

ICS 33.040.40

M 32



# 中华人民共和国通信行业标准

YD/T 1911-2009

---

## 软交换业务接入控制设备 安全技术要求和测试方法

Security Technical Requirements and Test Methods for  
Softswitch Services Access Control Device

2009-06-15 发布

2009-09-01 实施

---

中华人民共和国工业和信息化部 发布

# 目 次

前 言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
4 软交换业务接入控制设备在软交换网络中的位置 .....	2
5 信令面安全 .....	2
5.1 概述 .....	2
5.2 SAC和软交换终端之间接口的安全要求 .....	3
5.3 SAC和软交换网络相关实体之间接口的安全要求 .....	3
6 媒体面安全 .....	3
7 可靠性要求 .....	3
8 管理安全要求 .....	4
8.1 权限管理 .....	4
8.2 日志管理 .....	4
8.3 远程管理的安全要求 .....	4
8.4 消息跟踪要求 .....	5
8.5 故障管理 .....	5
9 地址溯源和防火墙相关功能（可选） .....	5
10 SAC安全测试方法 .....	5
10.1 测试配置图及测试说明 .....	5
10.2 测试项目 .....	6

## 前 言

本标准是软交换网络安全系列标准之一，该系列标准的名称及结构预计如下：

1. 软交换网络网管与运维安全技术要求
2. 软交换设备安全技术要求和测试方法
3. 基于软交换的应用服务器设备安全技术要求和测试方法
4. 基于软交换的媒体服务器设备安全技术要求和测试方法
5. 软交换业务接入控制设备安全技术要求和测试方法
6. 基于软交换的信令网关设备安全技术要求和测试方法
7. 媒体网关设备安全技术要求和测试方法
8. IP 智能终端设备安全技术要求和测试方法

由于软交换业务接入控制设备是保证软交换网络安全的重要边缘接入设备，相关技术、规范仍在不断的研究、发展之中，因此随着技术的发展，将不断完善本标准的内容。

本标准与YD/T 1927-2009《软交换业务接入控制设备技术要求》配套使用。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院

本标准主要起草人：李海花、蒋晓琳、段世惠

# 软交换业务接入控制设备安全技术要求及测试方法

## 1 范围

本标准给出了和软交换业务接入控制设备相关的安全技术要求，主要包括信令面安全要求、媒体面安全要求、可靠性要求、管理安全要求、地址溯源和防火墙相关功能要求，并根据安全要求制定了相应的测试方法。

本标准适用于软交换网络中由运营商提供、维护和管理的软交换业务接入控制设备。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1466-2006	IP 安全协议（IPSec）穿越网络地址翻译（NAT）技术要求
YD/T 1707-2007	防火墙设备测试方法
YD/T 1927-2009	软交换业务接入控制设备技术要求
YDC 045-2007	基于软交换的网络组网总体技术要求

## 3 术语、定义和缩略语

下列术语和定义适用于本标准。

### 3.1 术语和定义

**软交换业务接入控制设备** Service Access Controller

软交换业务接入控制设备是软交换网络的边缘汇聚设备，主要功能为用户接入和业务控制，并完成用户的信令流和媒体流的代理功能。该设备同时具有会话管理、地址转换（包括IP层地址转换和应用层地址转换）等功能，并可以配合软交换核心设备完成一定的安全防护、QoS管理等功能。

### 3.2 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	接入控制列表
DDoS	Distributed Deny of service	分布式的拒绝服务
DoS	Deny of service	拒绝服务
ESP	Encapsulation Security Payload	封装安全载荷
IAD	Integrated Access Device	综合接入设备
MGCP	Media Gateway Control Protocol	媒体网关控制协议
PE	Provider Edger Router	运营商边缘路由器
PPPoE	PPP over Ethernet	以太网点到点协议
SAC	Service Access Controller	软交换业务接入控制设备

SIP	Session Initiation Protocol	会话初始协议
SNMP	Simple Network Manage Protocol	简单网络管理协议
SS	Soft Switch	软交换
VPN	Virtue Private Network	虚拟专用网
HLSR	Home Location and Service Register	归属位置业务寄存器
NBP	Network Border Point	网络边界点
IAD	Integrated Access Device	综合接入设备
SCN	Switched Circuit Network	电路交换网
NGN	Next Generation Network	下一代网

#### 4 软交换业务接入控制设备在软交换网络中的位置

软交换业务接入控制设备（SAC，Service Access Controller）在软交换网络中的位置如图1所示。

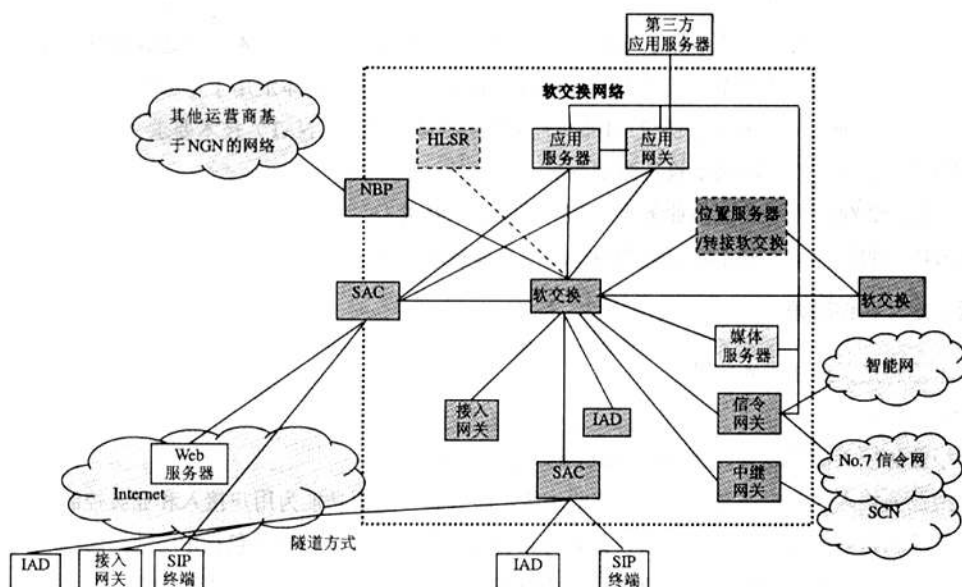


图1 SAC在软交换网络中的位置

SAC位于软交换网络边缘，用于接入不可信任设备（不可信任的用户终端主要指IAD和SIP终端），对通过不可信任设备接入到软交换网络中的用户进行接入和业务控制，提供用户的信令流和媒体流的代理功能，同时该设备具有安全防护、媒体管理、地址转换（包括IP层地址转换和应用层地址转换）等功能，配合软交换核心设备实现用户管理和业务管理，配合承载网实现QoS管理。

#### 5 信令面安全

##### 5.1 概述

软交换网络中信令流采用分段的保护机制。

## 5.2 SAC 和软交换终端之间接口的安全要求

### 5.2.1 信令流代理功能

SAC提供信令流代理功能，向不可信任的用户终端（本标准中特指不可信任的IAD或SIP终端，以下简称用户终端）屏蔽软交换设备的具体信息，不可信任的用户终端和软交换之间的所有信令消息必须经SAC转发。

### 5.2.2 信令流通信安全要求

#### 5.2.2.1 注册/注销阶段

SAC和软交换终端应该提供对信令的强安全保护，SAC作为软交换设备的代理，应和软交换设备配合实现对软交换用户或软交换终端的身份认证。

收到用户终端发送的注册消息时，如果SAC能够获得该用户终端所对应的接入数据线相关信息，则将这些信息插入到注册消息中并执行地址翻译功能，然后向软交换转发。在其他情况下，SAC向注册消息中插入所获得的和用户终端相关的网络信息（如IP地址、VLAN标识等），并执行地址翻译功能，然后向软交换转发该消息。

