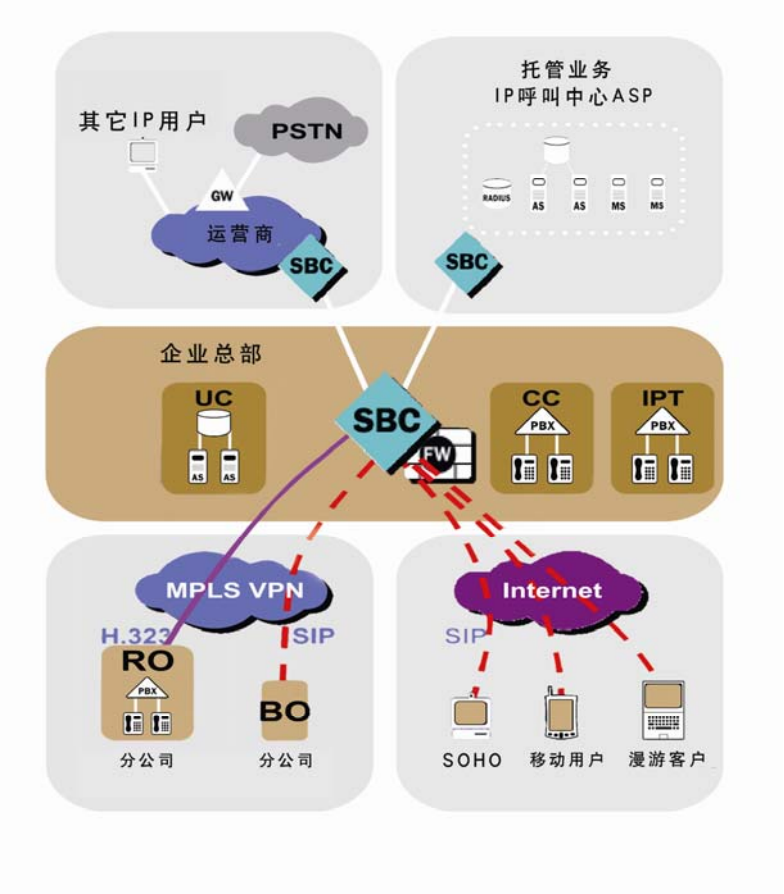
呼叫中心内的Acme Packet会话边界控制器(SBC)

Acme Packet SBC in Contact Center

*Acme Packet的*会话边界控制器为今天的呼叫中心和明天的统一通信提供值得信赖的第一流业务保障



Whitepaper(白皮书)

Introduction(简介)

呼叫中心将处在由传统TDM的电话语音向IP网络电话过渡的过程中。
由于VoIP的使用，大幅降低了日常费用，而呼叫中心虚拟化带来的一个显着优点是使得员工可以在任何只要有IP网络接入的，包括在家中或有移动网络的地方就能工作。VoIP正迈出关键性的第一步即面向真正全IP化为基础的交互式通信方式，在线出席功能的音频和视频会议，聊天/实时消息(IM) ，多媒体协作和通信功能的业务应用。许多呼叫中心把增加的这些服务作为综合性的应用软件称为统一通信(UC)。

VoIP 和统一通信（UC）被广泛地用以帮助商业机构更有效地联络其它办事处及不在呼叫中心的同事，增加了第一通话的接通率，降低解决问题的平均呼叫次数。经过IP网络的语音和其它实时通信服务将帮助呼叫中心提升客户满意度，降低整体经营和投资成本。但是当联络中心开始从传统TDM转向以IP网络语音，会议和其它实时交互式服务时，会面临来自安全性，互操作性，服务保证和遵守法规等方面的重大挑战。

运营商和其它增值业务提供商早已广泛采用会话边界控制器SBC，为正在部署的呼叫中心来解决这些不足以便提供更安全，优质， 实时交互式通信，包括VoIP和统一通信（UC） 。同样地，运营商也将会话边界控制器安装砸在其托管的呼叫中心和外包的呼叫中心的新产品解决方案中。

Business challenges (商业挑战)

呼叫中心正面临两个不同群体寄予的厚望：管理部门越来越倾向用呼叫中心来应付紧张的预算，同时还要求实现更高的性能，服务质量和创造利润，提高经营效率和建立良好客户忠诚度和品牌效应；另一方面，最终客户期望呼叫中心服务的服务水平能不断提高，让他们能够利用最便捷的联系渠道在第一次通话便能快速解决他们的问题，这种双重压力意味着以下挑战：

