

国际电信联盟

ITU-T

国际电信联盟

电信标准化部门

J.160

(11/2005)

J系列：有线网和电视、声音节目和其它多媒体信号的传输
IPCablecom

**使用电缆调制解调器在有线电视网上提供时间紧迫型
业务的结构框架**

ITU-T J.160建议书

ITU-T J.160建议书

使用电缆调制解调器在有线电视网上提供时间紧迫型业务的结构框架

摘要

本建议书为确定功能的组件提供了一个高层参考框架，并为提供数字语音和电话业务定义了必要的接口。为实施这一结构，现已制定了一系列建议书（ITU-T J.161-J.178建议书）。

来源

ITU-T第9研究组（2005-2008年）按照ITU-T A.8建议书规定的程序，于2005年11月29日批准了ITU-T J.160建议书。

前 言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联2006

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

	Page
1 范围	1
2 参考文献	1
3 术语和定义	2
4 缩写词和惯用词解	2
4.1 缩写词	2
4.2 惯用词解	4
5 IPCablecom	4
5.1 IPCablecom 结构框架	4
5.2 IPCablecom 的区域和域	5
5.3 IPCablecom 建议书	6
5.4 有关IPCablecom 设计的考虑	7
6 IPCablecom 功能组件	9
6.1 媒体终端适配器 (MTA)	10
6.2 电缆调制解调器 (CM)	12
6.3 HFC 接入网	12
6.4 电缆调制解调器终接系统 (CMTS)	12
6.5 呼叫管理服务器 (CMS)	12
6.6 PSTN 网关	13
6.7 OSS 后台 (back-office) 组件	15
6.8 通知服务器 (ANS)	16
7 协议接口	17
7.1 呼叫信令接口	17
7.2 媒体流	19
7.3 MTA 设备配置	21
7.4 SNMP 网元管理层接口	22
7.5 事件消息接口	23
7.6 服务质量 (QoS)	24
7.7 CMS 用户配置	27
7.8 电子监视	28
7.9 安全性	29
8 网络设计考虑	35
8.1 计时和报告问题	35
8.2 执行缓冲器和编码速率间的时间匹配	35
8.3 IP 寻址	35
8.4 动态 IP 寻址指配	36
8.5 FQDN 指配	36
8.6 信令和媒体流数据包的优先级标记	36
8.7 传真支持	37

	Page
8.8 模拟调制解调器支持	37
附件 I – 术语表	38
I.1 定义	38
I.2 缩写词	40
参考书目	43

ITU-T J.160建议书

使用电缆调制解调器在有线电视网上提供时间紧迫型业务的结构框架

1 范围

IP-Cablecom项目定义了一系列可用于互操作设备开发的建议书，这些设备可以根据交互式有线电视业务传输系统（DOCSIS）系列建议书的规定，使用电缆调制解调器在混合光纤同轴网（HFC）上提供基于分组的话音、视频和其它高速多媒体业务。将来的工作会扩展这一架构，将多媒体应用纳入其中。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

- ITU-T Recommendation G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*。
- ITU-T Recommendation J.83 (1997), *Digital multi-programme systems for television, sound and data services for cable distribution*。
- ITU-T Recommendation J.112 (1998), *Transmission systems for interactive television services, plus Annex A (2001), Digital Video Broadcasting: DVB interaction channel for Cable TV (CATV distribution systems)*, Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification and Annex C (2002), Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique*。
- ITU-T Recommendation J.161 (2001), *Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems*。
- ITU-T Recommendation J.162 (2005), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*。
- ITU-T Recommendation J.163 (2005), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*。
- ITU-T Recommendation J.164 (2005), *Event message requirements for the support of real-time services over cable television networks using cable modems*。
- ITU-T Recommendation J.166 (2005), *IP-Cablecom management information base (MIB) framework*。
- ITU-T Recommendation J.167 (2005), *Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems*。
- ITU-T Recommendation J.170 (2005), *IP-Cablecom security specification*。
- ITU-T J.171.0建议书 (2005年), *IP-Cablecom 中继网关控制协议(TGCP): 特征概述*

- ITU-T Recommendation J.178 (2005), *IPCablecom CMS to CMS signalling*。
- ITU-T Recommendation Q.704 (1996), *Signalling network functions and messages*。
- ITU-T Recommendation T.38 (2005), *Procedures for real-time Group 3 facsimile communication over IP networks*。
- IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*。
- IETF RFC 1119 (1989), *Network Time Protocol*。
- IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*。
- IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control*。
- IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*。
- IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*。
- IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*。
- IETF RFC 3261 (2002), *SIP:Session Initiation Protocol*。
- IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*。
- IETF RFC 3415 (2002) *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*。
- IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*。

3 术语和定义

本建议书定义了如下术语：

3.1 IPCablecom：包括能够利用电缆调制解调器在有线电视网上提供实时业务的结构和一系列建议书的ITU-T项目。

3.2 电缆调制解调器 (cable modem)：电缆调制解调器是一种可终止DOCSIS连接的客户端第二层终接设备。

3.3 受管IP网络 (managed IP network)：一种由单一实体管理的IP网络，用于传送IPCablecom信令和媒体数据包。

3.4 受管IP骨干网 (managed IP backbone)：用于IPCablecom域互连的受管IP网络。

4 缩写词和惯用词解

4.1 缩写词

本建议书使用了下述缩写词：

ANC	通知控制器 (Announcement Controller)
ANP	通知播放器 (Announcement Player)
ANS	通知服务器 (Announcement Server)
CM	电缆调制解调器 (Cable Modem)

CMS 呼叫管理服务器 (Call Management Server)

CPE 客户所在地设备 (Customer Premises Equipment)

DHCP 动态主机配置协议 (Dynamic Host Configuration Protocol)

DNS 域名系统 (Domain Name System)

DTMF 双音多频 (Dual Tone Multi-Frequency)

FQDN 完全限定域名 (Fully Qualified Domain Name)

GC 门控制器 (Gate Controller)

HFC 混合光纤同轴网 (Hybrid Fibre/Coax)

HTTP 超文本传输协议 (HyperText Transfer Protocol)

IEEE 电气与电子工程师学会 (Institute of Electrical and Electronic Engineers)

IETF 互联网工程任务组 (Internet Engineering Task Force)

IP 互联网协议 (Internet Protocol)

IPsec IP安全性 (IP security)

ISTP 互联网信令传输协议 (Internet Signalling Transport Protocol)

ISUP 综合业务数字网用户部分 (Integrated Services Digital Network User Part)

MAC 媒体访问控制 (Media Access Control)

MF 多频 (Multi-Frequency)

MG 媒体网关 (Media Gateway)

MGC 媒体网关控制器 (Media Gateway Controller)

MIB 管理信息库 (Management Information Base)

MMH 多线性模块散列 (Multilinear Modular Hash)

MTA 媒体终端适配器 (Media Terminal Adapter)

MTP 消息传输部分 (Message Transfer Part)

NAT 网络地址翻译器 (Network Address Translator)

NCS 基于网络的呼叫信令 (Network-Based Call Signalling)

OSS 操作支援系统 (Operations Support System)

PSTN 公共交换电话网 (Public Switched Telephone Network)

QoS 服务质量 (Quality of Service)

RKS 记录保存服务器 (Record Keeping Server)

RTP 实时传输协议 (Real-Time Transfer Protocol)

SA 源地址 (Source Address)

SCCP 信令连接控制部分 (Signalling Connection Control Part)

SG 信令网关 (Signalling Gateway)

SID 系统识别号 (System Identification number)

SNMP 简单网络管理协议 (Simple Network Management Protocol)

TCAP 事务处理能力应用部分 (Transaction Capabilities Application Part)

TFTP 小文件传输协议 (Trivial File Transfer Protocol)

TGCP 中继网关控制协议 (Trunking Gateway Control Protocol)

TGS 票证授予服务器 (Ticket Granting Server)

ToS 服务类型 (Type of Service)

UDP 用户数据报协议 (User Datagram Protocol)

4.2 惯用词解

如果本建议书得以实施，则“必须”、“应”和“需”等关键字应理解为本建议书具有的强制力。

现将本建议书各处使用的说明特定要求重要性等级的关键字总结如下。

“必须”	此关键字或形容词“必要的”表示所涉及的内容是本建议书要求绝对遵守的。
“不得”	此短语表示这所涉及的内容是本建议书中绝对禁止的。
“应”	此关键字或形容词“建议”表示在某些特定情况下，可能有合理的理由忽略此项内容，但用户应了解由此产生的所有影响，并在选择不同方式之前进行仔细权衡。
“不应”	此短语表示在某些特定情况下，可能有合理的理由表明书中列出的行为是可以接受的或者甚至是有益的，但用户应了解由此产生的所有影响，并在实施此短语描述的任何行为之前，进行仔细权衡。
“可能”	此关键字或形容词“可选”，表示涉及的内容的确为可选项。一家厂商可能会因为其自身的市场需求，或该项内容能够提高产品的水平等原因而加以使用，而另一家厂商则能忽略不用。

5 IPCablecom

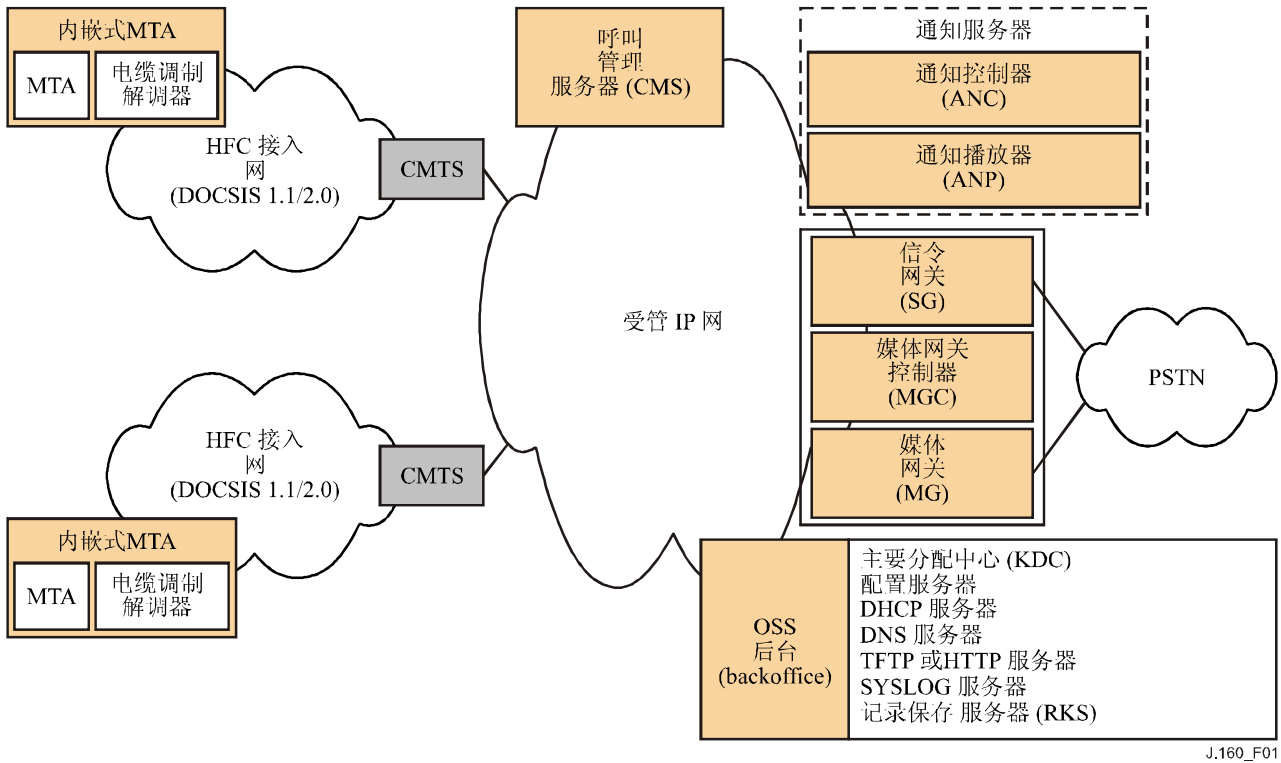
5.1 IPCablecom 结构框架

在很高的层面，IPCablecom结构包括三个网络：“DOCSIS HFC接入网”、“受管IP网”和PSTN。由电缆调制解调器终端系统 (CMTS) 提供“DOCSIS HFC接入网”和“受管IP网”之间的连接。信令网关 (SG) 和媒体网关 (MG) 都提供“受管IP网”与PSTN之间的连接。IPCablecom的参考结构如图1所示。

DOCSIS HFC接入网在客户所在地与电缆前端之间提供高速、可靠、安全的传输。此接入网提供包括服务质量在内的所有DOCSIS能力。DOCSIS HFC接入网包括下述功能组件：电缆调制解调器 (CM)、多媒体终端适配器 (MTA) 和电缆调制解调器终端系统 (CMTS)。

受管IP网有几种功能。首先，它在负责信令、媒体、配置与确定接入网服务质量的基本IPCablecom功能组件之间实现互连。此外，受管IP网在其它受管IP网与DOCSIS HFC网络间提供长途IP连接。受管IP网包括下述四个功能组件：呼叫管理服务器 (CMS)、若干操作支援系统 (OSS)、后台 (back-office) 服务器、信令网关 (SG)、媒体网关 (MG) 和媒体网关控制器 (MGC)。

第6部分对图1所示独立的网络组件进行了详细描述。



J.160_F01

图1/J.160 – IPCablecom参考结构

5.2 IPCablecom的区域和域

IPCablecom区域如图2所示，包括由一台可工作的CMS管理的一个或多个DOCSIS HFC接入网中的MTA组。单一区域内和区域间（例如，CMS ↔ CMS）的功能组件间的接口在IPCablecom建议书中给出了定义。

