



SBC8000 会话边界控制器

用户手册 V1.0



深圳鼎信通达股份有限公司

地址：深圳南山区西丽街道创科路万科云城一期7栋A座18楼

邮编：518052

传真：+86-755-26456664

电话：+86-755-61919966

邮箱：sales@dinstar.com, support@dinstar.com

网址：www.dinstar.cn

前言

欢迎选购

欢迎您选购鼎信通达 SBC8000 会话边界控制器！深圳鼎信通达股份有限公司为您提供全方位的技术支持，需要更多在线技术支持，请拨打技术支持热线电话：0755-61919966。

内容介绍

为了更好的帮助您了解和使用 SBC8000 会话边界控制器，我们编写了该产品的用户手册，主要介绍了该产品的应用场景、功能特性、安装方法、网络连接和 Web 配置&操作等。在使用 SBC8000 会话边界控制器的过程中，请仔细阅读本手册。

适用对象

本手册适合下列人员阅读：

- 用户
- 安装、配置和维护 SBC8000 会话边界控制器的工程师

修订记录

文档名称	文档版本	软件版本
SBC8000 会话边界控制器用户手册	V1.0	2.94.1.0

文档约定

本文档中所提及的系统或设备均指 SBC8000 会话边界控制器；文档中有注意或说明的内容，表示为需要用户特别注意的内容。

特别声明

1. SBC8000 会话边界控制器为深圳鼎信通达股份有限公司自主研发的通信和网络产品,该手册中包含的所有内容,包括但不限于文字表述、图标、图表、页面设计、数据等等均享有完整的著作权、专利权和商标权等相关权利,并受《中华人民共和国著作权法》、《中华人民共和国商标法》、《中华人民共和国专利法》等相关法律法规和中国加入的所有知识产权方面的国际条约、国际公约的保护。
2. 未经深圳鼎信通达股份有限公司的书面授权许可,任何单位、组织或个人不得以任何目的、使用任何形式或方法擅自对本手册进行抄袭、翻译等违法侵权行为,否则深圳鼎信通达股份有限公司将追究其法律责任,特此郑重声明!
3. 本公司保留对本手册中所描述的产品进行改进的权利,手册中涉及的图片及文字等内容解释如有出入,请以最终实际系统为准。
4. 由于产品版本升级或其它原因,本手册内容会不定期更新,恕不另行通知。

特性声明

本文档仅作为使用指导,其内容依据我司实验室设备信息编写,并不确保涵盖所有平台部署的所有使用场景。因硬件部署、虚拟机部署、公有云部署不同等原因,可能造成文档中提供的内容(包括但不限于用户界面、安装流程、性能配置等)与用户使用的设备信息不一致。请以用户设备实际信息为准,本文档不再针对前述情况造成的差异一一说明。

安全规则设置提示

为保障系统业务安全,请根据具体业务需求设置安全规则。如:IP 防攻击策略、SIP 防攻击策略、系统安全、访问控制、黑白名单、IP 地址白名单等。
配置和参数如有不明之处,可联系技术支持咨询。

个人数据使用说明

使用个人数据的场景	收集的个人信息项	个人数据收集的来源和方式	使用个人数据的目以及安全保护措施	个人数据的存留期限与存留策略	个人数据的销毁方式
不涉及个人信息	不涉及个人信息	不涉及个人信息	不涉及个人信息	不涉及个人信息存留	不涉及个人信息

前言

1 产品概述	1
1.1 产品简介	1
1.2 应用场景	1
1.3 功能和特性	2
2 安装指导	6
2.1 安装前准备	6
2.1.1 安全注意事项	6
2.1.2 检查机房环境是否维持良好的温/湿度条件	6
2.1.3 检查配套设备	6
2.2 服务器安装	7
2.2.1 安装服务器	7
2.2.2 安装操作系统	7
2.2.3 安装 SBC8000	7
2.2.4 连接到以太网	7
2.2.5 故障排查	7
3 参数配置	8
3.1 登录	8
3.1.1 登录准备	8
3.1.2 登录	8
3.2 Web 界面结构和导航树	9
3.3 首页	11
3.3.1 运行信息	11
3.3.2 接入网状态	13

3.3.3 接入中继状态	13
3.3.4 核心中继状态	14
3.3.5 呼叫状态	15
3.3.6 注册状态	16
3.3.7 SIP 账户状态	17
3.3.8 监控状态	20
3.3.9 话单状态	20
3.3.10 BFD 状态	21
3.3.11 radius 状态	21
3.3.12 SIP 防攻击状态	22
3.4 业务配置	22
3.4.1 接入网	23
3.4.2 接入中继	27
3.4.3 核心网中继	32
3.4.4 路由规则	37
3.4.5 业务管理	41
3.4.6 话单管理	42
3.4.7 编解码分组	45
3.4.8 TLS 配置	46
3.4.9 主备	47
3.4.10 号码规则	50
3.4.11 黑白名单	51
3.4.12 号码变换	52
3.4.13 号码池	53
3.4.14 SIP 账户	54
3.4.15 时间规则	56

3.4.16 速率控制	57
3.4.17 SIP 头域修改	57
3.4.18 SIP 头域透传	59
3.4.19 质量监控	60
3.4.20 带宽限制	61
3.5 安全配置	62
3.5.1 访问控制	62
3.5.2 防攻击策略	62
3.5.3 web 认证	64
3.6 系统	65
3.6.1 系统管理	65
3.6.2 web 配置管理	66
3.6.3 接口管理	66
3.6.4 静态路由	67
3.6.5 用户管理	68
3.6.6 版本升级	69
3.6.7 备份与恢复	70
3.6.8 License 管理	70
3.6.9 数字证书管理	71
3.6.10 用户板管理	71
3.7 维护	72
3.7.1 日志	72
3.7.2 Ping	73
3.7.3 tracert	74
3.7.4 正则表达式	75
3.7.5 SNMP	76

3.7.6 远程连接配置	78
4 术语	79
附录 【跟踪命令】	80

1 产品概述

1.1 产品简介

随着通信网络融合与 ALL IP 发展趋势，越来越多的企业开始采用 IP-PBX、软交换、MCU 等产品技术构建内部 IP 通信系统，以降低通信成本、实现灵活部署、提供新业务功能，提升企业内外部沟通效率与核心竞争力。

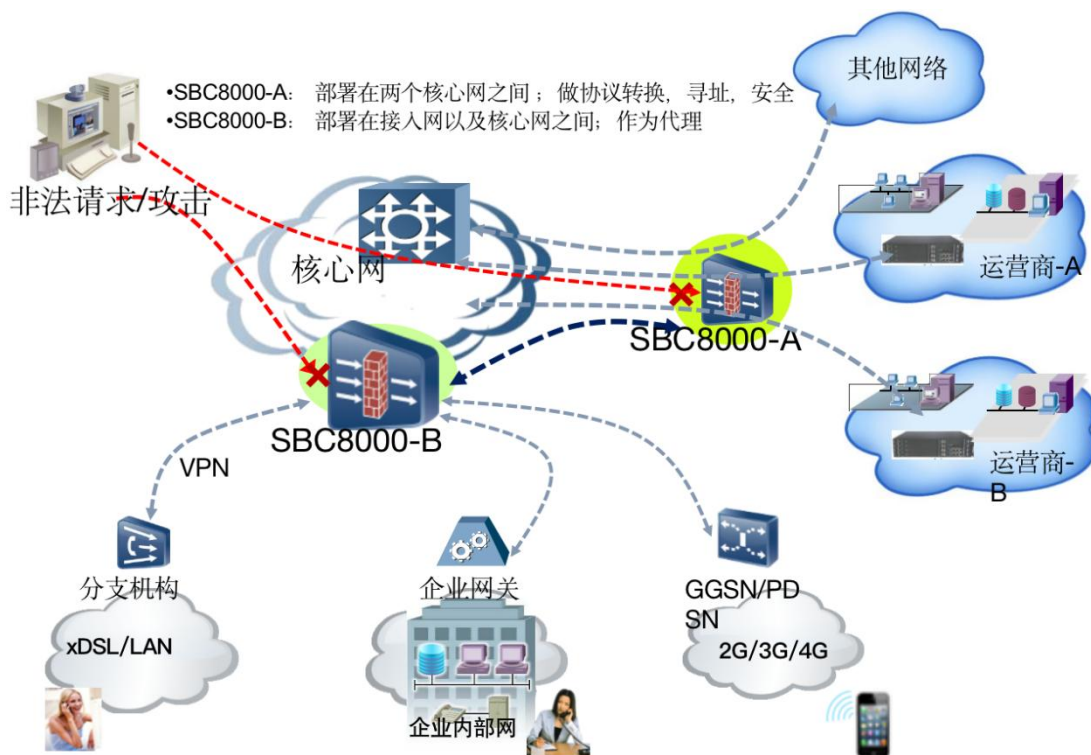
IP 通信系统为用户带来诸多便利的同时，也造成了一些其他麻烦。其中在复杂网络情况下的 IP 多媒体业务 NAT 穿越、终端用户的安全接入是许多企业建设管理 IP 通信系统时非常困扰的问题。

SBC8000（Session Border Controller，会话边界控制器）相关解决方案能够低成本解决针对企业 IP 通信系统建设实施的两大问题：终端接入安全和 IP 多媒体业务 NAT 穿越。

SBC8000 脱离了嵌入式硬件的限制，可以安装在各种服务器平台上：x86、ARM、鲲鹏或华为云/阿里云等，极大地提高了性能，部署迁移方便。其支持高达 10000 并发会话和 5000 路语音媒体转码处理，支持双机热备，并支持 SIP over TLS、SRTP 加密会话、webrtc。除了传统电信编解码，媒体处理还支持 AMR、OPUS 和 iLBC 等无线和互联网编解码转换。

1.2 应用场景

SBC8000 会话边界控制器的应用场景如下图所示：



1.3 功能和特性

➤ 关键特性

- 支持 10000 并发会话和 5000 路语音媒体转码处理
- 支持 100000 个用户注册
- 支持 HA
- 支持通用的物理机或虚拟机部署、公有云部署
- 标准 SIP 协议和灵活的路由规则，完美兼容 IMS 系统 提供 VoIP 防火墙，安全防攻击，保护核心网
- 支持智能带宽限制和动态黑名单
- 支持跨网、NAT 穿越，适应多种组网环境
- 支持 SIP over TLS，SRTP 加密会话，安全可靠
- 支持信创国产麒麟 OS 操作系统，支持信创国产数据库（达梦数据库）、国密（加解密算法）
- 多种编码标准: G.711A/U,G.723.1,G.729A/B, iLBC, AMR, OPUS



说明

如在其他软件安装部署，因购买的许可证不同或软件基础平台不同，支持的功能特性有所不同，具体差异可咨询我司技术支持工程师。

➤ 平台部署

- 硬件部署
X86 或 ARM
- 虚拟机部署
VMware、Fusionsphere、FusionComputer、KVM
- 公有云部署
阿里云、华为云、电信云等

➤ 性能

- 呼叫并发
最大支持 10000 路并发
- 转码并发
支持 5000 路媒体编解码转换处理
- 呼叫 CPS
每秒最大处理 800 路并发
- 用户注册数
最大支持 100000 个用户注册
- 注册 CPS
每秒最大处理 800 个注册报文

➤ 语音特性

- 语音编码: G.711a/μ, G.723, G.729A/B, iLBC, G.726, AMR, OPUS
- 静音抑制
- 舒适噪声生成(CNG)
- 语音活动检测(VAD)
- 回声抵消 (G.168), 最大 128ms
- RTP/RTCP
- 语音中断保护
- 自适应动态缓冲
- 可调整增益控制
- 自动增益控制
- 传真: T.38 和 Pass-through
- DTMF 模式: RFC2833/Signal/Inband

➤ VoIP 协议

- SIP v2.0 , UDP, TCP, TLS, RFC3261
- SIP 中继工作模式: Peer/Access
- SIP 用户注册代理: 最大 3000 个
- B2BUA 用户代理
- SIP 呼叫流控
- SIP 注册流控
- SIP 注册报文攻击动态扫描检测
- SIP 异常呼叫攻击动态扫描检测
- SIP 头域变换
- SIP 报文冗余机制
- 支持多软交换和软交换防封杀
- QoS (ToS, DSCP)
- NAT 穿越

➤ 安全

- DOS/DDOS 攻击防御
- 访问控制策略
- 基于策略的 IP 和 SIP 防攻击
- 畸形报文检测与处理
- UDP-Flood 攻击防御
- TCP-Flood 攻击防御
- TLS&SRTP 加密会话
- 主被叫号码黑白名单
- ACL 控制
- VoIP 防火墙

➤ 管理维护

- 基于 Web 的可视化配置及维护
- 数据备份/恢复
- Web 固件升级
- 内置网络抓包功能
- 系统日志
- 操作日志

-
- 呼叫话单
 - NTP 自动时间同步
 - 多语言切换
 - SNMP
 - TR069
 - 远程 Web 和 Telnet

➤ **呼叫处理**

- 灵活路由规则
- 冗余路由备份/选择
- 按时段控制呼叫路由
- 按主/被叫号码前缀路由
- 按 SIP URL 域匹配路由
- 按 SIP 请求方法匹配路由
- 主被叫号码变换
- IP 中继冗余和均衡负载
- 数字正则表达式

2 安装指导

2.1 安装前准备

2.1.1 安全注意事项

在安装和使用 SBC8000 过程中，用户请遵照下列安全注意事项进行操作，以确保安全。

- 保证安装 SBC8000 服务器远离潮湿及热源；
- 检查并确认服务器供电电源在设备允许的使用范围；
- 请有经验或者受过培训的人员负责安装、维护 SBC8000；

2.1.2 检查机房环境是否维持良好的温/湿度条件

为保证设备正常工作和使用寿命，机房内需维持一定的温度和湿度。

- 机房环境湿度要控制在 10-90%（非冷凝），若湿度过大，则易造成绝缘材料绝缘效果不良甚至漏电，还会产生金属部件锈蚀等现象；若湿度过低，则易产生静电及绝缘垫片干缩而引起的紧固螺丝松动现象；
- 机房环境温度要控制在 0-45℃，若温度过高，则会加速元器件及绝缘材料的老化过程；若温度过低，则可能造成系统运行不稳定。

2.1.3 检查配套设备

- **服务器**

保证安装 SBC8000 的服务器设备运行正常，电源供电稳定。

- **中继线路**

确定已向电信运营商申请了中继线，并已开通。

- **IP 网络**

服务器标准以太网口连接到 IP 网上，与网络上各设备连接。检查 IP 承载网是否就绪，包括路由器、以太网交换机、网线布放情况，以保证服务器可以正确地接入到 IP 网上。

2.2 服务器安装

2.2.1 安装服务器

SBC8000 支持安装在 X86、鲲鹏或云服务器平台，请先按照服务器的安装标准将指定服务器正确安装好，并通过网线连接到 IP 网络上。

2.2.2 安装操作系统

SBC8000 目前支持 Ubuntu18 或 centos7 以上操作系统，请先按照操作系统的安装步骤，将操作系统安装到服务器上，安装完成后通过系统排查一下网络连接是否正常，并创建好虚拟网口，设定好 IP 地址。

2.2.3 安装 SBC8000

SCB8000 软件的安装请联系您所在地的经销商或拨打我司的技术支持热线。

2.2.4 连接到以太网

SBC8000 提供的以太网口是基于服务器的物理网口或安装的操作系统后创建的虚拟网口，网口名称等同于操作系统命名的网口名称。

对 SBC8000 设备的管理既可通过管理网口进行(需要通过 Web 打开相应权限)，也可以通过业务网口进行。当需要隔离设备的管理和设备的业务处理时，才使用管理网口。一般情况下，只使用业务网口连接以太网进行对设备的管理。

2.2.5 故障排查

当服务器连接到千兆以太网后，服务器无法连接到相同以太网的其它设备时，可确定为网络连接故障。网络连接故障的排查一般遵从以下步骤：

步骤 1：观察服务器网口指示灯是否正常；

步骤 2：如果服务器指示灯不正常，那么可以确定为服务器物理网口发生故障；将网线连接到便携机（笔记本电脑或固定计算机），并访问网络，如果便携机（计算机）可以正常访问网络，则可判定服务器网络端口出现故障；

步骤 3：如果服务器通讯正常，可以判定设备接入以太网的网线存在问题，须重新制作；如果服务器通讯失败，那么请通知机房网络管理员，由网络管理员解决。

3

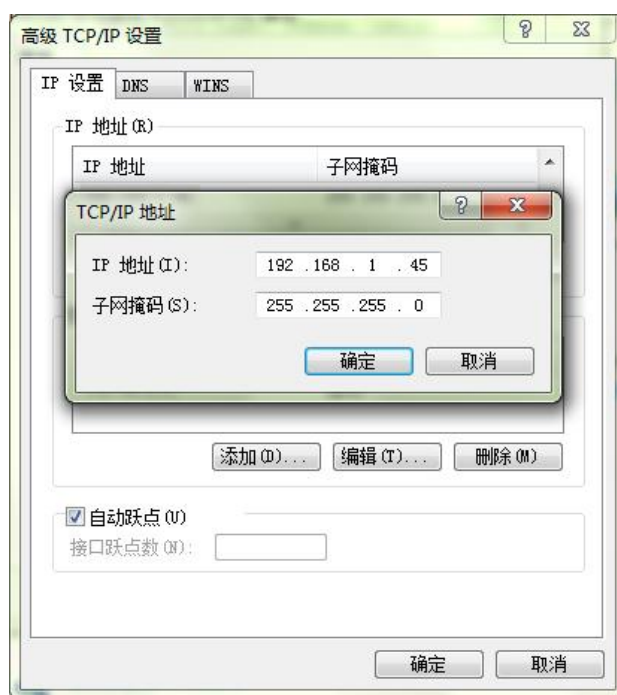
参数配置

3.1 登录

3.1.1 登录准备

SBC8000 提供的以太网口地址与操作系统设置的网口地址 相同，以下用 192.168.11.1 地址来举例。

初次使用设备时，直接找一条网线，将 PC 与 SBC8000 的服务器网口直接连接，点开 PC 的 Internet 协议（TCP/IP）属性界面中的“高级”，添加个 192.168.11.XXX 地址，使 PC 和设备处在同一网段，以便登录到设备的 Web 界面。



