Project	**IEEE 802.16 Broadband Wireless Access Working Group**	
Title	Media Access Control Layer Proposal for the 802.16.1 Air Interface Specification	
Date Submitted	2000-07-07	
Source	Glen Sater Motorola Inc. 8220 E. Roosevelt Street, M/D R1106 Scottsdale, AZ 85257	Voice: 480-441-8893 Fax: 480-675-2116 E-mail: g.sater@motorola.com
	Ken Stanwood Ensemble Communications Inc. 9890 Town Centre Dr. San Diego, CA 92121	Voice: 858-404-6544 Fax: 858-458-1401 E-mail: ken@ensemblecom.com
	<u>Additional Contirbutions</u>	<u>Company</u>
	Arun Arunachalam, George Stamatelos	Nortel Networks
	Jeff Foerster	Alcatel
	Scott Marin, Bill Myers	SpectraPoint Wireless, LLC.
	Leland Langston, Wayne Hunter	Crosspan, a Raytheon Telecommunications Company
	Phil Guillemette	SpaceBridge Networks Corporation
	Chet Shirali, Menashe Shahar	Vyyo Inc.
	Karl Stambaugh	Motorola, Inc.
	George Fishel	Communications Consulting Services
	Ray Sanders	CircuitPath Networks Systems
	Moshe Ran	TelesciCOM, Ltd.
	Andrew Sundelin	iSKY
	Yonatan Manor	Oren Semiconductors
	Brian Petry, Mark Vogel	3Com
	James Mollenauer	Technical Strategy Associates
	Carl Eklund, Juha Pihlaja, Kari Rintanen	Nokia
	Doug Gray	Lucent Technologies
	Paolo Baldo	Siemens
	Paul Kennard	Digital Microwave
	Andrea Nascimbene	Ericsson
	Naftali Chayat, Leonid Shousterman, Vladimir Yanover	BreezeCOM
	Demosthenes Kostas	Adaptive Broadband
	Jay Klein	Ensemble Communications
Re:	802.16.1 INVITATION TO CONTRIBUTE: Session #8, Document 80216-00_13r1	
Abstract	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. 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 serivce 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.	
Purpose	To provide a detailed description of a proposed MAC layer specification for IEEE 802.16 WG.	
Notice	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.	

Release	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. Portions of this document are reprinted with permission from Cable Television Laboratories, Inc.
IEEE Patent Policy	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 0.9) <http://ieee802.org/16/ipr/patents/policy.html>, 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." 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 <mailto:r.b.marks@ieee.org> 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 <http://ieee802.org/16/ipr/patents/letters.html>.

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>.

2. Normative References

This standard shall be used in conjunction with the following publications.

[FIPS-46-2]Federal Information Processing Standard Publications 46-2, Data Encryption Standard (DES), December 30, 1993.

[FIPS-74]Federal Information Processing Standards Publication (FIPS PUB) 74, Guidelines for Implementing and Using the Data Encryption Standard, April 1981.

[FIPS-81]Federal Information Processing Standards Publication (FIPS PUB) 81, DES Modes of Operation, December 1980.

[FIPS-140-1]Federal Information Processing Standards Publication (FIPS PUB) 140-1, Security Requirements for Cryptographic Modules, April 1982.

[FIPS-180-1]Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard, April 1995.

[FIPS-186]Federal Information Processing Standards Publication (FIPS PUB) 186, Digital Signature Standard, 18 May 1994.

[IEEE1]IEEE Std 802-1990, IEEE Standards for Local and Metropolitan Area Net-works:Overview and Architecture, December 1990.

[RFC1750]D. Eastlake, S. Crocker, J. Schiller, “Randomness Recommendations for Security”, RFC 1750, December 1994.

[RFC2104]H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, February 1997.

[RFC2202]P. Cheng, R. Glenn, “Test cases for HMAC-MD5 and HMAC-SHA-1”, RFC2202, September 1997.

[RFC2459]R. Housley, W. Ford, W. Polk, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC2459, January 1999.

[RSA]RSA Laboratories, “The Public-Key Cryptography Standards”, RSA Data Security, Inc., Redwood City, CA.

[RSA1]RSA Laboratories, “PKCS #1: RSA Encryption Standard. Version 1.5”, November 1993.

[RSA2]RSA Laboratories, “Some Examples of the PKCS Standards,” RSA Data Security, Inc., Redwood City, CA, November 1, 1993.

[RSA3]RSA Laboratories, “PKCS #1 v2.0: RSA Cryptography Standard”, October

3. Definitions

3.1 Base Station (BS): A generalized equipment set providing connectivity, management, and control of the CPE.

3.2 Burst Profile: Set of parameters that describe the upstream transmission properties that are associated with an IUC. Each profile contains parameters such as modulation type, preamble length, guard times, etc.

3.3 Connection: A unidirectional mapping between equivalent BS and CPE peers. Connections are identified by a CID. All traffic is carried on a connection.

3.4 Connection Identifier (CID): A unidirectional, MAC-layer address that identifies a connection to equivalent peers in the CPE and BS MAC. A CID maps to a SFID, which defines the QoS parameters to the Service Flow associated with that connection. Security associations also exist be keying material and CIDs.

3.5 Customer Premises Equipment (CPE): A generalized equipment set providing connectivity between subscriber equipment and a BS.

3.6 Downlink: A flow of information that exists in the downstream.

3.7 Downstream: The direction from a BS to the CPE.

3.8 Frame: A frame is a fixed duration of time, which contains both transmit and receive intervals.

3.9 Information Element (IE): A component of the UL-MAP that defines the length and address assignment associated with an IUC. Taken as a whole, each IE represents a type of upstream transmission. Mulitple IEs may exist in the UL-MAP.

3.10 Interval Usage Code (IUC): Defines the type of usage of an Information Element. IUCs are defined for bandwidth requests, data grants, etc.

3.11 Grant Per Connection (GPC): A bandwidth allocation method in which grants are aggregated for all connections and are allocated to the CPE terminal as that aggregate. Note that bandwidth requests are always made for a connection.

3.12 Grant Per Terminal (GPT): A bandwidth allocation method in which grants are allocated to a connections within a CPE. Note that bandwidth requests are always made for a connection.

3.13 Mini-slot: A unit of bandwidth allocation equivalent to N PS, where $N = 2^m$ (m = 0,...7).

3.14 Multicast Group: Agroup of zero or more CPEs or connections that are assigned a mulitcast address for the purposes of polling.

3.15 Physical-Slot (PS): A unit of granularity equal to 4 modulation symbols. Each PS represents 8, 16, or 24 bits (using QAM-4, QAM-16, or QAM-64 modulation, respectively).

3.16 Privacy Key Management Protocol (PKM): A client/server model between the BS and CPE that is used to secure distribution of keying material.

3.17 Security Association (SA): The set of security information a BS and one or more of its client CPE share in order to support secure communications across the BWA network.

3.18 Service Flow: A Service Flow is a unidirectional flow of PDUs on a connection that is provided a particular Quality of Service.

3.19 Service Flow Class: A grouping of Service Flow properties to allow higher layer entities and external applications to request Service Flows with desired QoS parameters in a globally consistent way.

3.20 Service Flow Name: An ASCII string that is used to reference a set of QoS parameters that (partially) define a Service Flow.

3.21 Uplink: A flow of information that exists in the upstream.

3.22 Uplink MAP (UL-MAP): A set of information that defines the entire access for a scheduling interval.

3.23 Upstream: The direction from a CPE to the BS.

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

5. MAC Service Definition

<TBD>.

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 unsolicitied 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 throught 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	Request IE Usage 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.

6.2 Message Formats

MAC Protocol Data Units (PDU) shall be of the form illustrated in Figure 1. Each PDU is preceeded by a fixed-length generic MAC header. The PDU may contain optional payload information from a convergence sub-layer. The payload information can vary in length, so that a MAC PDU will represent a variable number of bytes. The payload information is divided into a convergence sub-layer header and data portions. The definition and use of these message components is defined outside of the scope of the core MAC protocol. This allows the MAC to tunnel various higher layer traffic types without knowledge of the formats or bit patterns of those messages.

Messages are always transmitted in the order: Most-Significant-Byte first with the Most-Significant-Bit first in each byte.

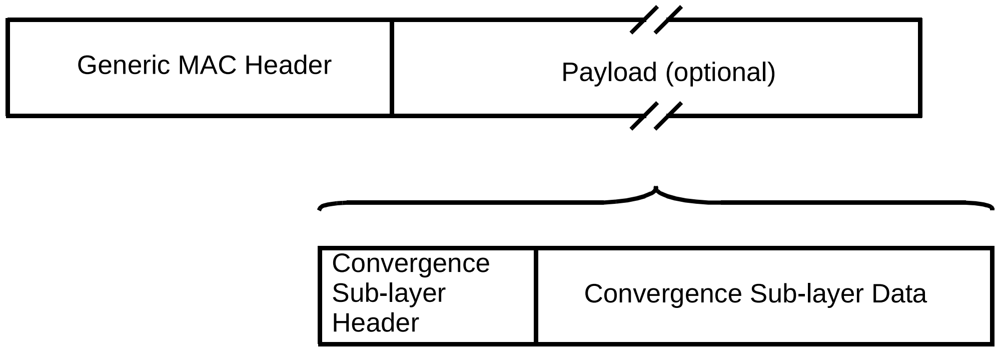


Figure 1—MAC PDU Formats

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 3 shall be used.

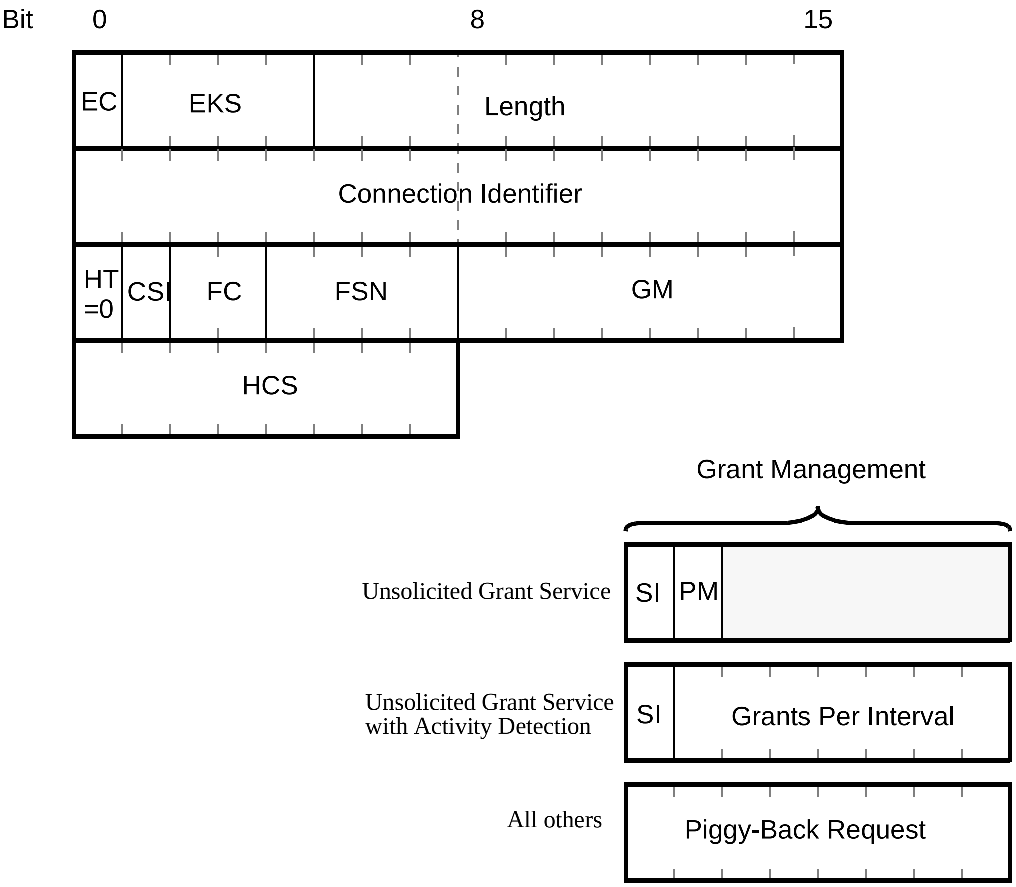


Figure 2—Generic MAC Header Format (Uplink)

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

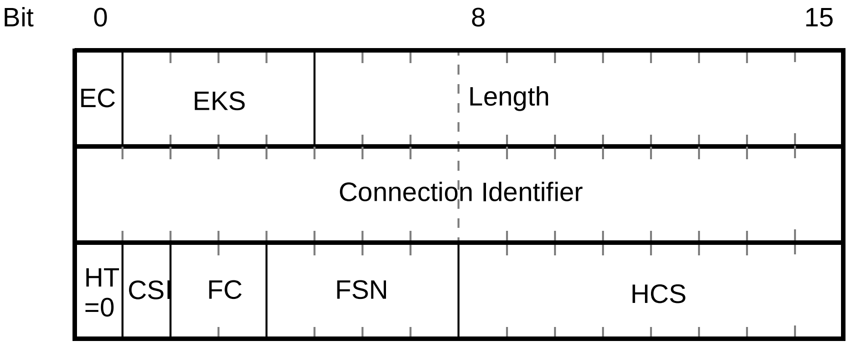


Figure 3—Generic MAC Header Format (Downlink)

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 4.

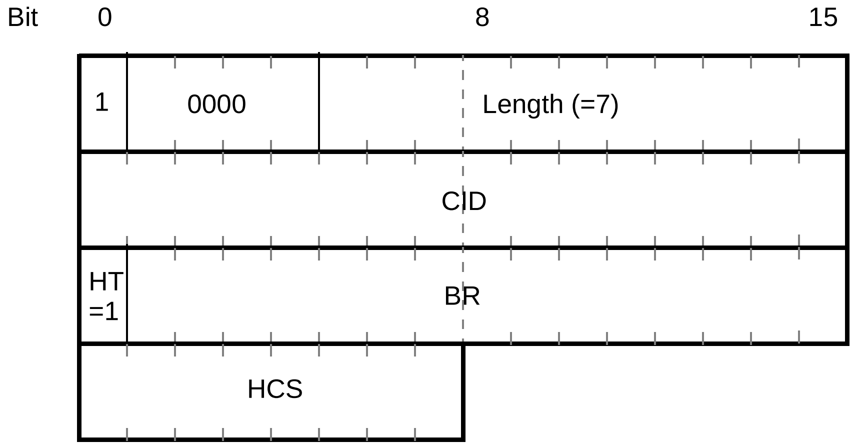


Figure 4—Bandwidth Request Header Format

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 0xFX. This prevents false detection on the stuff byte used in the Transmission Convergence Sublayer.

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 5 illustrates this concept for an uplink burst transmission. Since each PDU is identifiied 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 tranmission.

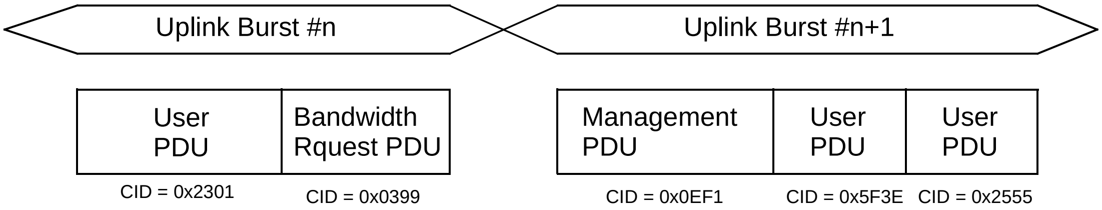


Figure 5—MAC PDU Concatention

6.2.1 Convergence Sub-layer PDU Formats

The format of the convergence sub-layer PDU shall be as shown in Figure 6. A Convergence Sub-layer PDU may have a zero length payload.

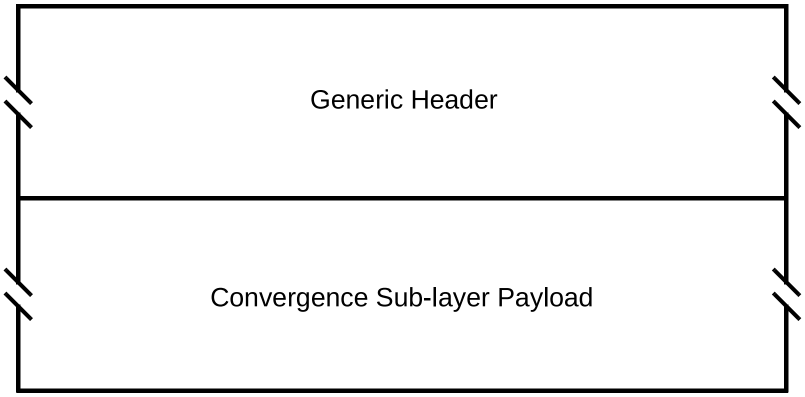


Figure 6—Convergence Sub-layer PDU Format

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 7. The encoding of the Message type field is given in Table 3.

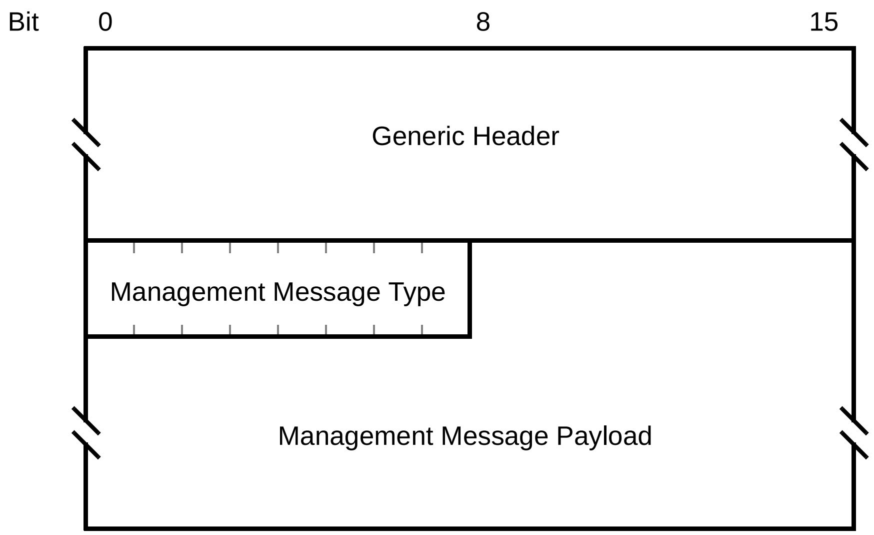


Figure 7—MAC Management Message Format

Table 3—MAC Management Messages

Type	Message Name	Message Description
1	PCD	Physical Channel Descriptor
2	DL-MAP	Downlink Access Definition
3	UL-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.

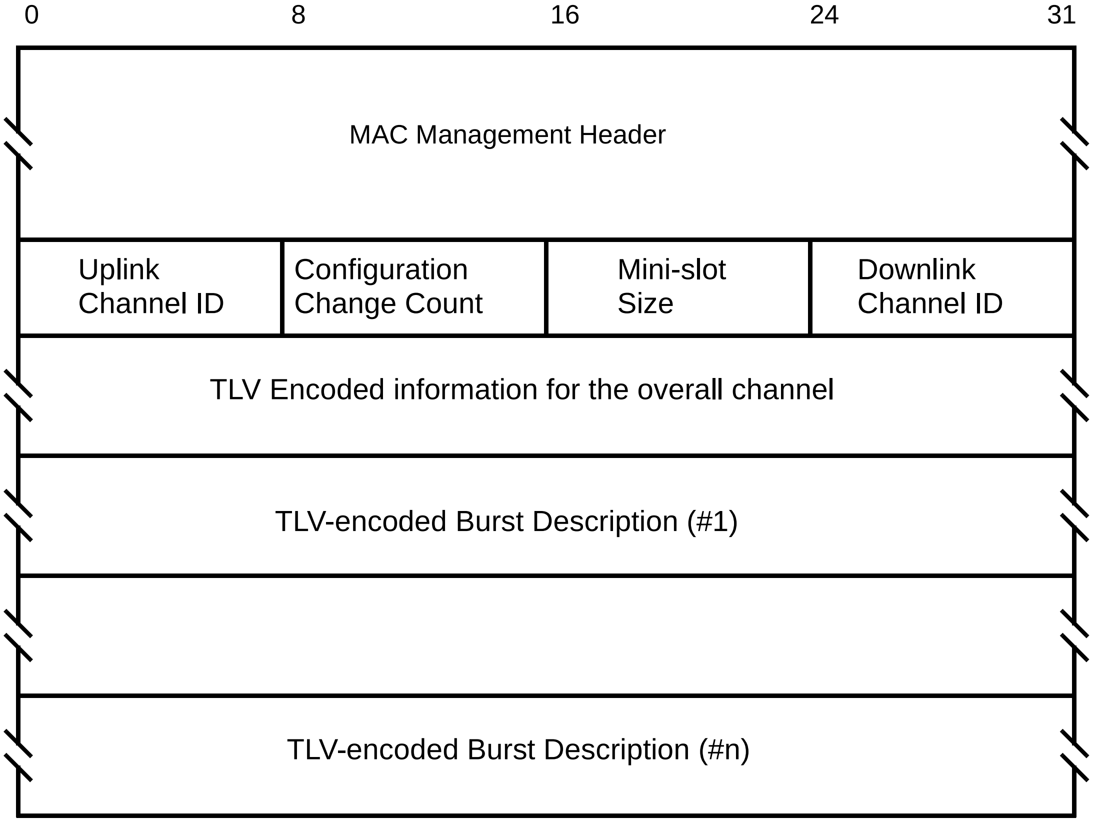

0
8
16
24
31
MAC Management Header
Uplink Channel ID
Configuration Change Count
Mini-slot Size
Downlink Channel ID
TLV Encoded information for the overall channel
TLV-encoded Burst Description (#1)
TLV-encoded Burst Description (#n)

Figure 8—Physical Channel Descriptor (PCD) Message Format

A BS shall generate PCDs in the format shown in Figure 8, 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 UL-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,...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 preceed 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	Preamble superstring. All burst-specific preamble values are chosen as bit-substrings of this string. 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.
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 DL-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 DL-MAP message is {0, 1} (TDD).
Shortened Downlink CPE Preamble Length	7	1	TBD by the PHY Group.
BS Transmit Power	8	1	Signed in units of 1dB
MAC Version	9	1	Version number of the MAC supported on this channel.

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 UL-MAP Message. illustrates the format of each Burst Descruption TLV. Each TLV is encoded with a Type of 1, an eight bit length, and a four bit IUC.

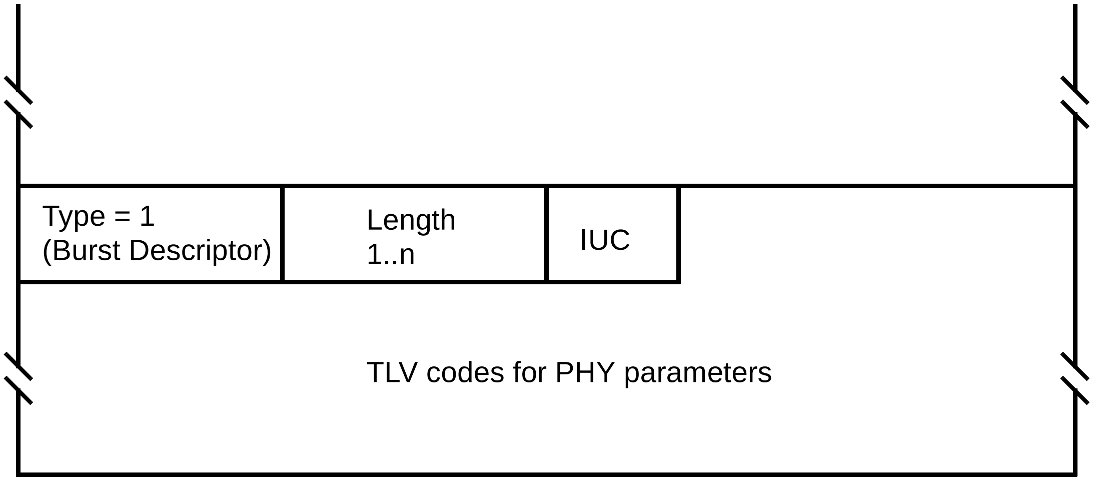


Figure 9—Top-Level Encoding for a Burst Descriptor

A Burst Descriptor shall be included for each Interval Usage Code that is to be used in the UL-MAP. The Interval Usage Code shall be one of the values from Table 6.

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

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 Table 4). 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 bytes 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 shall be present and greater than zero.
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 (DL-MAP) Message

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

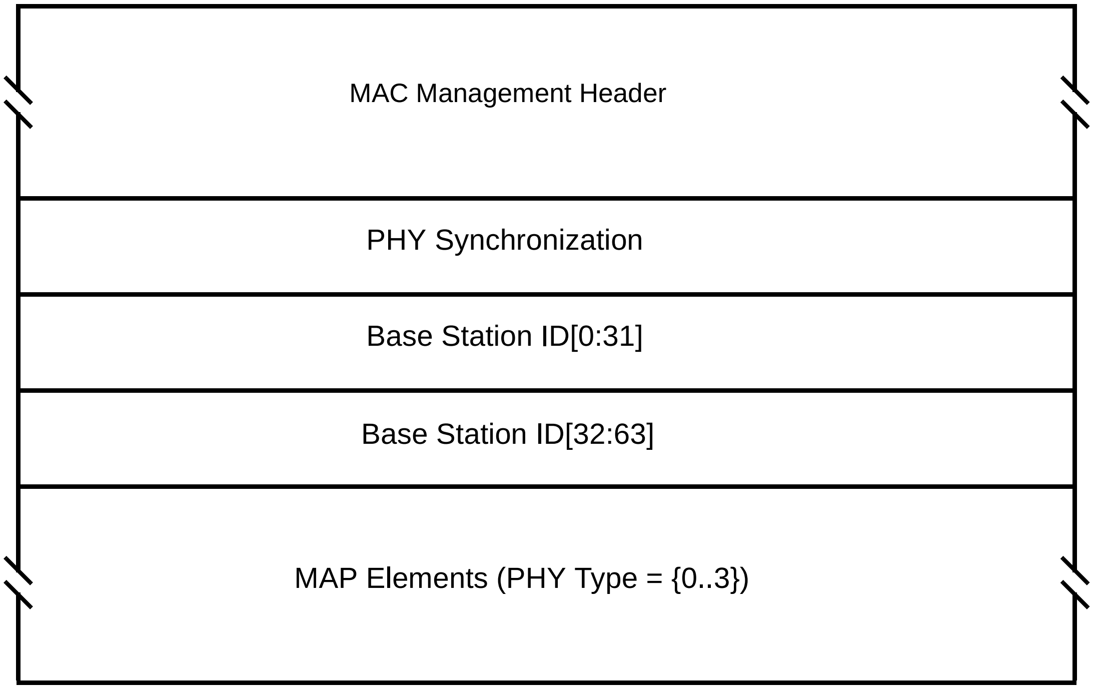


Figure 10—Downlink MAP Message Format (PHY Type = 4)

A BS shall generate DL-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 = TDD
> 1 = FDD/TDM (Burst Downlink PHY)
> 3 = FDD/TDMA
> 5 = FDD/TDM (Continuous Downlink PHY)
>
> The remaining 29 bits are encoded as shown in Figure 11 for PHY Type = {0..2} or Figure 12 for PHY Type = 3. 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 DL-MAP message are also based upon the PHY field. For PHY Type = 3, no additional information follows the Base Station ID field. For PHY Type = {0, 1}, a set of mapping information sorted by modulation type is defined as in Figure 13. For PHY Type = 2, a set of mapping information sorted by Connection ID is defined as in Figure 14.

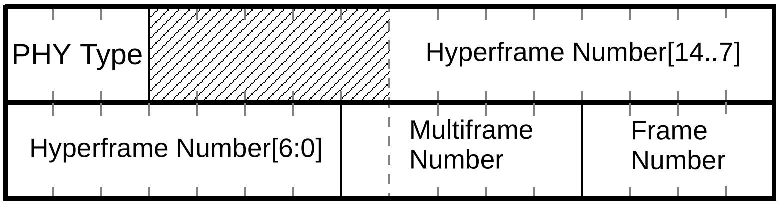


Figure 11—PHY Synchronization Field (PHY Type = {0..3})

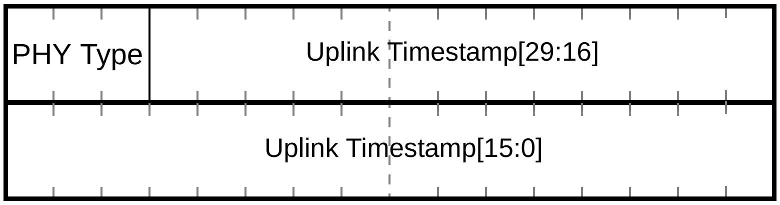


Figure 12—PHY Synchronization Field (PHY Type = 1)

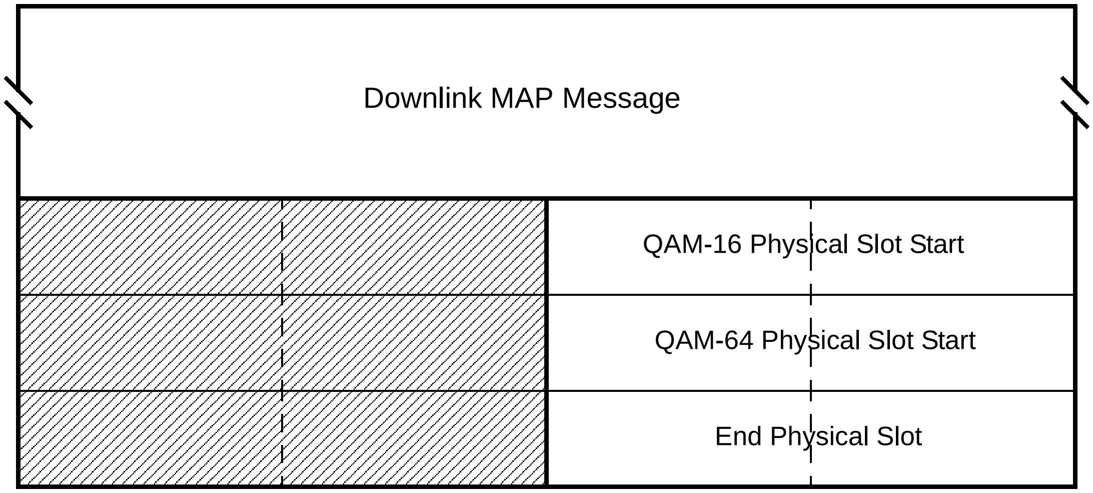


Figure 13—Downlink TDM MAP Message Element Format

The CID entry in the TDMA version of the DL-MAP message defines the allocation of bandwidth for that connection. For a CPE operating in GPC mode, the CID shall be the Transport CID. For a CPE operating in GPT mode, the CID shall be the Basic CID.

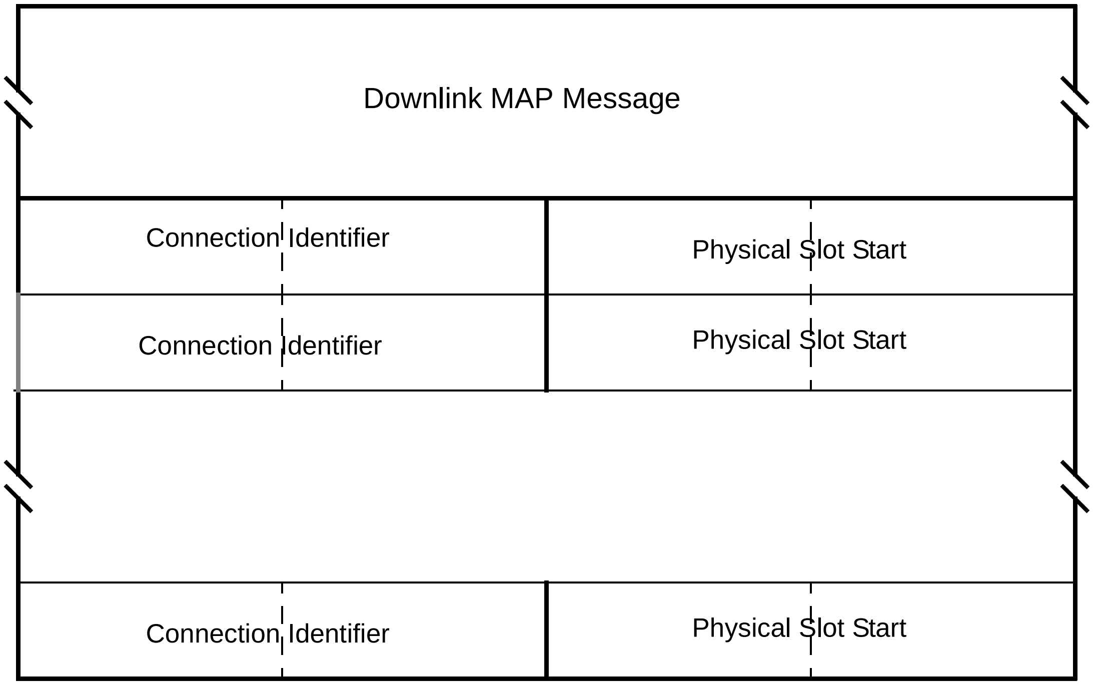


Figure 14—Downlink TDMA MAP Message Element Format

6.2.4 Uplink MAP (UL-MAP) Message

The Uplink MAP (UL-MAP) message allocates access to the upstream channel. The UL-MAP message shall be as shown in .Figure 16

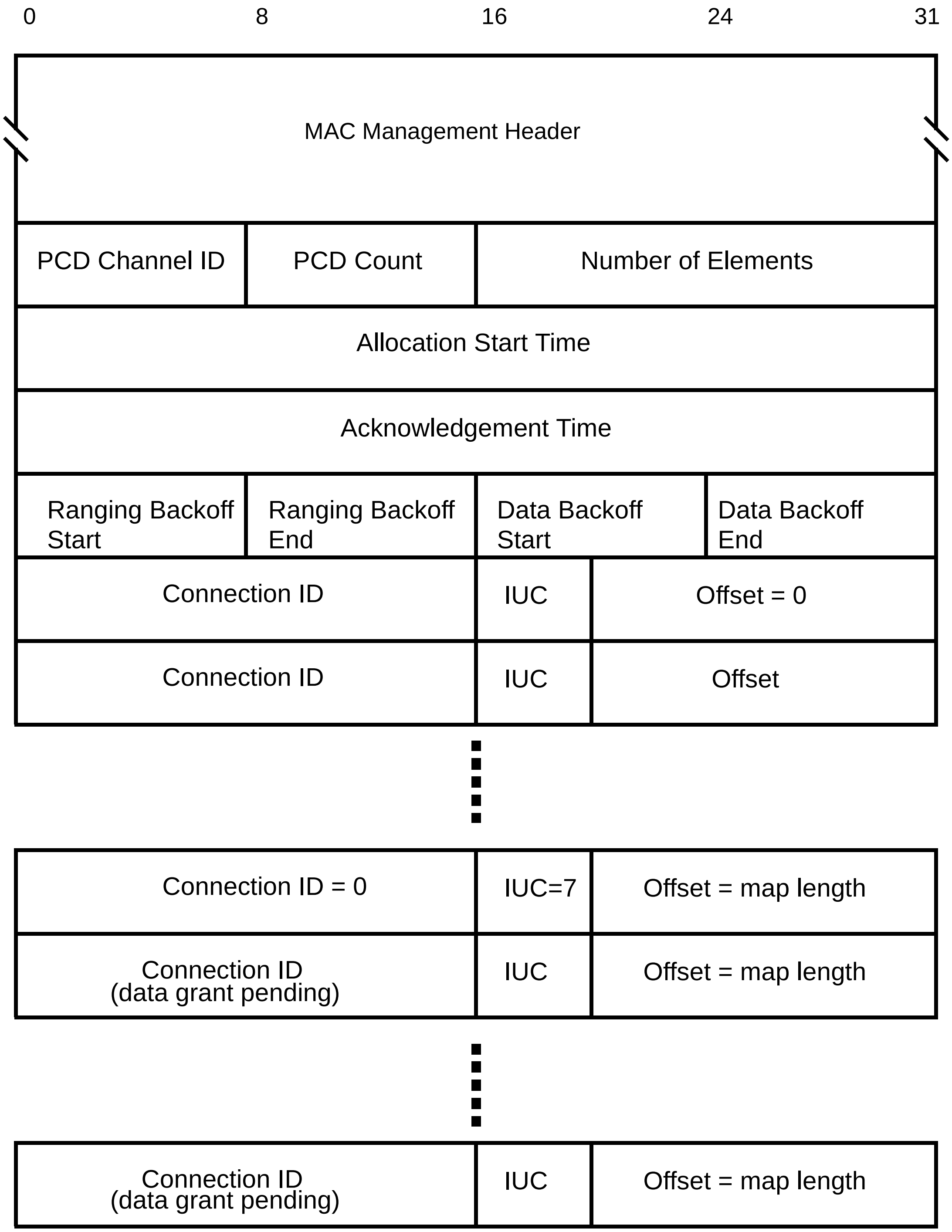


Figure 15—Uplink MAP Message Format

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 UL-MAP in units of mini-slots. The start time is relative to the start of a frame in which UL-MAP message is transmitted (PHY Type = {0..2}) or from BS initialization (PHY Type = 3).

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 UL-MAP message is transmitted (PHY Type = {0..2}) or from BS initialization (PHY Type = 3).

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 UL-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 Identifer, 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.

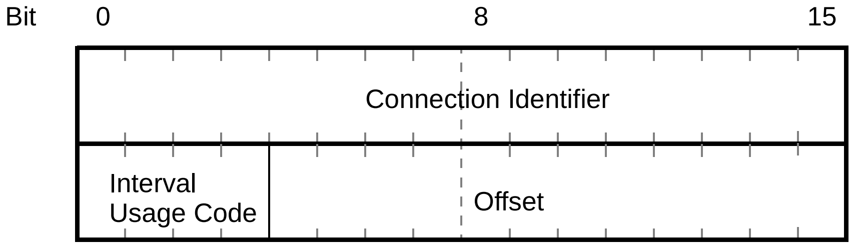


Figure 16—UL-MAP Information Element

Three pairs of data grant Information Elements are defined. This allows each pair to be assigned to a different burst profile pair, typically based upon modulation type. For example, the first pair would be assigned to use QPSK, the second pair would use 16-QAM, and the third would use 64-QAM. Within each pair, the short and long grant usage is distinguished by the maximum burst size. This allows short PDU transmissions for services that are tolerant of packet loss to use less FEC coding (relative to longer grants).

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)

Table 6—Uplink MAP Information Elements

IE Name	Interval Usage Code (IUC)	Connection ID	Mini-slot Offset
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.
Reserved	11-14	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 shall be transmitted by a CPE 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.

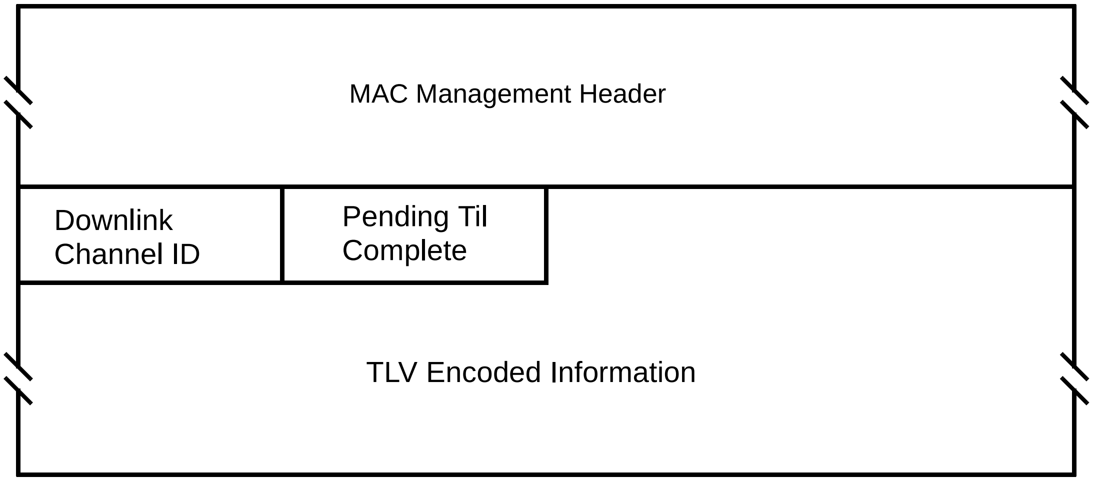


Figure 17—RNG-REQ Message Format

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

Parameters shall be as follows:

CID (from the MAC Management Header)

For RNG-REQ Messages transmitted in Initial Maintenance intervals:

a) Initialization CID if modem is attempting to join the network
b) Initialization CID if modem has not yet registered and is changing downlink (or both downlink and uplink) channels as directed by a downloaded parameter file
c) Temporary CID if modem has not yet registered and is changing uplink (not downlink) channels as directed by a downloaded parameter file
d) Registration CID (previously assigned in REG-RSP) if modem is registered and is changing uplink channels

For RNG-REQ Messages transmitted in Station Maintenance intervals:
Basic CID

Downlink Channel ID

The identifier of the downlink channel on which the BS received the PCD which described this uplink. This is an 8-bit field.

Pending Till Complete

If zero, then all previous Ranging Response attributes have been applied prior to transmittting 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.

CPE MAC Address (EUI-64 Bit)

A required parameter. The MAC address of the CPE.

6.2.5.1 RNG-REQ TLV Encodings

The type values used shall 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 shall 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
CPE MAC Address	2	8	CPE MAC Address in EUI-64 format
Reserved	3-255	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.

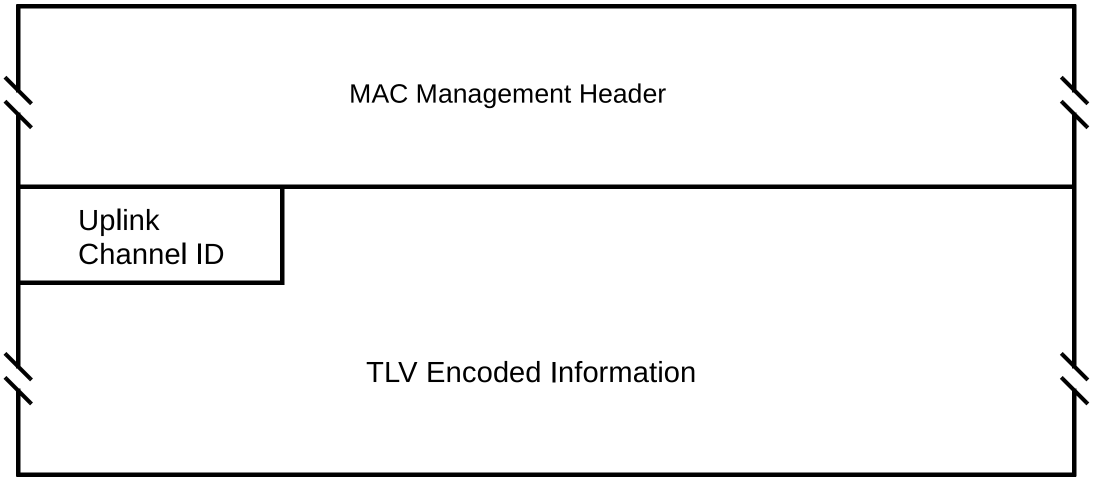


Figure 18—RNG-RSP Message Format

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

Uplink Channel ID

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

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.

P**ower 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.

Ranging Status

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

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 conjuction 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.

CID

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

Note that in all other cases, the CID is encoded in the MAC Management Header is not sent as a TLV.

CPE MAC Address (EUI-64 Bit)

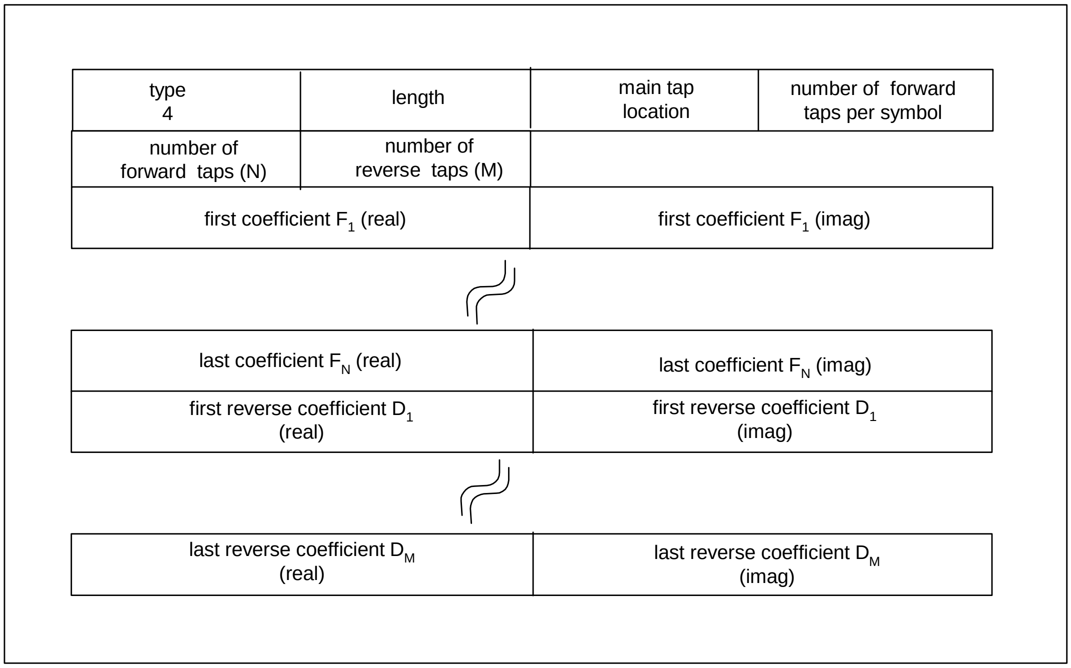
A required parameter. The MAC address of the CPE.

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

Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Timing Adjust	1	4	Tx timing offset adjustment (signed 32-bit, units of ¼ symbols)
Power Level Adjust	2	1	Tx Power offset adjustment (signed 8-bit, ¼-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 ¼ dB.
64-QAM Threshold	9	1	C/I+N for minimum 64-QAM operation in ¼5 dB.
Threshold Delta	10	1	Hysteresis delta for modulation threholds in ¼ dB.
Modulation Type	11	1	1 = QPSK, 2 = QPSK or 16-QAM, 3 = QPSK or 16/64-QAM
CPE MAC Address	12	8	CPE MAC Address in EUI-64 format
Reserved	13-255	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.

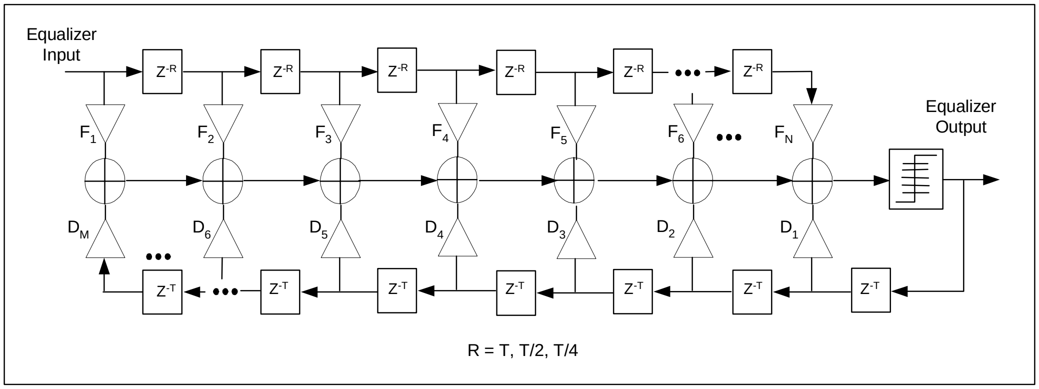


Figure 20—Generalized Equalizer Tap Location Definition

6.2.7 Registration Request (REG-REQ) Message

A Registration Request shall be transmitted by a CPE at initializatioollowing the CID shall be encoded in a type/length/value form. A CPE shall generate Registration Requests in the form shown in Figure 21

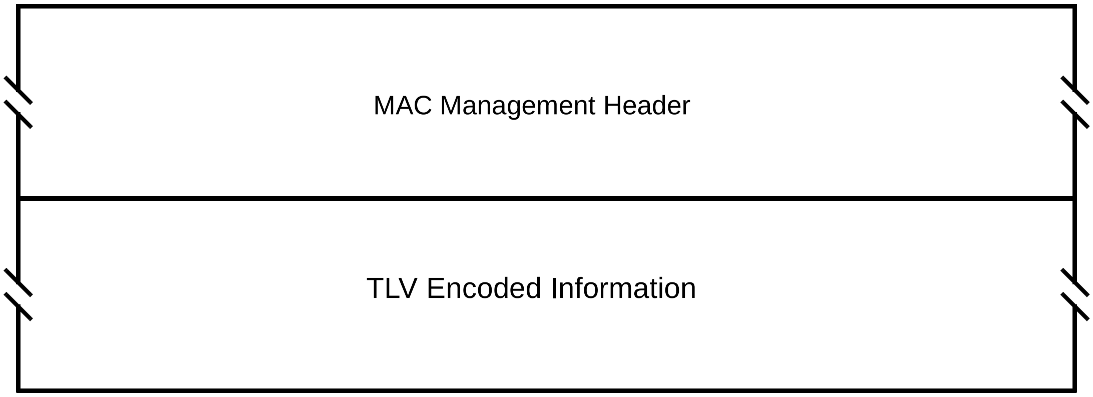


Figure 21—REG-REQ Message Format

CID (from the MAC Management Header)

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 shall 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 shall be transmitted by BS in response to received REG-REQ.