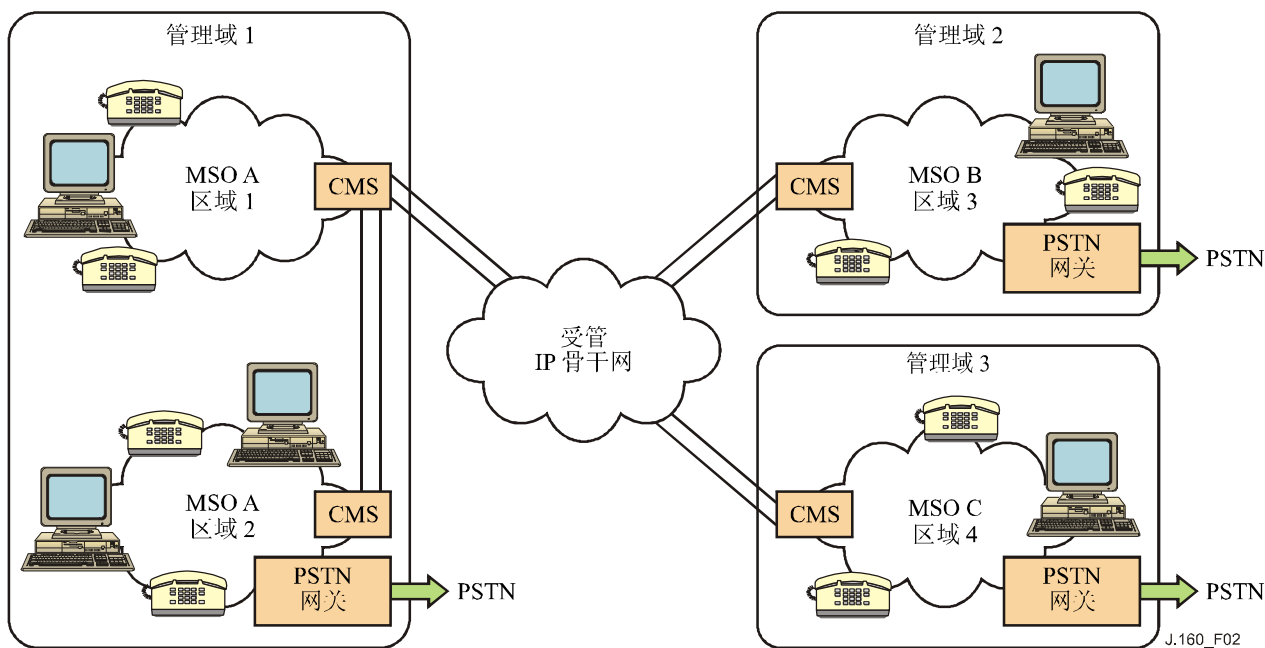


图 2/J.160 – 区域和管理域

IP Cablecom 域由一个或多个由单一管理实体运营和管理的 IP Cablecom 区域组成。IP Cablecom 域也被称为管理域。

5.3 IP Cablecom 建议书

表 1/J.160 – IP Cablecom 建议书

J.160	使用电缆调制解调器在有线电视网上提供时间紧迫型业务的结构框架
J.161	使用电缆调制解调器在有线电视网上提供双向音频业务的音频编解码器要求
J.162	使用电缆调制解调器在有线电视网上提供时间紧迫型业务的网络呼叫信令协议
J.163	使用电缆调制解调器在有线电视网上提供实时业务的动态服务质量
J.164	使用电缆调制解调器在有线电视网上提供实时业务的事件消息要求
J.165	IP Cablecom 互联网信令传输协议 (ISTP)
J.166	IP Cablecom 管理信息库 (MIB) 框架
J.167	使用电缆调制解调器在有线电视网上提供实时业务的媒体终端适配器 (MTA) 设备配置要求
J.168	作为附件 E 附于 J.166
J.169	作为附件 C 附于 J.166
J.170	IP Cablecom 安全性规范
J.171.1	IP Cablecom 中继网关控制协议 (TGCP)：类别 1
J.171.2	IP Cablecom 中继网关控制协议 (TGCP)：类别 2
J.172	IP Cablecom 管理事件机制

J.173	IPCablecom内嵌MTA的主线支持
J.174	IPCablecom域间服务质量
J.175	音频服务器协议
J.176	作为附件D附于/J.166
J.177	IPCablecom CMS用户配置规范
J.178	IPCablecom CMS间信令
J.179	IPCablecom 对多媒体的支持

5.4 有关IPCablecom设计的考虑

为在整个有线网络基础设施中启动实时多媒体通信，IPCablecom建议书定义了下述领域的协议：

- 呼叫信令；
- 服务质量；
- 媒体流传送和编码；
- 设备配置；
- 事件消息；
- 安全性；
- 电子监视；
- 操作支持系统。

本段概述了制定定义IPCablecom参考结构建议书时使用的高层设计目标和概念。应查阅各独立的IPCablecom建议书，以获取这些领域中详细的协议要求。

5.4.1 总体结构目标

- 具备使最终用户感受到与PSTN相似或更好的话音质量的能力。
- 提供可升级并能支持上百万用户的网络结构。
- 确保单向本地IP接入和IP出口（即不包括IP骨干网）的单向时延小于45 ms。
- 利用现有标准。IPCablecom力求指定那些已被商用通信网络广泛使用的、开放且经产业认可的标准，包括由国际电联、IETF、IEEE和其它通信标准组织批准的标准。
- 利用和提高通过J.112基础设施实现的数据传送和服务质量能力。
- 定义一种结构，使多个厂商能够快速制定低成本的可互操作的解决方案，以满足上市时间的要求。
- 确保呼叫阻塞概率在每日最忙时（HDBH）小于1%。
- 确保在每10 000次完成的呼叫中，呼叫中断和呼叫故障的数量少于1次。

- 支持调制解调器（最多V.90 56 kbit/s）和传真（最多14.4 kbit/s）。
- 确保在每分钟的呼叫信令中因非同步取样时钟或因丢失数据包而产生的滑帧数量少于0.25。

5.4.2 呼叫信令

- 定义一种基于网络的信令结构。
- 为下述呼叫模式提供端到端呼叫信令：
 - 始发于PSTN并终接于有线网络的呼叫；
 - 始发于有线网络并终接于有线网络的呼叫；
 - 始发于有线网络并终接于PSTN的呼叫；
 - 跨区（域内）和域（域间）的呼叫。
- 提供支持呼叫特性的信令，例如：
 - 呼叫等待；
 - 取消呼叫等待；
 - 呼叫前转（无应答、忙、可变）；
 - 三方呼叫；
 - 语音邮件消息等待指示符；
 - 主叫号码传送；
 - 主叫名传送；
 - 呼叫等待的主叫识别传送；
 - 主叫识别传送阻塞；
 - 匿名呼叫拒绝；
 - 自动回叫；
 - 自动重叫；
 - 区别振铃/呼叫等待；
 - 客户发起的跟踪。
- 支持在有线运营商的IPCablecom网络中和在与PSTN相连时使用符合现有IP电话标准的信令。
- 支持直拨任何国内和国际电话号码的能力（ITU-T E.164建议书的涉及范围）。
- 接收来自任何PSTN支持的国内和国际电话号码的能力。
- 确保新用户通过本地号码可移植性（LNP）功能保留当前电话号码的功能。
- 使用选定运营商进行长途呼叫的能力。这包括预签约和每次呼叫都进行选择的功能。
- 支持呼叫阻塞/长途呼叫阻塞限制。（例如，阻塞对某些特定前缀的呼叫）

5.4.3 服务质量

- 提供一套丰富的政策机制，以便在接入网上启动并管理IPCablecom业务的QoS。
- 为上下行方向提供接入控制机制。
- 允许IPCablecom 呼叫过程中QoS发生动态变化。

- 尽量降低并防止QoS的滥用，包括服务盗用和拒绝服务形式的攻击。确保由可信网元制定和实施QoS政策。
- 为紧急业务和其它基于优先级的信令业务提供优先级机制。

5.4.4 编解码器和媒体流

- 将IP电话环境中延时、丢包和抖动对话音质量的影响降到最低。
- 定义一套最低数量的音频编解码器，且这些编解码器必须在所有IPCablecom端点设备（MTA和MG）都得到支持。强制性编解码器评估标准的制定，是基于那些对话音质量、带宽使用和实施复杂度最有效的编解码器。
- 采用发展中的窄带与宽带编解码器技术。
- 指定回声消除和话音活动检测机制。
- 通过带内发射和DTMF中继，支持透明、无差错DTMF传输与检测。
- 支持失聪者和听力受损者使用的终端设备。
- 当需要传真和调制解调器业务时，提供编解码器切换机制。
- 为确保传真在IP网络上传输的可靠性，支持传真中继。
- 为监视话音质量，支持VoIP矩阵的计算和报告。

5.4.5 设备配置和OSS

- 支持客户所在地设备的动态和静态配置（MTA和CM）。
- 公共配置的改变不应要求重新启动MTA。
- 允许对用户设备的IP地址进行动态指配和管理。
- 确保实时配置，且MTA软件的配置不会对用户业务产生负面影响。
- 定义MIB模块，以管理使用IETF的简单网络管理协议（SNMP）的客户所在地设备（MTA）。

5.4.6 安全性

- 实现具有相等或高于在PSTN体验到的私密性的住宅话音功能。
- 防范MTA攻击。
- 保护电缆运营商不受各类拒绝服务、网络中断和服务盗用的攻击。
- 设计考虑包括保密、鉴权、完整性和接入控制。

5.4.7 电子监视

- 通过报告呼叫数据和呼叫内容支持电子监管的能力。

6 IPCablecom功能组件

本节描述了IPCablecom网络中的功能组件（见图3）。组件的说明并不是要定义或间接给出产品实施的要求，而是要描述参考结构中各组件的作用。请注意，特定的产品实施可能会根据需要将功能组件组合进去，但并不是所有组件都要在IPCablecom网中出现。

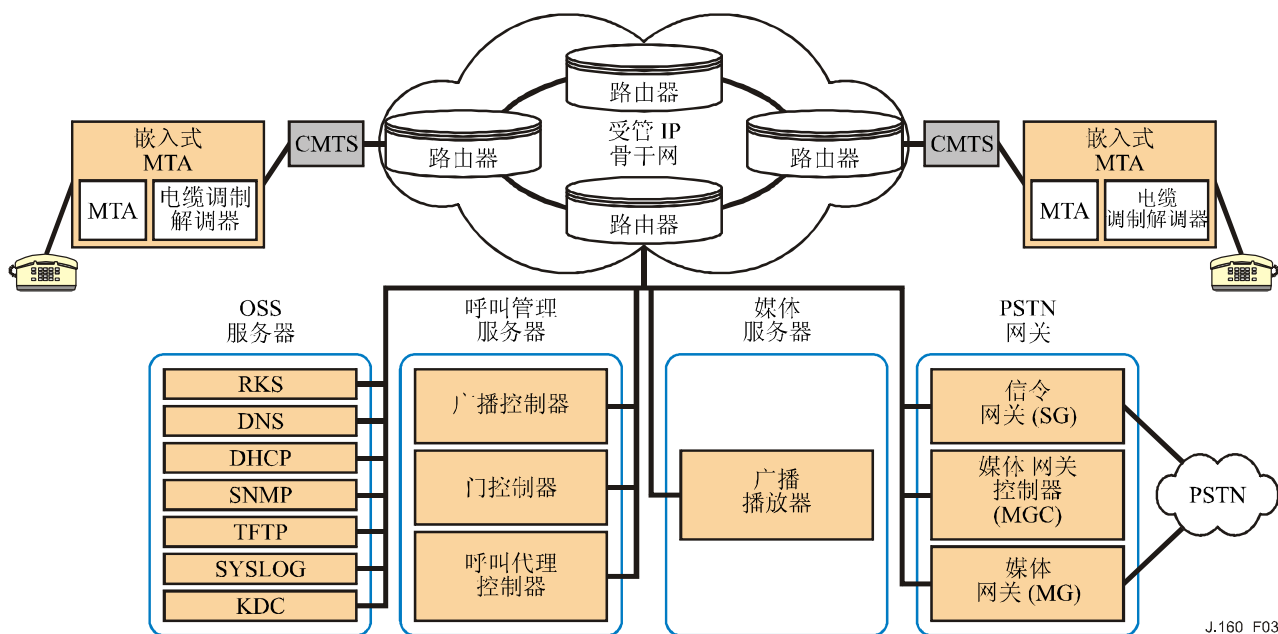


图3/J.160 – IPCablecom组件的参考模式

IPCablecom结构包含可信网元和不可信网元。可信网元通常位于电缆运营商的受管骨干网内。CM和MTA等不可信网元一般位于用户的家中和电缆运营商的设施之外。

6.1 媒体终端适配器 (MTA)

MTA是IPCablecom的客户端设备，其中包括连接用户CPE（如电话）的客户侧接口，以及网络侧与网络中呼叫控制网元相连的信令接口。MTA提供媒体传送和呼叫信令所需的编解码器、所有信令和封装功能。

MTA位于客户站点并通过HFC接入网与其它IPCablecom网元相连（ITU-T J.112建议书）。IPCablecom MTA需支持网络呼叫信令（NCS）协议（ITU-T J.162建议书）。