- 改善客户体验，以满足日益增长的对服务的期望，并带来更高的客户满意度和忠诚度
- 利用呼叫中心的代理，实时连接其它员工(相关问题的专家、其它的第二和第三级内部资源）以改善第一次通话接通率和解决问题的平均通话时间，这实际上使每一位员工成为虚拟联络中心一个潜在成员
- 利用所有代理可以找到其它同事和顾客可以找到代理的手段，如增加更多的语音服务与实时通信服务，如在线出席，实时通讯，会议，和通讯功能的应用；
- 高效地管理代理在高度分布式，虚拟联络中心环境下运行；
- 挖掘客户信息以寻找交叉销售机会，增加收入
- 提高代理的积极性，士气，忠诚度和工作满意度，以提高生产率和降低人员更换率;这意味着使代理可以从规模较小的远程办公室或在家办公
- 降低联络中心的资本和运营支出
- 在虚呼叫中心环境保持并满足政府有关法律遵从的要求

Technology trends and challenges (科技趋势和挑战)

IT设计师面临竞争日益激烈的世界，他们利用在呼叫中心中加入企业所需的工具，来适应这种技术发展的趋势和挑战。

语音服务将不可避免地从迁移TDM到IP。大多数呼叫中心已成功部署了IP - PBX的技术（纯IP或IP / TDM混合模式）。在IP – PBX的运营商接入侧，ISDN-PRI的电话中继线正在升级到SIP或H.323协议的电话中继线。在用户侧，传统话机正在被SIP或采用其它公开VoIP信令标准的IP端点取代;其中包括IP电话，以及PC和手持设备运行的VoIP客户软终端段或UC客户端。在这种演变到新技术的过程中必须加以管理，同时延长现有投资设备的生命周期，以最大限度地保护在旧的传统线路交换设备的投资及尽量减少过渡到新技术的风险。

呼叫中心的虚拟化已经成为一个重要需求。让员工可以在世界任何地方办公作的灵活性，包括在集中式的呼叫中心或分布式的工作场所、家庭办公室、外包服务供货商和移动网络办公，已经成为呼叫中心优化劳动力成本，保持代理稳定工作必须重视的两个关键。代理能够从几乎在世界任何地方工作，只需通通过广泛的互连网络连结至联络中心的基础设施。而呼叫中心管理，包含通话的路由保持，监测，记录和报告，可以像单一集中的代理方式工作一样，管理这些远端资源。而当传统的孤立信号设备接入虚呼叫中心时，就会出现不同厂商的设备互操作性问题。

呼叫中心的业务连续性的重要性与日俱增。随着呼叫中心逐渐变为客户服务和新的赢利的中心，IT设计师正在努力改进呼叫中心基础设施的可靠性。这一努力的重点是使呼叫中心在高峰负荷的状况下，或连接运营商的线路故障时，或呼机iao中心本身的核心设施的故障时如何能继续工作的能力。策略是改善呼叫中心的业务连续性，包括各虚呼叫中心资源的通话负载均衡和使用相结合的路由情报、运营商的备份连接和内部基础设施的冗余。这些容错系统可以在超负荷条件下连接运营商的线路与呼叫中心的IP通信基础设施，让系统可以更快，更顺利恢复中断。

电话录音系统的发展必须跟上变化的联络中心。作为联络中心推动从TDM到IP的语音服务和面向虚拟化架构，

电话录音解决方案必须同样变得更加开放，稳健，灵活。联络中心要充分利用新的功能以提供在线通话的IP录音解决方案，如能够集中已分散的资源或添加地理冗余功能(geo-redundancy) 。

此外，新的基于IP化的应用服务，包括统一通信已是迫在眉睫。大多数联络中心的发展策略师已经认识到来自在线出席为基础的实时通讯，视频会议和在线协作应用的潜力，以提高效率和代理进行员工外部的联系来解决问题，以达到更高的服务质量指标。在许多情况下，这一目标也提供这些新的渠道供客户使用的。

联络中心的转型是利用 VoIP 和统一通信被普遍期待的可以降低的日常费用，提高代理工作效率，更好地弹性面对沉重的呼叫量和基础设施故障。但是一般的实时交互式通信和特别是 VoIP，需要一定程度的控制，联络中心现有的数据网络和安全基础设施，其中包括路由器，防火墙，网络入侵防护系统，不能提供这样的功能。因此在最关键的新技术挑战，是要维护所有 IP 交互式通信穿越联络中心的边界的这个控制权。

呼叫中心的服务提供商应注意的榜样是运营商，包括运营商托管的和外包的联络中心服务，他们在几年前已被迫面对处理同样的问题。会话边界控制器的技术，早已被运营商、包括那些专注于联络中心的服务所广泛部署。

New control requirements (新的控制要求)

基于 IP 的交互式通信的成功交付，整个联络中心需要在五个关键领域额外的控制：

Security (安全)