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

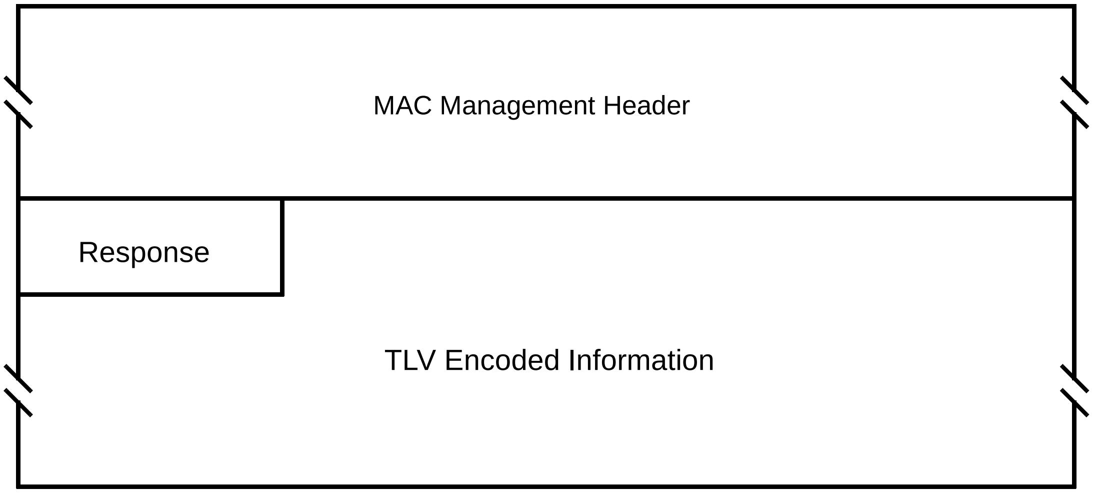


Figure 22—REG-RSP Message Format

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

CID (in the MAC Management Header) from Corresponding REG-REQ

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

Response

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

Note: 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 shall 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 shall be expanded into the full set of TLVs defining the Service Flow. Every uplink Service Flow that was admitted/activated[1] shall have a Connection 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 Service Flow ID.

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

Service Flow Error Set

A Service Flow Error Set and identifying Service Flow Reference shall be included for every failed Service Flow in the corresponding REG-REQ. Every Service Flow Error Set shall 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 shall not include any additional QoS Parameters except the Service Flow Identifier.

All other parameters are coded as TLV tuples:

CID #2

CID for secondary management purposes

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

[1] The ActiveQoSParamSet or AdmittedQoSParamSet is non-null.

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

6.2.8.1 Encodings

The type values used shall 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 shall 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 shall 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 it REG-RSP. The format of a REG-ACK shall be as shown in Figure 23.

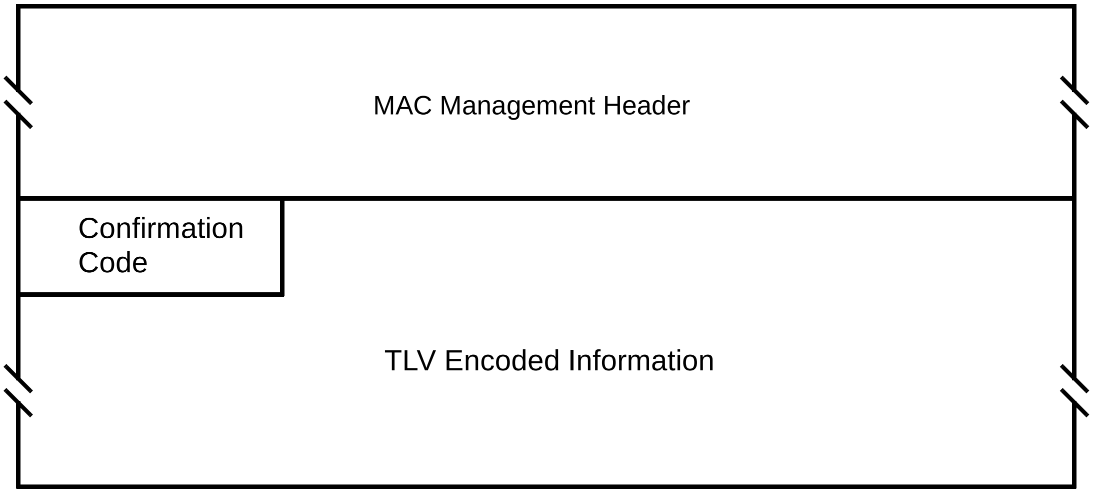


Figure 23—REG-ACK Message Format

The parameter shall be as follows:

CID (in the MAC Management Header) 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 shall forward all provisioned Service Flows to the BS. Since any of these provisioned items can fail, the REG-ACK shall 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 shall be included for every failed QoS Parameter of every failed Service Flow in the corresponding REG-RSP Message. This parameter shall 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.

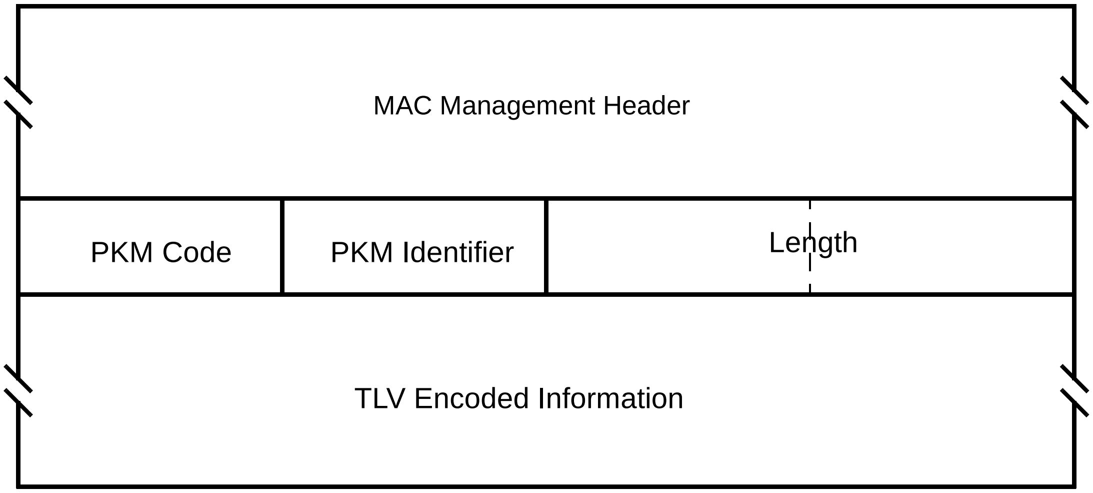


Figure 24—PKM-REQ Message Format

Parameters shall be as follows:

PKM Code

The Code field is one octect and identifies the type of PKM packet. When a packet is recieved with an invalid Code field, it shall be silently discarded. The Code values are defined in Section 7.3.2.1.

PKM Identifier

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

The CPE shall 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 shall 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 BS's PKM response Message shall match the Identifier field of the PKM Request Message the BS is responding to. The Identifier field in Traffic Encryption Key (TEK) Invalid Messages, which are not sent in response to BPKM requests, shall be set to zero. The Identifier field in unsolicited Authorization Invalid Messages shall 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 Security Association (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 shall 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.

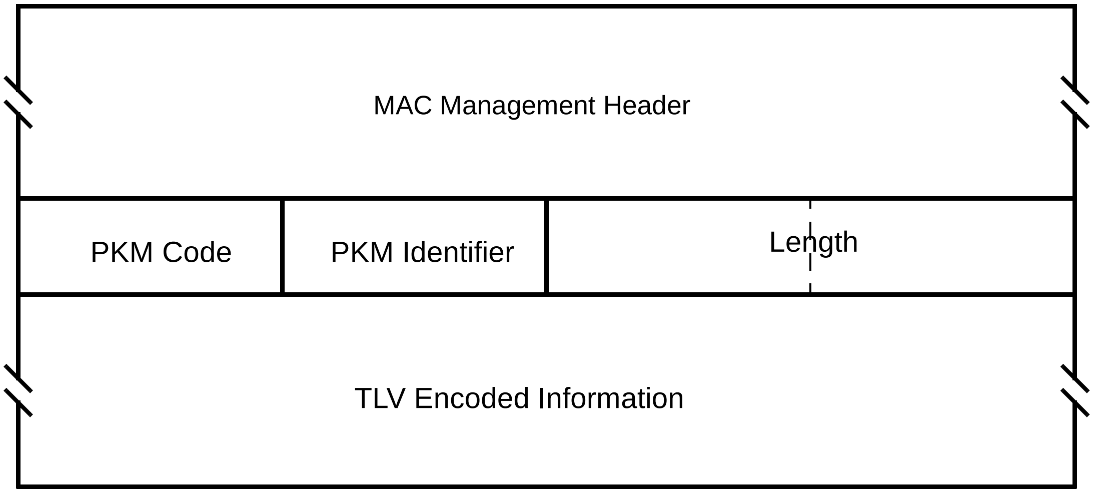


Figure 25—PKM-RSP Message Format

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.

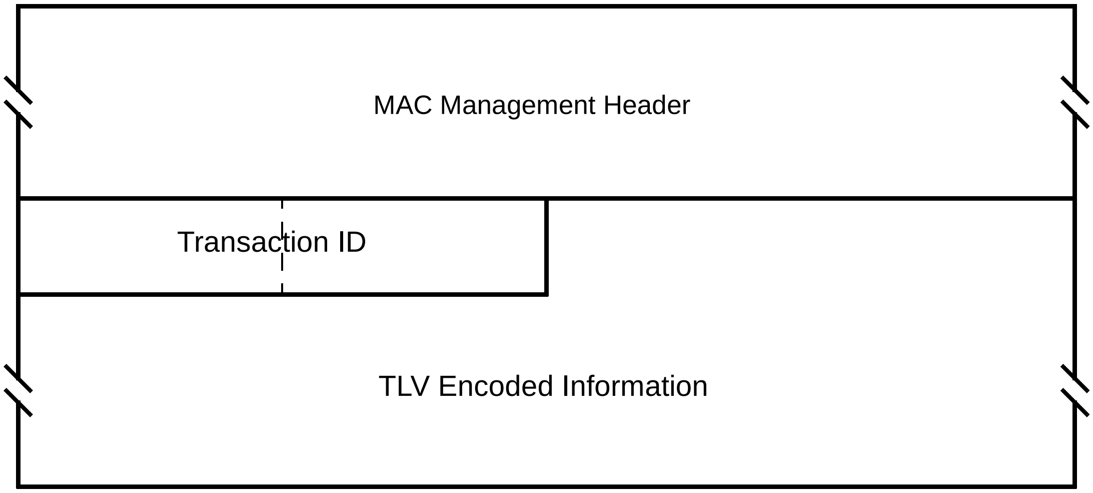


Figure 26—DSA-REQ Message Format

A CPE or BS shall 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 shall not contain parameters for more than one Service Flow in each direction, i.e., a DSA-REQ Message shall 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 shall contain:

Service Flow Parameters

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

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

HMAC-Digest

> The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12.4.1)

6.2.12.1 CPE-Initiated Dynamic Service Addition

Values of the Service Flow Reference are local to the DSA Message; each Service Flow within the DSA-Request shall 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 Section 6.12.5.3.4) 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 shall also include a Connection ID. Connection Identifiers are unique within the MAC domain.

BS-initiated DSA-Requests for named Service Classes shall 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 shall be as shown in Figure 27.

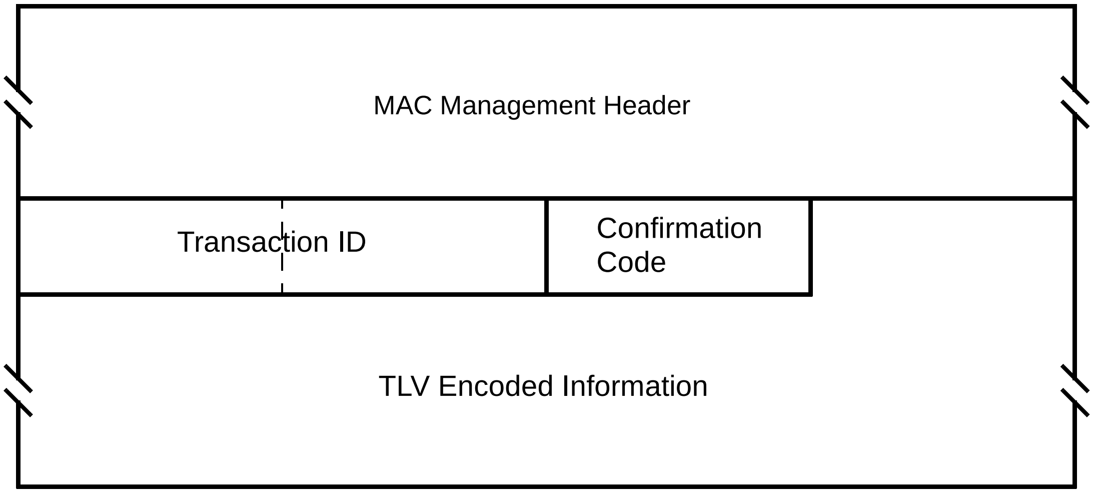


Figure 27—DSA-RSP Message Format

Parameters shall 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 shall 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 shall include:

Service Flow Error Set

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

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

HMAC-Digest

> The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12.4.1)

6.2.13.1 CPE-Initiated Dynamic Service Addition

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

If the corresponding DSA-Request uses the Service Class Name (refer to Section 6.12.5.3.4) to request service addition, a DSA-Response shall 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 shall 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 shall use the DSA-Request values as overrides for those of the Service Class.

If the transaction is unsuccessful, the BS shall 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 shall 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 shall be generated in response to a received DSA-RSP. The format of a DSA-ACK shall be as shown in Figure 28.

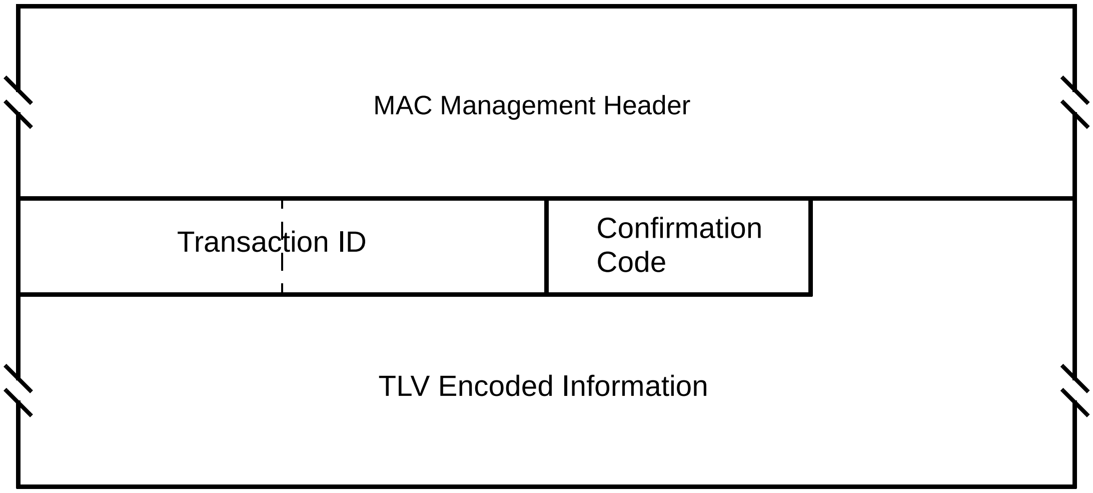


Figure 28—DSA-ACK Message Format

Parameters shall be as follows:

Transaction ID

Transaction ID from corresponding DSA-Response.

Confirmation Code

The appropriate Confirmation Code (refer to Section 6.12.7) for the entire corresponding DSA-Response.[2]

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 shall be included for every failed QoS Parameter of every failed Service Flow in the corresponding DSA-REQ Message. This parameter shall be omitted if the entire DSA-REQ is successful.

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

HMAC-Digest

[2] The confirmation code is necessary particularly when a Service Class Name (refer to Section 6.12.5.3.4) 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).

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12.4.1)

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.

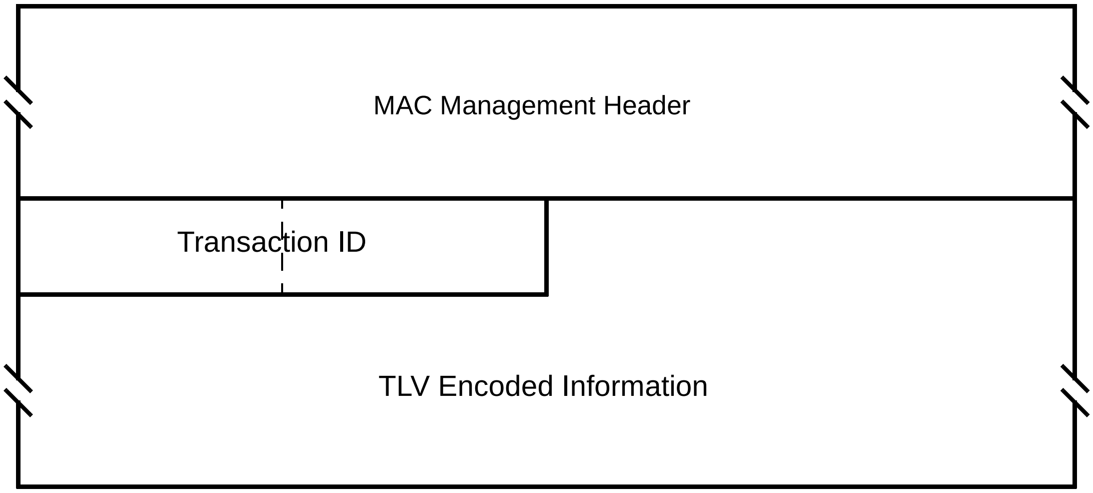


Figure 29—DSC-REQ Message Format

A CPE or BS shall generate DSC-REQ Messages in the form shown inFigure 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 shall not carry parameters for more than one Service Flow in each direction, i.e., a DSC-REQ Message shall 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 shall 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) shall be set to null. If included, the Service Flow Parameters shall contain a Service Flow Identifier.

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

HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12.4.1)

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

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

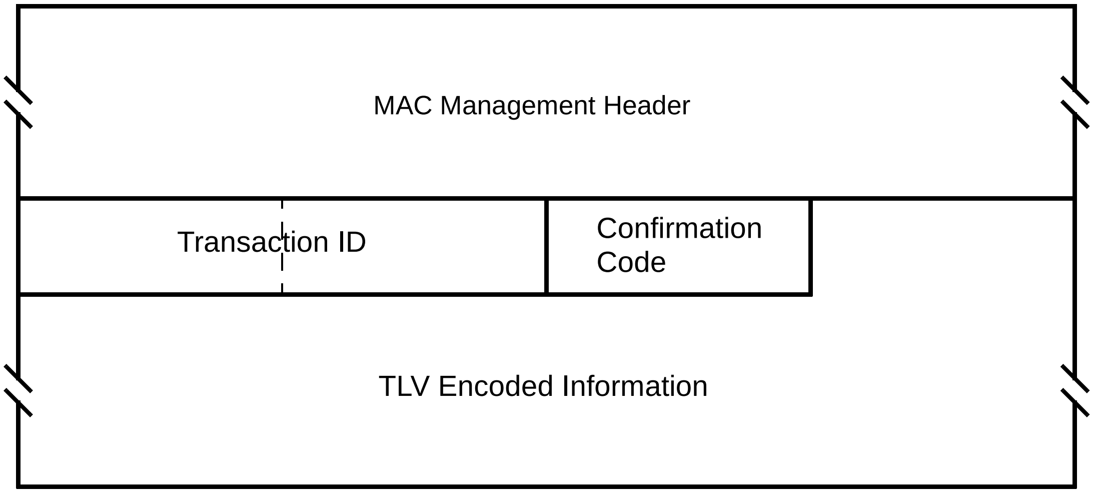


Figure 30—DSC-RSP Message Format

Parameters shall be as follows:

Transaction ID

Transaction ID from corresponding DSC-REQ

Confirmation Code

The appropriate Confirmation Code (refer to Section 6.12.7) 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 shall 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 shall include a CID. If a Service Flow Parameter set contained a Service Class Name and an Admitted QoS Parameter Set, the DSC-RSP shall 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 shall 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 shall contain the following:

Service Flow Error Set

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

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

HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list. (Refer to Section 6.12.4.1)

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

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

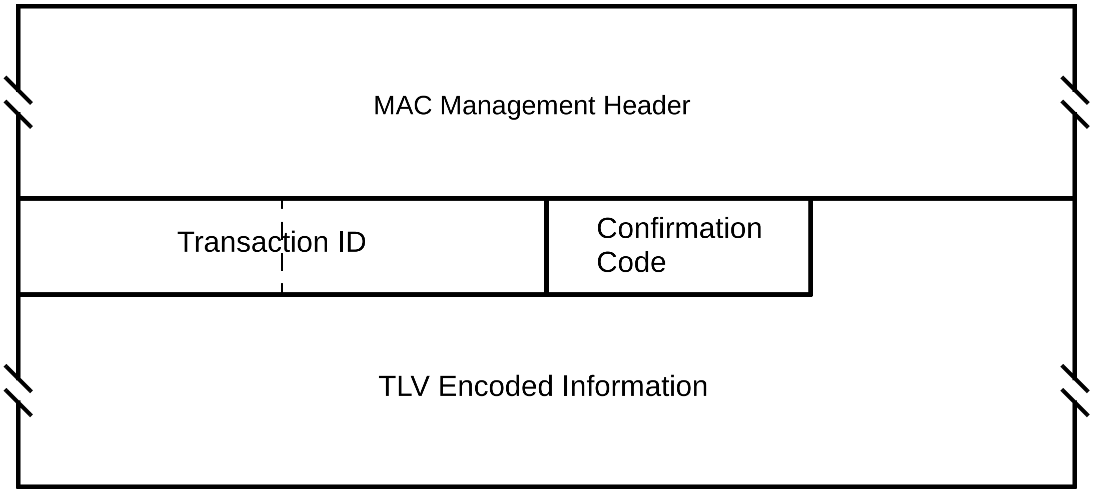


Figure 31—DSC-ACK Message Format

Parameters shall be as follows:

Transaction ID

Transaction ID from the corresponding DSC-REQ

Confirmation Code

The appropriate Confirmation Code (refer to Section 6.12.7) 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 shall be included for every failed QohS Parameter of each failed Service Flow in the corresponding DSC-RSP Message. This parameter shall be omitted if the entire DSC-RSP is successful.

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

HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message’s Attribute list. (Refer to Section 6.12.4.1)

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 shall be as shown in Figure 32.

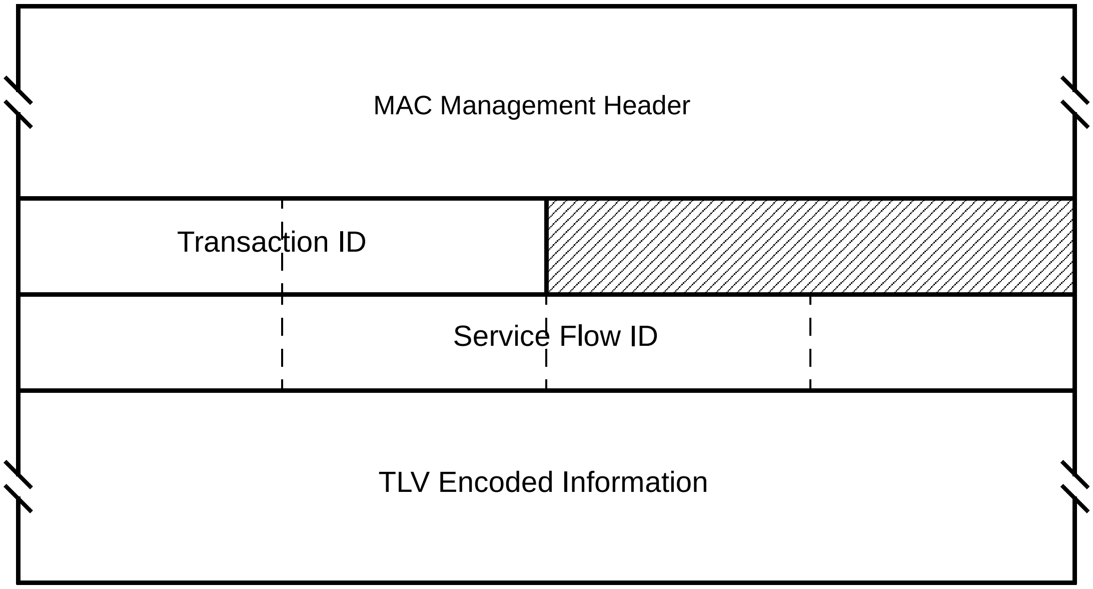


Figure 32—DSD-REQ Message Format

Parameters shall 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 shall include:

HMAC-Digest

The HMAC-Digest Attribute is a keyed Message digest (to authenticate the sender). The HMAC-Digest Attribute shall be the final Attribute in the Dynamic Service Message’s Attribute list. (Refer to Section 6.12.4.1)

6.2.19 Dynamic Service Deletion — Request (DSD-RSP) Message

A DSD-RSP shall be generated in response to a received DSD-REQ. The format of a DSD-RSP shall be as shown in Figure 33.

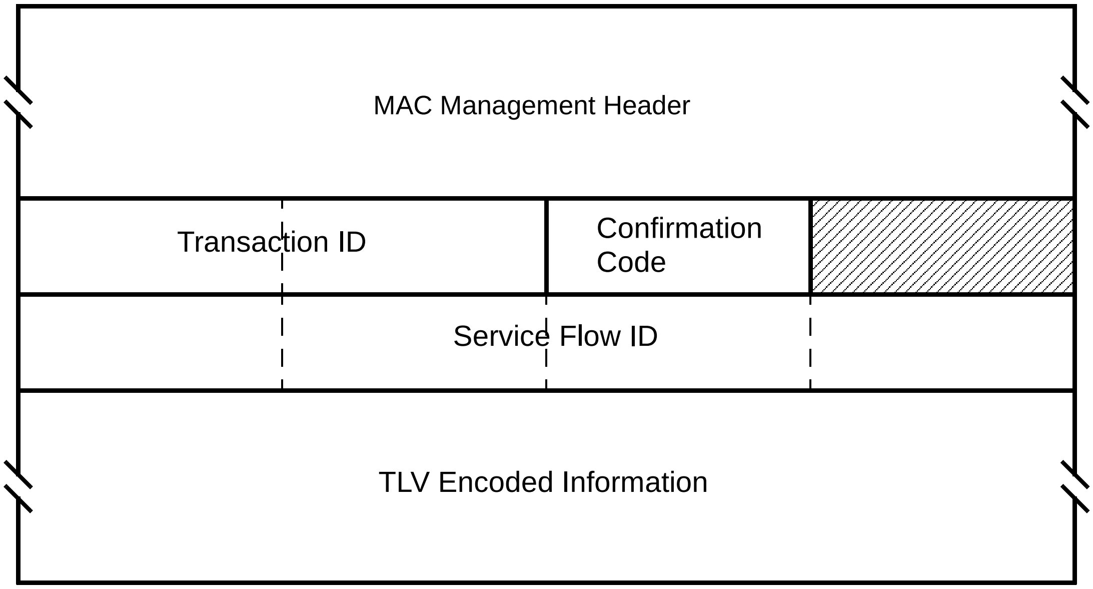


Figure 33—DSD-RSP Message Format

Parameters shall be as follows:

Service Flow Identifier

SFID from the DSD-REQ to which this acknowledgement refers.

Transaction ID

Transaction ID from the corresponding DSD-REQ.

Confirmation Code

The appropriate Confirmation Code (refer to Section 6.12.7) for the corresponding DSD-REQ.

6.2.20 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 34.

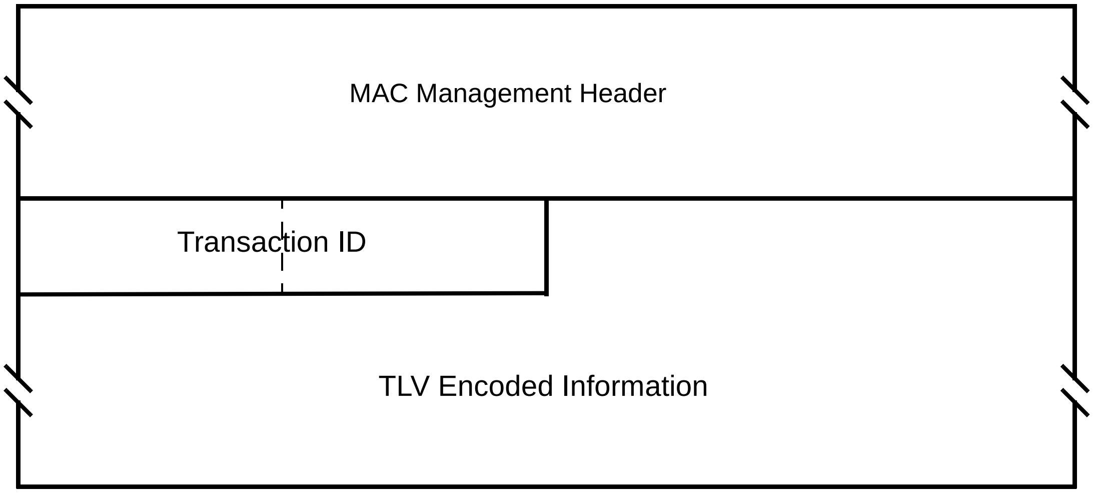


Figure 34—Multicast Polling Assignment Request (MCA-REQ) Message Format

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

6.2.20.1 MCA-REQ TLV Encodings

The type values used shall be those defined in Table 9. The type and length fields shall each be 1 octet in length.

Table 9—Multicast Assigment Request Message Encodings

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

6.2.21 Multicast Polling Assignment Response (MCA-RSP) Message

The Multicast Polling Assigment Response is sent by the CPE in response to a MCA-REQ. The message format shall be as shown in Figure 35.

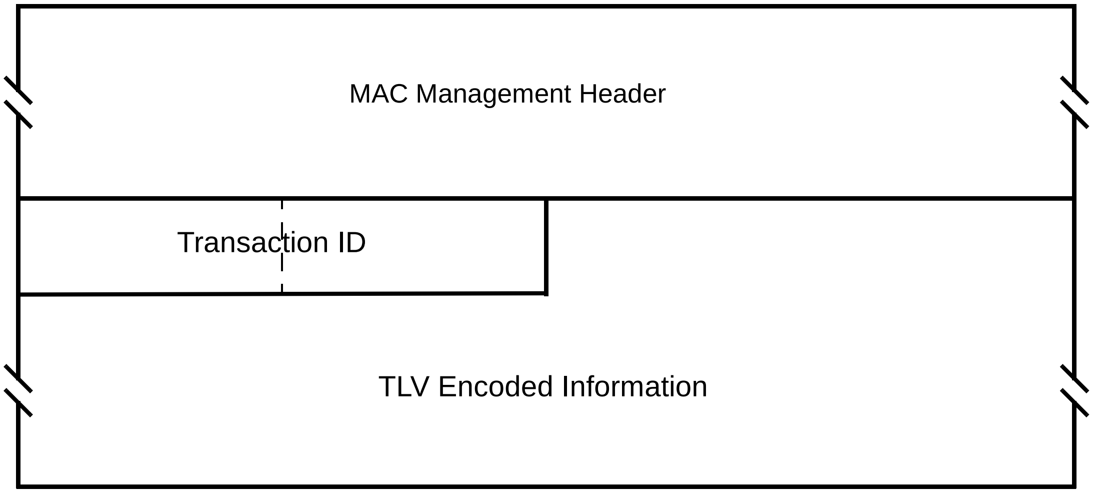


Figure 35—Multicast Polling Assignment Response (MCA-RSP) Message Format

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)

6.2.22 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 inactive 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. The message formant shall be as shown in Figure 36.

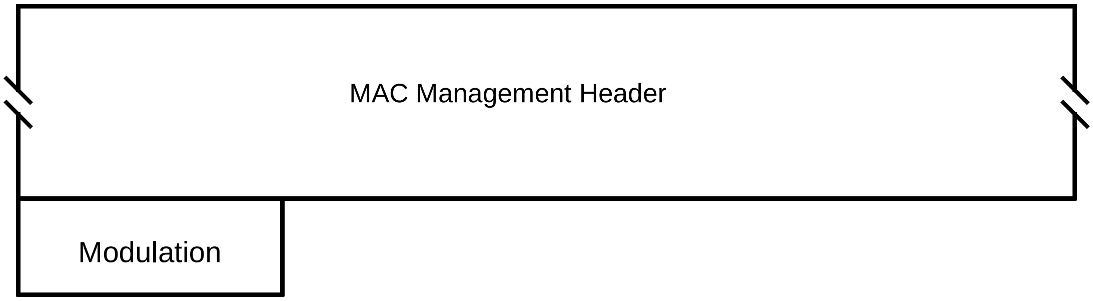


Figure 36—Downlink Modulation Change Request (DMC-REQ) Message Format

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 defines 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. For example, a 20 Mbaud modulation rate, there are 5000 PS within each 1 mS 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 37, 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.

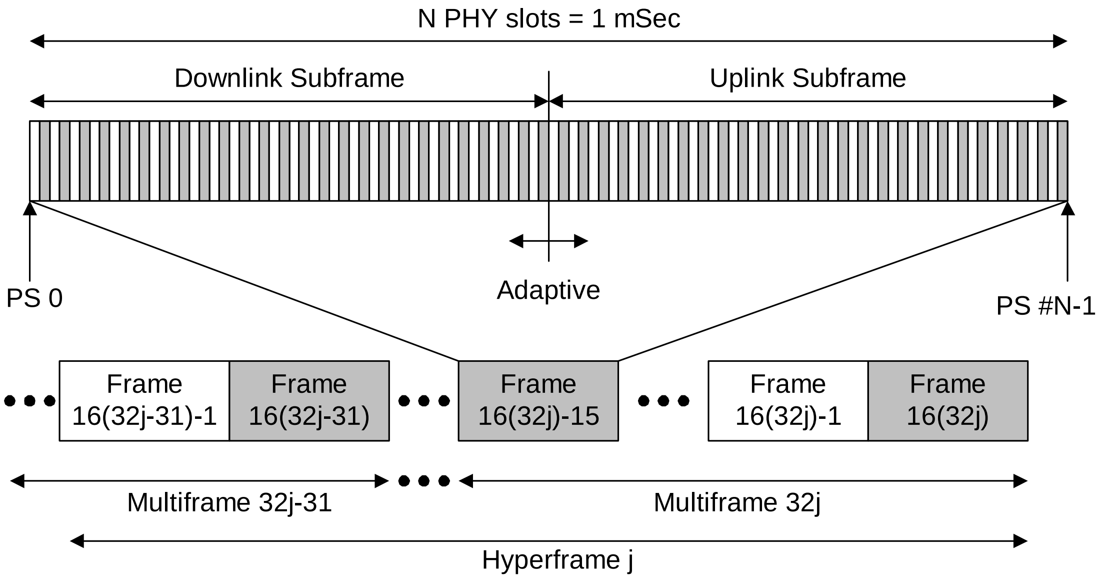


Figure 37—TDD and Multiframe Structure

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. 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 38 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 timed 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.

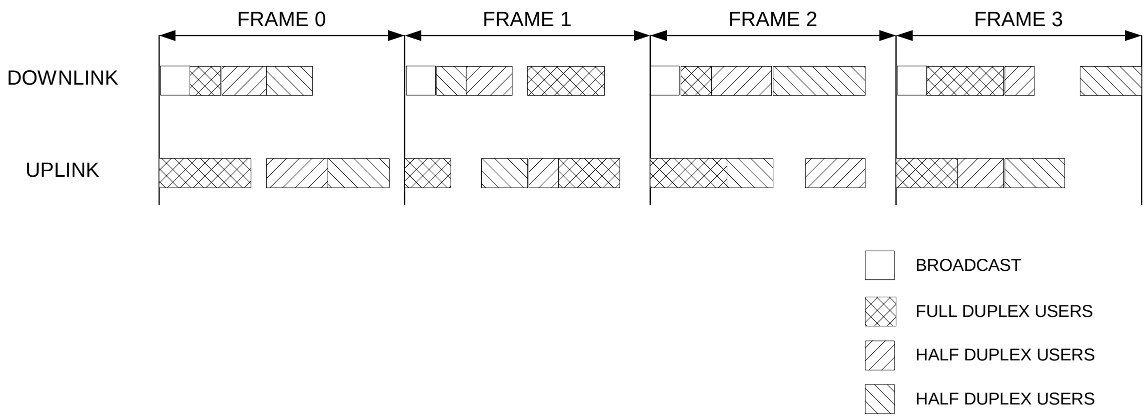


Figure 38—Burst Downstream FDD/FSDD Mapping

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 downstream and upstream MAP messages, which are used to syncronize the upstream burst transmissions with the downstream. The usage of the mini-slots 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 40. 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 39. 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 40. Note that ordering by modulation type is not required for TDMA downlinks and not required for any uplinks.

The Frame Control Header also may periodically contain a PHY Parameters as defined in the PCD.

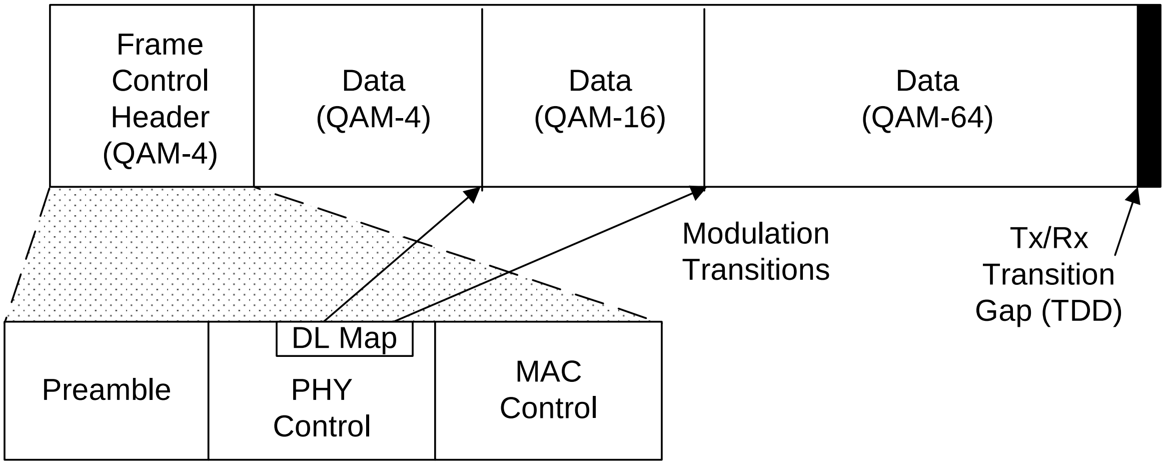


Figure 39—TDD and Burst FDD/TDM Downstream Subframe Structure

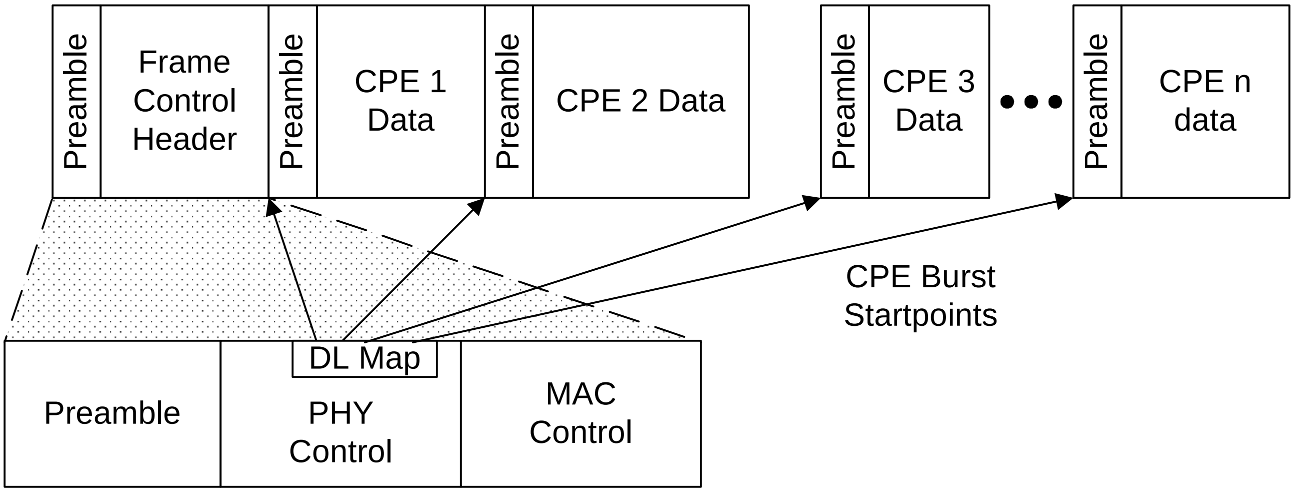


Figure 40—Burst FDD/TDMA Downstream Subframe Structure

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) DL-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 and the PHY mode is burst downstream, 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 41. There are three main classes of MAC/TC messages transmitted by the CPEs during the uplink frame:

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

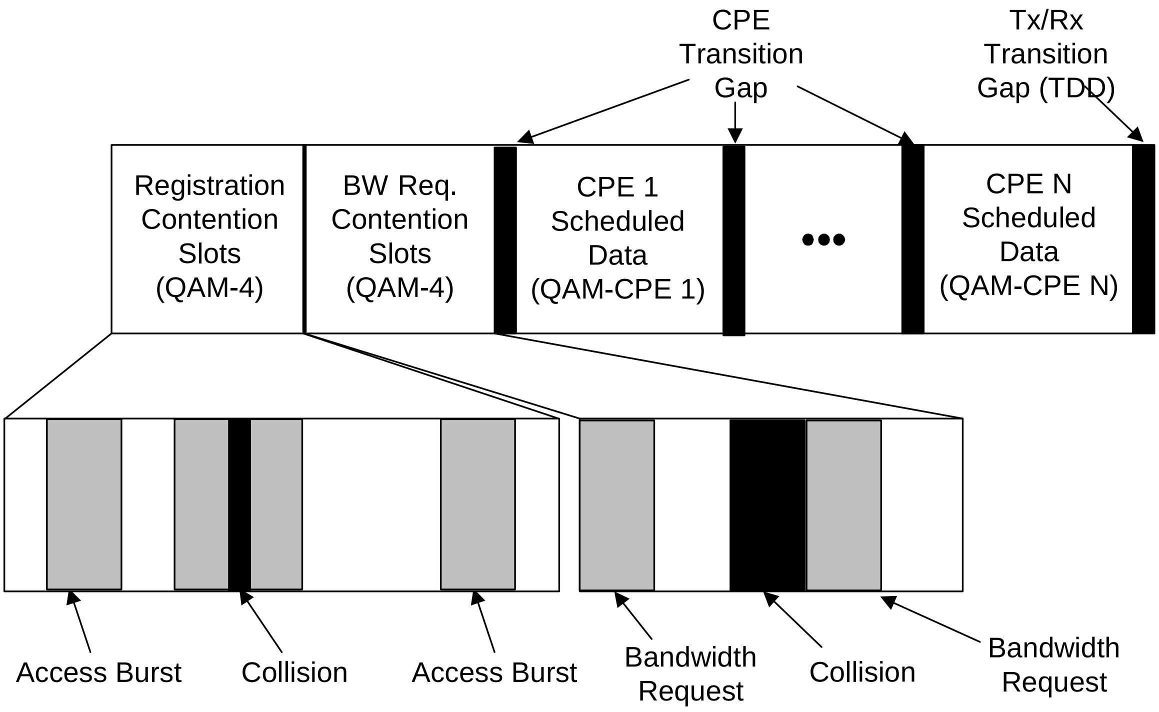

CPE Transition Gap
Tx/Rx Transition Gap (TDD)
Registration Contention Slots (QAM-4)
BW Req. Contention Slots (QAM-4)
CPE 1 Scheduled Data (QAM-CPE 1)
•••
CPE N Scheduled Data (QAM-CPE N)
Access Burst
Collision
Access Burst
Bandwidth Request
Collision
Bandwidth Request

Figure 41—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 allowing the BS to synchronize to the new CPE. The preamble and gap lengths are broadcast periodically in the PCD message 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 42). The timing of the upstream bursts are based upon a downstream syncronization message (DS-SYNC). The US-MAP messages are transmitted approximately 250 times a second, but this can vary to optimise the system’s operation.

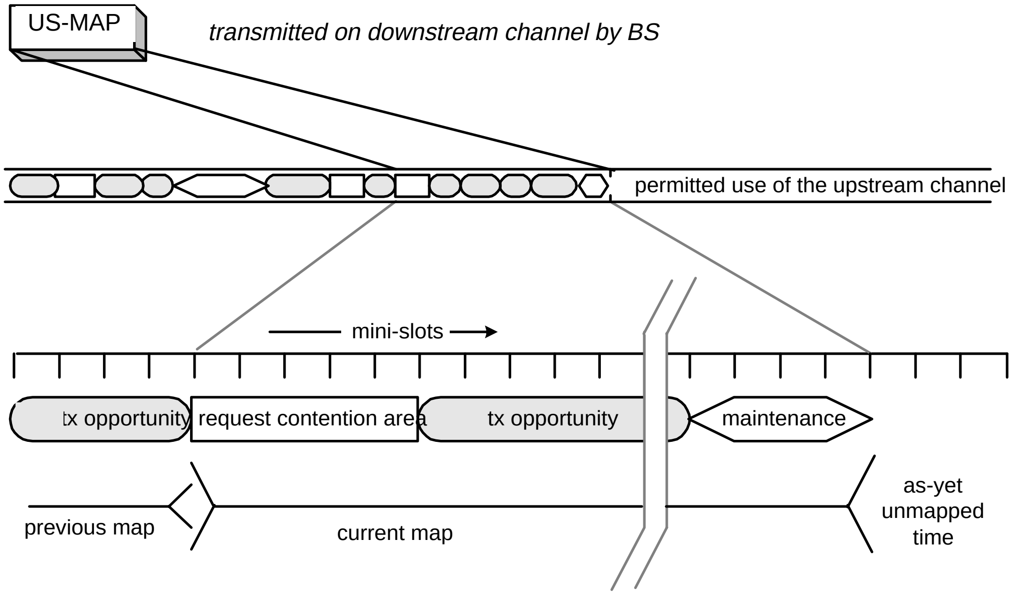


Figure 42—Continuous Downstream FDD Mapping

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 mini-slots using a series of Information Elements (IE), which define the useage of each upstream interval. The US-MAP defines the upstream usage in terms of the offset from the prevoius IE start (the lenfth) in numbers of mini-slots.

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 shall 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 ¼th of the modulation symbol period. This allows the CPE 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 CPE maintains its own Upstream Time Stamp so that it is syncronous with the BS Time stamp for the upstream channel that it is using. The CPE 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 CPE internal Time

Stamp so that it tracks the BS timing. The CPE 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 CPE 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 CPE it is reset using the current Timing Adjustment value as sent from the BS using the RNG-RSP message. Thus, the CPE 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.

In a framed mode of operation, the mini-slot represents the granularity of upstream allocation units. In the non-frame mode, the mini-slot definition is related to a timestamp generated by the BS. Figure 42 illustrates the mapping of the Upstream Time Stamp maintained in the BS to the BS Mini-slot Counter.

