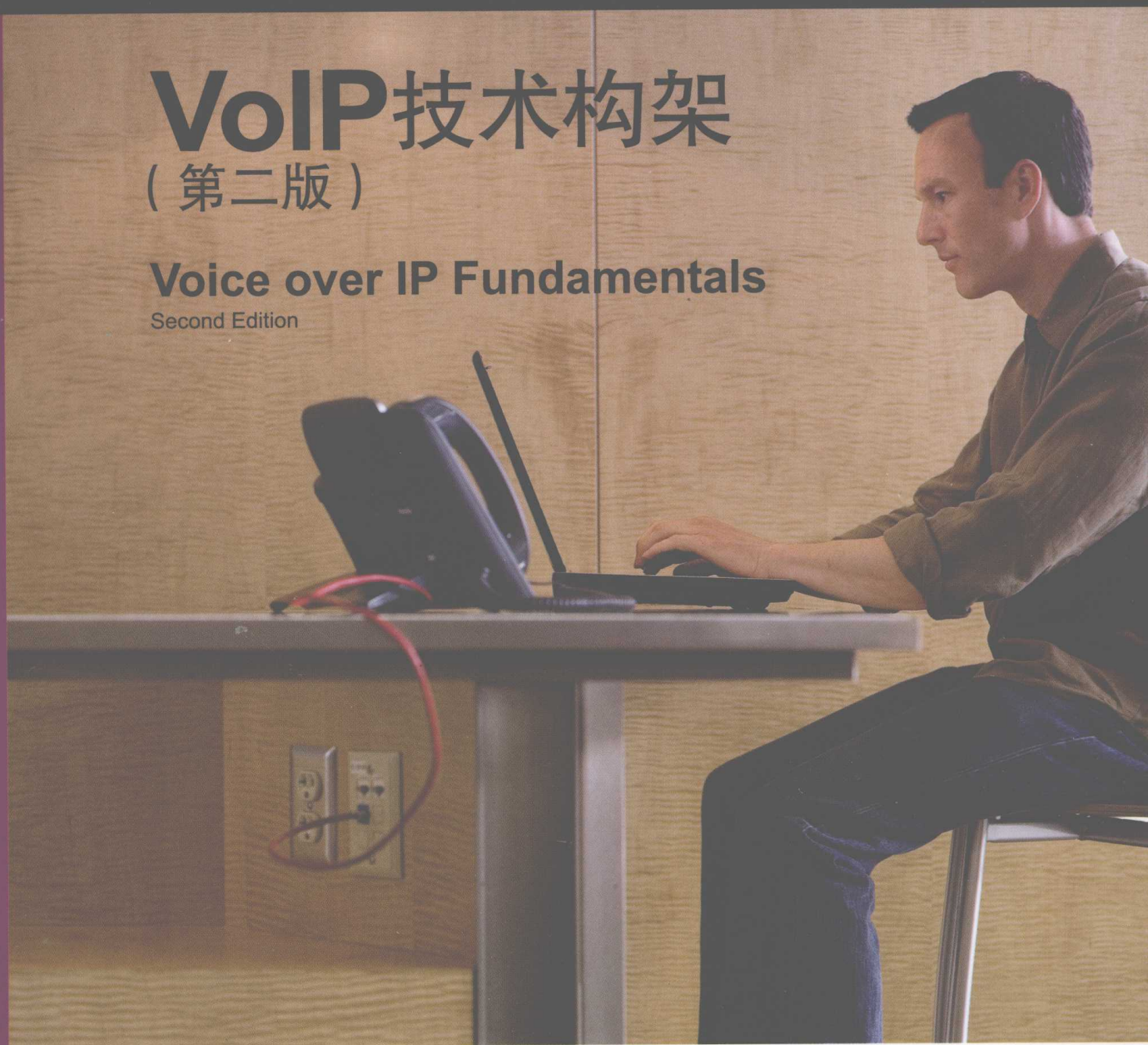
CISCO

ciscopress.com

VoIP技术构架
（第二版）

Voice over IP Fundamentals
Second Edition



〔美〕Jonathan Davidson James Peters Manoj Bhatia 著
Satish Kalidindi Sudipto Mukherjee
高艳 译

人民邮电出版社
POSTS & TELECOM PRESS

VoIP技术构架
（第二版）

- 理解企业与公共电话组网、IP组网和IP网络语音传输的相关知识；
- 了解数据和语音网络集成的各种注意事项；
- 验证基本VoIP信令协议（H.323、MGCP/H.248、SIP）和已有的主要语音信令协议（ISDN、C7/SS7）；
- 探索VoIP怎样更有效和更广泛地运行现有电话系统上的应用；
- 深入研究抖动、时延、丢包、编码、QoS工具和安全等VoIP主题。

本书全面介绍了VoIP相关知识，解释了目前一个基本IP电话架构是怎样建设和工作的，阐述了关于数据和语音组网的主要概念和数据网络上的语音传输等多方面内容。通过阅读本书，您将掌握语音怎样在已有的电话网络上传输，IP信令协议怎样用于与已有的电话系统互联，以及怎样用QoS保证语音质量。

在时分复用（time-division multiplexing，TDM）和IP合一的时代，同时理解语音与数据技术已经变得非常重要。书中阐述了语音专家理解数据组网和数据专家理解语音组网所需要的所有细节知识。

ISBN 978-7-115-17590-8

9 787115 175908 >

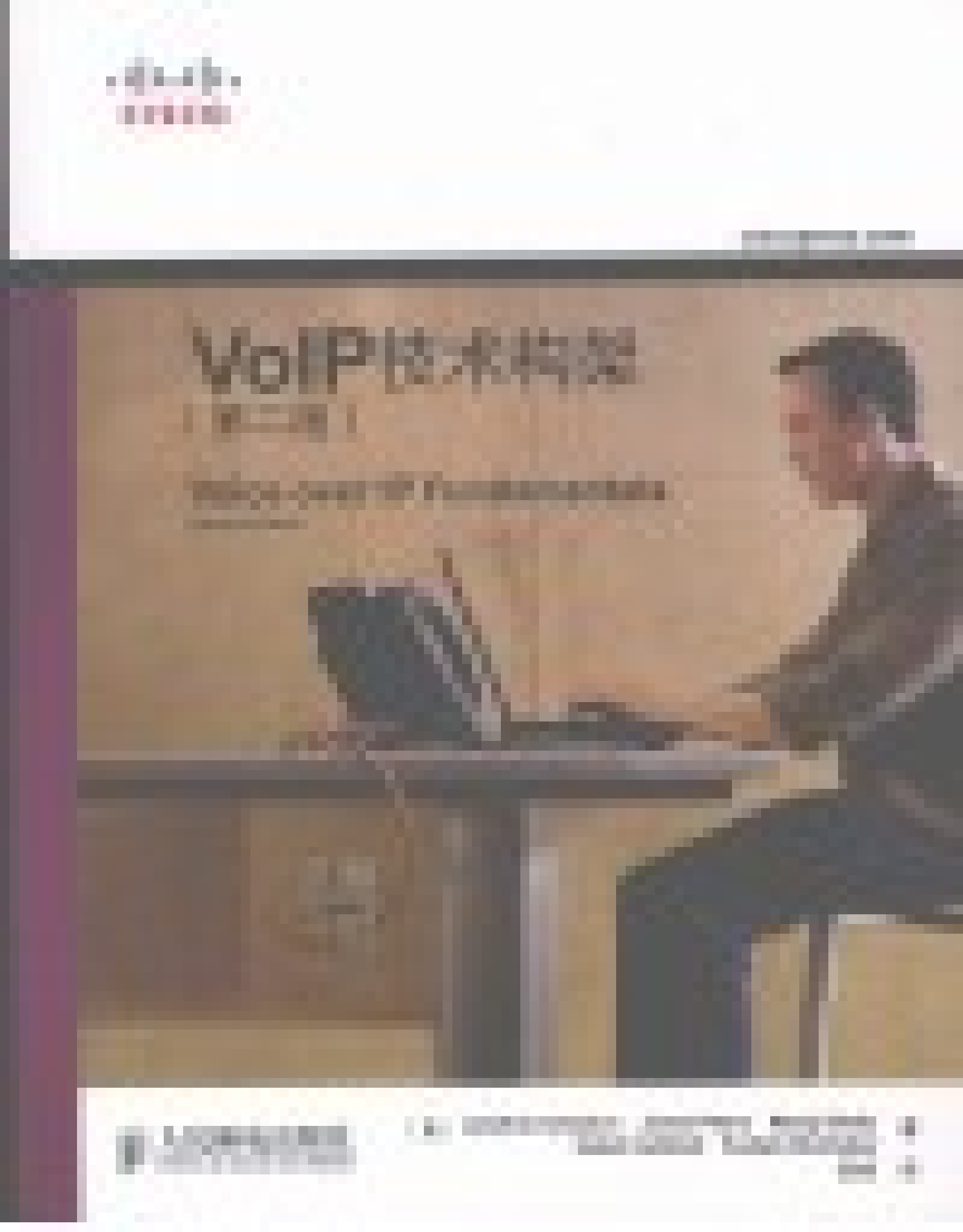
ISBN 978-7-115-17590-8/TP

定价：45.00 元

封面设计：胡平利

分类建议：计算机/网络技术/思科技术

人民邮电出版社网址：www.ptpress.com.cn



VoIP技术构架
（第二版）

Voice over IP Fundamentals
Second Edition

〔美〕 Jonathan Davidson James Peters Manoj Bhatia
Satish Kalidindi Sudipto Mukherjee 著
高艳 译

人民邮电出版社
北京

图书在版编目（CIP）数据

VoIP 技术构架/（美）戴维森（Davidson, J.）等著；高艳译. —2 版. —北京：人民邮电出版社，2008.4
ISBN 978-7-115-17590-8

Ⅰ. V… Ⅱ. ①戴…②高… Ⅲ. 互联网络—语音数据处理 Ⅳ. TN912.3

中国版本图书馆 CIP 数据核字（2008）第 016150 号

VoIP 技术构架（第二版）

◆ 著 [美] Jonathan Davidson James Peters
Manoj Bhatia Satish Kalidindi
Sudipto Mukherjee
译 高 艳
责任编辑 付 飞

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 ciscobooks@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：800×1000 1/16
印张：19.5
字数：441 千字 2008 年 4 月第 1 版
印数：1 – 4 000 册 2008 年 4 月北京第 1 次印刷
著作权合同登记号 图字：01-2007-0993 号
ISBN 978-7-115-17590-8/TP

定价：45.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书解释了今天的一个基本的电话架构的建立和工作、有关语音和数据组网的主要概念、在数据网上传输语音和与电话系统互联的IP信令协议。通过阅读本书，读者可以理解企业与公共电话组网、IP组网和语音在IP网络传输的相关知识；学习数据语音网络集成的种种注意事项；验证基本VoIP信令协议（H.323、MGCP/H.248、SIP）和已有的主要语音信令协议（ISDN、C7/SS7）；探索VoIP怎样以更有效和更广泛的方式来实现现有电话系统上的应用；深入研究抖动、时延、分组丢失、编码、QoS工具和安全等VoIP主题。

本书可供任何需要理解怎样使用 IP 网络传输数据的读者参考，对于那些语音、数据专家将极有帮助，也为网络管理员、软件工程师和其他对此项技术感兴趣的读者介绍了理解 VoIP 网络所需的相关知识。

关于作者

Jonathan Davidson, CCIE #2560，是集成网络系统工程部（Integrated Network Systems Engineering）的SP解决工程主管。与其他合著者一起编写了本书的第一版，并担任《Deploying Cisco Voice over IP》一书的编辑。他在思科工作已经10年了，先后服务于售前支持、市场和工程部等部门。

James Peters是思科公司的载体核心和多服务业务部门（Carrier Core and Multiservice Business Unit）的产品市场主管。他参与编写了本书的第一版，目前正在编写一本关于多服务组网的书。James在基于互联网的语音和数据网络的设计和建设及产品开发方面有超过20年的经验。

Manoj Bhatia是思科公司IP通信业务部（IPCBU，IP Communications Business Unit）的业务发展经理，负责合作伙伴项目。他是最早在思科VoIP网关和基于IOS路由器上用软件开发SIP技术的人员之一。 他参与了包括媒体网关、呼叫代理和基于SIP的驻留语音解决方案等许多VoIP产品技术的推广工作。 在加盟思科前，Manoj曾工作于Nortel Networks（北电网络公司）和Summa Four（现已被思科收购），在SS7、呼叫控制和VoIP等通信协议领域有超过14年的经验。

Satish Kalidindi是思科公司的软件工程师。他在开发和部署VoIP技术方面有超过6年的经验。他曾参与包括IOS网关和思科CallManager等多种产品的开发工作。最近他主要从事于CCM的安全功能的开发。他毕业于普渡大学，获工程硕士学位。

Sudipto Mukherjee是思科公司的软件工程师。他拥有许多通信产品的开发部署经验，例如有线、无线和VoIP网络上的通信设备。他最近正在参与SIP网关开发工作。Sudipto拥有GS技术学院（GS Institute of Technology, Indore）的电子电信工程学士学位和印度科学研究院（Indian Institute of Science, Bangalore）的电子设计与技术硕士学位。

关于技术审稿人

Brian Gracely, CCIE #3077，是思科Linksys小企业系统业务部门（Cisco/Linksys Small Business Systems Business Unit）的技术组长。他负责Linksys One 解决方案的整体架构，Linksys One解决方案的目标是小企业的统一组网。Brian在思科已经工作了10年，曾先后担任了设计、工程、市场和技术支持等多个职位。 他也是本书第一版的作者之一。

Jesse J. Herrera 是位于得克萨斯休斯敦的一家大型企业的高级系统分析员。他拥有亚利桑那大学（University of Arizona）的计算机科学学士学位和南方卫理公会大学（Southern Methodist University）的通信管理硕士学位。他的职责包括企业网络架构的设计与部署，其中包括容量计划、性能监控和网络集成服务。目前他主要负责无线网络和虚拟网络计划和对电子商务的支持。

Brion S. Washington 是一位网络咨询顾问，拥有超过 10 年的组网经验，近 4 年致力于 VoIP 方面的工作。

致谢

Jonathan Davidson：

衷心感谢John Kane，感谢他在我们整理本书时勤勉耐心的工作。我还要感谢 Manoj Bhatia、Satish Kalidindi和Sudipto Mukherjee ，是他们使本书得以出版。

我还要感谢我的两个孩子，Megan和Ethan，感谢你们容忍你们的父亲总是工作在笔记本电脑前。你们俩是最好的。

Manoj Bhatia:

我要感谢Cisco Press小组、我的合著者和审阅者们，以及我的经理Chris Losack，是他们鼓励我编写此书。

我还要感谢我的妻子 Anu，以及我的孩子 Dhvani 和 Rhythm，在我长时间研究和录入时与我在一起。我希望他们越来越了解 VoIP 这个很有意思的单词，因为他们是现在和不久的将来的 VoIP 的真正使用者！

Satish Kalidindi:

我要感谢John Kane和Cisco Press的编辑小组，感谢他们始终如一的努力和鼓励。感谢审阅者和合著者的勤勉工作。

也感谢我的妻子 Valli，她与我一起忍受了那么多夜晚。

Sudipto Mukherjee:

我感谢我的合著者、审阅者和我的经理Kimberly Quinn，感谢他们的支持和鼓励。特别感谢思科出版小组等待本书的耐心和理解。

我感谢我父母的鼓励和支持。

感谢我的妻子 Chandrima，我的孩子 Shreyasi 和 Joydeep，感谢他们在我为此书工作时的爱和支持。

前言

本书的第一版完成于 1999 年，在该版中我们描述了一个发生在“新世界服务提供商(new-world service providers)”与已有的“整体式提供商和集团（monolithic providers and corporations)”之间的争斗。现在，我们都已知道这个故事的结果——大多数的新世界公司和服务提供商都已经停业了，而他们的资产已经被清算或者被那些整体式服务提供商所吞并。

这些泡沫的爆裂也给 VoIP 带来了辐射效应。VoIP 也会成为另一个使用新方式运营的技术开端的牺牲品吗？您没有必要去向水晶球询问答案，市场已经决定了一切。VoIP 或者通常所说的“IP 通信（IP communication)”，作为目前和将来的主要通信机制，已经是不言而喻的事实。

最近的美国电信工业协会（Telecommunications Industry Association，TIA）的报告指出，住宅 VoIP 用户在 2005 年增加了 3 倍还多。TIA 同时预测了直到 2009 年年均复合增长率（compounded annual growth rate）将超过 40%。这将会增加超过 1800 万的 VoIP 用户。这些都证明了，分组话音（packet voice）不但增长迅速，而且已经占稳了市场。这只是一个消费者接纳此项技术的例子，而中小企业和大型企业的接受能力一向是惊人的。

已有的 TDM PBX（专用小交换机）正在迅速地被功能丰富的企业级商务通信工具所代替。与其说这是一个经济的语音传送方式，不如说是一个全新的与客户和合作伙伴沟通的方式。

本书的最初版本已销售了很多年。我最初的合著者 James Peters 和我编写这本书时，主要致力于提供基础知识以使其成为人们长期的参考书。虽然市场可能日新月异，但最基本的基础技术一旦在经过最初的飞速增长后，通常会稳定下来并在新应用的驱动下稳定发展。

本书的第一版也许会像恐龙一样消逝，但其中的许多最初理念仍然是正确的。修订这本书的一个目的就是将过去 6 年里所有技术上的变化更新进来。例如，会话发起协议（SIP，Session Initiation Protocol）在 1999 年就已经成熟，到现在仍然是许多新应用（像手机的“一键通”或称为“即按即说”（push to talk)，以及 IMS 架构）的基石。修订的另一个同样重要的目的就是讨论以这些基本技术为基础的新应用，以及它们对使用者的影响。

本书的编写目的

什么是 VoIP，它是怎样应用于你的生活中的？VoIP 就是将声音分解（称为采样）然后将它们放在 IP 分组中。语音和数据组网本身是复杂的技术，有很多书是关于这个技术的。本书解释了当今一个基本的电话架构是怎样建立和工作的，有关语音和数据组网的主要概念，在数据网上传输语音以及与现在电话系统交互工作的 IP 信令协议。同时它也回答了如

下的主要问题：

- 什么是 IP；
- 当今的电话网络中，声音是怎样被信号化的；
- 都有哪些 IP 信令协议，都是针对哪种网络的；
- 什么是 QoS（服务质量），怎样保证一个网络上的语音质量。

除了上述这些，本书也描述了网络管理员、软件工程师和只是对此项技术感兴趣的读者要理解 VoIP 网络所需的基本知识。

本书努力完成以下目标：

- 提供一个企业和公共电话网络的基本介绍；
- 介绍 IP 网络概念；
- 提供语音是怎样在 IP 网络上传输的详实介绍；
- 覆盖数据语音网络的种种说明；
- 提供各种公共交换电话网（Public Switched Telephone Network，PSTN）和 IP 信令协议的参考信息。

虽然本书包含了大量关于怎样建设一个 VoIP 网络的技术信息和建议，但它不是一本设计和实施指南，所以没有提供部署的详细信息。

谁应该阅读本书

本书是为所有试图理解怎样使用 IP 网络传输数据的读者而写的，对那些语音和数据组网的专家也很有帮助。在过去，语音与数据方面的权威们没有必要理解对方是怎样做的。然而在时分复用（Time Division Multiplexing，TDM）和 IP 合一的时代，同时理解这些技术是怎样工作的就很重要了。这本书解释了语音专家们开始理解数据组网和数据专家们开始理解语音组网所需的详细信息。

本书的编排还考虑了另一部分读者：那些拥有有限的数据和语音组网知识但具有技术悟性的读者可以在从本书了解到语音和数据组网的同时了解两者是怎样合一的。

除了讨论语音和数据组网外，本书真正是有关 VoIP 的，有关 VoIP 的协议都将做详细介绍。于是这本书就成了设计、建设 VoIP 网络，甚至为 VoIP 网络开发软件的参考指南。

熟悉 IP 网络的读者可以跳过第 6 章；同样，语音组网专家们可以跳过第 3 章。

章节组织

第 1 章比较了传统 TDM 网络与运行分组语音网络的相似与不同。

第 2 章、第 3 章、第 4 章和第 5 章覆盖了企业电话、PSTN 信令基础、7 号信令系统（Signaling System 7，SS7）以及其他 PSTN 服务。这些章节为那些拥有数据组网知识但初涉语音领域的专业人士提供了背景信息。对于那些熟悉特定语音领域并想涉及多个语音组

网协议的读者来讲，这些也是很好的初级读物。

第 6 章是一个 IP 世界的深入介绍。覆盖了基本的子网划分和开放系统互联（OSI，Open Systems Interconnection）参考模型，并且比较了传输控制协议（TCP，Transmission Control Protocol）与用户数据报协议（UDP，User Datagram Protocol）。

第 7 章和第 8 章将深入网络电话（VoIP）的细节，并详细介绍各个功能组件是怎样组合在一起形成解决方案的。这两章主要讨论了信号抖动、延时、分组丢失、编解码（codecs）、QoS 工具、平均评定得分（MOS，Mean Opinion Score）和其他实施分组语音网络所需要考虑的因素。

第 9 章回顾了无连接 IP 环境下计费的重要性。没有固定的物理位置和在任意地方都可以接入的特点，使这种新的业务模型需要我们重新考虑在 VoIP 网络上如何计费和仲裁。

第 10 章讨论了分组语音环境下常见的威胁。

第 11 章、第 12 章和第 13 章内容覆盖了各种信令协议及他们潜在的应用。这些章节使网络实施者理解建立呼叫、解除呼叫和提供服务所需要的网络组件及信令。

第 14 章和第 15 章内容覆盖了使用思科网关部署一个 VoIP 网络所需的功能组件。这两章内容包括了配置细节和案例研究。

第 16 章内容覆盖了企业使用网关部署语音网络所需的架构和功能组件，讨论了 VoIP 技术是怎样通过协同使用如 Web 会议（Web conferencing）和存在察觉服务（presence-aware services）等应用来激发企业的生产力的。

特色与约定

本书的设计和内容特色都力图使 VoIP 的复杂性变得清晰而容易接受。

当关键术语第一次被定义和使用时，使用斜体表示。并且，关键术语被拼出并在后面的括号中给出其缩写（如果有的话）。

注释框指出了那些需要特别注意的地方，以及虽然与正在讨论的问题不是特别匹配，但是很有趣，值得考虑的地方。这些注释框有时以提示形式给出的额外信息，有时以警告的方式给出来帮助您躲开一些陷阱。

每章总结使您有机会回顾和思考一下每章讨论的内容。您也可以通过这些小结来决定此章是否适合您全章阅读。

在大多数章的后面，给出了可以进一步参考的资料，包括许多 RFC 草案。虽然我们可能没有在每一章中引用所有这些参考资料，但这些资料对于我们编写这本书提供了很大的帮助。

时效性

从开始编写这本书起，我们就明确了本书的技术基线。然而，这些技术的使用，以及

使用哪种架构机制来部署和开发，都才刚刚开始。虽然许多应用已经成功地开发部署，但对于整个网络来讲，才刚刚开始迁移至一个高速发展的应用开发构架上。在第一次编写本书的时候，VoIP 的合法性在许多发展中国家并不存在，即使有也没有太大的意义，现在这已经有了很大的改变，而且在大多数地方 VoIP 是合法的，而且蒸蒸日上。本书仍然是新 VoIP 技术专家的基本指南。请记住这些技术将继续发展以支持新的应用。建议继续关注因特网工程任务组（Internet Engineering Task Force，IETF，http://www.ietf.org）和国际电信联盟（International Telecommunication Union，ITU，http://www.itu.int/）的相关信令草案。

未来之路

VoIP 已经彻底地改变了我们每个人的日常沟通方式。也许您现在就正与某个人在 IP 网上交谈。由于 VoIP 将数据网络和语音网络合二为一，您将继续发现例如即时语音（presence-based voice）这样的新应用，以及一些新的沟通合作方式。我们希望您带着和我们编写本书一样的喜悦心情来阅读本书！

目录

第1章

PSTN 概览及与 VoIP 的比较

自从亚历山大·格雷厄姆·贝尔（Alexander Graham Bell）在 1876 年第一次在线路上成功传输声音以来，公共交换电话网（PSTN，Public Switched Telephone Network）一直在不断地向前发展。所以在我们讲述 PSTN 的现状和将来之前，我们有必要先去看一看它的历史。因此，本章我们主要通过讨论 PSTN 起源来解释它目前的状况。

本章覆盖了 PSTN 的基础、构件和服务等内容，以使您更好地理解现在的 PSTN 是怎样运作的。最后，我们讨论了 PSTN 还能改进到什么程度，以及它和其他的语音网络怎样发展以达到数据、视频与语音的三者合一。

1.1 PSTN 起源

第一次语音传输是 1876 年，亚历山大·贝尔用振铃（ring-down）电路实现的。振铃电路没有号码拨打，两个设备由物理线路直接连接。基本上，当一端的人拿起电话时，另一端也就在线路上了（没有振铃声）。

随着时间的推移，这个简单的设计慢慢由一方通话（只能有一端用户讲话）发展到双方通话（两端用户都可以谈话）。在线路上传播声音需要的材料有炭精麦克风（carbon microphone）、电池、电磁铁（electromagnet）和铁膜片（iron diaphragm）。

那个时候需要通话的用户之间必须有物理线路连接。那时候，还没有拨一个号码给对方的概念。

为了更好地说明 PSTN 的起源，我们在图 1-1 中展示了一个拥有 4 部电话的电话网络。从这张图中我们可以看出，每个点之间都必须有物理线路连接。

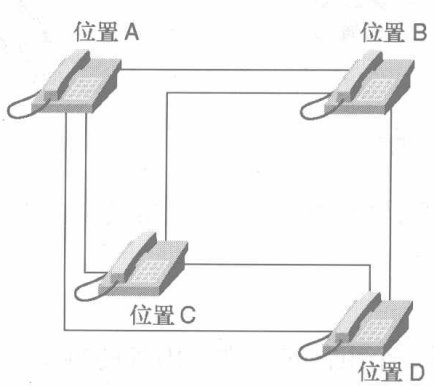


图 1-1　基本的 4 电话网络

在每一个需要电话的家庭间铺设物理线路，并不是一个可行的方法（见图 1-2）。假设您想通话的人数为 N，通过公式 $N(N-1)/2$ 就可以计算出您需要在家里铺设多少条线路。也就是说，如果你想与 10 个人通话，那你就需要在家里铺设 45 对线。

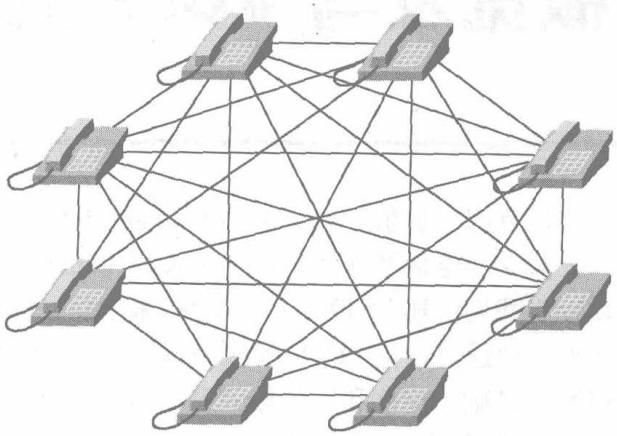


图 1-2 所有电话用户之间的物理线路连接

出于对费用的考虑，以及不可能在地球上所有的想使用电话的人之间都铺设物理线路，一种可以将一部电话映射到另一部电话的机制产生了，我们称这个装置为交换机（switch）。有了交换机，电话用户只需要一条通往中心交换机办公室的线路，而不是 7 条。

最开始的时候，是电话接线员而不是交换机负责转接电话。电话接线员询问打电话的人想打给谁，然后手工接通双方的电话。图 1-3 显示了一个有接线员转接电话的 4 电话网络。

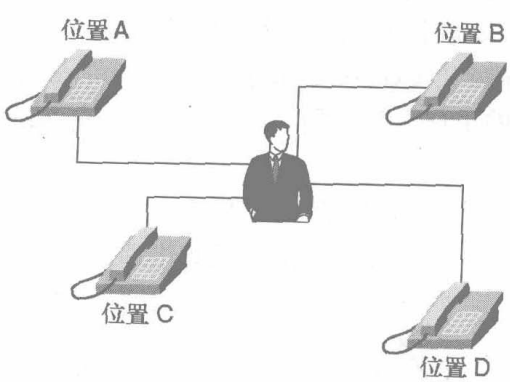


图 1-3 中心接线员：*人工交换机*

大约 100 年前，电子交换机替代了人工交换机。也就是说，现代意义的 PSTN 出现了。

1.2 PSTN 基础

解释 PSTN 网络的每一个组件是一件很困难的事情，所以我们在本节里只解释 PSTN

网络的一些重要组成。下面我们将主要讨论声音如何在数字网络上传播的、基本电路交换概念和电话号码为什么要遵从 E.164 编码格式。

> 注释：E.164 是 ITU-T 定义的国际公共通信编码规则，主要应用于 PSTN 和其他数据网络。它也定义了电话号码的格式。E.164 号码最多有 15 位数字且通常使用 + 开头。如果是国际电话，那就添加相应的国际区号。

1.2.1 模拟与数字信号

我们所听到的所有声音，包括人说话的声音，都是模拟的。就在几十年前，电话网络也是基于模拟构架的。

虽然对于人类的交流来说，模拟信号非常理想，但很难将其与线路的噪声区分开来。（语音线路旁的电器或无线发射器经常会产生线路噪声（Line noise））。电话线路对于自感应及附近的电路电线产生的电压非常敏感。在早期的电话网络中，模拟信号的传送通过放大器来传送信号。但是放大器不仅放大了声音，也放大了噪声。而这些线路噪声经常导致线路不可连接。

模拟通信是时间和振幅的混合。图 1-4 展示了一个模拟波形，这就是在示波器下人的声音的示例。

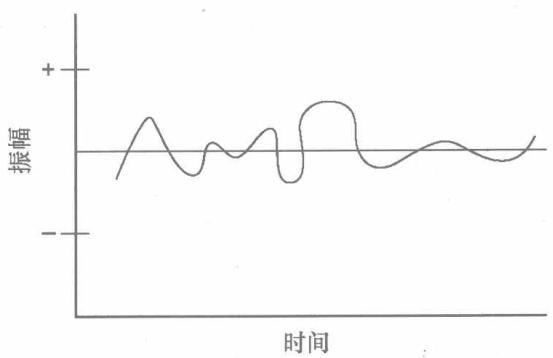


图 1-4 模拟波形

如果电话离端局交换机（end office switch）（电话的物理线路就是连在这台交换机上的）很远的话，就需要一个放大器来传送模拟信号（您的声音）。如果模拟信号混杂了线路噪声，会扭曲模拟波形而使接听断断续续。如果在您的家和端局交换机之间有许多放大器的话，那么对于听者会更为明显。图 1-5 表明了放大器只是简单地放大了进入的信号（包括语音的失真），而不是使信号清晰。这种一个语音信号通过几台放大器的过程称为累积噪声（accumulated noise）。

在数据网络中，线路噪声就不是什么问题了。因为中继器（repeaters）不仅仅是放大信号，而且会清除噪声，使信号回到初始状态。因为数据通信是基于 1 和 0 的，所以才能做到这点。因此，如图 1-6 所示，中继器（repeater，数字放大器）只需要决定是重新产生 1 还是 0。

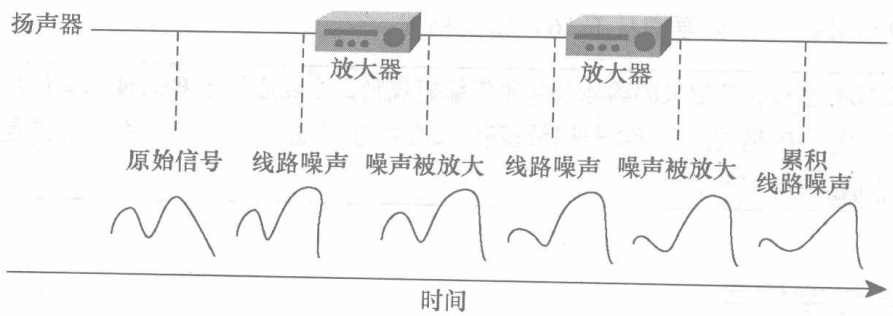


图 1-5 模拟线路失真

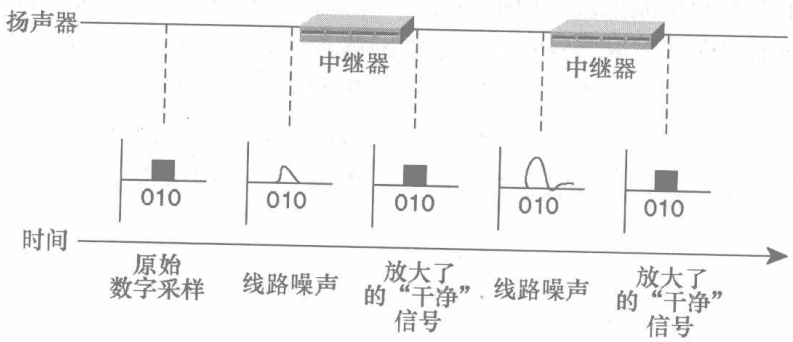


图 1-6 数据线路失真

这样，当信号被重复发送时，一个清晰的声音就产生了。当这种数字表示方法的好处被人们意识到的时候，电话网络进入了脉冲编码调制（pulse code modulation, PCM）时代。

1.2.2 数字语音信号

PCM 是一种最通用的将模拟语音信号转成以 1 和 0 表示的数字信号的方法。所有的采样技术都采用 Nyquist *定理*。按照 Nyquist 定理，如果您的取样率是最高模拟频率的两倍，就可以得到高质量的语音传输。

下面介绍 PCM 的编码过程。

1．模拟波形通过一个音频过滤器（voice frequency filter）时将所有超过 4kHz 的部分过滤出来。过滤 4kHz 的部分是为了尽量减少语音网络中的串话。根据 Nyquist 定理，您需要每秒采样 8 000 次以得到高质量的语音传输。

2．过滤后的模拟信号以每秒 8 000 次的频率采样。

3．波形被采样后转成离散数字形式。采样数据用一个代码表示。这个数字指示了被采样时的振幅。PCM 的电话学形式使用 8bit 表示代码（code）和压缩算法以给予低振幅信号更多的位数。

用 8 位乘以 8 000 次/s，就可以得到 64 000bit/s。所以电话基础设施的基础是 64 000bit/s

（或者说 64kbit/s）。

通常使用的 64kbit/s 的 PCM 有两种：μ律，北美标准和 A 律，欧洲标准。这两种方法很相似，都是采用压缩算法使 8bit 的 PCM 编码可以得到 12bit 到 13bit 的质量。

但他们也有着细小的差别。比如说，μ律在低信号/噪声比率的情况下要比 A 律好。

注释：在长途电话情况下，所有μ律到 A 律的转换都由使用μ-law 国家负责。

1.2.3 本地回路，中继线以及交换机间通信

电话基础设施开始于您家中的一对铜线。这对铜线称为本地回路（local loop）。本地回路物理上连接了家中的电话和中心局交换机（central office switch，也称为 5 类交换机（Class 5 switch）或端局交换机（end office switch））。家中电话与中心局之间的通信线路称为电话线（phone line），电话线通常运行在本地回路上。

中心局（central office）之间的通信线路称为中继线（trunk）。和在每个想通话的人家之间都铺设物理线路是不经济的一样，在每个中心局交换机之间都铺设物理线路也是不经济的。由图 1-7 您可以看出，一个网状的电话网络不如一个层次的电话网络易于扩展。

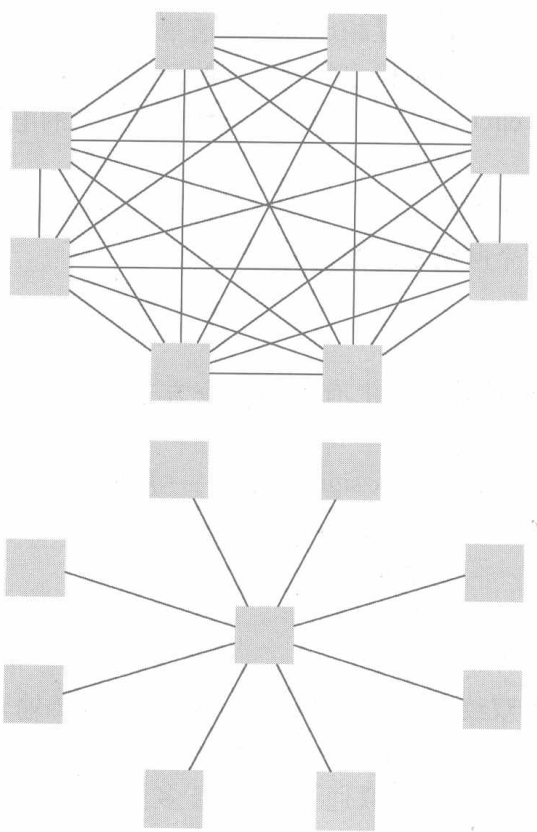


图 1-7 网状网络与层次网络

目前的交换机都是以层次结构部署的。端局交换机（或中心局交换机）通过中继线与级联交换机（tandem switche）（也称为四类交换机）相连，高层的级联交换机与区域级联交换机相连接。图 1-8 展示了一个典型的交换机层次模型。

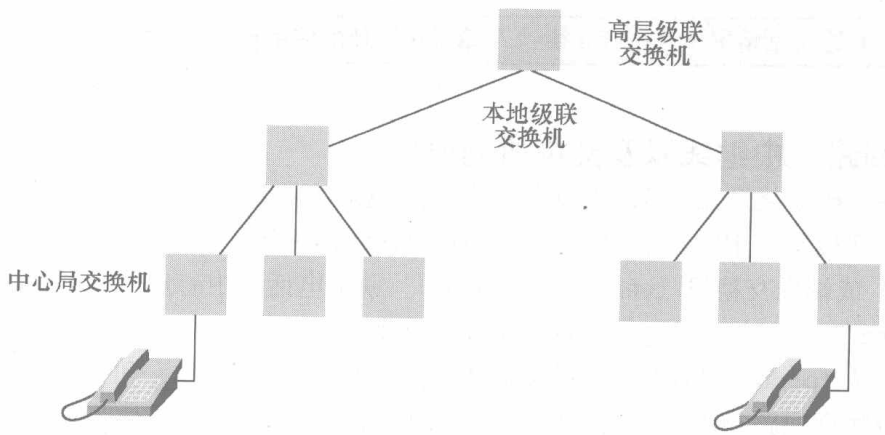


图 1-8 电路交换机层次结构

中心局的交换机经常是直接互相连接的。通常根据话务量来决定中心局交换机是否直接相连接。如果两个中心局交换机之间有足够的话务量，那么一般在这两个交换机之间铺设一条专线（dedicated circuit）来负载来自区域级联交换机的电话流量。PSTN 的某些部分使用多达 5 层的交换机。

到这里您应该了解了 PSTN 为什么和怎样被分成交换机层次结构的，您需要了解他们是怎样物理连接以及这个网络是怎样通信的。

1.2.4 PSTN 信令

一般来讲，在各种传输介质上有两种信令方式（signaling method）。这两类信令方式为：

- 用户信令（user to network signaling）——用户电话怎样与 PSTN 通信；
- 局间信令（network to network signaling）——PSTN 中的交换机之间是怎样通信的。

1. 用户信令

通常来说，当使用双绞线（twisted copper pair）作为传输介质时，用户电话通过模拟、综合业务数字网（Integrated Services Digital Network，ISDN）或 T1 线路连接至 PSTN。

电话机与交换机之间的模拟通信使用最多的信令方式是双音多频（Dual Tone Multi-Frequency，DTMF）。因为音调通过语音线路传播，所以 DTMF 属于带内信令（In-band signaling）。图 1-9 表明了 DTMF 的键盘是怎样组织的。

图 1-9 DTMF 键盘

DTMF 的拨号键盘是一个 4×4 的矩阵，每一行代表一个低频，每一列代表一个高频。

每按一个键（比如 0）就发送一个高频和低频的正弦信号组合（941 和 1336Hz）。因为发送两个音调，所以称为双音多频。这些音调随后由交换机解码来确定所对应的按键。

当用户摘下电话听筒按键时（见图 1-9），拨号音通过您的电话传送给您的电话所连接的终端局交话机，告诉它您想拨叫的号码。

ISDN 使用另一种称为带外（out-of-band）信令的方式。在这种方式下，信令通过声音以外的频道传送。用于传输声音、数据和传真的频道称为 B 信道（B channel），B 信道是 64kbit/s 的。承载信号的信道称为控制信道（control channel）或 D 信道（D channel）。

基本速率接口（Basic Rate Interface, BRI）服务是入门级的服务，提供了两个 64kbit/s 的 B 信道和一个 16kbit/s 的 D 信道，简称 2B+D。BRI 主要是为了迎合大多数个人用户和小办公室用户的需要。

基群速率接口（Primary Rate Interface, PRI）服务比 BRI 服务有了更多的扩展。PRI 提供 23 个 64kbit/s 的 B 信道和一个 64kbit/s 的 D 信道（23B+D）。PRI 主要提供给有大量语音，数据和传真需求的大企业使用。图 1-10 展示了 BRI 由两个 B 信道和一个 D 信道组成。

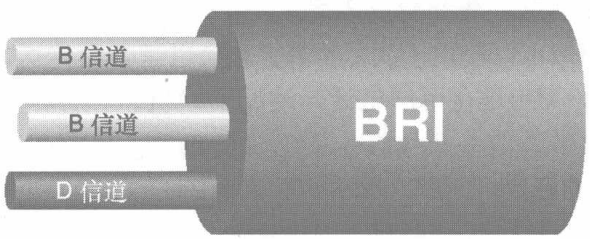


图 1-10 BRI

带外信令有如下的优点：

- 信令被整合到一个信道内；
- 减少了双占用（glare，当通话双方同时通话时出现双占用）；
- 较低的拨号后时延；
- 实现了如更高的带宽等附加功能；
- 因为建立消息不像 DTMF 音频那样受线路噪声影响，所以连接成功率更高。

带内信令受到很多问题的干扰，其中最大的就是音调丢失（lost tones）。音调丢失经常发生在信令在语音线路上承载时，这也是人们在远程访问语音信箱时会遇到问题的一个主要原因。

2. 局间信令

局间通信通常在如下的传输介质上传送。

- 双绞线上的 T1/E1 载波线路。
  T1 主要用于北美和日本，为 1.544Mbit/s 的数字传输链路；
  E1 主要用于欧洲，为 2.048Mbit/s 的数字链路。
- 同轴电缆上的 T3/E3，T4 载波线路。
  T3 承载 28 条 T1 或者 672 个 64kbit/s 连接，速率为 44.736Mbit/s；T3 承载 16 条 T1 或者 512 个 64kbit/s 连接，速率为 34.368Mbit/s；T4 承载 168 条 T1 或者 4 032 个 4kbit/s 连接，速率为 274.176Mbit/s。
- 微波线路上的 T3，T4 载波线路。
- 光介质上的同步光纤网络（Synchronous Optical Network，SONET）。

SONET 通常部署为 OC-3（155.52Mbit/s），OC-12（622.08Mbit/s），与 OC-48（2.488Gbit/s）速率。

局间信令包括如多频（Multi-Frequency，MF）与强取比特信令（Robbed Bit Signaling，RBS）在内的带内信令。这些信令类型也可以用于承载网络信令方式。

数字承载系统（T1，T3）使用 A 和 B 位来表明摘挂机状态（on/off hook）。通过设置 A/B 位来模仿单频（Single Frequency，SF）音调。（SF 通常使用信号的出现、消失来传送 A/B 位）。这些信息位可能被从信息信道中强取（robbed）出来或者整合到一个普通信道中。关于信令类型的更多信息，请参看第 3 章。

MF 与 DTMF 相似，但使用不同的频率。MF 也是带内传送，不同的是，MF 是在交换机之间传送的，而 DTMF 是在用户电话与端局交换机。

局间信令也使用带外信令 7 号信令系统（Signaling System 7，SS7）（或者欧洲的 C7）。本小节中只涉及 SS7 的好处，更多的内容在第 4 章中。

> 注释：SS7 因为是带外信令而有很多好处。它主要用于智能网（IN，Intelligent Network）。连接到智能网使 PSTN 可以提供定制本地信令业务（CLASS，Custom Local Area Signaling Service）

SS7 是一种在交换机之间传送信息的方式，它是拨叫控制和 CALSS 的基础。CLASS 服务仍然依靠端局交换机和 SS7 网络。SS7 被用来连接交换机和数据库以提供基于网络的服务（如 800 服务和本地号码可移植性（Local Number Portability，LNP））。

使用 SS7 有如下的好处。

- 减少拨号后延迟。
  没有必要在每个 PSTN 跳上传送 DTMF 音频。SS7 网络在一个初始建立消息中传送所有呼叫与被叫号码。在使用带内信令时，传送每个 MF 音频通常需要 50ms。也就是说，在每一个 PSTN 跳跃上有至少 0.5s 的延迟。我们是按照 11 位号码拨叫（11MF 音频 × 50ms = 550ms）计算出这个数字的。
- 提高了成功接通率。
  SS7 是一个基于分组交换的，带外信令协议，而 DTMF 与 MF 是带内信令。在一个分组中包含了所有的必要信息（电话号码、服务，等等）比在带内每次拨号都要产生一个音频要快多了。
- 到智能网（IN）的连接。
  这些连接提供了可以在众多厂商的交换设备上透明传输的新应用与业务，同时也能够更快地产生新的业务和应用。

为了进一步描述 PSTN，让我们来举例说明——比如说我要从我的家里给我 10 英里外的祖母家打电话。这个电话要经历一个端局交换机、7 号信令网络（只是信令）和另一个端局交换机。图 1-11 表明了这个电话是怎样从我家到祖母家。

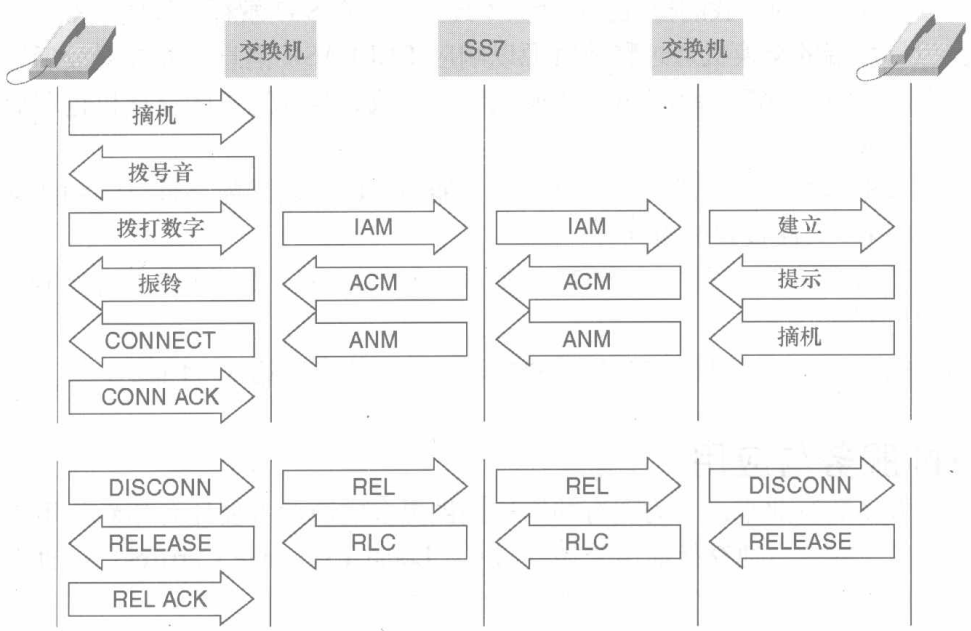


图 1-11 到祖母家的电话呼叫流程

为了更好地解释图 1-11，我们来跟踪一下这个电话。

1．我拿起电话，则电话机向端局交换机发送一个摘机指示。

2．交换机回送一个拨号音。

3．我拨打祖母家的电话号码（它们通过 DTMF 带内传送）。

4．交换机解释这些数字，然后向 SS7 网络发送一个初始地址消息（Initial Address Message，IAM，或建立消息（setup message））。

5．SS7 网络阅读到达的 IAM 后向祖母的交换机发送一个新的 IAM。

6．祖母的交换机向祖母家的电话传送一个建立消息（她的电话会振铃）。

7．祖母的交换机向 SS7 网络通过地址完全消息（ACM，Address Complete Message）回送警告消息（警告与电话振铃是一样的）。

8．SS7 网络阅读到达的 ACM 消息，然后产生一个 ACM 消息给我的交换机。

9．我听到铃声响了，知道奶奶家的电话正在振铃（铃声是不同步的，您的地域交换机通常在接到来自 SS7 网络的 ACM 消息后振铃）。

10．奶奶拿起电话，则电话会向她的交换机发送一个摘机指示。

11．奶奶的交换机向 SS7 网络发送一个应答消息（ANM，Answer Message），然后向我的交换机发送一个新的 ANM 消息。

12．连接消息被发送给我的话机（只有当我的电话是 ISDN 电话时），然后一个连接确认被回送（同样，只有当我的电话是 ISDN 电话时）。如果不是 ISDN 电话，则摘机或挂机信号被传送到端局交换机。

13．直到挂机前我都可以和我祖母谈话（挂机指示）。

14．当我挂机时，我的挂机被解释为不连接，而在 SS7 解释为释放（RELEASE，REL）消息。祖母那端的交换机通过释放资源以响应 RELEASE 消息，并在释放后发送释放完成消息（RLC，RELEAE Complete）来确认释放完成。当我这方的交换机也释放完资源，呼叫断开就完成了。

如果我祖母的电话占线，我可以使用智能网（IN）的功能来预订她的线路，当她结束谈话后，PSTN 会回拨我的电话。

到目前为止，我们描述了 PSTN 的基本功能。在下一节中我们会讨论 PSTN 中的通用服务和应用。

如果您需要有关 PSTN 信令类型的更多信息，请参照第 3、4 章。

1.3 PSTN 服务与应用

对于大多数行业来说，为现有的用户提供更多的新业务要比开拓新的用户容易得多。对 PSTN 也一样。本地交换通信公司（LEC，Local Exchange Carrires）一直在不断地增加他们可以提供的功能以从每个客户那里得到更高的收入。

每年都有很多新的服务可以提供给用户。这些服务有两种类型：定制呼叫（custom calling）功能和 CLASS 功能。

定制呼叫功能依赖于端局交换机来完成电路交换到电路交换的信息传递，而不是整个

PSTN 网络。而 CLASS 功能，则需要 SS7 来完成 PSTN 端到端的功能传递。

下面我们列出了当今 PSTN 网络上的常用定制服务功能。

- 呼叫等待（call waiting）——通知正在使用电话的用户又有一个新的电话进来。
- 呼叫转移（call forwarding）——使用户可以将呼入电话转移到另一个地方。
- 三方通话（three-way calling）——使会议呼叫成为可能。

通过部署 SS7 网络，可以使用一些更高级的功能。下面列出了一些 CLASS 功能。

- 来电显示（display）——显示主叫方的电话簿号码或称为自动号码识别（Automatic Number Identification，ANI）。
- 呼叫阻止（call blocking）——阻止一些特定的呼入号码。这样呼叫方将得到呼叫不被接受的提示。
- 号码隐藏（calling line ID blocking）——使自己的电话号码不会在对方显示。（当呼叫 800 电话或一些其他特定电话时，此功能不可用。）
- 自动回叫（automatic callback）——当呼叫的电话占线时，您可以预订该电话，则该电话空闲时会回拨您的电话。有时也称作回铃（camp on）。
- 呼叫回拨（*69）——可以使用户快速响应漏听电话。

这里面的大部分功能依赖于 SS7 和智能网（IN）。许多长途电信运营商（IXC，inter-exchange carriers）也提供如下商务功能。

- 电路交换长途电话（circuit-switched long distance）——基本的长话服务（通常会给一个很好的折扣）。
- 电话卡业务（calling cards）——预付费或后付费的电话卡。在使用时需要先拨一个电话号码，然后输入密码，再拨打要呼叫的电话。
- 800/888/877 号码——呼叫方不为呼叫付费，而是由被叫方付费（通常需要额外的费用）。
- 虚拟专用网（VPN，Virtual Private Networks）——由电话公司管理一个私有的拨号计划。这样可以大大减少内部的信息服务（Information Service，IS）人员。
- 专线（private leased lines）——专线速率从 56kbit/s 到 OC-48s，可以承载数据和语音业务。在北美最流行的速率是 T1。
- 虚拟电路（virtual circuits）（帧中继（frame relay）或异步传输模式（Asynchronous Transfer Mode，ATM）——电信运营商（IXC 或 LEC）负责帧的交换。不是占用一条专线而是一帧一帧地（或在 ATM 中一个单元一个单元的）传送。

这里列出的 IXC 商务业务只是 PSTN 中常用功能的一部分。虽然 PSTN 一直在发展，而且用户在使用越来越多的功能，但基本的客户体验从最初电话通信的数字组网开始还是一致的。

1. PSTN 编号计划

其中一个变化很缓慢的功能就是拨号计划（dial plan）。因为需要另外的线路来接入因

特网、手机和传真，电话号码相对短缺。在下一节里我们将讨论 PSTN 拨号计划是怎样使用的，以及我们在以后的几年中能期待什么。

在美国的一些地区，拨打本地电话也需要拨 1+10 位数字。当更多的设备需要一个电话号码时，这将越来越普遍。本地电话也需要拨打 1+10 位数字主要是因为区号的重叠覆盖（overlay）。重叠产生时，相邻的两家可能拥有不同的区号。当一个已有一个区号地区又拥有了另一个区号时，在产生区号重叠。对于已有的用户不需要更换区号，但要求该区域的每个人都需要拨打 10 位数字。

有些区域不要求拨打 1 但需要拨打 10 位数字。比如在休斯敦，如果电话的开头拨打 1，则会得到无需拨打 1 的自动提示。但其他 10 位数字还是需要的。

基本上说，在 PSTN 中主要使用两种编号计划：北美编号计划（North American Numbering Plan，NANP）与国际电信联盟电信标准组（ITU-T）的国际编号计划（International Numbering Plan）。在下面的章节里我们主要讨论这两种编号计划。

2. 北美编号计划（NANP）

NANP 是一个由 3 部分组成的 11 位拨叫计划：编号计划区（NPA，Numbering Plan Area），通常也称为区号（area code）；中心局号码（NXX，Central Office Code）和分机号码（station number）。这个计划也通常被引用为 NPA-NXX-XXXX。

NPA 编号使用以下格式：

NXX，其中 N 为 2～9，X 为 0～9 的数字；

NANP 也被引用为 1+10。这就意味着如果拨叫的第一个数字为 1，其后会跟着 10 位 NPA-NXX-XXXX 号码。这使端局交换机可以判断是 7 位的还是 10 位的电话号码。

在端局交换机上，有一个静态表。根据这个静态表 LEC 可以跟踪用户使用的长话提供商。每一个长途电话运营商都对应一个编码。这个长途编码由北美编号计划协会（North American Numbering Plan Association，NANPA）分配的，如果添加到您呼叫的电话号码里，您的呼叫就会被路由到相应的长途电话运营商（或 IXC）。

> 注释：现在很流行的是，人们可以通过运营商选择号码来选择另一家长途电话运营商。在北美，通过在拨叫电话前拨打一个 7 位的号码，就可以选择一个长途电话运营商。许多广告都在告诉电话用户通过拨打特定的 10+XX+XXX 来不使用他们的主运营商。
>
> 人们要选择运营商的道理很简单。您不需要更换运营商，就可以根据您每天、每周的电话量，以及经常拨打的地区、拨叫的类型或其他因素来选择长话运营商。

3. ITU-T 国际编号计划

ITU-T 建议书 E.164 定义：国家号（CC，Country Code）、国内区号（NDC，National Destination Code）和用户号（SN，Subscriber Number）用来路由一个呼叫到特定的订户。

其中 CC 包含 1 位、2 位或 3 位数字。第一位数字（1～9）定义了世界编号区域（world

numbering zones)。所有已定义的 CC 可以在 ITU-T 建议书 E.164 附录 A 中找到。

NDC 与 SN 的长度可以根据所在国家变化，但都不能超过 15 位。

许多其他有关国际编号计划的建议和规定可以参照 ITU-T 的 E.系列建议书。

虽然拨号计划目前看来不那么重要，但他们对分组语音网络（VoIP，Voice over IP）和传统的电路交换网络（circuit switched networks）的成功部署是非常重要的。

不论您所在的国家使用哪种拨号计划，都将发现拨号方式和拨叫的对象都会改变。

1.4 语音与数据网合二为一的驱动力

了解 PSTN 的基础包括了解现有的 PSTN 网络为什么已经不能满足它的建设者和使用者的需求。当您了解了现在的 PSTN 缺少什么的时候，也就知道了到哪里去找解决方案。本节讲述为什么语音网络和数据网络要合二为一。

PSTN 的缺陷

虽然 PSTN 对于建设它的最初目的（也就是交换语音）来说已经足够好了，但商业驱动力（business drivers）正在努力将其转变到一个新的网络上去。在新的网络上，语音只是数据网络上的一个应用。为什么会这样呢？有如下的原因。

- 对于大多数为语音而建设的网络来说，数据已经是其上的主要流量。

数据目前很有效地运行在为语音而建的网络之上。但数据有着不同的特色，比如需要变化的带宽和更高的带宽。

不久的将来，语音网络将运行在以数据为中心的网络之上。流量将根据应用而不是物理电路而分。新的技术（如快速以太网（fast ethernet），吉比特以太网（Gigabit Ethernet）和光纤网络（optical networking））被用来部署高速网络以承载所有这些附加数据。

- PSTN 不能足够快地建立部署新的功能。

对于竞争越来越激烈的电信市场，LEC 在不停地寻找挽留客户的方法。而挽留客户的主要手段就是提供给他们足够诱人的各种新业务和应用。

而 PSTN 是建造在由设备厂商提供应用的基础架构上的。这就意味着用户一次购买了所有需要的。但一个公司满足所有客户的需求是非常困难的。一个许多厂商都可以提供应用的开放架构，可以开发出许多有创意的解决方案和应用。在目前的架构上，许多厂商为 PSTN 开发新应用是不可能的。可以想象一下，如果厂商，比如说微软，不允许其他厂商为它的软件编写新的应用，世界现在会是什么样子的。

- 数据/语音/视频（Data/Voice/Video，D/V/V）在目前建设的 PSTN 网络上无法三者合一。

  对于大多数只有模拟线路的家庭来说，您无法使用一个 56kbit/s 的调制解调器同时完成数据接入（因特网接入）、电话接入和视频接入。高速宽带接入，例如数字用户线路（digital subscriber line，DSL），宽带（cable）和无线网络，可以促成三者合一。当带宽问题解决后，我们就可以在家中使用这 3 种应用了。在 PSTN 的

主干网上，三者合一已经开始实施了。

- 为语音而建的架构不能足够灵活地承载数据。
  因为承载信道（bearer channel）（B 信道和 T1 线路）、呼叫控制（call-control、SS7 和 Q.931）和服务逻辑（应用）被紧紧地捆绑在一个封闭的平台上，哪怕做一点点小小的改动以提高语音质量都是不可能的。

更值得指出的是，电路交换需要一条 64kbit/s 的专线来连接两部电话。不管呼叫双方是否在通话，这条 64kbit/s 的连接都不能被其他人使用。这就意味着电话公司不能将这部分带宽用于他用，所以也必须向其占用者收费。

而数据组网则可以按需使用带宽。这个区别虽然看起来并不大，却是分组交换电话网络的主要优点。

1.5 分组电话网络的驱动力

在上一节里我们讨论了 PSTN 内竞争的政策驱动力。这一节里我们将主要讲述为什么运营商会选择开发分组交换电话网络来替代传统的电路交换网络。

D/V/V 的集成并不仅仅改变架构。D/V/V 的集成不仅使许多新的功能可以快速地开发，而且使成千上万的独立软件开发商（ISV，Independent Software Vendors）都可以进行开发。D/V/V 的集成就像由大型机开发向客户/服务器方式转变一样。只有有限的开发商可以为大型机开发应用，而在分布式系统上，大量的开发商都可以开发应用。

图 1-12 列出了电路交换模型是怎样被划分成为新模型的。在新模型中，它被划分成了有开放式标准的 3 层。一个分组交换架构将承载真实的语音（媒体），呼叫控制层从媒体层分离出来，开放的应用程序接口（API，Application Programming Interfaces）使新的服务可以由独立软件开发商（ISV）开发。

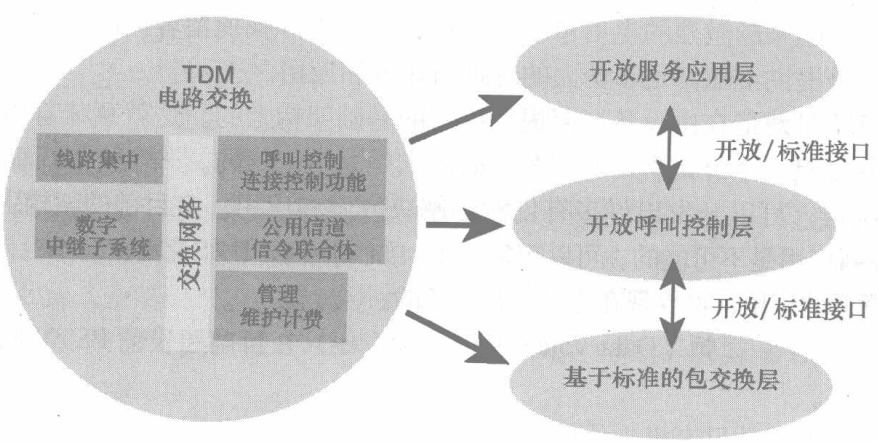


图 1-12

图 1-12 简单对比了两者的区别。为了进一步讨论这些变化，我们需要更深地了解 3 层结构的每一层。

1.5.1 基于标准的分组架构层

在新的模型中，分组交换架构代替了电路交换架构。这个架构最可能采用 IP，虽然下层使用 ATM 上层使用 IP 也是可行的。IP 对分组架构如此有吸引力主要是因为它无处不在的特性和它已经是应用接口的既成事实。这就意味着人们无需了解 IP 上运行的软件应用。IP 只是将数据从一端传到另一端，而对传输什么没有兴趣。

实时传输协议（Real-time Transport Protocol，RTP）被用来在用户数据报协议（User Datagram Protocol，UDP）/IP 分组头上提供*时间戳（timestamping）*。在 UDP 和 IP 上运行的 RTP 通常被记作 RTP/UDP/ IP。RTP 目前是在 IP 网络上承载实时流量的基石（比如微软的网络会议就是使用 RTP 承载音频和视频通信）。到目前为止，所有的 VoIP 信令协议都是采用 RTP/UDP/IP 作为他们的语音流量的传输机制。RTP 数据包流通常被称作 *RTP 流（RTP streams）*。这个术语被用来描述音频路径。

在 IP 网络中，分组丢失是很常见的事情。实际上，TCP/IP 协议就是通过分组丢失来控制数据传输的。在 TCP/IP 中，如果分组丢失的话，就重新传送。而在大多数实时的应用中，因为信息的时间性问题，重传还不如丢弃。

> 注释：当为拥挤（congested ）IP 网络提供优先级时，IP 网络必须知道传输的是什么应用。

ITU-T 建议在一个方向的延时不要超过 150ms。在思科的 VoIP 网络中，单向延迟大约是 120ms（目前，在两个使用 G.729 的思科网关上 120ms 的延时为 65ms 到 85ms）。如果接收方要求一个包必须重传，那么延时会太大而造成通话的间隙。

> 注释：RTP 流也通常被称为*媒体流（media stream）*。这样，您就可以使用 IP 与 UDP 和 RTP 一起代替 64kbit/s 的传统语音电路。

RTP 有一个域表明包被传送的实际时间（与整个 RTP 流有关）。这个信息被称为 *RTP 时间戳（RTP timestamps）*，设备使用这个信息来决定中止/接收音频流。接收设备通过 RTP 时间戳来决定一个包应当到达的时间，包是否是有序到达和在应当到达时包是否到达。所有这些信息帮助接收设备调整自己的设置以对应潜在的网络问题，如时延、抖动和分组丢失。

> 注释：*抖动（Jitter）*是指包到达间隔时间的不同，或者实际接收到包的时间与预期要接收到包的时间之间的差异。

IP 的一个主要优点是合理建设的 IP 网络是可以*自愈的（self-healing）*。这就意味着当使用动态路由协议和有多个可能的目的地存在时，数据可以根据最佳路由传送。这也就意味着您的声音（在 IP 中已被分组）有可能通过多条线路传送到一个目的地。目前，您无法在两个目的地之间指定一条路径。每个分组都在发送者和接收者之间选择最佳路径。

因为包交换层（packet layer）基于开放的标准使大量的厂商可以共同提供解决方案，这些开放的标准也增加了本层的竞争。ITU-T，因特网工程任务组（Internet Engineering Task Force，IETF），欧洲电信标准组织（European Telecommunication Standards Institute，ETSI），与电子工业协会－电信工业联合会（EIA-TIA）是一些标准化组织。

而拥有一个基于标准的分组交换架构的主要因素是在呼叫控制层有开放的标准。在图 1-12 中，这些开放的标准由 SIP、H.323、SGCP、MGCP、MEGACO 等协议提供。这些协议拥有开放的定义接口且已经被广泛地部署在分组交换架构中。呼叫控制协议的一个工作就是告诉 RTP 流在哪里开始又在哪里结束。呼叫控制是通过 IP 地址和电话编码计划的转换来完成这项任务。

1.5.2 开放呼叫控制层

简单来说，呼叫控制就是为一个呼叫选择路由来促成呼叫的过程。在当今的 PSTN 网络上，这些决定由业务控制点（Service Control Point，SCP）决定，由 SS7 承载。第 7 章讨论了不同 VoIP 协议的工作方式以及是怎样解决不同的网络设计问题的。

在新模型中将承载（RTP 流）从呼叫控制层中分离出来，并且将呼叫控制层从业务中分离出来。在新模型中使用的是基于标准的协议，确认这一点很有必要。数据组网因为在一个网络中可以同时存在多种协议而显得很独特。您可以根据具体的网络需求来使用这些协议。

比如有许多不同的 IP 路由协议，而且每一种都为特定的网络设计。这些协议包括路由信息协议（Router Information Protocol，RIP）、内部网关路由协议（Interior Gateway Routing Protocol，IGRP）、增强的内部网关路由协议（Enhanced Interior Gateway Routing Protocol，EIGRP）、中间系统对中间系统（Intermediary System to Intermediary System，IS-IS）协议、开放最短路径优先（Open Shortest Path First，OSPF）协议和外部边界网关协议（Border Gateway Protocol，BGP）。每种协议都解决一个类似的问题——路由信息的更新。每种路由问题都有些不同，因此需要不同的工具解决。在这种情况下，这些工具就是解决每个问题的路由协议。

对于 VoIP 的呼叫控制协议也是一样的。他们都解决一个类似的问题——电话号码到 IP 地址的转换。但因为目的的细微差异，他们可能都被使用。

许多 VoIP 呼叫控制协议正在被开发。最值得一提的是 SIP，它将继续掀起 IP 通信的风暴。在最近几年里，基于 SIP 的架构为端点提供了更多的智能并且在提供 VoIP 服务上得到了充分的发展。他们带来了网络上的一系列变化，通过使用会话控制器（session controller）与使用 H.323、MGCP 和 H.248/MEGACO 协议的*软交换（softswitch）*来集中呼叫控制。每种协议都是为了解决某个特定的问题和为特定的目的服务而开发的。简单地说，那就是许多协议都将被使用。我们将拥有一个解决不同网络拓扑需求的混合型网络。

1.5.3 VoIP 呼叫控制协议

到写这本书为止，主要的 VoIP 呼叫控制协议有 SIP、H.323、MGCP 与 H.248/MEGACO。另一种非常流行的网络电话的拓展是点对点（Peer to Peer，P2P）IP 电话。Skype 采用这种模型，但还没有形成标准。目前的标准协议有如下几种。

- MGCP 来源于 SGCP 和 1998 年开始开发的 IPDC，通过在集中平台（或网关控制器）上添加智能呼叫控制以减少末端（网关）的费用。第 13 章将详细论述这些协议。
- ITU 的 H.248，也称作 MEGACO 协议，是一个有关媒体网关控制的国际标准。它是由 ITU 与 IETF 联合推出的。它主要被用来在网关上将呼叫控制逻辑从媒体处理逻辑中分离出来。用于负责呼叫控制功能的设备称为媒体网关控制器（Media Gateway Controller，MGC），而用来负责媒体流量的设备称为媒体网关（Media Gateway）。
- SIP 是一种基于媒体的协议。它可以使末端设备（端点或网关）更智能，而且使很多增强业务可以在呼叫控制层完成。第 12 章覆盖了 SIP 的详细信息。

> 注释：点对点 VoIP 才刚刚起步，已被积极地推荐为 VoIP 技术的另一种选择。P2P 组网利用位于因特网边缘的功能相对强大的计算机（个人计算机），使这些计算机不单单完成客户端任务。除了收发 E-mail 和浏览网页外，现代 PC 足够强大的架构还可以完成音频/视频会议的任务。对于许多类型的应用来讲，现代 PC 可以同时充当客户端和服务器端（一个对等体）。微软和 Skype 是在 P2P 网络上测试部署 VoIP 的两个主要厂商。

为了简单说明这些呼叫控制协议的区别，让我们来看一下他们是怎样与端点通信的。

1. H.323

H.323 是 ITU-T 定义多媒体信息如何在分组交换网络上承载的建议书。H.323 使用一些已有的标准（如 Q.931）来实现这个目标。H.323 是一个相当复杂的协议，它不是为了简化应用开发而建立的，而是为了在“不可靠的”的数据网络传输多媒体应用而建立的。语音只是 H.323 中的一个应用。在这个领域的大部分的初始工作都集中在多媒体应用上，视频和数据共享这个协议的一大部分内容。

为了使应用适用 H.323，需要做大量的工作。比如完成一个呼叫需要另一个规范（H.450.2）。而 SGCP 与 MGCP 只需要给网关或终端设备一个简单的命令 modify connection（MDCX），就可以完成呼叫。这个简单例子也说明了构造协议的不同方式：一种是为完成简单应用（MGCP）；另一种是为了更复杂的应用，但又有它的局限性（H.323）。

为了更进一步的演示 H.323 的复杂性，图 1-13 列出了一个在两个 H.323 终端设备之间通话。

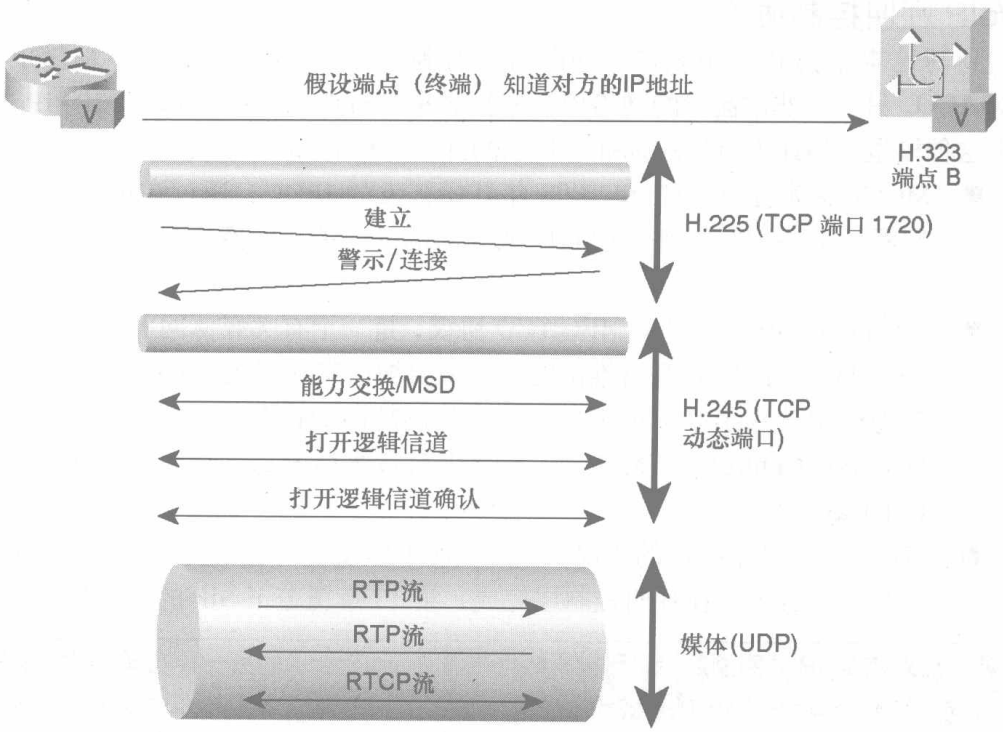


图 1-13 H.323 呼叫流程

图 1-13 演示了最基本的 H.323 通话流程。在大多数情况下，因为关守的参与，可能会需要更多的步骤。

让我们一步一步地来看这个通话流程，以更好地解释图 1-13。

1．终端设备 A 通过 TCP 端口 1720 向终端设备 B 发送一个建立（setup）消息。

2．终端设备 B 发送一个信号（alerting）消息和一个开始 H.245 协商的端口号来响应建立消息。

3．H.245 协商包含编码类型（G.729 和 G.723.1），RTP 流的端口号以及终端设备所拥有的其他功能。

4．UDP 流的逻辑信道被协商、打开和确认。

5．语音在 RTP 流上承载。

6．在两个终端设备上均采用实时传输协议（real time transport control protocol）传输 RTP 流。

这个呼叫流程基于 H.323 v1。H.323 v2 可以使 H.245 协商在 H.225 建立消息中完成。这被称作*快速启动（fast-start）*，它减少了建立 H.323 呼叫所需要的来回协商数，但它并没有简化协议。有关 H.323 的更多分析见第 11 章。

2．MGCP（由 SGCP 与 IPDC 发展而来）

SGCP 与 MGCP 为了使一个中心设备，被称为媒体网关控制器（Media Gateway

Controller，MGC）或*软交换机（softswitch）*来控制终端设备或媒体网关（Media Gateway，MG）而设计的。您可以通过 MGC 的标准的 API 来开发应用以提供附加功能（像呼叫等待和 CLASS 功能）及应用。

思科在这个技术上有两个知名设备：Cisco PGW2200 与 Cisco BTS10200。Cisco PGW2200 是一个呼叫代理，它包含思科媒体网关控制器（Media Gateway Controller，MGC）软件、思科信令链路终端（Signaling Link Terminals，SLT）、Cisco PGW2200 组件 IP 互联的局域网交换机等。在这个情景下，整个 IP 网络就像一个大的虚拟交换机，而 PGW 控制了所有的媒体网关（MG）。

图 1-14 展示了一个运行 MGCP 虚拟交换机的典型网络设计。

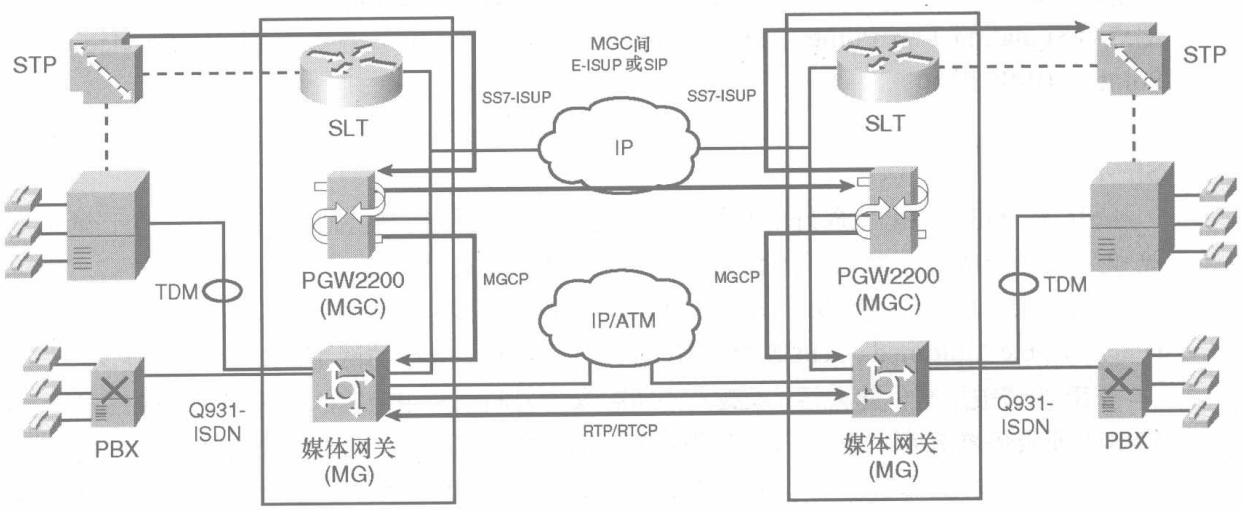


图 1-14 思科 PGW2200：*分组级联*

图 1-14 也展示了已有的 PSTN 和企业网络是怎样通过连接到网关或终端设备来访问新的分组网络的。这个分组网关从呼叫代理（call agent，PGW2200）处得到指示。呼叫代理连接到 SS7 网络和智能网可以通知网关或终端设备怎样和什么时候建立呼叫。

要想更深地理解图 1-14，我们还需要讨论其他组件。现有的 PSTN/SS7 网络是连接到交换传输点（Switching Transfer Point，STP）上的，而 STP 也连接到 MGC 与呼叫代理上。这个连接是信令（SS7）链路的终点，称作信令链路终端（Signaling Link Terminal，SLT）。SLT 为 PGW 提供 SS7 接口，从而形成一个任何 MGC 提供 SS7 接口的 MGC 一个完整的组件。

PSTN/SS7 网络也连接到一个 MG 上，这条链路是一条没有信号的中继线，也称作*机间中继线（Inter-Machine Trunk）*或 IMT. 64kbit/s 的语音中继线在 MG 处被转换为分组而运行在 IP 网上。

MGC 与呼叫代理（在我们这里就是 PGW200）也是互相通信的。然而还没有标准化组织为其制订通用协议。在目前的行业情况下，SIP 的各种版本或在 IP 上的综合业务数字网

用户部分（ISDN User Part，ISUP）（在 IP 上运营的 SS7 的一部分）是目前的主流协议。MGC 有一个到智能网的连接（我们在本章的前一部分已经讨论过）来提供 CLASS 业务。MGC 接收来自 SS7 网络的信号，告诉 MG 什么时候和哪个 MG 建立 IP 连接。

PGW2200 在这种情况下是一个典型的 MGC，通过称作 E-ISUP 的 ISUP 的扩展来与其他 PGW 通信。它同样从 B 信道中分离出 D 信道，然后将 D 信道通过 IP 传送给 MGC。这个机制称为*信令回程（signaling backhaul）*，它是通过由 sigtran 开发的一系列协议完成的。SIGTRAN （信令传输，signaling transport）是 IETF 标准化组织中的一个工作小组。这些协议阐明了在 IP 网络上传输 PSTN 信令的功能和性能要求。SIGTRAN 协助区分什么信令协议怎样在 IP 点与点之间进行传输、转换和/或终结。这些点包括信令网关（Signaling Gateways，SG）、媒体网关控制器（Media Gateway Controllers，MGC）、信令端点（Signaling End Points，SEP）和基于 IP 的数据库或者业务控制点（Service Control Points，IP-SCP）。

SIP

SIP 在 RFC 3261 被很好的解释：SIP 是一个应用层控制（信令）协议，用于建立、修改和终止一个或多个参与者的会话。然而，IETF 委员会开发了许多附加的 RFC，为核心 RFC 提供新的功能，使 SIP 成为一个在 VoIP 中的会话控制协议，同时也是分组多媒体（PacketCable Multimedia，PCMM）和无线及基于集团电话的网络的会话控制协议。

SIP 邀请被用来创建会话，承载允许所有参与者同意一组兼容的媒体类型的会话描述。SIP 使用代理服务器来帮助路由请求到用户目前所在的位置、认证和授权用户，实施提供商的呼叫选路策略以及为用户提供相关功能。SIP 也提供注册功能，以允许用户上传他们现在的位置供代理服务器使用。SIP 可以运行在多种传输协议之上。

尽管大多数的厂商及用户都倾向于在一个混合的模型中将 SIP 与 H.323 或 MGCP 联合使用以允许网络中的其他各点对等来部署增强业务，但目前有多种 SIP 实施正在运行中。

更详细的 SIP 信息请参见第 12 章。

H.248/MEGACO

媒体网关控制协议（Media Gateway Control Protocol，MEGACO)是 IETF 与 ITU-T 研究组 16 联合工作的结果。此协议的定义参见 ITU-T 建议书 H.248。

MGCP/MEGACO 打破了 H.323 的关守模型，将信令协议从网关中移出，并添加到媒体网关控制器（Media Gateway Controller，MGC）或*软交换机（softswitch）*中。MGC 或软交换机控制多个“媒体网关（media gateways)”，也就是将 H.323 架构分解到与 SS7 相对等的部分，从而使信令智能化。

在 MGCP/MEGACO 架构中，这些智能部分没有与媒体捆绑在一起。这是一个主从协议，其中主设备享有完全控制权，而从设备只是执行命令。主设备是媒体网关控制器或软交换机（或呼叫代理），从设备是媒体网关（这可能是 VoIP 网关，数字用户线接入复用设

备（Digital Subscriber Line Access Multiplexer，DSLAM），多协议标记交换（Multiprotocol Label Switching，MPLS）路由器、IP 电话，等等）。这与 SIP 以及如 Skype 的其他模型的对等的特性正好相反，在那些模型中，一个客户端可以同另一个客户端直接建立会话。

MEGACO 指示媒体网关将从外面分组网络上来的流量连接到一个分组网上去，如 RTP 的包流。软交换机下达如发送接收来自其他地址的媒体，产生音调、修改配置等命令。然而，整个体系结构要求 SIP 作为媒体网关控制器（MGC）之间的通信协议。MEGACO 主要有以下几部分构成：

- 信令网关 （Signaling Gateway，SG）；
- 媒体网关控制（Media Gateway Control，MGC）；
- 媒体网关（Media Gateway，MG）。

1.5.4 开放业务应用层

在任何网络协议中，最有趣的层是应用层。没有好的应用，网络架构的建设也就失去了意义。当转移到一个新的架构上去时，没有必要把老架构上的所有功能都转移过去。只要转移用户需要的功能或应用就可以了。

当建设一个拥有分组包层到呼叫控制层的开放接口，呼叫控制层到应用层的开放接口的网络时，设备提供商不再必须开发应用。他们只需书写标准的应用程序接口（API），开放整个新的架构就可以了。当一个新的分组架构建设完成后，许多新的应用都可以开发。

已有的应用，如企业网络的呼叫中心、标准的 PSTN 应用如呼叫等待和呼叫转移，都必须在最终用户没有意识到的情况下转移到新的架构上面来。当这些已有的应用转移过来后，成千上万的新的增强应用就可以定义开发了。这些应用包括（但不局限于）因特网呼叫等待（Internet call waiting）、一键通（push to talk）、发现—跟踪（find me-follow me）以及统一消息(unified messaging)等。这些应用将在第 6 章中详细讨论。

1.6 新 PSTN 网络架构模型

正如我们前面几节讨论的一样，新的模型将致力于将老的僵化的架构分离出来，从而能允许大量的厂商可以在新架构上为用户开发应用和功能。图 1-15 表明了思科系统准备怎样推进新模型。

图 1-15 清楚地显示了 3 层之间的关系以及 3 层与在网络中将用到的其他组件的关系。运营商们很欢迎这种方式，因为这意味着他们无需在每层固定选择一个解决方案。他们可以根据需要来选择提供的业务、功能和面市时间。

也许一些运营商可能还在犹豫采用超过一家的设备提供商会增加集成的难度，但很多运营商都会选择至少两家设备提供商以增强竞争。

在图 1-15 中，承载者（bearers）、连接层或媒体传输可能是 IP 网关或 ATM 网关，或者是他们两者的组合。刚开始时会有多个设备供应商，但他们会逐渐合并为 3 到 5 个参与者。

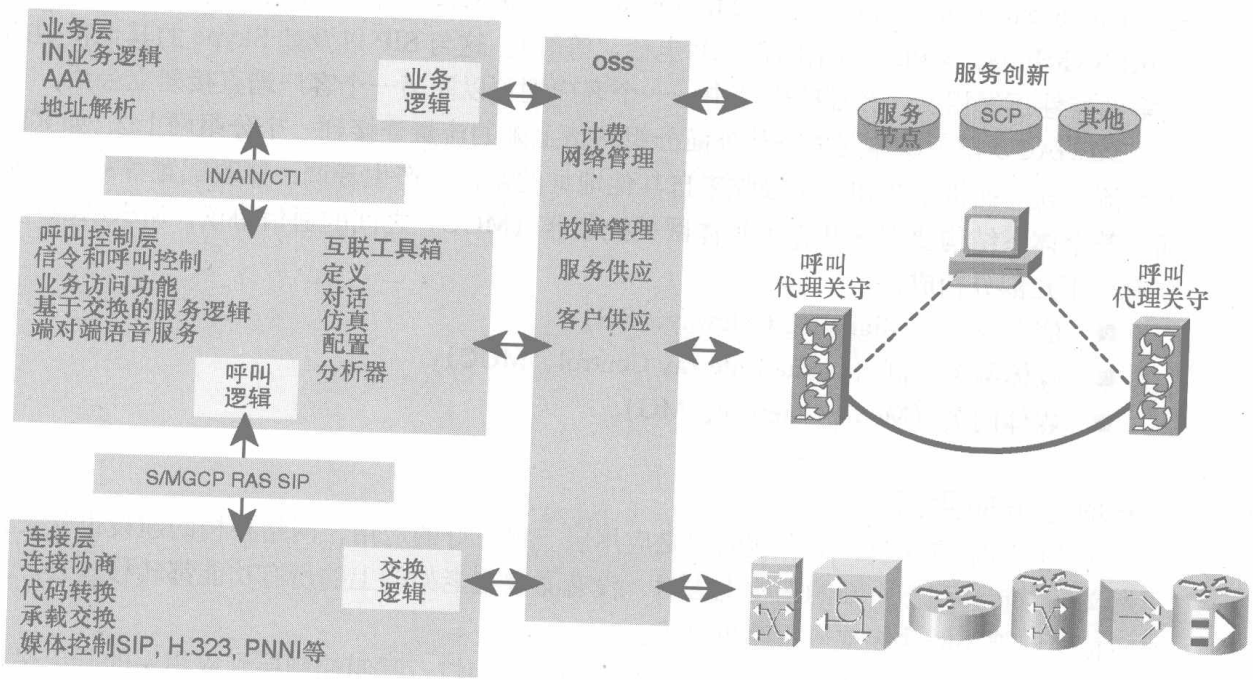


图 1-15 分组电话网络元素

> 注释：在制造商和运营商舞台上，有一个*整合（consolidation）*趋势。制造商之间的整合是这个领域中参与者数目急剧减少的原因。

呼叫控制层对于新 PSTN 网络架构来讲是非常重要的一部分，因为它必须与连接层和服务（应用）层很好地共存。许多供应商正在扩展 SIP 与 MTCP 技术以提供增强业务。

事实上，我们（本书的作者们）正在与大约 15 家供应商一起工作，以确保从连接层面到呼叫控制以及服务/应用层的兼容性。

许多供应商将继续在呼叫控制层工作，因为服务提供商将根据他们要部署的服务而为此项主要技术选择多家供应商。呼叫代理供应商的责任就是确保自己的设备与其他供应商兼容。呼叫代理的协同工作能力是保证服务提供商使用大规模的、基于分组交换语音网络的一个重要因素。

服务或应用层是可能发生网络变革的地方。影响服务层的一个重要因素就是它要依赖软交换机供应商开放足够有用的 API 以开发应用。正是由于这个原因，你会发现许多应用供应商直到呼叫代理商完全友好地开放了 API 才开始开发应用。

成千上万的独立软件开发商（ISV）将一起在服务层开发新的利润增强型应用。这就与在客户/服务器革命中微软清扫了拥有视频编码驱动的障碍等一样，ISV 可以将精力集中在应用上了。同样的革命发生在当今的 PSTN 上，它终将改变服务以及电话/多媒体网络的设计、建设和部署的方式。

1.7 总结

从 1876 年发展到今天，PSTN 上的语音服务已经相当复杂，它是几种不同技术的共同产物。正如您所了解的一样，今天的 PSTN 面临着变革。

在日常使用多媒体会话所需的技术已经成熟。这并不像您所了解的那样需要一台计算机。并且，电话/通信架构正在转移到一个新模型上，而且很快将会承载这些多媒体会话。

这个难题的最后因素就是能完成多媒体会话的足够的带宽。这个难题将最终通过 DSL 与有线宽带之间在带宽上的战役解决。最后，用户将是最终的胜利者。他们将使用排除了距离和通信的障碍的技术，并彻底改变目前工作的方式。

本章讨论网络架构框架和设计模型，包含以下主题：

- 2.1 PSTN 与 ET 的相似之处
- 2.2 PSTN 与 ET 的不同之处
- 2.3 PSTN 与 ET 互联的通用方式
- 2.4 总结

第2章

企业电话的今天

企业电话（Enterprise Telephony，ET）是一个可以提供诸如呼叫保持（call hold）、三方通话（three way calling）、呼叫转移（call forwarding）、呼叫转接（call transfer）等基本商务功能的商务电话系统。企业电话（ET）与公共交换电话网络（Public Switched Telephone Network，PSTN）有许多相似的地方，但也有着许多不同。本章主要讨论这两种网络的相似与不同、他们合作的方式和典型 ET 网络设计。

2.1 PSTN 与 ET 的相似之处

在以下几个方面，PSTN 与 ET 是相似的。

- 电路交换（Circuit Switching）——两种网络都是基于 64kbit/s 电路上的时分多路复用（time-division multiplexing，TDM）交换。
- 公共架构模型（Common Infrastructure Model）——承载信道、呼叫控制和业务面都在一个平台上。这些特点在第 1 章中已经介绍过了。
- 本地回路（Local Loop）——电话“直接”连接到交换机来接收拨号音，拨叫或接听电话，等等。
- 可提供的业务——两种网络都可以提供如呼叫保持（call hold）、三方通话（three way calling）、呼叫转移（call forwarding）、呼叫转接（call transfer）等基本业务。

两个网络都使用 64kbit/s 交换电路，但范围有很大的不同。PSTN 使用 5 类交换机可以支持几万条的本地回路。对应于 5 类交换机，ET 使用专用小交换机（Private Branch eXchange，PBX），支持 5 个到几千条本地回路。

5 类交换机的主要任务是提供住宅电话服务，但它也提供一些例如呼叫等待和来电回拨等在内的商务功能。而专用小交换机（PBX）通常会提供更多的功能，包括呼叫保持、三方通话或会议、呼叫转接、自动总机（autoattendant）和语音信箱等。

2.2 PSTN 与 ET 的不同之处

PSTN 与 ET 的不同之处在于它们处理信令的方式和它们提供的业务方面。

2.2.1 信令处理

PSTN 使用的信令接口是由行业团体开发出来的。PBX 的制造商们为了使他们的 PBX

可以在ET语音网络上互通并透明传输附加功能，往往采用私有协议。

第1章讨论了PSTN是怎样使用7号信令系统（Signaling System 7，SS7），ISDN以及带内信令作为它的信令链路的。这些都是已经很好文档化而且已经发展了许多年的标准。但这些信令协议不能解决当今的所有信令问题，任何人都可以开发与PSTN网络接口的软件。

> 注释：这些软件和硬件都必须通过它要入网的每个国家的许可（homologated）。许可就是每个国家证明设备可以接入该国家PSTN网络的过程。对于一些国家，当一个已经接入网络的设备的软件更新时需要重新被许可。

目前在ET中的许多PBX使用CAS（随路信令发送）、PRI（基群速率接口）与PSTN信令通信。很多时候，为使第三方计算机应用可以控制一些PBX的操作，也使用计算机电话集成（computer telephony integration，CTI）链路。但是大多数PBX设备供应商实施私有的信令机制。这就迫使企业网络只能使用一种品牌的PBX。虽然这对于制造厂商有好处，但是企业商务用户只好为他们的语音传输、服务和应用锁定一个供应商。

另外，许多PBX厂商使用私有信令为该厂商私有的电话机提供增强功能。这还迫使企业用户采用同一厂商的电话机来保持与PBX的兼容。

> 注释：许多厂商目前为了能兼容它们之间的PBX正在实施基于标准的信令协议。目前都有如下协议：
>
> - Q信令（Q Signaling，QSIG）——这是一个使许多厂商在附加服务，拨号计划和其他许多方面达成一致的开放式标准。（其中，“Q”来自国际电信联盟电信标准化部（International Telecommunication Union Telecommunication Standardization Sector，ITU-T）的Q.xxx系列标准。）
> - 数字专用网络信令系统（Digital Private Network Signaling System，DPNSS）——这是一个使跨厂商或多厂商PBX协同工作的英国标准，这个标准包含在QSIG中。

2.2.2 增强功能

在提供增强功能方面，ET与PSTN也有着很多不同。与普通的住宅用户来相比，商务对电话网络的要求会更高一些。企业用户需要高实用性、功能丰富的系统，他们需要如下应用。

- 呼入呼出呼叫中心（Inbound and outbound call centers）——拥有这项功能的ET网络通常拥有CTI（计算机电话集成）链路，该链路上可以运行许多新应用——比如，在销售代表的计算机屏幕上显示来电号码，以及该呼叫者的其他信息（购买倾向、邮购地址等）。
- 金融企业电话（Financial Enterprise Telephony）——包含此项功能的ET网络通常包含一个 *hoot-n-holler* 网，这样就可以允许一个人讲话而许多人接听。这在证券公司非常常见。

ET 用户也可以使用 PSTN 来提供 PBX 的基本服务，但是已有的 PSTN 一般没有像呼叫中心这样的高级应用。而且，使用 PSTN 也没有使用 ET 经济。

2.3 PSTN 与 ET 互联的通用方式

虽然在企业领域，ET 功能丰富且深入人心，但它必须与 PSTN 互联以呼叫企业外部的用户。这种交互可能简单地通过 PSTN 的一条模拟线路或者是两个 PBX 之间的专线连接，也可以复杂到使用交互运营商（inter-exchange carrier，IXC's）提供的异步传输模式（Asynchronous Transfer Mode，ATM）连接。本节覆盖了大多数 ET 网络中所采取的常用方式和网络设计。

企业大约有 5 种方式可以选择，每种选用的组件有些少许的不同。这些方式如下。

- 简单商务线路（Simple business line）——这种方式直接使用一条 PSTN 线路作为商务线路。这条线路与住宅线路相似，但商务客户通常需要支付更高的费用。这种方式会被不需要太多功能的小企业采用。这项服务由本地通信运营商（Local Exchange Carrier，LEC）或本地通信运营商的竞争者（Challenger LEC，CLEC）提供和管理。
- PBX——专用小交换机（PBX）提供了商务用户需要的许多功能（如呼叫保持、呼叫转移、呼叫驻留，等等）。PBX 交换机通常通过 T1 或 E1 线路连接到 PSTN。这些系统通常集成了语音信箱、本地线路和 PSTN 中继。
- 交钥匙系统（Key system）——这是一个较小版本的 PBX，一般被少于 50 人的办公室使用。交钥匙系统通常拥有较少的功能，一个完整的语音信箱系统和在交钥匙系统电话上的多“列席”功能代替了呼叫转移功能。
- 汇线通（Centrex line）——由 LEC 或 CLEC 提供和管理，这条线路提供类似 PBX 的附加功能，但需要缴纳额外的月租费。这些业务包括呼叫转移，三方通话和一个封闭的用户拨号计划。
- 虚拟专用网（Virtual Private Network，VPN）——通过 VPN，PSTN 为企业用户提供一个专用的拨号计划。LEC，CLEC 与 IXC 可以提供 VPN。另外，本地的 PBX 可以提供附加功能。

这些方式可以大致分为两类：由 PSTN 提供和管理的和私有的只须与 PSTN 连接的。在下面的章节里我们分别讨论这两类方式。

2.3.1 PSTN 提供的 ET 网络

当一个企业只有有限的资源，不能成立一个专门的部门来管理电话网络时，它通常会寻找 PSTN 服务商或增值服务商（Value Added Reseller，VAR）来提供电话服务。PSTN 运营商会提供设备、人员和通信服务，VAR（增值服务商）会安装 PBX 设备并提供连接到 PSTN 的必要服务。因为让内部的信息化（Information Technology，IT）部门有效地管理整个网络是不经济的，所以企业一般都会采用 PSTN 提供的 ET 服务。由 PSTN 提供的电话

网络有：

- 简单商务线路（simple business line）；
- 汇线通线路（A Centrex line）；
- 虚拟专用网络（A VPN）。

1. 简单商务线路（Simple Business Line）

这3种方式中最基本的方式就是简单商务线路。这项业务通常被只有一两个人而不需要太多电话功能的小企业所采用。

对于一个只有一个雇主和一个雇员的小公司来说，一条装有留言机的电话线就足够用了。这样的公司不需要呼叫等待和呼叫转移等功能。简单商务线路与住宅线路很类似，但它通常有着更高的月租费，这是因为本地运营商为商务用户提供了更多更好的服务。