联络中心的核心设备必须得到保护，使其免受那些削弱语音服务和其它 IP 的交互式通信服务的蓄意攻击和非恶意产生的不利事件影响。这些直接威胁包括针对对 IP-PBX 和自动呼叫分配器(ACDs)通信设备信令端口的 DoS/DDoS 攻击，以及非恶意产生的活动，例如停电后的造成的重新注册请求洪峰。

由于法规上的限制或是一些具有敏感性质的联络中心通话（例如医疗记录，信用卡号码等），隐私是一个重要的议题。IP 网络的开放性也有利基于某些隐私资料的攻击。因此联络中心将需要加密某些端到端的会话（信令，媒体或两者），或者至少是部分必须穿越不可信赖之 IP 网络的会话。

必须尽量减少所有的安全威胁，譬如其它重要的安全威胁，包括新的、明确以实时通信为目标病毒入侵，不请自来的讯息被用作广告或恶意软件的媒介，被称为垃圾邮件型式的网络电话，或来自利用熟悉网络拓扑结构和用户习惯的指向性攻击。其它安全威胁也包括未经授权的访问，其中包括拒绝服务/分布式拒绝服务攻击，窃取使用者身份和数据。

Application reach maximization (应用达到最大化)

语音和其它 IP 网球的交互式通信必须超越传统的集中式代理联合群组到分布式群组，在家工作的代理，移动工作的代理，代理在外包供货商工作，并最终实现处理所有的来电。但是 IP 通信的硬件和软件不总是很容易从一个供货商与其它供货商互通，或与相应的运营商的基础设施互通。例如，它是常见于对 SIP 信令协议实现轻微变化，以防止一个供货商的 IP 电话交换机成功与另一个供货商的软交换互通。

为了实现普遍的 IP 交互式通信至整个虚拟联络中心，其各种不同外部服务供货商和用户，这些不兼容必须有所调解。许多其它潜在的不兼容问题也存在，必须有所调解：
不同的信令协议（如 SIP 协议与 H.323 协议），传输协议（TCP，UDP 和 SCTP 协议），加密协议（TLS，MTLS，SRTP 和 IPsec）和编译码器（G.711，G.729A/B，G.729E，G.723.1，G.726，G.728，iLBC）。不兼容的拨号计划，重迭的 IP 地址空间和不兼容的 IP 协议版本（ IPv4 与 IPv6）也可以阻碍 IP 通信服务贯穿至整个虚拟联络中心。

许多家庭或小型办公室工作的代理，现在可通过公共互联网连接到联络中心。然而，大多数互联网接入服务使用客户端设备（ CPE ），如 DSL 调制解调器或电缆调制解调器，其中已包括防火墙，网络地址转换（ NAT ）网关的功能，这是 IP 交互式通信的两大障碍。防火墙只允许用户侧发起的入站流量请求，但防止任何人与该电信用户在防火墙外发起的实时通信。 NAT 网关使用单一的 IP 地址连向外部世界，如果有一个以上的 IP 电话或统一通信的客户端在网关之后，会产生另一个 IP 互动沟通的问题。

一些 NAT 穿越技术可以避免这两个问题，但并不是每一种技术（例如，STUN，ICE，TURN）对所有的接入设备可以工作。对于联络中心的 IT 人员，支持东拼西凑的 NAT 穿越技术也是一个挑战，不能指望不懂相关技术的远程用户可以在他们的终端设备作出必要的配置解决问题。联络中心因此必须部署 NAT 穿越解决方案，它可以扩展到支持许多使用互联网连接的远程代理，而无需繁琐的 IT 支持或远程用户的任何配置更改。

SLA assurance (服务质量的保障)

鉴于联络中心的业务重要性，它的实时通信的基础设施必须具有非常高的服务质量和可用性。防御信令单元遭受恶意DoS/DDoS攻击击是保证部分服务水平协议（ SLA ）的一个关键。另一个关键是提供非恶意超负荷情况下的保护，如联络中心在突然停电后产生的如潮水般的IP电话注册风暴，或由于商家促销宣传活动的带来的通话量猛增。由此产生的对信令的突发浪涌式的呼叫率会导致和DoS攻击同样的后果，即呼叫中心控制单元的瘫痪。

另外，提供有服务保证的业务及遵守业务分级的计划是目前许多联络中心采用的方法，这种方式已以减少实时业务时延并以牺牲部分非实时业务为代价。IP交互式通信流量必须进行分配服务质量标记和VLAN映像，通过适当的路径连接网络。基于确保适当的端到端业务优先级别、对语音质量的报告（based on R-factor or MOS scoring），应答率（ASR）采用不同的策略方案和VPN类型可能是必要的，以提供网络性能监控，容量规划和运营商的服务水平协议校验。

