

上海迅时通信设备有限公司

SX3000 企业级会话边界控制器 管理员指南

网址: www.newrocktech.com

论坛: bbs.newrocktech.com

电话: 021-61202700

传真: 021-61202704

文档版本: 201504



1 产品结构	1
1.1 前面板	1
1.2 后面板	2
1.3 网络接口.....	2
1.4 配置口	3
2 参数设置	1
2.1 登录.....	1
2.2 界面常用按钮介绍	2
2.3 网络配置.....	2
2.4 软交换配置	4
2.5 服务端口配置.....	5
2.6 高级配置.....	6
2.6.1 系统	6
2.6.2 SSL 证书管理.....	8
2.6.3 安全管理	9
2.6.4 白名单	11
2.6.5 静态路由表.....	11
2.7 呼叫状态与统计	12
2.7.1 在线设备	12
2.7.2 当前呼叫信息	13
2.7.3 设备电话号码	14
2.7.4 基本统计信息	15
2.8 日志管理.....	15
2.8.1 调试日志管理	15
2.8.2 呼叫信息日志	18
2.8.3 启动信息日志	18
2.9 系统工具.....	19
2.9.1 修改密码	19
2.9.2 配置下载	20
2.9.3 配置导入	20
2.9.4 软件升级	21
2.9.5 设备重启	22
2.9.6 恢复出厂配置	22
2.10 版本信息.....	23
2.11 退出.....	23

插图目录

图 1-1 前面板.....	1
图 1-2 后面板.....	2
图 2-1 登录界面.....	1
图 2-2 网络配置界面.....	3
图 2-3 软交换配置界面.....	5
图 2-4 服务端口配置界面.....	6
图 2-5 系统高级配置界面.....	7
图 2-6 SSL 证书管理界面.....	9
图 2-7 安全管理配置界面.....	10
图 2-8 白名单配置界面.....	11
图 2-9 静态路由表配置界面.....	12
图 2-10 在线设备信息界面.....	12
图 2-11 当前呼叫信息界面.....	13
图 2-12 设备电话号码界面.....	14
图 2-13 基本统计信息界面.....	15
图 2-14 调试日志管理界面-无 SD 卡时.....	16
图 2-15 调试日志管理界面-有 SD 卡时.....	16
图 2-16 保存日志界面.....	17
图 2-17 保存路径界面.....	17
图 2-18 呼叫信息日志界面.....	18
图 2-19 启动信息日志界面.....	19
图 2-20 修改密码界面.....	19
图 2-21 配置下载界面.....	20
图 2-22 配置导入界面.....	21
图 2-23 软件升级界面 1.....	21
图 2-24 软件升级界面 2.....	22
图 2-25 软件升级界面 3.....	22

表格目录

表 1-1 前面板说明	1
表 1-2 指示灯含义表	1
表 1-3 后面板说明	2
表 1-4 网络接口插脚引线规范	2
表 1-5 网络接口指示灯状态	2
表 1-6 RJ45 配置口插脚引线规范表	3
表 1-7 配置口属性表	3
表 2-1 默认登录密码说明	2
表 2-2 网络配置参数	3
表 2-3 软交换配置参数	5
表 2-4 服务端口配置参数	6
表 2-5 系统高级配置参数	7
表 2-6 SSL 证书管理配置参数	9
表 2-7 安全管理配置参数	10
表 2-8 在线设备信息参数	13
表 2-9 当前呼叫信息参数	14
表 2-10 设备电话号码参数	14
表 2-11 基本统计信息参数	15
表 2-12 调试日志管理配置参数-无 SD 卡时	16
表 2-13 调试日志管理配置参数-有 SD 卡时	16

1 产品结构

1.1 前面板

图1-1 前面板

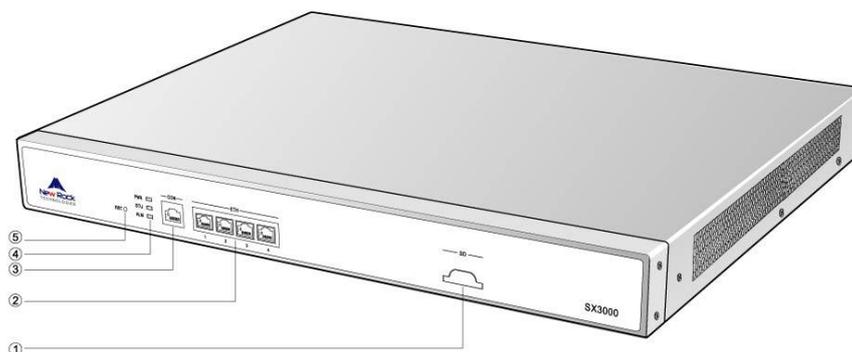


表1-1 前面板说明

序号	说明
①	SD 卡接口
②	4 个网口
③	CON 配置接口
④	指示灯。详见表 1-2 指示灯含义
⑤	RST 按键。用尖状物按压 3 秒以上再松开，即可全部恢复出厂配置