如果收到软交换回送的注册响应消息，则：

- 如果注册成功，SAC保存用户的在线状态以及相关的网络信息，然后执行地址翻译功能，并将该消息发送给相应终端；
- 如果注册失败，SAC执行地址翻译功能，并将该消息发送给用户终端，同时删除所保存的和用户相关的信息。

如果SAC收到终端发送的注销消息，执行地址翻译功能并向对应的软交换转发该消息；当收到对应的注销响应消息时，SAC执行地址翻译功能并将该消息发送给用户终端，同时删除所保存的和用户相关的信息。

#### 5.2.2.2 呼叫阶段

SAC应该能够根据用户的在线状态以及所保存的用户（用户终端）信息，对用户终端发送的IP分组包进行合法性分析，如果报文不合法，SAC将丢弃该报文，防止对软交换设备的恶意攻击。

## 5.3 SAC 和软交换网络相关实体之间接口的安全要求

软交换网络应能够保证SAC和软交换网络相关实体之间（主要是软交换设备、媒体服务器、其他SAC）的通信安全，SAC和软交换网络相关实体之间的通信安全可优先通过承载网的规划构建安全信任域的方式实现，构建安全信任域的方式见YDC 045-2007《基于软交换的网络组网总体技术要求》中对承载网的技术要求。

## 6 媒体面安全

SAC具有媒体流代理功能，用户终端发送和接收的所有媒体信息都可以经过SAC。具体要求见YD/T 1927-2009《软交换业务接入控制设备技术要求》。

## 7 可靠性要求

SAC作为电信设备，应提供以下通用功能。

1) SAC应能够满足YD/T 1927-2009《软交换业务接入控制设备技术要求》中“可靠性要求”一章的相关要求。

## 2) 硬件要求

设备应提供对重要部件的冗余备份和容错管理,设备内关键的物理部件均支持冗余配置,如主CPU部件、数据库部件、管理中心接口、操作维护工作站接口、时钟源输入接口、时钟系统、风扇等,主要单板采用热备份方式,所有单板均支持热插拔。当相关模块发生故障时,能自动切换到备用处理模块而不影响当前呼叫的状态。

## 3) 软件要求

在不影响正常通信的情况下,能够完成对程序的打补丁或对系统的升级。

能够实时地接受操作维护对数据的查询、更改、生成和删除,但不影响软件的正常运行。

支持对打补丁或升级软件的回退功能。

## 4) 过负荷控制要求

设备应具有过负荷控制能力,能够对过负荷进行4级控制,根据过负荷的情况自动判定过负荷的级别,拒绝一定比例的新请求。

## 5) 系统重新启动时间

SAC的重新启动时间应小于20min。

上述具体要求见YD/T 1927-2009《软交换业务接入控制设备技术要求》。

# 8 管理安全要求

## 8.1 权限管理

在管理员进入系统之前,应鉴别管理员身份,鉴别时采用账户和密码机制,密码应是不可见的,并在存储和传输时加密保护,并且系统对每次访问应进行记录。

在经过一定次数的身份鉴别失败以后,SAC应锁定该账号。最多失败次数仅由授权管理员设定。

SAC应对管理员的访问权限有严格的规定。根据维护员的需要,系统可以对其权限进行分类,如系统管理员、配置管理员、维护管理员等,防止非授权登录和操作。

## 8.2 日志管理

SAC应记录所有操作员的所有操作日志,内容至少应包括:操作时间、命令执行时间、操作员、操作终端、输入的命令内容、命令的执行结果等。

## 8.3 远程管理的安全要求

设备应具有与本地和远端操作员工作站的接口,以支持相关的监控、管理和维护。

SAC至少支持以下一种远程管理安全机制。

### 1) SNMP

采用SNMPv2c作为远程管理安全机制。

### 2) 远程登录

建议支持SSHv1和SSHv2,通过认证算法和加密算法实现对管理信息的机密性和完整性保护。

### 3) Web 管理

可通过支持SSL/TLS安全协议,实现对管理信息的机密性和完整性保护。

### 4) 其他

对于设备特定的远程管理机制,也应提供相应的机制实现对管理信息的机密性和完整性保护。

另外,设备应提供关闭远程管理功能和管理员认为不必要服务的能力,且所有远程管理功能缺省是

关闭的。

#### 8.4 消息跟踪要求

设备应该具有消息（信令消息和/或媒体消息）跟踪的能力，可以根据操作员的指令，对各种消息进行跟踪，包括从设备发出的和收到的消息。

消息跟踪的结果可以显示在终端上或输出到打印机。

#### 8.5 故障管理

设备要具有以下故障管理功能。

##### （1）告警的级别

应具备完善的告警系统，并可以按照故障的严重程度分类，一般至少应分为两大类，即紧急告警和非紧急告警。

##### （2）告警的记录

要具有记录所有告警消息的功能，并能够查询告警记录。

##### （3）告警的显示

设备的操作维护管理终端上应该能够显示告警信息，对紧急告警应可提供可见或可闻的警示信息。

### 9 地址溯源和防火墙相关功能（可选）

当用户向软交换设备发起注册请求时，SAC应能够记录并提供源MAC地址、源IP地址、接口、VLAN的绑定。SAC应丢弃不符合绑定关系的数据包。当用户发起呼叫时，SAC应能识别用户的合法性并保留呼叫状态，从而拒绝状态机之外的消息的接入。SAC设备应在本地保存用户登录日志信息。

SAC应能配置端口镜像，应能配置基于物理端口的镜像，可以配置基于逻辑端口的镜像和基于访问控制列表的流镜像。

SAC可选提供防火墙相关功能，应考虑实现的功能如下。

1) 包过滤技术：SAC能够产生一定的过滤规则集，根据过滤规则对IP包进行过滤，如可以根据IP地址、TCP/UDP/ICMP、应用层协议等过滤。

2) 信息内容过滤技术：SAC可以识别应用层协议，根据所设置的过滤条件，对信息流进行控制。

3) VPN功能：SAC应该支持IPSec VPN功能，具体见YD/T 1466-2006。

4) 抗攻击性要求：SAC应能够抵抗对受保护网络内部的攻击，能够抵抗抗大流量攻击能力，具备抗畸形包处理功能。SAC应该具有防DoS攻击能力，应该至少支持某些防DoS和分布式DoS攻击的机制，如TCP SYN Flood攻击、Ping超大包攻击、Smurf攻击、ICMP攻击、IP分片攻击等。

5) 带宽管理功能：SAC应该支持每端口、每VLAN、每用户的带宽管理，可以设置每端口、每VLAN、每用户的接收和发送速率，并对每端口、每VLAN、每用户的接受包、发送包和包丢失率进行统计。

### 10 SAC 安全测试方法

#### 10.1 测试配置图及测试说明

SAC测试配置图如图2所示。

图2中，SAC1（SAC1）为被测试设备，该设备和用户终端、软交换设备之间建立连接，用户终端包括SIP终端、H.248终端和MGCP终端，图2中的软交换设备、SAC2以及SAC2下面连接的用户终端属于配合测试设备，测试中可能用到多个软交换设备，网络模拟器用来模拟IP网络的各种情况，协议分析仪则