2. 汇线通线路（Centrex Line）

当企业发展到了一定程度，通常会需要一些附加服务，如呼叫转移、呼叫保持和呼叫等待。企业可以购买一个交钥匙系统或PBX，大概需要2 000美元，或者每月多付大概20到30美元来获得这些附加服务。

这些业务使PSTN可以向闭合用户群（Closed User Group，CUG）提供功能。这个闭合用户群中的所有电话构成了一个虚拟交换机，人们可以通过拨打4到5位数字互相呼叫、转接呼叫或让呼叫等待。这项业务比简单商务线路提供更多的功能，但对于企业来讲成本也较高。

3. VPN

企业还有一种选择就是VPN。VPN为企业客户提供一个专用网络而不需要客户投入管理，或提供一个大的*直达线路（tie-line）*（直达线路是指两点之间的固定线路）网络所需的设备。

VPN允许企业客户拨打一个特定的号码，这个号码则指示PSTN将客户按一个闭合用户群（CUG）对待。我们来举个例子，一个大的零售公司在全美都有办公室，他不想在他的3000多个分支上使用交钥匙系统或PBX。这将是一个庞大的网络。

这个公司与长途电话公司（IXC）联系为他的3 000个分支提供VPN服务。公司为每个分支分配一个4位的分支号码用于公司内部的联系。这样分支号码就很好地区分了各个分支机构。图2-1表明了该网络的架构和呼叫流程。

IXC给零售店一个号码来拨打-1-700-123-3154。IXC通知LEC将这个呼叫转交给IXC负责，这样IXC知道这个号码所对应的拨叫计划（最后4位是分支号码）。

位于加利福尼亚的圣何塞（San Jose）分支的分支号码为5134。这家店的烤面包快卖完了需要呼叫附近的弗里蒙特店（分支号码3145）。老方法是拨打一个由1-408局（圣何塞）到1-510局（弗里蒙特弗里蒙特）的长途电话。但是今天，5134只要知道弗里蒙特店的分支号就可以拨打1-700-123-3154来呼叫弗里蒙特店了。

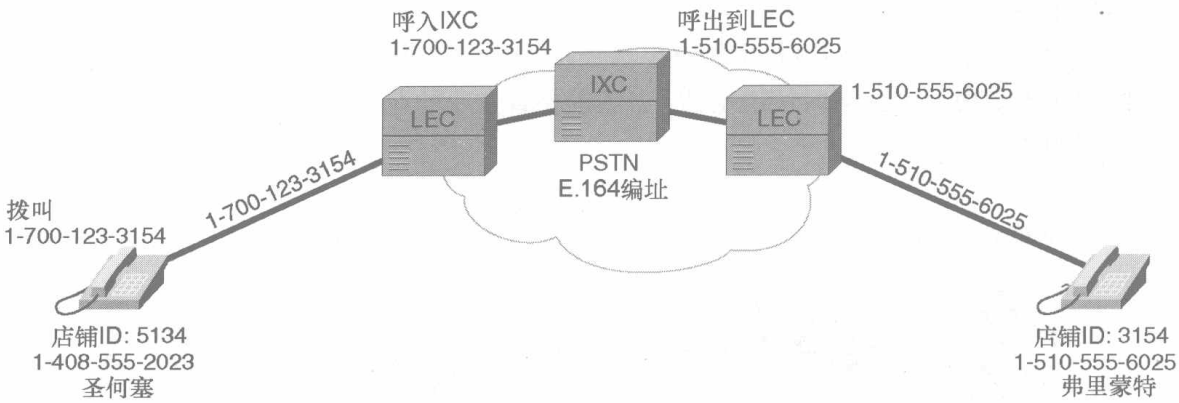


图 2-1 虚拟专用网络

IXC 将 1-700-123-3154 这个号码翻译成真正的电话号码，但对于零售店店员来讲，这是完全透明的（弗里蒙特店接到电话后很快就将烤面包机送了过来）。

参照图 2-1，这个呼叫更详细的步骤如下。

1．在圣何塞的用户拨打 1-700-123-3154。

2．LEC 接收到拨打的号码。

3．LEC 交换机将这些数字发送给 IXC。

4．IXC 接到 1-700-123-3154，知道这是一个 VPN 号码，将其翻译成 1-510-555-6025，也就是弗里蒙特店的真正的电话号码。

5．IXC 将该呼叫以 1-510-555-6025 号码发送给本地的 LEC，因为 LEC 只认识这个号码。如果 IXC 发送 1-700，LEC 会将这个呼叫重新路由到 IXC。

6．LEC 交换机将这些数字发送给 IXC。

7．LEC 查找 555-6025 本地线路然后路由该呼叫到本地回路。

8．零售店接听呼叫，但并不知道这是从 VPN 来的呼叫。

VPN 在为企业的 3 000 多个远程办公室提供一个简单的网络使用的同时，为企业节省了内部信息化服务的费用。

我们前面所举的例子省略了许多中间部分以求简单。在这个例子中，呼叫查找应该发生在 SS7 或 C7 网络。为了从宏观上解释 VPN，我们省略了这部分的描述。

2.3.2 私有 ET 网络

到目前为止，企业最常用的为其员工提供电话接入的方式是购买自己的交钥匙系统或 PBX。这些方式有如下的许多优点。

- 没有附加收费——拥有自己的 PBX 均摊到每月的费用比从 PSTN 购买集中交换机业务（Centrex services）要低。
- 可以自己控制添加、转移和修改——当需要添加新的电话线、移动一个电话或者更改使用者的信息时，没有必要联系 PSTN 运营商，完全可以自己完成。

PBX 网络

图 2-2 显示了从 PSTN 租用所有电话线路和使用 PBX 而租用比电话数少的线路的区别。因为大多数用户不会同时使用电话（当然也要看企业的业务类型），使用 PBX 节省了 PSTN 线路的费用。

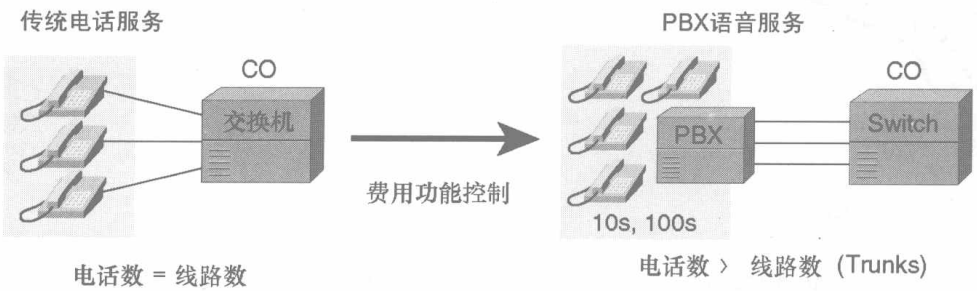


图 2-2 PBX 与 PSTN 的区别

企业用户使用他们自己的专用小交换机（PBX）的另外一个优势是可以自己控制。如果您需要添加一个用户，改变某个功能或者移动一个用户到另一个位置，都没有必要跟 PSTN 运营商联系。

PBX 的使用增加了另一个层次的复杂性。企业用户必须自己应付配置和维护 PBX 上的呼叫路由的压力。图 2-3 显示了通过 PBX 拨叫 PSTN 的呼叫流程图。

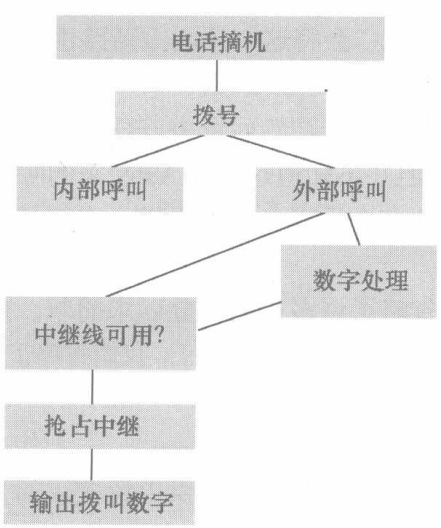


图 2-3 通过 PBX 的 PSTN 呼叫

图 2-3 详细列出了 PBX 怎样路由一个呼叫到 PSTN 或内部分级。这个过程对用户来讲可以是隐蔽（比如所有以“1”开始的呼叫使用外部中继线路）的，或者要求用户协助 PBX

选择正确路径（例如要求用户拨“9”拨打外线）。

在很多情况下，是由用户先拨打一个数字来拨打外线（在美国通常为“9”，在欧洲通常为“0”）的。其他情况，用户根本就没有意识到呼叫被路由到了 PSTN。我们以一个在广大的地理区域内有很多分支公司的 5 位编码计划为例。如图 2-4 所示，每个 PBX 都可以将 5 位号码翻译成 1+10 号码（ITU-T 建议书 E.164）并路由呼叫到 PSTN。这个 1+10 号码遵从了 ITU-T 建议书，可以被认为是 E.164 号码。

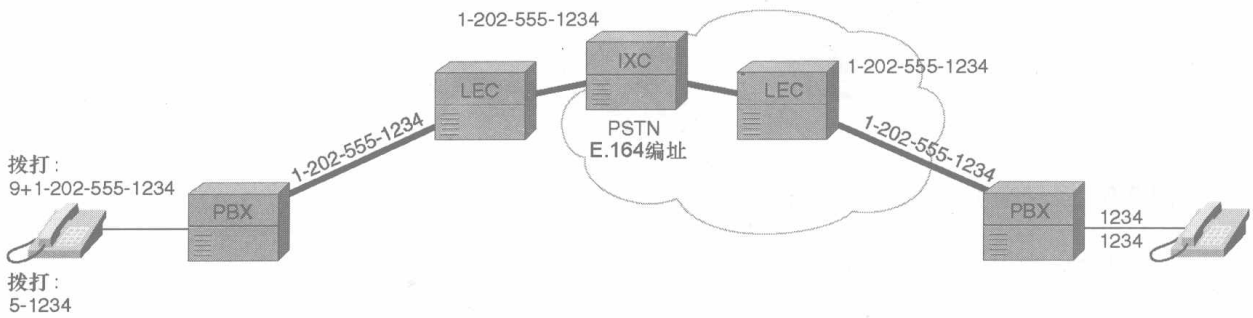


图 2-4 PBX 号码转换

在图 2-4 中，发生了如下动作：

1．用户拨打 5-1234（与拨打 9+1+202+555+1234 相当），本地 PBX 将这个呼叫翻译成 1-202-555-1234 发送给 LEC 交换机。

2．LEC 将这个 1+10 号码转发给 IXC，IXC 又将其转给另一个 LEC。

3．202 局的 LEC 将整个 10 位号码转到远程 PBX。

4．远程 PBX 修改呼入的 202-555-1234 号码为一个 4 位号码，然后振铃相应线路（1234）。

这个号码操作过程，使 PBX 用户可以拨打最少位数的号码。这不仅节省了用户的时间，还使用户比较容易记住常用的分机。

PBX 互联直达线路

如果一个企业有两个办公地点，且这两个办公地点之间有大量的电话通话量，企业通常会购买直达线路。直达线路就是两点之间的固定电路（T1，E1，部分 T1/E1，或其他传输介质）在这种情景下，要想经济的话，使用直达线路必须要比使用 PSTN 省钱。

图 2-5 展示了使用 T1 链路连接的两个点（一个在加利福尼亚的圣何塞（San Jose，California）另一个是得克萨斯的达拉斯（Dallas，Texas））。

此时连接线路仍然采用 PSTN，但企业只需为 San Jose 与达拉斯（Dallas）之间的专线付通常费率。

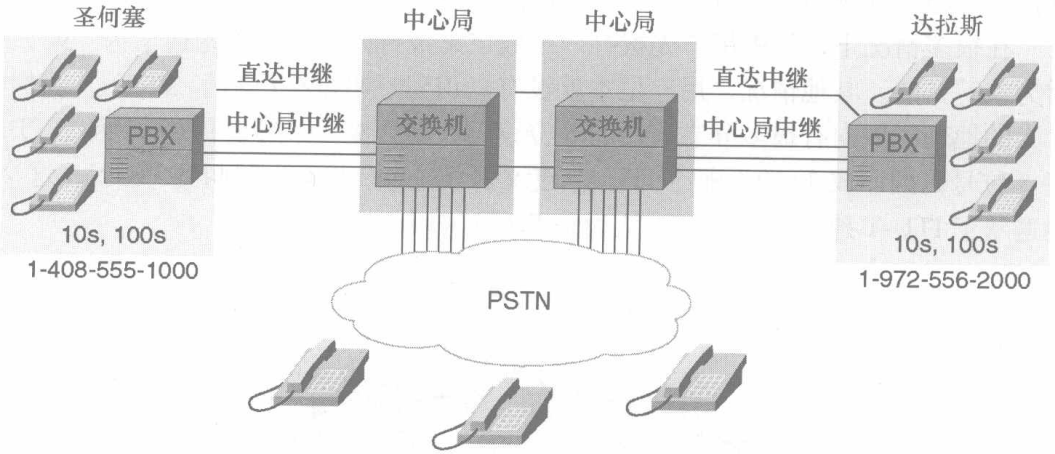


图 2-5 圣何塞（San Jose）与达拉斯（Dallas）间的直达线路

PBX 使用事先编程实现的自动路由选择（Automatic Route Selection，ARS）表来决定选择哪条中继线。让我们回过头来再看一下图 2-5，图中的 PBX 被配置成使用圣何塞与达拉斯之间的直达线路。如果直达线路超载，则 PBX 使用 PSTN 或中心局（Central Office，CO）中继来承载超载部分。

我们需要仔细分析圣何塞与达拉斯之间的电话流量和与 T1 线路的费用比较，来知道直达线路是否经济。图 2-6 显示，当每个月两地之间的通话时间在 30～35 小时之间时，两者费用持平。（这只是简单数据，通常，需要通过一个爱尔兰分析（Erlang analysis）来决定所需的中继线数目）。超过 30～35 小时的部分，就是企业节省的部分。只要流量是均衡的，则所有的呼叫都使用专用 T1 线路。

直达线路是 ET 网络设计者所采用的另一种路由他们流量的方法。路由呼叫流量是一件相当复杂的事情，需要多年的经验和知识。话务流量模型是一个很完善的研究领域。第 15 章将更细致的覆盖流量分析部分的内容。

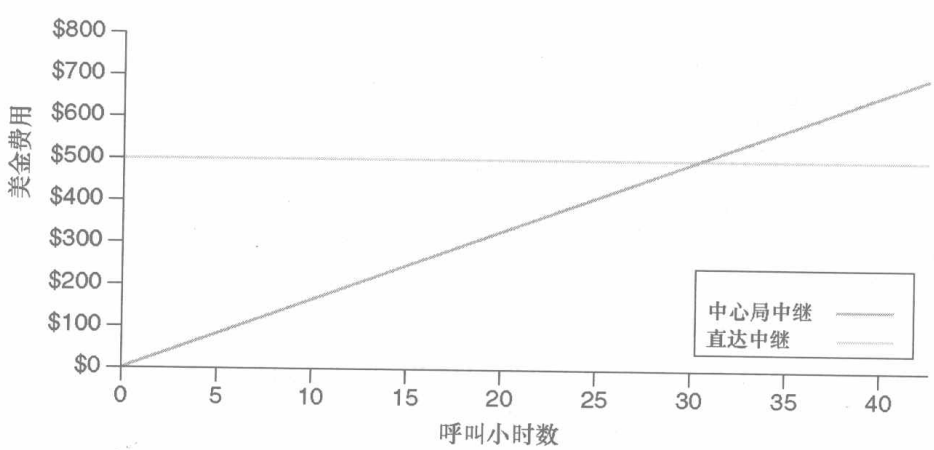
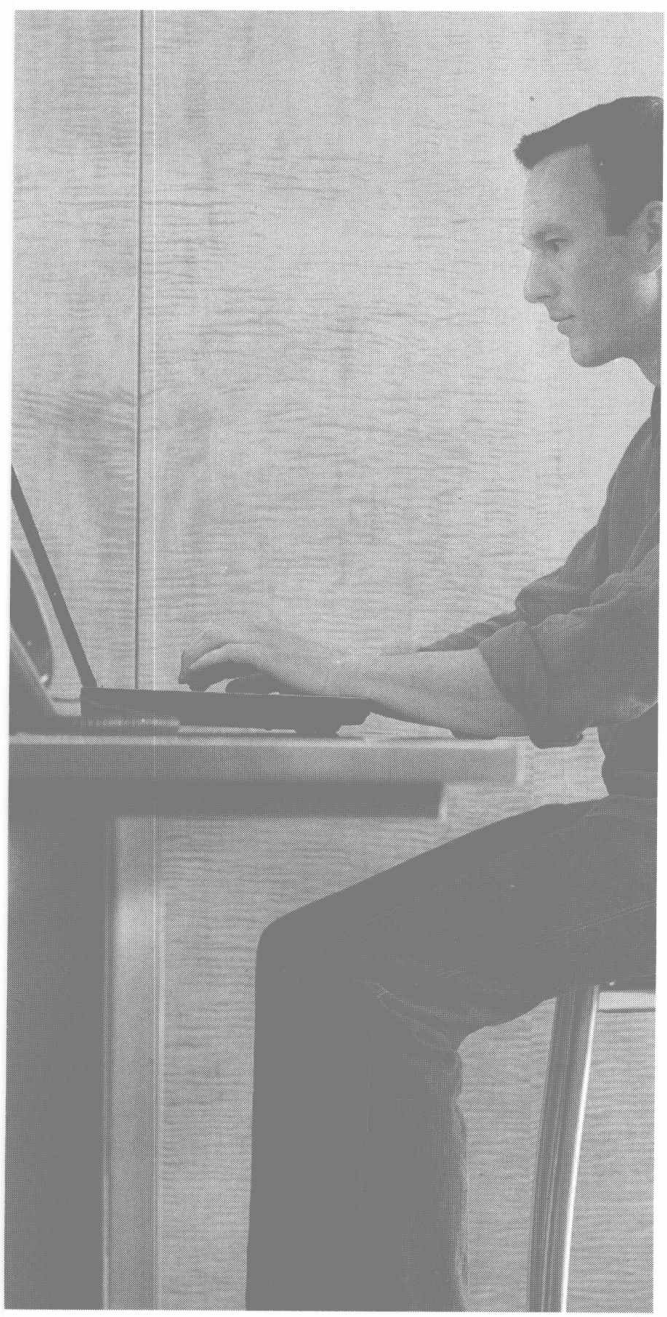


图 2-6 直达线路与 PSTN 费用比较

2.4 总结

ET 用户与 PSTN 上的普通用户的有不同的需求。因此，ET 用户要为这些需求而建设网络和设备。随着电信标准的放开，企业用户可以选择的对象也将呈指数上升。

这些可替代的方式——包括语音数据的分组包交换网络、综合接入和许多其他方式——将改变最小代价路由的方法，从而完成中继/忙小时数的计算。



本章讨论网络架构框架和设计模型，包含以下主题：

- 3.1 信令概览
- 3.2 E&M 信令
- 3.3 CAS
- 3.4 ISDN
- 3.5 QSIG
- 3.6 DPNSS
- 3.7 总结

第3章

基本电话信令

许多企业意识到了拥有自己语音网络的优势，所以他们通过使用专线连接 PBX 来完成办公室间的通信，或者使用语音虚拟专用网（Virtual Private Network，VPN）。最初，PBX 被连接到公共交换电话网络（Public Switched Telephone Network，PSTN）上提供语音服务，或者他们之间通过模拟直达线路连接来传输语音。当需要更多的语音中继线及技术成熟时，模拟直达线路会被高速的功能丰富的数据网络设备代替。本章将主要分析在模拟与数据网络之间，协同网络工作的信令技术。

本章也讨论了随路信令（channel-associated signaling，CAS），例如贝尔系统的 MF，国际电报电话咨询委员会（Consultative Committee for International Telegraph and Telephone，CCITT）的 No. 5、R1 和 R2，并回顾了这些 CAS 系统是怎样操作的。

本章也会涉及综合业务数据网（Integrated Services Digital Network，ISDN）、Q 信令（QSIG）和数据专用网络信令系统（Digital Private Network Signaling System，DPNSS）等接入协议。

这些协议将 PBX 信令通过网络传送给远端 PBX。专用的 ISDN 网络使用 PSTN 互相连接和提供服务。QSIG 是一个 PBX 间的信令系统，与 ISDN 类似，它协同 PBX 工作而形成一个私有的语音网络。DPNSS 是一个使 PBX 互联的 ISDN 类型的协议，但没有 ISDN 和 QSIG 使用广泛。

3.1 信令概览

在论述各种信令方式与标准之前，我们有必要先讨论一下一些基本概念。这些应用于每个单独信令方式的基本概念将贯穿本章。

3.1.1 模拟与数字信令

PBX 最初使用简单的模拟线路互联来传输语音和信息。但是现在使用模拟系统的情况已经不多见了，大多数情况下使用的是比模拟线路更经济可靠的高速数据链路。

数字信令是目前服务供应商网络和企业网路使用的最多的信令技术。在数字网络中使用了多种形式的信令技术。

其中一种是强取比特信令（robbed-bit signaling）。在这种方式下，指定的帧中的 1 位被“强取”用于信令。强取彼特信令在数字语音信息流中增加了信令信息，但不影响语音质量。在 3.3 节中我们将仔细讨论这项技术。除了 CAS，还有如 R1，R2，ISDN，QSIG 和 DPNSS

等其他数字协议。

3.1.2 直流信令

这种形式的信令依赖于直流（direct current，DC）来向终端交换机或办公室发送信号。DC 信令通过开关直流电来表明目前的传输状态。这些端局交换机使用直流探测器来探测状态的转变。以下两个信令协议使用的是 DC 信令。

用户环路（Subscriber Loop）——在本地终端局与用户之间的简单 DC 信令。当用户拿起听筒时，在用户电话与本地终端局之间的线路上产生一个–48V 的直流电流。终端局的线卡（Line cards）装有直流探测器，该探测器用于决定什么时候有一个呼叫连接。当用户挂上电话时，电话上的电容器将掐断电流。

跟摘机操作一样，DC 信号的改变通知端局交换机呼叫终止了。在这种情况下，使用同一对线路来提供语音和信令路径。

接收与发射（recEive and transMit，E&M）——这是一个中继线路协议，使用 DC 信令方式来显示中继线或直达线路上的状态转换。在 E&M 中，两条导线——称为“E”和“M”——被指定给信令。您可以通过使用地线（ground，earth）或电压互感器（voltage potential（magneto））来检测 E&M 导线的状态。这种形式的信令，我们将在本章后面的 3.2 节中仔细讨论。

DC 信令有一些局限性。比如，信令受 DC 可以表示的状态限制。而且，当语音与信令使用同一对线路时，电话线或中继线在两个用户还没有连接时也有可能被占用。

3.1.3 带内和带外信令

带内信令使用音调代替 DC。这些音调根语音使用同样的设施，也就是说在 0～4kHz 带宽内。这些音调包含单频（Single Frequency），多频（Multi-Frequency，MF）双音多频（Dual-Tone Multi-Frequency，DTMF）等，下面我们一一介绍。

- 单频（Single Frequency）——这种音调主要用于局间中继线，有两种可能状态：挂机或空闲，摘机或忙。单频音调基于一个 2 600Hz 的音频，用于显示状态的改变。因此，在线路连接时没有音调显示。不管那端挂起电话，一个 2 600Hz 音调被发送到电路上来通知所有的局间交换机断开该呼叫。

  单频音调曾经被用来从服务供应商那里骗得长途服务。犯罪者在用户线路处添加一个“蓝盒子”，使用这个盒子欺骗局间交换机将 2 600Hz 音调解释成一个前向拆线信号（clear forward signal）。局间交换机接受呼叫方号码，认为本地交换机会向该呼叫收费。接入局间交换机一般伴随拨“0”操作，在接线员接听之前就已瞒过了局间交换机。服务供应商最终通过实施一些保护措施来终止这些操作。
- MF——MF 音调被局间中继线路用来显示如占用、释放、应答或确认等事件以及传送呼叫方号码等信息。MF 信令使用有频率定义的组合脉冲来在网络上传输信令。这些频率是由系统定义的，我们将在本章后面的 3.3 节详细论述。MF 信令与语音使

用同一信道，所以不如像 7 号信令系统那样的公共信道信令（common channel signaling，CCS）有效。

- DTMF——DTMF 被用来将电话号码由用户传送到终端局办公室。随着 DTMF 的发展，电话内晶体管振荡器（transistor oscillators）将逐步被键盘和双音频振荡器取代。DTMF 音调区分 0～9 的数字和“*”与“#”。当用户按下这些键中的一个时，振荡器发送两个同步音调。数字由一定的频率组合来代表。一个是低频（697、770、852、941Hz），另一个是高频（1 290Hz、1 336Hz、1 447Hz、1 633Hz）。共有 16 种组合，但只有其中的 12 种被应用到键盘上。

3.1.4 回路启动和接地启动信令

两个最通用的回路终端信令（end loop signaling）方式是回路启动和接地启动信令（Loop Start and Ground-Start Signaling）。

- 回路启动信令（Loop Start Signaling）是两种信令协议中最简单的也是最不智能的。但也是用户回路信令中最常用的。这个协议基本工作在电话和本地终端局，建立一个回路来发起呼叫，关闭一个回路来终止呼叫。回路启动信令不被用于 PBX 信令，而且它有一个致命的缺点，那就是可能会产生双占用。当两个端点同时试图抢占线路时，双占用就会产生。经常会将两个互不相关的用户连接起来。当用户拿起电话应当听到拨号音时，没有意识到他被连接到了一个呼叫他的电话上。
- 接地启动信令（Ground Start Signaling）——与回路启动不同，该协议提供正确的连接断开信息。电流监测机制被用于每条中继线的末端，使端局交换机中继被占用前就抢占哪端达成一致。与回路启动信令费用相同，但此种信令将双占用的可能性降到了最低。所以，它被用作 PBX 间的信令方式。

3.1.5 CAS 与 CCS

CAS 存在于许多网络中。CAS 系统在中继系统内承载中继信令信息。CAS 系统最早是由不同的设备提供商开发的，所以也就存在着多种版本。当今的通信网络需要更有效的信令方式，所以他们正在逐步采用公共信道系统，如 CCS。

CCS 采用一条公共的信道为一组中继线承载信令信息。与 CAS 相比，CCX 更经济且快速连接。SS6 是第一代 CCS，SS7 是第二代，我们将在第 4 章介绍。

3.2 E&M 信令

E&M 是一个用于电话交换机和 PBX 上的通用中继信令技术。E&M 中的信令和语音中继是分开的。在 E&M 语音使用 6 种信令方式在 2 或 4 条线路上传输。E&M 信令方式为 I、II、III、IV 和 V 类信令，以及英国电信标准——SSDC5。

本小节后面的部分我们将集中在 4 线 E&M 类 I 到 V。表 3-1 总结了 E&M 类 I 到类 V

的摘机与挂机接线方式。

表 3-1 E & M 信令

类型	M 导线		E 导线	
	摘机	挂机	摘机	挂机
I	电池	接地	接地	开放
II	电池	开放	接地	开放
III	回路电流	接地	接地	开放
IV	接地	开放	接地	开放
V	接地	开放	接地	开放

3.2.1 I 类

如图 3-1 所示，使用 I 类接口，中继设备通过将 E 线接地产生一个 E 信号。PBX 通过电阻性负载探测到电流的增加来探测 E 信号。同理，PBX 通过向中继设备发起一个电流产生 M 信号，中继设备也是通过电阻性负载来探测这个信号。RJ-48c 连接器的 7、2、6、3 针被使用。

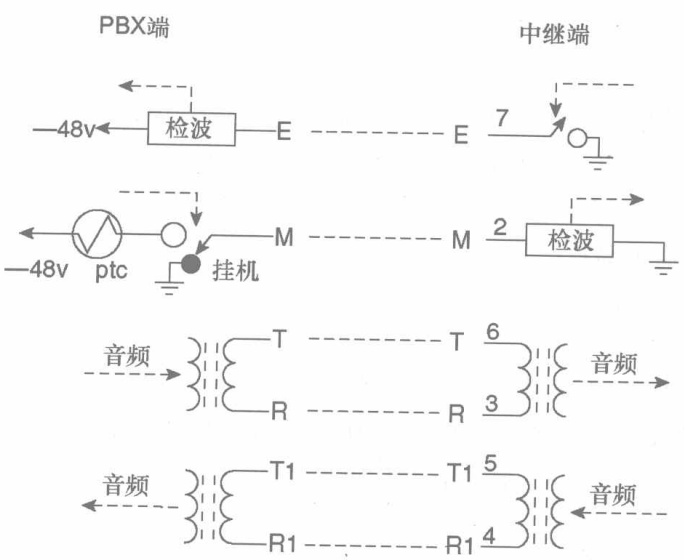


图 3-1 E&M I 类

3.2.2 II 类

E&M II 类比 I 类多使用两条导线：电池信号（signal battery，SB）和接地信号（signal ground，SG）。在这种方式下，E 导线与 SG 导线配对，M 导线与 SB 导线配对。当 E 与 M 导线断开的时候，PBX 端知道挂机了。当 E 线被接地，M 线接电池的时候，就意味着摘机

了（见图 3-2）。

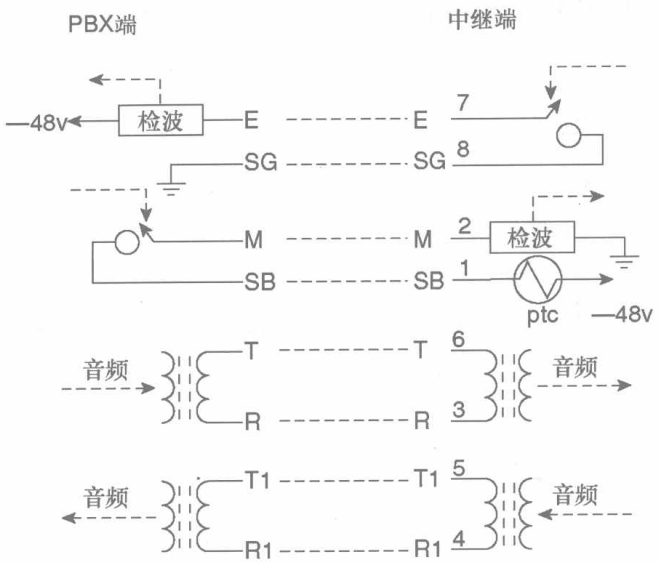


图 3-2 E&M II 类

3.2.3 III 类

在老的电话交换中心，通常会使用 E&M III 类。图 3-3 显示了 III 类的建立。

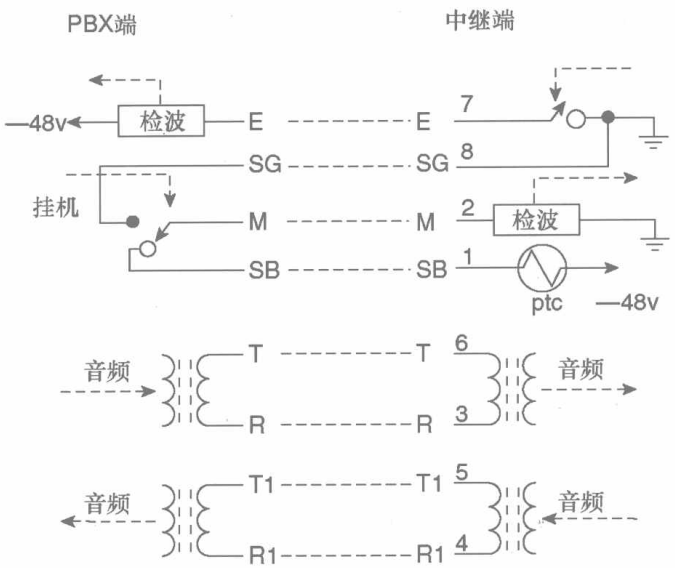


图 3-3 E&M III 类

3.2.4 IV类

E&M IV类与II类类似，但对于PBX侧，当E和M导线断开时挂机，当两条线都接地时摘机。

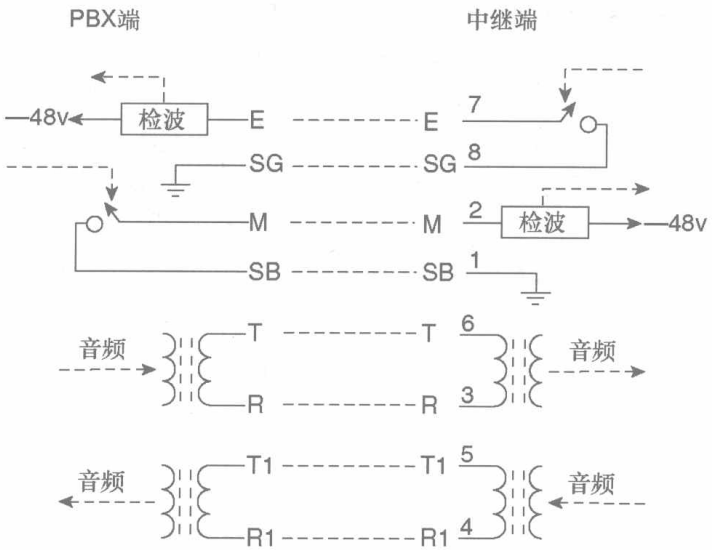


图 3-4 E&M IV类

3.2.5 V类

在E&M V类下，PBX和交换机终端都是用电池（见图3-5）。在PBX端，电池接到E导线；在终端交换机端，电池接到M线。类V是北美以外地区的最常用的E&M信令。

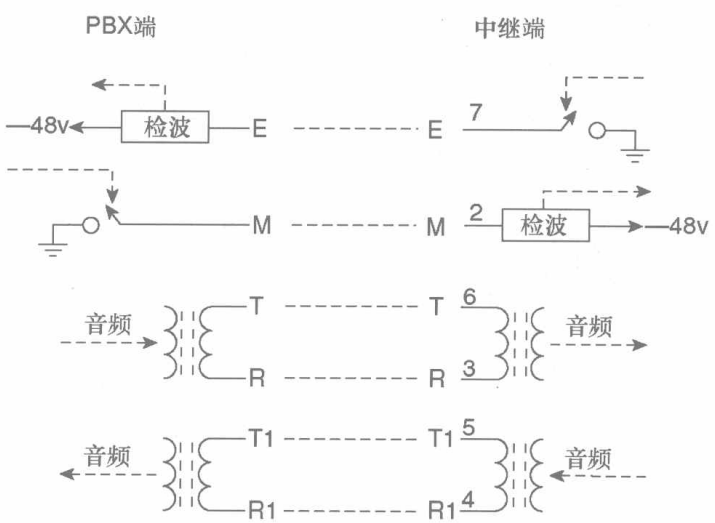


图 3-5 E&M V类

3.3 CAS

CAS 有各种类型以对应各式各样的模拟和数字设备。模拟设备是两或四线的，数字设备是北美的 T1 或欧洲的 E1。本小节讨论贝尔系统 MF，CCITT 的 No.5、R1 与 R2 CAS 系统。

我们讨论 CAS 系统的主要领域在于模拟与数字链路上的监管信令与寻址信令。贝尔系统为寻址信令使用带内 MF。对于监管信令，在模拟线路上使用单频，在数字链路上使用 a/b 位。CCITT 的 No.5 是为模拟中继线路设计的，为监管与寻址信令使用不同的 MF 信号。带内音频监测被用来探测与解释 MF 信号。

在继续讨论 CAS 系统之前，我们有必要先讨论以下几点。当一个呼叫发生在交换机 A 与交换机 B 之间时，交换机 A 认为是呼出交换，交换机 B 认为是呼入交换。

单向中继是指在该中继上，只用交换机 A 或交换机 B 就可以发起呼叫。交换机 A 与 B 可以在双向中继上发起呼叫。当两个交换机同时试图抢占双向线路时，双抢占放生了。当双抢占发生时，可以使用计时器等机制来探测和解决这个问题。

在随路互控信令系统中，主要有如下 3 种信号。

- 监管信号——这些信号用于表示中继上发生的事件，可以为不同的 CAS 定义。这些信号包括抢占、闪烁和应答，通常也被称作线路信号。
- 地址信号——这些信号通常表示拨叫的数字或者对方的号码。以及在某些情况下的其他信息。在本章，地址信号是基于 MF 信令的，可以被系统重新定义。
- 音调与提示——这些包括振铃声，忙音调和诸如“您拨打的号码已经取消”的提示。

另一个我们必须提到的概念是服务线路。服务线路（Service circuits）在大多数交换机中用于发送、接收地址信号和音频，同时也提供提示。这些线路是系统相关的，处理器连接从中继到交换机内的服务线路而形成一条路径。服务线路池被临时用作发送和接收音调或者广播提示。

3.3.1 贝尔系统 MF 信令

本小节介绍 20 世纪 50 年代由贝尔系统开发的 MF 信令系统。美国的本地网络仍使用贝尔系统。贝尔系统与本章后面要介绍的 R1 信令系统几乎一样。

使用贝尔系统 MF 信令，可以使用单向或双向中继线，监管和地址信令被一条链路一条链路地传送。对于模拟设备，监管信令与一个单频音调一起传送，而在数字设备上则通过强取比特信令传送。地址信息则通过 MF 音调传送。

1. 监管信令

监管信令被终端交换机连续传送，用于指明中继线的状态。这被称为*连续双状态信令（continuous two-state signaling）*。每个中继的终端的状态可能是不一样的。如表 3-2 所示，

MF 信令被用来指明摘挂机状态。

表 3-2 监 管 信 号

方向	信号类型	转换
前向	抢占	挂机到摘机
前向	前向拆除	摘机到挂机
后向	应答	挂机到摘机
后向	后向拆除	摘机到挂机
后向	请发码（闪烁）	摘机脉冲 120～290ms

对于模拟和数字中继，监管信令的操作有些不同。

2. 模拟中继

一个 2 600Hz 的单频音调被用来指示模拟设施上的交换设备之间的中继状态。这个音调在中继线上带内传送，当呼叫正在处理或建立后，此音调被关闭。这样，当摘机或空闲时，此音调出现；挂机或正在使用时，此音调消失。图 3-6 展示了单频方式下的监管信令。

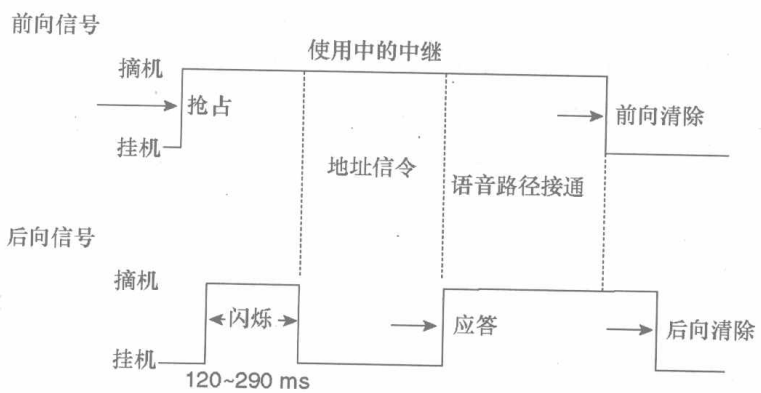


图 3-6 一个呼叫的前向与后向信号

在图 3-6 中假设交换机 A 发送前向信号，交换机 B 发送反向信号。在一条中继上，交换机 A 向交换机 B 发送一个抢占或摘机信号给交换机 B。接到该信号后，交换机 B 发送一个后向闪烁或请发码信号（proceed-to-send）给交换机 A，交换机 B 等待地址信令或拨叫的数字。在数字被发送且呼叫被应答后，交换机 B 发送一个后向应答或摘机信号给交换机 A，这样就形成了一条端对端的语音路径。

在这种情况下，如果呼叫方先挂机，前向拆线信号由交换机 A 发送给交换机 B。如果被叫方先挂机，那么交换机 B 发送一个后向拆线信号。

我们需要讨论这种信令的以下两个方面。

- 首先，贝尔系统 MF 没有连接失败的后向信令。所以，当呼叫失败时，交换机必须连接一个通告服务器来通知呼叫方不能连接。

这时，信令系统只能依靠呼叫方挂断或放弃电话来发起前向拆线信号。

- 另外，没有释放监视类的信号存在，所以当中继被释放后，计时器被使用。这样，当一个交换机释放了一个中继时，它启动一个大概 1 秒钟计时器。当计时器失效时，交换机认为中继的另一端被释放，该中继可以使用。

3. 数字中继

目前最常用的数字中继是 T1 或 E1 线路（该部分将在 4.2.1 小节介绍）。使用数字中继，将从特定帧中强取位用于信令传送。这里主要就 T1 数字中继进行讨论。

T1 有两种帧格式：超帧（Super Frame，SF）与扩展的超帧（Extended Superframe，ESF）。最不重要的位被从 SF 的帧 6 和 12 中，或 ESF 的帧 6、12、18 和 24 中强取出来。这些位在 SF 中被称做 Sa 和 Sb 位，在 ESF 中被称做 Sa，Sb，Sc 和 Sd 位。强取这些位对语音质量几乎没有影响。

ST 信令位——Sa 与 Sb——彼此相等，都提供双状态的连续监管信令。位值为 0 表明挂机，为 1 表明摘机。

4. 地址信令

地址信令用于表明拨叫双方的电话号码以及地址信息的开始与结束。如表 3-3 所示，贝尔系统 MF 方式中，地址信令由六种音频的两个组合表示。

表 3-3　　贝尔系统 Mf 地址信号

信号	频率（Hz）
数字 1	700 和 900
数字 2	700 和 1 100
数字 3	900 和 1 100
数字 4	700 和 1 300
数字 5	900 和 1 300
数字 6	1 100 和 1 300
数字 7	700 和 1 500
数字 8	900 和 1 500
数字 9	1 100 和 1 500
数字 0	1 300 和 1 500
KP（开始）	1 100 和 1 700
ST（结束）	1 500 和 1 700

地址信令序列开始于一个 KP 或开始脉冲（start-of-pulsing）信号，终止于一个 ST 或结束脉冲（end-of-pulsing）信号。这里有两种重要的时间间隔。

KP 信号间隔为 90～100ms，ST 信号的时间间隔为 61～75ms。信号之间的间隔也是 61～75ms。图 3-7 演示了监管和地址信令序列。

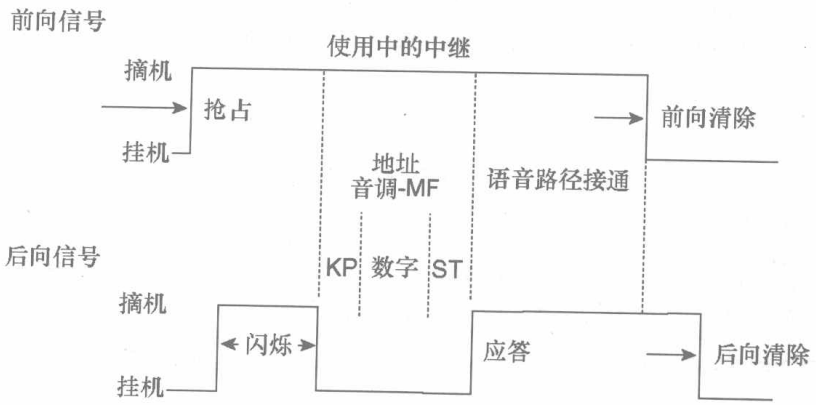


图 3-7 监管和地址信令序列

地址信令使用两个其他重要的信息数字。这个信息编码（或 I 位）表明了呼叫号码或 Automatic Number ID（ANI），以及接线员服务，如表 3-4 所示。

表 3-4 地址信令编码（Address Signaling Codes）

I-代码	信息
I = 00	呼叫号码有效
I = 02	呼叫号码无效
I = 06	需要房间号
I = 10	测试呼叫

信息编码在 KP 信号后，呼叫方号码之前发送。I 编码 02 和 06 表明这些呼叫需要接线员的干预才能完成。

3.3.2 CCITT No.5 信令

CCITT 在 20 世纪 60 年代为国际网络采用了 CCITT No.5 信令系统。这套信令系统目前仍在使用，多被使用在国际中继线路上以及某些海底电缆和卫星链路上。这套信令系统是设计在装备了时间分配话音插空（Time Assignment Speech Interpolation，TASI）模拟中继线路上的。TASI 与话音激活检测（voice activity detection，VAD）相似，它允许其他电话交谈可以使用未被使用的带宽（无声或声音的间断）。监管和地址信令都使用一段链路一段链路和带内信令传送方式。

1. 监管信令

监管信令由分别或组合发送的两个频率构成。CCITT No.5 使用强制监管信令，在确认

收到前，信令音调将一直保留。

这两个带内频率是$f1$（2 400Hz）和$f2$（2 600Hz）。$f1$与$f2$的组合形成一个组合信号，这些信号和频率如表 3-5 所示。

表 3-5 CCITT No.5 监管信号

方向	信号类型	频率
前向	抢占	$f1$
后向	请发码继续发送（闪烁）	$f2$
后向	应答	$f1$
前向	确认	$f1$
后向	后向拆除	$f2$
前向	确认	$f1$
前向	前向拆除	$F1$ 和 $f2$
后向	释放监护	$F1$ 和 $f2$
后向	示忙-闪烁	$f2$
前向	确认	$f1$
前向	前向-转移	$f2$

表 3-5 介绍了三种新信号：释放监护（Release-guard）、示忙闪烁（Busy-flash）和前向转移（Forward-transfer）。

- 释放监护（Release-guard）——这个信号被呼入交换机用来确认来自呼出交换机的前向拆线信号。它同时也通知呼出交换机呼入呼叫占用的中继空闲。
- 示忙闪烁——呼入交换机使用这个信号通知呼出交换机呼叫不能建立。
- 前向转移（Forward-transfer）——此信号用于需要接线员服务的呼叫。

2. 地址信令

在 CCITT No.5 中，如表 3-6 所示，地址信令基于两个频率的组合。国内号码的地址信令序列以 KP1 开始，国际的以 KP2 开始。编码 11 和 12 被用在国际接线员服务。

表 3-6 CCITT No.5 地址信号

信号	频率（Hz）
数字 1	700 和 900
数字 2	700 和 1 100
数字 3	900 和 1 100
数字 4	700 和 1 300
数字 5	900 和 1 300

续表

信号	频率（Hz）
数字 6	1 100 和 1 300
数字 7	700 和 1 500
数字 8	900 和 1 500
数字 9	1 100 和 1 500
数字 0	1 300 和 1 500
代码 11	700 和 1 700
代码 12	900 和 1 700
KP1	1 100 和 1 700
KP2	1 300 和 1 700
ST	1 500 和 1 700

3.3.3 R1

被称为 R1 的 CAS 系统定义在 ITU-T 的 Q.310～Q.332 规范中。这个信令系统几乎和贝尔系统 MF 信令一样，所以在这里我们不再介绍。

3.3.4 R2

R2 是 20 世纪 60 年代开发的 CAS 信令，目前仍在欧洲、拉丁美洲、澳大利亚和亚洲使用。R2 最初被称为多频码（multi-frequency code，MFC）信令，有许多国家版本，其中的国际版本为 CCITT-R2。

R2 信令可以操作两线或四线模拟中继和数字中继，不能操作在装有 TASI 的中继和卫星链路上。R2 信令对于相对较短的国际中继更为合适。与 R1 相比，它们的不同之处在于它的寄存器或寄存器间的信令。

本小节主要集中在 CCITT-R2 与国家 R2 信令系统的监管和寄存器间信令。

1. 模拟中继上的监管信令

本节基于四线中继上的操作来介绍模拟中继上的监管信令。传输路径被分为两个部分一个 300～3400Hz 的语音带和一个 3825Hz 的信令窄带。在这种方式下，过滤器将信令音调从语音路径上分离出来。虽然信令是在同样的设备上传输的，但也被认为是带外信令。

CCITT-R2 采用音调空闲（tone-on-idle signaling）信令监管方式，国家 R2 采用脉冲信令（pulse signaling）。

2. CCITT-R2

这种方式一般用在单向中继，是音调空闲的，提供双状态信令。如表 3-7 所示，前向、后向信令以及传送状态与贝尔系统相像。

表 3-7 CCITT-R2 监管信号

方向	信号类型	转换
前向	抢占	有音调到无音调
前向	前向拆除	无音调到有音调
后向	应答	有音调到无音调
后向	后向拆除	无音调到有音调
后向	释放监护	无音调到有音调
后向	阻塞（Blocking）	有音调到无音调

3. 国家 R2

国家 R2 有许多版本。但大多数版本的国家 R2 采用脉冲带外监管信令。表 3-8 列出了一些国家监管信令的例子。

表 3-8 国家 R2 监管信号举例

方向	信号类型	脉冲间隔（ms）
前向	抢占	150
前向	前向拆除	600
后向	应答	150
后向	后向拆除	600
后向	释放监护	600
后向	阻塞（Blocking）	继续

4. 数字中继上的监管信令

R2 信令操作在 E1 数字线路上（将在 4.2.1 小节介绍）。E1 有编码为 TS0 到 TS31 的 32 个时间槽，其中 TS1～TS15、TS17～TS31 用于承载脉码调制（pulse code modulation，PCM）的语音编码或者承载 64kbit/s 数据。

编码为 0～15 的 16 个连续帧采用 SF 格式。帧 0 中的 TS16 被用于 SF 对列，在剩余帧中的 TS16 被用于中继信令。TS16 中的四个状态被用于信令，它们是 a、b、c 和 d。

在 CCITT-R2 信令中，只有 a 和 b 为被使用。c 和 d 位被分别设为 0 和 1。当 a 和 b 等于 0 或 1 时，指示了空闲状态。信令是连续的。在双向链路上，前向和后向的监管角色随着呼叫的改变而改变。表 3-9 列出了数字中继上使用的 R2 监管信令、转换和方向。

表 3-9 数字中继上的 R2 监管信令

方向	信号类型	转换
前向	抢占	a，b：1，0 到 0，0
前向	前向拆除	a，b：0，0 到 1，0

续表

方向	信号类型	转换
后向	抢占确认	a，b：1，0到1，1
后向	应答	a，b：1，1到0，1
后向	后向拆除a	a，b：0，1到1，1
后向	释放警卫	a，b：0，1到1，0

5．寄存器间信令

R2中地址信令的概念与我们刚讨论的CAS系统中的有一些不同。在R2中，交换机可以考虑为寄存器，那么交换机之间的信令被称做寄存器间信令。寄存器间信令（Inter register signaling）使用前向后向带内MF信号传输呼叫双方的号码和呼叫方分类。

在这种情况下，因为呼入呼出交换机中的寄存器保留信号直至收到确认，所以信令是被迫的。信号由如表3-10所列的两个语音带频率表示。

表3-10 CCITT-R2与国家R2寄存器间信号频率

信号	前向频率（Hz）	后向频率（Hz）
数字1	1 380和1 500	1 140和1 020
数字2	1 380和1 620	1 140和900
数字3	1 500和1 620	1 020和900
数字4	1 380和1 740	1 140和780
数字5	1 500和1 740	1 020和780
数字6	1 620和1 740	900和780
数字7	1 380和1 860	1 140和660
数字8	1 500和1 860	1 020和660
数字9	1 620和1 860	900和660
数字0	1 740和1 860	780和660
没有使用	1 380和1 980	1 140和540
没有使用	1 500和1 980	1 020和540
没有使用	1 620和1 980	900和540
没有使用	1 740和1 980	780和540
结束#	1 860和1 980	660和540

6．寄存器间信令分组

在R2信令中，因为使用组别的不同，前向和后向信号有不同的意义。有3组前向信号和两组后向信号。前向组分别为I、II与III，后向组为A与B。

- 组 I——前向信号通常表示拨叫的数字或者被叫方的号码。
- 组 II——前向信号表明呼叫方分类。
- 组 III——前向信号表明呼叫方号码的数字。
- 组 A——后向信号表明信令结束或者需要特定的前向信号。
- 组 B——后向信号被终端交换机发送以确认一个前向信号或者提供呼叫计费和被叫方的信息。

使用如下寄存器间信令组顺序规则来区别信号所属的组。

- 呼入交换机发起的初始信号属于组 I。
- 呼出交换机认为后向信号为组 A 信号。
- 呼出交换机接收到的组 A 信号被用来确定下一个信号为组 B 信号。
- 组 B 信号总是被用来指明信令结束。

7. 功能支持

国家 R2 信令提供的端对端信息以及状态可以支持许多功能。这些功能包括免费电话（free calls），被叫方保持（called party hold），恶意电话跟踪（malicious call tracing）和失败连接释放（release on failed connections）。

3.4 ISDN

ISDN 从 20 世纪 80 年代开始公开生效。国际电信联盟（International Telecommunication Union，ITU，前身为 CCITT）I 系列建议书定义了 ISDN 的国际标准。这个基于用户接口的协议为用户提供多种服务的单一接入。

ISDN 信令与 SS7 兼容，可以与 ISDN 用户部分（ISDN User Part，ISUP）协议协同工作。协同工作使 ISDN 用户可以访问他们在 SS7 网络上同样的服务和信息。ISDN 也允许 PBX 通过 PSTN 连接和建立 VPN。这是通过将 PBX 信令通过网络传送给远端 PBX 实现的。

ISDN 序列定义了到网络的接入。下面列出了一些 ISDN 的功能和能力。

- ISDN 为用户提供基于电路的（语音和数据）通信和分组交换通信。
- 许多新的服务可以提供给用户。
- ISDN 包括 2 种接入方式：基本速率接口（Basic Rate Interface，BRI）和基群速率接口（Primary Rate Interface，PRI）。
- ISDN 包含到 PSTN 的单一接入、直接向内拨号（Direct-Inward-Dial，DID）、直接向外拨号（Direct-Outward-Dial，DOD）、800、外部交换机（Foreign Exchange，FX）、直达线路、分组交换数据、电路交换数据和专线数据。
- ISDN 可以为高速数据通信提供附加信道。
- ISDN 可以在同一链路上传输语音和数据。
- ISDN 为信令使用分离信道。

- ISDN 信令与 SS7 兼容。
- ISDN 可以创建 VPN。

3.4.1 ISDN 业务

在电路交换 ISDN 网络中，可以提供如下通信业务。

- 承载业务（Bearer Services）——有三种类型的承载业务：话音、3.1kHz 音频（调制解调器数据）和 64kbit/s 数字数据。
  呼叫用户在呼叫建立（setup）消息中确定承载业务类型，然后通过网络传送给被叫用户。网络中的交换机使用这些信息来选择中继。对于语音，交换机可以使用模拟或者数字中继互联，而 64kbit/s 数字数据则需要数字中继。
- 电信业务（Teleservice）——呼叫方使用这项服务确定数据业务类型是 3.1kHz 音频还是 64kbit/s 数字数据。电信业务信息（传真、电报等）通过网络透明传送给被叫方。被叫方处理这些信息，选择合适的终端设备了终结呼入呼叫。
- 附加业务——ISDN 可以提供多种附加业务。这些业务通常也可以在 PBX 和虚拟专用语音网络中找到。以下是一些附加业务的例子：来电显示、闭合用户群、呼叫等待、用户间信令、计费通知（advice of charge）、呼叫转移和呼叫保持。当用户请求这些服务时，附加业务消息被发送给网络以调用请求过程。对于用户间信令，两个 ISDN 用户在呼叫建立和拆除部分透明传输信令信息。

3.4.2 ISDN 接入接口

在讨论 ISDN 接入方式之前，有必要先介绍一下 B 和 D 信道概念。

- B 信道——B 信道是用于承载用户信息流的一条 64kbit/s 信道。B 信道不承载信令信息。B 信道的用户流量包括根据 ITU G.711 编码的 64kbit/s 的话音，64kbit/s 或少于 64kbit/s 的数据以及以更低的速率编码的声音。
- D 信道——D 信道主要用于为 ISDN 网络电路交换承载信令。根据接入方式的不同，D 信道速率不同。D 信道也可以传输高达 9.6kbit/s 的分组数据。

ISDN 有 BRI 和 PRI 两种接入模式。

1. BRI

BRI 在标准的两线电话线上提供两条双向 64kbit/s 的 B 信道和一条双向 16kbit/s 的 D 信道。基本速率 ISDN 业务一般被住宅用户、小企业及家庭办公（SOHO）应用使用。每个 B 信道都可以传输话音和数据。D 信道传输信令和呼叫控制消息。

图 3-8 定义了 BRI 的配置和参照点。

ISDN 的参考配置定义在 ITU 规范 I.411。参照点（reference point）明确定义了传输媒体、接口和连接器（如果使用的话）。

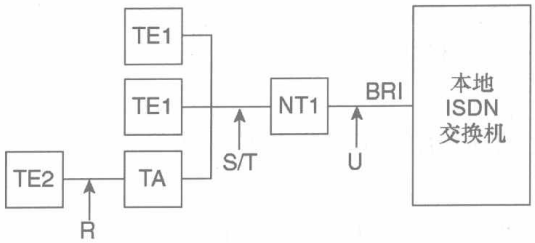


图 3-8 ISDN BRI 参照点

- U 参考点——U 参考点定义了本地回路的传输特性。在 BRI 中，这个两线接口在标准的铜芯双绞线上在 160kbit/s（2B+D+16kbit/s 其他开销）速率上操作。
- S/T 参照点——对于基本速率接入，这个接口为 ISDN 兼容的终端或终端适配器提供四线连接。这个接口在 ISDN 设备与网络中介设备间操作在 144kbit/s（2B+D）速率上。您最多可以在 S/T 接口上连接 8 个 ISDN 设备。
- R 参照点——R 参照点为非 ISDN 设备提供连接。这些设备通过如 RS-232 和 V.35 接口与中断适配器连接。

这个参考配置同时也定义了一系列接入 ISDN 网络所需的功能。

— 网络终端 1（Network Termination 1，NT1）——在非北美的地区，NT1 位于用户网络接口的网络端，被认为是服务供应商网络的一部分。NT1 终结两线本地回路，为 ISDN 终端设备（terminal equipment，TE）提供四线 S/T 总线。

— TE1——TE1 是直接连接在 NT1 上的 S/T 连接器的 ISDN 兼容设备。

— TE2——TE2 是非 ISDN 兼容设备，需要终端适配器（terminal adapter，TA）互联。

— TA——TA 为 NT1 提供 ISDN 兼容接口，为 TE2 提供标准接口。这些标准接口包括 RS-232、V.35、RS-449 和 X.21。

2. PRI

PRI 对应两种主要速率：1.544 Mbit/s（T1）与 2.048 Mbit/s（E1）。PRI 通常是用在中大型企业应用。PRI 由若干条 B 信道和一条 D 信道组成。T1 的接口结构是 23B+D（北美和日本），T1 的接口结构是 30B+D（欧洲）。

图 3-9 定义了 PRI 的配置和参照点。

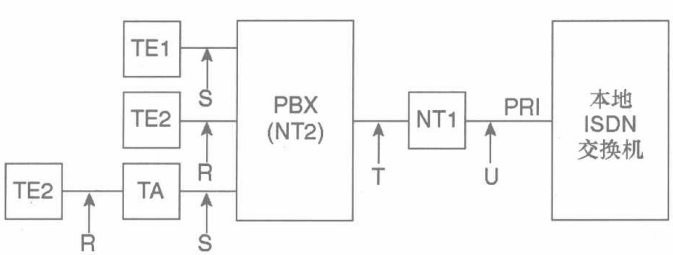


图 3-9 ISDN PRI 参照点

PRI 的配置和参照点与 BRI 相似。这两种参考模型的区别如下。

- U 参照点——对于 PRI，U 接口是操作在 T1（1.544 Mbit/s）或 E1（2.048 Mbit/s）上的四线接口。
- T 参照点——对于 PRI，T 接口提供到网络终端 2（Network Termination 2，NT2）设备的接入。
- NT2——PBX 设备可以提供层 2（L2）和层 3（L3）NT2 功能以及多路复用、交换、接口终结和维护。NT2 也可以提供到 ISDN 兼容 TE1 和非 ISDN 兼容 TE2 的连接。

3.4.3 ISDN L2 和 L3 协议

ISDN 用户网络接口 L2 和 L3 规范也被称作 1 号数字用户信令系统（Digital Subscriber Signaling System No. 1，DSS1）。L2 通过 ISDN 参考配置为两个终端点提供无错误的安全连接。L3 提供呼叫建立、控制和业务接入等机制。ISDN 的 L2 协议是 Q.920/921，L3 协议是 Q.930/931。Q.932 定义接入和控制附加服务的通用过程。

L2 规范被称为 D 信道上的链路接入协议（Link Access Procedures on the D channel，LAPD）。这个协议在本地交换机与 TE 之间提供可靠的帧传输。Q.920 与 Q.921 规范是可拓展的，可以从 ITU 的 Q 系列建议书中获得。

L3 规范定义了在本地交换机和 TE 间的消息。这些消息被用作呼叫建立、呼叫监管、呼叫断开和附加服务。下一小节讨论 ISDN 消息的细节。

Q.931 呼叫控制消息（Q.931 Call Control Messages）

ISDN 网络使用 Q.931 消息结构和信令元素提供呼叫控制能力。Q.931 在用户和网络之间传送。他们被称作用户网络和网络用户消息，如表 3-11 与表 3-12 所示。

表 3-11 列出了一些最重要的 Q.931 消息。Q.931 普通格式消息中的消息类型域被用于标识被传送消息的类型。

表 3-11 Q.931 消息和类型代码

Q.931 消息类型	消息类型值
建立消息（SETUP）	00000101
建立确认消息（SETACK）	00001101
呼叫处理消息（CALPRC）	00000010
进行消息（PROG）	00001111
警示消息（ALERT）	00000011
连接消息（CONN）	00000101
连接确认消息（CONACK）	00000111
断开消息（DISC）	01000101

续表

Q.931 消息类型	消息类型值
释放消息（RLSE）	01001101
释放完成消息（RLCOM）	01011010
信息消息（INFO）	01111011

来源：ITU-T Q.931（3/93）

表 3-12 列出了每个消息类型的信息或信令元素。表 3-12 也指出了每个网络到用户消息必需的（M）或可选的（O）域。

表 3-12　　Q. 931 中用户到网络的信息元素

信息元素	SETUP	CALPC	ALERT	CONN	CONAK	DISC	RLSE	RLCOM	INFO
承载能力	M								
被叫方号码	M								
主叫方号码	O								
被叫方子地址	O								
主叫方子地址	O								
原因						M	O	O	
信道签订	O	M	O	O					
高层兼容性	O								
键盘	O								M
低层兼容性	O								
经过网络选择	O								
用户到用户信息	O		O	O		O	O	O	

表 3-13 明确指出了每个网络到用户消息的必需（M）和可选（O）域。

表 3-13 Q.931 中网络到用户的信息元素

信令元素	SETUP SETACK CALPC			PROG	ALET	CONN CONAK DISC			RLSE	RLCOM INFO	
承载能力	M										
被叫方号码	M										
主叫方号码	O										
被叫方子地址	O										
主叫方子地址	O										
原因				O				M	O	O	
信道签订	M	M	O								
高层兼容性	OO										
低层兼容性	O										
进展指示器	O	O		M	O	O					
信号	M	O		O	M	O	O	O	O	O	O
用户到用户信息	O	O			O			O	O	O	

3.4.4 基本 ISDN 呼叫

本小节大致描述一个在同一本地交换机上的两个用户之间的 ISDN 呼叫。图 3-10 显示了用户 A（TE-A）、本地交换机和用户 B（TE-B）之间的信令序列。

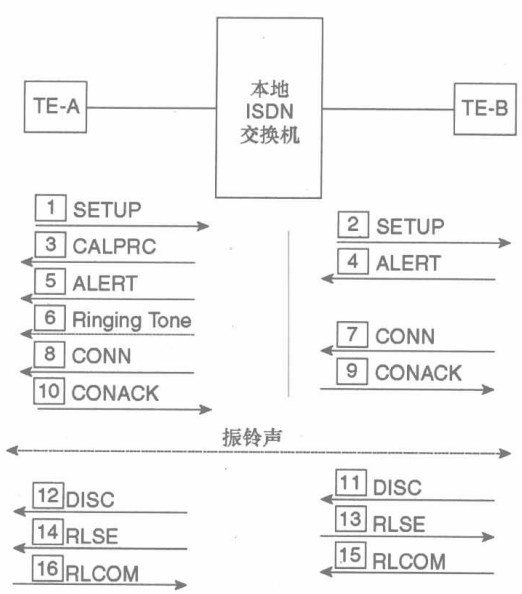


图 3-10 基本 ISDN 呼叫

1. 呼叫建立

TE-A 通过发送一个建立（SETUP）消息给 TE-B 发起一个呼叫。SETUP 消息含有全部的被叫方号码（也称作整体信号（en-bloc signal））本地交换机向 TEB 发送一个 SETUP 消息，该消息中包含 B 信道分配。

注释：当拨叫的号码被一位一位地在分别消息中传送时，会造成信令重叠。

这时，本地交换机向 TE-A 发送一个 CALPRC 消息通知呼叫建立开始。如果 TE-B 接受呼入呼叫，则返回一个 ALERT 消息。本地交换机则发送一个 ALERT 给 TE-A，如果是一个话音呼叫，那么在 B 信道上振铃。

当 TE-B 回答呼叫时，一个 CONN 消息被发送给 B 信道连接的交换机，也会向 TE-A 发送一个 CONN 消息。本地交换机使用一个 CONACK 来确认 TE-B 的 CONN，TE-A 也可以使用 CONACK 确认 CONN。

2. 呼叫断开

我们下面讨论 TE-B 首先断开连接的情况。TE-B 发送一个 DISC，然后本地交换机发送一个 DISC 到 TE-A。

这时，本地交换机清除到 TE-B 的 B 信道并且发送一个 RLSE 消息给 TE-B。紧接着，TE-B 释放终端点的 B 信道并且发送一个 RLCOM 消息。同样的释放过程也发生在 TE-A 和本地交换机之间。

3.5 QSIG

QSIG 是语音组网中的点对点（peer to peer）信令系统。QSIE 在国际上称为私有信令系统 No.1（Private Signaling System No. 1，PSS1）。这是一个基于 ITU-T Q.9XX 系列建议书的基本业务和附加业务的开放标准。所以，QSIG 处理提供 PBX 间的通信外，也与公共和专用的 ISDN 相兼容。

QSIG 有一个被称为通用功能过程（Generic Functional Procedures，QSIG GF）的重要机制，这个机制提供在网络上透明传输功能的标准方式。

下面是 QSIG 全球信令系统的一些特征。

- 它是一个允许多家厂商设备互联的基于标准的协议。
- 它允许 PBX 间的基本的、功能透明的和附加的业务。
- 它可以与公共的和专用的 ISDN 共同工作。
- 它可以在各种网络架构上操作（星型，网状等）且与多种 PBX 类型接口兼容。
- 它不给私有编码计划施加限制。

QSIG 是一个非常重要的信令系统。本节剩余部分将覆盖 QSIG 的以下几个方面：

- 服务；

- 体系架构和控制点；
- 协议栈；
- 基本呼叫建立和拆除。

3.5.1 QSIG 服务

QSIG 支持与 PBX 网络合作的一套服务和功能。三种主要的服务包括：基本服务、通用功能过程和附加服务。

- 基本服务（Basic service，QSIG BC）——这项服务提供基本的建立、管理和断开呼叫功能。与 ISDN 承载服务类似，基本服务包括话音，3.1kHz 音频和 64kbit/s 无限制。
- QSIG GF——这是一个传输非标准功能的标准方式，这样就可以提供功能透明。此机制可以在合作网络上交换附加网络功能的信令信息。
- 附加服务——此类服务包括服务和附加网络功能（ANF）。附加服务和 ANF 包括呼叫完成、呼叫转移、呼叫牵制（call diversion）、呼叫转接、呼叫等待、来电显示和计费通知。

3.5.2 QSIG 体系架构和参照点

将 ISDN 参考模型为合作网络扩展，使其包含有 PBX 到 PBX 信令是十分必要的。如图 3-11 所示，标准定义了“Q”和“C”两个参照点。

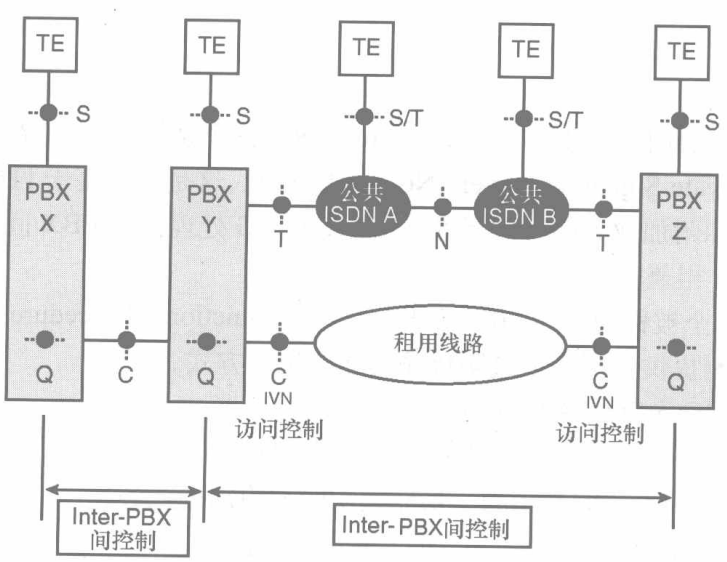


图 3-11 合作网络参考模型

Q 参照点定义了 PBX 间的逻辑信令，C 参照点定义了物理互联。一个合作网络可以拥有专线模拟或数字信道，或者拥有 VPN 交换连接，通常假设使用 T1 或 E1 数字接口连接网络。

QSIG 端对端信令被从 PBX 到 PBX 维护，并且 ISDN 与 ISUP 的合作对于 ISDN 网络上的端对端信令来讲是十分重要的。我们前面已经提到，QSIG 与 ISDN 兼容。图 3-11 列出了这些参照点。

T 参照点为 ISDN PRI 定义了到 NT2 的接入。C 参照点是 PBX 的物理互联点。该控制点与很多接口兼容，包括两线和四线模拟，BRI，PRI 以及广播和卫星链路。Q 参照点定义了两个 PBX 的逻辑信令点。这个参照点被用来定义信令系统以及相关协议。

3.5.3 QSIG 协议栈

QSIG 协议栈在参照点 Q 定义了一个信令系统，如表 3-14 所示。QSIG 有与 ISDN 一样的结构，在 L2 和 L3 协议是一样的。然而，在 L3，QSIG 将其分为如下两个子层。

- QSIG BC——这是一个用户和网络端的接口和消息都一样的对称协议。通过本节后面的例子，我们可以很容易理解这个协议的消息和序列。
- QSIG GF——这个协议为附加服务和 ANF 定义了控制实体。该协议没有控制这些服务的能力，但是它提供了能够允许这些服务的通用层能力。在不同的 PBX 的应用实体间，该协议提供了面向连接的无连接机制。
- QSIG 附加服务和 ANF 协议——这些协议定义了个别的或特定的服务和功能过程。这些服务和 ANF 分别定义在不同的规范中。欧洲计算机制造商协会（European Computer Manufacturers Association，ECMA）与 欧洲电信标准协会（European Telecommunication Standards Institute，ETSI）正在开发这些协议标准。

表 3-14 QSIG 协议栈

OSI 参考	QSIG 协议	QSIG 标准
L1	无	基于使用的接口
L2	无	等同于 ISDN L2（LAPD）
L3	QSIG BC	ECMA 142/143; ETS300* 171/172
	QSIG GF	ECMA 165; ETS300 239
	附加服务的 QSIG 协议	各单独规范，如呼叫转移（ECMA173/174，ETS300 256/257）和呼叫转接（ECMA177/178，ETS300 260/261）
L4–L7	基于应用的服务元素	对网络透明

*ETS300 是基于 ETSI 的标准

QSIG 基本呼叫建立和拆除示例

QSIG BC 协议提供呼叫建立和拆除的基本功能。这个协议扩展了 ISDN 接入协议以用于合作网络或私有 ISDN 中。QSIG BC 是一个用户端和网络端的接口和消息都一样的对称协议。图 3-12 演示了一个基本呼叫的消息序列。QSIG BC 消息与本章中讨论的“ISDN”消息很类似。

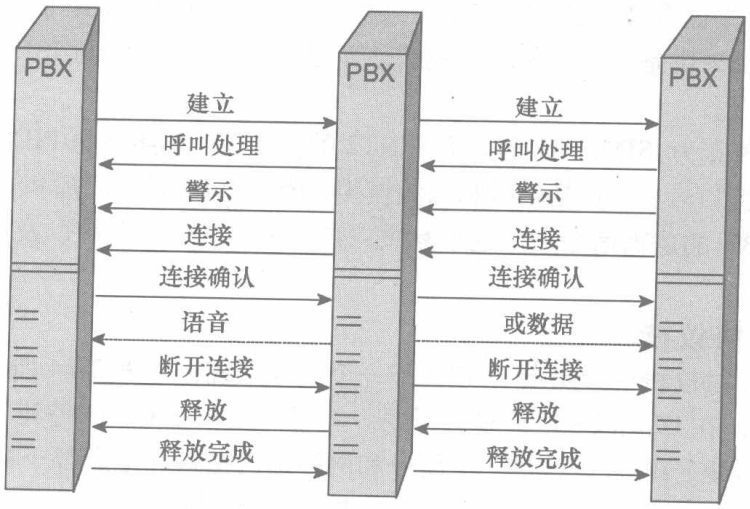


图 3-12 QSIG BC 消息序列

3.6 DPNSS

20 世纪 80 年代，BT 与一些 PBX 厂商一起开发了 DPNSS。他们在 ISDN 和 QSIG 标准正在定义时，为数字专用网络设计了这个开放标准。

DPNSS 拥有丰富的服务和功能集并且提供了 QSIG 协议的许多基础工作。DPNSS 与 QSIG 信令系统的互用性在两个协议中都作了定义。

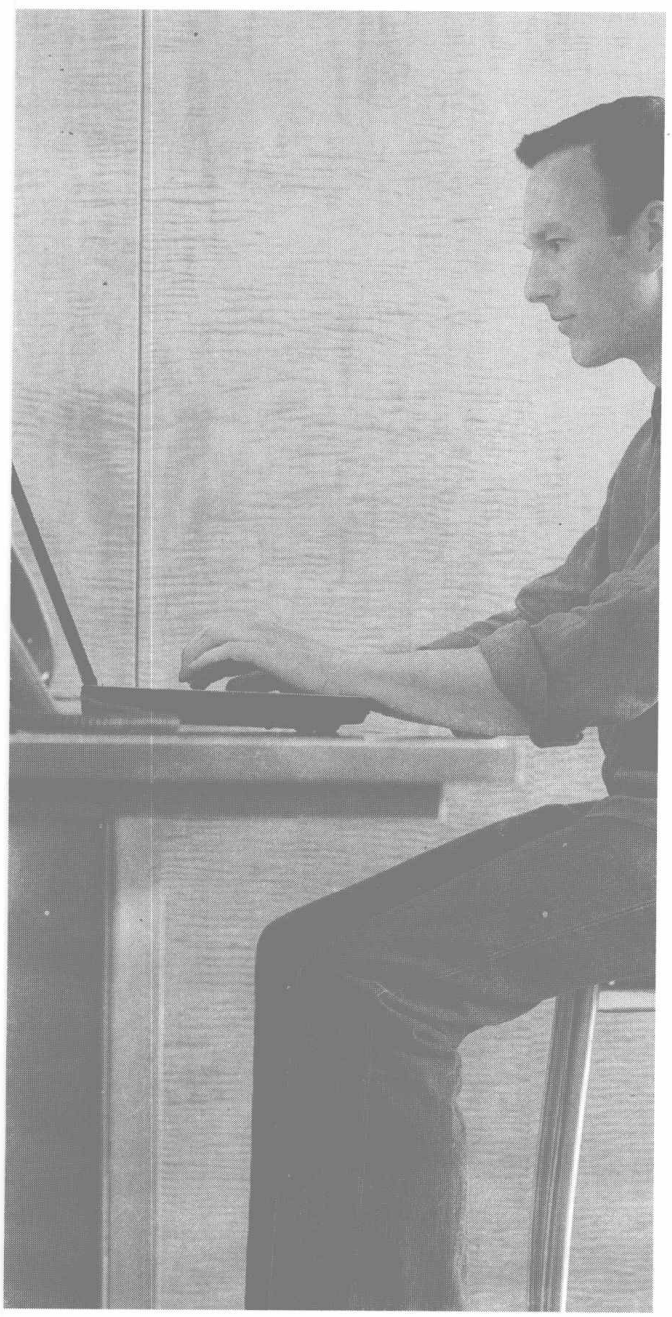
ISDN 和 QSIG 协议自从他们被开发以来，已经非常流行，但 DPNSS 在现在的私有网络上并没有被广泛使用。DPNSS 规范可以从 BT PLc 处获得，被定义在以下 4 个文件中。

- BTNR 188——DPNSS1。
- BTNR 188-T——DPNSS1 测试时间表（DPNSS1 testing schedule）。
- BTNR 189——DPNSS1 与其他信令系统的互联。
- BTNR 189-I——DPNSS1 与 ISDN 信令系统的互联。

3.7 总结

本章讨论的信令系统非常广泛且有多个版本。需要一定的时间才能使 VoIP 系统能全部支持这些协议和他们的各种版本。包括 Internet 工程任务组（Internet Engineering Task Force，IETF）在内的标准化组织正在起草使这些协议互通的建议书。

当这些标准被采纳实施后，电话信令系统与 VoIP 系统之间将相互合作“照常营业”。



本章讨论网络架构框架和设计模型，包含以下主题：

- 4.1 SS7 体系结构
- 4.2 SS7 协议概览
- 4.3 SS7 举例
- 4.4 SS7 规范
- 4.5 总结

第4章

7 号信令系统

*7 号信令系统（Signaling System 7，SS7）*是 20 世纪 70 年代后期由国际电信联盟电信标准化部门（International Telecommunication Union Telecommunication Standardization Sector，ITU-T）开发的一个公共信道信令标准。该部门的前身是国际电报电话咨询委员会（Consultative Committee for International Telegraph and Telephone，CCITT）。SS7 起源于 SS6。SS6 开发于 20 世纪 60 年代后期，是第一代公共信道信令。SS7 最早是为电话呼叫控制应用而设计的。自从它们被开发以来，SS7 应用已经有了巨大的扩展。目前 SS7 的功能包含了数据库查询、事务处理、网络操作和综合业务数据网络（Integrated Services Digital Network，ISDN）等。

SS7 网络为现有的 PSTN 网络提供智能应用。SS7 被用来执行 PSTN 网络中的带外信令。SS7 通过处理呼叫建立、信息互换、选路、记账和对智能网（Intelligent Network，IN）业务的支持来增强 PSTN。

在过去 VoIP 快速发展的 10 年里，SS7 协议对于分组语音网络（Voice over IP，VoIP）和 VoIP 与 PSTN 的互动起了非常重要的作用。当 VoIP 网络的用户需要连接已有的 PSTN 用户时，两个网络的转换点（网关）能无缝有效地连接两个网络是至关重要的。虽然将来所有的通信可能都会转移到 VoIP 网络上，但能够平稳过渡对于最终用户和运营商来讲都非常重要。

虽然 SS7 对于 VoIP 网络来讲，通常被认为是一个边缘技术，本章主要通过已有的经验来介绍 SS7 是怎样工作的。一旦清晰地理解了这个观点，就不难理解 SS7 是怎样被集成于 VoIP 网络的了。

SS7 的目的是提供一个电话网络信令的国际标准。但许多国家都开发了自己的标准，如北美使用的美国国家标准协会（American National Standards Institute，ANSI）与 Bell 通信研究室（Bell Communications Research，Bellcore）的标准，以及欧洲的欧洲电信标准协会（European Telecommunication Standards Institute，ETSI）标准。

本章主要从以下几个方面介绍 ITU-T 定义的 SS7 标准：

- SS7 网络元素与链路；
- SS7 协议组与消息；
- SS7 举例与呼叫流程。

4.1 SS7 体系结构

SS7 网络主要用来交换建立、管理、释放电话呼叫和维护信令网络的信息。装配了 SS7 功能的 SS7 网络节点成为 SS7 信令点或元素。SS7 是一种公共信道信令网络，所用的信令

信息都在一条公共的信令信道上传输。信令信道与语音线路是逻辑上分开的。

SS7 网络由三个信令点——业务交换点（Service Switching Point，SSP）、信令转接点（Signal Transfer Point，STP）和业务控制点（Service Control Point，SCP）——和它们之间的链路组成，如图 4-1 所示。本节覆盖了信令点和信令链路的主要内容。

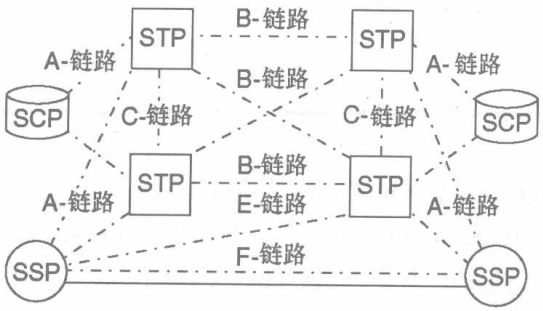


图 4-1 SS7 网络体系结构

4.1.1 信令元素

信令元素，通常也被称作信令点（signaling points）、端点（endpoints）、交换点（exchanges，switches）或节点（nodes），被用来分离语音网络与信令网络。在信令网中的每个信令元素都有一个编码来作为 SS7 中的路由地址。每个信令消息中都包含源和目的地的信令点编码地址。信令元素路由信令消息并提供到 SS7 网络和数据库的连接。

图 4-2 显示了 SS7 网络中的 3 种信令元素类型。

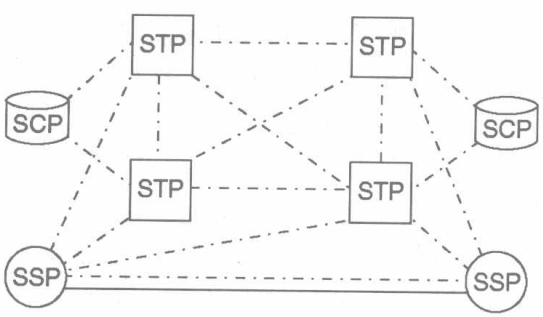


图 4-2 信令元素/点

- SSP 是用来连接语音电路，执行引起或终止呼叫所必要的信令功能的终端局或级联交换机。
- STP 路由 SS7 网络中的所有信令信息。
- SCP 提供到数据库的连接以获取在呼叫处理过程所需的附加路由信息。同时，SCP 是在电话网络中发布智能网（IN）应用的主要元素。

下面的各节将主要论述 SS7 网络中的这 3 个元素。

1. SSP

SSP 是提供 SS7 功能的电话交换机。终端局 SSP 发起和终止呼叫，中心网络交换机（core network switches）（STP）提供级联及转接呼叫。SSP 为其他 SSP 提供以连接、断开和管理语音呼叫为目的的基于电路的信令信息。当拨叫的号码不能完成呼叫时，非基于电路的消息被用于查询数据库。

终端局 SSP 直接与用户电话相连。使用的协议可以是模拟或数字的，这些协议可以基于 ISDN 的基群速率接口（Primary Rate Interface，PRI）或随路信令（channel associated switching，CAS）。终端局负责将用户的协议要求转换为 SS7 消息以建立呼叫。

如果用户拨打的号码不是 800、8xx、9xx 或本地电话可携带号码（Local Number Portability exchange）（或为 NXX 形式），SSP 使用拨打的号码来完成呼叫。如果是这些号码，那么就发送给 SCP 一个查询请求，来查找为完成呼叫所必需的路由信息（号码）。

我们用如下几步来更好地解释 SSP 为完成一个呼叫所使用的功能。我们假设源和目的的 SSP 如图 4-2 所示的那样是直接连接的。

① SSP 使用呼叫方所呼叫的号码，或者是从数据库中查到的路由号码建立电路连接信令消息。

② 然后 SSP 根据它的路由表来决定使用哪个中继组或电路来连接呼叫。

③ 此时，一个信令建立消息发送给目的 SSP 请求一条由源 SSP 定义的电路连接。

④ 目的 SSP 回应一个到特定中继线的确认许可并连接呼叫到最终目的地。

2. STP

STP，如图 4-2 中显示的那样，是 SS7 架构提供网络连接的主要部分。STP 根据路由信息以及消息中所含的目的地编码地址路由或交换所有的信令消息。

STP 为 SSP 间提供逻辑连接，无需两者之间连接。STP 成对配置以提供冗余和高可靠性。这些成对的 STP 完成同样的功能，并且认为主 STP 直接与 SSP 或 SCP 相连。STP 也完成全局标题翻译（global title translation）功能，我们将在本小节的后面讨论。

基于电路的消息是在 SSP 上建立的。然后，这些消息被封装在 SS7 包内由 SSP 发送，通常它们包含建立或断开呼叫请求。这些分组将被传送到终结呼叫的目的 SSP。路由这些分组到目的地是 STP 网络的工作。

由 SSP 发起的非基于电路的消息是一些数据库查询，这些查询为完成呼叫而请求一些附加信息。STP 网络负责在 SSP 和被称为 SCP 的数据库接口之间路由分组。这些包被路由到目的 SCP 或被寻址到相应的数据库子系统。SCP 是数据库的接口，提供为完成呼叫所需的路由编码。

STP 也负责度量流量和使用率。流量度量提供如网络事件、消息类型等统计信息，使用率度量提供接入和每种消息的数量等统计信息。这些信息被运营商的规划部门用来掌握整个系统的容量以考虑将来的规划。

3. 全局标题翻译（Global Title Translation）

除了基本的SS7分组路由外，STP也具有如全局标题翻译（global title translation）在内的网关功能。这个功能被用来集中SCP和数据库，而不是将所有的目的选择信息分布在成百上千的分布交换机上。如果SSP不知道目的SCP的地址，它可以向它的本地STP发送数据库查询请求。STP执行全局标题翻译，重新定位数据库查询目标到相应的SCP。

全局标题翻译通过允许将查询直接定位到STP来集中正确数据库选择。这样，SSP就没有必要负责维护所有的潜在目的数据库地址。全局标题翻译来自另一个术语全局标题数字（global title digits），是拨叫数字（dialed digits）的另一种说法。

STP在它自己的转换表中查找全局拨叫数字来解决以下问题：

- 相应SCP在数据库中的编码地址；
- 数据库子系统号码。

STP也可以通过在它的转换表中查找另一个STP来执行中间全局标题翻译（intermediate global title translation）中间的STP然后路由消息到另一个STP来完成最终的全局标题翻译。

4. STP层次结构

STP系统定义了网络互联和将功能分成几个特定的领域。STP可以分级实施，例如：

- 本地信令转接点（Local Signal Transfer Point）；
- 区域信令转接点（Regional Signal Transfer Point）；
- 国内信令转接点（National Signal Transfer Point）；
- 国际信令转接点（International Signal Transfer Point）；
- 网关信令转接点（Gateway Signal Transfer Point）。

本地、区域和国内STP在同样的网络上转接基于标准的SS7消息。这些STP一般不能转换处理不同格式和版本的消息。

国际STP提供两个基于同样的ITU标准网络之间的国际连接。

网关STP可以提供以下功能：

- 从国家版本向ITU标准的转换；
- 网间互联点；
- 网络安全功能如屏蔽，屏蔽功能检查所有呼入呼出电话来保证授权认可。

您可以将STP功能部署和安装在分离的专用设备上或者与在一个终端局或串联交换机上与其他SSP功能合作。在欧洲和澳大利亚，集成SSP和STP功能是非常常用的。这也是全关联SS7或CCS7（CCS7是ITU-T版本的SS7）网络在这些区域流行的原因。全关联SS7出现在当同一传输信道承载承载信息（bearer's information）和信令信息（signaling information）时。

5. SCP

如图 4-2 所示，SCP 提供数据库接口，非基于电路消息的附加路由信息存储在数据库中。服务供应商的 SCP 没有保存所需信息，它们只提供系统数据库的接口。SCP 与数据库系统之间采用标准协议，通常是采用 X.25 接口。SCP 提供 SS7 与 X.25 协议之间的转换。如果 X.25 不是该数据库接入协议，SCP 还可以使用原语提供通信能力。

数据库存储了与它应用相关的信息，并使用对每个数据库都唯一的子系统号码来标识定位。子系统号码在 SSP 层使用，在 PSTN 内发起请求由含这个标识。这个子系统编码标识了存储信息的数据库，被 SCP 用来响应请求。

在 SS7 网络中，以下数据库最为常用。

- 800 数据库——为如 800，877，888，900 和 976 等特定号码提供路由信息。800 数据库以相应的路由号码响应特殊号码查询。对于 800，888 和 900 号码，路由号码就是相对应的实际电话号码。
- 线路信息数据库（Line Information Database，LIDB）——提供用户线路信息，例如屏蔽与阻止（screening and barring）、电话卡业务包括卡与用户密码的认证授权和计费。数据库的计费功能决定您为被叫方付费、电话卡业务和第三方服务等计费方法。
- 本地电话号码可携带数据库（Local Number Portability Database，LNPDB）——提供被叫方交换机的 10 位位置路由选择号码（Location Routing Number，LRN）。LRN 用于在网络上路由呼叫，被叫方号码用于在终结 SSP 上完成呼叫。
- 归属位置登记器（Home Location Register，HLR）——在移动网络中记录了如当前移动用户电话位置，计费和用户信息等信息。
- 访问位置登记器（Visitor Location Register，VLR）——在移动网络中存储用户漫游出主网的信息。VLR 使用这个信息与 HLR 数据通信以确认用户漫游时的位置。

4.1.2 信令链路

在 SS7 网络中，所有的信令点由信令链路连接。这些全双工链路在网络链路上同时传送和接收 SS7 消息。这些信令链路通常是 56kbit/s 到 64kbit/s 的数据网络线路，使用单独线路或者使用如 T1/E1 中继线路上的信道。

本节覆盖以下内容：

- 信令模式（Signaling Modes）；
- 信令链路或链路集；
- 信令路由；
- 信令链路性能。

1. 信令模式（Signaling Modes）

SS7 网络有 3 种信令模式：

- 关联信令（Associated Signaling）；
- 非关联信令（Nonassociated Signaling）；
- 准关联信令（Quasi-associated Signaling）。

如图 4-3 所示，关联信令是最简单的信令方式。在这种方式下，信令和语音路径直接与两个信令端点相连。在北美，这种信令方式通常不被采用，因为那里的终端交换机需要与另外的终端交换机直接连接。但在欧洲，因为信令路径实际上起源于 E1 中继设施，关联信令非常常用。

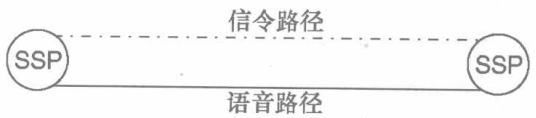


图 4-3 关联信令

非关联信令为信令和语音使用分开的逻辑信道，如图 4-4 所示。在到达最终目的前，信令消息经过多个端点，而语音路径可与目的终端交换机之间有一个直接连接。非关联信令是 SS7 网络中最常用的信令方式。

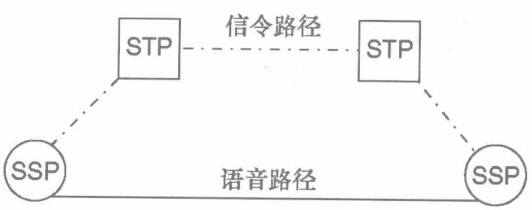


图 4-4 非关联信令

如图 4-5 所示，准关联信令使用到达最终目的地的分离逻辑路径传输信令，这条路径有最少的转接点。准关联信令的优点在于在源和目的地之间有最少的转接点，所以将网络延时最小化了；但与非关联方式相比，因为需要信令路径需要最少数量的 STP，花费增加了。

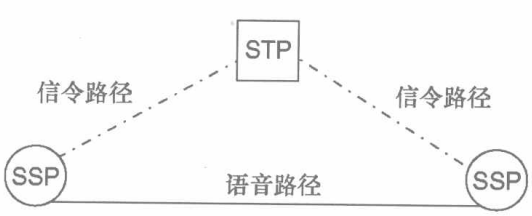


图 4-5 准关联信令

2. 信令链路和链路集

如图 4-6 所示，SS7 中的信令链路根据相应端点提供的功能划分。

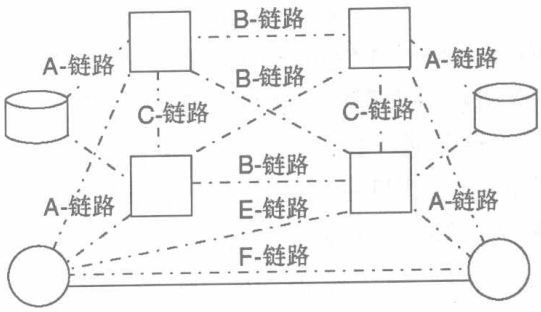


图 4-6 信令链路

下面我们列出了 SS7 网络中厂家的 6 种类型：

- 如图 4-6 所示，A-链路互联信令端点和 STP。信令端点是 SSP 或 SCP，每个至少有两个 A-链路连接“主”STP 对。一个 STP 只有一个 A-链路也是可以的，但并不通用。这些链路为传输和接收信令消息而接入网络。STP 将从 SSP 或 SCP 接收到 A-链路信令消息向目的地路由。
- 桥链路（Bridge Link，B-link，B-链路）互联两个成对的 STP，如图 4-6 所示。这些配对的 STP 对等地操作在同一层，通过 B-链路的一个四芯线组互联。B-链路承载由源到目的地的信令消息。
- 交叉链路（Cross Link，C-link，C-链路）连接 STP 与它的配对，如图 4-6 所示。STP 对履行同样的功能以提供网络冗余。C-链路只有在失败或拥挤产生时使用，因为这些链路是此时网络中的唯一有效路径。在通常情况下，这些链路止承载管理流量。
- 对角线链路（Diagonal Link，D-link，D-链路）连接在同一层中的 STP 对到另一层的 STP 对，如图 4-7 所示。D-链路同 B-链路一样，通过四芯线组连接。这些链路提供与 B-链路相同的功能。B-链路与 D-链路之间是硬性区分的。

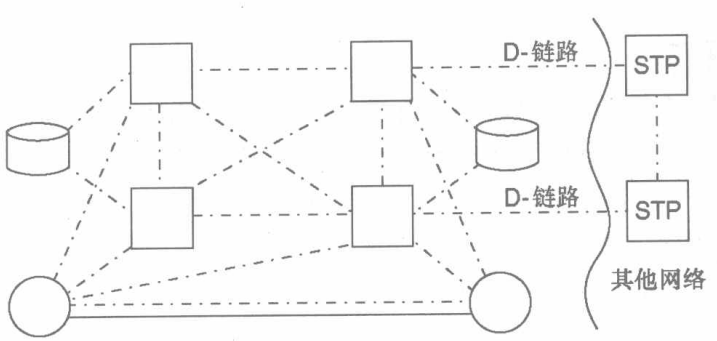


图 4-7 D-链路连接不同层次的 STP 对

- 扩展链路（Extended Link，E-link，E-链路）用于连接一个 SSP 和一个备用 STP，如图 4-6 所示。因为 SSP 有两条 A-链路到冗余 STP 对，这种链路并不常见。只有在主 STP 失败或拥挤时才使用这种链路。
- 如图 4-6，E-链路被用来直接连接两个信令端点。当 STP 不可用或者流量过大时，使用这些链路。这是唯一的一种信令流量被允许追随同一语音路径的链路方式。两个信令端点的信令消息只与两个信令端点直接连接的语音电路相关联。这种方式在北美不多见，但在欧洲相当常见。

当链路连接同一端点时，信令链路组在一起形成链路集（linkset）。信令端点提供链路集中所有链路之间的负载均衡。组合链路集（Combined linkset）被用于连接有不同的点编码地址 STP 对。在这种情况下，链路被分配给不同的链路集，并被配置成一个组合链路集。

当信令端点重新定位消息到相邻点编码时，发生组合链路集间的负载分配。您可以配置另一个链路集以提供冗余路径，以提高如 E-链路和 F-链路的可靠性，本节后面将介绍这部分内容。

3. 信令路由

信令端点拥有到目的端点预定义的静态路由。这些路由由链路集组成，链路集可以是多个路由的一部分。一组路由被称作路由集（routesets）。路由集被定义在路由表中，在当前路由不可用时提供可选备用路由。

4. 信令链路性能

SS7 网络中信令的可靠性对连接和服务电话网络用户来讲是至关重要的。因为信令链路提供信令传输和到 SS7 网络的接入，所以必须随时有效。当网络中发生拥挤或失败时，链路和 STP 对必须处理附加的流量。STP 对和链路集配置为 SS7 网络的可靠性提供必要的负载均衡和冗余。

4.2 SS7 协议概览

SS7 协议栈和层与第 6 章中要的介绍开放系统互联（Open Systems Interconnection，OSI）模型有些许不同。图 4-8 展示了 SS7 协议层与 OSI 模型各层之间的比较。比较明显的是，SS7 只有 4 层，而 OSI 有 7 层。SS7 层 1-3（L1-L3）与 OSI 的 L1-L3 一致，SS7 的层 4（L4）对应 OSI 的层 4-层 7（L4-L7）。