表1-2 指示灯含义表

标识	功能	颜色/状态	说明
PWR	电源指示	绿色	电源开启
		熄灭	电源关闭
STU	状态指示	熄灭	系统故障，不工作
		红色持续约 10 秒后变绿	红色时表示系统已上电，尚未进入正常运行状态，变绿后表示已进入正常运行状态
		绿色	正常运行
ALM	告警指示	绿色	无告警情况
		红色持续约 10 秒后变绿	红色时表示系统已上电，尚未进入正常运行状态，变绿后表示已进入正常运行状态
		红色长亮	存在告警情况

1.2 后面板

图1-2 后面板

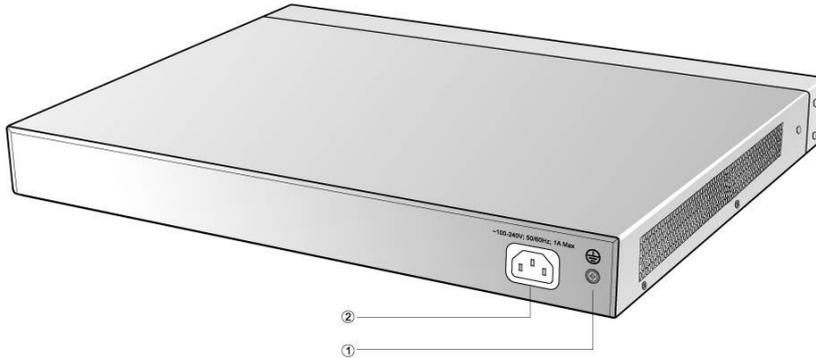


表1-3 后面板说明

序号	说明
①	接地柱
②	交流电源输入接口，输入 100 - 240 伏交流电（AC）电压

1.3 网络接口

SX3000 提供 4 个 10/100/1000 兆的网络接口，接头规格为 RJ45，配备指示灯。表 1-4 中给出了网络接口的插脚引线以及指示灯的规范。

表1-4 网络接口插脚引线规范

速率	插脚							
	1	2	3	4	5	6	7	8
1000Base-T	BIDB-	BIDB+	BIDA-	BIDD-	BIDD+	BIDA+	BIDC-	BIDC+
100Base-TX/ 10Base-T	Tx+	Tx-	Rx+	保留	保留	Rx-	保留	保留

表1-5 网络接口指示灯状态

指示灯	颜色/状态	含义
左灯	长亮	端口连接成功，无业务流
	闪亮	端口连接成功，有业务流
	灭	端口未连接或连接不成功
右灯	亮	端口速率 1000M
	灭	端口速率 100M 或 10M

1.4 配置口

SX3000 提供 1 个配置口（CON），接头规格为 RJ45，表 1-6 中给出了插脚引线及配对连接规范。

表1-6 RJ45 配置口插脚引线规范表

RJ45 配置口插脚引线编号	1	2	3	4	5	6	7	8
说明	NC	NC	TXD	GND	GND	RXD	NC	NC
与 DB9 母头的配对连接			2		5	3		
与 DB25 公头的配对连接			3		7	2		

配置口与本地 PC 的 RS232 端口相连，用于本地管理和调试，PC 可以通过终端仿真程序与 SX3000 建立连接。如表 1-7 所示，配置口使用 3 条插脚引线：TXD、RXD 和 GND，分别用于发送数据、接收数据和接地。

请使用专用的 RJ45-RS232 串口连接电缆连接 SX3000 端的配置口和 PC 端的 RS232 端口。此连接电缆需自行制作或购买。若与未配备有 RS232 端口的笔记本电脑连接，则还需使用 USB 转 RS232 串口连接电缆。上述两种电缆的示意图如下。

RJ45 -RS232 串口连接电缆



USB-RS232 串口连接电缆



表1-7 配置口属性表

属性	描述
连接器	RJ45
接口数量	1
接口标准	RS232
波特率	115200
数据位	8
奇偶校验	无
停止位	1
流量控制	无

2 参数设置

2.1 登录

说明：登录设备 Web 界面的浏览器支持 IE9~IE11、火狐、谷歌。本文以 IE 浏览器为例进行说明。在 IE 浏览器的地址栏中输入设备的 IP 地址：<https://192.168.2.240>（出厂缺省 IP 地址），在登录界面输入用户名、密码和验证码，即可进入配置界面。



注意

用 HTTPS 访问设备，如果未安装证书，IE 浏览器会提示“此网站的安全证书有问题”，单击“继续浏览此网站”进入。采用系统默认证书和公私钥对，存在安全风险，请用户及时替换为自己公司的证书和公私钥对。具体操作参见 2.6.2 SSL 证书管理。

图2-1 登录界面

用户

密码

验证码 4787 [刷新](#)

版权所有 © 上海迅时通信设备有限公司 2014. 保留一切权利

登录用户分管理员和操作员两级，默认密码如表 2-1 所示。



注意

采用系统默认密码存在安全风险，请在首次登录后进入“系统工具”页面及时修改密码。

表2-1 默认登录密码说明

用户	默认密码	说明
admin	SX3000@123（必须大写）	管理员 admin 可进行所有配置
operator	operator@123（必须小写）	操作员 operator 只可浏览部分配置