联络中心还必须能够在业务过载及对运营商的网络连接或关键的内部信令单元故障情况下仍然可以工作，这些信令相关的故障如自动呼叫分配器（ACDs），IP-PBX的交换机，软交换，媒体网关和SIP代理。维护基于策略外部中继的接入控制，有助于避免对信令单元的超负荷状况。运营商之间的连接和内部信令设备负载平衡，还增加了生存能力。理想的情况下，负载平衡机制 应监测服务供货商线路连接和信号单元的健康和负载容量阀值，智能化地重新分配会话，核心设施故障和超负荷条件下尽量减少调整的影响。

Cost optimization (成本优化)

联络中心面临减少资本支出和运营成本的双重压力。一个实现的方法是采用互通性和标准化的协议，允许继续使用原有设备的同时，同时部署新的 IP 通信服务。这不仅延长了旧系统的使用寿命，还实现逐步的、渐进的向新技术的过渡。这种互通能力也对于将原有的独立 IP-PBX 交换机融合到到虚拟联络中心系统至关重要，这可以在商业兼并和收购之后整合为多级的分层式呼叫中心架构。

目前大多数典型呼叫中心仍采用基于每分钟的收费，因此如何选择高效地使用运营商的服务可以获取巨大的成本节约。
因此，如何在多个服务供货商之间采用负载均衡话务量，并选择最优时间段或日期的费率，根据来电者的位置选取最佳路由，或根据中继干线挤塞等因素来重路由通话业务，成为极其宝贵的功能。随着免费电话已广泛使用在招回和呼转服务，也被称为连接呼转或代理复位向服务，运营商可以向大型联络中心，收取每年为数百万美元的话务费用。在联络中心自己的语音核心设备执行这些免费电话转移，而不是在运营商网络执行这些免费电话转移的机制，能够带来明显的成本节约。

Regulatory compliance (法规遵从)

不遵守各项政府和商业的监管任务将导致联络中心被罚款，商业费用的增加，法律责任和客户流失，这往往造成声誉和品牌形象破坏。当联络中心从传统的TDM环境迁移到IP通信服务时，必须保持所有遵从法规为目标的机制。

例如，紧急呼叫（119，110）的规定要求，各地代理的紧急呼叫，虚拟联络中心必须优先处理。在一些联络中心，为遵从法规而将不同的业务部门的分置在不同网域是非常重要的，例如，为了防止一家投资银行的企业融资部泄漏内幕信息至其所属的研究机构。在其它情况下语音通话的记录存盘也是必备的，如在股票交易订单过程中的录音是必要的。此外，实时通信的隐私必须通过使用信号和/或媒体加密受到保护。

Acme Packet SBC solutions for IP contact centers(ACME PACKET IP 呼叫中心的会话边界控制解决方案)

SBC使联络中心保持四个关键IP网络边界上的这些控制，如图1所示

- IP中继边界--与运营商IP网络连接的SIP或H.323的中继，通过运营商的媒体网关IP网络提供连接到PSTN的终端。
- 私网管理的IP网络边界-商业和消费的顾客来自本地拨打IP电话和VoIP或统一通信的PC软客户端和手持设备对等连接到IP网络服务供货商；在通话中TDM和IP网络之间的任何连接没有发生媒体转换。
- 互联网边界--在家工作的代理，移动办公员工透过公共互联网的连接及远程小型的代理群组建立VPN连接到联络中心，和
  在客户建立的不安全VoIP呼叫和其它使用公共互联网的VoIP服务的IP交互式通信联络，例如Skype或Vonage。
- 虚拟联络中心的边界--从私有IP网络服务（如MPLS ）连接到分布式联络中心群组的代理，联络中心外包服务提供商和联络中心托管服务提供商。

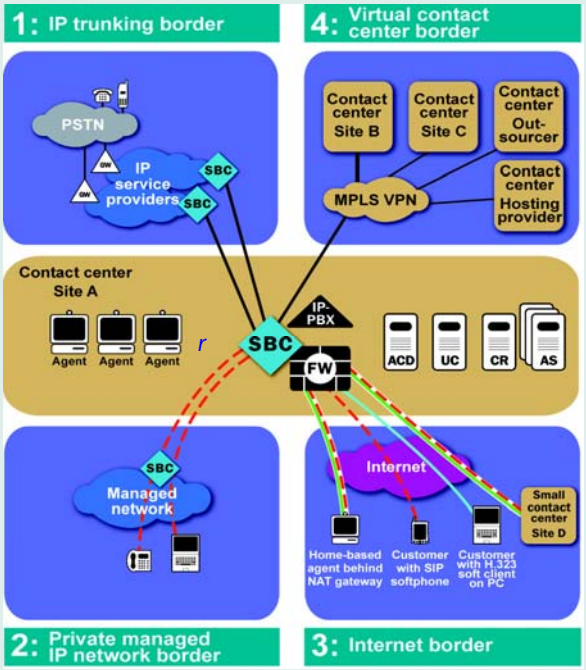


图1 ： 联络中心四个关键的IP网络边界

1: IP trunking border (IP中继边界)