3.1.2 登录

在浏览器中用 https 方式输入 IP 地址，即 https:// 192.168.11.1，并在登录页面输入正确的用户名和密码，默认的用户名是 **admin**，密码是 **admin@123#**。



注意

- 1) SBC8000 设备不支持 http 连接，必须采用 https 连接才能登录设备的 Web 页面。
- 2) 如果用户修改默认 IP 地址后忘记了新的 IP 地址而导致不能进入配置页面，

请用串口线将 PC 和 SBC8000 设备的串口连接起来,进入 en 模式,输入 show interface 即可查看设备的 IP 地址。



图 3-1-1 登录界面

输入默认用户名、密码和随机生成的验证码后进入下面的配置页面。为了确保系统安全,当你登录后,建议你进入“系统→用户管理→密码设置”界面及时更改密码。

图 3-1-2 更改密码

3.2 Web 界面结构和导航树

设备 Web 界面正上方是主配置菜单栏,左侧是导航树,右侧显示的是相应节点的具体内容。通过遍历菜单栏和导航树,可以在右侧配置界面完成对设备的查看、修改和配置。

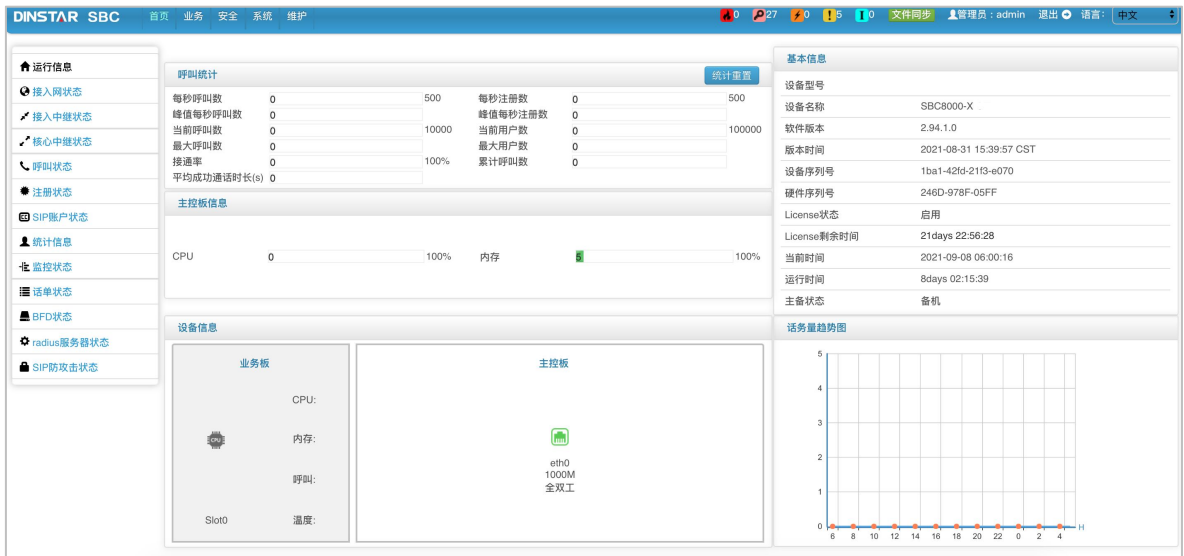


图 3-2-1 首页运行信息界面

配置 SBC8000 一般流程如下图：

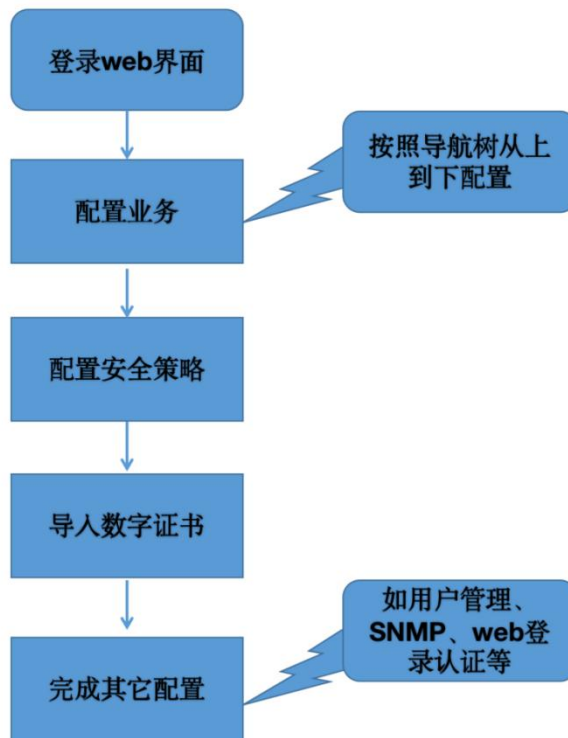


图 3-2-2 配置流程

3.3 首页

3.3.1 运行信息

进入 Web 界面后首先显示的是运行信息。运行信息界面显示了设备的呼叫统计、系统信息、设备信息、基本信息和话务量趋势图。

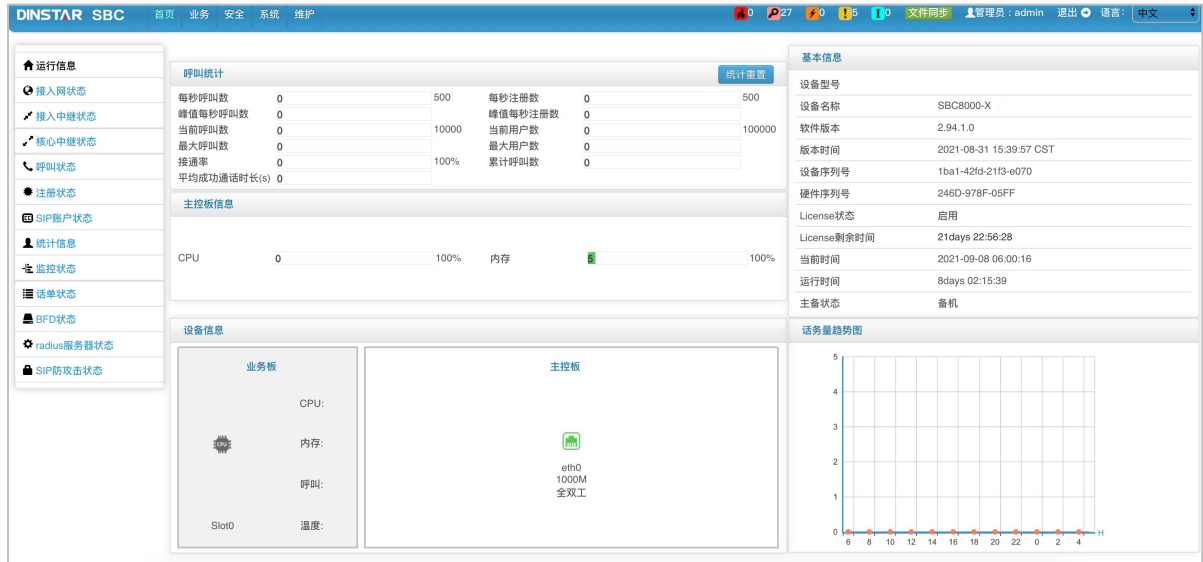


图 3-3-1 设备运行信息

表 3-3-1 呼叫统计的描述

参数	参数描述
每秒呼叫次数	当前时间每秒新增的呼叫次数
峰值每秒呼叫次数	从系统启动运行到现在最大的每秒新增呼叫次数
当前呼叫数	当前正在通话的呼叫次数
平均呼叫接通率	从系统启动运行到现在呼叫成功次数除以全部合法呼叫请求数的百分比
每秒注册数	当前时间点每秒新增的注册请求次数
峰值每秒注册数	从系统启动运行到现在最大的每秒新增注册请求次数
当前用户数	当前注册成功并在线的用户总数
累计呼叫数	从系统启动运行到现在全部合法的呼叫请求数

表 3-3-2 系统信息的描述

参数	参数描述
CPU	当前 CPU 占用率百分比

应用存储区	当前应用存储区占用率百分比
数据存储区	当前数据存储区占用率百分比
内存	当前内存占用率百分比
温度	当前正在使用主控板 CPU 的温度
电源	当前电源输出值
风扇	当前风扇转数

表 3-3-3 设备信息说明

配置项	参数	参数描述
业务板	CPU	当前业务板的 CPU 占用率百分比
	内存	当前业务板的内存占用率百分比
	呼叫	当前业务板的 CPU 正在呼叫的呼叫数
	温度	当前业务板的 CPU 的温度
主控板	网口（Admin/GE0/GE1/GE2/GE3）	主控板具有的网口，其中处于使用状态的网口是绿色，未使用的网口是灰色

表 3-3-4 基本信息说明

参数	参数描述
设备型号	该产品的设备型号为 SBC8000
设备名称	用户可在 Web 界面中“系统→系统设置”页面里修改设备名称
软件版本	当前产品运行的软件版本号
License 状态	在 License 授权期内显示“启用”，过期显示“启用，剩余时间为 0”
License 剩余时间	显示 License 授权剩余时间
当前时间	SBC8000 设备当前的系统时间，用户可以在“系统→时间管理”页面里调整时区或者同步浏览器时间
运行时间	系统本次启动后运行的时长



注意

如果已同步过系统时间，但每次系统启动后当前时间仍然不正确，则表示设备内置电池亏电，需要更换电池；另外，NTP 时间同步，只能通过 Admin 网口进行时间同步。

3.3.2 接入网状态

接入网用于终端用户向 SBC8000 设备注册，接入网状态总是显示为“true”。



图 3-3-2 设备运行信息

表 3-3-5 中继状态描述

参数	参数描述
名称	接入网的名称，名称一般为关键字，添加配置成功后不可修改
状态	接入网的状态总显示为“true”
每秒呼叫数	当前时间每秒新增的呼叫次数
当前用户数	通过该接入网成功注册并在有效期内的总用户数
接通率	系统运行开始到现在，该接入网的总接通率： $(\text{呼叫成功数} / \text{总合法呼叫数}) * 100$
转码连接数	当前接入网正在转码呼叫通话数
呼叫数	当前接入网正在呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数



注意

- 1) 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。
- 2) 接通率、转码连接数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从其他终端用户到该 SBC 设备，目的则表示呼叫从该 SBC 设备到其它终端用户。

3.3.3 接入中继状态

接入网中继通过 SIP Trunk 方式使终端设备对接到 SBC 设备。如果接入网中继未开启心跳和注册，中继状态都显示为“true”；如果接入网中继已开启注册，则以注册结果判断中继

状态；如果已开启心跳策略，则以 option 响应的结果判断中继状态。

名称	状态	呼入				呼出				
		每秒呼叫数	接通率%	当前转码数	呼叫数	注册用户数	接通率%	当前转码数	呼叫数	累计呼叫
1111	true	0	0	0	0	0	0	0	0	0
justtest	true	0	0	0	0	0	0	0	0	0
pchu	true	0	0	0	0	0	0	0	0	0
tgtest	true	0	0	0	0	0	0	0	0	0

图 3-3-3 接入中继状态

表 3-3-6 接入中继状态描述

参数	参数描述
名称	接入网中继的名称，一般为关键字，添加配置成功后不可修改
状态	true: 表示该接入网中继连接正常， false: 则表示该接入网中继连接中断
每秒呼叫数	当前时间每秒新增的呼叫次数
当前用户数	通过该中继成功接入 SBC 设备并在有效期内的总用户数
接通率	系统运行开始至现在，该中继的总接通率： $(\text{呼叫成功数} / \text{总合法呼叫数}) * 100$
转码连接数	当前中继正在转码呼叫通话数
呼叫数	当前中继正在呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数



- 1) 如果该接入网中继未开启心跳和注册，中继状态则都显示为 **true**；如果中继开启注册，则以注册结果判断中继状态；如果开启心跳策略，会以 option 响应的结果判断中继状态。
- 2) 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。
- 3) 接通率、转码连接数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从接入网的其他设备到该 SBC 设备，目的则表示呼叫从该 SBC 设备到接入网的其它设备。

3.3.4 核心中继状态

核心网中继通过 SIP Trunk 方式使核心网的设备对接到 SBC 设备。如果核心网中继未开

启心跳和注册，中继状态都显示为“true”；如果核心网中继已开启注册，则以注册结果判断中继状态；如果已开启心跳策略，则以 option 响应的结果判断中继状态。

名称	状态	呼入					呼出				
		每秒呼叫数	接通率%	当前转码数	呼叫数	累计呼叫	注册用户数	接通率%	当前转码数	呼叫数	累计呼叫
10016	true	0	0	0	0	0	0	0	0	0	0
ag	true	0	0	0	0	0	0	0	0	0	0
sipserver	true	0	0	0	0	0	0	0	0	0	0
lgtestout	true	0	0	0	0	0	0	0	0	0	0

图 3-3-4 核心中继状态

表 3-3-7 核心中继状态描述

参数	参数描述
名称	核心网中继的名称，一般为关键字，添加配置成功后不可修改
状态	true : 表示该核心网中继连接正常， false : 则表示该核心网中继连接中断
每秒呼叫数	当前时间每秒新增的呼叫次数
当前用户数	通过该中继成功接入 SBC 设备并在有效期内的总用户数
接通率	系统运行开始至现在，该中继的总接通率： $(\text{呼叫成功数} / \text{总合法呼叫数}) * 100$
转码连接数	当前中继正在转码呼叫通话数
呼叫数	当前中继正在呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数



- 1) 如果该核心网中继未开启心跳和注册，中继状态则都显示为 true；如果中继开启注册，则以注册结果判断中继状态；如果开启心跳策略，会以 option 响应的结果判断中继状态。
- 2) 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。
- 3) 接通率、转码连接数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从核心网的其他设备到该 SBC 设备，目的则表示呼叫从该 SBC 设备到核心网的其它设备。

3.3.5 呼叫状态

呼叫页面显示的是当前通话的呼叫的状态以及该呼叫的主叫、被叫和通话时长信息。

呼叫状态														
刷新														
10	search:	主叫(来源)	被叫(目的)	名称(源)	名称(目的)	提交								
来源														
状态	媒体端口	通话时长(s)	名称	主叫	被叫	编解码	RTP	远端地址	名称	主叫	被叫	编解码	RTP	远端地址
answer	45668	60	tg53	3333	6666	PCMA	2498/2499	192.168.2.53:13334	tg77	3333	6666	PCMA	2499/2498	172.30.20.77:13426
answer	38716	60	tg53	3333	6666	PCMA	2497/2498	192.168.2.53:13332	tg77	3333	6666	PCMA	2498/2497	172.30.20.77:13424
answer	32816	60	tg53	3333	6666	PCMA	2498/2499	192.168.2.53:13330	tg77	3333	6666	PCMA	2499/2498	172.30.20.77:13422
answer	37156	60	tg53	3333	6666	PCMA	2498/2498	192.168.2.53:13328	tg77	3333	6666	PCMA	2498/2498	172.30.20.77:13420
answer	34434	60	tg53	3333	6666	PCMA	2498/2499	192.168.2.53:13326	tg77	3333	6666	PCMA	2499/2498	172.30.20.77:13418
answer	37096	60	tg53	3333	6666	PCMA	2497/2498	192.168.2.53:13324	tg77	3333	6666	PCMA	2498/2497	172.30.20.77:13416
answer	41118	60	tg53	3333	6666	PCMA	2497/2498	192.168.2.53:13322	tg77	3333	6666	PCMA	2498/2497	172.30.20.77:13414
answer	49028	60	tg53	3333	6666	PCMA	2498/2499	192.168.2.53:13320	tg77	3333	6666	PCMA	2499/2498	172.30.20.77:13412
answer	41808	60	tg53	3333	6666	PCMA	2497/2498	192.168.2.53:13318	tg77	3333	6666	PCMA	2498/2497	172.30.20.77:13410

图 3-3-5 呼叫状态

表 3-3-8 呼叫状态描述:

参数	参数描述
状态	<p>Init: 收到 invite 请求，刚开始初始化该呼叫的控制块的状态；</p> <p>Outgoing: 选路成功，发起呼出呼叫，等待响应；</p> <p>Early: 接收到 18x 响应；</p> <p>Completed: 接收到 2xx 响应，等待 ack；</p> <p>Answer: 接收到 ack，呼叫建立成功</p>
媒体端口	该通话的本地 rtp 端口，如果显示为 0，表示该 rtp 尚未建立成功
通话时长(S)	该呼叫建立成功到现在的时长，以秒为单位显示
名称	该呼叫通过接入网中继、核心网中继或接入网的名称
主叫	该呼叫的主叫号码
被叫	该呼叫的被叫号码
编解码	该通话采用的编解码，如果是转码，来源和目的的编解码会不一致
RTP	该通话接收/发送的 rtp 报文数，5 秒统计一次
远端地址	该通话 rtp 媒体的远端地址和端口

3.3.6 注册状态

注册状态页面显示的是终端设备向 SBC 设备注册的状态。

注册状态											刷新
10	search:	用户名	来源名称	提交							
状态	用户名	刷新时间	名称	来源			目的				
				注册间隔	地址/NAT地址	协议	名称	注册间隔	地址/NAT地址	协议	
registered	1965	3236	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1971	3236	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1972	3236	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1223	3236	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1224	3236	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1220	3235	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1182	3235	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1229	3235	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	
registered	1961	3235	reg464	60	192.168.4.12:5060/192.168.2.16:1024	udp	fs100160	3600	172.30.100.160:5060/172.30.100.160:5060	udp	

