



三汇 **UMG** 系列网关

Uniway6000

用户手册

Version 2.0.0

杭 州 三 汇 信 息 工 程 有 限 公 司

www.synway.cn

目 录

目 录	i
版权申明	iii
版本修订记录	iv
第 1 章 产品介绍	1
1.1 应用场景图	1
1.2 功能列表	1
1.3 硬件描述	2
1.3.1 网关外观及接口说明	2
1.3.2 网关硬件架构	4
1.4 告警信息说明	5
第 2 章 基本使用	6
第 3 章 WEB 配置	7
3.1 登录系统	7
3.2 运行信息	8
3.2.1 系统信息	8
3.2.2 子板状态	10
3.2.3 告警信息	11
3.3 网关配置	11
3.3.1 子板网关管理	12
3.3.2 子板配置信息	12
3.3.3 热备份设置	12
3.4 子板组	13
3.5 路由设置	15
3.5.1 IP to TEL/PSTN 路由	15
3.5.2 SIP 中继	17
3.6 系统工具	17
3.6.1 网络设置	19
3.6.2 管理参数	21
3.6.3 IP 路由表	23
3.6.4 访问控制	24
3.6.5 DDOS 设置	24
3.6.6 集中管理	26
3.6.7 配置文件	27
3.6.8 信令抓包	28
3.6.9 呼叫跟踪	29
3.6.10 Action URL	29
3.6.11 PING 测试	30
3.6.12 TRACERT 测试	31
3.6.13 修改记录	32
3.6.14 备份载入	33
3.6.15 恢复出厂	33
3.6.16 软件升级	34
3.6.17 用户管理	34
3.6.18 更改口令	35

3.6.19 重启网关.....	36
附录 A 主要技术/性能参数.....	37
附录 B 常见问题	38
附录 C 技术/销售支持.....	39

版权申明

本文档版权属杭州三汇信息工程有限公司所有。

杭州三汇信息工程有限公司保留对此文件进行修改而不另行通知之权利。

杭州三汇信息工程有限公司承诺所提供的信息为正确且可靠，但并不保证本文件绝无错误。

请在使用本产品前，自行确定所使用的相关技术文件及规格为最新有效之版本。若因贵公司使用本公司之文件或产品，而需要第三方之产品、专利或者著作等与其配合时，则应由贵公司负责取得第三方同意及授权。关于上述同意及授权，非属本公司应为保证之责任。

版本修订记录

版本号	发布日期	修订内容
Version 2.0.0	2024.12	新创建此文档。

请访问我们的网站（www.synway.cn）以获取该文档的最新版本。

第1章 产品介绍

欢迎使用三汇 UMG 系列网关产品（以下简称 UMG 网关）。UMG 网关融合了模拟和数字两种子板，既可以连接传统电话机、传真机，也可以连接 PSTN 和企业交换机，以及无线集群、调音台，实现模拟网关和数字网关的多种功能，为大容量 IP 呼叫中心和多分支机构提供功能强大、稳定可靠和高性价比的 VoIP 解决方案。

1.1 应用场景图

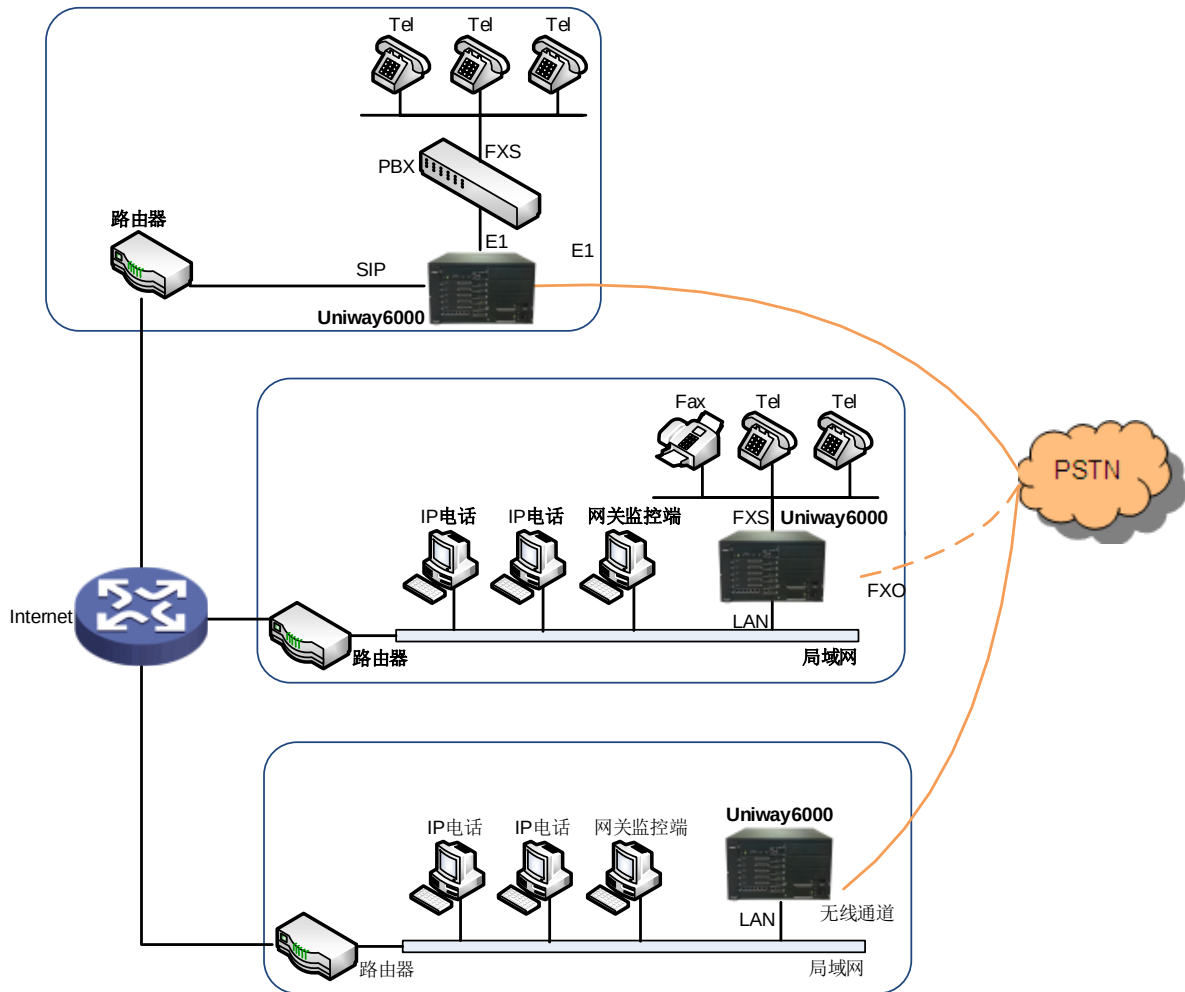


图 1-1 联合网关应用场景图

1.2 功能列表

基本功能	说明
IP 呼叫	IP 线路呼入，经过路由和号码变换，连接指定的 SIP 中继进行语音通信

VoIP 路由	用户可以设置路由路径，从 IP 到 TEL/PSTN	
信令和协议	说明	
SIP 信令	兼容的协议：SIP V1.0/2.0、RFC3261	
语音	音频编解码格式	G.711A、G.711U、G.729、G723、G722、AMR、iLBC
	DTMF 模式	RFC2833、SIP INFO、INBAND、RFC2833+信令、带内+信令
网络特性	说明	
网络协议	TCP/UDP、HTTP、ARP/RARP、DNS、NTP、TFTP、TELNET	
静态 IP	IP 地址修改	
DNS	域名解析	
安全性	说明	
管理认证	支持管理员认证确保资源和数据的安全性	
维护升级	说明	
WEB 配置	通过 WEB 界面修改配置	
支持语言	中文，英文	
软件升级	基于 WEB 的用户界面、网关服务、内核及固件升级	
跟踪测试	基于 WEB 的 Ping 测试和 Tracert 测试	
SysLog 类型	ERROR、WARNING、INFO	

1.3 硬件描述

UNIWAY6000 联合网关采用 6U 高度标准机架式设计，主控板采用 RK3568，ARM Cortex-A55 架构四核处理器。网关机箱可装载 2 块主控板和 30 块子板，支持双主控，装载 2 个热插拔式风扇盒，2 个热插拔式电源盒。