对用户终端和SAC1之间、SAC1和软交换设备之间、SAC1传送的媒体数据包进行监测。

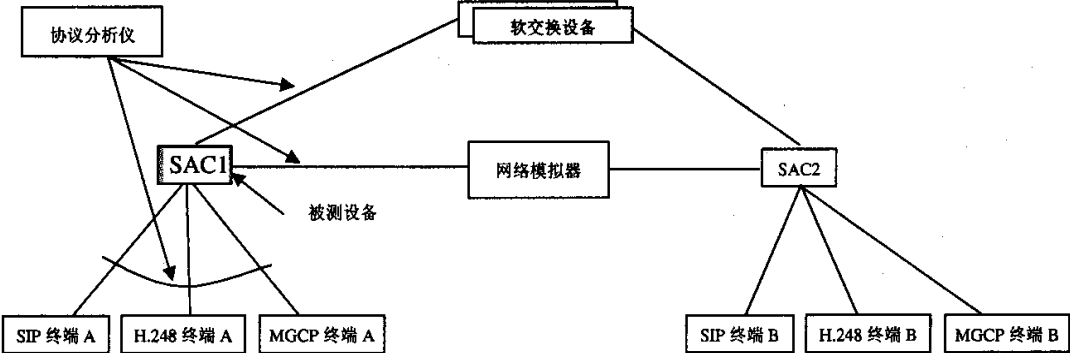


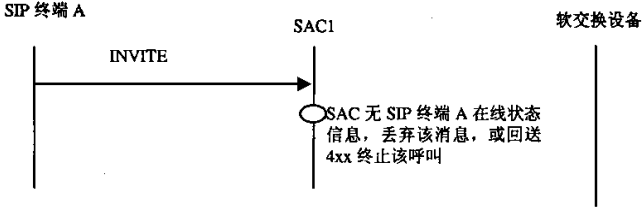
图2 SAC安全测试配置

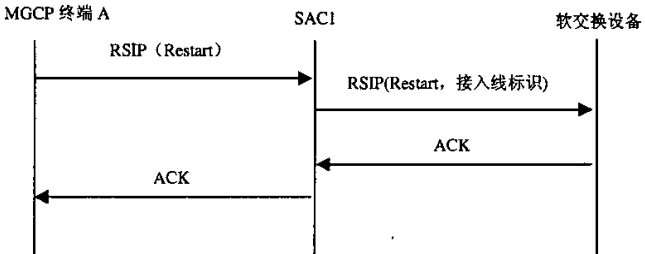
10.2 测试项目

10.2.1 信令面安全测试（SAC 和软交换终端之间）

测试编号：	1.1.1
测试项目：	SIP 信令代理功能测试——注册过程
预置条件：	1) SAC 正常工作。 2) SIP 终端 A 还未注册。 3) 用协议分析仪检测 SAC 和 SIP 终端 A、软交换设备之间的信令消息
测试配置：	图 2
测试步骤：	1) SIP 终端 A 向软交换设备发起注册，注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果：	1) SIP 终端 A 注册成功。 2) 消息流程如下所示： <div><div>SIPA 终端 A</div><div>SAC1</div><div>软交换设备</div><div>REGISTER</div><div>REGISTER</div><div>401</div><div>401</div><div>REGISTER</div><div>REGISTER</div><div>200 OK</div><div>200 OK</div></div> 3) 检查信令消息，SAC1 应该将 SIP 终端 A 发送的信令消息中（即图中的两个 Register 消息）和 SIP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备。同时 SAC1 应该将软交换设备发送的信令消息中（图中的 401 和 200OK 消息）和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 SIP 终端 A。 4) 检验软交换设备和 SAC1 上 SIP 终端 A 相关的状态信息
测试结果：	1) SIP 终端 A 在软交换设备上注册成功。 2) SAC1 上保存了 SIP 终端 A 的在线状态信息和相关的网络信息（线标识或 IP 地址等）

测试编号:	1.1.2
测试项目:	SIP 信令代理功能测试——呼叫过程
预置条件:	1) SAC 正常工作。 2) SIP 终端 A 已经在软交换设备上成功注册。 3) 用协议分析仪检测 SAC 和 SIP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) 从 SIP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 SIP 终端 A 释放呼叫
预期结果:	<div>1) 消息流程如下 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。</div> <div><div><div>SIP 终端 A</div><div>SAC1</div><div>软交换设备</div></div><div><div><div>INVITE</div><div>100 Trying</div><div>180 Ringing</div><div>200 OK</div><div>ACK</div><div>BYE</div><div>200 OK</div></div><div><div>INVITE</div><div>100 Trying</div><div>180 Ringing</div><div>200 OK</div><div>ACK</div><div>BYE</div><div>200 OK</div></div><div><div>INVITE</div><div>100 Trying</div><div>180 Ringing</div><div>200 OK</div><div>ACK</div><div>BYE</div><div>200 OK</div></div></div><div><div>主被叫通话</div></div></div> <div>2) 检查信令消息, SAC1 应该将 SIP 终端 A 发送的信令消息中和 SIP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 SIP 终端 A</div>
测试结果:	SAC1 正确执行了 SIP 信令代理功能

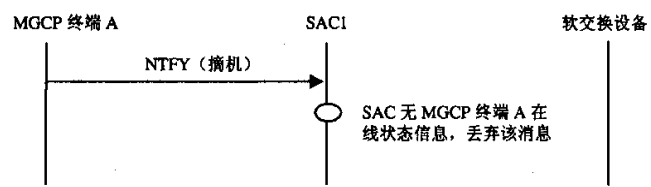
测试编号:	1.1.3
测试项目:	SIP 信令代理功能测试——异常呼叫过程, 未注册
预置条件:	1) SAC 正常工作。 2) SIP 终端 A 未在软交换设备上注册。 3) 用协议分析仪检测 SAC 和 SIP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	从 SIP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户
预期结果:	1) 消息流程如下所示:  <pre>sequenceDiagram     participant A as SIP 终端 A     participant SAC1     participant Soft as 软交换设备     A-&gt;&gt;SAC1: INVITE     Note over SAC1: SAC 无 SIP 终端 A 在线状态信息, 丢弃该消息, 或回送 4xx 终止该呼叫</pre> 2) 检查信令消息, SAC1 应丢弃该消息, 或向 SIP 终端 A 回送 4xx 终止该呼叫
测试结果:	1) SAC1 没有 SIP 终端 A 的在线状态信息。 2) SIP 终端 A 的呼叫不成功

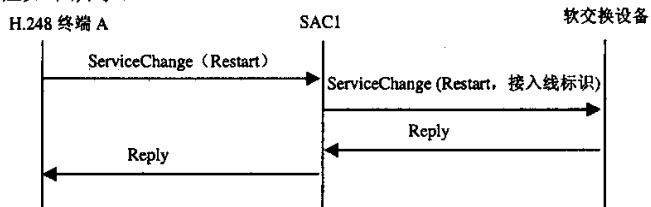
测试编号:	1.1.4 (可选)
测试项目:	MGCP 信令代理功能测试——线认证注册过程
预置条件:	1) SAC 正常工作。 2) MGCP 终端 A 还未注册。 3) MGCP 终端 A 采用接入线标识认证方式, 并在 SAC1 和软交换设备上相应的配置。 4) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) MGCP 终端 A 向软交换设备发起注册, 注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果:	1) MGCP 终端 A 注册成功。 2) 消息流程如下所示:  <pre>sequenceDiagram     participant A as MGCP 终端 A     participant SAC1     participant Soft as 软交换设备     A-&gt;&gt;SAC1: RSIP (Restart)     SAC1-&gt;&gt;Soft: RSIP(Restart, 接入线标识)     Soft-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK</pre> 3) 检查信令消息, SAC1 向收到的 RSIP 消息中插入接入线标识信息, 然后转发给软交换设备
测试结果:	1) MGCP 终端 A 在软交换设备上注册成功。 2) SAC1 上保存了 MGCP 终端 A 的在线状态信息和相关的网络信息 (线标识或 IP 地址等)

