GY

中华人民共和国广播电影电视行业标准

GY/T 200.2—2004

HFC 网络数据传输系统技术规范 第 2 部分：射频接口及协议

Specification for HFC data transmission system
Part 2: RF interface and protocol

(ITU-T J.112, Transmission Systems for Interactive Cable Television Services, MOD)

2004-03-22 发布　　2004-05-01 实施

国家广播电影电视总局　发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 1
3.1 术语和定义 1
3.2 缩略语 7
4 通讯协议 8
4.1 协议栈 8
4.2 MAC 转发器 11
4.3 网络层 13
4.4 在网络层之上 14
4.5 数据链路层 14
4.6 物理层 15
5 物理媒介依从子层（PMD）规范 15
5.1 上行 16
5.2 下行 29
6 下行传输会聚子层 32
6.1 MPEG 包格式 32
6.2 HFC 数据传输的 MPEG 包头 33
6.3 MPEG 有效负载 33
6.4 与 MAC 子层的交互 33
6.5 与物理层的交互 34
6.6 MPEG 包头同步和恢复 34
7 媒介接入控制技术要求 34
7.1 简介 34
7.2 MAC 帧的格式 36
7.3 MAC 管理消息 49
8 媒介接入控制协议操作 78
8.1 上行带宽分配 78
8.2 对多信道的支持 82
8.3 定时和同步 82
8.4 上行传输和争用解决 84
8.5 数据链路加密的支持 86
9 服务质量和分段 86
9.1 操作原理 86
9.2 上行业务流调度业务 97
9.3 分段 100
9.4 有效负载包头抑制 106
10 CM—CMTS 交互作用 111
10.1 CMTS 初始化 111
10.2 CM 初始化 111
10.3 标准操作 129
10.4 动态业务 132
10.5 故障检测和恢复 173
11 支持未来新 CM 的能力 174
附　录　A　（规范性附录）　常用地址 176
附　录　B　（规范性附录）　参数与常量 178
附　录　C　（规范性附录）　公用射频接口编码 181
附　录　D　（规范性附录）　CM 配置接口规范 212
附　录　E　（资料性附录）　MAC 业务定义 217
附　录　F　（资料性附录）　前同步码序列实例 224
附　录　G　（资料性附录）　多个上行信道 225
附　录　H　（规范性附录）　HFC 数据传输生成树协议 230
附　录　I　（规范性附录）　错误代码和错误信息 233
附　录　J　（资料性附录）　DOCSIS 传输和争用解决 240
附　录　K　（资料性附录）　IGMP 举例 245
附　录　L　（资料性附录）　主动授权业务 247
参考文献 252

前　言

GY/T 200《HFC网络数据传输系统技术规范》分为如下两部分：

——第1部分：总体要求；

——第2部分：射频接口及协议。

本部分为GY/T 200的第2部分。

本部分修改采用了ITU-T J.112《Transmission Systems for Interactive Cable Television Services》，主要采纳该建议书的附录B（Data-over-cable radio frequency interface）。本部分与ITU-T J.112附录B的主要区别在于，根据标准的先进性原则和我国实际情况，扩展了QoS动态分配机制和有效负载包头抑制技术,删除了原建议书中涉及加密的相关内容,其相关内容在其他标准中另行规定。

本部分的附录A、附录B、附录C、附录D、附录H、附录I为规范性附录，附录E、附录F、附录G、附录J、附录K、附录L为资料性附录。

本部分由全国广播电视标准化技术委员会归口。

本部分起草单位：国家广播电影电视总局标准化规划研究所、国家广播电影电视总局广播影视信息网络中心、歌华有线电视网络股份有限公司、青岛有线电视台、华为技术公司、成都康特电子高新科技公司、中国科学院声学研究所、上海广电股份有限公司、深圳傲龙宽频科技有限公司、中兴通讯有限公司、香港电讯盈科公司、深圳迪科信息技术公司、广东环网公司、创维数字技术有限公司。

本部分主要起草人：金国钧、陈家兴、陈罗光、程伟耀、李熠星、龙永庆、罗晓宏、聂锋、施弛、吴涛、杨宾华、俞迁如、曾春、曾庆军、曾学文、张朝阳。

引　言

本标准的本部分从射频接口的角度，规定了在符合GY/T 106-1999《有线电视广播系统技术规范》和GY/T 180-2001《HFC网络上行传输物理通道技术规范》的网络上建立数据传输系统的物理层、链路层及网络层通信协议，并对QoS动态分配机制、有效负载包头抑制及CMTS与CM的互操作进行了详细描述。它保持了ITU-T J.112/ EuroDOCSIS 1.1的高速数据传输特性和QoS的扩展功能，并兼容EuroDOCSIS 1.0。

HFC 网络数据传输系统技术规范
第 2 部分：射频接口及协议

1 范围

本部分规定了HFC网络数据双向传输系统的物理层、数据链路层及网络层通信协议。

本部分适用于HFC网络数据双向传输系统。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 11595-1999 用专用电路连接到公用数据网上的分组式数据终端设备（DTE）与数据电路终接设备（DCE）之间的接口

GB 13836-2000 电视和声音信号电缆分配系统 第2部分：设备的电磁兼容

GB/T 15629.2-1995 信息处理系统 局域网 第2部分：逻辑链路控制

GB/T 15629.3-1995 信息处理系统 局域网 第3部分：带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范

GB/T 16263-1996 信息处理系统 开放系统互连 抽象语法记法--(ASN.1)基本编码规则规范

GB/T 16646-1996 信息技术 开放系统互连 局域网 媒体访问控制（MAC）服务定义

GB/T 17975.1-2000 信息技术 运动图像及其伴音信息的通用编码 第1部分：系统

GY/T 106-1999 有线电视广播系统技术规范

GY/T 170-2001 有线数字电视广播信道编码与调制规范

GY/T 180-2001 HFC网络上行传输物理通道技术规范

YD/T 1076-2000 接入网技术要求——电缆调制解调器（CM）

ISO/IEC 10038 信息技术——系统间电信与信息交换—局域网—媒体访问控制(MAC)桥

IEC 60728-11 电视和声音信号电缆分配系统 第11部分 安全

ITU-T Z.100 规范和描述语言 (SDL)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本部分。

3.1.1

激活的业务流 active service flow

获得允许可用于数据包传送的从CM到CMTS的业务流。

3.1.2

地址解析协议 address resolution protocol (ARP)

网络地址转换到48位以太地址的IETF协议。

3.1.3

容许的业务流 admitted service flow

预置的或动态告知的业务流，该业务流已被授权且预留了资源，但尚未被激活。

3.1.4

授权模块 authorization module

一个抽象模块，使CMTS能联系该模块以授权业务流和分类器。授权模块通知CMTS，发出请求的CM是否获得所请求的资源授权。

3.1.5

可用性 availability

在有线电视系统中，可用性是指基于假定的误码率（BER），实际RF信道操作时间与预定RF信道操作时间的比（以百分比表示）。

3.1.6

带宽分配映射 bandwidth allocation map

CMTS用来向CM分配发送机会的MAC层管理消息。

3.1.7

桥接协议数据单元 bridge protocol data unit (BPDU)

按ISO/IEC10038规定的生成树协议消息。

3.1.8

广播地址 broadcast addresses

指明所有数据网络业务访问点的预定的目的地址。

3.1.9

突发错误秒 burst error second

任何包括至少100个错误的错误秒。

3.1.10

电缆调制解调器 cable modem (CM)

位于用户端的调制解调器，用于在有线电视系统上进行数据通信。

3.1.11

电缆调制解调器前端系统 cable modem termination system (CMTS)

位于有线电视系统前端或分配中心（hub），它对CM提供互补的功能以便同广域网建立数据连接。

3.1.12

CMTS-网络侧接口 cable modem termination system – network side interface （CMTS-NSI）

CMTS与其网络侧设备之间的接口。

3.1.13

CM 与 CPE 的接口 cable modem to CPE Interface （CMCI）

CM与CPE之间的接口。

3.1.14

分类器 classifier

一组根据TCP、UDP、IP、LLC和/或 802.1P/Q的数据包域用于数据包的匹配标准。分类器把每个数据包映射到一个业务流。CMTS使用下行分类器把数据包分配到下行业务流，CM使用上行分类器把数据包分配到上行业务流。

3.1.15

用户端设备 customer premises equipment (CPE)
在终端用户侧的设备。

3.1.16

数据链路层 data link layer
在开放系统互连（OSI）结构中的第二层，该层提供在开放系统间传输链路上传输数据的业务。

3.1.17

分配中心 distribution hub
位于有线电视网中，它对本区域的本地用户执行前端功能，并从在同一城市或地区的主前端接收部分或所有的电视节目源。

3.1.18

动态主机配置协议 dynamic host configuration protocol （DHCP）
用于分配网络层（IP）地址的因特网协议。

3.1.19

动态范围 dynamic range
最大信号功率和最小信号功率之比。最大信号功率是指在一个多信道模拟传输系统上传送，且不超过失真和其它性能限制的信号功率。最小信号功率是指能利用的不超过噪声、误码率和其它性能限制的信号功率。

3.1.20

终端用户 end user
通过网络提供的服务而接入网络进行通信的个人、组织或通信系统。

3.1.21

错误秒 errored second
任何包括至少一比特错误的1秒间隔。

3.1.22

扩展的子分割 extended subsplit
一种频率分割方案，它允许在单根同轴电缆上双向传输信号。前端的上行信道信号的频率为5MHz到65MHz，前端的下行信道信号频率为从87MHz到上限频率。

3.1.23

保护时间 guard time
在上行中在突发之间分配的最小时间。其参考点是从一个突发的最后一个符号的符号中心到下一个突发的第一个符号的符号中心。保护时间应至少为5个符号加上最大系统定时误差。

3.1.24

前端 headend
在有线电视网络的中心位置，它负责向下行方向发送广播电视信号和其他信号。也可参见主前端或分配中心。

3.1.25

信息单元 information element
构成MAP、定义单独授权、延迟授权等的域。

3.1.26

间隔使用码 interval usage code

MAP和UCD中的一个域，用于把突发特征和授权连接起来。

3.1.27

延迟 latency

以符号的数量表示的时间，用于表示一个信号单元通过一个设备的时间。

3.1.28

层 layer

开放系统互连（OSI）结构的一个子划分，由同一等级的子系统组成。

3.1.29

逻辑链路控制过程 logical link control （LLC）procedure

在一个局域网或城域传输网中，管理数据链路层帧的组装及其在数据站之间的数据交换的协议，它与如何共享传送媒介无关。

3.1.30

主前端 master headend

一个前端，它从不同的信源通过卫星、微波、光纤及其它手段收集电视节目源，并把这些节目源分配到同一个城市或地区的分配中心（Hub）。在它的临近区域，一个主前端也可能对客户执行分配中心的功能。

3.1.31

MAC 地址 media access control (MAC) address

连接到一个共享媒介的设备的内置硬件地址。

3.1.32

媒介访问控制过程 media access control (MAC) procedure

在一个子网中，管理访问与媒介的物理特性无关的传输媒介的协议，但是为了在节点之间能够交换数据，需要考虑子网的拓扑结构。MAC过程包括组帧、错误保护和获取使用底层的传输媒介的权利。

3.1.33

媒介访问控制子层 media access control (MAC) sublayer

数据链路层的一部分，它依赖于拓扑功能并使用物理层业务为逻辑链路子层提供服务。

3.1.34

微时隙 mini-slot

一个微时隙是6.25μs增量的整数倍。微时隙、字节和时间节拍之间的关系如8.3.4条所述。

3.1.35

多点访问 multipoint access

单个网络终端支持多于一个终端设备的用户访问。

3.1.36

多点连接 multipoint connection

在两个以上数据网络终端之间的连接。

3.1.37

网络层 network layer

开放系统互连（OSI）结构的第三层，该层为在开放系统之间建立信道提供业务。

3.1.38

网络管理 network management

与数据链路层和物理层资源以及其在HFC系统支持的数据网络上的台站等的管理有关的功能。

3.1.39

唯一组织标识符 organizationally unique identifier （OUI）

是由IEEE分配的3个8位组的标识符。根据IEEE 802，产生通用的局域网MAC地址和协议标识符，以供在局域网和城域网应用中使用。

3.1.40

包标识符 packet identifier （PID）

一个唯一的整数值，在单个或多个节目的MPEG-2流中标识一个节目的基本流。

3.1.41

部分授权 partial grant

一个比CM请求带宽小的授权。

3.1.42

有效负载包头抑制 payload header suppression （PHS）

有效负载数据包中的包头抑制（例如，在转发的数据包中抑制以太包头）。

3.1.43

有效负载单元起始指示符 payload unit start indicator （PUSI）

MPEG包头中的一个标志。值为1表示指针域存在，并为有效负载的第一个字节。

3.1.44

物理层 physical（PHY）layer

开放系统互连（OSI）结构的第一层。该层在开放系统之间的传输链路上提供服务，以传送比特或比特组，并且该层详细地规定了各种电气的、机械的和握手的过程。

3.1.45

物理媒介依从（PMD）子层 physical media dependent (PMD) sublayer

物理层的一个子层，涉及在开放系统之间特定的传输链路上传送比特或比特组，并且该层详细地规定了各种电气的、机械的和握手的过程。

3.1.46

基本的业务流 primary service flow

所有的CM都有一个基本的上行业务流和一个基本的下行业务流。它们确保CM总是可管理的，并且为没有分类到任何其它业务流的转发的数据包提供一个缺省的通道。

3.1.47

预置的业务流 provisioned service flow

一个业务流，已经被预置作为注册过程的一部分，但还没有被激活或者被容许。在容许之前，它可能仍需与一个策略模块或者外部策略服务器进行授权交换。

3.1.48

QoS 参数集 QoS parameter set

描述一个业务流或者一个业务类别的业务属性质量的业务流编码集，见附录C.2.2.5。

3.1.49

路由信息协议 routing information protocol(RIP)

一个IETF协议，用来交换IP网络和子网的路由信息。

3.1.50

业务接入点 service access point(SAP)
由一个层或子层向紧邻的上一层提供业务的点的位置。

3.1.51

安全关联标识符 security association identifier
在CMTS和CM之间的一个加密安全标识符

3.1.52

业务类别 service class
在CMTS中命名和配置的一组排队和调度属性。业务类别用业务类别名称来标识。一个业务类别有一个相关的QoS参数集。

3.1.53

业务类别名 service class name
一个ASCII字符串，在CM配置文件和协议交换中通过它引用业务类别。

3.1.54

业务数据单元 service data unit(SDU)
在对等业务接入点之间，作为一个单位传送的信息。

3.1.55

业务流 service flow
一个MAC层的传输业务：

- 提供从上层业务实体到 RF 的单向数据包传输；
- 根据为该业务流定义的 QoS 流量参数，整形、监管并为流量划分优先级。

3.1.56

业务流标识符 service flow identifier(SFID)
由CMTS分配给业务流的标识符，长度为32比特。

3.1.57

业务标识符 service identifier (SID)
由CMTS分配给一个激活的或容许的上行业务流、除业务流标识符（SFID）之外的业务流标识符，长度为14位比特。

3.1.58

业务流参考 service flow reference
在配置文件和动态业务MAC消息中的一个消息参数，用于把消息中的分类器和其它对象与被请求业务流的业务流编码联系起来。

3.1.59

子层 sublayer
在开放系统互连(OSI)参考模型中一个层的子划分。

3.1.60

子网 subnetwork
是相邻节点和传输链路的物理连接。

3.1.61

子网访问协议 subnetwork access protocol (SNAP)
LLC包头的一个扩展，以便可以把802-类型网络用作IP网络。

3.1.62

时间节拍 tick

6.25μs的时间间隔，用作上行微时隙定义和上行传输时间的参考。

3.1.63

传送延时 transit delay

从PDU的第一比特通过一个指定边界到同一PDU的最后比特通过第二个指定边界之间的时间差。

3.1.64

传输会聚子层 transmission convergence sublayer

物理层的一个子层，它提供数据链路层和PMD子层之间的接口。

3.1.65

简单文件传送协议 trivial file-transfer protocol(TFTP)

一个用来传送文件的Internet协议，不需要用户名和密码。通常用于自动下载数据和软件。

3.1.66

类型/长度/值 type /length/value (TLV)

一种三个域的编码，其中第一个域指信息单元的类型，第二个域指信息单元的长度，第三个域指信息单元的值。

3.1.67

上行信道描述符 upstream channel descriptor (UCD)

MAC管理消息，用于向CM传送上行物理层的特性参数。

3.2 缩略语

下列缩略语适用于本部分。

ARP Address Resolution Protocol 地址解析协议

ATM Asynchronous Transfer Mode 异步转移模式

BPDU Bridge Protocol Data Unit 桥接协议数据单元

CBR Constant Bit Rate 固定比特率

CCCM CPEcontrolled CM CPE控制的CM

CM Cable Modem 电缆调制解调器

CMCI Cable Modem to CPE Interface CM同CPE的接口

CMTS Cable Modem Termination System 电缆调制解调器前端系统

CMTS-NSI Cable Modem Termination System – Network Side Interface CMTS-网络侧接口

CNT Concatenation 级联

CPE Customer Premises Equipment 用户端设备

CSO Composite Second Order Beat 复合二次差拍

CTB Composite Triple Beat 复合三次差拍

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

EHDR Extended Header 扩展包头

ELEN Extended Header length 扩展包头长度

FC Frame Control 帧控制

FDDI Fiber Distributed Data Interface 光纤分配数据接口

HCS Header Check Sequence 包头校验序列

ICMP Internet Control Message Protocol Internet 控制消息协议

IE Information Element 信息元

IEEE Institute of Electrical and Electronic Engineers 电子电气工程师学会
IETF Internet Engineering Task Force Internet工程任务组
IGMP Internet Group Management Protocol Internet组播管理协议
IUC Interval Usage Code 间隔使用码
LLC Logical Link Control Procedure 逻辑链路控制过程
MAC Media Access Control 媒介访问控制过程
MSAP MAC Service Access Point MAC业务接入点
OSI Open System Interconnection 开放系统互连
OUI Organizationally Unique Identifier 唯一组织标识符
PDU Packeted Data Unit 打包的数据单元
PHS Payload Header Suppression 有效负载包头抑制
PHSF Payload Header Suppression Field 有效负载包头抑制域
PHSI Payload Header Suppression Index 有效负载包头抑制索引
PHY Physical Layer 物理层
PID Packet Identifier 包标识符
PMD Physical Media Dependent Sublayer 物理媒介依从子层
PUSI Payload Unit Start Indicator 有效负载单元起始指示符
REQ Request 请求
RFI Radio Frequency Interface 射频接口
SAID Security Association Identifier 安全关联标识符
SAP Service Access Point 业务接入点
SFID Service Flow Identifier 业务流标识符
SID Service Identifier 业务标识符
SNAP Subnetwork Access Protocol 子网访问协议
SNMP Simple Network Management Protocol 简单网络管理协议
TFTP Trivial File-Transfer Protocol 简单文件传送协议
TLV Type/Length/Value 类型/长度/值
UCC Upstream Channel Change 上行信道变更
UCD Upstream Channel Descriptor 上行信道描述符
UDP User Datagram Protocol 用户数据报协议
XID Exchang Identification command 交换识别指令

4 通讯协议

本章简要介绍HFC网络数据传输系统中应使用的高层通讯协议。有关与物理介质、下行传输和媒介访问控制子层的详细技术要求则分别在第5章、第6章、第7章予以说明。

4.1 协议栈

CM和CMTS可作为转发代理运行，也可作为末端系统（主机）运行。不同的运行模式所使用的协议栈有所不同。

电缆调制解调器系统的主要功能是在前端和用户端之间透明地传送IP信息包，IP协议上还包含着某些管理功能。HFC网络上的协议栈如图1所示。

4.1.1 作为主机的 CM 和 CMTS

CM和CMTS将按照IEEE 802作为IP和LLC主机来运行，通过HFC网络进行通信。在CM和CMTS RF接口上的协议栈如图1所示。

CM和CMTS应作为IP主机来工作。这样CM和CMTS应支持DIX链路层组帧（见DIX）上的IP和ARP。CMTS不应在下行信道中传输小于DIX最小值64字节的帧。然而，CM可以在上行信道中传输小于DIX最小值64字节的帧。

CM和CMTS也可以支持SNAP组帧（见RFC-1042）上的IP和ARP。

CM和CMTS还应作为LLC主机来工作。因此CM和CMTS应按照GB/T 15629.2适当地响应TEST和XID的请求。

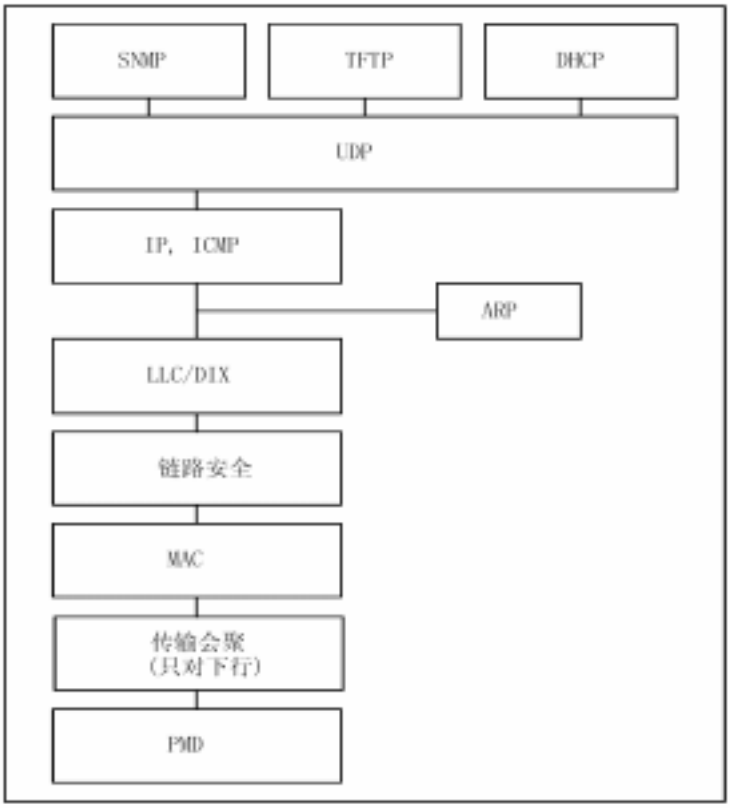


图1　射频接口上的协议栈

4.1.2　通过 CM 和 CMTS 的数据转发

4.1.2.1　概要

通过CMTS的数据转发可以是透明桥方式，或者也可以使用网络层转送方式（路由选择、IP交换），如图2所示。

通过CM的数据转发是如图2所示的链路层透明桥方式。传输规则类似于经过修改的ISO/IEC 10038，修改的内容在4.1.2.2和4.1.2.3中予以介绍。这里允许支持多种网络层。

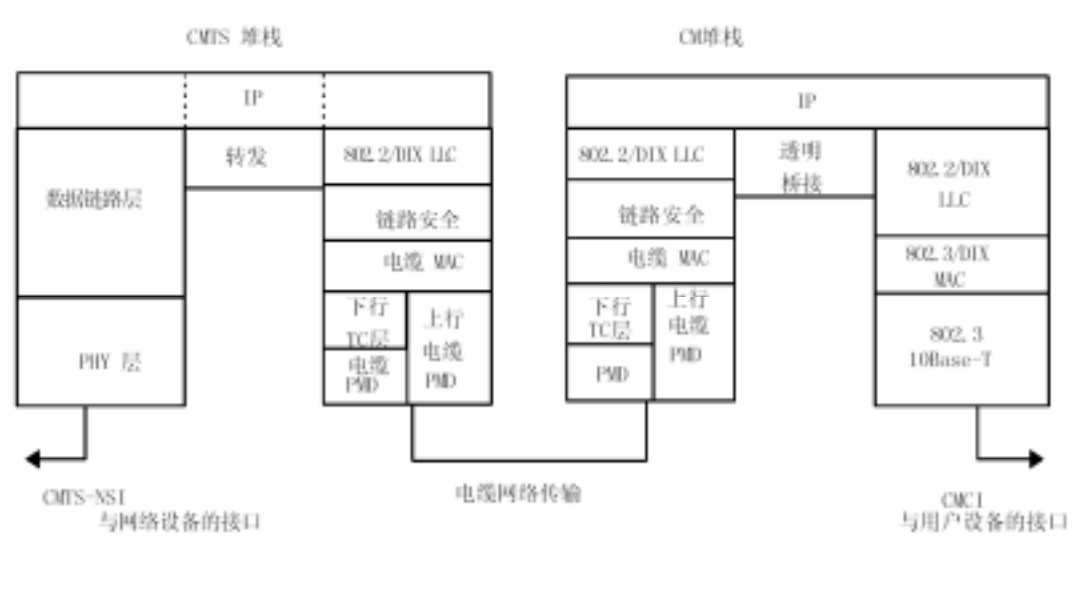


图2　通过 CM 和 CMTS 转发数据示例

CM和CMTS应支持对IP业务的转发，同时也可以支持其它网络层协议。应具备把网络层限制为单一协议（例如IP）的能力。

用于住宅区的CM可支持按附录H中所介绍的修改过的ISO/IEC 10038 802.1d生成树协议。用于商业目的CM应支持这一版本的生成树。CM和CMTS应具有过滤（和忽略）802.1d BPDU的能力。

本部分假设用于住宅区的CM不会被连接成如图3所示的网络环路结构。

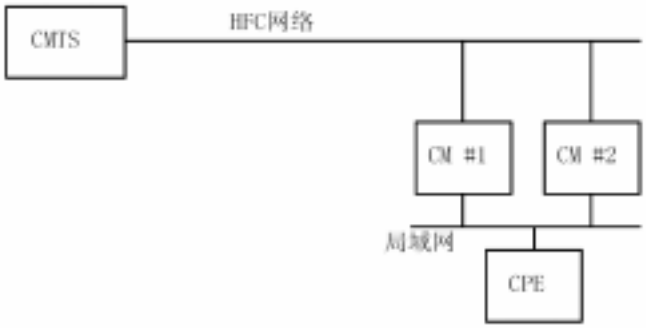


图3　网络环路示例情况

4.1.2.2　CMTS 转发规则

在CMTS中，如果使用链路层转发，那么它应遵循如下的通用802.1d规则。

- 链路层帧不能被复制；
- 陈旧的帧（那些不能被及时传送的帧）应被丢弃；
- 在给定的业务流（见 7.1.2.3）中，链路层的帧应按其接收顺序传送。

所使用的地址学习和刷新机制由厂家确定。

如果使用网络层转发，那么CMTS在CMTS-RFI和CMTS-NSI接口方面应当符合IETF路由器的要求（见RFC-1812）。

从概念上讲，CMTS在两个抽象的接口上传输数据包：即在CMTS-RFI和CMTS-NSI之间和在上行和下行信道间。CMTS可以在这两个接口中使用链路层（桥接）和网络层（路由分配）语义的任意组合。在两个接口中使用的方法不必相同。

在MAC层里，上行和下行信道之间的传输和传统的LAN传输有所不同，这表现在如下几个方面：

- 单信道是单工的，对于大多数协议功能（例如：802.1 d 生成树，按 RFC-1058 的路由信息协议）来说，不能完全看作是一个接口；
- 上行信道本质上是点对点的，而下行信道则是介质共享的；
- 策略决定可以取代所有的连接。

由于这些原因，在CMTS中存在一个称为MAC转发器的抽象实体，以便在一个MAC域内的站点之间提供连接性（见4.2）。

4.1.2.3 CM 转发规则

通过CM的数据转发是带有下面这些特殊规则的链路层桥接。

4.1.2.3.1 CPE MAC 地址获得

CPE MAC地址获得遵循以下规则：

- CM 应获得已连接的 CPE 装置的以太网 MAC 地址，该地址可以通过预置的方式获得也可以通过学习的方式获得，直到 CM 获得其最大数目（为一个由具体设备决定的值）的 CPE 地址为止。一旦 CM 获得了它最大数目的 CPE MAC 地址，那么新发现的 CPE MAC 地址不能替换以前获得的地址。CM 应支持至少获得一个 CPE MAC 地址；
- 在预置过程中（直到最大数目的 CPE 地址），CM 应允许 CPE 地址的配置，以支持不适合使用学习方式或者不希望采用学习方式时的配置；
- 在 CM 预置地址过程中所提供的地址应优先于学习到的地址；
- CPE 地址不应被更新；
- 为允许修改用户 MAC 地址或移动 CM，地址不应保存在非易失性存储器中。当 CM 复位时（如上电周期），所有预置过程提供的和学习到的地址都应被丢弃。

4.1.2.3.2 转发

在两个方向上的CM转发应遵循如下的802.1d规则：

- 链路层帧不应被复制；
- 陈旧的帧（那些不能被及时传送的帧）应被丢弃；
- 在给定的业务流（见 7.1.1.3）中的链路层帧应按其接收的顺序传送。

电缆网到以太网的转发应遵循下列的特定规则：

- 未知目的地址的帧不应从电缆端口向以太网端口转发；
- 广播帧应转发到以太网端口；除非这些帧的源地址是预置的或学习到的 CPE 设备的地址，在这种情况下这些帧不应被转发；
- 组播的传输由设定策略过滤服务参数和特定的组播跟踪算法共同控制（见 4.3.1）。只有同时采用这两种机制时，组播帧才能被转发。

以太网到电缆网的转发应遵循下列的特定规则：

- 未知目的地址的帧应从以太网端口向电缆端口转发；
- 广播帧应向电缆端口转发；
- 组播帧应按照运营商的操作和业务支持系统所规定的过滤配置设定值向电缆端口转发；
- 来自所支持 CPE 设备的预置的或学习到的地址之外的源地址的帧不应转发；
- 如果单用户 CM 已经获得了一个 MAC 地址（见 4.1.2.3.1），则不应转发来自第二个源地址的数据。其它（不支持的）CPE 源地址应从以太网端口学习得到，并且用这一信息来过滤本地通信业务；
- 如果单用户 CM 已经获得了 MAC 地址 A 作为它支持的 CPE 设备，并学习到 B 作为连接到以太网端口的第二个设备，则该 CM 应过滤从 A 到 B 的任何通信业务。

4.2 MAC 转发器

MAC转发器是一个位于CMTS之上、MSAP之下的MAC子层，如图4所示。MAC转发器负责将上行帧转发到：

- 一个或多个下行信道；
- MSAP 接口。

图4中，HFC网络中上行和下行信道的LLC子层和链路安全子层终止于MAC转发器处。

MSAP接口的使用者可以是NSI—RFI转发过程或CMTS的主机协议栈。

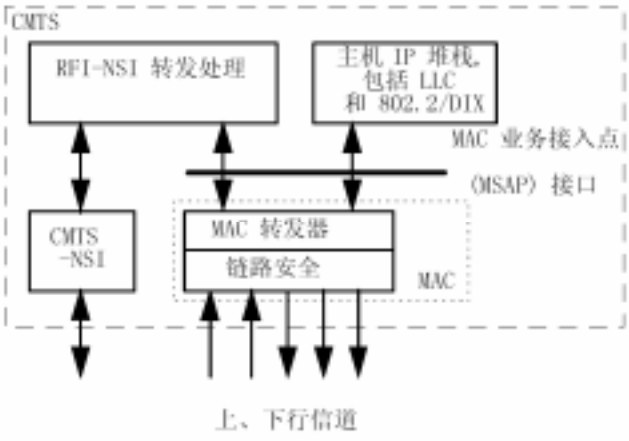


图4　MAC 转发器

帧的传送可以基于数据链路层（桥接）语义、网络层（路由分配）语义、或其组合，也可以使用高层语义（如对UDP通道端口号码的过滤）。CMTS应在连接到CM上的各主机之间提供IP连接，而且这种连接应以一种符合连接到以太网上的用户设备所要求的方式来进行。例如，CMTS应转发ARP包，或者使用代理ARP业务。CMTS MAC转发器也可以为非IP协议提供业务。

本部分并不要求所有上行和下行信道都如图4所示聚集在一个MSAP之下，厂商也可以选择应用多个MSAP，每个MSAP有一个上行和下行信道。

数据链路层转发规则

本条中的要求适用于MAC转发器仅使用数据链路层语义的情况。

帧的传送取决于该帧内的目的地址。学习每个地址的方法可由厂商确定，包括：

- 类似于透明桥接的源地址学习和刷新；
- 从 MAC 注册请求消息中收集；
- 管理设置的方法。
- 如果某一帧的目的地址是单播地址，且该地址与一个特定的下行信道相联系，那么此帧应转发到该信道。

注：厂商可以使用类似于802.1d/ISO 10038桥接中所述的静态地址的扩展方式，此种方式按其它的方法过滤或处理这样的帧。

如果某一帧的目的地址是单播地址，并且该地址位于MSAP接口的另一侧（上一层），则此帧应转发到MSAP接口。

如果目的地址是广播、组播、或未知的地址，则此帧应转发到MSAP和所有的下行信道。（4.3.1.1多信道传输规则除外）

注：组播是指所有的组播，包括802.1d/ISO 10038生成树桥接BPDU。

传送规则与透明桥接的传输规则类似：

- 帧不应被复制；
- 不能及时传送的帧应丢弃；
- 帧校验序列应予保留而不应重新生成；
- 在给定的业务流（见 7.1.2.3）中的帧应按其接收的顺序传送。

4.3 网络层

网络层协议是RFC—791所规定的互联网协议（IP v4），并将过渡至IP v6。

本部分对IP数据包的重组不做强制要求。

IGMP管理要求

对IGMP的支持有两种方式适用于CM和CMTS。第一种为被动模式，设备基于已知的用户端组播会话活动状态来选择转发IGMP（在附录K中给出一例），在被动模式下设备基于在4.3.1.1条中的规则推导出其IGMP定时。第二种模式为主动模式，设备基于已知的用户端组播会话活动状态来结束和开始IGMP。主动模式常指IGMP代理执行端或组播路由器。

主动和被动的IGMP设备都应支持IGMPv2（见RFC-2236）。

4.3.1 IGMP 定时器要求

以下IGMP定时器要求仅适用于设备（CM和CMTS）工作在被动IGMP模式：

- 设备不应对相关联的组播定时器值有任何特定配置要求，并且应遵循本条规定的定时器；
- 设备可提供配置控制取代这些定时器的缺省值；
- 设备应通过查看成员资格查询消息到达的时间间隔来推算成员资格查询间隔（Membership Query Interval）。公式表示：若 n＜2，MQI=125，否则，MQI=MAX（125，MQ_n - MQ_{n-1}），其中 MQI 为成员资格查询间隔，以秒为单位，n 为所看到的成员资格查询消息数，MQ_n是看到第 n 个成员资格查询的时间点，并计算到最接近的秒数；
- 查询响应间隔被携带在成员资格查询包中，若在成员资格查询包中未设定（或设定为零），则应假定为 10s。

4.3.2 CMTS 规则

CMTS规则如下：

- 如果使用了链路层转发组播包，CMTS 应使用适当的 802.3 组播组（例如：01:00:5E: XX:XX:XX，其中 XX:XX:XX 为用十六进制符号表示的组播地址的低 23 位，参见[IMA]）来转发所有下行信道中的所有成员资格查询（Membership Queries）；
- CMTS 应将其在上行 RF 接口上接收到的对任意给定组的请求及非请求成员资格报告的第一副本传送到其所有的下行 RF 接口。如果成员资格是按照下行 RF 接口来管理的，成员资格报告和 IGMP v2 Leave 消息只能传送到报告该 CPE 的 CM 所连接的下行接口；
- 至少在查询响应期间内，CMTS 应当禁止附加成员资格报告（对于任意给定组）的下行传输。如果 CMTS 使用数据链路层传输，则应将成员资格报告传送出所有适当的网络边界接口；
- CMTS 应当禁止向下行 RF 接口没有用户的（受到管理控制）IP 组播组传输下行通信业务；
- 如果 CMTS 进行组播信息包的网络层转发，则应支持 IGMP 主动模式；
- 如果使用了链路层转发组播包，CMTS 应支持 IGMP 被动模式，也可以支持 IGMP 主动模式。

4.3.3 CM 规则

为支持IGMP，CM应遵循下列规则。

CM应实现被动IGMP模式，也可实现主动IGMP模式；若采用主动模式，则应支持在两者间切换。组播转发要求如下：

a) 下列要求对主动和被动 IGMP 模式都适用：
   1) CM 不应从其 CPE 接口向其 RF 接口传送成员资格查询；
   2) CM 不应将从其 RF 接口接收到的成员资格报告或 IGMP v2 Leaves 传送到其 CPE 接口；
   3) CM 不应将组播信息从其 RF 接口传送到其 CPE 接口，除非其 CPE 接口上的设备是该 IP 组播组的一个成员；
   4) CM 应将组播信息从其 CPE 接口传送到其 RF 接口，除非在管理上（通过配置或其它机制）已将其禁止；

5) 在 CPE 接口上收到成员资格报告后，CM 应开始向适当的 IP 组播组转发。一旦 CM 未收到来自 CPE 的成员资格报告的时间超过成员资格时间间隔，CM 应停止传送从 RF 到 CPE 的组播信息，这里成员资格时间间隔为（2×MQI）+QRI，其中 MQI 是成员资格查询时间，QRI 是查询响应时间；

6) 若 CM 能判定（如通过 IGMP LEAVE 消息和适当的协议交换）没有 CPE 设备属于某特定组，CM 可在成员资格间隔时间（如上所述）超时之前针对该特定组停止从 RF 侧向 CPE 侧转发组播信息。

b) 以下要求只在 CM 工作于被动 IGMP 模式时适用：

1) CM 应将所有主机组播组的通信信息从其 CPE 接口传送到其 RF 接口，除非在管理上已将其禁止。CPE 应始终被看作是这个组的一个成员。CM 应将所有通过其 RF 接口上许可过滤的主机组查询转发到其 CPE 接口；

2) 一旦在 CPE 接口上收到成员资格报告，CM 应开启 0 到 3 秒的随机定时器，在此期间，CM 应丢弃在 CPE 接口上收到的相关组播组的任何另外的成员资格报告。若 CM 从 HFC 接口上收到相关组的成员资格报告，CM 应丢弃在 CPE 接口上收到的成员资格报告。若随机定时器超时还未收到 HFC 接口来的成员资格报告，CM 应发送在 CPE 接口侧所收到的成员资格报告。

c) 下列要求只在 CM 工作于主动 IGMP 模式时适用：

1) CM 应在其 RF 接口上对有活动组的 CPE 实现 IGMP v2 协议 RFC—2236 规定的主机部分，且不应作为其 RF 接口上的一个查询方；

2) 在 CPE 接口上，CM 应作为 IGMP v2 查询方；

3) 如果在查询响应时间间隔内 CM 在其下行 RF 接口上接收到在 CM 的 CPE 接口上活动组的成员资格报告，则应禁止在上行 RF 接口中传送从该组的 CPE 接口上收到的所有成员资格报告；

4) CM 应抑制该组的所有后续的成员资格报告，直到 CM 在其 RF 接口上收到一个成员资格查询（通用的或者专门对该组的）或者从 CPE 接口接收到该组的 IGMP v2 Leave 消息为止；

5) CM 应把来自 CPE 的非请求成员资格报告（IGMP JOINs）当作对在其 RF 接口上接收到的成员资格查询的响应来对待。收到来自 CPE 接口的 JOIN 消息之后，CM 应按照 RFC－2236 中规定的主机状态图启动一个随机定时器，而且应使用 3s 的查询响应间隔。正如上面所规定的那样，如果在此随机时间内 CM 在其 RF 接口上接收到该组的成员资格报告，则应抑制在其上行 RF 接口上传输此 JOIN 消息。

注： 本条的规定并未禁止对CM进行特定的配置，使之根据网络策略不转发某些组播业务。

4.4 在网络层之上

用户可以使用透明IP性能作为更高层业务的载体。对于CM来说使用这些业务是透明的。

除了传送用户数据以外，还有一些依赖于网络层的网络管理和操作的性能。这些性能包括：

- 应支持 SNMP（简单网络管理协议，参见 RFC－1157），用于网络管理；
- 应支持 TFTP（简单文件传送协议，参见 RFC－1350），用于下载操作软件和配置信息，由 TFTP 超时间隔和传送文件大小的选项（参见 RFC－2349）对协议进行修改；
- 应支持 DHCP（动态主机配置协议，参见 RFC－2131），用于在 TCP/IP 网络上将配置信息传送到主机的帧结构；
- 应支持 ToD（Time of Day）协议（参见 RFC－868），用来获得时间。

4.5 数据链路层

数据链路层分为若干子层（见IEEE 802），此外还有附加的链路层安全性能。从上向下各子层依次是：

- 逻辑链路控制（LLC）子层（只有类型 I）；
- 链路层安全子层；
- 媒介访问控制（MAC）子层。

4.5.1 LLC 子层

应按照GB/T 16646的规定提供LLC子层。应参考RFC－826中的规定来解析地址。MAC到LLC的服务定义见GB/T 16646的规定。

4.5.2 链路安全子层

链路安全子层所遵从的标准待定。

4.5.3 MAC 子层

MAC子层为每个下行信道定义单个发送者——CMTS。所有CM都侦听它们已注册的下行信道上传送的所有的帧，并接受那些目的地与CM本身相符的帧或者各CPE通过CMCI口达到的帧。各CM只能通过CMTS与其它CM通信。

上行信道具有多个发送者（CM）和一个接收者（CMTS）的结构。上行信道里的时间是时隙，按规定的时间标记提供时分多址（TDMA）。CMTS提供时间参考，并控制每个间隔的合法使用。可以将时间间隔分配给特定的某些CM来传输，或者供所有CM争用。CM可以争用请求传输时间。在一定的范围内，CM也可以争用传输实际数据。在两种情况下，都会发生碰撞，并采用重试的方法解决。

第7章介绍了来自CMTS的MAC子层的消息，规定了CM在上行信道上的行为，以及从CM向CMTS传送的消息。

MAC子层服务的定义参见附录E。

4.6 物理层

物理层（PHY）由两个子层组成：

- 传输会聚子层（仅出现在下行方向）；
- 物理媒介依从（PMD）子层。

4.6.1 下行传输会聚子层

下行传输会聚子层只存在于下行方向，为在物理层比特流上传送附加的服务提供机会。这些附加的服务包括数字视频等，本部分不作详细规定。

该子层定义为连续的188字节MPEG（见GB/T 17975.1）信息包流，每一个信息包由4字节包头和184字节有效负载组成。该包头可以识别出有效负载属于HFC数据MAC。不同的包头值表示不同类型的有效负载。有效负载的混合方法是任意的，并由CMTS控制。

下行传输会聚子层在本部分的第6章中予以定义。

4.6.2 PMD 子层

PMD在本部分的第5章中予以定义。

接口点

三个RF接口点在PMD子层中予以规定：

- 在 CMTS 的下行输出；
- 在 CMTS 的上行输入；
- CM 的电缆输入/输出。

为了与前端中典型的下行和上行信号混合和分割安排方法兼容，在CMTS上要有分开的下行输出和上行输入接口。

5 物理媒介依从子层（PMD）规范

本章定义CM和CMTS的电气特性和协议。本章的目的是定义CM和CMTS的互操作性，使任何一个CM都能与任何CMTS一起工作。

5.1 上行

5.1.1 概述

上行PMD子层使用FDMA/TDMA突发调制方式，提供5种符号率和2种调制方式(QPSK和16QAM)。调制方式包括增强频谱效率的脉冲整形、灵活的载波频率和可选的输出功率电平。PMD子层格式包括一个可变长度的调制突发，该突发在以6.25μs(最高速率为16个符号)的整数倍为间隔的边界用准确的定时开始。

每个突发都支持灵活的调制方式、符号率、前同步码、有效负载随机化及可编程FEC编码。

所有上行传输参数均由CMTS通过MAC消息来设置，许多参数是逐个突发可编程的。

PMD子层能支持近似连续方式的传输，一个突发的下降沿可以与后一个突发的上升沿相交，这就使传输的包络永远不是零。来自不同CM的TDMA传输的系统定时，应在一个突发的最后一个符号的中心与紧随其后突发的前同步码的第一个符号的中心之间提供至少有5个符号的间隔。保护时间应大于或等于5个符号加上最大定时误差。定时误差是由CM和CMTS共同造成的。CM的定时性能在5.1.7、5.1.8和5.2.7等条中规定。不同厂商的CMTS的最大定时误差和保护时间可以不同。

上行调制器是CM的一部分，并与HFC网络对接。调制器包含实际的电平调制功能和数字信号的处理功能，后者提供FEC、前同步码预置、符号映射及其它处理步骤。本条考虑了在信号处理部分缓冲突发的概念。在信号处理部分：

a) 一次接收一个突发信息流；

b) 将该信息流处理成一个完整的突发符号进入调制器；

c) 在准确的突发传送时刻，将正确定时的突发符号流馈给一个无记忆的调制器。

调制器的无记忆部分只完成脉冲整形和正交上变频。

与调制器一样，解调器有两个基本功能：解调功能和信号处理功能。与调制器不同的是，解调器在CMTS内，并且本部分规定，每个使用的载波频率都可解调(不必是一个实际的物理解调器)，即在一个给定频率上能解调接收所有的突发符号。

注： 前端的整体设计应考虑到解调和信号处理的多信道特征，优化和共享适用于多信道应用的部分。

解调器的解调功能接收以规定的功率电平为中心的可变电平信号，并完成符号定时、载波恢复和跟踪、突发识别及解调。另外，解调功能提供与参考边界相关的突发定时估计、接收信号功率的估计、信噪比的估计及使用自适应均衡来缓解电缆网络中的回波、窄带干扰和群时延带来的影响。

解调器的信号处理功能与调制器的信号处理功能相反。包括接收已解调的突发数据流和解码等，以及将来自多信道的数据复用为一个单独的输出流。信号处理功能还提供边界定时参考和解调器的选通启动信号，以激活每一个分配突发时隙的突发获取。信号处理功能还可以提供成功解码的指示、解码误差或对每个码字的解码失败及在每个码字中的Reed-Solomon符号校正数。对于每个上行突发，CMTS能在符号中预知确切的突发长度(见5.1.6，5.1.10.1和附录A.2)。

5.1.2 调制方式

上行调制器应提供QPSK和16QAM两种调制方式。

上行解调器应支持QPSK和16QAM两种调制方式。

5.1.2.1 调制速率

上行调制器应提供QPSK和16QAM的160ksym/s、320ksym/s、640ksym/s、1280ksym/s及2560ksym/s的调制速率。

该调制速率的多样性和在设置上行载波频率时的灵活性，可允许操作员在窄带干扰分布的隙缝间设置载波。

每个上行信道的符号率在上行信道描述符(UCD)的MAC消息中定义。所有使用该上行信道的CM应使用所定义的符号率来进行传输。对于每个上行频率，上行符号率应固定。

5.1.2.2 符号映射

调制方式(QPSK或16QAM)是可编程的。每种方式中传输的符号和输入到I，Q座标的比特映射应如表1所规定。表1中，I_1是符号映射的MSB，Q_1是QPSK的LSB，Q_0是16QAM的LSB。在16QAM中Q_1和I_0位于中间。MSB应是串行数据中的首位进入符号映射器。

表1　I/Q 映射

调制方式	输入数位定义
QPSK	I_1 Q_1
16QAM	I_1 Q_1 I_0 Q_0

上行QPSK符号映射应如图5所示。

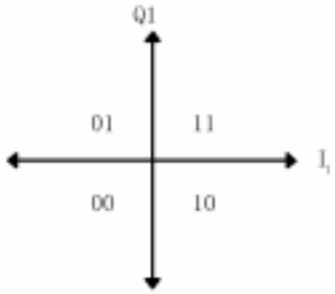


图5　QPSK 符号映射

16QAM非反转（格雷码）符号映射应如图6所示。

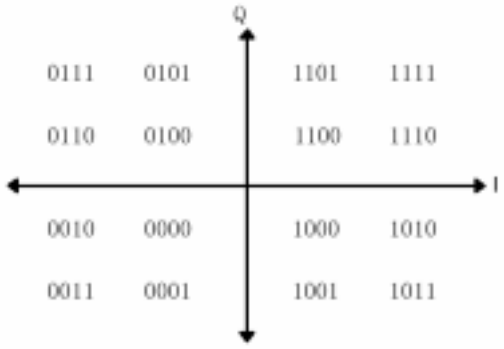


图6　16QAM 格雷码符号映射

16QAM差分编码符号映射应如图7所示。

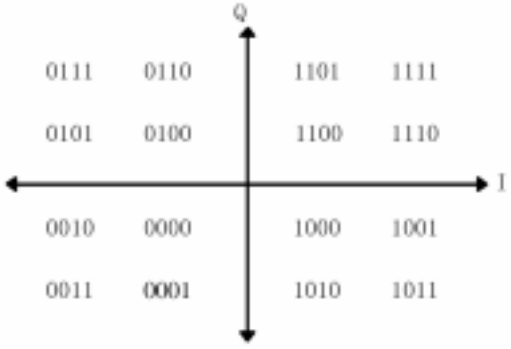


图7　16QAM 差分编码符号映射

如果允许差分象限编码，则当前传输符号象限取决于前一个传输符号象限和当前输入的比特值，如表2所示。

表2　符号象限生成表

当前输入比特I(1)Q(1)	象限相位变化	前一个传输符号的MSB	当前传输符号的MSB
00	0°	11	11
00	0°	01	01
00	0°	00	00
00	0°	10	10
01	90°	11	01
01	90°	01	00
01	90°	00	10
01	90°	10	11
11	180°	11	00
11	180°	01	10
11	180°	00	11
11	180°	10	01
10	270°	11	10
10	270°	01	11
10	270°	00	01
10	270°	10	00

5.1.2.3　频谱整形

上行PMD子层应支持25%奈奎斯特升余弦平方根整形。

占用频谱不应超出表3所示的信道带宽。

表3　最大信道带宽

符号速率 ksym/s	信道带宽 kHz[a]
160	200
320	400
640	800
1280	1600
2560	3200
a 信道带宽为-30dB 带宽	

5.1.2.4　上行频率调整及范围

上行PMD子层应工作在5MHz~65MHz频率范围内。频率偏移应在±32kHz范围内(±10Hz范围内，增量=1Hz)。

5.1.2.5　频谱格式

上行调制器运行应符合式（1）。

$$s(t)=I(t).\cos(\omega t)-Q(t).\sin(\omega t) \quad \cdots\cdots (1)$$

其中t代表时间，ω代表角频率。

5.1.3　FEC 编码

5.1.3.1　FEC 编码方式

上行调制器应能提供：在GF(256)上的Reed-Solomon码，其中T=1到10或无FEC编码。

应支持如下的Reed-Solomon码生成多项式，见式（2）。

$$g(x)=(x+\alpha^{0})(x+\alpha^{1})...(x+\alpha^{2T-1}) \quad \cdots\cdots (2)$$

其中本原元素α是十六进制的0x02。

应支持如下的Reed-Solomon码本原多项式，见式（3）。

$$p(x)=x^{8}+x^{4}+x^{3}+x^{2}+1 \quad \cdots\cdots (3)$$

上行调制器应提供码字从最小18字节(对于T=1误码校正，为16个信息字节［k］加上2个奇偶字节)到最大255字节(k字节加奇偶字节)，未编码字最小为1字节。

在截短的最后码字方式中，CM应提供按每个码字k字节指配长度缩短的一个突发的最后码字，如5.1.11.1.2所示。

T值应在CMTS对上行信道描述符的响应中设置。

5.1.3.2 FEC 比特到符号排序

Reed Solomon编码器的输入是来自CM MAC子层的串行比特流，且该数据流的第一位应映射到进入编码器的第一个Reed Solomon符号的MSB。编码器输出的第一个符号的MSB应映射到送往扰码器的串行比特流的第一位扰码器。

注： MAC字节到串行的上行数据流字节的LSB被映射进入串行比特流的第一位，见7.2.1.3条。

5.1.4 扰码器(随机化发生器)

上行调制器应实现扰码功能(如图8所示)，其15比特扰码种子值应是任意可编程的。

在每个突发发送开始，寄存器被清除，种子值被装入。种子值用于计算扰码比特，扰码比特在异或器（XOR）中与每个突发(前同步码后的第一个符号的MSB)数据的第一个比特相异或。扰码器种子值应在CMTS响应的上行信道描述符中设置。

其多项式见式（4）。

$$x^{15}+x^{14}+1 \quad \cdots\cdots (4)$$

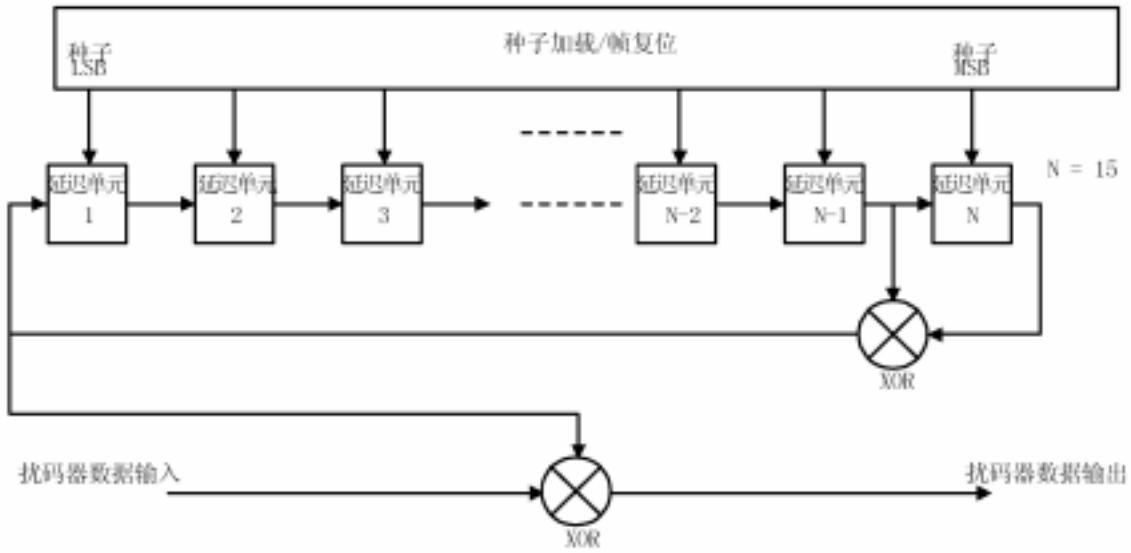


图8 扰码器的结构

5.1.5 前同步码预置

上行PMD子层应支持可变长度的前同步码域，该域是针对经随机化处理和Reed Solomon编码后的数据预置的。

前同步码模式的第一位是进入符号映射器的第一位(见图13)，且是在突发中第一个符号的I_1(见5.1.2.2)。前同步码模式的第一位由前同步码值偏移指定，见表35。

预置的前同步码值应是可编程的，其长度应是QPSK时的0，2，4，……或1024比特及16QAM时的0，4，8，……或1024比特。因此，前同步码的最大长度是512个QPSK符号或256个QAM符号。

前同步码的长度和值应在CMTS发送的上行信道描述符消息的响应中配置。

5.1.6　发送预均衡器

发送预均衡器结构是线性的，如图9所示，应由CM在响应CMTS发送的测距响应(RNG-RSP)消息时进行配置。预均衡器应支持一个符号(T)间隔、8个抽头的均衡器结构。预均衡器每个符号1～4个取样点，抽头长度要大于8个符号。

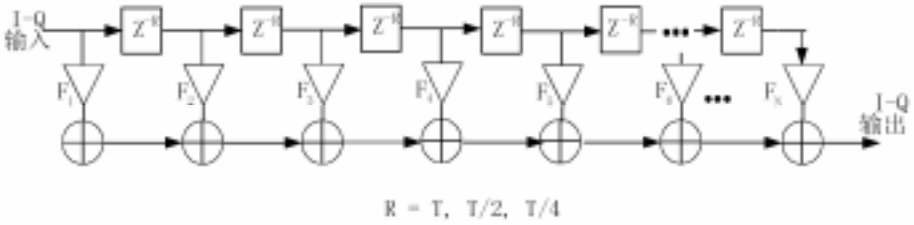


图9　发送预均衡器的结构

RNG-RSP MAC消息(见7.3.6.1)对每个系数使用16比特小数形式的二进制补码——“s1.14”(符号位、整数位、二进制小数点和14个小数位)来定义CM发送均衡器信息。CM应用CMTS发送的系数与现有的系数卷积以得到新的系数。

当CMTS响应初始测距请求和响应CM注册之前的周期性测距请求而发送预均衡系数时，该CMTS应用单符号间隔、均衡长度为8抽头的格式计算并发送预均衡系数。在CM注册后，CMTS可使用分数间隔(T/2或T/4格式)的均衡器格式以更长的抽头长度与CM的预均衡器性能匹配，CMTS能从REG-REQ消息Modem性能域中获知CM的预均衡器性能。Modem性能域的正确使用见7.3.8.a）。

在发生一个最初的测距请求前，无论何时变更上行信道频率或上行信道符号率，CM应清除预均衡器的系数到缺省状态，即除第一个抽头的系数(即F1)外，其余系数均设为零。

在初始测距期间，CM应补偿从均衡器第一个抽头位置到CMTS发送的新的均衡系数的主抽头的偏移时延(测距偏移)，通过随后的周期性测距更新预均衡器系数。在周期性的测距过程中CMTS不能改变主抽头的位置。在每个RNG-RSP消息中可包括均衡器系数，但通常只有在CMTS判定信道响应显著改变时才发生。在RNG-RSP消息中，均衡器系数的更新频率由CMTS决定。

为了保证正常工作(如防止上溢或下溢)，CM应规范预均衡器系数。CM还应补偿由于获得（或丢失）新系数(抽头)导致的发送功率的变化。如果CM均衡器的结构实现与在RNG-RSP消息中指定的抽头数相同，则CM不应改变在RNG-RSP消息中主抽头的位置。如果CM均衡器的结构实现与在RNG-RSP消息中的抽头数不同，则CM可以移动主抽头位置，在这种操作中，除了在RNG-RSP消息中的任何调整外，CM应适当调整其测距偏移以补偿主抽头位置的移动。

5.1.7　突发特性

传输特性包括3个部分：

- 信道参数；
- 突发简要特性；
- 用户专用参数。

信道参数包括：

- 符号率(5 种速率，160/320/640/1280/2560（ksym/s）)；
- 中心频率(Hz)；
- 1024 比特前同步码超字节串。

信道参数的详细描述见7.3.3和表34,这些特性在给定信道上由所有用户共享。突发简要特性见表4，详细表述见7.3.3和表35，这些参数对应于突发类型分享特征。用户专用参数对每个用户是可变的，甚至在该用户与另一个用户在同一信道上使用相同的突发类型时(例如，功率电平)也会如此，该参数见表5。

表4　突发简要特性

突发特性	配置设置
调制	QPSK、16QAM
差分编码	开/关
前同步码长度	0比特～1024比特（见5.2.5）
前同步码值偏移	0到1022
FEC纠错（T字节）	0到10（‘0’指FEC关）
FEC码字信息字节（k）	固定：16到253（假定FEC开） 截短：16到253（假定FEC开）
扰码器种子	15比特
最大突发长度（微时隙）[a]	0到255
保护时间	5到255符号
最后编码字长度	固定，截短
扰码器开/关	开/关
a 突发包长度为0微时隙，表示这种突发在该通道内的长度可变。突发长度不固定时，其突发长度由CMTS在MAP中向CM授权。	

表5　用户专用突发参数

用户专用参数	配置设定
功率电平[a]	+8dBmV到+55dBmV（16QAM） +8dBmV到+58dBmV（QPSK） 1dB步进
偏移频率[a]	范围 = ±32kHz；增量= 1Hz； 在 ±10Hz的范围内执行
测距偏移	0到（2^{16}-1），增量为6.25μs/64
突发长度(微时隙),如果在该信道上可变(突发到突发的变化)	1到255个微时隙
发送均衡器系数[a]（仅适用高级的调制解调器）	高达64系数；每系数4字节：2个实数和2个复数
a　表中的值适用于指定信道和符号率。	

CM应在适当的时间产生突发并在微时隙中传送，此时隙由CMTS的MAP消息给定(见7.3.4)。

CM应支持全部突发特性，该特性由CMTS经UCD中的突发描述决定(见7.3.3)，随后分配在MAP中以用于传输(见7.3.4)。

CM应实现频率偏移在±10Hz内。

测距偏移用于CM到CMTS上行传输时延校正，以便在TDMA方式中同步上行传输。测距偏移是一种预补偿，约等于从CMTS到CM的往返时延。基于接收到的一个或多个成功接收的突发(即从所用的每种技术取得的有效结果：误差校正和CRC)，CMTS应为CM校正这种偏移提供反馈，其准确度在1/2符号内，分辨率为1/64的帧信号微增量(6.25μs/64=0.09765625μs=1/4最高符号率的符号宽度为$10.24MHz^{-1}$)。CMTS发送给CM的调整信号，其负值意味着测距偏移要减少，即CM晚些时间传输。CM应实现校正，校正分辨率最多1个符号宽度（即在所用的给定突发中的符号率的一个符号宽度)，其准确度(非固定偏移)应为±0.25μs加上由于分辨率引起的±1/2符号。±0.25μs加上±1/2符号的CM突发定时的准确度与微时隙边界相关，该边界由CM按照从CMTS接收到的时戳信号的理论推算得出。

CM应在不给突发之间留有重新配置时间的情况下即可改变突发特性，但以下参数有变化的情况下除外：

- 输出功率；
- 调制方式；
- 符号率；
- 频率偏移；
- 信道频率；
- 测距偏移。

对于符号率、频率偏移及测距偏移的变化，只要CMTS在一个突发的最后符号中心与其后一个突发的第一个符号中心之间分配至少96个符号，CM就应能够连续发送。96个符号的最大重新调整时间需补偿该突发的下降沿时间和下一个突发的上升沿时间以及总的传输时延，包括线路时延和可选的预均衡器时延。对于调制类型的改变，只要CMTS在一个突发的最后符号中心与其后一个突发的第一个符号中心之间分配至少96个符号，CM就应能够连续发送。只有当CMTS在突发之间为CM提供足够的时间后，输出功率、符号率、频率偏移、信道频率及测距偏移才可改变。当前一个突发的任何符号能量超过-30dB有待发送时，或下一个突发的任何符号能量超过-30dB已被发送时，发送的输出功率、符号率、频率偏移、信道频率及测距偏移都不应改变。同样情况下，在排除发送均衡器(如果CM中存在)的影响后，调制方式也不应改变。(在发送均衡器不提供滤波时可以验证这一点，此时其影响只有时延。需要注意的是，如果CMTS在其均衡器中有判决反馈，它就需要在不同的调制类型的突发之间提供多于96个符号间隔给同一CM使用，这是一个CMTS的判决。)。负的测距偏移需要超过96个符号长度时间，因此CMTS应为其配置更多的保护时间，该时间至少等于负测距偏移量。

如果要改变信道频率，只要CMTS在一个突发的最后符号中心与其后的突发的第一个符号中心之间分配至少96个符号加100ms，则CM应能够在突发之间完成改变。

CM的信道频率开始改变的100ms内，其相位噪声和准确度要求满足5.1.10.5和5.1.10.6的规定。

如果输出功率变化≤1dB，则CM应在96个符号加上5μs内完成改变。

如果输出功率变化＞1dB，则CM应在96个符号加上10μs内完成改变。

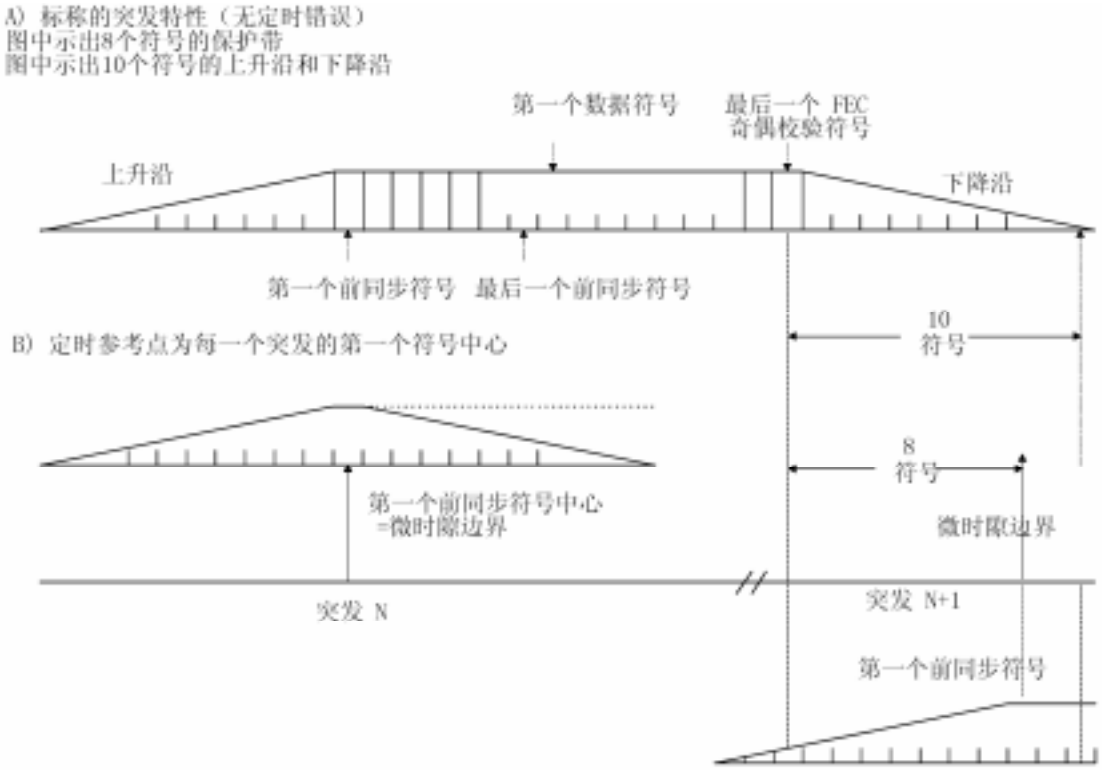
CM的输出功率应在下列时间内稳定到输出功率电平的±0.1dB内：

- 在开始变化的5μs内，若变化≤1dB；
- 在开始变化的10μs内，若变化＞1dB。

发送功率输出应保持恒定，在一个TDMA突发内波动应小于0.1dB(在16QAM的情况下，脉冲整形和振幅调制理论上引入的波动除外)。

5.1.8 突发定时规则

图10描述标称的突发定时。



注： 即使发射机分配两个突发时，前一个突发的下降沿也可与后一个突发的上升沿重叠。

图10　标称突发定时

图11描述了最坏情况下的突发定时。在这个例子中，突发N晚于1.5个符号到达，突发N+1早于1.5个符号到达，但保持5个符号的间隔，并显示出8个符号的保护带。

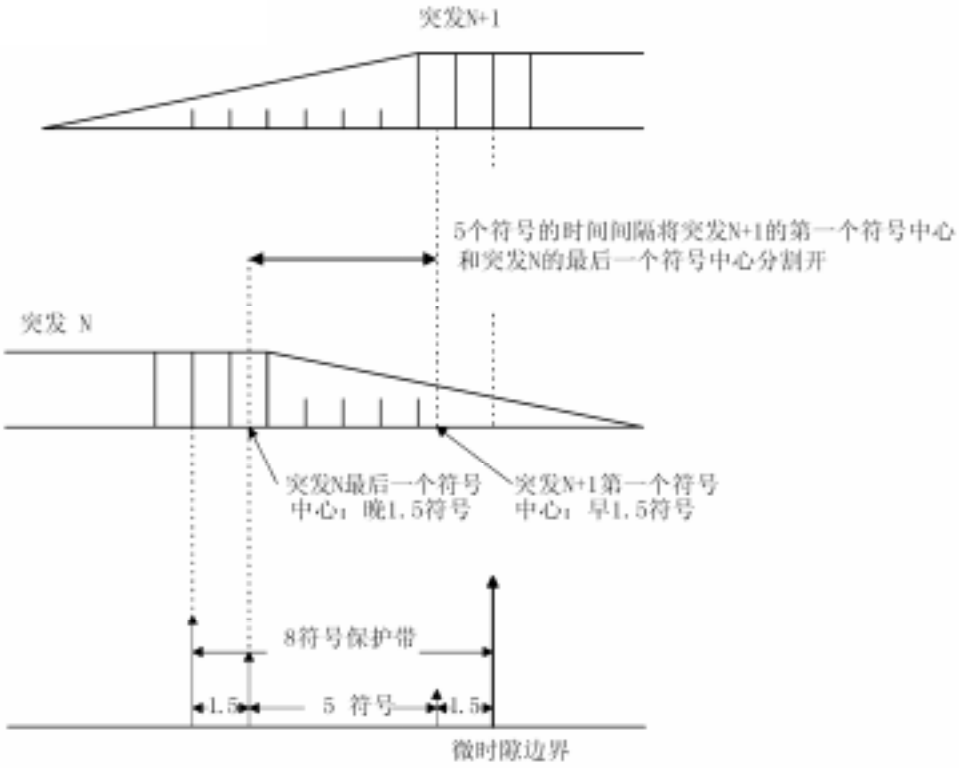


图11　最坏情况的突发定时

如符号率为Rs，则符号以Ts=1/Rs秒一个的速度出现，上升沿和下降沿是由于符号整形滤波器引起的在时域内的扩展。因为整形滤波器的脉冲响应长于Ts，如只有一个符号被传输，其持续时间长于Ts。在突发传输中，突发的第一个和最后一个符号的扩展使整个突发持续时长超过N×Ts，N为突发中的符号数。

5.1.9 发送功率要求

上行PMD子层应支持发送功率可变，其要求表示为：

- 指定发送功率范围；
- 功率步长大小；
- 响应精度(实际输出功率与指定量的比较)。

功率调节的运行机制在本部分的10.2.4中进行阐述，且调节应在以下表述的容许范围内。

输出功率调节和范围

在设定带宽中输出的传送功率应是可变的，其范围在+8dBmV～55dBmV(16QAM)，或+8dBmV～58dBmV(QPSK)，1dB步进。

传送功率的绝对准确度应为±2dB，步进的准确度为±0.4dB，当切换输入／输出步进衰减器(例如20dB)时允许滞后，在这种情况的准确度要求可放松到±1.4dB。例如，在CM的下一个发送突发中，增加功率电平1dB的指令导致的实际功率增加应在0.6dB～1.4dB之间。

步进分辨率应≤1dB。当CM被指定用更高的分辨率时，应转到最近的可支持的步进档。如果指令的步进在两个可支持步进档之间的一半，CM应选择较小的步进档。

5.1.10 保真度要求

5.1.10.1 寄生辐射

噪声和寄生功率应不超过表6、表7和表8中给定的电平。

在表6中，带内寄生包括噪声、载波泄漏、时钟、合成器的寄生成分及其它不需要的发射成分，但不包括码间干扰(ISI)。带内寄生的测量带宽等于符号率(例如160kHz对应于160ksym/s)。

对于3个(或更少)载波相关频带(65MHz以下)的测量带宽是160kHz，其中不超过-47dBc的至多3个160kHz频带可以不受表8规定的“ 5MHz～65MHz带内发送突发 ”的限制。

对于表6规定65MHz以下的突发之间的测量带宽也是160kHz，发送突发规定适用于给CM的授权的微时隙期间(当CM使用全部或部分的授权时)及授权的微时隙之前和之后的一个微时隙(一个微时隙可以短到32个符号，或在2.56Msym/s速率时的12.5μs，或短到在160ksym/s速率时的200μs)。除使用授权微时隙的期间和使用授权前后的微时隙外，其他情况使用突发之间的规定。

表6　寄生辐射

参数	传送突发	突发之间
带内［带内寄生包括噪声、载波泄漏、时钟、合成器寄生成分及其它不需要的发射成分。不包括码间干扰(ISI)］	-40dBc	-72dBc或5dBμV，取其中大者
相邻频带	见表7	-72dBc或5dBμV，取其中大者
3个或更少的载波相关频带(例如二次谐波，若＜65MHz)	-47dBc	-72dBc或5dBμV，取其中大者
5MHz-65MHz带内(除指定信道、相邻信道及载波相关信道)	见表8	-72dBc或5dBμV，取其中大者
CM综合寄生辐射限制(250KHz，包括离散的) 87.5MHz～108MHz	30dBμV	5dBμV
CM综合寄生辐射限制(4.75MHz，包括离散的)[a] 65MHz～87.5MHz 108MHz～136MHz 136MHz～862MHz	max(-40dBc，34dBμV) 20dBμV 15dBμV	34dBμV 15dBμV max(15dBμV，-40dBc[b])
CM离散寄生辐射限制[c] 65MHz～87.5MHz 108MHz～862MHz	max(-50dBc，24dBμV) 10dBμV	24dBμV 10dBμV

a 这些限制不包括关于已调接收信道的单一离散寄生辐射，这种单一离散的寄生辐射不应大于20dBμV。

b “dBc”是相对于接收到的下行信号电平。

c 本表所列的限制不包括3个或更少的离散寄生成分，这类寄生成分不应大于20dBμV。

5.1.10.1.1　相邻信道寄生辐射

寄生辐射可能来自一个符号率相同或不同的相邻信道。表7所列为全部组合的发送载波符号率和邻信道符号率所要求的邻信道寄生辐射限值，该值是在一个邻信道间隔内测量得到的，测量带宽和频率的设置与本信道和邻信道的符号率有关。

表7　邻信道寄生辐射

传输载波符号速率	在间隔内的的规定	测量间隔和距载波边缘的距离	邻信道载波符号率
160ksym/s	-45dBc	20kHz～180 kHz	160 ksym/s
	-45dBc	40kHz～360 kHz	320 ksym/s
	-45dBc	80kHz～720 kHz	640 ksym/s
	-42dBc	160kHz～1440 kHz	1280 ksym/s
	-39dBc	320kHz～2880 kHz	2560 ksym/s
所有其他符号率	-45dBc	20kHz～180 kHz	160 ksym/s
	-45dBc	40kHz～360 kHz	320 ksym/s
	-45dBc	80kHz～720 kHz	640 ksym/s
	-44dBc	160kHz～1440 kHz	1280 ksym/s
	-41dBc	320kHz～2880 kHz	2560 ksym/s

5.1.10.1.2　在5MHz～65MHz内的寄生辐射

除与邻信道内或上述表中所列的载波相关的辐射外，寄生辐射还可能由于其它相同或不同符号率的载波所产生。寄生辐射的测试带宽应等于相应于在该频段内发送的载波符号率的带宽。

表8所列为在一个间隔内可能发送的符号率、相应间隔内所要求的寄生电平，及在开始测量寄生辐射处的初始测量间隔。测量从初始距离处开始，并逐渐增加与载波的距离重复测量，直到达到上行频带边界5MHz或65MHz。测量间隔不包括载波相关的寄生辐射。

表8　5MHz～65MHz 范围内寄生辐射

在间隔内可能的符号率	在间隔内的规定	初始测量间隔和距载波边缘的距离
160ksym/s	-53dbc	220kHz～380kHz
320ksym/s	-50dbc	240kHz～560kHz
640ksym/s	-47dbc	280kHz～920kHz
1280ksym/s	-44dbc	360kHz～1640kHz
2560ksym/s	-41dbc	520kHz～3080kHz

5.1.10.2　突发开/关瞬时寄生辐射

在上升沿之前和上升期间、下降沿之后和下降期间、在TDMA方式中的突发之前和之后，每个发射机都应控制寄生辐射。

由于驱动或停止发送所产生的上行发射机输出端的电压变化有可能产生开／关瞬间的寄生辐射，该辐射不应超过100mV，且此跃变时间不快于2μs。此要求适用于CM以≥115dBμV发送的情况；在回退发送电平时，电压的最大变化应从＋115dBμV开始以每6dB（即功率电平一半）减少，下降到≤91dBμV时的最大变化为7mV。这一要求不适用于CM电源的开／关瞬时。

对于＜7mV的DC瞬变，没有2μs的摆率限制。

5.1.10.3　符号差错率（SER）

对QPSK和16QAM，未编码SER低于10^{-6}时，调制器的理论符号差错率对应的载噪比变化应在0.5dB范围内。

SER劣化取决于理想升余弦平方根接收滤波器输出的发送波形引起的汇聚误差，包括ISI的作用、寄生、相位噪声及所有其它的发射机劣化因素。

载噪比应高于30dB，测量时使用α＝0.25的升余弦平方根接收滤波器。

5.1.10.4　滤波器失真

以下要求假定未使用任何预均衡。

5.1.10.4.1　幅度

频谱特性应是理想升余弦平方根频谱，α=0.25，且在以下指定范围内：

- $f_c-R_s/4$Hz 到 $f_c+R_s/4$Hz：－0.3dB～＋0.3dB；
- $f_c-3R_s/8$Hz 到 $f_c+R_s/4$Hz 和 $f_c+R_s/4$Hz 到 $f_c+3R_s/8$Hz：－0.5dB～0.3dB；
- $f_c-R_s/2$Hz 和 $f_c+R_s/2$Hz：－3.5dB～2.5dB；
- $f_c-5R_s/8$Hz 和 $f_c+5R_s/8$Hz：≤－30dB。

其中，f_c为中心频率，R_s为符号率，分辨率带宽≤10kHz。

5.1.10.4.2　相位

fc-5Rs/8 Hz到fc+5Rs/8 Hz：群延时的变化不应大于100ns。

5.1.10.5　载波相位噪声

上行发射机总的综合相位噪声(包括离散的寄生噪声)应小于或等于-43dBc，测量带宽在载波上、下的1kHz～1.6MHz。

5.1.10.6　信道频率准确度

自生产日期5年以内，在0℃～40℃范围内，CM频率变化应在$\pm50\times10^{-6}$范围内。

5.1.10.7　符号率准确度

自生产日期5年以内，在0℃～40℃范围内，上行调制器符号率绝对准确度为$\pm 50\times 10^{-6}$。

5.1.10.8　符号定时抖动

在2S期间，发送波形峰到峰符号抖动应少于0.02个标称符号周期。

参照第一符号，不考虑固定频偏，在0.1秒期间内峰到峰累积的相位误差应少于0.04个标称符号周期。

5.1.11　帧结构

图12所示为2个帧结构的实例：一个是包的长度等于在一个码字中的信息字节的数目，另一个是包的长度比1个码字中信息字节数目多，但是少于2个码字中的数目。例1说明了固定的码字长度模式，例2说明了截短最后码字模式。这些模式在5.1.11.1中定义。

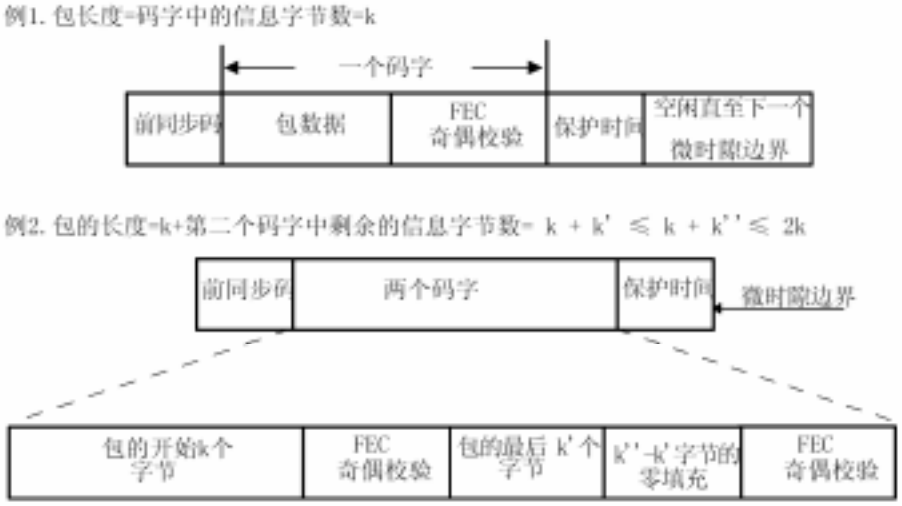


图12　具有可变突发长度模式的帧结构示例

码字长度

当使用FEC时，CM工作在固定长度码字或截短最后码字模式下。两种模式下一个码字所含的信息长度≥16字节。当信息长度大于16字节时，使用截短最后码字模式才有意义。

a)　固定码字长度

对于固定长度的码字，在所有的数据被编码后，如果码字长度未达到k字节，需要使用零填充。零填充应持续到该授权分配的最后微时隙结束前不能再增加固定长度码字时，且应考虑到FEC校验和保护时间符号；

b)　截短最后码字

如图12所示，令k'等于一个突发的信息字节分割为若干整长(k突发数据字节)码字后的剩余字节数，k'小于k。令k"等于截短最后码字中突发数据字节与零填充字节的数量之和。当工作在截短最后码字模式下时，CM将突发的数据字节(包括MAC包头)按指配的码字大小(每个码字k信息字节)编码，直到所有的数据完成编码，或余下的字节数小于k。

截短的最后码字不能少于16个信息字节，在CM有微时隙请求时应该被考虑。CM应在必要时填充零，直到微时隙结束，通常也即下一个微时隙的边界处，这时还应考虑FEC校验和保护时间符号。在很多情况下，只有k＂-k＇个零填充字节应填充到微时隙位置，此时$16\leq k＂\leq k$且$k＇\leq k＂$。但还需注意，通常情况下，要求CM填充零数据，直到没有额外的固定长度码字可以被加到授权的最后指配的微时隙的末端时(应考虑FEC校验和保护时间符号)，然后可能的话，应该将一个截短的最后零填充码字加到指定的微时隙。

如果在零填充的额外的k信息字节码字后，在指配授权的微时隙中有不到16个字节剩余，且考虑了FEC校验和保护时间符号，则CM将不产生这个最后截短的码字。

5.1.12　信号处理要求

每个突发数据包类型的信号处理顺序应与图13和图14所示一致。

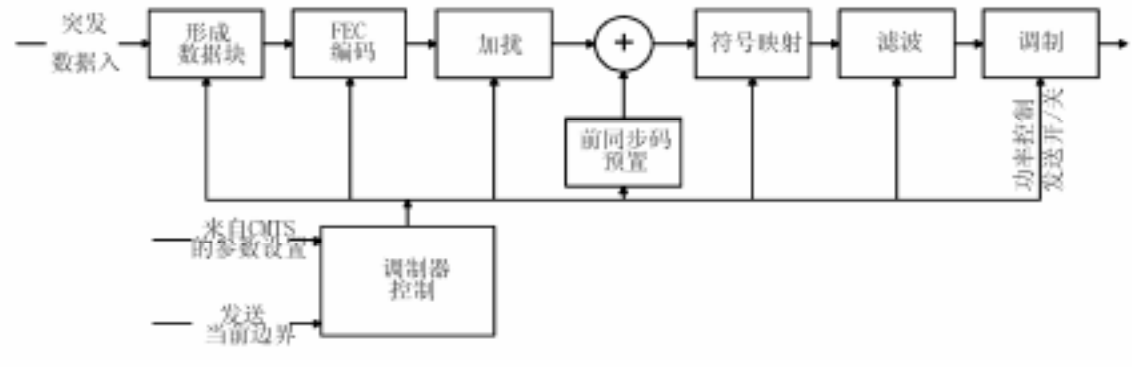


图13　信号处理顺序

图14　TDMA 上行传输过程

5.1.13　上行解调器输入功率特性

在5MHz～65MHz工作频率范围内，到上行解调器的最大总输入功率不应超过95dBμV。

每个载波预期的接收功率，应符合表9的规定。

解调器应工作在其规定的性能指标内，接收的突发信息在额定接收功率的±6dB范围内。

表9　在每个载波中所要求的额定接收功率最大范围

符号率 ksym/s	最大范围 dBμV
160	+44～+74
320	+47～+77
640	+50～+80
1280	+53～+83
2560	+56～+86

5.1.14　CM 的上行电气输出

CM输出的射频调制信号特性满足表10的要求。

表10　CM 的电气输出

参数	数值
频率	5MHz～65MHz
电平范围(一个信道)	+68dBμV～+115dBμV(16QAM) +68dBμV～+118dBμV(QPSK)
调制方式	QPSK和16QAM
符号率(标称)	160ksym/s,320ksym/s,640ksym/s,1280ksym/s和2560ksym/s
带宽	200kHz,400kHz,800kHz,1600kHz和3200kHz
输出阻抗	75Ω
输出反射损耗	＞6dB（5MHz～65MHz）
连接器	F型连接器（与输入同）

5.2　下行

5.2.1　下行协议

下行PMD子层应遵守GY/T 170-2001的规定。

5.2.2　交织

下行PMD子层应支持在表11中规定特性的交织器，交织器模式全部遵守GY/T 170-2001。

表11　交织器特性

I 抽头数	J 增量	突发保护 64QAM/256QAM	等待时间 64QAM/256QAM
12	17	18μs／14μs	0.43ms／0.32ms

5.2.3　下行频率划分

下行频率划分将包括在112MHz～858MHz之间的所有中心频率，增量250kHz。

5.2.4　CMTS 电气输出

CMTS输出的RF调制信号应具有表12中规定的特性。

表12　CMTS 输出

参数	数值
中心频率（fc）	112MHz～858MHz±30kHz
电平	在110dBμV～121dBμV内可调
调制类型	64QAM和256QAM
符号率（标称） 64QAM 256QAM	 6.952Msym/s 6.952Msym/s
标称信道间隔	8MHz
频率响应 64QAM 256QAM	 15%升余弦平方根整形 15%升余弦平方根整形
带内(fc±4MHz)总离散寄生 带内(fc±4MHz)寄生和噪声 邻信道寄生（fc±4MHz）～（fc±4.75MHz） 邻信道寄生（fc±4.75MHz）～（fc±12MHz） 下一个邻信道寄生（fc±12MHz）～（fc±20MHz） 其他信道寄生（80MHz～1000MHz）	＜-57dBc ＜-46.7dBc；信道的寄生和噪声包括所有的离散寄生、噪声、载波泄漏、时钟、合成器产物及其它不需要的发射成分。在载波的±50kHz范围内的噪声除外 在750kHz内＜-58dBc 在7.25MHz内＜-60.6dBc，3个以下含3个寄生尖峰除外，当每个以10kHz带宽测量时，均应小于-60dBc ＜-63.7dBc或在8MHz内＜49.3dBμV中的较大者，3个以下含3个寄生尖峰除外。当每个以10kHz带宽测量时，寄生总功率均应＜-60dBc 在每8MHz信道内＜49.3dBμV，3个以下含3个寄生尖峰除外。当每个以10kHz带宽测量时，寄生总功率均应＜-60dBc。
相位噪声	1kHz～10kHz：-33dBc双边带噪声功率 10kHz～50kHz：-51dBc双边带噪声功率 50kHz～3MHz：-51dBc双边带噪声功率
输出阻抗	75Ω
输出反射损耗	每信道＞14dB（108MHz -750MHz，含750MHz）； 每信道＞13dB（750MHz -862MHz）
连接器	F型

5.2.5　下行到 CM 的电气输入

CM接收RF调制信号的电气输入特性见表13。

表13　到 CM 的电气输入特性

参数	值
中心频率	（112MHz～858MHz）±30kHz
电平范围(一个信道)	43dBμV～73dBμV，64QAM；47dBμV～77dBμV，256QAM
调制类型	64QAM和256QAM
符号率(标称值)	6.952Msym/s(64QAM和256QAM)
带宽	8MHz(0.15升余弦平方根，64QAM和256QAM)
总输入功率(80MHz～862MHz)	＜90dBμV
输入(负载)阻抗	75Ω
输入回波损耗	＞6dB（85MHz～862MHz）
连接器	F型（与输出端共用）

5.2.6　CM 误码率(BER)特性

本条描述了CM误码率(BER)，适用于I=12，J=17交织模式。

5.2.6.1　64QAM

5.2.6.1.1　64QAM CM 误码率特性

当工作在载噪比≥25.5dB时，CM在FEC后的BER≤10^{-8}。

5.2.6.1.2　64QAM 镜像抑制特性

除相邻频道外，在RF频带的任何部分中的模拟或数字信号为+10dBc时，应满足5.2.6.1.1中描述的性能。

5.2.6.1.3　64QAM 邻信道特性

在相邻信道中数字信号为0dBc时，应满足5.2.6.1.1中描述的性能。

在相邻信道中模拟信号为+10dBc时，应满足5.2.6.1.1中描述的性能。

在相邻信道中数字信号为+10dBc时，应满足5.2.6.1.1中描述的性能，并附加0.2dB裕量。

5.2.6.2　256QAM

5.2.6.2.1　256QAM CM 误码率特性

当工作在载噪比如表14中规定时，CM在FEC后的BER≤10^{-8}。

表14　256QAM CM BER 特性

输入接收信号电平	载噪比
47dBμV～54dBμV	34.5dB
＞54dBμV～77dBμV	31.5dB

5.2.6.2.2　256QAM 镜像抑制特性

除相邻信道外，在RF频带的任何部分中的模拟或数字信号为+10dBc时，应满足5.2.6.2.1中描述的性能。

5.2.6.2.3　256QAM 邻信道特性

在邻信道中模拟或数字信号为0dBc时，应满足5.2.6.2.1中描述的性能。

在邻信道中模拟信号为+10dBc时，应满足5.2.6.2.1中描述的性能，并附加0.5dB裕量。

在相邻信道中数字信号为+10dBc时，应满足5.2.6.2.1中描述的性能，并附加1.0dB裕量。

5.2.6.2.4　QAM 的附加规定

QAM调制的附加规定见表15。

表15　QAM 调制的附加规定

参数	规定
I/Q相位偏移	＜1.0°
I/Q串扰	≤-50dB
I/Q振幅失衡	最大0.05dB
I/Q定时偏移	＜3.0ns

5.2.7　CMTS 时戳抖动

在下行传输会聚子层，CMTS时戳抖动峰－峰值应小于500ns。这种抖动是相对于一个理想的下行传输会聚子层，该子层以完全连续和平滑的时钟传送MPEG包到下行PMD子层。在产生和传送时戳到下行PMD子层时不应考虑下行PMD子层的处理。

因此，在时间T1和T2向下行PMD子层传送任何2个时戳N1和N2(N2≥N1)，应满足式（5）。

$$|(N2-N1)/10240000-(T2-T1)|<500ns \quad (5)$$

时戳抖动包括在时戳值中的不准确度和所有时钟的抖动。考虑到下行PMD子层引入抖动的影响，对于在下行传输会聚子层输出端的抖动分配的500ns应减少。

当时戳包含最坏情况下的抖动时，CM应满足在4.1.7中所要求的突发定时准确度。

抖动是相对于CMTS主时钟的误差(即测量值)(CMTS主时钟是10.24MHz时钟，用来产生时戳)。

CMTS 10.24MHz主时钟应满足频率稳定度≤±5ppm、频率漂移率≤10^{-8}／s、及边界抖动≤10ns p-p(±5ns)。(由于在每个分段区间上的10ns抖动及10ns的频率漂移，因此从CMTS主时钟上的漂移率和抖动要求，可以得出10240000周的2个相邻段的时间区间应在30ns内。其它计数的时间区间也可推导：相邻1024000段，≤21ns；由一个10240000周段分析出的1024000长度段，≤30ns；相邻102400000段，≤120ns。CMTS主时钟应在99%或更多测量中满足这些测试极限。)

6　下行传输会聚子层

为了改善解调的抗干扰性，简化视频和数据的公共接收硬件，以及为在第5章已经定义过的PMD子层上的视频和数据的比特流在未来可能的复用提供机会，因此，在下行PMD子层和HFC数据传输MAC子层之间插入了一个子层。

下行比特流定义为188个字节的MPEG[GB/T 17975.1-2000]包的连续序列。这些包包括4个字节的包头及其后的184个字节有效负载信息。包头标识有效负载信息属于HFC数据传输MAC，包头的其他值说明其他有效负载信息。MAC有效负载和其他业务的混合是任选的，并受CMTS控制。

图15说明HFC数据传输(DOC)MAC字节和其他数字信息的交织(在实例中为数字视频)。

包头=HFC数据（DOC）	HFC数据MAC有效负载
包头=视频	数字视频有效负载
包头=视频	数字视频有效负载
包头=HFC数据（DOC）	HFC数据MAC有效负载
包头=视频	数字视频有效负载
包头=HFC数据（DOC）	HFC数据MAC有效负载
包头=视频	数字视频有效负载
包头=视频	数字视频有效负载
包头=视频	数字视频有效负载

图15　下行 MPEG 包交织的实例

6.1　MPEG 包格式

传送数据的MPEG包格式如图16所示。MPEG包由4字节的MPEG包头、1个字节的指针域(不是所有的包都有)和有效负载组成。

MPEG包头 4个字节	指针域 1个字节	有效负载 183字节或184字节

图16　MPEG 包格式

6.2　HFC 数据传输的 MPEG 包头

MPEG传输流的包头格式定义见GB/T 17975.1-2000。表16中定义了区分HFC数据传输MAC流的特殊域值。

MPEG包头由4个字节组成，用于指明188个字节的MPEG包的开始。在HFC数据PID上使用的包头格式有所限制，如表16所示，包头格式和MPEG标准一致，但是在使用时不允许包括MPEG包的自适应域。

表16　HFC 数据包的 MPEG 包头格式

域	长度 bit	描述
同步字节	8	0x47；MPEG包同步字节
传输误码指示	1	表明在接收包时有误码发生。该位在发端置0，在包的传输过程中有误码发生时置1。
有效负载单元起始指示	1	值‘1’表明指针域为有效负载的第一个字节（包的第5个字节）
传送优先级	1	保留；置为0
PID	13	HFC数据PID（0x1FFE）
传送加扰控制	2	保留；置为’00’
自适应域控制	2	‘01’；HFC数据PID中不允许使用自适应域
连续计数器	4	在此PID内的循环记数器