注意

- SX3000 允许多人登录。多人登录时，先登录的管理员有修改权限，后登录的管理员只能浏览。
- 登录时需要输入的验证码有效时间为 90 秒，超时后请点击“刷新”重新生成验证码后输入。
- 以 admin 账号登录，如连续输错 3 次密码，则 10 分钟内将禁止 admin 登录，但允许以 operator 登录。若再连续输错 operator 登录密码 3 次，则该 IP 地址在 10 分钟内禁止登录。
- 连续输错登录用户名 6 次，则该 IP 地址在 10 分钟内禁止登录。
- 登录后 10 分钟内未进行操作，系统认定超时。继续操作需重新登录。
- 配置完成后，请点击“注销”按钮退出，以免影响其他管理员的操作。

2.2 界面常用按钮介绍

按钮“提交”位于配置界面下方，用于提交配置信息。管理员完成页面参数配置后，点击“提交”。出现成功提示表示系统接受配置信息；出现“重启后配置生效”对话框，则表示该参数需系统重启方可生效。管理员应在完成所有修改操作后，点击“系统工具 > 设备重启”，激发配置生效。

2.3 网络配置

设备出厂默认只启用网口 1，若需要使用多个网口，需给各网口配置不同网段的 IP 地址。点击“网络”，进入该配置界面。

图2-2 网络配置界面

名称	值	说明
主机名	SX3000	由字母，数字，“-”组成的字符串，首字符必须为字母
MAC 地址	00:0E:A9:65:66:66	
网口 1		
IP 地址	192.168.77.77	
子网掩码	255.255.0.0	
网口 2		
IP 地址		
子网掩码		
网口 3		
IP 地址		
子网掩码		
网口 4		
IP 地址		
子网掩码		
默认网关		
网关 IP 地址	192.168.2.1	
域名解析服务器		
启用	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭	
首选服务器	8.8.8.8	
备用服务器		
时间服务器		
首选服务器	198.60.22.240	
备用服务器	133.100.9.2	
超时	0 分钟	

表2-2 网络配置参数

名称	说明
主机名	配置设备名称，缺省值 SX3000。管理员可根据部署规划，给每台 SX3000 设置不同名称，以示区别。 主机名最多允许 48 个字符，可以是字母(A-Z 或 a-z)、数字(0-9)和加号(+), 也可以是 IP 地址。主机名不允许为空或空格。除 IP 地址格式，首字符必须是字母，结尾字符不允许是减号。
MAC 地址	显示设备的 MAC 地址。
网口 n	
IP 地址	在此处填写网口 n 的 IP 地址。 注：只使用一个网口时，可选择四个网口中的任意一个进行配置。使用多个网口，需给各网口配置不同网段的 IP 地址。
子网掩码	在此处填写网口 n 的子网掩码。
默认网关	
网关 IP 地址	在此处填写默认网关的 IP 地址。
域名解析服务器	
启用	启动 DNS 服务。
首选服务器	启动 DNS 服务后，必须在此输入首选 DNS 服务器 IP 地址，无缺省值。
备用服务器	启动 DNS 服务后，可以在此输入备用 DNS 服务器 IP 地址，非必填项，无缺省值。
时间服务器	
首选服务器	在此输入首选时间服务器 IP 地址。此项无缺省值，必填项。
备用服务器	在此输入备用时间服务器 IP 地址。此项非必填项，无缺省值。
超时	如果在该参数指定的时间内未找到时间服务器，将重新查找。单位为分钟。

名称	说明
查询间隔	同步到时间服务器后，设备每间隔该参数规定的时间将重新查询时间服务器，更新时间同步。单位为分钟。
时区	选定时区，参数值包括： (GMT-11:00) 中途岛 (GMT-10:00) 夏威夷檀香山 (GMT-09:00) 阿拉斯加安克雷奇 (GMT-08:00) 提亚瓦纳 (GMT-06:00) 丹佛 (GMT-06:00) 墨西哥城 (GMT-05:00) 印地安纳波利斯 (GMT-04:00) 格莱斯贝 (GMT-04:00) 南乔治亚 (GMT-03:30) 纽芬兰 (GMT-03:00) 布宜诺斯艾利斯 (GMT-02:00) 维德角 (GMT) 伦敦 (GMT+01:00) 阿姆斯特丹 (GMT+02:00) 开罗 (GMT+03:00) 莫斯科 (GMT+03:30) 德黑兰 (GMT+04:00) 马斯喀特 (GMT+04:30) 喀布尔 (GMT+05:30) 加尔各答 (GMT+05:00) 卡拉奇 (GMT+06:00) 阿拉木图 (GMT+07:00) 曼谷 (GMT+08:00) 北京 (GMT+09:00) 东京 (GMT+10:00) 堪培拉 (GMT+10:00) 亚特雷德 (GMT+11:00) 马加丹 (GMT+12:00) 奥克兰

