



用户手册

FWR9202/FWR9601

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 | 10 |
| FWR9202/FWR9601..... | 11 |
| 指示灯和接口..... | 12 |
| LED 指示灯介绍..... | 12 |
| 接口介绍..... | 13 |
| 硬件安装..... | 14 |
| 安装准备..... | 14 |
| 安装步骤..... | 14 |
| 第 2 章 IVR(互动式语音应答) | 15 |
| 配置设备的方法(IVR)..... | 16 |
| 启动 IVR..... | 16 |
| IVR 描述..... | 16 |
| 第 3 章 基本配置设置 | 20 |
| 两级管理..... | 21 |
| Web 管理界面..... | 21 |
| Web 界面管理..... | 23 |
| Web 界面..... | 23 |
| 设备相关信息..... | 24 |
| 配置..... | 25 |
| 配置网络连接..... | 25 |
| 设置无线连接..... | 26 |
| 无线安全设置..... | 27 |
| 配置会话初始协议..... | 28 |
| 拨打电话..... | 30 |
| 打电话或分机号码..... | 30 |
| IP 直拨..... | 30 |
| 呼叫保持..... | 30 |
| 呼叫转移..... | 30 |
| 呼叫等待..... | 31 |
| 三方会议..... | 31 |

| | |
|-----------------------------|-----------|
| 第 4 章 Web 界面管理 | 32 |
| 登录..... | 33 |
| 状态..... | 34 |
| 系统信息..... | 34 |
| 内网主机信息..... | 34 |
| 系统日志..... | 35 |
| 网络和安全..... | 36 |
| WAN 口设置..... | 36 |
| LAN 口设置..... | 41 |
| IPv6 设置..... | 42 |
| VPN 设置..... | 44 |
| 端口映射..... | 46 |
| DMZ..... | 47 |
| Vlan..... | 47 |
| QOS..... | 48 |
| 端口限速..... | 48 |
| 端口管理..... | 49 |
| 路由配置..... | 49 |
| 高级设置..... | 50 |
| 无线 2.4GHz..... | 51 |
| 基本设置..... | 51 |
| 无线安全..... | 52 |
| Wi-Fi 多媒体(WMM)..... | 55 |
| 无线分布式部署(WDS)..... | 56 |
| 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..... | 60 |
| VOIP..... | 61 |
| 账号 1..... | 61 |
| SIP 设置..... | 66 |
| VoIP QoS..... | 67 |
| 电话..... | 68 |
| 首选项..... | 68 |
| 数图..... | 70 |
| 电话本..... | 71 |
| 黑名单..... | 72 |
| 通话日志..... | 73 |
| 安全..... | 74 |
| MAC/IP/Port/ACL..... | 74 |
| 内容过滤..... | 76 |
| 应用..... | 78 |
| 高级 NAT..... | 78 |
| UPnP..... | 78 |
| 管理..... | 80 |
| 管理..... | 80 |

| | |
|------------------------|-----------|
| 固件升级..... | 83 |
| 计划任务..... | 84 |
| 自动跟新 (Provision) | 85 |
| SNMP..... | 86 |
| Tr069..... | 87 |
| 诊断..... | 88 |
| 工作模式..... | 89 |
| 第 5 章 故障排除..... | 90 |
| 接通电源后无反应..... | 91 |
| 无法登录设备的网页..... | 91 |
| 忘记密码..... | 91 |

关于本指南

感谢您购买我们的千兆双频无线 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 IEEE802.11b/g/n 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：IVR\(互动式语音应答\)](#)
- [第三章：基本配置设置](#)
- [第四章：系统规划](#)
- [第五章：常见故障排除](#)

联系飞音时代

网站: <http://www.flyingvoice.cn/>
热线: 010-67886296 0755-26099365
销售查询通道 sales1@flyingvoice.com
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

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：

- [FWR9202/FWR9601](#)
- [指示灯和接口](#)
- [硬件安装](#)
- [安装准备](#)
- [安装步骤](#)

FWR9202/FWR9601

| 功能/型号 | FWR9202 | FWR9601 |
|----------|---|---|
| 产品图片 |  |  |
| WAN 口 | 1 | 1 |
| LAN 口 | 4 | 4 |
| FXS 口 | 0 | 1 |
| 以太网口 | 5* RJ45 10/100/1000M | 5* RJ45 100/100/1000M |
| 传真 | T.30, T.38 Fax | |
| WiFi 支持 | 2.4G 2T2R (300Mbps) 5G 2T2R (867Mbps) | 2.4G 2T2R (300Mbps) 5G 2T2R (867Mbps) |
| Voice 编码 | G.711 (A-law, U-law), G.729A/B, G.723, G.722 (Wide band) | |
| 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

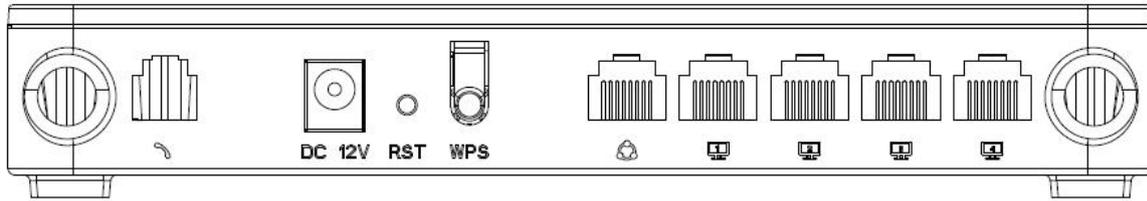
FWR9601



| LED | 状态 | 说明 |
|----------|------|-----------------------|
| Power | 绿色常亮 | 系统正常上电 |
| | 熄灭 | 系统未上电 |
| WAN | 绿色常亮 | 网络连接成功（物理连接建立），没有数据传输 |
| | 绿色闪烁 | 有数据传输 |
| | 熄灭 | 系统未上电或者网口未连接网络设备 |
| LAN（1-4） | 绿色常亮 | 网络连接成功（物理连接建立），没有数据传输 |
| | 绿色闪烁 | 有数据传输 |
| | 熄灭 | 系统未上电或者网口未连接网络设备 |
| 2.4G | 绿色常亮 | 2.4G WIFI 开关开启，AP 工作 |
| | 绿色闪烁 | 2.4G 连接有数据传输 |
| | 熄灭 | 2.4G 未开启或设备断电 |
| 5G | 绿色常亮 | 5G WIFI 开关开启，AP 工作 |
| | 绿色闪烁 | 5G 连接有数据传输 |
| | 熄灭 | 5G 未开启或设备断电 |
| FXS(1-2) | 绿色常亮 | 成功注册到软交换机，但无业务流 |
| | 绿色闪烁 | 有业务流传输或者正在注册（摘机/通话） |
| | 熄灭 | 系统未上电或未注册，或注册不成功 |

接口介绍

FWR9601



| 界面 | 说明 |
|------------|--------------------------|
| PHONE | 连接电话 |
| POWER | 连接电源适配器 |
| RST | 恢复出厂设置按钮，长按 5s 后设备恢复出厂设置 |
| WPS | 一键连接 WIFI |
| WAN | 连接访问互联网 |
| LAN1/2/3/4 | 连接本地网络设备 |

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（仅针对 FWR9601）；
- 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 IVR(互动式语音应答)

本章内容包含：

- [配置路由器的方法 \(IVR\)](#)
- [IVR 描述](#)

配置设备的方法(IVR)

该设备可通过两种方式实现配置，具体如下：

- (1) 使用 IVR
- (2) 使用网页方式

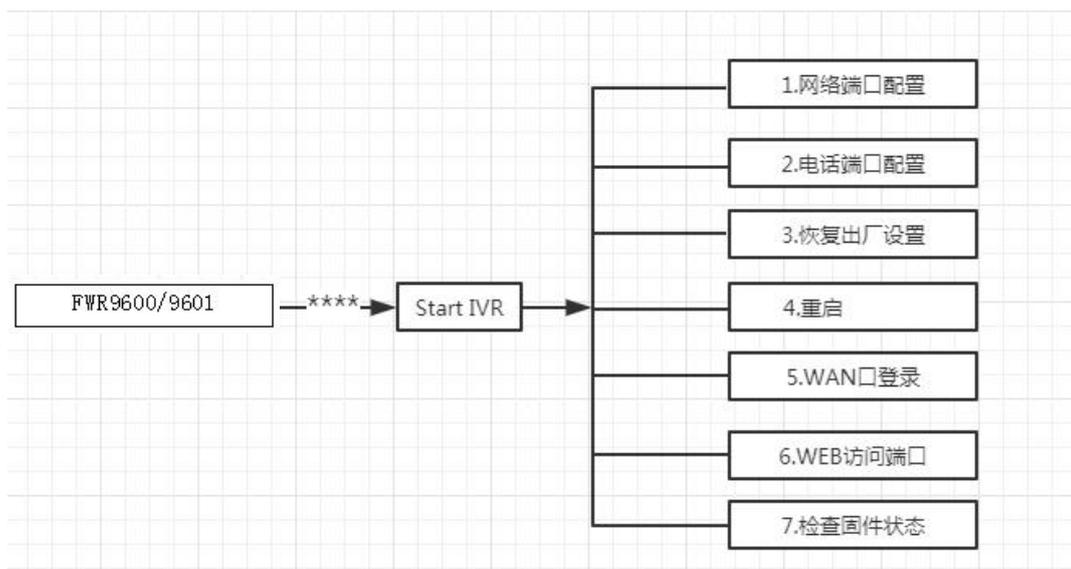
启动 IVR

用户按照以下步骤实现 IVR：

- (1) 摘机并按下“****”键启动 IVR，然后用户将听到设备的语音提示“请输入选项，1 是 WAN 端口……”。
- (2) 根据不同的选项，按下 0 到 9 之间的任何一位数字，设备则会播报相应的内容，数字 0 到 9 代表的内容具体请参见下面的图表。
- (3) 每次设置成功后，设备会再次播放“请输入选项，1 是 WAN 端口……”。