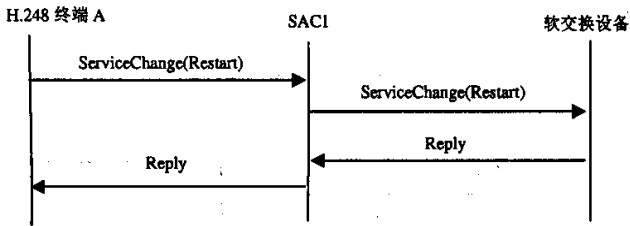
测试编号：	1.1.5（可选）
测试项目：	MGCP 信令代理功能测试——单向认证注册过程
预置条件：	1) SAC 正常工作。 2) MGCP 终端 A 还未注册。 3) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息
测试配置：	图 2
测试步骤：	1) MGCP 终端 A 向软交换设备发起注册，注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果：	1) MGCP 终端 A 注册成功。 2) 消息流程如下所示： <div data-bbox="276 693 1209 964"><pre>sequenceDiagram     participant A as MGCP 终端 A     participant SAC1     participant S as 软交换设备     A-&gt;&gt;SAC1: RSIP (Restart)     SAC1-&gt;&gt;S: RSIP(Restart)     S--&gt;&gt;SAC1: ACK     SAC1--&gt;&gt;A: ACK</pre></div> 3) 检查信令消息，SAC1 应该将 MGCP 终端 A 发送的信令消息中和 MGCP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备；同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 MGCP 终端 A。 4) 检验软交换设备和 SAC1 上 MGCP 终端 A 相关的状态信息
测试结果：	1) MGCP 终端 A 在软交换设备上注册成功。 2) SAC1 上保存了 MGCP 终端 A 的在线状态信息和相关的网络信息（线标识或 IP 地址等）

测试编号:	1.1.6 (可选)
测试项目:	MGCP 信令代理功能测试——双向认证注册过程
预置条件:	1) SAC 正常工作。 2) MGCP 终端 A 还未注册。 3) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) MGCP 终端 A 向软交换设备发起注册, 注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果:	<div>1) MGCP 终端 A 注册成功。 2) 消息流程如下所示:</div> <div><pre>sequenceDiagram     participant A as MGCP 终端 A     participant SAC1 as SAC1     participant S as 软交换设备      A-&gt;&gt;SAC1: RSIP (Restart)     SAC1-&gt;&gt;S: RSIP (Restart)     S-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     S-&gt;&gt;SAC1: RQNT     SAC1-&gt;&gt;A: RQNT     A-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;S: ACK     S-&gt;&gt;SAC1: RQNT     SAC1-&gt;&gt;A: RQNT     A-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;S: ACK     A-&gt;&gt;SAC1: NTFY     SAC1-&gt;&gt;S: NTFY     S-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK</pre></div> <div>3) 检查信令消息, SAC1 应该将 MGCP 终端 A 发送的信令消息中和 MGCP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 MGCP 终端 A。 4) 检验软交换设备和 SAC1 上 MGCP 终端 A 相关的状态信息</div>
测试结果:	1) MGCP 终端 A 在软交换设备上注册成功。 2) 相关信令消息中携带的认证和鉴权参数满足《媒体网关控制协议 (MGCP) 技术要求》中的相关要求。 3) SAC1 上保存了 MGCP 终端 A 的在线状态信息和相关的网络信息 (线标识或 IP 地址等)

测试编号:	1.1.7 (可选)
测试项目:	MGCP 信令代理功能测试——呼叫过程
预置条件:	1) SAC 正常工作。 2) MGCP 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) 从 MGCP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 MGCP 终端 A 释放呼叫
预期结果:	1) 消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。 <div><div>MGCP 终端 A</div><div>SAC1</div><div>软交换设备</div><pre>sequenceDiagram     participant A as MGCP 终端 A     participant S as SAC1     participant E as 软交换设备      A-&gt;&gt;S: NTFY (摘机)     S-&gt;&gt;E: NTFY (摘机)     E-&gt;&gt;S: ACK     S-&gt;&gt;A: RQNT     A-&gt;&gt;S: ACK     S-&gt;&gt;E: ACK     A-&gt;&gt;S: NTFY (被叫号码)     S-&gt;&gt;E: NTFY (被叫号码)     E-&gt;&gt;S: ACK     S-&gt;&gt;A: CRCX (Receiveonly)     A-&gt;&gt;S: ACK     S-&gt;&gt;E: ACK     A-&gt;&gt;S: RQNT (回铃音)     S-&gt;&gt;E: RQNT (回铃音)     E-&gt;&gt;S: ACK     A-&gt;&gt;S: RQNT (停回铃音)     S-&gt;&gt;E: RQNT (停回铃音)     E-&gt;&gt;S: ACK     A-&gt;&gt;S: MDCX (SendReceive)     S-&gt;&gt;E: MDCX (SendReceive)     E-&gt;&gt;S: ACK     Note over S: 主被叫通话     A-&gt;&gt;S: NTFY (挂机)     S-&gt;&gt;E: NTFY (挂机)     E-&gt;&gt;S: ACK     S-&gt;&gt;A: DLCX     A-&gt;&gt;S: ACK     S-&gt;&gt;E: ACK     A-&gt;&gt;S: RQNT     S-&gt;&gt;E: RQNT     E-&gt;&gt;S: ACK</pre></div> 2) 检查信令消息, SAC1 应该将 MGCP 终端 A 发送的信令消息中和 MGCP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 MGCP 终端 A
测试结果:	SAC1 正确执行了 MGCP 信令代理功能

测试编号:	1.1.8 (可选)
测试项目:	MGCP 信令代理功能测试——异常呼叫过程, 未注册
预置条件:	1) SAC 正常工作。 2) MGCP 终端 A 未在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	从 MGCP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户
预期结果:	1) 消息流程如下所示:  2) 检查信令消息, SAC1 应丢弃该消息
测试结果:	1) SAC1 没有 MGCP 终端 A 的在线状态信息。 2) MGCP 终端 A 的呼叫不成功

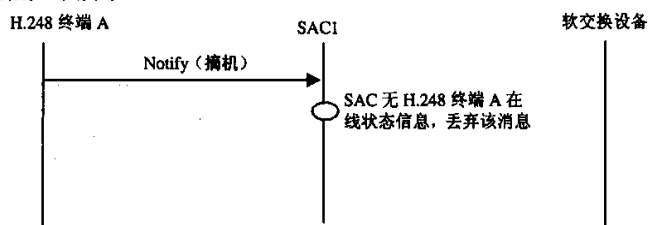
测试编号:	1.1.9 (可选)
测试项目:	H.248 信令代理功能测试——线认证注册过程
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 还未注册。 3) H.248 终端 A 采用接入线标识认证方式, 并在 SAC1 和软交换设备上进行了相应的配置。 4) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) H.248 终端 A 向软交换设备发起注册, 注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果:	1) H.248 终端 A 注册成功。 2) 消息流程如下所示:  3) 检查信令消息, SAC1 向收到的 Service Change 消息中插入接入线标识信息, 然后转发给软交换设备
测试结果:	1) H.248 终端 A 在软交换设备上注册成功。 2) SAC1 上保存了 H.248 终端 A 的在线状态信息和相关的网络信息(线标识或 IP 地址等)