内嵌MTA（E-MTA）是一台包括电缆调制解调器和IPCablecom MTA组件的独立硬件设备。图4显示了具有代表性的E-MTA功能图。

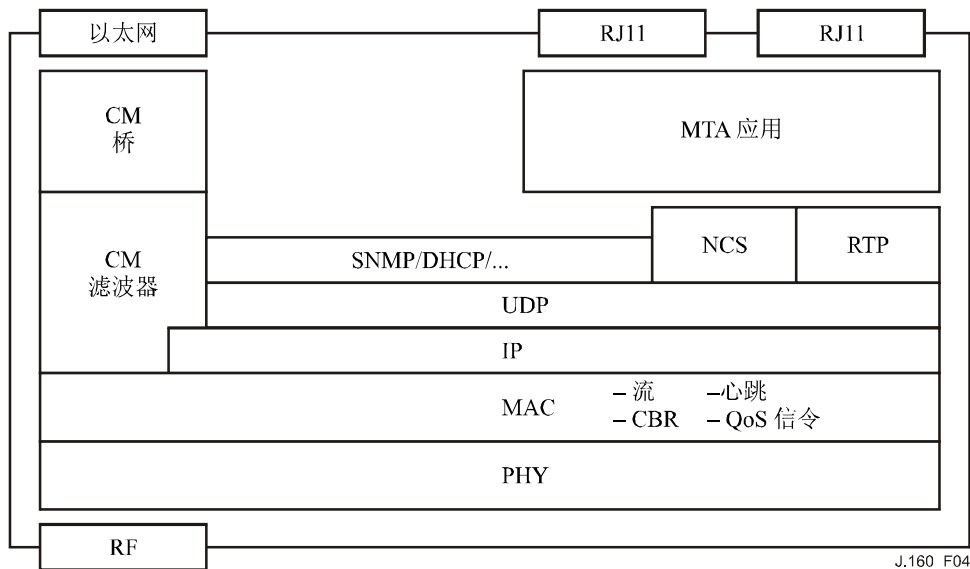


图4/J.160 – E-MTA概念功能结构

6.1.1 MTA功能需求

MTA具有如下功能：

- 与CMS之间的NCS呼叫信令。
- 与CMS和CMTS之间的QoS信令。
- MTA和其它IPCablecom网元间某些消息的鉴权、保密性和完整性。
- 将媒体流映射至DOCSIS接入网的MAC业务。
- 媒体流的编码/解码。
- 为电话提供多种音频提示，例如振铃音、呼叫等待音、特异拨号音、拨号音等。
- 可听音、话音传送、呼叫者识别信令、DTMF和消息等待指示符等的标准PSTN模拟线路信令。
- G.711音频编解码器和低比特率编解码器。
- 一个或多个模拟和/或ISDN BRI 接口。

其它IPCablecom建议书定义了附加MTA功能。

6.1.2 MTA属性

E-MTA具有以下属性：

- 嵌入式MTA有两个MAC地址：一个用于CM，另一个用于MTA。
- 嵌入式MTA有两个IP地址：一个用于CM，另一个用于MTA。
- 嵌入式MTA有两个完全限定域名（FQDN）：一个用于CM，另一个用于MTA。
- 每个配置的物理端口至少有一个电话号码。
- 设备能力。
- MTA相关的CMS。

6.2 电缆调制解调器 (CM)

CM是一台位于客户所在地内的、使用DOCSIS协议在有线网络上提供数据传输的调制器/解调器。在IPCablecom中，CM在处理媒体流和提供诸如按业务流对业务进行分类、速率整形和优先级排队等服务方面发挥着关键作用。

6.3 HFC接入网

基于IPCablecom的业务由混合光纤同轴网 (HFC) 的接入网承载。该接入网是一种双向、媒体共享的系统，其中包括CM、CMTS、DOCSIS MAC和PHY接入层。

6.4 电缆调制解调器终接系统 (CMTS)

CMTS通过HFC接入网为CM提供数据连接和补充功能。它还提供与广域网的连接。CMTS位于有线电视系统的前端或分配中枢。

CMTS具备如下功能：

- 根据与政策进行对照的DOCSIS的请求，为CM提供所需的QoS。
- 根据CM的请求和网络的QoS政策，分配上行带宽。
- 区分来自网络侧接口的所有数据包，并根据定义的滤波器规范为其指配一个QoS水平。
- 监管从有线网络接收的数据包的TOS字段，以便根据网络运营商的政策实施TOS字段的设置。
- 根据网络运营商的政策，改变下行IP数据包头的TOS字段。
- 根据流量规范的要求进行业务整形与监管。
- 使用指配的QoS将下行数据包前转至DOCSIS网络。
- 使用指配的QoS将上行数据包前转至骨干网设备。
- 将QoS门参数转换成DOCSIS QoS参数。
- 使用IPCablecom事件消息记录各个呼叫资源的使用情况。

6.4.1 CMTS门

CMTS负责根据MTA请求和门控制器的QoS授权，划分和规划上下行带宽。

CMTS在DOCSIS有线网络和IP骨干网之间安装IPCablecom动态QoS门或CMTS门。CMTS门是CMTS的功能组件，负责业务的划分并根据门控制器 (GC) 的规定对媒体流实施QoS政策。CMTS门由门控制器 (GC) 控制，该控制器是CMS内的逻辑QoS管理组件，负责协调所有服务质量的授权与控制。

6.5 呼叫管理服务器 (CMS)

呼叫管理服务器为IPCablecom网络中的MTA、CMTS和PSTN网关提供呼叫控制和与信令相关的服务。CMS是一个位于IPCablecom网络受控IP部分的可信网元。

IPCablecom CMS包括以下逻辑IPCablecom组件：

- **呼叫代理（CMS/CA）** – “呼叫代理”是一个通常可以与CMS互换的术语，特别是在MGCP中。在IPCablecom中，呼叫代理（CA）是指CMS的控制组件，它负责使用NCS协议为MTA提供信令服务（ITU-T J.162建议书）。在此情况下，呼叫代理的职责包括但不限于：
 - 实施呼叫功能；
 - 维持呼叫进程状态；
 - 在用户MTA设备内使用编解码器；
 - 收集并预处理已拨数字；
 - 对用户操作进行收集和分类；
 - 控制MTA对话音测量的使用。
- **门控制器（CMS/GC）** – 门控制器（GC）是CMS内负责协调服务质量授权与控制的逻辑QoS管理组件。门控制器的功能在动态服务质量建议书中进行了定义。

CMS可能还包括下述逻辑组件：

- **媒体网关控制器** –MGC是一种用于控制PSTN媒体网关的逻辑信令管理组件。本节后半部分将详细定义MGC功能。

CMS还可以提供下述功能：

- 呼叫管理和增强型功能；
- 目录业务和地址翻译；
- 呼叫路由；
- 记录本地号码携带业务的使用。

就本建议书而言，实施CMS功能的协议被确定为在CMS终接：而在实际实施时，可能会将此功能分配到呼叫管理服务器“后面”的一台或多台服务器。

6.6 PSTN网关

通过使用PSTN网关，IPCablecom可使MTA与当前的PSTN进行互操作。

为使运营商把成本降到最低并优化其PSTN互连协议，PSTN网关被分成了三个功能组件：

- **媒体网关控制器（MGC）** – MGC保持呼叫状态并控制PSTN网关的整体表现。
- **信令网关（SG）** – SG在PSTN SS7信令网和IP网之间提供信令互连功能。
- **媒体网关（MG）** – MG终接承载路径并在PSTN和IP网络间进行媒体变码。

6.6.1 媒体网关控制器（MGC）

媒体网关控制器（MGC）接收并协调IPCablecom网和PSTN之间的呼叫信令。它维持并控制需要PSTN连接的呼叫的整体呼叫状态。

MGC通过通知MG创建、修改和删除向IP网络上的媒体流提供支持的连接，对MG施加控制。MGC还指示MG检测并生成事件和信号，例如用于ISUP中继的连续性测试音。每个中继表现为一个端点。

下面列出了媒体网关控制器的一系列功能：

- **呼叫控制功能** – 维持并控制穿越PSTN网关那部分呼叫的整体PSTN网关呼叫状态。此功能以生成TCAP的方式，根据PSTN网关呼叫控制的需要与外部PSTN网元通信。
- **IPCablecom信令**– 终止和生成来自和发往IPCablecom侧网络的呼叫信令。
- **MG控制** – MG控制功能对媒体网关的端点实施整体控制：
 - 事件检测功能指示MG进行事件检测，例如检测端点、甚至可能是连接的带内音。
 - 信号生成功能指示MG在端点以及可能在连接上生成带内音和信号。
 - 连接控制功能指示MG如何对进出端点的连接进行基本处理。
 - 属性控制功能通知MG适用于端点和/或连接的属性，例如，编码方法、回声消除的使用、安全参数等。
- **外部资源监测** – 使MGC能够持续观测到外部可视的MG资源和数据包网络资源，例如端点可用性。
- **呼叫路由** – 做出呼叫路由决定。
- **安全性** – 确保所有与MGC通信的实体都遵守安全要求。
- **通过事件消息进行使用记录** – 记录每次呼叫中资源的使用情况。

6.6.2 媒体网关（MG）

媒体网关提供PSTN和IPCablecom网络之间的承载连接。每个承载均体现为一个端点，且MGC指示MG建立并控制与IPCablecom中其它端点的媒体连接。MGC还指示MG检测并生成与MGC所知呼叫状态相关的事件和信号。

6.6.2.1 媒体网关功能

下面列出了媒体网关执行的一系列功能：

- 终止和控制PSTN中以承载信道形式出现的物理电路。
- 根据MGC的请求检测端点和连接事件。
- 生成端点和连接的信号，例如MGC指示实施的连续性测试。
- 根据MGC的指示创建、修改和删除发往和来自其它端点的连接。
- 收到来自媒体网关控制器的请求后，控制并为特定连接指配内部媒体处理资源。
- 在PSTN和IPCablecom网络之间进行媒体代码转换。其中包括变码的各个方面，如编解码器、回声消除等。

- 确保与MG通信的所有实体都遵守安全规定。
- 确定相关资源的使用和与这些资源相关的属性，例如发送与接收的媒体字节数量。
- 向MGC报告资源的使用情况。

6.6.3 信令网关（SG）

信令网关功能可在IPCablecom网络的边缘发送和接收电路交换的网络信令。对于IPCablecom，信令网关功能只支持SS7形式的与设施无关的信令。

6.6.3.1 SS7 信令网关功能

下面列出了信令网关的一系列功能：

- 终接来自PSTN的SS7信令物理链路（A、F链路）。
- 实施安全功能，以确保网关的安全性符合IPCablecom和SS7对网络安全的要求。
- 终接消息传输部分（MTP）的第1、2和3层。
- 对所有SS7信令点实施MTP网络管理功能。
- 执行ISUP地址映射，以支持将点代码（同时包括目的地点代码和始发点代码）和/或SS7 ISUP消息中包含的点代码/CIC码的组合灵活地映射到相应的媒体网关控制器（MGC）（域名或IP地址）。编址的MGC将负责控制终接相应中继的媒体网关。
- 执行TCAP地址映射，以便将SS7 TCAP消息中的点代码/全局标题/SCCP子系统编号组合映射到相应媒体网关控制器或呼叫管理服务器。
- 在IPCablecom网中为某些可信实体（“TACP用户”）提供呼叫代理等机制，以便通过在SS7网络上发送的TCAP消息查询外部PSTN数据库。
- 实施在信令网关和媒体网关控制器间传送信令信息所需的传送协议。

6.7 OSS后台（back-office）组件

OSS 后台组件包括支持核心业务流程的业务、服务和网络管理组件。根据国际电联TMN框架的定义，OSS的主要工作范围包括故障管理、性能管理、安全管理、计费管理和配置管理。

IPCablecom定义了一套有限的OSS功能组件和接口，以支持MTA设备配置和承载计费信息的事件消息。

6.7.1 安全服务器 – 密钥分配中心（KDC）

对于IPCablecom，KDC这一术语用于Kerberos安全服务器。拥有公钥PKINIT扩展的Kerberos协议，用于MTA、CMS和配置服务器之间的密钥管理。

在通过PKINIT协议进行了MTA鉴权后，KDC将把Kerberos票据授予MTA。票据中包括用于MTA和CMS间（如果MTA将使用安全接口与CMS通信）呼叫信令安全性配置的信息，以及MTA和配置服务器（如果需要通过安全接口管理MTA）之间管理接口的信息。票据在如下时间发放：

- 在设备配置期间。在MTA重新启动而且保留票据仍然有效的情况下，MTA不必为从KDC申请新票据而执行PKINIT交换。
- 当票据过期时。在正常情况下，票据的有效期限约为一周。

6.7.2 动态主机配置协议（DHCP）服务器

DHCP服务器是一种后台网元，在MTA设备配置进程中用于动态划分IP地址和其它客户端配置信息。

6.7.3 域名系统（DNS）服务器

DNS服务器是一种用于在域名和IP地址之间进行映射的后台网元。

6.7.4 小文件传输协议或超文本传输协议服务器（TFTP或HTTP）

TFTP服务器一种后台网元，在MTA的配置过程中用于将配置文件下载至MTA。HTTP服务器可以替代TFTP服务器，用于将配置文件下载至MTA。

6.7.5 SYSLOG 服务器（SYSLOG）

SYSLOG服务器是一种可选后台网元，用于收集事件通知消息，对诸如设备出错等事件做出提示。

6.7.6 记录保存服务器（RKS）

RKS是一种可信网元组件，它接收来自CMS、CMTS、和MGC等其它可信IPCablecom网元的IPCablecom事件消息。RKS至少也可做为IPCablecom事件消息的一个短时存贮设备。RKS可将事件消息集中并将其组合成相关的集合或详细呼叫记录（CDR），再提供给计费或欺诈检测等其它后台系统。

6.8 通知服务器（ANS）

通知服务器是一种网络组件，它负责在网络中发生了某些事件后，管理和播放信息提示音和消息。通知服务器（ANS）这一逻辑实体由通知控制器（ANC）和通知播放器（ANP）组成。