1.3.1 网关外观及接口说明

联合网关产品示意图如下：



图 1-2 UNIWAY6000 正面示意图



图 1-3 UNIWAY6000 背面示意图

上图中各接口、按键及指示灯的详细介绍如下：

接口	说明
网络接口	数量：8 个
	类型：RJ-45+SFP（ETH2 支持光电选择，同一时间只能连接一种）
	带宽：10/100/1000 Mbps（ETH1 仅支持 10/100Mbps）
	自适应带宽：支持
	自动翻转：支持
串口	数量：1
	类型：RS-232
	波特率：115200 bps
	接口类型：Mini-USB 连接线
	数据位：8 bits
	停止位：1 bit
	校验：无
	流控：无
按键	说明
恢复出厂设置按键	将网关恢复到出厂设置状态
指示灯	说明
运行状态灯	指示设备运行状态，具体说明见 告警信息说明
告警指示灯	指示设备异常，告警，具体说明见 告警信息说明
Link 指示灯	网络接口左侧的绿色 LED 指示灯，用于指示网络连接状态
ACT 指示灯	网络接口右侧的橙色 LED 指示灯，该指示灯闪烁表示数据正在传输

1.3.2 网关硬件架构

UNIWAY6000 联合网关是在 UNIWAY2300 联合网关的基础上进行升级扩展的，板卡槽位号由 3 位升级到 5 位，在兼容 3 位槽位号板卡的同时可装载更多 5 位槽位号板卡。可插入处理器板、主控板、模拟网关子板、数字网关子板和集成/音频子板。UNIWAY6000 设计前面 12 个业务板插槽和 2 个主控板插槽，后面 18 个业务板插槽，共 32 个卡槽。板卡介绍如下：

UNIWAY6000 主控板具有多个独立的千兆网口，提供了一个高性能嵌入式 CPU 作为整机设备的管理，所有业务板都通过它和外部进行交互。主控板卡槽与子板卡槽存在差异，拥有专属的两个主控板卡槽，主控板必须插入主控板卡槽，而子板一定不能插入主控板槽位，否则可能造成短路或其它故障。

3 位槽位号板卡：

处理板即 CPU 板（占据 2 个业务板高度），基于 X86 架构，用于运行客户开发的 IVR 等业务程序。

模拟网关子板（UMG1000），最大支持 16 路模拟通道，子板型号为 UMG1000-D16S（16 路 FXS 口）、UMG1000-D8S8O（8 路 FXS 口、8 路 FXO 口）、UMG1000-D16O（16 路 FXO 口）、UMG1000-D4EM（4 路无线集群）、UMG1000-D4AU（4 路调音台）。

5 位槽位号板卡：

模拟网关子板（UMGX1000），子板型号为 UMGX1000-D32SP（32 路 FXS 口）、UMGX1000-D32O（32 路 FXO 口）。

数字网关子板（UMGX3000），子板型号为 UMGX3000-C4。

3 位槽位号板卡仅可装载在 UNIWAY6000 联合网关的前 8 个子板槽位, 5 位槽位号板卡可任意装载到 30 子板槽位, 可根据需求进行搭配。

硬件架构图如下:

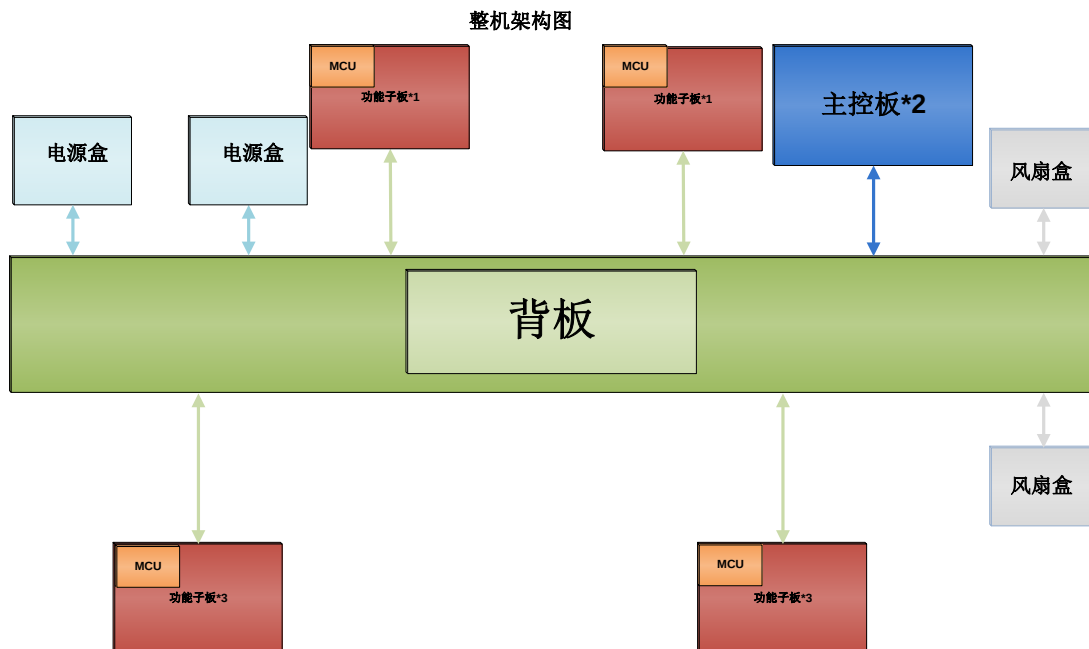


图 1-4 UMG 网关硬件架构图

1.4 告警信息说明

UMG 联合网关 UNIWAY6000 提供运行灯和告警灯, 运行灯为绿色, 告警灯为红色。指示灯的状态及含义说明如下:

指示灯	状态	含义
运行灯	熄灭	系统未启动
	点亮及快闪	系统正在启动
	慢闪	设备正常运行
告警灯	熄灭	设备无异常
	点亮	启动时: 设备正常 运行中: 设备异常
	闪烁	设备异常

说明:

- 开机过程包括系统启动和网关服务启动两个阶段。对于 UNIWAY6000, 系统启动过程大约持续 1 分钟, 系统启动成功后, 运行灯和告警灯均点亮; 网关服务启动成功且设备正常运行后, 运行灯闪烁, 告警灯熄灭。
- 运行过程中, 告警灯点亮或者闪烁表示设备异常, 用户如果无法自行排除故障, 请联系我们的技术人员处理故障, 技术支持联系方式见[附录 C 技术/销售支持](#)。

第2章 基本使用

本章节旨在帮助用户于最短的时间内掌握 UMG 网关产品的基本使用方法。

第一步：确认产品包装盒内包含以下物品。

- UMG 网关机箱 1 台
- 挂耳 2 个、脚垫 4 个、挂耳螺丝 8 颗
- 220V 电源线 2 根
- 保修卡 1 份
- 安装手册 1 份

第二步：固定 UMG 网关机箱。

如果不需要安放到机架上，先安装 4 个脚垫；如果需要安放到机架上，先将挂耳安装到机箱上，再固定机箱到机架上。

第三步：连接机箱电源。

在连接机箱电源之前，务必确认可靠接地。请查看电源插座是否有接地线。

注：UNIWAY6000 有两个电源接口，满足电源主从热备份功能需求。正确连接并开启两个电源后，当一个电源出现故障时，另外一个电源也能保证网关的正常工作。

第四步：接入网线。

第五步：登录网关。

通过浏览器输入 UMG 网关的初始 IP 地址(Uniway6000 ETH1 的初始 IP 地址：192.168.0.101；Uniway6000 ETH2 的初始 IP 地址：192.168.1.101；Uniway6000 ETH3 的初始 IP 地址：192.168.2.101)，进入 UMG 网关。具体登录方法见[登录系统](#)，UMG 网关的初始用户名为 admin，初始密码为 admin。用户在初次登录后，应尽快通过“系统工具 → 更改口令”界面修改初始用户名及密码。用户名、密码修改方法见[更改口令](#)。用户名及密码修改后，需要重新登录。

第六步：修改网关的 IP 地址。

通过“系统工具 → 网络设置”界面修改 IP，使之融入公司的局域网中。IP 地址的修改方法见[网络设置](#)。IP 地址修改后，需要使用新设置的 IP 地址重新登录。

第七步：检查子板是否连接。

子板插好启动成功后，用户可以通过“网关配置 → 子板网关管理”界面检查子板是否连接。

第八步：设置呼叫路由。

到各子板配置管理界面设置相应的路由，路由设置方法参见对应用户手册。

特别注意：

- 按照电信设备使用的常规要求，UMG 网关必须可靠接地(通过电源的第三只脚连接地线)，否则可能出现工作不稳定且抗雷击能力降低等情况。
- UMG 网关工作时会产生热量，切勿阻挡机箱两侧的散热孔，以免发生意外。
- 发现 UMG 网关运行时告警灯亮或者闪烁，用户如果无法自行排除故障，应及时联系我公司的技术人员分析告警类型，并进行相应处理，否则可能会出现性能下降或发生意外错误的情况。