6.3　MPEG 有效负载

MPEG包的有效负载部分携带 MAC帧。如果MPEG包头的有效负载单元起始指示（PUSI）设置为1，则MPEG有效负载的第一个字节为“指针域”。

6.3.1　stuff_byte(填充字节)

规定填充字节为0×FF，用来填充有效负载中 MAC帧之间的空隙。 MAC帧的第一个字节不会用到这个值，MAC包头的“FC”字节被规定永远不包含这个值。(FC_TYPE=“11”表明了一个特殊的MAC帧；本部分中FC_PARM=“11111”未使用，定义为非法值。)

6.3.2　pointer_field(指针域)

当MPEG包头的负载单元开始指示(PUSI)置为“1”时，指针域出现在MPEG包的第5个字节(MPEG包头后的第一个字节)。

指针域包含了跟在指针域后的包字节数，CM解码器应跳到指针域来寻找 MAC帧的起始。如果在包中开始一个HFC数据传输的MAC帧，则指针域应存在，并且应指向包的第一个MAC帧的开始处或任何前面的填充字节。

6.4　与 MAC 子层的交互

MAC帧可能开始于MPEG包的任何位置，MAC帧可能扩展到几个MPEG包，也可能几个MAC帧存在于一个MPEG包中。

图17显示了携带有规定 MAC帧的MPEG包的格式，在任何情况下，PUSI标志指明作为MPEG有效负载的第一个字节的指针域的存在。

图17所示为在指针域字节后紧跟MAC帧的情况，此时，指针域为0，解码器开始在指针域后搜索一个有效的FC字节。

MPEG 包头 (PUSI=1)	指针域 (=0)	MAC帧 (最多183字节)	填充字节 (0或多个)

图17　紧跟指针域的 MAC 帧的包格式

图18说明了更普通的一种格式，MAC帧的前面有前一个MAC帧的尾部信息和一系列填充字节。在这种情况下，指针域仍指明1号帧尾(1个填充字节)之后的第一个字节的位置，从此处开始，解码器就可以搜索合法的MAC子层的FC值。这种格式允许在CMTS中的复用，若MPEG包头和指针域已经传送出后，MAC帧才到达，可以立即插入该待传输的MAC帧。

为了使得携带标准数据的MPEG包流和其他MPEG编码数据的复用更方便，CMTS不传送携带有标准PID的MPEG包，这些包在有效负载区中只有一些填充字节，而代之传送MPEG的空包。需要注意，在MAC子层有暗含着的计时关系，任何MPEG复用操作应保留这种计时关系。

MPEG包头 (PUSI=1)	指针域 (=M)	1号MAC帧的尾部 (M字节)	填充字节 (0或更多)	2号MAC帧的开始

图18　前面有填充字节的 MAC 帧的包格式

图19表明了在MPEG包中可包含多个MAC帧的情况，MAC帧可以一帧接一帧链接，也可以由填充字节的可选序列来分开。

MPEG包头 (PUSI=1)	指针域 (=0)	1号MAC帧	2号MAC帧	填充字节 (0或更多)	3号MAC帧

图19　在一个包中有多个 MAC 帧的包格式

图20表示了一个MAC帧扩展到几个MPEG包的情况，在这种情况下，后续帧的指针域指向紧跟在第一帧的尾部的最后一个字节之后的字节。

MPEG包头 (PUSI=1)	指针域 (=0)	填充字节 (0或更多)	1号MAC帧的起始 (最多183字节)	
MPEG包头 (PUSI=0)	1号MAC帧的延续（184字节）			
MPEG包头 (PUSI=1)	指针域 (=M)	1号MAC帧尾部 (M字节)	填充字节 (0或更多)	2号MAC帧的起始 (M字节)

图20　一个 MAC 帧跨越多个包的包格式

传输会聚子层应和MAC子层密切合作，来提供一个用于插入到时间同步消息的准确时戳，见7.3.2和8.3。

6.5　与物理层的交互

MPEG－2包数据流应按照GY/T 170-2001来编码。

6.6　MPEG 包头同步和恢复

当从连续5个188字节都正确接收到同步字节时，应声明MPEG－2包数据“ 帧同步（in frame）”。

当接收到9个连续不正确的同步时节时，应声明MPEG－2包数据流“ 帧失步（out of frame）”，并开始搜索正确的包定位信息。

7　媒介接入控制技术要求

7.1　简介

本条描述MAC协议。MAC协议主要涉及以下方面：

a)　由 CMTS 控制的带宽分配；

b) 上行的微时隙流；
c) 基于争用和保留的上行发送机会的动态混合；
d) 支持可变长度包以提高带宽效率；
e) 为将来支持 ATM 或其它数据 PDU 时所提供的扩展；
f) 服务质量（QoS）包括：
   1) 对带宽和等待时间保证的支持；
   2) 包分类；
   3) 动态业务的建立；
g) 提供数据链路层安全性扩展接口；
h) 对多种数据速率的支持。

7.1.1 定义

下列定义和说明适用于本部分的本章。

7.1.1.1

MAC 子层域 MAC-sublayer domain

单个MAC分配和管理协议操作的上行和下行信道的集合，其附属部分包括一个CMTS和若干CM。CMTS应为所有的上行和下行信道服务；每个CM可以接入一个或多个上行和下行信道。对于源MAC地址不是单播的MAC地址的包，CMTS应丢弃。

7.1.1.2

MAC 业务接入点 MAC service access point

MAC子层域的附属部分（参见4.2）。

7.1.1.3

业务流 service flow

业务流的概念是MAC协议运行的核心。业务流提供了一种上行和下行服务质量管理的机制，对于带宽分配是必需的。

SFID(业务流标识符)定义了CM和CMTS之间特定的单方向映射。有效的上行SFID也具有其相关的SID。上行带宽由CMTS分配给SID，从而分配给CM。SID提供上行业务质量实现的机制。

CMTS可以根据CM需要的业务流给每个CM分配一个或多个SFID。这种映射可以在CM注册期间在CMTS与CM之间协商，或者通过动态业务建立来实现(见10.4)。

在基本的CM实现中，例如，可以使用两个业务流（一个上行，一个下行），来提供尽力传输的IP业务。然而，当支持与多个CM的互操作性时，业务流的概念允许开发更复杂的CM来支持多种业务类型。使用这些更复杂的CM，将对某些业务流进行配置，使之不能承载所有类型的业务，即可以有最大包长度的限制，或者被限制为小的固定长度的主动请求。此外，在供固定比特率（CBR）类型业务使用的业务流中可能不适合发送其它种类的数据。

即使在这些复杂的CM中，也需要能够发送某些MAC管理、SNMP管理等所需要的上行包。为使网络正常工作，所有的CM应至少支持一个上行和一个下行业务流。为使CM请求和发送最大可能的非级联的MAC帧，应一直提供这些业务流（参见7.2）。这些业务流称为上行和下行基本业务流。分配给上行基本业务流的SID称为主SID。

在注册过程中，主SID应总是被分给第一个预置的上行业务流（可能与注册过程中使用的临时SID不同）。在注册的时候，应使基本业务流立即启动。在注册之后，应总是使用主SID来进行台站的维护。基本业务流可以用作传输业务。所有单播业务流应使用为基本业务流制定的安全协定（安全加密标准待定）。

在单个MAC子层域中，所有SFID都是唯一的。SFID的长度是32比特。SID的长度是14比特（有时，SID放在一个16比特域的低位中）。

7.1.1.4

上行时间间隔、微时隙和 6.25μs 增量　upstream interval, mini-slot and 6.25μs increment

上行带宽分配机制把上行传输时间分成很多时间间隔。每个时间间隔是一个微时隙的整倍数。“ 微时隙 ”是上行传输中的基本单元。每个时间间隔由一个使用码来标识,该使用码规定了在该时间间隔内传输的业务类型和物理层调制编码的情况。一个微时隙是6.25μs增量的2的幂，即2、4、8、16、32、64或128乘6.25μs。微时隙、字节和时间节拍之间的关系将在8.3.4作进一步的介绍。使用码的数值在表36中规定，其允许的用途在7.3规定。这些数值与物理层参数之间的关系在表34中规定。

7.1.1.5

帧　frame

数据链路层中两个或多个实体间数据交换的单元。一个MAC帧包括MAC包头(由一个帧控制字节开始，见图23），并可插入可变长度的数据PDU。可变长度的PDU包括一对48比特的地址、数据和一个CRC码。在特殊情况下，MAC包头可以把多个MAC帧封装到一个MAC帧中（见7.2.5.5）。

7.1.2　将来的用途

在本部分的各种MAC帧的说明中，有许多域定义为“ 为将来使用 ”或“ 保留 ”，基于本MAC协议的产品，不应以任何方式解释或使用这些域。

7.2　MAC 帧的格式

7.2.1　一般 MAC 帧格式

MAC帧是CMTS和CM的MAC子层之间传送的基本单元。上行和下行方向使用相同的基本帧结构。MAC帧的长度是可变的。“ 帧 ”是用来表示对等的MAC子层之间传送的信息单位，而不是表示某种固定定时关系的术语“ 成帧 ”。

如图21所示的一般MAC帧结构中有3个不同的域。MAC帧之前是一个PMD子层开销(上行)或是一个MPEG流包头（下行）。MAC帧的第一部分是MAC包头。MAC包头唯一地标识了MAC帧的内容。包头之后是可选的数据PDU域。数据PDU的格式及其有无在MAC包头中定义。

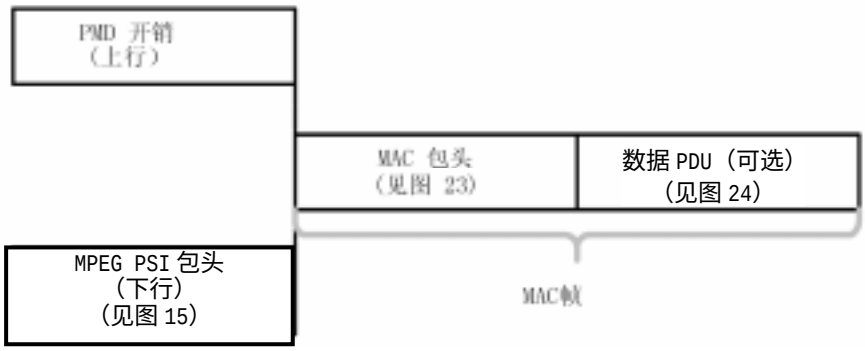


图21　一般 MAC 帧结构

7.2.1.1　PMD 开销

在上行方向，PHY层表明了到MAC子层的MAC帧的开始。从MAC子层的角度来看，只需要知道开销的总数，以便在带宽分配过程中予以考虑，见第5章PMD子层部分。

FEC开销分布在整个MAC帧中，并且应对MAC数据流透明。MAC子层在进行带宽分配时应考虑开销，见8.1。

7.2.1.2　MAC 帧传输

PMD子层上行信道MAC帧的传输见图22。

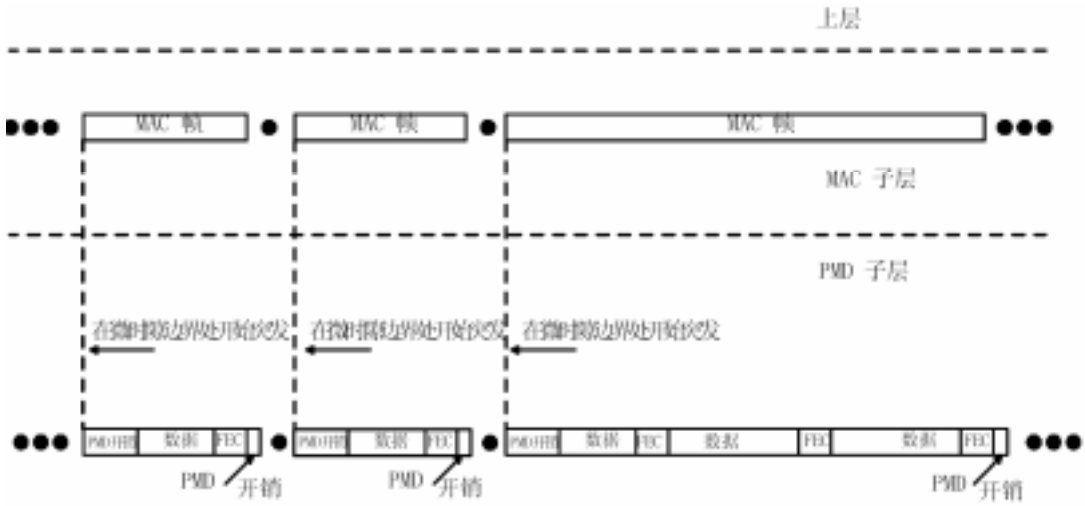


图22　上行 MAC/PMD 会聚

下行信道MAC帧的传输见第6章。

7.2.1.3　比特和 8 位组排序

在一个8位组中，首先传送LSB。按照以太网和GB/T 15629.3-1995中使用的惯例通常称为bit-little-endian顺序。

在MAC层中，当数值以多于一个的8位组（即16比特和32比特的值）来表示时，首先传送包含MSB的8位组。此时称为byte-big-endian顺序。

本条遵循了文本惯例，当表中出现比特域时，则MSB列在表的最上方。例如，在表18中，FC_TYPE占据前两位MSB，而EHDR_ON占据LSB。

7.2.1.3.1　负数的表示

带符号的整数值按2的补码格式来发送和接收。

7.2.1.3.2　Type_Length_Value(类型-长度-值，TLV)域

许多MAC消息都包括TLV域。TLV域可以是TLV字节组的无序排列。有些TLV是嵌套的（见附录C）。所有TLV长度域应大于0，EH_LEN除外（见7.2.6）。如无特别说明，类型为1个字节，长度为1个字节。

使用这种编码，可能会增加某些设备不能解释的新参数。CM或CMTS应跳过无法识别的参数类型，而不应将其作为错误事件处理。

7.2.1.4　MAC 包头格式

MAC包头格式如图23所示。

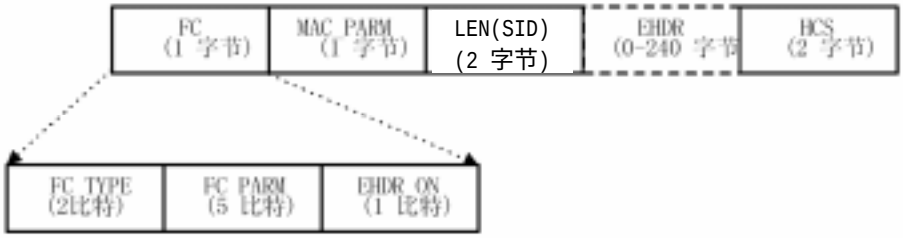


图23　MAC 包头格式

所有MAC包头都应具有表17所示的一般格式。帧控制（FC）域是第一个字节，唯一地标识MAC包头中的其余内容。FC域后随3个字节的MAC控制域、一个可选的扩展包头域（EHDR）、一个确保MAC包头完整性的包头校验序列（HCS）。

表17　一般 MAC 包头格式

MAC包头域	用法	长度
FC	帧控制：标识MAC包头的类型	8比特
MAC_PARM	参数域，用法取决于FC： 如果EHDR_ON=1，用于EHDR长度（ELEN）； 在级联帧中（见表26）用于MAC帧计数； 或表示所请求的微时隙的数目（只用于REQ）。	8比特
LEN（SID）	MAC帧的长度。定义为扩展包头中的字节数和HCS域后的字节数的总和。（对于REQ包头，该域表示SID）。	16比特
EHDR	扩展MAC包头（可变长度）。	0字节～240字节
HCS	MAC包头校验序列。	2字节
MAC包头的长度		6字节+EHDR

HCS域是一个16比特的CRC，在发生碰撞的情况下可用来保证MAC包头的完整性。HCS域应覆盖整个MAC包头，从FC域开始，并包括所有出现的EHDR域。HCS用CRC（$x^{16}+x^{12}+x^{5}+1$）进行计算。

FC域被分为FC-TYPE子域、FC-PARM子域和一个EHDR_ON指示标志。FC域的格式如表18。

表18　FC 域格式

FC域	用法	长度
FC_TYPE	MAC帧控制类型域： 00：包PDU的MAC包头； 01：ATM PDU的MAC包头； 10：保留PDU的MAC包头； 11：MAC特定包头。	2比特
FC_PARM	参数比特，用法取决于FC_TYPE	5比特
EHDR_ON	EHDR_ON=1时，表示有EHDR域。 （EHDR的长度（ELEN）由MAC_PARM域确定）。	1比特

FC_TYPE子域是FC域的两位MSB。这两比特表示可能的4种MAC帧格式之一，其类型包括：带有包PDU的MAC包头、带有ATM信元的MAC包头、为将来的PDU类型保留的MAC包头或用于特定的MAC控制的MAC包头。

FC_TYPE子域后面的5个比特是FC_PARM子域。这些比特的用法取决于MAC包头的类型。FC域的LSB是EHDR_ON指示符。如果该比特为1，则有扩展包头（EHDR）。EHDR给出了允许MAC包头扩展成互操作状态的机制。

传输会聚子层填充字节定义为0xFF，因此FC字节不应出现FC_TYPE=11和FC_PARM=11111的组合。

根据FC域，MAC包头的MAC_PARM域有多种用途。如果EHDR_ON置1，则MAC_PARM域应用于扩展包头长度（ELEN）；EHDR域长度可在0字节～240字节之间变化；如果这是一个级联MAC包头，那么MAC_PARM域代表级联MAC帧的数目（CNT）（见7.2.5.5）；如果这是一个REQ MAC包头，那么MAC_PARM域表示所请求的带宽。其它情况下，MAC_PARM域保留作将来使用。

第三个域有两种可能的用法。多数情况下，它指示该MAC帧的长度（LEN）；一种特殊情况下，即在REQ MAC包头中，MAC包头后没有跟随PDU时，它用于表示CM的SID。

扩展包头（EHDR）域为MAC帧格式提供扩展。它用于数据链路安全性、帧分段，并且可扩展用于支持新增功能。在初始化实现中，应将该域传递给处理器（见7.2.6）。

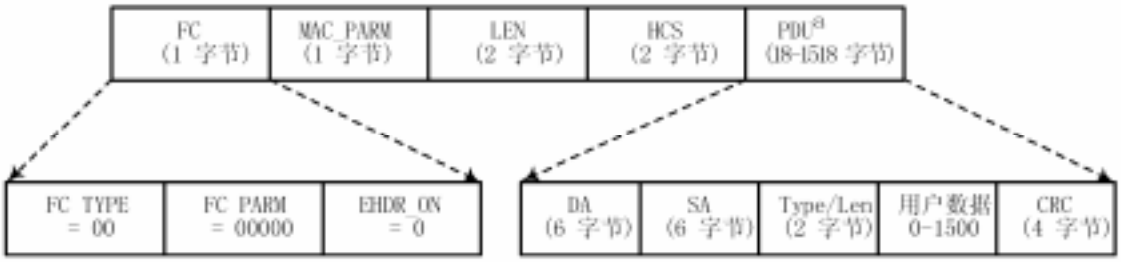
7.2.1.5　数据 PDU

MAC包头可以后随一个数据PDU。数据PDU的类型和格式在MAC包头的帧控制域中定义。FC域明确定义了包数据PDU、ATM数据PDU、MAC特定帧和一个保留编码（用于将来作扩展时的转义机制）。所有CM应使用MAC包头中的长度域来跳过所有保留数据。

7.2.2 基于包的 MAC 帧

可变长度包

MAC子层应支持可变长度的以太网GB/T 15629.3-1995类型的PDU。通常，包PDU通过网络时应保持含CRC在内的包的完整性。在包的开始处添加一个唯一的MAC包头。不带扩展包头的帧格式如图24和表19所示。



a 在没有 VLAN 填充的情况下，帧长度限制在 1518 字节以内。实现了 IEEE802.1Q VLAN 填充的设备可以使用长达 1522 字节的帧。

图24 以太网/802.3 PDU 格式

表19 PDU 格式

域	用法	长度
FC	FC_TYPE=00：MAC包头 FC_PARM[4：0]=00000：其它值保留 若无EHDR： EHDR_ON=0；若有则置为1	8比特
MAC_PARM	MAC_PARM= x；如果无EHDR则应置为0，否则置为EHDR的长度。	8 比特
LEN	LEN=n+x，PDU字节数+EHDR的长度	16比特
EHDR	如果有EHDR，表示扩展MAC头	x（0-240）字节
HCS	MAC包头校验序列	2字节
包数据	DA：48比特目的地址 SA：48比特源地址 类型/长度：16比特以太网类型或GB/T15629.3-1995长度域 用户数据（可变长度，0-1500字节） CRC：PDU的32比特CRC	n字节
MAC帧的长度		6+x+n个字节

在某些情况下（见附录M），可能需要发送不带实际PDU的PDU MAC帧，以便扩展包头用于承载业务流状态的特定信息。对这种帧，MAC包头中的长度域被置为0，由于没有包数据，也就没有CRC。这种情况只能发生在上行的传输帧中，因为下行的传输帧中至少有PDU的DA和SA域。

7.2.3 ATM 信元 MAC 帧

FC_TYPE 0x01保留给将来定义ATM信元MAC帧，它表示帧中有ATM PDU。本部分使用长度域跳过该ATM PDU。

7.2.4 保留 PDU 的 MAC 帧

MAC子层为支持将来的PDU格式提供了保留的FC编码。MAC包头的FC域表示帧中有保留的PDU。本部分使用长度域跳过该保留PDU。

不带扩展包头的保留PDU的格式如图25和表20所示。

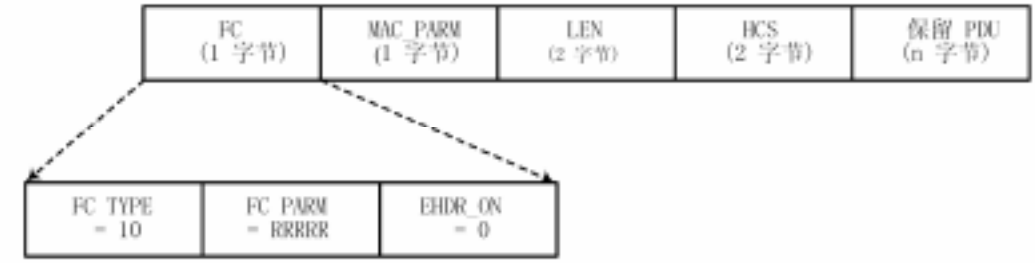


图25　保留 PDU 格式

表20　保留 PDU 格式

域	用法	长度
FC	FC_TYPE=10：保留PDU的MAC包头 FC_PARM[4：0]：保留供将来使用 若无EHDR： EHDR_ON=0；若有则为1	8比特
MAC_PARM	MAC_PARM=x;若无EHDR；应设为0；若有则为EHDR的长度。	8比特
LEN（SID）	LEN=n+x，包PDU的长度+EHDR的长度	16比特
EHDR	如果有EHDR，表示扩展MAC头	x（0-240）字节
HCS	MAC包头校验序列	2字节
用户数据	保留数据PDU	n字节
保留MAC帧的长度		6+x+n个字节

7.2.5　MAC 特定包头

有几种MAC包头用于特殊功能。这些功能可支持下行定时和上行测距/功率调整、请求带宽、分段和多个MAC帧的级联。

表21描述了MAC特定包头中的FC_PARM用法。

表21　MAC 特定包头和帧

FC_PARM	包头/帧类型
00000	定时包头
00001	MAC管理包头
00010	REQ帧
00011	分段包头
11100	级联包头

7.2.5.1　定时包头

定时包头用于支持所需的定时和调整。在下行方向，应传送这种MAC包头用于所有CM进行同步的全局定时参考。在上行方向，该MAC包头应是测距消息的一部分，用于CM的定时和功率调整。定时MAC包头后跟随一个PDU。其格式如图26和表22所示。

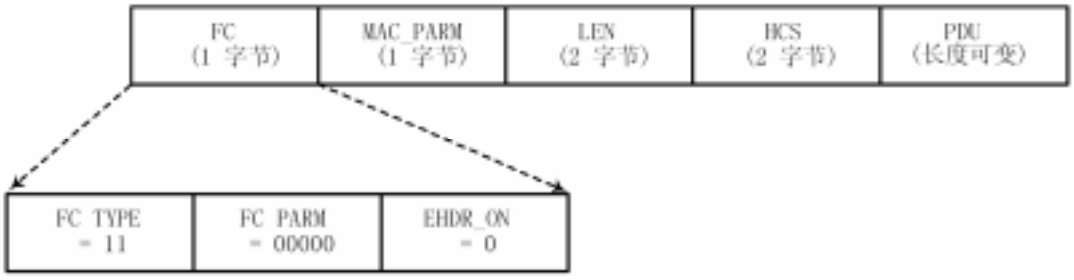


图26　定时 MAC 包头

表22　定时 MAC 包头格式

域	用法	长度
FC	FC_TYPE=11：MAC特定包头 FC_PARM[4：0]=00000：定时MAC包头 EHDR_ON=0：扩展包头禁止用作SYNC和RNG-REQ	8比特
MAC_PARM	保留为将来使用	8比特
LEN（SID）	LEN=n，包PDU的长度	16比特
EHDR	无扩展MAC包头	0字节
HCS	MAC包头校验序列	2字节
包数据	MAC管理消息： 同步信息（下行）； RNG-REQ（上行）。	n字节
定时MAC帧的长度		6+n字节

7.2.5.2　MAC 管理包头

MAC管理包头用于支持所需的MAC管理消息。该MAC包头应用于传送所有MAC管理消息（见7.3）。其格式如图27和表23所示。

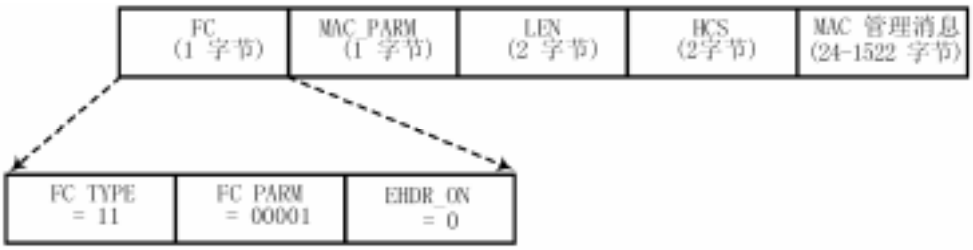


图27　MAC 管理包头

表23　MAC 管理包头格式

域	用法	长度
FC	FC_TYPE=11：MAC特定包头 FC_PARM[4：0]=00001：MAC管理包头 若无EHDR： EHDR_ON=0；若有则为1	8比特
MAC_PARM	MAC_PARM=x;若无EHDR,应设为0；否则设为EHDR的长度	8比特
LEN（SID）	LEN=n+x，包PDU的长度+EHDR的长度	16比特
EHDR	如果有EHDR，表示扩展MAC包头	x（0-240）字节
HCS	MAC包头校验序列	16比特
包数据	MAC管理消息	n字节
管理消息MAC帧的长度		6+x+n个字节

7.2.5.3　请求帧

请求帧是CM请求带宽用的基本机制，只适用于上行。请求帧后应没有数据PDU。请求帧的一般格式见图28和表24所示。

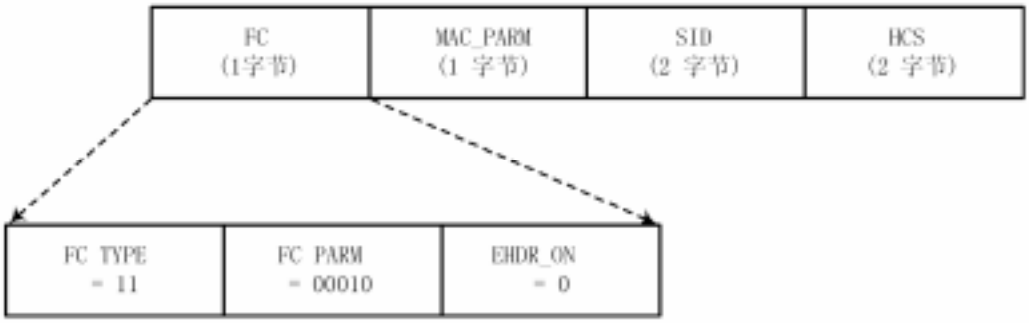


图28　请求帧格式

表24　请求帧（REQ）格式

域	用法	长度
FC	FC_TYPE=11：MAC特定包头 FC_PARM[4：0]=00010：只有MAC包头，无数据PDU跟随 EHDR_ON=0：不允许EHDR	8比特
MAC_PARM	REQ,请求的微时隙总数目	8比特
SID	SID（0...0x1FFF）	16比特
EHDR	不允许扩展MAC包头	0字节
HCS	MAC包头校验序列	2字节
REQ MAC包头长度		6字节

因为请求帧没有数据PDU，所以不需要LEN域。LEN域应用SID替代。SID应唯一地标识一个给定CM中的特定业务流。

带宽请求应以微时隙规定。REQ域应指示为该业务所请求的包括物理层开销在内的总带宽。

7.2.5.4　分段包头

分段MAC包头提供了将一个大的MAC PDU分割为若干个小片段并在CMTS中进行重组的基本机制，只用于上行方向。分段MAC包头的一般格式见图29和表25。

CM应支持分段，CMTS可以支持分段。为了减轻CMTS的负担及减少不必要的开销，分段包头不可用于非分段的帧。

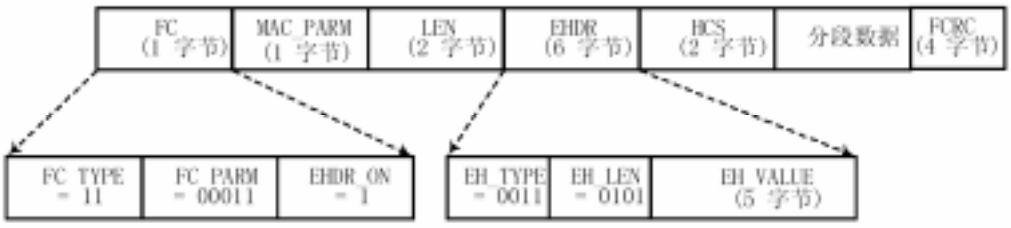


图29　分段 MAC 包头格式

表25　分段 MAC 帧（FRAG）格式

域	用法	长度
FC	FC_TYPE=11：MAC特定包头 FC_PARM[4：0]=00011：分段MAC包头 EHDR_ON=1：后跟分段EHDR	8比特
MAC_PARM	ELEN=6字节，分段EHDR的长度	8比特
LEN（SID）	LEN=分段有效负载长度+EHDR长度+FCRC长度	16比特
EHDR	见7.2.6.2	6字节
HCS	MAC包头校验序列	2字节
分段数据	分段有效负载，发送的总MAC PDU的一部分	n字节
FCRC	CRC：对分段数据有效负载的32比特CRC	4字节
MAC分段帧的长度		16+n个字节

7.2.5.5　级联包头

级联包头使得多个MAC帧可以进行级联，从而允许单个MAC“突发”在网上传送。PHY开销和级联MAC包头只出现一次。多个MAC帧的级联如图30所示。多个MAC帧的级联是CM能在一次传输机会中传送多个MAC帧的唯一方法。

注：物理层开销包括前同步码、保护时间以及最后一个码字中可能出现的零填充字节。FEC开销在每个码字中重复出现。

CM应支持级联，CMTS可以支持级联。级联只适用于上行业务，不能用于下行业务。

图30　多个 MAC 帧的级联

每个MAC“突发”，只能有一个级联MAC包头，不应嵌套级联。紧接在级联MAC包头之后的应是第一个MAC帧的MAC包头。MAC包头中的信息指示出第一个MAC帧的长度，并提供寻找下一个MAC帧起始位置的方法。级联的每一个MAC帧都应是唯一的，但可以是任何类型的帧。这表示包和MAC特定帧可以混合在一起。级联的所有帧应分配给同一业务流。如果CMTS支持级联，则应支持包含多个帧类型的级联，包括数据包和MAC特定帧。

嵌入的MAC帧可以有不同的目的地址，发送时应做到这些帧就象是独立传送一样。

级联MAC帧的格式如图31和表26所示。

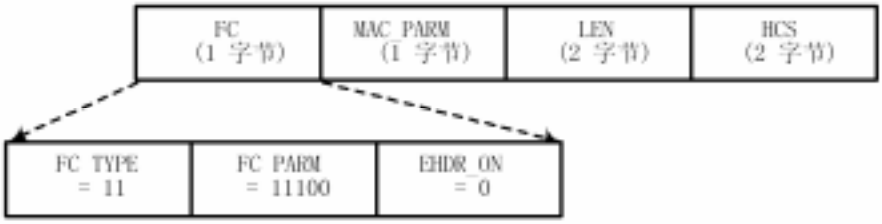


图31　级联 MAC 包头的格式

表26　级联 MAC 帧格式

域	用法	长度
FC	FC_TYPE=11：MAC特定包头 FC_PARM[4：0]=11100：级联MAC包头 EHDR_ON=0：级联包头无EHDR	8比特
MAC_PARM	CNT，级联MAC帧的数目 CNT=0表示未规定MAC帧的数目	8比特
LEN	LEN=x+...+y，后续MAC帧的字节长度	16比特
EHDR	不允许使用扩展MAC包头	0字节
HCS	MAC包头校验序列	2字节
MAC帧1	第一个MAC帧：MAC包头+可选的数据PDU	x字节
MAC帧n	最后一个MAC帧：MAC包头+可选的数据PDU	y字节
级联MAC帧的长度		6+LEN字节

级联MAC包头中的MAC_PARM域提供了MAC帧的数目。如果该域非零，则应指示该级联突发中的MAC帧的总数（CNT）。

7.2.6　扩展 MAC 包头

除定时MAC包头、级联MAC包头和REQ帧之外的每个MAC包头，都可以定义扩展包头域（EHDR）。EHDR域的出现通过FC域中的EHDR_ON标志设定来指示。一旦设定了EHDR_ON标志，MAC_PARM域就应被用作EHDR长度（ELEN）。EHDR最小定义为1字节，最大定义为240字节。

CMTS和CM应支持扩展包头。

带扩展包头的一般MAC包头的格式如图32和表27所示。

扩展包头不能用于级联MAC包头，但可以作为被级联的MAC包头的一部分。

扩展包头不能用于请求帧和定时MAC包头。

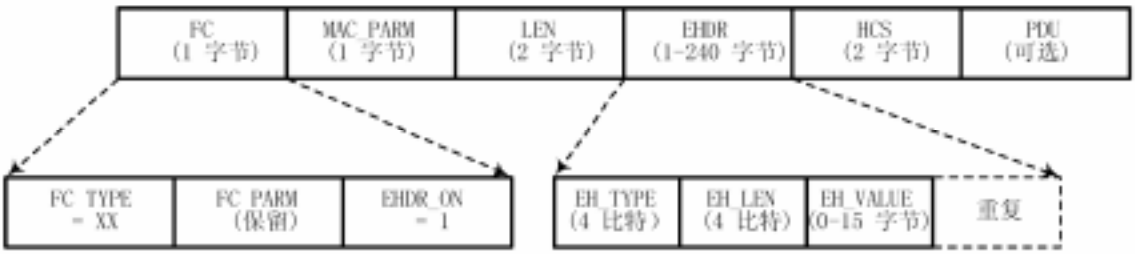


图32　扩展 MAC 格式

表27　扩展 MAC 包头格式

域	用法	长度
FC	FC_TYPE=xx：适用于所有MAC包头 FC_PARM[4：0]=xxxxx：取决于FC类型 EHDR_ON=1：有EHDR	8比特
MAC_PARM	ELEN=x，EHDR的长度，以字节为单位	8比特
LEN	LEN=x+y，EHDR长度+可选数据PDU长度	16比特
EHDR	扩展MAC包头	x字节
HCS	MAC包头校验序列	2字节
PDU	可选PDU	y字节
带有EHDR的MAC帧的长度		6+x+y字节

因为EHDR增加了MAC帧的长度，所以LEN域也应增加，其中包括PDU的长度和EHDR的长度。

EHDR域由一个或多个EH单字节组成。每个EH单元都是可变长度的。EH单元的第一个字节应包含一个类型域和一个长度域。每个CM都应使用该长度跳过任何未知的EH单元。EH单元的格式应如表28所示。

表28　EH 单元格式

EH单元域	用法	长度
EH_TYPE	EH单元类型域	4比特
EH_LEN	EH_VALUE的长度	4比特
EH_VALUE	EH单元数据	0-15字节

表29中定义的EH单元类型应得到支持。此处保留和扩展类型未被定义，应被忽略。

前10个EH单元类型用于CM与CMTS之间的单向传送，后面5个EH单元用于MAC子层域中的端到端传送。上行流中附属于EHDR的信息在转发时也应附上。最后一个EH单元类型是一种转义机制，允许更多的类型和更长的值，并应如表29所示。

表29　扩展包头类型

EH_TYPE	EH_LEN	EH_VALUE
0	0	空配置：可用于填充扩展包头。EH_LEN应为0，但配置设置可以重复。
1	3	请求：请求微时隙（1字节）；SID（2字节）[CM→CMTS]
2	2	请求确认；SID（2字节）[CM→CMTS]
3(=BP_UP)	4	上行加密EH单元（可选）
	5	带分段的上行加密EH单元（可选，见7.2.7）[a]
4(=BP_DOWN)	4	下行加密EH单元（可选）
5	1	业务流EH单元；下行有效负载包头抑制包头
6	1	业务流EH单元；上行有效负载包头抑制包头（1字节）
	2	业务流EH单元；上行有效负载包头抑制包头（1字节） 主动授权同步包头。（1字节）
7-9		保留
10-14		保留[CM→CMTS]
15	XX	扩展EH单元：EHX_TYPE（1字节），EHX_LEN（1字节），EH_VALUE（长度由EHX_LEN确定）
a：带分段的EH单元上行加密只能在分段MAC特定包头中出现(见7.2.5.4)。		

7.2.6.1　附带请求

一些扩展包头可被用于后续的传输请求带宽，这些请求一般称为附带请求。这对确保性能是极为有用的，因为此方式可避免一般请求帧所遇到的争用情况。

7.2.6.2　分段扩展包头

分段包是分段MAC头和上行加密扩展包头的组合，分段MAC包头参见7.2.5.4。带分段的上行加密扩展包头，即分段扩展包头的格式如表30所示。

表30　分段扩展包头格式

EH单元域	用法	长度
EH_TYPE	上行加密EH单元=3	4比特
EH_LEN	EH_VALUE的长度=5	4比特
EH_VALUE	Key_seq；与BP_UP中的相同	4比特
	Ver=1；EHDR版本号	4比特
	BPI_ENABLE 若BPI_ENABLE=0，则BPI关闭 若BPI_ENABLE=1，则BPI打开	1比特
	翻转比特，与BP_UP中的相同	1比特
	SID，与该分段相关的SID	14比特
	REQ，附带请求的微时隙数目	8比特
	保留，应置0	2比特
	First_Frag，只在第一个分段中置1	1比特
	Last_Frag，只在最后一个分段中置1	1比特
	Frag_seq，分段顺序计数，每个分段加1	4比特

7.2.6.3　业务流扩展包头

业务流扩展EH单元用来增强业务流的操作，由EH_VALUE中的一个或两个字节组成。有效负载包头抑制包头是一字节域中的唯一字节，或是两字节域中的第一个字节。非请求型同步包头是两字节域中的第二个字节。

7.2.6.3.1　有效负载包头抑制包头

在有效负载包头抑制（PHS）中，跟在HCS之后的有效负载包头中的重复部分由发送实体抑制，并由接收实体恢复。在上行方向，发送实体是CM，接收实体是CMTS。在下行方向，发送实体是CMTS，接收实体是CM。

对于有效负载较少的情况，有效负载包头抑制不必使用压缩技术，就能提高带宽利用率。有效负载包头抑制可以在上行和下行方向分别预置并以扩展包头单元为参考。

CM应支持有效负载包头抑制，CMTS可以支持有效负载包头抑制。

注：并不要求CM应能决定何时调用有效负载包头抑制，只在明确告知的情况下支持。

有效负载包头抑制扩展包头子单元格式如表31所示。

表31　有效负载包头抑制 EHDR 子单元格式

EH单元域	用法		长度
EH_TYPE	下行：EH_TYPE=5 上行：EH_TYPE=6		4比特
EH_LEN	EH_VALUE的长度=1		4比特
EH_VALUE	0	表示当前包中没有有效负载包头抑制	8比特
	1-255	有效负载包头抑制索引（PHSI）	

有效负载包头抑制索引在上行方向对每个SID是唯一的，在下行方向对每个CM是唯一的。如果该扩展包头单元被省略，则关闭有效负载包头抑制；如果有该扩展包头单元，则PHSI值被置为0。PHSI以被抑制的字节（即有效负载包头抑制域（PHSF））为参考。

注：PHS信令允许每个业务流最多可有255种有效负载抑制规则，实际可支持的PHS规则数目取决于设备实现。为了实现互操作，任何PHS规则都应支持64个字节的最小PHS长度。和动态业务请求中的其他请求参数一样，一个PHS相关的动态业务请求可以由于缺少资源而被拒绝。

上行抑制域应从紧接MAC包头校验和之后的第一个字节开始。下行抑制域应从MAC包头校验和之后的第13个字节开始。这样，CM就可以过滤以太网SA和DA。

PDU CRC应始终发送，且应只在被发送的字节上运算，被抑制的字节不应进行CRC运算，整个PDU被抑制的情况除外。

7.2.6.3.2 主动授权同步包头

主动授权同步包头可被用于传递CM和CMTS之间的业务流调度状态信息，本部分中只用于上行中的主动授权和带活动检测调度业务的主动授权（见9.2）。

该扩展包头与有效负载抑制EHDR相似，但EH-LEN为2，EH_VALUE多了一个关于主动授权同步信息的字节，见表32。对于所有其它业务流调度类型，该域不能出现在由CM产生的扩展包头单元中。CMTS可忽略该域。

表32 主动授权同步 EHDR 子单元格式

EH单元域	用法		长度
EH_TYPE	EH_TYPE=6		4比特
EH_LEN	EH_VALUE的长度=2		4比特
EH_VALUE	0	表示当前包中没有有效负载包头抑制	8比特（始终出现）
	1-255	有效负载包头抑制索引（PHSI）	
	队列指示符		1比特
	活动授权		7比特

7.2.7 分段 MAC 帧

如果允许分段，则在授权长度小于所请求的长度时进行分段。分段一般发生在CMTS授权的带宽比请求带宽小的时候。见图33。

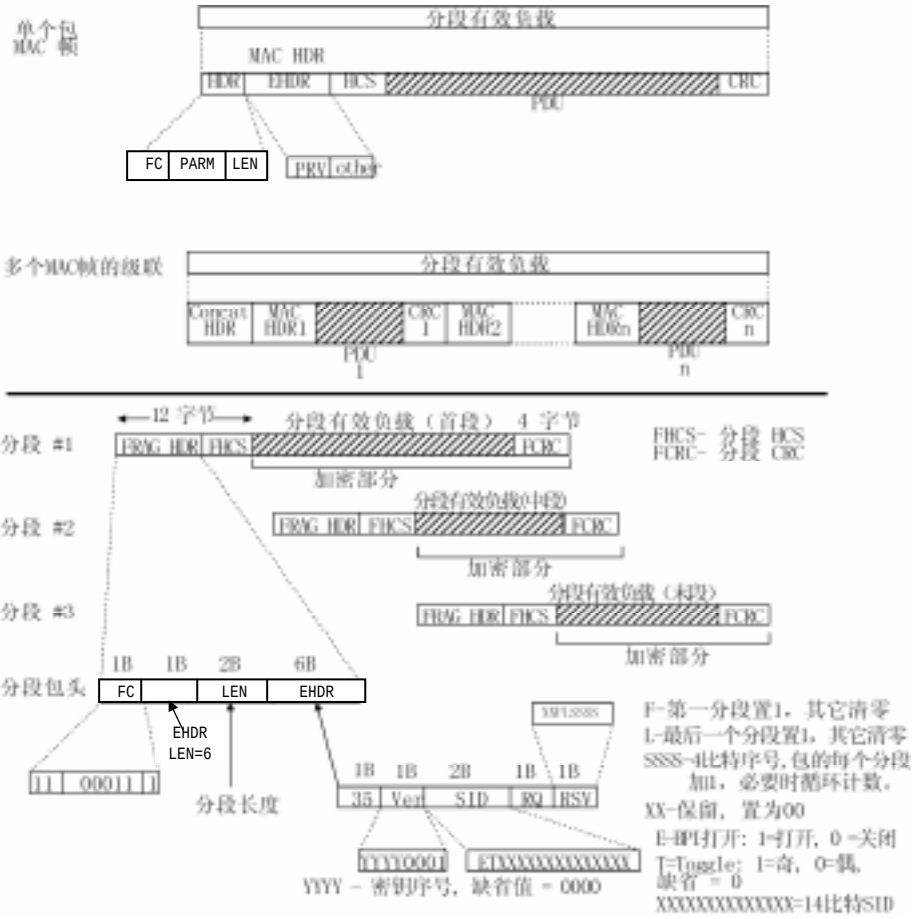


图33　分段细节

CM MAC计算收到的授权中可以发送的包括分段包头和CRC开销在内的原始帧的字节数。CM MAC为每一个分段产生一个分段包头。为了唯一地标识该分段包头，分段帧使用MAC消息类型（FC＝11），FC参数域被置为00011。为了重组和检测分段丢失，在扩展包头域的最后一个字节有一个4比特的序列域。CM为一个帧的第一个分段任意分配一个序号，第一个分段的序号一经选定，则每发送该帧的一个分段，CM使序号加1。与序号相关的有2个标记：F和L，F置1表示第一个分段，L置1表示最后一个分段，二者均为0表示中间的分段。CMTS存贮每个帧的第一个分段的序号，且应验证帧的每一个分段的序号逐次加1。

基于分段协议，分段包头中的REQ域用于第一个和中间的分段（见9.3）。对最后一个分段，REQ域用做后续帧的带宽请求。

分段包头的长度是固定的，并应只能含有一个分段扩展包头单元。扩展包头包括一个增加了一个字节的加密EH单元，以使分段开销长度恰好达到16字节。无论原始包头是否含有加密EH单元，都要使用加密EH单元。本部分中没有使用加密，但预留了加密EH单元且使能比特清零。分段EH单元使用中的SID应与发起分段的部分授权中用的SID相匹配。每个分段独立进行CRC运算（注意每个MAC帧有效负载也包含该包的CRC）。尽管每个分段都有一个FCRC，CMTS仍可对重组的包进行CRC校验。

CMTS应保证它所发出的任何分段授权都大到足以支持最少17个字节的MAC层数据。该大小与分段开销再加上至少1字节的数据相适应。因为小的分段效率不高，CMTS可能强制分配一个更大的限制。

级联包和分段

MAC管理消息和数据PDU可以在同一个级联帧中。

7.2.8　出错处理

HFC网络的环境会导致各种错误状况的产生。本条与10.5将描述发生在MAC成帧级的错误需要的处理过程。

最常见的一种MAC成帧级错误是MAC包头中的HCS错误。这种错误因网络噪声或上行信道中冲突而产生。下行信道的成帧恢复由MPEG传输会聚子层来完成。上行信道中，成帧恢复在每个被传送的突发上进行，这样，每个突发的成帧都与前一个突发成帧无关。因而，对于一个突发中的帧错误的处理，只是简单地忽略该突发。即在下一个突发之前错误不可恢复。

第二个异常只适用于上行，发生在长度域被破坏时，因此MAC层认为该帧比实际长度更长或更短。在下一个有效上行数据间隔中可以恢复同步。

对于每个MAC帧的传输，都应进行HCS验证。当检测到错误的HCS时，MAC包头及其有效负载应被丢弃。

对于PDU的传输，可能检测到坏的CRC。由于CRC只覆盖数据PDU而HCS覆盖MAC包头，所以MAC包头仍被认为是有效的。但数据PDU应被丢弃， MAC包头中的任何相关信息（例如带宽请求信息）仍可以被使用。

7.2.8.1 分段中的错误恢复

对于分段，有一些特殊的错误处理手段。每个分段都有自己的以HCS结尾的分段包头和自己的FCRC，在分段有效负载中还可以有其它的MAC包头和CRC。但是，在分段重组过程中只有分段包头中的HCS和FCRC用于错误检测。

如果一个分段的HCS校验失败，CMTS应丢弃该分段。如果HCS校验通过而FCRC校验失败，CMTS应丢弃该分段，但可以处理分段包头中的任何请求。如果一个请求在附带模式下进行分段，则CMTS应处理该请求（见9.3.2.2）。该帧的剩余部分可以尽可能迅速地传送。

如果CMTS在多授权模式下进行分段（见9.3.2.1），即使有分段丢失或被丢弃，也应完成所有必要的授权来满足CM的最初请求。该帧的剩余部分可以尽可能迅速地传送。

如果一个非级联MAC帧的任何分段丢失或被丢弃，则CMTS应丢弃该帧的剩余部分。如果一个级联MAC帧中有一个分段丢失或被丢弃，则CMTS可以转发该级联中的其他接收正确的帧，或可以丢弃该级联中的所有帧。

如果一个给定SID的任何分段上发生下述情况，则CMTS应终止分段重组：

- CMTS 接收到一个 L 比特置 1 的分段；
- CMTS 接收到一个 F 比特置 1 但不是第一个分段的上行分段；
- CMTS 接收到一个没有分段包头的 PDU 帧；
- CMTS 删除了该 SID。

此外，CMTS可以依据设备实现（例如重组定时器）来终止分段重组。CMTS终止分段重组时应丢弃或转发已重组的帧。

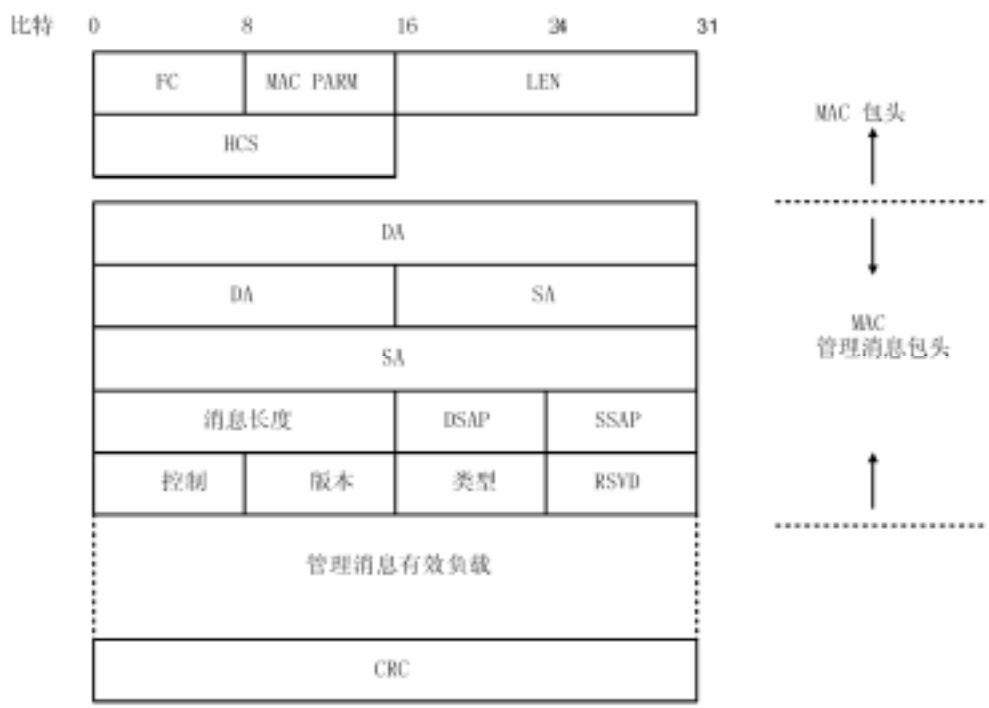
7.2.8.2 错误代码和消息

附录I列出了CM和CMTS的错误代码和错误消息。在报告错误状况时，应使用错误代码，在设备供应商专用接口上也可使用错误代码报告错误状况。如果使用了错误代码，则可以用其它描述性消息来取代错误描述消息。

7.3 MAC 管理消息

7.3.1 MAC 管理消息包头

MAC管理消息应按照GB/T 15629.2封装在LLC无编号消息帧中，然后封装在HFC网络的MAC帧中。图34所示是所有MAC管理消息公用的MAC包头和MAC管理消息包头域。



各参数定义如下：

FC、MAC、PARM、LEN、HCS：公共 MAC 帧包头，见 7.2.1.4。所有消息使用 MAC 特定包头；

目的地址（DA）：MAC 管理帧被赋以特定的 CM 单播地址或管理组播地址。MAC 管理地址见附录 A；

源地址（SA）：源 CM 或 CMTS 系统的 MAC 地址；

消息长度：从 DSAP 到有效负载结尾的 MAC 消息的长度；

DSAP：GB/T 15629.2-1995 定义的 LLC 空目的 SAP（00）；

SSAP：GB/T 15629.2-1995 定义的 LLC 空源 SAP（00）；

控制：GB/T 15629.2-1995 定义的无编号信息帧（03）；

版本和类型：各占 1 个 8 位字节，见表 33；

RSVD：1 个 8 比特组。该域用于消息有效负载在 32 比特边界上的定位。本部分置 0；

管理消息有效负载：可变长度。每个管理消息分别定义；

CRC：覆盖含包头域（DA，SA，…）在内的消息。生成多项式的定义见 GB/T15629.3-1995。

图34　MAC 包头和 MAC 管理消息包头域

CMTS和CM应支持表33中的MAC管理消息类型。

表33　MAC 管理消息类型

类型值	版本	消息名称	消息描述
1	1	SYNC	定时同步
2	1	UCD	上行信道描述符
3	1	MAP	上行带宽分配
4	1	RNG-REQ	测距请求
5	1	RNG-RSP	测距响应
6	1	REG-REQ	注册请求
7	1	REG-RSP	注册响应
8	1	UCC-REQ	上行信道变更请求
9	1	UCC-RSP	上行信道变更响应
10	1	TRI-TCD	电话信道描述符（待定）
11	1	TRI-TSI	终端系统信息（待定）
12	1	BPKM-REQ	加密密钥管理请求（待定）
13	1	BPKM-RSP	加密密钥管理响应（待定）
14	2	REG-ACK	注册确认
15	2	DSA-REQ	动态业务添加请求
16	2	DSA-RSP	动态业务添加响应
17	2	DSA-ACK	动态业务添加确认
18	2	DSC-REQ	动态业务变更请求
19	2	DSC-RSP	动态业务变更响应
20	2	DSC-ACK	动态业务变更确认
21	2	DSD-REQ	动态业务删除请求
22	2	DSD-RSP	动态业务删除响应
23	2	DCC-REQ	动态信道变更请求
24	2	DCC-RSP	动态信道变更响应
25	2	DCC-ACK	动态信道变更确认
26	2	DCI-REQ	设备类别识别请求
27	2	DCI-RSP	设备类别识别响应
28	2	UP-DIS	上行发射机关闭
29～255			保留为将来使用

7.3.2　定时同步（SYNC）

CMTS应周期性地传送定时同步（SYNC）消息来建立MAC子层的定时。该消息应使用FC_TYPE=MAC特定包头和FC_PARM=定时MAC包头的FC域，其后应跟随如图35所示的包PDU。

CMTS 时戳：以 CMTS 10.24MHz 主时钟为基准计时的 32 比特二进制计数器的计数状态。

图35　定时包头后的包 PDU 格式

CMTS时戳表示的是定时同步MAC管理消息的第一个字节（或是对第一个字节有固定偏移量）从下行传输会聚子层送到下行PMD子层瞬间的计数状态，见5.2.7。CMTS不允许SYNC消息跨越一个MPEG包的边界。

注： SYNC消息应用于此MAC域中的所有上行信道特性，与上行信道调制符号率无关。

7.3.3　上行信道描述符（UCD）

CMTS应周期性地发送上行信道描述符消息来规定上行信道的特性。该消息应对每个激活的上行信道分别发送。

紧接信道ID之后的的消息参数都应按照TLV的格式进行编码，其中类型和长度域各占一个字节。

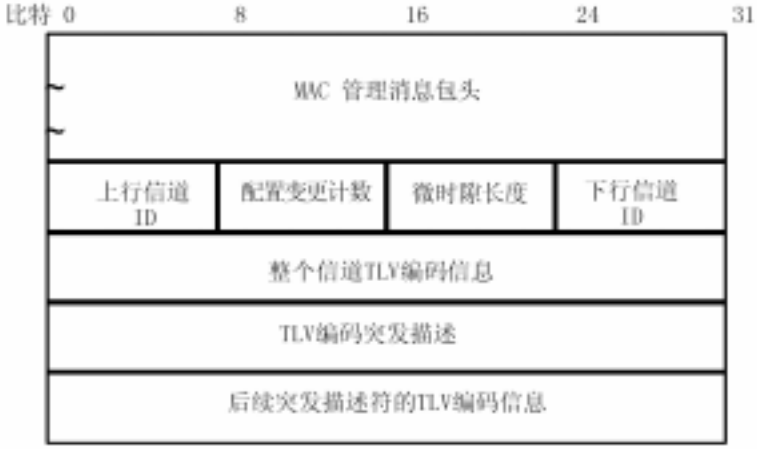


图36　上行信道描述符

CMTS应按照图36所示格式产生UCD，包括下述所有参数：

- 配置变更计数：该信道描述符的值发生任何改变，CMTS 就将计数值加 1（以域长度为模）。如果后续 UCD 中的此计数值保持一致，CM 可以立即确定剩余的域没有改变，可以忽略该消息的剩余部分。该值还可以从 MAP 中引用；
- 微时隙大小：上行信道的微时隙大小 T 以 6.25μs 为时间单元。允许 $T=2^M$，M=1、…7。即 T=2、4、8、16、32、64 或 128；
- 上行信道 ID：该信息所属的上行信道的标识符。该标识符由 CMTS 选定，在 MAC 子层域中是唯一的；
- 下行信道 ID：传送该信息的下行信道的标识符。该标识符由 CMTS 选定，在 MAC 子层域中是唯一的。

所有其它参数都编码为TLV字节组。类型值的取值应符合表34对信道参数和表35对上行物理层突发属性的规定。信道宽度参数（表34类型1-3）应在突发描述符（表35类型4）之前。

表34　信道 TLV 参数

名称	类型 (1字节)	长度 (1字节)	值 (可变长度)
符号率	1	1	160ksym/s基本速率的倍数（值为1，2，4，8或16）
频率	2	4	上行中心频率（Hz）
前同步码模式	3	1～128	前同步码超字符串。所有突发特定的前同步码值都是从该字符串中选出的子字符串。 前同步码超字符串的头8个比特位于该域的第一个字节，第1个比特是该域第一个字节的MSB，第8个比特是该域第一个字节的LSB；该域的第二个字节包含前同步码超字符串的第二个8比特，第9个比特是第二个字节的MSB，第16个比特是第二个字节的LSB；以此类推。
突发描述符	4	n	可能出现不止一次，下文描述。

突发描述符是由TLV编码的上行间隔使用码组成，它定义每一类上行使用间隔中所使用的物理层特性。上行间隔使用编码在MAP消息中定义（见7.3.4和表36）。突发描述符的格式如图37所示。

类型：4，为突发描述符；

长度：总字节数，包括 IUC 和嵌入的 TLV 项；

IUC：在表 36 中定义的间隔使用码，使用低 4 位，不使用高 4 位（=0）；

TLV：TLV 参数在表 35 中描述。

图37　突发描述符的上层编码

每个用于分配MAP消息的间隔使用码都应包括一个突发描述符。间隔使用码应是表36中的值。

在每个突发描述符中都有一个无序的物理层属性列表，编码为TLV值。这些属性见表35。

表35　上行物理层突发属性

名称	类型 (1字节)	长度 (1字节)	值 (可变长度)
调制类型	1	1	1=QPSK，2=16QAM
差分编码	2	1	1=开，2=关
前同步码长度	3	2	最大1024比特。该值应是整数个符号（对QPSK是2的倍数，对16QAM是4的倍数）。
前同步码值偏移	4	2	标识用于前同步码值的比特，它被规定为前同步码模式（见表34）中的起始偏移。即0值表示该突发类型的前同步码的第一个比特的值是前同步码模式中的第一个比特；100表示该前同步码使用前同步码模式中第101个比特及其后续比特。该值应是符号长度的整倍数。 前同步码模式的第一个比特首先进入符号映射器（见图13），而且是该突发的第一个符号的I_1（见5.1.2.2）。
FEC纠错（T）	5	1	0～10（0表示无FEC，码字奇偶校验字节数为2T）
FEC码字信息字节（k）	6	1	固定：16～253（假定有FEC） 截短：16～253（假定有FEC） （无FEC时不用，T=0）
加扰器种子	7	2	15比特，在该2字节域中左对齐。比特15是第一个字节的MSB，第二个字节的LSB不使用（若加扰器关闭则不使用）
最大突发长度	8	1	该突发类型中可传送的微时隙的最大数目。若没有配置，则表示突发长度在其它地方限制。当间隔类型是短数据授权时，该值应出现且应大于0。（见8.1.2.5）
保护时间长度	9	1	紧跟突发结束的符号数。（该值虽然可以从网络和结构参数中得到，这里包含它是为了保证CM和CMTS都使用相同的值。）
最后码字的长度	10	1	1=固定，2=截短
加扰器开/关	11	1	1＝开，2＝关

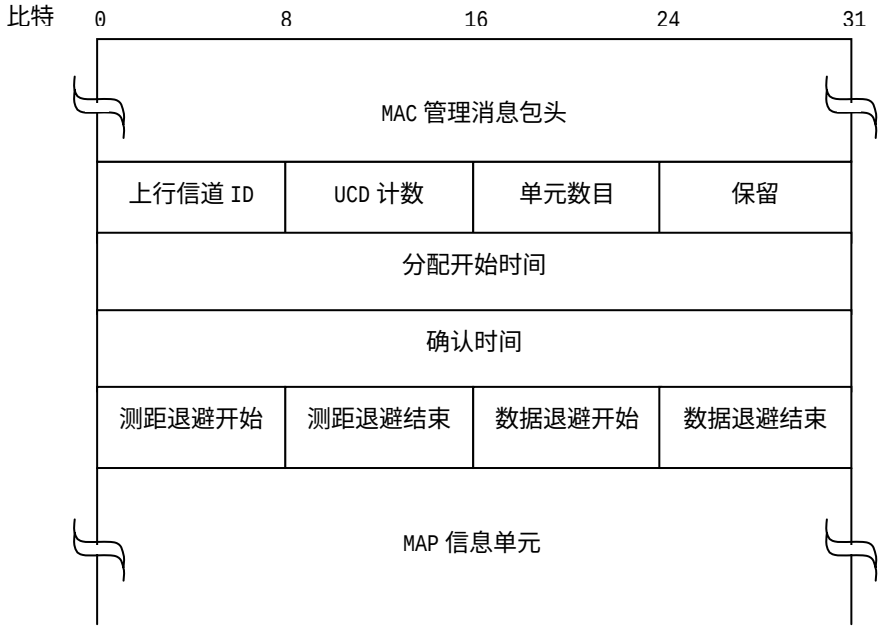
图38是一个UCD编码TLV数据的示例。

类型 1	长度 1	符号 速率
类型 2	长度 4	频率
类型 3	长度 1-128	前同步码超字符串
类型 4	长度 N	第一个突发描述符
类型 4	长度 N	第二个突发描述符
类型 4	长度 N	第三个突发描述符
类型 4	长度 N	第四个突发描述符

图38　UCD 编码 TLV 数据示例

7.3.4　上行带宽分配 MAP

CMTS应按照图39所示格式产生MAP消息。



各参数定义如下：

上行信道 ID:该消息所对应的上行信道的标识符；

UCD 计数:与描述该 MAP 消息突发参数的 UCD 的配置改变计数器相匹配；

单元数目:该 MAP 中信息单元的数目；

保留:用于边界对齐的保留域；

分配开始时间:CMTS 开始（在微时隙中）初始化分配的有效时间；

确认时间:最新时间，来自 CMTS 初始化后上行方向处理的微时隙。该时间被 CM 用于碰撞检测，见 8.4；

测距退避开始:初始测距争用的初始退避窗口，以 2 的幂次表示。值的范围在 0～15 之间（高位不用，应置 0）；

测距退避结束:初始测距争用的最终退避窗口，以 2 的幂次表示。值的范围在 0～15 之间（高位不用，应置 0）；

数据退避开始:争用数据和请求的初始退避窗口，以 2 的幂次表示。值的范围在 0～15 之间（高位不用，应置 0）；

数据退避结束:争用数据和请求的最终退避窗口，以 2 的幂次表示。值的范围在 0～15 之间（高位不用，应置 0）；

MAP 信息单元:如图 40 和表 36 的格式。IUC 的值见表 36 和 8.1.2。

注： 分配开始时间和确认时间的低位（26-M）比特应是有效的MAP开始和确认时间，M值见7.3.3。分配开始/确认时间计数器和时戳计数器之间的关系见8.4。

图39　MAP 格式

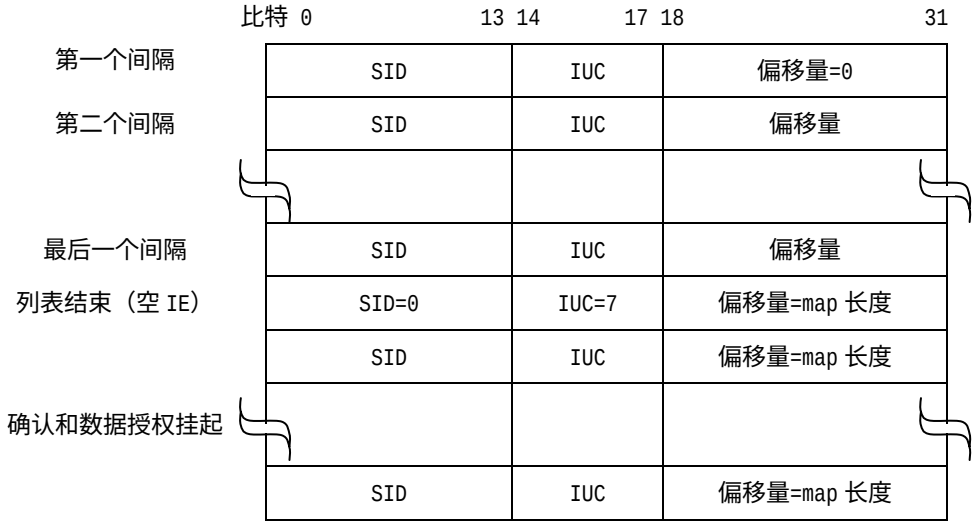


图40　MAP 信息单元结构

表36　分配 MAP 信息单元（IE）

IE名称[a]	间隔使用码(IUC) (4比特)	SID (14比特)	微时隙偏移（14比特）
请求	1	任意	REQ区域的开始偏移
REQ/数据(组播定义见附录A)	2	组播	IMMEDIATE数据区域的开始偏移 （常用的组播定义开始间隔）
初始维护	3	广播	MAINT区域的开始偏移（用于初始测距）
台站维护[b]	4	单播[c]	MAINT区域的开始偏移（用于周期测距）
短数据授权[d]	5	单播	数据授权分配的开始偏移；如果推算的长度=0，则是一个数据授权挂起。
长数据授权	6	单播	数据授权分配的开始偏移；如果推算的长度=0，则是一个数据授权挂起。
空IE	7	0	前一授权的结束偏移，用于最后一个实际间隔分配的长度定界。
数据确认	8	单播	CMTS置为map长度。
保留	9-14	任意	保留
扩展	15	扩展IUC	该IE中附加32比特码字数

a 每个 IE 都是 32 比特，最高 14 位比特表示 SID，中间 4 比特表示 IUC，低 14 比特是微时隙偏移。

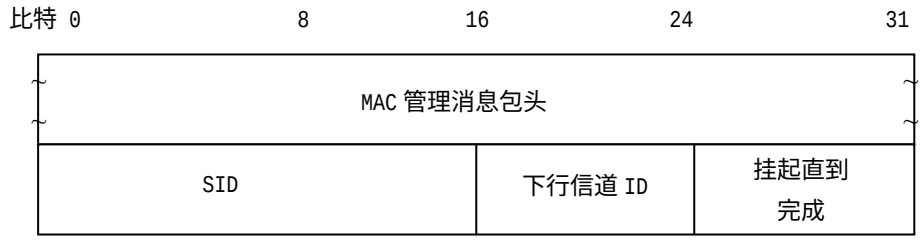
b 虽然初始维护和台站维护从 SID 类型就可以完全区分开来，但为了简化物理层的配置，仍使用了不同的编码（见表 35 突发描述符编码）。

c 用于台站维护 IE 的 SID 应是一个临时 SID，或是在 REG-RSP 消息中分配给 CM 的第一个注册 SID（可以是唯一的）。

d 长数据授权和短数据授权之间的区别在于该授权中可传送的数据数量。短数据授权间隔使用适于短包的 FEC 参数，而长数据授权的 FEC 编码利用率更高。

7.3.5　测距请求（RNG-REQ）

CM应在初始化时周期性地发送测距请求，请求CMTS确定网络时延和请求功率调整。该消息应使用FC_TYPE=MAC特定包头和FC_PARM=定时MAC包头，后接符合图41格式的PDU。



各参数定义如下：

SID：对于在初始维护间隔中传送的 RNG-REQ 消息：

- 如果 CM 试图加入网络，则为初始化 SID；
- 如果尚未注册的 CM 根据下载的参数文件变更下行（或上行和下行）信道，则为初始化 SID；
- 如果尚未注册的 CM 根据下载的参数文件变更上行（而非下行）信道，则为临时 SID；
- 如果已注册的 CM 变更上行信道，则为注册 SID（之前在 REG-RSP 中已分配）。

对于在台站维护间隔中传送的 RNG-REQ 消息：为分配的 SID。

该域是一个 16 比特域，低 14 位比特定义 SID，比特 14、15 置 0。

下行信道 ID：下行信道标识符，CM 在该下行信道上接收描述上行信道特性的 UCD。该域是一个 8 比特域。

挂起直到完成：如果为 0，则发送该请求之前已经使用了先前的所有测距响应属性。如果非 0，则该域预计完成测距参数同化所需的时间。需要注意的是只有均衡可以延迟。单位是无符号的百分之一秒（10ms）。

图41　定时包头后的包 PDU

7.3.6　测距响应（RNG-RSP）

CMTS应发送测距响应消息来响应收到的RNG-REQ消息。对测距过程状态机的描述见10.2.4。在该过程中需要注意， CM应准备好随时接收测距响应，不仅仅是在测距请求之后。

接在上行信道ID之后的消息参数应以TLV的格式进行编码。

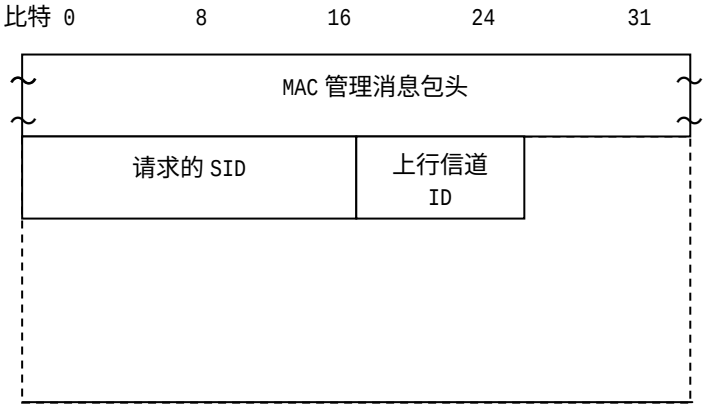


图42　测距响应

CMTS应按照图42所示格式产生测距响应消息，包括如下参数：

- SID：如果该响应消息通知 CM 更换信道，则为初始化 SID；否则，是所响应的 RNG-REQ 消息给出的 SID。但如果相应的 RNG-REQ 是一个规定了初始化 SID 的初始测距请求，则该 SID 是一个临时分配的 SID；
- 上行信道 ID：上行信道标识符，CMTS 在该上行信道上收到此响应消息的相应 RNG-REQ。在初始测距期间，CM 接受到的第一个测距响应中，该信道 ID 可能不同于 CM 用来发送测距请求的信道 ID（见附录 G）。因此，CM 应将该信道 ID 用于后续的交互，而不是其初始化测距请求的信道 ID。

所有其它参数编码为TLV字节组：

- 测距状态：用于指示在可接受的限值内 CMTS 是否收到了上行信息；

- 定时调整信息：为了使帧在期望的微时隙到达 CMTS 而使帧传输偏移的时间；
- 功率调整信息：为了使传输帧以期望的功率到达CMTS而规定的CM在传输功率电平的相对变化；
- 频率调整信息：为了更好地与 CMTS 相匹配而规定的 CM 在传输频率上的相对变化。（这是一个信道内的频率微调，而非不同信道的重新再分配）；
- CM 发射机均衡信息：为预均衡器提供均衡系数（可选）；
- 下行频率置换：可选参数，CM 应重新进行初始测距的下行频率。（见 7.3.6.3）；
- 上行信道 ID 置换：可选参数，CM 应重新进行初始测距的上行信道的标识符（见 7.3.6.3）。

7.3.6.1 编码

类型值如表37和图43所示，它们在测距响应消息中应是唯一的，但在整个MAC消息集中并非唯一的。类型和长度域应各占1个字节。

表37 测距响应消息编码

名称	类型（1字节）	长度（1字节）	值（可变长度）
定时调整	1	4	发送时间偏移调整（有符号的32比特，以6.25μs/64为单位）
功率电平调整	2	1	发送功率偏移调整（有符号的8比特，以1/4dB为单位）
频率偏移调整	3	2	发送频率偏移调整（有符号的16比特，以Hz为单位）
发送均衡调整	4	n	发送均衡数据
测距状态	5	1	1=继续，2＝放弃，3＝成功
下行频率置换	6	4	新的下行信道的中心频率（Hz）
上行信道ID置换	7	1	新的上行信道的标识符
保留	8～255	n	保留为将来使用

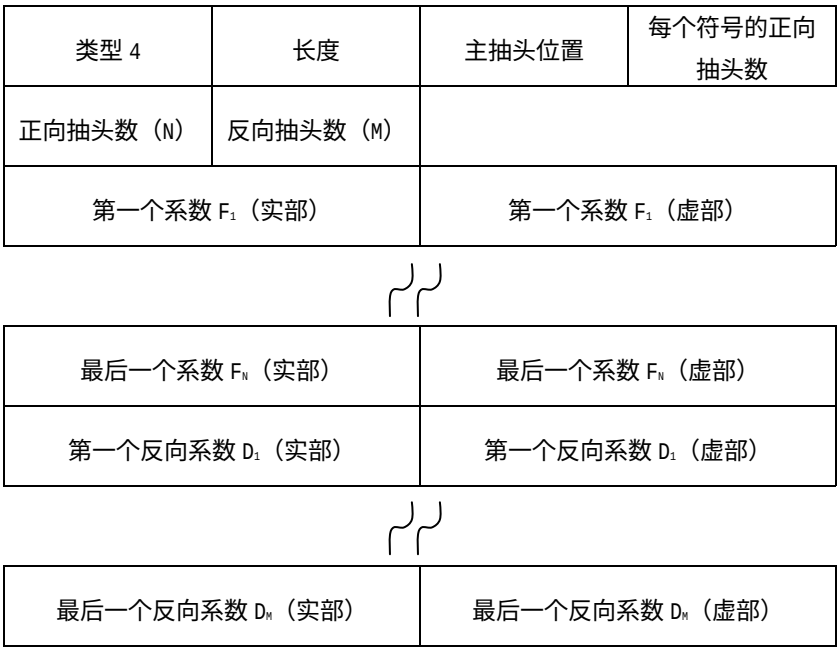


图43 一般判决反馈均衡系数

每个符号的正向抽头数应是1、2或4个。相当于0延时的主抽头位置在1和N之间。对于符号间隔的均衡器来说，每个符号的正向抽头数域应设定为“1”。 对于线性均衡器来说，反向抽头数（M）域应设定为“0”。总抽头数可达64个。每个抽头有一个实部和虚部系数。通用均衡器抽头位置定义见图44。

如果表达均衡信息要超过255字节，可以使用若干个类型为4的单元。数据应按照字节连续的方式来处理，即第二个类型为4的单元的长度域的第一个字节应紧接在第一个类型为4的单元的最后一个字节。

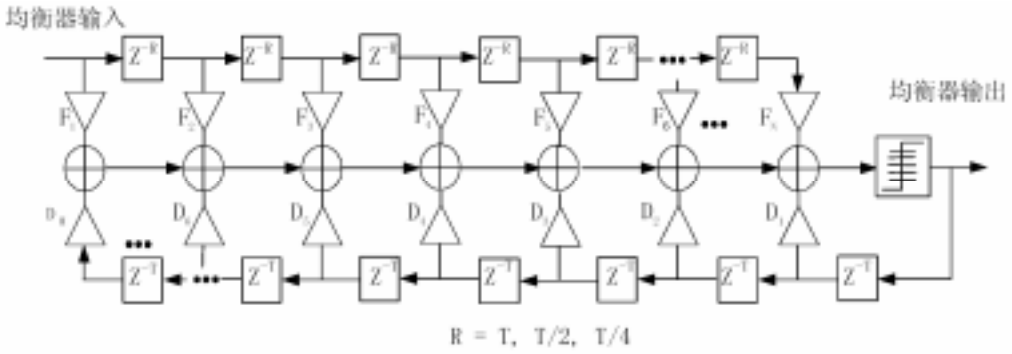


图44　通用均衡器抽头位置定义

7.3.6.2　TLV 数据示例

图45是TLV数据的一个例子。

类型1	长度4	定时调整
类型2	长度1	功率调整
类型3	长度2	频率调整信息
类型4	长度x	CM发端均衡信息：x字节
类型5	长度1	测距状态

图45　TLV 数据示例

7.3.6.3　在初始测距期间置换信道

RNG-RSP消息允许CMTS通知CM更换一个新的下行和/或上行信道并重新进行初始测距。但是，CMTS只有在响应欲加入网络的CM的初始测距请求时，或是响应从初始测距到CM周期性测距成功完成之间发生的任何一个单播测距请求时才能这么做。如果RNG-RSP消息中规定了下行频率置换，则CM应使用规定的下行中心频率重新初始化它的MAC层，并完成初始测距。对于上行信道，CM可根据收到的UCD消息选择任何有效信道。

如果RNG-RSP中规定了上行信道ID置换，则CM应重新初始化它的MAC层并使用规定的上行信道和接受RNG-RSP时所用的下行频率作为第一次尝试进行初始测距。

如果RNG-RSP中规定了下行频率和上行信道ID置换，则CM应重新初始化它的MAC层，并使用规定的下行频率和上行信道ID作为第一次尝试来进行初始测距。

若一个已分配了临时SID的CM被通知更换到新的下行和/或上行信道并重新进行初始测距，则CM应考虑解除该临时SID的分配。CM应使用初始化SID重新进行初始测距。

通过配置文件来设置上行信道ID和下行频率是可选的，但如果配置文件中进行了规定，则优先于测距响应参数。一旦测距完成，则只有C.1.1.2和UCC-REQ/ DCC-REQ机制可以将CM置换到一个新的上行信道，只有C.1.1.1和DCC-REQ中描述的机制可以将CM置换到一个新的下行信道。

7.3.7　注册请求（REG-REQ）

CM初始化收到CM参数文件后应发送注册请求消息。

SID后的消息参数应编码为类型/长度/值（TLV）的格式。

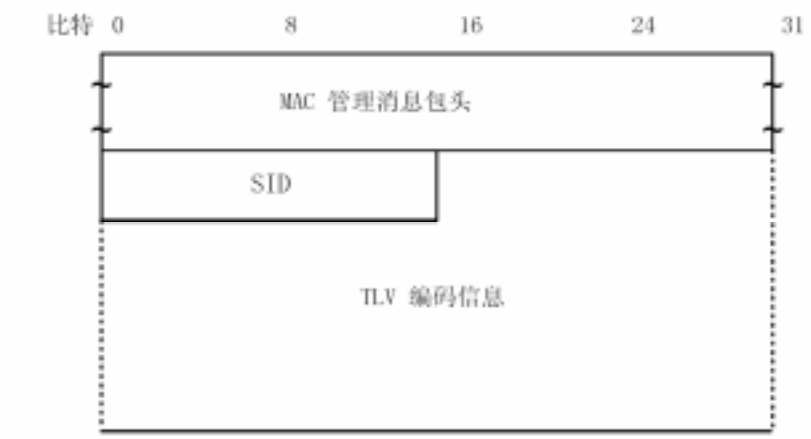


图46　注册请求

CM应按照图46所示格式产生注册请求，包括以下参数：

SID：该CM的临时SID；

其它参数编码为TLV字节组，定义见附录C。

注册请求消息可含有许多不同的TLV参数，其中一些由CM根据配置文件设置，另一些可由CM自己产生。如果在配置文件中含有下述设置，则下述请求设置应包括在注册请求中。

配置文件设定：

- 下行频率配置设定；
- 上行信道 ID 配置设定；
- 网络接入控制；
- 上行包分类配置设定；
- 下行包分类配置设定；
- 业务分类配置设定；
- 上行业务流配置设定；
- 下行业务流配置设定；
- 加密配置设定；
- CPE 最大数目；
- 分类器最大数目；
- 加密使能配置设定；
- 有效负载包头抑制；
- TFTP 服务器时戳；
- TFTP 服务器预置的 CM 地址；
- 厂商特定信息配置设定；
- CM MIC 配置设定；
- CMTS MIC 配置设定。

注： CM应按照配置文件中的顺序将厂商特定配置设定转发给CMTS，以保证消息的完整性。

在注册请求中应包含以下注册参数：

- 厂商特定参数：

厂商ID配置设定（CM的厂商ID）；

- 在注册请求中还应包含以下注册参数：

CM能力编码（根据C.1.3.1的限制，CM应在注册请求消息中确定其所有能力。如果CM在注册请求消息中没有明确指定，则CMTS不应假定CM的任何能力。）；

- 在注册请求中还可包含以下注册参数：

CM IP地址；

- 在注册请求中以下注册参数不应转发给 CMTS：
  1） 软件升级文件名；
  2） 软件升级 TFTP 服务器 IP 地址；
  3） SNMP 写访问控制；
  4） SNMP MIB 对象；
  5） SNMPv3 Kickstart 值；
  6） CPE 以太 MAC 地址；
  7） HMAC 摘要；
  8） 结束配置设定；
  9） 填充配置设定；
  10）电话设定选项。

7.3.8 注册响应（REG-RSP）

CMTS响应收到的REG-REQ消息时应发送注册响应消息。

响应域后的消息参数应按照TLV格式编码。

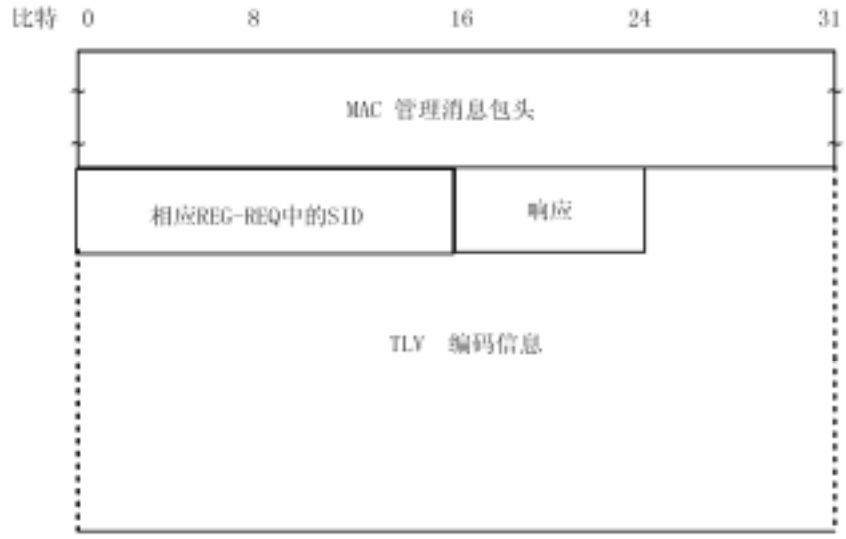


图47 注册响应消息格式

CMTS应按照图47所示格式产生注册响应消息，包括以下参数：

- 相应 REG-REQ 消息中的 SID：所响应的 REG-REQ 消息中的 SID（起交互作用）。
- 响应:对于 EuroDOCSIS 1.0 的 CM，REG-RSP 响应中包括：
  0＝OK；
  1＝鉴权失败；
  2＝业务类别失败。
  对于本部分的 CM，CMTS 发送的 REG-RSP 消息应包含附录 C.4 和 C.4.2 中定义的确认码。

注： 失败是指整个注册请求失败，即使仅有一个被请求业务流或EuroDOCSIS 1.0业务类别无效或不可传递，则整个注册就算失败。

如果REG-REQ成功，并且含有业务流参数、分类器参数、有效负载包头抑制参数，则REG-RSP应含有以下参数：

- 分类器参数：相应 REG-REQ 中所有的分类器参数，加上 CMTS 分配的分类器 ID；

- 业务流参数：相应 REG-REQ 中所有的业务流参数，加上 CMTS 分配的 SFID。每个含有容许的/激活的业务类别名称的业务流都应被扩展为 TLV 格式。每个容许的/激活的上行业务流都应有一个 CMTS 分配的 SID。唯一被预置的业务流将只含有 REG-REQ 消息中出现的那些 QoS 参数以及分配给它的 SFID；
- 有效负载包头抑制参数：相应 REG-REQ 中所有的有效负载包头抑制参数，加上 CMTS 分配的有效负载包头抑制索引。

如果REG-REQ失败，并含有业务流参数、分类器参数、有效负载包头抑制参数，则REG-RSP应包含以下参数之一：

- 分类器错误集：相对于 REG-REQ，如果至少有一个失败的分类器，则应包含一个分类器错误集以及起标识作用的分类器参考和业务流参考。每个分类器错误集都应至少包括相应分类器的一个失败分类器参数；
- 业务流错误集：相对于 REG-REQ，如果至少有一个失败的业务流，则应包含一个业务流错误集以及起标识作用的业务流参考。每个业务流错误集都应包括相应业务流的所有失败 QoS 参数；
- 有效负载包头抑制错误集：相对于 REG-REQ，如果至少有一个个失败的 PHS 规则，则应包含一个 PHS 错误集以及起标识作用的业务流参考和分类器参考对。每个 PHS 错误集都应至少包括相应失败 PHS 规则的一个失败 PHS 参数。

如果注册请求中含有用于延迟容许的/激活的业务流参考和业务类别名称，则注册响应中除业务流标识符之外不应包括任何其它QoS参数（见9.1.3）。

如果相应的注册请求含有EuroDOCSIS 1.0业务类别的TLV（见C.1.1.4），则注册响应应包含以下TLV字节字节组：

- EuroDCSIS1.0 业务类别数据：
  当响应=OK 时返回；
  每个授权业务类别的 SID/业务类别字节字节组；

注： 业务类别ID应是相应REG-REQ消息中所请求的。

- 业务不可用：
  当响应=业务类别失败时返回；
  如果不支持业务类别，该配置设定在业务类别数据的位置返回。

所有其它参数都编码为TLV字节组：

- CM 能力：CMTS 对 CM 的能力作出响应（如果等级请求信息中有 CM 能力）；
- 厂商特定数据：定义见附录 C。
  1） 厂商 ID 设置（CMTS 的厂商 ID）；
  2） 厂商特定扩展。

注： 一旦收到REG-RSP，不应再使用临时SID。

编码

类型值应如下述格式。类型和值的长度应各为1个字节。

a） CM 能力

该域定义CMTS对注册请求中CM能力域的响应。CMTS应对CM能力作出响应，表明是否使用该CM能力。如果CMTS不能识别某一CM能力，则应在注册响应中使用0值（关）TLV返回。

只有在REG-REQ中置为“开”，才可以在REG-RSP中置为“开”，这表示CM和CMTS已经成功地进行了握手协商。在REG-REQ中置为“关”，也应在REG-RSP中置为“关”。

编码定义同REG-REQ；

b） EuroDOCSIS1.0 业务类别数据

对于注册请求中出现的每个EuroDOCSIS 1.0 业务类别参数（参见C.1.1.4），应要在注册响应中出现一个 EuroDOCSIS 1.0 业务类别参数。

该编码定义了与所请求的业务类别相关的参数，其复杂性在于它由一些被封装的TLV域组成。该封装域规定了正在讨论的业务类别的特定参数。所定义的类型域只在封装的业务数据配置串中有效。

每个收到的EuroDOCSIS 1.0 业务类别参数中应有一个唯一的业务类别ID，范围从1至16。如果在注册请求中的每个EuroDOCSIS 1.0 业务类别TLV都没有业务类别ID出现，CMTS应发出一个带有业务类别失败响应的注册响应，且不带有EuroDOCSIS 1.0 业务类别TLV。

类型	长度	值
1	N	编码的业务类别数据

类别ID：该域的值定义了封装串所适用的业务标识符，且应是注册请求中请求的业务类别。

类型	长度	数值
1.1	N	来自REG-REQ

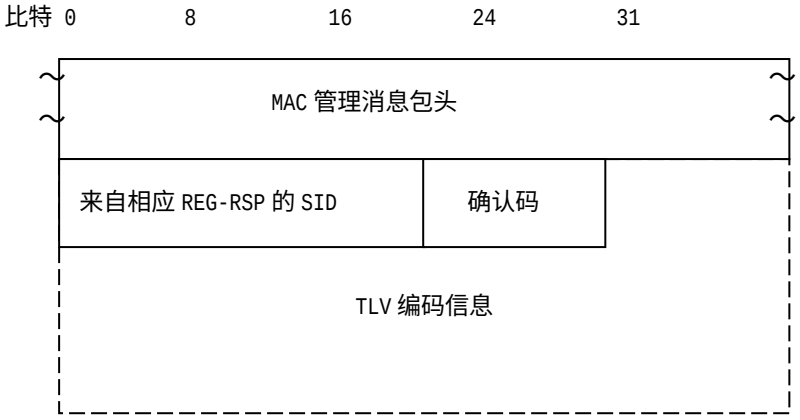
数值范围：业务类别ID范围应在1至16之间。

SID：这个域的值应规定业务类别相关的SID。

类型	长度	数值
1.2	2	SID

7.3.9 注册确认（REG_ACK）

注册确认应由CM发出，响应来自CMTS的REG-RSP。它表明CM接受了来自CMTS的注册响应中的QoS参数。注册确认的格式应如图48所示。



来自相应的 REG-RSP 的 SID：该确认所对应的注册响应中的 SID；

确认码：对应整个注册响应的合适的确认码（参见 C.4）。

图48 注册确认

CM应在REG-REQ把所有预置的分类器、业务流和有效负载包头抑制规则传给CMTS(见7.3.7)。由于这些预置项都有可能失败，注册确认中应包括这些预置项的所有失败相关错误集。

如果已有任一预置项目失败，则REG-ACK应包括相应于那些失败项目的错误集。错误集标识由相应的REG-RSP中的业务流ID和分类器ID来提供。如果分类器ID或SFID在REG-RSP中被省略，则CM应在REG-ACK中使用适当的参考（分类器参考、SF参考）。

分类器错误集：相对于REG-RSP，如果至少有一个失败的分类器，则应包含一个分类器错误集以及起标识作用的分类器参考/标识符和业务流参考/标识符对。每个分类器错误集都应包含相应分类器的至少一个失败分类器参数。如果整个注册请求/注册响应成功，则该参数应被省略。

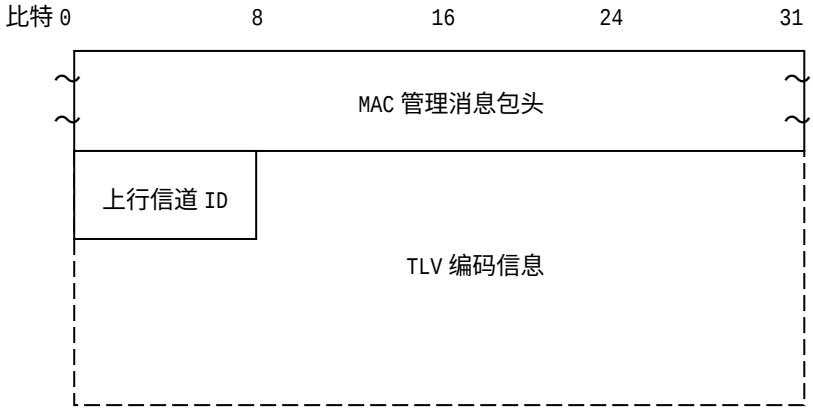
业务流错误集：REG-ACK消息的业务流错误集定义REG-RSP消息中的所有失败业务流。相对于REG-RSP消息，如果至少有一个失败业务流的一个失败QoS参数，则应包含一个业务流错误集以及起标识作用的业务流参考。如果整个注册请求/注册响应成功，则该参数应被省略。

有效负载包头抑制错误集：相对于REG-RSP，如果至少有一个失败的PHS规则，则应包含一个PHS错误集和起标识作用的PHS索引以及分类器参考/标识符对。每个PHS错误集中应包含对应于失败PHS规则的至少一个失败PHS参数。如果整个注册请求/注册响应成功，则该参数应被省略。

每个业务流都应给予确认，这不仅是为了CM与CMTS之间的同步，也是为了支持业务类别名称的使用（见9.1.3）。由于CM在进行注册请求时，可能并不知道一个业务类别名称的所有相关业务流参数。所以如果CM没有足够的资源支持该业务流，则CM有必要不确认注册响应。

