软交换网络组网方案分析

1997 年首次提出，很快便得到了业界的广泛重视和认同。几年中，在众多制造商和运营商的共同推动下，软交换产品逐步趋于成熟，功能日益丰富，性能逐渐稳定，标准化工作正稳步推进，软交换技术正走向市场。

迄今为止，全球范围内已有多家电信运营商积极开展了在软交换方面的实验和商用部署。在北美，地方运营公司中有 67%的运营商已经有软交换部署，有 43%的长途交换运营商也部署了软交换系统。在欧洲，运营商对软交换的发展和应用采用了比较谨慎的态度，但随着软交换技术的逐渐成熟，欧洲运营商也加快了软交换实施步伐；在亚太地区，香港、新西兰、澳大利亚、日本、韩国等国的运营商在软交换应用领域走在前列。2000 年至今，中国的电信行业对软交换网络技术也给予了极大的关注，中国电信、中国网通、中国联通、中国铁通、中国卫通和中国移动都已全面启动对软交换的应用尝试及商用部署。

各运营商软交换网络的技术测试和实际商用证明软交换体系在功能和性能上已经基本成熟，目前问题主要集中在以下方面：

随着软交换网络对 PSTN 网络的逐步取代，系统应采用何种模式进行大规模组网

如何回避 IP 网用户的高度自主性，实现电信运营商对业务的可管理性

相对于封闭、使用专用系统的电路交换网，架构于 IP 网之上的软交换网络易受到外来的入侵，面临安全性的挑战。如何才能解决网络节点、用户信息和业务的安全

如何提供具有 QoS 保证的端到端实时业务

对于处于企业私网内的用户，如何实现业务的企业 NAT 设备和防火墙的穿越

为了解决以上问题，并考虑到 IP 网自身要彻底解决安全及 QoS 问题尚需时日的现状，本文在现有软交换网络的基础上引入了新的网元设备，并提出了新的组网思路，该组网方案有助于软交换网络向商用化目标推进一步，有利于传统运营商近期内软交换网络的商业部署。