第3章 WEB 配置

3.1 登录系统

在浏览器地址栏输入网关的 IP 地址，进入登录界面，如图 3-1 所示：



图 3-1 登录界面

网关只有一个用户，初始用户名为 **admin**，初始密码为 **admin**。登录后，用户名和密码都可以修改，具体修改方法见[更改口令](#)。

用户登录后，界面显示如下：



图 3-2 登陆后的主界面

3.2 运行信息

运行信息显示了网关当前的工作状态，如图 3-3 所示，详细介绍如下：



图 3-3 运行信息列表

3.2.1 系统信息



图 3-4 系统信息界面

系统信息界面如图 3-4 所示，点击**刷新** 可以获取最新的系统信息。点击**版本详细信息** 可以获取 WEB、网关服务、Uboot 和内核的详细信息。以上各信息项的说明如下：

信息项	说明
MAC 地址	业务网口 1 或业务网口 2 的 MAC 地址。
IP 地址	从左到右依次为业务网口 1 或业务网口 2 的 IP 地址、子网掩码、默认网关。
DNS 服务器	业务网口 1 或业务网口 2 的 DNS 服务器地址。
接收数据包、发送数据包	网关启用后的接收/发送数据包数量，包括总包数、错包数和丢包数。
当前速率	显示网络当前发送和接收的速率。
工作模式	显示网络的工作模式，包括 10 Mbps 半双工、10 Mbps 全双工、100 Mbps 半双工、100 Mbps 全双工、1000 Mbps 全双工和断线六种。
运行时间	网关服务启动后，设备正常工作的时长。运行时间每 2s 更新一次。
CPU 温度	显示当前 CPU 的实时温度。
CPU 占用率	显示当前 CPU 的使用情况。
序列号	每台联合网关唯一的序列号。
WEB	当前使用的 WEB 界面版本。
网关服务	当前使用的网关服务版本。
Uboot	当前使用的 Uboot 版本。
内核	网关上运行的系统内核版本号。
固件	网关上运行的固件版本信息。

3.2.2 子板状态

子板状态		
槽号	类型	状态
1	模拟	连接
2	模拟	连接
3	模拟	连接
4	模拟	连接
5	模拟	连接
9	模拟	连接
10	模拟	连接
11	模拟	连接
12	模拟	连接
13	模拟	连接
14	模拟	连接
15	模拟	连接
16	模拟	连接
17	模拟	连接
18	模拟	连接
19	模拟	连接
20	模拟	连接
21	模拟	连接
22	模拟	连接
23	模拟	连接
24	模拟	连接
25	模拟	连接
26	模拟	连接
27	模拟	连接
28	模拟	连接
29	—	未连接
30	模拟	连接

图 3-5 子板状态列表

子板状态界面如图 3-5 所示，用于显示各个子板连接网关的在线状态，告知用户所在槽号子板的类型和连接状态。

3.2.3 告警信息

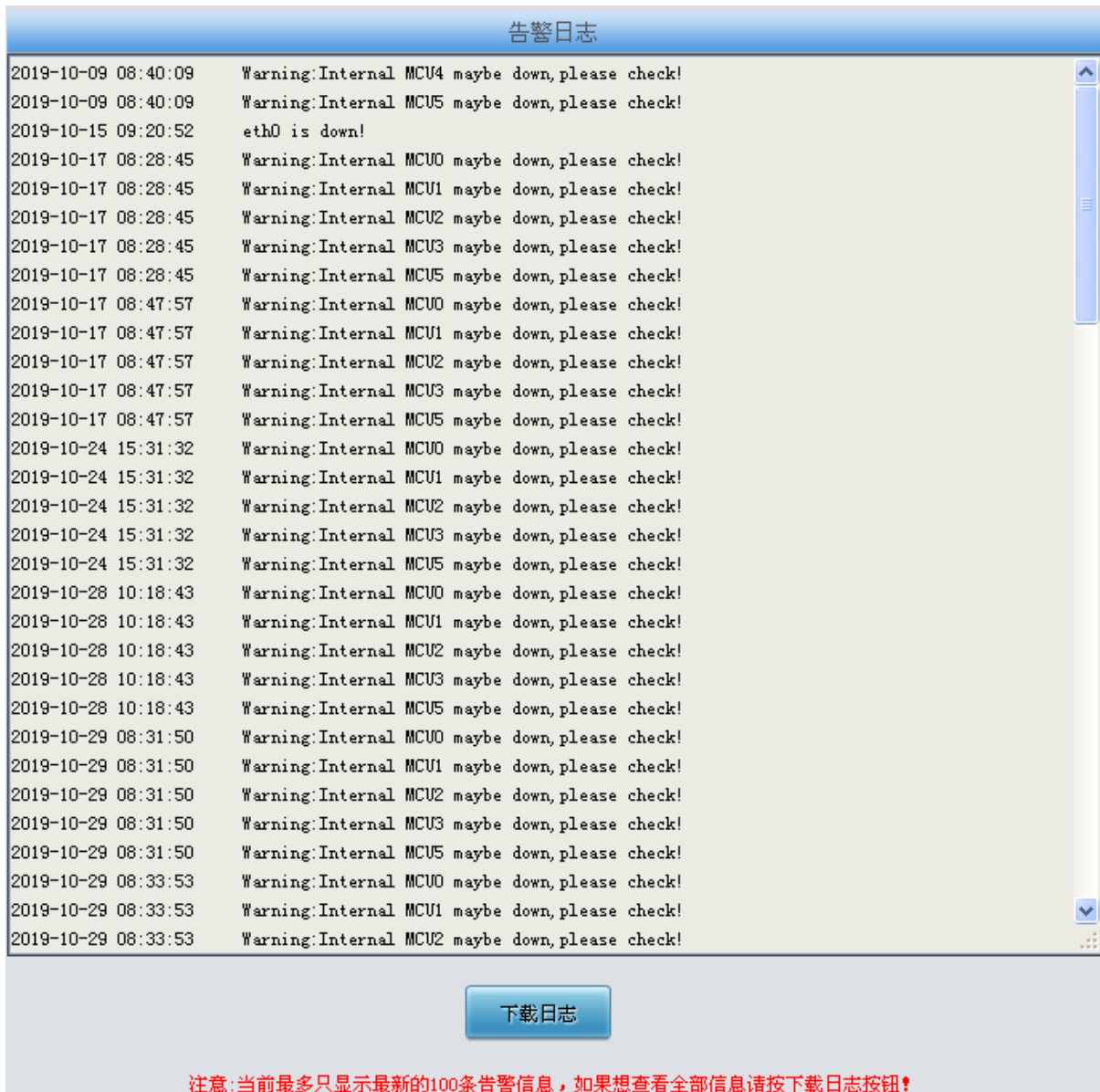


图 3-6 告警信息界面

告警信息界面如图 3-6 所示，网关上出现的所有告警信息都会输出并在该界面显示。

3.3 网关配置

网关配置用于配置子板网关，包含子板网关管理、子板配置信息和热备份设置三个部分，如图 3-7 所示：



图 3-7 网关配置界面

3.3.1 子板网关管理

子板网关管理界面显示联合网关所插子板类型，如图 3-8 所示，点击图中配置管理，进入各子板网关对应的配置界面，具体配置操作可参见网关对应的用户手册。

子板网关管理			
插槽号	子板IP	网关类型	配置管理
1	169.254.1.101	UMGX1000-D32SP	
2	169.254.1.102	UMGX1000-D32SP	
3	169.254.1.103	UMGX1000-D32SP	
4	169.254.1.104	UMGX1000-D32SP	
5	169.254.1.105	UMGX1000-D32SP	
9	169.254.1.109	UMGX1000-D32SP	
10	169.254.1.110	UMGX1000-D32SP	
11	169.254.1.111	UMGX1000-D32SP	
12	169.254.1.112	UMGX1000-D32SP	
13	169.254.1.113	UMGX1000-D32SP	
14	169.254.1.114	UMGX1000-D32SP	
15	169.254.1.115	UMGX1000-D32SP	
16	169.254.1.116	UMGX1000-D320	
17	169.254.1.117	UMGX1000-D320	
18	169.254.1.118	UMGX1000-D320	
19	169.254.1.119	UMGX1000-D320	
20	169.254.1.120	UMGX1000-D320	
21	169.254.1.121	UMGX1000-D320	
22	169.254.1.122	UMGX1000-D320	
23	169.254.1.123	UMGX1000-D320	
24	169.254.1.124	UMGX1000-D320	
25	169.254.1.125	UMGX1000-D320	
26	169.254.1.126	UMGX1000-D320	
27	169.254.1.127	UMGX1000-D320	
28	169.254.1.128	UMGX1000-D320	
29	—	—	—
30	169.254.1.130	UMGX1000-D320	

图 3-8 子板网关管理界面

3.3.2 子板配置信息

子板配置信息界面显示各子板网关的路由信息和端口信息，如图 3-9 所示。

路由信息		
IP->TEL/IP/PSTN路由		
IP/SIP中继组	端口组/IP/PCM中继组	子板
TEL/PSTN->IP路由		
端口组/PCM中继组	IP/SIP中继组	子板
端口组 [1]	172.16.30.6	8--UMG-1016S

