VoIP技术发展新动态
The New Development of VoIP Technology

何宝宏

近年来，IP电话(VoIP)一直是通信界和互联网界一个共同的热点话题。VoIP在信息产业部2003年4月1日起颁布施行的《电信业务分类目录》中被定义为“泛指利用IP网络协议，通过IP网络提供或通过电话网络和IP网络共同提供的电话业务”。该规定还指出，“在此特指由电话网络和IP网络共同提供的Phone-Phone以及PC-Phone的电话业务，其业务范围包括国内长途IP电话业务和国际长途IP电话业务。IP电话业务在整个信息传递过程中，中间传输段采用IP包方式。”

根据信息产业部的统计，到2005年8月，VoIP的国内长途通话时长超过了850亿分钟，比去年同期增长了17.4%，已经接近了固定电话和移动电话国内长途通话时长的总和。但现在商用的VoIP技术并非已经成熟，仍然处于快速发展和变化之中，比如出现了分布式的VoIP实现方式，面临着如何穿越网络地址翻译/防火墙设备以及各种安全威胁和挑战等。

分布式VoIP的兴起

与所有通信系统一样，参与VoIP业务的设备也可以被划分为网络侧设备(如服务器、各种网关)和用户侧设备(如终端)两类。从VoIP终端侧设备是否参与为其他VoIP用户提供服务的角度看，可以把VoIP的拓扑结构大致划分为集中式(只由网络设备提供服务，终端只是VoIP服务的消费者)和分布式(由网络设备和终端设备协同提供VoIP服务)两类。

1. 集中式VoIP技术

(1)第一阶段：H.323协议

目前全球大多数商用VoIP网络都是基于H.323协议构建的。H.323协议是ITU-T为包交换网络的多媒体通信系统设计的(目前主要用于VoIP)，主要由网关、网守以及后台认证和计费等支撑系统组成。网关是完成协议转换和媒体编解码的主要设备，而网守则是完成网关之间的路由交换、用户认证和计费的控制层设备。

基于H.323协议的VoIP系统本身就是从电信级网络的角度出发设计的，有着传统电信网的多种优点，如易于构建大规模网络、网络的可运营可管理性较好、不同厂商设备之间的互通性较好等。然而在实际部署和实施时也遇到了一些问题，比如协议设计过于复杂、设备成本高、投资建设成本高和协议扩展性较差等问题。

(2)第二阶段：H.248/MGCP协议

在下一代网络(NGN)的研究过程中，几年前出现了所谓的“以软交换为核心的下一代网络”的说法。所谓软交换，其核心思想是控制、承载和业务分离，采用软交换做控制，不同媒体网关做媒体处理来提供话音、数据、视讯等多媒体业务(甚至支持移动性)的实现方式。其核心协议是与媒体相关的控制协议，主流的协议是ITU-T制定的H.248和IETF制定的MGCP。

软交换的主要作用是逐步把传统电话网络IP化(到目前为止仍然只能提供话音业务)，可以起到承上启下的作用，但当用户

都以IP方式连接在网络上的时候，软交换就完成了其历史使命，因此软交换属于一种VoIP的过渡技术。

(3)第三阶段：SIP/IMS

在向NGN的演进过程中，会话初始协议(SIP)越来越引起业界的关注，基于该协议开发的系统，用户终端无论在何处接入互联网，都可以通过域名找到其归属服务器来进行语音和视频等的通信。自3GPP在R5的IP多媒体子系统(IMS)中宣布以SIP为核心协议以来，ETSI和ITU-T又在其NGN体系中采用了IMS，使得SIP协议正在成为人们关注的热点。

SIP协议本身在消息发送和处理机制上具有一定的灵活性，使得用SIP协议可以很方便地实现一些VoIP的补充业务，比如各种情况下的呼叫前转、呼叫转接、呼叫保持、呈现(Presence)、即时消息等业务。

现在业界一些企业和组织，又宣扬所谓的"以IMS为核心的下一代网络"的说法，这非常值得商榷。NGN是一种融合的网络，它有没有"核心"都需要研究和实践，更何况说什么是"核心"了。

2.分布式VoIP

近两年来，以Skype为代表的分布式VoIP开始快速兴起，给传统电信带来一股强烈的冲击波。Skype主要提供VoIP及其增值业务，其推出的软件和应用包括Skype、SkypeIn、SkypeOut、即时消息、电话会议以及Skype Voicemail等。但Skype的目标绝不仅仅是为了让通话费变得更加低廉，未来还将提供视频和其他许多尚未被开发出来的通信服务。

Skype具有很多特点，比如使用端到端(P2P)技术对全部用户的计算机资源进行连接和管理(共享)，良好的移动性支持，网络地址翻译/防火墙穿越能力和优异的语音编解码质量等。这些优点在PC2PC工作方式的Skype中得到很好的体现，但在Skype Out提供的Skype到固定电话或者Skype到手机的通话中音质失真严重，影响了Skype到固定电话或手机的通话质量。

当然，Skype也存在一些其他问题。比如其他Skype用户占用个人计算机上的资源，包括网络带宽等，这将使得用户计算机在接收呼叫时发生延迟。另外，可以利用Skype发送蠕虫病毒和其他网络病毒。这些不可管理性使得Skype只能通过这种免费的方式走向市场。但是无论如何，Skype的理念会给传统的电信市场带来突破性的变革，传统电信运营商决不可忽视其挑战。