7.3.10 上行信道变更请求（UCC-REQ）

上行信道变更请求可由CMTS发出，使得CM改变正在使用的上行信道。上行信道变更消息格式如图49所示。



各参数定义如下：

上行信道 ID：CM 将要切换到的上行信道的标识符，该域长度为 8 比特。

所有其它参数编码为 TLV 字节组。

测距技术：同步到新的上行信道后 CM 应采用的测距类型。

图49 上行信道改变请求

编码

应采用如下所示类型值。类型和长度域各为个1个字节。

测距技术

该TLV的出现允许CMTS指示CM进行什么级别的重新测距。CMTS可根据对新旧上行信道差异的了解来决定级别。

例如，上行频谱的区域通常是成组地进行配置，切换到同组中相邻信道的UCC-REQ可能不要求重新测距，但切换到不相邻信道的UCC-REQ则需要台站维护。而不同组之间的UCC-REQ可能要求初始维护。

类型	长度	值
1	1	0=在新信道上进行初始维护 1=在新信道上进行台站维护 2=在新信道上进行初始维护或台站维护[a] 3=直接使用新信道而不进行初始维护或台站维护

a 这个值授权 CM 使用先出现的初始维护或台站维护区。在 CM 不能确定何时执行上行信道改变，并会因此导致丢失台站维护时隙时，可使用这个值。

如果这个TLV没有出现，CM应进行初始维护测距。为了与EuroDOCSIS 1.0兼容，CMTS应接受此CM，而该CM忽略了此字节组并进行初始维护。

7.3.11 上行信道变更响应（UCC_RSP）

在收到上行信道变更请求消息后，CM应发送一个上行信道变更响应消息，表明已收到该消息且正遵照执行。上行信道变更消息格式如图50所示。

在切换到新的信道前，CM应在现有的上行信道中发送一个UCC-RSP消息。CM正在执行信道切换时，可忽略收到的UCC-REQ消息。如果CM收到一个UCC－REQ消息要求它切换到一个它正在使用的上行信道上，CM应在该信道上响应一个UCC-RSP消息表明它已经使用了正确的信道。

在切换到新的上行信道后，CM应根据UCC-REQ消息中规定的测距技术重新测距，无需重新注册。变更信道的过程见10.3.3。

上行信道 ID：CM 要切换到的新的上行信道的标识符。与上行信道变更请求消息中的信道 ID 相同。它应是一个 8 比特域。

图50　上行信道变更响应

7.3.12　动态业务添加请求（DSA_REQ）

CM或CMTS可以发送动态业务添加请求以生成一个新的业务流。

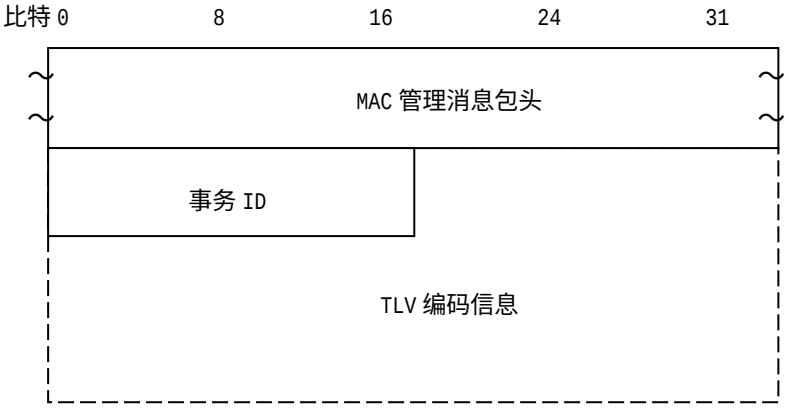


图51　动态业务添加请求

CM或CMTS产生的动态业务添加请求消息格式应如图51所示，参数定义如下：

事务ID:唯一地标识由发端分配的事务。

其他参数按照附录C规定的TLV字节组进行编码。在每个方向上，动态业务添加请求消息不能包含多于一个业务流的参数。动态业务添加请求消息中应包含单个上行业务流的参数，或单个下行业务流的参数，或是一个上行和一个下行业务流的参数。

DSA-REQ消息应包含：

业务流参数：规定业务流的业务量特性和调度要求。

DSA-REQ中可以包含业务流的相关分类器参数和有效负载包头抑制参数：

- 分类器参数：规定如何把包分类为特定业务流的规则；
- 有效负载包头抑制参数：规定相关分类器中所用的有效负载包头抑制规则。

7.3.12.1　CM 发起的动态业务添加

CM发起的动态业务添加（DSA）请求应使用业务流参考来链接分类器和业务流。业务流参考值对DSA消息是局部的。DSA请求中的每个业务流应有一个唯一的业务流参考，对于发送端所知的其它业务流，该值不必唯一。

CM发起的DSA请求应使用分类器参考和业务流参考来把有效负载包头抑制参数链接到分类器和业务流。DSA请求应使用业务流参考将分类器与业务流链接起来。分类器参考值对DSA消息是局部的；DSA请求中的每个分类器都应指定有一个唯一的分类器参考。

CM发起的DSA请求可以使用业务类别名称（见C.2.2.3.4）代替部分或全部的QoS参数。

7.3.12.2 CMTS 发起的动态业务添加

CMTS发起的动态业务添加请求应使用SFID把分类器和业务流链接起来。SFID在MAC域中是唯一的。CMTS为上行业务发起的DSA请求中应包含一个SID。

CMTS发起包含分类器的DSA请求，应基于业务流唯一地分配分类器。

CMTS为给定业务等级发起的DSA请求，应包含该业务类别的相关Qos参数集。

7.3.13 动态业务添加响应（DSA_RSP）

收到DSA-REQ消息，应产生动态业务添加响应。动态业务添加响应格式应如图52所示。

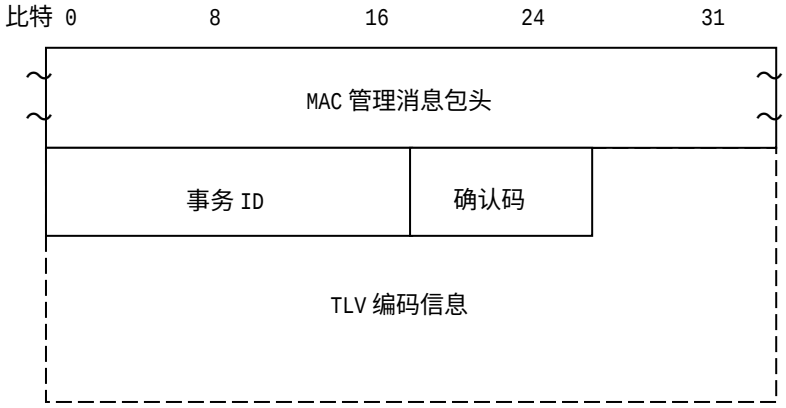


图52 动态业务添加响应

参数应如下定义：

- 事务 ID：来自相应的 DSA-REQ 消息的事务标识符；
- 确认码：相应 DSA-REQ 的合适的确认码（见 C.4）。

所有其他参数按照附录C规定的TLV字节组进行编码。

如果该事务成功，DSA-RSP可以包含一个或多个以下参数：

- 分类器参数：CMTS 在 DSA-RSP 中应包含该分类器的全部参数，其中含有一个新分配的分类器。CM 在 DSA-RSP 中不应包含该分类器参数；
- 业务流参数：CMTS 在 DSA-RSP 中应包含该业务流的全部参数，其中含有一个新分配的业务流 ID 和扩展业务类别名称。CM 在 DSA-RSP 中不应包含该业务流参数；
- 有效负载包头抑制参数：CMTS 在 DSA-RSP 中应包含该 PHS 全部参数，其中含有一个新分配的 PHS 索引。CM 在 DSA-RSP 中不应包含该 PHS 参数。

如果该事务失败，且确认码不是在C4.2中的一个主要错误码，则DSA-RSP中应至少包含一个下述参数：

- 业务流错误集：相对于 DSA-REQ 消息，如果至少有一个失败的业务流，则应包含一个业务流错误集和起标识作用的业务流参考/标识符。每个业务流错误集中应包含相应业务流的至少一个特定的失败者的 Qos 参数。如果整个 DSA-REQ 成功，则该参数应省略；

- 分类器错误集：相对于 DSA-REQ 消息，如果至少有一个失败的分类器，则应包含一个分类器错误集和起标识作用的分类器参考/标识符及业务流参考/标识符对。每个分类器错误集应包含相应分类器的至少一个特定的失败分类器参数。如果整个 DSA-REQ 成功，则该参数应省略；
- 有效负载包头抑制错误集：相对于 DSA-REQ 消息，如果至少有一个失败的 PHS 规则，则应包含一个 PHS 错误集和起标识作用的分类器参考/标识符和业务流参考/标识符对。每个 PHS 错误集中应包含相应失败 PHS 规则的至少一个 PHS 参数。如果整个 DSA-REQ 成功，则该参数应省略。

7.3.13.1 CM 发起的动态业务添加

CMTS对成功添加的业务流的DSA-RSP中应包含一个SFID。对于容许的或有效的上行QoS参数集的DSA-RSP，也应包含一个SID。

如果相应的DSA-REQ使用业务类别名称（见C.2.2.3.4）请求添加业务，则DSA-RSP中应包含与该命名业务类别相关的QoS参数集。如果在DSA-REQ中同时使用业务类别名称和其他QoS参数，则CMTS应根据DSA-REQ中的显式QoS参数决定接受或拒绝DSA-REQ。如果该业务流编码与业务类别属性冲突，CMTS应使用DSA-REQ给出的值替换业务类别给出的值。

如果该事务成功，CMTS应给每个被请求的分类器分配一个分类器ID并给每个所请求的PHS规则分配一个PHS索引。CMTS应使用初始分类器参考和业务流参考连接DSA-RSP中的成功参数。

如果该事务失败，CMTS在DSA-RSP中应使用初始分类器参考和业务流参考来标识失败参数。

7.3.13.2 CMTS 发起的动态业务添加

如果该事务失败，CM应使用分类器ID和SFID标识DSA-RSP中的失败参数。

7.3.14 动态业务添加确认（DSA_ACK）

收到DSA-RSP，应产生动态业务添加确认。DSA_ACK格式如图53所示。

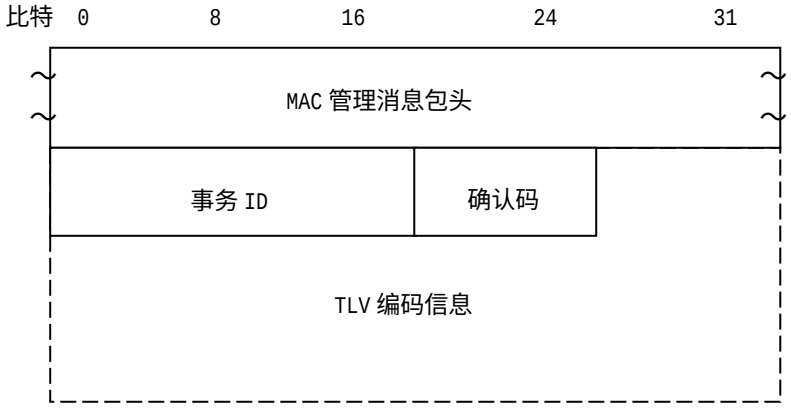


图53 动态业务添加确认

参数应如下定义：

- 事务 ID：相应 DSA-RSP 中的事务 ID；
- 确认确认码：相应整个 DSA-RSP 的适当的确认码（见 C.4）。

注： 如果在DSA-REQ中使用业务类别名称（见9.1.3），则应使用该确认码。这种情况下，DSA-RSP中可以包含CM不能支持的业务流参数（临时的或配置的）。

其他参数按照附录C规定的TLV字节字节组进行编码。

业务流错误集：DSA_ACK消息中的业务流错误集定义DSA-RSP消息中的失败业务流。相对于DSA-REQ消息，如果至少有一个失败业务流的一个失败QoS参数，则应包含一个业务流错误集和起标识作用的业务流参考/标识符。如果整个DSA-REQ成功，则该参数应被省略。

7.3.15 动态业务变更请求（DSC_REQ）

CM或CMTS都可以发送动态业务变更请求以便动态地变更当前业务流的参数。DSC变更分类应携带新分类器的所有TLV集。

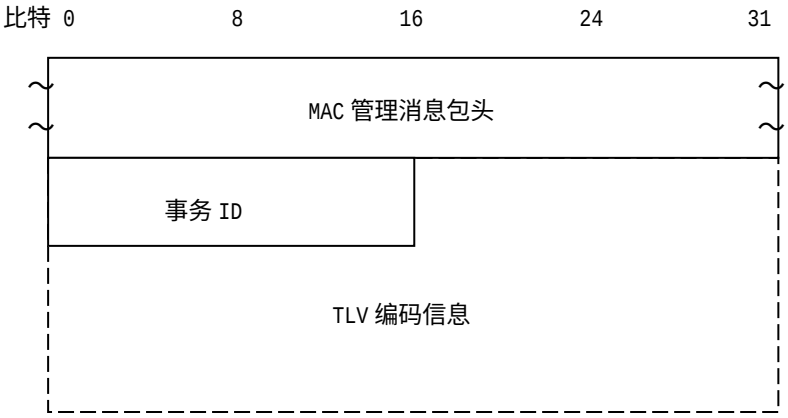


图54　动态业务变更请求

CM或CMTS产生的动态业务变更请求消息如图54，其中包含如下参数：

事务ID：唯一地由发送端分配的事务标识符。

其他参数按照附录C规定的TLV字节组进行编码。在每个方向上，一个DSC-REQ消息不能携带多于一个业务流的参数，即DSC-REQ中应包含单个上行业务流的参数，或单个下行业务流的参数，或是一个上行和下行业务流的参数。DSC-REQ中应至少包含以下参数中的一个。

- 分类器参数:规定了如何把包分类到特定的业务流中去。包含动态业务变更作用 TLV，它可以指示这个分类是否在业务流中添加、替代或删除（见 C.2.1.3.7）。如果包含了这个参数，该分类器参数应包含动态变更动作 TLV、分类参考/标识符和一个业务流标识符；
- 业务流参数:规定业务流的新业务特性和调度要求。该消息中的业务流容许的和有效的 QoS 参数集替代正在使用的业务流的相应 QoS 参数集。如果 DSC 消息成功并包括容许的和有效的 QoS 的替代集，则省略的集应设为空。如果有该参数，它应包含一个业务流标识符；
- 有效负载包头抑制参数:规定了特定分类器的有效负载包头抑制规则，包含动态业务变更作用 TLV，它可以指示该 PHS 规则是否在业务流中添加、替代或删除（见 C.2.1.3.7）。如果有该参数，则应包含一个分类器参考/标识符和一个业务流标识符，除非动态业务变更是删除所有 PHS 规则。如果动态业务变更是删除所有 PHS 规则，则 PHS 参数应包括具有动态业务变更的业务流标识符，且在这种情况下不需要其它 PHS 参数存在。然而，如果存在其他 PHS 参数，特别是有效负载包头抑制索引存在的话，则接收 DSC-REQ 消息时应将其忽略。

7.3.16　动态业务变更响应（DSC_RSP）

收到DSC-REQ，应产生动态业务变更响应。DSC-RSP的格式应如图55所示。

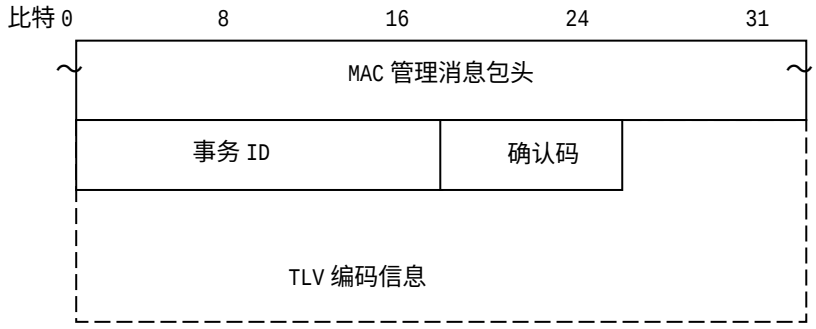


图55　动态业务变更响应

参数应如下：

- 事务 ID：来自相应的 DSC-REQ 的事务标识符；
- 确认码：相应 DSC-REQ 的合适的确认码（见 C.4）。

其他参数按照附录C规定的TLV字节组进行编码。

如果该事务成功，则DSC-RSP中可以包含一个或多个以下参数：

- 分类器参数：CMTS 在 DSC-RSP 中包含该分类器的全部参数，其中包含新分配的分类器的 ID。CM 不应在 DSC-RSP 中包含分类器参数；
- 业务流参数：CMTS 在 DSC-RSP 中包含业务流的全部参数，其中包含扩展业务类别名称。如果业务流参数集包含上行容许的 QoS 参数集且该业务流没有相关 SID，则 DSC-RSP 中应包含 SID。如果业务流参数集包含一个业务类别名称和容许的 QoS 参数集，则 DSC-RSP 中应包含该给定业务类别的相关 QoS 参数集。如果在业务流请求中包含特定 QoS 参数，则 DSC-RSP 中应包含这些 QoS 参数，而不含与命名业务类别同类的任何 QoS 参数。CM 不应在 DSC-RSP 中包含业务流参数；
- 有效负载包头抑制参数：CMTS 在 DSC-RSP 中包含全部 PHS 参数，其中包含一个新分配的 PHS 索引、一个分类器 ID 和一个 SFID。CM 不应包含 PHS 参数。

如果该事务失败，且确认码不是在C.4.2中的一个主要错误码，则DSA-RSP中应至少包含以下参数之一：

- 分类器错误集：相对于 DSC-REQ 消息，如果至少有一个失败的分类器，则在 DSC-RSP 中应包含一个分类器错误集和起标识作用的分类器参考/标识符对。每个分类器错误集应包含相关分类器的至少一个失败分类器参数。如果整个 DSA-REQ 成功，则该参数应被省略；
- 业务流错误集：相对于 DSC-REQ 消息，如果至少有一个失败的业务流，则在 DSC-RSP 中应包含一个业务流错误集和起标识作用的业务流标识符。每个业务流错误集中包含相关业务流的至少一个 Qos 参数。如果整个 DSA-REQ 成功，则该参数应被省略；
- 有效负载包头抑制错误集：相对于 DSC-REQ 消息，如果至少有一个失败的 PHS 规则，则在 DSC-RSP 中应包含一个 PHS 错误集和起标识作用的业务流参考/标识符及分类器参考/标识符对，除非动态业务变更是删除所有 PHS 规则。如果动态业务变更是删除所有 PHS 规则，则 PHS 参数应包括 SFID。每个 PHS 错误集中应包含相关失败 PHS 规则的至少一个失败 PHS 参数。如果整个 DSC-REQ 成功，则该参数应被省略。

7.3.17 动态业务变更确认（DSC_ACK）

收到动态业务变更响应，应产生动态业务变更确认。DSC_ACK的格式应见图56所示。

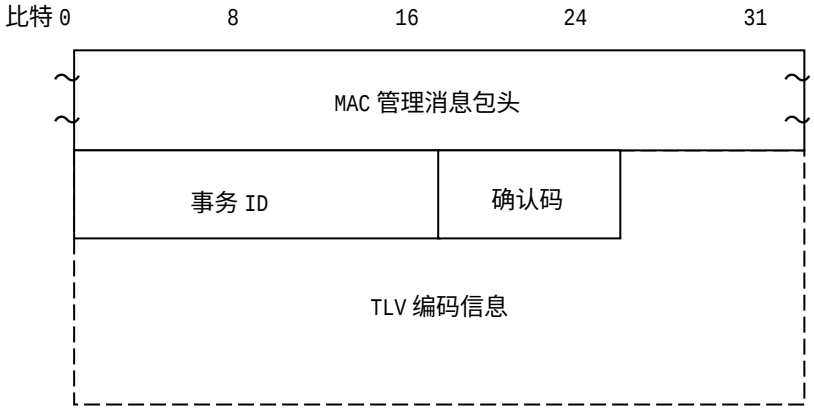


图56 动态业务变更确认

参数定义如下：

- 事务 ID：相应 DSC-REQ 的事务标识；
- 确认码：相应动态业务变更响应的合适的确认码（见 C.4）。

注： 如果DSA-REQ消息中使用了业务类别名称（见9.1.3），则应使用该确认码和业务流错误集。这种情况下，DSC-RSP中可以包含CM不能支持的业务流参数（暂时的或配置的）。

其他参数按照附录C规定的TLV字节组进行编码：

业务流错误集：DSC_ACK消息中的业务流错误集定义DSC-RSP消息中的失败业务流。应包含相应DSC-RSP消息中至少一个失败业务流的一个失败QoS参数的业务流错误集和起标识作用的SFID。如果整个DSC-REQ成功，则该参数应被省略。

7.3.18 动态业务删除请求（DSD_REQ）

CM或CMTS都可以发送DSD-REQ以删除现有的业务流。DSC-REQ的格式见图57所示。

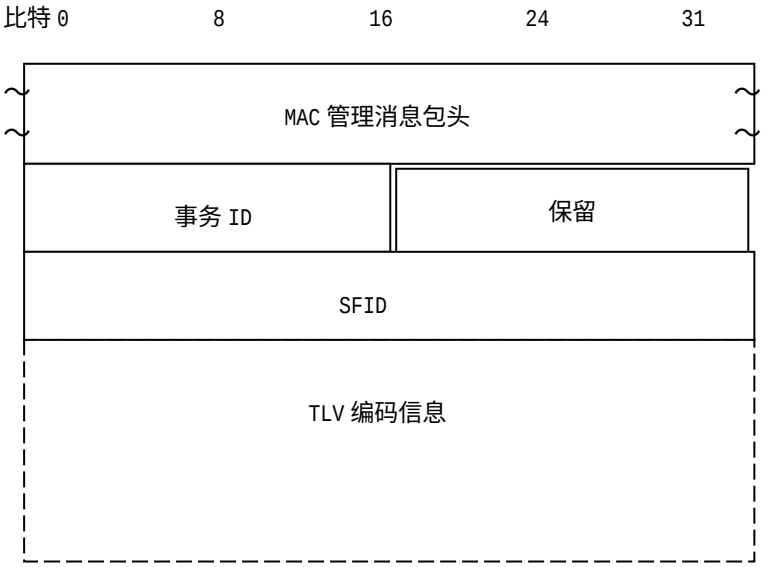


图57 动态业务删除请求

参数应如下：

- SFID：要删除的业务流标识符。
  如果 SFID 非零，是指要删除的业务流，并忽略 TLV 中的 SFID；如果 SFID 是零，则由 TLV 中的 SFID 指明要删除的业务流；
- 事务 ID：唯一地由发送端分配的事务标识符。

其他参数按照附录C规定的TLV字节组进行编码：

- 业务流 ID：指要删除的业务流按 C.2.2.3.2 编码。

7.3.19 动态业务删除响应（DSD_RSP）

对收到的动态业务删除请求应产生动态业务删除响应。DSD-RSP格式见图58所示。

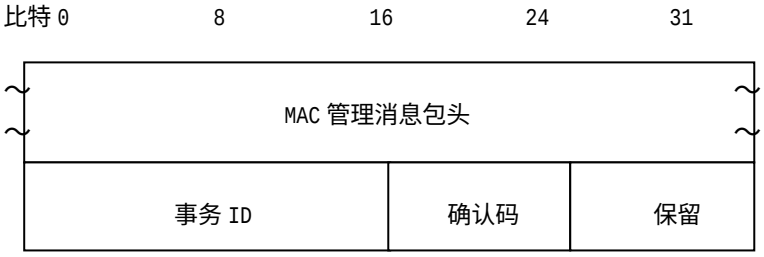


图58 动态业务删除响应

参数定义如下：

- 事务 ID：相应 DSD_REQ 的事务标识符；
- 确认码：相应 DSC-RSP 的合适的确认码（见 C.4）。

7.3.20 动态信道变更请求(DCC-REQ)

动态信道变更请求由CMTS发送，使CM能在下行信道接收DCC消息来变更其传送的上行/下行信道。

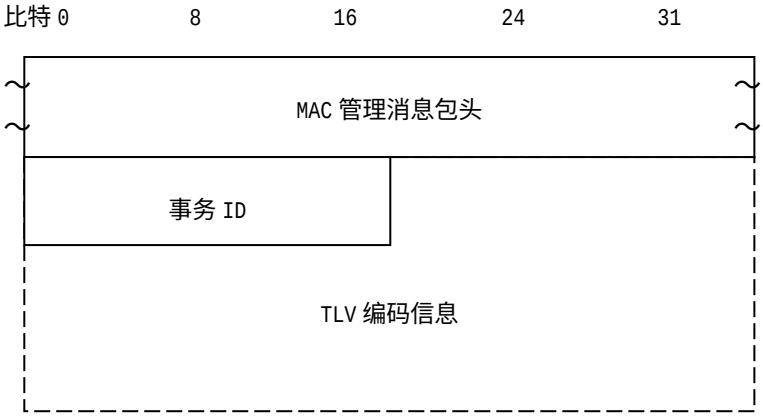


图59　动态信道变更请求

CMTS应按图59所示参数产生DCC-REQ消息，参数包括：

- 事务 ID：是由发送端为这项事务分配的 16 比特标识符。

下列参数是可选的，且是TLV编码：

- 上行信道 ID：发送到 CM 用来切换上行传输的上行信道的标识符；
- 下行参数：发送到 CM 用来切换下行接收的下行信道的频率；
- 初始化技术：如果 CM 一旦完成同步到新的信道，应进行的初始化类型；
- UCD 替代：提供一个新信道的 UCD 的复制。这种 TLV 出现一次且包含一个 UCD；
- SAID 替代：是一对安全关联标识符(SAID)，它包含当时的 SAID 和新信道的新 SAID。一旦 SAID 要求替代，这种 TLV 就出现一次；
- 业务流替代：一组子 TLV 可用来替代业务流中的业务流标识符、业务标识符、分类标识符及有效负载包头抑制索引。这种 TLV 对于要求替代参数的每个业务流是重复的。

编码

所用的类型值应如下所述。在动态信道变更请求消息中，这些值是唯一的，但不跨越整个MAC消息集。

如果CM完成了信道变更,没有进行重新初始化(如7.3.20.3定义),则CM的全部配置变量应保持不变，除非配置变量做如下显式变更。CM除了在DCC指令中已提供的配置变更外，它将不知道任何配置变更，因此在新旧信道之间提供的一致性的预置是重要的。

a)　上行信道 ID

当CM执行动态信道变更时，应使用TLV规定的新上行信道ID，且不考虑当时的上行信道ID。CMTS应确保新信道的上行信道ID不同于旧信道的上行信道ID。如果上行信道已变更,即使UCD替代TLV已被包括，也应包括该TLV。

类型	长度	值
1	1	0～255：上行信道ID

如果缺少该TLV，则CM不应变更其上行信道ID。CMTS可以包括该TLV，CM应遵守该TLV；

b)　下行参数

当出现时，这个TLV规定了新的下行信道的工作参数。该TLV的值域包含一系列的子类型。

类型	长度	值
2	n	

CMTS可以包括该TLV。如果缺少该TLV， CM不应变更其下行参数；

1)　下行频率

该TLV规定了新的接收频率。当CM执行动态信道变更时应使用。它置换当前的下行信道频率，这是下行信道的中心频率(Hz)，且以32位二进制数存储。下行频率应是62500Hz的倍数。

子类型	长度	值
2.1	4	Rx频率

CMTS应包括该子TLV。CM应遵守该子TLV；

2） 下行调制类型

该TLV规定了调制类型，在新的下行信道上使用。

子类型	长度	值
2.2	1	0＝64QAM 1＝256QAM 2～255：保留

CMTS应包括该子TLV。CM应遵守该子TLV；

3） 下行符号率

该TLV规定了符号率，在新的下行信道上使用。

子类型	长度	值
2.3	1	0＝5.056941Msym/s 1＝5.360537Msym/s 2＝6.952Msym/s 3～255：保留

CMTS应包括该子TLV。CM应遵守该子TLV；

4） 下行交织深度

该TLV规定了下行交织器的“I”和“J”参数。

子类型	长度	值
2.4	2	I：0～255 J：0～255

CMTS应包括该子TLV。CM应遵守该子TLV；

5） 下行信道标识符

该TLV规定了新下行信道的8比特下行信道标识符。

子类型	长度	值
2.5	1	0～255：下行信道ID

CMTS应包括该子TLV。CM应遵守该子TLV；

6） SYNC 替代

当出现时，该TLV允许CMTS通知CM在继续运行之前等待或不等待SYNC消息。如果CMTS通知CM在新信道上发送之前不等待同步消息，CMTS应在新旧信道之间有SYNC。SYNC意指时戳是从同一时钟导出并包含相同的值。

类型	长度	值
5	1	0＝继续运行前在新的下行频道上获得SYNC消息 1＝没有得到SYNC消息，继续进行 2～255：保留

如果该TLV不出现，CM应在继续运行前从新的信道上等待一个SYNC消息。当变更信道时，如果CM在等待一个新的SYNC消息，则运行可以推迟时间到“SYNC间隔”(见附录B)，或者如果SYNC消息丢失或与旧信道不同步，则推迟时间更长。

另一种方法是更频繁地发送SYNC消息(例如每10ms)，且要求CM在继续运行之前等待SYNC消息。这种方法等待时间稍长，但提供了一种附加的检查，以防止CM在不正确的时间间隔发送。

CMTS应包括该TLV。CM应遵守这个TLV；

c） 初始化技术

当出现时， 该TLV允许CMTS指导CM重新初始化的等级。无论何种等级，它应在开始通信前在新的信道上完成。CMTS能根据新旧MAC域之间的差别和它们的上行/下行信道的物理层特性做出这种决定。

通常，如果上行／下行信道之间的转移在同一MAC域内，则连接特性参数可保持不变。如果转移是在不同的MAC域之间，则可进行一个完整的初始化。

如果不要求完整的重新初始化，仍可要求做某些重新测距。例如，上行频谱的区域往往按组配置。对于在一组内的相邻上行信道的DCC-REQ可以不要求重新测距。相反，对非相邻上行信道的DCC-REQ可能要求台站维护，而从一个上行信道组到另一个的DCC-REQ可能要求初始维护。如果在新旧信道之间的PHY参数中有任何差异，也可能要求重新测距。

类型	长度	值
3	1	0＝重新初始化MAC 1＝在正常运行前，在新信道上完成初始维护 2＝在正常运行前，在新信道完成台站维护 3＝在正常运行前，在新信道上完成初始维护或台站维护 4＝没有重新初始化或进行初始化或台站维护的情况下,直接使用新的信道 5～255：保留

CM应根据上行信道ID TLV(见7.3.20.1)和下行频率TLV(见7.3.20.2.1)首先选择新的上行和下行信道。然后CM应遵守该TLV的指导。对选项0，CM应以初始化SID开始，对于选项1～4，CM应连续使用主SID进行测距。一个SID替代TLV(见7.3.20.6.2)可以规定新的主SID在新信道上使用(见7.3.20.6.2)。

- 选项 0：指导 CM 完成与 CM 初始化相关的所有操作(见 10.2)。包括取得下行 QAM、FEC 和 MPEG 锁定之后的所有事项及标准运行之前(见 10.3)的所有事件，包括得到 UCD、测距、建立 IP 连接、获得日期/时间、操作参数的传送、注册的初始化。当使用这种选项时，在 DCC-REQ 的其它 TLV 中，只有上行信道 ID TLV 和下行参数 TLV 与此选项相关；
- 选项 1：如果初始维护被指定，则在新信道上的运行将推迟几个测距间隔(见附录 B)；
- 选项 2：如果台站维护被指定，则在新信道上的运行将推迟 T4 值(见附录 B)；
- 选项 3：该值授权 CM 使用一个初始维护或台站维护区域，它们总是由 CM 选择。当不能确定 CM 何时执行 DCC 指令而导致可能错过台站维护时隙的机会，可使用该值；
- 选项 4：提供最少的业务中断，CM 一旦在新信道上达到同步，就可以继续其正常的运行。

注： 在上行传输特性不稳定的物理网中，不能使用这种选择。

如果缺乏这种TLV，CM应重新初始化MAC。CMTS可以包括这种TLV。CM应遵守这种TLV；

d) UCD 替代

当出现时，该TLV允许CMTS发送一个上行信道描述符消息给CM。这个UCD消息用于新的上行／下行信道。CM在其存储器中存储这个消息并在与新的信道同步后使用它。

类型	长度	值
4	n	新的上行信道UCD

该TLV包括了在7.3.3条中描述的所有UCD消息的参数，但MAC管理消息包头除外。CMTS应确保在UCD中的计数变化与在新信道的UCD中的计数变化匹配。CMTS应确保新信道的上行信道ID不同于旧信道的上行信道ID。

如果UCD的长度超过254字节，UCD应分段为2个或更多个类型为4的单元。除最后一个外，每个分段应为254字节。CM通过按DCC-REQ消息中的顺序级联类型为4的单元，重建UCD替代消息。例如，第二个类型4的单元的第一个字节好似跟着第一个类型4的单元的最后一个字节。

当变更信道时，如果CM已在等待新的UCD消息，则等待“ UCD间隔 ”(见附录B)，如果UCD消息丢失，则等待时间更长。

CMTS应包括该TLV。CM应遵守该TLV；

e) 安全关联标识符(SAID)替代

待定；

f） 业务流替代

当出现时， 该TLV允许CMTS用新指配信道的参数置换当前信道上的参数。每个要求改换参数的业务流用一个TLV。CMTS可以选择这种做法，以在旧信道上删去QoS预留之前，简化在新信道上建立新的QoS预留。CM不必同时响应新、旧业务流。

通过改变相关的的ID和索引，该TLV允许资源分配和业务在两个独立的ID和调度实体之间转移。两个信道之间可能不同的ID值包括业务流标识符、SID、分类标识符及有效负载包头抑制索引。该TLV不允许改变业务流QoS参数、分类参数或PHS规则参数。

在SFID内使用的业务分类名称应在新、旧信道之间保持相同。

类型	长度	值
7	n	子类型表

如果个别业务流不存在该TLV,则保持当前的业务流及其属性。CMTS可以包括该TLV。CM应遵守该TLV；

1） 业务流标识符替代

该TLV允许CMTS用一个新的业务流标识符来置换当前的业务流标识符(SFID)，这个参数的用法见附录C.2.2.3.2。

如果有任何其它业务流子类型替代，该TLV应存在。如果包括该TLV，且SFID不变更，则当前的和新的SFID将被设定到同一值。

类型	长度	值
7.1	8	当前的SFID，新的SFID

CMTS可以包括该TLV。CM应遵守该TLV；

2） 业务标识符替代

当出现时，该TLV允许CMTS用一个新的业务标识符来置换在当前的上行业务流中的业务标识符(SID)。这个参数的用法见附录C.2.2.3.3。

子类型	长度	值
7.2	4	当前的SID(16比特域的低14比特) 新的SID(16比特域的低14比特)

如果该TLV不存在，则保持当前的业务标识符。CMTS可以包括该TLV，CM应遵守该TLV；

3） 主动授权时间参考替代

当出现时，该TLV允许CMTS用一个新的主动授权时间参考来置换当前的主动授权时间参考。这个参数的用法见附录C.2.2.6.11。

如果新、旧上行的时戳使用不同的时间基准，则该TLV是有用的。如果主动授权传输窗口迁移到时间内的不同点，该TLV也是有用的。变更这个值可以使运行暂时超过抖动窗口的规定，见附录C.2.2.6.8。

子类型	长度	值
7.5	4	新的参考

如果该TLV不存在，则保持当前的主动授权时间参考。CMTS可以包括该TLV，CM应遵守该TLV；

g） CMTS MAC 地址

当出现时，允许当前CMTS发送对应于目的下行信道频率的CMTS MAC地址。

在以下情况下，应规定该TLV：

如果CM正在改变下行信道和规定了UCD替代；

或者正在改变下行信道和使用初始化技术选项4直接使用新信道。

类型	长度	值
8	6	目的CMTS MAC地址

CMTS应该包括该TLV，CM应遵守该TLV。

7.3.21　动态信道变更响应(DCC－RSP)

动态信道变更响应应由CM在响应已接收到的动态信道变更请求消息中发送,以表示它已接收到并遵守DCC－REQ。DCC－RSP消息的格式应如图60所示。

在CM开始切换到一个新的上行或下行信道之前，它应在其当前上行信道上发送一个DCC－RSP。当CM接收到DCC－REQ请求消息，要求切换到已经使用的上行和下行信道，或者只要求切换到已经使用的上行或下行信道，CM应在那个信道上发送DCC－RSP，以表示它已在使用该信道。

当CM处于执行信道变更过程中时，它可以忽略DCC－REQ消息。

在切换到一个新信道后，如果MAC不按DCC－REQ初始化TLV选项0重新初始化，则CM应发送DCC－RSP消息给CMTS。如果CM重新初始化它的MAC，则不必发送DCC－RSP。

变更信道的全部过程见10.4.5。

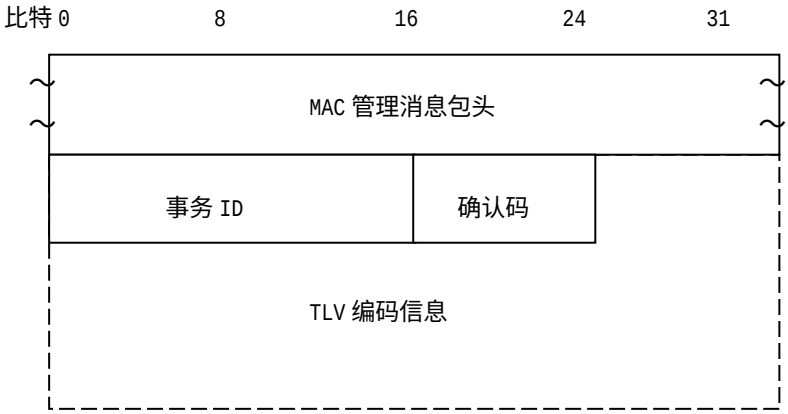


图60　动态信道变更响应

参数应如下：

- 事务 ID：一个对应于 DCC－REQ 的 16 比特事务 ID；
- 确认码：一个 8 比特确认码，如附录 C.4.1 所描述。

如下参数是任选的，且按TLV字节组编码：

- CM 切换时间：描述 CM 何时发生切换的定时参数。

编码

类型值的使用应如下所述，在动态信道变更响应消息内唯一的，但不跨越整个MAC消息集。

- CM 切换时间

当出现时， 该TLV允许CM用来向CMTS表示CM何时实施切换并从网络切断。用这个消息，CMTS可以采取预防措施，尽量减少或排除由于信道变更在下行信道中数据包的丢失。

类型	长度	值
1	n	

这些子TLV的时间参考和时间单元，是基于同样的在当前下行信道上使用的SYNC消息中的32比特时间基准。这个时戳根据10.24MHz时钟增加。

CM应包括该TLV。CMTS应遵守该TLV。

1)　切换的长度

该TLV是向CMTS表示从旧信道切换到新信道的时间长度。具体地说，它代表CM不能在下行信道接收数据的时间长度。

子类型	长度	值
1	4	时间长度(基于时戳)

CM应包括该子TLV。

2)　切换的起始时间

当出现时， 该TLV是向CMTS表示CM将开始切换的时间。

子类型	长度	值
2	8	起始时间(基于时戳)
		起始时间的偏差(基于时戳)

32比特、10.24MHz的时间基准大致按每7分钟转动一周。如果起始时间少于当前的时戳，CMTS将假定时戳计数器已转动一周。起始时间的偏差是起始时间之前和之后的绝对时间偏差量。

可能的切换时间窗是从(起始时间－偏差)到(起始时间＋偏差＋长度)。

CM应包括该TLV。

7.3.22 动态信道变更确认(DCC－ACK)

动态信道变更确认应由CMTS发送，并将其确认码设定为到达（1），以响应在新信道上接收到的动态信道变更响应消息。DCC－ACK消息的格式应如图61所示。

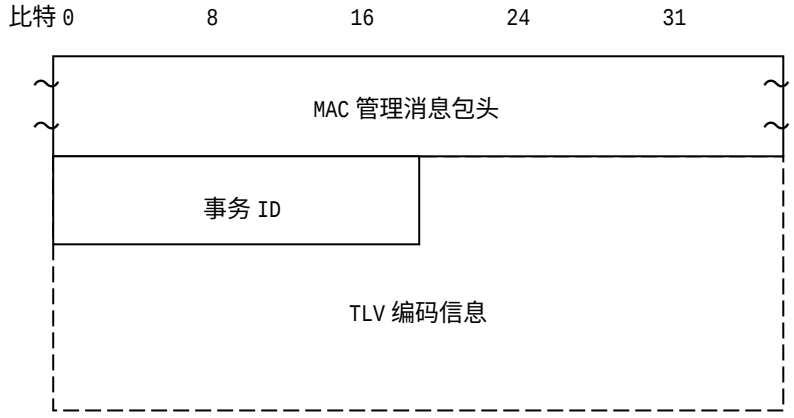


图61 动态信道变更确认

参数应如下：

事务ID：是一个相应于DCC－RSP的16比特事务ID。

7.3.23 设备分类识别请求(DCI－REQ)

CM可以实现DCI－REQ消息。

当实施时，从CMTS接收测距完成指示后，CM应立即发送DCI－REQ。从CMTS接收到DCI－RSP消息前，CM不应继续初始化。超时和重试信息在附录B中提供。

DCI－REQ的格式应如图62所示。

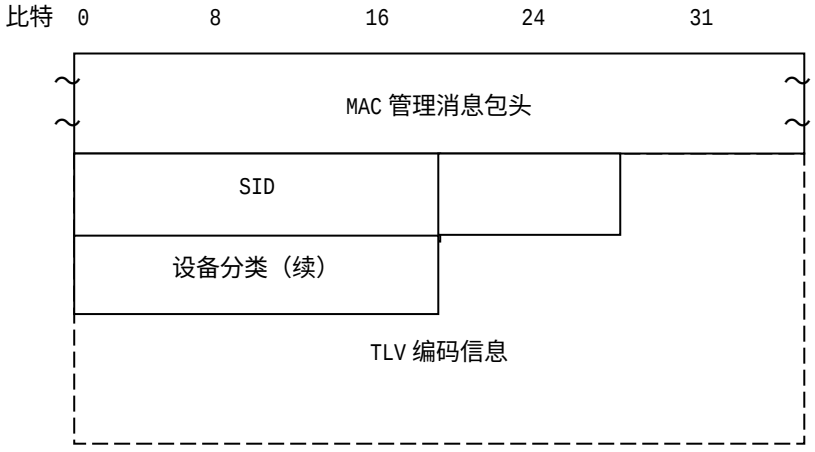


图62 设备分类识别请求

参数应如下：

- SID：在测距期间指定的临时 SID；
- 设备类别：这是一个 32 比特的域，不同比特表示了 CM 不同的属性。比特 0 为 LSB，若某位置 1，为选择以下定义的属性：
  比特# 0：CPE 控制的 CM (CCCM)；
  比特# 1～31：保留并应置于零。

7.3.24 设备分类识别响应(DCI-RSP)

DCI-RSP应由CMTS在接收到DCI-REQ后发送。

DCI-RSP的格式应如图63所示。

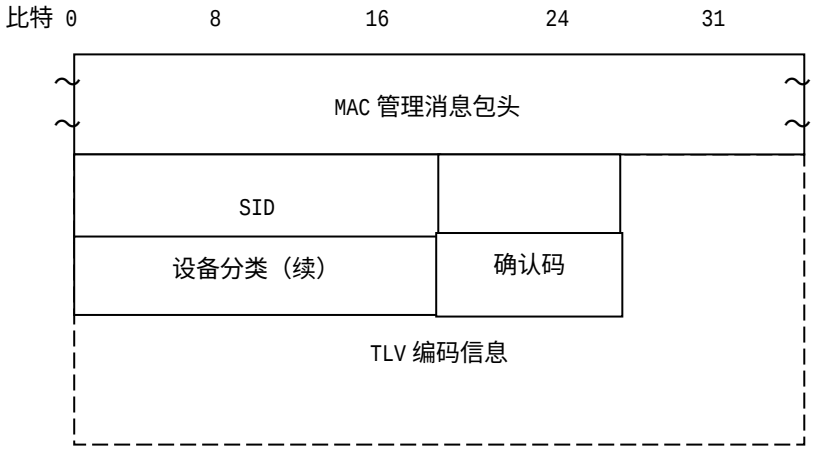


图63 设备分类识别响应

参数应如下：

- SID：指在相关的 DCI-REQ 中接收到的 SID；
- 设备分类：指在相关的 DCI-REQ 中接收到的设备分类域；
- 确认码：见 C.4。

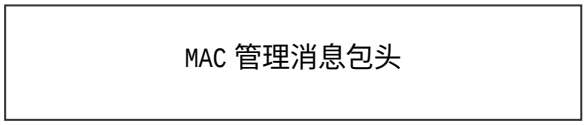
CMTS在DCI-RSP中只能使用3个确认码之一：

- 如果响应是临时拒绝(3)，CM 应复位其 DCI-REQ 计数器为零，且应重新发送 DCI-REQ，并在处理之前等待 DCI-RSP；
- 如果响应是永久拒绝(4)，CM 应放弃注册尝试，并应开始重新搜索不同的下行信道。CM 不必重试这个信道，直到其搜索了所有下行信道；
- 如果响应是成功(0)，CM 应继续注册。

CMTS应通过DHCP过程得到设备分类信息。CMTS应用设备分类消息产生DHCP代理（选项82）字节组，在CMTS转发DHCP DISCOVER到DHCP服务器前，将设备分类消息插入到DHCP DISCOVER的字节组中。

7.3.25 上行发射机禁用(UP-DIS)MAC 管理消息

UP-DIS应按如下编码：



UP-DIS从CMTS发送到CM，且没有响应消息从CM返送到CMTS。

CMTS应能发送UP-DIS消息。在何种状态下发送UP-DIS消息的检测和报告机制依赖于具体实现。同样，用信令触发UP-DIS消息的传输超出了本部分的范围。

CM可以支持UP-DIS消息。

如果支持的话，CM一旦收到UP-DIS消息，不管何种事务状态，应自动禁止其上行发送。（见第10章)。一旦由UP-DIS禁用，CM上行发射机只能靠CM重新上电接通。

因为UP-DIS机制没有在CM中规定，CMTS应引入机制来跟踪禁用MAC地址，并重新发送UP-DIS消息给重新上电和试图重新注册的CM。

8 媒介接入控制协议操作

8.1 上行带宽分配

上行信道被模型化为一连串的微时隙流。为了识别这些时隙，CMTS应产生时间基准。它还应控制CM对时隙的使用。例如，它可以授权若干相邻的时隙给CM，以便让CM传送一个数据PDU。CM应安排好该数据的传输时间，以便CMTS按规定的时间基准进行接收。本条介绍在请求、授权以及应用上行带宽时使用的协议要素。指定带宽管理工作的基本机制是分配MAP。见图64。

分配MAP就是由CMTS在下行信道上传送的一种MAC管理消息,它按照一定的间隔对应安排使用上行微时隙的方法进行说明。一个给定的MAP可能会说明：一些时隙授权用作某些特定台站的数据输入，另外一些时隙则可用作争用传送，而再有另外的一些时隙可以提供新台站加入链路的机会。

不同厂家制造的CMTS也许会应用不同的时序算法；本部分没有强制规定某一种特定的算法。它只是说明了带宽请求和授权的协议要素。

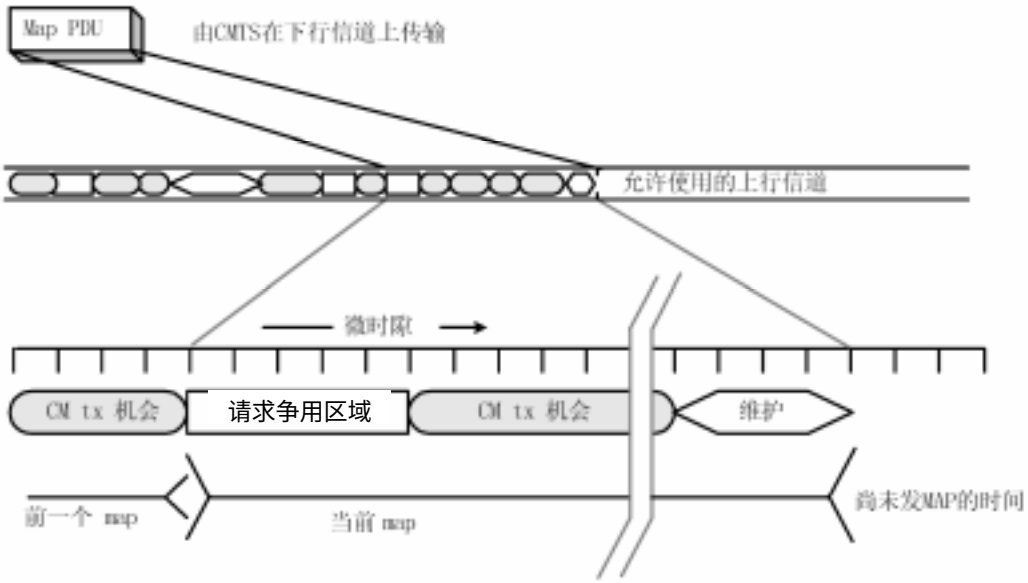


图64 分配 MAP

带宽分配包括以下基本要素：

- 每个 CM 有一个或多个短的（14 比特）业务标识符（SID）和一个 48 比特的地址；
- 上行带宽分为一串微时隙流。每个微时隙由 CMTS 维护的主参考基准来编号，时钟信息由 SYNC 包分发给各个 CM；
- 各个 CM 可以向 CMTS 发出上行带宽请求。

CMTS应在下行信道上传送分配MAP PDU，以规定对每个微时隙应用的许可。分配MAP如下所述。

8.1.1 分配 MAP 的 MAC 管理信息

分配MAP是一种由CMTS传送的可变长度的MAC管理消息，用来定义在上行信道上的传送机会。它包括固定长度的包头，后面跟着数量可变的信息单元（IE），其格式如7.3.4所示，每个信息单元规定了一批微时隙允许的用法。

注： CM和CMTS应将分配开始和确认时间的低（26-M）比特位用作有效的MAP开始和确认时间，其中的M在7.3.3中定

义。分配开始/确认时间计数器和时戳计数器之间的关系在8.3.4中进一步说明。

8.1.2 信息单元（IE）

每个IE由14比特SID、4比特类型码和14比特起始偏移组成，如7.3.4所定义。由于所有的台站应扫描所有的IE，因此缩短这些IE的长度并相对固定其格式是十分关键的。在MAP中的IE是严格按照起始偏移来排序的。由IE所描述的持续时间是可以从该IE的起始偏移与其后面的一个IE的起始偏移之差来推断出来。因此，这张表应以一个空的IE来结束。见表36。

4种类型的SID定义如下：

- 0x3FFF：广播，供所有的台台站使用；
- 0x2000-0x3FFE：组播，其目的由管理性质规定。见附录 A；
- 0x0001-0x1FFF：单播，针对特定的 CM 或与该 CM 间的特定业务；
- 0x0000：空地址，不寻址任何台站。

CM应支持下面定义的所有信息单元。CMTS在生成带宽分配MAP时可以使用这些信息单元的任意组合。

8.1.2.1 请求 IE

请求IE提供了一个上行间隔，该间隔可以被用作请求上行数据传送所需带宽。该IE的特点随着SID的类别而变化。如果是广播，这就是对各CM争用请求的邀请。8.4说明可以使用什么样的争用传送机会。如果是单播，则这是对特定CM请求带宽的邀请。可以使用单播作为业务质量控制时序方案的一部分（见9.2）。在此间隔传送的包应使用Request MAC帧格式（见7.2.5.3）。

少量的优先请求SID在附录A中定义。这样就使得请求IE争用被限制于给定通讯优先级的那些业务流（见C.2.2.5.2）。

8.1.2.2 请求/数据 IE

请求/数据IE提供了一个上行间隔，在此间隔中可以传送带宽请求或短数据包。请求/数据IE与请求IE的不同在于：

- 它提供了一种分配算法。在轻负荷的情况下，用这种方法可以提供立即的数据争用。而当网络负荷增大时又能够撤回这种争用的机会；
- 应使用组播 SID 来规定在该间隔之内的最大数据长度，以及允许的随机起始点。例如，一个特定的组播 SID 可以规定最大 64 字节的数据包，以及每隔 4 个微时隙的传送机会。

附录A中定义了几种常用的组播SID。

由于传送的数据包在此间隔内可能碰撞，CMTS应对成功接收的任何数据包做出确认。MAC包头中应确认成功接收的数据包（见表29）。

8.1.2.3 初始维护 IE

初始维护IE提供新台站可以接入网络的时间间隔。应提供一个等于最大往返传播延时加上测距请求消息（RNG-REQ）传播时间的间隔（见8.3.3），应允许新台站进行初始测距。在该间隔中传送的包应使用RNG-REQ MAC管理消息格式（见7.3.5）。

8.1.2.4 台站维护 IE

台站维护IE为台站进行测距、功率调整等常规的网络维护工作提供时间间隔。CMTS可以请求一个特定的CM进行某些与网络维护有关的工作，如周期性的发送功率调整。在这种情况下，台站维护IE是用单播来提供执行此任务的上行带宽。在此间隔中传送的包应使用RNG-REQ MAC管理消息格式（见7.3.5）。

8.1.2.5 短数据和长数据授权 IE

短数据和长数据授权IE为单个CM传送一个或多个上行PDU提供机会。这些IE可以为响应一个台站的请求而发布，或者出于管理策略为特定的台站提供一定量带宽（见下面业务类别的讨论）。这些IE也可以用于推断的0微时隙长度（0长度授权），以指出请求已经收到但处在挂起状态（数据授权挂起）。

短数据授权用于小于或等于在上行信道描述符中为此用途规定的最大突发长度的间隔中。如果短数据突发特性在UCD中被规定，则所有长数据授权占用的微时隙都应比短数据的最大微时隙数目还要多。长数据授权和短数据授权的区别可以在物理层前向纠错编码中使用；否则在带宽分配过程中没有意义。

如果此IE是一个数据授权挂起（0长度授权），则其后应跟着一个空IE，使CM在扫描MAP以寻找数据授权挂起和数据确认之前，首先处理所有的实际分配。

8.1.2.6 数据确认 IE

数据确认IE对接收到的数据PDU做出确认。该CM在数据PDU中应已经请求了此项确认（通常应当对于在争用的间隔中发送的PDU进行请求确认，以检测碰撞）。

此IE之后应跟随着空IE，使CM在扫描MAP以寻找数据授权挂起和数据确认之前，首先处理所有的实际分配。

8.1.2.7 扩展 IE

如果将来的IE需要16个以上的码字或32比特时，扩展IE提供了可扩展性。

8.1.2.8 空 IE

一个空IE结束IE列表中的所有实际分配操作。它用来推断最后间隔的长度。所有数据确认IE和所有数据授权挂起IE（推断长度为0的数据授权）的后面都应跟着空IE。

8.1.3 请求

请求是CM向CMTS表示它需要上行带宽分配的一种机制。请求可以作为一个独立的请求帧传送（见7.2.5.3），也可以作为另一个帧传送的EHDR（扩展头）中的附带请求（见7.2.6）。

请求帧可以在以下的任何一个间隔期间传送：

- 请求 IE；
- 请求/数据 IE；
- 短数据授权 IE；
- 长数据授权 IE。

附带请求可以包含在如下的扩展包头中：

- 请求扩展头（EH）单元；
- 上行加密扩展头（EH）单元；
- 带分段的上行加密扩展头（EH）单元。

请求应包括：

- 提出请求的 SID；
- 请求的微时隙数目。

请求的微时隙数目应是在请求时CM所要求的微时隙总数（包括所有的物理层开销），它受到UCD和管理的限制。CM应请求相应于一个完整帧的微时隙数目，附带模式中的分段的情况除外（见9.3.2.2）。

注 1：在请求中应考虑的物理层开销包括：保护带、前同步码和前向纠错（FEC），它们都依赖于突发的特性。

注 2：针对UCD中的长数据授权IUC ，CM受最大突发长度限制。

注 3：针对业务流，CM受最大级联突发的限制（见C.2.2.6.1）。

注 4：帧是指单个的MAC帧或一个级联MAC帧。

CM对每个SID、每次应只能有一个请求挂起。如果CMTS没有立即用数据授权进行响应，CM能够清楚地确定它的请求仍然挂起，因为只要请求尚未满足，CMTS就应继续在随后每个MAP中发布数据授权挂起。

在MAP中， CMTS对任何指定的SID都不能进行大于255个微时隙的数据授权。这就对CM应支持的授权长度给出了一个上限值。

8.1.4 IE 特征用途总结

表38总结了CM使用描述传输机会的每一种MAP IE类型所能够传输的各种帧的类型。在表中的“应”表示：如果合适的话，CM应能够在该类型机会传输该类型的帧；“可以”表示CM可以在该类型机会传输该类型的帧。“不应”表示CM不应在该类型机会传输该类型的帧。

表38 IE特征兼容性总结

IE	传输请求帧	传输级联MAC帧	传输分段的MAC帧	传输测距请求	传输任何其它的MAC帧
请求IE	应	不应	不应	不应	不应
请求/数据IE	应	可以	不应	不应	可以
初始维护IE	不应	不应	不应	应	不应
台站维护IE	不应	不应	不应	应	不应
短数据授权IE	可以	应	应	不应	应
长数据授权IE	可以	应	应	不应	应

8.1.5 MAP传输和定时

分配MAP应及时传输，并被各个CM接收和处理。这样，其被传输的时刻可能比其起作用的时间早很多。延时的主要因素如下：

- 最坏情况下的往返传播时延：可能取决于网络情况，在几百微秒的数量级；
- 在CMTS内部的排队时延：与实现方式有关；
- 在各CM内部的处理时延：每个CM应允许如附录B中规定的一个最小的处理时间（CM MAP处理时间）；
- PMD层FEC交织。

不同MAP所描述的微时隙数目可能不同。在最少时，一个MAP可能描述单个的微时隙。这将会对下行带宽及各CM内部的处理时间造成浪费。在最多时，一个MAP可能会延伸到几十毫秒。这样的MAP将会使上行反应时间变得很差。分配算法可以随着时间变更MAP的长短，以便在通讯负荷变化的情况下，使网络的利用率和反应时间保持平衡。

在最短时，一个MAP应包括两个IE：一个用来描述时间间隔，另一个是空IE以结束该列表。在最长时，一个MAP应受240个IE的限制。将来MAP还受到不应描述超过4096个微时隙的限制，以限制将来每个CM需要跟踪的微时隙的数目。一个CM应支持处理多个待处理MAP，但即便有多个MAP待处理，它们描述的微时隙总数也不能超过4096个。

所有MAP加在一起形成的集合应描述上行信道中的每一个微时隙。如果一个CM未能接收到描述一个特定间隔的MAP，则该CM不应在该间隔期间进行传输。

8.1.6 协议举例

本条说明当CM有数据要传输时，CM和CMTS之间的交互过程（见图65）。假定一给定CM有一个数据PDU要传输。

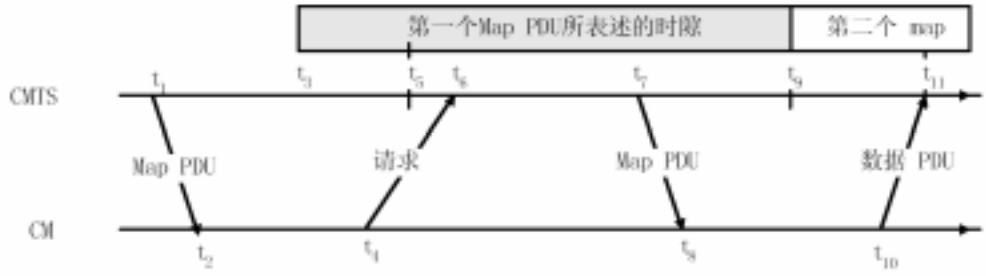


图65 协议举例

图65说明如下：

a) 在时刻 t_1，CMTS 传送一个 MAP，其有效起始时刻为 t_3。在此 MAP 中含有一个将在 t_5起始的请求 IE。时刻 t_1和 t_3之间的时间差是用于：
   1) 下行传播时延（包括前向纠错 FEC 交织），使得所有的 CM 都能够接收该 MAP；
   2) 在 CM 内部的处理时间（使得 CM 能够解析该 MAP，并将其转化成传输机会）；
   3) 上行传播时延（使得 CM 的第一个上行数据传输及时开始，从而使之在 t_3时刻到达 CMTS）；
b) 在 t_2时刻，CM 接收此 MAP 并对其扫描以找到请求机会。为了尽量减少请求碰撞，它以最近的 MAP 中的数据退避起始值为基点把 t_6作为一个随机偏移值(见 8.4 及 A.2 中的组播 SID 的定义)；
c) 在 t_4时刻,CM 按照该 PDU 所需要的微时隙数传送一个请求。时刻 t_4是基于测距偏移来选定的(见 8.3.3)，这样该请求将在 t_6时刻到达 CMTS；
d) 在 t_6时刻 CMTS 接收该请求并进行时序安排，以便在下一个 MAP 进行授权（选择授权哪些请求将随着请求的业务类别、有无竞争请求及 CMTS 所使用的算法不同而变化）；
e) 在时刻 t_7，CMTS 传送一个 MAP，其有效起始时刻为 t_9。在此 MAP 中，对该 CM 的授权将从 t_{11}开始；
f) 在 t_8时刻，CM 接收该 MAP 并扫描给它的数据授权；
g) 在 t_{10}时刻，CM 传送其数据 PDU，使其将在 t_{11}到达 CMTS。时刻 t_{10}由步骤 3 中所述的测距偏移计算而得。

如果各个CM保持一个请求机会表，则a）和b）不必考虑接入等待时间。

在c），该请求可能因与来自其它各CM的请求相碰撞而丢失。CMTS并不直接检测这种碰撞。当下一个MAP未能包括该请求的确认时，CM就认定发生了碰撞（或其它接收故障）。这时，CM应执行一个退避算法并进行重试，见8.4.1。

在d），CMTS时序处理可能未能把该请求容纳在下一个MAP中。如果是这种情况，它就应在该MAP中用一个零长度的授权来回答，或者丢弃该请求而不作任何授权。它还应继续在以后的所有MAP中报告此零长度的授权，直到该请求能够被授权或放弃为止。这种情况应通知该CM,请求仍处在挂起状态。只要该CM仍然接收到零长度授权，它就不应再向该业务队列提出新的请求。

8.2 对多信道的支持

各厂家可能选择在一个MAC业务接入点上提供上行信道和下行信道的各种不同组合的做法。上行带宽分配协议允许通过一个或多个下行信道来管理多个上行信道。

如果多个上行信道与一个下行信道相关联，则CMTS就应给每个上行信道发送一个分配MAP。MAP的信道标识符和上行信道描述符信息（见7.3.3）一起应规定每个MAP是用于哪个信道。并不要求各个MAP跨越各信道而同步。附录H提供了一个例子。

如果多个下行信道与一个上行信道相关联，则CMTS应保证分配MAP能到达所有的CM。也就是说，如果某些CM连接到一个特定的下行信道，则该MAP应在那个信道上传送。这样就可能需要传送同一个MAP的多个副本。该MAP包头中的分配起始时间应总是和传送MAP的下行信道上的同步基准相关联。

如果多个下行信道与多个上行信道相关联，则CMTS就可能需要传送多个MAP的多个副本，以保证所有上行信道都被指定MAP，并且所有的CM都已经接收到它们各自需要的MAP。

8.3 定时和同步

在为HFC网络设计MAC协议时，主要难点之一就是对其所设计的长时延的补偿问题。这些时延比上行传输突发时间要大一个数量级。为了补偿这些时延，CM应能够对其传输进行精确的定时，使之在指定的微时隙开始时到达CMTS。

为了实现这一点，每个CM需要如下的两个信息：

- 从 CMTS 向所有的 CM 下行传送一个全局定时参考；
- 为每个 CM 在测距过程中计算出一个定时偏移。

8.3.1 全局定时参考

CMTS应以一个标称的频率下行传送时间同步（SYNC）MAC管理消息，以建立一个全局的时间参考。该消息包括一个能精确识别CMTS何时发送该消息的时戳。这时，各个CM应将接收该消息时的实际时间与该时戳进行比较，并相应地调整它们各自的本地时钟参考。

传输会聚子层应和MAC子层密切配合，为该SYNC消息提供一个准确的时戳。如下面测距一节中所述的那样（见8.3.3），该模型假定通过PHY子层的其余部分的时延应是相对恒定的。PHY子层延时的任何变化都应在PHY子层开销的保护时间中加以考虑。

各SYNC消息之间的标称间隔有意做成几十毫秒。这样对于下行开销影响很小，又使得CM能够迅速地获得它们的全局定时同步。

8.3.2 CM 信道获取

任何CM在其成功地同步于下行信道之前，都不应使用上行信道。

首先，CM应建立PMD子层同步。这就意味着它已经锁定在正确的频率上，对该下行信道作了均衡，恢复了任何PMD子层帧，并且前向纠错（FEC）已经工作（见10.2.2）。这时，一个有效的比特流正在送往传输会聚子层。传输会聚子层执行其自己的同步（见第6章）。在检测到PID并按照GB/T 17975.1检测到有效负载单元起始指示符时，它就将MAC帧传送到MAC子层。

此时，MAC子层应搜索定时同步（SYNC）MAC管理消息。一旦CM已经接收至少两个SYNC消息，并且证实其时钟容差在规定的范围之内时，CM便获得了MAC同步。

一个CM只要能够继续成功地接收SYNC消息，它就会保持在“ SYNC ”状态。如果丢失的SYNC间隔（见附录B）超时而没有获得一个有效的SYNC消息，则CM不应使用该上行信道，并应尝试再重新建立同步。

8.3.3 测距

测距是获得正确的定时偏移而使得CM的传输与正确的微时隙边界对齐的过程。通过PHY子层的时延应相对恒定。PHY子层时延的任何变化都应在上行PMD子层开销的保护时间中加以考虑。

首先，CM应同步于下行信道，并通过上行信道描述符MAC管理消息来了解上行信道的特性。这时，CM 应扫描带宽分配MAP信息来寻找一个初始维护区（见8.1.2.4）。CMTS应建立一个足够大的初始维护区，以便考虑任意两个CM之间时延的变化。

CM应把要在初始维护区中发送的测距请求消息放置在一起。其SID域应设定为非初始化的CM值（0）。

测距工作将调整每个CM的定时偏移。CM应将其初始定时偏移设定为一个内部固定延时量，其数值相当于将此CM紧邻CMTS。这个时延量包括了通过某一特定的实现所引入的时延，并且应包括下行PHY交织等待时间。

当初始维护传输机会出现时，CM应将该测距请求消息发出。

一旦CMTS已经成功地接收到该测距消息，它应向该CM返回一个测距响应消息，并分配给该CM一个临时SID，在此CM完成注册过程之前临时SID一直有效。测距响应消息中还应包括关于RF功率电平调整、偏移频率调整以及任何定时偏移校正的信息。

此时，该CM应等待分配临时SID的单个台站维护区域，并使用该临时SID以任意功率电平和定时偏移校正参数来发送测距请求消息。

CMTS应向该CM返回另一个测距响应消息，其中包括任何所需要的附加的微调。这种请求/响应的步骤应重复多次，直到该响应中包括了测距成功通知或者CMTS异常中断该项测距为止。一旦测距成功，CM应加入到正常的上行数据业务中去。关于整个初始化序列的全部细节参见第10章。10.2.4中还特别规定了状态机、重试次数的适用性以及测距过程的定时器值等内容。

注： 任何传输所使用的突发类型由间隔使用码（IUC）规定。每一个IUC对应一种UCD消息中的突发类型。

8.3.4 定时单位和相互关系

SYNC消息传送一种时间参考，该时间参考是用6.25 μs的时间节拍来度量的。在SYNC消息中还有更高分辨率的6.25/64 μs时间节拍，使得CM能够以小相位偏移来跟踪CMTS的时钟。这些时间单位是按照各

种不同的调制方式和符号率的上行信道微时隙时间的最大公约数来选择的。由于这种做法不考虑任何特定上行信道的特性，所以对于与该下行信道相关联的所有上行信道均可以使用单一的SYNC时间参考。

带宽分配MAP使用微时隙作为时间单位。一个微时隙代表传送某一固定数量字节数所需要的时间。尽管可以选择其它的数值，但是微时隙的期望值是16个字节时间。以SYNC时间参考的倍数表示的微时隙的长度由UCD来传送。表39中的例子说明了微时隙和SYNC时间节拍之间的关系。

表39　微时隙和时间节拍之间关系的示例

参数	举例值
时间节拍	6.25μs
每个微时隙的字节数	16（标称值，当使用QPSK调制时）
符号/字节	4（假定使用QPSK）
符号/秒	2560000
微时隙/秒	40000
微秒/微时隙	25
时间节拍/微时隙	4
a　符号/字节是单个突发传输的特性，而不是信道的特性。在这个例子中，根据所选择的调制方式不同，一个微时隙可以代表 16 字节或 32 个字节。	

“微时隙”是用于上行传输机会的基本单位。

MAP对微时隙以32比特的计数器进行计数，该计数器通常计数到（2^{32}-1）然后回零。微时隙计数器的最低有效位（即比特0到比特25-M）应与SYNC时戳计数器的最高有效位（即比特6+M到比特31）相匹配。即微时隙N在时戳参考为（NxTx64）时开始，其中$T=2^{M}$是定义该微时隙的UCD倍数（即每个微时隙的时间节拍数）。

注 1：CM不需要32比特微时隙计数器的那些没用上的高比特位，并可能将这些比特位忽略掉。

注 2：由于UCD倍数限制为2的幂，结果每个微时隙的字节数目也应是2的幂。

8.4　上行传输和争用解决

CMTS通过MAP控制对上行信道的分配，并确定哪些微时隙可能发生碰撞。CMTS可以允许各个请求的碰撞或各个数据PDU的碰撞。

本条给出了上行传输和争用解决的概述，提到CM如何进行冲突检测与退避。因为一个CM能够有多个上行业务流（每个业务流具有自己的SID），它可以根据每个业务队列或每个SID作出决定。有关状态转移图和更详细的情况见附录J。

8.4.1　争用解决概述

应支持的争用解决的强制方法是基于一种截短的二进制指数退避值，而由CMTS控制其起始退避窗口和最大退避窗口。这些退避值规定为该带宽分配MAP MAC信息的一部分，并用一个2的幂的数值来表示。例如，数值4表示0～15的窗口；数值10表示0～1023的窗口。

当一个CM有信息要传送并想要进入争用解决过程时，它就将其内部退避窗口设定成等于当前有效MAP中的数据退避开始值。（当前有效MAP是其分配开始时间已经发生，但其包含的IE尚未发生的MAP。）

CM应在其退避窗口内随机地选择一个数。该随机数表示在传送之前CM应推迟的争用传送机会的数目。CM应只考虑对于此传送来说符合条件的传送机会。这种传送机会由该MAP中的请求IE或请求/数据IE来确定。每一个IE能够表示多个传送机会。

例如，一个CM的初始退避窗口为0～15，其随机选择的数为11，CM应推迟11个争用传送机会。如果第一个可用的请求IE有6个请求机会，则CM不使用它，还要再推迟5个机会。如果下一个请求IE有2个请求机会，则CM还需再推迟3个机会。如果第三个请求IE有8个请求机会，则CM在推迟了3个机会以后，在第4个请求时传送。

在争用传送以后，CM等待在后续的MAP中的数据授权（数据授权挂起）或数据确认。一旦接收到其中之一，该争用解决就完成了。当CM发现MAP没有对它的数据授权（数据授权挂起）或数据确认，并且确认时间比传送时间还近时，CM就会确定该争用传送已经丢失。此时CM应将其退避窗口增大2的因数倍，只要其值小于最大退避窗口的数值即可。CM应在其新的退避窗口中随机地选择一个数，并重复上述推迟过程。

注：数据确认IE只用于碰撞检测的目的，而不是设计用来提供可靠的传输（这是更高层的责任）。如果一个MAP丢失或受到损坏，则等待数据确认的CM应假定它的争用数据传送成功，并且不应重新传送该数据包。这就防止了CM不必要地发送重复的数据包。

这种重试的过程继续进行，直到达到最大的重试次数（16）。此时该PDU就应予以丢弃。最大重试次数与CMTS规定的初始退避窗口和最大退避窗口无关。

如果CM在推迟该SID的任何时候接收到一个单播请求或数据授权，它就应停止争用解决过程并使用该传送机会。

CMTS在控制争用解决上有很大的灵活性。在一种极端的情况下，CMTS可以模拟一种以太网型的退避，对数据退避开始和数据退避结束的设定进行选择，这种设定具有其关联的简单性和分布性，也具有公平性和有效性方面的特点。在MAP中将退避开始设定为0，将退避结束设定为10就可以做到这一点。在另一个极端情况下，CMTS可以使数据退避开始和数据退避结束相互一致并经常更新MAP中的这些数值，使得所有的CM都使用相同的、最佳的退避窗口。

8.4.2 传输机会

传输机会定义为在其间允许CM开始发送的任意一个微时隙。传输机会一般应用于争用机会，并用来在争用解决过程中计算适当的推迟量。见表40。

与一个MAP中特定的IE相关联的传输机会的数值决定于该区域的总体大小以及一次单个发送所允许的大小。例如，假定一个REQ IE定义了一个12个微时隙的区域，如果该UCD定义了一个适合装入一个单微时隙的REQ突发长度，则就有12个与此REQ IE相关联的传输机会，即每个微时隙对应一个。如果该UCD定义了一个适合装入2个微时隙的REQ，则就有6个传输机会，并且每隔一个微时隙可以开始一个REQ。

另一个例子，假定一个REQ/数据IE定义了一个24个微时隙的区域，如果它用0x3FF4的SID来发送(见附录A)，则一个CM可以每4个微时隙开始一次传送；因此，该IE总共包含6个传输机会。同样，SID为0x3FF6意味着4个传输机会；SID为0x3FF8意味着3个传输机会；SID为0x3FFC意味着2个传输机会。

对一个初始维护IE而言，CM应在该区域的第一个微时隙开始其传送；因此它有一个单个的传输机会。由于该CM还没有测距，该区域的其余部分就用来补偿往返时延。

台站维护IE、短/长数据授权IE和单播请求IE都是单播，所以它们通常都与争用传输机会无关。它们代表一个单个的、专用的或者保留的传输机会。

表40 传输机会

间隔	SID类型	传输机会
请求	广播	一个请求所需要的微时隙数
请求	组播	一个请求所需要的微时隙数
请求/数据	广播	禁用
请求/数据	常用的组播	在附录A中由SID所定义
请求/数据	组播	厂家定义
初始维护	广播	整个间隔是一个单个的传输机会

8.4.3 CM 带宽利用

以下规定了CM处理MAP的规则（这些标准的特性可以被CM的请求/传送策略所替代，见C.2.2.6.3）：

- CM 应首先使用指定给它的授权。然后，CM 应使用任何单播 REQ。最后，CM 应使用符合条件的下一个可用的广播/组播 REQ 或 REQ/数据 IE；

- 对一个特定的 SID，一次只有一个请求可以处于挂起状态；
- 如果 CM 有一个请求挂起，则它不能使用对该 SID 的争用间隔。

8.5 数据链路加密的支持

待定。

9 服务质量和分段

本章介绍了几种与服务质量（QoS）有关的概念，包括：

- 包分类和流标识；
- 业务流 QoS 调度；
- 动态业务建立；
- 分段；
- 两步激活模式。

9.1 操作原理

本部分中所介绍的各种协议机制，用于支持CM和CMTS之间的上行、下行通信的服务质量。本条给出了QoS协议机制的概述以及其在提供端对端的QoS中的作用。

对QoS的要求包括：

- 配置和注册功能，用于预先配置以 CM 为基础的 QoS 业务流和流量参数；
- 动态建立 QoS 业务流和流量参数的信令功能；
- 流量整形和流量策略功能，用于在上层业务接口和输出到 RF 的流量上进行以业务流为基础的流量管理；
- 对上行业务流的 MAC 调度和流量参数的利用；
- 对下行业务流的 QoS 流量参数的利用；
- 从上层业务接口到达规定的有效业务流的包分类；
- 将业务流特性分组为命名的业务类别，这样上层实体和外部应用（在 CM 和 CMTS 内）可以按完全一致的方式所需的 QoS 参数申请业务流。

提供增强型QoS的主要机制是将穿越RF MAC接口的包分类成业务流。业务流是提供特定QoS的包的单向流。根据对该业务流规定的QoS参数集，CM和CMTS通过流量整形、策略处理和优先级处理来提供这种QoS。

在这里定义QoS特点的主要目的是规定在射频接口上的传输顺序和调度。然而，为了提供端对端的QoS或监控CM的性能，这些特点通常需要与RF接口以外的机制一起工作。例如，允许下列的操作：

- 可以通过 CM MIB 定义来修改 TOS 字节，本部分未定义这种修改。不管 TOS 字节是如何获得的或者是由谁写的（始发者或 CM 处理），CMTS 都在上行方向接管 TOS 字节的设定;
- CMTS 在下行方向业务流的排队可以以 TOS 字节为基础;
- 下行业务流可以由 CM 重新分类，以便为用户侧网络提供增强的业务。

业务流在上行和下行两个方向存在，并且实际上可以在没有激活的通信流量的情况下存在。业务流具有由CMTS指定的32比特的业务流标识符（SFID）。所有的业务流都具有SFID；有效的和容许的上行业务流还具有一个14比特的业务标识符（SID）。

在每个配置文件中，至少应定义两个业务流：一个用于上行，另一个用于下行。第一个上行业务流表示基本上行业务流，并且用作其它无法分类的通信业务的缺省业务流，包括MAC管理消息和数据PDU。第一个下行业务流描述基本下行业务流的业务。在配置文件中定义的其它附加业务流建立提供QoS服务的业务流。

输入的包匹配到某个分类器以决定该包转发到哪个QoS业务流。分类器能够检查该包的LLC包头、该包的IP/TCP/UDP包头或者这二者的某种组合。如果该包和其中一个分类器相匹配，则它就转发到由该分类器的SFID属性所指出的业务流。如果该包和这些分类器都不匹配，则它就在基本业务流上转发。

9.1.1 概念

9.1.1.1 业务流

业务流是一种MAC层的传输业务，它为CM发送的上行包或CMTS发送的下行包提供单向的包传输。业务流的特性由等待时间、抖动和吞吐量保证等QoS参数集来表示。为了使CM和CMTS之间的操作标准化，这些属性包括CM如何请求上行微时隙以及期望的CTMS上行调度器的特性等细节。

注： 这里所定义的业务流和IETF的集成业务流（intserv）工作组（参见RFC－2212）所定义的“ 流 ”的概念没有直接的关系。一个集成业务流是共享传输层终点的包的集合。多个集成业务流可以由一个单个的业务流来服务。然而，一个业务流的分类器可以以802.1P/Q为基础，集成业务流与此无关。

业务流的特性可以部分地由下列属性来表示：

- 业务流标识符（SFID）：存在于所有的业务流中；
- 业务标识符（SID）：仅存在于容许的或激活的上行业务流中；
- ProvisionedQosParamSet(预置的 QoS 参数集)：在配置文件中定义，并在注册期间呈现的 QoS 参数集合。这定义了授权模块允许的初始授权限制。一旦经注册建立了了业务流,就定义了预置的 QoS 参数集；
- AdmittedQosParamSet(容许的 QoS 参数集)：定义了 CMTS（并且可能还有 CM）为其预留资源的 QoS 参数集。要预留的主要资源是带宽，但是也包括存储器或者用来后续激活该业务流的以时间为基础的任何其它资源；
- ActiveQosParamSet(激活的 QoS 参数集)：定义了实际上向业务流提供的的 QoS 参数集，只有激活的业务流可以传送包。

注 1：有些属性是从上面的属性表中获得的。业务分类名称是ProvisionedQosParamSet的一个属性。业务流的激活状态是由ActiveQosParamSet确定的。如果ActiveQosParamSet为空，则该业务流无效。

注 2：当一个流动态生成时，ProvisionedQosParamSet为空。

当CMTS为一个业务流指定SFID时，此业务流就存在。在CM和CMTS中，SFID是业务流的基本标识。一个存在的业务流至少有一个SFID以及一个与其相关联的方向。

授权模块是在CMTS内的一个逻辑功能，它同意或拒绝与每个业务流相关联的QoS参数和分类器的每一个变更。这样它就定义了一个限制AdmittedQosParamSet和ActiveQosParamSet的可能的数值的“ 信封 ”。

QoS参数集之间的关系如图66和图67所示。ActiveQosParamSet总是AdmittedQosParamSet的一个子集，而AdmittedQosParamSet总是授权“ 信封 ”的一个子集。在动态授权模型中，这个信封由授权模块（用AuthQoSParamSet(授权QoS参数集)的标号来表示）来决定。在预置的授权模型中，这个信封由ProvisionedQosParamSet来决定。（有关授权模型的更进一步的信息见9.1.4）。

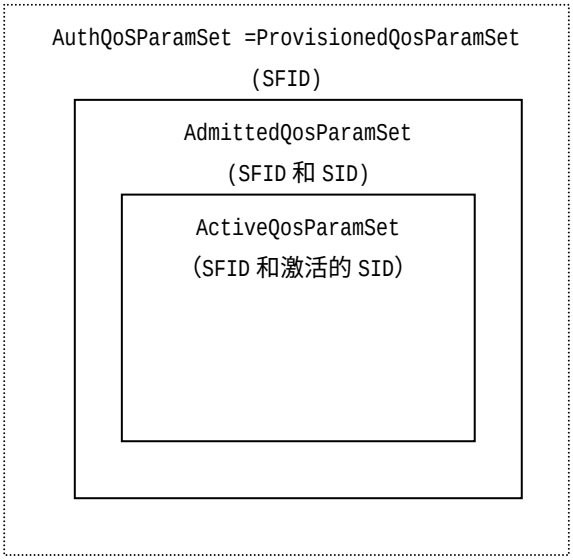


图66　预置的授权模型“ 信封 ”

注： 如果QoS参数集A是QoS参数集B的一个子集，则对于A集和B集中的所有QoS参数,下列各项应成立：

- 如果（较小的 QoS 参数值表示较少的资源，如最大的通信量速率）A 中的参数小于或等于 B 中的同一参数，则 A 为 B 的一个子集；
- 如果（较大的 QoS 参数值表示较少的资源，如容许的授权抖动）A 中的参数大于或等于 B 中的同一参数，则 A 为 B 的一个子集；
- 如果（QoS 参数规定了一个周期性的间隔，如标称的授权间隔）A 中的参数是 B 中的同一参数的整倍数，则 A 为 B 的一个子集；
- 如果（QoS 参数不是数量型的，如业务流调度型）A 中的参数等于 B 中的同一参数，则 A 为 B 的一个子集。

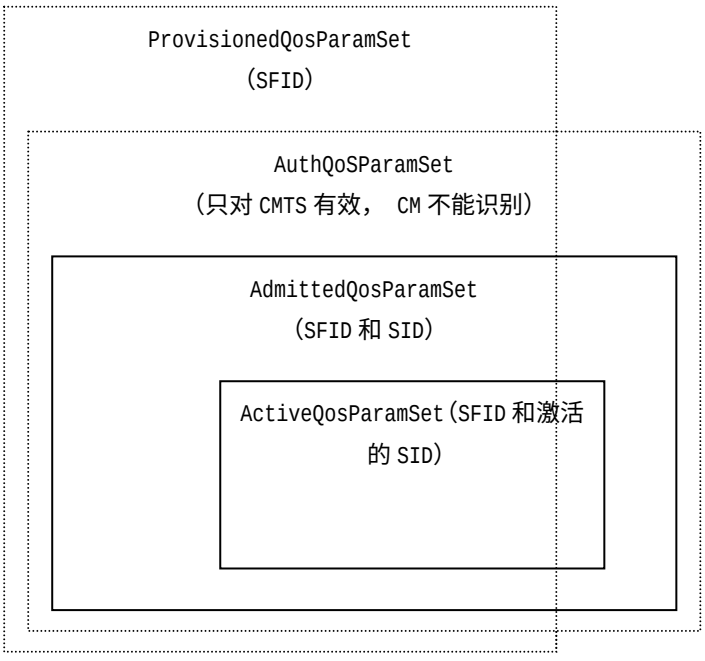


图67　动态授权模型“ 信封 ”

需要考虑三种类型的业务流：

- 预置的业务流：这种类型的业务流由于通过配置文件预置而得名，其 AdmittedQosParamSet 和 ActiveQosParamSet 均为空。一个预置的业务流可以有也可以没有其相关联的分类器。如果预

置的业务流有相关联的分类器，则不管分类器的激活状态如何，分类器不应用于把包分类到数据流上；

- 容许的业务流：这种类型的业务流具有由 CMTS 为其 AdmittedQosParamSet 预留的资源，但是这些参数并没有被激活（其激活的 QoS 参数集为空）。容许的业务流是可以被预置的，也可以是由某些其它机制标识。一般地说，容许的业务流有相关联的分类器，然而容许的业务流也可能使用基于策略的分类。如果容许的业务流有相关联的分类器，则不论分类器的激活状态如何，该分类器不应用于将包分类到流；
- 激活的业务流：这种类型的业务流具有由 CMTS 为它的 QoS 参数集承诺的资源（如，有效地发送包含基于 UGS 业务流的主动授权 MAP）。它的 ActiveQosParamSet 不为空。一般地说，激活的业务流有相关联的分类器，然而，激活的业务流也可能使用基于策略的分类。基本业务流可能具有相关联的分类器，但是除了与这种分类器相匹配的包外，所有不能与任何分类器相匹配的包将会在该方向上按照基本业务流发送。

9.1.1.2 分类器

分类器是应用于进入HFC网络的每个包的一组匹配准则。它包括一些包匹配准则（例如，目的地IP地址）、一个分类器优先级和一个对业务流的参考。如果一个包与规定的包匹配准则相匹配，则它就在参考的业务流中传送。

几个分类器可以都对应于同一个业务流。分类器优先级用于对包分类器的应用进行排序。由于分类器使用的方式可能重叠，所以应进行明确的排序。该优先级可以不是唯一的，但是在处理分类器优先级时应注意防止分类中的模糊性（见9.1.6.1）。下行分类器应用于CMTS下行发送包，上行分类器应用于CM中，并也可以用于CMTS中监控上行包的分类。图68说明了上面讨论的情况。

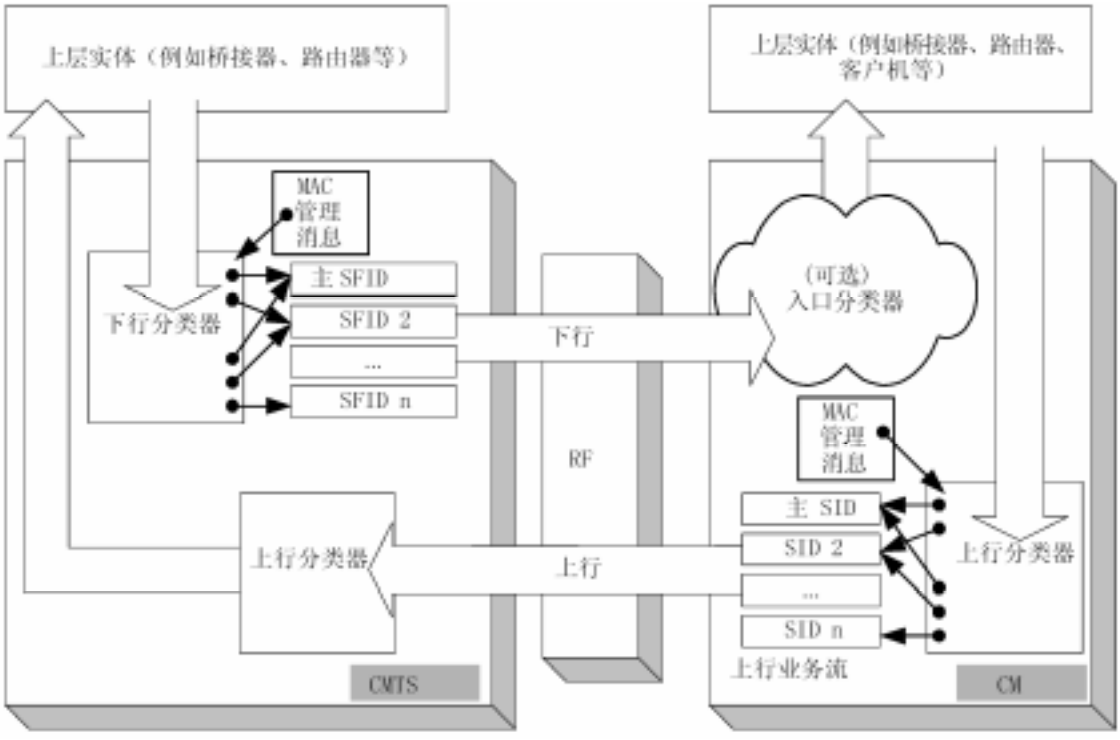


图68 MAC 层中的分类

CM和CMTS包分类包括了多个分类器，每个分类器包含一个优先级域，它决定了对分类器的搜索顺序。最高优先级的分类器应最先应用。如果发现一个分类器内所有的参数都与该包相匹配，则该分类器应把包传送到相应的业务流。如果数据包不能与任何分类器的参数相匹配，则该包就被分类到基本业务流中去。

包的分类表包含下列各域：

- 优先级：决定搜索分类表的顺序。高优先级的分类器比低优先级分类器先搜索；
- IP 分类参数：零或多个的 IP 分类参数（IP TOS 测距/掩码、IP 协议、IP 源地址/掩码、IP 目的地址/掩码、TCP/UDP 端口源起始、TCP/UDP 端口结束、TCP/UDP 目的端口起始，TCP/UDP 目的端口结束）；
- LLC 分类参数：零或多个的 LLC 分类参数。（目的 MAC 地址、源 MAC 地址、以太类型/SAP）；
- IEEE 802.1 P/Q 参数：零或多个的 IEEE 分类参数。（802.1P 优先级范围，802.1Q VLAN ID）；
- SFID：这个包要发往的特定业务流 ID。

分类器能够通过管理操作（配置文件、注册）或动态操作（动态信令、MAC子层业务接口）添加到分类表中。基于SNMP的操作能够观察由动态操作添加的分类器，但是不能修改或者删除由动态操作产生的分类器。分类表参数的格式在附录C中配置文件、注册消息或动态信令消息中规定。

分类器属性包括一个激活状态（见C.2.1.3.6）。设定“ 不激活 ”设置可用于为以后将激活的分类器预留资源。分类器是否真正激活依赖于这个属性和业务流的状态。如果一个业务流没有被激活，则无论分类器属性是什么，该分类器都不可用。

9.1.2 对象模型

该结构的主要对象在图69中用命名的矩形框来表示。每个对象有多个属性；唯一标识该对象的属性名称用下划线标出，可选择的属性则用括号标出。各对象之间的关系标在对象之间连线的两端。例如，一个业务流可以与从0～65535的分类器相关联，但是一个分类器却只能与一个业务流相关联。

业务流是MAC协议的核心概念。它由CMTS指定的一个32比特的SFID来唯一地标识。业务流可以在上行方向或下行方向。单播的SID是由CMTS预置的14比特表示，它仅与一个容许的上行业务流相关。

在典型的情况下，一个向外发送的用户数据包由上层协议（例如一个CM的前向桥接）提交，以便在HFC数据MAC接口传送。该包与一组分类器进行比较。与该包匹配的分类器通过SFID来标识相应的业务流。在有一个以上的分类器与该包相匹配的情况下，就选择优先级最高的分类器。

与一个包相匹配的分类器可以和一个包头抑制PHS规则相关联。PHS规则提供了关于如何忽略一个包PDU的包头字节，传送时用包头抑制索引来代替它，以及接收端恢复原有包头的细节。PHS规则由{SFID。PHSI}的组合来指示（见9.4）。当一个业务流被删除时，所有的分类器和它所关联的PHS规则也应被删除。

业务分类是一个可由CMTS实现的可选对象。它是由一个用作预置目的的ASCII名字来参考。在CMTS内定义的一个业务分类具有一个特定的QoS参数集。一个业务流的QoS参数集可以包含一个对该业务分类名称的参考，意味着选择该业务分类的全部QoS参数。在CMTS的授权下，该业务流的QoS参数集可以增大甚至替换该业务分类的QoS参数集（见C.2.2.5）。

如果上层策略机制已经确定一个包与一个特定的业务类别名称/优先级组合相关联，则该组合就把这个包和一个特定的业务流直接关联起来（见9.1.6.1）。上层也可以知道在MAC子层中的该特定业务流，并可能直接把这个包指定给一个业务流。在这种情况下，可以认为一个用户数据包直接地与由上层选择的业务流关联起来。这种情况在图69中用虚线箭头表示出来（见附录E）。