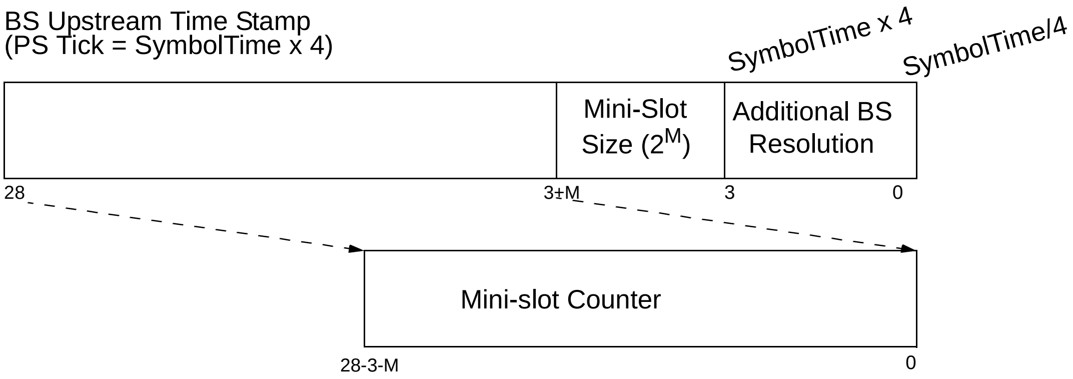


Figure 43—BS System and Mini-slot Clocks

The BS and CPE 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 shall 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*T*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 type of Connection ID used in the IE. If broadcast, this is an invitation for CPEs to contend for requests. 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 that is vendor dependent. PDUs transmitted in this interval shall use the Bandwidth Request Header Format (refer to Section 6.2).

A small number of Priority Request CIDs are defined in Section 6.1. These allow contention for Request IEs to be limited to service flows of a given Traffic Priority (Section 6.12.5.5.2).

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, shall be provided in some US-MAPs to allow new stations to perform initial ranging. Packets transmitted in this interval shall use the RNG-REQ MAC Management message format (refer to Section 6.2.5).

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 shall use the RNG-REQ MAC Management message format (see Section 6.2.5).

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 shall 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 shall 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 Expansion IE

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

6.3.6.3.6 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 shall be the total number that are desired by the CPE at the time of the request (excluding any physical layer overhead), subject to PCD[1] and administrative limits[2].

The CPE shall 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 shall continue to issue a Data Grant Pending in every MAP for as long as a request is unsatisfied.

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

[1] The CPE is limited by the Maximum Burst size for the Long Data Grant IUC in the PCD.

[2] The CPE is limited by the Maximum Concatenated Burst for the Service Flow

timing holds for both the TDD and FDD variants of the burst system. The TDD variant is shown in Figure 44. The FDD variant is shown in Figure 45.

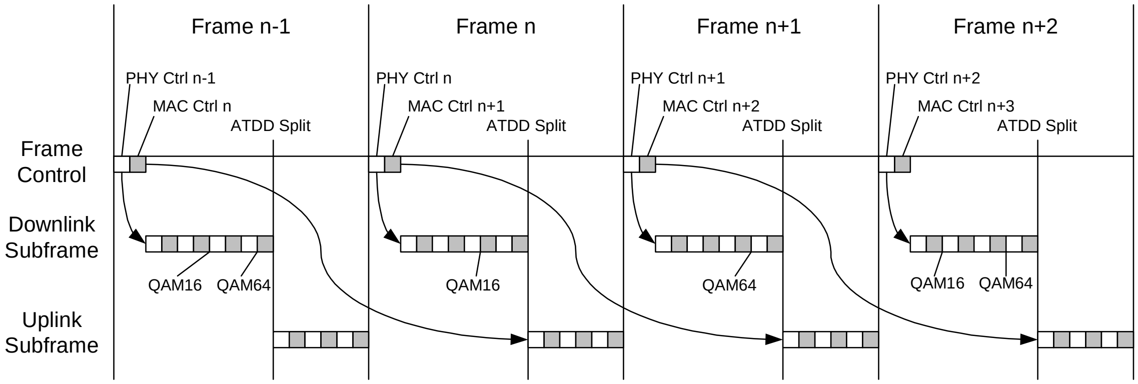


Figure 44—Time Relevance of PHY and MAC Control Information (TDD)

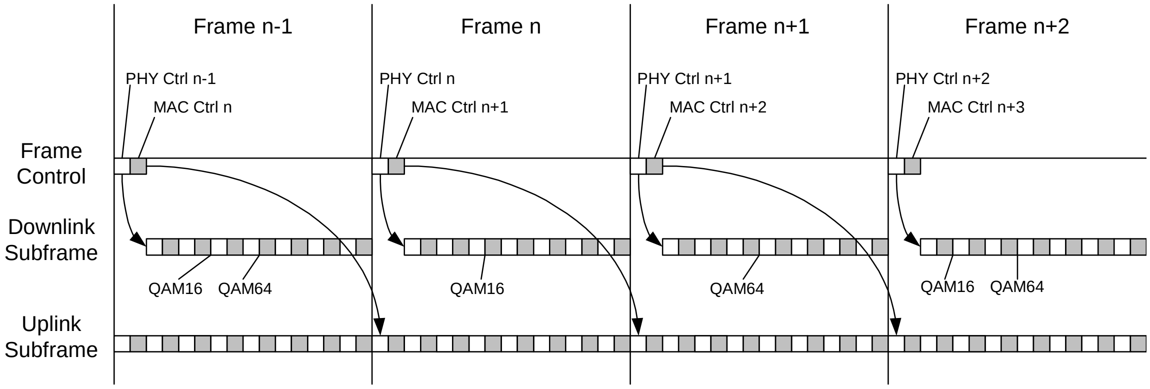


Figure 45—Time Relevance of PHY and MAC Control Information (FDD)

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 CPE.(see Figure 46)

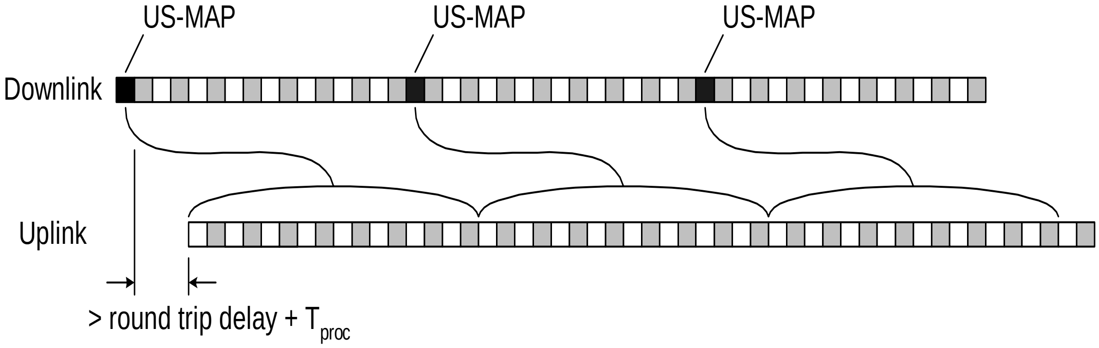


Figure 46—Time Relevance of Upstream MAP Information (Continuous FDD)

6.4 Contention Resolution

The BS controls assignments on the upstream channel through the US-MAP and determines which minislots 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 instructional tool. Since a CPE can have multiple upstream Service Flows (each with its own CID) it makes these decisions on a per service queue or per CID basis.

The mandatory method of contention resolution which shall 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 15; a value of 10 indicates a window between 0 and 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.[3]

The CPE shall randomly select a number within its back-off window. This random value indicates the number of contention transmit opportunities which the CPE shall defer before transmitting. A CPE shall only consider contention transmit opportunities for which this transmission would have been eligible. These are defined by either Request 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 15 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) in a subsequent MAP. Once received, the contention resolution is complete. The CPE determines that the contention transmission

[3] The MAP currently in effect is the MAP whose allocation start time has occurred but which includes IEs that have not occurred.

was lost when it finds a MAP without a Data Grant (Data Grant Pending) for it and with an Ack time more recent than the time of transmission. The CPE shall 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 shall 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 shall 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 CID, it shall 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.

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 PCD 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.

Transmit opportunities shall not overlap and the start time of the transmit opportunity shall align with either the start of the IE interval or at the end of the previous transmit opportunity.

6.5 Fragmentation

Fragmentation is the processby which a portion of a convergence sub-layer payload is divided into two or more MAC PDUs. This process is undertaken to allow efficient use of available bandwidth relative to the QoS requirements of a connections Service Flow.

Fragmentation may be initiated by a BS for a downlink connection. Fragmentation may be initiated by a CPE for an uplink connection. A connection may be in only one fragmentation state at any given time. A connection that is not in the fragmentation state shall set the FC and FSN fields of a Connection’s Service Flow to 0 and 0000, respectively.

The authority to fragment a traffic on a connection is defined when the connecion is created by a MSAP.

The fragments are set in accordance with Table 10.

Table 10—Fragmentation Rules

Fragment	FC	FSN
First Fragment	10	0000
Continuing Fragment	11	incremented modulo 16
Last Fragment	01	incremented modulo 16

The sequence number allows the receiving terminal to re-create the original payload and to detect the loss of any intermediate packets. Upon loss, the receiving station shall discard all PDUs on the connection until a new fragment is detected or a non-fragmented PDU is detected.

6.6 Upstream Service

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 Section 6.12.5.

Table 11—Scheduling Services and Usage Rules

Scheduling Type	Piggy-Back Request	Bandwidth Stealing	Pollng
UGS	Not Allowed[a]	Not allowed	PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections
UGS-AD	Not Allowed	Not allowed	Not allowed
rtPS	Allowed	Allowed for GPT	Scheduling only allows unicast polling
nrtPS	Allowed	Allowed for GPT	Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise all forms of polling are allowed
BE	Allowed	Allowed for GPT	All forms of polling allowed

[a] Also a function of the MAC Header

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.

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 T1/E1 and 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 shall 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 Section 6.12.5.6.3) setting shall be such that the CPE is prohibited from using any contention request opportunities and the BS SHOULD not provide any unicast request opportunities for that connection. Piggy-back requests may be used to request additional bandwidth for a different connection using the Bandwidth Request Header. This will result in the CPE only using unsolicited data grants for upstream transmission on that connection. 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 Bandwidth Management fiels in the Generic MAC Header (refer to Figure 2) 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 Bandwidth Management field is the Slip Indicator (SI) bit. The CPE shall 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 shall clear the SI 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 shall 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 SI bit of the Bandwidth Management field 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 Bandwidth Management field is ignored with UGS service.

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 shall provide periodic unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (refer to Section 6.12.5.6.3) shall be such that the CPE is prohibited from using any contention request opportunities for that connection. 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 opportunites (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 USG/AD combines UGS and rtPS, only one scheduling service is active at a time.

The BS shall provide periodic unicast grants, when the flow is active, but shall 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 Section 6.12.5.6.3) shall be such that the CPE is prohibited from using any contention request a opportunities. 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. Because the Service Flow is provisioned as a UGS flow with a specific grant interval and grant size, when restarting UGS, the CPE shall 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 Bandwidth Management Field 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 Slip Indicator Bit in the Bandwidth Management Field. The remaining seven bits of the Bandwith Management Field 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 shall indicate the number of requested grants per Nominal Grant Interval in this field. The Active Grants field 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 shall 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 CIDs on an (periodic or non-periodic) interval on the order of one second or less.

The BS shall provide timely unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (refer to Section 6.12.5.6.3) SHOULD be such that the CPE is allowed to use contention request opportunities. This will result in the CPE using contention request opportunities as well as unicast request opportunities and unsolicited data grants. 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 netowrk policy. The key service elements are Nominal Polling Interval, Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Request/Transmission Policy and Traffic Priority.

6.6.5 Best Effort Service

The intent of the Best Effort (BE) service is to provide efficient service to best effort traffic. In order for this service to work correctly, the Request/Transmission Policy setting SHOULD be such that the CPE is allowed to use contention request opportunities. This will result in the CPE using contention request opportunities as well as unicast request opportunities and unsoliced data grants. 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 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 two dedicated connection IDs for the purpose of sending and receiving control messages. Two connections are used to allow differentiated levels of QoS to be applied to the different connections carrying MAC management traffic. 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 connection with Best Effort scheduling service, 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 connections and/or CPEs actually define bandwidth request contention IEs. The allocations are not in the form of an explicit message, but are contained as a series of Information Elements (IE) within the Uplink Map.

Note that polling is done on either a CPE or connection basis. Bandwidth is always requested on a connection ID basis and bandwidth is allocated on either a connection or CPE basis (based on CPE capability).

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 UL-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.). CPEs operating in GPT mode, which have an active UGS connection, may not be polled individually unless they set the Poll Me (PM) bit in the header of a packet on the UGS connection. 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 UGS connections and Best Effort connections. For UGS connections, the effect of a bandwidth request is to change the bandwidth allocated every frame. For Best Effort 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 47.

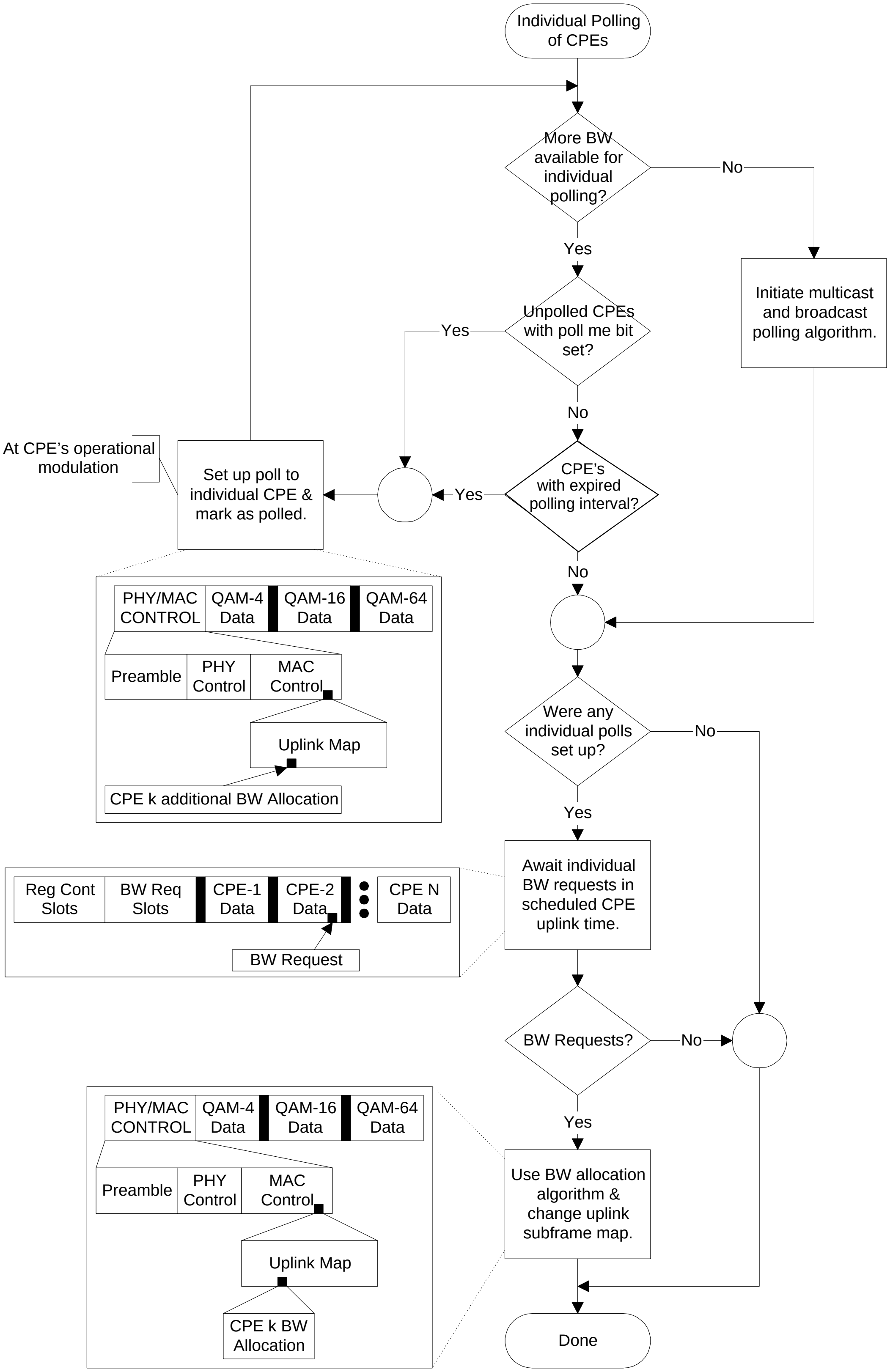

Individual Polling of CPEs
More BW available for individual polling?
No
Yes
Initiate multicast and broadcast polling algorithm.
Unpolled CPEs with poll me bit set?
Yes
No
At CPE's operational modulation
Set up poll to individual CPE & mark as polled.
Yes
CPE's with expired polling interval?
No
PHY/MAC CONTROL
QAM-4 Data
QAM-16 Data
QAM-64 Data
Preamble
PHY Control
MAC Control
Uplink Map
CPE k additional BW Allocation
Were any individual polls set up?
No
Yes
Reg Cont Slots
BW Req Slots
CPE-1 Data
CPE-2 Data
CPE N Data
BW Request
Await individual BW requests in scheduled CPE uplink time.
BW Requests?
No
Yes
PHY/MAC CONTROL
QAM-4 Data
QAM-16 Data
QAM-64 Data
Preamble
PHY Control
MAC Control
Uplink Map
CPE k BW Allocation
Use BW allocation algorithm & change uplink subframe map.
Done

Figure 47—Unicast Polling

6.7.1.2 Multicast and Broadcast

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 Table 1. 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.

Table 12—Sample Upstream Map with Multicast and Broadcast IE

Interval Description	Upstream MAP Information Element Fields		
	CID **(16 bits)**	**IUC** **(4 bits)**	**Offset** **(12 bits)**
Registration	0xFFFF	1	0
Multicast group 0xFFC5 Bandwidth Request	0xFFC5	1	405
Multicast group 0xFFDA Bandwidth Request	0xFFDA	1	200
Broadcast Bandwidth Request	0xFFFF	1	200
CPE 5 Uplink Grant	0x007B	4	156
CPE 21 Uplink Grant	0x01C9	7	75
*	*	*	*
*	*	*	*
*	*	*	*

When the poll is directed at a multicast or broadcast connection ID, CPEs belonging to the polled group may request bandwidth using Request Intervals allocated in the uplink frame. 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 Request intervals. CPEs always transmit using the modulation defined in the burst profile in the Request intervals. This will typically be at QPSK modulation.

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 the a truncated binary exponential back-off algorithm (see Section 6.4) to try at another contention opportunity. The multicast and broadcast polling process is shown in Figure 48.

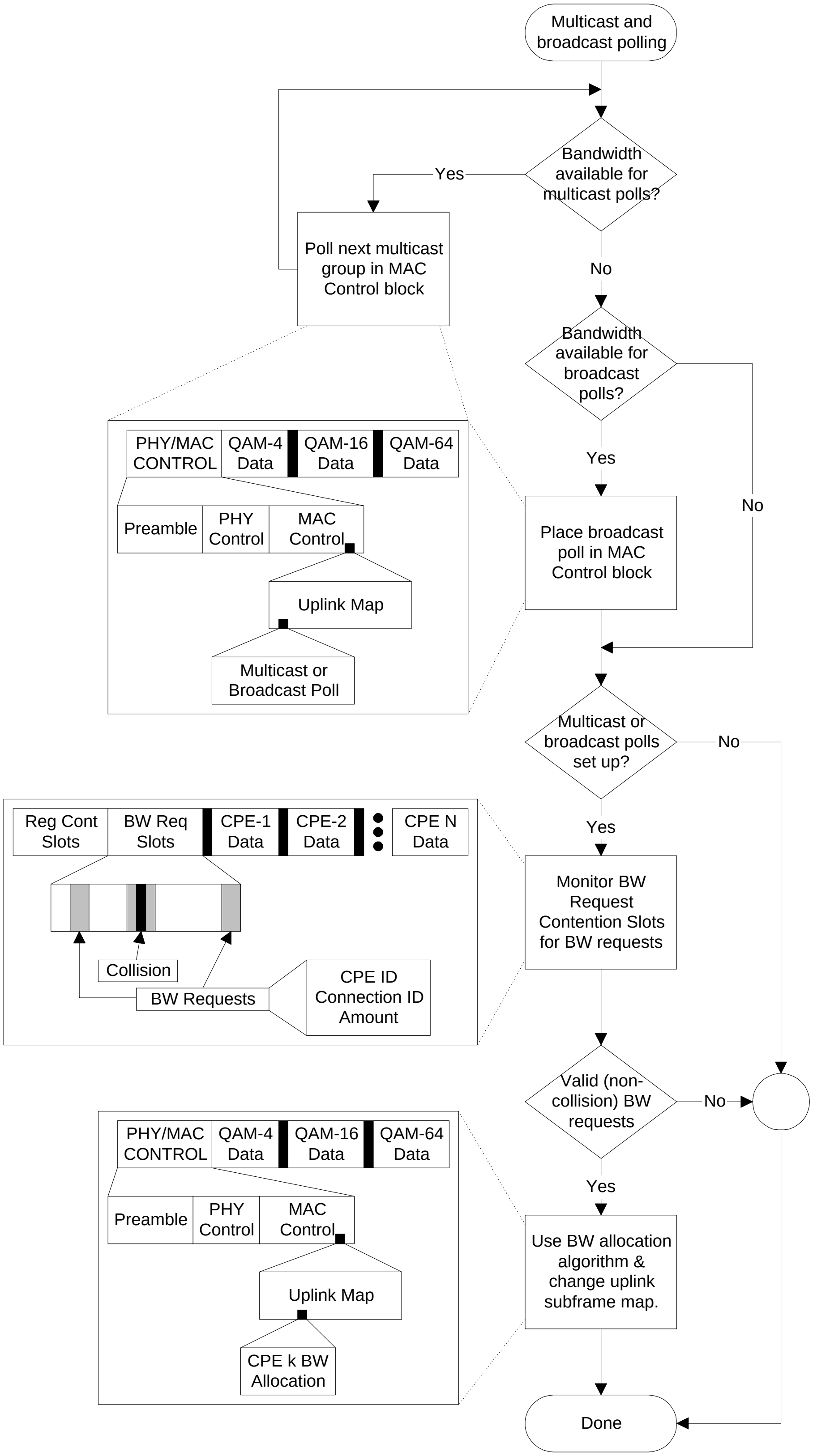

Multicast and broadcast polling
Bandwidth available for multicast polls?
Yes
No
Poll next multicast group in MAC Control block
Bandwidth available for broadcast polls?
Yes
No
PHY/MAC CONTROL
QAM-4 Data
QAM-16 Data
QAM-64 Data
Preamble
PHY Control
MAC Control
Uplink Map
Multicast or Broadcast Poll
Place broadcast poll in MAC Control block
Multicast or broadcast polls set up?
No
Yes
Reg Cont Slots
BW Req Slots
CPE-1 Data
CPE-2 Data
CPE N Data
Collision
BW Requests
CPE ID
Connection ID
Amount
Monitor BW Request Contention Slots for BW requests
Valid (non-collision) BW requests
No
Yes
PHY/MAC CONTROL
QAM-4 Data
QAM-16 Data
QAM-64 Data
Preamble
PHY Control
MAC Control
Uplink Map
CPE k BW Allocation
Use BW allocation algorithm & change uplink subframe map.
Done

Figure 48—Multicast and Broadcast Polling

6.7.2 Poll-Me Bit

CPEs with currently active USG connections may set the poll me bit (bit PM in the MAC header GM field) in a MAC packet of the USG connection to indicate to the BS that they need polled to request bandwidth. To reduce the bandwidth requirements of individual polling, CPEs with active USG connections need be individually polled only if the Poll-Me bit is set (or if the interval of the USG is too long to satisfy the QoS of the CPEs other connections). 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 49. To minimize the risk of the BS missing the poll me bit, the CPE may set the bit in all USG MAC headers in the frame.

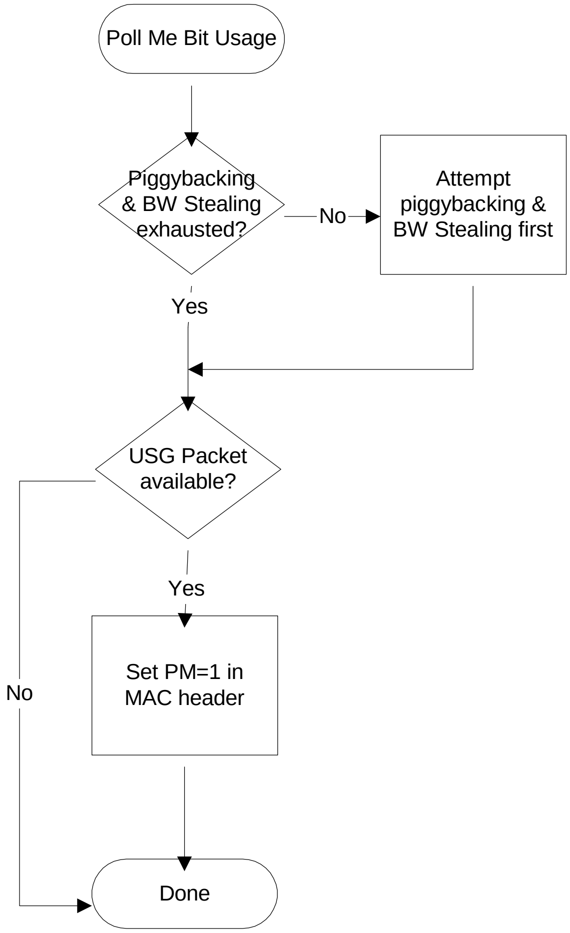

Poll Me Bit Usage
Piggybacking & BW Stealing exhausted?
No
Attempt piggybacking & BW Stealing first
Yes
USG Packet available?
Yes
No
Set PM=1 in MAC header
Done

Figure 49—Poll Me Bit Usage

6.8 Network Entry and Initialization

The procedure for initialization of a CPE modem shall be as shown in Figure 50. 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 Section 6.11.

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 PCD 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 EUI-64 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.

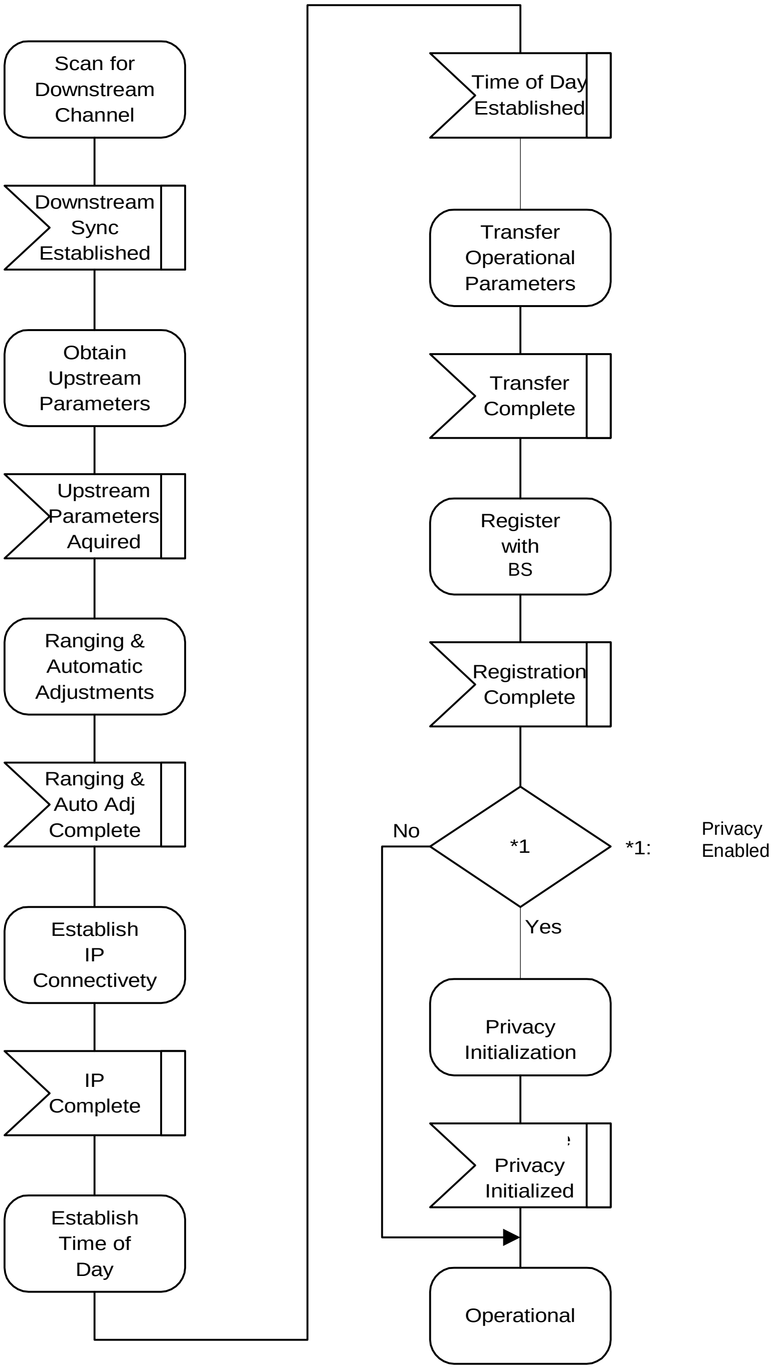

Scan for Downstream Channel
Downstream Sync Established
Obtain Upstream Parameters
Upstream Parameters Aquired
Ranging & Automatic Adjustments
Ranging & Auto Adj Complete
Establish IP Connectivety
IP Complete
Establish Time of Day
Time of Day Established
Transfer Operational Parameters
Transfer Complete
Register with BS
Registration Complete
No
*1
*1:
Privacy Enabled
Yes
Privacy Initialization
Privacy Initialized
Operational

Figure 50— CPE Initialization Overview

6.8.1 Scanning and Synchronization to Downstream

On initialization or after signal loss, the CPE modem shall acquire a downstream channel. The CPE shall have non-volatile storage in which the last operational parameters are stored and shall first try to re-acquire this downstream channel. If this fails, it shall 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 PCD 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.

6.8.2 Obtain Downstream Parameters

The MAC sublayer shall now search for the DS-MAP MAC management messages. The CPE achieves MAC synchronization once it has received at least one DS-MAP 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 PCD messages for its Upstream Channel ID. If the Lost SYNC Interval (refer to Section 6.11) has elapsed without a valid PCD message, a CPE shall not use the upstream and shall try to re-establish synchronization again.

6.8.3 Obtain Upstream Parameters

Refer to Figure 51. After synchronization, the CPE shall wait for a Physical Channel Descriptor message (PCD) 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 shall determine whether it can use the upstream channel from the channel description parameters.

The CPE shall collect all PCDs 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 shall continue scanning to find another downstream channel.

The CPE shall determine whether it can use the upstream channel from the channel description parameters. If the channel is not suitable, then the CPE shall try the next channel ID until it finds a usable channel. If the channel is suitable, the CPE shall extract the parameters for this upstream from the UCD. It then shall wait for the next DS-MAP message and extract the upstream mini-slot timestamp from this message. The CPE then shall 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 shall perform initial ranging at least once per Figure 52. If initial ranging is not successful, then the next channel ID is selected, and the procedure restarted from PCD extraction. When there are no more channel IDs to try, then the CPE shall continue scanning to find another downstream channel.

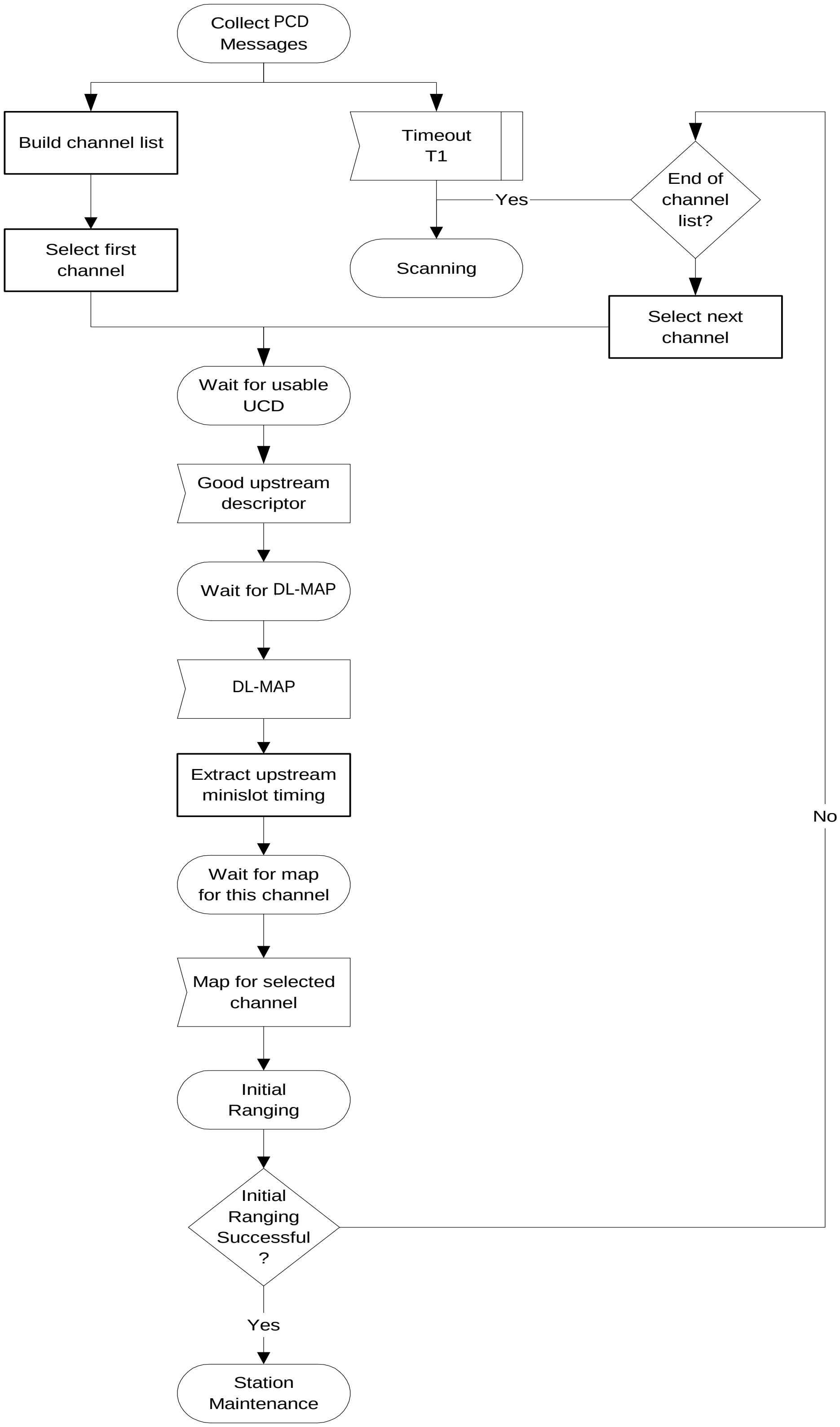


Figure 51— Obtaining Upstream Parameters

6.8.4 message Flows During Scanning and Upstream Parameter Acquisition

The BS shall generate DS-MAP and PCD messages on the downstream at periodic intervals within the ranges defined in Section 6.11. These messages are addressed to all CPEs. Refer to the following tables and figures.

Table 13—message Flows During Scanning and Upstream Parameter Acquisition

BS		CPE
clock time to send DS-MAP	----------------DS-MAP------------------->	|
clock time to send PCD	----------------PCD------------------------>	|
		|
clock time to send DS-MAP	----------------DS-MAP------------------->	|
		| Example of a PCD cycle
		| prior to CPE power-on
		|
clock time to send DS-MAP	----------------DS-MAP------------------->	|
		|
		|
		|
clock time to send DS-MAP	----------------DS-MAP------------------->	|
		|
		|
clock time to send DS-MAP	----------------DS-MAP------------------->	
clock time to send PCD	----------------PCD---------------------->	
clock time to send DS-MAP	----------------DS-MAP------------------->	
		power on sequence complete
clock time to send DS-MAP	----------------DS-MAP------------------->	
		establish PHY synchronization
		& wait for PCD
clock time to send DS-MAP	----------------DS-MAP-------------------->	
clock time to send DS-MAP	----------------DS-MAP-------------------->	
clock time to send PCD	----------------PCD---------------------->	
		obtain parameters for this upstream channel to use for initialization
clock time to send DS-MAP	----------------DS-MAP-------------------->	
		extract slot info for upstream & wait for transmit opportunity to perform ranging
clock time to send DS-MAP	----------------DS-MAP-------------------->	
clock time to send US-MAP	----------------US-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 a symbol that marks the beginning of a Mini-slot boundary. The timing delays through the PHY layer shall be relatively constant. Any variation in the PHY delays shall be accounted for in the guard time of the upstream PHY layer overhead.

First, a CPE modem shall synchronize to the downstream and learn the upstream channel characteristics through the Physical Channel Descriptor MAC management message. At this point, the CPE modem shall scan the US-MAP message to find an Initial Maintenance Region. The BS shall make an Initial Maintenance region large enough to account for the variation in delays between any two CPEs (maximum round trip propagation delay due to cell size plus maximum allowable implementation delay).

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

Ranging adjusts each CPE’s timing offset such that it appears to be co-located with the BS. The CPE shall set its initial timing offset to the amount of internal fixed delay equivalent to co-locating the CPE next to the BS. This amount includes delays introduced through a particular implementation, and shall include the downstream PHY interleaving latency, if any.

When the Initial Maintenance transmit opportunity occurs, the CPE modem shall send the Ranging Request message. Thus, the CPE sends the message as if it was co-located with the BS.

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

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

The BS shall return another Ranging Response message to the CPE modem with any additional fine tuning required. The ranging request/response steps shall be repeated until the response contains a Ranging Successful notification or the BS aborts ranging. Once successfully ranged, the CPE modem shall 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 Table 27.

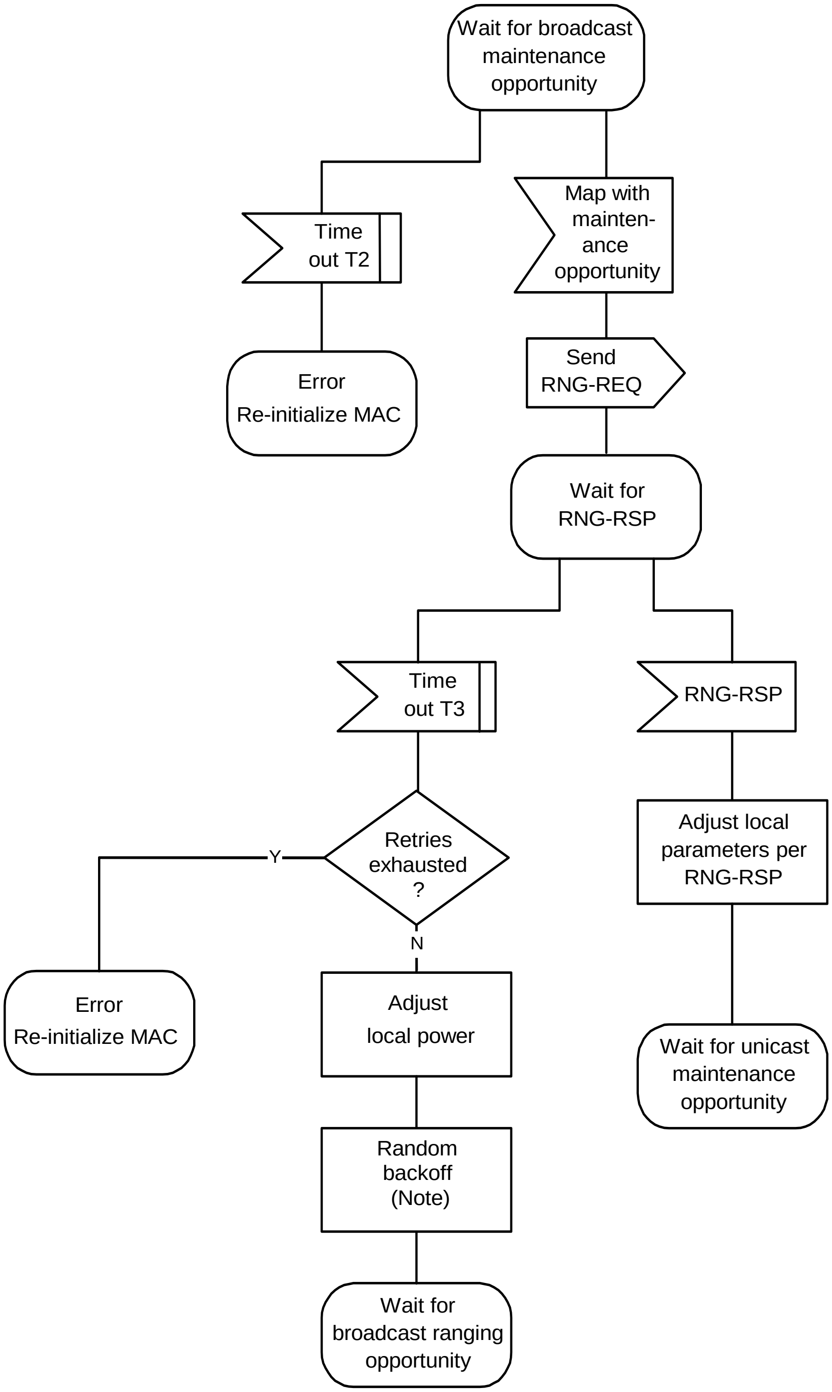
Note: The burst type to use for any transmission is defined by the Interval Usage Code (IUC). Each IUC is mapped to a burst type in the PCD message.

The message sequence chart and flow charts on the following pages define the ranging and adjustment process which shall be followed by compliant CPEs and BS.

Table 14—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 Connection ID	-----------US-MAP----------->	
	<---------RNG-REQ-------	transmit ranging packet in contention mode with Connection ID parameter = 0
[receive recognizable ranging packet]		
allocate temporary Connection ID		
send ranging response	----------RNG-RSP------->	
add temporary Connection ID to poll list		store temporary Connection ID & adjust other parameters
[time to send the next map]		
send map with Station Maintenance information element to modem using temporary CID	-----------US-MAP----------->	recognize own temporary Connection 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 Connection ID		
send periodic transmit opportunity to broadcast address	------------US-MAP---------->	

Note: The BS shall 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 Section 6.11.


Wait for broadcast maintenance opportunity
Time out T2
Map with mainten- ance opportunity
Error Re-initialize MAC
Send RNG-REQ
Wait for RNG-RSP
Time out T3
RNG-RSP
Retries exhausted ?
Y
N
Adjust local parameters per RNG-RSP
Error Re-initialize MAC
Adjust local power
Wait for unicast maintenance opportunity
Random backoff (Note)
Wait for broadcast ranging opportunity

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, theCPEMUST attempt initial ranging on every suitable upstream channel before moving to the next available downstream channel.

Figure 52—Initial Ranging - CPE

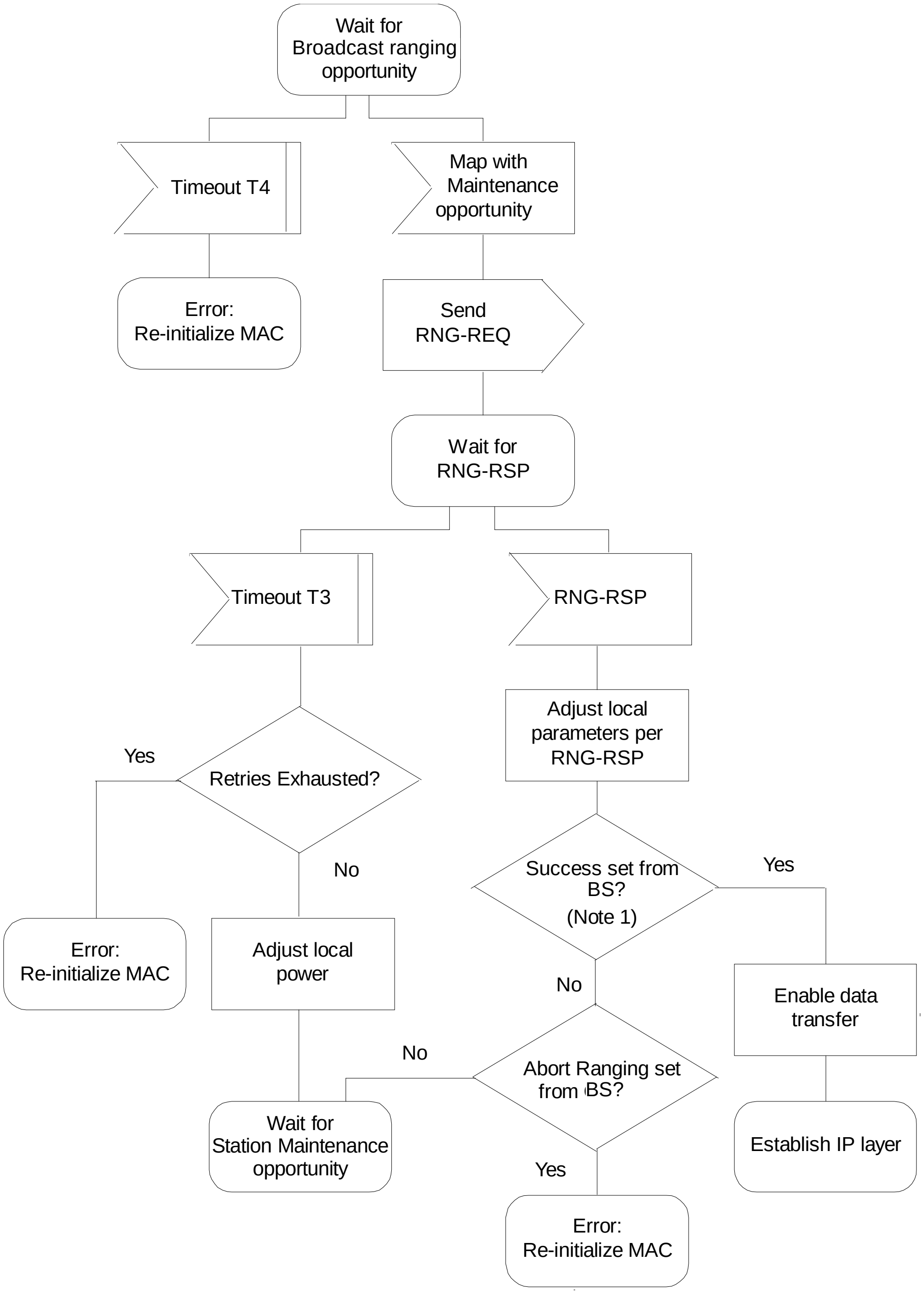


Figure 53—Initial Ranging - CPE (continued)

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

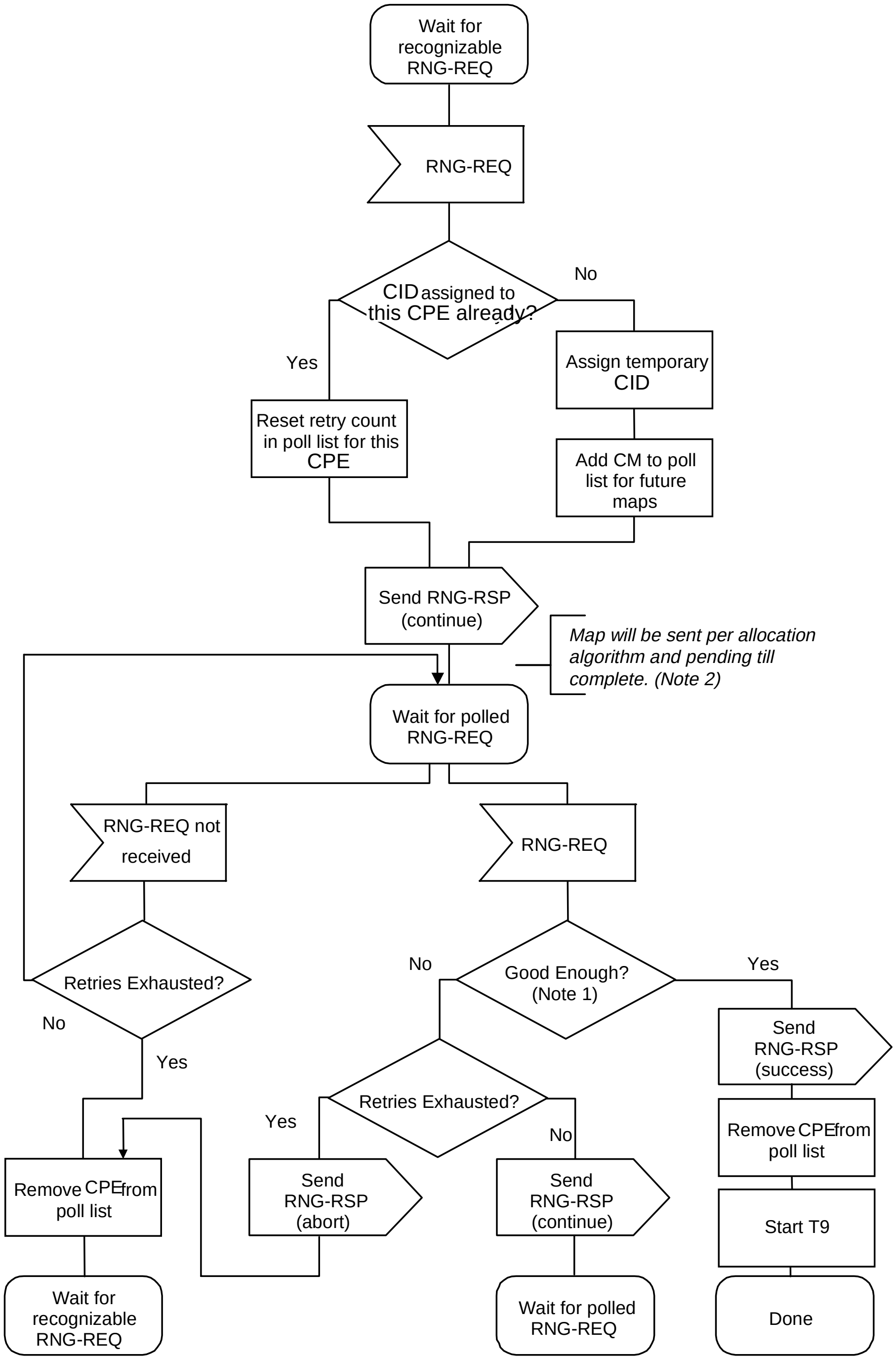

Wait for recognizable RNG-REQ
RNG-REQ
CID assigned to this CPE already?
No
Yes
Assign temporary CID
Reset retry count in poll list for this CPE
Add CM to poll list for future maps
Send RNG-RSP (continue)
Map will be sent per allocation algorithm and pending till complete. (Note 2)
Wait for polled RNG-REQ
RNG-REQ not received
RNG-REQ
Retries Exhausted?
No
Yes
Good Enough? (Note 1)
No
Yes
Send RNG-RSP (success)
Retries Exhausted?
Yes
No
Remove CPE from poll list
Send RNG-RSP (abort)
Send RNG-RSP (continue)
Remove CPE from poll list
Start T9
Wait for recognizable RNG-REQ
Wait for polled RNG-REQ
Done

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 shall 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:

All parameters shall be within the approved range at all times

a) Power adjustment shall start from the minimum value unless a valid power is available from non-volatile storage, in which case this shall be used as a starting point.
b) Power adjustment shall 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 shall wrap back to the minimum.

