

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

J.179

(11/2005)

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
IPCablecom

IPCablecom支持多媒体

ITU-T J.179建议书

摘 要

通过规定若干基于 IP 的信令接口的技术定义，本建议书对通用多媒体业务的配置情况进行了阐述，这些接口对 CableModem 固有的核心 QoS 和策略管理具有重要的作用。多媒体业务定义为基于 IP 的业务（例如在线游戏、视频会议、流媒体等），它们需要基于 QoS 的网络资源（相对互联网浏览、电子邮件、即时短信和文件共享等业务而言，这些业务通常需要通过尽力服务流来提供）。虽然未明确将电话或基于语音的业务排除于该定义之外，不过 IPCablecom-T 系列建议书规定了此类业务特定的覆盖范围，因此应适当考虑到这些建议书。

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.179 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“务必”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

页码

1	范围	1
2	参考文献	1
2.1	规范性参考文献	1
2.2	资料性参考文献	1
3	术语和定义	2
4	缩写词、首字母缩略语和惯例	2
4.1	缩写词和首字母缩略语	2
4.2	惯例	4
5	技术概述	4
5.1	QoS 背景	4
5.2	体系结构	8
6	授权接口描述	16
6.1	控制门：QoS 控制的框架	16
6.2	控制门转换	22
6.3	IP_Cablecom 多媒体的 COPS 简表	28
6.4	控制门控制协议消息格式	30
6.5	控制门控制协议操作	53
7	事件消息发布接口描述	62
7.1	引言	62
7.2	记录保持服务器要求	64
7.3	IP_Cablecom 多媒体网络元素一般要求	64
7.4	IP_Cablecom 多媒体的事件消息	66
7.5	IP_Cablecom 多媒体的事件消息发布属性	71
7.6	RADIUS 结算协议	79
8	安全性要求	81
8.1	CMTS — CM QoS 接口 (pkt-mm-1)	81
8.2	策略服务器 — CMTS COPS 接口 (pkt-mm-2)	81
8.3	应用管理器 — 策略服务器 COPS 接口 (pkt-mm-3)	82
8.4	策略服务器 — RKS 事件消息接口 (pkt-mm-4)	82
8.5	CMTS — RKS 事件消息接口 (pkt-mm-5)	83
9	将 FlowSpec 通信业务简表映射至 DOCSIS	83
9.1	将 FlowSpecs 映射至 DOCSIS 调度类型	83
9.2	将 FlowSpecs 映射至 DOCSIS 通信业务参数	84
9.3	DOCSIS 上行流参数	86
9.4	DOCSIS 下行流参数	89

	页码
10 消息流	91
10.1 基本的消息序列	92
10.2 详细的消息序列	94
11 有待今后研究的问题	113
附录一 — 背景信息	114
I.1 引言	114
I.2 IPCablecom 多媒体的目标和范围	115
I.3 IPCablecom 多媒体的框架	117
I.4 带策略推动的、代理的 QoS（情形 1）	122
I.5 带策略推动的、客户机请求的 QoS（情形 2）	130
I.6 带策略拉动的、客户机请求的 QoS（情形 3）	137
I.7 IPCablecom-T 与 IPCablecom 多媒体的比较	139
附录二 — 版本号分配指南	143

IPCablecom支持多媒体

1 范围

通过规定若干基于 IP 的信令接口的技术定义，本建议书对通用多媒体业务的配置情况进行了阐述，这些接口对 CableModem 固有的核心 QoS 和策略管理具有重要的作用。多媒体业务定义为基于 IP 的业务（例如在线游戏、视频会议、流媒体等），它们需要基于 QoS 的网络资源（相对互联网浏览、电子邮件、即时短信和文件共享等业务而言，这些业务通常需要通过尽力服务流来提供）。虽然未明确将电话或基于语音的业务排除于该定义之外，不过 IPCablecom-T 系列建议书规定了此类业务特定的覆盖范围，因此应适当考虑到这些建议书。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其它参考文献的条款，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。

- [1] ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification*.
- [2] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.
- [3] IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services*.
- [4] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service*.
- [5] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.
- [6] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.
- [7] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.
- [8] IETF RFC 2866 (2000), *RADIUS Accounting*.
- [9] ITU-T Recommendation J.163 (2005), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*.
- [10] ITU-T Recommendation J.164 (2005), *Event message requirements for the support of real-time services over cable television networks using cable modems*.
- [11] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.
- [12] ITU-T Recommendations J.125 (2004), *Link privacy for cable modem implementations*.

2.2 资料性参考文献

- [13] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview*.

- [14] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.
- [15] IETF RFC 2216 (1997), *Network Element Service Specification Template*.
- [16] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.
- [17] IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces*.
- [18] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.
- [19] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)*.
- [20] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.
- [21] CableLabs (<http://www.cablemodem.com/specifications>).
- [22] IETF RFC 2751 (2000), *Signaled Preemption Priority Policy Element*.

3 术语和定义

本建议书规定下列术语：

3.1 client type 1: 第 1 类客户机：第 1 类客户机代表现有的“传统”端点（如 PC 应用程序、游戏控制台），它缺少特定的 QoS 意识或信令能力。该类客户机不了解任何 CableModem、IPCable2Home 或 IPCablecom 消息发布，因此无法对其提出任何相关的要求。此类客户机可以包括：从简单的模拟音频与视频演示设备，到复杂的网络化外部设备与消费类电子设备，如机顶盒或游戏控制台。该类客户机与应用管理器进行通信，以请求服务，但不直接从运营商接入网络请求 QoS 资源。本建议书只支持第 1 类客户机。

3.2 client type 2: 第 2 类客户机：第 2 类客户机类似于一个 IPCablecom-T 电话 MTA，它支持基于 IPCablecom DQoS 的 QoS 信令。该类客户机知晓 IPCablecom 多媒体 QoS，并与应用管理器进行通信，以请求服务并获得一个有关接入网络资源的令牌。而后，在从接入网络请求 QoS 资源时，客户机提交该令牌（pkt-mm-1, pkt-mm-6）。本建议书对第 2 类客户机的支持仍有待进一步研究。

3.3 client type 3: 第 3 类客户机：第 3 类客户机依据 RSVP 来请求 QoS，而无须应用服务器的交互。该类客户机知晓基于 IETF 标准的 RSVP，并利用该协议向直接来自 CMTS 的接入网络请求 QoS 资源。本建议书对第 3 类客户机的支持仍有待进一步研究。

3.4 DOCSIS：用于描述一种特定的 CableModem 技术，它由有线电视实验室公司（“CableLabs”）开发，网址为：<http://www.cablemodem.com/specifications/>。国际版在附件 B/J.112 中定义。

3.5 IPCablecom-T：支持电话业务的 IPCablecom ITU-T 建议书集。

4 缩写词、首字母缩略语和惯例

4.1 缩写词和首字母缩略语

本建议书采用下列缩写：

AM	应用管理器（接口于策略服务器的一个系统，代表最终用户或网络管理系统请求基于 QoS 的服务）
----	--

BCID	记账相关 ID（在 IPCablecom 事件消息发布建议书中定义）
CM	电缆调制解调器
CMS	呼叫管理服务器
CMTS	电缆调制解调器终端系统
COPS	公共开放策略服务（在 RFC 2748 中定义）
DQoS	动态服务质量
DSx（消息发布）	J.112 附件 B “QoS 信令机制”，规定了动态业务的增加、修改和删除语义
FQDN	正式域名
HFC	混合光纤/同轴电缆
IETF	互联网工程任务组
IP	网际协议
KDC	关键分发中心
MG	媒体网关
MGC	媒体网关控制器
MTA	多媒体终端适配器
NAT	网络地址解析
PDP	策略决策点（在 RFC 2753 中定义）
PEP	策略执行点（在 RFC 2753 中定义）
PS	策略服务器
PSTN	公众电话交换网
QoS	服务质量
RADIUS	远程认证拨入用户服务（在 RFC 2138 和 RFC 2139 中定义）
RAP	资源分配协议（IETF 中的工作组 — 负责定义和维护 COPS 协议）
RCD	资源控制域
RFC	征求意见（IETF 批准的技术策略文件，可在以下网址中找到： http://www.ietf.org/rfc.html ）
RFI	射频接口（定义 MAC 以及 CMTS 与 CM 网络元素之间物理层接口的规范）
RKS	记录保持服务器
RSVP	资源预留协议（在 RFC 2205 中定义）
RSVP+	RSVP 的 IPCablecom 简表和扩展（在 IPCablecom DQoS 建议书中定义）
SCD	会话控制域
S-MTA	孤立的 MTA（一个包含一个 MTA 和一个非 DOCSIS MAC 的单个节点（如以太网））

TCP	传输控制协议
TLV	类型长度值（格式化协议单元过程中所用的技术）
UDP	用户数据报协议（建立在网际协议（IP）之上的无连接协议）
UGS	主动提供的授权服务（附件 B/J.112 “用于固定比特率业务的调度类型”（如语音编码解码器））
UGS/AD	带活动性检测的、主动提供的授权服务
VoIP	IP 电话
VPN	虚拟专用网

4.2 惯例

在整个本建议书中，用于定义特殊要求重要性的词用大写字母来表示。这些词是：

“务必”（MUST）	这个词或形容词“必需的（REQUIRED）”意指：该条款是本建议书的绝对要求。
“绝不”（MUST NOT）	这个词组意指：该条款是本建议书的绝对禁令。
“应”（SHOULD）	这个词或形容词“建议的（RECOMMENDED）”意指：在实际环境中有可能存在正当的理由对这一条款不予理会，但是，在选择不同的做法之前应充分理解全部含义和小心权衡理由。
“应不”（SHOULD NOT）	这个词组意指：在实际环境中有可能存在正当的理由，考虑到所列举的行为是可接受的或甚至是可用的。但是，在实际用这个标记描述的任何行为之前，应充分理解全部含义和小心权衡理由。
“可”（MAY）	这个词或形容词“可选的（OPTIONAL）”意指：这一条款是真正可选的。例如，某个供货商可以选择含有该条款，因为实际市场需要它或因为它能提高产品价值；而另外的供货商可以忽略同样的条款。

5 技术概述

本节由背景材料组成，一些读者可能会发现，对于之后所述的详细的协议接口建议书，这是一个有用的背景材料。本节旨在提供有关 IP-Cablecom 多媒体体系结构以及作为其基础的基本技术的高级概述。关于多媒体体系结构的更详细内容，请参见附录一。

5.1 QoS背景

正如整个本建议书所阐述的那样，IP-Cablecom 多媒体服务框架的其中一个主要特点基于这样的事实，即它提供对复杂 QoS 性能的 IP 层接入，这些性能在附件 B/J.112 和 IP-Cablecom-T 中加以定义。本节简要概述这些性能，作为之后详细讨论 QoS 策略和资源管理的预备背景材料。

5.1.1 附件B/J.112 QoS概述

附件 B/J.112 RFI 建议书[1]定义了基于基本网络资源管理结构的一组 QoS 设备，即众所周知的服务流。服务流定义为“MAC 层传输服务，它

- 1) 提供从上层服务实体到 RF 的单向分组传送；并且
- 2) 依据为流定义的 QoS 通信业务参数，形成、监管并排定通信业务的优先级”。

除了推动按每个流预留和调度共享的接入网络资源这一初级抽象概念之外，还定义了众多实质性的支持结构，并用这些结构来管理这些资源。其中的两种支持结构是：

- 服务流编码：类型长度值（TLV）编码的参数，用于定义与服务流相关的 QoS 参数。
- 分类符：类型长度值（TLV）编码的 IP、以太网和 IEEE802.1p/q 参数，用于依据发起和终止端点来定义和限制流的范围。

附件 B/J.112 支持提供的（即在 CM 注册过程中建立的、静态的、永久的服务流）和动态的（即在需要时增加、修改和删除的瞬时服务流）QoS 模型，而 IP Cablecom 多媒体框架主要关注的是动态变化，因为当服务要求需要时，这允许通过统计多路复用技术实现对网络资源的优化管理。

服务流管理通过 MAC 层 DOCSIS 动态服务增加/修改/删除（DSA/DSC/DSD）消息发布来执行，这种消息发布由 CM 发起或者由 CMTS 发起。DSA 和 DSC 事务处理采取三向交换的形式，其中，紧跟在请求（REQ）后面的是响应（RSP），然后是确认（ACK）该响应。DSD 消息只是双向交换。在各个 DSx 响应消息中，提供了一种称为确认码的特殊属性，指明事务处理成功与否的状态。

在评审附件 B/J.112 中所提供的 QoS 能力时，需要着重注意的一点是，在 CMTS 上，上行流和下行流服务流的处理是有根本区别的。这是因为，上行流 RF 信道是竞争式的、共享的接入媒体，在多个 CM 与单个 CMTS 之间，采取多对一的拓扑形式。相反地，下行流 RF 信道表现出与传统 IP 路由器更大的同类性，当中，对抵达的分组（或者来自接入网络，或者来自骨干网）进行排队，并转发至一个或多个目的地。因此，取决于是将特殊的单向服务流导入上行流方向还是导入下行流方向，需采用截然不同的 QoS 机制。

上行流服务流可依照以下五种服务流调度类型中的一种进行定义：

- 尽力服务型：一种标准的、基于竞争的资源管理策略，在该策略中，尽管有 CMTS 调度程序的协调，仍以“先来先服务”的方式授予传输机会。该调度类型可用 QoS 特性来补充，例如，在该类型中，针对特殊的服务流可运用最大速率限制。
- 非实时轮询：一种基于预留的资源管理策略，在该策略中，以固定间隔来轮询特定的 CM，以确定为了实现在特定服务流上的传输，数据是否已进行排队，如果已进行排队，那么调度程序为该服务流提供传输机会或予以授权。
- 实时轮询：除了固定的轮询间隔通常相当短（<500 ms）之外，它与非实时轮询调度类型相类似。轮询调度类型最适于等待时间和吞吐量需求不要求灵活的可变比特率通信业务。

- 主动提供的授权：一种基于预留的资源管理策略，在该策略中，向特定的服务流以（接近）固定的间隔提供固定大小的授权，而无须额外的轮询或交互。该调度类型最适于固定比特率的通信业务，并消除了与轮询类型相关的大量协议开销。
- 带活动性检测的、主动提供的授权：一种基于预留的资源管理策略，代表轮询和主动提供的授权相混合的一种调度类型，在该策略中，只要因传输而对数据进行排队，那么就以（接近）固定的间隔提供固定的授权。在非活动期间，为了保存未用的带宽，该调度类型恢复为轮询模式。

由于这些调度类型中的每一种都具有独特的性质和专有的特点，因此每一种都有特定的 QoS 参数。在以下各节中对这些参数进行了详细的描述。

运用与上行流中尽力服务调度类型相关的同一 QoS 参数集，定义了下行流服务流。

不管流的方向或请求的特殊调度类型是什么，所有的动态服务流都通过三种逻辑状态来进行，总结如下。虽然某些经过优化的信令情形允许所谓的“单阶段”提交操作，但在逻辑上，当它在 CMTS 上被服务时，仍然需要通过全部三个阶段来进行请求。

- 授权的：认证请求，并运用网络策略规则，结果是授权封装，它形成随后的预留请求的边界。
- 准许的（或预留的）：建立一个非活动的服务流，并由调度程序预留资源，以便保证随后的激活请求取得成功；预留的资源可由尽力服务通信业务（来自相同的或不同的 CM）使用，直至提交。
- 活动的（或提交的）：与相应的分类符一起，服务流得以激活；目前，QoS 增强性分组能够穿越该流。

注一从字面上看，DOCSIS 并不定义服务流的“状态”，而是定义服务流的“属性”，它们完全由各个 DSC 事务处理所替代。此处所述的状态是逻辑意义上的概念，在概念模型中使用，描述在 CMTS 上执行的资源管理过程。另外，在定义服务流的属性时，DOCSIS RFI 建议书还对“准许的”和“活动的”这两个术语进行了标准化，与此同时，IPCablecom 在描述控制门状态过程中采用了“预留的”和“提交的”这两个对等的术语。

尽管 DOCSIS 并不定义将应用于 DSx 消息的、特定的授权程序，但它通过一种称为授权块的设施，来为服务特定的授权方案提供协议支持。任何证书或授权令牌都经由授权块来提供，并在处理 CMTS 上的 DSx 请求之前，转发给适当的授权模块。IPCablecom 扩展使用了该授权机制，将在下面进行描述。

5.1.2 IPCablecom-T QoS概述

尽管附件 B/J.112 RFI 建议书定义了形成 IPCablecom DQoS 模型核心的基本的 QoS 机制，IPCablecom DQoS 建议书[9]仍用基于 COPS 的策略管理框架来增强这些性能。正如服务流代表了附件 B/J.112 QoS 模型中的主要的抽象概念，控制门仍在 IPCablecom DQoS 方案中发挥着比较重要的作用。控制门定义了资源授权封装，它包括 IP 级的 QoS 参数，以及用于定义服务流范围的分类符，这些服务流可依据控制门进行建立。根据上述的附件 B/J.112 授权机制，仅（逐个参数地）授予符合以下一般关系的 DSx 请求：

基于该策略管理模型，IPCablecom-T 定义了一种预授权方案，在该方案中，发布请求建立一个相应服务流的 DSx 消息之前，要对网络资源进行授权。因此，用于安装和管理控制门的 COPS 接口，比 RFC 2748 [7]中规定的标准 COPS 方案，更加符合 RFC 3084 [19]中定义的 COPS-PR 模型。另外，为了安装和管理这些控制门，IPCablecom DQoS 建议书定义了一组客户机特定的对象，这些对象构成了 CMS 与 CMTS 之间控制门控制信令接口的原型。

特别地，CMS 可从逻辑上分解为一个负责电话呼叫状态保持的呼叫代理和一个负责接收来自呼叫代理（通过一个内部接口）授权请求的控制门控制器，并以控制门的形式在 CMTS 上安装策略决定。在 IPCablecom 多媒体模型中，通过策略服务器（类似于 IPCablecom-T 控制门控制器）和应用管理器（定义 IPCablecom-T 模型中类似呼叫代理的、服务特定的功能性）这两个独立的网络元素，来规范这种分解过程。

作为对该预授权模型的说明和 CMTS 上控制门控制接口的使用，一个典型的单区域（即使用单个的 CMS）在线 IPCablecom-T 呼叫流将按以下步骤进行（这些步骤中的一些步骤通常会并行进行）：

- E-MTA_o 引导，利用 CMS 进行提供和注册；
- CMS 向 E-MTA_o 发出一个请求，通知摘机事件和拨号数字；
- E-MTA_t 引导，利用 CMS 进行提供和注册；
- CMS 向 E-MTA_t 发出一个请求，通知摘机事件和拨号数字；
- E-MTA_o 摘机，通知 CMS 并传送拨号数字；
- CMS 向 E-MTA_o 发出一个请求，以建立一个新的逻辑连接，并检索 SDP_o；
- CMS 向 E-MTA_t 发出一个请求，以建立一个新的逻辑连接，并检索 SDP_t；
- CMS 在 CMTS_o 上安装一个控制门，并检索相应的 GateID_o 令牌；
- CMS 在 CMTS_t 上安装一个控制门，并检索相应的 GateID_t 令牌；
- CMS 向 E-MTA_o 发出一个（带 GateID_o）的请求，以预留资源，并播放回铃音；
- E-MTA_o 向 CMTS_o 发出一个 DSA-REQ，以建立服务流，并预留资源；
- CMS 向 E-MTA_t 发出一个（带 GateID_t）的请求，以预留资源，并播放警告铃声；
- E-MTA_t 向 CMTS_t 发出一个 DSA-REQ，以建立服务流，并预留资源；
- E-MTA_t 摘机，并通知 CMS；
- CMS 向 E-MTA_o 发出一个请求，以停止播放回铃音、提交资源，并就近通过媒体路径；
- E-MTA_o 向 CMTS_o 发出一个 DSA-REQ，以提交资源；
- CMS 向 E-MTA_t 发出一个请求，以提交资源，并就近通过媒体路径；
- E-MTA_t 向 CMTS_t 发出一个 DSA-REQ，以提交资源；
- 呼叫继续进行。

与 IPCablecom 模型（在该模型中，客户机设备（即 E-MTA）启动资源预留并激活程序）形成对比，IPCablecom 多媒体资源管理模型允许代表端点，通过增强型控制门控制接口来代理进行这些步骤。

这形成了对附件 B/J.112 和 IP-Cablecom DQoS 基本原理的简要回顾。有关这些复杂主题中的任何一个主题，其进一步的详细内容请分别参考主要的文献资料[1]和[9]。下一个条目提供对 IP-Cablecom 多媒体体系结构的摘要概述，包括各主要网络元素和相关的接口，作为随后的技术协议建议书的进一步准备。

5.2 体系结构

附录一描述 IP-Cablecom 多媒体的体系结构框架和参考模型。本建议书采用包含在体系结构框架中的模型，并增加了规范的需求，以提供可升级的、可互操作的解决方案，它适于提供 IP-Cablecom 多媒体服务。

5.2.1 客户机类型

IP-Cablecom 多媒体技术报告定义了三种客户机类型：

- 第 1 类客户机：第 1 类客户机代表现有的“传统”端点（如个人电脑应用程序、游戏控制台），它缺少特定的 QoS 意识或信令性能。该类客户机不了解任何 CableModem、IP-Cable2Home 或 IP-Cablecom 消息发布，因此无法对其提出任何相关的要求。第 1 类客户机与应用管理器进行通信，以请求服务，但不（不能）直接向电缆运营商接入网络请求 QoS 资源。
- 第 2 类客户机：第 2 类客户机类似于一个 IP-Cablecom-T 电话 MTA，它支持基于 IP-Cablecom DQoS 建议书的 QoS 信令。
- 第 3 类客户机：第 3 类客户机直接向接入网络请求 QoS 处理，而无须与应用服务器的交互。该类客户机知晓基于 IETF 标准的 RSVP，并利用该协议直接向 CMTS 请求接入网络 QoS 资源。

在本建议书的这一版本中，仅支持第 1 类客户机。因此，本建设书的这一版本仅支持情形 1，即附录一中所描述的“带策略推动的代理 QoS”。在该情形下，应用管理器负责代表客户机请求 QoS 资源，而策略服务器将把请求下推给 CMTS，CMTS 是实际负责建立和管理应用所要求之 DOCSIS 服务流的设备。

5.2.2 IP-Cablecom 多媒体设备

除了客户机（一般驻留于订户住宅内），IP-Cablecom 多媒体还需要一些网络元素，它们驻留于电缆运营商的网络中，或者可接入电缆运营商的网络，或者受到电缆运营商网络的信任。在本建议书通篇描述这些网络元素的过程中，我们十分频繁地借用了标准 IETF 的术语和概念。对整体 IP-Cablecom 多媒体体系结构的更为全面的论述，包括对基本要求与目标的讨论，请参考附录一。

由于 COPS [7]和 COPS-PR [19]中存在巨大差异的交互情形中各自使用策略执行点（PEP）和策略决定点（PDP）术语，以及由于 IP-Cablecom 多媒体为这些概念增加了更为细微的差别（尤其在策略服务器的定义上），因此，人们有时会仅根据 PEP 和 PDP，混淆地理解 IP-Cablecom 多媒体体系结构各种不同部件的职责。为努力消除这种混淆，本建议书的部分内容采用了服务控制域和资源控制域的概念，以突出将要定义和执行的策略类型之间的区别。

资源控制域（RCD）定义为：沿着至终端和自终端的分组转发路径，提供连接性和网络资源级策略管理的元素逻辑分组。RCD 包括 CMTS 和策略服务器实体，其职责包括管理沿着分组转发路径的资源。

服务控制域（SCD）定义为：向服务订户提供应用和内容的元素逻辑分组。应用管理器驻留于 SCD 中。注意，可能有一个或多个 SCD 与单个 RCD 相关。反之，各 RCD 可与一个或多个 SCD 交互作用。

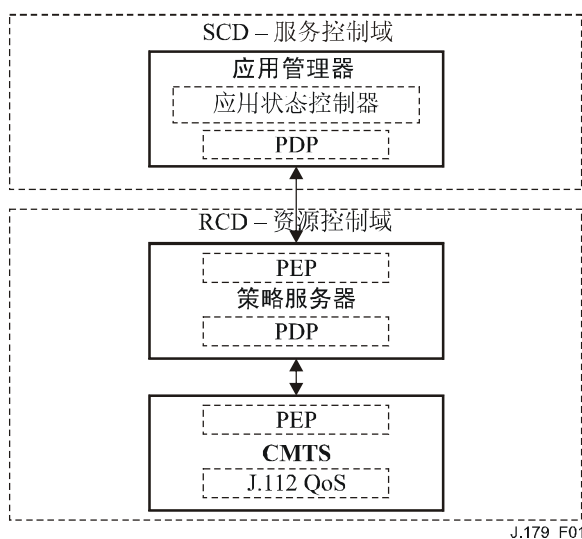


图 1/J.179—会话和资源控制域

在 IPCablecom 多媒体体系结构中，应用管理器的基本作用是保持应用的会话级状态，并依照客户机驱动的会话请求，来执行任何服务控制域（SCD）策略。如果客户机的会话请求通过了应用管理器 SCD 策略的检查，那么应用管理器将会话请求转变为资源请求，并将之传给策略服务器，以便进行资源控制域（RCD）策略检查。如果资源请求未通过 RCD 策略检查，那么策略服务器拒绝资源请求，应用管理器因此而拒绝客户机的会话请求。不过，如果资源请求通过了策略服务器的 RCD 检查，那么策略服务器将请求转发给 CMTS，以便实施网络级的准许进入控制。

不同 IPCablecom 多媒体部件的基本作用如下所述：

- 应用管理器负责应用或会话级状态，并负责应用 SCD 策略。
- 策略服务器负责应用 RCD 策略，并负责管理应用管理器与 CMTS 之间的关系。
- CMTS 负责执行准许进入控制，并通过 DOCSIS 服务流对网络资源进行管理。

在此阐明我们所用的“准许进入控制”和“策略授权”这两个术语可能是有用的。出于本建议书的目的，准许进入控制通常理解为管理一个有限的网络级资源集（例如，接入网络带宽、调度程序 DOCSIS 的小时间片，或是支持控制门和计时器的 CMTS 资源等）的过程，并依照该资源集接受请求。出于性能原因，准许进入控制通常在管理分组转发路径（如 CMTS）的网络元素上直接执行，尽管某些复杂的策略服务器实施方案可以选择保持与网络资源相关的状态，从而补充和推动准许进入控制进程。

相反地，此处使用策略授权来描述更高级的、聚合的使用策略（例如，对特殊订户或服务的并行授权数量），它们构成电缆运营商的网络管理策略。策略授权几乎总是在策略服务器上进行定义和执行。

本节的其余部分更为详细地描述了这些体系结构部件中各个部件及其相关接口的情况。

5.2.2.1 应用管理器（AM）

正如前面摘要中所提到的那样，应用管理器是一个网络实体，它定义 SCD 策略，通过接入满足那些请求所需之资源的方式来协调订户发起的应用会话请求，并保持应用级状态。

AM 可驻留于电缆运营商的网络中，或者可驻留于该域之外，并通过一种特殊的信任关系（一般基于服务级协议加以定义和执行）与电路运营商网络实现交互。类似地，AM 可由运营商直接控制，或由第三方进行控制。任何特定的应用管理器都可以在运营商网络上与一个或多个策略服务器进行通信；同样，一个或多个应用管理器可以在运营商网络上与任何特定的策略服务器进行通信（只要存在合适的信任关系）。

在大多数预先的服务配置情形中，应用管理器将通过信令协议与客户机进行通信，这超出了本建议书的讨论范围。使用这种非特定的协议，AM 基于服务控制域策略，对客户机请求进行认证和授权。对通过这些检查的客户机请求，AM 根据它对所请求服务的了解程度，来确定向客户机提供服务所需的特殊的 QoS 参数。然后，它为这些资源向合适的策略服务器发送请求，策略服务器可根据网络或 RCD 策略情况拒绝该请求，或者向 CMTS 传送该请求，以进行准许进入控制和执行。

5.2.2.2 策略服务器（PS）

如 RFC 2753 [18]中所讨论的那样，作为 IPCablecom 多媒体基础的策略管理框架，基于 IETF 资源分配协议（RAP）工作小组的工作成果。由于策略服务器位于应用管理器与 CMTS 之间，因此它同时起着双重作用，一是作为 AM 发起之会话请求的“代理”，二是作为定义和执行资源控制域策略的“哨兵”。

如[18]中所述的那样，并与 IPCablecom-T DQoS 模型一致，策略服务器发挥有关 CMTS 的策略决定点（PDP）的作用，这样，策略服务器将执行电缆运营商定义的授权和资源管理程序。相反，策略服务器发挥有关应用管理器的策略执行点（PEP）的作用，原因是，它代理通往 CMTS 元素和来自 CMTS 元素的控制门消息。

为了再次回到交互情形，应用管理器向策略服务器发出策略请求。策略服务器充当这些请求的“哨兵”，并采用一组已由电缆运营商预先规定的策略规则。一旦通过检查，策略服务器随后将担负有关应用管理器和 CMTS 的“代理”，负责转发策略请求，并返回任何相关的响应。各个策略请求事务务必逐个进行处理。

策略决定可基于许多因素，例如：

- 与请求和可用资源状态相关的参数；
- 特殊客户机和相关简表信息的身份；
- 应用参数；
- 安全性考虑；
- 时间。

策略服务器的主要功能包括：

- 由应用管理器调用的策略决定请求机制；
- 执行已安装策略规则的策略决定请求“管理”机制；
- 用于在 CMTS 上安装策略决定的策略决定提交机制；
- 允许代表应用管理器向 CMTS 代理发布 QoS 管理消息的机制；
- 用于记录策略请求的、与记录保持服务器的事件记录接口，这些策略请求可依次与网络资源使用情况记录相关联。

由于策略服务器充当 AM 和 CMTS 元素（带有补充的客户机和服务器接口）之间的代理，一些电缆运营商可选择部署多个策略服务器层，并在这些服务器中指定某些策略决定，以便满足与可升级性和容错性相关的要求。

5.2.2.2.1 有状态和无状态的策略服务器

有两种基本类别的策略服务器：有状态的和无状态的。无状态的策略服务器稍有用词不当之嫌，因为它保存足够多的状态信息，以便将应用管理器请求映射至适当的 CMTS，并保持 COPS 会话状态，而一个纯的、无状态的策略服务器不保持任何媒体会话的状态。有状态的策略服务器有若干不同形式：有些参与准许进入控制，并因而监控活动的媒体会话的 QoS 属性，有些则把 QoS 和准许进入控制留给 CMTS，而监控来自应用管理器的、基于时间或基于容量的请求，有些策略服务器则介于这两者之间。

有多种类型策略服务器的原因是，存在众多运营商试图支持的环境。例如，有些运营商可能希望在同一 CMTS 上支持 IP-Cablecom 多媒体，它们用于 IP-Cablecom 电话中，并且可能想要单一的 CMS/策略服务器，该 CMS/策略服务器对在用的网络资源具备更加全面的观点。另一方面，一些运营商可能希望运营只有 IP-Cablecom 多媒体的环境，或者，它们可能使用更加简单的 CMTS 驱动机制来分割 IP-Cablecom 多媒体和电话资源。这些更为简单的配置对策略服务器保持的状态信息数量的要求更低。

策略服务器状态需求也可由策略服务器与应用管理器之间的信任等级来驱动：有状态的策略服务器比无状态的策略服务器能够更容易地对应用管理器的会话控制行为实施监管。因此，有状态的策略服务器可能更适于运营商支持第三方应用管理器。其它运营商可能取决于自身的经济情况来实现其与应用管理器的信任关系，或者它们可以控制应用管理器自身。在这些情况下，可能更适合使用无状态的策略服务器。

由于不可能对所有不同的媒体会话部件和策略服务器保持的网络 QoS 状态进行分类，因此设计的协议应不受这种复杂性的约束。有状态的策略服务器收集来自它所代理的应用管理器请求的、IP-Cablecom 多媒体媒体会话信息；而它要求的任何其它信息则通过其它一些机制进行收集，这些机制超出了本建议书的讨论范围。CMTS 和应用管理器在它们所连接的策略服务器类型方面并无区别，并且协议以这样一种方式进行设计，即策略服务器的类型对端点而言是透明的。策略服务器的类型仅对运营商而言是重要的。

由于某些类型的策略服务器试图支持准许进入控制，并可能对网络及其资源进行更大范围的检查，因此额外的状态同步问题可能出现在网络设计中，它包含不止一种这些策略服务器类型。运营商的责任是确保这些策略服务器的努力不被包括其它自主策略服务器在内的网络所破坏。

5.2.2.2.2 策略服务器修改请求和响应

尽管策略服务器名义上属于资源控制域的一部分，除了发挥它执行运营商所定义的授权和资源管理程序这些常规作用之外，策略服务器还可以充当服务与资源控制域之间的媒介。在这些性能的任何一种性能中，它都可以在将请求转发给 CMTS 之前对进入的请求进行修改。

在发挥 SCD 与 RCD 之间媒介作用的过程中，策略服务器可以将 SCD 中使用的字段格式或大小，转换成 RCD 中使用的字段格式或大小。例如，策略服务器可修改来自应用管理器（对 MSO 网络之外的 AM 来说，这样做尤为重要）的请求的“优先级”，以便该优先级字段在运营商的 RCD 中始终使用一致的大小。在其作为媒介的性能中，策略服务器可使用双向转换——换言之，它应转换从 AM 到 CMTS 的请求，并“反向转换”从 CMTS 到 AM 的响应。通过记住初始请求，有状态的策略服务器能够支持这样性能，并且如果转换功能是可倒转的，那么无状态的策略服务器也可支持它。

对某些对象的修改，尤其是分类符和通信业务简表对象，可导致在发起 AM 中出现操作问题。同样，策略服务器绝不修改这些对象。除了这些例外，由 PS 决定，依据规定的策略规则，对所有其它对象进行管理和修改。

5.2.2.3 电缆调制解调器终端系统（CMTS）

在描述 CMTS 网络元素的作用时，重要的是要考虑 CableModem、IPCablecom-T 和 IPCablecom 多媒体功能性之间的关系。这些建议书集中的各个建议书都提出了一组特定的功能要求，各个建议书也都以这样一种方式予以定义，即相应的实施方案可以以模块化的方式进行构建；在附件 B/J.112 CMTS 基础之上，采用增加额外的、补充的功能性选项作为业务说明，既可对 IPCablecom-T 进行分层，也可对 IPCablecom 多媒体控制门控制进行分层。此外，应强调指出，电话和多媒体变量都利用了大量的体系结构上的相似之处，这是 IPCablecom 体系结构的重要资产，它使得在基本的控制门管理模型中有可能实现再用。

IPCablecom 多媒体 CMTS 是 IPCablecom-T CMTS 的一个普及版，为了在 IPCablecom-T 网络中提供电话服务而定义了它。CMTS 负责执行来自一个或多个策略服务器的 QoS 请求。通过安装类似[9]中所定义的控制门那样的控制门，CMTS 执行这一功能；控制门允许订户的电缆调制解调器通过建立具有保证之 QoS 级别的动态 DOCSIS 流，来向 CMTS 请求网络资源。CMTS 还向记录保持服务器发送事件消息，详细说明 QoS 资源的实际使用情况。

5.2.2.4 记录保持服务器（RKS）

IPCablecom 多媒体记录保持服务器执行与 IPCablecom-T [10]中 RKS 类似的功能。它从策略服务器处接收有关策略决定的事件消息，并从 CMTS 处接收有关 QoS 资源使用情况的事件消息。

在 IPCablecom 多媒体体系结构中，记录保持服务器并不接收直接来自应用管理器的消息。不过，应用管理器能够在其发送给策略服务器的消息中嵌入不透明的数据，这些数据而后可包括在之后发送给 RKS 的事件消息中。

5.2.3 IPCablecom多媒体接口

IPCablecom 多媒体建立在 IPCablecom-T 建议书集基础之上。在 IPCablecom-T 中，IPCablecom 多媒体接口存在这样的必然性，即 IPCablecom 多媒体使用相同的协议，或者是同一协议的一个扩展。

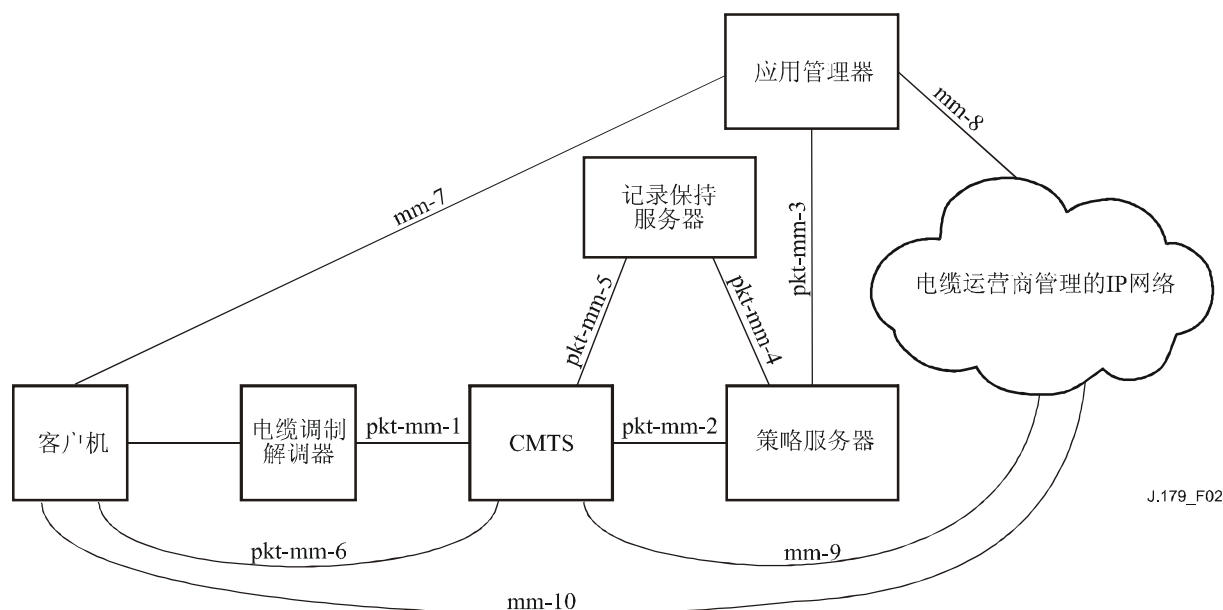


图 2/J.179—IPCablecom多媒体体系结构框架

表 1/J.179—IP Cablecom 多媒体接口

接 口	描 述	注 释
pkt-mm-1	CMTS – CM	电缆调制解调器 (CM) 可以通过附件 B/J.112 DSx 信令向 CMTS 提出请求。可选地, CMTS 可以再次通过 DSx 信令指导 CM 设立、拆卸或改变 DOCSIS 业务流, 以便满足 QoS 请求要求。
pkt-mm-2	PS – CMTS	该接口对策略管理框架至关重要, 它控制策略决定, 可以: a) 由策略服务器 (PS) 推送至 CMTS; 或者 b) 由 CMTS 自 PS 拉动。 接口还允许代理 QoS 代表客户机提出请求。 在某些情形下, 该接口还可用于告知 PS 何时 QoS 资源变得不活动了。
pkt-mm-3	AM – PS	应用管理器 (AM) 可以请求 PS 代表客户机在 CMTS 上安装策略决定。 该接口还可用于告知 AM 有关 QoS 资源状态的变化情况。
pkt-mm-4	PS – RKS	PS 向记录保持服务器 (RKS) 发送事件消息, 以跟踪与 QoS 相关的策略决定。
pkt-mm-5	CMTS – RKS	CMTS 发送 RKS 事件消息, 以跟踪有关 QoS 的请求和使用情况 (例如, 业务流增加、更改、删除和容量度量)。
pkt-mm-6	客户机 – CMTS	客户机可以使用该接口来直接请求和管理 QoS 网络资源。如果经授权, 这些资源由 CMTS 提供。
mm-7	客户机 – AM	客户机可以使用该接口来与 AM 进行交互作用, 并间接请求和管理 QoS 资源。该接口超出了本建议书该版本的讨论范围。
mm-8	AM – 对等	AM 可以使用该接口来与某些其它实体进行交互作用, 这些实体是在议应用的一部分。该接口超出了本建议书该版本的讨论范围。
mm-9	CMTS – 电缆运营商管理的 IP 网络	CMTS 上的该接口可用于支持接入网络之外的端到端 QoS 请求。该接口超出了本建议书该版本的讨论范围。
mm-10	客户机 – 对等	客户机可以使用该接口来与某些其它实体进行交互作用, 这些实体是在议应用的一部分。该接口超出了本建议书该版本的讨论范围。

5.2.3.1 客户机和应用管理器的接口 (mm-7)

客户机与应用管理器之间的接口超出了本建议书的讨论范围。典型地, 应用管理器将通过某种超出本建议书的方法, 来认证客户机, 并确保客户机有权使用多媒体服务。例如, 客户机可登录一个网页, 并通过提供用户名和密码来请求服务。不过, 当请求实现后, 应用管理器务必能够清楚无误地确定接收服务的电缆调制解调器, 原因是, 在能够交付 QoS 之前, 该信息务必能为网络运营商所用。

5.2.3.2 应用管理器和策略服务器的接口 (pkt-mm-3)

该接口对应呼叫代理与控制门控制器之间的 IPCablecom-T 接口。在 IPCablecom-T 中,它是一个隐蔽的、不可测试的接口,因此,关于此接口,并没有预先存在的协议要求。

IPCablecom 多媒体要求在该接口上使用 COPS [7]。为简化体系结构,并考虑到应用管理器与 CMTS 之间的策略服务器元素存在多个层次,该接口尽可能远地镜像策略服务器与 CMTS 之间的接口。尽管应用管理器是一种来自策略服务器的请求资源授权,实际上,它在 COPS 决定消息而不是在 COPS 请求消息中发出这一请求。这使得应用管理器与策略服务器之间的接口看起来和策略服务器与 CMTS 之间的接口是相同。应用管理器是相对策略服务器的 PDP,策略服务器是相对应用管理器的 PEP。

当应用管理器同意向客户机提供服务时,它将以 COPS 对象的形式发送一个 COPS 决定,COPS 决定(至少)包含下列信息:

- 发出请求的应用管理器的身份;
- 接受服务的客户机的身份;
- 规定通信业务封装的 RSVP 流规范。

在策略服务器的响应中,服务器包括一个认证令牌 Gate-ID,它由 CMTS 提供给服务器。

5.2.3.3 策略服务器和CMTS的接口 (pkt-mm-2)

该接口本质上等同于 IPCablecom-T 中的同等接口 (CMTS 与控制门控制器之间的接口)。与 IPCablecom-T 中的一样,COPS 用于转送策略服务器与 CMTS 之间的策略信息。CMTS 充当 COPS PEP 的作用,策略服务器充当 COPS PDP 的作用。依据 IPCablecom-T 模型,通过向 CMTS 发送一个 DQoS 控制门集消息(它是一个主动提供的 COPS DECISION 消息),策略服务器发起通信,进行多媒体会话。

该消息(至少)包含:

- 应用管理器 ID;
- 订户 ID;
- GateSpec;
- FlowSpec(s);
- 分类符。

与 DQoS 中一样,CMTS 或者以 Gate-Set-Ack,或者以 Gate-Set-Err (两者均为 COPS REPORT 消息)进行响应。

如果 CMTS 的响应是肯定的(即以 Gate-Set-Ack 响应),那么它包括一个 GateID。与 IPCablecom-T 中的一样,GateID 充当授权令牌的作用。不同于 IPCablecom-T,该令牌最终不发送给客户机(原因是,第 1 类客户机端点不了解 IPCablecom);相反,该令牌由策略服务器(如果是有状态的)和应用管理器持有,因此,允许它们发出关于本次 CMTS 会话的命令,在策略服务器的情况下,直接进行发送,在应用管理器的情况下,通过策略服务器间接进行发送。

5.2.3.4 记录保持服务器和策略服务器的接口 (pkt-mm-4) 以及记录保持服务器和CMTS的接口 (pkt-mm-5)

从策略服务器和 CMTS 至记录保持服务器的接口,等同于 IPCablecom-T 中的同等接口(分别自 CMS 和 CMTS)(参见[10])。这些接口用于传输 IPCablecom 事件消息,这些事件消息使用 RADIUS 格式化。在 IPCablecom 多媒体中,事件消息传送关于交付之服务的详细信息,包括建立和删除服务流的准确时间,以及(可选地)当服务流存在时,在其中通过的通信业务数量。

5.2.4 状态信息

在本节中，我们对 IPCablecom 多媒体系统中的状态定位做了概述。除了保留这些详细的状态信息外，出于记账、欺诈检测、会话重建等目的，设备还向记录保持服务器发送有关状态转变的信息。

5.2.4.1 应用状态

应用管理器始终负责保存有关应用媒体会话状态的详细资料。它具体是如何保存的超出了本建议书的讨论范围，但重要的是要认识到，除了应用管理器，不要求或期望其它任何设备保存有关应用状态的任何信息。

不过，应用管理器可以通过代理此类信息，经由策略服务器，将会话状态报告给记录保持服务器。此外，一些未经提炼的状态信息（如已对资源提出请求的事实）会自动地从策略服务器发送至记录保持服务器。

5.2.4.2 QoS资源状态

CMTS 自然知晓由它管理的流的详细状态。策略服务器（如果有状态的策略服务器）也可在单一的 CMTS 上保存 QoS 资源的状态信息；它还可比较若干 CMTS 上的状态信息，以便它（并且只有它）知晓整个系统的 QoS 状态。这可能是重要的，举例来说，如果运营商已经制定一个策略，依据该策略，只允许某个特定的应用消耗整个系统中规定百分比的资源，而不得超过。在只有无状态策略服务器的网络中，CMTS 是唯一保存 QoS 状态信息的设备。由于无状态策略服务器并不保存 GateID，因此它们甚至不能通过询问 CMTS 来获得有关特定多媒体会话的信息。

只要 QoS 资源的状态发生变化，只要删除 QoS 资源，就将从 CMTS 向记录保持服务器发送一个相应的事件消息。

6 授权接口描述

本节描述应用管理器与策略服务器之间以及策略服务器与 CMTS 之间的接口。

在转换时，应用管理器与策略服务器之间的接口和策略服务器与 CMTS 之间的接口是相称的。这些接口用于向 CMTS 传送授权、预留和激活信息，以提供从 CMTS 至策略服务器以及从策略服务器至应用管理器的状态信息。

应用管理器是服务控制域的 PDP。策略服务器是应用管理器的 PEP，并应用资源控制域策略。策略服务器是 CMTS 的 PDP，CMTS 是策略服务器的 PEP，位于实际的分组转发通路中。

本节描述使用 COPS 协议在应用管理器与策略服务器之间以及策略服务器与 CMTS 之间传送 IPCablecom QoS 消息。

6.1 控制门：QoS控制的框架

IPCablecom 多媒体控制门是有关已安装在 CMTS 上的策略决定的一种逻辑表述。控制门用于控制单个 IP 流对附件 B/J.112 电缆网络所提供之增强型 QoS 服务的访问。控制门是单向的；单个控制门控制上行流方向或下行流方向对流的访问，但不能同时控制两个方向上的访问。对双向 IP 会话，需要两个控制门，一个用于上行流方向，一个用于下行流方向，每个控制门通过唯一的 GateID 加以标识。重要的是认识到：这与 IPCablecom-T 有着根本区别，在 IPCablecom-T 中，单个 GateID 可同时涉及上行流和下行流控制门。

在 IPCablecom 多媒体中，各控制门均有一个单独的 GateID。控制门定义将由 CMTS 用于执行授权、预留和提交操作的授权、预留和提交封装。

在所有情形中，CMTS 都务必对封装执行准许进入控制检查，以确保提交的封装小于或等于预留的封装，而预留的封装小于或等于授权的封装（特定的 DOCSIS 准许进入控制要求请参见 [1]）。

在“代理的 QoS 策略推动”（情形 1）模型中，在 CMTS 对封装执行了必要的准许进入控制检查后，CMTS 使用控制门中的信息来直接创建附件 B/J.112 服务流。在附录一所述的其它两个模型中，即“带策略推动的、客户机请求的 QoS”（情形 2）和“带策略拉动的、客户机请求的 QoS”（情形 3）中，CMTS 使用控制门信息来对客户机请求的资源执行准许进入控制；CMTS 并不发起对流的创建。应用管理器负责向策略服务器发布控制门消息，策略服务器则负责应用策略规则，然后向 CMTS 发布控制门控制消息。

一个控制门由以下元素组成，将在本节后面对它们进行描述：

- GateID;
- AMID;
- SubscriberID;
- GateSpec;
- 分类符;
- 通信业务简表;
- 事件产生信息（可选的）;
- 基于事件的使用限制（可选的）;
- 基于容量的使用显示（可选的）;
- 不透明的数据（可选的）。

GateID 是控制门的句柄。GateID 由 CMTS 指定，并由应用管理器、策略服务器和客户机使用，用于引用控制门。

AMID 是用于标识应用管理器的句柄。

SubscriberID 唯一地标识客户机，策略是为该客户机而设置的。

GateSpec 描述特定的授权参数（即 QoS 限制、计时器等），用于定义一个控制门。

分类符描述将映射至 DOCSIS 服务流的 IP 流。

通信业务简表描述用于支持 IP 流的服务流 QoS 属性。

事件产生信息包含由 CMTS 用于记账和报告使用情况的信息。

基于容量的使用限制定义通信业务的容量上限，这些通信业务穿越与控制门相关的流。

基于时间的使用限制描述时间上限，它限制与控制门相关的流持续时间。

不透明的数据代表一个多用途的对象，它对 CMTS 和 PS 元素保持不透明，但可以包含对 AM 而言是重要的数据。如果由 AM 提供，那么该可选对象将保留在 CMTS 上，并在所有相关响应中予以返回（请参见第 6.4.2.11 节）。

这些元素通过 COPS 对象与策略服务器和 CMTS 进行通信，本节后面的内容将更详细地加以描述。在安装控制门的过程中，上述信息传送给 CMTS。在完成安装后，可创建一个 DOCSIS 服务流。在创建 DOCSIS 服务流后，控制门将与一个额外的元素相关联，即 DOCSIS 服务流。在 DOCSIS 服务流与控制门之间，存在严格的一对一映射。

控制门在多种状态间转换。在情形 2 和情形 3 中，客户机实体负责预留并随后激活 DOCSIS 服务流，多媒体控制门的工作方式与 IPCablecom-T DQoS 控制门的工作方式非常相似。当策略服务器在 CMTS 上安装控制门时，控制门被认为处于“授权”状态。在策略服务器明确删除控制门（或者，出于某种原因由 CMTS 自己删除，但这种情况不太可能出现）之前，或者来自客户机的动态流请求抵达之前，控制门继续保持这种状态。

当客户机请求增加动态服务流时，它将 GateID 作为一个授权令牌予以提交。CMTS 使用 GateID，依据控制门定义的授权封装，在 DOCSIS 动态流上执行准许进入控制。在情形 1 中，策略服务器指示 CMTS 代表应用管理器在状态间进行转换，CMTS 为负责发起和拆卸 DOCSIS 服务流的实体。本建议书中关于状态转换的这一节内容，描述的就是该行为。当 CMTS 得到指示拆卸 DOCSIS 服务流时，在 PS/AM 明确删除该服务流之前，或者服务流到期终止且其资源由 CMTS 回收（请参见第 6.5.8 节）之前，与之相关的控制门一直保持不变。不过，相反地，当 PS/AM 删除一个控制门时，CMTS 将删除相关的 DOCSIS 服务流。

6.1.1 控制门标识符 (GateID)

GateID 是由 CMTS 在本地分配的一个标识符，控制门驻留于其中。GateID 务必只与一个控制门相关联。尽管通常假定 IPCablecom-T DQoS 控制门模型是一对单向的控制门（一个上行流，一个下行流），每个 GateID 都支持典型的双向语音会话，但在此处，控制门 GateID 的关系是明确的一对一关系，这样是为了更易于支持广泛的多媒体服务。

当应用管理器发出 Gate-Set 请求时，它触发策略服务器向 CMTS 发出一个 Gate-Set 消息。当 CMTS 用一个包含 GateID 的确认消息进行响应时，策略服务器将这一包含 GateID 的响应回传给应用管理器。注意，由于 PS 与 CMTS 之间的关系可以是多对多的关系，不能保证由一个 CMTS 指派的 GateID 在整个网络中是唯一的，因此，PS 可使用 AM 的 AMID 以及 SubscriberID 和 GateID，以便唯一地确定控制门。

以下是可用于指派 GateID 值的算法。将 32 比特的字分为两部分，一个索引部分，一个随机部分。索引部分通过将控制门索引至一个小的表格来标识，同时，随机部分在某种程度上隐藏该数值。不管选择何种算法，通过确保在其结束或删除之前的三分钟内，任何 GateID 都不会再使用，CMTS 应尝试尽可能消除 GateID 的含糊性。对建议的算法，可以通过简单地为各个连续指派的 GateID 递增索引部分来实现，当索引部分达到最大整数值时，则归 0。

6.1.2 应用管理器标识符 (AMID)

各应用管理器都预提供一个 AMID，它在单个服务提供商领域内是唯一的；应用管理器在它发送给策略服务器的所有消息中都包括该标识符。经由控制门消息，策略服务器透明地将该信息发送给 CMTS。CMTS 务必将与控制门相关的 AMID 返回给策略服务器。策略服务器利用该信息将控制门消息与一个特定的应用管理器关联起来。

AMID 务必由服务提供商指派给应用管理器，其值在全球范围内是唯一的。应用管理器务必在其与策略服务器的所有交互中使用指派的 AMID。注意，由于应用管理器可以由第三方进行操作，而单个应用管理器可能与多个服务提供运营商交互，因此，可以为单个实际的应用管理器提供多个 AMID。

6.1.3 订户标识符 (SubscriberID)

SubscriberID 由客户机 CPE 设备或 CM 的 IP 地址组成，用于确定用户请求的服务。在复杂网络环境下，该地址可用于在众多策略服务器间路由控制门控制消息，并确定哪个 CMTS 正在向特定的端点提供服务。除了 P 地址之外，还可以通过 FQDN 或某种与在议服务相关的不透明数据（以下将要定义的对象）来确定订户。

6.1.4 控制门规范 (GateSpec)

GateSpec 描述控制门的某些高级属性，包含与控制门消息中规定的其它对象处理相关的信息。GateSpec 中包含的信息叙述如下：

- GateID;
- SessionClassID;
- 方向;
- 授权的计时器;
- 预留的计时器;
- 提交的计时器;
- 提交的回收计时器;
- DSCP/TOS 覆盖。

GateID 唯一地确定应为之执行操作的控制门。

SessionClassID 为应用管理器和策略服务器提供一种方法，用于将各控制门分为具有不同授权特性的不同类别。例如，人们可能使用 SessionClassID 来表示某种优先或抢占方案，这种方案将允许策略服务器或 CMTS 抢占预授权的控制门，以便允许具有更高优先级的新控制门获得授权。

方向指明控制门是用于上行流或是用于下行流。取决于这一方向，CMTS 务必相应地预留和激活 DOCSIS 流。

授权的计时器限定在预留之前务必保持有效的时间量（请参见第 6.2 节）。

预留的计时器限定在资源提交之前预留务必保持有效的时间量（请参见第 6.2 节）。

提交的计时器限定提交的服务流可保持空闲的时间量。

提交回收计时器限定以下时间量，即一旦 PS/AM 已被告知非活动，没有后续的、来自 PS/AM 的刷新消息的情况下，提交的服务流能够保持的时间量（请参见第 6.2 节）。

DSCP/TOS 覆盖字段可用于覆盖与对应控制门的、与 DSCP/TOS 服务流相关的 DSCP/TOS 分组字段。该字段可以是非特指的，在此情况下，分组中的 DSCP/TOS 字段不会被 CMTS 覆写。该字段既可用于上行流方向，也可用于下行流方向。

6.1.5 分类符

务必为控制门定义一个分类符。在最初的 Gate-Set 中，可以包括额外的分类符。在后续的 Gate-Set 中，可以增加或删除分类符。在处理 Gate-Set 消息时，符合要求的实施方案务必能够支持最少四个分类符。分类符确定将映射至控制门相关之 DOCSIS 服务流的 IP 流。用于构建一个服务流的分类符务必匹配于为控制门规定的分类符。在情形 1 中，当 CMTS 创建动态流时，它务必将控制门分类符用作 DOCSIS 服务流的分类符。

一个分类符是一个 8—多元组：

- 协议；
- 源 IP；
- 源端口；
- 目的地 IP；
- 目的地端口；
- 优先级；
- DSCP/TOS 掩码。

协议字段用于确定协议类型（如 IP、ICMP 等）。

源 IP 是 IP 流发起者的 IP 地址（如在 CMTS 上所看到的那样），而目的地 IP 是 IP 流的终点。

源端口与目的地端口用于规定 IP 流的 UDP 或 TCP 端口。

优先级可用于区分与某个特殊分组相匹配的多个分类符。由于分类符通常倾向于是唯一的，因此一般将优先级设为缺省值。

DSCP/TOS 字段用于确定 DSCP/TOS 字段，该字段务必对要在 IP 流上进行分类的分组相匹配。为在定义网络管理策略时提供最大的灵活性，定义了一个附加掩码，它决定在对分组进行分类时，DSCP/TOS 字节中使用那些位作为过滤器。这允许 DiffServ 和 TOS 这两种策略（在该字节内，各个策略定义和使用单独的位）。

分类符可以拥有通配的字段（由零字段表示），但务必小心，以便多个 IP 流不会无意中与同一个分类符相匹配，否则将导致无法预料的后果。

6.1.6 通信业务简表

表述控制门的通信业务简表有三种基本方法：

- 1) FlowSpec;
- 2) DOCSIS 服务类别名称；或者
- 3) DOCSIS 特定的参数。

策略服务器或应用管理器务必使用以下三种方法中的一种来定义控制门的通信业务简表：

- 1) FlowSpec;
- 2) DOCSIS 服务类别名称；或者
- 3) DOCSIS 特定的参数。

在通信业务简表中使用的所有封装务必为同一类型，也就是说，要么是 FlowSpec，要么是 DOCSIS 服务类别名称，要么是 DOCSIS 特定的参数。

第一次安装控制门时，务必至少规定一组通信业务简表参数。策略服务器和应用管理器可以规定第二组，用以代表预留的封装，第三组参数代表提交的封装。如果 CMTS 被告知，在收到 Gate-Set 消息（通过提交预留的或提交的封装）后应立即创建一个动态流，CMTS 务必使用预留的和提交的封装通信业务简表参数，来执行附件 B/J.112 消息发布，以便在 GateSpec 中方向字段规定的方向上创建流（假设请求已获授权，并存在满足请求要求的足够资源）。当获悉转换为提交状态时，CMTS 务必使用通信业务简表来激活 DOCSIS 服务流。作为一种最佳方案，策略服务器可告知 CMTS，代表应用管理器，经一个单个的控制门控制消息，来执行全部三种动作（授权、预留和提交）。可选地，PS/AM 可发出单独的 Gate-Set 消息，告知 CMTS 进行授权和预留，然后通过后续的 Gate-Set 消息来提交。

6.1.6.1 FlowSpec

FlowSpec 对象包含 RSVP FlowSpec，用于描述 IP 流的通信业务简表。FlowSpec 对象可包含多个 RSVP FlowSpec：

- 依据未来可能做出的预留定义授权资源封装的 FlowSpec。
- 依据未来可能做出的提交请求定义预留封装的 FlowSpec。
- 定义待提交资源的 FlowSpec。

RSVP FlowSpec 支持两种类型的服务：受控负载服务[4]和保证服务[5]。第 8 节讨论了两种服务类型之间的主要区别。根据在 RSVP FlowSpec 中规定的 FlowSpec 服务编号，可以区分这两种服务类型。服务编号 5 针对的是受控负载服务，服务编号 2 针对的是保证服务。受控负载服务务必只包含 TSpec 令牌桶参数，不得包括 Rspec。保证服务务必同时包含 TSpec 和 RSpec。

有关如何将 RSVP 参数明确地映射至 DOCSIS 参数的信息，请参考第 8 节。当使用 RSVP FlowSpec 参数获得 DOCSIS 参数时，某些 DOCSIS 参数极为相近。如果这些近似值没有提供它所期望的、对策略服务器或应用管理器的控制，那么 PS/AM 可使用其它方法来定义通信业务简表，包括定义某些 DOCSIS 特定参数的能力。这些参数允许策略服务器或应用管理器对 FlowSpec 至 DOCSIS 参数的标准映射进行微调。

6.1.6.2 DOCSIS服务类别名称

DOCSIS 服务类别名称指明用于描述 QoS 属性的 DOCSIS 服务类别。CMTS 务必支持 DOCSIS 服务类别名称。

DOCSIS 服务类别名称使人们能够使用在 CMTS 上预提供的 DOCSIS QoS 参数。在 CMTS 上，人们可以用不同的 DOCSIS QoS 简表来配置 DOCSIS 服务类别名称，然后，参考控制门中的 DOCSIS 服务类别名称，间接地将一个 QoS 简表与某个特殊的控制门关联起来。DOCSIS 还允许在使用 TLV 过程中对参数进行修改。在 IPCablecom 多媒体内，绝不能在 TVL 使用过程中对 DOCSIS 服务类别名称 QoS 参数进行修改。如果请求修改服务类别名称 QoS 参数，那么 CMTS 务必返回一个“未定义服务类别名称”错误（请参见第 6.4.2.14 节）。

有关 DOCSIS 服务类别名称的更多信息，请参考 B.10.1.3/J.112 [1]。

6.1.6.3 DOCSIS特定的参数化

定义通信业务简表的第三种方法包括使用 DOCSIS 特定的通信业务简表；这允许应用管理器明确规定 DOCSIS 流的 DOCSIS 参数。如果应用管理器希望使用第三种方法定义通信业务简表，那么它务必包括一个含有 DOCSIS 特定参数的对象。

通过若干不同的通信业务简表 S-Type，可支持所有的 DOCSIS 服务流调度类型。各 S-Type 拥有一个与该服务流调度类型相关的、DOCSIS 特定参数的不同编码。有关 DOCSIS 特定参数化的更多详情，请参考第 6.4.2.7 节。

6.1.7 事件产生信息

该对象包含与 CMTS 相关的信息，以支持结算和记账功能。属性包括：

- 主地址：主记录保持服务器的端口，CMTS 务必向它发送事件记录。
- 副地址：副记录保持服务器的端口，如果主记录保持服务器不可用，那么 CMTS 务必按 [10]中所规定的那样使用副记录保持服务器。
- 标志，指明 CMTS 是否务必实时向记录保持服务器发送事件消息，或者指明 CMTS 是否务必批处理事件消息，并定期发送它们。
- 记账相关 ID，CMTS 务必向带有各自事件记录的记录保持服务器传送记账相关 ID。

省略事件产生信息对象表示 CMTS 绝不为其特定的控制门产生事件消息。

6.1.8 基于时间的使用限制

该对象规定在达到该控制门的时间限制门限之前，控制门能够保持提交状态的时间量。该对象对 CMTS 是不透明的。CMTS 不负责执行时间限制，但务必保存该对象，并在请求时返回该对象。

6.1.9 基于容量的使用限制

当固定数量的数据已穿越控制门时，应用管理器使用基于容量的使用限制通知 CMTS 产生一个控制门控制消息。CMTS 不负责执行容量限制，但当达到容量限制时，务必通知 PS/AM。

6.1.10 不透明的数据

不透明的数据包括应用管理器或策略服务器能够储存于 CMTS 上的一般信息。该数据对 CMTS 保持不透明，但包含对 PS 或 AM 有用的信息。如果由 PS/AM 提供，那么 CMTS 将在所有响应中返回该对象（请参见第 6.4.2.11 节）。

6.1.11 控制门时间信息

控制门时间信息包括一个表示控制门提交时间的时戳。应用管理器或策略服务器可以查询和使用这一信息来执行基于时间的网络策略。

6.1.12 控制门使用信息

控制门使用信息包括一个八位字节计数器，指明通过该控制门传输的数据字节数（请参见第 6.4.2.13 节）。类似于控制门时间信息对象，该信息可由策略服务器或应用管理器使用，以执行基于容量的网络策略。

6.2 控制门转换

如之前所简要概述的那样，一个控制门可驻留于以下逻辑状态：

- 授权的 — 策略服务器已用定义的资源限制对流进行授权；
- 预留的 — 已为流预留的资源；
- 提交的 — 活动的和正在使用的资源；
- 提交的一回收 — 已在流上检测为非活动的；未决的资源回收。

对图 3 中所述的状态机，在其转换控制门状态之前，CMTS 务必以成功的结果完成触发事件。对控制门事件，在请求得到全面处理（包括任何因此发生的流转换）且 CMTS 确定传输了成功地确认消息之前，CMTS 绝不能改变状态。

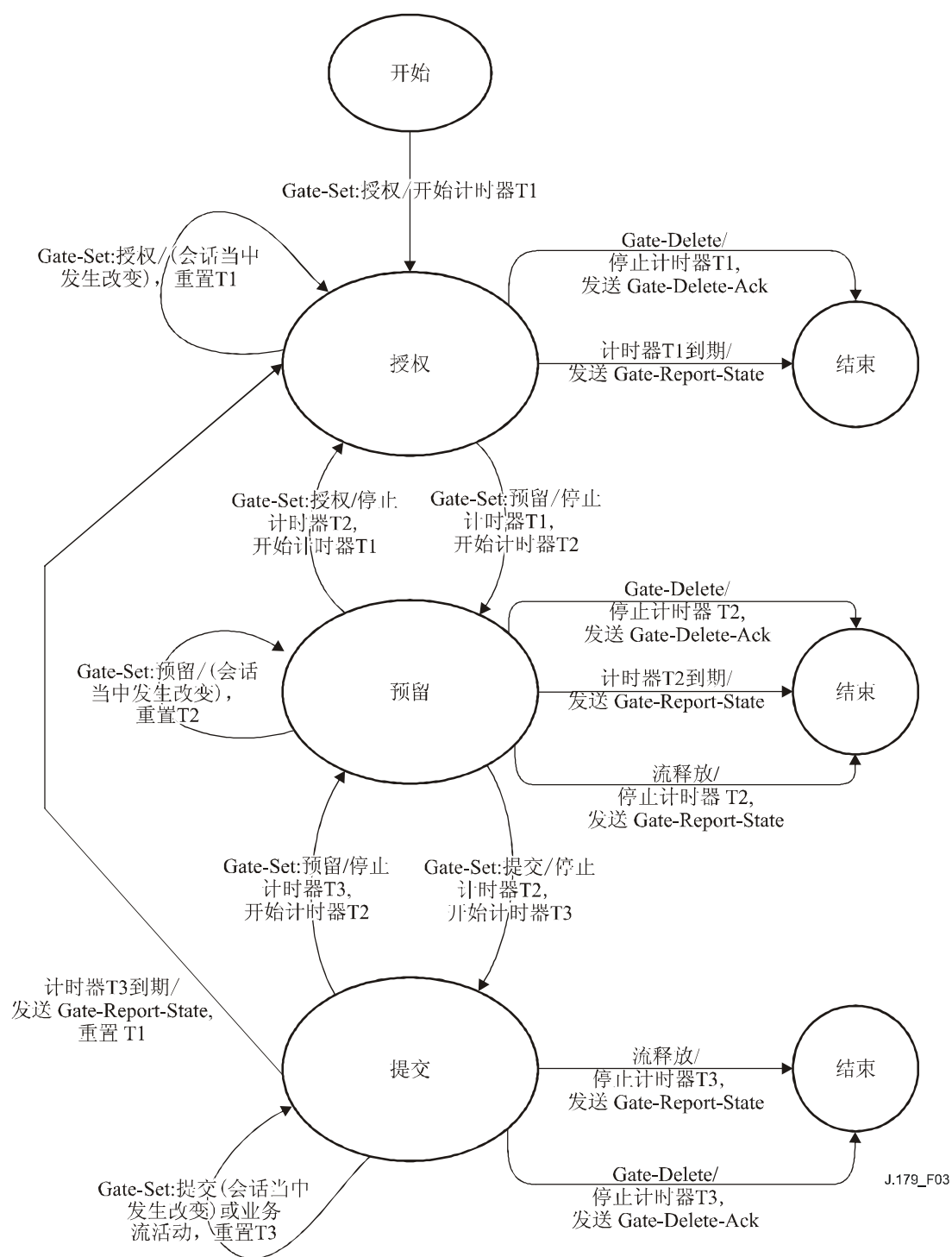


图 3/J.179—控制门状态转换

如图 3 所示及本节所述，CMTS 务必支持控制门状态和转换。CMTS 还务必为协议错误处理执行转换。

在本节中，我们描述了 CMTS 中因外部事件（来自策略服务器的控制门控制消息）而导致的控制门状态转换，以及因内部事件（如计时器到期）而导致的转换。注意，策略服务器并不是外部事件的源；相反，策略服务器只起策略服务器代理的作用，它是事件的触发器。

6.2.1 授权的

通过来自策略服务器的 **Gate-Set** 命令，在 CMTS 中建立一个控制门。CMTS 分配一个唯一的标识符，称为 **GateID**。现在，控制门被认为是处于授权状态，CMTS 务必启动计时器 T1。计时器 T1 限定授权保持有效的时间。

处于授权状态的控制门务必在收到 **Gate-Delete** 消息后予以删除。在删除控制门时，CMTS 务必用一个 **Gate-Delete-Ack** 消息予以响应，并务必停止计时器 T1。

当控制门处于授权状态时，要求 CMTS 支持以下状态转变：

授权的状态转变：

- 从授权回送到授权：修改授权的封装；
- 从授权到预留（定义预留的封装 $\leq$ 授权的封装）；
- 从授权到终止（删除授权的封装）。

当控制门处于授权状态时，CMTS 绝不支持任何其它状态转变，但许多单独的激励可以产生所述的转变。

在安装控制门时，控制门被认为是处于授权状态。在处于授权状态时，策略服务器可以修改任何与控制门相关的参数（如通信业务简表、分类符等）。如果在授权状态下收到一个 **Gate-Set** 消息，该消息表示并不将控制门转换至预留或提交状态，那么 CMTS 务必重新启动计时器 T1。

在处于授权状态时，CMTS 务必在成功请求策略服务器后，将控制门转换为预留状态。从策略服务器收到 **Gate-Delete** 后，或在 T1 计时器到期后，CMTS 务必将控制门转换为终止状态。

6.2.2 预留的

处于授权状态的控制门希望客户机努力预留资源。在情形 1 中，策略服务器代表客户机预留资源。为了预留资源，策略服务器务必发出一个带通信业务简表的后续 **Gate-Set** 消息，它包括预留的封装。在收到该预留请求后，CMTS 务必对请求进行校验，看它是否处于为控制门设定的授权权限内，并执行准许进入控制程序。

如果在计时器 T1 到期之前预留请求未抵达，那么 CMTS 务必删除控制门，并告知策略服务器有关状态变化情况。如果成功执行了准许进入控制，并且只请求了资源预留，那么 CMTS 务必使控制门处于预留状态。同时，CMTS 还务必停止计时器 T1，并启动计时器 2（预留的计时器）。如果准许进入控制程序未获成功，那么 CMTS 务必将控制门保持在授权的状态，并向 PS 提供一个 **Gate-Set-Err** 响应。

当控制门处于预留状态时，要求 CMTS 支持以下状态转变：

预留的状态转变：

- 从预留回送到预留：修改授权的封装（ $\geq$ 预留的封装）；
- 从预留回送到预留：修改预留的封装（ $\leq$ 授权的封装）；
- 从预留到提交（定义提交的封装 $\leq$ 预留的封装）；
- 从预留到终止（删除预留的和授权的封装）。

当控制门处于预留状态时，CMTS 绝不支持任何其它状态转变，但许多单独的激励可以产生所述的转变。

只要预留的封装小于或等于授权的封装，如果策略服务器提出请求，且请求通过了准许进入控制，并成功预留了流，那么 CMTS 务必将控制门从授权的状态转换为预留的状态。一旦处于预留的状态，那么可通过一个 Gate-Set 消息来修改控制门的授权封装。在预留的状态下，还可以修改控制门的预留封装（请参见第 6.5.6 节）。如果在预留的状态下收到一个 Gate-Set 消息，它不将控制门转换为授权的或提交的状态，那么 CMTS 务必重新启动计时器 T2。

如果在 T2 计时器到期之前，提交请求未抵达，那么 CMTS 务必删除控制门，并告知策略服务器状态变化情况。

预留的封装务必总是小于或等于授权的封装。在预留的状态下，为使 CMTS 将控制门状态转换为提交的状态，提交的封装务必小于或等于预留的封装（请参见第 6.5.3 节）。

当处于预留的状态时，策略服务器可通过在 Gate-Set 消息中规定一个新的通信业务简表来修改授权的封装。新的通信业务简表将定义一个修改后的授权封装，并且之前使用的同一预留封装将使控制门转换为预留的状态。不过，所有修改授权的、预留的或提交的封装的请求，都务必遵循以下一般规则：

授权的封装 $\geq$ 预留的封装 $\geq$ 提交的封装

通过发布一个 Gate-Delete 消息，策略服务器可以删除一个处于预留状态的控制门。

6.2.3 提交的

处于预留状态的控制门希望客户机提交资源，并在此激活它们。在情形 1 中，策略服务器代表客户机提交资源。为了提交资源，策略服务器务必发出一个带通信业务简表的 Gate-Set 命令，它包括提交的封装。CMTS 务必依据预留的封装，再次授权请求的 QoS。如果授权成功，那么 CMTS 务必启动计时器 T3，如果授权的封装等于提交的封装，那么停止计时器 T2，或者如果授权的封装大于提交的封装，那么重新启动计时器 T2。如果授权失败，那么 CMTS 务必重新设置计时器 T2。

注意，一旦激活 DOCSIS 服务流，当数据在流上进行传输时，CMTS 务必刷新计时器 T3。如果当时间等于 T3 时，流上没有活动，那么 CMTS 务必告知策略服务器有关状态变化情况。同样，策略服务器务必告知应用管理器有关状态变化情况。

在提交的状态下，应用管理器可通过向策略服务器发送一个 Gate-Delete 消息来删除控制门，它务必依次将该消息转发给 CMTS。如果策略服务器向 CMTS 发送一个 Gate-Delete 消息，那么 CMTS 务必删除控制门和相应的服务流，如果计时器 T2 和 T3 正在运行，那么停止它们。

当控制门处于提交状态时，要求 CMTS 支持以下状态转变：

提交的状态转变：

- 从提交回送到提交：修改授权的封装（ $\geq$ 预留的封装）；
- 从提交回送到提交：修改预留的封装（ $\geq$ 提交的封装）和（ $\leq$ 授权的封装）；
- 从提交回送到提交：修改提交的封装（ $\leq$ 预留的封装）；
- 从提交到预留（删除提交的封装）；
- 从提交到提交回收：（启动资源回收进程）；
- 从提交到终止（删除提交的、预留的和授权的封装）。

当控制门处于提交状态时，CMTS 绝不支持任何其它状态转变，但许多单独的激励可以产生所述的转变。

当处于预留的状态时，只要提交的封装小于或等于预留的封装，如果策略服务器提出请求，那么 CMTS 务必将控制门转换为提交的状态（请参见第 6.5.3 节）。当处于提交的状态时，只要授权的封装大于或等于预留的封装，那么通过 Gate-Delete 消息，策略服务器可以更改控制门的授权封装。在这种状态下，只要预留的封装大于或等于提交的封装，那么策略服务器还可以更改预留的封装。在这种状态下，只要新的封装小于或等于预留的封装，那么策略服务器甚至可以更改提交的封装。当控制门处于提交状态时，如果收到解除提交所有资源的请求（但保持它们预留的状态），那么 CMTS 务必停止计时器 T3，（重新）启动计时器 T2，并转换回预留的状态。在情形 1 下，通过发送一个包括授权封装和预留封装但不包括提交封装的、带通信业务简表的 Gate-Set 消息，策略服务器可以请求这种动作。

当处于提交的状态时，一旦收到来自策略服务器的 Gate-Delete 消息，CMTS 务必将控制门转换为终止状态。当处于提交的状态时，通过简单规定新的通信业务简表，策略服务器可以更改授权封装或预留封装；新的通信业务简表务必包含更改过的授权封装或预留封装，以及之前用于将控制门转换为提交状态的同一个提交封装。

当因收到 Gate-Set 消息而（重新）进入提交状态时，如果预留的封装大于提交的封装，那么 CMTS 务必（重新）启动计时器 2，或者如果之前它正在运行，且当前预留的封装等于提交的封装，那么务必停止计时器 T2。

当处于提交状态时：

- 1) 如果计时器 T2 到期，那么控制门务必保持在提交的状态，CMTS 务必向策略服务器发送一个带理由代码 9（控制门状态未改变，但 T2 计时器到期并导致预留减少）的控制门报告状态消息，指明预留的资源已减少；
- 2) 如果 Gate-Set 将控制门转换回预留的状态，那么若计时器 T2 未运行，则务必启动它，若计时器 T2 之前已运行，则务必重新启动；并且
- 3) 如果出现至终止状态的转换，那么若计时器 T2 和 T3 正在运行，则务必停止它们。

对情形 1，最理想的状况是：策略服务器通过发送一个带通信业务简表（包括全部三种封装设置）的 Gate-Set 消息，可以同时授权、预留和提交，这样告知 CMTS 继续执行全部三种动作，而无须与策略服务器做任何进一步的交互：也就是说，它们务必全部成功（如果这样，那么 CMTS 务必通过一个 Gate-Set-Ack 消息来指明这一点）或失败（如果这样，那么 CMTS 务必通过一个 Gate-Set-Err 消息来指明这一点）。

由于计时器 T3 到期，控制门从提交的状态转变为提交的一回收状态。如果在 T3 期间，CMTS 在相关的流上未检测任何活动，那么 CMTS 务必启动计时器 T4，产生一个控制门报告状态消息，发送至策略服务器，指明在计时器 T3 定义的时间期限内流是不活动的，并转换至提交的一回收状态，同时将相关的流继续保持激活状态。策略服务器务必将控制门报告状态消息转发给应用管理器。应用管理器务必执行以下操作：通过发送个 Gate-Set 消息，刷新策略，或者通过发送一个 Gate-Delete 消息，删除控制门。

当流上的活动停止时，可能不希望将之通知某些应用。在这种情况下，应用管理器可以将计时器 T3（它对应 DOCSIS 活动计时器）设为 0。如[1]中所规定的那样，DOCSIS 活动计时器其值为 0，表明对该流关闭了 CMTS 的活动性检测。因此，控制门将一直保持在提交的状态，直至收到一个 Gate-Delete 消息或者 CM 离线。

6.2.4 提交的一回收

在提交的状态，与流相关的控制门是活动的。如果 CMTS 检测到在超过 T3 计时器的一段时间内流未被使用，那么 CMTS 告知 PS（由 PS 告知 AM），与控制门相关的服务流未被使用，启动计时器 T4，并将控制门转换为提交的一回收状态。

注一 如果计时器 T2 正在运行，那么它将继续运行。绝不能对它重新进行设置。

AM 务必决定，要么通过向 PS 发送一个 Gate-Set 消息来刷新策略，要么通过向 PS 发送一个 Gate-Delete 消息来删除控制门。策略服务器务必向 CMTS 转发 Gate-Set 消息或 Gate-Delete 消息。

当处于提交的一回收状态时，如果 CMTS 在计时器 T4 到期之前收到一个控制门的 Gate-Set 消息，那么 CMTS 务必停止计时器 T4，重新启动计时器 T3，将控制门转换回提交的状态，如果预留的封装大于提交的封装，那么（重新）启动计时器 T2，或者，如果它正在运行，且新的预留封装等于提交封装，那么停止计时器 T2。

当处于提交的一回收状态时，如果 CMTS 在计时器 T4 到期之前收到一个 Gate-Delete 消息，那么 CMTS 务必停止计时器 T4，删除控制门和相应的服务流，如果它正在运转，那么停止计时器 T2。

当处于提交的一回收状态时，如果计时器 T4 到期，那么 CMTS 务必向 PS 发送一个控制门报告状态消息，如果计时器 T2 正在运行，那么停止它，拆卸与控制门相关的服务流，然后删除控制门。同样，策略服务器务必告知应用管理器有关状态变化情况。

当处于提交的一回收状态时，如果计时器 T2 到期，那么控制门务必保持在提交的一回收状态，CMTS 务必向策略服务器发送一个带理由代码 9 的控制门报告状态消息（控制门状态未改变，但计时器 T2 到期，导致预留减少），表明预留的资源已减少。

当控制门处于提交回收状态时，CMTS 务必支持以下状态转变：

提交回收状态转变：

- 从提交回收到提交：（策略已经更新）；
- 从提交回收到终止（删除提交的、预留的和授权的封装）；
- 从提交回收到提交回收（计时器 T2 到期；发送 Gate-Report-State）。

当控制门处于提交回收状态时，CMTS 绝不支持任何其它状态转变，但许多单独的激励可以产生所述的转变。

一旦检测到非活动，一些应用可能不希望保留控制门。在这种情况下，AM 可将计时器 T4 设为 0。当 T4 设为 0 时，本质上在提交的一回收状态中未耗费任何时间，并且当计时器 T3 到期时，务必删除控制门（和流）。

6.3 IPCablecom多媒体的COPS简表

如之前所定义的那样，准许进入控制涉及根据管理策略和可用资源对 QoS 资源请求进行管理的过程。附录一中描述了与该过程相关的高级操作模块。根据这一模型，管理策略保存在策略数据库中，且由策略服务器进行控制。

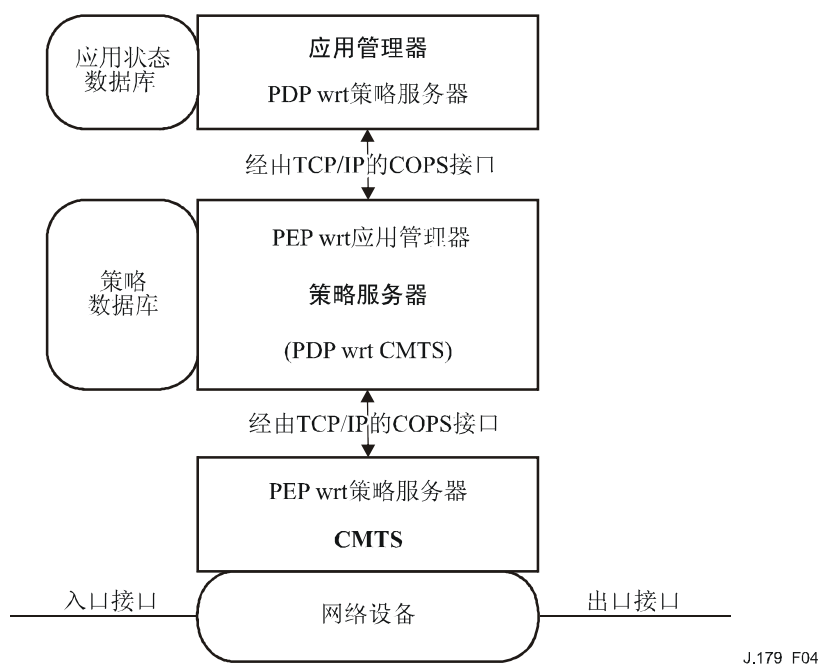


图 4/J.179—QoS准许进入控制计划

由策略服务器做出的准许进入控制决定，务必使用 COPS 传送给 CMTS 或应用管理器。CMTS 可依据通过 QoS 信令协议触发的网络事件，或者通过数据流检测机制触发的网络事件，提出 QoS 准许进入控制请求。网络事件也可能需要 QoS 带宽管理，例如，一个新的、具有 QoS 功能的接口变为可操作的接口。

依据来自应用管理器的请求，由策略服务器做出的 QoS 策略决定可推送至 CMTS。CMTS 可访问该决定的信息，以便对 CMTS 上收到的进入会话请求作出策略执行决定。在 IPCablecom 多媒体中，CMTS 绝不支持 CM 发起的 DSx 消息。CMTS 务必将由 CM 发起的 DSx 消息看作是一个带无效 GateID 的请求。

在 IETF 的 COPS 协议[7]中，规定了支持 QoS 准许进入控制的 COPS 客户机/服务器配置。该协议包括以下操作：

- 客户机—打开 (OPN) /客户机—接受 (CAT) /客户机—关闭 (CC)。COPS 客户机 (PEP) 发送一个 OPN 消息，与 COPS 服务器 (PDP) 建立连接，服务器以一个 CAT 消息予以响应，接受该连接。服务器或客户机发送一个 CC 消息，以停止连接。
- 请求 (REQ)。客户机向服务器发送一个 REQ 消息，请求准许进入控制决定信息或设备配置信息。REQ 消息可包含服务器使用的客户特定信息，加上在会话准入策略数据库中的数据，做出基于策略的决定。
- 决定 (DEC)。服务器通过向发出最初请求的客户机回送一个 DEC 来响应 REQ。为响应 REQ (即请求的 DEC)，或者在改变或更新之前的决定之后的任何时候 (即主动提供的 DEC)，可以立即发送 DEC 消息。

- 报告—状态（RPT）。客户机向服务器发送一个 RPT 消息，指明客户机中请求状态的变化情况。客户机发送这一消息来告知服务器有关服务器准许进入后实际预留的资源。客户机还可使用报告状态来定期告知服务器有关客户机当前状态的情况。
- 删除—请求—状态（DRQ）。客户机向服务器发送一个 DEL 消息，请求清除状态。这可以由客户机释放的 QoS 资源结果。
- 保持—活动（KA）。由客户机和服务器二者发送，旨在通知检测失败。
- 同步—状态—请求（SSQ）/同步—状态—完成（SSC）。服务器向客户机发送 SSQ 消息，请求当前状态信息。客户机向服务器重新发送请求查询，以执行同步，然后发送一个 SSC 消息，指明完成同步事件。如果是策略服务器从 CMTS 处获得或重新建立状态所需，那么策略服务器可支持 SSQ/SSC 同步功能。CMTS 务必支持 SSQ/SSC 同步功能。

在 IPCablecom 多媒体体系结构中，PDP-PEP 之间的关系如下所述：

- 相对策略服务器，应用管理器是一个 COPS 策略决定点（PDP）。
- 相对应用管理器，策略服务器是一个 PEP。
- 相对 CMTS，策略服务器是一个 PDP。
- 相对策略服务器，CMTS 是一个 PEP。

尽管 IPCablecom 多媒体要求的 COPS 消息内容与 COPS 协议是一致的，但在 COPS 会话开始的方式上仍存在微小差别，并在响应排序要求上有所放宽。RFC 2748 [7]声明：