以下各节覆盖了图 4-8 种定义的 SS7 协议。

- 消息传输部分（Message Transfer Part，MTP），L1，L2 和 L3 为所有的其他 SS7 协议提供了传输协议。MTP 功能包含了网络接口定义、可靠的信息传输、消息的处理和路由选择（routing）。

- 信令连接控制部分（Signaling Connection Control Part，SCCP）为 L4 协议（如事务处理能力应用部分（transaction capabilities application part，TCAP））提供端对端寻址和选路。
- 电话用户部分（Telephone User Part，TUP）连接电话或者话音呼叫以及传真呼叫，是一个链路一个链路传递信令的信令系统。
- ISDN 用户部分（ISDN User Part，ISUP）是一个基于电路的协议，被用来建立和维护语音和数据呼叫的连接。
- TCAP（事务能力应用部分）为路由信息提供到远程数据库的接入，使远程网络实体的功能有效。

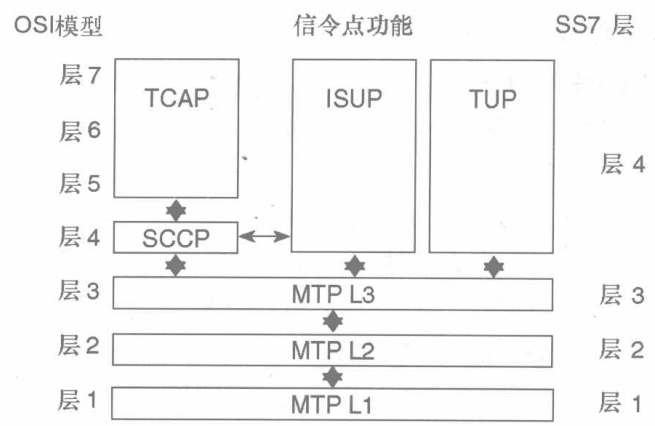


图 4-8 SS7 协议栈与 OSI 模型的比较

4.2.1 物理层——MTP L1

MTP（消息传输部分）的物理层（L1）定义了信令链路的物理和电器特征。此层也被称作 MTP1，这个 SS7 协议层事实上是与 OSI L1 一样的，而且都没有定义任何特定接口。下面我们列出了一些在现在网络中可能的会用到的 MTP1 网络接口：

- T1——T1 是北美、澳大利亚、中国香港和日本数字传输语音、数据和图像的标准。T1（也称为 *DS1*）信号在两对双绞线上以 1.544Mbit/s 的速率传送。T1 链路有 24 条全双工信道或数字信令第 0 级(DS-0)，每条 64kbit/s。所有负荷总共 1.536Mbit/s，剩余的 8kbit/s 被用于构成 T1 链路。
- DS-0——DS-0 是使用脉码调制（pulse code modulation，PCM）数字化语音的标准速度。每个 24 个单独的 DS-0 信道以每秒 8 000 次的速率采样，每次产生一个 8 位的值（每 125ms1 位）。这个 24 信道，8 位的值通过使用时分多路复用技术（time-division multiplexing，TDM）被复用成一个连续的位流以形成一个 192 位的帧，增加一个 8kbit/s 的位形成第 193 位。结果是一个每秒包含 8 000 帧的 T1 信号，其中每个帧包含 1 位构成位和 24 个 8 位采样信道。

- E1——E1 是南美，欧洲和墨西哥的数字传输语音，数据和图像的标准。E1 信号在两对双绞线上以 2.048Mbit/s 的速率传送。E1 有 32 条全双工信道，每条 64kbit/s，总共 2.048Mbit/s。

  E1 由 30 条语音和数据的 DS-0（与 T1 中的 DS-0 相同）和一条信令信道以及一条帧信道构成。
- 56/64kbit/s——T1 和 E1 中的 56kbit/s 和 64kbit/s 信道是 DS-0。56kbit/s 和 64kbit/s 接口速率是 SS7 网络中最常用的物理接口速率。
- V.35——V.35 是 ITU 关于数字业务单元（digital service unit，DSU）和包/数据设备之间的接口标准。V.35 接口定义了一个 37 针连接器的针及其电气配置。

4.2.2 数据层——MTP L2

SS7 协议的数据层（L2）是 MTP L2，也称为 MTP2。MTP2 协议被用来建立网络中端点之间的可靠的点对点连接。因为 MTP2 不在网络上运行，所以它的消息不关心最终目的地。MTP2 有下列机制。

- 纠错检错(Error Detection and Correction)—— 保持传输中数据的完整性。在 MTP2 中使用 16 位循环冗余检错（cyclic redundancy check，CRC-16）进行校验，如果 CRC-16 检测到错误，则 MTP2 要求重传。
- 包序列（Sequencing of Packets）——用于检测传输过程中消息的丢失。如果发现丢失消息，MTP2 要求重传。大多数协议都有一个特有的消息结构来指示重传。SS7 的消息结构允许任何消息的重传。重传请求可以由下一个消息的数据部分完成。重传消息的用户数据可能来自另一个 L4 应用（也就是 SCCP、ISUP、TUP 或 TCAP）。
- 链路状态指示器（Link Status Indicators）——用于维护和监视信令链路以及远程处理器的中断。

MTP2 使用称为消息单元（signal units）包来传输 SS7 消息。在 SS7 网络中，消息单元被用于错误检测，指示链路状态和传输信息消息。有三种类型的消息单元提供 MTP2 数据层功能。

- 填充信令单元 (Fill-in Signal Unit，FISU)——提供 SS7 网络中链路错误检测功能。就像它的名字的含义一样，FISU 包被用于当网络上没有流量时填充使用。这就允许您随时可以监视链路，甚至在网络上没有流量时。
- 链路状态信令单元（Link Status Signal Unit，LSSU）——在两个直接相连的信令单元间提供链路状态。
- 消息信令单元（Message Signal Unit，MSU）——提供在 SS7 网络中承载信息消息的结构。这些信息消息承载来自高层（如 SCCP、TUP、ISUP 和 TCAP）的负载。

下面的各小节将进一步讨论这些信令单元及其在 SS7 网络中的角色。

1. FISU

当没有 LSSU 和 MSU 在网络传输时，FISU 在信令链路不停地被传送。FISU 只在信令点之间传送，并不在整个 SS7 网络上传送。FISU 为链路两端的信令点提供错误检测能力。这就使信令点在 SS7 网络中可以执行错误检测功能，以验证链路的完整性及维护网络的可靠性。

如果信令端点接收到一个有错误的 FISU，那么这个信令单元将被丢弃。重传 FISU 是没有必要的，因为这类消息单元没有提供任何 L4 或用户消息。图 4-9 列出了 FISU 中的字段。

图 4-9 填充信令单元（Fill-In Signal Unit Fields）字段

下面我们来描述 FISU 中的各个字段（在 LSSU 与 MSU 中也是一样的）。

- 帧检验序列（frame check sequence，FCS）在 FISU 中是最重要的。我们使用这个字段来验证两个相邻信令单元链路的完整性。MTP 层 3（MTP3）使用 FCS 字段中的位来确定是否在 FISU，LSSU 和 MSU 中出现了错误。FCS 中的位使用 CRC-16 进行差错检测。源端点使用 CRC-16 来计算 FCS 位值。它使用 CRC-16 计算消息中的用户数据，将结果填入 FCS。接收端使用 CRS-16 计算接收到的用户数据，然后将结果与 FCS 字段进行比较。
- 长度指示器（Length Indicator，LI）指示信令单元的类型。如果信令单元是 FISU，LI 值为 0。LI 值为 1 或 2 的信令单元是 LSSU，MSU 信令单元的 LI 值为 3～63。
- 前向指示比特（Forward Indicator Bits，FIB）和后向指示比特（Backward Indicator Bits，BIBs）被用于重传。在通常状况下（没有链路错误时），FIB 与 BIB 有相同值。如图 4-9 所示，这个字段只有 1 比特长，所以只可能有两个值：0 或 1。

对于一个拒收的信令单元，BIB 值被转换且一个 FISU 被回送。转换 BIB 值使 BIB 与 FIB 的值不相等，这就表示一个拒收信号。拒收信号（negative acknowledgmen）指示了重传请求。当源端点重传信令单元时，FIB 被设为与 BIB 一样的值，直到需要下一个重传时。

- 前向序号（Forward Sequence Number，FSN）和后向序号（Backward Sequence Number，BSN）用于确认链路状态和 MSU。确认通过发送一个 BSN 与最后一个信令单元的 FSN 值相同的 FISU 实现。对于需要重传的情况，通过检查 BSN 值来确定哪个信令单元需要重传。

- 标志字段通过表示前一个信令单元的结束来指明这一个信令单元的开始。这些信令单元在信令链路上通过一个 8 位的二进制序列分隔，这个 8 位二进制序列值被设为 01111110。

2. LSSU

LSSU 在两个相邻的信令端点之间提供信令链路状态信息。您可以使用这个消息来维持链路并且可以识别远程端点的中断。LSSU 包含了 L2 接口链路的状态信息和 L3 传输端点的信息。因为这些端点并不同步，而是独立运行的，所以需要使用 LSSU 维持可靠性。LSSU 可以识别远程端点的链路接口和处理器的状态。如果信令端点接收有一个错误的 LSSU，那么这个信令单元被丢弃。重传 LSSU 是没有必要的，因为这类的消息单元没有提供任何 L4 或用户消息。

LSSU 包含与 FISU 的相同的字段，但增加了一个附加的状态字段（SF），如图 4-10 所示。LSSU 中的状态字段在端点传递了链路状态信息。LSSU 不在网络上传输，只承载在两个相邻的端点之间。

图 4-10 LSSU 格式

MTP3 使用 LSSU 提供的 L2 信息来跟踪链路和端点处理器状态，这些信息都被用于维持链路。您可以使用链路定位过程来纠正链路问题。

下面我们列出了 LSSU 自己所独有的字段。

- LI 字段用于表明信令单元的类型。对于 LSSU，LI 的值为 1 或 2。FISU 的 LI 值为 1，MSU 的 LI 值为 3～63。
- 状态字段（Status Field，SF）承载了端点之间的链路状态信息。这个字段是一个或两个 8 位，提供了承载它的链路的链路状态。在状态字段中，只有 3 位表明了链路状态，其他位被设为 0。

SF 指明了下列指示器。

- 状态指示器忙（Status Indicator Busy，SIB）表明 L2 在传输端点忙。接收到 SIB 后，MSU 接收终止，开始发送 FISU。
- 状态指示器中断（Status Indicator Processor Outage，SIPO）表明传输端点不能与上层协议通信。当处理器错误或其他端点组建发上错误时产生这个指示。接收到 SIPO 后，MSU 接收终止，开始发送 FISU。
- 状态指示器定位不准（Status Indicator Out-of-Alignment，SIO）表明链路错误，需要发起一个链路定位过程。

- 状态指示器服务中断（Status Indicator Out-of-Service，SIOS）表明传输端点不能发送和接收任何 MSU。当错误与处理器错误无关时使用 SIOS。接收到 SIOS 后，MSU 接收终止，开始发送 FISU。
- 状态指示器正常（Status Indicator Normal，SIN）与状态指示器紧急（Status Indicator Emergency，SIE）表明传输端点发起了链路定位过程（alignment prodedure）。在链路定位过程完成之前，一直发送 FISU 包，完成后，重新开始发送 MSU 包。

3. MSU

MSU 提供 SS7 网络中基于电路和非基于电路的消息传送结构。您可以使用基于电路的消息来建立，管理和释放电话呼叫。非基于电路的消息是指附加路由消息的查询及网络管理数据。MSU 起源于 MTP3 或 MTPS 用户。MTPS 用户包括 SCCP，ISUP，TUP 和 TCAP。这些消息被在信令端点上两个对等的 L4 协议间传送。

对于 ISUP 的情况，两个端点在 SS7 网络上传送 ISUP 消息。一个带有路由标签的 MSU 承载 ISUP 消息。路由标签包含了源和目的端点的点编码地址。

源端点将 ISUP 信息传送给 MTP3，MTP3 扩展 MTP3 消息后将消息传送给 MTP2，MPT2 将 MTP3 消息扩展到 MSU 中。然后，MSU 被传送给 MTP1，在信令链路上传送。目的端点接收到 MTP1 消息，然后 MTP2 抽出 MTP3 消息。L4 协议或用户数据被定义，消息被传送给目的端点的 ISUP 过程。

MSU 除拥有与 FISU 相同字段外，增加了 SIO 和 SIF，如图 4-11 所示。

图 4-11 MSU 字段

MSU 中新增字段定义如下。

- 使用 SIO 字段来指明 MSU 中携带消息的协议类型，如 SCCP，ISUP，TUP 和 TCAP。它也指明了 SS7 协议的版本。SIO 是一个 8 位的值，被分为两个部分：一个 4 位的子服务（subservice）字段和一个 4 位的服务指示器（service indicator）字段。

4 位的子服务字段表明了协议的版本（国家的还是国际的）和 MSU 的优先级。MSU 优先级位有四种可选择值，从最低优先级的 0 到最高优先级的 3。

4 位服务指示器指明了 MTP2 用户或 L4 协议，如表 4-1 所示。

表 4-1 服务指示器

MTP 用户	服务指示器值
信令网络管理（SNM）消息	0
正常维护（MTN）消息	1
特殊维护消息（MTNS）	2
SCCP	3
TUP	4
ISUP	5
用户数据部分（DUP）——基于电路的消息	6
DUP——设施消息	7

- 服务信息字段（Service Information Field，SIF）包含了路由标签和来自高层协议的控制信息（也就是 SCCP、ISUP、TUP、TCAP 或者网络管理）。SIF 字段最长 272 个字节。路由标签将 MSU 通过网络路由到最终目的地，在下一节中我们将详细讨论。SIF 的剩余部分承载用户消息或高层协议的控制数据。

4.2.3 网络层——MTP3

SS7 协议的网络层被称作 MTP3。MTP3 协议路由 SS7 消息，它依靠 MTP2 来传递消息。MTP3 也使用原语与 L4 协议（如 SCCP、ISUP、TUP 和 TCAP）通信，也转递和接收来自 MTP2 的消息。

MTP3 协议被分为两大功能。

- 信令消息处理（Signaling Message Handling，SMH）——在通常状况下路由 SS7 消息。
- SNM——当网络不可用时重新路由链路流量。

在本小节中，我们首先分析 MTP3 层的消息格式，然后说明 SMH 和 SNM 过程及功能。

1. 消息格式

MTP3 消息包括 SIO 与 SIF。我们前面已经讨论过，SIO 指明用户或协议类型（SCCP、TUP、ISUP 或 TCAP）以及 SS7 协议的版本（国家的或国际的）。SIF 被分为两个部分：路由标签和用户（或 L4）消息。用户消息包含高层协议控制信息，我们将在本章的 SCCP，ISUP 和 TCAP 小节详细讨论这部分内容。

信令端点 MTP3 过程使用路由标签来决定目的地地址。RL 包含目的点编码（Destination Point Code，DPC），源点编码（Originating Point Code，OPC）和信令链路选择器（Signaling Link Selector，SLS）字段，如图 4-12 所示。

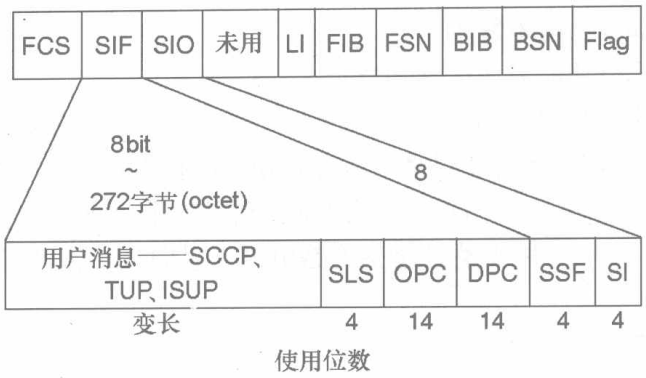


图 4-12 MTP3 消息格式

下面我们描述 RL 中的各字段。

- DPC 指明了目的端点的信令点编码或地址，有一个 14 位的地址空间。
- DPC 指明了源端点的信令点编码或地址，有一个 14 位的地址空间。

注释：您可以为信令端点提供超过一个的信令点编码地址。

- SLS 值指明了消息将路由到哪个信令链路上。MTP 用户或 L4 协议（SCCP，ISUP，TUP 和 TCAP）为每个传送出的消息制定一个 4 位 SLS 值。信令端点根据这些已经指定的值来路由消息到相应的链路。

2. SMH

SMH 功能在通常情况下路由 SS7 消息。SMH 指明目的地址是否是接收端点或者消息是否需要被路由。如果目的地址是接收端点，SMH 也指明用户应用（SCCP、ISUP、TUP 或 TCAP）。如果消息需要被传递，SMH 指明消息将要传递的路径。

SMH 被分为 3 个过程。

- SMH 消息鉴别（SMH Message Discrimination）决定 SS7 消息的目的端点地址。消息鉴别从 MSU 的 SIF 路由标签中读取 DPC。如果它是接收信令点地址，消息鉴别将消息转交个消息发布功能（message distribution function）。如果它不是接收信令点地址，消息鉴别将消息转交个消息路由功能（message routigng function）。
- SMH 消息发布（SMH Message Distribution）指明用户并将在 SS7 消息中的用户信息（SCCP、TUP、ISUP、TCAP 或网络管理）递送给上一层协议。如前所述，消息发布过程只有在消息是传送给接收端点或自己时被调用。MSU 业务指示器中业务指示器值决定消息的用户。

  如果消息用户不能处理消息，那么用户部分无效（User Part Unavailable，UPU）消息被发回传输端点。UPU 消息由网络管理过程发送，包含一个原因编码指明下列原因中的一种：

—用户部分功能没有被提供。
—用户部分功能不能用。
—用户部分功能无效但不知原因。

- SMH 消息路由选择（SMH Message Routing）与 MTP2 之间的接口，路由消息到网络上。SMH 路由过程路由消息到相应的信令链路。SMH 路由过程接收来自消息鉴别和 L4 应用的消息。当消息将要到另一个信令点时消息鉴别将消息递交给路由过程。高层应用将消息递交给路由过程以向外传输消息。

3. 路由选择概览

服务供应商静态地维护信令端点路由表。路由表为每个 DPC 指明链路、链路集、主路由和备用路由。在一个链路集中的所有链路均分负载。当一个特定的目的地有多个链路集时，这些链路集均分负载。

优先级编码指明主路由和备用路由。直接的、最直接的或最少跳数的路由（或链路）总是传出链路的第一选择。路由选择是根据链路类型（A 到 F 链路）和信令端点类型（SSP，STP 或 SCP）来决定的。例如一条在两个 SSP 之间的 F 链路，总是这两个端点消息的第一路由选择。最直接的路由的例子是 E 链路，当此链路有效时，这条链路总是该 E 链路依附的 SSP 和目标 SSP 之间的第 2 选择。

在 SS7 网络中，SNM 重新路由流量。当链路不可用时，SMH 做如下处理：

- 链路集重路由；
- 备用链路重路由；
- 路由流量到特定端点。

当链路故障时，SNM 过程通过备用链路或链路集重新路由流量。链路故障时，SNM 过程也控制流量到特定端点。

SNM 有 3 大功能。

- 链路管理——监视和控制信令端点的各条单独链路。链路管理管理信令端点的链路接口，该接口与端对端链路相对应。链路管理功能被分为 3 个部分，即链路激活（Link Activation）、链路恢复（Link Restoration）和链路释放（Link Deactivation）。
  - — 链路激活过程使用 LSSU 通知相邻端点链路状态。信令链路测试消息（Signaling Link Test Messages，SLTM）激活端点间的链路。SLTM 确认（SLTM acknowledgment，SLTA）恢复链路服务，使流量可以在链路上传输。
  - — 链路恢复过程使用 LSSU 来通知相邻端点 L3 定位活动。当定位过程完成时，发起链路激活过程。
  - — 当链路故障或发生错误时，链路停用过程将链路放入定位过程。链路停用过程使用本地 MTP2 信息和 LSSU 提供的远程信息发起定位过程。当链路故障或检测到错误时，链路停用功能触发流量管理过程。

- 路由管理——路由管理在信令端点间交换路由和状态信息。在网络故障时，路由问题通过转移消息传输以重新定向流量。这样就使其他信令端点选择备用路由。您可以为通用和集群路由管理选择多种类型的转移消息。这些消息的功能不属于本书的内容，我们将不一一论述。下面我们列出了当故障发生时使用的转移消息：
  - 禁止转移（Transfer Prohibited）；
  - 允许转移（Transfer Allowed）；
  - 转移受限（Transfer Restricted）；
  - 转移受控（Transfer Controlled）；
  - 信令路由集（Signaling Route Set）和拥挤测试（Congestion Test）；
  - 集群路由集测试（Cluster Router Set Test）。
- 流量管理——网络发生故障时，使用流量管理来重新路由或转移流量或控制拥挤。流量管理过程从 SNM 链路管理处接收有效信息，并从 SNM 路由管理处接受将问题路由到特定目的地的建议。

流量管理也可以向 SMH 和高层协议建议故障情况。流量管理使用如下功能：

- 到 SMH 的接口，用于重新路由或转移流量到备用路由；
- 建议高层协议信令链路状态的原语；
- 将消息转移到另一个信令端点对等 SNM 过程的 MSU；
- 给 MTP2 的有关信令链路的命令。

4. SNM 消息结构

SNM 消息在信令端点之间传输接收网络管理信息。SNM 使用 MTP3 消息（与到 L4 应用的相似）并且在 MSU 的用户消息（User Message，UM）字段传递信息。图 4-13 列出了 SNM 路由标签。

图 4-13 SNM 用户——MTP3 消息

SI 字段等于 0000，指明这个消息的用户是网络管理。SLS 被信令链路编码（Signaling Link Code，SLC）参数替代。SLC 参数提供一个特定链路的状态信息。如果消息不属于任何特定链路，SLC 被置 0。

5. 拥挤控制

MTP2 监视缓存中的消息队列（传出的和重传的），在出现拥挤时警告 SNM。

当缓存中的消息超过阀值时，拥挤出现（Onset of congestion）消息被发送给 SNM。SNM

过程认为链路上所有的目的地都发生拥挤。

现在我们从信令端点和 STP 的角度来考虑拥挤。

— 信令端点（SSP，SCP）从 MTP2 的拥挤出现得到拥挤信息。过多的高层消息会引起信令端点（SSP 和 SCP）链路的拥挤。在这种情况下，SNM 给应用发送消息。

指明哪些 DPC 受到了影响。这些应用应当在一段时间内较少外出的流量。直到 MTP2 接收到拥挤结束（end of congestion）指示之前，SNM 将继续发送拥挤（congestion）状态消息。收到拥挤结束指示后，SNM 停止发送状态消息，再经过一段时间后，用户应用恢复正常活动。

— 如果 STP SNM 过程接收到一个拥挤出现（onset of congestion）消息警告特定链路发生拥挤，它将认为到它相邻点的路由拥挤。当收到受影响的点的消息时，STP SNM 过程发送一个转移受控（Transfer Controlled，TFC）消息给传输端点的 SNM。STP 在 TFC 消息中指明受影响的点。这就使信令端点可以选择一条到受影响节点的备用路由。当 SNM 过程接收到一个*拥挤结束（end of congestion*）指示时，它将停止向传输端点发送状态指示。

6．重新路由

SNM 重新路由过程在不产生拥挤和丢失信息的情况下，重新路由受影响节点的流量。STP 在特定端点不可用的情况下使用这个过程。SNM 使用禁止转移（Transfer Prohibited，TFP）消息通知所有直接相连点到某个端点的路由丢失。这就使另一个 STP 可以选择一条到受影响节点的备用路由。当链路恢复时，允许传输（Transfer Allowed，TFA）消息通知直接相邻点可以恢复正常路由过程。

7．倒换（Changeover）和倒回（Changeback）

当信令链路不可用，消息需要转移到备用链路时，您可以使用倒换过程。在信令链路有效和需要重新建立平常路由时，您可以使用倒回过程。倒换和倒回过程需要两个信令点都使用 SNM 动作已维持序列和最小化丢失。

您使用两个信令点之间的倒换命令（changeover order，COO）消息来发起倒换过程。COO 消息在 MSU 的 SCL 字段指示受影响链路。SMH 功能将不选择 SLC 指示的信令链路作为传出链路，而是选择到各相邻点的备用路由。

当接收点接收 COO 消息时，它选择一条备用路由并且发送一条倒换确认（changeover acknowledgment，COA）消息给传输信令点。COO 和 COA 消息包含无效链路上最后一条消息的 FSN。两端信令点都在无效链路的传出缓冲区内找回消息并将这些消息转移到备用链路上。这样，所有的等待消息都按序列发出，不会发生丢失现象，完成了倒换过程。

当受影响链路恢复时使用倒回过程。两个信令点中的任一个都可以发起倒回过

程。SNM 通知 SMH 过程备用链路的消息应该存储在倒回缓冲区（changeback buffer，CBB）中。倒回声明（ChangeBack Declaration，CBD）被发送给相邻节点通知其链路可用。接收到 CBD 的信令点响应一个*倒回确认（changeback acknowledgment）*消息。当信令点接收到 CBA，SNM 通知 SMH 使用主链路发送消息，并且恢复平时路由过程。

4.2.4 SCCP

SCCP 在 MTP3 之上提供网络服务，这两层的组合称为 SS7 的网络业务部分（Network Service Part，NSP）。TCAP 一般使用 SCCP 的服务来访问 SS7 网络中的数据库。如图 4-8 所示，SCCP 提供到 TCAP 和 ISUP 的服务接口。SCCP 路由服务可以使 STP 通过确认 DPC 和目标数据库的子系统编号来执行全局标题翻译（Global Title Translation，GTT）。

下面几节里将覆盖以下 SCCP 功能：

- 面向连接的服务（Connection-Oriented Services）；
- 无连接的服务和消息（Connectionless Services and Messages）；
- SCCP 管理功能。

1. 面向连接的服务（Connection-Oriented Services）

SCCP 支持为 TCAP 和 ISUP 的面向连接的服务，但是现在都不再使用了。所以本小节就不描述这些 SCCP 面向连接的功能、消息和服务了。

2. 无连接的服务和消息（Connectionless Services and Messages）

SCCP 为 TCAP 提供传输层的无连接的服务（TCAP 将在 4.2.7 节中讨论。）基于 TCAP 的服务包括 800、888、900、电话卡业务和移动应用。SCCP 与 MTP3 一起传输这些服务中基于电路交换的消息。SCCP 也可以使 STP 代替端局交换机执行 GTT。端局交换机将 800 号码看作是一个功能地址，或者换句话说，看作是全局翻译地址。因为全局翻译地址是不可以路由的，终端交换机上的 SCCP 路由查询消息到它的主 STP。

在本小节中，无连接服务是基于端局交换机查询数据库以获得 800 号码的路由号码的。下面是一个在网络中如何工作的例子。

SCCP 与 MTP3 一起传输 TCAP 基于 800 的查询到中心数据库。在 SCCP 与 MTP 之间传送的无连接的消息为单元数据消息（Unitdata Messages，UDTs）和单元数据服务（Unitdata Service Messages，UDTSs）。

SCCP 发送一个 UDT 以传输子系统信息，并且它传送一个 UDT 以执行 GTT 功能。UDT 也被用于查询和接收数据的响应。表 4-2 列出了 UDT 消息中的参数。

表 4-2 UDT 参数

参数	类型	长度（8 位字节）
消息类型	M	1
协议类（PRC）	M	1
被叫方地址（CDA）	M	3 最小
主叫方地址（CGA）	M	3 最小
子系统数据	M	变量

来源： ITU-T Q.713 (7/96)

UDTS 被发送给源 SCCP，通知接收 SCCP 不能传输 UDT 到它的目的地。返回原因参数指明了 UDT 为什么被返回。表 4-3 列出了 UDTS 中使用的参数。

表 4-3 UDTS

参数	类型	长度（8 位字节）
消息类型	M	1
返回原因	M	1
CDA	M	3 最小
CGA	M	3 最小
子系统数据	M	变量

3. 无连接 SCCP 示例

这个例子演示了在一个典型的 800 呼叫中使用 SCCP 服务和消息的方法。

1．当端局交换机接收到一个 800 号码的呼叫建立请求时，它开始一个数据库查询。TCAP 将呼叫和被叫方地址参数传给 SCCP，SCCP 填写 UDT 的相应字段，并设置路由指示器位，表明需要 GTT SCCP 定位查询到主 STP，并将消息传递给 MTP。终端局的 MTP 建立 MSU 并将消息转交给 STP。

2．STP 的 SCCP 功能模块接收查询，使用它的转换表，使用数据库的子系统编码重新定位消息。SSN 中含有 DPC 和数据库子系统地址。STP 中的 MTP 然后将查询转交给 SCP 来服务数据库。

3．SCP 的 SCCP 将消息转交给 TCAP，TCAP 查询数据库。数据库将功能编码翻译成路由编码并将消息转交给 SCCP，SCCP 设置 DPC 并向源终端局发送响应消息。SCCP 为 MTP 设置了路由指示器，指示其路由选择应该基于 DPC。

4. SCCP 管理功能

SCCP 管理功能维护故障时 SCCP 消息的传输，故障包括网络或子系统故障。SCCP 管理过程在故障时，警告如 TCAP 或 ISUP 的 SCCP 用户。SCCP 管理功能模块包含到 MTP

的接口、SCCP 无连接控制和子系统（SCCP 用户）。SCCP 管理模块使用单元数据无连接消息格式。

SCCP 管理功能被分为 3 组。

- 信令点状态——依靠 MTP 服务，MTP 中断、恢复和状态信息被发给 SCCP 管理过程。
- 子系统状态——每个子系统向 SCCP 管理过程直接提供信息。这就使 SCCP 管理过程可以维护每个子系统的状态。
- 流量管理——包含从一个子系统到另一个副本子系统的重新路由消息。这样就保证了当一个子系统发生故障时，不会丢失服务。

4.2.5 TUP

当所有呼叫被认为是语音呼叫时，TUP 是第一个被定义的 SS7 语音部分。TUP 支持物理电路连接，但不能处理现在数字网络中使用的虚连接和承载电路。北美是第一个使用 ISUP 来取代 TUP 的。

ISUP 协议被定义为与 ISDN 互联并提供比 TUP 更多的能力和服务。所以，本章主要集中在 ISUP，而不是 TUP。

4.2.6 ISUP

ISUP 连接、管理和断开 PSTN 中的所有的语音和数据呼叫。ISUP 建立和拆除用于连接 PSTN 语音和数据用户的电路。这些用户包括 ISDN、模拟以及 ISDN 模拟用户。ISUP 也被用于在蜂窝和移动网络中提供中继连接。ISUP 在北美被广泛实施，比 TUP 更受欢迎。在国际上，ISUP 也被广泛采用，但是有几个国家版本。ISUP 比 TUP 提供更多的功能和服务。宽带网络服务的宽带 ISUP（broadband ISUP，BISUP）信令协议不是本书的内容。

ISUP 信息与其他 L4 协议相似，被在 MTP3 消息中传送。本节覆盖以下主题：

- ISUP 服务——基本的和附加的；
- 端对端信令——Pass-along 和 SCCP；
- 呼叫建立和拆除；
- ISUP 消息格式；
- ISUP 呼叫控制消息（ISUP Call Control Messages）。

本章后面的 4.3 节提供了包含 ISUP 消息的基本呼叫建立与拆除。

1. ISUP 服务

ISUP 服务提供在 PSTN 中到达一个端点目的地的能力。有两种类型的 ISUP 服务。

- ISUP 基本服务——提供建立、管理和拆除 PSTN 中的语音和数据呼叫。
- ISUP 附加服务——用于支持来电显示和呼叫转移等语音和数据连接的服务。端局交换机可以访问存储有这些服务订阅消息的数据库。

2. 端对端信令

端对端信令过程建立、维持和释放连接。端对端信令还允许信令端点使用信息请求（Information Request，INR）和信息（Information，INF）消息来交换信息。INR与INF将在本节稍后做详细介绍。

源和目的端点通过使用呼叫指示器来交换信令能力。源终端局在初始地址消息（Initial Address Message，IAM）中的前向呼叫指示器字段中显示它的信令能力；终结终端局在地址完整消息（Address Completion Message，ACM）、应答消息（ANswer Message，ANM）或呼叫进展消息（Call Progress，CPG）的后向呼叫指示器字段显示它的信令能力。

ISUP使用两种方式传递端对端信令：Pass-along方式和SCCP方式。

在pass-along方式中，信令信息从源交换机经过每个中间交换机，直到它到达终结终端局。起始建立信息与所有与此电路有关的后续信息使用同一路径。

SCCP方式与pass-along方式不同。ISUP使用SCCP在网络上路由信令信息。信令路径与该电路的其他消息不一定使用同一路径。SCCP使ISUP消息从源终端局直接路由到终结终端局。

3. 呼叫建立和拆除

当您理解了SS7网络中基本的呼叫建立和释放后，很容易理解ISUP功能。在下面的例子中，我们假设呼叫的目的地是一个远程终端局，ISUP信令端对端有效，中间只有一个交换机，拨叫的号码不需要查询数据库。

下面是在SS7网络中一个基本呼叫的建立和拆除步骤。

（1）用户摘机，本地的终端局给用户一个拨号音。呼叫方拨打要呼叫的号码，本地终端局收集拨叫的数字。

（2）本地终端交换机根据它的路由表决定怎样连接呼叫。路由表记录了建立端对端连接的有效电路。源办公室建立发送一个IAM给交换机，交换机提供第一个连接（pass-along方式）并指明要使用的电路。

（3）当中间交换机接收到IAM后，中间交换机向源交换机发送一个ACM消息。ACM确认了中间交换机保留了源终端局在IAM中指定的电路。ACM同时通知源办公室给拨叫方提供接通音调。

（4）在发送ACM的同时，中间交换机建立一个IAM来为建立下一个连接做好准备，该IAM含有源终端局提供的呼叫与被叫方信息的IAM。中间交换机使用它的路由表将IAM传送给终端办公室。

（5）接到IAM后，终结交换机需要确定被叫方是否占线。

如果被叫方没有占线，终结交换机发送一个ACM给中间交换机。紧跟着ACM，终结交换机呼叫被叫方电话。当被叫方接听电话时，终端交换机接通语音路径并在同一路径发送一个ANM到中间交换机。

（6）中间交换机也接通语音路径并发送一个ANM到源交换机。源交换机则可以接通语音路径，此时谈话就可以开始了。

（7）在这个例子中，我们假设被叫方首先挂断电话，在终结交换机上发起一个释放过程。终结交换机立刻向在中间交换机发起一个挂起（SUSPEND，SUS）消息，中间交换机接到该消息后向源交换机发送一个 SUS 消息。

（8）当呼叫方也挂断电话时，源交换机向中间交换机发送一个释放（Release，REL）消息，该消息的传递使用与其他信令消息一样的路径。中间交换机和终结交换机使用释放完成（RELEASE COMPLETE，RLC）消息确认释放。RLC 消息同时也表明了各电路重新空闲。

4. ISUP 消息格式

在 ISUP 消息中的消息类型值表明了在 MSU 中的消息类型，如图 4-14 所示。电路识别码（circuit identification code，CIC）表示电路是在使用中还是被释放了。

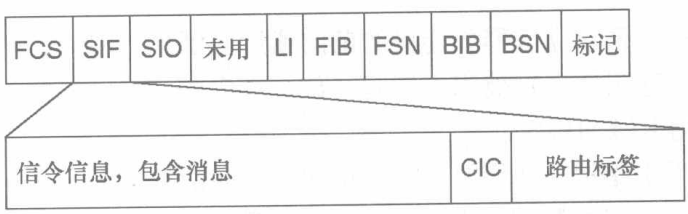


图 4-14 ISUP 消息

5. ISUP 呼叫控制消息（ISUP Call Control Messages）

表 4-4 列出了最重要的 ISUP 呼叫控制消息 所有的 ISUP 信令消息都含有 ISUP 消息类型参数。

表 4-4 ISUP 消息和消息类型

ISUP 信令消息	消息类型值
IAM	00000001
ACM	00000110
ANM	00001001
REL 消息	00001100
RLC 消息	00010000
连续测试（COT）	00000101
CPG 消息	00101100
SUS 消息	00001101
恢复消息（RES）	00001110
前向传输消息（FOT）	00001000
INR 消息	00000011
INF 消息	00000100

来源： ITU-T Q.763 (9/97)

ISUP 呼叫类型格式，包括信令参数，可选和必选字段以及每个字段的长度，可参照附录 A。

以下描述每个 ISUP 呼叫类型消息。

- IAM 是用来发起呼叫建立的第一个消息。IAM 通常包含完整的被叫方号码。完整的被叫方号码也称为*整体地址信令 (en-bloc address signal)*。当被叫方号码被再多于一个消息中传送时，会有*叠加地址信令 (overlap address signal)* 出现。
- ACM 是一个后向消息，终结终端局发送该消息用于指明是终端局正在呼叫被叫方电话。串联办公室也可以在 ISUP 信令不被支持的地方，通过发送 ACM 来表明外出中继被抢用。终结交换机发送*后向消息 (backward message)*，源交换机发送*前向消息 (forward message)*。ANM 是终结终端局发送的后向消息以指示被叫用户应答了呼叫。
- REL 是一个请求立即释放连接的前向或后向消息。REL 是前向还是后向消息，取决于是由呼叫方还是被叫方发起释放。在串联或终结终端局不能建立呼叫时，也可以使用 REL 消息。
- RLC 是用于指示交换释放中继的前向或后向消息。
- COT 是用于连续测试外出中继的前向消息。
- CPG 是一个后向消息，用于报告事件如呼叫建立时的警告。CPG 只在 ACM 后面被发送。
- SUS 是一个用于在连接正常时挂起呼叫的后向消息。
- RES 是用于恢复挂起电话的消息。SUS 和 RES 消息使用同样的消息格式和参数。
- FOT 是一个呼出局接线员用来请求呼入局接线员帮助的消息。
- INR 是用来获得跟呼叫有关附加信息的消息。通常，终结终端局会发送这个消息到源终端局。
- INF 是用来提供 INR 请求信息的消息。

4.2.7 TCAP

TCAP 提供非基于电路的消息的处理能力，这些消息被用于接入远程数据库并激发网络元素的远程功能。

TCAP 最早用于 800 号码的翻译。TCAP 消息指导 SCP 查询数据库特定消息。TCAP 也提供从交换机到交换机的查询与响应的承载机制。TCAP 使用 SCCP 和 MTP 协议端对端路由消息。这与 ISUP 不同，ISUP 在交换机间传递消息。TCAP 协议提供一个信令点的应用与另一个信令点的应用的通信方式。

数据库信息用于 800、888、900 服务，本地号码可携带，如 LIDB 的用户业务和移动用户的主/访问记录。

智能网（IN）也使用 TCAP 激活远程终端局的功能。智能网（IN）依靠 TCAP 服务来使信令点访问远程信令点的功能。智能网功能就是因为使用了 TCAP 激活消息才可行的，如自

动回拨就是当被叫方有效时使用 TCAP 激活消息通知本地交换机。

在下面各小节里我们将分析 TCAP 接口、消息类型和组件。在本章的最后，我们将介绍一个 800 查询使用 TCAP 协议的例子。

4.2.8 TCAP 接口

TCAP，如图 4-15 所示，在 SS7 网络中使用 SCCP 和 MTP 路由事务消息。您可以使用 TCP 消息在一个信令点（交换机 X）和另一个信令点（交换机 Y）之间通信。

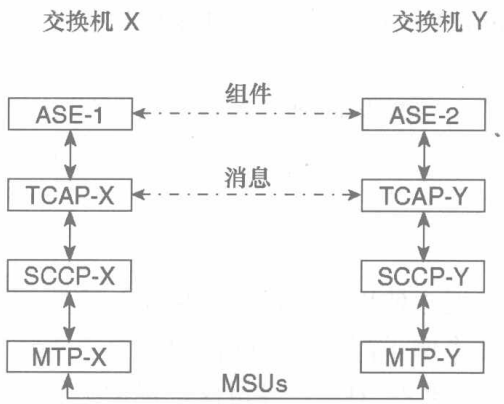


图 4-15 交换机 X 的 TCAP 接口和消息路径

应用服务元素（Application Service Element，ASE）在一端激活操作，另一端 ASE 执行操作。每个 ASE 被指定给一个应用，在远程实体间它们是对等的。在 800 呼叫中，交换机 X ASE-1 是查询交换机 Y ASE-2（也就是 SCP）对应 800 号码的路由选择号码的本地交换机。TCAP 消息包含在 MSU 的 SCCP 部分。TCAP 消息由一个事务部分（transaction portion）和组件部分（component portion）构成。

1. TCAP 事务部分

TCAP 消息的事务部分为信令点提供必要的信息，使用这些信息可以路由组件到相应目的地的。源和接收信令点的 ASE 使用同一个事务 ID。事务部分还有一个包类型指示器指示下一个消息的类型。

- 单向的——在一个方向传输组件时使用。接收方不必回应单向消息。
- 开始或查询——用于发起 TCAP 事务。开始消息发起 800 查询。
- 继续——在开始或继续消息后发起。这些消息继续 TCAP 事务。
- 结束或响应——用于终结 TCAP 事务。这个消息在开始或继续消息后发送。结束消息包含 800 查询的结果。
- 中止（Abort）——当一个事务中间出现问题时使用。这个消息中止事务。

2. TCAP 组件部分

TCAP 的组件部分可以包含执行 800 查询的请求。组件信息是在对等的 ASE 之间的通信，它包含了一个操作的请求或结果。TCAP 特有的组件如下。

- 请求（Invoke）——用于请求特定的操作。开始消息通常包括至少一个请求。继续和结束消息也可能包括请求。
- 返回结果（最终）（Return Result (Last)）——用于返回请求操作的结果。这个消息意味着操作成功完成，是响应的最后组件。
- 返回结果（非最终）（Return Result (Not Last)）——用于返回请求操作的部分结果。
- 返回错误（Return Error）——表明请求操作失败。返回错误组件也是一个请求操作的最后响应。
- 拒绝（Reject）——表明接收到的组件被认为是不正确的。拒绝组件也是对接收到的组件的最终响应。

4.3 SS7 举例

本节提供了在 PSTN 网中使用 SS7 的一些例子。这些例子覆盖了信令端点活动，使用的消息和事件序列等。每个例子都从不同的侧面介绍了使用 SS7 的方法，以及一些通常的操作。这些例子讨论了 ISUP 与 TCAP 等协议，包括主要的消息以及使用消息的顺序。这两个例子是：

- 基本呼叫建立和拆除；
- 800 数据库查询。

4.3.1 基本呼叫建立和拆除示例

这个例子演示了基本呼叫建立和拆除的步骤，也说明了在 SS7 网络中使用 ISUP 协议连接和断开呼叫的方法。图 4-16 是这个例子的网络拓扑。

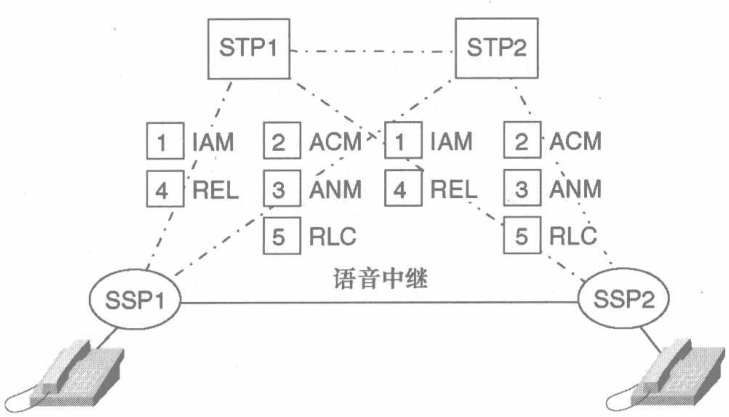


图 4-16 呼叫建立和拆除网络

在这个例子中，连接到 SSP1 的模拟用户呼叫连接到 SSP2 上的模拟用户。

以下是这个呼叫的步骤。

1．当用户摘机时，SSP1 开始呼叫处理。呼叫处理使 SSP1 进入*发起呼叫（originating call）*状态并转移到收集信息（collecting information）状态。SSP1 收集来自用户的信息或拨叫的数字。

2．当所有拨叫的数字被收集后，呼叫进入信息分析（analyzing information）状态。SSP1 分析拨叫的数字并决定是否将此呼叫发送给 SSP2。这是，呼叫进入路由选择（selecting route）状态，SSP1 在到 SSP2 的中继组中定位一条有效中继。

3．SSP1 选择一条空闲中继后，它创建一个指向 SSP2 的 IAM。这个 IAM 包含了源交换机（SSP1），目的交换机（SSP2），呼叫和被叫号码，选择的中继等信息。SSP1 使用一条到目的地的 A 链接发送 IAM（1）。

4．STP1 接收到 IAM 后，读取路由标签并将 IAM 路由到 SSP2。IAM 被接收后，SSP2 确定它就是服务中心。此时，SSP2 核实被叫方空闲并返回一个 ACM(2)给 SSP1。同时，SSP2 向后连接中继到 SSP1，在中继上采用振铃音调，并呼叫被叫方线路。STP2 接收到 ACM 后，读取路由标签并将 ACM 路由到 SSP2。ACM 证明已接收到 IAM 并且 SSP2 就是终结交换机。

5．STP1 接收到 ACM 后连接呼叫方的电话线到中继。此时，呼叫方可以听到振铃声。当被叫方拿起电话时，SSP2 创建并发送 ANM(3)到 SSP1。STP2 接收到 ANM 后，读取路由标签并将 ANM 路由到 SSP1。SSP1 核实用户和中继已经连接。

6．如果呼叫方首先挂断电话，SSP1 创建指向 SSP2 的 REL 消息（4）。REL 消息包含了与呼叫有关的中继的信息。SSP1 路由 REL 消息到 SSP2。

7．SSP2 接收到 REL 消息，断开中继与用户之间的连接，并使中继返回空闲状态。SSP2 接着创建包含呼叫使用的中继的 RLC(5)消息，SSP2 将 RLC 指向到 SSP1 并路由其到 SSP1。STP2 接收到 RLC 后，读取路由标签并将 RLC 路由到 SSP1。SSP1 接收到 RLC 消息后，将其中所指明的中继空闲。

4.3.2 800 数据库查询示例

这个例子演示了 800 查询所需的步骤，也说明了在 SS7 网络中使用 TCAP 协议的方法。图 4-17 是这个例子的网络拓扑。

这个例子中，连接到 SSP1 的模拟用户进行 800 呼叫。下面的各步将包含在这个呼叫中。

① 当用户摘机时，SSP1 开始呼叫处理。呼叫处理使 SSP1 进入*发起呼叫（originating call）*状态并转移到收集信息（collecting information）状态。SSP1 收集来自用户的信息或拨叫的数字。

② 当所有拨叫的数字被收集后，呼叫进入信息分析（analyzing information）状态。SSP1 分析被拨叫的号码，发现是 800 呼叫，不能直接路由。此时，呼叫进入*等待（wait）*状态，SSP1-TCAP 命令(800)ASE 发起一个与(800)SCP 的事务。

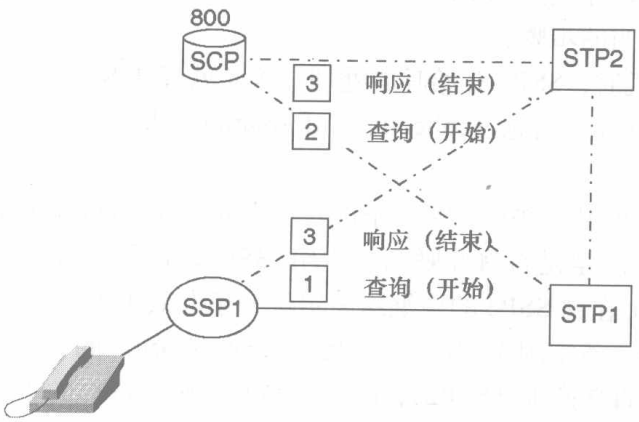


图 4-17 800 数据库查询举例

③ SSP1 创建 800 查询或开始（1）消息，这个消息包含了请求 800 号码路由号码的请求组件。SSP1 将查询或开始消息（1）转交给他的一个 STP。

④ STP1 接到消息，知道这是一个 800 查询。接着，STP1 选择相应的数据库来处理此事务。STP1 将这个查询或开始消息重新定位到（800）SCP 点编码（DPC）和 800 数据库子系统编码。STP1 接着路由查询或开始消息到（800）SCP。

⑤ 当 SCP 接到 800 查询或开始消息后，析取其中的请求并将相关信息转交给(800)ASE 执行数据库翻译。SCP 创建一个响应消息或结束消息（3），该消息在返回结果（最终）组件部分包含的路由选择号码。SCP 将消息定位到 SSP1 并将消息转发到 STP2。

⑥ STP2 接收到相应或结束消息后，读取路由标签并将消息路由到 SSP1。SSP1 接收到相应信息，得知 800 号码的路由选择号码。此时，呼叫进入*选择路由（selecting route）*状态，重复 4.3.1 节的步骤。

4.4 SS7 规范

ITU-T 的 SS7 标准可以在 Q 系列文档中找到。表 4-5 列出了 ITU-T 规范及相关的 Q 系列文档号。

表 4-5 ITU-T SS7 规范

标题	文档编号
CCITT7 号信令系统介绍	Q.700
消息转移部分（Message Transfer Part，MTP）	Q.701–Q.709
简化消息转移部分	Q.710
信令连接控制部分（Signaling Connection Control Part，SCCP）	Q.711–Q.719
电话用户部分（Telephone User Part，TUP）	Q.720–Q.729

续表

标题	文档编号
数据用户部分（Data User Part，DUP）	Q.740–Q.749
7 号信令系统管理	Q.750–Q.759
ISDN 用户部分	Q.760–Q.769
事务能力应用部分（TCAP）	Q.770–Q.779
智能网络（Intelligent Network，IN）	Q.1200–Q.1999

4.5 总结

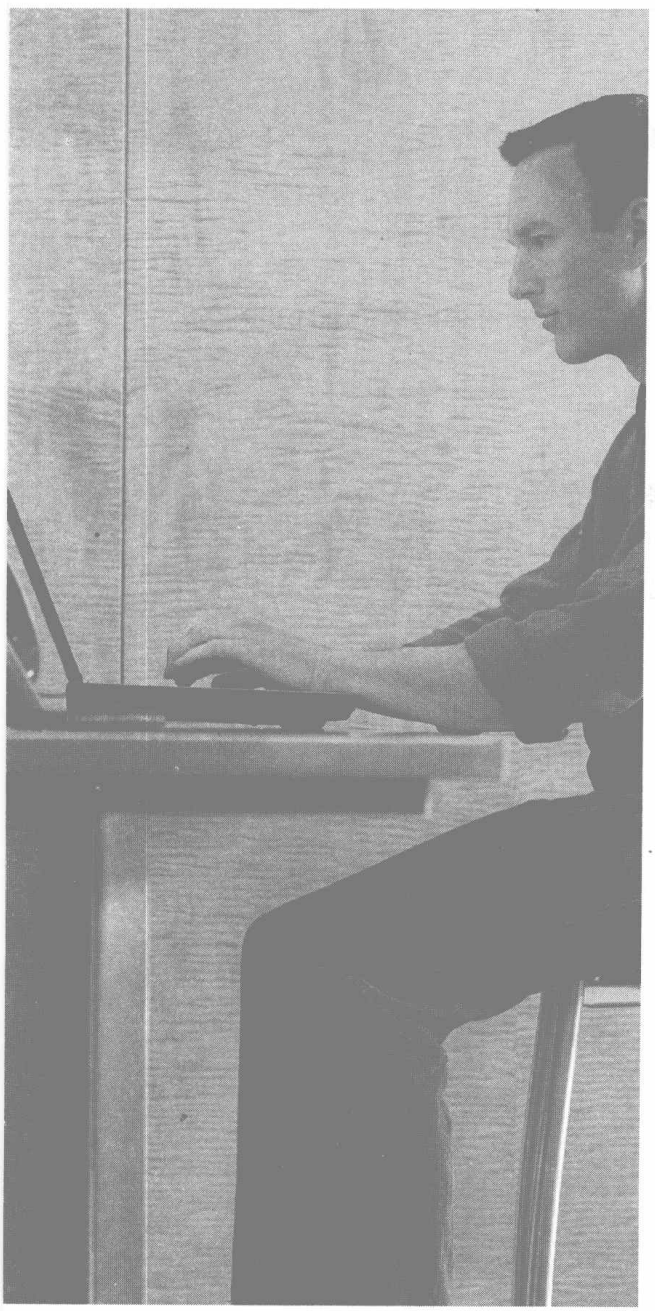
在当今的 PSTN 架构中，SS7/C7 是复杂而重要的一部分。分组语音必须与 SS7 网络集成，才能使分组语音真正成为服务供应商的一部分。

本章详细讲解了 SS7 的 4 层架构，以及 SS7 中呼叫所涉及的各种消息。

本章的细节部分可以帮助那些部署 SS7 和分组语音网络的读者更好地了解 SS7 是怎样工作的。同时，本章也说明了分组电话与 PSTN 成功集成所必须考虑的细节。VoIP 与 SS7 互连所必须考虑的有：

- MTP1 的物理链路互联；
- 信令单元终结和 MTP2 确认；
- 从 MSU（对于 ISUP 和 TCAP）析取 L4 数据用户信息；
- L4 协议支持呼叫完成和事务的服务（ISUP 和 TCAP）。

VoIP 网络必须考虑这些关键领域以便与 PSTN 无缝集成。



本章讨论网络架构框架和设计模型，包含以下主题：

- 5.1 普通老式电话业务
- 5.2 商务业务
- 5.3 服务提供商业务
- 5.4 总结

第5章

公共交换电话网（PSTN）服务

现今的公共交换电话网（PSTN）可以提供多种不同的业务，而且每一种都有着一套诱人的特色和功能。服务提供商（Service providers，SP）正是通过提供这些具有竞争力的、具有各自特色的业务来获得利润。虽然目前这其中的许多业务在现有的分组语音网络（packet voice networks）中还不能实现，但为了确定最好的能在最大限度内的将这些和许多其他的新的服务和功能添加到分组语音网络中的方法，大量的工作正在进行中。

从客观的角度——或者从用户可以使用什么——来看，目前的这一代数字交换系统提供了不能说完全一样，也是很相似的功能。这样 SP 就很难区分他们所提供的各项业务。传统上，大多数用于提供更高级服务的增值软件是与交换机捆绑在一起的。

本章主要解释了公共交换电话网（PSTN）是怎样为客户和商务客户提供服务的。主要讨论了企业是怎样通过使用不同的应用来驱动他们的业务和关键利润的，这些应用的主要功能，以及企业是怎样通过 PSTN 网络协同工作的。我们将讨论以下业务：

- 普通老式电话业务（Plain old telephone service，POTS）；
- 商务业务，包括虚拟专用网（Virtual private networks，VPNs）汇线通（Centrex），和呼叫中心（call center）服务；
- SP 业务，包括数据库和接线员业务。

5.1 普通老式电话业务

标准的电话服务通常称为普通老式电话业务（POTS）。这项业务为转盘式和按键式电话提供拨号音以及与国内和国际运营商的连接。标准的拨叫服务有：500 型电话（转盘式）、2500 型电话（按键式）、传真和与 POTS 兼容的调制解调器。

普通老式电话业务（POTS）在国际上包括紧急救援号码业务和接线员业务。普通老式电话业务（POTS）提供商也为广大 POTS 用户提供以下附加功能和服务：

- 定制呼叫业务（Custom calling features）；
- 自定义本地信令业务（Custom Local Area Signaling Service，CLASS）；
- 语音信箱（Voice mail）。

在下面的各小节中我们将详细讨论每项功能。

5.1.1 定制呼叫业务

自从 PSTN 提供此项业务以来，该项业务已经相当流行。虽然用户可以单独激活并使用这些业务，但服务提供商（SPs）通常为了简单方便而将这些业务包装成一个业务包。

提供商在端局交换机上直接开通控制定制呼叫业务。7 号信令系统（SS7）消息机制与服务的提供者不需要操作这些功能。以下列出了常用的定制呼叫业务。

- 呼叫转移(Call forwarding)——使呼叫可以跟随订户从一个地方转移到另一个地方。
- 呼叫等待（Call waiting）——当订户正在使用电话时通知有新的电话进来。
- 3 方通话（Three-way calling）——可以使订户在正在通话时邀请与第 3 方参与交谈。
- 快速拨号（Speed dialing）——为订户提供一个存储常用号码的易用方法（通常通过最终用户电话的内存实现）。
- 附加号码（Added number）——使定制者可以增加第 2 条线以区别特定的铃声和呼叫等待号音。

5.1.2 定制本地信令业务

CLASS 对订户来说是一套相当流行的业务。CLASS 功能为用户提供了一个强有力而且便捷的工具来控制呼入呼出电话。Telecorida，正式名称为贝尔通信研究（Bell Communications Research，Bellcore）定义了添加到定制呼叫业务内的 CLASS 标准。通过 CLASS，用户可以使用他们自己的电话机与交换软件互动设置或给出他们所需要的服务的指令。7 号信令（SS7）信息与功能将被激活并在网络中传送以执行相关操作。

以下列出了常用的 CLASS 功能。

- 源号码追踪（Customer-originated trace）——当用户接到骚扰电话后拨叫一个号码以通知当地相关法律部门。
- 遇忙回叫（Automatic callback）——当定制者得到忙信号时使用。这项业务在订户呼叫的占线电话不占线时，呼叫订户以通知订户。此项业务通常也被称为*回铃(camp on)*。
- 自动回拨（Automatic recall）——使定制者可以很容易地拨叫漏听电话。
- 来电显示（Display features）——需要一个来电显示电话以显示拨叫方的名字和电话号码。
- 号码隐藏（Calling number blocking）——当被叫方有来电显示功能时可以使拨叫方隐藏自己的号码。
- 呼叫屏蔽（Call screening）——使定制者可以根据电话列表来选择接听、拒听或转移呼叫。

5.1.3 语音信箱

基于 PSTN 的语音信箱可以使服务提供商提供除了留言机外的另一种选择。这项业务因为无需用户购买或操作其他设备而极具吸引力。这种基于网络的语音信箱的另一大好处

是即使电话占线，此项业务仍能使用。而且，基于网络的语音信箱还可以使用户远程提取他们的语音留言。对住宅用户和小企业有效的两种语音信箱业务包括下面两种。

- 语音消息——使用户可以存储播放问候语并且可以接听、重复接听、分发来自其他用户的留言信息。
- 传真消息——使用订户可以接收传真留待以后查看。

5.2 商务业务

因为服务提供商的大部分收入来自于商务业务，所以此项业务对他们来讲非常重要。目前需要协同工作的环境使企业需要大量的通信服务以支持他们的业务。在本节我们将描述如下服务：

- 虚拟专用语音网络（Virtual Private Voice Networks）；
- 汇线通服务（Centrex services）；
- 呼叫中心（call center）。

5.2.1 虚拟专用语音网络

使用虚拟专用语音网络可以经济可靠地连接协同位于 PSTN 上的多个地方的语音流量。如果不使用虚拟专用语音网络，则需要使用专用联络线（edicated tie-lines）来连接各个地方。因为不同的地方通常不会使用同一个交换机，所以无论如何，在这种情况下虚拟专用语音网络也是一个很经济的解决方案。

服务提供商提供虚拟专用语音网络以尽可能利用公用设施来提供私有服务。这样，公用网络设施就可以通过商务用户使用工作日而住宅用户使用晚上和周末而得到均衡使用。

虚拟专用语音网络用户通过互接他们的私网设施（例如 T1 线路）来访问公网。SS7 设施（SS7 facilities）、消息服务及网互通功能使 VPN 贯穿公网架构。SS7 功能也可以使合作及专用分组交换机（PBX）的功能在网络上透明地运行。部署带语音的网络（voice-capable network）的另一个好处是可以简化往一个已有的虚拟专用语音网络增加新的多个站点。在虚拟专用语音网上，这就像增加一个新的连接并为之提供相应的解释和拨号计划一样容易。而如果使用联络线，添加一个新的站点意味着需要新站点到每个已有连接的站点的端对端连接，这当然需要付出更高的代价。

公共交换系统使用不同的协议和拨号计划（dialing plans）来鉴别、处理和路由呼叫。可以根据通过 SS7 在公网上维护与传播的客户分组号码来区分每个虚拟专用语音网络。您可以使用这项功能来区别和路由来自公网的拨叫与私网上的拨叫。客户分组信息和其他信息被插入在综合业务数字网用户部分（ISDN User Part，ISUP）便于在公网上传播。

拨号计划能有效控制全北美编号计划（North American Numbering Plan，NANP）的 10 位选路和 7 位的在线到在线、在线到不在线和不在线到在线选路。呼叫处理、选路和呼叫能力为远端用户提供统一的呼叫计划和访问。

注释：专用连接线路（Dedicated Access Lines，DALs）连接到公用网络（public network）。DALs通过各种信令协议提供包括公网和私网的呼叫连接选路。这些协议包括 ISDN、随路信令（channel-associated signaling，CAS）、信令协议隧道（QSIG，Q Signaling）和数字专用电路网系统（Digital Private Network Signaling System，DPNSS）。这些协议已在第3章中详细介绍。

5.2.2 汇线通业务

汇线通（Centrex）使服务提供商可以为小企业提供专用、经济的类似于大企业的语音与数据业务。汇线通业务（Centrex services）使用公共交换设施提供服务，无需客户购买相关设备。

在交换机中的汇线通软件可以建立一个虚拟的专用商务网。汇线通服务可以与那些需要自行建设的系统（on-premise systems）相媲美，可以提供诸如端与端之间的呼叫控制，分布，计费和数据网等服务。您可以通过以下方式使用汇线通服务。

- POTS——您可以指定和使用这些线路作为汇线通线路。
- 功能线路（Feature lines）——配合全功能的话机，这些线路可以在标准的 POTs 线路、ISDN 和交换 56/64 线路上提供附加功能与应用。

汇线通可以为订户提供多种功能。下面列出了一些关于汇线通业务和功能。

- 呼叫处理（Call handling）——包括呼叫等待（call waiting）、呼叫转移（call forwarding）、呼叫驻留（call park）、自动呼叫分配（hunt grouping）和语音信箱（voice mail）。
- 便捷特色（Convenience features）——包括自动拨号、快速拨号、重新振铃（ring again）和来电显示（calling line identification，caller-ID）。
- 定制拨号计划（Custom dialing plans）——为每个客户组提供定制的计划以并支持内部缩位拨叫。
- 管理（Management）——可以追踪控制一个企业服务的各个方面。
- 安全（Security）——包括线路限制、雇员认证码、对私有网络的虚拟连接和记录通话明细以追踪异常活动等。

5.2.3 呼叫中心业务

呼叫中心需要将大量的呼入电话有效地处理和分配给多个代理。所以分配方式需要足够智能，以保证路由这些呼叫给合适的人。预定中心、快递公司和政府代理中心都需要呼叫中心业务。以下是在呼叫中心中最常用的实施。

- 自动呼叫分配（Automatic call distribution，ACD）——有效地将呼入电话路由到多个接听位置。ACDs 也可以使呼叫中心跟踪使用模式，电话流量和代理的绩效。ACD 系统提供多种特定功能，例如排队客户呼叫、按到达顺序接听和根据空闲时间来路由呼叫等。ACD 系统位于中心办公室或客户端。在中心办公室，服务提供商在公用线路如基本速率接口（Primary Rate Interface，PRI）分发服务。如果 ACDs 在客户端，则通常使用中继线连接公共网络。

- 交换机计算机应用接口（Switch –Computer Applications Interface，SCAI）——可以使服务提供商的交换机与呼叫中心的计算机互相通信，来合理地路由和处理呼叫。在 SCAI 模式，呼叫中心计算机存储协调呼入呼出电话并向交换机提供合适的路由信息。SCAI 服务包括当电话转给代理时提供呼叫方信息。这些服务也可以将呼叫方与互动式语音交互（Interactive Voice Response，IVR）系统相连接，在将电话转给合适坐席前收集更多的信息。

5.3 服务提供商业务

服务提供商（Service Provider，SP）业务是指在后台提供的支持 PSTN 用户的内部功能。这些服务包括号码翻译（nubmer translation）、选路（routing）、呼叫业务（calling services）和特需帮助（special assitance）。

在本节我们将描述如下服务提供商业务：

- 数据库业务；
- 接线员业务（秘书台业务）。

5.3.1 数据库业务

数据库可以使服务提供商维护、访问和翻译用于支持特定服务和访问号码的所需信息。这些信息数据库被集中存放且可以被所有的终端办公室访问。数据库存有订户正在呼叫和已有呼叫的信息，这些信息被用于局际交换所有处理。美国的数据库经常提供以下业务。

- 800 号码业务——此项服务可以使 SP 向被呼叫方，通常是商业客户，提供高水平的被大量使用的呼入电话。通过访问 SP 的 800 数据库来完成这些号码向真正号码的转换。
- 900 号码业务——通常被用于信息服务、竞赛拨入号码和公众意见调研。通过访问数据库，900 号码被翻译成真正的号码。与 800 服务不同，900 服务意味着由呼叫方付费。
- 电话卡业务（Calling card services）——订户可以使用电话卡在几乎所有种类的 PSTN 连接上拨打长途电话。数据库通过认证订户的帐户号码以及个人密码来接受订户的呼叫和计费，同时识别拨叫的号码来路由呼叫到长途业务或相应的运营商。
- 认证业务——通过激活和验证 5～7 位的认证号码来建立安全的到 VPN 服务的连接，并防止虚假连接。

5.3.2 接线员业务

在最近几年里，接线员业务（秘书台服务）已经有了很大的变化。造成这些变化的主要原因是自动系统、语音识别与记录、在线信息数据库和 SS7 服务激活能力等技术的高速发展。

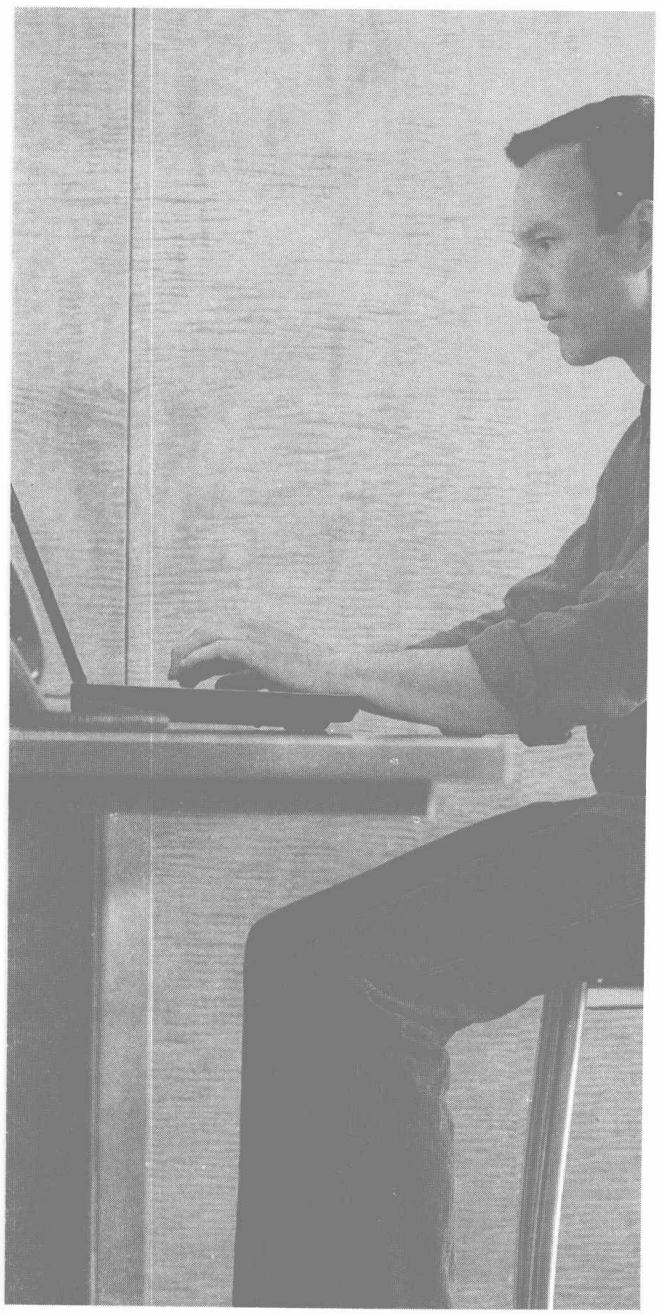
现在，呼叫中心交换系统可以处理大多数以前需要人工参与的呼叫。这样就可以使接线员集中精力在特需的服务和可以带来利润的增值服务。目前，经典的接线员业务（秘书台服务）有如下业务。

- 收费与帮助——对于今天的公共交换电话线路，接线员仍需要提供一些通常的帮助和帮助完成一些长途付费电话。当为使用硬币的公共付费电话上记账，改变付费方式如被叫方付费的长途电话，以及酒店客人的电话账单时等都需要操作员的参与。通过简单的拨零，酒店客人就可以接通酒店的接线员。接线员可以提供房费信息、准确地转接电话，还可以提供有价值的紧急服务。
- 查号业务——可以通过拨叫一个 3 位的国家号码或地方特定的号码来获得查号服务。查号服务台接线员可以根据目录列表来查找电话号码。当接线员找到一个匹配的电话号码后，他或她就将电话转到一个声音应答单元来将号码提供给客户。可供 SP 使用的数据库搜索引擎是广泛的，可以为客户的请求提供十分有效且及时的响应。
- 计费服务——在美国大约有 20%的长途电话需要接线员的参与。这些大量的参与包括对方付费电话（collect calls）、第 3 方账单、电话卡和信用卡业务。剩余的 80%长途电话通过自动系统、声音识别、记录技术以及数据库等一起在 SS7 网络上完成处理。

5.4 总结

普通的老式电话服务将不再普通。随着宽带（DSL，有线宽带（cable），无线等）入户，语音将只是每个人家中的另一个应用而已。我们前面所列的所有功能只是冰山的一角。本章所讨论了接线员们占据了重要的一部分的增值服务。

PSTN 向订户提供了许多很有价值的业务，而且对于中小和大型企业的运作来讲，这些业务十分重要。然而，这些订户和企业越来越依赖于数据网络和因特网的强大与价值。至此，本章所讨论的 PSTN 业务和一些新语音业务，将随着时间的推移在数据网和因特网上实现。



本章讨论网络架构框架和设计模型，包含以下主题：

- 6.1 OSI 参考模型
- 6.2 因特网协议
- 6.3 数据链路层地址
- 6.4 IP 地址
- 6.5 路由协议
- 6.6 IP 传输机制
- 6.7 总结
- 6.8 参考资料

第6章

IP 技术指南

VoIP 的许多优点是因为它采用了因特网协议（Internet Protocol，IP）作为传输机制。所以要想真正理解这些优点，我们必须首先了解 IP 的具体含义。IP 有什么特点，IP 分组是什么样的？这些问题和其他一些问题，都可以在本章中找到答案。

在您了解 IP 可以做什么以及在 IP 上运行应用的方法之前，有必要先了解开放式系统互联（Open Systems Interconnection，OSI）参考模型及其在 IP 上的应用。

6.1 OSI 参考模型

国际标准化组织（International Organization for Standardization，ISO）在 20 世纪 80 年代早期开发了 OSI 参考模型。OSI 是目前开发计算机通信协议的实际标准。虽然并不是所有的协议都遵从这个模型，但大多数新协议都采用了分层方式。此外，大多数人在学习网络知识时，都是从这个模型开始的。

OSI 参考模型将机器之间的通信问题拆成了 7 层。每层只同另一台机器相对应的同一层交谈（参见图 6-1）。这就意味着第 5 层只需考虑接收方机器的第 5 层，无需考虑实际的物理介质是什么。

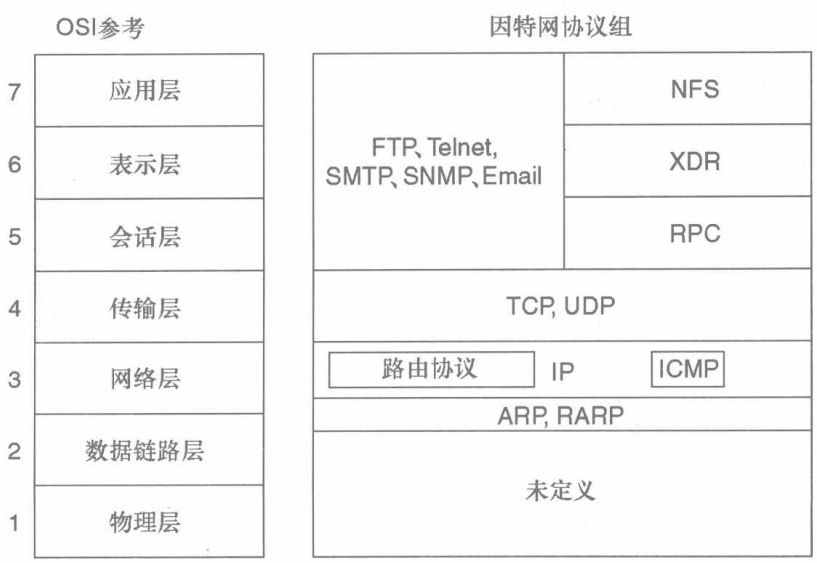


图 6-1　OSI 参考模型

另外，OSI参考模型的每层都为它的上一层提供服务（第5层对第6层，第6层对第7层，等等），而且向它的直接下一层请求特定的服务。

这种层次方法使每层只需处理信息的一小部分，就可以对数据进行必要的修改，并可以在将数据传递给下一层前增加必要的功能。数据在OSI参考模型中向下传送时，慢慢由更接近于人类变为更接近于计算机，最终在物理层变成1和0（电脉冲）。图6-1显示了OSI参考模型。

本章主要讨论以下7层：应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。理解了这些层有助于理解IP路由是怎样工作的，以及IP是怎样在第1层的各种各样的媒体上传输的。

因特网协议组（Internet Protocol suite）（见图6-1）可以映射到相应的OSI各层。从IP协议组图中，您可以看到应用（FTP或Email）在第1层上传输之前，是怎样在上层协议（如TCP）上运行的。

6.1.1 应用层

许多用户都熟悉应用层。被广泛了解的应用包括：

- 电子邮件（E-mail）；
- 页面浏览（Web browsing）；
- 文字处理（Word processing）。

6.1.2 表示层

表示层确保一个系统应用层发送的信息对另一个系统的应用层是可读的。在需要的时候，表示层将多种数据格式的数据用统一的格式表示。

应用层不仅关心他本层的格式以及所表示的实际用户数据，而且也关心程序们所采用的数据结构。所以，除了数据格式转换（如果必须），表示层也与应用层协商数据传输语法。

常用的有：

- 加密（Encryption）；
- 压缩（Compression）；
- ASCII、EBCDIC（美国信息交换标准码、扩充的二进制编码的十进制交换码）。

6.1.3 会话层

就像它名字一样，会话层负责建立、管理和终止应用间的会话。会话由两个或多个表示实体间的对话组成（会话层向表示层提供服务）。

会话层同步表示层实体间的对话以及管理它们的数据交换。除了提供会话的基本规则外，会话层也提供会话层、表示层和应用层的传输和异常报告。

6.1.4 传输层

传输层负责提供网络间的可靠数据传输。这通过流量控制（flow control）、错误检测（error

checking，checksum）、端对端确认（end-to-end acknowledgments）、重传（retransmissions）和数据队列（data sequencing）等方法来完成。

一些传输层，如传输控制协议（Transmission Control Protocol，TCP）中也包含拥挤处理机制。例如，当网络中出现拥挤或分组丢失时，TCP 将调整它的重传计时器。当拥挤出现时，TCP 将减缓它发送的流量。缺少目的地节点接收确认时，就认为出现了拥挤。

6.1.5 网络层

网络层提供了逻辑地址。这样，通过这个地址，可以使两个在完全不同的逻辑网络上的不同系统确认一条通信路径。路由协议位于网络层。

在今天的因特网上，IP 寻址是目前使用最广泛的寻址方法。路由协议，如增强内部网关路由选择协议（Enhanced Interior Gateway Routing Protocol，Enhanced IGRP，或 EIGRP）、最短路径优先（Open Shortest Path First，OSPF）、边界网关协议（Border Gateway Protocol，BGP）、中间系统到中间系统（Intermediary System to Intermediary System，IS-IS）和许多其他协议都被用于决定两个逻辑子网之间的最优路由。

注释：只有当您使用路由器时才可以在子网外交换 IP 流量。

传统的路由器根据它们的网络层地址路由 IP 分组。网络层的主要功能包括：

- 格式化包（Packet formatting）、网络和主机寻址（addressing networks and hosts）、地址识别（address resolution）和路由；
- 创建和维护路由表。

6.1.6 数据链路层

数据链路层通过物理层提供可靠传输。链路层有它自己的寻址方法。这个寻址方法关心物理连接，可以根据数据链路层地址传输帧。

传统的以太网交换机（Ethernet switches）基于数据链路层（第 2 层）地址交换网络流量。基于第 2 层地址的流量交换通常称为*桥接（bridging）*。实际上，以太网交换机就是一个有多个接口的高速桥。

6.1.7 物理层

物理层所关心的是如何使用电脉冲和电压变化来在物理介质上创建 1 和 0。常用的物理层通信规范包含以下几种。

- EIA/TIA-232——用于计算设备通信的电子工业协会/电信工业协会（Electrical Industries Association/Telecommunications Industry Association）规范。这个接口通常被用来接计算机和调制解调器，可能会使用不同的物理连接器。
- V.35——定义信令速率在 19.2kbit/s 和 1.544Mbit/s 的国际电信联盟电信标准部（International Telecommunication Union Telecommunication Standardization Sector，

ITU-T)的信令机制。这个物理接口是一个34针的连接器，也称为Winchester Block。

- RS-449——用于同步广阔区域通信的规范。RS-449物理连接器使用37针，可以比EIA/TIA-232连接更长的距离。
- 802.3——以太网上最广泛使用的物理媒体。目前的以太网网速为10Mbit/s到1 000Mbit/s。

6.2 因特网协议

IP本身是位于第3层（网络层）的无连接协议，这就意味着没有可靠机制、流量控制、队列和确认。其他的协议，如TCP，可以在IP之上（第4层，会话层），并可以增加流量控制、队列和其他功能。

因为IP在OSI参考模型中的位置，它无需考虑通用数据链路，如以太网、ATM、帧中继和令牌环，或者物理问题如同步光纤网络（Synchronous Optical Network，SONET）、铜缆或光纤。这就使IP可以无处不在。

您可以为家庭和企业通过多种物理媒体（如无线，宽带或基带）提供IP服务。这并不意味着网络的设计可以忽略最低的两层。它只是说物理介质对于任何您在IP上的应用都是独立的。

IP被认为是一个突发式（bursty）的协议,也就是说IP上的应用在经过一个长时间的无数据传输后，会突然需要带宽的一大部分。这方面的一个很好的例子就是电子邮件。如果您设置为每20分钟接收一次电子邮件，那么在这20分钟中只有很少的带宽被使用，而在接收邮件时，会突然使用大量带宽。当然电子邮件只是其中的一个应用，其他IP上的应用也与它一样也是突发式的（如银行应用，视频，语音电话等）。

IP的一个重要的优点是只需要书写应用一次,就可以在各式各样的媒体上发布该应用，不管是在家里的DSL连接还是公司的T1线路上。

IP包可以使用三种方式编址：单点（unicast）、多点（multicast）或广播（broadcast）方式。简单来说，这三种机制使每个IP包都被提供了一个目的地地址标签，且每种都有它的独特之处。

- 单点方式比较简单，在单点地址中只指定了一个主机地址而且只有这个节点才会将数据包向OSI参考模型的上层传送。
- 广播包将传送给本地子网上的所有用户。广播包可以通过桥和交换机，但不能通过路由器。
- 多点传送包可以使用一个特定的地址范围，这样在不同子网上的一组用户都可以接收到同样的流量。从而，发送者只需要发送一个包，几个不同的接收者都可以接收到。

单点、广播和多点传送包都有着重要的作用。单点传送包可以使两个站点之间互相通信，而不用考虑他们的物理位置。广播传送包可以使同一子网的每个用户同时通信。多点传送包可以使应用（如视频会议等）有一个发送者但有多个接收者。

无论使用什么类型的 IP 分组，数据链路层寻址都是必需的。

6.3 数据链路层地址

数据链路层地址和网络层地址是两种类型的地址。数据链路层地址——也被称为介质访问控制（Media Access Control，MAC）地址和物理层地址对于每个设备都是唯一的。在局域网（local-area network，LAN）中，每个设备都有一个 MAC 地址来在网络中唯一标识自己。这样计算机就知道了是谁发送的什么消息。以太网帧的前 12 个字节是目的和源的 MAC 地址。

如果您使用的是以太网交换机，流量将在交换机上基于数据链路层（MAC）地址传输。如果您使用的是转发器或集线器连接设备到局域网（LAN），不管 MAC 地址是什么，数据包将被转送给每个口。这是因为在集线器上传输是基于物理层的，而不是数据链路层。

当流量是基于 MAC 地址路由时，通常称为正在被交换或桥接。在 20 世纪 80 年代后期路由器被使用前，许多厂商开发了桥以连接两个分开的网络。桥可以提供简单而经济的方式，在数据链路层连接两个网络。因为这些桥根本不查看网络层地址，所以一些例如广播和多点传输数据流量会通过桥而占用大量带宽。

20 世纪 80 年代和 90 年代，大多数的局域网都是采用集线器来连接以太网工作站的。这个设备就是所谓的*转发器（repeater）*，只复制第 1 层的信息。所以，如果一个企业使用了一个八口的集线器，其中的一个口接收了一个数据分组，那么这个数据分组也会复制（完全复制，包括错误等）到其他七个口。

在 20 世纪 90 年代早期，一些公司开始开发局域网交换机。交换机基本上是集线器和桥的组合。这样，局域网交换机知道每个物理接口的第 2 层地址，只根据第 2 层地址来转发流量。当交换机在它的交换表中没有一个目的地的第 2 层地址时，或者数据包是一个广播包时，交换机会复制数据包到交换机的每一个接口。

网络交换机的使用可以更好地利用带宽。交换机可以通过阻止 IP 包被传输到不是接收设备的物理口来节省带宽。

到这里，您应该对 MAC 地址和网络怎样使用他们路由数据包有了一定了解，下面我们来讨论怎样使用 IP 寻址来进一步路由这些数据包。

6.4 IP 地址

理解 IP 地址是构建 IP 网络的基石。就像我们前面提到的，现在有很多种协议，每种都有自己的寻址方式。

网络层寻址通常都是分级的。比如，在北美公共交换电话网络（Public Switched Telephone Network，PSTN）中每个编码计划区域（Numbering Plan Area，NPA）包含一个区域，带有一个前缀（Nxx）表示子区域，工作站标识符（xxxx）表示具体的电话。

注释：北美编码计划协会（North American Numbering Plan Association，NANPA）管理北美的 PSTN 等级拨号计划。PSTN 是被等级的和地理的定义的。IP 编址是分级定义的，但跟地域没有必要的联系。

网络层寻址在 OSI 模型的第 3 层。这样一组计算机就可以被分配类似的逻辑地址。逻辑寻址与通过他或她的国家、省份、邮编、城市和街道地址来决定一个人的地址。

路由器根据第 3 层地址来转发流量。IP 寻址支持五类网络。目标 IP 地址的第一位指名了网络类型。

- A 类地址只用于少数的大型网络，它只使用 7 位作为网络地址，24 位作为主机地址（有效的网络地址有 126 个，主机地址有 16 777 214 个）。
- B 类地址使用 14 位作为网络地址，26 位作为主机地址。这类地址提供了很好的网络和主机地址空间的组合（有效的网络地址 16 384 个，主机地址 65 534 个）。
- C 类地址使用 21 位作为网络地址。它们只使用 8 位作为主机地址，所以每个网络中的主机数是有限的（有效的网络地址 2 097 152 个，主机地址 254 个）。
- D 类地址如在 RFC 1112 中描述的一样，为多点传播组保留。在 D 类地址中，最高的 4 位被设为 1、1、1 和 0（有效的网络地址 268 435 356 个，没有有效的主机地址）。
- E 类地址也被 IP 定义但保留为未来使用。在 E 类地址中，4 个高位被设为 1，第 5 位总为 0 （没有有效的网络地址和主机地址）。

IP 地址被书写为如 121.10.3.116 的点十进制格式。图 6-2 显示了 A，B，C 类的 IP 地址格式。一种简单地理解这几类地址的方法是：您如果拥有越多的网络地址则那么您的网络上就有越少的主机。

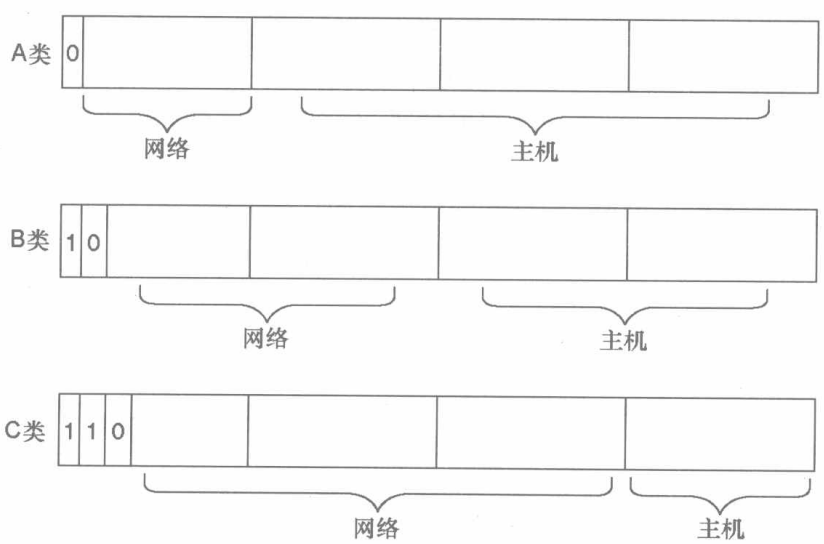


图 6-2 A、B、C 类地址格式

您也可以将 IP 网络分为更小的单位——子网。子网为网络管理员提供了更多的灵活性。我们设想网络被分配了一个 B 类地址，那么这个网络上的所有节点都遵从 B 类地址格式。假设这个网络的地址为 128.10.0.0 子网掩码为 255.255.0.0（主机部分用 0 表示，代表整个网络）。

与其将所有地址改为另一种基本网络号码，管理员还不如使用子网划分来划分网络。它可以借用地址的主机部分的一些位标识子网，如图 6-3 所示。

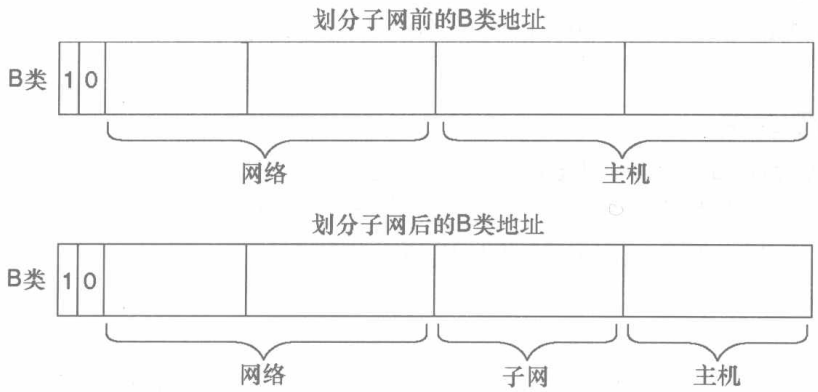


图 6-3 子网划分一个 B 类地址

我们在这个小节中讨论了 IP 地址是怎样构成的，在下一小节里，我们将讨论路由器是怎样知道将 IP 包转发到哪里的。

6.5 路由协议

IP 是一个可被路由的协议。一个可被路由的协议是一个承载数据的包。它与路由协议不同，后者更新路由器使他们知道应该使用哪条路径传递包。

在今天的 IP 网络上，有各种路由协议。本书不会深入探讨路由协议。

> 注释：这里有必要指出的是，通过使用路由协议，一个部属很好的数据网络是可以自愈和冗余的，这也就提高了网络的可靠性。一个可以自愈的网络，可以使其上的应用有最少的停工时间。对于 VoIP 应用，可自愈网络允许实时流量被连续接收。

当今的 IP 网络使用两种主要的动态路由协议：距离向量路由和链路状态路由。

简单来说，*距离向量（distance-vector）*路由关心的是将经过多少条（路由器），链路状态路由关心的是路由器接口的状态（换句话说，就是它们可用不可用，所以得名*链路状态（link state）*）。

这两种路由协议中包含内部和外部路由协议。内部路由协议被用来更新属于同一管理范围内的路由器（自治系统）。外部路由协议通常用来在不同的自治系统间传递路由表。因特网上使用的 BGP 协议是一个很好的外部路由协议的例子。

6.5.1 距离向量路由

距离向量路由是路由器用来选择最佳路径的一种算法。这个算法使用最少跳数（一个路由器为一跳）来决定到达目的地的最好路径。

广播包被定期发送以更新相邻的路由器信息。当一个路由器开始广播更新时，它包含了可到达的所有直接相连的网络。路由器接收到路由后将其保存在路由表中，路由器使用路由表来转发包。

这种方式是带宽敏感性的，因为整个路由表更新要定期发送（通常每个30秒）。

6.5.2 链路状态路由

链路状态路由与距离向量路由不同，它只需要在接口状态发生改变时发送路由更新。链路状态路由器维护着一个拓扑表，使用这个表可以构建网络整体拓扑图。这就意味着，只有当有一个接口被启用或禁用时，才会有更新流量发送，才会消耗带宽和更新拓扑表。

6.5.3 BGP

BGP 在 TCP/IP 网络中执行域间路由。BGP 是一种外部路由协议（Exterior Gateway Protocol，EGP），也就是说它在多个自治系统之间执行路由，与其他 BGP 系统交换路由和可到达信息。

BGP 被设计来代替它的前身 EGP 来作为全球因特网的外部网关路由协议，EGP 已经弃用。BGP 解决了 EGP 的一些严重问题，使因特网可以更有效地增长。

6.5.4 IS-IS

IS-IS 是一种 OSI 链路状态分级路由协议。它在网络上传输大量的链路状态信息以构建一个完整、一致的网络拓扑图。

为了简化路由器的设计与操作，IS-IS 分为第 1 级和第 2 级的中间系统（Intermediate Systems，ISs）：

- 第 1 级的 IS 与同一区域的第 1 级 IS 通信；
- 第 2 级 IS 在第 1 级区域间路由上形成域间路由主干。

因为第 1 级的 IS 只需要知道怎样到达最近的第 2 级 IS，分级路由简化了骨干的设计。骨干网的路由协议也可以在不影响域内路由协议的情况下进行修改。

6.5.5 OSPF

OSPF 是一种链路状态内部网管协议（Interior Gateway Protocol，IGP）。它被设计用来在 TCP/IP 网上弥补路由信息协议（Router Information Protocol，RIP）的不足。

OSPF 是从许多协议演化来的，这包括由 BBN（Bolt, Beranek, and Newman, Inc）公司

开发的最短路径优先（shortest path first，SPF）、OSI IS-IS 路由协议的早期版本和其他研究成果。

6.5.6 IGRP

IGRP 是一个很健壮的协议，用于在具有相当复杂拓扑和各种带宽介质及时延特性的自治网络内路由。

思科公司在 20 世纪 80 年代的中期开发了 IGRP。IGRP 是一个距离向量内部网关协议。在决定路由时，它综合考虑一组度量标准。

6.5.7 EIGRP

EIGRP 是由思科系统开发的增强版本的 IGRP。

EIGRP 使用和 IGRP 一样的距离向量算法和距离信息，但 EIGRP 的收敛特性和操作性能要比 IGRP 好很多。EIGRP 是一个距离向量内部网关协议，具有如下的特性。

- 它在做路由决定前综合考虑多种度量标准。
- 它使用扩散更新算法（Diffusing Update Algorithm，DUAL）使路由很快地汇聚。
- 它只发送路由表被更新的部分。
- 它实施了邻居发现机制。

6.5.8 RIP

RIP 是一种用跳数作为度量标准的距离向量协议。RIP 是内部网关协议，它在一个自治系统内执行路由。

所有这些协议根据他们的优点和缺点使用在不同的网络上。本书不再就什么时候应该选择哪一种协议作进一步讨论，但只有了解这些协议的基础才能更好的知道组网 IP 网络的方法。

理解不同的传输机制带给 IP 不同的特性也是很重要的。这些传输机制将在下面章节讨论。

6.6 IP 传输机制

TCP 和用户数据报协议（UDP）拥有不同的特性，多种应用程序都将使用这些特性。比如说如果可靠性比时延重要的话，可以使用 TCP/IP 来保证包的发送 相反，UDP/IP 不能实现包的重传输。这可能降低了可靠性，但对于一些情况，重传已经晚了的包是没有意义的。

为了比较不同的传输层协议，我们有必要先介绍一下 IP 分组的组成。图 6-4 显示了 IP 包的各个域。

图 6-4 IP 包格式

IP 包的各域定义如下。

- 版本号（Version）——指明是使用的 IPv4 还是 Ipv6 地址。
- IP 包头长（IP header length，IHL）——指明数据包的包头有多少 32 位字长。
- 服务类型（Type of service）——详细说明一个特定的上层协议希望这个数据包怎样被处理。可以根据这个域指定各种服务质量（quality of service，QoS）级别。
- 全部长度（Total length）——详细说明整个 IP 分组的长度，包括数据和分组头，以字节为单位。
- 标识符（Identification）——包含一个用以确定这个数据包的整数。这个域被用来组合拆分后的数据包。
- 标志位（Flags）——一个 3 位的域，低 2 位用于控制拆分包。最高的 1 位没有使用。1 位用于指明本包是不是可以再拆包，第 2 位指明本包是不是已拆分包的最后一包。
- 生存时间（Time To Live，TTL）——此域维护了一个计数器，当这个计数器减为 0 时，这个数据包就会被丢弃。这就防止了包的无限制循环。
- 协议（Protoco）——指明了当 IP 处理完毕后，由哪个上层协议接收这个数据包。
- 头部校验和（Header checksum）——用于检验头部没有受损。
- 源地址（Source address）——发送地址。
- 目的地址（Destination address）——接收数据包的地址。
- 选项（Options）——使 IP 可以支持各种选项，比如安全。
- 数据（Data）——包含有应用数据以及上层协议信息。

6.6.1 TCP

TCP 为上层协议提供全双工的、带确认的和流量控制的服务。它将数据转换为连续的、无结构的字节流，其中字节通过序列号标识。

为了得到最大的吞吐量，TCP 允许每个站点可以在确认到达前发送多个分组。当发送

者接收到一个发出分组的确认时，发送者滑行包窗口并再发送另一个包。这种流量控制机制被称为*滑动窗口（sliding window）*。

TCP 可以支持大量的上层同时对话。TCP 头部的端口号标识了一个上层对话。许多知名的端口为文件传输协议（File Transfer Protocol，FTP），万维网（World Wide Web，WWW）和远程登录（Telnet）等保留。

在 VoIP 的信令部分，TCP 可以被用来保证呼叫的建立。TCP 的运行机制使它不适合承载 VoIP 呼叫的语音媒体（RTP）。对于 VoIP 来讲，响应时间比分组丢失更重要。目前，H.323 使用 TCP，SIP 和 MGCP 使用 UDP 协议（SIP 也支持 TCP 作为传输机制）。

TCP 分组的各域定义如下。

- 源端口和目的端口——指明上层源和目的过程在哪一点接收 TCP 服务。
- 序列号——通常是当前消息数据的第一个字节被指定的号码。在一些特定的情况下，它也被用于指明下一个到来的传输的初始序列号。
- 确认号——包含了发包者期望接收的下一个序列号。
- 数据偏移（Data offset）——指明 TCP 头部 32 位字数量。
- 保留（Reserved）——为以后使用保留。
- 标志位（Flags）——承载一些列控制信息。
- 窗口大小（Window）——指明发送者接收窗口的大小（也就是接收数据缓存区的大小）。
- 校验和（Checksum）——指明头部和数据是否在传输中被损坏。
- 紧急指针（Urgent pointer）——指向包中的第一个紧急数据字节。
- 选项（Options）——详细说明 TCP 的各种选项。
- 数据（Data）——包含了上层信息。

6.6.2 UDP

与 TCP 相比，UDP 要简单许多，但在没有必要使用 TCP 可靠机制的地方非常有用。UDP 是一个无连接的协议，头部较小，这样为传输增加的负载也最小。

UDP 的头部有四个子段：源端口，目的端口，长度和 UDP 校验和。其中源和目的端口字段与 TCP 头部中的作用一样。长度字段是 UDP 头部和数据的长度，校验和字段进行包完整性校验。UDP 的校验和字段是可选的。

UDP 在 VoIP 中承载真正的语音流量（承载信道（bearer channels））。不使用 TCP 是因为流量控制和重传输对于语音视频数据来说是没有必要的。因为 UDP 被用来承载音频流，所以它不管是 5%的分组丢失还是 50%的分组丢失，都将连续传输。

