

Project	IEEE 802.16 Broadband Wireless Access Working Group	
Title	Media Access Control Layer Proposal for the 802.16 Air Interface Specification	
Date Submitted	2000-07-07	
Source	<p>Glen Sater Motorola Inc. 8220 E. Roosevelt Street, M/D R1106 Scottsdale, AZ 85257</p> <p>Voice: 480-441-8893 Fax: 480-675-2116 E-mail: g.sater@motorola.com</p> <p>Ken Stanwood Ensemble Communications Inc. 9890 Town Centre Dr. San Diego, CA 92121</p> <p>Voice: 858-404-6544 Fax: 858-458-1401 E-mail: ken@ensemblecom.com</p> <p><u>Additional Contributions</u> Arun Arunachalam, George Stamatelos Jeff Foerster Scott Marin, Bill Myers Leland Langston, Wayne Hunter Phil Guillemette Chet Shirali, Menashe Shahar Karl Stambaugh George Fishel Ray Sanders Moshe Ran Andrew Sundelin Yonatan Manor Brian Petry, Mark Vogel Dr. James Mollenauer Carl Eklund, Juha Pihlaja, Kari Rintanen Doug Grey Paolo Baldo Paul Kennard Andrea Nascimbene Naftali Chayat, Leonid Shousterman, Vladimir Yanover Dr. Demosthenes Kostas Jay Klein</p> <p><u>Company</u> Nortel Networks Alcatel SpectraPoint Wireless, LLC. Crossspan, a Raytheon Telecommunications Company SpaceBridge Networks Corporation Vyyo Inc. Motorola, Inc. Communications Consulting Services CircuitPath Networks Systems TelesciCOM, Ltd. iSKY Oren Semiconductors 3Com Technical Strategy Associates Nokia Lucent Technologies Siemens Digital Microwave Ericsson BreezeCOM</p> <p>Adaptive Broadband Ensemble Communications</p>	
Re:	802.16.1 INVITATION TO CONTRIBUTE: Session #8, Document IEEE 802.16-00/13r1	
Abstract	<p>This is a joint proposal that merges two contributions presented to the Working Group during Session #7 (documents IEEE 802.16.1mc-00/14 and IEEE 802.16.1mc-00/15). The process of combining the two documents was guided by the outline of agreements developed in Session #7.5, which amended the Call for Contributions for Session #8.</p> <p>The proposed MAC provides connection-oriented links between the Base Station and CPEs. Each connection is associated with peer convergence sub-processes and service flows. Higher-layer information is tunneled through the MAC using the QoS provided by the service flows. In this manner, the MAC can be extended to support a wide variety of bearer transport and signaling mechanisms without modification to the core MAC services. The MAC fully supports the merged PHY layer as defined in 802.16.1pc-00/29r1.</p>	
Purpose	<p>To provide a detailed description of a proposed MAC layer specification for IEEE 802.16 WG.</p> <p><b>Note: This is a preliminary submittal that will be updated during the IEEE 802.16.1 Working Group Session #8.</b></p>	
Notice	<p>This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.</p>	

Release	<p>The contributor grants a free, irrevocable license to the IEEE to incorporate text contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.</p> <p>Portions of this document are reprinted with permission from Cable Television Laboratories, Inc.</p>
IEEE Patent Policy	<p>The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 0.9) &lt;<a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a>&gt;, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."</p> <p>Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair &lt;<a href="mailto:r.b.marks@ieee.org">mailto:r.b.marks@ieee.org</a>&gt; as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site &lt;<a href="http://ieee802.org/16/ipr/patents/letters.html">http://ieee802.org/16/ipr/patents/letters.html</a>&gt;.</p>

PRELIMINARY SUBMITTAL

1.	Overview .....	7
1.1	Scope .....	7
1.2	Purpose .....	7
2.	Normative References .....	9
3.	Definitions .....	11
4.	Acronyms and abbreviations .....	13
5.	MAC Service Definition .....	17
6.	Media Access Control .....	19
6.1	Connections and Service Flows .....	19
6.1.1	Addressing and Connection Identifiers .....	20
6.2	DOWNLINKMessage Formats .....	23
6.2.1	Convergence Sub-layer PDU Formats .....	27
6.2.2	MAC Management Messages .....	27
6.2.3	Downlink MAP (DS-MAP) Message .....	34
6.2.4	Uplink MAP Message .....	37
6.2.5	Ranging Request (RNG-REQ) Message .....	40
6.2.6	Ranging Response (RNG-RSP) Message .....	41
6.2.7	Registration Request (REG-REQ) Message .....	46
6.2.8	Registration Response (REG-RSP) Message .....	47
6.2.9	Registration Acknowledge (REG-ACK) Message .....	49
6.2.10	Privacy Key Management — Request (PKM-REQ) Message .....	51
6.2.11	Privacy Key Management — Response (PKM-RSP) Message .....	52
6.2.12	Dynamic Service Addition — Request (DSA-REQ) Message .....	53
6.2.13	Dynamic Service Addition — Response (DSA-RSP) Message .....	54
6.2.14	Dynamic Service Addition — Acknowledge (DSA-ACK) Message .....	56
6.2.15	Dynamic Service Change — Request (DSC-REQ) Message .....	57
6.2.16	Dynamic Service Change — Response (DSC-RSP) Message .....	58
6.2.17	Dynamic Service Change — Acknowledge (DSC-ACK) Message .....	59
6.2.18	Dynamic Service Deletion — Request (DSD-REQ) Message .....	61
6.2.19	Multicast Polling Assignment Request (MCA-REQ) Message .....	62
6.2.20	Multicast Polling Assignment Response (MCA-RSP) Message .....	62
6.2.21	Downlink Modulation Change Request (DMC-REQ) Message .....	63
6.3	Framing and Scheduling Intervals .....	65
6.3.1	PHY Burst Mode Support .....	65
6.3.2	PHY Continuous Mode Support .....	67
6.3.3	Downlink Burst Subframe Structure .....	67
6.3.4	Uplink Burst Subframe Structure .....	70
6.3.5	Continuous Downstream and Upstream Structure .....	71
6.3.6	Upstream Map .....	71
6.3.7	Requests .....	74
6.3.8	MAP Relevance and Synchronization .....	75
6.4	Contention Resolution .....	76
6.4.1	Transmit Opportunities .....	78
6.5	Fragmentation .....	78
6.5.1	Policy and Rules .....	78
6.5.2	Error Conditions .....	78
6.6	Upstream Service .....	78

6.6.1	Unsolicited Grant Service.....	79
6.6.2	Real-Time Polling Service.....	79
6.6.3	Unsolicited Grant Service with Activity Detection .....	79
6.6.4	Non-Real-Time Polling Service.....	80
6.6.5	Best Effort Service.....	80
6.7	Bandwidth Allocation and Request Mechanisms .....	81
6.7.1	Polling.....	81
6.7.2	Poll-Me Bit .....	85
6.7.3	Piggy-Back and Bandwidth Requests.....	86
6.8	Network Entry and Initialization .....	87
6.8.1	Scanning and Synchronization to Downstream .....	88
6.8.2	Obtain Downstream Parameters .....	89
6.8.3	Obtain Upstream Parameters .....	89
6.8.4	message Flows During Scanning and Upstream Parameter Acquisition.....	91
6.8.5	Initial Ranging and Automatic Adjustments .....	92
6.8.6	Ranging Parameter Adjustment .....	98
6.8.7	Initial Connection Establishment.....	98
6.8.8	Transfer Operational Parameters .....	98
6.9	Ranging.....	106
6.10	Quality of Service .....	111
6.10.1	Theory of Operation.....	111
6.10.2	Service Flows.....	111
6.10.3	Object Model (FIX THIS SECTION) .....	114
6.10.4	Service Classes .....	115
6.10.5	Authorization .....	116
6.10.6	Types of Service Flows.....	117
6.10.7	General Operation.....	119
6.10.8	Dynamic Service.....	121
6.10.9	Dynamic Service Addition.....	130
6.10.10	Dynamic Service Change.....	142
6.10.11	Connection Release.....	153
6.10.12	Dynamic Service Deletion State Transition Diagrams .....	155
6.11	Parameters and Constants .....	163
6.12	Encodings for Configuration and MAC-Layer Messaging.....	165
6.12.1	Configuration File and Registration Settings.....	165
6.12.2	Configuration-File-Specific Settings .....	169
6.12.3	Registration-Request/Response-Specific Encodings .....	171
6.12.4	Dynamic-Service-Message-Specific Encodings .....	173
6.12.5	Quality-of-Service-Related Encodings .....	174
6.12.8	Privacy Configuration Settings Option.....	185
6.12.9	Confirmation Code .....	185
7.	Authentication and Privacy.....	187
8.	Transmission Convergence Sublayer.....	189

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

## **1. Overview**

### **1.1 Scope**

The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for broadband wireless access systems.

### **1.2 Purpose**

<TBD>.

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL



## 2. Normative References

This standard shall be used in conjunction with the following publications. [If the working group wishes to reference the most current edition of the standard, they should include the following line: When the following standards are superseded by an approved revision, the revision shall apply.]

Insert first reference here. For subsequent references, hit return so that the paragraph format References is used for each entry.

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

### **3. Definitions**

**3.1** Base Station (BS):

**3.2** Burst Profile:

**3.3** Connection:

**3.4** Connection Identifier (CID):

**3.5** Customer Premises Equipment (CPE):

**3.6** Downstream/Downlink:

**3.7** Frame:

**3.8** Information Element (IE):

**3.9** Interval Usage Code (IUC):

**3.10** Grant Per Connection:

**3.11** Grant Per Terminal:

**3.12** MAP:

**3.13** Mini-slot:

**3.14** Physical-Slot (PS):

**3.15** Scheduling Interval:

**3.16** Service Flow:

**3.17** Service Flow Class:

**3.18** Service Flow Name:

**3.19** Upstream/Uplink:

PRELIMINARY SUBMITTAL

#### 4. Acronyms and abbreviations

ATDD	Adaptive Time Division Duplexing
BR	Bandwidth Request
BS	Base Station
CG	Continuous Grant
CID	Connection Identifier
CPE	Customer Premises Equipment
CS	Convergence Subprocess
CSI	Convergence Subprocess Indicator
CTG	CPE Transition Gap
DAMA	Demand Assign Multiple Access
DES	Data Encryption Standard
DL	Down Link
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSD	Dynamic Service Deletion
EC	Encryption Control
EKS	Encryption Key Sequence
FC	Fragment Control
FDD	Frequency Division Duplex
FSN	Fragment Sequence Number
GM	Grant Management
GPC	Grant Per Connection
GPT	Grant Per Terminal
HCS	Header Check Sequence
H-FDD	Half-duplex FDD
HL-MAA	High Level Media Access Arbitration
HT	Header Type
IE	Information Element
IUC	Interval Usage Code
LL-MAA	Low Level Media Access Arbitration
MAC	Medium Access Control
MIC	Message Integrity Check
MTG	Modulation Transition Gap
PCD	Physical Channel Descriptor
PBR	Piggy-Back Request
PDU	Protocol Data Unit
PHY	Physical layer
PI	PHY Information element
PKM	Privacy Key Management
PM	Poll Me bit
PS	Physical Slot
QoS	Quality of Service
RS	Reed-Solomon
SAP	Service Access Point
SI	Slip Indicator
SDU	Service Data Unit
TC	Transmission Convergence
TDD	Time Division Duplex
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDU	TC Data Unit
TLV	Type-Length-Value

TRGT	Tx/Rx Transmission Gap
UGS	Unsolicited Grant Service
UGS-AD	Unsolicited Grant Service with Activity Detection
UL	Up Link

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL



## 5. MAC Service Definition

<TBD>.

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

## 6. Media Access Control

In a network that utilizes a shared medium, there must be a mechanism to provide an efficient way to share the medium. A two-way point-to-multipoint wireless network is a good example of a shared medium: here the medium is the space through which the radio waves propagate.

The downlink, from the base station to the user operates on a point-to-multipoint basis. The 802.16.1 wireless link operates with a central base station and a sectorized antenna which is capable of handling multiple independent sectors simultaneously. Within a given frequency channel and antenna sector, all stations receive the same transmission. The base station is the only transmitter operating in this direction, hence it can transmit without having to coordinate with other stations, except for the overall time-division duplexing that divides time into upstream and downstream transmission periods. It broadcasts to all stations in the sector (and frequency); stations check the address in the received messages and retain only those addressed to them.

However, the user stations share the upstream period on a demand basis. Depending on the class of service utilized, the CPE may be issued continuing rights to transmit, or the right to transmit may be granted by the base station after receipt of a request from the user.

In addition to individually-addressed messages, messages may also be sent to multicast groups (control messages and video distribution are examples of multicast applications) as well as broadcast to all stations.

Within each sector, users must adhere to a transmission protocol which minimizes contention between users and enables the service to be tailored to the delay and bandwidth requirements of each user application.

This is accomplished through five different types of upstream scheduling mechanism, which are implemented using unsolicited bandwidth grants, polling, and contention procedures. Mechanisms are defined in the protocol to allow vendors to optimize system performance using different combinations of these bandwidth allocation techniques while maintaining consistent inter-operability definitions. For example, contention can be used to avoid the individual polling of CPEs which have been inactive for a long period of time.

The use of polling simplifies the access operation and guarantees that applications receive service on a deterministic basis if it is required. In general, data applications are delay tolerant, but real-time applications like voice and video require service on a more uniform basis, and sometimes on a very tightly-controlled schedule.

### 6.1 Connections and Service Flows

The MAC is connection-oriented. For the purposes of mapping to services on CPEs and associating varying levels of QoS, all data communications are in the context of a connection. These connections are provisioned when a CPE is installed in the system, and set up over the air at CPE registration to provide a reference against which to request bandwidth. Additionally, new connections may be established when customer's service needs change. A connection defines both the mapping between peer convergence processes that utilize the MAC and a Service Flow. The Service Flow defines the QoS parameters for the PDUs that are exchanged on the connection.

The concept of a Service Flow on a Connection is central to the operation of the MAC protocol. Service Flows provide a mechanism for upstream and downstream Quality of Service management. In particular, they are integral to the bandwidth allocation process. A CPE requests upstream bandwidth on a per-connection basis (implicitly identifying the Service Flow). Bandwidth is granted by the BS either as an aggregate of all grants for a CPE (within a scheduling interval) or on a connection basis.

Once connections are established they must be maintained. The maintenance requirements vary depending upon the type of service connected. For example, unchannelized T1 services require virtually no connection maintenance since they have a constant bandwidth allocated every frame. Channelized T1 services require some maintenance due to the dynamic (but relatively slowly changing) bandwidth requirements if compressed, coupled with the requirement that full bandwidth be available on demand. IP services may require a substantial amount of ongoing maintenance due to their bursty nature and due to the high possibility of fragmentation across frames. As with connection establishment, modifiable connections may require maintenance due to stimulus from either the CPE or the network side of the connection.

Finally, connections may be terminated. This generally occurs only when a customer's service contract changes. The termination of a connection is stimulated by the BS or CPE.

All three of these connection management functions are supported through the use of static configuration and dynamic addition, modification, and deletion of connections.

### 6.1.1 Addressing and Connection Identifiers

Each CPE shall maintain a 64-bit EUI for globally unique addressing purposes. This address uniquely defines the CPE from within the set of all possible vendors and equipment types. This address is used during the registration process to establish the appropriate connections for a CPE. It is also used as part of the authentication process by which the BS and CPE each verify the identity of each other.

Connections are identified by a 16-bit Connection Identifier. Every CPE must establish at least two connections in each direction (upstream and downstream) to enable communication with the BS. The Basic Connection IDs, assigned to a CPE at registration, are used by the BS MAC and the CPE MAC to exchange MAC control messages, provisioning and management information.

For bearer services, the higher layers of the BS set up connections based upon the provisioning information distributed to the base station. The registration of a CPE, or the modification of the services contracted at a CPE, stimulates the higher layers of the BS to initiate the setup of the connections.

The connection ID can be considered a connection identifier even for nominally connectionless traffic like IP, since it serves as a pointer to destination and context information. The use of a 16-bit connection ID permits a total of 64K connections within the sector.

Requests for transmission are based on these connection IDs, since the allowable bandwidth may differ for different connections, even within the same service type. For example, a CPE unit serving multiple tenants in an office building would make requests on behalf of all of them, though the contractual service limits and other connection parameters may be different for each of them.

Many higher-layer sessions may operate over the same wireless connection ID. For example, many users within a company may be communicating with TCP/IP to different destinations, but since they all operate within the same overall service parameters, all of their traffic is pooled for request/grant purposes. Since the original LAN source and destination addresses are encapsulated in the payload portion of the transmission, there is no problem in identifying different user sessions.

The type of service is implicit in the connection ID; it is accessed by a lookup indexed by the connection ID.

There are several CIDs defined in Table 1 that having specific meaning. These identifiers shall not be used for any other purposes.

**Table 1—Connection Identifiers**

Connection Identifier	Value	Description
Initial Ranging	0x0000	Used by a CPE during initial ranging as part of network entry process.
Temporary Registration	0..m	
Basic CIDs	m..n	
Transport CIDs	n..0xFDFF	
Priority Request CIDs	0xFEXX	<u>Request IE Usage</u> If 0x01 bit is set, priority zero can request If 0x02 bit is set, priority one can request If 0x04 bit is set, priority two can request If 0x08 bit is set, priority three can request If 0x10 bit is set, priority four can request If 0x20 bit is set, priority five can request If 0x40 bit is set, priority six can request If 0x80 bit is set, priority seven can request
Multicast Polling CIDs	0xFF00..0xFFFE	A CPE may be included in one or more multicast groups for the purposes of obtaining bandwidth via polling. These connections have no associated Service Flow.
Broadcast CID	0xFFFF	Used for broadcast information that is transmitted on a downlink to all CPE.

PRELIMINARY SUBMITTAL

## 6.2 DOWNLINK Message Formats

Three MAC header formats are defined. The first two are generic headers that precede each MAC Message, including both management and convergence sub-layer data. The third format is used to request additional bandwidth. The single bit Header Type (HT) field distinguishes the generic and bandwidth request header formats. The HT field shall be set to 0 for generic headers. The HT field shall be set to 1 for a bandwidth request header.

The format shown in Figure 2 shall be used for all PDUs transmitted by the CPE to the BS in the uplink direction. For downlink transmissions, the format shown in Figure 2 shall be used.

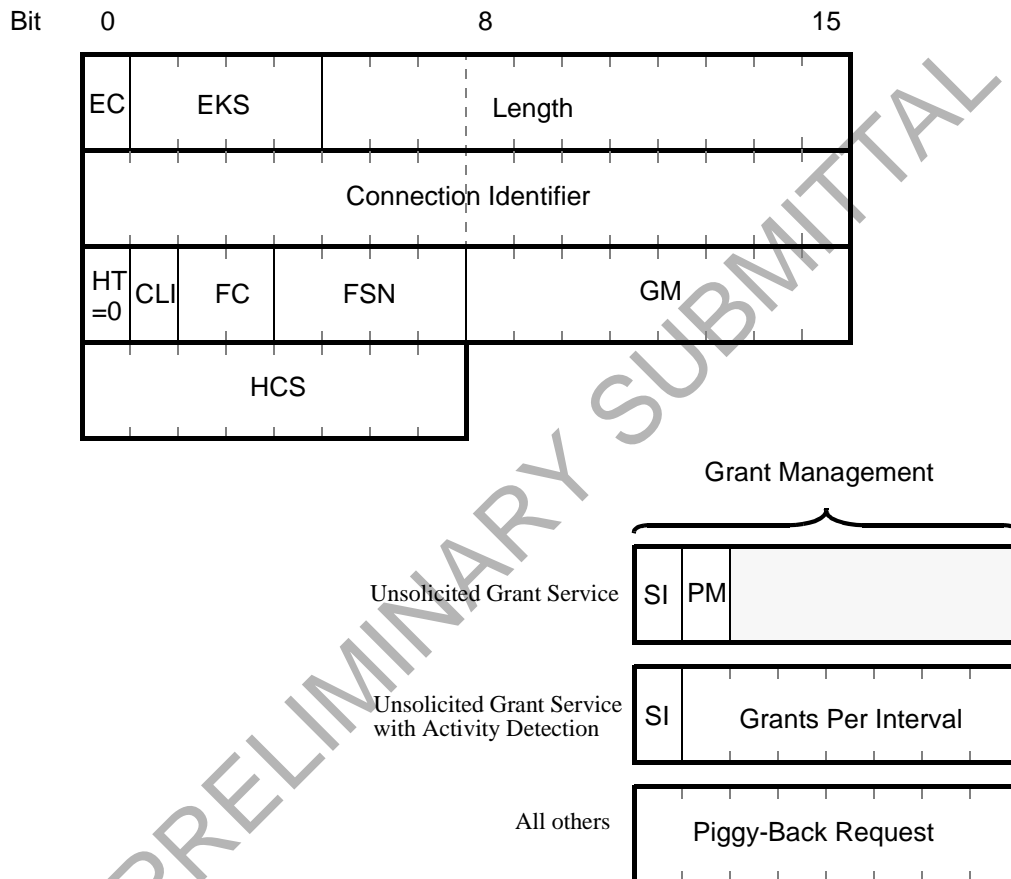


Figure 1—Generic MAC Header Format (Uplink)

These two generic header formats are equivalent with the exception of the Grant Mangament field, which is only present in uplink transmissions.

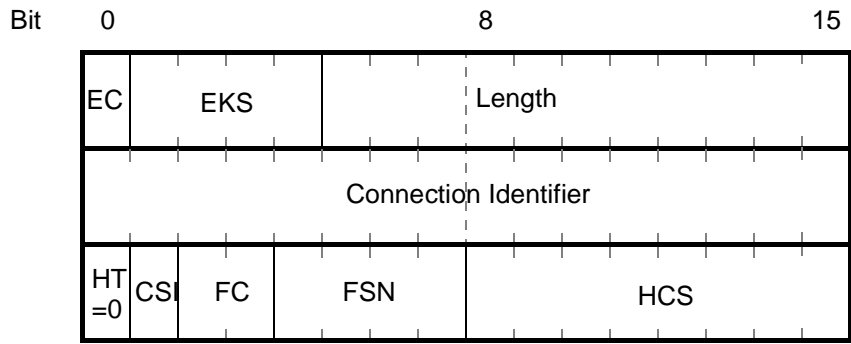


Figure 2—Generic MAC Header Format (Downlink)

The Grant Management field is one byte in length and is used by the CPE to convey bandwidth management needs to the BS. This field is encoded differently based upon the type of connection (as given by the Connection ID). The use of this field is defined in Section 6.7.

The third header is a special format used by a CPE to request additional bandwidth. This header shall always be transmitted without a PDU. The format of the Bandwidth Request Header is given in Figure 3.

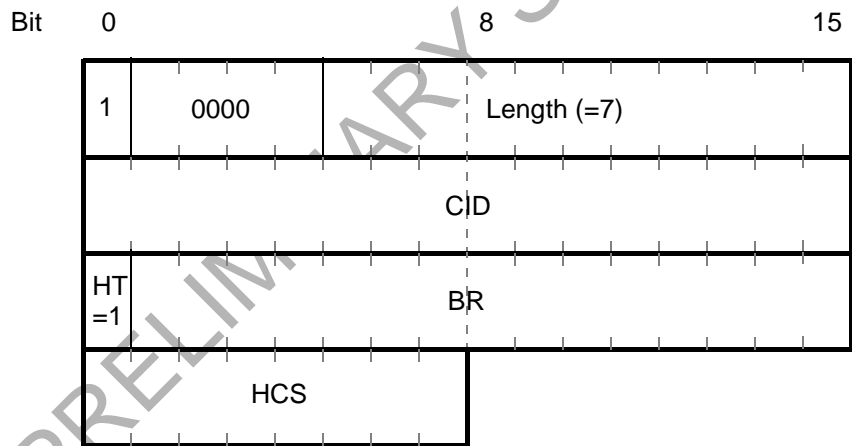


Figure 3—Bandwidth Request Header Format

The Bandwidth Request Header is used by a CPE to request uplink bandwidth. A Bandwidth Request Header shall not have an associated payload:

- a) The length of the header shall always be 7 bytes,
- b) The EC field shall be set to 1, indicating no encryption,
- c) The CID shall indicate the Service Flow for which uplink bandwidth is requested,
- d) The Bandwidth Request (BR) field shall indicate the number of mini-slots requested.

A CPE receiving a Bandwidth Request Header on the downlink shall discard the PDU.



The various fields of the header formats are defined in Table 2. Every header is encoded starting with the EC and EKS fields. The coding of these fields is such that the first byte of a MAC header shall never have the value of 0xFF. This prevents false detection on the stuff byte used in the Transmission Convergence Sub-layer.

**Table 2—MAC Header Fields**

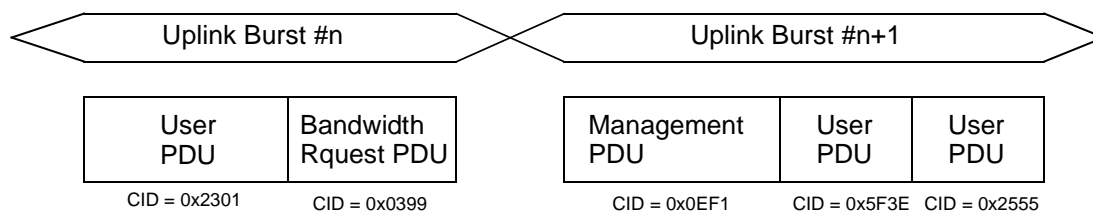
Name	Length (bits)	Description
BR	15	Bandwidth Request  The number of bytes of uplink bandwidth requested by the CPE. The bandwidth request is for the CID. The request shall not include any PHY layer overhead
CID	16	Connection Identifier
CSI	1	Convergence Sub-layer Indication  This bit is allocated to a convergence layer process for signaling between equivalent peers.
EC	1	Encryption Control  1 = Payload is not encrypted 0 = Payload is encrypted

**Table 2—MAC Header Fields**

Name	Length (bits)	Description
EKS	4	Encryption Key Sequence  The index of the Traffic Encryption Key and Initialization Vector used to encrypt the payload. This field is only meaningful if the Encryption Control field is set to zero. This field must be set to all zeros when the EC is 1.
FC	2	Fragmentation Control  Indicates the fragmentation state of the payload: 00 = no fragmentation 01 = last fragment 10 = first fragment 11 = continuing (middle) fragment
FSN	4	Fragmentation Sequence Number  Defines the sequence number of the current fragment. The initial fragment (FC=10) sets this field to 0. This field increments by one (modulo 16) for each fragment.  When fragmentation is not used (FC= 00), this field shall be set to 0.
GPI	7	Grants Per Interval  The number of grants required by a connection using UGS with Activity Detection
HCS	8	Header Check Sequence  An 8-bit field used to detect errors in the header. The generator polynomial is $g(D)=D^8 + D^2 + D + 1$ .
HT	1	Header Type  0 = Generic Header 1 = Bandwidth Request Header
LEN	11	Length  The length in bytes of the entire MAC header and any MAC PDU information that follows this specific header.
PBR	8	Piggy-Back Request  The number of bytes of uplink bandwidth requested by the CPE. The bandwidth request is for the CID. The request shall not include any PHY layer overhead.
PM	1	Poll-Me  0 = No action. 1 = Used by the CPE to request a bandwidth poll.
SI	1	Slip Indicator  0 = No action 1 = Used by the CPE to indicate a slip of uplink grants relative to the uplink queue depth.

Multiple MAC PDUs may be concatenated into a single transmission in either the uplink or downlink directions. Figure 4 illustrates this concept for an uplink burst transmission. Since each PDU is identified by a unique Connection Identifier, the receiving MAC entity is able to present the PDU to the correct SAP based

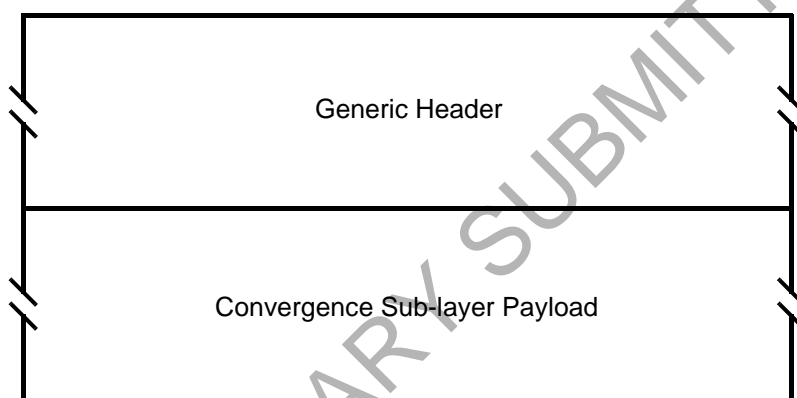
upon that Identifier. Management, user data, and bandwidth request PDUs may be concatenated into the same transmission.



**Figure 4—MAC PDU Concatention**

### 6.2.1 Convergence Sub-layer PDU Formats

The format of the convergence sub-layer PDU shall be as shown in Figure 5. A Convergence Sub-layer PDU may have a zero length payload.



**Figure 5—Convergence Sub-layer PDU Format**

### 6.2.2 MAC Management Messages

A set of management Messages are defined within the core MAC. These Messages shall use the standard Message format as given in Section 6.2.1. All management Messages shall begin the payload content with a

single byte field indicating the management Message type. The format of the management Message is given Figure 6. The encoding of the Message type field is given in Table 3.

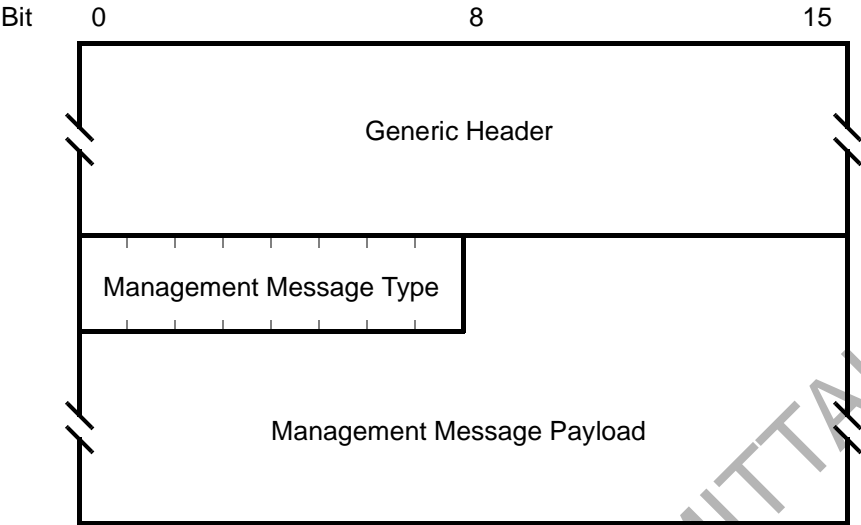


Figure 6—MAC Management Message Format

Table 3—MAC Management Messages

Type	Message Name	Message Description
1	PCD	Physical Channel Descriptor
2	DS-MAP	Downlink Access Definition
3	US-MAP	Uplink Access Definition
4	RNG-REQ	Ranging Request
5	RNG-RSP	Ranging Response
6	REG-REQ	Registration Request
7	REG-RSP	Registration Response
8	REG-ACK	Registration Acknowledge
9	PKM-REQ	Privacy Key Management Request
10	PKM-RSP	Privacy Key Management Response
11	DSA-REQ	Dynamic Service Addition Request
12	DSA-RSP	Dynamic Service Addition Response
13	DSA-ACK	Dynamic Service Addition Acknowledge
14	DSC-REQ	Dynamic Service Change Request

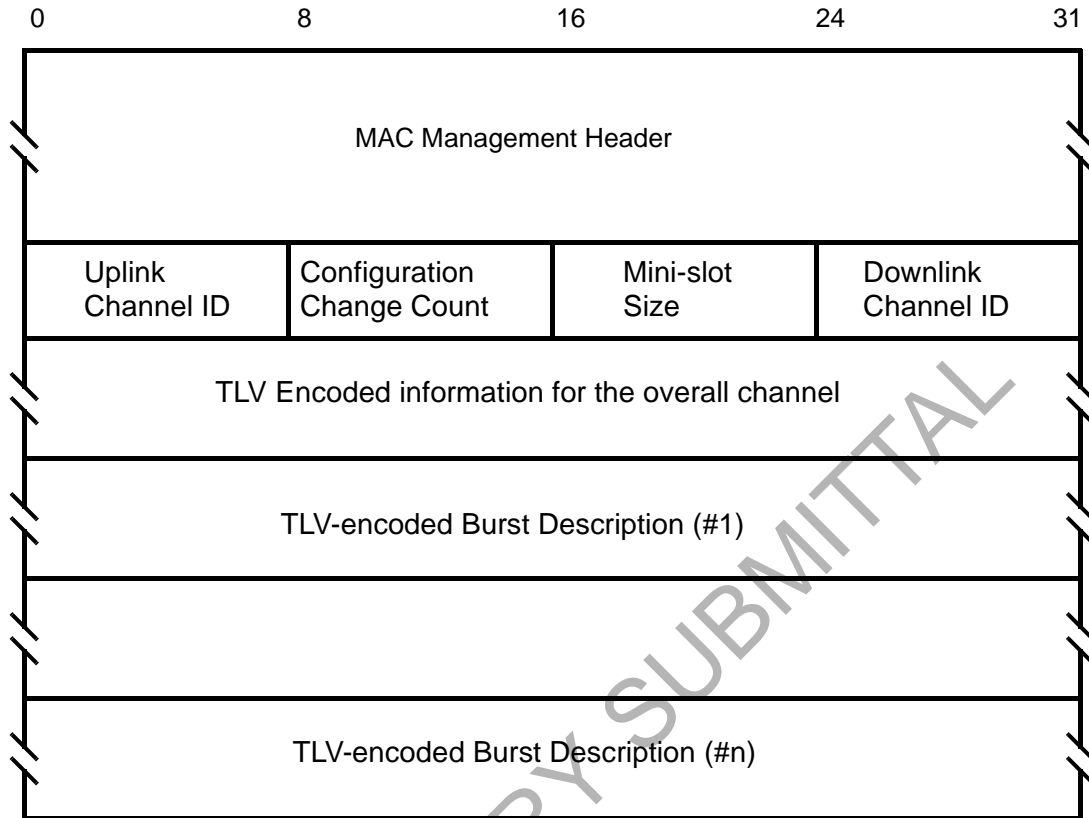
**Table 3—MAC Management Messages**

Type	Message Name	Message Description
15	DSC-RSP	Dynamic Service Change Response
16	DSC-ACK	Dynamic Service Change Acknowledge
17	DSD-REQ	Dynamic Service Deletion Request
18	DSD-RSP	Dynamic Service Deletion Response
19	DCC-REQ	Dynamic Channel Change Request
20	DCC-RSP	Dynamic Channel Change Response
21	MCA-REQ	Multicast Assignment Request
22	MCA-RSP	Multicast Assignment Response
23	DMC-REQ	Downlink Modulation Change Request
24-255		Reserved for future use

**6.2.2.1 Physical Channel Descriptor (PCD) Message**

An Physical Channel Descriptor shall be transmitted by the BS at a periodic interval to define the characteristics of an physical channel. A separate PCD Message shall be transmitted for each active uplink.

To provide for flexibility the message parameters following the channel ID shall be encoded in a type/length/value (TLV) form in which the type and length fields are each 1 octet long.



**Figure 7—Physical Channel Descriptor (PCD) Message Format**

A BS shall generate PCDs in the format shown in Figure 7, including all of the following parameters:

#### **Configuration Change Count**

Incremented by one (modulo the field size) by the BS whenever any of the values of this channel descriptor change. If the value of this count in a subsequent PCD remains the same, the CPE can quickly decide that the remaining fields have not changed, and may be able to disregard the remainder of the message. This value is also referenced from the US-MAP messages.

#### **Mini-Slot Size**

The size  $T$  of the Mini-Slot for this uplink channel in units of Physical Slots. Allowable values are  $T = 2^m$ , where  $m = 0, \dots, 7$ .

#### **Uplink Channel ID**

The identifier of the uplink channel to which this Message refers. This identifier is arbitrarily chosen by the BS and is only unique within the MAC-Sublayer domain.

#### **Downlink Channel ID**

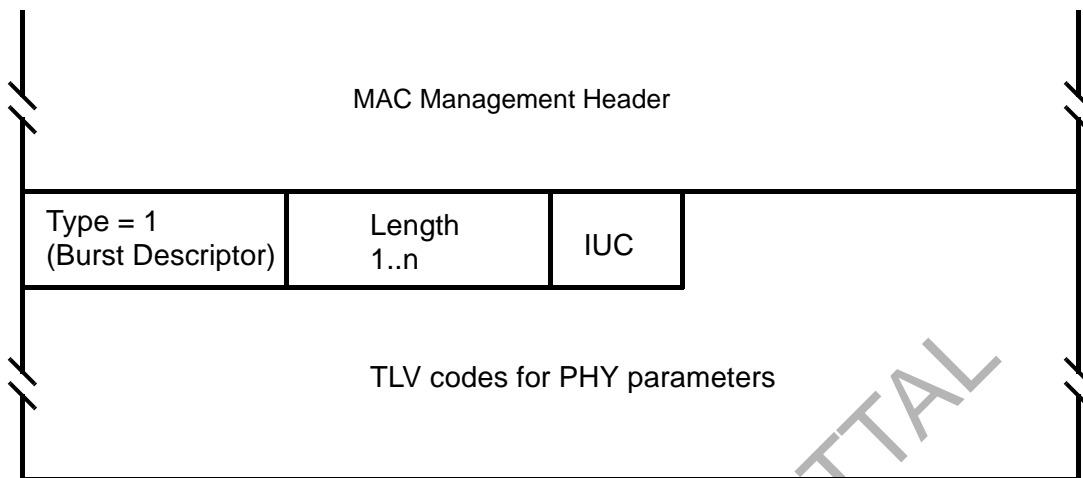
The identifier of the downlink channel on which this Message has been transmitted. This identifier is arbitrarily chosen by the BS and is only unique within the MAC-Sublayer domain.

All other parameters are coded as TLV tuples. The type values used shall be those defined in Table 4, for channel parameters, and Table 5, for uplink physical layer burst attributes. Channel-wide parameters (from Table 4) shall precede burst descriptors (type 1 below).

**Table 4—Physical Channel Attributes**

Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Burst Descriptor	1		May appear more than once; described below. The length is the number of bytes in the overall object, including embedded TLV items.
Symbol Rate	2	2	5 - 40 MBaud. The incremental rates are not yet defined for the PHY layer. The use of a TLV allows future clarification of this field without modification to the MAC.
Frequency	3	4	Uplink center frequency (kHz)
Preamble Pattern	4	1-128	<p>Preamble superstring. All burst-specific preamble values are chosen as bit-substrings of this string.</p> <p>The first byte of the Value field contains the first 8 bits of the superstring, with the first bit of the preamble superstring in the MSB position of the first Value field byte, the eighth bit of the preamble superstring in the LSB position of the first Value field byte; the second byte in the Value field contains the second eight bits of the superstring, with the ninth bit of the superstring in the MSB of the second byte and sixteenth bit of the preamble superstring in the LSB of the second byte, and so forth.</p>
Tx/Rx Gap	5	1	The number of PS between the end of the downlink and uplink transmissions. This TLV is only used if the PHY Type field of the DS-MAP message is {0, 1} (TDD).
Rx/Tx Gap	6	1	The number of PS between the end of the uplink and downlink transmissions. This TLV is only used if the PHY Type field of the DS-MAP message is {0, 1} (TDD).
Shortened Downlink CPE Preamble Length	7	1	The number of PS...<TBD>
BS Transmit Power	8	1	Signed in units of 1dB

Burst Descriptors are compound TLV encodings that define, for each type of uplink usage interval, the physical-layer characteristics that are to be used during that interval. The uplink interval usage codes are defined in the US-MAP Message.



**Figure 8—Top-Level Encoding for a Burst Descriptor**

A Burst Descriptor shall be included for each Interval Usage Code that is to be used in the allocation MAP. The Interval Usage Code shall be one of the values from Table 5.

Within each Burst Descriptor is an unordered list of Physical-layer attributes, encoded as TLV values. These attributes are shown in Table 5.

Type > 1	Length and Value Information
Type > 1	Length and Value Information
Other Type > 1 TLV Codes	
Type = 1	First Burst Descriptor
Type = 1	Second Burst Descriptor

**Figure 9—Top-Level Encoding for a Burst Descriptor**

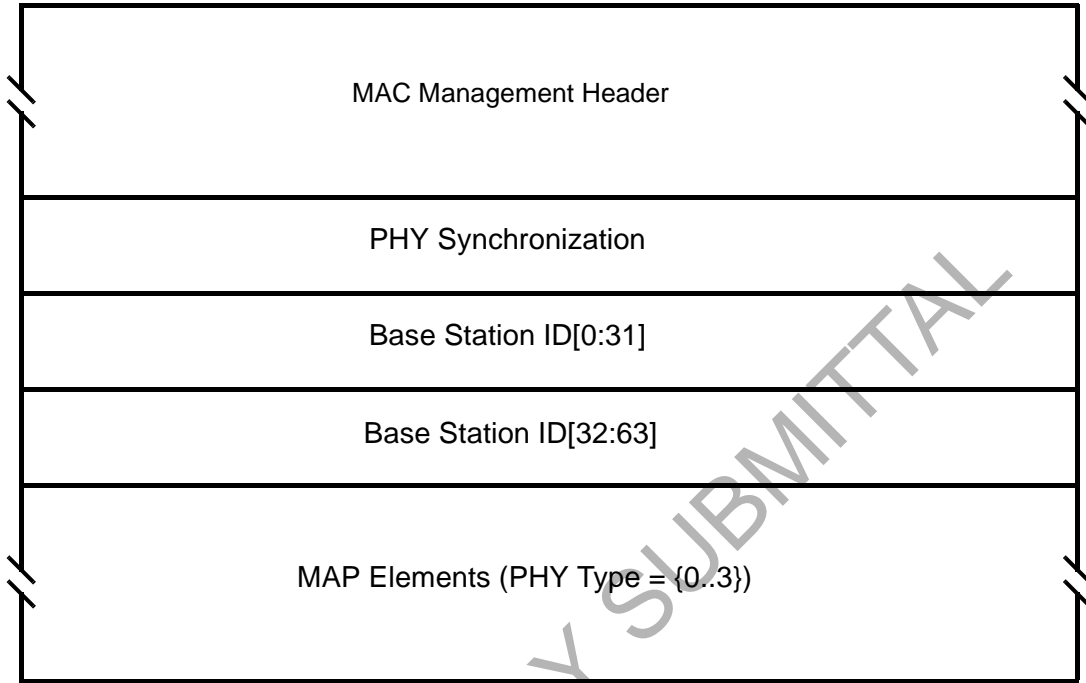


**Table 5—Uplink Physical Layer Burst Profile Parameters**

Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Modulation Type	1	1	1 = QPSK, 2 = 16QAM, 3 = 64-QAM
Differential Encoding	2	1	1 = on, 2 = off
Preamble Length	3	2	Up to 1024 bits. The value must be an integral number of symbols (a multiple of 2 for QPSK and 4 for 16QAM and 6 for 64QAM)
Preamble Value Offset	4	2	Identifies the bits to be used for the preamble value. This is specified as a starting offset into the Preamble Pattern (see <TBD>). That is, a value of zero means that the first bit of the preamble for this burst type is the value of the first bit of the Preamble Pattern. A value of 100 means that the preamble is to use the 101st and succeeding bits from the Preamble Pattern. This value must be a multiple of the symbol size.  The first bit of the Preamble Pattern is the firstbit transmitted in the uplink burst.
FEC Error Correction (T)	5	1	0-10 (0 implies no FEC. The number of codeword parity bytes is 2*T)
FEC Codeword Information Bytes (k)	6	1	Fixed: 16 to 253 (assuming FEC on) Shortened: 16 to 253 (assuming FEC on) (Not used if no FEC, T=0)
Scrambler Seed	7	2	The 15-bit seed value left justified in the 2 byte field. Bit 15 is the MSB of the first byte and the LSB of the second byte is not used. (Not used if scrambler is off)
Maximum Burst Size	8	1	The maximum number of mini-slots that can be transmitted during this burst type. Absence of this configuration setting implies that the burst size is limited elsewhere. When the interval type is Short Data Grant this value MUST be present and greater than zero. (See <TBD>)
Guard Time Size	9	1	Number of symbol times which must follow the end of this burst. (Although this value may be derivable from other network and architectural parameters, it is included here to ensure that the CPEs and BS all use the same value.)
Last Codeword Length	10	1	1 = fixed; 2 = shortened
Scrambler on/off	11	1	1 = on; 2 = off

### 6.2.3 Downlink MAP (DS-MAP) Message

The Downlink MAP (DS-MAP) message defines the access to the downlink information relative to the PHY mode. The DS-MAP message takes on different formats depending upon the value of the PHY Type field.



**Figure 10—Downlink MAP Message Format (PHY Type = 4)**

A BS shall generate DS-MAP messages in the format shown in Figure 10, including all of the following parameters:

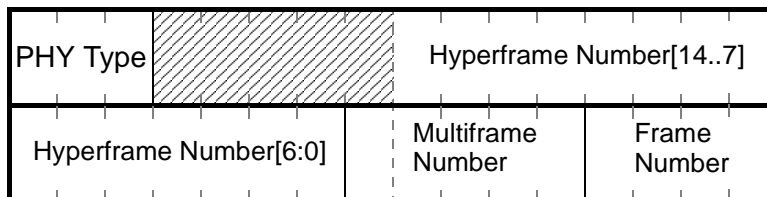
#### PHY Synchronization

A four byte field. The first three bits define the PHY type, as given by the following value:

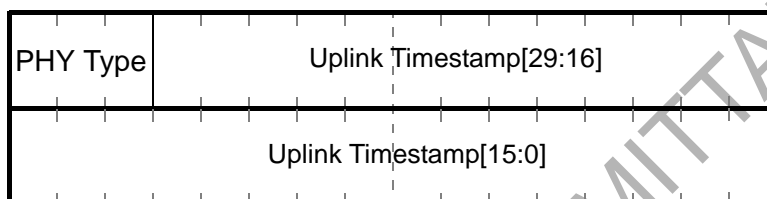
- 0 = non-adaptive TDD
- 1 = TDD
- 2 = FDD/TDM (Burst Downlink PHY)
- 3 = FDD/TDMA
- 4 = FDD/TDM (Continuous Downlink PHY)

The remaining 29 bits are encoded as shown in Figure 11 for PHY Type = {0..3} or Figure 12 for PHY Type = 4. For burst downlink PHY operations, the bits are encoded as the frame number. For continuous downlink PHY operations, the bits are encoded as a timestamp that synchronizes the uplink transmissions.

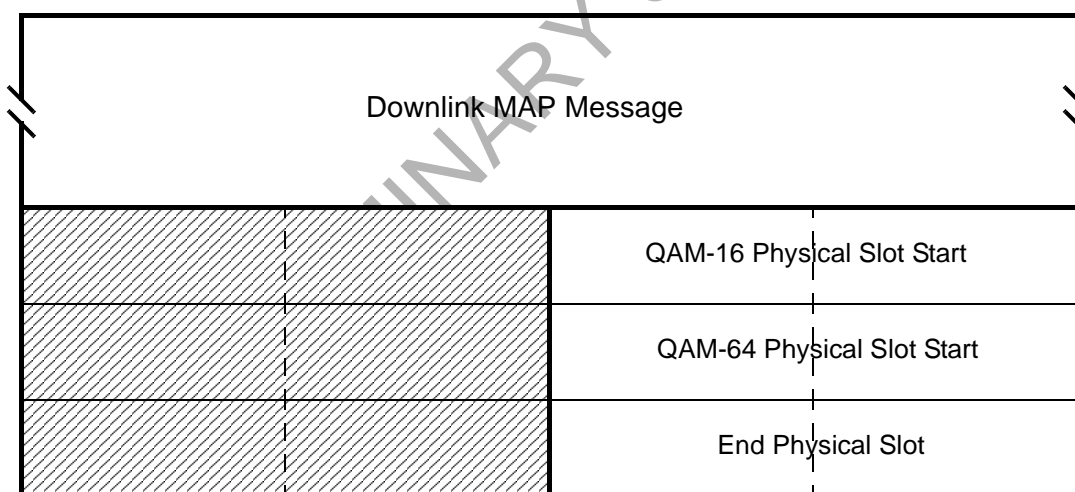
The encoding of remaining portions of the DS-MAP message are also based upon the PHY field. For PHY Type = {0, 1, 4} no additional information follows the Base Station ID field. For PHY Type = 2, a set of mapping information sorted by modulation type is defined as in Figure 13. For PHY Type = 3, a set of mapping information sorted by Connection ID is defined as in Figure 14.



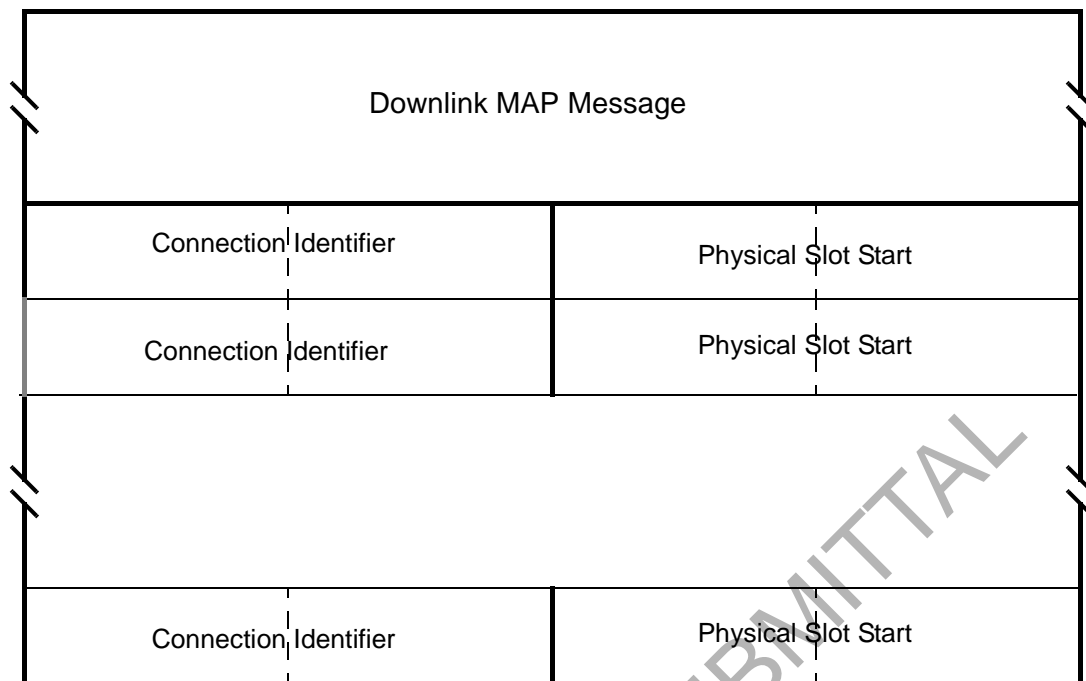
**Figure 11—PHY Synchronization Field (PHY Type = {0..3})**



**Figure 12—PHY Synchronization Field (PHY Type = 1)**

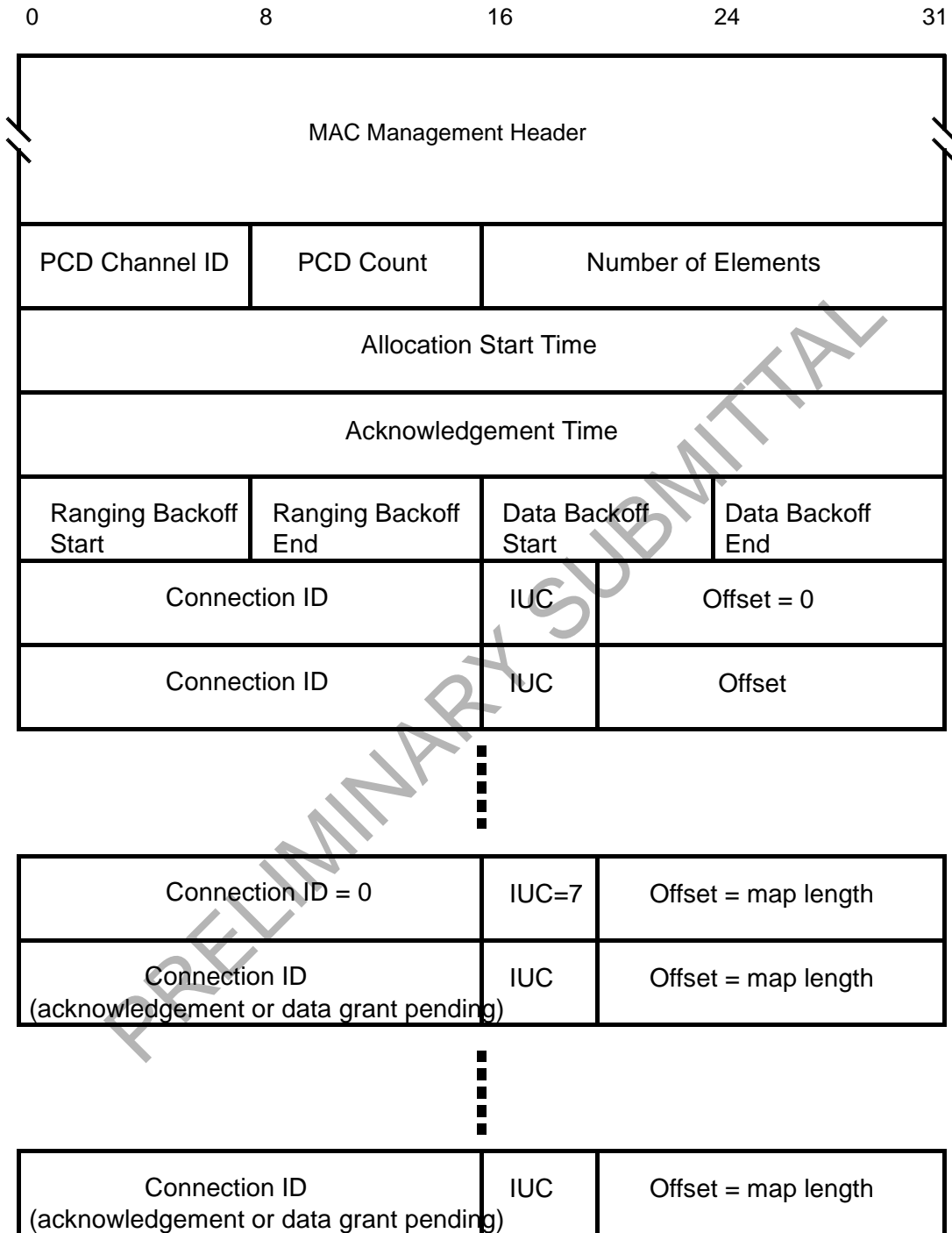


**Figure 13—Downlink TDM MAP Message Element Format**



**Figure 14—Downlink TDMA MAP Message Element Format**

## 6.2.4 Uplink MAP Message



**Figure 15—Uplink MAP Message Format**

### Uplink Channel ID

The identifier of the uplink channel to which this Message refers.