2.4 软交换配置

SX3000 可根据软交换的部署要求，将回复消息发送到指定的软交换端口或发送到软交换发送消息的端口。

点击“软交换”，进入该配置界面。

图2-3 软交换配置界面

序号	软交换	朝对方发送端口回复
1	192.168.15.88:5060	<input type="radio"/> 是 <input checked="" type="radio"/> 否
2		<input type="radio"/> 是 <input checked="" type="radio"/> 否
3		<input type="radio"/> 是 <input checked="" type="radio"/> 否
4		<input type="radio"/> 是 <input checked="" type="radio"/> 否
5		<input type="radio"/> 是 <input checked="" type="radio"/> 否

表2-3 软交换配置参数

名称	说明
软交换 1~5	最多可配置五个软交换的 IP 地址和信令端口号，地址和端口号之间要用':'分隔，格式示例：220.248.118.50:5060。



注意

此参数不能配置为 localhost、127.0.0.1、0.0.0.0 或者 SX3000 的 IP 地址。

SX3000 在将消息转发到软交换时,会优先选用与软交换地址在同一个网段的网口;其次选用与默认网关地址相同网段的网口转发。

2.5 服务端口配置

服务端口是 SX3000 设备接收来自于终端设备消息的信令端口。在收到终端信令消息后，经过处理 SX3000 会将消息转发到与接受端口对应的软交换。

每个网口最多可设置 5 个服务端口，端口号必须唯一，每个服务端口对应一个软交换。

SX3000 可以选择对每个服务端口上接收和发送的消息进行解密和加密，解密和加密可以对语音或信令单独进行，也可选择对两者都进行，默认为不进行解密和加密。如果端口上设置了加密，设备将对该端口上收到的消息进行解密后再转发到软交换，同时，设备将对软交换回复的消息进行加密后再转发给终端。

启用加密时可以设置密钥（UDP Encrypted、TLS 不需要加密密钥），SX3000 设置的密钥与对接设备使用的密钥必须一致。

选择 TLS 加密方式时，RTP 会自动使用 SRTP 方式加密。

SX3000 有 4 个网口，管理员可根据终端部署位置对服务端口进行配置。下面以终端部署在“网口 1”所连接的网络为例进行说明。

点击“服务端口 > 网口 1”，进入该配置界面。

图2-4 服务端口配置界面



表2-4 服务端口配置参数

名称	说明
网口 1 (IP 地址)	显示用户在“网络配置”小节配置的网口 1 的 IP 地址，只读，不能修改。
服务端口	配置该网口的服务端口对应的端口号，用来接收来自于终端的信令消息。
软交换序号	配置与该服务端口对应软交换，系统支持 5 个软交换。
备份软交换	每个服务端口可以设置两个备份软交换：备份软交换一和备份软交换二。SX3000 开启心跳监测功能后，若发现软交换宕机，SX3000 将自动切换到备份软交换；在原软交换恢复后，自动重新切换回来。
语音加密	加密方式有 3 种： <ul style="list-style-type: none"> • None（不加密） • RTP（加密 RTP 全部内容，包括 RTP Header 和 RTP Body） • RTP Header（加密 RTP 头文件） • RTP Body（加密 RTP 包内容）
加密方式	加密方式有 8 种： <ul style="list-style-type: none"> • None（不加密） • TLS • TCP Not Encrypted: 使用 TCP 协议对信令（和 RTP）进行封装，但不采用加密算法 • TCP Encrypted: 使用 TCP 协议对信令（和 RTP）进行封装，且使用加密算法 • UDP Not Encrypted: 使用 UDP 协议对信令（和 RTP）进行封装，但不采用加密算法 • UDP Encrypted: 使用 UDP 协议对信令（和 RTP）进行封装，且采用加密算法 • Using Keyword • Using Keyword2 • Encrypt 14
加密密钥	在此处设置密钥。终端设备也使用加密时需要设置和 SX3000 一样的密钥。UDP Encrypted、TLS 不需要加密密钥。

2.6 高级配置

2.6.1 系统

点击“高级 > 系统”，进入该界面。

图2-5 系统高级配置界面

网络	软交换	服务端	高级	状态与统计	日志管理	系统工具	版本信息
系统 SSL证书管理 安全管理 白名单 静态路由表 注销							
UDP端口最小值		10000					
RTP端口最小值		30000					
IP_TOS		0x0C					
语音流转发		<input type="radio"/> 不转发 <input checked="" type="radio"/> 转发					
语音流中断检测时长		300		秒			
最大注册周期		0		秒			
NAT穿越		<input checked="" type="radio"/> 是 <input type="radio"/> 否					
NAT IP 地址							
心跳监测		<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭					
心跳监测周期		30		(秒)			
TR069							
服务器URL				例: https://192.169.1.101:8089/tr069/services/acs			
用户名							
密码							
服务标识代码		1234					
模块名称		SBC					
定期通知间隔时长		60		(秒)			
ACS回连CPE地址							
ACS回连认证帐号							
ACS回连认证密码							
<input type="button" value="提交"/>							