IVR 描述

下面的图表列举了 IVR 的要求和详细的描述：



| 操作代码 | 内容 |
|------|---|
| 1(1) | <p>1) 摘机并按下“****”键启动 IVR;</p> <p>2) 选择“1”，然后设备将会播报当前的 WAN 端口连接类型;</p> <p>3) 如需改变 WAN 端口的网络连接类型，请用户在听到“请输入密码”后输入正确的密码，并以“#”结束;</p> <ul style="list-style-type: none"> · IVR 的密码和登录设备的 WEB 页面时的密码是相同的，用户只需直接按下相应的键，各键和字母的对应请参见注意事项。 · 例如：登录 WEB 页面的密码是“admin”，则 IVR 的密码也是“admin”，用户输入“23646”后即可开始设置 WAN 端口的网络连接类型。 <p>4) 如果输入的密码正确，设备播报“操作成功”;</p> <p>5) 选择新的 WAN 端口网络连接类型，1 代表 DHCP，2 代表静态 IP，输入数字后请以“#”结束。</p> <p>6) 设备播报“操作成功”，这表示用户已经成功设置了 WAN 端口的连接类型，设备将会再次播报“请输入选项， 1 是 WAN 端口.....”。</p> |
| 1(2) | <p>1) 摘机并按下“****”键启动 IVR;</p> <p>2) 按下“2”，然后设备会播报当前的 WAN 端口 IP 地址;</p> <p>3) 输入新的 WAN 端口的 IP 地址，并以“#”结束;</p> <ul style="list-style-type: none"> · 请用“*”替代“.”，例如用户可输入 192*168*20*168 来设置新的 WAN 端口 IP 地址为 192.168.20.168。 · 输入新的 IP 地址时请以“#”结束。 <p>4) 如果用户设置正确，则设备将会播报“操作成功”。</p> |
| 1(3) | <p>1) 摘机并按下“****”键启动 IVR;</p> <p>2) 选择“3”，设备会播报 WAN 端口子网掩码;</p> <p>3) 输入新的 WAN 端口子网掩码，并以“#”结束;</p> <ul style="list-style-type: none"> · 请用“*”替代“.”，例如用户可输入 255*255*255*0 来设置新的 WAN 端口子网掩码为 255.255.255.0。 · 输入新的子网掩码时请以“#”结束。 <p>4) 如果用户设置正确，则设备将会播报“操作成功”。</p> |
| 1(4) | <p>1) 摘机并按下“****”键启动 IVR;</p> <p>2) 选择“4”，设备会播报当前的网关;</p> <p>3) 输入新的网关时请以'#'结束。</p> <ul style="list-style-type: none"> · 请用“*”替代“.”，例如用户可输入 192*168*20*1 来设置新的网关地址为 192.168.20.1。 · 输入新的网关地址时请以“#”结束。 <p>4) 如果用户设置正确，则设备将会播报“操作成功”。</p> |

-
- (5) 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“5”，设备将会播报当前的 DNS;
- 3) 输入新的 DNS 地址并以“#”结束;
- 请用“*”替代“.”，例如用户可输入 **192*168*20*1** 来设置新的 DNS 为 **192.168.20.1**。
 - 输入新的 DNS 时请以“#”结束
- 4) 如果用户设置正确，则设备将会播报“**操作成功**”。
-
- 2 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“2”，然后设备将继续播报提示用户可选择 1.当前电话号码; 2.注册服务器地址; 3.注册端口; 4.呼叫转移配置; 5.DND 配置
- 3) 继续按下“1”，然后设备会继续播报当前的**电话端口的电话号码**。之后设备将会再次播报“**1.电话号码.....**”。
-
- 3 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“6”，设备会播报“**恢复出厂配置**”;
- 3) 在听到设备的提示音“**请输入密码**”后请用户输入密码，输入密码的方式和操作 1 相同;
- 4) 如果用户输入的密码正确，设备将播报“**操作成功**”，然后设备的设置被恢复到出厂状态;
- 5) 请按下“7”重启设备使更改生效。
-
- 4 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“7”，设备会播报“**重启**”;
- 3)在听到设备的提示音“**请输入密码**”后请用户输入密码，输入密码的方式和操作 1 相同;
- 4) 如果用户密码和设置都正确，设备将会自动重启。
-
- 5 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“8”，设备会播报“**WAN 端口登陆**”;
- 3) 在听到设备的提示音“**请输入密码**”后请用户输入密码，输入密码的方式和操作 1 相同;。
- 4) 如果用户输入密码正确，设备将播报“**操作成功**”
- 5) 设备播报“**1 启用 2 禁用**”，选择 1 或者 2，并以“#”结束;
- 6) 如果设置正确，设备将播报“**操作成功**”。
-
- 6 1) 摘机并按下“****”键启动 IVR;
- 2) 选择“9”，设备会播报“**WEB 访问端口**”;
- 3) 在听到设备的提示音“**请输入密码**”后请用户输入密码，输入密码的方式和操作 1 相同;
- 4) 如果用户输入密码正确，设备将播报“**操作成功**”;
-

-
- 5) 设备播报当前的 **WEB 访问端口**;
 - 6) 输入新的 WEB 接入端口号, 并以 “#” 结束;
 - 7) 设置成功后, 设备将播报 “**操作成功**”。
-
- 7
 - 1) 摘机并按下 “****” 键启动 IVR;
 - 2) 选择 “0”, 设备会播报当前的 “**固件版本**”。
-

注意:



- 输入密码或是选择 WAN 端口的网络类型后请以 “#” 号结束; 用户如需中途退出设置, 请按下 “**” 键。
 - 如果在 IP 分配模式下进行任何更改, 路由器必须重新启动才能使设置生效。
 - 使用 “#” 键完成输入 IP 地址或子网掩码, 使用 “*” 进入 “
例如, 要通过键盘输入 IP 地址 192.168.10.159, 请按以下键: 192 * 168 * 10 * 159, 使用 # 键来表示您已经完成了 IP 地址或子网掩码的输入
 - 在静态 IP 模式下分配 IP 地址时, 需要设置 IP 地址, 子网掩码和默认网关才能完成配置。如果在 DHCP 模式下, 请确保在连接设备的 WAN 端口的现有宽带连接中可以使用 DHCP 服务器。
 - 设备的默认网络端口 IP 地址为 192.168.1.1, 该地址不应分配给 LAN 端口同一网段的路由器的 WAN 端口 IP 地址。
 - 可以使用电话键盘输入密码, 数字和字母之间的映射表如下:
输入: D, E, F, d, e, f- 按'3'
输入: G, H, I, g, h, i- 按'4'
输入: J, K, L, j, k, l- 按'5'
输入: M, N, O, m, n, o- 按'6'
输入: P, Q, R, S, p, q, r, s- 按'7'
输入: T, U, V, t, u, v- 按'8'
-

第 3 章 基本配置设置

本章内容包含：

- 两级管理
- Web 界面管理
- 配置
- 拨打电话

两级管理

本节解释如何为管理员和用户设置密码，以及如何调整基本设置和高级设置。

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，该级别只能配置设备的部分参数。

Web 管理界面

设备可以提供一个基于 Web 浏览器的接口，可用于配置和管理设备。见下文获取信息

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：



该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。

普通级别的用户能够浏览以及配置所有的FWR9601参数，除了SIP线路中的一些不能被改变的参数之外，例如服务器地址和端口；管理员用户级别的用户能够配置其他所有的参数。

路由器默认管理级别登录名/密码：`admin/admin`

路由器默认普通用户登录名/密码：`user/user`

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>`。将打开以下登录页

面，输入用户名和密码，点击登录。



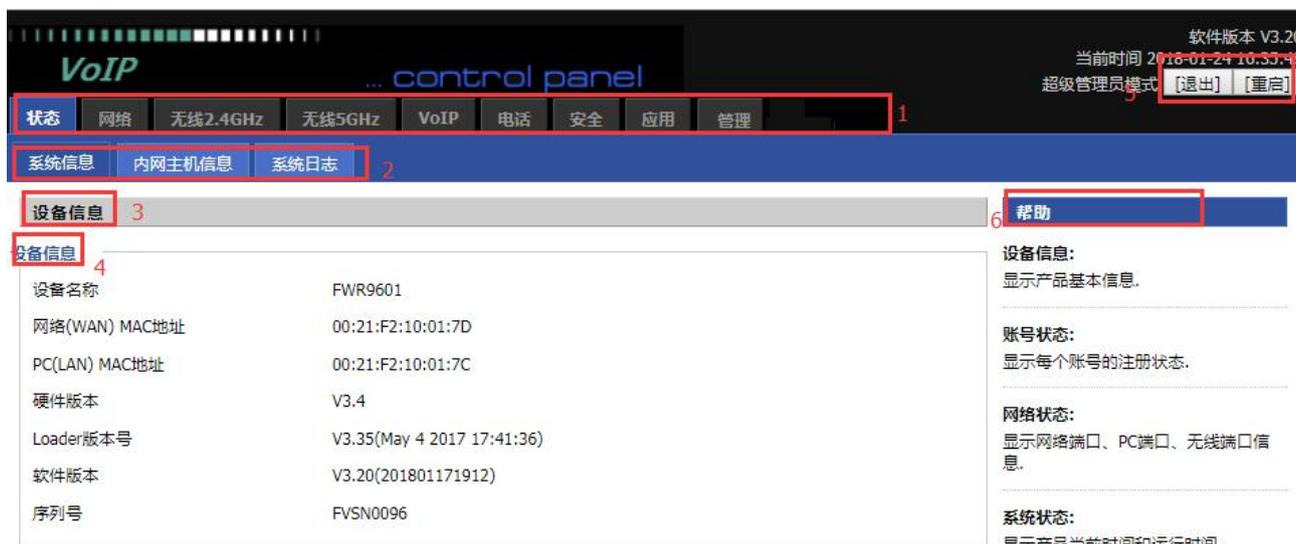
The image shows a login interface for a VoIP control panel. At the top, there is a dark blue header with the text "VoIP" in green and "... control panel" in light blue. Below the header, there are two input fields: "Username" and "Password". The "Username" field contains the text "admin". The "Password" field contains five dots. To the right of the "Password" field is a "Login" button.