**PCD Count**

Matches the value of the Configuration Change Count of the PCD which describes the burst parameters which apply to this map.

**Number Elements**

Number of information elements in the map.

**Alloc Start Time**

Effective start time of the uplink allocation defined by the US-MAP in units of mini-slots. The start time is relative to the start of a frame in which US-MAP message is transmitted (PHY Type = {0..3}) or from BS initialization (PHY Type = 4).

**Ack Time**

Latest time processed in uplink in units of mini-slots. This time is used by the CPE for collision detection purposes. The ack time is relative to the start of a frame in which US-MAP message is transmitted (PHY Type = {0..3}) or from BS initialization (PHY Type = 4).

**Ranging Backoff Start**

Initial back-off window size for initial ranging contention, expressed as a power of 2. Values of n range 0-15 (the highest order bits must be unused and set to 0).

**Ranging Backoff End**

Final back-off window size for initial ranging contention, expressed as a power of 2. Values of n range 0-15 (the highest order bits must be unused and set to 0).

**Data Backoff Start**

Initial back-off window size for contention data and requests, expressed as a power of 2. Values of n range 0-15 (the highest order bits must be unused and set to 0).

**Data Backoff End**

Final back-off window size for contention data and requests, expressed as a power of 2. Values of n range 0-15 (the highest order bits must be unused and set to 0).

**MAP Information Elements**

Information elements define uplink bandwidth allocations. Each US-MAP message shall contain at least one Information Element. The format of the IE shall be as shown in Figure 16. Each IE consists of three fields: a Connection Identifier, an Interval Usage Code, and an offset.

The Connection Identifier represent the assignment of the IE to either a unicast, multicast, or broadcast address. When specifically addressed to allocate a bandwidth grant, the CID may be either the Basic CID of the CPE or a Traffic CID for one of the connections of the CPE. A four-bit Interval Usage Code (IUC) shall be used to define the type of uplink access and the burst type associated with that access. Table 6 defines the use of the IUCs. The offset shall be the length from the start of the previous IE to the start of this IE in units of mini-slots. The first IE shall have an offset of 0.

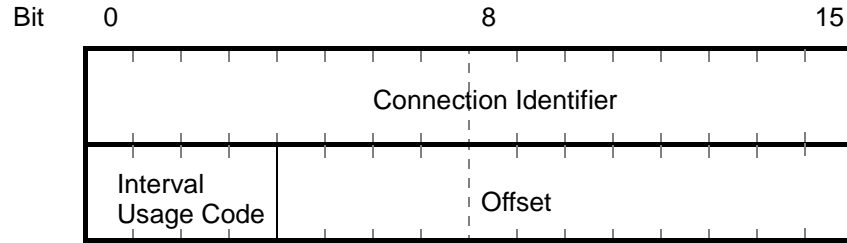


Figure 16—US-MAP Information Element

Table 6—Uplink MAP Information Elements

IE Name	Interval Usage Code (IUC)	Connection ID	Mini-slot Offset
Request	1	any	Starting offset of REQ region
Initial Maintenance	2	broadcast	Starting offset of MAINT region (used in Initial Ranging)
Station Maintenance	3	unicast	Starting offset of MAINT region (used in Periodic Ranging)
Short Data Grant	4	unicast	Starting offset of Data Grant assignment If inferred length = 0, then it is a Data Grant pending.
Long Data Grant	5	unicast	Starting offset of Data Grant assignment If inferred length = 0, then it is a Data Grant Pending
Short Data Grant 2	6	unicast	Starting offset of Data Grant 2 assignment If inferred length = 0, then it is a Data Grant pending.
Long Data Grant 2	7	unicast	Starting offset of Data Grant 2 assignment If inferred length = 0, then it is a Data Grant pending.
Short Data Grant 3	8	unicast	Starting offset of Data Grant 3 assignment If inferred length = 0, then it is a Data Grant pending.
Long Data Grant 3	9	unicast	Starting offset of Data Grant 3 assignment If inferred length = 0, then it is a Data Grant pending.
Null IE	10	zero	Ending offset of the previous grant. Used to bound the length of the last actual interval allocation.
Data Ack	11	unicast	BS sets to map length
Reserved	12-14	any	Reserved
Expansion	15	expanded IUC	# of additional 32-bit words in this IE

### 6.2.5 Ranging Request (RNG-REQ) Message

A Ranging Request MUST be transmitted by a BS at initialization and periodically on request from BS to determine network delay and request power and/or modulation adjustment. This shall be followed by a Packet PDU in the format shown in Figure 17.

PRELIMINARY SUBMITTAL



If zero, then all previous Ranging Response attributes have been applied prior to transmitting this request. If nonzero then this is time estimated to be needed to complete assimilation of ranging parameters. Note that only equalization can be deferred. Units are in unsigned centiseconds (10 msec).

All other parameters are coded as TLV tuples.

### Modulation Type

An optional parameter. The Modulation type requested by the BS for downlink traffic. The BS determines the appropriate modulation type to use based upon measurements of the downlink RF channel relative to the Modulation Transition Thresholds defined in the RNG-RSP Message.

#### 6.2.5.1 RNG-REQ TLV Encodings

The type values used MUST be those defined in Table 7. These are unique within the ranging request Message but not across the entire MAC Message set. The type and length fields MUST each be 1 octet in length.

**Table 7—Ranging Request Message Encodings**

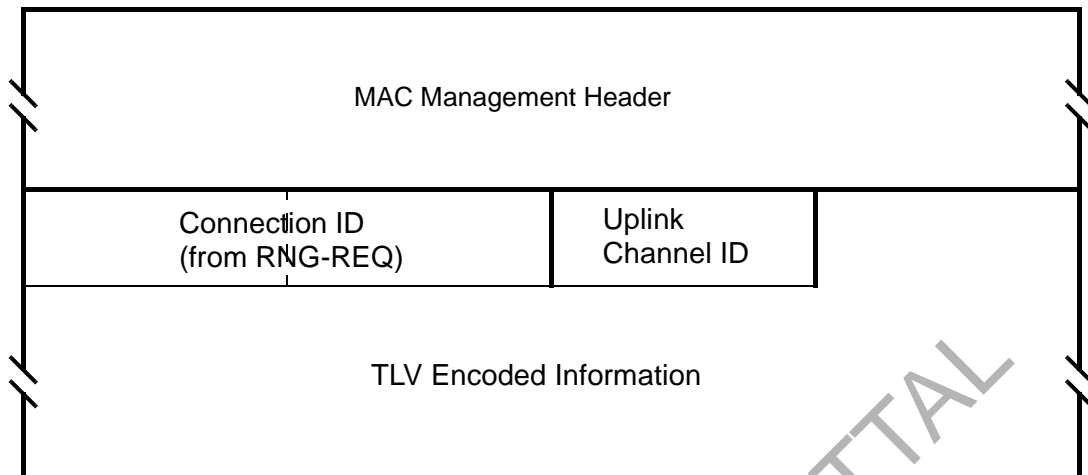
Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Modulation Type	1	1	1 = QPSK, 2 = 16-QAM, 3 = 64-QAM
Reserved	2-255	n	Reserved for future use

#### 6.2.6 Ranging Response (RNG-RSP) Message

A Ranging Response shall be transmitted by a BS in response to received RNG-REQ. It may be noted that, from the point of view of the CPE, reception of a Ranging Response is stateless. In particular, the CPE shall be prepared to receive a Ranging Response at any time, not just following a Ranging Request.

The RNG-RSP Message shall be transmitted using QPSK modulation.

To provide for flexibility, the Message parameters following the Uplink Channel ID shall be encoded in a type/length/value (TLV) form.



**Figure 18—RNG-RSP Message Format**

A BS shall generate Ranging Responses in the form shown in Figure 18, including all of the following parameters:

#### **CID**

If the modem is being instructed by this response to move to a different channel, this is initialization-CID. Otherwise, this is the CID from the corresponding RNG-REQ to which this response refers, except that if the corresponding RNG-REQ was an initial ranging request specifying a initialization CID, then this is the assigned temporary CID.

#### **Uplink Channel ID**

The identifier of the uplink channel on which the BS received the RNG-REQ to which this response refers.

#### **Ranging Status**

Used to indicate whether uplink Messages are received within acceptable limits by BS.

All other parameters are coded as TLV tuples.

#### **Timing Adjust Information**

The time by which to offset frame transmission so that frames arrive at the expected mini-slot time at the BS.

#### **Power Adjust Information**

Specifies the relative change in transmission power level that the CPE is to make in order that transmissions arrive at the BS at the desired power.

**Frequency Adjust Information**

Specifies the relative change in transmission frequency that the CPE is to make in order to better match the BS. (This is fine-frequency adjustment within a channel, not re-assignment to a different channel)

**CPE Transmitter Equalization Information**

This provides the equalization coefficients for the pre-equalizer.

**Downlink Frequency Override**

An optional parameter. The downlink frequency with which the modem should redo initial ranging.

**Uplink Channel ID Override**

An optional parameter. The identifier of the uplink channel with which the modem should redo initial ranging.

**16-QAM Threshold**

An optional parameter. The threshold for transition between QPSK and 16-QAM on a downlink channel is specified by the BS for use by the CPE.

**64-QAM Threshold**

An optional parameter. The threshold for transition between 16-QAM and 64-QAM on a downlink channel is specified by the BS for use by the CPE.

**Threshold Delta**

An optional parameter. The delta about which a hysteresis is defined for transition of the CPE between modulation types. Used by the CPE in conjunction with the 16-QAM and 64-QAM Thresholds to determine when to request a modulation change for the downlink channel.

**Modulation Type**



An optional parameter. The maximum allow set of Modulation types allowed for the CPE for downlink traffic. This parameter is sent in response to the RNG-REQ Modulation Type from the CPE. The CPE responds with the maximum allowed set of modulation types based upon the combination of the requested modulation type and the maximum allowable modulation type determined at registration or from a dynamic service operation.

**6.2.6.1 RNG-RSP TLV Encodings**

The type values used shall be those defined in Table 8 and Figure 21. These are unique within the ranging response Message but not across the entire MAC Message set. The type and length fields shall each be 1 octet in length.

**Table 8—Ranging Response Message Encodings**

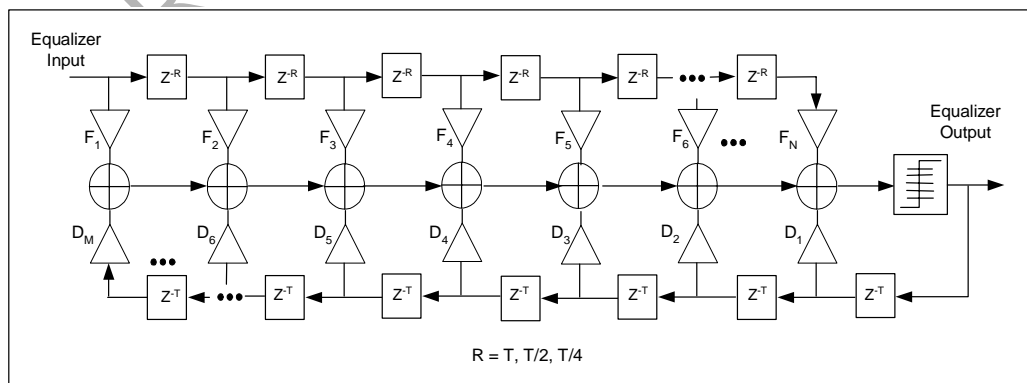
<b>Name</b>	<b>Type (1 byte)</b>	<b>Length (1 byte)</b>	<b>Value (Variable Length)</b>
Timing Adjust	1	4	Tx timing offset adjustment (signed 32-bit, units of mini-slot time/64)
Power Level Adjust	2	1	Tx Power offset adjustment (signed 8-bit, 1/4-dB units)
Offset Frequency Adjust	3	4	Tx frequency offset adjustment (signed 32-bit, Hz units)
Transmit Equalization Adjust	4	n	Tx equalization data - see details below
Ranging Status	5	1	1 = continue, 2 = abort, 3 = success
Downlink frequency override	6	4	Center frequency of new downlink channel in kHz
Uplink channel ID override	7	1	Identifier of the new uplink channel.
16-QAM Threshold	8	1	C/I+N for minimum 16-QAM operation in 0.25 dB.
64-QAM Threshold	9	1	C/I+N for minimum 64-QAM operation in 0.25 dB.
Threshold Delta	10	1	Hysteresis delta for modulation thresholds in 0.25 dB.
Modulation Type	11	1	1 = QPSK, 2 = QPSK or 16-QAM, 3 = QPSK or 16/64-QAM
Reserved	12-255	n	Reserved for future use

type 4	length	main tap location	number of forward taps per symbol
number of forward taps (N)	number of reverse taps (M)		
first coefficient $F_1$ (real)		first coefficient $F_1$ (imag)	
			
last coefficient $F_N$ (real)		last coefficient $F_N$ (imag)	
first reverse coefficient $D_1$ (real)		first reverse coefficient $D_1$ (imag)	
			
last reverse coefficient $D_M$ (real)		last reverse coefficient $D_M$ (imag)	

**Figure 19—Generalized Decision Feedback Equalization Coefficients**

The number of forward taps per symbol shall be in the range of 1 to 4. The main tap location refers to the position of the zero delay tap, between 1 and N. For a symbol-spaced equalizer, the number of forward taps per symbol field shall be set to “1”. The number of reverse taps (M) field shall be set to “0” for a linear equalizer. The total number of taps MAY range up to 64. Each tap consists of a real and imaginary coefficient entry in the table.

If more than 255 bytes are needed to represent equalization information, then several type-4 elements MAY be used. Data shall be treated as if byte-concatenated, that is, the first byte after the length field of the second type-4 element is treated as if it immediately followed the last byte of the first type-4 element.

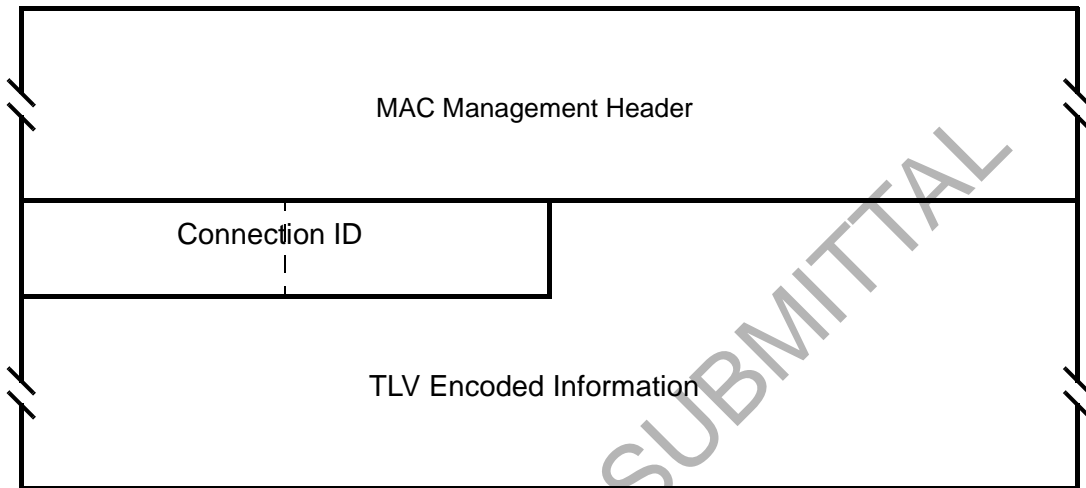


**Figure 20—Generalized Equalizer Tap Location Definition**

### 6.2.7 Registration Request (REG-REQ) Message

A Registration Request MUST be transmitted by a CPE at initialization after receipt of a CPE parameter file.

To provide for flexibility, the Message parameters following the CID shall be encoded in a type/length/value form.



**Figure 21—REG-REQ Message Format**

A CPE shall generate Registration Requests in the form shown in Figure 21, including the following parameters:

#### **CID**

Temporary CID for this CPE.

All other parameters are coded as TLV tuples as defined in Section 6.12.

Registration Requests can contain many different TLV parameters, some of which are set by the CPE according to its configuration file and some of which are generated by the CPE itself. If found in the Configuration File, the following Configuration Settings shall be included in the Registration Request.

Configuration File Settings:

- Downlink Frequency Configuration Setting
- Uplink Channel ID Configuration Setting
- Network access Control Object
- Uplink Service Flow Configuration Setting
- Downlink Service Flow Configuration Setting
- Privacy Configuration Setting
- Maximum Number of Subscribers
- Privacy Enable Configuration Setting

- TFTP Server Timestamp
- TFTP Server Provisioned Modem address
- Downlink Modulation Configuration Setting
- Vendor-Specific Information Configuration Setting
- CPE MIC Configuration Setting
- BS MIC Configuration Setting

**The CPE shall forward the vendor specific configuration settings to the BS in the same order in which they were received in the configuration file to allow the Message integrity check to be performed.**

The following registration parameter shall be included in the Registration Request.

Vendor Specific Parameter:

- Vendor ID Configuration Setting (Vendor ID of CPE)

The following registration parameter **MUST** also be included in the Registration Request.

- Modem Capabilities Encodings

The following registration parameter **MAY** also be included in the Registration Request.

- Modem IP address

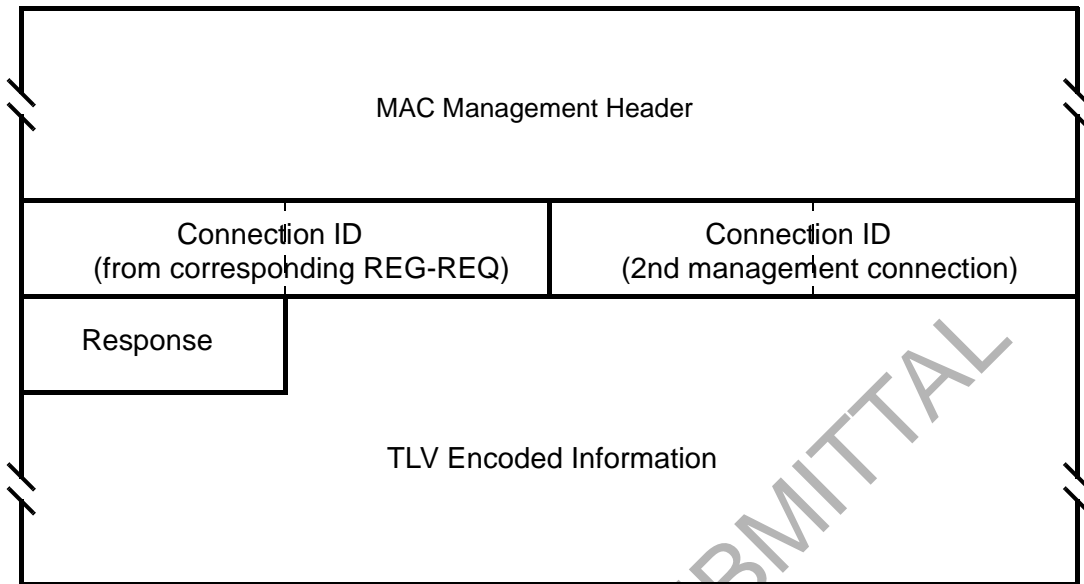
The following Configuration Settings shall not be forwarded to the BS in the Registration Request.

- Software Upgrade Filename
- Software Upgrade TFTP Server IP address
- SNMP Write-access Control
- SNMP MIB Object
- CPE EUI-64 MAC address
- HMAC Digest
- End Configuration Setting
- Pad Configuration Setting

### **6.2.8 Registration Response (REG-RSP) Message**

A Registration Response **MUST** be transmitted by BS in response to received REG-REQ.

To provide for flexibility, the Message parameters following the Response field **MUST** be encoded in a TLV format.



**Figure 22—REG-RSP Message Format**

A BS shall generate Registration Responses in the form shown in Figure 22, including both of the following parameters:

**CID from Corresponding REG-REQ**

CID from corresponding REG-REQ to which this response refers. (This acts as a transaction identifier)

**CID #2**

CID for secondary management purposes

**Response**

- 0 = Okay
- 1 = Authentication Failure
- 2 = Class of Service Failure

**Failures apply to the entire Registration Request. Even if only a single requested Service Flow is invalid or undeliverable the entire registration is failed.**

If the REG-REQ was successful and contained Service Flow Parameters, the REG-RSP **MUST** contain:

**Service Flow Parameters**

All the Service Flow Parameters from the REG-REQ, plus the Connection ID assigned by the BS. Every Service Flow that contained a Service Class Name that was admitted/activated **MUST** be



expanded into the full set of TLVs defining the Service Flow. Every uplink Service Flow that was admitted/activated<sup>1</sup> MUST have a Service Identifier assigned by the BS. A Service Flow that was only provisioned will include only those QoS parameters that appeared in the REG-REQ, plus the assigned Connection ID.

If the REG-REQ failed and contained Service Flow Parameters, the REG-RSP MUST contain the following:

#### Service Flow Error Set

A Service Flow Error Set and identifying Service Flow Reference MUST be included for every failed Service Flow in the corresponding REG-REQ. Every Service Flow Error Set MUST include every specific failed QoS Parameter of the corresponding Service Flow.

Service Class Name expansion always occurs at admission time. Thus, if a Registration-Request contains a Service Flow Reference and a Service Class Name for deferred admission/activation, the Registration-Response MUST NOT include any additional QoS Parameters except the Service Flow Identifier.

All other parameters are coded as TLV tuples:

#### Modem Capabilities

The BS response to the capabilities of the modem (if present in the Registration Request)

#### Vendor-Specific Data

As defined in Section 6.12

- Vendor ID Configuration Setting (vendor ID of BS)
- Vendor-specific extensions

**Note: The temporary CID MUST no longer be used once the REG-RSP is received.**

#### 6.2.8.1 Encodings

The type values used MUST be those shown below. These are unique within the Registration Response Message but not across the entire MAC Message set. The type and length fields MUST each be 1 octet.

#### Modem Capabilities

This field defines the BS response to the modem capability field in the Registration Request. The BS responds to the modem capabilities to indicate whether they may be used. If the BS does not recognize a modem capability, it must return this as “off” in the Registration Response.

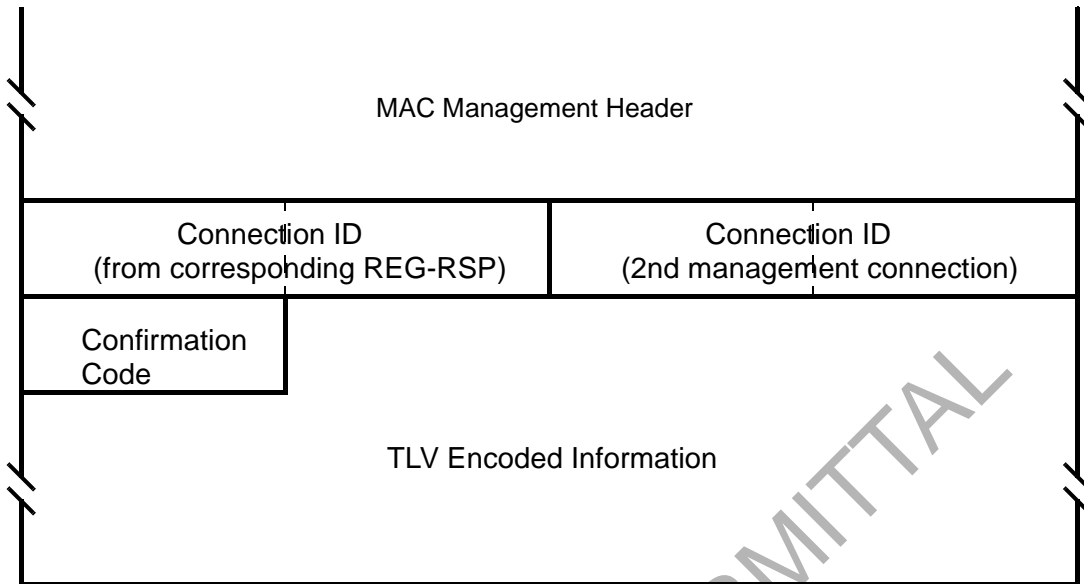
Only capabilities set to “on” in the REG-REQ may be set “on” in the REG-RSP as this is the handshake indicating that they have been successfully negotiated.

Encodings are as defined for the Registration Request.

#### 6.2.9 Registration Acknowledge (REG-ACK) Message

A Registration Acknowledge MUST be transmitted by the CPE in response to a REG-RSP from the BS. It confirms acceptance by the CPE of the QoS parameters of the flow as reported by the BS in its REG-RSP. The format of a REG-ACK MUST be as shown in Figure 23.

<sup>1</sup>The ActiveQoSParamSet or AdmittedQoSParamSet is non-null.



**Figure 23—REG-ACK Message Format**

The parameter **MUST** be as follows:

#### **CID from Corresponding REG-RSP**

CID from corresponding REG-RSP to which this acknowledgment refers. (This acts as a transaction identifier)

#### **Confirmation Code**

The appropriate Confirmation Code (refer to Section 6.12) for the entire corresponding Registration Response.

The CPE **MUST** forward all provisioned Service Flows to the BS. Since any of these provisioned items can fail, the REG-ACK **MUST** include Error Sets for all failures related to these provisioned items.

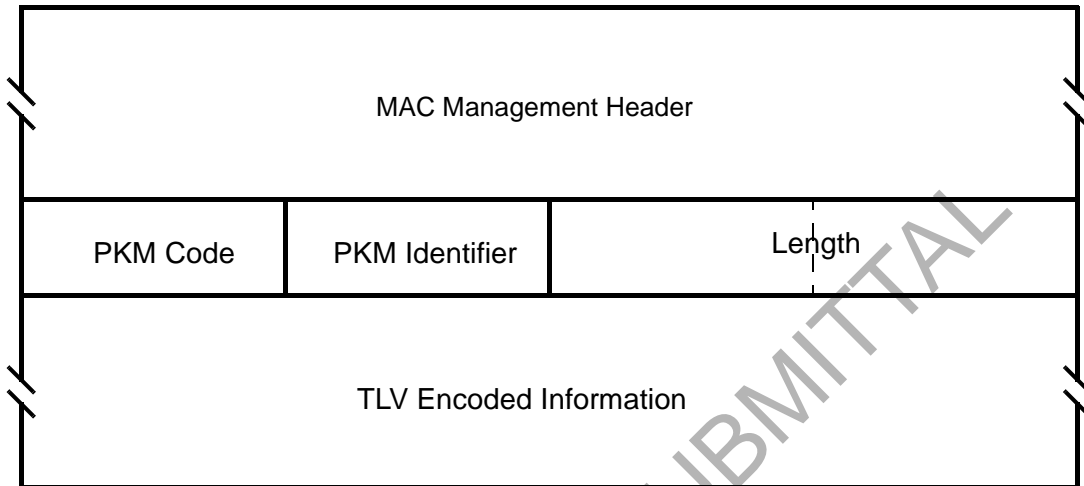
#### **Service Flow Error Set**

The Service Flow Error Set of the REG-ACK Message encodes specifics of any failed Service Flows in the REG-RSP Message. A Service Flow Error Set and identifying Service Flow Reference **MUST** be included for every failed QoS Parameter of every failed Service Flow in the corresponding REG-RSP Message. This parameter **MUST** be omitted if the entire REG-REQ/RSP is successful.

Note: Per Service Flow acknowledgment is necessary not just for synchronization between the CPE and BS, but also to support use of the Service Class Name. Since the CPE may not know all of the Service Flow parameters associated with a Service Class Name when making the Registration Request, it may be necessary for the CPE to NAK a Registration Response if it has insufficient resources to actually support this Service Flow.

### 6.2.10 Privacy Key Management — Request (PKM-REQ) Message

Privacy Key Management protocol Messages transmitted from the CPE to the BS shall use the form shown in Figure 24.



**Figure 24—PKM-REQ Message Format**

Parameters MUST be as follows:

#### **PKM Code**

The Code field is one octet and identifies the type of PKM packet. When a packet is received with an invalid Code field, it shall be silently discarded. The Code values are defined in Section 7.2.5.1.

#### **PKM Identifier**

The Identifier field is one octet. A CPE uses the identifier to match a BS response to the CPE's requests.

The CPE MUST change (e.g., increment, wrapping around to 0 after reaching 255) the Identifier field whenever it issues a new PKM Message. A "new" Message is an Authorization Request, Key Request or SA Map Request that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field MUST remain unchanged.

The Identifier field in Authentication Information Messages, which are informative and do not effect any response messaging, MAY be set to zero. The Identifier field in a CMTS's BPKM response Message MUST match the Identifier field of the BPKM Request Message the CMTS is responding to. The Identifier field in TEK Invalid Messages, which are not sent in response to BPKM requests, MUST be set to zero. The Identifier field in unsolicited Authorization Invalid Messages MUST be set to zero.

On reception of a BPKM response Message, the CPE associates the Message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization

Rejects, and Authorization Invalids; a particular TEK state machine in the case of Key Replies, Key Rejects and TEK Invalids; a particular SA Mapping state machine in the case of SA Map Replies and SA Map Rejects).

A CPE MAY keep track of the Identifier of its latest, pending Authorization Request. The CPE MAY silently discard Authorization Replies and Authorization Rejects whose Identifier fields do not match those of the pending requests.

A CPE MAY keep track of the Identifier of its latest, pending Key Request. The CPE MAY silently discard Key Replies and Key Rejects whose Identifier fields do not match those of the pending requests.

A CPE MAY keep track of the Identifier of its latest, pending SA Map Request. The CPE MAY silently discard SA Map Replies and SA Map Rejects whose Identifier fields do not match those of the pending requests.

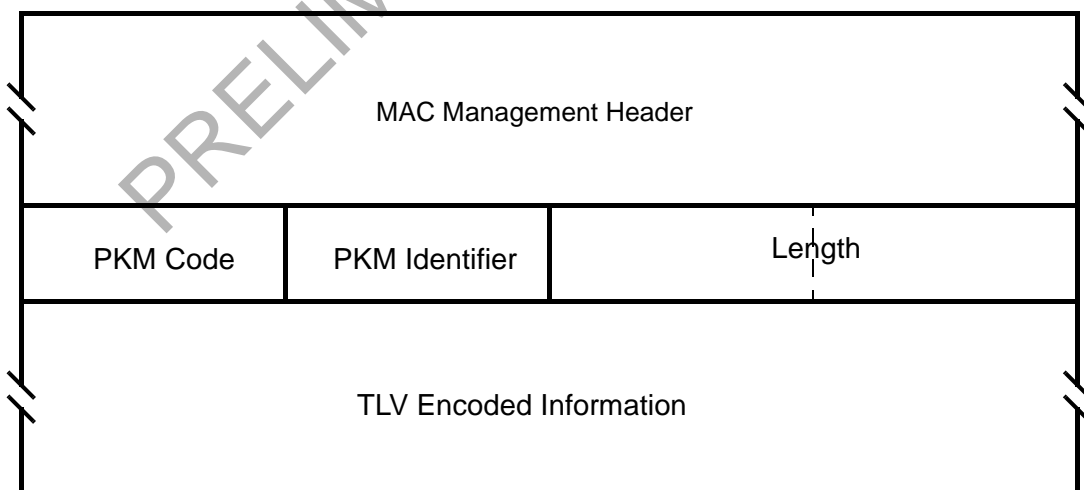
### Length

The Length field is two octets. It indicates the length of the Attribute fields in octets. The length field does not include the Code, Identifier and Length fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it SHOULD be silently discarded. The minimum length is 0 and maximum length is <TBD>.

All other parameters are encoded as TLV tuples as defined in Section 6.12.

### 6.2.11 Privacy Key Management — Response (PKM-RSP) Message

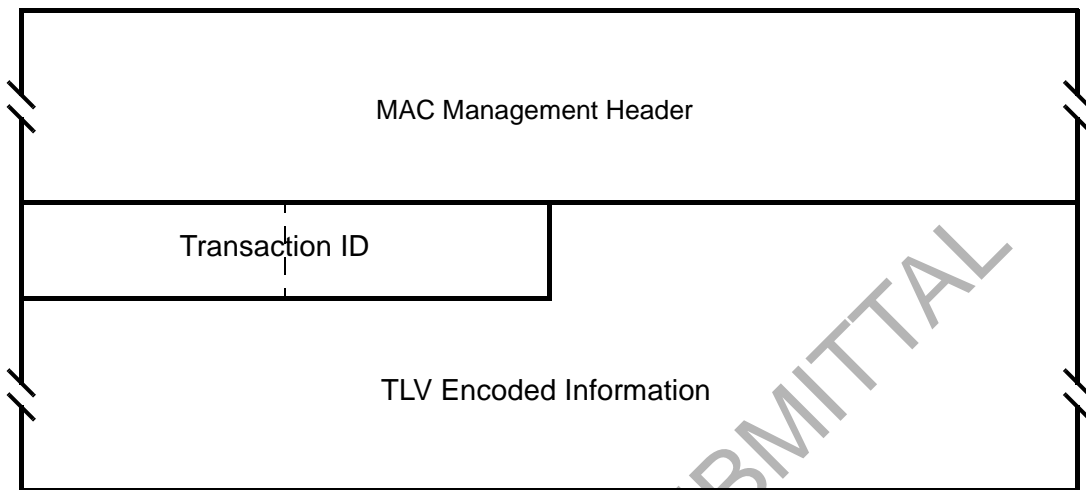
Privacy Key Management protocol Messages transmitted from the BS to the CPE shall use the form shown in Figure 25.



**Figure 25—PKM-RSP Message Format**

### 6.2.12 Dynamic Service Addition — Request (DSA-REQ) Message

A Dynamic Service Addition Request MAY be sent by a CPE or BS to create a new Service Flow.



**Figure 26—DSA-REQ Message Format**

A CPE or BS MUST generate DSA-REQ Messages in the form shown in Figure 26 including the following parameter:

#### **Transaction ID**

Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples as defined in Section 6.12. A DSA-REQ Message MUST NOT contain parameters for more than one Service Flow in each direction, i.e., a DSA-REQ Message MUST contain parameters for either a single uplink Service Flow, or for a single downlink Service Flow, or for one uplink and one downlink Service Flow.

The DSA-REQ Message MUST contain:

#### **Service Flow Parameters**

Specification of the Service Flow's traffic characteristics and scheduling requirements.

If Privacy is enabled, the DSA-REQ Message MUST contain:

#### **HMAC-Digest**

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12)

#### 6.2.12.1 CPE-Initiated Dynamic Service Addition

CPE-initiated DSA-Requests MUST use the Service Flow Reference to link Classifiers to Service Flows. Values of the Service Flow Reference are local to the DSA Message; each Service Flow within the DSA-Request MUST be assigned a unique Service Flow Reference. This value need not be unique with respect to the other service flows known by the sender.

CPE-initiated DSA-Requests MAY use the Service Class Name (refer to <TBD>) in place of some, or all, of the QoS Parameters.

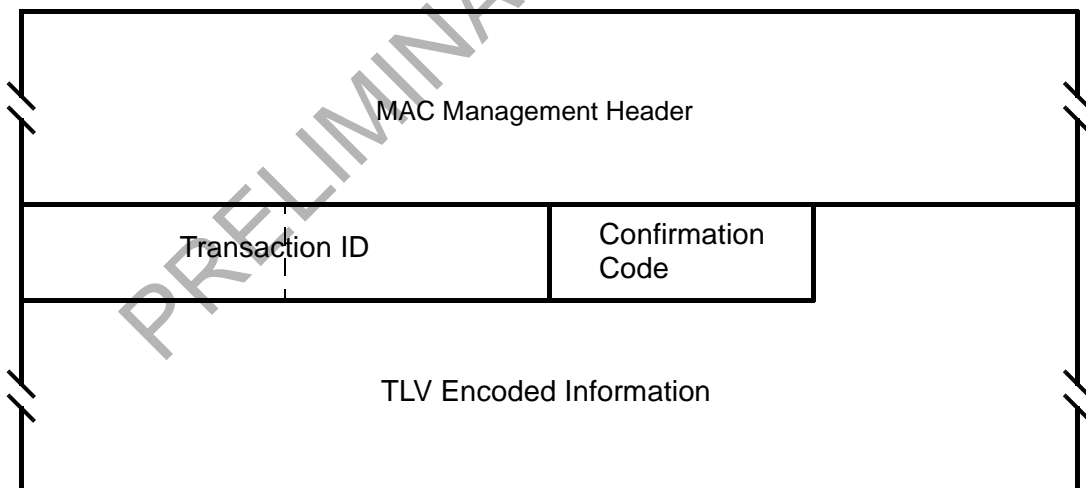
#### 6.2.12.2 BS-Initiated Dynamic Service Addition

BS-initiated DSA-Requests for Uplink Service Flows MUST also include a Connection ID. Connection Identifiers are unique within the MAC domain.

BS-initiated DSA-Requests for named Service Classes MUST include the QoS Parameter Set associated with that Service Class.

#### 6.2.13 Dynamic Service Addition — Response (DSA-RSP) Message

A Dynamic Service Addition Response shall be generated in response to a received DSA-Request. The format of a DSA-RSP MUST be as shown in Figure 27.



**Figure 27—DSA-RSP Message Format**

Parameters MUST be as follows:

**Transaction ID**

Transaction ID from corresponding DSA-REQ.

**Confirmation Code**

The appropriate Confirmation Code for the entire corresponding DSA-Request.

All other parameters are coded as TLV tuples as defined in Section 6.12.

If the transaction is successful, the DSA-RSP MAY contain the following:

**Service Flow Parameters**

The complete specification of the Service Flow MUST be included in the DSA-RSP only if it includes a newly assigned Connection Identifier or an expanded Service Class Name.

If the transaction is unsuccessful, the DSA-RSP MUST include:

**Service Flow Error Set**

A Service Flow Error Set and identifying Service Flow Reference/Identifier MUST be included for every failed Service Flow in the corresponding DSA-REQ Message. Every Service Flow Error Set MUST include every specific failed QoS Parameter of the corresponding Service Flow. This parameter MUST be omitted if the entire DSA-REQ is successful.

If Privacy is enabled, the DSA-RSP Message MUST contain:

**HMAC-Digest**

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Appendix <TBD>)

**6.2.13.1 CPE-Initiated Dynamic Service Addition**

The BS's DSA-Response for Service Flows that are successfully added MUST contain a Connection ID. The DSA-Response for successfully Admitted or Active uplink QoS Parameter Sets MUST also contain a Connection ID.

If the corresponding DSA-Request uses the Service Class Name (refer to <TBD>) to request service addition, a DSA-Response MUST contain the QoS Parameter Set associated with the named Service Class. If the Service Class Name is used in conjunction with other QoS Parameters in the DSA-Request, the BS MUST accept or reject the DSA-Request using the explicit QoS Parameters in the DSA-Request. If these Service Flow Encodings conflict with the Service Class attributes, the BS MUST use the DSA-Request values as overrides for those of the Service Class.

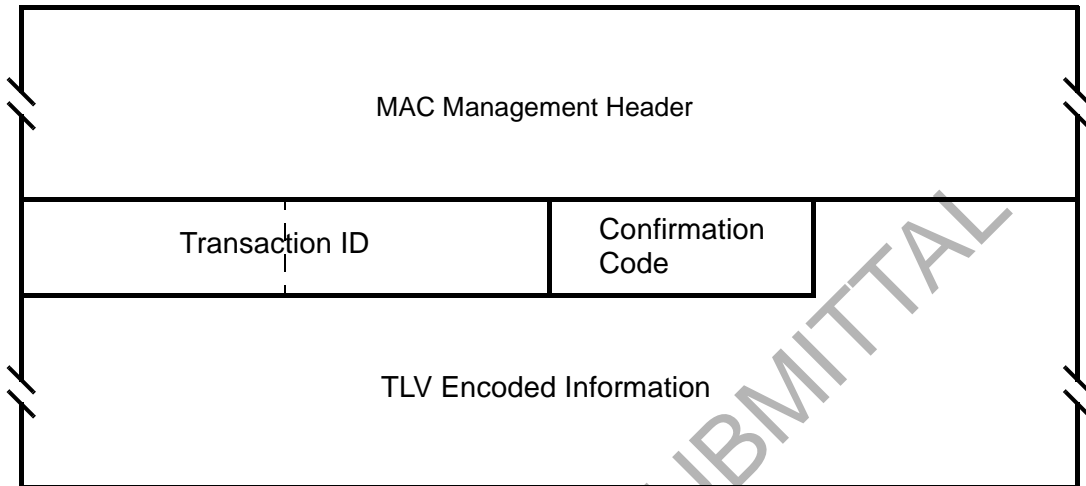
If the transaction is unsuccessful, the BS MUST use the original Service Flow Reference to identify the failed parameters in the DSA-RSP.

**6.2.13.2 BS-Initiated Dynamic Service Addition**

If the transaction is unsuccessful, the CPE MUST use the Connection Identifier to identify the failed parameters in the DSA-RSP.

### 6.2.14 Dynamic Service Addition — Acknowledge (DSA-ACK) Message

A Dynamic Service Addition Acknowledge MUST be generated in response to a received DSA-RSP. The format of a DSA-ACK MUST be as shown in Figure 28.



**Figure 28—DSA-ACK Message Format**

Parameters MUST be as follows:

#### Transaction ID

Transaction ID from corresponding DSA-Response.

#### Confirmation Code

The appropriate Confirmation Code (refer to <TBD>) for the entire corresponding DSA-Response.<sup>2</sup>

All other parameters are coded TLV tuples.

#### Service Flow Error Set

The Service Flow Error Set of the DSA-ACK Message encodes specifics of any failed Service Flows in the DSA-RSP Message. A Service Flow Error Set and identifying Service Flow Reference MUST be included for every failed QoS Parameter of every failed Service Flow in the corresponding DSA-REQ Message. This parameter MUST be omitted if the entire DSA-REQ is successful.

<sup>2</sup>The confirmation code is necessary particularly when a Service Class Name (refer to Section <TBD>) is used in the DSA-Request. In this case, the DSA-Response could contain Service Flow parameters that the CPE is unable to support (either temporarily or as configured).



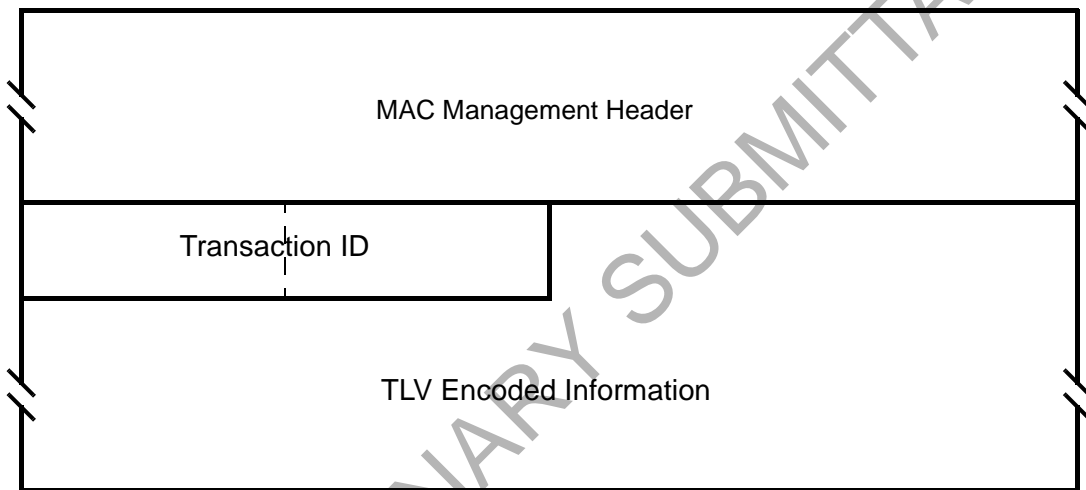
If Privacy is enabled, the DSA-ACK Message MUST contain:

#### HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Appendix <TBD>)

### 6.2.15 Dynamic Service Change — Request (DSC-REQ) Message

A Dynamic Service Change Request MAY be sent by a CPE or BS to dynamically change the parameters of an existing Service Flow.



**Figure 29—DSC-REQ Message Format**

A CPE or BS MUST generate DSC-REQ Messages in the form shown in Figure 29 including the following parameters:

#### Transaction ID

Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples as defined in Section 6.12. A DSC-REQ Message MUST NOT carry parameters for more than one Service Flow in each direction, i.e., a DSC-REQ Message MUST contain parameters for either a single uplink Service Flow, or for a single downlink Service Flow, or for one uplink and one downlink Service Flow. A DSC-REQ MUST contain the following:

#### Service Flow Parameters

Specification of the Service Flow's new traffic characteristics and scheduling requirements. The Admitted and Active Quality of Service Parameter Sets currently in use by the Service Flow. If the DSC Message is successful and it contains Service Flow parameters, but does not contain replacement sets for both Admitted and Active Quality of Service Parameter Sets, the omitted set(s) MUST be set to null. If included, the Service Flow Parameters MUST contain a Service Flow Identifier.

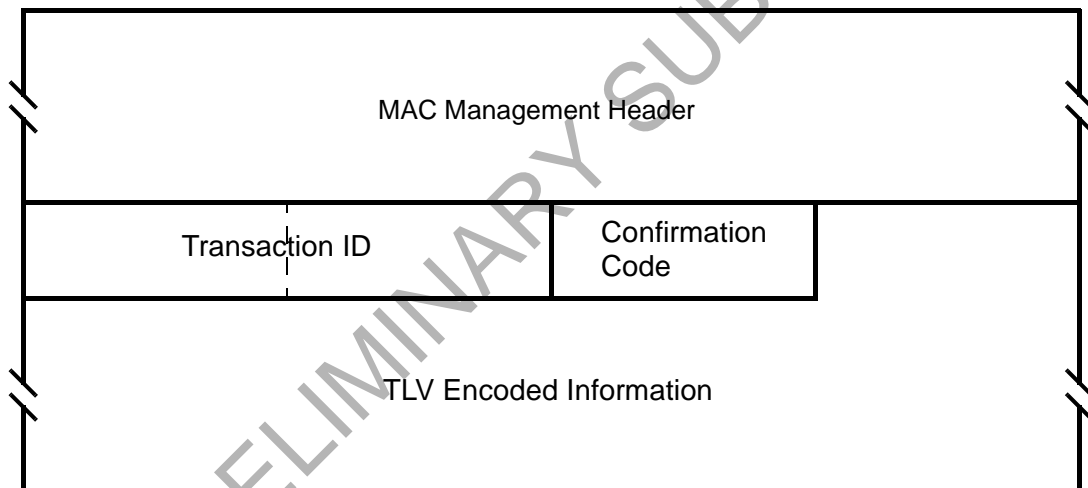
If Privacy is enabled, a DSC-REQ MUST also contain:

#### HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to <TBD>)

### 6.2.16 Dynamic Service Change — Response (DSC-RSP) Message

A Dynamic Service Change Response MUST be generated in response to a received DSC-REQ. The format of a DSC-RSP MUST be as shown in Figure 30.



**Figure 30—DSC-RSP Message Format**

Parameters MUST be as follows:

#### Transaction ID

Transaction ID from corresponding DSC-REQ

#### Confirmation Code

The appropriate Confirmation Code (refer to <TBD>) for the corresponding DSC-Request.

All other parameters are coded as TLV tuples as defined in Section 6.12.

If the transaction is successful, the DSC-RSP MAY contain the following:

#### **Service Flow Parameters**

The complete specification of the Service Flow MUST be included in the DSC-RSP only if it includes a newly assigned Connection Identifier or an expanded Service Class Name. If a Service Flow Parameter set contained an uplink Admitted QoS Parameter Set and this Service Flow does not have an associated CID, the DSC-RSP MUST include a CID. If a Service Flow Parameter set contained a Service Class Name and an Admitted QoS Parameter Set, the DSC-RSP MUST include the QoS Parameter Set corresponding to the named Service Class. If specific QoS Parameters were also included in the Classed Service Flow request, these QoS Parameters MUST be included in the DSC-RSP instead of any QoS Parameters of the same type of the named Service Class.

If the transaction is unsuccessful, the DSC-RSP MUST contain the following:

#### **Service Flow Error Set**

A Service Flow Error Set and identifying Connection ID MUST be included for every failed Service Flow in the corresponding DSC-REQ Message. Every Service Flow Error Set MUST include every specific failed QoS Parameter of the corresponding Service Flow. This parameter MUST be omitted if the entire DSC-REQ is successful.

Regardless of success or failure, if Privacy is enabled for the CPE the DSC-RSP MUST contain:

#### **HMAC-Digest**

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to <TBD>)

### **6.2.17 Dynamic Service Change — Acknowledge (DSC-ACK) Message**

A Dynamic Service Change Acknowledge MUST be generated in response to a received DSC-RSP. The format of a DSC-ACK MUST be as shown in Figure 31.

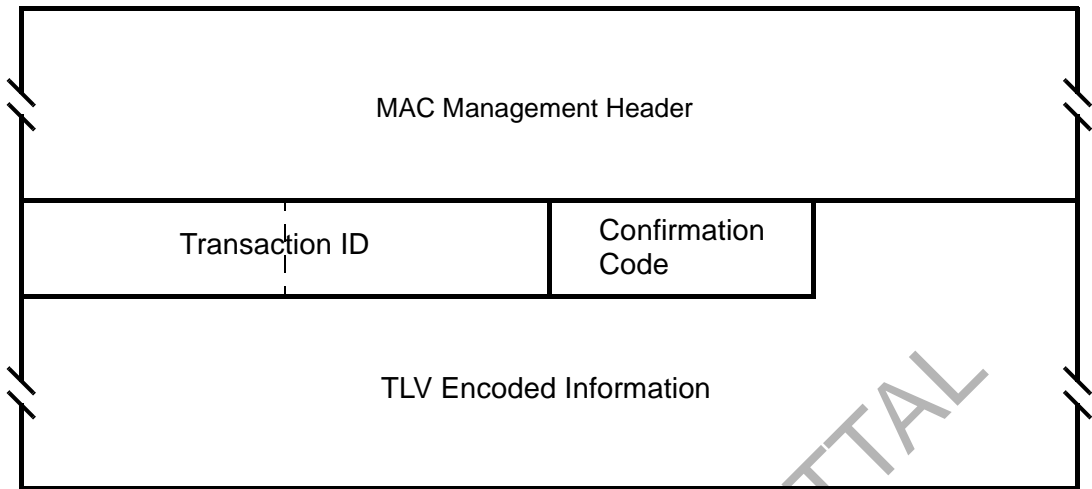


Figure 31—DSC-ACK Message Format

Parameters MUST be as follows:

**Transaction ID**

Transaction ID from the corresponding DSC-REQ

**Confirmation Code**

The appropriate Confirmation Code (refer to <TBD>) for the entire corresponding DSC-Response.