图 3-9 子板配置信息界面

3.3.3 热备份设置

热备份设置界面显示热备份功能的相关信息，如图 3-10 所示。

热备份设置

热备份

☒ 启用

公用虚拟IP

10.10.10.4

远端地址

10.10.10.3

心跳网口

网口1:10.10.10.2

保存

重置

图 3-10 热备份设置界面

以上界面中各配置项的说明如下：

配置项	说明
热备份	启用后可以热备份主控板，从而在切换主控板时保持通话不断。
公用虚拟 IP	主控板对外显示的虚拟 IP，用于访问网关和呼叫，热备的两块主控板填写相同 IP。
远端地址	填写热备的两块主控板的对端 IP，检测对方是否在线。
心跳网口	选择用于热备的网口，应与虚拟 IP 远端地址所填 IP 相对应。

3.4 子板组

子板组

选择	索引	包含子板	描述	修改
☐	0	2	默认	

全 选

全 不 选

反 选

删除所选

清空子板组

添加子板组

共 1 条记录 20 条/页 1/1 第一页 上一页 下一页 最后一页 到第 1 页，共 1 页

图 3-11 子板组界面

子板组界面如图 3-11 所示，可以通过点击列表右下角的添加子板组 添加，见图 3-12。

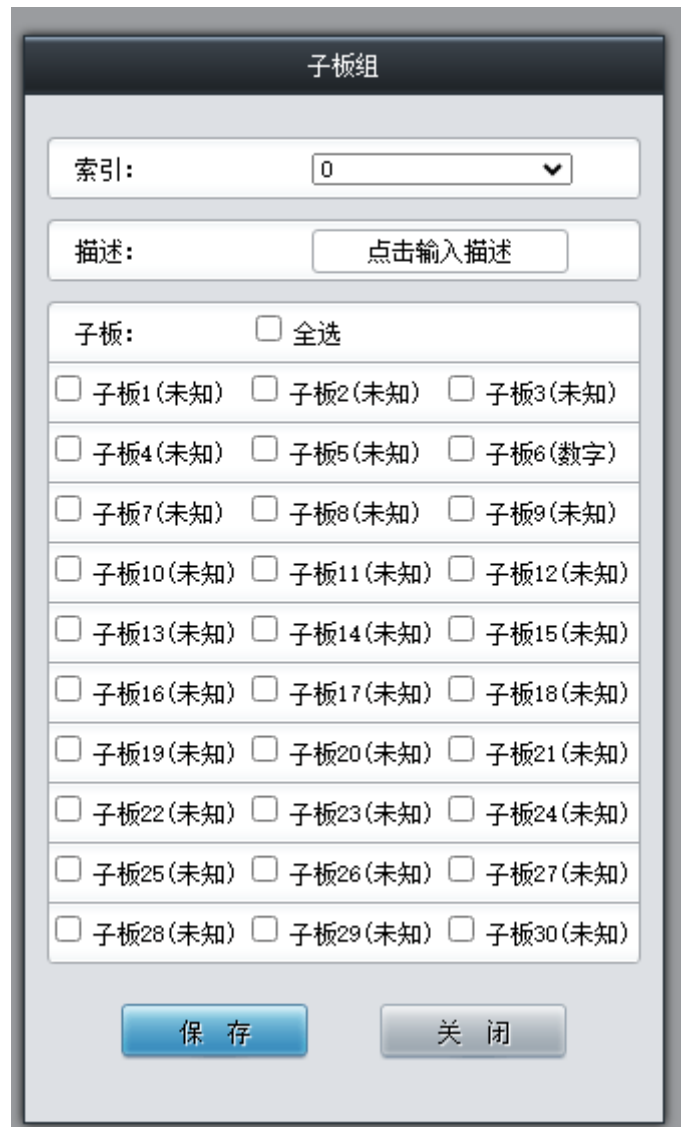


图 3-12 子板组添加界面

以上界面中各配置项的说明如下：

配置项	说明
索引	每个子板组的唯一标识，用于在配置路由规则时对应需要配置的子板组。
描述	标识每个子板组的信息，方便查看。
子板	子板组中包含的子板，子板前的复选框呈灰色表示该子板已被占用，不能选择。选中的子板在图 3-11 的列表中显示为 包含子板 。

配置完成后，点击**保存**将以上设置存入网关；点击**关闭**可直接取消设置。

点击图 3-11 中的**修改**可以对已经配置的子板组进行修改，修改界面各配置项的意义与**子板组添加**界面的对应配置项相同。

如果需要删除子板组，可以在图 3-11 界面中选择对应项目前的复选框，然后点击**删除所选**。**全选**指选中当前页面可以选定的全部项目；**全不选**指取消选中当前页面已经选定的全部项目；**反选**指取消选中当前页面已选中的项目，并选中原先未选中的项目。**清空子板组**用于一键清除所有子板组。

3.5 路由设置

路由设置用于规定 IP → TEL/PSTN 呼叫的路由选择方式，如图 3-13 所示。

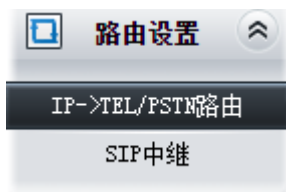


图 3-13 路由设置功能列表

3.5.1 IP to TEL/PSTN 路由

网关默认没有 IP→TEL/PSTN 路由规则，点击**添加路由规则**添加，见图 3-14。用户可以通过该界面添加路由规则相关信息。

图 3-14 IP→TEL/PSTN 路由规则添加界面

以上界面中各配置项的说明如下：

配置项	说明
索引	路由规则的索引，具有唯一性，并且规定了路由规则的优先级，该配置项的值越小优先级越高。用于当一通呼叫同时匹配多条路由规则时，选用优先级最高的路由规则来处理。
呼叫源 IP 地址	表示呼叫来自于哪个 IP 地址。

主叫前缀、被叫前缀	主被叫号码开头的字符串，可以用“*”来代表任意字符串。此配置项与呼叫来源一起规定了适用这条规则的呼叫。 规则说明： <table border="1" data-bbox="502 320 1362 712"> <thead> <tr> <th>字符</th><th>含义</th></tr> </thead> <tbody> <tr> <td>“0”~“9”</td><td>数字 0~9。</td></tr> <tr> <td>“[]”</td><td>表示一个数字，该数字是前后用一对“[”、“]”括起来的范围内的任意值，“[]”内的值只支持数字“0”~“9”、“-”和“,”。 举例：[1-3,6,8]表示集合 1、2、3、6、8 内的任意一个数字。</td></tr> <tr> <td>“-”</td><td>两个数字之间用“-”相隔，表示该区间之内的任何数字。“-”只能出现在“[]”中。</td></tr> <tr> <td>“,”</td><td>两个数字或数字区间之间用“,”相隔，表示两者之间为选择关系。“,”只能出现在“[]”中。</td></tr> </tbody> </table> 举例：规则“0[0-3,7][6-9]”表示前缀为 006、016、026、036、007、017、027、037、008、018、028、038、009、019、029、039、076、077、078、079。 注：主、被叫号码前缀支持多个规则，不同规则间用“.”分开。	字符	含义	“0”~“9”	数字 0~9。	“[]”	表示一个数字，该数字是前后用一对“[”、“]”括起来的范围内的任意值，“[]”内的值只支持数字“0”~“9”、“-”和“,”。 举例：[1-3,6,8]表示集合 1、2、3、6、8 内的任意一个数字。	“-”	两个数字之间用“-”相隔，表示该区间之内的任何数字。“-”只能出现在“[]”中。	“,”	两个数字或数字区间之间用“,”相隔，表示两者之间为选择关系。“,”只能出现在“[]”中。
字符	含义										
“0”~“9”	数字 0~9。										
“[]”	表示一个数字，该数字是前后用一对“[”、“]”括起来的范围内的任意值，“[]”内的值只支持数字“0”~“9”、“-”和“,”。 举例：[1-3,6,8]表示集合 1、2、3、6、8 内的任意一个数字。										
“-”	两个数字之间用“-”相隔，表示该区间之内的任何数字。“-”只能出现在“[]”中。										
“,”	两个数字或数字区间之间用“,”相隔，表示两者之间为选择关系。“,”只能出现在“[]”中。										
呼叫目的	指定这条路由规则最终路由的目的子板组。										
描述	用于标识路由规则，方便查看。										

配置完成后，点击**保存**将以上设置存入网关。点击**关闭**可直接取消设置。



图 3-15 IP→TEL/PSTN 路由规则列表

点击图 3-15 中的**修改**可以对已经配置的路由规则进行修改，修改界面各配置项的意义与**路由规则添加**界面的对应配置项相同。修改界面不允许修改**索引**。