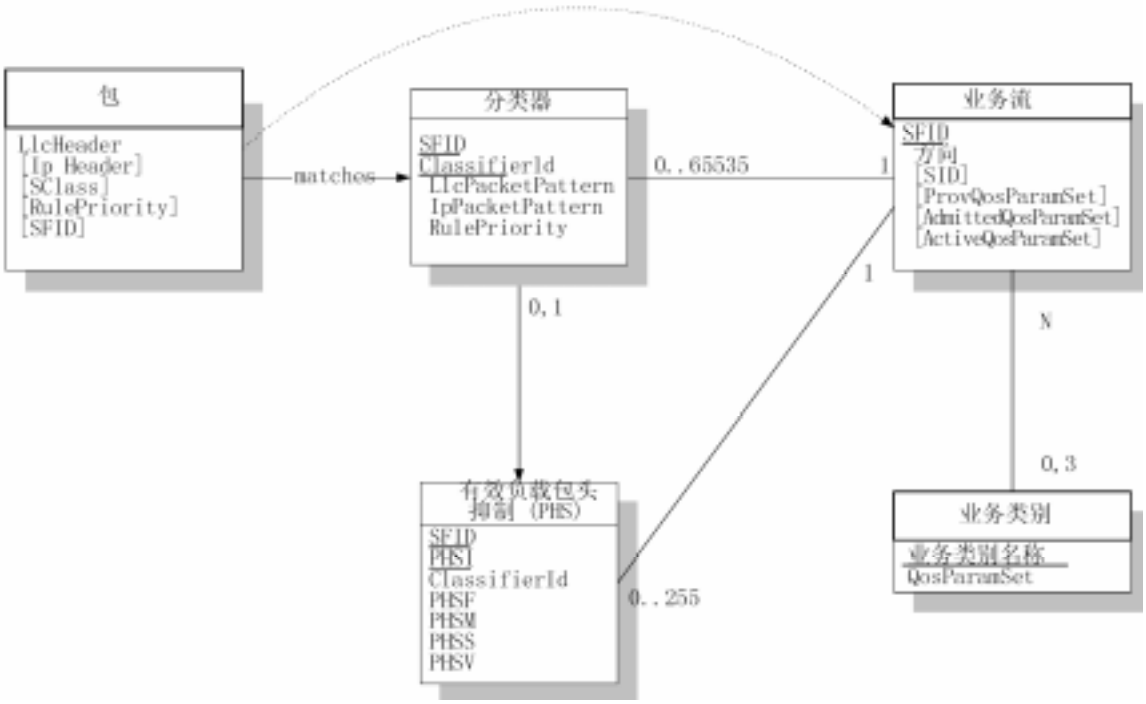


图69　工作对象模型理论

9.1.3　业务类别

一个业务流的QoS属性可以用两种方法来规定：可以明确地定义所有的属性，或通过规定一个业务类别名称来隐含地定义。业务类别名称是一个字符串，由CMTS把它和一个QoS参数集关联起来。

业务类别用于以下的各种目的：

a）　它允许操作员（操作员也希望这样做）把配置业务流的负担从预置服务器转移到 CMTS 去。操作员通过业务类别名称预置 CM；在 CMTS 内配置该业务类别名称。这就容许操作员在不改变 CM 预置的情况下，修改本地业务的实现。例如，在提供某种相同业务的时候，不同的 CMTS 需要不同的调度参数。又例如，在一天当中不同的时间也可能需要不同的服务特性；

b）　允许各个 CMTS 厂商提供基于类的队列，其中各业务流在它们的类内竞争、且各类间互相竞争带宽；

c）　它允许较高层的协议按照它的业务类别名称来产生业务流。例如，电话信令可以让 CM 说明“ G711 ”类的任何可用的预置业务流；

d）　它允许定义针对业务类别的包分类策略，而不必针对该类的特定业务流实例。

注：　业务类别是可选的：流调度技术特性可完整提供；一个业务流可以不属于任何业务类别。CMTS的实现可以用等效参数处理 与“ 分类业务流 ”不同“ 未分类 ”的流。

任何业务流都可以有下列三种方法之一规定的QoS参数集：

- 明确地包括所有流量参数；
- 通过规定一个业务类别名称间接地对应一个流量参数集；
- 规定一个带有修改参数的业务类别名称。

在CMTS成功地容许该业务流时，业务类别名称就“ 扩展 ”成它定义的参数集。业务类别的扩展可以包含在下列由CMTS发起的消息中：REG-RSP、DSA-REQ、DSC-REQ、DSA-RSP和DSC-RSP。在所有这些情况下，CMTS应包括一个业务流编码，该业务流编码包括业务类别名称和该业务类别的QoS参数集。如果一个CM发起的请求包含任何补充的或者替代的业务流参数，则一个成功的响应也应包括这些参数。

在容许的或激活的请求中给出一个业务类别名称时，返回的QoS参数集有可能随着激活的情况而变更。这是由于在CMTS里对业务类别的QoS参数集的配置的管理性变更。如果在CMTS定义的业务类别名称发生变更（例如其相关联的QoS参数集被修改），则它不影响与该业务类别相关联的已经存在的业务流的QoS参数。CMTS可以向引用该业务流类别名称的已经存在的业务流发起一个DSC事务，来影响该变更了的业务类别定义。

当一个CM使用业务类别名称来规定容许的QoS参数集时，该业务流的TLV编码的扩展集将会在其响应消息（REG-RSP、DSA-RSP或DSC-RSP）中返回到CM。如果业务类别名称的定义已经变更并且没有新的请求资源可以使用，则在以后的激活请求中使用该业务类别名称可能会失败。因此，在以后的激活请求中CM应当向该响应消息明确地请求TLV的扩展集。

9.1.4 授权

业务流QoS参数的每一变更应经过授权模块的批准。这包括了每个REG-REQ或DSA-REQ消息产生新业务流的情况，以及每个DSC-REQ消息变更已经存在的业务流的QoS参数集的情况。这些变化包括请求容许（例如设定AdmittedQoSParamSet）和请求激活业务流（例如设定ActiveQoSParamSet）。对于容许的或激活的资源的减少请求也要由授权模块来检查，这和添加或变更分类器时的情况一样。

在静态的授权模式中，授权模块接收所有的注册消息，并存储所有“推迟”的业务流的预置状态。只要容许的QoS参数集是预置的QoS参数集的一个子集，并且激活的QoS参数集是容许的QoS参数集的一个子集，则对这些预置的业务流的容许和激活请求将获得允许。变更预置QoS参数集的请求将被拒绝，产生新的动态业务流的请求也同样会被拒绝。这就定义了一个静态系统，其中所有可能的业务都在每个CM初始配置中定义。

在动态的授权模式中，授权模块不仅接收所有的注册消息，而且还通过一个分离的接口与独立的策略服务器进行通信。这个策略服务器可以为授权模块预先提供即将到来的容许的和激活的请求，并规定对这些请求要采取的授权行动。然后，来自CM的容许的和激活的请求由授权模块进行检查，以保证请求的ActiveQoSParamSet是由该策略服务器提供的一个子集。来自CM的、由外部策略服务器提前通告的容许的和激活的请求得到允许。而来自CM的、没有由外部策略服务器提前通告的容许的和激活的请求则可能会进入策略服务器实时队列，或者可能被拒绝。

在注册期间，CM应向CMTS发送从它的配置文件获得的TLV鉴别集，其中定义了预置的QoS参数集。CMTS接收并对其进行验证之后，这些消息将传送到CMTS内部的授权模块。CMTS应能够对预置的QoS参数集进行缓存，并且应能够使用这些消息来授权动态业务流，即一个预置的QoS参数集的子集。CMTS应该实现某种机制来替代该自动批准的过程（比如在动态授权模式中介绍的方式）。例如：

- 不论其是否已经提前预置，拒绝所有的请求；
- 建立丰富的策略机制内部表，但是用配置文件信息作为种子；
- 将所有的请求对应到一个外部策略服务器。

9.1.5 业务流的类型

本条只介绍三种基本的业务流类型。但应当注意到不仅仅只有这三种类型。（见C.2.2.3.5）。

9.1.5.1 预置的业务流

一个业务流可能被预置但没有立即被激活（有时称作“推迟”）。即在TFTP配置文件中任何这种业务流的说明包含预置的但推迟了激活和容许的属性（见C.2.2.3.5）。在注册期间，CMTS为这样的业务流指定一个SFID，但不预留资源。在容许之前CMTS也可能需要和策略模块进行协商。

对超出本部分范围的外部动作（例如[PKTCBL-MGCP]），CM可以选择通过传递该业务流ID和与其相关联的QoS参数集来激活一个预置的业务流。CM还应提供任何可应用的分类器。如果已经授权并有可用的资源，则CMTS应在响应中为该上行业务流指定一个唯一的单播SID。CMTS可以撤销撤消激活该业务流，但是不能在CM的注册期间删除该业务流。

对超出本部分范围的外部动作（例如[PKTCBL-MGCP]），CMTS可以选择通过传递该业务流ID和与其相关联的QoS参数集来激活该业务流。CMTS还应提供任可应用的分类器。CMTS可以使激活该业务流无效，但是不能在CM注册期间删除该业务流。这样的预置的业务流可以被激活和撤销激活很多次（通过DSC交换）。在所有情况下，当重新激活该业务流时应使用其原始的SFID。

9.1.5.2 容许的业务流

本部分支持一种两步的激活模式，这种模式常用于电话应用。在这种两步激活模式中，对一个“呼叫”的资源首先得到“容许”，然后一旦端到端的协商完成（例如被叫方的网关产生一个“摘机”事件），资源就被激活。这样一个两步的模式有下述的作用：

a) 在完整的端到端的连接建立之前保存网络资源；

b) 尽可能快地对资源进行策略检查和接纳控制，特别是向远端通知连接请求之前；

c) 防止一些潜在的业务盗用情况。

例如，如果一个上层业务正在使用主动授权业务，并且上层流的添加能够通过添加授权QoS参数中的每间隔时隙数来充分提供，则可以使用下述的方法。当第一个上层流挂起时，CM以容许的Grants-per-Interval参数等于1来发出一个DSA请求，激活的Grants-per-Interval参数等于0。当上层流被激活后，它以激活的Grants-per-Interval参数等于1来发出一个DSC请求。在保留的时间执行接纳控制之后，保证具有在前面保留范围的激活参数的DSC请求能够成功。后续的上层流也以同样方法来处理。如果有三个上层流建立连接，其第一个已经激活，该业务流将使容许的Grants-per-Interval参数等于4，并且激活的Grants-per-Interval参数等于1。

当新的ActiveQoSParamSet是AdmittedQoSParamSet的一个子集，并且没有添加新的分类器时，一个业务流的激活请求应得到允许（灾难性的失败的情况除外）。当AdmittedQoSParamSet是以前AdmittedQoSParamSet的一个子集，只要ActiveQoSParamSet仍然是AdmittedQoSParamSet的一个子集，则允许的请求应成功。

如果一个业务流已经有资源指定给它的AdmittedQoSParamSet，但它的资源还没有完全被激活，则这个业务流就处于过渡状态。CMTS应强制地确定一个超时的数值，要求在该时间内业务流被激活。（见C.2.2.5.7）。如果在这个时间间隔内没有完成业务流激活，则CMTS应释放多余的激活QoS参数中指定的资源。

某些应用中可能需要或希望长期的保留资源。例如：把一个电话呼叫占线不挂机将容许该呼叫所使用的资源暂时分配给其它用途，但是随后该呼叫恢复时还应可以再使用这些资源。在CMTS中该容许的QoS参数集保持在“软状态”；这种状态应周期性地刷新以便保持该状态，以免被上述超时功能释放其未激活的资源。这种刷新可以用带有相同QoS参数集的周期性的DSC-REQ消息作为信令，或者也可以用CMTS中的某些超出本部分范围的内部机制作为信令（例如，使用CMTS监视RSVP刷新消息）。每次刷新通知CMTS，CMTS应刷新“软状态”。

9.1.5.3 激活的业务流

具有非空的激活QoS参数集的业务流称为激活的业务流。该业务流正在请求并获得带宽授权以传输数据包。通过提供激活的QoS参数集，表明在当时实际所要求的资源，可以使一个容许的业务流成为激活的。这就完成了两步激活模式的第二步（见9.1.5.2）。

一个业务流可以被预置并立刻激活。这是用于基本业务流的情况。按月服务就是这种典型应用。这类业务流在注册的时候建立，并且应由支持MIC验证的CMTS授权。这些业务流也可以由CMTS授权模块授权。

另一种情况是，一个业务流可以动态地产生并立即激活。在这种情况下，就跳过两步激活，并且在授权之后立即可以使用。

9.1.6 业务流和分类器

基本模式是分类器将包严格地关联到一个业务流中。业务流的编码提供在RF接口上处理这些包所用的QoS参数。这些编码在C.2中介绍。

在上行方向，CM应把上行包分类到激活的业务流。CMTS应把下行流量分类到激活的下行业务流。对于那些未分类的广播和组播流量应有一个缺省的下行业务流。

CMTS监测上行业务流中的包以保证QoS参数的完整性和该包的TOS值。当包的发送速率大于CMTS的限定速率时，这些包就可能被CMTS丢弃（见C.2.2.5.2）。当TOS字节的数值不正确时，CMTS（基于策略）应改写TOS字节来校正这个流（见C.2.2.6.10）。

CM也许不能在特定业务流上转发特定上行包。特别是，不使用分段的主动授权业务的业务流不能用来传送大于授权长度的包。如果把一个包分类给一个不能传送它的业务流，则CM将根据该包被分类到的业务流的请求/传输策略来决定或者在基本业务流上传送这个包，或是将这个包丢弃。

只是在MAC管理消息包头（见7.3.1）的“类型”域与分类器相应参数匹配时，MAC管理消息才可通过包含C.2.1.6.3“以太网类型/DSAP/MAC类型”参数编码的分类器进行匹配。7.1.2.3是一种例外，即使分类器与台站维护的上行RNG-REQ相匹配，主SID应用于台站维护。对于没有任何匹配分类器的MAC管理消息，它应在基本业务流上发送。除了在C.2.1.6.3中被排除的MAC消息，CM或CMTS可以在任何业务流上以特定实现的方式转发另外的未分类MAC消息。

虽然MAC管理消息是服从于分类的，但它们不被看作是任何业务流的一部分。MAC管理消息的传输不应影响其将被分类的业务流的任何QoS计算。MAC管理消息的传递隐含地受到相关联的业务流的属性的影响。

基于策略的分类和业务类别

正如附录E中所述，有很多方法可以使包进入队列以便在MAC业务接口传输。一种极端的情况是和特定的有效负载包头抑制规则紧密捆绑的嵌入式的应用（见9.4），并且这种捆绑优先于一般的分类。另一个极端是一般传输包，在用MAC分类规则对其进行分析之前对它一无所知。另一种有用的方式是由更高层的实体对其进行策略处理，然后传递给MAC进一步分类到一个特定的业务流。

基于策略的分类超出了本部分的范围。这种策略可能比单独的业务流和MAC分类器存在的时间更长，所以在策略和MAC业务流分类之间使用定义良好的接口将这两种机制进行分层是比较合适的。

两层之间的接口是附加在MAC传输请求接口上的两种参数。这两种参数分别是业务类别名称和用于匹配该业务类别名称的规则优先级。策略优先级使用与MAC分类器包匹配规则的包优先级相同的级别。

MAC分类器的算法是：

```
MAC_DATA.request(PDU,
                    ServiceClassName,
                    RulePriority)
TxServiceFlowID = FIND_FIRST_SERVICE_FLOW_ID(ServiceClassName)
SearchID = SEARCH_CLASSIFIER_TABLE(All Priority Levels)
    IF (SearchID not NULL and Classifier.RulePriority>=MAC_DATA.RulePriority)
        TxServiceFlowID = SearchID
    IF (TxSearchFlowID = NULL)
        TRANSMIT_PDU(PrimaryServiceFlowID)
    ELSE
        TRANSMIT_PDU(TxServiceFlowID)
```

虽然策略优先级与包分类器优先级竞争，并且在理论上其选择可能有问题，应当选择常用的优先级范围以避免含糊。特别是，动态添加的分类器的优先级范围应为64到191。注册产生的分类器以及基于策略的分类器的优先级范围可以使用0到255，但是应避免上述的动态范围。

注：MAC子层之内的分类倾向于简单地把包和业务流关联起来。如果打算将一个包丢弃，则应由较高层实体来丢弃，而不传送到MAC子层。

9.1.7 一般操作

9.1.7.1 静态操作

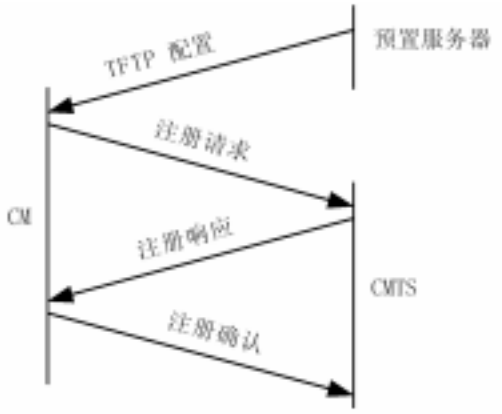


图70 注册消息流程

通过注册过程来完成分类器和业务流的静态配置。预置服务器为CM提供配置信息。CM在注册请求中将此信息传递给CMTS。CMTS添加一些信息，并用注册响应来应答。CM再发送注册确认以完成注册过程。见图70。

一个TFTP配置文件由一个或多个分类器实例和业务流编码组成。分类器按“优先级”松散地排序。每个分类器通过一个“业务流参考”对应于一个业务流。几个分类器可能对应于同一个业务流。此外，一个以上的分类器可能具有相同的优先级，此时所使用的特定分类器没有定义。见表41。

表41 TFTP 文件内容

项目	指向业务流参考	业务流参考	SFID
上行分类器 每个包括一个业务流参考（指针）	1..n		
下行分类器 每个包括一个业务流参考（指针）	(n+1)..q		
业务流编码 请求立即激活，上行		1..m	尚不存在
业务流编码 预置为以后的激活请求，上行		(m+1)..n	尚不存在
业务流编码 请求立即激活，下行		(n+1)..p	尚不存在
业务流编码 预置为以后的激活请求，下行		(p+1)..q	尚不存在

业务流编码包括业务属性的全部定义（可以省略那些可缺省的项目）或者包括一个业务分类名称。业务分类名称是一个CMTS知道的ASCII字符串，它间接地规定了一个QoS参数集。（见9.1.3和C.2.2.3.4）

注：在TFTP配置文件中，业务流参考由预置服务器定义。由于CMTS不知道这些业务流的定义，所以业务流标识符尚不存在。

注册请求数据包中包括下行分类器（如果被立即激活的话）和所有未激活的业务流。如果相应的业务流以推迟的激活来请求的话，则配置文件和注册请求一般不包括下行分类器。这就允许当流被激活时再绑定分类器。见表42。

表42　注册请求内容

项目	指向业务流参考	业务流参考	SFID
上行分类器 每个包括一个业务流参考（指针）	1..n		
下行分类器 每个包括一个业务流参考（指针）	(n+1)..p		
业务流编码 要求立即激活，上行 可以规定显式属性或业务类别名称		1..m	尚不存在
业务流编码 预置给以后的激活请求，上行 显式的属性或业务类别名称		(m+1)..n	尚不存在
业务流编码 请求立即激活，下行 显式的属性或业务名称		(n+1)..p	尚不存在
业务流编码 预置给以后的激活请求，下行 显式的属性或业务名称		(p+1)..q	尚不存在

注册响应根据注册请求中的QoS参数集类型来设定QoS参数集，见表43。

注册响应保留业务流参考属性，使得业务流参考能够和SFID/SID相关联。

表43　注册响应内容

项目	业务流参考	业务流标识符	业务标识符
激活的上行业务流 显式属性	1..m	SFID	SID
预置的上行业务流 显式属性	(m+1)..n	SFID	尚不存在
激活的下行业务流 显式属性	(n+1)..p	SFID	不适用
预置的下行业务流 显式属性	(p+1)..q	SFID	不适用

CMTS选择SFID以识别已经授权但尚未激活的上行或下行业务流。从CM来的容许或激活一个预置的业务流的DSC请求包含其SFID。如果是下行流则还包括下行分类器。

9.1.7.2　动态业务流的产生——由 CM 发起

业务流可以由动态业务添加过程产生，也可以通过上面介绍的注册过程产生。动态业务添加可以由CM或CMTS发起，并可以产生一个上行和/或一个下行动态业务流。用三步握手的方法产生业务流。由CM发起发起的协议在图71中示出，并在10.4.2.1中详细介绍。

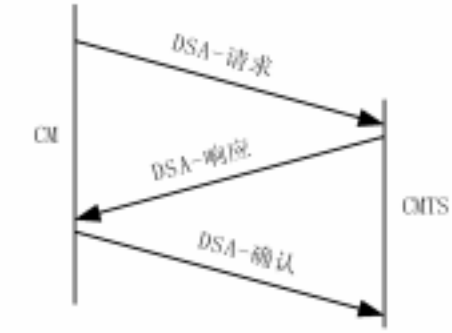


图71　动态业务添加消息流——CM 发起

来自CM的DSA请求包括业务流参考、QoS参数集（标明只对容许的或者对容许和激活的）以及任何需要的分类器。

9.1.7.3　动态业务流的产生——由 CMTS 发起

来自CMTS的DSA请求包括对一个上行业务流和/或一个下行业务流的业务流标识符，可能还会包括一个SID、激活的或容许的QoS参数集和任何其它需要的分类器。其协议在图72中示出，并在10.4.2.2中详细介绍。

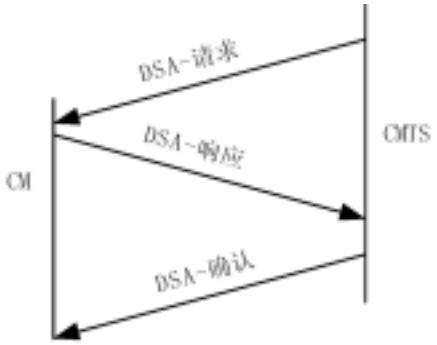


图72　动态业务添加消息流—CMTS 发起

9.1.7.4　动态业务流变更和删除

除了上面介绍的产生业务流的方法之外，还定义了修改和删除业务流的协议。见10.4.3和10.4.4。

预置的和动态产生的业务流都由DSC消息来修改，DSC消息能够变更该业务流的容许的和激活的QoS参数集。DSC还能够添加、替代或删除分类器，以及添加和删除PHS规则。

一个成功的DSC事务通过替代容许的和激活的QoS参数集来变更一个业务流的QoS参数。如果该消息只包括容许的集，则激活集就设定为空，并且该流撤销激活。如果该消息中的两个集都没有设定（所用的QoS参数集类型为'000' 见C.2.2.5.1），则两个集就都设定为空，并且该流为不容许。当该消息包括两个QoS参数集时，首先检查容许集。如果接纳控制成功，则按照该消息中的容许集来检查消息中的激活集，以保证其是一个子集（见9.1.1.1）。如果所有的检查均成功，则该消息中的QoS参数集就变成了该业务流的新的容许的和激活的QoS参数集。如果有一项检查没有成功，则该DSC事务失败，该业务流的QoS参数集不变。

9.2　上行业务流调度业务

以下定义基本上行业务流调度业务，并列出与每种业务相关联的QoS参数。每种QoS参数的详细说明在附录C中给出。本条还讨论如何将这些基本业务和QoS参数结合起来以形成新的业务，如承诺的信息速率（CIR）服务。

调度业务设计用来提高查询/授权过程的效率。通过规定调度业务及其相关的QoS参数，CMTS能够预计上行流量和等待时间需求，并在适当的时间提供查询和/或授权。

每种业务都针对如下所述的特定数据流类型而设计。基本业务包括：主动授权业务（UGS）、实时查询业务（rtPS）、具有活动检测的主动授权业务（UGS-AD）、非实时查询业务（nrtPS）和尽力而为（BE）业务。表44表示出调度业务与相关的QoS参数之间的关系。

9.2.1 主动授权业务

主动授权业务（UGS）设计用来支持周期性地产生固定长度数据包的实时业务流，如IP电话。该业务实时地周期性地分配固定长度时隙，免去了CM请求的开销和等待时间，并确保得到的授权满足该流的实时需求。CMTS应以周期性的间隔为该业务流分配固定长度的数据授权。为了使这种业务正确地工作，请求/传输策略（见C.2.2.6.3）设置应配为禁止CM使用任何争用请求或者请求/数据机会，并且CMTS应不提供任何单播请求机会。请求/传输策略也应禁止附带请求。这将导致CM对上行传送只使用主动数据授权。请求/传输策略的所有其它比特都和此调度业务的基本操作无关，并应当按照网络策略来设置。关键的业务参数是主动授权长度、标称授权时间间隔、容许的授权抖动和请求/传输策略（参见附录L）。

业务流EH单元（见7.2.6.3.2）中的主动授权同步包头（UGSH）用来从CM向CMTS传递有关UGS业务流状态的信息。UGSH的MSB是队列指示器（QI）比特。一旦检测到此业务流已经超出了它的传送队列深度，CM就应置位此标志。一旦CM检测到业务流传输队列回到其限制范围之内，它就应清零该QI标志。此标志使得CMTS以发布额外授权的方法对MAP丢失或时钟速率失配等情况下提供一定时间的补偿。

除了UGSH的QI比特被置位的情况外，CMTS给每个标称授权间隔分配的授权不能多于每个激活的QoS参数集的间隔参数的授权。在这种情况下，CMTS可以分配至多1%额外带宽作为时钟不匹配补偿。 如果CMTS分配额外带宽，它应在任何时间间隔到Max（T）期间限制在流上转发的总字节数，表示式为式（6）：

$$Max（T）=T×（R×1.01）+3B \quad \cdots\cdots（6）$$

式中：

Max（T）是时间T（单位秒）内在流上传送的最大字节数；

R=（授权长度×每间隔授权数）/标称授权间隔；

B=授权长度×每间隔授权数。

UGSH的激活授权域被UGS忽略。该业务流的CMTS策略保持不变。

9.2.2 实时查询业务

实时查询业务（rtPS）设计用来支持周期性地产生可变长度数据包的实时业务流，如MPEG视频。该业务提供实时的、周期性的、单播请求机会，以满足该流的实时需求，并允许CM请求期望的授权长度。此业务与UGS相比需要更多的请求开销，但能支持可变的授权长度以得到最佳的数据传送效率。

CMTS应提供周期性的单播请求机会。为了使这种业务正确地工作，请求/传输策略（见C.2.2.6.3）设定应设置为禁止CM使用任何争用请求或者请求/数据机会。请求/传输策略也应禁止附带请求。即使某个授权处于挂起状态，CMTS也可以照常分配单播请求时隙。这将导致为了得到上行传送机会，CM只能使用单播请求机会（CM仍然能够使用主动的数据授权用于上行传送）。请求/传输策略的所有其它比特都和此调度业务的基本操作无关，并应当按照网络策略来设置。关键的业务参数是标称查询间隔、容许的查询抖动和请求/传输策略。

9.2.3 具有活动检测的主动授权业务

具有活动检测的主动授权业务（UGS/AD）用来支持在大部分的时间（如几十毫秒或更长）里可能变为不激活的UGS流，如带静噪抑制的IP电话。当该流激活时该业务提供主动的授权，当该流不激活时该业务提供单播查询。这就把UGS的低开销和低等待时间与rtPS的效率结合了起来。虽然UGS/AD把UGS和rtPS组合起来，但是某一个时刻只有一个调度业务被激活。

当流激活时，CMTS应提供周期性的单播授权，但是当流不激活时，则应提供周期性的单播请求机会。CMTS能够通过检测未使用的授权来检测流的不激活状态。然而，检测一个流从激活变更到不激活的算法则取决于CMTS的实现。为了使这种业务正确地工作，请求/传输策略（见C.2.2.6.3）设定应设置为禁止CM使用任何争用请求或者请求/数据机会。请求/传输策略也应禁止附带附带请求。这将导致为了得到上行传送机会，CM只能使用单播请求机会。无论怎样，CM对上行传送也将使用主动的数据授权。请求/传

输策略的所有其它比特都和此调度业务的基本操作无关，并应当按照网络策略来设置。关键的业务参数是标称查询间隔、容许的查询抖动、标称授权间隔、容许的授权抖动、主动授权长度和请求/参数传输策略。

UGS-AD业务中，在一个rtPS间隔之后重新启动UGS时，CMTS应在第一个（和/或第二个）授权间隔中提供额外的授权，使得CM从重新启动UGS之时开始接收到每个授权间隔的一个完整授权，再加上一个额外的授权（参见附录L）。因为当重新启动UGS时业务流作为一个特定的授权间隔和授权长度来提供，CM不能请求与已经提供的UGS流不同长度的授权。和任何业务流一样，只能用DSC命令来请求变更。如果重新启动需要在一个授权间隔中有更多的授权，CM应在从第一个发送包开始的UGSH的激活授权域中标明。

业务流扩展包头单元允许CM动态地描述每个间隔需要多少授权来支持出现激活的流的数目。在UGS/AD中，CM可以使用UGSH中的队列指示器比特。UGSH的剩余7个比特定义了激活授权域。该域定义了在标称授权间隔中业务流当前需要的授权数目。当使用UGS/AD时，CM应在此域中指明每个标称授权间隔需要的授权数目。在UGS没有活动检测时，应忽略UGSH的激活授权域。这个域允许CM通知CMTS去动态地调整这个UGS业务流正在使用的每个间隔的授权数目。CM不能在激活的QoS参数集中请求更多的每个间隔授权数目。

如果CMTS在响应QI比特中分配了额外的带宽，它应使用和UGS相同的速率限制规则，但该规则仅适用于CMTS已调整到授权间隔与CM的激活授权请求相匹配的稳态期间。

当CM接收主动授权并不检测在业务流上的活动性时，它可以发送一个激活授权域设为零授权的数据包，然后结束传输。因为这个数据可能不被CMTS接收，因而当业务流从不激活到激活时，CM应用查询请求或主动授权重新开始传输。

9.2.4 非实时查询业务

非实时查询业务（nrtPS）用来支持按照规则需要可变长度数据授权的非实时业务流，如高带宽的FTP。该业务有规律地提供单播查询，以保证即使在网络拥塞期间该流也能接收到请求的机会。CMTS通常以数量级在1s或更短的周期性的或非周期性的间隔查询nrtPS SID。

CMTS应适时地提供单播请求机会。为了该业务正常工作，请求/传输策略（见C.2.2.6.2）设定应允许CM使用争用请求机会，这将导致CM使用争用请求机会、单播请求机会和主动的数据授权。请求/传输策略的所有其它比特都和此调度业务的基本操作无关，并应当按照网络策略来设置。关键的业务参数是标称的查询间隔、最低的预留流量速率、最大持续流量速率，请求/传输策略和流量优先级。

9.2.5 尽力传输业务

尽力传输业务（BE）的目的是提供高效业务以达到最大的通信流量。为了该业务正常工作，请求/传输策略设定应允许CM使用争用请求机会。这将导致CM使用争用请求机会、单播请求机会和主动的数据授权。请求/传输策略的所有其它比特都和此调度业务的基本操作无关，并应当按照网络策略来设置。关键的业务参数是最低的预留流量速率、最大持续流量速率和流量优先级。

9.2.6 其它业务

承诺的信息速率（CIR）

承诺的信息速率（CIR）业务可以用几种不同的方法定义。例如，可以使用一个具有最低通信速率的尽力传输业务或具有最低预留通信速率的nrtPS来配置。

9.2.7 上行业务调度的参数适用性

表44概括了调度业务和关键QoS参数之间的关系。在附录C中提供了每个QoS参数的详细说明。

表44　对上行业务调度的参数适用性

业务流参数	尽力传输业务	非实时查询	实时查询	主动授权	具有活动检测的主动授权
杂项					
流量优先级	可选的 缺省=0	可选的 缺省=0	不适用[a]	不适用	不适用
最大级联突发	可选的	可选的	可选的	不适用	不适用
上行调度业务类型	可选的 缺省=2	强制性的	强制性的	强制性的	强制性的
请求/传输策略	可选的 缺省=0	强制性的	强制性的	强制性的	强制性的
最大速率					
最大持续流量速率	可选的 缺省=0	可选的 缺省=0	可选的 缺省=0	不适用	不适用
最大流量突发	可选的 缺省=1522	可选的 缺省=1522	可选的 缺省=1522	不适用	不适用
最小速率					
最小预留流速率	可选的 缺省=0	可选的 缺省=0	可选的 缺省=0	不适用	不适用
假定的最小... 包长度	可选的[c]	可选的[c]	可选的[c]	可选的[c]	可选的[c]
授权					
主动授权长度	不适用	不适用	不适用	强制性的	强制性的
每个间隔的授权数	不适用	不适用	不适用	强制性的	强制性的
标称授权间隔	不适用	不适用	不适用	强制性的	强制性的
容许的授权抖动	不适用	不适用	不适用	强制性的	强制性的
查询					
标称查询间隔	不适用	可选的[c]	强制性的	不适用	可选的[b]
容许的查询抖动	不适用	不适用	可选的[c]	不适用	可选的[c]

a 不适用表示对这种业务流调度类型不适用。如果一个请求中包括这种业务流调度类型的业务流，此请求应被拒绝。

b 缺省值和标称授权间隔相同。

c 缺省值是 CMTS 规定的。

9.2.8　CM 传送特性

为了使这些业务工作正常，在一个业务流的传送性能方面对CM的全部要求就是它应当遵守8.4.3条规定的各项规则及对该业务流规定的请求/传输策略。

9.3　分段

分段是上行CM的一种能力。CMTS在注册响应中应能够用TLV在每个CM上打开或关闭此能力。在每个CM的基础上提供与EuroDOCSIS 1.0 CM的兼容性。对CM一旦打开分段，则分段就是基于每个业务流通过请求/传输策略设置来打开。当对一个业务流打开时，如果CMTS向一个特定的CM分配授权长度时隙小于该CM请求的相应带宽授权，则启动分段，这称为部分授权。

9.3.1　CM 分段支持

分段实质上是一个MAC帧的一部分的封装，带有一个固定长度的分段包头和分段CRC。级联PDU和单个PDU用相同的方法封装。

CM应根据图73中的流程图来进行分段。在图中，当分段尚未启动时“ 包的未传送部分 ”指的是：当分段尚未执行时指整个的MAC帧；当分段已经启动时指原始MAC帧的未传送部分。

分段规则：

a) 无论何时当分段打开且授权长度小于请求的长度时，CM 应考虑分段开销和物理层开销，用最大的数据量（分段有效负载）来填充它所收到的部分授权；
b) 无论何时，如果接收到的 MAP 中没有为 CM 的 SID 作后续授权或授权挂起，CM 应发送一个附带请求；
c) 如果 CM 正在对一个帧进行分段，则任何附带请求应在该分段包头的 BPI EHDR 部分进行；
d) 在对一个已经分段的帧（如果是级联，则指级联后的帧）的剩余部分计算带宽请求时，CM 应请求足够的带宽以传送该帧的整个剩余部分，还需加上 16 字节的分段开销和所有相关的物理开销；
e) 如果在发送请求的 ACK 时间之内 CM 没有接收到一个授权或授权挂起,则 CM 应退避并对该帧的未传送部分重新请求，直到带宽得到授权或 CM 超过其重试时间范围为止；
f) 在请求带宽时，如果 CM 超过其重试时间范围，则 CM 应丢弃以前没有发送帧的所有部分；
g) CM 应将帧的第一个分段中 F 比特置位，L 比特清零；
h) 对于帧的第一个分段和最后一个分段之间的任何分段，CM 应将其分段包头中的 F 和 L 比特清零；
i) CM 应将帧的最后一个分段中 F 比特清零，L 比特置位；
j) 对于发送帧的每一个分段，CM 应依次地添加其分段顺序号；
k) 在立即数据（请求/数据）区域发送的帧不应分段。

注： 帧总是指带有单个PDU的帧或者级联的帧。

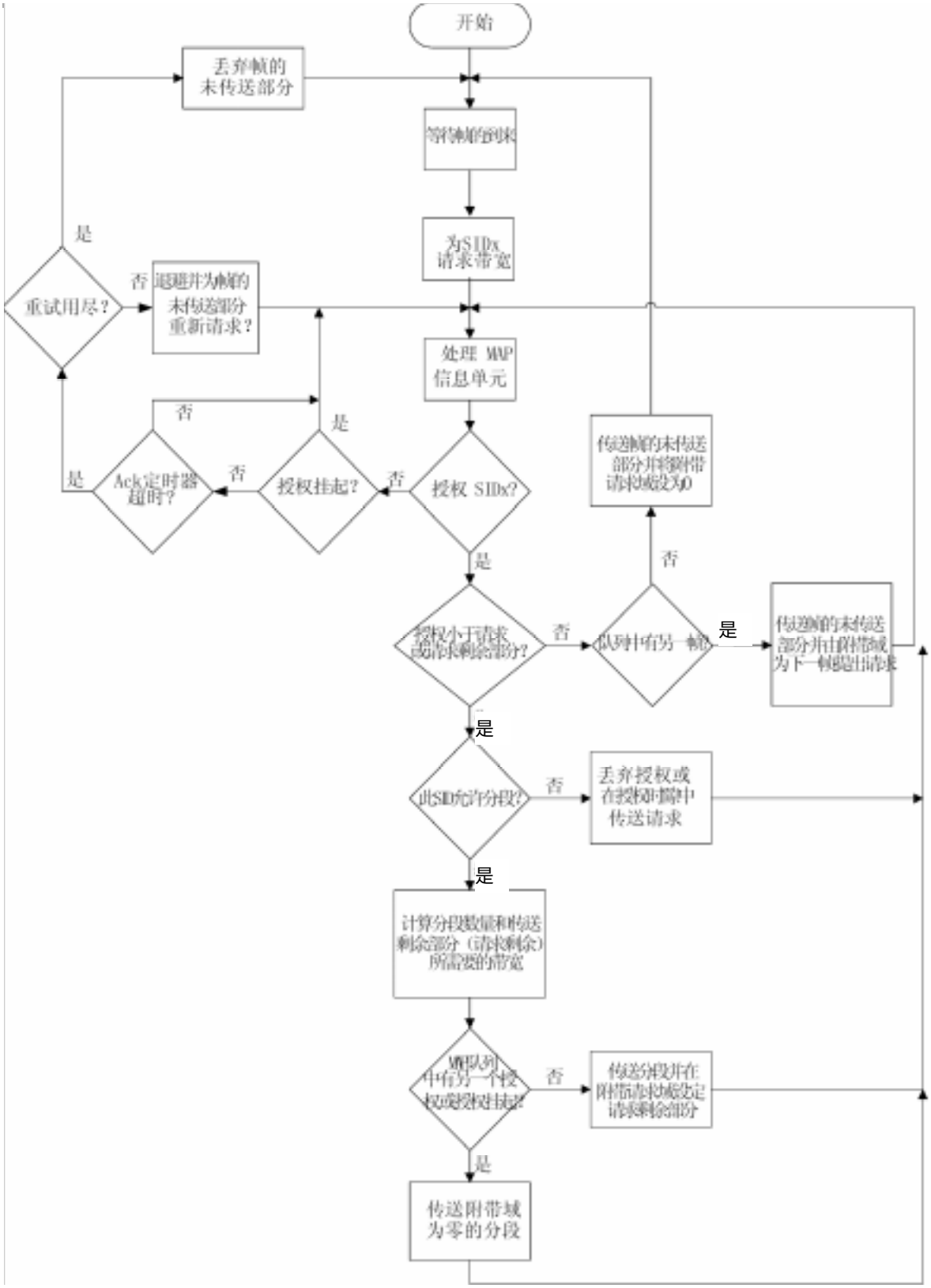


图73　CM 分段流程图

9.3.2　CMTS 分段支持

在CMTS中，处理分段的方法类似于处理普通包的方法，只是加密在分段包头之后立刻开始，而不是偏移12个字节。

CMTS有两种模式可以用来进行分段。多授权模式假定CMTS保留分段的状态。这种模式对于任何给定的SID，CMTS具有多个部分授权处于未完成状态；附带模式假定CMTS不保留任何分段状态，只能有一个分段授权处于未完成状态，因此CM把剩余的量插入分段包头的附带域。所使用的模式类型由CMTS决定。在所有的情况下，CM按一致的规则集来工作。

9.3.2.1 多授权模式

CMTS可以支持多授权模式来进行分段。

多授权模式允许CMTS把一个请求分成在单个的或者在后续的MAP中的两个或多个授权，并计算在剩余的部分授权中所需要的附加开销以满足该请求。在多授权模式中，如果CMTS不能在当前的MAP中给剩余部分授权，则它应在当前的MAP及所有后续的MAP中发送一个授权挂起（零长度的授权），直到它可以授权附加的带宽为止。如果在后续的MAP中没有授权或授权挂起，则CM应为剩余部分进行重新请求。重新请求的机制和正常的REQ没有在ACK时间之内接收到授权或授权挂起时所使用的机制一样。

如果CM接收到一个带有分段授权的授权挂起IE,它不应在该授权中所发送的分段扩展包头中加入附带请求。

CM错过一个授权并重新请求剩余部分的带宽时，CMTS应恢复且不丢失该帧。

由于微时隙到字节变换过程的不精确性，CMTS可能不能精确地计算分段开销所需的额外微时隙数。还可能因为CM已错过了带有部分授权的MAP，这样需要发送一个未传送分段请求而不是新的PDU，因此CMTS不能确定是否CM已在请求中计算了分段开销。CMTS应保证任何分段激活负载剩余部分至少比所需的微时隙数多一个微时隙，以包含分段（16字节）的开销加上传送一个最小长度分段的物理层开销。否则，将导致由于CM已经使用前一个部分授权传送了分段负载剩余部分，而使CMTS发布一个不需要的授权。这可能会使得CM由于不恰当地开始一个新的分段而失去与CMTS的同步。另外，CMTS需要处理如下情况，即对某些物理层参数组CM可以请求比短数据授权最大长度多一个的微时隙,但不是实际上需要的那么多时隙，这种情况发生在CM需要请求长度超过短数据授权限制的时候。CMTS需要一个策略，来确保在多授权模式中的分段请求不产生不必要的分段授权。

9.3.2.2 附带模式

CMTS 可以支持附带模式来进行分段。

如果由CMTS对某个SID发起的分段，没有在MAP中给予另一部分授权或授权挂起，则CM应自动地为剩余部分进行附带请求。CM 计算出在授权的带宽中能够传送一个帧的多大部分，并形成一个分段来传送它。CM使用分段扩展包头中的附带域来请求为传送该帧的剩余部分所需要的带宽。由于CMTS在第一个分段MAP中没有多个授权，CM应跟踪要发送的剩余部分。对于原始帧的剩余部分的请求长度，包括物理层开销和分段的开销，都将插入到该分段包头中的附带请求字节中去。

如果分段HCS是正确的，附带请求（如果存在的话）将传递到带宽分配模块，而分段则进入队列以便重新组装。一旦完整的MAC帧组装后，如果包HCS是正确的，则处理所有非加密的扩展包头，并将该包转发到适当的目的地。

9.3.3 分段举例

9.3.3.1 单个包的分段

如图73所示。这里假定一个给定的SID可以使用分段。

a) （请求状态）- CM 想要传送一个 1018 字节的包。CM 计算需要多少物理层开销（POH），并且申请适当数目的微时隙。CM 在争用区域提出一个请求。转向 b)；

b) （等待授权）- CM 监视 MAP，寻找一个对此 SID 的授权或授权挂起。如果在 CM 收到授权或授权挂起之前 CM 的 ACK 时间已经超时，则 CM 重试对该包的请求，直到重试的次数用完为止， 然后 CM 放弃该包，转向 c)；

c) （第一分段）- 在第二步放弃之前，CM 得到对此 SID 的一个授权，并且该授权少于请求的微时隙的数目。CM 使用规定的突发参数计算出在授权的微时隙数目中能够传送多少 MAC 信息。

在图 74 的例子中，第一个授权在减去 POH 之后能够容纳 900 个字节。由于分段开销（FRAG、HDR、FHCS 和 FCRC）为 16 个字节，所以在该分段中可以传送 884 个原始包的字节。CM 生成一个由 FRAG、HDR、FHCS、884 个字节的原始包和一个 FCRC 组成的分段。CM 使这个分段成为第一个分段，并准备发送该分段。转向 d)；

d) （第一分段，多授权模式）- CM 察看在队列中是否有对这个 SID 的其它的授权或授权挂起。如果有的话，CM 发送该分段，使 FRAG HDR 中的附带域设定为零，并等待后续的授权循环，转向 f)。如果没有任何授权或授权挂起，转向 e)；

e) （第一分段，附带模式）- 如果在该 MAP 中没有对 SID 其它的授权或授权挂起，则 CM 计算为了传送该分段包的剩余部分需要多少微时隙，其中包括分段开销和物理层开销，并把这个数目插入到 FRAG HDR 的附带域中。然后，CM 传送该分段，并启动其对此附带请求的 ACK 定时器。在图 74 的例子中，CM 发送一个能够容纳 POH 加上 150 字节（1018-884+16）的足够的微时隙。转向 f)；

f) （等待授权）- CM 现在等待对下一个分段的授权。如果在等待此授权的时候，CM 的 ACK 定时器超过其定时时间，CM 应当发送一个要求为传输该分段包的剩余部分所需的足够的微时隙的请求，包括分段开销和物理层开销。转向 g)；

g) （接受下一个分段授权）- 在放弃 f)之前，CM 得到对该 SID 的另一个授权。CM 将检查该授权的长度是否足够，以容纳该分段包的剩余部分，包括分段开销和物理层开销。如果授权的长度足够，则转向 j)。否则转向 h)；

h) （中间段，多授权模式）- 因为该包的剩余部分（加上开销）不能装入授权时隙中，CM 将计算该授权能够装下该包的多大部分。CM 将该包的这一部分封装为一个中间段。然后，CM 寻找给此 SID 的其它授权或在队列中的授权挂起。如果存在着两种情况之一的话，则 CM 发送该分段，将 FRAG HDR 中的附带域设定为零，并等待后续的授权循环，转向 f)。如果没有任何授权或授权挂起，转向 i)；

i) （中间段，附带模式）- CM 计算为了传送该分段包的剩余部分需要多少微时隙，其中包括分段开销和物理层开销，并把这个数目插入到 FRAG HDR 的附带域中。然后，CM 传送该分段，并启动其对此附带请求的 ACK 定时器。转向 j)；

j) （最后分段）- CM 将该包的剩余部分封装为一个最后分段。如果在队列中没有其它的包或者在队列中有对该 SID 的其它授权或授权挂起，则 CM 在 FRAG HDR 的 REQ 域中置零。如果队列中有另一个包，而没有授权或授权挂起，则 CM 计算发送下一个包所需要的微时隙数目，并把该数目放在 FRAG HDR 的 REQ 域中。然后 CM 发送该包。转向 k)。在图 74 的例子中，该授权足够容纳剩余的 150 个字节加上 POH；

k) （正常工作）- 然后 CM 回到等待授权和请求包的正常工作。如果在任何时候分段打开，并得到一个小于请求的授权，则分段过程按 b)重新开始。

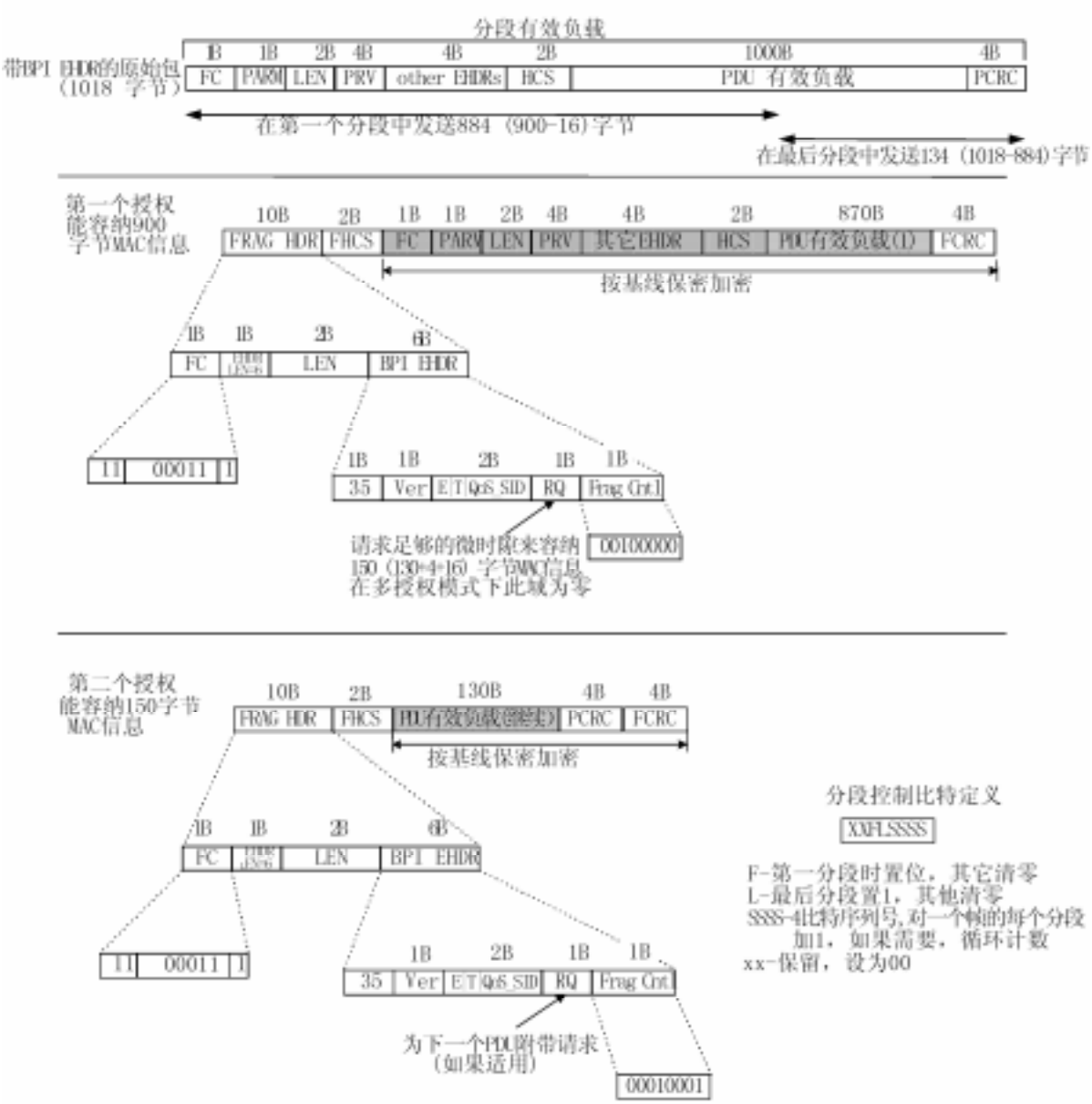


图74　单个包分段的例子

9.3.3.2　级联包的分段

CM产生了级联包以后，CM把级联包当作单个PDU处理。图75为一个级联的包分成3个分段的例子。在包分段时不考虑级联包中的包分界问题。

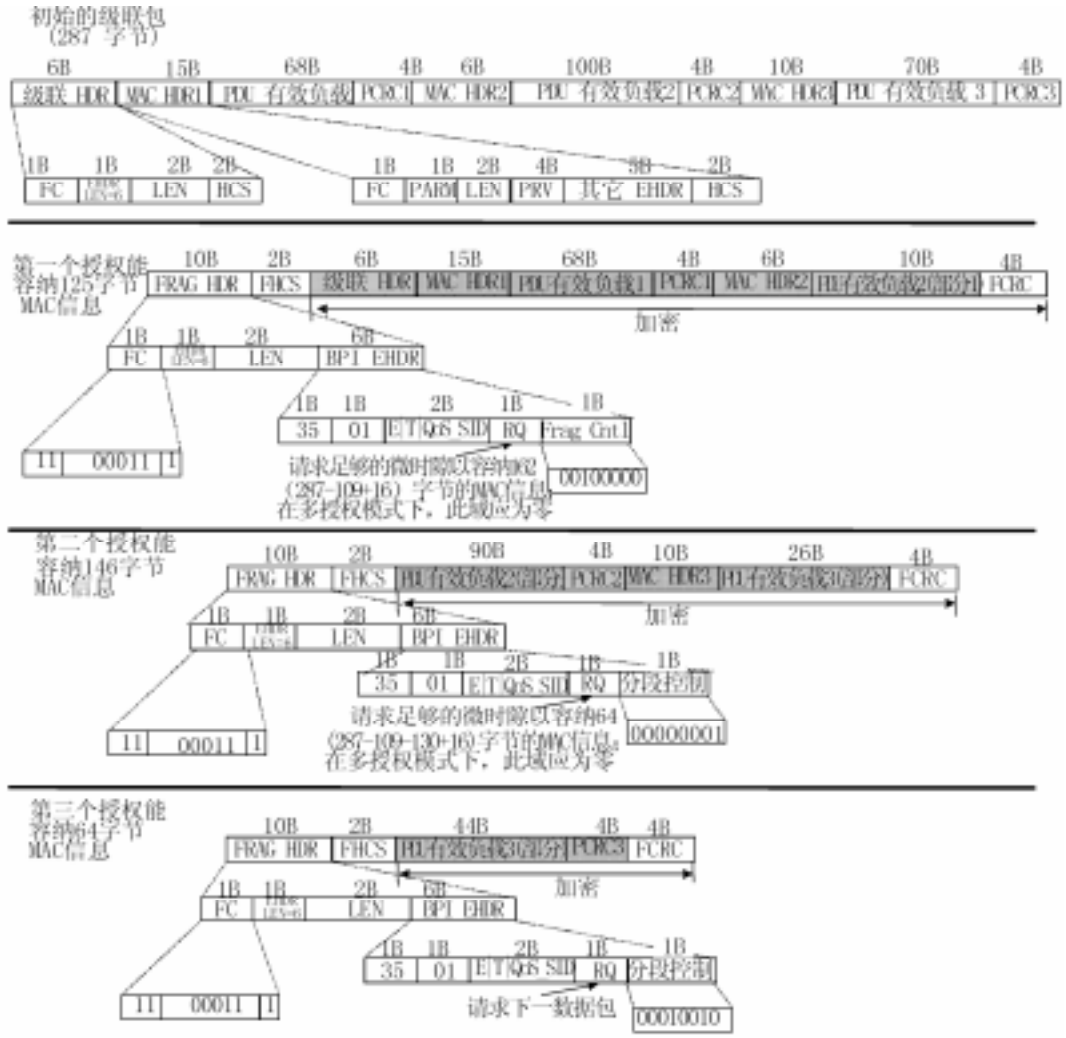


图75　级联包分段的例子

9.4　有效负载包头抑制

本条描述有效负载包头抑制的原理，并说明初始化、操作和结束的信令。最后，给出特定的上行和下行的例子。相关定义见表45。

表45　有效负载包头抑制的定义

PHS	有效负载包头抑制	在发送方抑制初始字节串并在接收时恢复该字节串
PHSR	有效负载包头抑制规则	应用于特定PHS索引的一组TLV
PHSF	有效负载包头抑制域	代表一个PDU包头部分的字节串，其中的一个或多个字节将被抑制掉（即包括抑制和未抑制字节的瞬态未压缩PDU包头）
PHSI	有效负载包头抑制索引	对应抑制字节串的一个8比特值
PHSM	有效负载包头抑制掩码	表明PHSF中哪些字节抑制哪些字节不抑制的比特掩码
PHSS	有效负载包头抑制长度	抑制域的字节长度。此值等于PHSF中的字节数也等于PHSM中的激活比特数。
PHSV	有效负载包头抑制验证	通知发送实体验证要抑制的所有字节的标志

9.4.1　概述

在有效负载包头抑制的情况下，发送实体将扩展包头域后面的有效负载包头的重复部分抑制掉，而接收实体又将其恢复。在上行时，发送实体是CM，接收实体是CMTS。在下行时，发送实体是CMTS，接收

实体是CM。MAC扩展包头包括一个有效负载包头抑制索引（PHSI），此索引对应着有效负载包头抑制域（PHSF）。

虽然PHS可以用于任何业务流类型，但是其初始设计目的是用于主动授权业务（UGS）调度类型。UGS以固定长度的包工作最有效。对于UGS， PHS工作得很好，这是因为与IP数据使用的其它包头抑制方案不同，PHS总是在每个包中抑制相同数目的字节。PHS将总是产生固定长度的压缩包包头。

发送实体使用分类器把包映射到一个业务流中。分类器唯一地将包映射到其相关的有效负载包头抑制规则上。接收实体使用SID和PHSI来恢复PHSR。

一旦已知规则的PHSF和PHSS域，规则就被看做“完全定义”且没有任何域能被变更。如果对包分类到流要求修改PHS操作，则旧的规则应从业务流中删除，而新的规则应被加入。

当删除一个分类器时，任何相关的PHS规则也应被删除。

PHS有一个PHSV可选项，以选择在抑制有效负载前校验或不校验该有效负载。PHS还有一个PHSM可选项，用来选择不需抑制的字节。这是为了用来发送会变更的字节，如IP序列号，而仍然抑制那些不变更的字节。

PHS规则对于所有的调度业务类型是一致的。带宽的请求和授权是在考虑了抑制的作用以后确定的。对于主动授权业务，其授权长度是按主动授权长度TLV来选择的。抑制了包头的包可能等于或小于该授权的长度。

CMTS应如指定所有SID数值那样指定所有的PHSI值。发送实体或接收实体都可以规定PHSF和PHSS。这种预置允许预配置包头或上层信令协议以建立缓存实体，该做法超出了本部分范围。PHS是针对单播业务的，而不是为组播业务定义的。

高层业务实体负责产生唯一识别业务流内被抑制的包头的PHS规则，并保证被抑制的字节串在激活业务流期间的各个包之间的一致性。

9.4.2 应用实例

a) 上行业务流的分类器通过规定 UDP 的协议类型、IP SA、 IP DA、UDP 源端口、UDP 目的端口、业务流参考和 42 字节的 PHS 长度来唯一地定义一个 IP 电话（VoIP）流。PHS 规则通过提供标识 VoIP 媒体流的 PHSI 对应此分类器。对于上行情况，需要校验和抑制 42 字节的有效负载包头，并对该媒质流中的每个包添加一个包含 PHSI 的 2 个字节的扩展包头；

b) 标识一个业务流的包分类器中 90%的包符合该 PHSR。验证功能打开。这可以应用于进行如此频繁地压缩复位而且包头变化的包压缩情况。在这个例子中，调度算法容许可变的带宽，并且只有 90%的包的包头可能被抑制。因为 PHSI 扩展包头表明所做的选择，所以在接收实体方简单地 SID/PHSI 查找就能产生正确的结果；

c) 上行业务流的分类器由发送实体通过规定 IP 的以太类型、SFID、14 个字节的 PHSS 和无校验来识别所有的 IP 包。在这个例子中，CMTS 已经决定该包的路由，即使知道某些部分如源地址或目的地址可能会变化，它也不需要 14 字节的以太包头。CM 从每个上行帧（以太包头）中删除 14 个字节，不校验其内容并将该帧转发到业务流。

9.4.3 操作

为了阐明操作包流，本条介绍一种可能的实现。只要遵循本条中规定的协议，CM和CMTS可以自由地实现有效负载包头抑制。图76说明了下列步骤。

一个包提交给CM MAC业务层。CM应用其分类器规则列表。匹配的结果是产生一个上行业务流、SID和一个PHS规则。该PHS规则提供PHSF、PHSI、PHSM、PHSS和PHSV。如果PHSV已设定为0或者不存在，则CM将该包包头中的字节与按照PHSM的指示将要抑制的PHSF中的字节进行比较。如果二者相符合，CM将抑制上行抑制域中除去被PHSM掩码的字节之外的所有字节。然后CM将把PHSI插入到该业务流EH单元的PHS-Parm域中，并且将该包在上行业务流中排队。

当CMTS接收该包时，CMTS将使用内部的方法或从其它的扩展包头单元，如BPI扩展包头，来确定相应的SID。CMTS使用该SID和PHSI来查找PHSF、PHSM和PHSS。CMTS重新组装该包并且按照正常的包的处理

方法处理。重新组装好的包将包含来自PHSF的字节。如果打开校验功能，则PHSF字节将等于初始的包头字节。如果没有打开校验功能，则不能保证PHSF字节会符合初始的包头字节。

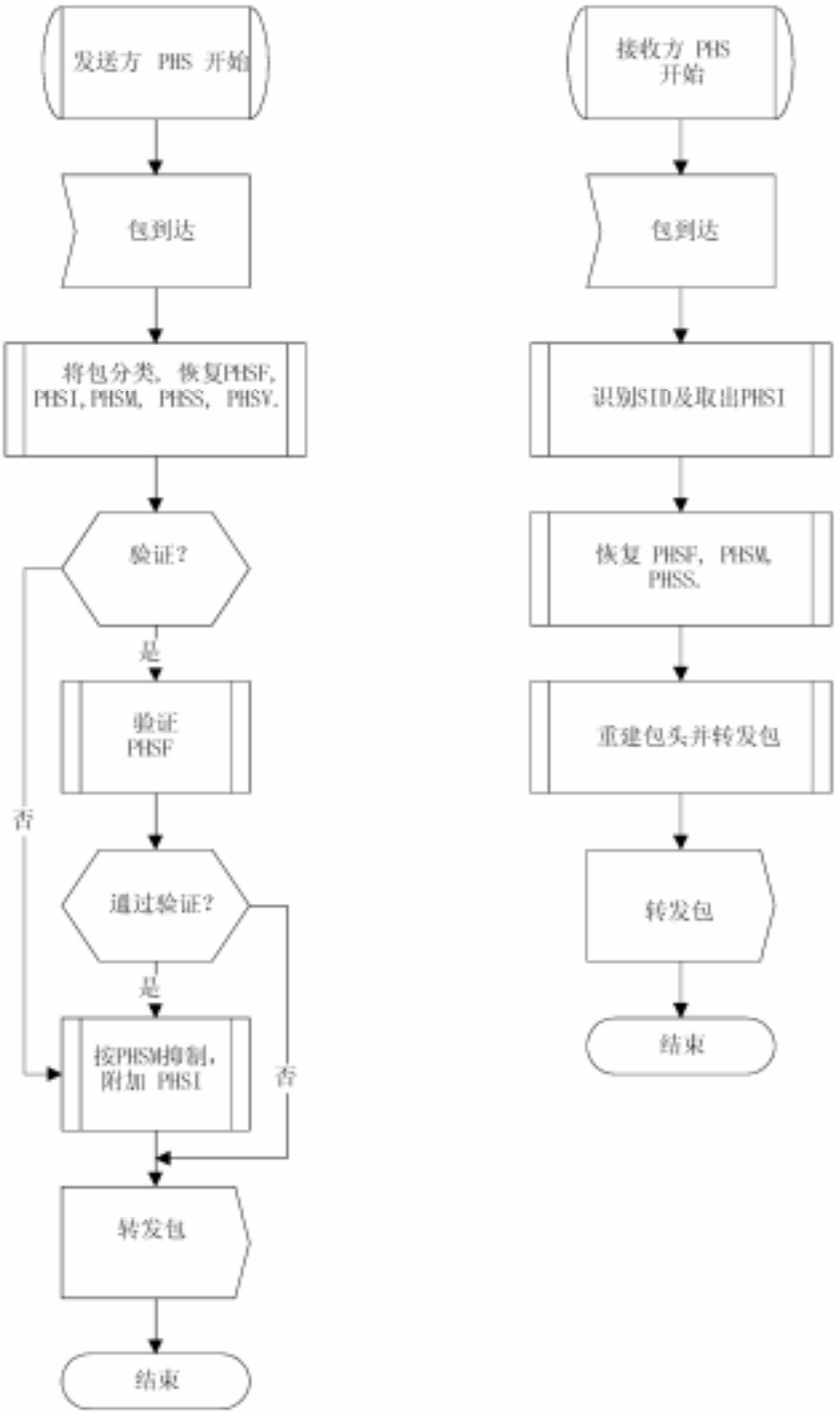


图76　有效负载包头抑制操作

在下行中有类似的操作。CMTS应使用其分类器的列表。符合分类器的结果将产生一个下行业务流和一个PHS规则。该PHS规则提供PHSF、PHSI、PHSM、PHSS和PHSV。如果PHSV置零或不存在，则CMTS将按照PHSF来验证该包中下行抑制域。如果二者相符合，CMTS将抑制下行抑制域中除被PHSM掩码的字节之外的所有字节。然后CMTS将把PHSI插入到该业务流EH单元的PHS-Parm域中，并且将该包在下行业务流中排队。

CM将根据以太网目的地址过滤接收该包。然后CM使用PHSI查找PHSF、PHSM和PHSS。CM重新组装该包并且按照正常的包的处理方法处理。

图77说明当使用PHS掩码时包的抑制和恢复，掩码只抑制那些不变的字节。PHSF和PHSS跨越整个抑制域，包括抑制的和不抑制的字节。

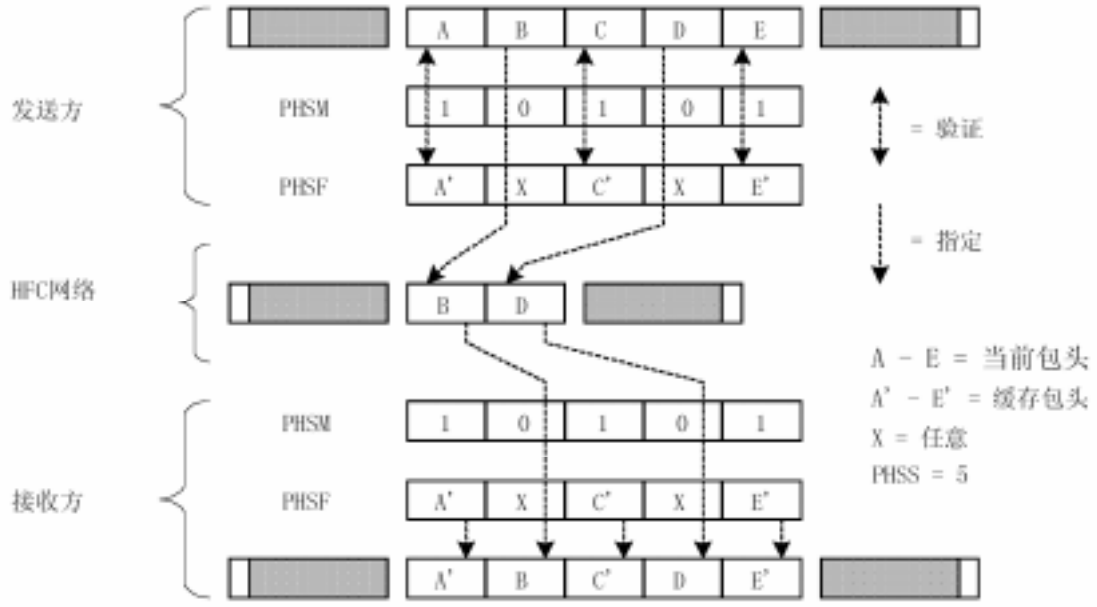


图77　带掩码的有效负载包头抑制

9.4.4　信令

有效负载包头抑制需要建立三个对象：

- 业务流；
- 分类器；
- 有效负载包头抑制规则。

这三个对象可以在单独的消息流中建立，也可以同时建立。

PHS规则由注册、DSA或DSC消息建立。当PHS规则建立时，CM应定义PHSI。PHS规则由DSC或DSD消息删除。CM或CMTS可以定义PHSS和PHSF。

图78所示为PHS规则建立的两种方法。

在业务流建立时，可以部分地规定PHS规则（特别是规则的大小）。

例如，有可能在一个业务流第一次被预置的时候，其将要抑制的包头域长度是已知的。但是该域的某些值（例如IP地址、UDP端口号等）可能未知，并将在后续的DSC中作为该业务流激活的一部分来提供（使用“ 设置PHS规则 ”的 DSC动作）。

当PHSF和PHSS域值都未知时，只能部分定义PHS规则。一旦PHSF和PHSS两者都已知，规则被看作完全定义，且不能通过DSC信令修改。PHSV和PHSM域有缺省值，因此不需要完全定义一个PHS规则。如果当规则变成完全定义时PHSV和PHSM未知，则使用其缺省值，且不能通过DSC信令修改。

PHS规则的每一步定义，无论注册请求、DSA或DSC，都应包含SFID（或参考）、分类器ID（或参考）来唯一地识别被定义的PHS规则。在上行包传送期间,一个PHS索引和SFID对用来唯一地识别其PHS规则。PHS索引能用来唯一地识别使用在下行包传送中的PHS规则。

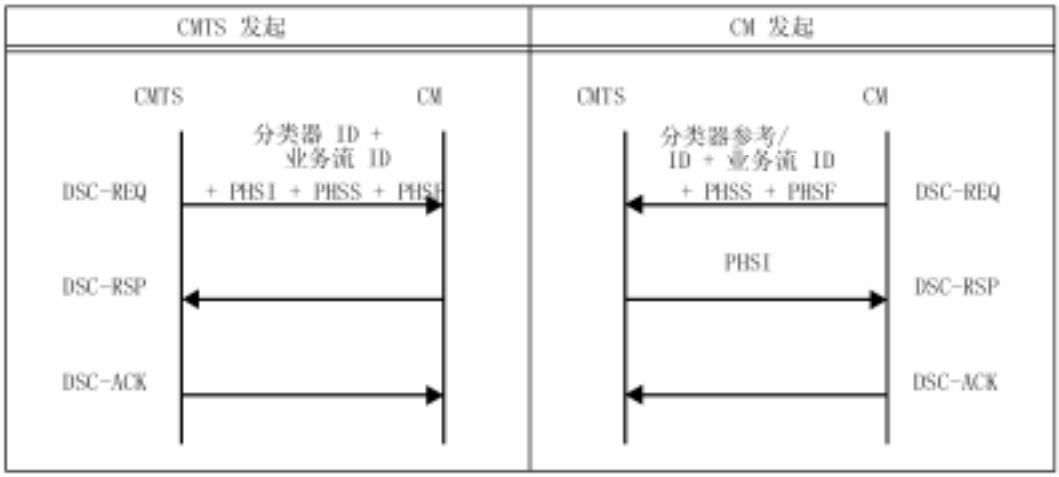


图78　有效负载包头抑制信令举例

9.4.5　有效负载包头抑制举例

9.4.5.1　上行举例

建立一个业务类别名称为“G711-US-UGS-HS-42”的业务类别，其目的是以主动授权业务在上行通道提供ITU-T G.711 VoIP通讯业务。在向该流添加包括42字节PHSS值的分类器，它明确地表示在该流中所有包的MAC扩展包头后面的42个字节都应进行验证、抑制和恢复。本例中运用的配置业务类别的方法不抑制任何不能正确验证的包的包头，因而又因包长超过主动授权长度而将其丢弃（见C.2.2.6.3）。

图79表示在上行中使用或者不使用有效负载包头抑制包的封装情况。其中使用一个不带IPsec的RTP IP电话有效负载作为特定的例子来说明其有效性。

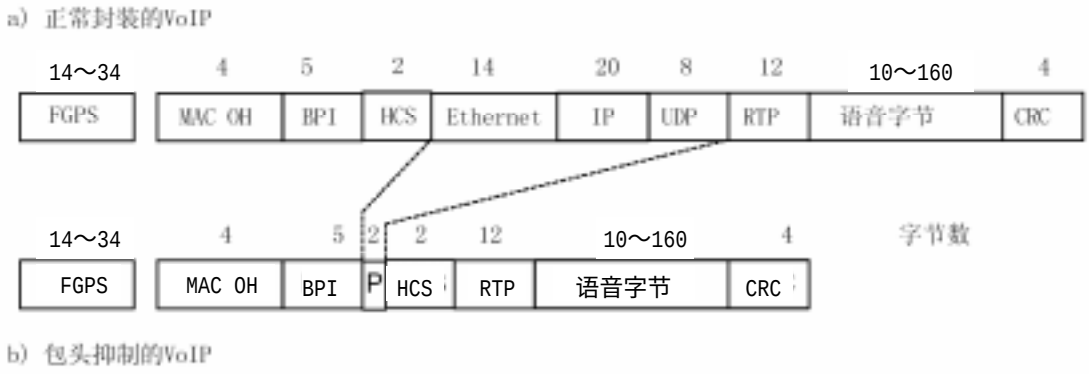


图79　上行有效负载包头抑制举例

图79a)表示在上行信道上传送的一个普通的RTP包。其帧的开始部分表示物理层开销（FGPS），包括FEC、保护时间、前同步码和填充字节。填充字节出现在将数据块映射到微时隙中时的最后码字中。紧接着是MAC层开销，包括6个字节的MAC包头（带5个字节的BPI扩展包头）、14个字节的以太包头和4个字节的以太CRC码。VoIP有效负载使用20个字节的IP包头、8个字节的UDP包头和12个字节的RTP包头。语音有效负载是可变的，并且决定于采样时间和使用的压缩算法。

图79b)表示的是当有效负载包头抑制打开时相同的有效负载的情况。在上行中，有效负载包头抑制开始于MAC包头校验和之后的第1个字节。14个字节的以太包头、20个字的IP包头、8个字节的UDP包头都已被抑制，并添加了2个字节的PHS扩展包头单元，共减少40个字节。在此例中，这些域在各个包之间是不变的，如果不被抑制，这些字节将是冗余的。

9.4.5.2　下行举例

建立一个业务类别名称为“G711-DS-HS-30”的业务分类，其目的是在下行提供ITU-T G.711 VoIP通信业务。在向该业务流添加包括30字节PHSS值的分类器时，它明确地表示对所有包的30个字节的有效负载包头应加以处理，以便按照PHSM来抑制和恢复。 没有正确校验的任何包的包头将不被抑制，但是将按照对于该业务流的流量整形规则来传送。

图80表示在下行中使用和不使用有效负载包头抑制的包的封装情况。其中使用一个不带IPsec的RTP IP电话有效负载作为特定的例子来说明其有效性。

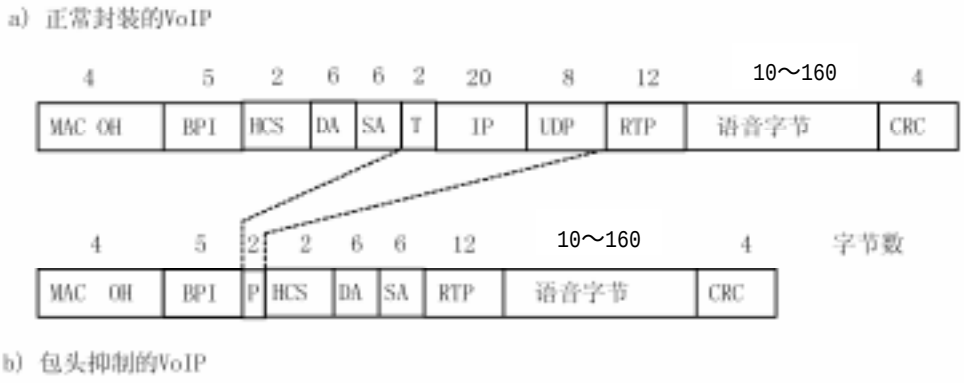


图80　下行有效负载包头抑制举例

图80a)表示在下行信道上传送的一个普通的RTP包。第2层开销包括6个字节的MAC包头（带5个字节的BPI扩展包头）、14个字节的以太包头（6个字节的目的地址、6个字节的源地址和2个字节的以太类型域）和4个字节的以太CRC码。第3层VoIP有效负载使用20个字节的IP包头、8个字节的UDP包头和12个字节的RTP包头。语音有效负载是可变的，并且决定于采样时间和使用的压缩算法。

图80b)表示的是当有效负载包头抑制打开时相同的有效负载的情况。在下行中，有效负载包头抑制在MAC包头校验和之后的第13个字节开始。这样保留了以太目的地址和源地址，以便CM过滤和接收包。以太包头剩余的2个字节、20个字节的IP包头、8个字节的UDP包头都已被抑制，并添加了2个字节的PHS扩展包头单元，共减少28个字节。在此例中，这些域在各个包之间是不变的，如果不压缩，这些字节将是冗余的。

10　CM—CMTS 交互作用

本章阐述对CM和CMTS之间交互作用的关键要求。关键要求可分为5种基本类别：初始化、鉴权、配置、授权和信令。

10.1　CMTS 初始化

CMTS的初始化机制（本地终端、文件下载、SNMP等）应符合下列系统互通性准则(见DOCSIS 5)：

- CMTS 应能够使用保存在非易失性存储器中的配置数据进行重新启动，并且在独立模式下运行；
- 如果从非易失性存储器中或者通过其它机制都得不到有效的参数时，CMTS 不应产生任何下行消息（包括 SYNC）。这将会阻止 CM 进行传送；
- CMTS 应向各个 CM 提供第 7 章中所规定的上行通道信息。

10.2　CM 初始化

CM的初始化过程如图81所示。该图为CM初始化步骤的总流程。图中不包括各种出错路径，只是简单地提供过程的概貌。各部分（包括出错路径）的更详细的有限状态机示意图在以后的各个图中示出。超时数值在附录B中规定。

CM初始化和CM重新初始化其MAC的过程可分为如下的各个阶段：

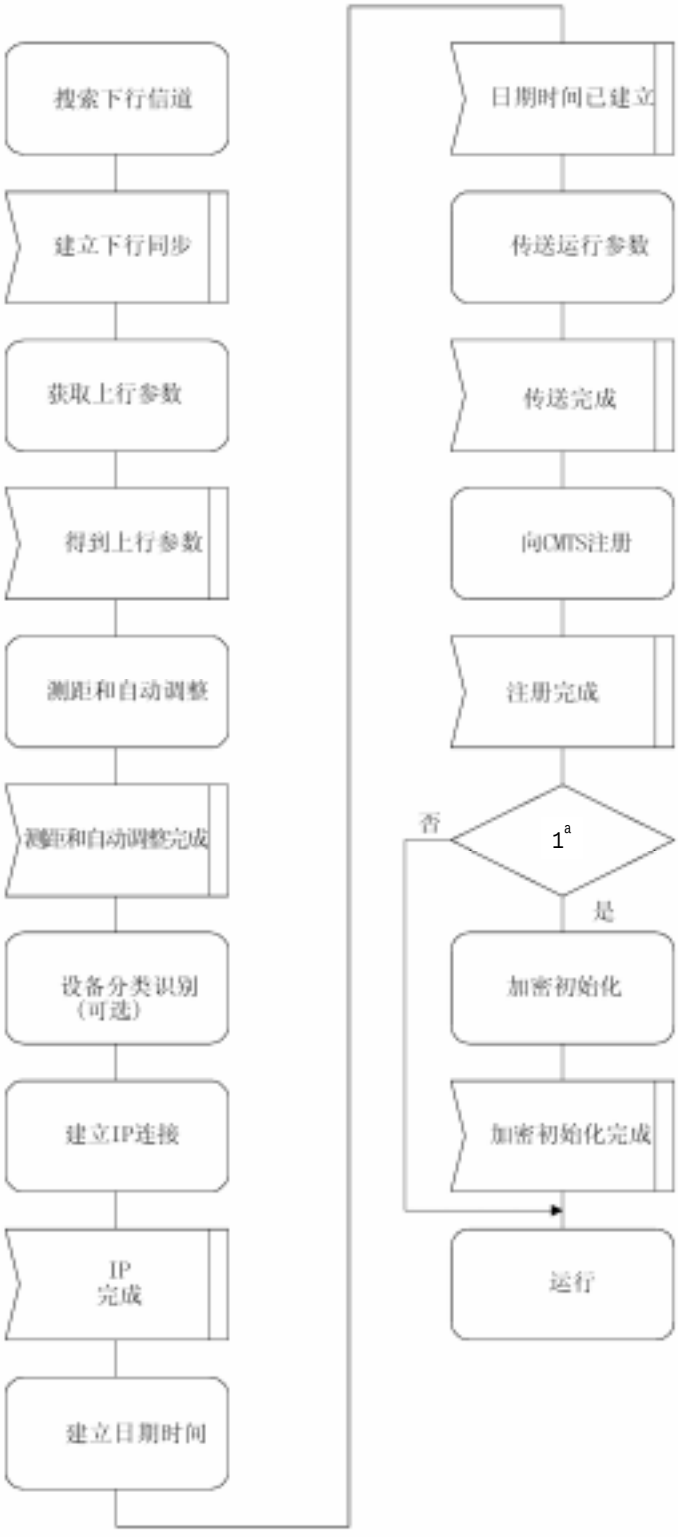
- 搜索并同步到下行信道；
- 获取上行信道参数；

- 进行测距和自动调整；
- 设备分类识别(可选)；
- 建立 IP 连接；
- 建立日期时间；
- 传送操作参数；
- 注册。

每个CM在制造厂家发货时都包含如下信息：

唯一的IEEE 802 48比特的MAC地址，该地址是在制造的过程中指定的。此地址用于在初始化期间各预置服务器识别CM。

下面各图中所使用SDL（规范和描述语言）符号在图82中示出（见ITU-T Z.100）。



a 1为加密使能，本部分中此值恒为0。

图81　CM初始化过程

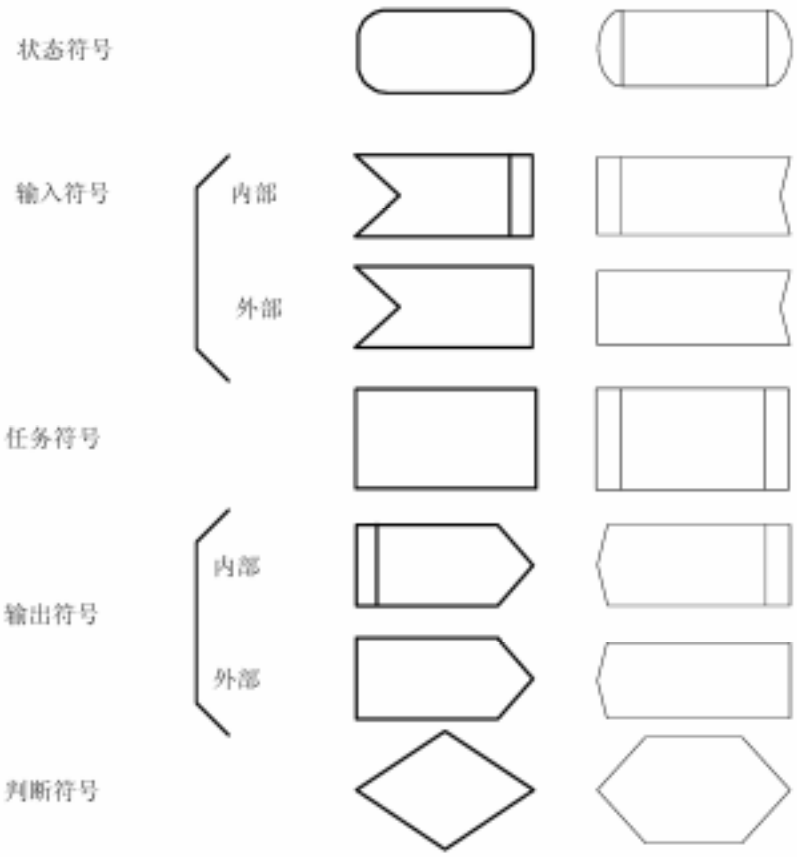


图82　SDL 符号

10.2.1　搜索并同步到下行信道

在初始化或“ 重新初始化MAC ”操作中，CM应获取一个下行信道。CM应具有非易失性存储器，以贮存上一次的工作参数。CM应首先尝试重新获取上次使用的下行信道。如果不成功，它就应开始连续搜索下行工作频带中的各个8MHz的信道，直至找到一个有效的下行信号为止。

当CM已完成下列各步骤时，就可以认为下行信号是有效的：

- QAM 同步；
- FEC 同步；
- MPEG 同步；
- 获取 SYNC 消息。

搜索时给用户一个指示，以表明CM正在进行此项工作。

为了支持冗余的CMTS体系，当一个CM检测到的下行信道无效时（例如，无法满足以上四个条件），CM不应立即执行重新初始化MAC操作。CM应试图重新在当前下行信道上建立同步（见10.5），直到10.3.1的图97中定义的周期测距在T4超时或16次T3超时后启动“ 重新初始化MAC ”操作。图97描述了CM应遵守的标准操作流程。

10.2.2　获取上行参数

见图83。同步后CM应等待来自CMTS的UCD，从中获得上行参数。CMTS周期性地用MAC广播地址发送所有可用的上行信道的UCD。CM应通过信道描述符参数来确定它是否能够使用此上行信道。

CM应收集信道ID域不相同的所有UCD，来建立一组可用的信道ID。如果在超时期间之后仍然找不到可用的上行信道，则CM应继续搜索以便寻找另一个下行信道。

CM应从信道描述符参数来确定它是否能够使用该上行信道。如果该信道不合适，则CM应尝试下一个信道ID，直到它找到一个可用的信道为止。如果这个信道是合适的，则CM应从其UCD中提取出该上行信

道的参数。然后等待下一个SYNC消息，并从该信息中提取出上行微时隙的时戳。随后CM应等待该选用信道的带宽分配MAP。于是CM即可按照MAC运行和带宽分配机制进行上行传送。

注： 还有另一种情况，由于SYNC应用于所有的上行信道，因此CM可能已经从前一个SYNC中获得了时间参考。此时，则CM就不需要等待新的SYNC。

CM应根据图86至少进行一次初始测距。如果初始测距不成功，则要选择下一个信道ID，并且从解析UCD重新开始上述过程。当没有更多信道ID再试时，CM应继续搜索以寻找另一个下行信道。

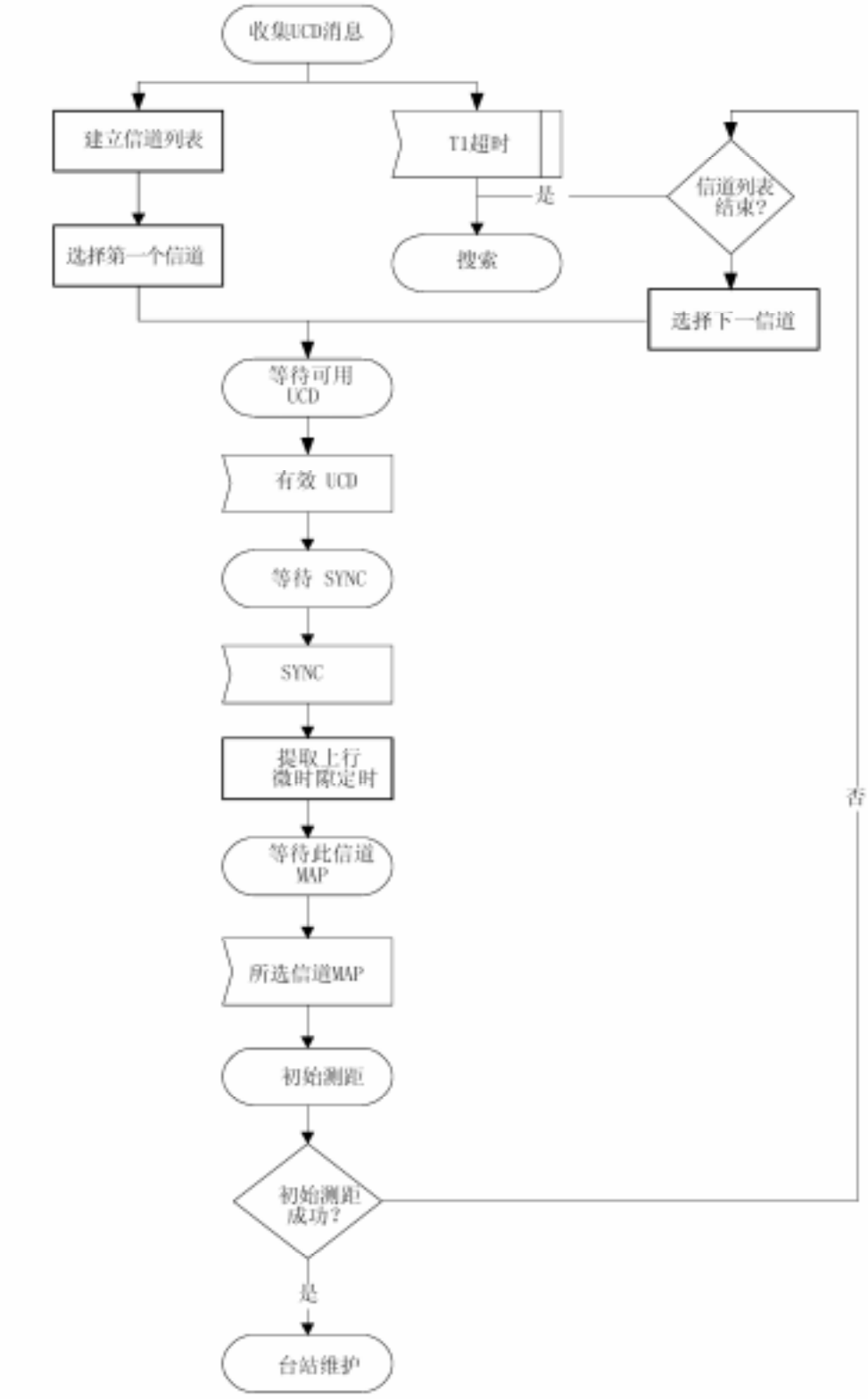


图83　获得上行参数

10.2.3　在搜索和获取上行参数期间的消息流

CMTS应在下行信道方向、周期性地、在附录B规定的范围内，产生SYNC和UCD消息。这些消息发送到所有的CM。见图84。

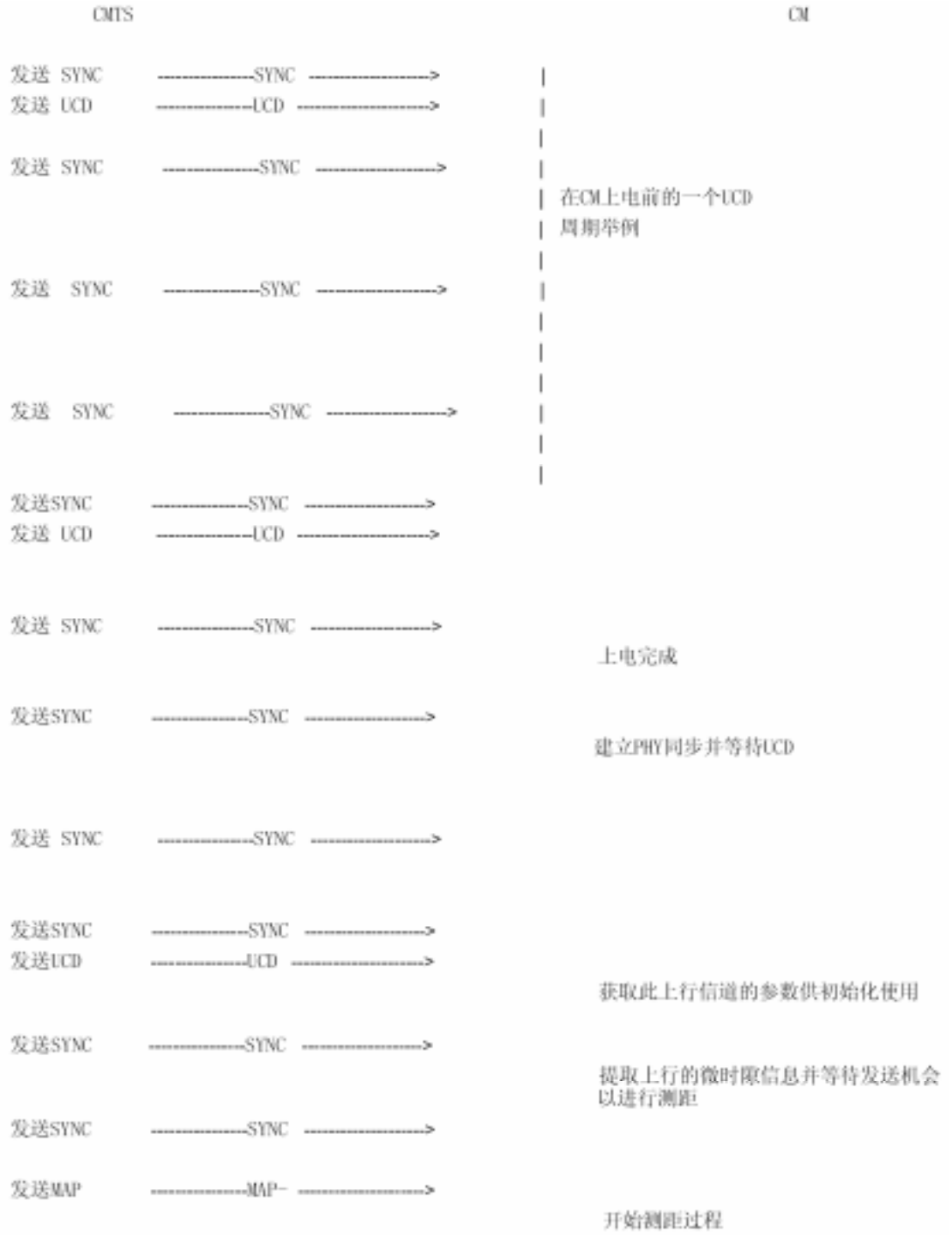


图84　在搜索和获取上行参数期间的消息流

10.2.4　测距和自动调整

在第7章中规定了测距和调整的全部过程。下面各消息顺序图和有限状态机规定了CM和CMTS应遵循的测距和调整过程，见图85至图88。

注： 各MAP传输按第7章所述。

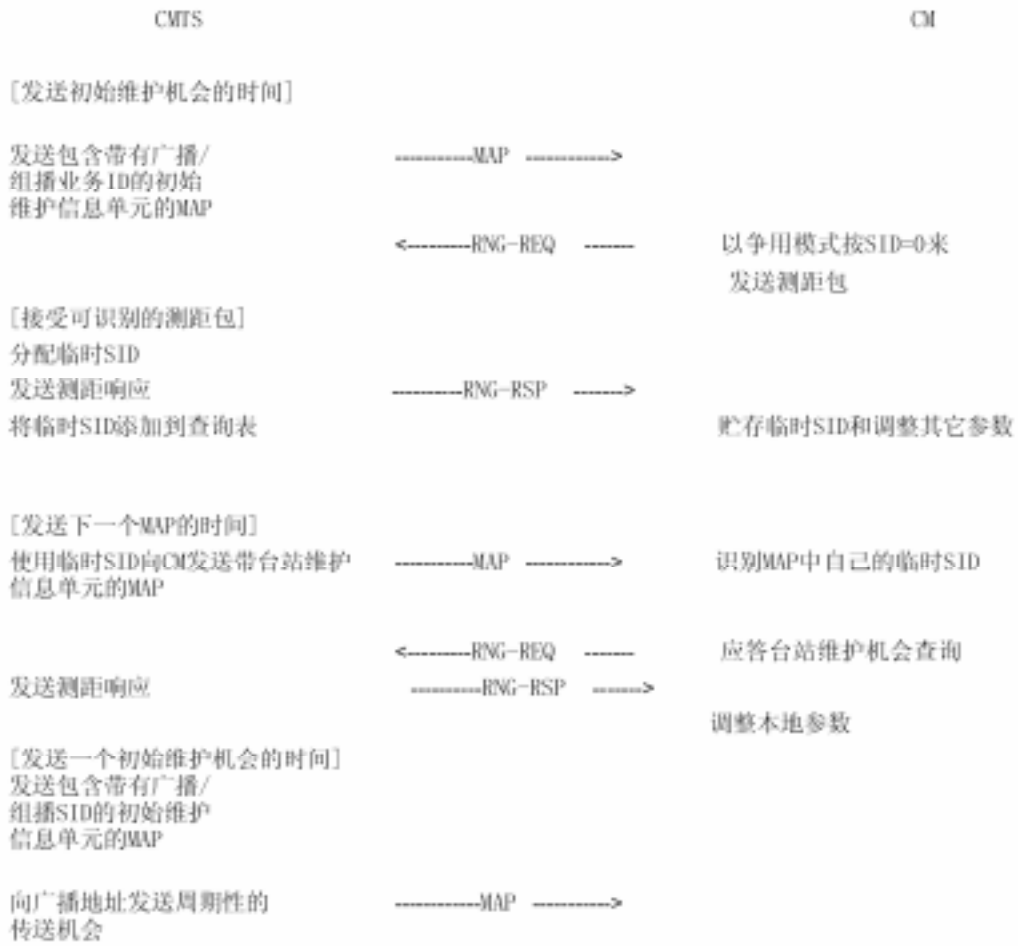
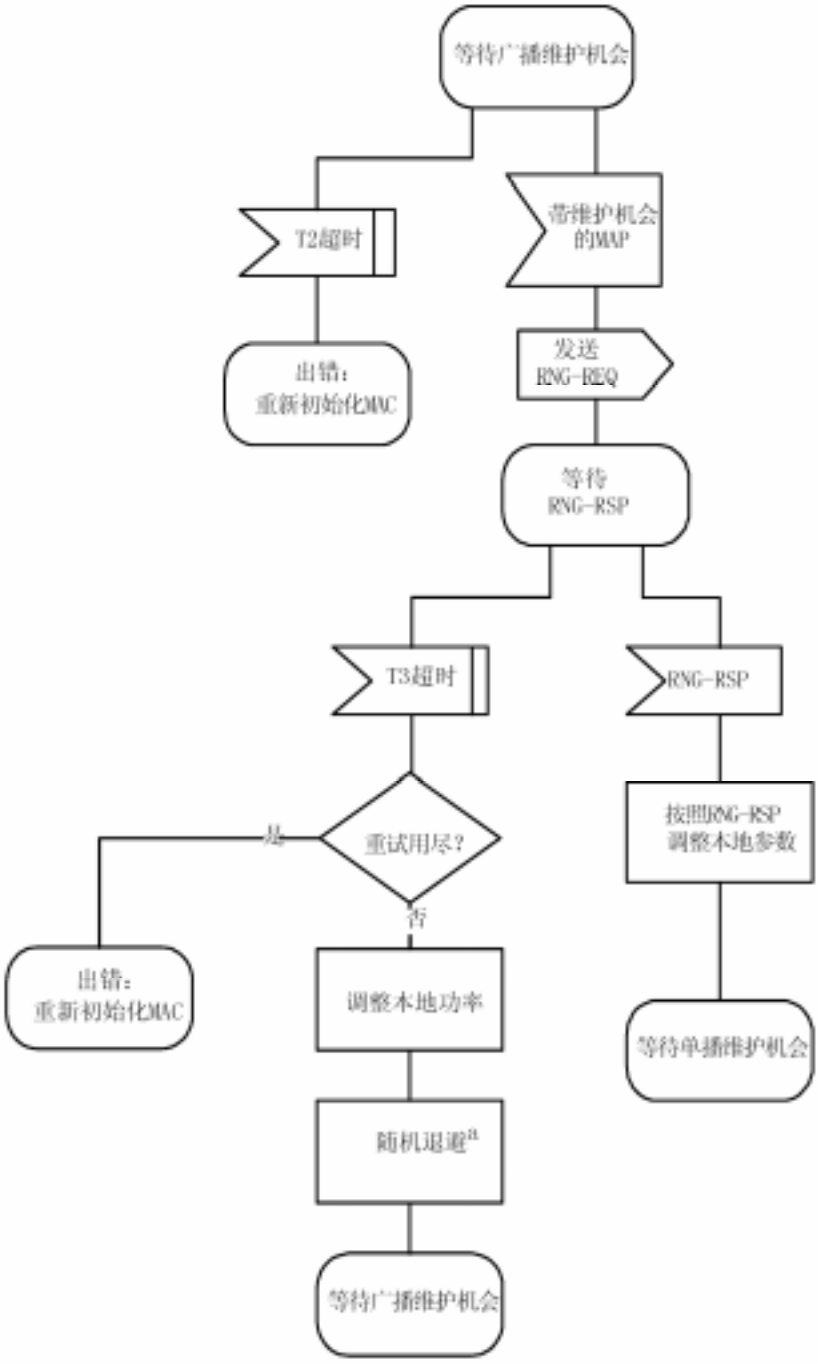