第一个关键的IP网络边界是该联络中心是必须控制的IP中继边界，连接它的IP中继服务（ SIP或H.323协议的中继）到运营商的IP网络，而这反过来又通过运营商媒体网关连接到PSTN。使用IP中继来取代ISDN -PRI提供了联络中心一些成本节约和业务优势（见侧栏） 。
尽管有这些好处，目前的IP中继仍面临一些挑战。第一，运营商的IP网络，如同任何IP网络一般不能被信任。它提供了一个信令攻击的媒介和媒体超载，DoS和DDoS攻击和病
毒和蠕虫。这些安全威胁可能破坏自动呼叫分配器和IP-PBX交换机，耗尽网络的性能和通话质量和危及语音业务的保密性。
其次， IP中继服务可能会使用不符合联络中心VoIP基础设施的信令，网络协议，加密方法和编译码器。这些不兼容必须加以转换。

从好的方面来说，在IP中继边界提供了一种更符合逻辑的
位置增加会话路由的智能，提高联络中心从网络故障后恢复的能力，选择最理想的最经济的服务提供商和外部通话路由（基于如成本，时间，编译码器类型，来电者的位和网络拥挤等特征），并生成必要的业务管理和规划报告。

Benefits of IP trunking **(IP中继的优点)**

一个或多个IP中继让联络中心取代ISDN-PRI，T1/E1或更大的TDM中继：

- 让IP中继路由到每一个外拨呼叫到最近路由的服务提供商的IP骨干网媒体网关，以减少PSTN呼叫落地费用
- 省去联络中心的媒体网关和TDM中继，并支持语音应用现有的数据网络以减少资本支出和运营成本
- 配置多个IP中继到各种不同的服务供货商以新增网络容错（也称为地理冗余）能力
- 减化面向运营商的媒体网关和PSTN互连管理以简化营运成本
- 采用新的IP连接将配置和部署的时间从原来ＴＤＭ的几个月减少到几天之内。

针对管理，质量管理和/或培训的目的，大多数的联络中心必须记录部分或全部的通话。对于交付一个电话录音系统，IP中继的边界提供了一个最佳的地点用以复制实时通信会话。

有效地利用IP中继服务，联络中心必须部署SBC，以执行下列功能：

Security (安全)

联络中心的脆弱在于服务提供商的IP中继的边界，运营商的雇员可能出于恶意或金钱诱惑袭击其IP中继的边界。其它如停电等活动也会造成非恶意的信令过载。这些攻击和过载会导致联络中心和其它交互式语音IP通信服务的运行中断。会话边界控制器可以捍卫联系中心的信令单元（和其本身）对抗这些DoS/DDoS攻击和过载。

为防止从外部IP网络的攻击，SBC必须加强接入控制策略，以限制从对等连接的服务供货商会话边界控制器IP地址的呼入。联络中心的IP地址规划和拓扑结构的讯息，可用被用来窃取用户隐私和安装指向攻击至联络中心的资源。网络地址转换(NAT)必须用来隐藏拓扑IP交互式通信服务器和内部端点防御针对攻击和保护用户的隐私。

SBC应提供入侵的监测和报告，帮助联络中心验证其服务提供者遵守安全性的服务水平协议。冒用联络中心的资源，如员工擅自使用国际电话或远程出席的服务，不仅昂贵而且会使合法性产生不利影响；会话边界控制器应能检测和报告这种未经授权的使用。

Application reach maximization (应用达到最大化)

联络中心信号单元和服务提供商基础设施的IP中继之间的不兼容必须被解释。SBC可以提供信令协议的互通，如SIP协议的中继连接H.323协议的IP-PBX交换机， H.323的中继到H.323或SIP的IP-PBX交换机和不同供货商之间实现的SIP协议。其它类型的互联互通要求，由会话边界控制器完成，可能需要提供包括：TCP，UDP和SCTP传输协议的互通;加密协议互通适用TLS，MTLS，SRTP，和IPsec ;和响应代码的翻译。会话边界控制器还可能需要提供重迭的IP私有地址的空间或IPv4和IPv6地址之间翻译

SLA assurance (服务质量的保障)

由于实时通讯是联络中心的关键业务，SBC必须提供机制，以增强正常运行时间和性能。为了使联络中心实现地理冗余，SBC必须能够跨越多个IP中继负载均衡业务，在中继达到上限值或服务中断，监测健康的中继和过载、服务中断等状况下调整负载均衡。路由选择的决定也应该能够作为因素计入，在一段时间内收集的质量指标，优先考虑历史上最好的通话质量或自动应答率(ASR)的服务提供商。