6.8.1 通知控制器（ANC）

ANC发起并管理通知播放器提供的所有通知服务。ANC请求ANP根据CMS确定的呼叫状态播放通知。当由ANP从最终用户处收集信息时，ANC负责解释这一信息，并相应地管理这一会话。因此，ANC也可以管理呼叫状态。

6.8.2 通知播放器（ANP）

通知播放器是一种媒体资源服务器。它负责接收和解释ANC的命令，并向MTA播放相应的通知。ANP还负责接受和报告用户输入的内容（例如，DTMF音）。ANP在ANC的控制下工作。

7 协议接口

IP-Cablecom结构中大部分组件接口的协议规范都已制定。本节给出了各协议接口的概述。有关完整的协议要求，请查阅各IP-Cablecom建议书。

有些接口可能并未出现在特定厂商的产品实施当中。例如，如果IP-Cablecom的某些组件被组合在一起，则这些接口有可能成为该组件的内部接口。

7.1 呼叫信令接口

呼叫信令需要在IP-Cablecom结构内有多个接口。图5给出了这些接口。图中标出了每个接口，表2中又做了进一步描述。

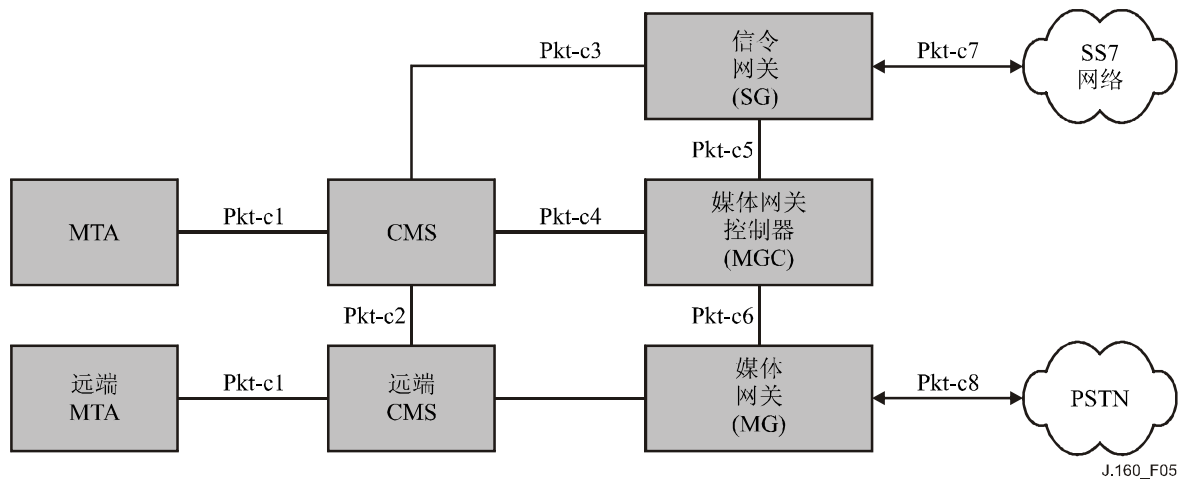


图 5/J.160 – 呼叫信令接口

表2/J.160 – 呼叫信令接口

接口	IP-Cablecom 功能组件	说明
Pkt-c1	MTA ↔ CMS	使用NCS协议（MGCP的一种特征）在MTA和CMS之间交换的呼叫信令消息。
Pkt-c2	CMS ↔ CMS	在CMS间交换的呼叫信令消息。此接口使用的协议为CMSS（ITU-T J.178建议书）。
Pkt-c3	CMS ↔ SG	CMS和SG之间交换的呼叫信令消息。
Pkt-c4	CMS ↔ MGC	CMS和MGC之间交换的呼叫信令消息。此接口使用的协议为CMSS。
Pkt-c5	SG ↔ MGC	MGC和SG之间交换的呼叫信令消息。
Pkt-c6	MGC ↔ MG	使用TGCP协议控制媒体网关的接口，该协议是一种与NCS相似的MGCP特征。

表2/J.160 –呼叫信令接口

接口	IPCablecom 功能组件	说明
Pkt-c7	SG ↔ SS7	SG终接来自PSTN（A、F链路）的SS7物理信令链路。支持下述协议： <ul style="list-style-type: none"> • ISUP 用户接口：为外部PSTN运营商提供SS7 ISUP信令接口。 • TCAP用户接口：在IPCablecom网中为某些可信实体（“TACP用户”）提供呼叫代理等机制，以便通过在SS7网络上发送的TCAP消息查询外部PSTN数据库。
Pkt-c8	MG ↔ PSTN	此接口定义媒体网关与PSTN之间的承载信道连接。

7.1.1 基于网络的呼叫信令（NCS）框架

IPCablecom基于网络的呼叫信令（NCS）协议（Pkt-c1）是IETF MGCP呼叫信令协议的扩展变体。NCS结构将呼叫状态和功能实施置于名为“呼叫管理服务器（CMS）”的集中式组件中，并将设备控制信息置于MTA内。MTA将设备事件发送至CMS，并对来自CMS的命令做出响应。可能含有多种地理或行政分布式系统的CMS，负责建立或断开呼叫，提供高级业务（增加型呼叫功能）、进行呼叫授权并生成计费事件记录等工作。

功能分配的实例包括，电话摘机后，CMS应指示MTA通知CMS，并确保输入了适当数量的DTMF数字。当这一系列事件发生时，MTA会通知CMS。此后，CMS可以指示MTA创建连接、通过接入网为处于等待状态的话音连接保留QoS资源、并播放本地生成的回铃音。CMS会相应地与远程CMS（或MGC）通信，以建立呼叫。当CMS从远端检测到应答后，它会指示MTA停止播放回铃音，以启动MTA与远端MTA之间的媒体连接，并开发始发送和接收媒体流数据包。

通过将呼叫和业务处理集中于CMS，业务供应商可以集中管理业务提供的可靠性。此外，在出现了影响用户业务的故障之后，业务提供商会获得所有软件和硬件的接入权。软件可以通过中央控制，并且可通过快速的调试和解决方案进行更新，而无需将外勤工作人员派至客户所在地。此外，业务提供商可以直接控制得到采用的服务，以及与这些业务相关的收入。

7.1.2 PSTN信令框架

表2（Pkt-c3至Pkt-c8）对PSTN信令接口做了总结。这些接口从IPCablecom网向基于PSTN的业务和PSTN用户提供接入。

IPCablecom PSTN信令框架包括一个由三个功能组件构成的PSTN网关：

- 媒体网关控制器（MGC）；
- 媒体网关（MG）；

- 信令网关 (SG)

媒体网关控制器和媒体网关分别类似于NCS框架中的CMS和MTA。媒体网关向PSTN提供承载和带内信令连接。媒体网关控制器实施所有呼叫状态和智能功能，并通过TGCP (J.171) 协议 (Pkt-c6) 控制媒体网关的操作。这包括连接的创建、修改和删除。TGCP是IETF MGCP呼叫信令协议的扩展变体。TGCP变体严格地与NCS保持一致。

CMS和MGC可能会通过SG (Pkt-c3和Pkt-c5) 分别向SS7业务控制点 (SCP) 发出路由查询 (如免费电话号码查询、LNP查询)。为进行中继管理和控制，MGC也通过SG与PSTN的SS7实体交换ISUP信令。

7.1.3 CMS间的信令框架

根据有关CMSS的ITU-T J.178建议书，IPCablecom支持域间和域内CMS-CMS和CMS-MGC信令。CMSS信令结构是以IETF会话发起协议 (SIP) (IETF RFC 3261) 为基础的。CMSS定义呼叫信令协议，但不负责网络中的路由选择。

CMS包括SIP用户代理客户机 (UAC) 和用户代理服务器 (UAS)。用户代理在整个呼叫过程中负责维持呼叫的状态，并监测MTA中影响呼叫的状态改变。CMS与MTA间的接口为NCS。建立新呼叫、或改变正在进行的呼叫的属性或参与方的CMSS消息，都是由CMS发起的。通常CMS也会通过来自MTA的信令被推入这一进程，例如通过接收通知已拨数字信息的NCS消息的方式。CMS包括门控制器 (GC) 功能。CMS的用户代理部分加入CMSS信令，而门控制器部分参加DQoS信令。它们共同控制呼叫建立和资源管理的信令协调。

7.2 媒体流

IETF的RTP标准 (RFC 1889, RTP: 实时应用的传输协议) 用于在IPCablecom网络中传输所有媒体流。IPCablecom根据IETF RFC 1890 (在最小控制情况下使用的音频视频会议RTP类别) 中的定义对音频和视频流使用RTP特征。

IPCablecom网络结构中使用的主要媒体流路径如图6所示，并在下文中作了进一步描述。

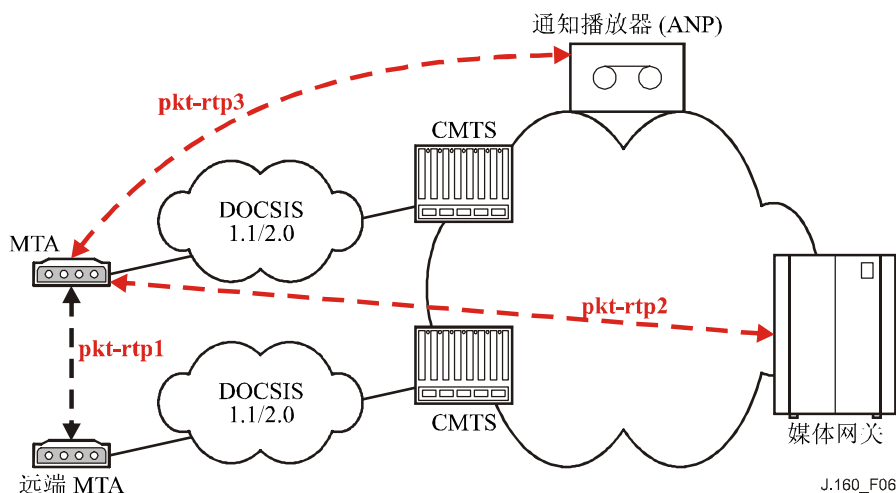


图 6/J.160 – IP-Cablecom网络中的RTP媒体流

表3/J.160 – RTP媒体流

接口	IP-Cablecom 功能组件	说明
pkt-rtp1	MTA ↔ MTA	MTA间的媒体流，包括编码语音和传真等。
pkt-rtp2	MTA ↔ MG	MG和MTA间的媒体流，包括音频、通知和PSTN媒体流。
pkt-rtp3	MTA ↔ ANP	ANP和MTA间的媒体流，包括由通知播放器发送到MTA的信号音和通知。

RTP在单一的方向编码单一信道的多媒体信息。在各RTP报头中，7比特有效负荷类型（PT）可以说明有效负荷数据包中使用了哪种编码算法（例如G.711）。大部分普通音频算法均被指配给特定的有效负荷类型，其取值范围为0至95。96至127是预留给“动态”RTP有效负荷类型的，且其中编码算法与有效负荷类型之间的绑定是通过信令建立的。

图7描述了通过以太网IP发送的RTP数据的数据包格式。



图 7/J.160 – RTP数据包格式

RTP有效负荷的长度以及数据包发送使用的频率取决于有效负荷类型字段中定义的加密算法。

RTP会话由相关端点动态建立，因此接收RTP信息不存在“众所周知”UDP端口号。由IETF制定的会话描述协议（SDP）旨在通知某特定RTP会话使用的特定IP地址和UDP端口。NCS和TGCP都使用SDP。

对于使用数据包的话音，RTP有效负荷可以小到10字节，因此以太网数据包、IP、UDP和RTP的报头开销与之相比要大许多。DOCSIS建议书处理这一问题的方式是使用有效负荷压缩功能对公共报头进行压缩。

ITU-T T.38建议书也被用于在IPCablecom网中传输传真媒体，详细信息请参见第8.7节。

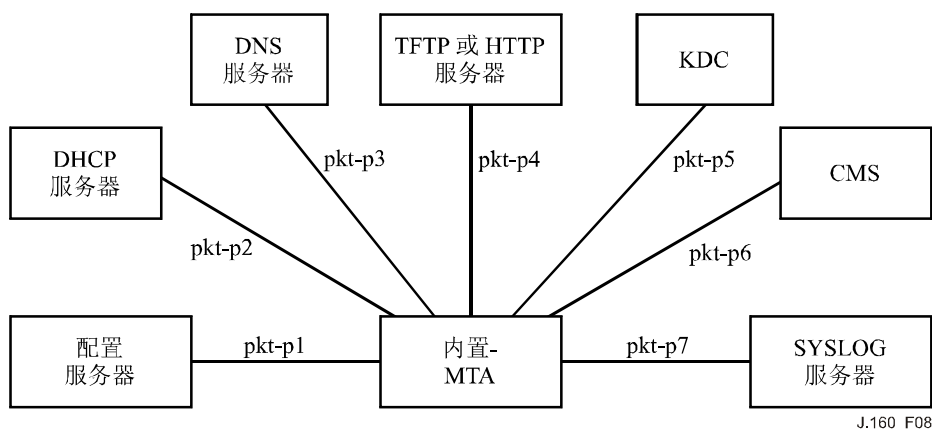
7.2.1 实时传输控制协议（RTCP）

RTCP在IETF RFC 1889中给出了定义。该协议是基于使用与数据包相同的分发机制，定期向会话中的所有参与方发送控制包。RTCP提供对数据分发质量的反馈。这是RTP作为传输协议的必不可少的组成部分，并且与其它传输协议的流和阻塞控制功能相关。IPCablecom支持对所有端点使用RTCP。

对RTCP进行的扩展是为了为更好地评估语音呼叫的质量，并更有效地诊断网络中出现的问题。这些扩展被称为RTCP扩展报告（RTCP XR），并在IETF RFC 3611中进行了定义。RTCP XR包括多种测量标准。IPCablecom只在各端点支持RTCP XR语音测量标准。