图 3-3-6 注册状态

表 3-3-9 注册状态描述

参数	参数描述
状态	Registering: 接收到终端设备发出的注册请求, 正在处理 registered: 接收到注册成功响应, 并在注册有效期内
用户名	终端设备注册时使用的用户名
刷新时间	SBC 设备需要向服务器刷新注册的剩余时间
名称	来源名称表示该注册是通过哪个接入网注册的; 目的名称表示该注册是向那个核心网中继注册的
注册间隔	来源注册间隔表示终端设备注册到 SBC 的 Expire 时间, 目的注册间隔表示 SBC 向核心网中继注册的 Expire 时间
地址/NAT 地址	对端设备的地址和 NAT 地址

3.3.7 SIP 账户状态

SIP 账户状态显示的是 SBC 自身 SIP 账户向服务器注册状态, SIP 账户配置参考业务→高级配置→SIP 账户:

序号	状态	名称	用户名	端点	当前并发数	最大并发数	使用次数
1	registering	mos	1780100	10016	0	5	0
2	registering	mos	178099	10016	0	5	0
3	registering	mos	178098	10016	0	5	0
4	registering	mos	178097	10016	0	5	0
5	registering	mos	178096	10016	0	5	0
6	registering	mos	178095	10016	0	5	0
7	registering	mos	178094	10016	0	5	0
8	registering	mos	178093	10016	0	5	0
9	registering	mos	178092	10016	0	5	0
10	registering	mos	178091	10016	0	5	0

图 3-3-7 SIP 账户状态

表 3-3-10 注册状态描述

参数	参数描述
状态	Registering: 接收到终端设备发出的注册请求，正在处理 registered: 接收到注册成功响应，并在注册有效期内
用户名	终端设备注册时使用的用户名
刷新时间	SBC 设备需要向服务器刷新注册的剩余时间
名称	来源名称表示该注册是通过哪个接入网注册的；目的名称表示该注册是向那个核心网中继注册的
端点	该 SIP 账户应用于对应的接入网中继或核心中继
当前并发数	当前该 SIP 账户正在被使用的呼叫数
最大并发数	SIP 账户最大同时使用的数量
使用次数	该 SIP 账户历史使用次数总和

统计信息

统计信息显示网口或端点的当前流量/历史流量、设备的历史呼叫统计、设备呼叫挂断原因统计。

1) 流量

可显示当前流量数据和历史流量数据

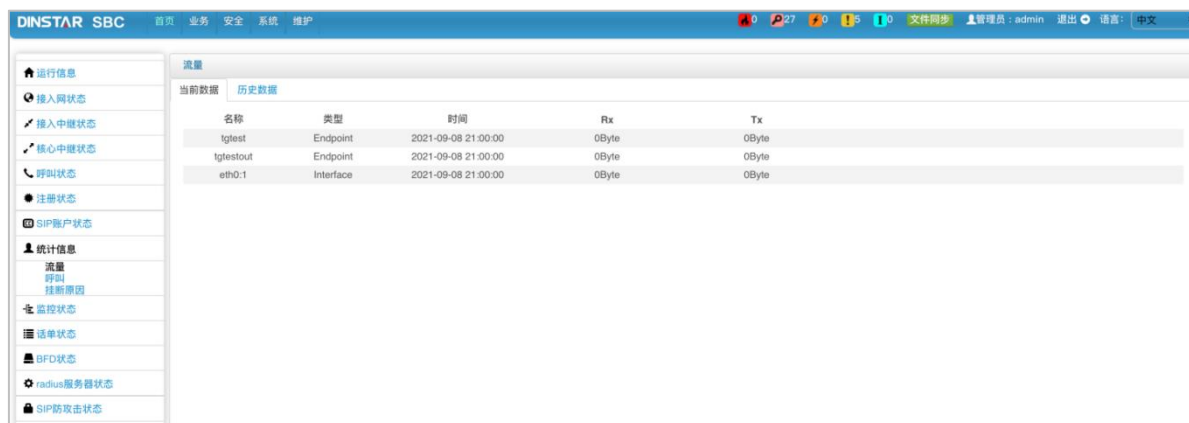


图 3-3-8 当前流量数据

历史流量数据可以按时间段查询设备指定时间段的历史流量数据，通过线段图表示，红色为发送数据，蓝色为接收数据

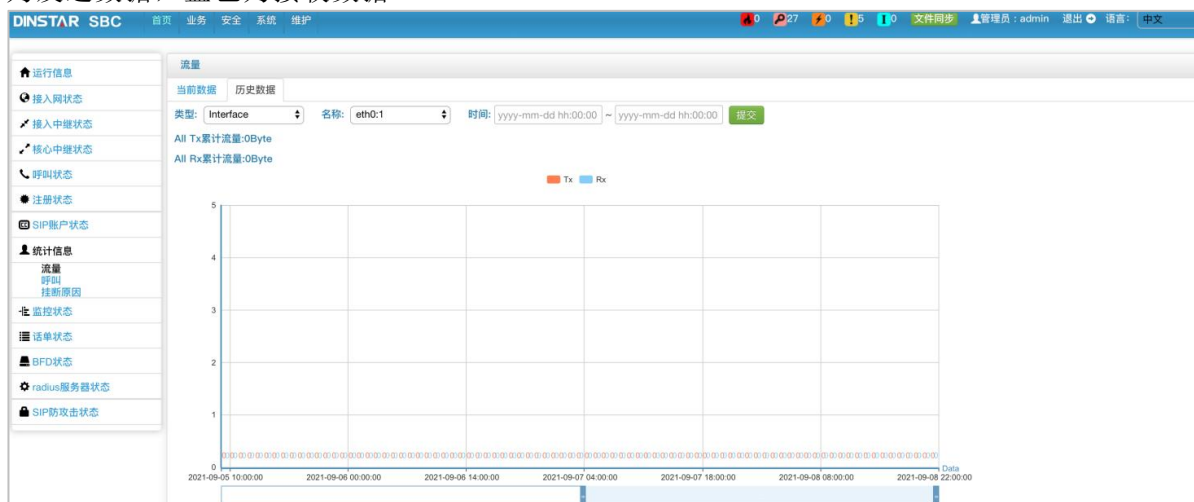


图 3-3-9 历史流量数据

2) 呼叫

呼叫统计显示设备历史呼叫数据，通过线段图表示，红色为总呼叫数（含成功与失败数），蓝色为总成功呼叫数

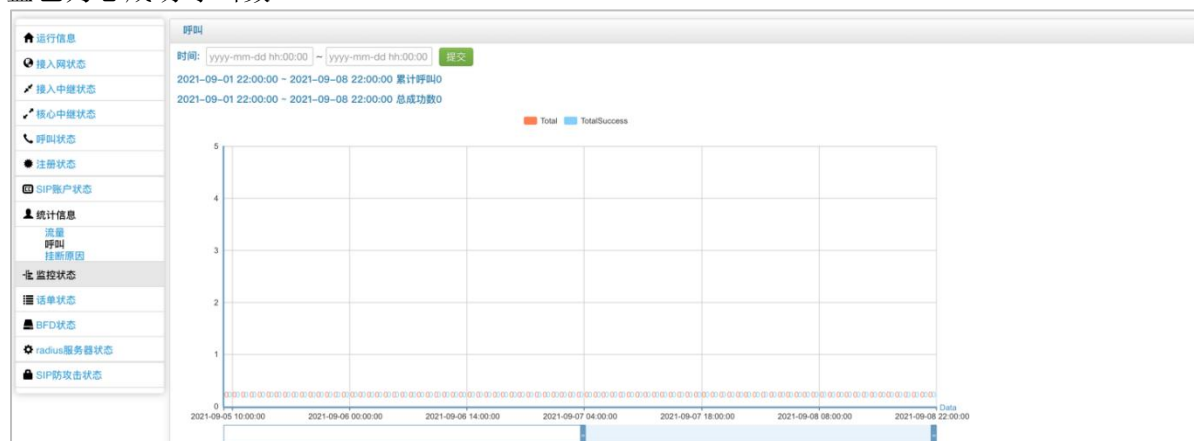


图 3-3-10 呼叫统计

3) 挂断原因

挂断原因统计设备所有呼叫通过何种响应结束通话的数据，以表格和饼状图表示：

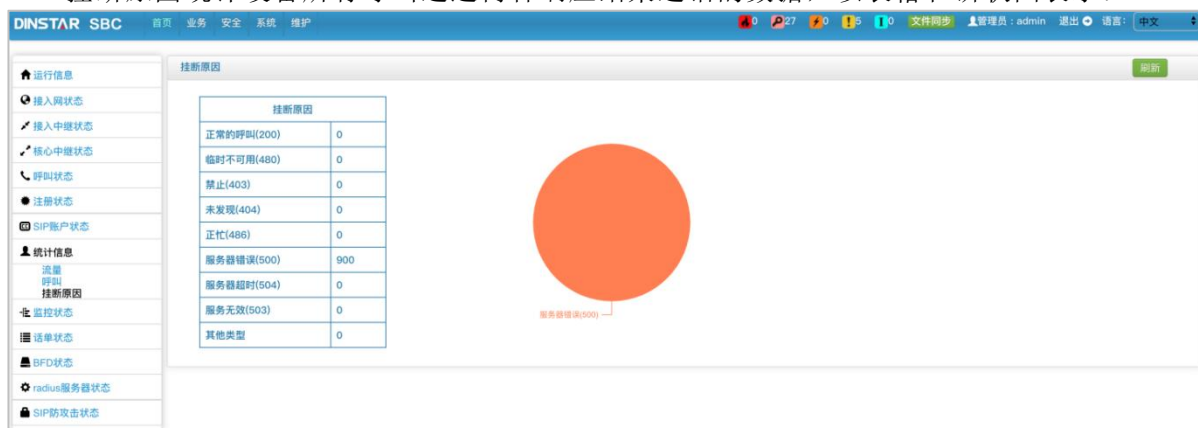


图 3-3-11 挂断原因统计

3.3.8 监控状态

监控状态统计历史呼叫的媒体通话质量，包括统计延时、丢包、抖动，并对通话质量进行评判



图 3-3-12 监控状态

3.3.9 话单状态

话单状态统计设备的呼叫历史话单记录：

话单状态											
呼入											
创建时间	通话时长(s)	名称	主叫	被叫	编解码	RTP	呼出				
							名称	主叫	被叫	编解码	RTP
2021-09-01 05:08:25	87	lgtest	123425631 187	018359488 751		0	lgtestout	123425631 187	018359488 751		0
2021-09-01 05:08:54	58	lgtest	123469824 927	018377280 252		0	lgtestout	123469824 927	018377280 252		0
2021-09-01 05:07:59	113	lgtest	123452990 194	018319323 039		0	lgtestout	123452990 194	018319323 039		0
2021-09-01 05:09:08	44	lgtest	123453909 509	018378351 836		0	lgtestout	123453909 509	018378351 836		0
2021-09-01 05:09:02	50	lgtest	123469857 650	018359140 922		0	lgtestout	123469857 650	018359140 922		0
2021-09-01 05:07:54	118	lgtest	123473939 344	018339959 254		0	lgtestout	123473939 344	018339959 254		0
2021-09-01 05:08:26	85	lgtest	123414711 564	018327629 495		0	lgtestout	123414711 564	018327629 495		0
2021-09-01 05:09:05	47	lgtest	123435709 546	018372097 067		0	lgtestout	123435709 546	018372097 067		0
2021-09-01	-	-	123476332	018351439	-	-	-	123476332	018351439	-	-

图 3-3-13 话单状态

3.3.10 BFD 状态

BFD 状态只在双机热备情况下有用。在双机热备时，热备的两个设备通过 BFD 报文握手，BFD 状态统计双机热备两个设备的当前连接状态、BFD 发送次数、BFD 报文丢包率、断链次数、BFD 报文的发送/接收间隔：

会话key	当前状态	运行时间	断链次数	当前丢包率	当前接收间隔

图 3-3-14 BFD 状态

3.3.11 radius 状态

显示 radius 话单服务器的连接状态，发送话单总数等：



图 3-3-15 radius 状态

3.3.12 SIP 防攻击状态

当某个 SIP 账户或 SIP 来源地址被判断为攻击时，SBC 会根据动作对改账户或地址进行处理，SIP 防攻击状态显示 SBC 受 SIP 攻击时被 block 的账户或 IP 地址：

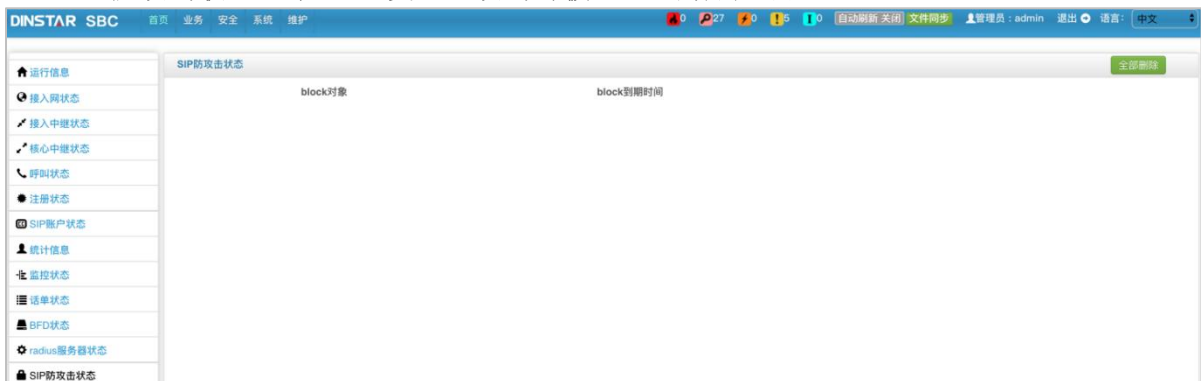


图 3-3-16 SIP 防攻击状态

表 3-3-11 攻击列表描述

参数	参数描述
block 对象	被 block 的账户或地址
block 到期时间	SIP 账户或地址只会被 block 一段时间，到期后 SBC 会重新接收访 SIP 账户或 IP 地址的 SIP 请求，并重新判断是否为攻击

3.4 业务配置

业务配置包括基本业务配置和高级业务配置：

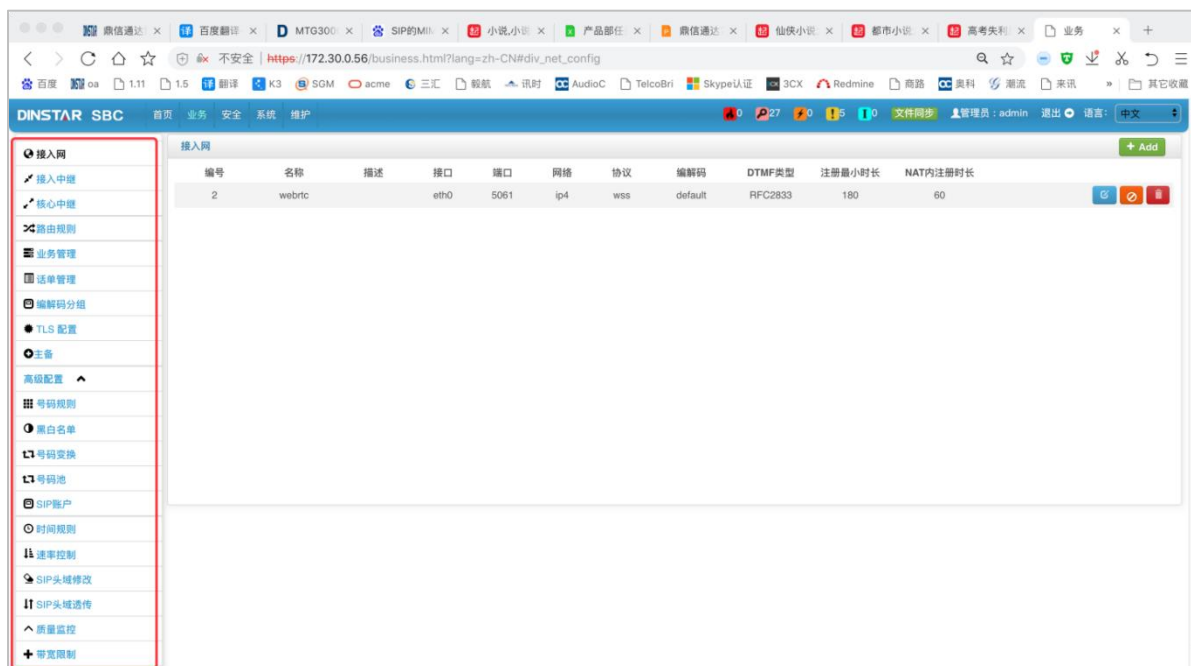


图 3-4-1 业务配置树形菜单

3.4.1 接入网

接入网用于配置允许配置终端通过 SBC 向软交换注册的接入域和各种参数。

编号 *	2
名称 *	webrtc
描述	
启用	<input checked="" type="checkbox"/>
启用radius	<input type="checkbox"/>
接口	eth0
媒体接口	eth0
协议	WSS
国密	<input type="checkbox"/>
PEM文件 *	
KEY文件 *	
端口 *	5061
网络	IPV4
IP地址段过滤	
子网掩码	
编解码	default
DTMF优先级	本地
DTMF类型	RFC2833
RFC2833净荷 *	101

高级配置 ^

带宽限制	0	Mbit/s	
信令DSCP	BE		
音频媒体DSCP	BE		
视频媒体DSCP	BE		
近端NAT			
刷新媒体透传	<input checked="" type="checkbox"/>		
响应多媒体刷新支持	<input type="checkbox"/>		
初始invite携带sdp	<input type="checkbox"/>		
单账户多设备注册	<input type="checkbox"/>		