图85　测距和调整过程

注： CMTS在向CM发送特定的测距机会之前，应让CM有足够的时间处理完前面的RNG-RSP（即修改发射机的参数）。在附录B中此时间定义为CM测距响应时间。

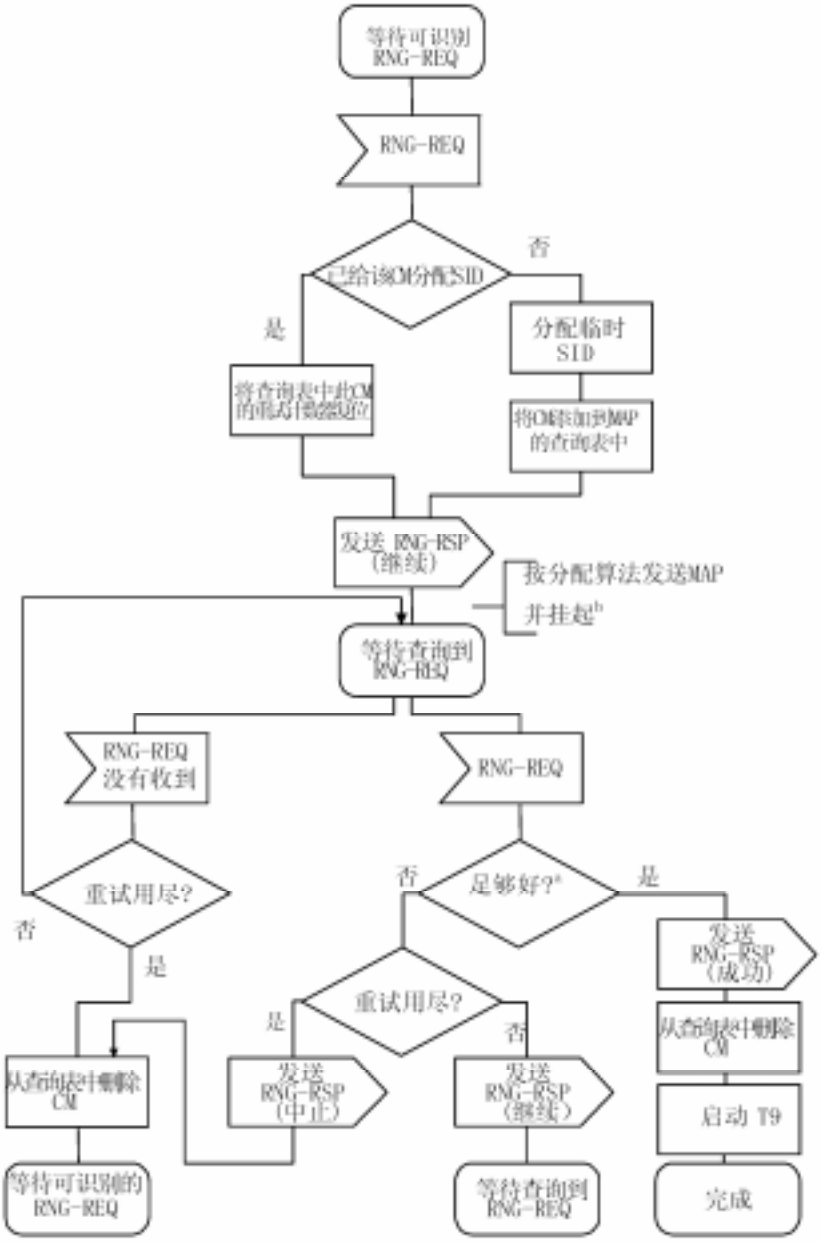


a 由于多个 CM 的测距请求相互碰撞，可能发生 T3 超时情况。为了避免这些 CM 陷入死循环，需要一种随机的退避机制。这就是 MAP 中规定的测距窗口上的退避时间。T3 超市时间也可能发生在多信道操作中。在有多个上行信道的系统中，CM 在移向下一个可用下行信道之前，应在每个合适的上行信道上尝试进行初始测距。

图86　初始测距-CM

a 测距请求在 CMTS 的容限范围之内。

图87　初始测距-CM（续）



a 指测距是在 CMTS 的容限范围内。

b RNG-REQ pending－till-complete（测距请求挂起-直到-完成）为非零值时，CMTS应推迟台站维护机会，需要进行该维护（例如要调整CM的功率电平）除外。如果在RNG-REQ pending－till-complete到期之前已经提供了这种机会，则接收RNG-RSP之后的“good enough（足够好）”测试不能判断CM的传输均衡。

图88　初始测距-CMTS

测距参数的调整

作为收到（或未收到）RNG-RSP（测距响应）的结果，CM本地参数（如发送功率）调整的实现受到下列的限制（见7.3.6）：

- 所有的参数在所有时间内都应在认可的范围内；
- 功率调整应从最小值开始，如果在非易失性存储器中有一个有效功率可用，则用该有效功率作为开始点；
- 功率调整应能够根据 RNG-RSP 消息中规定的量减小或增大；
- 在初始化时，如果功率已增大到其最大值（无来自 CMTS 的响应），则功率应回退到最小值；

- 对于多信道支持情况，CM 应在转向下一个可用下行信道之前对每一个合适的上行信道尝试初始测距；
- 对于多信道支持的情况,CM 应使用测距响应范围内的上行信道 ID,规定见 7.3.6 和附录 G。

10.2.5 设备类别识别

在完成测距之后和建立IP连接之前，为了预置，CM可以向CMTS标识它自己。参见图89。

图89 设备类别识别

如果实现设备类别识别，类似于TFTP， CM应使用基于二进制幂退避的设备类别识别的超时机制，见10.2.8。

10.2.6 建立 IP 连接

CM应调用DHCP机制（参见RFC-2131）以获得一个IP地址及为建立IP连接所需要的其它参数（见附录D）。DHCP响应应包括文件名称，该文件包含各种配置参数。见图90。

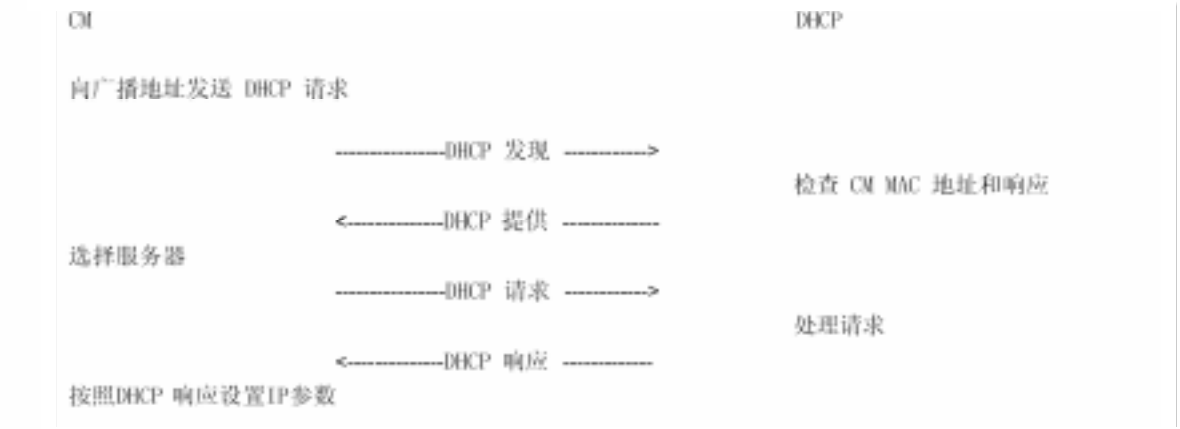


图90 建立 IP 连接

10.2.7 建立日期时间

CM和CMTS需要有当前的日期和时间，当前的日期时间是为了供带时戳记录的事件使用。而这种带时戳记录的事件可以由管理系统来检索。这种日期时间不需要鉴别，且只需精确到秒。

获取日期时间的协议在RFC-868中规定，见图91。请求和响应应使用UDP来传送。从服务器（UTC）得到的时间与从DHCP响应得到的时差计算出本地时间。

图91　建立日期时间

DHCP服务器可以为CM提供多个日期时间服务器IP地址。CM应尝试DHCP所提供的所有日期时间服务器，直到本地时间建立为止。

获取日期时间对于成功的注册并不是强制的，但对于该操作是必需的。如果CM不能在注册之前建立日期时间，则它应记录这次失败，并向管理设备发出告警，然后继续进行操作状态并周期性地重试。

对于日期时间请求的超时时间与实现有关。对于每个服务器，某个CM在任何5min的时段内不应发出超过3个日期时间请求。在最少情况下，CM应对每个指定的服务器每5分钟时段至少发出1个日期时间请求，直到建立本地时间。

10.2.8　传递工作参数

在DHCP成功以后，CM应使用TFTP下载参数文件，如图92所示。TFTP配置参数服务器由DHCP响应的“siaddr”域规定。CM对于TFTP应使用一种基于二进制幂退避的适当的超时机制，参见RFC 1123和RFC 2349。

DHCP响应中所需要的各参数域以及配置文件的格式和内容应如附录D所规定，这些域是互操作性的最低限度要求。

如果CM下载的配置文件中指定的上行信道和/或下行频率和CM正在使用的不相同，则CM不应向CMTS发送注册请求。CM应按照7.3.6.3的规定使用所配置的上行信道和/或下行频率重新进行初始测距。

10.2.9　注册

CM一旦经过初始化、配置以后，应得到授权才可将流量转发到网络上。通过注册，CM被授权向网络中转发通信包。为了向CMTS注册，作为注册请求的一部分，CM应向CMTS转发它所配置的业务类别和配置文件中的任何其它工作参数（见7.3.7）。CM应遵循的步骤如图92所示。

下载到CM的配置参数应包含一个网络接入控制对象（见C.1.1.3）。如果该对象设置为“不转发”，CM不应将数据从CPE转发到网络，然而CM还应响应网络管理请求。这就使得CM配置成一种可管理但不转发数据的模式。如果配置文件缺少一个网络接入控制对象，则CM不应发送REG-REQ。

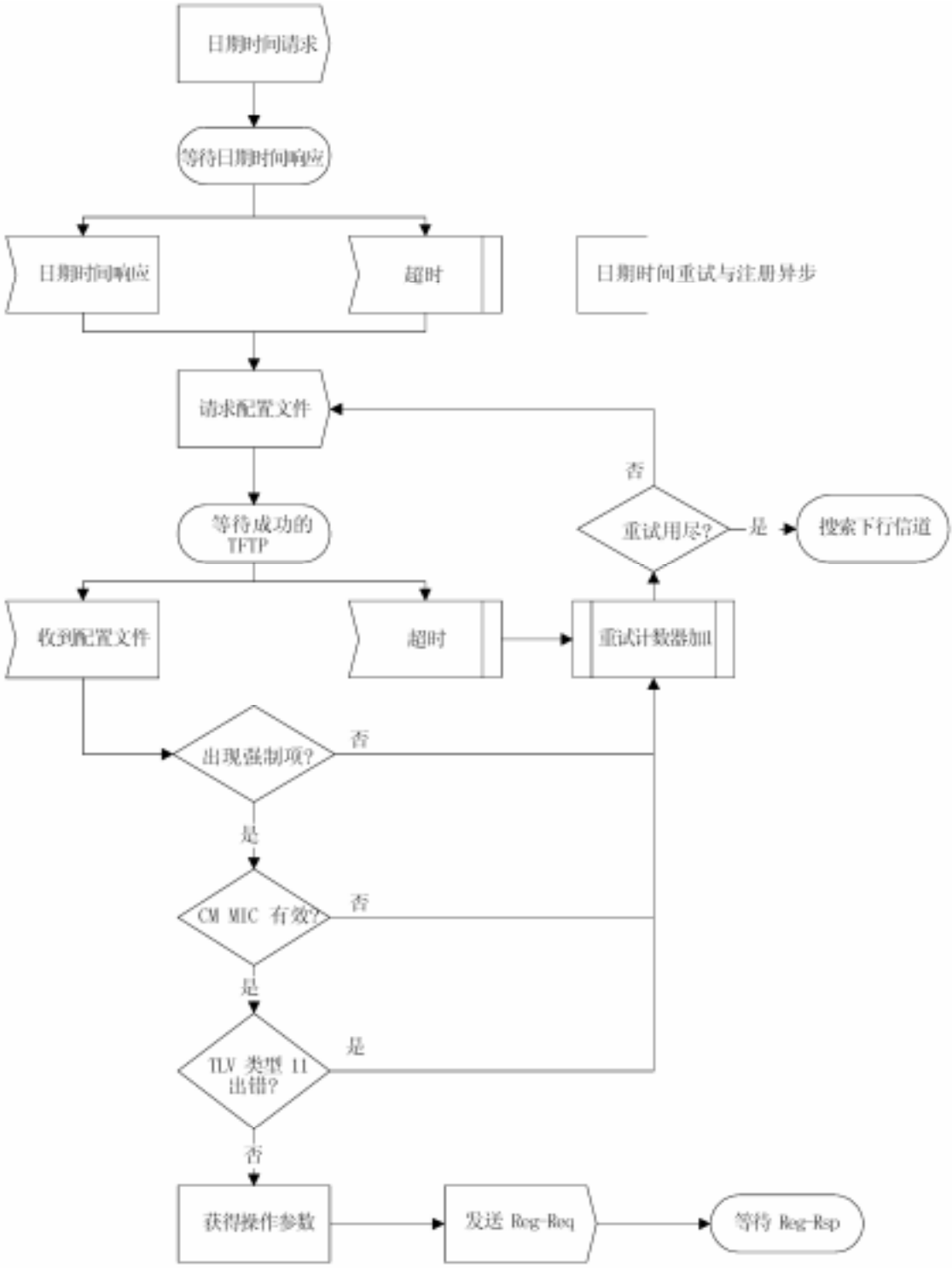


图92　注册-CM

一旦CM向CMTS发送了注册请求，它就应等待注册响应以授权它向网络转发流量，图93表示CM应遵循的等待过程。

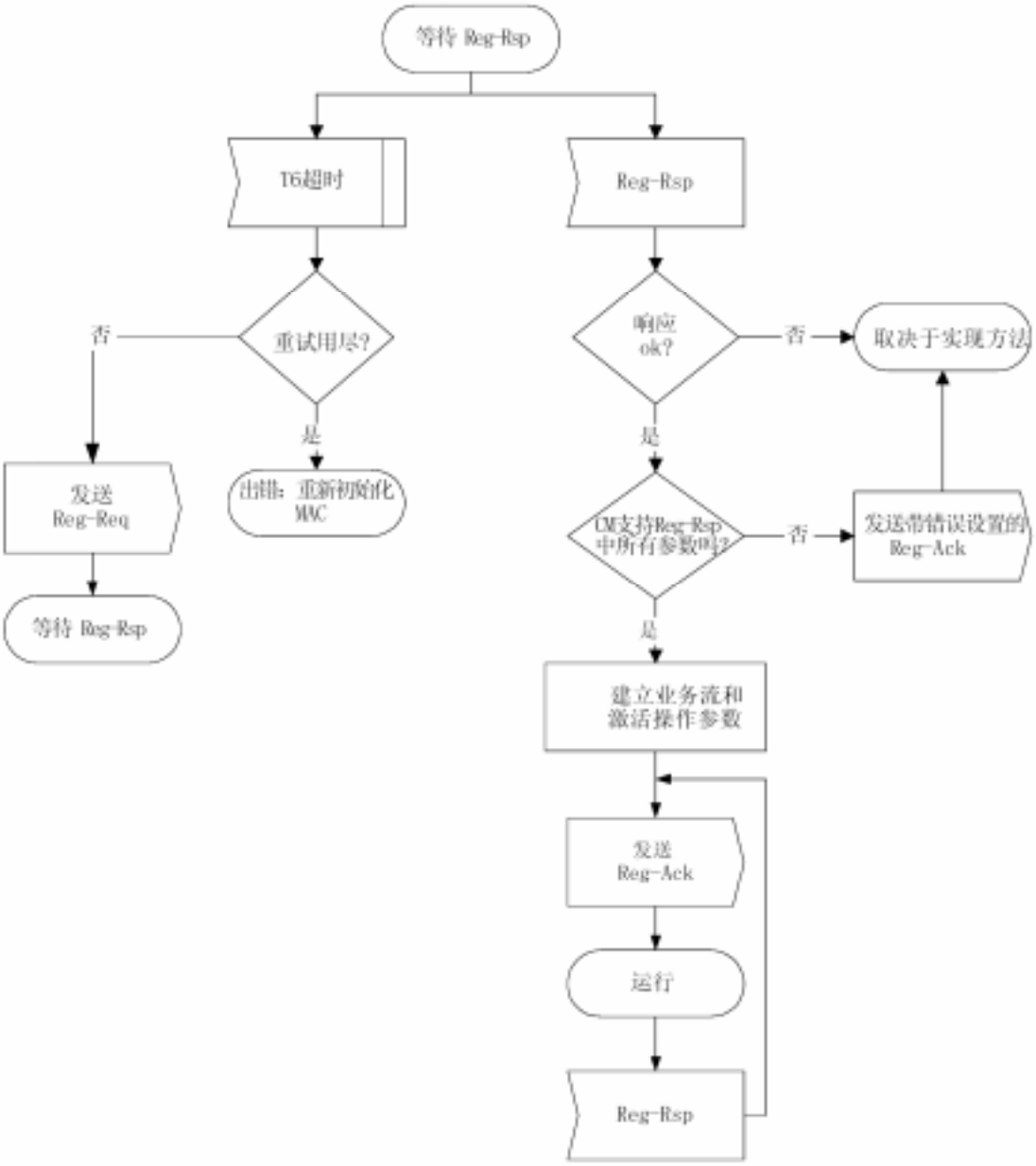


图93　等待注册响应-CM

CMTS应执行以下各操作来确认该CM的授权（见图94）：

- 根据 D.3.1 来计算 MIC，并将它与在注册请求中包含的 CMTS　MIC 相比较。如果 MIC 为无效，CMTS 应以授权失败来做出响应；
- 如果出现时戳域，则检查 TFTP 服务器时戳域。如果 CMTS 检测出该时间与其本地时间之差大于 CM 配置处理时间（见附录 B），则 CMTS 应在 REG-RSP（注册响应）中指示出鉴权失败。CMTS 还应该建立 CM MAC 地址的记录；
- 如果出现预置 CM 地址域，则检查 TFTP 服务器预置的 CM 地址域。如果预置的 CM 地址域和提出请求的 CM 的实际地址不相匹配，CMTS 应在 REG-RSP（注册响应）中指示出鉴权失败。CMTS 还应该建立 CM MAC 地址的记录；
- 如果注册请求包含 EuroDOCSIS 1.0 业务类别编码，则要验证所请求的业务类别是否可用。如果不能提供这种业务类别，CMTS 应以业务类别失败和适当的业务不可用响应码做出响应（见 C.1.3.4）；

- 如果注册请求包含业务流编码，则要在预置的业务流中验证请求的 QoS 是否可用。如果不能够提供这种业务流，则 CMTS 应以暂时拒绝或永久拒绝（附录 C.4）并给出适当的业务流响应；
- 如果注册请求包含 EuroDOCSIS 1.0 业务类别编码和业务流编码，则对于所有 EuroDOCSIS 1.0 的类别和请求的业务流，CMTS 应以业务类别失败以及将业务不可用响应代码设定为“永久拒绝”来做出响应；
- 验证任何 CM 请求的能力是否可用。如果不能或不愿意提供 CM 所请求的 CM 能力，则 CMTS 应将该 CM 能力设定为“关断”（见 7.3.8）；
- 为每一种支持的业务类别指定一个 SFID；
- 在注册响应中应答 CM；
- 如果注册请求中包含业务流编码，CMTS 应等待注册确认，如图 95 所示。如果注册请求包含 EuroDOCSIS 1.0 业务类别编码，则 CMTS 不应等待注册确认；
- 如果计时器 T9 超时，CMTS 要回收指定给该 CM 的临时 SID 以作它用。

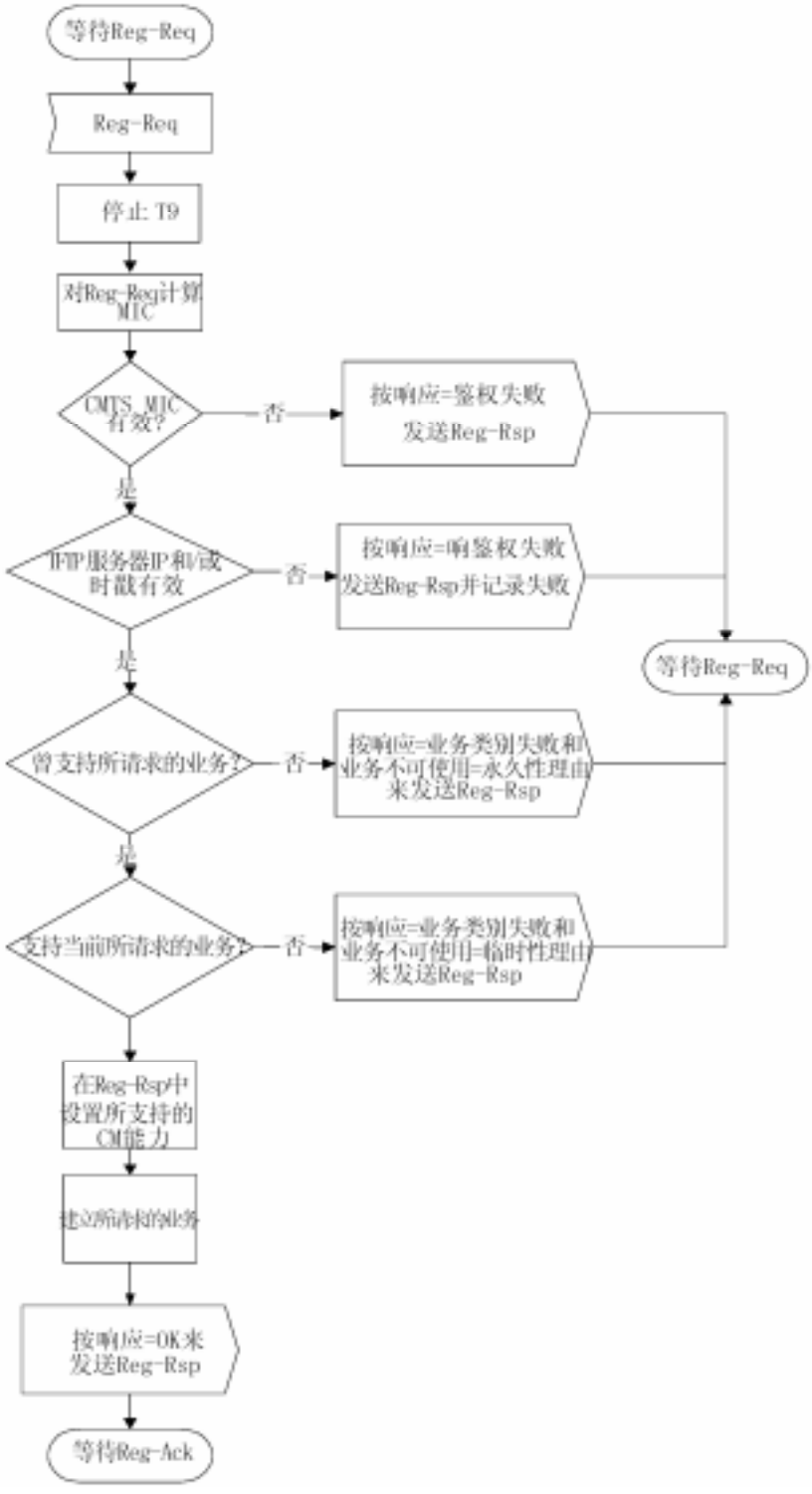

等待Reg-Req
Reg-Req
停止 T9
对Reg-Req计算MIC
CMTS_MIC有效?
否
按响应=鉴权失败发送Reg-Rsp
是
TFTP服务器IP和/或时戳有效
否
按响应=响鉴权失败发送Reg-Rsp并记录失败
是
等待Reg-Req
曾支持所请求的业务?
否
按响应=业务类别失败和业务不可使用=永久性理由来发送Reg-Rsp
是
支持当前所请求的业务?
否
按响应=业务类别失败和业务不可使用=临时性理由来发送Reg-Rsp
在Reg-Rsp中设置所支持的CM能力
建立所请求的业务
按响应=OK来发送Reg-Rsp
等待Reg-Ack

图94　注册-CMTS

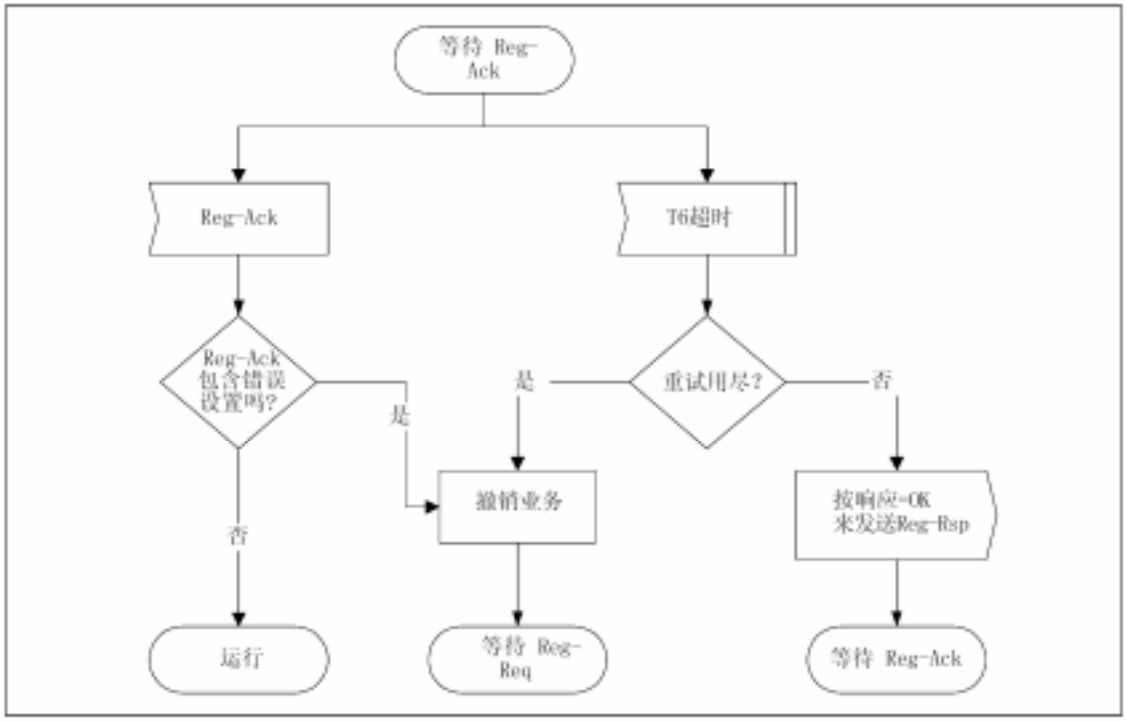


图95　注册确认-CMTS

10.2.10　加密初始化

在本部分中，配置文件中的加密设置为不使能，无需进行基线安全初始化。

10.2.11　在 CM 初始化期间的业务标识符（SID）

在完成注册过程之后（见10.2.9），CM已经被指定了SFID来匹配其预置的业务。然而，在该时间（例如测距、DHCP等）之前，CM应完成若干项协议事务，并需要一个临时的SID以便完成这些步骤。

在接收到一个初始测距请求后，CMTS应分配一个临时的SID，并将其指定给该CM供初始化之用。CMTS可以监视这一SID的使用情况，并将通讯量限制在初始化所需要的范围内。CMTS应在测距响应中将这一指定情况通知CM。

CM在接收到测距响应后，应使用指定的临时SID来进行进一步的初始化传输请求，直到接收到注册响应为止。

当接收一个移动到新的下行频率和/或上行信道ID的测距响应指令时，CM应考虑使临时SID失效,并应通过初始测距获得一个新的临时SID。

测距响应在由CMTS发送以后有可能丢失。CM应通过超时机制来进行恢复，并重新发出其初始测距请求。由于在测距请求中CM唯一地由源MAC地址来识别，所以CMTS可以立即再次使用以前指定的临时SID。如果CMTS指定一个新的临时SID，它就应采取某些措施使已经不用的旧的SID失效（见7.3.8）。

在接受注册请求的过程中指定预置的SFID时，CMTS可以再使用该临时SID，将其指定给请求的业务流之一。因为注册响应可能在传送中丢失，CMTS就应允许继续用该SID发送初始化消息。如果CMTS为预置的业务类别指定所有新的SID，它应使该临时SID失效。在注册响应在传送中丢失的情况下，这种失效过程应留有足够的时间以完成注册过程。

10.2.12　多信道支持

在系统中存在一个以上的下行信号的情况下,CM应使用在搜索过程中遇到的第一个有效的下行信号进行工作。如果有必要时，将会通过配置文件中的参数（见附录C）命令它转移到不同的下行频率和/或上行频率上工作。

在MAC管理消息中，上行信道和下行信道两者都应用信道标识符来加以识别。

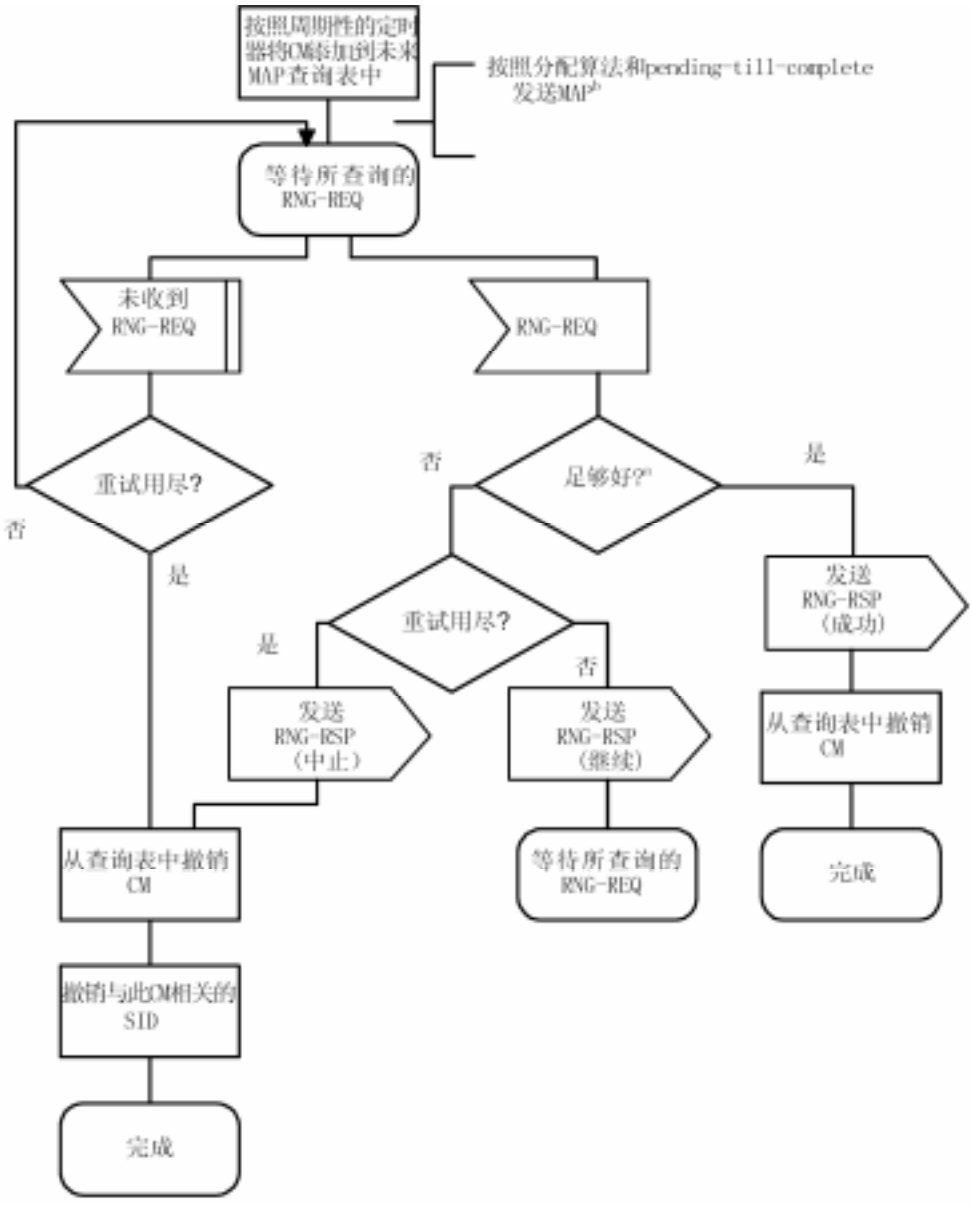
10.3 标准操作

10.3.1 周期性的信号电平调整

CMTS应至少按每T4s的间隔为每个CM提供一个周期性的测距机会。CMTS应以比T4短得多的间隔来传送周期性的测距机会，在此间隔中MAP可能丢掉而CM不会超时。这种“ 子间隔 ”的长度随CMTS而不同。

如果经过了T4s的时间之后还没有接收到一个周期性的测距机会，则CM应重新初始化MAC。

CM的远程RF信号电平调整是通过周期性的维护功能，即使用RNG-REQ和RNG-RSP MAC消息来进行的。这种情况类似于初始测距，如图96和图97所示。接收RNG-RSP消息时，在其RF信号尚未调整到与RNG-RSP的要求相符合并且达到稳定之前，CM不应发送数据（见第5章）。



a 指测距请求在 CMTS 对功率和发送均衡（如果支持）的容限范围内。

b RNG-REQ pending-till-complete（测距请求挂起-直到-完成）为非零值，除需要进行维护（例如调整 CM 的功率电平），CMTS 宜推迟台站维护机会。如果在 pending-till-complete 到期之前，已经提供了这种机会，则在 pending-till-complete 到期之前，接收 RNG-RSP 之后的"good enough（足够好）"测试不应衡量 CM 的发送均衡。

图96 周期性测距 – CMTS

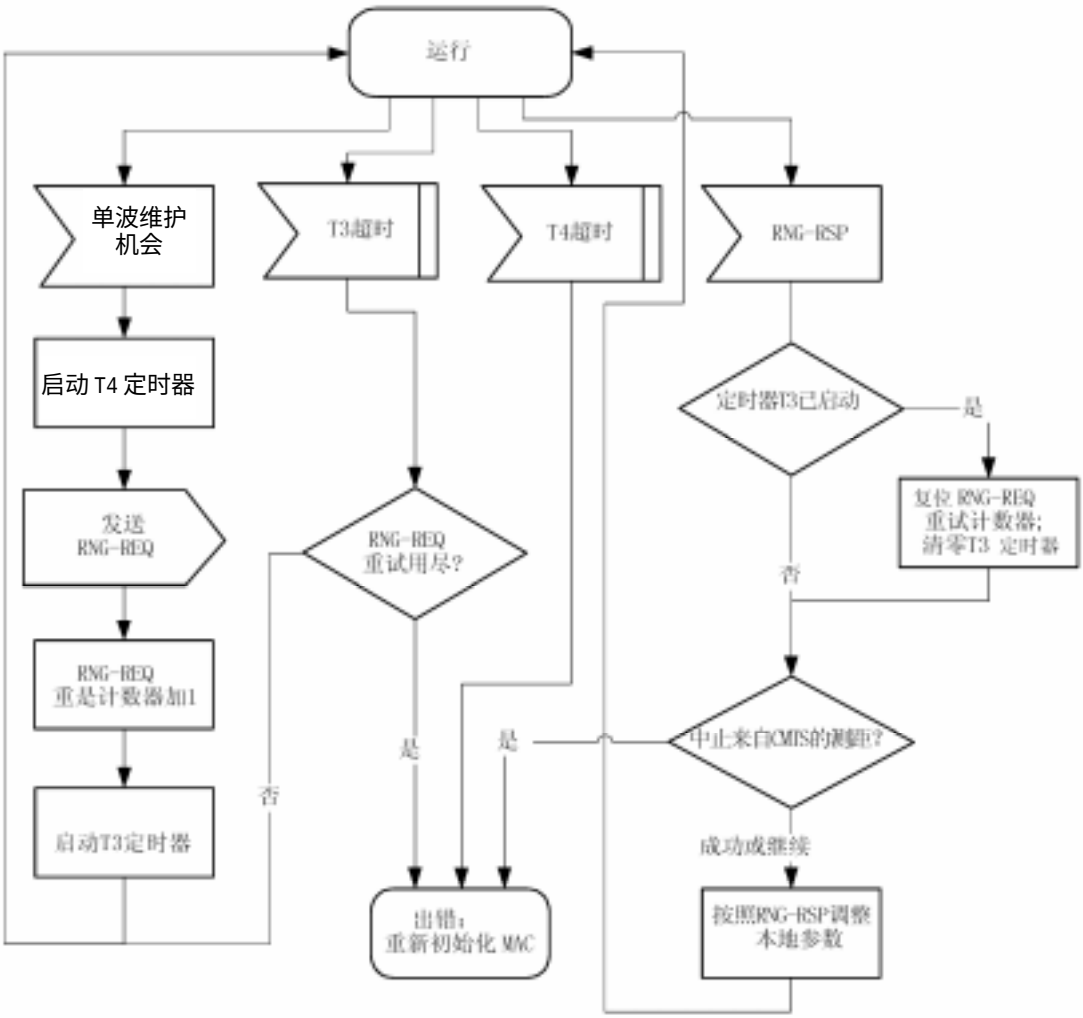


图97　周期性测距—CM

10.3.2　变更上行突发参数

每当CMTS要变更任何上行突发参数时，它应提供一种方法，使得所有的CM从旧的参数值到新的参数值进行有次序地转变。当CMTS要变更任何上行突发参数时，它应在一个上行信道描述符UCD消息中通知该新的参数值，并应使配置变更计数域加1以表示参数值已经变更。

发送了一个或多个带有新参数值的UCD消息以后，CMTS传送一个MAP消息，此消息中的UCD计数和新的配置变更计数一致。该MAP中的第一个间隔应是向空SID（0）的至少为1ms的数据授权。即CMTS应给出1ms的时间让所有的CM变更其PMD子层参数以符合该新的参数集。这个1ms和其它的MAP定时限制一起使用（见8.1.5）。

在发送了新的UCD之后，CMTS不应发送带有旧的UCD计数的MAP。

CM在对于MAP做出响应而发送任何数据的时候，应使用与该MAP的UCD计数相应的UCD中的参数。如果由于某种理由，CM没有接收到相应的UCD，则在该MAP所表述的间隔期间CM不能发送数据。

10.3.3　变更上行信道

在注册以后的任何时候，CMTS都可以指示CM变更其上行信道。这样做是为了流量均衡、规避噪声或者任何超出本部分范围的各种理由。图98示出了CMTS为此应遵循的步骤。图99示出了CM为此应遵循的步骤。

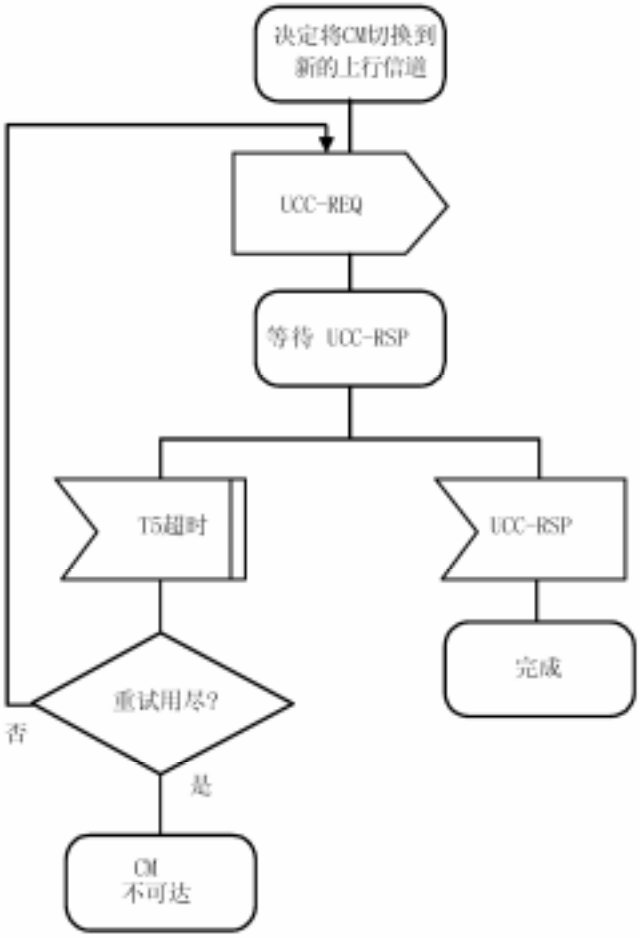


图98　变更上行信道—CMTS

如果CMTS重试UCC-REQ，则CM可能已经变更了信道（如果UCC-RSP在发送中丢失）。所以，CMTS应在旧的和新的两个信道上监听UCC-RSP。

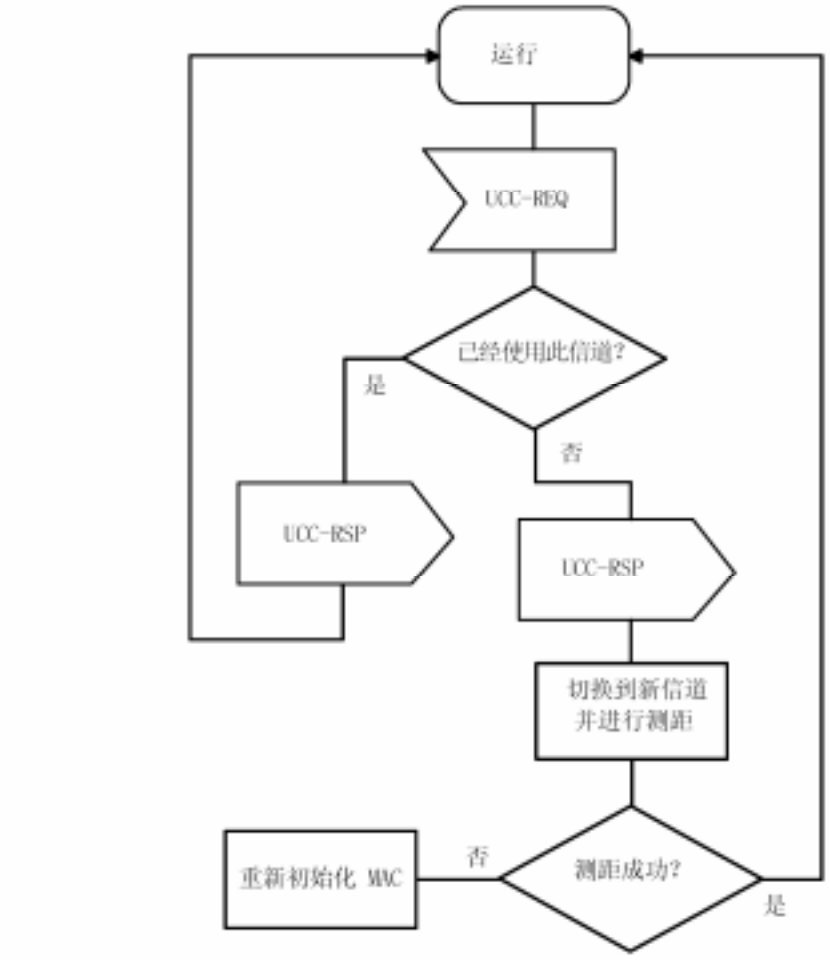


图99　变更上行信道—CM

在与新的上行信道同步之后，CM应使用在UCC-REQ测距技术TLV中规定的技术（如果有的话）来重新测距。如果在UCC-REQ中没有这个TLV，则CM应在该新的上行信道上进行初始维护（见7.3.10）。

如果CM以前曾经在该新的信道上建立了测距，并且在该信道上的这个测距仍然处于当前状态（从上一个成功的测距之后T4尚未超时），则CM可以使用缓存的测距信息而忽略测距工作。

CM应当缓存来自多个上行信道的UCD信息，以避免等待对应于新的上行信道的UCD。

CM不应进行重新注册，因为在该新的信道中其预置和MAC域仍然保持有效。

10.4　动态业务

业务流可以被产生、变更或删除。可以通过一组MAC管理消息来完成，包括动态业务添加（DSA）、动态业务变更（DSC）、动态业务删除（DSD）。DSA消息产生一个新的业务流。DSC消息变更一个已经存在的业务流。DSD消息删除一个已经存在的业务流。如图100所示。

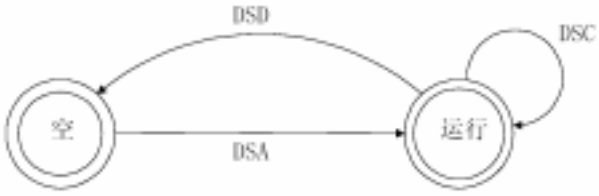


图100　动态业务流示意图

空状态意味着没有与消息中的SFID和/或事务ID相匹配的业务流。一旦业务流存在，它是可操作的并具有指定的SFID。在稳态操作中，业务流驻留在标称状态。当动态业务消息发生时，业务流可以转变到其它的状态，但是保持运行。因为可能存在多个业务流，所以可能有多个状态机激活，每个业务流一个。动态业务消息只影响与SFID和/或事务ID相匹配的那些状态机。

在注册时产生的业务流无需DSA直接进入SF_operational状态（SF_运行状态）。

事务ID对于每个事务是唯一的，并且由发起设备（CM或CMTS）来选择。为了避免模糊并提供简单的检查方法，事务ID号码空间按CM和CMTS进行划分。CM应从号码空间的前一半（0x0000到0x7FFF）来选择事务ID。CMTS应从号码空间的后一半（0x8000到0xFFFF）来选择事务ID。

每一个动态业务消息序列都是一个唯一的事务，并具有与其相关联的唯一的事务ID。DSA/DSC事务由一个请求/响应/确认序列组成。DSD事务由一个请求/响应序列组成。除非检检测到某些例外的条件，响应消息应包含一个OK确认码。确认消息应包含该响应中的确认码，除非发生了一个新的例外条件。更详细的状态图，包括转变状态，将在下面示出。每个事务的详细动作将在下文给出。

10.4.1 动态业务流的状态转变

动态业务流状态转变图是顶层状态图，它控制着总的业务流状态。在需要的时候，它产生状态转变，每个状态转变由事务状态转变图来表示，并以此来提供DSA、DSC和DSD信令。每个事务状态转变图只与其父动态业务流状态转变图相通信。顶层状态转变图对动态业务消息进行过滤，并将其传送到由SFID、业务流参考号码和事务ID所决定的适当的事务中去。

如果一个动态业务消息影响了一对业务流，则这个事务和两个父动态业务流状态转变图相通信。在这种情况下，这两个业务流在从DSx事务状态转变图中收到DSx成功或者DSx失败之前应保持锁定状态。在“锁定”时段，如果收到只针对其中一个业务流的消息，它应被作为是针对两个业务流的，即两个业务流应该保持在同样的状态。如果在锁定期间收到只针对一个业务流的DSD-REQ消息，设备应正常地处理事件，即通过启动DSD-Remote事务发送SF Delete-Remote给正在进行的DSx事务，并且，它应启动DSD-Local事务锁定业务流对中的第二个。

有6种不同类型的事务：每一种DSA、DSC和DSD消息都由本地发起或远端发起。大多数事务都有三种基本的状态：挂起、保持和删除。事务一旦产生就进入挂起状态等待响应。保持状态通常是在接收到响应以后进入的，此状态的目的是容许在丢失信息的情况下重新发送，即使本地实体已经发觉事务已完成也要这样做。删除状态只在正在处理事务时、业务流被删除的情况下才进入。

图101至图107所示的流图提供了事务状态转变图中每个状态的详细表示，所有的有效状态均示出。任何未示出的输入应按严重错误条件来处理。

除一种例外情况之外，这些状态图同等地适用于CMTS和CM。在动态业务流Changing-Local（变更-本地）状态，CM和CMTS的情况有一些细微的区别。这在状态转变和详细流程图中予以说明。

注：动态业务流状态转变图中的“Num Xacts”变量在每次顶层状态图产生一个事务时加1，在每次一个事务结束时减1。在业务流被删除并且所有的事务已经结束之前，动态业务流不应返回空状态。

状态图的各种输入标识如下：

a) 来自未规定的本地、高层实体的动态业务流状态转变图输入：
   - 添加；
   - 变更；
   - 删除；

b) 来自 DSx 事务状态转变图的动态业务流状态转变图输入：
   - 成功的 DSA；
   - 失败的 DSA；
   - 丢失的 DSA ACK；
   - 出错的 DSA；
   - 结束的 DSA；

- 成功的 DSC；
- 失败的 DSC；
- 丢失的 DSC ACK；
- 出错的 DSC；
- 结束的 DSC；
- 成功的 DSD；
- 出错的 DSD；
- 结束的 DSD；

c) 来自动态业务流状态转变图的 DSx 事务状态转变图输入：

- SF 添加；
- SF 变更；
- SF 删除；
- SF 中止添加；
- SF 变更-远端；
- SF 删除-本地；
- SF 删除-远端；
- 丢失的 SF DSA-ACK；
- 丢失的 SF DSC-REQ；
- 丢失的 SF DSC-ACK；
- 丢失的 SF DSD-REQ；
- 变更的 SF；
- 删除的 SF。

由动态业务流状态转变图所产生的DSx事务用以下的符号来表示：

DSx-[Local | Remote] (initial_input)

其中，initial_input依据事务类型和发起者可以为SF添加、DSA-REQ、SF变更、DSC-REQ、SF删除或DSD-REQ。

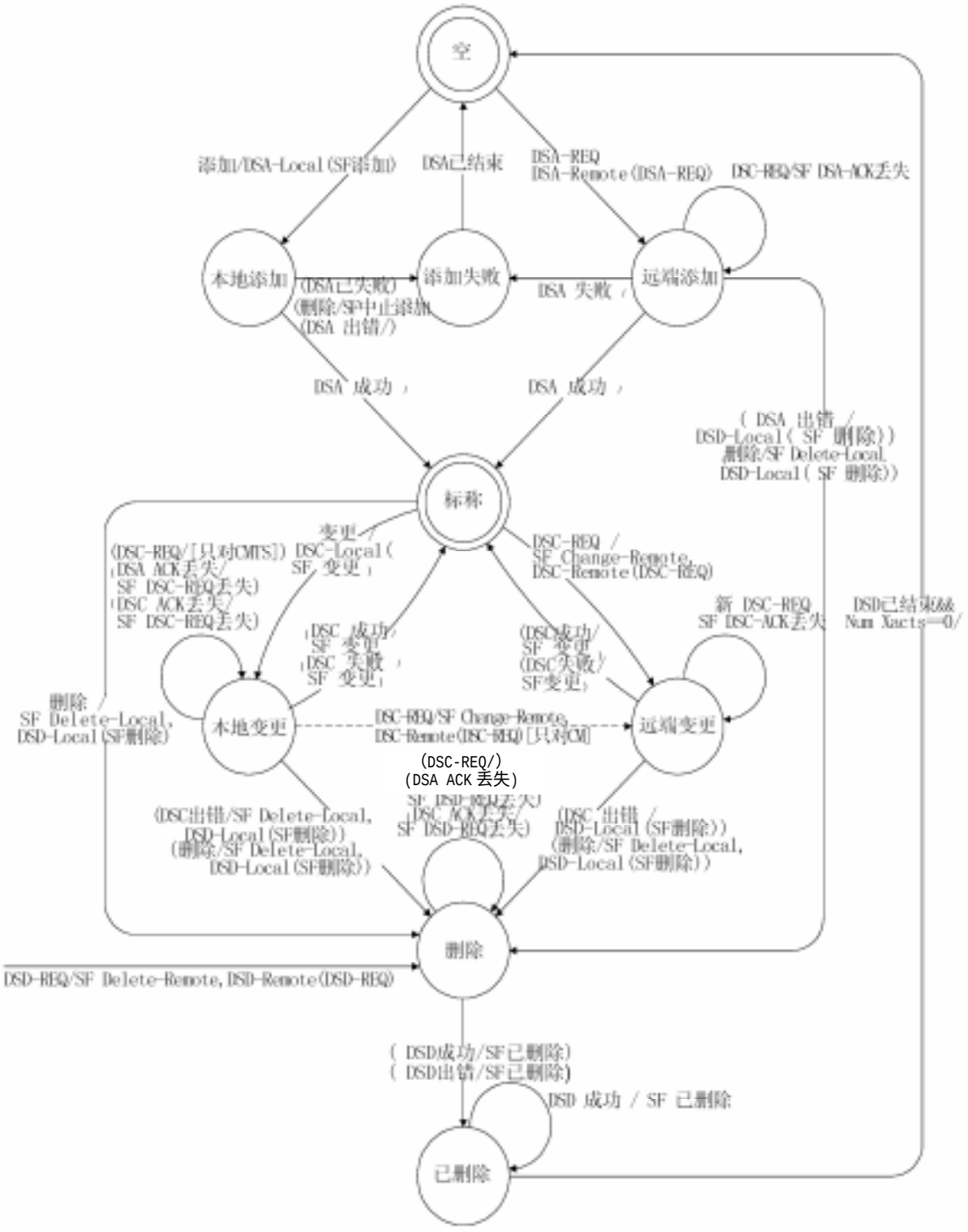


图101　动态业务流状态转变图

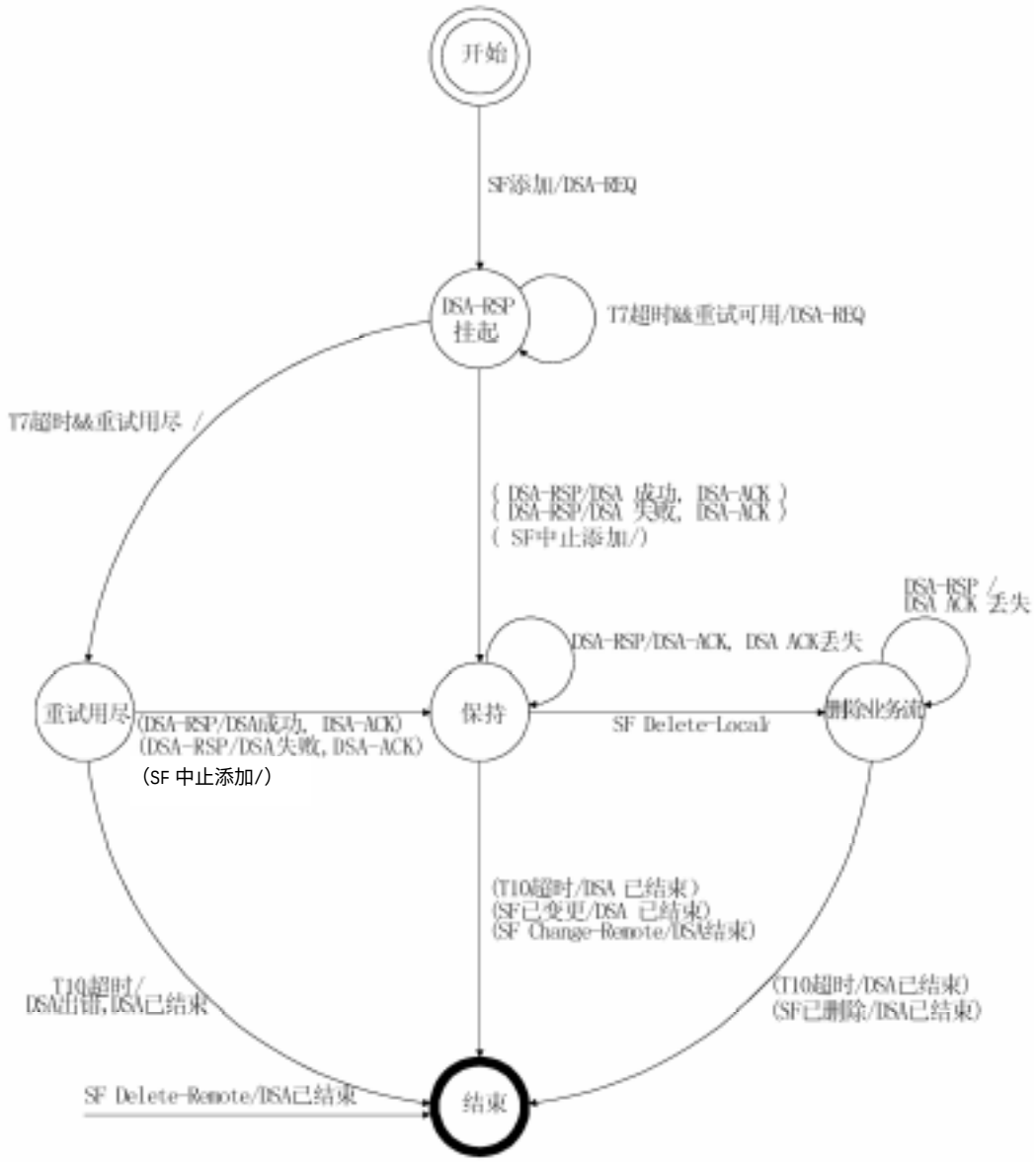


图102　DSA-本地启动事务状态转变图

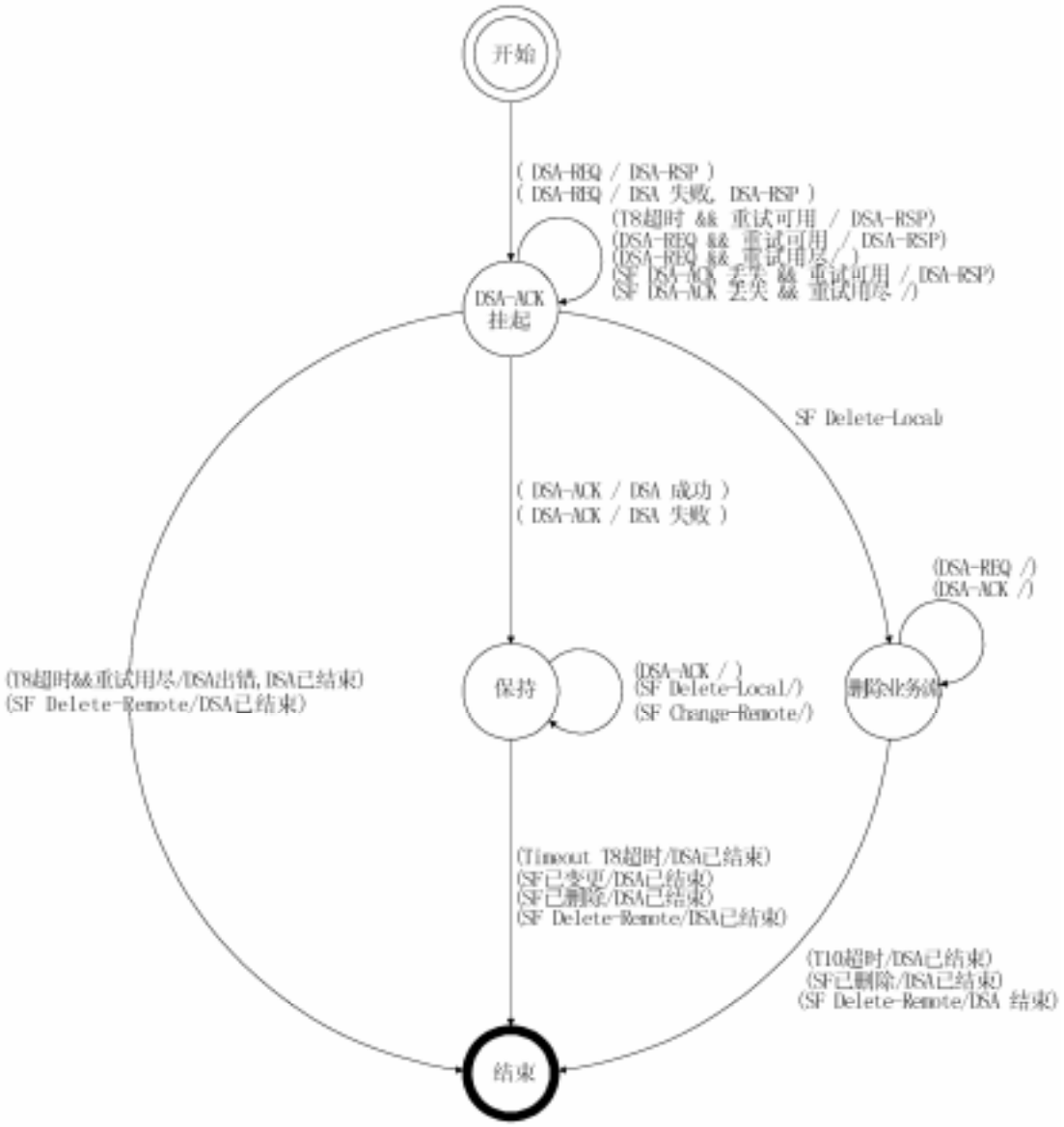


图103　DSA-远端启动事务状态转变图

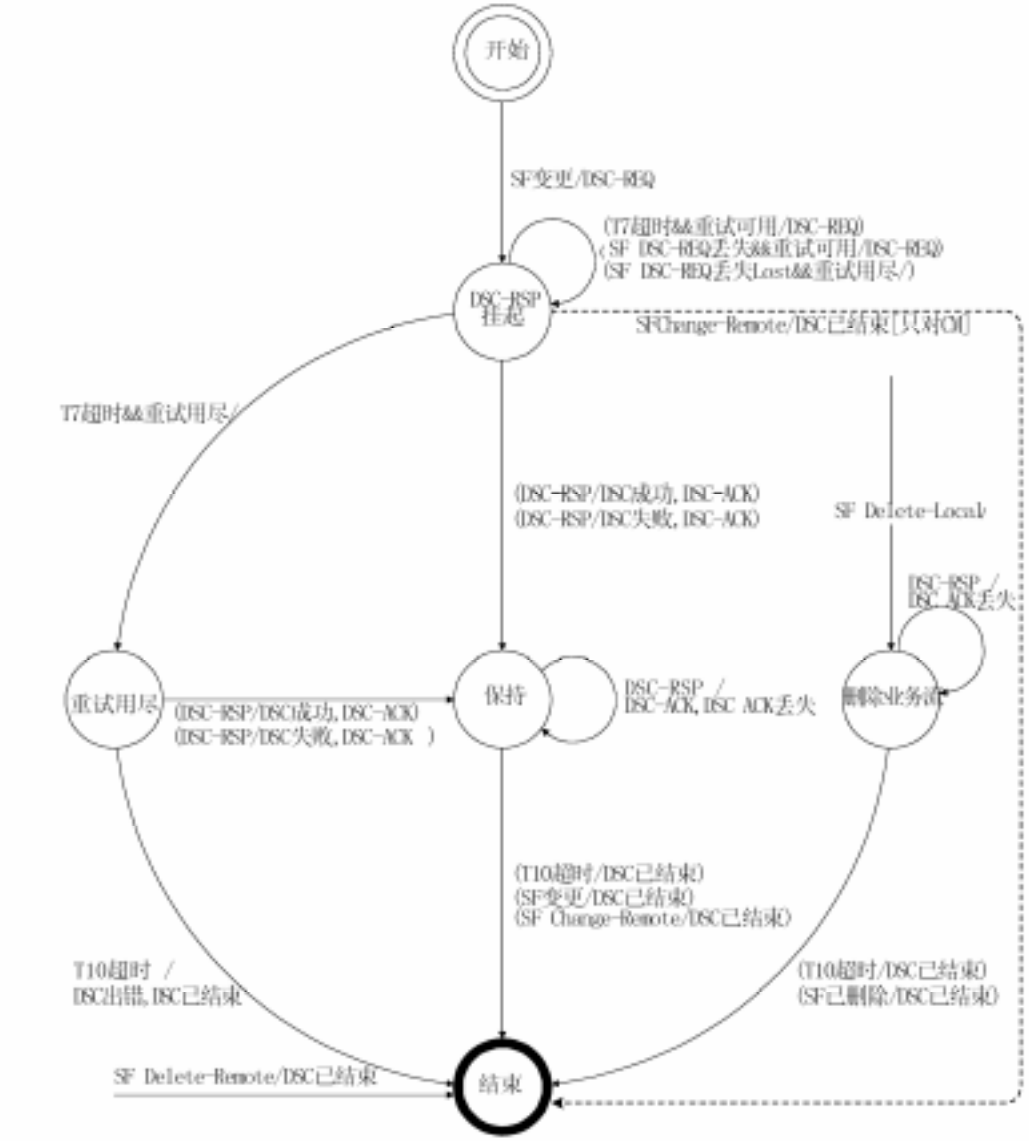


图104　DSC-本地启动事务状态转变图

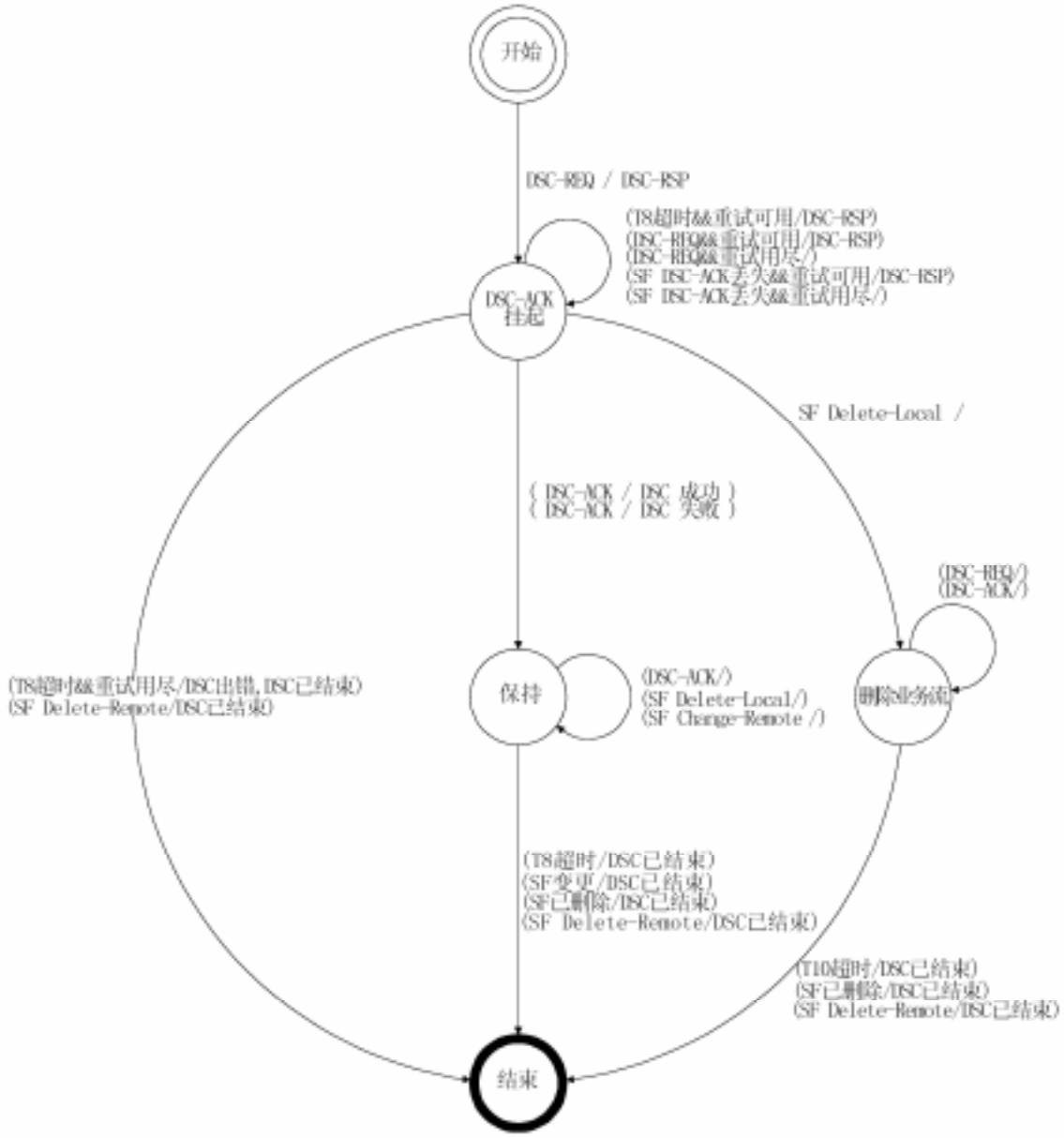


图105　DSC-远端启动事务状态转变图

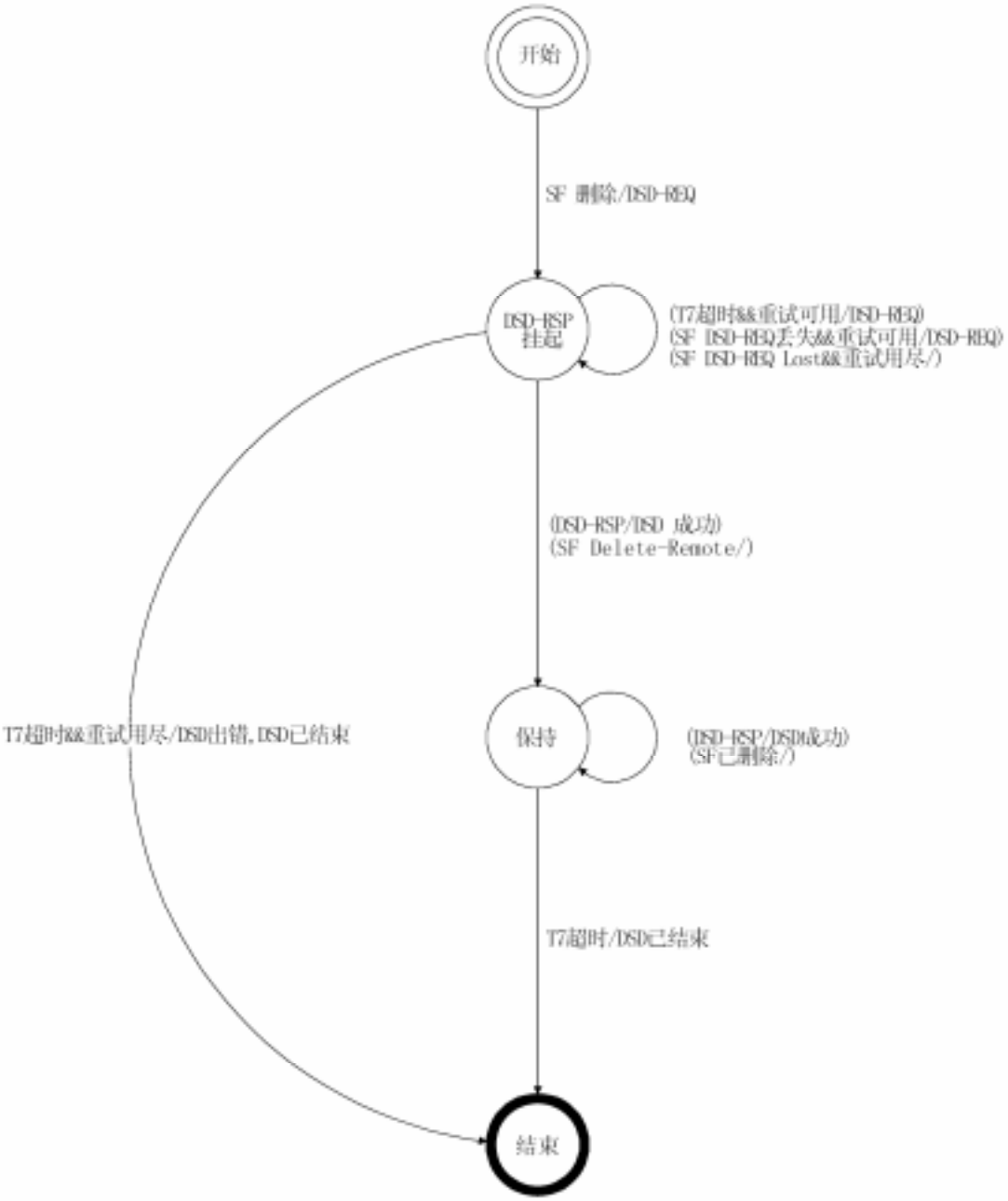


图106　DSD-本地启动事务状态转变图

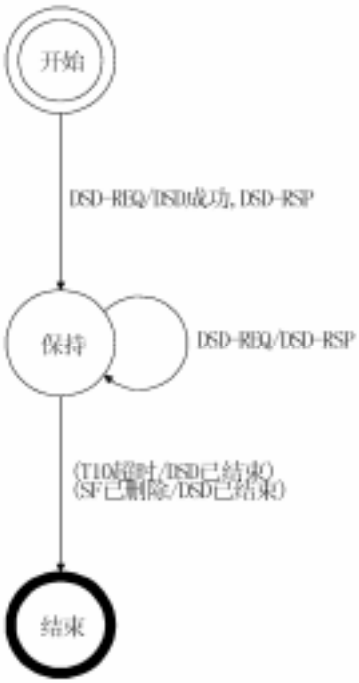


图107　DSD-远端启动事务状态转变图

10.4.2　动态业务添加（DSA）

10.4.2.1　CM 发起的动态业务添加

产生上行和/或下行业务流的CM使用动态业务添加请求消息（DSA-REQ）向CMTS发送一个请求。CMTS检查该CM对于所请求的业务的授权以及是否能够支持其QoS要求，并使用动态业务添加响应信息（DSA-RSP）来产生一个适当的响应。CM则用一个确认消息（DSA-ACK）来结束此事务。见图108。

在单个的DSA-REQ之中可包含一个上行和一个下行业务流。这两个业务流将一起被接受或拒绝。

CM		CMTS
需要新的业务流		
检查资源是否可用		
发送 DSA-REQ	---DSA-REQ-->	接收 DSA-REQ
		检查CM是否有业务授权[a]
		检查能否支持业务流QoS
		产生 SFID
		如果上行AdmittedQoSParamSet非空，则产生SID； 如果上行ActiveQoSParamSet非空，则允许在新上行业务流上接收数据
接收 DSA-RSP	<--DSA-RSP---	发送 DSA-RSP
如果ActiveQoSParamSet非空，则允许在新业务流上发送和/或接收数据		
发送 DSA-ACK	---DSA-ACK-->	接收 DSA-ACK
		如果下行ActiveQoSParamSet非空，则允许在新下行业务流上发送数据

a 授权能够在 CMTS 接收到 DSA-REQ 之前发生。CMTS 信令预测 DSA-REQ 的细节已超出本部分的范围。

图108　由 CM 发起的动态业务添加

10.4.2.2 CMTS 发起的动态业务添加

与CM建立上行和/或下行动态业务流的CMTS要进行下述的操作。CMTS检查目的CM所请求的业务类别的授权以及是否能够支持其QoS要求。如果能够支持该业务，CMTS就产生所需业务类别的新的SFID，并使用动态业务添加请求消息（DSA-REQ）来通知该CM。如果CM检查出它能够支持该业务，就使用动态业务添加响应消息（DSA-RSP）来做出响应。此事务以CMTS发送确认消息（DSA-ACK）来完成。见图109。

CM		CMTS
		CM需要新的业务流 检查CM业务的授权 检查能否支持业务流QoS 产生SFID（s） 如果上行AdmittedQoSParamSet非空，则产生SID； 如果上行ActiveQoSParamSet非空，则允许在新上行业务流上接收数据
接收 DSA-REQ	<--DSA-REQ---	发送 DSA-REQ
确认CM能够支持业务流 添加下行SFID（如果出现的话） 允许接收任何新下行业务流		
发送 DSA-RSP	---DSA-RSP-->	接收 DSA-RSP 允许在新业务流上发送和接收数据
接收 DSA-ACK 允许在新上行业务流上发送数据	<--DSA-ACK---	发送 DSA-ACK

图109 由 CMTS 发起的动态业务添加

10.4.2.3 动态业务添加状态转变图

动态业务添加状态转变图见图110至图118。

图110　DSA-本地发起的事务开始状态流程图

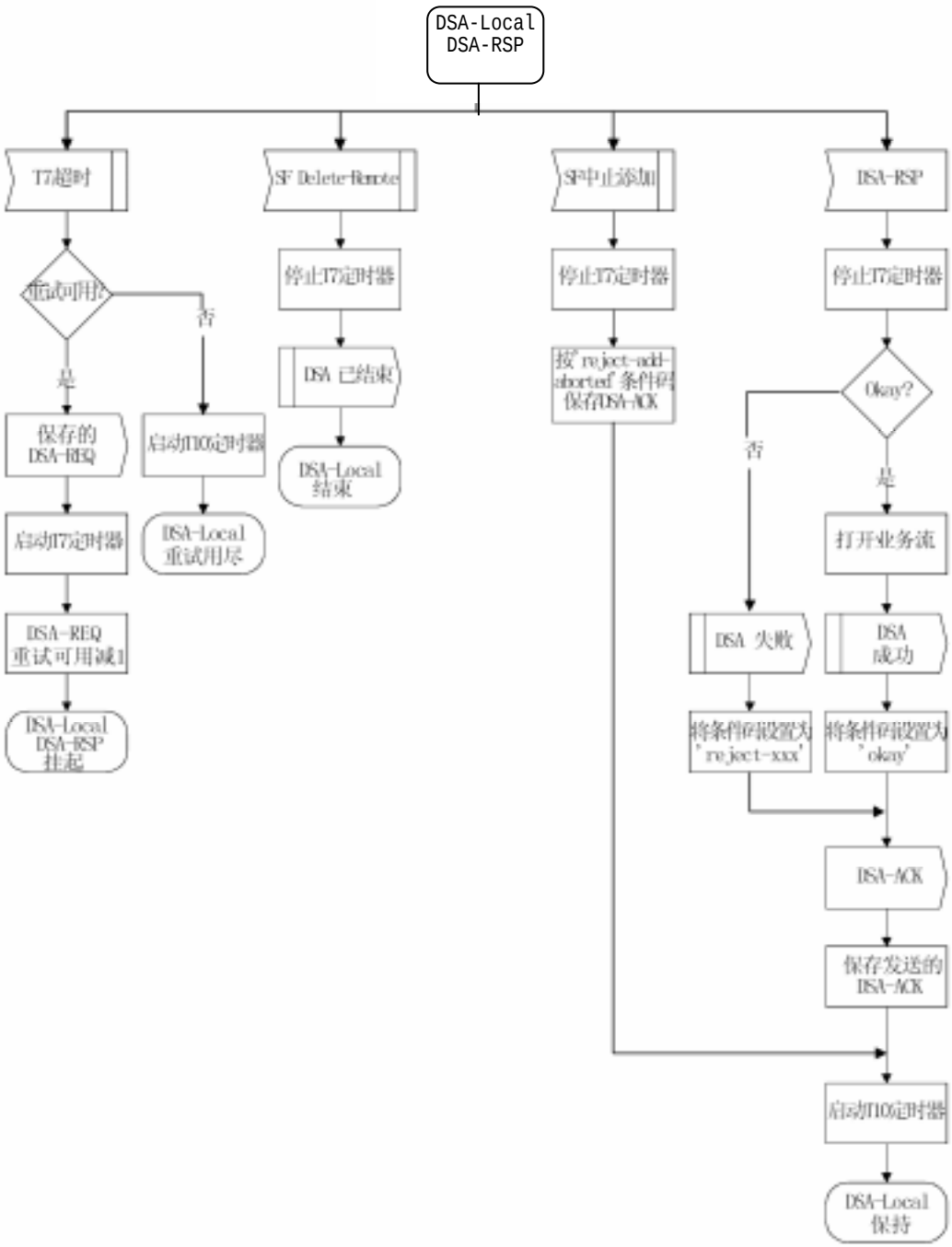


图111　DSA-本地发起的事务 DSA-RSP 挂起状态流程图

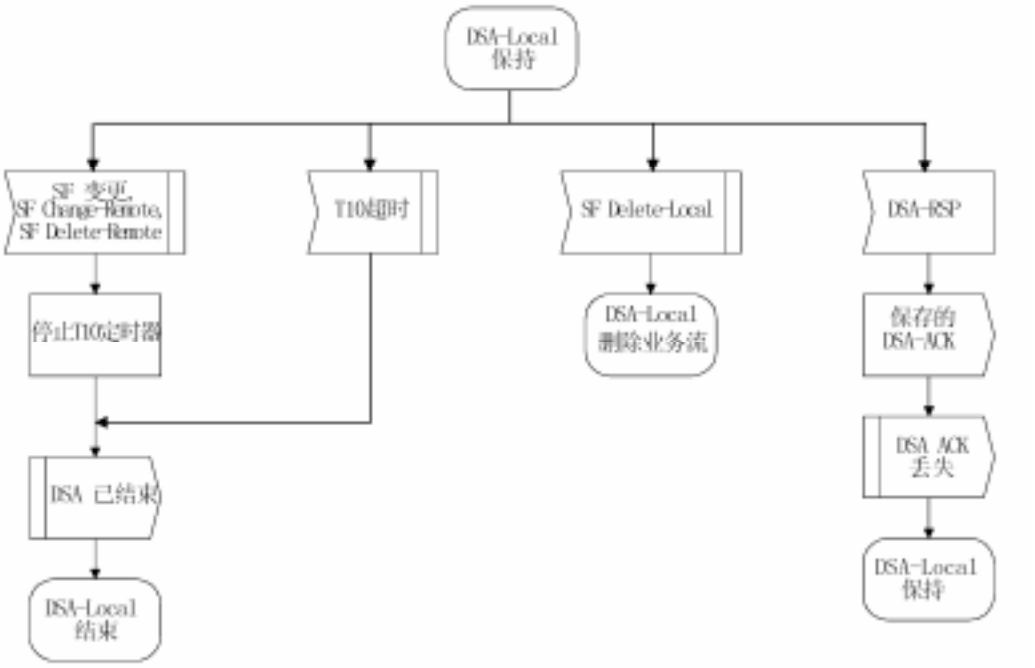


图112　DSA- 本地发起的事务保持状态流程图

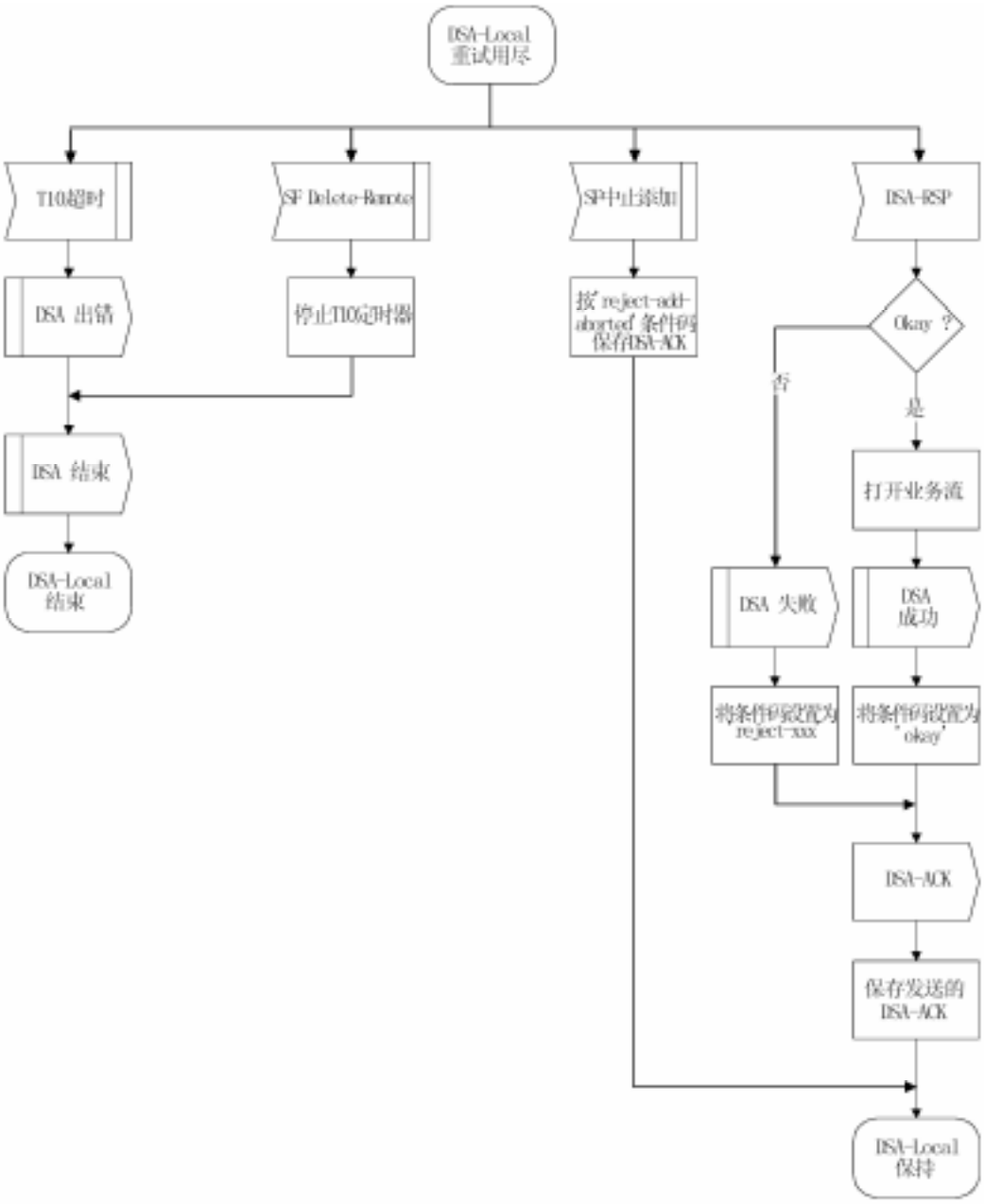


图113　DSA- 本地发起的事务重试用尽状态流程图

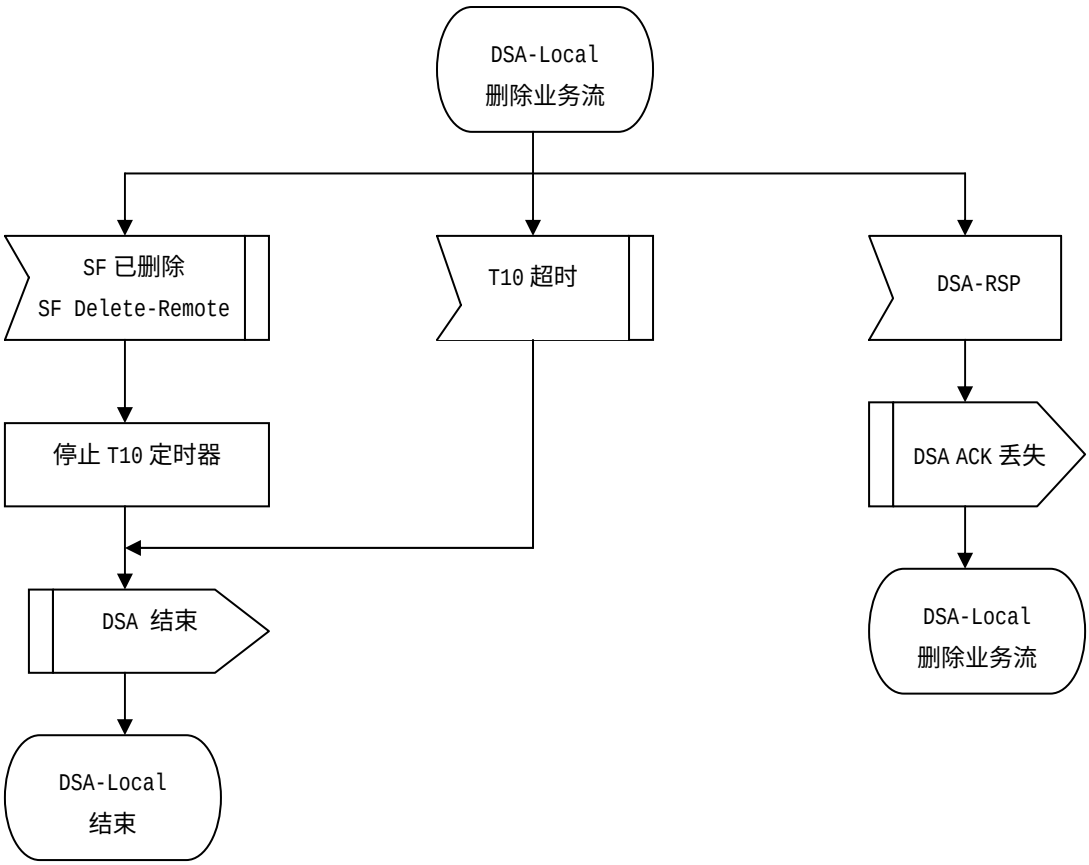


图114　DSA- 本地发起的事务删除业务流状态流程图

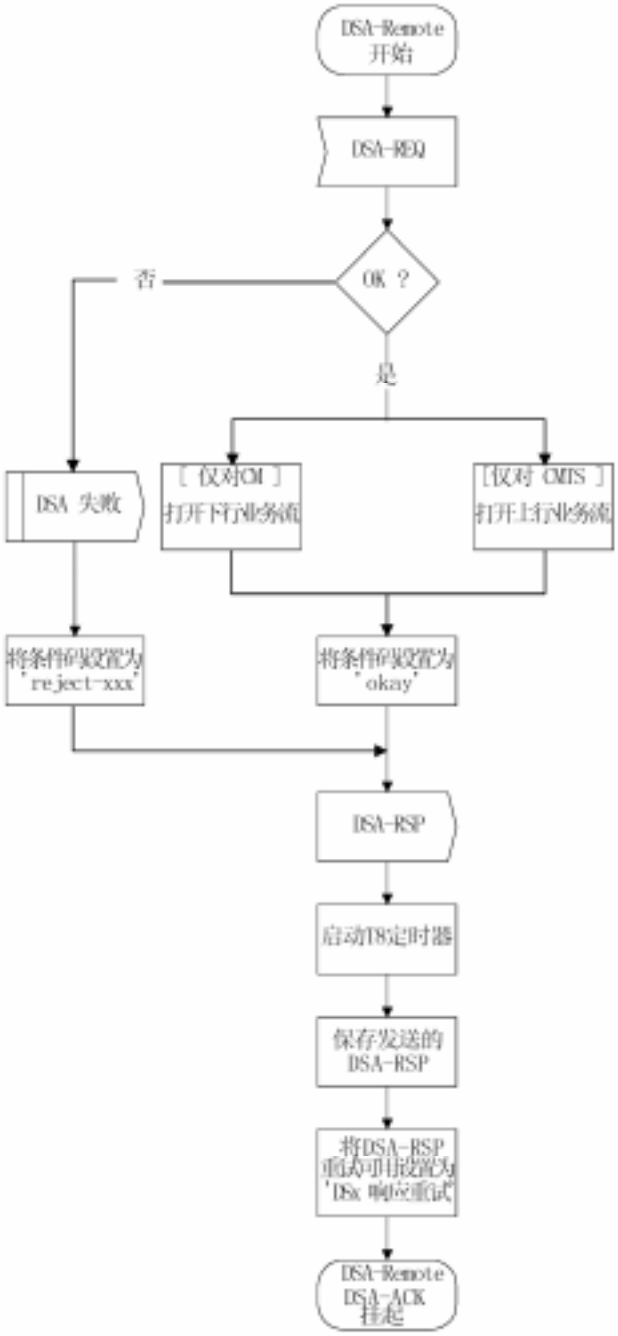


图115　DSA- 远端发起的事务开始状态流程图

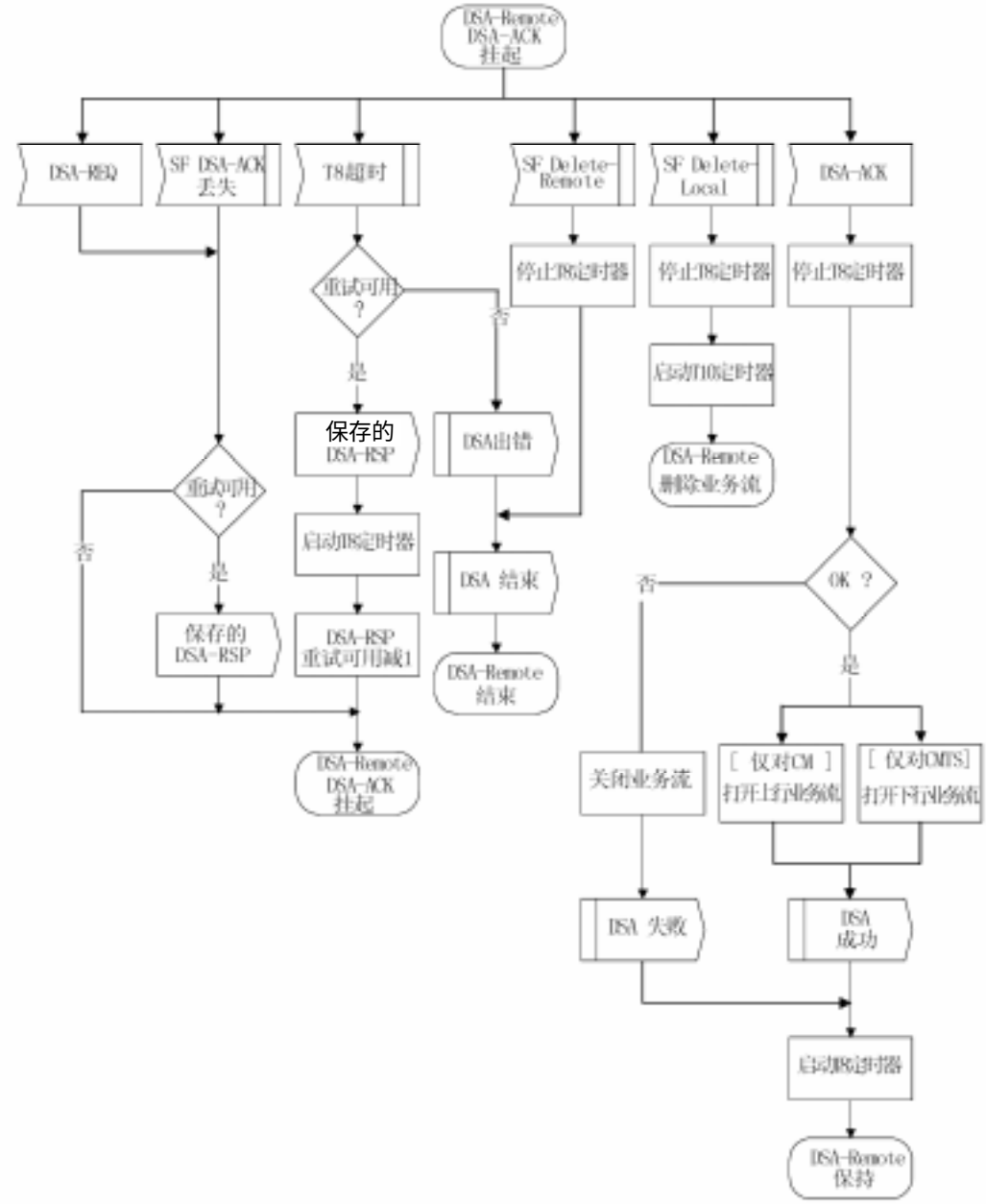


图116　DSA- 远地发起的事务 DSA-ACK 挂起状态流程图

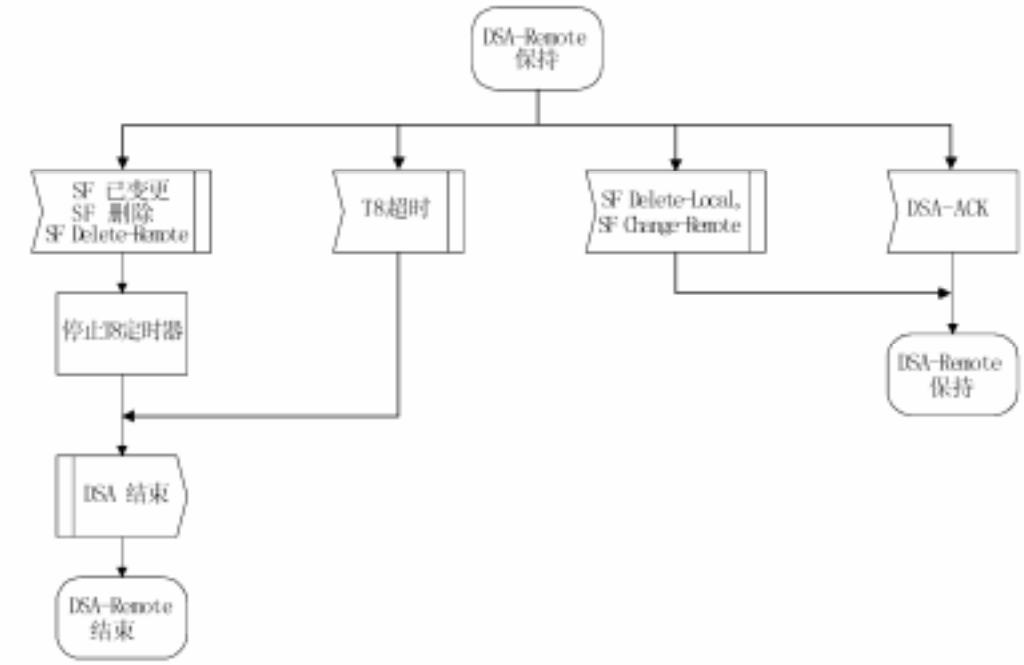


图117　DSA- 远端发起的事务保持状态流程图

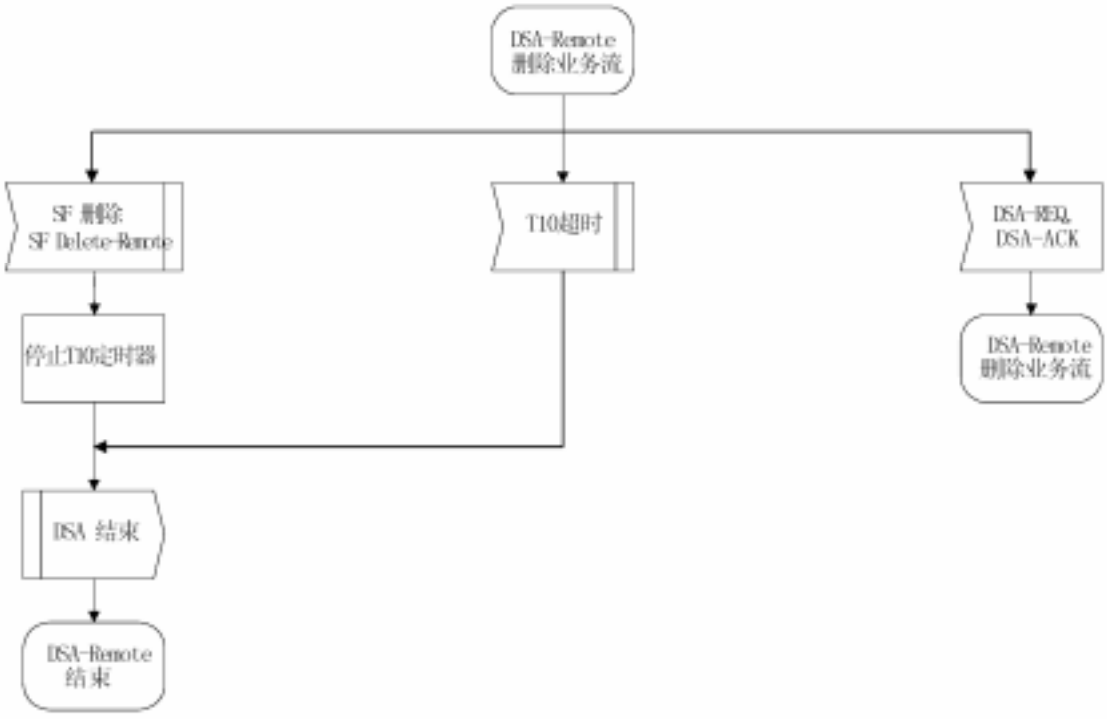


图118　DSA-远端发起的事务删除业务流状态流程图

10.4.3　动态业务变更

动态业务变更（DSC）消息集用来修改与业务流相关联的各种业务流参数。特别是，DSC能够：

- 修改业务流规范；
- 添加、删除或替换流分类器；
- 添加、删除或设定 PHS 单元。

单个DSC消息交换能够修改一个下行业务流和/或一个上行业务流的各种参数。

为了避免包的丢失，任何请求的带宽变更都在CM和CMTS之间顺序编号。

CMTS控制上行和下行的调度。调度变更的定时与信道的方向和带宽的添加或减少无关。CMTS总是在接收到DSC-REQ（CM发起的事务）或DSC-RSP（CMTS发起的事务）之后变更调度。