组网方案介绍

1. 网络结构

网络结构如下图所示：

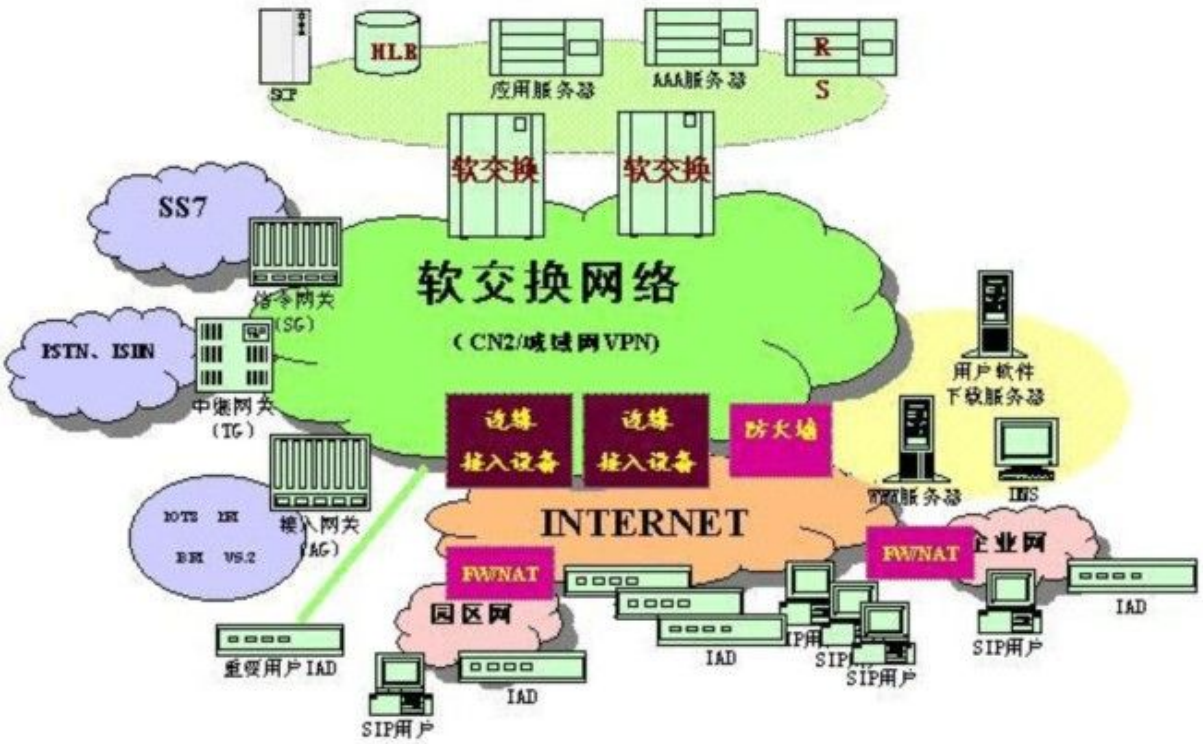

图1 软交换组网结构图

为了更好解决软交换组网问题，本方案引入了集中用户数据库 HLR 和集中路由服务器 RS，将原来存放的各软交换设备(SS)中的用户数据及路由数据分离出来，集中存放在 HLR 及 RS 之中，而 SS 只保留与网关资源相关的信息，如中继网关的 E1 资源的空闲情况等。

为了能够更好解决网络、业务的安全及 QoS 问题，本解决方案在传送层引入了具有一定安全及 QoS 保证的(软交换业务)专用承载网络及软交换业务边缘接入控制设备(BAC)。软交换设备、中继媒体网关(TG)、综合接入媒体网关(AG)、信令网关(SG)、重要客户使用的 IAD、媒体服务器(MS)、BAC 等设备基于专用网络部署，该专用网络可以是新建的专用网或采用 MPLSVPN 等技术的虚拟专用网，能通过各种手段来实现软交换设备间的相互通信及软交换设备和非软交换设备间的消息隔离。对于非重要客户使用的 IAD 及 SIP 软、硬终端等设备，由于设备数量多、分布广，将通过各种接入方式快速收敛于 BAC 设备，通过 BAC 设备实现与专用网络中其他设备的互通，此时 BAC 提供信令及媒体的代理功能及安全检测及隔离功能。

对于通过公共 Internet 接入软交换网络的 IAD 及 SIP 用户 当用户发起业务请求时，终端首先会去软交换网络的 DNS 进行 SS 的域名解析，得到根据用户所在位置或 IP 地址段所分配的 BAC 的 IP 地址，终端将呼叫请求送至该 BAC，BAC 去查询该用户是否在已通过安全注册的用户列表中，若是则对其进行用户和软交换间的信令代理(BAC 在用户来看相当于软交换，在软交换看相当于用户)。BAC 根据预设原则将呼叫请求送至相应 SS 进行处理。

对于部署在专网上的 TG 及 AG/部分 IAD 设备 当用户发起业务请求时，网关设备将根据预设的 SS IP 地址将呼叫送至相应的 SS。

主叫 SS 首先会去 HLR 查询用户的业务相关信息，判别用户该业务是否有权，是否符合预设的业务触发条件，然后根据查询结果去访问 RS 获得本次呼叫的路由信息，将呼叫接续至下一跳 SS 或业务平台。被叫 SS 收到呼叫请求将去查询 HLR，获得目前用户指定终端的 IP 地址，接至终端。

2.设备说明

关于 RS

在网络发展初期，软交换设备之间不分级，彼此之间为逻辑网状网结构，网络中任一软交换设备均存有全网的路由信息，可直接定位另一软交换设备。同一运营商网络内部软交换之间不分级，当与其他运营商网络互通将设置网间接口 SS 及网间接口中继网关。

随着网络规模的扩大，软交换设备数量的增多，将引入位置服务器设备实现软交换之间的路由查询。路由服务器接受主叫端 SS 的寻址请求，通过数据查询或向其他的路由服务器发出寻址请求，得到并向主叫端 SS 返回被叫的 SS 地址，不做呼叫控制信号的传递。

初期 RS 可以不分级，随着网络规模的扩大可以采用分级的结构。当 SS 路由数据发生变化时，应主动将变化更新到 RS，RS 之间能够实现路由数据动态自动更新。其他 RS 辖区内 SS 路由数据的变动，无须对该区域 SS 进行路由数据更改，而仅调整路由服务器中的路由数据。