7.3 MTA设备配置

MTA设备配置使MTA能够在运营商网络注册，并通过HFC网络提供用户业务。配置涵盖了MTA设备配置所需的初始化、鉴权和注册功能。配置建议书还包括MTA配置文件需要的属性定义（见图8）。



J.160_F08

图 8/J.160 – IP-Cablecom配置接口

表4 描述了图8所示的配置接口。

表4/J.160 – 设备配置接口

接口	IP-Cablecom 功能组件	说明
Pkt-p1	MTA ↔ PROV 服务器	交换设备容量、以及在MTA和使用SNMP协议的配置服务器间交换MTA设备和端点信息的接口。MTA还将在发送配置已经完成的通知的同时，使用SNMP协议发送通过 / 失败状态。
Pkt-p2	MTA ↔ DHCP 服务器	MTA和DHCP服务器间的DHCP接口，用于为MTA指配IP地址，并在MTA附着于网络时，提供额外的低级别信息。
Pkt-p3	MTA ↔ DNS 服务器	MTA和DNS服务器间的DNS接口，用于获取具有完全限定域名的IP-Cablecom服务器的IP地址。
Pkt-p4	MTA ↔ HTTP 或 TFTP 服务器	MTA配置文件从TFTP服务器或HTTP服务器下载到MTA。
Pkt-p5	MTA ↔ KDC	MTA使用Kerberos协议从密钥分配中心获得Kerberos票据。
Pkt-p6	MTA ↔ CMS	MTA使用Kerberos协议与CMS建立IPsec安全关联。
Pkt-p7	MTA ↔ SYSLOG	MTA将网络事件通知发送到SYSLOG服务器的接口，其中包括与设备配置状态相关的信息。

7.4 SNMP 网元管理层接口

IP-Cablecom要求SNMP将MTA与网元管理系统连接，以进行MTA设备配置。支持SNMPv3中用于事件处理的“陷阱”和“通知”，以及配置中的“设置”和“获取”。IP-Cablecom NCS MIB包括以设备和各端点为基础进行配置的网络呼叫信令信息。MTA MIB中包含设备配置数据和事件日志等支持配置功能的数据。有关MIB的更多详细信息，请参见IP-Cablecom MIB框架建议书（ITU-T J.166建议书）。

7.5 事件消息接口

7.5.1 事件消息框架

事件消息是一种包含网络使用和活动信息的数据记录。单独的事件消息可以包含有关使用的一套完整数据，也可能只包括全部使用信息的一部分。在与记录保存服务器（RKS）结合使用时，多条事件消息中包含的信息，提供了呼叫中使用服务的完整记录。这一完整的服务记录通常被称为详细呼叫记录（CDR）。事件消息或CDR可以被发送至一个或多个后台应用，例如计费系统、欺诈检测系统或预付费业务处理器。

此IPcablecom事件消息建议书（ITU-T J.164建议书）定义了事件消息数据记录的结构，并将RADIUS定义为传输协议。事件消息数据记录的格式设计十分灵活并能够扩展，以便为广泛的业务承载网络使用信息。图9显示了具有代表性的事件消息结构。

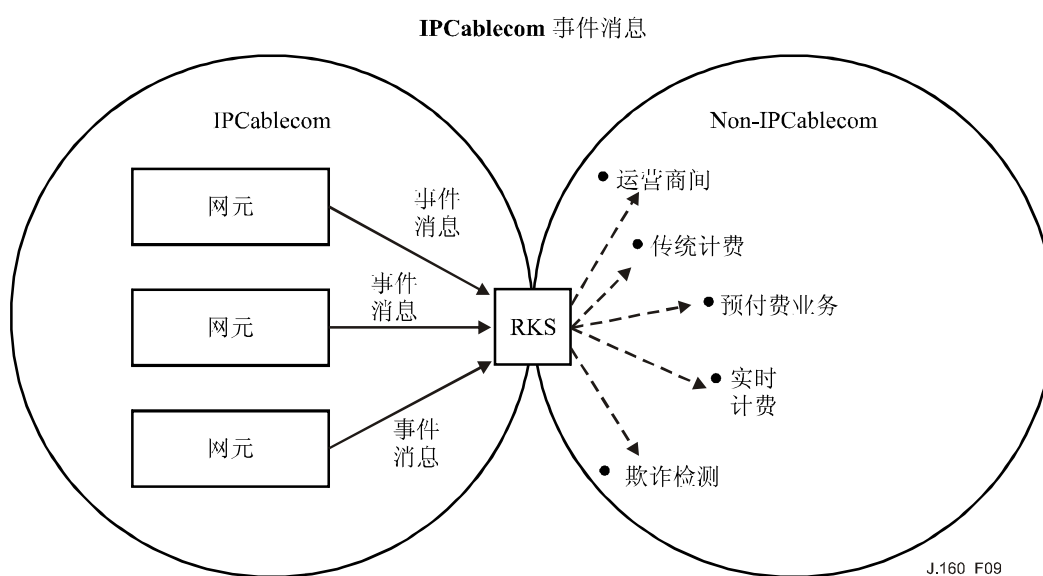
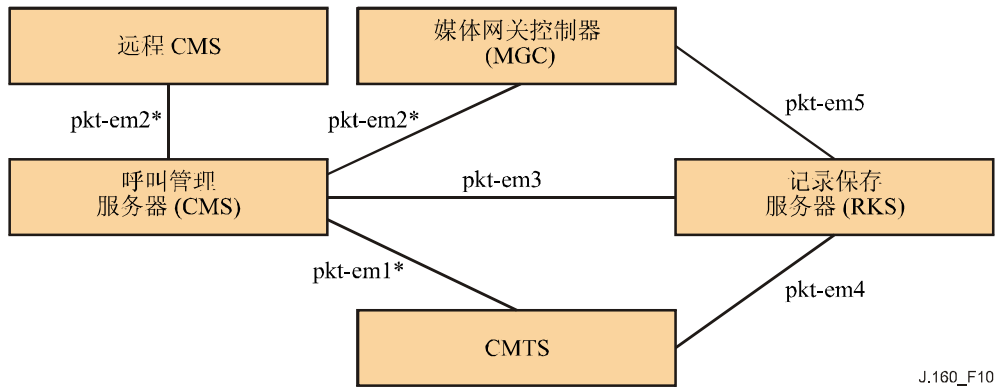


图9/J.160 – 有代表性的事件消息结构

表5描述了图10所示的事件消息接口。

表 5/J.160 – 事件消息接口

接口	IPcablecom 功能组件	说明
Pkt-em1	CMS ↔ CMTS	载有CMTS向RKS发送事件消息所需的计费关联ID和其它数据的DQoS Gate-Set 消息。
Pkt-em2	CMS ↔ MGC CMS ↔ CMS	此接口使用的协议为CMSS，用于承载计费相关ID和计费数据所需的其它数据。
Pkt-em3	CMS ↔ RKS	承载IPcablecom事件消息的RADIUS协议。
Pkt-em4	CMTS ↔ RKS	承载IPcablecom事件消息的RADIUS协议。
Pkt-em5	MGC ↔ RKS	承载IPcablecom事件消息的RADIUS协议。



J.160_F10

注 - * 指利用现有信令接口承载用于其它EM接口的数据

图 10/J.160 – 事件消息接口

7.6 服务质量 (QoS)

7.6.1 QoS 框架

IPCablecom QoS框架如图11所示:

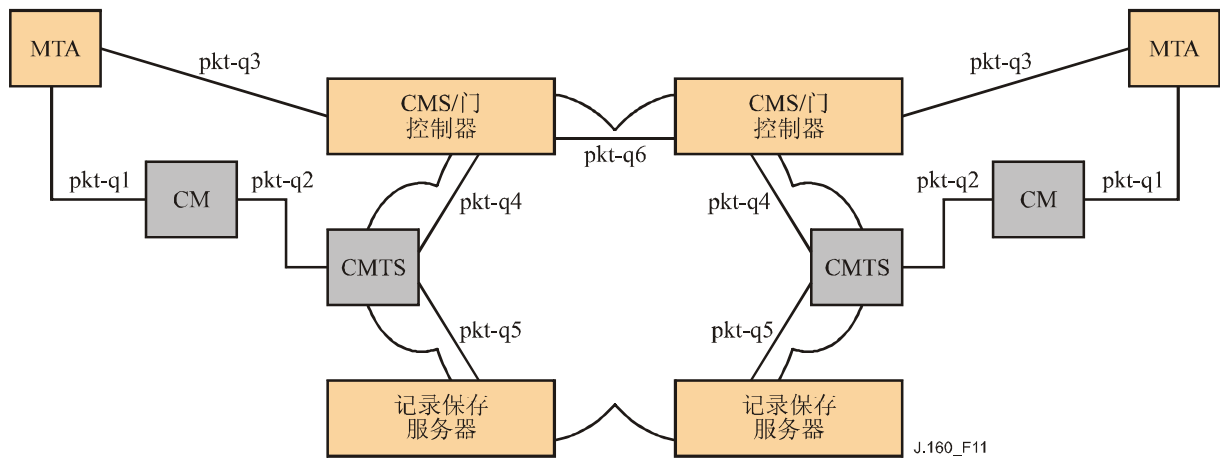


图11/J.160 – IPCablecom QoS信令接口

表6简单描述了各个接口以及各接口在动态QoS建议书中的用法 (DQoS/ITU-T J.163建议书)。

表 6/J.160 – QoS接口

接口	IPCablecom功能组件	DQoS说明
Pkt-q1	MTA ↔ CM	E-MTA、MAC控制业务接口
Pkt-q2	CM ↔ CMTS	J.112, CM始发
Pkt-q3	MTA ↔ CMS	NCS
Pkt-q4	GC ↔ CMTS	门管理
Pkt-q5	CMTS ↔ RKS	计费
Pkt-q6	CMS ↔ CMS	会话建立

表7进一步描述了各QoS接口的功能。

表7/J.160 – QoS接口

接口	IPCablecom功能组件	说明
Pkt-q1	MTA ↔ CM	<p>此接口可分为三个子接口：</p> <p>控制：用于管理DOCSIS业务流和与其相关的QoS业务参数与分类规则。</p> <p>同步：用于使数据包日程安排同步化，以最大限度减少延时和抖动。</p> <p>传输：用于处理媒体流中的数据包并执行相应的各数据包QoS处理。</p> <p>MTA/CM接口在ITU-T J.112建议书中进行了概念性定义。</p>
Pkt-q2	CM ↔ CMTS	<p>此为DOCSIS QoS接口（控制、计划和传输）。应注意，就结构而言，控制功能仅能从CM发起。CMTS是最终的政策评判者和进入DOCSIS接入网的授权者。在IPCablecom内使用DOCSIS MAC的下述功能：</p> <ul style="list-style-type: none"> • 多业务流，分属不同类别的上行业务，各DOCSIS业务流中同时存在单一和多重语音连接。 • 业务流程中业务流的优先级分类。 • 有保证的最小 / 恒定比特率规划服务。 • 业务活动检测服务的恒定比特率规划（减速、加速、停止和重启计划）。 • 增强呼叫密度的DOCSIS数据包报头压缩。 • 业务流中的话音流DOCSIS分类。 • CMTS时钟和批准间隔的编解码器DOCSIS同步。 • QoS资源的两相激活。 • 网络层的TOS数据包标记。 • 延迟与抖动的保障。 • IPCablecom MTA和CM（内嵌式MTA）之间的内部子层信令。 <p>此接口在ITU-T J.112建议书中做了进一步定义。</p>

表7/J.160 – QoS接口

接口	IPCablecom 功能组件	说明
Pkt-q3	MTA ↔ CMS	MTA和CMS间的信令接口。许多参数都是通过此接口发出信号，例如媒体流、IP地址、端口编号、编解码器的选择和打包。
Pkt-q4	CMS ↔ CMTS	此接口用于管理媒体流会话的动态门。此接口使IPCablecom网络能够请求并授权QoS。
Pkt-q5	CMTS ↔ RKS	CMTS使用此接口报告呼叫使用的QoS资源变化情况。事件消息建议书中定义了此接口。
Pkt-q6	CMS ↔ CMS	此接口用于建立域内和域间会话。此接口中包括的功能可以确保在呼叫完成之前，连接两端的QoS资源可用。

7.6.2 动态服务质量

IPCablecom动态QoS（DQoS）在呼叫期间使用呼叫信令信息来为呼叫进行动态资源授权。通过QoS消息与其它协议和网元的集成，动态QoS可以防止各种类型的业务盗窃攻击。动态QoS控制所需的网元如图11所示。

CMTS内定义业务类别和媒体流QoS政策的逻辑实体称为门。CMS的门控制器单元管理IPCablecom媒体流的门。下述关键信息包括在GC和CMTS间的信令中：

最大允许QoS包络 – 最大允许QoS包络定义了MTA可为某特定媒体流的承载流请求的最大QoS资源数量（例如，“每10 ms批准两次，共160字节”）。如果MTA请求的值大于包络中包含的参数，该请求将被拒绝。

媒体流端点的标识 – GC/CMS授权媒体流承载流程涉及的相关方。通过此信息，CMTS可以监管数据流，以确保数据流流向或发自被授权的相关方。

计费信息的目的地 – GC/CMS将该呼叫的主辅记录保存服务器标识通知CMTS，并提供唯一的计费标识，使跨多个网元的记录能够建立相关性。

各IPCablecom组件在实施DQoS时的作用如下：

呼叫管理服务器/门控制器 – CMS/GC负责QoS授权。QoS授权可能取决于呼叫类型、用户类型或政策定义的其它参数。CMS/GC还用CMSS来确保在域内和域间呼叫时，呼叫两端的QoS资源均可使用。