如果 VoIP 使用 TCP，那么在等待确认和重传输而造成的时延将使语音不可用。对于 VoIP 和其他的实时应用，控制时延要比保证每个包的正确传递重要得多。

所以，TCP 在大多 VoIP 信令协议中被用于呼叫建立。有关 VoIP 呼叫信令的细节，请参照第 11 章、第 12 章和第 13 章。

6.7 总结

对于机器对机器的通信来讲，IP是最为广泛使用的一种。它使分离的应用和网络可以采用一种新的方式通信。

本章接触了IP的基本部分。通过这些信息，您现在就可以开始探讨VoIP的可能性和其他许多基于IP的应用了。

对于IP更细节的信息，您可以参照如下图书：

- 《TCP/IP路由技术（第一卷）》（已由人民邮电出版社翻译出版），Jeff Doyle, ISBN: 7115154293。

6.8 参考资料

对于建议的新的需求使下列的一些协议已经被弃用。下面这些资料可以帮助您开始研究IP。

RFC 761——传输控制协议（Transmission Control Protocol）。

RFC 768——用户数据报协议（User Datagram Protocol）。

RFC 791——因特网协议（Internet Protocol）。

RFC 1058——路由信息协议（Routing Information Protocol）。

RFC 1131——开放式最短路径优先（Open Shortest Path First）。

RFC 1518——使用CIDR定位IP地址的体系结构（An Architecture for IP Address Allocation with CIDR）。

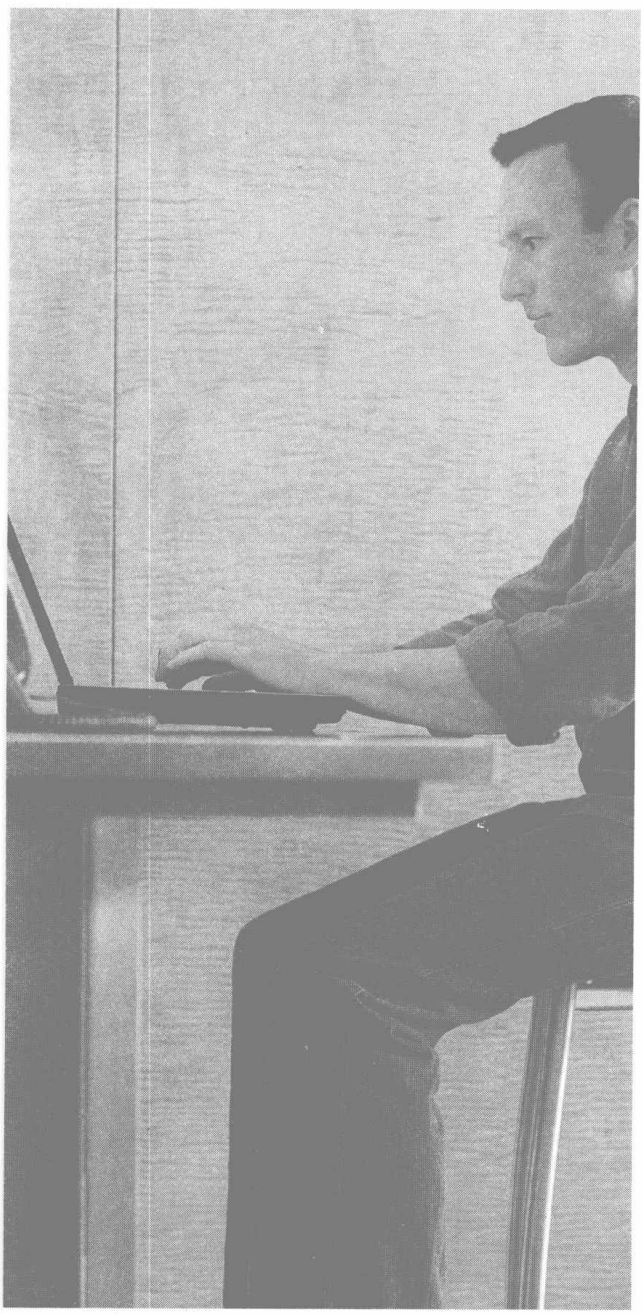
RFC 1583——开放式最短路径优先2（Open Shortest Path First 2）。

RFC 1654——边界网关协议4。

RFC 1723——路由信息协议2（Routing Information Protocol 2）。

RFC 1771——边界网关协议4（Border Gateway Protocol 4）最新版本。

RFC 1883——因特网协议v6（Internet Protocol, Version 6, IPv6）。



本章讨论网络架构框架和设计模型，包含以下主题：

- 7.1 延迟/时延
- 7.2 抖动
- 7.3 脉冲编码调制
- 7.4 语音压缩
- 7.5 回音
- 7.6 分组丢失
- 7.7 语音活动检测
- 7.8 数字到模拟的转换
- 7.9 串联编码
- 7.10 传输协议
- 7.11 拨号计划设计
- 7.12 端局交换机与 IP 电话呼叫流程
- 7.13 总结
- 7.14 参考书目

第7章

VoIP：深入分析

了解与网络拓扑有关的一切对设计一个好的网络是十分必要的。本章讨论了许多与VoIP有关的问题，以及思科是怎样解决这些问题的。

在公共交换电话网络上的通信有着它自己的问题，这些我们在第1章和第2章里有详细描述。VoIP技术也有相似的问题和很多其他的问题。本章详细讨论这些问题以及它们是怎样影响分组交换网络的。

我们将主要涉及以下几个问题：

- 延迟/时延（Delay/latency）；
- 抖动（Jitter）；
- 脉冲编码解调（Pulse Code Modulation，PCM）；
- 语音压缩（Voice compression）；
- 回音（Echo）；
- 分组丢失（Packet loss）；
- 语音活动监测（Voice activity detection）；
- 数据到模拟的转换（Digital-to-analog conversion）；
- 串联编码（Tandem encoding）；
- 传输协议（Transport protocols）；
- 编码设计（Dial-plan design）。

7.1 延迟/时延

VoIP的*延迟（delay）*或*时延（latency）*是由说话者开始说话到听者听到声音的这段时间。

在今天的电话网络中，有三种不可避免的延迟：*传播延迟（propagation delay）*，*序列化延迟（serialization delay）*和*处理延迟（handling delay）*。传播延迟是因为信号必须在光线或电缆网络上传输。处理延迟——也称为过程延迟（processing delay）——定义了许多造成延迟的原因（实际的打包时间、压缩和包交换等的时间），这类延迟是由网络中传输帧的设备造成的。

序列化延迟是将一位或一个字节传送到接口上的时间。因为序列化延迟的时间很少，本书将不做详细的介绍。

7.1.1 传播延迟

光在真空中的传输速度是每秒 186 000 英里，电子在同轴电缆或光纤上的传输速度大约每秒 125 000 英里。可绕地球一半（13 000 英里）的光纤网络可产生单向延迟 70ms。虽然人的耳朵几乎分辨不出这些时延，但是传播延迟与处理延迟一起将降低声音质量。

7.1.2 处理延迟

我们前面已经提到，网络中转发帧的设备造成处理延迟。在传统的电话网络中，处理延迟会造成一定的影响，但这个延迟在分组网络环境中尤为重要。在以下的各段里，我们将讨论不同的处理延迟，以及它们对声音质量的影响。

在思科的 IOS VoIP 产品中，数字信号处理器（Digital Signal Processor，DSP）在使用 G.729 时，每 10ms 产生一个语音样本。两个语音样本（每个都有 10ms 的延迟）被放在一个包中，所以每个包的延迟是 20ms。在使用 G.729 时，有一个 5ms 的初始延迟，这样，第一个语音帧有大概 25ms 的延迟。

生产厂商可以决定一个包中发送多少语音样本。因为 G.729 采用 10ms 的语音样本，每在帧中增加一个样本，就意味着增加 10ms 延迟。事实上，思科 IOS 允许用户选择每个帧中放多少个样本。

思科给予 DSP 更多形成帧的任务以保证路由器/网关负载较低。例如，实时传输协议（Real-Time Transport Protocol，RTP）的分组头，是放在 DSP 帧中，而不是由路由器来完成。

7.1.3 队列延迟

分组网络还有其他原因的延迟。其中的两个是将分组移到输出队列的所必需时间和序列化延迟。

当一个包因为输出接口阻塞而停留在队列中而造成的延迟，称为队列延迟。队列延迟在某段时间内发送出的包超出了接口的处理能力时产生。

输出队列里的队列延迟是造成延迟的另一种原因。您可以通过各种排队方式来优化您的网络使这个参数不超过 10ms。具体的细节请参照第 8 章。

ITU-T 的 G.114 建议书规定了好的语音质量单向端对端延迟应该不超过 150ms，如图 7-1 所示。使用思科 VoIP 实施，两个最小网络延迟（背靠背）的路由器间的端对端延迟只有 60ms。这就为将 IP 包从源转移到目的地预留了 90ms 的延迟。

如图 7-1 所示，有些延迟虽然较大，但因为没有其他可替代的，也只好接受。例如在卫星传送中，将数据发送给卫星大概需要 250ms，另一个 250ms 返回地球，总共需要 500ms 的延迟。虽然根据 ITU-T 建议这超出了语音质量的要求，但日常的很多会话是通过卫星链路完成的。所以，语音质量经常是以用户可以接受为标准的。

在缺乏管理，拥挤的网络中，队列延迟可能高到 2 秒（或者造成分组丢失）。对于大多数网络来讲，这种延迟是无法忍受的。队列延迟只是端对端延迟的一种，另一种影响端对端延迟的因素是抖动。

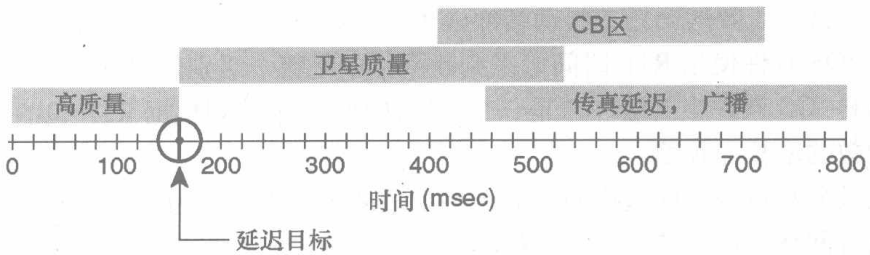


图 7-1 端对端延迟

7.2 抖动

简单来说，抖动（jitter）是指包到达时间的不规律。抖动是分组网络中的一个问题。在分组语音环境下，发送者希望语音包以稳定的间隔到达（比如每个分组间隔 20ms）。但这些包在网络上传输时可能不会以同样的间隔到达接收站点（比如，可能不是每 20ms 接收到一次，参见图 7-2）。分组期望到达的时间和包实际到达的时间之间的偏差就是抖动（jitter）。

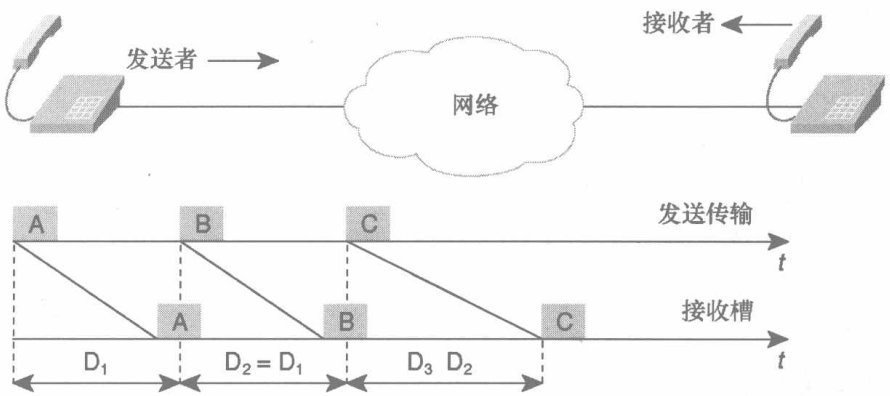


图 7-2 包到达时间的变化（抖动）

从图 7-2 中可以看出，包 A 与包 B 的发送和接收时间是一样的（D1=D2）。包 C 在网络中遇到延迟，所以比它期望的到达时间晚。这就需要一个抖动缓冲区（jitter buffer）来消除包到达时间的不规律。在 IP 网络中，语音包的到达间隔是很没有规律的。我们可以通过记录晚到达的包与成功处理的包的比例来调整抖动缓冲区的大小，以期达到一个合理的比例。缓冲区大小的调整对弥补延迟非常有效。

请注意虽然分组网络中的抖动可能会增加网络的整体延迟，但抖动和整体延迟不是同一回事。如果网络中有越多的抖动，就需要越大的缓冲区来弥补。

大多数的 DSP 不具有处理过分网络延迟的无限抖动缓冲区，所以有时丢弃包会比在抖

动缓冲区中产生更大的延迟要好一些。如果数据网络经过很好的设计，并预先作了预防，抖动一般不会是主要的问题，抖动缓冲区也不会减少太多的对端对端的延迟。

思科 IOS 软件使用 RTP 时间戳来判断网络中是哪个级别的抖动。

在思科 IOS 软件中的缓冲区是一个动态队列。这个队列根据 RTP 包的到达间隔时间可能会成指数的增长和收缩。

虽然大多数设备厂商选择使用静态抖动缓冲区，思科认为规划很好的动态抖动缓冲区是分组语音网络的最佳选择。静态抖动缓冲区不是过大就是过小，这就会因为过分分组丢失或延迟而造成音频质量的降低。思科的抖动缓冲区可以根据最后几包的到达延迟来调整抖动缓冲区的大小。

7.3 脉冲编码调制

虽然对于人类的交流来说，模拟信号非常理想，但模拟传输很难从线路的噪声中恢复出来。在最早的电话网络中，当模拟传输经过放大器时，放大语音的同时也放大了噪声。而这些线路噪声经常导致线路不可连接。

对于由 0 和 1 构成的数字采样来讲，分离噪声就容易多了。所以，当从数字样本中恢复模拟信号时，可以维持清楚的声音。当这种数字表示方法的好处被人们意识到的时候，电话网络到了*脉码调制（pulse code modulation，PCM）*时代。

7.3.1 什么是 PCM

如第 1 章所述，PCM 通过每秒 8 000 次的采样和量化，将模拟声音转化为数字形式。Nyquist 定理认为如果以最高频率的两倍的速率采样的话，你就可以将信号完整地恢复到模拟形式。因为大多数的声音都低于 4kHz，所以需要每秒 8 000 次的采样（每次间隔 125μs）。

7.3.2 卫星网络采样示例

卫星网络有 500ms 的延迟。这包括 250ms 到达卫星的时间和 250ms 回到地球的时间。在这种类型的网络中，因为带宽的消耗，分组丢失被严格控制。并且，如果有些语音应用已经运行在卫星链路上，这些服务的用户也习惯了有很大延迟的语音质量。

缺省情况下，思科 IOS 在每个包中传送两个 10ms 的 G.729 语音帧。虽然这对大多数应用是可接受的，但对于带宽昂贵的卫星链路，这不是最好的选择。每个包中都有包头，浪费了大量的带宽。在一个包中放的帧越多，需要的包头越少。

如果在每个分组中放 4 个 10ms 的 G.729 语音帧，就可以节省一半的包头。表 7-1 清楚地显示了每包不同帧数的比较。

在每个分组中增加 20 个字节（20 个字节相当于两个 10ms 的 G.729 样本），就可以多承载一倍的语音。

表 7-1 每包中的帧（G.729）

	IP/RTP/UDP	带宽	
每帧中的 G.729 样本	包头	消耗	时延*
缺省（每帧两个样本）	40 字节（byte）	24 000bit/s	25ms
卫星（每帧四个样本）	40 字节（byte）	16 000bit/s	45ms
低时延（每帧一个样本）	40 字节（byte）	40 000bit/s	15ms

*只包含压缩和打包时延

为了减少所有 IP/RTP/UDP 等的 54 字节头多带来的开销，可以将多个语音样本打包在一个以太帧中传送。虽然这可能会带来语音延迟，但增加每包中帧的数量可以提高整体的语音质量，尤其是在带宽紧张的情况下。

每帧中的语音样本数量取决于您选择的编码方式和带宽使用率和分组丢失影响力之间的平衡。每帧样本数越多，每个 UDP/RTP 包中携带的样本也越多，网络的其他开销也就降低了，从而带宽的使用率也就越高。分组丢失对声音质量的影响也会越高。

表 7-2 列出了一些常用编码方式所使用的值。

表 7-2 VoIP 编码器的每帧语音样本数

编码器类型	每帧语音样本数（缺省）	每帧语音样本数（最大）
PCMU/PCMA	2	10
G.723	1	32
G.726-32	2	20
G.729	2	64
G.728	4	64

7.4 语音压缩

两种经常使用的 64kbit/s 的 PCM 是 μ-law 和 a-law. 这两种方法相似之处在于他们都是使用压缩算法在 8 位中得到 12～13 位的 PCM 质量，只是在压缩细节上有着些许不同（μ-law 在低级别的信号噪声比的情况下有着轻微的优势）。历史上这两种 PCM 的使用是分国家和地域的 —— 北美使用 μ-law，欧洲和其他国家使用 A-law 调制。值得提出的是在长途呼叫中，如果需要 μ-law 到 A-law 的转换，是由 μ-law 的国家负责的。

另一种经常使用的压缩方式是自适应差分脉冲编码调制（adaptive differential pulse code modulation，ADPCM）ADPCM 的一个常用实例是 ITU-T 的 G.726。G.726 使用 4 位样本，传输速率为 32kbit/s。与 PCM 不同，4 位的 ADPCM 不直接编码声音的振幅，他们使用一些基本的线性预测来编码振幅的差异和振幅的变化速率。

PCM 和 ADPCM 是波形（waveform）编码器的例子——波形编码器是指使用波形冗余特性编码的压缩技术。在过去的 10～15 年里，通过进一步使用声音产生的源特性开发了一些

新的压缩技术。这些技术使用信号处理程序压缩声音，发送时只发送原始语音的简化特征信息，从而节省了带宽。

这一组技术可以称为源（source）编码器，源编码器包括线性预测编码（linear predictive coding，LPC），代码激励线性预测压缩（code excited linear prediction compression，CELP），以及多脉冲多级别量化（multipulse，multilevel quantization，MP-MLQ）等编码方法。

7.4.1 语音编码标准

ITU-T 在 G 系列建议书中标准化了 CELP，MP-MLQ PCM 和 ADPCM 编码方案。最流行的电话和分组语音的语音编码标准如下。

- G.711——描述了我们在前面大概介绍了的 64kbit/s PCM 语音编码技术；经过 G.711 编码后的语音已经可以在公共电话网上或 PBX 上作为数字语音传输。
- G.726——描述了在 40kbit/s、32kbit/s、24kbit/s 和 16kbit/s 速率上的 ADPCM 编码，如果 PBX 或公用电话网络由 ADPCM 功能，ADPCM 语音可以在这两个网络与分组语音网络之间互换。
- G.728——描述了 CELP 语音压缩的 16kbit/s 的低延迟版本。
- G.729——描述了可以将语音编码至 8kbit/s 流的 CELP 压缩技术；这个标准的两个版本（G.729 与 G.729 附件 A）在计算复杂度上差别很大，两种都可以提供与 32kbit/s ADPCM 一样的语音质量。
- G.723.1——描述了一种可以用于在低速率下压缩话音和其他多媒体音频信号的压缩技术，是 H.324 标准家族中的一部分。这个编码器有两种速率：5.3 和 6.3kbit/s。6.3kbit/s 是基于 MP-MLQ 技术，可以提供更高的质量。5.3kbit/s 基于 CELP，可以提供很好的质量，而且可以为系统设计者提供更多的自由。
- iLBC（因特网低比特率编码，Internet Low Bitrate Codec）——可以在 IP 上提供健壮的语音通信的免费话音编码。这个编码器是给窄带话音设计的。如果编码帧的长度是 30ms，那么该编码器的有效载荷为 13.33kbit/s，如果长度是 20ms，那么有效载荷为 15.20kbit/s。当 IP 包丢失或延迟时，可能会丢帧，iLBC 编码器可以平滑地过渡语音质量。该编码器的基本质量要高于 G.729A，在分组丢失时会更健壮一些。分组电缆（PacketCable）协会和许多厂商都已采用 iLBC 作为首选编码器。它也被用于许多 PC-to-Phone 应用，如 Skype、Google Talk、Yahoo Messenger 语音和 MSN Messenger。

7.4.2 平均意见得分

可以通过两种方式测试语音质量：主观的和客观的。人类可以执行主观语音测试，计算机（很难被可以欺骗人们耳朵的压缩方案愚弄）执行客观语音测试。

编码器是根据人们对语音质量的主观因素开发和调谐的。标准的客观质量测量，如总谐波畸变（harmonic distortion）和信号噪声比，与人们对语音质量的感觉是无关的，虽然人

们对语音质量的感觉是大多数语音压缩技术的最终目的。

用于定量话音编码器的性能的主观基准是平均意见得分（mean opinion score，MOS）。MOS 测试由一组听众完成。因为语音质量和声音都是针对听众的，所以广泛的选择听众和资料样本对于 MOS 测试是非常重要的。听众给每个语音样本打分（1（差）～5（优秀））。所有得分的平均值就是平均意见得分。

MOS 测试也经常用于比较一个编码器在不同环境下的表现，包括不同的背景噪声、多重编码解码等。然后您就可以使用这个数据和其他编码器进行比较了。

表 7-3 列出了 ITU-T 的几种编码器的分数。这张表比较了几种低比特率的编码器和标准 PCM 的关系。

表 7-3　　ITU-T 编码器 MOS 得分表

压缩方法	比特率（kbit/s）	样本大小（ms）	MOS 得分
G.711 PCM	64	0.125	4.1
G.726 ADPCM	32	0.125	3.85
G.728 低时延码激励线性预测（Low Delay Code Excited Linear Predictive，LD-CELP）	15	0.625	3.61
G.729 共轭结构——代数码激励线性预测编码（Conjugate Structure Algebraic Code Excited Linear Predictive，CS-ACELP）	8	10	3.92
G.729a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5.3	30	3.65
iLBC 免费软件	15.2	20	3.9
	13.3	30	

来源：思科实验室

iLBC 编码器——研究论文——在 VoIP 质量和带宽有效上的 FEC 与编码器健壮性的比较（COMPARISONS OF FEC AND CODEC ROBUSTNESS ON VOIP QUALITY AND BANDWIDTH EFFICIENCY）——WENYU JIANG AND HENNING SCHULZRINNE. 哥伦比亚大学，计算机系，美国（Columbia University，Department of Computer Science，USA.）

7.4.3 知觉语音质量测量

虽然 MOS 评分法判定语音质量的主观方法，但并不只有这一种办法。ITU-T 颁布了 P.861 建议书。该建议书覆盖了使用知觉语音质量测量（Perceptual Speech Quality Measurement，PSQM）客观确定语音质量的办法。

当使用语音编码器时（vocoders），PSQM 有许多缺点。其中的一个缺点就是“机器”或者 PSQM 听到的并不是人类耳朵感觉到的。用外行的话说，一个人可以使用特技使人类的耳朵感觉到高质量声音，但计算机不可能被特技欺骗。同样，PSQM 是被设计用于听取

由压缩和解压缩而不是分组丢失或抖动带来的损伤的，所以也不能完全模仿人的耳朵。

7.5 回音

当您访问大峡谷时，回音是一个有趣的现象。但在电话通话过程中的回音则会令人讨厌甚至不可忍受，使通话不清晰。

当您谈话正常，对方也清晰听到您的声音时，您在听筒里也听到自己的声音。如果您在听筒里听到自己的延迟超过 25ms，那就可能会造成中断使通话不流畅。

在传统的长途通信网中，回音经常是因为由四线网络到两线本地回路转换时阻抗不一致造成的。（参见图 7-3）。在标准的公用交换电话网络（PSTN）上，回音通过回音消除器和在相关点紧密控制电阻的不匹配来控制，如图 7-3 所示。

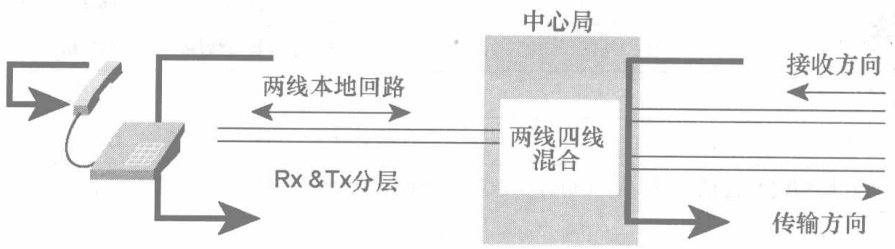


图 7-3 阻抗不一致造成的回音

回音有两大缺点：它可能会很大而且很长。回音越大越长，就会造成更恼人的回音。

在主要使用模拟语音的电话网络中，使用可以增大电路的电阻的回音抑制器来消除回音。这不是消除回音最好的办法，实际上还带来另外的麻烦。例如，在装有回音抑制器的线路上不能使用 ISDN，因为回音抑制其切掉了 ISDN 要使用的频率。

在今天的分组网络上，您可以在低彼特率的编码器上建立回音消除器，并在每个 DSP 上运行它们。一些厂商使用软件做回音消除器，但这大大降低了回音消除的好处。思科 VoIP 完全在它的 DSP 上实现回音消除。

在了解怎样消除回音之前，最好先了解回音是怎样产生的。

在我们的例子中，假设用户 A 正在与用户 B 交谈。用户 A 到用户 B 的语音为 G。当 G 碰到阻抗不一致或其他形成回音的情况时，它将弹回 A。当 A 说完一段话的数毫秒后，又听到了这段话。

要想从线路上消除回音，用户 A 使用的谈话设备（路由器 A）将 A 的话音的反转保留一段时间。这个话音称为反转话音（inverse speech）（–G）回应消除其听从用户 B 传来的声音，减去-G 则移去了所有的回音。

回音消除器局限于它们等待接受话音反射的总时间，这个现象称为回音尾（echo tail）。思科可以配置该值为 16ms、24ms、32ms、64ms 和 128ms。

在最初安装 VoIP 设备时，配置合适的回音消除是很重要的。如果不配备足够的回音消

除的话，呼叫方将在电话中听到回音。但如果配置过多的话，将占用更多的时间用来消除回音。

7.6 分组丢失

分组丢失在数据网络是很常见的，而且是可以预料的。实际上，大多数的数据协议根据分组丢失状况来判断网络状况，可以减少它们发包的数量。

在数据网络中承载重要流量时，控制网络中分组丢失的数量是十分重要的。

从 20 世纪 90 年代初期的系统网络体系结构（Systems Network Architecture，SNA）开始，思科系统已有了多年将业务重要的、时间敏感的流量放到了数据网络上的经验。对于像 SNA 那样不能容忍分组丢失的协议，需要建设一个可以给时间敏感数据早于其他数据处理的优先级，并能处理延迟和分组丢失的网络。

在将语音放到网络上时，建设一个可以成功、可靠、及时地传输语音的网络是至关重要的。而且，如果您有可以抵抗定期分组丢失的机制也是很有帮助的。

思科系统开发了许多服务质量（quality of service，QoS）工具来帮助管理员分类和管理数据网络上的流量。如果一个网络被很好的规划实施，您可以保证最小的分组丢失。

思科系统的 VoIP 实施可以使语音路由器相应定期分组丢失。如果在期待时间内的时候，没有接收到语音包（期待时间是可变的），就假设该报丢失，重放最后接收到的包，如图 7-4 所示。因为只丢失 20ms 的话音，一般的听众都不会注意到语音质量有了差别。

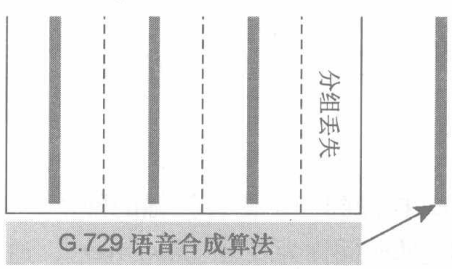


图 7-4 G.729 中的分组丢失

图 7-4 中使用思科的 G.729VoIP 实施，每一条线代表一个包。包 1、2、3 到达了目的地，包 4 在传输中丢失。接收工作站等待了一段时间（抖动缓冲区的时间）后执行*隐藏战略（concealment strategy）*。

隐藏战略重新播放接收到的最后一个包（在本例中，包 3），所以听者没有听到声音的间歇。因为丢失的话音只有 20ms，听者不可能听出区别。如果只丢失一个包，隐藏战略可以实现。如果连续丢失多个包，隐藏战略在接收到另一个包之前，只执行一次。

通过 G.729 的隐藏战略，就经验来讲，G.729 可以忍受整个呼叫的 5%的包丢失。

7.7 语音活动检测

在通常的谈话中，某个人讲话另一个人听。今天的电话网络包含一个双向的 64 000bit/s 的信道，不管是否有人在讲话。也就是说，在通常的通话中，至少 50%的带宽被浪费了。如果考虑到人们讲话过程中的中断和停顿，实际的带宽浪费更巨大。

而在使用 VoIP 时，如果采用语音活动监测（Voice activity detection，VAD），这部分被浪费的带宽也可以被利用起来。如图 7-5 所示，VAD 根据探测话音分贝（dB）的变化来决定是否该掐断语音帧的形成。

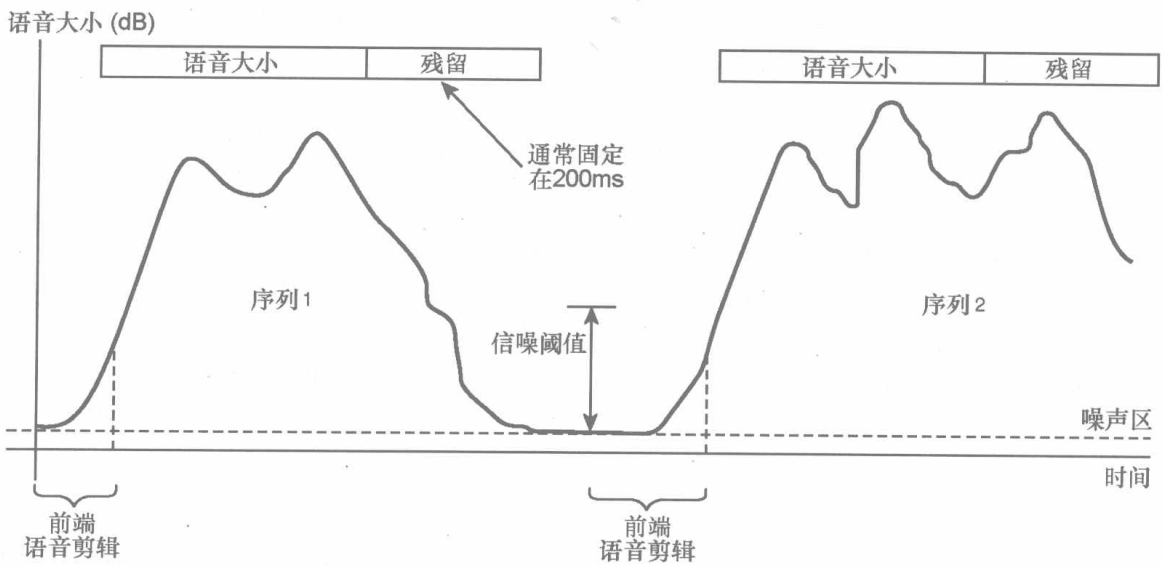


图 7-5 语音活动检测

通常情况是，当 VAD 探测到一个语音振幅的降落，它等待一段固定的时间，然后停止将语音帧打包。这段固定的时间称为*残留 (hangover)*，通常是 200ms。

对于任何一项技术，都是有长有短的。VAD 在判断语音结束开始，区分语音和背景噪声方面，有着固有的缺陷。这就意味着，如果你处于一个很吵的屋子，VAD 区分不出语音和噪声。这也被称为信噪阈值（signal-to-noise threshold）（参见图 7-5）在这些情景中，VAD 在呼叫开始的时候就失效了。

另一个 VAD 固有的问题是探测语音开始。通常一句话的开始被省略了（参见图 7-5）。这个现象被称为 front-end speech clipping。听讲者一般不会注意到开始被省略了。

7.8 数字到模拟的转换

数字到模拟的转换问题（D/A）目前是付费网络面对的主要问题。虽然第一世界国家的电话主干线几乎都是数字的了，但有时还会出现多次 D/A 转换。

每次从数字转为模拟再转换回去，语音或波形都会有些失真。虽然今天的付费网络在影响语音质量前可以处理至少 7 次的 D/A 转换，压缩语音在这些转换中就不那么健壮了。

值得一提的是，在压缩语音环境中，一定要紧紧控制 D/A 转换。在使用 G.729 时，只做两次 D/A 转换都会引起 MOS 分数的大大降低。唯一可以管理 D/A 转换的方法就是在设计 VoIP 环境时，尽量减少 D/A 转换的可能。

虽然 D/A 转换影响所有的语音网络，但在使用 PCM 编码器（G.711）的 VoIP 网络上，与在今天的电话网络上造成的影响是差不多的。

7.9 串联编码

如第 1 章所述，所有今天电路交换的网络都是以在数据链路层交换呼叫为前提的。电路交换器以层次模型管理，在这个层次模型中，高一级的交换机称为串联交换机 *(tandem switches)*。

串联交换机并不真正终结任一个本地回路，他们是作为*更高一层 (higher-layer)* 的电路交换机。在分层模型中，可能存在几层的电路交换机，如图 7-6 所示。这就使所有拥有电话者的端对端连接无需一条直接连接。

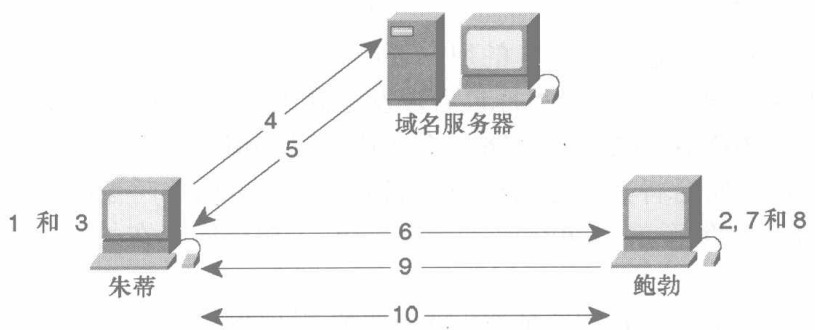


图 7-6 串联交换机层次结构

通常，对于一个穿越两个 TDM 交换机的语音呼叫，因为这些电路交换机之间采用 64kbit/s 信道连接，一个串联交换机不会导致语音质量的下降。

如果 TDM 交换机压缩语音，串联交换机必须解压缩和再压缩语音，语音质量将会受到彻底的影响。虽然在今天的 PSTN 网络中，压缩和解压缩不是那么常见，但您也必须在设计分组网络时考虑进去。

一个呼叫中，如果有超过一次的压缩/解压缩周期，语音质量就会大大下降。图 7-7 提供了一个这种场景会出现的例子。

图 7-7 描述了 3 个 VoIP 路由器被连接，并作为中心点 PBX 和 3 个远程 PBX 的直达线路。这个网络的设计是将所有的拨号计划信息放在中心点 PBX 上。这对于大多数保持拨号计划集中管理的企业来讲是很常见的。

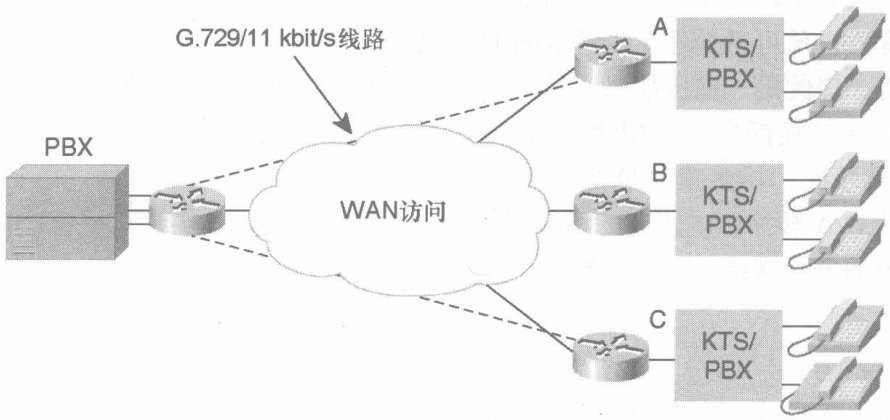


图 7-7 VoIP 串联编码

在 VoIP 中使用串联编码的一个缺陷是，当在分支 B 的用户要呼叫分支 C 的用户时，中心点 A 的两个 VoIP 端口要被使用到。这样就产生了两次压缩/解压缩周期，也就意味着声音质量将下降。

不同的编码器对串联编码的反应也不同。G.729 可以处理两次压缩/解压周期，而 G.723.1 对于多次压缩周期就缺少弹性。

举例来说，假设远程站点 B 的用户要呼叫远程站点 C 的用户。这个呼叫通过 PBX B，在 VoIP 路由器 B 被压缩和打包后被发送到中心站点 VoIP 路由器 A；A 解压缩呼叫，发送它到 PBX A。PBX A 电路交换该呼叫到 VoIP 路由器（路由器 A），路由器 A 压缩和打包该呼叫后将其发送到远程站点 C，在这里该呼叫被压缩发送给 PBX C。这个过程被称为*串联压缩（tandem-compression）*；在压缩存在的网络中一定要避免这种情况。

串联压缩容易避免。用户这种简化路由器配置的做法是以语音质量为代价的。思科 IOS 有另一种在简化拨号计划管理的情况下还能保持高语音质量的办法。

一种可能的方式是采用思科 IOS 多媒体会议管理器（Multimedia Conference Manager）（例如 H.323 的关守（Gatekeeper））。另一种方法是采用思科众多管理应用中的一种，如思科语音管理器（Cisco Voice Manager）来帮助配置和维护所有路由器上的拨叫计划。

还拿刚才 3 个 PBX 通过 3 个 VoIP 路由器连接的例子来看，只要改动路由器的配置，就可以简化呼叫流程避免串联压缩，如图 7-8 所示。

图 7-8 中，您可以发现 IP 的强大之处。不需要从电话公司租用直达线路就可以完成两个 PBX 间的呼叫。如果这些站点通过数据网络相连，那么 VoIP 就可以在整个网络上运行。

拨号计划由中心站点 PBX 移到了每个 VoIP 路由器上。这就使每个 VoIP 设备可以决定呼叫路由从而不需要直达线路。这个变化的最大好处就是消除了不必要的压缩/解压缩周期。

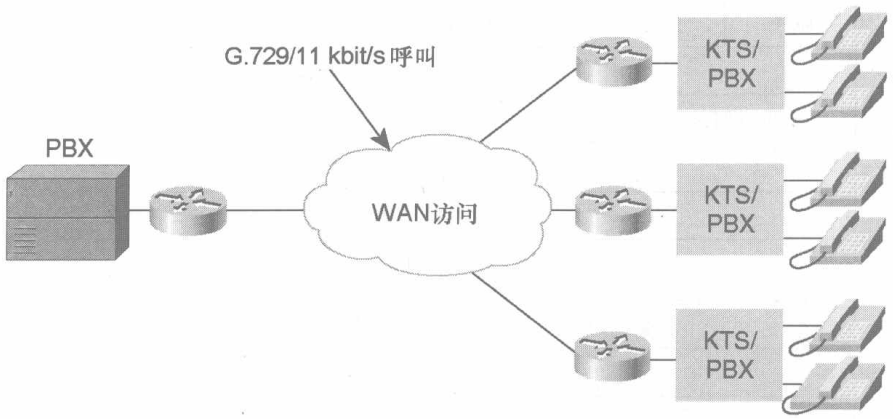


图 7-8 没有串联编码的 VoIP

7.10 传输协议

如第 6 章中讨论的一样，在因特网协议（Internet Protocol，IP）运行的两种流量为：用户数据报协议（User Datagram Protocol，UDP）和传输控制协议（Transmission Control Protocol，TCP）。通常情况下，当需要可靠连接时使用 TCP，当需要简单且不太关心可靠性时使用 UDP。

由于语音流量的时间敏感性，UDP/IP 是承载语音的合理选择。但是，按包发送的 UDP 不能提供所有的信息。因此，Internet 工程任务组（Internet Engineering Task Force，IETF）为实时或延迟敏感的流量采用了 RTP。VoIP 运行于 RTP 之上，RTP 运行在 UDP 之上。这样，VoIP 承载了 RTP/UDP/IP 的包头。

7.10.1 RTP

RTP 是在分组网络上传输延迟敏感流量的标准。RTP 运行在 UDP 和 IP 之上。RTP 为接收站点提供在无连接的 UDP/IP 流中没有的信息。如图 7-9 所示，两个重要的信息位是序列号和时间戳。RTP 使用序列信息判断包是否按顺序到达，使用时间戳信息判断包到达的间隔时间（抖动）。

您可以在按需点播应用中使用 RTP，也可以在如因特网电话等交互业务中使用。RTP（参见图 7-9）包含一个数据部分和一个控制部分，后者称为 RTP 控制协议（RTP Control Protocol，RTCP）。

RTP 的数据部分是一个瘦协议，为有实时特性的应用（像音频视频那样的连续媒体）提供了包括重建，分组丢失检测和内容识别等支持。

RTCP 为在因特网上任何规模的实时会议组提供支持。这些支持包括源识别和网关支持（如音频视频桥和多点导单点的转换等）。它同时向多点广播组提供接收者对 QoS 的回馈，以及对同步不同媒体流的支持。

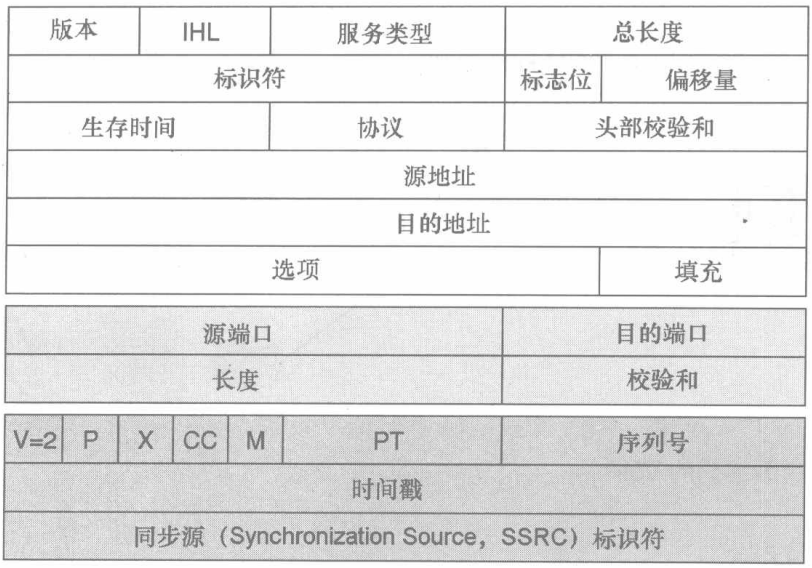


图 7-9 实时传输协议（RTP）分组头

另一个在 RFC 3611 种定义的新建议，RTP 控制协议扩展报告（RTP Control Protocol Extended Reports，RTCP XR）中提供了丰富的 VoIP 管理数据。扩展报告中的数据可以被如 VoIP 电话或网关中嵌入的 VQmon 技术提供，在呼叫过程中被定期发送以提供语音质量的实时回馈。报告中包含了有关网络分组丢失状况、RTP 往返延迟等大量的有用 VoIP 数据。

对于实时流量使用 RTP 是很重要的，但也有缺陷。IP/RTP/UDP 的报头分别是 20、8 和 12 个字节。这就增加了 40 个字节的包头，这是使用 G.729 两个样本（20ms）负载的两倍大小。您可以使用 RTP 包头压缩（RTP Header Compression，CRTP）技术将这个包头压缩到 2 或 4 个字节。CRTP 将在第 8 章介绍。

7.10.2 RUDP

可靠用户数据协议（Reliable User Data Protocol，RUDP）为无连接的 UDP 协议提供一些可靠性。RUDP 无需使用如 TCP 那样基于连接的协议而提供可靠性。RUDP 的基本方式就是传送多个同样的包，在接收站点丢弃不必要的或冗余的包。这样就增大了又一个包被接收的可能性。

这也被称为前向纠错（forward error correction，FEC）。根据带宽的不同，实施有不同的 FEC（要使用两倍或三倍的带宽）。如果有几乎无限的带宽，那么 FEC 是增强可靠性和语音质量的有价值的机制。

思科目前在 PGW2200 产品中使用了 RUDP。PGW2200 能够完成 7 号信令系统（Signaling System 7，SS7）到 IP 上的 Q.931 的转换。IP 上的 Q.931 是使用 RUDP 传输的。

7.11 拨号计划设计

在设计企业电话（Enterprise Telephony，ET）网络时，最让人头疼的是拨号计划定额设计。原因是集成各种不同网络要考虑各种复杂的问题，而且在设计网络时并没有考虑到集成问题。

这方面最好的例子就是当两个公司合并的时候。在这种场景下，公司的数据网（IP 编址，排序应用以及财产数据库）都必须合并。这两个公司在实施数据网络时几乎不可能采用同样的方式，所以也就带来了问题。

电话网络中也存在着同样的问题。如果两个公司合并，他们的电话系统（语音电话，记账，附加功能和拨号计划）都有可能与对方不兼容。

这些拨号计划问题也可能会发生在到一个公司决定要制定一个合适的拨号计划时。下面我们以公司 X 为例。公司 X 最近发展迅速，目前在全世界有 30 个站点，总部在达拉斯。公司 X 通过 PSTN 拨叫全部的 29 个站点。公司希望简化拨号计划，使其简单易用，促进员工之间的沟通。

在总部，公司 X 有一个大的 PBX，在其他远程分支使用小的 PBX。公司有如下选择。

- 在总部和所有站点之间租用（购买）专线。
- 向电话公司购买电话虚拟专用网络（Virtual Private Network，VPN），然后在各地拨叫接入号码以接入 VPN。
- 利用现有的数据网络设施，将声音在数据网上传输。

但不论公司 X 采用何种方式，它都面临着拨号计划设计、网络管理和费用等各种问题。

大多数公司根据以下问题决定他们的拨号计划，以避免涉及过多的细节：

- 增长计划；
- 专线或 VPN 的费用；
- 增加分组语音设备的费用；
- 号码重叠（当多个站点使用同一个号码时）；
- 呼叫流程（每个站点的呼叫模式）；
- 忙时间（在线路上出现最多呼叫的时间）。

根据公司的大小，拨号计划可以从 2 位扩展到 7 或 8 位数字。在没有弄清楚前面所列的问题之前，不要急于制定一个具体的计划，这是很重要的。

公司 X 将保持每年 20%～30%的增长，根据增长情况，公司 X 决定使用一个 7 位的拨号计划。这个选择也减少了号码重叠的可能性。

公司 X 将使用 3 位作为分支办公室编码，4 位作为实际用户线路号码。这样决定是因为公司认为它不可能拥有 999 个分支办公室。

> 注释：对于有几百个分支办公室的公司来说，通常有较多的分支办公室编码和较少的用户线。如果公司拥有几百个分支办公室，并且需要几千条用户线路，那么就必须使用更多的数字（也就是说，必须使用 8 位或 9 位数字拨号计划）。

7.12 端局交换机与 IP 电话呼叫流程

为了简化 TDM 或端局交换呼叫的流程和 IP 呼叫的流程，我们在本小节中假设您通过 PSTN 和因特网呼叫您隔壁的邻居。图 7-10 显示了使用目前 PSTN 的基本呼叫流程。将此与 IP 电话呼叫流程相比较，注意两者在建立呼叫过程中的相似性。

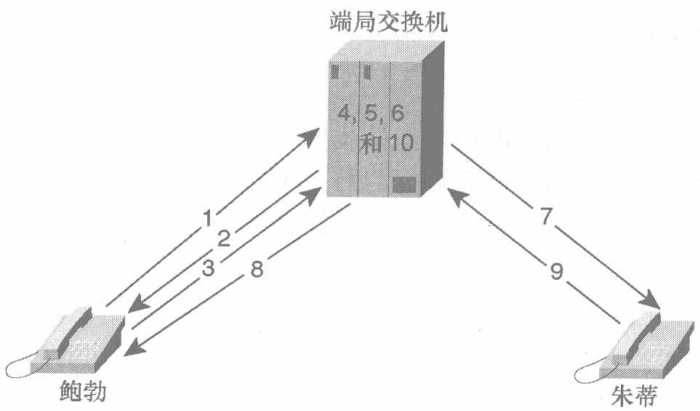


图 7-10 使用 PSTN 呼叫我的邻居

在这个例子中，鲍勃（Bob）要呼叫他的邻居朱蒂（Judy）。他们都是本地终端交换机的用户，所以 SS7 在这里是不需要的。此呼叫将遵从以下步骤。

1．鲍勃摘下电话听筒（摘机）。

2．本地端局交换机给鲍勃一个拨号音。

3．鲍勃拨叫朱蒂的 7 位电话号码。

4．端局交换机收集分析 7 位号码后决定呼叫的目的地。因为端局交换机的特定端口是分配给鲍勃的，所以端局交换机知道此呼叫是来自鲍勃家的。

5．交换机通过分析拨叫的 7 位号码来判断这是不是一个该交换机就可以处理的本地号码。

> 注释：如果不是同一个端局交换机为朱蒂提供服务，鲍勃的端局交换机通过查找它的路由表来决定怎样接通该呼叫。当连接朱蒂时，它可以增加前缀数字使该号码符合 E.164 标准。

6．交换机决定哪条是朱蒂的电话线。

7．决定后，端局交换机振铃朱蒂的电话。

8．一条端局交换机到鲍勃的语音路径接通，所以鲍勃可以听到终端交换机发送的回铃音调。这样鲍勃就知道朱蒂的电话正在振铃（朱蒂电话的振铃声和鲍勃的回铃声可能不同步）。

9．朱蒂摘下电话听筒（摘机）。

10．端局交换机接通鲍勃到朱蒂的语音路径。这是一条 64kbit/s 的，全双工的 DS-0（数

字服务，第 0 级）的端局交换线路提供此项服务。

图 7-11 演示了使用 PC 应用完成因特网电话呼叫的必要步骤。

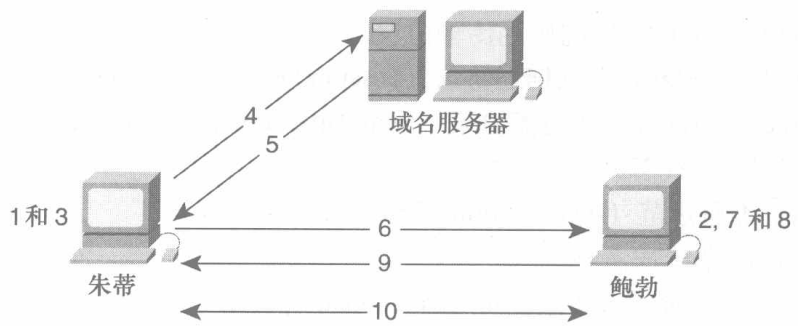


图 7-11 因特网到电话呼叫

鲍勃和朱蒂都需要在因特网上，或者他们之间通过 IP 网络连接才能相互交谈。假设他们已具备上述条件，那么他们将如下操作。

1．朱蒂启用她的因特网电话（I-phone）应用，该应用与 H.323 兼容。

2．鲍勃已经启动了他的 I-phone 应用。

3．朱蒂知道鲍勃的因特网“名字”，或者在域名系统（DNS）中叫 bob@nextdoorneighbor.com，于是她将其填入 I-phone 应用的“呼叫谁”栏目内按回车。

4．I-phone 应用将 Bob.nextdoorneighbor.com 转换为一个 DNS 主机名，查找朱蒂机器配置的 DNS 服务器将其转换为一个 IP 地址。

5．DNS 服务器将鲍勃的 IP 地址返回。

6．朱蒂的 I-phone 应用得到鲍勃的 IP 地址，发送一个 H.225 消息给鲍勃。

7．H.225 消息给鲍勃的计算机信号，使其振铃。

8．鲍勃电机接受按钮，他的 I-phone 应用发送 H.225 接受消息。

9．朱蒂的 I-phone 应用开始与鲍勃的 PC 进行 H.245 协商。

10．H.245 协商结束，逻辑信道打开。鲍勃和朱蒂现在就可以通过分组网络交谈了。

这个例子并没有演示所有的步骤，省略了服务供应商需要部署 VoIP 网络的细节。如第 6 章所述，因为 IP 是一个无处不在的网络协议，当呼叫被打包后，它可以被传送给您的邻居也可以传送给您远在挪威的亲戚。

7.13 总结

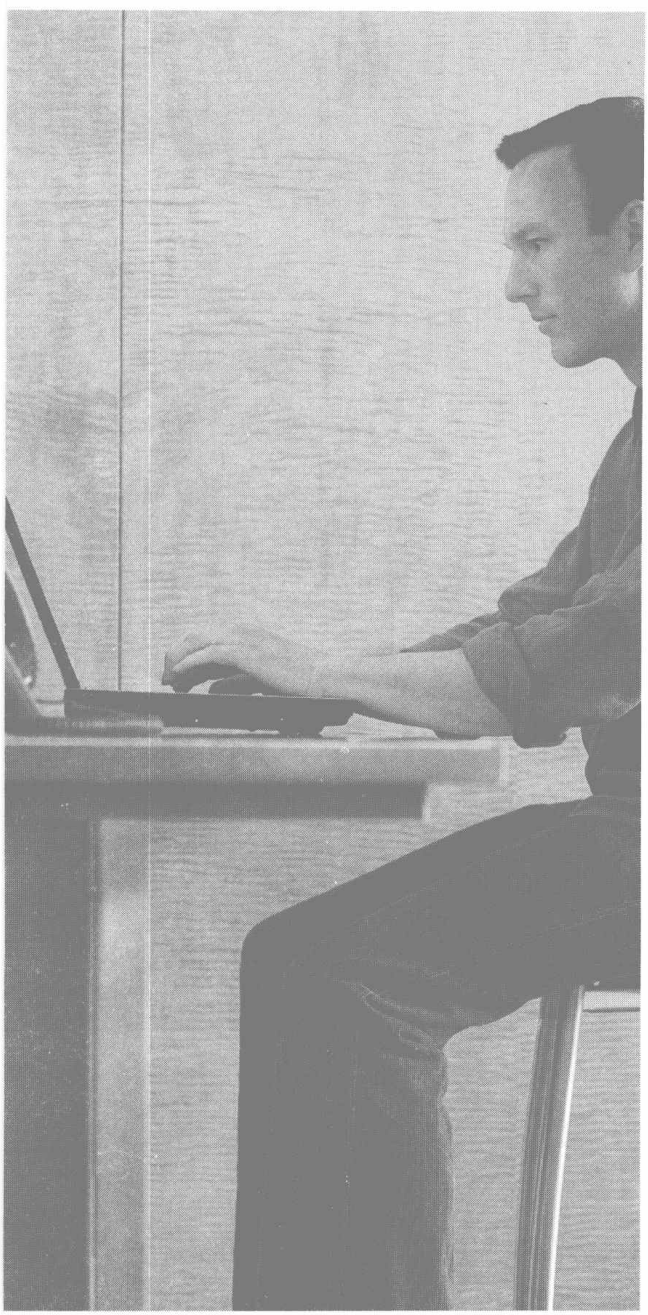
本章涉及了许多围绕 VoIP 的问题。这其中的许多问题，如压缩/解压缩语音帧、传播延迟，是 VoIP 所固有的问题，无法减少他们对 VoIP 网络的影响。

通过仔细考虑和网络设计，可以控制或避免一些问题，如抖动、整体延迟、处理延迟、采样速率、串联编码和拨叫计划设计等。

7.14 参考书目

下面是有助于研究 VoIP 的建议书

RFC 1889——RTP：实时应用传输协议
RFC 2327——SDP：会话描述协议（Session Description Protocol）
RFC 2326——RTSP：实时流协议（Real-Time Streaming Protocol）
ITU-T 建议书 H.323
ITU-T G. 编码规范（specifications for codecs）
ITU-T G.113 语音质量规范
ITU-T P.861 知觉语音质量测量（Perceptual Speech Quality Measure（ment）），PSQM
iLBC 编码——http：//www.ilbcfreeware.org/
RFC 3550——实时传输控制协议（Real Time Transport Control Protocol）
RFC 3611——RTCP 扩展报告（RTCP Extended Reports）



本章讨论网络架构框架和设计模型，包含以下主题：

- 8.1 QoS 网络工具箱
- 8.2 边缘功能
- 8.3 流量管制
- 8.4 主干网络
- 8.5 QoS 经验法则
- 8.6 思科实验室的 QoS 测试
- 8.7 总结

第8章

QoS

因为 QoS 有许多含义，服务质量（Quality of service，QoS）经常被用到，也经常被误用。在本书中，QoS 是指综合业务（Integrated Services，IntServ）和区分业务（Differentiated Services，DiffServ）中的服务质量。虽然这两种机制有很大的不同，IntServ 和 DiffServ 的基本目标都是为特定应用保证带宽与时间需求。

区分业务（DiffServ）经常使用在较大网络中，根据个人或集团的需求，来区分一个特定流或一组流量 QoS 合理级别。这是通过设置服务类型（Type of Service，ToS）字段或区分业务编码点（DiffServ Code Point，DSCP）完成的。

综合业务（IntServ）通常用来保证某个特定流量在被发送之前，该流量可以在通过整个网络传输后，被以某个 QoS 级别接收。IntServ（综合业务）通过资源预留协议（Resource ReSerVation Protocol，RSVP）完成。

为保证某个用户或应用的必要的 QoS，有大量的工具可以使用。本章主要讨论这些工具，什么时候使用他们，以及他们的一些潜在的缺陷。

值得注意的是，这些工具对于实施服务来讲，没有最终得到的结果重要。换句话说，就是在解决 QoS 问题时不要局限于 QoS 工具。应该做的是，将网络看成一个整体来判断哪个工具，如果有的话，属于网络中的哪一部分。

应当记住的是，越细粒度地控制网络，将增加信息技术（Information Technology，IT）部门的管理负荷，甚至超出他们的忍耐度。这些会再增加因为计算错误而使整个网络缓慢的可能性。

8.1 QoS 网络工具箱

在一个很好设计和实施的网络中，您需要很仔细地区分网络边缘功能和网络主干功能。这对于得到最佳 QoS 保证是非常重要的。

思科提供了许多实施 QoS 的工具。在许多情况下，您可以不使用 QoS 工具但仍能得到您应用所需要的 QoS。但在大多数情况下，每个网络都存在着需要一个或更多思科 QoS 工具解决的问题。本章讨论如下与网络边缘有关的工具。

- 附加带宽。
- 压缩的实时传输协议（Compressed Real-Time Transport，cRTP）。
- 队列（Queuing）：
  - 带权公平队列（Weighted Fair Queuing，WFQ）；
  - 定制队列（Custom Queuing，CQ）；

- 带优先级队列（Priority Queuing，PQ）；
- 基于类的带权公平队列（Class-Based Weighted Fair Queuing，CB-WFQ）；
- 带优先级的基于类的带权公平队列（Priority Queuing Class-Based Weighted Fair Queuing）。

■ 包分类：

- IP 优先/ToS/DiffServ；
- 路由策略；
- 资源预留协议（Resource Reservation Protocol，RSVP）。

■ 流量整形和策略：

- 通用流量整形（Generic Traffic Shaping，GTS）；
- 帧中继业务整形（Frame Relay Traffic Shaping，FRTS）；
- 承诺接入速率（Committed Access Rate，CAR）。

■ 分段（Fragmentation）：

- 多级多链路点对点协议（Multi-Class Multilink Point-to-Point Protocol，MCML PPP）；
- 帧中继论坛 12（Frame Relay Forum 12，FRF.12）；
- 最大传输单元（MTU）；
- IP 最大传输单元（IP Maximum Transmission Unit，IP MTU）。

本章也讨论了如下与网络主干有关的工具。

■ 快速排序：

- 加权随机早期检测（Weighted Random Early Drop/Detect，WRED）；
- 分布式等权排序（Distributed Weighted Fair Queuing，DWFQ）。

VoIP 有许多它自身的问题。就像在第 7 章分析一样，QoS 可以帮助解决这些问题中的一些——也就是分组丢失、抖动和处理延迟。（序列化延迟、传输各位到物理接口的时间不在本书中涉及）。

QoS 不能解决的问题有传播延迟（在打印这本书的时候，还没有能使光传得更快的方案问世）、编码延迟、采样延迟和量化延迟。

声音是一个传播至上的应用，需要大量的计划来保证符合相应的服务水平协议（service level agreement，SLA）。这些计划的一个元素就是理解应用中的延迟“预算”。有些延迟是可以被控制和调谐的，有些则是因为物理原因而不可改变的。参照图 8-1 可以知道可控制延迟预算的细节。

ITU-T 的 G.114 建议书建议维护好的语音质量的端对端延迟不超过 150ms。任何用户对“好”的可能多于或少于这个延迟，所以请记住 150ms 只是一个建议。

> 注释：“好”语音质量是相对于用户的经验和期望值的。有关 MOS 更广的讨论和*好*是怎样计算的包含本书的第 7 章中。

	固定延迟	可变延迟
编码延迟 G.729（预测5ms）	5 ms	
编码延迟 G.729（10ms每帧）	20 ms	
编码延迟中的打包延迟		
64kbit/s中继上的队列延迟		6 ms
64kbit/s中继上的序列化延迟	3 ms	
传播延迟（专线）	32 ms	
网络延迟（如，公共帧中继延迟）		
取消抖动缓冲区		2～200 ms
总计（假设抖动缓冲区为50ms）	**110 ms**	

图 8-1 端到端延迟预算

8.2 边缘功能

边缘功能通常被指定给服务商边缘（Provider Edge，PE）和客户边缘（Customer Edge，CE）设备。在设计一个 VoIP 网络时，本书中讨论的边缘 QoS 功能是与广域网（wide-area networks，WANs）相关的。WAN（广域网）的带宽比从中心点出来的 T1 或 E1 的带宽要小。当使用更高的边缘链路时，本章中描述的 QoS 机制就没有必要了。

注释：部署 QoS 机制或“会话控制”机制越来越平常了。这些机制可以允许各种用户策略在网络中实施。这些工作都是与本章中描述的 QoS 机制相关的。

8.2.1 带宽限制

在设计 VoIP 网络时的一大顾虑就是带宽有限。根据您采用的编码器以及在每个包中放的样本数的不同，每个呼叫要使用的带宽可能会急剧增加。有关分组的大小和消耗的带宽，参见表 8-1。

表 8-1 编码器和样本数对带宽的影响

编码器	带宽消耗	cRTP（2 字节包头）带宽消耗	采样等候时间
G.729 w/ 1 个 10ms 样本/帧	40 kbit/s	9.6 kbit/s	15ms
G.729 w/ 4 个 10ms 样本/帧	16 kbit/s	8.4 kbit/s	45ms
G.729 w/ 2 个 10ms 样本/帧	24 kbit/s	11.2 kbit/s	25ms
G.711 w/ 1 个 10ms 样本/帧	112 kbit/s	81.6 kbit/s	10ms
G.711 w/ 2 个 10ms 样本/帧	96 kbit/s	80.8 kbit/s	20ms

看过这张表后，您可能会问，为什么 8kbit/s 的编码器要使用 24kbit/s 的带宽。这个

现象的产生是因为“IP 税”。G.729 编码器使用两个 10ms 的样本消耗 20 字节每帧，这些是不在 8kbit/s 之内的。包头包括 IP、RTP 和 UDP，为每帧增加 40 个字节。这个“IP 税”包头是负载的两倍。

以使用两个 10ms 的样本的 G.729 为例，没有 RTP 包头压缩的话，呼叫的每个方向都要消耗 24kbit/s 的带宽。这对于 T1(1.544mbit/s)、E1 (2.048mbit/s)或更快的链路来讲没有什么，但它是 54kbit/s 线路的一大部分（42%）。

另外，需要注意的是，表 8-1 中的带宽没有包含第 2 层包头（PPP、帧中继（Frame Relay）等）。它只包含了第 3 层以上的包头。这样，当使用不同的数据链路（以太网、帧中继、PPP 等）时，同样的 G.729 呼叫消费的带宽不同。

8.2.2 cRTP

为了减少 G.72 语音呼叫消耗的点对点广域网链路带宽，您可以使用 cRTP。cRTP 在大多数情况下，可以将 40 字节（Byte）的 IP/RTP/UDP 包头压缩到 2 到 4 个字节（参见图 8-2）。

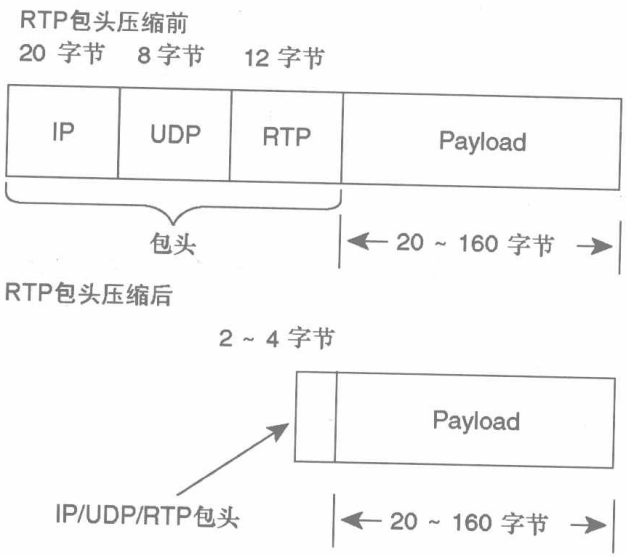


图 8-2 RTP 包头压缩

通过使用 cRTP，每个 VoIP 呼叫流量从 24kbit/s 降到了 11.2kbit/s。这对于低带宽链路来讲，是一个很大的改进。比如，一条 56kbit/s 的链路现在可以承载 4 个 11.2kbit/s 的 G.729 VoIP 呼叫。如果没有 cRTP 就只能承载两个 24kbit/s 的 G.729VoIP 呼叫。

为了避免无必要的带宽消耗，cRTP 被一条链路一条链路地使用。这个压缩方案在不使用 UDP 校验和时，可将 IP/RTP/UDP 包头减至 2 个字节，使用 UDP 校验和时，可减至 4 个字节。

cRTP 使用了与传输控制协议（TCP）压缩一样的技术。在 TCP 包头压缩中，帮助降低数据速率的两个因素，第一个是在 IP 和 TCP 包头中有一半的数据在整个连接中是保持

不变的。

另外一个因素则可以缩减更多，那就是虽然每个包中的几个字段都发生了改变，但包与包之间的区别是固定的。所以，该算法可以简单地在每个接收到的值上加 1。通过维护未压缩的包头，以及压缩和解压缩器共享会话状态的一阶差分，cRTP 只有二阶差分为 0 时才能通信。在这种情况下，解压缩器只需要在每次接收到压缩包时，在保存的未压缩的包头上添加一阶差分就可以重建原始的包头，没有任何信息丢失。

如 TCP/IP 包头压缩机制维护同步的多个 TCP 连接共享状态一样，IP/RTP/UTP 压缩也需要维护多个会话状况下的状态。一个会话上下文（session context）由 IP 源和目的地址、UDP 源和目的端口、RTP 同步源（RTP synchronization source，SSRC）字段联合定义。在实施压缩时可能会使用一个基于这些字段的哈希函数来索引存储会话上下文的表。

在压缩包中承载着一个小整数，称为*会话上下文标识符（session context identifier）*或 CID，来表示该包应该使用哪个会话上下文来解释。解压缩器可以使用 CID 来索引存储会话上下文的表。

在大多数情况下，cRTP 可以压缩 40 字节的包头到 2 至 4 字节。同样，98%的时间是发送压缩包的。然而，一个完整的未压缩包必须被定期发送以校验双方拥有正确的状态。有时，在通常固定的字段也会发生改变——例如负载类型字段。在某些情况下，IP/RTP/UDP 包头不能被压缩，所以也必须发送未压缩包头。

cRTP 应该被用在带宽有问题和有大量 RTP 流量存在的广域网接口。下列思科 IOS 软件相关配置提示显示了在串口和帧中继接口启用 cRTP 的方法。

例 8-1　在串口和帧中继接口启用 cRTP

```
Leased line
!
interface serial 0
  ip address 192.168.121.18 255.255.255.248
  no ip mroute-cache
  ip rtp header-compression
  encapsulation ppp
!
```

```
Frame Relay
!
interface Serial0/0
  ip 192.168.120.10 255.255.255.0
  encapsulation frame-relay
  no ip route-cache
  no ip mroute-cache
  frame-relay ip rtp header-compression
!
```

在高速接口不应该使用 cRTP，因为这样做的缺点多于优点。“高速网络”是一个相对的术语：一般任何高于 T1 或 E1 的速度都不需要 cRTP。是否需要压缩取决于传输链路费

用和压缩费用的比较。如果您乐意为压缩/解压缩和可能需要的附加硬件支付费用，那么压缩可以工作在任何传输链路上。

对于任何压缩，CPU 都要处理压缩包，导致更多的处理任务。这就增加了边缘设备的 CPU 使用率。因此，您必须考虑优点（低带宽）和缺点（高 CPU 利用率）之间哪个更重要。如果边缘设备的 CPU 利用率过高可能会导致其他问题。所以，保持 CPU 利用率少于 60%～70%是保持网络顺利运行的一个定律。

8.2.3 队列

队列本身是一个简单的概念。最简单的办法就是将队列和高速公路系统相比较。假设您驾驶在新泽西的收费公路上。当您经过一个收费站时，您必须减慢速度，停下来，付费。因为付费需要时间，一些车辆停下来等候，结果造成拥挤。

在收费站线上，存在一个先进先出（first in，first out，FIFO）队列，这就意味着如果您第一个到达，也将第一个离开。FIFO 队列是路由器使用的第一种队列方式，并且在某些网络拓扑上，它仍在使用。

今天的网络，及其上面的各种应用、协议和用户，需要一个区分不同流量的方法。回到刚才收费站的例子，一个特殊的可以使某些车辆开到前面去的车道是必须的。比如在新泽西和其他地方的许多收费公路上，有一条公用汽车车道或者一条可以电子付费的车道。

与其相类似的是，思科有几个队列工具可以使网络管理员指定哪一种流量比较“特殊”或重要，在排队的时候根据的是信息而不是包到达的时间。在排队技术中，最流行的是 WFQ。如有您使用的是思科路由器，最有可能使用的是 WFQ 算法。WFQ 算法是接口小于 2Mbit/s 的路由器的缺省算法。

1. 带权公平队列

FIFO 队列将所有到达的包都放在一个队列中，然后根据带宽情况依次发送。WFQ 则将流量分别使用多个队列，给予每个队列相同的带宽。这就防止了一个应用，如文件传输协议（File Transfer Protocol，FTP），消耗所有有效带宽。

WFQ 保证队列不独占带宽，流量可以得到预期的服务。小量数据流可以在一定时间内被传输以得到预期的服务。大量数据流则共享剩余带宽，获得平均或按比例的带宽。

WFQ 与时分多路复用（time-division multiplexing，TDM）类似，它为各数据流平均分配带宽，这样就没有应用独占带宽。而且 WFQ 要比 TDM 更高级一些，在某个流不再存在的时候，WFQ 可以动态调整，为仍在传送的剩余流量重新分配带宽。

公平队列根据几个因素动态确认数据流，根据数据流消费的带宽分配给数据流不同的优先级。这个算法可以在不使用接入列表或其他耗时的管理任务的情况下，公平分配带宽。WFQ 根据源和目的地址、协议类型、插口或端口号和 QoS/ToS 值来确定一个数据流。

公平队列使组成总流量的大部分低带宽应用按需使用带宽，高带宽的应用在公平的方

式下共享剩余带宽。公平队列减少了抖动，使所有应用有效地共享了有效带宽。

在思科 IOS 中，WFQ 使用快速交换路径。它可以使用 **fair-queue** 命令启用，且从思科 IOS 11.0 开始，在低于 2.048Mbit/s 的串口缺省配置是启用的。

WFQ 中的权值受到 3 种机制的影响。IP 优先（IP Precedence），帧中继前向显式拥塞通知（Frame Relay forward explicit congestion notification，FECN），后向显式拥塞通知（backward explicit congestion notification，BECN）以及可选择丢弃（Discard Eligible，DE）位。

IP 优先字段取值范围为 0（缺省值）～7。这个值越高，算法为其分配的带宽也越多。也就使该数据流被传输的更频繁。有关 WFQ 权值的更多信息请参见后面的 8.2.4 节。

在帧中继网络中，FECN 和 BECN 位通常是出现阻塞的标志。当阻塞出现时，算法中的权值就发生了改变，那么出现阻塞的数据流就会少传输一些。

在一个接口启用 WFQ，使用 **fair-queue** 接口配置命令。

在一个接口禁用 WFQ 时，使用这个命令的“不（no）”形式。

```
fair-queue [congestive-discard-threshold [dynamic-queues [reservable-queues]]]
```

- *拥挤丢弃阀值（congestive-discard-threshold）*——（可选）在每个队列中允许的消息数。缺省是 64 个消息，新的阀值必须是在 16～4096 范围内的 2 的指数值。当一个会话到达这个阀值时，新的消息包将被丢弃。
- *动态队列（dynamic-queues）*——（可选）最佳效果会话所需要的动态队列数。（也就是一个普通的不需要特殊网络服务的会话）。这个字段的值一般是 16、32、64、128、256、512、1 024、2 048 和 4 096。缺省为 256。
- 保留队列（reservable-queues）——（可选）为保留会话预留的队列数，值的范围在 0～1000 之间，缺省为 0。保留队列被使用在配置了如 RSVP 功能的接口上。

网络管理员必须留意 WFQ 中的权值被合理的设置。以防止某个流氓应用请求或使用高于它应该得到的优先级。怎样避免不合理的权重流将在 8.2.4 节讨论。

WFQ 不适于在高于 2.048Mbit/s 的接口使用。有关这些接口的队列技术，参见 8.4.1 节。

2．定制队列

定制队列（Custom queuing，CQ）允许用户为特定协议指定一定比例的带宽。最多可以定义 16 个输出队列。每个队列以轮叫（round-robin）方式调度，传输一定比例的流量后转到下一个队列。

由路由器根据接口的速度和配置流量的百分比决定每个队列传输多少字节的流量。换句话就是说，队列 A 完成它需要的正百分比后，其他类型的流量可以使用其没被使用的带宽。

例 8-2 显示了在串口上启用 CQ 的方法。您必须首先定义队列列表的参数，然后在物理接口（本例中，串口 0（serial 0））上启用队列列表。

例8-2 在串口上启用定制队列

```
Interface serial 0
ip address 20.0.0.1 255.0.0.0
custom-queue-list 1
!
queue-list 1 protocol ip 1 list 101
queue-list 1 default 2
queue-list 1 queue 1 byte-count 4000
queue-list 1 queue 2 byte-count 2000
!
access-list 101 permit udp any any range 16380 16480 precedence 5
access-list 101 permit tcp any any eq 1720
```

CQ 需要知道端口类型和流量类型。这就等于大量的管理任务。但是一旦这些任务完成后，CQ 提供一些客户所希望的高细粒度的队列。

3. 优先级队列

PQ 允许网络管理员配置 4 种流量优先级——高、普通、中等和低。内部流量被分配到这四个输出队列中的一个。高优先级队列中的数据都被传输完成后，才传输低一级队列中的包。

这种队列管理保证重要的数据总是被给予足够的带宽的同时，避免其他应用也这样做。

所以，在使用这种队列技术的时候，一定要特别了解流量，以避免应用独占带宽。PQ 最好用在高优先级的数据流只占用很少一部分带宽时。

例 8-3 演示了使用访问列表（本例中是 access-list 101）指定 UDP 和 TCP 端口范围，将 priority-list 1 应用在 access-list 101 上使其成为 PQ 中的最高优先级队列。然后再串口 1/1 使用命令 priority-group 启用 priority-list 1。

例8-3 为流量使用访问列表指定UDP/TCP端口范围

```
!
interface Serial1/1
  ip address 192.168.121.17 255.255.255.248
  encapsulation ppp
  no ip mroute-cache
  priority-group 1
!
access-list 101 permit udp any any range 16384 16484
access-list 101 permit tcp any any eq 1720
priority-list 1 protocol ip high list 101
!
```

PQ 使网络管理员可以“饿死”应用。没有配置好的 PQ 只服务一个队列，丢弃所有其他队列。这就可能造成一些应用停止工作。在系统管理员意识到这个问题的严重性时，就

可以合理配置 PQ 使其成为最佳选择。

4. CB-WFQ

CB-WFQ 拥有 WFQ 的所有优点，并可以为网络管理员提供提供细粒度的支持——定义流量类。CB-WFQ 可以运行在高速接口上（最高到 T3）。

CB-WFQ 允许您根据超出流量界限的标准来定义类。在 CB-WFQ 中，您可以专门为语音流量建立一个类。网络管理员通过访问列表定义这些流量类。这些流量类决定包怎样分组到不同队列中。

CB-WFQ 最值得一提的特点是允许网络管理员为各类流量精确分配带宽。它可以处理 64 个不同的类并控制各类所需的带宽。

标准的 WFQ 中，权重决定每个对话所分配的带宽。带宽的分配跟某一时刻流量产生的多少有关。

而在 CB-WFQ 中，每个类都关联到一个分离的队列。您可以使用链路带宽的百分比或 kbit/s 值为一个类分配一个最小的保证带宽。其他类按照它们权重的比例共享没被使用的带宽。在配置 CB-WFQ 时，应该考虑带宽分配并不一定意味着属于一个类的流量经历了低延迟，而且可以调整权重仿真 PQ。

5. CB-WFQ 中的 PQ（低延迟队列（Low Latency Queuing，LLQ）

CB-WFQ 中的 PQ（PQ within CB-WFQ，LLQ）是一个拗口的缩语。这个机制在一个接口上给予语音流量绝对的优先级。

LLQ 功能为 CB-WFQ 带来了 IP RTP 优先级所需的绝对优先级队列功能。IP RTP 优先级为像语音那样延迟敏感，实时流量提供优先级。LLQ 允许使用绝对优先队列（strict PQ）。

虽然在一个绝对优先队列中排队所有类型的流量是可行的，但强烈建议您只将语音流量放在这个队列中。之所以这样建议是因为语音流量行为规范，定期发送包。而其他应用是不定期发送包，如果配置不当，则有可能毁掉整个网络。

通过 LLQ，可以在最大范围内定义流量，保证严格优先发送。可以使用访问列表来在严格 PQ 中指定语音流量排队。这与 IP RTP 优先不同，IP RTP 优先只允许特定的 UDP 端口范围。

虽然这个机制对于 IOS 来说相对较新，但已经被证明是强有力的。它给予语音包好的语音所必需的优先级、响应时间和抖动控制。

6. 队列总结

虽然目前还没有能满足所有需求的队列技术，很多人使用 WFQ 来解决队列问题。WFQ 很容易部署，也不需要网络管理员太多的精力。为 WFQ 设置权重可以增强它的功能。

如果需要更细粒度和更严格的队列技术可以使用 CQ 或 PQ。但是在使用这些技术时要多加小心，因为您可能会损坏您的网络。使用 PQ 或 CQ 时，您必须对网络上的流量和应用非常熟悉。

大多数人在低带宽（小于 768kbit/s）环境部署 VoIP 网络时，使用 IP RTP 优先或 LLQ 使语音流量优于其他流量。

8.2.4 包分类

您必须知道怎样合理地为 WFQ 分配权重以获得想要的包传送状况。本小节集中讨论几种分配权重的技术，以及在各种网络上使用它们以获得所需 QoS 的方法。

1. IP 优先权（IP Precedence）

IP 优先权是指 IP 包头中的 ToS 字段中的三位，如图 8-3 所示。

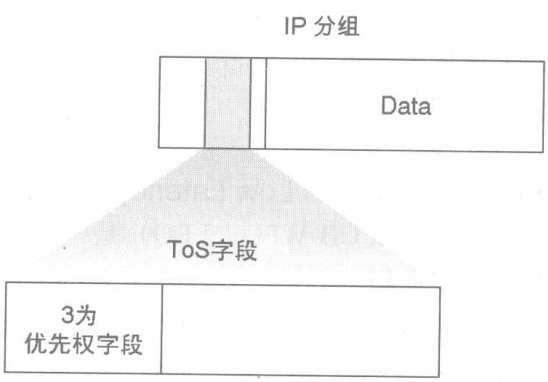


图 8-3 IP 包头和 ToS 字段

这三位允许八种不同的 CoS 类型（0～7）如表 8-2 所列。

表 8-2 ToS（IP 优先权）

服务类型	目的
日常事务	设置日常事务优先权（0）
优先	设置优先优先权（1）
即时	设置即时优先权（2）
Flash	设置 Flash 优先权（3）
Flash-override	设置 Flash override 优先权（4）
紧急	设置紧急优先权（5）
因特网	设置因特网控制优先权（6）
网络	设置网络控制优先权（7）

IP 优先权的 6 和 7 网络信息保留（路由更新、欢迎包（hello packets）等）。这样通常的 IP 流就有 6 种优先权。

IP 优先权可以使路由器根据 8 种优先权设置类分组流量，根据这个信息以及源地址、目的地址、端口号等来排队。

您可以将 IP 优先权看作是带内 QoS 机制。因为 IP 优先权不存在额外的信令和附加的包头负载，所以被广泛地采用。

在思科 IOS 中，有几种方式可以设置 IP 优先权。使用思科 VoIP 设计，可以根据电话号码（被叫号码）来设置 IP 优先权。使用这种方式设置优先权比较简单，而且根据呼叫的目的地的不同，还允许不同类型的 CoS。

注释：使用思科 IOS VoIP 设置 IP 优先权，如下操作：

```
dial-peer voice 650 voip
 destination-pattern 650
 ip precedence 5
 session target RAS
```

思科 IOS 也可以为任何经过路由器的 IP 流量根据访问列表或扩展的访问列表来设置优先级。这是通过一个称为*策略路由选择（policy routing）*的功能完成的。这项功能将在本节稍后介绍。

2. IP 优先权限定

IP 优先权没有拒绝不正确优先权设置的内在机制。网络管理员需要提高警惕以保证 IP 优先权是按计划设置的。下面的例子显示了如果 IP 优先权没有被仔细设置而出现的问题。

公司 B 在它所有的广域网（WAN）链路上使用 WFQ VoIP，并采用 IP 优先权来区分网络流量的优先次序。公司 B 为 VoIP 使用优先权设置 5，系统网络体系结构（Systems Network Architecture，SNA）流量使用 4。所有其他流量假设都使用优先权设置 0（最低优先权）。

虽然大多数应用的优先权是 0，但有些应用可能会被修改要求高一些的优先权。在这个例子中，一个软件工程师修改了他的游戏应用，要求使用优先权 7（最高设置）。这样当他和在另一个办公室的同事打游戏时，可以得到广域网（WAN）链路的最高优先级。虽然这只是个例子，但很可能发生。因为游戏程序需要大量的带宽，公司的 VoIP 和 SNA 流量无法通过。

如果使用工作区设置问题就会变得简单。您可以使用思科 IOS 将所有来自非许可主机的优先权位置 0，而保留其他流量不变。在本节稍后将作进一步讨论。

3. 通过策略路由选择重置 IP 优先权

配置路由器以重置 IP 优先权位（在网络边界这是一个很好的主意），您必须遵从以下步骤。在例 8-4 的配置建立了 **access-list 105** 以重置所有来自以太网的 IP 优先权位。只有在以太网口接收到的流量被发送到路由映射，在以太网口转发出去的流量不被处理到路由映射。

例 8-4 使用访问列表重置 IP 优先权位

```
!
interface Ethernet0/0
 ip address 192.168.15.18 255.255.255.0
 ip policy route-map reset-precedence
!
!
access-list 105 permit ip any any
route-map reset-precedence permit 10
  match ip address 105
  set ip precedence routine
```

4. 策略路由选择（Policy Routing）

使用基于策略的路由选择，您可以为流量配置一个定义好的策略，而不必完全依靠路由选择策略来决定流量的转发和路由选择。策略路由选择还允许您设置 IP 优先权字段，这样网络就可以使用不同级别的服务。

您可以使策略基于 IP 地址，端口号，协议或包的大小。您可以使用其中的一个描述符来建立一个简单的策略，或者使用全部建立一个复杂的策略。

一个接口启用基于策略的路由选择后，它所接收到的所有包都将通过一个增强的包过滤器。这个包过滤器称为*路由映射（route map）*。路由映射决定包将转发到何处。

您也可以标注 **route-map** 语句为**允许（permit）**或**禁止（deny）**。如果这个语句被标注为 **deny**，所有匹配的包都将会被发送回通常转发信道（换句话说，就是执行给予目的地的路由选择）。只有在这个语句被标注为 **permit** 时，所有匹配的包才被应用 set 子句。

如果该语句被标注为 **permit** 但包没有符合条件时，这些包也会通过通常通道转发。

> 注释：策略路由选择定义在接收包的接口，不是发送包的接口。

您可以使用 IP 标准的或扩展的访问控制列表（extended access control lists，ACLs）来建立匹配条件。标准的 IP 访问列表为源地址定义匹配条件，扩展的访问列表基于应用、协议类型、ToS 和优先权定义匹配条件。

匹配子句功能被扩展到可以在定义的最大值和最小值之间匹配包的长度，这样网络管理员就可以通过匹配长度来区分交互式流量和大流量（大流量通常包也比较大）。

策略路由选择处理整个路由映射，直至找到一个匹配。如果没有在路由映射中找到匹配，或者路由映射条目被标注为 **deny**，执行普通的基于目的地路由策略。

> 注释：在 **match** 语句列表的最后，总是一个 **deny** 语句。

必须仔细选择使用的路由策略类型，因为您可能会配置某个策略强制思科 IOS 路由器使用处理交换路径（这种方式要比转发包慢）。如果您足够仔细，就会避免这些。而且，缺省情况下，起源于路由器的流量也不会通过策略路由发送。使用一个特殊的命令，您可以通过策略路由发送内部流量（路由选择更新、VoIP 等）。

5. RSVP

RSVP（资源预留协议）允许端点为某个特定应用向网络提出某种需要的 QoS。这与网络盲目地假设应用所需的 QoS 正好相反。

网络管理员可以使用 RSVP 作为*动态访问列表（dynamic access lists）*。这就意味着网络管理员不必关心 IP 流的端口号，因为 RSVP 在最初的请求中会包含这些信息。

RSVP 是带外的，端对端信令协议，它需要一定的带宽和每个支持 RSVP 的网络跳上的响应时间。如果网络节点（路由器）不支持 RSVP，RSVP 直接转到下一跳。网络节点可以根据服务所要求的接口的负载来决定允许或禁止预留。

RSVP 工作模式就像救护车清除您前面的流量一样。您只需跟在救护车后面就可以了。RSVP，或者救护车司机，告诉每个站点（收费站，警察，等等）在他后面驾驶 1972 年的黄色 AMC Gremlin 的人非常重要，需要特殊的优先权。每个站点有权利决定 1972 年的黄色 AMC Gremlin 的驾驶者是否足够重要，可以享受哪些特权（比如说，不付路费，忽略交通灯，或者，在 IP 情况下，享有带宽和响应时间的界限）。

注释：在思科 IOS 中，每个需要 RSVP 的接口必须明确配置。而且，网络管理员必须配置该端口的带宽分配给 RSVP。

应用得到有关他们的 QoS 请求是否被批准的反馈。一些应用向任何人发送数据，不关心 QoS；但是，一些智能应用选择不发送或选择其他路径。对于 VoIP，有可能是公共交换电话网络（PSTN）。

值得注意的是，RSVP 中服务级别的请求者是接收站点而不是发送站点。这样，当 IP 多点传送技术被使用时，RSVP 可以控制范围（在 IP 多点传送技术中，有一个发送者多个接收者）。

RSVP 不是一个路由选择协议，并且目前不会根据流量和阻塞来修改路由选择表。RSVP 只是简单地运行于 IP 上，使 IP 路由选择协议选择最佳路径。这条最佳路径不一定是最理想的允许 QoS 的路径。而且，RSVP 无法调整路由器行为。

6. RSVP 语法

下面是 RSVP 语法

```
ip rsvp bandwidth
```

在一个接口启用 IP 的 RSVP，使用 **ip rsvp bandwidth** 接口配置命令　禁用 RSVP，使用该命令的“no”形式

```
ip rsvp bandwidth [interface-kbit/s] [single-flow-kbit/s]
no ip rsvp bandwidth [interface-kbit/s] [single-flow-kbit/s]
```

命令选项定义如下：

- *interface-kbit/s*——(可选)接口预留的带宽(以 kbit/s 为单位)，范围为 1～10 000 000。
- *single-flow-kbit/s*——(可选)为一个单一流预留的带宽(以kbit/s为单位)，范围为 1～10 000 000。

■ Default——如果没有指定带宽，接口带宽的75%预留。

显示当前设置的RSVP预留，使用show ip rsvp reservation命令：

```
show ip rsvp reservation [type number]
```

type number 是可选的；它指定了接口类型和号码。

7. RSVP限定

虽然RSVP在QoS领域是一个重要的工具，但它没有解决所有与QoS相关的问题。RSVP有三个缺陷：可量测性（scalability）、接入控制（admission control）和它用于建立端到端预留的时间。

RSVP有许多限定阻止它在因特网上广泛部署。在网络中没能很好使用RSVP的场景中，一个主干路由器必须管理上千个RSVP预留并且根据预留为每个流排队。

包围RSVP的可量测性问题将RSVP移交给网络边界，并且迫使主干网络使用其他QoS工具。长期以来，IETF一直致力于更好的使用RSVP，增强它的可量测性。

RSVP工作在整个IP分组上，不考虑任何压缩方案、循环冗余检测（CRC）或线路封装（帧中继、PPP或高级数据链路控制（High-Level Data Link Control，HDLC））。

比如在VoIP使用RSVP和G.729时，思科IOS软件预留要求为24kbit/s，使用cRTP的实际值是11 kbit/s。换句话说，在一条56 kbit/s链路上，虽然带宽足够4条11kbit/s的VoIP流，但只允许两条24kbit/s预留线路。

在这种情况下，您可以超额认购链路的有效带宽使RSVP预留超过实际有效带宽的带宽。您可以在特定接口上使用 *bandwidth* 语句来作预留。这个设定在网路正常运行和您能控制网络流量的情况下都是允许的。

例如在一条56kbit/s的链路上，带宽语句告诉接口有100kbit/s的带宽存在。然后您就可以使其中的75%带宽为RSVP流量预留。这样，就可以使RSVP为三条VoIP G.729呼叫预留必要的带宽。但是如果cRTP不被使用，链路就会超载。

8.3 流量管制

前面的各节中描述了为不同流量排队然后为其设置不同优先级的方法。这些是QoS非常重要的一部分。有些时候，管理或限制应用可以在各种接口或网络上的传输量是非常必要的。

思科有一些工具可以使网络管理员定义一个应用甚至一个用户可以使用多少流量。这些功能有两种类型：*速率限制工具（rate-limiting tools）*，如CAR，以及整形工具（shaping tools），如GTS或FRTS。

这两种类型的工具的主要不同在于：速率限制工具根据策略丢弃某些流量，而整形工具将过载的流量先缓存起来等到下一个空隙传输。

CAR与流量整形工具都相似的地方在于它们都识别什么时候网络流量超过网络管理员设置的阀值。

这两种工具经常一起使用。流量整形经常用于网络边界（以客户为前提）以保证用户业务的带宽需求。

CAR 经常用在服务供应商网络，保证用户没有超出与服务供应商签订的带宽。

8.3.1 CAR

CAR 是一个策略机制，它允许网络管理员设置超出（exceed）或遵守（conform）操作。通常使用遵守操作传输流量，超出操作分组丢失或将其设为低 IP 优先权值。

CAR 的速率限定机制允许用户：

- 控制接口传输或接收流量的最大速率；
- 在第 3 层给以细粒度控制，这样就可以使 IP 网络拥有 TDM 网络的质量。

您可以通过优先权，媒体接入控制（Media Access Control，MAC），IP 地址或其他参数限定流量速率。网络管理员还可以通过配置访问列表以创建细粒度的速率限制策略。

值得注意的是 CAR 不采用任何缓冲区以平缓流量。所以 CAR 适合于高速网络，不会因为排队而增加延迟。

在思科 7000 系列路由器上使用 RSP7000，或者在思科 7500 系列上使用 VIP2-40，或者为所有的 IP 流量使用更高的接口处理器配置 CAR 或分布式 CAR（Distributed CAR，DCAR）时，在全局配置模式（global configuration mode）下使用如下命令：

```
rate-limit {input | output} bit/s burst-normal
burst-max conform-action action exceed-action action
```

网络管理员可以为所有的 IP 流量定义一个基本的 CAR 策略。表 8-3 是一个有关遵守和超出操作关键字的描述。

要使 CAR 和 DCAR 有效，必须定义以下标准。

- 包的方向，输入或输出。
- 平均速率，由长时间的传输速率平均得到。在这个速率以下的流量总是遵守。
- 通常突发大小，决定在某些流量前多大的流量突发可以被认为是超出了速率界限。
- 额外突发大小。

在通常突发大小和额外突发大小之间的流量当突发大小增加时超出速率限制的可能性也会增大。CAR 传播突发。它不平滑或整形流量。

表 8-3 描述了遵守和超出操作。

表 8-3 rate-limit 命令操作关键字

关键字	描述
continue	评估下一个 rate-limit 命令
drop	分组丢失
set-prec-continue new-prec	设置 IP 优先权，并评估下一个 rate-limit 命令
set-prec-transmit new-prec	设置 IP 优先权并传输包
transmit	传输包

只能在 IP 流量上使用 CAR 和通用接口处理器 DCAR（VIP-DCAR）。非 IP 流量没有速率限制。

可以在接口或子接口上配置 CAR 或 VIP DCAR。但是，CAR 和 VIP-DCAR 不支持如下接口：

- 快速以太网（Fast EtherChannel）；
- 隧道（Tunnel）；
- 基群速率接口（Primary Rate Interface，PRI）；
- 其他任何不支持思科快速转发（Cisco express forwarding，CEF）的接口。

8.3.2 流量整形

思科 IOS QoS 软件包括两种类型的流量整形： GTS 和 FRTS。虽然这两中流量整形方式的命令行接口不同，保留和整形延迟流量的队列也不同，但它们的实施很相似。

如果一个包延迟了，GTS 使用 WFQ 保存延迟的流量。FRTS 根据具体配置，使用 CQ 或 PQ 保存延迟的流量。从 1999 年 4 月起，FRTS 也支持 WFQ。

通过整形流量，可以控制一个端口的输出流量与远程目标接口速度匹配，并保证流量遵守相关策略。这样，您就可以整形流量符合某个特定的配置文件以满足下游的需求，从而减少拓扑中因为速率不匹配而形成的瓶颈。

流量整形主要用于：

- 控制有效带宽的使用；
- 建立流量策略；
- 管制流量避免阻塞；

在下列情况下使用流量整形。

- 如果一个网络有不同的接入速率，可以在接口上配置流量整形。假设一端链路是 256kbit/s 的帧中继网络，另一端 128kbit/s。如果以 256kbit/s 的速率发送包则可能造成应用不能使用链路。
- 如果您提供次速率服务，则可以配置流量整形。在这种情况下，流量整形可以使您使用路由器将 T1 或 T3 链路分成小的信道。

流量整形可以防止分组丢失。在帧中继网络中使用流量整形尤为重要，因为交换机不能决定哪个包有优先权，所以在阻塞出现时无法决定哪个包应该丢弃。

此外，对于 VoIP 也是至关重要的，可以帮助您控制等待时间。通过限制网络中的流量大小和流量丢失，您可以平滑流量模式，给予实时流量优先权。

1. GTS 与 FRTS 的区别

如前所述，GTS 与 FRTS 实施非常相似，它们共享同样的编码和数据结构，但是它们使用的命令行接口和队列类型不同。

下面是 GTS 与 FRTS 不同的两个方面。

- FRTS CLI 支持基于每条数据链路连接标识符(data-link connection identifier，DLCI)的整形。GTS 可配置在每个接口或子接口。

■ GTS 支持 WFQ 整形队列。

您可以将 GTS 配置得与 FRTS 行为相似：为每个子接口分配一个 DLCI 并使用 GTS 加 BECN 支持。除了使用不同的整形队列外，他们的行为是一样的。

在思科 IOS 软件发布 12.04(T)之前的版本中，FRTS 与 WFQ 是不兼容的。目前已经没有了这个限制，FRTS 与 GTS 都可以与 WFQ 协同工作。这就使网络管理员可以选择更细粒度的 QoS 机制（FRTS 和 WFQ 每 DLCI）。