All other parameters are coded TLV tuples.

**Service Flow Error Set**

The Service Flow Error Set of the DSC-ACK Message encodes specifics of any failed Service Flows in the DSC-RSP Message. A Service Flow Error Set and identifying Service Flow Identifier MUST be included for every failed QoS Parameter of each failed Service Flow in the corresponding DSC-RSP Message. This parameter MUST be omitted if the entire DSC-RSP is successful.

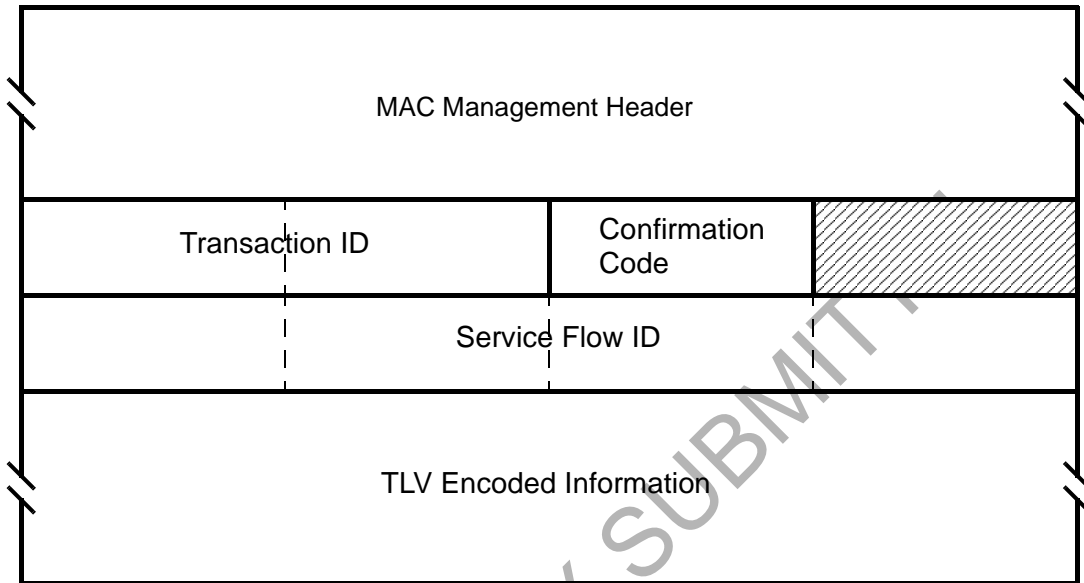
If Privacy is enabled, the DSC-ACK Message MUST contain:

**HMAC-Digest**

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message’s Attribute list. (Refer to <TBD>)

### 6.2.18 Dynamic Service Deletion — Request (DSD-REQ) Message

A DSD-Request MAY be sent by a CPE or BS to delete an existing Service Flow. The format of a DSD-Request MUST be as shown in Figure 32.



**Figure 32—DSD-REQ Message Format**

Parameters MUST be as follows:

#### **Service Flow Identifier**

The SFID to be deleted.

#### **Transaction ID**

Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples as defined in Section 6.12.

If Privacy is enabled, the DSD-REQ MUST include:

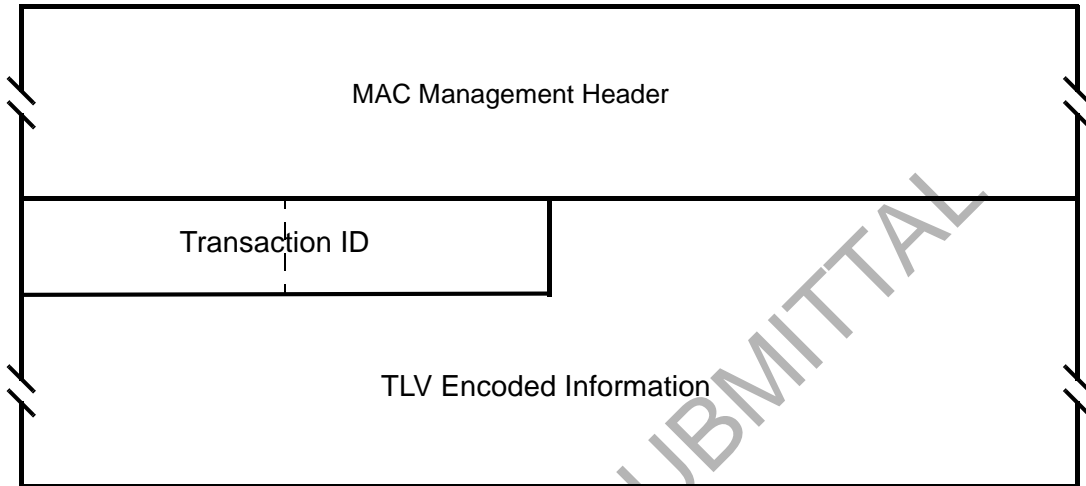
#### **HMAC-Digest**

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Appendix <TBD>)

#### **Service Flow Reference**

### 6.2.19 Multicast Polling Assignment Request (MCA-REQ) Message

The Multicast Polling Assignment message is sent to a CPE to include it in a multicast polling group. This message is normally sent on a CPE's basic connection ID. It may also be sent to a group of CPE's on a previously set up multicast connection ID. This shall be followed by a Packet PDU in the format shown in Figure 33.



**Figure 33—Multicast Polling Assignment Request (MCA-REQ) Message Format**

Parameters shall be as follows:

#### Transaction ID

Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples.

#### Multicast Connection Identifier

The CID to which the CPE is either added or removed.

#### Assignment

0x00 = Leave multicast group

0x01 = Join multicast group

#### 6.2.19.1 MCA-REQ TLV Encodings

The type values used MUST be those defined in Table 9. These are unique within the ranging request Message but not across the entire MAC Message set. The type and length fields MUST each be 1 octet in length.

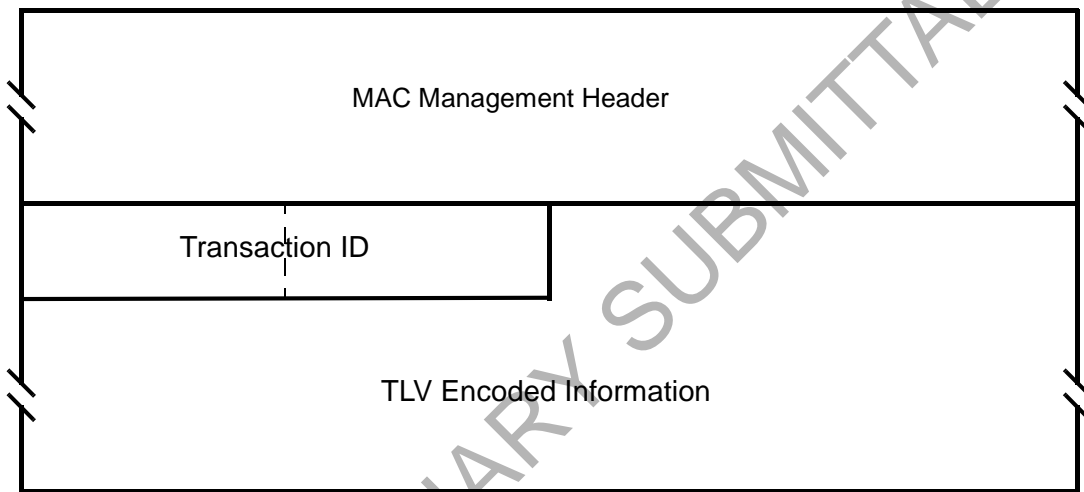
### 6.2.20 Multicast Polling Assignment Response (MCA-RSP) Message

The Multicast Polling Assignment message is sent to a CPE to include it in a multicast polling group. This message is normally sent on a CPE's basic connection ID. It may also be sent to a group of CPE's on a pre-

**Table 9—Multicast Assignment Request Message Encodings**

Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Multicast CID	1	2	
Assign- ment	2	1	0x00 = Leave multicast group 0x01 = Join multicast group
Reserved	2-255	n	Reserved for future use

viously set up multicast connection ID. This shall be followed by a Packet PDU in the format shown in Figure 34.

**Figure 34—Multicast Polling Assignment Response (MCA-RSP) Message Format**

Parameters shall be as follows:

#### **Transaction ID**

Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples.

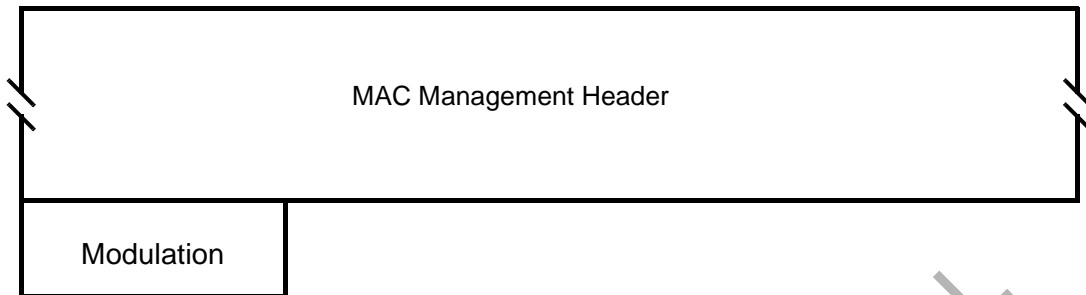
#### **Confirmation Code**

- 0 (okay)
- 1 (request failed)

### **6.2.21 Downlink Modulation Change Request (DMC-REQ) Message**

The Downlink Modulation Change Request message is sent by the CPE to the BS on the CPE's basic connection ID. Normally, it is sent at the current operational modulation for the CPE. If the CPE has been inac-

tive on its uplink for some period of time and detects fading on the downlink, the CPE uses this message to request to go to a more robust (lower bits per symbol) modulation. In this case, the message is sent using QPSK modulation to increase the likelihood of reception by the CPE. Since the CPE may not have been allocated any uplink bandwidth, the CPE uses contention slots. This shall be followed by a Packet PDU in the format shown in Figure 35.



**Figure 35—Downlink Modulation Change Request (DMC-REQ) Message Format**

Parameters shall be as follows:

**Modulation**

0x00 = QPSK  
 0x01 = 16-QAM  
 0x02 = 64-QAM



## 6.3 Framing and Scheduling Intervals

The MAC is able to support both a framed and non-framed physical layer. For a framed PHY layer, the MAC aligns its scheduling intervals with the underlying PHY layer framing. For an unframed PHY layer, the scheduling intervals are chosen by the MAC to optimize system performance.

A frame is a fixed duration of time, which contains both transmit and receive intervals. The relationship between upstream and downstream transmission intervals is fixed within the frame, and are both defined relative to the BS internal timing. The TDD, Burst FDD and FSDD modes of operation use a framed PHY layer. The Continuous FDD mode of operation has no explicit PHY layer framing. Instead, the upstream and downstream transmission timings are linked via the Upstream TimeStamp within the DS-MAP and the US-MAP messages.

### 6.3.1 PHY Burst Mode Support

In the burst mode, the uplink and downlink can be multiplexed in a TDD fashion as described in Section 6.3.1.1 or in an FDD fashion as described in Section 6.3.1.2. Each uses a frame with a duration of 1 millisecond. Within this frame are a downlink subframe and an uplink subframe. In the TDD case, the downlink subframe comes first, followed by the uplink subframe. In the burst FDD case, the downlink and uplink subframes occur simultaneously on their respective frequencies, and occupy the whole 1 millisecond frame. In both cases, the downlink subframe is prefixed with information necessary for frame synchronization.

To aid periodic functions, multiple frames are grouped into multiframes and multiple multiframes are grouped into hyperframes. There are 16 frames per multiframe and 32 multiframes per hyperframe. Frame numbers have the values of 0 to 15, multiframe numbers are 0 to 31, while Hyperframe numbers are from 0 to 32767. Each will roll over to zero after they reach their maximum value. Since frames are 1 millisecond in duration, 1 multiframe is 16 milliseconds in duration and 1 hyperframe is 512 milliseconds in duration.

The available bandwidth in both directions is allocated with a granularity of one PHY slot (PS), which has a length of 4 modulation symbols each. The number of PHY slots with each 1 mSec frame is a function of the modulation rate. The modulation rate is selected in order to obtain an integral number of PS within each frame. With a 20 Mbaud modulation rate, there are 5000 PHY slots within each 1 msec. frame.

#### 6.3.1.1 TDD Operation

In this mode of operation the downlink and uplink are on the same carrier frequency. The uplink and downlink share the same frequency in a TDM fashion. As shown in Figure 36, a TDD frame has a 1 millisecond duration and contains N PHY slots, with varying with the modulation rate. The TDD framing is adaptive in that the number of PS allocated to downlink versus uplink can vary. The split between uplink and downlink is a system parameter and is controlled at higher layers within the system.

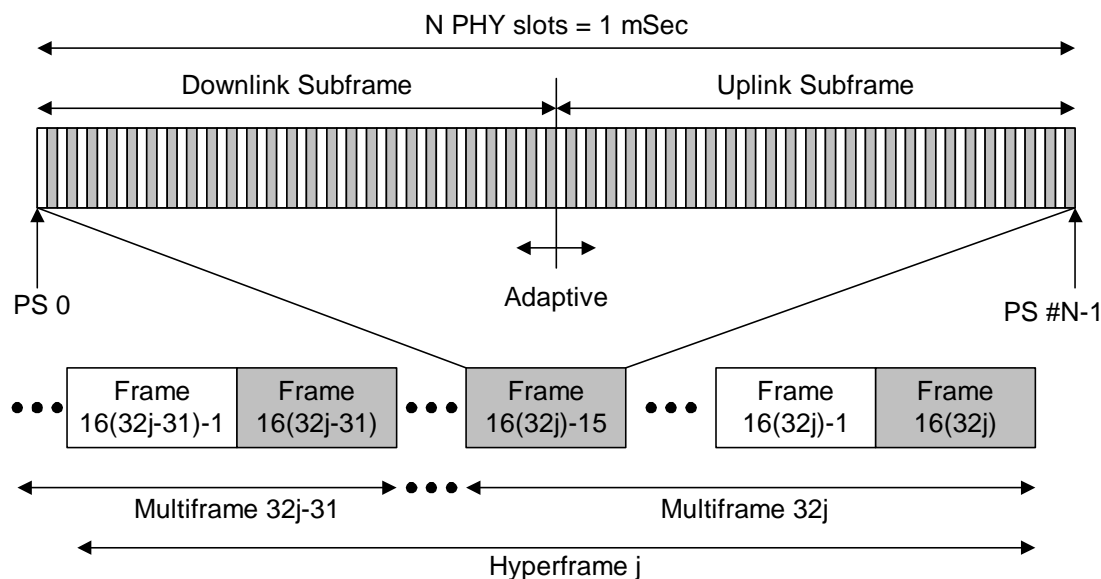


Figure 36—TDD and Multiframe Structure

It is recommended that frame numbering in a TDD system be synchronized with Universal Time. The frame, multiframe, and hyperframe are defined to be all 0 at Julian Date 2451179.0 (noon Jan. 0, 1990). The frame, multiframe, and hyperframe return to all 0 with a period of 16777216 milliseconds which equals 4 hours 39 minutes 37 seconds 216 milliseconds. Load leveling requires that the frame number be synchronized on all channels within a sector.

The base station MAC must be provided with time, in some form, which is synchronized to some universal synchronization signal with at least 1 millisecond accuracy.

### 6.3.1.2 Burst FDD and FSDD Operation

In this mode of operation the downstream and upstream are using 2 different carrier frequencies. Both carriers are equal in channel bandwidth and instantaneous baud rate. The frequency separation between carriers is set either according to the target spectrum regulations or to some value sufficient for complying with radio channel transmit/receive isolation and desensitization requirements. In the time domain both upstream and downstream are frame synchronized at the BS. Figure 37 describes the basics of the FDD and FSDD based operation.

A subscriber capable of full duplex FDD operation, meaning it is capable of transmitting and receiving at the same instant, imposes no restriction on the base station controller regarding its upstream bandwidth allocation management. On the other hand, a subscriber that is limited to half duplex FDD operation imposes a restriction on such a controller to not allocate upstream bandwidth for the subscriber during a time when the subscriber must also be receiving. It is mandatory that both types of subscribers could co-exist in a FDD deployment, meaning that radio channels could address both type of subscribers within the each frame.

At the beginning of each frame, only those users that are capable of full FDD operation can transmit during the time when the BS is broadcasting the Downstream MAP and Upstream MAP messages. The subscribers that are restricted to FSDD operation must wait until the broadcast messages are finished before transmitting anything on the upstream.

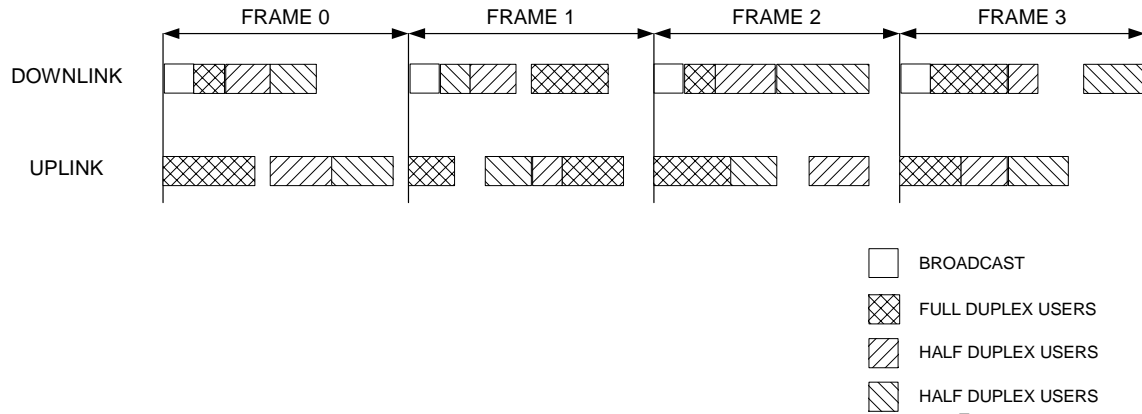


Figure 37—Burst Downstream FDD/FSDD Mapping

### 6.3.2 PHY Continuous Mode Support

#### 6.3.2.1 Continuous FDD Operation

In continuous FDD operation, the upstream and downstream signals have no defined framing, and they operate on separate frequencies, which allows all subscribers to transmit on the upstream independently of what is being transmitted on the downstream signal.

The BS periodically transmits synchronization and upstream MAP messages, which are used to synchronize the upstream burst transmissions with the downstream. The structure of the upstream is defined by the US-MAP message, and can change according to the needs of the system.

#### 6.3.3 Downlink Burst Subframe Structure

The downlink subframe defined here only applies to the burst modes (TDD, Burst FDD and FSDD).

The structure of the downlink subframe used by the BS to transmit to the CPEs has two optional forms as shown in Figure 39 and Figure 39. In both cases it starts with a Frame Control Header, which is always transmitted in QAM-4. This frame header contains a preamble used by the PHY for synchronization and equalization. It also contains control sections for both the PHY and the MAC. Preambles are not RS coded, but all other downlink traffic is FEC coded. The length of the preamble in the Frame Control Header is 24 QAM symbols.

In TDD systems, transmissions on the downlink for each frame are multiplexed sequentially into one continuous burst. The transmission is sorted by modulation with a map of the modulation changes in the PHY Control portion of the Frame Control Header. They may optionally be sorted by CPE. There is a Tx/Rx Transmission Gap (TRTG) separating the downlink subframe from the uplink subframe. This structure is shown in Figure 38. Note that any one or more of the 3 differently modulated data blocks may be absent.

Burst FDD systems may use the same structure with the restriction that each half duplex user must receive in the frame any downlink data directed to it before the user can transmit any uplink packets. If most users are full duplex, this restriction is minor.

Alternatively, if a burst FDD system contains many half duplex users, the preferred form is to generate the downlink subframe in a TDMA fashion. The downlink data destined to each individual CPE is grouped into

one (preferable) or more bursts, each starting with a short (e.g., 12 symbols) preamble. In this case, the PHY Control portion of the Frame Control Header contains a map of the bursts. This option allows FSDD users to receive or transmit in any portion of the frame as long as the bandwidth allocation preserves their half duplex nature. This allows for greater statistical multiplexing of FSDD users at the expense of bandwidth for the preambles and a more complex downlink map. This structure is shown in Figure 39.

The available bandwidth in both directions is allocated with a granularity of one PHY slot (PS), which has a length of 4 modulation symbols each. The number of PHY slots with each 1 mSec frame is a function of the modulation rate. The modulation rate is selected in order to obtain an integral number of PS within each frame. With a 20 Mbaud modulation rate, there are 5000 PHY slots within each 1 msec. frame.

EDITOR The Frame Control Header also may periodically contain a PHY Parameters section which contains system parameters which can vary from system to system rather than being well known. These include uplink preamble size, shortened downlink preamble size (FDD/TDMA systems), etc.

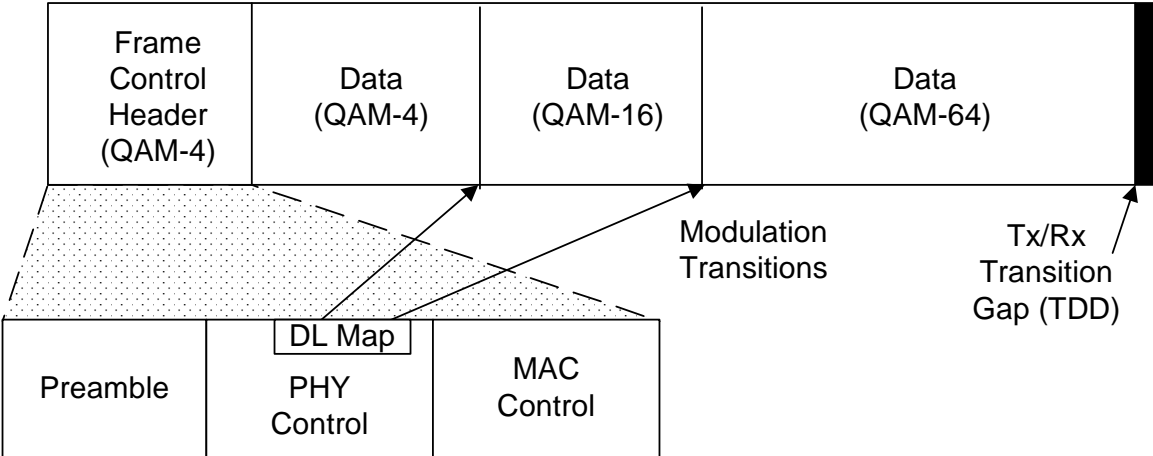
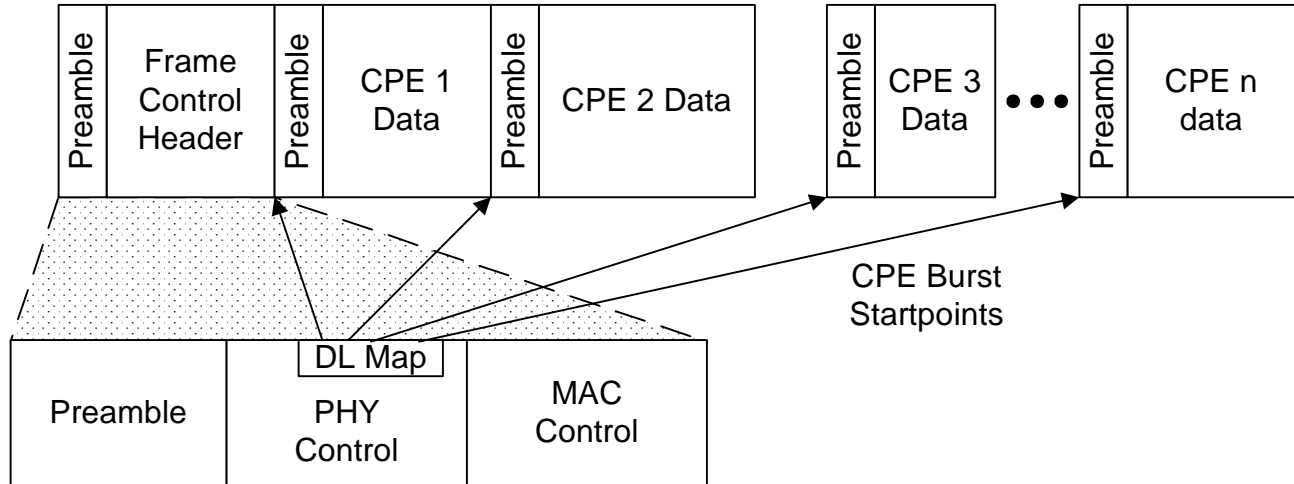


Figure 38—TDD and Burst FDD/TDM Downstream Subframe Structure



**Figure 39—Burst FDD/TDMA Downstream Subframe Structure**

#### 6.3.3.1 PHY Control

The PHY Control portion of the downlink subframe is used for physical information destined for all CPEs. The PHY Control information is FEC encoded, but is not encrypted. The information transmitted in this section is always transmitted in QAM-4 and includes:

- a) Broadcast physical layer information (PCD)
- b) DS-MAP
- c) Frame/multiframe/hyperframe numbering or BS Upstream TimeStamp

#### 6.3.3.2 MAC Control

The MAC Control portion of the downlink subframe is used for MAC messages destined for multiple CPEs. For information directed at an individual CPE, MAC messages are transmitted in the established control connection at the operating modulation of the CPE to minimize bandwidth usage. The MAC Control messages are FEC encoded, but are not encrypted. The information transmitted in this section is always transmitted in QAM-4 and includes:

- a) MAC Version Identifier
- b) Uplink Map (CPE/mini-slot/start symbol triplets)
- c) Whether any bandwidth request contention periods (see Section TBD) are included in the frame (in US-MAP)
- d) Starting point and length of bandwidth request contention period, if any (in US-MAP)
- e) Whether registration is allowed on this physical channel
- f) Whether a registration contention period is included the frame (in US-MAP)
- g) Starting point and length of registration contention period, if any (in US-MAP)

### 6.3.3.3 Downlink Data

The downlink data sections are used for transmitting data and control messages to the specific CPEs. This data is always FEC coded and is transmitted at the current operating modulation of the individual CPE. Message headers are sent unencrypted. Payloads of user data connections are encrypted. Payloads of MAC control connections are not encrypted. In the burst mode cases, data is transmitted in modulation order QAM-4, followed by QAM-16, followed by QAM-64. The PHY Control portion of the Frame Control Header contains a map stating the PS and symbol at which modulation will change. In the TDMA case, the data is grouped into CPE specific bursts, which do not need to be in modulation order.

If the downlink data does not fill the entire downlink subframe, the transmitter is shut-down.

### 6.3.4 Uplink Burst Subframe Structure

The structure of the uplink subframe used by the CPEs to transmit to the BS is shown in Figure 40. There are three main classes of MAC/TC messages transmitted by the CPEs during the uplink frame:

- Those that are transmitted in contention slots reserved for station registration.
- Those that are transmitted in contention slots reserved for response to multicast and broadcast polls for bandwidth needs.
- Those that are transmitted in bandwidth specifically allocated to individual

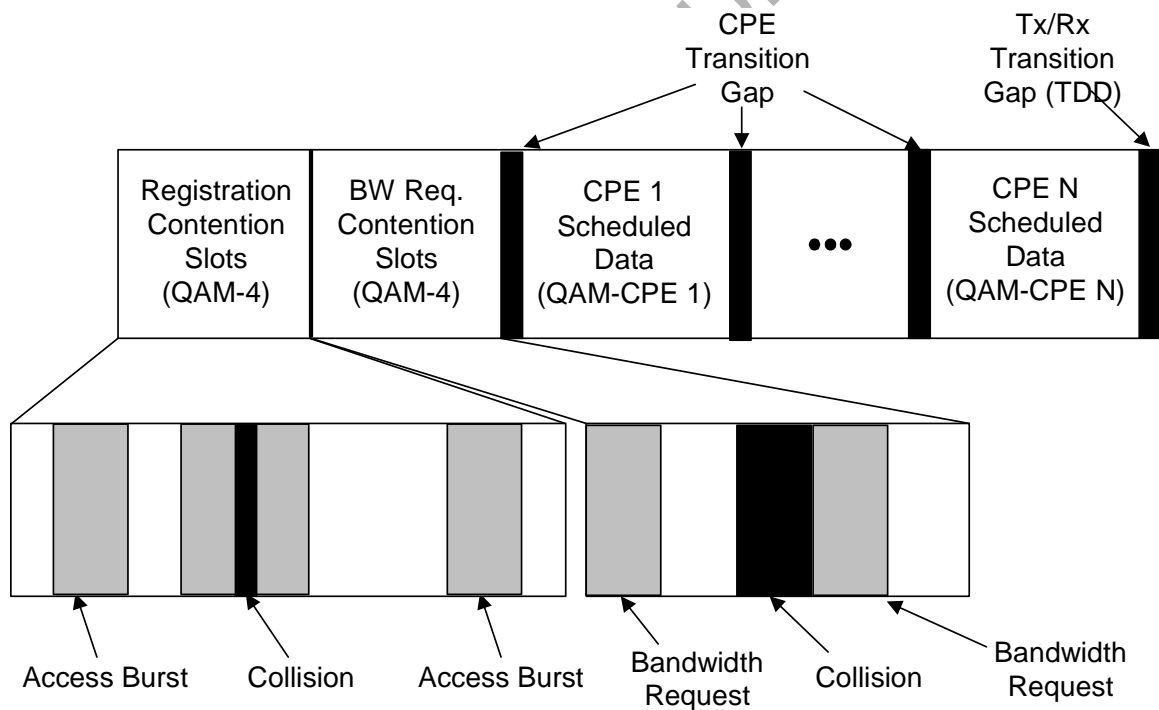


Figure 40—Uplink Subframe Structure

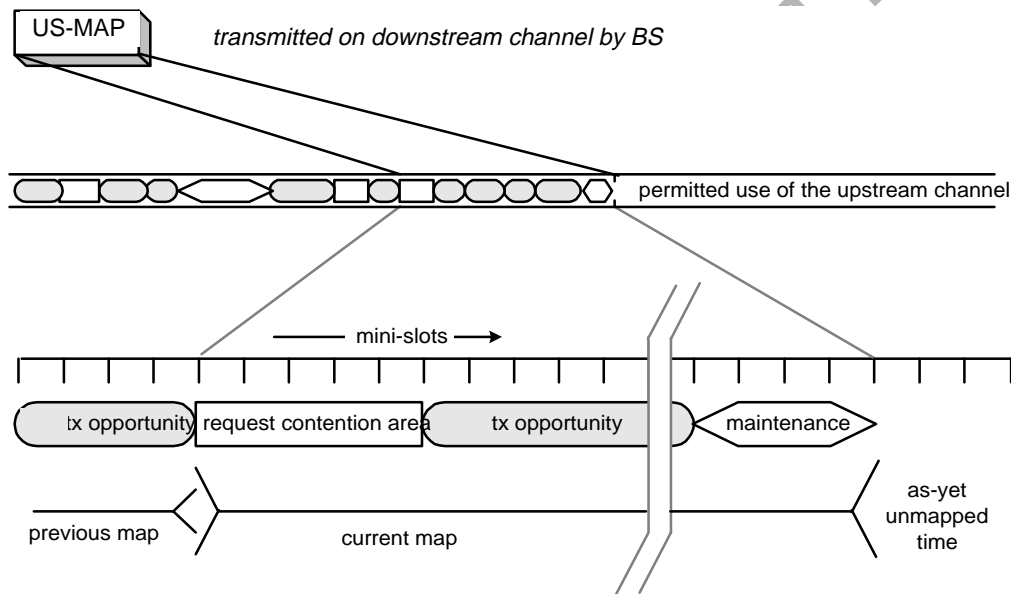
#### 6.3.4.1 Upstream Burst Mode Modulation

Adaptive modulation is used in the upstream, in which different users are assigned different modulation types by the base station.

In the adaptive case, the bandwidth allocated for registration and request contention slots is grouped together and is always used with QAM-4 modulation. The remaining transmission slots are grouped by CPE. During its scheduled bandwidth, a CPE transmits with the modulation specified by the base station, as determined by the effects of distance and environmental factors on transmission to and from that CPE. CPE Transition Gaps (CTG) separate the transmissions of the various CPEs during the uplink subframe. The CTGs contain a gap to allow for ramping down of the previous burst, followed by a preamble the BS to synchronize to the new CPE. The preamble and gap lengths are broadcast periodically by the base station in the Frame Control Header.

### 6.3.5 Continuous Downstream and Upstream Structure

In the continuous PHY mode, the BS periodically broadcasts the Upstream MAP message (US-MAP) on the downstream, which defines the permitted usage of each upstream mini-slot within the time interval covered by that MAP message (see Figure 41). The timing of the upstream bursts are based upon a downstream synchronization message (DS-SYNC). The US-MAP messages are transmitted approximately 250 times a second, but this can vary to optimise the system's operation.



**Figure 41—Continuous Downstream FDD Mapping**

### 6.3.6 Upstream Map

Whether in the Burst or Continuous PHY modes, the upstream MAP message (US-MAP) defines the usage for the upstream PS intervals. The US-MAP consists of a series of Information Elements (IE), which define the usage of each interval. The US-MAP defines the upstream usage in terms of the starting offset in numbers of mini-slots, which are defined below.

Each IE consists of a 16-bit Connection ID, a 4-bit type code, and a 12-bit starting mini-slot offset as defined in Section 6.2.4. Since all CPE must scan all IE within each MAP, it is critical that IEs be short and relatively fixed format. IEs within the MAP are strictly ordered by starting offset. For most purposes, the duration described by the IE is inferred by the difference between the IE's starting offset and that of the following IE. For this reason, a Null IE MUST terminate the list.

### 6.3.6.1 Upstream Timing

The upstream timing is based on the Upstream Time Stamp reference, which is a 29-bit counter that increments at a rate that is 4 times the modulation rate. It therefore has a resolution that equals 1/4th of the modulation symbol period. This allows the SS to track the BS clock with a small time offset.

The BS maintains a separate Upstream Time Stamp for each upstream at the base station. The value of the BS Upstream Time Stamp is broadcast to all the CPE using the Physical Channel Descriptor (PCD) message. Each SS maintains its own Upstream Time Stamp so that it is synchronous with the BS Time stamp for the upstream channel that it is using. The SS Time Stamp must change at the same rate as its BS counterpart, but will be offset so that the upstream bursts arrive at the BS at the correct time. This offset is set by the BS using the RNG-RSP message.

#### 6.3.6.1.1 Continuous Mode Upstream Timing

The downstream MAP message (DS-MAP) in the continuous PHY mode broadcasts the Upstream Time Stamp value to all CPE. The Upstream Time Stamp from the BS is then used to adjust the SS internal Time Stamp so that it tracks the BS timing. The SS Time Stamp is offset from the BS Time Stamp by the Timing Adjustment amount sent to each CPE in the RNG-RSP message. The offset causes the upstream bursts arrive at the BS at the proper time. After either the BS or SS Time Stamps reach the maximum value of  $2^{29}-1$ , they roll over to zero and continue to count.

#### 6.3.6.1.2 Burst Mode Upstream Timing

In the burst PHY modes, at the start of each 1 mSec frame the Upstream Time Stamp counter in the BS is reset to zero, while in the SS it is reset using the current Timing Adjustment value as sent from the BS using the RNG-RSP message. Thus, the SS Time Stamp will be offset from the BS Time Stamp so that the upstream bursts arrive at the BS at the proper time.

### 6.3.6.2 Upstream Mini-Slot Definition

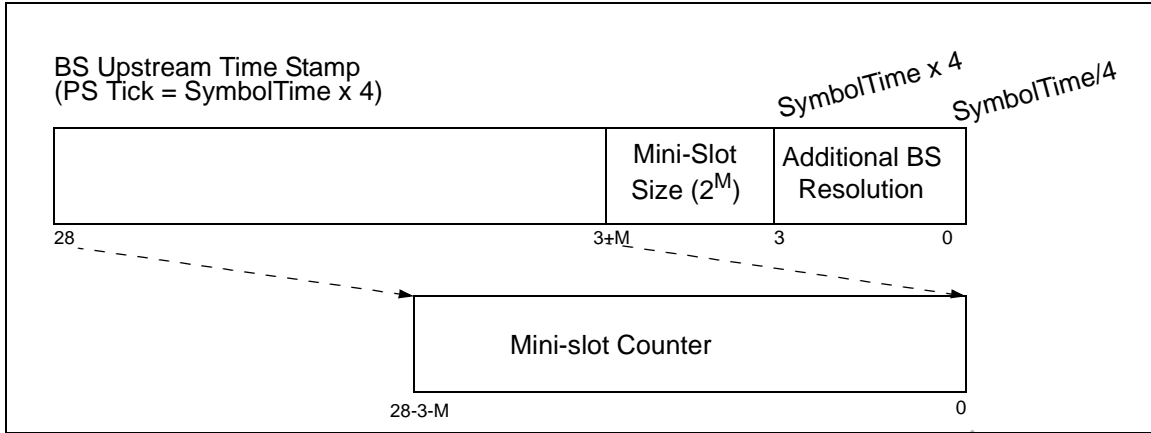
The upstream bandwidth allocation MAP (US-MAP) uses time units of “mini-slots.” The size of the mini-slot ( $N$ ) is specified as a number of PHY slots (PS) and is carried in the Physical Channel Descriptor for each upstream channel. One mini-slot contains  $N$  PHY slots (PS), where  $N = 2^m$  (where  $m = 0..7$ ). Since each PS contains 4 modulation symbols, the number of modulation symbols contained in one mini-slot equals  $4N$ .

Practical mini-slots are expected to represent relatively few PS to allow efficient bandwidth utilization with respect to the mini-slot size. Larger mini-slot sizes allow the BS to define large contention intervals (up to  $2^{12}-1$  or 4095 mini-slots) using the current US-MAP. Note that the modulation level and hence the symbols/byte is a characteristic of an individual burst transmission, not of the channel.

A “mini-slot” is the unit of granularity for upstream transmission allocations. There is no implication that any PDU can actually be transmitted in a single mini-slot.

Figure 42 illustrates the mapping of the Upstream Time Stamp maintained in the BS to the BS Mini-slot Counter.





**Figure 42—BS System and Mini-slot Clocks**

The BS and SS base the upstream allocations on a 29-bit counter that normally counts to  $(2^{29} - 1)$  and then wraps back to zero. The bits (i.e., bit 0 to bit 28-3-M) of the mini-slot counter **MUST** match the most-significant bits (i.e., bit 3+M to bit 28) of the DS-MAP timestamp counter. That is, mini-slot N begins at timestamp value  $(N \cdot T \cdot 16)$ , where  $T = 2^M$  is the PCD multiplier that defines the mini-slot size (i.e., the number of PS per mini-slot).

The constraint that the PCD multiplier be a power of two has the consequence that the number of PS per mini-slot must also be a power of two.

### 6.3.6.3 Upstream Interval Definition

All of the Information Elements defined below shall be supported by conformant CPEs. Conformant BS **MAY** use any of these Information Elements when creating a US-MAP message.

#### 6.3.6.3.1 The Request IE

The Request IE provides an upstream interval in which requests **MAY** be made for bandwidth for upstream data transmission. The character of this IE changes depending on the class of Service ID. If broadcast, this is an invitation for CPEs to contend for requests. Section TBD describes which contention transmit opportunity may be used. If unicast, this is an invitation for a particular CPE to request bandwidth. Unicasts **MAY** be used as part of a Quality of Service scheduling scheme (refer to Section TBD). Packets transmitted in this interval **MUST** use the Request MAC Frame format (refer to Section TBD).

A small number of Priority Request SIDs are defined in TBD. These allow contention for Request IEs to be limited to service flows of a given Traffic Priority (refer to Section TBD).

#### 6.3.6.3.2 The Initial Maintenance IE

The Initial Maintenance IE provides an interval in which new stations may join the network. A long interval, equivalent to the maximum round-trip propagation delay plus the transmission time of the Ranging Request (RNG-REQ) message (see Section TBD), **MUST** be provided in some US-MAPs to allow new stations to perform initial ranging. Packets transmitted in this interval **MUST** use the RNG-REQ MAC Management message format (refer to Section TBD).

### 6.3.6.3.3 The Station Maintenance IE

The Station Maintenance IE provides an interval in which stations are expected to perform some aspect of routine network maintenance, such as ranging or power adjustment. The BS MAY request that a particular CPE perform some task related to network maintenance, such as periodic transmit power adjustment. In this case, the Station Maintenance IE is unicast to provide upstream bandwidth in which to perform this task. Packets transmitted in this interval MUST use the RNG-REQ MAC Management message format (see Section TBD).

### 6.3.6.3.4 Short and Long Data Grant IEs

The Short and Long Data Grant IEs provide an opportunity for a CPE to transmit one or more upstream PDUs. These IEs are issued either in response to a request from a station, or because of an administrative policy providing some amount of bandwidth to a particular station (see class-of-service discussion in Section TBD). These IEs MAY also be used with an inferred length of zero mini slots (a zero length grant), to indicate that a request has been received and is pending (a Data Grant Pending).

Short Data Grants are used with intervals less than or equal to the maximum burst size for this usage specified in the Upstream Channel Descriptor. If Short Data burst profiles are defined in the UCD, then all Long Data Grants MUST be for a larger number of mini-slots than the maximum for Short Data. The distinction between Long and Short Data Grants may be exploited in physical-layer forward-error-correction coding; otherwise, it is not meaningful to the bandwidth allocation process.

If this IE is a Data Grant Pending (a zero length grant), it MUST follow the NULL IE. This allows CPE modems to process all actual allocations first, before scanning the Map for data grants pending and data acknowledgments.

### 6.3.6.3.5 Data Acknowledge IE

The Data Acknowledge IE acknowledges that a data PDU was received. The CPE MUST have requested this acknowledgment within the data PDU (normally this would be done for PDUs transmitted within a contention interval in order to detect collisions).

The Data Acknowledge IE MUST follow the NULL IE. This allows CPE modems to process all actual interval allocations first, before scanning the Map for data grants pending and data acknowledgments.

### 6.3.6.3.6 Expansion IE

The Expansion IE provides for extensibility, if more than 16 code points or 32 bits are needed for future IEs.

### 6.3.6.3.7 Null IE

A Null IE terminates all actual allocations in the IE list. It is used to infer a length for the last interval. All Data Acknowledge IEs and All Data Grant Pending IEs (Data Grants with an inferred length of 0) must follow the Null IE.

## 6.3.7 Requests

Requests refer to the mechanism that CPE use to indicate to the BS that it needs upstream bandwidth allocation. A Request MAY come as a stand-alone Bandwidth Request Header (refer to Section TBD) or it MAY come as a piggyback request (refer to Section 6.7.3).

Because the modulation format of the upstream can dynamically change, all requests for bandwidth shall be made in terms of the number of bytes needed to carry the MAC header and payload, but not the PHY layer overhead.

The Bandwidth Request Message may be transmitted during any of the following intervals:

- a) Request IE
- b) Short Data Grant IE
- c) Long Data Grant IE

The number of bytes requested **MUST** be the total number that are desired by the CPE at the time of the request (excluding any physical layer overhead), subject to PCD<sup>1</sup> and administrative limits<sup>2</sup>.

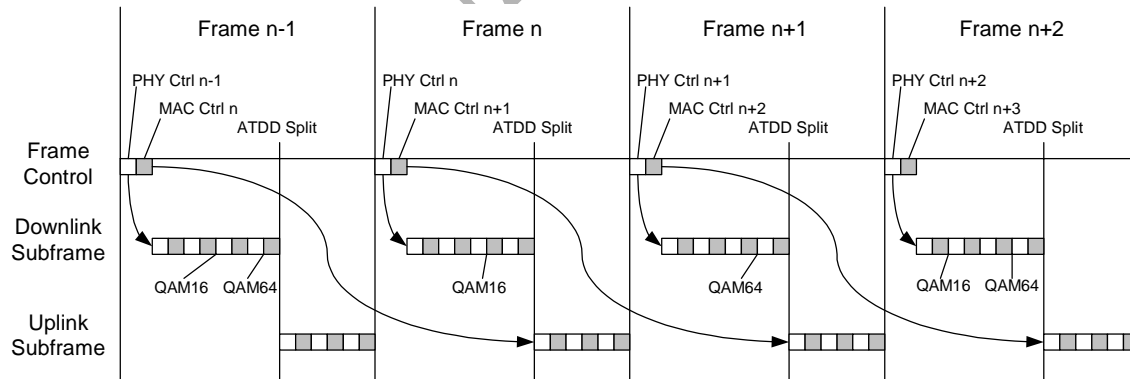
The CPE **MUST** have only one request outstanding at a time per Connection ID. If the BS does not immediately respond with a Data Grant, the CPE is able to unambiguously determine that its request is still pending because the BS **MUST** continue to issue a Data Grant Pending in every MAP for as long as a request is unsatisfied.

In US-MAPs, the BS **MUST NOT** make a data grant greater than 255 mini-slots to any CPE. This puts an upper bound on the grant size the CPE has to support.

### 6.3.8 MAP Relevance and Synchronization

#### 6.3.8.1 MAP Relevance for Burst PHY Systems

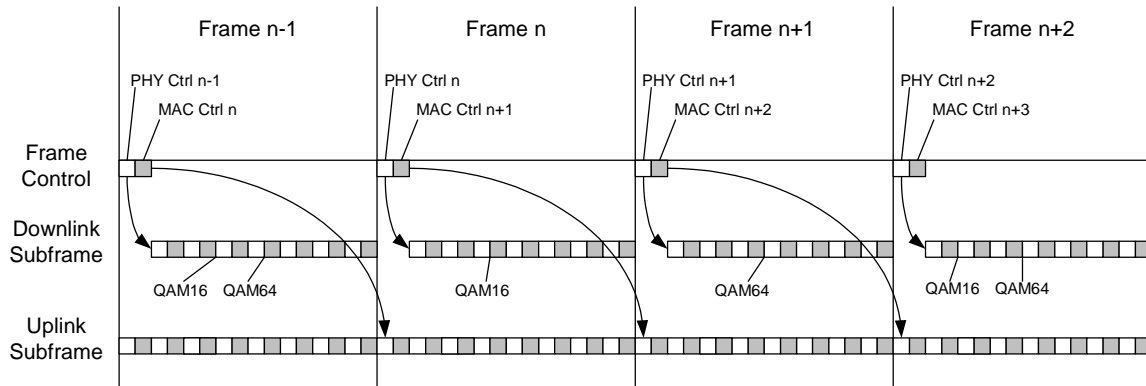
The information in the PHY Control portion of the Frame Control Header pertains to the current frame (i.e., the frame in which it was received). The information in the Uplink Subframe Map in the MAC Control portion of the Frame Control Header pertains to the following frame (i.e., one frame after it is received). This timing holds for both the TDD and FDD variants of the burst system. The TDD variant is shown in Figure 43. The FDD variant is shown in Figure 44.



**Figure 43—Time Relevance of PHY and MAC Control Information (TDD)**

<sup>1</sup>The CPE is limited by the Maximum Burst size for the Long Data Grant IUC in the UCD.

<sup>2</sup>The CPE is limited by the Maximum Concatenated Burst for the Service Flow

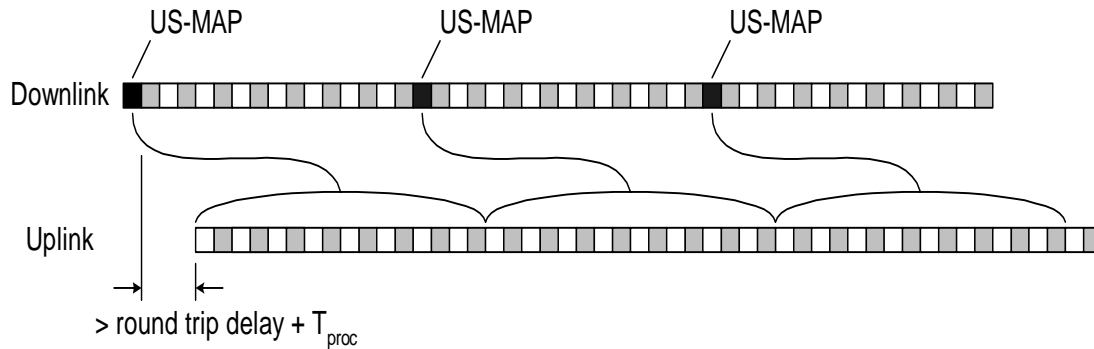


**Figure 44—Time Relevance of PHY and MAC Control Information (FDD)**

### 6.3.8.2 MAP Relevance for Continuous PHY Systems

In the Continuous PHY system, the downstream MAP (DS-MAP) only contains the Upstream Time Stamp, and does not define what information is being transmitted. All CPE continuously search the downstream signal for any downstream message that is addressed to them. The Upstream MAP (US-MAP) message in the downstream contains the Time Stamp that indicates the first mini-slot that the MAP defines.

The delay from the end of the US-MAP to the beginning of the first Upstream interval defined by the MAP shall be greater than maximum round trip delay plus the processing time required by the SS. (see Figure 45)



**Figure 45—Time Relevance of Upstream MAP Information (Continuous FDD)**

## 6.4 Contention Resolution

The BS controls assignments on the upstream channel through the US-MAP and determines which mini-slots are subject to collisions. The BS MAY allow collisions on either Requests or Data PDUs.

This section provides an overview of upstream transmission and contention resolution. For simplicity, it refers to the decisions a CPE makes, however, this is just a pedagogical tool. Since a CPE can have multiple

upstream Service Flows (each with its own SID) it makes these decisions on a per service queue or per SID basis.

The mandatory method of contention resolution which **MUST** be supported is based on a truncated binary exponential back-off, with the initial back-off window and the maximum back-off window controlled by the BS. The values are specified as part of the Upstream Bandwidth Allocation Map (US-MAP) MAC message and represent a power-of-two value. For example, a value of 4 indicates a window between 0 and 14 (total length of 15); a value of 10 indicates a window between 0 and 1022 (total length of 1023).

When a CPE has information to send and wants to enter the contention resolution process, it sets its internal back-off window equal to the Data Backoff Start defined in the US-MAP currently in effect.<sup>3</sup>

The CPE **MUST** randomly select a number within its back-off window. This random value indicates the number of contention transmit opportunities which the CPE **MUST** defer before transmitting. A CPE **MUST** only consider contention transmit opportunities for which this transmission would have been eligible. These are defined by either Request IEs or Request/Data IEs in the US-MAP. Note: Each IE can represent multiple transmission opportunities.

As an example, consider a CPE whose initial back-off window is 0 to 14 and it randomly selects the number 11. The CPE must defer a total of 11 contention transmission opportunities. If the first available Request IE is for 6 requests, the CPE does not use this and has 5 more opportunities to defer. If the next Request IE is for 2 requests, the CPE has 3 more to defer. If the third Request IE is for 8 requests, the CPE transmits on the fourth request, after deferring for 3 more opportunities.

After a contention transmission, the CPE waits for a Data Grant (Data Grant Pending) or Data Acknowledge in a subsequent MAP. Once either is received, the contention resolution is complete. The CPE determines that the contention transmission was lost when it finds a MAP without a Data Grant (Data Grant Pending) or Data Acknowledge for it and with an Ack time more recent than the time of transmission.<sup>4</sup> The CPE **MUST** now increase its back-off window by a factor of two, as long as it is less than the maximum back-off window. The CPE **MUST** randomly select a number within its new back-off window and repeat the deferring process described above.

This re-try process continues until the maximum number of retries (16) has been reached, at which time the PDU **MUST** be discarded. Note: The maximum number of retries is independent of the initial and maximum back-off windows that are defined by the BS.

If the CPE receives a unicast Request or Data Grant at any time while deferring for this SID, it **MUST** stop the contention resolution process and use the explicit transmit opportunity.

The BS has much flexibility in controlling the contention resolution. At one extreme, the BS **MAY** choose to set up the Data Backoff Start and End to emulate an Ethernet-style back-off with its associated simplicity and distributed nature, but also its fairness and efficiency issues. This would be done by setting Data Backoff Start = 0 and End = 10 in the US-MAP. At the other end, the BS **MAY** make the Data Backoff Start and End identical and frequently update these values in the US-MAP so all CPE are using the same, and hopefully optimal, back-off window.

<sup>3</sup>The MAP currently in effect is the MAP whose allocation start time has occurred but which includes IEs that have not occurred.