For multi-channel support, the CPE shall 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 shall invoke DHCP mechanisms [RFC-2131] in order to obtain an IP address and any other parameters needed to establish IP connectivity. The DHCP response shall contain the name of a file which contains further configuration parameters. Refer to Table 15.

Table 15—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		

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 shall be retrieved is defined in [RFC-868]. Refer to Table 16. The request and response shall be transferred using UDP. The time retrieved from the server (UTC) shall be combined with the time offset received from the DHCP response to create the current local time

Table 16—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		

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 shall 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 shall download the parameter file using TFTP, as shown in Section 55. The TFTP configuration parameter server is specified by the “siaddr” field of the DHCP response. The CPE shall use an adaptive timeout for TFTP based on binary exponential backoff. Refer to [RFC1123] and [RFC2349].

The parameter fields required in the DHCP response and the format and content of the configuration file shall be as defined in Section 6.13. Note that these fields are the minimum required for interoperability.

If a CPE downloads a configuration file containing an upstream channel and/or downstream frequency different from what the CPE is currently using, the CPE shall not send a Registration Request message to the BS. The CPE shall redo initial ranging using the configured upstream channel and/or downstream frequency.

6.8.8.1 Registration

A CPE shall 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 shall forward its provisioned set of service flows and any other operational parameters in the configuration file (refer to Section 6.13) to the BS as part of a Registration Request. Figure 55 shows the procedure that shall be followed by the CPE.

The configuration parameters downloaded to the CPE shall include a network access control object (see Section 6.12.1.3). If this is set to “no forwarding,” the CPE shall not forward data from attached CPE to the network, yet the CPE shall 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.

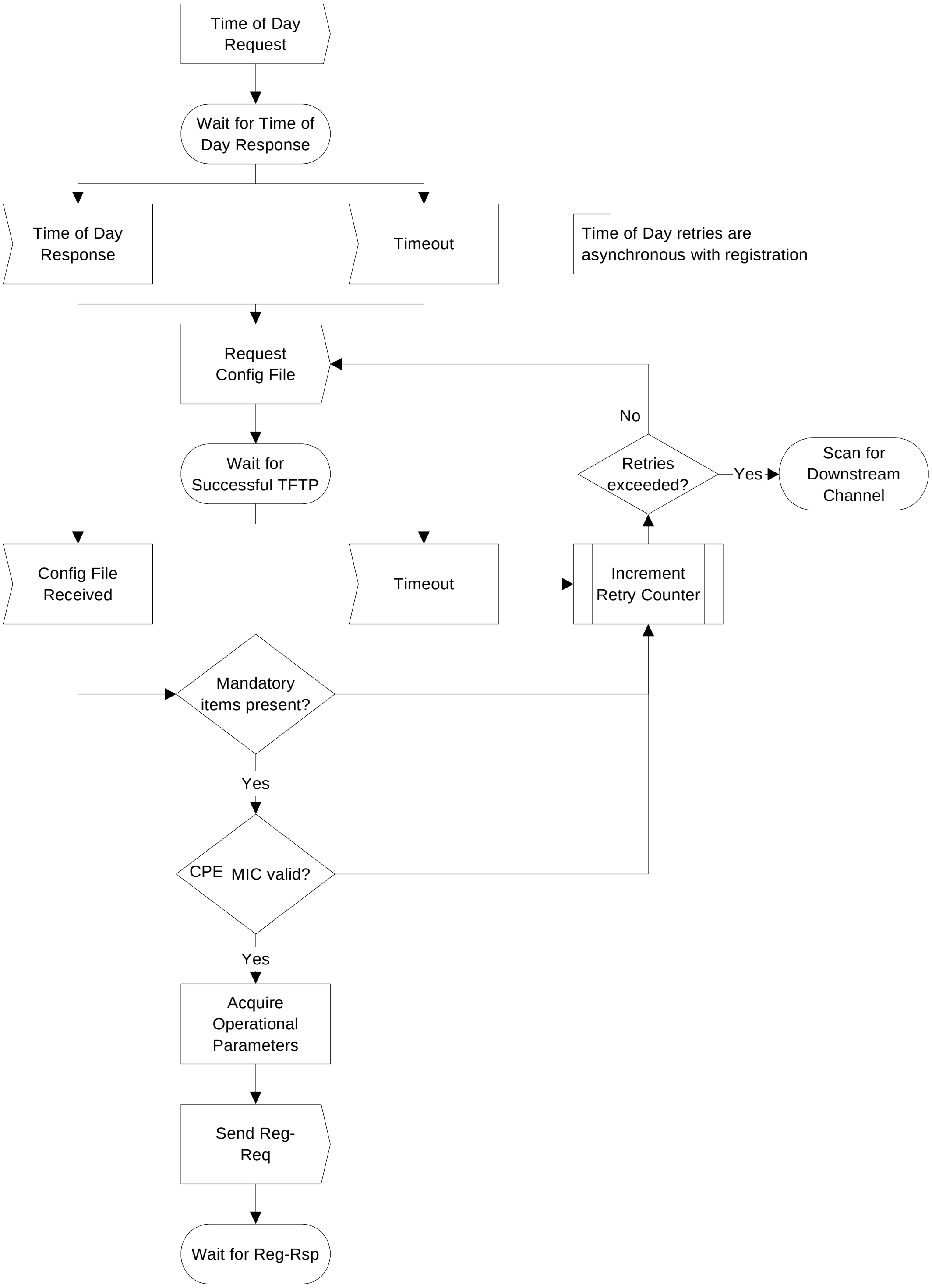


Figure 55—Registration — CPE

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

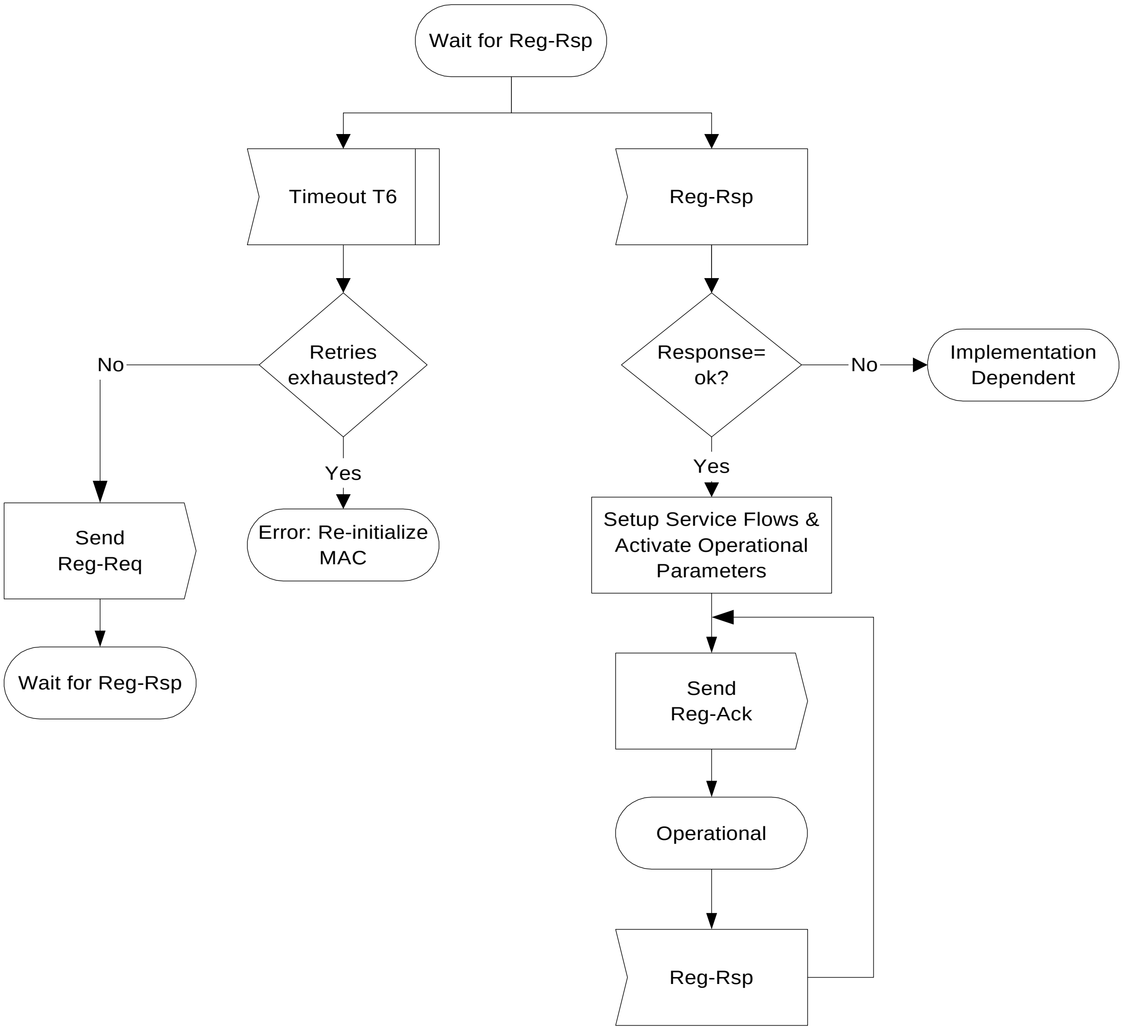


Figure 56—Wait for Registration Response — CPE

The BS shall perform the following operations to confirm the CPE authorization (refer to Figure 57):

a) Calculate a MIC per Section 6.13 and compare it to the BS MIC included in the Registration Request. If the MIC is invalid, the BS shall respond with an Authorization Failure.

b) 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 Table 27), the BS shall indicate authentication failure in the REG-RSP. The BS SHOULD also make a log entry stating the CPE MAC address from the message.

c) If present, check the TFTP Server Provisioned Modem Address field. If the Provisioned CPE Address does not match the requesting CPE’s actual address, the BS shall 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 shall respond with a Class of Service Failure and the appropriate Service Flow Response(s).
e) Verify the availability of any CPE Capabilities requested. If unable or unwilling to provide the CPE Capability requested, the BS shall turn that Modem Capability ‘off’ (refer to 6.2.8.1).
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 shall wait for a Registration Acknowedgment as shown in Figure 58.

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

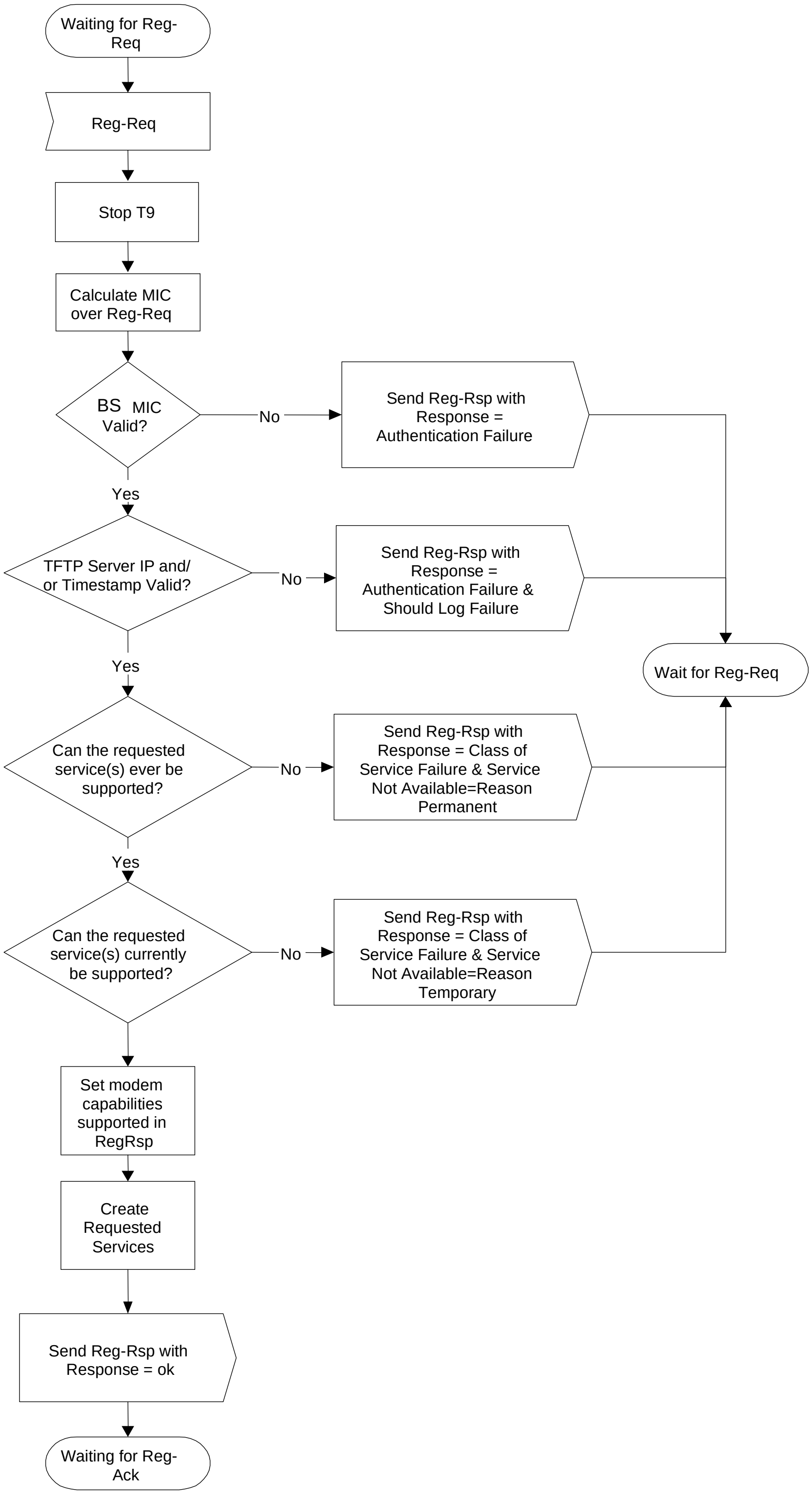

Waiting for Reg-Req
Reg-Req
Stop T9
Calculate MIC over Reg-Req
BS MIC Valid?
No
Send Reg-Rsp with Response = Authentication Failure
Yes
TFTP Server IP and/ or Timestamp Valid?
No
Send Reg-Rsp with Response = Authentication Failure & Should Log Failure
Yes
Wait for Reg-Req
Can the requested service(s) ever be supported?
No
Send Reg-Rsp with Response = Class of Service Failure & Service Not Available=Reason Permanent
Yes
Can the requested service(s) currently be supported?
No
Send Reg-Rsp with Response = Class of Service Failure & Service Not Available=Reason Temporary
Set modem capabilities supported in RegRsp
Create Requested Services
Send Reg-Rsp with Response = ok
Waiting for Reg-Ack

Figure 57—Registration — BS

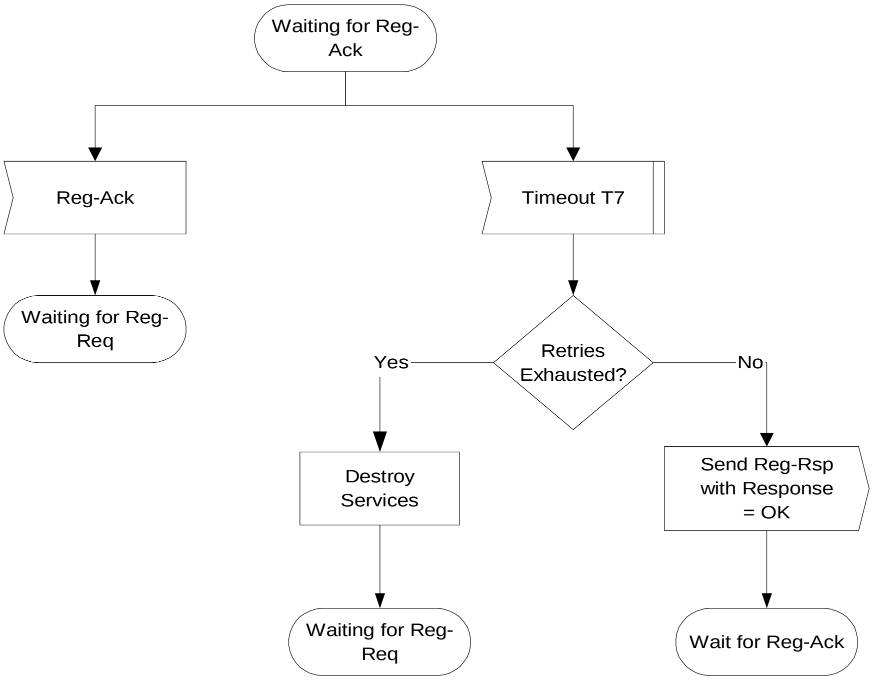


Figure 58—Registration Acknowledgment— BS

6.8.8.2 Privacy Initialization

Following registration, if the CPE is provisioned to run Privacy, the CPE shall initialize Privacy operations, as described in Section 7. A CPE is provisioned to run Privacy if its configuration file includes a Privacy Configuration Setting (Section 6.12.3.1.1) and if the Privacy Enable parameter (Section 6.12.1.12) 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 Connection ID in order to complete those steps.

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

On receiving a Ranging Response addressed to it, the CPE shall use the assigned temporary CID 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 shall consider any previously assigned temporary CID to be deassigned, and must obtain a new temporary CID via initial ranging.

It is possible that the Ranging Response may be lost after transmission by the BS. The CPE shall 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 CID previously assigned. If the BS assigns a new temporary CID, it shall make some provision for aging out the old CID that went unused (see Section TBD).

When assigning provisioned SFIDs on receiving a Registration Request, the BS may re-use the temporary CID, assigning it to one of the Service Flows requested. If so, it shall continue to allow initialization messages on that CID, since the Registration Response could be lost in transit. If the BS assigns all-new CIDs for class-of-service provisioning, it shall age out the temporary CID. The aging-out shall 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 shall operate using the best 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.

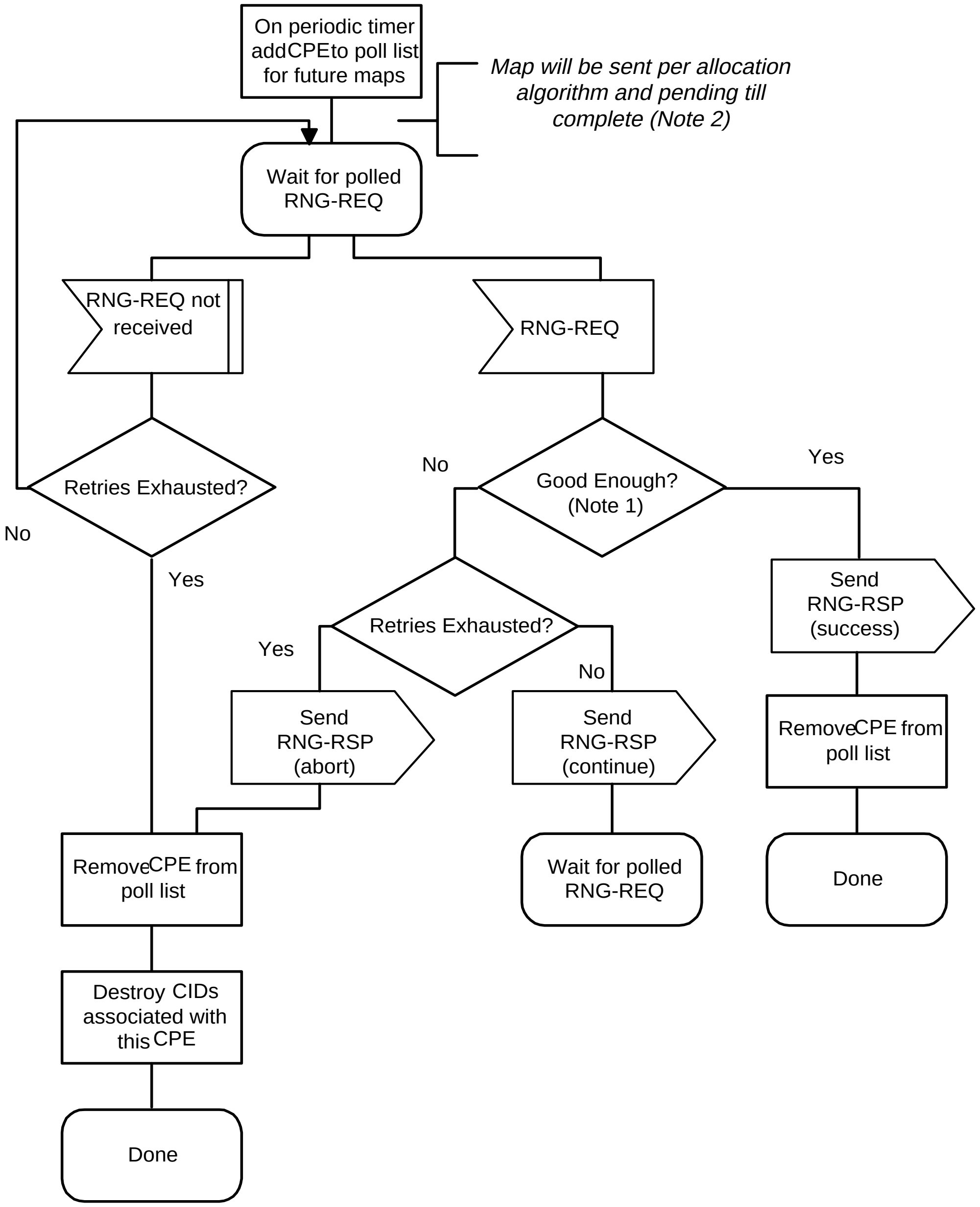
Both upstream and downstream channels shall be identified where required in MAC management messages using channel identifiers.

6.9 Ranging

The BS shall provide each CPE a Periodic Ranging opportunity at least once every T4 seconds. The BS shall 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 shall 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 59 and Figure 60. On receiving a RNG-RSP, the CPE shall not transmit until the RF signal has been adjusted in accordance with the RNG-RSP and has stabilized.


On periodic timer add CPE to poll list for future maps
Map will be sent per allocation algorithm and pending till complete (Note 2)
Wait for polled RNG-REQ
RNG-REQ not received
RNG-REQ
Retries Exhausted?
No
Yes
Good Enough? (Note 1)
No
Yes
Retries Exhausted?
Yes
No
Send RNG-RSP (success)
Send RNG-RSP (abort)
Send RNG-RSP (continue)
Remove CPE from poll list
Wait for polled RNG-REQ
Remove CPE from poll list
Done
Remove CPE from poll list
Destroy CIDs associated with this CPE
Done

Note 1: Means Ranging Request is within the tolerance limits of the BS for power and transmit equalization (if supported)
Note 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 power level. If opportunities are offered prior to the pending-till-complete expiry, the "good-enough" test which follows receiptof a RNG-RSP MUST NOT judge the CPE transmit equalization until pending-till-complete expires.

Figure 59—Periodic Ranging - BS

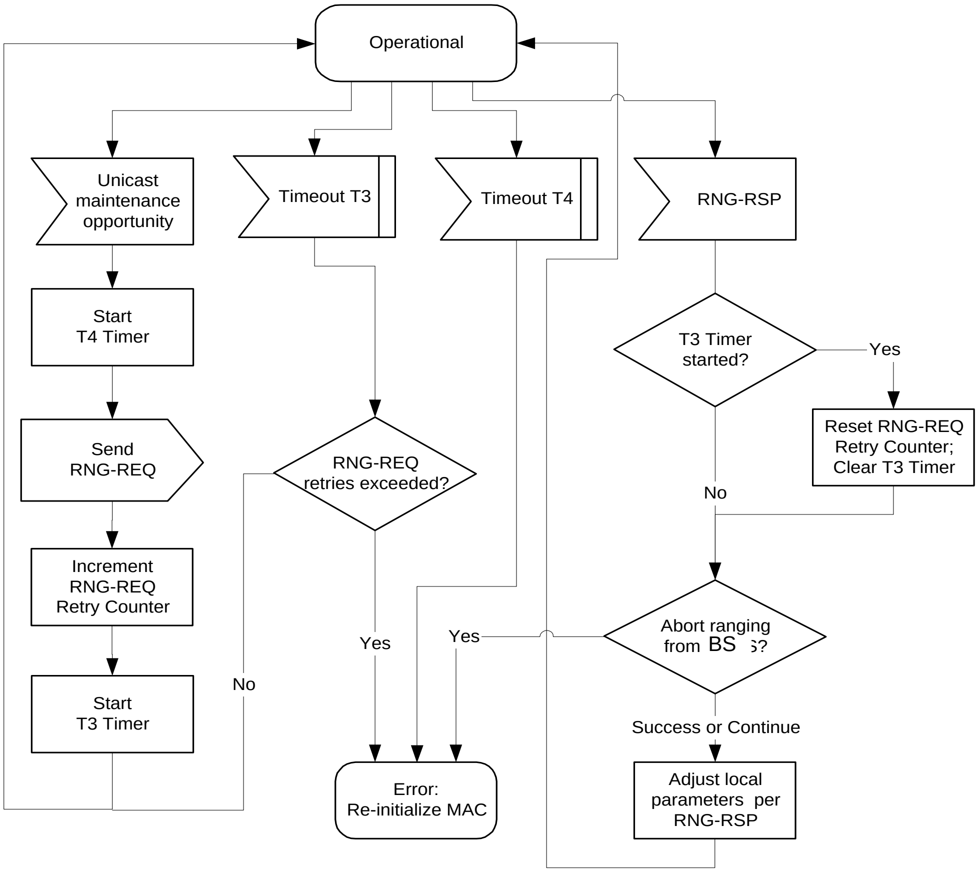


Figure 60—Periodic Ranging - CPE

6.9.1 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 straffic, 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 reciept 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 of different from the existing format.

Table 17—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		

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 shall be applied to the two threshold points in accordance with Figure 61. The Threshold Delta provides a hysterisis around which the CPE applies the thresholds.

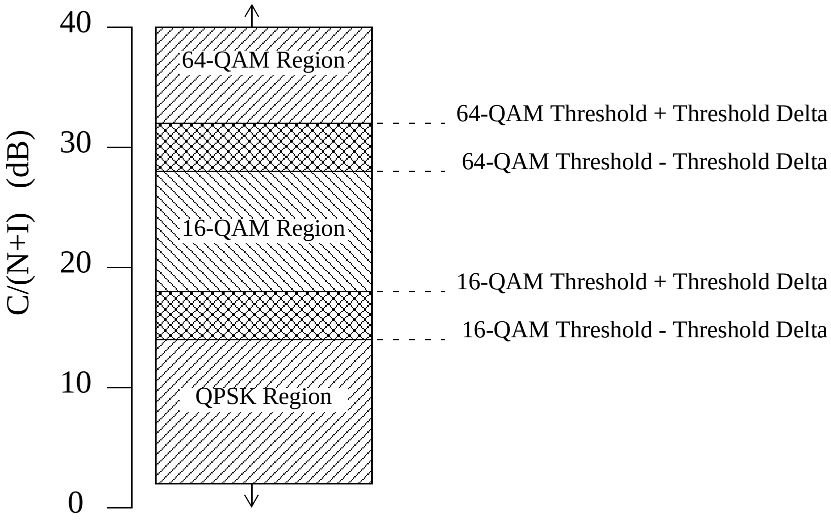

40
30
20
10
0
C/(N+I) (dB)
64-QAM Region
16-QAM Region
QPSK Region
64-QAM Threshold + Threshold Delta
64-QAM Threshold - Threshold Delta
16-QAM Threshold + Threshold Delta
16-QAM Threshold - Threshold Delta

Figure 61—Modulation Threshold Usage

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) Utilization of MAC scheduling and traffic parameters for upstream Service Flows.
d) Utilization of QoS traffic parameters for downstream Service Flows.
e) 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 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 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[1]. A Service Flow is characterized by a set of **QoS Parameters** such as latency, jitter, and throughput assurances. In order to

[1] A Service Flow, as defined here, has no direct relationship to the concept of a “flow” as defined by the IETF’s Integrated Services (intserv) 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.

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[2]:

a) **ServiceFlowID**: exists for all service flows
b) **Connection ID**: mapping to a SFID only exists when the connection has admitted or active service flow(s)
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.[3]
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[4] of the AdmittedQoSParameterSet which is always a subset of the authorized “envelope.” In the dynamic authorization model, this envelope is determined by the Authori-

[2] 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.

[3] The ProvisionedQoSParamSet is null when a flow is created dynamically.

[4] To say that QoS Parameter Set A is a subset of QoS Parameter Set B the following shall 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 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.

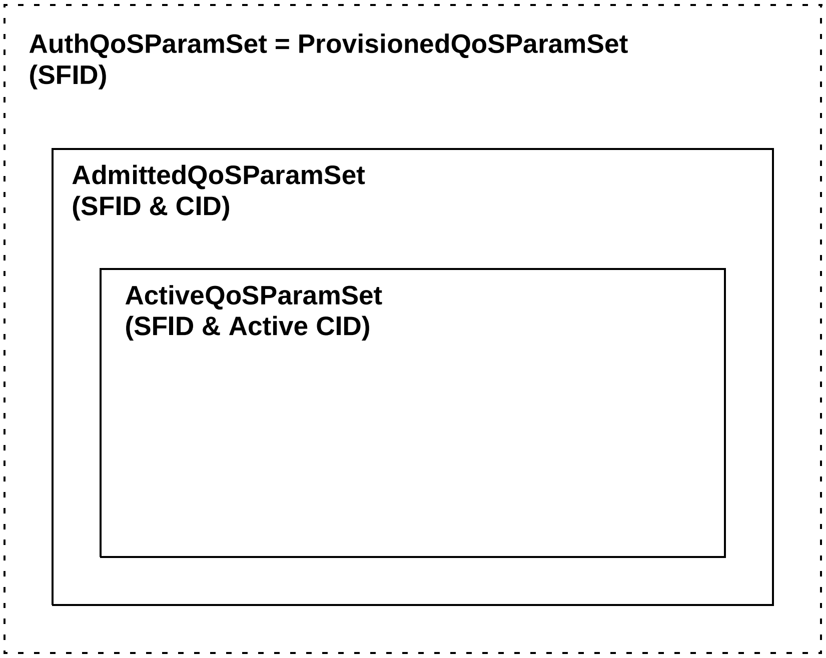


Figure 62—Provisioned Authorization Model “Envelopes”

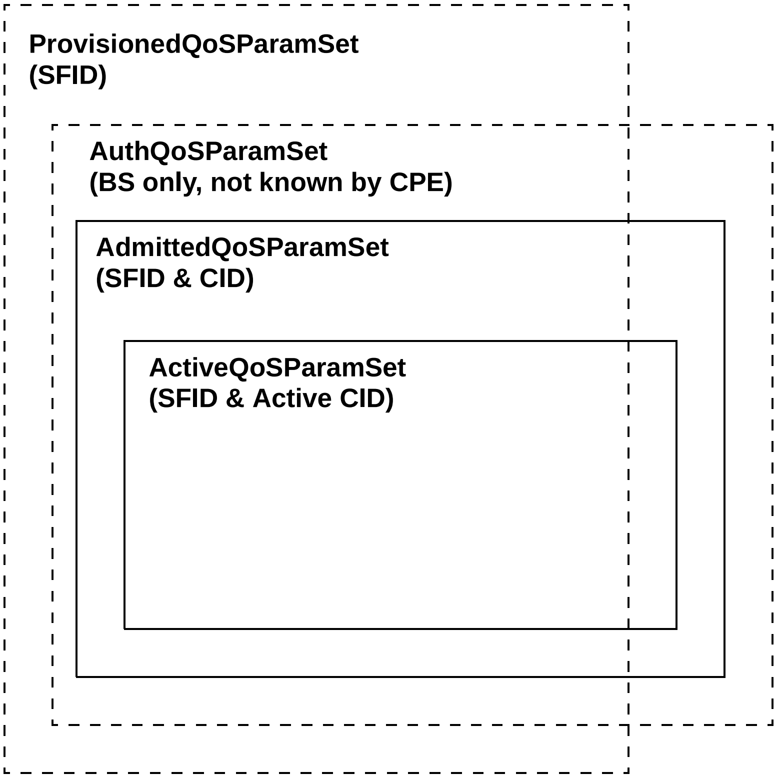


Figure 63—Dynamic Authorization Model “Envelopes”

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

The major objects of the architecture are represented by named rectangles in Figure 5-43. 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 Service Flows are mapped a 16-bit Connection ID (CID).

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 identfying 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.

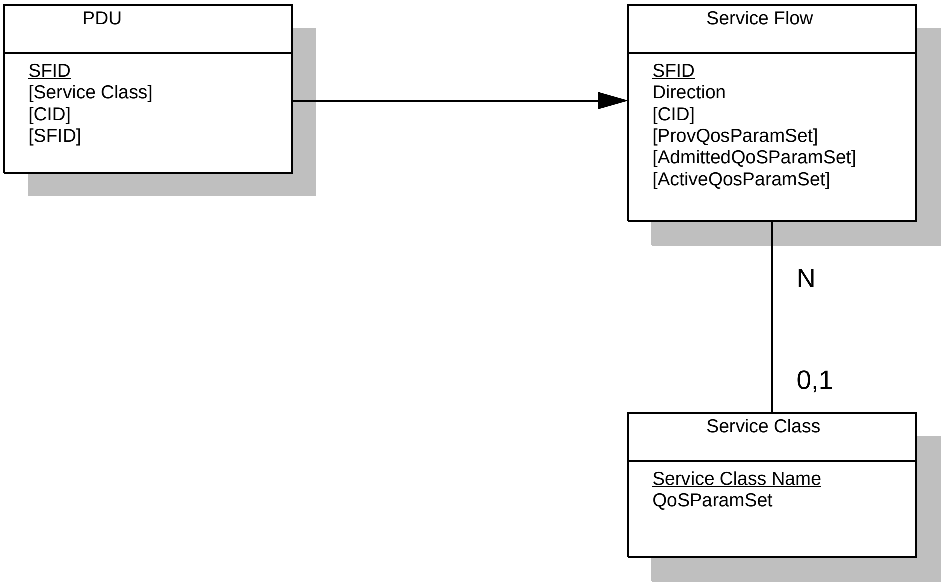


Figure 64—Theory of Operation Object Model

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 “unclassed” flows differently from “classed” 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 shall 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 shall 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 shall 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.

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 shall 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 shall be capable of caching the Provisioned QoS Parameter Set, and shall 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 Section 6.12.5.5.1)

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 Section 6.12.5.5.1). 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. If authorized and resources are available, the BS shall respond by mapping the Service Flow to a CID. 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, the BS may choose to activate a Service Flow by passing the Service Flow ID as well as the CID and the associated QoS Parameter Sets. 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 shall 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 are being added shall 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, shall 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 shall be enforced by the BS that requires Service Flow activation within this period. (Refer to Section 6.12.5.5.9) If Service Flow activation is not completed within this interval, the assigned resources in excess of the active QoS parameters shall 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 shall 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[5] 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 6.10.6.2)

A Service Flow may be Provisioned and immediately activated. This is the case for the Service Flows associated with the Basic CIDs. It is also typical of Service Flows for monthly subscription services, etc. These Service Flows are established at registration time and shall 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.

6.10.7 General Operation

6.10.7.1 Static Operation

Static configuration of 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

[5] According to its Request/Transmission Policy (refer toSection 6.12.5.6.3)

BS adds information and replies with a Registration Response. The CPE sends a Registration Acknowledge to complete registration.

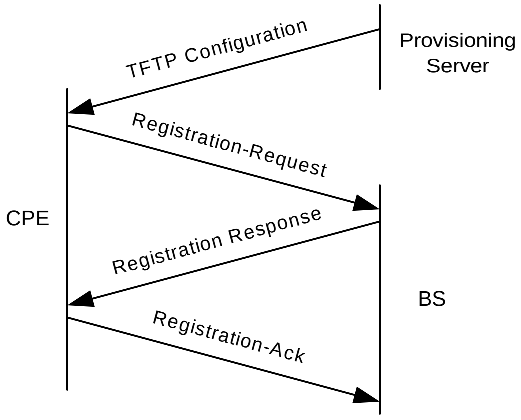


Figure 65—Registration Message Flow

A TFTP configuration file consists of one or more instances of Service Flow Encodings..

Table 18—TFTP File Contents

Items	Service Flow Reference	Service Flow ID
Service Flow Encodings Immediate activation requested, upstream	1..m	None Yet
Service Flow Encodings Provisioned for later activation requested, upstream	(m+1)..n	None Yet
Service Flow Encodings Immediate activation requested, downstream	(n+1)..p	None Yet
Service Flow Encodings 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 19—Registration Request Contents

Items	Service Flow	Service Flow ID
Service Flow Encodings Immediate activation requested, upstream May specify explicit attributes or service class name	1..m	None Yet
Service Flow Encodings Provisioned for later activation requested, upstream Explicit attributes or service class name	(m+1)..n	None Yet
Service Flow Encodings Immediate activation requested, downstream Explicit attributes or service name	(n+1)..p	None Yet
Service Flow Encodings 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 20—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.

6.10.7.2 Dynamic Service Flow Creation — CPE Initiated

Service Flows may be created by the Dynamic Service Addition process, as well as through the Registration process outlined above. The Dynamic Service Addition may be initiated by either the CPE or the BS, and may create one upstream and/or one downstream dynamic Service Flow(s). A three-way handshake is used to create Service Flows. The CPE-initiated protocol is illustrated in Figure 66 and described in detail in Section 6.10.8.4.1.

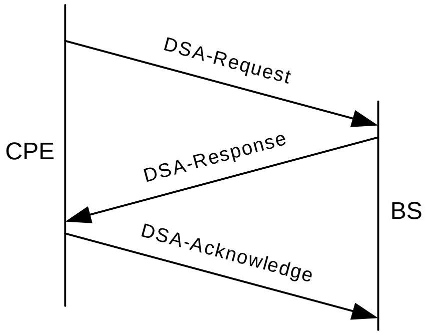


Figure 66—Dynamic Service Addition Message Flow — CPE Initiated

A DSA-Request from a CPE contains Service Flow Reference(s), and QoS Parameter set(s) (marked either for admission-only or for admission and activation).

6.10.7.2.1 Dynamic Service Flow Creation — BS Initiated

A DSA-Request from a BS contains Service Flow Identifier(s) for one upstream and/or one downstream Service Flow, possibly a CID, and set(s) of active or admitted QoS Parameters. The protocol is as illustrated in Figure 67 and is described in detail in Section 6.10.8.4.2.

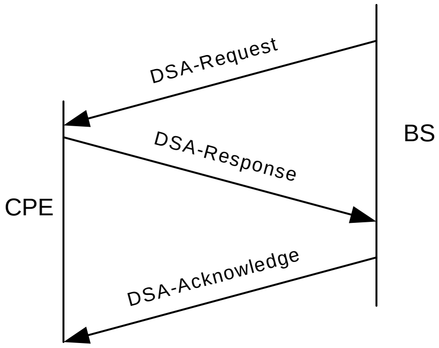


Figure 67—Dynamic Service Addition Message Flow — BS Initiated

6.10.7.2.2 Dynamic Service Flow Modification and Deletion

In addition to the methods presented above for creating service flows, protocols are defined for modifying and deleting service flows. Refer to Section 6.10.8.4 and Section 6.10.8.5.

Both provisioned and dynamically created Service flows are modified with the DSC message, which can change the Admitted and Active QoS Parameter sets of the flow.

A successful DSC transaction changes a Service Flow’s QoS parameters by replacing both the Admitted and Active QoS parameter sets. If the message contains only the Admitted set, the Active set is set to null and the flow is deactivated. If the message contains neither set (‘000’ value used for Quality of Service Parameter

Set type, see Section 6.12.5.5.1) then both sets are set to null and the flow is de-admitted. When the message contains both QoS parameter sets, the Admitted set is checked first and, if admission control succeeds, the Active set in the message is checked against the Admitted set in the message to ensure that it is a subse . If all checks are successful, the QoS parameter sets in the message become the new Admitted and Active QoS parameter sets for the Service Flow. If either of the checks fails, the DSC transaction fails and the Service Flow QoS parameter sets are unchanged.

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 68.

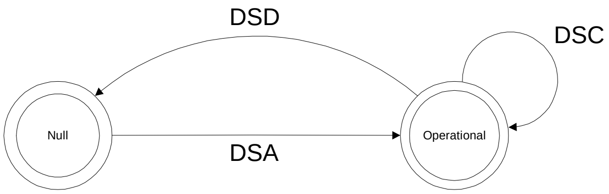


Figure 68—Dynamic Service Flow Overview

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 shall 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 shall select its TransactionIDs from the first half of the number space (0x0000 to 0x7FFF). The BS shall 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.

6.10.8.2 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 shall 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.