表2-5 系统高级配置参数

名称	说明
UDP 端口最小值	SX3000 上用于与软交换进行包交互的端口，必须小于 RTP 端口最小值，默认为 10000，UDP 端口范围为 UDP 端口的最小值~（RTP 端口的最小值-1）。
RTP 端口最小值	SX3000 上用于收发 RTP 语音包的端口的最小值，必须大于 UDP 端口最小值。默认为 30000。RTP 端口范围：RTP 端口最小值~（RTP 端口最小值+4799）。
IP_TOS	此项参数用来定义不同优先级别的服务等级质量保证，缺省值为 0x0C。例如：TOS=0xB8 表示优先级为 5，要求低时延和高吞吐量，对可靠性无要求。
语音流转发	此项参数用来设置 RTP 语音包是否经 SX3000 转发。默认为“转发”。
语音流中断检测时长	当在该参数设置的时间内没有检测到语音包时，关闭该语音通路。单位为秒，有效值范围为 180~1200 秒。默认为 300 秒。
最大注册周期	允许终端向 SBC 发送注册消息，并由 SBC 转发给软交换的最大周期。默认值为 0。 <ul style="list-style-type: none"> 若使用默认值 0，则 SBC 不会检查终端注册消息所带的 <code>expiry</code> 值，终端仍按原周期注册； 若输入的最大注册周期大于 <code>expiry</code> 值，则终端按填入的周期进行注册； 若输入的最大注册周期小于 <code>expiry</code> 值，则终端仍按原周期进行注册。
NAT 穿越	<ul style="list-style-type: none"> 是：将 SX3000 将来自于终端消息中的 <code>Via</code> 和 <code>Contact</code> 字段所带的 IP 地址改为 SX3000 的 IP 地址； 否：不作修改。

名称	说明
NAT IP 地址	<p>如果 SX3000 部署在 NAT 设备下游（即处于私网内），为确保 SX3000 和外网终端之间顺利交互，则需在此填写 NAT 设备的外网 IP 地址，并在 NAT 设备上做如下地址映射：</p> <ul style="list-style-type: none"> 将 SX3000 面向外网终端的网口地址映射为 NAT 设备的外网 IP 地址。 将 SX3000 面向外网终端的服务端口进行端口映射。例如连接 NAT 设备的是网口 1，则 SX3000 界面服务端口>网口 1中的服务端口要做一对一的端口映射。如端口 5070 映射为 5070，5080 映射为 5080。 将 SX3000 上开启的 UDP 和 RTP 端口做端口范围映射。具体需要映射的端口范围为：UDP 端口最小值到 RTP 端口最小值+4799。例如，高级>系统页面查到 UDP 端口最小值为 10000，RTP 端口最小值为 30000，则需要映射的端口范围为 10000~34799。
心跳监测	检测软交换是否在线。
心跳监测周期	发送 OPTIONS 消息到软交换的周期。
TR069	
服务器 URL	输入 TR069 网管服务器地址。支持 HTTP/HTTPS。
用户名	输入管理用户名。
密码	输入管理密码。
服务商标识代码	用于标识设备服务商的信息，可以是数字或英文字母。
模块名称	字符串，用于简单描述接口类型或名称。
定期通知间隔时长	向 TR069 网管服务器上报的间隔，单位为秒。
ACS 回连 CPE 地址	ACS 服务器回连 SX3000 的地址。
ACS 回连认证账号	输入回连认证账号。
ACS 回连密码	输入回连密码。

2.6.2 SSL 证书管理

点击“高级 > SSL 证书管理”，进入该界面。

图2-6 SSL 证书管理界面



表2-6 SSL 证书管理配置参数

名称	说明
证书口令	制作 SIP TLS 加密证书时输入的口令。制作方法参见《配置指南》中“SIP TLS 加密证书制作”。
根证书文件名	制作的 SIP TLS 加密根证书文件名称。制作方法参见《配置指南》中“SIP TLS 加密证书制作”。
用户证书文件名 (网口 1/2/3/4)	为网口 1/2/3/4 制作的证书文件名称。制作方法参见《配置指南》中“SIP TLS 加密证书制作”。
用户密钥文件名 (网口 1/2/3/4)	为网口 1/2/3/4 制作的证书密钥文件名称。制作方法参见《配置指南》中“SIP TLS 加密证书制作”。
SIP TLS 加密证书上传	上传制作好的证书 tar 包。具体参见《配置指南》中“配置步骤”的步骤 5。
SIP TLS 加密根证书下载	通过 SFTP 上传证书到设备后，此处会显示一个地址。可点击该链接地址下载 SIP TLS 加密根证书。
HTTPS 证书上传	上传证书颁发机构提供的 HTTPS 证书和密钥。 注意：采用系统默认证书和公私钥对，存在安全风险，请用户及时在此上传您自己公司的证书和公私钥对。并在 PC 的浏览器上导入根证书。