如果需要删除路由规则，可以在图 3-15 界面中选择对应项目前的复选框，然后点击**删除所选**。**全选**指选中当前页面可以选定的全部项目；**全不选**指取消选中当前页面已经选定的全部项目；**反选**指取消选中当前页面已选中的项目，并选中原先未选中的项目。**清空路由**可以一键清除所有路由规则。

3.5.2 SIP 中继



图 3-16 SIP 中继配置界面

网关默认没有 SIP 中继信息，如图 3-16 所示。点击**添加 SIP 中继**按钮进行添加，如图 3-17 所示。用户可以通过该界面添加 SIP 中继相关信息。

图 3-17 SIP 中继添加界面

以上界面中各配置项的说明如下：

配置项	说明
索引	SIP 中继的索引，具有唯一性。
描述	标识每个 SIP 中继组的信息，方便查看。
远端地址	SIP 中继的地址，即与网关通信的对方 SIP 设备的 IP 地址或域名。
本端网口	SIP 中继所在的网口。

3.6 系统工具

系统工具主要用于整个网关程序的维护，包括 IP 修改、时间同步、信息恢复、日志查询、连通性查询等功能，具体功能列表如图 3-18 所示。



图 3-18 系统工具功能列表

3.6.1 网络设置

网络设置

SIP地址选择

网口2:110.10.10.2

SIP信令端口

5060

管理网口设置

IPv4网络类型:

静态

IP地址(I):

10.10.10.2

子网掩码(U):

255.255.255.0

IPv6地址(I):

::

IPv6地址前缀(U):

64

业务网口1设置

IPv4网络类型:

静态

IP地址(I):

172.16.30.76

子网掩码(U):

255.255.255.0

默认网关(D):

172.16.30.254

IPv6地址(I):

::

IPv6地址前缀(U):

64

IPv6 Default Gateway(D):

fc02::200:ecff:fea7:198

业务网口2设置

IPv4网络类型:

静态

IP地址(I):

110.10.10.2

子网掩码(U):

255.255.255.0

默认网关(D):

110.10.10.1

IPv6地址(I):

fc03::200:ecff:fea7:133

IPv6地址前缀(U):

64

IPv6 Default Gateway(D):

fc03::200:ecff:fea7:197

DNS服务器设置

首选DNS服务器(P):

0.0.0.0

备用DNS服务器(P):

0.0.0.0

启用BOND:

☐是☒否

保存

重置

注意1:如果修改网关使用中的IP地址,请用修改后的IP地址重新登录。

注意2:如果修改网络类型为PPPoE后出现网页不能登录的情况,请修改web端口重新登录。

图 3-19 网络设置界面

网络设置界面如图 3-19 所示。SIP 地址选择，用来选择 SIP 信令的 IP 地址，默认使用网口 1。SIP 信令端口设置 SIP 信令用于监听的端口，取值范围为 5001~65535，默认值为 5060。网关上有一个管理网口（ETH1），不能走业务呼叫，只能用于网页登录和 FTP 等 IP 访问。网关上有两个业务网口，每个网口都可以配置独立的 IP 地址（缺省地址如图所示）、子网掩码、默认网关与 DNS 服务器。业务网口支持 Bond 功能，对网口 1 或网口 2 进行复制备份，实现网口 1 和网口 2 的热备份功能，默认为不启用。

注意：1，这两个业务网口不能使用相同网段的 IP 地址和默认网关。

2，连接速度和双工模式，网关默认配置为自动侦测，不建议客户随意修改，因为非自动侦测模式有可能引起网口异常情况。网关默认隐藏该配置项，可按“F”按键令其显示。

配置完成后，点击**保存**将以上设置存入网关。点击**重置**可恢复当前配置。IP 地址修改后，需要使用新设置的 IP 地址重新登录。

3.6.2 管理参数

管理参数配置

WEB管理配置

WEB 端口

80

访问设置

IP白名单

172.16.30.123, 172.16.30.156

多个IP

IP 地址

用“,“隔开

注销时长

1800

秒

SSH管理配置

启用 SSH

☒是 ☐否

SSH 端口

22

远程抓包配置

启用远程抓包功能

☒是 ☐否

☐是否抓取RTP

FTP配置

启用FTP

☒是 ☐否

SYSLOG参数配置

启用SYSLOG

☒是 ☐否

服务器地址

172.16.30.31

SYSLOG级别

INFO

CDR参数配置

发送CDR

☒是 ☐否

服务器地址

172.16.30.36

服务器端口

1234

参数配置

NAT穿透

☒启用

穿透类型

端口映射

网口1映射地址

网口2映射地址

RTP自适应

☐启用

SIP自适应

☐启用

根据原via字段发响应消息

☐启用

RTP端口范围

6000, 20000

时间参数配置

启用 NTP

☐是 ☒否

定时重启

☐是 ☒否

系统时间

☐ 修改 2019-09-19 14:50:58

时区

GMT+8:00 (北京, 新加坡, 台北,)

保存

重置

图 3-20 管理参数配置界面

管理参数配置界面如图 3-20 所示。界面中各配置项的具体说明如下：

配置项	说明
WEB 端口	WEB 进行访问时所携带的端口号。默认为 80。
访问位置	设置可以进行 WEB 访问的 IP 地址。默认为允许所有 IP。可以设置 IP 白名单允许该名单内的 IP 自由进行 WEB 访问。也可以设置 IP 黑名单，禁止该名单内的 IP 进行 WEB 访问。
注销时长	设置在该配置时长内无人操作，则网关自动注销。默认时长为 1800，单位为秒。
启用 SSH	设置是否开启 SSH 远程访问功能，默认为否。
SSH 端口	通过 SSH 远程访问时所携带的端口号。
启用远程抓包功能	启用远程抓包功能后，用户可远程使用抓包工具获取网关的数据包，默认为否。
是否抓取 RTP	设置是否抓取 RTP，功能启用后可在所网口上同时抓取 RTP 包。
启用 FTP	设置是否启用 FTP 服务器，默认值为是。
启用 SYSLOG	设置是否启用 SYSLOG。SYSLOG 启用后，需要填写 SYSLOG 服务器地址 和 SYSLOG 级别 。SYSLOG 默认为不启用。
服务器地址	设置接收日志的 SYSLOG 服务器地址。
SYSLOG 级别	设置 SYSLOG 等级。SYSLOG 等级包括：ERROR（错误）、WARNING（警告）和 INFO（一般信息）三种。
发送 CDR	设置是否启用 CDR。CDR 启用后，需要填写 服务器地址 和 服务器端口 。发送 CDR 默认为不启用。
服务器地址	设置接收 CDR 的服务器地址。
服务器端口	设置接收 CDR 的服务器端口。
NAT 穿透、穿透类型	设置是否开启 NAT 穿透，默认值为不开启。穿透类型仅包括端口映射。默认为不启用。
网口 1 映射地址、网口 2 映射地址	NAT 穿透启用后，网口 1 和网口 2 分别对应的映射地址。实现端口映射同时还需要路由器的配合。此处填写路由器设置的映射地址和端口。
RTP 自适应	该功能启用后，当远端发送的信令消息中携带的 RTP 接收地址或端口与实际情况不符时，自动更新其为实际的 RTP 接收地址或端口，提高网关 RTP 发送的自适应能力。默认为不启用。
SIP 自适应	该功能启用后，表示使用 invite 消息的来源地址做回复，默认为关闭。
根据原 via 字段发响应消息	IP->PSTN 呼叫，开启该功能可以关闭自动修改响应消息 Via 头。默认是不开启该功能。
RTP 端口范围	IP 端建立语音通话时网关端 RTP 适用的端口范围，取值范围为 5000-60000，默认下限为 6000，上限为 20000，且端口范围差值不能小于 4096。
启用 NTP	设置是否启用 NTP 服务器自动同步时间。NTP 自动同步启用后，需要填写 NTP 服务器的地址 、 同步周期 和 时区 。NTP 默认为不启用。
NTP 服务器地址	设置自动同步时间的 NTP 服务器地址。
同步周期	设置 NTP 自动同步时间的同步周期。
定时重启	设置是否定时重启网关，启用后需要填写 重启时间 。启用后网关每天会在设定的时间自动重启。默认为不启用此功能。
重启时间	设置网关定时重启的时间。
系统时间	系统时间，可勾选前面的复选框手动修改。
时区	网关所在时区。

3.6.3 IP 路由表

用户可以设置 IP 路由表，网关根据路由表设置信息，将 IP 包按指定路由发送到目的网段。网关默认没有 IP 路由信息，可以通过点击列表右下角的**添加**进行添加，见图 3-21。