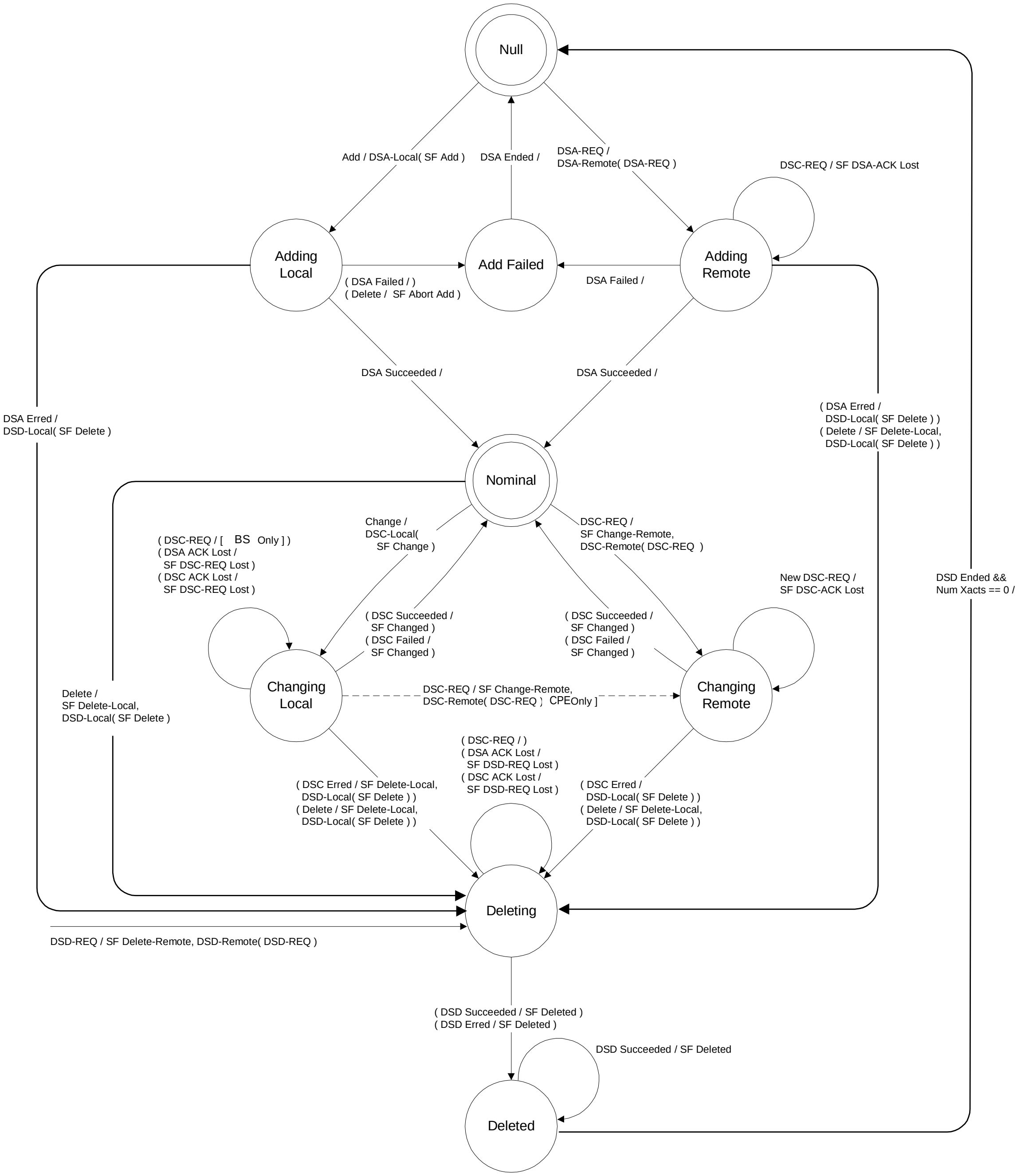


Figure 69—Dynamic Service Flow State Transition Diagram

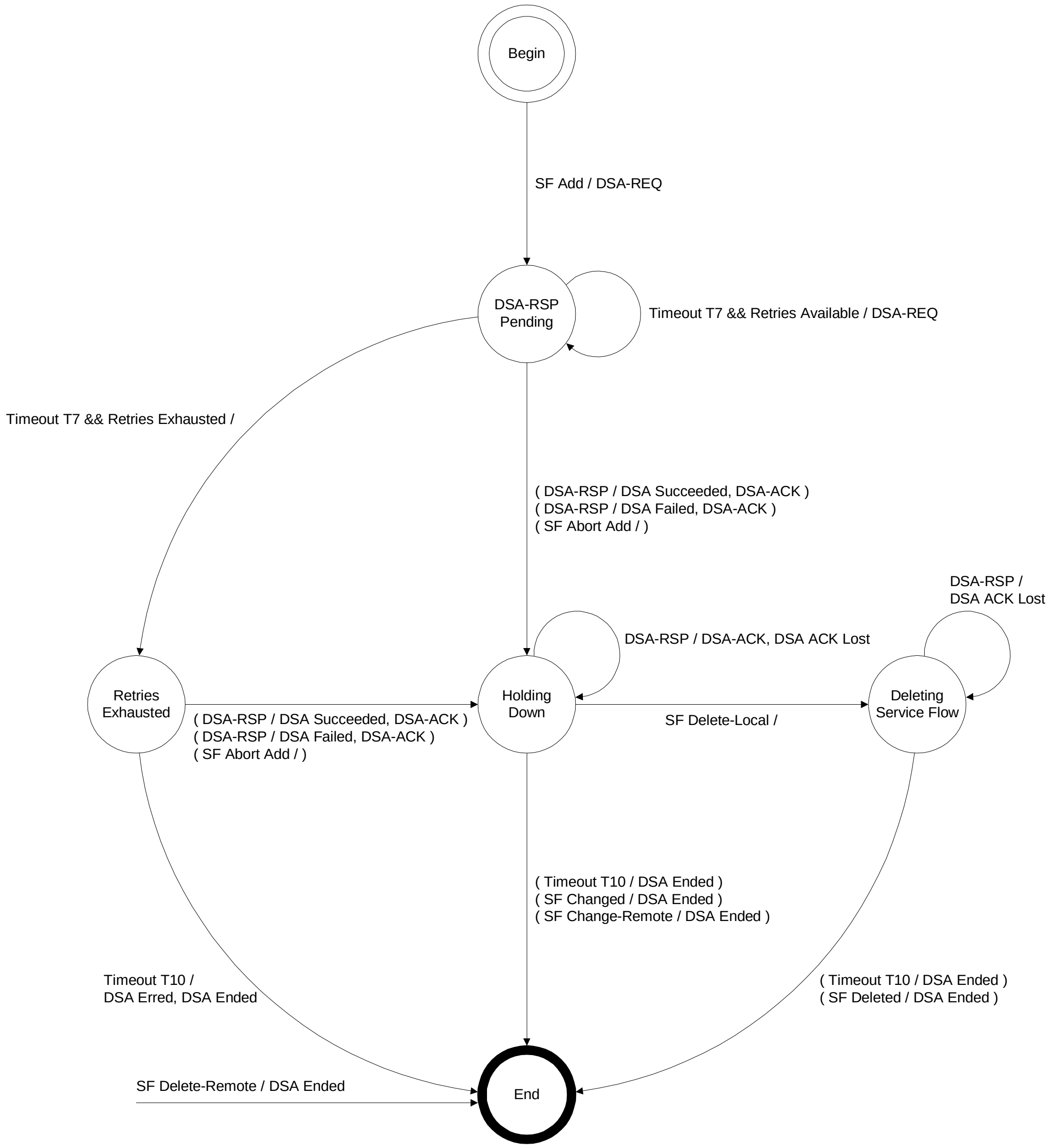

Begin
SF Add / DSA-REQ
DSA-RSP Pending
Timeout T7 && Retries Available / DSA-REQ
Timeout T7 && Retries Exhausted /
(DSA-RSP / DSA Succeeded, DSA-ACK)
(DSA-RSP / DSA Failed, DSA-ACK)
(SF Abort Add /)
DSA-RSP /
DSA ACK Lost
DSA-RSP / DSA-ACK, DSA ACK Lost
Retries Exhausted
Holding Down
Deleting Service Flow
(DSA-RSP / DSA Succeeded, DSA-ACK)
(DSA-RSP / DSA Failed, DSA-ACK)
(SF Abort Add /)
SF Delete-Local /
(Timeout T10 / DSA Ended)
(SF Changed / DSA Ended)
(SF Change-Remote / DSA Ended)
Timeout T10 /
DSA Erred, DSA Ended
(Timeout T10 / DSA Ended)
(SF Deleted / DSA Ended)
SF Delete-Remote / DSA Ended
End

Figure 70—DSA - Locally Initiated Transaction State Transition Diagram

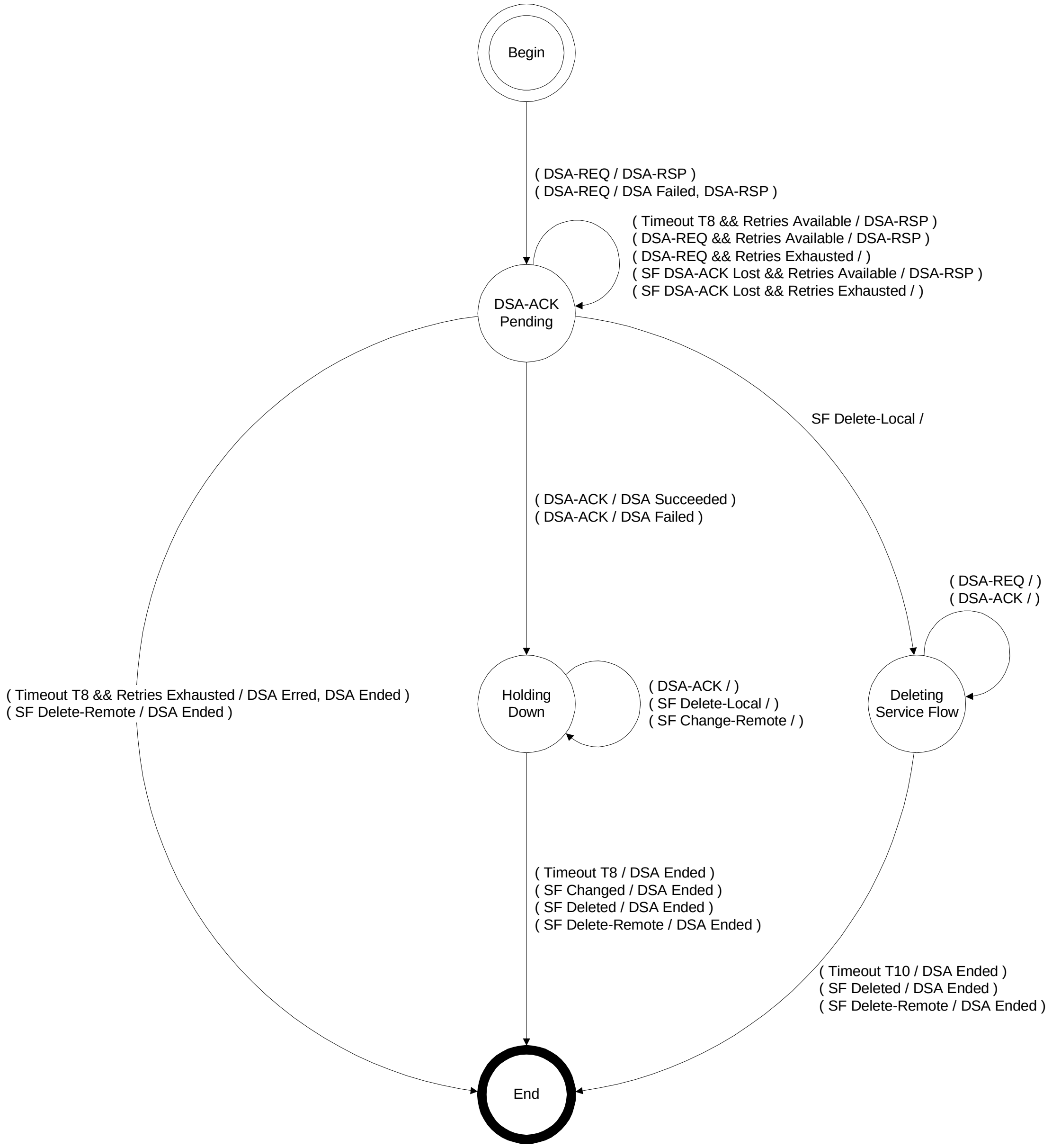

Begin
(DSA-REQ / DSA-RSP)
(DSA-REQ / DSA Failed, DSA-RSP)
(Timeout T8 && Retries Available / DSA-RSP)
(DSA-REQ && Retries Available / DSA-RSP)
(DSA-REQ && Retries Exhausted /)
(SF DSA-ACK Lost && Retries Available / DSA-RSP)
(SF DSA-ACK Lost && Retries Exhausted /)
DSA-ACK Pending
SF Delete-Local /
(DSA-ACK / DSA Succeeded)
(DSA-ACK / DSA Failed)
(DSA-REQ /)
(DSA-ACK /)
(Timeout T8 && Retries Exhausted / DSA Erred, DSA Ended)
(SF Delete-Remote / DSA Ended)
Holding Down
(DSA-ACK /)
(SF Delete-Local /)
(SF Change-Remote /)
Deleting Service Flow
(Timeout T8 / DSA Ended)
(SF Changed / DSA Ended)
(SF Deleted / DSA Ended)
(SF Delete-Remote / DSA Ended)
(Timeout T10 / DSA Ended)
(SF Deleted / DSA Ended)
(SF Delete-Remote / DSA Ended)
End

Figure 71—DSA - Remotely Initiated Transaction State Transition Diagram

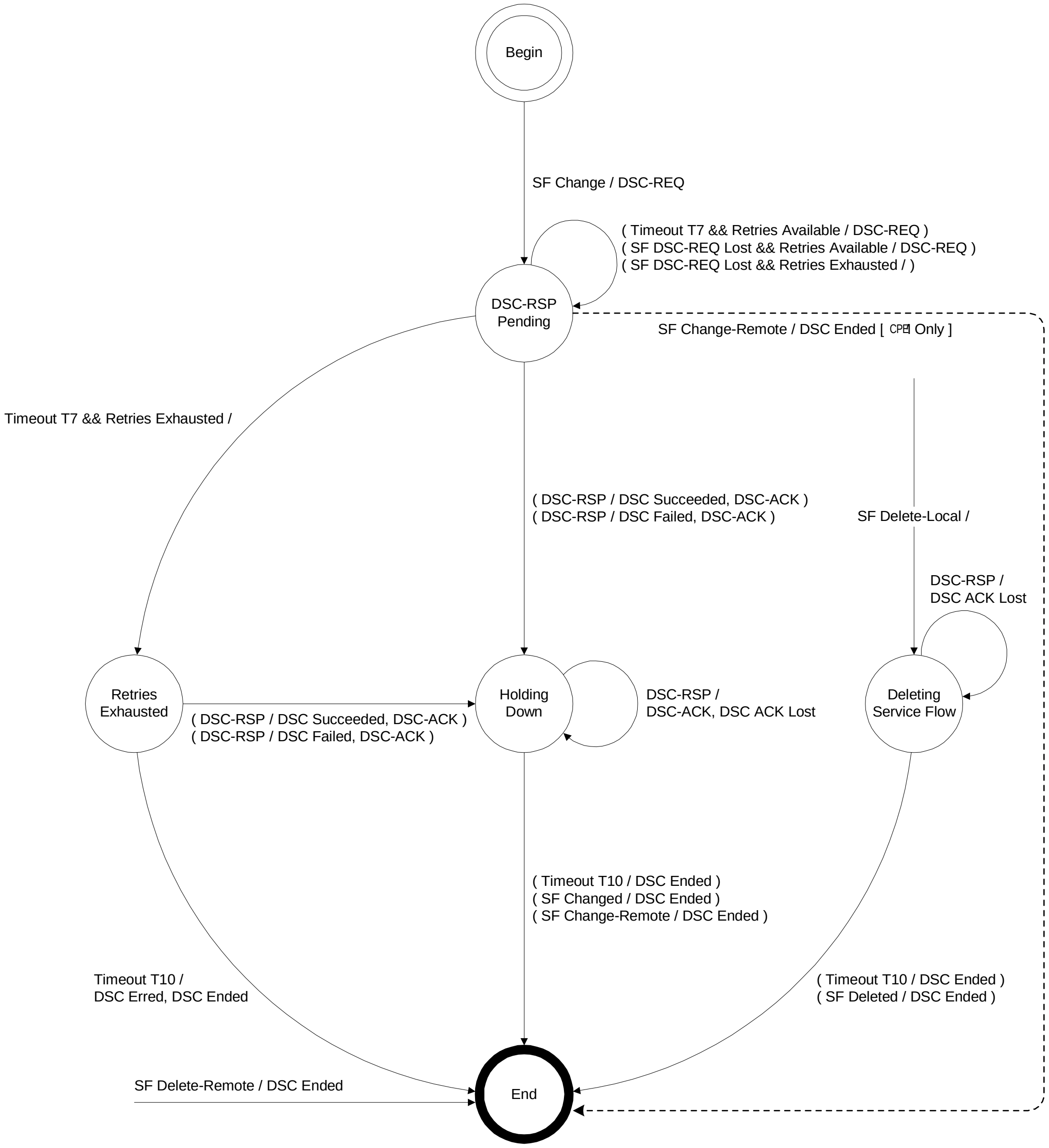

Begin
SF Change / DSC-REQ
(Timeout T7 && Retries Available / DSC-REQ)
(SF DSC-REQ Lost && Retries Available / DSC-REQ)
(SF DSC-REQ Lost && Retries Exhausted /)
DSC-RSP
Pending
SF Change-Remote / DSC Ended [CPE Only]
Timeout T7 && Retries Exhausted /
(DSC-RSP / DSC Succeeded, DSC-ACK)
(DSC-RSP / DSC Failed, DSC-ACK)
SF Delete-Local /
DSC-RSP /
DSC ACK Lost
Retries
Exhausted
(DSC-RSP / DSC Succeeded, DSC-ACK)
(DSC-RSP / DSC Failed, DSC-ACK)
Holding
Down
DSC-RSP /
DSC-ACK, DSC ACK Lost
Deleting
Service Flow
(Timeout T10 / DSC Ended)
(SF Changed / DSC Ended)
(SF Change-Remote / DSC Ended)
Timeout T10 /
DSC Erred, DSC Ended
(Timeout T10 / DSC Ended)
(SF Deleted / DSC Ended)
SF Delete-Remote / DSC Ended
End

Figure 72—DSC - Locally Initiated Transaction State Transition Diagram

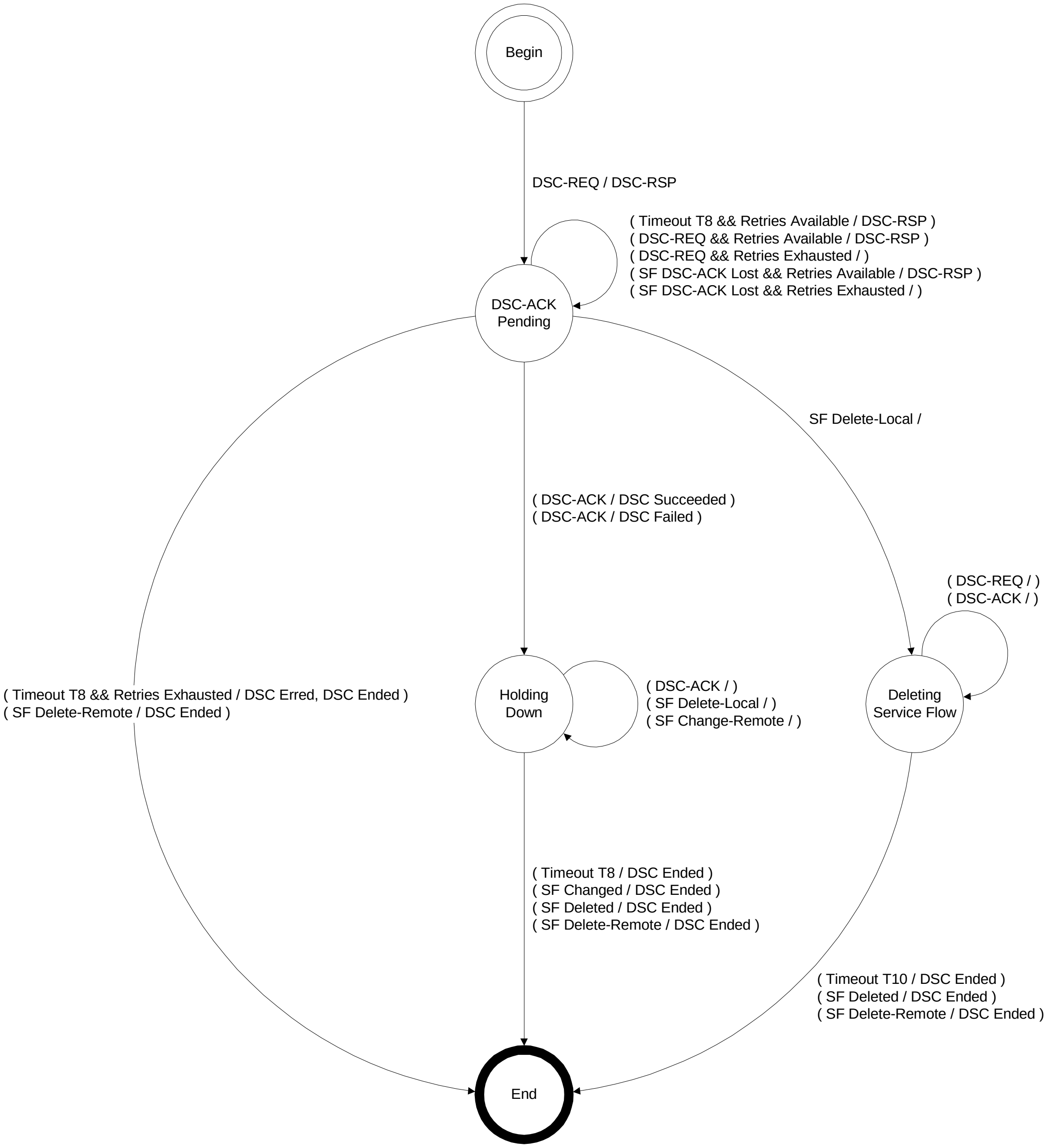

Begin
DSC-REQ / DSC-RSP
(Timeout T8 && Retries Available / DSC-RSP)
(DSC-REQ && Retries Available / DSC-RSP)
(DSC-REQ && Retries Exhausted /)
(SF DSC-ACK Lost && Retries Available / DSC-RSP)
(SF DSC-ACK Lost && Retries Exhausted /)
DSC-ACK Pending
SF Delete-Local /
(DSC-ACK / DSC Succeeded)
(DSC-ACK / DSC Failed)
(DSC-REQ /)
(DSC-ACK /)
(Timeout T8 && Retries Exhausted / DSC Erred, DSC Ended)
(SF Delete-Remote / DSC Ended)
Holding Down
(DSC-ACK /)
(SF Delete-Local /)
(SF Change-Remote /)
Deleting Service Flow
(Timeout T8 / DSC Ended)
(SF Changed / DSC Ended)
(SF Deleted / DSC Ended)
(SF Delete-Remote / DSC Ended)
(Timeout T10 / DSC Ended)
(SF Deleted / DSC Ended)
(SF Delete-Remote / DSC Ended)
End

Figure 73—DSC - Remotely Initiated Transaction State Transition Diagram

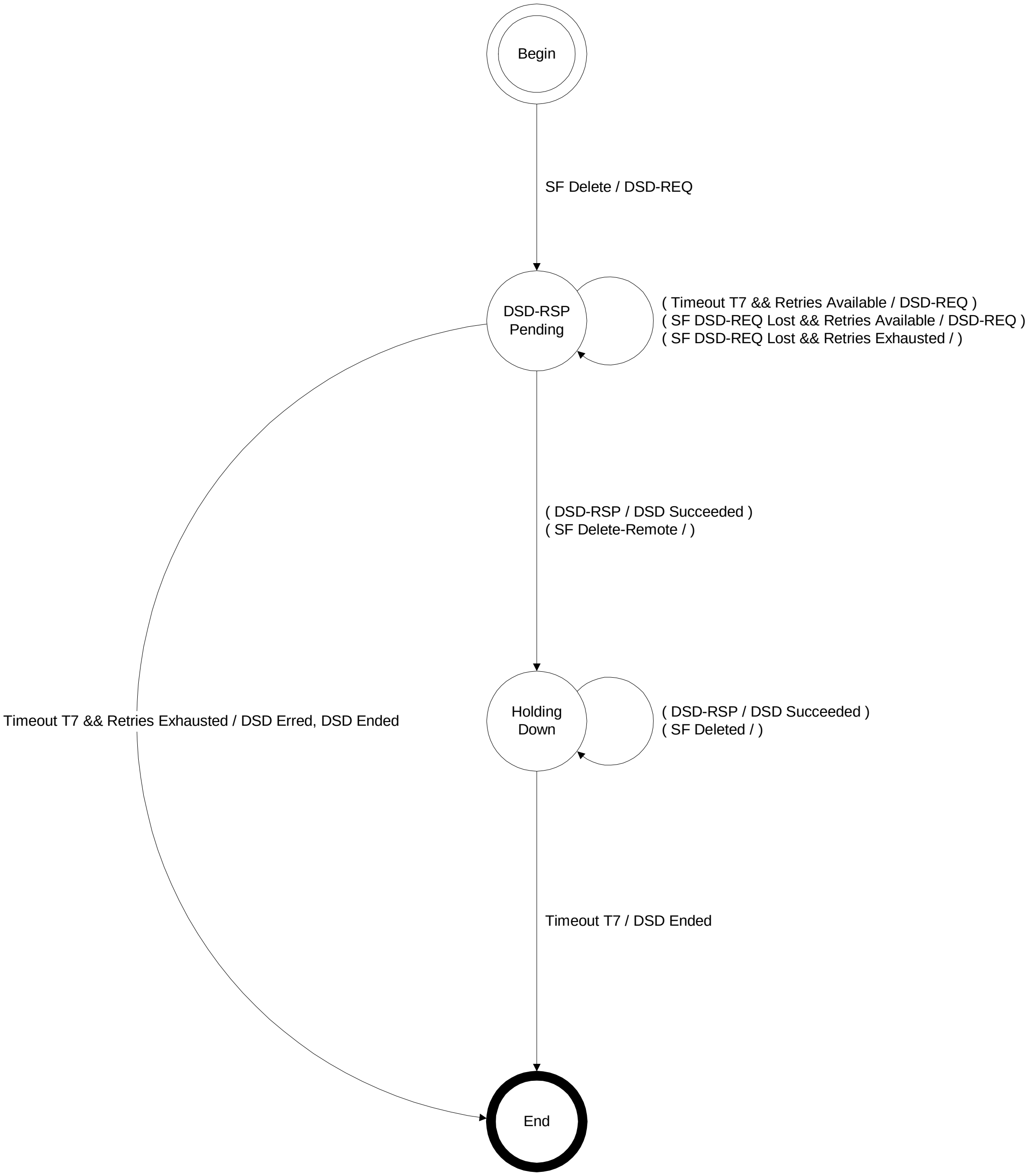

Begin
SF Delete / DSD-REQ
DSD-RSP Pending
(Timeout T7 && Retries Available / DSD-REQ)
(SF DSD-REQ Lost && Retries Available / DSD-REQ)
(SF DSD-REQ Lost && Retries Exhausted /)
(DSD-RSP / DSD Succeeded)
(SF Delete-Remote /)
Timeout T7 && Retries Exhausted / DSD Erred, DSD Ended
Holding Down
(DSD-RSP / DSD Succeeded)
(SF Deleted /)
Timeout T7 / DSD Ended
End

Figure 74—DSD - Locally Initiated Transaction State Transition Diagram

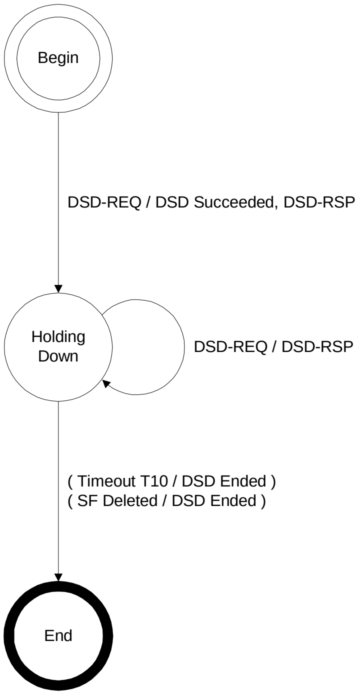

Begin
DSD-REQ / DSD Succeeded, DSD-RSP
Holding Down
DSD-REQ / DSD-RSP
(Timeout T10 / DSD Ended)
(SF Deleted / DSD Ended)
End

Figure 75—Dynamic Deletion (DSD) - Remotely Initiated Transaction State Transition Diagram

6.10.8.3 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.

CPE		BS
New Service Flow(s) needed		
Check if resources are available		
Send DSA-REQ	---DSA-REQ-->	Receive DSA-REQ
		Check if CPE authorized for Service(s)[a]
		Check Service Flow(s) QoS can be supported
		Create SFID(s)
		If upstream AdmittedQoSParamSet is non-null, map Service Flow to CID
		If upstream ActiveQoSParamSet is non-null, Enable reception of data on new upstream Service Flow
Receive DSA-RSP	<--DSA-RSP---	Send DSA-RSP
If ActiveQoSParamSet is non-null, Enable transmission and/or reception of data on new Service Flow(s)		
Send DSA-ACK	---DSA-ACK-->	Receive DSA-ACK
		If downstream ActiveQoSParamSet is non-null, Enable transmission of data on new downstream Service Flow

[a] 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 21—Dynamic Service Addition Initiated from CPE

6.10.8.3.1 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).

CPE		BS
		New Service Flow(s) required for CPE
		Check CPE authorized for Service(s)
		Check Service Flow(s) QoS can be supported
		Create SFID(s)
		If upstream AdmittedQoSParamSet is non-null, map Service Flow to CID
		If upstream ActiveQoSParamSet is non-null, Enable reception of data on new upstream Service Flow
Receive DSA-REQ	<--DSA-REQ---	Send DSA-REQ
Confirm CPE can support Service Flow(s)		
Add Downstream SFID (if present)		
Enable reception on any new downstream Service Flow		
Send DSA-RSP	---DSA-RSP-->	Receive DSA-RSP
		Enable transmission & reception of data on new Service Flow(s)
Receive DSA-ACK	<--DSA-ACK---	Send DSA-ACK
Enable transmission on new upstream Service Flow		

Table 22—Dynamic Service Addition Initiated from BS

6.10.8.3.2 Dynamic Service Addition State Transition Diagrams

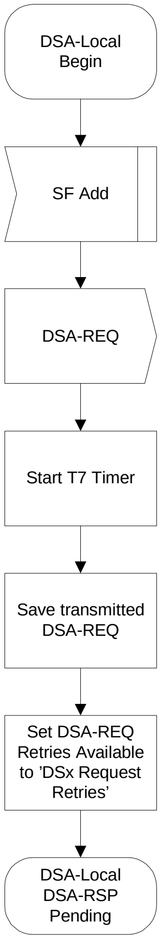


Figure 76—DSA - Locally Initiated Transaction Begin State Flow Diagram

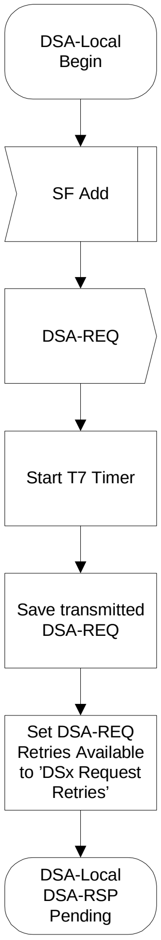


Figure 77—DSA - Locally Initiated Transaction Begin State Flow Diagram

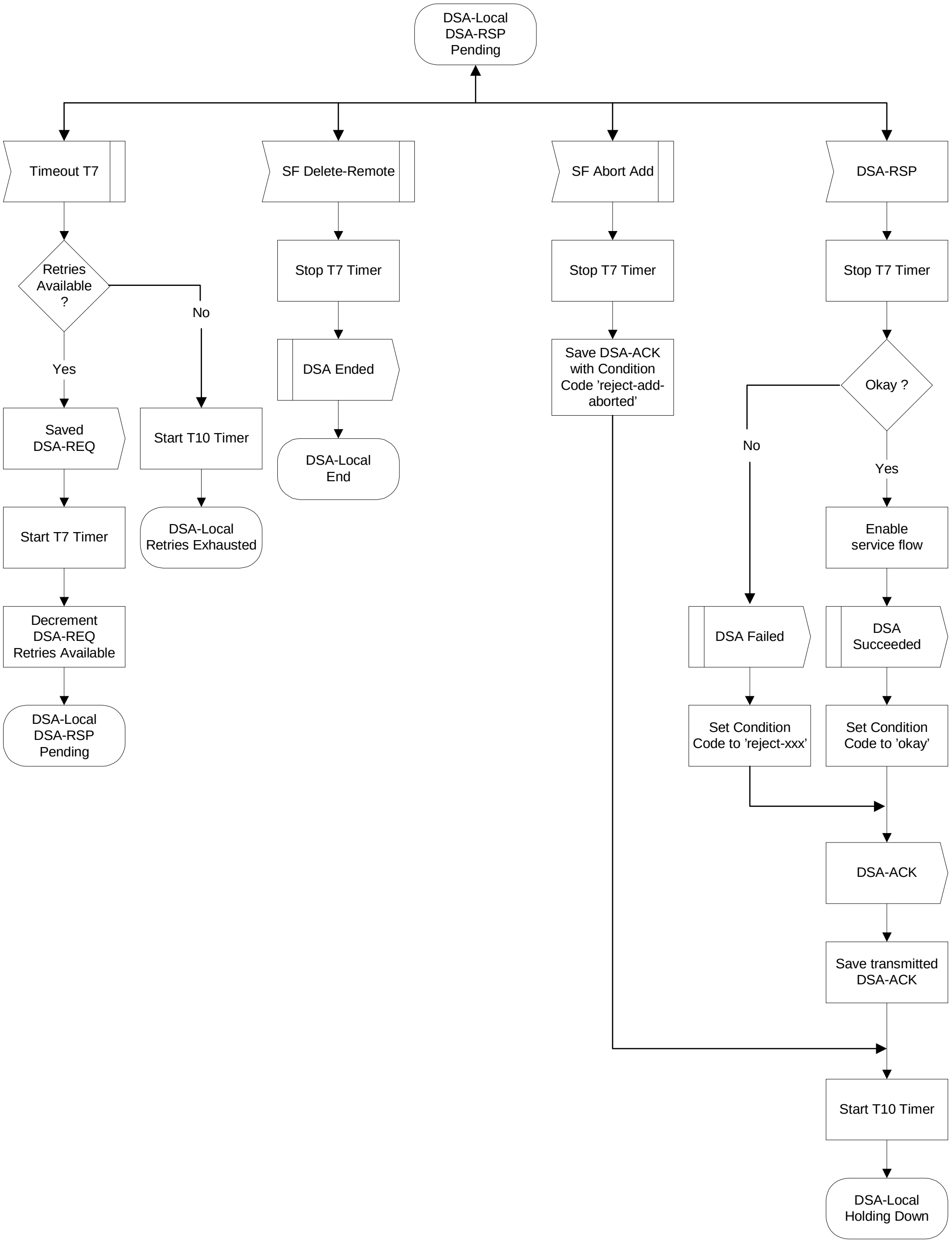


Figure 78—DSA - Locally Initiated Transaction DSA-RSP Pending State Flow Diagram

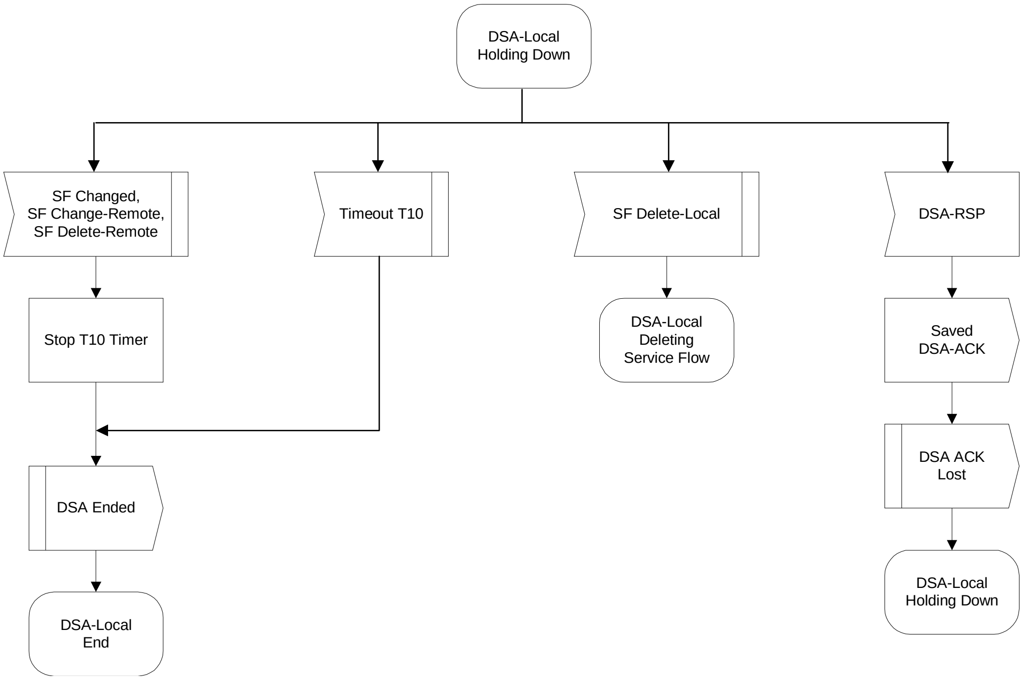


Figure 79—DSA - Locally Initiated Transaction Holding State Flow Diagram

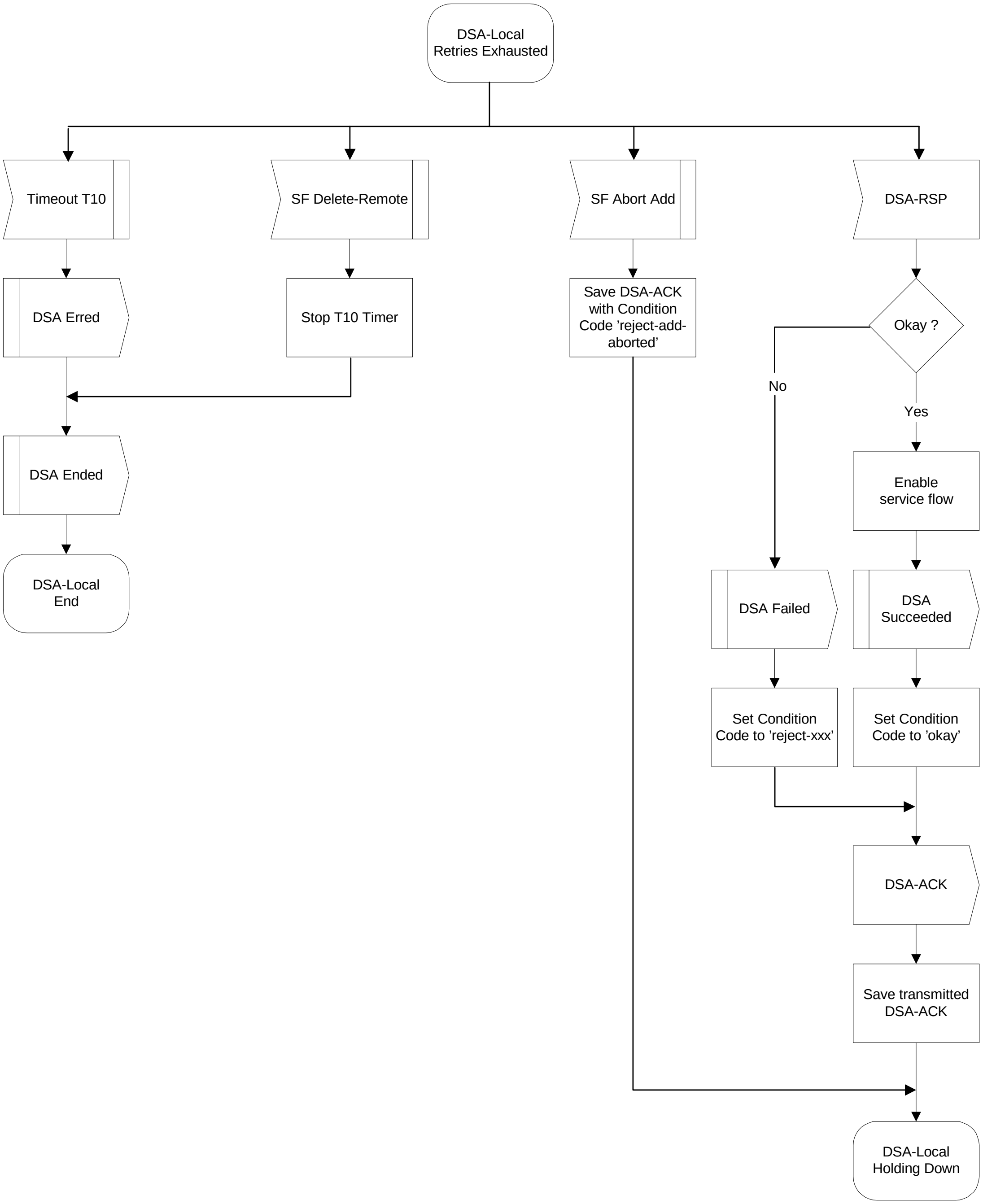


Figure 80—DSA - Locally Initiated Transaction Retries Exhausted State Flow Diagram

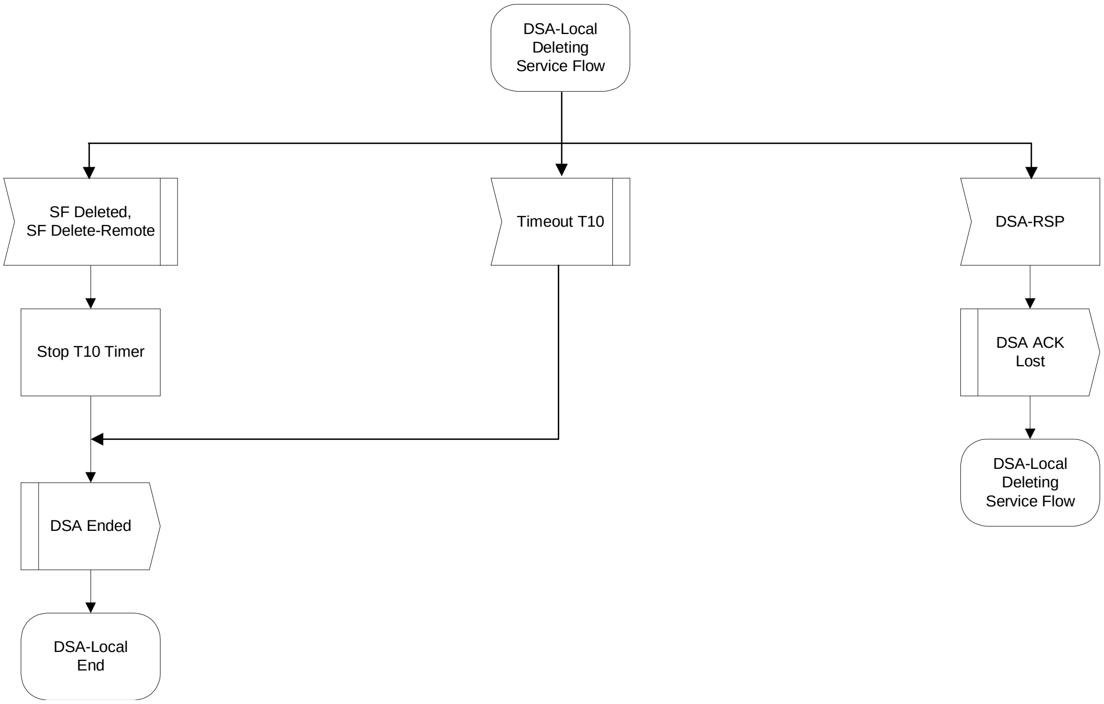


Figure 81—DSA - Locally Initiated Transaction Deleting Service Flow State Flow Diagram

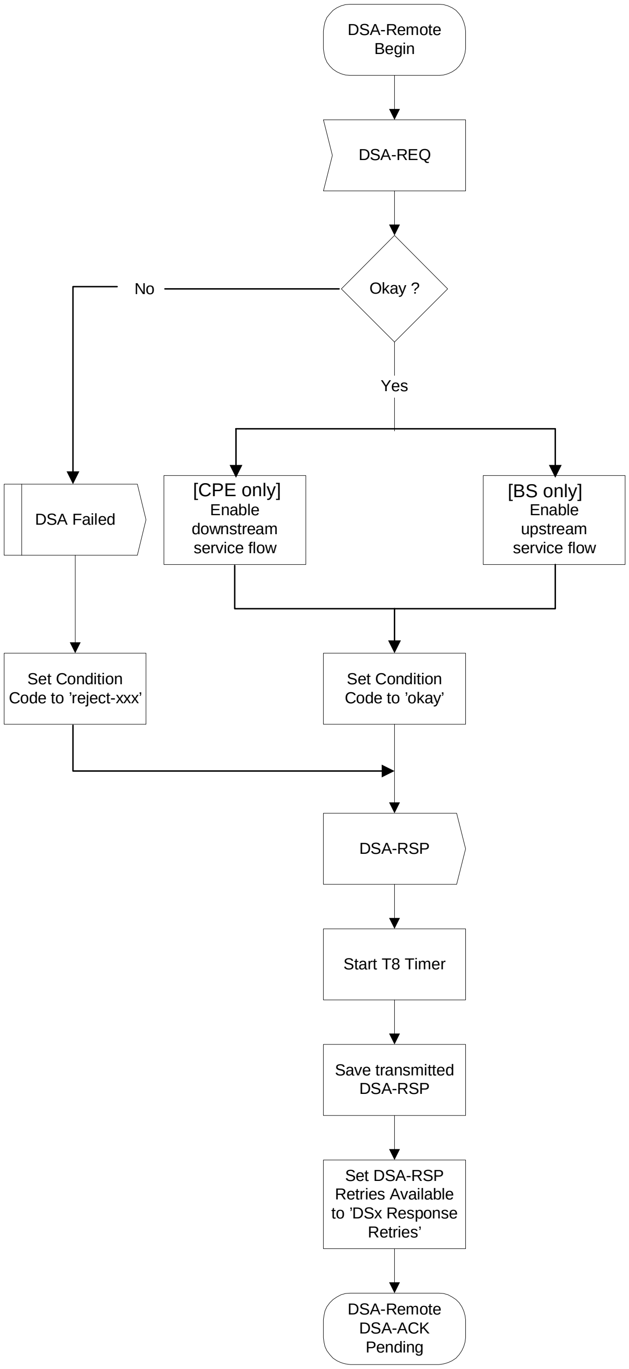


Figure 82—DSA - Remotely Initiated Transaction Begin State Flow Diagram

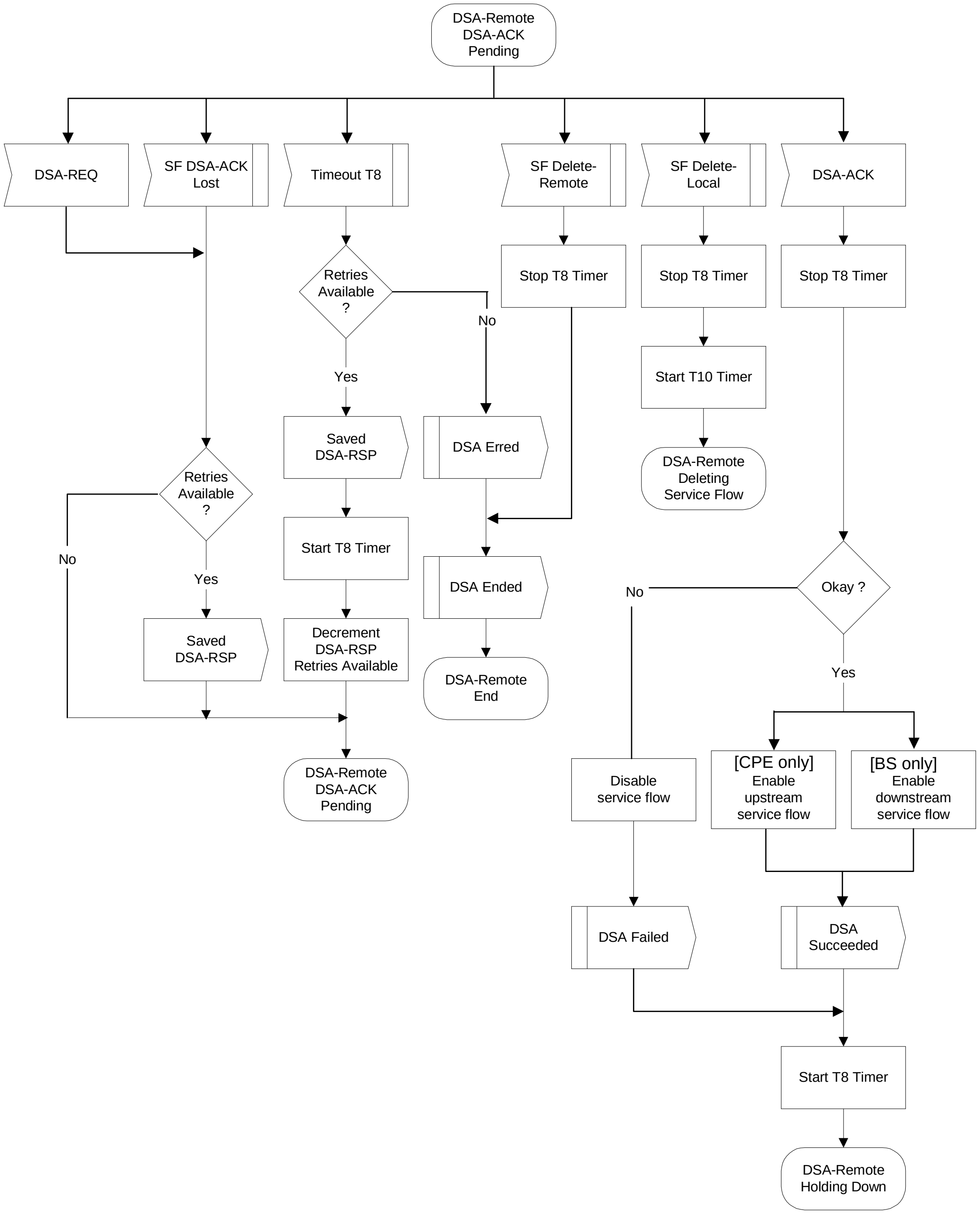


Figure 83—DSA - Remotely Initiated Transaction DSA-ACK Pending State Flow Diagram

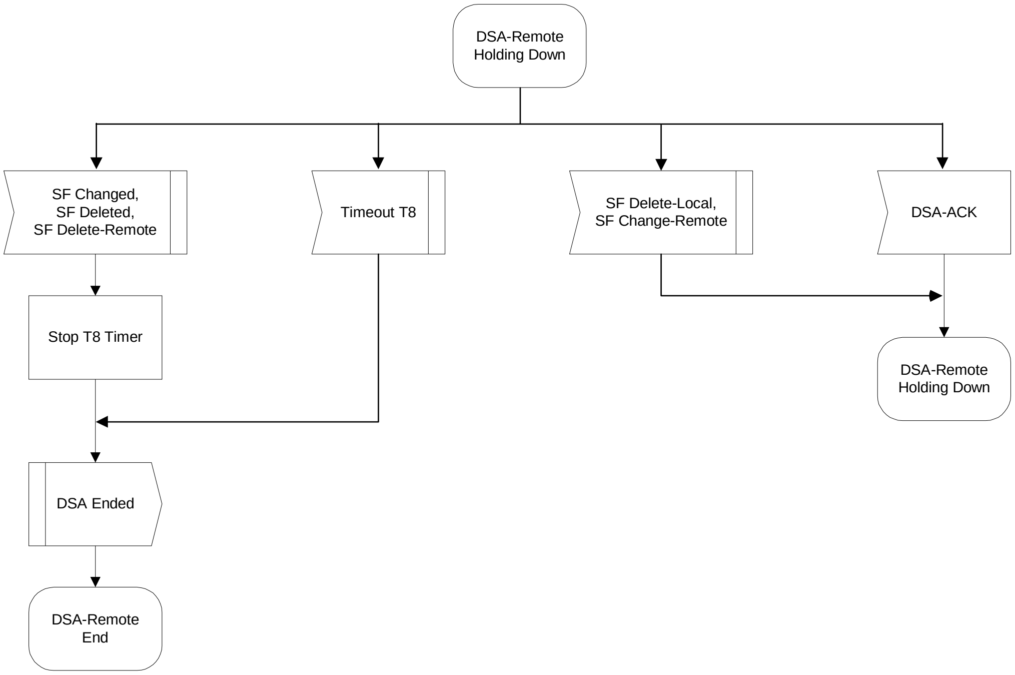


Figure 84—DSA - Remotely Initiated Transaction Holding Down State Flow Diagram

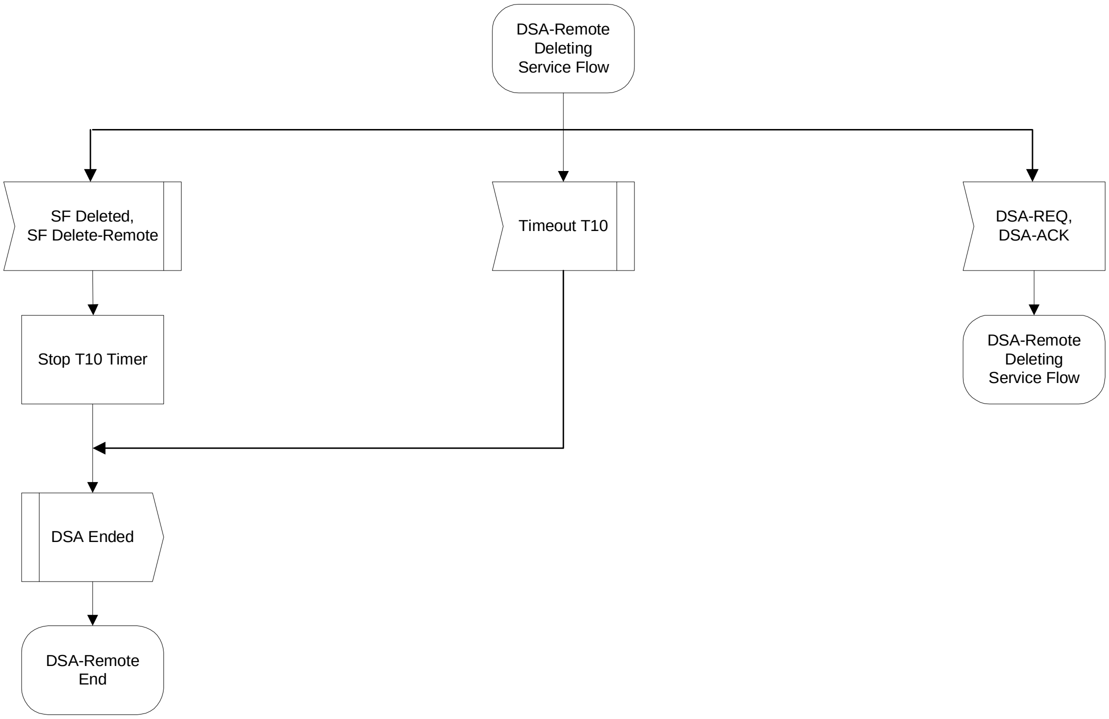

DSA-Remote Deleting Service Flow
SF Deleted, SF Delete-Remote
Timeout T10
DSA-REQ, DSA-ACK
Stop T10 Timer
DSA-Remote Deleting Service Flow
DSA Ended
DSA-Remote End

Figure 85—DSA - Remotely Initiated Transaction Deleting Service State Flow Diagram

6.10.8.4 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 modify the Service Flow Specification.