2.6.3 安全管理

在安全管理界面可以选择 SX3000 是否启用 Telnet/SSH 服务。

SX3000 可以灵活设置访问控制，具体请参考 linux 下 iptables 使用手册。



注意

- 设备默认关闭 Telnet/SSH 服务，默认禁 ping。

- 开启 Telnet/SSH 服务后存在安全风险，请在使用后及时关闭。
- 添加访问控制命令时，需要在命令前加路径“/var/run”，示例如下：
`/var/run/iptables -A INPUT -s 10.128.23.23 -p tcp --dport 80 -j ACCEPT`
 可直接在文本框添加或编辑命令，每行一条命令
- 错误的访问控制配置可能导致无法通过网口访问设备。

点击“高级 > 安全管理”，进入该界面。

图2-7 安全管理配置界面



表2-7 安全管理配置参数

名称	说明
Telnet/SSH 服务	SX3000 默认开放 HTTP/HTTPS 端口，用户只能通过 Web 访问、管理和维护设备。Telnet/SSH 服务根据实际需要可选，默认关闭。授权访问设备的 IP 地址，请在白名单页面设置。
Web 服务	通过 Web 访问设备时所使用的端口。默认为 80。

名称	说明
访问控制	<p>命令举例：</p> <ul style="list-style-type: none"> • <code>/var/run/iptables -A OUTPUT -d 192.168.250.230 -p icmp -j DROP</code> 这条命令使 SX3000 无法 Ping 通 IP 地址是 192.168.250.230 的主机，使用本命令，只需改变 IP 地址就可以阻止 SX3000 Ping 通对应的主机。 • <code>/var/run/iptables -A INPUT -p tcp --dport 80 -s 192.168.250.230 -j DROP</code> 这条命令使 IP 地址为 192.168.250.230 的主机不能通过 http 访问 SX3000，使用本命令，只需改变 IP 地址就可以阻止对应的主机访问 SX3000。 • <code>/var/run/iptables -F</code> 清除所有已存在的规则

2.6.4 白名单

启用该功能后，只有从列表中的地址才能登录 Web 或 Telnet。

点击“高级 > 白名单”，进入该界面。

图2-8 白名单配置界面



白名单的配置步骤如下：

步骤 1 点击“添加”。

步骤 2 在弹出的输入框中输入允许访问的 IP 地址，点击“确认”。

步骤 3 勾选“开启白名单”。



注意

- 不支持配置 IP 地址段。
- 配置完成需要重启设备生效。
- 要使 Telnet 白名单需要在安全管理页面开启 Telnet，如图 2-7。
- 当开启白名单但内容为空时允许来自任何地址的终端对设备进行访问。
- 白名单最多可配置 30 条地址。

2.6.5 静态路由表

通过配置静态路由，SX3000 可以按指定的规则转发消息。

点击“高级 > 静态路由表”，进入该界面。

图2-9 静态路由表配置界面



静态路由表的配置步骤如下：

步骤 1 点击“添加”。

步骤 2 在输入框中依次填写目的 IP 地址、子网掩码、网关地址等信息，并选择是否生效，再点击“确认”。



注意

目的 IP 地址与子网掩码遵循路由表配置规则，网关地址为路由转发的下一跳地址。
配置完成需要重启设备生效。

2.7 呼叫状态与统计

2.7.1 在线设备

点击“状态与统计 > 在线设备”，打开该界面。可以查看所有 Web 登录用户信息（包括登录用户的 IP 地址和级别）及在线终端（IP 话机、语音网关等）的信息。

图2-10 在线设备信息界面



表2-8 在线设备信息参数

名称	说明
登录用户信息 (Login User Info)	<p>显示当前登录设备的用户 IP 地址和用户身份。IP 地址后的数字代表用户身份：</p> <p>1 表示最先登录的管理员，具有修改权限</p> <p>2 表示操作员，仅具有浏览权限。</p> <p>3 表示在第一位管理员登录之后再登录设备的其它管理员，这时仅具有浏览权限。</p>
在线终端信息 (Online Gateways Info)	<p>显示在线终端的情况。</p> <ul style="list-style-type: none"> total: 在线终端数目 id: 在线终端序列号 gw ip:rport: 在线终端的 IP 地址及端口号 sbc ip:port: SX3000 的 IP 地址及端口号 sbc udp local port: SX3000 为该终端创建的面向软交换的 UDP 本地端口 ss sip:port: 软交换的 IP 地址及端口号 protocol: 所使用的协议

2.7.2 当前呼叫信息

点击“状态与统计 > 当前呼叫信息”，打开该界面。

图2-11 当前呼叫信息界面



表2-9 当前呼叫信息参数

名称	说明
当前呼叫信息	<ul style="list-style-type: none"> total: 当前呼叫数目 rtp local port: RTP 本地端口 gateway ip:rport: 在线终端的 IP 地址及端口号 call type: 呼叫类型, incoming 指呼入、outgoing 指呼出 gw sdp : 在线终端的 SDP 地址 ss sdp: 软交换的 SDP 地址



注意

如果“高级 > 系统”页面中的“语音流转发”设置为“不转发”，RTP 语音流将不经过 SX3000，“当前呼叫信息”页面为空，无法查看当前呼叫的语音流信息。

2.7.3 设备电话号码

点击“状态与统计 > 设备电话号码”，打开该界面。

图2-12 设备电话号码界面



表2-10 设备电话号码参数

名称	说明
设备电话号码	<ul style="list-style-type: none"> id: 在线终端序列号 gw ip:rport: 在线终端 IP 地址及端口号 phone number: 电话号码