<sup>4</sup>Data Acknowledge IEs are intended for collision detection only and is not designed for providing reliable transport (that is the responsibility of higher layers). If a MAP is lost or damaged, a CPE waiting for a Data Acknowledge **MUST** assume that its contention data transmission was successful and **MUST NOT** retransmit the data packet. This prevents the CPE from sending duplicate packets unnecessarily.

### 6.4.1 Transmit Opportunities

A Transmit Opportunity is defined as any mini-slot in which a CPE may be allowed to start a transmission. Transmit Opportunities typically apply to contention opportunities and are used to calculate the proper amount to defer in the contention resolution process.

The number of Transmit Opportunities associated with a particular IE in a MAP is dependent on the total size of the region as well as the allowable size of an individual transmission. As an example, assume a REQ IE defines a region of 12 mini-slots. If the UCD defines a REQ Burst Size that fits into a single mini-slot then there are 12 Transmit Opportunities associated with this REQ IE, i.e., one for each mini-slot. If the UCD defines a REQ that fits in two mini-slots, then there are six Transmit Opportunities and a REQ can start on every other mini-slot.

As another example, assume a REQ/Data IE that defines a 24 mini-slot region. If it is sent with an SID of 0x3FF4 (refer to TBD), then a CPE can potentially start a transmit on every fourth mini-slot; so this IE contains a total of six Transmit Opportunities (TX OP). Similarly, a SID of 0x3FF6 implies four TX OPs; 0x3FF8 implies three TX OPs; and 0x3FFC implies two TX OPs.

For an Initial Maintenance IE, a CPE MUST start its transmission in the first mini-slot of the region; therefore it has a single Transmit Opportunity. The remainder of the region is used to compensate for the round trip delays since the CPE has not yet been ranged.

Station Maintenance IEs, Short/Long Data Grant IEs and unicast Request IEs are unicast and thus are not typically associated with contention Transmit Opportunities. They represent a single dedicated, or reservation based, Transmit Opportunity.

## 6.5 Fragmentation

### 6.5.1 Policy and Rules

### 6.5.2 Error Conditions

## 6.6 Upstream Service

EDITOR - WHERE DOES TABLE 5-29 GO?

The following sections define the basic upstream Service Flow scheduling services and list the QoS parameters associated with each service. A detailed description of each QoS parameter is provided in TBD. The section also discusses how these basic services and QoS parameters can be combined to form new services, such as, Committed Information Rate (CIR) service.

Scheduling services are designed to improve the efficiency of the poll/grant process. By specifying a scheduling service and its associated QoS parameters, the BS can anticipate the throughput and latency needs of the upstream traffic and provide polls and/or grants at the appropriate times.

Each service is tailored to a specific type of data flow as described below. The basic services comprise: Unsolicited Grant Service (UGS), Real-Time Polling Service (rtPS), Unsolicited Grant Service with Activity Detection (UGS-AD), Non-Real-Time Polling Service (nrtPS) and Best Effort (BE) service. Table 8.4 (EDITOR - where is table?) shows the relationship between the scheduling services and the related QoS parameters.

### 6.6.1 Unsolicited Grant Service

The Unsolicited Grant Service (UGS) is designed to support real-time service flows that generate fixed size data packets on a periodic basis, such as Voice over IP. The service offers fixed size grants on a real-time periodic basis, which eliminate the overhead and latency of CPE requests and assure that grants will be available to meet the flow's real-time needs. The BS MUST provide fixed size data grants at periodic intervals to the Service Flow. In order for this service to work correctly, the Request/Transmission Policy (refer to TBD) setting MUST be such that the CPE is prohibited from using any contention request or request/data opportunities and the BS SHOULD NOT provide any unicast request opportunities. The Request/Transmission Policy MUST also prohibit piggyback requests. This will result in the CPE only using unsolicited data grants for upstream transmission. All other bits of the Request/Transmission Policy are not relevant to the fundamental operation of this scheduling service and should be set according to network policy. The key service information elements are the Unsolicited Grant Size, the Nominal Grant interval, the Tolerated Grant Jitter and the Request/Transmission Policy. (Refer to TBD)

The Unsolicited Grant Synchronization Header (UGSH) in the Service Flow EH Element (refer to Section TBD) is used to pass status information from the CPE to the BS regarding the state of the UGS Service Flow. The most significant bit of the UGSH is the Queue Indicator (QI) bit. The CPE MUST set this flag once it detects that this Service Flow has exceeded its transmit queue depth. Once the CPE detects that the Service Flow's transmit queue is back within limits, it MUST clear the QI flag. The flag allows the BS to provide for long term compensation for conditions such as lost maps or clock rate mismatch's by issuing additional grants.

The BS MUST NOT allocate more grants per Nominal Grant Interval than the Grants Per Interval parameter of the Active QoS Parameter Set, excluding the case when the QI bit of the UGSH is set. In this case, the BS MAY grant up to 1% additional bandwidth for clock rate mismatch compensation. The active grants field of the UGSH is ignored with UGS service. The BS policing of the Service Flow remains unchanged.

### 6.6.2 Real-Time Polling Service

The Real-Time Polling Service (rtPS) is designed to support real-time service flows that generate variable size data packets on a periodic basis, such as MPEG video. The service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allow the CPE to specify the size of the desired grant. This service requires more request overhead than UGS, but supports variable grant sizes for optimum data transport efficiency.

The BS MUST provide periodic unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (refer to TBD) SHOULD be such that the CPE is prohibited from using any contention request or request/data opportunities. The Request/Transmission Policy SHOULD also prohibit piggyback requests. The BS MAY issue unicast request opportunities as prescribed by this service even if a grant is pending. This will result in the CPE using only unicast request opportunities in order to obtain upstream transmission opportunities (the CPE could still use unsolicited data grants for upstream transmission as well). All other bits of the Request/Transmission Policy are not relevant to the fundamental operation of this scheduling service and should be set according to network policy. The key service information elements are the Nominal Polling Interval, the Tolerated Poll Jitter and the Request/Transmission Policy.

### 6.6.3 Unsolicited Grant Service with Activity Detection

The Unsolicited Grant Service with Activity Detection (UGS/AD) is designed to support UGS flows that may become inactive for substantial portions of time (i.e. tens of milliseconds or more), such as Voice over IP with silence suppression. The service provides Unsolicited Grants when the flow is active and unicast polls when the flow is inactive. This combines the low overhead and low latency of UGS with the efficiency of rtPS. Though UGS/AD combines UGS and rtPS, only one scheduling service is active at a time.

The BS MUST provide periodic unicast grants, when the flow is active, but MUST revert to providing periodic unicast request opportunities when the flow is inactive. [The BS can detect flow inactivity by detecting unused grants. However, the algorithm for detecting a flow changing from an active to an inactive state is dependent on the BS implementation]. In order for this service to work correctly, the Request/Transmission Policy setting (refer to TBD) MUST be such that the CPE is prohibited from using any contention request or request/data opportunities. The Request/Transmission Policy MUST also prohibit piggyback requests. This results in the CPE using only unicast request opportunities in order to obtain upstream transmission opportunities. However, the CPE will use unsolicited data grants for upstream transmission as well. All other bits of the Request/Transmission Policy are not relevant to the fundamental operation of this scheduling service and should be set according to network policy. The key service parameters are the Nominal Polling Interval, the Tolerated Poll Jitter, the Nominal Grant Interval, the Tolerated Grant Jitter, the Unsolicited Grant Size and the Request/Transmission Policy.

In UGS-AD service, when restarting UGS after an interval of  $rtPS$ , the BS SHOULD provide additional grants in the first (and/or second) grant interval such that the CPE receives a total of one grant for each grant interval from the time the CPE requested restart of UGS, plus one additional grant. (Refer to TBD) Because the Service Flow is provisioned as a UGS flow with a specific grant interval and grant size, when restarting UGS, the CPE MUST NOT request a different sized grant than the already provisioned UGS flow. As with any Service Flow, changes can only be requested with a DSC command.

The Service Flow Extended Header Element allows for the CPE to dynamically state how many grants per interval are required to support the number of flows with activity present. In UGS/AD, the CPE MAY use the Queue Indicator Bit in the UGSH. The remaining seven bits of the UGSH define the Active Grants field. This field defines the number of grants within a Nominal Grant Interval that this Service Flow currently requires. When using UGS/AD, the CPE MUST indicate the number of requested grants per Nominal Grant Interval in this field. The Active Grants field of the UGSH is ignored with UGS without Activity Detection. This field allows the CPE to signal to the BS to dynamically adjust the number of grants per interval that this UGS Service Flow is actually using. The CPE MUST NOT request more than the number of Grants per Interval in the ActiveQoSParameterSet.

#### 6.6.4 Non-Real-Time Polling Service

The Non-Real-Time Polling Service (nrtPS) is designed to support non real-time service flows that require variable size data grants on a regular basis, such as high bandwidth FTP. The service offers unicast polls on a regular basis which assures that the flow receives request opportunities even during network congestion. The BS typically polls nrtPS SIDs on an (periodic or non-periodic) interval on the order of one second or less.



set according to network policy. The key service elements are the Minimum Reserved Traffic Rate, the Maximum Sustained Traffic Rate, and the Traffic Priority.

## 6.7 Bandwidth Allocation and Request Mechanisms

Note that at registration every CPE is assigned a dedicated connection ID for the purpose of sending and receiving control messages. Increasing (or decreasing) bandwidth requirements is necessary for all services except uncompressible constant bit rate CG services. The needs of uncompressible CG services do not change between connection establishment and termination. The requirements of compressible CG services, such as channelized T1, may increase or decrease depending on traffic. DAMA services are given resources on a demand assignment basis, as the need arises.

When a CPE needs to ask for bandwidth on a DAMA connection, it sends a message to the BS containing the immediate requirements of the DAMA connection. QoS for the connection was established at connection establishment and is looked-up by the BS.

There are numerous methods by which the CPE can get the bandwidth request message to the BS.

### 6.7.1 Polling

Polling is the process by which the BS allocates to the CPEs bandwidth specifically for the purpose of making bandwidth requests. These allocations may be to individual CPEs or to groups of CPEs. Allocations to groups of CPEs actually define bandwidth request contention slots (see section TBD). The allocations are not in the form of an explicit message, but via an allocation (or increase) in the Uplink Map.

Note that polling is done on a CPE basis, bandwidth is requested on a connection ID basis, and bandwidth is allocated on a CPE basis.

#### 6.7.1.1 Unicast

When a CPE is polled individually, no explicit message is transmitted to poll the CPE. Rather, the CPE is allocated, in the Uplink Subframe Map, bandwidth sufficient to respond with a bandwidth request. If the CPE does not need bandwidth, it returns a request for 0 bytes (Note that 0 byte requests are only used in the individual polling case since explicit bandwidth for a reply has been allocated.). Active CPEs that do not set the Poll Me bit in some MAC packet header will not be polled individually. Only inactive CPEs and CPEs explicitly requesting to be polled will be polled individually. This saves bandwidth over polling all CPEs individually. Active CPEs respond to polling at their current uplink modulation, while inactive CPEs must respond at QAM-4 to ensure their transmission is robust enough to be detected by the BS.

The interpretation of bandwidth requests by the base station differs for CG connections and DAMA connections. For CG connections, the effect of a bandwidth request is to change the bandwidth allocated every frame. For DAMA connections, the effect is to reset the base station's perception of the data pending at the CPE for that connection.

The information exchange sequence for individual polling is shown in Figure 46.

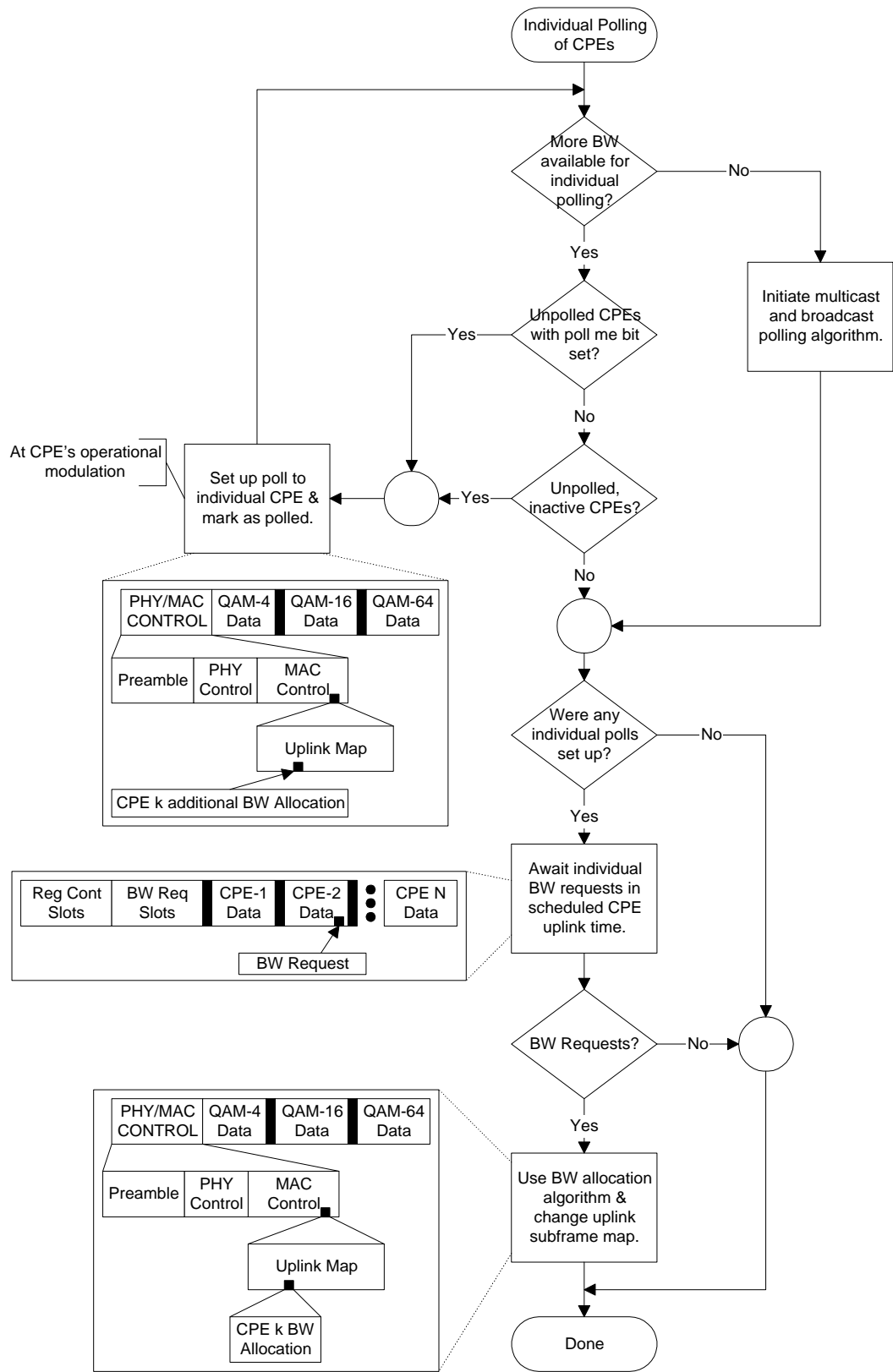
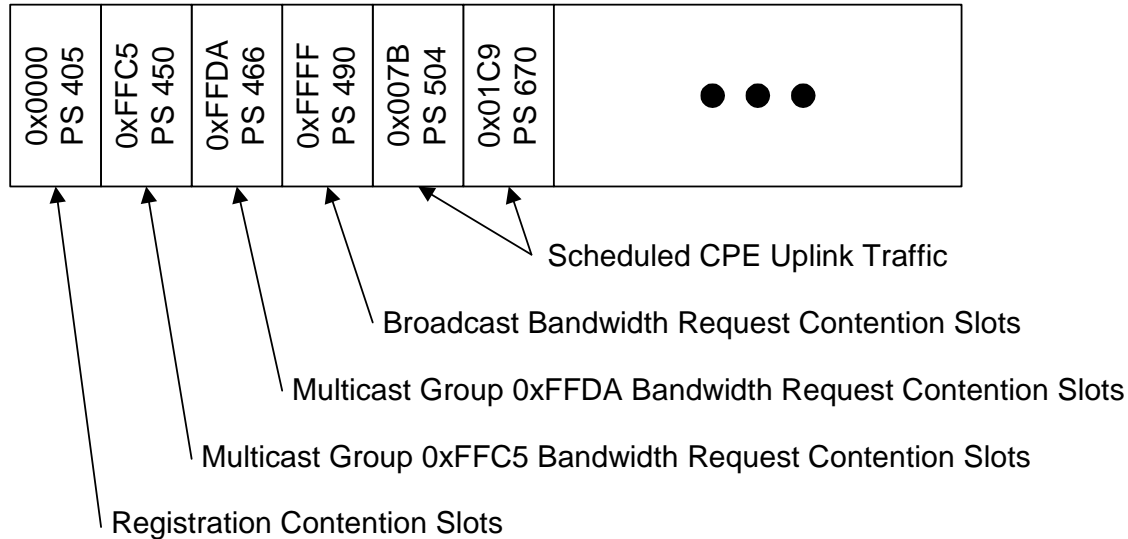


Figure 46—Unicast Polling

### 6.7.1.2 Multicast

If there are more CPEs that are inactive than there is bandwidth available for individual polling, some CPEs may be polled in multicast groups and a broadcast poll may be issued. Certain connection IDs are reserved for multicast groups and for broadcast messages, as described in section TBD. As with individual polling, the poll is not an explicit message but bandwidth allocated in the Uplink Map. The difference is that rather than associating allocated bandwidth with a CPE's basic connection ID, the allocation is to a multicast or broadcast connection ID. This is shown in Figure TBD



**Figure 47—US-MAP Example (Polling)**

When the poll is directed at a multicast or broadcast connection ID, CPEs belonging to the polled group may request bandwidth using Bandwidth Request Contention Slots allocated in the uplink subframe. With multicast and broadcast polling, to reduce the likelihood of collision, only CPE's needing bandwidth reply. Zero-length bandwidth requests are not allowed in bandwidth request contention slots. CPEs always transmit using the lowest modulation in the bandwidth request contention slots. The contention slots are sized to hold a CTG and a bandwidth request message. The message requires a shortened TDU.

If an error such as an invalid connection ID occurs the BS sends an explicit error message to the CPE. If the BS does not respond with an error message or a bandwidth allocation within the expiration of timer MT5, the CPE assumes a collision has occurred and uses a slotted ALOHA scheme to back off and try at another contention opportunity. The multicast and broadcast polling process is shown in Figure TBD.

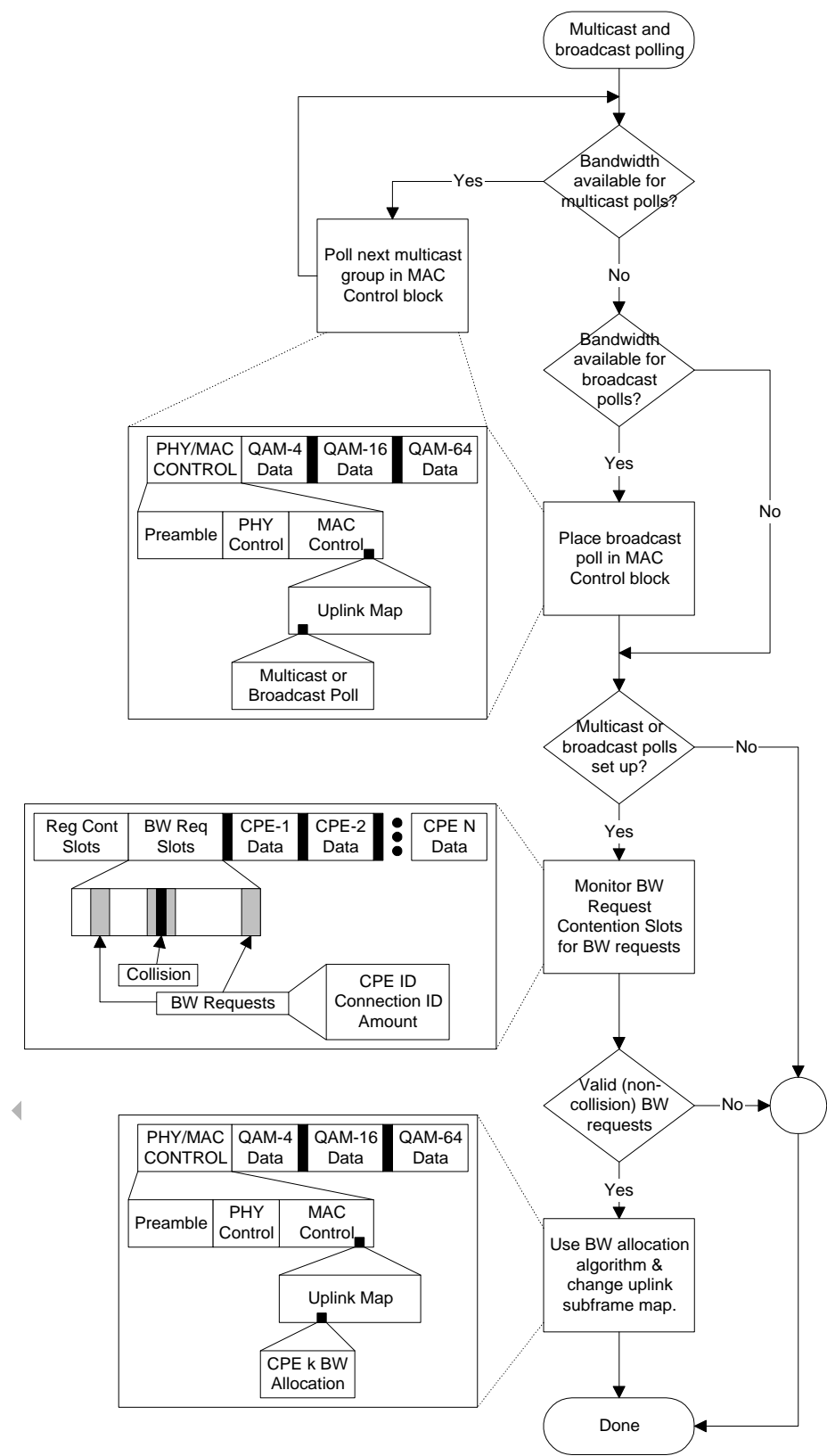


Figure 48—Multicast and Broadcast Polling

### 6.7.1.3 Broadcast

### 6.7.2 Poll-Me Bit

Currently active CPEs may set the poll me bit (bit PM in the MAC header) or the priority poll me bit (bit PPM in the MAC header) in a MAC packet to indicate to the BS that they need polled to negotiate a bandwidth change. To reduce the bandwidth requirements of individual polling, active CPEs will be individually polled only if one of these bits is set. Once the BS detects this request for polling, the process for individual polling is used to satisfy the request. The procedure by which a CPE stimulates the BS to poll it is shown in Figure TBD. To minimize the risk of the BS missing the poll me bit, the CPE may set the bit in all MAC headers in the frame.

PRELIMINARY SUBMITTAL

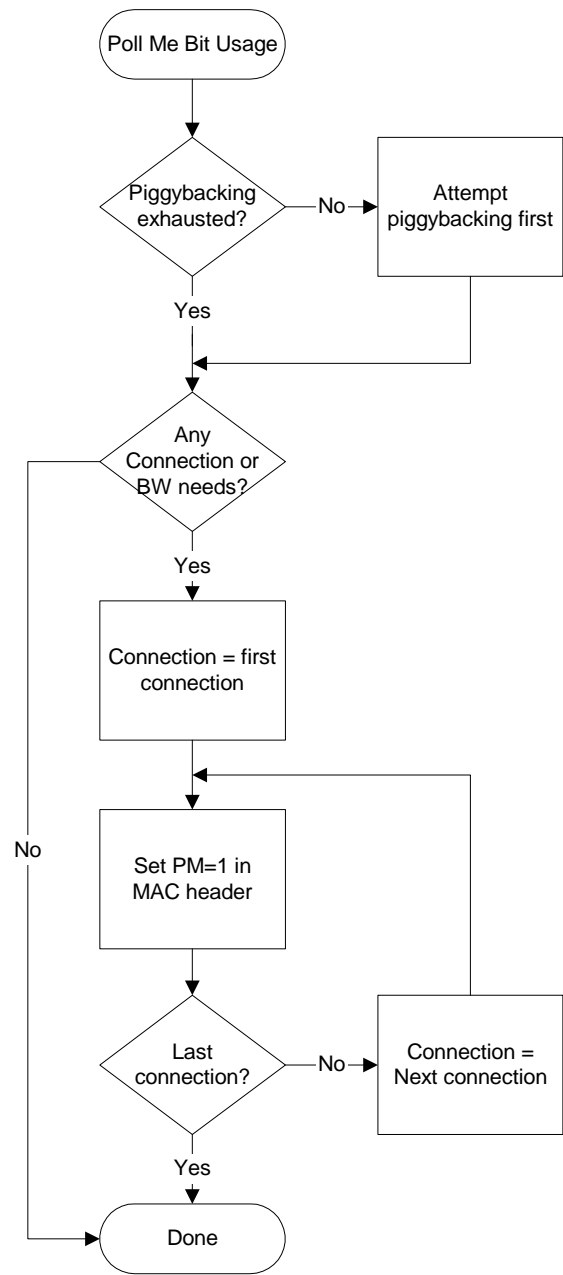


Figure 49—Poll Me Bit Usage

6.7.3 Piggy-Back and Bandwidth Requests

## 6.8 Network Entry and Initialization

The procedure for initialization of a CPE modem MUST be as shown in Figure TBD. This figure shows the overall flow between the stages of initialization in a CPE. This shows no error paths, and is simply to provide an overview of the process. The more detailed finite state machine representations of the individual sections (including error paths) are shown in the subsequent figures. Timeout values are defined in TBD.

The procedure can be divided into the following phases:

- a) Scan for downstream channel and establish synchronization with the BS.
- b) Obtain transmit parameters (from UCD message)
- c) Perform ranging
- d) Establish IP connectivity
- e) Establish time of day
- f) Transfer operational parameters
- g) Perform registration
- h) Privacy initialization (if provisioned to utilize Privacy capabilities)

Each CPE contains the following information when shipped from the manufacturer:

- a) A unique IEEE 802 48-bit MAC address which is assigned during the manufacturing process. This is used to identify the modem to the various provisioning servers during initialization.
- b) Security information as defined in Section 7 (e.g., X.509 certificate) used to authenticate the CPE to the security server and authenticate the responses from the security and provisioning servers.

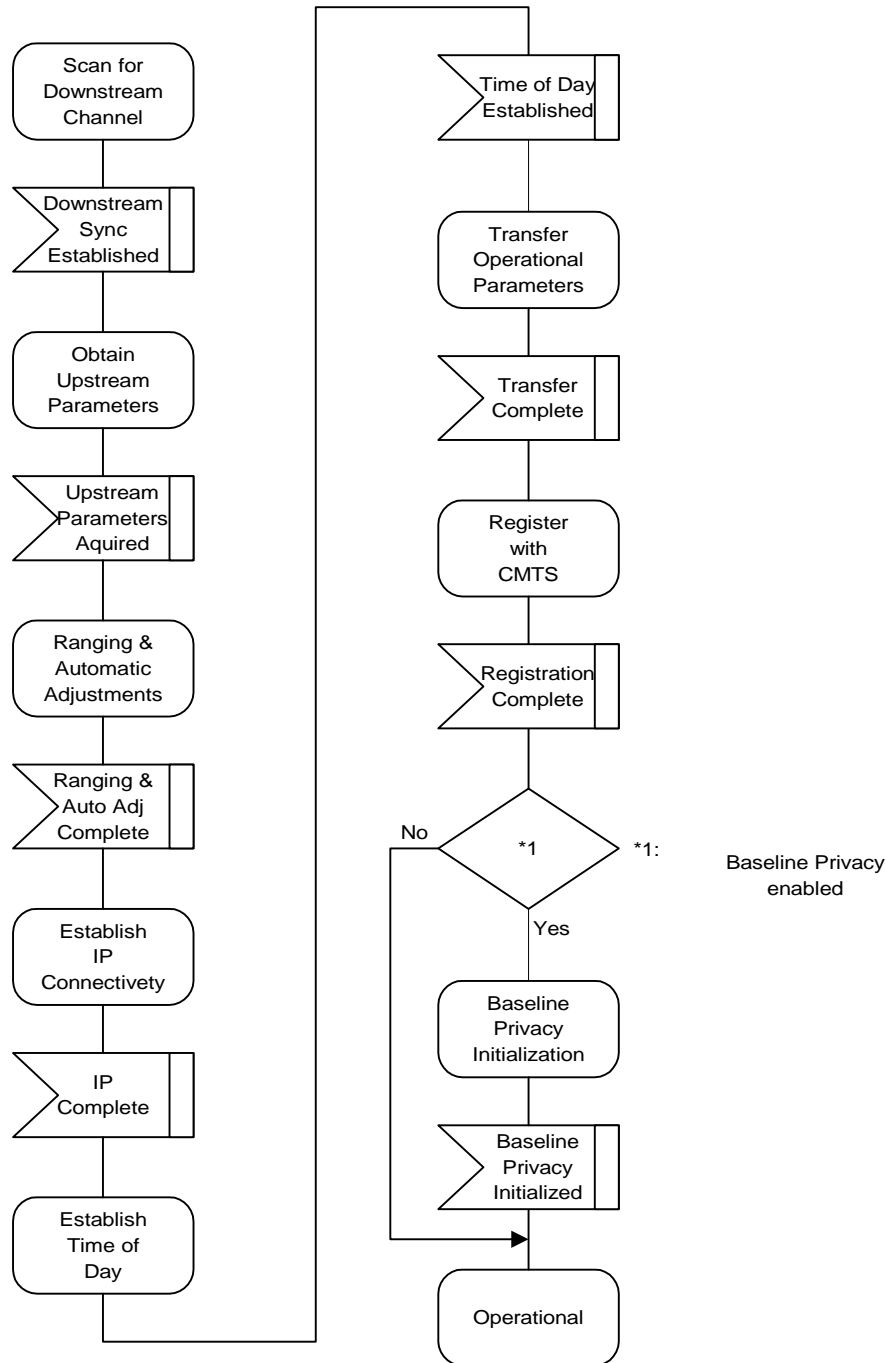


Figure 50— CPE Initialization Overview

### 6.8.1 Scanning and Synchronization to Downstream

On initialization or after signal loss, the CPE modem **MUST** acquire a downstream channel. The CPE **MUST** have non-volatile storage in which the last operational parameters are stored and **MUST** first try to re-acquire this downstream channel. If this fails, it **MUST** begin to continuously scan the possible channels of the downstream frequency band of operation until it finds a valid downstream signal.



A downstream signal is considered to be valid when the CPE has achieved the following steps:

- a) synchronization of the modulation symbol timing
- b) synchronization of the convolutional decoder if present
- c) synchronization of the FEC framing
- d) synchronization of the MPEG packetization
- e) recognition of SYNC downstream MAC messages

This implies that it has locked onto the correct frequency, equalized the downstream channel, recovered any PMD sublayer framing and the FEC is operational (refer to Section TBD). At this point, a valid bit stream is being sent to the transmission convergence sublayer. The transmission convergence sublayer performs its own synchronization. On detecting the well-known BWA PID, along with a payload unit start indicator per [ITU-T H.222.0], it delivers the MAC frame to the MAC sublayer.

The MAC sublayer **MUST** now search for the Timing Synchronization (SYNC) MAC management messages. The CPE achieves MAC synchronization once it has received at least two SYNC messages for the same Upstream Channel ID and has verified that its clock tolerances are within specified limits.

A CPE remains in “SYNC” as long as it continues to successfully receive the SYNC messages for its Upstream Channel ID. If the Lost SYNC Interval (refer to TBD) has elapsed without a valid SYNC message, a CPE **MUST NOT** use the upstream and **MUST** try to re-establish synchronization again.

## 6.8.2 Obtain Downstream Parameters

### 6.8.3 Obtain Upstream Parameters

Refer to Figure TBD. After synchronization, the CPE **MUST** wait for an upstream channel descriptor message (UCD) from the BS in order to retrieve a set of transmission parameters for a possible upstream channel. These messages are transmitted periodically from the BS for all available upstream channels and are addressed to the MAC broadcast address. The CPE **MUST** determine whether it can use the upstream channel from the channel description parameters.

The CPE **MUST** collect all UCDs which are different in their channel ID field to build a set of usable channel IDs. If no channel can be found after a suitable timeout period, then the CPE **MUST** continue scanning to find another downstream channel.

The CPE **MUST** determine whether it can use the upstream channel from the channel description parameters. If the channel is not suitable, then the CPE **MUST** try the next channel ID until it finds a usable channel. If the channel is suitable, the CPE **MUST** extract the parameters for this upstream from the UCD. It then **MUST** wait for the next SYNC message and extract the upstream mini-slot timestamp from this message. The CPE then **MUST** wait for a bandwidth allocation map for the selected channel. It **MAY** begin transmitting upstream in accordance with the MAC operation and the bandwidth allocation mechanism.

The CPE **MUST** perform initial ranging at least once per Figure TBD. If initial ranging is not successful, then the next channel ID is selected, and the procedure restarted from UCD extraction. When there are no more channel IDs to try, then the CPE **MUST** continue scanning to find another downstream channel.

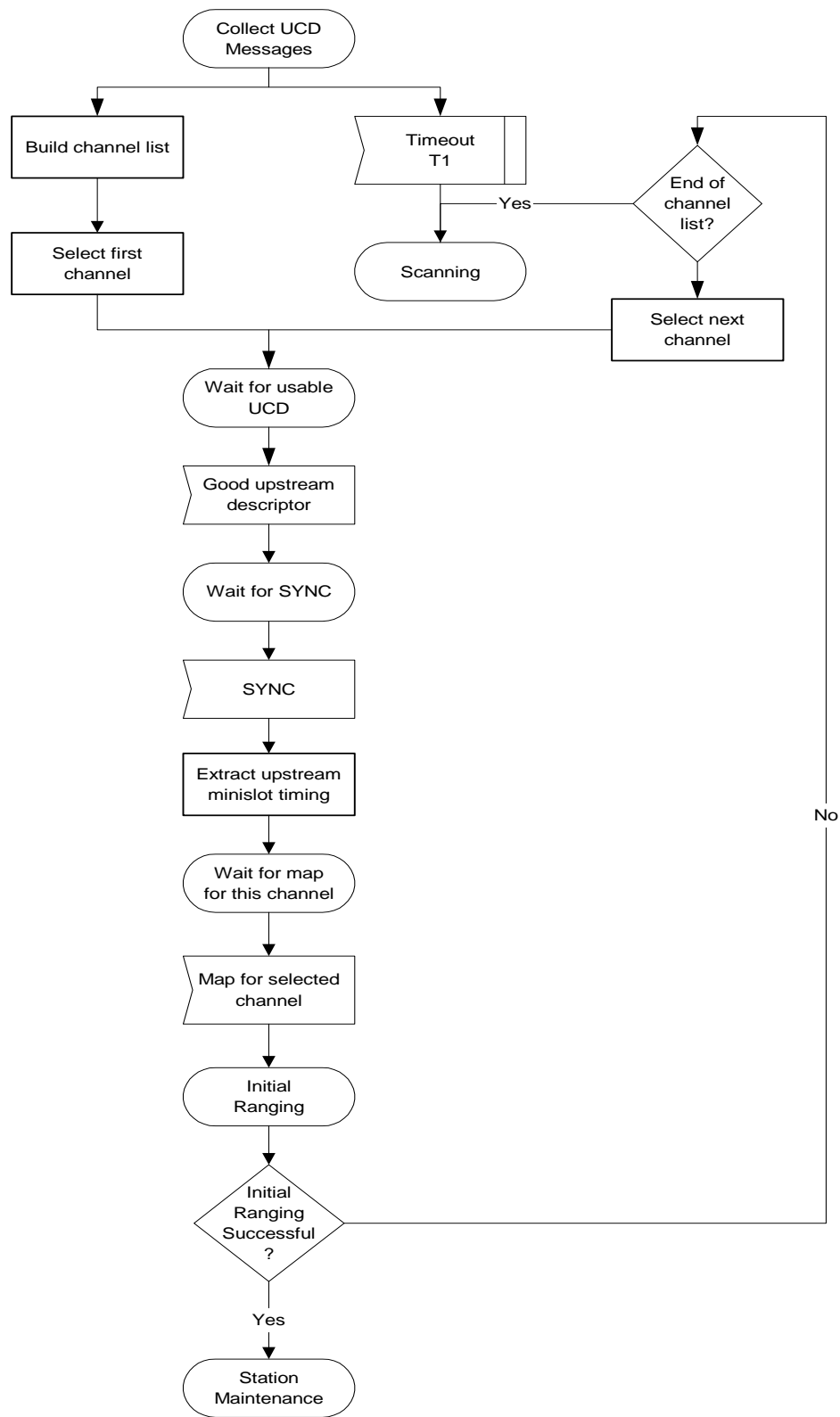


Figure 51— Obtaining Upstream Parameters

#### 6.8.4 message Flows During Scanning and Upstream Parameter Acquisition

The BS MUST generate SYNC and UCD messages on the downstream at periodic intervals within the ranges defined in Appendix B. These messages are addressed to all CPEs. Refer to Figure TBD.

**Table 10—message Flows During Scanning and Upstream Parameter Acquisition**

BS		CPE
clock time to send SYNC	-----SYNC----->	
clock time to send UCD	-----UCD----->	
clock time to send SYNC	-----SYNC----->	
		Example of a UCD cycle
		prior to CPE power-on
clock time to send SYNC	-----SYNC----->	
clock time to send SYNC	-----SYNC----->	
clock time to send SYNC	-----SYNC----->	
clock time to send UCD	-----UCD----->	
clock time to send SYNC	-----SYNC----->	
		power on sequence complete
clock time to send SYNC	-----SYNC----->	
		establish PHY synchronization

**Table 10—message Flows During Scanning and Upstream Parameter Acquisition**

BS		CPE
		& wait for UCD
clock time to send SYNC	-----SYNC----->	
clock time to send SYNC	-----SYNC----->	
clock time to send UCD	-----UCD----->	
		obtain parameters for this upstream channel to use for initialization
clock time to send SYNC	-----SYNC----->	
		extract slot info for upstream & wait for transmit opportunity to perform ranging
clock time to send SYNC	-----SYNC----->	
clock time to send MAP	-----MAP----->	
		start ranging process

### 6.8.5 Initial Ranging and Automatic Adjustments

Ranging is the process of acquiring the correct timing offset such that the CPE modem's transmissions are aligned to the correct mini-slot boundary. The timing delays through the PHY layer **MUST** be relatively constant. Any variation in the PHY delays **MUST** be accounted for in the guard time of the upstream PMD overhead.

First, a CPE modem **MUST** synchronize to the downstream and learn the upstream channel characteristics through the Upstream Channel Descriptor MAC management message. At this point, the CPE modem **MUST** scan the Bandwidth Allocation MAP message to find an Initial Maintenance Region. Refer to Section TBD. The BS **MUST** make an Initial Maintenance region large enough to account for the variation in delays between any two CPEs.

The CPE modem **MUST** put together a Ranging Request message to be sent in an Initial Maintenance region. The SID field **MUST** be set to the non-initialized CPE value (zero).

Ranging adjusts each CPE's timing offset such that it appears to be located right next to the BS. The CPE **MUST** set its initial timing offset to the amount of internal fixed delay equivalent to putting this CPE next to the BS. This amount includes delays introduced through a particular implementation, and **MUST** include the downstream PHY interleaving latency.

When the Initial Maintenance transmit opportunity occurs, the CPE modem **MUST** send the Ranging Request message. Thus, the CPE modem sends the message as if it was physically right at the BS.

Once the BS has successfully received the Ranging Request message, it MUST return a Ranging Response message addressed to the individual CPE modem. Within the Ranging Response message MUST be a temporary SID assigned to this CPE modem until it has completed the registration process. The message MUST also contain information on RF power level adjustment and offset frequency adjustment as well as any timing offset corrections.

The CPE modem MUST now wait for an individual Station Maintenance region assigned to its temporary SID. It MUST now transmit a Ranging Request message at this time using the temporary SID along with any power level and timing offset corrections.

The BS MUST return another Ranging Response message to the CPE modem with any additional fine tuning required. The ranging request/response steps MUST be repeated until the response contains a Ranging Successful notification or the BS aborts ranging. Once successfully ranged, the CPE modem MUST join normal data traffic in the upstream. In particular, state machines and the applicability of retry counts and timer values for the ranging process are defined in Section TBD.

**Note: The burst type to use for any transmission is defined by the Interval Usage Code (IUC). Each IUC is mapped to a burst type in the UCD message.**

The message sequence chart and the finite state machines on the following pages define the ranging and adjustment process which MUST be followed by compliant CPEs and BS. Refer to Figure TBD through Figure TBD

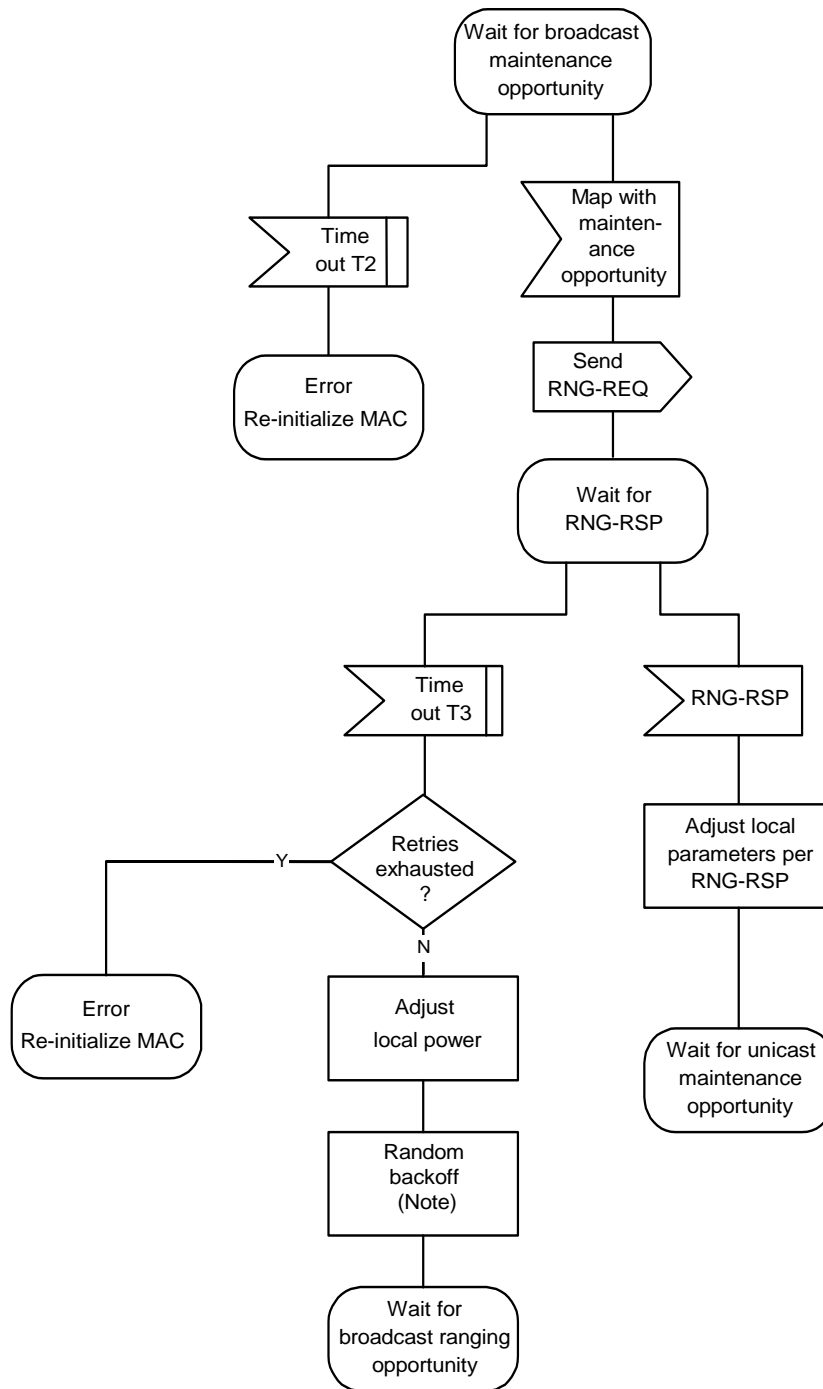
**Table 11—Ranging and Automatic Adjustments Procedure**

BS		CPE
[time to send the Initial Maintenance opportunity]		
send map containing Initial Maintenance information element with a broadcast/multicast Service ID	-----MAP----->	
	<-----RNG-REQ-----	transmit ranging packet in contention mode
with Service ID parameter = 0		
[receive recognizable ranging packet]		
allocate temporary Service ID		

**Table 11—Ranging and Automatic Adjustments Procedure**

BS		CPE
send ranging response	-----RNG-RSP----->	
add temporary Service ID to poll list		store temporary Service ID & adjust other parameters
[time to send the next map]		
send map with Station Maintenance information element to modem using temporary SID	-----MAP----->	recognize own temporary Service ID in map
	<-----RNG-REQ-----	reply to Station Maintenance opportunity poll
send ranging response	-----RNG-RSP----->	
		adjust local parameters
[time to send an Initial Maintenance opportunity] send map containing Initial Maintenance information element with a broadcast/multicast Service ID		
send periodic transmit opportunity to broadcast address	-----MAP----->	

**Note:** The BS MUST allow the CPE sufficient time to have processed the previous RNG-RSP (i.e., to modify the transmitter parameters) before sending the CPE a specific ranging opportunity. This is defined as CPE Ranging Response Time in TBD



*Note:* Timeout T3 may occur because the RNG-REQs from multiple modems collided. To avoid these modems repeating the loop in lockstep, a random backoff is required. This is a backoff over the ranging window specified in the MAP. T3 timeouts can also occur during multi-channel operation. On a system with multiple upstream channels, the CM MUST attempt initial ranging on every suitable upstream channel before moving to the next available downstream channel.

**Figure 52—Initial Ranging - CPE**

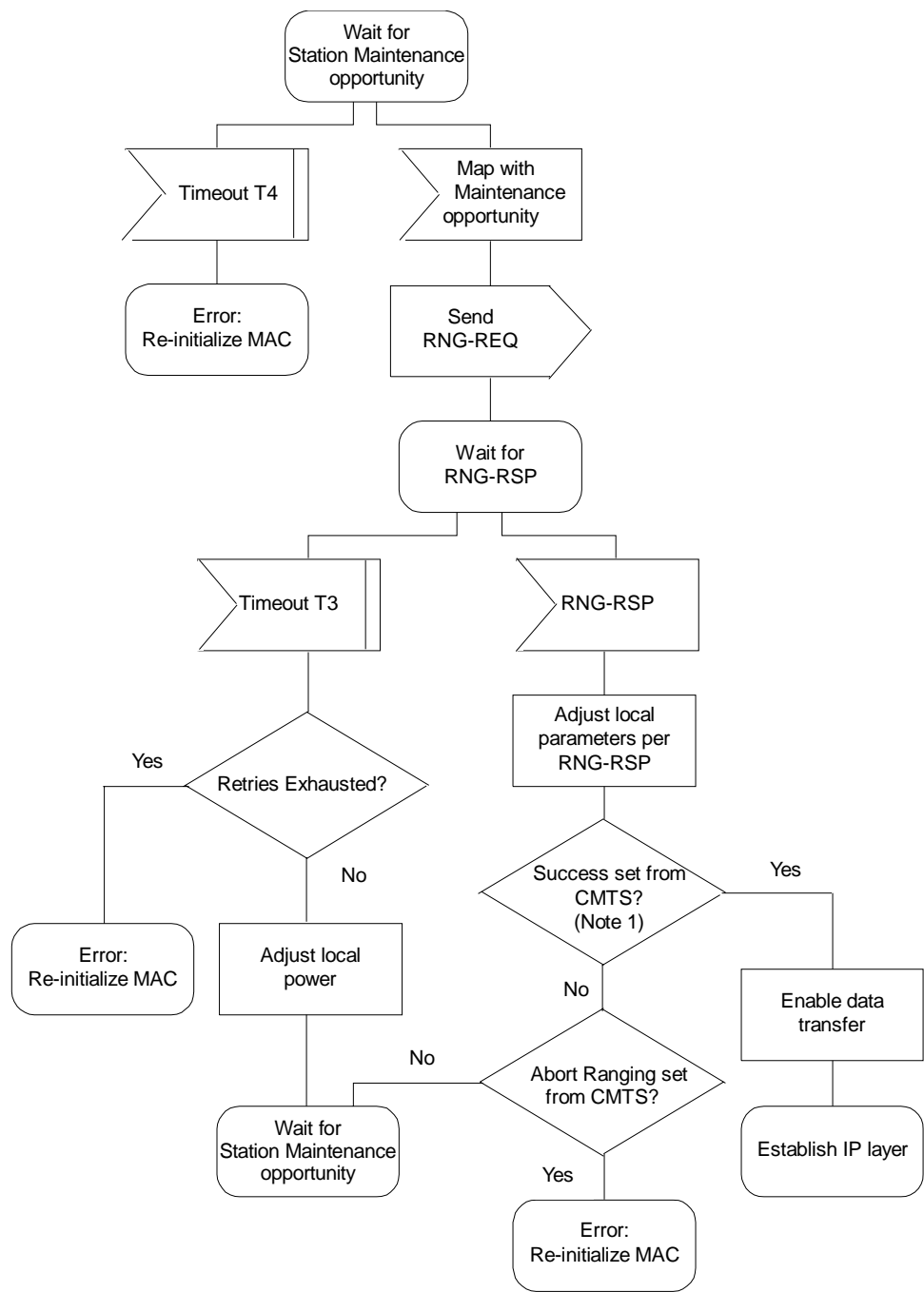


Figure 53—Initial Ranging - CPE (continued)

1) Ranging Request is within the tolerance of the BS.



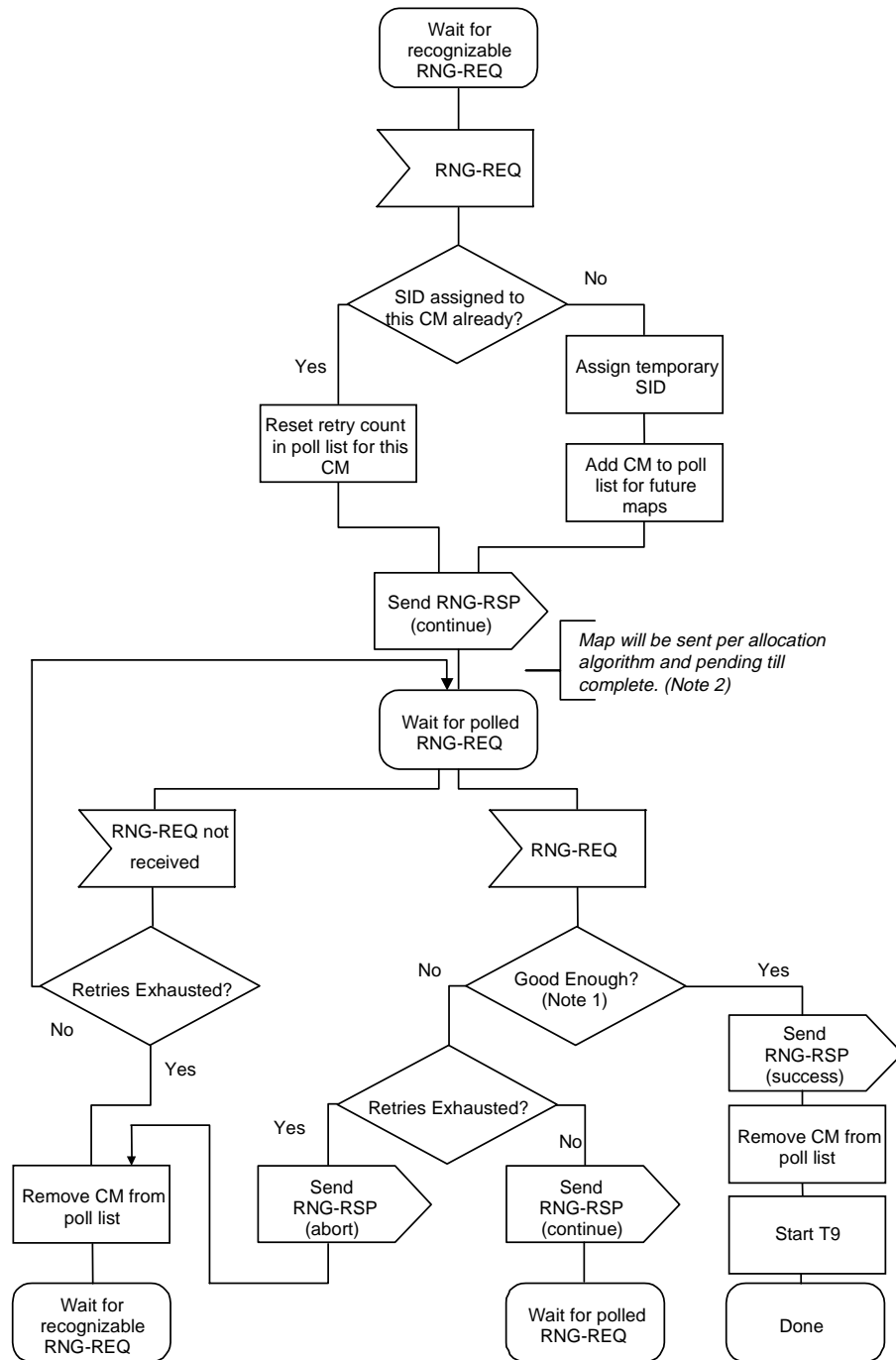


Figure 54—Initial Ranging - BS

- 1) Means ranging is within the tolerable limits of the BS.
- 2) RNG-REQ pending-till-complete was nonzero, the BS SHOULD hold off the station maintenance opportunity accordingly unless needed, for example, to adjust the CPE's power level. If opportunities are offered prior to the pending-till-complete expiry, the "good-enough" test which follows receipt of a RNG-RSP MUST NOT judge the CPE's transmit equalization until pending-till-complete expires.