测试编号:	1.1.10
测试项目:	H.248 信令代理功能测试——单向认证注册过程
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 还未注册。 3) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) H.248 终端 A 向软交换设备发起注册，注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果:	1) H.248 终端 A 注册成功。 2) 消息流程如下所示：  <pre>sequenceDiagram     participant A as H.248 终端 A     participant SAC1     participant S as 软交换设备     A-&gt;&gt;SAC1: ServiceChange(Restart)     SAC1-&gt;&gt;S: ServiceChange(Restart)     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply</pre> 3) 检查信令消息，SAC1 应该将 H.248 终端 A 发送的信令消息中和 H.248 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备；同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 H.248 终端 A。 4) 检验软交换设备和 SAC1 上 H.248 终端 A 相关的状态信息
测试结果:	1) H.248 终端 A 在软交换设备上注册成功。 2) SAC1 上保存了 H.248 终端 A 的在线状态信息和相关的网络信息(线标识或 IP 地址等)



测试编号:	1.1.11 (可选)
测试项目:	H.248 信令代理功能测试——双向认证注册过程
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 还未注册。 3) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) H.248 终端 A 向软交换设备发起注册, 注册消息中携带的信息正确。 2) 软交换设备正确进行响应
预期结果:	<div>1) H.248 终端 A 注册成功。 2) 消息流程如下所示:</div> <div><div><div>H.248 终端 A</div><div>SAC1</div><div>软交换设备</div></div><pre>sequenceDiagram     participant A as H.248 终端 A     participant SAC1     participant S as 软交换设备     A-&gt;&gt;SAC1: ServiceChange     SAC1-&gt;&gt;S: ServiceChange     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Modify     A--&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Modify     A--&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Reply</pre></div> <div>3) 检查信令消息, SAC1 应该将 H.248 终端 A 发送的信令消息中和 H.248 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 H.248 终端 A。 4) 检验软交换设备和 SAC1 上 H.248 终端 A 相关的状态信息</div>
测试结果:	1) H.248 终端 A 在软交换设备上注册成功。 2) 相关信令消息中携带的认证和鉴权参数满足《基于 H.248 的媒体网关控制协议》中的相关要求。 3) SAC1 上保存了 H.248 终端 A 的在线状态信息和相关的网络信息(线标识或 IP 地址等)

测试编号:	1.1.12
测试项目:	H.248 信令代理功能测试——呼叫过程
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	1) 从 H.248 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 H.248 终端 A 释放呼叫
预期结果:	<p>1) 消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。</p> <div><div>H.248 终端 A</div><div>SAC1</div><div>软交换设备</div><pre>sequenceDiagram     participant A as H.248 终端 A     participant SAC1 as SAC1     participant S as 软交换设备     A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Modify     A--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Add+Add     A--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Modify     A--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Notify     Note over A,SAC1: 主被叫通话     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Subtract+ Subtract     A--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Reply</pre></div> <p>2) 检查信令消息, SAC1 应该将 H.248 终端 A 发送的信令消息中和 H.248 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和软交换设备相关的地址信息修改为 SAC1 的地址信息再转发给 H.248 终端 A</p>
测试结果:	SAC1 正确执行了 H.248 信令代理功能

测试编号:	1.1.13
测试项目:	H.248 信令代理功能测试——异常呼叫过程, 未注册
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 未在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息
测试配置:	图 2
测试步骤:	从 H.248 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户
预期结果:	1) 消息流程如下所示:  <pre> sequenceDiagram     participant A as H.248 终端 A     participant SAC1 as SAC1     participant SW as 软交换设备     A-&gt;&gt;SAC1: Notify (摘机)     SAC1-&gt;&gt;SW: SAC 无 H.248 终端 A 在线状态信息, 丢弃该消息           </pre> 2) 检查信令消息, SAC1 应丢弃该消息
测试结果:	1) SAC1 没有 H.248 终端 A 的在线状态信息。 2) H.248 终端 A 的呼叫不成功

10.2.2 媒体面安全测试

测试编号：	2.1.1
测试项目：	SIP 媒体流代理功能测试——正常情况测试
预置条件：	1) SAC 正常工作。 2) SIP 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 SIP 终端 A、软交换设备之间的信令消息以及 SAC1 和 SIP 终端 A、SAC2 之间的媒体消息
测试配置：	图 2
测试步骤：	1) 从 SIP 终端 A 发起呼叫建立请求，呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 SIP 终端 A 释放呼叫
预期结果：	<p>1) 消息流程如下所示（注：本消息流程为了简化，只给出了涉及 SAC1 的相关信令消息）。</p> <div><p>SIP 终端 A                      SAC1                      软交换设备</p><pre>sequenceDiagram     participant A as SIP 终端 A     participant SAC1     participant SW as 软交换设备     A-&gt;&gt;SAC1: INVITE     SAC1-&gt;&gt;SW: INVITE     SW--&gt;&gt;SAC1: 100 Trying     SW--&gt;&gt;SAC1: 180 Ringing     SW--&gt;&gt;SAC1: 200 OK     SAC1--&gt;&gt;A: 100 Trying     SAC1--&gt;&gt;A: 180 Ringing     SAC1--&gt;&gt;A: 200 OK     A-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;SW: ACK     Note over A,SAC1: 媒体     Note over SAC1,SW: 到 SAC2</pre></div> <p>2) 检查信令消息，SAC1 应该将 SIP 终端 A 发送的信令消息 SDP 中和 SIP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备；同时 SAC1 应该将软交换设备发送的信令消息 SDP 中和 SAC2 相关的地址信息修改为 SAC1 的地址信息再转发给 SIP 终端 A</p>
测试结果：	1) SAC1 正确执行了 SIP 信令代理功能。 2) 主被叫用户之间的媒体信息将经过 SAC1 进行转接

测试编号:	2.1.2
测试项目:	SIP 媒体流代理功能测试——异常情况测试
预置条件:	1) SAC1 正常工作。 2) SIP 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪监测 SAC1 和 SIP 终端 A、SAC2 之间的媒体消息
测试配置:	图 2
测试步骤:	1) 从 SIP 终端 A 发起呼叫建立请求,呼叫 SAC2 下的终端用户。面向 SIP 终端 A 侧 SAC1 分配的端口号为 X。 2) 呼叫建立成功之后保持一段时间然后由 SIP 终端 A 释放呼叫。 3) 呼叫释放之后,继续从 SIP 终端 A 向 SAC1 上的端口号 X 发送 RTP 消息
预期结果:	1) 消息流程如下所示 (注:本消息流程为了简化,只给出了涉及 SAC1 的相关信令消息)。 <div><div>SIP 终端 A</div><div>SAC1</div><div>软交换设备</div><pre>sequenceDiagram     participant A as SIP 终端 A     participant SAC1 as SAC1     participant SW as 软交换设备     A-&gt;&gt;SAC1: INVITE     SAC1-&gt;&gt;SW: INVITE     SW--&gt;&gt;SAC1: 100 Trying     SAC1--&gt;&gt;A: 100 Trying     SW--&gt;&gt;SAC1: 180 Ringing     SAC1--&gt;&gt;A: 180 Ringing     SW--&gt;&gt;SAC1: 200 OK     SAC1--&gt;&gt;A: 200 OK     A-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;SW: ACK     A-&gt;&gt;SAC1: RTP 流 端口号 X     SAC1--&gt;&gt;SW: 到 SAC2 来自 SAC2     SW--&gt;&gt;SAC1: RTP 流     SAC1--&gt;&gt;A: RTP 流     A-&gt;&gt;SAC1: BYE     SAC1-&gt;&gt;SW: BYE     SW--&gt;&gt;SAC1: 200 OK     SAC1--&gt;&gt;A: 200 OK     A-&gt;&gt;SAC1: RTP 流 端口号 X     SAC1--&gt;&gt;SAC1: SAC1 丢弃该 RTP</pre></div>
测试结果:	1) 呼叫成功建立之后, SAC1 上保存了和呼叫状态相关信息;呼叫释放之后, SAC1 删除了相关信息。 2) SAC1 将丢弃呼叫释放后在相应接口上收到的 RTP 数据包