2. 流量整形和排队

流量整形通过将超出配置速率部分的流量存储到一个队列来中平滑流量。当一个包到达接口需要传输时，发生如下操作。

■ 如果队列是空的，流量整形器处理刚到达的包。如果可能，流量整形器发送包。否则，它将包放到队列中。

■ 如果队列中有包存在，流量整形器发送队列中的其他新包。

如果队列中有包，流量整形器每个时间间隔内从队列中移出它可以发送的包。

3. GTS（通用流量整形）

GTS 应用在每个接口上，可以使用访问列表来选择要整形的流量。它可以与多种第 2 层协议协同工作，包括帧中继、ATM、交换式多兆比特数据服务（Switched Multimegabit Data Service，SMDS）和以太网。

在一个帧中继子接口上，您可以使 GTS 与 BECN（后向显式拥塞通知）信号相结合动态使用有效带宽，也可以只简单地整形到预先设好的速率。您也可以在一个 ATM 接口上配置 GTS 以响应静态配置的 ATM 永久虚电路（permanent virtual circuits，PVCs）上的 RSVP。

大多数媒体和路由器上的封装类型支持 GTS。您也可以应用 GTS 在一个接口的特定访问列表上。图 8-4 显示了 GTS 是怎样工作的。

在接口上为输出流量启用流量整形，使用 **traffic-shape rate** 接口配置命令。使用此命令的“no”形式禁用接口的流量整形。

```
traffic-shape rate bit-rate [ burst-size [ excess-burst-size] ]
no traffic-shape rate
```

语法描述如下。

■ bit-rate——比特率　流量要整形到的比特率，以 bit/s 为单位。这是您与您的服务供应商签订的接入比特率，或者是您想维护的服务水平。

■ burst-size——突发大小，（可选）每个时间间隔可以持续传输的比特数。在帧中继接口，这是您与服务供应商签订的承诺突发大小，缺省是比特率除以 8。

■ excess-burst-size——过量突发大小（可选）在阻塞状态下，每个时间间隔可以超出突发大小（burst size）的最大比特数。在帧中继接口，这是您与服务供应商签订的过量突发大小，缺省值等于突发大小流量整形组。

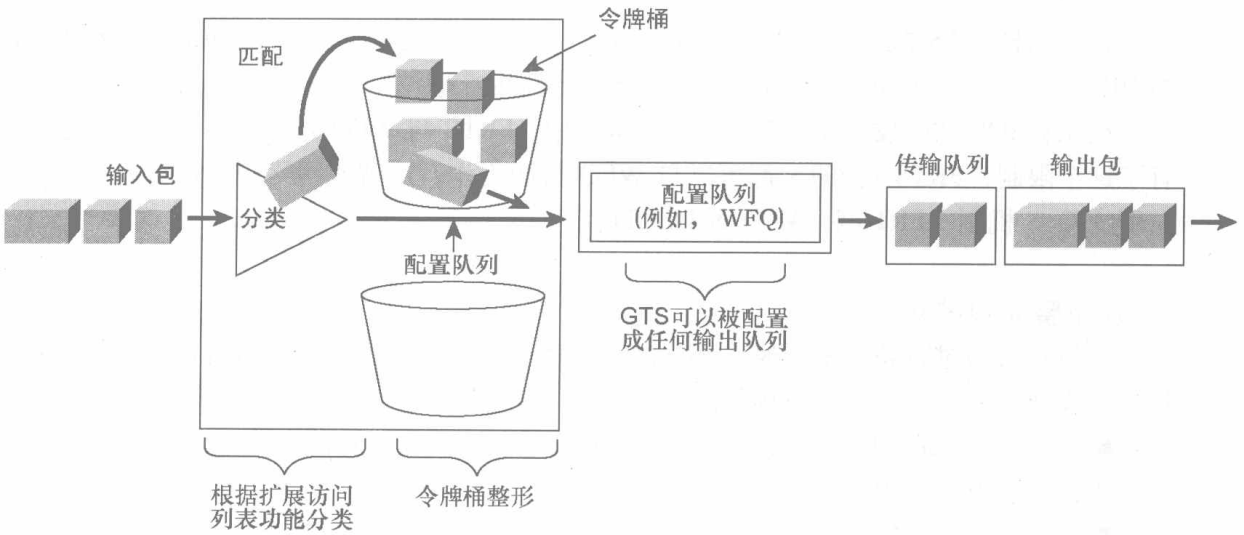


图 8-4 GTS 操作

启用基于接口的特定访问列表，为输出流量整形，使用 **traffic-shape group** 接口配置命令。使用此命令的“no”形式禁用接口访问列表的流量整形。

```
traffic-shape group access-list bit-rate [burst-size [excess-burst-size]]
no traffic-shape group access-list
```

考虑以下例子。公司 A 希望限制帧中继电路的输出流量到链路的 CIR 以防止包被标为可丢弃（discard eligible，DE）。帧中继电路的带宽为 56kbit/s，CIR 是 32kbit/s。例 8-5 显示了所需的配置。

例 8-5 公司 A 的流量整形配置

```
interface serial 0/0
encapsulation frame-relay
traffic-shape rate 32000 4000 0
```

公司 B 希望整形它的输出到广域网（WAN）的流量，从而 FTP 值使用它 256kbit/s 线路的 64kbit/s。例 8-6 显示了所需的配置。

例 8-6 公司 B 的流量整形配置

```
interface serial 0/0
traffic-shape group 101 64000 8000 0
!
access-list 101 permit tcp any eq ftp any
```

4. FRTS（帧中继业务整成形）

与 GTS 一样，FRTS 通过缓存过量流量来平滑输出流量。FRTS 也可以解决在帧中继

网络入口和出口不同接入速率而造成的问题。例如，在帧中继网络中心点，经常有一个高速（T1 或更高）连接到网络，而远程站点不会超过 384kbit/s。

中心点路由器可以使用 T1 速度传输到远程路由器，但远程路由器只能以 384kbit/s 或更少来接收。这就迫使帧中继网络缓存流量并可以为一个分组包流添加*秒数 (seconds)*。这使语音在大多数网络上不可接受。

FRTS 可以使用 FECN（前向显式拥塞通知）和 BECN（后向显式拥塞通知）动态使用多或少的带宽。

在帧中继网络中，BECN 和 FECN 象征了阻塞。在帧中继网络中，您可以按位定义 BECN 和 FECN。

通过使用从网络中接收到的 BECN 标记过的包中的信息，FRTS 也可以扼杀流量。通过基于 BECN 的扼杀，包被路由器保留以减少右路由器进入帧中继网络设数据流。

扼杀在虚电路（virtual circuit，VC）执行，传输速率根据接收到的 BECN 标记包的数目调整。

5. 分段（Fragmentation）

传播延迟和队列延迟都已在前面的章节中讨论过。需要分段的原因很简单——大的包（1500 字节 MTU）需要很长的时间在低带宽链路（768kbit/s 或更小）上传输。分段将大包分成小包，可以在 OSI 模型的第 2 层或第 3 层完成这些操作。

在任何数据应用中，因为低带宽而造成的等待时间对最终用户都是没有影响的。但在实时应用中，这就会引起很多问题（起伏的语音质量、帧丢失、呼叫中断，等等）。

比如一个 1500 字节的包在 56kbit/s 的链路上需要 214ms。ITU-T 建议单向最大的语音等待时间要小于 150ms。这样，一条 56kbit/s 的线路和一个 1 500 字节的包消费了整个 VoIP 延迟预算。例如：

包字节大小/秒 × 8=包位大小/秒；

包位大小/秒/线路位大小/秒=传输包所需的时间；

1 500 字节/秒 × 8=12 000 位/秒；

12 000bit/s/56 000bit/s=214s=214ms；

分段本身不能解决低带宽线路的等待时间问题。路由器必须能够基于分片或小包排队而不是分段前的包。

思科系统 VoIP 实施允许用户修改每包中样本数量。G.729 缺省每个帧中放两个 10ms 语音样本，也就是每 20ms 一个包。这就意味着需要每 20ms 传输一个 VoIP 包。

每帧 20ms 的间隔会因为您决定每帧中的样本数而发生改变。而且，这个数字很重要，因为它是您可以决定需要分段的大小。

如图 8-5 所示，可以根据链路速度和每帧中的样本数决定分片的大小。

链路速度 \ 帧大小	1 字节	64 字节	128 字节	256 字节	512 字节	1024 字节	1500 字节
56 kbit/s	143 μs	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbit/s	125 μs	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbit/s	62.5 μs	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbit/s	31 μs	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbit/s	15.5 μs	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbit/s	10 μs	640 μs	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms
1536 kbit/s	5 μs	320 μs	640 μs	1.28 ms	2.56 ms	5.12 ms	7.5 ms

图 8-5 固定帧传播延迟

6. 阻塞（Blocking）

分段可以帮助减少“阻塞（blocking）”问题。阻塞（Blocking）是指允许一个包消耗所有有效 WAN 带宽，迫使其他实时包排队的时间。阻塞直接影响延迟预算。您可能有不同的经验，但是一般来讲，最好保持阻塞延迟为总语音包大小的 80%。

例如，如果一个 20ms 包中包含两个 10ms 语音样本，需要最大的阻塞延迟为大约 16ms。假设 WAN 链路为 56kbit/s 并且使用图 8-5 作为一个例子，希望包被分段为 128 字节。如果您需要一个确切的数字，下面的算法可以用来决定包分段的大小。

WAN 带宽 × 阻塞延迟 = 分片位大小

根据前面的建议使用这个算法计算具体延迟：

WAN 带宽（56kbit/s）× 阻塞延迟（16ms）=896bit/s（112 字节/秒）

7. MCML PPP

多类多链路点对点协议（Multi-Class Multilink Point-to-Point Protocol，MCML PPP）允许建立两个“束（bundle）”。一束可以被分段和交叉存储，另一束只能被简单地交叉存储，如图 8-6 所示。这项功能从思科 IOS 软件发布 11.2（13）T 开始可以使用，为使用 ML PPP 提供了很多的便利。

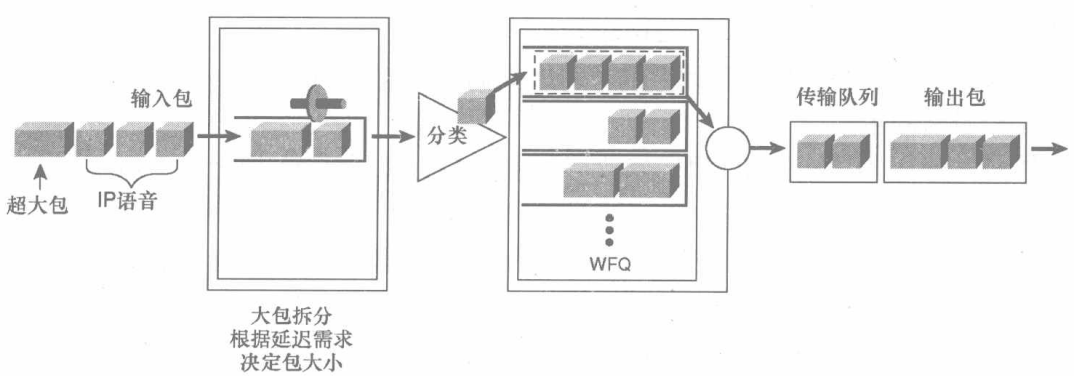


图 8-6 多类多链路 PPP

您只能在可以运行 PPP 的接口使用 MCML，这是一个立即将大部分 WAN 网络（帧中继、ATM 等）排除在外的规定。

MCML 只定义了分段的方式，它没有定义为分片区分优先级的队列技术。

8. FRF.12

FRF.12 是帧中继论坛技术委员会（Frame Relay Forum Technical Committee）制定的一个规范。您可以在 http://www.frforum.com 上找到它。这个规范允许帧中继网络能以与 MCML PPP 相类似的方式运行。因为分段也发生在链路层，上一层协议根本意识不到分段。

使用 MCML PPP 时，包在进入广域网之前被分段，在目的路由器接收到后重新组装。

FRF.12 也定义了帧中继和 ATM 组网。允许包在线路的帧中继端被 FRF.12 分段，在线路的 ATM 端被重组。

9. IP MTU 和 MTU

在不支持 MCML PPP 或 FRF.12 的接口，您可以给端口或协议的 MTU 设置一个较小的值来迫使分段。

串口的 MTU 通常为 1 500 字节。使用 FRF.12 和 MCML PPP，您可以在不干扰包流的情况下改变发送到接口的包的大小。当您使用较小的 MTU 或 IP MTU 时，则改变了包的旅行时间。

例 8-7 显示了 IP MTU 配置。

例 8-7 配置 IP MTU

```
interface Serial0/0
 ip mtu 300
 no ip address
 encapsulation frame-relay
 fair-queue 64 256 1000
!
interface Serial0/0.1 point-to-point
 ip mtu 300
 ip address 40.0.0.7 255.0.0.0
```

例 8-8 显示了 MTU 配置。

例 8-8 配置 MTU

```
interface Serial0/0
  mtu 300
  no ip address
  ip rsvp bandwidth 1158 1158
  encapsulation frame-relay
fair-queue 64 256 1000
!
interface Serial0/0.1 point-to-point
  mtu 300
  ip address 40.0.0.7 255.0.0.0
```

10. IP MTU 限定

在 IP 分组的整个生命中改变大小会带来很多问题。例如，接收站点的整体性能受到了影响，因为它需要处理许多小包，这比处理一个大包要费时。而且，每个分片都需要复制包头。

假设一个包头 40 字节的 1 500 字节的包，如果将这 1 460 字节的负载分成 100 字节的帧，将有 14 个 100 字节的包和 1 个 60 字节的分组。需要将 40 字节的包头放回在这 15 个分组中，这样做的结果是将 40 字节的包头增加到了 600 字节。

另一个 IP MTU 和 MTU 大小改变的主要问题是如果一个包的不允许分段字段(Do Not Fragment，DNF）被置位，这个包将被丢弃。许多应用置位此位以防止中间设备（路由器或其他网络元素）将它们的包分成许多片。DNF 位可能被设置的一个原因是避免接收站点将分片重组的负担。

11. MTU 限定

MTU 大小改变将改变所有接口输出包的大小，包括 IP、网间分组交换（Internetwork Packet eXchange，IPX）、Apple 计算机网络协议（AppleTalk）和路由选择更新。这对于路由选择更新可能是个问题，帧中继本地管理接口（Local Management Interface，LMI）更新和其他协议不支持分段。

8.3.3 边缘 QoS 总结

到目前为止，您应该了解了基本的包分类、分段、队列、带宽和策略机制。值得注意的是您可以在一个环境中同时使用一个或多个这些机制。

按照经验，在低带宽链路您应该总是使用包分类和队列机制。根据带宽情况和管理策略，可能会需要压缩和分段。

8.4 主干网络

主干网络与边缘网络完全不同，所以不能使用同样的 QoS 机制。两者的分类机制可能一样或近似，但队列、分段和带宽机制则通常不用或不同。

8.4.1 高速传输

您可以定义高速传输为任何高于 T1 的接口。虽然大多数人认为 DS-3 接口及其以上为高速网络，但这就像今天认为微处理器高速标准一样，以后会过时。

集中考虑高速网络的不同 QoS 机制是很有必要的。一般来讲，在高速接口上应用低速接口的所有规则和策略是不可行的。这主要是因为您应用的策略和 QoS 机制越多，路由器需要越多的时间来转发包。虽然这对于低速接口没有什么问题，但高速接口不可能花费太多时间去对每个包识别和排队。

因而，当客户转移到高速接口的时候（比如 OC-48），及时向他们提供建议使他们可以决定怎样在他们的网络上合理启用 QoS 时非常重要的。

改进的差额轮询

思科 12 000 吉比特位交换路由器（Gigabit Switch Router，GSR）是目前仅有的拥有 IP OC-48 接口的思科 IP 路由产品。改进的差额轮询（Modified Deficit Round Robin，MDRR）扩展了差额轮询（Deficit Round Robin，DRR）为如 VoIP 的实时流量提供优先级。在 MDRR 中，IP 包根据优先权位被影射到不同的 CoS 队列。

所有的队列都以轮询（round-robin）方式服务，除了处理语音流量的优先级队列。

DRR 为从 OC-3 到 OC-48 的更高速接口提供类似 WFQ 的队列。MDRR 扩展了 DRR 协议以包含一个高优先级队列，与其他与服务类有关的队列不同，该队列被区别对待。

由于每个 CoS 队列的支持的集，MDRR 包含一个为 VoIP 等实时流量的低等待时间、高优先级（low-latency，high-priority，LLHP）队列。处理 LLHP 队列，MDRR 都以 round-robin 的方式服务其他队列。

这就使需要高速队列的服务供应商和其他用户可以保证 VoIP 享有高于其他流量的优先级。

8.4.2 拥塞避免

正如前面讨论过的一样，WFQ，PQ 和 CQ 机制管理现有的拥塞和为高最高重要性的流量提供优先权。

拥塞避免从不同角度解决类似的问题。拥塞避免不是管理现有的拥塞，而是工作在怎样避免产生拥塞。简单来说，就是您可以抛弃不同数据流中使应用减慢发送的包以避免拥塞。这可以避免当 IP、TCP 流同时开始传输和停止传输时发生的全局同步（global synchronization）。全局同步是由于服务供应商的主干网缺少 QoS 造成的。

1. WRED

早期随机检测（Random Early Detection，RED）是一个拥塞避免机制（与拥塞管理机制相反），RED 尤其在高速传输网络上特别具有潜在的应用。RED 在 20 世纪 90 年代早期由 Sally Floyd and Van Jacobson 提出。

WRED 的理论基础，简单地说，就是大多数数据传输对丢失是敏感的，至少在他们流量中的一些被丢弃时会立刻慢下来。

想要指示一个 TCP 站点停止传输，您只需简单地丢弃向该站点发送的流量。WRED 是思科为避免全局同步而丢弃流量的措施。

WRED 组合了 RED 算法和 IP 优先权。这种组合为优先处理流量提供高优先级包。当接口开始出现拥塞时，它可以有选择地丢弃低优先级流量，为不同级别服务提供不同的性能特征。

WRED 也可以意识到 RSVP，并且它可以提供 IS 约束负载 QoS 服务。要想完全理解 WRED 是怎样工作的，您必须首先了解 TCP 分组丢失行为。

2. TCP

在 TCP 连接上传输的数据流被可靠有序地传送到目的地。传输通过使用序列号和确认来保证可靠。理论上，每个八位数据都被指定一个序列号。段的第一个八位数据序列号就是该段的序列号，被称为段序列号（segment sequence number）。

段也承载着一个确认号码，该确认号码是下一个希望接收到八位传输的序列号。当 TCP 传输一个段时，它在重传队列放一个副本并启动计时器；在接收到确认后，从队列中移出该段。如果在计时器失效前没有接收到确认，该段被重传。

TCP 确认并不保证数据被发送给了最终用户，只有接收 TCP 负责这个问题。

为了监管 TCP 的数据流，我们引入了流量控制机制。数据接收 TCP 向发送 TCP 汇报一个窗口。这个窗口定义了从接收 TCP 准备接收的下一个数据开始的 8 位数据的数量。

当一个用户发送一个 TCP 包，并检测到一个段被丢弃，用户的机器发送第一个段在它的等待确认列表中（用于重新开始数据流），进入到一个慢启动阶段。用户机器测试网络状况，找到一个它可以不丢弃数据的传输速率。

如有一个网络没有采用 RED，缓冲区满，尾部的包被丢弃。尾部包被丢弃发生在路由器缓冲区满，不能再接收包的情况下。

这会造成多个 TCP 会话重新开始它们的慢启动机制。在 TCP 窗口大小增加的情况下，这个场景最终会造成网络流量起伏不定。

路由器可以使用 RED 来管理 TCP 慢启动机制来扼杀一个单独的 TCP 流，在必要的情况下丢弃其他 TCP 流的包。

> 注释：启用 WRED，使用如下命令
>
> ```
> random-detect [weighting]
> ```
>
> *weighting* 是可选的。参数 weighting 常量是可选的，范围在 1～16 之间，决定拥塞出现时包被丢弃的速率，缺省为 9。

WRED 对于高速 TCP/IP 网络非常有用，它可以通过在可控的速率上分组丢失以避免拥塞。

8.4.3 主干 QoS 总结

值得注意的是，边缘 QoS 和主干 QoS 必须一起工作以保证网络上各种应用的 QoS 需求。

就经验来讲，在主干网和一些高速传输形式上，使用高速拥塞避免技术是明智的。您可以通过使用几种不同的机制来保证 IP QoS。具体使用哪种机制并不重要，重要的是确认您需要所有的工具都可以服务于您的应用。

8.5 QoS 经验法则

在边缘网络上实施 QoS 前，先思考如下问题。

1．您是否有一个低带宽 WAN 链路？如果有，使用 cRTP。

并且，选择一个分段方式（FRT.12 是帧中继网络的首选。MCML PPP 是其他网络的最好选择。不建议选择 MTU 和 IP MTU sizing）。

2．您的流量是否需要在 WAN 链路上区别对待？

如果需要，使用某些队列技术（建议使用 CB-WFQ 和 PQ）。

3．您选择 CB-WFQ 了吗？

如果是，选择一种分类方法。权重建议使用 IP 优先权（通常在主干网络上）。

4．您有一个 hub-and-spoke 帧中继网络或需要整形您的流量吗？

如果是，选择流量整形（首先建议 GTS，其次是 FRTS）。

在主干网络上实施 QoS 前，先思考如下问题。

1．您选择了高速网络技术了吗？

2．您确保边缘网络的 QoS 与主干网络的 QoS 或 CoS 兼容吗？（首先建议 IP 优先权。）

3．在高速使用的线路上您采用拥塞避免机制了吗？这些线路必须有一个高百分比的丢失容错协议（如 TCP 和 WRED）。

8.6 思科实验室的 QoS 测试

思科进行了如下测试，显示的不仅是 VoIP 质量，还有思科 QoS 工具是怎样有负荷工作的。

思科使用有两个思科 VoIP 网关和一个 56kbit/s WAN 作为实验环境。它完成了两个测试。

- 测试 A 测试了在有规则地增加 WAN 链路饱和度时启用 QoS 和不启用 QoS。
- 测试 B 测试了在以突发方式在 WAN 链路上传输时启用 QoS 和不启用 QoS。

在不使用 QoS 时，实施了 FIRO 队列。使用 QoS 时，使用了 MCML PPP、WFQ 和 IP 优先权。

思科使用两个室内发生工具来产生要发送的流量。使用一个语音质量测试工具来测量等待时间和语音质量，该工具使用了 ITU-T 知觉语音质量（Perceptual Speech Quality，PSQM）建议书 P.861。

当测量 PSQM 时，得分越高语音质量越差。表 8-4 显示了测试 A 的结果。

表 8-4 测试 A 结果

带宽饱和（百分比）	延迟（ms）	PSQM	延迟/QoS（ms）	PSQM QoS
0	76	1.43	76	1.43
40	233	1.94	106	1.5
60	242	2.1	104	1.43
75	280	7	102	1.51
90	300	9	104	1.51
100	350	10	105	1.51

图 8-7 更好地显示了不同 QoS 的效果。

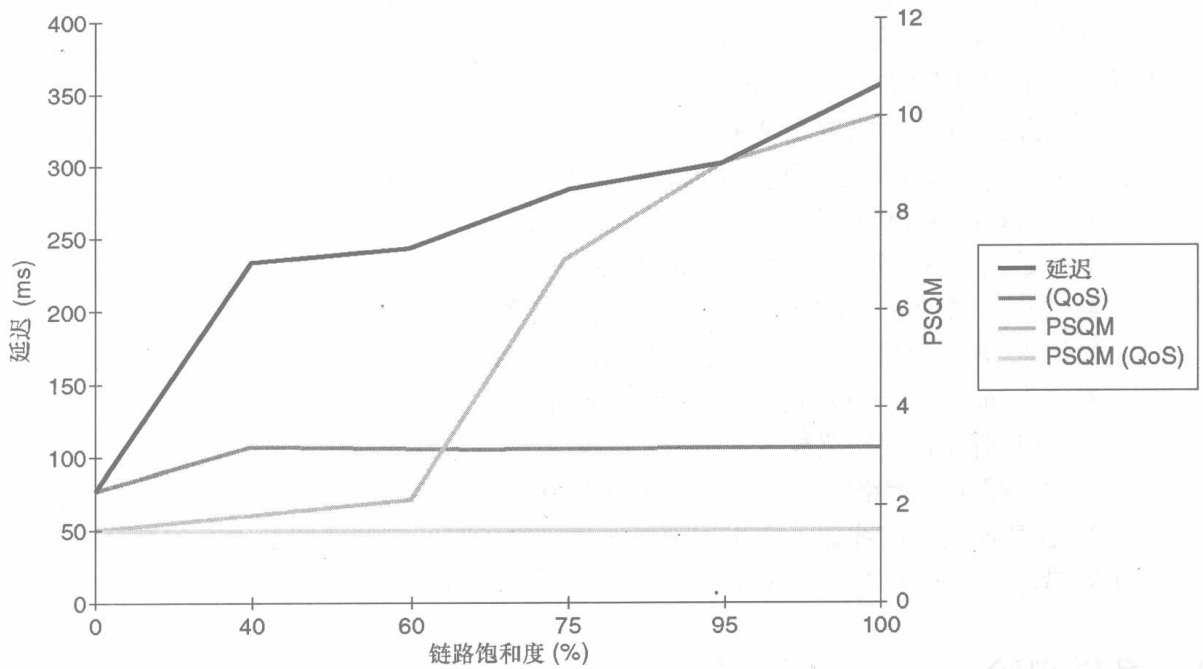


图 8-7 测试 A 结果

如图 8-8 所示，测试 B 是动态的。正确实施的思科 IOS 软件 QoS 工具，确实可以影响语音质量的稳定性和性能。

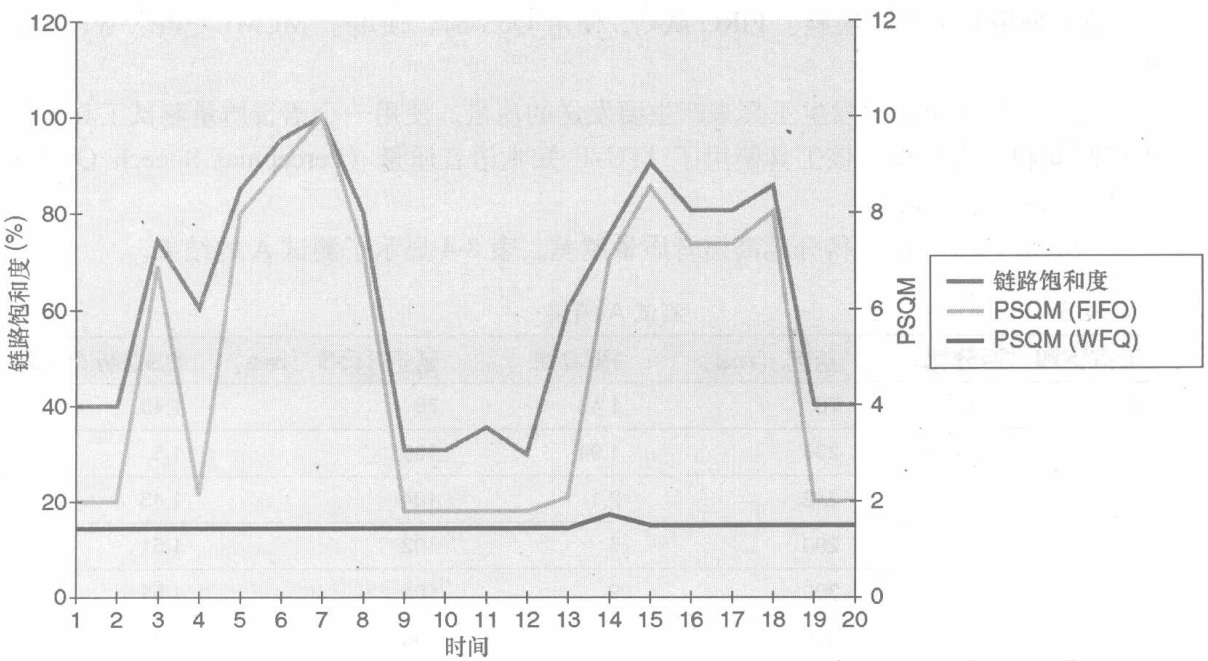


图 8-8 测试 B 结果

8.7 总结

本章系统阐述了 QoS 的话题。包发送后能够在发送者希望的时刻被接收到，是一个很复杂的问题。建设一个 VoIP 网络确实很复杂。合理的 QoS 是保证好的语音质量的一个重要步骤。

思科提供了一系列工具，让网络管理员可以建设合理的 VoIP 环境。虽然您不可能使用到所有的工具，了解它们对您网络的影响也是十分重要的。

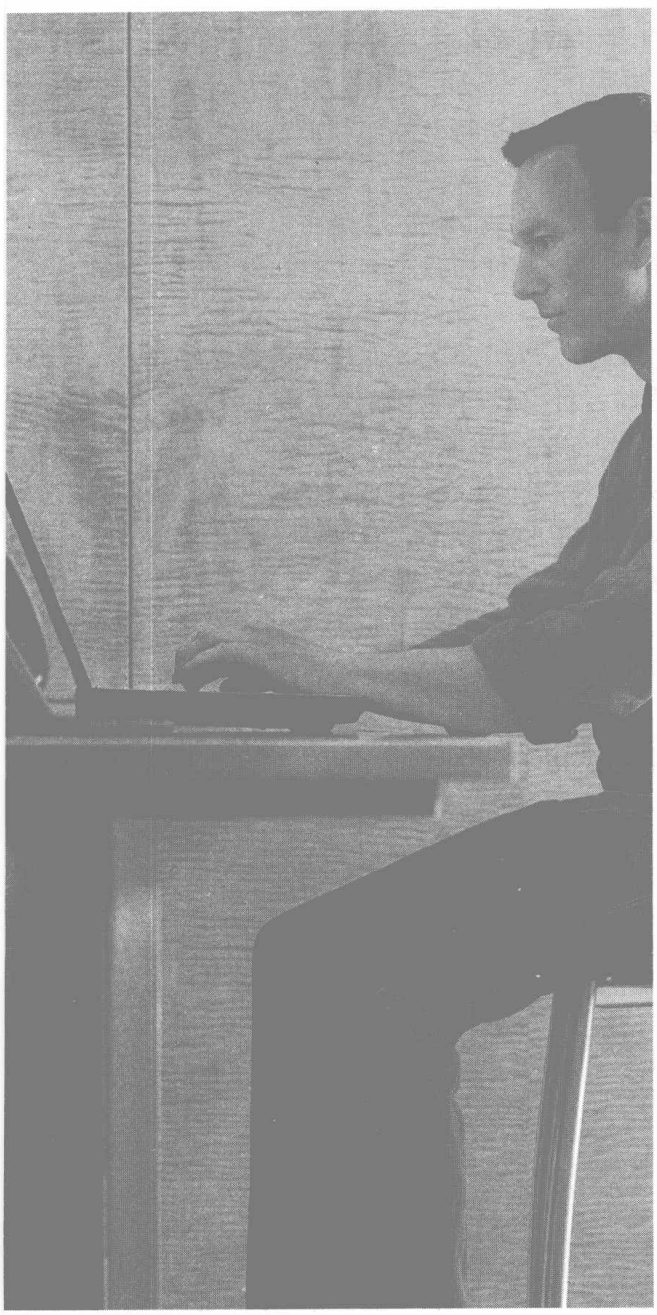
思科在区别对待 IP 网络上的延迟敏感流量方面有着多年的经验。这种经验开始于 20 世纪 90 年代早期，当思科开始为在 IP 网络上传输 SNA 流量开发产品时。尽管当时因为对等待时间和分组丢失的顾虑，很少有人认为 SNA 可以在 IP 网络上运行。然而今天，很大一部分 SNA 流量在 IP 网络上传输。

语音的情况也是一样的。2000 年本书的第一版发布时，很多人都怀疑 IP 是否可以给予实时应用合适的 QoS。然而，6 年以后，通过合理的网络设计和使用合适的工具，这已经被证明是可行的。

本章也讲解了许多队列技术，如 WFQ、CB-WFQ、LLQ、PQ 和 CQ，使读者了解这些工具是怎样随着时间发展而发展的。在部属 VoIP 网络时，目前我们强烈建议使用 LLQ。如果您不能将您的 IP 网络升级最新的版本，最好使用其他的队列技术，如 PQ 和 CQ。

有了队列技术就有了优先级的区分。虽然某些队列技术，如 LLQ，有内在的优先级，但必须保证所有的工具都合理地启用了它们。甚至如果您使用的是 LLQ，仍然应该使用 IP 优先权，因为主干网络可能会是由工具来根据优先级丢弃包。其他的组建如带宽节省技术、主干网工具等，都是帮助网络管理员提供合适 QoS 的工具箱。每个网络都是不同的，不仅需要注意各种细节，还需要网络管理员有足够的知识，知道怎样调整网络以提供最佳的 QoS。

QoS 将随着时间的推移继续发展。也许在不久的将来，IP 将成为事实上的传输方式。那时，语音不仅在 IP 上传输，TDM 线路也会如此。



本章讨论网络架构框架和设计模型，包含以下主题：

- 9.1 计费基础
- 9.2 案例学习：思科代理服务器和计费
- 9.3 VoIP 网络的挑战
- 9.4 仲裁服务
- 9.5 总结

第9章

计费与仲裁服务

计费与仲裁服务在 VoIP 上非常重要，它帮助服务供应商或企业的设备提供商在将其 TDM 网络向 VoIP 网络迁移时，了解财务相关区情况的主要因素，如投资回报（Return on Investment，ROI）。PSTN 的计费情况比较简单，因为呼叫的双方是静态的，并与具体物理位置紧密相连。我们期望语音流量（使用基于呼叫时间的分钟数）和数据流量（使用统一计费）的计费方式是不同的。VoIP 改变这种情况，允许端点移动。语音和数据流量都被打包，从网络上的一个地点到另一个地点传送。这就引起了一些问题，需要协议定义向谁计费，在哪里计费和计什么费。

9.1 计费基础

在 VoIP 中，除了在两个端点的呼叫外，您还需要考虑许多需要不同计费方式的服务种类。值得注意的是，实施这些服务的工具可能不同。这些服务的主要分类如下。

- 附加服务：
  - 分流（Forking）；
  - 转发（Forwarding）；
  - 传输（Transferring）；
  - 重定向（Redirecting）；
  - 保持（Holding）；
  - 发现跟踪（Find-me-follow-me）；
  - 同时振铃（Simultaneous ringing）。
- 服务类别：
  - 按时间计费（语音、传真、语音信箱记录/播放）；
  - 按字节数计费（调制解调器）；
  - 按页数计费（传真）；
  - 统一计费（例如股市查询）。
- 漫游（Roaming）：
  - 与数据库服务合作伙伴集成计费。
- 电话会议（Conference calling）：
  - 有计划的；
  - 随时发生的。

- 多种计费（Multibox billing）：
  - 会议服务器；
  - 语音信箱服务器（Voice-mail server）；
  - 翻译，基于 SCP 的服务；
  - 统一通信（Unified communications，UC）；
  - 集成计费/UC 合作伙伴。

9.1.1 AAA

AAA 和 RADIUS 是 IP 世界计费服务的两块基石。对于 VoIP 来讲，计费和仲裁是服务器请求的服务。客户端通常是拥有呼叫控制信息的实体（例如媒体网关控制协议（Media Gateway Control Protocol，MGCP）呼叫代理，会话发起协议（Session Initiation Protocol，SIP）代理服务器等），服务器是处理计费相关信息的地方。注意，VoIP 网络的计费服务器的客户端对于它控制呼叫的最终用户和 VoIP 客户端，也是服务器。AAA 的 3 个步骤如下。

1．认证提供一个工具来确认请求接入某个系统的客户，并逻辑地预先授权。认证通过客户端与服务器的逻辑钥匙或证书完成。

2．授权发生在认证之后，确认客户端是否被允许执行或请求某个任务或操作，所以授权是策略管理的核心部分。

3．记账是测量资源消耗的过程，允许监视和汇报事件以及包括计费、分析、在行策略管理等各种目的的使用情况。因为 VoIP 的许多功能如移动性、漫游性和在数据链路上承载的经济方法，它发展了创新的记账模型。

9.1.2 RADIUS

远程验证拨入用户服务（Remote Authentication Dial-In User Service，RADIUS）是一个数据通信协议，用于提供安全管理，以及在远程计算环境，尤其是像 VoIP 这样的分布式网络中的统计信息收集。对于记账系统来讲，中心存储的数据比在网络上或多个设备上分散存储的数据要更安全、更容易管理和扩展，这一点很容易理解。

RADIUS 以客户端/服务器方式操作。RADIUS *认证服务器（authentication server）* 提供安全服务和存储安全数据，记账服务器（accounting server）收集和存储统计数据。通常这两种服务是由一台机器提供的，虽然它们可以在分开的机器上运行。网络工程师可以配置 RADIUS 客户端使用 RADIUS 安全服务，RADIUS 记账服务或两者都使用。

RADIUS 客户端包含一个网络接入服务器（network access server，NAS），NAS 提供一个或多个用户访问网络资源。一个 RADIUS 服务器可以为几百个 RADIUS 客户端和几千个最终用户提供服务。从容错和冗余考虑，您可以为一个 RADIUS 客户端配置使用一个或多个可选 RADIUS 服务器。

RADIUS 提供三种网络服务：认证，授权和记账（AAA）。这些服务完成如下功能。

- 验证远程用户是不时可以访问网络的合法用户（认证）。

- 通过控制对网络资源的访问控制来定义每个用户可以做什么（授权）。
- 跟踪每个用户消费的资源以用于计费（记账）。

以下是 RADIUS 的主要功能。

- 网络安全——RADIUS 服务器和客户端的处理事务通过共享的秘密认证，这个秘密不会在网络上传输。而且，任何用户的口令都是加密传输的，减少了有人在不安全的网络上探听密码的可能性。
- 协议拓展——所有的处理事务都是由可变长度的属性—长度—值三元组（Attribute-Length-Value 3-tuples）组成的，可以在不改变现行协议实施的情况下添加新的属性值。RADIUS 允许设备厂商创立新的厂商定义属性（vendor-specific attributes，VSA），VSA 允许网络提供商在其中传递有价值的信息。
- 灵活的认证方案——RADIUS 服务器可以提供一系列的认证用户的方式。在它接收用户提供的到用户名和原始密码时，它可以支持 PPP 口令验证协议（PPP Password Authentication Protocol，PAP）或挑战握手验证协议（Challenge Handshake Authentication Protocol，CHAP）、UNIX 登录和其他认证机制。

9.1.3 厂商定义属性（VSA）

目前有几种版本的 VoIP 协议在使用中。每个协议都有自己的关于两个 VoIP 端点建立的会话的属性和信息字段。服务供应商所需要的计费数据经常对某个特定属性有特殊要求，只有在反馈给 RADIUS 服务器的 RADIUS 记账请求中添加了对该属性的特定补充，才可能将这个属性提供给服务供应商。这些补充通常是由协议定义的（如 H.323 和 SIP 可能会调用某个属性）。

9.1.4 计费格式

电话呼叫控制交换机根据计费周期收集每月的呼叫细节记录（Call Detail Records，CDR）。这些 CDR 是每个供应商提供计费相关信息的基本标准。如果网络中有多个供应商，它们也是调解费用的工具。

历史上，电话计费系统建立时，电话行业还没有什么竞争。现在，IP 电话因为 FCC（联邦通信委员会）和激烈竞争而使该行业缺乏管理。IP 电话服务的客户管理和计费系统可以跟踪管理实时活动变得越来越重要。

VoIP 呼叫通常如 PSTN 长途电话、手机和预付费电话卡有一定的呼叫时间，或像有线/卫星电视那样作为一组服务订购那样计费。对于所有情况，语音呼叫记录是计费的基础，所有的供应商都使用 CDR 来计费域间呼叫。下面的各节中将介绍呼叫记录的几种方式。

1. 典型的电话公司方式（Telco Approach）

在这种方式下，中心局（CO）交换机负责产生和交换 PSTN 拨叫呼叫的计费记录。CO 交换机产生自动消息记账（Automatic Messaging Accounting，AMA）记录，AMA 包

括呼叫号码、被叫号码、连接时间和日期、通话时间和服务特征等信息。AMA 记录基于 Telcordia GR-1100-CORE 文件定义的记录格式。它们被提供给为每个呼叫提供费率的仲裁/额定系统。税收保证和价格计算就是在这一步完成的。大多数情况下，这些由电话公司的计费办公室负责。下一步是费率计算完成后和交换数据前向最终用户计费系统与其他运营商（第三方计费）的最后的数据处理过程。图 9-1 列出了典型电话公司方式的计费流程。

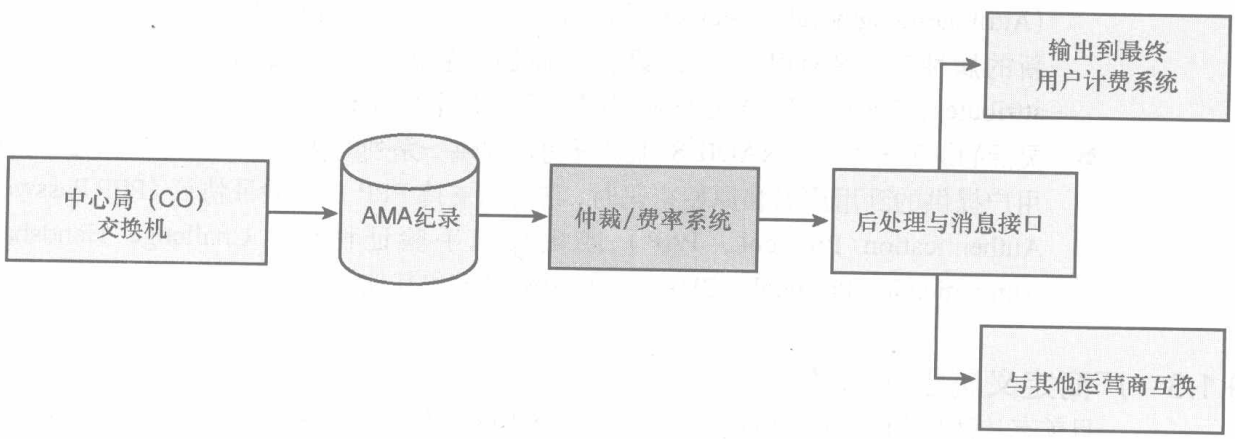


图 9-1 基本计费流程

虽然 Telcordia 负责维护和更新电话公司的通用需求（General Requirements，GR），但对大多数 US 市场来说，长途电话运营商（General Requirements，GR）和它们的设备提供商组成各种电信业解决方案联盟（Alliance for Telecommunications Industry Solutions，ATIS）委员会，一同负责他们之间的承载计费和其他运营问题。

2. 基于开放式结算协议（Open Settlements Protocol，OSP）方式

处理典型电话公司方式以外的方式是使用 OSP 来仲裁计费数据。欧洲电信标准协会（European Telecommunications Standards Institute，ETSI）的 TIPHON（Telecommunications and Internet Protocol Harmonization Over Networks）开发了 OSP。OSP 描述在 TS 101321 规范之下。这个方式包含开发一个票据交换所（clearinghouse）收集 IP 语音使用数据。当一个呼叫完成后，源和终结网关（或他们控制的看门人或 SIP 的代理服务器）的 OSP 客户端软件可以向 OSP 服务器汇报大量各种 ERSI 定义的使用数据。这个第三方的票据交换所通常控制输出 OSP 使用数据，或使用这些数据产生基于 XML 的 CDR。

OSP 最初是为 H.323 VoIP 网关开发的，OSP 被增强后可以与 SIP 一同工作。除了使计费简单外，OSP 规范定义了交换域间计费、路由选择和授权信息的方法。而且，OSP 组要票据交换所作为可信任的中间仲裁者，而且这个实施与多种票据交换所合作测试。再进一步，并不是网络上所有的呼叫都通过 OSP 服务器。

3. 基于 RADIUS 方式

IETF 开发了 RADIUS 协议，几乎所有的 ISP 都有使用 RADIUS 来作认证、授权和跟踪拨号上网的使用时间。RADIUS 记账服务器可以作为软交换机和网关 CDR 存档点 VoIP。它们还可以拓展为设备厂商专用的用于支持 VoIP、无线网络和预付费服务的附加数据收集。这些服务器必须有大量的存储空间和处理能力，以产生和保存所有计费记录，在需要的时候帮助审计。

VOIP 网关、软交换机和中间服务器拥有会话的相关信息，可以提供有关源和目的 IP 地址的信息，包口端口、呼叫时间、断开原因等。

在各种 VoIP 网络上，SIP 代理服务器，H.323 看门人和 MGCP 呼叫代理传递大部分的计费信息。

4. 基于 IPDR 方式

因特网协议细节记录（Internet Protocol Detail Record，IPDR）组织，一个行业协会，提供一系列的另一种使用记录格式——网络数据管理使用情况定义版本 2.5（the Network Data Management-Usage specification Version 2.5，NDM-U 2.5）。

这些标准的动机是为计费和仲裁系统设备厂商使用 VoIP CDR 提供一个标准格式。虽然许多 IPDR 参与者已经支持和签署 NDM-U，但仍有许多设备厂上拥有自己的版本。IPDR 成员包括 AceComm、ADC、Amdocs、Apogee、AP Engines 和 Daleen Technologies。

IPDR 方式更像将传统的 CDR，使用更成熟的方式包装。它基于 XML，可以扩展和转换。IPDR 格式允许系统提供计费工具可以很容易传输和处理的计费相关信息。许多系统倾向于使用 IPDR 格式，因为它允许使用 XML 方案和转换数据。

9.2 案例学习：思科代理服务器和计费

这个案例是关于一个典型的基于 SIP 的 VoIP 网络的。其中，思科 SIP 代理服务器（SPS）向 RADIUS 服务器发该服务器处理的 SIP 处理事务的记账请求分组（Accounting Request packets）。记账请求包包含标准 RADIUS 属性和思科定义的 VSA 的开始和结束记录。

思科 SPS 为所有分支的每个 INVITE 和 BYE 消息产生记账请求分组。这有助于将所有呼叫尝试的开始和停止记录都被发送给 RADIUS 服务器，包括所有分支的呼叫尝试，不管成功还是不成功，还是被取消。同一呼叫的所有记账请求包拥有同一个呼叫 ID、RADIUS 服务器或与 RADIUS 服务器一起工作的计费服务器，必须可以通过这个呼叫 ID 来关联记账请求包。图 9-2 从一个较高的层次显示了一个通过思科 SPS 的 SIP 呼叫和相关的思科 SPS 发送给 RADIUS 服务器的记账请求包。在这个例子中，RADIUS 服务器从记账请求包产生一个 CDR 并转发 CDR 到计费服务器用于关联。

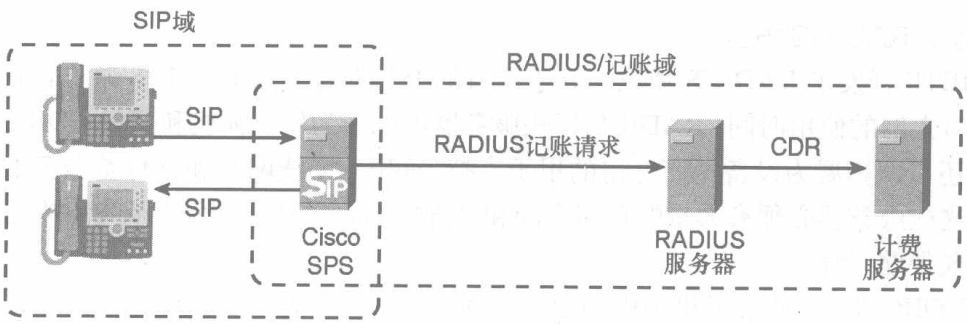


图 9-2 思科基于 SIP 的 VoIP 记账组件

思科 SPS 的配置选项允许定制记账触发器。对于上游实体，思科 SPS 是一个服务器端的控制请求实体。对于下游实体，思科 SPS 是一个客户端的发起请求实体。配置选项允许为所有的服务器端和客户端的呼叫尝试记账，不管成功与否。

图 9-3 中的呼叫流程演示了一个呼叫可能产生的各种记账记录。

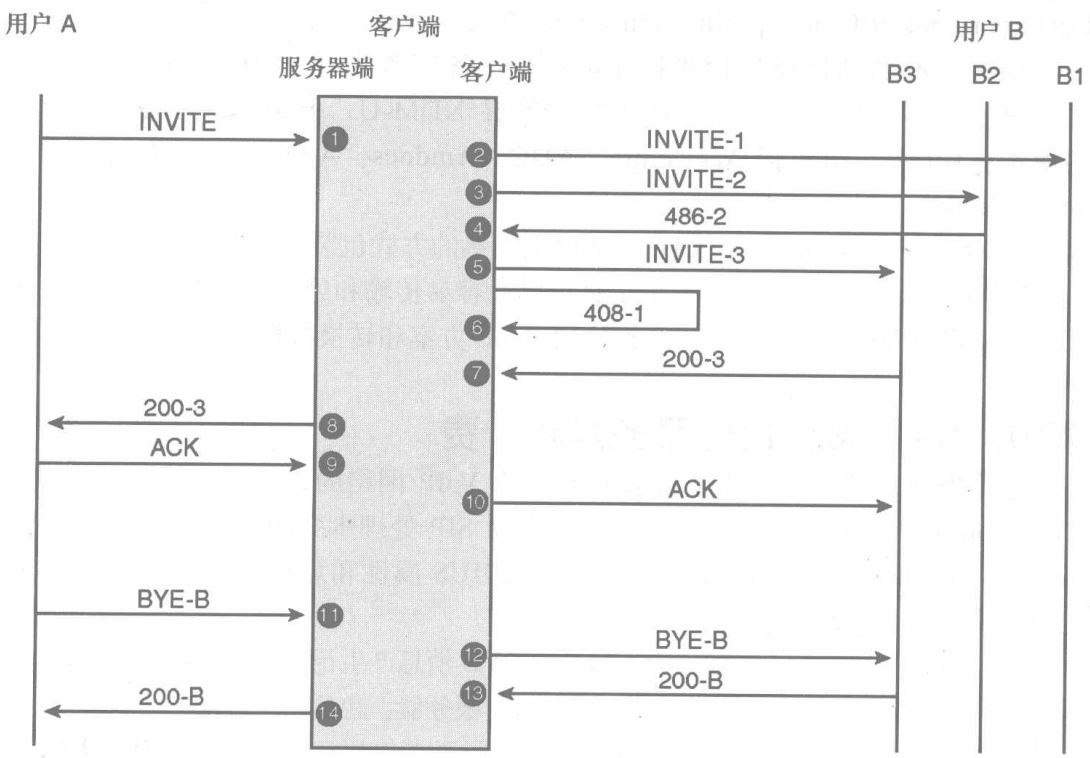


图 9-3 典型的基于 SIP 的 VIOP 记账呼叫流程

下面过程描述了图 9-3 中的呼叫流程协议。

1. 用户 A 想要呼叫用户 B。用户 A 向思科 SPS 发送一个给用户 B 的 INVITE。

2．用户 B 在 B1 和 B2 上都注册过。
3．思科 SPS 发送 INVITE 给 B1 和 B2。
4．B2 正在忙，返回 486。思科 SPS 发送客户端不成功停止（Stop）。
5．用户 B 有一个遇忙转移给 B3 的呼叫设置，所以思科 SPS 转发 INVITE 给 B3。
6．给 B1 的 INVITE 超时。思科 SPS 产生一个内部的 408，发送客户端不成功停止。
7．B3 响应呼叫，返回 200。思科 SPS 发送客户端开始（Start）。
8．思科 SPS 转发 200 给用户 A，发送服务器端开始。
9．用户 A 发送一个 ACK。
10．思科 SPS 发送 ACK 给用户 B。
11．用户 A 发送 BYE 给思科 SPS。
12．思科 SPS 转发 BYE 给 B3。
13．思科 SPS 接收到来自 B3 的 BYE 200，发送客户端成功停止。
14．思科 SPS 接转发 BYE 200 给用户 A，发送服务器端成功停止。

这就完成了思科 SPS 客户端接口使用 RADIUS 服务器的呼叫流程步骤。

RADIUS 服务器记账的详细内容在下面描述。

RADIUS 服务器记账

对于一个成功的服务器端呼叫尝试，开始（Start）记录在 INVITE 的 200 最终响应返回上游时被发送。停止（Stop）记录在 BYE 的最终响应被发送时发送。

1．思科 SPS RADIUS 接口

开始（Start）记录包含一个 **h323-start-time**，记录接收到 INVITE 的时间，一个 **h323-connect-time**，记录发送 200 的时间。**h323-call-origin** 被置为应答，表明这是一个服务器端的记账记录。sip-status-code VSA 被设为 200，这是最终响应 INVITE 的值。开始（Start）的文字表述，包含所有的 RADIUS 属性和思科定义的 VSA，如下所示。

```
NAS-IP-Address = a.4.61.72
NAS-Port-Type = Virtual
User-Name = "1230"
Service-Type = Login-User
Acct-Status-Type = Start
Acct-Session-Id = "04fb5d3908f3bfbe24fabfbe24f9bfbe@a.4.61.70"
Called-Station-Id = "<sip:5670@a.4.61.72:5060>"
Calling-Station-Id = "<sip:1230@a.4.61.70:9090>"
Vendor-Specific-9-25 = "h323-setup-time=21:31:14.578 GMT Mon Apr 14 2003"
Vendor-Specific-9-28 = "h323-connect-time=21:31:24.692 GMT Mon Apr 14 2003"
Vendor-Specific-9-26 = "h323-call-origin=answer"
Vendor-Specific-9-27 = "h323-call-type=VoIP"
Vendor-Specific-9-1 = "sip-status-code=200"
Vendor-Specific-9-1 = "session-protocol=sip"
Vendor-Specific-9-1 = "call-id=04fb5d3908f3bfbe24fabfbe24f9bfbe@a.4.61.70"
Vendor-Specific-9-1 = "method=INVITE"
Vendor-Specific-9-1 = "prev-hop-via=SIP/2.0/UDP a.4.61.70:9090"
```

```
Vendor-Specific-9-1 = "prev-hop-ip=a.4.61.70:9090"
Vendor-Specific-9-1 = "incoming-req-uri=sip:5670@a.4.61.72:5060"
Vendor-Specific-9-1 = "outgoing-req-uri=sip:5670@a.4.106.19:5060"
Vendor-Specific-9-1 = "next-hop-ip=a.4.106.19:5060"
```

停止（Stop）记录包含 **h323-disconnect-time**，记录了接收到 BYE 的时间。**h323-call-origin** 被置为应答，表明这是一个服务器端的记账记录。**h323-disconnect-cause** 没有被使用，取而代之的是添加了 **sip-status-code** VSA 为 BYE 的最终响应值。因为这个原因，停止（Stop）直到 BYE 的最终响应发送后才被发送。停止（Stop）的文字表述如下（包含了所有的标准 RADIUS 属性和思科定义的 VSA）。

```
NAS-IP-Address = a.4.61.72
NAS-Port-Type = Virtual
User-Name = "1230"
Service-Type = Login-User
Acct-Status-Type = Stop
Acct-Session-Id = "04fb5d3908f3bfbe24fabfbe24f9bfbe@a.4.61.70"
Called-Station-Id = "<sip:5670@a.4.61.72:5060>;tag=1F37F280-21AD"
Calling-Station-Id = "<sip:1230@a.4.61.70:9090>"
Vendor-Specific-9-29 = "h323-disconnect-time=21:31:44.770 GMT Mon Apr 14 2003"
Vendor-Specific-9-26 = "h323-call-origin=answer"
Vendor-Specific-9-27 = "h323-call-type=VoIP"
Vendor-Specific-9-1 = "sip-status-code=200"
Vendor-Specific-9-1 = "session-protocol=sip"
Vendor-Specific-9-1 = "call-id=04fb5d3908f3bfbe24fabfbe24f9bfbe@a.4.61.70"
Vendor-Specific-9-1 = "method=BYE"
Vendor-Specific-9-1 = "prev-hop-via=SIP/2.0/UDP a.4.61.70:9090"
Vendor-Specific-9-1 = "prev-hop-ip=a.4.61.70:9090"
Vendor-Specific-9-1 = "incoming-req-uri=sip:5670@a.4.61.72:5060"
Vendor-Specific-9-1 = "outgoing-req-uri=sip:5670@a.4.106.19:5060"
Vendor-Specific-9-1 = "next-hop-ip=a.4.106.19:5060"
```

没有成功的服务器端呼叫没有开始（Start）记录。停止（Stop）记录在 INVITE 的最好的非 200 响应被返回上游时发送，包括思科 SPS 等待来自下游的 487 将其返回上游的取消（CANCEL）情况。停止（Stop）记录包含一个 **h323-start-time** —— 记录接收到 INVITE 的时间，一个 **h323-connect-time** ——记录最终响应被发送的时间。**h323-call-origin** 被置为应答，表明这是一个服务器端的记账记录。**sip-status-code VSA** 被设为 INVITE 的最终响应值，使网络中最常用的属性拓展。

大多数思科 VoIP 网络元素提供 RADIUS 接口，作为 RADIUS 客户端提供 AAA 功能支持。

AAA 功能对应认证呼叫者、授权呼叫和呼叫记账。当用户有计费请求或需要支持白名单（whitelists）和黑名单（blacklists）时，使用认证和授权功能。所有的计费都需要记账功能，包括预付费、后付费计费和运营商间的结算。思科的 VoIP 网络元素支持 RADIUS 记账开始、记账停止、记账临时更新消息、记账启用和记账禁用消息。

与之相似的是，在今天的 H.323VoIP 实施中，允许语音的网关发送 RADIUS 记账开始和停止消息给基于 RADIUS 服务器的计费和仲裁系统。对于借记卡应用，网关与

RADIUS 服务器交互以得到信用值和呼叫剩余时间（呼叫授权）。许多商用基于 IP 的计费系统，如 Digiquant 和 Mind，都内置一个支持为基本没有仲裁设备的 VoIP 服务计费的 RADIUS 服务器。

然而，如果呼叫比较复杂的话，使用一个独立的仲裁系统最符合客户的利益。

思科有多家仲裁和计费合作伙伴，用户可以选择最适合他们需求的系统。有些思科的合作伙伴只提供仲裁服务，有些使用紧耦合方式提供仲裁和计费，有些则单独或者以集成方式出售仲裁和计费平台。

> 注释：H.323 是最初在思科 VoIP 网关上为 VoIP 开发的协议。这就是为什么 H.323 表现为命令形式。而且，因为 SIP 和 H.323 使用类似的分布式呼叫处理和计费模型，作为 VoIP 协议，同样的命令对 H.323 和 SIP 有效。

2. 预付费和后付费应用

预付费是最常用的计费应用之一。在预付费应用中，在呼叫前告诉用户还剩余多少余额可以用于呼叫是非常重要的。在知道呼叫目的地后，启动一个计时器，在所有余额被消费完后，断开呼叫。一个用户友好的方式可能是在必要时提醒用户剩余时间。另一个非常重要的功能可能是保持正在进行的呼叫，请求呼叫方充值，在充值后恢复呼叫。

更进一步说，这些应用需要正确地应用费率在呼叫上。在使用密码和多次呼叫尝试时，需要着重考虑安全和授权。

对于后付费应用，呼叫者需要认证。后付费的呼叫流程包括收集呼叫者的电话号码给 RADIUS 服务器，一般使用这个号码作为账户号。交互式语音（interactive voice response，IVR）系统指导呼叫者使用应用，允许他在整个验证过程中使用双音多频（DualTone MultiFrequency，DTMF）音调。

无论预付费还是后付费，每个呼叫的费用值得考虑。在 VoIP 中，费率问题变得更复杂，因为呼叫方的地点是移动的，与地理坐标无关。这就是为什么应该为各种位置组合指定协商费率或统一收费的原因。

VoIP 网络产生包括那个扩展拨打或接听哪个号码的呼叫、拨打了多长时间等数据。这些数据通常被存在服务器的文本日志文件，或在 PostgreSQL 或 MySQL 数据库中以备处理使用。计费过程只用在 CDR 的产生过程被很好定义后才开始。

9.3 VoIP 网络的挑战

VoIP 已经从只是需要证明的概念阶段发展到成熟的、可以提供回报和节省费用的服务。在这些年里，网络变成了混合了许多呼叫代理、代理服务器、VoIP 网关和其他增加了许多不同功能的元素。供应商目前面对这两大问题：

- 混合使用情况和计费记录格式；

- 容量。

所有不同软交换机和服务建立了混乱的、有多种形式的使用情况和计费记录。这些混合的格式对互联来讲已成为一个问题，并造成数据不一致。

至于容量，IP 相关的事件通常会比传统的语音呼叫产生更多的记录，这对于在软交换机上使用的语音协议是不可预知的。VoIP 为一个普通呼叫平均记录 9 个事件，对于特殊服务和出错的情况还会更多。将被分析的数据包括检查分组丢失的数量或传输方和接收方的延迟情况，检查源和目的之间媒体包的不活动情况，通常的呼叫时间，呼叫/被叫号码的细节。此外还有输入输出软交换机产生的不同记录，为提供整个呼叫的整体视图的记录的相互关系。甚至如果计费系统可以理解 VoIP 服务，它不得不处理的大量记录也是对自己的一个挑战。

为解决这些挑战，一个用来收集、关联、聚集计费和记账的新的仲裁（mediation）服务组出现了。

9.4 仲裁服务

仲裁系统收集、关联和聚集由各种允许 VOIP 网络元素产程的一个呼叫所包含的所有记账信息。仲裁系统将这些信息转换为标准的或专有的 CDR 格式，这样每个呼叫有且只有一个 CDR 产生。需要仲裁系统服务供应商经常已经拥有一个计费系统，并希望仲裁系统的输出格式可以被他们已有的计费系统识别。许多仲裁系统可以支持来自不同厂商的商业计费系统，这些厂商包括 Keenan、Amdocs、Portal 和 Solect 等。几乎所有在已有的计费系统的在营本地交换运营商（Incumbent LocalExchange Carriers，ILEC）、地区贝尔运营公司（Regional Bell Operating Companies，RBOC）和更多的传统的美国和加拿大服务供应商 VoIP 实施都希望 CDR 采用 Bellcore AMA 格式(Belcore AMA Format，BAF)。

然而，VoIP 也要求计费系统知道统计分析什么。被分析的信息可能是通话时间，但也可能是传输数据的字节数（语音/视频）、视频的固定价格，或短消息（instances of text-based messaging，SMS）和彩信（instances of text-based messaging，SMS）的数量。计费系统必须依赖依靠仲裁系统，仲裁系统可以识别最终用户正在根据他们的通话计划和服务水平协议做什么。系统则可以创建一个计费的事件类型记录。作为最终结果，这些系统在计费系统上增加了附加值，提供了客户数据和语音服务的整体视图。

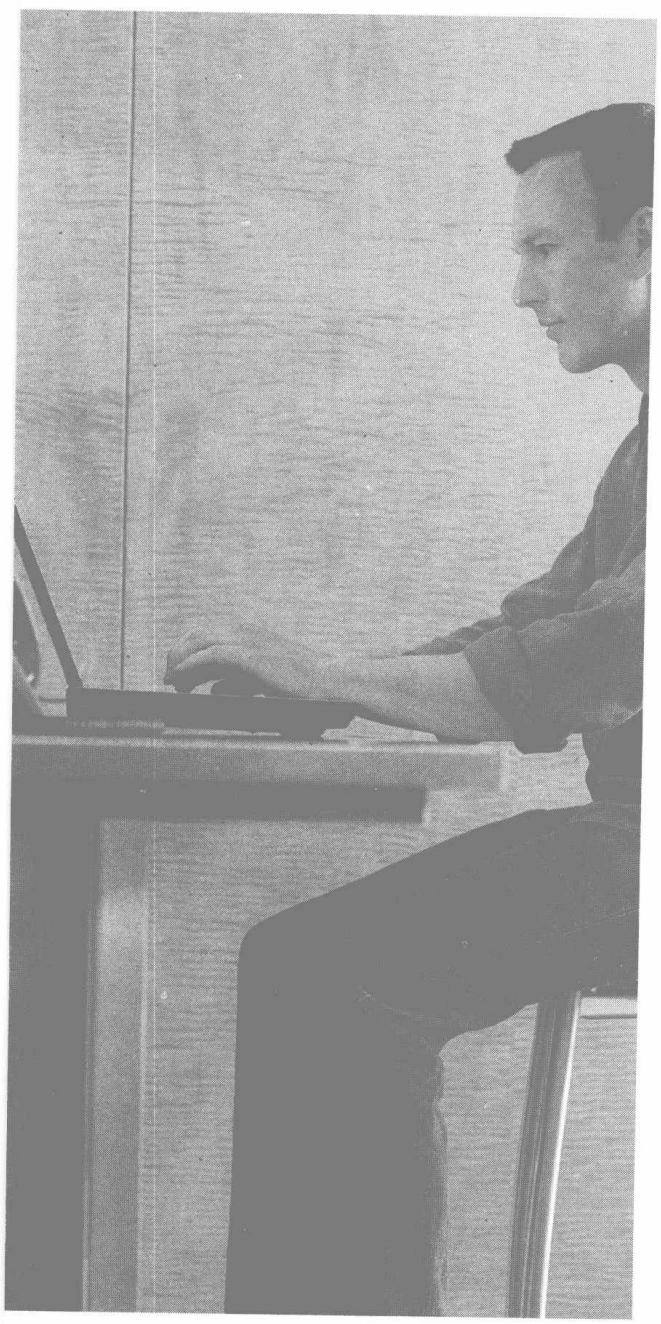
仲裁服务厂商目前可以提供从基本仲裁（捕获和聚集所有呼叫事件，多种 CDR 格式的产生）到以数据库为中心的服务，如汇报和分析的一系列服务，有些还可以通过增值模块为提供费率方式和关联服务提供更多技巧。由于 VoIP 呼叫与网页访问，音频/视频会议和远程出席等一同实施，在不久的将来关联将成为重要的组件。

9.5 总结

计费和仲裁对任何基于 VoIP 的服务都是非常重要的影响收入的部分。有这么多的 VoIP

协议和小服务供应商与 VoIP 业务推出，在推出服务之前计费过程标准化和格式化已经势在必行。

基于 VoIP 系统的全球增长在数据捕获、处理和计费方面向服务供应商提出了几大挑战。仲裁软件在 VoIP 网络上扮演着一个主要的角色。它从各种网络元素中接收数据（比如，软交换机、媒体服务器、信令网关和服务开发平台），并将其转换成可以被任何计费系统使用的行业标准计费数据结构，这些计费系统包括服务供应商已有的语音计费系统。



本章讨论网络架构框架和设计模型，包含以下主题：

- 10.1 安全需求
- 10.2 安全技术
- 10.3 语音设备保护
- 10.4 IP 网络设施保护
- 10.5 安全计划和策略
- 10.6 总结

第10章

语音安全

本章提供 VoIP 的基本安全需求概览。在本章中，您将知道有效满足这些需求和反击安全威胁的各种部署技术。

10.1 安全需求

在深入各种有效保证 VoIP 网络安全的技术细节前，您需要首先了解存在的问题和必须满足的需求。本节概述了一些典型的安全需求，而不是详细的完全列表。特定的 VoIP 服务可能会有附加的需求。

- 完整性（Integrity）——接收者应该接收到发送者发送的完整的包，没有任何改变。在传输过程中，第 3 方可能会修改包。

在 VoIP 信令中，这个定义被严格应用。然而在媒体方面，分组丢失通常是可以容忍的。

- 隐私性（Privacy）——第 3 方应该不能阅读数据。
- 真实性（Authenticity）——VoIP 信令或媒体消息的发送者和接收者应该是真正通信的双方。
- 有效/防护来自拒绝服务（Denial of Service，DoS）的攻击——VoIP 服务应该对用户随时有效。恶意或误操作用户/设备不应该能够干扰服务。缓解 DoS 攻击需要采取保护 VoIP 资源和 IP 网络的措施。

10.2 安全技术

在给予 VoIP 服务的安全需求之后，本小节讨论一些保证完整性、隐私和真实性的有效技术。本小节覆盖的技术如下：

- 共享秘钥（Shared key）；
- 公钥加密。

10.2.1 共享密钥方式

一种验证方法是在一个系统内发送者和接收者共享一个秘密口令（有时称为*共享密钥(shared-key)*），这个口令没有第 3 方知道。

发送者计算哈希消息内容并将哈希值添加到消息上。接收到消息后，接收方也使用共享口令哈希消息。然后将计算结果与消息中所带的值进行比较。如果匹配，证明消息是完

整的，也证明了发送者的真实性。

您可以使用共享口令加密消息内后传送给接收方。在这种情况下，满足了隐私要求，因为没有第 3 方可以探测传输数据，阅读其中明文消息内容。接收方将共享口令作为一个输入，运行解密算法，重建明文消息内容。

拥有多个数据源的系统可以通过保证每个发送方都有一个为发送数据使用的唯一密钥来满足真实性需求。

在共享密钥方式中，管理员必须提供共享的秘密口令。在一个拥有大量发送者/接收者的系统中，提供密钥会因为负载过大而被禁止。

另外，如果共享密钥被窃或丢失，所有使用共享密钥的设备都需要重新分配密钥。

10.2.2 公钥加密

为减轻共享密钥方式所带来的管理负载，您可以使用公钥加密方式。

公钥加密方式的基本概念是使用下面各节讨论的非对称密钥和数字签名。

1. 非对称密钥

非对称密钥对是一对称为公钥（public key）和私钥（private key）的密钥。公钥和私钥通常是固定长度的，具有数学上的相关性。他们通常采用 16 进制表示，具有如下特性：

- 只有相应的公钥可以解密有其私钥加密的数据；
- 只有相应的私钥可以解密有其公钥加密的数据；
- 这些密钥之间是一对一的关系。

私钥是保密的，公钥则由所有感兴趣的各方共享。

为了证明身份，发送者可以使用他自己的私钥加密消息。该消息只能由他的公钥解密。接收者可以在他可以访问发送者公钥的任何时候解密消息。因为只有发送者知道私钥，所以也只能是他加密了消息。

为了安全通信，发送者可以使用公钥加密技术加密消息内容。他使用接收者的公钥进行加密。接收者接到消息后可以使用私钥解密。因为接收者有私钥，所以他可以解密消息。没有第三方可以解密这个消息，因为除了接收者，没人知道这个私钥。

注意，发送者为了证明身份必须使用他的私钥加密，而为了安全通信，则使用接收者的公钥加密信息。在实际中，验证阶段首先发生。在发送者和接收者认证对方后，他们转到安全通信（secure communication）阶段。

使用非对称密钥加密，是一个漫长和耗费 CPU 资源的过程。因此，在有大量数据传输时，人们通常为每个会话使用公钥加密协商获得一个唯一的共享秘密。然后在剩余的会话中，使用这个共享的秘密产生的对称秘钥。

2. 数字签名（Digital Signature）

数字签名是消息内容和消息的签字者的一个属性。数字签名的目的与真实世界的签名是一样的——它是一个鉴别消息或部分数据的工具。数据签名使用了一对互补算法，一个

用于签名，另一个用于验证。

首先，在消息内容上运行哈希功能。然后使用签字者的私钥将哈希结果转成数字签名。数据签名通常添加到消息之后。

接收者通过在原始消息和签名者的公钥上运行验证程序来验证签名。

数字签名提供身份认证功能。(签名者必须有私钥）数字签名可以提供消息完整性，因为消息内容的任何改变，都将造成签名验证程序的失败。

然而，数字签名本身不提供隐私性。签名附加在消息之后，以明文传送，可以在传送过程中被查看。

3. 证书和证书机构（Certificate Authority）

现在的问题是，公钥是怎样传播给所有的可能接收者的。非对称密钥对难于维护和配置。证书是一种公钥发布问题的解决方案。

在秘钥产生时，实体（也称为主体（subject））的公钥被送往证书机构。CA 验证请求者的身份（可能需要人工参与），颁布证明请求者身份的证书和它的公钥。

CA 颁布的证书包括主体身份信息和其他信息，并由 CA 签字。

系统中的每个设备都由 CA 事先提供了证书（如果有多个 CA，每个 CA 都需要提供公钥给每个设备），并且都信任 CA 颁布的证书。

在会话开始建立时，主体向对方出示证书。对方运行一个签名验证程序验证是否一个受信任的 CA 签署了这个证书。如果签名有效，公钥和主体的身份（称为主体名称（subject name））被存在本地。

简单地说，受信任的 CA 的公钥提前提供给设备。所有其他实体使用证书验证，不需要手工给予。在证书（含有公钥）被传播后，系统实体间的通信就可以保密了。

4. 基于公钥的协议

在这一小节里，我们来看一下使用公钥加密技术的安全协议。这些协议并不仅局限于 VoIP 使用。您也可以使用他们安全其他服务。

① TLS

传输层安全(TLS)协议，在 RFC 2246 中定义，是从安全套接字层(Secure Socket Layer，SSL）发展而来的。TLS 运行在如 TCP 的可靠传输协议之上。在分层模型里，TLS 不依赖于在 TLS 之上的应用层。这样，除了 VoIP 外，您还可以在其他服务中使用 TLS。在 VoIP 中，TLS 主要用于保证信令安全。

TLS 有两层组成。

- 记录协议（Record Protocol）——提供安全连接的较低层，承担主要工作。它提供隐私权和完整性。

  记录协议使用如数据加密标准（Data Encryption Standard，DES）等对称加密算法和 RC4 对数据进行加密。在记录协议之上的另一层负责协商用于特定连接的密钥和

算法。您可以不加密使用记录协议。

每个信息都包含一个使用加密的 MAC 的消息完整性检测信息以保证完整性。MAC 计算使用安全哈希函数如 MD5 和安全哈希算法（Secure Hash Algorithm，SHA）计算。

- 客户层（Client layer）——在记录协议层上的上面。例如 TLS 握手协议等多个协议定义在客户层。TLS 握手协议主要开始于数据通信会话开始时。TLS 握手协议有两种主要功能：
  - 使用对称或公钥加密技术认证对方。
  - 在预连接情况下，有选择的协商一个公共密钥和对称加密算法。TLS 握手协议将共享秘密与协商的加密算法传递给记录协议层。记录协议层进行负载加密。

其他客户层协议包括警示协议（alert protocol）、改变密码描述协议（change cipher specification protocol）和应用数据协议（application data protocol）。

您可以在服务器认证方式或共有认证方式下使用 TLS。在服务器认证方式下，客户端通过 TLS 鉴定服务器的身份。服务器使用某些带外方式认证客户端。在相互验证方式下，每个实体通过验证证书认证对方。

图 10-1 显示了在 TLS 客户端和 TLS 服务器之间相互验证方式的消息流程。

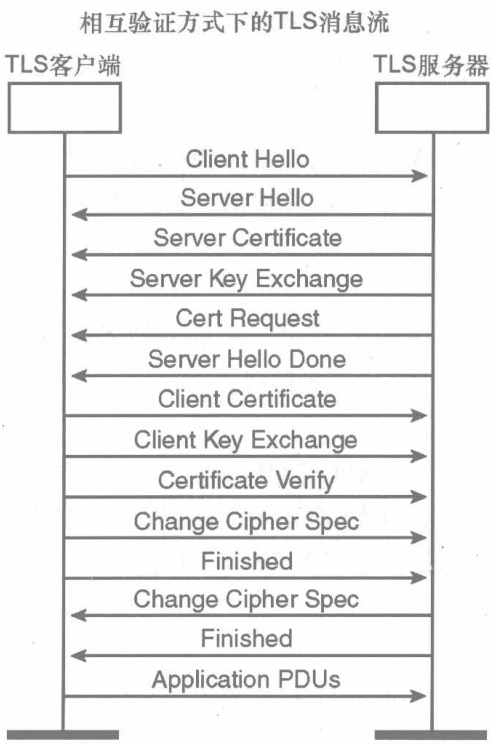


图 10-1 TLS 认证流程

② **IPsec**

TLS 运行在 TCP 上，IPsec 运行在 IP 层，使用公钥加密技术为 IP 数据包提供安全性。IPsec 使用两种协议提供安全性——验证头（Authentication Header，AH）和安全封装负载（Encapsulation Security Payload，ESP）。

AH 提供认证和完整性。ESP 在认证和完整性的基础上通过加密消息部分提供隐私性。IPsec 可以以两种方式运行。

- 传输模式（Transport mode）——在 IP 分组头和上层协议分组头（TCP/UDP）之间插入 IPsec 分组头。在这种方式下，只有 IP 数据包的负载部分被保护。
- 隧道模式（Tunnel mode）——整个 IP 分组被分装成另一个 IP 数据分组。在内部和外部 IP 分组头间添加一个 IPsec 包头。在这种方式下，整个 IP 分组都受到了保护。这种方式通常被使用在为设备没有发起这个包的情况下提供安全性。例如，这会出现在虚拟专用网（Virtual Private Network，VPN）连接上。

AH 和 ESP 都可以运行在传输模式或隧道模式上。不管使用哪种模式，它们的分组头是一样的。

图 10-2 显示了在传输模式和隧道模式下的 IPsec 封装。

图 10-2 IPSEC –隧道模式和传输模式

因特网密钥交换（Internet Key Exchange，IKE）协议被定义用来管理密钥。IKE 使用公钥加密技术协商认证密钥、安全协议（AH 或 ESP）、哈希算法和加密算法。

③ **SRTP**

由 RFC 3711 定义的安全实时传输协议（Secure Real time Transport Protocol，SRTP）是一种实时传输协议（Real time Transport Protocol，RTP）。SRTP 为 RTP 流量和 RTP 的控制流量，RTCP（实时传输控制协议，Real time Transport Control Protocol）提供完整性、真实性和隐私保护。

SRTP 不定义密钥是怎样在发送者和接收者之间交换的。密钥管理系统超出了 SRTP 定义的范围。对于 VoIP 来讲，在使用 SRTP 前，信令协议可以先交换密钥。如果使用信令协议交换密钥的话，需要通过使用 TLS，IPsec 或其他方式保证安全；否则，SRTP 使用的密钥可能会被黑客获得。

10.3 语音设备保护

您需要保护源和终端语音设备不受攻击以保证 VoIP 服务的有效性，具体细节在下面各节中介绍。

禁用未使用的端口/服务

通常您会发现语音设备上不被使用的端口或服务是打开的，使它们可能会遭到黑客的攻击。建议将 VoIP 设备和 VoIP 基础设施设备（如交换机，路由器等）的没有使用的服务或端口禁用。下面是您可能要进行的操作。

- 禁用远程登录（Telnet），简易文件传输协议（Trivial File Transfer Protocol，TFTP）或其他不用的类似服务。
- 如果您使用简单网络管理协议（Simple Network Management，SNMP）只是为收集数据，那么将 SNMP 设为只读模式。
- 如果您使用基于 WEB 方式的管理，则总是采用如安全套接字层（Secure Socket Layer，SSL）的安全访问协议。
- 将不被使用的第 2 层交换端口禁用。

您可以使用基于主机的入侵保护系统（Host based Intrusion Protection Systems，HIPS）来保护重要的语音设备如呼叫处理元素。HIPS 是典型的软件代理，用于收集大范围的资源使用情况，如 CPU、登录尝试、入侵次数等。通过将这些信息与一些规则进行比较来判断是否有安全漏洞。根据配置的参数，系统可以采取如终止入侵应用，终止来自入侵用户/IP 地址的实时数据等保护措施。

10.4 IP 网络设施保护

因为 VoIP 服务是运行在 IP 网络设施上的，只保护语音设备是不够的。保护 IP 网络使它可以承载语音流量是必要的。

本章讨论 IP 网络设施上的种种技术挑战和潜在的漏洞以及保护这些漏洞的有效技术。因为 IP 网络安全本事是一个广泛的领域，本节只介绍其中的一部分而不是全部。

10.4.1 分割

因为 VoIP 是一项重要的服务，VoIP 流量应该与其他流量分离。有许多分割策略可以完成这种流量的分离。

您可以应用其中的一部分策略，如第 2 层的 VLAN。将电话和其他语音设备放在一个与数据设备分离的 VLAN 上。

在第 3 层，通过使用单独的 IP 地址空间（如 VoIP 使用 64.10.x.x 数据使用 64.20.x.x ）来很容易地识别 VoIP 流量。即使在 VoIP 的内部，最好的做法也是将信令流量和媒体流量分开。

如果您使用 DHCP，最好也考虑为 VoIP 使用单独的 DHCP 服务器。

10.4.2 流量管制

即使实施了分割，一个 VoIP 设备也有可能占用所有分配给 VoIP 的带宽，从而扼杀其他 VoIP 设备。所以需要实施流量管制来避免这些。

大多数 VoIP 设备产生有一定限制的流量。例如，使用 G.711 编码的电话在每个方向不会产生高于 64kbit/s（包括打包的负载）的流量。您可以使用这些信息来管制来自这个设备的流量。

边缘 IP 设施需要实施合理的队列技术（就像思科 IOS 软件中的优先级队列一样）来防止流氓设备阻塞分配给语音的带宽。

10.4.3 802.1x 设备认证

您需要阻止未被授权的用户访问网络。第一道防线是阻止第 2 层的物理访问。在有线以太网上，您可以通过禁用不被使用的端口和 MAC 地址过滤完成。然而，过滤器比较难以管理，而且可能会被可编程的网卡（network interface cards，NIC）攻破。在无线环境中，因为没有物理端口的存在，偷听和 MAC 伪造变得比较容易。

802.1x 和可扩展身份验证协议（Extensible Authentication Protocol，EAP）是有线和无线的基于端口的访问控制标准。802.1x 和 EAP 在设备访问交换机前强制认证。EAP 允许多种认证机制，如 RADIUS。注意，客户端/主机机器需要支持 802.1x。虽然大多数客户端操作系统都支持 802.1x，但缺省方式下有可能被禁用。

客户端设备在初次接触无线访问点/有线交换机时，是未被授权的。此时，客户端设备只允许发送 802.1x 消息。客户端通过发送用户凭证 EAP 接入点，接入点将请求转发给认证服务器（例如，RADIU 服务器）验证。如果凭证是有效的，客户端通过 802.1x 和 EAP 请求来自无线访问点/有线交换机的凭证以验证身份。

图 10-3 显示了客户端和交换机之间的 802.1 消息流程。

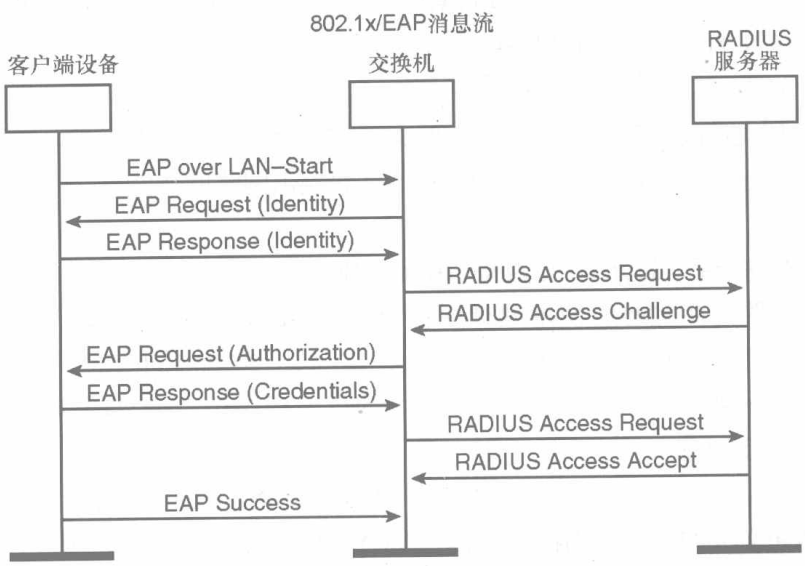


图 10-3 802.1 端口认证

在完成认证过程后，客户端设备被分配一个适当的 VLAN。

10.4.4 第 2 层工具

本节讨论第 2 层的减轻安全风险的一些有效工具。本节的讨论假设您已经有了第 2 层设备和协议的基础知识。在下面的每一段中都有第 2 层相关技术的简短介绍，但不包含详细的操作说明。本节中列出的工具在各种思科 Catalyst 系列产品中有效。

按照安全分层的精神，即使它们解决的安全问题有些重叠，您也应该采纳多种技术。

1. DHCP 监听（DHCP Snooping）

DHCP 监听通过过滤恶意 DHCP 消息和建立 IP 到 MAC 地址映射数据库来提供网络安全。DHCP 监听作为防火墙位于可信任的 DHCP 服务器和不可信任的发送 DHCP 请求的源之间。

当 DHCP 监听功能在第 2 层设备启用时，它截取所有的 DHCP 消息以保证所有的 DHCP 响应都来自 DHCP 服务器。任何有恶意的（比如，来自不可信任的端口的 DHCP 消息）消息都被丢弃。

另外，第 2 层交换机从 DHCP 消息中获得信息建立 IP 到 MAC 的地址映射数据库。这个映射数据库被称为 DHCP 监听捆绑数据库（DHCP snooping binding database）。

2. IP 源地址保护（IP Source Guard）

IP 源地址保护与 DHCP 监听一同工作，并将 DHCP 监听带到下一安全级。通过 IP 源地址保护，所有来自不可信任端口的 IP 流量除了 DHCP 消息以外，都被屏蔽。当接收到 DHCP 响应和建立 DHCP 监听捆绑数据库后，在该端口安装一个每个端口的 VLAN 访问控制列表（VLAN Access Control List，VACL）。

这个 VACL 应用于所有的来自该端口的后续 IP 流量，控制该端口只使用通过 DHCP 正当获得的 IP 地址。来自非 DHCP 监听捆绑数据库中的 IP 地址的流量都被过滤掉。这种过滤限制了主机通过声明为邻居主机的 IP 地址而攻击网络的功能。

3. 动态 ARP 检查（Dynamic ARP Inspection）

设备根据第 3 层地址，使用地址解析协议（Address Resolution Protocol，ARP）获得预期接收者的第 2 层地址。在广播介质上，通过在向广播域内的所有设备广播一个 ARP 请求来完成。IP 地址与 ARP 请求中的地址匹配的设备会通过一个 ARP 响应响应请求。其他设备在丢弃 ARP 请求。

ARP 定义不包含任何阻挡广播域内的恶意设备，在即使地址不匹配时也响应 ARP 请求。黑客可以利用这个缺陷，把自己的 MAC 地址放在 ARP 响应内伪造 ARP 响应。发送者（以及中间的第 2 层交换机）的 ARP 缓存在受到了污染。所有后续的要发送给

预期接收者的 IP 包被转向到了恶意设备。这通常称为“中间人”攻击（man in-the-middle attack）。

动态 ARP 检查是第 2 层技术，可以在交换机（或任何履行第 2 层功能的设备）上启用以减轻这个问题。DAI 与 DHCP 监听一同工作，并使用 DHCP 监听捆绑数据库。

DAI 功能需要将端口设为信任或不信任。DAI 检测所有来自不信任端口的 ARP 消息，与 DHCP 监听捆绑数据进行比较以证明该消息不是恶意的。最后，DAI 丢弃任何恶意 ARP 包。

另外，您可以配置一个 DAI 功能，执行 ARP 请求的速率限制以防止 flooding/DoS 攻击。

4. CAM 溢出和端口安全

以太网交换机在启动后进入一个学习阶段。在这个阶段，交换机检测来自每个端口的帧的源 MAC 地址。通过检测，交换机知道了拥有哪个源 MAC 地址的设备连接到了这个端口。交换机将这个映射作为一个表存储到内容可寻址存储器（Content Addressable Memory，CAM）中，这个表通常被称为 CAM 表（CAM table）。第 2 层交换机使用这个表发送第 2 层帧到正确的目的端口而不是发向每个端口。如果交换机在 CAM 表中没有找到目的地的 MAC 地址，它没有别的办法而只好将帧发到不是源的所有端口。

恶意设备可以通过溢出（overflowing）CAM 表来利用这个行为。他们向交换机发送大量含有不同源 MAC 地址的包，充满交换机的 CAM 表。因为 MAC 地址不能在 CAM 表中找到，所以交换机泛滥任何正常行为主机发送的第 2 层帧。（CAM 表已经满了）泛滥的包到达所有不是源的端口，而恶意设备可以访问这些帧。这就允许恶意设备执行“中间人”或 DoS 攻击。

思科端口安全功能通过为每个端口配置最大数量的 MAC 地址来解决这个问题。如果某个端口到达了这个上限，就在该端口执行特定的操作。侵犯端口可能被禁用或置入一个严格的模式。

5. BPDU 保护（BPDU Guard）和根卫士（Root Guard）

在第 2 层的布局中，为了冗余都存在物理环。但是，物理环可能会引起广播循环（永远循环广播某个帧）和网桥表的损坏。交换机通过运行生成树协议（Spanning Tree Protocol，STP）建立一个树状的没有循环的拓扑。这个树的根就是根网桥（root bridge）。没有循环的分支和叶跨越整个第 2 层网络。

管理员为每个交换机分配一个优先级。拥有最高优先级（最小数字，0 优先级比 1 优先级更有优先性）的交换机被选为根网桥 。交换机通过交换网桥协议数据单元（bridge protocol data units，BPDU）来沟通优先级信息和后续 STP 计算。BPDU 不具有内在的安全机制。这样，一个恶意设备可以假扮为交换机使自己成为根网桥。

两个思科功能：根保护（Root Guard）和 BPDU 保护可以阻止恶意设备发送 BPDU。BPDU 尝试阻止恶意设备发送 BPDU。如果一个端口被启用 PortFast 则禁止该端口接收 BPDU。

根保护（Root Guard）是在端口上设置的，确保启用了根保护的端口是指定的端口。如果交换机在启用根保护的端口上接收到较高的 STP BPDU（拥有较高优先级），该端口被转到根不一致 STP 状态。根不一致 STP 状态与侦听状态是等同的。根卫士在该设备试图成为根时，不允许其参与 STP。

6. 攻克 VLAN(Circumventing VLANs)

VLAN 将第 2 层物理网上的设备逻辑上分组。通常，交换机上的每个端口，除了中继端口，都被指定给一个 VLAN。中继线路在交换机间承载多个 VLAN 的流量。在中继线上，每个帧采用 802.1Q 或交换机间链路（InterSwitch Link，ISL）以识别源 VLAN。接收交换机从中继线上接收到帧后，剥离中继封装（802.1Q 或 ISL），将其转发到适当的 VLAN。通常，两个交换机协商一个端口是否启用了中继或是否承载了 VLAN。这种中继协商是不安全的，有可能暴露给恶意设备。

恶意设备可以和交换机协商中继。在交换机建立中继后，它将所有发给协商后的 VLAN 流量发给了恶意设备。这就使恶意设备攻克了 VLAN 分离，并与其他 VLAN 发送/接收帧。

为了避免这种威胁，您应该在面向用户的端口禁用中继协商。

10.4.5 NIPS

基于网络的入侵检测系统（Network based Intrusion Prevention Systems，NIPS）检测和分析网络流量以探测入侵。NIPS 有一个管理界面可以配置规则。当遇到有嫌疑的活动时，NIPS 提出警告。您可以有选择地配置 NIPS 执行重置数据连接，指导一个路由器拒绝来自恶意主机的流量等操作。

您可以在 IP 网络的 VoIP 侧和数据侧部署 NIPS。也就是，您可以配置 NIPS 检测语音流量或数据流量，防止入侵。因为在语音网络中可能的*流（flows）*是有限的，所以在 VoIP 环境中调谐 NIPS 相对容易。

10.4.6 第 3 层工具

除了上节讨论的第 2 层工具，在第 3 层也有各种工具用于减轻安全风险。本节假设您已经有了第 3 层设备和协议的基础知识。在下面的每一段中都有第 3 层相关技术的简短介绍，但不包含详细的操作说明。

1. 路由选择更新认证

路由选择协议用于在路由器间交换信息。缺省情况下，路由器部队发送路由选择更新

信息者进行认证。恶意设备可以假装成系统中的路由器，提供不正确的路由选择信息。这可能造成路由选择黑洞（DoS）或者使中间人攻击成为可能。

路由选择协议如最短路径优先（OSPF）和边界网关协议（BGP）支持路由选择消息的MD5 认证。如前所述，MD5 基于共享秘密方式。系统中的路由器可以通过共享密钥配置。发送者使用共享密钥对消息进行 MD5 哈希，将哈希结果添加到消息之后。接收者进行类似操作，以验证发送者和数据完整性。此过程不保证隐私性。

RIPv1 不支持内在安全机制。老的 RIPv2 实施只支持明文认证。

2. TCP 截取

TCP 客户端通过发送 TCP-SYN 消息来发起到服务器的连接。TCP 服务器为这个请求分配资源（接口、内存等），发送一个 SYN-ACK 给客户端。此时，TCP 服务器被认为拥有一个*半开放连接（ half-open connection*）。在 TCP 协议中，服务器等待一段时间（通常为 30 秒）来收取客户端回送的 ACK。

恶意设备可以通过大量的 TCP-SYN 消息使基于 TCP 的应用服务器泛滥。因为服务器不得不分配资源并等待每个 TCP 连接，资源很快就会被耗光，不能为其他请求提供服务。恶意设备还可以通过发送含有不可到达的源地址的 TCP-SYN 使情况更为严重。这就造成了攻击者的成功伪装并将服务器的 SYS-ACK 路由到一个黑洞。

路由器上的 TCP 截取功能（严格地讲，这是一个第 4 层功能）通过截取和验证 SYN 消息来降低 SYN 泛滥攻击的风险。

TCP 截取功能可以运行在*监视模式（watch mode）*和*截取模式（intercept mode）*。在监视模式中，第 3 层设备将 SYN 正常路由到服务器，等待一段时间看 TCP 连接是否建立。如果在一定时间内连接没有建立，第 3 层设备向服务器发送一个 RST，拆除连接。

在截取模式下，路由器应答来自客户端的 SYN。这个 SYN 不会到达服务器。路由器向客户端回送 SYN-ACK。如果客户端使用一个 ACK 回应，路由器就知道这是一个合法请求。然后路由器将原始的 SYN 发送给服务器，完成一次与服务器的三方握手。客户端和服务器此时拥有了一个 TCP 连接。

10.5 安全计划和策略

正如本章所讨论的一样，存在各种各样的威胁，同样存在各种各样的技术抵制这些威胁。就经验来讲，不可能部署可以抵制所有威胁的技术。您需要评估您网络的安全风险，确定最高风险。

您需要设计一个操作计划并形成文档，列出重要应用、设备和安全风险，并设定优先级。这个文档应该指导已部署的安全技术并为以后的实施区分优先级。这个操作计划应该也包含一个应急计划，略述安全突破后应采取的初始步骤。这个计划应该将内部政

策，如口令政策、访问控制和监控政策文档化，并与实施、执行和解决安全事务的主要联系人沟通。

下面各节中列出了您在制定这样一个计划时应该考虑的问题。

10.5.1 信任传递

信任传递（Transitive trust）是指由另一方传送过来的信任关系。例如，在一个有多个服务器元素的 VoIP 系统中，客户端可以只通过其中一个服务器的认证。其他服务器没有必要再认证一次。

在许多分布式系统中，这种信任模型非常普遍。当您使用这种模型时，服务器元素必须使他们的安全策略紧密一致，以防恶意设备攻击虚弱连接（weak links）。

10.5.2 VoIP 协议定义议题

如何定义已部署的 VoIP 技术和服务是制定安全计划时的一个重要角色。比如，运行在 PC 上的软电话（softphones）使数据和声音的分割更加复杂。

10.5.3 复杂性问题

在实施某项技术时，您还需要考虑复杂性和风险的比例。比如，公钥加密技术需要部署一些设施，如证书机构、证书等。而另一方面，一个公钥基础结构（Public Key Infrastructure，PKI）只需要最小日常维护。

10.5.4 NAT/防火墙穿越

防火墙通过检测信令消息内容来识别 VoIP 信令协议。根据信令消息的内容，他们为语音媒体打开一个针孔（pinholes）使其穿越。这些可以识别语音应用的防火墙有时被称作*应用层网关（Application-Layer Gateways，ALG）*。