+ 域名过滤

速率控制	default
主叫黑名单	
主叫白名单	
被叫黑名单	
被叫白名单	
入局号码变换	
入局SIP消息变换	
出局SIP消息变换	

Session Timer	Disable
注册最小时长	180 s
NAT内注册时长	60 s
PRACK	Disable
远端媒体发送地址	Unlock
远端媒体接收地址刷新	Enable
远端信令地址	Unlock
主叫号码提取方式	User
被叫号码提取方式	User

OPTIONS INFO
 REFER NOTIFY
 SUBSCRIBE UPDATE
 MESSAGE

保存
取消

图 3-4-2 接入网页面

表 3-4-1 接入网

参数	参数描述
名称	配置接入网的名字，用户自定义，添加成功后不可修改
描述	该接入网的描述，用户可以较为详细描述该接入网的作用和规则
启用	该接入网是否启用，新增时默认启用，如果不启动，则代表该接入网被禁用，对应的 SIP 监听端口会被关闭
启用 radius	是否启用 radius 计费
接口	接入网配置的 SIP 信令接口，对应接口参考系统→网络管理
媒体接口	SBC 支持信令媒体接口分离，对应接口参考系统→网络管理
端口	该接入网在本设备 eth0 口上的 SIP 监听端口，端口号在 eth0 口上唯一
网络	配置该接入网采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
协议	该接入网采用的传输协议:UDP/TCP/TLS/WSS,其中 TLS/WSS 需要指定对应的数字证书，参考系统→数字证书管理
网络	SBC 支持 IPV4/IPV6 两种网络
IP 地址过滤	IPV4 网络中可配置接收 SIP 请求的合法来源 IP 地址范围
子网掩码	IPV4 网络中可配置 IP 地址范围的子网掩码
编解码	配置从该接入网呼入或呼出支持的编解码格式，参考业务→编解码分组
DTMF 优先级	DTMF 协商时，如果对端和本地配置的 DTMF 不一致，SBC 会根据配置以对端还是本地 DTMF 类型为优先
DTMF 类型	DTMF 类型支持三种：RFC2833、SIP INFO、inband
带宽限制	限制该接入网的最大带宽
信令 DSCP	SIP 信令报文 QoS 标志配置
音频媒体 DSCP	音频媒体报文 QoS 标志配置
视频媒体 DSCP	视频媒体报文 QoS 标志配置
近端 NAT	近端 nat：设备在 nat 内部，在信令中需要带上 nat 的地址和对应的端口，默认不启用，在这里，启用时默认只需要配置对应防火墙出口 IP 地址即可，如果防火墙做了对应的端口变换，则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口（  说明）
刷新媒体透传	SBC 收到 update 信息时是否透传到另外一端，根据另外一端响应刷新媒体，还是 SBC 本身自己处理并响应 update 请求
响应多媒体刷新支持	响应 200ok 携带的 sdp 中不止一种编解码。我们是否携带一种编解码发起 reinvite 协商，还是直接自己选一种编解码通信。
初始 invite 携带	初始客户端的 invite 没有携带 sdp，经过 sbc 以后转发出去的 invite 是

sdp	否携带 sdp，勾选就会带 sdp
单账户多设备注册	同一个账户只允许一个设备注册，一个设备注册以后，其他的设备再注册直接拒绝。勾选允许的话，其他设备也能注册。sbc 使用的时候优先选最后注册的那个地址
域名过滤	启用域名过滤，SBC 会根据设置的域名条件，判断 to 头域携带的域名地址时（携带 IP 地址不做判断）是否符合要求，to 头域域名不符合过滤条件时，SBC 会拒绝该请求
速率控制	配置该接入网每秒最大注册、呼叫量和总呼叫量，参考业务→高级配置→速率控制
主叫黑名单	配置不允许从该接入网呼入时主叫号码黑名单，如果接入网配置了黑名单，在黑名单内的主叫号码都不能通过该接入网呼入，参考业务→高级配置→黑白名单
主叫白名单	配置允许从该接入网呼入时主叫号码白名单，如果接入网配置了白名单，只有白名单内的主叫号码才能通过该接入网呼入，参考业务→高级配置→黑白名单
被叫黑名单	配置不允许从该接入网呼入时被叫号码黑名单，如果接入网配置了黑名单，在黑名单内的被叫号码都不能通过该接入网呼入，参考业务→高级配置→黑白名单
被叫白名单	配置允许从该接入网呼入时被叫号码白名单，如果接入网配置了白名单，只有白名单内的被叫号码才能通过该接入网呼入，参考业务→高级配置→黑白名单
入局号码变换	配置从该接入网呼入时的号码变换规则（仅呼入，从该中继呼出该规则不生效），参考业务→高级配置→号码变换
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式，系统可根据配置选择对应的发送模式，一通电话如果 SBC 两侧的 dtmf 方式不一致，会通过 DSP 转换
入局 SIP 消息变换	即从该接入网呼入时的 SIP 头域修改，参考业务→高级配置→SIP 头域变换
出局 SIP 消息变换	即从该接入网呼出时的 SIP 头域修改，参考业务→高级配置→SIP 头域变换
Session Timer	会话定时器，是一种会话保存激活的机制，如果启用，SBC 会在会话周期内发送 reinvite 报文保持会话激活，如果在会话周期内未检测到该消息，则认为会话已经终止，系统会主动拆除该会话。如果采用的是 require 模式，通过该接入网呼出时，必须要求被叫也支持 timer
注册最小时长	终端注册的允许的最小时长，如果终端注册 REGISTER 报文中 expires 值小于这个值，SBC 可能会拒绝该注册请求
NAT 内注册时长	SBC 如果发现终端在 NAT 下，则 SBC 响应的注册时长会自动变为该值，NAT 内注册时长值一般比较小，以免 NAT 地址发生变化时 SBC 不能及时发现。
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制，可参考

	RFC3262 文档。配置为 <code>disable</code> 时，SBC 发送的请求或 <code>1xx</code> 响应默认都不带 <code>100rel</code> ；配置为 <code>support</code> 时，SBC 的请求或 <code>1xx</code> 响应会在 <code>supported</code> 域里带上 <code>100rel</code> ；配置为 <code>require</code> 时，SBC 的请求或 <code>1xx</code> 响应会在 <code>require</code> 域带上 <code>100rel</code> ，如果对端不支持，则响应 <code>420</code> ，如果支持，则会在收到 <code>1xx</code> 响应时，发送 <code>PRACK</code> 消息回来。
远端媒体地址	启用远端媒体地址锁定：当远端设备在公网时，那么锁定的就是 <code>sdp</code> 中的媒体地址；在私网时，就是动态锁定，要连续收到 30 个报文后就锁定该报文的原地址
远端信令地址	启用信令锁定：账户注册成功后，只接收该账户的主叫注册时同样地址来的呼叫报文
主叫号码提取方式	<code>user</code> : 提取 <code>invite</code> 报文 <code>from</code> 域中 <code>user</code> 字段作为主叫 <code>display</code> : 提取 <code>invite</code> 报文 <code>from</code> 域中 <code>display</code> 字段作为主叫
被叫号码提取方式	<code>user</code> : 提取 <code>invite</code> 报文 <code>to</code> 域中 <code>user</code> 字段作为被叫 <code>display</code> : 提取 <code>invite</code> 报文 <code>to</code> 域中 <code>display</code> 字段作为被叫 <code>request-uri</code> : 提取 <code>invite</code> 报文 <code>request-uri</code> 的中的 <code>user</code> 号码作为被叫
SIP 方法	配置该接入网允许接收的 SIP 请求方法，如果未启用对应的 SIP 请求方法，系统收到对应的 SIP 请求时，会直接拒绝。 <code>INVITE/REGISTER</code> 和拆除会话请求默认允许。



说明

配置静态 NAT 时，默认 SIP 和 RTP 起始端口为空即可，如果防火墙做了对应的端口映射，则需要根据映射规则进行配置（举个例子）：

- 1) SIP 端口：一条中继本地端口为 5061，但防火墙将公网的 5061 端口映射成 8888，则在静态 NAT 的 SIP 端口配置为 8888；
- 2) RTP 起始端口：SBC 默认的 RTP 起始端口为 32768，如果防火墙将 32768-50000 端口映射为 12768-30000，在静态 NAT 的 RTP 起始端口配置为 12768，也就是以 32768 为基准，根据防火墙端口映射规则进行基准偏移。

3.4.2 接入中继

配置 SBC 设备通过中继对接到接入网终端的服务器和相关参数。

编号 *	<input type="text" value="1"/>
名称 *	<input type="text" value="pchu"/>
描述	<input type="text" value="pchu"/>
启用	<input checked="" type="checkbox"/>
启用radius	<input type="checkbox"/>
接口	<input type="text" value="eth0:1"/>
媒体接口	<input type="text" value="eth0:1"/>
协议	<input type="text" value="UDP"/>
端口 *	<input type="text" value="5068"/>
网络	<input type="text" value="IPV4"/>
编解码	<input type="text" value="default"/>
DTMF优先级	<input type="text" value="本地"/>
DTMF类型	<input type="text" value="RFC2833"/>
RFC2833净荷 *	<input type="text" value="101"/>
中继模式	<input type="text" value="Static"/>
远端地址和端口 *	<input type="text" value="172.23.234.100:5068"/>
高级配置 ^	

带宽限制	<input type="text" value="0"/> Mbit/s <input type="text"/>
信令DSCP	<input type="text" value="BE"/>
音频媒体DSCP	<input type="text" value="BE"/>
视频媒体DSCP	<input type="text" value="BE"/>
近端NAT	<input type="text"/>
刷新媒体透传	<input checked="" type="checkbox"/>
响应多媒体刷新支持	<input type="checkbox"/>
初始invite携带sdp	<input type="checkbox"/>
本地处理去注册	<input type="checkbox"/>
速率控制	<input type="text" value="default"/>
主叫黑名单	<input type="text"/>
主叫白名单	<input type="text"/>
被叫黑名单	<input type="text"/>
被叫白名单	<input type="text"/>
入局号码变换	<input type="text"/>

入局SIP消息变换	<input type="text"/>
出局SIP消息变换	<input type="text"/>
SIP账户	<input type="text"/>
远端服务器域名	<input type="text"/>
接入访问ACL表	<input type="text"/>

接入访问ACL表	IP:支持正则	:	Port:支持正则	Del
	<input type="button" value="+ Add"/>			
注册	<input type="checkbox"/>			
OutBound Proxy	<input type="text"/>			
心跳策略	<input type="checkbox"/>			
Session Timer	<input type="text" value="Disable"/>			
PRACK	<input type="text" value="Disable"/>			
远端媒体发送地址	<input type="text" value="Unlock"/>			
远端媒体接收地址刷新	<input type="text" value="Enable"/>			
主叫号码提取方式	<input type="text" value="User"/>			
被叫号码提取方式	<input type="text" value="User"/>			
SIP方法	<input checked="" type="checkbox"/> OPTIONS <input checked="" type="checkbox"/> INFO <input checked="" type="checkbox"/> REFER <input checked="" type="checkbox"/> NOTIFY <input checked="" type="checkbox"/> SUBSCRIBE <input checked="" type="checkbox"/> UPDATE <input checked="" type="checkbox"/> MESSAGE			
	<input type="button" value="保存"/> <input type="button" value="取消"/>			

图 3-4-3 接入中继页面

表 3-4-2 接入中继

参数	参数描述
名称	配置接入中继的名字，用户自定义，添加成功后不可修改
描述	该接入中继的描述，用户可以较为详细描述该接入网的作用和规则
启用	该接入中继是否启用，新增时默认启用，如果不启动，则代表该接入中继被禁用，对应的 SIP 监听端口会被关闭
启用 radius	是否启用 radius 计费
接口	接入中继配置的 SIP 信令接口，对应接口参考系统→网络管理
媒体接口	SBC 支持信令媒体接口分离，对应接口参考系统→网络管理

端口	该接入中继在本设备 eth0 口上的 SIP 监听端口, 端口号在 eth0 口上唯一
网络	配置该接入中继采用的是 IPV4 还是 IPV6 网络, 默认为 IPV4
协议	该接入中继采用的传输协议:UDP/TCP/TLS/WSS, 其中 TLS/WSS 需要指定对应的数字证书, 参考系统→数字证书管理
网络	SBC 支持 IPV4/IPV6 两种网络
IP 地址过滤	IPV4 网络中可配置接收 SIP 请求的合法来源 IP 地址范围
子网掩码	IPV4 网络中可配置 IP 地址范围的子网掩码
编解码	配置从该接入中继呼入或呼出支持的编解码格式, 参考业务→编解码分组
DTMF 优先级	DTMF 协商时, 如果对端和本地配置的 DTMF 不一致, SBC 会根据配置以对端还是本地 DTMF 类型为优先
DTMF 类型	DTMF 类型支持三种: RFC2833、SIP INFO、inband
中继模式	支持 static 和 dynamic: Static: 对接的 IP 地址和端口是固定的 Dynamic: 对接的对端地址不固定, 对端通过配置的 SIP 账户密码注册过来, 注册成功后再获取对端的 IP 地址和端口
带宽限制	限制该接入中继的最大带宽
信令 DSCP	SIP 信令报文 QoS 标志配置
音频媒体 DSCP	音频媒体报文 QoS 标志配置
视频媒体 DSCP	视频媒体报文 QoS 标志配置
近端 NAT	近端 nat: 设备在 nat 内部, 在信令中需要带上 nat 的地址和对应的端口, 默认不启用, 在这里, 启用时默认只需要配置对应防火墙出口 IP 地址即可, 如果防火墙做了对应的端口变换, 则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口 ( 说明)
刷新媒体透传	SBC 收到 update 信息时是否透传到另外一端, 根据另外一端响应刷新媒体, 还是 SBC 本身自己处理并响应 update 请求
响应多媒体刷新支持	响应 200ok 携带的 sdp 中不止一种编解码。我们是否携带一种编解码发起 reinvite 协商, 还是直接自己选一种编解码通信。
初始 invite 携带 sdp	初始客户端的 invite 没有携带 sdp, 经过 sbc 以后转发出去的 invite 是否携带 sdp, 勾选就会带 sdp
本地处理去注册	启用本地处理去注册后, 通过 SBC 向服务器注册的账户, 在租期内发起去注册请求时, SBC 自行处理去注册请求, 不向服务器转发去注册请求, 如果不启用, SBC 收到去注册请求时会转发该请求, 由服务器处理
速率控制	配置该接入中继每秒最大注册、呼叫量和总呼叫量, 参考业务→高级

	配置→速率控制
主叫黑名单	配置不允许从该接入中继呼入时主叫号码黑名单，如果接入中继配置了黑名单，在黑名单内的主叫号码都不能通过该接入中继呼入，参考业务→高级配置→黑白名单
主叫白名单	配置允许从该接入中继呼入时主叫号码白名单，如果接入中继配置了白名单，只有白名单内的主叫号码才能通过该接入中继呼入，参考业务→高级配置→黑白名单
被叫黑名单	配置不允许从该接入中继呼入时被叫号码黑名单，如果接入中继配置了黑名单，在黑名单内的被叫号码都不能通过该接入中继呼入，参考业务→高级配置→黑白名单
被叫白名单	配置允许从该接入中继呼入时被叫号码白名单，如果接入中继配置了白名单，只有白名单内的被叫号码才能通过该接入中继呼入，参考业务→高级配置→黑白名单
入局号码变换	配置从该接入中继呼入时的号码变换规则（仅呼入，从该中继呼出该规则不生效），参考业务→高级配置→号码变换
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式，系统可根据配置选择对应的发送模式，一通电话如果 SBC 两侧的 dtmf 方式不一致，会通过 DSP 转换
入局 SIP 消息变换	即从该接入中继呼入时的 SIP 头域修改，参考业务→高级配置→SIP 头域变换
出局 SIP 消息变换	即从该接入中继呼出时的 SIP 头域修改，参考业务→高级配置→SIP 头域变换
SIP 账户	SBC 自身像服务器发起注册的账户，参考业务→高级配置→SIP 账户
远端服务器域名	配置了域名，SBC 发送请求时，request 行会用该域名替换 ip 地址
接入访问 ACL 表	该中继除配置指定的远端 IP 地址外，允许接入的 ACL 规则表
注册	启用注册后，该中继会根据配置的 SIP 账户密码向本中继的远端服务器发起注册。注意：中继模式为 dynamic 时不可使用
OutBound Proxy	Outbound 代理地址
心跳策略	配置中继的 option 心跳策略：心跳超时次数、心跳发送间隔、和是否仅认为响应为 200ok 的 option 请求为有效心跳握手
Session Timer	会话定时器，是种会话保存激活的机制，如果启用，SBC 会在会话周期内发送 reinvite 报文保持会话激活，如果在会话周期内未检测到该消息，则认为会话已经终止，系统会主动拆除该会话。如果采用的是 require 模式，通过该接入中继呼出时，必须要求被叫也支持 timer
注册最小时长	终端注册的允许的最小时长，如果终端注册 REGISTER 报文中 expires 值小于这个值，SBC 可能会拒绝该注册请求
NAT 内注册时长	SBC 如果发现终端在 NAT 下，则 SBC 响应的注册时长会自动变为该值，NAT 内注册时长值一般比较小，以免 NAT 地址发生变化时 SBC