CMTS还控制下行传送行为。下行传送行为的变更总是和下行调度的变更同时发生（即CMTS同时控制这二者并变更这二者）。

CM控制上行传送行为。CM传送行为变更的定时取决于什么设备启动该事务和是否“ 添加 ”或“ 减少 ”带宽。

如果上行业务流的带宽正在被减少，则CM首先减少其有效负载带宽，然后CMTS减少为该业务流授权的带宽。如果上行业务流的带宽正在被添加，则CMTS首先添加为该业务流授权的带宽，然后CM添加其有效负载带宽。

如果带宽变更情况复杂，则什么时候引起带宽变更对于CM可能是不明显的。这个信息可能通过更高层的实体告知CM。与此类似，如果DSC信令是由CMTS发起的，则CMTS可能向CM表明在接受DSC请求时它是否应该建立或取消分类器，或者它是否应该推迟建立该分类器直到接收DSC-ACK为止（见C.2.1.8）。

任何业务流都可以用动态业务变更命令，即通过发送DSC-REQ消息、引用该业务流标识符以及包括一个空的激活QoS参数集来撤消激活。然而，如果一个CM的基本业务流被撤消激活，则该CM就被撤销注册并应重新注册。所以，在撤消激活这种业务流之前应特别小心。如果在注册时一个业务流是被预置的，则这个业务流被撤消激活时，为该业务流预置的信息应保持到该业务流重新激活为止。

CM对于每个业务流只能有一个DSC事务处于未完成状态。如果它检测到第二个由CMTS发起的事务，则CM应中止它所发起的该事务，并且让CMTS发起的事务完成。

CMTS对于每个业务流只能有一个DSC事务处于未完成状态。如果它检测到第二个由CM发起的事务，则CMTS应中止CM所发起的该事务，并且让CMTS发起的事务完成。

注： 当前期望的应用可能通过CM或CMTS（但不是二者）来控制业务流。所以由CM和CMTS同时发起的DSC的情况被认为是一种例外条件，并且做为一个来处理。

10.4.3.1 CM 发起的动态业务变更

需要变更业务流定义的CM要进行下列操作。

CM使用一个动态业务变更请求消息（DSC-REQ）来告知CMTS。CMTS应决定该参考的业务流是否能够支持这项变更。CMTS应用一个DSC-RSP做出响应，以指明它接受或拒绝该请求。如果合适的话，CM就重新配置该业务流，然后应用一个DSC-ACK做出响应。见图119。

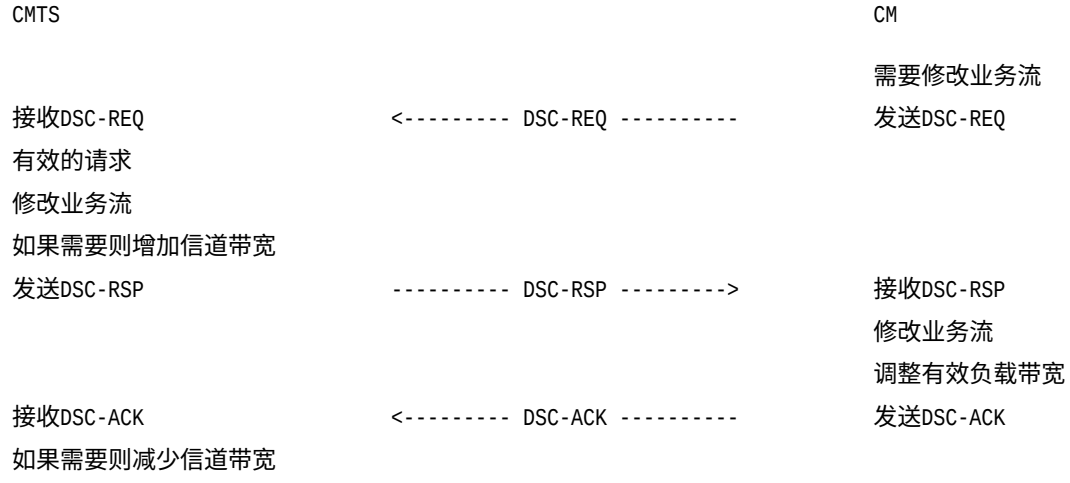


图119 CM 发起的 DSC

10.4.3.2 CMTS 发起的动态业务变更

需要变更业务流定义的CMTS要进行下列操作。

CMTS应决定参考的业务流是否能够支持该项变更。若支持，CMTS使用DSC-REQ告知CM。CM检查它是否能够支持该业务变更，并应使用DSC-RSP做出响应，以指明它接受或拒绝该请求。如果合适的话，CMTS就重新配置该业务流，然后应用DSC-ACK做出响应。见图120。

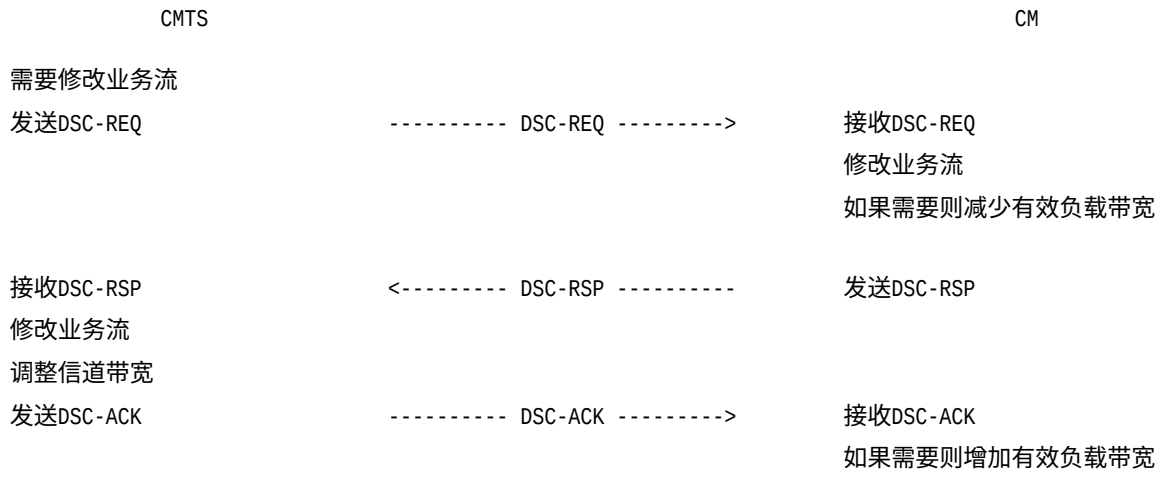


图120　CMTS 发起的 DSC

10.4.3.3　动态业务变更状态转变图

动态业务变更状态转变图见图121至图129。

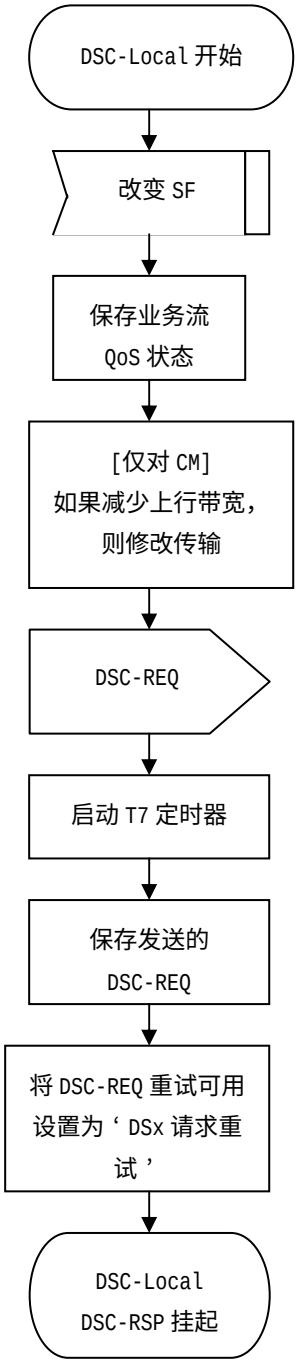


图121　DSC –本地发起的事务开始状态流程图

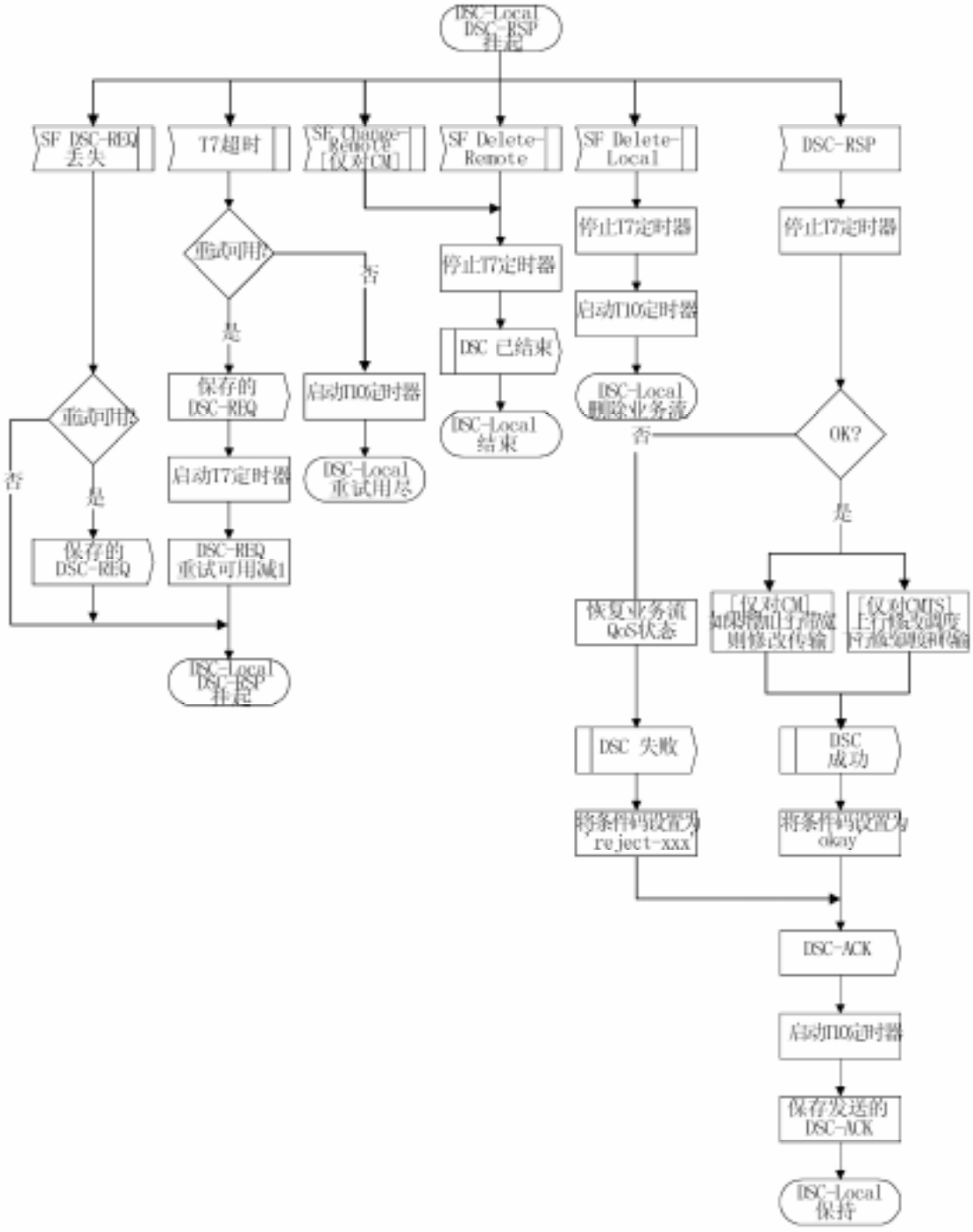


图122　DSC —本地发起的事务 DSC-RSP 挂起状态流程图

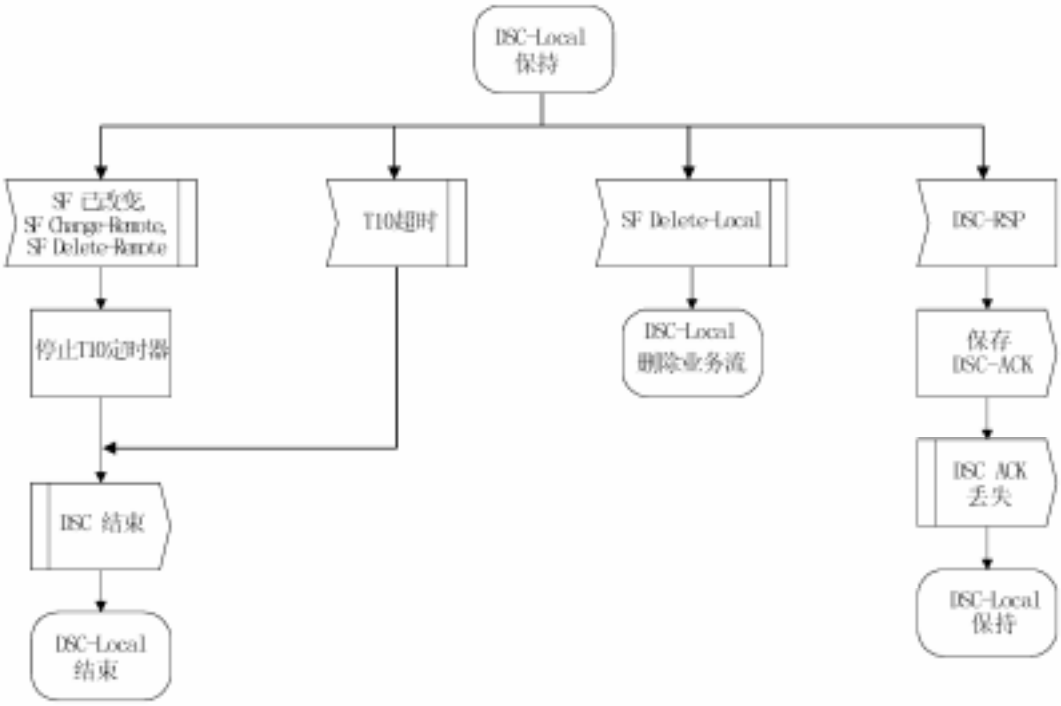


图123　DSC –本地发起的事务保持状态流程图

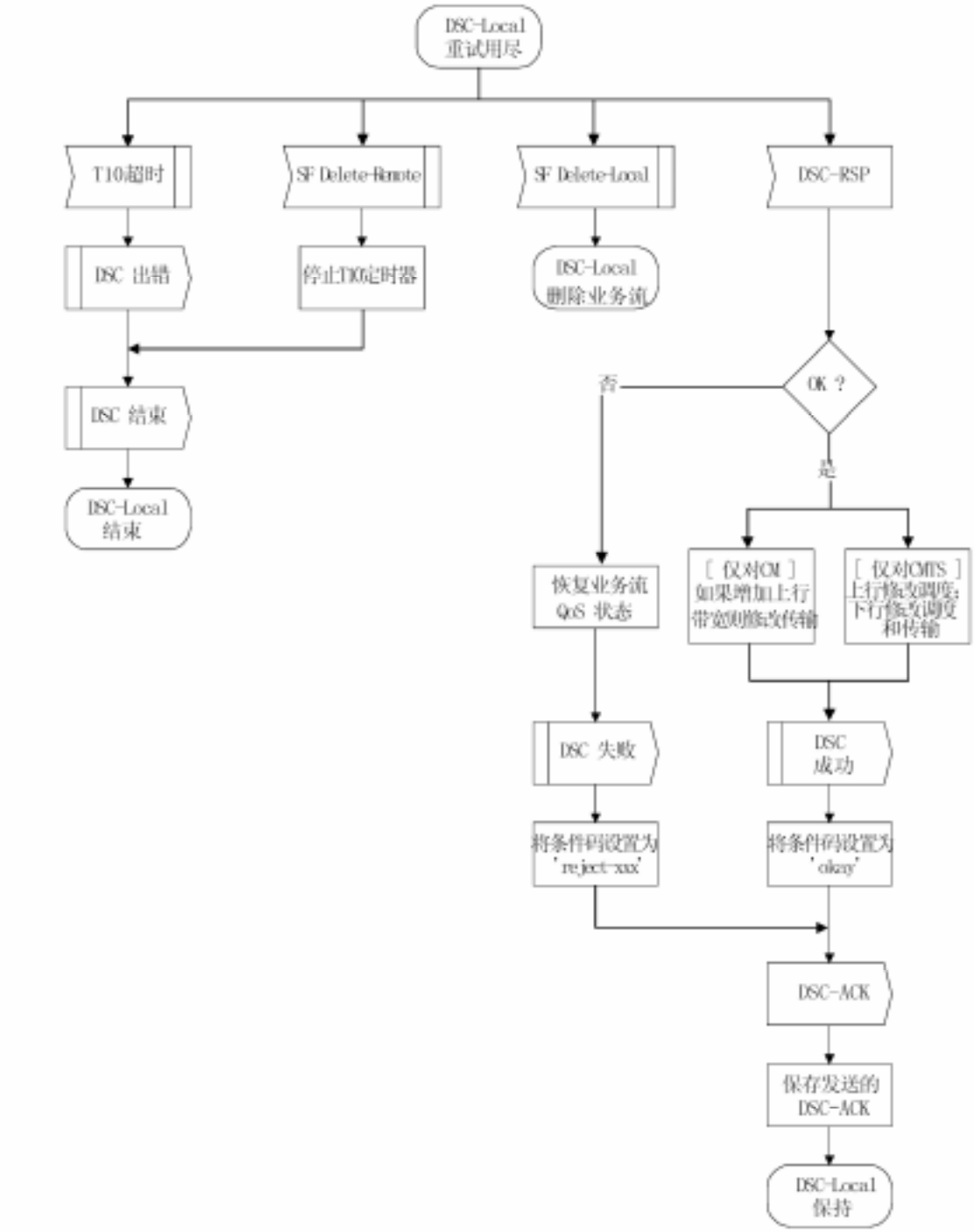


图124　DSC-本地发起的事务重试用尽状态流程图

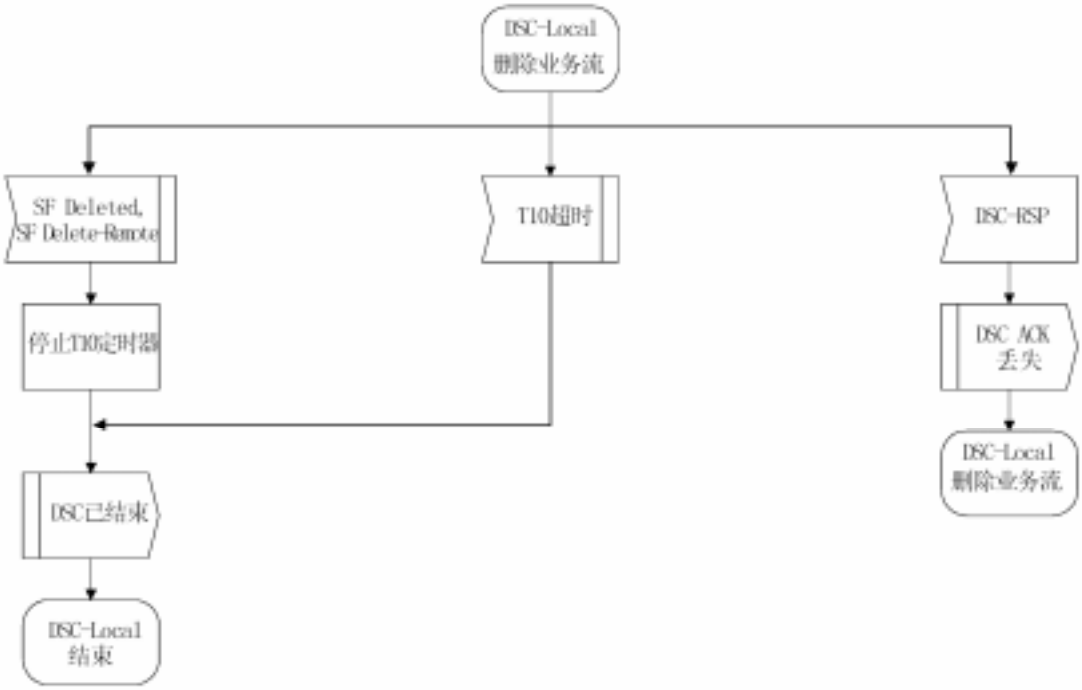


图125　DSC –本地发起的事务删除业务流状态流程图

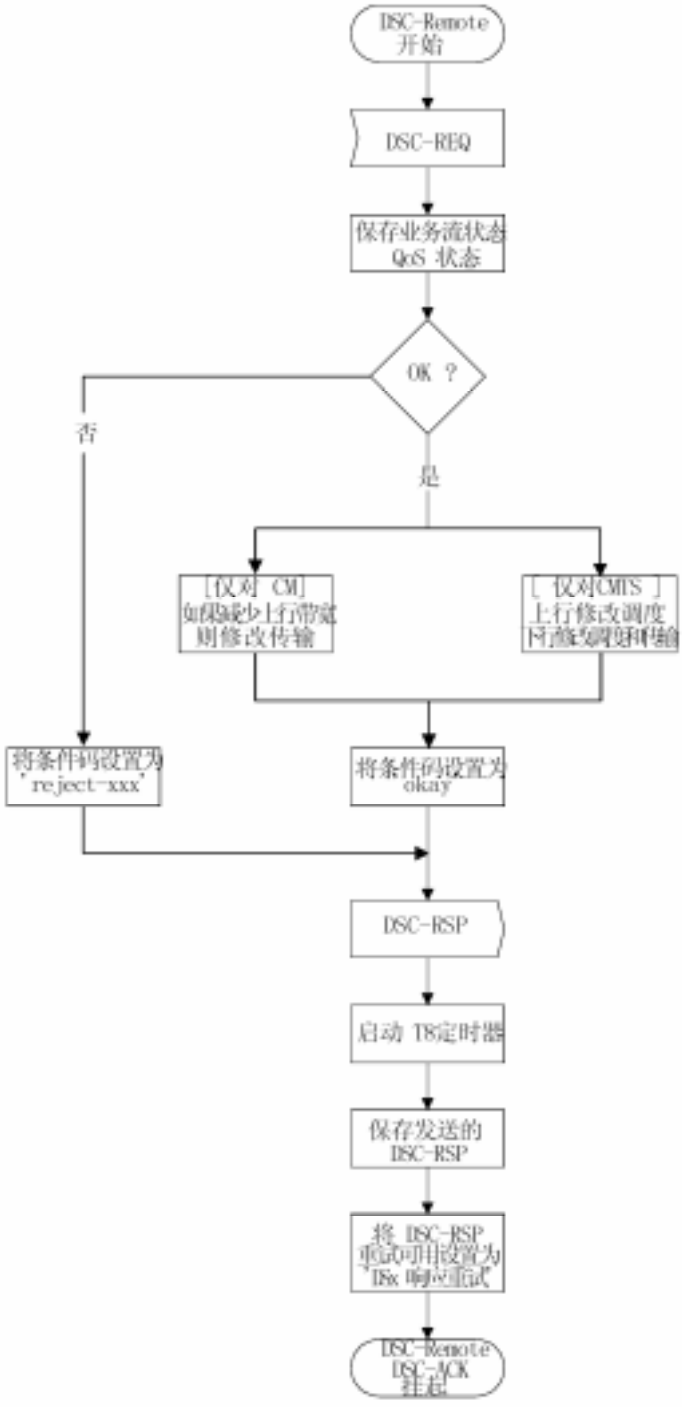


图126　DSC –远地发起的事务开始状态流程图

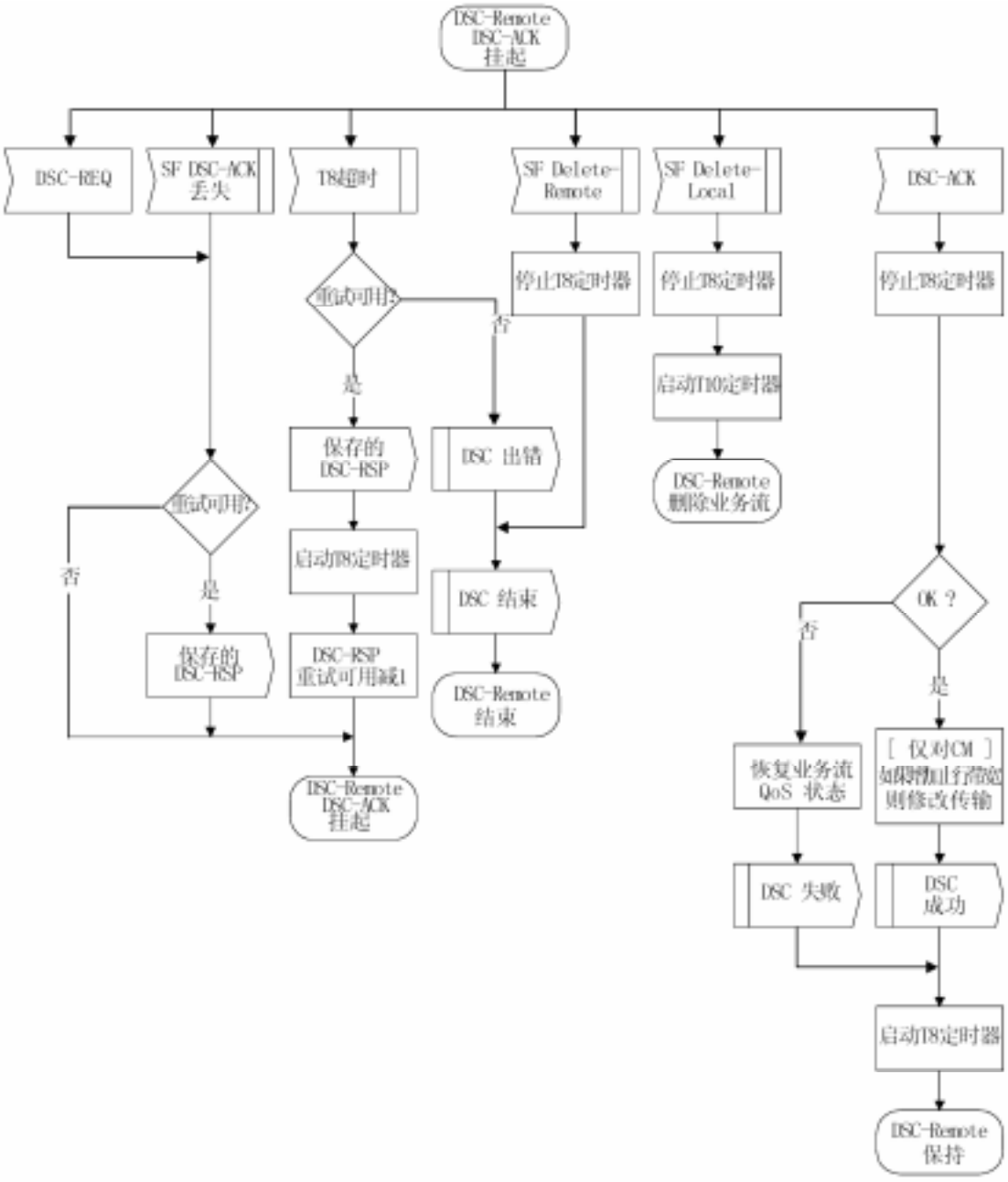


图127　DSC –远端发起的事务 DSC-ACK 挂起状态流程图

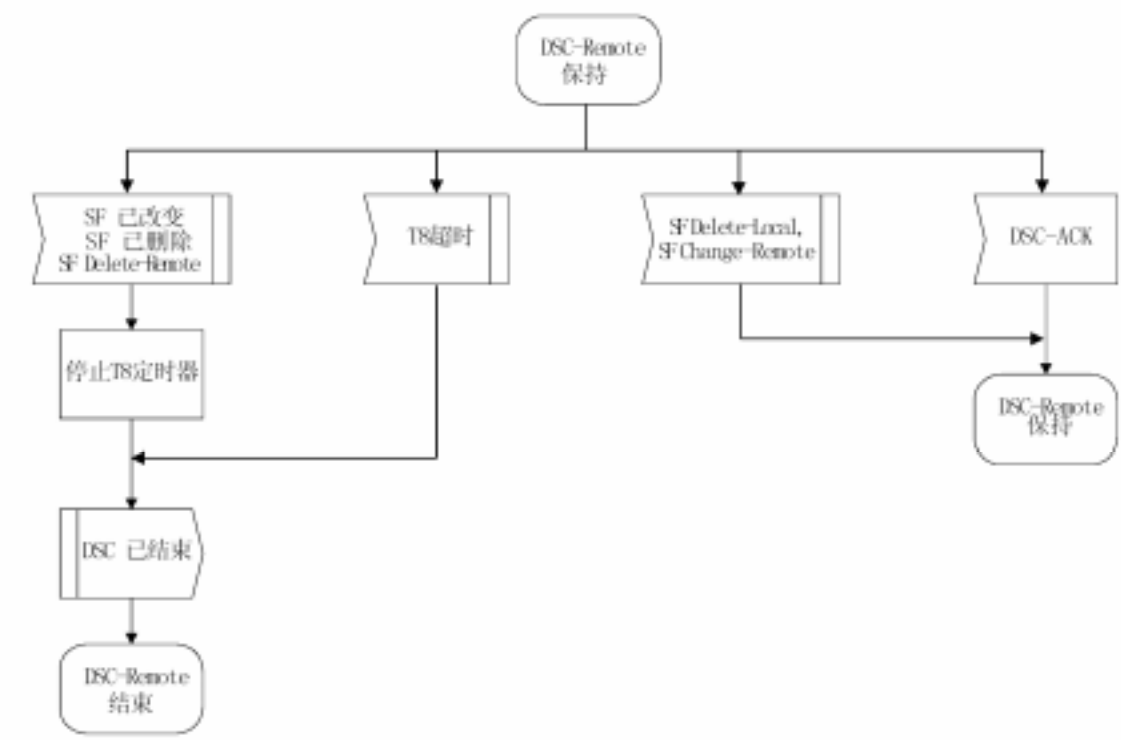


图128　DSC –远端发起的事务保持状态流程图

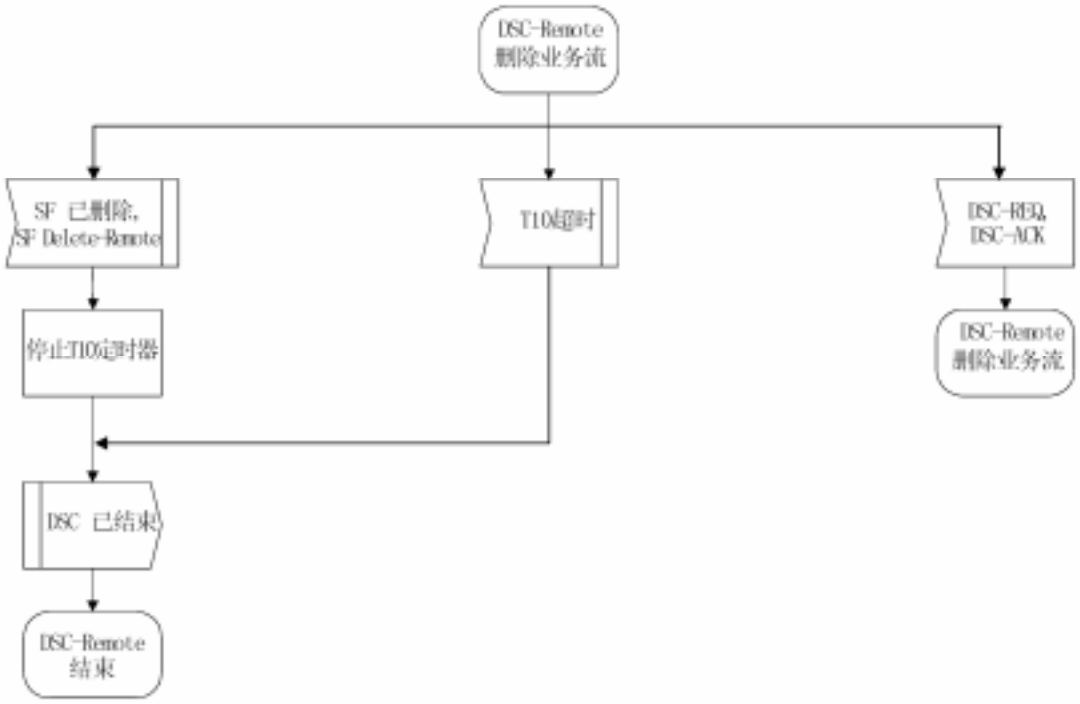


图129　DSC—远端发起的事务删除业务流状态流程图

10.4.4　动态业务删除

任何业务流都能够用动态业务删除（DSD）消息来删除。当一个业务流被删除的时候，所有与它相关联的资源都被释放，包括分类器和PHS。然而，如果一个CM的基本业务流被删除，则该CM就被撤销注册，并且应重新注册。此外，如果一个在注册期间曾被预置的业务流被删除，则在该CM重新注册之前，该业务流的预置的信息将会丢失。然而，预置的业务流的删除不应引起CM重新注册。所以在删除这样的业务流之前应当十分小心。

10.4.4.1　CM 发起的动态业务删除

删除一个上行和/或下行业务流的CM使用DSD-REQ产生一个向CMTS的删除请求。CMTS取消该业务流并使用DSD-RSP产生一个响应。每个DSD请求只能删除一个上行和/或下行业务流。见图130。

CM		CMTS
业务流不再需要 删除业务流		
发送DSD-REQ	--------- DSD-REQ ---------->	接收DSD-REQ 验证CM是业务流的“所有者” 删除业务流
接收DSD-RSP	<---------- DSD-RSP ---------	发送DSD-RSP

图130　CM 发起的动态业务删除

10.4.4.2　CMTS 发起的动态业务删除

删除一个上行和/或下行业务流的CMTS使用DSD-REQ产生相关CM的删除请求。该CM取消此业务流并使用DSD-RSP产生响应。每个DSD请求只能删除一个上行和/或下行业务流（见图131）。

CM		CMTS
		业务流不再需要 删除业务流 确定与此业务流有关的 CM
接收DSD-REQ	<--------- DSD-REQ ----------	发送DSD-REQ
删除业务流		
发送DSD-RSP	---------- DSD-RSP --------->	接收DSD-RSP

图131　CMTS 发起的动态业务删除

10.4.4.3　动态业务删除状态转变图

动态业务删除状态转变图见图132至图136。

图132　DSD –本地发起的事务开始状态流程图

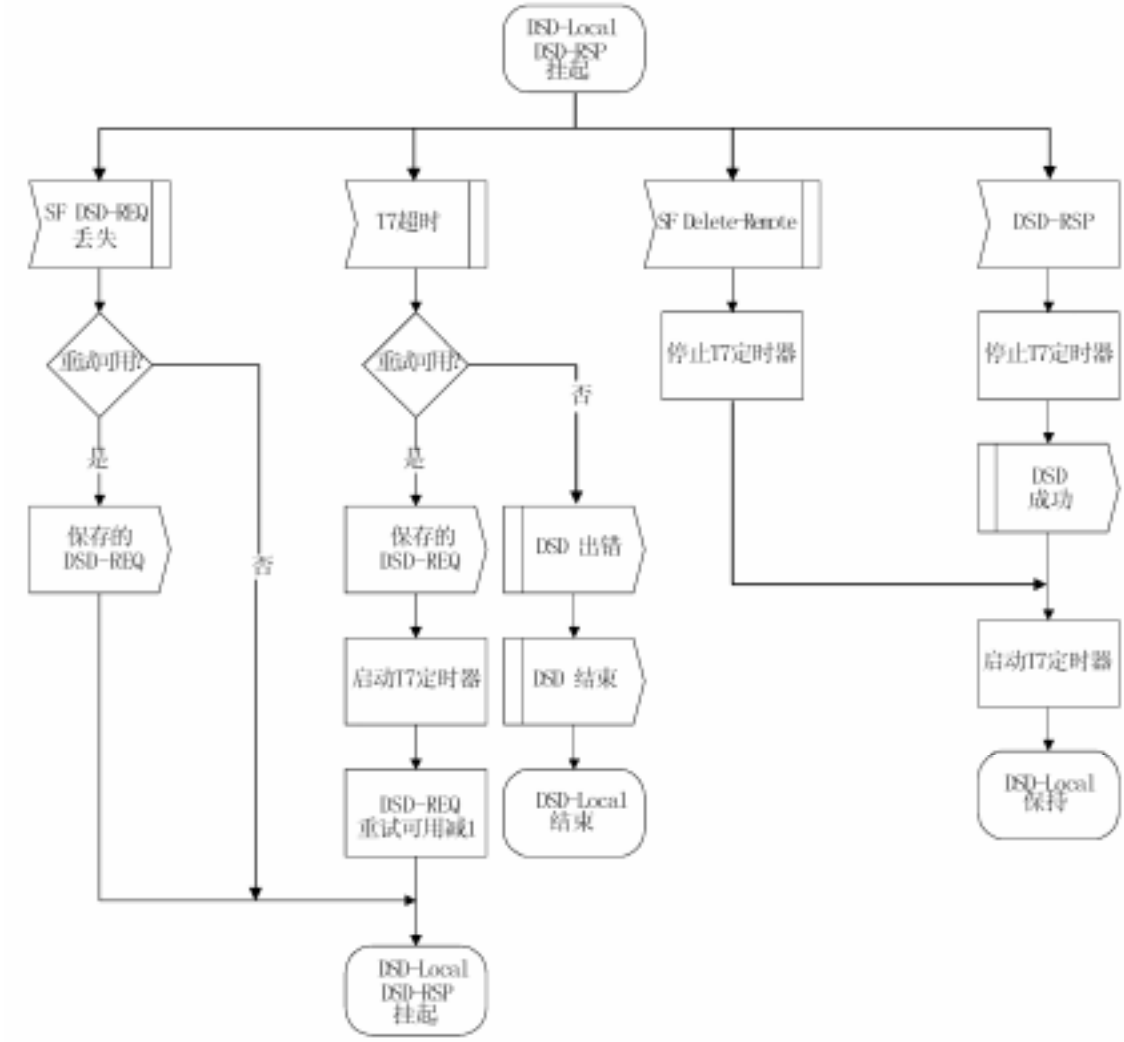


图133　DSD —本地发起的事务 DSD-RSP 挂起状态流程图

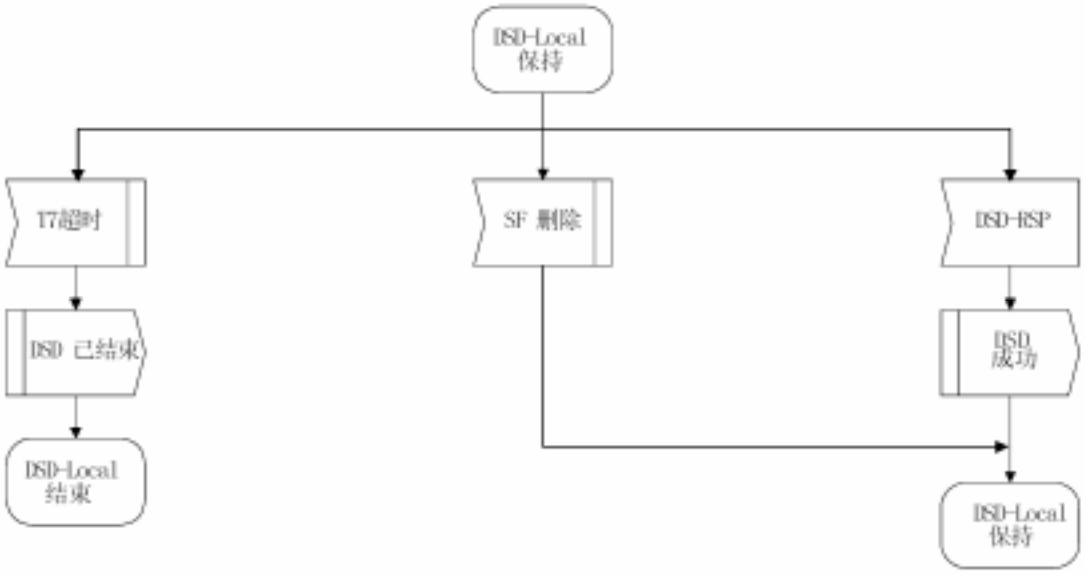


图134　DSD —本地发起的事务保持状态流程图

图135　DSD –远端发起的事务开始状态流程图

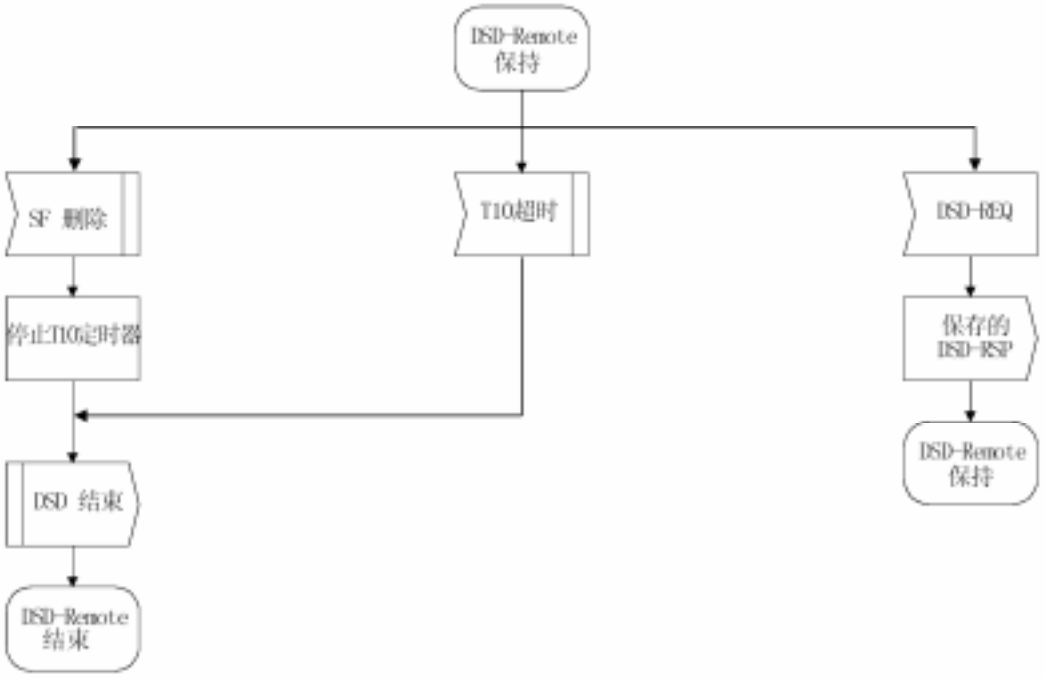


图136　DSD –远端发起的事务保持状态流程图

10.4.5　动态变更下行和/或上行信道

10.4.5.1　DCC 一般操作

在注册后的任何时候，CMTS可能会指导CM来变更下行和/或上行信道。这可能为了均衡流量、规避噪声，或其它超出本部分范围的原因。图138和图139所示为CMTS应遵循的步骤。图140和图141所示为CM应遵循的步骤。

DCC命令用于变更上行频率、变更下行频率，或上行频率和下行频率都变更。当仅变更上行频率或仅变更下行频率时，该变更通常是在一个MAC域内。当上行频率和下行频率两者都变更时，该变更可能是在一个MAC域内，或是在MAC域之间。

上行信道ID在新旧信道都应是唯一的。在这里，旧信道是指CM在变更之前的信道，而新信道则为CM在变更之后的信道。

在与新上行和/或下行信道同步以后，CM应使用在DCC-REQ初始化技术TLV中规定的技术，如果该TLV存在，则可决定是否应进行重新初始化、仅做测距，或两者都不进行。如果该TLV在DCC-REQ中不存在，则CM应在新的指配信道上重新初始化MAC（见10.2）。如果要求CM重新初始化，则CMTS不必等待新的信道上的DCC-RSP。

如果CM在一个MAC域内切换，则可能不需要重新初始化，如果CM在MAC域之间移动，则可能需要重新初始化。如需要，则进行重新初始化，以获得上行参数、建立IP连接、建立日期时间、传递工作参数和注册。如果进行重新初始化，CM不应在新信道上发送DCC-RSP。

对重新测距的决定，是基于CMTS对任何信道差异的识别，这种差异可能存在于新旧信道之间，或是上行、下行信道的任何主要参数，诸如符号率、调制类型，或微时隙长度变化时。

当DCC-REQ不包含重新初始化或重新测距时，CM的设计目标通常是将用户通信中断时间减到最小。为了达到这个目标，CM可以在接收一个DCC-REQ之后并在实际执行信道更改之前，在其当前的信道上选择继续使用QoS资源（如带宽授权），这时CM也可能需要在变更信道之前刷新内部队列或复位状态机。

在发送一个DCC-RSP（离开）消息之后和变更之前,CM可以在旧信道上继续使用QoS资源，它包括发送和接收数据包。在变更之后和发送一个DCC-RSP（到达）消息之前，CM可以在新信道上使用QoS资源，

它包括发送和接收数据包。CMTS不应在旧信道上使用DCC-RSP（离开）消息来回收QoS资源。在容许QoS资源使用之前CMTS不必在新信道上等待DCC-RSP（到达）。这样就保证了主动授权业务在变更信道过程中能在新旧信道上的通信中断时间最小。

CMTS应在当前的信道上保持QoS资源，直到上一个DCC-REQ发送后T13超时，或直到它能在新的指配信道上根据本地信息确认CM存在。CM应在T13超时之前实现从旧信道离开并到达新信道，不必重新初始化。CM可以在响应DCC-RSP之后和T13超时之前在当前的信道上继续使用QoS资源。

一旦CM变更信道，以前所有通过请求IE或请求/数据IE发出的未完成的带宽请求都无效,CM应在新信道上重新请求带宽。在上行中的主动授权业务的情况下,授权是隐含在QoS资源预留中的,并不需要重新请求。

10.4.5.2 DCC 例外情况

如果CM发出DSA-REQ或DSC-REQ以请求更多资源，而CMTS需要执行DCC以得到那些资源，则CMTS将拒绝DSA或DSC指令，不分配任何资源给CM。CMTS在DSC-RSP消息中包括“reject –temporary-DCC”的确认码（见C.1.3.1）来表明在收到DCC之前新的资源将不可用，直到接收到一个DCC。然后在DSA或DSC事务之后，CMTS发起DCC事务。

在CM变更到一个新信道并完成DCC事务后，CM要重试DSA或DSC指令。如果CM在T14超时之后没有更改信道，T14从CM收到来自CMTS的DSA-RSP或DSC-RSP的时刻算起，CM可能重试资源请求。

如果CMTS需改变信道，以满足除CM发起DSA或DSC指令之外的资源请求，则CMTS应首先执行DCC命令，然后发出DSA或DSC指令。

如果CMTS发送重新初始化的DCC，则配置文件能使CM返回到原来的信道，这会造成死循环。为防止这种情况，如果预置系统缺省是指定上行信道ID和/或下行频率，则CMTS应不使用带有重新初始化选项的DCC-REQ。

如果CMTS已事先发出DSA或DSC指令，且该指令仍未完成，则CMTS不应发出DCC指令。如果CMTS仍在等待来自发起DSA-REQ或DSC-REQ指令的CM的DSA-ACK或DSC-ACK，则CMTS不应发出DCC指令。

如果CMTS已先发出DCC指令，且该指令仍未完成，则CMTS不应发出DSA或DSC指令。

如果CMTS发出DCC-REQ，且CM同时也发出DSA-REQ或DSC-REQ，则以CMTS的指令优先。CMTS以“reject-temporary”的确认码响应（见C.1.3.1），CM继续执行DCC指令。

如果CM不能在新的信道上实现与CMTS的通信，则CM应回到以前的信道并重新初始化MAC。这个以前指配的信道代表着一个已知的好运行点，它可以加速重新初始化过程。回到以前的信道对于CMTS找到在新信道上连接失败的CM提供了更健壮的运行环境。

如果CMTS发送了DCC-REQ，且在T11时间内没有接收到DCC-RSP，则它应在宣布事务失败以前重新发送DCC-REQ，直到“DCC-REQ Retries”的最大值（见附录B）。如果DCC-RSP在发送中丢失，且CMTS重试DCC-REQ，则CM可能已经变更了下行信道。

如果CM在新的信道上发送了DCC-RSP，且在T12时间内没有接收到从CMTS来的DCC-ACK，则CM应重试DCC-RSP，直到“DCC-ACK Retries”的最大值（见附录B）。

如果CM接收到的DCC-REQ带有上行信道ID TLV（如果存在，则等同于当前的上行信道ID）和下行频率TLV（如果存在，则等同于当前的下行频率），则CM应把该DCC-REQ考虑为冗余的指令。剩余的DCC-REQ TLV参数不被执行，且CM应以“reject-already-there”的确认码返回DCC-RSP给CMTS（见C.4.1）。

10.4.5.3 准无缝信道变更

当CMTS希望给CM添加新的QoS预留时，为此它可能需要将CM转移到新的上行和/或下行信道。在信道变更期间，对现行的QoS业务诸如IP电话和视频会议，最好是将中断时间减到最小。这种准无缝信道变更是DCC指令的首要设计目标。CMTS和CM可以支持准无缝信道变更。

以下动作是为完成一个准无缝信道变更的建议操作步骤。假定上行和下行信道两者正在变更。如果只有上行或下行信道变更，则应用所列的子集。

为支持准无缝信道变更，应在网络中应用如下条件：

- 对于新的上行和下行信道的物理层参数相对于旧的上行和下行信道将不变更。下行参数变更使测距参数无效；
- 测距参数将不在新旧信道之间变更，这可能要求对称的电缆网和设备条件；
- CMTS 对所有下行信道应使用相同的时戳和 SYNC 机制；
- 应配置 IP 路由，使 CM 及其相连的 CPE 能继续使用它们现行的 IP 地址。可避免中断 RTP 会话或其它进行中的应用。

为实现准无缝信道变更，CMTS：

- 应在发送 DCC-REQ 之前，在新旧信道上复制与 CM 所有相关的 QoS 预留；
- 应在发送 DCC-REQ 之前（对下行信道变更）复制下行数据包流，在新旧信道上传给 CM；
- 如果新旧下行信道使用相同的时戳，则应至少在 T13 期间在旧的下行信道上发送对于新的上行信道的 MAP 消息。（如果 CM 不能缓存旧下行信道上发送的新上行 MAP，则信道变更延时需要加上将来产生 MAP 的时间量。这样 CMTS 应制止比其将来需要的更长的 MAP 调度）；
- 在 CM 变更前应规定新的下行和上行参数；
- 应规定在新信道上不等待 SYNC 消息；
- 应规定跳过初始化（在 10.2 定义）；
- 应规定跳过初始维护和台站维护；
- 应管理新旧业务流替代，包括 SID、SAID、SFID、分类器 ID、有效负载包头抑制索引及所要求的主动授权时间参考。业务分类名称应在新旧信道之间保持相同。

为实现准无缝信道变更，CM：

- 应在 DCC-RSP 消息中应答估计的 CM 跳变时间；
- 应在旧的下行信道上监听并存储应用于新的上行信道的 MAP 消息，这应在 T13 期间来做；
- 当跳变时，应用 DCC 命令中的下行参数和缓存中的 UCD 消息来迫使加速物理层会聚；
- 如果 CMTS 允许，应在 PHY 会聚之后和发送之前不等待 SYNC 消息；
- 如果可用，应使用缓存的 MAP，以快速启动；
- 直到跳变瞬间前和紧接新信道重新同步之后，在两个方向中允许传送连续流，使两个方向上通信的中断时间最小；
- 应在跳变期间将到达的数据包排队，并在跳变之后发送它们；
- 当引起上行主动授权业务排队超过其限制时，应在跳变之后丢掉 VoIP 包，如没有超过则不必要。

该应用能处理可能发生在CM变更信道期间的包丢失。

10.4.5.4 操作举例

DCC的使用和与其它MAC消息的关系示例见图137。本例描述了CM以DSA消息尝试分配新资源的一种情况。CMTS临时拒绝请求，通知CM变更信道，然后CM重新请求资源。该例（不包括所有例外情况）描述如下（见10.2）：

a) 一个事件发生，诸如 CM 发出一个 DSA-REQ 消息；
b) CMTS 为服务该资源请求，决定其需要变更信道。CMTS 用 DSA-RSP 消息响应，它包含“ reject-temporary-DCC ”的确认码（见 C.1.3.1），以表明没有可用的新资源，直到接收到 DCC。CMTS 拒绝任何后续的 DSA 或 DSC 消息，直到 DCC 指令被执行；
c) 在新的上行和/或下行信道上 CMTS 发起 QoS 预留。QoS 预留包括新的资源分配，以及当前指定给 CM 的资源。在该例中，上行和下行信道都被变更；
d) 由于 CMTS 不能确认 CM 将切换信道的时刻，为了实现准无缝信道变更，CMTS 要在新旧下行信道上复制数据包流；
e) CMTS 发出 DCC-REQ 给 CM；
f) CM 发送 DCC-RSP（离开）。然后 CM 清除队列和状态机，并变更信道；

g) 如果发生下行信道变更，则 CM 要同步到 QAM 符号定时、FEC 组帧和 MPEG 组帧；
h) 如果 CM 已得到指示重新初始化，它使用新的上行和/或下行信道执行。CM 从这里表述的事件流退出，并从识别下行 SYNC 消息开始进入在 10.2 中表述的事件流；
i) CM 搜索 UCD 消息，除非它已有先前的拷贝；
j) CM 等待下行 SYNC 消息，除非它已得到指令不用等待；
k) CM 收集 MAP 消息，除非在其缓存中已有可用的消息；
l) CM 进行初始维护和台站维护，除非已得到指示跳过它们；
m) CM 以其新的资源分配恢复正常的数据传输；
n) CM 发送 DCC-RSP（到达）消息给 CMTS；
o) CMTS 以 DCC-ACK 响应；
p) CMTS 回收旧信道上的 QoS 预留。如果下行数据包流已被复制，则清除旧下行信道上的复制包；
q) CM 重新发出 DSA-REQ 指令；
r) CMTS 保留请求资源并用 DSA-RSP 响应；
s) CM 以 DSA-ACK 结束。

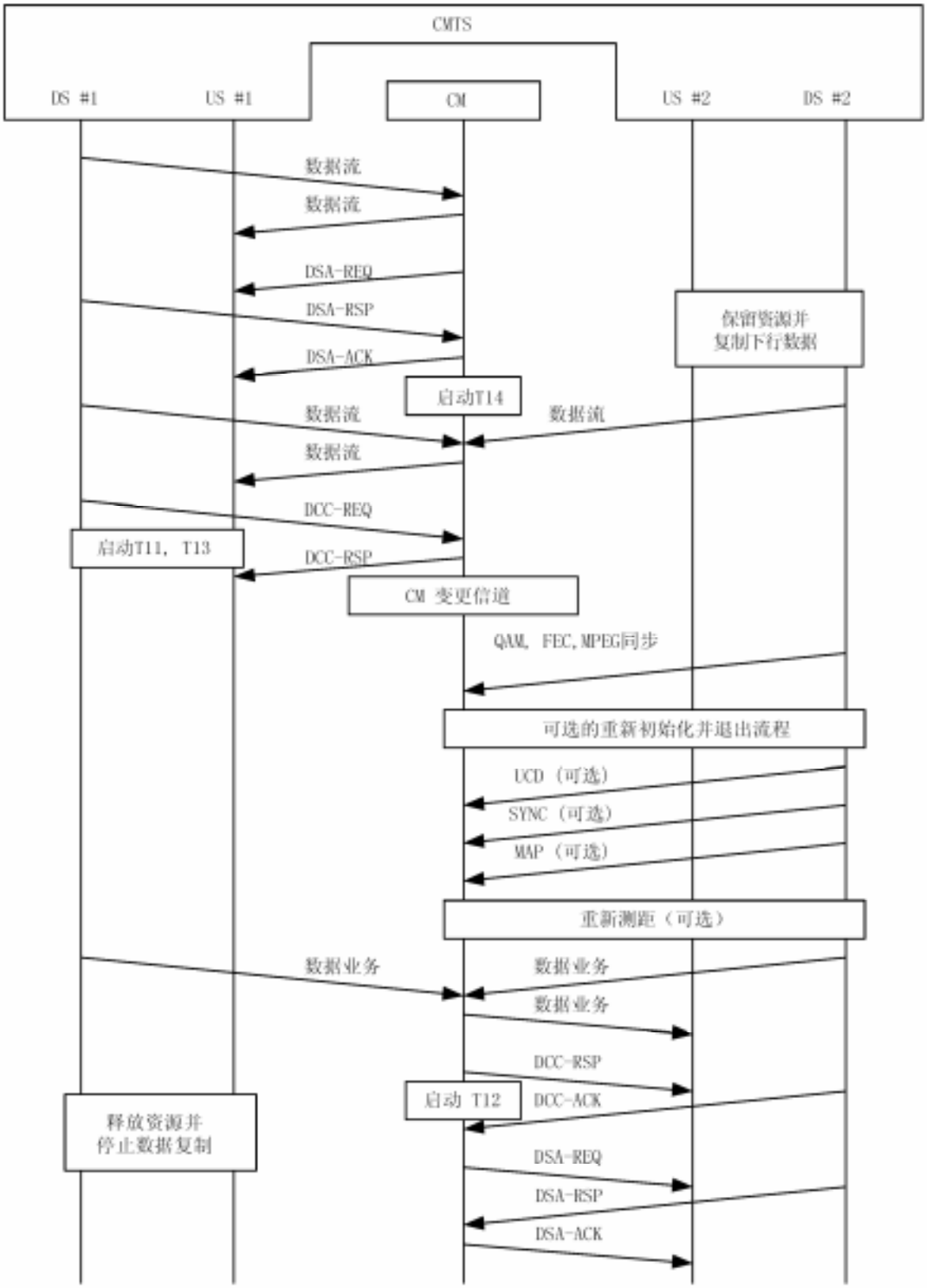


图137　DCC 操作流程示例

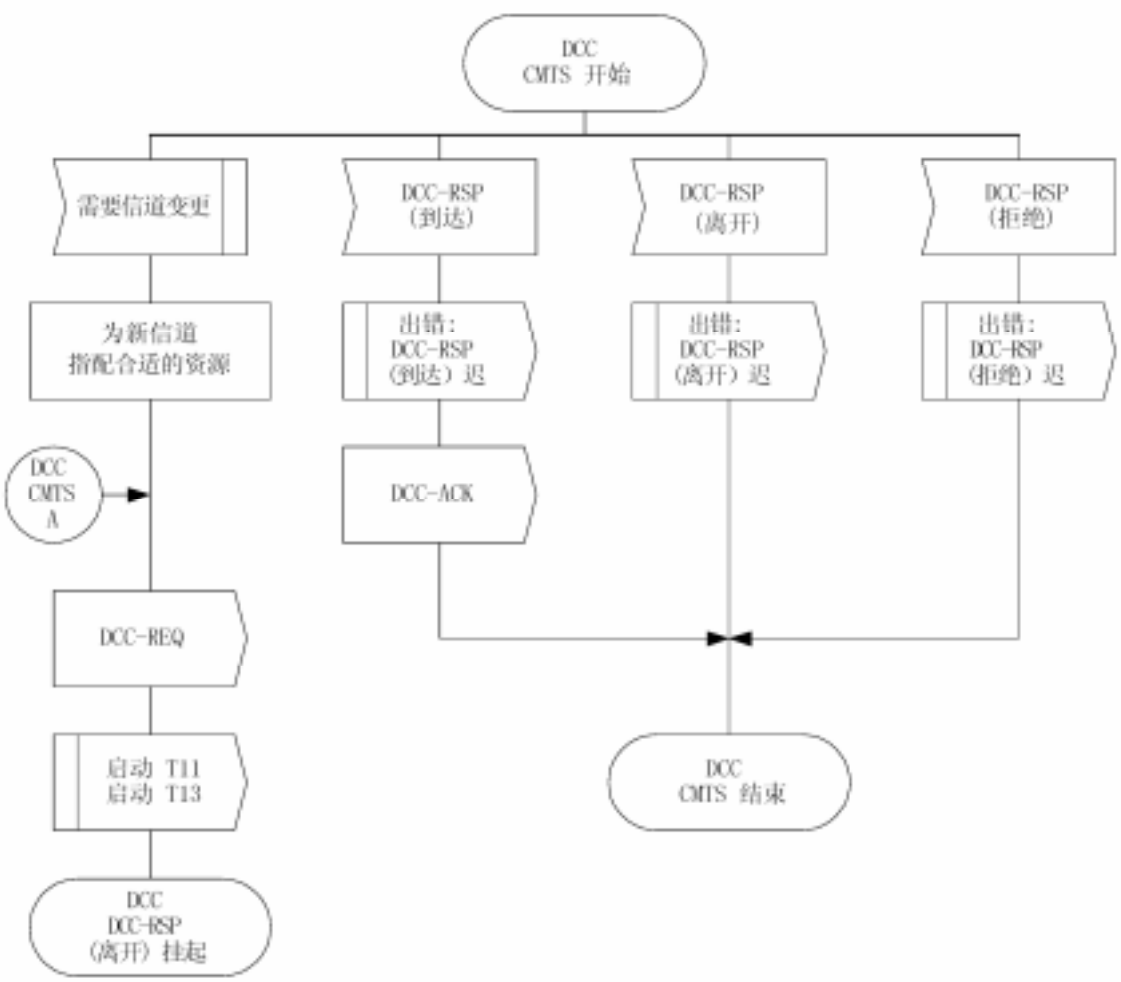


图138　动态变更信道—CMTS：部分 1

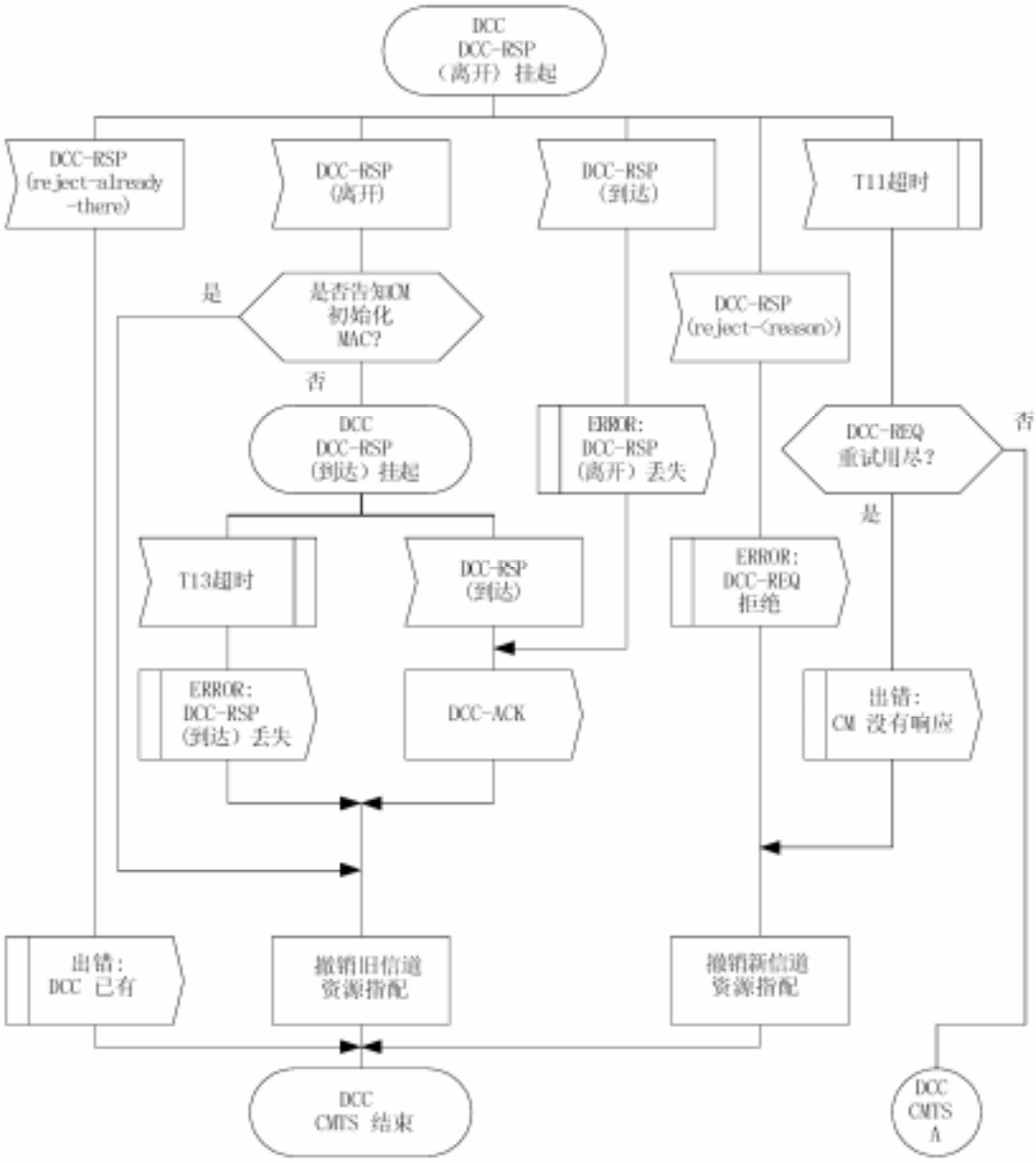
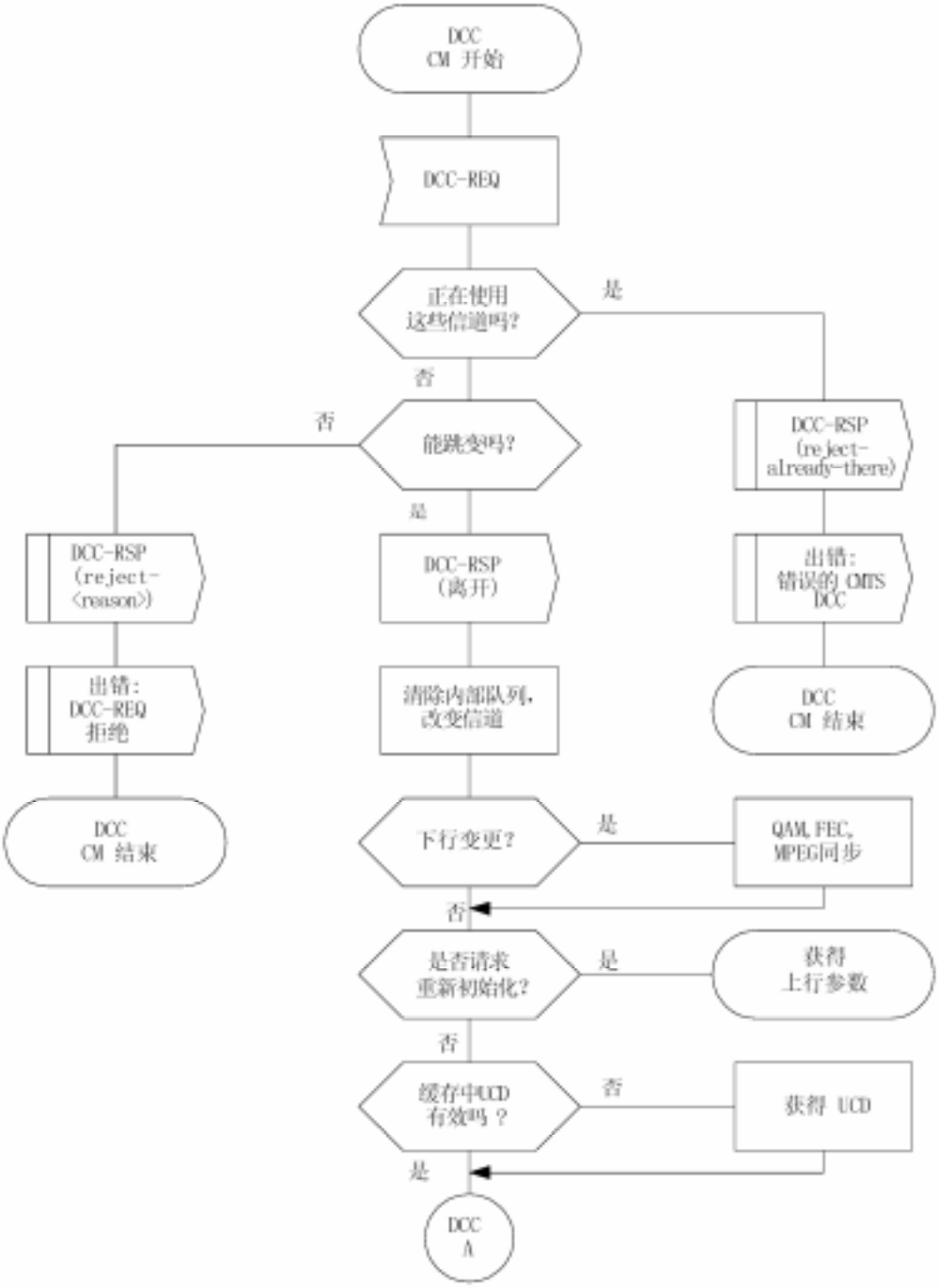


图139　动态变更信道—CMT：部分２



注： 状态“ 获得上行参数 ”连到图81中的状态机。

图140　动态变更信道—CM：部分 1

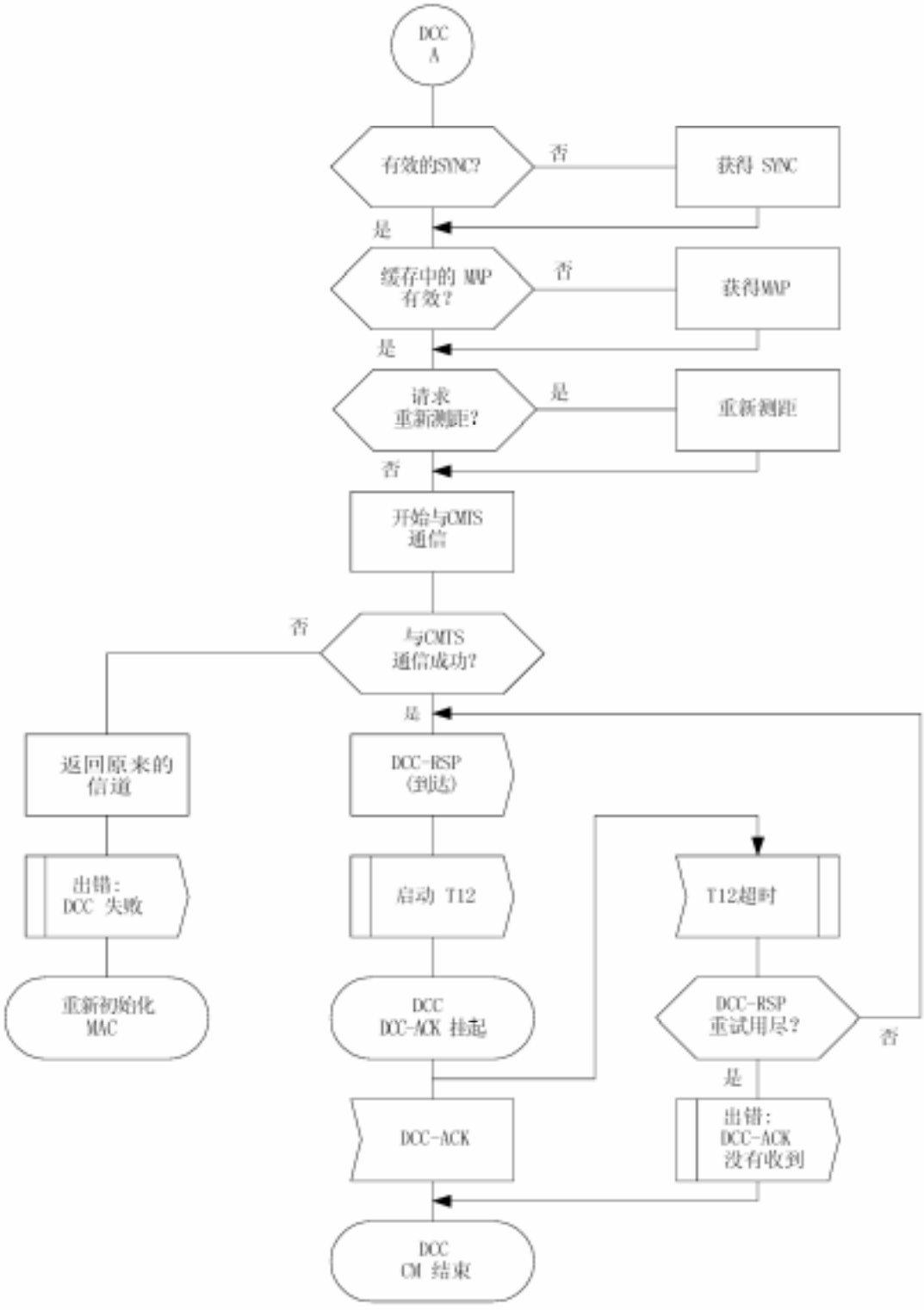


图141　动态变更信道—CM：部分 2

10.5　故障检测和恢复

故障检测和恢复在多个层次上发生：

- 在物理层，使用 FEC（前向纠错）来纠正可能的错误，见第 5 章；
- MAC 协议通过使用 MAC 包头和包的数据部分的校验和来避免发生错误，见第 7 章；

- 所有的 MAC 管理消息都通过覆盖整个消息的 CRC 校验来避免发生错误，见第 7 章。任何发生 CRC 错误的消息都应由接收方丢弃。

表46表示出各种特定类型的MAC消息丢失之后应采取的恢复过程。

表46　特定的 MAC 消息丢失时的恢复过程

消息名称	消息丢失后的动作
SYNC	CM在失去与网络的同步之前能够在丢失SYNC间隔的时间内丢失SYNC消息（见附录B）。失去同步的CM不应使用上行信道，并且应尝试重新建立同步。
UCD	在CM初始化期间，CM应在上行发送前接收一个可用的UCD[a]。当在CM初始化过程的“获得上行参数”状态中时，如果CM在T1超时前没有收到可用的UCD，则CM不应在上行发送数据，且应搜索另一个下行信道。在接收可用的UCD后，每当CM接收不可用的UCD或带有UCD计数的MAP，而该计数又不符合已收到的上一个UCD的配置变更计数时，CM不应在上行发送，并应启动T1定时器。如果在这些情况下，T1定时器超时，则CM应复位并重新初始化MAC。
MAP	在没有有效的上行带宽分配时，CM不应传送。如果由于出错而错过MAP，则在该MAP所覆盖的期间内CM不应传送。
RNG-REQ RNG-RSP	如果CM在发送了一个请求之后，在规定的超时间隔内没有接收到有效的测距响应，则应重试若干次请求（见附录B）。如果经过规定次数的尝试之后仍然不能够接收到有效的测距响应，则CM应复位并重新初始化MAC。
REG-REQ REG-RSP	如果CM在发送了一个请求之后，在规定的超时间隔内没有接收到有效的注册响应，则应重试若干次请求（见附录B）。如果经过规定次数的尝试之后仍然不能够接收到有效的注册响应，则CM应复位并重新初始化MAC。
UCC-REQ UCC-RSP	如果CMTS在发送了一个请求之后，在规定的超时间隔内没有接收到有效的上行信道变更响应，则应重试若干次请求（见附录B）。如果经过规定次数的尝试之后仍然不能接收到有效的响应，则CMTS应认为该CM不可达。
a：可用的UCD是CM能理解的合法特性表。在考虑UCD可用性时，CM要求接收到的MAP的UCD计数与上一个接收到UCD的配置变更计数相匹配。	

MAC子层把网络层及其上层的消息认为是数据包。这些消息受到数据包的CRC域的保护，并且要丢掉任何CRC出错的数据包。这些丢掉的数据包的恢复按照上层协议进行。

避免未授权传送

当检测到自己的载波已经持续超过最长可能的有效传送时间时，CM应当有办法结束RF传输。

11　支持未来新 CM 的能力

下载CM操作软件

CMTS应能通过网络下载软件，进行远程升级。

CM应能通过网络下载软件，进行远程升级。

下载机制应使用TFTP文件传送。这种传送应以下列任一方法来启动：

- SNMP 管理员要求 CM 升级；
- 如果在 CM 的配置文件中的软件升级文件名称和 CM 的当前软件的映像不一致，则 CM 应通过 TFTP 从软件服务器请求该规定的文件。

注：软件服务器的IP地址是一个单独的参数。如果该参数出现，CM应尝试从这个服务器下载规定的文件。如果该参数不出现，CM应尝试从配置文件服务器下载规定的文件。

CM应验证下载的软件对其自身是合适的。如果该软件是合适的，CM应将此新的软件映像写入非易失性存储器。一旦文件传送成功，CM应用新的代码重新启动。

如果由于某种原因CM不能完成此文件传送，即使在各次尝试之间供电电源或线路中断，CM也应保持接收新软件下载的能力（不需要操作员或用户的介入）。CM应记录这种失败的情况，并可以异步地向网络管理员报告。

在操作软件升级之后，CM可能需要遵照上面描述的一种步骤变更信道，以使用增强的功能。

如果CM继续工作在升级之前的上行和下行信道，则它应能够和那些可能还在运行以前软件版本的其它CM一起工作。

在软件已经升级满足新版本技术规范时，关键是CM应能够和以前版本一起工作，以允许网络上其它的CM逐步地升级。

附 录 A
（规范性附录）
常用地址

A.1 MAC地址

这里所描述的MAC地址根据以太网/GB/T 15629.3协议定义为低位在前（bit-little-endian）。

应采用以下组播地址对所有CM的MAC子层进行寻址。例如，传送分配MAP PDU时地址为01-E0-2F-00-00-01。地址范围01-E0-2F-00-00-02至01-E0-2F-00-00-0F被保留为将来使用，被指定为这些地址的帧不会被转发至MAC子层域之外。

A.2 MAC SID

A.2.1 所有CM和非CM SID

在MAP中使用这些SID以达到特定目的或表明任何CM能够在相应的时间间隔内做出响应。

0x0000 不发给任何CM。一般当改变上行突发参数时会用到，使CM在新的上行设置生效前有时间去调节自己的调制器。CM初始测距期间也可以用作初始化SID。

0x3FFF 发给所有CM。一般用于广播请求时间间隔或初始维护时间间隔。

A.2.2 常用“组播”SID

该组标识符仅用于请求/数据信息单元。它们指明任何CM均能在一个给定的时间间隔内对该组标识符做出响应，但应把传输长度限定为特定的微时隙数（由分配给该间隔的特定组播SID来说明）。

0x3FF1-0x3FFE 发给所有CM。对所有的短数据PDU和请求（仅用于请求/数据信息单元）有效。最后一位数字说明了帧长度和传输机会，具体如下：

- 0x3FF1 在指定的时间间隔中，发送可以从任意微时隙开始，并只能用一个微时隙的长度；
- 0x3FF2 在指定的时间间隔中，发送可以从任意相隔一个的微时隙开始，并且只能用两个微时隙的长度（例如，在这个时间间隔内台站可以从第 1 个微时隙开始发送，可以从第 3 个、第 5 个……微时隙开始）；
- 0x3FF3 在指定的时间间隔中，发送可以从任意相隔两个微时隙开始，并且只能用 3 个微时隙的长度（例如，从第 1 个、第 4 个、第 7 个……微时隙开始）；
- 0x3FF4 从第 1 个、第 5 个、第 9 个……微时隙开始；
  ……
- 0x3FFD 从第 1 个、第 14 个、第 27 个……微时隙开始；
- 0x3FFE 在指定的时间间隔中，发送可以从任意第 14 个微时隙开始，并且只能用 14 个微时隙的长度。

A.2.3 优先级请求SID

SID（0x3Exx）保留用于请求IE（见C.2.2.5.1），其他优先级请求SID见表A.1。

表A.1优先级请求SID

SID值	优先级
0x01	0
0x02	1
0x04	2
0x08	3
0x10	4
0x20	5
0x40	6
0x80	7

这些比特位可以由CMTS上行请求IUC的调度器按需组合。

A.3 MPEG PID

所有数据都应在包头PID域为0x1FFE的MPEG-2包中传送。

附 录 B
（规范性附录）
参数与常量

见表B.1。

表 B.1 参数与常量

系统	名称	时间参考	最小值	缺省值	最大值
CMTS	Sync Interval	SYNC 消息之间的标称时间间隔（见 7.3.2）			200ms
CMTS	UCD Interval	UCD 消息之间的时间间隔（见 7.3.3）			2s
CMTS	Max MAP Pending	允许 CMTS 在将来分配的最大微时隙数（见 7.3.4）			4096 个微时隙时间
CMTS	Ranging Interval	广播测距请求之间的时间间隔（见 8.3.3）			2s
CM	Lost Sync Interval	最后一次收到 SYNC 消息到同步被认为丢失之间的时间			600ms
CM	Contention Ranging Retries	争用测距请求重试的次数（见 10.2.4）	16		
CM CMTS	Invited Ranging Retries	邀请测距请求重试的次数	16		
CM	Request Retries	带宽分配请求的重试次数	16		
CM CMTS	Registration Request /Response Retries	注册请求/响应重试的次数	3		
CM	Data Retries	直接数据发送的重试次数	16		
CMTS	CM MAP processing time	CM 收到 MAP 帧的最后一位到该 MAP 帧生效之间的时间(见 8.1.1)	200μs		
CMTS	CM Ranging Response processing time	收到一个测距响应后，在 CM 对受邀测距请求作出应答前，给 CM 的最小时间	1ms		
CMTS	CM Configuration	从收到配置文件后，到向 CMTS 发送注册请求前，给 CM 的最大时间	30s		
CM	T1	等待 UCD 超时			5xUCD 间隔最大值
CM	T2	等待广播测距超时			5x 测距间隔
CM	T3	等待测距响应	50ms	200ms	200ms
CM	T4	等待单播测距机会，如果 pending-till -complete 域以前被这个 CM 使用，那么这个域的值应加到这个时间间隔中	30s		35s
CMTS	T5	等待上行信道变更响应			2s
CM CMTS	T6	等待注册响应和注册确认			3s
CM CMTS	Mini-slot size	上行传输的微时隙值。应为 2 的幂（以时间节拍为单位）	32 个符号时间		