但是当信令信息被加密后，防火墙就丧失了这种能力。因为防火墙无法检测信令消息的内容，媒体可能会被屏蔽。

所以，建议为 VoIP 使用专有的地址空间，而不是在 VoIP 地址空间内进行网络地址转换（Network Address Translation，NAT）。

10.5.5 口令和访问控制

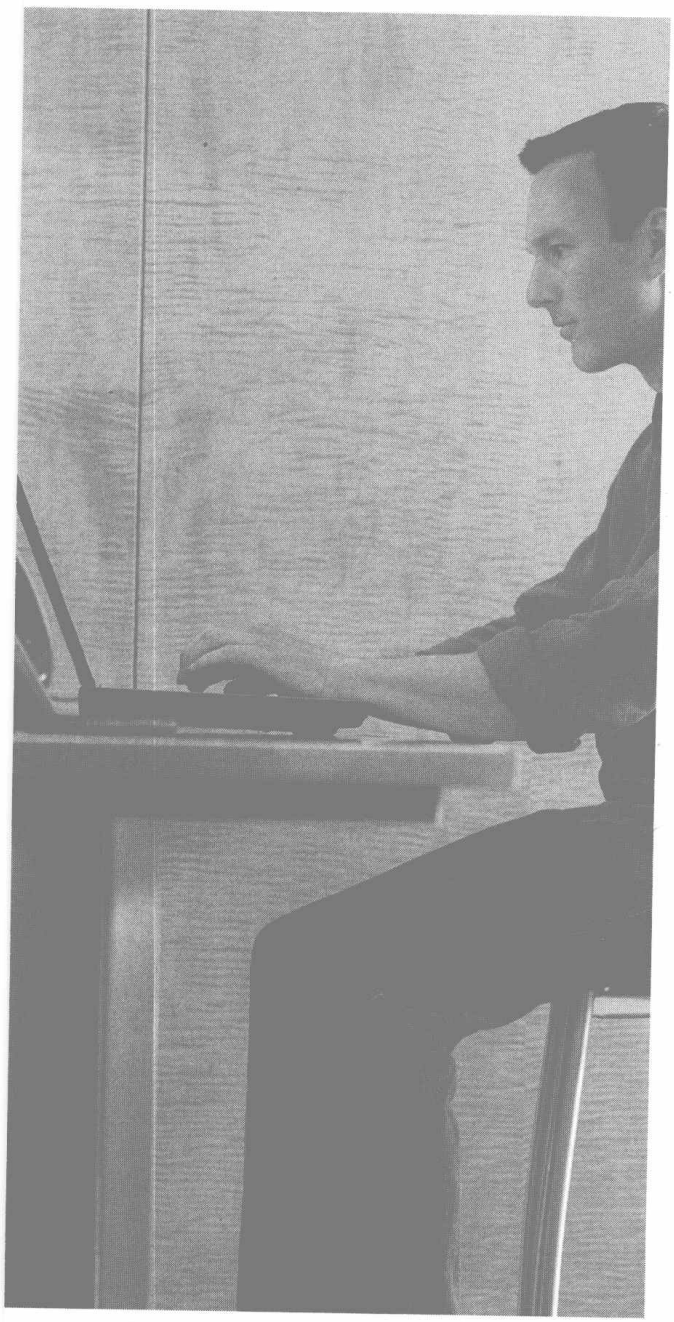
大多数设备有缺省又很容易被猜测的口令。对于所有的口令，您都得注意警惕它们被修改并保持秘密。比如，在 VoIP 环境中，您应该保密管理员和 SNMP 服务器的口令。

另外，如果用户可以物理接触到设备，设备可能允许重置口令（比如 IOS 设备的开机口令重置）。远程管理设备也很普遍。因为这些以及其他广泛的原因，严格控制物理接触设备和使用严格的带外管理系统是非常重要的。

10.6 总结

在设计和实施 VoIP 服务时，安全是一个重要的考虑因素。很自然地，它包含了从第 2 层设备到防火墙和证书机构等网络的各个方面。

目前有多种安全技术。评估安全风险和部署相关技术对保护 VoIP 服务来讲是十分必要的。



本章讨论网络架构框架和设计模型，包含以下主题：

- 11.1 H.323 元素
- 11.2 H.323 协议组
- 11.3 H.323 呼叫流程
- 11.4 总结

第11章

H.323

H.323 是 ITU-T 在 IP 网络上传输音频、视频和数据的规范。当符合 H.323 时，各厂商的产品和应用可以彼此互联。H.323 标准主要针对呼叫信令和控制、多媒体传输和控制，以及点对点和多点会议的带宽控制。H 系列的规范也为综合服务数据网络（Integrated Services Digital Network，ISDN）定义了 H.320，为普通老式电话（Plain Old Telephone Service，POTS）作为传输机制定义了 H.324。

目前，H.323v5（版本 5）是 ITU 批准的最新版本。表 11-1 列出了 H.323 标准包含的组件和协议。

表 11-1　　H.323 ITU 草案及相关草案附录

ITU 草案	相关附件	标题
H.323		分组多媒体通信系统
	附件 A	H.323 端点使用的 H.245 消息
	附件 B	分层视频编码器过程
	附件 C	ATM 上的 H.323
	附件 D	H.323 上的实时传真
	附件 E	UDP 上的多路呼叫信令
	附件 F	音频简单端点类型
	附件 G	文本简单端点类型
	附件 J	安全简单端点类型
	附件 K	基于 HTTP 的服务控制
	附件 L	刺激源控制协议
	附件 M1	H.323 信令隧道协议（QSIG）
	附件 M2	H.323 信令隧道协议（ISUP）
	附件 M3	贯穿 H.323 的 DSS1 隧道
	附件 P	在 H.323 上的调制解调信号转换
	附件 Q	远端相机控制和 H.281/H.224
	附件 R	H.323 实体的健壮方式

续表

ITU 草案	相关附件	标题
H.225.0		分组多媒体通信系统的呼叫信令协议和媒体流包优化
	附件 A	RTP/RTCP
	附件 B	RTP 轮廓
	附件 C	H.261 视频流的 RTP 负载格式
	附件 D	H.261A 视频流的 RTP 负载格式
	附件 E	视频包优化
	附件 F	音频和多元包优化
	附件 G	管理域间的通信
	附件 H	H.225.0 消息语法（ASN.1）
	附件 I	H.263+视频包优化
H.245		多媒体通信控制协议
	附件 A	消息：语法
	附件 B	消息：语义定义
	附件 C	过程
	附件 D	对象标识符分配
	附件 E	ISO/IEC 14496-2 功能定义
	附件 F	逻辑信道比特率管理功能定义
	附件 G	ISO/IEC 14496-1 功能定义
	附件 H	ISO/IEC 14496-3 功能定义
	附件 I	GSM 适应多速率功能定义
H.246		H 系列多媒体终端及 GSTN 和 ISDN 语音终端的互联
	附件 A	H.323-H.320 互联
	附件 C	ISUP/H.225.0 互联
	附件 E.1	MAP/H.225.0 互联
	附件 E.2	ANSI-41 MAP/H.225.0 互联
	附件 F	H.323-H.324 互联
H.235.0		H 系列（基于 H.323 和另外 H.245）多媒体系统的安全框架
H.235.1		基线安全规范
H.235.2		签名安全规范
H.235.3		混合安全规范
H.235.4		直接和选择路由呼叫安全
H.235.5		RAS 中使用弱共享秘密的安全认证框架

续表

ITU 草案	相关附件	标题
H.235.6		H.235/H.245 秘钥管理语音加密规范
H.235.7		SRIP 的 MIKEY 密钥管理协议的使用
H.235.8		使用安全信令信道交换 SRTP 密钥
H.235.9		H.323 的安全网关支持
H.450.1		支持 H.323 附加协议的通用功能协议
H.450.2		H.323 的呼叫转移附加服务
H.450.3		H.323 的呼叫转接附加服务
H.450.4		H.323 的呼叫保持附加服务
H.450.5		H.323 的呼叫驻留和呼叫提取附加服务
H.450.6		H.323 的呼叫等待附加服务
H.450.7		H.323 的消息等待提示附加服务
H.450.8		H.323 的名字鉴别附加服务
H.450.9		H.323 的呼叫完成附加服务
H.450.10		H.323 的呼叫提供附加服务
H.450.11		呼叫入侵附加服务
H.450.12		H.323 的通用信息附加网络功能
H.460.1		通用扩展框架使用指导
H.460.2		H.323 和 SCN 网络的可携带号码因特网络
H.460.3		电路状态图
H.460.4		呼叫优先设定
H.460.5		多 Q.931 IEs 传输
H.460.6		扩展快速连接
H.460.7		数字映射
H.460.8		备用路由查询
H.460.9		QoS 监控报告
H.460.10		呼叫方分类
H.460.11		延迟呼叫建立
H.460.12		双占用控制指示器
H.460.13		被叫用户释放控制
H.460.14		多级优先和占先
H.460.15		呼叫信令传输信道中止和转向
H.460.16		多消息释放序列功能

续表

ITU 草案	相关附件	标题
H.460.17		H.225.0 的 RAS 隧道
H.460.18		H.323 信令的 NAT 与防火墙穿透
H.460.19		H.323 媒体的 NAT 与防火墙穿透
H.460.20		H.323 的位置号码
H.501		移动管理和多媒体系统的域内/间通信协议
H.510		H.323 多媒体协议的移动性
H.530		H.510 的对称安全过程

H.323 系统在下面 3 节中讨论：

- H.323 元素；
- H.323 协议组；
- H.323 呼叫流程。

11.1 H.323 元素

图 11-1 列出了 H.323 系统元素。这些元素包括终端、网关、关守和多点控制单元（Multipoint Control Units，MCU）。

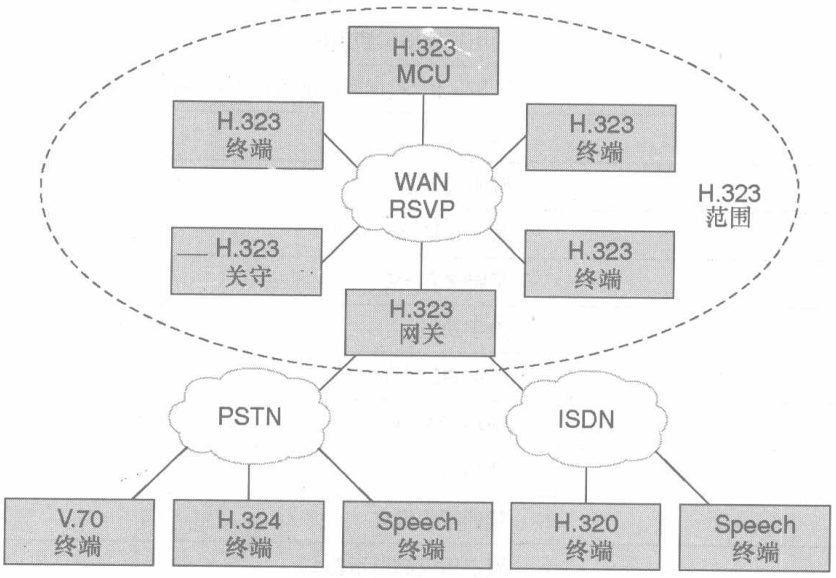


图 11-1 H.323 组网元素

终端经常被称作端点，主要为音频、视频和数据提供点对点和多点会议。网关连接到公共交换电话网络（PSTN）或 ISDN 网络上，使 H.323 端点可以交互工作。关守为终端或网关提供入场控制以及服务地址的转换。MCU 是允许两个或多个终端或网关通过音频和/

或视频会话进行会议的设备。

11.1.1 终端

图 11-2 中列出的网络元素在 H.323 中定义为终端（terminal）。H.323 终端必须有一个系统控制单元、媒体传输、音频编码器和基于包的网络接口。可选的需求包括一个视频编码器和用户数据应用。

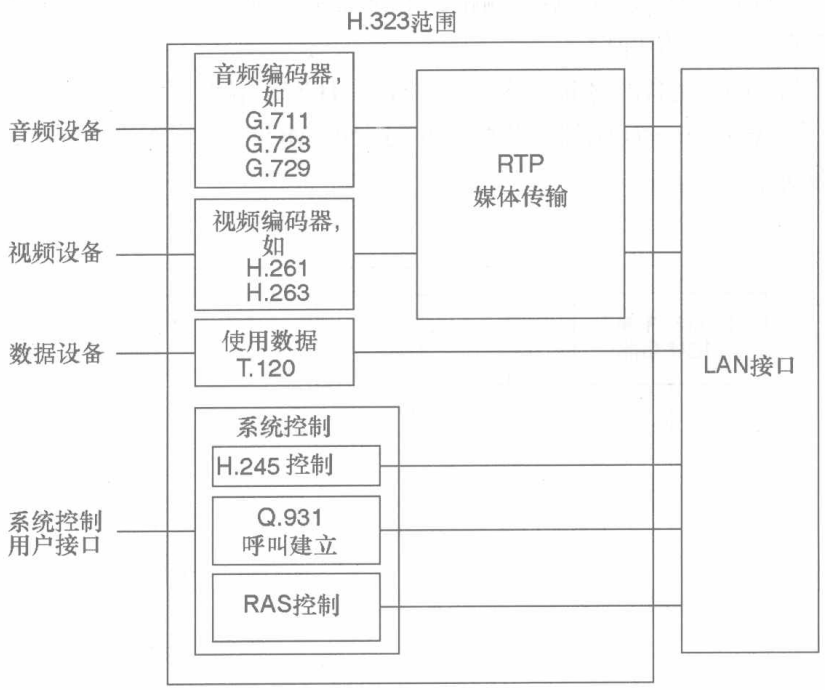


图 11-2 H.323 组件关系

下列是 H.323 终端范围内的功能和能力。

- 系统控制单元（System Control Unit）——提供 H.225 和 H.245 呼叫控制，可以为终端的核实操作交换、消息和信令命令。
- 媒体传输（Media Transmission）——格式化传输的音频、视频、数据、控制流和消息到网络接口。媒体传输也从网络接口接收音频、视频、数据、控制流和消息。
- 音频编码器（Audio Codec）——编码来自音频设备的信号用以传输，解码接收到的音频编码。所需要的功能包括编码和解码 G.711 语音，传输和接收 a-law 和 μ-law 格式。可选的有支持 G.722、G.723.1、G.728 和 G.729 编码和解码。
- 网络接口（Network Interface）——一个基于包的接口，允许单点和多点传送服务的端到端的传输控制协议（TCP）和用户数据报协议（UDP）。
- 视频解码器（Video Codec）——可选，但如果提供，必须可以根据 H.261/H.263 标准编码和解码视频。

- 数据信道（Data Channel）——如 T.120 建议书定义的支持入数据库访问、文件传输、*音频图形会议（audiographics conferencing）*（在多个用户计算机上同时修改图像的能力）。

11.1.2 网关

H.323 网关反映了交换电路网络（Switched Circuit Network，SCN）端点和 H.323 端点的特性。它在音频、视频、数据传输格式和通信系统和协议之间进行转换，包括 IP 网络和 SCN 的所有呼叫建立和拆除。

只有在与 SCN 互联时才需要网关。所以，H.323 端点可以同分组网络直接通信，无须连接网关。网关担当一个 H.323 终端或网络上的 MCU 和 SCN 终端或者 SCN 上的 MCU，如图 11-3 所示。

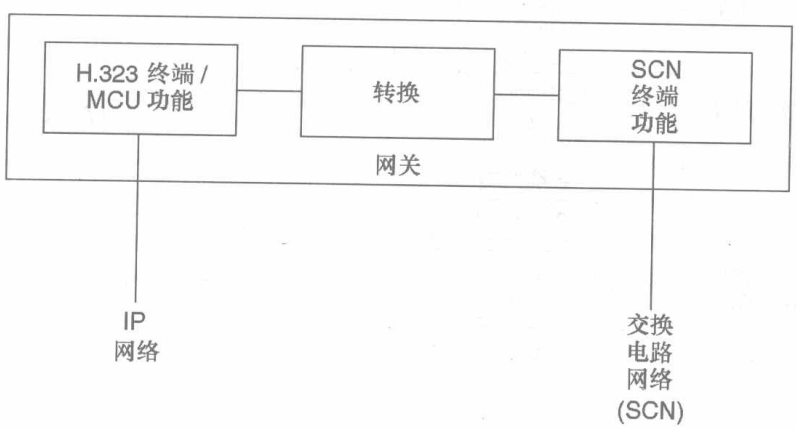


图 11-3 H.323 网关元素

11.1.3 关守

关守为 H.323 端点提供呼叫前和呼叫级控制服务，是一个可选的功能。在 H.323 环境中，关守被逻辑地从其他网络元素分开。如果实施了多个关守，它们之间的通信以不确定的方式完成。

关守可以为远程用户使用简单的查询/响应序列（位置请求（Location Request，LRQ）或位置确认（Location Confirmation，LCF）新版本的 H.323，如 H.323 版本 4 和 5 已经试图建议关守间通信规范。H.323 v3 附件 G/H.225.0 提供“管理域间的通信（Communication between Administrative Domains）”。这个新的附件为 H.323 关守提供了执行以可拓展的方式地址解析和价格交换的能力，这有助于开发大规模的 H.323 网络。

另一种协议，开放结算协议（Open Settlements Protocol，OSP）也定义为欧洲电信标准协会（European Telecommunication Standards Institute，ETSI）TS 101 321 被广泛应用在从网关和关守的域间交互。OSP 提供允许网络电话操作员之间交换域间定价、认证和结算

信息的机制。

如果在 H.323 系统中存在关守，它必须履行如下职能。

- 地址转换（Address Translation）——根据 H.323 别名（如 pc1@cisco.com）或 E.164 地址（标准的电话号码）提供端点的 IP 地址。
- 许可控制（Admissions Control）——使用许可请求/许可确认/许可拒绝（Admission Request/ Admission Confirm/Admission Reject，ARQ/ACF/ARJ）消息提供 H.323 访问授权，将在本章后面的 11.2.1 节讨论。
- 带宽控制（Bandwidth Control）——使用带宽请求/带宽确认/带宽拒绝（Bandwidth Request/Bandwidth Confirm/Bandwidth Reject，BRQ/BCF/BRJ）消息管理端点贷款需求，将在本章后面的 11.2.1 节讨论。
- 区域管理（Zone Management）——为注册后的终端，网关和 MCU 提供，将在本章后面的 11.2.1 节中进一步讨论。

关守还提供如下可选功能：

- 呼叫控制信令（Call Control Signaling）——使用关守路由的呼叫信令（Call Control Signaling）模型，将在本章后面的 11.2.2 节讲述。
- 呼叫授权（Call Authorization）——使关守限定对某个终端和网关的访问，或根据时间日期策略控制访问。
- 带宽管理（Bandwidth Management）——在所需带宽不被满足时，允许关守拒绝使用。
- 呼叫管理（Call Management）——维护一个活动呼叫列表，用来确定一个端点是否忙。

11.1.4 MCU 和元素

多点控制器（MC）支持三方或更多端点的多点会议。MC 向每个多点会议中的端点传送功能集，还可以在会议中修改功能集。MC 功能可以存在于终端、网关、关守或 MCU 中。

多点处理器（multipoint processor，MP）接收音频、视频和/或数据流，分发他们到参加多点会议的端点。

MCU 是一个支持多点会议并且最少由一个 MC 以及一个或多个 MP 组成的端点。如果它支持集中的多点会议，一个典型的 MCU 由一个 MC 和一个音频、视频和数据的 MP 组成。

11.1.5 H.323 代理服务器

H.323 代理服务器是专门为 H.323 协议设计的代理。这个代理运行在应用层，可以检查两个通信应用间的包。代理可以确定呼叫的目的地，在需要的时候执行连接。代理支持如下主要功能。

- 不支持资源预留协议（Resource Reservation Protocol，RSVP）的端点可以通过有相对较好 QoS 的局域网访问到代理。代理对然后可以协商通过 IP 网络的足够 QoS。代理可以使用 RSVP 和/或 IP 优先权位管理 QoS。
- 代理通过基于应用的路由选择（application-specific routing，ASR）将 H.323 流量从日常数据流中分离进行路由选择。
- 代理与网络地址转换（NAT）相兼容，允许 H.323 使用私有地址空间在网络中部署。
- 没有防火墙或独立于防火墙部署的代理提供安全防护，只允许 H.323 流量通过。与防火墙一起部署的代理允许防火墙将代理简单设为一个可信任点，允许通过所有的 H.323 流量。这就使防火墙提供数据组网的安全性，代理提供 H.323 安全性成为可能。
- H.323 代理在这种模型中也被称为*双关守(DUAL Gatekeeper)*，因为它执行了 H.323 关守和代理服务器的双重功能。更常用的是，H.323 网关允许在私网上或防火墙后面的 H.323 客户端如 NetMeeting 在因特网上打多媒体电话。

11.2 H.323 协议组

H.323 协议组由如图 11-4 所示的多种协议组成。这组协议支持呼叫许可、建立、状态、拆除、媒体流和 H.323 系统消息。这些协议支持数据网上的可靠和不可靠包传输。

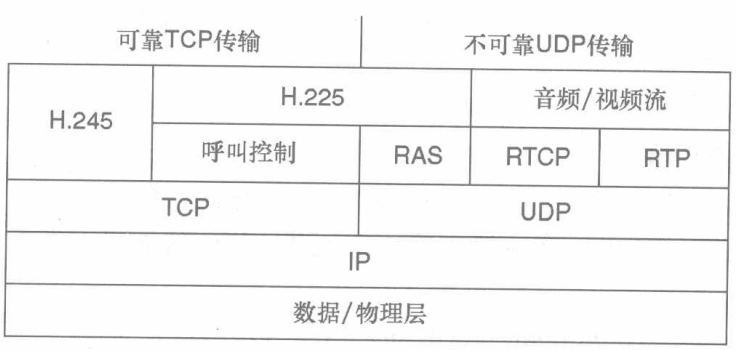


图 11-4 H.323 协议组层次模型

虽然目前大多数 H.323 实施使用 TCP 作为信令传输机制，H.323 版本 2 支持基本的 UDP 传输。而且，其他标准化组织也在致力于使用其他可靠 UDP 机制以建立更广泛的信令模式。

H.323 协议组主要进行 3 方面的控制。

- 注册、许可和状态（Registration，Admissions，and Status，RAS）信令——在 H.323 基于关守网络中提供呼叫前控制。
- 呼叫控制信令（Call Control Signaling）——被用来连接、维护和断开端点间呼叫。

- 媒体控制和传输（Media Control and Transport）——提供可靠的 H.245 信道承载媒体控制消息。传输在不可靠的 UDP 流进行。

本节剩余部分将集中讨论这 3 种主要信令功能。

11.2.1 RAS 信令

在关守和区域（zone）存在的 H.323 网络中，RAS 信令提供呼叫前控制。RAS 信道通过 IP 网络在端点和关守之间建立。在其他信道建立前，RAS 信道是开放的，而且独立于呼叫控制信令和媒体传输信道。这个不可靠的 UDP 连接承载执行注册、许可、带宽改变、状态和脱离过程的 RAS 消息。

1. 关守发现

关守发现是一个端点确定注册哪个关守的手工或自动的过程。在手工方式，端点使用关守 IP 地址配置，这样就可以立即尝试注册，但只能注册预先定义的关守。自动方式允许端点和关守之间的关系随着时间变化，但需要一个被称为*自动发现（auto discovery）*的机制。

自动发现允许不知道关守的端点通过一个多点广播消息来发现它的关守。因为端点没有必要被静态配置或重新配置关守，所以这种方式不需要太多的管理任务。关守发现的多点广播地址是 224.0.1.41，关守 UDP 发现端口是 1718，关守 UDP 注册和状况端口是 1719。下列 RAS 消息被用来 H.323 关守自动发现。

- 关守请求（Gatekeeper Request，GRQ）——由端点发送用来查找关守的多点广播传播消息。
- 关守确认（Gatekeeper Confirm，GCF）——回复端点 GRQ，指明关守 RAS 信道的传输地址。
- 关守拒绝（Gatekeeper Reject，GRJ）——通知端点关守不接受它的注册。这通常是由于网关和关守的配置造成的。

图 11-5 显示了自动发现的消息和序列过程。

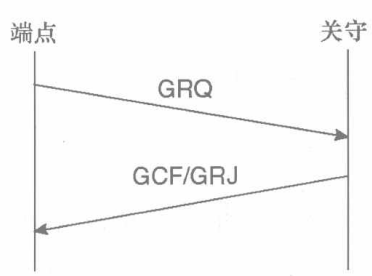


图 11-5 关守自动发现

为了冗余，关守在 GCF 消息中可以指明备用关守。在主关守不能使用时，您可以使用备用关守。

2. 注册

注册是允许网关、端点和 MCU 加入一个区域和通知关守他们 IP 和别名地址的过程。注册是在发现过程之后，尝试任何呼叫之前的必要过程。可以使用以下 6 个消息进行端点注册和取消注册：

- 注册请求（Registration Request，RRQ）——由端点发给关守 RAS 信道地址；
- 注册确认（Registration Confirm，RCF）——由关守发送，确认端点注册；
- 注册拒绝（Registration Reject，RCJ）——由关守发送，拒绝端点注册；
- 取消注册请求（Unregister Request，URQ）——由端点或关守发送取消一个注册；
- 取消注册确认（Unregister Confirm，UCF）——由端点或关守发送，确认取消注册请求；
- 取消注册拒绝（Unregister Reject，URJ）——表明端点没有在该关守注册。

图 11-6 显示了端点注册以及端点和关守取消注册的消息和序列过程。

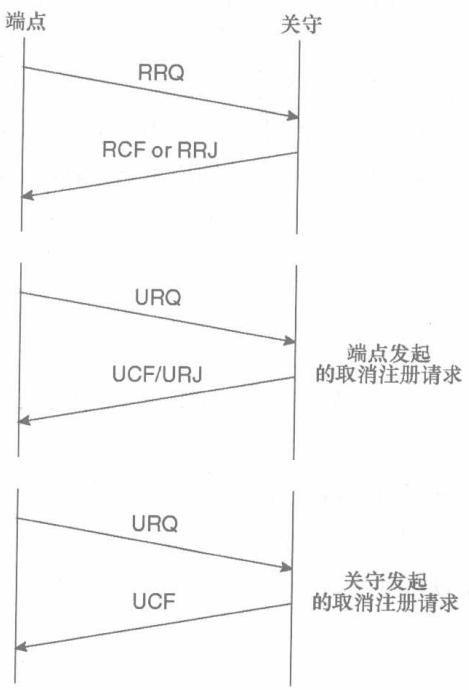


图 11-6 端点注册以及端点和关守取消注册

3. 端点位置

当只有别名信息时，端点和关守使用*端点位置（endpoint location）*来获得联系信息。位置消息被发送到关守 RAS 信道地址或多点广播到关守发现的多点广播地址。关守通过指明它自己的或端点的联系信息来请求端点的响应。

端点或关守在请求中可以包含一个或多个区域外 E.164 地址。使用如下 3 个消息定位端点。

- 位置请求（Location Request，LRQ）——被发送为一个或多个 E.164 地址请求端点或关守的联系信息。

- 位置确认（Location Confirm，LCF）——由关守发送，包含它自己的或被请求的端点的呼叫信令信道或 RAS 信道地址。在使用 GKRCS 时它使用它自己的地址，当使用直接端点呼叫信令（Direct Endpoint Call Signaling）时使用被请求的端点地址。
- 位置拒绝（Location Reject，LRJ）—— 由接收到 LRQ 的关守发送，指明被请求的端点没有注册或有无效资源。

4．许可

在端点和关守之间的许可（Admission）消息提供基本的呼叫许可和带宽控制。关守通过确认或拒绝许可请求来授权访问 H.323 网络。一个许可请求包含请求的带宽，关守在确认时可以减少该带宽。以下消息在 H.323 网络中提供许可控制。

- 许可请求（Admission Request，ARQ）——发起呼叫端点的一个尝试。
- 许可确认（Admission Confirm，ACF）——关守容许呼叫的授权。
- 许可拒绝（Admission Reject；ARJ）——拒绝端点为某个呼叫访问网络。

ACF 消息包含终结网关或关守的 IP 地址，使起源网关立即发起呼叫信令过程。

5．状态信息

关守可以使用 RAS 信道获得端点的状态信息。在失败情况下，您可以使用这个消息监控端点是否在线。通常状态消息的轮询时间是 10 秒。在 ACF 中，关守也可以请求端点在呼叫中定期发送状态信息。您可以使用如下消息在 RAS 信道中提供状态情况。

- 信息请求（Information Request，IRQ）——由关守发送个端点请求状态。
- 信息请求响应（Information Request Response，IRR）——从端点发送给关守，响应 IRQ。当关守请求定期状态更新时，端点也发送这个消息。
- 状态查询（Status Enquiry）——被发送出 RAS 信道，在呼叫信令信道上。端点或关守可以向另一个端点发送状态查询消息以验证呼叫状态。关守通常使用这个消息来验证呼叫是否还在进行中。

6．带宽控制

带宽控制最初是通过端点与关守的许可交换管理的，使用 ARQ/ACF/ARJ 序列完成。然而，在呼叫过程中，带宽是可以改变的。您可以使用以下消息来改变带宽。

- 带宽请求（Bandwidth Request，BRQ）——由端点发给关守请求增加或减少呼叫带宽。
- 带宽确认（Bandwidth Confirm，BCF）——由关守发送，确认接受带宽改变请求。
- 带宽拒绝（Bandwidth Reject，BRJ）——由关守发送，拒绝带宽改变请求（当请求的带宽无效时发送）。

注释：带宽控制只与关守与网关有关，不考虑当前的网络状态和端点的媒体能力（如编码器类型）。关守目前只根据它的静态带宽表来决定接收还是拒绝带宽请求。

11.2.2 呼叫控制信令（H.225）

在H.323网络中，呼叫控制过程基于ITU的H.225建议书，H.225建议书定义了对Q.931信令消息的使用和支持。可靠的呼叫控制信道在IP网络上TCP端口1720建立。这个端口在两个端点之间为连接、维护和断开呼叫发起Q.931呼叫控制消息。

实际呼叫控制和保持活动消息在发起呼叫建立后移到临时端口（该端口由机器的IP栈为特殊用途分配）。1720是一个H.323呼叫的常用端口。H.225也为附加服务定义了Q.932消息的使用。以下的Q.931和Q.932消息是在H.323网络中最常使用的信令消息。

- 建立（Setup）——由H.323呼叫实体在试图建立连接时发给H.323被叫实体的前向消息。这个消息通过著名的H.225 TCP端口1720发送。
- 呼叫进行（Call Proceeding）——由被叫实体发给呼叫实体的后向消息，通知开始呼叫建立过程。
- 发信号（Alerting）——由被叫实体发送，通知被叫实体开始振铃。
- 连接（Connect）——由被叫实体发给主叫实体的后向消息，表明被叫方接听呼叫。连接消息中可以含有为H.245控制信令的UDP/IP传输地址。
- 释放完成（Release Complete）——由端点发送，开始断开连接，表明呼叫正在被释放。只有在呼叫信令信道开放或活动时，才可以发送这个消息。
- 功能（Facility）——被用于请求或确认附加服务的Q.932消息。也被用来表明一个呼叫是否应该被控制或者通过一个关守。

图11-7显示了呼叫建立的信令消息。与关守的交互被限制在为呼叫许可，可能和状态的RAS消息上。

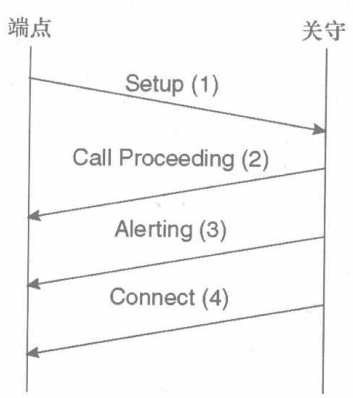


图 11-7 呼叫建立信令消息

您可以通过两种方式在H.323网路中路由呼叫信令信道：

- 直接端点呼叫信令（Direct Endpoint Call Signaling）；
- GKRCS。

在直接端点呼叫信令方式中，呼叫信令消息在两个端点之间直接传送，如图11-8所示。端点可以通过多种方式提供源信息，例如中继组ID、H.323 ID和中继组（trunk group，TG）

等。利用了这种方式优点的 GK 应用/功能有最少呼叫路由选择（Least Call Routing，LCR）、控制列表等，因为他们接受所有类型的源消息。

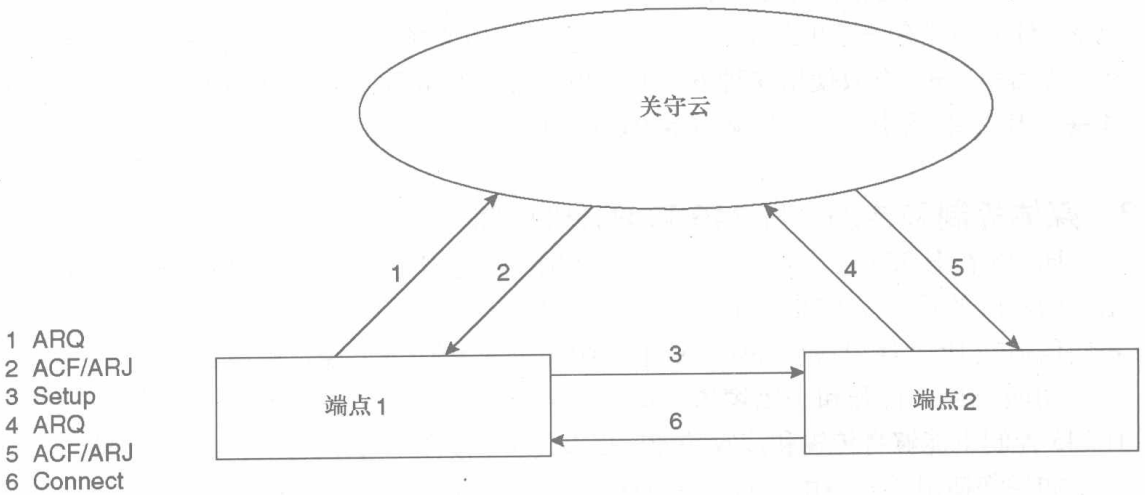
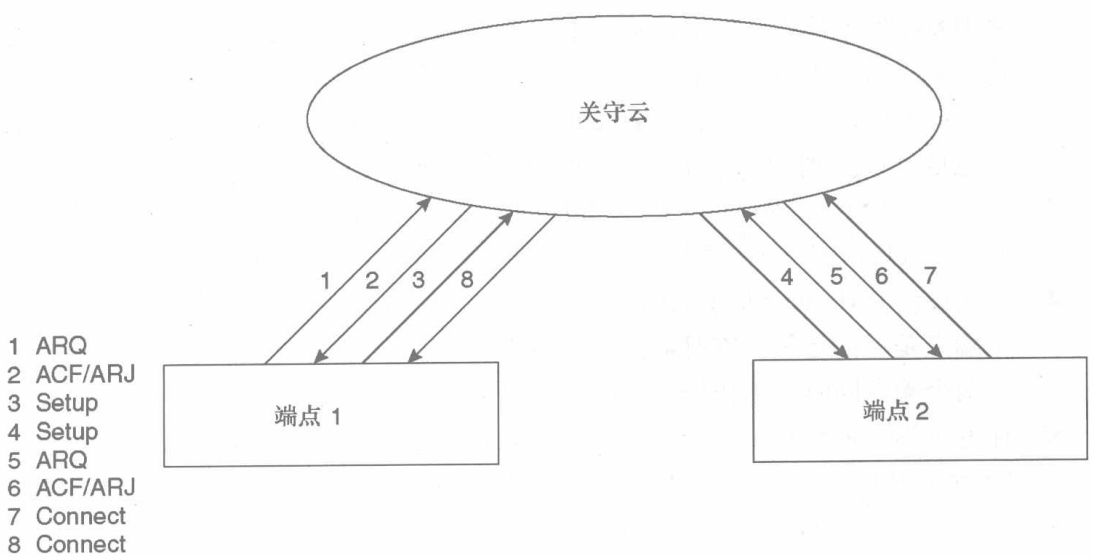


图 11-8 直接端点呼叫信令

在 GKFCS 方式，端点间的呼叫信令消息通过关守路由，如图 11-9 所示。在这种方式中，端点向关守中的路由引擎（route engines，RE）提供源信息（如客户 ID）来协助不同集团间的呼叫。端点应该将从 RE 接收到的任何客户 ID 以保证正确的来电显示服务。



注：在图11-8和图11-9中，建立（Setup）和连接（Connect）消息是呼叫信令消息，剩余的消息是RAS信道消息。

图 11-9 关守路由的呼叫信令

如果呼叫信令信道在呼叫过程中是开放的，您可以通过 GKRCS 方式提供附加服务。关守也可以在呼叫建立完成后，关闭呼叫信令信道。一些应用（例如，VoIP 批发(Wholesale VoIP)）需要准确的呼叫使用情况报告和集中供应网络元素，所以倾向于 GKRCS 方式。在其他情况下，GW 不能有一点儿失败，客户 ID 和智能路由选择是非常重要的因素时，应用倾向于直接端点信令方式。有效使用这种方式的应用有最少费用路由选择（Least Cost Routing，LCR）和基于 IP 的联系中心（IP based Contact Center）。

11.2.3 媒体控制和传输（H.245 和 RTP/RTCP）

H.245 在 H.323 实体之间处理端到端控制消息。H.245 过程为音频、视频、数据和控制信道信息的传输建立逻辑信道。端点为每个呼叫建立一条与参与端点的 H.245 信道。可靠控制信道在 IP 上使用最后呼叫信令消息中动态分配的 TCP 端口被建立。

功能交换、打开和关闭逻辑信道、优先选择模式和消息控制都发生在这条信道上。H.245 控制也能够将传输和接收功能，以及协商函数如决定使用哪种编码器分离。

如果您使用关守路由呼叫信令（Gatekeeper Routed call signaling），您可以通过两种方式控制信道路由选择。您可以使用在两个参与端点之间的直接发生的*直接 H.245 控制 (Direct H.245 Control)*。或者，您可以使用发生在端点和它的关守之间的*关守路由的 H.245 控制 (Gatekeeper Routed H.245 Control)*。

您可以使用以下的过程和消息来启动 H.245 控制操作。

- 功能交换——由在两个端点（也被称为终端）之间安全交换功能的消息组成。这些消息指明了终端传输和接收音频、视频和数据到参与终端的能力。对于音频，功能交换包括声音编码器之间的转换，如 G 系列 8kbit/s 的 G.729、16kbit/s 的 G.728、64 kbit/s 的 G.711、5.3 或 6.3kbit/s 的 G.723，或者 48、56 和 64 kbit/s 的 G.722。它还包括 ISO 系列的 32、44.1 和 48 kHz 采样速率的 IS.11172-3，以及 16-、22.05-、24、32、44.1 和 48 kHz 采样速率的 IS.13818-3，以及 GSM 全速率（full-rate）、半速率（half-rate）和增强全速率（enhanced full-rate）的音频解码器。
- 主从终结（Master-Slave Termination）——用于确定特定呼叫中哪个端点是主，哪个端点是从的过程。在呼叫过程中这个关系被维持并被用于解决端点间的冲突。当两个端点同时请求相似操作时，使用主从规则。
- 往返延迟（Round Trip Delay）——用于确定起始和终结端点间的延迟的过程。**RoundTripDelayRequest** 消息测量延迟并验证远程 H.245 协议实体是否活动。
- 逻辑信道信令（Logical Channel Signaling）——打开和关闭承载音频、视频和数据信息的逻辑信道。在真正传输之前，信道已经被建立保证终端已经准备好接收和解码信息。建立单向和双向信道使用一样的信令消息。在逻辑信道信令成功建立后，RTP 媒体的 UDP 端口被从终结端点发送给起始端点。而且，在使用关守呼叫控制模型时，此时关守可以通过提供终结端点的真实的 UDP/IP 地址转向 RTP 流。

1. 快速连接过程（Fast Connect Procedures）

两个有效的在端点间建立媒体信道的过程是 H.245 和快速连接（Fast Connect）。快速连接为基本点到点呼叫启用媒体连接建立，该呼叫有一个往返消息交换。这些过程指示主叫端点在初始建立消息中包含*快起（faststart）*元素。

快起部分包括逻辑信道序列、媒体信道功能和必要的用来打开开始媒体传输的参数。作为响应，被叫端点返回一个 H.225 消息（呼叫进行、进展、警示或连接）包含一个选择接收终端功能的快起元素。此时，如果基于 H.225 的建立序列到达连接状态，主叫和被叫端点可以开始传输媒体。

这种方式加快了呼叫建立的时间，而且比执行 H.245 控制消息要简单得多。

2. H.245 隧道

您可以将 H.245 消息封装在 H.224 呼叫信令信道内，而不是建立一条单独的 H.245 控制信道。这种方式改进了呼叫建立时间和资源分配，并且可以提供呼叫信令和控制的同步。您可以封装多个 H.245 消息在任何 H.225 消息中。而且，任何时间、任何端点都可以转到一个单独的 H.245 连接。

快起方式（也被称为 H.450.6 扩展快速连接（Extended Fast Connect，EFC））对于某些应用特别有用，例如在网络中间的一个网络元素想向主叫端点在连接呼叫前播放某个媒体时（比如，通知余额或者表明呼叫正在进行）。在没有快起之前，内部网络元素不得不执行 H.245 逻辑信道建立来传输消息。内部网络元素然后不得不发送一个“空功能集（Empty Capability Set）”消息给主叫端点，将 H.225.0 和 H.245 信令重定向到被叫端点，并交换一个 H.245 数字来复原媒体。使用快起，过程简单化了而且呼叫建立时间被减少了。

3. 呼叫终结

参与呼叫的任一端点可以发起呼叫终结过程。首先，端点必须停止媒体传输（如音频、视频或数据）并关闭所有逻辑信道。然后，它必须结束 H.245 会话并在呼叫信令信道上（如果它仍然打开或活动的话）发送一个完全释放消息。此时，如果没有关守出现，呼叫就被终结了。当关守出现时，下面的消息被用在 RAS 信道上来完成呼叫终止。

- 脱离请求（Disengage Request，DRQ）——由端点或关守发送以终止一个呼叫。
- 脱离确认（Disengage Confirm，DCF）——由端点或关守发送，确认断开了呼叫连接。
- 脱离拒绝（Disengage Reject，DRJ）——由端点或关守发送，拒绝了断开呼叫连接。

4. 媒体传输（RTP/RTCP）

RTP 提供 H.323 中的媒体传输。更确切地说，RTP 允许在单点或多点网络上的音频、

视频和数据实时、端到端地传输。打包和传输服务包括负载识别、序列化、时间戳和监管。

RTP 依靠其他机制和下面几层来保证按时发送、资源预留、可靠性和 QoS。RTCP 监管数据传输，也控制和鉴别服务。媒体信道使用 UDP 建立，RTP 流在运行在一个偶数端口，相应的 RTCP 流运行在高一个（奇数）端口上。

11.3 H.323 呼叫流程

在本节中勾画的呼叫流程演示了 H.323 协议家族在两个端点间建立呼叫的方法。假设它们是语音呼叫，所有端点都已经注册到了相应的关守上。呼叫建立的例子包含了两个不同的关守实施和两个不同的信令方式。

图 11-10 和图 11-11 的例子列出了单个关守实施的呼叫建立过程 图 11-10 列出了两个端点共享一个关守使用直接端点信令的呼叫流程。

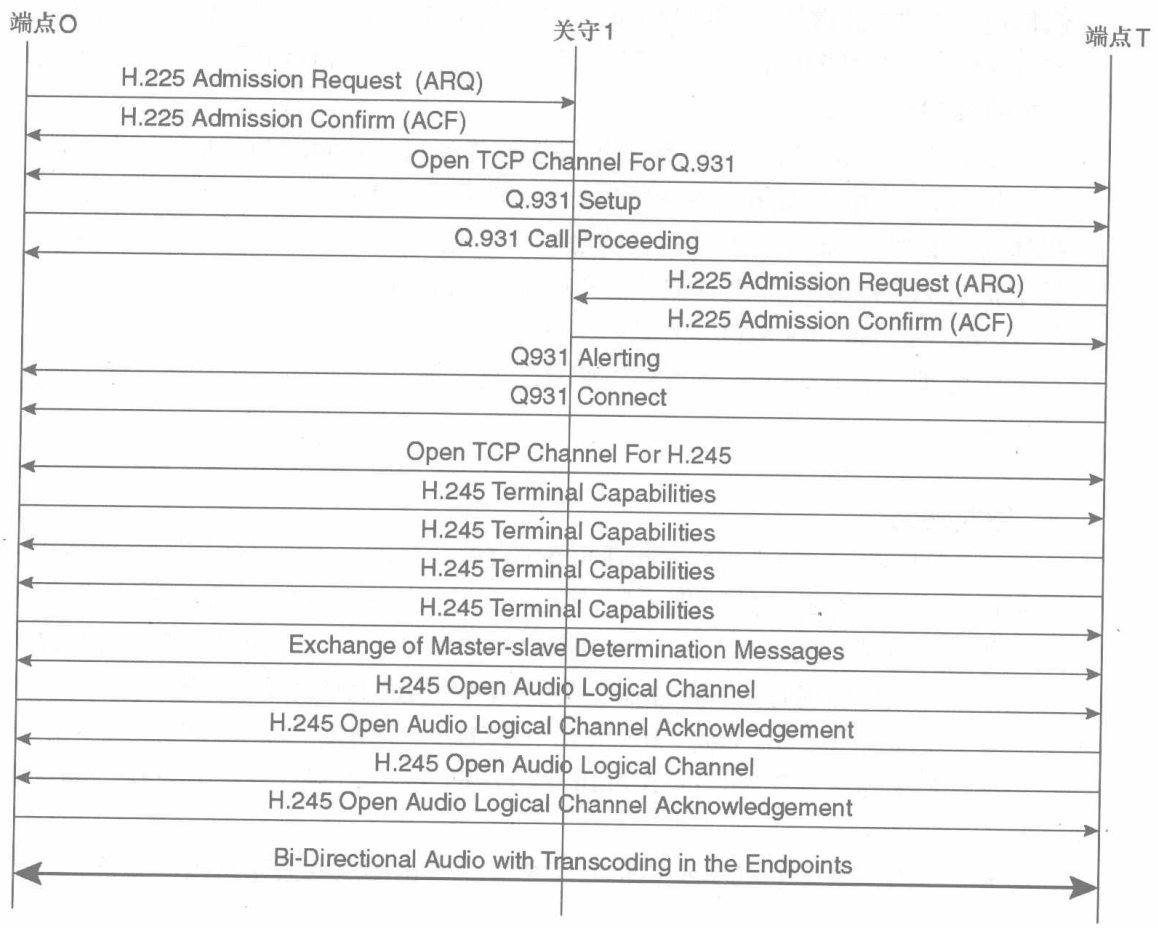


图 11-10 直接端点信令——同一关守

图 11-11 显示了两个共享关守的端点使用关守呼叫路由信令的呼叫流程。注意，H.245 过程被在端点间处理而不是由关守路由。

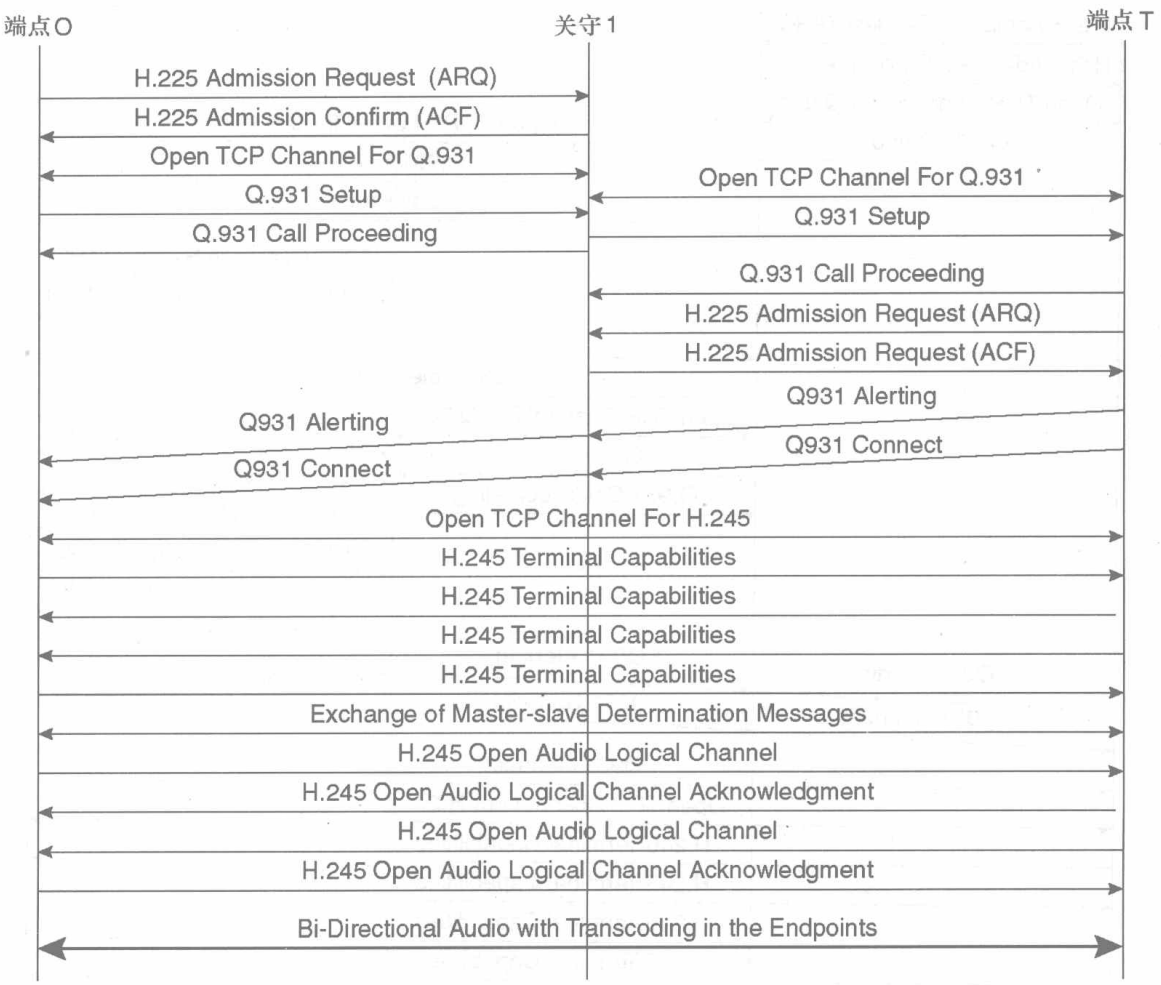


图 11-11 关守路由呼叫信令——同一关守

图 11-12 和图 11-13 的例子列出了两个关守实施的呼叫建立过程。特别要指出的是，图 11-12 显示的是两个有不同关守的端点间使用直接端点信令的呼叫流程。GKRCS 与直接呼叫信令的区别在于，在 GKRCS 中，建立消息指向关守，而直接呼叫信令中指向终结端点。

最后的 H.323 呼叫流程例子演示了两个有不同的关守的端点使用 GKRCS 方式的呼叫建立过程。这允许 LRQ 和 LCF 在两个关守间发送，因为所有的建立和控制信息都通过关守，所以允许在关守上控制计费记录。

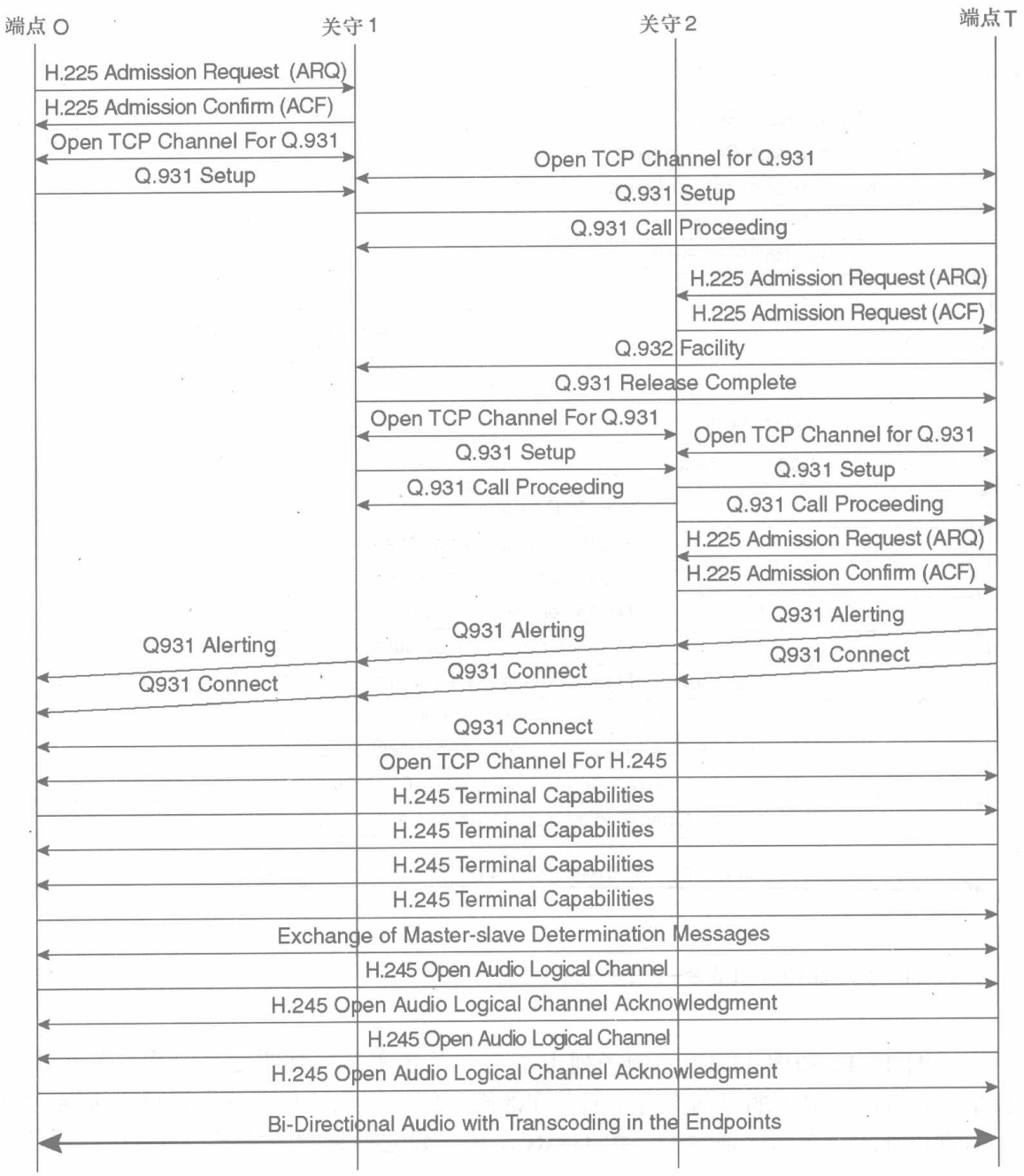


图 11-12 直接端点信令——两个关守

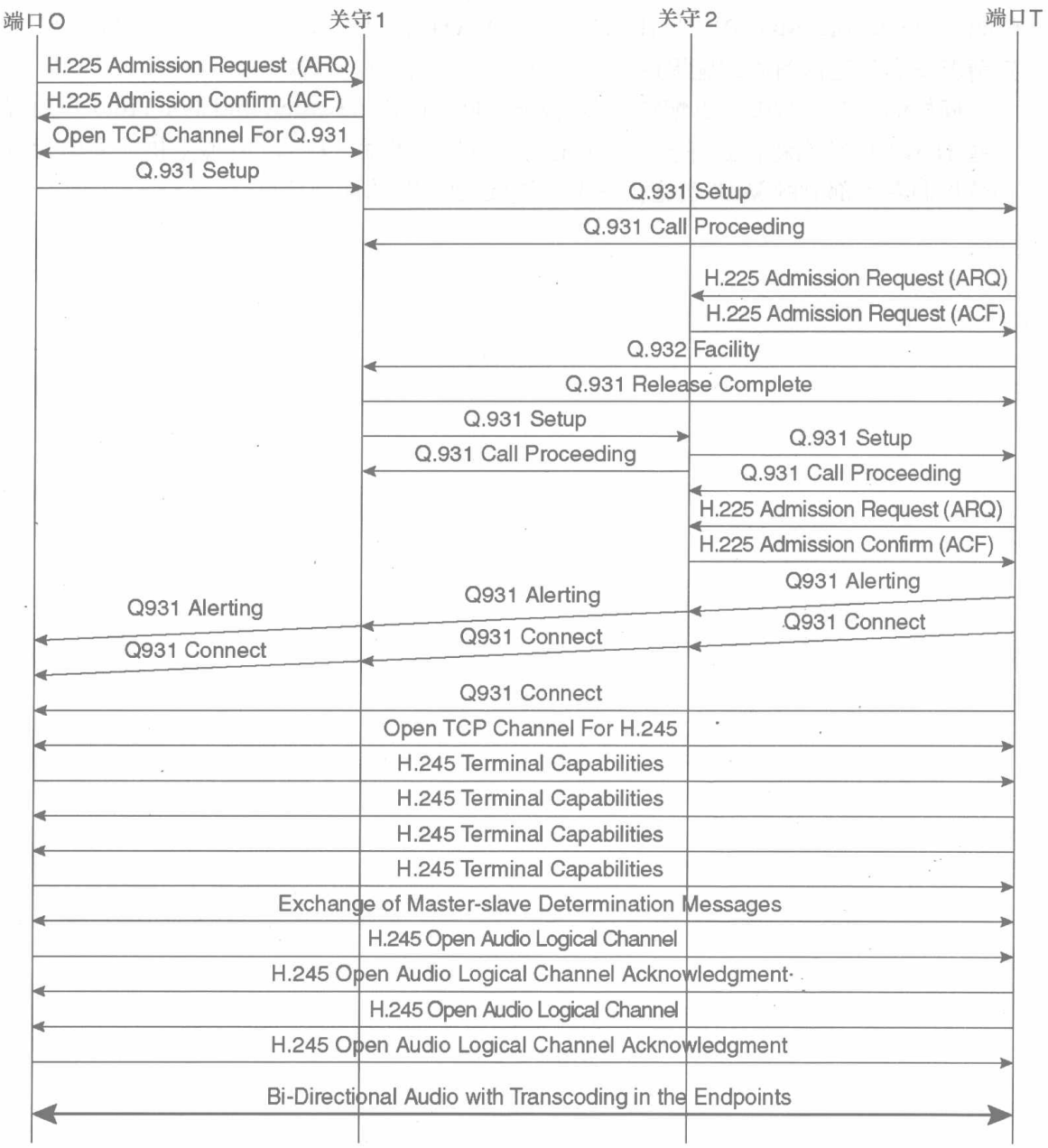


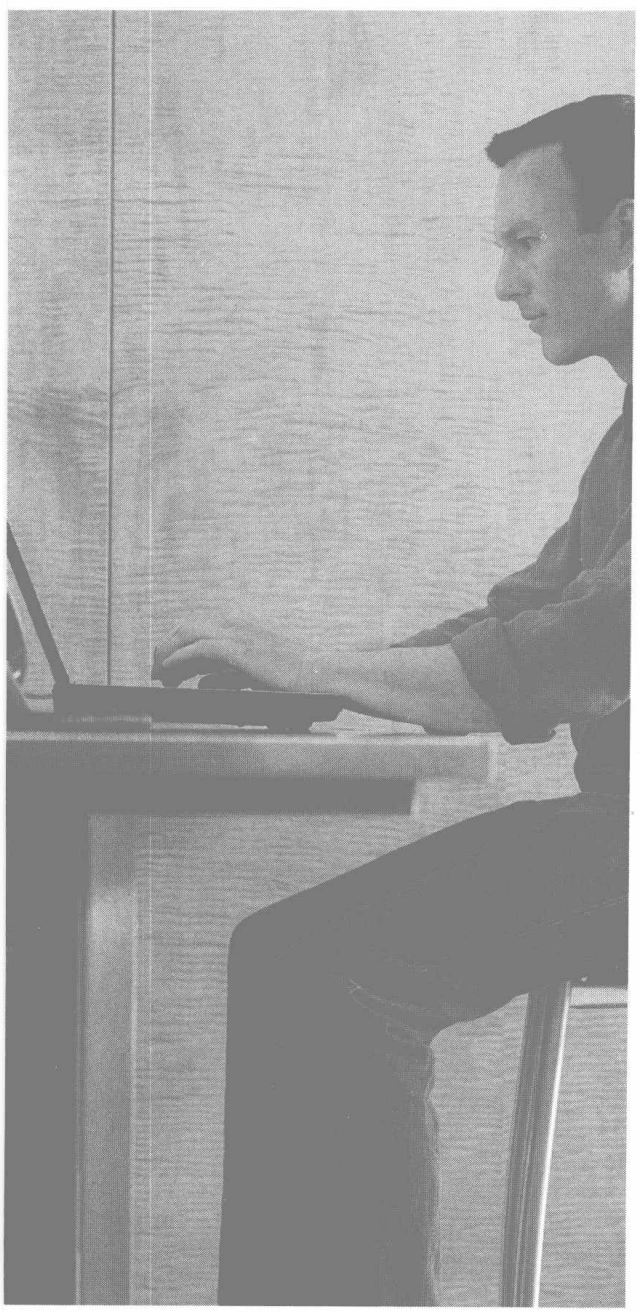
图 11-13 关守路由呼叫信令——两个关守

11.4 总结

H.323 是一个由集中的智能关守、MCU 和较少智能的端点组成的混合系统。虽然 H.323 标准在最近的版本中更趋于完整，但问题也在产生，如呼叫建立时间长、一个全功能会议协议的高额开销、每个关守需要太多功能和关守呼叫路由实施的拓展顾虑等。

当 PSTN 互联需要高密度网关时，其他选择，如媒体网关控制协议（Media Gateway Control Protocol，MGCP）和 H.245（MEGACO）也可以考虑。这些呼叫控制系统为在特定情况下满足运营商级实施提供了一个更有效和可拓展的解决方案。

同样的，对于智能端点配置，会话发起协议（SIP，Session Initiation Protocol）解决了一些 H.323 中的问题，是许多网络上的可选方案。然而，H.323 在服务供应商语音市场，仍然控制着大部分的 VoIP 实施。第 12 章描述了 SIP 的详细信息。



本章讨论网络架构框架和设计模型，包含以下主题：

- 12.1 SIP 概览
- 12.2 SIP 消息构造基础
- 12.3 基本 SIP 操作
- 12.4 SIP 注册和路由选择过程
- 12.5 SIP 扩展
- 12.6 总结

第12章

SIP

会话发起协议（Session Initiation Protocol，SIP）是一个控制发起、修改和终结交互式多媒体会话的信令协议。多媒体会话是多样化的，包括双方或多方音频、视频呼叫、聊天会话或游戏会话。已经为即时消息、列席和事件通知定义了 SIP 的扩展。SIP 是一个基于文本的协议，在这一点上与 HTTP 和简单邮件传输协议（SMTP）相似。

SIP 是一个对等方到对等方的协议，这就意味着如呼叫路由选择和会话管理功能等网络功能被分布在 SIP 网络的所有节点（包括端点和网络服务器）上。这与传统的电话模型是不同的。在传统的电话模型中，电话或最终用户的呼叫建立和服务完全依赖于网络中的中心交换机。

SIP 在 RFC 2542（1999 年 3 月）中由 Internet 工程任务组（Internet Engineering Task Force，IETF）的多方多媒体会话控制（Multiparty Multimedia Session Control，MMUSIC）工作组定义。2002 年 6 月，IETF 发布了一个新的 SIP RFC（RFC 3261）。IP 电话仍然还在部署过程中，仍然需要附加信令功能。SIP 的可拓展性允许在发展中不断增加功能。本章也会描述一些主要的扩展。

本节覆盖以下主题：

- SIP 概览——阐述功能、网络元素和与其他协议的交互；
- SIP 消息构造基础——阐述 SIP 寻址，消息和标题头、处理事务和对话；
- SIP 的基础操作——提供一个代理、重订向服务器和 B2BUA 服务器的例子；
- SIP 注册和路由选择过程——阐述定位 SIP 服务器，注册和消息路由选择；
- SIP 扩展——阐述主叫和被叫偏好，订阅通知、REFER、列席和 IM。

12.1 SIP 概览

本节描述 SIP 网络的主要组件和它们的功能，以及它们之间的交互。

12.1.1 SIP 提供的功能

SIP 提供以下功能以支持多媒体会话。

- 用户位置——SIP 提供探索最终用户位置，用以建立一个会话或分发 SIP 请求的功能。SIP 支持用户的移动性。
- 用户功能（User capabilities）——SIP 可以确定参加会话的设备的媒体功能。
- 用户有效（User availability）——SIP 可以确定最终用户是否乐意参与会话。

- 会话建立（Session setup）——SIP 允许为参与会话的各方建立会话参数。
- 会话处理（Session handling）——SIP 允许修改、转移和中止一个活动会话。

12.1.2 SIP 网络元素

SIP 网络通常有以下设备组成。

- 用户代理（User agent）—— 用户代理（UA）是在 SIP 网络中发起或响应 SIP 事务处理的逻辑功能。UA 在 SIP 事务处理中，可以充当客户端或服务器。UA 可能直接与人交互，也可能不这样做。UA 是有状态的——也就是说，它维护会话或对话状态。
- 用户代理客户端（User agent client）——用户代理客户端（UAC）是发起 SIP 请求和接受 SIP 响应的逻辑功能。UAC 的例子有，一个 SIP 电话代表用户发起呼叫，或者一个 SIP 代理代表 UAC 转发请求。
- 用户代理服务器（User agent server）——用户代理服务器（UAC）是接受 SIP 请求和返回 SIP 响应的逻辑功能。一个 SIP 电话接受一个 INVITE 请求就是一个例子。
- 代理（Proxy）——代理是在 SIP 网络中的一个中间实体。代理负责代表 UAC 转发 SIP 请求到目的 UAS 或另一个代理。在 SIP 网络中，代理主要提供路由选择功能。代理也可能执行网络中的策略，如在提供用户服务之前认证用户。代理可能是无状态的，处理事务状态的或呼叫状态的。通常，代理是处理事务状态的——也就是说，他们为一个处理事务（大概 32 秒）维护状态。
- 重定向服务器（Redirect server）——重定向服务器是一个 UAS，它为它接收到的请求产生 300 类 SIP 响应，指导 UAC 与另一个统一资源标识符（Uniform Resource Identifiers，URI）集联系。
- 注册服务器（Registrar server）——注册服务器是一个 UAS，它接受 SIP REGISTER 请求，将请求消息中的信息更新到本地数据库。
- 背靠背用户代理（Back-to-back user agent）—— 背靠背用户代理（B2BUA）是一个中间实体，它像一个 UAS 那样处理到来的 SIP 请求。为应答到来的 SIP 请求，B2BUA 充当 UAC，重新产生一个 SIP 请求并将它发送到网络上。B2BUA 必须维护对话的状态，并且参与对话中的所有事务。

12.1.3 与其他 IETF 协议交互

SIP 本身不具备所有建立交互式多媒体会话所需的功能。它只是用于建设多媒体架构的标准协议框架中的一部分。

SIP 代理或应用需要以下其他协议提供的功能。

- 描述会话特性——这些特性包括，一个会话是音频还是视频会话、使用的是什么解码器、媒体源是什么和目的地址是什么。
- 处理媒体——这些协议为一个会话传输和控制音频/视频包。

- 支持功能——这些需要包括为认证，授权和记账的 AAA；为预留网络资源的资源预留协议（Resource Reservation Protocol，RSVP）；为网关选择和平衡负载的 IP 电话路由选择（Telephony Routing over IP，TRIP）；为防火墙和 NAT 穿越的 UDP 对 NAT 的简单穿越方式（Simple Traversal of UDP Through NAT，STUN）/通过中继方式穿越 NAT（Traversal Using Relay NAT，TURN）/交互式连接建立（Interactive Connectivity Establishment，ICE）协议；为主机名到 IP 地址的解析的域名系统（Domain Name System，DNS）；和为避免偷听、篡改或消息伪造的传输层安全协议（Transport Layer Security，TLS）。

使用 SIP 建立的会话通常使用以下 IETF 协议：

- DNS——SIP 会话建立可能要求使用 DNS 解析主机或域名到刻录有的 IP 地址。DNS 还可以被用来在一个通过主机名识别的集群中的多个服务器上均衡负载。
- 会话描述协议（Session Description Protocol，SDP）——SIP 消息中使用 SDP 描述多媒体会话参数。这些信息包括会话类型（音频、视频或两者都有）和如编码器，用以建立媒体流的端口号等参数。RFC 2327 定义 SDP。
- 实时传输协议（Real-time Transport Protocol，RTP）——RTP，最初定义在 RFC 1889 种，传输实时数据（如音频或视频包）到参与会话的端点。实时传输控制协议（Real-time Transport Control Protocol，RTCP），定义在 RFC 1890，为发送者提供 QoS 反馈。RFC 3550 废弃了 RFC 1889。
- RSVP——SIP 可以使用 RSVP 在建立媒体会话前来预留如带宽的网络资源。这就保证了网络资源在通知被叫方有呼叫前就已经就绪。
- TLS——SIP 建议使用 TLS，在 RFC 224 中定义，提供网络上 SIP 信令信息的隐私性和完整性。TLS 允许客户和服务器应用在网络上发送信令信息前互相认证，协商加密算法，建立加密秘钥。
- STUN——SIP UAC 可以使用 STUN 协议发现他们与公网之间是否有网络地址转换（NAT）及其类型。STUN 也允许客户发现分配给 NAT 的公网 IP 地址。除了对称 NAT 外，这个过程都是有效的。当所有请求都来自同一个内部 IP 地址和端口，到特定的被映射到同一外部源地址和端口的目的IP地址和端口时，出现对称NAT。

上述绝不是全部的 SIP 使用的协议列表。根据信令和应用的需求，SIP 可能会使用其他协议。

SIP 并不是必须使用前面所列的协议。将来，当有新的或增强的协议执行类似的功能时，SIP 可以不修改或少量修改后就使用它们。大多数与这些协议相关的信息被承载载在 SIP 消息体内。SIP 将消息体作为不透明的容器传输给接收者。SIP 协议层不解释消息体。

SIP 信令则独立于任何类型要建立的会话。所以，从 SIP 信令的角度来看，无论建立的是音频会话，音频—视频会话还是其他类型的会话，所用的消息集是一样的。

12.1.4 SIP 网络中的消息流程

图 12-1 显示了一个基本的 SIP 网络，该网络由 SIP 代理和连接到 PSTN 的用户代理组成。SIP UA，代理和 SIP PSTN 网关位于 IP 网络内。SIP-PSTN 网关有到 PSTN 交换机的 SS7/PRI 中继。

在图 12-1 中，实线代表 SIP 请求，点划线代表 SIP 响应。

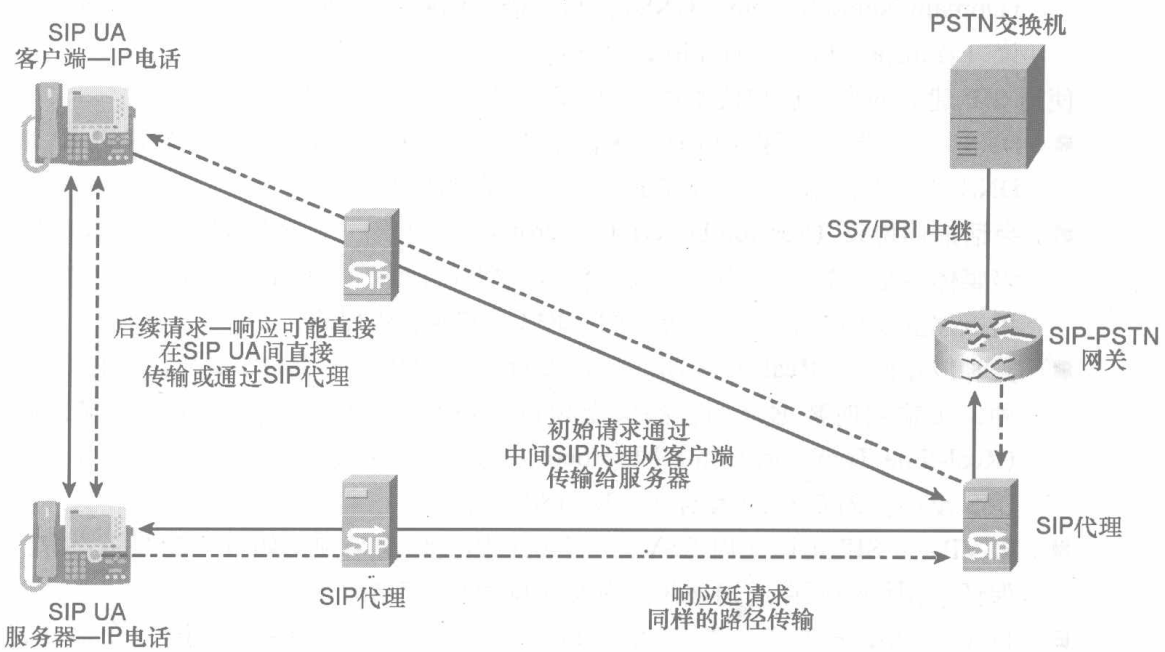


图 12-1 SIP 网络中的请求和响应消息路径

12.2 SIP 消息构造基础

本节描述 SIP 消息结构，寻址方案和主要的标题头字段。大多数 SIP 消息和标题头字段的语法与 HTTP/1.1 一样。进一步的描述请参照 RFC 3261。

> 注释：在 http://www.ietf.org/rfc/rfcxxx.txt 上您可以找到所有的 RFC 大纲，其中 xxxx 代表 RFC 号。如果不知道 RFC 号的话，可以在 http://www.rfc-editor.org/cgi-bin/rfcsearch.pl 通过主题搜索。

12.2.1 SIP 寻址

SIP 地址在网络域中识别一个用户或资源。SIP 地址通常被称为 *SIP URI*。SIP URI 通常是有如下格式的 E-mail 类型的地址：

sip:user@domain:port

sip:user@host:port

在一个域或主机内，用户字段使用名字唯一标识用户，例如 john.doe，或使用电话号

码，如 4081234567。端口（port）是一个可选字段。如果没有端口被定义，默认的 SIP URI 端口是 5060。如果端口被明确定义，您就必须使用明确定义的端口。SIP URI 的例子如下：

sip:john.doe@company.com

sip:4081234567@proxy1.company.com

用户或资源的公共 SIP 地址被称为地址记录（Address-of-Record，AOR）。AOR 是一个可以全球路由的并指向一个域的 SIP URI，该域的服务可以将 AOR 影射到另一个用户所在的 SIP URI。

RFC 3261 定义了一个被称为 SIPS URI 的安全 SIP URI 格式。SIPS URI 的格式如下：

sips:user@domain:port

或

sips:user@host:port

SIPS URI 的默认端口是 5061。

12.2.2 SIP 消息

SIP 消息可以大致被分为 SIP 请求和响应，在下面各节中进一步讨论。

1. SIP 请求

SIP 请求是由客户端发给服务器激活一个 SIP 操作的消息。RFC 3261 定义了六种 SIP 请求或方式，它们使 UA 或代理定位用户，发起、修改和拆除会话。

- INVITE——INVITE 消息表明接收用户或服务被邀请加入一个会话。您也可以使用这种方式来修改先前建立会话的特性。INVITE 消息体可能包含要建立或修改媒体会话的描述，使用 SDP 编码。INVITE 的成功响应（200 OK 响应）表明了被叫方愿意参与会话。
- ACK——ACK 请求确认 UAC 已经接收到了 INVITE 请求的最终响应。ACK 只与 INVITE 请求一起使用。ACK 用于结束一个 200 OK 响应。前一个代理或 UAC 为其他最终响应发送 ACK。如果 INVITE 请求中不含有会话描述信息，ACK 可以包含一个最终会话描述的消息体。
- OPTIONS——UA 使用 OPTIONS 请求向 UAS 查询它的功能。如果 UAS 可以向用户递送会话，则响应 UAS 的功能集。
- BYE——UA 使用 BYE 请求终结一个先前建立的会话。
- CANCEL——CANCEL 请求使 UAC 和网络服务器取消一个正在进行的请求，如 INVITE。这不会影响 UAC 已经发送最终相应的请求。
- REGISTER——客户端使用 REGISTER 请求注册它目前的位置信息。

2. SIP 响应

服务器向客户端发送 SIP 响应，指明客户端先前发给服务器的 SIP 请求的状态。

UAS 或代理产生回应 UAC 发起的 SIP 请求的 SIP 响应。SIP 响应被从 100 到 699 编码，分组为 1xx、2xx～6xx 组。SIP 响应被分为*临时的 (provisional)* 和*最终的 (final)* 两类。

临时响应表明了服务器处理请求的过程，而不是最后处理结果。1xx 组的 SIP 响应表明临时状态。最终响应表明 SIP 请求的终结和最终状态。所有的 2xx、3xx、4xx、5xx 和 6xx 组的响应都是最终响应，分别为：

- 2xx 响应表明 SIP 请求的成功处理；
- 3xx 响应表明 SIP 请求需要转向到另一个 UAS 处理；
- 4xx、5xx 或 6xx 响应表明 SIP 请求处理失败。

表 12-1 列出了 RFC 3261 中的各种 SIP 响应。

表 12-1 SIP 响应

响应类型	状态编码	描述
信息	100	尝试中
	180	振铃中
	181	呼叫正在转移中
	182	排队
	183	会话进行
成功	200	OK
重定向	300	多种选择
	301	永久移动
	302	临时移动
	305	使用代理
	380	备用服务
客户端错误	400	错误请求
	401	未被授权
	402	需要付费
	403	禁止
	404	没有找到
	405	不允许使用方式
	406	不接受
	407	需要代理认证
	408	请求超时
	410	已离开

续表

响应类型	状态编码	描述
	413	请求实体过大
	414	请求 URL 过大
	415	不支持媒体类型
	416	不支持 URI 方案
	420	错误扩展
	421	需要扩展
	423	间隔过短
	480	临时不可用
	481	呼叫分支或事务不存在
	482	发现循环
	483	跳数过多
	484	地址不全
	485	模糊
	486	忙
	487	请求已被终结
	488	不接受
	491	未觉请求
	493	难辨认
服务器错误	500	内部服务器错误
	501	没有实施
	502	错误网关
	503	服务不可用
	504	服务器超时
	505	不支持的 SIP 版本
	513	消息过长
全局错误	600	到处忙
	603	拒绝
	604	不存在
	606	不接受

3. SIP 消息结构

SIP 消息由如下组成：

- 一个开始行（start-line）；
- 一个或多个标题头字段；
- 一个空行表明标题头字段的结束；
- 一个可选的消息体。

必须使用回车换行符（Carriage Return Line Feed，CRLF）终结开始行、每个消息标题头行和空行。

SIP 请求的开始行是一个请求行（Request-Line）；SIP 响应的开始行是一个状态行（Status-line）。

请求行定义 SIP 方式、请求 URI（Request URI）和 SIP 对话。状态行描述 SIP 版本，SIP 响应编码和一个可选的原因短语（reason phrase）。原因短语是 3 位 SIP 响应编码的文字描述。

表 12-2 显示了 SIP 请求消息的各种组件。

表 12-2 SIP 请求组件

INVITE sip:bob@proxy.company.com SIP/2.0	请求行
Via: SIP/2.0/UDP ph1.company.com:5060;branch=z9hG4bK83749.1 From: Alice <sip:alice@company.com>;tag=1234567 To: Bob <sip:bob@proxy.company.com> Call-ID: 12345601@ph1.company.com CSeq: 1 INVITE Contact: <sip:alice@ph1.company.com> Content-Type: application/sdp Content-Length: ...	SIP 消息标题头
	SIP 标题头字段与 SDP 体之间的空行
v=0 o=alice 2890844526 28908445456 IN IP4 172.18.193.102 s=Session SDP c=IN IP4 172.18.193.102 t=0 0 m=audio 49170 RTP/AVP 0 a=rtpmap:0 PCMU/8000	SIP 消息中的 SDP 体

*表 12-2 中的信息摘自 RFC 3261

表 12-3 显示了 SIP 响应消息的各种组件。

表 12-3 SIP 响应组件

SIP/2.0 200 OK	（响应）状态行
Via: SIP/2.0/UDP ph1.company.com:5060;branch=z9hG4bK83749.1 From: Alice <sip:alice@company.com>;tag=1234567 To: Bob <sip:bob@proxy.company.com>;tag=9345678 Call-ID: 12345601@ph1.company.com CSeq: 1 INVITE Content-Length: ...	SIP 消息标题头
	SIP 标题头字段与 SDP 体之间的空行
v=0 o=bob 3800844316 3760844696 IN IP4 172.18.193.109 s=Session SDP c=IN IP4 172.18.193.109 t=0 0 m=audio 48140 RTP/AVP 0 a=rtpmap:0 PCMU/8000	SIP 200 OK 响应消息中的 SDP 体

*表 12-3 中的信息摘自 RFC 3261

4. SIP 标题头

SIP 消息由为 SIP 网络实体传送信令和路由信息的标题头字段（在 RFC3261 中定义）组成。SIP 遵从 HTTP 标题头（RFC 2616）定义的同样格式。每个标题头字段由字段名，紧跟着冒号（:）和字段值组成。

表 12-4 描述了主要 SIP 标题头的功能。

表 12-4 主要 SIP 标题头

SIP 标题头	描述
From	此标题头定义了 SIP 请求发起者。From 标题头通常是发送者的 AOR。它包含了 SIP 或 SIPS URI 和一个可选的显示名字
To	此标题头定义了 SIP 请求的接收者。To 标题头通常是接收者的 AOR。因为重定向和转移，SIP 请求不一定分发给“希望的”接收者。To 标题头包含了 SIP 或 SIPS URI 和一个可选的显示名字
Call-ID	此标题头定义了一系列的 SIP 消息。对于所有的由对话中的 UA 发送的所有 SIP 请求和响应，Call-ID 必须唯一
Cseq	此标题头由一个整数值和一个方式名称组成，在一个对话中标识和序列 SIP 请求。Cseq 标题头也区分重传消息和新消息

续表

SIP 标题头	描述
Via	Via 标题头定义请求路径和响应要发送的地址
Contact	此标题头定义 US 希望接收新 SIP 请求的 SIP 或 SIPS URI
Allow	Allow 标题头字段列出了产生 SIP 消息的 UA 所支持的功能集合
Supported	这个标题头列出了所有 UA 支持的 SIP 扩展。SIP 扩展是除了 RFC 3261 外的其他 SIP RFC。SIP 扩张表示为在 RFC 3262 中定义的如 100rel 的标记
Require	此标题头与 Supported 标题头有相同的语义，包含的是远端 UA 必须支持的 SIP 扩展
Content-Type	此标题头定义了 SIP 请求或响应的消息体类型。如果 SIP 消息有一个消息体，则必须有此标题头
Content-Length	此标题头定义了 SIP 请求或响应的消息体的大小（十进制）。如果 SIP 消息被承载在基于如 TCP 协议时，此标题头是必须的

12.2.3 SIP 事务和对话

在两个用户代理之间的 SIP 信令会话可能有一个或多个 SIP 事务。SIP 事务发生在 UAC 和 UAS 之间，可能会关系到一个或多个 SIP 服务器如代理服务器或重定向服务器。一个 SIP 事务包含从 UAC 引发的 SIP 请求到 UAS 接收到的最终响应在内的所有消息。SIP 事务通过呼叫 ID（Call ID），经由分支（via-branch）、本地标记（local tag）、远程标记（remote tag）和 CSeq 值（CSeq value）识别。图 12-2 显示了在 UAC 和注册服务器之间的 SIP REGISTER 事务。SIP 事务由一个 SIP 请求消息和其后的一个或多个响应消息组成。在这个例子中，REGISTER 消息是由 UAC 发给注册服务器的一个 SIP 请求。100 Trying 和 200 OK 是 SIP 响应。用户代理服务器发送 SIP 响应给 UAC 指明 SIP 请求的状态。

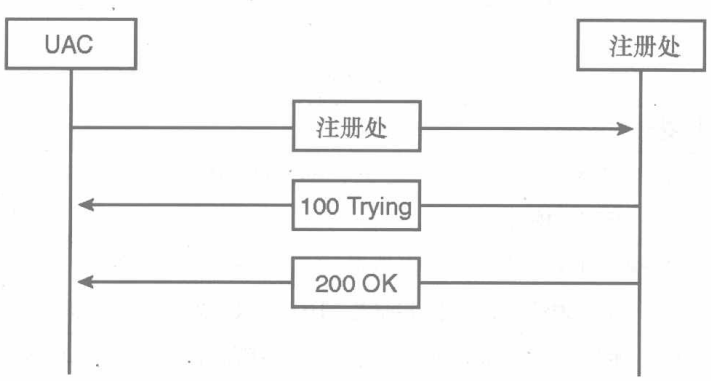


图 12-2 SIP REGISTER 事务

SIP 事务的结果可能是建立、修改或终结一个媒体会话。会话的建立也在对等方间建立了一个 SIP 信令关系，被称为对话（dialog）。对话就是在会话期间，一个或多个组成会话的 UA 之间的对等 SIP 关系。对话是一个由呼叫 ID（Call ID）、本地标记（local tag）和远程标记（remote tag）表示的状态。不是所有的 SIP 事务都会影响对话的状态。多个 SIP 事务可能发生在一个 SIP 对话中。对话中的每个 SIP 事务在 CSeq 标题头中有一个顺序渐增的整数值。

成功的 INVITE-200 OK 事务的结果是建立一个 SIP 对话和在参与者之间的一个音频或视频会话。在媒体会话被建立后，您可以在已存在的对话中使用同一呼叫 ID（Call-ID）和标记来交换 INVITE 消息以修改媒体会话参数。其后，在同一对话上下文中，您可以使用 BYE 事务拆除会话或使用 REFER 事务转移它到另一个设备。

一个成功的 SUBSCRIBE-200 OK 事务建立一个对话。SUBSCRIBE（定阅）请求将在 12.5 节讨论。

对话和事务的状态在 SIP UA 或端点维护。SIP 服务器，如代理和重定向，通常在事务持续期间内维持状态——也就是说，他们只维持事务状态。在 RFC 3261 中，事务状态应该被保持最少 32 秒。SIP 服务器，如代理和重定向服务器维持事务状态，但不维持对话状态，这就允许他们可以为许多 SIP 端点服务。因为网络服务器只维持事务状态，在集群中的一个代理失效时，会影响到正在进行的事务，但不会影响到已建立的对话。

12.2.4 SIP 信令的传输层协议

SIP 事务使用如 TCP 或流控制传输协议（Stream Control Transmission Protocol，SCTP）等面向连接的传输层协议，或如 UDP 的无连接的协议。对于无连接的协议，SIP 定义 SIP 应用重传输计时器来重试 SIP 请求以保证端对端的可靠性。

SIP 定义了一个 SIPS URI，这表明了网络上端到端 SIP 信令信息的安全需求。SIP RFC 3261 定义了使用 TLS 或 IPsec 来加密信令信息。

12.3 基本 SIP 操作

SIP 服务器使用两种方法来处理到达的请求。这个基本实施是基于邀请一个呼叫的参与者的。在本节中，将描述如下 3 种基本 SIP 服务器操作方式：

- 代理服务器；
- 重定向服务器；
- B2BUA 服务器。

12.3.1 代理服务器举例

图 12-3 列出了使用代理服务器的 INVITE 的通信交换。

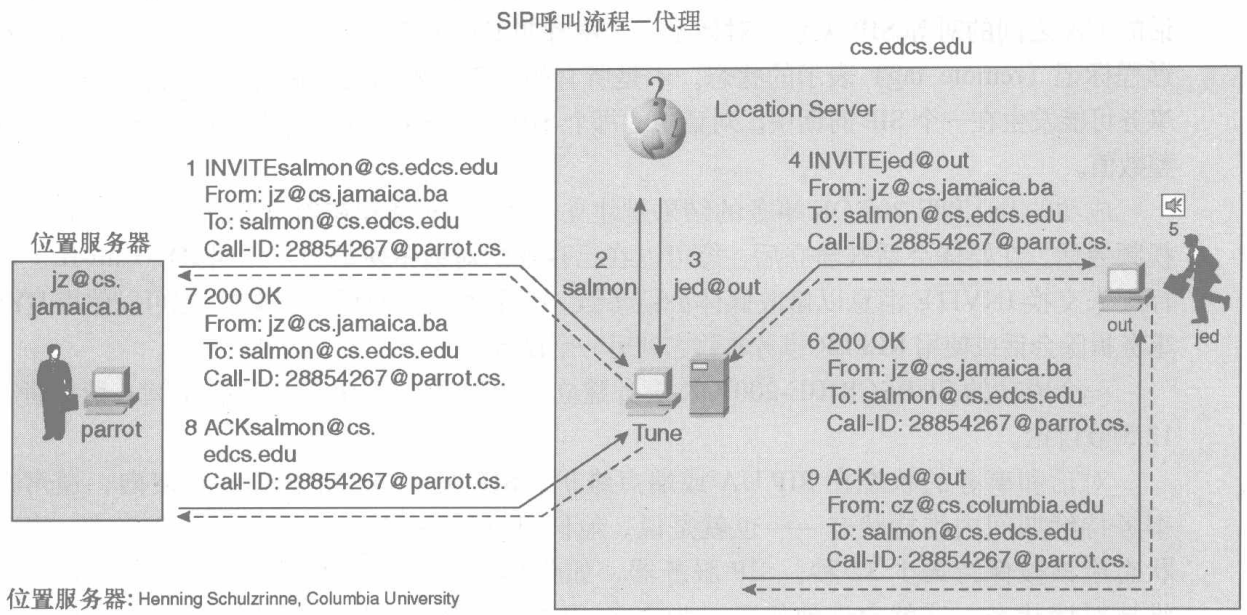


图 12-3 代理模式操作

在代理方式下成功建立双向呼叫的操作步骤如下。

1．代理服务器接受来自客户端的 INVITE 请求。

2．代理服务器联系位置服务器，请求被叫方 UA 的地址。

3．位置服务器确认被叫方的位置并将地址提供给目的服务器。

4．INVITE 请求被转发到返回的目的地址。代理可能会在 INVITE 消息上添加记录路由（Record-Route）标题头以保证所有的该对话的后续消息都经过代理路由。计费或其他需要对话消息的应用需要这样做。

5．被叫方 UA 提示用户。用户应答呼叫。

6．UAS 返回一个 200 OK 指示给请求的代理服务器。

7．200 OK 响应被从代理服务器转发到主叫方 UA。

8．主叫方 UA 发送 ACK 请求，确认收到 200 OK,该请求被发送给代理（当代理在 INVITE 消息中加入记录路由标题头时）或直接发送给被叫方 UA。

9．代理转发 ACK 给被叫方 UA。

12.3.2 重定向服务器举例

图 12-4 列出了使用重订向服务器的 INVITE 的通信交换。

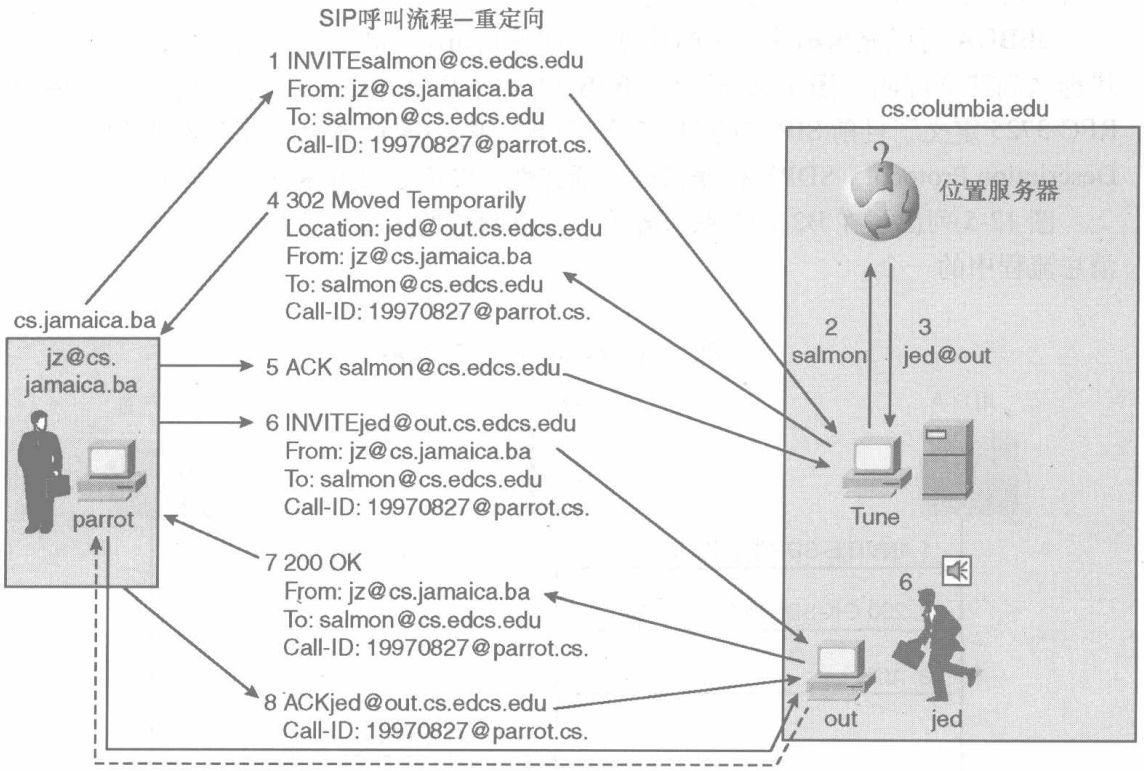


图 12-4 重定向模式操作

在重定向模式中，建立双向会话的操作步骤如下：

1．重定向服务器接受来自主叫方 UA 的 INVITE 请求。

2．重定向服务器联系位置服务器，请求被叫方 UA 的地址。

3．位置服务器返回被叫方 UA 的地址。

4．在用户被定位后，重定向服务器使用 3xx 消息连同更新后的联系信息直接将地址返给主叫方：指向新目的地的标题头。与代理服务器不同，重定向服务器不转发 INVITE。

5．UAC 发送一个 ACK 给重定向服务器，确认收到 3xx 响应。

6．UAC 发送一个 INVITE 请求直接给由重定向服务器返回的联系地址。

7．被叫方 UA 提示用户，用户应答呼叫。被叫方 UA 给 UAC 提供一个成功指示（200 OK）。

8．UAC 发送一个 ACK 给 UAS，确认收到 200 OK 响应。

12.3.3 B2BUA 服务器举例

RFC 3261 没有定义 B2BUA 功能。将其描述为 UAC 和 UAS 的串联。然而，在 SIP 网络中 B2BUA 在集中呼叫控制和功能管理方面有着重要的作用。与代理不同，B2BUA 可以发起新的 SIP 呼叫，以及修改和终结现有的呼叫。经由 B2BUA 服务器的 SIP 呼叫建立两个不同的

对话，以允许修改一个 SIP 会话时不会影响另一个会话。

BEBUA 可以充当第 3 方呼叫控制器（third-party call controller，3PCC），在两个用户代理之间建立呼叫。图 12-5 显示了 B2BUA 在用户 A 和 B 之间建立呼叫时充当 3PCC。RFC 3725 定义了目前 SIP 中的 3PCC 的最佳实践。3PCC 通过修改会话描述协议（Session Description Protocol，SDP）体来修改会话特性。SDP 定义在 RFC 2327 中。

图 12-5 列出了在 B2BUA 服务器模式建立呼叫的步骤。这是 RFC 3725 中描述的四个消息流程中的一个。

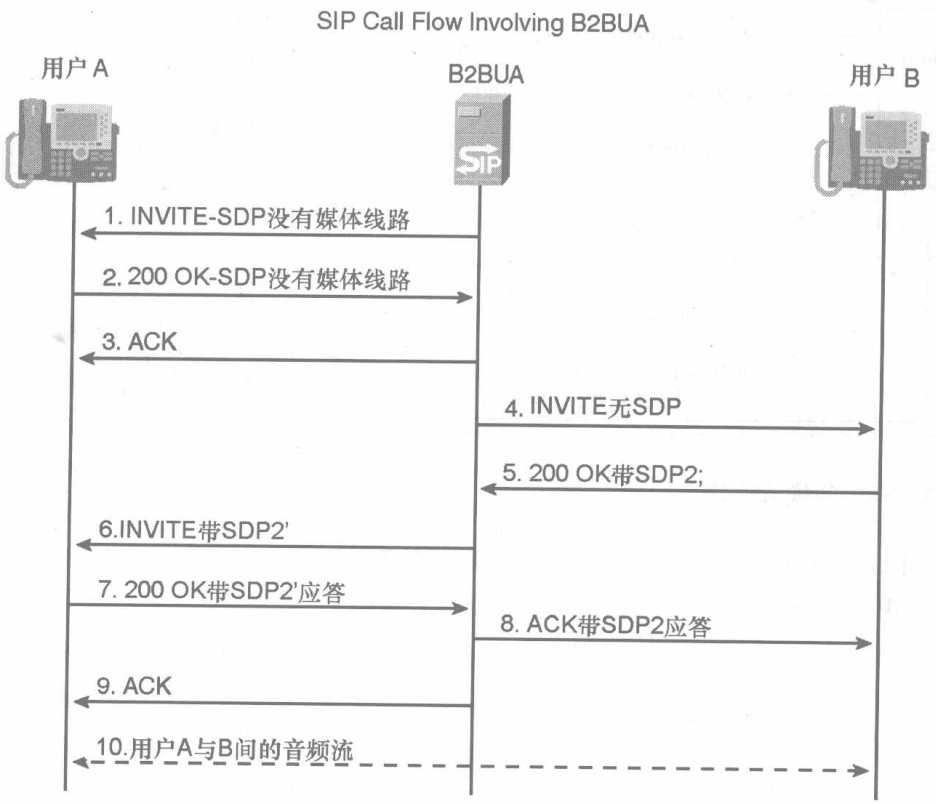


图 12-5 B2BUA 服务器模式操作

1．B2BUA 发送一个 INVITE 给用户 A。这个 INVITE 包含一个没有媒体行的 SDP 体。这意味着媒体特性将在其后的另一个 INVITE 中定义。

2．用户 A 被提示。一个 180 Ringing（振铃）消息从被用户 A 发给 B2BUA，但在这个消息在流程中没有显示。当呼叫被应答后，一个 200 OK 被发送给 B2BUA。这个 200 OK 有一个没有媒体行的 SDP 体。