图 3-21 IP 路由表添加界面

以上界面中各配置项的说明如下：

配置项	说明
编号	该路由在路由表中的编号。
目的网段	IP 包可以到达的网段地址。
子网掩码	目的网段对应的子网掩码。
网口	该路由表对应的网口。

配置完成后，点击**保存**将以上设置存入网关。点击**关闭**可直接取消设置。保存配置后的界面如图 3-22 所示。

IP路由表					
选择	编号	目的网段	子网掩码	网口	修改
☐	0	201.123.112.0	255.255.255.0	网口1 (198.254.1.200)	
删除所选 清空					添加

图 3-22 IP 路由表列表

点击中的**修改**可以对已经配置的 IP 路由表进行修改，修改界面各配置项的意义与 **IP 路由表添加** 界面的对应配置项相同。修改界面不允许修改**编号**。

IP 路由表列表下方的**删除所选**用于删除选中的路由表；**清空**用于一键清除所有路由表。

3.6.4 访问控制

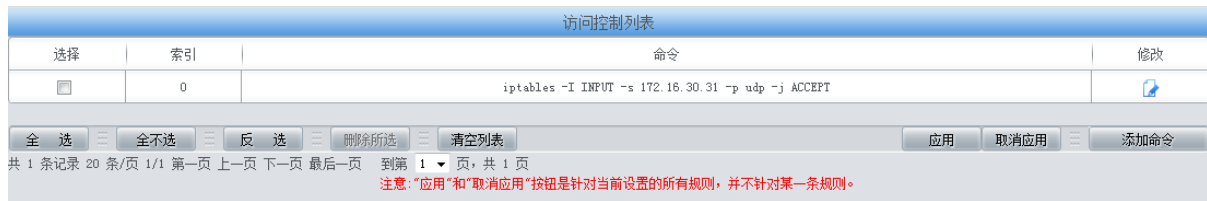


图 3-23 访问控制列表

访问控制列表（ACL）界面如图 3-23 所示，配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。点击**添加命令**，可以添加访问控制命令，如图 3-24 所示。



图 3-24 添加访问控制命令

在命令栏输入 ACL 命令，配置完成后，点击**保存**将以上设置存入网关。点击**关闭**可直接取消设置。命令添加后需点击**应用**使其生效。

点击图中的**修改**可以对已经配置的命令进行修改，修改界面各配置项的意义与**访问控制命令添加**界面的对应配置项相同。修改界面不允许修改**索引**。

如果需要删除访问控制列表，可以在图界面中选择对应项目前的复选框，然后点击**删除所选**。命令删除后，点击**应用**使删除的命令失效。**全选**指选中当前页面可以选定的全部项目；**全不选**指取消选中当前页面已经选定的全部项目；**反选**指取消选中当前页面已选中的项目，并选中原先未选中的项目。**清空列表**可以一键清除所有访问控制列表。

注：

- 1、目前网关只支持 iptables 命令。
- 2、如果是手动添加、修改命令后，不会立即生效，需点击**应用**使命令生效，手动删除命令也需点击**应用**，使删除的命令失效。如果是重启以及导入配置的时候，则命令自动生效，无需点击**应用**。

3.6.5 DDOS 设置

DDoS 指分布式拒绝服务攻击（Distributed Denial of Service，简称 DDoS）。处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。（参考《[分布式拒绝服务攻击与防范措施](#)》）

DDOS设置

WEB 端口防攻击

☒ 启用

WEB 限制次数

8

FTP 端口防攻击

☒ 启用

FTP 限制次数

2

SSH 端口防攻击

☒ 启用

SSH 限制次数

2

TELNET 端口防攻击

☒ 启用

TELNET 限制次数

2

门禁时间设置

设置时间内限制

时间设置(分)

2

保存

重置

信息

图 3-25 DDOS 设置界面

DDOS 设置界面如图 3-25 所示，可以设置部分端口对 DDOS 攻击的防御功能，以上界面中各配置项的说明如下：

配置项	说明
WEB 端口防攻击	该功能启用后，WEB 端口将具有阻止 DDOS 攻击的功能。
WEB 限制次数	同一个 IP 地址通过 WEB 访问网关时，当超过设置的限制次数（访问进程数/5）后将被禁止登录。
FTP 端口防攻击	该功能启用后，FTP 端口将具有阻止 DDOS 攻击的功能。
FTP 限制次数	同一个 IP 地址通过 FTP 访问网关时，当超过设置的限制次数（=访问进程数）后将被禁止登录。
SSH 端口防攻击	该功能启用后，SSH 端口将具有阻止 DDOS 攻击的功能。
SSH 限制次数	同一个 IP 地址通过 SSH 访问网关时，当超过设置的限制次数（=访问进程数）后将被禁止登录。
TELNET 端口防攻击	该功能启用后，TELNET 端口将具有阻止 DDOS 攻击的功能。
TELNET 限制次数	同一个 IP 地址通过 TELNET 访问网关时，当超过设置的限制次数后（=访问进程数）将被禁止登录。

门禁时间设置	是否开启攻击黑名单有效时间设置。包含永久限制 和 设置时间内限制 两种。
时间设置	设置黑名单起作用的有效时间。

配置完成后，点击**保存** 将以上设置存入网关；点击**重置** 可恢复当前设置。

注：重启系统、软件升级或应用防火墙后，临时黑名单会被清空。

3.6.6 集中管理

图 3-26 集中管理设置界面

集中管理配置界面如上图所示，启用该功能后，网关可以注册到一个集中管理平台，实现集中管理平台对网关的远程管理。界面中各配置项的具体说明如下：

配置项	说明
集中管理	是否启用集中管理功能。
自动切换默认网关	该功能启用后，当连接设备云管理平台的网线松动或被拔出时，网关会自动通过另一个网口连接设备云管理平台，默认为关闭。
管理平台	选择网关需要注册到的管理平台。
公司名	网关在设备云管理平台中注册的公司名，仅在管理平台选择为设备云管理平台有效。
网关描述	网关挂载到三汇设备云管理平台中显示的描述，便于在设备分组时进行识别，仅在管理平台选择为三汇设备云管理平台有效。
SNMP 服务器地址	允许访问 SNMP 功能的 IP 地址。
授权码	授权码限制最大长度 64 位，输入内容没有限制。初次连接集中管理服务器时，输入正确的授权码才可以连接上，连接成功后，即使改成错误的授权码，仍可以一直连接上，但是用错误的授权码集中管理功能不可关闭。
工作状态	显示网关与集中管理服务端的连接状态，仅在管理平台选择为设备云管理平台有效。