对于管理员模式操作，在用户名/密码上键入 `admin / admin`，然后单击登录开始配置。

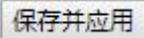
对于用户模式操作，请在用户名/密码上键入 `user/user`，然后单击登录开始配置。

Web 界面管理

Web 界面



账号状态

| 序号 | 名称 | 描述 |
|------|---|--|
| 位置 1 | 主导航栏 | 点击此导航栏，会出现相应子导航栏 |
| 位置 2 | 次导航栏 | 点击子导航栏进入到配置网页 |
| 位置 3 | 设备信息 | 配置标题 |
| 位置 4 | 主要信息 | 显示的固件版本、DSP 版本、当前的时间和管理模式。 |
| 位置 5 | 设备名称 | 配置栏 |
| 位置 6 | 帮助 | 显示帮助信息，用户可以这里获取一些帮助 |
| |  | 点击此按钮将配置提交并立即生效，有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。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 |
| |  | 点击设备重新启动 |

设备相关信息

在此页面，用户可以查看设备的系统信息、内网主机信息和系统日志信息。用户通过网页方式登陆后首先跳转进入就是该页面。



设备信息

设备信息

| | |
|---------------|----------------------------|
| 设备名称 | FWR9601 |
| 网络(WAN) MAC地址 | 00:21:F2:10:01:7D |
| PC(LAN) MAC地址 | 00:21:F2:10:01:7C |
| 硬件版本 | V3.4 |
| Loader版本号 | V3.35(May 4 2017 17:41:36) |
| 软件版本 | V3.20(201801171912) |
| 序列号 | FVSN0096 |

| 序号 | 名称 | 描述 |
|--------|--------|--|
| 次导航栏 1 | 系统信息 | 该页面是设备状态显示页面，可在此得到设备的一些信息，比如设备信息，WAN 口 IP 信息 |
| 次导航栏 2 | 内网主机信息 | 该页面是设备 LAN 连接的终端设备的 IP 地址和 MAC 地址信息 |
| 次导航栏 3 | 系统日志 | 该页面可查看设备系统日志，便于调试人员获取一些信息 |

配置

配置网络连接



注意

可在管理---工作模式页面设置工作模式：基本模式和高级模式

在高级模式下，Web 页面导航到网络---WAN 页面，WAN 连接可被插入或删除。有关 Internet 连接设置的更多信息，请参见下表。

| 状态 | 网络 | 无线2.4GHz | 无线5GHz | VoIP | 电话 | 安全 | 应用 | 管理 | | | |
|------|-----|----------|----------|----------|-----|------|-----|------|-----|------------|------|
| WAN | LAN | IPv6高级设置 | IPv6 WAN | IPv6 LAN | VPN | 端口映射 | DMZ | Vlan | QoS | Rate Limit | 端口管理 |
| 高级设置 | | | | | | | | | | | |

| INTERNET | | 帮助 |
|--|---|---|
| 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 | | |
| 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 | | |
| 从DNS地址 | | |
| DHCP | | |
| DHCP更新 | 更新 | |
| DHCP 供应商(选项 60) | FLYINGVOICE-FWR9601 | |
| 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"/> 无线(SSID) | <input checked="" type="checkbox"/> 无线(SSID1) | <input checked="" type="checkbox"/> 无线(SSID2) |
| | | <input checked="" type="checkbox"/> 端口_4 |
| | | <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 |
| NAT 使能 | 需要在多 WAN 口页面设置 |
| 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 | 因特网端口的首选 DNS |
| 从 DNS | 因特网端口的备选 DNS |
| DHCP | 当 WAN IP 模式设置为 DHCP 时显示 |
| DHCP 跟新 | 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 |

设置无线连接

要设置无线连接，请执行以下步骤。

使能无线和设置无线网络名称:打开无线>基本页面如下图所示：

| 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 |

| | |
|---------------|--|
| | 请注意：此参数更改所需的“保存” |
| 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 |
| 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) | 从下拉列表中选择设备操作通道。 |
| 工作模式 | 混合模式：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 节电模式：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 |

无线安全设置

打开无线/无线安全页面，配置自定义安全参数。

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 FWR9601-10017C ▼

"FWR9601-10017C"

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 禁止 ▼

新增：[] (最大规则数为 64)

| 参数名称 | 描述 |
|---------|-----------------------------|
| SSID 选择 | 选择 SSID 从下拉列表中会淹没的安全配置 |
| 安全模式 | 选择适当的加密模式，以改善无线数据包的安全性和隐私性。 |

每个加密模式都会启动一个额外的 Web 页面，并要求您提供额外的配置。高安全性，该设备可以配置为安全模式为 WPA2-PSK 和 WPA 算法作为 AES。

| | |
|--------|---|
| WPA 算法 | 该参数用于选择无线家庭网关的加密算法；选择 TKIP，AES 和 tkipaes。 |
| 通行口令 | 配置预共享密钥的安全密码。 |
| 私钥更新间隔 | 设置关键计划的更新周期，默认是 3600s。 |
| 策略 | 禁止：访问策略规则不强制执行 允许：只允许站内 MAC 列表中的客户端访问拒绝：阻止来自站点 MAC 列表中的客户从注册 |
| 新增 | 输入您想要允许或拒绝的客户端的 MAC 地址 |

配置会话初始协议

账号配置

FWR9601 设备有 1 个电话接口，在注册之前，设备用户应该有一个由系统管理员或提供者配置的账号。有关更多信息，请参见下面一节。

The screenshot displays the configuration page for VoIP Account 1. The navigation tabs at the top include '状态', '网络', '无线2.4GHz', '无线5GHz', 'VoIP', '电话', '安全', '应用', and '管理'. The 'VoIP' tab is active, and '账号 1' is selected. Below the navigation, there are sub-tabs for '账号 1', 'SIP设置', and 'VoIP QoS'. The main content area is divided into three sections: '常规' (General), '基本设置' (Basic Settings), and '代理和注册' (Proxy and Registration). Under '基本设置', '账号使能' (Account Enabled) is set to '开启' (Enabled) and '非注册拨打模式' (Unregistered Call Mode) is set to '禁止' (Prohibit). Under '代理和注册', there are input fields for '注册服务器' (Registration Server), '代理服务器' (Proxy Server), and '备份代理服务器' (Backup Proxy Server), each with a corresponding port field set to '5060'. The '启动DHCP选项120服务器设置' (Start DHCP Option 120 Server Setting) is set to '禁止'. Under '用户信息' (User Information), there are input fields for '显示名称' (Display Name), '注册账户' (Registration Account), '认证名称' (Authentication Name), and '密码' (Password).

步骤

- 1.打开帐号的网页，如上图所示
- 2.将 SIP 服务器地址和 SIP 服务器端口号（从管理员或提供者）填充到代理服务器名称和代理端口参数中
- 3.将收到的管理员帐户明细填写到显示名称、电话号码和帐户详细信息
- 4.输入您收到的管理员的密码参数

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。

查看注册状态

要查看设备的 SIP 帐户状态，打开状态页面并查看注册状态的值，如下图所示，可以查看注册状态是否成功：

SIP 账号状态

SIP 账号状态

| | |
|----------------|---------|
| FXS 1 SIP 账号状态 | 注册失败 |
| 主服务器 | 0.0.0.0 |
| 备份服务器 | 0.0.0.0 |

拨打电话

打电话或分机号码

ATA和其他VOIP设备（例如，另一个ATA或者其他SIP产品）。

IP 直拨

ATA与模拟电话或者另一台VoIP设备，在不使用SIP代理的情况下相互交谈，两个电话之间可以建立VoIP呼叫。

1. ATA和其他有公共IP地址的VoIP设备（例如，另一个ATA或其他SIP产品）。
2. ATA和其他使用私有或公共IP地址的VoIP设备（例如，另一个ATA或其他SIP产品）的局域网下。
3. ATA和其他VoIP设备（例如，另一个ATA或其他SIP产品）可以通过一个使用公共的或私有IP地址的路由器连接。
4. IP直拨时，首先拿起模拟电话或打开模拟电话的扬声器，直接输入对方电话的IP地址，以“#”结束，以“*”代替“.”。

呼叫保持

当ATA上的模拟话机正在进行通话时：

1. 模拟话机按下“*77”可保持当前通话，之后你会听到拨号音，对方将听到保持音乐
2. ATA模拟话机用户可以继续输入电话号码拨打第三方电话
3. 再次按下“*77”，释放以前保持状态，并恢复之前的通话。

呼叫转移

盲转

盲目呼叫转移（Blind Transfer）指ATA作为电话转接的中间方，将接通的电话，在不询问目的方的情况下，直接转接到目的方。

1. 在通话过程中按下“*98”。当前通话被保持，你会听到拨号音，对方将听到保持音乐。
2. 拨打第二人的电话号码以“#结束”，电话被转接，ATA断开通话，听到忙音。

咨询转

咨询转移（Attended Transfer）指ATA作为电话转接的中间方，将接通的电话，在问询目的方后，转接到目的方。

1. 要转移当前接通的呼叫，首先在通话过程中按“*77”，当前通话被保持，你会听到拨号音，对方将听到保持音乐。
2. 拨打第二人的电话号码。
3. 与第二个人建立通话（并询问是否接听转接电话）。
4. 第二人若同意接听转接电话，则中间方按下“*98”，完成转移。中间方将从通话被断开。
5. 第二人若不同意接听转接电话，则与之通话结束后按“*77”，可继续在第一人通话。

呼叫等待

1. 在 VOIP->账号 页面下找到“增值业务”标签，开启“呼叫等待”功能（默认开启）。
2. 在通话过程中，当有其他电话打入时，可以听到一种特殊的停顿音。
3. 用户可以按下“*77”使正在通话的一方处于保持状态，来接通新来电，使用“*77”可以在两个会话之间切换。

三方会议

1. ATA发起会议通话，在通话过程中按下“*77”，当前通话被保持，你会听到拨号音，对方将听到保持音乐。
2. ATA拨打第二人的电话号码
3. 第二人应答呼叫后，ATA按“*88”，作为会议主持方开启电话会议，三方都将在参加同一电话会议。
4. 如果你（会议主持方）挂断，其他两方通话将被断开；如果一方首先挂断，你仍可以与另一方通话。