RS 中将存放被叫号码所映射的路由信息，可以是下一条 SS 的 IP 地址、或是下一跳 RS 的 IP 地址、或是宽带用户帐号下所登记多个终端的地址信息、串并振顺序等。

关于 HLR

众所周知，移动网的智能程度高于 PSTN 网络，其中 HLR 的功劳是无法忽视的。对于软交换这样一个新型的网络更应当借鉴其他网络的成功之处，在网络中引入集中的用户数据库，进行用户数据的集中管理，内部可存放所管区域内宽窄带用户的业务属性(如业务权限、业务用户属性触发条件等)等。由于 HLR 的存在，使得被叫侧业务可以在主叫侧进行触发；使得用户数据可以集中存放于一地，解决了采用分离用户数据库时软交换异地相互备份时无法将用户修改的业务数据实时同步到备份软交换的问题。

HLR 采用多机备份方式提高自身可靠性。

关于 BAC 设备

软交换业务边缘接入控制(BAC)设备是为了解决网络的安全、QoS、私网穿越等问题而引入的。主要功能包括：

(1)业务穿越功能

设备支持软交换用户和软交换设备一方处于私网或双方处于不同私网时用户业务的穿越。

设备支持用户的注册流程的穿越，不改变用户的注册流程，用户的认证鉴权由软交换执行。

设备支持所有软交换提供业务的业务穿越，不改变业务流程，不引入业务安全隐患。

(2)安全保护功能

设备能对终端用户屏蔽软交换设备、中继媒体网关、综合接入媒体网关、媒体服务器等设备的地址，保护重要网元设备。

设备具备包过滤型防火墙的功能，隔离网络层攻击。

设备能阻断未经允许的协议对软交换设备的访问。

设备能进行简单的应用层攻击防护，实现部分代理服务型防火墙功能。

设备能根据业务需要、用户安全需求和运营需求屏蔽通信对方地址的能力

(3)业务质量保障(QoS)功能

设备能对进出设备消息的 ToS/CoS 的识别、标记和重标记功能，能根据标记优先级进行业务 QOS 处理。

设备可支持链路 QoS 参数探测功能，将 QoS 参数统计结果实时上报软交换或其他制定设备。

(4)业务控制管理功能

能配合软交换进行业务和呼叫控制，能协助收集、上报软交换进行呼叫处理需要的用户参数。

支持对媒体流的控制管理，可以实现对媒体的转接控制、统计、分析、监视、过滤、带宽控制等功能。

(5)用户管理功能

设备可与终端配合进行用户存活状态检测，并将检测结果上报软交换处理。

在网络组织上，BAC 设备根据用户量大小可放置在城域网汇聚层或接入层，多个 BAC 设备间相互备份，当一个设备受攻击停止服务时，可以通过 DNS 解析到网络上的其他 BAC 接替提供服务，备份不受 BAC 所处网络位置的限制。

3. 解决的问题

实现网络拥塞控制

对于新建的专用网络，可以进行带宽规划，配合以 SS 的呼叫数控制功能可实现网络呼叫拥塞控制功能。

首先预先规划好两地之间软交换业务可用的数据总带宽；根据总带宽、业务类型计算出可支持业务的同时连接总数 S；当呼叫请求来到 SS，SS 首先判断 S 当前是否为 0，若 S=0，则拒绝此次新呼叫，若 S>0 则继续处理；当 SS 完成一个业务接续则 S=S-1。

若两地之间数据带宽发生变化，则应通知 SS 进行连接总数 S 的修正。

关于 SS 可靠性

对于承担窄带域呼叫控制功能的 SS 来说，采用主备用双机工作方式。对于所控制用户的用户数据将集中存放在 HLR 中，路由数据集中存放在 RS 中，主机及备用机激活后都可访问这部分数据，至于 SS 所使用的网关资源相关数据则必须预先在备用机中保留备份。该种方式是采用资源闲置冗余的方式获得 SS 的可靠性。