3.6.7 配置文件

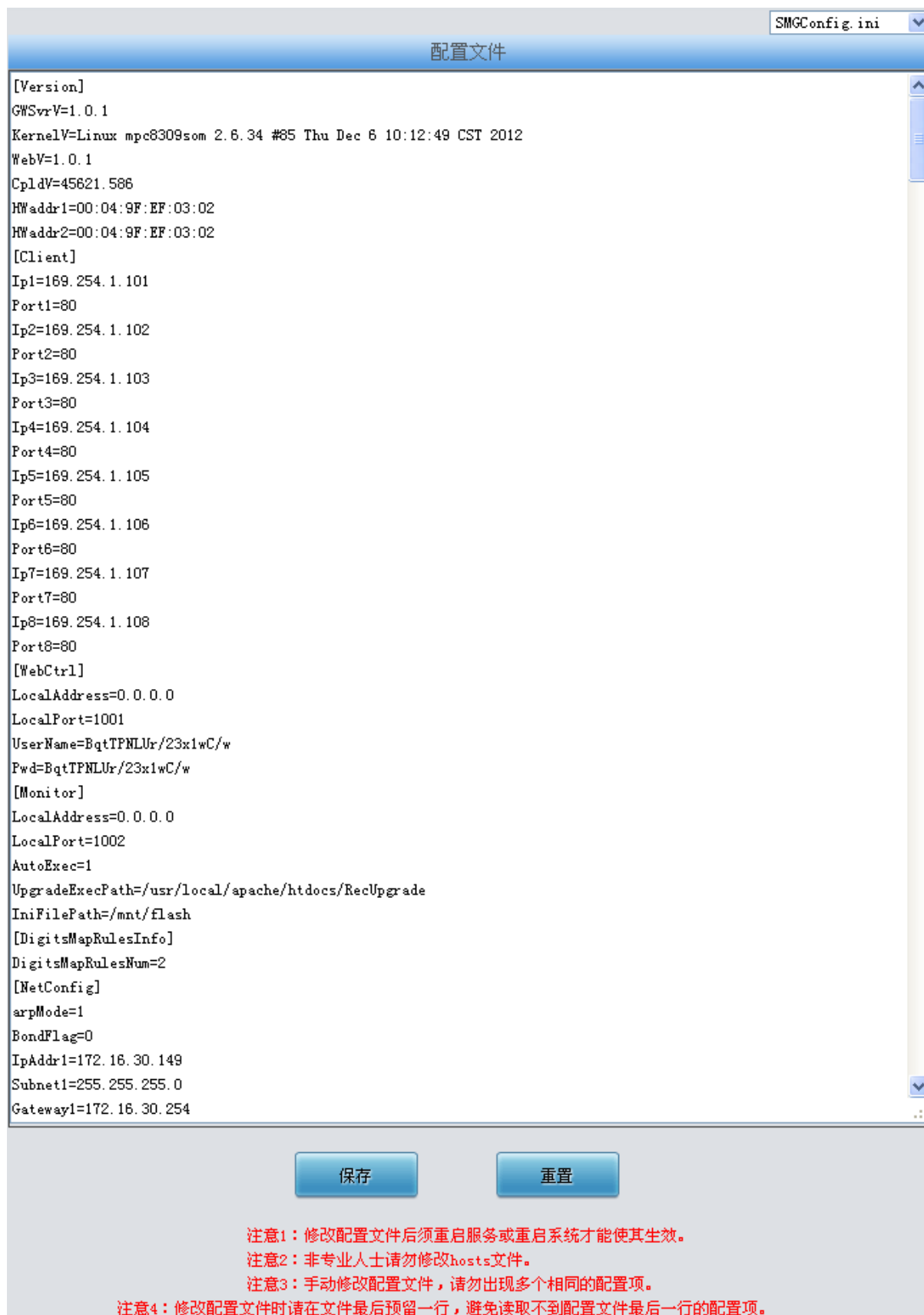


图 3-27 配置文件界面

配置文件界面如图 3-27 所示，通过该界面可以查看和修改网关相关配置文件，包含 SMGConfig.ini 和 ShConfig.ini。其中，SMGConfig.ini 是网关服务的配置文件，路由规则、号码变换、号码过滤等的配置都包含在这个文件中；ShConfig.ini 是板卡相关的配置文件。用户可直接在界面上修改配置，点击**保存**将以上设置存入网关，点击**重置**可恢复当前配置。

3.6.8 信令抓包

The interface is titled "网口抓包" (Network Port Packet Capture). It contains the following elements:

- A label "请选择需要抓包的网口" (Please select the network port to be captured) next to a dropdown menu showing "网口1 (172.16.30.149)".
- A checkbox labeled "是否抓取RTP" (Whether to capture RTP) which is currently unchecked.
- A label "请设置Syslog目的地址" (Please set the Syslog destination address) next to a text input field containing "172.16.30.254".
- A red note: "注意:开始抓包后,会关闭远程抓包功能。" (Note: After starting packet capture, the remote packet capture function will be closed).
- Two buttons on the right: "开始" (Start) and "停止" (Stop).
- Two buttons at the bottom: "清理录音及抓包" (Clear recordings and captures) and "下载日志" (Download logs).

图 3-28 信令抓包界面

信令抓包界面如图 3-28 所示，网口抓包用于设置需要抓包的网口。点击**开始**，将对相应的网口进行抓包（最大能抓 1024000 个包），目前支持 SIP 和 SysLog 抓包，用户可输入 Syslog 目的地址，将 Syslog 文件发送至需要的地址。点击**停止**，停止抓包并下载已抓到的信令包。点击**清理抓包**，可清空所有抓包文件；点击**下载日志**，下载 core 文件、配置文件、错误信息等文件在内的所有日志。

3.6.9 呼叫跟踪



图 3-29 呼叫跟踪界面

呼叫跟踪界面如图 3-29 所示。主要用来输出和保存呼叫相关信息，方便出问题跟踪信息及调试。包含三种模式：过滤主叫、过滤被叫和全部跟踪。点击**开始**执行呼叫跟踪，具体信息将显示在下面的跟踪信息栏中。点击**停止**，可暂停呼叫跟踪。点击**过滤**可根据相关设置，对相关呼叫信息进行过滤。点击**清空**，清空所有跟踪到的呼叫信息。点击**下载**，下载跟踪到的呼叫信息。

3.6.10 Action URL

Action URL 配置，用于指定上报 FXS 通道摘挂机状态的服务器路径，用户可分别设置上报通道摘机和通道挂机两种状态的服务器地址。设置后，当任何一个 FXS 通道发生摘机或者挂机时，网关都会将该状态上报给指定服务器。配置完成后，点击**保存**将以上设置存入网关。点击**重置**可恢复当前配置。

3.6.11 PING 测试

Ping测试

源IP地址选择

网口2:201.123.111.158

目的地址

127.0.0.1

Ping的次数 (1-100)

4

包长 (56-1024 字节)

56

开始

结束

信息

图 3-30 Ping 测试界面

Ping 测试界面如图 3-30 所示，用户可以通过网关对指定的 IP 地址进行 Ping 测试，检测网关与指定地址的连接情况。以上界面中各配置项的说明如下：

配置项	说明
源 IP 地址选择	发起 Ping 操作的源 IP 地址。
目的地址	需要进行 Ping 测试的 IP 地址。
Ping 的次数	进行 Ping 操作的次数，取值范围为 1~100。
包长	进行 Ping 操作的每个数据包的数据长度，取值范围为 56~1024 字节。
信息	执行 Ping 操作时的返回信息，用户可以通过这些信息了解网关与目的地址之间的网络连接情况。

配置完成后，点击**开始**执行 Ping 操作。点击**结束**可以立即结束 Ping 操作。

3.6.12 TRACERT 测试



图 3-31 Tracert 测试界面

Tracert 测试界面如图 3-31 所示，该测试用于查看网关与指定的 IP 地址之间的路由情况。以上界面中各配置项的说明如下：

配置项	说明
源 IP 地址选择	发起 Tracert 操作的源 IP 地址。
目的地址	需要进行 Tracert 测试的 IP 地址。
最大跳转数	能够显示的网关与目的 IP 之间的最大跳转次数，取值范围为 1~255。
信息	执行 Tracert 操作时的返回信息，用户可以通过这些信息了解网关与目的地址之间的详细跳转情况。