### 6.8.6 Ranging Parameter Adjustment

Adjustment of local parameters (e.g., transmit power) in a CPE as a result of the receipt (or non-receipt) of an RNG-RSP is considered to be implementation-dependent with the following restrictions (refer to Section TBD):

All parameters MUST be within the approved range at all times

- a) Power adjustment MUST start from the minimum value unless a valid power is available from non-volatile storage, in which case this MUST be used as a starting point.
- b) Power adjustment MUST be capable of being reduced or increased by the specified amount in response to RNG-RSP messages.
- c) If, during initialization, power is increased to the maximum value (without a response from the BS) it MUST wrap back to the minimum.

For multi-channel support, the CPE MUST attempt initial ranging on every suitable upstream channel before moving to the next available downstream channel.

### 6.8.7 Initial Connection Establishment

#### 6.8.7.1 Establish IP Connectivity

At this point, the CPE MUST invoke DHCP mechanisms [RFC-2131] in order to obtain an IP address and any other parameters needed to establish IP connectivity (refer to TBD). The DHCP response MUST contain the name of a file which contains further configuration parameters. Refer to Figure 5-64

#### 6.8.7.2 Establish Time of Day

The CPE and BS need to have the current date and time. This is required for time-stamping logged events which can be retrieved by the management system. This need not be authenticated and need only be accurate to the nearest second.

The protocol by which the time of day MUST be retrieved is defined in [RFC-868]. Refer to Figure TBD. The request and response MUST be transferred using UDP. The time retrieved from the server (UTC) MUST be combined with the time offset received from the DHCP response to create the current local time

Successfully acquiring the Time of Day is not mandatory for a successful registration, but is necessary for on-going operation. The specific timeout for Time of Day Requests is implementation dependent. However, the CPE MUST NOT exceed more than 3 Time of Day requests in any 5 minute period.

### 6.8.8 Transfer Operational Parameters

After DHCP is successful, the modem MUST download the parameter file using TFTP, as shown in Figure TBD. The TFTP configuration parameter server is specified by the "siaddr" field of the DHCP response. The CPE MUST use an adaptive timeout for TFTP based on binary exponential backoff. Refer to [RFC1123] and [RFC2349].

**Table 12—Establishing IP Connectivity**

CPE		DHCP
send DHCP request to broadcast address		
	-----DHCP discover----->	
		check CPE MAC address & respond
	<-----DHCP offer -----	
choose server		
	-----DHCP request----->	
		process request
	<-----DHCP response-----	
set up IP parameters from DHCP response		

**Table 13—Establishing Time of Day**

CPE		Time Server
send request to time server		
	-----time of day request----->	
		process request
	<-----time of day response-----	
set up / correct time of day from response		

The parameter fields required in the DHCP response and the format and content of the configuration file MUST be as defined in Section TBD. Note that these fields are the minimum required for interoperability.

If a modem downloads a configuration file containing an upstream channel and/or downstream frequency different from what the modem is currently using, the modem MUST NOT send a Registration Request message to the BS. The modem MUST redo initial ranging using the configured upstream channel and/or downstream frequency per Section TBD.

#### 6.8.8.1 Registration

A CPE MUST be authorized to forward traffic into the network once it is initialized and configured. The CPE is authorized to forward traffic into the network via registration. To register with a BS, the CPE MUST

forward its configured class of service and any other operational parameters in the configuration file (refer to Section TBD) to the BS as part of a Registration Request. Figure TBD shows the procedure that **MUST** be followed by the CPE.

The configuration parameters downloaded to the CPE **MUST** include a network access control object (see Section TBD). If this is set to “no forwarding,” the CPE **MUST NOT** forward data from attached CPE to the network, yet the CPE **MUST** respond to network management requests. This allows the CPE to be configured in a mode in which it is manageable but will not forward data.

PRELIMINARY SUBMITTAL

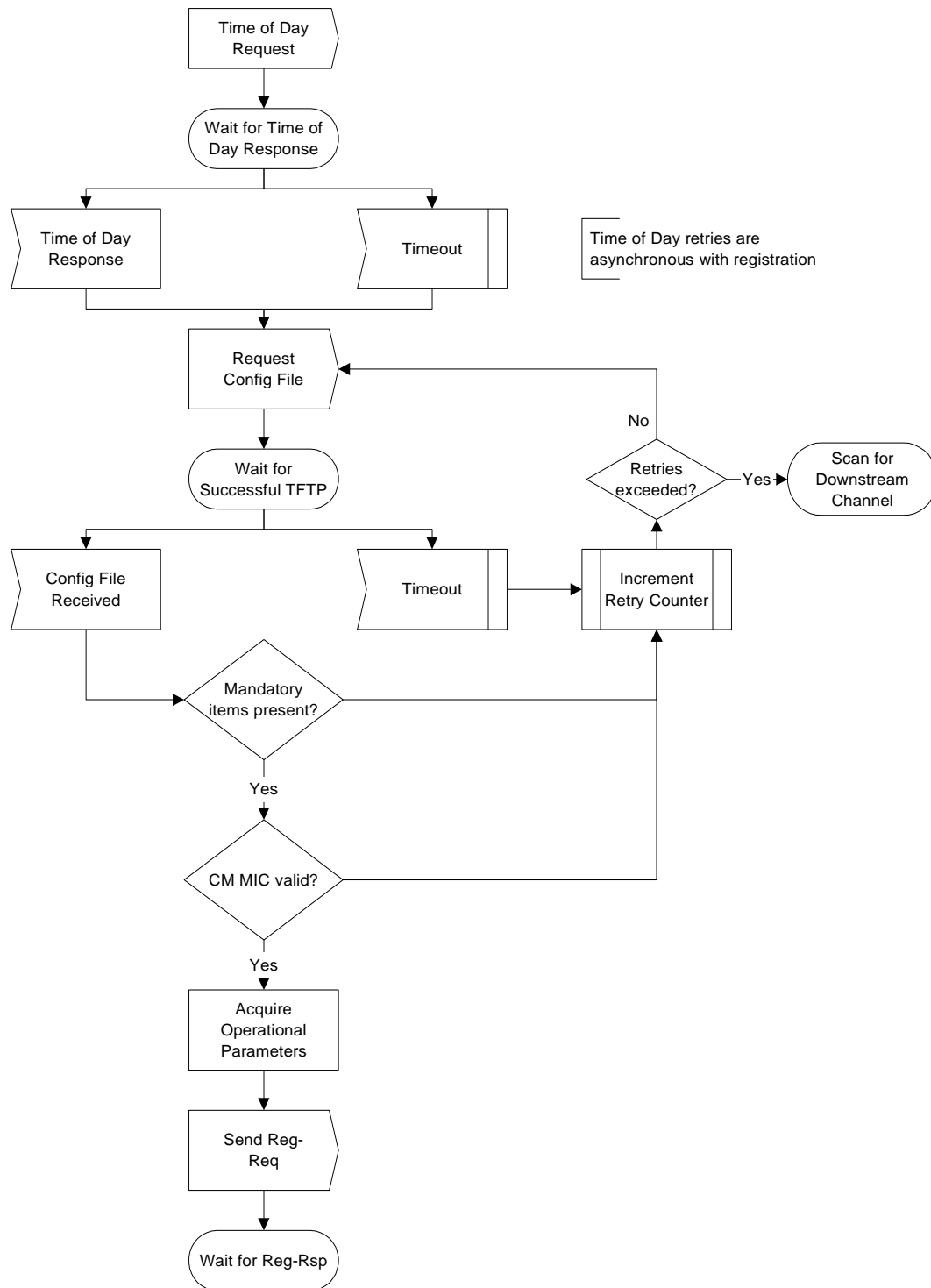
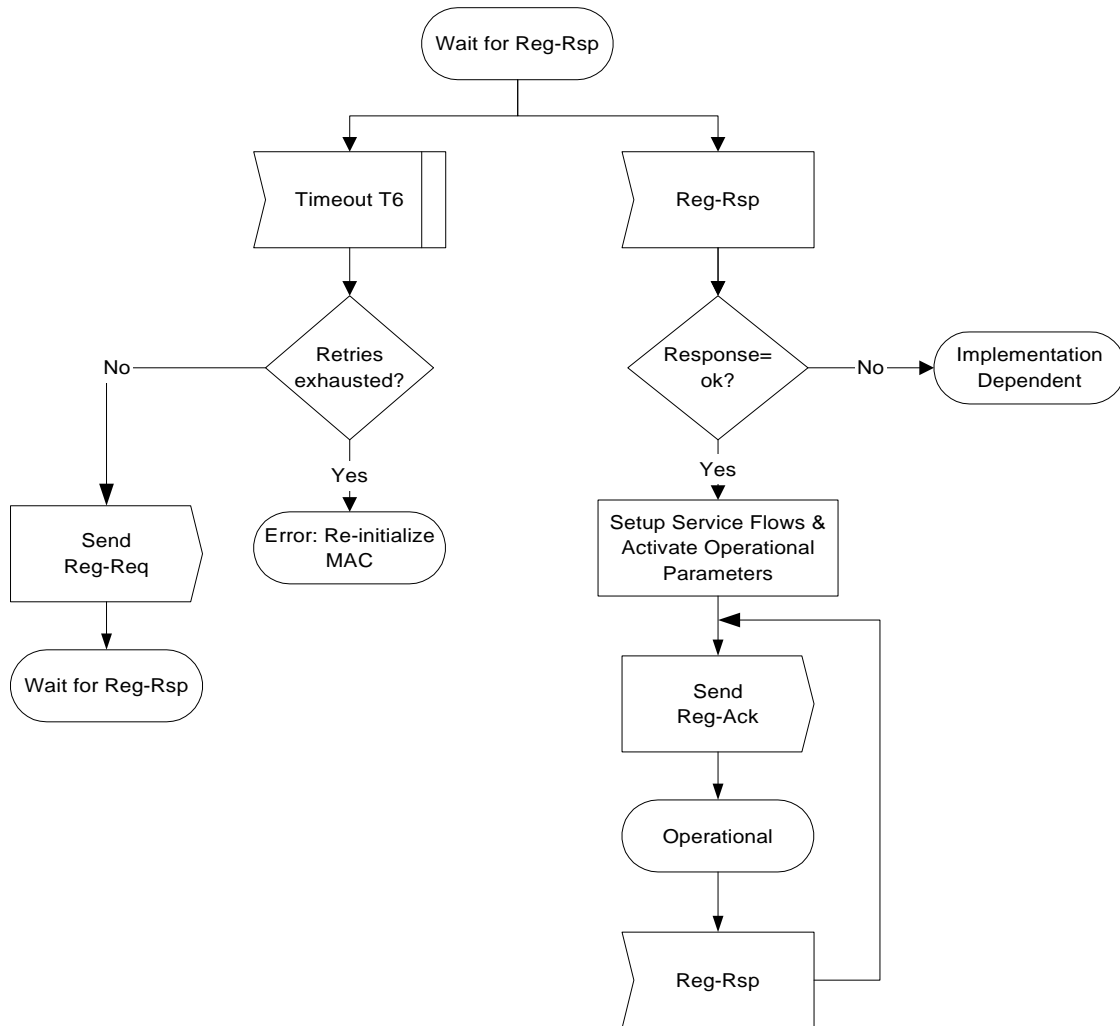


Figure 55—Registration — CPE

Once the CPE has sent a Registration Request to the BS it MUST wait for a Registration Response to authorize it to forward traffic to the network. Figure 56 shows the waiting procedure that MUST be followed by the CPE.



**Figure 56—Wait for Registration Response — CPE**

The BS MUST perform the following operations to confirm the CPE authorization (refer to Figure TBD):

- Calculate a MIC per TBD and compare it to the BS MIC included in the Registration Request. If the MIC is invalid, the BS MUST respond with an Authorization Failure.
- If present, check the TFTP Server Timestamp field. If the BS detects that the time is different from its local time by more than CPE Configuration Processing Time (refer to TBD), the BS MUST indicate authentication failure in the REG-RSP. The BS SHOULD also make a log entry stating the CPE MAC address from the message.
- If present, check the TFTP Server Provisioned Modem Address field. If the Provisioned Modem Address does not match the requesting modem's actual address, the BS MUST indicate authentication failure in the REG-RSP. The BS SHOULD also make a log entry stating the CPE MAC address from the message.

- d) If the Registration Request contains Service Flow encodings, verify the availability of the Quality of Service requested in the provisioned Service Flow(s). If unable to provide the Service Flow(s), the BS MUST respond with a Class of Service Failure and the appropriate Service Flow Response(s).
- e) Verify the availability of any Modem Capabilities requested. If unable or unwilling to provide the Modem Capability requested, the BS MUST turn that Modem Capability 'off' (refer to TBD).
- f) Assign a Service Flow ID for each class of service supported.
- g) Reply to the modem in a Registration Response.
- h) If the Registration Request contains Service Flow encodings, the BS MUST wait for a Registration Acknowledgment as shown in Figure TBD.

If timer T9 expires, the BS MUST both de-assign the temporary SID from that CPE and make some provision for aging out that SID.

PRELIMINARY SUBMITTAL

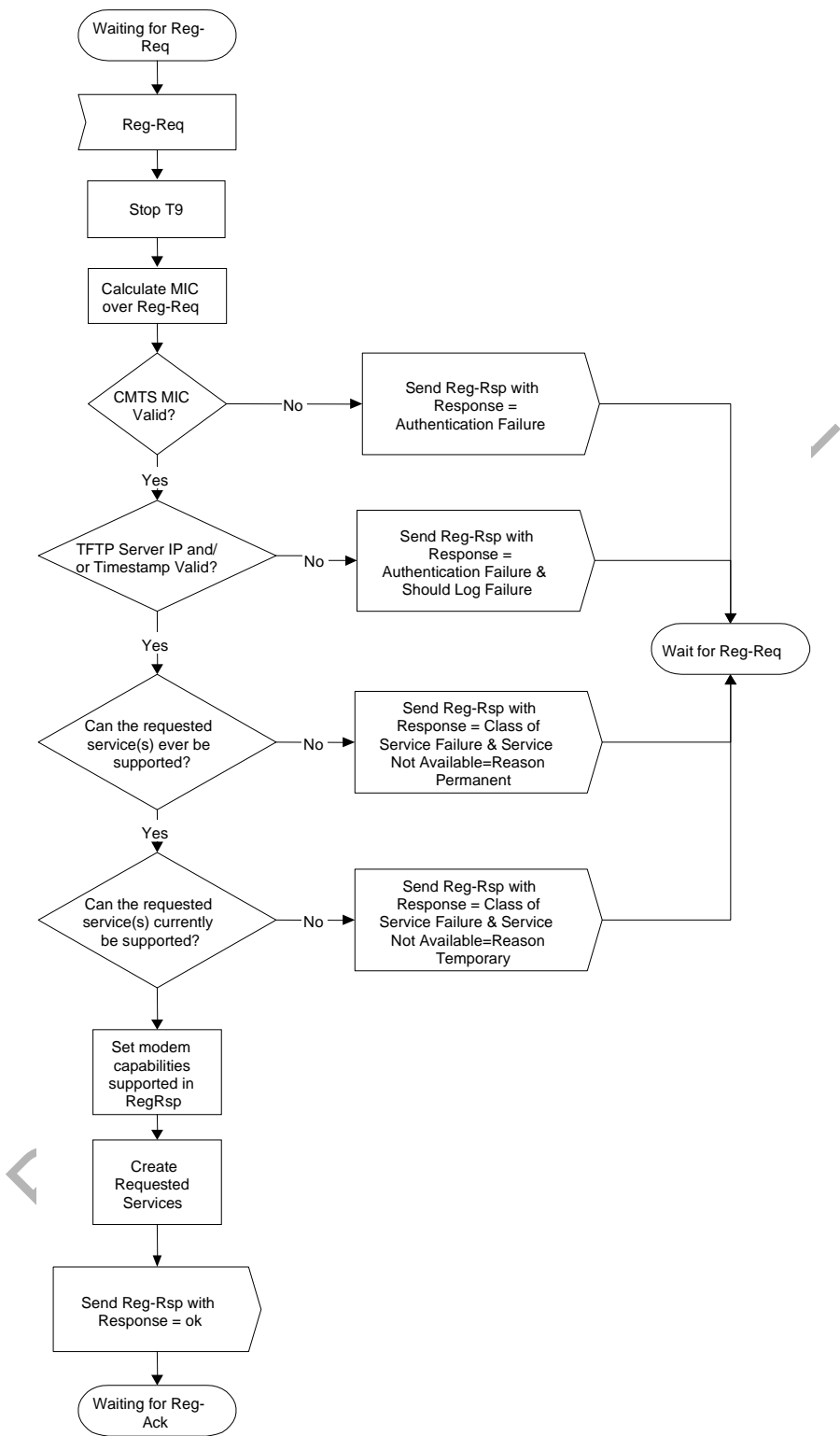
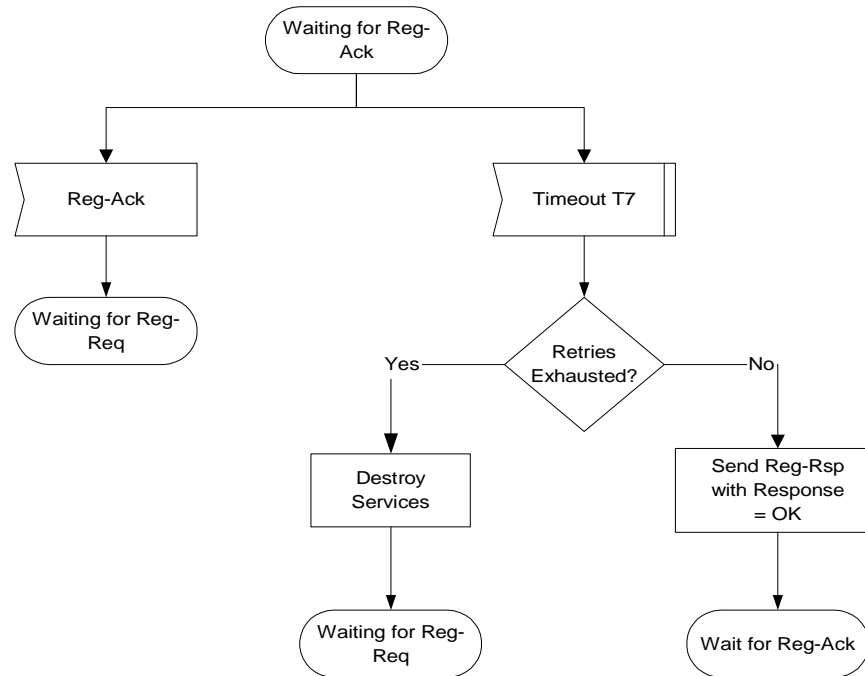


Figure 57—Registration — BS





**Figure 58—Registration Acknowledgment— BS**

#### 6.8.8.2 Baseline Privacy Initialization

Following registration, if the CPE is provisioned to run Baseline Privacy, the CPE MUST initialize Baseline Privacy operations, as described in [DOCSIS8]. A CPE is provisioned to run Baseline Privacy if its configuration file includes a Baseline Privacy Configuration Setting (section C.3.2) and if the Privacy Enable parameter (section TBD) is set to enable.

#### 6.8.8.3 Service IDs During CPE Initialization

After completion of the Registration process, the CPE will have been assigned Service Flow IDs (SFIDs) to match its provisioning. However, the CPE must complete a number of protocol transactions prior to that time (e.g., Ranging, DHCP, etc.), and requires a temporary Service ID in order to complete those steps.

On reception of an Initial Ranging Request, the BS MUST allocate a temporary SID and assign it to the CPE for initialization use. The BS MAY monitor use of this SID and restrict traffic to that needed for initialization. It MUST inform the CPE of this assignment in the Ranging Response.

On receiving a Ranging Response addressed to it, the CPE MUST use the assigned temporary SID for further initialization transmission requests until the Registration Response is received.

On receiving a Ranging Response instruction to move to a new downstream frequency and/or upstream channel ID, the CPE MUST consider any previously assigned temporary SID to be deassigned, and must obtain a new temporary SID via initial ranging.

It is possible that the Ranging Response may be lost after transmission by the BS. The CPE MUST recover by timing out and re-issuing its Initial Ranging Request. Since the CPE is uniquely identified by the source MAC address in the Ranging Request, the BS MAY immediately re-use the temporary SID previously assigned. If the BS assigns a new temporary SID, it MUST make some provision for aging out the old SID that went unused (see Section TBD).

When assigning provisioned SFIDs on receiving a Registration Request, the BS may re-use the temporary SID, assigning it to one of the Service Flows requested. If so, it MUST continue to allow initialization messages on that SID, since the Registration Response could be lost in transit. If the BS assigns all-new SIDs for class-of-service provisioning, it MUST age out the temporary SID. The aging-out MUST allow sufficient time to complete the registration process in case the Registration Response is lost in transit.

#### **6.8.8.4 Multiple-Channel Support**

In the event that more than one downstream signal is present in the system, the CPE MUST operate using the first valid downstream signal that it encounters when scanning. It will be instructed via the parameters in the configuration file to shift operation to different downstream and/or upstream frequencies if necessary.

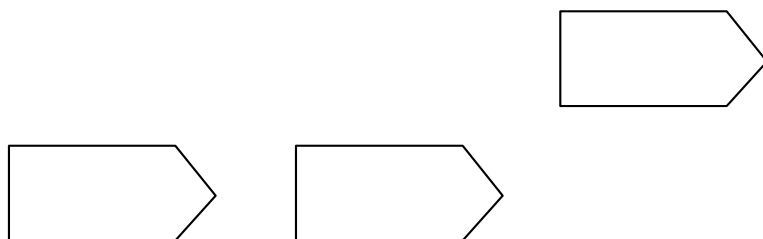
Both upstream and downstream channels MUST be identified where required in MAC management messages using channel identifiers.

### **6.9 Ranging**

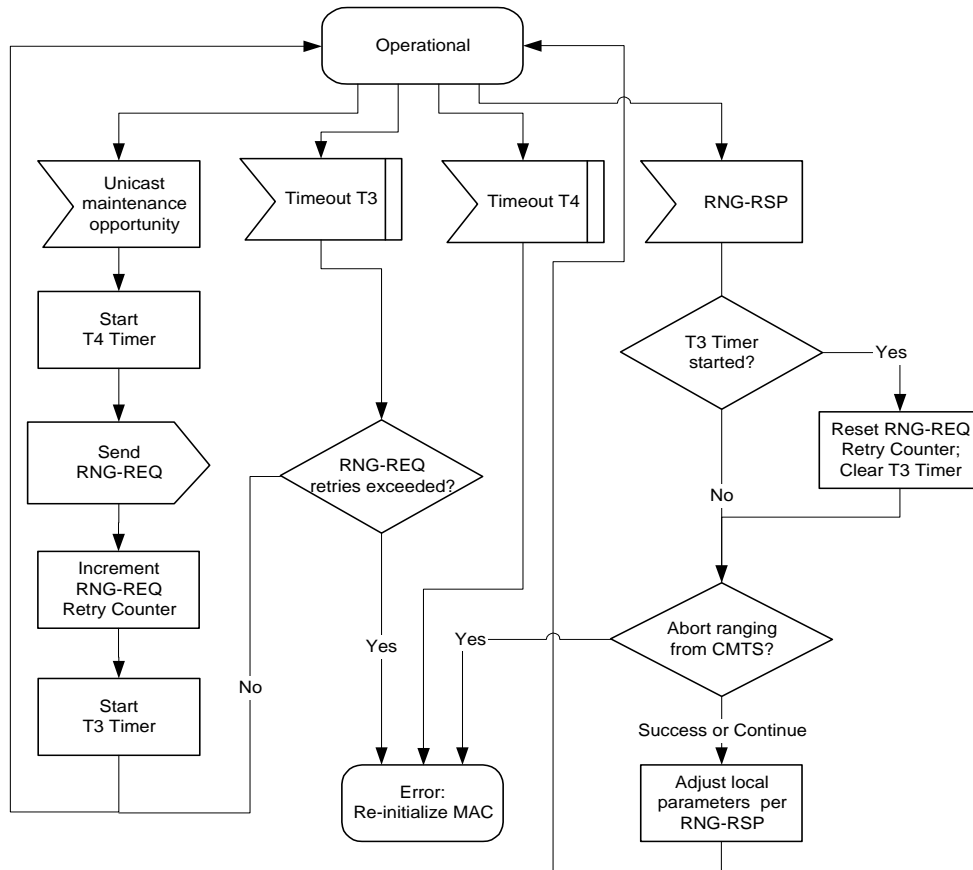
The BS MUST provide each CPE a Periodic Ranging opportunity at least once every T4 seconds. The BS MUST send out Periodic Ranging opportunities at an interval sufficiently shorter than T4 that a MAP could be missed without the CPE timing out. The size of this “subinterval” is BS dependent.

The CPE MUST reinitialize its MAC layer after T4 seconds have elapsed without receiving a Periodic Ranging opportunity.

Remote RF signal level adjustment at the CPE is performed through a periodic maintenance function using the RNG-REQ and RNG-RSP MAC messages. This is similar to initial ranging and is shown in Figure TBD and Figure TBD. On receiving a RNG-RSP, the CPE MUST NOT transmit until the RF signal has been adjusted in accordance with the RNG-RSP and has stabilized.



**Figure 59—Periodic Ranging - BS**



**Figure 60—Periodic Ranging - CPE**

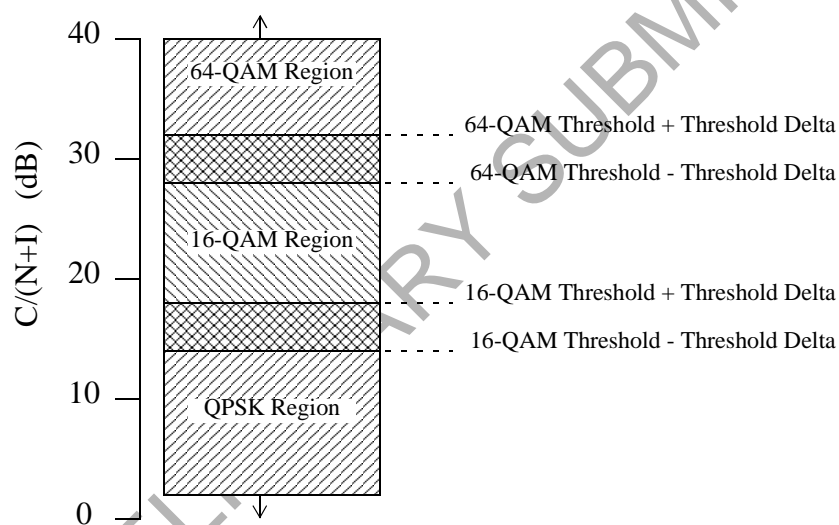
### 6.9.0.1 Downstream Modulation Management

The downstream modulation format (QPSK, 16-QAM or 64-QAM) is determined by the BS according to the signal quality of the signal that is received by each CPE. To reduce the volume of upstream traffic, the CPE monitors the carrier to noise and interference ratio (CNIR), and compares the averaged value against the allowed region of operation. This region is bounded by threshold levels. If the received CNIR goes outside of the allowed operating region, the CPE requests a change to a new modulation format using the RNG-REQ message. The BS acknowledges the receipt of the RNG-REQ message using the RNG-RSP message. The RNG-RSP message contains the new CPE operating modulation format, which can be either the same or different from the existing format.

The CPE applies an algorithm to determine its maximum operating modulation type in accordance with the 16 and 64-QAM Threshold parameters as established in the RNG-RSP message. The Threshold Delta parameter MUST be applied to the two threshold points in accordance with Figure 61. The Threshold Delta provides a hysteresis around which the CPE applies the thresholds.

**Table 14—Downstream Modulation Change Initiated from CPE**

BS		CPE
		DS Modulation Requires Modification
Receive RNG-REQ	<----- RNG-REQ ----->	Send RNG-REQ
Determine modulation type that is now appropriate		
Modify modulation type within provisioned limits established for CPE		
Send RNG-RSP	----- RNG-RSP ----->	Receive RNG-RSP
Begin using new modulation type for the CPE		

**Figure 61—Modulation Threshold Usage**

PRELIMINARY SUBMITTAL

## 6.10 Quality of Service

This standard defines several Quality of Service (QoS) related concepts. These include:

- a) Service Flow QoS Scheduling
- b) Dynamic Service Establishment
- c) Two-Phase Activation Model

### 6.10.1 Theory of Operation

The various BWA protocol mechanisms described in this document can be used to support Quality of Service (QoS) for both upstream and downstream traffic through the CPE and the BS. This section provides an overview of the QoS protocol mechanisms and their part in providing end-to-end QoS.

The requirements for Quality of Service include:

- a) A configuration and registration function for pre-configuring CPE-based **QoS Service Flows** and traffic parameters.
- b) A signaling function for dynamically establishing QoS-enabled Service Flows and traffic parameters
- c) A traffic-shaping and traffic-policing function for Service Flow-based traffic management, performed on traffic arriving from the upper layer service interface and outbound to the RF.
- d) Utilization of MAC scheduling and traffic parameters for upstream Service Flows.
- e) Utilization of QoS traffic parameters for downstream Service Flows.
- f) Grouping of Service Flow properties into named **Service Classes**, so upper layer entities and external applications (at both the CPE and BS) can request Service Flows with desired QoS parameters in a globally consistent way.

The principal mechanism for providing QoS is to associate packets traversing the RF MAC interface into a **Service Flow** as identified by the **Connection ID**. A Service Flow is a unidirectional flow of packets that is provided a particular Quality of Service. The CPE and BS provide this QoS by shaping, policing, and prioritizing traffic according to the **QoS Parameter Set** defined for the Service Flow.

The primary purpose of the Quality of Service features defined here is to define transmission ordering and scheduling on the air interface. However, these features often need to work in conjunction with mechanisms beyond the air interface in order to provide end-to-end QoS or to police the behavior of CPE modems.

Service Flows exist in both the upstream and downstream direction, and MAY exist without actually being activated to carry traffic. Service Flows have a 32-bit **Service Flow Identifier** (SFID) assigned by the BS. All Service Flows have an SFID; active upstream Service Flows also have a 16-bit **Connection Identifier** (CID).

At least two Service Flows must be defined in each configuration file: one for upstream and one for downstream service. The first upstream Service Flow describes the **Primary Upstream Service Flow**, and is the default Service Flow used for otherwise unclassified traffic and all MAC Messages. The first downstream Service Flow describes service to the **Primary Downstream Service Flow**. Additional Service Flows defined in the Configuration file create Service Flows that are provided QoS services.

### 6.10.2 Service Flows

A **Service Flow** is a MAC-layer transport service that provides unidirectional transport of packets either to upstream packets transmitted by the CPE or to downstream packets transmitted by the BS<sup>1</sup>. A Service Flow is characterized by a set of **QoS Parameters** such as latency, jitter, and throughput assurances. In order to standardize operation between the CPE and BS, these attributes include details of how the CPE requests upstream minislots and the expected behavior of the BS upstream scheduler.

A Service Flow is partially characterized by the following attributes<sup>2</sup>:

- a) **ServiceFlowID**: exists for all service flows
- b) **Connection ID**: only exists for admitted or active service flows
- c) **ProvisionedQoSParamSet**: defines a set of QoS Parameters which appears in the configuration file and is presented during registration. This MAY define the initial limit for authorizations allowed by the authorization module. The ProvisionedQoSParamSet is defined once when the Service Flow is created via registration.<sup>3</sup>
- d) **AdmittedQoSParamSet**: defines a set of QoS parameters for which the BS (and possibly the CPE) are reserving resources. The principal resource to be reserved is bandwidth, but this also includes any other memory or time-based resource required to subsequently activate the flow.
- e) **ActiveQoSParamSet**: defines set of QoS parameters defining the service actually being provided to the Service Flow. Only an Active Service Flow may forward packets.
- f) A Service Flow exists when the BS assigns a Service Flow ID (SFID) to it. The SFID serves as the principal identifier in the CPE and BS for the Service Flow. A Service Flow which exists has at least an SFID, and an associated Direction.
- g) The **Authorization Module** is a logical function within the BS that approves or denies every change to QoS Parameters and Classifiers associated with a Service Flow. As such it defines an “envelope” that limits the possible values of the AdmittedQoSParameterSet and ActiveQoSParameterSet.

The relationship between the QoS Parameter Sets is as shown in Figure 62 and Figure 63. The ActiveQoSParameterSet is always a subset<sup>4</sup> of the AdmittedQoSParameterSet which is always a subset of the authorized “envelope.” In the dynamic authorization model, this envelope is determined by the Authori-

<sup>1</sup>A Service Flow, as defined here, has no direct relationship to the concept of a “flow” as defined by the IETF’s Integrated Services (int-serv) Working Group [RFC-2212]. An intserv flow is a collection of packets sharing transport-layer endpoints. Multiple intserv flows can be served by a single Service Flow.

<sup>2</sup>Some attributes are derived from the above attribute list. The Service Class Name is an attribute of the ProvisionedQoSParamSet. The activation state of the Service Flow is determined by the ActiveQoSParamSet. If the ActiveQoSParamSet is null then the service flow is inactive.

<sup>3</sup>The ProvisionedQoSParamSet is null when a flow is created dynamically.

<sup>4</sup>To say that QoS Parameter Set A is a subset of QoS Parameter Set B the following MUST be true for all QoS Parameters in A and B:  
if (a smaller QoS parameter value indicates less resources, e.g. Maximum Traffic Rate)

A is a subset of B if the parameter in A is less than or equal to the same parameter in B

if (a larger QoS parameter value indicates less resources, e.g. Tolerated Grant Jitter)

A is a subset of B if the parameter in A is greater than or equal to the same parameter in B

if (the QoS parameter specifies a periodic interval, e.g. Nominal Grant Interval),

A is a subset of B if the parameter in A is an integer multiple of the same parameter in B

if (the QoS parameter is not quantitative, e.g. Service Flow Scheduling Type)

A is a subset of B if the parameter in A is equal to the same parameter in B



zation Module (labeled as the AuthorizedQoSParameterSet). In the provisioned authorization model, this envelope is determined by the ProvisionedQoSParameterSet.

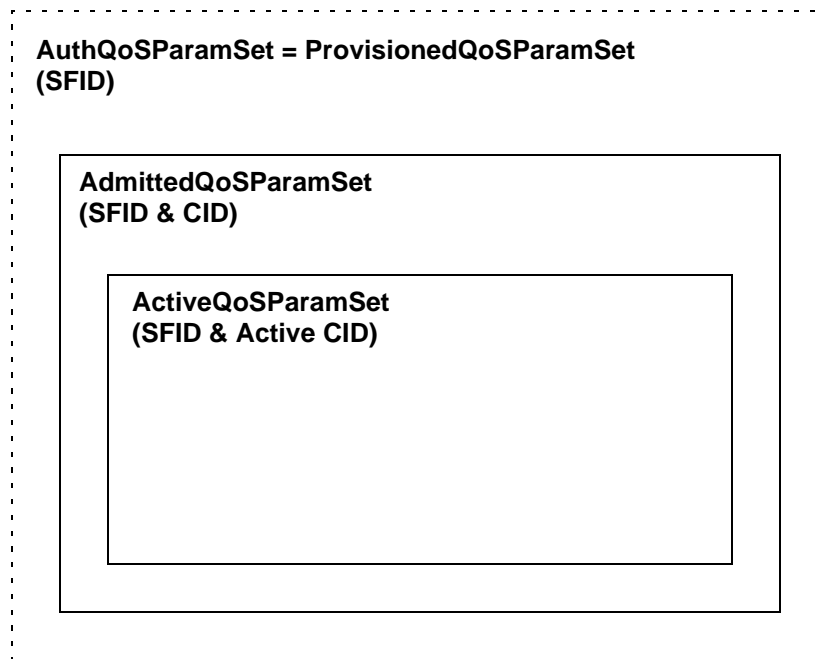
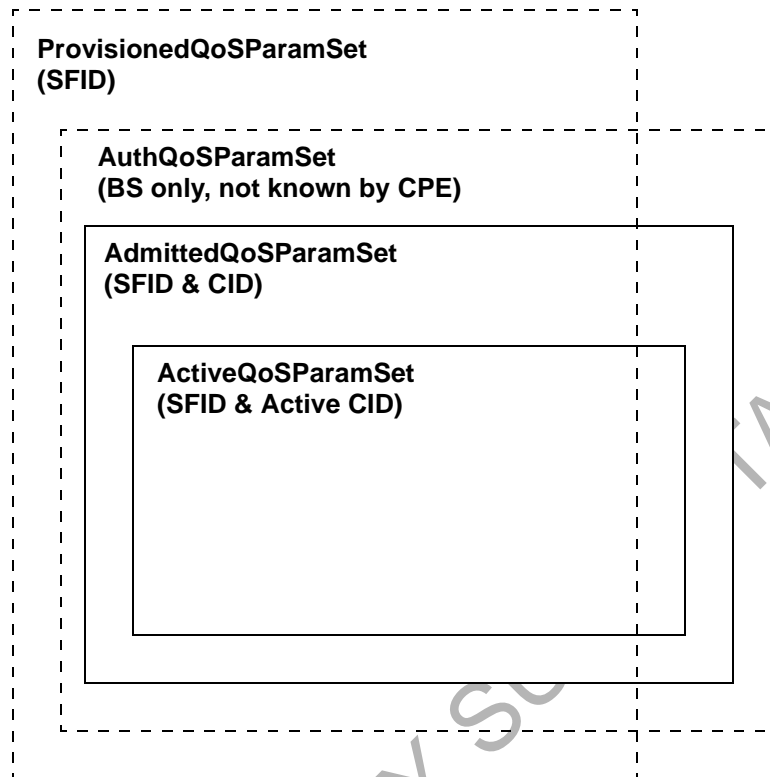


Figure 62—Provisioned Authorization Model “Envelopes”



**Figure 63—Dynamic Authorization Model “Envelopes”**

It is useful to think of three types of Service Flows:

- a) **Provisioned:** this type of Service Flow is known via provisioning through the configuration file, its AdmittedQoSParamSet and ActiveQoSParamSet are both null.
- b) **Admitted:** this type of Service Flow has resources reserved by the BS for its AdmittedQoSParamSet, but these parameters are not active (its ActiveQoSParamSet is null). **Admitted Service Flows** may have been provisioned or may have been signalled by some other mechanism.
- c) **Active:** this type of Service Flow has resources committed by the BS for its QoS Parameter Set, (e.g. is actively sending MAPs containing unsolicited grants for a UGS-based service flow). Its ActiveQoSParamSet is non-null.

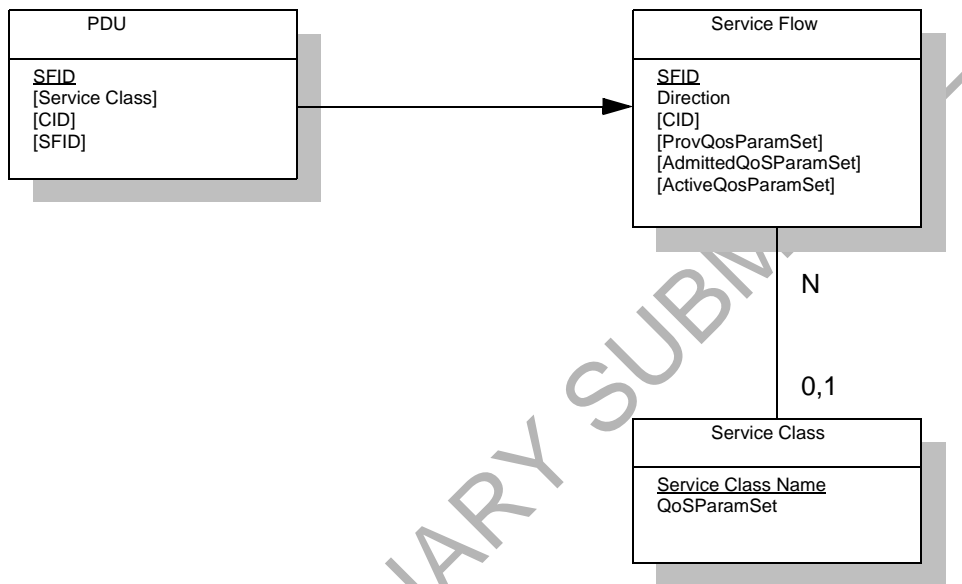
### 6.10.3 Object Model (FIX THIS SECTION)

The major objects of the architecture are represented by named rectangles in Figure 5-43. Each object has a number of attributes; the attribute names which uniquely identify the object are underlined. Optional attributes are denoted with brackets. The relationship between the number of objects is marked at each end of the association line between the objects. For example, a Service Flow may be associated with from 0 to 65535 Classifiers, but a Classifier is associated with exactly one Service flow.

The Service Flow is the central concept of the MAC protocol. It is uniquely identified by a 32-bit Service Flow ID (SFID) assigned by the BS. Service Flows may be in either the upstream or downstream direction. Admitted Upstream Service Flows are assigned a 14-bit Service ID (SID).

Outgoing user data is submitted to the MSAP by an convergence sub-layer process for transmission on the MAC interface. The information delivered to the MSAP includes the Connection Identifier identifying the connection across which the information is delivered. The Service Flow for the connection is mapped via the Connection ID (CID).

The Service Class is an optional object that may be implemented at the BS. It is referenced by an ASCII name which is intended for provisioning purposes. A Service Class is defined in the BS to have a particular QoS Parameter Set. The QoS Parameter Sets of a Service Flow may contain a reference to the Service Class Name as a “macro” that selects all of the QoS parameters of the Service Class. The Service Flow QoS Parameter Sets may augment and even override the QoS parameter settings of the Service Class, subject to authorization by the BS.



**Figure 64—Theory of Operation Object Model**

#### 6.10.4 Service Classes

The Service Class serves the following purposes:

- 1) It allows operators, who so wish, to move the burden of configuring service flows from the provisioning server to the BS. Operators provision the modems with the Service Class Name; the implementation of the name is configured at the BS. This allows operators to modify the implementation of a given service to local circumstances without changing modem provisioning. For example, some scheduling parameters may need to be tweaked differently for two different Bss to provide the same service. As another example, service profiles could be changed by time of day.
- 2) It allows BS vendors to provide class-based-queuing if they choose, where service flows compete within their class and classes compete with each other for bandwidth.
- 3) It allows higher-layer protocols to create a Service Flow by its Service Class Name. For example, telephony signaling may direct the CPE to instantiate any available Provisioned Service Flow of class “G711”.

**Note: The Service Class is optional: the flow scheduling specification may always be provided in full; a service flow may belong to no service class whatsoever. BS implementations MAY treat such “unclassified” flows differently from “classified” flows with equivalent parameters.**

Any Service Flow MAY have its QoS Parameter Set specified in any of three ways:

- a) By explicitly including all traffic parameters.
- b) By indirectly referring to a set of traffic parameters by specifying a Service Class Name.
- c) By specifying a Service Class Name along with modifying parameters.

The Service Class Name is “expanded” to its defined set of parameters at the time the BS successfully admits the Service Flow. The Service Class expansion can be contained in the following BS-originated Messages: Registration Response, DSA-REQ, DSC-REQ, DSA-RSP and DSC-RSP. In all of these cases, the BS MUST include a Service Flow Encoding that includes the Service Class Name and the QoS Parameter Set of the Service Class. If a CPE-initiated request contained any supplemental or overriding Service Flow parameters, a successful response MUST also include these parameters.

When a Service Class name is given in an admission or activation request, it is possible that the returned QoS Parameter Set MAY change from activation to activation. This can happen because of administrative changes to the Service Class’ QoS Parameter Set at the BS. If the definition of a Service Class Name is changed at the BS (e.g. its associated QoS Parameter Set is modified), it has no effect on the QoS Parameters of existing Service Flows associated with that Service Class. A BS MAY initiate DSC transactions to existing Service Flows which reference the Service Class Name to affect the changed Service Class definition.

When a CPE uses the Service Class Name to specify the Admitted QoS Parameter Set, the expanded set of TLV encodings of the Service Flow will be returned to the CPE in the response Message (REG-RSP, DSA-RSP, or DSC-RSP). Use of the Service Class Name later in the activation request MAY fail if the definition of the Service Class Name has changed and the new required resources are not available. Thus, the CPE SHOULD explicitly request the expanded set of TLVs from the response Message in its later activation request.

### 6.10.5 Authorization

Every change to the Service Flow QoS Parameters MUST be approved by an authorization module. This includes every REG-REQ or DSA-REQ Message to create a new Service Flow, and every DSC-REQ Message to change a QoS Parameter Set of an existing Service Flow. Such changes include requesting an admission control decision (e.g. setting the AdmittedQoSParamSet) and requesting activation of a Service Flow (e.g. setting the ActiveQoSParameterSet). Reduction requests regarding the resources to be admitted or activated are also checked by the authorization module, as are requests to add or change the Classifiers.

In the static authorization model, the authorization module receives all registration Messages, and stores the provisioned status of all “deferred” Service Flows. Admission and activation requests for these provisioned service flows will be permitted, as long as the Admitted QoS Parameter Set is a subset of the Provisioned QoS Parameter Set, and the Active QoS Parameter Set is a subset of the Admitted QoS Parameter Set. Requests to change the Provisioned QoS Parameter Set will be refused, as will requests to create new dynamic Service Flows. This defines a static system where all possible services are defined in the initial configuration of each CPE.

In the dynamic authorization model, the authorization module not only receives all registration Messages, but also communicates through a separate interface to an independent policy server. This policy server may provide to the authorization module advance notice of upcoming admission and activation requests, and specifies the proper authorization action to be taken on those requests. Admission and activation requests from a CPE are then checked by the Authorization Module to ensure that the ActiveQoSParameterSet being requested is a subset of the set provided by the policy server. Admission and activation requests from a CPE

that are signalled in advance by the external policy server are permitted. Admission and activation requests from a CPE that are not pre-signalled by the external policy server may result in a real-time query to the policy server, or may be refused.

During registration, the CPE **MUST** send to the BS the authenticated set of TLVs derived from its configuration file which defines the Provisioned QoS Parameter Set. Upon receipt and verification at the BS, these are handed to the Authorization Module within the BS. The BS **MUST** be capable of caching the Provisioned QoS Parameter Set, and **MUST** be able to use this information to authorize dynamic flows which are a subset of the Provisioned QoS Parameter Set. The BS **SHOULD** implement mechanisms for overriding this automated approval process (such as described in the dynamic authorization model). For example:

- a) Deny all requests whether or not they have been pre-provisioned
- b) Define an internal table with a richer policy mechanism but seeded by the configuration file information
- c) Refer all requests to an external policy server

### 6.10.6 Types of Service Flows

It useful to think about three basic types of Service Flows. This section describes these three types of Service Flows in more detail. However, it is important to note that there are more than just these three basic types. (Refer to Appendix C.2.2.5.1)

#### 6.10.6.1 Provisioned Service Flows

A Service Flow may be Provisioned but not immediately activated (sometimes called “deferred”). That is, the description of any such service flow in the TFTP configuration file contains an attribute which provisions but defers activation and admission (refer to Appendix C.2.2.5.1). During Registration, the BS assigns a Service Flow ID for such a service flow but does not reserve resources. The BS **MAY** also require an exchange with a policy module prior to admission.

As a result of external action beyond the scope of this specification, the CPE **MAY** choose to activate a Provisioned Service Flow by passing the Service Flow ID and the associated QoS Parameter Sets. The CPE **MUST** also provide any applicable Classifiers. If authorized and resources are available, the BS **MUST** respond by assigning a SID for the upstream Service Flow. The BS **MAY** deactivate the Service Flow, but **SHOULD NOT** delete the Service Flow during the CPE registration epoch.

As a result of external action beyond the scope of this specification (e.g. [PKTCBL-MGCP]), the BS **MAY** choose to activate a Service Flow by passing the Service Flow ID as well as the SID and the associated QoS Parameter Sets. The BS **MUST** also provide any applicable Classifiers. The BS **MAY** deactivate the Service Flow, but **SHOULD NOT** delete the Service Flow during the CPE registration epoch. Such a Provisioned Service Flow **MAY** be activated and deactivated many times (through DSC exchanges). In all cases, the original Service Flow ID **MUST** be used when reactivating the service flow.

#### 6.10.6.2 Admitted Service Flows

This protocol supports a two-phase activation model which is often utilized in telephony applications. In the two-phase activation model, the resources for a “call” are first “admitted,” and then once the end-to-end negotiation is completed (e.g. called party’s gateway generates an “off-hook” event) the resources are “activated.” Such a two-phase model serves the purposes a) of conserving network resources until a complete end-to-end connection has been established, b) performing policy checks and admission control on resources as quickly as possible, and, in particular, before informing the far end of a connection request, and c) preventing several potential theft-of-service scenarios.

For example, if an upper layer service were using unsolicited grant service, and the addition of upper-layer flows could be adequately provided by increasing the Grants Per Interval QoS parameter, then the following might be used. When the first upper-layer flow is pending, the CPE issues a DSA-Request with the Admit Grants Per Interval parameter equal one, and the Activate Grants Per Interval parameter equal zero. Later when the upper-layer flow becomes active, it issues a DSC-Request with the instance of the Activate Grants-per-Interval parameter equal to one. Admission control was performed at the time of the reservation, so the later DSC-Request, having the Activate parameters within the range of the previous reservation, is guaranteed to succeed. Subsequent upper-layer flows would be handled in the same way. If there were three upper-layer flows establishing connections, with one flow already active, the Service Flow would have Admit(ted) Grants-per-Interval equal four, and Active Grants-per-Interval equal one.

An activation request of a Service Flow where the new ActiveQoSParamSet is a subset of the AdmittedQoSParamSet and no new classifiers are being added MUST be allowed (except in the case of catastrophic failure). An admission request where the AdmittedQoSParamSet is a subset of the previous AdmittedQoSParamSet, so long as the ActiveQoSParamSet remains a subset of the AdmittedQoSParameterSet, MUST succeed.

A Service Flow that has resources assigned to its AdmittedQoSParamSet, but whose resources are not yet completely activated, is in a transient state. A timeout value MUST be enforced by the BS that requires Service Flow activation within this period. (Refer to Appendix C.2.2.5.8) If Service Flow activation is not completed within this interval, the assigned resources in excess of the active QoS parameters MUST be released by the BS.

It is possible in some applications that a long-term reservation of resources is necessary or desirable. For example, placing a telephone call on hold should allow any resources in use for the call to be temporarily allocated to other purposes, but these resources must be available for resumption of the call later. The AdmittedQoSParamSet is maintained as “soft state” in the BS; this state MUST be refreshed periodically for it to be maintained without the above timeout releasing the non-activated resources. This refresh MAY be signalled with a periodic DSC-REQ Message with identical QoS Parameter Sets, or MAY be signalled by some internal mechanism within the BS outside of the scope of this specification (e.g. by the BS monitoring RSVP refresh Messages).

#### 6.10.6.3 Active Service Flows

A Service Flow that has a non-NULL set of ActiveQoSParameters is said to be an Active Service Flow. It is requesting<sup>5</sup> and being granted bandwidth for transport of data packets. An admitted Service Flow may be made active by providing an ActiveQoSParameterSet, signaling the resources actually desired at the current time. This completes the second stage of the two-phase activation model. (Refer to Section 5.3.6.1.5.2)

A Service Flow may be Provisioned and immediately activated. This is the case for the Primary Service Flows. It is also typical of Service Flows for monthly subscription services, etc. These Service Flows are established at registration time and MUST be authorized by the BS MIC. These Service Flows MAY also be authorized by the BS authorization module.