“COPS 协议在 PEP 与远程 PDP 之间使用单一持久的 TCP 连接。每个服务器的一次 PDP 执行务必监听一个众多周知的 TCP 端口号（COPS = 3288 [IANA]）。PEP 负责开始建立与 PDP 的 TCP 连接”。

该声明的最后一句说，由 PEP 负责建立 TCP 连接。相反，在 IPCablecom 模型中，CMTS（PEP）是负责监听所指派端口 3918 的设备，且策略服务器务必建立与 CMTS 的 TCP 连接。这与 RFC 中所描述的模型是相反的。不过，只要存在 TCP 连接，在 COPS 协议中，CMTS 以一种与客户机或 PEP 一致的方式开展工作。同样，策略服务器（PEP）监听所指派的端口 3918，且应用管理器务必建立与策略服务器的 TPC 连接。

注意，IPCablecom 多媒体和 IPCablecom-T DQoS 监听不同的端口，以便 CMTS 可以用适当的客户机类型发起 COPS 会话。

RFC 2748 还声明：

“由特定客户机句柄的决定所请求的 RPT 消息，务必设定请求的消息标志，并务必以与其收到的相应决定消息相同的次序进行发送”。

COPS 协议使用 RPT 次序和决定消息，以使请求与响应相匹配。相反，PacketCable 多媒体实施方案务必使用 TransactionID，以使响应与请求相匹配，并应在其准备就绪后立即发送 RPT 消息。

RFC 2748 提供了有关 COPS 协议的详细资料。该 IETF RFC 描述了基本的 COPS 协议，它独立于客户机类型。IPCablecom 体系结构也与 IETF RFC 3084 [19] 相一致。COPS-PR 声明：

“在 COPS-PR 中，策略请求描述 PEP 及其可配置的参数（不仅是一个操作事件）。如果这些基本参数发生变化，那么发送一个最新的请求。因此，很少发送请求。决定不必直接映射至请求，并且通常在 PDP 对外部事件或 PDP 事件（策略更新）做出响应时，予以发布”。

当这一概念映射至 IPCablecom 多媒体体系结构时，PEP 向 PDP 发出一个请求，规定客户机句柄。然后，该客户机句柄将用在今后从 PDP 到 PEP 的所有决定消息中。这些决定消息传输为 DQoS 和多媒体客户机类型而定义的控制门控制消息（即 Gate-Set、Gate-Info 和 Gate-Delete）。客户机句柄用于唯一确定 PDP-PEP 关联。

在 IPCablecom 多媒体体系结构中，可以有多个应用管理器，它们与一个或多个策略服务器相互作用。以下是每个 TCP 连接的 IPCablecom 多媒体 COPS 会话的一个例子；当中，IPCablecom 多媒体 COPS 会话指的是与单个客户机句柄相关联的 PEP 与 PEP 之间的控制门消息。这意味着，在应用管理器与策略服务器之间存在一个 COPS-TCP 连接。同样，可能有一个或多个策略服务器与一个或多个 CMTS 对话。当连接至多个 PDP 时，PEP 务必确保使用的客户机句柄对每个连接是唯一的。

6.4 控制门控制协议消息格式

控制门控制协议消息务必在 COPS 协议消息中进行传输。PDP 和 PEP 务必为通信建立和使用 TCP 连接，并使用[11]中规定的机制来保证通信通路的安全。

6.4.1 COPS公共消息格式

各 COPS 消息包括 COPS 报头，之后是诸多类型的对象。应用管理器、策略服务器和 CMTS 务必使用下面定义的 COPS 公共消息格式作为所有消息交换的消息格式。在随后的对象规范中，由于所有的对象都务必在 4-字节的边界上对齐，因此每一行都表示一个 4-字节。

0		1	2	3
版本	标志	操作码	客户机类型	
消息长度				

版本是提供当前 COPS 版本号的一个 4-位字段。该字段务必设为 1。

标志是一个 4-位字段。最低有效位是请求的消息标志。当发送一个 COPS 消息以响应另一个消息时（例如，为响应一个请求而发送的一个请求决定），该标志务必设为 1。在其它情况下（例如，一个主动提供的决定），绝不能设定此标志（值 = 0）。与 DQoS 模型一致，响应请求消息的第一个决定消息是一个请求的响应，并且务必设定其请求的消息标志。所有其它的决定消息都是主动提供的，并且务必清除请求的消息标志。所有其它的标志务必设为 0。

操作码是一个 1-字节的无符号整数字段，给出将要执行的 COPS 操作。在本 IPCablecom 建议书中使用的 COPS 操作是：

- 1 = 请求 (REQ);
- 2 = 决定 (DEC);
- 3 = 报告—状态 (RPT);

- 4 = 删除请求状态 (DRQ);
- 5 = 同步状态请求 (SSQ);
- 6 = 客户机—打开 (OPN);
- 7 = 客户机—接受 (CAT);
- 8 = 客户机—关闭 (CC);
- 9 = 保持—活动 (KA);
- 10 = 同步状态完成 (SSC)。

客户机类型是一个 2-字节的无符号整数标识符。为供 IPcablecom 多媒体使用，客户机类型务必设为 IPcablecom 多媒体客户机 (0x800A)。对保持活动消息 (操作码 = 9)，客户机类型务必设为 0，原因是，KA 用于连接验证，而不是用于每个客户机的会话验证。

消息长度是一个 4-字节的无符号整数值，以八位字节为单位给出整个消息的大小。消息务必在 4-字节的边界上对齐，因此，长度务必是 4 的倍数。

在 COPS 公共报头之后是一个或多个对象。所有的对象都务必遵循相同的对象格式，其中，各对象包括一个或多个带有一个 4-八位字节报头的 4-字节字，使用以下格式。

0	1	2	3
长度		C-Num	C-Type
对象内容			

长度是一个 2-字节的无符号整数值，它务必提供组成该对象的字节数 (包括报头)。如果以八位字节为单位的最初长度不是 4 的倍数，那么务必在对象末端添加填充字节，以便使之能够与下一个 4-字节边界对齐。

C-Num 确定包含在对象中的信息类别，而 C-Type 确定包含在对象中的信息子类型或版本。在本建议书中使用的标准 COPS 对象 (如[7]所定义) 及其 C-Num 值为：

- 1 = 句柄;
- 2 = 正文;
- 6 = 决定;
- 8 = 错误;
- 9 = 客户机特定的信息;
- 10 = 保持—活动—计时器;
- 11 = PEP 身份;
- 12 = 报告类型。

这些对象中的各个对象都务必满足与 RFC 2748 中定义之单个对象有关的格式和规则要求。

6.4.2 控制门控制的额外COPS对象

利用 COPS-PR 和 COPS-RSVP 简表，IPcablecom 客户机类型定义了许多额外的对象格式。当在决定消息中从 PDP 传送至 PDP 时，这些对象务必置于决定对象内，C-Num = 6、C-Type = 4 (客户机特定的决定数据)。当在报告状态消息或客户机打开消息中从 PEP 传送至 PDP 时，它们也务必置于 ClientSI 对象中，C-Num = 9、C-Type = 1 (告知的 ClientSI)。

这些对象与 COPS-PR 的客户机特定对象编码方式等同，并使用独立于最高级 COPS 对象号码空间的客户机特定号码空间，对这些对象与 COPS-PR 中的对象一样进行编码。出于该原因，对象号码和类型分别假定为 S-Num 和 S-Type。S-Num 和 S-Type 务必分别为一个八位字节。COPS 长度字段务必为两个八位字节。定义额外的 COPS 对象供以下各节中的 IPCablecom 多媒体使用。

6.4.2.1 TransactionID

TransactionID 是一个 2-字节的无符号整数，它包含一个令牌，该令牌由应用管理器使用，以匹配来自策略服务器的响应，并由策略服务器使用，以使来自 CMTS 的响应与之前的请求相匹配。TransactionID 还务必包含命令类型，它确定将要采取的行动或做出的响应。TransactionID 务必遵循以下格式。

长度 = 8	S-Num = 1	S-Type = 1
事务标识符	控制门命令类型	

当包括在 Gate-Report-State 消息中时，事务标识符务必设为 0。

控制门命令类型是一个 2-字节的无符号整数值，它确定控制门控制消息的类型，务必为下列之一：

<预留的>	1-3
Gate-Set	4
Gate-Set-Ack	5
Gate-Set-Err	6
Gate-Info	7
Gate-Info-Ack	8
Gate-Info-Err	9
Gate-Delete	10
Gate-Delete-Ack	11
Gate-Delete-Err	12
<预留的>	13
<预留的>	14
Gate-Report-State	15

6.4.2.2 AMID

AMID，即应用管理器标识符，是一个 4-字节的无符号整数值，它确定负责处理会话的应用管理器。应用管理器务必在其向策略服务器发送的所有消息中包括该对象。策略服务器务必在其向下载送至 CMTS 的所有消息中包括收到的 AMID，以响应它从应用管理器处收到的消息。CMTS 务必在其发送给策略服务器的所有消息中包括收到的 AMID 对象，同样，策略服务器务必包括收到的 AMID，并发送给应用管理器。策略服务器可以在来自 CMTS 的消息中使用 AMID，以解决应用管理器，对应用管理器，可能需要产生一个消息。AMID 对象务必遵循下列格式。

长度 = 8	S-Num = 2	S-Type = 1
AMID		

6.4.2.3 SubscriberID

SubscriberID 是一个 4-字节值，它为订户的该服务请求提供 IPv4 地址（表示为四个串联的八位字节值）。该地址可以是请求服务的订户 CPE 设备的真实 IP 地址（如果该地址是可路由的，且从报头端是可见的），或者，该地址可以是为该订户提供服务的 CM 的 IP 地址（如果在 CM 之后执行 NAT 的话）。该对象用于在 PS 和 CMTS 元素的复杂网络中路由控制门控制消息。它还可用于定义和执行每个订户的策略规则。SubscriberID 对象务必遵循下列格式。

长度 = 8	S-Num = 3	S-Type = 1
SubscriberID（4 个八位字节的 IPv4 地址）		

6.4.2.4 GateID

GateID 是一个 4-字节的无符号整数值，它确定在命令消息中引用的控制门，或者由 CMTS 为响应消息而引用的控制门。CMTS 务必确保 GateID 是唯一的。如果 CMTS 还支持 IPCablecom-T，GateID 绝不能复制当前正在使用的 IPCablecom-T GateID。GateID 对象务必遵循下列格式。

长度 = 8	S-Num = 4	S-Type = 1
GateID		

6.4.2.5 GateSpec

GateSpec 定义与控制门相关的一组特定属性。GateSpec 对象务必遵循下列格式。

长度 = 16		S-Num = 5	S-Type = 1
标志	DSCP/TOS 字段	DSCP/TOS 掩码	SessionClassID
计时器 T1		计时器 T2	
计时器 T3		计时器 T4	

标志是一个 1-字节位字段值，定义如下：

- 第 0 位：方向位，对下行流控制门，务必为 0，对上行流控制门，务必为 1。
- 第 1 位：DSCP/TOS 使能位，为使 DSCP 无法覆写，务必为 0，为使 DSCP 能够覆写，务必为 1。
- 第 2-7 位：预留的位，务必为 0。

SessionClassID 是一个 1-字节的无符号整数值，它确定将用于该控制门的、适当地准许进入控制策略或参数。SessionClassID 是一个为字段，定义如下：

- 第 0-2 位：优先级，为一个 0 到 7 的数值，其中，0 是低优先级，7 是高优先级。
- 第 3 位：抢占，如有必要，设为能够实现分配给较低优先级会话的带宽抢占（如果支持的话）。
- 第 4-7 位：可配置的，缺省值为 0。

优先级字段描述与同一个 PDP 产生的其它会话相比的相对重要性。PEP 可使用该值，一方面执行基于优先级的准入（与抢占位联合使用），一方面保护因被抢占而产生的流（请参见 RFC 2751 [22] “保护优先级”）。CMTS 的优先级粒度可以小于 8 位有效数值。在这种情况下，CMTS 应在整个优先级范围内分发其级别。例如，如果 CMTS 定义优先级为 2 级，那么它应将 0 到 3 级理解为低优先级，将 4 到 7 级理解为高优先级。策略服务器应将该值规格化，或以其它方式对该值进行转换，以确保在整个运营商 CMTS 中存在一个一致的优先级体系，但对任何 AM 请求，应以最初的优先级值予以响应。

PDP 使用抢占位来指示 PEP 采用基于优先级的准许进入控制。抢占支持是可选的；PEP 可忽略该比特。如果 PDP 未请求抢占，或 PEP 未执行抢占，那么准许进入控制将基于“先来先服务”的原则。如果 PEP 决定抢占，那么它务必从优先级低于本次会话优先级的会话中抢占带宽，从优先级最低的会话开始。不用该位来控制哪次会话是可抢占的；相反，通过使用最高优先级，可以请求不可被抢占的会话。如果一个较低优先级的会话因抢占而终止，那么 PEP 务必利用 GateState 对象理由字段 1“由于预留重新分配而导致 CMTS 结束会话”，向 PDP 发送一个控制门报告状态消息，并将控制门转换为“结束”状态。

提供新型服务的应用管理器可以使用可配置的字段来规定新的会话类别。策略服务器可根据该值来支持可配置的策略，并可以在向 CMTS 转发消息之前重写该字段。利用这些位，CMTS 可以执行新型的会话类别标准，但值 0 务必映射至 PDP 合理的缺省值上，它在本标准中是无利害关系的。

DSCP/TOS 字段是一个 1-字节的位字段[6]，由下列可选的结构定义，取决于网络管理策略。该字段，加上 1-字节的 DSCP/TOS 掩码，用于确定在 IPv4 DSCP/TOS 字节中的特殊位。

0	1	2	3	4	5	6	7
不同的业务代码点（DSCP）						未用	未用

0	1	2	3	4	5	6	7
IP 优先级			IP TOS				未用

如果在 GateSpec 标志字段中设定了“使能”位，那么 CMTS 务必标记穿越 CMTS DSCP/TOS 值的各分组。如果清除了“使能”位，那么 CMTS 绝不执行任何标记。

计时器 T1、T2、T3 和 T4 都是 2-字节的无符号整数，以秒为单位进行规定，并务必按控制门转换图表中所示的那样进行使用，如第 6.2 节中所述。T1 的值为零表示务必使用 CMTS 为计时器提供的值。T2 对应 DOCSIS 许可的计时器，T3 对应 DOCSIS 活动的计时器。所有相应的 DOCSIS 需求均适用于这些计时器。特别是，对这些计时器中的任何一个，其值为 0 表示务必使相应的计时器失效。

6.4.2.6 分类符

分类符对象规定与控制门相关的分组匹配规则。如第 6.4.3.1 节和第 6.4.3.2 节中所定义的那样，多个分类符可包含在 Gate-Set 中，以便虑及复杂的分类符规则。分类符对象务必遵循下列格式。

长度 = 24		S-Num = 6	S-Type = 1
协议 ID		DSCP/TOS 字段	DSCP/TOS 掩码
源 IP 地址（4 个八位字节）			
目的 IP 地址（4 个八位字节）			
源端口		目的地端口	
优先级	预留		

源 IP 地址和目的地 IP 地址务必是一对 4-八位字节的 IPv4 地址，或者，对不匹配的情况，其值为 0（也就是说，一个通配符规范将匹配任何分组）。

源端口和目的地端口务必是一对 2-字节的无符号整数值，或者，对不匹配的情况，其值为 0。

协议标识符务必遵循[1]第 B.C.2.1.5.2 节的规定，或者，对不匹配的情况，其值为 0。

DSCP/TOS 字段是一个 1-字节的位字段，它务必遵循下列可选结构：

0	1	2	3	4	5	6	7
不同的业务代码点（DSCP）						未用	使能

0	1	2	3	4	5	6	7
IP 优先级			IP TOS			使能	

DSCP/TO 掩码是一个 1-字节的位字段，提供一个位掩码，用于从附加的 DSCP/TO 字段值中选择相关的位。

如果设定了“使能”位，那么 CMTS 务必使用这些值来构建其 DSx 消息中规定的 IP TOS 范围和掩码字段。如果清除了“使能”位，那么 CMTS 务必从其 DSx 消息发布中省略 IP TOS 范围和掩码值，并从分组分类过程中排除 IP TOS 字节。

优先级是一个允许区分可能重叠的分类符的 1-字节字段。如果不要求使用特定的优先级，那么应使用缺省值 64。对优先级字段的进一步讨论，请参考[1]第 B.C.2.1.3.5 节。

6.4.2.7 通信业务简表

有三种不同的方法来表述通信业务简表。通信业务简表可通过 FlowSpec、DOCSIS 服务类别名称或 DOCSIS 特定的参数来表示。通过在通信业务简表（S-Num = 7）对象中的一个不同的 S-Type 值，可以区分这三种方法。S-Type 为 1，表明对象包含一个在 RSVPFlowSpec 格式中规定的通信业务简表。S-Type 为 2，表明对象包含一个在 DOCSIS 服务类别名称格式中规定的通信业务简表。S-Type 为 3 或 3 以上，表明对象包含一个通过 DOCSIS 特定的参数规定的通信业务简表。

所有的通信业务简表都使用“替代”这一语义，意思是存在于该通信业务简表中的封装替换所有与控制门和相应的服务流相关的现有封装。因此，与某个特定控制门相关的所有通信业务参数，都务必包括在含有通信业务简表的每一个消息中。

所有的通信业务简表共享一个公共字段，称为封装字段。该字段是一个位字段，它告知对象中给出的封装类型（即授权的、预留的和提交的）。在给定的位字段中值为 1，表示在通信业务简表中给出了封装类型。

- Bit 0: 授权的封装。
- Bit 1: 预留的封装。
- Bit 2: 提交的封装。

因此，位模式为 001（或 0x01），表示只存在授权的封装，而位模式为 111（或 0x7），表示存在全部三种封装。只有下列值是合法的：001、011 和 111；封装字段务必设为这三个合法值中的一个。对封装字段值的更多限定可以是当前控制门状态的一个函数。更多的信息请参考第 6.2 节。

对允许多组封装参数的通信业务简表格式，封装参数组的映射遵循以下方法中的一种：

如果在封装字段中表示的所有封装类型共用一组公共的封装参数，那么 PDP 应确保在通信业务简表中确实存在一组封装参数。这使得在整个系统中能够对通信业务简表实现最为有效的传输和处理。

否则，PDP 务必确保封装字段中表示的每个封装类型都确实包括一组封装参数。封装参数组的确切次序如第 6.4.2.7.1 节、第 6.4.2.7.3 节至第 6.4.2.7.8 节中相应的消息图所示。

尽管所有的通信业务简表都以提供接入网络上的 QoS 为终点，但重要的是注意到信令机制之间存在的一些细微差别。如前所述，由 CMTS 执行的、从 FlowSpec (S-Type 1) 到 DOCSIS 的转换，通常比规定 DOCSIS 参数本身效率要低。也就是说，明确规定 DOCSIS 参数 (S-Types 3-7) 并不是万能的解决方案，QoS MIB 只记录有关其 ServiceFlowLogTable 中已命名服务流的 QoS 信息。因此，只有经由 S-Type 2 建立的流，才有可能在该表中记录了 QoS 信息。对某些操作来说，这可能不是一个大问题，但对调试和一般性的操作跟踪而言，运营商和应用管理器供货商应考虑到这种细微之处，并评估由本建议书提供的通信业务简表信令选项。

6.4.2.7.1 流规范

FlowSpec 对象通过一个类似 RSVP 参数化的方案来定义与控制门相关的通信业务简表。第 8 节规定了这些参数到 DOCSIS 参数的映射。FlowSpec 对象务必遵循下列规范：

长度 = 36 或 64 或 92		S-Num = 7	S-Type = 1
封装	服务号码	预留	预留
授权的封装			
令牌桶速率 [r] (IEEE 浮点数)			
令牌桶大小 [b] (IEEE 浮点数)			
峰值数据率 (p) (IEEE 浮点数)			
最小监管单位 [m] (整数)			
最大分组大小 [M] (整数)			
速率 [R] (IEEE 浮点数)			
空隙期限 [S] (整数)			
预留的封装 (可选的)			
令牌桶速率 [r] (IEEE 浮点数)			
令牌桶大小 [b] (IEEE 浮点数)			
峰值数据率 (p) (IEEE 浮点数)			
最小监管单位 [m] (整数)			
最大分组大小 [M] (整数)			
速率 [R] (IEEE 浮点数)			
空隙期限 [S] (整数)			
提交的封装 (可选的)			
令牌桶速率 [r] (IEEE 浮点数)			
令牌桶大小 [b] (IEEE 浮点数)			
峰值数据率 (p) (IEEE 浮点数)			
最小监管单位 [m] (整数)			
最大分组大小 [M] (整数)			
速率 [R] (IEEE 浮点数)			
空隙期限 [S] (整数)			

服务编号字段与[3]中定义的 RSVP FlowSpec 服务编号相对应。如果服务编号设为 5，那么表明是受控负载服务，CMTS 务必只使用 TSpec 值（即令牌桶参数），来执行必要的授权、预留和提交操作。对受控负载服务，CMTS 务必忽略 RSpec R 和 S 字段。

如果服务编号设为 2，那么表明是保证服务，CMTS 务必同时使用 TSpec 和 RSpec 值来执行必要的授权、预留和提交操作。

r、b、p、m、M、R 和 s 在第 9 节进行定义和描述。

6.4.2.7.2 DOCSIS服务类别名称

DOCSIS 服务类别名称对象定义与控制门相关的、预配置的服务类别名称。DOCSIS 服务类别名称对象务必遵循下列规范：

长度 = 12 或 16 或 20 或 24		S-Num = 7	S-Type = 2
封装	预留	预留	预留
服务类别名称			

服务类别名称务必是 2-16 字节的、以空值结尾的 ASCII 字符串（请参考[1]第 B.C.2.2.3.4 节）。该名称务必用空字节加以填充，以便在 4-字节边界上对齐。

注意，不同于 FlowSpec 通信业务简表，它允许不同的参数与各封装相关联，DOCSIS 服务类别名称通信业务简表支持封装字段规定的不同控制门状态，但各个封装由同一相关的 DOCSIS 服务类别名称进行定义。这允许使用 DOCSIS 服务类别名称的、两阶段提交操作，但各个封装务必是相同的。还应注意，改变与控制门相关的 DOCSIS 服务类别名称是可能的，但这种改变适用于与特定控制门相关的所有封装。

6.4.2.7.3 尽力服务

通过上行流 DOCSIS 特定的参数化方案，尽力服务对象定义了与控制门相关的通信业务简表。尽力服务对象务必遵循下列规范：

长度 = 32, 56 或 80		S-Num = 7	S-Type = 3
封装	预留	预留	预留
授权的封装			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
预留的封装（可选的）			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
提交的封装（可选的）			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	

通信业务优先级是一个 1-字节的无符号整数字段，它规定指派给服务流的相应优先级，以便与其它的流进行比较。[1]第 B.C.2.2.5.1 节中全面定义了该字段。如果未要求特定的通信业务优先级值，那么应使用缺省值 0。

请求/传输策略是一个 4-字节的位字段，如[1]第 B.C.2.2.6.3 节中所定义。如果未要求特定的请求/传输策略值，那么应使用缺省值 0。

最大持续通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定速率参数，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.2 节中全面定义了该字段。其值为 0 表明未请求任何显性执行的最大保持速率。如果未要求特定的最大持续通信业务速率，那么应使用缺省值 0。

最大通信业务突发是一个 4-字节的无符号整数字段，它以字节为单位来规定令牌桶大小，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.3 节中全面定义了该字段。如果未要求特定的最大通信业务突发值，那么应使用缺省值 3044 字节。除非已为最大持续通信业务速率参数规定了一个非零值，否则，该参数值没有任何效用。

最小预留通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定为该服务流预留的最小速率。[1]第 B.C.2.2.5.4 节中全面定义了该字段。如果未要求使用特定的最小预留通信业务速率，那么应使用缺省值 0。

假定的最小预留通信业务速率分组大小是一个 2-字节的无符号整数字段，它以字节为单位来规定假定的最小分组大小，对之，将为该流规定最小预留通信业务速率。[1]第 B.C.2.2.5.5 节中全面定义了该字段。如果未要求使用特定的假定最小预留通信业务速率分组大小，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 字节。

6.4.2.7.4 非实时轮询服务

通过 DOCSIS 特定的参数化方案，非实时轮询对象定义了与上行流控制门相关的通信业务简表。非实时轮询对象务必遵循下列规范：

长度 = 36, 64 或 92		S-Num = 7	S-Type = 4
封装	预留	预留	预留
授权的封装			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			
预留的封装（可选的）			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			
提交的封装（可选的）			
通信业务优先级	预留		
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			

通信业务优先级是一个 1-字节的无符号整数字段，它规定指派给服务流的相应优先级，以便与其它流进行比较。[1]第 B.C.2.2.5.1 节全面定义了这一字段。如果未要求特定的通信业务优先级值，那么应使用缺省值 0。

请求/传输策略是一个 4-字节的位字段，如[1]第 B.C.2.2.6.3 中所定义。

注一 对这种服务流调度类型，不存在请求/传输策略的缺省值，同时，在 DOCSIS 中，所有的值（包括 0）都是有意义的。

最大持续通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定速率参数，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.2 节中全面定义了该字段。其值为 0 表明未请求任何显性执行的最大保持速率。如果未要求特定的最大持续通信业务速率，那么应使用缺省值 0。

最大通信业务突发是一个 4-字节的无符号整数字段，它以字节为单位来规定令牌桶大小，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.3 节中全面定义了该字段。如果未要求特定的最大通信业务突发值，那么应使用缺省值 3044 字节。除非已为最大持续通信业务速率参数规定了一个非零值，否则，该参数值没有任何效用。

最小预留通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定为该服务流预留的最小速率。[1]第 B.C.2.2.5.4 节中全面定义了该字段。如果未要求使用特定的最小预留通信业务速率，那么应使用缺省值 0。

假定的最小预留通信业务速率分组大小是一个 2-字节的无符号整数字段，它以字节为单位来规定假定的最小分组大小，对之，将为该流规定最小预留通信业务速率。[1]第 B.C.2.2.5.5 节中全面定义了该字段。如果未要求使用特定的假定最小预留通信业务速率分组大小，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 字节。

标称的轮询间隔是一个 4-字节的无符号整数字段，它规定在上行流信道上有关该服务流的连续单播请求机会之间的标称间隔（以微秒为单位）。[1]第 B.C.2.2.6.4 节中全面定义了该字段。如果未要求特定的标称轮询间隔，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小——而不是 0 字节。

6.4.2.7.5 实时轮询服务

通过 DOCSIS 特定的参数化方案，实时轮询服务对象定义了与上行流控制门相关的通信业务简表。实时轮询对象务必遵循下列规范：

长度 = 36, 64 或 92		S-Num = 7	S-Type = 5
封装	预留	预留	预留
授权的封装			
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			
容许的轮询抖动			
预留的封装（可选的）			
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			
容许的轮询抖动			
提交的封装（可选的）			
请求传输策略			
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
标称的轮询间隔			
容许的轮询抖动			

请求/传输策略是一个 4-字节的位字段，如[1]第 B.C.2.2.6.3 节中所定义。

注 — 对这种服务流调度类型，不存在任何有关请求/传输策略的缺省值，在 DOCSIS 中，所有的值（包括 0）都是有意义的。

最大持续通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定速率参数，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.2 节中全面定义了该字段。其值为 0 表明未请求任何显性执行的最大保持速率。如果未要求特定的最大持续通信业务速率，那么应使用缺省值 0。

最大通信业务突发是一个 4-字节的无符号整数字段，它以字节为单位来规定令牌桶大小，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.3 节中全面定义了该字段。如果未要求特定的最大通信业务突发值，那么应使用缺省值 3044 字节。除非已为最大持续通信业务速率参数规定了一个非零值，否则，该参数值没有任何效用。

最小预留通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定为该服务流预留的最小速率。[1]第 B.C.2.2.5.4 节中全面定义了该字段。如果未要求使用特定的最小预留通信业务速率，那么应使用缺省值 0。

假定的最小预留通信业务速率分组大小是一个 2-字节的无符号整数字段，它以字节为单位来规定假定的最小分组大小，对之，将为该流规定最小预留通信业务速率。[1]第 B.C.2.2.5.5 节中全面定义了该字段。如果未要求使用特定的假定最小预留通信业务速率分组大小，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 字节。

标称的轮询间隔是一个 4-字节的无符号整数字段，它规定在上行流信道上有关该服务流的连续单播请求机会之间的标称间隔（以微秒为单位）。[1]第 B.C.2.2.6.4 节中全面定义了该字段。对这种服务流调度类型，不存在标称的轮询间隔缺省值。

容许的轮询抖动是一个 4-字节的无符号整数字段，它规定单播请求间隔可以自标称的定期调度（以微秒计）延迟的最大时间量。[1]第 B.C.2.2.6.5 节中全面定义了该字段。如果未要求特定的容许轮询抖动，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 微秒。

6.4.2.7.6 主动提供的授权服务

通过 DOCSIS 特定的参数化方案，主动提供的授权服务定义了与上行流控制门相关的通信业务简表。主动提供的授权对象务必遵循下列规范：

长度 = 24, 40 或 56		S-Num = 7	S-Type = 6
封装	预留	预留	预留
授权的封装			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			
预留的封装（可选的）			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			
提交的封装（可选的）			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			

请求/传输策略是一个 4-字节的位字段，如[1]第 B.C.2.2.6.3 节中所定义。

注一 对这种服务流调度类型，不存在任何有关请求/传输策略的缺省值，在 DOCSIS 中，所有的值（包括 0）都是有意义的。

主动提供的授权大小是一个 1-字节的无符号整数字段，它规定授权大小（以字节为单位），如[1]第 B.C.2.2.6.6 节中所定义。不存在任何有关主动提供的授权大小的缺省值。

授权/间隔是一个 1-字节的无符号整数字段，它规定每个标称授权间隔的授权数量，如[1]第 B.C.2.2.6.9 节中所定义。不存在任何有关授权/间隔的缺省值，但建议使用 1 这个值。

标称的轮询间隔是一个 4-字节的无符号整数字段，它规定在有关该服务流的连续数据授权机会之间的标称间隔（以微秒为单位），如[1]第 B.C.2.2.6.7 节中所定义。不存在任何有关标称轮询间隔的缺省值。

容许的容许抖动是一个 4-字节的无符号整数字段，它规定传输机会可以自标称的定期调度（以微秒计）延迟的最大时间量，如[1]第 B.C.2.2.6.8 节中所定义。不存在任何有关容许的授权抖动的缺省值。

6.4.2.7.7 带活动性检测的、主动提供的授权服务

通过 DOCSIS 特定的参数化方案，带活动性检测的、主动提供的授权对象定义了与上行流控制门相关的通信业务简表。带活动性检测的、主动提供的授权对象务必遵循下列规范：

长度 = 32, 56 或 80		S-Num = 7	S-Type = 7
封装	预留	预留	预留
授权的封装			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			
标称的轮询间隔			
容许的轮询抖动			
预留的封装（可选的）			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			
标称的轮询间隔			
容许的轮询抖动			
提交的封装（可选的）			
请求传输策略			
主动提供的授权大小		授权/间隔	预留
标称的授权间隔			
容许的授权抖动			
标称的轮询间隔			
容许的轮询抖动			

请求/传输策略是一个 4-字节的位字段，如[1]第 B.C.2.2.6.3 节中所定义。

注一 对这种服务流调度类型，不存在任何有关请求/传输策略的缺省值，在 DOCSIS 中，所有的值（包括 0）都是有意义的。

主动提供的授权大小是一个 2-字节的无符号整数字段，它规定授权大小（以字节为单位），如[1]第 B.C.2.2.6.6 节所定义。对主动提供的授权大小，不存在任何缺省值。

授权/间隔是一个 1-字节的无符号整数字段，它规定每个标称的授权间隔的授权编号，如[1]第 B.C.2.2.6.9 节所定义。对授权/间隔，不存在任何缺省值，但建议使用 1 这个值。

标称的授权间隔是一个 4-字节的无符号整数字段（以微秒为单位），它规定该服务流的连续数据授权机会之间的标称时间，如[1]第 B.C.2.2.6.7 节所定义。对标称的授权间隔，不存在任何缺省值。

容许的授权抖动是一个 4-字节的无符号整数字段，它规定传输机会可以自标称的定期调度（以微秒计）延迟的最大时间量，如[1]第 B.C.2.2.6.8 节所定义。对容许的授权抖动，不存在任何缺省值。

标称的轮询间隔是一个 4-字节的无符号整数字段，它规定在上行流信道上有关该服务流的连续单播请求机会之间的标称间隔（以微秒为单位）。[1]第 B.C.2.2.6.4 节中全面定义了该字段。对标称的轮询间隔，不存在任何缺省值。

容许的轮询抖动是一个 4-字节的无符号整数字段，它规定单播请求间隔可以自标称的定期调度（以微秒计）延迟的最大时间量。[1]第 B.C.2.2.6.5 节中全面定义了该字段。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 微秒。

6.4.2.7.8 下行流业务

通过下行流业务 DOCSIS 特定的参数化方案，下行流业务定义了与控制门相关的通信业务简表。下行流对象务必遵循下列规范：

长度 = 32, 56 或 80		S-Num = 7	S-Type = 8
封装	预留	预留	预留
授权的封装			
通信业务优先级	预留		
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
最大下行流等待时间			
预留的封装（可选的）			
通信业务优先级	预留		
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
最大下行流等待时间			
提交的封装（可选的）			
通信业务优先级	预留		
最大持续通信业务速率			
最大通信业务突发			
最小预留通信业务速率			
假定的最小预留通信业务速率分组大小		预留	
最大下行流等待时间			

通信业务优先级是一个 1-字节的无符号整数字段，它规定指派给服务流的相应优先级，以便与其它的流进行比较。[1]第 B.C.2.2.5.1 节全面定义了这一字段。如果未要求特定的通信业务优先级值，那么应使用缺省值 0。

最大持续通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定速率参数，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.2 节中全面定义了该字段。其值为 0 表明未请求任何显性执行的最大保持速率。如果未要求特定的最大持续通信业务速率，那么应使用缺省值 0。

最大通信业务突发是一个 4-字节的无符号整数字段，它以字节为单位来规定令牌桶大小，为该服务流限定基于令牌桶的速率。[1]第 B.C.2.2.5.3 节中全面定义了该字段。如果未要求特定的最大通信业务突发值，那么应使用缺省值 3044 字节。除非已为最大持续通信业务速率参数规定了一个非零值，否则，该参数值没有任何效用。

最小预留通信业务速率是一个 4-字节的无符号整数字段，它以比特/秒为单位来规定为该服务流预留的最小速率。[1]第 B.C.2.2.5.4 节中全面定义了该字段。如果未要求使用特定的最小预留通信业务速率，那么应使用缺省值 0。

假定的最小预留通信业务速率分组大小是一个 2-字节的无符号整数字段，它以字节为单位来规定假定的最小分组大小，对之，将为该流规定最小预留通信业务速率。[1]第 B.C.2.2.5.5 节中全面定义了该字段。如果未要求使用特定的假定最小预留通信业务速率分组大小，那么应使用缺省值 0。一旦收到 0 值，CMTS 务必使用其有关该参数的实施方案特定的缺省大小，而不是 0 字节。

最大下行流等待时间是一个 4-字节的无符号整数字段，它规定在 CMTS 的 NSI 上收到分组与在其 RF 接口上转发分组之间的最大等待时间，如[1]第 B.C.2.2.7.1 节所定义。如果未要求使用特定的最大下行流等待时间，那么应使用缺省值 0。一旦收到 0 值，对该服务流，CMTS 绝不能在其 DOCSIS 信令中包括该参数。

6.4.2.8 事件产生信息

事件产生信息对象包含支持事件消息所需的全部信息，ITU-T J.164 建议书对此做出了规定并提出了要求。事件产生信息对象务必遵循下列规范：

长度 = 44	S-Num = 8	S-Type = 1
主记录保持服务器 IP 地址（4 个八位字节）		
主记录保持服务器端口	预留	
副记录保持服务器 IP 地址（4 个八位字节）		
副记录保持服务器端口	预留	
记账相关 ID（24 个字节）		

主记录保持服务器 IP 地址是一个 4-字节字段，它务必包含接收事件记录的主 RKS 的 IPv4 地址。

主记录保持服务器端口字段是一个 2-字节的无符号整数，它务必包含发送事件记录的主 RKS 的端口号。

副记录保持服务器 IP 地址是一个 4-字节字段，它务必包含副 RKS 的 IPv4 地址，如果主 RKS 不可用，那么副 RKS 接收事件记录。

副记录保持服务器端口字段是一个 2-字节的无符号整数，它务必包含发送事件记录的副 RKS 的端口号。

记账相关 ID 是一个 24-字节字段，它务必包含由 AM 或 PS 为所有与本次会话相关的记录指派的标识符。有关该属性的定义和格式，请参见[10]。

6.4.2.9 基于容量的使用限制

基于容量的使用限制对象规定在达到容量门限之前能够经该控制门传输的数据量。该对象在 Gate-Set 和 Gate-Info-Ack 消息中是可选的。它绝不能在其它任何消息中使用。基于容量的使用限制对象务必遵循下列规范：

长度 = 12	S-Num = 9	S-Type = 1
使用限制		

使用限制是一个 8-字节的无符号整数，以千字节为单位进行定义。其值为零表示不存在任何容量限制。对在与该控制门相关的服务流上传输的所有分组，往限制计算的字节数指的是从 DOCSIS MAC 报头 HCS 后到 CRC 结束的字节。

6.4.2.10 基于时间的使用限制

基于时间的使用限制对象规定在达到时间限制门限之前控制门可以保持提交状态的时间量。基于时间的使用限制务必须遵循下列规范：

长度 = 8	S-Num = 10	S-Type = 1
时间限制		

时间限制是一个 4-字节的无符号整数，以秒为单位进行定义。这是控制门可以处于提交状态的时间量限度。在 Gate-Set 消息中，该对象是可选的。如果包括在 Gate-Set 中，那么该对象务必由 CMTS 保存，并在响应任何后续的控制门查询时予以提供。尽管要求应用管理器删除已超出其基于时间的使用限制的、与媒体会话相关的控制门，CMTS 或策略服务器仍可使用该对象来监管应用管理器对基于时间的使用限制的执行。作为故障恢复或其它机制的一部分，应用管理器或策略服务器还可以对该对象进行查询。

值为 0 表明对相关的控制门不存在任何时间限制。

6.4.2.11 不透明的数据

不透明的数据对象包含以下信息，即一个策略服务器或应用管理器可存储于 CMTS 中，对 CMTS 保持不透明。不透明的数据对象在 Gate-Set 消息中是可选的。它绝不能用在任何由 PDP 向 PEP 发送的其它消息中。如果存在该对象，那么 CMTS 务必在本地存储不透明的数据，并将之纳入它为与控制门相关的策略服务器产生的所有消息中。

如果从应用管理器至策略服务器的 Gate-Set 消息中包括不透明数据对象，那么策略服务器务必将该对象转发给 CMTS。不透明数据的长度固定为 8-字节。

长度 = 12	S-Num = 11	S-Type = 1
不透明的数据		

6.4.2.12 控制门时间信息

控制门时间信息对象包含控制门已处于提交的和提交的一回收状态的总的时间量。该计数器务必在控制门从提交的或提交的回收状态转换为预留的状态或授权的状态后，停止计数。如果控制门随后转换回提交的状态，务必在其最后停止处重新启动该计数器，也就是说，在完成提交的或提交的回收状态转换后。控制门时间信息对象务必遵循下列规范：

长度 = 8	S-Num = 12	S-Type = 1
提交的时间		

提交的时间是一个 4-字节的无符号整数，指明控制门已处于提交的或提交的回收状态的秒数。

注 — 这旨在与来自 QoS MIB [17]的 docsQosServiceFlowTimeActive 保持一致。

6.4.2.13 控制门使用信息

控制门使用信息对象包含一个计数器，指明经该控制门传输的千字节数。控制门使用信息对象务必遵循下列规范：

长度 = 12	S-Num = 13	S-Type = 1
八位字节计数		

八位字节计数是一个 4-字节的无符号整数，代表已穿越与控制门相关的业务流字节数(从 DOCSIS MAC 报头 HCS 开始计数，至 CRC 结束)，以 1024-字节为单位进行计数。

6.4.2.14 IPCablecom错误

IPCablecom 错误对象包含有关已发生错误类型的信息。错误在响应控制门控制命令时产生，并包含在 Gate-Set-Err、Gate-Info-Err 和 Gate-Delete-Err 消息中。IPCablecom 对象错误务必遵循下列规范：

长度 = 8	S-Num = 14	S-Type = 1
错误代码	错误子代码	

错误代码是一个 2 字节的无符号整数，代表一个特定的错误，它务必为以下代码中的一个：

- 1 = 资源不足；
- 2 = GateID 未知；
- 6 = 丢失要求的对象；
- 7 = 无效的对象；
- 8 = 超出基于容量的使用限制；
- 9 = 超出基于时间的使用限制；
- 10 = 超出会话类别限制；
- 11 = 未定义的服务类别名称；

- 12 = 不兼容的封装;
- 13 = 无效的订户 ID;
- 14 = 未授权的 AMID;
- 15 = 不支持的分类符号码;
- 127 = 其它, 未指明的错误。

错误子代码是一个 2-字节的无符号整数字段, 用于提供有关错误的进一步信息。在错误代码 6 和 7 中, 该 16-比特字段务必包含丢失或出错对象的 S-Num 和 S-Type 这两个 8-比特值。在错误子代码中, S-Num 和 S-Type 值的次序务必与最初消息中的相同。如果丢失对象的 S-Type 存在多个有效的选择, 那么错误子代码的这一部分务必设为 0。在错误代码 15 中, 错误子代码字段务必包含每个控制门支持的分类符数。

错误代码 8、9 和 10 是因不能满足策略服务器授权要求的策略请求而产生的。当应用管理器向策略服务器发出一个带基于容量的限制或基于时间的限制的 Gate-Set 消息时, 策略服务器可依据安装在策略服务器上的策略规则拒绝请求。例如, 这种策略规则可以声明, 如果容量限制请求超出最大值, 那么策略服务器务必拒绝请求。

6.4.2.15 控制门状态

控制门状态对象中的信息反映控制门的当前状态。CMTS 务必在其发往策略服务器的任何主动提供的消息中包括控制门状态对象。策略服务器可使用该信息向应用管理器报告状态, 或者用于执行可能要求控制门状态信息的复杂规则。

典型地, 策略服务器知道状态转换, 原因是, 它通常为这些至 CMTS 的转换提供激励, 但在某些情况下, 无须策略服务器的介入, 控制门可以在 CMTS 本地完成转换。在这些情况下, CMTS 务必通过主动提供的 Gate-Report-State 消息, 向策略服务器报告状态转换情况。当发出 Gate-Report-State 消息时, PEP 务必确保已清除 COPS 消息报头中的请求标志, 并将报头中的报告类型设为结算。控制门状态对象务必遵循下列规范:

长度 = 8	S-Num = 15	S-Type = 1
状态	理由	

状态是一个 2 字节的无符号整数字段, 它务必指明以下状态中的一个:

- 1 = 空闲/关闭的;
- 2 = 授权的;
- 3 = 预留的;
- 4 = 提交的;
- 5 = 提交—回收。

理由是一个 2-字节的无符号整数字段, 它务必指明有关该更新的下列理由之一:

- 1 = 由于预留重新分配而由 CMTS 发起的关闭;
- 2 = 由于缺少 DOCSIS MAC 层响应而由 CMTS 发起的关闭;
- 3 = 由于计时器 T1 到期而由 CMTS 发起的关闭;

- 4 = 由于计时器 T2 到期而由 CMTS 发起的关闭；
- 5 = 由于服务流非活动而导致的非活动计时器到期（计时器 T3 到期）；
- 6 = 由于缺少预留保持而由 CMTS 发起的关闭；
- 7 = 控制门状态未改变，但达到容量限制；
- 8 = 由于计时器 T4 到期而由 CMTS 发起的关闭；
- 9 = 控制门状态未改变，但计时器 T2 到期，导致预留减少；
- 65535 = 其它。

6.4.2.16 版本信息

版本信息对象用于使多媒体应用能够实现与其它设备的互动，以便支持不同协议版本的产品之间实现互操作。大版本号和小版本号都是 2-字节的无符号整数。如第 6.5.1 节中所规定的那样，PEP 和 PDP 都务必包括该对象。

长度 = 8	S-Num = 16	S-Type = 1
大版本号	小版本号	

6.4.3 控制门控制消息

控制门控制消息有两个独立的简表：一个针对应用管理器与策略服务器之间交换的消息，另一个针对策略服务器与 CMTS 之间的消息。尽管非常相似，但这两个简表之间仍存在某些小的差别。

以下声明描述了包括 COPS 和 PCMM 的 PCMM 消息格式。这些声明规定了消息的内容，但并不意味着各个消息内对象的特定次序。特别是，务必认为 PCMM 对象的任何次序都是有效的，并被接受（并可以产生），COPS 对象的次序务必如 RFC 2748 中所规定的那样。注意，由于 PCMM 对象只存在于 COPS 对象中，因此这两组对象之间的差别是明显的。该包含模型也确保了与 COPS 和 PCMM 对象的相对次序之间不存在任何问题。

6.4.3.1 应用管理器与策略服务器接口简表

定义了执行应用管理器与策略服务器之间控制门控制的消息，这些消息务必按如下方式进行格式化。

注意，从应用管理器发往策略服务器的消息，务必格式化为 COPS 决定消息，从策略服务器发往应用管理器的消息务必格式化为 COPS 报告状态消息。

```

<客户机打开> = <COPS 公共报头> <COPS PEPID> <ClientSI 信息>
<ClientSI 信息> = <COPS 客户机 SI 报头> <MM 版本信息>
<控制门控制命令> = <COPS 公共报头> <客户机句柄> <正文>
                    <决定标志> <ClientSI 数据>
<ClientSI 数据> = <Gate-Set> | <Gate-Info> | <Gate-Delete>
<控制门控制响应> = <COPS 公共报头> <客户机句柄> <报告类型>
                    <ClientSI 对象>
<ClientSI 对象> = <Gate-Set-Ack> | <Gate-Set-Err> | <Gate-Info-Ack> | <Gate-Info-Err>
                  | <Gate-Delete-Ack> | <Gate-Delete-Err> | <Gate-State-Report>
<Gate-Set> = <决定报头> <TransactionID> <AMID> <SubscriberID> [<GateID>]
```

<GateSpec> <通信业务简表> <分类符> [<分类符>
 [<事件产生信息>
 [<基于容量的使用限制>] [<基于时间的使用限制>] [<不透明的数据>]
 <Gate-Set-Ack> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<不透明的数据>]
 <Gate-Set-Err> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID>
 <IPCCablecom 错误> [<不透明的数据>]
 <Gate-Info> = <决定报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 <Gate-Info-Ack> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<事件产生信息>] <GateSpec> <GateState> <分类符>
 <分类符> <通信业务简表> <控制门时间信息>
 <控制门使用信息> [<基于容量的使用限制>]
 [<基于时间的使用限制>] [<不透明的数据>]
 <Gate-Info-Err> = <ClientSI 报头> <TransactionID> <AMID> <GateID> <IPCCablecomErr>
 [<不透明的数据>]
 <Gate-Delete> = <决定报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 <Gate-Delete-Ack> = <ClientSI 报头> <TransactionID> <AMID> <GateID> [<不透明的数据>]
 <Gate-Delete-Err> = <ClientSI 报头> <TransactionID> <AMID> <GateID>
 <IPCCablecom 错误> [<不透明的数据>]
 <Gate-Report-State> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID> <GateState>
 <控制门时间信息> <控制门使用信息> [<不透明的数据>]

6.4.3.2 策略服务器和CMTS接口简表

定义了执行策略服务器与 CMTS 之间控制门控制的消息，这些消息务必按如下方式进行格式化。

注意，从策略服务器发送到 CMTS 的消息务必作为 COPS 决定消息进行格式化，从 CMTS 发送到策略服务器的消息务必作为 COPS 报告状态消息进行格式化。

<客户机打开> = <COPS 公共报头> <COPS PEPID> <ClientSI 信息>
 <ClientSI 信息> = <COPS 客户机 SI 报头> <MM 版本信息>
 <控制门控制命令> = <COPS 公共报头> <客户机句柄> <正文>
 <决定标志> <ClientSI 数据>
 <ClientSI 数据> = <Gate-Set> | <Gate-Info> | <Gate-Delete>
 <控制门控制响应> = <COPS 公共报头> <客户机句柄> <报告类型>
 <ClientSI 对象>
 <ClientSI 对象> = <Gate-Set-Ack> | <Gate-Set-Err> | <Gate-Info-Ack> | <Gate-Info-Err>
 | <Gate-Delete-Ack> | <Gate-Delete-Err> | <Gate-State-Report>
 <Gate-Set> = <决定报头> <TransactionID> <AMID> <SubscriberID> [<GateID>]
 <GateSpec> <通信业务简表> <分类符> [<分类符>] [<事件产生信息>]

[<基于容量的使用限制>] [<基于时间的使用限制>] [<不透明的数据>]
 [<基于容量的使用限制>] [<基于时间的使用限制>] [<不透明的数据>]
 <Gate-Set-Ack> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<不透明的数据>]
 <Gate-Set-Err> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID>
 <IPCablecom 错误> [<不透明的数据>]
 <Gate-Info> = <决定报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 <Gate-Info-Ack> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<事件产生信息>] <GateSpec> <分类符> <分类符>
 <通信业务简表> <控制门时间信息> <控制门使用信息> [<基于容量的使用限制>]
 [<基于时间的使用限制>] [<不透明的数据>] <控制门状态>
 <Gate-Info-Err> = <ClientSI 报头> <TransactionID> <AMID> <GateID> <IPCablecomErr>
 [<不透明的数据>]
 <Gate-Delete> = <决定报头> <TransactionID> <AMID> <SubscriberID> <GateID>
 <Gate-Delete-Ack> = <ClientSI 报头> <TransactionID> <AMID> <GateID> [<不透明的数据>]
 <Gate-Delete-Err> = <ClientSI 报头> <TransactionID> <AMID> <GateID>
 <IPCablecom 错误> [<不透明的数据>]
 <Gate-Report-State> = <ClientSI 报头> <TransactionID> <AMID> <SubscriberID> <GateID> <GateState>
 <控制门时间信息> <控制门使用信息> [<不透明的数据>]

基本的控制门控制命令消息有三种：Gate-Set、Gate-Info 和 Gate-Delete。这些消息嵌入在 COPS 决定消息内的客户机特定决定数据中。对控制门控制命令消息，COPS 决定消息中的正文对象（C-Num = 2，C-Type = 1）务必具备设为 0x08（配置请求）的 R-Type（请求类型标志）值以及设为 0 的 M-Type。在强制性决定标志对象中（C-Num = 6，C-Type = 1）的命令代码字段务必设为 1（安装配置）。其它值务必引起 CMTS 产生一个表明失败的报告状态消息。标志子字段可以设为任何值，且务必被 PEP 忽略。在 TransactionID 中的控制门命令类型字段用于区分正在发送的命令类型。

控制门控制响应消息有七种：Gate-Set-Ack、Gate-Set-Err、Gate-Info-Ack、Gate-Info-Err、Gate-Delete-Ack、Gate-Delete-Err 和 Gate-Report-State。前六个控制门控制响应消息是对控制门控制命令消息的请求响应。第七个响应消息，即 Gate-Report-State，是 CMTS 向 PS 主动提供的响应，告知状态的变化情况。

这些消息嵌入在 COPS 报告状态消息中的客户机特定信息对象内。取决于控制门控制命令的结果，有关控制门控制响应的 COPS 报告状态消息中包括的 Report-Type 对象（C-Num = 12，C-Type = 1）务必具有设为 1（成功）或 2（失败）的 Report-Type 字段。响应控制门控制命令的报告状态消息务必具有在 COPS 报头中设定的请求消息标志位。在 TransactionID 中的控制门命令类型字段用于区分正在发送的响应类型。

当控制门上发生了不是因决定消息而引起的状态转换，或者当已达到某些策略限制时，CMTS 产生一个 Gate-Report-State 消息。对该 Gate-Report-State 消息，Report-Type 字段务必设为 3（结算），并务必清除在公共报头中的请求标志字段。

如果在控制门控制消息中收到的一个对象包含未被认可的 S-Num 或 S-Type, 那么务必忽略该对象。假如在抛弃该参数后, 所有要求的对象仍存在于消息中, 那么在控制门控制消息中存在此类对象绝不能视为是一个错误。

6.5 控制门控制协议操作

6.5.1 初始化序列

当 PEP (策略服务器或 CMTS) 引导时, 它务必监听在 IANA 指派的 TCP 端口号 3918 上的进入 COPS 连接。任何需要与 PEP 接触的应用管理器或策略服务器 (PDP) 务必在该端口上建立一个与 PEP 的 TCP 连接。期望多个应用管理器将与多个策略服务器建立 COPS 连接, 多个策略服务器将与多个 CMTS 建立 COPS 连接。当 PEP 与 PDP 之间的 TCP 连接已建立时, PEP 务必以 Client-Open 消息的形式, 向 PDP 发送关于其自身的信息。该消息务必包括多媒体版本信息对象, 它将告知 PDP 有关 PEP 上使用的、当前支持的多媒体协议版本。

一旦成功接收 Client-Open 消息, 如果支持版本信息对象中规定的协议版本, 那么 PDP 务必发送一个 Client-Accept 消息。该消息务必包括 Keep-Alive-Timer 对象, 它告知 PEP 有关 Keep-Alive 消息间的最大间隔。

如果不支持 PEP 提供的协议版本, 那么 PDP 务必发送一个带 COPS 错误对象的 Client-Close 消息, 指明错误代码 4 (不能处理)。在发送 Client-Close 消息后, PDP 务必保持 TCP 连接以及与 PEP 的安全性关联, 以便 PEP 可以重新尝试 COPS 初始化, 而无须重新建立 TCP 连接和安全性关联。在从 PDP 处收到一个包括 COPS 错误对象 (规定错误代码为 4) 的 Client-Close 消息后, 通过发送另一个带版本信息对象中另一个版本号 Client-Open 消息, PEP 可以重新尝试初始化 COPS 连接。该过程可以继续进行, 直至从 PDP 收到一个 Client-Accept 消息, 或者已用完所有可用的协议版本。一旦 PEP 已经尝试其支持的所有协议版本, PEP 务必发送一个带大版本号 0 和小版本号 0 的 Client-Open 消息, 以示它未能成功完成版本协商过程。然后, PDP 务必向 PEP 发送一个 Client-Close 消息, 以确认协议协商已失败。收到 Client-Close 消息后, PEP 务必关闭 TCP 连接。此时, PDP 可定期尝试重新建立连接。

遵循该规范的设备务必使用 1.0 版本, 即带大版本号 1 和小版本号 0 的版本信息对象。

一旦成功收到 Client-Accept 消息后, PEP 务必发送一个请求消息, 包括 Client-Handle 和 C 正文对象。正文对象 (C-Num = 2, C-Type = 1) 务必具有设为 0x08 (配置请求) 的 R-Type (请求类型标志) 和设为 0 的 M-Type。Client-Handle 对象包含一个务必由 PEP 选择的值。对该值, 唯一的要求是, PEP 绝不能为单个 TCP 连接上的两个不同请求使用同一个值。这完成了初始化序列, 该过程用图表描述如下。

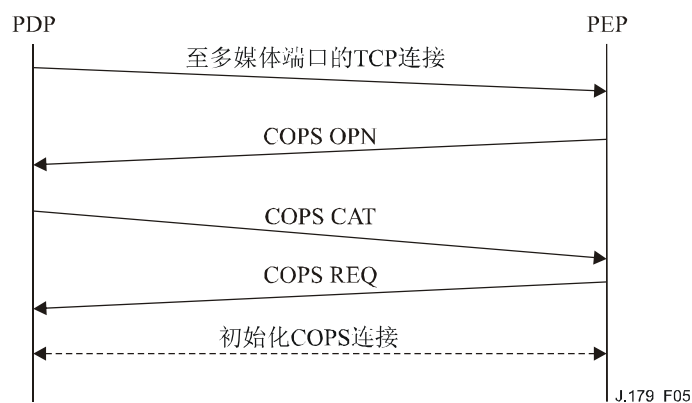


图 5/J.179—COPS连接建立

PEP 务必定期向 PDP 发送一个 COPS 保持活动 (KA) 消息。一旦收到 COPS KA 消息, PDP 务必向 PEP 回应一个 COPS KA 消息。下图说明了这一事务处理过程, [7]中对该过程进行了详细描述。至少, PEP 务必按 Keep-Alive-Timer 对象(在 Client-Accept 消息中返回)中规定的频度发送一个 Keep-Alive 消息。Keep-Alive 消息务必与设为 0 并清除了请求标志的 Client-Type 一同发送。

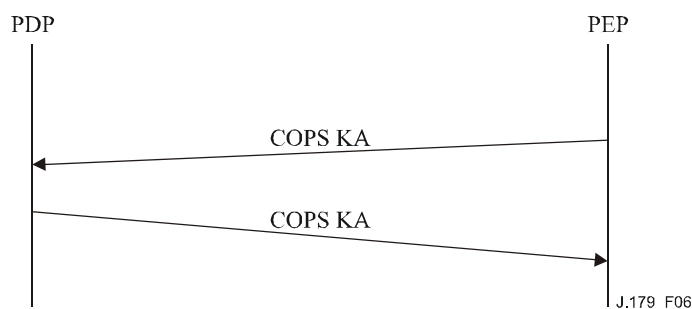


图 6/J.179—COPS保持活动交换

6.5.2 操作序列

PDP 与 PEP 之间的协议用于资源控制和资源分配策略之目的。应用管理器请求来自策略服务器的策略决定, 策略服务器授权这些请求, 并在 CMTS 上安装它们, 以便通过使用控制门来执行它们。

可由应用管理器和策略服务器发出的消息, 包括 Gate-Set、Gate-Info 和 Gate-Delete。CMTS 可以发出 Gate-Report-State 消息。在以下章节中描述有关这些消息的程序。所有从 PDP 发往 PEP 的消息都务必利用 COPS 决定消息的决定对象中的客户机特定对象来发送。来自 PEP 的请求消息务必作为 ClientSI 对象中带客户机特定对象的 Report-State 消息来发送, 并务必设定请求的标志。来自 CMTS 的 Gate-Report-State 消息务必作为主动提供的 Report-State 消息, 经由 ClientSI 对象中的客户机特定对象进行发送。

决定消息和 Report-State 消息务必包含与最初请求提供的 Client-Handle 相同的 Client-Handle, 当 COPS 连接开始建立时, 由 CMTS 发送这些最初请求。

Gate-Set 初始化和根改控制门的所有策略和通信业务参数，并建立记账信息。Gate-Set 还可用于控制和更新 CMTS 上的控制门状态。

Gate-Info 是一种机制，通过它，策略服务器可以查询现有控制门的所有当前状态和参数设置情况。

Gate-Delete 允许策略服务器删除特定控制门以及任何相关的服务流。

Gate-Report-State 允许 CMTS 告知策略服务器，控制门已转换为新的状态。当状态转换出现不同步时（即不是作为对 Gate-Set 消息的响应），务必产生 Gate-Report-State 消息。当状态转换同步时，绝不能产生 Gate-Report-State 消息。

PEP 务必定期向 PDP 发送一个保持活动（KA）消息，以利于对 TCP 连接故障的检测。PDP 务必随时了解何时收到 KA。如果在[7]规定的时间间隔内，PEP 未收到来自 PDP 的 KA 消息，或者 PDP 未收到来自 TCP 连接的错误指示，那么 PDP 务必拆卸 TCP 连接，并尝试重新建立 TCP 连接。

下列规则用于通过 IPCablecom 多媒体框架路由控制门控制消息。特别地，为在整个复杂的分层网络中前向（即从 AM 经 PS 到 CMTS）和后向（即从 CMTS 经 PS 到 AM）传输控制门控制消息做出了规定，在这种复杂的分层网络中，各元素的多个实例都与相邻层中的元素发生相互作用。

如第 6.4.3.1 节所述，由 AM 发出的各控制门控制请求（即 Gate-Set、Gate-Info 和 Gate-Delete）务必同时包括 AMID 和 SubscriberID 对象。

一旦收到来自 AM 的控制门控制消息，PS 将运用任何提供的策略规则，确定准许或拒绝请求。如果请求得以成功认可，那么 PS 务必依据包括在消息中的 SubscriberID 将消息路由至合适的 CMTS。这种 SubscriberID 至 CMTS 的映射，可依据查询 OSS 基础设施来动态地执行，或者可以反映预先提供的路由信息，这些信息与各 CMTS 关联的 IP 子网范围有关。

如果 PS 拒绝了控制门控制请求，那么务必通过收到最初请求的连接，向发出请求的 AM 返回一个错误响应。如果在收到请求与发出响应的时间间隔中，检测到该连接上有故障，那么 PS 务必抛弃响应。

一旦收到一个来自 PS 的控制门控制消息，CMTS 将执行请求的操作。如果该操作获得成功，涉及一个 Gate-Set 操作或者一个 Gate-Info 操作，那么 CMTS 务必记录包括在消息中的 AMID 和 SubscriberID，并保持与参考控制门的关联。务必使用该信息来确保只有最初建立控制门的 AM 获准查询或更改该控制门。任何引用控制门但包含一个不同于与控制门相关的 AMID 的控制门控制消息，务必由 CMTS 使用“未授权的 AMID”错误加以拒绝。最后，务必向 PS 元素提交 Gate-Report-State 消息，该 PS 元素通过其最初建立控制门的 IP 地址加以标识。如果与该 PS 的连接不可用，那么 CMTS 务必禁止发出 Gate-Report-State 消息。

当 PS 从 CMTS 处收到一个 Gate-Report-State 消息时，PS 务必将该消息转发给与包括在消息中的 AMID 相关的 AM。为了保持非相邻层之间一定程度的抽象，并隐藏来自 AM 层的、与网络拓扑相关的信息，PS 绝不能包括以下信息，即直接用于确定至 AM 层的特殊 CMTS。

6.5.3 验证资源封装程序

对提供增强型服务质量之目的而言，数据服务流特征集是重要的，称为封装。IPCablecom 多媒体控制门包含至多三种封装：一个表示授权的资源，一个表示预留的资源，一个表示对应控制门的、服务流的提交的资源。在任何一个时间点，提交的封装务必安装在预留的封装内，预留的封装务必安装在授权的封装内。

当 CMTS 收到一个 Gate-Set 消息时，它务必验证控制门提交的、预留的和授权的封装之间的关系。如果封装关系是无效的，那么 CMTS 务必以一个带“不兼容封装”IPCablecom 错误代码的 Gate-Set-Err 消息做出响应。

无论何时当请求的预留封装发生变化（包括增加），CMTS 还务必执行准许进入控制。准许进入控制是为控制门对应的流分配资源的过程。如果无法分配资源，那么 CMTS 务必以一个带“无足够资源”IPCablecom 错误代码的 Gate-Set-Err 消息做出响应。

6.5.3.1 流规范

在表 2 中，第二列指明了应用于比较 A 封装参数与 B 封装中对应参数的操作。换言之，如果封装 A 的各个参数符合表中所规定的准则，那么封装 A 适合封装 B。

表 2/J.179—封装比较规则

参 数	A {操作符} B
令牌桶速率 [r]	$\leq$
令牌桶大小 [b]	$\leq$
峰值数据率 [p]	$\leq$
最小监管单位 [m]	$\geq$
最大分组大小 [M]	$\leq$
速率 [R]	$\leq$
空隙期限 [S]	$\geq$

6.5.3.2 DOCSIS服务类别名称

对服务类别名称形式的通信业务简表，服务类别名称字符串务必与 CMTS 上预先存在的服务类别名称准确匹配。无须任何封装比较，因为全部三种封装务必共用相同的封装参数。

6.5.3.3 DOCSIS业务流参数

6.5.3.3.1 上行流编码

在表 3 中，第二列指明了应用于比较 A 封装参数与 B 封装中对应参数的操作。换言之，如果封装 A 的各个参数符合表中所规定的准则，那么封装 A 适合封装 B。

表 3/J.179—上行流封装比较

参 数	A {操作符} B
通信业务优先级 (BE & NRTPS)	$\leq$
请求传输策略 (所有的)	$=$
最大持续通信业务速率 (BE, NRTPS, RTPS)	$\leq$
最大通信业务突发 (BE, NRTPS, RTPS)	$\leq$
最小预留通信业务速率 (BE, NRTPS, RTPS)	$\leq$
假定的最小预留通信业务速率分组大小 (BE, NRTPS, RTPS)	$\geq$
标称的轮询间隔 (NRTPS, RTPS, UGS/AD)	见以下有关间隔的描述
容许的轮询抖动 (RTPS, UGS/AD)	$\geq$
主动提供的授权大小 (UGS & UGS/AD)	$\leq$
授权/间隔 (UGS & UGS/AD)	$\leq$
标称的授权间隔 (UGS & UGS/AD)	见以下有关间隔的描述
容许的授权抖动 (UGS & UGS/AD)	$\geq$

间隔 — 如果 A 中的参数是 B 中相同参数的整数倍, 那么 A 是 B 的一个子集。

6.5.3.3.2 下行流编码

在表 4 中, 第二列表示应用于比较 A 封装参数与 B 封装对应参数的操作。换言之, 如果封装 A 的各个参数都符合表中规定的准则, 那么封装 A 适于封装 B。

表 4/J.179—下行流封装比较

参 数	A {操作符} B
通信业务优先级	$\leq$
最大持续通信业务速率	$\leq$
最大通信业务突发	$\leq$
最小预留通信业务速率	$\leq$
假定的最小预留通信业务速率分组大小	$\geq$
最大下行流等待时间	$\geq$

6.5.4 通过控制门进行资源授权的程序

Gate-Set 消息可由 PDP 向 PEP 发送, 以初始化或修改控制门的操作参数。图 7 提供了有关 Gate-Set 信令的例子。

注 — 作为一个例子, 可使用“开始会话”消息向客户机指出资源已获授权。

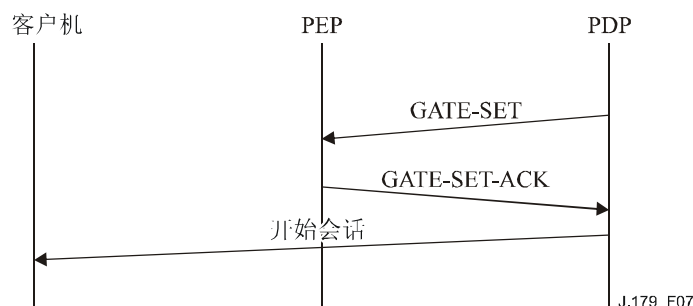


图 7/J.179—控制门设立的样本信令

如果 GateID 对象出现于 Gate-Set 消息中，那么请求将修改现有的控制门。如果 Gate-Set 消息中缺少 GateID 对象，那么它是一个分配新控制门的请求。Gate-Set 消息务必准确地包含一个 GateSpec 对象，用于描述上行流或下行流控制门。

Gate-Set 消息还包含 SubscriberID。CMTS 务必使用该 IP 地址（即 SubscriberID）来确定服务的 CM，并务必使用 CM 的 MAC 地址，用于后续的 MAC 层消息发布。

PEP 务必以 Gate-Set-Ack 消息对 Gate-Set 消息做出响应，表示成功，或者以 Gate-Set-Err 消息对 Gate-Set 消息做出响应，表示失败。响应中的 TransactionID 务必与请求的 TransactionID 相匹配。在分配或授权控制门过程中出现的错误务必通过 Gate-Set-Err 响应来报告。请参考第 6.4.2.14 节。

在情形 1 中，策略服务器可通过在 Gate-Set 消息中发送的通信业务简表，来规定授权的、预留的和提交的封装。它同时可指示 CMTS 授权、预留和提交资源。

一旦收到 Gate-Set 消息，CMTS 务必首先满足第 6.5.3 节中所规定的要求，然后执行请求的动作。一旦成功执行在 Gate-Set 中请求的动作（如创建一个 DOCSIS 服务流），CMTS 务必以一个 Gate-Set-Ack 消息做出响应。在其完成足够的步骤之前，CMTS 绝不能以一个 Gate-Set-Ack 消息来响应，以确保任何用于准许或提交控制门的后续请求不会因缺少资源而失败。

不仅依据请求的 QoS 和控制门授权的流规范，而且依据 GateSpec 中规定的 SessionClassID，CMTS 可执行复杂的授权。CMTS 可能已经规定了策略，这些策略定义了专门分配给特殊会话类别以及“借用”与“抢占”规则（申请使用资源）的资源量。这些策略类型的细节以及有关 CMTS 的规则，超出了本建议书的讨论范围。

一旦从 CMTS 收到一个 Gate-Set-Ack 或 Gate-Set-Err 消息，策略服务器务必将此消息转发给对应 Gate-Set-Ack 中 AMID 的应用管理器。在从 CMTS 收到一个 Gate-Set-Ack 消息之前，策略服务器绝不向应用管理器传送 Gate-Set-Ack 消息。不过，如果应用管理器请求并未通过策略服务器策略检查的服务，那么策略服务器绝不向 CMTS 发送 Gate-Set 消息，且务必向应用管理器发送带有适当错误集的 Gate-Set-Err 消息。

6.5.5 查询控制门程序

当策略服务器或应用管理器希望查询控制门当前参数设置时，它向 CMTS 发送一个 Gate-Info 消息。CMTS 务必对该消息做出响应，以 Gate-Info-Ack 响应，表示成功，或者以 Gate-Info-Err 响应，表示失败。Gate-Info-Ack 务必包含 Gate-Info 消息中 GateID 相关的控制门的信息。如果被查询的控制门目前带有基于容量的与/或基于时间的使用限制，那么 CMTS 务必在 Gate-Info-Ack 消息中包括这些对象。PS 或 AM 可使用该信息来恢复来自 CMTS 的状态信息，用于监管、错误恢复或其它目的。响应中的 TransactionID 务必与请求中的 TransactionID 相匹配。

Gate-Info-Err 响应务必报告在查询控制门中发生的错误。Gate-Info-Err 消息中的错误对象务必包含下列错误代码之一：

2 = 未知的 GateID；

127 = 其它，未详细说明了的错误。

6.5.6 修改控制门程序

为修改与现有控制门相关的通信业务简表，应用管理器可发送一个 Gate-Set 消息和新的通信业务简表，Gate-Set 消息带有待修改之控制门的 GateID。如果 Gate-Set 未能通过策略服务器的检查，那么策略服务器务必向应用管理器发送一个 Gate-Set-Err 消息，并绝不能向 CMTS 发送一个 Gate-Set 消息。不过，如果 Gate-Set 通过了策略服务器的检查，那么策略服务器务必向 CMTS 发送 Gate-Set 消息。策略服务器 Gate-Set 中的 TransactionID 务必与应用管理器 Gate-Set 中的 TransactionID 相匹配。

一旦收到 Gate-Set，CMTS 务必首先满足第 6.5.3 节中规定的要求，然后执行请求的动作。随着新控制门的建立，一旦成功执行在 Gate-Set 中请求的动作（如更改一个 DOCSIS 服务流），CMTS 务必以一个 Gate-Set-Ack 消息做出响应。在其完成足够的步骤之前，CMTS 绝不能以一个 Gate-Set-Ack 消息来响应，以确保任何用于准许或提交控制门的后续请求不会因缺少资源而失败。

一旦从 CMTS 处收到一个 Gate-Set-Ack 或 Gate-Set-Err 消息，策略服务器务必将响应转发给应用管理器。

为修改与现有控制门相关的使用限制，应用管理器可发送一个 Gate-Set 消息，消息带有将要修改的控制门的 GateID。如果 Gate-Set 中的通信业务简表不同于当前与控制门相关的通信业务简表，那么之前的规则依然适用。另一种情况是，如果存在有关流的、基于时间的使用限制或基于容量的使用限制，那么务必用新的参数替换与这个/这些参数相关的现有限制，并重新设置任何现有的计数器或计时器。不过，Gate-Set 消息中不存在这些参数，表示即使要修改控制门的通信业务简表，控制门现有的、基于时间的限制或基于容量的限制依然适用。如果这些参数未出现在 Gate-Set 消息中，那么务必维持现有的限制，其相关的计数器/计时器务必从当前值继续进行，而无需重新设置。

6.5.7 支持使用限制程序

在执行使用限制方面，应用管理器、策略服务器和 CMTS 都起着作用。在基于时间的限制和基于容量的限制之间，存在一些微小的差别，因此，分别对其进行描述。

6.5.7.1 达到基于容量的使用限制时的程序

由于在分组路径中，CMTS 是唯一被信任的 IPCablecom 多媒体设备，因此它也是唯一能够准确跟踪单个控制门使用情况的设备。因而，CMTS 务必跟踪所有控制门的使用情况，不管它们是否拥有相关的、基于容量的使用限制。CMTS 务必在所有 Gate-Info-Ack 消息和所有 Gate-Report-State 消息中，报告经由控制门传输的数据量。

如果当穿越控制门的数据量等于基于容量的使用限制时，控制门拥有相关的、基于容量的使用限制，那么 CMTS 务必发送一个 Gate-Report-State 消息，其请求位设为 0。Gate-State-Report 消息务必包括一个控制门状态对象，其理由设为 7（表示控制门状态未发生变化，但达到了容量限制）。一旦收到 Gate-Report-State 消息，PDP 的行为将取决于其作用；策略服务器务必向应用管理器转发 Gate-Report-State 消息，或者自己处理报告。策略服务器应只在以下情况才处理报告，即如果通过更改最初的控制门设置，它导致产生了报告。换言之，策略服务器的动作对应用管理器而言应是透明的。应用管理器务必对收到的报告进行处理。PDP 处理理由设为 7 的 Gate-Report-State 消息，通过执行下列动作之一来实现：

- 发送一个带有新的、基于容量的使用限制的 Gate-Set 消息，CMTS 务必用之来“重新开始”对该控制门的结算；
- 发送一个带有设为 0 的、基于容量的使用限制的 Gate-Set 消息，以禁止此特性，并允许 CMTS 继续为会话提供服务；
- 通过发出一个 Gate-Delete 命令，来关闭控制门。

6.5.7.2 达到基于时间的使用限制时的程序

尽管期望的设计目标是使基于容量的和基于时间的使用限制程序尽可能地保持相似，但支持 CMTS 执行基于时间的使用限制所要求的 CMTS 中断次数，使该方法变得不可能。因此，应用管理器务必执行该控制门的基于时间的使用限制。一旦收到带基于时间的使用限制的控制门 Gate-Set-Ack 消息，AM 务必启动一个应用计时器。当该应用计时器等于基于时间的使用限制时，应用管理器务必通过执行以下动作之一，来做出响应：

- 发送一个带有新的、基于时间的使用限制的 Gate-Set 消息，并重新设置其应用计时器；
- 发送一个带有设为 0 的、基于时间的使用限制的 Gate-Set，以禁止此特性；
- 通过发出一个 Gate-Delete 命令，来关闭控制门。

注一 在某些方面，应用管理器执行使用限制更有意义，因为基于时间的使用限制和基于容量的使用限制反映了正在提供的服务，并且是服务控制域的责任。基于容量的使用限制程序确实是不寻常的，但 CMTS 是唯一能够准备执行这一限制的设备。

6.5.7.3 资源和错误恢复

虽然当达到控制门使用限制时，要求应用管理器执行若干动作中的其中一个动作，但总是存在这样的可能性，即应用管理器未做出正确的响应。在这种情况下，RKS 仍将记录控制门的使用情况，这样，该活动依将是可记账的，但在某些例子中，恢复由应用管理器“非法”使用的资源可能是有益的。策略服务器可以根据它正在代理的、AM 与 CMTS 之间的消息，收集已超出控制门基于容量的或基于时间的使用限制的事实。使用“收集”技术，意味着策略服务器是有状态的，但一个无状态的策略服务器依然可通过下述的第二种方法恢复资源。

可选地，策略服务器有时可用 Gate-Info 消息来查询 CMTS。响应将包含任何相关的、基于容量的使用限制和控制门使用信息（或基于时间的使用限制和控制门时间信息）。策略服务器而后可以对这些值进行比较。不管策略服务器如何获知控制门超限，它都可以为超限的控制门发出一个 Gate-Delete 消息。一旦收到来自 CMTS 的 Gate-Set-Ack（或 Gate-Set-Err）消息，策略服务器务必将消息发送给应用管理器。

同样，虽然不要求恢复来自超限控制门的资源，CMTS 仍可自己进行同样的对比，并可删除超限的控制门。第 6.5.8 节描述了有关该情形的额外要求。

6.5.7.4 跟踪基于时间和基于容量的使用限制

IPCablecom 多媒体控制门能多次提交和不提交（例如，以便在游戏或流媒体中支持“暂停”功能）。由于当控制门不处于提交的状态时，订户无法传输/接收数据，因此这些期限不应依据它们进行计算。对基于容量的使用限制，该要求没有影响——由于当控制门未提交时不能发送任何分组，因此不可能多算任何分组。不过，对基于时间的使用限制，当控制门未处于提交的状态或提交的一回收状态时，CMTS 务必停止其控制门时间信息计时器。如果未改变基于时间的限制而重新提交控制门，那么务必从其停止点重新开始控制门时间信息计时器。如果改变了基于时间的限制，那么务必将控制门时间信息计时器重新设置为 0，并在重新提交控制门时，重新启动计时器。

注一 要求应用管理器保持计时器独立于 CMTS 计时器，以便执行基于时间的使用限制。由于该计时器与 CMTS 本身是分开的，因此消息发布延迟可能导致这两个计时器之间存在差异。针对时间精度要求高的应用，在其将控制门转换为提交的状态后，或从提交的状态转换为其它状态后，AM 可就其时间信息对象查询 CMTS。

6.5.8 删除控制门程序

通常，当多媒体会话结束时，应用管理器告知策略服务器该会话已结束，策略服务器依次指示 CMTS，通过 Gate-Delete 消息删除控制门。CMTS 务必对 Gate-Delete 消息做出响应，要么通过一个 Gate-Delete-Ack 消息，表示成功，要么通过一个 Gate-Delete-Err 消息，表示失败。响应中的 TransactionID 务必与请求的 TransactionID 相匹配。

在删除控制门时出现的错误务必通过 Gate-Delete-Err 响应予以报告。错误对象务必包含下列错误代码之一：

2 = 未知的 GateID；

127 = 其它，未详细说明的错误。

在 CMTS 上，如果计时器 T1、T2（仅当处于预留状态时）或 T4 到期，那么务必删除控制门。当 CMTS 未经策略服务器请求而删除控制门时，CMTS 务必向策略服务器发送一个 Gate-Report-State 消息（请求的位设为 0），表示已删除控制门。如果 T2 计时器在处于预留状态时到期，那么 CMTS 务必通过 DOCSIS 机制（即一个 DSD 消息）删除 DOCSIS 流，并向 PS 发出一个 Gate-Report-State 状态（请求的位设为 0），告知它状态已转换。注意，如果 T2 计时器在处于提交或提交的一回收状态时到期，那么 CMTS 务必如 DOCSIS 中所定义的那样，发送一个 DSC，以便释放超过活动资源的那部分预留资源，向 PS 发送一个 Gate-Report-State 消息，告知它预留的资源已减少，并保持在相同的状态。一旦收到 Gate-Report-State 消息，策略服务器务必将之转发给应用管理器。

6.5.9 提交控制门程序

在情形 1 中，策略服务器通过包含提交封装的通信业务简表，负责提交控制门。CMTS 利用策略服务器向其下传的参数来提交控制门，并激活 DOCSIS 服务流。

6.5.10 终结序列

当 PEP 关闭其通往 PDP 的 TCP 连接时，它可首先发送一个删除请求状态（DRQ）消息（包括在最初请求消息中使用的句柄对象）。如果 PEP 选择发送 DRQ 消息，那么 PEP 务必使用 COPS 理由代码 4（拆卸）。PEP 之后可以是一个客户机关闭消息。当 TCP 连接终止时，响应中的 PDP 务必自动删除任何与 PEP 相关的

状态。当 PDP 准备关闭时，它应向 PEP 发送一个 COPS 客户机关闭消息。在 COPS 客户机关闭消息中，PDP 不应发送 PDP 重新定向地址对象 PDPRedirAddr。如果 PEP 收到一个来自 PDP 的、带 PDPRedirAddr 对象的 COPS 客户机关闭消息，那么在处理 COPS 客户机关闭消息时，PEP 务必忽略 PDPRedirAddr。

PS 和 CMTS 绝不会因为 COPS 连接失败而移去控制门。

6.5.11 状态同步程序

当策略服务器希望与 CMTS 保持状态同步时，它可发送一个状态同步请求（SSQ）消息。该 SSQ 可包含策略服务器的客户机句柄。如果存在可选的客户机句柄，那么只有与该句柄相关的状态才是同步的。如果 CMTS 未意识到请求的句柄，那么它务必立即为 SSQ 消息中规定的句柄向策略服务器发送一个 DRQ 消息。如果 SSQ 消息中未规定任何客户机句柄，那么带 IPCablecom 多媒体客户机类型的客户机，其所有的活动状态都务必与 PDP 保持同步。

通过为与客户机句柄（如果包括在 SSQ 中的话）相关的控制门发布请求消息，或者为所有已知的控制门（如果未提供任何客户机句柄的话）发布请求消息，CMTS 执行状态同步。当同步完成时，CMTS 务必向 PDP 发送一个同步状态完成（SSC）消息。如果发起的 SSQ 包含一个客户机句柄，那么相应的 SSC 也务必包含该客户机句柄。

7 事件消息发布接口描述

7.1 引言

与 IPCablecom-T 体系结构中一样，IPCablecom-T 多媒体中的事件消息提供了关于 QoS 资源使用情况的详细信息，如预留、激活和释放。对 IPCablecom-T 多媒体框架，新的内容是需要跟踪策略决定（请求、更新、删除）的状况。同时，由于网络资源的使用超出了 IPCablecom-T 中简表的范围（用法不随时间变化），有必要报告基于容量的和基于时间的使用信息。

如本框架中的定义，事件消息由网络元素产生，并保存在记录保持服务器（RKS）中。随后，这些 EM 通过 RKS 或其它后台系统实现关联，以便记录单个的服务例子。可用这些记录得到服务记账信息、网络资源使用样式、性能规划等。不过，EM 不是用来监控故障的。

当前，只有作为电缆运营商网络的一部分且被认为是信任实体的 CMTS 和策略服务器，才在多媒体框架中产生事件消息。其它网络元素，如各种各样的客户机类型，都被视为是不可信任的。对应用管理器的情况，该元素可以是或可以不是电缆运营商网络的一部分，因此不会直接向 RKS 提供 EM。不过，AM 可以提供补充信息，作为发往 PS 的不透明数据字段的一部分，而后它们将包括在由 PS 产生的 EM 中。

多媒体的 IPCablecom 事件消息代表 IPCablecom-T 事件消息的一种简化和修订版本。电话特定的事件，如 Call_Answer 和 Call_Disconnect，被视为是可选的，电话服务特定的事件消息也一样（如服务实例 y）。目的是尽可能发挥现有 EM 实施方案的作用，同时提供足够的抽象机制，以支持一般的多媒体服务。

为支持 IPCablecom-T 语音服务而定义的十四种 EM 中，有四种是 IPCablecom 多媒体特别要求的，包括 QoS_Reserve、QoS_Commit、QoS_Release 和 Time_Change。定义了三种与策略决定相关的新的 EM 消息类型：Policy_Request、Policy_Delete 和 Policy_Update。表 5 概括描述了 IPCablecom 多媒体 EM 消息类型。

表 5/J.179—IPCablecom多媒体EM消息类型

事件消息ID	事件消息	发起要素	描 述
7	QoS_Reserve	CMTS	指明 CMTS 预留 IPCablecom 接入网络上带宽的时间。如果预留的带宽发生变化，那么 CMTS 还务必产生该事件。
8	QoS_Release	CMTS	指明 CMTS 发布其 IPCablecom 接入网络上带宽提交的时间。
17	Time_Change	PS, CMTS	捕获时间变化实例。无论何时，当可信的网络元素（PS 和 CMTS）上的（IPCablecom）时钟变化大于 200 毫秒时，网络元素务必产生一个 Time_Change 消息。
19	QoS_Commit	CMTS	指明 CMTS 提交 IPCablecom 接入网络上带宽的时间。如果提交的带宽发生变化，那么 CMTS 还务必产生该事件。
31	Policy_Request	PS	指明策略服务器从 AM 接收新的策略请求的时间。
32	Policy_Delete	PS	指明策略服务器删除策略的时间。
33	Policy_Update	PS	指明策略服务器接收更新策略请求的时间。

尽管 IPCablecom 多媒体事件消息基于 IPCablecom-T，电话特定的事件消息对 IPCablecom 多媒体而言还是可选的，列于下表中。有关这些事件及其相关属性的更多详情，请参见 ITU-T J.164 建议书 [10]。

表 6/J.179—IPCablecom-T电话EM消息类型

事件消息ID	事件消息	描 述
1	Signaling_Start	指明信令开始时间。
2	Signaling_Stop	指明信令终止时间。
3	Database_Query	指明智能外设完成一次请求/响应事务处理或数据库浏览的时间（如 800 数量数据库、LNP 数据库）。
6	Service_Instance	指明 CMS 提供一个呼叫控制/特性服务实例（如呼叫保持、呼叫等待）的时间。
9	Service_Activation	指明 CMS 记录一次激活服务尝试（如呼叫转送、呼叫等待）的时间。

表 6/J.179—IPCablecom-T电话EM消息类型

事件消息ID	事件消息	描 述
10	Service_Deactivation	指明 CMS 记录一次解除服务尝试（如呼叫转送、呼叫等待）的时间。
13	Interconnect_Start	指明开始出现网络互连信令的时间。
14	Interconnect_Stop	指明 IPCablecom 网络与 PSTN 之间的带宽终止。
15	Call_Answer	指明因发生应答事件而打开了媒介连接。
16	Call_Disconnect	指明因呼叫方通过拖延来终止呼叫，或者目的地地方拖延和被呼叫方呼叫持续计时器到期，而关闭媒介连接的时间。
20	Media_Alive	指明因持续存在载体连接，而使服务保持活动。该消息可以由任何供货商认为合适的可信 IPCablecom 网络元素（CMS、MGC 和 CMTS）产生。

7.2 记录保持服务器要求

记录保持服务器（RKS）是一向可信的网络元素功能。本建议书通常将 RKS 描述为截然不同的、单独的元素，但本建议书并不排除某些源于执行 RKS 功能的其它应用，前提是应用应遵循此处所述的要求。