测试编号:	2.1.3 (可选)
测试项目:	MGCP 媒体流代理功能测试——正常情况测试
预置条件:	1) SAC 正常工作。 2) MGCP 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 MGCP 终端 A、软交换设备之间的信令消息以及 SAC1 和 MGCP 终端 A、SAC2 之间的媒体消息
测试配置:	图 2
测试步骤:	1) 从 MGCP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 MGCP 终端 A 释放呼叫
预期结果:	<p>1) 消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。</p> <div><div>MGCP 终端 A</div><div>SAC1</div><div>软交换设备</div><pre>sequenceDiagram     participant A as MGCP 终端 A     participant SAC1 as SAC1     participant Softswitch as 软交换设备     A-&gt;&gt;SAC1: NTFY (摘机)     SAC1-&gt;&gt;Softswitch: NTFY (摘机)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: RQNT     SAC1-&gt;&gt;Softswitch: RQNT     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: NTFY (被叫号码)     SAC1-&gt;&gt;Softswitch: NTFY (被叫号码)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: CRCX (Receiveonly)     SAC1-&gt;&gt;Softswitch: CRCX (Receiveonly)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: RQNT (回铃音)     SAC1-&gt;&gt;Softswitch: RQNT (回铃音)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: RQNT (停回铃音)     SAC1-&gt;&gt;Softswitch: RQNT (停回铃音)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A-&gt;&gt;SAC1: MDCX (SendReceive)     SAC1-&gt;&gt;Softswitch: MDCX (SendReceive)     Softswitch-&gt;&gt;SAC1: ACK     SAC1-&gt;&gt;A: ACK     A--&gt;&gt;SAC1: 媒体     SAC1--&gt;&gt;Softswitch: 媒体     Softswitch--&gt;&gt;SAC2: 到 SAC2</pre></div> <p>2) 检查信令消息, SAC1 应该将 MGCP 终端 A 发送的信令消息 SDP 中和 MGCP 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息 SDP 中和 SAC2 相关的地址信息修改为 SAC1 的地址信息再转发给 MGCP 终端 A</p>
测试结果:	1) SAC1 正确执行了 MGCP 信令代理功能。 2) 主被叫用户之间的媒体信息将经过 SAC1 进行转接

测试编号:	2.1.4 (可选)
测试项目:	MGCP 媒体流代理功能测试——异常情况测试
预置条件:	1) SAC1 正常工作。 2) MGCP 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪监测 SAC1 和 MGCP 终端 A、SAC2 之间的媒体消息
测试配置:	图 2
测试步骤:	1) 从 MGCP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户, 面向 MGCP 终端 A 侧 SAC1 分配的端口号为 X。 2) 呼叫建立成功之后保持一段时间然后由 MGCP 终端 A 释放呼叫。 3) 呼叫释放之后, 继续从 MGCP 终端 A 向 SAC1 上的端口号 X 发送 RTP 消息
预期结果:	消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。 <pre>sequenceDiagram     participant A as MGCP 终端 A     participant S1 as SAC1     participant S as 软交换设备      A-&gt;&gt;S1: NTFY (摘机)     S1-&gt;&gt;S: NTFY (摘机)     S-&gt;&gt;S1: ACK     S1-&gt;&gt;A: RQNT     A-&gt;&gt;S1: ACK     S1-&gt;&gt;S: ACK     A-&gt;&gt;S1: NTFY (被叫号码)     S1-&gt;&gt;S: NTFY (被叫号码)     S-&gt;&gt;S1: ACK     S1-&gt;&gt;A: CRCX (Receiveonly)     A-&gt;&gt;S1: ACK     S1-&gt;&gt;S: ACK     A-&gt;&gt;S1: RQNT (回铃音)     S1-&gt;&gt;S: RQNT (回铃音)     S-&gt;&gt;S1: ACK     A-&gt;&gt;S1: RQNT (停回铃音)     S1-&gt;&gt;S: RQNT (停回铃音)     S-&gt;&gt;S1: ACK     A-&gt;&gt;S1: MDCX (SendReceive)     S1-&gt;&gt;S: MDCX (SendReceive)     S-&gt;&gt;S1: ACK     A-&gt;&gt;S1: RTP流 端口号 X     S1-&gt;&gt;S: 到 SAC2     S-&gt;&gt;S1: 来自 SAC2     S1-&gt;&gt;A: NTFY (挂机)     A-&gt;&gt;S1: ACK     S1-&gt;&gt;S: ACK     A-&gt;&gt;S1: DLCX     S1-&gt;&gt;S: DLCX     S-&gt;&gt;S1: ACK     A-&gt;&gt;S1: RQNT     S1-&gt;&gt;S: RQNT     S-&gt;&gt;S1: ACK     A-&gt;&gt;S1: RTP流 端口号 X     S1-&gt;&gt;S: SAC1 丢弃该 RTP</pre>
测试结果:	1) 呼叫成功建立之后, SAC1 上保存了和呼叫状态相关信息; 呼叫释放之后, SAC1 删除了相关信息。 2) SAC1 将丢弃呼叫释放后在相应接口上收到的 RTP 数据包

测试编号:	2.1.5
测试项目:	H.248 媒体流代理功能测试——正常情况测试
预置条件:	1) SAC 正常工作。 2) H.248 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪检测 SAC 和 H.248 终端 A、软交换设备之间的信令消息以及 SAC1 和 H.248 终端 A、SAC2 之间的媒体消息
测试配置:	图 2
测试步骤:	1) 从 H.248 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 2) 呼叫建立成功之后保持一段时间然后由 H.248 终端 A 释放呼叫
预期结果:	<p>1) 消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。</p> <div><div>H.248 终端 A</div><div>SAC1</div><div>软交换设备</div><pre>sequenceDiagram     participant A as H.248 终端 A     participant SAC1     participant S as 软交换设备     A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     S-&gt;&gt;SAC1: Modify     SAC1--&gt;&gt;A: Modify     A-&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Reply     A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Add+Add     SAC1-&gt;&gt;S: Add+Add     S--&gt;&gt;SAC1: Reply     A-&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Reply     A-&gt;&gt;SAC1: Modify     SAC1--&gt;&gt;A: Modify     A-&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Reply     A-&gt;&gt;SAC1: Modify     SAC1--&gt;&gt;A: Modify     A-&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Reply     A==&gt;&gt;SAC1: 媒体     SAC1==&gt;&gt;S: 到 SAC2</pre></div> <p>2) 检查信令消息, SAC1 应该将 H.248 终端 A 发送的信令消息 SDP 中和 H.248 终端 A 相关的地址信息修改为了 SAC1 的地址信息再转发给软交换设备; 同时 SAC1 应该将软交换设备发送的信令消息中和 SAC2 相关的地址信息修改为 SAC1 的地址信息再转发给 H.248 终端 A</p>
测试结果:	1) SAC1 正确执行了 H.248 信令代理功能。 2) 主被叫用户之间的媒体信息将经过 SAC1 进行转接