3．B2BUA 发送一个 ACK 给用户 A。

4．B2BUA 发送一个 INVITE 给用户 B。这个 INVITE 消息不含有一个 SDP 体。

5．用户 B 被提示并应答呼叫。200 OK 和 SDP 被送回 B2BUA。

6．B2BUA 使用在 200 OK 中接收到的 SDP 建立一个含有 SDP 体的 INVITE，并将其发送给用户 A。INVITE 消息中的 SDP 体是一个从用户 B 200 OK 中接收到的 SDP 体的修改版本。这就是它在消息流程中被标为 SDP2'的原因。

7．用户 A 使用 200 OK 和应答 SDP 响应 B2BUA。

8．B2BUA 将 ACK 与应答 SAP 一起发给用户 B。

9．B2BUA 发送一个 ACK 给用户 A 以确认 200 OK。

10．在用户 A 和 B 之间建立了一个呼叫。音频包在用户 A 和用户 B 之间使用 RTP 发送。这里有两个不同的 SIP 对话——一个在用户 A 和 B2BUA 之间，另一个在用户 B 和 B2BUA 之间。

B2BUA 功能还可以帮助 SIP 设备和其他协议的互联，如 H.323 和媒体网关控制协议（Media Gateway Control Protocol，MGCP）。B2BUA 允许传输层互联，如 TCP 和 UDP，IPv4/IPv6 地址映射，隐藏在 SIP 标题头中的拓扑和地址，如 Via、Contact 和 Record-Route。

使用 B2BUA 功能的产品有：基于 SIP 的 IP-PBX、软交换机、防火墙/NAT 穿越应用、呼叫中心应用和会议服务器。

12.4 SIP 注册和路由选择过程

本节描述 RFC 3261 和 SIP 扩展 RFC 中定义的 SIP 功能。注册和路由选择方面覆盖如下内容：

- UA 在网络中探索 SIP 服务器；
- SIP 注册和用户移动；
- SIP 消息路由；
- 在 SIP 对话中路由后续请求；
- 代理服务器上的信令分路；
- 增强的代理路由选择。

12.4.1 用户代理在网络中探索 SIP 服务器

UA 需要注册服务器或代理服务器的 IP 地址以注册和提供 SIP 服务。而 UAC 可能没有 SIP 代理服务器的 IP 地址，需要在它所在的域中发现一个 SIP 代理服务器的地址。

UA 在获得 IP 地址的 DHCP 过程中得到一个 DNS 服务器的地址。UA 发起一个 DNS 过程，发现它所在网络中能提供 SIP 路由选择功能的服务器。这就允许 UA 不需要明确配置，就可以到达对方用户代理或 SIP 网络服务。

UAC 可以使用 DNS 过程（在 RFC 3263 中定义）如名称权威指针（Naming Authority Pointer，NAPTR）来确定域中提供哪些服务。NAPTR 记录返回一系列终端 DNS 记录，如服务记录（Service Record，SRV）（在 RFC 2782 中定义），来指明域中支持的服务和协议。

UAC 过滤指向支持 SIP 的服务器记录。

DNS SRV 记录帮助客户端通过查询域中特定服务和传输协议来发现支持一个应用协议的服务器，如 SIP。为确定在 company.com 域中的支持 UDP 协议的 SIP 服务器的地址，您需要在 DNS 服务器中查询字符串**_sip_udp.company.com**。DNS SRV 查询产生 DNS A 记录，然后解析该记录，得到 SIP 服务器的 IP 地址。UA 然后发送 INVITE 请求到解析到的 IP 地址。

12.4.2 SIP 注册和用户移动

SIP 端点注册在一个 SIP 注册服务器上。通常，注册和代理功能都实施在同一台服务器上。在注册过程中的 SIP 端点通常是如 SIP IP 电话的最终用户设备，或者是提供特殊功能如语音邮件和列席状态的服务器。

SIP 用户和服务通常有一个被广泛知道的或公共的 SIP 或 SIPS URI，这个地址被称为 AOR。AOR 应该是全球可到达的地址。SIP AOR 与电话号码相似，是另一种联系用户的方式，可能会出现在名片或个人主页上。

UA 被激活后，在代理服务器上建立一个用户 AOR 和他目前 IP 地址的捆绑，这个捆绑是一个有时间限制的。这个过程称为注册。用户的 AOR 通常注册在 UA 上，如 IP 电话上。电话的 IP 地址因为通常通过 DHCP 获得，所以是可变的。

UA 发送一个 SIP REGISTER（SIP 注册）请求到域内的注册服务器，在 Contact（联系）标题头提供它目前的 IP 地址。UA 在 REGISTER（注册）消息的 To 标题头内指明它的 AOR。

注册服务器更新位置服务数据库，将用户的 AOR 与它目前的地址或位置捆绑。用户的位置也被称为联系地址（contact address），在 REGISTER（注册）消息的 Contact（联系）标题头中被传递。代理和注册服务器使用的位置数据库就可以将 AOR 映射到 0 个或多个联系地址。

Contact（联系）标题头有一个期满参数，指明这个捆绑的有效期。在如图 12-6 所示的呼叫流程中，期满参数被设为 3 600 秒或 1 小时。在这段时间内，UA 被期望刷新注册信息以保持这个捆绑在注册服务器上有效。因此，UA 定期发动注册消息以刷新信息。如果没有及时刷新，注册服务器将删除这个捆绑。

代理服务器使用更新后的位置数据库路由 SIP 请求。

这个向注册服务器/位置服务注册联系地址的机制使 SIP 支持用户的移动。例如，一个在他的笔记本上有 SIP 软电话的雇员可能在公司内移到了另一个位置上。当 SIP 软电话或 UA 启动时，他发送一个 REGISTER（注册）消息给它的 SIP 注册服务器，使用目前访问的地址更新位置服务。代理服务器则可以根据他在位置服务数据库中的联系地址，无缝地将该用户的呼叫转到他现在访问的位置。对于用户通过登录公司的 VPN 也是一样的。图 12-6 演示了 SIP 注册过程和相关标题头的使用。

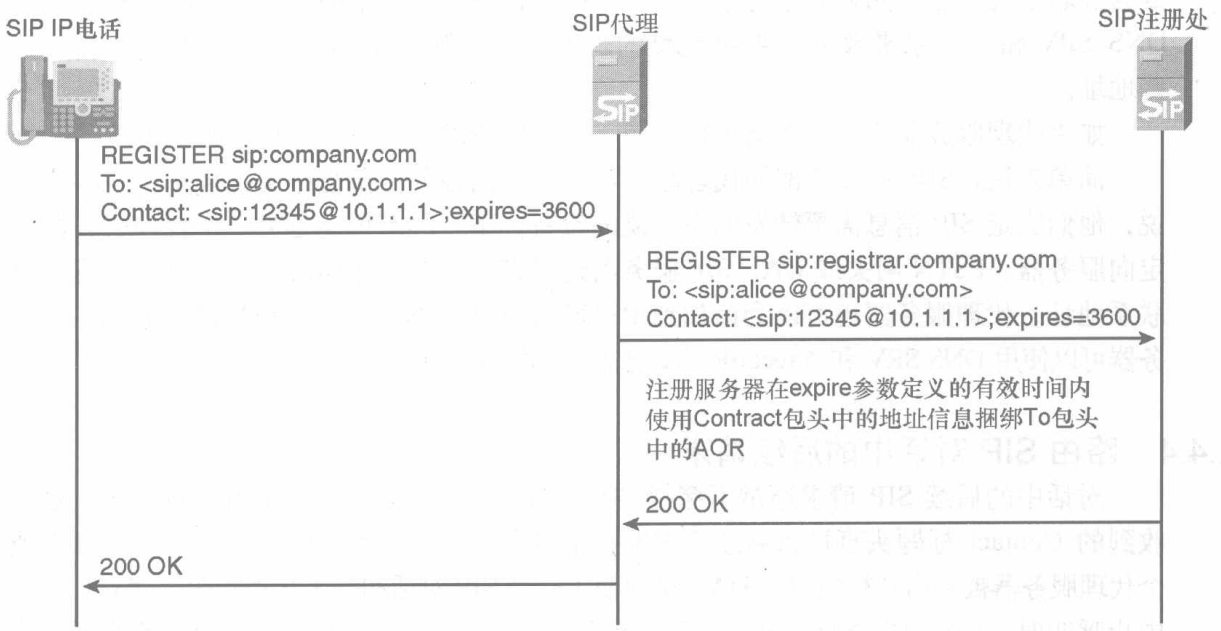


图 12-6 SIP 注册过程

12.4.3 SIP 消息路由

代表用户的 UAC 想要与另一个用户建立一个音频或音频-视频会话。INVITE（邀请）请求行中有被叫方用于路由选择的 SIP AOR。UAC 现在已经就绪，可以发送 INVITE（邀请）到一个 SIP 代理服务器以将 SIP 消息路由到预期的接收者。

当接收到如 INVITE 的 SIP 请求后，在转发请求前，代理服务器使用 INVITE 请求行中的被叫方 AOR 查找目的或下一跳的地址。

SIP 代理服务器用来路由 SIP 请求到 UAS 和 SIP 响应到 UAC 的元素。在到达目标 UAS 前，请求可能会经过多个代理。路上的每个代理服务器在将请求转发到下一跳设备前，都要作路由选择决定和修改请求。SIP 代理服务器在转发请求消息到下一条设备前，可能重写 Request（请求）URI，增加 Via（经由）标题头。代理服务器也可能在请求中插入标题头，如 Record-Route（记录路由）标题头。SIP 响应反向通过与请求相同的一组代理服务器。

实际中，SIP 代理服务器与 SIP 注册服务器是配置在一起的——也就是说，代理服务器通常实施 SIP 注册功能。这样，代理服务器就有权访问在 SIP 注册过程中建立的位置数据库。UA 将初始请求，如 INVITE（邀请）或 SUBSCRIBE（订阅），路由给它所在域的本地代理服务器。这个服务器然后负责根据它的位置数据库和静态路由信息来路由 SIP 请求。这样，代理服务器是域内的所有 SIP UA 和服务器的集合点。

如果代理服务器负责在请求行中域，它将查询位置服务数据库。这个查询返回一个或多个可以联系被叫方的地址。注意，这些联系地址捆绑有效是因为前面描述的注册过程或

因为静态配置信息。如果联系地址是一个主机名，则应用在前面节中描述的过程，如使用 DNS SRV 和 A 记录来做主机到 IP 地址的解析。代理服务器然后将 INVITE 请求转发到这些地址。

如果代理服务器不负责在请求行中域，它转发请求到请求行中指定的主机。

简单来说，SIP 服务器例如代理服务器或重定向服务器执行路由选择功能——也就是说，他们决定 SIP 消息需要转发的下一跳的设备。下一跳有可能是另一个代理服务器、重定向服务器、PSTN 网关或 UA。SIP 服务器通过咨询位置服务器决定下一跳地址或用户的联系地址。代理服务器还可以为诸如到 PSTN 和其他域网关的设备设置静态路由。代理服务器可以使用 DNS SRV 和 A records（A 记录）路由消息到下一跳。

12.4.4 路由 SIP 对话中的后续请求

对话中的后续 SIP 请求通常不穿越 SIP 代理服务器。UA 通常使用在对话建立事务接收到的 Contact 标题头直接将后续请求发送给对方。例如，INVITE 事务可能经过一个或多个代理服务器被路由到被叫方的 UA。这促使了一个 SIP 对话和一个活动呼叫的建立。当一方中止呼叫时，UA 通常直接发送 BYE 请求给另一个 UA。这就使 SIP 代理服务器可以给大量的 UA 提供服务。

然而，SIP 代理服务器可以通过在建立对话请求（如 INVITE 或 SUBSCRIBE）中插入 Record-Route（记录路由）标题头来表明他们希望对话中的后续请求经由他们。在这种情况下，在对话建立之后，UA 根据 Record-Route 和 Contact 标题头的组合产生 Route 标题头。UA 和中间代理服务器则使用 Route 标题头来路由后续事务。

这对于代理服务提供路由选择以外的服务是很有帮助的。代理服务器可能为呼叫产生记账记录，如时间戳，参与方等等。此时，代理服务器不仅要处理起始 INVITE（也就是呼叫建立）还要处理 BYE 事务（也就是呼叫终止）。这就帮助记录了呼叫的开始时间、连接时间和断开时间。

您也可以使用代理服务器来执行策略，或在网络中的中心点进行检查，在这些情况下，代理服务器插入 Record-Route 标题头来保证后续请求都经过它。

图 12-7 列出了包含 SIP 代理服务器的 SIP 呼叫建立和终结的消息流程。

图 12-7 显示了 Alice 和 Bob 间经由代理服务器的 SIP 呼叫建立。Alice 和 Bob 的 SIP 电话属于同一个企业，company.com。他们的 SIP IP 电话都注册到 company.com 域的注册服务器。

1．Alice 的 UA 发送一个带有 Request-URIsip:bob@company.com 的 INVEITE 到代理服务器。INVITE 请求有一个唯一的 Call-ID 标题头和一个 From-Tag（来标记）。在 INVITE 请求的 Contact 标题头有 Alice 的 UA 地址。

2．代理服务器接受 INVITE 并回发 100 Trying 给 Alice 的 UA。

3．代理服务器查找位置服务器，得到 Bob 的 UA 地址，并转发 INVITE 给 Bob 的 UA。

4．Bob 的电话接受到来的 INVITE 请求，回发 100 Trying 给代理服务器。

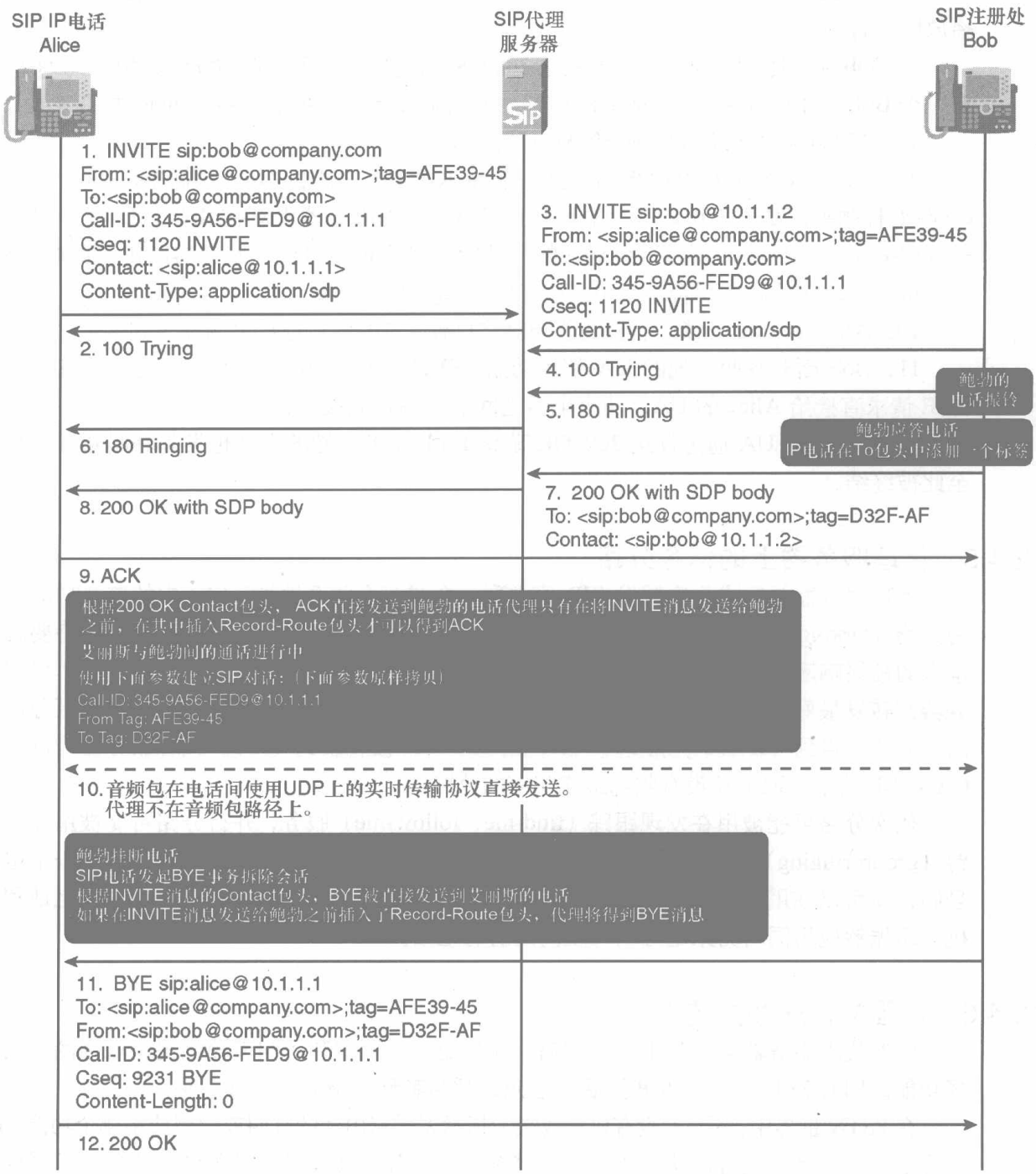


图 12-7 SIP 包含 SIP 代理服务器的呼叫建立和拆除

5．Bob 的 UA 开始振铃，提醒用户有来电。Bob 的 UA 发送 180 Ringing 给代理服务，表明振铃状态。

6. 代理服务器转发 180 Ringing 给 Alice 的 UA。在 Alice UA 得到 180 后，开始为 Alice 播放回铃音调。

7. Bob 应答呼叫。Bob 的 UA 发送 200 OK 给代理服务器。在 200 OK 中的 To 标题头有一个 Bob 产生的 To-Tag。200 OK 还有一个说明 Bob 的 UA 地址的 Contact 标题头。

8. 代理服务器转发 200 OK 给 Alice 的 UA。

9. Alice 的 UA 确认 200 OK,并发送一个 ACK 直接给 Bob 的 UA。根据 200 OK 响应中的 Contact 标题头，发送一个 ACK 给 Bob 的 UA。代理服务器没有在 INVITE 消息中插入 Record-Route 标题头，所以这个对话的后续的消息不再通过代理服务器路由。此时，SIP 对话被建立。对话的标识符是 Call-ID、From-Tag 和 To-Tag。

10. Alice 和 Bob 交谈。音频包在电话之间使用 UDP 上的 RTP 直接发送。

11. Bob 断开呼叫。他的 UA 使用初始 INVITE 消息中的 Contact 标题头，发送一个 BYE 请求直接给 Alice 的 UA。两个电话之间的音频包流被停止。

12. Alice 的 UA 通过发送 200 OK 确认 BYE 事务。她的电话也发起呼叫断开。呼叫至此被终结。

12.4.5 代理服务器上的信令分路

代理服务器并行或依次转发 SIP 请求到一个或多个联系地址。SIP 中的这个功能被称为*分路 (forking)*。在依次分路中，代理服务器在转发请求到下一个位置前，要等待要转发请求的最终响应。在并行分路中，请求被并行发送给所有的位置。在每种情况下，代理服务器都转发最好的最终响应给前一跳设备，该设备是一个 UAC。例如，如果代理服务器从两个分路中得到 486 Busy 和 200 OK，则 200 OK 被转发到 UAC。代理服务器可以使用 CANCEL 请求，取消还没有收到最终响应的分路。

依次分路可能被用在发现跟踪（find-me，follow-me）服务，并行分路可能被用在组振铃（group-ringing）应用中。发现跟踪（find-me，follow-me）服务使用户只需要一个电话号码，就可以在用户定义的顺序上依次联系多个物理电话，如办公室电话、家庭电话和手机。组振铃应用同时为来电呼叫一组内的所有电话。

12.4.6 增强的代理路由选择

SIP 代理服务器可以基于本地策略，应用定义的脚本和呼叫者预制提供增强的路由选择功能。RFC 3841 是一个 SIP 扩展，它允许呼叫者预制服务器处理请求。

在 PSTN 世界中，呼叫者没有权利或能力指示怎样路由他的呼叫或他想使用哪个功能。SIP 允许他在呼叫者预制标题头里指示。这些标题头让呼叫者定义：是否经过代理服务器或重定向服务器路由，将呼叫只是路由到被叫方的移动电话上，还是不振铃被叫方的手机而接通语音留言。

预制标题头提供了高度灵活并可以定制的呼叫路由选择应用。这项功能将在本章后面讨论。

12.5 SIP 扩展

IETF 定义了核心 SIP 规范的扩展以支持更高级的功能，如列席、应用定义路由选择、即时消息和呼叫功能。本节中介绍了为基于呼叫者预制的 SIP Subscribe-Notify（订阅通知）、Refer（提交）和路由选择的扩展。

12.5.1 SIP 扩展协商机制：Require（需要）、Supported（支持）和 Allow（允许）标题头

SIP 参与的和新的功能正在通过 IETF 草案和 RFC 建议。这些新的 RFC 是核心 SIP RFC 3261 的扩展。为了维护与基本 SIP 实施的后向兼容性和帮助不支持新扩展设备协同工作，SIP 定义了扩展协商机制。这个扩展协商通过 Require 和 Supported 标题头实现。

SIP 要求 SIP 实体忽略接收到的 SIP 消息中不知道的标题头。如果 UAC 坚持 UAS 必须理解 SIP 扩展以处理一个请求，UAC 必须使用 Require 标题头指明这一点。Require 标题头包含了在 SIP 扩展中定义的标签。

SIP 扩展可以在现有的方式下定义新的标题头字段，这不能被只支持核心 SIP RFC 的 UAS 或代理服务适当处理。所以，SIP 扩展需要定义选项标记（tag）。选项标记被使用在 Require 或 Supported 标题头。

Require 标题头指明，UAC 坚持 UAS 必须理解处理请求的扩展。如果 UAS 不支持 Require 标题头中的选项标签，它必须通过在 Unsupported 标题头中包含不支持的选项标签来拒绝请求。UAC 可以重新发送不含扩展的请求或选择终结事务。

Supported 标题头告诉 UAS，UAC 支持一定的扩展。由 UAS 决定在响应消息中它是否需要使用这些扩展。比如，在 INVITE 请求中的选项标签 100 rel 表示 UAC 支持 RFC 3262。实施 SIP 扩展的 UA 通常有允许管理员控制启用和禁用功能的配置选项。

Allow 标题头字段列出了产生 SIP 消息的 UA 所支持的功能集合。在如 INVITE 和 SUBSCRIBE 的发起对话事务中，这个标题头可以使 UAS 发现 UAC 支持哪种 SIP 方式。类似地，UAS 可以在如 200 OK 的最终响应中向 UAC 提供类似的信息。例如，一个接收到的在 Allow 标题头不含有 REFER 方式的 INVITE 请求可能会使 UAS 在它的用户界面上禁用“transfer（转发）”。

SIP UA 还可以发送一个 OPTIONS（选项）请求来查询如代理服务器或 UA 等远程设备的功能。OPTION 请求包括 Allow（描述 SIP 方法），Accept（内容类型）和 Supported（SIP 扩展）标题头。远程设备回发一个包含 Allow、Accept、Accept-Language（接收语言）、Accept-Encoding（接收编码）和 Supported 的 OPTIONS 响应（200 OK）。

12.5.2 主叫和被叫偏好

RFC 3841 是一个 SIP 扩展，它允许呼叫者描述中间服务器处理请求时它的偏好。这就允许 SIP 服务器使用如主叫偏好等附加信息来路由 SIP 请求。这些信息包括被叫用户终端

设备能力与主叫偏好的匹配。例如，主叫可能希望建立一个音频和视频会话。在这种情况下，代理服务器不应该将 INVITE 请求路由到只有音频和即时消息功能的联系人那里去。类似的还有，主叫可能只希望联系到被叫的无线 IP 电话并给他留言，而不想与之交谈。

UAC 在 INVITE 和 SUBSCRIBE 请求中通过增加 Accept-Contact（接受联系）、Reject-Contact（拒绝联系）和 Request-Disposition（请求部署）标题头（全部定义在 RFC3841）来定义它的偏好。

Request-Disposition 标题头使主叫方定义服务器应该处理 SIP 请求的方法。主叫方可能会指明服务器是否应该代理或重定向 SIP 请求。在重定向服务器方式，所有与被叫方有关的位置信息在 3xx 响应的 Contact 标题头中返给 UAC。主叫方的 UA 可以在从重定向服务器得到的位置信息上应用定制的路由选择策略。

用户也可以定义代理服务器是否应该以并行方式或依次（在接收到一个前地址的非 2xx 或非 6xx 最终响应后联系下一个地址）将请求转发到所有的可能联系位置。例如：

```
Request-Disposition: proxy, parallel
```

在注册过程中，UA 可以向代理服务器指明它的能力，如的 SIP 方式、音频、视频和 IM。当一个 UA 注册时，它可以选择指明与一个已注册联系人有关的功能集。（细节请参照 RFC 3840）。在消息路由过程中，代理服务器试图将主叫预制和被叫 UA 能力相匹配。

一些在 INVITE 和 SUBSCRIBE 请求中添加的标题头的使用方法如下。

- Accept-Contact: *; video;require;explicit——强制 INVITE 路由到支持视频能力的端点。
- Accept-Contact: *;msgserver;require;explicit——指明用户希望直接访问被叫方的语音信箱。
- Accept-Contact:*;mobility="mobile";require;explicit——只将呼叫发送给被叫方的无线电话上。
- Request-Disposition: proxy，parallel——指明服务器应该代理请求，并在多个联系地址存在的情况下使用并行分路。
- Reject-Contact: *;msgserver——指明用户希望避开被叫方的语音信箱。在这种情况下，代理服务器在路由 INVITE 事务时，不应该包含“msgserver”标签。因此，主叫也不会路由到被叫方的语音信箱服务器。

12.5.3 SIP 事件通知框架：Subscription（订阅）和 Notifications（通知）

RFC 3265 描述了允许 SIP UA 向另一个 SIP 设备订阅当特定事件发生时通知它的 SIP 扩展。这是一个 SIP 节点可以请求来自远程对方当监管事件发生时，得到通知的框架。当有网络事件发生时，产生通知。网络事件的例子有：用户注册或取消注册，语音信箱中有新的语音邮件或有语音邮件被取出，或一个用户将他的在线状态由空闲转为忙或离开。这其实是一个如 SIP 网络的分布式网络上共享状态信息的机制。这个框架是独立于被监控的事件的。所以可以很容易地应用在广大范围的应用上。

例如，SIP 电话可以从 SIP 消息系统订阅的它的用户的语音信箱的状态。订阅的有效时间在 SUBSCRIBE 的 Expires 标题头定义。

12.5.4 SUBSCRIBE 和 NOTIFY 方法

FEC 3265 为 SIP 定义了订阅和通知框架，它使用了两种新的 SIP 方法：SUBSCRIBE（订阅）和 NOTIFY（通知）。

当 SIP 实体为一个特定的事件类型(如 message-summary(消息总结))发送 SUBSCRIBE 请求时，它充当了订阅者。该请求发给 Request URI 定义的 SIP 实体。一个新标题头“Event（事件）”定义了事件类型或事件类型类。对于 SUBSCIRBE 请求来讲，Event 标题头是必须的。订阅的有效时间在 Expires 标题头定义。

SUBSCRIBE 请求的 Request URI 中包含了路由该请求到相应实体的足够信息，还包括了识别事件通知渴望得到的资源的足够信息，但不包含能唯一识别事件属性的足够信息。Event 标题头定义了订阅所请求地确定状态。例如：**Event: presence** 指明了用户的列席状态，**Event: reg** 指明了实体的注册注册状态。

处理 SUBSCRIBE 请求的 UAS 充当通知者；当一个状态发生改变而且订阅有效时，它回送 NOTIFY 请求订阅者。例如，当有一个新语音留言时，基于 SIP 的消息系统发送一个 NOTIFY 给订阅者的 SIP 电话。NOTIFY 请求必须包含一个 Subscription-State（订阅状态）标题头来指明订阅的状态：活动、未决还是终结。

如果 NOTIFY 请求中 Subscription-State 的值是未决（pending），那么通知者已经收到订阅但还没有授权。这可能发生在通知者正在等待最终用户的输入来决定是否接受来自这个订户的订阅。

如果 Subscription-State 是活动（active），则通知者已经接受和授权这个订阅。terminated（终结）则表明通知者已经终结这个订阅。

您还可以在先前存在的对话中发送 SUBSCRIBE 消息。如果在对话后发送，SUBSCRIBE 可能会建立一个新的对话。后续的 NOTIFY 消息将在 SUBSCRIBE 消息建立的对话中发送。订阅者可以通过发送一个含有 Expires 值的新 SUBSCRIBE 来刷新订阅。

最常使用这种机制的有：提供语音信箱状态通知、监管注册和显示用户的列席状态。您也可以使用这种机制来仿效 PBX 功能，这需要在设备间共享状态信息，如共享线路状态。

12.5.5 使用订阅—通知框架监管注册状态

注册过程表现为一个注册服务器在网络中维护的动态状态。当用户注册到网络上或取消注册时，注册状态发生改变。应用可能会对监管注册或用户在线状态感兴趣。

例如，应用服务器向注册服务器订阅 Alice 的注册状态。最初，Alice 没有注册，注册服务器在开始的 NOTIFY 中指出。后来，Alice 在线并注册。注册服务器向应用发送 NOTIFY 通知应用新状态。

注册状态在 NOTIFY 请求的消息体内 使用一个 XML 文档来承载。RFC 3680 定义了注册状态的 XML 格式。

图 12-8 显示了使用订阅来监管注册状态。

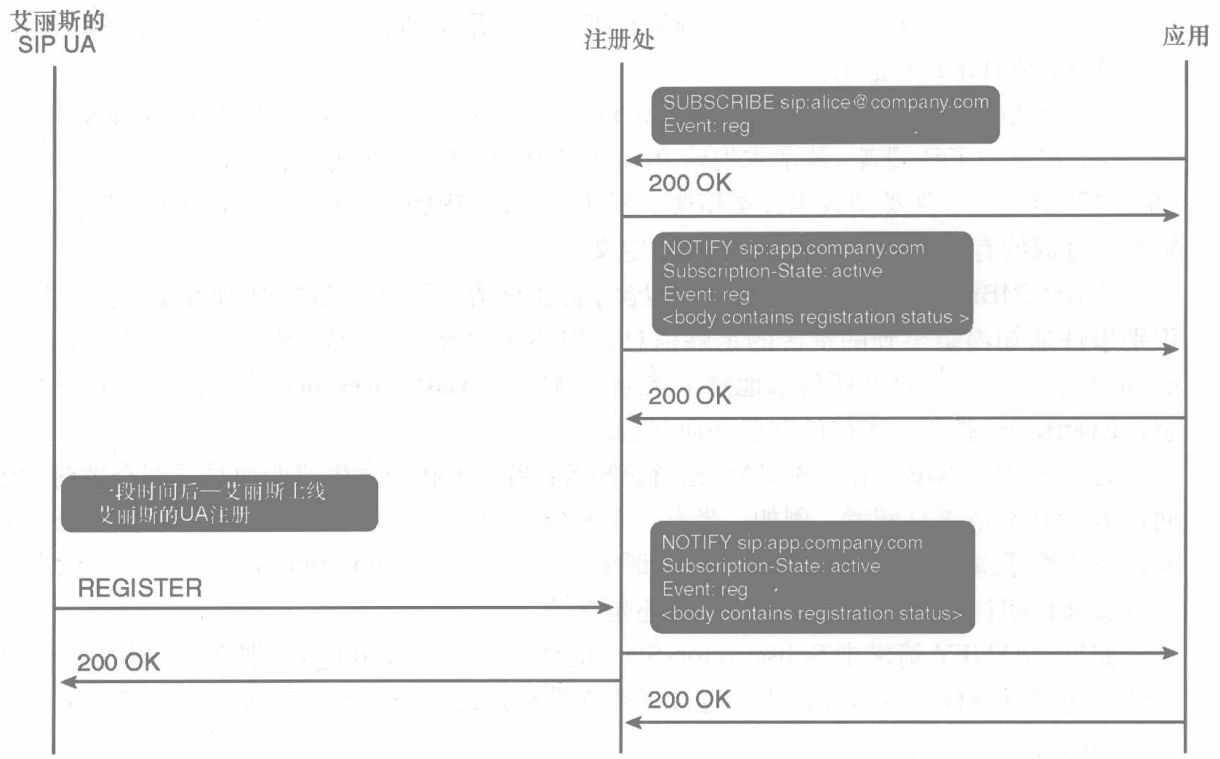


图 12-8 使用订阅—通知框架监管注册状态

12.5.6 SIP REFER 请求

RFC 3515 是一个 SIP 扩展，它定义了一个新的 SIP 请求 REFER。REFER 请求接收者（由 REFER Request-URI 定义）访问在 Refer-To 标题头中描述的资源。REFER 方法的接收者同时被要求通知发送者访问资源的进展。通知使用 NOTIFY 方法发送。这个 RFC 还描述了一个新的事件包“refer”，该包被用在 REFER 的通知消息中。这样，REFER 就在接收方建立一个明确的订阅。

您可以在一个已建立的对话中发送 REFER，如在 INVITE 对话中以触发呼叫传输。在这种情况下，Refer-To 标题头定义了传输目标的 SIP URI。

如果您在已建立的对话之外发送 REFER，则建立一个对话。可能发送对话外 REFER 的应用是点击拨号（click-to-dial）服务。在这种情况下，用户点击一个在线目录则它的电话就呼叫想要呼叫的电话。点击拨号（click-to-dial）功能的应用服务器向发起人的电话发送一个带有指向被叫方的 Refer-To 的 REFER 消息。在电话接收到 REFER 后，它提示他的

用户（点击拨号的发起人）然后通过给 Refer-To 标题头提供的 URI 发送 INVITE 请求拨打电话。

您可以使用 REFER 给一个会议中添加第 3 方参与者。客户端可以给参与者发送 REFER，请求他给会议 URI 发送 INVITE 请求。另外，客户端发送一个 REFER 请求给会议的控制者，请求它发送一个 INVITE 给参与者，请求他参加会议桥。这只是 REFER 请求的一些简单应用。REFER 是一个灵活的功能强大的概念，您可以在许多应用中使用。

12.5.7 列席和即时消息概览

列席描述了一个人与其他人通信的意愿、有效性和能力。列席服务允许用户将他们的有效状态和显示信息或图标作为一种自我表达的形式来发布。即时消息（Instant Messaging，IM）指在用户间以近似实时的方式传递文字消息。

IM 提供了实时的、基于文本的通信，但是它只有在接收者可以参与时有用。列席则提供了订阅一个用户的在线状态来决定他是否可以接受 IM 会话和呼叫的能力。当用户列席被集成在通信架构中时，决定联系目标的最可能的方式变得简单。例如，一个繁忙的主管可能正在电话会议中，不能接听另一个呼叫。但是，他可能可以接受 IM 会话。类似地，SIP 电话中的漏听电话列表可能指示了呼叫者的状态。这就使用户可以区分他应该首先回谁的呼叫。

一个人的列席状态是他的各种设备如固话、日历应用、计算机上的 IM 客户端和手机的状态集合。列席服务收集这些信息并提供一个统一的视图。这个集合不仅显示了一个人的有效性，还显示了联系他的最佳办法。这样列席就提高了呼叫成功的可能性。

一个基本的列席服务允许用户与其他人发布和共享信息，使通信经历更人性化、更有效。列席服务允许用户控制谁可以得到他们的列席状态，以及共享信息的程度。列席服务可以提供默认状态，如对那些拒绝访问的用户显示为无效（也称为*礼貌屏蔽（polite blocking）*）。

IM 和列席的 SIP 扩展

SIP 在即使通信和列席中的扩展（SIP for Instant Messaging and Presence Leveraging Extensions，SIMPLE）是一个 IETF 工作组，这个工作组的主要工作是使用 SIP 和建议 SIP 扩展为 IM 和列席服务提供协同工作能力。RFC 3856 为 SIP 定义了一个列席事件包。

一个用户使用 SUBSCRIBE 方法订阅另一个用户的列席状态。虽然您可以发送订阅直接给另一个用户，通常使用一个列席服务器来处理列席订阅请求和代表用户发布列席状态。

一个列席服务器（presence server）是一个 SIP 网络服务器，用来代表目标最终用户处理列席请求和代表用户发布列席信息。列席服务器因为不需要轮询来监管远程用户是否在线，所以对于对等架构来讲很有优势。另外，服务器还允许基于网络的策略，如安全性和隐私控制实施。

UA 发送一个带有列席事件包的 SUBSCRIBE 来订阅另一个用户的列席状态。要跟踪

列席信息的目标用户或资源被称作列席实体（presentity）。列席实体被定义在 RFC 2778 中，RFC 2778 提供了一个列席和即时消息的模型。SIP URI 通常标识列席实体。

SIP 代理服务器路由这个 SIP 请求到网络中列席服务器。列席服务器代表用户订阅目标用户的列席实体或列席状态。目标用户的 SIP UA 或端点设备接收列席订阅。这个 UA 也被称为列席代理（Presence Agent，PA）。

当目标用户的状态改变时，PA 通知列席服务器列席状态的改变。SIP NOTIFY 请求使用一个包含列席状态的 XML 体提供通知功能。列席服务器随后通知所有其他订阅这个列席信息的用户。

因为列席服务器控制列席信息的分发，在远程用户请求订阅列席信息时，列席服务器必须寻求目标用户的许可。如果列席服务器有一个预定义的策略，服务器使用这个策略允许或拒绝列席状态的订阅。如果服务器没有这样的策略，它发送一个请求给本地用户来授权订阅或使用缺省的系统策略来处理订阅。

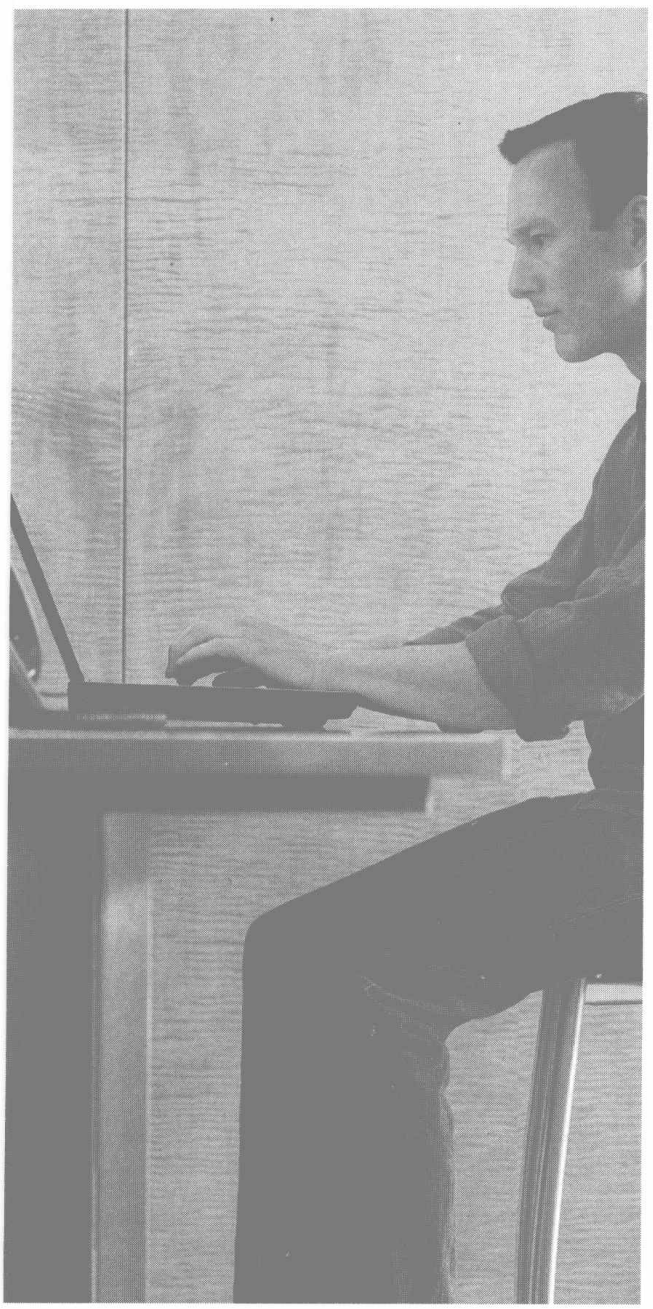
RFC 3428 扩展了 SIP 并定义了一个新 SIP 请求 MESSAGE（消息）允许传送即时消息。MESSGE 请求以 MIME 体形式承载消息内容。类似的，RFC 3903 定义了一个新 SIP 请求——PUBLISH（发布），来发布如列席状态的事件状态。

12.6 总结

SIP 是一个 IETF 为包含一个或多个参与者的多媒体应用的信令协议。IETF 方式是建立一个层次的功能架构，在这个架构中高度优化的协议实现特定功能。SIP 是一个灵活的协议，支持新应用和服务的扩展。

SIP 是分布的，在网络服务器上有较好的扩展性。SIP 对话状态在端点维护。SIP 网络服务器或者是无状态的，或者维持事务状态信息至少 32 秒。

本章提供了 SIP 及其操作的概览。进一步的详细内容请参照适当的 SIP RFC。



本章讨论网络架构框架和设计模型，包含以下主题：

- 13.1 MGCP 概览
- 13.2 MGCP 模型
- 13.3 MGCP 命令和消息
- 13.4 MGCP 呼叫流程
- 13.5 高级 MGCP 功能
- 13.6 H.248/MEGACO
- 13.7 总结

第13章

网关控制协议

本章覆盖了两个 IETF 控制来自外部呼叫控制元素的 VoIP 网关的网关控制协议：媒体网关控制协议（Media Gateway Control Protocol，MGCP）和 H.248/MEGACO。这些网关控制协议支持媒体功能与呼叫信令功能分开的 VoIP 体系结构。因此，他们被广泛的应用在大的中继网关和驻留网关中。MGCP 被广泛部署，也是本章的核心。H.248/MEGACO 是另一种竞争协议，在本章的最后将作简单介绍。MEGACO 代表媒体网关控制，不要与 MGCP 混淆。

13.1 MGCP 概览

MGCP 是一种媒体网关控制器（media gateway controllers，MGC，也称为呼叫代理），一种控制媒体网关（Media Gateways，MG）的协议。MGCP 是基于主/从结构的，其中 MGC 是主，向 MG（从）发布命令。MG 确认命令，执行命令并通知 MGC 结果（成功或不成功）。在这个体系结构中，MG 处理媒体功能，例如转换时分多路复用（time-division multiplexing，TDM）/模拟信号到实时传输协议（Real time Transport Protocol，RTP）/实时传输控制协议（Real-time Transport Control Protocol，RTCP）流。MGC 处理呼叫信令功能。

在这个模型中，呼叫控制智能在 MGC 中，MG 是一个“哑（dumb）”实体，根据 MGC 的命令行动。

MGCP 消息通过用户数据报协议（User Datagram Protocol，UDP）承载。因为 UDP 不保证数据的传输，在需要时，消息被重传。

MGCP 来源于两种早期协议： 简单网关控制协议（Simple Gateway Control Protocol，SGCP）和互联网协议设备控制（Internet Protocol Device Control，IPDC）本章覆盖在 RFC 2705 中描述的 MGCP 版本 1.0，对于 SGCP，IPDC 和 MGCP 的早期版本，不作深入介绍。

MGCP 使用会话描述协议（Session Description Protocol，SDP）来描述媒体会话。SDP 为在 MG 之间的媒体流描述会话参数，如 IP 地址，UDP 端口，RTP 档案和多媒体会议能力。MGCP 遵从 RFC 2327 中定义的 SDP 约束，并期望实施遵从。SDP 规范定义了几种媒体类型，然而 MGCP 将 SDP 的使用限制为两种媒体类型：音频线路和数据访问线路。

呼叫代理将如下的 SDP 参数提供给电话网关。

- IP 地址——使用远程网关，本地网关或多点音频会议地址来交换 RTP 包。
- UDP 端口——指明用于从远程网关接收 RTP 包的传输端口。
- 音频媒体——定义音频媒体，包括编码器。

13.2 MGCP 模型

MGCP 设想了一个连接模型，其中基本构造是端点和连接（参见图 13-1）。连接按呼叫分组。一个或多个连接属于一个呼叫。连接和呼叫被 MGC 主动建立。在进一步探讨 MGCP 细节前，下面的小节先详细介绍端点和连接。

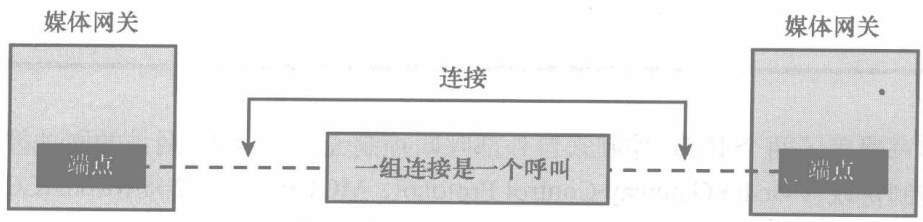


图 13-1 MGCP 连接模型

13.2.1 端点

端点是数据源或接收器。他们是存在于 MG 内的物理的或逻辑的实体。

一个物理端点的例子是 MG 上的一个终结一条来自 PSTN 交换机的电路的接口。

一个逻辑端点的例子是一个根据呼叫代理的命令发表公告的公告服务器端点。

物理端点通常需要硬件安装，逻辑端点的建立可以在软件中执行。

每个端点通过有两个组件的端点标识符表示：

- 包含端点的 MG 所在的域名；
- 网关内的本地名或标识符。

13.2.2 连接

连接可以是点对点的也可以是多点的。一个点对点的连接是在两个端点间为传输数据的联合。您可以通过将端点连接到一个多点会话建立多点连接。

在每个将被卷入一个呼叫的端点建立一条连接。每个连接被本地指定一个连接 ID，通过一组连接属性识别。

被卷入一个连接的端点可能在不同的或同一个网关上。

13.2.3 呼叫（Calls）

一组连接组成一个呼叫。呼叫代理分配呼叫标识符，这个标识符对于每个呼叫都是唯一的，而且在整个系统中也是唯一的。呼叫标识符将所有属于一个呼叫的连接联系在了一起。这个标识符允许对呼叫的记账或计费仲裁。

13.3 MGCP 命令和消息

MGCP 实施媒体网关控制接口为一组事务。事务由一个命令和一个必需的响应组成。

所有的 MGCP 命令有一个命令行，紧跟着是一组参数行和可选的会话描述。命令行有如下格式：

<Command name> <Transaction-ID> <Endpoint-ID> <MGCP ver>

每个参数行依次包含一个参数代码，紧跟着是一个参数值。所有的响应由响应包头紧跟着可选会话描述组成。

虽然在 RFC 2705 种没有正式的分类，但为了易于理解，您可以将 MGCP 命令分为三类。

- 基本呼叫控制命令——这些命令几乎被用于每个呼叫交互。这些命令如下：
  - CreateConnection（CRCX，建立连接）；
  - ModifyConnection（MDCX，修改连接）；
  - DeleteConnection（DLCX，删除连接）。
- 高级呼叫控制命令——MGC 也许需要知道在一个端点的呼叫有关事件的出现。这些事件的典型的例子是双音多频（dual-tone multifrequency，DTMF）数字、传真音调、摘机/挂机事件等。MGCP 为 MGC 请求网关监视端点上特定事件并报告它们的出现提供了一个接口。MGC 使用 NotificationRequest（RQNT，通知请求）命令请求网关汇报特定事件的出现。网关使用 Notification（NTFY，通知）命令向 MGC 汇报这些事件的出现。
- 管理命令——这些与呼叫控制不直接相关，但是 MGC 和网关交换它们来通知对方某个与呼叫无关的时间。比如说，一个网关可能在一些它的端点上有硬件错误，需要通知 MGC。MGCP 为管理目的提供 4 个不同的命令：
  - AuditConnection（AUCX，审计连接）；
  - AuditEndpoint（AUEP，审计端点）；
  - RestartIn-Progress（RSIP，重新处理）；
  - EndpointConfiguration（EPCF，端点配置）。

下面的小节中介绍每个经常用到的 MGCP 命令，并简要介绍常用的参数。每个参数代码在括号中给出。这不是详细的完全列表。参数的详细列表参照 RFC 2705（http://www.ietf.org/rfc/rfc2705.txt）。

13.3.1 CreateConnection（CRCX，建立连接）

就像它的名字表明的那样，这个命令在两个端点间建立一个连接。CreateConnection 命令的参数提供给网关建立连接的必要信息。

- 呼叫 ID——这是一个由 MCC 分配的全球唯一的参数。所有与该呼叫有关的连接共享这个标识符。
- 通知实体（Notified Entity（N））——这是一个可选参数，定义向哪里发送通知。
- 位置连接选项（Local Connection Options（L））——这个参数描述在执行 CreateConnection 命令时所使用的数据通信特性。这个参数的字段包括编码方式、打包

阶段、带宽、服务类型（ToS）和回声消除的使用。在默认情况下，回声消除总被执行。

- 模式（Mode（M））——这个参数指明连接的操作模式。选项有全双工、只接收、只发送、不活动和回放（loopback）。
- 远程连接描述符（Remote Connection Descriptor，RC）——这个参数为连接的远程侧说明连接描述符，通常在 IP 网络的另一侧。当还不知道远程终端信息时，此参数可能为空。

13.3.2 ModifyConnection（MDCX，修改连接）

ModifyConnection 命令修改一个连接或呼叫的网关视图的特性。在 ModifyConnection 命令中的参数和字段与 CreateConnection 命令中的相同，增加了一个 Connection ID（连接 ID）参数。Connection ID 参数唯一标识了端点上的连接。您可以使用 ModifyConnection 命令修改如下连接参数：编码方案、打包周期、回声消除和激活和失效连接。

13.3.3 DeleteConnection（DLCX，删除连接）

呼叫代理或网关使用 DeleteConnection 命令来终结一个连接。呼叫代理使用这个请求终结在两个端点间的连接，或清除所有在终结在给定端点的连接。如果网关检测到一个端点不能再发送或接收音频时，使用此命令清除连接。在网关清除一个连接时，在消息中包含的原因代码以说明原因。

在连接被终结后，网关应该将端点置为非活动模式，这样端点对于一个后续会话就是有效的了。DeleteConnection 命令的一个有价值的属性是它散布乐一个呼叫统计数字。表 13-1 列出了在 DeleteConnection 消息中的统计数据。

表 13-1 DeleteConnection 消息中的统计信息

数据	描述
发送包数	在连接上发送的包数
发送字节数	在连接上发送的字节数
接收包数	在连接上接收的包数
接收字节数	在连接上接收的字节数
分组丢失数	丢弃的使用序列号标识的包数
抖动	以毫秒记平均包间延迟
时延	以毫秒记平均延迟

13.3.4 NotificationRequest（RQNT，通知请求）

MGC 使用 NotificationRequest 命令请求网关根据一个端点上的特定事件的出现发送通知。在这个命令中两个重要的参数是 Requested Events（请求事件）参数，使用参数代码 **R** 表示，和 Signal Requests（信号请求）参数，使用参数代码 **S** 表示。在本章进一步讨论其他参数之前，理解 R 和 S 参数是非常重要的。

请求事件参数（**R**）包含网关被要求检测和汇报给呼叫代理的事件列表。在这个列表中可能的事件有：传真和调制解调器音调、连续音调和检测、摘挂机转换、闪跳（flash hook）、随路信令（CAS）、闪烁（wink）和 DTMF（或脉冲数字）。另外，被请求的操作可以限定每个事件。在定义操作时，使用被编码的关键字列表，用括号括起来，使用逗号分割。表 13-2 列出了各种操作的编码。

表 13-2 MGCP 事件操作代码

操作	编码
立即通知	N
累积	A
根据数字映射对待	D
交换	S
忽略	I
保持信号活动	K
嵌入通知请求	E

当没有明确定义操作时，默认是通知 MGC 事件。下面是一个“requested events”参数行的例子：

```
R: hu(N)
```

这个例子中，网关被要求查找 **hu**（摘/挂机事件）并在事件发生时立即通知（使用操作代码 N 表示）。

信号请求（**S**）参数定义了网关被要求应用在端点的一系列信号。经常使用的信号有：振铃和特色振铃（ringing and distinctive ringing）、回铃（ring back）、拨号（dial）、截取（intercept）、忙、应答、呼叫等待、摘机提示、连续音。根据它们的行为，信号被分为三种不同的类型。

- 开/关（On/Off，OO）——这些信号将被应用直到它们被关闭。
- 超时（Time-Out，TO）——在这些信号被应用后，它们保持直至超时，具体时间根据信号定义的时间周期。
- 短促（Brief，BR）——这个信号的持续时间很短，自己停止。

表 13-3 列出了常见的事件和信号。对于信号，时间类型也定义了。注意同样的事件根据

它所在包部分不同有不同的持续时间。

表 13-3 事件和信号

事件符号	定义	持续时间
Hd	摘机	OO
Hu	挂机	OO
Dl	拨号音	话筒仿真包-TO（120s）
Rg	振铃	话筒仿真包-TO（30s）
Hf	闪跳（Flash hook）	BR
Bz	忙音调	话筒仿真包- OO
Aw	应答音调	OO
Wt	呼叫等待音调	TO（30 s）
ci（string）	呼叫 ID	BR
Mt	检测到体制解调器音调	-
Ft	检测到传真音调	-
Cg	网络拥挤音调	TO
It	截取音	OO
Wk	闪烁	BR
Wko	闪烁停止	BR
dtmf 8	DTMF 数字 8	BR
mf 9	MF 数字 9	BR
Ann	播放提示	TO（var.）
Java	加载 Java 脚本	TO（var.）

其他在 NotificationRequest 中使用的参数如下。

- 通知实体（Notified Entity）（N）——如果有，定义向哪里发送通知。如果没有，则表明通知应该发送个起始者。
- 请求标识符（Request Identifier）（X）——这个参数将 NotificationRequest 命令与它出发的通知相关联。

13.3.5 Notification（NTFY，通知）

网关根据在通知请求中请求的事件和这些被观察事件的出现来发送一个 *Notification（通知）*。Notification 命令包含如下参数。

- 通知实体（Notified Entity）（N）——如果有，定义向哪里发送通知。如果没有，则表明通知应该发送个起始者。

- 被请求标识符（Requested Identifier）（X）——这个参数等于在 NotificationRequest（通知请求）中的“request identifier”（请求标识符）。它将请求与通知关联。
- 被观察事件（Observed Events）（O）——这个参数包含了一系列的事件，这些事件是网关根据早先来自 MGC 的 NotificationRequest 命令中被请求事件参数检测的事件。

13.3.6 AuditEndpoint（AUEP，审计端点）

呼叫代理可以使用 *AuditEndpoint* 命令来判断一个端点的状态。这通常在呼叫代理初始化时，要寻找所有由它控制的端点的状态时进行。这个请求包含一个端点 ID 参数，用来表示要审计的端点，以及一个请求的信息参数包含如下子参数。

- 端点列表（Endpoint List）——这个指明了要审计的端点。您可以使用通配符来指出所有匹配的端点。
- 通知实体（Notified Entity）（N）——这是活动通知请求要通知的实体。
- 请求的事件（Requested Events）（R）——这是一个目前被请求的事件列表。
- 数字映射（Digit Map）——端点目前使用。数字映射将在后面的 13.5 节中介绍。
- 信号请求（Signal Requests）（S）——目前所应用在一个端点的信号请求。
- 请求标识符（Request Identifier）（X）——端点最后接收到的“NotificationRequest”的标识符。
- 连接标识符（Connection Identifiers）（I）——在给定端点上目前存在的连接的列表。
- 探测事件（Detect Events）（T）——在隔离模式下目前被探测的事件的列表。
- 本地连接选项（Local Connection Options）（L）——目前所有值的列表，如编码器、包优化周期等。您可以使用这个参数来查询给定端点的目前事件包。

来自网关的 AUEP 将包括被请求的审计的每项的信息。

13.3.7 AuditConnection（AUCX，审计连接）

呼叫代理使用 AuditConnection 命令得到连接的信息。这个命令包括要审计的位置和连接的端点 ID（Endpoint ID）和连接 ID（Connection ID）。请求信息的子参数包括如下信息。

- 呼叫 ID（Call ID）——被审计信息所述的呼叫的唯一标识符。
- 通知实体（Notified Entity）（N）——目前连接要通知的实体。
- 本地连接选项（Local Connection Options）（L）——目前应用在连接上的选项。
- 模式（Mode）（M）——目前的连接模式。
- 远程连接描述符(Remote Connection Descriptor)(RC)——被用于连接的远程 SDP。
- 本地连接描述符（Local Connection Descriptor）（LC）——用于连接的网关。
- 连接参数（Connection Parameters）（P）——被审计连接的目前参数值。

13.3.8 RestartIn-Progress（RSIP，重新处理）

网关使用 RestartIn-Progress 命令通知呼叫代理一个端点或一组端点实效或重新服务。RestartIn-Progress 命令包含如下参数。

- 端点 ID（Endpoint ID）——标识重返服务或失效的端点。
- 重启动方式（Restart Method）（RM）——说明如下几种不同的重启动类型：
- graceful（优美）重启方式说明特定的端点间在给定的时间后重启，呼叫代理不要再建立新的连接。
- forced（被迫）重启方式说明该端点突然失效，所有连接丢失。
- restart（重起）重启方式说明当端点没有连接时将重新服务。
- disconnected（断开）方式是指端点已经被断开，正在试图建立连接。
- 重起延迟（Restart Delay）（RD）——用以说明延迟的秒数。

13.3.9 EndpointConfiguration（EPCF）（端点配置）

EndpointConfiguration 命令允许呼叫代理定义端点接收信号的编码方式。这在μ-law 和 A-law 编码技术都被使用的国际环境非常有用。这个命令使用 Bearer Information（B）（承载信息）参数将编码信息传递给网关，该参数说明了它定义的端点这一侧接收数据的编码技术。目前，子参数仅定义了 A-law 和 μ-law。

13.3.10 MGCP 响应消息

所有的 MGCP 命令都需要确认。确认承载一个返回码（return code）用以说明命令的当前状态。返回码是一个定义了 4 个范围整数：

- 100～199 说明是一个临时响应；
- 200～299 说明是一个成功响应；
- 400～499 说明是一个暂时错误；
- 500～599 说明是一个永久错误。

表 13-4 列出了返回码及其解释。

表 13-4 MGCP 返回码

返回码	描述
100	命令正在执行中。最终响应随后
200	一般事务执行
250	连接被删除
400	因为瞬时错误，无法执行事务处理
401	电话已摘机
402	电话已挂机

续表

返回码	描述
500	因为端点未知，无法执行事务处理
501	因为端点未准备好，无法执行事务处理
502	因为没有充足端点资源，无法执行事务处理
510	因为协议错误，无法执行事务处理
511	因为包含不可识别扩展，无法执行事务处理
512	因为网关无法探测请求事件，无法执行事务处理
513	因为网关无法产生请求信号，无法执行事务处理
514	因为网关无法发送特定公告，无法执行事务处理
515	事务指向不正确的连接 ID
516	事务指向未知的呼叫 ID
517	不支持模式
518	不支持事件包
519	网关没有数字映射
520	因为端点重起，无法完成事务处理
522	不存在这个事件或信号
523	未知操作或操作组合
524	与本地连接选项不一致

13.4 MGCP 呼叫流程

本节列出了一些典型的呼叫流程，以及每个消息的语义解释。呼叫流程以复杂度渐增的顺序描述。注意所有这里的呼叫流程只是为了演示举例。具体使用一个 MGCP 厂商设备的实施可能是另一种流程。

13.4.1 基本 MGCP 呼叫流程

一个简单的点对点呼叫建立使用两个命令：CreateConnection 和 ModifyConnection。

图 13-2 显示了在两个端点间建立一个呼叫的流程。端点假设在不同的网关上，MGC 控制两个网关。图中只显示了相关部分的消息。这个双发呼叫的起始侧和终结侧分别通过后缀 *Orig* 和 *Term* 标明。图中的消息以对应后面说明的数字标注。当然，这些标签不是消息的一部分。

1．呼叫代理发送一个起始的 CRCX 给 GW-Orig 并指定端点 S1/DS1-0/1。连接方式被设为 recvonly（只接收）。这个设置向 GW-Orig 说明端点应该只从 IP 网络上接收媒体，不在 IP 网络上发送。这是必要的，因为呼叫代理没有在 GW-Term 上建立连接，所以不知道它的会话描述。

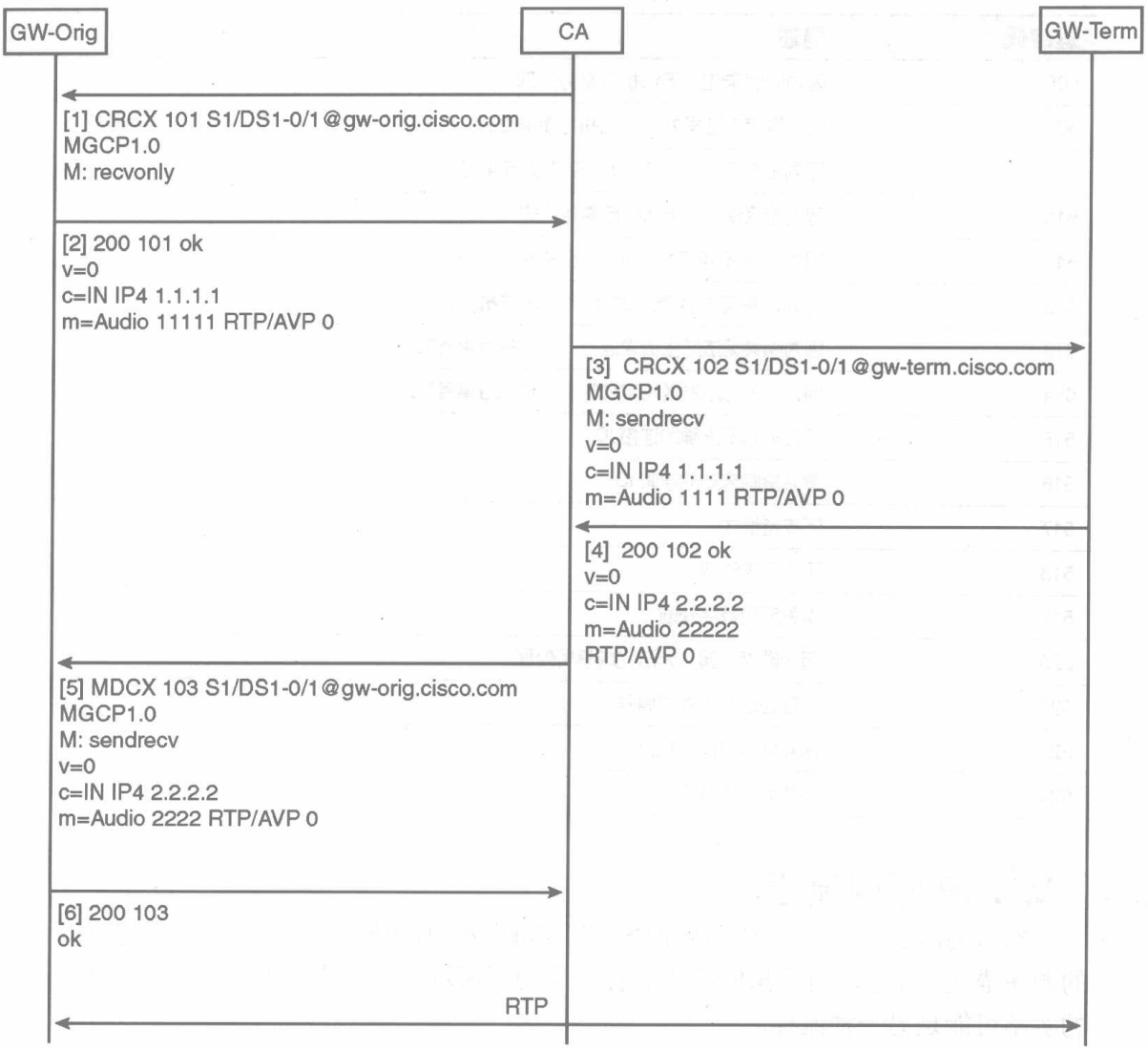


图 13-2 基本呼叫流程

2．GW-Orig 使用一个 200/OK 响应，指明该连接已经成功建立并提供一个本地会话描述（根据 SDP 规范编码）。这个会话描述包括网关打开的用以接收 RTP 流的本地 IP 和端口（1.1.1.1 和 11111）。SDP 也说明了使用 G.711μ-law 编码（使用 RTP/AVP 0 说明）。

3．呼叫代理发送一个 CRCX 给 GW-Term 上的端点 S1/DS1-0/1。从 GW-Orig 上接收到的会话描述被包括在这个 CRCX 的 RemoteConnectionDescriptor（远程连接描述符），模式被设为 sendrecv（发送接收）。

4．GW-Term 使用 200/OK 响应，响应中包括它自己的会话描述。

5．呼叫代理在一个 MDCX 命令中传递 GW-Term 的 SDP 给 GW-Orig，并改变连接模式为 sendrecv（发送接收）。

6．在 GW-Orig 执行 MDCX 命令并使用 200/OK 响应后，呼叫建立完成，RTP 流在 GW-Orig 和 GW-Term 之间流动。

13.4.2 中继网关到中继网关的呼叫流程

在前面小节中介绍的使用 MGCP 建立连接的呼叫流程是相当直接的。而且，这个呼叫流程也没有告诉您怎样和为什么呼叫代理决定建立那两个端点间的连接。在实际生活中，呼叫代理通过外部信令知道这些信息。一个典型的例子就是终结在呼叫代理上的 SS7 中继。在这种情况下，SS7 消息触发了呼叫代理的操作。

图 13-3 显示了 SS7 消息与 MGCP 之间的交互。

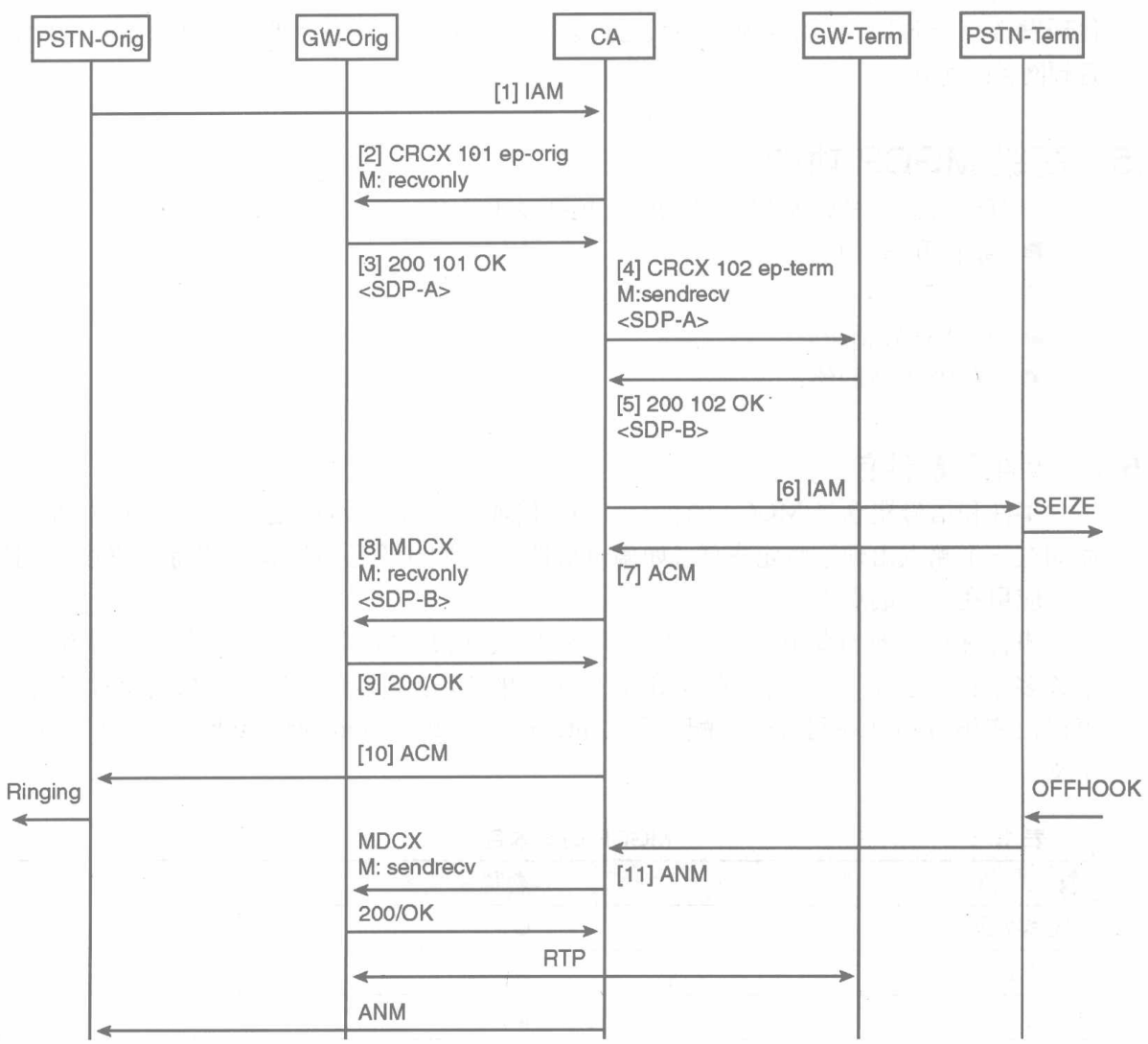


图 13-3 中继网关到中继网关的呼叫流程

在 SS7 中继上的呼叫代理接收到一个发起地址消息（initial address message）（IAM）[1]。这个操作触发呼叫代理分析 IAM，并根据本地配置决定如何处理。本地配置（或外部数据库查询）告诉呼叫代理在两个在 GW-Orig 和 GW-Term 网关上的端点 ep-orig 和 ep-term 建立一个呼叫。

呼叫代理发送两个 CreateConnection 消息[2] 和 [4]，与图 13-2 显示的流程相似。在 PSTN-term 抢占该线后，给呼叫代理发送一个 SS7 ACM [7] 消息。然后呼叫代理发送一个 MDCX [8]给 GW-Orig。注意目前的 ConnectionMode（连接方式）被设为 recvonly（只接收）。这是因为，在此时只有振铃声需要回送给起始侧。起始侧还不能发送音频。

在终结电话被拿起后，PSTN-Term 发送一个 ANM [11] 消息给呼叫代理。这触发呼叫代理发送一个 MDCX 给 GW-Orig 设置模式为 sendrecv（发送接收）。这就完成了一个两路音频网关的建立。

13.5 高级 MGCP 功能

本节概括了一些高级 MGCP 功能，包括以下几个：

- 事件和事件包；
- 数字映射；
- 嵌入通知请求；
- 非 IP 承载网络。

13.5.1 事件和事件包

事件和信号概念是 MGCP 的核心。呼叫代理可以请求 MG（通过一个 RQNT 消息）被通知在一个端点出现了特定事件（如摘机事件），呼叫代理还可以请求将特定信号（如拨号声）应用在一个端点上。

事件和信号被分组在一个包内，在该包内它们共享命名空间。一个端点可能支持一个或多个包。表 13-5 列出了在 MGCP 中定义的 10 个基本包。注意附加的事件名称和包可以由实施者向互联网号码分配当局（Internet Assigned Numbers Authority，IANA）注册定义。

表 13-5 MGCP 的基本包

包	名称
普通媒体包	G
DTMF 包	D
MF 包	M
中继包	T
线路包	L

续表

包	名称
话筒包	H
RTP 包	R
网络接入服务器包	N
公告服务器包	A
脚本包	Script

RFC 2705 对在特定端点类型上应该实施哪个事件包有特别的建议。这样做是为了允许不同厂商的网关和呼叫代理可以互通。表 13-6 列出了基本的端点类型、它们的基本配置以及它们支持的包。

表 13-6 端点类型和支持的包

网关（Gateway）	支持的包
中继网关（ISUP）	G，D，T，R
中继网关（MF）	G，M，D，T，R
网络接入服务器（NAS）	G，M，T，N
NAS/VoIP 网关	G，M，D，T，N，R
接入网关（VoIP）	G，D，M，R
接入网关（VoIP，NAS）	G，D，M，R
驻留网关	G，D，L，R
公告服务器	A，R

13.5.2 数字映射

在许多情况下，MGC 需要收集在端点上出现的数字事件。驻留网关通常使用这个系统来收集用户拨叫的号码。中继网关可以使用数字映射来收集访问代码和其他事情。一种方式是在数字被拨打后，网关立即通知 MGC 被拨叫的数字。这种一个数字一个数字的方式在网关和 MGC 间产生了大量的 RQNT 和 NTFY 消息交换。

另一种方式就是使用数字映射，MGC 给 GW 一个可能拨叫数字的匹配列表，GW 只有在匹配时才通知 MGC。数字映射使用源自 UNIX **egrep** 命令的语法描述。

13.5.3 嵌入通知请求

您在给定时间可以在一个媒体网关上应用一个 RQNT 命令。当在 RQNT 中定义的事件在端点上发生时，媒体网关发送一个 NTFY 给 MGC 通知它的发生。只有在这时，MGC 可以发送一个带有新的 RequestedEvents 集的 RQNT。这就有可能产生一种紊乱的情况，在网关已经发送了给原有的 RQNT 的 NTFY 后，但还没有接收到新的来自 MGC 的 RQNT 时，

会发生一些有趣的事件。

为了减轻这个问题，MGCP 引入了嵌入通知请求（*embedded notification request*）概念。使用这个构造，MGC 可以将通知请求嵌入到另一个里面。媒体网关在一个 Requested Event（被请求事件）发生时就将其嵌入到通知请求中，不再等待来自 MGC 的指示。嵌入通知请求可以包含一个新的被请求的事件列表，请求信号和一个新的数字映射。在被请求的事件列表中，嵌入通知请求使用操作代码 **E** 表示。下面是一个在被请求的事件（Requested Events）（R）命令行中的一个嵌入通知请求的例子：

```
R: hd (E (R[0-9]) )
```

这是告诉网关查找一个 **hd** 事件。当 **hd** 事件发生时，网关应该应用[0-9] 作为被请求的事件。

13.5.4 非 IP 承载网络

MGCP 通常用在 IP 网络承载媒体时。然而，MGCP 也允许自在其他类型的承载网络上建立连接。这包括在 ATM 网络上使用 ATM 适配层 2（ATM adaptation Layer 2，AAL2）和 TDM 到 TDM 连接（“发卡”（hairpinning），起始于 PSTN 的呼叫被送回 PSTN）。

13.6 H.248/MEGACO

H.248（在 ITU 中）或者 MEGACO（在 IETF 中）在体系结构和目的方面与 MGCP 类似。本节简要介绍一下 H.248 的构造，不作深入探讨。

在 H.248 连接模型中，主要构造是终结（terminations）、上下文（contexts）和命令。

终结（Termination） 是一个或多个媒体流的源或接收器。上下文（context）是一组终结的关联。一个终结在给定时间内只能在一个上下文中。一个特殊的上下文类型，空上下文（null context），包含了所有的不在其他上下文中的终结。例如，在一个访问网关，所有空闲的线路被表示为一个空上下文的终结。

您使用命令来操作终结和上下文。**Add** 命令在一个上下文中添加一个终结。**Subtract** 命令将一个终结从一个上下文中移出，如果上下文中没有终结存在可能会引起释放该上下文。**Move** 命令将终结从一个上下文中移到另一个上下文中。**Modify** 命令改变终结的状态。

在 MGCP 中，您可以认为，一个终结类似一个端点，一个上下文类似一个呼叫。而且，**Add** 命令类似 CRCX 命令，**Subtract** 命令类似 DLCX 命令。

H.248 与 MGCP 的一个区别在于，H.248 是以连接为中心的，而 MGCP 是以端点为中心的。

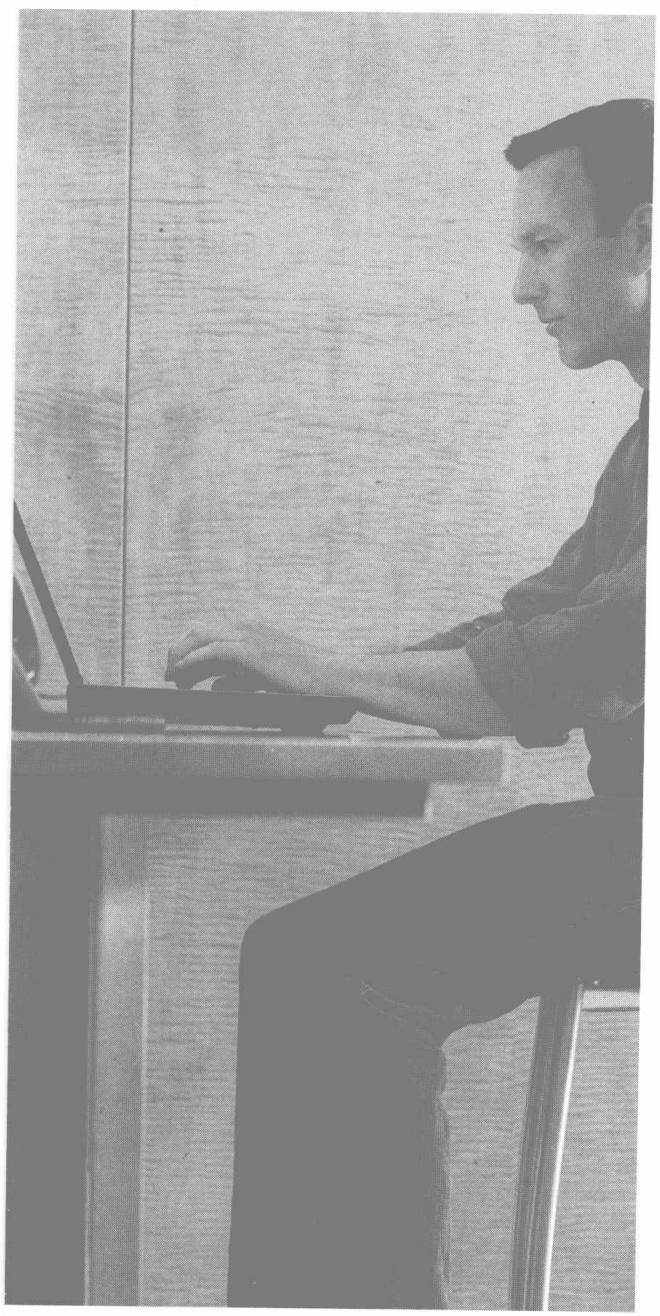
13.7 总结

MGCP 对于一个基于媒体和信令功能分离的分布式体系结构来讲，是一个至关重要的组件，在从已有网络的迁移过程中将继续扮演一个重要的角色，这个迁移是从所有组件都

在一个单一平台到组件分布的网络的迁移。

因为这是一个新的且快速发展的行业，MGCP 和 H.248 不得不随着时间发展以适应行业使用。

MGCP 就核心来讲，非常简单。在随后的多年里，它将继续在分组语音网络上扮演至关重要的角色。



本章讨论网络架构框架和设计模型，包含以下主题：

- 14.1 思科分组电话
- 14.2 分组语音网络概览
- 14.3 PGW2200 体系结构与操作
- 14.4 PGW2200 实施
- 14.5 PSTN 在 IP 上的信令
- 14.6 PSTN-IP 互联的变迁
- 14.7 会话边界控制器（SBC）
- 14.8 总结

第14章

PSTN 与 VoIP 互联

在前面的各章节中，我们介绍了公共交换电话网络（Public Switched Telephone Network，PSTN）和分组语音（Voice over IP，VoIP）技术，两者是彼此孤立的。在实际的承载网络中，VoIP 和 PSTN 技术是共存的，而且在以后的几年中也将如此。本章介绍 VoIP 与 PSTN 的各种互联。

14.1 思科分组电话

思科分组电话（Cisco Packet Telephony）体系结构是建立在 3 个逻辑平台上的： 连接控制、呼叫控制和服务。每个平台代表语音服务的一个不同功能面，平台之间可以通过很好定义的开放接口交互作用。这 3 个平台被层次组织，连接控制在最底层，呼叫控制在连接控制之上，服务层在最上面。图 14-1 展示了思科分组电话体系结构的功能组成。

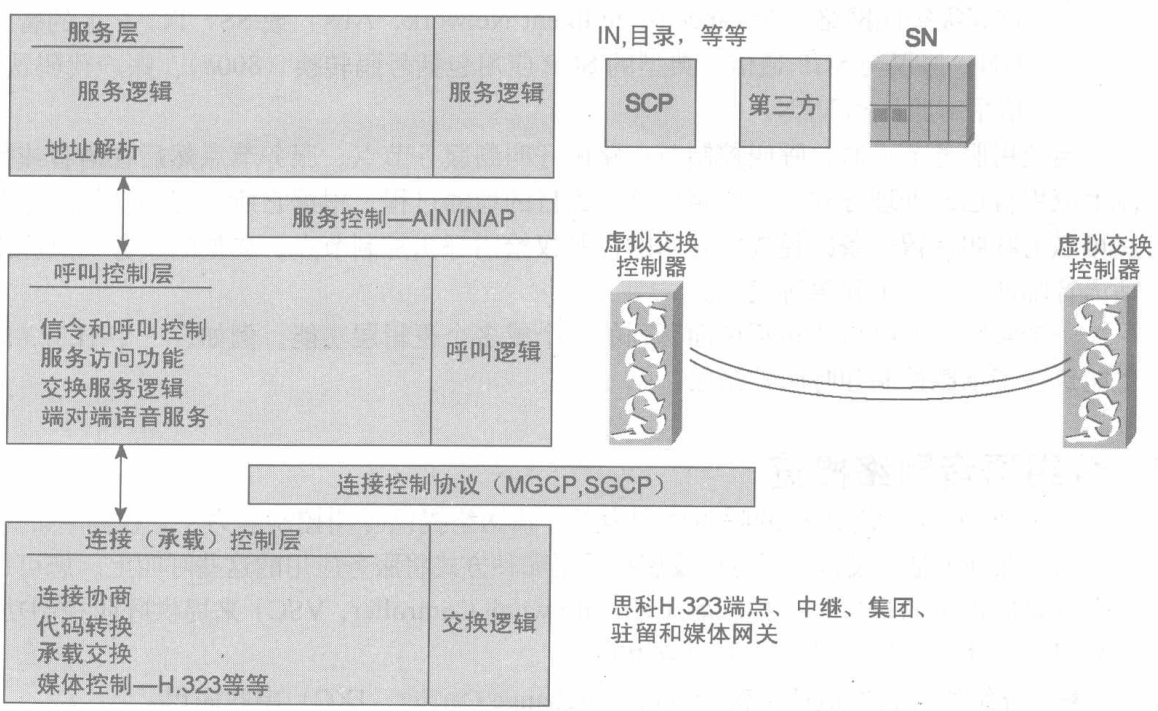


图 14-1 思科分组电话体系结构

在思科分组电话体系结构中，软交换机提供如下呼叫控制平台功能。

- 连接或承载控制层处理在分组网络上建立，维护和拆除语音路径的必要功能。思科 AS5850、MGX8850、2600、3600 和 3810 是执行承载控制功能的媒体网关（MG）的例子。承载控制层与呼叫控制层使用行业标准控制协议，如媒体网关控制协议（Media Gateway Control Protocol，MGCP）通信。
- 呼叫控制层由信号、过程和在分组网络上路由语音和数据呼叫的必要功能组成。本层的功能与在时分多路复用（Time-Division Multiplexing，TDM）交换机的呼叫处理逻辑中的功能类似。典型的呼叫控制功能包括 7 号信令系统（Signaling System 7，SS7）协议处理、数字分析和操作、路由选择、发现，基于交换的功能（switch-based features）和与外部逻辑程序的接口。

  呼叫控制层与连接控制层使用 MGCP、SIP、H.323 和 MEGACO 通信。使用这个接口的目的是使连接控制和呼叫控制分离，呼叫控制层对于语音传输是独立的（并且未知的）。这样不管是第 3 层（IP）还是第 2 层（ATM/FR）都可以使用一样的呼叫控制层。

  呼叫控制层还可以与服务层通信以提供灵活的、增强的服务。虽然有许多厂商专有的和扩展的版本存在，这个接口通常是一个基于标准的运行于 SS7 事务能力应用部分（Transaction Capabilities Application Part，TCAP）上的智能网络（IN）协议。
- 服务层包含为提供增强非交换驻留服务的必要逻辑。您可以使用服务控制点（Service Control Points，SCP）或服务节点来完成本层功能。当您使用 SCP 时，控制层通过高级智能网络（Advanced Intelligent Network，AIN）或 SS7 TCAP 上的智能网（IN）协议与 SCP 通信。典型的 SCP 应用包括号码转换（800#）、账户代码认证、信用卡验证和 VPN。

当使用服务节点时，呼叫控制节点路由呼叫到服务节点。服务节点然后在语音或数据流上应用自己的处理方式，完成路由呼叫到目的地的过程。根据它所采用的功能，服务节点可以为呼叫保留一条路径或将呼叫的控制权给回呼叫控制节点。典型的服务节点应用包括语音邮件，借记卡和语音拨号。

一个实际的产品可能包括前面所列的一个或多个逻辑层功能。例如，一个 H.323 网关可能包含了承载控制和呼叫控制层。

14.2 分组语音网络概览

一个像 PGW2200 那样的呼叫代理为下一代网络提供呼叫控制能力。它控制窄带 TDM 流量怎样在分组基础设施上运行以及您将采用哪种方式将服务应用的这些呼叫上。您可以使用在许多应用中的虚拟交换控制器（Virtual Switch Controller，VSC）来提供呼叫控制功能。在分组语音体系结构中可以使用的应用有：

- 分组语音长途电话运营商（Interexchange Carrier，IXC）串联应用；
- 分组语音本地电话运营商（Local Exchange Carrier，LEC）第 4 类应用；

- 端点客户端多媒体应用；
- 企业语音的网上和网下服务；
- 在电缆设施上的 VoIP 本地/终端局办公室应用。

图 14-2 显示了一个基本的分组语音应用并列出了各个部件及他们之间是怎样交互的。

14.2.1 网络元素

本节介绍在图 14-2 中的各个网络元素，它们是：

- 呼叫代理（PGW2200）；
- MG；
- 服务控制点（Service Control Point，SCP）；
- 服务节点（Service node）；
- 电缆数据转发器（Cable headend）；
- 驻留网关（Residential gateway）；
- H.323/SIP 端点/客户端。

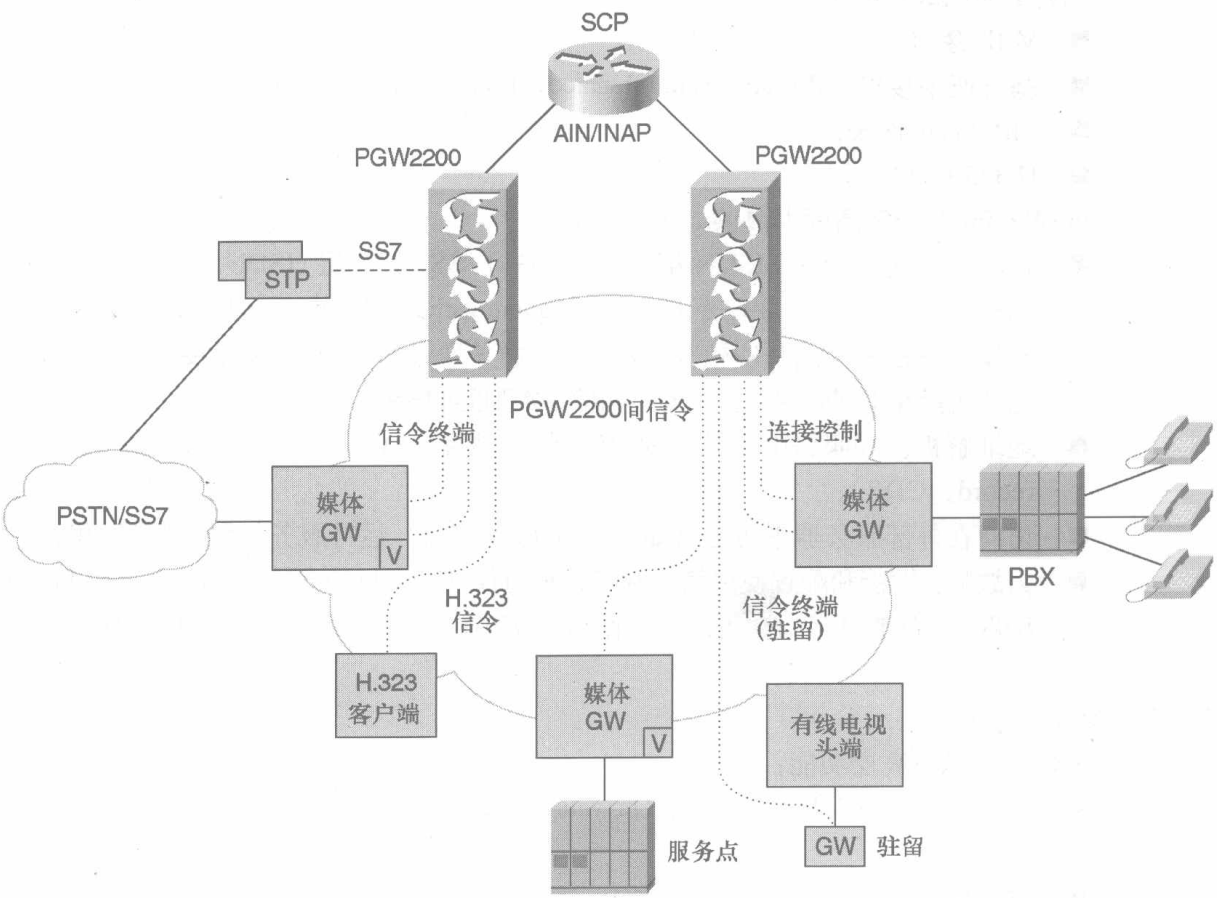


图 14-2 分组语音网络体系结构

14.2.2 呼叫代理：PGW2200

思科 PGW2200 是一个运营商级的呼叫代理，它在 PSTN 网关基础架构中执行信令和呼叫控制任务（如数字分析、路由选择、电路选择等）。利用庞大的 SS7 信令协议库和对行业控制协议的支持，包括 MGCP、H.323 和 SIP，思科 PGW2200 为服务供应商提供了在 PSTN 和分组网络上无缝地路由语音和数据能力。

思科 PGW2200 包含如下 3 种必需元素：

- 思科媒体网关控制器（MGC）软件，运行在 SUN 的通用计算平台上；
- 思科信令链路终端（Signaling Link Terminals，SLT）；
- 思科 PGW2200 元素 IP 互联的局域网交换机。

以下是可选元素。

- H.323 信令接口（Signaling Interface，HSI）附属处理器。
- 管理产品，包括思科 MGC 节点管理器（ Cisco MGC Node Manager）、思科语音服务提供工具（Cisco Voice Services Provisioning Tool，VSPT）和思科计费和测量服务器（Cisco Billing and Measurement Server，BAMS）。

思科 PGW2200 允许以下 PSTN 网关。

- VoIP 穿越。
- 基群速率接口（Primary Rate Interface，PRI）修饰和多路复用负载。
- SIP PSTN 网关。
- H.323 PSTN 网关。

PGW2200 在一定高度上提供如下核心能力。

- 呼叫信号处理，包括 ISDN 第 3 层（Q.931）、SS7 第 4 层（ISDN 用户部分（ISUP））、H.323、多频/信道关联信令（Multi-Frequency/channel-associated signaling，MF/CAS）和发向驻留网关的呼叫信令（这些驻留网关通过宽带或 DSL 连接）用户室内设备。它还包括在不同呼叫分支上的不同信令类型间的转换。
- 地址解析、呼叫路由选择、资源管理、连接控制和产生呼叫细节记录（call detail record，CDR）。
- 访问在外部服务器平台上（如 SCP 或服务节点）运行服务的服务访问功能。
- 为故障、性能和配置使用简单网络管理协议（Simple Network Management Protocol，SNMP）的管理接口。可以被用作基于 WEB 的配置工具和元素管理系统。

14.2.3 媒体网关

MG 执行以下高层功能：

- 来自 PSTN 或专用小交换机（private branch exchanges，PBX）的物理 T1/E1 TDM 设备终结；
- 在电路交换网络上的回声消除；
- 平衡抖动缓冲区；

- 语音活动探测（Voice Activity Detection，VAD），例如静音抑制（silence suppression）和再生舒适噪声（comfort noise regeneration）；
- 实用 ITU 建议如 G.711，G.723.1 和 G.729 的语音压缩；
- 音调产生、产生拨号、忙、回铃和阻塞音调；
- 双音多频（Dual-Tone MultiFrequency，DTMF）传输，允许为包含支持 DTMF 探测/传输编码器的语音邮件应用使用音频（touch tones）；
- 需要时的μ-law 和 A-law 的代码转换；
- 支持服务质量（Quality of Service，QoS）。

14.2.4 服务控制点

SCP 为服务逻辑提供运行平台。它负责处理事务请求和返回一个响应。在语音世界的一个典型的事务请求是号码转换。

这个服务的例子有 800（免费电话）服务和本地号码可携带（Local Number Portability，LNP）。例如，一个在 SCP 上运行的免费电话有一个允许最终用户控制怎样路由来电的成熟逻辑。您可以将免费电话的路由选择基于拨叫的号码、每天的时间、每周的日期、起始的地理位置，甚至于在给定的时间时一个终结自动呼叫分发（terminating Automatic Call Distribution，ACD）的繁忙程度。客户或服务供应商可以拥有 SCP。

14.2.5 缆线数据转发器

通用带宽路由器（Universal Broadband Router）是一个电缆调制解调器终端系统（cable modem termination system，CMTS）和使用射频（Radio Frequency，RF）线卡的思科 7200 系列路由器的集成。

通用带宽路由器是一个单一的综合解决方案，提供了 CMTS 功能，终结电缆数据传输服务接口规范（Data-over-Cable Service Interface Specifications，DOCSIS）协议的能力，以及执行所有必须的数据路由功能的能力。这个组件的实例还包括一个数字用户线接入多路复用器（digital subscriber line access multiplexer，DSLAM）。

14.2.6 驻留网关

驻留网关是一个语音/数据 CPE 设备，它提供老式普通电话（plain old telephone service（POTS））的两到四口能力。这个设备运行 DOCSIS 协议以提供在混合光纤同轴电缆（Hybrid Fiber-Coaxial，HFC）线缆到 CMTS 上的分组数据和电话服务。这个组件的另一个例子是 DSL 调制解调器。

14.2.7 H.323/SIP 端点/客户端

H.323/SIP 客户端代表了广泛的语音/多媒体应用。它们在 IP 网络之内，由使用 SIP 或 H.323 作为它们的 VoIP 协议的端点运行。除了语音外，这些端点可能还有多媒体能力。

14.2.8 网络接口

PGW2200 呼叫代理的 4 个主要网络接口有：信令终结、呼叫代理间信令、连接控制和服务控制，如图 14-3 所示。

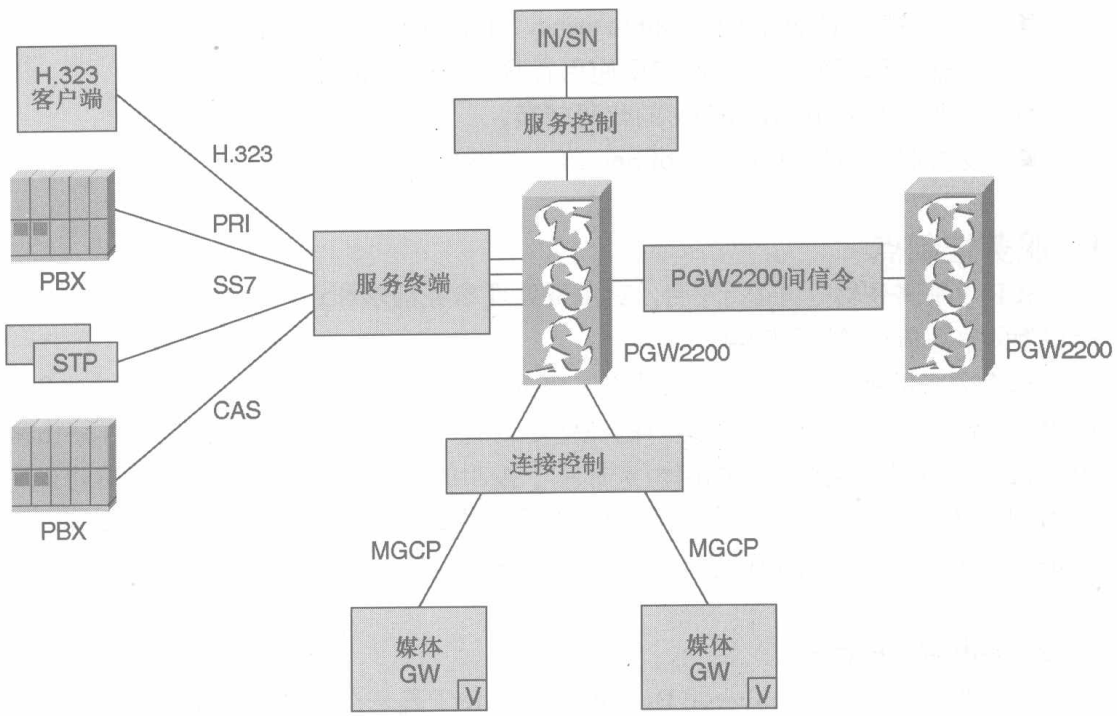


图 14-3 网络接口

每个 PGW2200 网络接口将在下面讨论。

14.2.9 信令终结

信令终结能力允许 PGW2200 在多种信令（如 SS7、PRI 和 H.323 等）间进行仲裁。

1. SS7 链路

有几种机制可以在 PGW2200 上面终结 SS7。

- 非关联信令（Nonassociated signaling）（A-links，A 链路）——这些信令在 v.35 或 T1/E1 物理接口上直接终结。为了提高可靠性，您可以选择配置一些信令链路终端（Signaling Link Terminals，SLT）来处理 SS7 的低层。SLT 是通过使用在运行 PGW2200 应用的 SUN 服务器前的思科 2600 系列路由器部署的。
- 全关联信令（Fully associated signaling）（F-links，F 链路）——这些传输承载流量，终结在分组网关。分组网关负责执行消息传输部分（Message Transfer Parts，MTPs）1 和 2，封装 MTP 第 3 层（MTP L3）协议数据单元，并发送它们到 PGW2200 以进