第 4 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：

- 登录
- 状态
- 网络和安全
- 无线
- SIP
- FXS1
- 安全
- 应用
- 存储
- 管理

登录

如图所示：



VoIP ... control panel

用户名

密码

步骤

1. 用一条以太网电缆把路由器的 LAN 端口连接到你的计算机
2. 打开您的 PC 和一个 Web 浏览器类型的 HTTP：输入设备 LAN 口 IP 192.168.1.1
3. 输入用户名和密码，点击“登录”进入网页
4. 检查是否正确登录

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：

The screenshot shows the 'VoIP ... control panel' interface. The '状态' (Status) tab is selected. Underneath, the '系统信息' (System Information) sub-tab is active. The '设备信息' (Device Information) section is expanded, displaying the following details:

| | |
|---------------|----------------------------|
| 设备名称 | FWR9601 |
| 网络(WAN) MAC地址 | 00:21:F2:10:01:7D |
| PC(LAN) MAC地址 | 00:21:F2:10:01:7C |
| 硬件版本 | V3.4 |
| Loader版本号 | V3.35(May 4 2017 17:41:36) |
| 软件版本 | V3.20(201801171912) |
| 序列号 | FVSN0096 |

内网主机信息

此页显示了连接设备 LAN 口的设备的信息。

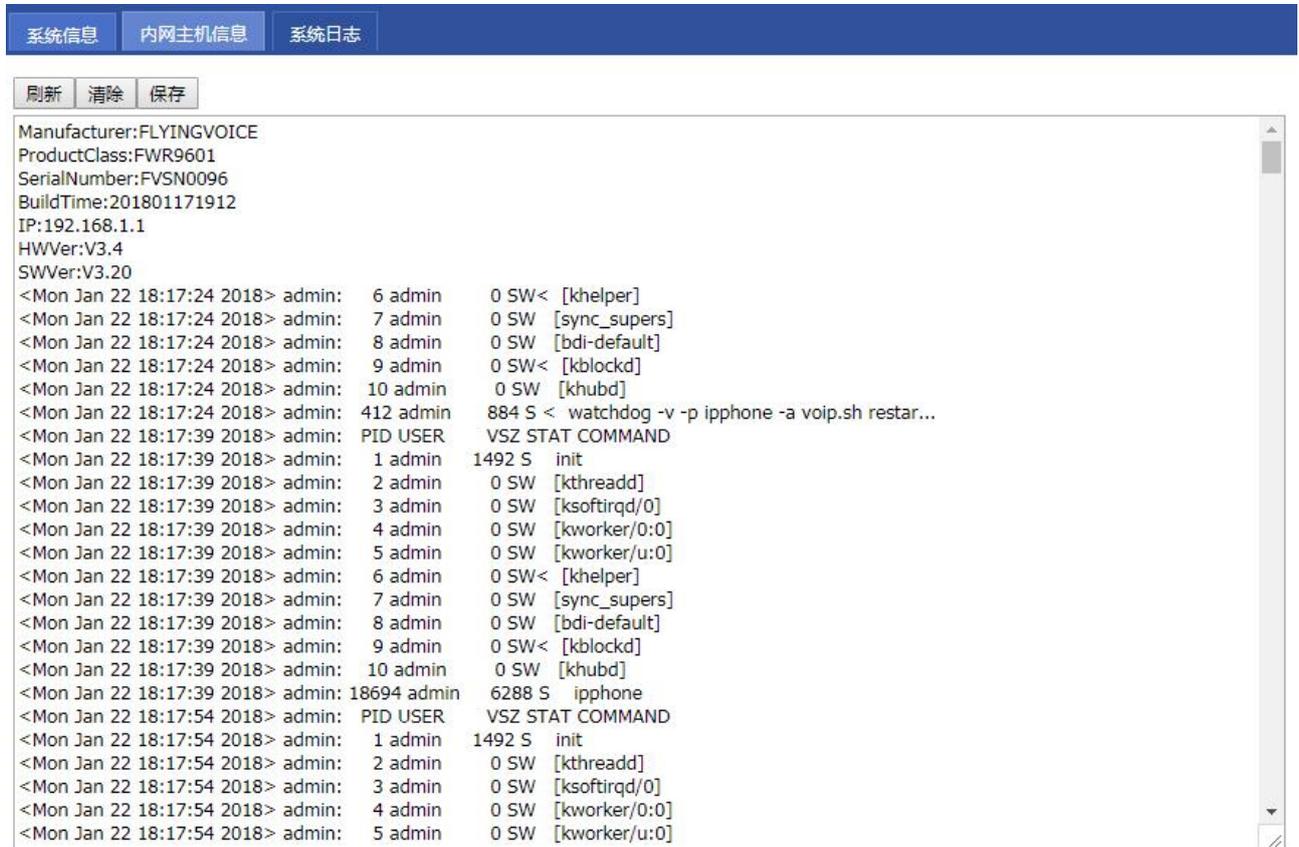
The screenshot shows the '内网主机信息' (Internal Network Host Information) section. It contains two tables:

| 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 | 192.168.1.84 | LAN2 | DHCP | 23:3:31 | SKY-20170519RRJ | 活跃 |

| MAC地址 | IPv6地址 | 租剩时间 |
|-------|--------|------|
|-------|--------|------|

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 FWR9202/FWR9601 的重要的配置信息。在该页面用户可以使用**清除**按钮删除全部日志，清除所有信息；使用**刷新**按钮刷新系统日志；使用**保存按钮**保存日志到本地电脑上，即可以导出日志。



The screenshot displays the system log management interface. At the top, there are three navigation tabs: "系统信息" (System Information), "内网主机信息" (Intranet Host Information), and "系统日志" (System Log), with "系统日志" being the active tab. Below the tabs are three action buttons: "刷新" (Refresh), "清除" (Clear), and "保存" (Save). The main area shows a scrollable log window with the following content:

```
Manufacturer:FLYINGVOICE
ProductClass:FWR9601
SerialNumber:FVSN0096
BuildTime:201801171912
IP:192.168.1.1
HWVer:V3.4
SWVer:V3.20
<Mon Jan 22 18:17:24 2018> admin: 6 admin 0 SW< [khelper]
<Mon Jan 22 18:17:24 2018> admin: 7 admin 0 SW [sync_supers]
<Mon Jan 22 18:17:24 2018> admin: 8 admin 0 SW [bdi-default]
<Mon Jan 22 18:17:24 2018> admin: 9 admin 0 SW< [kblockd]
<Mon Jan 22 18:17:24 2018> admin: 10 admin 0 SW [khubd]
<Mon Jan 22 18:17:24 2018> admin: 412 admin 884 S < watchdog -v -p ipphone -a voip.sh restar...
<Mon Jan 22 18:17:39 2018> admin: PID USER VSZ STAT COMMAND
<Mon Jan 22 18:17:39 2018> admin: 1 admin 1492 S init
<Mon Jan 22 18:17:39 2018> admin: 2 admin 0 SW [kthreadd]
<Mon Jan 22 18:17:39 2018> admin: 3 admin 0 SW [ksoftirqd/0]
<Mon Jan 22 18:17:39 2018> admin: 4 admin 0 SW [kworker/0:0]
<Mon Jan 22 18:17:39 2018> admin: 5 admin 0 SW [kworker/u:0]
<Mon Jan 22 18:17:39 2018> admin: 6 admin 0 SW< [khelper]
<Mon Jan 22 18:17:39 2018> admin: 7 admin 0 SW [sync_supers]
<Mon Jan 22 18:17:39 2018> admin: 8 admin 0 SW [bdi-default]
<Mon Jan 22 18:17:39 2018> admin: 9 admin 0 SW< [kblockd]
<Mon Jan 22 18:17:39 2018> admin: 10 admin 0 SW [khubd]
<Mon Jan 22 18:17:39 2018> admin: 18694 admin 6288 S ipphone
<Mon Jan 22 18:17:54 2018> admin: PID USER VSZ STAT COMMAND
<Mon Jan 22 18:17:54 2018> admin: 1 admin 1492 S init
<Mon Jan 22 18:17:54 2018> admin: 2 admin 0 SW [kthreadd]
<Mon Jan 22 18:17:54 2018> admin: 3 admin 0 SW [ksoftirqd/0]
<Mon Jan 22 18:17:54 2018> admin: 4 admin 0 SW [kworker/0:0]
<Mon Jan 22 18:17:54 2018> admin: 5 admin 0 SW [kworker/u:0]
```

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。

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。

| 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 | | | | | | | | | | |
| 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 | <input type="text"/> | | | | | | | | | |
| MAC地址克隆 | 禁止 ▼ | | | | | | | | | |
| NAT 使能 | 开启 ▼ | | | | | | | | | |
| VLAN 模式 | 禁止 ▼ | | | | | | | | | |
| VLAN ID | <input type="text" value="1"/> (1-4094) | | | | | | | | | |
| DNS模式 | 自动 ▼ | | | | | | | | | |
| 主DNS地址 | <input type="text"/> | | | | | | | | | |
| 从DNS地址 | <input type="text"/> | | | | | | | | | |
| DHCP | | | | | | | | | | |
| DHCP更新 | <input type="button" value="更新"/> | | | | | | | | | |
| DHCP 供应商(选项 60) | <input type="text" value="FLYINGVOICE-FWR9601"/> | | | | | | | | | |
| 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 |
|------|----|
|------|----|

| | |
|---------------|---|
| 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。 |

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 FWR9202/FWR9601 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。

The screenshot shows the router's configuration page for the Internet connection. The 'INTERNET' section is active, and the 'WAN' tab is selected. The 'INTERNET接入方式' (Internet Access Mode) is set to 'DHCP', which is highlighted with a red box. Other settings include: Connection Name: 1_MANAGEMENT_VOICE_INTERNET_R_VID, Service Mode: MANAGEMENT_VOICE_INTERNET, IP Protocol Version: IPv4, DHCP Server: (empty), MAC Address Cloning: 禁止, NAT: 开启, VLAN Mode: 禁止, VLAN ID: 1, DNS Mode: 自动, Main DNS Address: (empty), and Secondary DNS Address: (empty). A '删除此连接' (Delete this connection) button is visible in the top right corner.