测试编号:	2.1.6
测试项目:	H.248 媒体流代理功能测试——异常情况测试
预置条件:	1) SAC1 正常工作。 2) H.248 终端 A 已经在软交换设备上成功进行注册。 3) 用协议分析仪监测 SAC1 和 H.248 终端 A、SAC2 之间的媒体消息
测试配置:	图 2
测试步骤:	1) 从 H.248 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户, 面向 H.248 终端 A 侧 SAC1 分配的端口号为 X。 2) 呼叫建立成功之后保持一段时间然后由 H.248 终端 A 释放呼叫。 3) 呼叫释放之后, 继续从 H.248 终端 A 向 SAC1 上的端口号 X 发送 RTP 消息
预期结果:	消息流程如下所示 (注: 本消息流程为了简化, 只给出了涉及 SAC1 的相关信令消息)。 <pre>sequenceDiagram     participant A as H.248 终端 A     participant SAC1 as SAC1     participant S as 软交换设备      A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Notify     SAC1-&gt;&gt;S: Notify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Add+Add     SAC1-&gt;&gt;S: Add+Add     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: RTP 流 端口号 X     Note over A,SAC1: (RTP stream to port X)     SAC1--&gt;&gt;S: 到 SAC2     Note over SAC1,S: (Forward to SAC2)     S--&gt;&gt;SAC1: 来自 SAC2     Note over S,SAC1: (RTP stream from SAC2)     SAC1-&gt;&gt;A: Notify     A-&gt;&gt;SAC1: Reply     SAC1-&gt;&gt;S: Subtract+ Subtract     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: Modify     SAC1-&gt;&gt;S: Modify     S--&gt;&gt;SAC1: Reply     SAC1--&gt;&gt;A: Reply     A-&gt;&gt;SAC1: RTP 流 端口号 X     Note over A,SAC1: (RTP stream to port X)     Note over SAC1: SAC1 丢弃该 RTP     Note over SAC1: (SAC1 discards the RTP)</pre>
测试结果:	1) 呼叫成功建立之后, SAC1 上保存了和呼叫状态相关信息; 呼叫释放之后, SAC1 删除了相关信息。 2) SAC1 将丢弃呼叫释放后在相应接口上收到的 RTP 数据包

## 10.2.3 可靠性相关测试

## 10.2.3.1 硬件要求

测试编号:	3.1.1
测试项目:	主、备电源的切换测试
预置条件:	1) SAC 正常工作。 2) SAC 配置主、备用电源
测试配置:	图 2
测试步骤:	将 SAC 主电源切断, 使 SAC 采用备用电源工作
预期结果:	SAC 应能自动启用备用电源, 并且不影响正常通信
测试结果:	

测试编号:	3.1.2
测试项目:	主、备系统处理板的切换测试
预置条件:	1) SAC 正常工作。 2) SAC 配置主、备系统处理板
测试配置:	图 2
测试步骤:	1) 拔掉主系统处理板。 2) 观察备用系统处理板是否进入工作状态, 通信是否中断, 并记录切换所用时间。 3) 将拔掉的系统处理板插回, 观察该板卡是否进入 (备用) 工作状态
预期结果:	1) 在主系统处理板拔下后, 能够在网管系统或设备的指示灯上看到用户处理板处于未安装状态。 2) 拔掉主系统处理板后, 备用系统处理板进入 (主用) 工作状态, 通信未中断。 3) 将拔掉的系统处理板插回后, 该板卡可进入 (备用) 工作状态
测试结果:	

## 10.2.3.2 软件要求

测试编号:	3.2.1
测试项目:	在线软件版本升级
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 在 SAC 上加载新版本的系统软件。 2) 查看版本升级后的 SAC 是否可正常工作
预期结果:	1) 更新版本后的 SAC 可正常工作。 2) 更新版本的操作不影响已有的通信
测试结果:	

测试编号:	3.2.2
测试项目:	在线软件版本回退
预置条件:	1) SAC 正常工作。 2) SAC 已经加载了新的软件版本
测试配置:	图 2
测试步骤:	1) 在 SAC 上加载新版本的系统软件。 2) 查看版本升级后的 SAC 是否可正常工作
预期结果:	1) 版本回退后的 SAC 可正常工作。 2) 版本回退操作不影响已有的通信
测试结果:	

测试编号:	3.2.3
测试项目:	数据维护功能
预置条件:	1) SAC 正常工作。 2) 系统管理人员可通过远程管理终端或本地操作维护终端登录到 SAC, 进行数据维护操作
测试配置:	图 2
测试步骤:	通过终端登录到 SAC, 对 SAC 的配置数据进行查询、修改、删除的操作, 查看是否影响 SAC 的正常工作
预期结果:	系统管理人员对 SAC 配置数据的维护操作不会影响 SAC 的正常工作
测试结果:	

#### 10.2.3.3 过负荷控制要求

测试编号:	3.3.1
测试项目:	过负荷控制功能
预置条件:	1) SAC 正常工作。 2) 在 SAC 上配置过负荷控制策略
测试配置:	图 2
测试步骤:	1) 用模拟软件向SAC发出过量的请求。 2) 查看 SAC 是否能检测出请求数达负荷阈值, 并拒绝新的请求
预期结果:	当请求达到负荷阈值时, SAC 开始拒绝新的请求
测试结果:	

10.2.3.4 重新启动时间

测试编号:	3.4.1 (可选)
测试项目:	重新启动时间
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 重新启动 SAC, 记录开始时间。 2) 待 SAC 重新启动完成后, 记录结束时间。 3) 从 SIP 终端 A 发起呼叫建立请求, 呼叫 SAC2 下的终端用户。 4) 呼叫建立成功之后保持一段时间然后由 SIP 终端 A 释放呼叫
预期结果:	1) SAC 重新启动时间应小于 20min。 2) 重新启动后 SAC 应正常工作
测试结果:	

10.2.4 安全管理相关测试

10.2.4.1 权限管理

测试编号:	4.1.1
测试项目:	权限的设置
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 系统管理员登录设备进行权限管理。 2) 输入用户名和密码, 进入系统。 3) 增加配置和维护管理员列表, 并为不同用户设置不同类型的权限。 4) 设置身份鉴别失败后锁定该账号的次数。 5) 设置登录超时锁定的时长。 6) 管理员退出
预期结果:	1) 系统能够提供登录提示 (允许用户输入用户名和密码), 输入的密码不以明文显示。 2) 授权管理员可以为不同用户设置不同的权限。 3) 授权管理员可以设置身份鉴别失败后锁定账号的次数以及登录超时锁定的时长。 4) 管理员的登录操作有日志记录
测试结果:	

测试编号:	4.1.2
测试项目:	鉴别失败处理
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	管理员输入 $N$ 次错误的用户名和密码 ( $N$ 为设置的身份鉴别失败后锁定该账号的次数)
预期结果:	$N$ 次登录不成功, 退出登录界面, 用户账号被锁定
测试结果:	

测试编号:	4.1.3
测试项目:	越权操作测试
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 管理员输入用户名和密码, 进入系统。 2) 进行权限内的操作。 3) 进行权限外的操作
预期结果:	1) 系统能够提供登录提示 (允许用户输入用户名和密码), 输入的密码不以明文显示。 2) 管理员可以进行权限内的操作, 且有日志记录。 3) 管理员无法进行权限外操作, 且越权操作有日志记录
测试结果:	

#### 10.2.4.2 日志管理

测试编号:	4.2.1
测试项目:	安全日志的记录
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 以不存在的用户身份试图登录。 2) 以管理员用户名和错误的口令试图登录。 3) 检查设备是否记录了上述非法登录的企图
预期结果:	设备记录了非法登录的时间、连接的方式 (本地, Telnet 及远程地址) 等
测试结果:	

测试编号:	4.2.2
测试项目:	操作日志的记录
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 以系统管理员的身份登录, 增加一个新的管理员账号。 2) 检查是否记录了上述操作。 3) 以维护管理员的身份登录, 增加一条配置数据。 4) 检查是否记录了上述操作
预期结果:	设备应记录操作时间、命令执行时间、操作员、操作终端、输入的命令内容、命令的结果等
测试结果:	