	不能及时发现。
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制,可参考 RFC3262 文档。配置为 disable 时, SBC 发送的请求或 1xx 响应默认都不带 100rel;配置为 support 时, SBC 的请求或 1xx 响应会在 supported 域里带上 100rel;配置为 require 时, SBC 的请求或 1xx 响应会在 require 域带上 100rel, 如果对端不支持, 则响应 420, 如果支持, 则会在收到 1xx 响应时, 发送 PRACK 消息回来。
远端媒体地址	启用远端媒体地址锁定: 当远端设备在公网时, 那么锁定的就是 sdp 中的媒体地址; 在私网时, 就是动态锁定, 要连续收到 30 个报文后就锁定该报文的原地址
远端信令地址	启用信令锁定: 账户注册成功后, 只接收该账户的主叫注册时同样地址来的呼叫报文
主叫号码提取方式	user: 提取 invite 报文 from 域中 user 字段作为主叫 display: 提取 invite 报文 from 域中 display 字段作为主叫
被叫号码提取方式	user: 提取 invite 报文 to 域中 user 字段作为被叫 display: 提取 invite 报文 to 域中 display 字段作为被叫 request-uri: 提取 invite 报文 request-uri 的中的 user 号码作为被叫
SIP 方法	配置该接入中继允许接收的 SIP 请求方法, 如果未启用对应的 SIP 请求方法, 系统收到对应的 SIP 请求时, 会直接拒绝。INVITE/REGISTER 和拆除会话请求默认允许。

3.4.3 核心网中继

配置 SBC 设备通过中继对接到核心网的服务器和相关参数。

编号	*	1
名称	*	pchu
描述		pchu
启用		<input checked="" type="checkbox"/>
启用radius		<input type="checkbox"/>
接口		eth0:1
媒体接口		eth0:1
协议		UDP
端口	*	5068
网络		IPV4

编解码	default
DTMF优先级	本地
DTMF类型	RFC2833
RFC2833净荷 *	101
中继模式	Static
远端地址和端口 *	172.23.234.100:5068
高级配置 ^	

带宽限制	0	Mbit/s
信令DSCP	BE	
音频媒体DSCP	BE	
视频媒体DSCP	BE	
近端NAT		
刷新媒体透传	<input checked="" type="checkbox"/>	
响应多媒体刷新支持	<input type="checkbox"/>	
初始invite携带sdp	<input type="checkbox"/>	
本地处理去注册	<input type="checkbox"/>	
速率控制	default	
主叫黑名单		
主叫白名单		
被叫黑名单		
被叫白名单		
入局号码变换		
入局SIP消息变换		
出局SIP消息变换		
SIP账户		
远端服务器域名		
接入访问ACL表		

接入访问ACL表 :

注册

OutBound Proxy

心跳策略

Session Timer

PRACK

远端媒体发送地址

远端媒体接收地址刷新

主叫号码提取方式

被叫号码提取方式

SIP方法

OPTIONS INFO

REFER NOTIFY

SUBSCRIBE UPDATE

MESSAGE

图 3-4-4 核心中继页面

表 3-4-3 核心中继

参数	参数描述
名称	配置核心中继的名字，用户自定义，添加成功后不可修改
描述	该核心中继的描述，用户可以较为详细描述该核心中继的作用和规则
启用	该核心中继是否启用，新增时默认启用，如果不启动，则代表该核心中继被禁用，对应的 SIP 监听端口会被关闭
启用 radius	是否启用 radius 计费
接口	核心中继配置的 SIP 信令接口，对应接口参考系统→网络管理
媒体接口	SBC 支持信令媒体接口分离，对应接口参考系统→网络管理
端口	该核心中继在本设备 eth0 口上的 SIP 监听端口，端口号在 eth0 口上唯一
网络	配置该核心中继采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
协议	该核心中继采用的传输协议:UDP/TCP/TLS/WSS,其中 TLS/WSS 需要指定对应的数字证书，参考系统→数字证书管理
网络	SBC 支持 IPV4/IPV6 两种网络
IP 地址过滤	IPV4 网络中可配置接收 SIP 请求的合法来源 IP 地址范围

子网掩码	IPV4 网络中可配置 IP 地址范围的子网掩码
编解码	配置从该核心中继呼入或呼出支持的编解码格式，参考业务→编解码分组
DTMF 优先级	DTMF 协商时，如果对端和本地配置的 DTMF 不一致，SBC 会根据配置以对端还是本地 DTMF 类型为优先
DTMF 类型	DTMF 类型支持三种：RFC2833、SIP INFO、inband
中继模式	支持 static 和 dynamic: Static: 对接的 IP 地址和端口是固定的 Dynamic: 对接的对端地址不固定，对端通过配置的 SIP 账户密码注册过来，注册成功后再获取对端的 IP 地址和端口
带宽限制	限制该核心中继的最大带宽
信令 DSCP	SIP 信令报文 QoS 标志配置
音频媒体 DSCP	音频媒体报文 QoS 标志配置
视频媒体 DSCP	视频媒体报文 QoS 标志配置
近端 NAT	近端 nat: 设备在 nat 内部，在信令中需要带上 nat 的地址和对应的端口，默认不启用，在这里，启用时默认只需要配置对应防火墙出口 IP 地址即可，如果防火墙做了对应的端口变换，则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口 ( 说明)
刷新媒体透传	SBC 收到 update 信息时是否透传到另外一端，根据另外一端响应刷新媒体，还是 SBC 本身自己处理并响应 update 请求
响应多媒体刷新支持	响应 200ok 携带的 sdp 中不止一种编解码。我们是否携带一种编解码发起 reinvite 协商，还是直接自己选一种编解码通信。
初始 invite 携带 sdp	初始客户端的 invite 没有携带 sdp，经过 sbc 以后转发出去的 invite 是否携带 sdp，勾选就会带 sdp
本地处理去注册	启用本地处理去注册后，通过 SBC 向服务器注册的账户，在租期内发起去注册请求时，SBC 自行处理去注册请求，不向服务器转发去注册请求，如果不启用，SBC 收到去注册请求时会转发该请求，由服务器处理
速率控制	配置该核心中继每秒最大注册、呼叫量和总呼叫量，参考业务→高级配置→速率控制
主叫黑名单	配置不允许从该核心中继呼入时主叫号码黑名单，如果核心中继配置了黑名单，在黑名单内的主叫号码都不能通过该核心中继呼入，参考业务→高级配置→黑白名单
主叫白名单	配置允许从该核心中继呼入时主叫号码白名单，如果核心中继配置了白名单，只有白名单内的主叫号码才能通过该核心中继呼入，参考业务→高级配置→黑白名单
被叫黑名单	配置不允许从该核心中继呼入时被叫号码黑名单，如果核心中继配置了黑名单，在黑名单内的被叫号码都不能通过该核心中继呼入，参考业务

	→高级配置→黑白名单
被叫白名单	配置允许从该核心中继呼入时被叫号码白名单,如果核心中继配置了白名单,只有白名单内的被叫号码才能通过该核心中继呼入,参考业务→高级配置→黑白名单
入局号码变换	配置从该核心中继呼入时的号码变换规则(仅呼入,从该中继呼出该规则不生效),参考业务→高级配置→号码变换
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式,系统可根据配置选择对应的发送模式,一通电话如果 SBC 两侧的 dtmf 方式不一致,会通过 DSP 转换
入局 SIP 消息变换	即从该核心中继呼入时的 SIP 头域修改,参考业务→高级配置→SIP 头域变换
出局 SIP 消息变换	即从该核心中继呼出时的 SIP 头域修改,参考业务→高级配置→SIP 头域变换
SIP 账户	SBC 自身像服务器发起注册的账户,参考业务→高级配置→SIP 账户
远端服务器域名	配置了域名, SBC 发送请求时, request 行会用该域名替换 ip 地址
接入访问 ACL 表	该中继除配置指定的远端 IP 地址外,允许接入的 ACL 规则表
注册	启用注册后,该中继会根据配置的 SIP 账户密码向本中继的远端服务器发起注册。注意:中继模式为 dynamic 时不可使用
OutBound Proxy	Outbound 代理地址
心跳策略	配置中继的 option 心跳策略:心跳超时次数、心跳发送间隔、和是否仅认为响应为 200ok 的 option 请求为有效心跳握手
Session Timer	会话定时器,是种会话保存激活的机制,如果启用, SBC 会在会话周期内发送 reinvite 报文保持会话激活,如果在会话周期内未检测到该消息,则认为会话已经终止,系统会主动拆除该会话。如果采用的是 require 模式,通过该核心中继呼出时,必须要求被叫也支持 timer
注册最小时长	终端注册的允许的最小时长,如果终端注册 REGISTER 报文中 expires 值小于这个值, SBC 可能会拒绝该注册请求
NAT 内注册时长	SBC 如果发现终端在 NAT 下,则 SBC 响应的注册时长会自动变为该值, NAT 内注册时长值一般比较小,以免 NAT 地址发生变化时 SBC 不能及时发现。
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制,可参考 RFC3262 文档。配置为 disable 时, SBC 发送的请求或 1xx 响应默认都不带 100rel;配置为 support 时, SBC 的请求或 1xx 响应会在 supported 域里带上 100rel;配置为 require 时, SBC 的请求或 1xx 响应会在 require 域带上 100rel,如果对端不支持,则响应 420,如果支持,则会在收到 1xx 响应时,发送 PRACK 消息回来。
远端媒体地址	启用远端媒体地址锁定:当远端设备在公网时,那么锁定的就是 sdp 中的媒体地址;在私网时,就是动态锁定,要连续收到 30 个报文后就锁

	定该报文的原地址
远端信令地址	启用信令锁定：账户注册成功后，只接收该账户的主叫注册时同样地址来的呼叫报文
主叫号码提取方式	user:提取 invite 报文 from 域中 user 字段作为主叫 display: 提取 invite 报文 from 域中 display 字段作为主叫
被叫号码提取方式	user:提取 invite 报文 to 域中 user 字段作为被叫 display: 提取 invite 报文 to 域中 display 字段作为被叫 request-uri: 提取 invite 报文 request-uri 的中的 user 号码作为被叫
SIP 方法	配置该核心中继允许接收的 SIP 请求方法，如果未启用对应的 SIP 请求方法，系统收到对应的 SIP 请求时，会直接拒绝。INVITE/REGISTER 和拆除会话请求默认允许。

3.4.4 路由规则

1) 中继组

中继组将接入中继或核心中继进行分组，让该中继组呼出时能够做主备或负载均衡。

名称 *	<input type="text"/>
描述	<input type="text"/>
路由组类型	接入中继组
组内选择方式	Backup
中继名称	1<pchu> <input type="button" value="删除"/>
容量分配	<input type="text"/>
中继名称	2<justtest> <input type="button" value="删除"/>
容量分配	<input type="text"/>
+ Add	
<input type="button" value="提交"/> <input type="button" value="取消"/>	

图 3-4-5 中继组页面

表 3-4-4 中继组

参数	参数描述
名称	配置中继组的名字，用户自定义，添加成功后不可修改
描述	该中继组的描述，用户可以较为详细描述该核心网的作用和规则
路由组类型	分为接入中继组和核心网中继组，参考业务→路由规则→中继组
组内选择方式	主备 Backup: 中继组主备模式下，当第一个中继状态为 true 时，呼出只走主中继，其它情况才走下一个备用中继，直到可用中继或无可用中继为止 负载均衡 Load Balance: 呼出时根据负载均衡策略，按比重把呼叫送到对应中继上
中继名称	接入网中继或核心网中继的名称
容量分配	主备模式时，配置对应中继的最大并发呼叫数，当对应中继当前呼叫数超过指定容量时，后续发起的呼叫会分配给下一条中继
权重	负载均衡模式时，该中继组内所有中继的呼叫数权重比，所有中继的权重比之和为 100

2) 路由

索引	* 1020
描述	
启用	<input checked="" type="checkbox"/>
dtmf 协商	<input checked="" type="checkbox"/>
透传不带sdp的183	<input checked="" type="checkbox"/>
媒体payload值适配	Normal(2833&rtp)
条件	
号码规则	
主叫用户名	
被叫用户名	
时间规则	
主叫SIP URL	
被叫SIP URL	
来源	接入中继
	4<tgtest> <input type="button" value="Del"/>
	<input type="button" value="+ Add"/>
SIP方法	
Request URI	
目的	
	核心中继
	3<tgtestout>
号码变换	
SIP头域透传	
request-uri 用户名	to inManipulation user
request-uri 地址	remote address
to 用户名	to inManipulation user
to 地址	remote address
to 显示用户名	to display
from 用户名	from inManipulation user
from 地址	local address
from 显示用户名	from display
	<input type="button" value="保存"/> <input type="button" value="取消"/>

图 3-4-6 路由页面

表 3-4-5 路由

参数	参数描述
优先级	相同条件下，优先级数字越小，优先级越高，呼叫选择路由会从高优先级的路由开始匹配，一旦条件都匹配成功，呼叫就根据该路由进行呼叫，路由选择不支持二次选路
描述	该优先级的描述，用户可以较为详细描述该优先级的作用和规则
启用	路由规则启用，如果不启动，则表示禁用：匹配该路由的呼叫将被拒绝
dtmf 协商	呼叫时，SBC 两侧是否自行协商 dtmf 类型，如果不启用，SBC 将会透传主叫的 dtmf 模式给被叫
透传不带 sdp 的 183	收到 183 响应时，如果该响应不带 sdp，是否透传该响应
媒体 payload 值适配	启用后，协商的 payload 值与实际 payload 值不一致时，SBC 会强制修改 payload 值为协商值
号码规则	选择路由时匹配的主被叫号码池（参考业务→高级配置→号码池），如果号码池选择为空，用户在下面主叫用户名和被叫用户名中配置主被叫号码的匹配条件
主叫用户名	主叫号码的匹配规则，如果为空，则表示主叫号码任意，支持正则表达式匹配
被叫用户名	被叫号码的匹配规则，如果为空，则表示被叫号码任意，支持正则表达式匹配
时间规则	本条路由规则生效的时间段（参考业务→高级配置→时间规则），如果时间配置为空，则表示该路由任意时间段都可以使用
主叫 SIP URL	配置请求报文中 from 域的 SIP URL 字段匹配规则，如果为空，则表示主叫 SIP URL 不限制
被叫 SIP URL	配置请求报文中 to 域的 SIP URL 字段匹配规则，如果为空，则表示被叫 SIP URL 不限制
来源	设置该路由的呼叫来源是从接入网、接入中继、核心中继、接入中继组、核心中继组，可配置一条或多条来源
SIP 方法	该路由支持的 SIP 请求方法如 INVITE、REGISTER 等，如果为空，表示不限制
Request url	该路由限制的 request 域的 url 字段，支持正则表达式匹配
目的	设置该路由的呼叫是从接入网、接入中继、核心中继、接入中继组、核心中继组出局，只可配置一条出局
号码变换	通过该路由时是否启用号码变换规则（参考 业务→高级配置→号码变换），默认不启用，号码替换会在在路由选择后完成
SIP 头域透传	通过该路由时是否启用 SIP 头域透传规则（参考业务→高级配置→SIP 头域透传），默认不启用，SIP 头域透传会在在路由选择后完成

Request-url 用户名	设置出局时 sip 头域中 request-url 字段中引用的用户名
Request-url 地址	设置出局时 sip 头域中 request-url 字段中引用的地址
to 用户名	设置出局时 sip 头域中 to 域中引用的用户名
to 地址	设置出局时 sip 头域中 to 域中引用的地址
to 显示用户名	设置出局时 sip 头域中 to 域中引用的 dispname
from 用户名	设置出局时 sip 头域中 from 域中引用的用户名
from 地址	设置出局时 sip 头域中 from 域中引用的地址
from 显示用户名	设置出局时 sip 头域中 from 域中引用的 dispname



注意

接入网、接入网中继和核心网中继配置中也有号码替换，这些号码替换只针对该接入网或中继呼入时生效，并且在路由选择前生效。

3.4.5 业务管理

图 3-4-7 业务管理

表 3-4-6 业务管理

参数	参数描述
匹配会话时只使用 callid	判断收到的一系列请求是否属于同一个会话的标准是否只判断 callid 相同即可
语音中断保护	通话时是发现语音中断，是否启用保护机制，保护机制有告警和断流拆线
断流拆线	启用后，通话时在检测时长内某一侧语音媒体都无收或发报文，则拆除该通话
检测时长	设置判断触发断流拆线的检测时长

媒体端口起始值	设置整个 SBC 设备发送所有 rtp 报文的本地起始端口，媒体端口起始值范围必须为 16K 的整数倍，K=1024
上报时长	通话接通后多少秒上报 rtp 统计信息，信息包括丢包、延时、抖动和收发报文数
媒体异常统计	是否对出现异常的媒体进行统计
sdp crypto key base64 加解密模式	设置 sdp crypto key base64 的加解密模式：normal 或 padding

3.4.6 话单管理

本地存储话单，可以存储在内存或 flash 中，由于空间有限，建议只保存异常话单，需要所有话单的话最好通过话单服务器保存。

话单管理中的话单服务器默认不启用，需要启用后才能配置话单服务器。



图 3-4-8 启用话单服务器

名称 *	<input type="text"/>
描述	<input type="text"/>
接口 *	eth0
编码格式	SYSLOG
IP地址 *	<input type="text"/>
端口 *	514
协议	UDP

属性名	描述	自定义 属性名	启用
SessionId	会话 Id	<input type="text"/>	<input type="checkbox"/>
HangupStatus	错误码	<input type="text"/>	<input type="checkbox"/>
HangupReason	挂断原因	<input type="text"/>	<input type="checkbox"/>
HangupRole	挂断方	<input type="text"/>	<input type="checkbox"/>
TalkTime	通话时间	<input type="text"/>	<input type="checkbox"/>
CreateTime	创建会话时间	<input type="text"/>	<input type="checkbox"/>
RingTime	振铃时间	<input type="text"/>	<input type="checkbox"/>
AnswerTime	应答时间	<input type="text"/>	<input type="checkbox"/>
HangupTime	挂断时间	<input type="text"/>	<input type="checkbox"/>