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.

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 shall 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 shall be maintained until the Service Flow is reactivated.

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

A BS shall have only one DSC transaction outstanding per Service Flow. If it detects a second transaction initiated by the CPE, the BS shall 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.

6.10.8.4.1 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 shall decide if the referenced Service Flow can support this modification. The BS shall respond with a Dynamic

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

BS		CPE
		Service Flow Requires Modifying
Receive DSC-REQ	<--------- DSC-REQ ----------	Send DSC-REQ
Validate Request		
Modify Service Flow		
Increase Channel Bandwidth if Required		
Send DSC-RSP	---------- DSC-RSP --------->	Receive DSC-RSP
		Modify Service Flow
		Adjust Payload Bandwidth
Receive DSC-ACK	<--------- DSC-ACK ----------	Send DSC-ACK
Decrease Channel Bandwidth if Required		

Table 23—CPE-Initiated DSC

6.10.8.4.2 BS-Initiated Dynamic Service Change

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

The BS shall 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 shall respond using a Dynamic Service Change Response (DSC-RSP) indicating acceptance or rejection. The BS reconfigures the Service Flow if appropriate, and then shall respond with a Dynamic Service Change Acknowledgment (DSC-ACK)

BS		CPE
Service Flow Requires Modifying		
Send DSC-REQ	---------- DSC-REQ --------->	Receive DSC-REQ
		Modify Service Flow
		Decrease Payload Bandwidth if Required
Receive DSC-RSP	<--------- DSC-RSP ----------	Send DSC-RSP
Modify Service Flow		
Adjust Channel Bandwidth		
Send DSC-ACK	---------- DSC-ACK --------->	Receive DSC-ACK
		Increase Payload Bandwidth if Required

Table 24—BS-Initiated DSC

6.10.8.4.3 Dynamic Service Change State Transition Diagrams

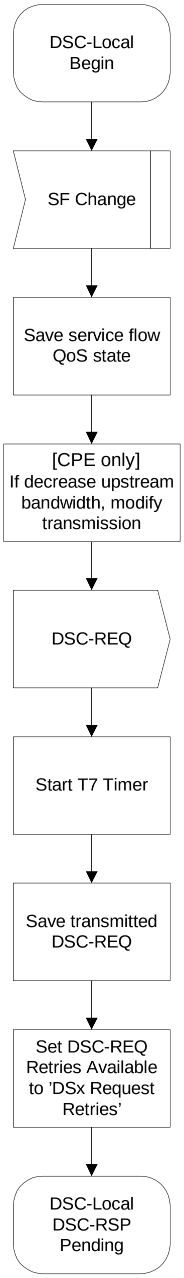


Figure 86—DSC - Locally Initiated Transaction Begin State Flow Diagram

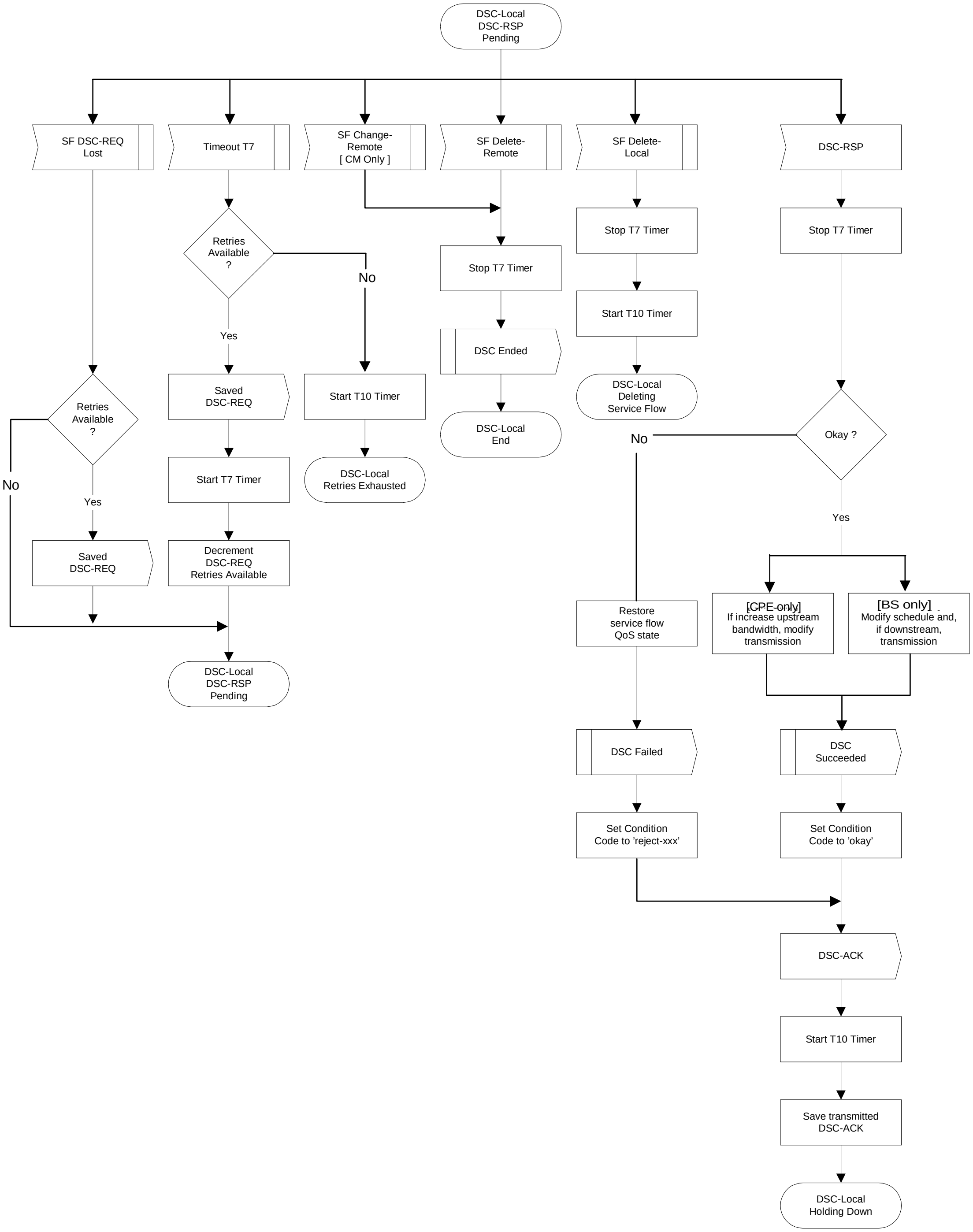


Figure 87—DSC - Locally Initiated Transaction DSC-RSP Pending State Flow Diagram

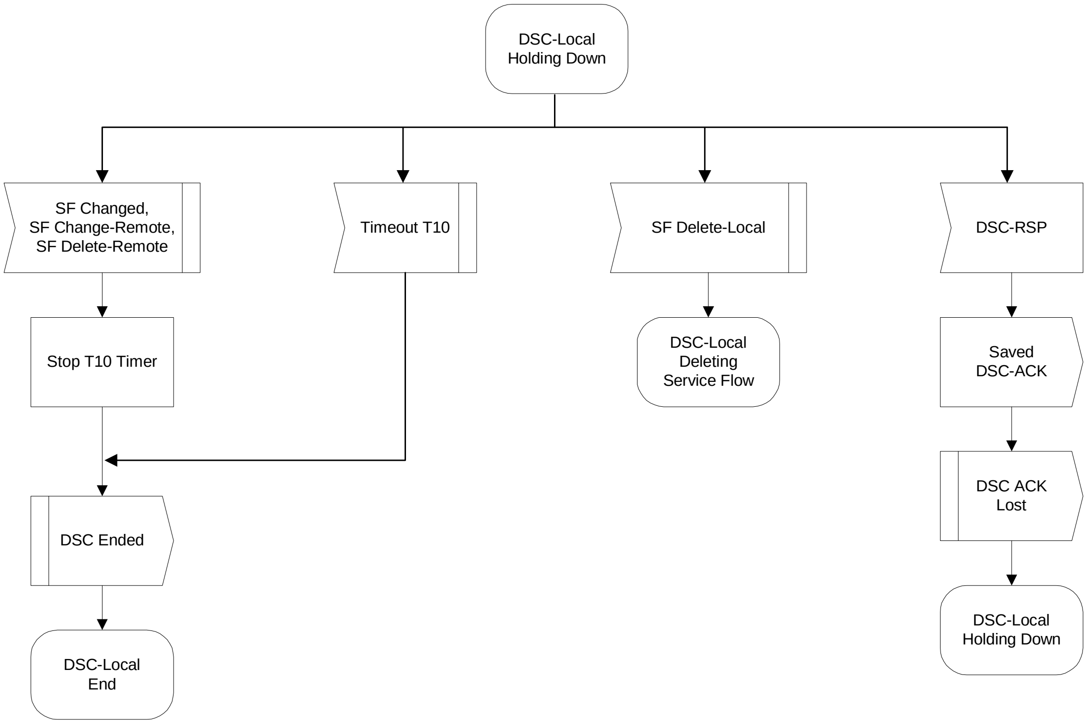


Figure 88—DSC - Locally Initiated Transaction Holding Down State Flow Diagram

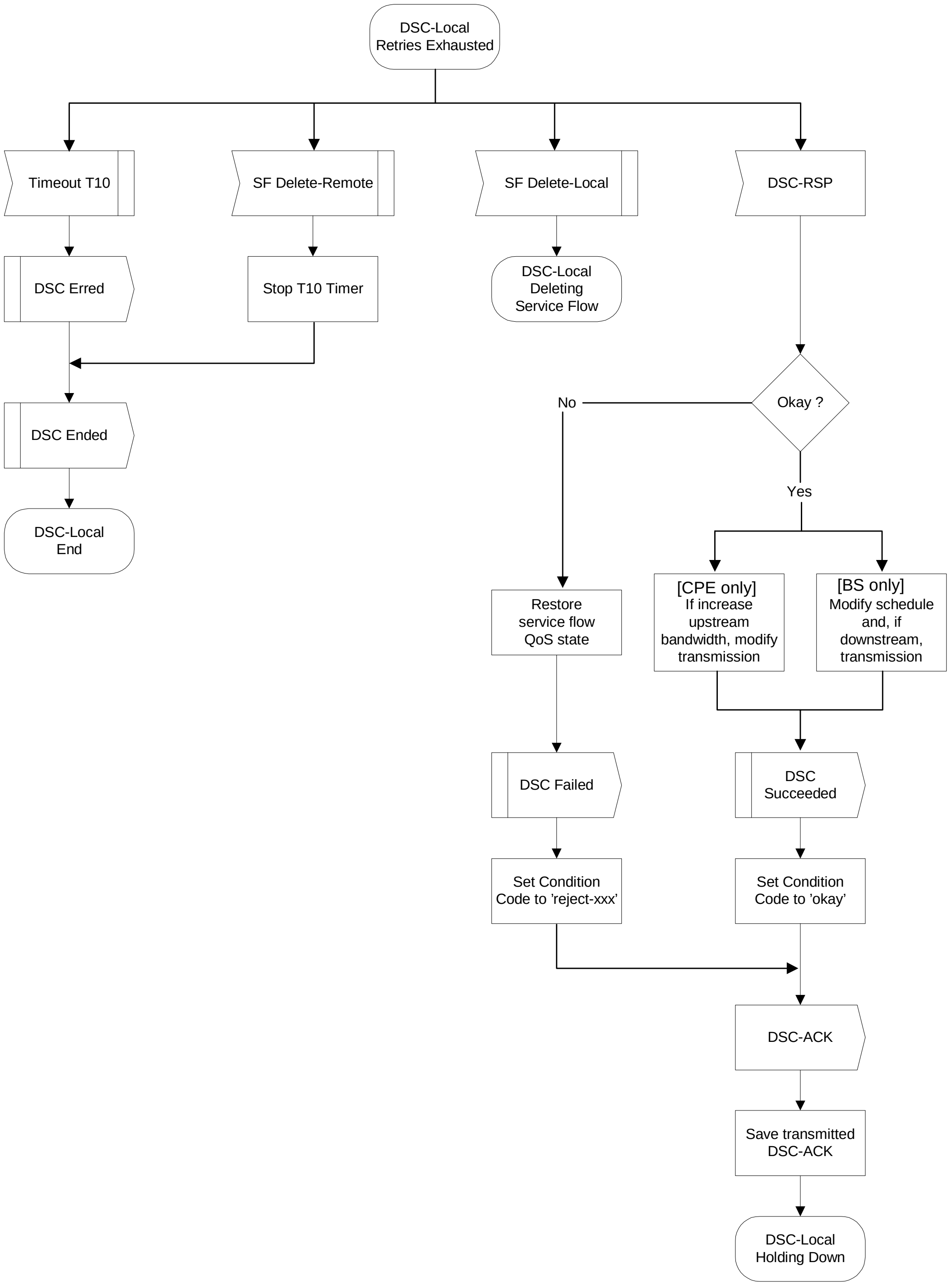

DSC-Local Retries Exhausted
Timeout T10
SF Delete-Remote
SF Delete-Local
DSC-RSP
DSC Erred
Stop T10 Timer
DSC-Local Deleting Service Flow
Okay ?
No
Yes
DSC Ended
DSC-Local End
Restore service flow QoS state
[CPE only] If increase upstream bandwidth, modify transmission
[BS only] Modify schedule and, if downstream, transmission
DSC Failed
DSC Succeeded
Set Condition Code to 'reject-xxx'
Set Condition Code to 'okay'
DSC-ACK
Save transmitted DSC-ACK
DSC-Local Holding Down

Figure 89—DSC - Locally Initiated Transaction Retries Exhausted State Flow Diagram

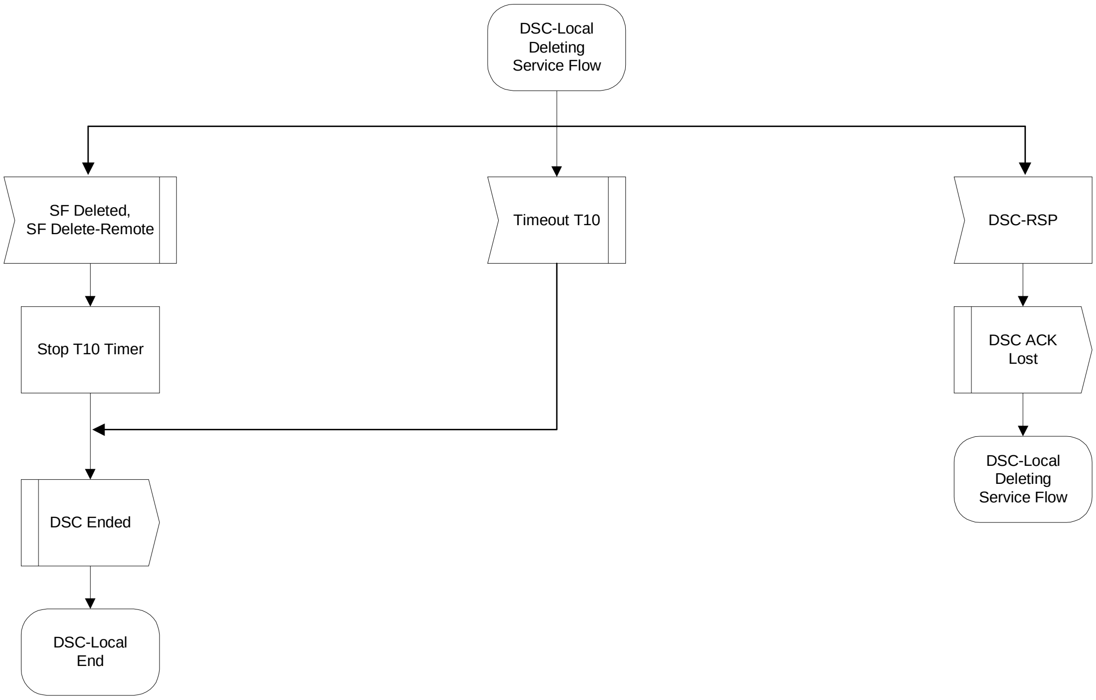


Figure 90—DSC - Locally Initiated Transaction Deleting Service Flow State Flow Diagram

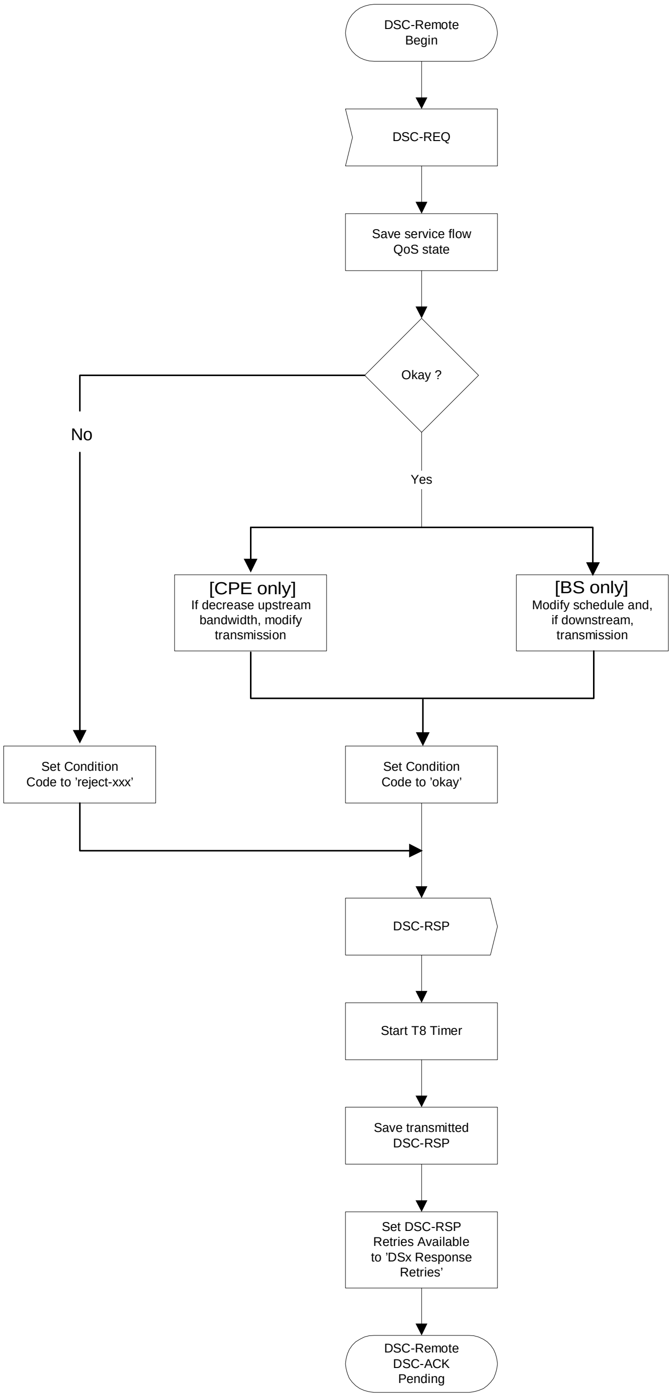


Figure 91—DSC - Remotely Initiated Transaction Begin State Flow Diagram

\

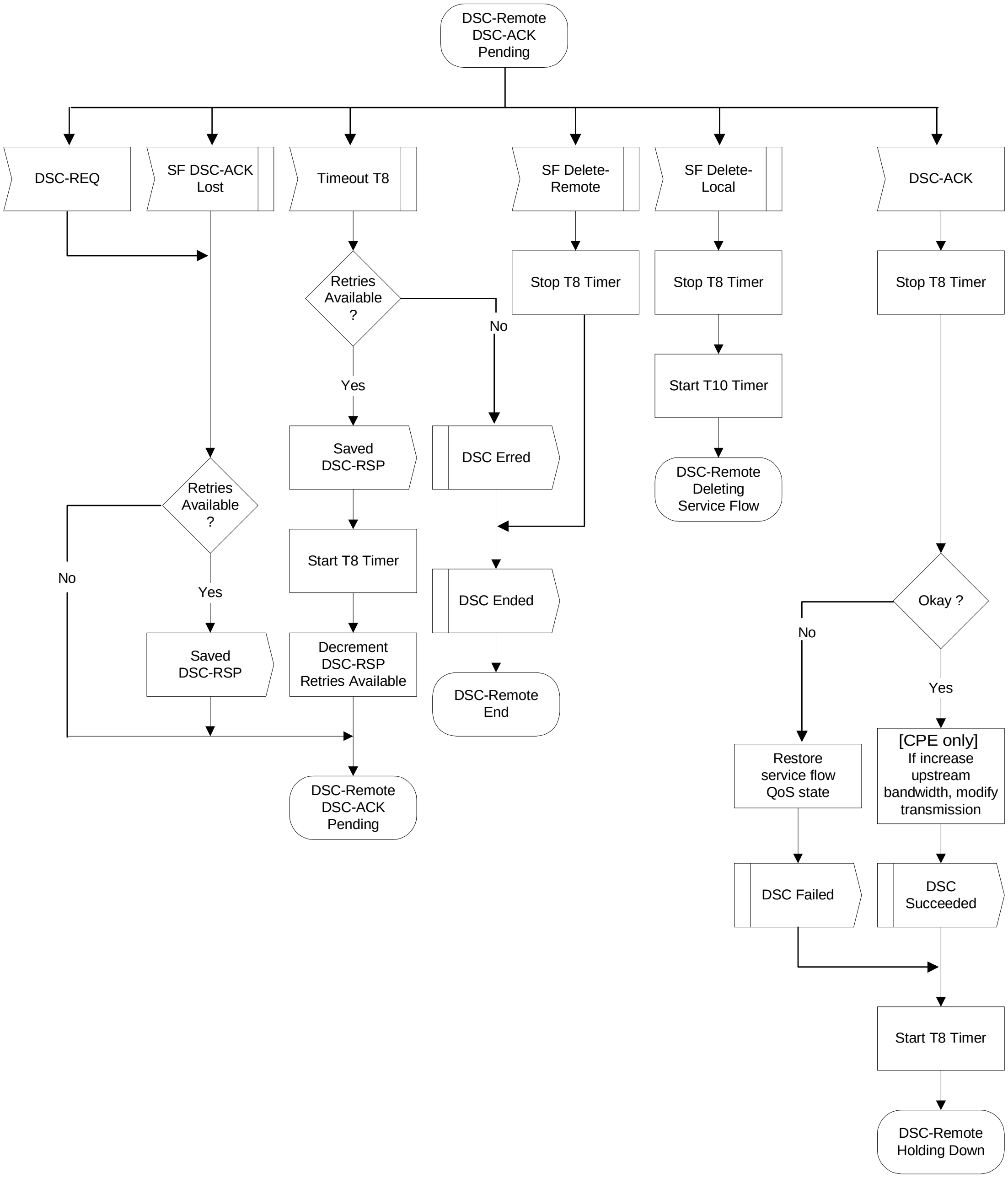


Figure 92—DSC - Remotely Initiated Transaction DSC-ACK Pending State Flow Diagram

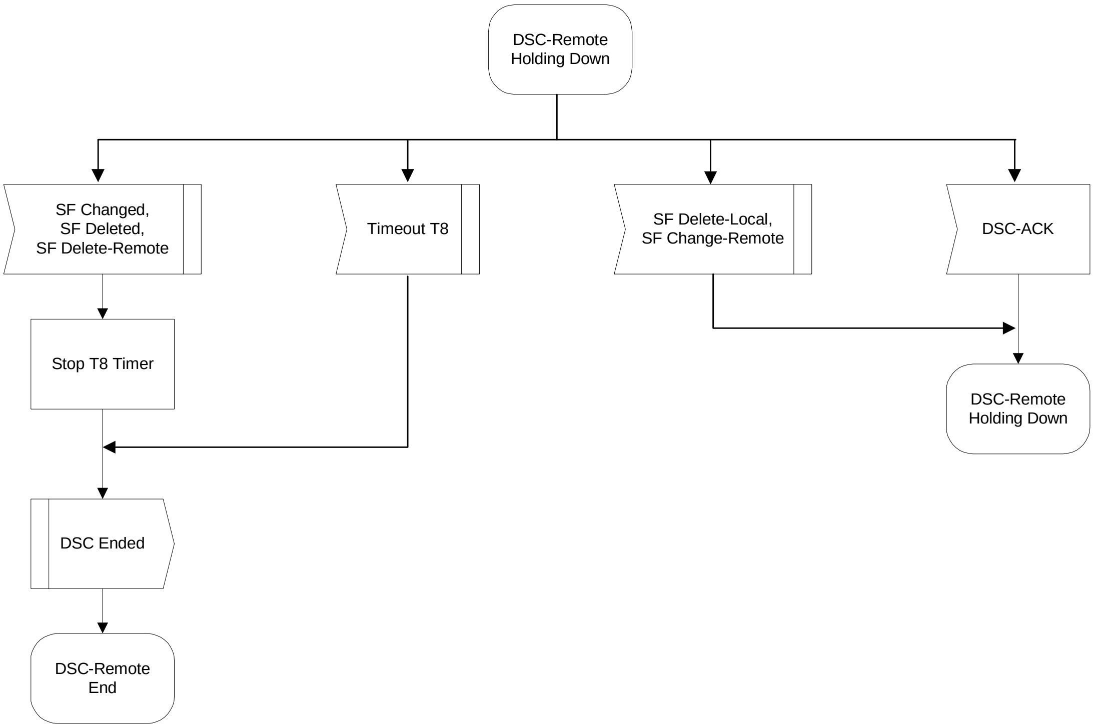


Figure 93—DSC - Remotely Initiated Transaction Holding Down State Flow Diagram

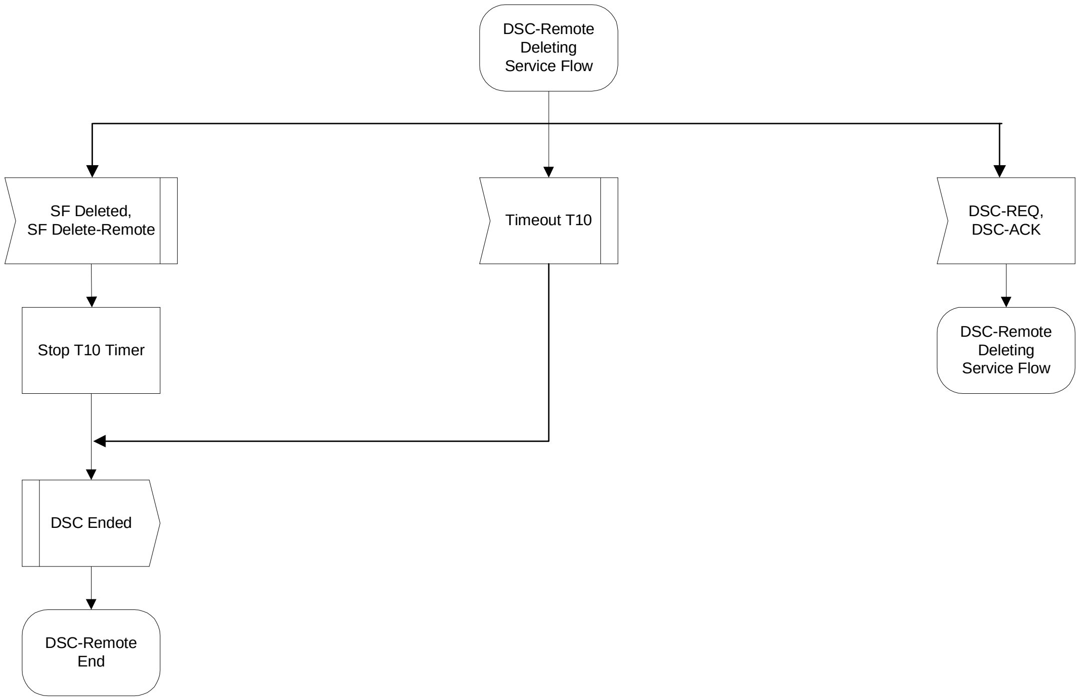

DSC-Remote Deleting Service Flow
SF Deleted, SF Delete-Remote
Timeout T10
DSC-REQ, DSC-ACK
Stop T10 Timer
DSC-Remote Deleting Service Flow
DSC Ended
DSC-Remote End

Figure 94—DSC - Remotely Initiated Transaction Deleting Service Flow State Flow Diagram

6.10.8.5 Connection Release

Any service flow can be deleted with the Dynamic Service Deletion (DSD) Messages. When a Service Flow is deleted, all resources associated with it are released. However, if a Basic Service Flow of a CPE is deleted, that CPE is de-registered and shall re-register. Also, if a Service Flow that was provisioned during registration is deleted, the provisioning information for that Service Flow is lost until the CPE re-registers. However, the deletion of a provisioned Service Flow shall not cause a CPE to re-register. Therefore, care should be taken before deleting such Service Flows.

Note: Unlike DSA and DSC Messages, DSD Messages are limited to only a single Service Flow.

6.10.8.5.1 CPE Initiated Dynamic Service Deletion

A CPE wishing to delete a Service Flow generates a delete request to the BS using a Dynamic Service Deletion-Request Message (DSD-REQ). The BS 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		
Send DSD-REQ	---DSD-REQ-->	Receive DSD-REQ

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

Table 25—Dynamic Service Deletion Initiated from CPE

6.10.8.5.2 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 26—Dynamic Service Deletion Initiated from BS

6.10.8.5.3 Dynamic Service Deletion State Transition Diagrams

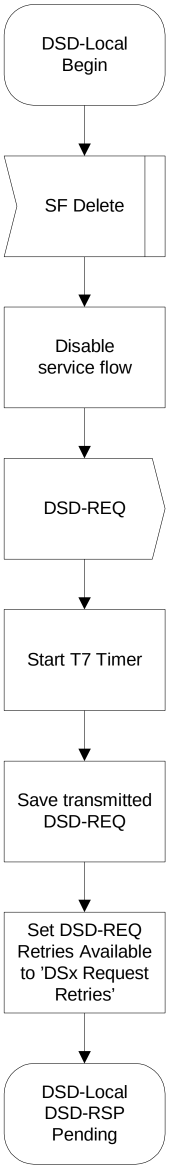


Figure 95—DSD - Locally Initiated Transaction Begin State Flow Diagram

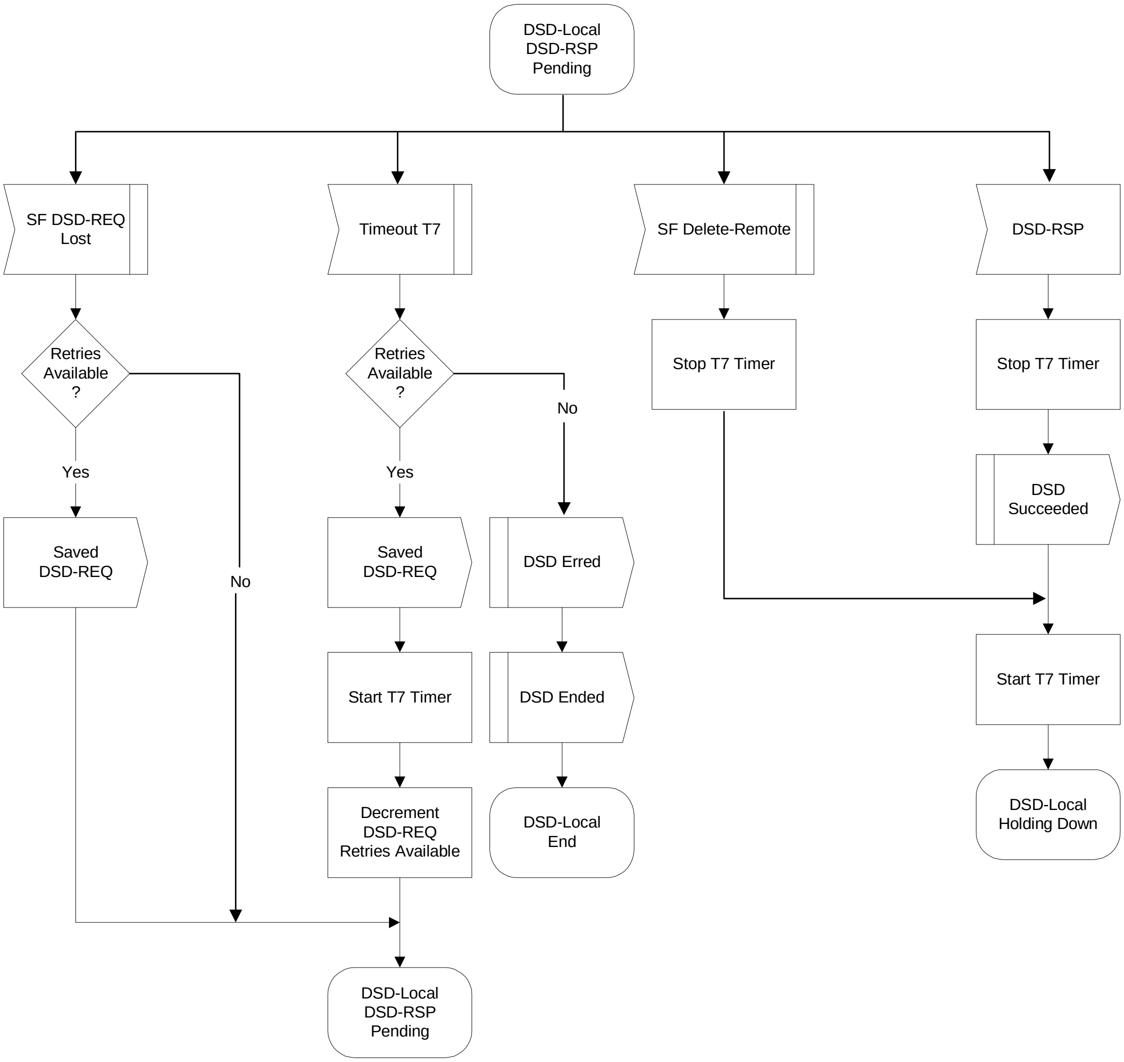


Figure 96—DSD - Locally Initiated Transaction DSD-RSP Pending State Flow Diagram

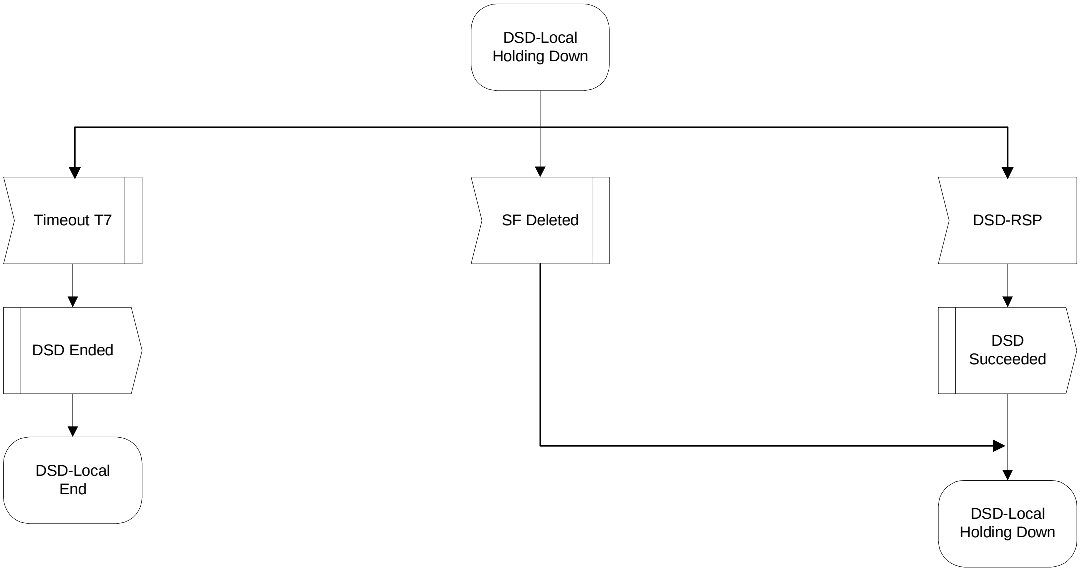


Figure 97—DSD - Locally Initiated Transaction Holding Down State Flow Diagram

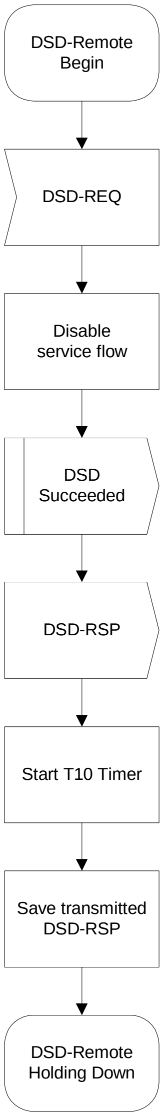


Figure 98—DSD - Remotely Initiated Transaction Begin State Flow Diagram

6.11 Parameters and Constants

Table 27—Parameters and Constants

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
BS	Sync Interval	Nominal time between transmission of SYNC messages			200 msec
BS	UCD Interval	Time between transmission of UCD messages			2 sec
BS	Max MAP Pending	The number of mini-slots that a BS is allowed to map into the future)			4096 mini-slot times
BS	Ranging Interval	Time between transmission of broadcast Ranging requests			2 sec
CPE	Lost DS-MAP 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	16		
CPE, BS	Invited Ranging Retries	Number of Retries on inviting Ranging Requests	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 UL-MAP processing time	Time provided between arrival of the last bit of a UL-MAP at a CPE and effectiveness of that MAP	200 us		
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		
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		

Table 27—Parameters and Constants

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
CPE	T1	Wait for PCD timeout			5 * PCD 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	¼ Symbol		
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

Table 27—Parameters and Constants

System	Name	Time Reference	Minimum Value	Default Value	Maximum Value
CPE, 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 backoff	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 shall be used in both the configuration file (see Section 6.13), 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 shall 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, shall 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 shall be a multiple of 1000 Hz.

6.12.1.2 Upstream Channel ID Configuration Setting

The upstream channel ID which the CPE shall use. The CPE shall 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, Subscriber Equipment 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 shall not forward traffic from attached Subscriber Equipment to the MAC network, but shall 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 Subscriber equipment onto the BWA network. (A Subscriber 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.
- ICPEP: 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 Subcribers 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 shall be enforced by the CPE.

Type	Length	Value
18	1	

If present, the value shall 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 CPE Address

The IP Address of the CPE 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, shall 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 shall 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 shall 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 shall 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 6.12.1.9.

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

someTabledisallow write-access
someTable.1.3allow 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 shall treat this object as if it were part of an SNMP Set Request with the following caveats:

a) It shall treat the request as fully authorized (it cannot refuse the request for lack of privilege).
b) SNMP Write-Control provisions (see previous section) do not apply.
c) 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 shall be treated as if simultaneous.

Each VarBind shall 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 Section 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 shall include Modem Capabilities Encodings in its Registration Request. If present in the corresponding Registration Request, the BS shall 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 shall 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 shall 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 #3-7: 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 shall be used in a Registration Request, but shall 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 shall 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 shall 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 6.12.7.

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 shall 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 Section 7.

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.

The Authorization Block may be present in CPE-initiated DSA-REQ and DSC-REQ messages. This parameter shall 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, shall 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 shall 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 shall 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 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 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 shall 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 shall not contain this parameter.

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

6.12.5.3.3 Connection Identifier

The value of this field specifies the Connection 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 shall be present in BS-initiated DSA-REQ or DSC-REQ message related to establishing an admitted or active upstream Service Flow. This field shall 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 Connection ID) the Service Flow ID shall 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 Connection ID may be reassigned by the BS.

SubType	Length	Value
[24/25].3	2	CID

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 shall 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 shall 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 shall 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 shall be included for only the rejected Service Flow.

On success of the entire transaction, the RSP or ACK message shall 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 shall not contain any QoS Parameters.

A Service Flow Error Parameter Set shall 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 shall 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 6.12.7. A Service Flow Error Parameter Set shall 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 shall 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 shall appear zero or one times per Service Flow Encoding.

6.12.5.5.1 Quality of Service Parameter Set Type

This parameter shall 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 diferent. Bit 0 is the LSB of the Value field.

For every Service Flow that appears in a Registration-Request or Registration-Response message, there shall 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 28—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 29—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

Value	Messages
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 shall 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 shall reply with error code 2, reject-unrecognized-configuration-setting.

6.12.5.5.2 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 shall 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 6.12.5.6.3).

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

Note: The default priority is 0.

6.12.5.5.3 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[1]. The number of bytes forwarded-(in bytes) is limited during any time interval T by Max(T), as described in the expression

Max(T) = T * (R / 8) + B, (1)

where the parameter B (in bytes) is the Maximum Traffic Burst Configuration Setting (refer to 6.12.5.5.5).

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.

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.

[1] The payload size includes every PDU in a Concatenated MAC Frame.

6.12.5.5.4 Upstream Maximum Sustained Traffic Rate

For an upstream Service Flow, the CPE shall 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 shall 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 shall 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 shall report this condition to a policy module. If the BS is policing by discarding either packets or requests, the BS shall 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 shall enforce expression (1) on all downstream data transmissions. The BS shall not forward downstream packets that violates (1) in any interval T. The BS SHOULD “rate shape” the downstream traffic by enqueuing 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)

6.12.5.5.5 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[2].

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 6.12.5.6.1).

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.

6.12.5.5.6 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 the excess reserved bandwidth for other purposes. The aggregate Minimum Reserved Traffic Rate of all

[2] The payload size includes every PDU in a Concatenated MAC Frame.

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[3]. 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 shall 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.

6.12.5.5.7 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[4]. 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 shall 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	

6.12.5.5.8 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 shall change the active and admitted QoS Parameter Sets to null. The BS shall signal this resource change with a DSC-REQ to the CPE.

If defined, this parameter shall 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 shall not be timed out due to inactivity. The default value is 0.

6.12.5.5.9 Timeout for Admitted QoS Parameters

The value of this parameter specifies the duration that the BS shall 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

[3] The payload size includes every PDU in a Concatenated MAC Frame.

[4] The payload size includes every PDU in a Concatenated MAC Frame.

but not activated shall be released, and only the active resources retained. The BS shall 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 shall not be timed out due to inactivity. However, this is subject to policy control by the BS.

This parameter shall 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

6.12.5.5.10 Vendor Specific QoS Parameters

This allows vendors to encode vendor-specific QoS parameters. The Vendor ID shall 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	

6.12.5.6 Upstream-Specific QoS Parameter Encodings

6.12.5.6.1 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 shall 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.

6.12.5.6.2 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 shall be assumed.

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

Type	Length	Value
24.15	1	0 Reserved
		1 for Undefined (BS implementation-dependent[5])
		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

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

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

[5] The specific implementation dependent scheduling service type could be defined in the 24.43 Vendor Specific Information Field.

[6] 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 shall be ignored

[7] 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.

6.12.5.6.4 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 $t_i = t_0 + i*interval$. The actual poll times, t'_i shall be in the range $t_i <= t'_i <= t_i + jitter$, 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 shall be enforced by the BS.

Type	Length	Value
24.17	4	µsec

6.12.5.6.5 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 $t_i = t_0 + i*interval$. The actual poll, t'_i shall be in the range $t_i <= t'_i <= t_i + jitter$, 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	µsec

6.12.5.6.6 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 shall 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.

6.12.5.6.7 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 $t_i = t_0 + i*interval$. The actual grant times, t'_i shall be in the range $t_i <= t'_i <= t_i + jitter$, 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 shall define the start of this interval, i.e. the first grant shall be for an ideal transmission time, t_i. When multiple grants per interval are requested, all grants shall be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter shall 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 shall be enforced by the BS.

Type	Length	Value
24.20	4	µsec

6.12.5.6.8 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 $t_i = t_0 + i*interval$. The actual transmission opportunities, t'_i shall be in the range $t_i <= t'_i <= t_i + jitter$, 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 shall be enforced by the BS.

Type	Length	Value
24.21	4	µsec

6.12.5.6.9 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 $t_i = t_0 + i*interval$. The actual grant times, t'_i shall be in the range $t_i <= t'_i <= t_i + jitter$, where interval is the Nominal Grant Interval, and jitter is the Tolerated Grant Jitter. When multiple grants per interval are requested, all grants shall be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter shall 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 shall be enforced by the BS.

Type	Length	Value	Valid Range
24.22	1	# of grants	0-127

6.12.5.7 Downstream-Specific QoS Parameter Encodings

6.12.5.7.1 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 shall 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

6.12.6 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	

6.12.7 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)

6.12.8 Convergence Sub-Layer Parameter Encodings

Configuration files will contain parameter information used by the convergence sub-layers. Each convergence sub-layer defines a set of TLV parameters that are encoded as a set of TLVs within a subindex under the type value 99. For example, convergence sub-layer “a” would define a set of TLVs using the subtype index of 99.1. Convergence sub-layer “b” would define a set of TLVs using a subtype index of 99.2, etc.

Type	Length	Value
99	n	TLV Subindex

6.13 Configuration File

6.13.1 CPE IP Addressing

6.13.1.1 DHCP Fields Used by the CPE

The following fields shall be present in the DHCP request from the CPE and shall be set as described below:

a) The hardware type (htype) shall be set to 1 (Ethernet).
b) The hardware length (hlen) shall be set to 6.
c) The client hardware address (chaddr) shall be set to the 48 bit MAC address associated with the RF interface of the CPE.
d) The “client identifier” option shall be included, with the hardware type set to 1, and the value set to the same 48 bit MAC address as the chaddr field.
e) The “parameter request list” option shall be included. The option codes that shall be included in the list are:
    1) Option code 1 (Subnet Mask)
    2) Option code 2 (Time Offset)
    3) Option code 3 (Router Option)
    4) Option code 4 (Time Server Option)
    5) Option code 7 (Log Server Option)
    6) Option code 60 (Vendor Specific Option) — A compliant CPE shall send the following ASCII coded string in Option code 60, “802.16.1:xxxxxxx”. Where xxxxx shall be the hexidecimal encoding of the Modem Capabilities, refer to Section 6.12.3.1.