测试编号:	4.2.3
测试项目:	操作日志的记录
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 查看日志文件。 2) 根据操作时间、操作员、操作终端等条件查询系统的日志
预期结果:	1) 可以根据操作时间、操作员、操作终端等条件查询系统的日志。 2) 系统日志能够存储到文件中 (例如: excel)
测试结果:	

#### 10.2.4.3 管理

4.3.1—4.3.4至少选一项进行测试。

测试编号:	4.3.1 (可选)
测试项目:	支持 SNMPv2c
预置条件:	1) SAC 正常工作。 2) 配置 SAC 为 SNMPv2c 代理
测试配置:	图 2
测试步骤:	管理员使用 SNMPv2c 客户端软件验证、查询并管理设备
预期结果:	管理员能正确查询和管理被测设备
测试结果:	

测试编号:	4.3.2 (可选)
测试项目:	远程登录支持 SSH 连接
预置条件:	1) SAC 正常工作。 2) 配置 SAC 支持 SSH 远程登录
测试配置:	图 2
测试步骤:	1) 管理员以 SSH 协议发起连接并登录系统。 2) 检查数据的加密算法。 3) 关闭 SSH 远程登录
预期结果:	1) 管理员成功登录。 2) 随后的数据被正确加密。 3) 设备上可以关闭 SSH 远程登录
测试结果:	

测试编号:	4.3.3 (可选)
测试项目:	基于 Web 的管理支持 SSL/TLS 方式
预置条件:	1) SAC 正常工作。 2) 配置 SAC 支持 SSL/TLS 方式
测试配置:	图 2
测试步骤:	1) 管理员以 SSL/TLS 方式基于 Web 对设备进行管理。 2) 检查数据的加密算法。 3) 关闭基于 Web 的管理
预期结果:	1) 管理员可以成功实现基于Web的管理。 2) 管理数据以SSL/TLS方式加密传输。 3) 设备上可以关闭基于 Web 的管理
测试结果:	

测试编号:	4.3.4 (可选)
测试项目:	其他远程管理方式
预置条件:	1) SAC 正常工作。 2) SAC 配置其他的远程管理方式 (可以是厂商基于私有接口开发的远程管理软件)
测试配置:	图 2
测试步骤:	通过其他远程管理方式对 SAC 进行管理, 包括登录、数据的维护等操作
预期结果:	1) 管理员可采用其他远程管理方式对SAC进行管理。 2) 其他远程管理方式可保证管理操作所进行的数据交互的机密性和完整性
测试结果:	

#### 10.2.4.4 故障管理

测试编号:	4.4.1
测试项目:	故障告警级别
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) SAC 正常工作时, 观察是否有告警产生。 2) 构造条件使 SAC 产生告警, 分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警。 3) 观察 SAC 是否上报告警, 告警信息是否正确。 4) 观察 SAC 的告警是否分级
预期结果:	1) SAC正常工作时不产生告警。 2) 当 SAC 出现故障时, SAC 能自动、正确地上报告警内容。 3) SAC 的告警可以分级, 至少包括紧急告警和非紧急告警
测试结果:	

测试编号:	4.4.2
测试项目:	告警记录
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 构造条件使SAC产生告警, 分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警。 2) 查看 SAC 是否记录告警内容, 并以文件形式保存
预期结果:	SAC 可对故障告警的内容进行记录, 并以文件形式保存
测试结果:	

测试编号:	4.4.3
测试项目:	告警显示
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 构造条件使SAC产生告警, 分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警。 2) 对于非紧急告警, 查看 SAC 是否能在操作维护终端、网管系统或设备自身上产生可视的警示信息。 3) 对于紧急告警, 查看 SAC 是否能在操作维护终端、网管系统或设备自身上产生可视和可闻的警示信息
预期结果:	1) SAC 可在出现非紧急告警的情况下采用可视的方式显示告警信息。 2) SAC 可在出现紧急告警的情况下采用可视和可闻的方式显示告警信息
测试结果:	

#### 10.2.4.5 消息跟踪

测试编号:	4.5.1
测试项目:	消息跟踪
预置条件:	SAC 正常工作
测试配置:	图 2
测试步骤:	1) 进入SAC的操作维护界面, 启用消息跟踪界面。 2) 使用终端或信令模拟器发起正常业务。 3) 检查 SAC 是否能监测以下协议消息: MGCP、H.248、SIP。 4) 检查 SAC 是否可根据用户标识、IP 地址、端口、协议进行消息过滤
预期结果:	1) SAC 可以提供消息监测功能。 2) 消息跟踪的结果可显示在终端上或输出到文件或输出到打印机
测试结果:	



10.2.5 地址溯源和防火墙相关功能测试（可选）

10.2.5.1 地址溯源测试

测试编号：	5.1.1（可选）
测试项目：	地址绑定信息功能
预置条件：	各设备正常运行，网络正常
测试配置：	图 2
测试步骤：	1) 按测试环境连接设备。 2) 终端通过 SAC 向软交换发起注册请求。 3) 从 SAC 管理系统查询接入用户账户和端口信息
预期结果：	SAC 管理系统应能打印以接入用户的源 IP 地址、接入端口和用户标识的绑定信息
测试结果：	

测试编号：	5.1.2（可选）
测试项目：	地址绑定信息功能——带有 VLAN 信息
预置条件：	各设备正常运行，网络正常
测试配置：	图 2
测试步骤：	1) 按测试环境连接设备。 2) 终端通过 SAC 向软交换发起注册请求。 3) 从 SAC 管理系统查询接入用户账户和端口信息
预期结果：	ISAC 管理系统应能打印以接入用户的源 MAC 地址、源 IP 地址、接口、VLANID 和用户标识的绑定信息
测试结果：	

测试编号：	5.1.3（可选）
测试项目：	用户登录日志
预置条件：	各设备正常运行，网络正常
测试配置：	图 2
测试步骤：	1) 按测试环境连接设备。 2) 终端通过 SAC 向软交换发起注册请求。 3) 从 SAC 管理系统查询用户日志
预期结果：	网元管理系统应能打印以太网接入成功的用户日志
测试结果：	

10.2.5.2 防火墙安全策略功能（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.1节“防火墙安全策略功能”。

#### 10.2.5.3 包过滤功能测试（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.2节“包过滤功能测试”。

#### 10.2.5.4 状态检测包过滤功能测试（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.3节“状态检测包过滤功能测试”。

#### 10.2.5.5 信息内容过滤功能测试（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.5节“信息内容过滤功能测试”。

#### 10.2.5.6 虚拟专网（VPN）功能测试（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.7节“虚拟专网（VPN）功能测试”。

#### 10.2.5.7 抗网络攻击测试（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.10节“抗网络攻击测试”。

#### 10.2.5.8 带宽管理功能（可选）

具体测试项目见YD/T 1707-2007《防火墙设备测试方法》第7.8节“带宽管理功能”。

---

中 华 人 民 共 和 国  
通 信 行 业 标 准  
软交换业务接入控制设备安全技术要求及测试方法  
YD/T 1911-2009

\*

人民邮电出版社出版发行  
北京市崇文区夕照寺街 14 号 A 座  
邮政编码: 100061  
北京新瑞铭印刷有限公司印刷  
版权所有 不得翻印

\*

开本: 880 × 1230 1/16 2009 年 8 月第 1 版  
印张: 2.5 2009 年 8 月北京第 1 次印刷  
字数: 62 千字

ISBN 978 - 7 - 115 - 1892/09 - 134

定价: 25 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922