前时间
NTP 设置	设置时区
主 NTP 服务器	首选 NTP 服务器的 IP 地址或是域名
从 NTP 服务器	备选 NTP 服务器的 IP 地址或是域名
NTP 同步	NTP 的同步周期，周期时长可以为 1 到 1440 分钟的任何一个，默认设置是 60 分钟

4)系统日志功能**系统日志设置****系统日志设置**

系统日志使能	开启 ▾
系统日志级别	INFO ▾
登录日志使能	开启 ▾
呼叫日志使能	开启 ▾
网络日志使能	开启 ▾
设备管理日志使能	开启 ▾
设备告警日志使能	开启 ▾
内核日志使能	开启 ▾
远程系统日志使能	禁止 ▾
远程系统日志服务器	

参数名称	描述
系统日志使能	是否启用系统日志功能
系统日志级别	选择系统日志等级，有 INFO 和 Debug 两种等级，其中 Debug 能比 INFO 获取更多的信息
远程系统日志使能	是否启用远程系统日志功能
远程系统日志服务	添加远程服务器 IP 地址

5)出厂状态设置

出厂状态设置

出厂状态设置
 锁定恢复出厂状态 禁止 ▾

出厂设置

恢复出厂设置 恢复出厂设置

参数名称	描述
出厂状态设置	当启用时，该设备可能不会重置为出厂默认值，直到这个参数被重置为禁用
出厂设置	点击恢复出厂设置来恢复设备到出厂设置

固件升级

状态
网络
IPPBX
无线2.4GHz
无线5GHz
安全
应用
存储
管理

管理
固件升级
计划任务
证书
自动更新
SNMP
TR069
诊断
工作模式

固件管理

固件升级
 本地升级 选择文件 未选择任何文件

升级

描述
1.点击选择文件
2.选择所需要升级的文件

3. 按 **升级** 开始升级设备

计划任务

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式

计划任务

定时wifi

编号	开启	无线名称	星期选择	开启时间	关闭时间
----	----	------	------	------	------

删除已选择项 添加 编辑

定时重启

定时重启

工作模式

时间 :

重启DDPoE

定时重启

定时重启

工作模式

时间 :

重启PPPoE

重启PPPoE

工作模式

时间 :

保存并应用 保存 取消 重启

参数名称	描述
定时 WIFI	
开启	开启/禁止定时 WIFI
无线名称	此处不可选
工作模式	选择工作模式，每周/每天
WIFI 工作周期	设置 WIFI 工作周期
应用	修改完参数后选择应用，或取消
定时重启	
定时重启	开启/禁止定时重启
工作模式	选择工作模式，每天/每周

时间	设置定时重启的时间
----	-----------

重启 PPPoE

重启 PPPoE	开启/禁止重启 PPPoE
----------	---------------

工作模式	选择工作模式，每天/每周
------	--------------

时间	设置重启 PPPoE 的时间
----	----------------

自动更新 (Provision)

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式

Provision

配置简介

Provision 使能	开启 ▼
同步复位	开启 ▼
同步随机延时(秒)	40
同步周期(秒)	3600
同步错误重试延迟(秒)	3600
强制同步延时(秒)	14400
升级后重新同步	开启 ▼
Resync From SIP	禁止 ▼
Option 66	开启 ▼
Option 67	禁止 ▼
配置文件名	\$(MA)
用户代理名称	
配置文件规则	http://prv1.flyingvoice.net:69/config/\$(MA)?mac=\$(MA)&

参数名称	描述
Provision 使能	是否使能 provision
同步复位	重启后是否重新同步启用
同步随即延时	设置请求同步文件的最大延迟，默认是 40
同步周期	如果最后重新同步是失败的，在“Resync Error Retry Delay”时间之后，设备将重试重新同步，默认是 3600 秒
同步错误重试延时	设置定时重新同步，默认值是 3600 秒
强制同步延时	如果到了重新同步的时间，但设备正忙，在这种情况下，设备会等待一段时间，最长的是“强制重新同步延迟”，默认为 14400s，时间过后，设备将被迫重新同步。
升级后重新同步	重新同步后，是否使能固件更新功能，默认是 enable
Resync From SIP	启用/禁用同步从 SIP

Option 66	它仅用于公司内部规定的模式。当使用 TFTP 与选项 66 实现配置时，用户必须在设备的网页输入正确的配置文件名。当禁用选项 66，此参数不起作用
Option 67	启用/禁止 Option 67
配置文件	配置文件名称
用户代理名称	用户代理名称
配置文件规则	配置文件的 URL 注意，指定的文件路径是相对于 TFTP 服务器的根目录

固件升级

升级使能	开启 ▾
升级错误重试延迟(秒)	3600
升级规则	<input type="text"/>

参数名称	描述
升级使能	开启或关闭升级使能
升级错误重延时	如果最后一次升级失败，FPX9102H 将会尝试升级，再次在“升级错误重试延迟”期间，默认为 3600s
升级规则	URL 是升级规则

SNMP

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式

SNMP 配置

SNMP 配置

SNMP 服务	禁止 ▾
Trap 服务地址	<input type="text"/>
SNMP只读口令	public
SNMP读写口令	private
Trap 口令	trap
Trap 时间间隔(秒)	300

参数名称	描述
SNMP 服务	是否使能 SNMP
Trap 服务地址	输入 trap server 地址
SNMP 只读口令	用作通过 SNMP 从设备请求信息的密码的字符串值