2.7.4 基本统计信息

点击“状态与统计 > 基本统计信息”，打开该界面，可以查看一些基本的统计信息。

图2-13 基本统计信息界面



表2-11 基本统计信息参数

名称	说明
系统信息 (System Info)	<ul style="list-style-type: none"> • System Up Time: 系统启动时间 • Online Gateways: 当前在线终端数 • Current Calling Counter: 当前正在通话的呼叫数
系统统计 (System Statistic)	SIP Server Change: 连接软交换改变的次数
呼叫统计 (Call Statistic)	统计过去 24 小时内的以下呼叫数据： <ul style="list-style-type: none"> • Call Counter: 过去 24 小时之内的呼叫总数 • Call Duration (minutes): 过去 24 小时之内所有呼叫的通话时长，单位为分钟 • Abnormal Release Call: 过去 24 小时之内已接通但未收到挂机(BYE)信令的呼叫数
信令传送统计 (Signal Transmit Statistic)	统计过去 24 小时之内的信令传送信息，包括：INVITE、Re-INVITE、18X、200OK、BYE、CRCX、MDCX、DLCX 等消息在过去 24 小时内传送的个数。

2.8 日志管理

2.8.1 调试日志管理

点击“日志管理 > 调试日志管理”，打开该界面。可以下载设备的调试日志文件。当设备上没有 SD 卡时，调试日志保存在内存中；当设备上有 SD 卡时，调试日志保存在 SD 卡中。

请不要在设备运行过程中插拔 SD 卡，以免引起设备运行异常。

图2-14 调试日志管理界面-无 SD 卡时

表2-12 调试日志管理配置参数-无 SD 卡时

名称	说明
系统日志服务器	系统日志的服务器 IP 地址。
调试日志服务器	调试日志的服务器 IP 地址。
调试日志事件级别	选择调试日志文件的事件级别，级别越高，产生的调试日志文件越详细。缺省值为 3。 注：调试日志级别通常应设在 3 或以下，以免影响设备性能。

图2-15 调试日志管理界面-有 SD 卡时

表2-13 调试日志管理配置参数-有 SD 卡时

名称	说明
系统日志服务器	系统日志的服务器 IP 地址。
调试日志服务器	调试日志的服务器的 IP 地址。
调试日志事件级别	选择调试日志文件的事件级别，级别越高，产生的调试日志文件越详细。缺省值为 3。 注：调试日志级别通常应设在 3 或以下，以免影响设备性能。
单个调试日志容量	SD 卡最多存储 20 个调试日志，此处设置每个调试日志的大小。达到 20 个后，新的日志覆盖老的日志。
调试日志下载	选择 SD 卡中保存的调试日志序号后点击下载。序号越大表示日志越新。下载步骤见下文描述。
其他日志下载	下载系统其他日志（包括 Web 操作日志、SSH 后台操作命令记录以及暂未写入 SD 卡的调试日志）。下载步骤见下文描述。

调试日志下载操作步骤如下：

步骤 1 点击“下载”，设备开始将日志打包。

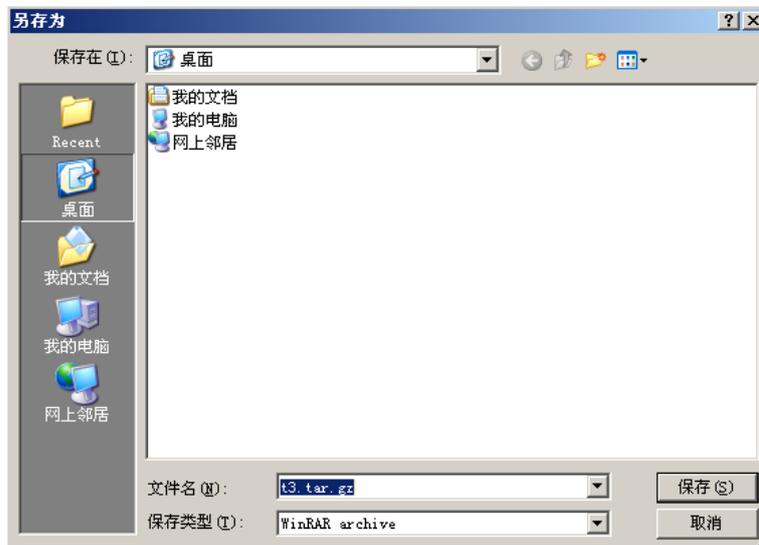
步骤 2 等待一段时间（日志信息量越大，等待时间越长）后，出现保存日志界面，如下图。