| 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。 |

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。

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

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 style="width: 100%;" type="text"/> | |
| 从DNS地址 | <input style="width: 100%;" type="text"/> | |
| <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> PPPoE </div> <div style="margin-bottom: 5px;"> 用户名 <input style="width: 100%;" type="text"/> </div> <div style="margin-bottom: 5px;"> 密码 <input style="width: 100%;" type="password"/> </div> <div style="margin-bottom: 5px;"> 确认密码 <input style="width: 100%;" type="password"/> </div> <div style="margin-bottom: 5px;"> 服务名称 <input style="width: 100%;" type="text"/> </div> <div style="font-size: x-small; text-align: center;">空为自动检测</div> | | |

| 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。 |

桥接模式

在管理---工作模式中可设置多 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。

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

INTERNET

WAN

连接名称 1_MANAGEMENT_VOICE_INTERNET_R_VID ▼

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)

删除此连接

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 |
|------|----|
|------|----|

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。FWR8102 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 DHCP 报文 |
| 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

| | | | | | | | | | | |
|------|-----|----------|----------|----------|-----|------|-----|------|-----|------------|
| 状态 | 网络 | 无线2.4GHz | 无线5GHz | VoIP | 电话 | 安全 | 应用 | 管理 | | |
| 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 | | | | | | | | | | |

LAN口设置

LAN口设置

| | |
|-------------------|--|
| 本地IP地址 | <input type="text" value="192.168.1.1"/> |
| 子网掩码 | <input type="text" value="255.255.255.0"/> |
| DHCP服务器 | <input type="button" value="开启"/> |
| 地址池开始地址 | <input type="text" value="192.168.1.2"/> |
| 地址池结束地址 | <input type="text" value="192.168.1.254"/> |
| DNS模式 | <input type="button" value="自动"/> |
| 主DNS | <input type="text" value="192.168.1.1"/> |
| 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"/> |

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"/> | | |

DNS代理

| 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 |
| 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 侧网络 |

IPv6 设置

您可以在这里这些页面设置 IPv6 的相关信息：

IPv6 高级设置

开启或禁止 IPv6。

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



IPv6高级设置

IPv6使能

IPv6使能 开启 ▾

保存并应用 保存 取消 重启

IPv6 WAN

如图所示为 IPv6 WAN 相关信息：



IPv6 WAN设置

IPv6 WAN设置

连接类型 DHCPv6 ▾

DHCPv6获取地址方式 无状态 ▾

前缀分发 禁止 ▾

| 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，FWR9202/FWR9601 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 FWR8402 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 | fec0::1 | | | | | | | | | |
| IPv6前缀长度 | 64 (0-128) | | | | | | | | | |
| DHCPv6服务 | | | | | | | | | | |
| DHCPv6状态 | 禁止 ▾ | | | | | | | | | |
| DHCPv6模式 | 无状态 ▾ | | | | | | | | | |
| 域名 | | | | | | | | | | |
| Server首选 | 255 (0-255) | | | | | | | | | |
| 主DNS服务器地址 | | | | | | | | | | |
| 次DNS服务器地址 | | | | | | | | | | |
| 租约时间 | 86400 (0-86400秒) | | | | | | | | | |
| IPv6地址池 | [] - [] / [] | | | | | | | | | |
| 路由器通告 | | | | | | | | | | |
| 路由器通告 | 禁止 ▾ | | | | | | | | | |
| 通告间隔 | 30 (10-1800秒) | | | | | | | | | |
| RA管理标志 | 禁止 ▾ | | | | | | | | | |
| RA其它标志 | 开启 ▾ | | | | | | | | | |
| 前缀 | [] / [] | | | | | | | | | |
| 前缀有效时间 | 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，FWR9202/FWR9601 支持 PPTP 和 L2TP。

PPTP

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

VPN设置

管理

| | |
|------------|--|
| VPN使能 | <input type="text" value="PPTP"/> |
| 服务器IP | <input type="text"/> |
| 用户名 | <input type="text"/> |
| 密码 | <input type="password" value="....."/> |
| VPN 作为默认路由 | <input type="text" value="禁止"/> |
| 有状态MPPE | <input type="text" value="禁止"/> |
| 请求MPPE | <input type="text" value="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

VPN设置

管理

VPN使能 L2TP ▼

服务器IP

用户名

密码

L2TP 隧道名

L2TP 隧道密码

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 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：

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

高级设置

| 端口映射 | | | | |
|------|----|------|------|----|
| 编号 | 注解 | IP地址 | 端口范围 | 协议 |

删除已选择项
添加
编辑

端口映射

注解

IP地址

端口范围 -

协议 TCP&UDP ▼

(最大规则数为 32)

应用
取消

| 虚拟服务器 | | | | | |
|-------|----|------|------|------|----|
| 编号 | 注解 | IP地址 | 公共端口 | 私有端口 | 协议 |

删除已选择项
添加
编辑

虚拟服务器

注解

IP地址

公共端口

私有端口

协议 TCP&UDP ▼

(最大规则数为 32)

应用
取消

| 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 |

Vlan

在这里您可以配置 Vlan 相关信息：

| Port VLAN ID Configuration | | | | | |
|----------------------------|------|------|------|------|--|
| WAN | LAN1 | LAN2 | LAN3 | LAN4 | |
| 1 | 2 | 2 | 2 | 2 | |

| VLAN配置 | | | | | |
|---------------------------------------|-------|-------|-------|-------|-------|
| VLAN ID | 端口 | | | | |
| | WAN | LAN1 | LAN2 | LAN3 | LAN4 |
| <input checked="" type="checkbox"/> 1 | Untag | Unset | Unset | Unset | Unset |
| <input checked="" type="checkbox"/> 2 | Unset | Untag | Untag | Untag | Untag |

| 参数名称 | 描述 |
|-----------|--|
| Vlan 划分模式 | 在下拉列表中选择需要的模式，分为自动/自定义 |
| Vlan 配置 | 在下拉列表中选择需要的配置，分为 unset/Tagged/unTagged |

QoS

如图是 QoS 相关信息配置:

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

高级设置

QoS 配置

QoS 配置

启用QoS 禁止 ▼

上行带宽 (0-102400)kbit/s

下行带宽 (0-102400)kbit/s

算法 WFQ ▼

| 注解除 | 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 |
| 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

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

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 |

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：

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：

| 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：

| 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 | | | | | | | | | | |
| Nat最大连接数(512-8192) | | 4096 | | | | | | | | |
| Mss模式 | | <input checked="" type="radio"/> 指定 <input type="radio"/> 自动 | | | | | | | | |
| Mss值(1260-1460) | | 1440 | | | | | | | | |
| 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 |

无线 2.4GHz

基本设置

如图是无线的基本设置相关信息配置：

| 状态 | 网络 | 无线2.4GHz | 无线5GHz | VoIP | 电话 | 安全 | 应用 | 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 | <input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭 |
| 连接模式 | 无线接入点 |
| 网络模式 | 11b/g/n混合模式 |
| 无线网络名称 | FWR9601-10017C <input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 最大客户端数 16 |
| 无线网络名称1 | <input type="text"/> <input type="checkbox"/> 开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 最大客户端数 16 |
| 无线网络名称2 | <input type="text"/> <input type="checkbox"/> 开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 最大客户端数 16 |
| 无线网络名称3 | <input type="text"/> <input type="checkbox"/> 开启 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 隔离 最大客户端数 16 |
| 广播网络名(SSID) | <input checked="" 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 | 8C:88:2B:40:00:A0 |
| 频率(频道) | 自动侦测 |
| 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 type="radio"/> 20 <input checked="" 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 |
| 自动单区块确认 | <input type="radio"/> 禁止 <input checked="" type="radio"/> 开启 |
| 拒绝单区块确认要求 | <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 |
| HT LDPC | <input checked="" type="radio"/> 禁止 <input type="radio"/> 开启 |

| 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 |
| 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 启用: 使用单个块确认多个帧。 |
| 自动单一区确认 | 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:

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:

"FWR9601-10017C"

安全模式:

WPA

WPA算法: TKIP AES TKIPAES

通行口令:

私钥更新间隔: 秒 (0 ~ 86400)

访问策略

策略:

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) OPENWEP：WEP 加密的一种握手方式，是通过 WEP 密钥来进行加密：

SSID

选择SSID

SSID选择 FWR9601-10017C ▼

"FWR9601-10017C"

安全模式 OPENWEP ▼

有线等效加密(WEP)

默认密钥 WEP密钥1 ▼

| | | | | |
|-------|--------|------------------------------------|--------------------|----------------------|
| | WEP密钥1 | <input type="text" value="*****"/> | Hex ▼ | 64bit ▼ |
| | WEP密钥2 | <input type="text" value="*****"/> | Hex ▼ | 64bit ▼ |
| WEP密钥 | WEP密钥3 | <input type="text" value="*****"/> | Hex ▼ | 64bit ▼ |
| | WEP密钥4 | <input type="text" value="*****"/> | Hex ▼ | 64bit ▼ |

| 参数名称 | 描述 |
|--------|---|
| WEP 表示 | WEP 表示 Wired Equivalent Privacy，它是一种基本的加密方式。 |
| 默认密钥 | 用来选择 4 个 WEP 密钥中的一个，客户端网卡上的密钥设置也需与此对应 |
| WEP 密钥 | 设置 WEP 密钥。选择 64 位密钥需输入 Hex 字符 10 个，或 ASCII 码字符 5 个；选择 128 位密钥需输入 Hex 字符 26 个，或 ASCII 码字符 13 个 |

(2) WPA-PSK，路由器将采用基于共享密钥的 WPA 模式：

SSID

选择SSID

SSID选择 FWR9601-10017C ▼

"FWR9601-10017C"

安全模式 WPA-PSK ▼

WPA

WPA算法 TKIP AES TKIPAES

通行口令

私钥更新间隔 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 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 |

(3) WPA2-PSK，路由器将采用基于共享密钥的 WPA2 模式：

| SSID | |
|------------------|---|
| 选择SSID | |
| SSID选择 | FWR9601-10017C ▼ |
| "FWR9601-10017C" | |
| 安全模式 | WPA2-PSK ▼ |
| 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/AES11N 模式不支持 TKIP 算法 |
| 通行口令 | 设置 WPA-PSK/WPA2-PSK 安全密码 |
| 私钥更新间隔 | 置密钥定时更新周期，默认为 3600s |