Alternatively, a Service Flow may be created dynamically and immediately activated. In this case, two-phase activation is skipped and the Service Flow is available for immediate use upon authorization.

#### 6.10.6.4 Service Flows and Classifiers

The basic model is that the Classifiers associate packets into exactly one Service Flow. The Service Flow Encodings provide the QoS Parameters for treatment of those packets on the RF interface. These encodings are described in Appendix C.2.

<sup>5</sup>According to its Request/Transmission Policy (refer to C.2.2.6.3)

In the upstream direction, the CPE MUST classify upstream packets to Active Service Flows. The BS MUST classify downstream traffic to Active Downstream Service Flows. There MUST be a default downstream service flow for otherwise unclassified broadcast and multicast traffic.

The BS polices packets in upstream Service Flows to ensure the integrity of the QoS Parameters and the packet's TOS value. When the rate at which packets are sent is greater than the policed rate at the BS, then these packets MAY be dropped by the BS (refer to C.2.2.5.3). When the value of the TOS byte is incorrect, the BS (based on policy) MUST police the stream by overwriting the TOS byte (refer to C.2.2.6.10).

It may not be possible for the CPE to forward certain upstream packets on certain Service Flows. In particular, a Service Flow using unsolicited grant service with fragmentation disabled cannot be used to forward packets larger than the grant size. If a packet is classified to a Service Flow on which it cannot be transmitted, the CPE MUST either transmit the packet on the Primary Service Flow or discard the packet depending on the Request/ Transmission Policy of the Service Flow to which the packet was classified.

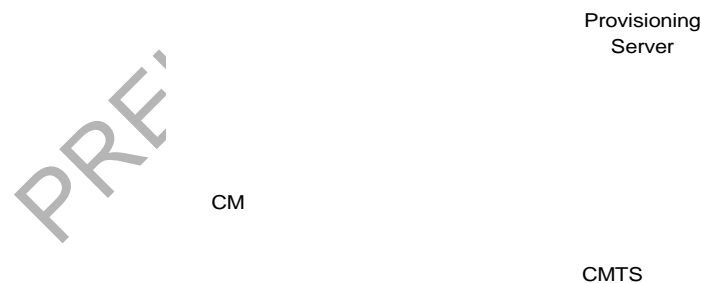
MAC Management Messages are not subject to classification and are not part of any service flow. Although MAC Management Messages are transferred on the Primary Service Flow, they MUST be excluded from any QoS calculations of the Primary Service Flow. Delivery of MAC Management Messages is implicitly influenced by the attributes of the associated service flow.

## 6.10.7 General Operation

### 6.10.7.1 Static Operation

Static configuration of Classifiers and Service Flows uses the Registration process. A provisioning server provides the CPE with configuration information. The CPE passes this information to the BS in a Registration Request. The BS adds information and replies with a Registration Response. The CPE sends a Registration Acknowledge to complete registration.

### 6.10.7.2 Dynamic Operation



**Figure 65—Registration Message Flow**

A TFTP configuration file consists of one or more instances of Classifiers and Service Flow Encodings. Classifiers are loosely ordered by 'priority'. Each Classifier refers to a Service Flow via a 'service flow ref-

erence'. Several Classifiers may refer to the same Service Flow. Additionally, more than one Classifier may have the same priority, and in this case, the particular classifier used is not defined.

**Table 15—TFTP File Contents**

Items	Service Flow Reference	Service Flow ID
<b>Service Flow Encodings</b> Immediate activation requested, upstream	1..m	None Yet
<b>Service Flow Encodings</b> Provisioned for later activation requested, upstream	(m+1)..n	None Yet
<b>Service Flow Encodings</b> Immediate activation requested, downstream	(n+1)..p	None Yet
<b>Service Flow Encodings</b> Provisioned for later activation requested, downstream	(p+1)..q	None Yet

Service Flow Encodings contain either a full definition of service attributes (omitting defaultable items if desired) or a service class name. A service class name is an ASCII string which is known at the BS and which indirectly specifies a set of QoS Parameters. (Refer to Section 5.3.6.1.3 and C.2.2.3.4)

**Note: At the time of the TFTP configuration file, Service Flow References exist as defined by the provisioning server. Service Flow Identifiers do not yet exist because the BS is unaware of these service flow definitions.**

The Registration Request packet contains Downstream Classifiers (if to be immediately activated) and all Inactive Service Flows. The configuration file, and thus, the Registration Request, generally does not contain a Downstream Classifier if the corresponding Service Flow is requested with deferred activation. This allows for late binding of the Classifier when the Flow is activated.

**Table 16—Registration Request Contents**

Items	Service Flow	Service Flow ID
<b>Service Flow Encodings</b> Immediate activation requested, upstream May specify explicit attributes or service class name	1..m	None Yet
<b>Service Flow Encodings</b> Provisioned for later activation requested, upstream Explicit attributes or service class name	(m+1)..n	None Yet
<b>Service Flow Encodings</b> Immediate activation requested, downstream Explicit attributes or service name	(n+1)..p	None Yet
<b>Service Flow Encodings</b> Provisioned for later activation requested, downstream Explicit attributes or service name	(p+1)..q	None Yet



The Registration Response sets the QoS Parameter Sets according to the Quality of Service Parameter Set Type in the Registration Request.

The Registration Response preserves the Service Flow Reference attribute, so that the Service Flow Reference can be associated with SFID and/or SID.

**Table 17—Registration Response Contents**

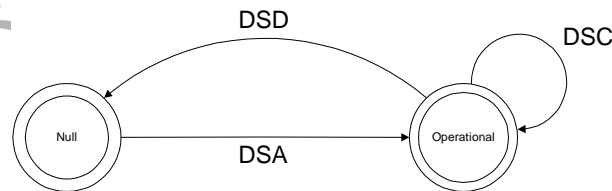
Items	Service Flow Reference	Service Flow Identifier	Service Identifier
Active Upstream Service Flows Explicit attributes	1..m	SFID	SID
Provisioned Upstream Service Flows Explicit attributes	(m+1)..n	SFID	Not Yet
Active Downstream Service Flows Explicit attributes	(n+1)..p	SFID	N/A
Provisioned Downstream Service Flows Explicit attributes	(p+1)..q	SFID	N/A

The SFID is chosen by the BS to identify a downstream or upstream service Flow that has been authorized but not activated. A DSC-Request from a modem to admit or activate a Provisioned Service Flow contains its SFID. If it is a downstream Flow then the Downstream Classifier is also included.

## 6.10.8 Dynamic Service

### 6.10.8.1 Connection Establishment

Service Flows MAY be created, changed or deleted. This is accomplished through a series of MAC management Messages referred to as Dynamic Service Addition (DSA), Dynamic Service Change (DSC) and Dynamic Service Deletion (DSD). The DSA Messages create a new Service Flow. The DSC Messages change an existing Service Flow. The DSD Messages delete an existing Service Flow. This is illustrated in Figure 66.



**Figure 66—Dynamic Service Flow Overview**

The Null state implies that no Service Flow exists that matches the SFID and/or TransactionID in a Message. Once the Service Flow exists, it is operational and has an assigned SFID. In steady state operation, a Service Flow resides in a Nominal state. When Dynamic Service messaging is occurring, the Service Flow may transition through other states, but remains operational. Since multiple Service Flows MAY exist, there may be multiple state machines active, one for every Service Flow. Dynamic Service Messages only affect those state machines that match the SFID and/or Transaction ID. If privacy is enabled, both the CPE and BS

MUST verify the HMAC digest on all dynamic service Messages before processing them, and discard any Messages that fail.

Service Flows created at registration time effectively enter the SF\_operational state without a DSA transaction.

TransactionIDs are unique per transaction and are selected by the initiating device (CPE or BS). To help prevent ambiguity and provide simple checking, the TransactionID number space is split between the CPE and BS. The CPE MUST select its TransactionIDs from the first half of the number space (0x0000 to 0x7FFF). The BS MUST select its TransactionIDs from the second half of the number space (0x8000 to 0xFFFF).

Each dynamic service Message sequence is a unique transaction with an associated unique transaction identifier. The DSA/DSC transactions consist of a request/response/acknowledge sequence. The DSD transactions consist of a request/response sequence. The response Messages will return a confirmation code of okay unless some exception condition was detected. The acknowledge Messages will return the confirmation code in the response unless a new exception condition arises. A more detailed state diagram, including transition states, is shown below. The detailed actions for each transaction will be given in the following sections.

#### Dynamic Service Flow State Transitions

The Dynamic Service Flow State Transition Diagram is the top-level state diagram and controls the general Service Flow state. As needed, it creates transactions, each represented by a Transaction state transition diagram, to provide the DSA, DSC, and DSD signaling. Each Transaction state transition diagram only communicates with the parent Dynamic Service Flow State Transition Diagram. The top-level state transition diagram filters Dynamic Service Messages and passes them to the appropriate transaction based on Service Flow Identifier (SFID), Service Flow Reference number, and TransactionID.

There are six different types of transactions: locally initiated or remotely initiated for each of the DSA, DSC and DSD Messages. Most transactions have three basic states: pending, holding and deleting. The pending state is typically entered after creation and is where the transaction is waiting for a reply. The holding state is typically entered once the reply is received, the purpose of this state is to allow for retransmissions in case of a lost Message, even though the local entity has perceived that the transaction has completed. The deleting state is only entered if the Service Flow is being deleted while a transaction is being processed.

The flow diagrams provide a detailed representation of each of the states in the Transaction state transition diagrams. All valid transitions are shown. Any inputs not shown should be handled as a severe error condition.

With one exception, these state diagrams apply equally to the BS and CPE. In the Dynamic Service Flow Changing-Local state, there is a subtle difference in the CPE and BS behaviors. This is called out in the state transition and detailed flow diagrams.

[Note: The 'Num Xacts' variable in the Dynamic Service Flow State Transition Diagram is incremented every time the top-level state diagram creates a transaction and is decremented every time a transaction terminates. A Dynamic Service Flow MUST NOT return to the Null state until it's deleted and all transactions have terminated.]

The inputs for the state diagrams are identified below.

Dynamic Service Flow State Transition Diagram inputs from unspecified local, higher-level entities:

- a) Add
- b) Change

- c) Delete

Dynamic Service Flow State Transition Diagram inputs from DSx Transaction State Transition diagrams:

- a) DSA Succeeded
- b) DSA Failed
- c) DSA ACK Lost
- d) DSA Erred
- e) DSA Ended

- a) DSC Succeeded
- b) DSC Failed
- c) DSC ACK Lost
- d) DSC Erred
- e) DSC Ended

- a) DSD Succeeded
- b) DSD Erred
- c) DSD Ended

DSx Transaction State Transition diagram inputs from the Dynamic Service Flow State Transition Diagram”

- a) SF Add
- b) SF Change
- c) SF Delete

- a) SF Abort Add
- b) SF Change-Remote
- c) SF Delete-Local
- d) SF Delete-Remote

- a) SF DSA-ACK Lost
- b) SF-DSC-REQ Lost
- c) SF-DSC-ACK Lost
- d) SF DSC-REQ Lost

- a) SF Changed
- b) SF Deleted

The creation of DSx Transactions by the Dynamic Service Flow State Transition Diagram is indicated by the notation

DSx-[ Local | Remote ] ( initial\_input )

where initial\_input may be SF Add, DSA-REQ, SF Change, DSC-REQ, SF Delete, or DSD-REQ depending on the transaction type and initiator.

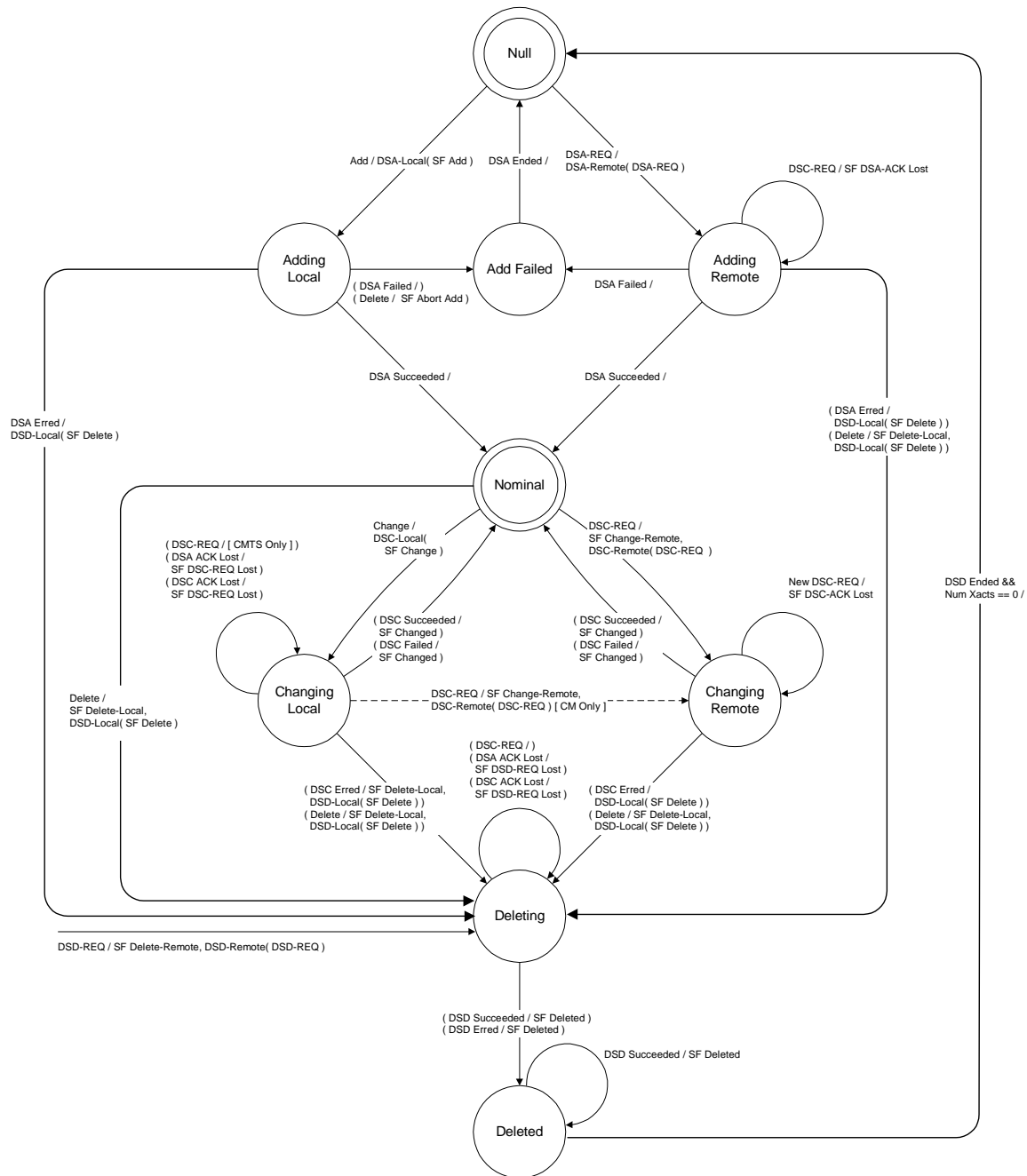
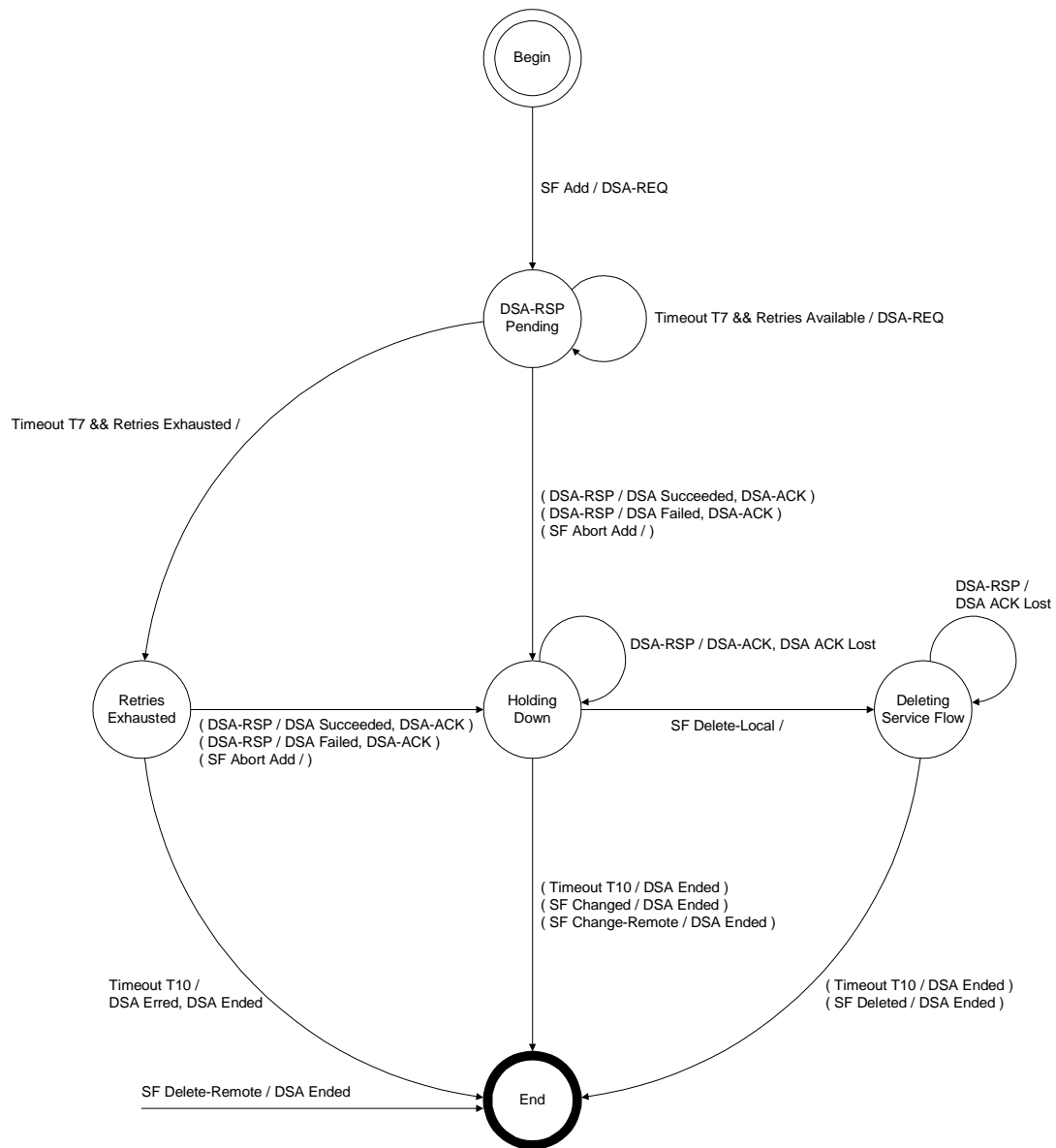
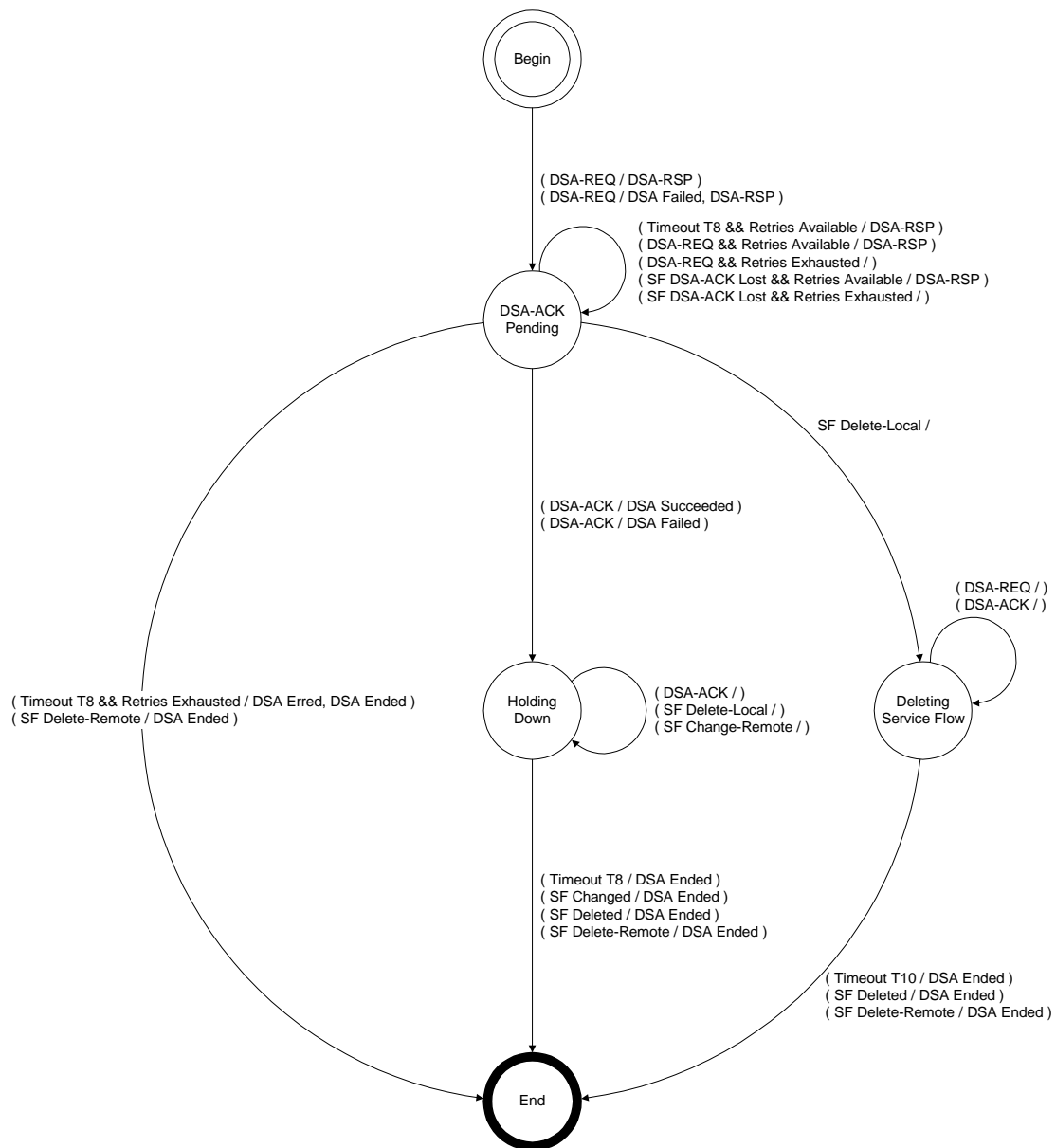


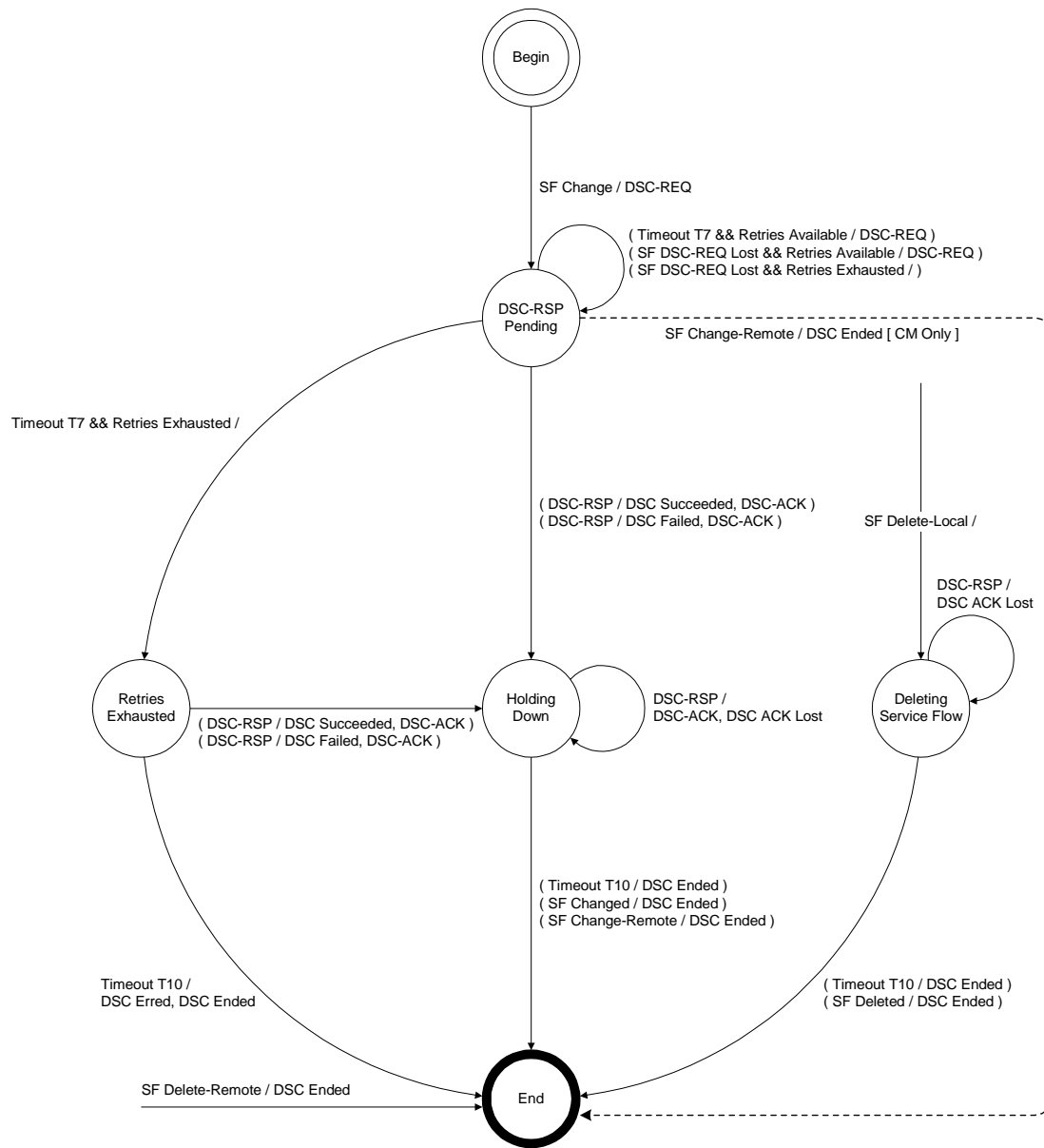
Figure 67—Dynamic Service Flow State Transition Diagram



**Figure 68—DSA - Locally Initiated Transaction State Transition Diagram**



**Figure 69—DSA - Remotely Initiated Transaction State Transition Diagram**



**Figure 70—DSC - Locally Initiated Transaction State Transition Diagram**

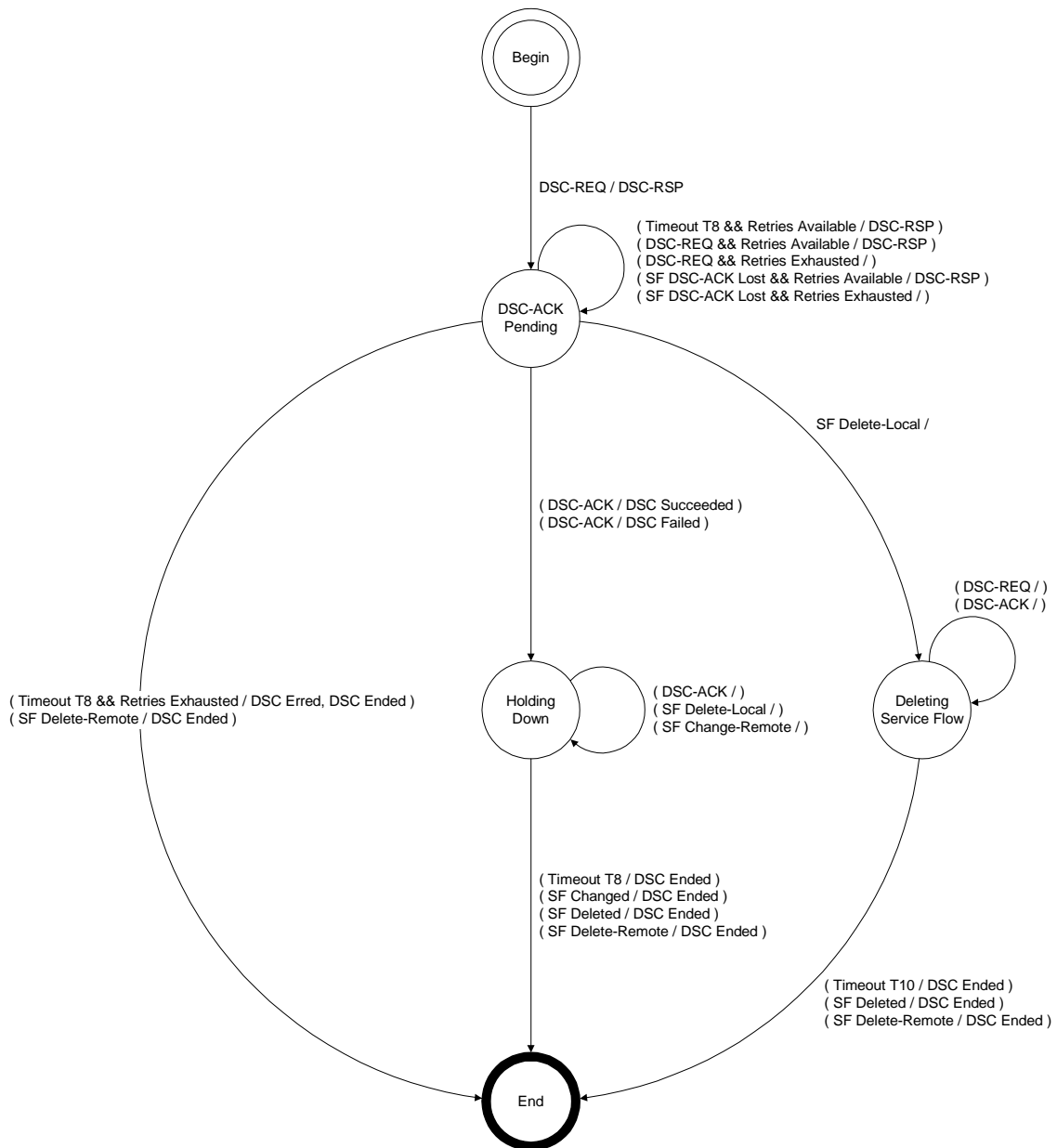
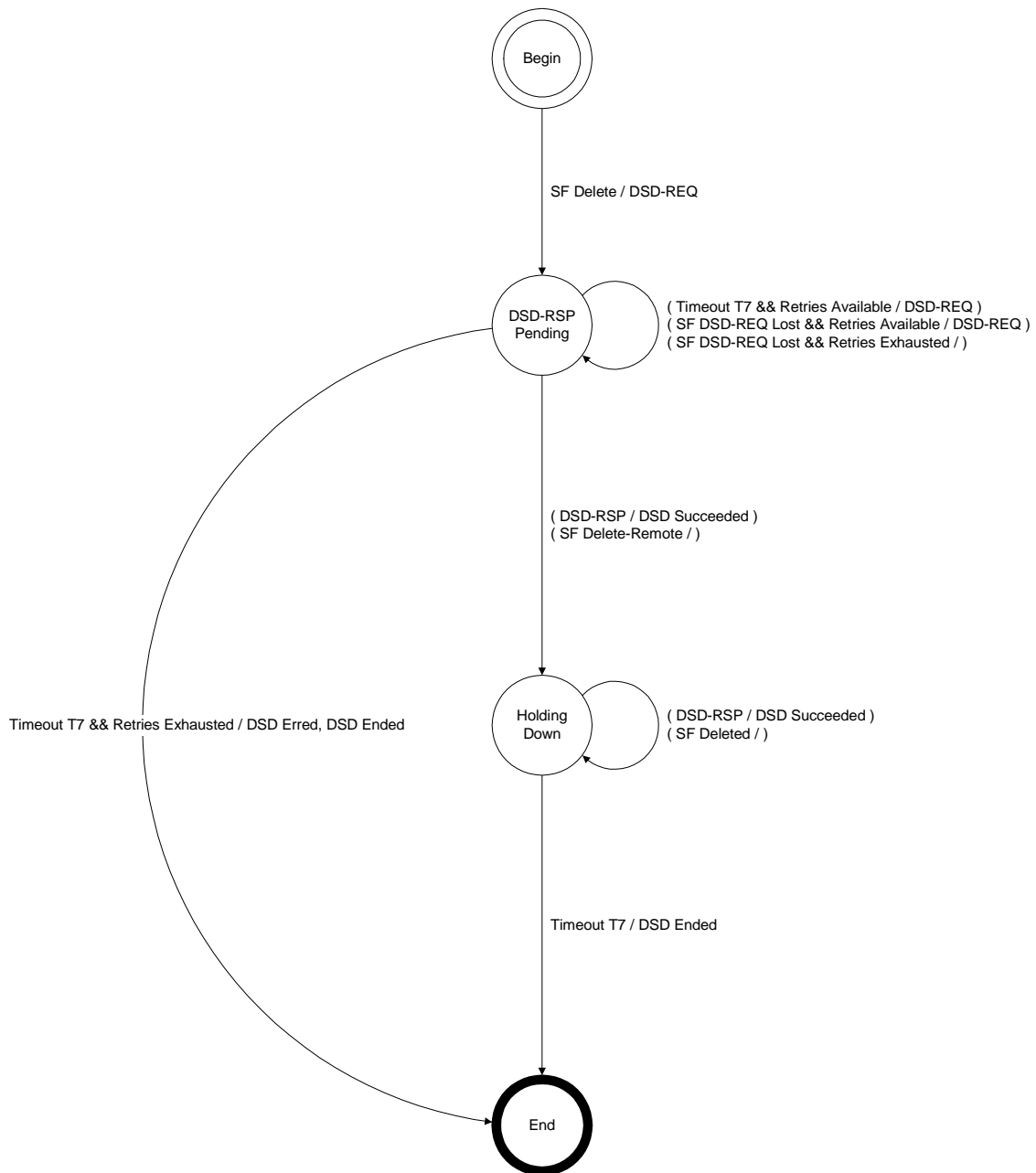
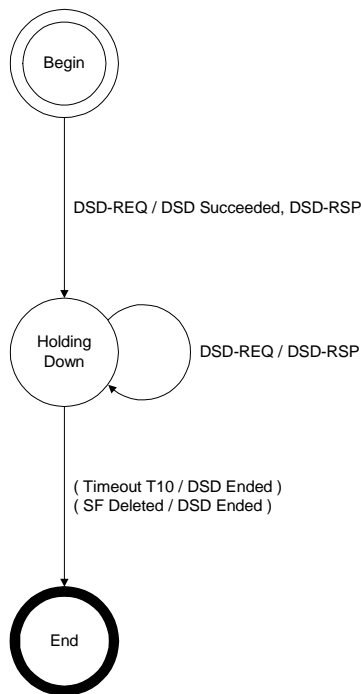


Figure 71—DSC - Remotely Initiated Transaction State Transition Diagram





**Figure 72—DSD - Locally Initiated Transaction State Transition Diagram**

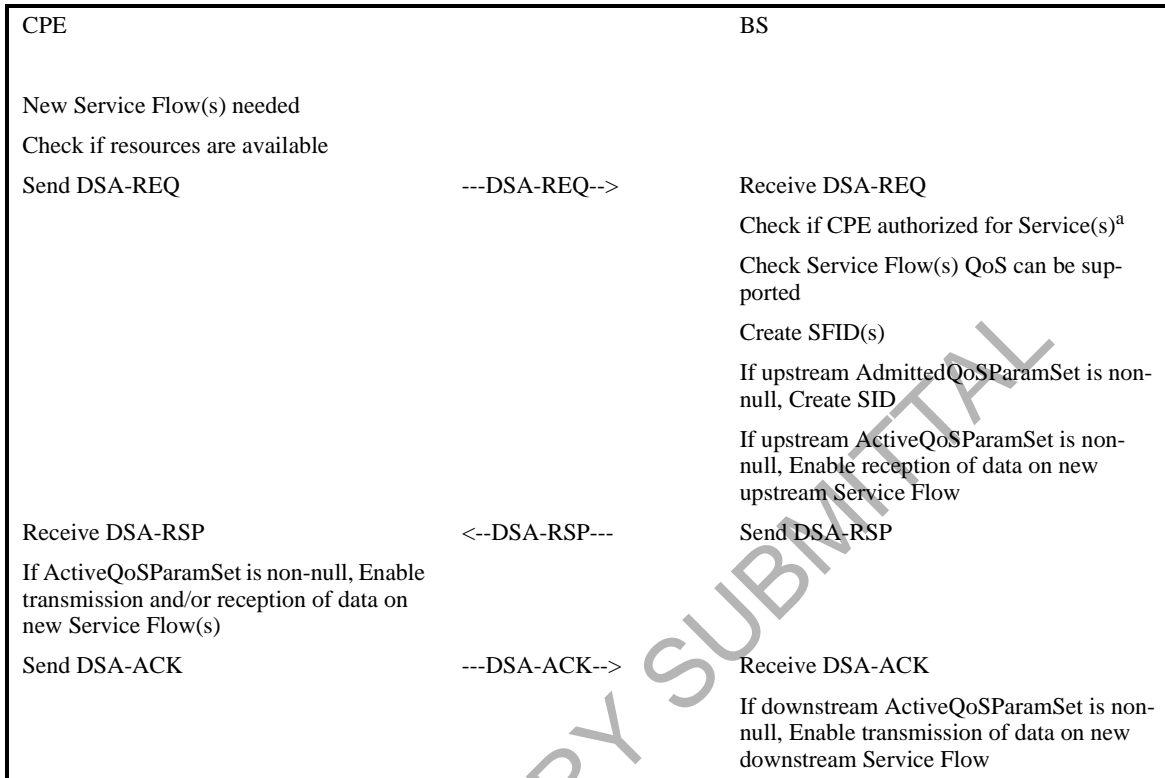


**Figure 73—Dynamic Deletion (DSD) - Remotely Initiated Transaction State Transition Diagram**

#### 6.10.9 Dynamic Service Addition

A CPE wishing to create an upstream and/or a downstream Service Flow sends a request to the BS using a dynamic service addition request Message (DSA-REQ). The BS checks the CPE's authorization for the requested service(s) and whether the QoS requirements can be supported and generates an appropriate response using a dynamic service addition response Message (DSA-RSP). The CPE concludes the transaction with an acknowledgment Message (DSA-ACK).

In order to facilitate a common admission response, an upstream and a downstream Service Flow can be included in a single DSA-REQ. Both Service Flows are either accepted or rejected together.



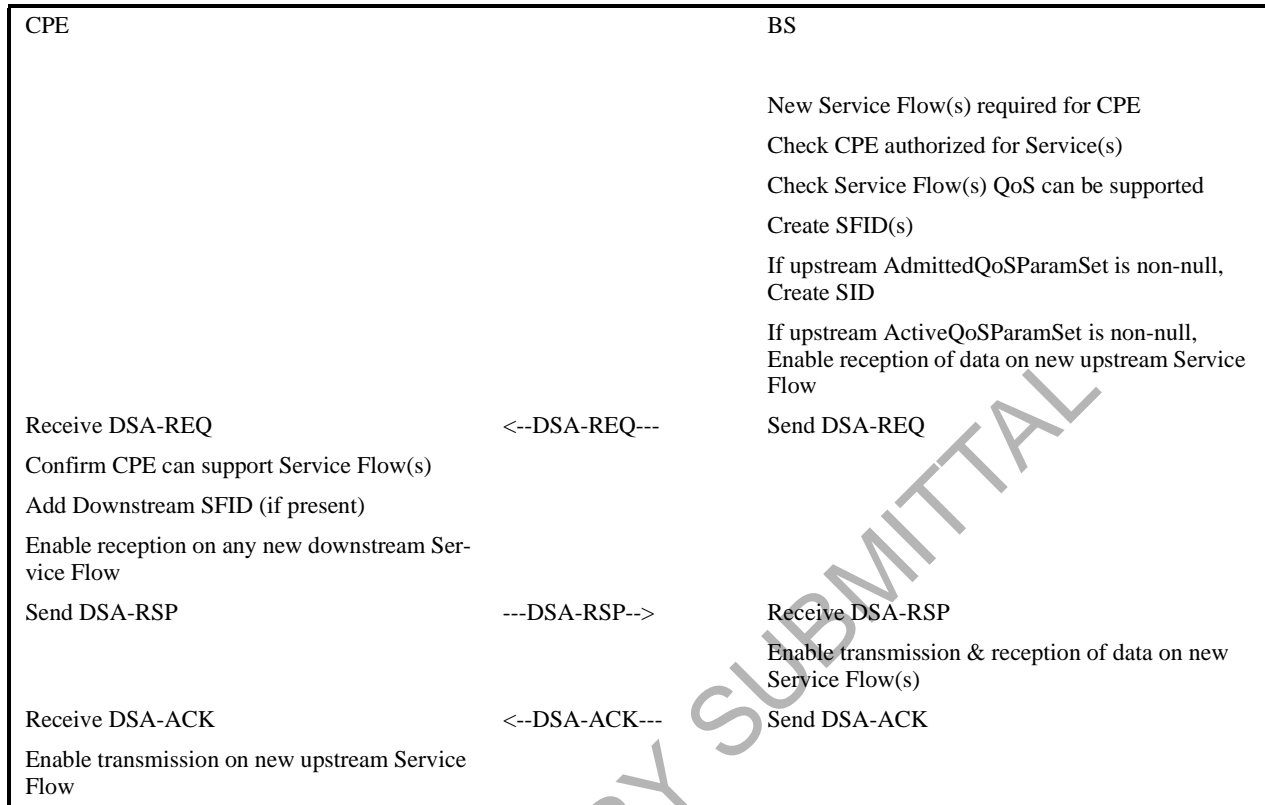
<sup>a</sup>Note: authorization can happen prior to the DSA-REQ being received by the BS. The details of BS signalling to anticipate a DSA-REQ are beyond the scope of this specification.

**Table 18—Dynamic Service Addition Initiated from CPE**

#### 6.10.9.1 BS Initiated Dynamic Service Addition

A BS wishing to establish an upstream and/or a downstream dynamic Service Flow(s) with a CPE performs the following operations. The BS checks the authorization of the destination CPE for the requested class of service and whether the QoS requirements can be supported. If the service can be supported the BS generates new SFID(s) with the required class of service and informs the CPE using a dynamic service addition request Message (DSA-REQ). If the CPE checks that it can support the service and responds using a

dynamic service addition response Message (DSA-RSP). The transaction completes with the BS sending the acknowledge Message (DSA-ACK).



**Table 19—Dynamic Service Addition Initiated from BS**

### 6.10.9.2 Dynamic Service Addition State Transition Diagrams

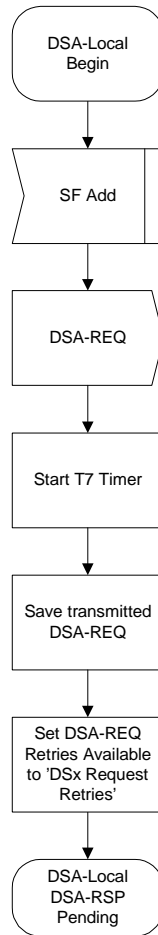


Figure 74—DSA - Locally Initiated Transaction Begin State Flow Diagram

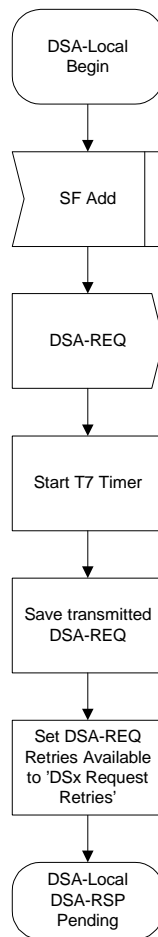


Figure 75—DSA - Locally Initiated Transaction Begin State Flow Diagram

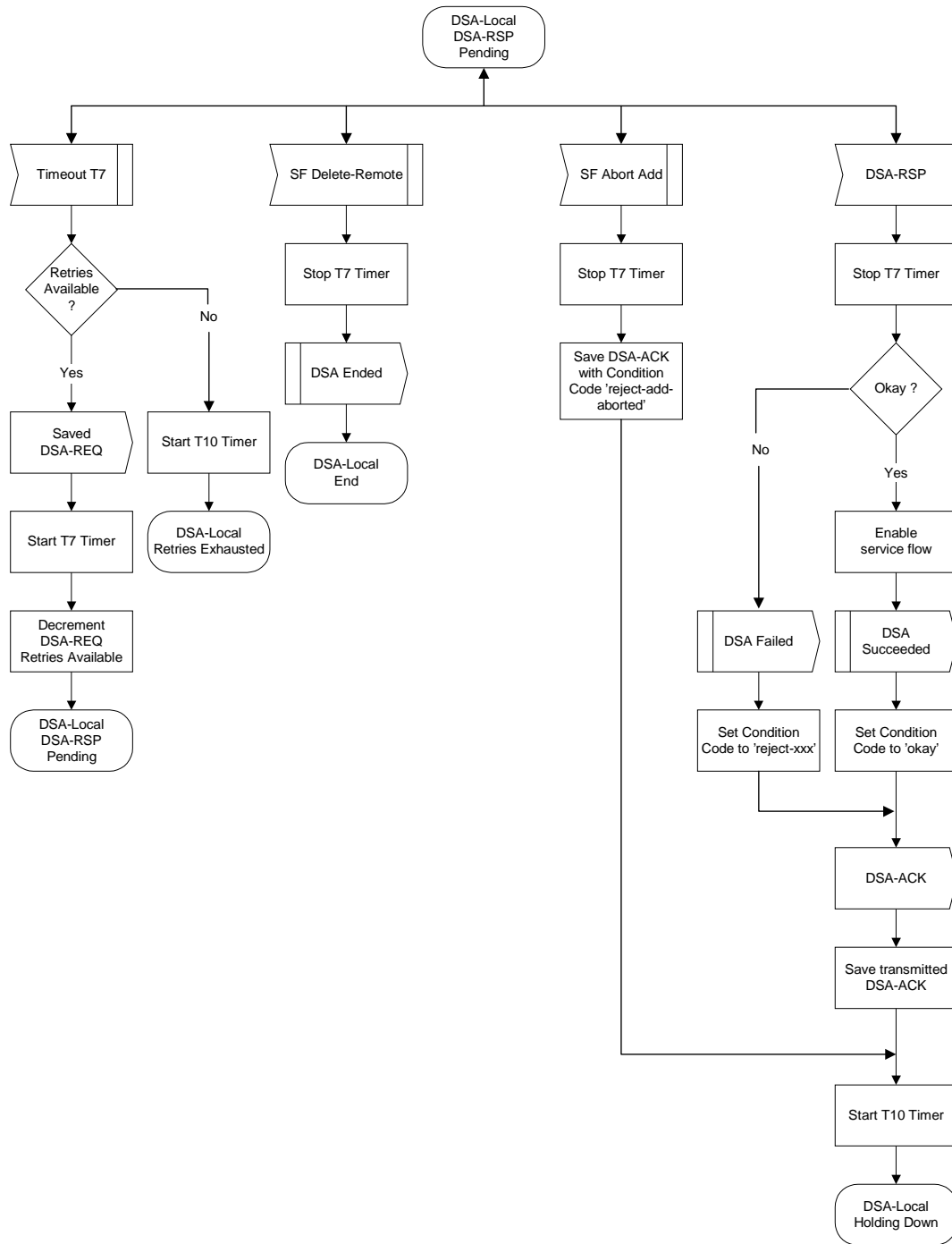


Figure 76—DSA - Locally Initiated Transaction DSA-RSP Pending State Flow Diagram

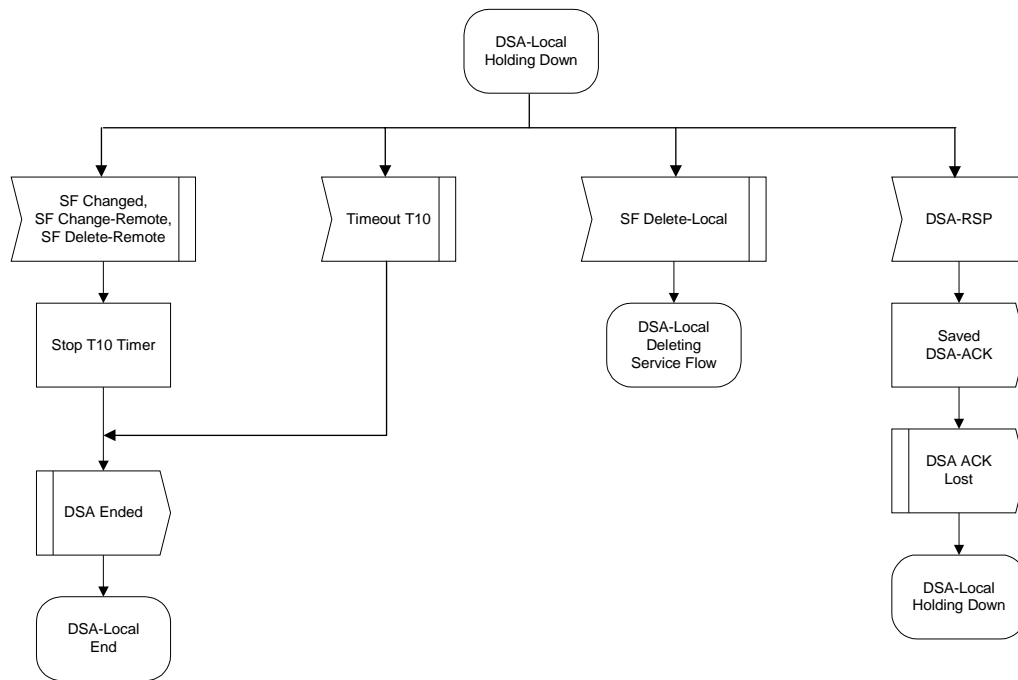
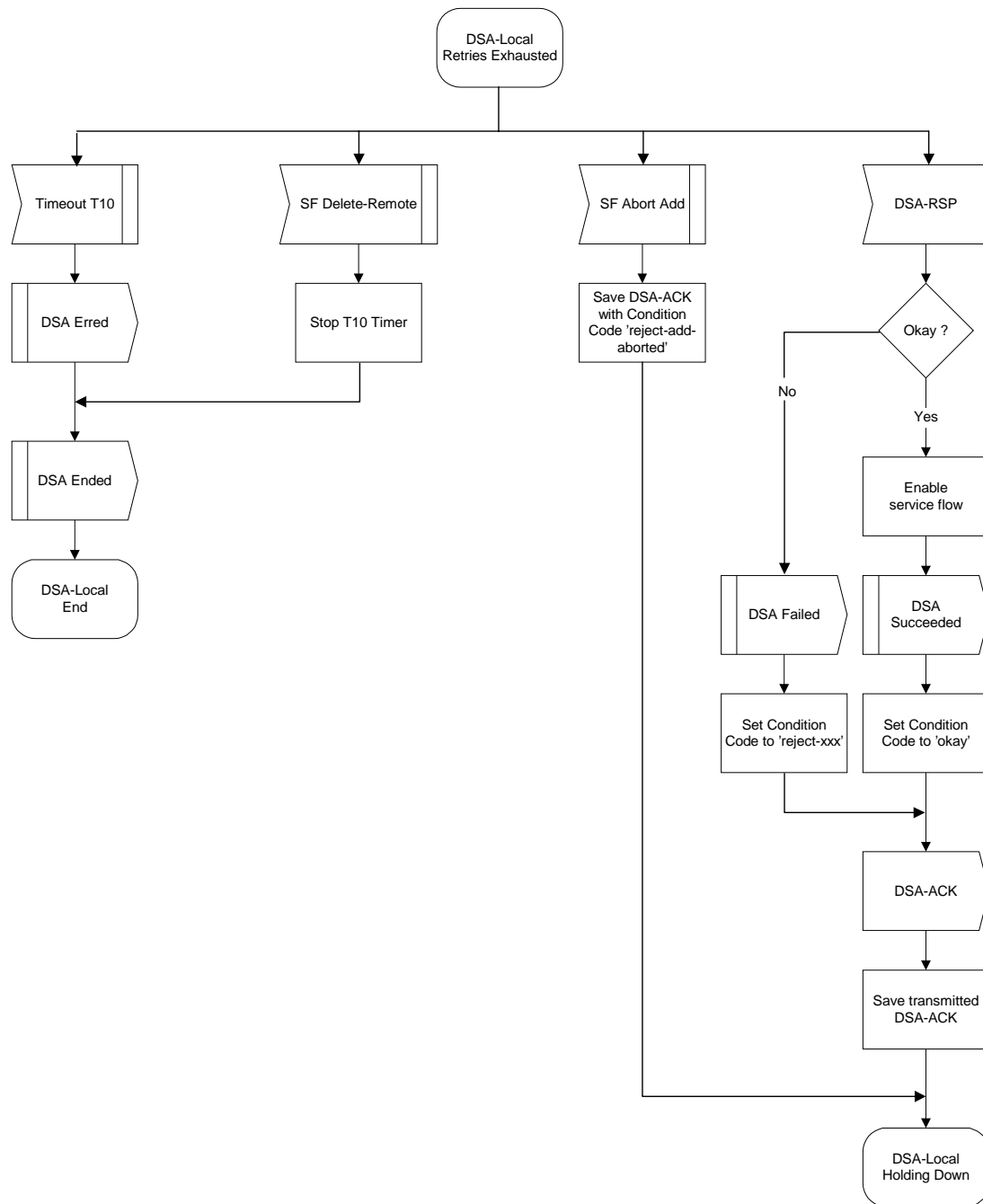
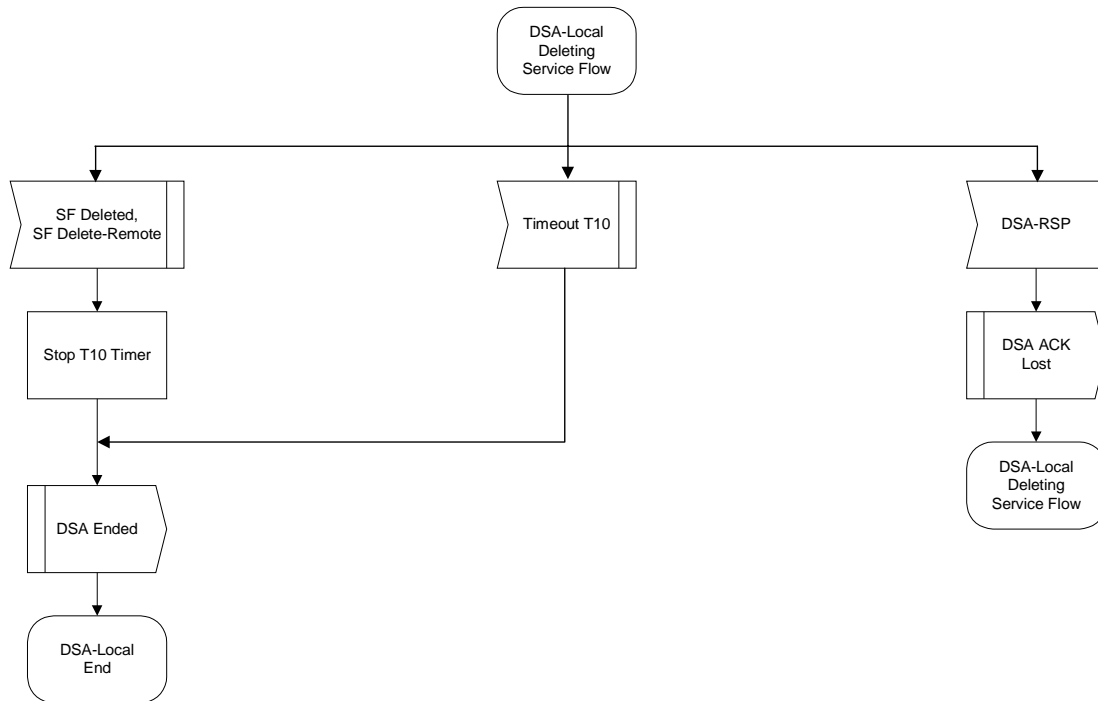