表B.1 参数与常量（续）

系统	名称	时间参考	最小值	缺省值	最大值
CM CMTS	Timebase Tick	系统定时单位	6.25μs		
CM CMTS	DSx Request Retries	DSA/DSC/DSD 请求重试超时次数	3		
CM CMTS	DSx Response Retries	DSA/DSC/DSD 响应重试超时次数	3		
CM CMTS	T7	等待 DSA/DSC/DSD 响应超时			1s
CM CMTS	T8	等待 DSA/DSC 确认超时			300ms
CM	TFTP Backoff Start	TFTP 退避初始值	1s		
CM	TFTP Backoff End	TFTP 退避结束值	16s		
CM	TFTP Request Retries	TFTP 请求重试次数	16		
CM	TFTP download Retries	TFTP 完全下载重试次数	3		
CM	TFTP Wait	TFTP 重试序列之间的等待时间	10min		
CM	ToD Retries	每个 ToD 重试时段内的重试次数	3		
CM	ToD Retry Period	TFTP 重试时段时间	5min		
CMTS	T9	注册超时，CMTS 成功地向一个 CM 发送 RNG-RSP 消息与收到来自该 CM 的 REG-REQ 消息之间的时间	15min	15min	
CM CMTS	T10	等待事务结束超时			3s
CMTS	T11	等待旧信道上的 DCC 响应			300ms
CM	T12	等待 DCC 确认			300ms
CMTS	T13	用于 DCC 的 QoS 资源的最大保持时间			1s
CM	T14	DSx reject-temp-DCC 和下一个 DSx 命令重试之间的最小时间	2s		
CMTS	DCC-REQ Reties	动态信道变更请求的重试次数	3		
CM	DCC-RSP Reties	动态信道变更响应的重试次数	3		
CM	Lost DCI-REQ Interval	从发送 DCI-REQ 到没有收到 DCI-RSP 的时间			2s
CM	DCI-REQ retry	重启之前的 DCI-REQ 重试次数			16

表B.1 参数与常量（续）

系统	名称	时间参考	最小值	缺省值	最大值
CM	DCI Backoff Start	DCI 退避初始值	1s		
CM	DCI Backoff end	DCI 退避结束值	16s		

附 录 C
（规范性附录）
公用射频接口编码

C.1 配置和MAC层消息的编码

下列类型/长度/值（TLV）编码应用于配置文件（见附录D）、CM注册请求和动态业务消息中。所有的多字节都按网络字节顺序传送，即首先发送包含MSB的字节。

CM应支持以下配置设定。

C.1.1 配置文件和注册设置

这些设置可以在配置文件中找到，如果存在，应在注册请求中由CM发送给CMTS。

C.1.1.1 下行频率配置设定

CM使用的接收频率。在搜索下行信道期间，它替代已选择的信道的频率。它表示下行信道的中心频率，以Hz为单位，以32位二进制数存储。

类型	长度	值
1	4	接收频率

有效范围：接收频率应是62500Hz的整数倍。

C.1.1.2 上行信道ID配置设定

CM应使用的上行信道ID。CM应监听已定义的下行信道直到发现带有该ID的上行信道描述符消息。在初始化期间，它替代已选择的信道。

类型	长度	值
2	1	信道ID

C.1.1.3 网络接入控制对象

如果该域值为1，在CM预置的基础上，则允许与该CM相连的CPE接入网络。如果该域值为0，则不准从与之相连的CPE向RF MAC网络转发业务，而应继续接收并产生来自CM自身的业务。该域的值不会影响CMTS业务流操作，也不会影响CMTS数据转发操作 。

类型	长度	值
3	1	1或0

“ NACO=0 ”表示CM并不从与之相连的CPE向HFC网络转发业务。（CPE是与CM相连的客户设备，不管这种连接是如何实现的。）然而，当NACO=0时，对CM的业务管理并不受限制。当NACO关闭时，CM仍然是可管理的，包括发送/接收管理业务，如（但并不局限于此）：

- ARP：允许 CM 解析 IP 地址，使它可以响应查询或发送；
- DHCP：允许 CM 更新 IP 地址列表；
- ICMP：使能网络故障诊断工具（例如 ping，traceroute）；
- ToD：允许 CM 在启动后继续与其时钟同步；
- TFTP：允许 CM 下载新的配置文件或新的软件映像；
- SYSLOG：允许 CM 报告网络事件；
- SNMP：允许进行管理活动。

当NACO关闭时，CM的基本上行业务流、基本下行业务流仅保持对出入CM的业务管理进行操作。CMTS应可以忽略NACO的值并分配已由预置服务器授权的业务流。

C.1.1.4　EuroDOCSIS1. 0业务类别配置设定

该域定义了与EuroDOCSIS1.0业务类别有关的一些参数。任何用EuroDOCSIS1.0业务类别配置设定进行注册的CM都会被当作EuroDOCSIS1.0的CM。见7.3.8。

该域定义了与业务类别有关的参数。其中封装的类型/长度/值域有些复杂。这些封装的域定义了相关的业务类的业务参数的详细分类。定义的类型域只在业务配置设定值字符串的封装类别中有效。单个业务类别配置设定用来规定单个业务类别的参数。多个业务类别配置设定则用来规定多个业务类别参数。

类型	长度	值
4	n	

C.1.1.4.1　类别ID

该域的值指定了封装的字符串所使用的业务类别的标识符。

类型	长度	值
4．1	1	

有效范围：类别ID应在1～16的范围内。

C.1.1.4.2　最大下行速率配置设定

对于单SID CM，该域值指定了CMTS允许向其已知或已配置为映射到注册CM的CPE单播MAC地址进行转发的最大下行速率（以bps为单位）。

对于一个多SID CM，这些域的合计值指定了CMTS允许向其已知或已配置为映射到注册CM的CPE单播MAC地址进行转发的最大速率（以bps为单位）。

这是在一秒时间间隔内的PDU（包括目的MAC地址和CRC）的峰值数据率。它不包含用于广播或组播MAC地址的MAC包。CMTS应限制下行转发不超过该速率。CMTS可能延时但不能丢失超过限制的包。

类型	长度	值
4．2	4	

注：这是一个限制值，但并不保证该速率有效。

C.1.1.4.3　最大上行速率配置设定

该域值指定了CM允许向射频网络发送的最大上行速率（以bps为单位）。

它是在1s时间间隔内的PDU数据（包括目的MAC地址和CRC）的峰值速率。CM应针对相应的SID限制所有上行转发（包括争用和预留的）不超过该速率。在计算这个速率时，CM应包括用于广播或组播地址的PDU数据包。

CM要求执行最大上行速率，但不应该仅仅因为超过这个速率就丢弃上行业务。

CMTS要求所有的上行数据发送都遵守这个限制，包括以争用方式发送数据。如果CM超过了它所允许的速率，则CMTS应发出告警。

类型	长度	值
4．3	4	

该参数的目的是要CM在射频网络的输入端执行流量控制，并使CMTS进行流量监督以确保CM不超过速率限制。

CMTS可以通过以下方法来实施限制：

- 丢弃超过限制的请求；
- 延迟（通过零长度授权）授权，直到该 CM 遵守速率限制；
- 丢弃超过限制的数据包；
- 向策略监督器报告（例如使用报警机制），该监督器可以使出错的 CM 失去功能。

注： 这是一个限制值，但不保证该速率有效。

C.1.1.4.4 上行信道优先级配置设定

该域值指定了在上行信道数据传送中分配给该业务类别的相对优先级。数字越大表示优先级越高。

类型 长度 值

4．4 1

有效范围：0～7。

C.1.1.4.5 保证的最小上行信道数据速率配置设定

该域值指定了在上行信道中要保证该业务类别所需的以bps为单位的数据速率。

类型 长度 值

4．5 4

C.1.1.4.6 最大上行信道突发传送配置设定

该域值指定了上行信道中所允许的业务类别对应的最大突发传送数据（以字节为单位）。零值表示无限制。

注： 该域值不包含任何物理层开销。

类型 长度 值

4．6 2

C.1.1.4.7 业务类别加密使能

该域值在一个预置的CoS上关闭基线加密功能（BPI）。

类型 长度 关闭

4.7（=CoS_BP_ENABLE） 0

业务类别编码举例见表C.1。

表 C.1 EuroDOCSIS1.0 业务类别编码举例

类型	长度	值（子）类型	长度	值	
4	28				业务类别配置设定
		1	1	1	业务类别 1
		2	4	10 000 000	最大下行速率为 10Mbps
		3	4	300 000	最大上行速率为 300kbps
		4	1	5	回传信道优先级为 5
		5	4	64 000	保证的最小速率为 64kbps
		6	2	1 518	最大发送突发数据为 1 518 字节
4	28				业务类别配置设定
		1	1	2	业务类别 2
		2	4	5 000 000	最大转发速率为 5Mbps
		3	4	300 000	最大回传速率为 300kbps
		4	1	3	回传信道优先级为 3
		5	4	32 000	保证的最小速率为 32kbps
		6	2	1 518	最大发送突发数据为 1 518 字节

C.1.1.5 CM消息完整性校验（MIC）配置设定

该域值包含CM消息完整性校验码。它用于检验配置文件中未经授权的修改或错误。

类型	长度	值
6	16	d1、d2……d16

C.1.1.6 CMTS消息完整性校验（MIC）配置设定

CMTS消息完整性校验码。它用于检验配置文件中未经授权的修改或错误。

类型	长度	值
7	16	d1、d2……d16

C.1.1.7 最大CPE个数

在CM运行期间，通过CM可以接入的用户端设备（CPE）最大个数。CM运行期间是从CM启动到硬复位之间的时间（见4.1.2.3.1）。最大CPE数应由CM执行。

该参数不应与CM可以学习到的CPE地址个数相混淆。一个CM可以学习到的以太网MAC地址数可以达到该CM的CPE地址的最大个数（见4.1.2.3.1）。经授权通过CM接入的CPE的最大个数由这个配置设定值进行控制。

类型	长度	值
18	1	

CM应把这个值解读为无符号整数。如该选项不存在，或值为0，则应看作为缺省值1。

注： 这是对CM授权接入的CPE最大数目的限制。已给定CM实现的硬件上的限制可能要求CM使用更低的值。

C.1.1.8 TFTP服务器时间戳

它是以秒为单位的配置文件的发送时间。该时间的定义见RFC-868。

类型	长度	值
19	4	从1900年1月1日00：00至今的秒数

注： 该参数的目的是防止再次使用旧配置文件。

C.1.1.9 TFTP服务器预置CM地址

请求配置文件的CM的IP地址。

类型	长度	值
20	4	IP地址

注： 本参数的目的是防止注册期间的IP欺骗。

C.1.1.10 上行数据包分类配置设定

该域定义了与上行业务类别表中某一条目相关联的参数。见C.2.1.1。

类型	长度	值
22	n	

C.1.1.11 下行数据包分类配置设定

该域定义了与下行业务类别表中的一个分类器相关联的参数。见C.2.1.2。

类型	长度	值
23	n	

C.1.1.12 上行业务流编码

该域定义了与上行调度一个业务流有关的参数。见C.2.2.1。

类型	长度	值
24	n	

C.1.1.13 下行业务流编码

该域定义了与下行调度一个业务流相关联的参数。见C.2.2.2。

类型	长度	值

25 n

C.1.1.14 有效负载包头抑制

该域定义了与有效负载包头抑制相关联的参数。

类型 长度 值

26 n

C.1.1.15 最大分类器数

这是CM允许接纳的与确认的或激活的上行业务流相关联的最大分类器数目，激活的和未激活的分类器均包含在内。

在使用预置资源延迟激活时，这个参数是必要的。预置业务流的数目可以较高，且每个业务流可能支持多个分类器。预置代表了CM可以选择的业务流设置。CMTS可以通过限制容许的业务流数目来控制已向CM承诺的QoS资源。但仍然要限制与承诺的QoS资源相关的分类器数目。这个参数提供了这种限制。

类型 长度 值

28 2 与容许的或激活的上行业务流相关的激活的和未激活的分类器最大个数

缺省值应为0，即无限制。

C.1.1.16 加密使能

该域值禁止对CM基本业务流和其余所有业务流的基线加密。

类型 长度 值

29 1 0

值0表示禁止基线加密。

C.1.1.17 厂商专用信息

如果有的话，CM厂商专用信息应在厂商专用信息域(VSIF)(code 43)中使用Vendor ID域 (见C.1.3.2)进行编码来说明哪个TLV字节组应用于哪个厂商产品。Vendor ID 应是包含在VSIF中的第一个TLV。如果VSIF中的第一个TLV不是Vendor ID，应丢弃这个TLV。

该配置设定可能出现多次。同样，相同的Vendor ID也可能出现多次。这种配置设定可能会被嵌套在数据包的分类配置设定、业务流配置设定或业务流响应中。然而，在单个的VSIF中不应有超过一个的Vendor ID TLV。

类型 长度 值

43 n 按厂商定义

例如：

- 厂商 A 专用域配置如下：
  - —— VSIF（43）+n（该 VSIF 中的字节数）；
  - —— 8（Vendor ID 类型）+3（长度域）+厂商 A 的 Vendor ID；
  - —— 厂商 A 专用类型#1+域长度+值#1；
  - —— 厂商 A 专用类型#2+域长度+值#2；
- 厂商 B 专用域配置如下：
  - —— VSIF（43）+n（该 VSIF 中的字节数）；
  - —— 8（Vendor ID 类型）+3（长度域）+厂商 B 的 Vendor ID；
  - —— 厂商 B 专用类型+域长度+值。

C.1.1.18 用户管理TLV

这些TLV中的信息不能被CM使用，而由CMTS用来填充CM的用户管理MIB。

如果在配置文件中存在这些TLV，则CM应在随后的REG-REQ中包括这些TLV，以被CMTS用来填充该CM的用户管理MIB。如果用户管理TLV存在于配置文件中，那么CM应包含CMTS MIC中的这些TLV。

C.1.1.19 用户管理控制

这3个字节的域将控制信息提供给CMTS用于用户管理MIB。前两个字节代表CM所允许的IP地址。第三个字节用于控制域。

类型	长度	值
35	3	字节1、2：docsSubMgtCpeControlMaxCpeIP（低10 比特） 字节3，比特0：docsSubMgtCpeCpntrolActive 字节3，比特1：docsSubMgtCpeEontrolLearnable 字节3，比特2～7：保留，应置0

C.1.1.19.1 用户管理CPE IP表

该域列举了用来填充CMTS用户管理MIB中docsSubMgtCpeIpTable的IP地址。

类型	长度	值
36	N（4的倍数）	Ipa1、Ipa2、Ipa3、Ipa4

C.1.1.19.2 用户管理过滤组

用户管理MIB允许过滤组被指配给一个CM和连接在该CM上的CPE。包含两个CM过滤组（上行和下行），两个CPE过滤组（上行和下行）。这四个过滤组在配置文件中通过下列单个TLV来编码。

类型	长度	值
37	8	字节1、2：docsSubMgtSubFilterDownstream组 字节3、4：docsSubMgtSubFilterUpstream组 字节5、6：docsSubMgtCmFilterDownstream组 字节7、8：docsSubMgtCmFilterUpstream组

C.1.2 专用配置文件设置

仅在配置文件中有这些设置，且不应在注册请求中被转发给CMTS。

C.1.2.1 数据结束标志

这是一个表示数据结束的专门标志，它没有长度和值域。

类型
255

C.1.2.2 填充配置设定

该配置没有长度和值域，且仅用于数据结束标志之后，用以把文件填充为一个完整的32比特的整倍数。

类型
0

C.1.2.3 软件升级文件名

CM软件升级的文件名，该文件名是一个完整有效的目录路径名。该文件应存放在D.2.2定义的配置设定选项中所指定的TFTP服务器上。见第11章。

类型	长度	值
9	n	文件名

C.1.2.4 SNMP写访问控制

该对象可以不允许SNMP“设置”访问个别的管理信息库（MIB）对象。该对象的每种实例都控制访问与Object ID（OID）前缀匹配的所有可写的MIB对象。它可以重复出现以禁止访问任何数目的MIB对象。

类型	长度	值
10	n	OID前缀+控制标志

其中n表示ASN.1基本编码规则（见GB/T16263－1996）对OID前缀加上一个控制标志字节的编码的长度。

控制标志可以取以下值：

- 允许写访问；
- 不允许写访问。

可以使用任何OID前缀。全零OID 0.0可以被用于控制访问所有的MIB对象（OID1.3.6.1有相同的效果）。

当该对象的多个实例出现并交迭时，最长的（最明确的）前缀有优先权。因此，可以这样举例：

- someTable　　不允许写访问；
- someTable.1.3　允许写访问。

这个例子允许访问someTable.1.3中的对象，但不允许访问someTable中除someTable.1.3的其它对象。

C.1.2.5　SNMP MIB对象

该对象允许通过TFTP-注册过程设置任意的SNMP MIB对象。

类型	长度	值
11	n	可变的绑定

其中值是一个由RFC-1157定义的SNMPVarBind。VarBind按ASN.1基本编码规则进行编码，把它看作是SNMP设置请求的一部分。

CM应把这个对象看作是带有以下警告的SNMP设置请求的一部分：

- 应把该请求当作已完全授权（不能因缺少特许而拒绝该请求）；
- 不能使用 SNMP 写控制预置（见前节）；
- CM 不产生 SNMP 响应。

该对象可以用不同的VarBind来重复“ 设置 ”若干MIB对象。所有这些设置应被看作是同时进行的。

每个VarBind应限制在255个字节内。

C.1.2.6　CPE以太网MAC地址

该对象用CPE设备的以太网MAC地址（见4.1.2.3.1）来配置CM。它可以重复配置任意数量的CPE设备地址。

类型	长度	值
14	6	CPE的以太网MAC地址

C.1.2.7　软件升级TFTP服务器

位于CM侧软件升级文件中的TFTP服务器的IP地址。见第11章及C.1.2.3。

类型	长度	值
21	4	ip1、ip2、ip3、ip4

C.1.2.8　SNMP V3Kickstart值

符合规范的CM应理解紧随的TLV及其子单元的含义，并能够启动SNMPv3访问CM。

类型	长度	值
34	n	合成值

在配置文件中可以包含多达5个对象。每个对象都产生一个附加行，并被加到usmDHKickstartTable和usmUserTable中，为该行产生一个代理公共数。

C.1.2.8.1　SNMP V3　Kickstart安全名

类型	长度	值
34.1	2～16	UTF8编码的安全名

对于ASCII字符集，UTF8和ASCII编码是相同的。通常，UTF8编码的安全名被描述为EuroDOCSIS内置USM用户之一，例如：“ eurodocsisManager ”、“ eurodocsisOperator ”、“ eurodocsisMoniter ”、“ eurodocsisUser ”等等。安全名不会以0结束，它在 usmDHKickStartTable 中记录为usmDHKickStartSecurityName,在usmUserTable中记录为usmUserName和usmUserSecurityName。

C.1.2.8.2 SNMP V3 Kickstart管理者公共数

类型	长度	值
34.2	n	表示为一个8bit字符串的管理者Diffie-Helman公共数

该数是Diffie-Helman 公共数，它由管理者或操作者秘密产生的随机数寻出，并根据RFC-2786变换而得。在usmDHKickStartTable中，它被记录为usmKickstartMgrPublic。当该数与同一行中记录为usmKickstartMyPublic的对象结合在一起时，它能用来从usmUserTable中的相应行中得到密钥。

C.1.2.9 制造商代码校验证书（可选）

类型	长度	值
32	n	制造商代码校验证书

C.1.2.10 联合签名代码校验证书（可选）

类型	长度	值
33	n	联合签名代码校验证书

C.1.3 注册请求/响应专用编码

注册请求/响应专用编码在配置文件中找不到，但却包含在注册请求和DHCP请求的选项60中。有些编码也用于注册响应中。

CM应在注册请求中包含所有可能要与CMTS协商的CM性能编码，那些不必与CMTS协商的CM性能编码要在特定的CM性能描述中明确指出。CMTS应在注册响应中包含CM性能。

C.1.3.1 CM性能编码

CM性能编码的域值描述了特定CM的性能，即对CM所支持的特性或特性数目进行与实现有关的限制。它由一些封装的类型/长度/值域组成，封装的子类型定义了该CM的特殊性能。定义的子类型域仅在封装的性能配置设定字符串中才有效。

类型	长度	值
5	n	

封装域的可能设置描述如下：

所有这些性能都将包括在注册请求和DHCP请求的选项60中，除非有性能明确不允许这样做的描述。

C.1.3.1.1 级联支持

如果该域值为1，则CM向CMTS请求级联支持。

类型	长度	开/关
5.1	1	1或0

C.1.3.1.2 版本说明

该CM的协议版本说明。

类型	长度	开/关
5.2	1	0：EuroDOCSIS v1.0 1：本部分 2～255：保留

如果缺少该字节组，则CMTS应假定按EuroDOCSIS 1.0来操作。缺少该字节组或值为“ EuroDOCSIS1.0 ”并不意味着CM只支持EuroDOCSIS1.0功能，CM可能通过其它的CM性能编码表明它支持其他特性（参见G.3）。

C.1.3.1.3 分段支持

如果该域值为1，则CM向CMTS请求分段支持。

类型	长度	值
5.3	1	1或0

C.1.3.1.4 有效负载包头抑制支持

如果该域值为1，则CM向CMTS请求有效负载包头抑制支持。

类型	长度	值
5.4	1	1或0

C.1.3.1.5 IGMP支持

如果该域值为1，则CM支持符合本部分的IGMP。

类型	长度	值
5.5	1	1或0

C.1.3.1.6 加密支持

待定。

C.1.3.1.7 下行SAID支持

该域表明了CM 所能够支持的下行安全关联标识符（SAID）的数目。

类型	长度	值
5.7	1	CM所能支持的下行SAID的数目

如果SAID值为0，则意味着CM只能支持一个SAID。

C.1.3.1.8 上行SID支持

该域表明了CM所能支持的上行SID数目。

类型	长度	值
5.8	1	CM所能支持的上行SID数目

如果SID数为0，则意味着CM仅能支持一个SID。

C.1.3.1.9 可选过滤支持

该域表明CM的可选过滤支持。

类型	长度	值
5.9	1	包过滤支持队列 比特#0：802.1P过滤 比特#1：802.1Q过滤 比特#2-7：保留，应置0

该CM性能不必与CMTS协商。CM应在DHCP请求中包含该性能，但不应在注册请求中包含该性能。如果CMTS确实在注册请求中收到该性能，则应在注册响应中以同样的值返回该性能。

C.1.3.1.10 每符号传送均衡器抽头

该域表明了CM所支持的每个符号的预均衡器抽头最大数目。

所有CM应支持以符号为间隔的均衡器系数。CM支持每符号的抽头数为2或4。如果缺少这个字节组，则意味着CM只支持单符号间隔的均衡器系数。

类型	长度	值
5.10	1	1、2或4

C.1.3.1.11 传送均衡器抽头数

该域表明CM 所支持的均衡器抽头数。

所有CM应支持至少8个符号的均衡器长度。CM支持多达64个T间隔，T/2间隔或T/4间隔抽头。如果缺少该字节组，CM就只能支持8抽头的均衡器长度。

类型	长度	值
5.11	1	8～64

C.1.3.1.12 DCC支持

该值是CM的DCC支持。

类型	长度	值

5.12	1	0：不支持DCC 1：支持DCC

C.1.3.2 Vendor ID编码

该域值包含厂商标识信息，是用CM MAC地址的3字节厂商专用的唯一组织标识符（OUI）来规定的。

厂商标识符应用于注册请求中，但不应用作一个孤立的配置文件单元。它也可以在配置文件中用作厂商专用信息域的一个子域。当作此用处时，它标识了试图使用该信息的CM的Vendor ID。如果Vendor ID用在注册请求中，则它也是发送请求的CM的Vendor ID.

类型	长度	值
8	3	v1、v2、v3

C.1.3.3 CM IP地址

为了向后兼容EuroDOCSIS1.0版本，用“ TFTP服务器预置CM地址 ”来替代。

类型	长度	值
12	4	IP 地址

C.1.3.4 无效业务响应

如果CMTS不能或不愿意对在注册请求中出现的被请求业务类别进行授权，则应在注册响应消息中包含这个配置设定。尽管该值仅应用于失败的业务类别，但整个注册请求都应被视为失败（没有业务类别配置获得授权）。

类型	长度	值
13	3	类别ID、类型、确认码

其中：

- 类别 ID：来自无效请求的业务类别；
- 类型：请求被拒绝的业务类中的专用业务类别对象；
- 确认码：见 C.4。

C.1.4 动态业务消息专用编码

在配置文件和注册请求/响应信令中不会发现这些编码，而只会在DSA-REQ、DSA-RSP、DAS-ACK、DSC-REQ、DSC-RSP、DSC-ACK和DSD-REQ消息中找到（见7.3.12～7.3.18）。

C.1.4.1 HMAC-Digest

HMAC-Digest设置是一个密钥消息摘要，参数内容及格式待定。

C.1.4.2 授权块

授权块中包含一个从CM到CMTS的授权“ 提示 ”，本部分对该授权“ 提示 ”的内容不做规定，具体可参见PKT-DQOS。

授权块可能存在于在初始化CM的DSA-REQ和DSC-REQ消息中。这个参数不应出现在DSA-RSP、DSC-RSP消息中，也不应出现在初始化CMTS的DSA-REQ、DSC-REQ消息中。

授权块信息应用于全部DSA-REQ或DSC-REQ消息。这样，每个消息可能只存在一个授权块。如果授权块存在，它应传递到CMTS上的授权模块。授权块信息仅由授权模块处理。

类型	长度	值
30	n	n个8bit序列

C.1.4.3 密钥顺序号

待定。

C.2 与QoS相关的编码

C.2.1 包分类编码

下面的类型/长度/值编码应用在所有配置文件、注册消息和动态业务消息中，用来对数据包分类和调度参数进行编码。所有多字节数以网络字节顺序发送，即包含MSB的8bit首先在线路中被发送。

一个分类器应至少包含一个由C.2.1.5“IP包分类编码”、C.2.1.6“以太网LLC包分类编码”或C.2.1.7“IEEE 802.1 P/Q包分类编码”定义的编码。

所有符合本部分的CM应支持下列配置设置。所有的CMTS应支持基于IP包头域的下行包分类（见C.2.1.5）。

C.2.1.1 上行包分类编码

该域定义了与一个上行分类器有关的参数。

已定义的相同子类型域对已封装的上行和下行包分类配置设定字符串都有效。这些类型域在其它编码内容中是无效的。

类型	长度	值
22	n	

C.2.1.2 下行包分类编码

该域定义了与下行分类器有关的参数。

已定义的相同子类型域对已封装的上行和下行包分类配置设定字符串都有效。这些类型域在其它编码内容是无效的。

类型	长度	值
23	n	

C.2.1.3 通用包分类器编码

C.2.1.3.1 分类器参考

该域的值规定了分类器的参考。该值在每个动态业务消息、配置文件或注册请求消息中是唯一的。

类型	长度	值
[22/23].1	1	1～255

C.2.1.3.2 分类器标识符

该域值规定了用于分类器的标识符，每个业务流有唯一分类器标识符。CMTS分配数据包分类器标识符。

类型	长度	值
[22/23].2	2	1～65 535

C.2.1.3.3 业务流参考

该域值规定了一个用来标识相应业务流的业务流参考。

在出现在业务流标识符未知（例如，对CM启动的DSA-REQ和REG-REQ）的任何消息中发生的所有包分类器TLV中应包含此业务流参考TLV。在出现在DSC-REQ和初始化CMTS DSA-REQ消息中的所有包分类器中，不应规定业务流参考。

类型	长度	值
[22/23].3	2	1～65 535

C.2.1.3.4 业务流标识符（SFID）

该域值规定了识别相应业务流的SFID。

在SFID未知的包分类器TLV中，不应包含该TLV（例如，初始化CM DSA-REQ和REG-REQ）。在出现在DSC-REQ和初始化CMTS DSA-REQ消息中的包分类器TLV中，则应指定SFID。

类型	长度	值
[22/23].4	4	1～4 294 967 295

C.2.1.3.5 优先级规则

该域值规定了分类器的优先级，用来决定分类器的顺序。值越大，表明优先级越高。

在配置文件和注册消息中的分类器优先级范围可以为0～255，缺省值为0。出现在DSA/DSC消息中的分类器优先级范围应为64～191，缺省值为64。

类型	长度	值
[22/23].5	1	

C.2.1.3.6 分类器激活状态

该域值规定了在为业务流选择数据包时是否应激活分类器。一个未激活的分类器一般用AdimittedQoSParameterSet来确保资源对后面的激活有效。分类器的实际激活取决于该参数属性和业务流状态。不管该参数属性如何设置，如果业务流未激活，则不使用分类器。

类型	长度	值
[22/23].6	1	0：未激活 1：激活

缺省值为1，表示激活分类器。

C.2.1.3.7 动态业务变更动作

当接收到动态业务变更请求时，表明该分类器应该采取的动作。

类型	长度	值
[22/23].7	1	0：DSC添加分类器 1：DSC替换分类器 2：DSC删除分类器

C.2.1.4 分类器错误编码

该域定义了与分类器错误有关的参数。

类型	长度	值
[22/23].8	n	

分类器错误编码包含单个分类器错误参数集，该参数集由以下各个参数来定义：错误参数、确认码和错误消息。

分类器错误编码通过REG-RSP、DSA-RSP和DSC-RSP消息返回到CM，以表明接收者对在REG-REQ、DSA-REQ或DSC-REQ消息中对分类器建立请求的消极响应的原因。

一旦失败，REG-RSP、DSA-RSP或DSC-REQ应包括一个分类器错误编码，用于在REG-REQ、DSA-REQ或DSC-REQ消息中请求的至少一个失败的分类器。失败分类器的分类器错误编码应包含确认码和错误参数，并且可以包含一个错误消息。如果拒绝某些分类器集而接收了其它分类器设置，则分类器错误编码应仅包含在被拒绝的分类器中。如果整个事务成功，则RSP或ACK消息不应包含分类器错误编码。

由于可能会有多个分类器参数出错，因此在REG-RSP、DSA- RSP或DSC- RSP消息中可能会出现多个分类器错误编码。即使是一个带有单个分类器错误编码的消息也不应包含任何其它协议的分类器编码（例如，IP、802.1P/Q）。

在任何REG-REQ、DSA-REQ或DSC-REQ消息中都不应出现分类器错误编码。

C.2.1.4.1 出错参数

该参数值标识了在一个被拒绝的分类器请求中，出错的被请求的分类器参数的子类。在一个给定分类器错误编码中，一个分类器错误参数集只能有一个出错参数TLV。

子类型	长度	值
[22/23].8.1	n	出错的分类器编码子类

如果长度为1，那么在发现错误的地方，值是单级（single-level）子类，例如，7表示一个无效的变更动作。如果长度为2，那么在发现错误的地方，值是多级（multi-level）子类，例如，9-2表明一个无效的IP协议值。

C.2.1.4.2 错误码

该参数表示请求状态。非0值对应于C.4描述的确认码。在一个给定的分类器错误编码中，一个分类器错误参数集只能有一个错误码。

子类型	长度	值
[22/23].8.2	1	确认码

0值表示分类器请求成功。由于一个分类器错误参数集仅应用于出错参数，因此不应使用该值。

C.2.1.4.3 错误消息

这个子类型在分类器错误消息集中是可选的。如果存在，它表示在CM的控制台上显示出来的一个文本字符串和/或进一步描述被拒绝的分类器请求的记录日志。在给定的分类器错误编码中，分类器错误参数集可能没有或有一个错误消息子类型。

子类型	长度	值
[22/23]8.3	n	以0值结束的ASCII字符串

注： 长度n包含结尾的0。整个分类器编码消息总长度应小于256个字符。

C.2.1.5 IP包分类编码

该域定义了与IP包分类相关的参数。

类型	长度	值
[22/23].9	n	

C.2.1.5.1 IP业务类型的范围和掩码

该域值规定了IP业务类型（IP ToS）字节范围和掩码的匹配参数。如果tos-low<=(ip-tos AND tos-mask)<=tos-high，则一个带有IP ToS字节值“ip-tos”的IP包与该参数匹配。如果省略该域，则IP包业务类型（ToS）字节的比较与这个条目无关。

类型	长度	值
[22/23].9.1	3	tos-low、tos-high、tos-mask

C.2.1.5.2 IP协议

该域值规定了IP协议域[RFC-1700]的匹配值。如果省略该参数，那么IP包头协议域的比较与该条目不相关。

有两个特殊的IP协议域值：“256”匹配带有任何IP协议值的业务，“257”匹配TCP和UDP业务。一个包含大于257的IP协议域值的条目应是无效比较（即没有业务能够匹配这个条目）。

类型	长度	值
[22/23].9.2	2	prot1、prot2

有效范围：0～257。

C.2.1.5.3 IP源地址

该域值规定了IP源地址的匹配值。如果src=(ip-src AND smask)，则一个带有IP源地址“ip-arc”的IP包匹配该参数。其中“smask”是由C.2.1.5.4定义的参数。如果省略该参数，则IP包源地址的比较与该条目无关。

类型	长度	值
[22/23].9.3	4	src1、src2、src3、src4

C.2.1.5.4 IP源地址掩码

该域值规定了IP源地址的掩码值。如果省略该参数，则缺省IP源地址掩码是255.255.255.255。

类型	长度	值
[22/23].9.4	4	mask1、mask2、mask3、mask4

C.2.1.5.5 IP目的地址

该域值规定了IP目的地址的匹配值。如果dst=(ip-dst AND dmask)，则带有IP目的地址“ ip-dst ”的IP包与该参数匹配。其中“ dmask ”由C.2.1.5.6定义。如果省略该参数，则IP包目的地址的比较与该条目无关。

类型	长度	值
[22/23].9.5	4	dst1、dst2、dst3、dst4

C.2.1.5.6 IP目的地址掩码

该域值规定了IP目的地址的掩码值。如果省略该参数，则缺省IP目的地址掩码为255.255.255.255。

类型	长度	值
[22/23].9.6	4	dmask1、dmask2、dmask3、dmasd4

C.2.1.5.7 TCP/UDP源端口起始

该域值规定了低端TCP/UDP源端口值。如果sportlow<=src-port<=sporthigh，则带有TCP/UDP端口值“ src-port ”的IP包匹配该参数。如果省略该参数，则sportlow的缺省值是0。该参数与非TCP/UDP的IP业务无关。

类型	长度	值
[22/23].9.7	2	sportlow1、sportlow2

C.2.1.5.8 TCP/UDP源端口终止

该域值规定了高端TCP/UDP源端口值。如果sportlow<=src-port<=sporthigh,则带有TCP/UDP端口值“ src-port ”的IP包与该参数匹配。如果省略该参数,则sporthigh的缺省值是65535。该参数与非TCP/UDP的IP业务无关。

类型	长度	值
[22/23].9.8	2	sporthigh1、sporthigh2

C.2.1.5.9 TCP/UDP目的端口起始

该域值规定了低端TCP/UDP目的端口值。如果dportlow<=dst-port<=dporthigh，则带有TCP/UDP端口值“ dst-port ”的IP包匹配该参数。如果省略该参数，则dportlow的缺省值是0。该参数与非TCP/UDP的IP业务无关。

类型	长度	值
[22/23].9.9	2	dportlow1、dportlow2

C.2.1.5.10 TCP/UDP目的端口终止

该域值规定了高端TCP/UDP目的端口值。如果dportlow<=dst-port<=dporthigh，则带有TCP/UDP端口值“ dst-port ”的IP包与该参数匹配。如果省略该参数，则dporthigh的缺省值是65535。该参数与非TCP/UDP的IP业务无关。

类型	长度	值
[22/23].9.10	2	dporthigh1、dporthigh2

C.2.1.6 以太网LLC包分类编码

该域定义了与以太网LLC数据包分类相关的参数。

类型	长度	值
[22/23].10	n	

C.2.1.6.1 目的MAC地址

该域值规定了MAC目的地址的匹配参数。如果dst=(etherdst AND msk)，则带有MAC目的地址“ etherdst ”的以太网数据包与该参数匹配。如果省略该参数，则以太网MAC目的地址的比较与该条目无关。

类型	长度	值
[22/23].10.1	12	dst1、dst2、dst3、dst4、dst5、dst6、

msk1、msk2、msk3、msk4、msk5、msk6

C.2.1.6.2 源MAC地址

该域值规定了MAC源地址的匹配值。如果省略该参数，则以太网MAC源地址的比较与该条目无关。

类型	长度	值
[22/23].10.2	6	src1、src2、src3、src4、src5、src6

C.2.1.6.3 Ethertype/DSAP/MacType

在以太网数据包中type、eprot1、eprot2表明了第三层协议ID格式如下：

当type=0时，规则不使用第三层协议作为匹配准则。此时考虑一个数据包是否匹配当前规则时，忽略eprot1、eprot2。

当type=1时，规则仅应用于包含Ethertype值的帧。Ethertype值包含在使用DEC-Intel-Xerox（DIX）封装或RFC1042子网接入协议（SNAP）封装格式的数据包中。此时为了符合规则，eprot1、eprot2给出数据包应与之匹配的16-bit的Ethertype。

当type=2时，规则仅应用于使用带有目的业务（DSAP）的IEEE802.2封装格式的帧，而不用于0xAA（为SNAP保留）。此时为了符合规则，eprot1、eprot2的低8位应匹配数据包的DSAP字节。

当type=3时，规则仅应用于MAC管理消息（FC域为1100001x），该MAC管理消息包头（见7.3.1）的type域在eprot1与eprot2值之间。作为例外情况，以下的MAC管理消息类型不应被分类，且总是在基本业务流中发送：

- Type4：RNG_REQ；
- Type6：REG_REQ；
- Type7：REG_RSP；
- Type14：REG_ACK。

当type=4时，该规则可看作一个“全捕获”（catch-all）规则，它匹配所有的PDU包。该规则并不匹配MAC管理消息。在这种情形下，可忽略eprot1、eprot2的值。

如果以太网帧含有一个802.1P/Q Tag包头（即Ethertype 0x8100），则这个对象用于802.1P/Q包头内的嵌入Ethertype域。

类型的其它值被保留，如果该TLV被省略，则Ethertype或IEEE802.2 DSAP的比较都与此规则无关。

类型	长度	值
[22/23].10.3	3	type、eprot1、eprot2

C.2.1.7 IEEE802.1P/Q包分类编码

该域定义了与IEEE802.1P/Q包分类有关的参数。

类型	长度	值
[22/23].11	n	

C.2.1.7.1 IEEE 802.1P用户优先级

该域值规定了与IEEE 802.1Puser_priority比特匹配的参数。如果pri-low<=priority<=pri-high，则带有IEEE 802.1Puser_priority值为“priority”的以太网数据包匹配该参数。如果省略该域，那么IEEE 802.1P user_priority比特的比较与该条目无关。

如果规定了该参数，则不含IEEE 802.1Q封装的以太网数据包不应与之匹配。如果在不支持转发IEEE 802.1Q封装业务的CM上规定该参数，那么该条目不应用于任何业务。

类型	长度	值
[22/23].11.1	2	pri-low、pri-high

有效范围：对pri-low和pri-high为0～7。

C.2.1.7.2 IEEE 802.1Q VLAN_ID

该域值规定了IEEE 802.1Q vlan_id比特的匹配值。只有已规定的vlan_id域值的前12bit（即最高的12位）才有意义，在比较时应忽略最后的4bit。如果忽略该域，则IEEE 802.1Q vlan_id的比较与该条目无关。

如果规定了该参数，则不含IEEE 802.1Q封装的Ethernet数据包不应与之匹配。如果在不支持转发IEEE 802.1Q封装业务的CM上规定该参数，则该条目不应用于任何业务。

类型	长度	值
[22/23].11.2	2	vlan_id1、vlan_id2

C.2.1.7.3 厂商专用分类器参数

该参数允许厂商来编码厂商专用分类器参数。厂商标识符（Vendor ID）应是嵌入在厂商专用分类器参数中的第一个TLV，如果这个TLV不是Vendor ID，则应将其丢弃。（见C.1.1.17）。

类型	长度	值
[22/23].4.3	n	

C.2.1.8 上行专用分类编码

分类器激活信号

该域只能用在来自CMTS且影响激活参数集的动态业务变更消息中。该域不出现在任何别的业务流的信令消息中。

类型	长度	值
22.12	1	1：请求时激活/去激活分类器 2：确认时激活/去激活分类器

该域指示CM改变其上行传输特性，以匹配DSC中的参数，或者在收到DSC-Request时立即改变或者仅在收到DSC-Ack后改变。尤其是，它给出了此DSC变更所改变的任何分类器的激活（去激活）的时间。

带宽增加的缺省值是2，带宽减少的缺省值是1。如果不能确定是带宽增加还是带宽减少，则缺省值为2。

C.2.2 业务流编码

以下TLV编码应用在配置文件、注册消息和动态业务消息中，用以对业务流参数进行编码。所有的8bit组都是以网络字节顺序排列，即首先发送包含MSB位的8bit组。

CM应支持下列配置设定。

C.2.2.1 上行业务流编码

该域定义了与业务流上行调度有关的参数。上行业务流编码由一些已封装的TLV域组成。

因为许多已定义的子类型域对两种配置设定的类型来说是有效的，所以已封装的上行和下行业务流配置设定字符串共享同样的子类型域编号方式。在其它编码内容中，这些类型域是无效的。

类型	长度	值
24	n	

C.2.2.2 下行业务流编码

该域定义了与业务流下行调度有关的参数。下行业务流编码由一些已封装的TLV域组成。

因为除了业务流编码外，许多已定义的子类型域对两种配置设定的类型来说是有效的，所以这些已封装的上行和下行业务流分类配置设定字符串共享同样的子类型域编号方式。在其它编码中，这些类型域是无效的。

类型	长度	值
25	n	

C.2.2.3 一般业务流编码

C.2.2.3.1 业务流参考

业务流参考用于把一个数据包分类器编码和业务流编码联系起来。一个业务流参考仅用于建立一个SFID。一旦业务流存在，并且有一个指定了的SFID，那么该业务流参考不应再使用。业务流参考在每个配置文件、注册消息交换或动态业务添加消息交换中是唯一的。

类型	长度	值
[24/25].1	2	1～65535

C.2.2.3.2 业务流标识符（SFID）

CMTS使用SFID作为一个业务流的主参考。只有CMTS能够发出SFID。在CMTS初始化的DSA-请求和CM初始化的REG/DSA-请求的REG/DSA-响应中，CMTS使用该参数化法来发出SFID。CM使用DSC-REQ消息中的这个参数来说明SFID。CM和CMTS都可以使用该TLV值来对DSD-REQ消息中的SFID进行编码。

配置文件不应包含该参数。

类型	长度	值
[24/25].2	4	1～4 294 967 295

C.2.2.3.3 业务标识符（SID）

该域值规定了由CMTS分配给业务流的SID，该业务流带有非零的AdmittedQosParameterSet或ActiveQosParameterSet。它用在带宽分配MAP中来分配上行带宽。该域应在CMTS初始化的DSA-REQ消息或DSC-REQ消息中存在，这些消息与建立一个容许的或激活的上行业务流有关。该域在REG-RSP，DSA-RSP和DSC-RSP消息中也应存在，这些消息与成功建立一个容许的或激活的上行业务流有关。

即使成功地容许或激活了一个业务流（即已经分配了SID），该SFID应被用于随后的DSx消息信令，因为它是对业务流的基本处理。如果一个业务流不再被容许或激活（通过DSC-REQ），则该业务流的SID可以由CMTS重新分配。

子类	长度	值
[24/25].3	2	SID （低14bit）

C.2.2.3.4 业务类别名

该域值涉及用于该业务流的已定义的CMTS业务配置。

类型	长度	值
[24/25].4	2～16	以0结束的ASCII字符串

注： 长度包含结束的0。

当业务类别名用在一个业务流编码中时，它表明了需要由CMTS提供的业务流中所有未规定的QoS参数。在CMTS和配置文件中业务类别名定义的同步是操作员的责任。

C.2.2.3.5 业务质量参数集类型

该参数应出现在每个业务流编码中。它规定了QoS参数集或业务类别名的正确应用：预置的集、容许的集、和/或激活的集。当两个QoS参数集相同时，该参数的多比特值可能被用于不止一个参数集的QoS参数。对于相同的业务流，在单独的类型24/25业务流编码中，单个消息可能包含多个QoS参数集。当参数不同时，容许规定QoS参数集。比特0是值域的LSB。见表C.2和表C.3。

对于出现在注册请求或注册响应消息中的每个业务流，应有一个业务流编码来说明ProvisionedQoSParameterSet。该业务流编码，或其它的业务流编码，也可以说明一个容许的和/或激活的集。

出现在动态业务消息中的任何业务流编码不应规定ProvisionedQoSParameterSet。

类型	长度	值
[24/25].6	1	比特#0：预置的集 比特#1：容许的集 比特#2：激活的集

表 C.2　REG-REQ 和 REG-RSP 消息中使用的值

值	消息
001	仅用于预置集
011	用于预置和容许集，并执行容许控制
101	用于预置和激活集，执行单个业务流编码中容许集的容许控制，并激活该业务流
111	用于预置的、容许的和激活的集，执行容许控制并激活该业务流

表 C.3　REG-REQ、REG-RSP 和动态业务消息中使用的值

值	消息
010	执行容许控制并用于容许集
100	核对单独业务流编码中的容许集，如有必要执行容许控制，激活该业务流并用于激活的集
110	执行容许控制并激活该业务流，将参数用于容许的和激活的集

值000仅用于动态业务变更消息，用于将激活的和容许的集设为空（见9.1.7.4）。

CMTS应处理每个激活的和容许的QoS参数集的单个更新，但并不要求具有处理规定同样QoS参数集的多业务流编码的能力，而将该能力留作厂商专用功能。如果DSA/DSC包含对单个QoS参数集的多个更新，而厂商并不支持这种更新，则CMTS应以错误代码2进行响应，即拒绝未知配置设定。

C.2.2.4　业务流错误编码

该域定义了与业务流错误有关的参数。

类型	长度	值
[24/25].5	n	

业务流错误编码包含一个业务流错误参数集，它由以下各参数来定义：出错参数、确认码及错误消息。

业务流错误编码在REG-RSP、DSA-RSP和DSC-RSP消息中被返回，用来表明接收者对REG-REQ、DSA-REQ或DSC-REQ消息中的业务流建立请求作出消极响应的原因。

业务流错误编码也可以在REG-ACK、DSA-ACK和DSC-ACK消息中返回，用来表明接收者对相应的REG-RSP、DSA-RSP和DSC-RSP消息中的业务类别名的扩展作出消极响应的原因。

在失败时，对于REG-REQ、DSA-REQ或DSC-REQ消息中请求的至少一个失败业务流，REG-RSP、DSA-RSP或DSC-RSP消息应包含一个业务流错误编码。在失败时，对于REQ-RSP、DSA-RSP或DSC-RSP消息中至少一个失败的业务类别名称扩展，REG-ACK、DSA-RSP或DSC-ACK消息应包含一个业务错误编码。失败业务流的业务流错误编码应包含确认码和出错参数，也可以包含错误消息。如果某些业务流参数集被拒绝，而其它的业务流参数集被接收，那么业务流错误编码应只包含在被拒绝的业务流中。

对成功的整个事务，RSP或ACK消息不应包含业务流错误编码。

因为多业务流参数可能出错，所以多业务流错误编码可以出现在REG-RSP、DSA-RSP、DSC-RSP、REG-ACK、DSA-ACK或DSC-ACK消息中。即使带有单业务流错误编码的消息也不应包含任何QoS参数。

业务流错误编码不应出现在任何REG-REQ、DSA-REQ或DSC-REQ消息中。

C.2.2.4.1　出错参数

该参数值表示一个出错的已请求的业务流参数的子类型，它存在于被拒绝的业务流请求或业务类别名扩展响应中。在给定的业务流错误编码中业务流错误参数集应只有一个出错参数TLV。

子类	长度	值
[24/25].5.1	1	错误的业务流编码子类型

C.2.2.4.2　错误代码

该参数表明了请求的状态。非0值对应于C.4所述的确认码。在给定的业务流错误编码中业务流错误参数集应只有一个错误代码。

类型	长度	值
[24/25].5.2	1	确认码

值为0表示业务流请求成功。由于业务流错误参数集只用于出错参数，所以不应使用该值。

C.2.2.4.3 错误消息

该子类型在业务流错误参数集中是可选的。如果存在，则它表示在CM控制台上显示的文本字符串和/或进一步描述被拒绝的业务流请求的记录日志。在已给定的业务流错误编码中，业务流错误参数集可以没有或有一个错误消息子类。

子类	长度	值
[24/25].5.3	n	以0结束的ASCII字符串

注 1：长度n包含结束标识的0。

注 2：整个业务流编码消息的总长度不应超过256字符。

C.2.2.5 公共的上行和下行QoS参数编码

类型24、25的剩余部分是QoS参数，任何给定的QoS参数类型都应在每个业务流编码中出现0或1次。

C.2.2.5.1 流量优先级

该参数值规定了分配给业务流的优先级。给定除优先级以外所有QoS参数都相同的两个业务流，则优先级较高的业务流延时应该较少，并且享有更高的缓冲优先权。此外，对于QoS参数不同的业务流来说，优先级参数不应比任何冲突的业务流QoS参数更优先。本部分不规定执行该参数的具体算法。

对于上行业务流，在决定请求业务和授权生成的优先级时，CMTS应使用该参数，并且CM应为基于这种优先级及其请求/传送策略（见C.2.2.6.3）的优先级请求SID（见A.2.3）优先选择争用请求机会。

类型	长度	值
[24/25].7	1	0～7：数字越大表示优先级越高

注： 缺省优先级为0。

C.2.2.5.2 最大持续流量速率

该参数是一个基于令牌池的数据包速率限定的速率参数R。R以每秒的比特数来表示，并且应考虑该业务流的所有MAC帧数据PDU，包括从跟在MAC包头HCS后面的字节到CRC结束（注：有效负载的长度包括链接MAC帧中的每一个PDU）。在任何时间间隔T内，被转发的字节数(以字节为单位)都限制在Max(T)之内。如式（C.1）所示。

$$Max(T)=T\times(R/8)+B \quad \text{(C.1)}$$

式中B(以字节为单位)是最大流量突发配置设定(见C.2.2.5.4)。

注 1：该参数不限制业务流的瞬时速率。

注 2：这里不规定执行该参数的专门算法，满足式（C.1）的任何方法都可适用。

注 3：如果省略该参数或设为0，则表示没有明确的强制最大流量速率。该域只规定了一个范围，并不保证该速率有效。

C.2.2.5.2.1 最大上行持续流量速率

对于上行业务流来说，在任何T时间间隔内，CM不应请求超过式（C.1）中要求的Max（T）值的带宽，因为该参数可以强迫CMTS用延迟授权来填充MAP。

CM应延迟发送不满足式（C.1）的上行数据包，并对它们进行“速率调整”来满足该表达式，直到受厂商的缓冲限制的最大速率。

CMTS应在所有上行数据传送，包括在争用中发送的数据中，强制执行式（C.1）。CMTS可以在涉及该参数的计算中考虑未使用的授权。它可以通过以下方法中任何一种执行速率限制：

a） 丢弃超过限制的请求；

b） 延迟（通过 0 长度授权）授权，直到与允许的限制相一致；

c） 丢弃超过限制的数据包。

CMTS应向策略模块报告这种情况。如果CMTS通过丢弃数据包或请求来执行，则CMTS应允许CM和CMTS算法之间的错误容限。

类型	长度	值
24.8	4	R(bps)

C.2.2.5.2.2 最大下行持续流量速率

对于下行业务流，该参数仅用在CMTS上。CMTS应在所有下行数据传送时执行式（C.1）。CMTS不应转发在T时间间隔内不满足式（C.1）的下行数据包。CMTS应通过把超过式（C.1）到达的数据包进行排队来对下行流量进行速率调整，并将它们延时，直到满足式（C.1）。

该参数不强制CM执行。

类型	长度	值
25.8	4	R(bps)

C.2.2.5.3 最大突发流量

该参数的值规定了表达式（C.1）所述业务流的令牌池大小B（以字节为单位）。该值由跟在MAC包头HCS后的字节到CRC结束的字节计算得来（有效负载的大小包括链接的MAC帧中的每一个PDU）。

如果省略该参数，则B的缺省值是1 522字节。1 522字节和最大级联突发数据长度二者中的较大者是B的最小值（见C.2.2.6.1）。

类型	长度	值
[24/25].9	4	B(字节)

注： 这里不规定执行该参数的专门算法，任何满足上面公式的方法都可适用。

C.2.2.5.4 最小保留流量速率

该参数规定了该业务流保留的最小速率（单位为bps）。CMTS应能够满足业务流的带宽请求直到它的最小保留流量速率。如果一个业务流请求比其最小保留流量速率更小的带宽，那么CMTS可以重新分配剩下的保留带宽用于其它目的。所有业务流的最小保留流量速率的总计可以超出可用带宽。该参数值由跟在MAC包头HCS后的字节到CRC结束的字节计算而来（有效负载的大小包括链接的MAC帧中的每一个PDU）。如果省略该参数，则它的缺省值是0bps（即缺省没有为业务流保留带宽）。

该域仅用于CMTS，并且应由CMTS强制执行。

类型	长度	值
[24/25].10	4	

注： 这里不规定执行该域中规定的值的专用算法。

C.2.2.5.5 假定的最小保留速率的数据包大小

该域值规定了一个假定的最小数据包大小（以字节为单位），并将为其提供最小保留流量速率。该参数用字节来定义，并规定为从跟在MAC包头HCS后的字节直到CRC结束的所有字节（有效负载的大小包括链接的MAC帧中的每一个PDU）。如果业务流发送的数据包大小小于该参数所规定的值，则该数据包将按该参数中的规定大小来处理，用于计算最小保留流量速率以及计算最终可用于计费的字节数（如发送的字节）。

CMTS应把该参数用于最小保留流量速率算法。CMTS用该参数来估算业务流中每个数据包的开销。

如果省略这个参数，则其缺省值取决于CMTS实现的方法。

类型	长度	值
[24/25].11	2	

C.2.2.5.6 激活的QoS参数的超时

该参数值规定了在一个激活的业务流上仍未使用的最大资源区间。如果在这个时间间隔内业务流上没有活动，CMTS应将激活的和容许的QoS参数集变更为0。CMTS应用DSC-REQ向CM发出这种资源变更的信号。

类型	长度	值
[24/25].12	2	s

该参数应在CMTS端强制执行，而不应在CM执行。CMTS对每一个包含在注册消息和动态业务消息中的QoS集处理该参数。如果省略该参数，则假设缺省值为0（即无限暂停）。对激活的QoS集，该值应小于或等于相应的容许的QoS集中的值，该容许的QoS集中的值也应小于或等于相应的已预置/经授权的QoS集中的值。如果请求的值太大，CMTS可以拒绝该消息，或以小于请求的值来响应。如果注册或动态业务消息被CMTS接受，并且得到CM的确认，则激活的MQoS暂停定时器被加载新的暂停值。如果该消息激活了相关的业务流，则这个定时器也被激活了。如果该消息设置激活的QoS集为空，则将去激活该定时器。

C.2.2.5.7　容许的QoS参数的超时

该参数值规定了在超出激活的QoS参数集时，CMTS应为业务流的容许的QoS参数集保留资源的时间期限。如果在这个时间间隔内没有DSC-REQ来激活容许的QoS参数集，而且也没有DSC来更新QoS参数集并重新开始暂停（见9.1.5.2），那么被容许的而没有被激活的资源应要释放掉，并且只能保留激活的资源。CMTS应设置业务流容许的QoS参数集等于激活的QoS参数集，并且初始化与CM进行的DSC-REQ交换来通知CM这种变更。

类型	长度	值
[24/25].13	2	s

该参数应在CMTS端强制执行，而不应在CM执行。CMTS对每一个包含在注册消息和动态业务消息中的QoS集处理该参数。如果省略该参数，那么假设缺省值为200s。0值意味着业务流能保持在容许状态下无限长的时间，且不应因为没有活动而暂停。但这要受制于CMTS的策略控制。对激活的QoS集，该值应小于或等于相应的容许的QoS集值，该容许的QoS集的值也应小于或等于相应的已预置/已授权QoS集中的值。如果请求的值太大，CMTS可以拒绝该消息，或以小于请求的值来响应。如果包含该参数的注册消息或动态业务消息被CMTS接受，并且得到CM的确认，则容许的QoS暂停定时器被加载新的暂停值。如果该消息所容许的资源大于激活的集，则激活定时器。如果该消息将激活的QoS集与容许的QoS集设为相等，则去激活定时器。

C.2.2.5.8　厂商专用QoS参数

该参数允许厂商对厂商专用QoS参数进行编码。厂商ID应是嵌入在厂商专用QoS参数中的第一个TLV。如果第一个TLV不是厂商ID，则应丢弃该TLV（见C.1.1.17）。

类型	长度	值
[24/25].43	n	

C.2.2.6　上行专用QoS参数编码

C.2.2.6.1　最大级联突发

该参数值规定了业务流所允许的最大级联突发（以字节为单位）。该参数从级联MAC包头的FC字节到级联MAC帧中最后的CRC字节来计算。

0值意味着没有限制。缺省值为0。

该域仅用于CM。如果定义了该参数，则应在CM上强制执行。

注：该值不包含任何物理层的开销。

类型	长度	值
24.14	2	

注：这里只用于级联突发数据。事实上，将该值设置为小于最大以太网数据包容量，该值是合法的，也是有用的。当然，设置为等于或大于最大以太网数据包容量也是合法的。

C.2.2.6.2 业务流调度类型

该参数值规定了哪一个上行调度业务用于上行发送请求和数据包发送。如果省略该参数，则应假定为尽最大努力的业务。

该参数仅用于CMTS。如果已定义，则该参数应由CMTS强制执行。

类型	长度	值
24.15	1	0：保留 1：未定义（取决于CMTS实现方法） 2：最大努力 3：非实时查询业务 4：实时查询业务 5：带有活动检测的主动授权业务 6：主动授权业务 7～255：预留为将来的应用

注： 决定于实现方法的调度业务类型可在24.43厂家特定信息域中规定。

C.2.2.6.3 请求/发送策略

该参数值规定了CM用哪一个IUC机会来为这个业务流发送上行传输请求和数据包，而不论对该业务流的请求是否附带了数据，也不论在该业务流上进行传送的数据包是否能够被级联、分段或抑制有效负载包头。对于UGS，该参数也规定了怎样处理那些不适合UGS授权的数据包。关于对每个业务流调度类型设置该参数的各比特的要求见9.2。

除了最大努力业务以外，所有业务流调度类型都需要该参数。如果在最大努力业务流QoS参数集中省略该参数，则应使用0值作为缺省值。第0位比特（bit#0）是该值域的LSB。比特设置为1用来选择下面定义的行为：

类型	长度	值
24.16	4	Bit#0：业务流不应使用“所有CM”广播请求机会 Bit#1：业务流不应使用优先级请求组播广播请求机会（见A.2.3） Bit#2：业务流不应对请求使用请求/数据机会 Bit#3：业务流不应对数据使用请求/数据机会 Bit#4：业务流不应使用数据进行附带请求 Bit#5：业务流不应级联数据 Bit#6：业务流不应分段数据 Bit#7：业务流不应抑制有效负载包头 Bit#8[1)]：业务流应丢弃不适合主动授权大小的数据包[2)] 所有其它比特保留

注： 数据授权包括长、短两种数据授权。

C.2.2.6.4 标称查询时间间隔

该参数值规定了在上行信道中该业务流连续单播请求机会之间的标称时间间隔（以μS为单位）。它特别适合于实时和非实时查询业务。

执行该参数的理想调度由参考时间t_0来定义，所希望的传输时间见式（C.2）。

$$t_i=t_0+i \times interval \quad \text{(C.2)}$$

1) 此比特只用于主动授权业务流调度类型的业务流。如果此比特在任何其它业务流调度类型中被设定，则应将其忽略。

2) 分类为主动授权业务流的数据包和大于该业务流授权长度的数据包通常在基本业务流上传送。此参数不考虑这种默认的行为。

实际查询时间t'_i应在$t_i<=t'_i<=t_i$+jitter范围内，式中的interval是此TLV规定的时间间隔值，jitter是可容忍的查询抖动。理想查询时间t_i的准确度的测量与用于产生时间戳的CMTS主时钟有关（见8.3）。

该域仅在CMTS端使用。如果定义了该参数，则CMTS应强制执行此参数。

类型	长度	值
24.17	4	μs

C.2.2.6.5 可容忍的查询抖动

该参数值描述了单播请求时间间隔从业务流的标称周期调度（以μs测量）开始延迟的的最大时间值。

执行该参数的理想调度由参考时间t_0来定义，所希望的查询时间见式（C.3）。

$$t_i=t_0+i \times interval \quad (C.3)$$

实际查询时间t'_i应在$t_i<=t'_i<=t_i$+jitter范围内，此处jitter是由此TLV描述的抖动值，interval是标称查询时间间隔。理想查询时间t_i精确度的测量与用于产生时间戳的CMTS主时钟有关（见8.3）。

该参数仅在CMTS端使用。如果定义了该参数，那么该参数代表了CMTS上的一个业务承诺（或容许标准）。

类型	长度	值
24.18	4	μs

C.2.2.6.6 主动授权大小

该参数值规定了以字节为单位的主动授权的大小。授权大小包括从帧控制字节到MAC帧结束的全部MAC帧数据PDU。

该参数在CMTS端使用，且应由CMTS强制执行。

类型	长度	值
24.19	2	

注： 对于UGS，该参数应该由CMTS使用，来计算以微时隙为单位的主动授权的大小。

C.2.2.6.7 标称授权时间间隔

该参数值规定了该业务流的连续数据授权机会之间的标称时间间隔（以μs为单位）。主动授权的和具有活动检测的主动授权的业务流都需要这个参数。

执行该参数的理想调度由参考时间t_0来定义，所希望的发送时间见式（C.4）。

$$t_i=t_0+i \times interval \quad (C.4)$$

实际授权时间t'_i应在$t_i<=t'_i<=t_i$+jitter范围内，其中interval是由此TLV规定的时间间隔值，jitter是可容许的授权抖动。当每个间隔的多个授权被请求时，所有授权应在该间隔内，这样，标称授权时间间隔和可容许的授权抖动都应被CMTS保持以用于该业务流中的所有授权。理想授权时间t_i的准确度的测量与用于产生时间戳的CMTS主时钟有关（见8.3）。

该域对主动授权和具有活动检测调度类型的主动授权来说是强制性的。它仅在CMTS端使用，并应由CMTS执行。

类型	长度	值
24.20	4	μs

C.2.2.6.8 可容忍的授权抖动

该参数值规定了从该业务流的标称周期调度（以μs测量）开始可能被延时的传输机会的最大时间值。

执行该参数的理想调度由参考时间t_0来定义，所希望的传输时间见式（C.5）。

$$t_i=t_0+i \times interval \quad (C.5)$$

实际发送机会t'_I应在$t_i<=t'_i<=t_i$+jitter 范围内，其中jitter是由此TLV规定的抖动值，interval是标称授权时间间隔。理想授权时间ti的准确度的测量与用于产生时间戳的CMTS主时钟有关（见8.3）。

该域对于主动授权和具有活动检测调度类型的主动授权来说是强制性的。它只在CMTS端使用，并应由CMTS强制执行。

类型	长度	值
24.21	4	μs

C.2.2.6.9 每时间间隔的授权数

对于主动授权业务，该参数值表明了每个标称授权时间间隔内数据授权的实际个数。而对于具有活动检测的主动授权业务，该参数值表明了每个标称授权时间间隔内的激活授权的最大数量。该参数的目的是通过动态业务变更机制，使得会话能添加到对一个已存在的主动授权业务流，而不会消极地影响现有的会话。

执行该参数的理想调度由参考间t_0来定义，所希望的传输时间见式（C.6）：

$$t_i=t_0+i \times interval \quad (C.6)$$

实际授权时间t'_i应在$t_i<=t'_i<=t_i$+jitter范围内，其中interval是标称授权时间间隔，jitter是可容许的授权抖动。当每时间间隔的多个授权被请求时，所有的授权都应在这个时间间隔内，这样，标称授权时间间隔和可容许的授权抖动都应被CMTS保持以用于业务流中的所有授权。

该域对主动授权和具有活动检测调度类型的主动授权来说是强制性的。它只在CMTS端使用，并应由CMTS强制执行。

类型	长度	值	有效范围
24.22	1	授权数目	0～127

C.2.2.6.10 业务重写的IP类型

CMTS应用值“new-ip-tos”重写带有IP ToS字节值“orig-ip-tos”的IP包，其中，new-ip-tos=((orig -ip –tos AND tos-and-mask) OR tos-or-mask)。如果省略该参数，则IP包ToS字节不被重写。

该参数仅在CMTS端使用。如果定义了该参数，则CMTS应强制执行。

类型	长度	值
24.23	2	tos-and-mask、tos-or-mask

C.2.2.6.11 主动授权时间参考

对于主动授权业务和具有活动检测的主动授权业务，该参数的值规定了参考时间t_0，从t_0可以导出所希望的传输时间见式（C.7）。

$$t_i=t_0+i \times interval \quad (C.7)$$

其中interval是标称授权时间间隔（见C.2.2.6.7）。该参数只用于从CMTS向CM发送的消息，且仅当一个UGS或UGS-AD业务流正被激活时才可使用。在这种情况下，它是一个强制性的参数。

类型	长度	值	有效范围
24.24	4	CMTS时间戳	0～4 294 967 295

在该参数中规定的时间戳表示CMTS的10.24MHz主时钟的计数状态。因为在向CM发送该参数之前，UGS或UGS-AD业务流总是被激活的，所以只有参考时间t_0紧接着当前时间时，t_0才被CM解释为下一个授权的理想时间。如果t_0在当前时间之前，则CM能够根据式（C.8）计算出从当前时间到下一个授权的理想时间之间的偏移时间间隔。

interval-(((current time-t_0)/10.24)模 interval)……(C.8)

其中：

interval（时间间隔）以μs为单位；

current time（当前时间）和t_0以10.24MHz为单位。

C.2.2.7 下行专用QoS参数编码

最大下行延迟时间

该参数值规定了从CMTS在NSI上接收一个数据包到向它的RF接口转发该数据包之间的最大延迟时间。

如果定义了该参数，则它就代表了CMTS的一项业务承诺（或容许标准），并应得到CMTS的保证。CMTS不必向那些超过CMTS最小下行保留速率的业务流提供此业务承诺。

类型	长度	值
25.14	4	μs

C.2.2.8 有效负载包头抑制

该域定义了与有效负载包头抑制（PHS）有关的参数。

类型	长度	值
26	n	

注： 整个有效负载包头抑制的TLV的长度应小于255字符。

C.2.2.8.1 分类器参考

该域值规定了标识对应分类器的分类器参考（见C.2.1.3.1）。

类型	长度	值
26.1	1	1～255

C.2.2.8.2 分类器标识符

该域值规定了标识对应分类器的分类器标识符（见C.2.1.3.2）。

类型	长度	值
26.2	2	1～65 535

C.2.2.8.3 业务流参考

该域值规定了标识对应业务流的业务流参考（见C.2.2.3.1）。

类型	长度	值
26.3	2	1～65 535

C.2.2.8.4 业务流标识符（SFID）

该域值规定了标识PHS规则应用的业务流的SFID。

类型	长度	值
26.4	4	1～4 294 967 295

C.2.2.8.5 动态业务变更动作

当接收到动态业务变更请求时，该参数表明了应对该有效负载包头抑制字节串所采取的动作。

类型	长度	值
26.5	1	0：添加PHS规则； 1：设置PHS规则； 2：删除PHS规则； 3：删除所有的PHS规则。

“设置PHS规则”命令用于向一个已部分定义的有效负载包头抑制规则添加特定的TLV。当PHSF和PHSS的值不都知道时，PHS规则为部分定义的。当PHSF和PHSS的值都为已知时，PHS规则就变成完全定义的。一旦PHS规则被完全定义，“设置PHS规则”命令就不应用来修改已有的TLV。

“删除所有的PHS规则”命令用来删除一个给定业务流的所有PHS规则。使用该选项时DSC-REQ所需要的PHS参数见7.3.15。

注： 试图添加一个已经存在的PHS规则是错误的。

C.2.2.9 有效负载包头抑制错误编码

该域定义了与有效负载包头抑制错误有关的参数。

类型	长度	值
26.6	n	

一个有效负载包头抑制错误编码包含一个有效负载包头抑制错误参数集，该参数集由以下各个参数定义：出错参数、确认码和错误消息。

有效负载包头抑制错误编码在REG-RSP、DSA-RSP和DSC- RSP消息中返回，以表明接收者对于在REG-REQ、DSA-REQ或DSC-REQ消息中的有效负载包头抑制规则建立请求做出消极响应的原因。

在失败时，对于REG-REQ、DSA-REQ或DSC-REQ消息中至少一个失败的有效负载包头抑制规则请求，REG-RSP、DSA-RDP或DSC-RSP应包括一个有效负载包头抑制错误编码。对于失败的有效负载包头抑制规则，有效负载包头抑制错误编码应包含确认码和出错参数，并且可能包含一个错误消息。如果某些有效负载包头抑制规则集被拒绝，而其它的有效负载包头抑制规则集被接受了，则只有被拒绝的有效负载包头抑制规则应含有有效负载包头抑制错误编码。当整个事务成功时，RSP或ACK消息不应包括有效负载包头抑制错误编码。

因为可能会有多个有效负载包头抑制参数出错，所以在REG-RSP、DSA-RSP或DSC-RSP消息中可能出现多个有效负载包头抑制错误编码。一个即使带有单有效负载包头抑制错误编码的消息也不应包含任何其它协议的有效负载抑制编码（例如，IP，802.1P/Q）。

有效负载包头抑制错误编码不应出现在REG-REQ、DSA-REQ或DSC-REQ消息中。

C.2.2.9.1 出错参数

该参数值标识了在被拒绝的有效负载包头抑制请求中出错的被请求有效负载包头抑制参数的子类型。在已给出的有效负载包头抑制错误编码中，有效负载包头抑制错误参数集应只有一个出错参数的TLV。

类型	长度	值
26.6.1	1	出错的有效负载包头抑制编码子类型

C.2.2.9.2 错误码

该参数表明了请求状态。非0值对应于C.4中所述的确认码。在已给出的有效负载包头抑制错误编码中，有效负载包头抑制错误参数集应只有一个错误码。

类型	长度	值
26.6.2	1	确认码

0值表示有效负载包头抑制请求成功。因为有效负载包头抑制错误参数集仅用于出错参数，所以不应使用该值。

C.2.2.9.3 错误消息

该子类型在有效负载包头抑制错误参数集中是可选的。如果存在，它表示在CM的控制台上显示的文本字符串和/或用于进一步描述被拒绝的有效负载包头抑制请求的日志。在已给出的有效负载包头抑制错误编码中，有效负载包头抑制错误参数集可能没有或有1个错误消息子类型。

类型	长度	值
26.6.3	n	以0结束的ASCII字符串

注 1：长度n包含结尾的0。

注 2：整个的有效负载包头抑制编码消息的总长度应小于256字符。

C.2.2.10 有效负载包头抑制规则编码

C.2.2.10.1 有效负载包头抑制域（PHSF）

该域（PHSF）值是由发送实体抑制并由接收实体恢复的包头字节。在上行时，PHSF对应着从MAC包头校验和之后的第一个字节开始的PDU字节串。在下行时，PHSF对应着从MAC包头校验和之后的第13个字

节开始的PDU的字节串。这个字节串含有PDU包头抑制的和未抑制的字节。在PHSF中未抑制字节的值依赖于具体实现。

PHSF的TLV串域中的字节应按下面的顺序排列：

a) 上行

- PHSF 值的 MSB=PDU 的第 1 个字节；
- PHSF 值的第 2 个 MSB=PDU 的第 2 个字节；
- ……；
- PHSF 值的第 n 个字节（PHSF 值的 LSB）=PDU 的第 n 个字节；

b) 下行

- PHSF 值的 MSB=PDU 的第 13 个字节；
- PHSF 值的第 2 个 MSB=PDU 的第 14 个字节；
- ……；
- PHSF 值的第 n 个字节（PHSF 值的 LSB）=PDU 的第（n+13）个字节。

类型	长度	值
26.7	n	被抑制的字节串

其中长度n值应始终与PHSS的值相同。

C.2.2.10.2 有效负载包头抑制索引（PHSI）

有效负载包头抑制索引（PHSI）为1～255之间的值，该值仅参照被抑制的字节串。该索引对上行方向的每个业务流是唯一的，对下行方向的每个CM上也是唯一的。上行和下行PHSI值相互独立。

类型	长度	值
26．8	1	索引值

C.2.2.10.3 有效负载包头抑制掩码（PHSM）

有效负载包头抑制掩码（PHSM）域值用于解释PHSF中的值，它用在链路上的发送和接收实体。PHSM允许诸如序列号或校验和等数值可变的域不被抑制，而在其周围的固定字节则被抑制掉。

类型	长度	值
26．9	n	0比特位：0=不抑制抑制域的第一个字节； 1=抑制抑制域的第一个字节； 1比特位：0=不抑制抑制域的第二个字节； 1=抑制抑制域的第二个字节； x比特位：0=不抑制抑制域的第（x+1）个字节； 1=抑制抑制域的第（x+1）个字节。

长度n是PHSM的最高限度(PHSS/8)。0比特位是该值域的MSB。PHSM中每一个顺序比特位的值都用来表示PHSF中相应的顺序字节属性。

如果比特位值是"1"(并且校验通过或关闭)，发送实体应抑制该字节，并且接收实体应从其高速缓冲PHSF中恢复该字节。如果比特位值是"0",则发送实体不应抑制该字节，并且接受实体应使用数据包中的下一个字节来恢复该字节。

如果不包含此TLV，则缺省为抑制所有字节。

C.2.2.10.4 有效负载包头抑制大小（PHSS）

该域值表示使用PHS的业务流在PHSF中的总字节数量。

类型	长度	值
26.10	1	抑制字符串中的字节数

当正在建立业务流时,要使用这个TLV。对于所有被分类并被指定给带有激活的PHS业务流的数据包，应根据PHSM的要求对PHSS指明的字节数进行抑制。如果该TLV包含在由0字节值的业务流定义中，则PHS

关闭。非0值表示PHS打开。直到PHSS值已知，PHS规则才被认为得到了部分的定义，并将不执行抑制。当PHSS和PHSF都为已知时,PHS规则成为完全定义。

C.2.2.10.5 有效负载包头抑制校验（PHSV）

该域值向发送实体表明，在进行抑制之前数据包包头的内容是否需要进行校验。如果PHSV打开，则发送者应将数据包包头中的字节和PHSM中指出的PHSF中的要被抑制的字节进行比较。

类型	长度	值
26.11	1	0:校验； 1:不校验。

如果不包括该TLV，则缺省为需要校验。只有发送者应校验要抑制的字节。如果校验失败，则不应抑制有效负载包头(见9.4.3)。

C.2.2.10.6 厂商专用PHS参数

该参数允许厂商对厂商专用PHS参数进行编码。厂商标识符(Vendor ID)应是嵌入在厂商专用PHS参数中的第一个TLV。如果厂商专用PHS参数中的第一个TLV不是厂商ID。则应丢弃这个TLV（见C.1.1.17）。

类型	长度	值
26.43	n	

C.3 其它接口编码

电话设定选项

该配置设定值描述了专用于电话回传系统的参数。它由一些封装了的类型/长度/值（TLV）域组成。参见DOCSIS6。

类型	长度	值
15(=TRI_CFG01)	n	

C.4 确认码

确认码(CC)提供了一种通用方法来指明注册响应、注册确认、动态业务添加响应、动态业务添加确认、动态业务删除响应、动态业务变更响应和动态业务变更确认MAC管理消息的失败。本章中的确认码既可用作消息确认码，又可用作在上述消息中载荷的错误集编码中的错误码。

确认码为下述之一：

- okay/success(0)；
- reject-other(1)；
- reject-unrecognized-configuration-setting(2)；
- reject-temporary/ reject-resource(3)；
- reject-permanent/ reject-admin(4)；
- reject-not-owner(5)；
- reject-service-flow-not-found(6)；
- reject-service-flow-exists(7)；
- reject-required-parameter-not-present(8)；
- reject-header-suppression(9)；
- reject-unknown-transaction-id(10)；
- reject-authentication-failure(11)；
- reject-add-aborted(12)；
- reject-multiple-errors(13)；
- reject-classifier-not-found(14)；

- reject-classifier-exists(15)；
- reject-PHS-rule-not-found(16)；
- reject-PHS-rule-exists(17)；
- reject-duplicate-reference-ID-or-index-in-message(18)；
- reject-multiple-upstream-service-flows(19)；
- reject-multiple-downstream-service-flows(20)；
- reject-classifier-for-another-service-flow(21)；
- reject-PHS-for-another-seivice-flow(22)；
- reject-parameter-invalid-for-context(23)；
- reject-authorzation-failure(24)；
- reject-temporary-DCC(25)。

确认码应按以下方式使用：

- okay/success(0)：指消息被成功接收；
- reject-other(1)：当没有应用其它的原因代码时，使用该代码；
- reject-unrecognized-configuration-setting(2)： 当一个配置设定没有被识别或它的值超出了规定的范围时，使用该代码；
- reject-temporary(3)：也称作 reject-resource，它表明了当前 CMTS 或 CM 的加载阻止了授权请求，但该请求可能在其它时间成功；
- reject-permanent(4)：也称作 reject-admin，表明因为策略、配置或性能的原因，除非手动配置或替换 CMTS 或 CM，否则请求决不会得到授权；
- reject-not-owner(5)：请求者与该业务流无关；
- reject-service-flow-not-found(6)：请求中指出的业务流不存在；
- reject-service-flow-exists(7)：被添加的业务流已存在；
- reject-required-parameter-not-present(8)：请求的参数已被省略；
- reject-header-suppression(9)：由于某种原因，请求的包头抑制不能得到支持；
- reject-unknown-transaction-id(10)： 因为接收端点未将事务视作“正在进行中”(即该消息是预料之外的或次序颠倒了)，故请求的事务延续为无效；
- reject-authentication-failure(11)：因为消息包含一个无效的 CMTS-MIC 或 HMAC-digest，故请求的事务被拒绝；
- reject-add-aborted(12)：动态业务流的添加被动态业务添加初始化程序中断；
- reject-multiple-errors(13)：当检测到多个错误时，使用该代码；
- reject-classifier-not-found(14)：当请求包含一个不认识的分类器 ID 时，使用该代码；
- reject-classifier-exists(15)：表示要添加的分类器的 ID 已经存在；
- reject-PHS-rule-not-found(16)：表示请求包含一个 PHS 规则不存在的 SFID/分类器 ID 对；
- reject-PHS-rule-not-exists(17)：表示添加 PHS 规则的请求包含一个 PHS 规则已经存在的 SFID/分类器 ID 对；
- reject-duplicate-reference-ID-or-index-in-message(18)：表示请求以非法的方式使用了两次 SFR、分类器参考、SFID 或分类器 ID；
- reject-multiple-upstream-service-flows(19)：当 DSA/DSC 包含超过一个上行业务流的参数时，使用该参数；
- reject-multiple-downstream-service-flows(20)：当 DSA/DSC 包含超过一个下行业务流的参数时，使用该参数；
- reject-classifier-for-another-service-flow(21)：当 DSA-REQ 包含正由 DSA 添加的 SF 而不是新 SF 的分类器参数时，在 DSA-RSP 中使用该参数；

- reject-PHS-for-another-service-flow(22)：当 DSA-REQ 包含正由 DSA 添加的 SF 而不是新 SF 的 PHS 规则时，在 DSA-RSP 中使用该参数；
- reject-parameter-invalid-for-context(23)：表示被提供的参数不能在已包含该参数中的编码使用，或表示一个参数值对于已包含该参数的编码是无效的；
- reject-authorization-failure(24)：请求的事务被授权模块拒绝；
- reject-temporary-DCC(25)：表示此时当前信道中被请求的资源不可用，并且在对 CMTS 将发送的 DCC 命令作出响应完成了信道变更后，CM 应该在新信道上重新请求这些资源。如果没有收到 DCC，那么 CM 在当前信道上重新请求资源前应等待至少 T14 的时间。

C.4.1 动态信道变更的确认码

根据C.4，CM可以在DCC-RSP消息中返回一个适当的拒绝码，也可以返回下列确认码中的一个，这些确认码对DCC-RSP来说是唯一的。

- depart（180）；
- arrive（181）；
- reject-already-there（182）。

确认码应按以下方式使用：

- depart（180）：表示 CM 在旧信道上并将要执行跳转到新信道上；
- arrive（181）：表示 CM 已经执行了跳转，并已到达了新信道；
- reject-already-there（182）：表示 CMTS 已要求 CM 移到一个它已经占用的信道。

C.4.2 对主要错误的确认码

这些确认码应只用作在REG-ACK、DSA-RSP、DSA-ACK、DSC-RSP或DSC-ACK消息中的消息确认码，或者用作CM的REG-RSP消息中的响应码。一般来说，与这些确认码有关的错误不可能产生分别与REG-REQ、DSA-REQ或DSC-REQ消息中的参数集有关的错误集，也不可能产生一个完整的RSP消息。这些确认码如下：

- reject-major-service-flow-error（200）；
- reject-major-classifier-error（201）；
- reject-major-PHS-rule-error（202）；
- reject-multple-major-errors（203）；
- reject-message-syntax-error（204）；
- reject-primary-service-flow-error（205）；
- reject-message-too-big（206）；
- reject-invalid-modem-capabilities（207）。

确认码应只按以下方式使用：

- reject-major-service-flow-error（200）：表示 REQ 消息在业务流编码中没有 SFR 或 SFID，且业务流主要错误是唯一的主要错误；
- reject-major-PHS-rule-error（201）：表示 REQ 消息没有分类器参考，或没有分类器 ID 和 SFID，且分类器主要错误是唯一的主要错误；
- reject-multiple-syntax-error（202）：表示 REQ 消息没有业务流参考/标识符和分类器参考/标识符，且 PHS 规则主要错误是唯一的主要错误；
- reject-multiple-major-errors（203）：表示 REQ 消息包含类型 200、201、202 的多个主要错误。
- reject-message-syntax-errors（204）：表示 REQ 消息包含导致解析失败的语法错误（例如 TLV 长度错误）；
- reject-primary-service-flow-error（205）：表示 REG-REQ 或 REG-RSP 消息没有定义一个请求的基本业务流，或一个请求的基本业务流没有被规定为激活的；

- reject-message-too-big（206）：当需要响应的消息长度超过了所允许的最大消息长度时，使用该参数；
- reject-invalid-modem-capabilities（207）：表示 REG-REQ 包含了无效的 CM 性能组合或者与 REG-REQ 中的业务不一致的 CM 性能。

附 录 D
(规范性附录)
CM 配置接口规范

D.1 CM IP寻址

CM使用的DHCP域

下列域应出现在来自CM的DHCP请求中并应按下面所述设置：

- 硬件类型（htype）应设置为 1（以太网）；
- 硬件长度（hlen）应设置为 6；
- 客户硬件地址(chaddr)应设置成与 CM 的 RF 接口相关的 48bit MAC 地址；
- 应包括“ 客户标识符 ”选项， 其硬件类型设置为１，其值设置为与 chaddr 域相同的 48bit MAC 地址；
- 选项码 60（供应商分类 ID）— 允许区分 DOCSIS 1.1 和 DOCSIS 1.0 的 CM 请求，CM 应在选项码 60 中发送 ASCII 代码串“ docsis1.1:xxxxxxx ”。其中 xxxxx 应是该 CM 性能 16 进制编码的 ASCII 表示，见 C.1.3.1。例如，某 DOCSIS1.1 CM 的前两个 TLV（级联和 DOCSIS 版本）的 ASCII 编码应该是 05nn 010101020101。注意，DOCSIS1.1 CM 需要更多的 TLV 并且域“ nn ”将包含所有 TLV 的长度。本例为简单起见只给出了两个 TLV；
- 应包括“ 参数请求列表 ”选项。在列表中应包括的选项码为：
  —— 选项代码１（子网掩码）；
  —— 选项代码２（时间偏移）；
  —— 选项代码３（路由器选项）；
  —— 选项代码４（时间服务器选项）；
  —— 选项代码７（日志服务器选项）。

在返回到CM的DHCP响应中期待下列域出现。CM应根据DHCP响应来配置自己：

- 由 CM 使用的 IP 地址（yiaddr）；
- 在下一阶段引导过程中使用的 TFTP 服务器的 IP 地址（siaddr）；
- 如果 DHCP 服务器在不同网络上则需要一个中继代理，从而需要中继代理的 IP 地址（giaddr）；

注： 这可能与第一跳路由器的IP地址不同。

- CM 从 TFTP 服务器读取的 CM 配置文件名（file）；
- 由 CM 使用的子网掩码（子网掩码，选项 1）；
- CM 与统一协调时（UTC）的偏差（时间偏移，选项 2）。它被 CM 用来计算本地时间，供时戳错误日志使用；
- 用于转发由 CM 发出的 IP 数据的一个或多个路由器的地址列表（路由器选项，选项 3）。CM 不必使用多于一个的路由器 IP 地址用于转发，但应至少使用一个地址；
- 时间服务器清单参见 RFC-868，从中可获得当前时间（时间服务器选项，选项 4）；
- SYSLOG 服务器清单，有关记录日志的信息可以送到这些服务器（记录服务器选项，选项 7）参见 DOCSIS5。

如果初始化期间在DHCP响应中关键域丢失或失效，CM应记录一条错误日志，并重新初始化其MAC，继续扫描信道。

如果初始化期间在DHCP响应中非关键域丢失或失效,CM应记录一条告警日志,忽略该域并继续运行,并作如下考虑：

- 如果子网掩码丢失或无效，CM 应使用 RFC-791 定义的 A、B 或 C 类默认的子网掩码；
- 如果时间服务器丢失或无效，CM 应按 1970 年 1 月 1 日 0 时 0 分 0 秒初始化时间。

如果续约或重新绑定期间在DHCP响应中IP地址域丢失或失效，CM应记录一条错误日志，并重新初始化其MAC，继续扫描信道。

如果续约或重新绑定期间在DHCP响应中任何其他关键或非关键域丢失或失效,CM应记录一条告警日志，忽略该域并保持运行。

为帮助DHCP服务器区分CM的和来自CPE侧局域网的发现请求，CMTS应按如下执行：

- 所有 CMTS 都应支持 DHCP 中继代理信息选项 [ID-DHCP]。特别是，在发现请求将转发到 DHCP 服务器之前，CM 产生或用代理远端 ID 子选项域桥接 DHCP 发现请求，CMTS 应包括 CM 的射频接口 48bitMAC 地址；
- 当 CMTS 是一个路由器，如果 CM 和 CPE 侧的工作站被配置到不同的 IP 子网，则 CMTS 应利用 giaddr 域来区分它们。桥接型 CMTS 也应该提供该项功能。

D.2 CM的配置

D.2.1 CM的二进制配置文件格式

CM专用的配置数据应包含在通过TFTP下载到CM的文件中。该文件是一个二进制文件，其格式与厂商扩展数据为DHCP定义的格式相同（参见RFC-2132）。

它应由若干配置设置组成（每参数一个设置），设置的形式为：

类型　　长度　　数值

其中：

- “ 类型 ”是一个定义该参数的 8bit 标识符；
- “ 长度 ”是一个单 8bit 组,它包含数值域的以 8bit 组形式表示的长度(不包括类型和长度域)；
- “ 数值 ”为从 1 至 254 个 8bit 组，它表示该参数的特定值。

这些配置设置应在文件中相互直接跟随，成为一个没有记录标记的8bit组数据流。

配置设置分为三类：

- 应提出的标准配置设置；
- 可以提出的标准配置设置；
- 厂商特定的配置设置。

CM应能够处理所有的标准配置设置，应忽略配置文件中出现的它不理解的任何配置设置。

为了统一管理 CM应支持最小8192字节的配置文件。

预置信息的鉴权由两个消息完整性检验（MIC）配置设置提供，即CM MIC和CMTS MIC：

- CM MIC 是为确保从预置服务器发送的数据在途中不被修改的一个摘要。它不是一个被鉴权的摘要（它不包括任何共享的秘密）；
- CMTS MIC 是在注册期间为 CMTS 鉴权预置服务器的一个摘要。它是从若干域得出的，其中一个域是 CMTS 与预置服务器之间的共享秘密。

使用CM MIC可使CMTS不必接受整个文件就可鉴别预置数据。

文件的格式如图D.1所示。

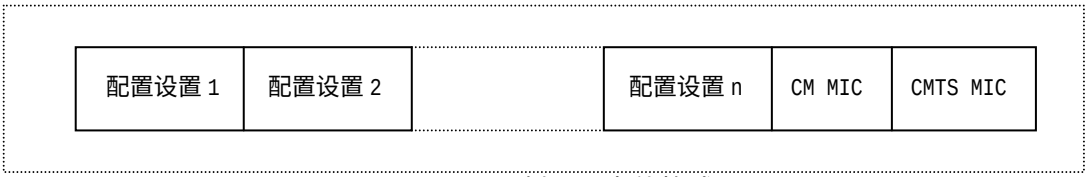


图 D.1 二进制配置文件格式

D.2.2 配置文件设置

下列配置设置应包含在配置文件中，且应得到所有CM支持。CM不应发送缺少这些强制性条目的配置文件的REG-REQ。

- 网络接入配置设置；
- CM MIC 配置设置；
- CMTS MIC 配置设置；
- 结束配置设置；
- DOCSIS 1.0 业务分类配置设置。

--或--

- 上行业务流配置设置；
- 下行业务流配置设置。

注： 应为EuroDOCSIS 1.0的CM提供EuroDOCSIS 1.0业务分类配置。如果是EuroDOCSIS 1.0的CM，则应该只为其预置EuroDOCSIS 1.0业务分类配置信息，否则，它应该按业务流配置设置预置。

下列配置设置可以包含在配置文件中，如果存在，则所有CM都应支持。

- 下行频率配置设置；
- 上行信道 ID 配置设置；
- 加密配置设置；
- 软件升级文件名配置设置；
- 上行数据包分类设置；
- 下行数据包分类设置；
- SNMP 写接入控制；
- SNMP MIB 对象；
- 软件服务器 IP 地址；
- CPE 以太网 MAC 地址；
- 最大 CPE 个数；
- 最大分类器数；
- 加密使能配置设置；
- 有效负载包头抑制；
- TFTP 服务器时戳；
- TFTP 服务器预置 CM 地址；
- 填充配置设置。

下列配置设定可以包含在配置文件中，如果存在且适用于这类CM，则应得到支持：

- 电话设置选项。

下列配置设置可以包含在配置文件中，如果存在则CM可以支持：

- 厂商专用的配置设置。

注： 对注册请求帧和注册响应帧的大小都有限制（见7.2.5.2）。配置文件不能太大而使CM或CMTS超过该限制。

D.2.3 配置文件的生成

生成配置文件所需的步骤见图D.2至图D.5。

a) 为 CM 所需的所有参数创建类型/长度/数值（TLV）条目，见图 D.2。

参数 1 的类型、长度、值
参数 2 的类型、长度、值
……
……
参数 n 的类型、长度、值

图 D.2 创建 CM 所需参数的 TLV 条目

b) 计算 CM MIC 计算中定义的 CM 消息完整性检验（MIC）配置设置值，并且使用该域中定义的码及长度值将其添加到文件的最后一个参数后，见图 D.3。

参数 2 的类型、长度、值
……
……
参数 n 的类型、长度、值
CM MIC 的类型、长度、值

图 D.3 添加 CM MIC

c) 计算 CMTS MIC 计算中定义的 CMTS 消息完整性检验（MIC）配置设置值。并且使用该域中定义的码及长度值将其添加到文件的 CM MIC 后。见图 D.4。

参数 1 的类型、长度、值
参数 2 的类型、长度、值
……
……
参数 n 的类型、长度、值
CM MIC 的类型、长度、值
CMTS MIC 的类型、长度、值

图 D.4 添加 CMTS MIC

d) 添加数据结束标记，见图 D.5。

参数 1 的类型、长度、值
参数 2 的类型、长度、值
……
……
参数 n 的类型、长度、值
CM MIC 的类型、长度、值
CMTS MIC 的类型、长度、值
数据结束标记