图2-16 保存日志界面



步骤 3 点击“另存为”，选择保存路径，如下图。

图2-17 保存路径界面



步骤 4 日志下载完毕后，可到相应的服务器上查看日志。



注意

当 SD 卡剩余存储空间只有 500MB 时，系统自动清理过期日志（删除当前年份之前 5 年的日志文件）。

2.8.2 呼叫信息日志

点击“日志管理 > 呼叫信息日志”，打开该界面。

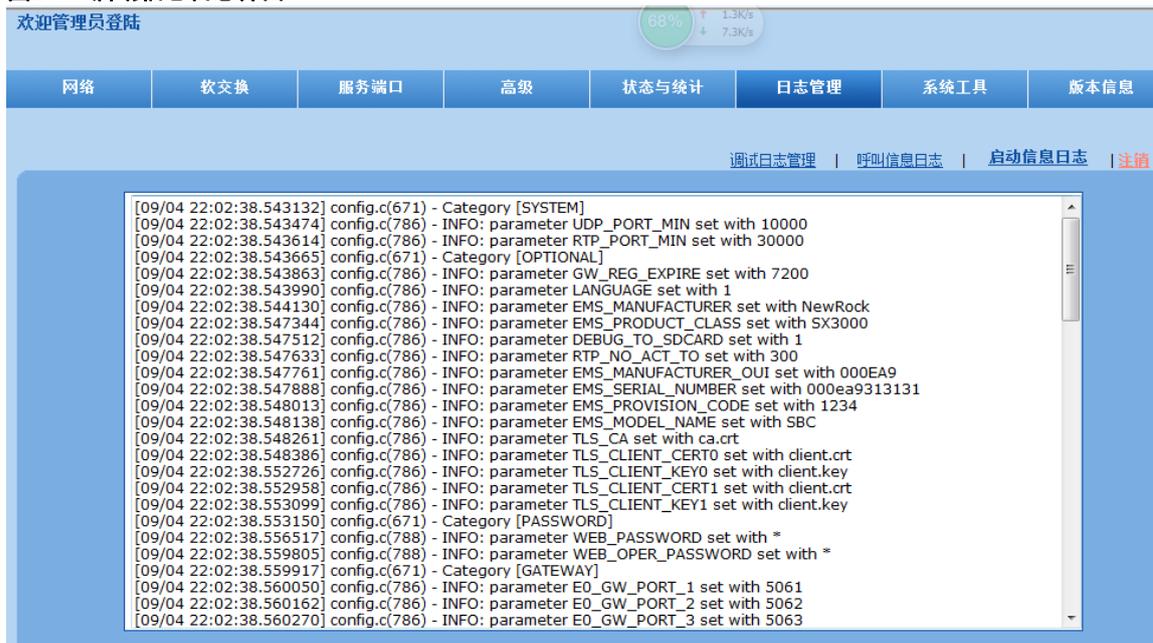
图2-18 呼叫信息日志界面



2.8.3 启动信息日志

点击“日志管理 > 启动信息日志”，打开该界面。

图2-19 启动信息日志界面



2.9 系统工具

2.9.1 修改密码

点击“系统工具”，打开该界面。只有管理员才有权限修改登录密码。

修改管理员密码，需在“新密码”栏和“确认新密码”栏输入新的密码，然后点击“提交”即可。

操作员的当前密码以暗码显示，管理员可直接在“操作员密码 > 密码”栏直接修改操作员的密码。

图2-20 修改密码界面





注意

新密码以暗码显示。

2.9.2 配置下载

点击“系统工具 > 配置导出”，打开该界面。可以下载设备的配置文件。

图2-21 配置下载界面



注意

白名单、安全管理（访问控制配置除外）、静态路由，以及网络页面的配置不会包含在下载的配置中。

2.9.3 配置导入

点击“系统工具 > 配置导入”，打开该界面。操作步骤与“软件升级”步骤相同。

图2-22 配置导入界面



2.9.4 软件升级

点击“系统工具 > 软件升级”，打开该界面。软件升级操作步骤如下：

步骤 1 索取升级文件（tar.gz文件），并存放到本地PC的任意路径（如：存放路径为桌面）。

步骤 2 点击“系统工具 > 软件升级”，进入软件升级界面。

图2-23 软件升级界面 1



步骤 3 点击“浏览”，选择存放在本地路径的升级文件。

步骤 4 点击“上传”，将升级文件上传至设备。

步骤 5 上传完成后，点击“下一步”，启动升级程序。

图2-24 软件升级界面 2



步骤 6 出现提示“软件升级成功，系统将立即重启”后，点击“确定”。

图2-25 软件升级界面 3



注意

设备升级约持续几分钟时间。在此期间不要对设备进行操作（特别是断电、断网或重启）。

当管理系统界面无法显示时，说明设备正在重启过程中。

约二分钟后重新访问管理系统界面，点击“版本信息”并进入版本信息界面查看软件版本信息，确认版本为所升级的版本。

2.9.5 设备重启

点击“系统工具 > 设备重启”，将重新启动设备，所需时间较长。

2.9.6 恢复出厂配置

点击“系统工具 > 恢复出厂配置”，相关参数将恢复到出厂时的值。

出厂参数设置考虑到满足常用应用的需要，在一般应用场合下用户无须更改。

2.10 版本信息

点击“版本信息”，可查看设备的版本信息。

2.11 退出

点击右上角“注销”，即可退出设备管理系统操作界面，返回重新登录界面。