Figure 77—DSA - Locally Initiated Transaction Holding State Flow Diagram

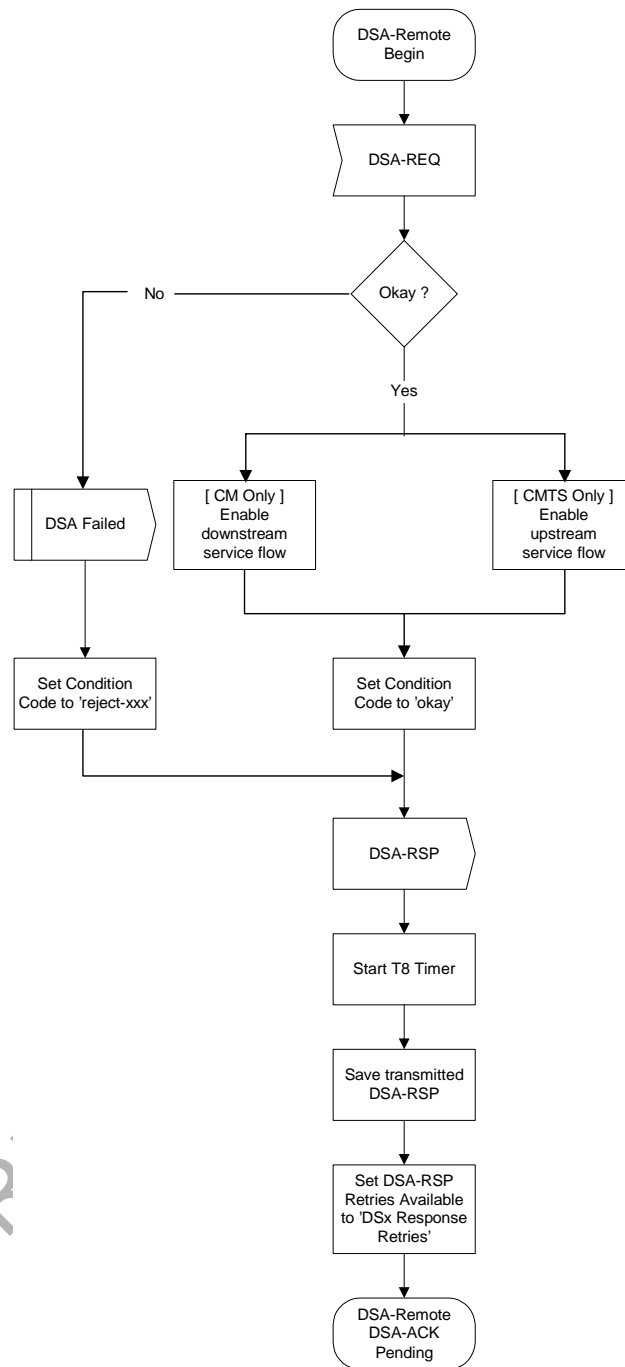




**Figure 78—DSA - Locally Initiated Transaction Retries Exhausted State Flow Diagram**



**Figure 79—DSA - Locally Initiated Transaction Deleting Service Flow State Flow Diagram**



**Figure 80—DSA - Remotely Initiated Transaction Begin State Flow Diagram**

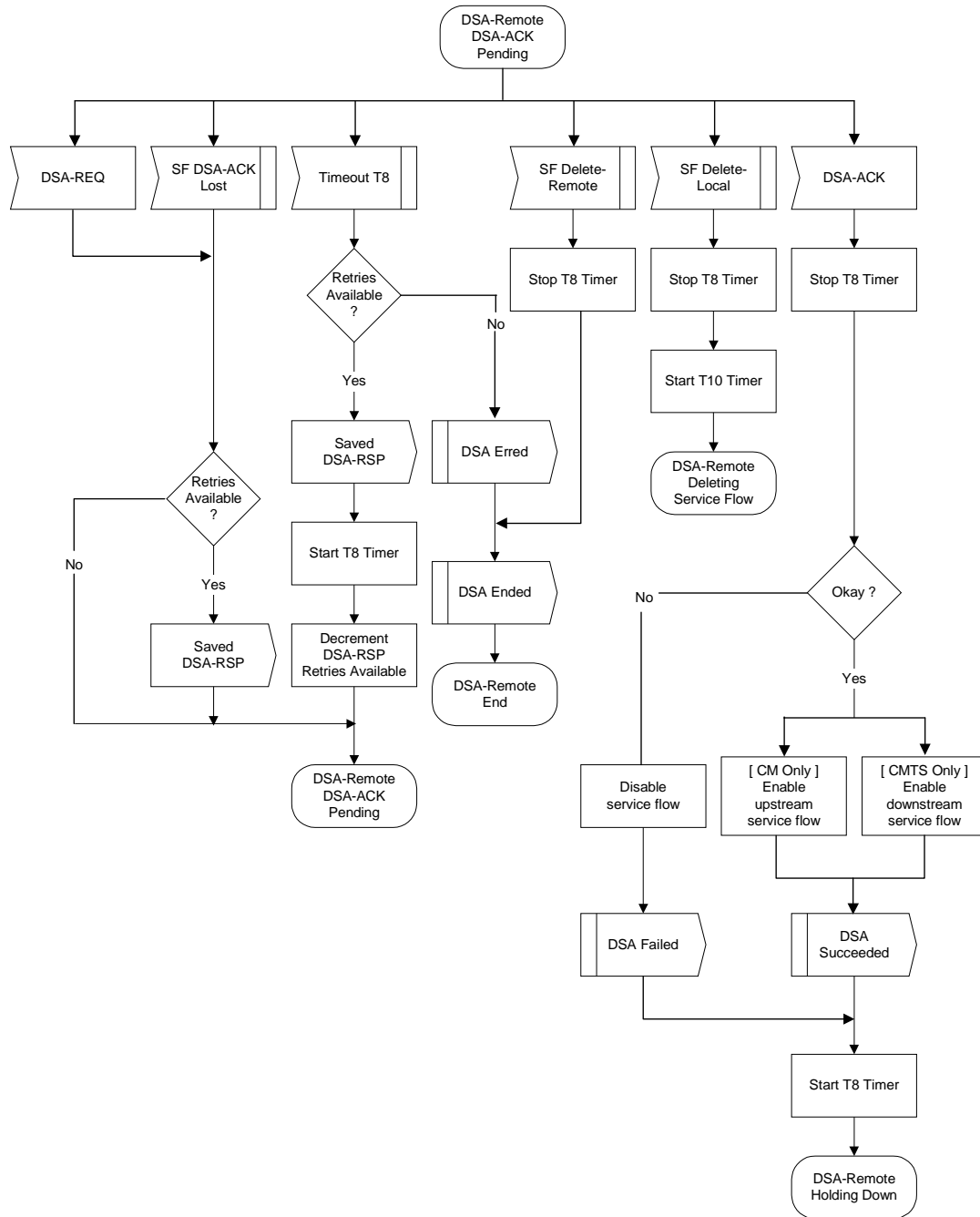
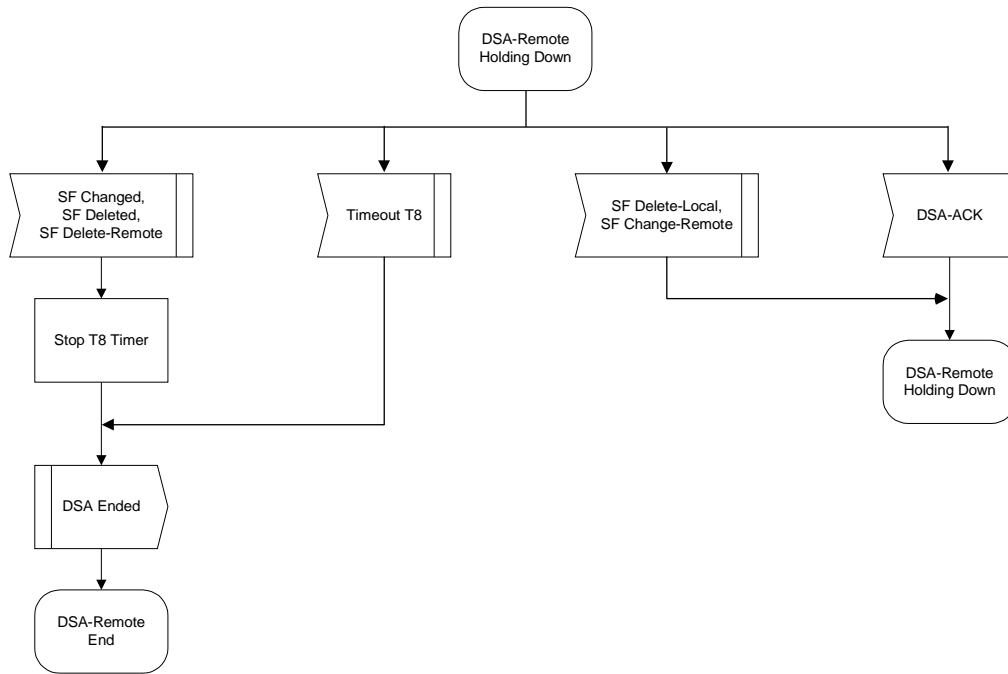
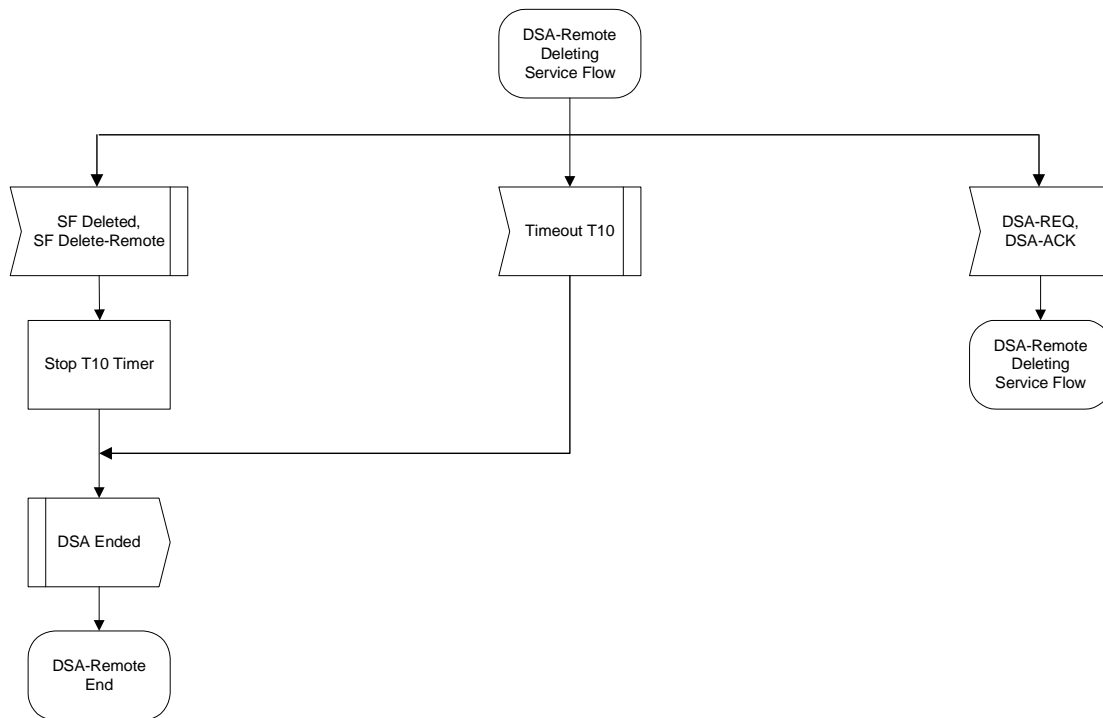


Figure 81—DSA - Remotely Initiated Transaction DSA-ACK Pending State Flow Diagram



**Figure 82—DSA - Remotely Initiated Transaction Holding Down State Flow Diagram**



**Figure 83—DSA - Remotely Initiated Transaction Deleting Service State Flow Diagram**

### 6.10.10 Dynamic Service Change

The Dynamic Service Change (DSC) set of Messages is used to modify the flow parameters associated with a Service Flow. Specifically, DSC can:

- a) Modify the Service Flow Specification
- b) Add, Delete or Replace a Flow Classifier
- c) Add, Delete or Set PHS elements

A single DSC Message exchange can modify the parameters of one downstream service flow and/or one upstream service flow.

To prevent packet loss, any required bandwidth change is sequenced between the CPE and BS.

The BS controls both upstream and downstream scheduling. The timing of scheduling changes is independent of direction AND whether it's an increase or decrease in bandwidth. The BS always changes scheduling on receipt of a DSC-REQ (CPE initiated transaction) or DSC-RSP (BS initiated transaction).

The BS also controls the downstream transmit behavior. The change in downstream transmit behavior is always coincident with the change in downstream scheduling (i.e. BS controls both and changes both simultaneously).

The CPE controls the upstream transmit behavior. The timing of CPE transmit behavior changes is a function of which device initiated the transaction AND whether the change is an “increase” or “decrease” in bandwidth.

If an upstream Service Flow's bandwidth is being reduced, the CPE reduces its payload bandwidth first and then the BS reduces the bandwidth scheduled for the Service Flow. If an upstream Service Flow's bandwidth is being increased, the BS increases the bandwidth scheduled for the Service Flow first and then the CPE increases its payload bandwidth.

If the bandwidth changes are complex, it may not be obvious to the CPE when to effect the bandwidth changes. This information may be signalled to the CPE from a higher layer entity. Similarly, if the DSC signaling is initiated by the BS, the BS MAY indicate to the CPE whether it should install or remove Classifiers upon receiving the DSC-Request or whether it should postpone this installation until receiving the DSC-Ack (refer to C.2.1.9)

Any service flow can be deactivated with a Dynamic Service Change command by sending a DSC-REQ Message, referencing the Service Flow Identifier, and including a null ActiveQoSParameterSet. However, if a Primary Service Flow of a CPE is deactivated that CPE is de-registered and MUST re-register. Therefore, care should be taken before deactivating such Service Flows. If a Service Flow that was provisioned during registration is deactivated, the provisioning information for that Service Flow MUST be maintained until the Service Flow is reactivated.

A CPE MUST have only one DSC transaction outstanding per Service Flow. If it detects a second transaction initiated by the BS, the CPE MUST abort the transaction it initiated and allow the BS initiated transaction to complete.

A BS MUST have only one DSC transaction outstanding per Service Flow. If it detects a second transaction initiated by the CPE, the BS MUST abort the transaction the CPE initiated and allow the BS initiated transaction to complete.

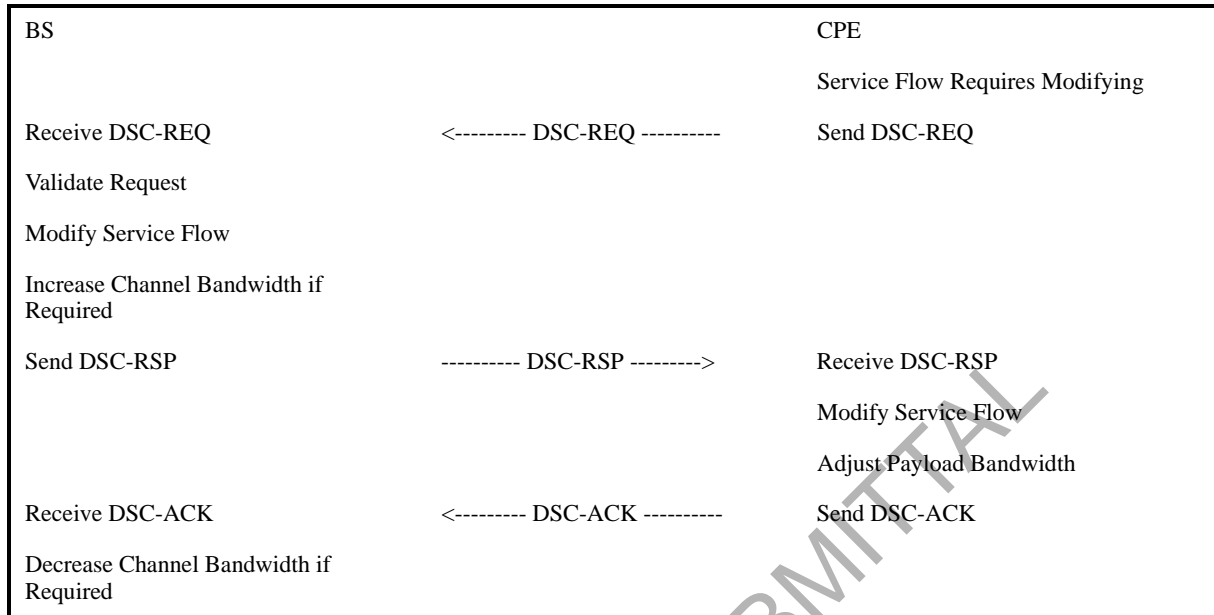
**Note:** Currently anticipated applications would probably control a Service Flow through either the CPE or BS, and not both. Therefore the case of a DSC being initiated simultaneously by the CPE and BS is considered as an exception condition and treated as one.

#### 6.10.10.1 CPE-Initiated Dynamic Service Change

A CPE that needs to change a Service Flow definition performs the following operations.

The CPE informs the BS using a Dynamic Service Change Request Message (DSC-REQ). The BS MUST decide if the referenced Service Flow can support this modification. The BS MUST respond with a Dynamic

Service Change Response (DSC-RSP) indicating acceptance or rejection. The CPE reconfigures the Service Flow if appropriate, and then MUST respond with a Dynamic Service Change Acknowledge (DSC-ACK).

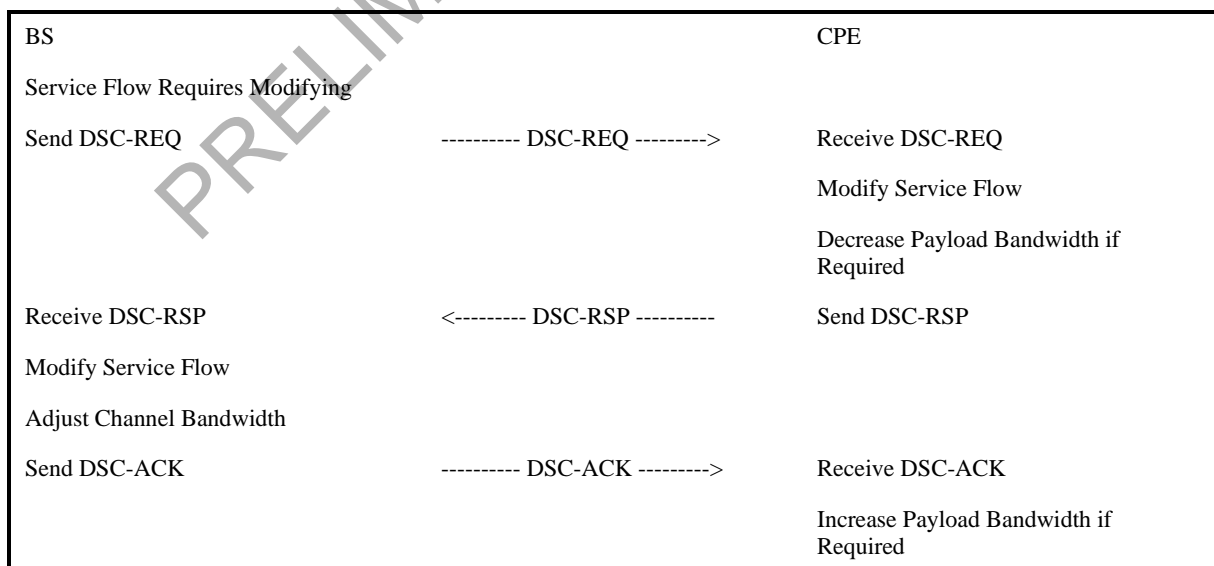


**Table 20—CPE-Initiated DSC**

#### 6.10.10.2 BS-Initiated Dynamic Service Change

A BS that needs to change a Service Flow definition performs the following operations.

The BS MUST decide if the referenced Service Flow can support this modification. If so, the BS informs the CPE using a Dynamic Service Change Request Message (DSC-REQ). The CPE checks that it can support the service change, and MUST respond using a Dynamic Service Change Response (DSC-RSP) indicating acceptance or rejection. The BS reconfigures the Service Flow if appropriate, and then MUST respond with a Dynamic Service Change Acknowledgment (DSC-ACK)



**Table 21—BS-Initiated DSC**



## 6.10.10.3 Dynamic Service Change State Transition Diagrams

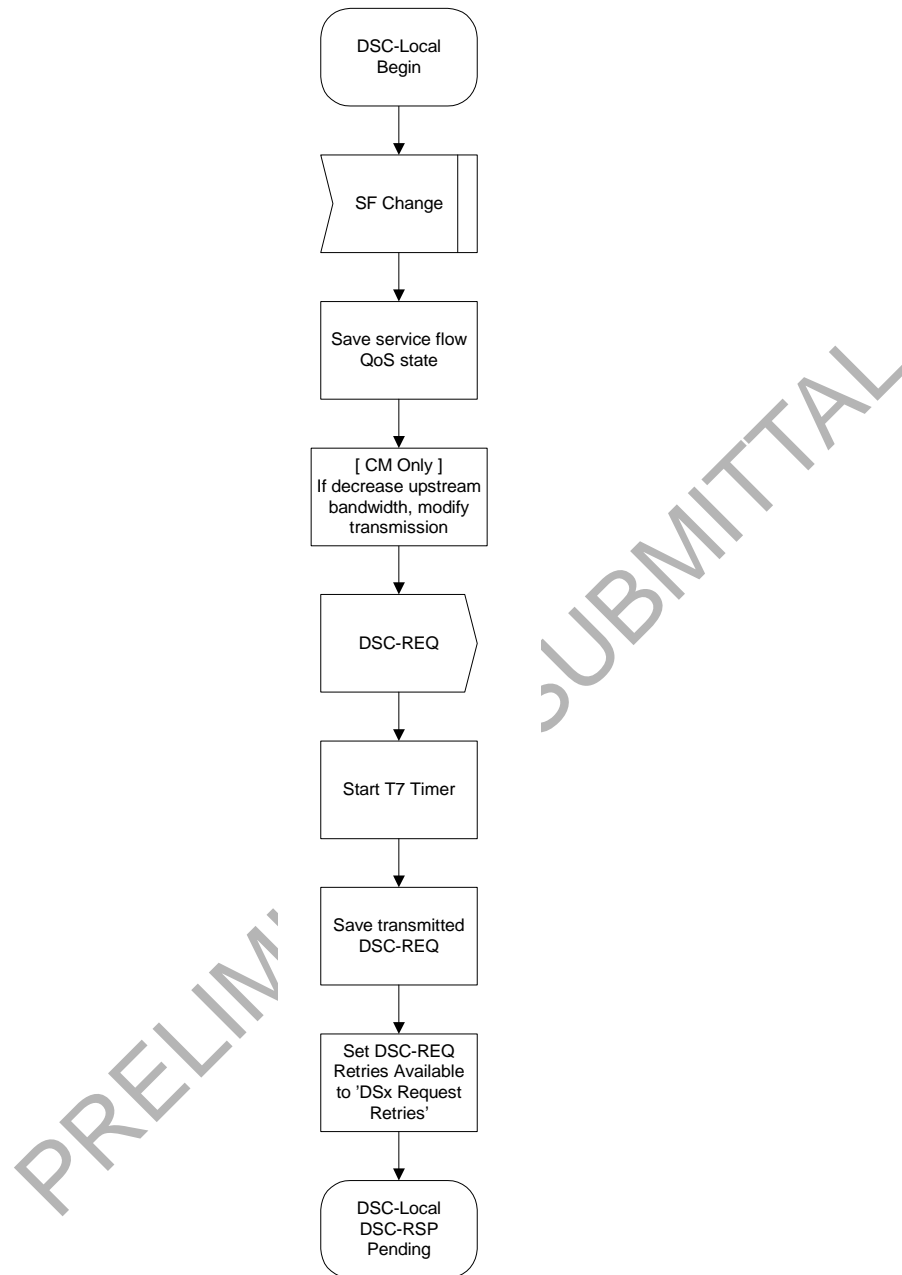


Figure 84—DSC - Locally Initiated Transaction Begin State Flow Diagram

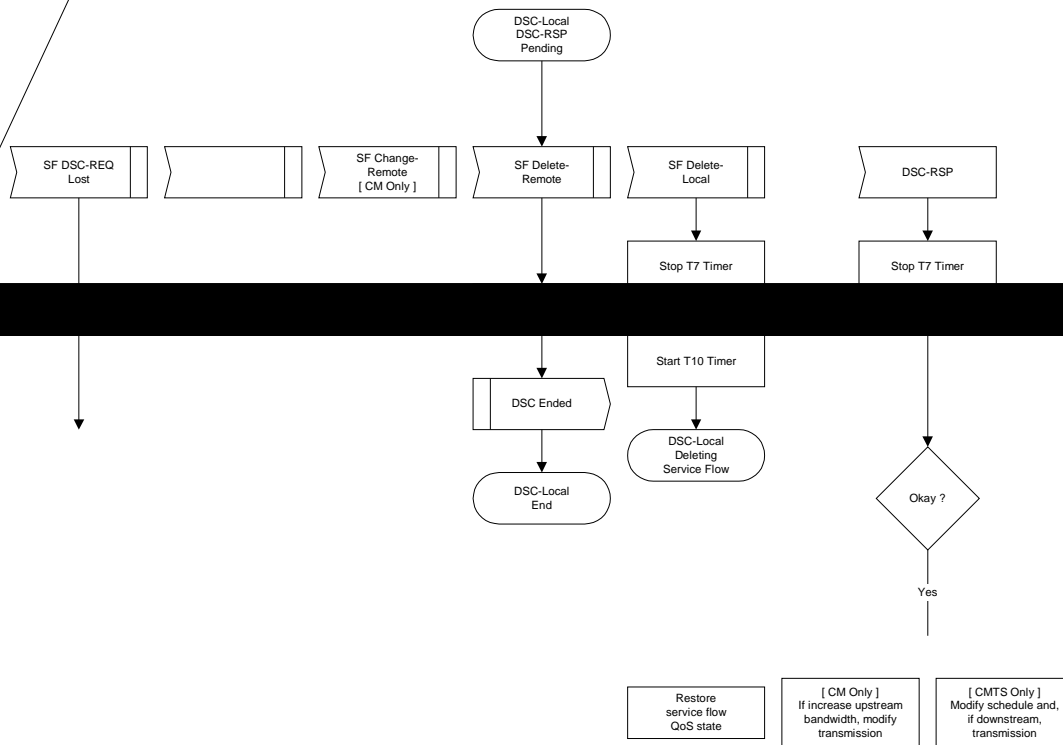


Figure 85—DSC - Locally Initiated Transaction DSC-RSP Pending State Flow Diagram

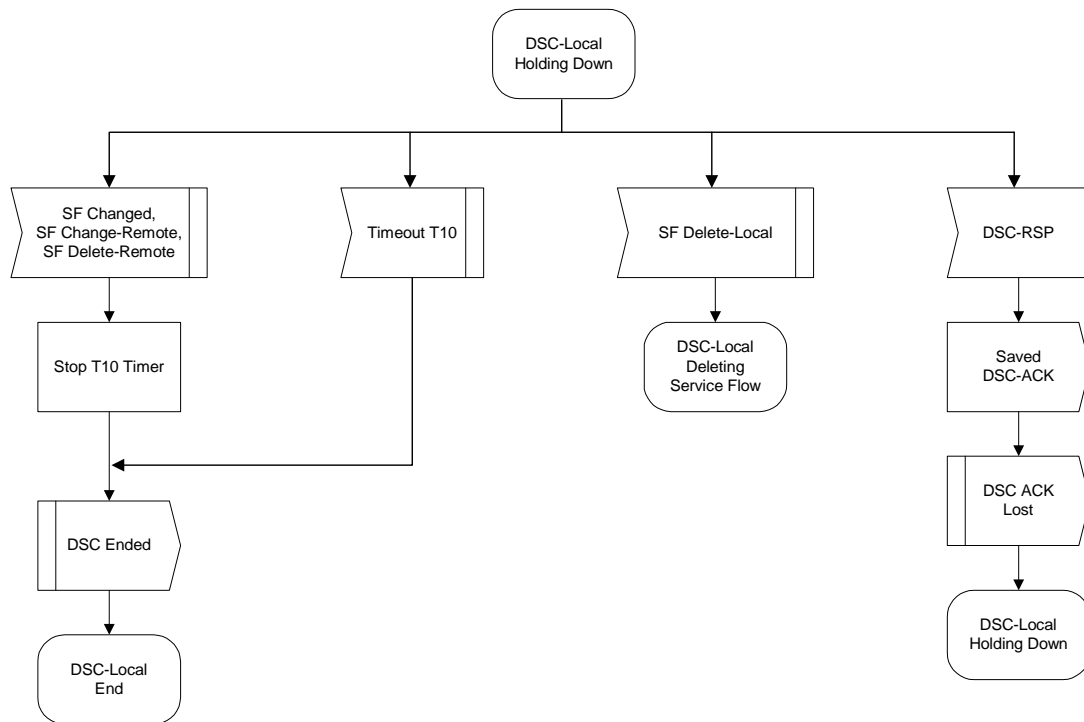


Figure 86—DSC - Locally Initiated Transaction Holding Down State Flow Diagram

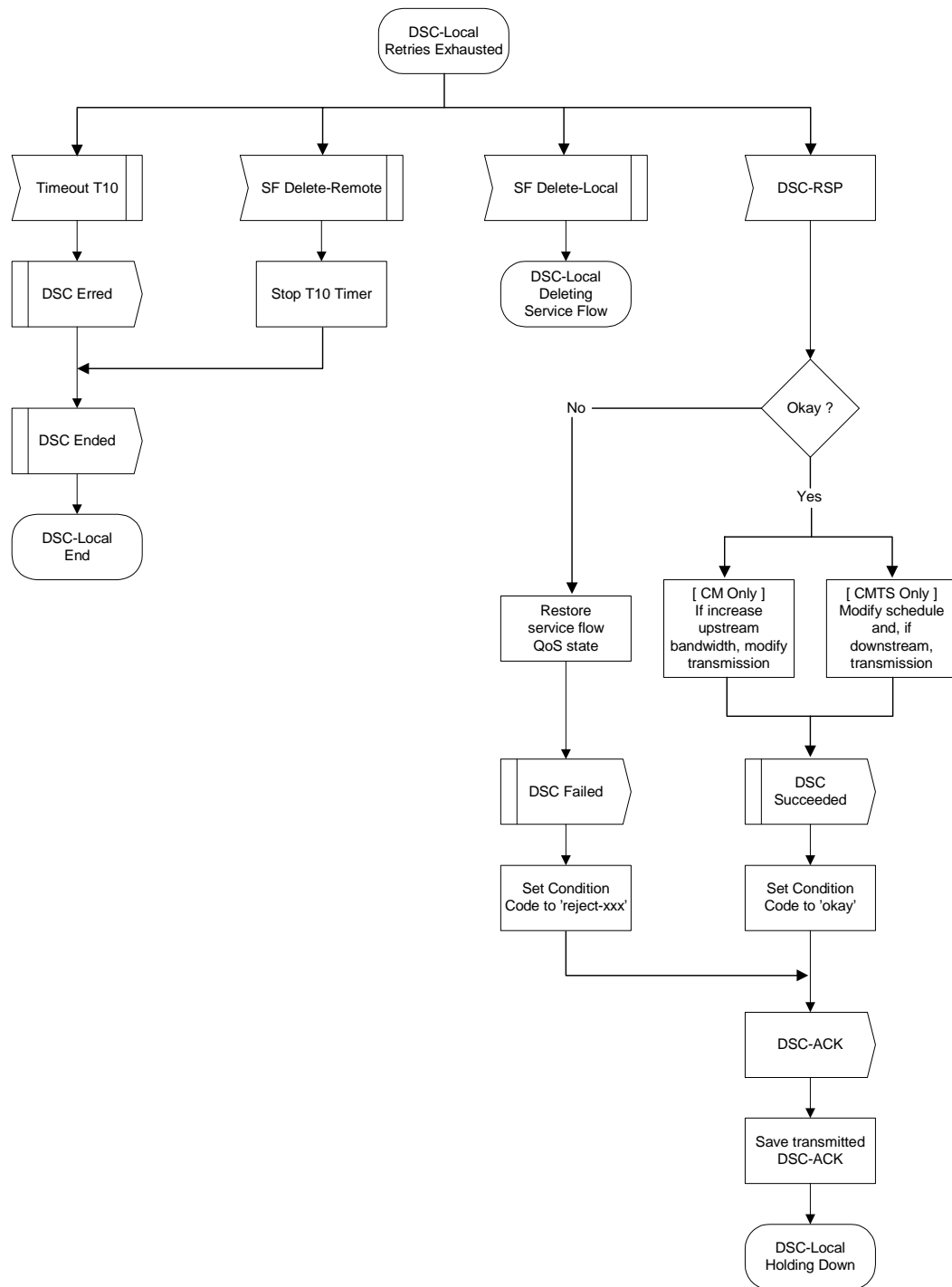
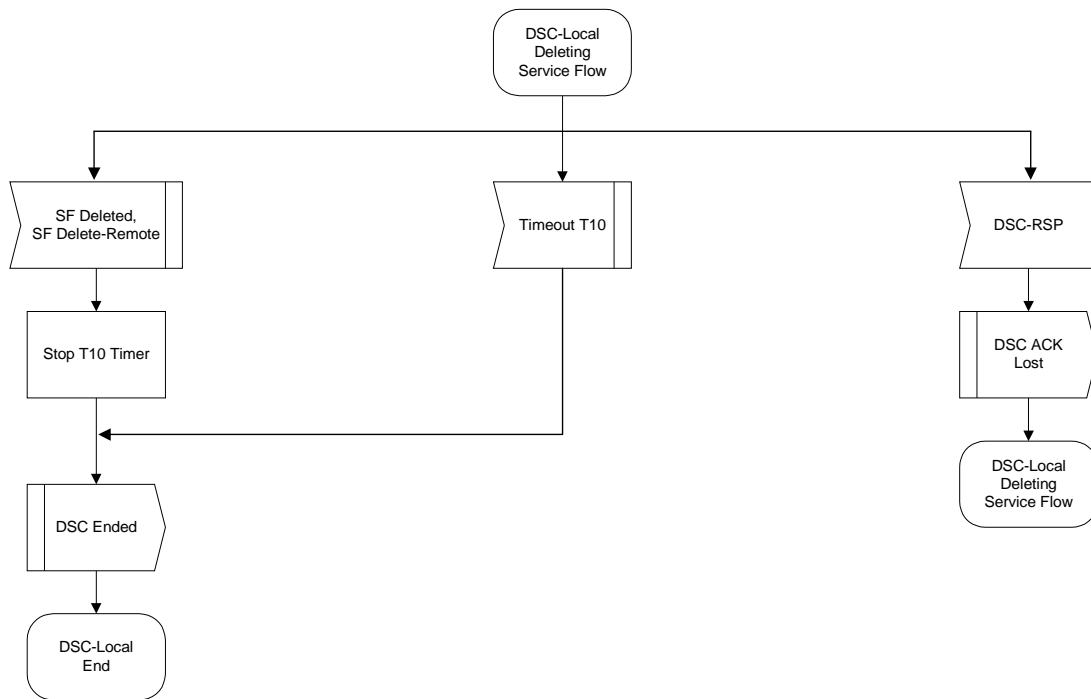
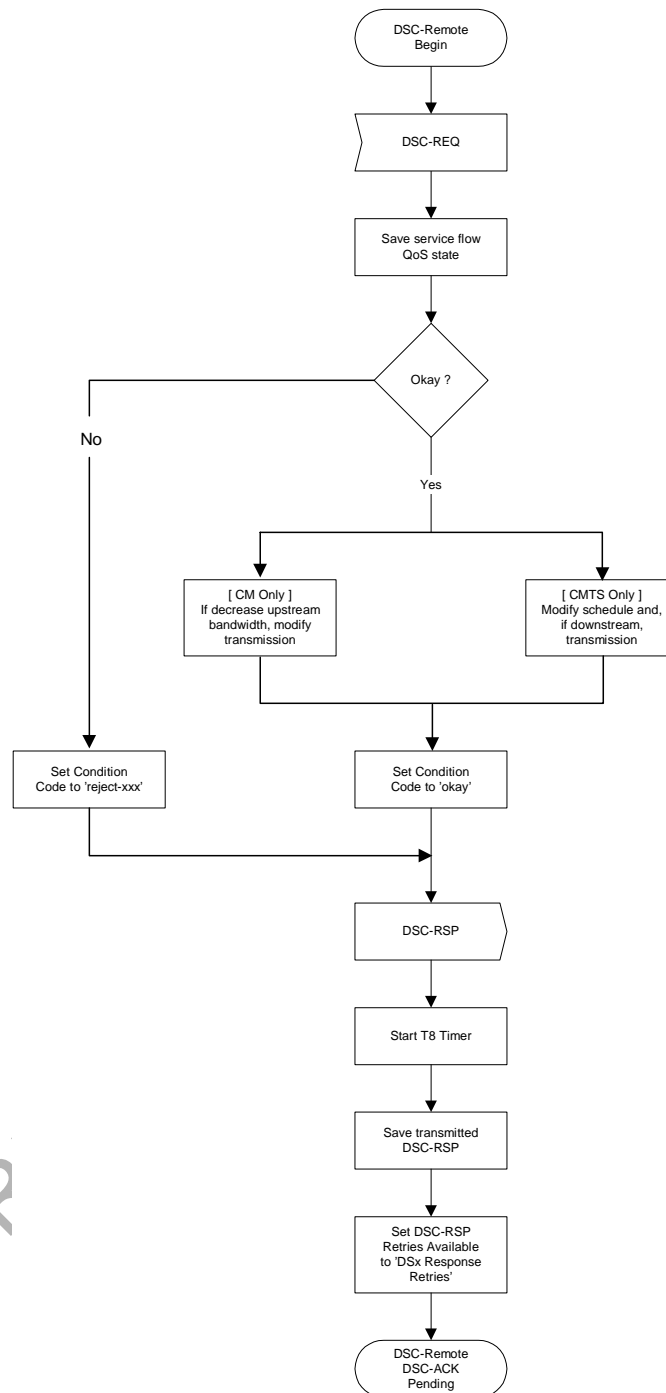


Figure 87—DSC - Locally Initiated Transaction Retries Exhausted State Flow Diagram



**Figure 88—DSC - Locally Initiated Transaction Deleting Service Flow State Flow Diagram**



**Figure 89—DSC - Remotely Initiated Transaction Begin State Flow Diagram**

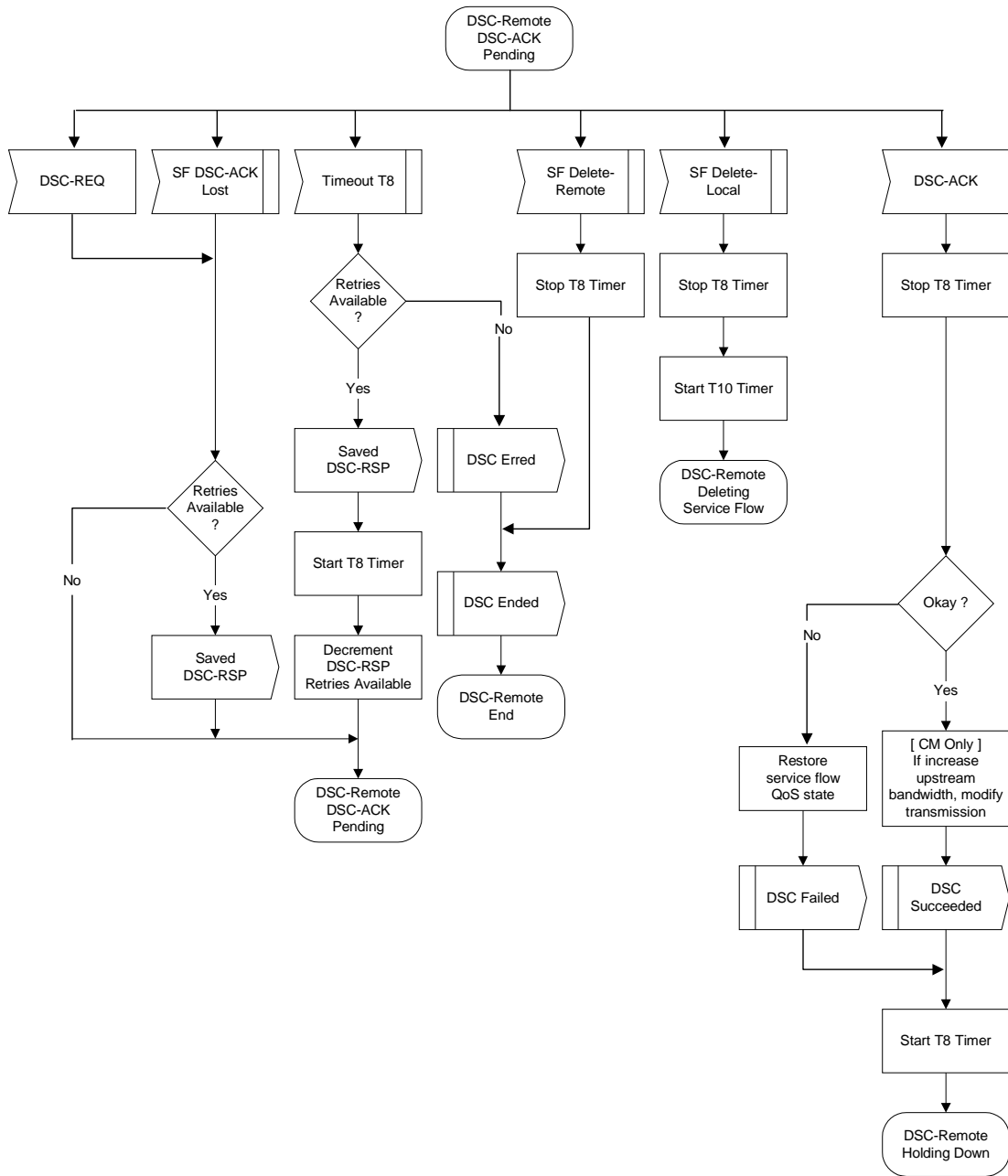
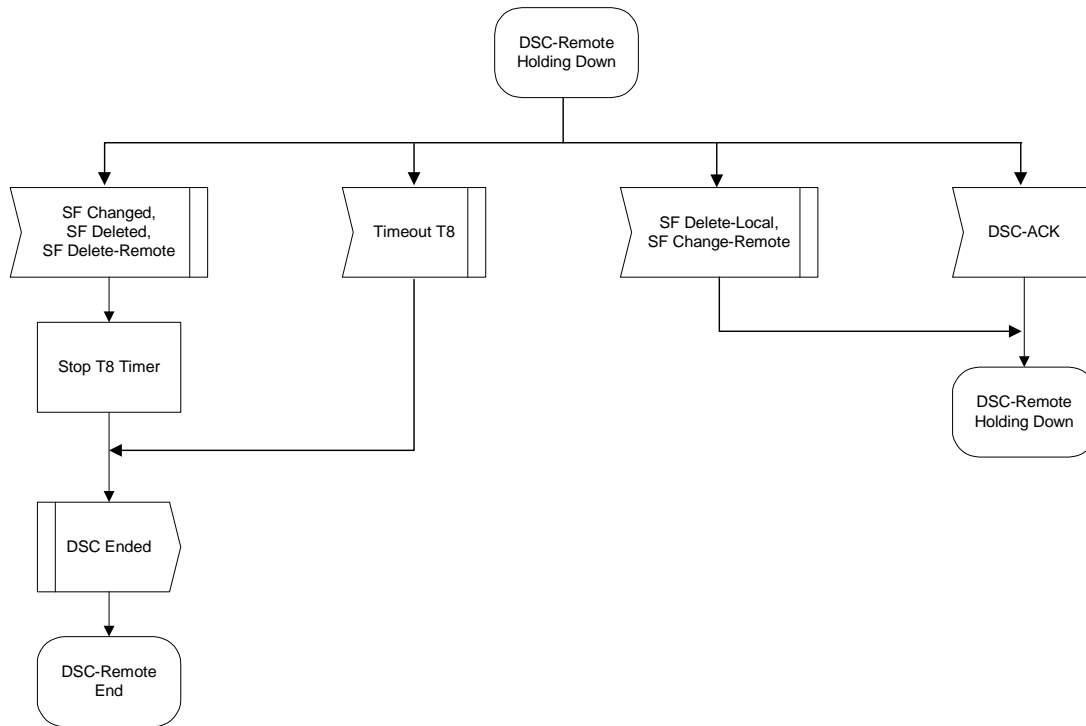


Figure 90—DSC - Remotely Initiated Transaction DSC-ACK Pending State Flow Diagram



**Figure 91—DSC - Remotely Initiated Transaction Holding Down State Flow Diagram**



#### **6.10.11 Connection Release**

Any service flow can be deleted with the Dynamic Service Deletion (DSD) Messages. When a Service Flow  
.(iDSD-REQ<sub>low</sub>)]TET

		Verify CPE is Service Flow 'owner'
		Delete Service Flow
Receive DSD-RSP	<--DSD-RSP--	Send DSD-RSP

**Table 22—Dynamic Service Deletion Initiated from CPE****6.10.11.2 BS Initiated Dynamic Service Deletion**

A BS wishing to delete a dynamic Service Flow generates a delete request to the associated CPE using a Dynamic Service Deletion-Request Message (DSD-REQ). The CPE removes the Service Flow and generates a response using a Dynamic Service Deletion-Response Message (DSD-RSP). Only one Service Flow can be deleted per DSD-Request.