呼入

InCaller	变换前主叫号码	<input type="text"/>	<input type="checkbox"/>
InCallee	变换前被叫号码	<input type="text"/>	<input type="checkbox"/>
OutCaller	变换后主叫号码	<input type="text"/>	<input type="checkbox"/>
OutCallee	变换后被叫号码	<input type="text"/>	<input type="checkbox"/>
IngressRealm	中继名称	<input type="text"/>	<input type="checkbox"/>
IngressLocalAddr	信令本地 IP	<input type="text"/>	<input type="checkbox"/>
IngressMediaRemoteAddr	媒体远端 IP	<input type="text"/>	<input type="checkbox"/>
IngressRemoteAddr	信令远端 IP	<input type="text"/>	<input type="checkbox"/>
IngressMediaLocalAddr	媒体本地 IP	<input type="text"/>	<input type="checkbox"/>
IngressRtpEncode	编解码	<input type="text"/>	<input type="checkbox"/>
IngressRtpPayload	净荷值	<input type="text"/>	<input type="checkbox"/>
IngressCallId	CallId	<input type="text"/>	<input type="checkbox"/>

IngressInterface	网卡	<input type="text"/>	<input type="checkbox"/>
RtpAstat	收发包 数	<input type="text"/>	<input type="checkbox"/>
呼出			
InCaller	变换前主 叫号	<input type="text"/>	<input type="checkbox"/>
InCallee	变换前被 叫号	<input type="text"/>	<input type="checkbox"/>
OutCaller	变换后主 叫号	<input type="text"/>	<input type="checkbox"/>
OutCallee	变换后被 叫号	<input type="text"/>	<input type="checkbox"/>
EgressRealm	中继名 称	<input type="text"/>	<input type="checkbox"/>
EgressLocalAddr	信令本地 IP	<input type="text"/>	<input type="checkbox"/>
EgressMediaRemoteAddr	媒体远端 IP	<input type="text"/>	<input type="checkbox"/>
EgressRemoteAddr	信令远端 IP	<input type="text"/>	<input type="checkbox"/>
EgressMediaLocalAddr	媒体本地 IP	<input type="text"/>	<input type="checkbox"/>
EgressRtpEncode	编解 码	<input type="text"/>	<input type="checkbox"/>
EgressRtpPayload	净荷 值	<input type="text"/>	<input type="checkbox"/>
EgressCallId	CallId	<input type="text"/>	<input type="checkbox"/>
EgressInterface	网卡	<input type="text"/>	<input type="checkbox"/>
RtpBstat	收发包 数	<input type="text"/>	<input type="checkbox"/>
		<input type="button" value="提交"/>	<input type="button" value="取消"/>

图 3-4-9 话单配置

表 3-4-7 话单管理

参数	参数描述
名称	话单服务器名字，用户自定义，添加成功后不可修改
描述	话单服务器的描述，用户可以较为详细描述该服务器位置、作用、类型等

接口	发送话单采用的网络接口，参考系统→网络管理
IP 地址	话单服务器的 IP 地址
端口	话单服务器接收话单采用的端口
协议	传输话单采用的传输协，有 UDP 和 TCP 两种，目前只支持 UDP
编码格式	话单的编码格式，目前支持 syslog 和 json
其它	自定义每条话单内容的属性

3.4.7 编解码分组

SBC8000 设备支持 G729、G723、PCMU、PCMA、iLBC_13K、iLBC_15K、OPUS、AMR、AMR_WB 和 G726 这几种编解码，用户可以根据需求将这几种编解码任意分组和调整优先级。



图 3-4-10 编解码分组页面

表 3-4-8 编解码分组

参数	参数描述
名称	编解码分组的名称，可自定义，添加成功后不可修改
描述	该编解码分组的描述，用户可以较为详细描述该编解码分组的作用和原因

最大打包时长	该编解码分组所有编解码支持的最大打包时长
编码名称	SBC8000 设备支持的编解码一共有以下几种： PCMA, PCMU, G.729A/B, G.723, iLBC_13K, iLBC_15K, AMR, AMR_WB, OPUS, G.726
净荷值	每种编解码对应的 codec 值，不可修改
打包时长	每种编解码支持的默认打包时长，不可修改
禁用视频媒体	禁止视频编解码透传
透传 MIME	是否透传 MIME



注意

名称为 default 的编解码分组为默认值，默认支持全部编解码，该条数据只可修改，不可删除。

3.4.8 TLS 配置

用户设置 TLS 最低支持的版本 V1.1/V1.2/V1.3 和采用的加密套件

名称	描述	最低支持版本	服务器优选
default	default	version1.2	true

名称 * default

描述 default

最低支持版本 Version1.2

服务器优选

Cipher Suites

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384



图 3-4-11 TLS 配置页面

3.4.9 主备

该功能仅在双机热备情况下使用

1) 主备配置

配置主备服务器和检测方式



图 3-4-12 主备配置页面

表 3-4-9 主备配置

参数	参数描述
网络	支持 IPV4 和 IPV6 模式
本地管理口 IP	该 IP 是引用系统→网络管理中管理口的 IP 地址
本地端口	默认采用 4222，不可修改
远端管理口 IP	双机热备中另外一台设备用于主备握手的管理口 IP 地址
远端端口	双机热备中另外一台设备用于主备握手的管理口 IP 端口，不可修改
用户板个数	用于判断设备是否正常的用户板个数，不得超过设备的实际用户板个数
禁用视频媒体	禁止视频编解码透传
对端设备序列号	双机热备中另外一台设备的 SN 号，输入格式为 xxxx-xxxx-xxxx-xxxx
主备最大心跳次数	判断主备是否正常连接的最大心跳次数，超过次数无响应则认为主备连接中断，备模式的设备就会自动升级为主模式
主备心跳周期时长	发送心跳的时间间隔 S
呼叫同步延时	设置主设备的呼叫，在延时多少秒后，同步到备设备上
呼叫检测时长	如果主备中断，备设备已经同步的通话未收到拆线消息时的保护时长，为 0 代表不检测
服务最大心跳次数	判断与该 SBC 与 HA 进程之间连接的最大心跳次数，超过次数无响应则认为服务连接中断，主设备会自动掉到备机模式
复位心跳周期时长	判断与该 SBC 与 HA 进程之间连接发送心跳的时间间隔 S

2) BFD 检测

主备通过 BFD 报文检测连通性

BFD 检测							+Add
服务类型	本地IP类型	本地IP	本地端口	远端IP类型	远端地址	远端端口	
主备服务类型	IPV4	172.30.0.56	8868	IPV4	172.30.0.234	8888	⊗ ⊕

图 3-4-13 BFD 检测页面

表 3-4-10 BFD 检测

参数	参数描述
网络	支持 IPV4 和 IPV6 模式
本地管理口 IP	该 IP 是引用系统→网络管理中管理口的 IP 地址
本地端口	默认采用 4222，不可修改
远端管理口 IP	双机热备中另外一台设备用于主备握手的管理口 IP 地址
远端端口	双机热备中另外一台设备用于主备握手的管理口 IP 端口，不可修改
用户板个数	用于判断设备是否正常的用户板个数，不得超过设备的实际用户板个数
禁用视频媒体	禁止视频编解码透传
对端设备序列号	双机热备中另外一台设备的 SN 号，输入格式为 xxxx-xxxx-xxxx-xxxx
主备最大心跳次数	判断主备是否正常连接的最大心跳次数，超过次数无响应则认为主备连接中断，备模式的设备就会自动升级为主模式

3) 网口检测

通过检测 SBC 业务口的网络连接情况进行主备竞争，业务网口参考系统→网络管理中的业务口：

网口检测					+ Add
名称	IPv4地址	IPv6地址	Mac地址	子网掩码	

图 3-4-14 网口检测页面

4) 切换规则

配置网口检测时，对应业务口的权重，值越大代表权重越高，其它条件相同情况下，当主与备设备各有一个业务口故障，则权重低的故障业务口设备会升为主设备，权重高的故障业务口设备会降为备设备。

切换规则		+ Add
名称	权重	

图 3-4-15 网口检测页面

3.4.10 号码规则

号码规则用于呼叫选择路由时主/被叫号码的前缀匹配。此处配置的号码规则不支持正则表达式。

号码规则				+ Add
导出	导入	Choose File No file chosen		
名称	描述	主叫号码	被叫号码	

名称 *

描述

主叫号码

被叫号码

图 3-4-16 添加号码规则

表 3-4-11 号码规则相关参数描述

参数	参数描述
名称	号码规则的名称，用户自定义，添加成功后不可修改
描述	号码规则的描述，用户可以较为详细描述该号码规则的作用
主叫号码	用于呼叫选择路由时匹配主叫号码前缀的号码规则，不支持正则表达式
被叫号码	用于呼叫选择路由时匹配被叫号码前缀的号码规则，不支持正则表达式

3.4.11 黑白名单

在“业务→高级配置→黑白名单”页面，用户通过把号码列入白名单或黑名单来决定 SBC 设备是否接受该号码的呼叫和注册。

图 3-4-17 黑名单页面

图 3-4-18 白名单页面

表 3-4-12 黑白名单相关参数描述

参数	参数描述
黑名单组	黑名单组的名称，可自定义，添加成功后不可修改
白名单组	白名单组的名称，可自定义，添加成功后不可修改
描述	描述黑/白名单组，用户可以较为详细描述该黑/白名单组的作用
号码	黑/白名单的号码，不支持正则表达式
描述	该条黑/白名单号码的具体描述

3.4.12 号码变换

号码变换用于呼叫选择路由时根据匹配规则将主/被叫号码变换成指定的主/被叫号码。

名称 *	<input type="text"/>
描述	<input type="text"/>
主叫变换规则	
删除前缀	<input type="text"/>
删除后缀	<input type="text"/>
添加前缀	<input type="text"/>
添加后缀	<input type="text"/>
替换条件	正则表达式 <input type="text"/>
替换值	替换值 <input type="text"/>
被叫变换规则	
删除前缀	<input type="text"/>
删除后缀	<input type="text"/>
添加前缀	<input type="text"/>
添加后缀	<input type="text"/>
替换条件	正则表达式 <input type="text"/>
替换值	替换值 <input type="text"/>
<input type="button" value="提交"/> <input type="button" value="取消"/>	

图 3-4-19 号码变换页面

表 3-4-13 号码变换

参数	参数描述
名称	配置号码变换的名字，用户自定义，添加成功后不可修改
描述	该号码变换的描述，用户可以较为详细描述该号码变换的作用和原因
删除前缀	删除掉匹配到的前缀内容，例如：号码为 67890000，删除前缀内容为 678，则匹配该号码变换规则后，号码变为 9000，如果号码为 16789000，则不删除该号码前缀，支持正则表达式配置，一条号码变换规则同时可以配置多条删除前缀规则
删除后缀	删除掉匹配到的后缀内容，例如：号码为 90000678，删除后缀内容为 678，则匹配该号码变换规则后，号码变为 9000，如果号码为 90006789，则不删除该号码后缀，支持正则表达式配置，一条号码变换规则同时可以配置多条删除前缀规则
添加前缀	在号码最前面添加上前缀，如原号码为 9000，添加前缀为 678，匹配该号码变换规则后，号码变换为 6789000，不支持正则表达式配置
添加后缀	在号码最后面添加上后缀，如原号码为 9000，添加后缀为 678，匹配该号码变换规则后，号码变换为 9000678，不支持正则表达式配置
替换条件	用正则表达式配置号码变换规则，如果号码能够匹配替换条件中的一条规则，则将号码变换为下面选项中的替换值
替换值	原号码如果能够匹配上面的替换条件中的一条规则，这替换为该替换值，替换值配置不支持正则表达式



注意

一条号码变换规则，会将号码从删除前缀、删除后缀、添加前缀、添加后缀依次处理，然后根据以上处理结果，再用来匹配替换条件。

入局号码变换，指的是对应中继（或接入网）呼入时选路前的号码变换，出局号码变换，指的是选路后的号码变换，所以入局号码变换配置在中继（或接入网）配置中；出局号码变换配置放在路由配置中。

3.4.13 号码池

呼叫选择路由后，如设置号码池规则，那么从该路由出局的主叫或被叫号码会被号码池的号码随机替换。

图 3-4-20 号码池设置

表 3-4-14 号码池相关参数描述

参数	参数描述
名称	该号码池的名称，可自定义，添加成功后不可修改
描述	该号码池的描述，可较为详细描述该号码池的作用和原因
主叫/被叫变换规则	<p>当此处设置的前缀匹配同一路由出局的主叫或被叫号码，主叫或被叫号码会被号码池的号码随机替换。</p> <p>前缀：用于匹配主叫/被叫号码的前缀</p> <p>起始数值：号码池的起始数值</p> <p>结束数值：号码池的结束数值</p>

3.4.14 SIP 账户

SIP 账户是 SBC 设备本地添加 SIP 客户端账户，用于通过接入中继或核心中继，向服务器发起注册，注册成功后，可以通过 SBC 从该中继呼出的呼叫，主叫号码替换成 SIP 账户号码。SIP 账户可以导入和导出，支持 txt 格式和 csv 格式。

名称	描述	流控个数	流控单位时间(s)	账户数量	账户
mos	mos ipbpx	10	10	100	17801,17802,17803,17804,17805,17806,17807,17808,17809,178010,...

名称 *

描述

流控个数 *

流控单位时间 * s

注意: (账户总数 / 流控个数) * 流控单位时间 < 注册周期的50%~90%
否则部分用户注册不上, 流控只适用于register报文

账户

用户名 认证ID 注册周期 最大并发呼叫数

用户名 *

认证ID *

密码 *

注册周期 *

最大并发呼叫数 *

起始数值 *

步进 *

账户数量 *

注意: 为了实现多种应用场景,用户名,认证ID,密码选项支持规则适配,可变量符\$1

规则: 除\$1以外的字段定义为保留字,\$1根据起始数值,步进和账户数量选项进行控制

例如: 要添加10001000 ~ 10003000账户, 选项填写1000\$1,起始字段1000,步进1,账户数量3000

图 3-4-21 SIP 账户设置界面

表 3-4-15 SIP 账户相关参数描述

参数	参数描述
名称	该 SIP 账户集的名称
描述	该 SIP 账户集的描述, 可较为详细描述该 SIP 账户集的作用和原因
流控个数	用于控制该 SIP 账户集在流控单位时间内向服务器发起注册的注册请求 register 个数, 含续租的请求, 流控个数
流控单位时间	流控个数需要在设置的时间内发送完注册; 流控个数/流控单位时间=每秒发起 register 报文的个数
用户名	SIP 账户名称
认证 ID	SIP 账户的认证 ID
密码	SIP 账户的认证密码
最大并发呼叫数	每个 SIP 账户支持的最大并发数
起始数值	批量添加 SIP 账户, 通过\$1 配置时, 第一个数值, 比如 870\$1,起始数值是 1, 那么批量添加的 SIP 账户第一个账户就是 8701

步进	批量添加 SIP 账户,通过\$1 配置时,相连两个 SIP 账户数值,比如 870\$1,步进是 2,那么批量添加的 SIP 账户第一个账户就是 8701,第二个 SIP 账户就是 8703
账户数量	改 SIP 账户集的总账户数量



注意

SIP 账户总数不能超过 3000 个,每秒发起的 register 个数(终端通过 SBC 向服务器发起的 register+SBC 本身添加的 SIP 账户自身发起的 register)总数不能超过 SBC 的 license 限制

3.4.15 时间规则

时间规则页面配置路由生效时间段,可以按照日期、工作日、时间点进行配置。路由配置添加时间后,在配置时间内能该路由生效,配置时间外该路由不生效(呼叫匹配不到该路由)。

图 3-4-22 路由时间配置

表 3-4-16 路由时间相关参数描述

参数	参数描述
名称	路由时间的名称,用户可以自定义,添加成功后不可修改
描述	该路由时间的描述,用户可以较为详细描述该路由时间的作用
日期	路由生效的开始日期到结束日期,可以配置多个日期段
工作日	路由生效的工作日(周一到周日),可以复选
时间	路由生效的开始时间点到结束时间点,可以配置多个时间段

3.4.16 速率控制

速率控制页面主要是配置接入网、接入网中继和核心网中继的每秒最大注册数、每秒最大呼叫数和最大的呼叫并发数。

名称	描述	注册速率	呼叫速率	最大并发呼叫数
default	default	200	200	3000

名称 *	default
描述	default
注册速率 *	200
呼叫速率 *	200
最大并发呼叫数 *	3000

保存 取消

图 3-4-23 速率控制页面

表 3-4-17 速率控制相关参数的描述

参数	参数描述
名称	配置该调速率控制的名称，可自定义，添加成功后不可修改
描述	该速率控制的描述，用户可以较为详细描述该速率限制的作用和原因
注册速率	每秒最大注册数
呼叫速率	每秒最大呼叫数
最大并发呼叫数	最大总呼叫并发数



注意

- 1) 速率控制有一条默认数据，该数据在配置 License 时自动生成，配置速率控制的最大值，不能超过这条默认值。
- 2) 实际呼叫时所有总注册速率、总呼叫速率、总最大并发数，不会超过 license 限制值。