当SIP中继达到会话的容限值，让更多的会话再进入在同一中继将降低所有中继上会话的质量。同样地，过高的话务接受率可以使信令设备超载。为了保证会话高质量，并防止信令单元故障，SBC必须维持呼叫接入控制，在必要时拒绝通话请求，以防止中继饱和与信令过载的状况发生。

大多数的联络中心利用某种VLAN组合的数据包标记，以确保适当的带宽和可接受实时业务的延迟而牺牲非实时数据的传输。会话边界控制器应支持服务质量标记和VLAN映像于传入话务流量遵应守这些策略机制。它也应监测和报告的服务质量和应答率，以帮助联络中心验证服务供货商服务水平协议的遵守。

Cost optimization (成本优化)

SBC必须帮助联络中心利用多种参数，通过灵活的会话路由策略，包括成本最低的路由、观察通话质量和编译码器类型，降低服务提供商对VoIP和统一通信业务的收费。例如，SBC可能路由联络中心呼出的通话到不同服务提供商的中继，这取决于这些业者提供商基于同一天的不同时段的资费或来电者的位置的最低收费。如有可能，应处理免费电话转移回联络中心网络，以减少服务供货商回拨和转接业务的相关费用。SBC可以提供成本会计和业务规划为目的灵活使用量报告。

传统的IP电话录音机制，是在第2层交换机镜像端口执行会话复制。对每一个必须被记录下来的通话，这种做法并不提供最佳的可靠性并会消耗额外的自动呼叫分配器端口。而通过SBC内部执行呼叫记录的会话复制，提供了两个明显的优势：第一，对电话录音系统要求，它提供了比第2层交换机更可靠的呼叫记录和会话复制。二，会话复制移动到中继侧，对每一个必须被记录下来的通话，自动呼叫分配器减少消耗额外的自动呼叫分配器端口;这些昂贵的自动呼叫分配器的端口，可以被回收用做如代理的席位功能。

Regulatory compliance (法规遵从)

除了用于培训和质量管理的目的，电话录音是被广泛用于联络中心是否符合法规要求，如支付卡行业（ PCI ）数

据安全标准和健康保险流通与责任法案（ HIPAA ） 。SBC须对于IP通信服务的信令和媒体，提供符合成本效益和可靠的会议记录的复制机制。

在北美，联络中心必须遵守911服务的条例，需要适当且优先处理紧急呼叫。SBC须能够确定来自虚拟联络中心内任何地方的紧急呼叫，它可以通过免除准入控制的策略和路由紧急呼叫至适当且优先的公共安全应答点PSAP。

2: Private managed IP network border (私有管理的IP网络的边界)

这条边界提出了一些额外的挑战。例如，供货商内部人士透露除了非恶意信号超载和威胁服务，联络中心在边界中对于DoS攻击和来自私营管理网络的IP端点的恶意软件来说非常脆弱。信令协议的多样和其它私人管理的IP网络和联络中心的不兼容，必须通过互通化和正常化来克服。为了保护通话质量，以及联系中心的可用性的最大化，必须采用接入控制和关键信令设备运行的健康状况监测。

联络中心必须在IP网络的边界部署SBC，以履行下列职能：

Security （安全）

联络中心在这条边界对于袭击来自本土IP的最终用户和服务供货商内部人员是脆弱的。尽管其威胁的发生比公共互联网边界少，私人管理的IP网络边界比IP中继边界（第一种边界）带有明显地更高的安全风险。例如，恶意DoS/DDoS攻击和非恶意过载信令（例如，大众呼叫事件）可以穿越这条边界，以降低联络中心的信令资源。

因此，SBC必须在此边界维持接入会话的治安，以避免非恶意超载事件和恶意攻击，它必须保卫自己免受攻击和超载，否则，一个成功针对会话边界控制器的DoS攻击的将使无防备的联络中心核心设为给随后的攻击城门大开。

SBC必须使用NAT来隐藏拓扑和信令和媒体的内容的IP地址，从而挫败针对性攻击。它还应提供用于异常检测和后攻击取证的监测和报告。关于恶意软件方面，会话边界控制器应履行的深度封包检测（DPI）对传入的会话来检测和消除病毒和蠕虫，和使用行为分析，以识别和拦截垃圾电话。

Application reach maximization (应用业务最大化)

本地管理的IP语音服务供货商可能会使用与联络中心基础设施不兼容的IP通信服务。SBC能够消除这些分歧，通过互联互通的能力，包括技术能力，调解分歧信令协议（如SIP协议与H.323协议），供货商实现信令原列（例如，不兼容的SIP之间的联络中心所使用的信号的内容和服务提供商的基础设施，如有线电视多系统运营商的有线调制解调器终端系统），传输协议（TCP，UDP和SCTP协议），加密协议（TLS，MTLS，SRTP和IPsec），和不同版本的IP（IPv4与IPv6协议） 。