CMTS – 利用CMS/GC提供的信息，CMTS应QoS的请求实施准入控制，并在此后对准入的数据流进行监管，以确保该数据流的来源和目的地与被授权作为流端点的各方匹配。CMTS与MTA的CM部分和RKS互操作。与这些网元相关的CMTS的职责包括：

- **记录保存服务器的CMTS**– 每当特定呼叫的CMTS与MTA之间的QoS发生变化时，CMTS都会通知记录保存服务器（RKS）。
- **MTA的CMTS** – MTA提出创建和修改与承载电路业务承载的DOCSIS动态业务流相关的QoS业务参数请求。当CMTS接收到请求后，它会检查请求的特性是否在授权QoS包络之内，并检查媒体流端点是否被授权承载此业务。检查成功后，CMTS会相应地创建或修改动态业务流。

记录保存服务器（RKS）–RKS接收CMTS发出的各个事件（以事件消息的形式）。RKS通常具有与一个或多个后端系统相连的接口，并在将从CMTS接收到的信息重新格式化后前转至其它系统。

MTA – MTA是一种由CMTS提供业务级协议的实体。MTA负责QoS链路的恰当使用（由于MTA是不可信设备，CMTS负责保证使用得当）。如果MTA试图超出服务级协议授权的业务包络，则CMTS确保MTA不会收到超出其请求的QoS。

7.7 CMS用户配置

CMS用户配置建议书通过定义配置服务器（或经授权的后台组件）与CMS之间的接口提供了一种自动激活业务的方法。CMS用户配置的框架如图12所示。

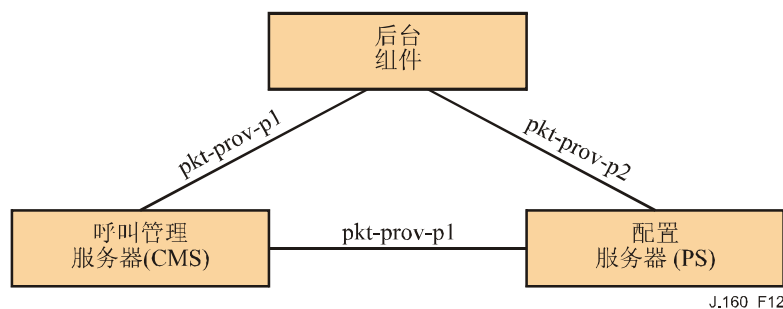


图12/J.160 – CMS用户配置接口

表8中进一步描述了各CMS用户配置接口的功能。

表8/J.160 – CMS用户配置接口

接口	功能组件	说明
pkt-prov-p1	PS-CMS Back-office-CMS	此为CMS用户配置接口。可以通过PS或经授权的后台（Back Office）组件提供用户信息。
pkt-prov-p2	Back-office-PS	此接口允许后台组件与配置服务器交换信息。此接口并未在IPCablecom中定义。

用户配置包括：

- **客户记录/计费支持**– 建立客户记录，其中包括与提供服务、计费以及从客户处收费的信息。客户记录创建/计费被视为后台OSS应用的一部分，但目前超出了IPCablecom的范围。
- **设备安装/配置**–可能包括设备的物理安装和/或连接以及任何软件和/或为向客户提供服务而进行的数据库更新。就CMS用户配置接口而言，设备设置会影响CMS。CMS自身的配置分为两个主要领域：
 - **基本普通老式电话（POTS）配置（BPP）**–BPP在IPCablecom网络中向CMS提供简单电话业务路由所需的最低限度的数据。这一最低限度的数据中包含映射到相关MTA FQDN和NCS端点标识符的电话号码。此数据将用于建立翻译表，使CMS能够将呼叫路由到相应的、给出特定电话号码的设备/端口。在客户能够从IPCablecom网络接收任何呼叫之前，需对所有客户进行BPP配置。
 - **呼叫功能配置（CFP）**–除BPP外，CFP可为客户提供呼叫功能。CFP比BPP更复杂，因为通过的参数既可能会因各特性不同而有所差异，也可能取决于各厂商自己的实施情况。

7.8 电子监视

IPCablecom的电子监视框架能够实现对其网络的合法授权的电子监视（LAES）。IPCablecom支持将呼叫数据和呼叫内容传送到执法机构（LEA）。呼叫数据和呼叫内容被从网络的不同部分送到交付功能（DF）。DF负责集成呼叫数据和呼叫内容，然后将其交给相应的LEA。LEA作为收集功能，负责从DF收集呼叫数据和呼叫内容。

IPCablecom仅定义执行电子监视的机制，但不定义实施电子监视命令的方式（即，IPCablecom运营商接受并在网络中进行配置）。

IPCablecom电子监视的框架如图13所示。

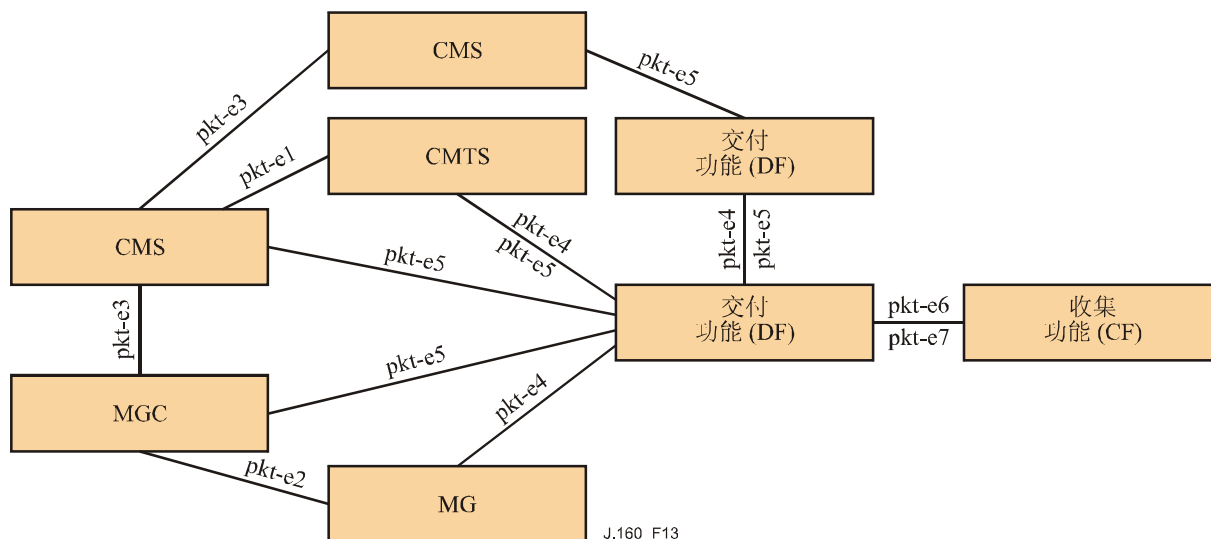


图13/J.160 – 电子监视接口

表9进一步描述了各电子监视接口的功能。

表 9/J.160 – 电子监视接口

接口	IPCablecom 功能组件	说明
pkt-e1	CMS ↔ CMTS	此为COPS DQoS接口，允许CMS进行呼叫数据和呼叫内容监视。
pkt-e2	MGC ↔ MG	此为TGCP接口，允许MGC命令MG执行电子监视。
pkt-e3	CMS ↔ CMS CMS ↔ MGC	此为CMSS接口，在某些域内和域间呼叫的情况下，支持发出电子监视需求通知的能力（例如，主题前转呼叫）。
pkt-e4	CMTS ↔ DF MG ↔ DF DF ↔ DF	此接口是基于IPCablecom事件消息，并被用于从IPCablecom组件向DF或从DF向DF交付呼叫数据。
pkt-e5	CMTS ↔ DF MGC ↔ DF DF ↔ DF CMS ↔ DF	此接口用于以封装RTP数据包的形式，从IPCablecom组件向DF或从DF向DF交付呼叫内容。
pkt-e6	DF ↔ CF	此接口用于向CF交付呼叫数据。
pkt-e7	DF ↔ CF	此接口用于向CF交付呼叫内容。

7.9 安全性

7.9.1 概述

每个IPCablecom协议接口都会受到可能危及用户和业务提供商的安全威胁。IPCablecom结构通过为各定义的接口协议规定提供其所需的安全性服务的下层安全机制（例如IPsec），来消除这些威胁。

对于大部分接口，IPSec要求使用定义的安全机制；对一些接口，该结构允许运营商使用不安全的链路，尽管这样做会使运营商把用户和其自身置于攻击之下，而当使用IPSec安全性建议书中定义的机制时，这些链路不会受到攻击（ITU-T J.170建议书）。

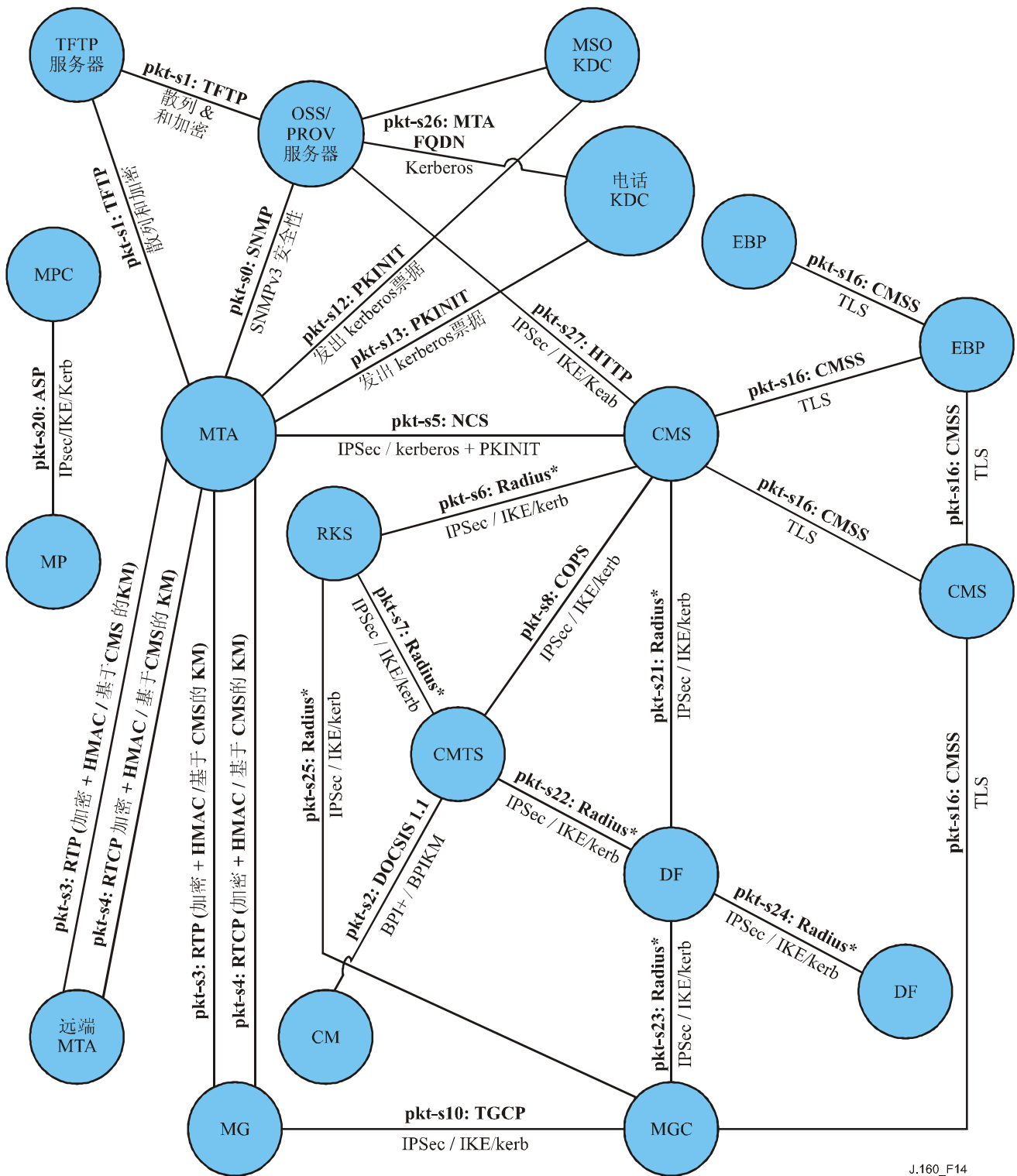
可通过IPSec核心业务层获得的安全业务包括鉴权、接入控制、完整性和保密性。IPSec协议接口可能使用零个、一个或多个此类业务来满足特定的安全性需求。

IPSec安全性功能通过下述方式来满足各协议接口的安全性要求：

- 确定各协议接口各自的威胁模式；
- 确定应对已发现的威胁所需的安全性业务（鉴权、授权、保密性、完整性和不可否认性）；
- 规范特定的能够提供所需安全性业务的安全机制。