对于承担宽带域呼叫控制功能的 SS 来说，可以采用前述的主备用双机工作方式，但处于更高的设备使用效率考虑，还可以采用多机负荷分担的工作方式。每个 BAC 负责 n 个 SS 设备(如同一省内采用 SS 进行宽带域业务的负荷分担处理)的控制信息分发，当其收到 SIP 用户发来的呼叫请求后，会根据预先设定的话务分配原则(如轮询等)，每个 SS 具有自己的 IP 地址，但只对 BAC 公布。这些 SS 的功能完全相同，处理 BAC 送来的呼叫请求，查询统一的 HLR 获得用户业务属性信息及用户状态、查询 RS 获得用户 IP 地址进行路由或下一跳 SS 或业务平台，以实现业务接续及控制。当某一 SS 出现故障将影响本次呼叫处理，下一次序新的呼叫请求将会由其他的 SS 进行处理，网络业务处理能力将损失 1/n，但不用空置部分 SS 资源。

BAC 实现至 SS 的呼叫控制信息动态分发功能，具有协议解析功能，能够根据应用协议的参数识别哪些消息属于同一呼叫，将其分发至同一 SS 进行呼叫处理。BAC 自身的可靠性将通过多机备份得到保证。

对于部署在专网内的信令网关、中继网关、大容量用户综合接入网关、重要客户使用的 IAD/小容量用户综合接入网关等设备，应支持在本机上设置备用 SS 地址的功能，当主用 SS 故障退出服务后应能够将后续新的呼叫请求送到备用 SS 进行处理。

对于部署在公共 Internet 之上的各类 SIP 用户及 IAD 终端，在用户侧只写入需访问的软交换设备或各类管理及应用服务器(如 IAD 网管系统、文件服务器等)的域名而非 IP 地址，通过软交换网络的域名解析器 DNS 解析后返回相应的 BAC 设备的地址。BAC 收到呼叫请求后将首先判别用户类型(采用协议类型或是否带有主机名进行判别)，对于 IAD 用户的呼叫请求，BAC 将根据预设值将呼叫指向主用 SS；对于 SIP 用户的呼叫请求，BAC 将根据预设原则(如轮询等)将呼叫均匀指向一组 SS 中的一个。

安全问题的解决

首先，软交换、中继媒体网关、综合接入媒体网关、媒体服务器等设备基于专用网络部署，该网络可以是新建的专用网或采用 MPLSVPN 等技术的虚拟专用网，能通过各种手段来实现软交换设备间的相互通信及软交换设备和非软交换设备间的消息隔离，大量的软交换散户及其他非软交换网络的设备难以直接访问到这些软交换网络设备，大大减小了受互联网用户攻击的可能。由于软交换专用网络中的设备可信任度高，通过信令协议保障(如认证)、设备管理等手段，基本可以避免专用网络内用户攻击。

对于非重要客户使用的 IAD 及 SIP 软、硬终端等设备，由于设备数量多、分布广，将通过各种接入方式快速收敛于 BAC 设备，通过 BAC 设备实现与专用网络中其他设备的互通，此时 BAC 提供信令及媒体的代理功能及安全检测及隔离功能。由于 IAD 及 SIP 终端分布于用户侧，对软交换核心设备的安全存在极大的威胁，因此在本方案中，运营商对于 IAD 或 SIP 终端应采用用户零配置方案，运营商应负责所有网络及用户数据的配置及后续的更新及修改，用户无法自行修改数据。在用户侧只写入需访问的软交换设备或各类管理及应用服务器(如 IAD 网管系统、文件服务器等)的域名而非 IP 地址，避免 SS 暴露 IP 地址易受到非法攻击。

在信令协议中启动加密和鉴权机制，SS 定期检测用户身份合法性，保证 SS 对网关及用户的控制权，防止非法用户对业务的盗用或干扰。

通过域名解析机制及 BAC 设备的信令及媒体的全代理功能，对基于公共 Internet 接入的用户屏蔽软交换、中继媒体网关、综合接入媒体网关、媒体服务器等设备的地址，保护重要的软交换网络设备。