RKS 是 IPCablecom 多媒体网络与后台应用之间的中间层。RKS 有望处理从 IPCablecom 多媒体网络处接收的数据，并以电缆运营商认为必要的格式以及时间限制内将之提交给后台应用。因此，RKS 充当 IPCablecom 网络与后台应用之间的分界点。

RKS 务必能够接收和处理依据本建议书进行了格式化的事件消息。

事件消息在 RADIUS 消息内进行封装，RADIUS 消息在 UDP 上进行传输，UDP 不保证能够可靠地交付消息；因此，在此定义了协议的请求/响应特性。当 RKS 收到并成功记录所有包含在 RADIUS 结算请求消息中的 IPCablecom 事件消息时，它务必向客户机传送一个结算响应消息。如果它未能成功记录 RADIUS 结算请求消息中的所有 IPCablecom 事件消息，那么 RKS 绝不传送结算响应答复。

如果 IPCablecom “事件消息类型”未被认可，那么 RKS 应忽略事件消息。当事件属性 ID 未被认可时，RKS 还应忽略 IPCablecom 事件属性。

7.3 IPCablecom多媒体网络元素一般要求

本节列举针对 IPCablecom 多媒体网络元素的要求。

7.3.1 元素ID

产生事件消息的各个 IP-Cablecom 网络元素务必使用一个静态的、唯一的元素 ID 来确定其自身。元素 ID 是一个静态配置的元素号码，在一个 IP-Cablecom 域内是唯一的，它务必处于 0~99999 的范围内。

7.3.2 时序

对产生事件消息的元素而言，重要的是各元素相互之间保持密切的同步，并与一个标准的时钟保持密切的同步。本节中所述的要求将确保这些元素能够保持这种同步，并以既准确又精确的时戳报告事件。

产生事件消息的元素务必使用[2]中定义的网络时间协议。元素务必以模式 3（客户机模式）进行操作。NTP.MAXPOLL 值绝不能超过 11，该值对应的时间为 2048 秒。

事件消息务必包含精确到 1 毫秒的时戳。

7.3.3 有关主RKS和副RKS的考虑

IP-Cablecom 多媒体支持由主 RKS 和副 RKS 组成的体系结构。当网络元素（PS、CMTS）无法成功地向主 RKS 发送消息时，副 RKS 将用做失效备援 RKS。IP-Cablecom 多媒体网络元素务必支持向主 RKS 传送事件消息，并当与主 RKS 的通信失败时，作为失效备援发送至副 RKS。一旦网络元素对副 RKS 实现失效备援，那么在该会话期间或控制门上，副 RKS 将变为主 RKS。对策略服务器支持的应用，要求提供主 RKS 和副 RKS。PS 务必在策略决定消息（Gate-Set）中向 CMTS 提供主 RKS 的 IP 地址、端口以及可选的副 RKS。PS 务必支持多对主 RKS 和副 RKS。

为保证数据的可靠传输，网络元素应执行客户机重传事件所需的、用户可配置的重试时间间隔和次数。时间间隔应是可配置的（建议为：10 毫秒至 10 秒），重试的次数应是可配置的（建议为：0 次至 9 次）。重试次数应在主 RKS 和副 RKS 上都做尝试。在用完重试次数之后，应将事件消息写入错误文件中，然后，能从网络元素中删除事件消息。

如果在配置的重试间隔中，IP-Cablecom 网络元素未收到结算响应消息，那么它务必继续重新发送结算请求消息，直至它自 RKS 收到一个结算响应消息，或已达到最大的重试次数。IP-Cablecom 网络元素务必向主 RKS 重新发送同一个结算请求消息，并且如果已达到重试限制，那么向副 RKS 重新发送同一个结算请求。

在网络元素自 RKS 收到一个确认（结算响应）消息、指明已正确接收和存储数据之前，或者在达到最大重试次数之前，所有网络元素都务必保存事件消息。只有当收到一个确认消息或者已达到最大重试次数时，才允许网络元素删除这些事件消息。

一旦网络元素成功向副 RKS 发送事件消息，就出现了向副 RKS 的失效备援。这是一种不可恢复的失效备援，意味着副 RKS 将变成活动的，并成为新的主 RKS。所有后续的、有关会话的事件消息，务必发送给当前活动的副 RKS。对所有新的会话，PDP 务必指示 PEP 使用新的、活动的 RKS 作为主 RKS（也就是说，对后续的会话，之前的副 RKS 将变成为新的主 RKS）。注意，在某些情况下，存在这样的可能性：一个元素，PS 或 CMTS，可以与主 RKS 进行通信，而对同一个会话，其它些元素则不能与之进行通信。在这些情况下，希望 RKS 能够协调主 RKS 与副 RKS 之间的事件消息。

7.3.4 与PacketCable RKS的交互作用

应用管理器可在 Gate-Set 消息中提供一个可选的事件产生信息对象。如果存在该对象，那么它务必包含一个有效的 BCID，该 BCID 能够由 AM、PS 和 CMTS 用于关联流的记账信息。如果应用管理器为 PS 提供了 BCID，且 PS 信任 AM，那么 PS 可使用由应用管理器提供的 BCID。

如果应用管理器提供了一个可选的事件产生信息对象，该对象规定了策略服务器不知晓的主、副 RKS 的 IP 地址，策略服务器务必为该事务向缺省的主 RKS IP 地址发送事件消息，但在失效备援情况下除外，在此情况下，事件消息务必发送至缺省的副 RKS IP 地址。

应用管理器可在可选的事件产生信息对象中规定一个主 RKS IP 地址，或者应用管理器可允许策略服务器使用其缺省的主、副 RKS IP 地址。如果 AM 规定了主 RKS IP 地址，那么它还可规定副 RKS IP 地址。应用管理器指出，不能通过将主、副 RKS IP 地址和端口设为 0 来规定 RKS。

不管策略服务器可以从应用管理器那里接收到什么消息，PS 务必指示 CMTS 使用与策略服务器选择使用的、相同的 BCID 和主/副 RKS IP 地址与端口。PS 应根据 AMID 决定向哪对 RKS 发送消息。

7.4 IPCablecom多媒体的事件消息

本节详细描述和定义为 IPCablecom 多媒体定义的几个事件消息。

7.4.1 策略事件

对 IPCablecom-T 多媒体而言，策略事件消息是新的。它们指明策略服务器收到策略动作请求的时间，并用于划分随之产生的、针对任何资源使用情况的事件消息集，资源使用情况与服务各种各样实例有关。策略事件消息用于指明初始的策略请求、策略的更新以及策略的删除。

收到来自 AM 的策略请求消息后，PS 务必为策略事件消息打上时戳。收到初始策略请求后，PS 务必立即创建一个记账相关 ID (BCID)。各个产生的 BCID 务必符合表 17 中所列记账相关 ID (BCID) 属性结构格式的要求。

对所有随后产生的、与该请求相关的策略事件消息，PS 务必将 BCID 纳入 EM 报头中。PS 也务必将 BCID 纳入发给 CMTS 的 Gate-Set 消息中。

在确定策略请求的结果后，PS 务必立即产生策略事件消息。策略请求的结果可基于 PS 内部授权和准许进入控制机制，或者基于自 CMTS 收到对其 Gate-Set 和 Gate-Delete 消息的响应。当 PS 自 AM 收到一个请求时，PS 为事件消息创建一个时戳，但在它知道请求结果之前，不会产生事件。

7.4.1.1 Policy_Request

如果收到一个创建新策略的请求，那么策略服务器务必向 RKS 发送一个策略请求事件消息。PS 务必将 Policy_Ddecision_Status 设为批准 (1)，或者拒绝 (2)，这基于授权和准许进入控制的结果。

注 — 由于在 CMTS 对 Gate-Set 消息做出响应之前，PS 不发送策略请求事件消息，因此来自 CMTS 的 QoS 事件消息有可能先于策略请求事件消息抵达 RKS。

表 7/J.179—Policy_Request事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
Application_Manager_ID	R	包含网络范围内 AM 的唯一标识符
Subscriber_ID	R	订户 IPv4 地址
Policy_Decision_Status	R	1 – 批准策略 2 – 否定策略
Policy_Denied_Reason	O	当 Policy_Decision_Status = 2（否定策略）时所要求 1 – 策略服务器准许进入控制失败 2 – 资源不足 3 – 订户未知 127 – 其它
FEID	R	财政实体 ID。确定支付实体。由 PS 提供。
AM_Opaque_Data	O	如果应用管理器在“策略请求”（COPS DEC）中包括该对象（ClientSI: Opaque-Data），那么策略服务器务必在 Policy-Event 事件消息中包括它。
Volume_Usage_Limit	O	如果应用管理器在“策略请求”（COPS DEC）中包括该对象（ClientSI: Volume-Based-Usage-Limit），那么策略服务器务必在 Policy-Event 事件消息中包括它。
Time_Usage_Limit	O	如果应用管理器在“策略请求”（COPS DEC）中包括该对象（ClientSI: Time-Based-Usage-Limit），那么策略服务器务必在 Policy-Event 事件消息中包括它。

7.4.1.2 Policy_Delete

当策略服务器收到来自 AM 的 Gate-Delete 消息（指明会话不再需要资源）时，或者当收到为响应 PS 发起的 Gate-Delete 而从 CMTS 发出 Gate-Delete-Ack 时，或者当收到来自 CMTS 的 Gate-Report-State（指明对话资源不再可用）时，PS 务必向 RKS 发送一个 Policy_Delete 事件消息。如果 PS 之前产生过一个 Policy-Request 事件消息，以开启会话，那么它务必总是产生一个 Policy_Delete 事件消息，以结束会话。

表 8/J.179—Policy_Delete事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
Application_Manager_ID	R	包含网络范围内 AM 的唯一标识符
Subscriber_ID	R	订户 IPv4 地址

表 8/J.179—Policy_Delete事件消息

属 性 名 称	要求的或 可选的	注 释
Policy_Deleted_Reason	R	1 – 应用管理器请求 2 – CMTS 决定 127 – 其它
FEID	R	财政实体 ID。确定支付实体。由 PS 提供。
AM_Opaque_Data	O	如果应用管理器在“策略请求”(COPS DEC)中包括该对象 (ClientSI: Opaque-Data)，那么策略服务器务必在 Policy-Event 事件消息中包括它。

7.4.1.3 Policy_Update

如果从 AM 收到一个更改控制门通信业务简表、分类符、容量限制、时间限制或不透明数据的请求，那么策略服务器务必向 RKS 发送一个 Policy_Update 事件消息。

表 9/J.179—Policy_Update事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
Application_Manager_ID	R	包含网络范围内 AM 的唯一标识符
SubscriberID	R	订户 ID
Policy_Decision_Status	R	1 – 批准策略 2 – 否定策略
Policy_Denied_Reason	O	当 Policy_Decision_Status = 2 (否定策略) 时所要求 1 – 策略服务器准许进入控制失败 2 – 资源不足 3 – 订户未知 4 – AMID 未授权 5 – 服务类别名称未定义 6 – 封装不兼容 127 – 其它
Policy_Update_Reason	R	1 – 通信业务简表 2 – 分类符 3 – 容量限制 4 – 时间限制 5 – 不透明的数据 6 – 多个更改 (1-5 的组合) 127 – 其它

表 9/J.179—Policy_Update事件消息

属 性 名 称	要求的或 可选的	注 释
FEID	R	财政实体 ID。确定支付实体。由 PS 提供。
AM_Opaque_Data	O	如果应用管理器在“策略请求”(COPS DEC)中包括该对象(ClientSI: Opaque-Data), 那么策略服务器务必在 Policy-Event 事件消息中包括它。
Volume_Usage_Limit	O	如果应用管理器在“策略请求”(COPS DEC)中包括该对象(ClientSI: Volume-Based-Usage-Limit), 那么策略服务器务必在 Policy-Event 事件消息中包括它。
Time_Usage_Limit	O	如果应用管理器在“策略请求”(COPS DEC)中包括该对象(ClientSI: Time-Based-Usage-Limit), 那么策略服务器务必在 Policy-Event 事件消息中包括它。

7.4.2 QoS_Reserve

该事件消息指明 CMTS 在 IPCablecom 接入网络上预留带宽的时间。如果预留的带宽发生变化, 那么 CMTS 也务必产生该事件消息。

传输 DSA-ACK 或 DSC-ACK 消息、确认已成功向 CM 发送 DSA-RSP 或 DSC-RSP、完成一次资源预留事务处理后, CMTS 务必立即为这一消息打上时戳。

如果来自 CM 的 DSA-RSP 或 DSC-RSP 确认码未获成功, 那么 CMTS 绝不产生这一消息。

表 10/J.179—QoS_Reserve事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
QoS_Descriptor	R	无
SF_ID	R	无
Flow_Direction	R	无
Element_Requesting_QoS	R	0 = 客户机 1 = 策略服务器 2 = 嵌入式客户机

7.4.3 QoS_Commit

QoS_Commit 事件消息指明 CMTS 在 IPCablecom 接入网络上提交带宽的时间。如果提交的带宽发生变化, 那么 CMTS 也务必产生这一事件消息。

传输 DSA-ACK 或 DSC-ACK 消息、确认已成功向 CM 发送 DSA-RSP 或 DSC-RSP、完成一次资源预留事务处理后, CMTS 务必立即为这一消息打上时戳。

如果来自 CM 的 DSA-RSP 或 DSC-RSP 确认码未获成功，那么 CMTS 绝不产生这一消息。

表 11/J.179—QoS_Commit事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
QoS_Descriptor	R	无
SF ID	R	无
Flow_Direction	R	无

7.4.4 QoS_Release

QoS_Release 事件消息指明 CMTS 在 IPCablecom 接入网络上释放其预留与/或带宽提交的时间。

传输 DSD-REQ 消息、指明请求删除带宽后，CMTS 务必立即为这一消息打上时戳。

表 12/J.179—QoS_Release事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
SF ID	R	无
Flow_Direction	R	无
QoS_Release_Reason	R	1 – 由 PS 关闭的控制门 2 – 不活动资源回收 (T4) 计时器到期 3 – CM 失败 4 – 抢占式 5 – RSVP 路径拆卸请求 6 – CM 请求 7 – 准许进入 (T2) 计时器到期 127 – 其它
Gate_Usage_Info	R	无
Gate_Time_Info	R	无

7.4.5 Time_Change

该事件获取一个时间变更实例。无论网络元素 (PS 或 CMTS) 上的 (IPCablecom) 时钟何时改变了超过 200 毫秒，网络元素都务必产生一个时间变更消息。这包括时移事件 (日光节省时间)、为与 NTP 参考时钟和人工时间设置改变保持同步而做的步骤调整。事件消息报头中的 Event_Time 属性务必体现新的 (经过调整的) 时间概念。注意，对由 NTP 执行的回转调整，不要求 Time_Change 消息。

网络元素 (PS 和 CMTS) 务必向活动的 RKS (当前的主 RKS) 发送 Time_Change 事件消息。当控制门当前存在于 CMTS 中时，务必产生 Time_Change 事件消息。当 CMTS 中没有任何控制门时，不必产生

Time_Change 事件消息。不管 CMTS 上存在多少个控制门，只向各个主 RKS 发送一个 Time_Change 事件消息。换言之，如果 CMTS 有若干个控制门，所有的控制门都指向同一个 RKS，那么应只向该 RKS 发送一个 Time_Change 事件消息。

Time_Change 事件消息事件消息报头中的 BCID 务必在事件发生之时，由网络元素在本地产生。BCID 不与任何会话相关的 BCID 相关联，对该事件而言它是一个唯一的 BCID。

表 13/J.179—Time_Change 事件消息

属 性 名 称	要求的或 可选的	注 释
Event_Message_Header	R	见表 16
Time_Adjustment	R	无

7.5 IPCablecom 多媒体的事件消息发布属性

本节描述和定义包括在 IPCablecom 事件消息中的 IPCablecom 属性。

表 14 提供了各个 IPCablecom 事件消息与其相关属性之间的映射关系。表 15 对这些属性分别进行了详细描述。

表 14/J.179—映射至 IPCablecom MM 事件消息的 IPCablecom 属性

EM 属性 ID	EM 属性名称	7 – QoS_Reserve	8 – QoS_Release	17 – Time_Change	19 – QoS_Commit	31 – Policy_Request	32 – Policy_Delete	33 – Policy_Update
1	Event_Message_Header	X	X	X	X	X	X	X
30	SF_ID	X	X		X			
32	QoS_Descriptor	X			X			
38	Time_Adjustment			X				
49	FEID					X	X	X
50	Flow_Direction	X	X		X			
61	AM_Opaque_Data					X	X	X
62	Subscriber_ID					X	X	X
63	Volume_Usage_Limit					X		X
64	Gate_Usage_Info		X					
65	Element_Requesting_Qos	X						
66	QoS_Release_Reason		X					
67	Policy_Denied_Reason					X		X
68	Policy_Deleted_Reason						X	
69	Policy_Update_Reason							X

表 14/J.179—映射至IPCablecom MM事件消息的IPCablecom属性

EM属性ID	EM属性名称	7 – QoS_Reserve	8 – QoS_Release	17 – Time_Change	19 – QoS_Commit	31 – Policy_Request	32 – Policy_Delete	33 – Policy_Update
70	Policy_Decision_Status					X		X
71	Application_Manager_ID					X	X	X
72	Time_Usage_Limit					X		X
73	Gate_Time_Info		X					

表 15 详细定义了 IPCablecom 事件消息的各个属性。属性的数值可用简单的数据格式（一个数据字段）来表示，或用更为复杂的数据结构来表示。

表 15/J.179—IPCablecom MM事件消息属性

EM 属性 ID	EM 属性长度	EM 属性名称	EM 属性值类型	属性数据描述
1	76 字节	EM_Header	数据结构见表 16	每个 IPCablecom 事件消息都需要的公共数据。
30	4 字节	SF_ID	无符号整数	业务流 ID，由 CMTS 为 DOCSIS RF MAC 域内各个 DOCSIS 业务流指派的一个 32 位整数。SFID 认为是上行流方向（USFID）或下行流方向（DSFID）。从同一 SFID 数值空间分配 USFID 和 DSFID。
32	可变的； 最小 8 字节	QoS_Descriptor	数据结构见表 19	QoS 参数数据
38	8 字节	Time_Adjustment	有符号整数	调整元素（PS、CMTS）时钟的时间。 该时间以毫秒计，具体说明了时间的变化量。

表 15/J.179—IPCablecom MM事件消息属性

EM 属性 ID	EM 属性长度	EM 属性名称	EM 属性值类型	属性数据描述
49	长度可变，最大 247 字节	FEID	ASCII 字符串	财政实体 ID。最初的 8 个字节构成电缆运营商定义的数据。缺省地，最初的 8 个字节用 0 填充。从字段的第 9 个字节起，包含电缆运营商的域名，出于记账和结算目的，它唯一地确定电缆运营商。电缆运营商的域名限制为 239 个字节。
50	2 字节	Flow Direction	无符号整数	流方向： 0 = 预留 1 = 上行流 2 = 下行流
61	8 字节	AM_Opaque_Data	无符号整数	从应用管理器传过来的不透明数据。
62	4 字节	Subscriber_ID	无符号整数	代表 IPv4 地址的 4 个串接的字节值。
63	8 字节	Volume_Usage_Limit	无符号整数	由 AM 设定的、以八位字节计的容量限制值。
64	8 字节	Gate_Usage_Info	无符号整数	从 MAC 报头 HCS 之后字节到 CRC 结尾的、在 DOCSIS RF 网络上传送的八位字节数。
65	2 字节	Element_Requesting_QoS	无符号整数	0 = 客户机 1 = 策略服务器 2 = 嵌入式客户机
66	2 字节	QoS_Release_Reason	无符号整数	1 – 由 PS 关闭的控制门 2 – 不活动资源回收 (T4) 计时器到期 3 – CM 失败 4 – 抢占式 5 – RSVP 路径拆卸请求 6 – CM 请求 7 – 准许进入 (T2) 计时器到期 127 – 其它

表 15/J.179—IPCablecom MM事件消息属性

EM 属性 ID	EM 属性长度	EM 属性名称	EM 属性值类型	属性数据描述
67	2 字节	Policy_Denied_Reason	无符号整数	1 – 策略服务器准许进入控制失败 2 – 资源不足 3 – 订户未知 4 – AMID 未授权 5 – 服务类别名称未定义 6 – 封装不兼容 127 – 其它
68	2 字节	Policy_Deleted_Reason	无符号整数	1 – 应用管理器请求 2 – CMTS 决定 127 – 其它
69	2 字节	Policy_Update_Reason	无符号整数	1 – 通信业务简表 2 – 分类符 3 – 容量限制 4 – 时间限制 5 – 不透明的数据 6 – 多个更改（1-5 的组合） 127 – 其它
70	2 字节	Policy_Decision_Status	无符号整数	1 – 批准策略 2 – 否定策略
71	4 字节	Application_Manager_ID	无符号整数	指派给应用管理器的、网络范围内唯一的标识符。
72	4 字节	Time_Usage_Limit	无符号整数	由 AM 设定的、以秒计的时间限制。
73	4 字节	Gate_Time_Info	无符号整数	控制门处于提交或提交回收状态的秒数。

7.5.1 EM_Header属性结构

表 16 包含对 EM 报头属性结构中各字段的详细描述。该事件消息报头属性务必是每个 IPCablecom 事件消息的第一个属性。

表 16/J.179—EM_Header属性结构

字 段 名	语 义	值 类 型	长 度
版本 ID	确定该 EM 报头结构的版本。 1 = IPCablecom 1.0 2 = IPCablecom 1.1 3 = IPCablecom 多媒体 注 — 值 2 或 3 表明使用了该报头中的 Event_Object 字段。 PS 和 CMTS 网络元素务必将 Version_ID 的值设为 3。	无符号整数	2 字节
BCID	网络中某个事务的唯一标识符。	数据结构见表 17	24 字节
事件消息类型	确定事件消息的类型。	无符号整数	2 字节
元素类型	确定发起元素的类型： 0 = 预留 1 = 预留 2 = CMTS 3 = 预留 4 = 策略服务器	无符号整数	2 字节
元素 ID	网络范围内唯一的标识符 5 位（静态配置的、IPCablecom 域内唯一的元素号，范围为 0~99999）。	右对齐，空格填充 ASCII 字符串	8 字节
时区	确定白天节省的时间以及与世界时间（UTC）的偏移量。 白天节省的时间： 0 = 标准时间 1 = 白天节省的时间 UTC 偏移量：+ HHMMSS 从网络元素（PS、CMTS）角度报告的偏移量；它不基于订户的观点。	ASCII 字符串	1 字节 7 字节
序列号	各个网络元素务必为发送给某个特定 RKS 的事件消息指派一个唯一的、单调上升的无符号整数。出于本建议书的目的，单调上升解释为以 1 递增。RKS 利用它来确定事件消息是否从特定的网络元素中丢失了。	无符号整数	4 字节

表 16/J.179—EM_Header属性结构

字 段 名	语 义	值 类 型	长 度
事件时间	事件产生时间和日期。以毫秒计。 格式: yyyymmddhhmmss.mmm	ASCII 字符串	18 字节
状态	状态指示器	见表 18	4 字节
优先级	指明相对其它事件消息的指派重要性: 255 = 最高优先级 0 = 最低优先级 128 = 缺省值	无符号整数	1 字节
属性计数	指明当前事件消息中, 该报头之后 (或添加至该报头) 的属性数量。	无符号整数	2 字节
事件对象	Event_Object 字段允许对业务进行分组。 0 = 结算事件消息 1 = 预留 如果 EM_Header Version_ID 为 3 (发送给 RKS 的 IPCablecom 多媒体事件消息), 那么 PS 和 CMTS 网络元素务必将 Event_Object 字段的值设为 0。 当 Event_Object 字段设为 1 时, RKS 务必将 EM 消息抛弃。	无符号整数	1 字节

7.5.2 记账相关ID (BCID) 字段结构

表 17 描述了记账相关 ID 字段 (BCID)。RKS 或某些其它后台应用, 使用 BCID 来与为单个事务而产生的事件消息实现关联。它是事件消息报头属性中的其中一个字段。BCID 对网络中的各个事务而言是唯一的。带有相同 BCID 的同一个网络元素产生的所有事件消息, 务必发送至同一个主 RKS, 失效的情况除外, 在这种情况下, 务必将事件消息发送至副 RKS。

表 17/J.179—BCID字段描述

字 段 名	语 义	值 类 型	长 度
时戳	高阶 32 位的 NTP 参考时间	无符号整数	4 字节
要素 ID	网络范围内唯一的标识符 5 位（静态配置的、IPCablecom 域内唯一的元素号，范围为 0～99999）。	右对齐，空格填充 ASCII 字符串	8 字节
时区	确定白天节省的时间以及与世界时间（UTC）的偏移量。 白天节省的时间： 0 = 标准时间 1 = 白天节省的时间 UTC 偏移量：+ HHMMSS 从网络元素（PS、CMTS）角度报告的偏移量；它不基于订户的观点。	ASCII 字符串	1 字节 7 字节
事件计数器	对各个事务单调上升	无符号整数	4 字节

7.5.3 状态字段结构

事件消息报头属性中的状态字段是一个 32 位的掩码。第 0 位是最低位；该字段视为一个 4-字节的无符号整数。表 18 描述了状态字段。

表 18/J.179—状态字段描述

开 始 位	语 义	位 计 数
0-1	错误指示器： 0 = 没有错误 1 = 可能的错误 2 = 已知的错误 3 = 预留	2
2	事件起源： 0 = 可信的元素 1 = 不可信的元素	1
3	代理的事件消息： 0 = 未代理，发送方元素知晓所有数据 1 = 代理，由可信的元素代表不可信的元素来发送数据	1
4-31	预留。状态字段位 4-31 务必设为 0。	28

7.5.4 QoS描述符属性结构

表 19 描述了 QoS 描述符数据结构。

表 19/J.179—QoS描述符数据结构

字 段 名	语 义	值 类 型	长 度
Status_Bitmask	描述结构内容的位掩码（见表 20）。	位图	4 字节
Service_Class_Name	服务简表名称。	右对齐，空格填充 ASCII 字符串	16 字节
QoS_Parameter_Array	QoS 参数。由状态位掩码确定的内容。	无符号整数数组	长度可变的 32 位无符号整数 数组

表 20 描述了 QoS 描述符属性的 QoS 状态位掩码字段。第 2~17 位用于描述 QoS_Parameter_Array 的内容。这些位中的各个位指明在数组中存在（位=1）或不存在（位=0）命名的 QoS 参数。特定 QoS 参数在数组中的位置与参数位在位掩码中的次序相匹配，均起始于最低位。

存在于 QoS_Parameter_Array 中的各个 QoS 参数务必占据四个字节。QoS 参数的定义和编码可在 DOCSIS RFI 建议书的附件 C 中获得。其定义规定，小于四个字节的 QoS 参数务必在为数组元素分配的四个字节中右对齐（此处，4 个字节视为一个无符号的整数）。

表 20/J.179—QoS状态位掩码

开 始 位	语 义	位 计 数
0	状态指示： 0 = 无效值 1 = 预留但不激活的资源 2 = 无效值 3 = 预留并激活的资源	2
2	业务流调度类型	1
3	标称的授权间隔	1
4	容许的授权抖动	1
5	授权/间隔	1
6	主动提供的授权大小	1
7	通信业务优先级	1
8	最大持续速率	1
9	最大通信业务突发	1
10	最小预留通信业务速率	1
11	最小分组大小	1
12	最大连续突发	1
13	请求/传输策略	1

表 20/J.179—QoS状态位掩码

开 始 位	语 义	位 计 数
14	标称的轮询间隔	1
15	容许的轮询抖动	1
16	IP 类型的业务覆盖	1
17	最大下行流等待时间	1

7.6 RADIUS结算协议

本节描述产生事件消息的 IPCablecom 网络元素（PS、CMTS）与记录保持服务器（RKS）之间所用的协议。如本建议书所定义，这些网络元素务必支持带 IPCablecom 扩展的 RADIUS 结算（RFC 2866）[8]。

RADIUS 结算协议是一个客户机/服务器协议，包括两种消息类型：结算请求和结算响应。产生事件消息的 IPCablecom 网络元素为 RADIUS 客户机，它们向 RKS 发送结算请求消息。RKS 为一个 RADIUS 服务器，它向 IPCablecom 网络元素回送结算响应消息，指明它已成功收到并保存事件消息。

事件消息按照[8]中的规定格式化为 RADIUS 结算请求和结算响应分组。

7.6.1 认证和机密性

对于使用 IPsec 提供 RADIUS 消息认证和机密性的详细情况，以及正确使用 RADIUS 共享秘密的详细情况，请参考第 8 节。

7.6.2 标准的RADIUS属性

各 RADIUS 消息以表 21 中所示的标准 RADIUS 报头作为起点。

表 21/J.179—RADIUS消息报头

字 段 名 称	语 义	字 段 长 度
代码	结算请求 = 4 结算响应 = 5	1 字节
标识符	用于匹配结算请求和结算响应消息。	1 字节
长度	RADIUS 消息总的长度 最小值 = 20 最大值 = 4096	2 字节
认证符	依据 RADIUS 规范进行计算	16 字节

RADIUS 消息报头之后务必紧跟两个标准的 RADIUS 属性：NAS-IP-Address 和 Acct_Status_Type。由于这两个字段在 RADIUS 结算请求分组中是强制性属性，因此需要包括这两个属性，以便改善与现有 RADIUS 服务器实施方案的互操作性。

NAS-IP-Address 指明结算请求消息的发起者，务必包含发起 IPCablecom 网络元素的 IP 地址。

Acct-Status-Type 属性一般指明结算请求是否标志着用户服务的开始（起始）或结束（终止）。一个 IPCablecom 结算请求消息可包含用户服务的开始、结束或更新。出于这一原因，使用临时更新的 Acct-Status-Type 值来代表 IPCablecom 事件消息。

表 22/J.179—强制性RADIUS属性

名 称	类型	长度	值
NAS-IP-Address	4	6	IPCablecom 网络起始元素的 IP 地址
Acct-Status-Type	40	6	Interim-Update=3

表 23/J.179—RADIUS Acct_Status_Type

类 型	长 度	值
40	6 字节	Interim-Update = 3

如本节所述，在 RADIUS 供货商特定的属性（VSA）结构中对 IPCablecom 属性进行编码。通过向消息增加额外的 RADIUS VSA，可以将额外的 IPCablecom 或供货商特定的属性添加至现有的事件消息中。

供货商特定的属性包括一个用于标识供货商的字段，并且国际互联网指定的号码主管部门（IANA）为 IPCablecom 指定了一个 SMI 网络管理私营企业号码，其值为 4491，用于这些属性的编码。

表 24/J.179—IPCablecom属性的Radius VSA结构

字 段 名 称	语 义	字 段 长 度
类型	供货商特定的 = 26	1 字节
长度	总的属性长度 注 — 值为供货商长度+8。	1 字节
供货商 ID	CableLabs = 4491	4 字节
供货商属性类型	IPCablecom 属性类型	1 字节（见表 15）
供货商属性长度	IPCablecom 属性长度 注 — 值为供货商长度+2。	1 字节（见表 15）
供货商属性值	IPCablecom 属性值	供货商长度字节数

7.6.3 IPCablecom RADIUS结算请求分组语法

```
<<RADIUS Accounting-Request> ::=
    <RADIUS 消息报头>
    <RADIUS NAS-IP-Address 属性>
    <RADIUS Acct-Status-Type 属性>
    <分组电缆 EM>
<分组电缆 EM> ::=
    <有关 IPCablecom EM 报头属性的 RADIUS VSA>
    <IPCablecom EM 属性列表>
```

```
<IPCablecom EM 属性列表> ::=
    <有关 IPCablecom EM 属性的 RADIUS VSA> |
    <IPCablecom EM 属性列表>
    <有关分组电缆 EM 属性的 RADIUS VSA>>
```

事件消息报头是特定事件消息中的第一项属性。事件消息报头之后的事件消息属性次序是任意的。

通过为现有的属性引入新的属性和新的值,IPCablecom 扩展了 RADIUS 结算。由于以这种方式 RADIUS 协议是可扩展的,因此现有的 RADIUS 服务器实施方案有望需要最小的修改,以支持成批收集 IPCablecom 事件消息。

8 安全性要求

IPCablecom 多媒体接口的安全性利用了[11]和[1]中所定义的安全性机制。表 25 概述了各个 IPCablecom 多媒体接口的安全性机制。

表 25/J.179—多媒体安全性接口

接 口	描 述	安 全 机 制
pkt-mm-1	CMTS – CM	由附件 B/J.112 定义的、基于 HMAC 的认证。
pkt-mm-2	PS – CMTS	使用 IKE 或基于 Kerberos 的密钥管理的 IPsec ESP。
pkt-mm-3	AM – PS	使用 IKE 或基于 Kerberos 的密钥管理的 IPsec ESP。
pkt-mm-4	PS – RKS	使用 IKE 或基于 Kerberos 的密钥管理的 IPsec ESP。
pkt-mm-5	CMTS — RKS	使用 IKE 或基于 Kerberos 的密钥管理的 IPsec ESP。
pkt-mm-6	客户机 — CMTS	超出了本建议书该版本的讨论范围。
pkt-mm-7	客户机 — AM	超出了本建议书该版本的讨论范围。
pkt-mm-8	AM — 对等	超出了本建议书该版本的讨论范围。
pkt-mm-9	CMTS — 电缆运营商管理的 IP 网络	超出了本建议书该版本的讨论范围。
pkt-mm-10	客户机 — 对等	超出了本建议书该版本的讨论范围。

以下各节描述了应用于各个 IPCablecom 多媒体接口的安全性,并对附加的需求和需要的扩展做了详细说明。

8.1 CMTS — CM QoS接口 (pkt-mm-1)

利用 HMAC (散列消息认证代码)对附件 B/J.112 QoS 消息进行认证,它是一个关键的密码散列。务必包括在附件 B/J.112 QoS 消息中的、对 HMAC 属性的计算,在[1]的第 B.C.1.4.1 节中予以详细说明。

8.2 策略服务器 — CMTS COPS接口 (pkt-mm-2)

务必利用 IPsec ESP 协议保证策略服务器—CMTS COPS 接口的安全,如[11]第 7.2.1.3.2 节中所规定的那样。有关该接口的密钥管理务必符合[11]第 7.2.1.4.1 节的要求。对该接口,策略服务器务必符合[11]第 7.2.1.3.2 节和第 7.2.1.4.1 节中所列之所有控制门控制器的要求。要求执行带预共享密钥的 IKE,而带证书的 IKE 和 Kerberos 化的 IPsec 的执行都是可选的。

在利用 Kerberos 化的 IPsec 的情况下,[11]第 6.4.5 节定义了有关各种各样 Kerberos 化的服务的主要名

称。对各个类型的 Kerberos 化的服务而言，主要名称的第一部分是唯一的。[11]第 6.4.5 节已经规定了 CMTS 主要名称的第一部分。策略服务器主要名称的第一部分必须为：

policyserver:<ElementID>

其中<ElementID>在[11]的第 6.4.5 节中定义。

在利用带证书的 IKE 的情况下，服务器证书中的主题名称拥有下列属性，它们在[11]第 8.2.3.4.3 节中进行定义：

OU=<分系统名称>

<分系统名称>的值用于确定服务器类型。CMTS 的<分系统名称>值已经在[11]第 8.2.3.4.3 节中进行定义。策略服务器的<分系统名称>值必须为以下字符串：policyserver。

8.3 应用管理器 — 策略服务器COPS接口（pkt-mm-3）

务必利用 IPsec ESP 协议保证应用管理器—策略服务器 COPS 接口的安全，如[11]第 7.2.1.3.2 节中所规定的那样。有关该接口的密钥管理必须符合[11]第 7.2.1.4.1 节的要求。对该接口，应用管理器必须符合[11]第 7.2.1.3.2 节和第 7.2.1.4.1 节中所列之所有控制门控制器的要求。要求执行带预共享密钥的 IKE，而带证书的 IKE 和 Kerberos 化的 IPsec 的执行都是可选的。

在利用 Kerberos 化的 IPsec 的情况下，[11]第 6.4.5 节定义了有关各种各样 Kerberos 化的服务的主要名称。对各个类型的 Kerberos 化的服务而言，主要名称的第一部分是唯一的。8.2/J.170 规定了策略服务器主要名称的第一部分。应用管理器主要名称的第一部分必须为：

am:<ElementID>

其中<ElementID>在[11]的第 6.4.5 节中定义。

在利用带证书的 IKE 的情况下，服务器证书中的主题名称拥有下列属性，它们在[11]第 8.2.3.4.3 节中进行定义：

OU=<分系统名称>

<分系统名称>的值用于确定服务器类型。策略服务器的<分系统名称>值在 8.2/J.170 中进行定义。应用管理器的<分系统名称>值必须为以下 2-字符串：am。

8.4 策略服务器 — RKS事件消息接口（pkt-mm-4）

务必利用 IPsec ESP 协议保证策略服务器—RKS 事件消息接口的安全，如[11]第 7.3.2 节中所规定的那样。有关该接口的密钥管理要求务必等同于在[11]第 7.3.3.2 节中为 CMTS-RKS 接口所规定的要求。要求执行带预共享密钥的 IKE，而带证书的 IKE 和 Kerberos 化的 IPsec 的执行都是可选的。

在利用 Kerberos 化的 IPsec 的情况下，[11]第 6.4.5 节定义了有关各种各样 Kerberos 化的服务的主要名称。对各个类型的 Kerberos 化的服务而言，主要名称的第一部分是唯一的。[11]第 6.4.5 节已经规定了 RKS 主要名称的第一部分。策略服务器主要名称的第一部分在 8.2/J.170 进行规定。

在利用带证书的 IKE 的情况下，服务器证书中的主题名称拥有下列属性，它们在[11]第 8.2.3.4.3 节中进行定义：

OU=<分系统名称>

<分系统名称>的值用于确定服务器类型。RKS的<分系统名称>值已经在[11]第 8.2.3.4.3 节中进行定义。策略服务器的<分系统名称>值在[11]第 8.2 节中进行规定。

8.5 CMTS – RKS事件消息接口 (pkt-mm-5)

务必利用 IPsec ESP 协议保证 CMTS—RKS 事件消息接口的安全，如[11]第 7.3.2 节中所规定的那样。有关该接口的密钥管理在[11]第 7.3.3.2 节中进行说明。要求执行带预共享密钥的 IKE，而带证书的 IKE 和 Kerberos 化的 IPsec 的执行都是可选的。

9 将FlowSpec通信业务简表映射至DOCSIS

通信业务简表定义了 IP 流或附件 B/J.112 中业务流的 QoS 属性，它们在执行授权、预留和提交操作时使用。通信业务简表可通过以下方法中的一种来定义：

- FlowSpec;
- DOCSIS 服务类别名称;
- DOCSIS 特殊的参数化。

本节描述了从各种不同的通信业务简表表示中获得 DOCSIS 特定的 QoS 参数的映射程序。通信业务简表可包括授权、预留或提交封装。如[3]中所定义，一个 FlowSpec 由一个 TSpec 和一个可选的 RSpec 组成。

9.1 将FlowSpecs映射至DOCSIS调度类型

FlowSpec 支持两种类型的业务：受控负载业务和保证业务。受控负载业务提供最小带宽保证，但没有等待时间/延迟方面的保证。保证业务既有带宽保证，也有等待时间/延迟保证。保证业务可通过 DOCSIS 实时轮询和 UGS 调度类型来近似估计。受控负载业务可通过 DOCSIS 尽力服务调度类型来近似估计。在 FlowSpec 定义中，受控负载业务与保证业务之间的 FlowSpec 业务编号不同，受控负载业务的业务编号是 5，保证业务的业务编号是 2。此外，受控负载业务只包含 TSpec 令牌桶参数，而没有 RSpec 参数。保证业务务必同时包含 TSpec 和 RSpec 参数。

对那些等待时间和抖动敏感的应用，如语音、MPEG 视频或游戏，则可考虑请求保证业务。然后，CMTS 可使用 FlowSpec 中规定的通信业务简表参数，从能提供保证业务的两种 DOCSIS 调度类型中选择一种：RTPS 和 UGS。对其它那些等待时间不敏感的应用，则可考虑请求能用于提供最小带宽保证的受控负载业务。表 26 对各选择方案做了概述。

表 26/J.179—映射FlowSpecs类型

DOCSIS调度类型	FlowSpec业务编号	应用 举例
主动提供的授权服务（UGS）	2（保证的）	IP 语音
实时的轮询服务（RTPS）	2（保证的）	VPN
尽力服务（BE）	5（受控的负载）	尽力服务的互联网数据

上行流业务流的 FlowSpec 到 DOCSIS 的一般映射过程如下所述：

- 一旦接收到带 FlowSpec 的 Gate-Set 消息，CMTS 务必要分析 TSpec 业务报头，以确定请求的是受控负载业务还是保证业务。
- 如果是受控负载业务，那么 CMTS 务必要只能使用 TSpec 参数，来解析 DOCSIS 调度参数，以便为 DOCSIS 尽力服务调度类型定义 DOCSIS 通信业务参数。
- 如果是保证业务，那么 CMTS 务必要检查 TSpec 参数的预留速率（R）和桶速率（r）值。如果这两个值相等，那么 CMTS 务必要使用 TSpec 和 RSpec，来为 DOCSIS UGS 调度类型定义 DOCSIS 通信业务参数。
- 如果预留速率（R）和桶速率（r）的值不相等，那么 CMTS 务必要使用 TSpec 和 RSpec，来为 DOCSIS 实时轮询调度类型定义 DOCSIS 通信业务参数。

注意，另外还有两种类型的 DOCSIS 调度类型未在上面提到，它们是：

- 带活动性检测的、主动提供的授权服务；
- 非实时轮询服务。

如果应用管理器希望请求这些业务中的任何一种，那么只能通过在定义通信业务简表时使用服务类别名称或 DOCSIS 特定的参数化方法来进行。

9.2 将FlowSpecs映射至DOCSIS通信业务参数

FlowSpec 由以下两部分组成：TSpec 和 RSpec。TSpec 描述流的通信业务量，RSpec 描述所希望的服务；注意，对受控负载业务，不使用 RSpec。对保证业务，务必要规定 RSpec 参数。对受控负载业务，CMTS 务必要忽略 RSpec 参数。RSpec 为保证业务提供等待时间保证。有关应用管理器如何使用这些参数来规定通信业务简表的更详细信息，请参考 RFC 2210 [3]、RFC 1305 [2]、RFC 2211 [4] 和 RFC 2212 [5]。注意，Flowspec 的 IPCablecom 多媒体解释与 RFC 在以下几方面是有区别的：

- 如[5]中定义的保证业务控制第 3 层排队延迟（即与分组调度相关的延迟），而在 IPCablecom 多媒体中，我们主要关心的是控制 DOCSIS MAC 层的访问延迟。因此，我们根据 TSpec 的 r 参数来预留带宽资源，而不是根据 RSpec 的 R 参数。
- 如[4]中定义，受控负载业务只为流定义了一个最低保证速率。IPCablecom 多媒体的受控负载业务既为流定义了最高速率，又定义了无最低保证速率的流。
- 在 IPCablecom 多媒体中不需要保证业务空隙期限参数，因此将重新定义该字段，以便能够控制 DOCSIS 轮询抖动。

TSpec 参数有：

- 桶深度（b），以字节为单位；
- 桶速率（r），以字节/秒为单位；
- 最大数据报大小（M），以字节为单位；
- 最小监管单元（m），以字节为单位；
- 峰值速率（p），以字节/秒为单位。

RSpec 参数有:

- 预留速率 (R), 以字节/秒为单位;
- 空隙期限 (S), 以毫秒为单位。

DOCSIS 上行流 BE (尽力服务) 和下行流受控负载业务流的参数映射关系大致包括以下几种。实际的映射过程将涉及对这些参数的归一化, 以便考虑到第 2 层和第 3 层报头因素。

- TSpec 桶深度 (b) $\sim$ DOCSIS 最大通信业务突发;
- TSpec 最大数据报大小 (M) $\sim$ <DOCSIS 不需要>;
- TSpec 最小监管单元 (m) $\sim$ DOCSIS 假定的最小预留速率分组大小;
- TSpec 桶速率 (r) $\sim$ DOCSIS 最小预留速率;
- TSpec 峰值速率 (p) $\sim$ 受控负载业务的 DOCSIS 最大持续速率。

对下行流保证业务流, 增加了 RSpec 参数, 用于提供等待时间和预留保证:

- TSpec 桶深度 (b) $\sim$ DOCSIS 最大通信业务突发;
- TSpec 最大数据报大小 (M) $\sim$ <DOCSIS 不需要>;
- TSpec 最小监管单元 (m) $\sim$ DOCSIS 假定的最小预留速率分组大小;
- TSpec 桶速率 (r) $\sim$ DOCSIS 最小预留速率;
- RSpec 预留速率 (R) $\sim$ 保证业务的 DOCSIS 最大持续速率;
- RSpec 间隙期限 $\sim$ DOCSIS 下行流等待时间。

DOCSIS UGS 业务流的参数映射关系大致包括以下几种:

- TSpec 桶深度 (b) = TSpec 最大数据报大小 (M) = TSpec 最小监管单元 (m) $\sim$ DOCSIS 主动提供的授权大小;
- TSpec 桶速率 (r) = TSpec 峰值速率 (p) = RSpec 预留速率 (R) $\sim$ <DOCSIS 不需要>;
- RSpec 间隙期限 $\sim$ DOCSIS 容许的授权抖动。

类似地, DOCSIS 实时轮询服务流的参数映射关系包括以下几种:

- TSpec 桶深度 (b) $\sim$ DOCSIS 最大通信业务突发;
- TSpec 最大数据报大小 (M) $\sim$ <DOCSIS 不需要>;
- TSpec 桶速率 (r) $\sim$ 保证业务的 DOCSIS 最大持续速率;
- RSpec 预留速率 (R) $\sim$ 用于计算轮询间隔;
- RSpec 间隙期限 $\sim$ 容许的轮询抖动。

该抽象模型允许基于标准的 RSVP 实现 (如情形 2 和情形 3 中所预期的那样) 从网络请求和接收受控负载业务或保证业务, 而不必需要 DOCSIS 特定的信息。

在某些情况下, 即应用管理器和策略服务器深知 DOCSIS, 则可以使用 DOCSIS 服务类别名称或 DOCSIS 特定的参数化格式来规定控制门的通信业务简表。

注意，有若干 DOCSIS 服务流参数并不能直接从 FlowSpec 中得到；在这些情况下，IPCablecom 多媒体建议书为这些服务流参数定义了缺省值。如果应用管理器/策略服务器希望将那些服务流参数设为不同于本建议书所规定的缺省值的其它值，那么应用管理器/策略服务器必须使用服务类别名称或 DOCSIS 特定的参数化格式，定义通信业务简表。

对保证业务，最小预留速率和最大持续速率设为同一值，均基于桶速率 (r)。这是因为，保证业务提供等待时间保证，这意味着流速率不会保持在源端同意产生的速率（当最初进行预留时）之上。利用通信业务简表生成的预留规定一个桶速率 (r)，意味着源端通信业务流速率不会高于 r 。因此，在保证业务情况下，使用预留速率 ‘ R ’ 来表示任一 DOCSIS 持续速率（不论是还是最大）都是不正确的。

不过，对实时轮询调度，CMTS 使用预留速率 R 来计算轮询间隔，以便通信业务源速率可以突发到 R ，而不会增加分组等待 DOCSIS 上行流传输机会的延迟。虽然这种情况下通信业务源可以 ‘ R ’ 速率产生通信业务，但 CMTS 将确保持续速率不低于 ‘ r ’。

对受控负载业务，由于没有等待时间保证，并且由于我们希望使之能够使用 DOCSIS 特定的保证最小以及最大持续速率概念，因此，将 TSpec 桶速率 ‘ r ’ 映射至 DOCSIS 最小速率，将 TSpec 峰值速率 ‘ p ’ 映射至 DOCSIS 最大持续速率。如果 ‘ r ’ 值为 0 或无穷大，那么务必忽略 DOCSIS 最小预留速率参数。如果 ‘ p ’ 值为 0 或无穷大，那么务必忽略 DOCSIS 最大持续速率参数。

如果 DOCSIS RFI 规范与本规范之间存在语法或语义上的冲突，那么除非另有说明，否则以 DOCSIS RFI 规范为准。

9.3 DOCSIS上行流参数

除非另有说明，否则务必使用下面的公式来计算所有的上行流分组大小：分组 PDU 务必从 DOCSIS MAC HCS 之后的第一个字节计算到 CRC 的最后一个字节。该值包括 18 个字节的以太网报头开销（源地址占 6 个字节，目的地地址占 6 个字节，长度占 2 个字节，CRC 占 4 个字节）。另外还包括 DOCSIS MAC 层的开销，即 DOCSIS 基报头占 6 个字节，UGS 扩展报头占 3 个字节，BPI+扩展报头占 5 个字节。

在所有后续各节中所用的等式里，会用到以下变量：

ENET = 以太网开销（18 或 22 个字节），除非另有说明，否则它缺省务必使用 18 个字节（CMTS 如何确定使用 22 个字节超出了本建议书的讨论范围）。在 UGS 流情况下，使用未做说明的扩展型以太网报头的分组将导致分组被抛弃（超过授权大小的分组肯定被抛弃）。在 RTPS 流情况下，使用未做说明的扩展型以太网报头的分组将导致在主（尽力服务）服务流上传送分组。

DOCSIS = DOCSIS 报头 = 6 字节

BPI = DOCSIS BPI 报头 = 5 字节

UGS = DOCSIS UGS 扩展报头 = 3 字节

9.3.1 主动提供的授权调度 (UGS)

当服务编号为 2 时 (保证业务), 务必使用主动提供的授权调度。峰值速率、桶速率和预留速率都相等, 最大数据报大小等于最小监管单元。

DOCSIS 上行流对象务必要如下面所述的那样进行设置。未在此进行定义的所有服务流服务质量 TLV 编码务必要如 DOCSIS 所指明的那样给出缺省值。

除了使用第 9.3 节中规定的公式计算得到的分组 PDU 大小之外, DOCSIS 主动提供的授权大小还合并了 DOCSIS MAC 层的开销。DOCSIS MAC 层的开销包括 DOCSIS 基本报头 (6 个字节)、UGS 扩展报头 (3 个字节), 以及可选的 BPI+扩展报头 (5 个字节)。

$$\text{DOCSIS 主动提供的授权大小} = M + \text{ENET} + \text{DOCSIS} + \text{UGS} + \text{BPI}$$

上面的例子假设能够实现 BPI+ [12]。

DOCSIS 最大持续通信业务速率和 DOCSIS 假定的最小预留速率分组大小参数绝不能用于上行流。

每个间隔参数的 DOCSIS 授权务必设为 1。

DOCSIS 标称的授权间隔参数务必设为: 最大数据报大小除以预留速率, 并转换为微秒。

$$\text{DOCSIS 标称的授权间隔} = M/R \times 1\,000\,000。$$

DOCSIS 容许的授权抖动参数务必设为间隙期限。如果值小于一个 DOCSIS 小时间片的时间, 那么务必使用小时间片的时间作为该值。如果规定的值为 0, 那么务必使用缺省值 800 μs 。

对 UGS 服务流, 绝不能在通信业务简表中规定 DOCSIS 标称的轮询间隔参数。对 UGS 服务流, 绝不能在通信业务简表中规定 DOCSIS 容许的轮询抖动参数。

DOCSIS 请求/传输策略参数是一个位掩码; 对 UGS 服务流, 务必要设置第 0-6 位和第 8 位。

9.3.2 实时轮询调度

当服务编号为 2 (保证业务) 以及峰值速率不等于桶速率或最大数据报大小不等于最小监管单元时, 务必使用实时轮询调度。

DOCSIS 上行流对象务必要如下面所述的那样进行设置。未在此进行定义的所有服务流服务质量 TLV 编码务必要如 DOCSIS 所指明的那样给出缺省值。

DOCSIS 最大持续通信业务速率参数以比特/秒为单位给出, 包括以太网层的开销。IP 特定参数的转换首先涉及确定分组化的速率, 通过桶速率除以最小监管单元来实现。然后, 用该值乘以分组大小、最小监管单元, 经修正, 包括 MAC 层的开销, 然后将整个乘积从字节转换为比特。

$$\text{DOCSIS 最大持续通信业务速率} = r/m \times (m + \text{ENET}) \times 8$$

DOCSIS 最大通信业务突发参数务必设为以下两个参数中的较大者:

- 1) 桶深度 (包含以太网开销的桶深度, 用最小监管单元计算得到); 或者

2) DOCSIS 规定的最小值 1522。

$$\text{DOCSIS 最大通信业务突发} = \max((\text{桶深度} / m) \times (m + \text{ENET}), 1522)$$

DOCSIS 最小预留通信业务速率参数同 DOCSIS 最大持续通信业务速率。

$$\text{DOCSIS 最小预留通信业务速率} = r/m \times (m + \text{ENET}) \times 8$$

DOCSIS 请求/传输策略参数是一个位掩码；建议的缺省值应为 0x1F。

DOCSIS 标称的轮询间隔参数务必设为：最小监管单元除以预留速率，并转换为微秒。

$$\text{DOCSIS 标称的轮询间隔} = m/R \times 1\,000\,000$$

DOCSIS 容许的轮询抖动参数务必设为间隙期限。如果值不为 0，并且小于一个小时间片的时间，那么它务必要设为小时间片的时间。如果规定的值为 0，那么 DOCSIS 容许轮询抖动务必使用缺省值 800 μs 。

$$\text{DOCSIS 标称的轮询抖动} = S$$

9.3.3 尽力服务调度

当服务编号为 5 时（受控负载），务必使用尽力服务调度。

DOCSIS 上行流对象务必要如下面所述的那样进行设置。未在此进行定义的所有服务流服务质量 TLV 编码务必要如 DOCSIS 所指明的那样给出缺省值。

DOCSIS 通信业务优先级务必设为 5。

DOCSIS 最大持续通信业务速率参数以比特/秒为单位给出，包括以太网层的开销。IP 特定参数的转换首先涉及确定分组化的速率，通过峰值速率除以最小监管单元来实现。然后，用该值乘以分组大小、最小监管单元，经修正，包括以太网层的开销，然后将整个乘积从字节转换为比特。DOCSIS 最大持续通信业务速率务必按以下方式从最小监管单元转换而来：

$$\text{DOCSIS 最大持续通信业务速率} = p/m \times (m + \text{ENET}) \times 8$$

DOCSIS 最大通信业务突发参数务必设为以下两个参数中的较大者：

- 1) 桶深度（包含以太网开销，用最小监管单元计算得到）；或者
- 2) DOCSIS 规定的最小值 1522。

$$\text{DOCSIS 最大通信业务突发} = \max((\text{桶深度} / m) \times (m + \text{ENET}), 1522)$$

DOCSIS 最小预留通信业务速率参数计算方式与 DOCSIS 最大持续通信业务速率相似，除了要用桶速率取代峰值速率参数。

$$\text{DOCSIS 最小预留通信业务速率} = r/m \times (m + \text{ENET}) \times 8$$

9.3.4 上行流分组分类编码

9.3.4.1 DOCSIS上行流分组分类请求

DOCSIS 上行流对象务必要如下面所述的那样进行设置。未在此进行定义的所有分类 TLV 编码务必要如 DOCSIS 所指明的那样给出缺省值。

务必要设置 DOCSIS 分类符标识符参数。

务必要设置 DOCSIS 服务流标识符参数。

DOCSIS 规则优先级参数务必要在分类符对象中设为优先级值。

当控制门使用服务流被提交时，DOCSIS 分类激活状态参数务必要设为活动的（1），对任何其它情况，都务必将之设为非活动的（0）。

DOCSIS 动态服务修改活动可使用 DOCSIS RFI 建议书中的 DSC 增加分类符（0）、DSC 替换分类符（1）和 DSC 删除分类符（2）操作。

如果值不为 0，那么 DOCSIS IP 协议参数务必要设为分类符对象中规定的协议 ID 值，否则忽略之。

如果值不为 0，那么 DOCSIS IP 源地址参数务必要设为与分类符对象中相同的地址。如果分类符对象中规定的地址为 0，那么务必忽略该参数。

务必忽略 DOCSIS IP 源掩码参数。

如果值不为 0，那么 DOCSIS IP 源端口起始和 DOCSIS IP 源端口终止参数务必要设为与分类符对象中相同的端口值。如果分类符对象中规定的值为 0，那么务必忽略 DOCSIS IP 源端口起始和 DOCSIS IP 源端口终止参数。

如果值不为 0，那么 DOCSIS IP 目的地地址参数务必要设为与分类符对象中相同的地址。如果分类符对象中规定的地址为 0，那么务必忽略该参数。

务必忽略 DOCSIS IP 目的地掩码参数。

如果值不为 0，那么 DOCSIS IP 目的地端口起始和 DOCSIS IP 目的地端口终止参数务必要设为与分类符对象中相同的端口值。如果分类符对象中规定的值为 0，那么务必忽略 DOCSIS IP 目的地端口起始和 DOCSIS IP 目的地端口终止参数。

务必忽略 DOCSIS 以太网 LLC 分组类别编码参数。

务必忽略 DOCSIS 802.1P/Q 分组类别编码数据。

9.4 DOCSIS下行流参数

9.4.1 有关担保业务的下行流QoS编码

DOCSIS 下行流服务流服务质量 TLV 编码务必要如下面所述的那样进行设置。未在此进行定义的所有服务流服务质量 TLV 编码务必要如 DOCSIS 所指明的那样给出缺省值。

下行流 DOCSIS 参数使用 DOCSIS MAC 报头进行计算，从 HCS 之后的第一个字节计算到 CRC 的最后一个字节。该值包括以太网报头的开销。

基于此开销，DOCSIS 假定的最小预留速率分组大小参数务必按以下方式进行计算：

$$\text{DOCSIS 假定的最小预留通信业务速率分组大小} = m + \text{ENET}$$

DOCSIS 最大持续通信业务速率参数以比特/秒为单位给出，包括 MAC 层的开销。IP 特定参数的转换首先涉及确定分组化的速率，通过桶速率除以最小监管单元来实现。然后，用该值乘以分组大小、最小监管单元，经修正，包括 MAC 层的开销，然后将整个乘积从字节转换为比特。DOCSIS 最大持续通信业务速率务必按以下方式进行计算：

$$\text{DOCSIS 最大持续通信业务速率} = r/m \times (m + \text{ENET}) \times 8$$

DOCSIS 最小预留通信业务速率等于 DOCSIS 最大持续通信业务速率。

注意，DOCSIS 最大持续通信业务速率和 DOCSIS 最小预留通信业务速率的计算方法在 IP-Cablecom 多媒体和 IP-Cablecom DQoS 中是稍有区别的。IP-Cablecom 多媒体基于 r 来计算，而 IP-Cablecom DQoS 是基于 p 来计算。这是因为在 DQoS 中 $r=p$ ，而在多媒体中，这些值是不同的（此时应使用 r 这个正确的速率值）。

DOCSIS 最大通信业务突发参数必须设为以下两个参数中的较大者：

- 1) 桶深度（包含 DOCSIS 开销，用最小监管单元计算得到）；或者
- 2) DOCSIS 规定的最小值 1522。

DOCSIS 最大通信业务突发 = $\max((\text{桶深度} / m) \times (m + \text{ENET}), 1522)$

DOCSIS 通信业务优先级参数必须设为 5。

如果间隙期限不为 0，那么 DOCSIS 下行流等待时间参数必须设为间隙期限。如果间隙期限为 0，那么该参数绝不能设置值。

9.4.2 有关控制负载业务的下行流 QoS 编码

DOCSIS 下行流服务流服务质量 TLV 编码务必要像下面所述的那样进行设置。没有在此定义的所有服务流服务质量 TLV 编码务必要像 DOCSIS 所指出的那样给出其缺省值。

下行流 DOCSIS 参数使用 DOCSIS MAC 报头进行计算，从 HCS 之后的第一个字节计算到 CRC 的最后一个字节。该值包括以太网报头的开销。

基于此开销，DOCSIS 假定的最小预留速率分组大小参数必须按以下方式进行计算：

DOCSIS 假定的最小预留速率分组大小 = $m + \text{ENET}$

DOCSIS 最大持续通信业务速率参数以比特/秒为单位给出，包括 MAC 层的开销。IP 特定参数的转换首先涉及确定分组化的速率，通过峰值速率除以最小监管单元来实现。然后，用该值乘以分组大小、最小监管单元，经修正，包括以太网层的开销，然后将整个乘积从字节转换为比特。DOCSIS 最大持续通信业务速率必须按以下方式进行计算：

DOCSIS 最大持续通信业务速率 = $p/m \times (m + \text{ENET}) \times 8$

DOCSIS 最小预留通信业务速率参数计算方式与 DOCSIS 最大持续通信业务速率类似，只是用桶速率取代了峰值速率。

DOCSIS 最小预留通信业务速率 = $r/m \times (m + \text{ENET}) \times 8$

DOCSIS 最大通信业务突发参数必须设为以下两个参数中的较大者：

- 1) 桶深度（包括 DOCSIS 开销，利用最大数据报大小计算得到）；或者
- 2) DOCSIS 规定的最小值为 1522。

DOCSIS 最大通信业务突发 = $\max((\text{桶深度} / M) \times (M + \text{ENET}), 1522)$

DOCSIS 通信业务优先级参数必须设为 5。

DOCSIS 下行流等待时间参数绝不能设置值。

9.4.3 下行流分组分类编码

9.4.3.1 DOCSIS下行流分组分类请求

DOCSIS 下行流分类对象务必要像下面所述的那样进行设置。没有在此定义的所有分类 TLV 编码务必要像 DOCSIS 所指示的那样给出其缺省值。

务必使用 DOCSIS 分类符标识符参数。

务必使用 DOCSIS 服务流标识符参数。

DOCSIS 规则优先级参数务必设置为分类符对象中规定的优先级值。

当提交使用服务流的控制门时，DOCSIS 分类激活状态参数务必设为活动的（1），除此之外的所有其它情况，都务必将之设为不活动的（0）。

DOCSIS 动态服务变化活动可依据 DOCSIS RFI 建议书，使用 DSC 增加分类符（0）、DSC 替换分类符（1）和 DSC 删除分类符（2）操作。

如果值不为 0，那么 DOCSIS IP 协议参数务必设为分类符对象中规定的协议 ID 值，如果为 0，那么忽略之。

如果提供的值不为 0，那么 DOCSIS IP 源地址参数务必设为分类符对象中提供的源地址。如果分类符对象中规定的地址为 0，那么务必忽略该参数。

务必忽略 DOCSIS IP 源掩码参数。

如果提供的值不为 0，那么 DOCSIS IP 源端口起始和 DOCSIS IP 源端口终止参数务必设为同分类符对象相同的端口值。如果分类符对象中规定的值为 0，那么务必忽略 DOCSIS IP 源端口起始和 DOCSIS IP 源端口终止参数。

如果提供的值不为 0，那么 DOCSIS IP 目的地地址参数务必设为分类符对象中规定的目的地地址。如果分类符对象中规定的地址为 0，那么务必忽略该参数。

务必忽略 DOCSIS IP 目的地掩码参数。

如果提供的值不为 0，那么 DOCSIS IP 目的地端口起始和 DOCSIS IP 目的地端口终止参数务必设为同分类符对象相同的端口值。如果分类符对象中规定的值为 0，那么务必忽略 DOCSIS IP 目的地端口起始和 DOCSIS IP 目的地端口终止参数。

务必忽略 DOCSIS 以太网 LLC 分组分类编码。

务必忽略 DOCSIS 802.1P/Q 分组分类编码。

10 消息流

本节为本建议书之前介绍的各种网络元素提供了两种交互方式。第一种交互方式在较高的层次上描述了基本的消息交换，它出现于 IPCablecom 多媒体框架中，用于实现情形 1 下的接入网络资源授权、预留和提交。第二种交互方式对 IPCablecom 多媒体 QoS 和 EM 接口中所涉及的各种消息和属性进行了非常详细的描述。

10.1 基本的消息序列

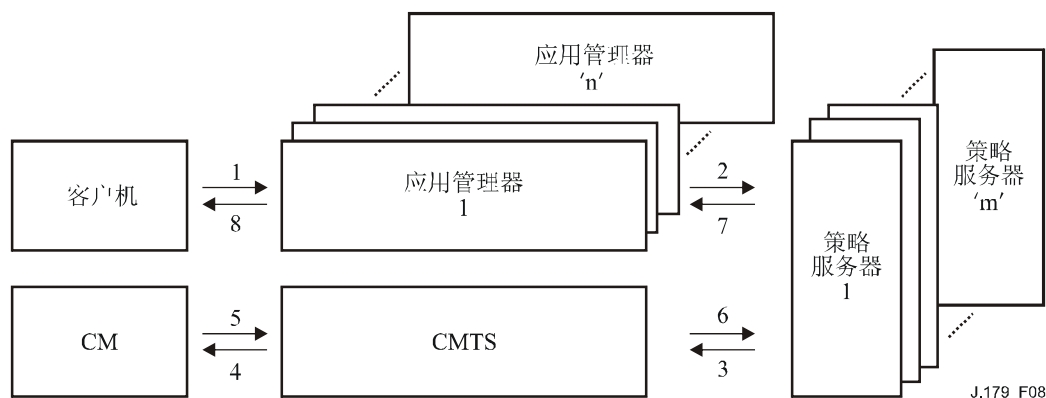


图 8/J.179—基本的消息序列

- 1) 客户机通过应用层信令向应用管理器发出一个会话设置请求。在此步期间，客户机可以向应用管理器验证自己。
- 2) 在应用管理器激活会话之前，应用管理器发出一个 Gate-Set（在 COPS DECISION 消息中），并将之发送给策略服务器，以便确定是否应允许处理会话设置请求。消息包括：
 - i) AMID;
 - ii) SubscriberID;
 - iii) TransactionID;
 - iv) 分类符;
 - v) 流的通信业务简表;
 - vi) 控制门规范。
- 3) 一旦收到请求，策略服务器将依据策略规则对请求进行检查，如果请求得以批准，那么向 CMTS 发送一个 Gate-Set。消息包括：
 - i) AMID;
 - ii) SubscriberID;
 - iii) TransactionID;
 - iv) 分类符;
 - v) 流的通信业务简表（授权的、预留的和提交的）;
 - vi) 控制门规范。
- 4) 通过发出适当的 DOCSIS DSx 消息，CMTS 利用分类符和通信业务简表信息来激活流。
- 5) CM 以适当的 DSx 消息予以确认。
- 6) CMTS 向策略服务器发出一个 Gate-Set-Ack，以响应在第 3 步中收到的 Gate-Set 消息。消息包括：
 - i) AMID;
 - ii) TransactionID;
 - iii) GateID;
 - iv) SubscriberID。

- 7) 在响应策略服务器过程中，将向 AM 产生一个 **Gate-Set-Ack**；它告知 AM：已允许策略请求，可以进行客户机请求，并已预留基础网络中必要的资源。消息包括：
- i) AMID;
 - ii) TransactionID;
 - iii) GateID;
 - iv) SubscriberID。
- 8) 一旦收到 **Gate-Set-Ack**，应用管理器将通知客户机：可以进行会话建立。

10.2 详细的消息序列

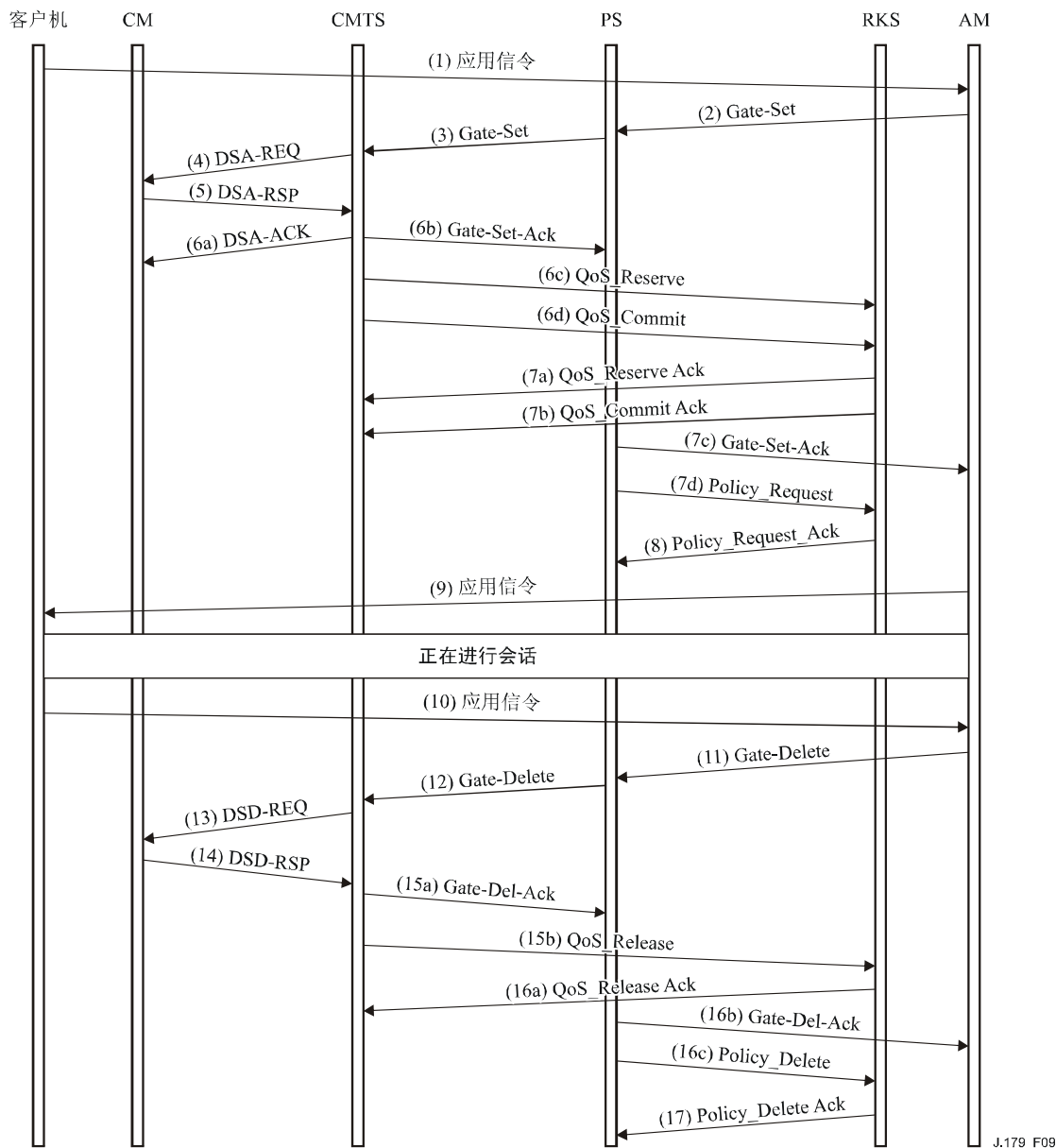


图 9/J.179—详细的消息序列

下面详细描述 IPCablecom 多媒体会话举例中所进行的消息交换。带宽数量纯粹只是用于举例说明，与任何特定业务无关。另外，为了清楚起见，在 DOCSIS 消息中未考虑 BPI 相关的 TLV。

- 1) 通过向应用管理器查询应用所需的资源，客户机对会话进行初始化。有关它的一个例子是基于软件的视频游戏，它请求资源，以便能够进行在线游戏。该信令超出了本建议书的讨论范围。

- 2) 从客户机收到应用信令后，应用管理器向策略服务器发出一个 Gate-Set，请求该会话所需的资源。

0		1	2	3
COPS 报头				
版本 0x1	标志 0x0	操作码 0x02	客户机类型 0x800A	
消息长度 0x00000088				
COPS 句柄对象				
长度 0x0008		C-Num 0x01	C-Type 0x01	
句柄 0x00001234				
COPS 正文对象				
长度 0x0008		C-Num 0x02	C-Type 0x01	
请求类型（R-Type） 0x0008（配置请求）		消息类型（M-Type） 0x0000		
COPS 决策标志对象				
长度 0x0008		C-Num 0x06	C-Type 0x01	
指令代码 0x0001（安装配置）		标志 0x0000		
COPS 决策客户机特定的决策数据对象报头				
长度 0x00A0		C-Num 0x06	C-Type 0x04	
多媒体 TransactionID 对象				
长度 0x0008		S-Num 0x01	S-Type 0x01	
TransactionID 0x9999		控制门指令 0x0004（Gate-Set）		
多媒体 AMID 对象				
长度 0x0008		S-Num 0x02	S-Type 0x01	
AMID 0x00005678				
多媒体 SubscriberID 对象				
长度 0x0008		S-Num 0x03	S-Type 0x01	
SubscriberID 0x01010101				
多媒体 GateSpec 对象				
长度 0x0010		S-Num 0x05	S-Type 0x01	
标志 0x01	DSCP/TOS 字段 0x00		DSCP/TOS 掩码 0x00	SessionClassID 0x00
计时器 T1 0x00C8（200 秒）		计时器 T2 0x012C（300 秒）		
计时器 T3 0x003C（60 秒）		计时器 T4 0x001E（30 秒）		

0	1	2	3
多媒体 FlowSpec 对象			
长度 0x0024		S-Num 0x07	S-Type 0x01
封装 0x07	业务号 0x02	预留	预留
组合的、授权的、预留的和提交的封装			
令牌桶速率 [r] (编码为 IEEE 浮点数) 0x461C4000 (10 000 位/秒)			
令牌桶大小 [b] (编码为 IEEE 浮点数) 0x43480000 (200 字节)			
峰值数据速率 [p] (编码为 IEEE 浮点数) 0x461C4000 (10 000 位/秒)			
最小监管单位 [m] 0x000000C8 (200 字节)			
最大分组大小 [M] 0x000000C8 (200 字节)			
速率 [R] (编码为 IEEE 浮点数) 0x461C4000 (10 000 位/秒)			
空隙期限 [S] 0x00000320 (800 μs)			
多媒体分类符对象			
长度 0x0018		S-Num 0x06	S-Type 0x01
预留	ProtocolID 0x11 (17 UDP)	DSCP/TOS 字段 0x00	DSCP/TOS 掩码 0x00
源 IP 地址 0x01010101			
目的 IP 地址 0x02020202			
源端口 0x1234		目的地端口 0x9876	
优先级 0x0040 (64)		预留	

- 3) PS 从应用管理器收到 Gate-Set 后, 进行检查, 看请求是否已经授权, 如果已经授权, 那么向 CMTS 发送一个 Gate-Set。

0	1	2	3
COPS 报头			
版本 0x1	标志 0x0	操作码 0x02	客户机类型 0x800A
消息长度 0x000000B4			
COPS 句柄对象			
长度 0x0008		C-Num 0x01	C-Type 0x01
处理 0x00005678			
COPS 正文对象			
长度 0x0008		C-Num 0x02	C-Type 0x01
请求类型 (R-Type) 0x0008 (配置请求)		消息类型 (M-Type) 0x0000	

0		1		2		3	
COPS 决策标志对象							
长度 0x0008				C-Num 0x06		C-Type 0x01	
指令代码 0x0001 （安装配置）				标志 0x0000			
COPS 决策客户机特定的决策数据对象报头							
长度 0x00CC				C-Num 0x06		C-Type 0x04	
多媒体 TransactionID 对象							
长度 0x0008				S-Num 0x01		S-Type 0x01	
TransactionID 0x0001				控制门指令 0x0004 （Gate-Set）			
多媒体 AMID 对象							
长度 0x0008				S-Num 0x02		S-Type 0x01	
AMID 0x00005678							
多媒体 SubscriberID 对象							
长度 0x0008				S-Num 0x03		S-Type 0x01	
SubscriberID 0x01010101							
多媒体 GateSpec 对象							
长度 0x0010				S-Num 0x05		S-Type 0x01	
方向 0x01	DSCP/TOS 字段 0x00			DSCP/TOS 掩码 0x00		SessionClassID 0x00	
计时器 T1 0x00C8 （200 秒）				计时器 T2 0x012C （300 秒）			
计时器 T3 0x003C （60 秒）				计时器 T4 0x001E （30 秒）			
多媒体 FlowSpec 对象							
长度 0x0024				S-Num 0x07		S-Type 0x01	
封装 0x07	业务号 0x02			预留		预留	
组合的、授权的、预留的和提交的封装							
令牌桶速率 [r] （编码为 IEEE 浮点数） 0x461C4000 （10 000 位/秒）							
令牌桶大小 [b] （编码为 IEEE 浮点数） 0x43480000 （200 字节）							
峰值数据速率 [p] （编码为 IEEE 浮点数） 0x461C4000 （10 000 位/秒）							
最小监管单位 [m] 0x000000C8 （200 字节）							
最大分组大小 [M] 0x000000C8 （200 字节）							
速率 [R] （编码为 IEEE 浮点数） 0x461C4000 （10 000 位/秒）							
空隙期限 [S] 0x00000320 （800 μs）							

0	1	2	3
多媒体分类符对象			
长度 0x0018		S-Num 0x06	S-Type 0x01
预留	ProtocolID 0x11	DSCP/TOS 字段 0x00	DSCP/TOS 掩码 0x00
源 IP 地址 0x01010101			
目的 IP 地址 0x02020202			
源端口 0x1234		目的地端口 0x9876	
优先级 0x0040 （64）		预留	
多媒体事件产生信息对象			
长度 0x002C		S-Num 0x08	S-Type 0x01
主 RKS 地址 0x03030303			
主 RKS 端口 0x1111		预留	
副 RKS 地址 0x04040404			
副 RKS 端口 0x1111		预留	
BCID 0x3e4812082020202020313436302d30353030300003db77			

- 4) 如果 CMTS 准许进入控制得以成功, 那么 CMTS 将通过向电缆调制解调器发出一个 DSA 来初始化预留和提交接入网络资源。

0	1	2	3
MAC 管理报头			

TransactionID 0x0007		US 业务流 0x18	长度 0x29
业务流 ID 0x02	长度 0x04	值 0x0000	
值 (续) 0001		业务 ID 0x03	长度 0x02
值 0x0001		QoS 参数集 0x06	长度 0x01
值 0x06 (Ad.+Act.)	调度类型 0x0F	长度 0x01	值 0x06
UGS 大小 0x13	长度 0x02	值 0x00E8 (232 字节)	

0	1	2	3
标称的授权间隔 0x14	长度 0x04	值 0x0000	
值（续） 4E20（20 000 μs）		每个间隔的授权 0x16	长度 0x01
值 0x01	RX/TX 策略 0x10	长度 0x04	值 0x00
值（续） 00017F			容许的授权抖动 0x15
长度 0x04	值 0x000003		
值（续） 20（800 μs）	US 分组分类符 0x16	长度 0x0x2B	分类符 ID 0x02
长度 0x02	值 0x0001		业务流 ID 0x04
长度 0x04	值 0x000000		
值（续） 01	规则优先级 0x05	长度 0x01	值 0x40
分类符活动性状态 0x06	长度 0x01	值 0x01（活动的）	IP 分组分类符 0x09
长度 0x001A	IP 协议 0x02	长度 0x02	值 0x00
值（续） 11（17 UDP）	IP 源地址 0x03	长度 0x04	值 0x01
值（续） 010101			IP 源端口开始 0x07
长度 0x02	值 0x1234		IP 源端口结束 0x08
长度 0x02	值 0x1234		IP 目的地端口开始 0x09
长度 0x02	值 0x9876		IP 目的地端口结束 0x0A
长度 0x02	值 0x9876		

5) CM 用一个 DSA-RSP 来响应 CMTS。

0	1	2	3
MAC 管理报头			
.....			
.....			
.....			
.....			
TransactionID 0x0007		确认码 0x00	

6a) CMTS 用一个 DSA-ACK 来结束事务处理。

0	1	2	3
MAC 管理报头			
.....			
.....			
.....			
.....			
TransactionID 0x0007		确认码 0x00	

- 6b) 一旦 CMTS 从 CM 处收到一个 DSA-RSP，确认事务处理获得成功，那么 CMTS 将向策略服务器发送一个 Gate-Set-Ack。

0		1		2		3	
COPS 报头							
版本 0x1		标志 0x1		操作码 0x03		客户机类型 0x800A	
消息长度 0x0000003C							
COPS 句柄对象							
长度 0x0008				C-Num 0x01		C-Type 0x01	
句柄 0x00005678							
COPS 报告类型对象							
长度 0x0008				C-Num 0x12		C-Type 0x01	
报告类型（R-Type） 0x0001 （成功）				预留			
COPS ClientSI 对象报头							
长度 0x0024				C-Num 0x09		C-Type 0x01	
多媒体 TransactionID 对象							
长度 0x0008				S-Num 0x01		S-Type 0x01	
TransactionID 0x0001				控制门指令 0x0005 （Gate-Set-Ack）			
多媒体 AMID 对象							
长度 0x0008				S-Num 0x02		S-Type 0x01	
AMID 0x00005678							
多媒体 SubscriberID 对象							
长度 0x0008				S-Num 0x03		S-Type 0x01	
SubscriberID 0x01010101							
多媒体 GateID 对象							
长度 0x0008				S-Num 0x04		S-Type 0x01	
GateID 0x12345678							

6c) CMTS 还将发送一个 QoS Reserve 事件消息来告知 RKS，已经预留接入网络资源。

[illegible]

7a) 在收到和记录 QoS_Reserve 事件消息后，RKS 对消息予以确认。

0	1	2	3
结算响应 Radius 报头			

7b) 在收到和记录 QoS_Commit 事件消息后，RKS 对消息予以确认。

0	1	2	3
结算响应 Radius 报头			

7c) 从 CMTS 处收到 Gate-Set-Ack 后，CMTS 将向应用服务器发送一个 Gate-Set-Ack 来结束事务处理。

0		1		2		3	
COPS 报头							
版本 0x1		标志 0x1		操作码 0x03		客户机类型 0x800A	
消息长度 0x0000003C							
COPS 句柄对象							
长度 0x0008				C-Num 0x01		C-Type 0x01	
句柄 0x00001234							
COPS Report-Type 对象							
长度 0x0008				C-Num 0x12		C-Type 0x01	
报告类型（R-Type） 0x0001 （成功）				预留			
COPS ClientSI 对象报头							
长度 0x0024				C-Num 0x09		C-Type 0x01	
多媒体 TransactionID 对象							
长度 0x0008				S-Num 0x01		S-Type 0x01	
TransactionID 0x9999				控制门指令 0x0005			
多媒体 AMID 对象							
长度 0x0008				S-Num 0x02		S-Type 0x01	
AMID 0x00005678							
多媒体 SubscriberID 对象							
长度 0x0008				S-Num 0x03		S-Type 0x01	
SubscriberID 0x01010101							

0	1	2	3
多媒体 GateID 对象			
长度 0x0008		S-Num 0x04	S-Type 0x01
GateID 0x12345678			

7d) 策略服务器还将向 RKS 发送一个 Policy_Request 事件消息，以跟踪策略请求和相关的结果。

0	1	2	3
结算请求 Radius 报头			

Radius 供货商规范 0x1A	长度 0x54	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 （EM 报头） 0x01	长度 0x4E
版本 0x0001		BCID 0x3E48	
BCID （续） 120820202020313436302D3035303030300003DB77			

		事件消息类型 0x0015 （Policy_Request）	
元素类型 0x0004 （策略服务器）		元素 ID 0x2020202035363738	

		时区 0x302E303530303030	

		序列号 0x0000	
序列号 （续） 0001		事件时间 0x3230	
事件时间 （续） 3033313230363030303030302E323130			

状态 0x00000000			
优先级 0x80 （128）	属性计数 0x0004		事件对象 0x00
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x3D	长度 0x06
Application_Manager_ID 0x00005678			
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	

0	1	2	3
供货商 ID （续） 118B		类型 0x34	长度 0x06
Subscriber_ID 0x01010101			
Radius 供货商规范 0x1A	长度 0x0A	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x3C	长度 0x04
Policy_Decision_Status 0x0001 （批准的策略）		Radius 供货商规范 0x1A	长度 0x1C
供货商 ID 0x0000118B			
类型 0x31	长度 0x16	FEID 0x0000	
FEID （续） 000000000000005061636B65744361626C65			

8) 在收到和记录 Policy_Request 事件消息后, RKS 对消息予以确认。

0	1	2	3
结算请求 Radius 报头			

9) 应用管理器将对客户机做出答复, 以告知客户机它现在可以玩游戏。该信令超出了本建议书的讨论范围。

10) 当客户机完成应用时, 它将通知应用管理器。该信令超出了本建议书的讨论范围。

11) 应用管理器将通过向策略服务器发送一个 Gate-Delete 来结束会话。

0	1	2	3
COPS 报头			
版本 0x1	标志 0x0	操作码 0x02	客户机类型 0x800A
消息长度 0x00000044			
COPS 句柄对象			
长度 0x0008		C-Num 0x01	C-Type 0x01
句柄 0x00001234			
COPS 正文对象			
长度 0x0008		C-Num 0x02	C-Type 0x01
请求类型 (R-Type) 0x0008 (配置请求)		消息类型 (M-Type) 0x0000	

0	1	2	3
COPS 决策标志对象			
长度 0x0008	C-Num 0x06	C-Type 0x01	
指令代码 0x0001 （安装配置）	标志 0x0000		
COPS 决策客户机特定的决策数据对象报头			
长度 0x0014	C-Num 0x06	C-Type 0x04	
多媒体 TransactionID 对象			
长度 0x0008	S-Num 0x01	S-Type 0x01	
TransactionID 0x9998	控制门指令 0x000A （Gate-Delete）		
多媒体 AMID 对象			
长度 0x0008	S-Num 0x02	S-Type 0x01	
AMID 0x00005678			
多媒体 SubscriberID 对象			
长度 0x0008	S-Num 0x03	S-Type 0x01	
SubscriberID 0x01010101			
多媒体 GateID 对象			
长度 0x0008	S-Num 0x04	S-Type 0x01	
GateID 0x12345678			

12) 策略服务器将通过发送一个 Gate-Delete 来指导 CMTS 拆卸会话。

0		1		2		3	
COPS 报头							
版本 0x1		标志 0x0		操作码 0x02		客户机类型 0x800A	
消息长度 0x00000044							
COPS 句柄对象							
长度 0x0008				C-Num 0x01		C-Type 0x01	
句柄 0x00005678							
COPS 正文对象							
长度 0x0008				C-Num 0x02		C-Type 0x01	
请求类型（R-Type） 0x0008 （配置请求）				消息类型（M-Type） 0x0000			
COPS 决策标志对象							
长度 0x0008				C-Num 0x06		C-Type 0x01	
指令代码 0x0001 （安装配置）				标志 0x0000			
COPS 决策客户机特定的决策数据对象报头							
长度 0x0014				C-Num 0x09		C-Type 0x01	