SLA assurance (服务质量的保障)

SBC通过会话接纳智能控制政策，来保持联络中心的IP语音和统一通信基础设施的正常运行时间和性能，评估可用带宽和会话代理的能力。边界控制器管理呼入的会话，使其不超过允许的最大数量核可会话，或联络中心的信令设备对于会话建立的可处理最高速率。SBC还应监测相邻逻辑设备（如IP-PBX的交换机，自动呼叫分配器，软交换机和SIP注册），在他们遭受超载或失败时复位路线与重新分配的流量的健康状况。

第三个关键，IP网络的边界是该联络中心必须控制是互联网边界，界定为公共互联网的连接。这条边界提供的联

络中心的两个关键小区：一个是通过公共互联网使用VPN联系的员工，即虚拟联络中心的参与成员，包括分布式办事处的代理，以家庭为基础的代理人，和移动办公的员工；另一个是通过公共互联网致电联络中心的VoIP服务的最终用户，如Skype和Vonage。

通过公共互联网VPN连接是联络中心虚拟化的一个重要的推动因素，它使得在远程办公地点的代理群组以及以家庭为基础的代理和移动办公的员工的低成本高效地连接到联络中心。但相较于其它联络中心的IP网络边界，在互联网边界包括了广泛的安全威胁，如恶意的针对会话控制组件的DoS/DDoS攻击，非恶意的信令超载事件，病毒和蠕虫，以及创建利用实时通信和垃圾电话的规范。

由于防火墙/ NAT穿越的限制，如何扩大呼叫中心和远程代理人之间的交互式通信通也会在这条边界也存在问题。达到以家庭为基础的代理人和透过公共互联网连接的小联络中心池需具备有可扩展、可管理的NAT穿越解决方案的需求，不要求远程用户重新配置他们的互联网接入设备。

根据行业和员工的角色，从这个边界实现会话的保密可能是必要的，这取决于充分的商业理由或强制性的法规要求，尤其是考虑到公共互联网窃听的高风险情况下。然而，均匀地端到端加密是并非总是可行的，因为不是所有的IP电话，媒体网关或语音邮件服务器都拥有必要的加密功能。

最后，会话的质量在公共互联网连接可以有很大差异，而且必须定期监测，这需要选择是否从互联网连接到更高质量的专用网络连接中如具有MPLS技术的连接来提高代理的私网接入质量。

为了应对这些挑战，联络中心需要在互联网上的边界布署SBC,以达到下列功能：

Security （安全）

SBC必须保护的联络中心的信令和媒体设备和其自身免受来自于互联网连接端点的广泛的攻击，包括恶意的DoS/DDoS和非恶意的信令过载事件。它应履行传入会话的深度封包检测和消除病毒和蠕虫，并使用行为分析以识别和拦截垃圾电话产生器。

SBC 应该隐藏拓扑和信令和媒体内容的IP地址，挫败来自互联网边界的针对攻击。还应当监视互联网边界的异常流量和攻击后取证的生成报告。在适当的情况下由于高价值或敏感性质的内容，SBC支持加密的信令和媒体，以保护机密会话的远程代理和客户的来电。

Application reach maximization (应用达到最大化)

SBC必须提供托管网络地址转换穿越，建立以家庭为基础的代理人的IP的交互式通信会话，而远程的员工无需安装新的设备或重新配置现有的防火墙/网关的网络地址转换。在会话的每个端点使用不同的编译码器或帧速率，由SBC提供转码或转速。

SLA assurance (服务质量的保障)

SBC提供了各种功能，以提高性能，高冗余能力，在不暴露呼叫中心的信令设备给DoS/DDoS攻击和信令超载情况下将代理和消费者来电接入呼叫中心。会话接入控制坚持抵御DoS/DDoS攻击和避免中继饱和化引起的通话质量问题。为了提高实时远程终端之间通信的会话质量，SBC可以择释放媒体部分的会话，以便终端可以直接、点对点的沟通，而不需将媒体流通过SBC。

SBC 也必须提供优质的体验（ QoE ）的报告，以帮助规划者了解何时通过互联网连接到一个偏远的代理库需要升级到更高质量的私人广域网连接，如MPLS。

Regulatory compliance (法规遵从)

对于分布式代理群组和家庭为基础的代理，SBC必须遵守政府和行业监管条例，包括119处理，以确保放在一个偏远的代理的任何紧急呼叫能提供必要的优先地位。

在需要遵守政府或商业隐私条例，SBC必须支持加密的信令和媒体，以保护远程代理会话和客户来电的保密性。它还应提供互联加密技术，端对端加密（使用不同的加密协议的任何一方的SBC ）或部分加密（使SBC至少支持与有加密功能终端之间的会话加密）。