(4) 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。

| SSID | |
|------------------|---|
| 选择SSID | |
| SSID选择 | FWR9601-10017C ▼ |
| "FWR9601-10017C" | |
| 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: (最大规则数为 64)

保存并应用
保存
取消
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。

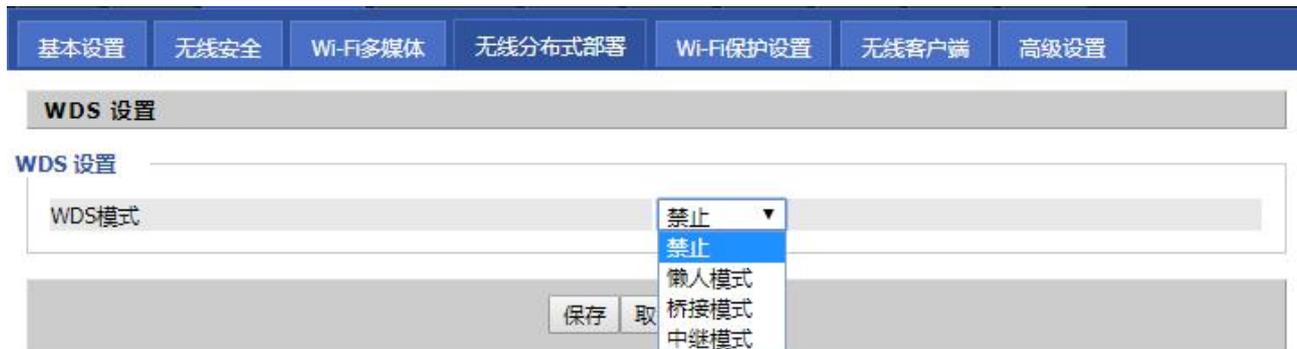
| WMM参数 | | | | | | |
|-------|--------|--------|--------|------|--------------------------|--------------------------|
| | 仲裁帧间隙数 | 最小竞争窗口 | 最大竞争窗口 | 传输机会 | 强制接入控制 | 响应规则 |
| 尽力而为流 | 3 | 15 ▼ | 63 ▼ | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| 背景流 | 7 | 15 ▼ | 1023 ▼ | 0 | <input type="checkbox"/>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

WDS 代表无线分配系统，使 WDS 接入点互连，扩展无线网络。FWR9202/FWR9601 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。



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。



| 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)

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：

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 1 |
| FWR9601-10017C | 8C:88:2B:40:00:A0 |

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 |
|-------|----|------|--------|------|----|-------|------|

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 | US (United States) ▼ | | | | | |
| 支持的频道 | Ch1~11 ▼ | | | | | |
| 载波检测 | <input type="radio"/> 开启 | | <input checked="" type="radio"/> 禁止 | | | |
| Wi-Fi多媒体 (WMM) | | | | | | |
| Wi-Fi多媒体能力 | | | | | | |
| 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 | | | |

| 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](#)。

VOIP

账号 1

请参考[配置会话初始协议](#)

设置您的 VoIP 服务提供商提供基本的信息，如电话号码、帐号、密码、SIP 代理等。

| 账号 1 | SIP设置 | VoIP QoS | |
|------------------|-------------------------------------|-----------|-------------------------------------|
| 常规 | | | |
| 基本设置 | | | |
| 账号使能 | <input type="button" value="开启 ▼"/> | 非注册拨打模式 | <input type="button" value="禁止 ▼"/> |
| 代理和注册 | | | |
| 注册服务器 | <input type="text"/> | 注册服务器端口 | <input type="text" value="5060"/> |
| 代理服务器 | <input type="text"/> | 代理服务器端口 | <input type="text" value="5060"/> |
| 备份代理服务器 | <input type="text"/> | 备份代理服务器端口 | <input type="text" value="5060"/> |
| 启动DHCP选项120服务器设置 | <input type="button" value="禁止 ▼"/> | | |
| 用户信息 | | | |
| 显示名称 | <input type="text"/> | 注册账户 | <input type="text"/> |
| 认证名称 | <input type="text"/> | 密码 | <input type="text"/> |

| 参数名称 | 描述 |
|-----------|-------------------------------|
| 账号使能 | 是否启用相应的 Line |
| 注册服务器 | SIP 服务器的域名或 IP |
| 注册服务器端口 | SIP 服务器支持 VoIP 服务的端口，默认是 5060 |
| 代理服务器 | 代理服务器 IP 或域名 |
| 代理服务器端口 | 代理服务器的服务端口 |
| 备份代理服务器 | 备份代理服务器 |
| 备份代理服务器端口 | 备份代理服务器端口 |
| 显示名称 | 这个字符将显示在液晶显示屏 |
| 注册账户 | SIP 服务器提供的电话号码 |
| 认证名称 | SIP 服务器提供的 SIP 帐户 |

音频设置

选择音频编码格式：

| 音频配置 | | | |
|-----------|------------|----------------------------|-----------|
| 编码设置 | | | |
| 编码方式1 | G.711U ▼ | 编码方式2 | G.711A ▼ |
| 编码方式3 | G.729 ▼ | 编码方式4 | G.722 ▼ |
| 编码方式5 | G.723 ▼ | 编码方式6 | G726-32 ▼ |
| 编码方式7 | iLBC ▼ | | |
| G.723编码速率 | 5.3k bps ▼ | 打包周期(毫秒) | 20 ▼ |
| 静音抑制 | 禁止 ▼ | 回声抵消 | 开启 ▼ |
| 自动增益控制 | 开启 ▼ | 使用第一个匹配的语音编码(在2000K SDP 中) | 禁止 ▼ |
| 编码优先策略 | 远端 ▼ | 打包周期以对端为准 | 禁止 ▼ |

| 参数名称 | 描述 |
|--------------------------|--|
| 编码方式 1, 2, 3, 4, 5, 6, 7 | 从 G.711A、G.711U、G.722、G.729 和 G.723 五种编码方式中选择相应的编码方式 |
| G.723 编码速率 | 选择 G.723 的编码速率，有 5.3kbps 和 6.3kbps 两种 |
| 打包周期 | 设置 RTP 的打包周期，默认的配置为 20ms |
| 静音抑制 | 是否静音 |
| 回声抵消 | 是否启用回音消除，默认的是启用 |
| 自动增益控制 | 是否开启自动增益控制，自动增益控制是使放大电路的增益自动地随信号强度而调整的自动控制方法 |
| 使用第一个匹配的语音编码 | 是否开启使用第一个匹配的语音编码 |
| 编码优先策略 | 编码优先策略包括本地和远端 |
| 打包周期以对端为准 | 打包周期是否以对端为主 |

辅助功能

增值业务

增值业务

| | | | |
|--------------------|---------------------------------------|--------|---------------------------------------|
| 呼叫等待 | 开启 ▼ | 热线呼叫号码 | <input type="text"/> |
| MWI使能 | 开启 ▼ | 语音信箱号码 | <input type="text"/> |
| MWI订阅使能 | 禁止 ▼ | | |
| 去电阻止密码 | <input type="password" value="...."/> | 去电使能密码 | <input type="password" value="...."/> |
| Emergency Call Num | <input type="text"/> | | |

| 参数名称 | 描述 |
|----------|---|
| 呼叫等待 | 是否启用呼叫等待 |
| 热线呼叫号码 | 填入热线号码。用户设置成功后，摘机，立刻会自动地拨出该热线号码 |
| MWI 使能 | 是否启用 MWI(信息等待指示)，若用户需要使用语音邮箱，请启用该功能 |
| 语音信箱号码 | 填入 SIP 服务商提供的语音邮箱的特征码，以 Elatix 平台为例，其语音邮箱的特征码为*97 |
| MWI 订阅使能 | 是否启用 MWI 的订阅功能 |

高级设置

高级

SIP高级设置

| | | | |
|-------------------|------------|------------------|----------|
| 域名格式 | 开启 ▾ | 携带端口信息 | 禁止 ▾ |
| 本地SIP端口 | 54195 | DTMF模式设置 | Inband ▾ |
| RFC2833载荷类型(>=96) | 101 | 注册刷新时间(秒) | 3600 |
| 来电显示头域 | FROM ▾ | 移除上次注册消息使能 | 开启 ▾ |
| 会话刷新时间(秒) | 0 | 刷新 | UAC ▾ |
| SIP 100REL 使能 | 禁止 ▾ | SIP OPTIONS使能 | 禁止 ▾ |
| 初始注册携带认证信息 | 禁止 ▾ | 呼叫等待回应182 | 禁止 ▾ |
| NAT保活间隔(10-60秒) | 15 | 匿名呼叫 | 禁止 ▾ |
| 拒绝匿名呼叫 | 禁止 ▾ | Proxy DNS 类型 | A Type ▾ |
| 在会话中使用OB代理 | 禁止 ▾ | 完整注册 | 禁止 ▾ |
| 注册订阅使能 | 禁止 ▾ | 注册订阅时间(秒) | 0 |
| 拨号前缀 | | 对端用户类型 | Phone ▾ |
| 呼叫保持方法 | ReINVITE ▾ | 请求用户检查 | 开启 ▾ |
| 仅接受来自服务器的请求 | 禁止 ▾ | 服务器地址 | |
| SIP Received 检测 | 禁止 ▾ | VPN | 禁止 ▾ |
| SIP 加密方式 | 禁止 ▾ | RTP 加密方式 | 禁止 ▾ |
| 国家码 | | 移除国家码使能 | 禁止 ▾ |
| Tel URL | 禁止 ▾ | 使用随机SIP端口 | 开启 ▾ |
| 最小随机SIP端口 | 50000 | 最大随机SIP端口 | 60000 |
| 优选主服务器 | 禁止 ▾ | 呼叫保持Inactive属性使能 | 禁止 ▾ |
| BLF List URI | | BLF Pickup Code | |
| 去除所有绑定 | 禁止 ▾ | VAD&CNG | 禁止 ▾ |