行 MTP L3 和 ISDN 用户部分（ISUP）处理。在 PGW2200 与分组网关的传输使用可靠用户数据报协议（RUDP），RUDP 是在用户数据报协议（UDP）上的一个瘦可靠层。

2. PRI 链路

PRI 链路承载一个 D 信道，直接终结在语音网关。语音网关外围行第 1 层（L1）和第 2 层（L2）——PRI 接口的较低层（Q.921），第 3 层（L3;Q.931）被封装在 RUDP 包中发送到 PGW2200 进行呼叫处理。

3. CAS 链路

CAS 链路直接终结在语音网关。网关外围处理低层 CAS 协议，如线路和地址信令。使用一个 CAS 应用编程接口（API）来将 IP 上的呼叫处理事件回送给 PGW2200 处理。

4. H.323

PGW2200 处理除 Q.931 请求外的来自 H.323 客户端的呼叫前注册、许可和状态（RAS）请求。这个信令终结遵从 H.323 标准中的分发过程。换句话说，PGW2200 有 H.225 RAS/Q.931 能力，但它不具有 H.323 关守功能。

14.2.10 PGW2200 间信令

PGW2200 到 PGW2200 协议通过在多个 PGW2200 平台分布控制扩展了网络规模。一个被称为增强 ISUP（E-ISUP）的 ISUP 修改协议在 PGW2200 之间互换控制信息，这些 PGW2200 运行在使用 RUDP 的 IP 网络上。因为不需要 MTP 信息，所以不需要传送。

E-ISUP 消息也承载在 ISUP 一般数字信息元素中的会话描述协议（Session Description Protocol，SDP）元素，PGW2200 使用这些元素描述 MGCP 中的连接。

注释：行业已经在转向使用 SIP 或被称为 SIP-T 的 SIP 的另一个版本来作为 MGC 间的通信协议。

14.2.11 连接控制：MGCP

可以使用 MGCP，一个在 IP 网络上建立连接的开放机制，来在分组网络建立一个端对端的语音连接。MGCP 是一个基于 TCP/UDP 的事务协议，它允许操作物理或逻辑端点间的连接。该连接使用如 IP 地址、编码器等属性描述。MGCP 管理呼叫建立请求和连接到网关（如电缆或 DSL 调制解调器）的电话的连接。

14.2.12 服务控制

可以从下面两种途径访问服务。

- IN（AIN/INAP/convergence sublayer-1 [CS-1]）平台如 SCP 接口，最初在基于标准的 AIN/INAP 接口上在 SS7 网络上传输，将来将迁移到基于 IP 的传输。

- 服务节点服务（例如电话卡和语音邮件）最初连接在 TDM PRI 接口上。将来，服务节点平台将转移到 IP 网络上，以避免不必要的 TDM/IP 互联。

图 14-4 显示了使用 PGW2200 互联。

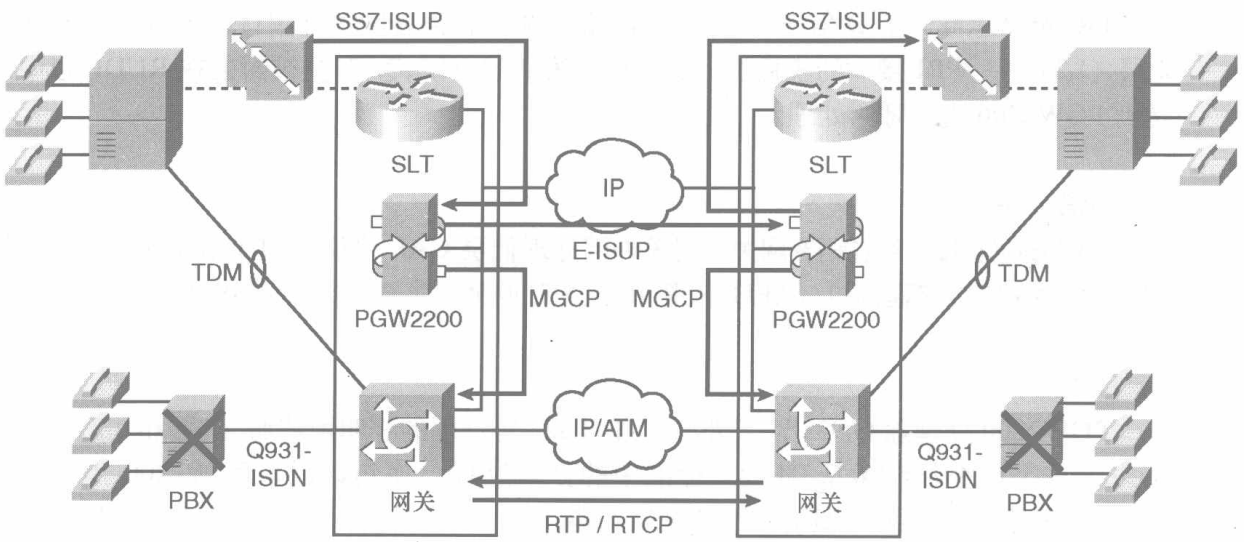


图 14-4 呼叫代理转换

14.3 PGW2200 体系结构与操作

图 14-5 描述了思科 PGW2200 平台的主要功能模块

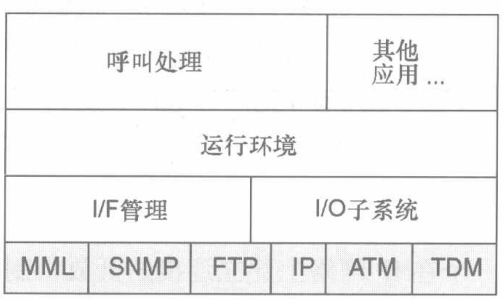


图 14-5 PGW2200 的功能组件

思科 PGW2200 是一个开放式平台，为第 3 方应用开发提供了一系列强大的应用/协议构建工具和 API。

下面介绍这些工具。

- 应用工具箱——PGW2200 应用工具箱允许用户定制协议和他们的互联功能。这个工具箱也提供了强有力的语言工具和 API 来在 PGW2200 平台上开发状态、事件驱动应用。

- 转换分析器——转换分析器跟踪互联引擎，产生输出报告。报告中的信息包括消息输入、转换和输出。
- 仿真器——仿真器允许用户建立消息集并在一个仿真互联引擎上运行来诊断应用或协议错误。细节报告包括消息输入、转换和输出。

14.3.1 PGW2200 支持的协议

PGW2200 的一个重要功能是它的体系结构支持多种访问和网络协议。新协议和现有协议的更新正陆续的添加到库中。表 14-1 提供了一个它支持的完整协议列表。

表 14-1 SC 支持的协议

ANSI ISUP（SS7）	ITU Q.931 PRI	比利时 Q761 ISUP
BTNUP	ETSI ISUP V2	阿尔卡特 4400 PRI
BTNUP NRC	ETSI Q.SIG	NI-2（Bell-1268）
中国 TUP	ITU Q.767 ISUP	NI-2+（Bell-1268-C3）
DNPSS	法国 ISUP	波兰 ISUP
荷兰 ISUP	德国 ISUP	芬兰 Q761 ISUP
ETSI PRI	中国香港 Q761 ISUP	澳大利亚 Q761 ISUP

14.3.2 运行环境

运行环境（Execution Environment，XE）为在信令主机上运行的应用程序提供通用服务。XE 的主要目的如下：

- 为应用程序提供一个灵活、稳定和一致的基础架构；
- 允许运行在同一平台的新应用可以更容易地与现有应用集成；
- 使应用开发者为建立一个新应用所做的工作最少；
- 为操作系统服务提供一个简单的接口，这样第 3 方可以开发能在 PGW2200 过程上运行的定制应用。

XE 提供的服务如下。

- 过程管理——允许 XE 管理过程。这包括依次启动、停止和监控过程的健康情况。过程管理也被用来在最少影响服务的情况下完成向一个新版本过程的切换。
- 警告——允许过程注册、设置和清除警告。警告的设置和清除被自动地汇报给请求这项服务的过程。您可以使用这项功能向附加的管理接口汇报警告，使过程可以实施必要的恢复操作。
- 日志——允许过程向共享的日志文件中基于设备和日志要求的等级来记录日志消息。
- 统计——允许过程更新用于汇报和警告的共享计数器。基于共享计数器的警告代表平台上的所有过程自动产生。测量报告定期自动产生。
- 命令管理——允许过程互换命令和响应。这项服务也被用于为协议转换引擎提供一

个统一接口，或者为通过一个管理界面（如跨路径人机语言（TransPath Man-Machine Language，MML））控制和监管 XE 平台的外部系统控制提供一个统一的接口。

- 配置管理——允许在配置数据发生改变时，通知一个过程。它在平台上的所有过程间匹配动态配置。
- 访问控制——保证平台服务只提供给被授权的过程。
- 过程 shell——为过程使用 XE 提供的服务提供一个接口框架。它使用一个统一的过程分派机制，支持过程间通信（IPC）、计时器、信号和一组为应用开发的基础类。
- IPC——允许平台上的过程互换消息。
- 信号处理——为与操作系统的信号联系提供接口。

14.3.3 北美编号计划

PGW 可以处理使用串联或 IXC 网络的北美编码计划（North American Numbering Plan，NANP）。

- 带有或不带有 10XXX 或 101XXXX 的接线员服务（0−，0+，00）被路由到一个北美号码（NXX-XXXX 或 NPA-NXX-XXXX）或一个国际号码（CC+NN）。
- 带有或不带有 10XXX 或 101XXXX 的普通电话被路由到一个北美号码（NXX-XXXX 或 NPA-NXX-XXXX）或一个国际号码（CC+NN）。
- 支持使用#作为号码结束指示。这就允许呼叫者通过按#键提示交换机停止等待另一个数字，开始处理拨叫号码。
- 将电话转给运营商（10XXX+# 或 101XXXX+#）。
- 支持 950-XXXX 格式号码（都属于地址种类（NOA））。
- NXX-XXXX 向 NPA-NXX-XXXX 号码的转换。
- 支持 IN 触发器（免费，优惠服务和 LNP）。

1．路由分析

PGW2200 呼叫路由选择将一个呼叫从入口 MG 路由到合适的出口 MG。呼叫路由选择并不是指在网上路由包，这由连接控制层负责。如果有同一 PGW2200 控制起始和终结 MG，呼叫路由选择在 PWG2200 内一步完成。

如果由另一个 PGW2200 控制出口网关，那么起始和终结 PGW2200 都将参与呼叫路由选择。起始 PGW2200 分析呼叫请求消息，如 SS7 起始地址消息（initial address message，IAM），选择一个路由到达出口网关或服务出口网关的终结 PGW2200。路由分析将从下面几个中做出选择：

- 一个连接在所选中继组的“跳跃”或出口网关；
- 决定出口网关的终结 PGW2200 的 IP 地址；
- 驻留网关；
- 在入口网关的回到起始网络的一个“发卡”（hair pinned）连接。

如果需要两个 PGW2200，起始 PGW2200 使用 E-ISUP 与终结 PGW2200 进行通信、建立呼叫。图 14-6 显示了主、次和拥挤溢出选择，由路由选择过程决定。

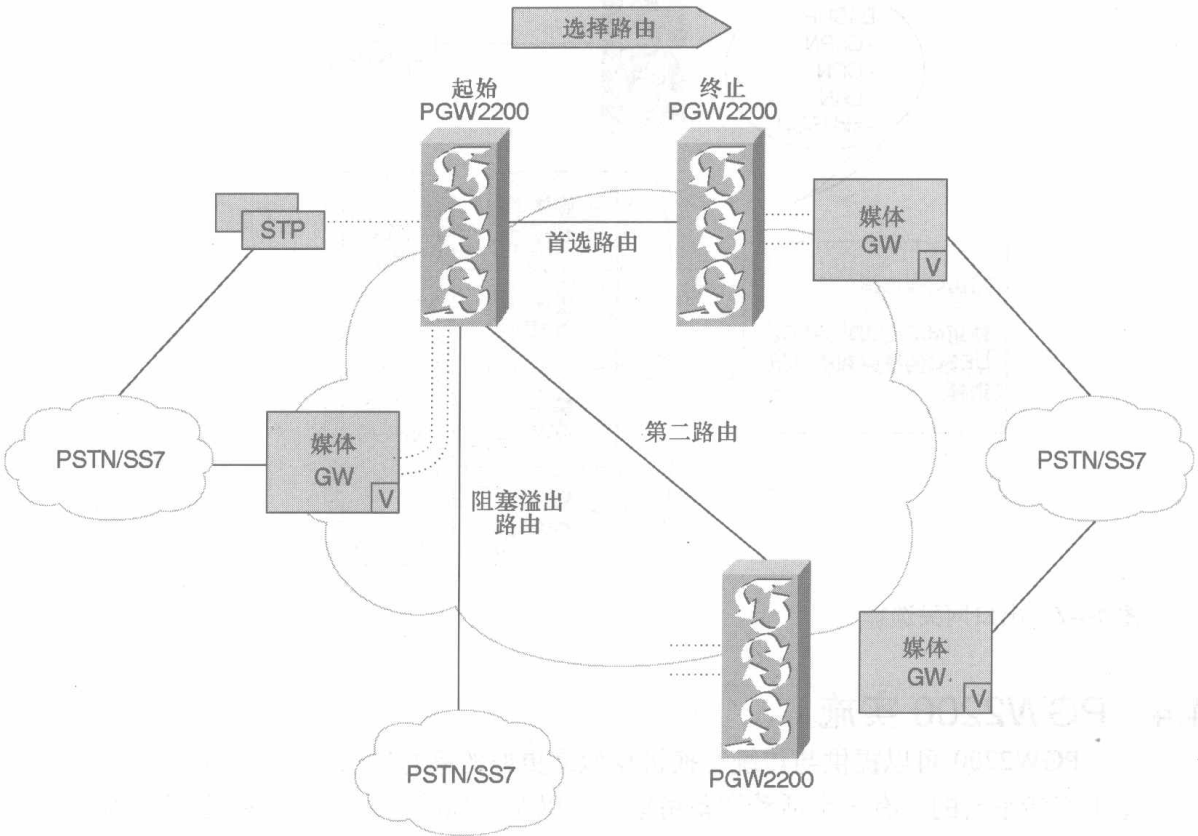


图 14-6 路由选择过程

2. 数字分析

PGW2200 在 A 或 B 号码上执行数字分析和屏蔽功能。拨叫的或转换过来的号码需要选择路径，终结 PGW2200 网关负责选择出口网关。首先，通过数字分析选择“首选的”跳跃网关（如中继组）；然后通过对终结网关资源的忙/闲处理，在 TDM 接口上选择外出电路，激发相应的到终结 PSTN 交换机的信令过程（ISUP IAM）。图 14-7 显示了出口网关选择过程。

3. 阻塞重路由

PGW2200 包含连接到由 PGW2200 控制的出口网关的中继状态（忙/空闲状态表），当因为内部资源错误，出口网关不能完成一个呼叫时，一个明确的指示通过 MGCP 否定确认被送回 PGW2200。PGW2200 可以选择另一条路由来尝试呼叫。如果有两个 PGW2200 参与，终结 PGW2200 使用 E-ISUP（拥挤释放（REL）消息）通知起始 PGW2200；如果有另一条路由存在，则尝试重新路由。

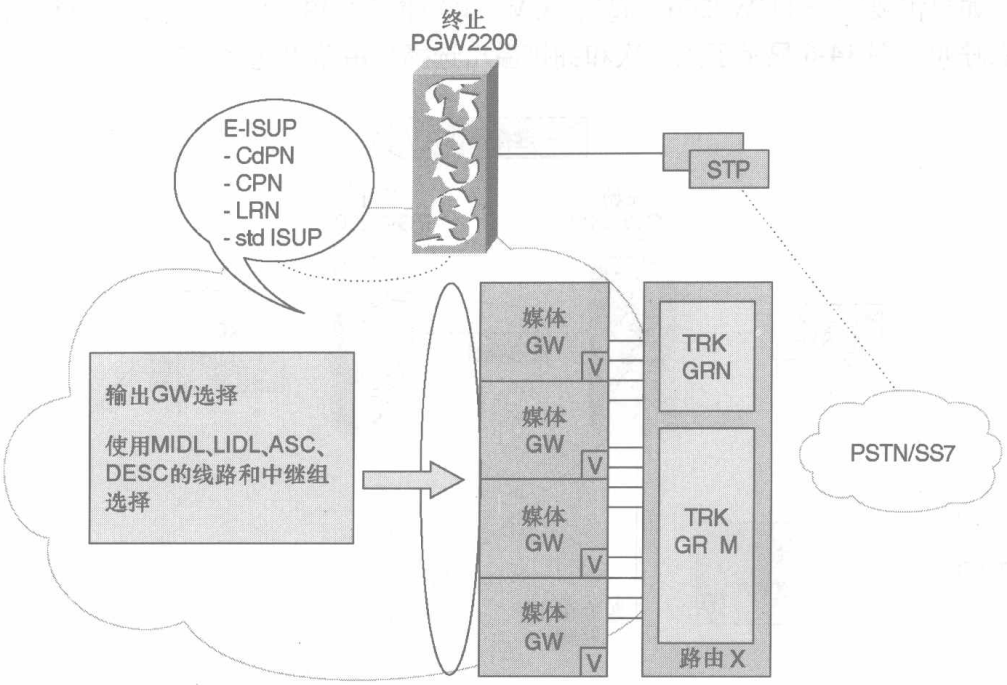


图 14-7 出口网关选择

14.4 PGW2200 实施

PGW2200 可以提供与传统交换机相似或更好的高有效性。如图 14-8 所示的系统，是基于容错平台的，有一个活动和备用单元，以及单独的终结 SS7 流量的 SLT 集组成。

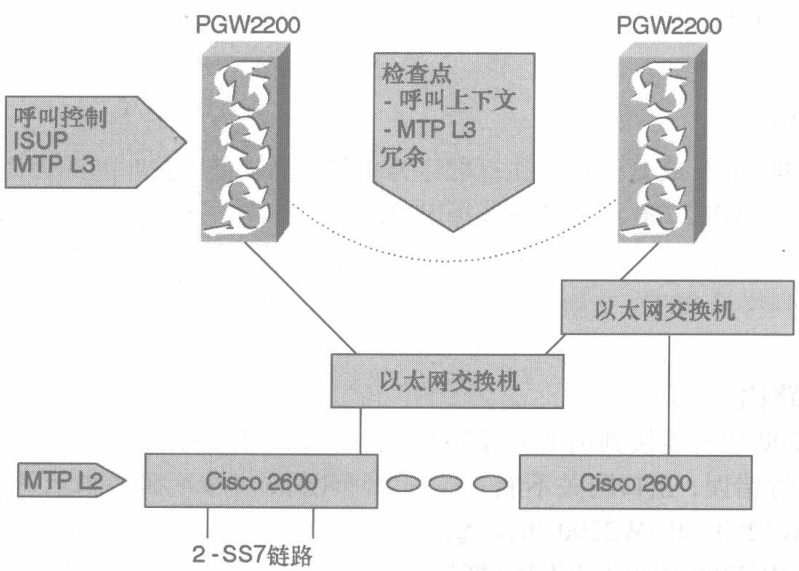


图 14-8 PGW2200 实施

呼叫状态信息由活动单元拷贝到备用单元。这个过程也被称作 check-pointing（检查点）用来保证在由活动向备用 PGW2200 切换时，呼叫不会丢失。SLT 终结 MTP L2 流量，并发送 MTP L3 信息到活动单元。通过初步分析显示，组合系统的有效性是每年 0.9999985 或 0.782min 的故障时间。

为最大化 PGW2200 的容错能力，MTP L2 流量终结在单独的硬件平台上，MTP L3 流量通过双以太网交换机传输。这个级别的冗余，使活动和备用系统可以共享 SS7 链路和 LAN/WAN。

思科 2600 是支持 SLT 功能的第一台路由器。您可以在不打扰 SS7 网络的前提下，移除、增加和服务一个 SLT。思科 2600 SLT 支持两个 SS7 链路端口，每个端口可以处理 2 个 erlang 的累积流量。（一个 erlang 是呼叫数乘以呼叫的平均处理时间（average handle time，AHT）除以 3600）。SLT 通过标准以太网连接，通过 RUDP 在 LAN/WAN 上传送 MTP L3 消息给 PGW2200。

14.4.1 应用检查点

检查点（Check-pointing）发生在 PGW2200 之间，保证正在进行的呼叫在故障发生时，可以很好保持。呼叫处理引擎在呼叫建立和呼叫释放阶段，发送检查点事件到本地检查点过程。

在呼叫建立阶段，第一个检查点事件在资源管理器向包网关确认物理电路资源时产生。这个事件包括允许远程资源管理器更新被分配电路逻辑状态的足够信息。在呼叫被应答时，产生第二个检查点。保存在远程资源管理器的事件数据仅包括远程呼叫处理引擎维持呼叫直到被释放的足够信息。因此，在故障发生时，呼叫仍然进行，但不再支持服务功能。

在呼叫释放阶段，当资源管理器从分组网关收到呼叫释放请求相关联的确认时，产生一个检查点。

检查点还可以应用在协议监管消息上，以防在呼叫建立和释放之间承载链路的逻辑状态发生改变。这些消息包括：

- 阻止和取消阻止消息和命令；
- 电路重置消息和命令。

14.4.2 MGC 节点管理器

MGC 节点管理器（MGC Node Manager，MNM）是为端对端网络管理提供 SS7 服务的基于电信管理网（Telecommunication Management Network，TMN）的解决方案。MNM 提供思科网络元素的统一管理，这样就使虚交换系统可以按照一个管理元素来处理。MNM 的负责管理组成虚交换系统语音和信令部分的物理网络元素包括：

- PGW2200；
- 语音编码单元；
- 虚交换域内的语音流量；

- 交换机内和虚交换机间的信令流量；
- 在 PSTN 或 PBX 与 PGW2200 虚交换网络之间的信令流量。

MNM 的职责不包括：

- 外部语音网络元素（电话交换机）；
- 提供语音或信令到虚交换机的数据或 TDM 网络；
- 去往或来自 PSTN 和虚交换机域的信令流量。

MNM 域包含如图 14-9 所示的信令和语音流量元素。

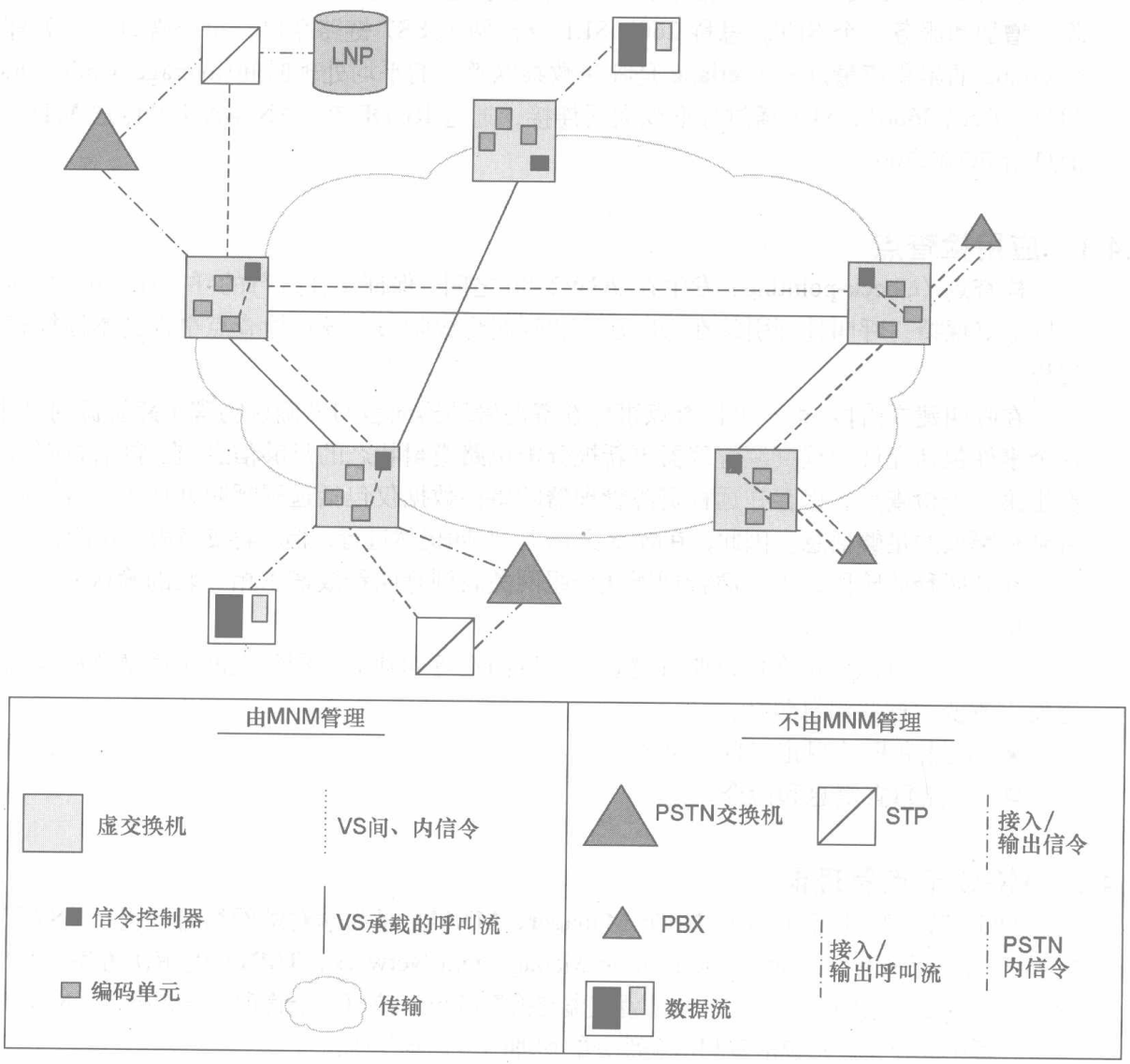


图 14-9 MGC 节点管理器域

在这个域中，MNM 为故障、配置、性能和安全管理提供传统的 FCAPS 功能。记账服务由 PGW2200 产生的 CDR 提供。MNM 直接管理 PGW2200 和通过 SNMP 与其他接口来与外部元素管理系统（ Element Management Systems，EMS）合作。

外部 EMS 实际管理组成虚交换机其他部分的 NE。MNM 的域内故障、配置、性能和安全功能如下。

- 故障管理——以图形的方式表示在域中定义的警告消息和控制等级。也支持尖端的事件相关、问题隔离和状态信息技术，在组件级汇总。故障管理浏览器支持在警告层次和网络拓扑图上的点击导航，以识别简单元素。
- 配置管理——提供图形和文本方式的工具，以及支持域中所有 NE 的用户图形界面。MNM 与思科元素管理器集成或接口可以形成健壮的客户已部署产品的管理线。您可以通过网络拓扑图的点击界面来访问各元素的管理工具。
- 性能管理——MNM 从相关元素那里收集流量和性能数据并将它们归档在中心数据库。MNM 为浏览收集的数据提供基本的报告和图形应用。为离线和客户自定义的报告和分析工具提供了开放数据库结构化查询语言（Structured Query Language，SQL）接口。
- 安全管理——MNM 为各种管理功能和 NE 提供支持基于角色的访问。您可以定义用户组来简化用户管理，支持标准的用户名和口令功能。标准 SNMP 社区字符串安全管理 SNMP 访问。

MNM 也将警告传播到上层网络管理层提供 SNMP、TL1 和 SQL（非实时的）接口。除了这些接口，MNM 为还可以提供操作支持系统（Operations Support System，OSS）网络管理系统提供基于标准的接口，包括公共管理信息协议（Common Management Information Protocol/Q2，CMIP/Q2）和通用对象请求经纪体系结构（Common Object Request Broker Architecture，CORBA）。MNM 提供图形用户界面使用户可以直接控制 EMS。

MNM 体系结构考虑到了以下的几个主要 SP 需求。

- 从 TMN 规范中分离配置、记账、性能、故障和安全。
- 提供一个层次的管理体系结构，该结构具备与已有的网络管理系统和将来的系统集成的能力。
- 使用一个递归的层次的网络对象模型。
- 采用 CORBA 作为战略指导接口。
- 提供流通过供应。
- 管理网络流量性能。
- 关联警告。
- 提供基于标准的接口。

14.4.3 记账

PGW2200 处理的每个呼叫都有详细的信息记录。生成的记录是广泛而详细的，每个

CDR 包括如下信息：

- 主叫被叫号码；
- 应答时间，断开时间和呼叫完成代码；
- 路由信息，起始中继组和成员，终结中继组和成员；
- ISUP 信息；
- ISDN 服务信息和扩展；
- 记账代码和指针。

与这些信息一起，还有超过 80 个的附加元素可以在灵活的用户自定义格式中定义 CDR 配置。如果没有有效的数据或使用元素，TransPath 消息定义语言（Message Definition Language，MDL）可以在标有“custom”的特殊数组中为未来 CDR 需求产生单独字段。这些数组被置为 IRU 和 ANSI 标准。

CDR 被写入一个循环文件中，该文件在用户定义的周期或到达一定大小时关闭。您可以查阅被关闭的文件，或如果需要的话，将它们发送到下流处理系统，如自动消息记账（Automatic Messaging Accounting，AMA）或计费仲裁设备。您还可以产生呼叫内的 CDR 信息，这些信息可以记录一个呼叫中最多 8 个事件点的数据。

14.5 PSTN 在 IP 上的信令

在软交换机的体系结构中，运营商向基于 IP 的基础设施转移的需求中包括在 IP 网络上传输 PSTN 信令的过渡技术。

VoIP 信令协议如 SIP 和 H.323 是假设 IP 是传输介质二定义的。已有的 PSTN 信令协议如 SS7 和 ISDN 有着 IP 还不能满足的严格的性能和功能上的要求。

为了满足这些要求，需要附加在 IP 上面的协议层。IETF 的 SIGTRAN 工作组定义了一组封装方式和端到端协议机制来支持 PSTN 功能和性能的需求。SIGTRAN 体系结构包含如下内容。

- 每个 PSTN 信令协议（如 MTP3、ISDN 等）的改写层以支持特定 PSTN 协议所期望的从它的下层协议得到的服务。这些改写层的例子有：MTP3-用户改写层（M3UA），ISDN Q.921-用户改写层（IUA）等。
- 流控制传输协议（Stream Control Transmission Protocol，SCTP）是支持一个信令传输通用功能的传输协议。

为满足运营商级网络的可靠性和性能需求，SIGTRAN 规范引入了应用服务器（Application Server，AS）和应用服务器过程（Application Server Process，ASP）概念。

AS 被定义为一个服务特定应用实力的逻辑实体。AS 的一个例子是一个处理 Q.931 的 MGC。就实际经验来讲，一个 AS 是在 SG 上的一个或多个相关 ASP 的有序列表（如主要的、次要的和再次的）。

ASP 是一个 AS 的过程实例。ASP 的例子有主要和备份的 MGC 实例。以下各节描述 SIGTRAN 工作组定义的 SCTP 和 IUA。

14.5.1 SCTP

TCP 是在 IP 网络上最常使用的可靠传输协议。但是，它因为如下原因不适合承载 PSTN 信令。

- 线头阻塞现象（Head of line blocking occurs）。当一个包丢失时，将造成应用中后续包的延迟。
- 面向流的 TCP 不适应面向消息的 PSTN 信令。消息定界和直接“PUSH”操作对响应时间等有一定的要求。
- TCP 没有对多宿主主机的支持。PSTN 需要这项功能为高有效性应用提供服务。
- TCP 相对来讲易受到 DoS 攻击。

因为 TCP 的局限性，SIGTRAN 工作组在 RFC 2960.SCTP 中定义了有如下功能的 SCTP。

- 消息定位。
- 用户数据公认的无差错非重复传输。
- 用户消息的顺序传输（带有可选的非顺序传输）以避免线头阻塞现象（Head-of-line blocking occurs）。
- 捎带（Piggybacking），通过其多个用户的消息可以捆绑在一个 SCTP 包中传送。这就大大提高了效率。
- 引入了端点间联合概念以支持多宿主（Multihoming）。在启动的时候，每个 SCTP 端点可以为对方提供一个传输地址的列表（多个 IP 地址），表明它可以通过这些地址被联系到和从这些地址发起包。SCTP 联合将数据传输扩展到所有可能的源/目的地址和，且对于用户应用来讲是透明的。
- 可以反抗一些 DoS 攻击。

14.5.2 IUA

如前所述，在软交换体系结构中，媒体功能于呼叫控制功能是分离的。媒体功能是 MG 的一部分，呼叫控制功能是 MGC 或呼叫代理的一部分。

ISDN，作为带内信令机制，与媒体一起到达 MG。ISDN 信令消息需要被传送到 MGC（也被称为回程（backhaul））以开始呼叫过程。在 IUA 规范中，GW 终结 Q.921 并 backhauls Q.931 到 MGC。

RFC 3057 定义了 IUA，如图 14-10 所示。

IUA 为上一层提供如下服务。

- 支持 Q.921/Q.931 的分界原语传输 在回程（backhaul）场景中，Q.921/Q.931 分界原语被曝光。IUA 层需要支持这个分界线的所有原语以成功回程 Q.931。
- 支持 SG 和 MGC 上的层管理模块之间的通信。帮助层管理模块管理 SG 和 MGC 间的 SCTP 联合。例如，层管理模块可以指导 IUA 层为对方 IUA 节点建立一个 SCTP 联合。
- 支持在信令网关（SG）和 MGC 间的活动联合。SG 上的 IUA 层维护所有 ASP 的有效性和活动/非活动状态。它管理 SCTP 联合和 SG 与 ASP 之间的流量。

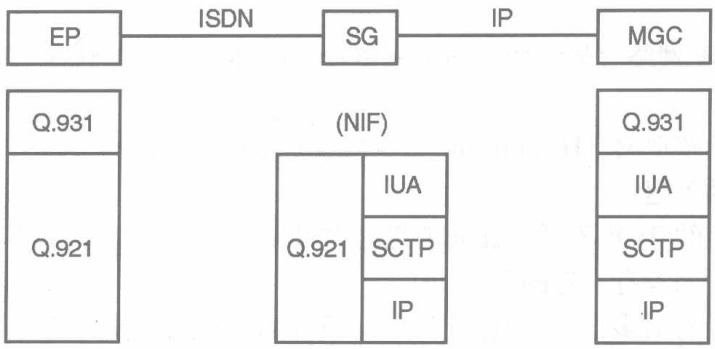


图 14-10 ISDN 用户改写层体系结构

14.6 PSTN-IP 互联的变迁

因为注意力由得到基本的 VoIP 网络转到互联不同的 VoIP 岛，服务提供商和运营商面临着通过支持不同协议和网络元素以建立网络的新的挑战。如果再考虑到计费和安全问题，则问题会变得更加复杂。曾经被一些 VoIP 提供商预见到的与拓扑无关的互联多个 IP 域趋势，现在是随处可见的功能。表 14-2 显示了驱动 VoIP 向前发展的动力中最普遍的趋势。

表 14-2 新 VoIP 互联趋势

以前	现在和将来
统一带宽收费	按使用量计费
尽力	服务等级协议（SLA）和 QoS
开发网络连接	拓扑无关
TDM 互联	IP 互联，信令协作
相同编码器互连	代码转换
以信任为前提	安全
相同 IP 域	互联 IP 域
合法截取（LI）能力—可选	需要合法截取（LI）

当 VoIP 运营商和提供商连接其他运营商时，他们使用如下方式中的一种互联。

- 与运营商合作，并拉动数据连接。
- 增加向本地运营商租用的数据连接容量。
- 使用一个网关或一个中间盒子（intermediary box）连接到一个在营运营商的 TDM 网络。

对于运营商来讲，最经济的解决方案是第 3 种。这种方案还可以并允许使用对接（peering）作为一个重要工具联结不同的地域的 H.323 或 SIP 网络。

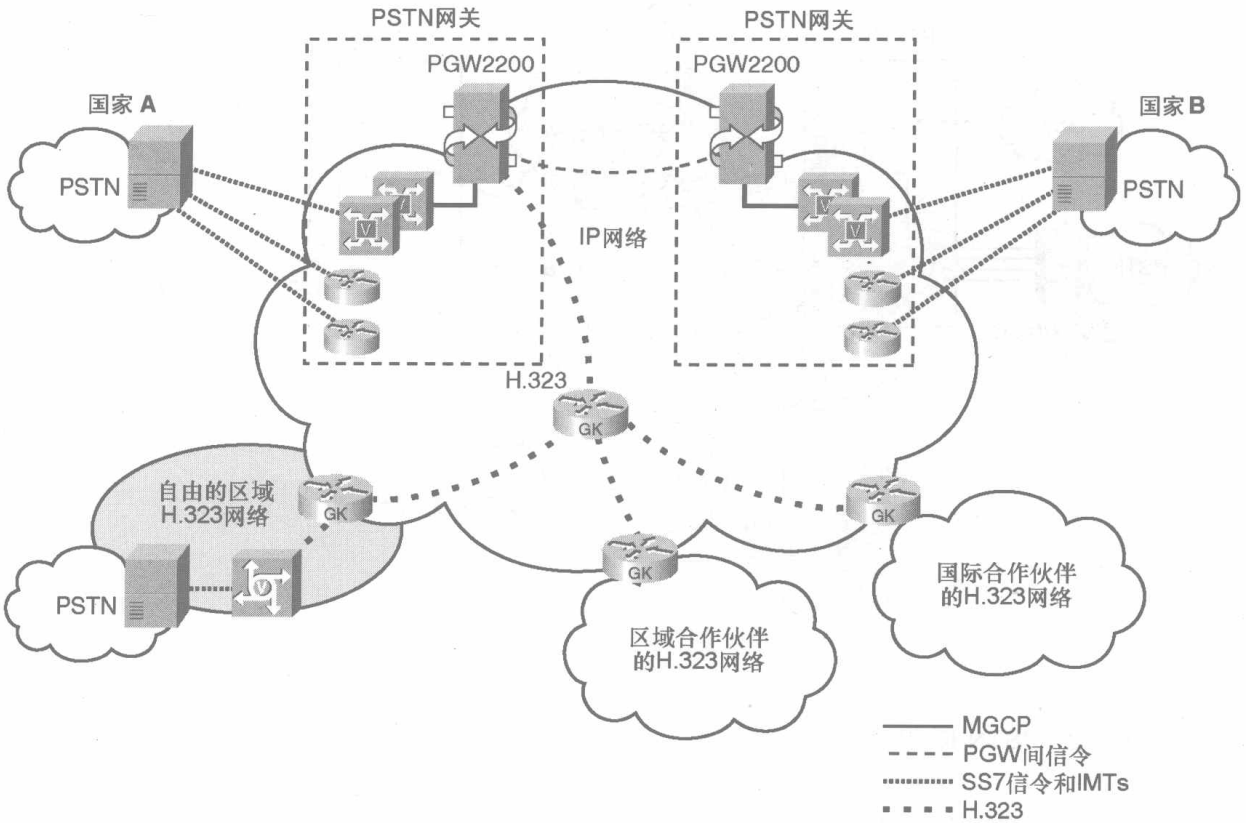


图 14-11 PSTN-IP 组网

使用这种中间盒子的方式允许如下应用和服务：

- 国际转换；
- 国际或国内的 H.323 VoIP 流量终结；
- H.323 VoIP 接线员的网络互联。

这种方式使用如下技术/设备：

- 为在中心和远程区域控制呼叫和收集 CDR 信息的 PGW2200；
- 运营商级的 VoIP 网关带 VISM-PR 卡的 MGX8230、AS5300 语音网关和 AS5000 通用网关。

SIP 正在被用于许多 VoIP 网络中，图 14-12 给出了一幅更真实的由 PGW2200 处理的 SIP 和 H.323 网络终结图。

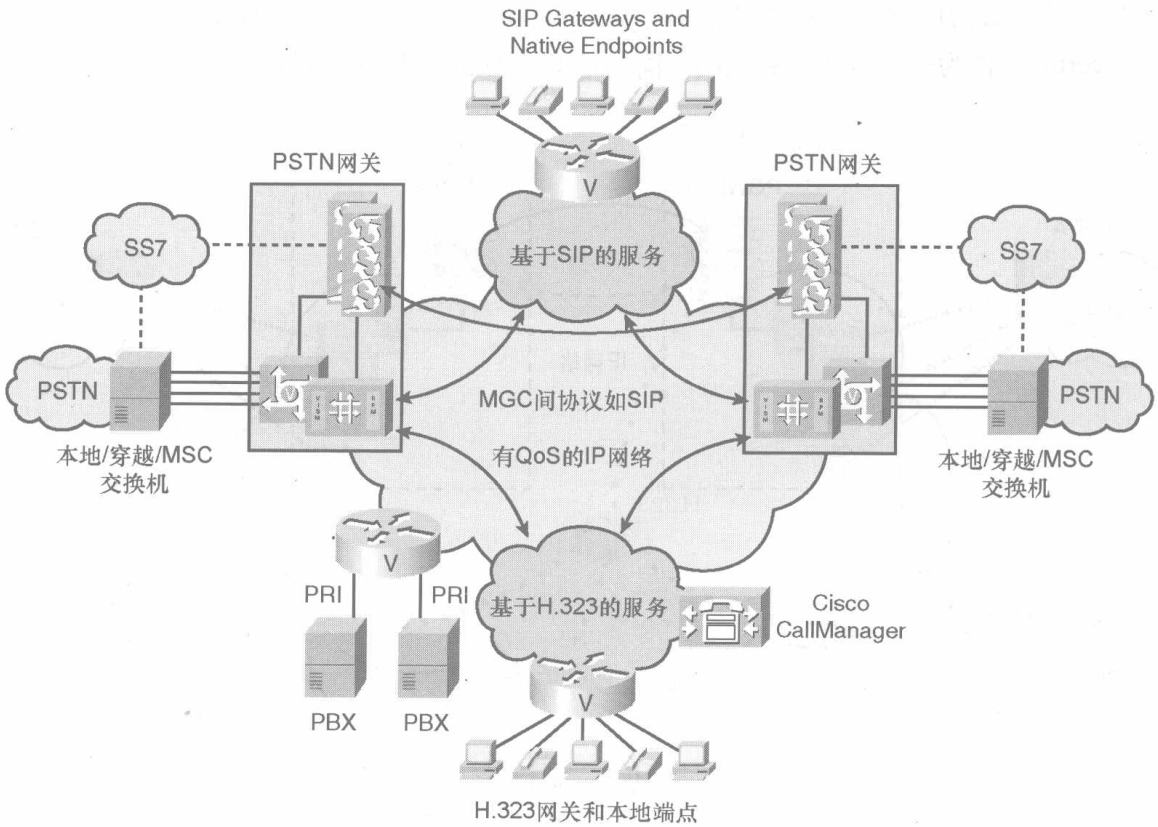


图 14-12 PSTN-IP 组网

14.7 会话边界控制器（SBC）

VoIP 两个或多个网络间连通和对接正在成为较大部署的一项重要任务。

通过部署，服务供应商和企业可以直接互联 VoIP 网络而不需要通过 PSTN 来做中转。供应商还可以因为更低的费率和税率、较少的管理等进一步减少运行费用。因此，对于一些厂商提出会话边界控制器（Session Border Controller，SBC）的概念是合乎逻辑的，SBC 不仅可以作为一个有用的对等点，还可以解决 VoIP 流量岛间的协同问题。虽然有 SBC 在网络中可以做或应该做什么的多种解释，SBC 最初的想法应该具有如下互联功能（InterWorking Functions，IWF）（参见图 14-13）：

- IP 地址和端口转换；
- 计费和 CDR 标准化；
- VoIP 安全（NAT 穿越、LI、认证等）；
- 媒体互联以解决编码器、DTMF-RELAY 和 FAX 问题；
- QoS 和带宽管理；
- 丰富的信令和应用互联；
- 与 VoIP 协议一致。

图 14-13 SBC 组件

连接不同网络时所遇到的协同问题可以通过这些 IWF 解决。

在下列各类设备中可以找到 SBC 功能：

- 单独 SBC；
- 路由选择设备；
- 媒体网关；
- 安全设备。

许多厂商已经实施了一个或多个这些功能，并在网络对接中有效使用 SBC。在过去的两年中，独立设备非常流行，并通过提供各种级别的能吸引服务供应商和 VoIP 运营商的功能而占领了市场，创造了可观的利润。

SBC 给予了互联分割网络时供应商所需要的附加值。图 14-14 列出了 SBC 在各种互联场景中是怎样帮助 SP 的。

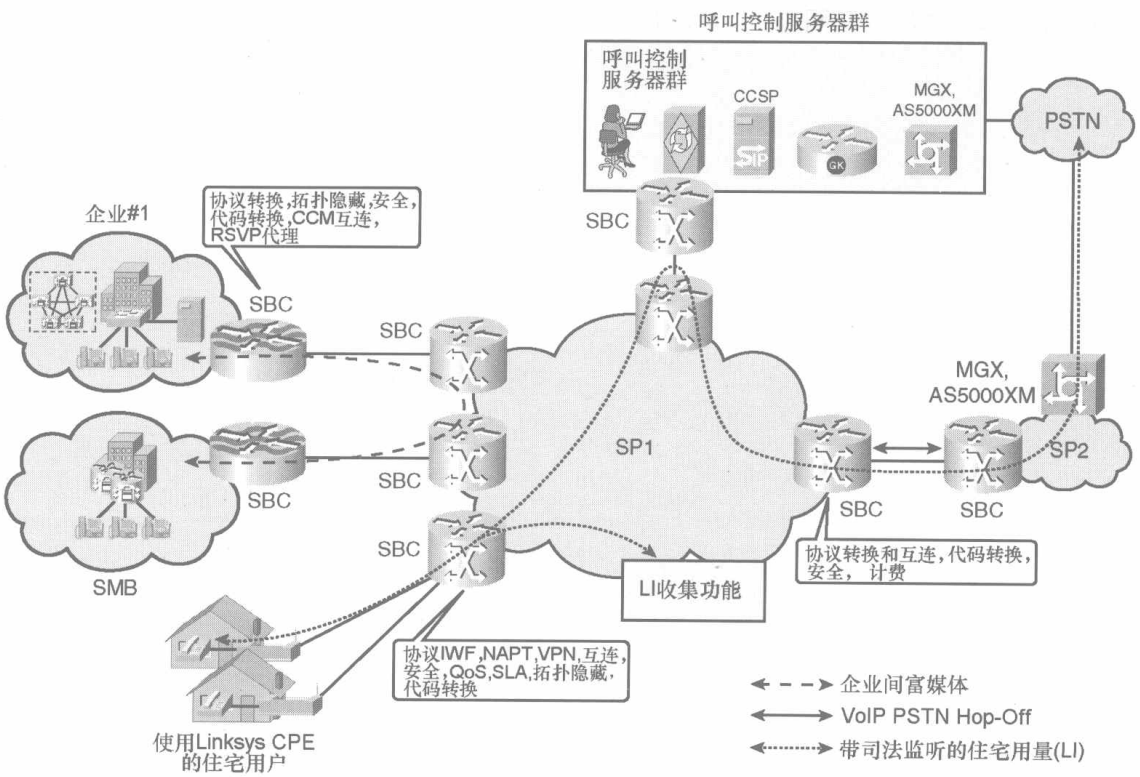


图 14-14 VoIP 网络互联

图中的 SP1 被连接到另一个 SP 网络，SP2，并与另一个 VoIP 岛——以他们拥有的企业命名（企业 1），一些中小企业（some Small and Medium Business，SMB）或者是另一个供应商的住宅 VoIP 网络。这些单独的网络也许有他们自己的 VoIP 管理系统，但因为来自他们的所有流量都须通过大的供应商 SP1，在每个对等点上的 SBC 提供标准化和最需要的协同能力。

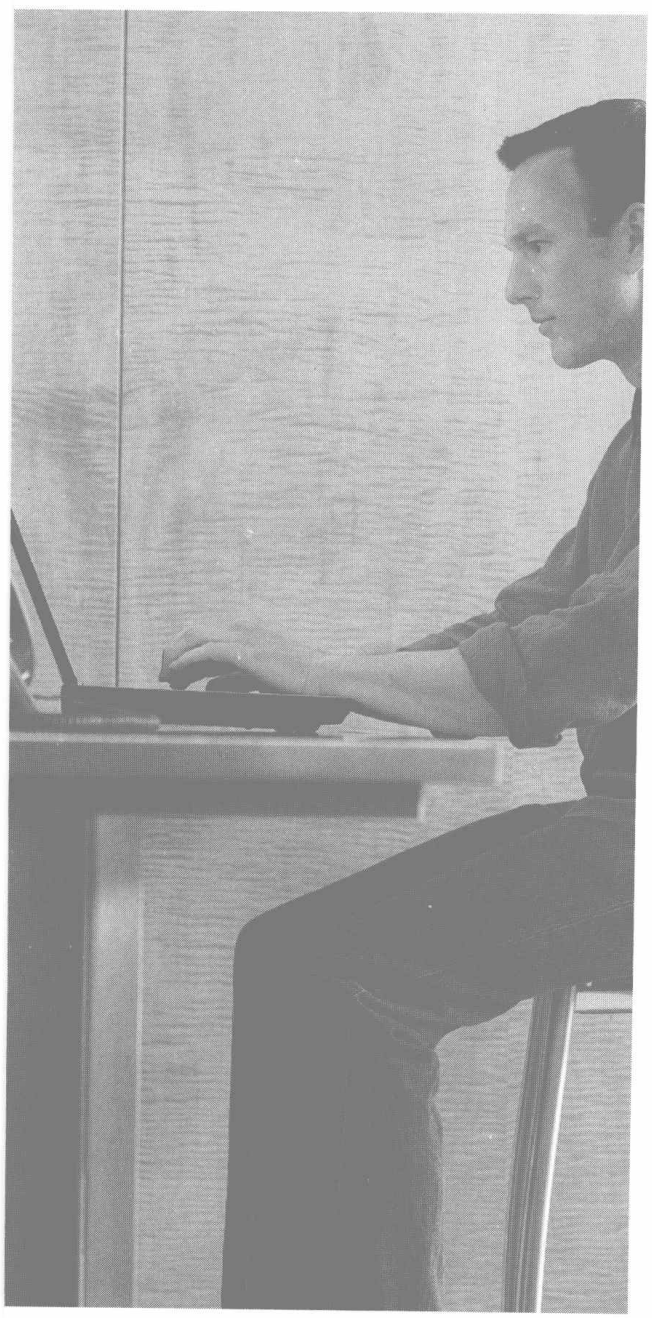
14.8 总结

思科分组电话体系结构允许您分离应用、呼叫控制和承载层。在这个体系结构中，呼叫代理是一个主要的组件，因为它帮助连接应用到承载层。PGW2200 呼叫代理的一个思科实例。如这个体系结构所暗示的一样，PGW 允许在每个组件中（应用、呼叫控制和承载层），客户可以使用不同的厂商设备。

这就允许您将思科 MG 与其他厂商的呼叫代理和 PGW2200 一起使用。

为一个 SP 客户建立一个呼叫代理，需要注意许多细节。路由选择、呼叫控制和可靠性只是在建立这部分思科分组电话体系结构时所要涉及的有限几个问题。

除了呼叫代理，SBC 还提供了 VoIP 网络中的另一个有价值的组件。目前，SIP、H.323 和 MGCP 是 VoIP 网络承载大量 VoIP 流量时的明确选择。SBC 作为两个 VoIP 供应商之间的连接设备存在。每个供应商使用一个 SBC 可以连接多个对等网络，这样就可以帮助供应商减少大量部署 VoIP 网络的运行费用。



本章讨论网络架构框架和设计模型，包含以下主题：

- 15.1 服务供应商的困难选择
- 15.2 服务供应商的应用和利益
- 15.3 服务供应商 VoIP 部署：Vonage
- 15.4 服务供应商案例分析：预付费电话卡
- 15.5 会话边界控制：增值
- 15.6 VoIP 对接网络：服务供应商的最佳选择
- 15.7 服务供应商 VoIP 和消费者固网移动融合
- 15.8 总结

第15章

服务供应商 VoIP 应用和服务

第 14 章向我们描述了企业是怎样更有效地使用 VoIP 来管理他们业务中的通信的。企业清楚地看到了 VoIP 是保持竞争力和提高他们客户服务的有力工具。服务供应商应该为主要市场提供良好定义的服务，有合理价位和满足服务质量的连贯服务。

2004 年年底，In-State（一个电信研究机构）估计在美国有大概 130 万的宽带 IP 链路正在使用，并在 2005 年年底增加到 390 万。全球的大多数供应商公认 IP 已经赢得了网络的传输层，IP 网络上的语音与数据、视频和增值服务是电信市场上的主要驱动力。In-StaT 报告，VoIP 服务消费的全球市场已经来到。2005 年全球的 VoIP 的订户是 1 600 万，2009 年将超过到 5 500 万。

服务供应商根据他们所运行的网络，传统上分为有线、电信和宽带无线公司。随着 VoIP 和高级服务的提供，出现了一些新的使用传统供应商的网络设施提供增值服务的供应商。这些供应商包括 AOL、Vonage、Yahoo! Broadband、Skype 和 Google。通过使用 IP 作为通用的传输基础，这些公司正在为 VoIP 的市场份额而竞争。在他们提供的服务中存在着重叠，然而，对于供应商来讲最首要的问题是解决怎样在控制运行费用的同时驱动利润的增长。

15.1 服务供应商的困难选择

今天供应商面临的一个主要难题是随着越来越多的 VoIP 上的服务和新技术如会话发起协议（Session Initiation Protocol，SIP）的出现，服务供应商正在逐步减少用以服务的呼叫控制层。网络的核心呼叫控制曾经是最重要的一部分，电话听筒/端点则不那么重要。当客户要求自己掌握更多的智能时，用户室内设备（Consumer Premise Equipment，CPE）和家庭办公（Small Office Home Office，SOHO）设备将提供这些智能。

位于供应商网络内的呼叫控制交换机目前在地理上是分布的，并且许同不同的服务器在共享所有功能。目前的技术减少了 VoIP 业务所面临的障碍，而且服务供应商也发现语音市场已经很难产生利润，市场正在向 VoIP 应用转移。服务供应商所面临的困境基于 VoIP 应用可以赢得利润。

这不仅仅是谁能提供 VoIP 的问题。这是关于在考虑利润的情况下可以提供哪些服务的问题，在将享有的和新的在 IP 主干上运行的通信服务集成后，他们所扮演的角色又是什么。很清楚的是，客户和中小企业正在越来越多地需要新的业务和应用。目前的趋势已经将越来越多地控制交到了最终用户手中，并集成了现在有效的多种通信方式（语音、电子邮件、

即时消息（IM）、会议、短消息服务（SMS）、多媒体消息服务（MMS），等等）。

供应商没有其他选择，只能与多个厂商合作，保证 VoIP 网络在保证利润空间的前提下可以穿越许多服务器。

SP 需要如下：

- 运营商级的可靠性和可量测性；
- 对所用订户的一个共享平台——多种租赁；
- 减少运营费用。

用户需要如下：

- 强壮的特色功能；
- 多媒体，可预测拨号、语音识别、自动呼叫分配（Automatic Call Distribution，ACD）、记录等；
- 拥有自己的虚呼叫中心/家庭网络的所有管理权限；
- 快速部署；
- 与 CPE 的强有力集成。

本章回顾了 SP 正在试图开发新应用以满足用户需要和帮助他们达到预定目标的方法。本章还覆盖了一些新出现的超出了 VoIP 和基于 IP 包的服务的技术和部署，这些技术和部署综合了不同市场需求，不管是有线、宽带还是简单数据网络。供应商们经常将这些融合了数据、语音和视频服务捆绑业务模式称为“3 重服务（triple play）”，这样他们就能从每个用户那里得到的最优收入，加速企业发展。他们现在可以将这些分组业务整合到一个单一的交换传输网络。如果他们将无线移动添加到 3 重服务中，将变为 4 重服务。

15.2 服务供应商的应用和利益

当企业开始考虑将他们的语音和数据网络整合到一个多服务网络时，他们最先考虑的应用是 toll-bypass（收费旁路）。Tol bypass（收费旁路）允许企业在他们现有的 TCP/IP 网络上发送公司内部的语音和传真呼叫。通过将这些公司内部的流量从 PSTN 上移走而使用他们数据网络的剩余带宽又不丧失功能，企业立即就可以节省电话费用。

企业可以立即看到使用 toll bypass（收费旁路）所带来的效益。实际上，一些企业有大量的办公室内呼叫——包括国内和国际的——在 3 到 6 个月就可以看到投资回报。

在企业越来越适应 VoIP 和 toll-bypass 时，下一个他们通常考虑的应用是应用在客户服务、交互工程组和远程培训。下面是一些可以应用在这些领域应用的例子。

- Microsoft Communicator—— Communicator 2005 是一个集成的通信客户端，使用户可以实时通信。作为 Microsoft Office Live Communications Server（LCS）2005 的建议客户端，Communicator 2005 集成了 Microsoft Office 系统应用和企业电话设施。

  微软还推出了 Microsoft Office Communicator Mobile。基于 Microsoft Office Communicator 2005 微机客户端的用户界面，Communicator Mobile 是作为一个统

一的通信客户端投放市场的。它通过特别为移动应用而设计的总和应用和企业级的实时通信工具，为信息工作者提供了一个以移动为首选的合作体验。这个客户端不仅仅是语音，还集成了安全增强的 IM、列席信息和集成的 VoIP 电话。

- Microsoft NetMeeting——在 Microsoft LCS 发布之前，NetMeeting 是公司最通用的 VoIP 客户端。它在一些网络中仍在使用，提供传统电话服务与共享应用和基于 H.323 的视频会议的集成。这个综合服务允许在不同位置的雇员可以很容易地在一个项目上合作，通过整合设备和数据/语音网络减少了费用。
- 思科 IP 电话——它看起来和感觉上都跟传统电话一样，但是增加了 IP 连接功能。IP 电话与更新的基于 IP 的 PBX 一起工作，不再依赖于一个已有 PBX 的功能，比如拨号音。这些 IP PBX 不仅提供和传统 PBX 一样的功能（拨号音、语音信箱和会议），它们还利用了所有基于 IP 的服务以提供新功能。因为它是一个 IP 设备，IP 电话不仅可以使用 VoIP 服务，还可以使用任何在网络上有效的基于 IP 的多种服务应用。
- 基于 PC 的软电话——思科基于 PC 的 SoftPhone（软电话）将电话机功能通过一个图形用户界面扩展到 PC，该界面提供与电话听筒一样的功能，并集成了与其他多服务应用如 web 浏览，微软网络会议（Microsoft Netmeeting）和基于轻目录访问协议（Lightweight Directory Access Protocol，LDAP）的目录服务。它还不需要附加设备（如听筒），因为在标准 PC 上通常都配备了 SoftPhone（软电话）所需的听筒和麦克风。
- 集成 VoIP 的 IM 客户端——随着 VoIP 软电话的使用，需要将 IM、基于列席的应用和语音传输集成在一起。GoogleTalk、Skype、Yahoo!、Gizmo 和 AOL 只是一些最近完成这项功能并引起注意的最新软件应用。虽然目前的解决方案与他们自己的 IM 应用紧密相连，但是趋势是 IM 无关的解决方案。（例如，Google IM 应用应该可以与 Yahoo 或 Skype 等交谈。）

所有目前讨论的服务都被认为是第一代的基于标准的服务。正如 TCP/IP 数据服务高速发展一样，第二代 VoIP 和基于 TCP/IP 的集成数据/语音服务也在快速发展。这些服务将被与日俱增的企业竞争，开放标准应用编程接口（API），各种协议如 H.323、LDAP、电话应用编程接口（Telephone Application Programming Interface，TAPI）、Java 电话 API（Java Telephony API，JTAPI），Linux 和企业网络经理和程序员的创造性所驱动。

15.3 服务供应商 VoIP 部署：Vonage

Vonage 是一个位于新泽西的公司，它领导了基于宽带连接的电话学。它拥有 120 万的客户，是在因特网上发送呼叫的最大的国内供应商。它清楚地示范了大范围的真实世界的 VoIP 部署。从 http://www.vonage.com 上摘自的一些有关它的事实如下。

- Vonage 通过 5%的 VoIP 服务的市场份额领导了行业发展。
- 2006 年 3 月，Vonage 宣布已经完成在 150 万条活动线路上完成了超过 18 亿的 VoIP 呼叫。

- 在超过 150 个的全球市场上，它已经建立了超过 200 个的活动费用中心。
- 它目前有超过 5 000 个零售点。
- Vonage 与本地交换通信公司（Local Exchange Carriers，LEC））和多系统运营公司（Multiple Service Operator，MSO）ISP 有分发协议。

Vonage 作为服务供应商部署 VoIP，以有竞争力的费率为住宅和商业客户提供语音服务，从而挑战了已有的供应商。Vonage 使用 SIP 作为呼叫建立和服务的会话协议，不管客户的因特网是什么接入方式，他们可能是：

- DSL；
- Wi-Fi；
- 电缆调制解调器；
- 电力线宽带（Broadband over PowerLine，BPL）。

对于与 PSTN 的互联，基于 SIP 的 Vonage VoIP 应用采用两种方式： IP 到 IP 和 IP 到 PSTN。这就允许了与 PSTN 的向后兼容，并允许与下一代无线或对等 IP 网络通信。

Vonage 在全球的成功部署已经将对 VoIP 的理解由增值技术转到了增值服务。最近，许多其他公司，如 SS8、Lingo、B2、Packet8 和 RocketVoip 也成功部署了 VoIP 业务。

VoIP 运营优势

商业和住宅用户电话市场的需求变化要求在 TDM 设施中通过使用有效的方法、最少的延迟和低的管理运行费用，来添加新的电信功能和能力。VoIP 提供如下的优势允许供应商们在现有的 TDM 设施上重新考虑投资。

- 设备使用和呼叫控制容量是动态的。
- 呼叫控制逻辑和智能的分布更透明和易于管理。
- 信令资源的使用是非常有效的。
- 可以在运行中进行设备供应和更新，比在 PSTN 中类似的工作要简单。
- 随着时间的发展，很容易添加新的功能和应用。
- 因为网络资源在应用中共享，所以远程管理和第三方控制比较容易。

15.4 服务供应商案例分析：预付费电话卡

下面的案例分析讨论了一项允许服务供应商操作预付费电话卡的业务。通过这项新业务，服务供应商可以使用他们现有的 VoIP 网络、网关和关守。他们还可以通过提供捆绑服务来区别其他 VoIP 服务供应商并实现更大的利润，从而可以投资扩展网络活减少 toll-bypass 费用。一个 BOWIE.net 的简单案例随后讲述。同样的服务架构也可以使用在 Vonage 部署上。

BOWIE.net 多服务网络

BOWIE.net 是一个地方因特网服务供应商，在美国的东南部和东海岸有 60 个电话接入

点（Points Of Presence，POP）。它有一个配备思科设备的网络，目前提供住宅和商务因特网接入，可管理的网络服务和主机托管。

BOWIE.net 在所有的 60 个 POP 上提供 4¢/min 的长途 VoIP 服务。这项服务主要是针对它已有的商务和住宅客户的，这些客户通常是临时工作者，需要短时期的使用。大多数没有带月计划的手机或者没有一个长途电话服务提供商。

当在住宅电话市场的竞争变得剧烈时，BOWIE.net 寻求能区分自己与其他竞争者的方法。它采取的一个主动措施就是利用它的 VoIP 网络提供预付费电话卡业务。

因为 BOWIE.net 已经为 VoIP 访问采用了 AS5400s，所以它很自然地适合使用添加在思科 IOS 系统软件中的预付费电话卡功能。这项业务不仅为 BOWIE.net 带来了预付费收入，而且因为它的灵活性，它还可以有很优惠的价格。

BOWIE.net 与思科系统以及它的合作伙伴一起实施预付费电话卡业务。其中，合作伙伴负责提供计费应用，思科负责提供 VoIP 基础架构。因为这些合作关系，BOWIE.net 可以判定哪个合作伙伴可以满足它的技术和费用需求，不需要关心解决方案会不配合。

BOWIE.net 通过很少的配置修改和设备添加，部署了预付费电话卡解决方案。它所必须添加的最大的设备是计费应用服务器。BOWIE.net 在实施中使用了它已有的 RADIUS 认证服务器和简易文件传输协议（Trivial File Transfer Protocol，TFTP）服务器。它使用 RADIUS 服务器做账户号码和口令的认证，TFTP 服务器存储用户进入服务时的提示。另外，它还使用现有的 AS5400s 和 3640s 作为 VoIP 网关和 SIP 代理服务器。在试运行时，它甚至使用 H.323 关守并提供了一个基于 H.323 的 VoIP 网络。

图 15-1 显示了简化了的 BOWIE.net 网络拓扑。值得注意的是计费、TFTP 和 RADIUS 服务器可以在 IP 网络的任一位置，已有的 IP 主干和 VoIP 网关都可以使用。

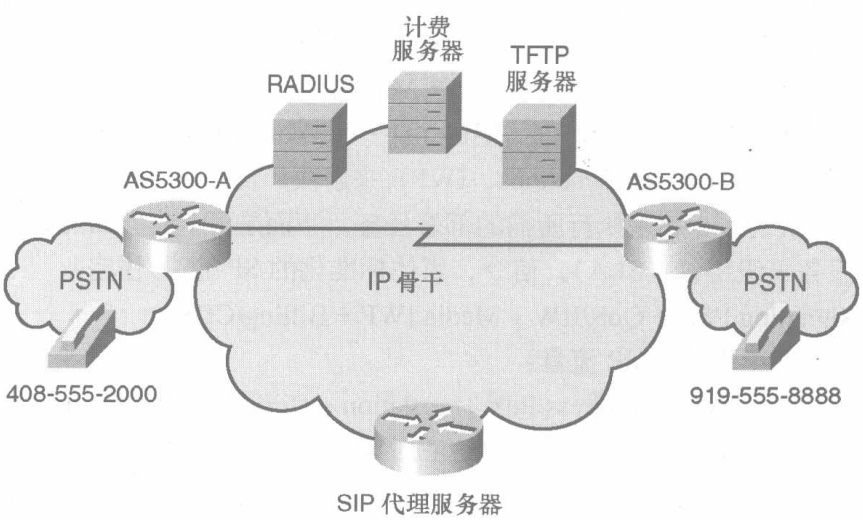


图 15-1 BOWIE.net SIP 网络组件

典型的预付费电话卡呼叫处理如下。

1．用户从 BOWIE.net 购买$10、$20、$50 或 $100 的预付费电话卡。卡被激活，账户号和密码定义在 RADIUS 服务器和计费系统中。

2．当用户要打电话时，他拨叫一个 800 接入号码拨进 BOWIE.netVoIP 网络。

3．AS5400 接收到来自 PSTN 的呼叫，用户将听到来自 BOWIE.net 的提示，请用户选择提示语言。用户可以选择英语或其他语言，如西班牙语或中文。

4．然后用户被请求输入电话卡的账号和密码。此时，RADIUS/计费服务期认证用户信息。用户被认证后，被要求输入要拨打的电话号码。根据被叫方号码，计费服务器决定费率，用户被提示他可通话的时间以及账户内剩余金额。

5．用户输完被叫号码后，计费服务器开始源和终结网关的呼叫细节记录（call detail record，CDR）。

6．当用户的账户余额到达一个低限时，他被提示这个账号将被终止。如果用户仍然使用直至用完所剩余额，呼叫被自动终止。此时，用户可以给这张卡里续费或从 BOWIE.net 购买新卡。

7．呼叫终止后，计费服务器完成特定呼叫的呼叫细节记录（CDR）。

TFTP 服务器存储 AS5400VoIP 网关播放的问候、账户状态、余额状态及剩余时间等提示（以.au 格式）。这些文件需要比 AS5400 闪存更多的空间，所以用户必须从 TFTP 服务器上下载。这些提示可以从 Cisco.com 网站上下载，或者 BOWIE.net 可以使用任何.au 的工具自己建立。

15.5 会话边界控制：增值

因为会话边界控制器（Session Border Controller，SBC）可以使服务提供商很快调整他们的 VoIP 网络到一个可靠的使用其他运营商的 VoIP 服务的接口，所以 SBC 为服务供应商应用增加了一个新的空间。各厂商间实施 VoIP 信令，SIP RFC/草案解释，T.38 传真支持、VoIP 编码和 DTMF 传输时的不同，阻碍了下一代 VoIP 网络的部署。SBC 盒子通过开发设计互联功能（InterWorking Functions，IWF）来解决厂商之间的不兼容。根据厂商和应用，这些 IWF 可以组在一起来执行所需的部署任务。下面是两个典型 SP 部署的例子。

- 服务等级协议（SLA），信令，媒体标准化的 SP-企业/住宅：

  Signaling IWF + QoS/BW + Media IWF + Billing/CDR

- SP 到 SP 互换 VoIP 流量：

  Signaling IWF + Address/Port Translation + Billing/CDR + Rich Signaling

通过这些 IWF，SBC 部署可以管理在对等运营商间的多媒体流，并允许进一步的媒体处理和操作。SBC 应用服务器部署在网络边缘，单独或与任何呼叫控制引擎一起运行。正如您在第 9 章了解的一样，SP 经常抱怨的是计费丢失或未名收入。带有状态的呼叫控制服务器（如 SIP B2BUA 或 MGCP 呼叫代理）可以提供集中的 CDR 收集，并且可以与 SBC 提供的 IWF 一起共同控制和管理 CDR 相关信息。这些信息可以使运营商恢复与丢失 CDR/

计费数据相关的收入，从而增加可能的收入和利润。

另外，多协议信令交换机（ Multiprotocol Signaling Switch，MSW）的成熟路由选择引擎最大化了路由收入，加强了企业间的合作，从而获得最大的收入和利润。

15.6 VoIP 对接网络：服务供应商的最佳选择

虽然 VoIP 作为一项技术来讲，在世界的不同地方有着爆炸性的增长（到 2007 年，VoIP 的市场是 1 970 亿美元，Insight Research），目前的应该是因特网电话供应商（ITSPs 和 VoBBs）、VoIP 运营商和应用服务供应商建立一些通用标准来连接不同 VoIP 岛的时候。这些网络岛在连接中解决结算（与大量呼叫计费/收费有关）并将呼叫从一个 VoIP 移交到另一个网络中。供应上门还减少或彻底消除这些网络中通过 PSTN 终结来对接的费用。VoIP 与 VoIP 的对接和互连是所有供应商的首选。

许多公司正在寻求这些为题的解决方案。SBC，如前面小节中介绍，对此很有帮助，但不能完全解决问题，尤其是当提供一个全球的分布式 VoIP 对接网络，并且这个网络可以无缝提供一种即插即用的连接各种网络的方法时。供应商努力解决多种 VoIP 流量回合时务所遇到的如下问题：

- 号码/拨号计划问题；
- 协议标准和实施的合作问题；
- 主叫方识别和验证，呼叫 ID 欺骗、语音兜售等等的隐私和安全问题。

供应商们正在努力解决这些在部署端对端 VoIP 网络是新近出现的问题。管理着大量数据流量的网络管理员现在不得不考虑新的策略，因为 VoIP 传输为他们的 IP 网络增加了更多的负载和挑战。另外，无线供应商也在寻找在所有 IP 世界中固网和移动网络合一时 VoIP 的优势。

15.7 服务供应商 VoIP 和消费者固网移动融合

像 SBC 一样，消费者固网移动融合弥补和扩展了供应商的语音/无线解决方案。MSO 总在寻求为现有的蜂窝电话提供增强服务的创新方法。通过消费者 FMC，他们允许通过 Wi-Fi 路由器建立的所有呼叫在使用 VoIP 连接到 MSO 上，尽管发生在同一无线客户端的设备呼叫要在合作移动运营商网络上完成。

这项服务也可以在企业环境中部署，公司雇员更倾向采用一个单一的设备来使用企业的 Wi-Fi 和企业提供的移动电话服务。

许多厂商正在开发可携带的 Wi-Fi 电话听筒。厂商们试图通过为消费者他们提供可供选择的手机来将他们从传统的固话中解脱出来。这样他们就可以在任何有他们运营商 Wi-Fi 热点的地方打 VoIP 电话（家庭、工作地点、学校、城区、机场、咖啡店、旅馆，甚者其他国家）然而，这种只 Wi-Fi 方式的有许多未覆盖区域。消费者固定移动融合（FMC）的价值在于当没有 Wi-Fi 信号时，用户可以漫游到一个蜂窝网络并保持与 MSO 的服务（带移动

的 3 重服务）的能力。

图 15-2 显示了在不同的语音网络中平滑移交的想法。

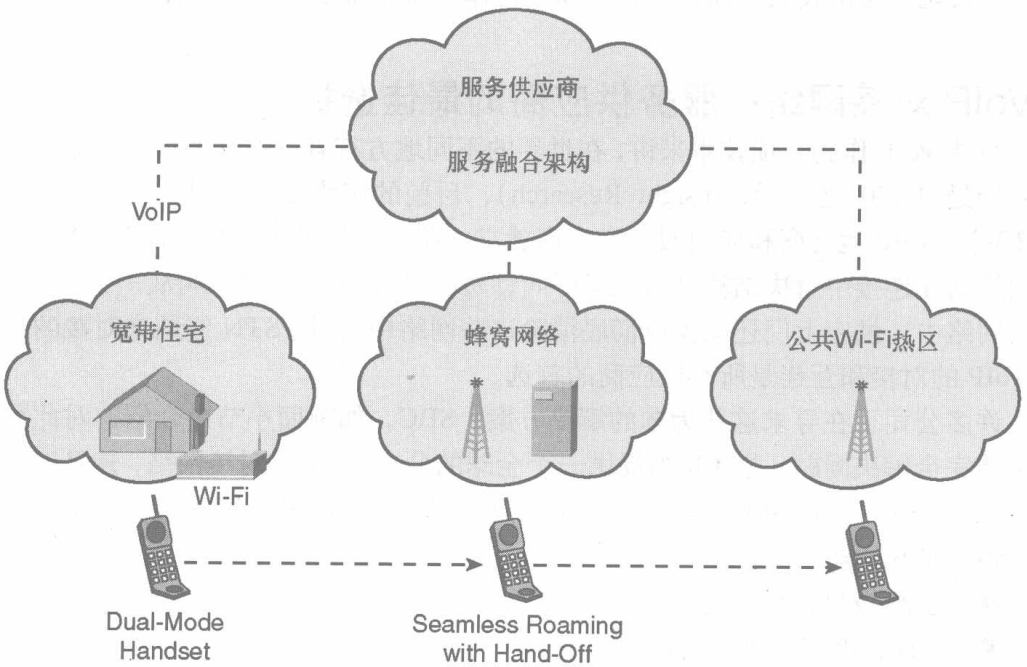


图 15-2 固网移动融合基础

表 15-1 概括了固网移动融合对于消费者和供应商的好处。

表 15-1 固网移动融合的服务供应商和消费者利益

服务提供商利益	用户利益
客户忠实度	单一电话——家里，路上，工作中
增加的 ARPU 值	节省移动话费
扩大市场覆盖率	移动中的 Triple-play 服务
通过提供 Wi-Fi 呼叫优化无线领域	

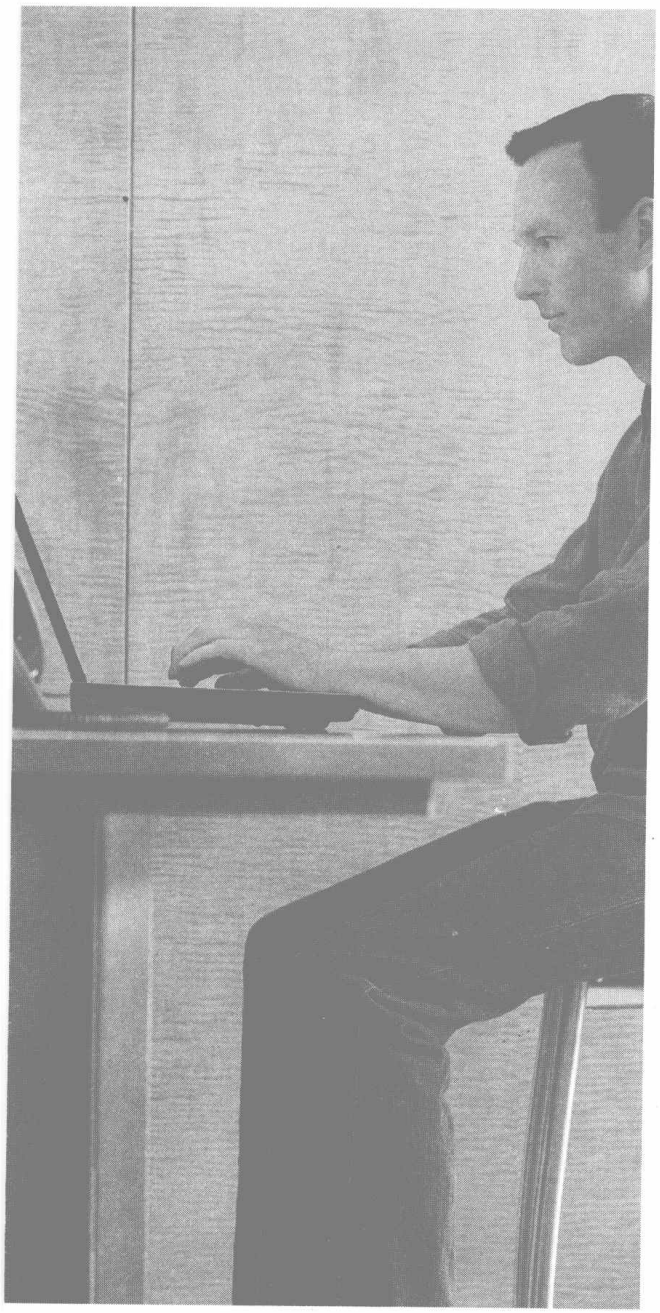
消费者 FMC 为服务供应商扩展 VoIP 相关服务提供了从有线到无线的巨大的潜力空间，从而为最终用户节省了大量话费。通过无缝集成固网服务的优点与手机的方便，运营商和服务提供商可以收回移出流量从而保护核心设施的收入。

15.8 总结

在 SP 市场，IP 作为一种网络传输方式是一种驱动力。世界数据语音和视频在有线无线的合一（也称为融合（convergence））是建立在 VoIP 基础上的。而且，通过 IP 融合的新的利润驱动应用和消减运营费用的能力是服务供应商们正在期望的。与 toll bypass、借记

卡等有关的传统 SP VoIP 应用正在发展为新的使用 IM、文字消息、按需点播、高级 CPE 等应用，这些新应用允许从有线到无线的无缝过渡。SP 的前景/使命证明了 VoIP 有提供比传统电话服务好的服务的潜力。

本章还回顾了以解决分离 VoIP 网络互联问题为目标的 SBC 功能的重要性和驱动这些应用的一些重要部分。类似的，FMC 是扩展 VoIP 到新级别融合服务的另一个过渡。



本章讨论网络架构框架和设计模型，包含以下主题：

- 16.1 向 VoIP 体系结构迁移
- 16.2 企业语音应用及其优势
- 16.3 高级企业应用
- 16.4 Wi-Fi 电话
- 16.5 使用多频编码的更好的语音质量
- 16.6 总结

第16章

企业 VoIP 应用和服务

当企业进入 21 世纪时，他们面临着建立更多的商品和服务、提高客户服务质量、减少开支以保持竞争力等持续的需求。另外，他们发现他们的数据网络不仅是业务的一个至关重要部分，而且如果合理使用的话，它是一个获得和保持客户忠实度的很有竞争力的优势。

在许多年里，企业一直在建设基于传输控制协议/因特网协议（Transmission Control Protocol/Internet Protocol）（TCP/IP）的网络以利用 TCP/IP 网络的力量和它所能提供的许多服务。这些服务包括到无处不在的远程用户因特网访问、易用的网页浏览器、企业内部网和 Web 服务器、Java 应用，以及与贸易伙伴和供应商的扩展内部网。所有这些服务使企业可以很容易地建设新的企业应用，可以通过浏览器访问信息数据库，并为内部和外部客户提供新的服务。

企业 VoIP 应用包括商务语音服务和功能、在 IP 网络上的端对端语音呼叫、PSTN 接入、统一消息和即时消息与列席等高级 IP 服务。

当更多的雇员在家工作或旅行时，企业需求也在发展。人们越来越多地地理分散地协同工作。将企业的基础设施跨越地理障碍，扩展到远程办公室或家中以促进生产力也是至关重要的。这就包括拨打接听电话、访问消息服务的能力，以及不需接入设备（例如普通电话在 PC 上运行的软电话或者手机）的表示通信有效性的能力。

16.1 向 VoIP 体系结构迁移

IP 通信的采用是分阶段迁移的。第一步可能是将一些时分多路复用（time-division multiplexing，TDM）中继从旧有的企业专用小交换机（PBX）移到语音网关上。语音网关提供旧有 TDM 网络和 IP 网络的互联。语音网关使用 IP 网络在旧有的位于企业各处的 PBX 间传输语音。用户在继续使用传统的 PBX 提供的各种呼叫功能的同时通过使用语音和数据合一的网络减少了开支。

当客户已经准备好实施基于 IP 的通信基础时，下一步可能是使用混合 TDM IP PBX 或一个 IP PBX。IP PBX 处理网上（on-net）（在企业内部呼叫）并支持网下（off-net）（PSTN）呼叫路由选择。在两种模型中，VoIP 客户端被实施为桌面的 IP 电话或在计算机上运行的客户端。由 VoIP 客户端发起的呼叫由 IP PBX 服务，IP PBX 提供所有与旧有的 PBX 相似的呼叫路由选择服务和功能。与 PSTN 的连接由语音网关提供。语音网关支持信道关联信令（channel associated signaling，CAS）、基群速率接口（primary rate interface，PRI）和 7 号信令系统（Signaling System 7，SS7）信令。

企业网络也为优先语音流量、网络安全、有效性和容错提供必要的服务质量保证（QoS）。

思科 CallManager（CCM）是一个 IP PBX，它是思科 IP 电话解决方案的一个重要组件。CCM 扩展了企业电话功能，服务于分组电话网络设备。CCM 为配制的设备，包括 IP 电话、软电话、VoIP 网关和消息服务器，提供呼叫处理、信令和连接服务。它使用如 H.323 和 SIP 等标准协议作为与其他的 IP PBXIP 电话和语音网关之间的呼叫信令。

16.2 企业语音应用及其优势

当企业开始考虑将他们的语音和数据网络整合到一个多服务网络时，他们最先考虑的应用是 *toll-bypass*（收费旁路）。Toll-bypass 允许企业在他们现有的 TCP/IP 网络上发送公司内部的语音和传真呼叫。通过将这些公司内部的流量从 PSTN 上移走而使用他们数据网络的剩余带宽又不丧失功能，企业立即就可以节省电话费用。

> 注释：在实施基于 VoIP 的 toll-bypass（收费旁路）服务前，确保 VoIP 技术一般使用和 toll-bypass 的特殊使用，不与现行法律或与国家或地区的操作惯例相冲突。

企业可以立即看到使用 toll-bypass 所带来的效益。实际上，一些有着大量办公室内呼叫（包括国内国际的）的企业在 3～6 个月就可以收回投资。

在企业越来越适应 VoIP 和 toll-bypass 时，下一个他们通常考虑的应用是应用在客户服务、交互工程组和远程培训。下面是一些可以应用在这些领域应用的例子。

- 点击拨号（Click-2-Call）允许企业在他们的网页上建立一个连接，这个连接可以自动拨叫一个客户服务代表到一个客户的呼叫。
- 微软网络会议（Microsoft Netmeeting）综合了传统电话服务，应用共享和基于 H.323 视频会议的功能。这个综合服务允许在不同位置的雇员可以很容易地在一个项目上合作，通过整合设备和数据/语音网络减少了费用。
- 思科 IP 电话看起来和感觉上都跟传统电话一样，但是增加了 IP 连接功能。IP 电话与更新的基于 IP 的 PBX 一起工作，不再依赖于一个已有 PBX 的功能，比如拨号音。这些 IP PBX 不仅提供和传统 PBX 一样的功能（拨号音、语音信箱和会议），它们还利用了所有基于 IP 的服务以提供新功能。因为它是一个 IP 设备，IP 电话不仅可以使用 VoIP 服务，还可以使用任何在网络上有效的基于 IP 的多种服务应用。
- 思科基于 PC 的 SoftPhone（软电话）将电话机功能通过一个图形用户界面扩展到 PC，该界面提供与电话听筒一样的功能，并集成了与其他多服务应用如 web 浏览、微软网络会议（Microsoft Netmeeting）和基于轻目录访问协议（Lightweight Directory Access Protocol，LDAP）的目录服务。它还不需要附加设备（如听筒），因为在标准 PC 上通常都配备了 SoftPhone（软电话）所需的听筒和麦克风。

所有目前讨论的服务都被认为是第一代的基于标准的服务。正如 TCP/IP 数据服务

高速发展一样，第二代 VoIP 和基于 TCP/IP 的集成数据/语音服务也在快速发展。这些服务将被与日俱增的企业竞争，开放标准应用编程接口（API），如 SIP 的协议、LDAP、电话应用编程接口（Telephone Application Programming Interface，TAPI）、Java 电话 API（Java Telephony API，JTAPI），Linux 和企业网络经理和程序员的创造性所驱动。

16.3 高级企业应用

使用 VoIP 的 toll-pass 和所带来的费用节省是企业采用一个融合的语音数据基础架构的第一步。企业用户通过将企业网络覆盖他们总部、分支办公室和家庭办公室，可以成功地电话服务中解脱出来。这将节省大量的企业内部呼叫，从而节省了费用。

IP 电话的使用还帮助员工随时随处可以访问公司内部资源如内网和通信设施。员工可以使用 VPN 登录企业网络，使用在 PC 上运行的软电话和他们的分机号码进行通信。通过 VoIP，在家里或在宾馆乐的员工可以使用他们办公室号码发起呼叫或接听电话。他还可以通过他的软电话使用其他功能如保持，转移或会议。他可以使用统一的消息系统来访问他的语音信箱和电子邮件。

因此，IP 通信使员工在路上或在家中也可以连接到办公室。日益增加的移动性和员工的地域分散为通信的协作性、可到达性和有效性带来了新的挑战。企业正在通过广泛使用先进的服务如视频通信、协作工具和列席服务等来驱动生产力。

16.3.1 基于 Web 的协作和会议

企业越来越多地使用语音和视频会议应用、文档共享及协作工具来消减出差时间和费用。这些应用通过提供感觉像在一间屋子开会那样的工具来提高生产力。文档共享和协作允许在高度交互方式下的实时检阅和修改文档。这个交互式经验极大地减少了需要聚在一起做决定的时间，帮助收集意见或建议，并减少了出差和发电子邮件的时间。所有这些都提供了员工的生产力，对企业利润有着直接的影响。

Cisco MeetingPlace——思科 IP 通信系统中的一部分——是一个多种媒体会议的解决方案，它集成了语音、视频和 Web 会议功能，使远程会议就像面对面的会议一样自然和有效。Cisco MeetingPlace 部署在企业网络上，与组织安全性、语音和数据基础设施相集成。会议参加者需要一个电话和浏览器。它还可以被扩展到公司的外部会员。使用公司网络传输语音和视频流量为公司节省了大量费用。

Cisco MeetingPlace 与用户的计算机集成。它提供了一个易于使用，直观的基于 Web 的界面来：

- 建立和管理会议；
- 加入和离开会议；
- 在与会者加入和离开会议时定制铃声和提示。

Cisco MeetingPlace 与浏览器、思科 IP 电话、IM 客户端和诸如 Microsoft Outlook 的日历系统相集成。

在一个会议会话过程中，参与者使用一个基于浏览器的界面来：

- 查看共享数据和对话的参与者列表——实时更新；
- 共享和查阅文档，如演讲稿和数据报表；
- 允许参与者之间的文本消息（IM）；
- 通过与会者认证和安全媒体会话传输来提供安全性；
- 记录、保存和回放会议；
- 在任何应用和文档间协作，在与会者之间传递控制。

与 MeetingPlace 集成的视频需要附加的视频会议硬件，如多点控制单元、增强的媒体处理器卡和有视频能力的网关。客户也将需要视频端点或桌面照相机作为视频会议部署的一部分。

16.3.2 需要列席信息

大多数不能联系到被叫方的呼叫都以语音信箱结束。被叫方可能不在他或她的座位上——他们可能出差了，正在开会或正在远程位置工作。作为一个结果，主叫和被叫都有可能多次试图联系对方——这可能的结构就是延迟了重要的商务决定。

这个问题的关键是主叫不确切知道什么时候和怎样能联系到被叫方。大多数人都不会在他们知道对方在忙或不在的时候给对方打电话。如果主叫提前知道被叫是否可以接听电话，那么打通电话的成功率就大大提高了。列席提供这项至关紧要的信息。

列席（Presence）描述了一个人与其他人通信的意愿、有效性和能力。即时消息系统允许最终用户在发送消息给朋友前知道他是不是在线。这个概念被扩展为监视一系列的最终用户设备如传统电话、无线电话、笔记本上的 IP 客户端和 PDA。与最终用户的日历的集成也放到了一个人的列席状态中。

列席允许用户计划他们与网络中其他用户通信的时间。列席信息的有效允许同事或朋友先选择最合适的时间和方式进行通信。列席状态有多种，如：

- 登录/退出；
- 忙/空闲；
- 注册/没注册；
- 在会议中；
- 不在办公室；
- 度假；
- 不要打扰。

这些信息向其他人呈现的时候，就避免了正在与客户的重要会议过程中被打扰的可能性。它还可以让呼叫方使用一个低打扰性的通信方式，如即时消息来代替拨打电话。

列席信息主要基于以下状态：

- 设备状态；
- 用户状态。

网络和其相关联的设备报告最终用户设备状态，如移动和 IP 电话的注册信息。这些报告的状态有空闲、忙和退出。这些设备还可以报告他们是否支持音频、视频和 IM 等。这些提供关于可以联系到用户的端点的信息。

在设备状态上，用户可以在他的设备上设置用户状态，如不要打扰，和提供有用的消息如“在会议中直至 4pm”。类似地，用户还可以提示虽然他在会议中，但是可以使用即时消息。

列席状态因此是设备状态和用户提供状态的综合。

16.3.3 Presence-Aware（列席相关）服务

将列席信息与企业的基础通信设施集成将产生更多的增强服务和获得更高的生产力。下列是使用列席信息的增强服务的例子。

- 电话上的联系人列表——用户可以在 IP 电话系统上建立联系人列表或通信录，类似于 IM 系统中的好友列表。当通信网络允许列席时，通信录就可以增强以显示用户是否有效。通信录显示设备和用户状态并实时更新。呼叫方可以根据列表中的联系人的有效性来呼叫。这项功能集成了快速拨号和有效性信息。
- 根据有效性能和功能来路由呼叫——一个企业用户可以通过多种设备被联系到，如桌面电话、笔记本上的软电话、Wi-Fi 有效 IP 电话、PDA 等。列席信息如登录状态、注册状态、忙/空闲状态在呼叫路由选择中的使用增加了联系到这个人的可能性，避免了使用语音信箱。比如，如果用户没有在他的办公桌注册，但是他的 Wi-Fi 电话注册到了企业 PBX，呼叫则直接被路由到 Wi-Fi 电话。
- 增强的漏听电话列表——漏听电话列表显示了用户不在的时候不能接听的电话。列席信息可以与这些电话号码一起显示呼叫方设备和呼叫方的状态，以及联系他们的最好方式。用户可以尝试回那些状态显示有效的呼叫者的电话。
- ad-hoc 会议用户的有效性——试图邀请其他用户参加即时会议的用户在邀请前可以先检查那些用户的设备和状态，以及他们对音频/视频会议的有效性。
- Camp-on 服务——当一个用户希望联系一个目前正忙或已退出的联系人时，用户可以使用 Camp-on 服务。企业 PBX 继续监视该联系人的状态。当目标电话和 camp-on 服务的请求着都在空闲状态时，首先呼叫 camp-on 服务的请求者。当请求者应答电话时，PBX 将电话延伸到目标电话号码。
- 点击拨号（Click to dial）应用——列席信息越来越多地与 E-MAIL 客户端如 Microsoft Outlook 和企业目录信息集成。企业用户可以在企业目录里或在他们的收件箱内看到列席状态。他们可以在对方有效时使用点击（click to dial）应用来引起一个呼叫或 IM 会话。
- 增强的联系中心应用——列席信息可以在联系中心帮助在不同地理位置的代理之间路由呼叫。当使用开放的基于标准的协议来分发列席信息时，所有的联系中心的代理不再试图使用同样的 PBX 系统或厂商。这就允许应用服务器收集各种位置

上的代理信息，在多个联系中心之间无缝的分发呼叫。列席和 IM 还可以帮助代理实时联系某个领域或主题事物的专家来更快更有效地回答客户的咨询。

16.4 Wi-Fi 电话

企业中允许 Wi-Fi 的（与 802.11a/b/g/n 标准兼容）IP 电话使用户可以在企业的任何地方联系到，从公共热点到自己的办公室。Wi-Fi 电话与蜂窝系统相比，能提供所有的功能和更好的语音质量。Wi-Fi 电话允许企业内部的用户接听打向他分机的电话，而无须非得在他们办公桌旁。

一些 Wi-Fi 电话还允许用户在 VoIP 和蜂窝电话网络之间互换。用户可能会使用他办公室的电话发起 VoIP 呼叫。当他不在办公室时，呼叫被无缝地转换到蜂窝网络上。当他回到企业网络范围内时，呼叫也移回企业的 VoIP 网络。

这种方式的优势在于移动网络更高的灵活性和将呼叫时间从蜂窝网络转移到企业网络所节省的费用。

16.5 使用多频编码的更好的语音质量

最初的 VoIP 的实施试图达到由旧有的 PSTN 设置的标准。旧有的 PSTN 交换机和 PBX 有一个 4kHz 的有限带宽，这个带宽允许在 300Hz 和 3 400Hz 之间采样语音频率。PSTN 受限于窄带频率，而 VoIP 允许多频编码。多频编码在 16kHz 采样，允许高达 8kHz 的传输。这些编码提供更清楚的语音，切对网络带宽没有过高的要求。

G722.2 是由 ITU 定义的多频编码。G722.2 是一个适应多速率的编码器，支持 6～23.85kbit/s 的比特率。Global IP Sound 的 iSAC 是另一个多频编码器，允许的传输速率是 10～32kbit/s。iSAC 对于分组丢失很健壮。这些编码器都在 16kHz 采样。

这些编码器对于如远程教育、按需培训、会议和如在线游戏等多媒体会话等 VoIP 应用非常有用。这些编码器通过提供更真实的声音质量来提高用户的经历。

16.6 总结

企业最初使用 VoIP 来整合他们的语音和数据网络。当整合网络的最初利益实现后，企业用户已经开始使用整合网络来提供广泛的新应用来促进生产力的提高。企业使用 VoIP 来提供他们全球各站点之间的协作能力。VoIP 提供一些新工具，如列席和即时消息，使员工可以同世界另一侧的伙伴协同工作。使用多频编码的高质量语音、视频会议和文档共享提供了更有效和更愉快的沟通。

这全部的好处就是企业 VoIP 通过促进合作与沟通帮助提高员工的生产力。

{
  "filename": "MTE5Mzk1Nzguemlw",
  "filename_decoded": "11939578.zip",
  "filesize": 69399317,
  "md5": "540af259dbddd91c64a84f5714db3878",
  "header_md5": "77198a19f74be44f8f14668f88739376",
  "sha1": "f3c586434cb3443c66321f77dd33bbbb6ba34105",
  "sha256": "173bfc170667070573540b1461f067a27332a911413057f41d3d54a7360d4bcd",
  "crc32": 308228094,
  "zip_password": "julian",
  "uncompressed_size": 86717488,
  "pdg_dir_name": "11939578",
  "pdg_main_pages_found": 292,
  "pdg_main_pages_max": 292,
  "total_pages": 314,
  "total_pixels": 1897664192,
  "pdf_generation_missing_pages": false
}