安全性机制包括安全协议（例如，IPsec、RTP层安全性或SNMPv3安全性）和支持性密钥管理协议（例如，IKE或PKINIT/Kerberos）。

图14对IPSec所有安全接口作了总结。



J.160_F14

4/J.160 – IP图1Cablecom安全性接口

在图14中，各接口被标为：

<标记>: <协议> { <安全性协议> / <密钥管理协议> }

如果没有密钥管理协议，则意味着该接口不需要此协议。无需安全性的IPCablecom接口未在图14中显示。

表10描述了图14中的各个接口。

表10/J.160 – 安全性接口

接口	IP Cablecom 功能组件	说明
Pkt-s0	MTA ↔ PS/OSS	在安全配置流的DHCP序列后，MTA会立即在配置服务器中执行基于Kerberos的密钥管理，以建立SNMPv3密钥。MTA绕过Kerberized SNMPv3，并使用基本与混合流中的SNMPv2c。
Pkt-s1	MTA ↔ TFTP 或 PS/OSS	MTA配置文件下载。当安全配置流中的安全配置服务器向MTA发送SNMP Set命令后，它会同时包括配置文件的文件名和文件的散列。其后，当MTA下载文件时，它会使用散列值对配置文件进行鉴权。配置文件可以加密。也可以用HTTP取代TFTP。
Pkt-s2	CM ↔ CMTS	此接口应使用BPI密钥管理，通过BPI+提供安全性保障。HFC链路提供BPI+私密性。
Pkt-s3	MTA ↔ MTA MTA ↔ MG	RTP：两个MTA或MTA与MG间的端到端媒体包。RTP包直接使用所选密码进行加密。可选的消息完整性由MMH MAC提供。密钥随机生成，并在信令消息内的两个端点之间通过CMS或其它应用服务器进行交换。
Pkt-s4	MTA ↔ MTA MTA ↔ MG	RTP的RTCP控制协议。通过选择的密码确保消息的完整性和加密。使用在RTP密钥管理期间获得的相同密码，提供RTCP密钥。不需要或使用额外的密钥管理消息。
Pkt-s5	MTA ↔ CMS	NCS。通过IPsec确保消息的完整性和私密性。密钥管理使用带PKINIT扩展（公钥初始鉴权）的Kerberos。
Pkt-s6	RKS ↔ CMS	RADIUS: IPsec用于消息的完整性和私密性。密钥管理为IKE或Kerberos。
Pkt-s7	CMTS ↔ RKS	Radius、IPsec可用于消息的完整性和私密性。密钥管理为IKE-或Kerberos。
Pkt-s8	CMS ↔ CMTS	GC和CMTS之间的COPS协议，用于将QoS授权下载至CMTS。IPsec.密钥管理提供的消息完整性和私密性为IKE-或Kerberos。
Pkt-s10	MGC ↔ MG	TGCP: IP Cablecom 与PSTN媒体网关的接口。IPsec用于消息的完整性和私密性。密钥管理使用IKE-或Kerberos。
Pkt-s12	MTA ↔ MSO KDC	PKINIT：与用于鉴权的公钥加密一同发往KDC的AS-REQ消息。KDC 核准该证书，并根据AS请求的内容，颁发业务票据或票据授予票据（TGT）。KDC返回的AS 应答包括MTA用来对此消息进行鉴权的证书链和数字签名。当KDC返回TGT时，MTA会向KDC发送一个TGS请求，而KDC会对此作出内容包含业务票据的TGS应答。对TGS请求/应答消息的鉴权是利用TGT内的对称会话密钥进行的。

接口	IPCablecom 功能组件	说明
pkt-s13	MTA ↔ 电话KDC	PKINIT: 见pkt-s12。此接口单独显示，因为独立的KDC可用于电话业务的鉴权服务。
pkt-s16	CMS ↔ CMS CMS ↔ MGC CMS ↔ EBP EBP ↔ EBP	SIP: TLS可用于消息的完整性和私密性。证书在TLS握手期间被用于相互鉴权。
pkt-s20	MPC ↔ MP	ASP: IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。
pkt-s21	DF ↔ CMS	RADIUS: IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。
pkt-s22	DF ↔ CMTS	RADIUS: IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。
pkt-s23	DF ↔ MGC	RADIUS: IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。
pkt-s24	DF ↔ DF	RADIUS: IPsec用于消息的完整性和私密性。密钥管理使用IKE+。
pkt-s25	RKS ↔ MGC	RADIUS: IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。
pkt-s26	OSS/Prov 服务器 ↔ MSO KDC OSS/Prov 服务器 ↔ 电话KDC	KDC使用Kerberos将MTA的MAC地址映射到FQDN，以便在颁发票据前对MTA进行鉴权。
Pkt-s27	CMS ↔ PS/OSS	HTTP. IPsec用于消息的完整性和私密性。密钥管理使用IKE或Kerberos。

7.9.2 设备配置的安全性

IPCablecom允许用非安全模式和安全模式进行设备配置。IPCablecom还允许在MTA已进行安全配置的情况下使用非安全模式的SNMPv2管理。鉴于本建议书的此节专门讨论安全性，我们假设网络在安全模式下运行。

IPCablecom安全结构将设备配置分为三种不同活动：用户接纳、设备配置和设备授权。

7.9.2.1 用户接纳

用户接纳程序建立了一个永久性的用户计费帐户，它可以通过MTA的MAC地址确定CMS唯一的MTA。计费帐户还用于确定用户签约的MTA业务。

用户接纳可以在带内或带外进行。用户接纳流程的实际规范不在IPCablecom的范围之内，且可能会因业务提供商不同而异。

7.9.2.2 设备配置

MTA设备利用Kerberos的PKINIT扩展实施KDC鉴权。在检查了鉴权证书并确保后端配置系统能够识别此MTA后，KDC会为配置服务器颁发票据。MTA使用该票据，以安全的方式与配置服务器交换SNMPv3密钥。一旦SNMPv3会话已经建立，MTA会从TFTP或HTTP请求其配置文件（配置文件已经鉴权且可能被加密）。

7.9.2.3 动态配置

SNMPv3安全性将用于动态配置和管理MTA的话音通信能力和MTA的其它方面。

7.9.2.4 设备授权

设备授权是在配置的MTA设备通过鉴权进入呼叫服务器时，以及在其完全进入工作状态前与该服务器建立安全关联时进行的。设备授权允许根据已建立的安全性关联保护后续的呼叫信令。

MTA设备利用Kerberos的PKINIT扩展实施KDC鉴权。在检查了鉴权证书并确保后端配置系统能够识别此MTA后，KDC会为CMS颁发票据。MTA使用票据以安全方式建立通向CMS的IPsec管道。IPsec可以使用零加密，此时NCS信令消息在此接口上以不加密的形式传送。

7.9.2.5 信令的安全性

包括QoS信令、呼叫信令和PSTN网关接口信令在内的所有信令业务，都通过IPsec管道传输。IPsec安全关联管理是使用Kerberos与IKE的某些组合进行的。具有PKINIT扩展的Kerberos，被用于在MTA客户机与其CMS服务器之间交换密钥；IKE，或Kerberos，将用于管理所有其它信令IPsec SA。

7.9.2.6 媒体流安全性

在呼叫建立阶段，MTA通过协商为承载电路流制定一种特别加密算法。设备至少需要能够支持零加密和AES加密。加密被用于RTP包的有效负荷，但未被用于其报头。

基于MMH算法，各RTP包可能包括可选的消息鉴权码（MAC）。MAC计算包括数据包未加密的报头和加密的（或未加密的）有效负荷。

加密和MAC计算的密钥来自一个密码，作为呼叫建立时呼叫信令的一部分，该密码在发送与接收MTA之间交换。这样，媒体流安全性的密钥交换，将由负责保证呼叫信令IPsec传输的安全性等级来确保。

7.9.2.7 OSS和计费系统安全性

IPcablecom MTA中的SNMP代理在安全模式下使用SNMPv3。SNMPv3用户安全性模式（RFC 3414）为SNMP业务提供鉴权和私密性服务。SNMPv3可视接入控制（RFC 3415）可用于MIB对象的接入控制。

IKE或Kerberos密钥管理协议用于在记录保存服务器（RKS）和各生成事件消息的IPcablecom网元之间建立加密和鉴权密钥。符合PacketCable安全性建议书规定的设备需使用有预共享密钥的IKE；这些设备也可能会使用允许厂商实施全面自动化密钥变更机制的、具备证书或Kerberos的IKE。事件消息通过由IPsec确保安全性的RADIUS传输协议从CMS和CMTS发送到RKS。

8 网络设计考虑

8.1 计时和报告问题

为保持服务的质量，强烈建议所有网络设备时钟的误差不超过200毫秒协调世界时（UTC）。发送事件消息的设备需保持与网络时间协议（NTP）（根据RFC 1119）的时间同步。

建议在IPCablecom网络中，保证有一个能够在特定协调世界时（NTC）时间段保持准确的时钟。

8.2 执行缓冲器与编码速率间的时间匹配

数据包生成与处理设备一般使用自由运行的时钟。由于这些时钟的准同步属性，在提供同步业务时可能会出现时差问题。这些准同步实体间的时钟速率差别，通常会体现为缓冲区的超载运行或欠载运行。

为将这些条件出现的频率降至最低，所有CMTS都应将其下行传输速率与反映第3层时钟情况的时钟锁定。MTA应使用下行传输速率来获取用于确定打包时间段的时钟。MTA还应使用这一时钟来确定接收缓冲器的执行速率。

8.3 IP寻址

MTA是一个多功能实体，其中一个为CM管理所需的功能，另一个为MTA自身的功能。

所有IPCablecom MTA都需要有两个IP地址—一个用于CM，另一个用于MTA。所有IPCablecom 内嵌式MTA都需要有两个MAC地址—一个用于CM，另一个用于MTA。IPCablecom仅支持IPv4地址。

使用双IP地址配置可以满足下述要求：

- 如果未在IPCablecom网络的其它部分提供NAT，则IPCablecom运营商可以为CM主机功能指配一个专用IP地址。
- 每个MTA使用两个IP地址，IPCablecom运营商可以通过语音骨干网路由语音业务数据包，而通过数据骨干网路由所有其它数据包（数据）。在这种情况下，路由骨干网的配置必须保证两个目的地IP地址遵循不同的路径。
- IPCablecom运营商可以使用独立的IP地址，简化网络侧的管理。例如，可以使用策略筛选程序阻止或允许提供来自该设备MTA组件的业务。此外，网络业务提供商可以提供资源地址屏蔽业务，且可以根据MTA的IP地址诊断并收集网络业务数据。

关于双IP地址会对以下内容产生影响的特别考虑：

- MTA的IP协议栈实施；
- IPCablecom OSS和设备配置协议的实施；
- 网络路由实施。

8.4 动态IP寻址指配

无论对于设备配置和管理还是各类协议操作，都存在一种为MTA动态指配IP地址的操作要求。NCS建议书（ITU-T J.162建议书）规范的呼叫信令模式，是基于呼叫管理服务器将用户业务映射到端点标识符和MTA完全限定域名（FQDN）的能力。如果指配给MTA的地址在有效呼叫期间发生变化，呼叫处理操作将受到影响（如果DHCP租赁在有效呼叫期间过期，则可能会出现）。DHCP不允许在更新过程中改变IP地址；只有通过强制MTA重新初始化才能进行改变（以明示或拒绝更新的方式）。建议MTA的IP地址通过DHCP更新的方式进行维护。“IP地址重编号”等操作应考虑这类影响。

8.5 FQDN指配

假设OSS后台系统将对IPCablecom设备生成FQDN，并将这一数据发送到相应的IPCablecom设备和其它网元。这些接口并未在IPCablecom（第1阶段）中定义。

8.6 信令和媒体流数据包的优先级标记

基于IPCablecom业务的媒体流和信令流，需要在足够高的服务质量的基础上，为在DOCSIS接入网和受管IP骨干网内恰当的标记并传输数据包提供方法。

为媒体流在接入网中提供低时延服务质量的主要机制是DOCSIS流分类业务。此业务根据IP源、目的地地址和UDP端口号等数据包字段将数据包分成特定的流。在上行流中，按照CMTS的动态规划，此类数据包会通过相应的恒定比特率业务（用于目前支持的编解码器）传输。在下行数据流中，数据流通过相应的高优先级排队和规划机制传输。DQoS（CMS与CMTS之间）和DOCSIS（CMTS与CM之间）信令机制被用于动态配置媒体流分类规则和业务流QoS业务参数。

除流分类之外，为媒体流数据包做相应的优先级标记也很重要。此类优先级标记可在CMTS/CM排队系统和Diffserv管理的QoS骨干网中使用，以便为此类数据包提供高优先级的QoS处理。IPCablecom并没有定义如何在受管骨干网中使用QoS政策，只是提供了协议机制来创建特殊类别的业务。

信令包也能够从经过优先级处理的QoS业务中获益。特别是随着接入网逐渐达到其最大容量，在前转数据包之前先转高优先级的信令数据包，以避免信令的过度延时，可能也是很必要的。如果需要信令优先级排序，提供区分优先级的QoS的方法则要基于两种机制。首先在所有信令数据包上都标上高优先级标记，其次，提供一个对将要在高优先级业务流上传输的此类数据包进行分类的DOCSIS分类符。该分类符可以仅是简单地将所有具有此类优先级的上行数据映射到高优先级的SID，也可以更为复杂，并确定始发此信令的MTA的IP地址。高优先级的业务流既可以是静态配置也可以由CMTS管理员动态创建。应注意，如果管理员担心高优先级业务流的业务被盗，则可将此业务流配置为高优先级（低时延），但低带宽。

IPCablecom结构可以使用差分业务框架（IETF RFC 3260）区分IPCablecom媒体和信令与高速数据包。媒体流的数据包（RTP和RTCP）以及信令流（NCS, TGCP）的标记均由MTA/MG和/或CMS/MGC实施。数据包的标记可以使用Diffserv代码点（DSCP）在IP层进行。请注意，IETF RFC 2474试图分别将IPv4包头的TOS八位字节和IPv6包头的业务类八位字节重新命名至DS字段。DS字段中有六比特Diffserv代码点，和两个“当前未使用的”比特。对IETF RFC 2474进行了更新的IETF RFC 3168确认，两个“未使用”比特是“显式拥塞通知（ECN）”比特。大力提倡使用DSCP字段，而不使用IPv4 TOS字节。

媒体和信令流的DSCP值，是通过MTA的IPCablecom MIB模块配置的。应注意，在NCS中的信号SDP参数可能包含优先级高于已配置媒体数据流优先级标记值（各连接不同）的值。