0	1	2	3
多媒体 TransactionID 对象			
长度 0x0008	S-Num 0x01		S-Type 0x01
TransactionID 0x0002	控制门指令 0x000A （Gate-Delete）		
多媒体 AMID 对象			
长度 0x0008	S-Num 0x02		S-Type 0x01
AMID 0x00005678			
多媒体 SubscriberID 对象			
长度 0x0008	S-Num 0x03		S-Type 0x01
SubscriberID 0x01010101			
多媒体 GateID 对象			
长度 0x0008	S-Num 0x04		S-Type 0x01
GateID 0x12345678			

13) CMTS 将通过向 CM 发送一个 DSD-REQ 来拆卸接入网络资源。

0	1	2	3
MAC 管理报头			

TransactionID 0x0008		预留	
SFID 0x00000001			

14) CM 将用一个 DSD-RSP 来确认会话删除。

0	1	2	3
MAC 管理报头			

TransactionID 0x0008		确认码 0x00	预留

15a) CMTS 将用一个 Gate-Delete-Ack 来结束 Gate-Control 事务处理。

0	1	2	3
COPS 报头			
版本 0x1	标志 0x1	操作码 0x03	客户机类型 0x800A
消息长度 0x00000034			

0	1	2	3
COPS 句柄对象			
长度 0x0008	C-Num 0x01	C-Type 0x01	
句柄 0x00005678			
COPS 报告类型对象			
长度 0x0008	C-Num 0x12	C-Type 0x01	
报告类型（R-Type） 0x0001	预留		
COPS ClientSI 对象报头			
长度 0x001C	C-Num 0x09	C-Type 0x01	
多媒体 TransactionID 对象			
长度 0x0008	S-Num 0x01	S-Type 0x01	
TransactionID 0x0002	控制门指令 0x000B （Gate-Delete-Ack）		
多媒体 AMID 对象			
长度 0x0008	S-Num 0x02	S-Type 0x01	
AMID 0x00005678			
多媒体 GateID 对象			
长度 0x0008	S-Num 0x04	S-Type 0x01	
GateID 0x12345678			

15b) 一旦收到 DSD-RSP, CMTS 还将告知 RKS, 接入网络资源已通过发送一个 QoS_Release 而得以释放。

0	1	2	3
结算请求 Radius 报头			

Radius 供货商规范 0x1A	长度 0x54	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 （EM 报头） 0x01	长度 0x4E
版本 0x0001		BCID 0x3E48	
BCID （续）			
12082020202020313436302D3035303030300003DB77			

		事件消息类型 0x0008 （QoS Release）	

0	1	2	3
元素类型 0x0002 （CMTS）		元素 ID 0x2020202031323334	
		时区 0x302D303530303030	
		序列号 0x0000	
序列号 （续） 0003		事件时间 0x3230	
事件时间 （续） 30323132303630303030302E333030			
状态 0x00000000			
优先级 0x80 （128）	属性计数 0x0005		事件对象 0x00
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x1E	长度 0x06
SF_ID 0x00000001			
Radius 供货商规范 0x1A	长度 0x0A	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x32	长度 0x04
流方向 0x0001 （上行流）		Radius 供货商规范 0x1A	长度 0x0A
供货商 ID 0x0000118B			
Type 0x38	长度 0x04	QoS_Release_Reason 0x0001 （通过 PS 关闭控制门）	
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		Type 0x36	长度 0x06
QoS_Usage_Info 0x77777777 （字节）			
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x3F	长度 0x06
QoS_Time_Info 0x77777777 （秒）			

16a) 在收到和记录 QoS_Release 事件消息后, RKS 对消息予以确认。

0	1	2	3
结算响应 Radius 报头			

16b) 在从 CMTS 收到和记录 Gate-Delete-Ack 后, 策略服务器将发送一个 Gate-Delete-Ack, 以结束 Gate-Control 处理。

0		1		2		3	
COPS 报头							
版本 0x1	标志 0x1	操作码 0x03		客户机类型 0x800A			
消息长度 0x00000034							
COPS 句柄对象							
长度 0x0008				C-Num 0x01		C-Type 0x01	
句柄 0x00001234							
COPS 报告类型对象							
长度 0x0008				C-Num 0x12		C-Type 0x01	
报告类型（R-Type） 0x0001 （成功）				预留			
COPS ClientSI 对象报头							
长度 0x001C				C-Num 0x09		C-Type 0x01	
多媒体 TransactionID 对象							
长度 0x0008				S-Num 0x01		S-Type 0x01	
TransactionID 0x9998				控制门指令 0x000B （Gate-Delete-Ack）			
多媒体 AMID 对象							
长度 0x0008				S-Num 0x02		S-Type 0x01	
AMID 0x00005678							
多媒体 GateID 对象							
长度 0x0008				S-Num 0x04		S-Type 0x01	
GateID 0x12345678							

16c) 策略服务器向 RKS 发送一个 Policy_Delete 事件消息, 以结束整个过程。

0		1		2		3	
结算请求 Radius 报头							

Radius 供货商规范 0x1A		长度 0x54		供货商 ID 0x0000			
供货商 ID （续） 118B				类型 （EM 报头） 0x01		长度 0x4E	
版本 0x0001				BCID 0x3E48			

0	1	2	3
BCID （续） 12082020202020313436302D3035303030300003DB77			
		事件消息类型 0x0016 （Policy_Delete）	
元素类型 0x0004 （策略服务器）		元素 ID 0x2020202035363738	
		时区 0x302D303530303030	
		序列号 0x0000	
序列号 （续） 0002		事件时间 0x3230	
事件时间 （续） 30323132303630303030302E343030			
状态 0x00000000			
优先级 0x80	属性计数 0x0004		事件对象 0x00
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x3D	长度 0x06
Application_Manager_ID 0x00005678			
Radius 供货商规范 0x1A	长度 0x0C	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x34	长度 0x06
Subscriber_ID 0x01010101			
Radius 供货商规范 0x1A	长度 0x0A	供货商 ID 0x0000	
供货商 ID （续） 118B		类型 0x3A	长度 0x04
Policy_Deleted_Reason 0x0001 （应用管理器请求）		Radius 供货商规范 0x1A	长度 0x1C
供货商 ID 0x0000118B			
类型 0x31	长度 0x16	FEID 0x0000	
FEID （续） 000000000000005061636B65744361626C65			

17) 在收到和记录 Policy_Delete 事件消息后，RKS 对消息予以确认。

0	1	2	3
结算响应 Radius 报头			

11 有待今后研究的问题

确定以下问题是有待今后研究的主题：

- 错误处理要求（即对特定的条件需要特定的错误代码）。
- 多媒体框架内的控制门控制消息路由选择。
- 状态同步要求（即粒度、范围、频率等）和协议机制。
- 对故障和冗余策略的协议支持，以及在 COPS 连接出现故障的情况下应如何处置控制门。
- 策略服务器规则格式和供应机制：带多媒体特定的 XML DTD 的 CMS 供应。
- 对负载报头压缩（PHS）的支持。
- 对故障连接的控制门控制消息提交（当前这些消息是经过压缩的）。

附录一

背景信息

I.1 引言

本附录描述这样一种体系结构，它提供一个基于 IP 的平台，以支持多种多媒体应用和服务，这些应用和服务要求在 CableModem 接入网络上对 QoS 进行处理。该体系结构定义了功能部件和协议接口，它们将使各个电缆运营商能够交付 QoS 增强型多媒体服务，以满足其独特的商业需求。

由于尚不清楚该体系结构有关特殊多媒体产品的、应用级的详细情况，因此提供特殊服务所需的特定供应、信令和操作支持系统（OSS）功能等超出了本建议书的讨论范围。更确切地说，IPCablecom 多媒体重点关注的是在接入网络上提供可靠的 QoS，尤其是解决策略授权、QoS 信令、资源结算和安全性的技术问题。

I.1.1 IPCablecom概述

IPCablecom 项目旨在定义由供货商团体使用的接口规范，以开发可互操作的设备，这种设备能够在符合 CableModem 宽带接入网络建议书要求的光纤同轴电缆混合（HFC）电缆系统上提供基于 IP 的音频、视频和其它高速多媒体服务。

IP 电话（VoIP）是第一种确定在 IPCablecom 平台上交付的此类服务。当前的 IPCablecom 建议书集，即众所周知的 IPCablecom-T，定义了为交付住宅 VoIP 服务而进行了优化的 IPCablecom 体系结构。请参见 ITU-T J.160 建议书。

I.1.2 IPCablecom多媒体的意图

如同 VoIP，大多数流行的多媒体应用（如在线游戏、流媒体、实时视频通信）都对网络内的传输延时敏感。此外，随着旨在利用宽带网络优势的新的应用不断涌现，它们也将提出独特的带宽和等待时间要求。

当前，宽带用户通过尽力服务数据传输来接收多媒体服务。这导致在线体验的不一致，其质量因网络中带宽可用性和拥塞程度的不同而不同。能够根据服务需求指令预留资源和提供带宽的网络，将使自己能够很好地为其客户提供众多的新的服务。

为了解决 VoIP 服务的这些需求，目前，IPCablecom 定义了动态服务质量（DQoS）信令机制，允许应用从 CableModem 数据链路层处请求和获得带宽。当前的 DQoS 框架还通过端点认证与授权以及一种基于 QoS 的使用跟踪模型，来支持建立可靠的会话。基于这些核心性能，IPCablecom 体系结构可以更好地支持电话业务之外的、当前和未来的 QoS 增强型应用和服务。

IPCablecom 多媒体的首要目标是定义支持基于 QoS 的多媒体应用所需的核心体系结构框架。该框架的中心是在 CableModem 和 IPCablecom DQoS 规范中定义的服务质量机制。成功完成这一倡议将为支持正在发展中的特殊多媒体服务产品提供强大的技术基础。

I.2 IPCablecom多媒体的目标和范围

IPCablecom 多媒体的主要目标是开发多用途的体系结构，该体系结构：

- 支持众多的、语音服务之外的、具有 QoS 功能的服务；
- 基于 IPCablecom-T 和 CableModem 建议书中所定义的现有机制；
- 需要一个超出 IPCablecom-T 的最小扩展组；
- 通过消除不适用的、电话特定的要求（如 PSTN 互连、电子监视、电话记账模型等），简化开发复杂性；
- 以这样一种方式与 IPCablecom-T 体系结构共存，即：
 - IPCablecom 多媒体要求足以支持基于 QoS 的多媒体服务交付平台；
 - IPCablecom 多媒体要求可增加到相应的现有 IPCablecom-T 功能部件上；
 - IPCablecom-T 要求可增加到相应的 IPCablecom 多媒体功能部件上；
- 如“第 2 类客户机”设备（在体系结构内定义）那样，在 IPCablecom 多媒体体系结构中支持 IPCablecom-T MTA；
- 与 IPCable2Home（ITU-T J.191 建议书）和 CableModem（ITU-T J.112 和 J.122 建议书）体系结构相互操作。

本节描述为满足以上目标而确定的要求，并概述可以由体系结构解决的工作范围。

I.2.1 要求

该体系结构对众多网络元素的相互作用做了概述，包括客户机设备、应用管理器、策略服务器、CMTS 和电缆调制解调器。在本附录的多媒体框架条款中，对这些网络元素做了正式定义。不过，对这些网络元素中的某些元素，在管理权威部门和信任关系方面做了特定的假设，作为 IPCablecom 多媒体的需求，可以在下面获得这些假设。本节还包括用于解决 QoS 信令、资源管理、事件消息发布和安全性等问题的高级要求。

IPCablecom 多媒体是发送协议尚未明确的、有关客户机设备与应用管理器之间相互作用的应用。可以理解为客户机设备和应用管理器可以支持众多应用和信令协议（如 HTTP、SIP、H.323、DCS、NCS 等）。

在 IPCablecom 多媒体体系结构中，客户机设备：

- 1) 直接驻留于运营商接入网络中或家庭网络内；
- 2) 可以是单独的设备，或可以包含一个嵌入式 CableModem；并且
- 3) 可以认为是非信任的网络元素，这样，运营商网络可要求提供某种形式的用户认证、申请或应用消息发布。

在 IPCablecom 多媒体体系结构中，应用管理器：

- 1) 驻留于运营商管理的网络中；
- 2) 由运营商管理；并且
- 3) 负责确保客户机请求的、来自运营商网络的服务获得授权，以便接收该服务。

在 IPCablecom 多媒体体系结构中，策略服务器：

- 1) 驻留于运营商管理的网络中；
- 2) 由运营商管理；并且
- 3) 负责根据运营商定义的策略规则，做出 QoS 相关的策略决定。

IPCablecom 多媒体体系结构中的 CMTS 负责执行 QoS 相关的策略决定。

QoS 信令和资源管理要求：

- 务必定义动态资源请求机制，包括：
 - 使用所有的 CableModemQoS 调度模型；
 - 受时间限制的资源请求；
 - 受容量限制的资源请求。
- 务必支持单阶段和两阶段的资源预留模型；
- 务必支持单向预留；应允许支持双向预留；
- 应用管理器可代表客户机设备提出 QoS 预留请求；
- 体系结构务必提供一种用于检测与资源相关的、客户机与/或服务器故障和回收的方法。

事件消息信息收集要求：

- 务必定义一个全面的事件消息集，以跟踪每个流资源的使用情况，包括：
 - 表示接入网络资源请求的策略事件，服从于运营商定义的策略规则；
 - 表示接入网络资源释放的策略事件；
 - 表示预留、提交和释放 QoS 资源的 QoS 事件；
 - 基于容量（测量的分组数量）支持每个流资源使用情况的其它事件。
- 消息中应包含下列信息：
 - 请求源（如订户或服务提供商）；
 - 所请求资源的特性；
 - 策略授权决定。

安全性要求：

- 务必为相关接口要求和定义安全性；
- 发起 QoS 信令的客户机可要求提供某种形式的用户或应用认证。

1.2.2 范围

下列条目概述了 IPCablecom 多媒体倡议当前的、最初阶段的范围：

- 体系结构将论及网络元素，它们驻留在：
 - 1) 接入网络上；或
 - 2) 在一个单独的运营商管理的 IP 网络内。

- 体系结构将定义支持策略授权、QoS 准许进入控制、资源结算和安全性机制所需的协议与接口；
- 体系结构将不论及应用特定的问题（如服务提供、信令、记账等）；
- 体系结构将不论及有关 IPCablecom 多媒体网络元素的供应和 OSS 需求问题；
- 体系结构将主要关注 CMTS 与 CM 之间的 QoS 管理问题；
- 即使不明确论及多播问题，体系结构也将不排除提交多播服务；
- 当前，体系结构将不解决网络地址转换（NAT）穿越和互操作需求问题；
- 在当前阶段，体系结构将不定义端到端的 QoS 需求；
- 在当前阶段，体系结构将为“第 1 类客户机”和“情形 1”（如体系结构内所定义）提供支持。为了完善和预计未来的细节，本附录对所有三种类型的客户机和三种服务情形进行描述；
- 在当前阶段，体系结构将不提供动态拓扑发现（即应用管理器、策略服务器、CMTS 与 RKS 等之间的关系）；
- 体系结构将不解决由应用管理器进行客户机认证的问题；
- 体系结构将不解决特殊的机制，通过这些机制，策略服务器获得和管理策略规则；
- 体系结构将不支持为溶入资源使用审计跟踪中而收集应用或服务特定的事件。

I.3 IPCablecom 多媒体的框架

为了有利于提交要求 QoS 担保的高质量宽带多媒体应用，多媒体框架提供了基于核心 IPCablecom-T 规范中定义之机制的多用途 QoS 功能。为支持这一目标，确定和简要介绍了若干关键的网路元素。图 I.1 描述了驻留于运营商管理的 IP 网络内的 IPCablecom 多媒体部件。

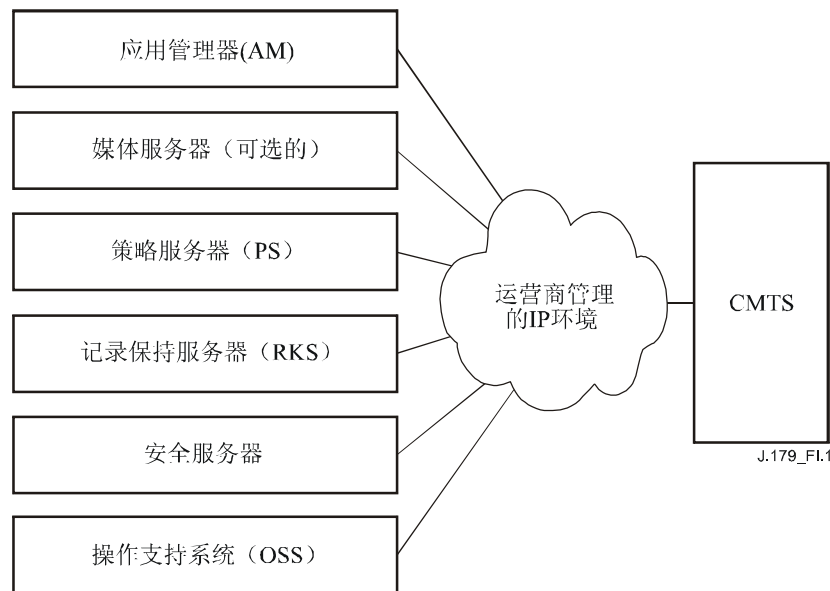


图 I.1/J.179—运营商多媒体网络元素

除了增强基于参数的 QoS 性能的 CMTS，运营商多媒体网络体系结构由一个服务器群组成，它可进一步划分为以下领域：

- 应用管理器和（可选的）媒体服务器，作为具有 QoS 功能的应用的主机；
- 提供 QoS 授权和准许进入控制的策略管理框架，支持每个流的网络资源管理；
- 用于监控和记录资源使用信息的事件消息子系统。

用于执行供应、网络管理和监控功能的操作支持系统也可以包括在运营商多媒体网络配置中，尽管这些元素超出了当前体系结构的范围。

I.3.1 IPCablecom多媒体体系结构参考模型

除了驻留于运营商头端网络内的各元素，为了完善该模型，还定义了许多部署于客户住宅内的客户机设备。图 I.2 显示了 IPCablecom 多媒体体系结构框架，并确定了部件之间的关键接口。这些接口都已贴上了标识符，将在之后的讨论中被引用。

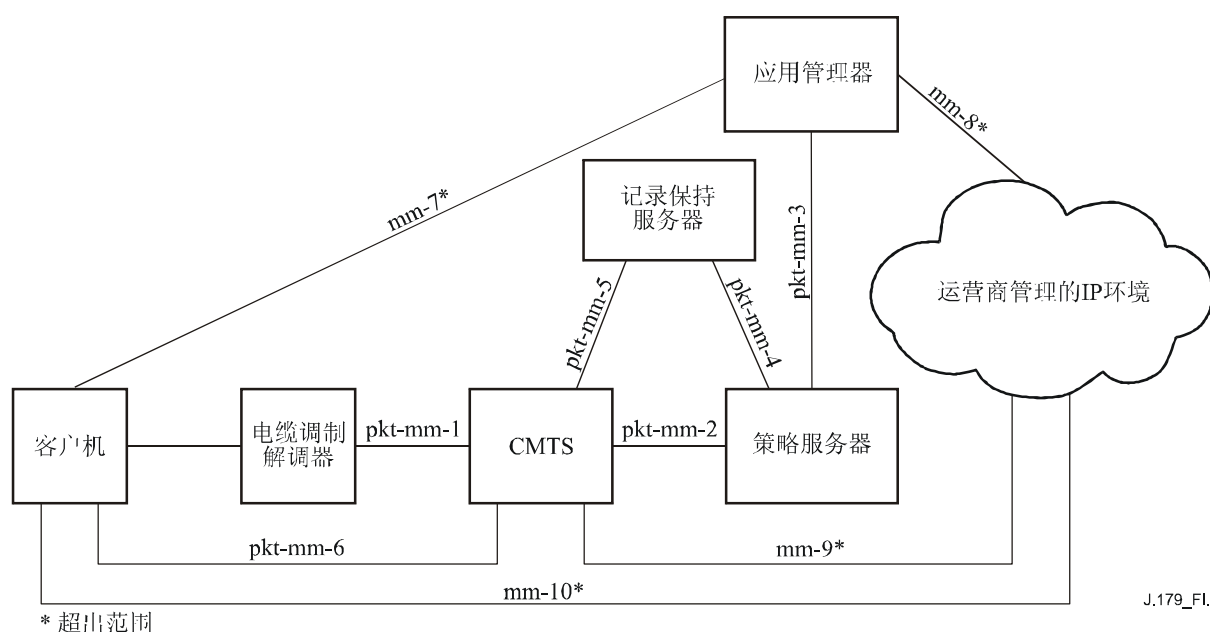


图 I.2/J.179—IPCablecom多媒体体系结构框架

在该体系结构中，客户机可以支持或不支持 IPCablecom 多媒体框架。支持框架的客户机及其 QoS 信令机制代表它们自己对网络资源明确地提出请求，这些网络资源在头端由策略服务器进行授权。不支持 QoS 信令机制的客户机由应用管理器代表它们提出代理的网络资源请求，并与这种请求进行交互。

无论采用何种 QoS 信令方法，接入网络资源请求总是受制于策略控制，策略控制在电缆调制解调器终端系统（CMTS）中执行，作为策略执行点（PEP），并在策略服务器（PS）中加以定义，作为策略决定点（PDP）。

- 策略决定可以由 CMTS 从策略服务器处拉动。在这种情况下，CMPS 一般发出一个策略请求，作为当前未授权但服从 QoS 资源请求的结果。基于作为结果的决定，服务或拒绝最初的 QoS 请求。

- 可选地，策略决定可以由策略服务器推送至 CMTS。在这种情况下，策略服务器应在 QoS 资源请求之前安装一个策略决定，它基于来自应用管理器的策略请求。基于客户机相互作用（通过某种未做详细说明的信令机制），应用管理器产生这样一个策略请求。

策略服务器和 CMTS 都产生事件消息，以跟踪 QoS 请求和使用情况。这些事件消息发送给记录保持服务器（RKS），在 RKS 中，这些事件消息可用于记账或其它结算目的。

表 I.1 概述了图 I.2 中所示的接口。本建议书定义的接口都贴有“pkt-mm-x”标签，那些出于完善之目的而包括在内的其它接口，都贴有“mm-x”标签。

表 I.1/J.179—IP Cablecom 多媒体接口

接 口	描 述	注 释
pkt-mm-1	CMTS – CM	CM 可以通过 CableModem DSx 信令向 CMTS 请求 QoS。可选地，CMTS 可以再次通过 DSx 信令，指导电缆调制解调器（CM）建立、拆卸或更改一个 CableModem 业务流，以满足 QoS 请求。
pkt-mm-2	PS – CMTS	该接口是策略管理框架的基础。它控制着策略决定，它可以： a) 通过策略服务器（PS）推送至 CMTS；或者 b) 由 CMTS 拉自 PS。 该接口还允许代表客户机提出代理的 QoS 请求。 在某些情形下，该接口还可以用于告知 PS 何时 QoS 资源变得不活动。
pkt-mm-3	AM – PS	应用管理器（AM）可以请求 PS 在 CMTS 上安装一个策略。此外，AM 还可以请求 PS 代理 QoS 代表客户机向 CMTS 提出请求。 该接口还可用于告知 AM 有关 QoS 资源的变化情况。
pkt-mm-4	PS – RKS	PS 向记录保持服务器（RKS）发送事件消息，以跟踪与 QoS 相关的策略决定情况。
pkt-mm-5	CMTS – RKS	CMTS 发送 RKS 事件消息，以跟踪 QoS 请求和使用情况（如业务流增加、更改、删除和容量度量）。
pkt-mm-6	客户机 – CMTS	客户机可以使用该接口来直接请求和管理 QoS 网络资源。如果得到授权，那么这些资源将由 CMTS 提供。
mm-7	客户机 – AM	客户机可以用该接口来与 AM 进行交互，并间接请求和管理 QoS 资源。该接口超出了本附录的讨论范围。

表 I.1/J.179—IPCablecom多媒体接口

接 口	描 述	注 释
mm-8	AM – 对等	AM 可以用该接口来与其它一些实体进行交互，这些实体是所议应用的一部分。该接口超出了本附录的讨论范围。
mm-9	CMTS – 运营商管理的 IP 网络	CMTS 上的该接口可以用于支持接入网络之外的端到端 QoS 请求。该接口超出了本附录的讨论范围。
mm-10	客户机 – 对等	客户机可以用该接口来与其它一些实体进行交互，这些实体是所议应用的一部分。该接口超出了本附录的讨论范围。

I.3.2 多媒体部件

在本节中，我们进一步扩充了之前有关体系结构框架的讨论，为每个网络元素提供了更多的详细内容。

I.3.2.1 客户机

多媒体客户机是一个可发送或接收数据的逻辑实体。IPCablecom 多媒体定义了三种不同类型的客户机，它们的区别在于客户机怎样发送 QoS 信号，以及怎样在 CMTS 中安装与 QoS 相关的策略决定。

第 1 类客户机代表现有的“传统”端点（如个人电脑应用程序、游戏控制台），它们缺少特定的 QoS 意识或信令能力。此类客户机不了解任何 CableModem、IPCable2Home 或 IPCablecom 消息发布，因此无法对其提出任何相关的要求。此类客户机可以包括：从简单的模拟音频与视频演示设备，到复杂的网络化外部设备与消费类电子设备，如机顶盒或游戏控制台。此类客户机与应用管理器进行通信，以请求服务，但不直接向运营商接入网络请求 QoS 资源。

第 2 类客户机类似于一个 IPCablecom-T 电话 MTA，它支持基于 IPCablecom DQoS 的 QoS 信令。此类客户机了解 IPCablecom 多媒体 QoS，并与应用管理器进行通信，以请求服务并获得一个有关接入网络资源的令牌。然后，当向接入网络请求 QoS 资源时，客户机提交该令牌（pkt-mm-1、pkt-mm-6）。

第 3 类客户机依据 RSVP 请求 QoS，而无须应用服务器的交互。此类客户机了解基于 IETF 标准的 RSVP，并利用该协议向直接来自 CMTS 的接入网络请求 QoS 资源。

I.3.2.2 策略服务器

IPCablecom 多媒体倡议的策略管理框架基于 IETF 资源分配协议(RAP)工作组的工作成果。如 RFC 2753 中所定义和描述的那样，策略服务器（PS）网络元素执行运营商定义的授权和资源管理程序。除了所请求资源的参数和可用资源的状况，策略决定可以涉及客户机身份和相关的简表信息、应用参数、安全性因素、时间等。另外，特殊运营商可选择部署多个策略服务器，并在这些服务器中委托某些策略决定，以便满足可量测性和容错性的要求。

策略服务器的主要功能包括：

- 由应用管理器（pkt-mm-3，推动模型）或 CMTS（pkt-mm-2，拉动模型）调用的策略决定请求机制；

- 用于在 CMTS (pkt-mm-2) 上安装策略决定的策略决定提交机制;
- 允许代表应用管理器 (为那些不具备固有 QoS 信令性能的客户机) 向 CMTS 委托 QoS 管理消息的机制;
- 用于记录策略请求的、与记录保持服务器 (pkt-mm-4) 的事件记录接口, 它还可以与网络资源使用记录相关联。

策略服务器可以支持两种不同的模型, 以便在 CMTS 上安装策略决定:

- 在 QoS 预留请求抵达 CMTS 之前, 策略服务器可以在 CMTS 上安装 (推动) 一个策略决定。
- 当 QoS 预留请求抵达 CMTS 之时, CMTS 可以从策略服务器处请求 (拉动) 一个策略决定。

策略规则可以包含下列信息:

- 由策略服务器授权的、用于定义资源的规则:
 - 每个服务;
 - 每个订户;
 - (使用令牌桶参数规定的) 带宽;
 - 等待时间保证;
 - 策略终止时间;
 - 策略容量限制。
- 根据时间定义可量测性/带宽值的规则;
- 抢占式规则。

根据“推动”情形, 策略服务器务必至少执行下列功能:

- 认证和校验来自应用管理器的策略消息;
- 根据运营商定义的规则处理策略消息;
- 决定 CMTS 的确切身份, 该 CMTS 是策略的推动目的地;
- 策略决定和其它消息安全地与 CMTS 进行通信;
- 向 RKS 发送跟踪这些请求的事件消息。

根据“拉动”情形, 策略服务器务必至少执行下列功能:

- 如果服务中涉及应用管理器, 那么认证和校验来自应用管理器的策略消息;
- 策略决定和其它消息安全地与 CMTS 进行通信;
- 根据运营商定义的规则处理策略消息;
- 向 RKS 发送跟踪这些请求的事件消息。

策略服务器可以执行下列附加功能:

- 根据内部保持的状态信息 (如计时器) 跟踪资源使用情况;
- 根据每个用户、每个服务或二者的综合, 对授权的资源进行跟踪。

I.3.2.3 电缆调制解调器终端系统

如 CableModem 建议书中所定义的那样, IPCablecom 多媒体提供了对全套 CMTS 上行流调度算法的使用。尤其是, 体系结构定义了 IPCablecom 多媒体“通信业务简表”, 它提供了一个提取自相关 CableModem 调度类型 (UGS、UGS/AD 等) 的层。此外, 在 IPCablecom-T DQoS 规范中发现的、电话特定的特征和假设将得到普及, 以提供能够由多种类型客户机和应用使用的 QoS 基础设施。

为管理接入网络资源，CMTS 既支持单阶段预留模型，也支持两阶段预留模型。在两阶段模型中，首先预留接入网络资源，然后在之后当需要使用它们时予以提交。CMTS 还支持单阶段预留模型，在该模型中，为立即交付使用，可同时预留和提交接入网络资源。

通过 pkt-mm-1, CMTS 在 CableModem 接入网络上建立相应的服务流。为了预留和使用 QoS 资源, CMTS 通过 pkt-mm-5 接口标识符向记录保持服务器发送事件消息。最后, CMTS 对基于 QoS 的服务流实施监控, 并将之解释为 CableModem 建议书 (可选的) 结算管理子系统中所定义的那样。

I.3.2.4 应用管理器

应用管理器发挥协调作用, 涉及应用信令、语义以及与 IPCablecom 多媒体策略框架的交互, 如先前的策略服务器元素讨论中所述的那样。注意, 应用管理器可以共同成为媒体服务器的主机, 或者, 根据一个分开的模型, 两个元素可以单独存在。

通过 mm-7, 应用管理器与客户机实现接口。基于它对特殊服务产品的认识, 应用管理器务必推断或定义向第 1 类客户机提交服务所需的、特殊的 QoS 参数。一旦确定该信息, 则应用管理器通过 pkt-mm-3 向策略服务器发送一个策略请求。如果需要的话, 应用管理器可以使用 mm-8 来与媒体服务器保持同步。

第 2 类客户机也与应用管理器相互作用, 并通过 mm-7 与服务请求信息进行通信。应用管理器务必再次推断向第 2 类客户机提交服务所需的 QoS 参数。应用管理器通过 pkt-mm-3 向策略服务器发送一个策略请求。一旦成功授权, 应用管理器自策略服务器接收一个令牌, 并通过 mm-7 将该令牌发送给客户机。如果需要的话, 应用管理器可以使用 mm-8 来与媒体服务器保持同步。

尽管在复杂的服务提交情形中存在应用管理器的可能性十分大, 第 3 类客户机并不需要一个应用管理器。

I.3.2.5 记录保持服务器

记录保持服务器 (RKS) 接收指明接入网络 QoS 资源使用情况的事件消息。RKS 与策略服务器 (pkt-mm-4) 和 CMTS (pkt-mm-5) 实现接口。RKS 并不接收直接来自应用管理器的、应用特定的信息。相反地, 应用特定的信息可以包括在一个事件消息中, 作为从应用管理器发送到策略服务器的不透明数据, 并嵌入于发送到 RKS 的策略请求事件消息中。

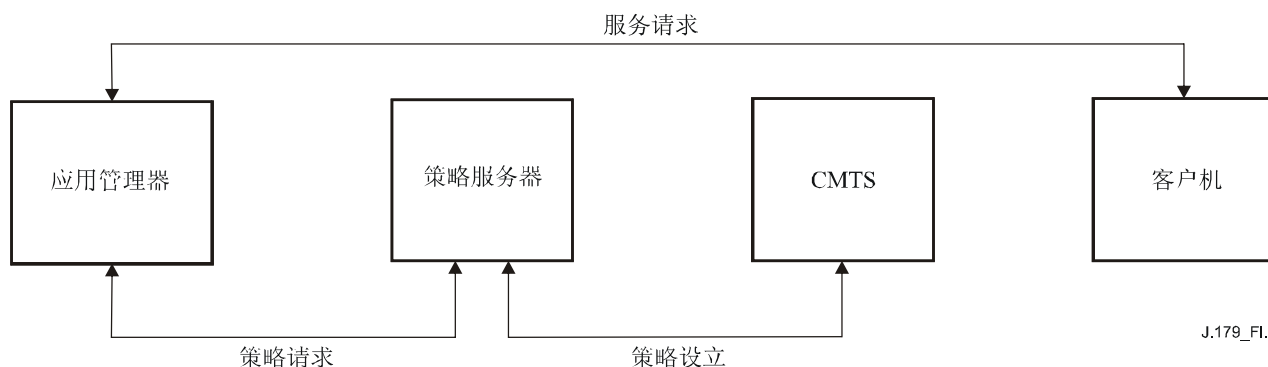
I.4 带策略推动的、代理的 QoS (情形1)

如上所述, 为支持三种客户机类型, 确定了三种体系结构情形。“带策略推动的、代理的 QoS” 授权模型 (情形 1) 支持第 1 类客户机, 它本身并不支持固有的 QoS 信令机制。图 I.3 显示了此情形所涉及的、对元素互动所做的高级概述。

通过向应用管理器发送一个“服务请求”, 客户机请求应用特定的服务。一旦收到该请求, 应用管理器将确定所请求服务的 QoS 需求, 并向策略服务器发送一个“策略请求”。对照运营商定义的策略规则, 策略服务器依次验证“策略请求”, 如果确定决定是肯定的, 那么向 CMTS 发送一个“策略集”消息。CMTS 在所请求的 QoS 封装上执行准许进入控制 (校验相应的资源是否可用, 以满足该请求要求), 安装策略决定, 并 (最终) 以所请求的 QoS 级别建立服务流。

应指出的是，通过此处所述的基本信令机制的扩展，应用管理器可以密切控制和监控对服务流的实际管理情况（即增加、变更、删除请求），以便安装策略决定。在情形 1 中，客户机与 CMTS 之间不存在任何直接的通信。

注意，客户机与应用管理器之间的接口，包括“服务请求”的详细说明，都超出了本建议书的讨论范围。一种情况可能是，客户机对 QoS 一无所知，并只是在“服务请求”消息中向应用管理器请求服务（例如，用户希望与朋友玩一种多个玩家参与的游戏）。另一种情况可能是，客户机完全了解其 QoS 需求（例如，在 IPsec 保护下，用户为接入其企业 VPN 而请求担保的 128 kbit/s 服务），并在“服务请求”中传递这一附加的信息。应用管理器为所请求的服务确定 QoS 要求而借助的机制，超出了本体系结构的范围。



J.179_FI.3

图 I.3/J.179—情形1的授权框架

在情形 1 下，如图 I.4 所示，CMTS 支持单阶段的资源预留模型，使客户机能够立刻激活和使用接入网络资源（如本节后面部分中所述的那样，在此情形下，还支持两阶段的资源预留模型）。

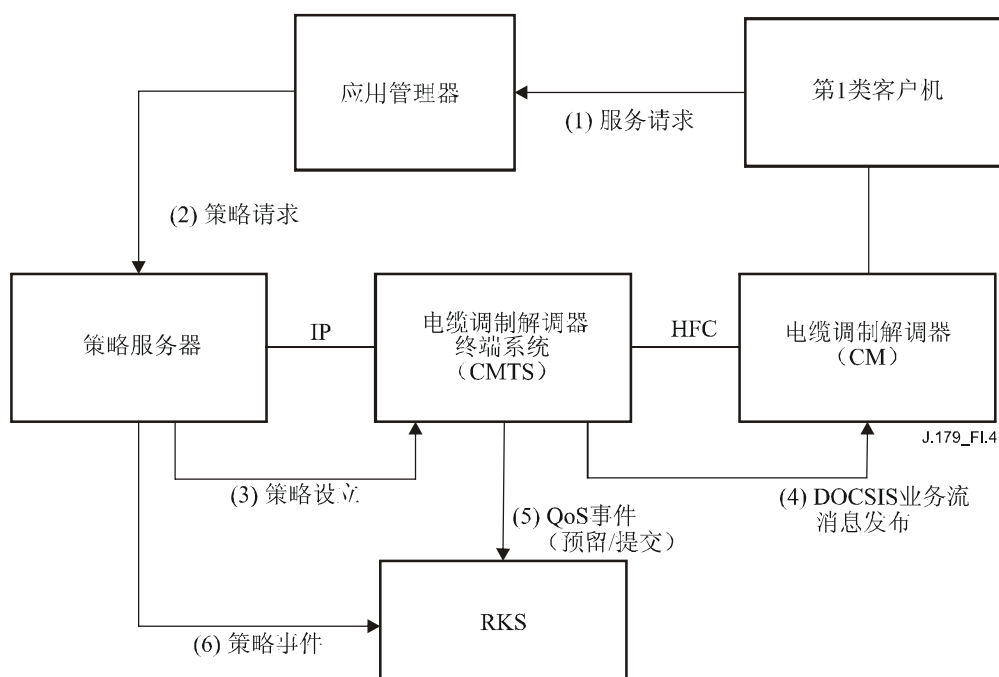


图 I.4/J.179—情形1的单阶段资源预留模型

基于这种单阶段的消息发布序列，表 I.2 提供了有关每一条这些消息的高级摘要。协议消息和对象特定的详细内容服从各自的 IPCablecom 多媒体规范。

表 I.2/J.179—情形1的单阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(1) 服务请求	客户机向应用管理器请求服务。	<无>	超出 IPCablecom 多媒体的范围	该协议应支持对客户机和应用管理器的认证。另外，该协议应为应用管理器提供充分的信息，以传达所请求服务的 QoS 需求。
(2) 策略请求	应用管理器代表客户机请求 QoS 设置。	IPCablecom 多媒体 QoS 类型，IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索	控制门控制 (COPS)	策略服务器使用运营商管理的策略规则，以准许或不准许请求。

表 I.2/J.179—情形1的单阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(3) 策略设立	策略服务器向 CMTS 发送一个消息,安装其策略决定,并请求业务流建立。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS)	控制门控制 (COPS)	在单阶段模型下, 该请求针对的是 QoS 资源的授权、预留和提交。
(4) CableModem 消息发布	CMTS 建立 QoS 增强型业务流。	CableModem 调度类型, 带宽和等待时间参数, 通信业务分类符	CableModem DSx 消息发布	此处的 QoS 功能基于 CableModem RFI 规范中所定义的机制。
(5) QoS 事件	CMTS 产生适当的事件消息, 指明 QoS 用法和其它记账参数。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定, 业务使用数据, 日期时间	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。
(6) 策略事件	策略服务器产生适当的事件消息, 指明策略请求和采取的行动。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。

表 I.2 字段栏中所概述的信息, 旨在举例说明每个消息所传送的信息类型。各个协议消息的详细内容遵从适当的规范文档。

如图 I.5 所示，情形 1 还支持两阶段资源预留模型。此处，应用管理器首先请求授权和预留接入网络 QoS 资源。一旦预留了这些资源，应用管理器可以继续其与客户机进行有关服务的对话。如果适当，应用管理器请求提交接入网络 QoS 资源。这种两阶段预留/提交模型确保在服务提供给客户机之前接入网络资源是可用的。

注意，对所示的各个消息的确认，都不是显性包含在内的，而是暗含的。各个确认消息都只有在已知相应请求最终结果的情况下才能发送。这在确认消息 5（DOCSIS 预留）、3（策略集）和 2（策略请求）的排序中尤其重要，因为在应用管理器继续其与客户机的对话并最终提交资源之前，它可能需要等待预留阶段的成功确认。

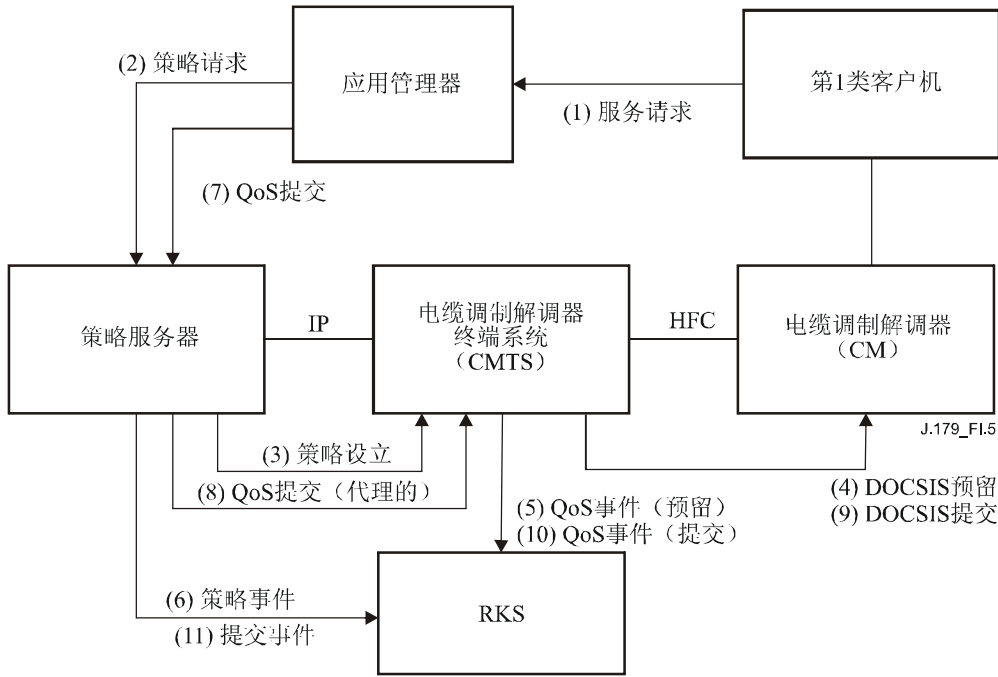


图 I.5/J.179—情形1的两阶段资源预留模型

以下的表 I.3 总结了图 I.5 中所述的各消息。注意，为支持提交信令阶段，加上了消息（7-10）。

表 I.3/J.179—情形1的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(1) 服务请求	客户机向应用管理器请求服务。	<无>	超出 IPCablecom 多媒体的范围	该协议应支持对客户机和应用管理器的认证。另外，该协议应为应用管理器提供充分的信息，以传达所请求服务的 QoS 需求。

表 I.3/J.179—情形1的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(2) 策略请求	应用管理器代表客户机请求 QoS 设置。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索	控制门控制 (COPS)	策略服务器使用运营商管理的策略规则, 以准许或不准许请求。
(3) 策略设立	策略服务器向 CMTS 发送一个消息, 安装其策略决定, 并请求业务流预留。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS)	控制门控制 (COPS)	在两阶段模型下, 该请求针对的是 QoS 资源的授权、预留和提交。
(4) DOCSIS 预留	CMTS 建立 QoS 增强型业务流, 并将之置于“准许”状态。	CableModem 调度类型, 带宽和等待时间参数, 通信业务分类符	CableModem DSx 消息发布	此处的 QoS 功能基于 CableModem RFI 规范中所定义的机制。预留的资源仍是不活动的, 并可由尽力服务通信业务用于其它的流, 直至提交。
(5) QoS 事件	CMTS 产生适当的事件消息, 指明 QoS 预留和其它记账参数。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定, 业务使用数据, 日期时间	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。
(6) 策略事件	策略服务器产生适当的事件消息, 指明策略请求和采取的行动。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。