3.4.17 SIP 头域修改

当需要修改接入网、接入网中继或核心网中继时，可对指定 SIP 报文进行相应的头域修改，以满足某些对 SIP 头域有特殊要求（原始报文未提供）的需求。

名称 * SIPheadfrom

描述 SIP head from user

类型过滤 Request

名称	描述	类型	条件列表	值
ip	ip=80.113	header	\$network.\$remote	\$from.\$uri.\$user

图 3-4-24 SIP 头域修改页面

表 3-4-18 SIP 头域修改

参数	参数描述
名称	配置头域变换的名字，用户自定义，添加成功后不可修改
描述	该 SIP 头域变换的描述，用户可以较为详细描述该号码变换的作用和原因
类型过滤	Request: 该规则只处理 SIP 的请求报文，响应报文不处理 Response: 该规则只处理 SIP 的响应报文，请求报文不处理 List: 该规则只处理选中的请求和响应报文，未选中的报文不处理。
操作规则	根据源标识的匹配条件列表（与关系），对目的标识进行头域变换（add、modify、remove）
类型	一条 SIP 头域修改规则可以有多条子规则，每条子规则只能处理一种类型，如果要同时处理多种类型，必须配置多条子规则： Request-line: SIP 报文请求行中的内容 Status-line: SIP 报文状态行中的内容 Header: SIP 报文中 header 的内容
源标识	指的是 SIP 原始来源报文，可以指定到原始 SIP 报文中某一个参数的内容
匹配方式	Equal: 值为完全匹配，只有指定源标识的值完全等于配置的值，该规则才会生效 Regex: 值为正则表达式匹配，当指定源标识的值符合配置的正则表达式，该规则就会生效
值	匹配条件指定的目标标识值
目标标识	指的是需要修改 SIP 报文指定的头域
操作类型	Add: 在指定目标标识内容后面添加上对应的值 Modify: 修改指定目标标识的值为对应的值 Remove: 删除指定目标标识的值，如果目标标识为一个域，则删除该域
值类型	Token: 值中带\$标志的内容代表引用原始源报文指定域的内容，不带\$标志的内容为配置是什么就是什么 Equal: 值内容为配置是什么就是什么 Regex: regex 比较特殊，多了一个三级子规则，源报文内容必须和对应的匹配规则内容相同，该子规则才会生效

值

Token 和 Regex 值类型中，带\$的标识引用原始报文指定域的值，Equal 中如果有\$，无特殊意义



注意

用\$引用原始报文的值时，必须参考目标标识的配置方式，如，要引用原始报文中 to 域中的 user 值，输入的方式为\$to.\$uri\$.user。

所有用\$引用的值，都是原始报文（未变换前的 SIP 报文）的值，不是经过处理的值（如号码变换、前面 SIP 头域修改等）。

每个 SIP 头域参数有对应的规格，用户修改建议严格按照参数规则来修改或匹配，用户可以参考附件中的《SMM 规则和变量（SIP 头域修改）.xlsx》确定每种域的参数规则和修改权限。

3.4.18 SIP 头域透传

“SIP 头域透传”可用来在指定路由中透传 SIP 消息中指定的扩展域。

名称 * default

描述 default

SIP头域

- User-Agent
- X-Genesys-businessid
- X-Genesys-skillid
- X-Genesys-user
- X-Genesys-vid

保存 取消

tips: 注册代理头域透传: Allow, Supported

图 3-4-25 SIP 头域透传页面

表 3-4-19 SIP 头域透传

参数	参数描述
名称	配置 SIP 头域透传的名字，用户自定义，添加成功后不可修改
描述	该 SIP 头域透传的的描述，用户可以较为详细描述该接入网的作用和规则
SIP 头域	允许透传的头域，一行一个头域，头域区分大小写，完全匹配，不要有额外的标点符号



注意

请谨慎使用 Allow 和 Supported 头域透传，因为可能会和 SBC 自身的配置冲突。以下头域不允许透传：

Network, To, From, Contact, Cseq, Max-Forwards, Content-Length, Content-Type, Via, Require, Proxy-Require, Unsupported, Authorization, Proxy-Authorization, Www-Authenticate, Proxy-Authenticate, Accept, Route, Record-Route, Refer-To, Referred-By, Auto-Defined。

3.4.19 质量监控

设置语音媒体的质量监控规则，当呼叫接通后音视频媒体流的丢包、延时、抖动或收发的 RTP 报文总数大于设置的数值时，进行丢弃、日志记录或告警。

索引 *	<input type="text" value="127"/>
描述	<input type="text"/>
通话时长	<input type="text"/> s
触发规则(来源)	
接口	<input type="text"/>
远端地址	<input type="text"/>
丢包率	<input type="text"/> %
时延	<input type="text"/> ms
网络抖动	<input type="text"/> %
Rtp接收包数	<input type="text"/>
Rtp发送包数	<input type="text"/>

触发规则(目的)	
接口	<input type="text"/>
远端地址	<input type="text"/>
丢包率	<input type="text"/> %
时延	<input type="text"/> ms
网络抖动	<input type="text"/> %
Rtp接收包数	<input type="text"/>
Rtp发送包数	<input type="text"/>
动作	
	<input type="text" value="丢弃"/>
<input type="button" value="提交"/> <input type="button" value="取消"/>	

图 3-4-26 质量监控页面

3.4.20 带宽限制

用于设置指定中继允许使用的最大带宽:指定编解码的每路带宽*最大可以呼叫的并发量=最大带宽。

每一种音频和视频编解码每路占用的带宽都不一样,音频每种编解码基础带宽占用已经给出默认值,视频编解码每路占用带宽需要自行计算。

名称 *	<input type="text"/>
描述	<input type="text"/>
音频	
PCMU:	<input type="text" value="90.4"/> kbps
PCMA:	<input type="text" value="90.4"/> kbps
G723:	<input type="text" value="23.9"/> kbps
G729:	<input type="text" value="34.4"/> kbps
OPUS:	<input type="text" value="12"/> kbps
AMR:	<input type="text" value="12.2"/> kbps
ILBC_13K:	<input type="text" value="13.3"/> kbps
ILBC_15K:	<input type="text" value="15.2"/> kbps
视频	
VP8:	<input type="text" value="0"/> kbps
VP9:	<input type="text" value="0"/> kbps
H.263:	<input type="text" value="0"/> kbps
H.264:	<input type="text" value="0"/> kbps
H.265:	<input type="text" value="0"/> kbps
<p>注意: 带宽限制预分配每路语音通话20kbps、视频通话2mbps,接通后,根据配置带宽数值多退少补</p>	
<input type="button" value="提交"/> <input type="button" value="取消"/>	

图 3-4-27 带宽限制页面

3.5 安全配置

3.5.1 访问控制

设置设备的 WEB（https）和 SSH 访问控制端口，以及 GE0、GE1、GE2 和 GE3 网口的访问控制策略，网口默认不能通过 web 和 SSH 访问。




图 3-5-1 访问控制设置

表 3-5-1 访问控制

参数	参数描述
HTTPS 端口	通过 web 的 https 协议访问时的端口，默认为 443，用户可以修改成其它端口；

3.5.2 防攻击策略



图 3-5-2 SIP 防攻击策略

点击 ADD 按钮添加 IP 防攻击策略，在这里也可以删除或修改 P 防攻击策略。

The screenshot shows a configuration window for adding a SIP anti-attack strategy. It contains the following fields and options:

- 优先级 (Priority):** A numeric input field containing the value 123.
- 描述 (Description):** An empty text input field.
- 攻击类型 (Attack Type):** A dropdown menu with '用户攻击' (User Attack) selected.
- 检测类型 (Detection Type):** A dropdown menu with '注册次数' (Registration Count) selected.
- 接入端点 (Access Point):** An empty dropdown menu.
- 动作类型 (Action Type):** A dropdown menu with '记录日志' (Log) selected.
- Buttons:** Two green buttons labeled '提交' (Submit) and '取消' (Cancel) are located at the bottom.

图 3-5-3 添加 SIP 防攻击策略

表 3-5-2 SIP 防攻击策略

参数	参数描述
注册检测时间间隔	SIP 防攻击注册报文的检测周期
呼叫检测时间间隔	SIP 防攻击呼叫报文的检测周期
优先级	优先级的数字越低，优先级等级越高
名称	SIP 防攻击策略名称，添加后不可修改
攻击类型	<p>IP 防攻击: 当某一个 IP 在检测周期内发过来的 SIP 报文数超过设定阈值时，系统会根据动作类型对该 IP 发过来的 SIP 报文做相应的处理。</p> <p>用户防攻击: 在检测周期内发过来相同用户和接入网监听端口的注册/呼叫（主叫）报文数超过设定阈值时，系统会根据动作类型对该用户 SIP 报文做相应的处理。</p>
检测类型	<p>注册次数: 检测同一 IP 或用户发过来 SIP 报文中的 REGISTER 报文次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 REGISTER 报文做相应处理</p> <p>呼叫次数: 检测同一 IP 或主叫用户发过来 SIP 报文中的 INVITE 报文次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 REGISTER 报文做相应处理</p>
接入端点	用户攻击检测的接入网，如果接入端点不配置，那么检测的是用户名，如果配置了接入网，那就是只对这个接入网进行规则匹配，参考 3.4.9 接入网
动作	<p>记录日志: 该策略生效时，只记录该事件日志，不做其它处理</p> <p>流量限制: 该策略生效时，对该远端 IP 或设置的本地端口做 SIP 包流量限制，在限制时间内超过流量的 SIP 注册/呼叫报文全部丢弃</p>

	包速率限制：该策略生效时，对该远端 IP 或设置的本地端口做 SIP 包速率限制，在限制时间内超过的 SIP 注册/呼叫报文全部丢弃 丢弃：该策略生效时，对该远端 IP 或设置的本地端口收到的 SIP 注册/呼叫报文，在限制时间内全部丢弃
时间	SIP 防攻击策略生效时的时间，一个策略生效时，超过设置时间后需要重新判断策略是否生效

3.5.3 web 认证

SBCweb 登录支持三种认证方式：本地认证、tacacs 认证和 radius 认证

1) 本地认证

图 3-5-4 本地认证

2) tacacs 认证

图 3-5-5 tacacs 认证

3) radius 认证

radius配置

启用 radius	<input checked="" type="checkbox"/> 启用
重传超时时间(1-10s)	<input type="text" value="5"/>
最大重传次数	<input type="text" value="5"/>
服务器最大连接失败次数	<input type="text" value="5"/>
服务器恢复时间(1-30min)	<input type="text" value="15"/>
服务器心跳间隔(s)	<input type="text" value="30"/>
认证超时时间(s)	<input type="text" value="30"/>
话单是否保存到数据库	<input type="checkbox"/>
厂商id	<input type="text"/>
发送start消息	<input type="text"/>
发送stop消息	<input type="text" value="所有呼叫"/>
服务器模式	<input type="text" value="主备"/>
本地接口	<input type="text" value="eth0"/> <input type="button" value="删除"/>

本地认证端口	<input type="text"/>
本地计费端口	<input type="text"/>
网络	<input type="text" value="IPV4"/>
远端地址	<input type="text"/>
远端认证端口	<input type="text"/>
远端计费端口	<input type="text"/>
共享密钥	<input type="text"/>

标准属性	<input type="button" value="隐藏"/>
扩展属性	<input type="button" value="全选"/> <input type="button" value="隐藏"/>

注意：本地认证端口和本地计费端口填0为随机分配
远端认证端口和远端计费端口填0为不启用此功能
使用服务器做计费功能时，本地接口不要使用管理口GE1

图 3-5-6 radius 认证

3.6 系统

系统配置包括系统管理、接口管理、静态路由、用户管理、时间管理、版本升级、备份与恢复、License 管理、数字证书管理。

3.6.1 系统管理

系统管理用来配置 SBC8000 设备的名称。



图 3-6-1 系统管理

3.6.2 web 配置管理

web 配置管理用于管理 TLS 证书和访问 web 的超时自动退出时间

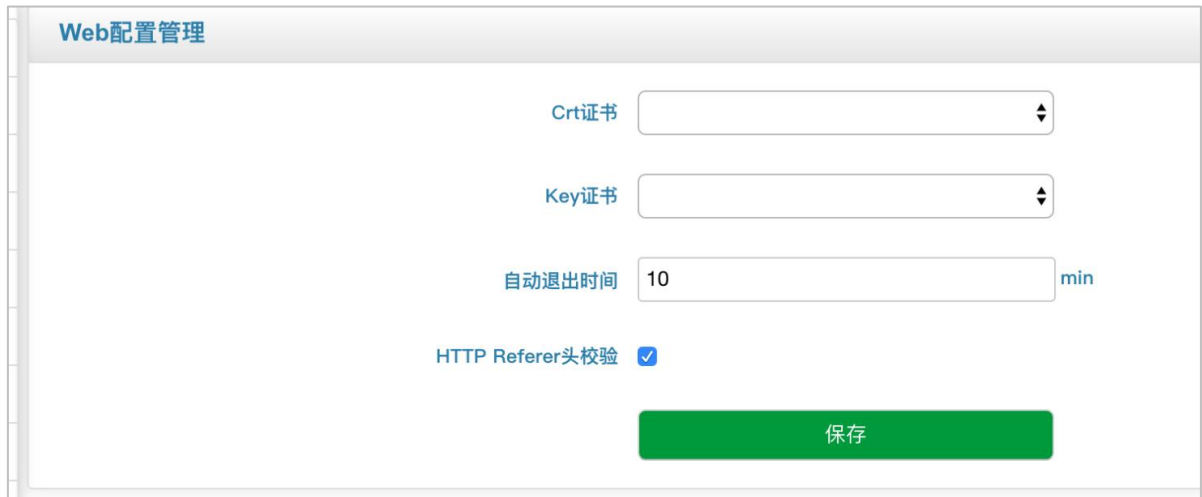


图 3-6-2 web 配置管理

3.6.3 接口管理

接口管理配置设备网口的属性---管理口/业务口，注意 SBC8000 只是对应操作系统的的一个应用程序，所以 SBC8000 应用的 IP 地址、子网掩码、网关和 DNS 等配置需要在对应操作系统里配置。

网络管理											
名称	业务管理	MTU大小	Mac地址	IPV4地址	子网掩码	IPV4网关	IPV4 DNS	IPV6地址	IPV6网关	IPV6 DNS	索引
eth0	管理口	1500	00:0c:29:3c:bc:25	172.30.0.56	255.255.0.0	172.30.0.1	/				0
lo	未定义	65536		127.0.0.1	255.0.0.0		/				

浮动IP管理				+ Add
接口	索引	IP地址	子网掩码	
eth0:1	1	172.30.0.177	255.255.0.0	

图 3-6-3 接口管理

图 3-6-4 网络管理的网口配置

浮动 IP 管理，用户双机热备时配置的辅助 IP 地址，非双机权限不显示

图 3-6-5 浮动 IP 管理

表 3-6-1 接口管理

参数	参数描述
接口	网络管理里的接口名称，名称基于物理网口名称
索引	正整数数字
IP 地址	对应网络接口的 IP 地址
子网掩码	对应网络接口的子网掩码

3.6.4 静态路由

当设置静态路由后，去往指定目的地的报文将按照指定的路径进行转发。点击  按钮，即进入静态路由设置页面。

The screenshot shows a configuration form for a static route. The fields are:

- 优先级 (Priority): 127
- 描述 (Description): [Empty]
- 目的IP (Destination IP): [Empty]
- 子网掩码 (Subnet Mask): [Empty]
- 接口 (Interface): eth0
- 下一跳 (Next Hop): [Empty]

 At the bottom, there are two green buttons: '提交' (Submit) and '取消' (Cancel).

图 3-6-5 静态路由配置

表 3-6-2 静态路由

参数	参数描述
优先级	静态路由的优先级，数字越小优先级越高
描述	对该静态路由的详细描述
目的 IP	静态路由需要到达的目的 IP 地址
子网掩码	静态路由需要到达的目的地址的子网掩码
接口	该静态路由发送报文时走的网络接口
下一跳	数据在到达目的地址前，需要经过的下一跳网关地址

3.6.5 用户管理

用户管理用来修改超级用户 `admin` 的密码和添加其它能够登录该设备的用户、密码和对应权限。

1) 密码设置

The screenshot shows the '密码设置' (Password Settings) interface. It contains four input fields:

- 旧密码 (Old Password)
- 新密码 (New Password)
- 密码强度 (Password Strength)
- 密码确认 (Password Confirmation)

 Each field has a small eye icon to the right, indicating it is a password field. At the bottom, there is a green '提交' (Submit) button.

图 3-6-6 超级用户 admin 的密码设置

出于系统安全方面的考虑，建议设置较为复杂的密码。

2) 用户列表

在用户列表页面，可添加除 admin 外的可以登录该 SBC 设备的其它用户。

The screenshot shows a '用户列表' (User List) interface. At the top, there is a table with columns '用户名' (Username) and '角色' (Role). The table contains one entry: 'mos' with the role '管理员' (Administrator). To the right of the table are '+ Add', '刷新' (Refresh), and '删除' (Delete) buttons. Below the table is a form for adding a new user. The form includes fields for '用户名' (Username), '密码' (Password), '密码强度' (Password Strength), '密码确认' (Password Confirmation), and '角色' (Role) set to 'Admin'. There is also a 'Web Access Permission' section with checkboxes for '首页' (Home), '业务' (Business), '安全' (Security), '系统' (System), and '维护' (Maintenance), each with a 'View' button. At the bottom of the form are '提交' (Submit) and '取消' (Cancel) buttons.