CPE		BS
		Service Flow no longer needed
		Delete Service Flow
		Determine associated CPE for this Service Flow
Receive DSD-REQ	<---DSD-REQ---	Send DSD-REQ
Delete Service Flow		
Send DSD-RSP	---DSD-RSP-->	Receive DSD-RSP

**Table 23—Dynamic Service Deletion Initiated from BS**

### 6.10.12 Dynamic Service Deletion State Transition Diagrams

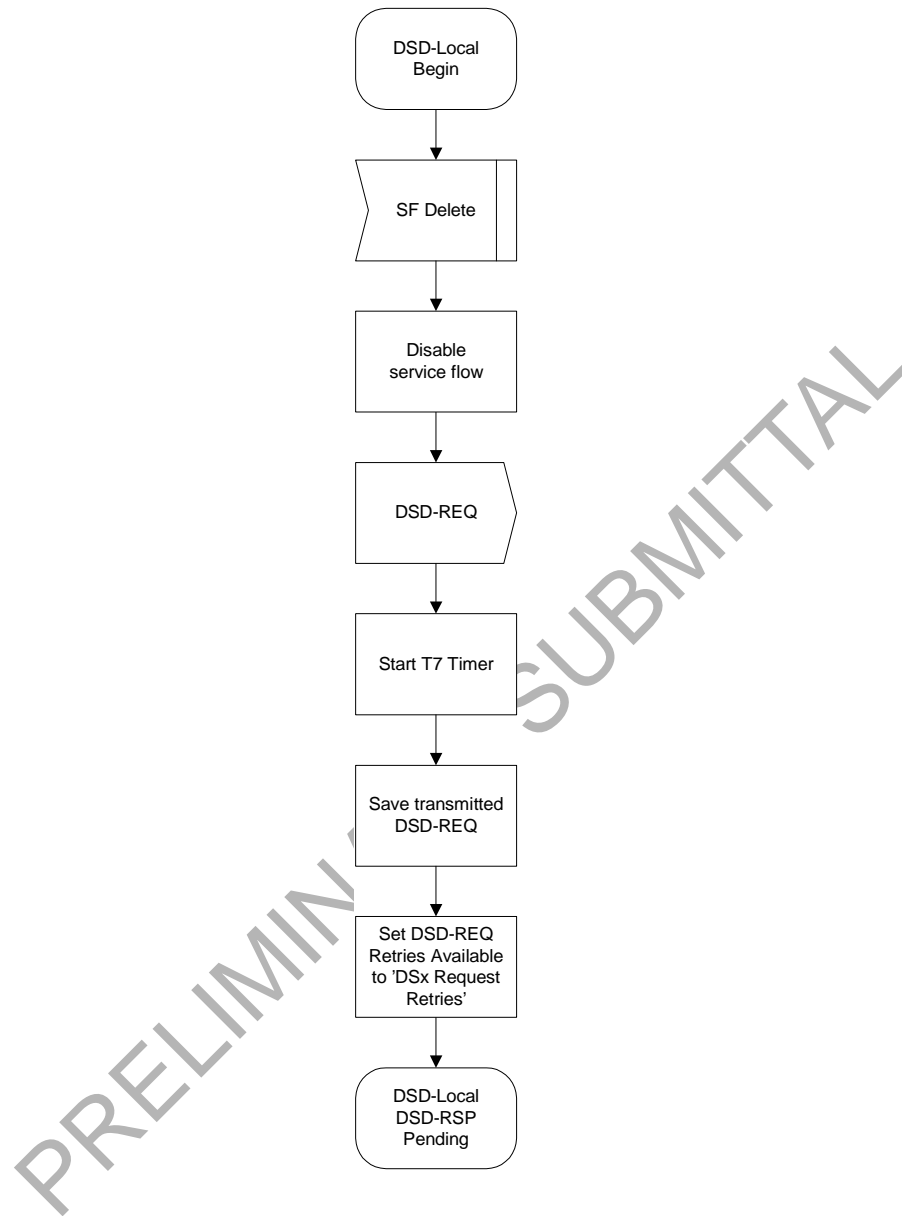


Figure 93—DSD - Locally Initiated Transaction Begin State Flow Diagram

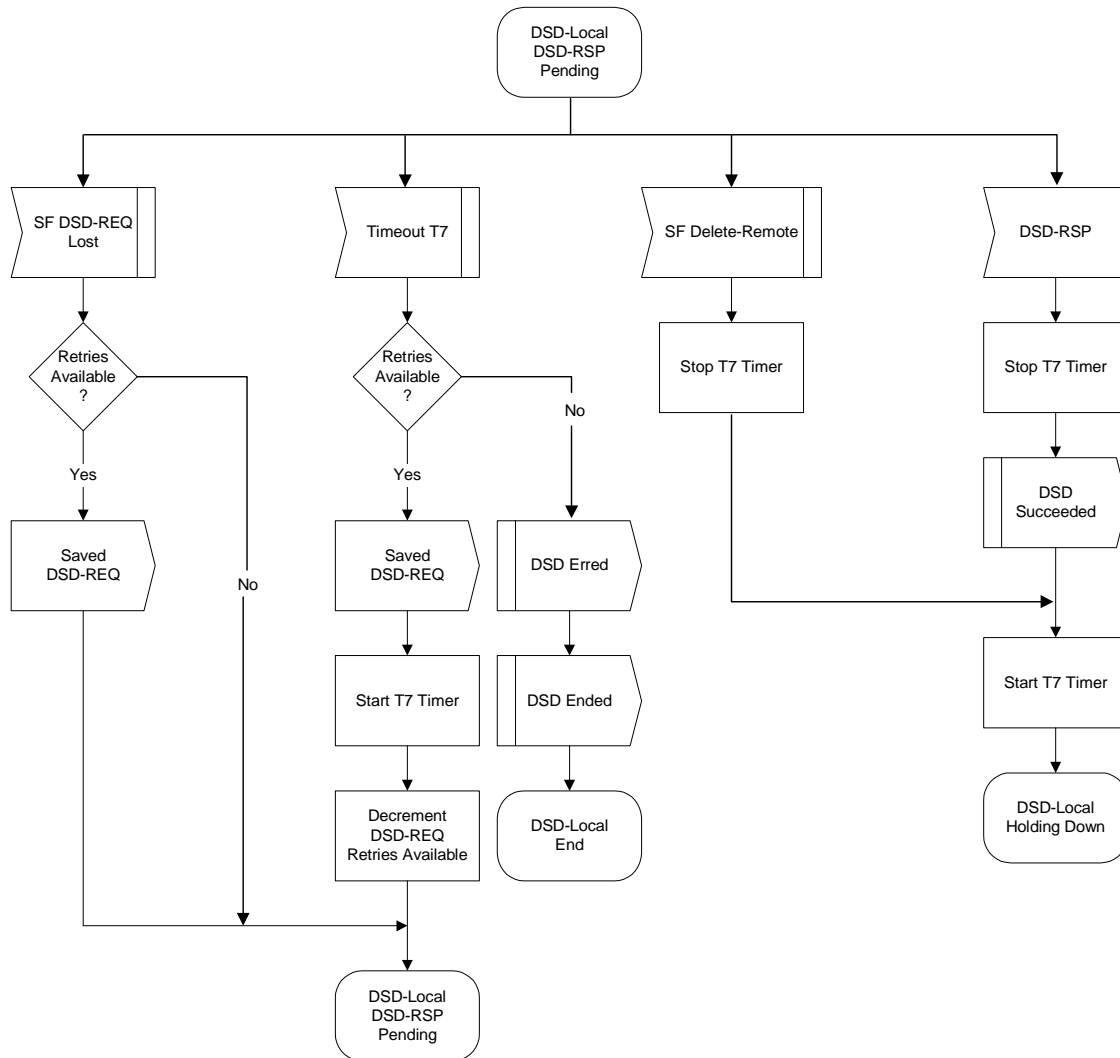
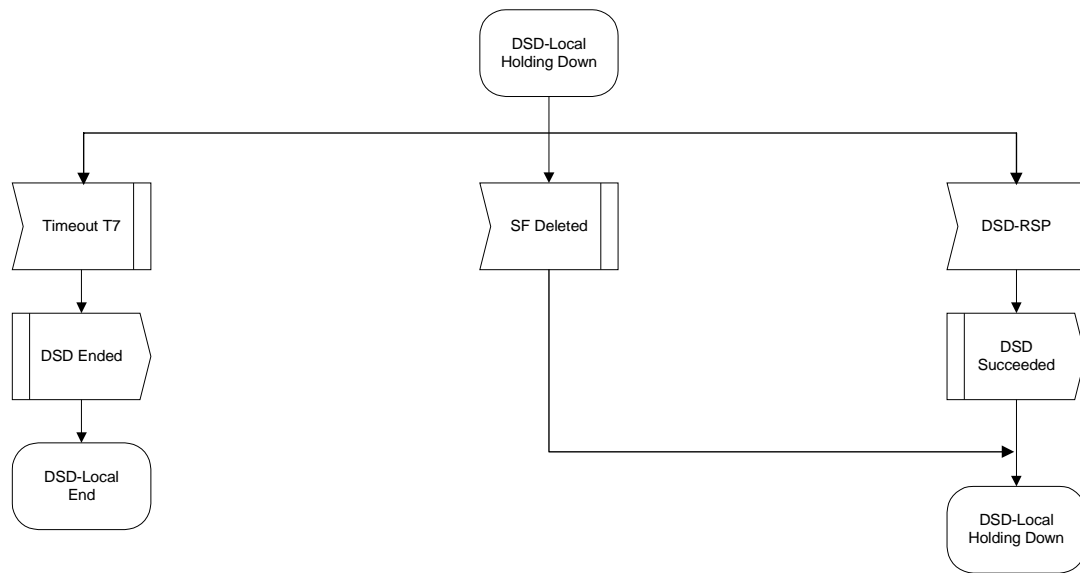


Figure 94—DSD - Locally Initiated Transaction DSD-RSP Pending State Flow Diagram



**Figure 95—DSD - Locally Initiated Transaction Holding Down State Flow Diagram**

PRELIMINARY SUBMIT

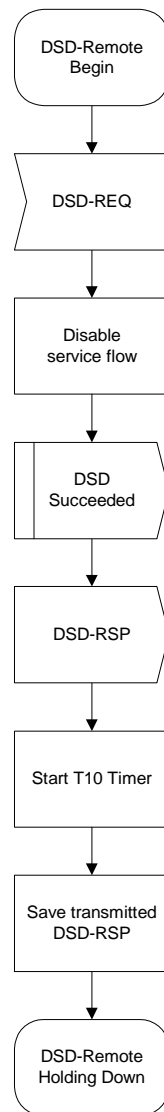


Figure 96—DSD - Remotely Initiated Transaction Begin State Flow Diagram

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL



PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

## 6.11 Parameters and Constants

**Table 24—Parameters and Constants**

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
BS	Sync Interval	Nominal time between transmission of SYNC messages (ref. 5.3.4.3.7)			200 msec
BS	UCD Interval	Time between transmission of UCD messages (ref. 5.3.4.3.8)			2 sec
BS	Max MAP Pending	The number of mini-slots that a BS is allowed to map into the future (ref. 5.3.4.4.1)			4096 mini-slot times
BS	Ranging Interval	Time between transmission of broadcast Ranging requests (ref. 5.4.2.1)			2 sec
CPE	Lost Sync Interval	Time since last received Sync message before synchronization is considered lost			600 msec
CPE	Contention Ranging Retries	Number of Retries on contention Ranging Requests (ref. 5.4.2.4)	16		
CPE, BS	Invited Ranging Retries	Number of Retries on inviting Ranging Requests (ref. 5.4.2.4)	16		
CPE	Request Retries	Number of retries on bandwidth allocation requests	16		
CPE	Registration				
Request Retries	Number of retries on registration requests	3			
CPE	Data Retries	Number of retries on immediate data transmission	16		
BS	CPE MAP processing time	Time provided between arrival of the last bit of a MAP at a CPE and effectiveness of that MAP (ref. 5.5.3.3.2)	200 ms		
BS	CPE Ranging Response processing time	Minimum time allowed for a CPE following receipt of a ranging response before it is expected to reply to an invited ranging request	1 msec		

**Table 24—Parameters and Constants**

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
BS	CPE Configuration	The maximum time allowed for a CPE, following receipt of a configuration file, to send a Registration Request to a BS.	30 sec		
CPE	T1	Wait for UCD timeout			5 * UCD interval maximum value
CPE	T2	Wait for broadcast ranging timeout			5 * ranging interval
CPE	T3	Wait for ranging response	50 msec	200 msec	200 msec
CPE	T4	Wait for unicast ranging opportunity. If the pending-till-complete field was used earlier by this modem, then the value of that field must be added to this interval.	30 sec		35 sec
BS	T5	Wait for Upstream Channel Change response			2 sec
CPE	T6	Wait for registration response			3 sec
CPE					
BS	Mini-slot size	Size of mini-slot for upstream transmission. Must be a power of 2 (in units of the Timebase Tick)	32 symbol times		
CPE					
BS	Timebase Tick	System timing unit	6.25 msec		
CPE					
BS	DSx Request Retries	Number of Timeout Retries on DSA/DSC/DSD Requests		3	
CPE					
BS	DSx Response Retries	Number of Timeout Retries on DSA/DSC/DSD Responses		3	
CPE					
BS	T7	Wait for DSA/DSC/DSD Response timeout			1 sec
CPE					

**Table 24—Parameters and Constants**

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
BS	T8	Wait for DSA/DSC Acknowledge timeout			300 msec
CPE	TFTP Backoff Start	Initial value for TFTP backoff	1sec		
CPE	TFTP Backoff End	Last value for TFTP back-off	16 sec		
CPE	TFTP Request Retries	Number of retries on TFTP request	16		
CPE	TFTP Download Retries	Number of retries on entire TFTP downloads	3		
CPE	TFTP Wait	The wait between TFTP retry sequences	10 min		
CPE	ToD Retries	Number of Retries per ToD Retry Period	3		
CPE	ToD Retry Period	Time period for ToD retries	5 min		
BS	T9	Registration Timeout, the time allowed between the BS sending a RNG-RSP (success) to a CPE, and receiving a REG-REQ from that same CPE.	15 min	15 min	
CPE					
BS	T10	Wait for Transaction End timeout			3 sec

## 6.12 Encodings for Configuration and MAC-Layer Messaging

The following type/length/value encodings MUST be used in both the configuration file (see <TBD>), in CPE registration requests and in Dynamic Service Messages. All multi-octet quantities are in network-byte order, i.e., the octet containing the most-significant bits is the first transmitted on the wire.

The following configuration settings MUST be supported by all CPEs which are compliant with this specification.

### 6.12.1 Configuration File and Registration Settings

These settings are found in the configuration file and, if present, MUST be forwarded by the CPE to the BS in its Registration Request.

### 6.12.1.1 Downstream Frequency Configuration Setting

The receive frequency to be used by the CPE. It is an override for the channel selected during scanning. This is the center frequency of the downstream channel in Hz stored as a 32-bit binary number.

Type	Length	Value
1	4	Rx Frequency

Valid Range:

The receive frequency MUST be a multiple of 1000 Hz.

### 6.12.1.2 Upstream Channel ID Configuration Setting

The upstream channel ID which the CPE MUST use. The CPE MUST listen on the defined downstream channel until an upstream channel description message with this ID is found. It is an override for the channel selected during initialization.

Type	Length	Value
2	1	Channel ID

### 6.12.1.3 Network Access Control Object

If the value field is a 1, CPE attached to this CPE are allowed access to the network, based on CPE provisioning. If the value of this field is a 0, the CPE MUST NOT forward traffic from attached CPE to the RF MAC network, but MUST continue to accept and generate traffic from the CPE itself. The value of this field does not affect BS service flow operation and does not affect BS data forwarding operation.

Type	Length	On / Off
3	1	1 or 0

Note: The intent of “NACO = 0” is that the CPE does not forward traffic from any attached CPE onto the BWA network. (A CPE is any client device attached to that CPE, regardless of how that attachment is implemented.) However, with “NACO = 0”, management traffic to the CPE is not restricted. Specifically, with NACO off, the CPE remains manageable, including sending/receiving management traffic such as (but not limited to):

- ARP: allow the modem to resolve IP addresses, so it can respond to queries or send traps.
- DHCP: allow the modem to renew its IP address lease.
- ICMP: enable network troubleshooting for tools such as “ping” and “traceroute.”
- ToD: allow the modem to continue to synchronize its clock after boot.
- TFTP: allow the modem to download either a new configuration file or a new software image.
- SYSLOG: allow the modem to report network events.
- SNMP: allow management activity

With NACO off, the primary upstream and primary downstream service flows of the CPE remain operational only for management traffic to and from the CPE. With respect to BWA provisioning, a BS should ignore the NACO value and allocate any service flows that have been authorized by the provisioning server.

#### 6.12.1.4 Downstream Modulation Configuration Setting

The allowed downstream modulation types that can be used by the CPE.

Type	Length	Value
4	1	bit #0: QPSK bit #1: 16-QAM bit #2: 64-QAM bit #3-7: reserved must be set to zero

#### 6.12.1.5 CPE Message Integrity Check (MIC) Configuration Setting

The value field contains the CPE message integrity check code. This is used to detect unauthorized modification or corruption of the configuration file.

Type	Length	Value
6	16	d1 d2..... d16

#### 6.12.1.6 BS Message Integrity Check (MIC) Configuration Setting

The value field contains the BS message integrity check code. This is used to detect unauthorized modification or corruption of the configuration file.

Type	Length	Value
7	16	d1 d2..... d16

#### 6.12.1.7 Maximum Number of Subscribers

The maximum number of Subscribers that can be granted access through a CPE during a CPE epoch. The CPE epoch is the time between startup and hard reset of the modem. The maximum number of Subscribers's MUST be enforced by the CPE.

Type	Length	Value
18	1	

If present, the value MUST be positive and non-zero. The non-existence of this option means the default value of 1.

Note: This is a limit on the maximum number of CPEs a CPE will grant access to. Hardware limitations of a given modem implementation may require the modem to use a lower value.

#### 6.12.1.8 TFTP Server Timestamp

The sending time of the configuration file in seconds. The definition of time is as in [RFC-868]

Type	Length	Value
19	4	Number of seconds since 00:00 1 Jan 1900

Note: The purpose of this parameter is to prevent replay attacks with old configuration files.

### 6.12.1.9 TFTP Server Provisioned Modem Address

The IP Address of the modem requesting the configuration file.

Type	Length	Value
20	4	IP Address

Note: The purpose of this parameter is to prevent IP spoofing during registration.

### 6.12.1.10 Upstream Service Flow Encodings

This field defines the parameters associated with upstream scheduling for one Service Flow. Refer to Section 6.12.5.1.

Type	Length	Value
24	n	

### 6.12.1.11 Downstream Service Flow Encodings

This field defines the parameters associated with downstream scheduling for one Service Flow. Refer to Section 6.12.5.2.

Type	Length	Value
------	--------	-------

### 6.12.1.12 Privacy Enable

This configuration setting enables/disables Privacy on the Primary Service Flow and all other Service Flows for this CPE.

Type	Length	Value
29	1	0 — Disable 1 — Enable

The default value of this parameter is 1 — privacy enabled.

### 6.12.1.13 Vendor-Specific Information

Vendor-specific information for CPE modems, if present, MUST be encoded in the vendor specific information field (VSIF) (code 43) using the Vendor ID field (6.12.3.2) to specify which TLV tuples apply to which vendors products. The Vendor ID MUST be the first TLV embedded inside VSIF. If the first TLV inside VSIF is not a Vendor ID, then the TLV must be discarded.

This configuration setting MAY appear multiple times. The same Vendor ID MAY appear multiple times. This configuration setting MAY be nested inside a Packet Classification Configuration Setting, a Service Flow Configuration Setting, or a Service Flow Response. However, there MUST NOT be more than one Vendor ID TLV inside a single VSIF.

Type	Length	Value
43	n	per vendor definition

Example:

Configuration with vendor A specific fields and vendor B specific fields:



VSIF (43) + n (number of bytes inside this VSIF)  
 8 (Vendor ID Type) + 3 (length field) + Vendor ID of Vendor A  
 Vendor A Specific Type #1 + length of the field + Value #1  
 Vendor A Specific Type #2 + length of the field + Value #2

VSIF (43) + m (number of bytes inside this VSIF)  
 8 (Vendor ID Type) + 3 (length field) + Vendor ID of Vendor B  
 Vendor B Specific Type + length of the field + Value

### 6.12.2 Configuration-File-Specific Settings

These settings are found in only the configuration file. They MUST NOT be forwarded to the BS in the Registration Request.

#### 6.12.2.1 End-of-Data Marker

This is a special marker for end of data.

It has no length or value fields.

Type
255

#### 6.12.2.2 Pad Configuration Setting

This has no length or value fields and is only used following the end of data marker to pad the file to an integral number of 32-bit words.

Type
0

#### 6.12.2.3 Software Upgrade Filename

The filename of the software upgrade file for the CPE. The filename is a fully qualified directory-path name. The file is expected to reside on a TFTP server identified in a configuration setting option defined in Appendix D.2.2. See Section 5.3.1.3.1.1.

Type	Length	Value
9	n	filename

#### 6.12.2.4 SNMP Write-Access Control

This object makes it possible to disable SNMP “Set” access to individual MIB objects. Each instance of this object controls access to all of the writeable MIB objects whose Object ID (OID) prefix matches. This object may be repeated to disable access to any number of MIB objects.

Type	Length	Value
10	n	OID prefix plus control flag

Where n is the size of the ASN.1 Basic Encoding Rules [ISO8025] encoding of the OID prefix plus one byte for the control flag.

The control flag may take values:

- 0 - allow write-access
- 1 - disallow write-access

Any OID prefix may be used. The Null OID 0.0 may be used to control access to all MIB objects. (The OID 1.3.6.1 will have the same effect.)

When multiple instances of this object are present and overlap, the longest (most specific) prefix has precedence. Thus, one example might be

someTable disallow write-access

someTable.1.3 allow write-access

This example disallows access to all objects in someTable except for someTable.1.3.

#### 6.12.2.5 SNMP MIB Object

This object allows arbitrary SNMP MIB objects to be Set via the TFTP-Registration process.

Type	Length	Value
11	n	variable binding

where the value is an SNMP VarBind as defined in [RFC-1157]. The VarBind is encoded in ASN.1 Basic Encoding Rules, just as it would be if part of an SNMP Set request.

The CPE modem MUST treat this object as if it were part of an SNMP Set Request with the following caveats:

- It MUST treat the request as fully authorized (it cannot refuse the request for lack of privilege).
- SNMP Write-Control provisions (see previous section) do not apply.
- No SNMP response is generated by the CPE.

This object MAY be repeated with different VarBinds to “Set” a number of MIB objects. All such Sets MUST be treated as if simultaneous.

Each VarBind MUST be limited to 255 bytes.

#### 6.12.2.6 CPE Ethernet MAC Address

This object configures the CPE with the Ethernet MAC address of a CPE device. This object may be repeated to configure any number of CPE device addresses.

Type	Length	Value
14	6	Ethernet MAC Address of CPE

#### 6.12.2.7 Software Upgrade TFTP Server

The IP address of the TFTP server, on which the software upgrade file for the CPE resides. See Section 5.3.1.3.1.1 and Appendix 6.12.2.3

Type	Length	Value
21	4	ip1,ip2,ip3,ip4

### 6.12.3 Registration-Request/Response-Specific Encodings

These encodings are not found in the configuration file, but are included in the Registration Request. Some encodings are also used in the Registration Response.

The CPE MUST include Modem Capabilities Encodings in its Registration Request. If present in the corresponding Registration Request, the BS MUST include Modem Capabilities in the Registration Response.

#### 6.12.3.1 Modem Capabilities Encoding

The value field describes the capabilities of a particular modem, i.e., implementation dependent limits on the particular features or number of features which the modem can support. It is composed from a number of encapsulated type/length/value fields. The encapsulated sub-types define the specific capabilities for the modem in question. Note that the sub-type fields defined are only valid within the encapsulated capabilities configuration setting string.

Type	Length	Value
5	n	

The set of possible encapsulated fields is described below.

##### 6.12.3.1.1 Privacy Support

The value is the BPI support of the CPE.

Type	Length	Value
5.6	1	0 Privacy Supported 1 - 255 Reserved

##### 6.12.3.1.2 Upstream CID Support

The field shows the number of Upstream CIDs the modem can support.

Type	Length	Value
5.8	1	Number of Upstream CIDs the CPE can support.

If the number of CIDs is 0 that means the Modem can support only 1 CID.

##### 6.12.3.1.3 Transmit Equalizer Taps per Symbol

This field shows the maximal number of pre-equalizer taps per symbol supported by the CPE.

Note: All CPEs MUST support symbol-spaced equalizer coefficients. CPE support of 2 or 4 taps per symbol is optional. If this tuple is missing, it is implied that the CPE only supports symbol spaced equalizer coefficients.

Type	Length	Value
5.10	1	1, 2 or 4

##### 6.12.3.1.4 Number of Transmit Equalizer Taps

This field shows the number of equalizer taps that are supported by the CPE.

Note: All CPEs MUST support an equalizer length of at least 8 symbols. CPE support of up to 64 T-spaced, T/2-spaced or T/4-spaced taps is optional. If this tuple is missing, it is implied that the CPE only supports an equalizer length of 8 taps.

Type	Length	Value
5.11	1	8 to 64

#### 6.12.3.1.5 CPE Demodulator Types

This field indicates the different modulation types supported by the CPE for downstream reception.

Type	Length	Value
5.12	1	bit #0: QPSK bit #1: 16-QAM bit #2: 64-QAM bit #3: 8-PSK bit #4-7: reserved must be set to zero

#### 6.12.3.1.6 CPE Modulator Types

This field indicates the different modulation types supported by the CPE for upstream transmission.

Type	Length	Value
5.13	1	bit #0: QPSK bit #1: 16-QAM bit #2: 64-QAM bit #3-7: reserved must be set to zero

#### 6.12.3.1.7 Duplexing Support

This field indicates the different duplexing modes the CPE is able to support.

Type	Length	Value
5.14	1	bit #0: FDD (continuous downstream) bit #1: FDD (burst downstream) bit #2: Half-Duplex FDD bit #3: TDD bit #4-7: reserved must be set to zero

#### 6.12.3.1.8 Bandwidth Allocation Support

This field indicates the different bandwidth allocation modes the CPE is able to support.

Type	Length	Value
5.15	1	bit #0: Grant per Connection bit #1: Grant per Terminal (CPE) bit #2-7: reserved must be set to zero

#### 6.12.3.2 Vendor ID Encoding

The value field contains the vendor identification specified by the three-byte vendor-specific Organization Unique Identifier of the CPE MAC address.

The Vendor ID **MUST** be used in a Registration Request, but **MUST NOT** be used as a stand-alone configuration file element. It **MAY** be used as a sub-field of the Vendor Specific Information Field in a configuration file. When used as a sub-field of the Vendor Specific Information field, this identifies the Vendor ID of the CPEs which are intended to use this information. When the vendor ID is used in a Registration Request, then it is the Vendor ID of the CPE sending the request.

Type	Length	Value
8	3	v1, v2, v3

### 6.12.3.3 Service(s) Not Available Response

This configuration setting **MUST** be included in the Registration Response message if the BS is unable or unwilling to grant any of the requested classes of service that appeared in the Registration Request. Although the value applies only to the failed service class, the entire Registration Request **MUST** be considered to have failed (none of the class-of-service configuration settings are granted).

Type	Length	Value
13	3	Class ID, Type, Confirmation Code

Where

Class ID	is the class-of-service class from the request which is not available
Type	is the specific class-of-service object within the class which caused the request to be rejected
Confirmation Code	Refer to 6.12.9.

### 6.12.4 Dynamic-Service-Message-Specific Encodings

These encodings are not found in the configuration file, nor in the Registration Request/Response signaling. They are only found in Dynamic Service Addition, Dynamic Service Change and Dynamic Service Deletion Request/Response messages:

#### 6.12.4.1 HMAC-Digest

The HMAC-Digest setting is a keyed message digest. If privacy is enabled, the HMAC-Digest Attribute **MUST** be the final Attribute in the Dynamic Service message's Attribute list. The message digest is performed over the all of the Dynamic Service parameters (starting immediately after the MAC Management Message Header and up to, but not including the HMAC Digest setting), other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiver to authenticate the message. The HMAC-Digest algorithm, and the upstream and downstream key generation requirements are documented in [DOCSIS8].

This parameter contains a keyed hash used for message authentication. The HMAC algorithm is defined in [RFC2104]. The HMAC algorithm is specified using a generic cryptographic hash algorithm. Baseline Privacy uses a particular version of HMAC that employs the Secure Hash Algorithm (SHA-1), defined in [SHA].

A summary of the HMAC-Digest Attribute format is shown below. The fields are transmitted from left to right.

Type	Length	Value
27	20	A 160-bit (20 octet) keyed SHA hash

### 6.12.4.2 Authorization Block

The Authorization Block contains an authorization “hint” from the CPE to the BS. The specifics of the contents of this “hint” are beyond the scope of this specification, but include [PKT-DQOS].

The Authorization Block MAY be present in CPE-initiated DSA-REQ and DSC-REQ messages. This parameter MUST NOT be present in DSA-RSP and DSC-RSP message, nor in BS-initiated DSA-REQ nor DSC-REQ messages.

The Authorization Block information applies to the entire contents of the DSC message. Thus, only a single Authorization Block MAY be present per DSA-REQ or DSC-REQ message. The Authorization Block, if present, MUST be passed to the Authorization Module in the BS. The Authorization Block information is only processed by the Authorization Module.

Type	Length	Value
30	n	Sequence of n octets

### 6.12.5 Quality-of-Service-Related Encodings

The following type/length/value encodings MUST be used in the configuration file, registration messages, and Dynamic Service messages to encode parameters for Service Flows. All multi-octet quantities are in network-byte order, i.e., the octet containing the most-significant bits is the first transmitted on the wire.

The following configuration settings MUST be supported by all CPEs which are compliant with this specification.

#### 6.12.5.1 Upstream Service Flow Encodings

This field defines the parameters associated with upstream scheduling for a Service Flow. It is somewhat complex in that it is composed from a number of encapsulated type/length/value fields.

Note that the encapsulated upstream and downstream Service Flow configuration setting strings share the same subtype field numbering plan, because many of the subtype fields defined are valid for both types of configuration settings. These type fields are not valid in other encoding contexts.

Type	Length	Value
24	n	

#### 6.12.5.2 Downstream Service Flow Encodings

This field defines the parameters associated with downstream scheduling for a Service Flow. It is somewhat complex in that it is composed from a number of encapsulated type/length/value fields.

Note that the encapsulated upstream and downstream flow classification configuration setting strings share the same subtype field numbering plan, because many of the subtype fields defined are valid for both types of configuration settings except Service Flow encodings.

Type	Length	Value
25	n	

### 6.12.5.3 General Service Flow Encodings

#### 6.12.5.3.1 Service Flow Reference

The Service Flow Reference is used to associate a packet classifier encoding with a Service Flow encoding. A Service Flow Reference is only used to establish a Service Flow ID. Once the Service Flow exists and has an assigned Service Flow ID, the Service Flow Reference MUST no longer be used.

Type	Length	Value
[24/25].1	2	1 - 65535

#### 6.12.5.3.2 Service Flow Identifier

The Service Flow Identifier is used by the BS as the primary reference of a Service Flow. Only the BS can issue a Service Flow Identifier. It uses this parameterization to issue Service Flow Identifiers in BS-initiated DSA/DSC-Requests and in its REG/DSA/DSC-Response to CPE-initiated REG/DSA/DSC-Requests. The CPE specifies the SFID of a service flow using this parameter in a DSC-REQ message.

The configuration file MUST NOT contain this parameter.

Type	Length	Value
[24/25].2	4	1 - 4,294,967,295

#### 6.12.5.3.3 Service Identifier

The value of this field specifies the Service Identifier assigned by the BS to a Service Flow with a non-null AdmittedQosParameterSet or ActiveQosParameterSet. This is used in the bandwidth allocation MAP to assign upstream bandwidth. This field MUST be present in BS-initiated DSA-REQ or DSC-REQ message related to establishing an admitted or active upstream Service Flow. This field MUST also be present in REG-RSP, DSA-RSP and DSC-RSP messages related to the successful establishment of an admitted or active upstream Service Flow.

Even though a Service Flow has been successfully admitted or activated (i.e. has an assigned Service ID) the Service Flow ID MUST be used for subsequent DSx message signalling as it is the primary handle for a service flow. If a Service Flow is no longer admitted or active (via DSC-REQ) its Service ID MAY be reassigned by the BS.

SubType	Length	Value
[24/25].3	2	SID (low-order 14 bits)

#### 6.12.5.3.4 Service Class Name

The value of the field refers to a predefined BS service configuration to be used for this Service Flow.

Type	Length	Value
[24/25].4	2 to 16	Zero-terminated string of ASCII characters.

Note: The length includes the terminating zero.

When the Service Class Name is used in a Service Flow encoding, it indicates that all the unspecified QoS Parameters of the Service Flow need to be provided by the BS. It is up to the operator to synchronize the definition of Service Class Names in the BS and in the configuration file.

#### 6.12.5.4 Service Flow Error Encodings

This field defines the parameters associated with Service Flow Errors.

Type	Length	Value
[24/25].5	n	

A Service Flow Error Parameter Set is defined by the following individual parameters: Confirmation Code, Errored Parameter and Error Message.

The Service Flow Error Parameter Set is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the recipient's response to a Service Flow establishment request in a REG-REQ, DSA-REQ or DSC-REQ message. The Service Flow Error Parameter Set is returned in REG-ACK, DSA-ACK and DSC-ACK messages to indicate the recipient's response to the expansion of a Service Class Name in a corresponding REG-RSP, DSA-RSP or DSC-RSP.

On failure, the sender **MUST** include one Service Flow Error Parameter Set for each failed Service Flow requested in the REG-REQ, DSA-REQ or DSC-REQ message. On failure, the sender **MUST** include one Service Flow Error Parameter Set for each failed Service Class Name expansion in the REG-RSP, DSA-RSP or DSC-RSP message. Service Flow Error Parameter Set for the failed Service Flow **MUST** include the Confirmation Code and Errored Parameter and **MAY** include an Error Message. If some Service Flow Parameter Sets are rejected but other Service Flow Parameter Sets are accepted, then Service Flow Error Parameters Sets **MUST** be included for only the rejected Service Flow.

On success of the entire transaction, the RSP or ACK message **MUST NOT** include a Service Flow Error Parameter Set.

Multiple Service Flow Error Parameter Sets **MAY** appear in a REG-RSP, DSA-RSP, DSC-RSP, REG-ACK, DSA-ACK or DSC-ACK message, since multiple Service Flow parameters may be in error. A message with even a single Service Flow Error Parameter Set **MUST NOT** contain any QoS Parameters.

A Service Flow Error Parameter Set **MUST NOT** appear in any REG-REQ, DSA-REQ or DSC-REQ messages.

##### 6.12.5.4.1 Errored Parameter

The value of this parameter identifies the subtype of a requested Service Flow parameter in error in a rejected Service Flow request or Service Class Name expansion response. A Service Flow Error Parameter Set **MUST** have exactly one Errored Parameter TLV within a given Service Flow Encoding.

Subtype	Length	Value
[24/25].5.1	1	Service Flow Encoding Subtype in Error

##### 6.12.5.4.2 Error Code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in 6.12.9. A Service Flow Error Parameter Set **MUST** have exactly one Error Code within a given Service Flow Encoding.

Subtype	Length	Value
[24/25].5.2	1	Confirmation code

A value of okay(0) indicates that the Service Flow request was successful. Since a Service Flow Error Parameter Set only applies to errored parameters, this value **MUST NOT** be used.



#### 6.12.5.4.3 Error Message

This subtype is optional in a Service Flow Error Parameter Set. If present, it indicates a text string to be displayed on the CPE console and/or log that further describes a rejected Service Flow request. A Service Flow Error Parameter Set MAY have zero or one Error Message subtypes within a given Service Flow Encoding.

SubType	Length	Value
[24/25].5.3	n	Zero-terminated string of ASCII characters.

Note: The length N includes the terminating zero.

Note: The entire Service Flow Encoding message must have a total length of less than 256 characters.

#### 6.12.5.5 Common Upstream and Downstream Quality-of-Service Parameter Encodings

The remaining Type 24 & 25 parameters are QoS Parameters. Any given QoS Parameter type MUST appear zero or one times per Service Flow Encoding.

##### 6.12.5.5.1 Quality of Service Parameter Set Type

This parameter MUST appear within every Service flow Encoding. It specifies the proper application of the QoS Parameter Set: to the Provisioned set, the Admitted set, and/or the Active set. When two QoS Parameter Sets are the same, a multi-bit value of this parameter MAY be used to apply the QoS parameters to more than one set. A single message MAY contain multiple QoS parameter sets in separate type 24/25 Service Flow Encodings for the same Service Flow. This allows specification of the QoS Parameter Sets when their parameters are different. Bit 0 is the LSB of the Value field.

For every Service Flow that appears in a Registration-Request or Registration-Response message, there MUST be a Service Flow Encoding that specifies a ProvisionedQoSParameterSet. This Service Flow Encoding, or other Service Flow Encoding(s), MAY also specify an Admitted and/or Active set.

Type	Length	Value
[24/25].6	1	Bit # 0 Provisioned Set
		Bit # 1 Admitted Set
		Bit # 2 Active Set

**Table F-6. Values Used in REG-REQ and REG-RSP Messages**

Value	Messages
001	Apply to Provisioned set only
011	Apply to Provisioned and Admitted set, and perform admission control
101	Apply to Provisioned and Active sets, perform admission control, and activate this Service flow
111	Apply to Provisioned, Admitted, and Active sets; perform admission control and activate this Service Flow

**Table F-7. Values Used In Dynamic Service Messages.**

Value	Messages
000	Sect Active and Admitted sets to Null
010	Perform admission control and apply to Admitted set
100	Check against Admitted set in separate Service flow Encoding, perform admission control if needed, activate this Service Flow, and apply to Active set
110	Perform admission control and activate this Service Flow, apply parameters to both Admitted and Active sets

A BS MUST handle a single update to each of the Active and Admitted QoS parameter sets. The ability to process multiple Service Flow Encodings that specify the same QoS parameter set is NOT required, and is left as a vendor-specific function. If a DSA/DSC contains multiple updates to a single QoS parameter set and the vendor does not support such updates, then the BS MUST reply with error code 2, reject-unrecognized-configuration-setting.

#### 6.12.7.5.2 Traffic Priority

The value of this parameter specifies the priority assigned to a Service Flow. Given two Service Flows identical in all QoS parameters besides priority, the higher priority Service Flow SHOULD be given lower delay and higher buffering preference. For otherwise non-identical Service Flows, the priority parameter SHOULD NOT take precedence over any conflicting Service Flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.

For upstream service flows, the BS SHOULD use this parameter when determining precedence in request service and grant generation, and the CPE MUST preferentially select contention Request opportunities for Priority Request Service IDs (refer to A.2.3) based on this priority and its Request/Transmission Policy (refer to 6.12.7.6.3).

Type	Length	Value
[24/25].7	1	0 to 7 — Higher numbers indicate higher priority

Note: The default priority is 0.

#### 6.12.7.5.3 Maximum Sustained Traffic Rate

This parameter is the rate parameter R of a token-bucket-based rate limit for packets. R is expressed in bits per second, and must take into account all MAC frame data PDU of the Service Flow from the byte following the MAC header HCS to the end of the CRC<sup>1</sup>. The number of bytes forwarded-(in bytes) is limited during any time interval T by Max(T), as described in the expression

$$\text{Max}(T) = T * (R / 8) + B, (1)$$

where the parameter B (in bytes) is the Maximum Traffic Burst Configuration Setting (refer to 6.12.7.5.5).

Note: This parameter does not limit the instantaneous rate of the Service Flow.

Note: The specific algorithm for enforcing this parameter is not mandated here. Any implementation which satisfies the above equation is conformant.

<sup>1</sup>The payload size includes every PDU in a Concatenated MAC Frame.

Note: If this parameter is omitted or set to zero, then there is no explicitly-enforced traffic rate maximum. This field specifies only a bound, not a guarantee that this rate is available.

#### 6.12.7.5.4 Upstream Maximum Sustained Traffic Rate

For an upstream Service Flow, the CPE **MUST NOT** request bandwidth exceeding the Max(T) requirement in (1) during any interval T because this could force the BS to fill MAPs with deferred grants.

The CPE **MUST** defer upstream packets that violate (1) and “rate shape” them to meet the expression, up to a limit as implemented by vendor buffering restrictions.

The BS **MUST** enforce expression (1) on all upstream data transmissions, including data sent in contention. The BS **MAY** consider unused grants in calculations involving this parameter. The BS **MAY** enforce this limit by any of the following methods: (a) discarding over-limit requests, (b) deferring (through zero-length grants) the grant until it is conforming to the allowed limit, or (c) discarding over-limit data packets. A BS **MUST** report this condition to a policy module. If the BS is policing by discarding either packets or requests, the BS **MUST** allow a margin of error between the CPE and BS algorithms.

Type	Length	Value
24.8	4	R (in bits per second)

Downstream Maximum Sustained Traffic Rate

For a downstream Service Flow, this parameter is only applicable at the BS. The BS **MUST** enforce expression (1) on all downstream data transmissions. The BS **MUST NOT** forward downstream packets that violates (1) in any interval T. The BS **SHOULD** “rate shape” the downstream traffic by enqueueing packets arriving in excess of (1), and delay them until the expression can be met.

This parameter is not intended for enforcement on the CPE.

Type	Length	Value
25.8	4	R (in bits per second)

#### 6.12.7.5.5 Maximum Traffic Burst

The value of this parameter specifies the token bucket size B (in bytes) for this Service Flow as described in expression (1). This value is calculated from the byte following the MAC header HCS to the end of the CRC<sup>2</sup>.

If this parameter is omitted, then the default B is 1522 bytes. The minimum value of B is the larger of 1522 bytes or the value of Maximum Concatenated Burst Size (refer to 6.12.7.6.1).

Type	Length	Value
[24/25].9	4	B (bytes)

Note: The specific algorithm for enforcing this parameter is not mandated here. Any implementation which satisfies the above equation is conformant.

#### 6.12.7.5.6 Minimum Reserved Traffic Rate

This parameter specifies the minimum rate, in bits/sec, reserved for this Service Flow. The BS **SHOULD** be able to satisfy bandwidth requests for a Service Flow up to its Minimum Reserved Traffic Rate. If less bandwidth than its Minimum Reserved Traffic Rate is requested for a Service Flow, the BS **MAY** reallocate

<sup>2</sup>The payload size includes every PDU in a Concatenated MAC Frame.

the excess reserved bandwidth for other purposes. The aggregate Minimum Reserved Traffic Rate of all Service Flows MAY exceed the amount of available bandwidth. This value of this parameter is calculated from the byte following the MAC header HCS to the end of the CRC<sup>3</sup>. If this parameter is omitted, then it defaults to a value of 0 bits/sec (i.e., no bandwidth is reserved for the flow by default).

This field is only applicable at the BS and MUST be enforced by the BS.

Type	Length	Value
[24/25].10	4	

Note: The specific algorithm for enforcing the value specified in this field is not mandated here.

#### 6.12.7.5.7 Assumed Minimum Reserved Rate Packet Size

The value of this field specifies an assumed minimum packet size (in bytes) for which the Minimum Reserved Traffic Rate will be provided. This parameter is defined in bytes and is specified as the bytes following the MAC header HCS to the end of the CRC<sup>4</sup>. If the Service Flow sends packets of a size smaller than this specified value, such packets will be treated as being of the size specified in this parameter for calculating the minimum Reserved Traffic Rate and for calculating bytes counts (e.g. bytes transmitted) which may ultimately be used for billing.

The BS MUST apply this parameter to its Minimum Reserved Traffic Rate algorithm. This parameter is used by the BS to estimate the per packet overhead of each packet in the service flow.

If this parameter is omitted, then the default value is BS implementation dependent.

Type	Length	Value
[24/25].11	2	

#### 6.12.7.5.8 Timeout for Active QoS Parameters

The value of this parameter specifies the maximum duration resources remain unused on an active Service Flow. If there is no activity on the Service Flow within this time interval, the BS MUST change the active and admitted QoS Parameter Sets to null. The BS MUST signal this resource change with a DSC-REQ to the CPE.

If defined, this parameter MUST be enforced at the BS and SHOULD NOT be enforced at the CPE.

Type	Length	Value
[24/25].12	2	seconds

The value of 0 means that the flow is of infinite duration and MUST NOT be timed out due to inactivity. The default value is 0.

#### 6.12.7.5.9 Timeout for Admitted QoS Parameters

The value of this parameter specifies the duration that the BS MUST hold resources for a Service Flow's Admitted QoS Parameter Set while they are in excess of its Active QoS Parameter Set. If there is no DSC-REQ to activate the Admitted QoS Parameter Set within this time interval, the resources that are admitted

<sup>3</sup>The payload size includes every PDU in a Concatenated MAC Frame.

<sup>4</sup>The payload size includes every PDU in a Concatenated MAC Frame.

but not activated **MUST** be released, and only the active resources retained. The BS **MUST** set the Admitted QoS Parameter Set equal to the Active QoS Parameter Set for the Service Flow and initiate a DSC-REQ exchange with the CPE to inform it of the change.

If this parameter is omitted, then the default value is 200 seconds. The value of 0 means that the Service Flow can remain in the admitted state for an infinite amount of time and **MUST NOT** be timed out due to inactivity. However, this is subject to policy control by the BS.

This parameter **MUST** be enforced by the BS. The BS **MAY** set the response value less than the requested value.

Type	Length	Value
[24/25].13	2	seconds

#### 6.12.7.5.10 Vendor Specific QoS Parameters

This allows vendors to encode vendor-specific QoS parameters. The Vendor ID **MUST** be the first TLV embedded inside Vendor Specific QoS Parameters. If the first TLV inside Vendor Specific QoS Parameters is not a Vendor ID, then the TLV must be discarded. (Refer to 6.12.1.13)

Type	Length	Value
[24/25].43	n	

#### 6.12.7.6 Upstream-Specific QoS Parameter Encodings

##### 6.12.7.6.1 Maximum Concatenated Burst

The value of this parameter specifies the maximum concatenated burst (in bytes) which a Service Flow is allowed. This parameter is calculated from the FC byte of the Concatenation MAC Header to the last CRC in the concatenated MAC frame.

A value of 0 means there is no limit. The default value is 0.

This field is only applicable at the CPE. If defined, this parameter **MUST** be enforced at the CPE.

Note: This value does not include any physical layer overhead.

Type	Length	Value
24.14	2	

Note: This applies only to concatenated bursts. It is legal and, in fact, it may be useful to set this smaller than the maximum Ethernet packet size. Of course, it is also legal to set this equal to or larger than the maximum Ethernet packet size.

##### 6.12.7.6.2 Service Flow Scheduling Type

The value of this parameter specifies which upstream scheduling service is used for upstream transmission requests and packet transmissions. If this parameter is omitted, then the Best Effort service **MUST** be assumed.

This parameter is only applicable at the BS. If defined, this parameter MUST be enforced by the BS.

Type	Length	Value
24.15	1	0 Reserved 1 for Undefined (BS implementation-dependent <sup>5</sup> ) 2 for Best Effort 3 for Non-Real-Time Polling Service 4 for Real-Time Polling Service 5 for Unsolicited Grant Service with Activity Detection 6 for Unsolicited Grant Service 7 through 255 are reserved for future use

### 6.12.7.6.3 Request/Transmission Policy

The value of this parameter specifies which IUC opportunities the CPE uses for upstream transmission requests and packet transmissions for this Service Flow, whether requests for this Service Flow may be piggybacked with data and whether data packets transmitted on this Service Flow can be concatenated, fragmented, or have their payload headers suppressed. For UGS, it also specifies how to treat packets that do not fit into the UGS grant. See section 8.2 for requirements related to settings of the bits of this parameter for each Service Flow Scheduling Type.

This parameter is required for all Service Flow Scheduling Types except Best Effort. If omitted in a Best Effort Service Flow QoS parameter Set, the default value of zero MUST be used. Bit #0 is the LSB of the Value field. Bit 0 is the LSB of the Value field

Type	Length	Value
24.16	4	Bit #0 The Service Flow MUST NOT use “all CPEs” broadcast request opportunities. Bit #1 The Service Flow MUST NOT use Priority Request multicast request opportunities. (Refer to A.2.3) Bit #2 The Service Flow MUST NOT use Request/Data opportunities for Requests Bit #3 The Service Flow MUST NOT use Request/Data opportunities for Data Bit #4 The Service Flow MUST NOT piggyback requests with data. Bit #5 The Service Flow MUST NOT concatenate data. Bit #6 The Service Flow MUST NOT fragment data Bit #7 The Service Flow MUST NOT suppress payload headers Bit #8 <sup>6</sup> The Service Flow MUST drop packets that do not fit in the Unsolicited Grant Size <sup>7</sup> All other bits are reserved.

Note: Data grants include both short and long data grants.

<sup>5</sup>The specific implementation dependent scheduling service type could be defined in the 24.43 Vendor Specific Information Field.

<sup>6</sup>This bit only applies to Service Flows with the Unsolicited Grant Service Flow Scheduling Type, if this bit is set on any other Service Flow Scheduling type it MUST be ignored

<sup>7</sup>Packets that classify to an Unsolicited Grant Service Flow and are larger than the Grant Size associated with that Service Flow are normally transmitted on the Primary Service Flow. This parameter overrides that default behavior.

#### 6.12.7.6.4 Nominal Polling Interval

The value of this parameter specifies the nominal interval (in units of microseconds) between successive unicast request opportunities for this Service Flow on the upstream channel. This parameter is typically suited for Real-Time and Non-Real-Time Polling Service.

The ideal schedule for enforcing this parameter is defined by a reference time  $t_0$ , with the desired transmission times  $t_i = t_0 + i \cdot \text{interval}$ . The actual poll times,  $t'_i$  MUST be in the range  $t_i \leq t'_i \leq t_i + \text{jitter}$ , where interval is the value specified with this TLV, and jitter is Tolerated Poll Jitter. The accuracy of the ideal poll times,  $t_i$ , are measured relative to the BS Master Clock used to generate timestamps (refer to Section 5.4.1.1).

This field is only applicable at the BS. If defined, this parameter MUST be enforced by the BS.

Type	Length	Value
24.17	4	$\mu\text{sec}$

#### 6.12.7.6.5 Tolerated Poll Jitter

The values in this parameter specifies the maximum amount of time that the unicast request interval MAY be delayed from the nominal periodic schedule (measured in microseconds) for this Service Flow.

The ideal schedule for enforcing this parameter is defined by a reference time  $t_0$ , with the desired poll times  $t_i = t_0 + i \cdot \text{interval}$ . The actual poll,  $t'_i$  MUST be in the range  $t_i \leq t'_i \leq t_i + \text{jitter}$ , where jitter is the value specified with this TLV and interval is the Nominal Poll Interval. The accuracy of the ideal poll times,  $t_i$ , are measured relative to the BS Master Clock used to generate timestamps (refer to Section 5.4.1.1).

This parameter is only applicable at the BS. If defined, this parameter represents a service commitment (or admission criteria) at the BS.

Type	Length	Value
24.18	4	$\mu\text{sec}$

#### 6.12.7.6.6 Unsolicited Grant Size

The value of this parameter specifies the unsolicited grant size in bytes. The grant size includes the entire MAC frame data PDU from the Frame Control byte to end of the MAC frame.

This parameter is applicable at the BS and MUST be enforced at the BS.

Type	Length	Value
24.19	2	

Note: For UGS, this parameter should be used by the BS to compute the size of the unsolicited grant in minislots.

#### 6.12.7.6.7 Nominal Grant Interval

The value of this parameter specifies the nominal interval (in units of microseconds) between successive data grant opportunities for this Service Flow. This parameter is required for Unsolicited Grant and Unsolicited Grant with Activity Detection Service Flows.

The ideal schedule for enforcing this parameter is defined by a reference time  $t_0$ , with the desired transmission times  $t_i = t_0 + i \cdot \text{interval}$ . The actual grant times,  $t'_i$  MUST be in the range  $t_i \leq t'_i \leq t_i + \text{jitter}$ , where interval is the value specified with this TLV, and jitter is the Tolerated Grant Jitter. When an upstream Service Flow with either Unsolicited Grant or Unsolicited Grant with Activity Detection scheduling becomes active, the first grant MUST define the start of this interval, i.e. the first grant MUST be for an ideal transmission time,  $t_i$ . When multiple grants per interval are requested, all grants MUST be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter MUST be maintained by the BS for all grants in this Service Flow. The accuracy of the ideal grant times,  $t_i$ , are measured relative to the BS Master Clock used to generate timestamps (refer to Section 5.4.1.1).

This field is mandatory for Unsolicited Grant and Unsolicited Grant with Activity Detection Scheduling Types. This field is only applicable at the BS, and MUST be enforced by the BS.

Type	Length	Value
24.20	4	$\mu\text{sec}$

#### 6.12.7.6.8 Tolerated Grant Jitter

The values in this parameter specifies the maximum amount of time that the transmission opportunities MAY be delayed from the nominal periodic schedule (measured in microseconds) for this Service Flow.

The ideal schedule for enforcing this parameter is defined by a reference time  $t_0$ , with the desired transmission times  $t_i = t_0 + i \cdot \text{interval}$ . The actual transmission opportunities,  $t'_i$  MUST be in the range  $t_i \leq t'_i \leq t_i + \text{jitter}$ , where jitter is the value specified with this TLV and interval is the Nominal Grant Interval. The accuracy of the ideal grant times,  $t_i$ , are measured relative to the BS Master Clock used to generate timestamps (refer to Section 5.4.1.1).

This field is mandatory for Unsolicited Grant and Unsolicited Grant with Activity Detection Scheduling Types. This field is only applicable at the BS, and MUST be enforced by the BS.

Type	Length	Value
24.21	4	$\mu\text{sec}$

#### 6.12.7.6.9 Grants per Interval

For Unsolicited Grant Service, the value of this parameter indicates the actual number of data grants per Nominal Grant Interval. For Unsolicited Grant Service with Activity Detection, the value of this parameter indicates the maximum number of Active Grants per Nominal Grant Interval. This is intended to enable the addition of sessions to an existing Unsolicited Grant Service Flow via the Dynamic Service Change mechanism, without negatively impacting existing sessions.

The ideal schedule for enforcing this parameter is defined by a reference time  $t_0$ , with the desired transmission times  $t_i = t_0 + i \cdot \text{interval}$ . The actual grant times,  $t'_i$  MUST be in the range  $t_i \leq t'_i \leq t_i + \text{jitter}$ , where interval is the Nominal Grant Interval, and jitter is the Tolerated Grant Jitter. When multiple grants per interval are requested, all grants MUST be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter MUST be maintained by the BS for all grants in this Service Flow.

This field is mandatory for Unsolicited Grant and Unsolicited Grant with Activity Detection Scheduling Types. This field is only applicable at the BS, and MUST be enforced by the BS.

Type	Length	Value	Valid Range
24.22	1	# of grants	0-127



## 6.12.7.7 Downstream-Specific QoS Parameter Encodings

### 6.12.7.7.1 Maximum Downstream Latency

The value of this parameter specifies the maximum latency between the reception of a packet by the BS on its NSI and the forwarding of the packet to its RF Interface.

If defined, this parameter represents a service commitment (or admission criteria) at the BS and **MUST** be guaranteed by the BS. A BS does not have to meet this service commitment for Service Flows that exceed their minimum downstream reserved rate.

Type	Length	Value
25.14	4	μsec

### 6.12.8 Privacy Configuration Settings Option

This configuration setting describes parameters which are specific to Privacy. It is composed from a number of encapsulated type/length/value fields.

Type	Length	Value
17 (= P_CFG)	n	

### 6.12.9 Confirmation Code

The Confirmation Code (CC) provides a common way to indicate failures for Registration Response, Registration Ack, Dynamic Service Addition-Response, Dynamic Service Addition-Ack, Dynamic Service Delete-Response, Dynamic Service Change-Response and Dynamic Service Change-Ack MAC Management Messages.

Confirmation Code is one of the following:

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)

PRELIMINARY SUBMITTAL

## 7. Authentication and Privacy

<TBD>

PRELIMINARY SUBMITTAL

PRELIMINARY SUBMITTAL

## 8. Transmission Convergence Sublayer

<TBD>

PRELIMINARY SUBMITTAL