The following fields are expected in the DHCP response returned to the CPE. The CPE shall configure itself based on the DHCP response.

a) The IP address to be used by the CPE (yiaddr).
b) The IP address of the TFTP server for use in the next phase of the bootstrap process (siaddr).
c) If the DHCP server is on a different network (requiring a relay agent), then the IP address of the relay agent (giaddr). Note: this may differ from the IP address of the first hop router.
d) The name of the CPE configuration file to be read from the TFTP server by the CPE (file).
e) The subnet mask to be used by the CPE (Subnet Mask, option 1).
f) The time offset of the CPE from Universal Coordinated Time (UTC) (Time Offset, option 2). This is used by the CPE to calculate the local time for use in time-stamping error logs.
g) A list of addresses of one or more routers to be used for forwarding CPE-originated IP traffic (Router Option, option 3). The CPE is not required to use more than one router IP address for forwarding.
h) A list of [RFC-868] time-servers from which the current time may be obtained (Time Server Option, option4).
i) A list of SYSLOG servers to which logging information may be sent (Log Server Option, option 7).

6.13.2 CPE Configuration

6.13.2.1 CPE Binary Configuration File Format

The CPE-specific configuration data shall be contained in a file which is downloaded to the CPE via TFTP. This is a binary file in the same format defined for DHCP vendor extension data [RFC-2132].

It shall consist of a number of configuration settings (1 per parameter) each of the form

Type Length Value

Where

Type is a single-octet identifier which defines the parameter

Length is a single octet containing the length of the value field in octets (not including type and length fields)

Value is from one to 254 octets containing the specific value for the parameter

The configuration settings shall follow each other directly in the file, which is a stream of octets (no record markers).

Configuration settings are divided into three types:

a) Standard configuration settings which shall be present
b) Standard configuration settings which may be present
c) Vendor-specific configuration settings.

CPEs shall be capable of processing all standard configuration settings. CPEs shall ignore any configuration setting present in the configuration file which it cannot interpret. To allow uniform management of CPE's conformant to this specification, conformant CPE's shall support a 8192-byte configuration file at a minimum.

Authentication of the provisioning information is provided by two message integrity check (MIC) configuration settings, CPE MIC and BS MIC.

a) CPE MIC is a digest which ensures that the data sent from the provisioning server were not modified en route. This is not an authenticated digest (it does not include any shared secret).
b) BS MIC is a digest used to authenticate the provisioning server to the BS during registration. It is taken over a number of fields one of which is a shared secret between the BS and the provisioning server.

Use of the CPE MIC allows the BS to authenticate the provisioning data without needing to receive the entire file.

Thus the file structure is of the form shown in Figure 99:

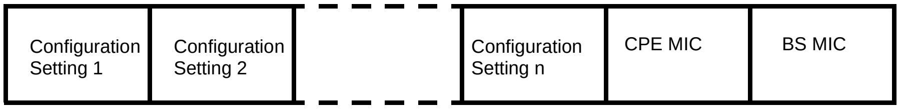


Figure 99—Binary Configuration File Format

6.13.2.2 Configuration File Settings

The following configuration settings shall be included in the configuration file and shall be supported by all CPEs.

a) Network Access Configuration Setting
b) CPE MIC Configuration Setting
c) BS MIC Configuration Setting
d) End Configuration Setting
e) Upstream Service Flow Configuration Setting
f) Downstream Service Flow Configuration Setting

The following configuration settings shall be included in the configuration file and shall be supported by all CPEs that support the specific Convergence Sub-layer:

a) Convergence Sub-layer Configuration Setting(s)

The following configuration settings may be included in the configuration file and if present shall be supported by all CPEs.

a) Downstream Frequency Configuration Setting
b) Upstream Channel ID Configuration Setting
c) Privacy Configuration Setting
d) Software Upgrade Filename Configuration Setting
e) SNMP Write-Access Control
f) SNMP MIB Object
g) Software Server IP Address
h) CPE Ethernet MAC Address
i) Maximum Number of CPEs
j) Privacy Enable Configuration Setting
k) Payload Header Suppression
l) TFTP Server Timestamp
m) TFTP Server Provisioned Modem Address
n) Pad Configuration Setting

The following configuration settings may be included in the configuration file and if present may be supported by a CPE.

- Vendor-Specific Configuration Settings

Note: There is a limit on the size of registration request and registration response frames (see section 6.2.5.2). The configuration file shall not cause the CPE to BS to exceed that limit.

6.13.2.3 Configuration File Creation

The sequence of operations required to create the configuration file is as shown in Figure 100 through Figure 103.

1) Create the type/length/value entries for all the parameters required by the CPE.

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter n

Figure 100—Create TLV Entries for Parameters Required by the CPE

2) Calculate the CPE message integrity check (MIC) configuration setting as defined in Section 6.13.2.3.1 and add to the file following the last parameter using code and length values defined for this field.

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter n
type, length, value for CPE MIC

Figure 101—Add CPE MIC

3) Calculate the BS message integrity check (MIC) configuration setting as defined in Section 6.13.3.1 and add to the file following the CPE MIC using code and length values defined for this field.
4)

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter n
type, length, value for CPE MIC
type, length, value for BS MIC

Figure 102—Add BS MIC

5) Add the end of data marker.

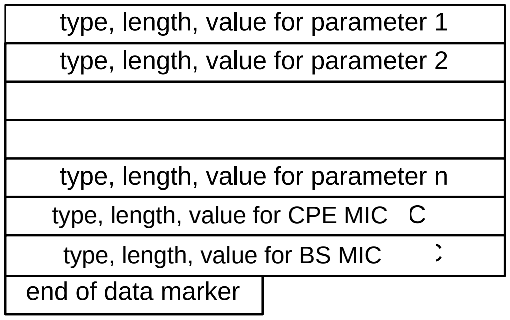

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter n
type, length, value for CPE MIC C
type, length, value for BS MIC
end of data marker

Figure 103—Add End of Data Marker

6.13.2.3.1 CPE MIC Calculation

The CPE message integrity check configuration setting shall be calculated by performing an MD5 digest over the bytes of the configuration setting fields. It is calculated over the bytes of these settings as they appear in the TFTPed image, without regard to TLV ordering or contents. There are two exceptions to this disregard of the contents of the TFTPed image:

1) The bytes of the CPE MIC TLV itself are omitted from the calculation. This includes the type, length, and value fields.
2) The bytes of the BS MIC TLV are omitted from the calculation. This includes the type, length, and value fields.

On receipt of a configuration file, the CPE shall recompute the digest and compare it to the CPE MIC configuration setting in the file. If the digests do not match then the configuration file shall be discarded

6.13.3 Configuration Verification

It is necessary to verify that the CPE's configuration file has come from a trusted source. Thus, the BS and the configuration server share an Authentication String that they use to verify portions of the CPE's configuration in the Registration Request.

6.13.3.1 BS MIC Calculation

The BS message integrity check configuration setting shall be calculated by performing an MD5 digest over the following configuration setting fields, when present in the configuration file, in the order shown:

a) Downstream Frequency Configuration Setting
b) Upstream Channel ID Configuration Setting
c) Network Access Configuration Setting
d) Privacy Configuration Setting
e) Vendor-Specific Configuration Settings
f) CPE MIC Configuration Setting
g) Maximum Number of CPEs
h) TFTP Server Timestamp
i) TFTP Server Provisioned Modem Address
j) Upstream Service Flow Configuration Setting
k) Downstream Service Flow Configuration Setting
l) Privacy Enable Configuration Setting

The bulleted list specifies the order of operations when calculating the BS MIC over configuration setting Type fields. The BS shall calculate the BS MIC over TLVs of the same Type in the order they were received. Within Type fields, the BS shall calculate the BS MIC over the Subtypes in the order they were received. To allow for correct BS MIC calculation by the BS, the CPE shall not reorder configuration file TLVs of the same Type or Subtypes within any given Type in its Registration-Request message.

All configuration setting fields shall be treated as if they were contiguous data when calculating the CPE MIC.

The digest shall be added to the configuration file as its own configuration setting field using the BS MIC Configuration Setting encoding.

The authentication string is a shared secret between the provisioning server (which creates the configuration files) and the BS. It allows the BS to authenticate the CPE provisioning. The authentication string is to be used as the key for calculating the keyed BS MIC digest as stated in D.3.1.1.

The mechanism by which the shared secret is managed is up to the system operator.

On receipt of a configuration file, the CPE shall forward the BS MIC as part of the registration request (REG-REQ).

On receipt of a REG-REQ, the BS shall recompute the digest over the included fields and the authentication string and compare it to the BS MIC configuration setting in the file. If the digests do not match, the registration request shall be rejected by setting the authentication failure result in the registration response status field.

6.13.3.1.1 Digest Calculation

The BS MIC digest field shall be calculated using HMAC-MD5 as defined in [RFC-2104].

7. Authentication and Privacy

7.1 Privacy Plus Overview

Privacy provides subscribers with privacy across the fixed broadband wireless network. It does this by encrypting connectionss between CPE and BS.

In addition, Privacy provides operators with strong protection from theft of service. The BS protects against unauthorized access to these data transport services by enforcing encryption of the associated traffic flows across the network. Privacy employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to client CPE. Additionally, the basic privacy mechanisms are strengthened by adding digital-certificate based CPE authentication to its key management protocol.

7.1.1 Architectural Overview

Privacy has two component protocols:

a) An encapsulation protocol for encrypting packet data across the fixed broadband wireless access network. This protocol defines (1) a set of supported *cryptographic suites*, i.e., pairings of data encryption and authentication algorithms, and (2) the rules for applying those algorithms to a MAC header's payload.

b) A key management protocol (Privacy Key Management, or "PKM") providing the secure distribution of keying data from BS to CPE. Through this key management protocol, CPE and BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

7.1.1.1 Packet Data Encryption

Encryption services are defined as a set of capabilities within the MAC sublayer. MAC Header information specific to encryption is allocated in the Generic MAC Header Formant.

This specification supports a single packet date encryption algorithm: the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46-1] [FIPS-81]. It does not pair DES CBC with any packet data authentication algorithm. Additional data encryption algorithms may be supported in future enhancements to the protocol specification, and these algorithms may be paired with data authentication algorithms.

Encryption is always applied to the MAC PDU payload; the Generic MAC Header is not encrypted. All MAC management messages shall be sent in the clear to facilitate registration, ranging, and normal operation of the MAC sublayer.

Section 7.2 specifies the format of MAC PDUs carrying encrypted packet data payloads.

7.1.1.2 Key Management Protocol

CPE use the Privacy Key Management protocol to obtain authorization and traffic keying material from the BS, and to support periodic reauthorization and key refresh. The key management protocol uses X.509 digital certificates [ITU1], RSA [RSA, RSA1, RSA3] (a public-key encryption algorithm) and two-key triple DES to secure key exchanges between CPE and BS.

The Privacy Key Management protocol adheres to a client/server model, where the CPE, a PKM "client", requests keying material, and the BS, a PKM "server", responds to those requests, ensuring individual CPE clients only receive keying material they are authorized for. The PKM protocol uses MAC management messaging.

Privacy uses public-key cryptography to establish a shared secret (i.e., an Authorization Key) between CPE and BS. The shared secret is then used to secure subsequent PKM exchanges of traffic encryption keys. This two-tiered mechanism for key distribution permits refreshing of traffic encryption keys without incurring the overhead of computation-intensive public-key operations.

A BS authenticates a client CPE during the initial authorization exchange. Each CPE carries a unique X.509 digital certificate issued by the CPE's manufacturer. The digital certificate contains the CPE's Public Key along with other identifying information; i.e., CPE MAC address, manufacturer ID and serial number. When requesting an Authorization Key, a CPE presents it's digital certificate to a BS. The BS verifies the digital certificate, and then uses the verified Public Key to encrypt an Authorization Key, which the BS then sends back to the requesting CPE.

The BS associates a CPE's authenticated identity to a paying subscriber, and hence to the data services that subscriber is authorized to access. Thus, with the Authorization Key exchange, the BS establishes an authenticated identity of a client CPE, and the services (i.e., specific traffic encryption keys) the CPE is authorized to access.

Since the BS authenticates CPE, it can protect against an attacker employing a *cloned* CPE, masquerading as a legitimate subscriber's CPE. The use of the X.509 certificates prevents cloned CPEs from passing fake credentials onto a BS.

CPE shall have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If a CPE relies on an internal algorithm to generate its RSA key pair, the CPE shall generate the key pair prior to its first Privacy initialization, described in Section 7.1.2.1. CPE with factory-installed RSA key pairs shall also have factory-installed X.509 certificates. CPE that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer-issued X.509 certificate following key generation.

The PKM protocol is defined in detail in Section 7.5.

7.1.1.3 Security Associations

A *Security Association* (SA) is the set of security information a BS and one or more of its client CPE share in order to support secure communications across the BWA network. Three types of Security Associations are defined: *Primary*, *Static*, and *Dynamic*. A Primary Security Association is related to the Basic CID that every CPE establishes during registration. Static Security Associations are provisioned within the BS. Dynamic Security Associations are established and eliminated, on the fly, in response to the initiation and termination of specific traffic flows. Both Static and Dynamic SAs can by shared by multiple CPE.

A Security Association's shared information includes traffic encryption keys and CBC initialization vectors. In order to support, in future protocol enhancements, alternative data encryption and data authentication algorithms, Security Association parameters include a cryptographic suite identifier, indicating a the particular pairing of packet data encryption and packet data authentication algorithms employed by the security association. At the time of release of this specification, 56-bit DES is the only packet data encryption algorithms supported, and neither are paired with a PDU authentication algorithm.

Security Associations are identified using a SAID.

Each (Privacy enabled) CPE establishes an exclusive Primary Security Association with its BS. All of a CPE's upstream traffic, and typically all downstream unicast traffic directed at CPE device(s) behind the CPE, are encrypted under the CPE's exclusive, Primary Security Association. (Selected downstream unicast traffic flows may be encrypted under Static or Dynamic SAs.) The CID corresponding to a CPE’s Primary SA shall be equal to the CPE’s Basic CID. Downstream traffic may be encrypted under any of the three types of SAs. A downstream multicast PDU, however, is typically intended for multiple CPE and hence is more likely to be encrypted under Static or Dynamic SAs, which multiple CPE can access, as opposed to a Primary SA, which is restricted to a single CPE.

Using the PKM protocol, a CPE requests from its BS a SA’s keying material. The BS ensures that each client CPE only has access to the Security Associations it is authorized to access.

A SA's keying material (e.g., DES key and CBC Initialization Vector) has a limited lifetime. When the BS delivers SA keying material to a CPE, it also provides the CPE with that material's remaining lifetime. It is the responsibility of the CPE to request new keying material from the BS before the set of keying material that the CPE currently holds expires at the BS. The PKM protocol specifies how CPE and BS maintain key synchronization.

7.1.2 Operational Overview

7.1.2.1 CPE Initialization

CPE initialization is divided into the following sequence of tasks:

a) scan for downstream channel and establish synchronization with the BS
b) obtain transmit parameters
c) perform ranging
d) establish IP connectivity (DHCP)
e) establish time of day
f) transfer operational parameters (download parameter file via TFTP)
g) BS Registration

Privacy establishment follows BS registration.

If a CPE is to run Privacy, its parameter file, downloaded during the transfer of operational parameters, shall include Privacy Configuration Settings. These additional configuration settings are defined in <TBD>.

Upon completing BS registration, the BS will have assigned one or more static CIDs to the registering CPE that match the CPE’s static class-of-service provisioning. The first static CID assigned during the registration process is the Basic CID, and this CID will also serve as the CPE’s Privacy Basic SAID. If a CPE is configured to run Privacy, BS registration is immediately followed by initialization of the CPE’s Privacy security functions.

Privacy initialization begins with the CPE sending the BS an Authorization Request, containing:

a) data identifying the CPE (e.g., MAC address),
b) the CPE’s RSA public key,
c) an X.509 certificate verifying the binding between the CPE’s identifying data and the CPE’s public key,
d) a list of the CPE’s security capabilities (i.e., the particular pairings of encryption and authentication algorithms the CPE supports) and
e) the CPE’s Primary SAID.

If the BS determines the requesting CPE is authorized for the Authorization Request’s Basic SAID, the BS responds with an Authorization Reply containing an Authorization Key, from which CPE and BS derive the keys needed to secure a CPE’s subsequent requests for traffic encryption keys and the BS’s responses to these requests. The BS encrypts the Authorization Key with the receiving CPE’s public key.

The Authorization Reply also contains a list of security association descriptors, identifying the primary and static SAs the requesting CPE is authorized to access. Each SA descriptor consists of a collection of SA parameters, including the SA's SAID, type and cryptographic. The list contains at least one entry: a descriptor describing the CPE's primary security association. Additional entries are optional, and would describe any static SAs the CPE was provisioned to access.

After successfully completing authentication and authorization with the BS, the CPE sends key requests to the BS, requesting traffic encryption keys to use with each of its SAIDs. A CPE's traffic key requests are authenticated using a keyed hash (the HMAC algorithm [RFC2104]); the Message Authentication Key is derived from the Authorization Key obtained during the earlier authorization exchange. The BS responds with key replies, containing the Traffic Encryption Keys (TEKs); TEKs are triple DES encrypted with a key encryption key derived from the Authorization Key. Like the Key Requests, Key Replies are authenticated with a keyed hash, where the Message Authentication Key is derived from the Authorization Key.

7.1.2.2 CPE Key Update Mechanism

The traffic encryption keys which the BS provides to client CPE have a limited lifetime. The BS delivers a key's remaining lifetime, along with the key value, in the key replies it sends to its client CPE. The BS controls which keys are current by flushing expired keys and generating new keys. It is the responsibility of individual CPEs to insure the keys they are using match those the BS is using. CPE do this by tracking when a particular SAID's key is scheduled to expire and issuing a new key request for the latest key prior to that expiration time.

In addition, CPEs are required to periodically reauthorize with the BS; as is the case with Traffic Encryption Keys, an Authorization Key has a finite lifetime which the BS provides the CPE along with the key value. It is the responsibility of each CPE to reauthorize and obtain a fresh Authorization Key (and an up-to-date list of SA descriptors) before the BS expires the CPE's current Authorization Key.

Privacy initialization and key update is implemented within the Privacy Key Management protocol, defined in detail in Section 7.5.

7.2 MAC Frame Formats

When operating with Privacy enabled, CPE and BS encrypt the payload regions of particular MAC PDUs they transmit onto the FBWA network.

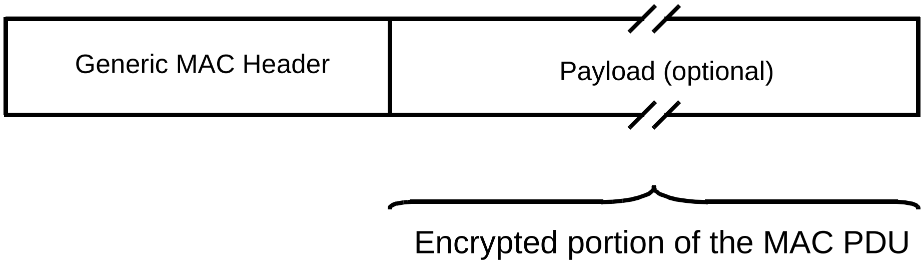


Figure 104—MAC PDU Encryption

The Generic MAC header shall not be encrypted. The Header contains all the Encryption information (Encryption Control Field, Encryption Key Sequence Field, and CID) needed to decrypt a Payload at the receiving station.

Four bits of a MAC Header contains a key sequence number. Recall that the keying material associated with a SA has a limited lifetime, and the BS periodically refreshes a SA's keying material. The BS manages a 4-bit key sequence number independently for each SA and distributes this key sequence number along with the SA's keying material to client CPE. The BS increments the key sequence number with each new generation of keying material. The MAC Header includes this sequence number, along with the SAID, to identify the specific generation of that SA keying material being used to encrypt the attached payload. Being a 4-bit quantity, the sequence number wraps around to 0 when it reaches 15.

Comparing a received PDU's key sequence number with what it believes to be the "current" key sequence number, a CPE or BS can easily recognize a loss of key synchronization with its peer. A CPE shall maintain the two most recent generations of keying material for each SA. Keeping on-hand the two most recent key generations is necessary for maintaining uninterrupted service during a SA's key transition.

Encryption of the payload is indicated by the Encryption Control (EC) bit field. A value of 0 indicates the payload is encrypted and the EKS field contains meaningful data. A value of 1 indicates the payload is not encrypted and the EKS field is set to all zeros.

7.2.1 Fragmentation and Encryption

A fragment may have its payload encrypted. Encryption is applied after fragmentation. Likewise, decryption is applied before reassembly of the PDU fragments.

7.3 Privacy Key Management (PKM) Protocol

7.3.1 State Models

7.3.1.1 Introduction

The PKM protocol is specified by two separate, but interdependent, state models: an authorization state model (the Authorization state machine) and an operational service key state model (the Traffic Encryption Key, or *TEK* state machine). This section defines these two state models. The state models are for explanatory purposes only, and should not be construed as constraining an actual implementation.

CPE authorization, controlled by the Authorization state machine, is the process of:

a) the BS authenticating a client CPE's identity
b) the BS providing the authenticated CPE with an Authorization Key, from which a Key Encryption Key (KEK) and message authentication keys are derived
c) the BS providing the authenticated CPE with the identities (i.e., the SAIDs) and properties of primary and static security associations the CPE is authorized to obtain keying information for

The KEK is a two-key triple DES encryption key that the BS uses to encrypt the Traffic Encryption Keys (TEKs) it sends to the modem. Traffic encryption keys are used for encrypting user data traffic. CPE and BS use message authentication keys to authenticate, via a keyed message digest, the key requests and responses they exchange.

After achieving initial authorization, a CPE periodically seeks re-authorization with the BS; reauthorization is also managed by the CPE's Authorization state machine. A CPE must maintain its authorization status with the BS in order to be able to refresh aging Traffic Encryption Keys. TEK state machines manage the refreshing of Traffic Encryption Keys.

A CPE begins authorization by sending an Authentication Information message to its BS. The Authentication Information message contains the CPE manufacturer’s X.509 certificate, issued by an external authority. The Authentication Information message is strictly informative, i.e., the BS may choose to ignore it; however it does provide a mechanism for a BS to learn the manufacturer certificates of its client CPE.

The CPE sends an Authorization Request message to its BS immediately after sending the Authentication Information message. This is a request for an Authorization Key, as well as for the SAIDs identifying any Static Security Associations the CPE is authorized to participate in. The Authorization Request includes:

a) the CPE’s manufacturer ID and serial number
b) the CPE’s MAC address
c) the CPE's public key
d) a manufacturer-issued X.509 certificate binding the CPE’s public key to its other identifying information
e) a description of the cryptographic algorithms the requesting CPE supports; a CPE’s cryptographic capabilities is presented to the BS as a list of cryptographic suite identifiers, each indicating a particular pairing of packet data encryption and packet data authentication algorithms the CPE supports
f) the CPE’s Basic CID. The Basic CID is the first static CID the BS assigns to a CPE during RF MAC registration -- the primary SAID is equal to the Basic CID

In response to an Authorization Request message, a BS validates the requesting CPE’s identity, determines the encryption algorithm and protocol support it shares with the CPE, activates an Authorization Key for the CPE, encrypts it with the CPE's public key, and sends it back to the CPE in an Authorization Reply message. The authorization reply includes:

a) an Authorization Key encrypted with the CPE's public key
b) a 4-bit key sequence number, used to distinguish between successive generations of Authorization Keys
c) a key lifetime
d) the identities (i.e., the SAIDs) and properties of the single primary and zero or more static security associations the CPE is authorized to obtain keying information for

While the Authorization Reply may identify Static SAs in addition to the Primary SA whose SAID matches the requesting CPE’s Basic CID, the Authorization Reply shall not identify any Dynamic SAs.

The BS, in responding to a CPE’s Authorization Request, will determine whether the re-questing CPE, whose identity can be verified via the X.509 digital certificate, is authorized for basic unicast services, and what additional statically provisioned services (i.e., Static SAIDs) the CPE's user has subscribed for. Note that the protected services a BS makes available to a client CPE can depend upon the particular cryptographic suites CPE and BS share support for.

Upon achieving authorization, a CPE starts a separate TEK state machine for each of the SAIDs identified in the Authorization Reply message. Each TEK state machine operating within the CPE is responsible for managing the keying material associated with its respective SAID. TEK state machines periodically send Key Request messages to the BS, requesting a refresh of keying material for their respective SAIDs. A Key Request includes:

a) identifying information unique to the CPE, consisting of the manufacturer ID, serial number, MAC address and RSA Public Key
b) the SAID whose keying material is being requested
c) an HMAC keyed message digest, authenticating the Key Request

The BS responds to a Key Request with a Key Reply message, containing the BS's active keying material for a specific SAID. This keying material includes:

a) the triple-DES-encrypted traffic encryption key
b) CBC initialization vector
c) a key sequence number
d) a key's remaining lifetime
e) an HMAC keyed message, authenticating the Key Reply

The traffic encryption key (TEK) in the Key Reply is triple DES (encrypt-decrypt-encrypt or EDE mode) encrypted, using a two-key, triple DES key encryption key (KEK) derived from the Authorization Key.

Note that at all times the BS maintains two active sets of keying material per SAID. The lifetimes of the two generations overlap such that each generation becomes active halfway through the life of it predecessor and expires halfway through the life of its successor. A BS includes in its Key Replies *both* of a SAID's active generations of keying material.

The Key Reply provides the requesting CPE, in addition to the TEK and CBC initialization vector, the remaining lifetime of each of the two sets of keying material. The receiving CPE uses these remaining lifetimes to estimate when the BS will invalidate a particular TEK, and therefore when to schedule future Key Requests such that the CPE requests and receives new keying material before the BS expires the keying material the CPE currently holds.

The operation of the TEK state machine's Key Request scheduling algorithm, combined with the BS's regimen for updating and using a SAID's keying material (see Section 7.5), insures that the CPE will be able to continually exchange encrypted traffic with the BS.

A CPE shall periodically refresh its Authorization Key by re-issuing an Authorization Request to the BS. Reauthorization is identical to authorization with the exception that the CPE does not send Authentication Information messages during reauthorization cycles. Section 7.3.1.2's description of the authorization state machine clearly indicates when Authentication Information messages are sent.

To avoid service interruptions during reauthorization, successive generations of the CPE's Authorization Keys have overlapping lifetimes. Both CPE and BS shall be able to support up to two simultaneously active Authorization Keys during these transition periods. The operation of the Authorization state machine's Authorization Request scheduling algorithm, combined with the BS's regimen for updating and using a client CPE's Authorization Keys (see Section 7.5), insures that CPE will be able to refresh TEK keying information without interruption over the course of the CPE's reauthorization periods.

A TEK state machine remains active as long as:

a) the CPE is authorized to operate in the BS's security domain; i.e., it has a valid Authorization Key, and
b) the CPE is authorized to participate in that particular Security Association; i.e. BS continues to provide fresh keying material during re-key cycles.

The parent Authorization state machine stops *all* of its child TEK state machines when the CPE receives from the BS an Authorization Reject during a reauthorization cycle. Individual TEK state machines can be started or stopped during a reauthorization cycle if a CPE's Static SAID authorizations changed between successive re-authorizations.

Communication between Authorization and TEK state machines occurs through the passing of events and protocol messaging. The Authorization state machine generates events (i.e., Stop, Authorized, Authorization Pending, and Authorization Complete events) that are targeted at its child TEK state machines. TEK state machines do not target events at their parent Authorization state machine. The TEK state machine affects the Authorization state machine indirectly through the messaging a BS sends in response to a modem's requests: a BS may respond to a TEK machine's Key Requests with a failure response (i.e., Authorization Invalid message) that will be handled by the Authorization state machine.

7.3.1.1.1 Preliminary Comment on Dynamic Security Associations and Dynamic SA Mapping

Section 7.1 introduced Dynamic SAs and mentioned how a BS can establish or eliminate a Dynamic SA in response to the initiation or termination of downstream traffic flows (e.g., a particular multicast group's traffic). In order for a CPE to run a TEK state machine to obtain a Dynamic Security Association's keying material, the CPE needs to know the corresponding SAID value. The BS, however, does not volunteer to client CPE the existence of Dynamic SAs; instead, it is the responsibility of CPE to request of the BS the mappings of traffic flow identifiers (e.g., an multicast address) to dynamic SAIDs.

The protocol defines a messaging exchange by which a CPE learns the mapping of a downstream traffic flow to a Dynamic SA (all upstream traffic is encrypted under a CPE's Primary SA). A SA Mapping state machine specifies how CPEs manage the transmission of these mapping request messages. This is a forward-looking definition designed to support multicast traffic encryption.

The Authorization state machine controls the establishment and termination of TEK state machines associated with the Primary and any Static SAs; it does not, however, control the establishment and termination of TEK state machines associated with Dynamic SAs. CPE shall implement the necessary logic to establish and terminate a Dynamic SA's TEK state machine. This interface specification, however, does not specify how CPE should manage their Dynamic SA's TEK state machines.

A full description of the SA Mapping state model is deferred to Section 7.4.

7.3.1.1.2 Security Capabilities Selection

As part of their authorization exchange, the CPE provides the BS with a list of all the cryptographic suites (pairing of data encryption and data authentication algorithms) the CPE supports. The BS selects from this list a single cryptographic suite to employ with the requesting CPE's primarySA. The Authorization Reply the BS sends back to the CPE includes a primary SA descriptor which, among other things, identifies the cryptographic suite the BS selected to use for the CPE's primary SA. A BS shall reject the authorization request if it determines that none of the offered cryptographic suites are satisfactory.

The Authorization Reply also contains an optional list of static SA descriptors; each static SA descriptor identifies the cryptographic suite employed within the SA. The selection of a static SA's cryptographic suite is typically made independent of the requesting CPE's cryptographic capabilities. A BS may include in its Authorization Reply static SA descriptors identifying cryptographic suites the requesting CPE does not support; if this is the case, the CPE shall not start TEK state machines for static SAs whose cryptographic suites the CPE does not support.

The above selection framework was incorporated in order to support future enhancements to MAC hardware and to the Privacy protocol. At the time of release of this specification, 56-bit DES and 40-bit DES are the only packet data encryption algorithms supported, and neither are paired with a packet data authentication algorithm.

7.3.1.2 Authorization State Machine

The Authorization state machine consists of six states and eight distinct events (including receipt of messages) that can trigger state transitions. The Authorization finite state machine (FSM) is presented below in a graphical format, as a state flow model (Figure 105), and in a tabular format, as a state transition matrix (Table 30).

The state flow diagram depicts the protocol messages transmitted and internal events generated for each of the model's state transitions; however, the diagram does not indicate additional internal actions, such as the clearing or starting of timers, that accompany the specific state transitions. Accompanying the state transition matrix is a detailed description of the specific actions accompanying each state transition; the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

The following legend applies to the Authorization State Machine flow diagram in depicted in Figure 105.

a) Ovals are states.
b) Events are in *italics*.
c) Messages are in normal font.
d) State transitions (i.e. the lines between states) are labeled with <what causes the transition>/<messages and events triggered by the transition>. So "*timeout*/Auth Request" means that the state received a "timeout" event and sent an Authorization Request ("Auth Request") message. If there are multiple events or messages before the slash "/" separated by a comma, *any* of them can cause a transition. If there are multiple events or messages listed after the slash, *all* of the specified actions must accompany the transition.

The Authorization state transition matrix presented in Table 30 lists the six Authorization machine states in the top-most row and the eight Authorization machine events (includes message receipts) in the left-most column. Any cell within the matrix represents a specific combination of state and event, with the next state (the state transitioned to) displayed within the cell. For example, cell 4-B represents the receipt of an Authorization Reply (Auth Reply) message when in the Authorize Wait (Auth Wait) state. Within cell 4-B is the name of the next state, "Authorized." Thus, when a CPE's Authorization state machine is in the Authorize Wait state and an Authorization Reply message is received, the Authorization state machine will transition to the Authorized state. In conjunction with this state transition, several protocol actions must be taken; these are described in the listing of protocol actions, under the heading 4-B, in Section 7.3.1.2.5.

A shaded cell within the state transition matrix implies that either the specific event cannot or should not occur within that state, and if the event does occur, the state machine shall ignore it. For example, if an Authorization Reply message arrives when in the Authorized state, that message should be ignored (cell 4-C). The CPE may, however, in response to an improper event, log its occurrence, generate an SNMP event, or take some other vendor-defined action. These actions, however, are not specified within the context of the Authorization state machine, which simply ignores improper events.

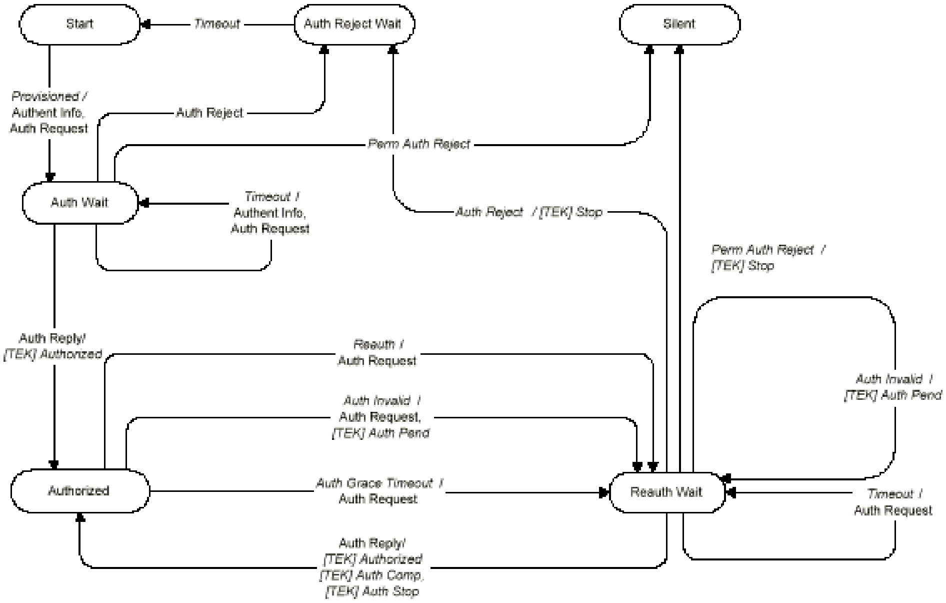


Figure 105—Authorization State Machine Flow Diagram

Table 30— Authorization FSM State Transition Matrix

State ***Event or Rcvd Message***	**(A)** **Start**	**(B)** **Auth Wait**	**(C)** **Authorized**	**(D)** **Reauth Wait**	**(E)** **Auth Reject Wait**	**(F)** **Silent**
(1) *Provisioned*	Auth Wait					
(2) Auth Reject		Auth Reject Wait		Auth Reject Wait		
(3) Perm Auth Reject		Silent		Silent		
(4) Auth Reply		Authorized		Authorized		
(5) Timeout		Auth Wait		Reauth Wait	Start	
(6) Auth Grace Timeout			Reauth Wait			
(7) Auth Invalid			Reauth Wait	Reauth Wait		
(8) Reauth			Reauth Wait			

7.3.1.2.1 States

Start

This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state—e.g., all timers are off, and no processing is scheduled.

Authorize Wait (Auth Wait)

The CPE has received the “Provisioned” event indicating that it has completed RF MAC registration with the BS. In response to receiving the event, the CPE has sent both an Authentication Information and an Authorize Request message to the BS and is waiting for the reply.

Authorized

The CPE has received an Authorization Reply message which contains a list of valid SAIDs for this CPE. At this point, the modem has a valid Authorization Key and SAID list. Transition into this state triggers the creation of one TEK FSM for each of the CPE’s privacy-enabled SAIDs.

Reauthorize Wait (Reauth Wait)

The CPE has an outstanding re-authorization request. The CPE was either about to time out its current authorization or received an indication (an Authorization Invalid message from the BS) that it’s authorization was no longer valid. The CPE sent an Authorization Request message to the BS and is waiting for a response.

Authorize Reject Wait (Auth Reject Wait)

The CPE received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject’s error code indicated the error was not of a permanent nature. In response to receiving this reject message, the CPE set a timer and transitioned to the Authorize Reject Wait state. The CPE remains in this state until the timer expires.

Silent

The CPE received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject’s error code indicated the error was of a permanent nature. This triggers a transition to the Silent state, where the CPE is not permitted to pass Subscriber traffic, but is able to respond to SNMP management requests arriving from across the cable network.

7.3.1.2.2 Messages

Note that the message formats are defined in detail in Section 7.3.2.

Authorization Request (Auth Request)

Request an Authorization Key and list of authorized SAIDs. Sent from CPE to BS.

Authorization Reply (Auth Reply)

Receive an Authorization Key and list of authorized, static SAIDs. Sent from BS to CPE. The Authorization Key is encrypted with the CPE’s public key.

Authorization Reject (Auth Reject)

Attempt to authorize was rejected. Sent from the BS to the CPE.

Authorization Invalid (Auth Invalid)

The BS can send an Authorization Invalid message to a client CPE as:

a) an unsolicited indication, or
b) a response to a message received from that CPE

In either case, the Authorization Invalid message instructs the receiving CPE to re-authorize with its BS.

The BS responds to a Key Request with an Authorization Invalid message if (1) the BS does not recognize the CPE as being authorized (i.e., no valid Authorization Key associated with CPE) or (2) verification of the Key Request's keyed message digest (in HMAC-Digest Attribute) failed. Note that the Authorization Invalid *event*, referenced in both the state flow diagram and the state transition matrix, signifies either the receipt of a Authorization Invalid message or an internally generated event.

Authentication Information (Authent Info)

The Authentication Information message contains the CPE manufacturer's X.509 Certificate, issued by an external authority. The Authent Info message is strictly an informative message the CPE sends to the BS; with it, a BS may dynamically learn the manufacturer certificate of client CPE. Alternatively, a BS may require out-of-band configuration of its list of manufacturer certificates.

7.3.1.2.3 Events

Provisioned

The Authorization state machine generates this event upon entering the Start state if the RF MAC has completed initialization, i.e., BS registration. If the RF MAC initialization is not complete, the CPE sends a Provisioned event to the Authorization FSM upon completing BS registration. The Provisioned event triggers the CPE to begin the process of getting its Authorization Key and TEKs.

Timeout

A retransmission or wait timer timed out. Generally a request is resent.

Authorization Grace Timeout (Auth Grace Timeout)

The Authorization Grace timer timed out. This timer fires a configurable amount of time (the Authorization Grace Time) before the current authorization is supposed to expire, signalling the CPE to re-authorize before its authorization actually expires. The Authorization Grace Time is specified in a configuration setting within the TFTP-downloaded parameter file.

Reauthorize (Reauth)

CPE's set of authorized static SAIDs may have changed. Event generated in response to an SNMP set, meant to trigger a reauthorization cycle.

Authorization Invalid (Auth Invalid)

This event can be internally generated by the CPE when there is a failure authenticating a Key Reply or Key Reject message, or externally generated by the receipt of an Authorization Invalid message, sent from the BS to the CPE. A BS responds to a Key Request with an Authorization Invalid if verification of the request's message authentication code fails. Both cases indicate BS and CPE have lost Authorization Key synchronization.

A BS may also send a CPE an unsolicited Authorization Invalid message to a CPE, forcing an Authorization Invalid event.

Permanent Authorization Reject (Perm Auth Reject)

The CPE receives an Authorization Reject in response to an Authorization Request. The error code in the Authorization Reject indicates the error is of a permanent nature. What is interpreted as a permanent error is subject to administrative control within the BS. Authorization Request processing errors that can be interpreted as permanent error conditions include:

a) unknown manufacturer (do not have CA certificate of the issuer of the CPE Certificate)
b) invalid signature on CPE certificate
c) ASN.1 parsing failure
d) inconsistencies between data in the certificate and data in accompanying PKM data Attributes
e) incompatible security capabilities

When a CPE receives an Authorization Reject indicating a permanent failure condition, the Authorization State machine moves into a Silent state where the CPE is not permitted to pass Subscriber traffic, but is able to respond to SNMP management requests received across the cable network interface. CPE shall issue an SNMP Trap upon entering the Silent state.

Authorization Reject (Auth Reject)

The CPE receives an Authorization Reject in response to an Authorization Request. The error code in the Authorization Reject does not indicate the failure was due to a permanent error condition. As a result, the CPE’s Authorization state machine will set a wait timer and transition into the Authorization Reject Wait State. The CPE remains in this state until the timer expires, at which time it will re-attempt authorization.

[Note: the following events are sent by an Authorization state machine to the TEK state machine.]

[TEK] Stop

Sent by the Authorization FSM to an active (non -START state) TEK FSM to terminate the FSM and remove the corresponding SAID’s keying material from the CPE’s key table.

[TEK] Authorized

Sent by the Authorization FSM to a non-active (START state), but valid TEK FSM.

[TEK] Authorization Pending (Auth Pend)

Sent by the Authorization FSM to a specific TEK FSM to place that TEK FSM in a wait state until the Authorization FSM can complete its re-authorization operation.

[TEK] Authorization Complete (Auth Comp)

Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait (Op Reauth Wait) or Rekey Reauthorize Wait (Rekey Reauth Wait) states to clear the wait state begun by a TEK FSM Authorization Pending event.

7.3.1.2.4 Parameters

All configuration parameter values are specified in the TFTP-downloaded parameter file (see 7.7: TFTP Configuration File Extensions).

Authorize Wait Timeout (Auth Wait Timeout)

Timeout period between sending Authorization Request messages from Authorize Wait state. See 7.7.1.1.1.

Authorization Grace Time (Auth Grace Time)

Amount of time before authorization is scheduled to expire that the CPE starts reauthorization. See .

Authorization Grace Time (Auth Grace Timeout)

Amount of time before authorization is scheduled to expire that the CPE starts re-authorization. See 7.7.1.1.2.

Authorize Reject Wait Timeout (Auth Reject Wait Timeout)

Amount of time a CPE's Authorization FSM remains in the Authorize Reject Wait state before transitioning to the Start state. See .

7.3.1.2.5 Actions

Actions taken in association with state transitions are listed by <event/rcvd message> - <state> below:

<u>1-A</u> Start (*Provisioned*) → Auth Wait

a) send Authentication Information message to BS
b) send Authorization Request message to BS
c) set Authorization Request retry timer to Authorize Wait Timeout

<u>2-B</u> Auth Wait (Auth Reject) → Auth Reject Wait

a) clear Authorization Request retry timer
b) set a wait timer to Authorize Reject Wait Timeout

<u>2-D</u> Reauth Wait (Auth Reject) → Auth Reject Wait

a) clear Authorization Request retry timer
b) generate TEK FSM Stop events for all active TEK state machines
c) set a wait timer to Authorize Reject Wait Timeout

<u>3-B</u> Auth Wait (Perm Auth Reject) → Silent

a) clear Authorization Request retry timer
b) disable all forwarding of CPE traffic

<u>3-D</u> Reauth Wait (Perm Auth Reject) → Silent

a) clear Authorization Request retry timer
b) generate TEK FSM Stop events for all active TEK state machines
c) disable all forwarding of CPE traffic

<u>4-B</u> Auth Wait (Auth Reply) → Authorized

a) clear Authorization Request retry timer
b) decrypt and record Authorization Key delivered with Authorization Reply

c) start TEK FSMs for all SAIDs listed in Authorization Reply (provided the CPE supports the cryptographic suite that is associated with a SAID) and issue a TEK FSM Authorized event for each of the new TEK FSMs
d) set the Authorization Grace timer to go off “Authorization Grace Time” seconds prior to the supplied Authorization Key’s scheduled expiration

4-D Reauth Wait (Auth Reply) → Authorized

a) clear Authorization Request retry timer
b) decrypt and record Authorization Key delivered with Authorization Reply
c) start TEK FSMs for any newly authorized SAIDs listed in Authorization Reply (provided the CPE supports the cryptographic suite that is associated with the new SAID) and issue TEK FSM Authorized event for each of the new TEK FSMs
d) generate TEK FSM Authorization Complete events for any currently active TEK FSMs whose corresponding SAIDs were listed in Authorization Reply
e) generate TEK FSM Stop events for any currently active TEK FSMs whose corresponding SAIDs were not listed in Authorization Reply
f) set the Authorization Grace timer to go off “Authorization Grace Time” seconds prior to the supplied Authorization Key’s scheduled expiration

5-B Auth Wait (*Timeout*) → Auth Wait

a) send Authentication Information message to BS
b) send Authorization Request message to BS
c) set Authorization Request retry timer to Authorize Wait Timeout

5-D Reauth Wait (*Timeout*) → Reauth Wait

a) send Authorization Request message to BS
b) set Authorization Request retry timer to Reauthorize Wait Timeout

5-E Auth Reject Wait (*Timeout*) → Start

a) no protocol actions associated with state transition

6-C Authorized (*Auth Grace Timeout*) → Reauth Wait

a) send Authorization Request message to BS
b) set Authorization Request retry timer to Reauthorize Wait Timeout

7-C Authorized (*Auth Invalid*) → Reauth Wait

a) clear Authorization Grace timer
b) send Authorization Request message to BS
c) set Authorization Request retry timer to Reauthorize Wait Timeout
d) if the Authorization Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Authorization Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the BS responded to with an Authorization Invalid message)

7-D Reauth Wait (*Auth Invalid*) → Reauth Wait

a) if the Authorization Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Authorization Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the BS responded to with an Authorization Invalid message)

8-C Authorized (*Reauth*) → Reauth Wait

a) clear Authorization grace timer
b) send Authorization Request message to BS
c) set Authorization Request retry timer to Reauthorize Wait Timeout

7.3.1.3 TEK State Machine

The TEK state machine consists of six states and nine events (including receipt of messages) that can trigger state transitions. Like the Authorization state machine, the TEK state machine is presented in both a state flow diagram and a state transition matrix. And as was the case for the Authorization state machine, the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

Shaded states in Figure 106 (Operational, Rekey Wait, and Rekey Reauthorize Wait) have valid keying material and encrypted traffic can be passed.

The Authorization state machine starts an independent TEK state machine for each of its authorized SAIDs.

As mentioned previously in Section 7.3.1.1, the BS maintains two active TEKs per SAID. The BS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. The BS encrypts downstream traffic with the older of its two TEKs and decrypts upstream traffic with either the older or newer TEK, depending upon which of the two keys the CPE was using at the time. The CPE encrypts upstream traffic with the newer of its two TEKs and decrypts downstream traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See Section 7.5 for details on CPE and BS key usage requirements.

Through operation of a TEK state machine, the CPE attempts to keep its copies of a SAID’s TEKs synchronized with those of its BS. A TEK state machine issues Key Requests to refresh copies of its SAID’s keying material soon after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for CPE/BS clock skew and other system processing and transmission delays, the CPE schedules its Key Requests a configurable number of seconds before the newer TEK’s estimated expiration in the BS. With the receipt of the Key Reply, the CPE shall always update its records with the TEK Parameters from both TEKs contained in the Key Reply Message. Figure 106 illustrates the CPE’s scheduling of its key refreshes in conjunction with its management of a SA’s active TEKs.