BAC 支持访问控制列表(ACL)功能，能够根据源、目的 IP 地址和端口号设置访问控制规则进行报文过滤；能够针对特定控制协议进行包过滤，阻挡非法设备及未经允许的协议对软交换设备的访问；能进行简单的应用层攻击防护，实现部分代理服务型防火墙功能，具体包括：根据用户注册状态进行消息的处理，对未注册用户发送的非注册消息进行丢弃处理；对注册鉴权失败的用户终端建立监视列表，当失败的注册尝试达到一定的频率则采取相应措施；设置 IP 地址/端口允许的正常信令消息流量值，当 1 分钟内收到同一源 IP 和端口的消息超过该值时，将该地址/端口列入黑名单并采取相应措施。

具备根据业务需要、用户安全需求和运营需求屏蔽通信对方地址的能力。

为配合安全的软交换网络的实施，各设备需要进行相应的改进，如支持多个网段，可以通过提供多个分离的物理端口或在一个物理端口上支持多个 VLAN 的方式实现；对媒体端口进行动态开闭管理；能进行最小化端口设置；面向用户的服务可采取由 Web 或 Portal 面对用户，进行业务代理方式来降低风险；设备需要专门的软/硬件平台设计等。

QoS 问题的解决

目前的 IP 网络技术还不能彻底地解决 QoS 问题，在现有的公共 IP 网络上还不能为软交换网络提供大规模地有 QoS 保障的承载服务。本方案将采用专用网络+BAC 的信令媒体全代理功能对 QoS 问题进行一定程度的解决。

专用网络组网可以采用专线、专用 IP 网、MPLSVPN 等方式，MPLSVPN 方式要提供 QoS 保障，仍然需要全 IP 网络设备的支持，而目前的 IP 网络还不能全程全网地提供 QoS。专线和专用 IP 网方式可以通过网络流量预测和规划，按软交换业务需求组织网络，由于专网专用，使用过程中容易掌握业务流量和流向的变化，可以及时调整网络，通过与软交换设备呼叫数控制功能结合，可以有效解决网络拥塞控制问题。如新建专用网络，还可以在引进网络设备时统一考虑设备 QoS 功能，区分对待不同业务等级的软交换业务，设置为某些业务实现带宽预留。

全代理设备可以根据不同用户、不同业务分别对信令和媒体进行 QoS 标记，为后续 IP 网络设备的 QoS 处理提供帮助。在今后的 QoS 解决方案中，该设备还可以接受软交换设备或其他 QoS 控制设备的指令，在呼叫建立阶段根据用户 QoS 要求和网络 QoS 状况进行不同的后续处理(如接续、拒绝、重定向、更改编码方式等)。

防止非法业务旁路

通过在 PC 机上加载一定的 SIP 通信软件的 SIP 软终端用户，可以通过 Internet 的通达性在世界各地接入运营商的软交换系统实现通信功能，当用户在异地使用软终端呼叫用户归属地其他用户时，运营商只能收到本地呼叫的费用，而无法收到国际或国内长途呼叫收入。另外，某些终端软件也可能在获得 SS 返回的对端用户地址信息，停止与 SS 之间的继续交互，通过获得的被叫地址采用其他 IP 电话软件直接进行通信，使得运营商帮助其完成了用户寻址后话务被旁路而无法获得收益。

以上问题可以通过 BAC 在一定程度上得到改善。

对于第一个问题的做法是，终端只配软交换域名，通过 DNS 解析至应去所属的 SBC；SBC 将本身及用户的 IP 地址送给软交换；软交换进行 IP 地址分析，判

断用户的 IP 地址与使用的 BAC 的 IP 地址是否匹配，若相匹配则呼叫接续继续，若不匹配则呼叫拒绝。当然该解决办法的前提是 SS 已经了解 IP 地址与地域之间的分布对应关系。

对于第二个问题的做法是，通过 BAC 设备从信令和媒体上屏蔽通信对端用户的地址，可以有效防止业务旁路，并满足某些业务(如匿名聊天)的特殊需求，该功能建议由边缘业务接入设备完成。

结束语

本解决方案中的重要部件 BAC 已完成了企业设备规范制定，包括产品的功能、性能、相关的协议扩展等，目前已在信息产业部通信标准协会申请立项。已有设备制造商意识到该设备的重要性，完成了该设备的研制。