4: Virtual contact center border (虚拟联络中心的边界)

第四个关键，IP网络边界能超越极力维护其控制权的联络中心的在于它的虚拟联络中心的边界，包括私有IP网络连接到远程联络中心的代理。这些地点可能包括成立以营运为目的大型联络中心，区域办事处，国际分公司，并代理工作的联络中心外包服务提供商。这些地点依靠私有IP网络服务提供足够大的带宽和可靠性，如MPLS。这些服务也普遍授权连接联络中心外包或托管服务提供商。

因为安全对于企业导向的私有IP网络服务提供商的、外包、托管等商业营运是非常重要的，相较之下第2和3种的边界的安全风险是较低的。然而，连接跨越边界的虚拟联络中心的性能和可用性的是至关重要的。

为了克服这些挑战，联络中心需要在虚拟联络中心的边界部署SBC,以达到下列功能：

Security （安全）

SBC必须达到的一些功能，以防卫联络中心的IP交互式通信信号设备（以及本身）对抗源于内部服务供货商、外包供货商或托管服务提供商网络的拒绝服务和分布式拒绝服务攻击和信令超载。这里的主要威胁会是服务提供商的内部员工，基于畜意或金钱上的获益。

SBC应加强访问控制政策，经由限制传入会话的服务供货商对等会话边界控制器的IP地址。网络地址转换（ NAT ）必须采用隐藏联络中心的信号设备和内部终端的拓扑，从而挫败针对攻击和保护用户的隐私。SBC必须提供的入侵监测和报告能力，以验证服务提供者遵守有关安全和网络性能SLA.

Application reach maximization (应用达到最大化)

SBC应提供互联互通的技术能力，以调解的分歧信令和媒体的基础设施要素跨越这条边界，包括信令协议（如SIP协议与H.323协议），不同的供货商实现的信令协议，传输协议（TCP，UDP和SCTP协议），以及加密协议（TLS的，MTLS，SRTP和IPsec）。SBC也需要提供的介于重迭私有IP地址空间或IPv4和IPv6地址之间的IP地址翻译。

SLA assurance (服务质量的保障)

SBC有一个重要的角色，就是维持虚拟联络中心服务的水平。SBC必须明智地在冗余联络中心的基础设备之间做流量负

载平衡，例如， IP电话交换机集群。它应能监测健康和流量负荷的IP通信基础设施的关键要素，包括自动呼叫分配器， IP-PBX交换机，媒体网关，软交换机和SIP代理。当它检测到一个问题，硬件故障或超过阈值的能力，它应作出相应调整，切换流量到一个或多个冗余待机或负载共享系统。这同样的智能负载均衡可以帮助联络中心处理高峰期，呼吁量路由会话联络中心外包溢出呼叫处理。在适当情况下，SBC会维护会话接取控制，以防止中继和和信令设备超载。

SBC也必须与业务的优先次序和服务质量机制一同运作，以确保实时通讯传输接收带宽和低延迟，它需要以牺牲非实时数据。因此，它必须提供运输控制与传入会话的服务质量标记和VLAN映像，和像服务质量、应答率报告的监测能力，以验证服务供货商的服务水平协议。这一功能可要求会话边界控制器提供互通不同类型的VLAN 。

Summary 小结

基于传统TDM语音服务的联络中心正在向以IP网络为核心的应用的转移，这带来新增加的、基于IP网络的应用服务，如统一通信业务实现将为时不远。IT设计师看到这个迁移是联络中心必不可少的战略目标：满足客户日益增长的对服务的期望，实现更高的性能和质量指针，提高代理保留率，增长的收入和减少资本投入及运营成本。

但是现有的网络和安全是为早期部署的 TDM 语音服务而非实时数据的设计的，因此，对于 IP 互动通信业务会带来许多关键缺陷。呼叫中心设计规划师应仿效运营商（包括呼叫中心外包商和托管服务提供商）通过部署 SBC 弥补这些缺陷。SBC 使联络中心，以控制其四种关键 IP 网络的边界：它透过 IP 主干网络连接到服务提供商，以管理私有 IP 网络与公众互联网，虚拟联络中心的位置。SBC 在上述的网络边界提供的五个关键方面的强大功能如，安全，应用业务覆盖，SLA 保证，成本优化和法规遵从，可以将呼叫中心在网络演进的潮流中成功地导航到以全 IP 网为基础的未来世界。

71 Third Avenue
Burlington, MA 01803 USA

t +1.781.328.4400 f +1.781.425.5077
www.acmepacket.com

/01/08