图 D.5 添加数据结束标记

CM MIC的计算

CM的消息完整性检验配置设置应通过对所有配置设置域的字节进行MD5摘要计算得到。计算时应按照它们出现在TFTP中的映像进行，而不管TLV顺序或内容如何。有两种例外可以不考虑TFTP中的映像内容：

a) 计算中 CM MIC TLV 的字节本身已被省略，这包括类型、长度及值域；

b) 计算中 CMTS MIC TLV 的字节本身已被省略；这包括类型、长度及值域。

在收到配置文件后，CM应重新计算摘要（digest）并将其与文件中的CM MIC配置设置进行比较。如果摘要不能与之匹配，则应丢弃该配置文件。

D.3 配置检验

检验CM的配置文件来自一个可靠的源是必要的。CMTS和配置服务器共享一个鉴权字符串用来检验注册请求中的CM配置部分。

CMTS MIC的计算

CMTS消息完整性检验配置设置应通过对下列存在于配置文件中的配置设置域按所示的次序进行MD5摘要来计算：

- 下行频率配置设置；
- 上行信道 ID 配置设置；
- 网络接入配置设置；
- EuroDOCSIS 1.0 业务分类配置设置；
- 加密配置设置；
- 厂商专用的配置设置；
- CM MIC 配置设置；
- 最大 CPE 个数；
- TFTP 服务器时戳；
- TFTP 服务器预置 CM 地址；
- 上行数据包分类设置；
- 下行数据包分类设置；
- 上行业务流配置设置；
- 下行业务流配置设置；
- 最大分类器数；
- 加密使能配置设置；
- 有效负载包头抑制；
- 用户管理控制；
- 用户管理 CPE IP 表；
- 用户管理过滤组。

上述清单说明了对配置设置类型域计算CMTS MIC值时的操作顺序。CMTS应按接收时的顺序在相同类型的TLV上计算CMTS MIC。在类型域内，CMTS应按接收时的顺序在子类型上计算CMTS MIC。为了使CMTS正确计算CMTS MIC，CM不应在其注册请求信息的任何给定类型内对相应类型或子类型的配置文件的TLV重新排序。

在计算CM MIC时，应把所有的配置设置域当作相邻的数据处理。

应将摘要添加到配置文件中，类似于其自身采用CMTS MIC配置设置编码的配置设置域。

鉴权字符串是预置服务器（它创建配置文件）与CMTS间的共享秘密。它允许CMTS来鉴别CM预置。鉴权字符串将用作计算D.3所述的加密CMTS MIC摘要时的密钥。

共享秘密的管理机制由系统操作员决定。

收到配置文件后，CM应将CMTS MIC作为注册请求（REG-REQ）的一部分转发。

收到REG-REQ后，CMTS应对所包括的域和鉴权字符串重新计算摘要并将其与文件中的CMTS MIC配置设置相比较。若摘要不能与之匹配，则应通过在注册响应状态域中设置鉴权失败结果来拒绝注册请求。

摘要的计算

CMTS MIC摘要域应使用RFC-2104中定义的HMAC-MD5来进行计算。

附 录 E
(资料性附录)
MAC 业务定义

当本附录与本部分的正文不一致时，以本部分正文内容为准。

E.1 MAC业务综述

MAC提供了一个与上层业务的协议服务接口。上层业务的例子包括桥接、嵌入式应用（例如Packetcable/VOIP）、主机接口(例如带NDIS驱动的NIC适配器）以及第三层路由器（例如IP路由器）。

MAC业务接口定义了上层业务与MAC之间的功能分层。因此，它定义了MAC协议之下所提供的MAC功能。该接口是一个协议接口，不是特定的实现接口。

下列数据业务由MAC业务接口提供：

- 将数据包分类并发送到 MAC 业务流上的一种 MAC 业务；
- 从业务流上接收数据包的一种 MAC 业务。可以接收带抑制包头的数据包；
- 发送及接收带抑制包头数据包的一种 MAC 业务。发送的数据包包头按匹配分类器规则抑制。接收到的抑制数据包的包头根据 CM 和 CMTS 议定的数据包包头索引来重新生成；
- 用于 MAC 和上层业务之间授权定时同步的一种 MAC 业务。在诸如嵌入的 Packetcable/VOIP 客户的应用中需要这种时钟同步，此时，数据分组的周期需要与来自 CMTS 的授权调度同步；
- 用于上层时钟与 CMTS 控制的主时钟同步的一种 MAC 业务。

应注意的是，基于过滤业务的防火墙和策略可以插入MAC层和上层业务之间，但这种业务未包括在MAC业务模型定义中。

下列控制业务由MAC业务接口提供：

- 用于在注册时使上层认知预置业务流的存在并了解 QoS 流量参数设置的一种 MAC 业务；
- 用于使上层创建业务流的一种 MAC 业务。使用该业务，上层启动业务流的有效的/激活的 QoS 参数集、分类器规则以及数据包抑制包头；
- 用于使上层删除业务流的一种 MAC 业务；
- 用于使上层改变业务流的一种 MAC 业务。通过该业务使上层可以修改有效的/激活的 QoS 参数集、分类器规则及数据包抑制包头；
- 用于控制带抑制包头 PDU 的分类和传输的一种 MAC 业务。对于单个分类规则最多定义一个抑制包头。上层业务负责定义抑制包头（包括 wild－card don't suppress 域）和区分各个包头的唯一分类规则。除分类规则外，如果上层业务如此配置，MAC 业务还能进行所有剩余包头字节的全匹配，以防止产生错误包头；
- 用于 QoS 流量资源双阶段控制的一种 MAC 业务。由上层业务控制的双阶段激活在合适的业务请求内提供容许的 QoS 参数和激活的 QoS 参数。收到一个肯定的指示后，上层业务就知道容许的 QoS 参数集已由 CMTS 保留，且容许的 QoS 参数已被 CMTS 激活。除了灾难性的故障（诸如重新改变上行物理层带宽的大小），容许的资源将确保供激活使用，且激活的资源将确保可用于数据包传输。

还可能存在一种控制功能，它用于定位一个未使用的业务流并把它或者一个特定标识的业务流绑定到特定的上层业务上。这种功能的细节没有规定且与具体的执行方法有关。

在MAC业务接口处还可能存在其它控制功能，诸如对激活的业务流状态和数据包分类表排队功能，或者从MAC业务至上层业务的一些功能，使上层业务能为对等MAC层业务所请求的业务流授权。但该功能未包括在MAC业务模型定义中。

还存在其它与业务流不相关的MAC业务，诸如控制MAC业务的MAC地址及SAID组播过滤功能，但该功能未包括在MAC业务模型定义中。

MAC业务参数

MAC业务利用下列参数。有关这些参数的详细描述可参阅工作原理和本部分的其它有关章条。

a） 业务流 QoS 流量参数

MAC的激活-业务-流和改变-业务-流原语允许提供通用、上行及下行QoS流量参数。当提供这些参数时，它们将替代在预置时间或由上层业务建立业务流时为这些参数配置的任何数值；

b）激活的/容许的QoS流量参数

如果正在使用双阶段业务流激活，则要控制两个完整的QoS流量参数集。容许的QoS参数说明对CMTS授权资源的保留要求。激活的QoS参数说明对CMTS授权资源激活的要求。容许的QoS参数可以由上层业务在将来激活。激活的QoS参数可以被上层业务立即使用；

c）业务流分类过滤规则

对于由上层业务控制的每个业务流，可以提供零个或多个分类过滤规则。分类器用一个分类器标识符来识别；

d）业务流PHS抑制包头

可以为每个业务流定义零个或多个带有其相关的校验控制和掩码变量的PHS抑制包头字符串。当这些包头被定义时，它们就与特定的分类规则建立了一对一的联系。为了重新产生带抑制包头的数据包，应在CM和CMTS之间议定一个有效负载包头抑制索引。

E.2 MAC数据业务接口

MAC业务被定义为向业务流发送和从业务流接收数据。典型情况是：一个上层业务通过将各类别数据流量映射到不同的业务流的方式使用业务流。对业务流的映射可定义为低优先级数据流、高优先级数据流、及诸如恒比特速率数据流等多种特定级别数据流，由CMTS在MAC层通过周期性授权进行调度。

下列特定的数据业务接口由MAC业务向上层业务提供。它们表示所提供业务的一个抽象概念并不意味着一个特定的实现：

- MAC_DATA.request；
- MAC_DATA.indicate；
- MAC_GRANT_SYNCHRONIZE.indicate；
- MAC_CMTS_MASTER_CLOCK_SYNCHRONIZE.Indicate。

E.2.1 MAC_DATA.request

由上层业务发出，用于请求分类并向射频传输一个IEEE 802.3或DIX格式的PDU。

参数：

- PDU——IEEE 802.3 或 DIX 编码的 PDU 包括所有第二层的包头域及选项 FCS。PDU 是唯一的强制性参数；
- 填充——用于当 PDU 长度小于 60 字节，又要求保持 GB/T15629.3-1995 透明性时；
- SFID——如果存在，则 MAC 业务跳过数据包分类功能并将数据包映射到由 SFID 指定的业务流上；

- 业务分类名、规则优先级——如果存在，只要不存在比所提供的规则优先级更高的规则优先级分类器，则该元组将识别数据包所映射到的激活业务流的业务分类名。

扩展业务描述：

从上层业务发送一个PDU到MAC/PHY。唯一的强制性参数是PDU，它包含所有第二层的包头、第三层的包头、数据及(可选的)第二层校验和。

如果PDU是唯一的参数，则数据包要受MAC数据包分类过滤功能的控制，以便确定该数据包怎样映射到特定的业务流。数据包分类操作的结果决定了该数据包将在哪一个业务流上发送、以及是否应带抑制包头发送。

如果提供了参数SFID，则数据包可被引导到特别标识的业务流。

如果提供了参数元组业务分类名、规则优先级，只要不存在比所提供的规则优先级高的分类器，则数据包被引导到第一个与业务分类名匹配的激活业务流。上层策略执行者使用该服务允许零个或多个动态规则与选定的数据流(例如语音)相匹配，而所有其它数据流被强制到已命名业务流类别内的业务流上。如果不存在具有该业务分类名的激活业务流，则该业务执行正常的数据包分类。

在所有情况下，如果未发现匹配分类器，或没有任何映射到特定业务流的参数组合，则数据包将被引导到基本业务流。

下述伪代码描述了MAC_DATA请求业务接口打算要做的操作：

```
MAC_DATA.request
    PDU
    [SFID]
    [ServiceClassName，RulePriouity]
```

FIND_FIRST_SERVICE_FLOW_ID(ServiceClassName) 当其业务分类名等于该程序参数时，则返回第一个业务流的SFID；如果未发现匹配的业务流，则为空。

SEARCH_CLASSIFIER_TABLE(PriorityRange) 在特定优先范围内搜索所有的规则并返回与规则相关的业务流标识符；如果未发现分类器规则，则为空。

```
TxServiceFlowID = NULL
IF (ServiceFlowID DEFINED)
TxServiceFlowID = MAC_DATA.ServiceFlowID
ELSEIF (ServiceClassName DEFINED and RulePriority DEFINED)
TxServiceFlowID = FIND_FIRST_SERVICE_FLOW_ID (ServiceClassName)
SearchID = SEARCH_CLASSIFIER_TABLE (All Priority Levels)
IF (SearchID not NULL and ClassifierRule.Priority >= MAC_DATA.RulePriority)
TxServiceFlowID = SearchID
ELSE [PDU only]
TxServiceFlow = SEARCH_CLASSIFIER_TABLE (All Priority Levels)
IF (TxServiceFlowID = NULL)
TRANSMIT_PDU (PrimaryServiceFlowID)
ELSE
TRANSMIT_PDU (TxServiceFlowID)
```

E.2.2 MAC_DATA.indicate

由MAC发出，指示上层业务接收来自射频的IEEE 802.3或DIX PDU。

参数：

PDU —IEEE 802.3或DIX编码的PDU，包括所有第2层的包头域和FCS。

E.2.3 MAC_GRANT_SYNCHRONIZE.Indicate

由MAC业务向上层业务发出，指示来自CMTS的授权到达的时间。如果从收到来自CMTS的授权到达指示到授权实际到达之间存在时延且在充许的授权抖动范围内，它不说明上层是如何造成该时延的。应注意在UGS应用中， MAC层业务将根据每个间隔QoS流量参数的授权数来增加授权速率或减少授权速率；随着每个间隔授权数的增加或减少，授权到达的时间也将变化；当与CMTS下行主时钟达到同步时，每个激活的业务流只需要一次这种指示。这里没有指出如何实现该项功能。

参数：

ServiceFlowID —接收授权的特定激活业务流的唯一的标识符值。

E.2.4 MAC_CMTS_MASTER_CLOCK_SYNCHRONIZE.indicate

由MAC业务发出到上层业务，指示CMTS主时钟的定时。这里没有给出由MAC业务将该指示传送到上层业务的传送频度或次数，也没有指出如何实现该项功能。

参数：

未指定参数。

E.3 MAC控制业务接口

定义了一个MAC业务的集合用于MAC业务流和分类器的控制。应注意，上层业务可使用这些业务来提供上层流量的结构，诸如：“ 连接 ”或“ 子业务流 ”或“ 微业务流 ”。然而，除了修改个别分类器的能力外，上层模型没有明确的语义。因而MAC业务流QoS参数的控制在该集合中规定。

下列具体的控制业务接口功能由MAC业务向上层业务提供。它们表示所提供业务的一个抽象概念，不表示一个具体的实现：

- MAC_REGISTRATION_RESPONSE. Indicate；
- MAC_CREATE_SERVICE_FLOW. request/response/indicate；
- MAC_DELETE_SERVICE_FLOW. request/response/indicate；
- MAC_CHANGE_SERVICE_FLOW. request/response/indicate。

E.3.1 MAC_REGISTRATION_RESPONSE. indicate

由DOCSIS MAC发出到上层业务，指示完整业务流集和业务流QoS流量参数在MAC注册阶段已被预置和授权。后续对业务流激活状态的改变或业务流的添加、删除都被传输到上层业务，并由其它MAC控制业务指示。

参数：

注册TLV — 业务流和业务流参数定义所需要的所有TLV，包括预置QoS参数。见本部分的正文。

E.3.2 MAC_CREATE_SERVICE_FLOW. request

由上层业务发出到MAC，请求在MAC业务内建立新业务流。该原语不对已配置的和已注册的业务流发出，而是对被动态创建的业务流发出。该原语也可为业务流定义分类器并提供容许的和激活的QoS参数。本项功能调用DSA信令。

参数：

- SFID — 正在创建的具体业务流的唯一标识符值；
- 业务分类名 — 正在创建的业务流分类名称；
- 容许的 QoS 参数 — 业务流的零个或多个上行、下行及一般通信流量参数；
- 激活的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 业务流有效负载包头抑制规则 — 每个由上层业务控制的业务流的零个或多个 PHS 规则；
- 业务流分类过滤规则 — 每个由上层业务控制的业务流的零个或多个分类过滤规则。分类器由分类标识符来标识。

E.3.3 MAC_CREATE_SERVICE_FLOW.response

由MAC业务发出到上层业务，指出创建业务流请求的成功或失败。

参数：

- SFID — 正在创建的特定业务流的唯一标识符值；
- 响应码 — 成功或失败码。

E.3.4 MAC_CREATE_SERVICE_FLOW.indicate

由MAC业务发出，通知上层业务在MAC业务内创建了一个新业务流。该原语不对已从管理上预配置的业务流发出，而是对动态定义的业务流发出。在本部分中，此项通告仅作参考。

参数：

- SFID — 正在创建的特定业务流的唯一标识符值；
- 业务分类名 — 正在创建的业务流分类名称；
- 容许的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 激活的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 业务流有效负载包头抑制规则 — 每个由上层业务控制的业务流的零个或多个 PHS 规则；
- 业务流分类过滤规则 — 每个由上层业务控制的业务流的零个或多个分类过滤规则。分类器由分类标识符来标识。

E.3.5 MAC_DELETE_SERVICE_FLOW.request

由上层业务发出到MAC，请求删除一个业务流和所有QoS参数，包括所有相关的分类器和PHS规则。本功能调用DSD信令。

参数：

SFID - 被删除业务流的唯一标识符值。

E.3.6 MAC_DELETE_SERVICE_FLOW.response

由MAC发出到上层业务，指示删除业务流请求的成功或失败。

参数：

响应码 - 成功或失败码。

E.3.7 MAC_DELETE_SERVICE_FLOW.indicate

由MAC发出，通知上层业务在MAC业务内业务流的删除。

参数：

SFID - 被删除业务流的唯一标识符值。

E.3.8 MAC_CHANGE_SERVICE_FLOW.request

由上层业务发出到MAC，请求修改特定已创建并获得的业务流。本项功能可以定义完全的分类器集和分类器的添加/删除。本项功能定义了业务流完整的容许和激活QoS参数集。该功能调用了DSC MAC 层信令。

参数：

- SFID — 正被修改的特定业务流的唯一标识符值；
- 具有添加/删除语义及 LLC、IP 和 802.1pq 参数的零个或多个分类规则；
- 容许的 QOS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 激活的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 业务流有效负载包头抑制规则 — 每个由上层业务控制的业务流的零个或多个 PHS 规则；
- 业务流分类过滤规则 — 每个由上层业务控制的业务流的零或多个规则。分类器由分类标识符来标识。

E.3.9 MAC_CHANGE_SERVICE_FLOW.response

由MAC业务发出到上层业务，指示业务流变更请求的成功或失败。

参数：

- SFID — 正在被释放的特定业务流的唯一标识符值；

- 响应码 — 成功或失败码。

E.3.10 MAC_CHANGE_SERVICE_FLOW.indicate

由DOCSIS MAC业务发出，通知上层业务有一个业务流变更的请求。本部分中这种通告仅作参考，在业务流被改变前不需要确认。“改变业务流”的指示是在DSC信令基础上产生的。DSC信令的启动可以基于对等上层业务间及其MAC业务间的“改变业务流”事件，或基于网络资源故障，诸如物理层总可用带宽的改变。上层业务如何对容许的或保留的QoS流量参数的强制性减少做出反应并未作规定。

参数：

- SFID — 正在被激活的业务流的唯一标识符；
- 具有 LLC、IP 和 802.1pq 参数及零个或多个 PHS_CLASSIFIER_IDENTIFIER 的包分类规则；
- 容许的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 激活的 QoS 参数 — 业务流的零个或多个上行、下行及通用流量参数；
- 业务流有效负载包头抑制规则 — 每个由上层业务控制的业务流的零个或多个 PHS 规则。

E.4 MAC业务用法梗概

上层实体利用由MAC提供的业务是为了控制业务流和收发数据包。上层业务与MAC业务之间的功能划分由下列梗概示出。

E.4.1 从上层业务到MAC数据业务的PDU传输

从上层业务到MAC数据业务的PDU传输包括：

- 上层业务通过 MAC_DATA 业务发送 PDU；
- MAC_DATA 业务使用分类表对传送来的 PDU 分类并在适当的业务流上发送该 PDU。分类功能也可使数据包包头按照与分类规则一起保存的包头抑制模板抑制。上层业务有可能跳过该分类功能；
- MAC_DATA 业务基于 QoS 流量整形参数强制所有业务流执行；
- MAC_DATA 业务按 MAC 层调度在射频上发送 PDU。

E.4.2 从MAC数据业务到上层业务的PDU的接收

从MAC数据业务到上层业务的PDU的接收包括：

- PDU 是从射频接收的；
- 如果 PDU 带抑制包头发送，则在数据包被进一步处理之前，恢复包头；
- 在 CMTS 中，MAC_DATA 业务使用分类表将来自射频的 PDU 进行分类，然后监督 QoS 流量整形并如同 CM 中所进行的那样使寻址生效。在 CM 中，不需要对来自射频的每个数据包进行业务流分类；
- 上层业务从 MAC_DATA.indicate 业务中接收 PDU。

E.4.3 MAC控制和MAC数据业务顺序示例

一种可能的CM侧MAC业务功能（建立、获取、修改，然后使用一个特定业务流）的顺序如下：

- MAC_REGISTER_RESPONSE.indicate

获知任何预置的业务流及它们预置的QoS通信流量参数；

- MAC_CREATE_SERVICE_FLOW.request/response

如果已知道业务流没有被MAC_REGISTER_RESPONSE业务接口预置，则利用此业务接口创建新业务流。创建一个业务流要调用DSA信令；

- MAC_CHANGE_SERVICE_FLOW.request/response

定义容许的和激活的QoS参数集、分类器及数据包抑制包头。改变一个业务流要调用DSC信令；

- MAC_DATA.request

将PDU送到MAC业务进行分类和传输；

- MAC_DATA.indication

接收来自MAC业务的PDU；

- MAC_DELETE_SERVICE_FLOW.request/response

删除业务流。很可能只在动态建立业务流时调用，而不对预置的业务流调用。删除业务流使用DSD信令。

附 录 F
（资料性附录）
前同步码序列实例

F.1 引言

可编程的前同步码超字符串（前同步码模式）长度可达1024比特，是整个信道的特征或属性的一部分，它通常适用于该信道的所有突发特征（见7.3.3，表34），但每个突发特征都可以指定前同步码在前同步码模式中的起始位置及前同步码长度（见7.3.3，表35）。前同步码的第一比特由7.3.3表35中前同步码偏移值指定。前同步码模式的第一比特是进入符号映射器的第一比特（图13），并且是突发的第一个符号的I1（见5.1.2.2）。例如，根据表35，对于前同步码偏移值=100，则前同步码模式的第101比特是进入符号映射器的第一比特，第102比特是进入符号映射器的第二比特，且被映射到Q1…等等。F.2给出了一个1024比特长的前同步码超字符串。

F.2 前同步码序列举例

下面是1024比特长的前同步码序列举例。

比特1～128：

1100 1100 1111 0000 1111 1111 1100 0000 1111 0011 1111 0011 0011 0000 0000 1100
0011 0000 0011 1111 1111 1100 1100 1100 1111 0000 1111 0011 1111 0011 1100 1100

比特129～256：

0011 0000 1111 1100 0000 1100 1111 1111 0000 1100 1100 0000 1111 0000 0000 1100
0000 0000 1111 1111 1111 0011 0011 0011 1100 0011 1100 1111 1100 1111 0011 0000

比特257～384：

1100 0011 1111 0000 0011 0011 1111 1100 0011 0011 0000 0011 1100 0000 0011 0000
0000 1110 1101 0001 0001 1110 1110 0101 0010 0101 0010 0101 1110 1110 0010 1110

比特385～512：

0010 1110 1110 0010 0010 1110 1110 1110 1110 1110 0010 0010 0010 1110 1110 0010
1110 1110 1110 0010 1110 0010 1110 0010 0010 0010 0010 1110 0010 0010 1110 0010

比特513～640：

0010 0010 1110 1110 1110 1110 1110 1110 0010 1110 0010 1110 0010 1110 1110 0010
0010 1110 1110 0010 1110 1110 1110 0010 1110 1110 0010 1110 0010 0010 1110 0010

比特641～768：

0010 1110 1110 1110 0010 0010 0010 1110 0010 1110 1110 1110 1110 0010 0010 1110
0010 1110 0010 0010 0010 1110 1110 0010 0010 0010 0010 1110 0010 0010 0010 0010

比特769～896：

0010 1110 1110 1110 1110 1110 1110 0010 1110 0010 1110 0010 1110 1110 0010 0010
1110 1110 0010 1110 1110 1110 0010 1110 1110 0010 1110 0010 0010 1110 0010 0010

比特897～1024：

1110 1110 1110 0010 0010 0010 1110 0010 1110 1110 1110 1110 0010 0010 1110 0010
1110 0010 0010 0010 1110 1110 0010 0010 0010 0010 1110 0010 0010 0010 0010 1110

附 录 G
（资料性附录）
多个上行信道

本附录与本部分正文之间发生冲突时，以本部分正文为准。

6.2描述了对多个上行信道和多个下行信道的支持。CM在它所连接的电缆网段上可以看到的变化包括：

- 每个电缆网段上单个下行和单个上行；
- 每个电缆网段上单个下行和多个上行；
- 每个电缆网段上多个下行和单个上行；
- 每个电缆网段上多个下行和多个上行。

每个CM要求一个上行和一个下行信道的典型应用是浏览(Web browsing)。网上浏览倾向于非对称的带宽需求，正好与有线网的非对称带宽相适应。

每个CM要求接入到多个上行中的一个信道的典型应用是IP电话。IP电话倾向于对称的带宽需求。如果在一个地区有大量集中的CM，且所有业务都通过同一个光节点，则为了提供足够的带宽和防止呼叫阻塞，可能需要多于1个上行。

每个CM要求接入到多个下行中的一个信道的典型应用是IP流媒体视频。IP流媒体视频倾向于非常大的下行带宽需求。如果在一个地区有大量集中的CM，且所有业务都通过一个光节点，则为了提供足够的带宽和把多路IP视频流传送到多个CM，可能需要多于1个下行。

多个下行和多个上行的典型应用是当上述应用被组合在一起时，且具有多个信道比对HFC网络进行物理细分更经济。

在这些情况中，CM的作用是能在多个上行之间和多个下行之间移动。CMTS的作用是管理与其相连接的所有CM的流量负载，即根据各CM的资源需求和可用资源，并通过动态地移动CM，在多个上行和下行之间平衡流量。

本附录考虑这些情况的具体实施。特别是对第一种和最后一种应用作出简要介绍。这些示例用图解说明一种拓扑结构和该拓扑结构的一种实现。

G.1 每个电缆段单个下行信道和单个上行信道

本章介绍一个下行信道和4个上行信道的例子。在图G.1中，4个上行信道分别位于独立的4条光纤支线上，这4条光纤支线分别为4个地区的CM提供服务。CMTS接入到一个下行和全部4个上行，而每个CM接入到一个下行和唯一一个上行。

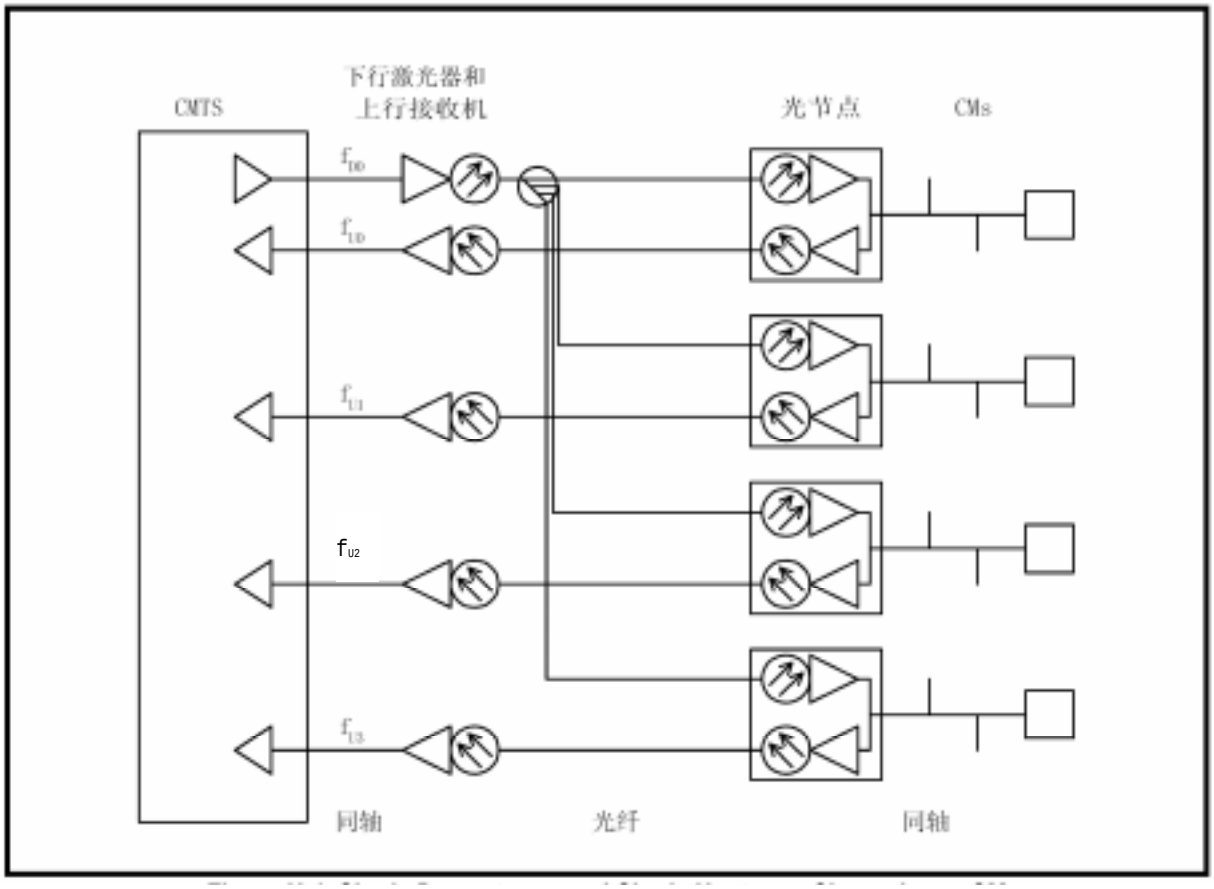


图 G.1　每个 CM 单个下行信道和单个上行信道

在这种拓扑结构中，CMTS向共享该下行信道的4个相关上行信道中的每一个信道发送上行信道描述符(UCD)和MAP。

遗憾的是，每个CM不能决定它连接到哪根光纤支线，因为在共享的下行信道上无法传送地理信息。在初始化时，CM随机地拾取一个UCD信号及其相应的MAP，然后CM在那个信道上选择一个初始维护机会并发送一个测距请求。

CMTS将接收测距请求，并通过在测距响应中指定上行信道ID来将CM再指向到适合的上行信道。然后，CM应使用测距响应的信道ID，而不是在启动测距请求时使用的的信道ID。这只是在CM接收的第一个测距响应时才是必要的。CM应正常地继续其测距过程并继续等待台站维护IE。

然后，CM将使用它所连接的光纤支线上的适当的MAP。如果CM需要重新进行初始维护，则它可能使用其先前已知的UCD来启动，而不必随机地选择一个。

这种拓扑结构带来一些限制：

- 跨越所有光纤节点的所有的初始维护机会都应是校准的。当 CM 选择一个 UCD 来使用，然后顺序地使用那个信道的 MAP 时，CMTS 应在该初始维护机会时准备接收测距请求。注意只有初始化间隔才应校准。一旦 CM 在一个上行信道上成功地测距，它的活动只需要与在同一上行信道上其它用户校准。在图 G.1 中，普通的数据传输和带宽请求可以在 4 个上行信道独立发生；
- 在不同节点上的所有上行信道应工作在相同的一个或多个频率上，除非我们知道其它的上行业务将不会由于 CM 在一个初始维护机会期间在“错误的”频率上传输测距请求而受到影响。如果 CM 任意地选择一个上行信道描述符，且所选的 UCD 应用到不同光节点的上行信道上，则它就会在错误的频率上发送。这种可能使初始维护的时间更长。然而，为了在电缆网段之间保持独立的频谱管理，这可能是一个可接受的系统折中方案；

- 所有上行信道可以工作在不同的符号率之下。然而，在获取测距参数的时间和上行信道符号率的灵活性之间存在一种折衷。如果上行信道符号率不相同，且其测距请求以错误的符号率发送给特定的上行信道接收机时，CMTS 将不能解调测距请求。结果将是 CM 按本部分中的规定进行重试，之后最终会在与当前使用的下行信道相关连的其它上行信道上进行尝试。增加在多信道上尝试测距的可能性，就增加了 CM 的初始化时间，但在不同的光节点上使用不同的符号率，使得在设置突发噪声抑制程度中具有灵活性；
- 在不同信道上所有的初始维护机会可以使用不同的突发特性，因此 CMTS 能解调测距请求。同样，这也是在获得测距的时间和在不同的上行信道中灵活设置物理层参数之间的一种折衷办法。如果初始维护的上行突发参数是不相同的，且对特定的信道用错误的突发参数发送了测距请求，则 CMTS 将不能解调测距请求。结果将是 CM 按本部分中的规定进行测距请求重试，之后最终在与当时使用的下行信道相关的其它上行信道上进行尝试。增加在多信道上尝试测距的可能性，增加了 CM 的初始化时间，但在不同的光节点上使用不同的突发参数进行初始维护，使得在一个规定节点上能设定适合设备情况的参数。

G.2 每个电缆段多个下行信道和多个上行信道

本章介绍一组更复杂的CM的例子，这些CM用于多个下行信道和多个上行信道，而这些上行和下行信道是一个MAC区域的一部分。简要地说明了初始维护、正常的运行及动态信道变更的交互作用，并说明了多个下行信道使用同步或非同步时戳时的影响。

同步时戳指的是两个下行通道发送一个时戳，该时戳来自公共的时钟频率，并具有共同的时基。由于同步，在每个下行信道上的时戳不必在同一时间发送。

G.2.1 拓扑结构

假定2个下行信道与4个上行信道连接起来使用，如图G.2所示。在所有3种拓扑结构中，都有2个装有CM的社区，且都使用相同的2个下行信道。其拓扑结构的差别在于它们的上行信道连接上的不同。

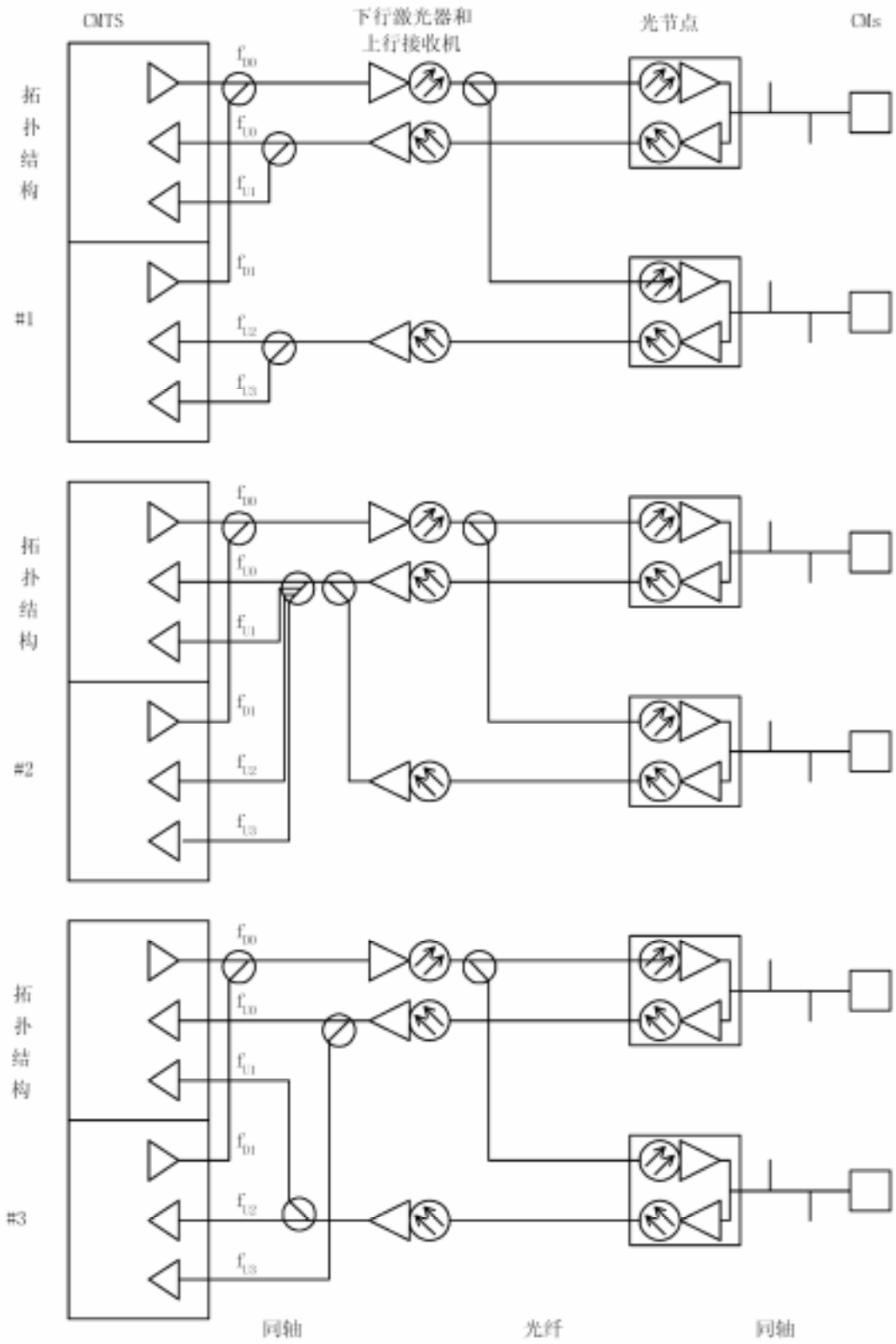


图 G.2　每个 CM 多个下行信道和多个上行信道

拓扑结构1#具有从每个光节点连接到专门设计的上行接收装置的回传通道。一个CM可看到2个下行信道，但只能有与2个下行信道之一相关的一个上行信道。

拓扑结构2#具有从每个光节点合成来的回传信道然后分配到所有上行接收机。一个CM可看到2个下行信道并使用与2个下行信道相关的全部4个上行信道。

拓扑结构3#具有从每个光节点来的回传通道，先分配然后送到多个上行接收机，每个上行接收机分别与不同的下行信道相关。一个CM可看到2个下行信道，及与每个下行道相关的一个上行信道。

拓扑结构1#是在使用中的典型拓扑结构。只有时戳在两个下行信道上同步时，才发生下行信道之间的移动。拓扑结构2#和拓扑结构3#对有非同步时戳的下行信道进行补偿，并且只要上行信道同时变更，就允许在下行信道之间移动。

CM具有单频率接收和单频率发送的能力。

G.2.2 正常运行

表G.1列出了包含信道ID的MAC消息。

表 G.1 带有信道 ID 的 MAC 消息

MAC 消息	下行信道 ID	上行信道 ID
UCD	有	有
MAP	无	有
RNG-REQ	有	无
RNG-RSP	无	有
DCC-REQ	有	有

用非同步时戳：

- 由于上行同步依靠下行时戳，故每个上行信道应与下行信道之一的时戳相联系；
- 下行信道只应发送属于关联上行信道的 MAP 消息和 UCD 消息。

用同步时戳：

- 由于上行同步能从两个下行信道之一得到，故所有的上行信道都能与任何下行信道相关联；
- 所有上行信道的所有 MAP 和 UCD 都应在所有下行信道上发送。UCD 消息包含一个下行信道 ID，所以 CMTS 能通过 RNG-REQ 消息来决定 CM 在哪个下行信道上。这样，在每个下行信道上的 UCD 消息将包含不同的下行信道 ID，即使它们可能包含相同的上行信道 ID。

G.2.3 初始维护

当CM实施初始维护时，拓扑结构是未知的，且下行信道之间时戳的一致性也是未知的。因此，CM选择任一下行信道和所选下行信道上发送的任一UCD。

在两种情况下：

- 在单一的上行物理信道或组合的上行物理信道内，上行信道频率应是不同的；
- 制约要求在 G.1 应用中规定。

G.2.4 动态信道变更

用非同步时戳：

- 当提交一个 DCC-REQ 时，应包含与同一时戳相联系的新的上行和新的下行频率对；
- 当 CM 重新同步到新的下行时，它应允许时戳重新同步而不必重新测距，除非 DCC-REQ 指令要求它进行重新测距；
- 拓扑结构 1#将支持在一个电缆网段内的本地上行信道之间的信道变更，但不支持在下行信道之间的变更。只要新的上行和下行信道对与同一个时戳相关，拓扑结构 2#和 3#将支持在光节点范围内的所有上行和下行信道的变更。

用同步时戳：

下行信道变更和上行信道变更是相互独立的。

拓扑结构1#、2#及3#将支持在电缆网段内的所有上行和下行信道的变更。

附 录 H
（规范性附录）
HFC 数据传输生成树协议

4.1.2.1需要在商用CM和桥接CMTS上应用生成树协议。本附录描述了如何使802.1d生成树协议适用于HFC数据传输系统。

H.1 背景

生成树协议通常应用于桥接的网络中以使网络的冗余连接无效。即：将任意的网络拓扑结构简化为一个有效的从树根延伸到网络所有分支的拓扑结构。不应该将生成树算法和协议与数据转发功能本身混淆；数据转发可以遵循透明学习桥接规则，或可使用其它几种机制中的任一种。通过使冗余连接无效，生成树协议消除了拓扑环，否则，这种拓扑环将导致很多种转发设备将数据包永远转发。

标准的生成树协议(见IEEE 802.1d)被用于大多数桥接的局域网。该协议原用于专用局域网，而用于HFC数据传输时则需要进行某些修改。

H.2 公共生成树

要在一个诸如HFC数据传输的公共接入网中使用生成树协议，需要对基本的IEEE 802.1 d 过程进行若干改进。首先，公共生成树应同任何与之相连的专用生成树网络隔离。这是为了保护公共HFC网络和与之相连的专用网络。图H.1示出其一般拓扑结构。

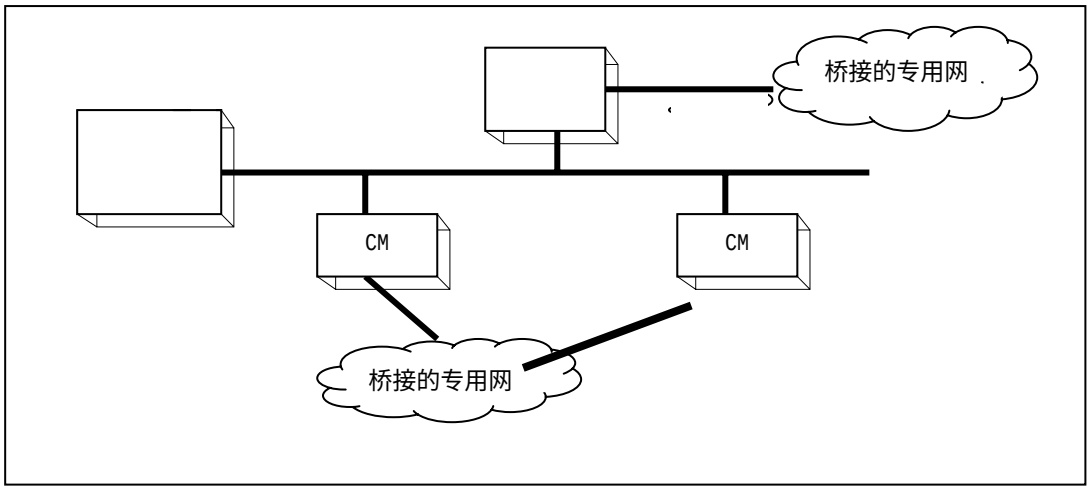


图 H.1 生成树协议

公共生成树协议的任务见图H.1：

- 使专用的桥接网络相互隔离。如果两个专用网络合并成生成树，则每个网络在另一个网络中都可能不稳定。还有，合并的生成树可能超过允许的最大桥接直径；
- 将公共网络与专用网络的生成树隔离开。公共网络的稳定性不应受用户专用网的影响，它也不应该改变用户专用网的生成树特性；
- 禁止两个冗余链路中的一个进入 HFC 网络，以防止形成转发环路。这种情况可能发生在 CM 上，而不是发生在用户网络内的任一桥接上。

该生成树协议也应适用于图H.2所示出的拓扑结构。

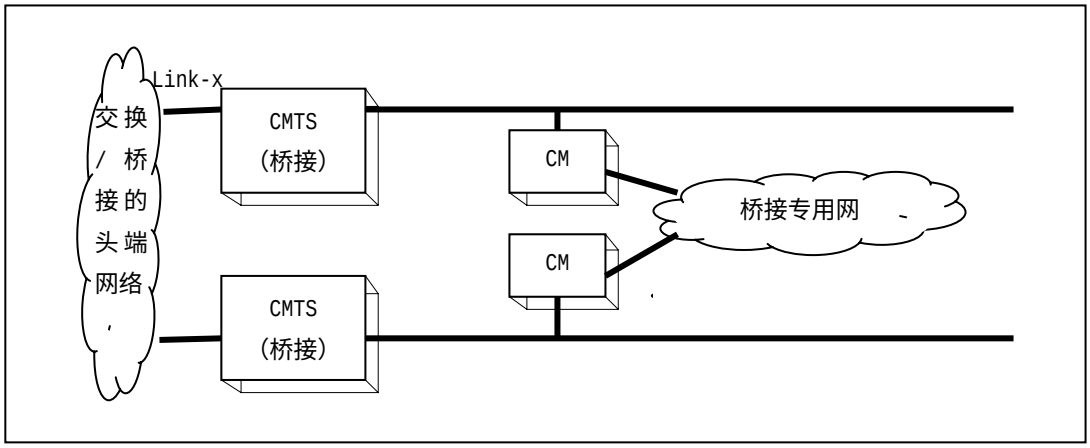


图 H.2 生成树接入 CMTS

在图H.2中，在正常工作时生成树协议应该使两个CM之一的链接无效。它不应通过专用网转移通信信息。注意在某些情况下，例如使链接-X无效时，生成树将在专用网上转移通信信息（虽然对学习到的MAC地址的限制可能扼制大多数中转通信）。如果不希望要这种转移，则应用生成树以外的方法来避免，例如使用路由器。

H.3 公共生成树细节

HFC数据传输生成树算法和协议等同于IEEE 802.1 d中的定义。但下列情况例外：

- 当传送配置桥接协议数据单元（BPDU）时，应采用 HFC 数据传输生成树组播地址 01-E0-2F-00-00-03 而不是采用 IEEE 802.1 d 中定义的地址。这些 BPDU 将被转发而不是按普通 IEEE 802.1 d 桥重新计算；
- 当传送配置 BPDU 时，应使用 SNAP 包头 AA-AA-03-00-E0-2F-73-74 而不是 IEEE802.1 d 所使用的 LLC 42-42-03 包头。在某些桥没有正确识别组播 MAC 地址的事件中，这种做法将使这些 BPDU 与 IEEE 802.1 d 桥所使用那些 BPDU 进一步区别开来；

注：可能配置了几种只靠LSAP来区分IEEE 802.1 d数据包的生成树桥。如果HFC数据传输BPDU也使用LSAP=0x42，则这些装置将不能正确工作。

- IEEE 802.1 d BPDU 应被忽略并丢弃；
- 不应传送（或处理）拓扑结构改变通告（TCN）PDU。TCN 在 IEEE 网络中用于当网络拓扑可能已发生变化时，提高学习数据库的时效。由于 HFC 网络中的学习机理不同，所以该信息不必要且可能导致不必要的泛滥；
- 用作桥接的 CMTS 应参与该协议并赋予比 CM 更高的优先权（很可能是树根）。CMTS 的 NSI 接口应该指定一个连接速度至少为 100Mbps 的端口。这两个条件加在一起，应该确保：
  —— 一个 CMTS 是树根；
  —— 任何其它的 CMTS 将使用头端网络而不是使用用户网络来到达该树根；
- 无论 CMTS 是起路由器的作用还是起桥接器的作用，CMTS 的 MAC 转发器都应将 BPDU 从上行信道转发到下行信道。

注意，允许该协议的CM将把BPDU传送到用户网，以便识别在同一个用户网上其它的CM。这些公共生成树BPDU将透明地通过任何桥接的用户专用网。同样，桥接CMTS将在NSI接口以及RFI接口上发送BPDU。所有的链路中将使用上面定义的组播地址和SNAP包头。

H.4 生成树参数和缺省值

IEEE 802.1 d的4.10.2规定了若干推荐的参数值。除了下述情况，应该使用这些值。

通道成本:

在IEEE 802.1 d中使用了式（H.1）。

通道成本＝1000/已连接的局域网速度（Mb/s）.....（H.1）

对于CM，使用式（H.2）。

通道成本＝1000/（上行符号率×长数据授权的每个符号的bit数）....（H.2）

即，长数据授权IUC的调制类型（QPSK或16QAM）乘以未处理的符号率来决定标称的通道成本。表H.1提供了计算值。

表 H.1　CM 的通道成本

符号率	缺省通道成本	
ksym/s	QPSK	16QAM
160	3125	1563
320	1563	781
640	781	391
1280	391	195
2560	195	98

对CMTS，使用式（H.3）。

通道成本＝1000/（下行符号率×每个符号的bit数）.....（H.3）

桥接优先权：

CM的桥接优先权缺省值应该是36 864 （0x 9000）。这用于网络偏置，以便使树根邻近CMTS处。按照IEEE 802.1 d，CMTS的缺省值应该是32 768。

注意：这两个推荐值只影响缺省的设置。这些参数以及其它在IEEE 802.1 d中定义的参数应该可以通过桥接MIB（参见RFC-1493）或其它方式进行全范围的管理。

附 录 I
（规范性附录）
错误代码和错误信息

这些是CM和CMTS的错误代码和错误信息。这些错误代码仿效ISDN报告错误情况的标准形式而不管生产设备的厂商是谁。

报告的错误代码有同步丢失、UCD失败、MAP失败、测距REQ/RSP失败、UCC失败、登录失败、动态业务请求失败以及DHCP/TFTP失败。在某些情况下，有详细的错误报告，而在其它错误代码中仅仅是“它失败了”。见表I.1。

表 I.1 MAC 管理消息错误代码

错误代码	错 误 信 息
T00.0	SYNC 定时同步
T01.0	获取 QAM/QPSK 符号定时失败。错误状态？重试次数？
T02.0	获取 FEC 帧失败。错误状态？重试次数？错误帧数？
T02.1	获取 FEC 帧，获取 MPEG2 同步失败。重试次数？
T03.0	获取 MAC 帧失败。错误状态？重试次数？错误帧数？
T04.0	在暂停期内接收 MAC SYNC 帧失败。
T05.0	同步丢失（每次同步后，连续丢失 5 次同步）。
U00.0	UCD 上行信道描述符
U01.0	没有收到 UCD，暂停。
U02.0	UCD 无效，或信道不能使用。
U03.0	UCD 有效，但没有收到 SYNC，暂停。
U04.0	UCD 以及 SYNC 有效，但这个信道没有 MAPS。
U05.0	收到的 UCD 带有无效或乱序的配置改变计数。
U06.0	在突发描述符之前没有设置上行信道带宽参数。
M00.0	MAP 上行带宽分配
M01.0	因为 MAP 到达太迟，发送机会丢失。
R00.0	RNG-REQ 测距请求
R01.0	接收到的测距机会无维护广播，T2 暂停。
R04.0	收到对广播维护请求的响应，但没有收到单播维护机会，T4 暂停。
R101.0	没有从被查询的 CM 收到测距请求(CMTS 产生的查询)。
R102.0	16 次 R101.0 错误后，被查询的 CM 重试用完(报告 MAC 地址)。
R103.0	不能成功测距 CM（报告 MAC 地址），重试用完。 注意：这有别于 R102.0，因为它能够测试，即得到 REQ，但不能完成测距。

错误代码	错 误 信 息
R104.0	接收来自 CM（SID X）的周期性的 RNG-REQ 失败，暂停 SID。
R00.0	RNG-RSP 测距响应
R02.0	没有收到测距响应，T3 暂停。
R03.0	测距请求重试用完。
R05.0	开始单播维护测距，没有收到响应，T3 暂停。
R06.0	试图单播维护测距，没有响应，重试用完。
R07.0	单播测距收到异常结束响应。重新启动 MAC。
I00.0	REG-REQ 注册请求
I04.0	不可用的业务，原因：其它。
I04.1	不可用的业务，原因：不能识别的配置设定。
I04.2	不可用的业务，原因：暂时不可用。
I04.3	不可用的业务，原因：永久的。
I05.0	注册被拒绝，鉴权失败：CMTS MIC 无效。
I101.0	无效的 MAC 包头。
I102.0	无效的 SID。没有使用。
I103.0	所需的 TLV 次序混乱。
I104.0	所需的 TLV 不存在。
I105.0	下行频率格式无效。
I105.1	下行频率没有使用。
I105.2	下行频率无效，不是 62500Hz 的倍数。
I106.0	上行信道无效，未分配。
I106.1	注册请求紧随上行信道变更之后。
I107.0	上行信道过载。
I108.0	网络访问配置有无效参数。
I109.0	业务分类配置无效。
I110.0	不支持的业务分类 ID。
I111.0	业务分类 ID 无效或超出范围。
I112.0	最大下行比特率配置是无效格式。
I112.1	最大下行比特率配置设定不支持。
I113.0	最大上行比特率配置是无效格式。
I113.1	最大上行比特率配置设定不支持。
I114.0	上行优先级配置格式无效。
I114.1	上行优先级配置设定超出范围。
I115.0	保证的最小上行信道比特率配置设定格式无效。
I115.1	保证的最小上行信道比特率配置设定超过最大的上行比特率。
I115.2	保证的最小上行信道比特率配置设定超出范围。
I116.0	最大上行信道发送突发配置设定格式无效。
I116.1	最大上行信道发送突发配置设定超出范围。

错误代码	错 误 信 息
I117.0	CM 性能配置设定格式无效。
I117.1	CM 性能配置设定。
I200.0	本部分特定的 REG-REQ 注册请求
I201.0	未指明原因，拒绝注册。
I201.1	不能识别的配置设定，注册被拒绝。
I201.2	暂时没有资源，注册被拒绝。
I201.3	永久的管理设置，注册被拒绝。
I201.4	请求的参数不存在，注册被拒绝。
I201.5	包头抑制设置不支持，注册被拒绝。
I201.6	多个错误，注册被拒绝。
I201.7	在信息中有双重的参考 ID 或索引，注册被拒绝。
I201.8	参数对上下文内容无效，注册被拒绝。
I201.9	授权失败，注册被拒绝。
I201.10	基本业务流错误，注册被拒绝。
I201.11	主要分类器错误，注册被拒绝。
I201.12	主要 PHS 规则错误，注册被拒绝。
I201.13	多个主要错误，注册被拒绝。
I201.14	信息语法错误，注册被拒绝。
I201.15	基本业务流错误，注册被拒绝。
I201.16	信息太大，注册被拒绝。
I00.0	REG-RSP 注册响应
I01.0	注册响应格式无效或不能识别。
I02.0	未收到注册响应。
I03.0	带有错误 SID 的注册响应。
I250.0	本部分特定的 REG-RSP 注册响应
I251.0	注册 RSP 包含 CM 不能支持的业务流参数。
I251.1	注册 RSP 包含 CM 不能支持的分类器参数。
I251.2	注册 RSP 包含 CM 不能支持的 PHS 参数。
I251.3	未指明原因，注册 RSP 被拒绝。
I251.4	信息语法错误，注册 RSP 被拒绝。
I251.5	信息太大，注册 RSP 被拒绝。
I300.0	REG-ACK 注册确认
I301.0	没有 REG-ACK，注册异常结束。
I302.0	未指明原因，注册 ACK 被拒绝。
I303.0	信息语法错误，注册 ACK 被拒绝。

错误代码	错 误 信 息
C00.0	UCC-REQ 上行信道变更请求
C01.0	收到带有无效或超出 US 信道 ID 范围的 UCC-REQ。
C02.0	收到 UCC-REQ，没有 Tx 机会，不能发送 UCC-RSP。
C100.0	UCC-RSP 上行信道变更响应
C101.0	在前一个信道 ID 上没有收到 UCC-RSP。
C102.0	收到带有无效信道 ID 的 UCC-RSP。
C103.0	在新信道收到带有无效信道 ID 的 UCC-RSP。
D00.0	DHCP CM 网络配置下载和日期时间
D01.0	发送发现请求，没收到响应，没有可用的 DHCP 服务器。
D02.0	发送请求后，没有响应。
D03.0	请求的信息不支持。
D03.1	DHCP 响应未包括所有的在本部分附录 D 中描述的有效域。
D04.0	没有设置日期时间或数据无效。
D04.1	日期时间请求被发送，没有收到响应。
D04.2	日期时间响应收到，但数据/格式无效。
D05.0	TFTP 请求已发送，没有响应/没有服务器。
D06.0	TFTP 请求失败，配置文件没有找到。
D07.0	TFTP 失败，数据包次序混乱。
D08.0	TFTP 完成，但完整性检查（MIC）失败。
S00.0	动态业务请求
S01.0	未指明原因，拒绝业务添加。
S01.1	不能识别的配置设定值，拒绝业务添加。
S01.2	暂时没有资源，拒绝业务添加。
S01.3	永久的管理设置，拒绝业务添加。
S01.4	请求的参数不存在，拒绝业务添加。
S01.5	包头抑制设置不支持，拒绝业务添加。
S01.6	业务流已存在，拒绝业务添加。
S01.7	HMAC 鉴权失败，拒绝业务添加。
S01.8	添加被异常结束，拒绝业务添加。
S01.9	多个错误，拒绝业务添加。
S01.10	分类器没有找到，拒绝业务添加。
S01.11	分类器已存在，拒绝业务添加
S01.12	PHS 规则没有找到，拒绝业务添加
S01.13	PHS 规则已存在，拒绝业务添加
S01.14	在信息中有双重的参考 ID 或索引，拒绝业务添加。
S01.15	多个上行流，拒绝业务添加。
S01.16	多个下行流，拒绝业务添加。

错误代码	错 误 信 息
S01.17	有另一个业务流的分类器，拒绝业务添加。
S01.18	有另一个业务流的 PHS 规则，拒绝业务添加。
S01.19	参数对上下文内容无效，拒绝业务添加。
S01.20	授权失败，拒绝业务添加。
S01.21	主要业务流错误，拒绝业务添加。
S01.22	主要分类器错误，拒绝业务添加。
S01.23	主要 PHS 规则错误，拒绝业务添加。
S01.24	多个主要错误，拒绝业务添加。
S01.25	信息语法错误，拒绝业务添加。
S01.26	信息太大，拒绝业务添加。
S01.27	临时 DCC，拒绝业务添加。
S02.0	未指明原因，拒绝业务变更。
S02.1	不能识别配置设定，拒绝业务变更。
S02.2	暂时没有资源，拒绝业务变更。
S02.3	永久的管理设置，拒绝业务变更。
S02.4	请求者不是业务流的所有者，拒绝业务变更。
S02.5	业务流没找到，拒绝业务变更。
S02.6	请求的参数不存在，拒绝业务变更。
S02.7	多个错误，拒绝业务变更。
S02.8	分类器没找到，拒绝业务变更。
S02.9	分类器已存在，拒绝业务变更。
S02.10	PHS 规则没找到，拒绝业务变更。
S02.11	PHS 规则已存在，拒绝业务变更。
S02.12	在信息中有双重的参考 ID 或索引，拒绝业务变更。
S02.13	多个上行流，拒绝业务变更。
S02.14	多个下行流，拒绝业务变更。
S02.15	另一个业务流的分类器，拒绝业务变更。
S02.16	另一个业务流的 PHS 规则，拒绝业务变更。
S02.17	参数对上下文的内容无效，拒绝业务变更。
S02.18	授权失败，拒绝业务变更。
S02.19	主要业务流错误，拒绝业务变更。
S02.20	主要分类器错误，拒绝业务变更。
S02.21	主要 PHS 规则错误，拒绝业务变更。
S02.22	多个主要错误，拒绝业务变更。
S02.23	信息语法错误，拒绝业务变更。
S02.24	信息太大，拒绝业务变更。
S02.25	临时的 DCC，拒绝业务变更。
S02.26	有效负载包头抑制设置不支持，拒绝业务变更。
S02.27	HMAC 鉴权失败，拒绝业务变更。
S03.0	未指明原因，拒绝业务删除。

错误代码	错 误 信 息
S03.1	请求者不是业务流的所有者，拒绝业务删除。
S03.2	业务流没发现，拒绝业务删除。
S03.3	HMAC 鉴权失败，拒绝业务删除。
S03.4	信息语法错误，拒绝业务删除。
S100.0	动态业务响应
S101.0	无效的事务 ID，拒绝业务添加响应。
S101.1	没有响应，业务添加被异常结束。
S101.2	HMAC 鉴权失败，拒绝业务添加响应。
S101.3	信息语法错误，拒绝业务添加响应。
S102.0	无效的事务 ID，拒绝业务变更响应。
S102.1	没有响应，业务变更被异常结束。
S102.2	HMAC 鉴权失败，拒绝业务变更响应。
S102.3	信息语法错误，拒绝业务变更响应。
S103.0	无效的事务 ID，拒绝业务删除响应。
S200.0	动态业务确认
S201.0	无效的事务 ID，拒绝业务添加 ACK。
S201.1	没有 ACK，业务添加异常结束。
S201.2	HMAC 鉴权失败，拒绝业务添加 ACK。
S201.3	信息语法错误，拒绝业务添加 ACK。
S202.0	无效的事务 ID，拒绝业务变更 ACK。
S202.1	没有 ACK，业务变更异常结束。
S202.2	HMAC 鉴权失败，拒绝业务变更 ACK。
S202.3	信息语法错误，拒绝业务变更 ACK。
C200.0	动态信道变更请求（DCC）
C201.0	已经在该信道，拒绝 DCC。
C202.0	DCC 离开老的信道。
C203.0	DCC 到达新的信道。
C204.0	不能获得新的下行信道，DCC 被异常结束。
C205.0	没有新上行信道的 UCD，DCC 被异常结束。
C206.0	不能在新的上行信道上通信，DCC 被异常结束。
C207.0	未指明原因，拒绝 DCC。
C208.0	DCC 不支持，永久拒绝 DCC。
C209.0	未找到业务流，拒绝 DCC。
C210.0	所需的参数不存在，拒绝 DCC。
C211.0	鉴权失败，拒绝 DCC。
C212.0	多个错误，拒绝 DCC。
C213.0	未找到分类器，拒绝 DCC。

错误代码	错 误 信 息
C214.0	未找到 PHS 规则，拒绝 DCC。
C215.0	在信息中有双重的参考 ID 或索引，拒绝 DCC。
C216.0	参数对上下文内容无效，拒绝 DCC。
C217.0	信息语法错误，拒绝 DCC。
C218.0	信息太大，拒绝 DCC。
C300.0	动态信道变更响应（DCC-RSP）
C301.0	在老的信道上没有收到 DCC-RSP。
C302.0	在新的信道上没有收到 DCC-RSP。
C303.0	未指明原因，拒绝 DCC-RSP。
C304.0	未知事务 ID，拒绝 DCC-RSP。
C305.0	鉴权失败，拒绝 DCC-RSP。
C306.0	信息语法错误，拒绝 DCC-RSP。
C400.0	动态信道变更确认
C401.0	DCC-ACK 没收到。
C402.0	未指明原因，拒绝 DCC-ACK。
C403.0	未知事务 ID，拒绝 DCC-ACK。
C404.0	鉴权失败，拒绝 DCC-ACK。
C405.0	信息语法错误，拒绝 DCC-ACK。
B00.0	加密
B01.0	待定。

附 录 J
（资料性附录）
DOCSIS 传输和争用解决

本附录试图阐明DOCSIS传输和争用解决算法如何工作。它做了较少的简化和假设，但有助于清楚地阐明本部分的这方面内容。

本例作了如下简化：

- 当延迟或等待挂起的授权时，它并不能明确地讨论信息包的到达且不清楚附带请求的大小；
- 大部分可级联使用，但并不试图讨论其所有细节。

本例也做了如下假设：

- 它假设请求总是适用于任意请求/数据包中；
- 当一个附带请求与一个争用数据包一起发送时，状态机制仅检查对请求的授权，并假设对竞争数据包的确认由 CMTS 完成；
- 它也许假设一些其它的事情，以满足对基本要点的理解。

传输状态图见图J.1。

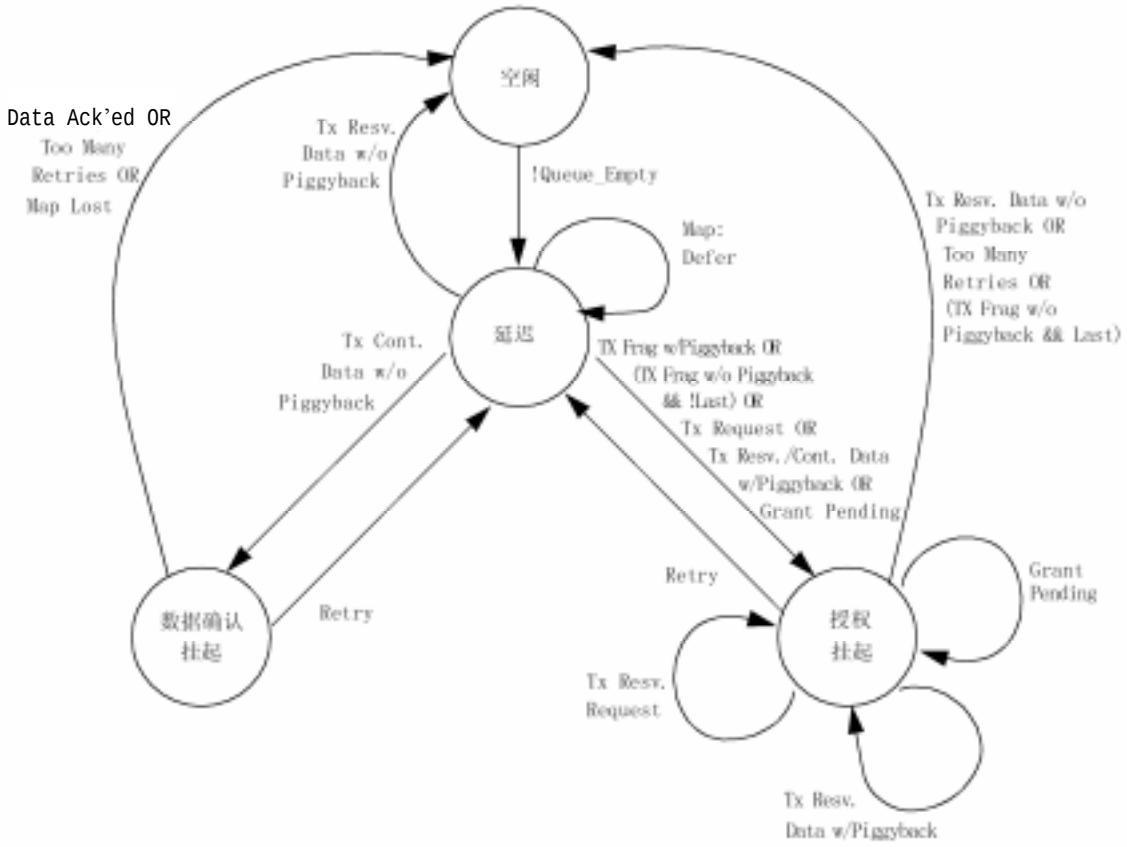


图 J.1 传输状态转变图

其中变量定义如下：

- Start= 当前正起作用的 MAP 数据退避起始域；

- End = 当前正起作用的 MAP 数据退避结束域；
- Window = 当前退避窗口；
- Random[n] = 随机数发生器，它在 0 到 n-1 之间选择一个数；
- Defer= 在发送前延迟的发送机会数；
- Retries= 挂起时试图发送数；
- Tx_time= 当请求或请求/数据被发送时节省的时间；
- Ack_time= 从当前 Map 来的 ACK 时间域；
- Piggyback= 当一个附带请求添加到发送包时的标志设置；
- Queue_Empty= 当一个 SID 的数据队列被清空时的标志设置；
- Lost_Map= 当一个 Map 丢失和处于状态数据 ACK 挂起时的标志设置；
- My_SID= 有一个包要发送的队列的业务 ID；
- pkt size= 包括 MAC 和物理层开销的数据包大小（如果使用则包括附带域）；
- frag_size= 分段的大小；
- Tx_Mode= {FULL_Pkt; First_Frag; Middle_Frag; Last_Frag}；
- min_frag= 最小分段的大小。

状态：空闲（Idle）——等待包发送

```
Window = 0；
Retries = 0；
Wait for ! Queue_Empty;          / * 发送有效数据包 * /
CalcDeferO；
Go to Deferring
```

状态：数据确认挂起——仅等待数据应答

```
Wait for next Map;
if (Data Acknowledge SID==my_SID) / * 成功! CMTS 收到数据包 * /
go to state Idle;
else if (Ack_time  Tx_time)      / * 发生冲突 !!! 或包丢失或Map丢失 * /
{
if (Lost_Map)
go to state Idle;       / * 假定包得到确认，以避免重复发送 */
else
Retry( );
}
stay in state Data Ack Pending;
```

状态：授权挂起——等待授权

```
Wait for next Map;
While (Grant SID==my_SID)
   UtilizeGrant( );
if (Ack_time  Tx_time)  / * 发生冲突 !!!! 或请求被拒绝/丢失或Map丢失 */
Retry ( );
stay in state Grant Pending
```

状态：延迟——决定适当的发送定时并发送

```
if (Grant SID==my_SID)      / * 主动请求 */
    {
    Utilize Grant ( );
```

```
        }
    else if (unicast Request SID==my_SID)  / * 主动单播请求 */
        {
        transmit Request in reservation;
        Tx_time=time;
        Go to state Grant Pending;
        }
    else
        {
        for (each Request or Request /Data Transmit Opportunity)
            {
            if (Defer ! =0)
            Defer = Defer – 1;       / *  保持延迟状态，直到Defer=0 * /
            Else
                {
                if (Request / Data tx_op) and (Request /Data size  =pkt size)
                                          / * 发送争用数据 * /
                    {
                    transmit data pkt in contention;
                    Tx_time = time;
                    if (Pinggydack)
                        go to state Grant Pending;
                    else
                        go to state Data Ack Pending;
                      }
                 else        / * 发送争用请求 * /
                    transmit Request in contention;
                  Tx_time = time;
                  Go to state Grant Pending;
               }
           }
        }
    }
    Wait for next Map;
    stay in state Deferring
```

函数：CalcDefer( )——决定延迟量

```
    if (Window  Start)
           Window=Start;
    if (Window    End)
           Window =End;
    Defer = Random[2 Window];
```

函数：UtilizeGrant ( )——决定授权的最佳使用

```
    if (Grant size  = pkt size)     / * CM 可以发送完整的包数据 * /
        {
```

```
    transmit packet in reservation;
    Tx_time=tine;
Tx_mode=Full_pkt
if (Piggyback)
    go to state Grant Pending
Else
   Go to state Idle;
}
else if (Grant size   min_frag && Grant Size  Request size)
/ *  不能发送分段数据，但可发送请求 * /
        {
        transmit Request in reservation;
        Tx_time = time;
        go to state Grant Pending;
         }
else if (Grant size==0 )          / *  请求挂起 */
        go to state Grant Pending;
else
{
while (pkt_size  0 && Grant Sid ==my_SID)
{
if (Tx_mode==Full_Pkt)
  Tx_mode=First_frag;
Else
Tx_mode=Middle_frag;
pkt_size=pkt_size-frag_size;
if (pkt_size==0)
    Tx_mode=Last_frag;
if (another Grant SID==my_SID)    / *  多授权模式 * /
piggyback_size=0
else
piggyback_size=pkt_size       /  *  附带模式 * /
if(piggyback_size>0)
transmit fragment with piggyback request for remainder of packet in reseruation
else
transmit fragment in reservation;
}
go to state Grant Pending;
```

函数：Retry( )

```
Retries=Retries+1;
if (Retries>16)
{
discard pkt, indicate exception condition
go to state Ible;
```

```
    }
    Window=Window+1;
    CalcDefer( );
    go to state Deferring.
```

附 录 K
（资料性附录）
IGMP 举例

4.3.1定义了CMTS和CM支持IGMP信令的要求。本附录进一步提供了CM支持IGMP的细节。
CM可能支持以下定义的过程。见图K.1。
本附录提供了用来维护单个组播组成员的CM被动模式状态机的例子。

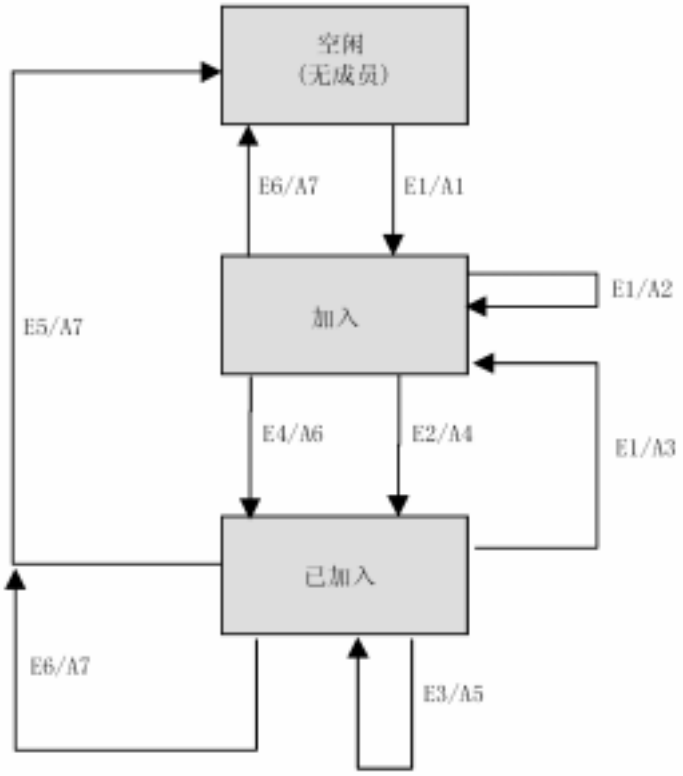


图 k.1 IGMP 支持-CM 被动模式

a) 事件：
   1) E1：在 CPE I/f 上收到 MR；
   2) E2：M1 定时器超时；
   3) E3：在 RF I/f 上收到 MQ；
   4) E4：在 RF I/f 上收到 MR；
   5) E5：M2 定时器超时；
   6) E6：授权失败；
b) 动作：
   1) A1：MQI=125s；I=10s； 以 0s 到 3s 之间的任意值启动 M1 定时器；启动 M2 定时器=2×MQI+QRI；如果必要，启动 TEK 机；添加组播地址到组播过滤器；
   2) A2：丢失 MR 数据包；
   3) A3：复位 M2 定时器=2×MQI+QRI；以 0s 到 3s 之间的任意值启动 M1 定时器；
   4) A4：在 RF I/f 上传送 MR；设置 I=当前时间；
   5) A5：重新计算 MQI=MAX（125，当前时间- I）；设置 I=当前时间，在 CPE I/f 上转发 MQ；

6) A6：取消 M1 定时器；

7) A7：从组播过滤器删除组播地址。

附 录 L
（资料性附录）
主动授权业务

本附录讨论主动授权业务（UGS）和带活动检测的主动授权业务（UGS-AD）的用途并包含具体示例。

L.1 主动授权业务（UGS）

L.1.1 介绍

主动授权业务是一个上行数据流调度业务类型，它用于将恒定比特率（CBR）的流量映射成业务流。由于上行是预定带宽，一个CBR业务能通过CMTS调度一个稳定的授权流来建立。因为带宽是预先决定的，并且勿需请求，所以这些授权被认为是非请求的。

CBR应用的典型例子是在IP协议数据包上传输语音（VoIP）。其它应用也可能存在。

上行数据流调度业务与业务流有关，每一种业务流与一单个业务ID（SID）有关。每一个业务流可能有多个分类器。每一个分类器可能与唯一的CBR媒体流有关。分类器可以从一个业务流上添加或删除。因而UGS的语义应适用于每个SID的单个或多个CBR的媒体流。

本附录中，一个子流被定义为一个分类器的输出。由于一个VoIP会话由一个分类器来标识，所以在本附录中的子流就是指一个VoIP会话。

L.1.2 配置参数

配置参数如下：

- 标称授权间隔；
- 主动授权大小；
- 可容忍的授权抖动；
- 每间隔的授权。

这些参数的解释和它们的缺省值在附录C中提供。

L.1.3 操作

当为UGS预置一个业务流时，选择标称授权间隔等于CBR应用的包间隔。例如，10ms包大小的VoIP应用需要一个10ms的标称授权间隔。授权大小的选择应满足CBR应用的带宽需求，它直接与包的长度有关。

当多个子业务流被指配给一个UGS业务时，每间隔发出多个授权，子流与授权间没有映射关系。每间隔的多个授权形成一个授权池，每个子流都能使用任一授权。

在操作示例中假定UGS缺省状态没有级连和分段。

L.1.4 抖动

图L.1所示为授权间隔和容忍的授权抖动之间的关系，并给出一个子流抖动的示例。

对每间隔只有一个授权来说，可容忍的授权抖动是实际授权时间（ti’）和标称授权时间（ti）之间的最大差值。对每间隔有多个授权来说，可容忍的授权抖动是这一组授权中最后一个授权的实际时间和标称授权时间（ti）的最大差值。如果任一授权到达是在ti’，则ti≤ti’≤ti+抖动。

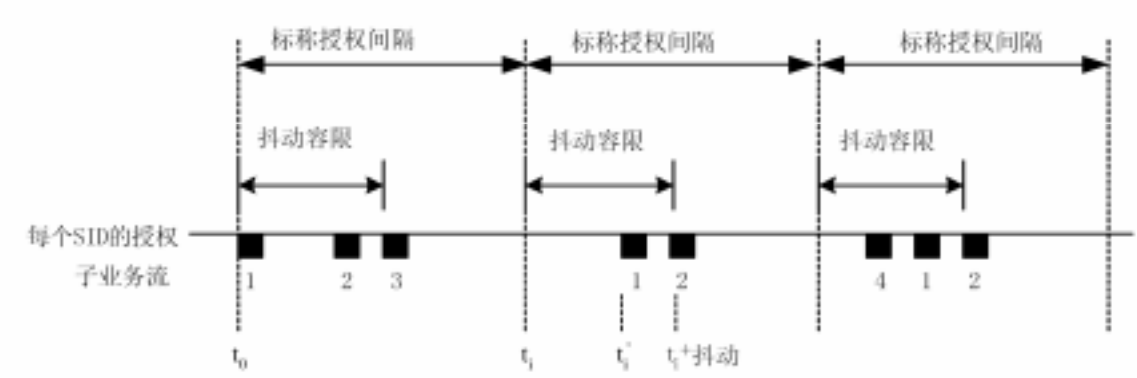


图 L.1 每个 SID 带多个授权的抖动举例

图L.1说明了即使各个授权不从它们相关的位置移动，一个子流将如何抖动。在第一个间隔期间，建立了3个VoIP会话，它们发生在3个授权上。在第二个间隔中，VoIP会话3已经撤去。由于CMTS不知道哪个子流与哪个授权有关，它决定除去第一个授权。剩余两个呼叫转向其它两个授权。在第三个间隔中，增加一个新的VoIP会话4和一个新的授权，新的呼叫发生在新的授权上。最后效果是子流可以在它的抖动间隔内来回移动。

小的抖动间隔的好处是VoIP接收抖动缓冲器可以保持很小。缺点是对CMTS增加了调度限制。

标称授权间隔的边界是任意的，且在CMTS和CM之间不通信。

注： 许多戏剧性的事件如丢失一个下行MAP或上行的频率跳变可能导致子流抖动超出该抖动窗口。

L.1.5 同步问题

当在网上传送诸如VoIP会话的CBR流量时，存在两个同步问题。第一个是源时钟和目的时钟的频率不匹配。这由VoIP应用程序管理，它超出了本部分的范围。第二个是在CBR源/接收和承载信道之间的频率不匹配。

特别是，如果产生上行VoIP包的时钟与提供UGS业务的CMTS时钟不同步，则这些VoIP包可能开始在CM处累积。如果MAP丢失，也可能导致时钟失步，从而出现包的累积。

当CM检测到这个状态时，它在业务流EH单元中发出队列指示。CMTS通过发出一个临时的额外授权作出响应，但额外授权不超过其预置带宽的1% （即每100个授权对应最多一个额外授权）。CMTS继续提供这种额外的带宽直到CM不再发出该比特位。

类似的问题发生在下行。远端发送源的频率可能与驱动CMTS的时钟不同步。这样CMTS应该以一个略高于精确预置速率的速率校正,来允许这种失配和防止延迟积累或在CMTS处的包丢失。

L.2 具有活动检测的主动授权业务（UGS-AD）

L.2.1 介绍

具有活动检测的主动授权业务（UGS-AD）是一个上行数据流调度业务类型。本条描述UGS-AD的一个应用，它支持语音活动检测（VAD）。VAD也被称为无声抑制，这是一种语音技术。在这种技术中只有当有足够大的语音能量时，发送CODEC才发送语音信号。接收CODEC通过嵌入无声或者会话背景噪声的等效舒适噪声来补偿无声间隔。

VAD的优点是减少会话的网络带宽要求。估计60%的语音会话是无声的。去掉那些无声的部分，就能使网络处理更多的业务量。

本条中的子流被描述为活动的或非活动的，而MAC层中的QoS参数状态称作“ 激活 ”。

L.2.2 MAC层配置参数

配置参数包括所有正常的UGS参数，再加上以下各项：

- 标称的查询间隔；
- 可容忍的查询抖动。

这些参数的解释和它们的缺省值见附录C。

L.2.3 操作

当没有活动子流时，CMTS向CM发送查询请求；当有活动子流时，CMTS向CM发送主动授权。CM在每个主动授权的每个包中的UGSH的活动授权域中指出当前每间隔需要的授权数目。CM可以请求直到每间隔最大的活动授权数目。CM持续发送此状态信息，且不需要CMTS的确认。

决定活动状态的具体方法依CM而定。可选的实现方法包括：

- 由 MAC 层业务为每个分类器提供一个活动定时器。如果在一定时间内包停止到达，MAC 层业务将把该子流标志为非活动的。而当一个新包到达时，则标志这个子流为活动的。请求的授权数目等于活动子流的数目；
- 由一个更高层的业务实体诸如一个嵌入媒体客户来向 MAC 层业务指示活动性。

当CM正在接收查询请求并检测到活动时，CM按每间隔一个授权来请求足够的带宽。如果活动子流多于一个，CM将从其发送的第一个包开始，在UGS的活动授权域指出这种情况。

当CM正在接收主动授权，接着又检测到新的活动并请求一个以上的授权时，则在它收到新的授权之前将有一个延时。在这个延时过程中，数据包可能在CM内积累起来。当新的主动授权被添加时，CMTS将突发额外的授权，以清除积累的数据包。

当CM正在接收主动授权，而检测到子流不活动并请求减少一个授权时，则在授权减少之前，将有一个延时。如果在上行发送队列中已有任何包的积累，则额外的授权将减少或清空此队列，这有助于保持较低的系统延迟。子流与授权的关系也随之改变，这种情况可认为是低频抖动并应由远端管理。

当CM正在接收主动授权，并在它的任一子流上没有检测到活动时，它将发送一个包，其UGSH的活动授权域设为0，然后停止发送。CMTS将从UGS模式切换到实时查询模式。当CM再次检测到活动时，它在其中一个查询中发出一个请求，以便恢复主动授权的传递。CMTS忽略请求的大小，并恢复分配给该CM的主动授权。

由于CM已按上述内容操作，CMTS就不必分别监控包的活动。最坏的情况是，如果CMTS丢失了指示零授权的最后包，则CMTS和CM将同步退回到下一次会话的开始。因此，当CM从非活动转到活动时，它应重新开始发送查询请求或主动授权。

L.2.4 举例

图L.2所示为单个G.711（64 kbps）话音呼叫在话音重现之前的处理示例，其包大小是10ms,接收抖动缓冲器需要容纳最小20ms的话音长度（即2个包长）。

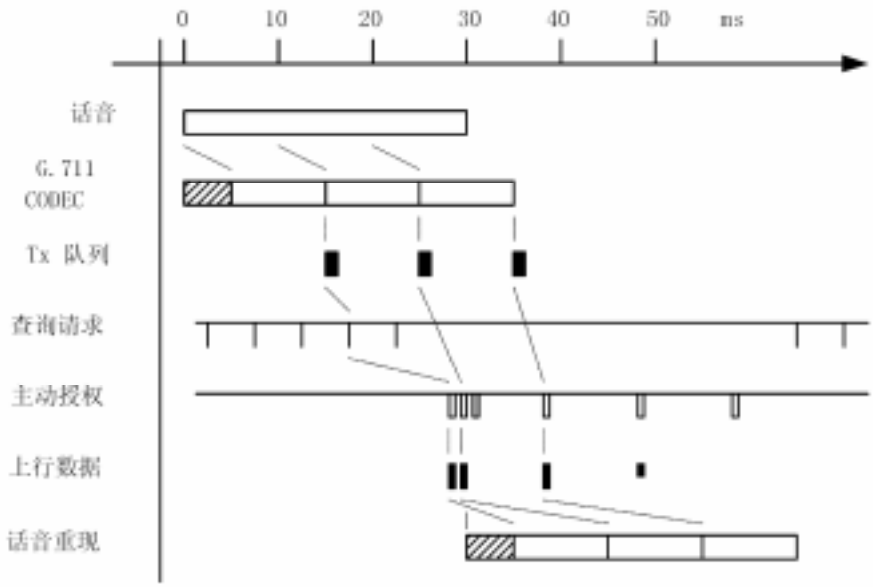


图 L.2　VAD 启动和停止

假定话音在零时间开始。在标称的处理延时和10ms的打包延时后，DSP CODEC 产生话音数据包，数据包接着被传送到上行发送队列中。使用下一个查询请求，该查询请求导致经过一段时间之后主动授权开始。额外的主动授权立即发出，以清除上行队列。

这些包通过网络传输到达接收抖动缓冲器。当第二个包到达时，20ms的最小抖动缓冲器已满足要求。因为这些包紧挨着到达，只增加了几毫秒的延迟。在标称的处理延时后，开始重现话音。

当语音突发结束时，CM发送一个保持包，这个包没有有效负载，其UGSH活动授权域置为零授权。一段时间之后，UGS停止，实时查询开始。

L.2.5　会话的突发授权

当一个业务流变成活动时，主动授权的额外突发是必要的，因为话音在开始重现之前，在接收CODEC处的抖动缓冲器通常要等待最小量的语音抽样。这些初始包到达之间的任何延时都将加到电话呼叫的最后延迟上去。这样，CMTS识别到CM有包要发送并能够越快清空CM缓冲队列，则这些包就会越快到达接收端，且在电话呼叫中发生的延迟也就越低。

这里无法确定需要多少个突发授权。当CM请求一个额外的授权时，一个话音包就已经积累起来了。CM不知道要请求多少个额外授权，因为它不知道从CMTS接收所需的往返响应时间，因而也不知道可能积累起多少个包。CMTS对此情况的了解要好一些，尽管它不知道远端抖动缓冲器的需求情况。

解决办法是由CMTS来选择突发的大小，并在会话突发开始处紧接着发送这些突发授权。这种情况发生在从实时查询转移到UGS时和增加每间隔的UGS授权的数目时。

表L.1所示为请求到授权响应时间所引入的典型的启动延迟。

表 L.1　请求到授权响应时间的举例

序号	变　　量	举例值 ms
1	从话音包建立到话音包到达 CM 上行队列的时间。	0～1
2	直到收到一个查询请求的时间。最坏情况下的时间是查询请求间隔。	0～5
3	CMTS 的请求授权响应时间。该值受 MAP 长度和待处理的 MAP 数目影响。	5～15
4	HFC 设备的往返延时包括下行交织延时。	1～5
总　　计		6-26

这个数字随CMTS的实现方法而变化，但从上面的例子可以看出，所期望的合理的额外授权数目见表L.2。

表 L.2 新会话突发的额外授权举例

UGS 间隔	对新会话突发的额外授权数目
10ms	2
20ms	1
30ms	0

再一次提醒注意的是：CMTS和CM不能也不会将各个子流和各个授权映射起来。这意味着在当前的子流是活动的和一个新的子流也变得活动时，新的子流将立即使用已存在的授权池。这就潜在地减少了新的会话突发的启动延迟，但增加了其它子流的延迟。当突发授权到达时，它被所有子流共享，并恢复或甚至减少其原来的延迟。这里包含抖动成分。活动的子流越多，添加一个新子流的影响就越小。

L.2.6 接纳考虑

注意，在配置CMTS的接纳控制时，应考虑下述因素。

VAD允许上行信道被过度预置。例如，一个正常情况下可处理24个VoIP会话的上行信道可以被过度预置为高达36个（50%）或甚至48个（100%）。每当有过度预置时，就存在所有的上行VoIP会话都处于活动状态的概率。此时，CMTS有可能不能调度所有的VoIP流量，另外，会话的突发授权将会延长。VAD的CM实现方法应能识别这种可能性，并限制队列中所积累的包的数量。

通过把最大允许的VoIP会话数目预置为少于整个上行信道所支持的最大话音容量(在上例中为24)，在VAD期间的上行信道的偶尔饱和是能够被消除的。这样，VAD使话音业务在整个信道容量中的比例由100%降到约40%，剩余的60%则用于数据和维护业务。

参考文献

[1] DIX Ethernet Protocol Version 2.0, Digital, Intel, Xerox, 1982.

[2] DOCSIS3 Data-Over-Cable Service Interface Specifications, Cable Modem Termination System -Network Side Interface Specification, SP-CMTS-NSI-I01-960702.

[3] DOCSIS4 Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, SP-CMCI-I04-000714.

[4] DOCSIS5 Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, SP-OSSIv1.1-I04-010829.

[5] DOCSIS6 Data-Over-Cable Service Interface Specifications, Cable Modem Telephony Return Interface Specification, SP-CMTRI-I01-970804.

[6] EIA-S542 EIA Standard 542 (1997), “Cable Television Channel Identification Plan”, May 1997.

[7] EN 50081-1 CENELEC EN 50081-1 Electromagnetic compatibility generic emission standard Part 1: Residential, commercial and light industry.

[8] EN 50082-1 CENELEC EN 50082-1 Electromagnetic compatibility generic immunity standard Part 1: Residential, commercial and light industry.

[9] EN 60950 CENELEC EN 60950: “Safety of information technology equipment”.

[10] EG 201 212 ETSI EG 201 212: “Electrical safety; Classification of interfaces for equipment to be connected to telecommunication networks”. This document is also available from CENELEC as ROBT-002.[1]

[11] FCC15 Code of Federal Regulations, Title 47, Part 15, October 1998.

[12] FCC76 Code of Federal Regulations, Title 47, Part 76, October 1998.

[13] ID-DHCP Patrick, M., DHCP Relay Agent Information Option, IETF DHC Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-dhc-agent-options-10.txt, (work in progress).

[14] ID-IGMP Fenner W., IGMP-based Multicast Forwarding (“IGMP Proxying”), IETF Internet Draft,http://www.ietf.org/internet-drafts/draft-fenner-igmp-proxy-03.txt.[2]

[15] IEEE802 IEEE Std 802-1990, Local and Metropolitan Area Networks: Overview and Architecture

[16] IEEE802.1Q IEEE Draft Standard 802.1Q/D4. Draft Standard for Virtual Bridged Local Area Networks. December 20, 1996.

[17] IMA Internet Assigned Numbers Authority, Internet Multicast Addresses, http://www.isi.edu/in-notes/iana/assignments/multicast-addresses

[18] ISO/IEC15802-1 ISO/IEC 10039:1991 Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Common specifications — Part 1: Medium Access Control (MAC) service definition.

[19] ISO-169-24 ISO-169-24 F connector, female, indoor[3]

[20] NCTA NCTA Recommended Practices for measurement on Cable Television Systems — National Cable Television Association, Washington DC, 2nd Edition, revised October, 1993.

[21] PKTCBL-MGCP PacketCable Specifications, Network-Based Call Signaling Protocol Specification, PKTSP-EC-MGCP-I02-991201.

[22] PKT-DQOS PacketCable Specifications, Dynamic Quality of Service Specification, PKT-SP-DQOSI01-991201.

[23] RFC-791 Postel, J., Internet Protocol, IETF RFC-791 (MIL STD 1777), September, 1981.

[24] RFC-826 Plummer, D., Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48-bit Ethernet address for transmission on Ethernet hardware, November,1982.

[25] RFC-868 Harrenstien, K., and Postel, J., Time Protocol, IETF RFC-868, May 1983.

[26] RFC-1042 Postel, J., and Reynolds, J., A Standard for the Transmission of IP Datagrams over IEEE 802 Networks, IETF RFC-1042, February, 1988.

[27] RFC-1058 Hedrick, C., Routing Information Protocol, IETF RFC-1058, June, 1988.

[28] RFC-1123 Braden, R., Requirements for Internet Hosts – Application and Support, IETF RFC-1123, October 1989.

[29] RFC-1157 Schoffstall, M., Fedor, M., Davin, J. and Case, J., A Simple Network Management Protocol (SNMP), IETF RFC-1157, May, 1990.

[30] RFC-1350 Sollings, K., The TFTP Protocol (Revision 2), IETF RFC-1350, July, 1992.

[31] RFC-1493 Definitions of Managed Objects for Bridges. E. Decker, P. Langille, A. Rijsinghani, & K.McCloghrie. July 1993. (Obsoletes RFC1286)

[32] RFC-1633 Braden, R., Clark, D., and Shenker, S., Integrated Services in the Internet Architecture: An Overview, IETF RFC-1633, June, 1994.

[33] RFC-1812 Baker, F., Requirements for IP Version 4 Routers, IETF RFC-1812. June, 1995.

[34] RFC-2104 Krawczyk, H., Bellare, M., and Canetti, R., HMAC: Keyed-Hashing for Message Authentication, IETF RFC-2104, February, 1997.

[35] RFC-2131 Droms, R., Dynamic Host Configuration Protocol, IETF RFC-2131, March, 1997.

[36] RFC-2132 Alexander, S., and Droms, R., DHCP Options and BOOTP Vendor Extensions, IETF RFC-2132, March, 1997.

[37] RFC-2210 Wroclawski, J., The Use of RSVP with the IETF Integrated Services, IETF RFC-2210, September, 1997.

[38] RFC-2211 Wroclawski, J., Specification of the Controlled-Load Network Element Service, IETF RFC-2211, September, 1997.

[39] RFC-2212 Shenker, S., Partridge, C., and Guerin, R., Specification of Guaranteed Quality of Service, IETF RFC-2212, September, 1997.

[40] RFC-2236 Fenner, W., Internet Group Management Protocol, Version 2, IETF RFC-2236, November 1997.

[41] RFC-2349 Malkin, G. and Harkin, A., TFTP Timeout Interval and Transfer Size Options, IETF RFC-2349, May 1998.

[42] RFC-2669 St. Johns, M., DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems, IETF RFC-2669, August 1999.

[43] RFC-2786 St. Johns, M., Diffie-Helman USM Key Management Information Base and Textual Convention, IETF RFC-2786, March, 2000.