VoIP的防火墙/NAT穿越技术

对IP地址资源需求的迅速增加超出了最初预期和设计的32比特(IPv4地址长度)。很多专家学者，尤其是IP标准领域的主导性国际组织IETF一直把IPv6看作是一种长期的IP地址短缺的解决方案，把网络地址翻译(NAT)看作是一种中短期的地址短缺解决方案。NAT的大量使用，使得在协议设计中将IP地址作为通信标志符的VoIP协议无法正常工作。目前已经出现了多种典型的穿越技术，有些还在发展中。比较典型的有：

·应用网关(ALG：Application Level Gateway)：是最早出现的NAT穿越解决方案，在传统的NAT上进行协议扩展，使之具备感知SIP、H.323、H.324和MGCP等VoIP呼叫控制协议的能力，从而完成呼叫控制协议的解析和地址翻译功能。

·代理技术：是为缓解ALG方式所带来的现有NAT升级困难而出现的，它也是目前中国国内比较看好的一种NAT穿越解决方案，已经得到ITU-T的支持。

·隧道/VPN机制：逻辑上由隧道客户端和隧道服务器两部分构成，隧道客户端和隧道服务器通过隧道协议建立一条隧道，实现信令和媒体流透明穿越NAT。

·MIDCOM技术：是为了解决ALG和代理技术所共有的可扩展性不强而出现的一种NAT穿越解决方案，采用可信的第三方(MIDCOM Agent)对Middlebox(NAT)进行控制，由MIDCOM Agent控制Middlebox打开和关闭媒体端口。

·单边自我绑定地址(UNISAF：Unilateral Self-Address Fixing)：RFC3424定义的UNSAF技术，可以让位于NAT后的一个客户设法发现位于NAT公网一侧的该客户的地址，然后让应用使用新学习到的地址而不是它自己真正的IP地址。这样做需要在NAT公网一侧增加一个UNSAF服务器，并且修改客户端，以便让UNSAF服务器知道如何使用该UNSAF服务器，而真正的应用服务器 (下转第39页)

SP都应抓住这个良机进行发展。但是，对于VoIP的服务提供商而言，仅仅专注于个人语音通信或者PC-to-PC领域都是不够的。SP应该多考虑利用VoIP技术能够带来哪些创新性的应用，尤其是企业级的应用（例如在线的Call Center、人工语音服务等），以此来扩展盈利的可能。对于运营商而言，除非在位的大运营商能够和其它小运营商形成很好的共识，否则运营商这端对于VoIP的封锁就不会是坚不可破的，更何况VoIP还有利用终端的智能化和移动数据业务来破冰的可能。因此，运营商也应早作筹谋，在形势还没有完全被颠覆之前，看准合适的时机与拥有领先技术的VoIP服务提供商进行合作，或者加大投入开发出自己的VoIP核心技术，以此将未来的语音通信控制在自己而非竞争对手的手中。

刘 建 北京邮电大学经济管理学院硕士研究生

Liu Jian Master Candidate, School of Economics & Management, BUPT

（上接第36页）并不改变。典型的UNSAF技术包括STUN，TURN等。

·服务器做NAT导航（SINN：Server Involvement in NAT Navigation）：修改服务器，改变对应用的真正处理，这种改变可能会违反应用标准本身的规定。但在某些应用协议中，SINN技术允许不改变客户端或NAT就可以实现NAT的穿越。这种技术能否使用完全取决于应用层协议，通常会对客户端的行为有一个假设。典型应用就是SIP中的会话控制器（SBC）。

·协议扩展：是针对各个信令协议的特点，在信令消息中增加新的消息参数，或者对原有的呼叫流程进行改进，使之可以工作在NAT环境中。该方案的优点是无需对现有NAT设备进行改动，缺点是现有的终端和软交换设备、网守和SIP服务器等控制设备需要同时进行扩展。因此协议扩展时应重点考虑协议的向下兼容问题，以保证与未扩展的终端的完整互通性。

·IPv6：如果一种穿越技术需要修改全部的相关部分，那就是IPv6了。

VoIP安全问题日益重要

随着VoIP发展和应用范围的不断扩大，VoIP也吸引了黑客、网络钓鱼者和垃圾邮件制造者等的更多注意，导致VoIP的安全问题日益突出。典型的VoIP安全问题主要有：

·防病毒与防攻击：VoIP的网关、网守和和终端等设备的安全情况将直接影响到整个VoIP系统的安全。

·防盗打：虽然VoIP话机无法通过传统搭线方式来盗打电话，但通过窃取用户VoIP的登录密码同样能够获得IP话机的权限。

·防窃听：如今多数VoIP基于实时性的考虑，都不对语音数据进行加密，容易被窃听。

·端口扫描：对VoIP系统各个组成部分的拒绝服务（DoS）攻击，将造成这些设备上操作系统资源被消耗殆尽。任何一个潜在的内部黑客可以通过一些工具，获取VoIP各个组成部分（语音服务器、语音网关、IP话机等）的详细信息，如IP地址、服务应用的TCP/UDP端口等。

·话费欺诈：虽然VoIP话机无法通过并线的方式来打电话，但通过IP网络管理的漏洞或通过Sniffer等软件，可以窃取VoIP系统管理的密码或VoIP话机的登录密码，同样会使非法用户获得相应的语音功能和权限。

为此，VoIP工业界已经组成了VoIP安全联盟（VoIPSA：VoIP Security Alliance）。VoIPSA主要负责有关VoIP网络安全方面的研究，同时发布白皮书和业界前沿的VoIP动态，是一个旨在提高公众对VoIP安全性和保密性问题的意识的开放性组织，是目前惟一一个专注于VoIP安全性研究和教育的组织。

何宝宏 信息产业部电信研究院通信标准研究所IP与多媒体研究部主任

He Baohong Director, IP & Multimedia Department, Communications Standard Research Institute, CATR of MII