SNMP 读写口令	用作通过 SNMP 将配置值写入设备的密码的字符串值
Trap 口令	用作从设备中检索陷阱的密码的字符串值
Trap 时间间隔	陷阱从设备发送的时间间隔

TR-069

TR-069 提供了自动配置互联网接入设备，并降低了管理成本。 TR-069（技术报告 069 的简称）是 DSL 论坛技术规范，名称为 CPE WAN 管理协议（CWMP），它定义了用于远程管理终端用户设备的应用层协议。 使用 TR-069，终端与自动配置服务器（ACS）建立连接并自动配置。

设备配置使用的 TR - 069

TR-069 配置页面在管理菜单下是可用。

状态	网络	IPPBX	无线2.4GHz	无线5GHz	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式

TR069 设置	
ACS	
TR069 使能	开启 ▾
CWMP	开启 ▾
ACS URL	http://acs1.flyingvoice.net:8080/tr069
用户名	FLY69167000116
密码	*****
定期通知启用	开启 ▾
定期通知时间间隔(秒)	99787
连接请求	
用户名	FPX9102H
密码	*****

参数名称	描述
ACS 参数	
TR069 使能	是否使能 TR069
CWMP	是否使能 CWMP
ACS URL	ACS URL 地址
用户名	ACS 用户名
密码	ACS 用户名密码
定期通知启用	是否开启周期通知功能，默认为开启

定期通知时间间隔 周期通知间隔，单位为 s，默认为 43200s

连接请求

用户名 用于将 TR069 服务器连接到 DUT 的用户名

密码 用于将 TR069 服务器连接到 DUT 的密码

诊断

在此页面中，用户可以进行数据包跟踪，ping 测试和跟踪路由测试，以诊断设备的连接状态。

状态	网络	无线2.4GHz	无线5GHz	SIP	FXS1	FXS2	安全	应用	存储	管理
管理	固件升级	计划任务	证书	自动更新	SNMP	TR069	诊断	工作模式		

报文追踪

报文追踪

追踪接口

报文追踪

Ping 测试

Ping 测试

IP 地址或主机名

广域网连接

Traceroute 测试

Traceroute 测试

IP 地址或主机名

广域网连接

描述

1.报文追踪

用户可以使用数据包跟踪功能来拦截穿越设备的数据包，单击开始按钮开始家庭网关跟踪，并保持刷新页面，直到消息跟踪显示停止，单击保存按钮以保存捕获的数据包

2.Ping 测试

输入目的 IP 或主机名，然后单击“应用”，设备将执行 ping 测试

Ping 测试

IP 地址或主机名

广域网连接

1_MANAGEMENT_VOICE_INTERNET_R_VID_ ▾

```
PING www.baidu.com (61.135.169.125): 56 data bytes
64 bytes from 61.135.169.125: seq=0 ttl=56 time=5.083 ms
64 bytes from 61.135.169.125: seq=1 ttl=56 time=2.585 ms
64 bytes from 61.135.169.125: seq=2 ttl=56 time=2.556 ms
64 bytes from 61.135.169.125: seq=3 ttl=56 time=2.259 ms
64 bytes from 61.135.169.125: seq=4 ttl=56 time=2.221 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.221/2.940/5.083 ms
```

提交

取消

3.Traceroute 测试

输入目标 IP 或主机名，然后单击应用，设备将执行跟踪路由测试

Traceroute 测试

IP 地址或主机名

广域网连接

1_MANAGEMENT_VOICE_INTERNET_R_VID_ ▾

```
traceroute: warning: www.baidu.com has multiple addresses; using 61.135.169.125
traceroute to www.baidu.com (61.135.169.125), 30 hops max, 38 byte packets
 1 FPX9102H (192.168.10.1) 1.000 ms 0.528 ms 0.473 ms
 2 192.168.18.1 (192.168.18.1) 0.963 ms 1.275 ms 0.886 ms
 3 114.245.112.1 (114.245.112.1) 2.631 ms 2.709 ms 2.880 ms
 4 61.148.160.173 (61.148.160.173) 1.821 ms 2.019 ms 1.817 ms
 5 *
```

提交

取消

工作模式

工作模式设置

工作模式设置

工作模式

高级模式
基本模式
高级模式

保存并应用 取消 重启

描述

用户可再此选择自己所需要的工作模式

第 4 章 故障排除

本章内容包含：

- 接通电源无反映
- 登录不上 Web
- 忘记密码

接通电源后无反应

解决方案：

检查电源适配器是否正确连接。

无法登录设备的网页

解决方案：

检查以太网电缆是否正确连接。

检查 URL 是否是正确的写，URL 格式：`http:// Internet 端口 IP address`。

检查你的防火墙/ NAT 设置是否正确。

如果 IE 版本是 IE8 的检查，或使用其他浏览器如 Firefox 或 Mozilla，或联系您的管理员，供应商或 ITSP

忘记密码

网站和菜单的默认密码为 `admin`。

如果用户更改密码，然后忘了，你不能访问需要密码的配置网站或菜单项。

解决方案：

出厂默认值：按“RST”按钮，等待 5 秒后放开，设备会回复出厂设置，如果您选择出厂默认，您将返回到原始出厂设置的路由器，将删除所有当前的设置，包括系统日志和通话记录等。