RTP高级设置

| | | | |
|---------|----------------|---------|-------|
| 最小RTP端口 | 0 (0 为自动选择) | 最大RTP端口 | 50000 |
|---------|----------------|---------|-------|

保存并应用 保存 取消 重启

| 参数名称 | 描述 |
|--------------------|--|
| 域名格式 | 是否在 SIP URI 中启用域名识别功能 |
| 携带端口信息 | 是否携带 SIP URI 的端口信息 |
| 本地 SIP 端口 | SIP 协议的本地端口号 |
| DTMF 模式设置 | 选择二次拨号的方式，可选项目有 In-band，RFC2833 和 SIP Info. |
| RFC2833 载荷类型(>=96) | 用户可使用默认设置 |
| 注册刷新时间 | 两个正常的注册消息之间的时间间隔。用户可以使用默认设置。 |
| RTP 端口 | 设置发送 RTP 的端口；如果设置为“0”，IP 电话将选择一个空闲的端口发送 RTP |
| 来电显示头域 | 启用时，将发送一个未注册的消息在注册前，禁用时，不会被发送未注册的消息在注册之前；应根据不同的服务器要求进行设置 |
| 移除上次注册消息使能 | 是否移除上次注册消息 |
| 会话刷新时间(秒) | 两个会话之间的间隔时间，用户可使用默认设置 |
| 刷新 | 从 UAC 和 UAS 中选择刷新 |
| SIP 100REL 使能 | 如果启用此选项，IP 电话将发送 SIP- OPTION 到服务器，而不是 |

| | |
|--------------------|---|
| | 定期发送 Hello 报文。发送的时间间隔为” NAT 保活间隔” 参数设置的参数。 |
| SIP OPTIONS 使能 | 是否开启 SIP OPTION 功能 |
| 初始注册携带认证信息 | 注册时是否携带认证信息 |
| 呼叫等待回应 182 | 呼叫等待时是否允许发送 182 |
| NAT 保活间隔 (10-60 秒) | 发送空包的时间间隔 |
| 匿名呼叫 | 是否启用匿名呼叫 |
| 拒绝匿名呼叫 | 是否启用匿名来电的阻拦 |
| Proxy DNS 类型 | 设置 DNS 服务器类型, 可选项目有 A 类型, DNS SRV 和自动 |
| 在会话中使用 OB 代理 | 是否在对话中使用 OB 代理 |
| 完整注册 | 是否启用完整注册 |
| 注册订阅使能 | 启用时将在注册消息后发送订阅消息; 禁用时不发送订阅消息 |
| 注册订阅时间(秒) | |
| 拨号前缀 | 拨号前加的前缀 |
| 对端用户类型 | 对端用户是 IP 还是 Phone |
| 呼叫保持方法 | 呼叫保持是 REINVITE 还是 INFO |
| 请求用户检查 | 是否允许请求用户检查 |
| 仅接受来自服务器的请求 | 如果开启, 将只接受来自服务器的请求, 不接受别的请求 |
| 服务器地址 | SIP 服务器的地址 |
| SIP Received 检测 | 是否允许 SIP 接收检测 |
| VPN | 是否启用 VPN |
| SIP 加密方式 | 是否允许 SIP 报文加密 |
| RTP 加密方式 | 是否允许 RTP 报文加密 |
| 国家码 | 国家编码 |
| 移除国家码使能 | 是否允许移除国家编码 |
| Tel URL | 是否开启 Tel URL |
| 使用随机 SIP 端口 | 是否使用最小随机端口 |
| 最小随机 SIP 端口 | SIP 的最小随机端口 |
| 最大随机 SIP 端口 | SIP 的最大随机端口 |
| 优选主服务器 | 是否启用优选主服务器 |
| 呼叫保持 Inactive 属性使能 | 是否使能呼叫保持 inactive 属性 |
| BLF List URL | |
| BLF PickUp Code | |
| 去除所有绑定 | 是否去除所有绑定 |
| VAD&CNG | 是否启用 VAD&CNG |
| 最小 RTP 端口 | RTP 的最小端口 |
| 最大 RTP 端口 | RTP 的最大端口 |
| 保存并应用 | |
| 保存 | 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。 |
| 取消 | 点击取消变更 |
| 重启 | 点击重新启动 |

SIP 设置

| 账号 1 | SIP设置 | VoIP QoS | |
|---------------|-------------------------|--------------|----------|
| SIP参数 | | | |
| SIP参数 | | | |
| SIP T1 | 500 毫秒 | 最大跳数 | 70 |
| SIP用户代理头域名称 | | 最大认证失败次数 | 2 |
| 注册失败再次注册间隔 | 30 秒 | 注册失败再次注册长间隔 | 1200 秒 |
| 标记所有AVT包 | 开启 ▾ | RFC 2543呼叫保持 | 开启 ▾ |
| SRTP | 禁止 ▾ | SRTP 不加密 | AES_CM ▾ |
| 服务类型 | 通用 ▾ | DNS刷新周期 | 0 秒 |
| 响应码处理 | | | |
| 重新注册处理的响应码 | | | |
| NAT 穿越 | | | |
| NAT 穿越 | | | |
| NAT 穿越 | 禁止 ▾ | STUN 服务地址 | |
| NAT 刷新间隔(秒) | 60 | STUN 服务端口 | 3478 |
| 参数名称 | 描述 | | |
| SIP T1 | 默认值为 500 | | |
| SIP 用户代理头域名称 | 输入 SIP User Agent 头域 | | |
| 最大跳数 | 修改最大跳数值，默认为 70 | | |
| 最大认证失败次数 | 修改认证失败次数，默认值为 2 | | |
| 注册失败再次注册间隔 | 注册失败再次注册间隔时间，默认值为 30 | | |
| 注册失败再次注册长间隔 | 注册失败再次注册长间隔时间默认 1200 | | |
| 标记所有 AVT 包 | 默认使能开启 | | |
| REC 2543 呼叫保持 | 默认使能开启 | | |
| SRTP | 默认使能禁止 | | |
| SRTP 不加密 | 支持 AES_CM 和 ARIA_CM | | |
| 服务类型 | 默认通用 | | |
| DNS 刷新周期 | 修改 DNS 刷新时间，默认值 0 | | |
| 传输类型 | 传输类型默认为 UDP | | |
| NAT 穿越 | 是否启用 NAT 模式，或选择 STUN 穿透 | | |
| STUN 服务器地址 | STUN 服务器 IP 地址 | | |
| NAT 刷新时间 | 刷新间隔 | | |
| STUN 服务端口 | STUN 端口，默认为 3478 | | |

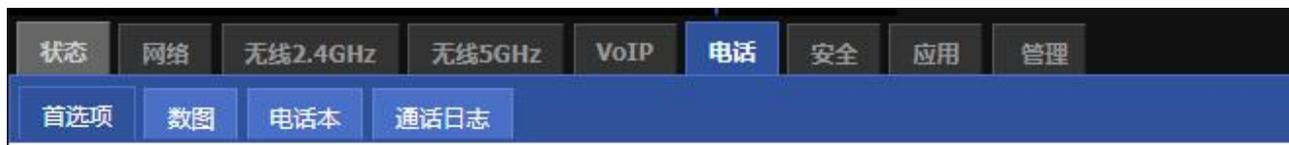
VoIP QoS

QoS 服务可以提高语音应用的质量。默认值为 46，可以设置值的范围是 0~63。

| 账号 1 | SIP设置 | VoIP QoS |
|---|---------------------------------|----------|
| QoS 设置 | | |
| 第三层QoS | | |
| SIP QoS(0-63) | <input type="text" value="46"/> | |
| RTP QoS(0-63) | <input type="text" value="46"/> | |
| <input type="button" value="保存"/> <input type="button" value="取消"/> <input type="button" value="重启"/> | | |

电话

此页面用户可以配置音量、呼叫转移、拨号计划、电话簿等参数。



首选项

音量设置

音量设置

| | | | |
|---------------|-----|------------------------|------|
| 输入音量 | 5 ▼ | 输出音量 | 5 ▼ |
| dtmf音量(0~-45) | -19 | 扬声器音量 | 5 ▼ |
| 免提输入增益 | 5 ▼ | Speakerphone Mic Boost | 禁止 ▼ |
| 铃声音量 | 5 ▼ | | |

| 参数名称 | 描述 |
|------------------------|---------------------|
| 输入音量 | 调整手柄 MIC 的音量输入大小。 |
| 输出音量 | 调整手柄输出的音量大小。 |
| Dtmf 音量(0-45) | 设置 DTMF 的音量 |
| 免提输入增益 | 调整外置 MIC 的音量输入大小。 |
| 扬声器音量 | 调整外置喇叭音量大小。 |
| 铃声音量 | 调整振铃的音量大小。 |
| Speakerphone Mic Boost | 是否将 MIC 的音量放大 20db。 |

区域铃声设置

区域铃声设置

| | | | |
|-----------------|----------------------|-------------------|-----|
| 铃声标准 | 中国 ▼ | | |
| 拨号音 | <input type="text"/> | | |
| 忙音 | <input type="text"/> | | |
| 催挂音 | <input type="text"/> | | |
| 回铃音 | <input type="text"/> | | |
| 呼叫等待音 | <input type="text"/> | | |
| 振铃音 | <input type="text"/> | | |
| 最小抖动延时(0-600毫秒) | 20 | 最大抖动延时(20-1000毫秒) | 160 |
| 振铃时间(10-300秒) | 60 | | |

| 参数名称 | 描述 |
|-------------|---|
| 铃声标准 | 选择音调类型。 |
| 拨号音 | 拨号音音调。 |
| 忙音 | 忙音音调。 |
| 催挂音 | 挂机警告音音调。 |
| 回铃音 | 回铃音音调。 |
| 呼叫等待音 | 呼叫等待音音调。 |
| 最小抖动延时(ms) | jitter delay 的最小值，电话的 jitter 采用的是自适应机制。 |
| 最大抖动延时(ms): | jitter delay 的最大值，电话的 jitter 采用的是自适应机制。 |
| 振铃时间 (Sec): | 振铃时间。 |