配置完成后，点击**开始**执行 Tracert 操作，点击**结束**可以立即结束 Tracert 操作。

3.6.13 修改记录

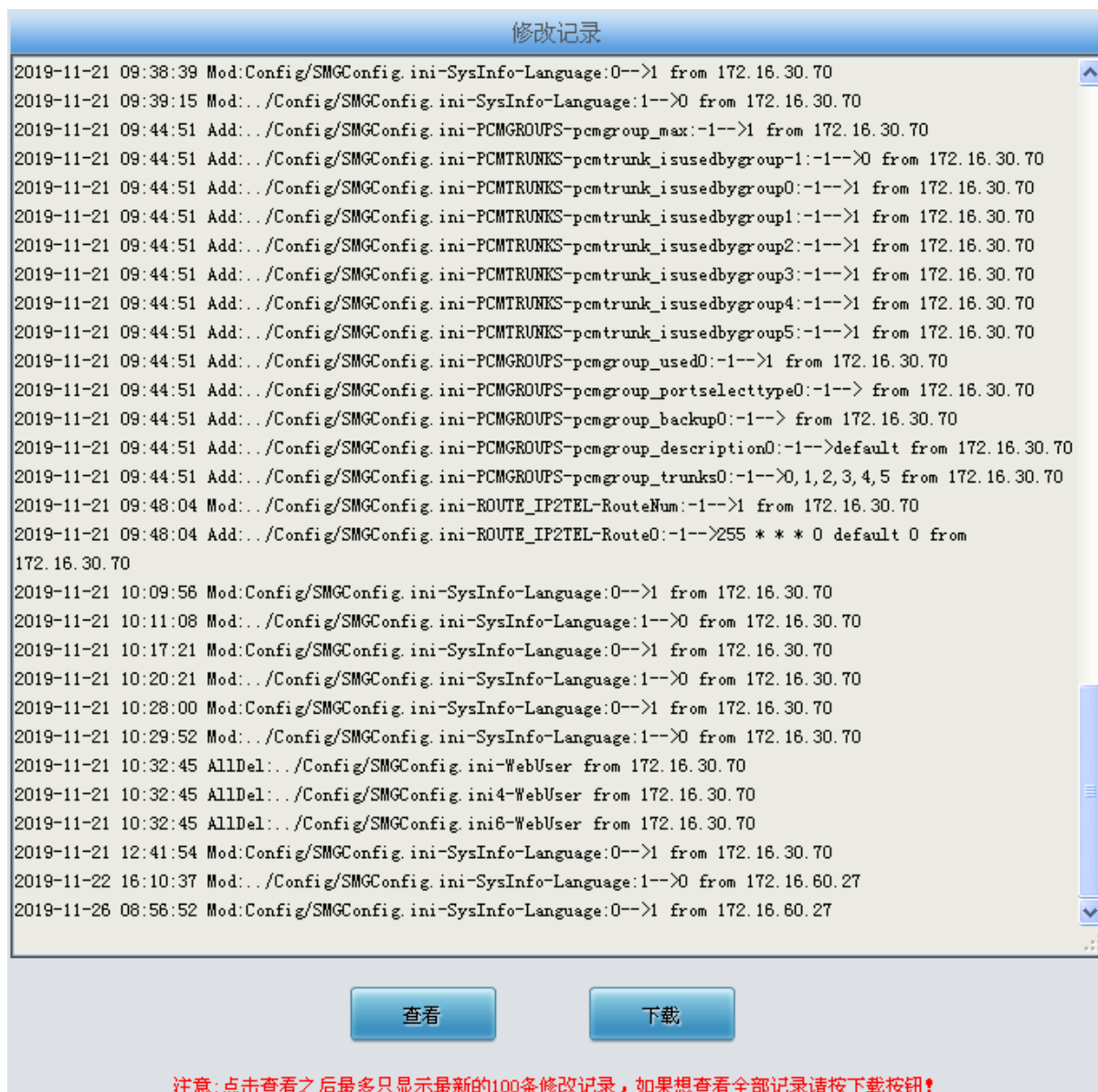


图 3-32 修改记录界面

修改记录界面用于查看网关上配置修改的相关记录。点击**查看**，页面上将显示这些修改记录，如图 3-32 所示。点击**下载**，可下载修改记录。

3.6.14 备份载入

数据备份

请选择需要备份的文件 配置文件 请点击右边按钮开始备份到您的电脑 备份

数据载入

如果需要载入文件，请选择您要载入的文件，再点击右边的上传按钮

请选择需要载入的文件类型 配置文件 浏览... 上传

图 3-33 数据备份、载入界面

数据备份及数据载入界面如图 3-33 所示。用户进行数据备份操作时，需要首先通过数据备份栏的下拉菜单选择需要备份的文件类型，然后点击右侧的**备份**按钮将对应的文件备份到本地。用户也可以进行数据载入操作，首先通过数据载入栏的下拉菜单选择需要载入的文件类型，其次点击右侧的**浏览...**按钮加载本地备份的文件，最后点击**上传**将加载的文件上传至网关。网关会自动使用载入的配置信息覆盖当前的配置。

3.6.15 恢复出厂

恢复出厂

请点击下方按钮恢复出厂设置

恢复

图 3-34 恢复出厂界面

恢复出厂设置界面如图 3-34 所示，用户可以点击**恢复**将网关上的配置恢复到出厂时的默认配置。

3.6.16 软件升级

当前版本信息	
序列号	5274
WEB	2.0.0_2024090214
网关服务	2.0.0_2024090214
Uboot	1.0.0_20240730
内核	#259 SMP Mon Sep 2 14:40:09 +08 2024

请选择更新文件: 未选择任何文件

图 3-35 软件升级界面

软件升级界面如图 3-35 所示,用于升级网关的 WEB 界面、网关服务以及内核与固件的版本。升级时,通过 **选择文件** 加载对应的*.tar.gz 升级包,然后点击**更新**等待升级,这时网关会先进行 MD5 校验,校验通过,方可继续升级。点击**重置**可取消上传的更新文件,但不能用于取消**更新**。

3.6.17 用户管理

暂无用户信息!

图 3-36 添加用户信息界面

如上图,点击添加用户,可以添加用户信息,界面如下图所示:

用户信息	
索引:	0
用户名:	
密码:	
权限:	查看权限
保存 关闭	

图 3-37 用户信息添加界面

以上界面中各配置项的说明如下：

配置项	说明
索引	用户信息的索引，具有唯一性，从 0 开始，最大支持 64 条用户信息添加。
用户名/密码	WEB 登录的用户名和密码。并且都只支持数字、字母或者下划线。
权限	操作权限，可选择查看权限和查看/修改权限。

配置完成后，点击**保存**将以上设置存入网关。点击**关闭**可直接取消设置。用户信息列表如图所示：

用户信息				
选择	编号	用户名	用户权限	修改
☐	0	123	查看权限	
共1条记录20条/页1/1第一页上一页下一页最后一页 到第 1 ▼ 页，共1页 全选 全不选 反选 删除所选 清空用户 添加用户				

图 3-38 用户信息列表

点击图 3-38 中的**修改**可以对已经配置的用户信息进行修改，修改界面各配置项的意义与**用户列表添加**界面的对应配置项相同。修改界面不允许修改**索引**。

如果需要删除用户信息，可以在图 3-38 中选择对应项目前的复选框，然后点击**删除所选**。**全选**指选中当前页面可以选定的全部项目；**全不选**指取消选中当前页面已经选定的全部项目；**反选**指取消选中当前页面已选中的项目，并选中原先未选中的项目。**清空用户**可以一键清除所有用户信息。

3.6.18 更改口令

更改口令	
原用户名	admin
原密码	•••••
新用户名	
新密码	
确认密码	
保存重置 注意1:用户名和密码只能包含数字、字母或者下划线。	

图 3-39 更改口令界面

更改口令界面如图 3-39 所示，用户可以在此界面更改网关 WEB 界面的登录用户名和密码。更改口令需要输入原密码，然后输入新用户名及新密码并确认新密码，修改后点击**保存**即可。点击**重置**可恢复当前配置。用户名及密码修改后，需要重新登录。

3.6.19 重启网关



图 3-40 重启网关界面

重启服务及重启系统界面如图 3-40 所示，用户可以点击**重启服务**对网关服务进行重启，或点击**重启系统**对网关系统进行重启。

附录 A 主要技术/性能参数

外形尺寸:

长×高×深=523×266×442 mm³

重 量:

UNIWAY6000 (含 2 个风扇和 1 块主控板):
约 13kg

环境要求:

工作温度: -10℃—40℃

储存温度: -20℃—85℃

湿 度: 8%—90% 无结露

储存湿度: 8%—90% 无结露

网络接口:

接口数量: 8 (10/100/1000 BASE-TX (RJ-45)
+SFP)

自适应带宽: 支持

自动翻转: 支持

串口:

接口数量: 1 (RS-232)

波特率: 115200bps

接口类型: Mini-USB 连接线

数据位: 8 bits

停止位: 1 bit

校验: 无

流控: 无

注意: 串口连接时, 请按照以上配置进行设置, 否则可能造成异常。

电源要求:

UNIWAY6000 交流电源:

接入电压: 100~240V AC

最大消耗功率: ≤600W

UNIWAY6000 直流电源:

接入电压: 48V DC

最大消耗功率: ≤600W

信令和协议:

7 号信令: TUP 协议、ISUP 协议

ISDN 协议: ISDN 用户侧、ISDN 网络侧

1 号信令: SS1 协议

SIP 信令: SIP V1.0/2.0、RFC3261

音频编解码速率:

G.711A 64 kbps

G.711U 64 kbps

G.729A/B 8 kbps

G723 5.3/6.3 kbps

G722 64 kbps

AMR 4.75/5.15/5.90/6.70/7.40
/7.95/10.20/12.20 kbps

iLBC 13.3/15.2 kbps

采样率:

8kHz

安全防护:

防雷击能力: 4 级

附录 B 常见问题

1、忘记 UMG 网关的 IP 地址，如何重新获得？

长按恢复出厂设置键恢复网关的出厂设置，使网关回到缺省的 IP 地址，三个网口缺省的地址分别为：

Uniway6000 ETH1: 192.168.0.101

Uniway6000 ETH2: 192.168.1.101

Uniway6000 ETH3: 192.168.2.101

2、哪些情况下可以确定 UMG 网关设备出现故障，需要联系我公司的技术支持协助解决？

- a) 网关设备运行时，运行灯不闪烁或告警灯点亮或闪烁，且重启设备或长按恢复出厂设置键并重启设备后，该状态都不消失。

其它问题比如注册失败等情况，一般是由配置错误引起的。用户可以参照[第 3 章 WEB 配置](#)仔细检查网关的配置状况。检查配置后，如果仍旧无法排除问题，也可以联系我公司的技术支持。

3、通过某些浏览器进入网关的 WEB 界面时无法正常登陆，应该如何处理？

请按如下方法在浏览器上进行设置：进入工具→Internet 选项→安全，在“受信任的站点”设置中，添加网关当前的 IP 地址即可。在使用网关的过程中，如果修改了 IP 地址，需要将新的 IP 地址添加到以上设置中。

附录 C 技术/销售支持

您在使用我们产品的过程中，有任何疑问都可以与我们联系，我们将尽心尽力提供服务。

公司联系方法：

杭州三汇信息工程有限公司

http: //www.synway.cn

地址：杭州滨江区南环路 4028 号中恒世纪科技园 1 号楼 9 层

邮编：310053

电话：0571-88861158（总机）

传真：0571-88850923

微信二维码：请扫描下图二维码添加公司微信订阅号了解更多详情。



技术支持：

电话：0571-88921532（工作日 8:30 - 17:00）

手机：（0）13306501675（24 小时热线）

Email: support@sanhuid.com

销售部：

电话：0571-86695356

Email: 13989830066@139.com