8.7 传真支持

IPCablecom支持实时传真传输。在IPCablecom中，最好使用ITU-T T.38建议书规定的IP网络传真中继发送传真（即，本地传真终端，并将传真流转换成IP传真中继数据流）。如果用编解码器建立呼叫，则指示MTA查找传真音）。如果检测到传真音，则会通知CMS并指示MTA将承载流切换到T.38。IPCablecom还支持传真传递功能，其中传真音将作为G.711编码的音频流通过IP网。传真传递还支持回声消除功能。

需要支持从语音呼叫向传真的切换。对于传真中继，还支持从传真向语音的反向切换。

8.8 模拟调制解调器支持

模拟调制解调器的支持方式与传真传递的支持方式相似。将请求MTA检测调制解调器音，在检测到此声音后，如果G.711编解码器未被使用，CMS会指示MTA切换至G.711编解码器。调制解调器传递还支持回声消除功能。

支持从低带宽编解码器切换至G.711，以支持语音呼叫的模拟调制解调器信令。此外，还支持在调制解调器信令结束后返回低带宽编解码器。

不需要本地调制解调器终端和将调制解调器流转换成IP调制解调器中继数据流。

附录一

术语表

本附录包括IP-Cablecom系列建议书中使用的一套完整的术语、定义、首字母缩写词和缩写词。

I.1 定义

I.1.1 接入控制 (access control) : 限制某系统资源的信息,使其只流向被授权人、程序、流程或网络中的其它系统资源。

I.1.2 有效 (active) : 当J.112流被允许前转数据包时,可称为“有效”。在其有效前,J.112流必须首先获得批准。

I.1.3 鉴权 (authentication) : 验证某一实体对另一实体声明的身份的过程。

I.1.4 真实性 (authenticity) : 确保给定的信息不存在修改或伪造,且该信息的确由声明给出此信息的实体产生的能力。

I.1.5 授权 (authorization) : 在某人有接入权的情况下,授权此人接入业务或设备的行为。

I.1.6 电缆调制解调器 (cable modem) : 电缆调制解调器是一种第二层终端设备,负责连接J.112连接的客户端。

I.1.7 呼叫 (call) : 呼叫是一种由用户发起的话音通信能力的实例。在传统的电话业务中,呼叫通常被认为是直接在两点间,即主叫方和被叫方之间建立的连接。根据有关IP-Cablecom的部分,上述各方之间的通信是传统意义上的“无连接”通信。

I.1.8 密码 (cipher) : 在普通文本和加密文本之间转换数据的算法。

I.1.9 密码集 (ciphersuite) : 必须包含加密算法和消息鉴权算法(例如,MAC或HMAC)的集。一般来讲,它也许还应包含对IP-Cablecom不适用的密钥管理算法。

I.1.10 保密性 (confidentiality) : 确保信息不被披露给目标对象以外的人的方法。通过加密来确保信息的保密性。又称“私密性”。

I.1.11 下行 (downstream) : 从前端指向用户位置的方向。

I.1.12 加密 (encryption) : 将信息从普通文本翻译成加密文本的方法。

I.1.13 端点 (endpoint) : 终端、网关或MCU。

I.1.14 事件消息 (event message) : 事件消息是一组能够表示IP-Cablecom结构内出现的事件的数据,它可以指出一种或多种可计费IP-Cablecom能力的使用情况。事件消息本身可能无法全面显示客户的可计费行为,但与其它事件消息建立了关联的事件消息构成了可计费详细使用记录的基础。

I.1.15 事件消息属性 (event message attribute) : 事件消息属性是一种用属性定义和属性类型描述的预定义数据元素。

I.1.16 网关 (gateway) : IP-Cablecom的IP话音通信部分与PSTN之间的桥接设备。其示例包括提供PSTN承载电路接口并对媒体流进行代码转换的媒体网关,向IP-Cablecom网边缘发送和接收电路交换网信令的信令网关。

I.1.17 报头 (header) : 位于协议数据单元开始处的协议控制信息。

- I.1.18 完整性 (integrity) :** 确保信息只能由被授权人进行修改的方法。
- I.1.19 IP-Cablecom:** 包括能够利用电缆调制解调器在有线电视网上提供实时业务的结构和一系列建议书的ITU-T项目。
- I.1.20 IP-Cablecom事务处理 (IP-Cablecom transaction) :** IP-Cablecom事务处理是向用户交付业务时IP-Cablecom网络中发生的一系列事件。相同事务处理的事件消息使用唯一的计费关联ID识别。对于某些业务,为收集全部业务使用情况提供所需的信息,可能需要多重事务处理。可能需要使用多重事件消息来跟踪各业务所用的资源。事件处理可能会持续一段时间。
- I.1.21 J.112流:** 属于MAC层信令和符合ITU-T J.112建议书规定的QoS指配的单向或双向数据包流。
- I.1.22 Kerberos:** 一种选用密码算法,进行加密并将集中密钥数据库用于鉴权的密钥网络鉴权协议。
- I.1.23 密钥 (key) :** 一种输入被选密码算法的数值。
- I.1.24 密钥交换 (key exchange) :** 在实体之间交换的公钥,用于实体间的加密通信。
- I.1.25 密钥管理 (key management) :** 运行安全协议所需的共享对称密钥分配流程。
- I.1.26 管理信息库 (Management Information Base (MIB)) :** 允许通过网络管理协议进行标准接入的信息规范。
- I.1.27 不可否认性 (non-repudiation) :** 防止发送者事后否认他或她曾经发送过某个消息或采取过某一行动的能力。
- I.1.28 私密性 (privacy) :** 确保信息不被披露给目标对象以外的人的方法。通常通过加密来确保信息的保密性。又称“保密性”。
- I.1.29 私钥 (private key) :** 在公钥加密中使用的、属于某独立实体且必须保密的密钥。
- I.1.30 代理服务器 (proxy) :** 间接提供某些服务或作为提供信息的代理,以使主机不必亲自支持这些业务的设施。
- I.1.31 公钥 (public key) :** 在公钥加密中,属于某独立实体且进行公开分配的密钥。其它实体利用此密钥对发往密钥所有者的数据进行加密。
- I.1.32 公钥证书 (public key certificate) :** 一个实体的公钥与与其身份相关的一个或多个属性间的绑定。也称为“数字证书”。
- I.1.33 公钥加密 (public key cryptography) :** 使用一对密钥,即公钥和私钥,进行加密与解密的程序;又称不对称算法。用户的公钥对其它用户是公开的,他们可以使用这些公钥向公钥的所有者发送消息。用户的私钥是保密的,且是唯一能够对用户公钥加密的消息进行解密的密钥。
- I.1.34 根私钥 (root private key) :** 最高级别证书机构的私用签名密钥。通常用来为低级证书机构或其它实体签署公钥证书。
- I.1.35 根公钥 (root public key) :** 最高级别证书机构的公钥通常用来为低级证书机构或其它实体签署公钥证书。

I.1.36 业务 (service) : 业务是用户可选的一个或一系列通信功能。业务是通过旨在向用户提供所需功能的一个或多个“呼叫”或交易确定的。业务示例包括：两个本地IPCablecom用户间的话音通信，3方呼叫、按收视付费的电影和网上冲浪会话。业务既可以是瞬时的也可以在一段时间内存在。

I.1.37 信令网关 (SG) : SG是一种代理设备，负责在IP网络边缘接收/发送SCN本地信令。SS7 SG的具体功能是将SS7互联网网关的变体ISUP和TCAP转换成公共版本的ISUP和TCAP。

I.1.38 X.509证书 (X.509 certificate) : 作为ITU-T X.500系列建议书标准目录组成部分制定的公钥证书规范。

I.2 缩写词

AH	鉴权报头 (Authentication Header)
AMA	自动消息计费 (Automated Message Accounting)
AN	接入节点 (Access Node)
ANC	通知控制器 (Announcement Controller)
ANP	通知播放器 (Announcement Player)
ANS	通知服务器 (Announcement Server)
API	应用程序接口 (Application Programming Interface)
BPI+	增强型基线私密性接口 (Baseline Privacy Interface Plus)
CA	呼叫代理 (Call Agent)
CBC	密码块链接 (模式) (Cipher Block Chaining (mode))
CDR	详细呼叫记录 (Call Detail Record)
CIC	电路识别码 (Circuit Identification Code)
CID	电路ID (Circuit ID)
CM	电缆调制解调器 (Cable Modem)
CMS	呼叫管理服务器 (Call Management Server)
CMS	加密消息语法 (Cryptographic Message Syntax)
CMTS	电缆调制解调器终端系统 (Cable Modem Termination System)
COPS	公共开放政策业务 (Common Open Policy Service)
CPE	客户所在地设备 (Customer Premises Equipment)
DCS	分布式呼叫信令 (Distributed Call Signalling)
DHCP	动态主机配置协议 (Dynamic Host Configuration Protocol)
DNS	域名系统 (Domain Name System)
DPC	目的地点代码 (Destination Point Code)
DQoS	动态服务质量 (Dynamic Quality of Service)
DTMF	双音多频 (Dual Tone Multi-Frequency)
ESP	IPsec 封装安全性 (IPsec Encapsulation Security)
FID	流标识符 (Flow Identifier)

FQDN	完全限定域名 (Fully qualified Domain Name)
GC	门控制器 (Gate Controller)
HFC	混合光纤同轴网 (电缆) (Hybrid Fibre/Coaxial (cable))
HMAC	散列消息鉴权码 (Hashed Message Authentication Code)
HTTP	超文本传输协议 (HyperText Transfer Protocol)
IANA	互联网号码分配机构 (Internet Assigned Numbers Authority)
IEEE	电气电子工程师学会 (Institute of Electrical and Electronics Engineers)
IETF	互联网工程任务组 (Internet Engineering Task Force)
IKE	互联网密钥交换 (Internet Key Exchange)
IKE-	有鉴权预共享密钥的IKE (IKE with pre-shared keys for authentication)
IKE+	被定义用来表示IKE使用的符号, 此IKE需要使用数字证书进行鉴权
INA	互动网络适配器 (Interactive Network Adapter)
IP	互联网协议 (Internet Protocol)
IPsec	IP安全性 (IP security)
ISTP	互联网信令传输协议 (Internet Signalling Transport Protocol)
ISUP	集成业务数字网用户部分 (Integrated Services Digital Network User Part)
LNP	本地号码可携带性 (Local Number Portability)
MAC	消息鉴权码 (Message Authentication Code)
MAC	媒体接入控制 (Media Access Control)
MD5	消息摘要5 (Message Digest 5)
MF	多频 (Multi-Frequency)
MG	媒体网关 (Media Gateway)
MGC	媒体网关控制器 (Media Gateway Controller)
MGCI	媒体网关控制器接口 (Media Gateway Controller Interface)
MGCP	媒体网关控制器协议 (Media Gateway Control Protocol)
MIB	管理信息库 (Management Information Base)
MMH	多线性模块化散列 (Multilinear Modular Hash)
MTA	媒体终端适配器 (Media Terminal Adapter)
MTP	消息传输部分 (Message Transfer Part)
MWD	最长等待延时 (Maximum Waiting Delay)
NCS	网络呼叫信令 (Network Call Signalling)
NTP	网络时间协议 (Network Time Protocol)
OSS	操作支持系统 (Operations Support System)
PHS	有效负荷报头压缩 (Payload Header Suppression)
PKI	公钥基础设施 (Public Key Infrastructure)
PKINIT	公钥加密初始鉴权 (Public Key Cryptography Initial Authentication)

PSTN	公共交换电话网 (Public Switched Telephone Network)
QoS	服务质量 (Quality of Service)
RADIUS	远程接入拨号用户服务 (Remote Access Dial-In User Service)
RAP	资源划分协议 (Resource Allocation Protocol)
RC4	密码集中提供的可变长密钥流密码, 用于IPSec中的媒体业务加密。
RFC	请求评论 (Request for Comments)
RFI	无线电频率接口 (Radio Frequency Interface)
RKS	记录保存服务器 (Record Keeping Server)
RSVP	资源预留协议 (Resource reSerVation Protocol)
RTCP	实时控制协议 (Real-Time Control Protocol)
RTO	重传超时 (Retransmission Timeout)
RTP	实时传输协议 (Real-Time Transfer Protocol)
SA	源地址 (Source Address)
SA	安全性关联 (Security Association)
SCCP	信令连接控制部分 (Signalling Connection Control Part)
SCP	业务控制点 (Service Control Point)
SCTP	流控制传输协议 (Stream Control Transmission Protocol)
SDP	会话描述协议 (Session Description Protocol)
SG	信令网关 (Signalling Gateway)
SHA-1	安全散列算法1 (Secure Hash Algorithm 1)
SID	系统识别号 (System IDentification number)
SIP	会话发起协议 (Session Initiation Protocol)
SIP+	增强型会话发起协议 (Session Initiation Protocol Plus)
SNMP	简单网络管理协议 (Simple Network Management Protocol)
SPI	安全参数索引 (Security Parameter Index)
SS7	7号信令系统 (Signalling System No. 7)
SSP	信号交换点 (Signal Switching Point)
TCAP	事务处理能力应用部分 (Transaction Capabilities Application Part)
TCP	传输控制协议 (Transmission Control Protocol)
TGS	票据授予服务器 (Ticket Granting Server)
TLV	类型长度值 (Type-Length-Value)
ToS	服务类型 (Type of Service)
UDP	用户数据报协议 (User Datagram Protocol)
VAD	语音活动检测 (Voice Activity Detection)
VoIP	IP语音 (Voice Over IP)

参考书目

- IETF RFC 2131 (1997) , *Dynamic Host Configuration Protocol*.
- IETF RFC 2132 (1997) , *DHCP Options and BOOTP Vendor Extensions*.
- IETF RFC 2274 (1998) , *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* .
- IETF RFC 2575 (1999) , *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* . (Obsoletes RFC 2275) .

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题