图 3-6-7 添加用户及设置权限

表 3-6-3 用户列表

参数	参数描述
用户名	用户登录 SBC 设备的账户名称
密码	用户登录 SBC 设备的密码
确认密码	确认用户登录 SBC 设备的密码，要求与密码要求一致
密码强度	设置的密码的强度
角色	<p>管理员：可以添加操作员和维护员角色用户，可以重置其它用户密码，可以对 web 数据进行增加、修改和删除，管理员用户只有 admin 一个</p> <p>操作员：可以访问大部分配置，修改配置数据等</p> <p>维护员：只能查看 web 上的状态和大部分配置，无修改删除权限</p>

3.6.6 版本升级

通过 Web 界面，可以将设备版本进行升级或回退。版本升级后需要重启设备才能生效。



图 3-6-8 版本升级

一般情况下，版本升级文件为 1.91.x.x.ldf 文件，请不要选择其它产品的版本文件进行升级。

3.6.7 备份与恢复

在“备份与恢复”页面，用户可将 Web 上菜单栏业务的所有配置、网络配置和数字证书管理配置的数据进行备份或者恢复。恢复数据后设备会自动重启生效。



图 3-6-9 备份与恢复

表 3-6-4 备份与恢复

参数	参数描述
备份	下载需备份的 web 的配置数据，可以分别备份业务、证书文件、和网络配置，也可以任意组合备份，网络配置包括接口管理和静态路由的数据。
恢复	将备份的数据恢复到设备系统上，恢复成功设备会自动重启。
恢复出厂设置	将配置数据恢复到设备的出厂默认值

3.6.8 License 管理

License 管理限制设备的使用时长、注册最大用户数、最大并呼叫发数、最大每秒注册数、最大每秒呼叫数和最大转码呼叫数。License 过期后，其它设备将不能通过 SBC8000 进行注册和呼叫。

License管理	
当前SN号	2
设备序列号	1ba1-42fd-21f3-e070
硬件序列号	246D-978F-05FF
License类型	demo
License创建时间	2021-08-31 16:15:53.141568643 +0800 +0800
有效期	30days 00:00:00
License剩余时间	20days 05:29:56
最大并发呼叫数	10000
最大转码呼叫数	5000
最大用户数	100000
最大每秒注册数	500
最大每秒呼叫数	500
主备	双机热备

请输入你的License

提交
清除

图 3-6-10 License 管理

3.6.9 数字证书管理

数字证书管理用于添加登录设备的 Web 界面的安全证书，只有证书认证通过，主机才能登录到设备的 Web 界面。

数字证书管理			+ Add
证书组名称	Crt证书	Key证书	
test	cert_servercert.cer	key_serverkey.key	<input type="button" value="刷新"/> <input type="button" value="删除"/>

名称

CRT文件 未选择文件。

KEY文件 未选择文件。

提交
取消

图 3-6-11 数字证书管理

3.6.10 用户板管理

用户板管理用于显示媒体端口范围

用户板管理		
类型	端口范围	用户板端口启用
MFU0	16384-57343	<input checked="" type="checkbox"/>
CPU0	16384-57343	<input checked="" type="checkbox"/>

保存

图 3-6-12 数字证书管理

3.7 维护

3.7.1 日志

在日志页面，用户可以查看系统的登录日志、操作日志和安全日志可做日志管理和日志服务器配置。

登录日志						
10	搜索: 名称	类型	开始时间	结束时间	来源	提交
编号	用户名	角色类型	时间	公网IP	来源	事件描述
1	admin	admin	2017-11-29 23:59:25	172.16.120.143:64871	web	登录成功
2	admin	admin	2017-11-29 19:39:07	172.16.120.143:51461	web	登录成功
3	admin	admin	2017-11-29 19:11:12	172.16.120.143:50756	web	登录成功
4	admin	admin	2017-11-28 19:57:31	172.16.120.143:63273	web	登录成功

图 3-7-1 登录日志

操作日志							
10	搜索: 名称	类型	开始时间	结束时间	来源	提交	
序号	用户名	角色类型	操作时间	登录IP	来源	操作	操作内容
1	admin	admin	2021-09-09 04:20:48	172.23.234.100:59045	web	Apply	intmanacfg
2	admin	admin	2021-09-09 04:20:46	172.23.234.100:59045	web	Mod.	intmanacfg
3	admin	admin	2021-09-09 04:20:09	172.23.234.100:55359	web	Apply	intmanacfg
4	admin	admin	2021-09-09 04:20:07	172.23.234.100:55359	web	Mod.	intmanacfg
5	admin	admin	2021-09-09 02:39:54	172.22.1.188:51609	web	Apply	号码池
6	admin	admin	2021-09-08 23:40:48	172.22.1.188:51609	web	Add	号码池/3r
7	admin	admin	2021-09-08 21:45:06	172.22.1.188:50540	web	Apply	核心中继
8	admin	admin	2021-09-08 21:45:02	172.22.1.188:49651	web	Mod.	核心中继/10016
9	admin	admin	2021-09-08 21:44:22	172.22.1.188:50540	web	Apply	SIP账户
10	admin	admin	2021-09-08 21:44:18	172.22.1.188:50543	web	Add	SIP账户/mos

图 3-7-2 操作日志

安全日志									
10	search: Start Time	End Time	Type	Source	IP	Interface	Port	提交	
编号	攻击时间	攻击类型	告警来源	IP地址	接口	端口	触发条件	动作	

图 3-7-3 安全日志



图 3-7-4 日志管理



图 3-7-5 日志服务器

3.7.2 Ping

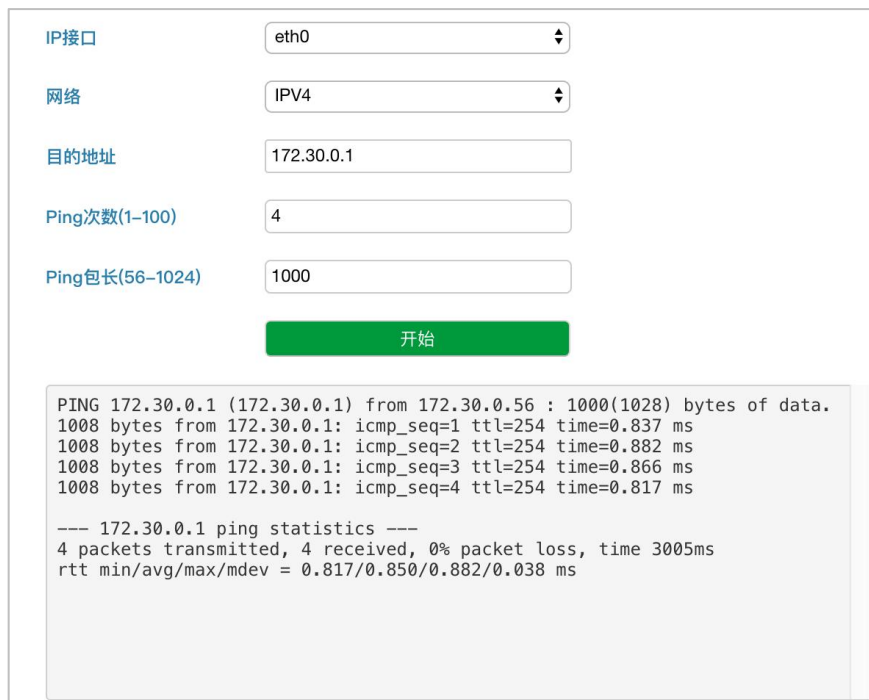


图 3-7-6 ping

Ping 命令详解：Ping 是对一个网址发送测试数据包，看对方网址是否有响应并统计响应时间，以此测试网络。

应用格式：Ping IP 地址。它是用来检查网络是否通畅或者网络连接速度的命令。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

Ping 命令使用说明：

- 1) 选择要 ping 的网络接口 admin、eth0、eth1、eth2 或者 eth3；
- 2) 在 ping 输入框内输入要 ping 的 IP 地址或者域名，并设置 ping 的次数和 ping 报文的长度，点击开始进行连通性检测；
- 3) 收到全部响应报文表明网络连接正常，否则网络连接有故障。

3.7.3 tracert

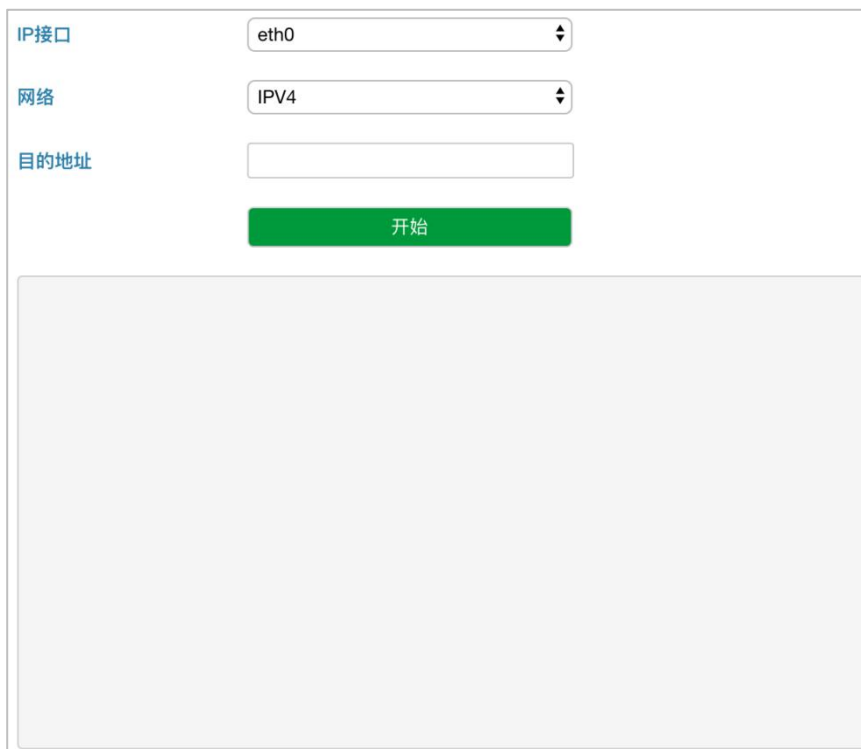


图 3-7-7 tracert

Tracert 命令详解：Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

通过向目标发送不同 IP 生存时间 (TTL) 值的“Internet 控制消息协议 (ICMP)”回应数据包，Tracert 诊断程序确定到目标所采取的路径，要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已

超时”的消息发回源系统。

Tracert 使用说明：

- 1) 选择要 tracert 的网络接口 admin、eth0、eth1、eth2 或者 eth3；
- 2) 在 tracert 输入框内输入 IP 地址或者域名，点击开始开始进行路由跟踪；
- 3) 根据结果查看路由跟踪信息。

3.7.4 正则表达式

正则表达式测试

正则表达式

待匹配文本

测试匹配

测试结果

例如

- `^0755.*` 匹配以0755开头的所有电话号码
- `^(0755|^8899|^0110).*` 匹配以0755、8899或0110开头的所有电话号码
- `^[1][358][0-9]{9}$` 匹配第一个数字为1、第二个数字是3/5/8、剩下9个数字为0-9中的任意数字的号码

正则表达式都兼容于PCRE

常用的正则表达式

- `^` 匹配输入字符串的开始位置，例如：`^134.*`匹配以134开头的电话号码。
- `$` 匹配输入字符串的结束位置，例如：`.*2$`匹配以2结束的电话号码。
- `|` 用来分开可匹配的多种可能性，例如：`2|3|4`匹配2、3或者4。
- `\` 将下一个字符标记为一个特殊字符、原义字符、向后引用或者八进制转义符。
- `[]` 字符集合。匹配所包含的任意一个字符，例如：`[123]`匹配1、2或者3；`[0-9]`匹配0到9之间的任意一个字符。
- `[^]` 负值字符集合。匹配未包含在[]里的任意字符。例如：`[^9]`匹配除9以外的任何字符。
- `.` 匹配除换行符之外的任何单一字符。例如：`3.4`匹配314、324、334、344.....等
- `?` 匹配此符合之前的字符0次或1次，例如：`colou?r`匹配color或colour。
- `*` 匹配此符合之前的字符0次或多次，例如：`ab*c`匹配ac、abc、abbc、abbbc等。
- `+` 匹配此符合之前的字符1次或多次，例如：`ab+c`匹配abc、abbc、abbbc等，但不匹配ac。
- `\d` 表示一个数字字符，等价于`[0-9]`。
- `\D` 匹配一个非数字字符，等价于`[^0-9]`。
- `\s` 匹配空白字符，包括空格、制表符、换页符等等。
- `\S` 匹配不是空白字符的任意字符。

图 3-7-8 正则表达式

SBC 的路由匹配、黑白名单匹配等众多业务配置中大多都支持正则表达式，这里可以校验设置正则表达式规则是否符合预期要求。

告警

显示 SBC8000 的告警信息。

序号	名称	时间	告警级别	类别	内容	告警类型	来源	确认
1	BFD Packet Delay	2021-09-08 05:14:11	警告	service	key : 8868:172.30.0.56:172.30.0.234, delay > 24951ms, default : 100ms	alarm	BFD	未确认 <input type="checkbox"/>
2	board	2021-09-08 04:51:44	关键	system	a plate with a slot number 0 is pulled out	alarm	boardstate	未确认 <input type="checkbox"/>
3	subboard	2021-09-08 04:51:44	关键	system	a plate with a slot number 0 is pulled out	alarm	subboardstate	未确认 <input type="checkbox"/>
4	subboard	2021-09-08 04:51:01	关键	system	a plate with a slot number 0 is inserted	repair	subboardstate	未确认 <input type="checkbox"/>
5	board	2021-09-08 04:51:00	关键	system	a plate with a slot number 0 is inserted	repair	boardstate	未确认 <input type="checkbox"/>
6	board	2021-09-08 04:51:00	关键	system	a plate with a slot number 0 is pulled out	alarm	boardstate	未确认 <input type="checkbox"/>
7	subboard	2021-09-08 04:51:00	关键	system	a plate with a slot number 0 is pulled out	alarm	subboardstate	未确认 <input type="checkbox"/>
8	subboard	2021-09-01 05:09:22	关键	system	a plate with a slot number 0 is inserted	repair	subboardstate	未确认 <input type="checkbox"/>
9	board	2021-09-01 05:09:21	关键	system	a plate with a slot number 0 is inserted	repair	boardstate	未确认 <input type="checkbox"/>
10	board	2021-09-01 05:09:21	关键	system	a plate with a slot number 0 is pulled out	alarm	boardstate	未确认 <input type="checkbox"/>

图 3-7-9 告警

3.7.5 SNMP

SNMP(Simple Network Management Protocol,简单网络管理协议)的前身是简单网关监控协议(SGMP),用来对通信线路进行管理。随后,人们对 SGMP 进行了很大的修改,特别是加入了符合 Internet 定义的 SMI 和 MIB: 体系结构,改进后的协议就是著名的 SNMP。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台,因此 SNMP 受 Internet 标准网络管理框架的影响也很大。现在 SNMP 已经出到第三个版本的协议,其功能较以前已经大大地加强和改进了。

目前 SBC8000 可以能够支持 SNMP 的三个版本:

SNMP配置	
开启 SNMP	SNMP监听端口
开启	554

开启 SNMP	是 <input checked="" type="radio"/> 否 <input type="radio"/>
SNMP 版本	v2c
SNMP监听端口	* 554

共同体配置	
共同体	源地址
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

注意：源地址的缺省值为default。如果不是，输入IP地址！

共同体加入组	
组名	共同体
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

mib视图配置			
视图名	视图类型	mib树	掩码
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

注意：mib树的格式:x.x.x.x.x,如果只有一个x,格式为:x(x为正整数)

访问规则配置(v1/v2c)			
组名	读视图	写视图	陷阱视图
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

陷阱配置			
陷阱类型	IP地址	端口	共同体
v2c	<input type="text"/>	162	public

图 3-7-10 SNMP

3.7.6 远程连接配置

用于配置 DRP 远程连接管理

远程连接配置

加入远程管理计划

接口

服务器URL/IP

服务器端口

图 3-7-11 远程连接配置

4 术语

术语	解释
SBC	会话边界控制器 (Session Border Controller)
SIP	会话发起协议 (Session Initiation Protocol)
DTMF	双音多频 (Dual Tone Multi Frequency)
NAT	网络地址转换 (Network Address Translation)
VoIP	互联网协议电话 (Voice over Internet Protocol)
DSP	数字信号处理器 (Digital Signal Processor)
SIP	会话发起协议 (Session Initiation Protocol)
DTMF	双音多频 (Dual Tone Multi Frequency)
USSD	非结构化补充数据业务 (Unstructured Supplementary Service Data)
PSTN	公共交换电话网 (Public Switched Telephone Network)
IVR	语音交互式应答 (Interactive Voice Response)

附录 【跟踪命令】

一、en 模式下常用命令：

Welcome to Command Shell!

Username:admin

Password:*****

ROS>en

ROS#

- 1、查看系统当前时间，启动时间和运行时间 ROS#sh clock
- 2、查看各用户板状态..... enable# show board state
- 3、查看 dsp 信息..... enable#sh dsp info
- 4、查看当前呼叫..... enable#Show call info
- 5、查看系统时间..... enable#show date
- 6、查看产品型号和序列号..... enable# show device
- 7、查看接入网/接入网中继/核心网中继状态..... enable# show endpoint callstat
- 8、查看系统故障日志..... enable# show error
- 9、查看系统内存使用情况..... enable# show flash
- 10、查看网络 IP 信息..... enable# show interface
- 11、查看网络端口信息..... enable# show netstat
- 12、查看用户注册状态..... enable# show register info
- 13、查看系统服务运行状态..... enable# show service
- 14、查看系统运行时间..... enable# show uptime
- 15、查看系统版本..... enable# show version

二、常用跟踪命令

SSH 登录后

Username: admin

Password:

> enable

admin@SBC8000 enable#

-
- 1、打开跟踪开关..... `enable # trace ?`
- `all` 打开全部跟踪
- `board` 打开用户板跟踪（输入? 可以查看后续参数）
- `call` 打开呼叫跟踪（后面还有四个参数 主叫号码 被叫号码 呼入中继名称 呼出中继名称； *代表任意）
- `level` 设置跟踪等级(disable/emerg/alert/crit/err/warning/notice/info/debug/detail)
- `register` 打开注册跟踪（后面还有三个参数 用户名 接入网名称 核心网名称； *代表任意）
- `transport` 打开传输跟踪（后面还有六个参数 传输协议 源 IP:端口 目的 IP:端口 主叫号码 被叫号码 SIP 方法，输入? 可以查看后续参数说明）
- 2、进入跟踪..... `enable#ada`
- 3、退出跟踪..... `ada> exit`
- 4、查看进程占用情况..... `enable#top`
- 5、查看系统进程..... `enable #ps`
- 6、重启设备..... `enable #reboot system`
- 7、重启用户板..... `enable #reboot board [0-3]`
- 8、关闭跟踪..... `enable #no trace all`