Miscellaneous

Miscellaneous

| | | | |
|--------------|------|----------------|------|
| 自动应答 | 禁止 ▼ | 通过CallINFO自动应答 | 禁止 ▼ |
| 自动回答延时时间 | 0 | | |
| 拨号超时(秒) | 5 | 快拨键 | # ▼ |
| 自动 Hookon 模式 | 开启 ▼ | 首选连接耳机 | 禁止 ▼ |
| ICMP Ping | 禁止 ▼ | 特殊字符转义 | 禁止 ▼ |
| 背光灯激活时间 (秒) | 15 ▼ | 话机锁 | 禁止 ▼ |
| Hook Disable | 禁止 ▼ | | |

| 参数名称 | 描述 |
|------------------|--|
| 自动应答 | 是否启用自动应答，若启用电话自动接听电话。 |
| 通过 CallINFO 自动应答 | 是否启用 CallINFO 下的自动应答。 |
| 自动回答延时时间 | |
| 拨号超时 | 电话拨号后多长时间听到拨号音。 |
| 快拨键 | 使用“#”、“*”做快速拨号，或者禁用。 |
| ICMP Ping | 是否启用 ICMP Ping。 若启用，电话每隔间隔时间会 ping SIP 服务器；否则会发“hello”的空包给 SIP 服务器。 |
| 特殊字符转义 | 使能开启或禁止，默认禁止。 |

数图

首选项
数图
电话本
通话日志

数图

通用

数图 禁止 ▼

未匹配策略 接受 ▼

| 编号 | 账号 | 数图 | 功能 | 上移 | 下移 | |
|----|-----|-----|----|----|----|---|
| 1 | 账号1 | cio | 阻止 | ▲ | ▼ | ■ |

账号 账号1 ▼

数图

功能 阻止 ▼

确定
取消

| 参数名称 | 描述 |
|------|--|
| 数图 | 开启/禁止拨号规则 |
| FXS | 设置 line |
| 树图 | 输入用于匹配输入编号的顺序 语法请参考以下拨号方案语法 |
| 功能 | 从拒绝和拨出选择拨号计划模式 拒绝意味着路由器将拒绝匹配的号码，而拨出意味着路由器将拨出匹配的号码 |
| 上移 | 将拨号计划上移到列表中 |
| 下移 | 将拨号计划下移到列表中 |

添加一个树图步骤：

1. 开启树图
2. 单击添加按钮和配置表
3. 填写参数的值
4. 按确认按钮结束配置

数图规则：

| No. | 字符 | 描述 |
|-----|-------------------------|-------------------|
| 1 | 0 1 2 3 4 5 6 7 8 9 * # | 合法字符 |
| 2 | x | 小写字母 x 匹配任何一个合法字符 |

| | | |
|---|----------------------|--|
| 3 | [sequence] | 匹配一个序列 例如： ◆ [0-9]: 匹配数字 0 到 9 中的任何一个 ◆ [23-5*]: 匹配字符 2 或 3 或 4 或 5 或* |
| 4 | x. | 匹配 x, xx, xxx, xxxx 等等 例如：“01.” 可以匹配“0”，“01”，“011”……“011111……” |
| 5 | <dialed:substituted> | 替换 例如： <#:23%>xx<#:23%>，输入为#56#时，输出为23%5623% |
| 6 | x, y | 输入“x”后会有拨号音，输入“y”后拨号音结束 例如<5, :><:241333>8101，输入为58101，输出为2413338101。此外 FWR9601 输入 5 后将会有拨号音，在拨 8 后停止 |
| 7 | T | 设定延迟时间。FWR9601 将会在 2 秒后拨出有效号码 |

电话本

电话本上传与下载

首选项
数图
电话本
通话日志

电话本上传与下载

本地文件 选择文件 未选择任何文件

上传 XML 下载 XML

远程电话本下载 (xml格式)

间隔时间 (秒)

URL 保存

黑名单上传与下载

黑名单上传与下载

本地文件 选择文件 未选择任何文件

上传 CSV 下载 CSV

电话本，远程电话本，黑名单上传下载步骤：

1. 点击 **选择文件**，选择本地存储的电话本。
2. 选择完毕后，web 上会出现提示



3. 点击 **上传 XML**，开始上传

4. 点击 **下载 XML**，可直接将电话本下载到本地电脑上。

远程电话本下载 (xml 格式)

远程电话本下载 (xml格式)

间隔时间 (秒)

URL **保存**

| 描述 | |
|---------|--------------|
| 远程电话本下载 | |
| 间隔时间 | 下载电话本时间间隔 |
| URL | 填入下载所需要的 URL |

黑名单

在这个页面中，用户可以上传或下载黑名单文件，并可以添加或删除或编辑黑名单一个接一个。

| 黑名单 | | | |
|-----|----|----|--|
| 编号 | 名称 | 号码 | |
| | | | |

名称

号码

确定 **取消**

黑名单添加删除有两种方式：

第一种：单击添加添加一个黑名单，输入名称和电话号码，单击确定确认并单击取消去取消

第二种：点击 **选择文件** 选择黑名单文件然后点击 **上传 CSV** 上传到 FWR9601； 点击 **下载 CSV** 保存黑名单并下载到你的电脑

通话日志

在该页面用户可以查看重播列表(呼出电话)、已接来电和未接来电。

重拨列表

| 重拨列表 | | | | |
|------|-------|-------------|----------|--------------------------|
| 编号 | 号码 | 开始时间 | 通话时长 | <input type="checkbox"/> |
| 1 | 63625 | 09/22 11:21 | 00:00:01 | <input type="checkbox"/> |
| 2 | 626 | 09/22 11:21 | 00:00:27 | <input type="checkbox"/> |
| 3 | 626 | 09/22 11:22 | 00:00:04 | <input type="checkbox"/> |

已接电话

| 已接电话 | | | | |
|------|-----|-------------|----------|--------------------------|
| 编号 | 号码 | 开始时间 | 通话时长 | <input type="checkbox"/> |
| 1 | 625 | 09/22 11:21 | 00:00:28 | <input type="checkbox"/> |
| 2 | 626 | 09/22 11:22 | 00:00:13 | <input type="checkbox"/> |

未接电话

| 未接电话 | | | | |
|------|-----|-------------|----------|--------------------------|
| 编号 | 号码 | 开始时间 | 通话时长 | <input type="checkbox"/> |
| 1 | 625 | 09/22 11:22 | 00:00:00 | <input type="checkbox"/> |

安全

在该页面可以进行过滤设置、内容过滤

MAC/IP/Port/ACL

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 白名单 ▼

不匹配任何规则的数据包将被 丢弃

MAC/IP/Port 过滤设置

传输类型 INPUT ▼

Mac 地址

目的 IP 地址

源 IP 地址

协议 无 ▼

目的 Port 区间 -

源 Port 区间 -

行为 接收 ▼

注解

(最大规则数为 32)

MAC/IP/Port 过滤列表

| 编号 | 传输类型 | 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 |
|---------------|------|--------|----------|---------|----|------------|-----------|----|----|
| WAN: 其他的会被丢弃. | | | | | | | | | |

| 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

[帮助](#)

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 |
|----|-----|
| 删除 | 取消 |

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 |
|----|-----|
| 删除 | 取消 |

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

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。

| 高级Nat | | UPnP | IGMP |
|--|------------|------|------|
| UPnP | | | |
| UPnP 配置 | | | |
| UPnP | 开启 ▼ | | |
| <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 | | |
| 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。

| 高级Nat | | UPnP | IGMP |
|--|--------------|------|------|
| IGMP | | | |
| IGMP 配置 | | | |
| IGMP 代理 | 禁止 ▼ | | |
| IGMP Snooping enable | 禁止 ▼ | | |
| <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 | | |
| IGMP 代理 | 是否开启 IGMP 功能 | | |

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

保存配置文件

| 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 |

管理员设置

| 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 ▼ |
| Web端口 | 80 |
| 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 | FWR9601 |

| 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 |

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 - 10 - 26 . 17 : 27 : 39 |
| 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 |

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 ▾ |
| 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 |

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

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

升级步骤：

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

| 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 | | | | | |
| 开启 | 禁止 ▼ | | | | | | | |
| 无线名称 | FWR9601-10017C ▼ | | | | | | | |
| 工作模式 | 每天 ▼ | | | | | | | |
| wifi工作周期 | 00 ▼ : 00 ▼ -- 00 ▼ : 00 ▼ | | | | | | | |
| 应用 | | 取消 | | | | | | |
| 定时重启 | | | | | | | | |
| 定时重启 | 禁止 ▼ | | | | | | | |
| 工作模式 | 每天 ▼ | | | | | | | |
| 时间 | 00 ▼ : 00 ▼ | | | | | | | |
| 重启PPPoE | | | | | | | | |
| 重启PPPoE | 禁止 ▼ | | | | | | | |
| 工作模式 | 每天 ▼ | | | | | | | |
| 时间 | 00 ▼ : 00 ▼ | | | | | | | |
| 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/没天 | | | | | | | |
| 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 | | | | | | | |

自动跟新（Provision）

| Provision | |
|-----------------|--|
| 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 | 开启 ▾ |
| 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，G201N4 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 IP542N 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 |
| 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，FWR8102 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

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 |

保存并应用
保存
取消
重启

| 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 |

Tr069

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。



| TR069 设置 | |
|-------------|--|
| ACS | |
| TR069 使能 | 开启 ▾ |
| CWMP | 开启 ▾ |
| ACS URL | http://acs1.flyingvoice.net:8080/tr069 |
| 用户名 | FVSN0096 |
| 密码 | •••••••• |
| 定期通知启用 | 开启 ▾ |
| 定期通知时间间隔(秒) | 99817 |
| 连接请求 | |
| 用户名 | FWR9601 |
| 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。

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。

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

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

Traceroute 测试

IP 地址或主机名

广域网连接

工作模式

设备分为高级模式和基本模式，用户可再此选择自己所需要的工作模式

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

工作模式设置

工作模式设置

工作模式

第 5 章 故障排除

本章内容包含：

- 接通电源无反应
- 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，密码恢复成 `admin`。

如果您选择出厂默认，您将返回到原始出厂设置的电话，将删除所有当前的设置，包括系统日志和通话记录。