表 I.3/J.179—情形1的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(7) QoS 提交	AM通知提交 QoS 资源。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别,带宽和等待时间参数,通信业务分类符, 策略标识符	控制门控制 (COPS)	AM 的提交可取决于客户机进一步的消息发布。
(8) QoS 提交 (代理的)	策略服务器接收 AM 请求, 并委托给 CMTS。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别,带宽和等待时间参数,通信业务分类符, 策略标识符	控制门控制 (COPS)	即使 PS 在提交阶段可以应用策略规则, 通常也假定 AM 可以在任何时候提交预留的带宽。
(9) DOCSIS 提交	CMTS 将业务流置于“活动”状态。	CableModem 调度类型, 带宽和等待时间参数,通信业务分类符, 业务流 ID	CableModem DSx 消息发布	此处的 QoS 功能基于 CableModem RFI 规范中所定义的机制。
(10) QoS 事件 (提交)	CMTS 产生适当的事件消息, 指明 QoS 用法和其它记账参数。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别,带宽和等待时间参数,通信业务分类符, 不透明的记账线索 (对 AM 和 PS),策略决定, 业务使用数据, 日期时间	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。
(11) 提交事件	策略服务器产生适当的事件消息, 指明 QoS 提交和采取的行动。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别,带宽和等待时间参数,通信业务分类符, 策略标识符	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。

一旦 QoS 资源在接入网络上得以成功授权、预留和提交, 将对这些资源在 CMTS 上的活动性予以监控。一般而言, 使用一种软状态模型, 在该模型中, 在预留的和提交的服务流非活动期间, 要求定期对消息进行刷新。如果活动计时器在没有刷新的情况下终止了, 那么 CMTS 可以恢复相关的资源。这为网络在故障端点的情况下提供了弹性。

此情形下还提供了—个更为标准的资源恢复序列，在该序列中，当服务会话结束时，应用管理器向策略服务器发出信号。策略服务器通过产生—个事件消息来做出回应，将该事件消息发送至 RKS，并向 CMTS 发出—个指示，以拆卸相关的服务流，并恢复相关的资源。不管服务流的终止是由于非活动性，还是由于被显性删除，都将保留—个牢靠的审计跟踪，通过在 CMTS 中产生并发送给 RKS 的事件消息来跟踪资源的实际使用情况。

I.4.1 举例：基于互联网的带宽要求

有关服务交付背景下如何应用情形 1 中机制的—个例子是：运营商所有的—个安全网站将准许订户按需请求带宽预留。

例如，假设订户的正常服务速率限制在 128 kbit/s 的下行流和 128 kbit/s 的上行流。虽然对大多数使用而言，该服务级别可能是适当的，但可能存在这样的时刻，即订户正在使用的应用需要更多的带宽，或具有不同的 QoS 需求。如果用户决定按需使用带宽服务来暂时改变其正常的服务级别，那么它们可以简单地在运营商网站（应用管理器）上进行注册，并请求临时升级服务。

对此类请求，—种可能的动机是希望从内容提供商那里流出高比特率的媒体文件。在这种情况下，订户可以显性地为后面的三个小时请求 512 kbit/s 下行流的最小预留速率服务。可选地，准确的应用的 QoS 需求对订户而言可以是不透明的，订户可以只简单地请求某个特定的三小时视频片断（订户不知道的是，此类视频恰好以 512 kbit/秒的速率进行编码）。另—种方法是，这种交换代表订户向应用管理器提出的“服务请求”。

在另—种情况下，应用管理器将为三小时的 512 kbit/s 最小预留速率服务，代表订户向策略服务器提出“策略请求”。然后，策略服务器将采用自己的授权准则，并且，如果该请求得以批准，那么请求 CMTS（通过—个“策略集”）为用户提供带宽。CMTS 将依次执行内部准许进入控制，并使用 CableModem 消息发布来建立 QoS，通过 QoS 事件消息来跟踪这一过程。

I.4.2 举例：经由网络化控制台的在线游戏

可选地，考虑两个游戏控制台希望通过网络隧道相互进行交战的这一情况。在该例子中，只有当两个用户同处—地时，通常才可以将其控制台联结成网。不过，安装在各个用户个人电脑上的专门软件，它们同处—个局部网中，并充当远程控制台的代理，能够使得将这样的两个游戏控制台联结成网不再需要同处—地。这种新方法的唯一问题是，作为结果的隧道需要足够的 QoS，以便能够控制游戏控制台，就好像它们同处在一个高速网络上。

在这种情形下，用户将通过个人电脑与应用管理器相连，通过隧道来传递他们的分组。通过应用特定的消息发布，他们实现对自身的认证，并表明其相互进行—个游戏的请求。应用管理器批准该请求，并代表用户产生“策略请求”。策略服务器作出它的决定，并将该消息作为“策略集”转递给 CMTS。CMTS 执行准许进入控制，使得对使用 CableModem 消息发布的游戏隧道能够在个人电脑之间实现接入网络 QoS。从这—刻起，游戏控制台可以进行分组交换，而无须知道它们并未同处—地。注意：为简化起见，在本例子中未考虑事件消息发布。

在该假定的例子中，如果用户驻留于单独的 HFC 节点上，那么由运营商负责，确保在其策略和服务协议要求的层面上，对通往和来自 CMTS 的骨干网 QoS 进行适当处理。简化起见，图 I.6 提供了该例子的图解说明，当中，两个用户都从—个单个的 CMTS 处接收服务。

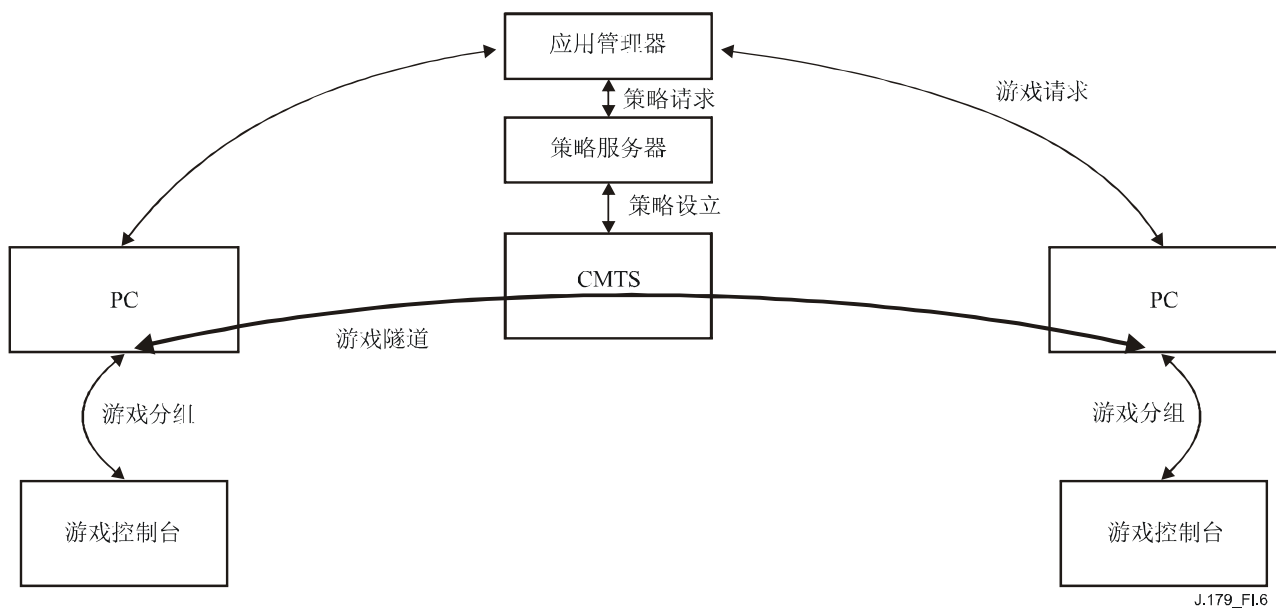


图 I.6/J.179—通过QoS增强型IP隧道联结成网的游戏控制台

I.5 带策略推动的、客户机请求的QoS（情形2）

情形 2 的“带策略推动的、客户机请求的 QoS”模型支持第 2 类客户机，它能够发出信令，并管理其自身的 QoS 资源，但要求通过应用管理器预先对这些请求进行授权。在该情形下，策略授权和 QoS 预留模型与 DQoS 规范中所定义的 IPCablecom-T 电话模型非常相似。策略服务器以一种类似于控制门控制器通过 COPS 向 CMTS 发送策略的方式，向 CMTS 推送策略。第 2 类客户机或者使用 CableModem DSx，或者使用类似于 IPCablecom-T 中 MTA 设备的 RSVP+消息发布。

图 I.7 显示了对情形 2 的高级概述。请注意它与为情形 1 所述之授权框架的相似性。此处，客户机通过向应用管理器发送一个“服务请求”，再次请求一个应用特定的服务。然后应用管理器决定所请求服务的 QoS 需求，并向策略服务器发送一个“策略请求”。“策略请求”包含“授权的封装”或客户机允许的最大 QoS。依据运营商定义的策略规则，策略服务器依次对“策略请求”进行验证，如果验证表明决定是肯定的，那么向 CMTS 发送一个“策略集”。CMTS 对所请求的 QoS 执行准许进入控制，并安装策略授权。如同情形 1，策略服务器和 CMTS 产生事件消息，并将之发送至 RKS。策略服务器在任何做出决定的时候都记录一个事件，或者更新其状态，CMTS 则跟踪 QoS 资源的保持与使用情况。

在情形 2 中，不像情形 1，为了增加、变更和删除资源预留，客户机与 CMTS 之间存在直接的通信。CMTS 从策略服务器处收到“策略集”消息后，客户机可以使用先前提及的 QoS 信令机制请求直接来自 CMTS 的 QoS。只要所请求的 QoS 处于策略服务器批准的“授权封装”内，客户机就还可以动态地改变 QoS。该方法的优势在于应用管理器不必协商客户机的带宽使用情况，当客户机的 QoS 需求动态地发生变化时，这是一个非常有益的要素。

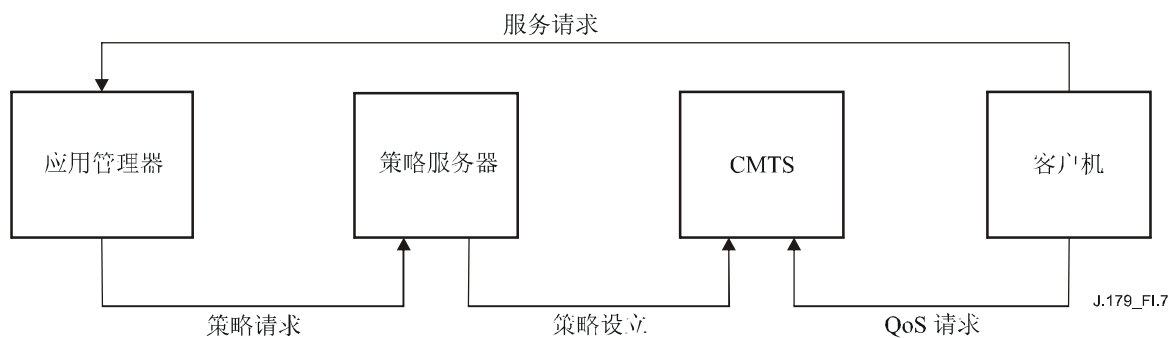


图 I.7/J.179—情形2的授权框架

与之前的情形一样，情形 2（如图 I.8 所示）支持单阶段的资源预留模型，以使客户机能够立刻激活和使用接入网络资源。

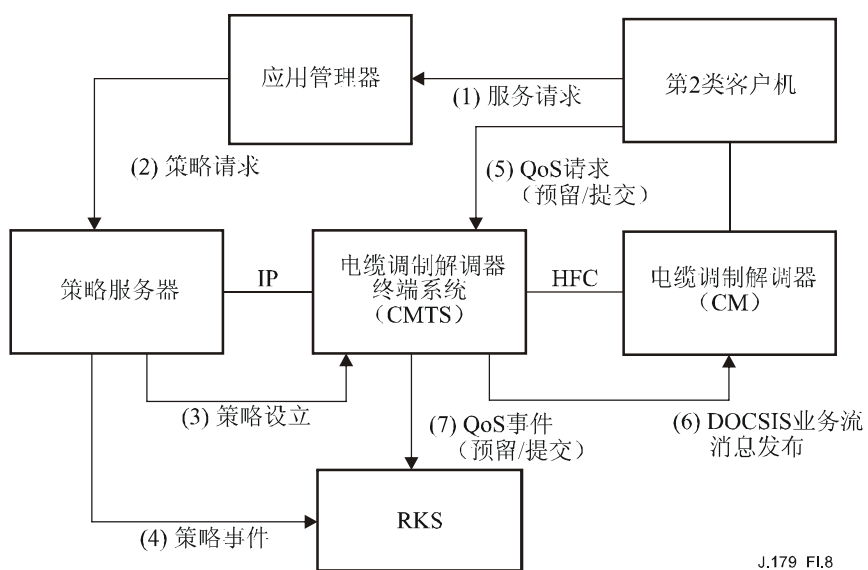


图 I.8/J.179—情形2的单阶段资源预留模型

基于这种单阶段消息发布序列，表 I.4 提供了有关这些消息中每一个消息的高级摘要。

表 I.4/J.179—情形2的单阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(1) 服务请求	客户机向应用管理器请求服务。	<无>	超出 IPCablecom 多媒体的范围	该协议应支持对客户机和应用管理器的认证。另外，该协议应为应用管理器提供充分的信息，以传达所请求服务的 QoS 需求。
(2) 策略请求	应用管理器代表客户机请求 QoS 授权。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索	控制门控制 (COPS)	策略服务器使用运营商管理的策略规则，以准许或不准许请求。
(3) 策略设立	策略服务器向 CMTS 发送一个消息，安装其策略决定。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索（对 AM 和 PS）	控制门控制 (COPS)	在该情形下，该请求仅针对授权。
(4) 策略事件	策略服务器产生适当的事件消息，指明策略请求和采取的行动。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索（对 AM 和 PS），策略决定	事件消息发布 (RADIUS)	该消息应包含充分的构件，以便出于支持与/或调解之目的，准许重新构建有关某项特殊服务的事件及所做的决定。
(5) QoS 请求 (预留/提交)	客户机请求预留 QoS 资源，并立即提交，以供使用。	带宽和等待时间参数，通信业务分类符	CableModem DSx 或 RSVP+	客户机可以通过 DSx 消息发布来直接建立 CableModem 业务流，或可以通过发布 RSVP+消息来建立这些流。

表 I.4/J.179—情形2的单阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(6) DOCSIS 消息发布	CMTS 建立 QoS 增强型业务流, 并将之置于“活动”状态。	CableModem 调度类型, 带宽和等待时间参数, 通信业务分类符	CableModem DSx 消息发布	只有当 RSVP+信令是在前一消息中提供给 CMTS 时, 该步骤才是必需的, 否则的话, 业务流已经通过 CableModem DSx 消息发布予以设置和激活。此处的 QoS 功能基于 CableModem 建议书中所定义的机制。
(7) QoS 事件	CMTS 产生适当的事件消息, 指明 QoS 用法和其它记账参数。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定, 业务使用数据, 日期时间	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。

如图 I.9 所示, CMTS 也支持两阶段资源预留模型。在该模型中, 客户机首先请求预留接入网络 QoS 资源。一旦预留了这些资源, 客户机随后将通知提交这些 QoS 资源。在向客户机提供服务之前, 两阶段预留/提交模型保证接入网络资源是可用的。

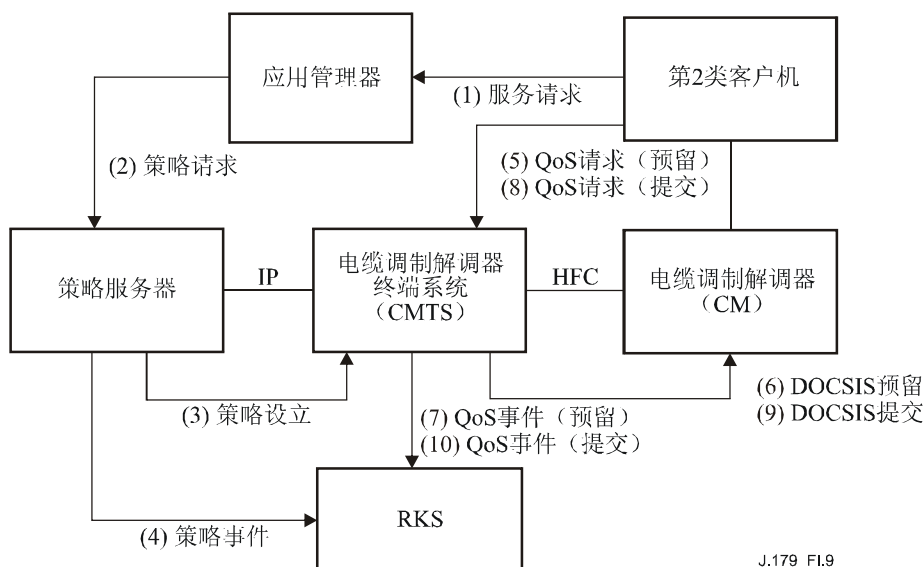


图 I.9/J.179—情形2的两阶段资源预留模型

表 I.5/J.179—情形2的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(1) 服务请求	客户机向应用管理器请求服务。	<无>	超出 IPCablecom 多媒体的范围	该协议应支持对客户机和应用管理器的认证。另外，该协议应为应用管理器提供充分的信息，以传达所请求服务的 QoS 需求。
(2) 策略请求	应用管理器代表客户机请求 QoS 授权。	IPCablecom 多媒体 QoS 类型，IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索	控制门控制 (COPS)	策略服务器使用运营商管理的策略规则，以准许或不准许请求。
(3) 策略设立	策略服务器向 CMTS 发送一个消息，安装其策略决定。	IPCablecom 多媒体 QoS 类型，IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索 (对 AM 和 PS)	控制门控制 (COPS)	在该情形下，该请求仅针对授权。

表 I.5/J.179—情形2的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(4) 策略事件	策略服务器产生适当的事件消息，指明策略请求和采取的行动。	IPCablecom 多媒体 QoS 类型，IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索（对 AM 和 PS），策略决定	事件消息发布（RADIUS）	该消息应包含充分的构件，以便出于支持与/或调解之目的，准许重新构建有关某项特殊服务的事件及所做的决定。
(5) QoS 请求（预留）	客户机请求预留 QoS 资源。	带宽和等待时间参数，通信业务分类符	CableModem DSx 或 RSVP+	客户机可以通过 DSx 消息发布来直接建立 CableModem 业务流，或可以通过发布 RSVP+消息来建立这些流。
(6) DOCSIS（预留）	CMTS 建立 QoS 增强型业务流，并将之置于“准许”状态。	CableModem 调度类型，带宽和等待时间参数，通信业务分类符	CableModem DSx 消息发布	只有当 RSVP+信令是在前一消息中提供给 CMTS 时，该步骤才是必需的，否则的话，业务流已经通过 CableModem DSx 消息发布予以设置和激活。此处的 QoS 功能基于 CableModem 建议书中所定义的机制。
(7) QoS 事件（预留）	CMTS 产生适当的事件消息，指明 QoS 用法和其它记账参数。	IPCablecom 多媒体 QoS 类型，IPCablecom 多媒体会话类别，带宽和等待时间参数，通信业务分类符，不透明的记账线索（对 AM 和 PS），策略决定，业务使用数据，日期时间	事件消息发布（RADIUS）	该消息应包含充分的构件，以便出于支持与/或调解之目的，准许重新构建有关某项特殊服务的事件及所做的决定。

表 I.5/J.179—情形2的两阶段资源预留消息详细内容

消 息	功 能	字 段	候 选 协 议	注 释
(8) QoS 请求 (提交)	客户机请求提交 QoS 资源。	带宽和等待时间参数, 通信业务分类符	CableModem DSx 或 RSVP+	客户机可以通过 DSx 消息发布来直接建立 CableModem 业务流, 或者可以通过发布 RSVP+消息来建立这些流。
(9) DOCSIS (提交)	CMTS 将业务流置于“活动”状态。	CableModem 调度类型, 带宽和等待时间参数, 通信业务分类符, 业务流 ID	CableModem DSx 消息发布	只有当 RSVP+信令是在前一消息中提供给 CMTS 时, 该步骤才是必需的, 否则的话, 业务流已经通过 CableModem DSx 消息发布予以设置和激活。此处的 QoS 功能基于 CableModem 建议书中所定义的机制。
(10) QoS 事件 (提交)	CMTS 产生适当的事件消息, 指明 QoS 用法和其它记账参数。	IPCablecom 多媒体 QoS 类型, IPCablecom 多媒体会话类别, 带宽和等待时间参数, 通信业务分类符, 不透明的记账线索 (对 AM 和 PS), 策略决定, 业务使用数据, 日期时间	事件消息发布 (RADIUS)	该消息应包含充分的构件, 以便出于支持与/或调解之目的, 准许重新构建有关某项特殊服务的事件及所做的决定。

与之前的情形一样, 关于 QoS 资源的拆卸和恢复, 有两种可选方案。由于未通知计时器刷新而引起的非活动性, 或者客户机在完成一次服务会话后显性地将之删除, 那么资源可以终止 (如在 CMTS 上所检测到的那样)。为了显性地告知服务流删除而提供的机制, 是客户机设备 2 所定义的 QoS 协议的一部分。为情形 1 定义的资源恢复序列与为情形 2 定义的资源恢复序列之间存在的唯一差异是: 在第一种情形中, 通过客户机直接告知服务流删除, 而在第二种情形中, 则通过应用管理器代理告知服务流删除。

I.5.1 举例：经由网络化控制台的在线游戏

对在第 I.4.2 节中为情形 1 所述的网络化游戏控制台的例子，可以简便地进行改变，以便符合情形 2 中所述的 QoS 资源管理模型的要求。在这种情况下，为了相互定位并建立应用特定的信令，控制台将继续与应用管理器进行协调。此外，应用管理器将向策略服务器提交一个资源请求，请求对所需的 QoS 资源进行授权。不过，一旦在 CMTS 上成功安装这种授权决定，那么应用管理器将向各个人电脑代理简单地返回一个肯定的确认消息，该确认消息包含一个授权令牌。然后，为了预留、提交和删除游戏隧道所需的服务流，个人电脑在其向 CMTS 发送的 QoS 信令中可以使用这一令牌。

I.6 带策略拉动的、客户机请求的QoS（情形3）

第三种情形及其“带策略拉动的、客户机请求的 QoS”授权模型，支持第 3 类客户机。情形 3 定义了一种模型，在该模型中，策略授权决定不是预先建立的，通过应用管理器和在先前情形中所述的策略服务器机制推送至 CMTS，但当输入的预留请求发出指令时，由 CMTS 从策略服务器处根据需要提出请求。这允许一种由客户机激励的、非常灵活和动态的资源预留模型，同时在头端为所有的资源请求保留了授权的运营商控制。

在该情形中，在策略服务器安装策略决定之前，CMTS 从客户机处接收一个 QoS 请求。与该 QoS 请求一同包括在内的是使客户能够得以认证的证书。CMTS 建立一个策略请求，并将其发送至策略服务器。在策略服务器处，请求得以认证，并依据运营商特定的准则（如资源可用性、客户简表、信用等级、服务类别、与其它网络元素的互动等）做出授权决定。如果策略授权成功，那么允许在 CMTS 上继续预留资源，并基于请求的 QoS 建立适当的 CableModem 服务流。在这种互动中涉及的 IPcablecom 多媒体接口（在第 I.3.1 节中加以定义）包括：pkt-mm-1、pkt-mm-2、pkt-mm-4、pkt-mm-5、pkt-mm-6 和 mm-9。pkt-mm-3 接口和特定应用信令要求指令都可以使用，但并不假定是在用的。

图 I.10 描述了情形 3 下核心接入网络元素之间的信息流。紧接在图 I.10 之后的表 I.6 对每个消息做了进一步的描述。在以下所示的例子中，只在 CM 与 CMTS 之间的上行流方向才建立 QoS。为了建立对称的下行流 QoS，需要一个类似的流。

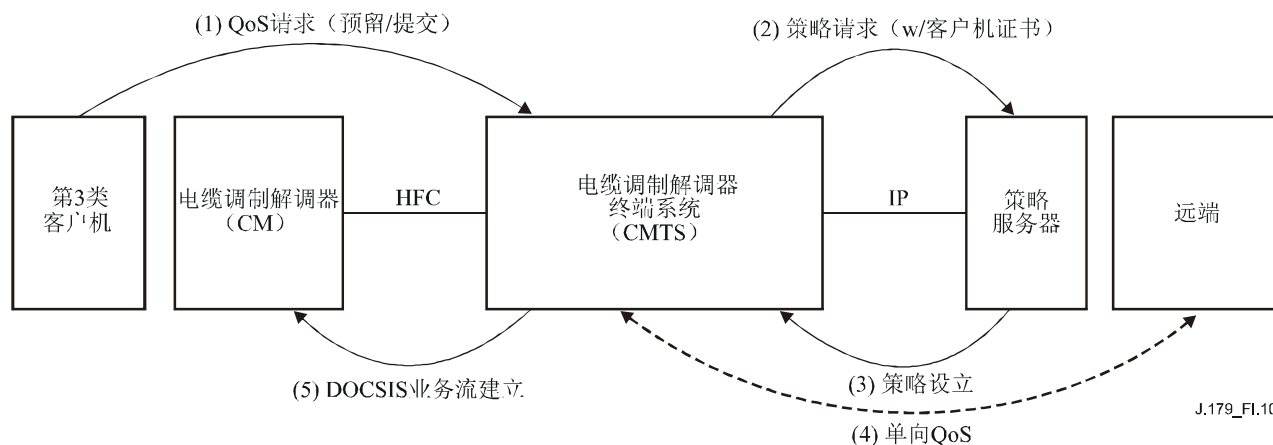


图 I.10/J.179—情形3的授权框架

表 I.6/J.179—情形3的消息详细内容

消 息	功 能	字 段	候选协议	注 释
(1) QoS 请求 (预留/提交)	客户机向 CMTS 请求预留资源。	带宽和等待时间参数, 通信业务分类符, 授权证书	RSVP	该情形假设客户机存在 RFC 2205 性能。
(2) 策略请求	CMTS 向策略服务器请求策略授权决定。	带宽和等待时间参数, 通信业务分类符, 授权证书	COPS	RFC 2748
(3) 策略设置	策略服务器在 CMTS 上安全授权。	带宽和等待时间参数, 通信业务分类符	COPS	RFC 2748
(4) 单向 QoS	CMTS 发送远端 RSVP 信令。	带宽和等待时间参数, 通信业务分类符, 授权证书	RSVP	RFC 2205
(5) CableModem 业务流建立	CMTS 与 CM 协商 CableModem 排定的业务流建立。	CableModem 调度类型, 带宽和等待时间参数, 通信业务分类符, 业务流 ID	CableModem DSx 消息发布	此处的 QoS 功能基于 CableModem 建议书中所定义的机制。

此情形的其中一个主要而突出特点是它支持 RSVP, RSVP 是一种基于标准的 QoS 信令机制。然而情形 1 论及的是不具备固有 QoS 信令性能的客户机, 情形 2 则定义了一种 IP-Cablecom 特定的 QoS 信令机制 (基于 RSVP, 但包括专用的扩展), 该情形基于 IETF 标准自身。这将提供与基于标准的客户机之间的互操作性, 基于标准的客户机预订了运营商的 QoS 服务, 并拥有一种在接入网络上安全地认证自己的方法。它也不要求应用提前推动策略决定, 因此, 它对应用信令没有体系结构方面的限制。

情形 3 假定在客户机与远端之间交换 RSVP 消息发布。不过, 要注意, 这并不要求客户机与远端之间的所有网络元素都需要支持 RSVP, 也不意味着使用集成服务 (IntServ [13]) 端到端 QoS 策略。例如, 超出 CMTS, 可使用不同的服务 (DiffServ [16]) 或另一个 QoS 方案。另外, 也不希望支持 RSVP 的中间路由器可以不加处理地而简单地实现 RSVP 消息的传递。选择地, 如果能够通过其它方法获得 QoS 保证, 那么此类路由器可以定义为聚合区域, 并因此可以透明地传送 RSVP 消息, 如 RFC 3175 [20] 中所定义的那样。

注 — RFC 3175 要求在近端和远端边缘路由器上都执行这种聚合功能。

此外, 应注意到, 在该情形中使用 RSVP 几乎完全符合标准的 (即 RFC 2205) 的 RSVP 操作, 因此, 在接入网络上预留的资源是单向的。这样, 客户机预留上行资源, 而远端负责预留下行资源。

通过软状态更新，成功的资源预留与其它情形中的预留是类似的。RSVP 客户机务必定期发送消息，以保持其预留，否则，预留将终止，并在 CMTS 上被回收。

最后，RSVP 协议中包括了特殊的机制，以便传送端点和接收端点能够告知终止和拆卸某个服务流。基于 RSVP 预留的单向特点，保持多个服务流的端点负责在服务会话结束之时显性地删除这些流中的每一个流。

假定这种模式，为了能够满足下行资源预留所需的特殊考虑，需要进行远端请求认证。一种解决方案是要求策略服务器既能认证近端客户机，也能认证远端客户机。其它的解决方案也是可能的，但务必谨慎考虑安全问题，尤其是潜在的窃取服务的可能性。

I.6.1 举例：经由固有QoS信令的在线游戏

可利用情形 3 的一种潜在的服务是在线游戏。在该例子中，所有的要求都是在客户机上支持集成的、基于标准的 RSVP。也就是说，有或没有应用服务器，所设计的在线游戏都可以工作。

当一个客户机希望加入游戏时，它们将只需向远端发送一个应用特定的消息，然后通过发送一个 RSVP 消息，继续进行请求网络 QoS，并再一次提交给远端。当 CMTS 收到此消息时，为了认证客户机，并决定是否应授予 QoS，它将向策略服务器发送一个请求。成功的授权将导致单向的 QoS 预留。

同样，远端将向客户机发送一个 RSVP 消息。当 CMTS 再次收到该消息时，它将被发送至策略服务器，以确定是否应授予 QoS。一旦成功授权和提供服务，客户机随后将在两个方向上拥有 QoS，并继续进行在线游戏。

I.7 IPCablecom-T与IPCablecom多媒体的比较

本节从高级层面上描述了 IPCablecom-T 与 IPCablecom 多媒体体系结构之间的主要区别。考虑到本建议书的大多数特定协议特性和 IPCablecom 多媒体功能细节还有待定义，对这些已知的区别做了总结，如表 I.7 所示，以便提供快速参考。

表 I.7/J.179—IPCablecom-T与IPCablecom多媒体的对照

	IPCablecom-T	IPCablecom多媒体
支持的业务	住宅电话 基本的住宅电话特性 扩展的电话特性	多媒体业务 基于客户机（对等） 基于服务器
事件消息发布	对所有策略和 QoS 事件稳健的审计跟踪 支持 PSTN 记账模型	对所有策略和 QoS 事件稳健的审计跟踪 支持基于 QoS 的记账 支持基于时间和容量的记账

表 I.7/J.179—IPCablecom-T与IPCablecom多媒体的对照

	IPCablecom-T	IPCablecom多媒体
QoS 性能	CableModem QoS 调度算法 主动提供的授权服务 带活动性检测的、主动提供的授权服务 带宽特性 恒定的比特率 对称的上行流/下行流 保证的 QoS 水平 客户机到客户机（即经由分段模型的端到端）	CableModem QoS 调度算法 主动提供的授权服务 带活动性检测的、主动提供的授权服务： • 实时轮询 • 非实时轮询 • 带优先级或不带优先级的尽力服务 带宽特性： • 恒定的比特率 • 可变的比特率 • 对称的上行流/下行流 • 非对称的上行流/下行流 保证的 QoS 水平： • CMTS 到 CM（即接入网络）
安全性	安全的信令和媒介 安全的设备提供和配置管理	经 Ipsec 保护的 COPS 和 RADIUS；带预共享密钥认证的、经 IKE 的密钥管理（带证书的 IKE 或 Kerberos 化的密钥管理是可选的）。 客户机信令超出了本附录的讨论范围，因此，对客户机信令接口未定义任何安全性。

I.7.1 DQoS

IPCablecom-T 的首要焦点是住宅电话服务。作为该服务的一部分，动态服务质量（DQoS）规范得以开发，它定义了 IP 网络基于 CableModem 的接入部分上提交 QoS 所需的机制。也就是说，IPCablecom-T 采用了一种分段的方法（将端到端媒介和信令通道划分为通过骨干网连接的近端和远端接入网络），在此方法下，DQoS 在接入段对资源预留做了特殊处理，而不是在骨干网上或是在端到端 QoS 上进行处理。

IPCablecom 多媒体的目标是实现更加普遍的多媒体应用，这些应用胜过语音支持。不过，它建立于某些基本的 IPCablecom-T DQoS 机制基础之上，以便为这些应用提供 QoS 增强型服务。

I.7.1.1 接入网络元素

IPCablecom-T 支持下列网络元素：MTA、CM、CMTS、CMS（逻辑上由一个呼叫代理和一个控制门控制器组成）和 RKS。在 IPCablecom 多媒体体系结构中，可以在功能上将呼叫代理映射至应用管理器，并在功能上将控制门控制器映射至策略服务器。在 IPCablecom 多媒体体系结构中，可引入额外的网络元素，包括如媒体服务器等。应用管理器和媒体服务器实际上可以驻留在同一设备中，或者也可以分别对其进行配署。

1.7.1.2 DQoS体系结构

IPCablecom DQoS [9]体系结构基于 CableModem、RSVP+，以及由 CMS（控制门控制器）安装在 CMTS 上的 QoS 策略。

正如在本建议书中一直所描述的那样，IPCablecom 多媒体体系结构也基于这些技术。除此之外，多媒体服务还有一个目标，即支持更加基于标准的 RSVP 信令模型（情形 3），其目的是，该性能将使 QoS 增强型服务能为更多的消费者所用。

IPCablecom-T DQoS 体系结构中的 CMTS 充当 QoS 策略的策略执行点。CMTS 将在 IPCablecom 多媒体体系结构中执行类似的功能。除了服务于客户机发出的 QoS 请求，CMTS 还可以从策略服务器（情形 1）处接收代理的 QoS 请求。这有别于 IPCablecom-T DQoS 体系结构，在后者中，只有单独的 MTA 或嵌入的 MTA 才可以启动激活 QoS 的行为。

1.7.1.3 QoS接口

在 IPCablecom-T 体系结构中，在所有网络元素之间和 CMTS 之间，已定义了信令接口，以实现在线到在线的呼叫，它们支持控制门协调。在概述中，MTA 与呼叫代理之间的信令协议为 NCS，嵌入的 MTA 与 CMTS 之间的信令协议为 CableModem，单独的 MTA 与 CMTS 之间的信令协议为 RSVP+。从 GC 到 CMTS 的信令为基于 COPS 的控制门控制消息发布。

IPCablecom 多媒体建立于这些信令接口之上，并额外支持应用管理器与策略服务器之间的信令接口。回顾一下，发生于应用管理器及其客户机之间的任何应用特定的信令，均超出了本体系结构的讨论范围。

1.7.1.4 IPCablecom QoS框架

在 IPCablecom-T QoS 体系结构中，“一个称为‘控制门’的 QoS 定义的结构，为接入网络与高质量骨干网业务的连接提供了控制点”（参见 DQoS 规范 [14]）。出于策略执行的目的，一个控制门代表了安装于 CMTS 之上的一个 QoS 授权。IPCablecom 多媒体定义了一个类似的 QoS 策略结构，并且 IPCablecom-T DQoS 控制门结构有望发挥其优势，在 IPCablecom 多媒体中提供策略功能。为提供衰减的 QoS 控制（例如，为了支持情形 1），可以要求对现有的 IPCablecom-T 控制门控制机制进行更改。

1.7.1.5 接入网络资源管理要求

IPCablecom-T 体系结构“旨在提供高度的通用性，目的是使之能够提供新的业务，并推动网络体系结构的未来发展”。对可行的 QoS 体系结构，此目标在以下几方面提出了要求（注意：这些与 QoS 相关的性能要求中的每一个要求都在 IPCablecom DQoS 规范中予以了明确定义和论述）：

- 会话期间的资源变化；
- 资源的动态绑定；
- 会话类别（优先级指定）；
- 两阶段资源交付；
- 分阶段的资源分配；
- 骨干网 QoS 支持；
- 防止窃取服务。

IPCablecom 多媒体体系结构还将支持单阶段资源预留模型。最初,多媒体体系结构将不解决骨干网的 QoS 支持问题,虽然该功能可以作为运营商的需求规定予以正式解决。有关现有 IPCablecom-T DQoS 要求的更多信息请参见 IPCablecom-T DQoS 规范[14]。

I.7.1.6 操作理论

IPCablecom-T DQoS 涉及不同的预留和提交阶段,以获得接入网络资源。在预留阶段结束之时,留出资源,但并不激活,或者尚不能为 MTA 所用。在第二阶段结束之时,提交资源,并使之可供使用。依据传统的电话模型,记账开始于提交阶段期间。

在嵌入式 MTA 模型中,在 MTA 与 CMTS 之间并不要求 RSVP+。相反地,E-MTA 可以通过 CableModem DSx 消息发布来发送资源预留和提交信号。在独立的 MTA 模型中,RSVP+消息发布用于执行这些步骤。然后,CM 和 CMTS 通过 CableModem DSx 消息发布进行协调,以排定接入网络上要求的服务流顺序。

如本附录所述,IPCablecom 多媒体支持一种类似于 IPCablecom-T 的模型,并另外支持更为标准的 RSVP 用法。它还提供了一种代理的 QoS 请求模型,在该模型中,应用管理器代表客户机对 QoS 进行管理。这些模型在本附录的情形条款中做了详细论述。现有的 IPCablecom-T 模型映射至情形 2。另外两种模型在 IPCablecom 多媒体体系结构中予以支持,以便为多媒体服务提供更大的灵活性,使之能够更加灵活地部署于运营商网络中。

I.7.2 记账的事件消息

为了能够为众多经 IPCablecom 体系结构交付的服务传送有关网络使用的信息,将 IPCablecom 事件消息设计为是灵活的和可扩展的。IPCablecom-T 事件消息规范定义了一般的事件消息体系结构和特殊的要求,以支持 IPCablecom-T 语音业务。IPCablecom 事件消息规范(ITU-T J.164 建议书)详细论述了独立于传输协议的事件消息 TLV 格式、事件消息文件格式以及强制的和可选的传输协议。

这些消息包含了足够多的、有关每次会话的信息,以支持客户对服务的记账。包含在事件消息中的信息支持众多记账和结算模型。IPCablecom 不强制要求使用特定的记账或结算模型,原因是这些模型由单个电缆运营商进行定义,并基于特定的商业需求。IPCablecom 既不强制也不排除对结算使用票据交换所。

IPCablecom 事件消息基于这样一种模型,即它将会话或服务分割成两半,一半为发起部分,一半为终止部分。发起 CMS 或 MGC 务必产生一个唯一的记账相关 ID (BCID),以确定所有与会话发起部分相关的事件消息。终止 CMS 或 MGC 务必产生一个唯一的 BCID,以确定所有与会话终止部分相关的事件消息。对话或服务的各个部分,产生事件消息(CMS、MGC、CMTS)的 IPCablecom 网络元素集务必提供所有必要的信息,需要的话,根据业务情况,记账与/或结算需要这些信息。由发起部分产生的信息务必发送至支持发起部分的 RKS 处。由终止部分产生的信息务必发送至支持终止部分的 RKS 处。

IPCablecom 多媒体服务要求一个有限的事件消息集。这些消息包括：

- 由策略服务器产生的、针对“增强型 QoS 服务”的 Signal_Start，它指明了策略服务器收到接入网络 QoS 请求的时间；
- 由策略服务器产生的、针对“增强型 QoS 服务”的 Signal_Stop，它指明了策略服务器收到终止使用网络 QoS 通知的时间。
- 由 CMTS 产生的 QoS_Reserve、QoS_Commit、QoS_Stop。这些消息指明了 CMTS 预留、提交或发布接入网络 QoS 的时间。

I.7.3 安全性

IPCablecom-T 安全性体系结构定义了符合安全性服务要求的机制、算法和协议。利用有关相应接口的相同机制，IPCablecom 多媒体接口的安全得以保护。

附 录 二

版本号分配指南

不同协议版本之间的互操作性基于以下原则：

健壮性原则：

RFC 791 为互联网协议定义了以下一般性“健壮性原则”：

- “实施方案在其发送行为上必须是保守的，但在其接收行为上必须是自由的”。
- 遵循这样一个健壮性原则，当仍保持后向兼容性时，有可能允许在协议上出现小的变动。

在 PacketCable 多媒体控制门控制协议中，协议版本编号的一般性规则如下所述：

- 在相同大版本号内的协议版本必须是后向兼容的。不期望大版本号不同的各版本是后向兼容的。
- 至关重要的是，PacketCable 多媒体规范小组检查所有将包括在新版协议中的变动，并基于影响最大的变动选择一个协议版本号。如果任何变动都满足有关大协议版本变动的准则，那么务必递增大版本号。

可能导致小版本号变动的协议变化例子如下所述：

- 只要在消息中纳入新的对象不会对接收消息的网络元素引入新的强制性功能要求，那么可以引入一个新的可选对象，这样就可以安全地忽略该对象。
- 反对可选对象。

可能导致大版本号变动的协议变化例子如下所述：

- 新消息的引入。
- 特定对象的格式变化。
- 禁止在特定消息中纳入特定对象的语法变更。
- 使特定消息中的对象变为强制性对象的语法变更。
- 使消息中曾经的强制性对象变为可选对象的语法变更。
- 引入一个新的可选对象，当它包括在一个消息中时，对接收消息的网络元素引入新的强制性功能要求，这样就不可以安全地忽略该新的对象。
- 与协议相关的算法或状态的语义变更（如控制门状态机），这种变更可能导致运行新旧协议版本的不同设备之间出现状态不一致的现象。

有些变化，如那些引入新功能的变化，难以进行归类。例如，有人可能想象这样一种变化，它引入一个新的对象和一些针对接收消息中对象的网络元素的功能要求。如果接收对象的网络元素正在较低的协议版本上运行，在该协议版本中未定义新的对象，那么缺省的行为将是：该对象将被忽略，并因此不执行新对象所指的行为。如果因对象被忽略而不执行的新行为相对网络元素而言是局部的，那么在这种情况下，人们可以坚持认为，两个网络元素成功地在较低的协议版本上实现了互操作。另一方面，如果在消息中出现新的对象要求接收网络元素发送一个新的应答，或者基于新的对象对现有应答进行修改，那么忽略新的对象可能有碍互操作性。在后一种情况中，要求进行大版本变更。

其它的变化，如那些将消息中对象状态从强制的改为可选的或者从可选的改为强制的，将导致基于发射机行为的互操作执行。不过，由于不能保证有关可选参数发射机的行为，因此此类变化应归为大的变更。

假定许多类型的版本变更将要求大的协议版本变化，那么对协议改变进行分组是有意义的，它使得很少发生大版本的变化，且使新的版本能够提供巨大的价值，这种价值将证明进行这些变化是恰当的。

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