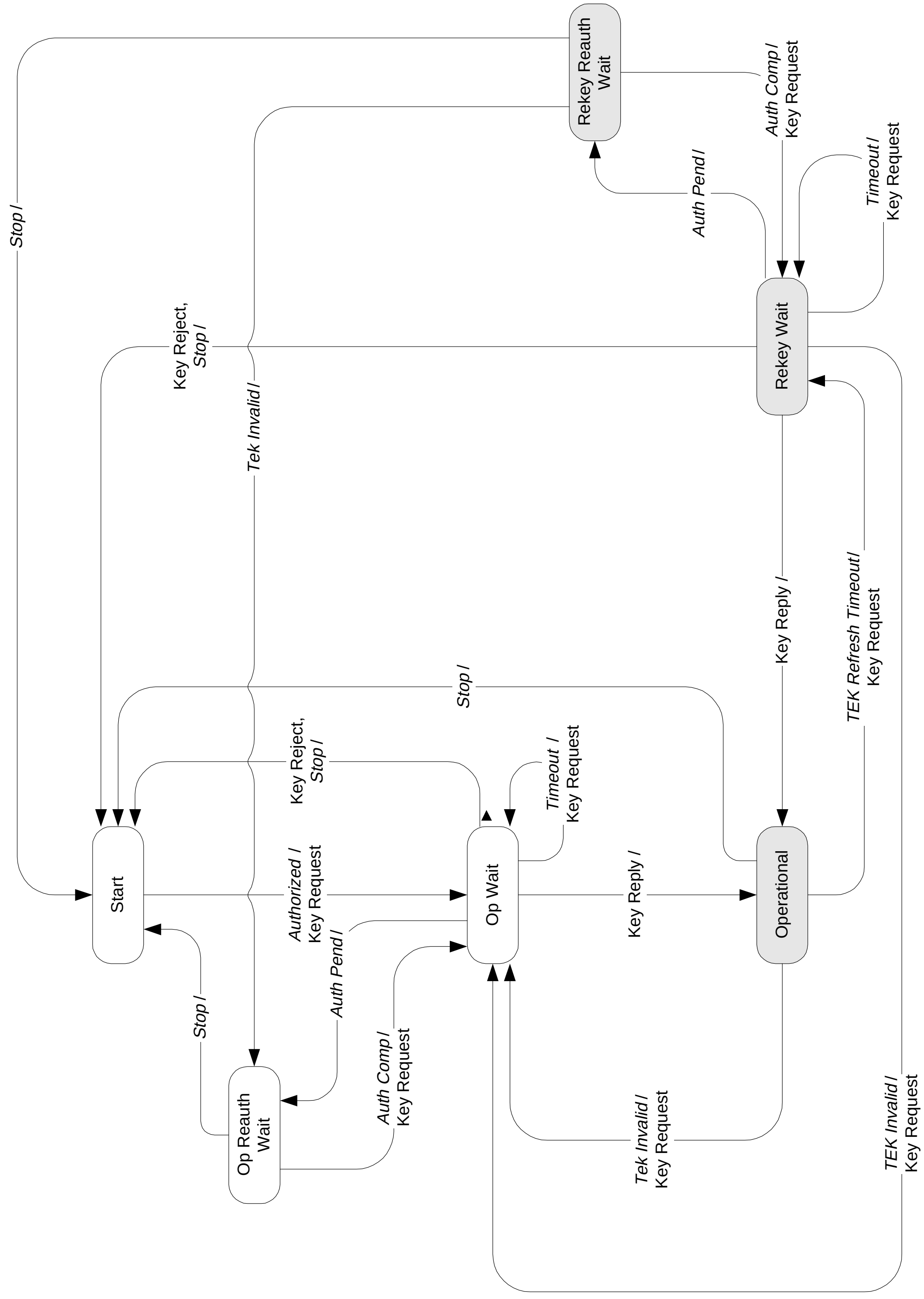


Figure 106—TEK State Machine Flow Diagram

Table 31—TEK FSM State Transition Matrix

State ***Event or Rcvd Message***	**(A) Start**	**(B) Op Wait**	**(C) Op Reauth Wait**	**(D) Op**	**(E) Rekey Wait**	**(F) Rekey Reauth Wait**
(1) *Stop*		Start	Start	Start	Start	Start
(2) *Authorized*	Op Wait					
(3) *Auth Pend*		Op Reauth Wait			Rekey Re-auth Wait	
(4) *Auth Comp*			Op Wait			Rekey Wait
(5) *TEK Invalid*				Op Wait	Op Wait	Op Reauth Wait
(6) *Timeout*		Op Wait			Rekey Wait	
(7) *TEK Refresh Timeout*				Rekey Wait		
(8) Key Reply		Operational			Operational	
(9) Key Reject		Start			Start	

7.3.1.3.1 States

Start

This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state—e.g., all timers are off, and no processing is scheduled.

Operational Wait (Op Wait)

The TEK state machine has sent its initial request (Key Request) for its SAID’s keying material (traffic encryption key and CBC initialization vector), and is waiting for a reply from the BS.

Operational Reauthorize Wait (Op Reauth Wait)

The wait state the TEK state machine is placed in if it does not have valid keying material while the Authorization state machine is in the in the middle of a reauthorization cycle.

Operational

The CPE has valid keying material for the associated SAID.

Rekey Wait

The TEK Refresh Timer has expired and the CPE has requested a key update for this SAID. Note that the newer of its two TEKs has not expired and can still be used for both encrypting and decrypting data traffic.

Rekey Reauthorize Wait (Rekey Reauth Wait)

The wait state the TEK state machine is placed in if the TEK state machine has valid traffic keying material, has an outstanding request for the latest keying material, and the Authorization state machine initiates a reauthorization cycle.

7.3.1.3.2 Messages

Note that the message formats are defined in detail in Section 7.3.2.

Key Request

Request a TEK for this SAID. Sent by the CPE to the BS and authenticated with keyed message digest. The message authentication key is derived from the Authorization Key.

Key Reply

Response from the BS carrying the two active sets of traffic keying material for this SAID. Sent by the BS to the CPE, it includes the SAID's traffic encryption keys, triple DES encrypted with a key encryption key derived from the Authorization Key. The Key Reply message is authenticated with a keyed message digest; the authentication key is derived from the Authorization Key.

Key Reject

Response from the BS to the CPE to indicate this SAID is no longer valid and no key will be sent. The Key Reject message is authenticated with a keyed message digest; the authentication key is derived from the Authorization Key

TEK Invalid

The BS sends a CPE this message if it determines that the CPE encrypted an upstream PDU with an invalid TEK; i.e., a SAID's TEK key sequence number, contained within the received PDU's MAC Header, is out of the BS's range of known, valid sequence numbers for that SAID.

7.3.1.3.3 Events

Stop

Sent by the Authorization FSM to an active (non-START state) TEK FSM to terminate TEK FSM and remove the corresponding SAID's keying material from the CPE's key table. See Section .

Authorized

Sent by the Authorization FSM to a non-active (START state) TEK FSM to notify TEK FSM of successful authorization. See Section .

Authorization Pending (Auth Pend)

Sent by the Authorization FSM to TEK FSM to place TEK FSM in a wait state while Authorization FSM completes re-authorization. See Section .

Authorization Complete (Auth Comp)

Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait or Rekey Reauthorize Wait states to clear the wait state begun by the prior Authorization Pending event. See Section <TBD>.

TEK Invalid

This event can be triggered by either a CPE's data packet decryption logic, or by the receipt of a TEK Invalid message from the BS.

A CPE's data packet decryption logic triggers a TEK Invalid event if it recognizes a loss of TEK key synchronization between itself and the encrypting BS; i.e., a SAID's TEK key sequence number, contained within the received, downstream PDU's MAC Header, is out of the CPE's range of known sequence numbers for that SAID.

A BS sends a CPE a TEK Invalid message, triggering a TEK Invalid event within the CPE, if the BS's decryption logic recognizes a loss of TEK key synchronization between itself and the CPE.

Timeout

A retry timer timeout. Generally, the particular request is retransmitted.

TEK Refresh Timeout

The TEK refresh timer timed out. This timer event signals the TEK state machine to issue a new Key Request in order to refresh its keying material. The refresh timer is set to fire a configurable length of time (*TEK Grace Time*) before the expiration of the newer TEK the CPE currently holds. This is configured via the BS to occur after the scheduled expiration of the older of the two TEKs.

7.3.1.3.4 Parameters

All configuration parameter values are specified in TFTP downloaded parameter file (see Section 7.7,: TFTP Configuration File Extensions).

Operational Wait Timeout

Timeout period between sending of Key Request messages from the Op Wait state. See Section 7.7.1.1.3.

Rekey Wait Timeout

Timeout period between sending of Key Request messages from the Rekey Wait state. See Section 7.7.1.1.4.

TEK Grace Time

Time interval, in seconds, before the estimated expiration of a TEK that the CPE starts rekeying for a new TEK.

TEK Grace Time is specified in a configuration setting within the TFTP-downloaded parameter file, and is the same across all SAIDs. See Section 7.7.1.1.5.

7.3.1.3.5 Actions

<u>1-B</u>   Op Wait (*Stop*) → Start

a) clear Key Request retry timer
b) terminate TEK FSM

<u>1-C</u> Op Reauth Wait (*Stop*) → Start

a) terminate TEK FSM

<u>1-D</u> Operational (*Stop*) → Start

a) clear TEK refresh timer, which is timer set to go off *"Tek Grace Time"* seconds prior to the TEK's scheduled expiration time
b) terminate TEK FSM
c) remove SAID keying material from key table

<u>1-E</u> Rekey Wait(*Stop*) → Start

a) clear Key Request retry timer
b) terminate TEK FSM
c) remove SAID keying material from key table

<u>1-F</u> Rekey Reauth Wait(*Stop*) → Start

a) terminate TEK FSM
b) remove SAID keying material from key table

<u>2-A</u> Start (*Authorized*) → Op Wait

a) send Key Request Message to BS
b) set Key Request retry timer to Operational Wait Timeout

<u>3-B</u> Op Wait (*Auth Pend*) → Op Reauth Wait

a) clear Key Request retry timer

<u>3-E</u> Rekey Wait (*Auth Pend*) → Rekey Reauth Wait

a) clear Key Request retry timer

<u>4-C</u> Op Reauth Wait (*Auth Comp*) → Op Wait

a) send Key Request message to BS
b) set Key Request retry timer to Operational Wait Timeout

<u>4-F</u> Rekey Reauth Wait (*Auth Comp*) → Rekey Wait

a) send Key Request message to BS
b) set Key Request retry timer to Rekey Wait Timeout

<u>5-D</u> Operational (*TEK Invalid*) → Op Wait

a) clear TEK refresh timer
b) send Key Request message to BS
c) set Key Request retry timer to Operational Wait Timeout
d) remove SAID keying material from key table

5-E Rekey Wait (*TEK Invalid*) → Op Wait

a) clear Key Request retry timer
b) send Key Request message to BS
c) set Key Request retry timer to Operational Wait Timeout
d) remove SAID keying material from key table

5-F Rekey Reauth Wait (*TEK Invalid*) → Op Reauth Wait

a) remove SAID keying material from key table

6-B Op Wait (*Timeout*) → Op Wait

a) send Key Request message to BS
b) set Key Request retry timer to Operational Wait Timeout

6-E Rekey Wait (*Timeout*) → Rekey Wait

a) send Key Request message to BS
b) set Key Request retry timer to Rekey Wait Timeout

7-D Operational (*TEK Grace Timeout*) → Rekey Wait

a) send Key Request message to BS
b) set Key Request retry timer to Rekey Wait Timeout

8-B Op Wait (Key Reply) → Operational

(Note: Key Reply passed message authentication.)

a) clear Key Request retry timer
b) process contents of Key Reply message and incorporate new keying material into key database
c) set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the key’s scheduled expiration

8-E Rekey Wait (Key Reply) → Operational

(Note: Key Reply passed message authentication.)

a) clear Key Request retry timer
b) process contents of Key Reply message and incorporate new keying material into key database
c) set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the key’s scheduled expiration

9-B Op Wait (Key Reject) → Start

(Note: Key Reject passed message authentication.)

a) clear Key Request retry timer
b) terminate TEK FSM

9-E Rekey Wait (Key Reject) → Start

a) clear Key Request retry timer

b) terminate TEK FSM
c) remove CID keying material from key table

7.3.2 Key Management Message Formats

Privacy Key Management employs two MAC message types: PKM-REQ and PKM-RSP.

Table 32—Privacy Key Management MAC Messages

Type Value	Message Name	Message Description
9	PKM-REQ	Privacy Key Management Request [CPE -> BS]
10	PKM-RSP	Privacy Key Management Response [BS -> CPE]

While these two MAC management message types distinguish between PKM requests (CPE to BS) and responses (BS to CPE), more detailed information about message contents is encoded in the PKM messages themselves. This maintains a clean separation between privacy management functions and MAC bandwidth allocation, timing and synchronization.

7.3.2.1 Packet Formats

Exactly one PKM message is encapsulated in the Management Message Payload field of a MAC management message.

A summary of the PKM message format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

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 SHOULD be silently discarded.

PKM Codes (decimal) are assigned as follows:

Table 33—Privacy Key Management Message Codes

Code	PKM Message Type	MAC Management Message Name
0-3	Reserved	-
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Authent Info	PKM-REQ
13	Map Request	PKM-REQ
14	Map Reply	PKM-RSP
15	Map Reject	PKM-RSP
16-255	Reserved	-

Identifier

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

The CPE shall 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 shall 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 BS's PKM response message shall match the Identifier field of the PKM Request message the BS is responding to. The Identifier field in TEK Invalid messages, which are not sent in response to PKM requests, shall be set to zero. The Identifier field in unsolicited Authorization Invalid messages shall be set to zero.

On reception of a PKM 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 shall 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 1490.

Attributes

PKM Attributes carry the specific authentication, authorization and key management data exchanged between client and server. Each PKM packet type has its own set of required and optional Attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a PKM message.

The end of the list of Attributes is indicated by the Length of the PKM packet.

Attributes are type/length/value (TLV) encoded, as shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             | Value...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Packet formats for each of the PKM messages are described below. The descriptions list the PKM attributes contained within each PKM message type. The Attributes themselves are described in Section 7.3.2.2. Unknown attributes shall be ignored on receipt, and skipped over while scanning for recognized attributes.

The BS shall silently discard all requests that do not contain ALL required attributes. The CPE shall silently discard all responses that do not contain ALL required attributes.

7.3.2.1.1 Authorization Request (Auth Request)

Code: 4

Attributes:

Table 34—Authorization Request Attributes

Attribute	Contents
CPE-Identification	contains information used to identify CPE to BS
CPE-Certificate	contains the CPE’s X.509 user certificate
Security-Capabilities	describes requesting CPE’s security capabilities
SAID	CPE’s primary SAID equal to the Basic CID

The CPE-Identification attribute contains a set of data that identifies the requesting CPE to the BS. Note that the BS is in all likelihood using only a single item in the CPE-Identification attribute (e.g., CPE MAC address) as a CPE handle. While a specific item could be selected for inclusion in the Authorization Request message, including the entire CPE-Identification attribute for client identification provides vendors with greater flexibility in the headend’s system design.

The CPE-Certificate attribute contains an X.509 CPE certificate issued by the CPE’s manufacturer. The CPE’s X.509 certificate is a public-key certificate which binds the CPE’s identifying information to it’s RSA public key in a verifiable manner. The X.509 certificate is digitally signed by the CPE’s manufacturer, and that signature can be verified by a BS that knows the manufacturer’s public key. The manufacturer’s public key is placed in an X.509 certification authority (CA) certificate, which in turn is signed by a higher level certification authority.

The Security-Capabilities attribute is a compound attribute describing the requesting CPE’s security capabilities. This includes the data encryption algorithm(s) a CPE supports and the data authentication algorithm(s) supported (of which there are currently none).

A SAID attribute contains a Privacy security association identifier, or SAID. In this case, the provided SAID is the CPE’s Basic CID, which is equal to the Basic CID assigned the to CPE during MAC registration.

7.3.2.1.2 Authorization Reply (Auth Reply)

Sent by the BS to a client CPE in response to an Authorization Request, the Authorization Reply message contains an Authorization Key, the key’s lifetime, the key’s sequence number, and a list of SA-Descriptors identifying the Primary and Static Security Associations the requesting CPE is authorized to access and their particular properties (e.g., type, cryptographic suite). The Authorization Key shall be encrypted with the CPE’s public key. The SA-Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding Authorization Request. The SA-Descriptor list may include descriptors of Static SAIDs the CPE is authorized to access.

Code field: 5

Attributes:

Table 35—Authorization Reply Attributes

Attribute	Contents
AUTH-Key	Authorization (AUTH) Key, encrypted with the target client CPE’s public key
Key-Lifetime	Authorization key lifetime
Key-Sequence-Number	Authorization key sequence number
(one or more) SA-Descriptor	Each SA-Descriptor compound Attribute specifies a SAID and additional properties of the SA.

7.3.2.1.3 Authorization Reject (Auth Reject)

BS responds to a CPE’s authorization request with an Authorization Reject message if the BS rejects the CPE’s authorization request.

Code field: 6

Attributes:

Table 36—Auth Rej Attributes

Attribute	Contents
Error-Code	Error code identifying reason for rejection of authorization request
Display-String (optional)	Display String providing reason for rejection of authorization request

The Error-Code and Display-String attributes describe to the requesting CPE the reason for the authorization failure.

7.3.2.1.4 Key Request

Code: 7

Attributes:

Table 37—Key Request Attributes

Attribute	Contents
CPE-Identification	Contains information used to identify CPE to BS
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute shall be the final Attribute in the Key Request’s Attribute list. The message digest is performed over the PDU header and all of the Key Request’s Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the BS to authenticate the Key Request message. The HMAC-Digest’s authentication key is derived from the Authorization Key. See Section 7.6, Cryptographic Methods, for details.

7.3.2.1.5 Key Reply

Code: 8

Attributes:

Table 38—Key Reply Attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
TEK-Parameters	“Older” generation of key parameters relevant to SAID
TEK-Parameters	“Newer” generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

The TEK-Parameters Attribute is a compound attribute containing all of the keying material corresponding to a particular generation of a SAID's TEK. This would include the TEK, the TEK’s remaining key lifetime, its key sequence number, and the CBC initialization vector. The TEK is encrypted. See Section 7.3.2.2.13 for details.

At all times the BS maintains two sets of active generations of keying material per SAID. (A set of keying material includes the a TEK and its corresponding CBC initialization vector.) One set corresponds to the “older” generation of keying material, the second set corresponds to the “newer” generation of keying material. The newer generation has a key sequence number one greater than (modulo 16) that of the older generation. Section 7.5.1 specifies BS requirements for maintaining and using a SAID’s two active generations of keying material.

The BS distributes to a client CPE both generations of active keying material. Thus, the Key Reply message contains two TEK-Parameters Attributes, each containing the keying material for one of the SAIDs two active sets of keying material.

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute shall be the final Attribute in the Key Reply’s Attribute list. The message digest is performed over the PKM message header (starting with the PKM Code field) and all of the Key Reply’s Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the Key Reply message and ensure CPE and BS have synchronized Authorization Keys. The HMAC-Digest’s authentication key is derived from the Authorization Key. See Section 7.6, Cryptographic Methods, for details.

7.3.2.1.6 Key Reject

Receipt of a Key Reject indicates the receiving client CPE is no longer authorized for a particular SAID.

Code: 9

Attributes:

Table 39—Key Reject Attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
Error-Code	Error code identifying reason for rejection of Key Request
Display-String (optional)	Display string containing reason for Key Reject
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute shall be the final Attribute in the Key Reject’s Attribute list. The message digest is performed over the PKM message header (starting with the PKM Code field) and all of the Key Reject’s Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the Key Reject message and ensure CPE and BS have synchronized Authorization Keys. The HMAC-Digest’s authentication key is derived from the Authorization Key. See Section 7.6, Cryptographic Methods, for details.

7.3.2.1.7 Authorization Invalid

The BS can send an Authorization Invalid message to a client CPE as:

a) an unsolicited indication, or
b) a response to a message received from that CPE

In either case, the Authorization Invalid message instructs the receiving CPE to re-authorize with its BS.

The BS sends an Authorization Invalid in response to a Key Request if (1) the BS does not recognize the CPE as being authorized (i.e., no valid Authorization Key associated with the requesting CPE) or (2) verification of the Key Request's keyed message digest (in HMAC-Digest Attribute) failed, indicating a loss of Authorization Key synchronization between CPE and BS.

Code: 10

Attributes:

Table 40—Authorization Invalid Attributes

Attribute	Contents
Error-Code	Error code identifying reason for Authorization Invalid
Display-String (optional)	Display String describing failure condition

7.3.2.1.8 TEK Invalid

The BS sends a TEK Invalid message to a client CPE if the BS determines that the CPE encrypted an upstream PDU with an invalid TEK; i.e., a SAID's TEK key sequence number, contained within the received packet's MAC Header, is out of the BS's range of known, valid sequence numbers for that SAID.

Code: 11

Attributes:

Table 41—TEK Invalid Attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
Error-Code	Error code identifying reason for TEK Invalid message
Display-String (optional)	Display string containing vendor-defined in-formation
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute shall be the final Attribute in the TEK Invalid's Attribute list. The message digest is performed over the PKM message header (starting with the PKM Code field) and all of the TEK Invalid's Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the TEK Invalid message and ensure CPE and BS have synchronized Authorization Keys. The HMAC-Digest’s authentication key is derived from the Authorization Key. See Section 7.6, Cryptographic Methods, for details.

7.3.2.1.9 Authentication Information (Authent Info)

The Authentication Info message contains a single CA-Certificate Attribute, containing an X.509 CA certificate for the manufacturer of the CPE. The CPE’s X.509 user certificate shall have been issued by the certification authority identified by the X.509 CA certificate. All X.509 CA certificates shall be issued by an external root certification authority.

Authentication Information messages are strictly informative: while the CPE shall transmit Authent Info messages as indicated by the Authentication state model (Section 7.3.1.2), the BS may ignore them.

Code: 12

Attributes:

Table 42—Authentication Information Attributes

Attribute	Contents
CA-Certificate	certificate of manufacturer CA that issued CPE certificate

The CA-certificate attribute contains an X.509 CA certificate for the CA that issued the CPE’s X.509 user certificate. The external certification authority issues these CA-certificates to CPE manufacturers.

7.3.2.1.10 SA Map Request (MAP Request)

A CPE modem sends SA Map Requests to its BS to request the mapping of a particular downstream traffic flow to a SA. Section 7.4 describes the SA Mapping state model which uses the message.

Code: 13

Attributes:

Table 43—SA Map Request Attributes

Attribute	Contents
CPE-Identification	Contains information used to identify CPE to BS
SA-Query	Contains addressing information identifying the downstream traffic flow CPE is requesting an SA mapping for

7.3.2.1.11 SA Map Reply (Map Reply)

A BS sends an SA Map Reply as a positive response to a client CPE's SA Map Request. The SA Map Reply informs the CPE of a mapping between a queried address and a SA. Section 7.4 describes the SA Mapping state model which uses the message.

Code: 14

Attributes:

Table 44—SA Map Reply Attributes

Attribute	Contents
SA-Query	Contains addressing information identifying the downstream traffic flow CPE is requested an SA mapping for
SA-Descriptor	SA-Descriptor compound Attribute specifies the mapped SA's SAID and other properties.

7.3.2.1.12 SAID Map Reject (Map Reject)

A BS sends SA Map Reject as a negative response to a client CPE's SA Map Request. The SA Map Reject informs the CPE that either (1) downstream traffic flow identified in the SA-Query Attribute is not being encrypted or (2) the requesting CPE is not authorized to receive that traffic. The contents of an error code attribute distinguishes between the two cases. Section 7.4 describes the SA Mapping state model which uses the message.

Code: 15

Attributes:

Table 45—SA MAP Reject Attributes

Attribute	Contents
SA-Query	Contains addressing information identifying the downstream traffic flow CPE requested an SA mapping for
Error-Code	Error code identifying reason for rejection of SA Map Request
Display-String (optional)	Display string containing reason for Map Reject

7.3.2.2 PKM Attributes

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             | Value...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

The Type field is one octet. Values of the PKM Type field are specified below. Note that Type values between 0 and 127 are defined within the Privacy Specification, values between 128 and 255 are vendor-assigned Attribute Types.

A PKM server shall ignore Attributes with an unknown Type.

A PKM client shall ignore Attributes with an unknown Type.

PKM client and server (i.e., CPE and BS) may log receipt of unknown attribute types.

Table 46—PKM Attribute Types

Type	BPKM Attribute
0	Reserved
1	Serial-Number
2	Manufacturer-ID
3	MAC-Address
4	RSA-Public-Key
5	CPE-Identification
6	Display-String
7	AUTH-KEY
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	Reserved
15	CBC-IV

Table 46—PKM Attribute Types

Type	BPKM Attribute
16	Error-Code
17	CA-Certificate
18	CPE-Certificate
19	Security-Capabilities
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	Version
23	SA-Descriptor
24	SA-Type
25	SA-Query
26	SA-Query-Type
27	IP-Address
28-126	Reserved
127	Vendor-Defined
128-255	Vendor-assigned attribute types

Length

The Length field is 2 octets, and indicates the length of this Attribute’s Value field, in octets. The length field *does not include* the Type and Length fields. The minimum Attribute Length is 0, the maximum Length is <TBD>.

Packets containing attributes with invalid lengths SHOULD be silently discarded.

Value

The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields. All multi-octet integer quantities are in network-byte order, i.e., the octet containing the most-significant bits is the first transmitted on the wire.

Note that a “string” does not require termination by an ASCII NULL because the Attribute already has a length field.

The format of the value field is one of five data types.

Table 47—Attribute Value Data Types

string	**0 – n octets**
uint8	8-bit unsigned integer
uint16	16-bit unsigned integer
uint32	32-bit unsigned integer
compound	collection of Attributes

7.3.2.2.1 Serial-Number

Description

This Attribute indicates the serial number assigned by the manufacturer to a CPE device.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type = 1  |            Length             | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

1 for Serial-Number

Length

>= 0 and =<255

String

The String field is zero or more octets and contains a manufacturer-assigned serial number.

The manufacturer-assigned serial number shall be encoded in the ISO 8859-1 character encoding.

The characters employed shall be restricted to the following:

a) A-Z (0x41-0x5A)
b) a-z (0x61-0x7A)
c) 0-9 (0x30-0x39)
d) “-” (0xD2)

7.3.2.2.2 Manufacturer-ID

Description

This Attribute identifies the manufacturer. The identifier is 3 octets long and contains the 3-octet Organizationally Unique Identifier (OUI) assigned to applying organizations by the IEEE [IEEE1]. The first two bits of the 3-octet string are set to zero.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type = 2  |            Length             | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

2 for Manufacturer-ID

Length

3

String

The String field is three octets and contains an IEEE OUI.

7.3.2.2.3 MAC-Address

Description

This Attribute identifies the IEEE MAC address assigned to the CPE. Guaranteed to be unique, it is likely to be used as a CPE handle/index at the BS.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type = 3  |            Length             | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

3 for MAC-Address

Length

6

String

The String field contains a 6-octet MAC address.

7.3.2.2.4 RSA-Public-Key

Description

This Attribute is a string attribute containing a DER-encoded RSAPublicKey ASN.1 type, as defined in the RSA Encryption Standard PKCS #1 v2.0 [RSA3].

PKCS #1 v2.0 specifies that an RSA public key consists of both an RSA public modulus and an RSA public exponent; the RSAPublicKey type includes both of these as DER-encoded INTEGER types.

PKCS #1 v2.0 states that the RSA public exponent may be standardized in specific applications, and the document suggests values of 3 or 65537 (F4). The protocol standardizes on F4 for a public exponent and employs a 1024-bit modulus.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type = 4  |            Length             | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

4 for RSA-Public-Key

Length

140 (length of DER-encoding, using F4 as the public exponent, and a 1024-bit public modulus)

String

DER-encoded RSAPublicKey ASN.1 type

7.3.2.2.5 CPE-Identification

Description

This Attribute is a compound attribute, consisting of a collection of sub-attributes. These sub-attributes contain information that can be used to uniquely identify a CPE. Sub-attributes shall include:

a) Serial-Number
b) Manufacturer-ID
c) MAC-Address
d) RSA-Public-Key

The CPE-Identification may also contain optional Vendor-Defined Attributes.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type = 5  |            Length             | Compound
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

5

Length

>= 126

7.3.2.2.6 Display-String

Description

This Attribute contains a textual message. It is typically used to explain a failure response, and might be logged by the receiver for later retrieval by an SNMP manager. Display strings shall be no longer than 128 bytes.

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

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type = 6  |            Length             | String...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

6 for Display String

Length

>=0 and <= 128

String

A string of characters. There is no requirement that the character string be null terminated; the length field always identifies the end of the string.

7.3.2.2.7 AUTH-Key

Description

The Authorization Key is an 20 byte quantity, from which a key encryption key, and two message authentication keys (one for upstream requests, and a second for downstream replies) are derived.

This Attribute contains either a 96 or a 128-octet quantity containing the Authorization Key RSA-encrypted with the CPE's 1024-bit RSA public key. Details of the RSA encryption procedure are given in section 7.5. The ciphertext produced by the RSA algorithm will be the length of the RSA modulus, i.e., 128 octets.

```
0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type = 7  |            Length             | String ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

7 for AUTH-Key

Length

96 or 128

String

96 or 128-octet quantity representing an RSA-encrypted Authorization Key.

7.3.2.2.8 TEK

Description

This Attribute contains an 8-octet quantity that is a TEK DES key, encrypted with a Key Encryption Key derived from the Authorization Key. TEK keys are encrypted using the Encrypt-Decrypt-Encrypt (EDE) mode of two-key triple DES. See Section 7.6, Cryptographic Methods, for details.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Type = 8   |            Length             | String ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

8 for TEK

Length

8

String

64-bit quantity representing a (two-key triple DES EDE mode) encrypted traffic encryption key.

7.3.2.2.9 Key-Lifetime

Description

This Attribute contains the lifetime, in seconds, of an Authorization Key or TEK. It is a 32-bit unsigned quantity representing the number of remaining seconds that the associated key will be valid.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Type = 9    |             Length            |   uint32 ...  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 ... uint32                    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

9 for Key-Lifetime

Length

4

uint32

32-bit quantity representing key lifetime

A key lifetime of zero indicates that the corresponding Authorization Key or traffic encryption key is not valid.

7.3.2.2.10 Key-Sequence-Number

Description

This Attribute contains a 4-bit sequence number for a TEK or Authorization Key. The 4-bit quantity, however, is stored in a single octet, with the high-order 4 bits set to 0.

A summary of the Key-Sequence-Number Attribute format is shown below. The fields are transmitted from left to right.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Type = 10   |             Length            |   uint8       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

10 for Key-Sequence-Number

Length

1

uint8

4-bit sequence number

7.3.2.2.11 HMAC-Digest

Description

This Attribute 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. Privacy uses a particular version of HMAC that employs the Secure Hash Algorithm (SHA-1), defined in [FIPS-180-1][FIPS-180-1].

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 11   |            Length             |   String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

11 for HMAC-Digest

Length

20-octets

String

A 160-bit (20 octet) keyed SHA hash

7.3.2.2.12 SAID

Description

This Attribute contains a 16-bit SAID (SAID) used by the Privacy Protocol as the security association identifier.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type = 12    |             Length            |    uint16 ... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| ...uint16     |
+-+-+-+-+-+-+-+-+
```

Type

12 for SAID

Length

2

uint16

16-bit quantity representing a SAID

7.3.2.2.13 TEK-Parameters

Description

This Attribute is a compound attribute, consisting of a collection of sub-attributes. These sub-attributes represent all security parameters relevant to a particular generation of a SAID’s TEK.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 13   |             Length            |   Compound...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

13 for TEK-Parameters

Length

33

Compound

The Compound field contains the following sub-Attributes:

Table 48—TEK-Parameters Sub-Attributes

Attribute	Contents
TEK	TEK, encrypted (two-key triple DES-EDE mode) with the KEK
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

7.3.2.2.14 CBC-IV

Description

This Attribute contains a 64-bit (8-octet) value specifying a Cipher Block Chaining (CBC) Initialization Vector.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 15   |              Length           |   String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

15 for CBC-IV

Length

8 octets

String

A 64-bit quantity representing a DES-CBC initialization vector.

7.3.2.2.15 Error-Code

Description

This Attribute contains a one-octet error code providing further information about an Authorization Reject, Key Reject, Authorization Invalid, or TEK Invalid.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 16   |             Length            |    uint8      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

16 for Error-Code

Length

1

uint8

1-octet error code

A BS shall include the Error-Code Attribute in all Authorization Reject, Authorization Invalid, Key Reject and TEK Invalid messages. Table 49 lists code values for use with this Attribute. The BS may employ the nonzero error codes (1-8) listed below; it may, however, return a code value of zero (0). Error code values other than those defined in Table 49 shall be ignored. Returning a code value of zero sends no additional failure information to the CPE; for security reasons, this may be desirable.

Table 49—Error-Code Attribute Code Values

Error Code	Messages	Description
0	all	no information
1	Auth Reject, Auth Invalid	Unauthorized CPE
2	Auth Reject, Key Reject	Unauthorized SAID
3	Auth Invalid	Unsolicited
4	Auth Invalid, TEK Invalid	Invalid Key Sequence Number
5	Auth Invalid	Message (Key Request) authentication failure
6	Auth Reject	Permanent Authorization Failure
7	Map Reject	not authorized for requested downstream traffic flow
8	Map Reject	downstream traffic flow not mapped to SAID

Error code 6, Permanent Authorization Failure, is used to indicate a number of different error conditions affecting the PKM authorization exchange. These include:

a) an unknown manufacturer; i.e., the BS does not have the CA certificate belonging to the issuer of a CPE certificate

b) CPE certificate has an invalid signature
c) ASN.1 parsing failure during verification of CPE certificate
d) CPE certificate is on the “hot list”
e) inconsistencies between certificate data and data in accompanying PKM attributes
f) CPE and BS have incompatible security capabilities

Their common property is that the failure condition is considered permanent: any re-attempts at authorization would continue to result in Authorization Rejects. Details about the cause of a Permanent Authorization Failure may be reported to the CPE in an optional Display-String Attribute that may accompany the Error-Code Attribute in Authorization Reject messages. Note that providing this additional detail to the CPE should be administratively controlled within the BS. The BS may log these Authorization failures, or even trap then to an SNMP manager.

7.3.2.2.16 Vendor-Defined

The Vendor-Defined Attribute is a compound attribute whose first sub-attribute shall be the Manufacturer-ID Attribute. Subsequent Attribute(s) are user defined, with Type values as-signed by the vendor identified by the previous Manufacturer-ID Attribute.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type = 127   |              Length           |   Compound ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

1 27 for Vendor-Defined

Length

>= 6

Compound

The first sub-attribute shall be Manufacturer-ID. Subsequent attributes can include both universal Types (i.e., defined within this specification) and vendor-defined Types, specific to the vendor identified in the preceding Manufacturer-ID sub-attribute.

7.3.2.2.17 CA-Certificate

Description

This Attribute is a string attribute containing an X.509 CA Certificate, as defined in [X.509].

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 17  |            Length             | String...
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

17 for CA-Certificate

Length

Variable. Length shall not cause resulting MAC management message to exceed the maximum allowed size.

String

X.509 CA Certificate (DER-encoded ASN.1)

7.3.2.2.18 CPE-Certificate

Description

This Attribute is a string attribute containing a CPE’s X.509 User Certificate, as defined in [X.509].

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 18  |            Length             | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

18 for CPE-Certificate

Length

Variable. Length shall not cause resulting MAC management message to exceed the maximum allowed size.

String

X.509 User Certificate (DER-encoded ASN.1)

7.3.2.2.19 Security-Capabilities

Description

The Security-Capabilities Attribute is a compound attribute whose sub-attributes identify the version of Privacy a CPE supports and the cryptographic suite(s) a CPE supports.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type = 19    |              Length           |   Compound ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

19 for Security-Capabilities

Length

>=9

Compound

The Compound field contains the following sub-Attributes:

Table 50—Security-Capabilities Sub-Attributes

Attribute	Contents
Cryptographic-Suite-List	list of supported cryptographic suites
Version	version of Privacy supported

7.3.2.2.20 Cryptographic-Suite

Description

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Type = 20    |              Length           |    uint16 ... |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | ...uint16     |
   +-+-+-+-+-+-+-+-+
```

Type

20 for Cryptographic-Suite

Length

2

Uint16

A 16-bit integer identifying a pairing of a data encryption algorithm (encoded in the left-most, most significant, byte) and a data authentication algorithm (encoded in the right-most, least significant, byte). Currently, 56-bit and 40-bit DES are the only algorithms specified for use within security, and neither are paired with a data authentication algorithm.

Table 51—Data Encryption Algorithm Identifiers

Value	Description
0	Reserved
1	CBC-Mode, 56-bit DES
2	CBC-Mode, 40-bit DES
3-255	Reserved

Table 52—Data Authentication Algorithm Identifiers

Value	Description
0	No Data Authentication
1-255	Reserved

Table 53—Cryptographic-Suite Attribute Values

Value	Description
256 (0x0100 hex)	CBC-Mode 56-bit DES & no data authentication
512 (0x0200 hex)	CBC-Mode 40-bit DES & no data authentication
all remaining values	Reserved

7.3.2.2.21 Cryptographic-Suite-List

Description

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 21  |             Length            | String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

21 for Cryptographic-Suite-List

Length

2*n, where n=number of cryptographic suites listed

Uint8

A list of byte pairs identifying a collection of cryptographic suites. Each byte pair represents a supported cryptographic suite, with an encoding identical to the value field of the Cryptographic-Suite Attribute (Section 7.3.2.2.20). The BS shall not interpret the relative ordering of byte pairs in the list as a CPE’s preferences amongst the cryptographic suites it supports.

7.3.2.2.22 Version

Description

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 22  |           Length              |     uint8     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

22 for Version

Length

1

Uint8

A 1-octet code identifying a version of Privacy security.

Table 54—Version Attribute Values

Value	Description
0	Reserved
1	Current Privacy
2-255	Reserved

7.3.2.2.23 SA-Descriptor

Description

The SA-Descriptor Attribute is a compound attribute whose sub-attributes describe the properties of a Security Association. These properties include the SAID, the SA type, and the cryptographic suite employed within the SA.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 23  |             Length              |  Compound...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

23 for SA-Descriptor

Length

14

Compound

The Compound field contains the following sub-Attributes:

Table 55—SA-Descriptor Sub-Attributes

Attribute	Contents
SAID	Security Association ID
SA-Type	Type of SA
Cryptographic-Suite	pairing of data encryption and data authentication algorithms employed within the SA

7.3.2.2.24 SA-Type

Description

Identifies Type of SA. Privacy defines three SA types: Primary, Static, Dynamic.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 24  |             Length              |     uint8     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

24 for SA-Type

Length

1

Uint8

A 1-octet code identifying the value of SA-type as defined in Table 56.

Table 56—SA-Type Attribute Values

Value	Description
0	Primary
1	Static
2	Dynamic
3-127	Reserved
128-255	Vendor-specific

7.3.2.2.25 SA-Query

Description

Compound Attribute used in SA Map Request to specify mapping query arguments. Query arguments include the query type and any addressing attributes particular to that query type - the addressing attributes identify a particular downstream traffic flow that a SA mapping is being requested for. Currently, the only query type specified is Multicast, and the addressing argument associated with that type is an IP group address.

```
   0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 25  |            Length             |  Compound...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

25 for SA-Query

Length

11

Compound

The Compound field contains the following sub-Attributes:

Table 7-3. SA-Query Sub-Attributes

Attribute	Contents
SA-Query-Type	Type of Query
IP-Address	required if SA-Query-Type = IP-Multicast; contains an IP group address whose SA mapping is being requested.

7.3.3.2.26 SA-Query-Type

Description

This Attribute identifies an IP address used to identify an encrypted IP traffic flow. It is used, for example, to specify an IP multicast group address.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type = 26  |            Length              |    uint8      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

26 for SA-Query-Type

Length

1

Uint8

A 1-octet code identifying the value of SA-Query-Type as defined in Table 57.

Table 57—SA-Query-Type Attribute Values

Value	Description
0	Reserved
1	IP Multicast
2-127	Reserved
128-255	Vendor-specific

7.4 Dynamic SA Mapping

7.4.1 Introduction

Dynamic Security Associations (Dynamic SAs), introduced in Section 7.1.1.3, are SAs that a BS establishes and eliminates, dynamically, in response to its enabling and disabling of specific downstream traffic flows. These traffic flows may be initiated by the actions of:

a) a CPE (Customer Premise Equipment) device attached to one of the BS's client CPE,
b) an application server within the head end,
c) an OSS system, or
d) other unspecified mechanisms.

Regardless of what triggers the establishment of a Dynamic SA within the BS, client CPE need a mechanism for learning the mapping of a particular Privacy-protected downstream traffic flow to that flow's dynamically assigned Security Association (and that SA's corresponding SAID).

The details of this mechanism and the associated requirements are TBD.

7.5 Key Usage

7.5.1 BS

After a CPE completes MAC Registration, it initiates an Authorization exchange with its BS. The BS's first receipt of an Authorization Request message from the unauthorized CPE initiates the activation of a new Authorization Key (AK), which the BS sends back to the requesting CPE in an Authorization Reply message. This AK will remain active until it expires according to its predefined lifetime, *Authorization Key Lifetime*, a BS system configuration parameter (see Appendix A.2).

The BS shall use keying material derived from the CPE's Authorization Key for:

a) verifying the HMAC-Digest in Key Requests received from that CPE
b) encrypting (EDE mode two-key triple DES) the TEK in the Key Replies it sends to that CPE (TEK is a sub-attribute of a Key Reply's TEK-Parameters Attribute)
c) calculating the HMAC-Digests it writes into Key Replies, Key Rejects and TEK Invalids sent to that CPE

The BS must always be prepared to send a CPE an AK upon request. The BS shall be able to support up to two simultaneously active AKs for each client CPE. The BS has two active AKs during an Authorization Key transition period; the two active keys have overlapping lifetimes.

An Authorization Key transition period begins when the BS receives an Authorization Request from a CPE and the BS has a single active AK for that CPE. In response to this Authorization Request, the BS activates a second AK, which it sends back to the requesting CPE in an Authorization Reply. The BS shall set the active lifetime of this second AK to be the remaining lifetime of the first AK, plus the predefined *Authorization Key Lifetime*; thus, the second, "newer" key will remain active for one *Authorization Key Lifetime* beyond the expiration of the first, "older" key. The key transition period will end with the expiration of the older key. This is depicted in the top half of Figure 6-1.

The Authorization Key lifetime a BS reports in a Authorization reply shall reflect, as accurately as an implementation permits, the remaining lifetimes of AK at the time the reply message is sent.

As long as the BS is in the midst of a CPE's Authorization Key transition period, and thus is holding two active Authorization Keys for that CPE, it will respond to Authorization Requests with the newer of the two active keys. Once the older key expires, an Authorization Request will trigger the activation of a new AK, and the start of a new key transition period.

If a CPE fails to reauthorize before the expiration of its most current AK, the BS will hold no active Authorization keys for the CPE and will consider the CPE *unauthorized*. A BS shall remove from its keying tables all TEKs associated with an unauthorized CPE's Primary SA.

A BS shall use a CPE's active AK(s) to verify the HMAC-digest in Key Requests received from the CPE. If a BS receives a Key Request while in an AK transition period, and the accompanying AK Key Sequence Number indicates the Request was authenticated with the newer of the two AKs, the BS identifies this as an *implicit acknowledgment* that the CPE has obtained the newer of the CPE's two active AKs.

A BS shall use an active AK when calculating HMAC-Digests in Key Replies and Key Rejects, and when encrypting the TEK in Key Replies. When sending Key Replies or Key Rejects within a key transition period (i.e., when two active AKs are available), if the newer key has been implicitly acknowledged, the BS shall use the newer of the two active AKs; if the newer key has not been implicitly acknowledged, the BS shall use the older of the two active AKs.

The upper half of Figure 6-1 illustrates the BS's policy regarding its use of AKs.

The BS shall maintain two sets of active traffic encryption keys (and their associated CBC initialization vectors) per SAID. They correspond to two successive generations of keying material, and have overlapping lifetimes. The newer TEK shall have a key sequence number one greater than (modulo 16) that of the older TEK. Each TEK becomes active half way through the lifetime of its predecessor, and expires half way through the lifetime of its successor. Once a TEK's lifetime expires, the TEK becomes inactive and shall no longer be used.

The BS transitions between the two active TEKs differently depending on whether the TEK is used for downstream or upstream traffic. For each of its SAIDs, the BS shall transition between active TEKs according to the following rules:

a) The BS shall use the older of the two active TEKs for encrypting downstream traffic. At expiration of the older TEK, the BS will immediately transition to using the newer TEK for encryption.
b) For decryption of upstream traffic, a transition period is defined that begins once the BS has sent the newer TEK to a CPE within a Key Reply Message. The upstream transition period begins from the time the BS sends the newer TEK in a Key Reply Message and concludes once the older TEK expires. While in the transition period, the BS shall be able to decrypt upstream frames using either the older or newer TEK.

Note that the BS encrypts with a given TEK for only the second half of that TEK's total lifetime. The BS is able, however, to decrypt with a TEK for the TEK's entire lifetime.

The upper half of Figure 6-2 illustrates this BS's management of a Privacy Security Association's TEKs.

The BS is responsible for maintaining keying information for both primary and multicast SAIDs in the above manner. The Privacy Key Management protocol defined in this specification describes a mechanism for synchronizing this keying information between a BS and its client CPE. It is the responsibility of the CPE to update its keys in a timely fashion; the BS will transition to a new downstream encryption key regardless of whether a client CPE has retrieved a copy of that TEK.

The Key Replies sent by a BS contain TEK parameters (the TEK itself, a key lifetime, a key sequence number and a CBC IV) for the two active TEKs. The key lifetimes a BS reports in a Key Reply shall reflect, as accurately as an implementation permits, the remaining lifetimes of these TEKs at the time the Key Reply message is sent.

7.5.2 CPE

The CPE is responsible for sustaining authorization with its BS and maintaining an active Authorization Key. A CPE shall be prepared to use its two most recently obtained AKs.

AKs have a limited lifetime and must be periodically refreshed. A CPE refreshes its Authorization Key by re-issuing an Authorization Request to the BS. The Authorization state machine (Section 7.3.1.2) manages the scheduling of Authorization Requests for refreshing AKs.

A CPE's Authorization state machine schedules the beginning of reauthorization a configurable length of time (the *Authorization Grace Time*) before the CPE's latest AK is scheduled to expire. The Authorization Grace Time is configured to provide a CPE with an authorization retry period that is sufficiently long to allow for system delays and provide adequate time for the CPE to successfully complete an Authorization exchange before the expiration of its most current AK.

Note that the BS does not require knowledge of the Authorization Grace Time. The BS, however, tracks the lifetime of its Authorization Keys and shall deactive a key once it has expired.

A CPE shall use the newer of its two most recent Authorization Keys when calculating the HMAC-Digests it attaches to Key Requests. It shall be able to use either of its two most recent AKs to authenticate Key Replies or Key Rejects, and to decrypt a Key Keply's encrypted TEK. The CPE uses the accompanying AK Key Sequence Number to determine which of the two AKs to use.

The lower half of Figure 6-1 illustrates a CPE's maintenance and usage of its Authorization Keys.

A CPE shall be capable of maintaining two successive sets of traffic keying material per authorized SAID. Through operation of its TEK state machines, a CPE attempts to always maintain a SAID's two most recent sets of traffic keying material.

For each of its authorized SAIDs, the CPE:

a) shall use the newer of its two TEKs to encrypt newly received upstream traffic. Traffic already queued up may use either TEK (in no specific order) for a brief period of time covering the transition from the old to the new key.
b) shall be able to decrypt downstream traffic encrypted with either of the TEKs

7.6 Cryptographic Methods

This section specifies cryptographic algorithms and key sizes protocol uses.

7.6.1 Packet Data Encryption

Privacy shall use the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81] to encrypt the MAC PDU payloads.

Privacy implementations shall support 56-bit DES.

CBC shall be initialized with an initialization vector that is provided, along with other SAID key material, in a BS's Key Reply. Chaining is done block to block within a frame and reinitialized on a frame basis in order to make the system more robust to potential frame loss.

Residual termination block processing shall be used to encrypt the final block of plaintext when the final block is less than 64 bits. Given a final block having n bits, where n is less than 64, the next-to-last ciphertext block is DES encrypted a second time, using the ECB mode, and the least significant n bits of the result are exclusive ORed with the final n bits of the payload to generate the short final cipher block. In order for the receiver to decrypt the short final cipher block, the receiver DES encrypts the next-to-last ciphertext block, using the ECB mode, and exclusive ORs the left-most n bits with the short final cipher block in order to recover the short final cleartext block. This encryption procedure is depicted in Figure 9.4 (pg. 195) of [SCHNEIER].

In the special case when the frame's to-be-encrypted plaintext is less than 64 bits, the initialization vector shall be DES encrypted, and the left-most n bits of the resulting ciphertext corresponding to the number of bits of the payload shall be exclusive ORed with the n bits of the payload to generate the short cipher block.[1]

7.6.2 Encryption of TEK

The BS encrypts the value fields of the TEK in the Key Reply messages it sends to client CPE. This field is encrypted using two-key triple DES in the encrypt-decrypt-encrypt (EDE) mode [SCHNEIER]:

encryption: $C = E_{k1}[D_{k2}[E_{k1}[P]]]$
decryption: $P = D_{k1}[E_{k2}[D_{k1}[C]]]$
P = Plaintext 64-bit TEK
C = Ciphertext 64-bit TEK
k1 = left-most 64 bits of the 128-bit KEK
k2 = right-most 64 bits of the 128-bit KEK
E[ ] = 56-bit DES ECB (electronic code book) mode encryption
D[ ] = 56-bit DES ECB decryption

Section 7.6.4 below describes how the KEK is derived from the Authorization key.

7.6.3 HMAC-Digest Algorithm

The keyed hash employed by the HMAC-Digest Attribute shall use the HMAC message authentication method [RFC 2104] with the SHA-1 hash algorithm [FIPS-180-1].

Upstream and downstream message authentication keys are derived from the Authorization Key (see Section 7.6.4 below for details).

7.6.4 Derivation of TEKs, KEKs and Message Authentication Keys

The BS generates Authorization Keys, TEKs and IVs. A random or pseudo-random number generator shall be used to generate Authorization Keys and TEKs. A random or pseudo-random number generator may also be used to generate IVs; regardless of how they are generated, IVs shall be unpredictable. [RFC1750] provides recommended practices for generating random numbers for use within cryptographic systems.

[FIPS-81] defines DES keys as 8-octet (64-bit) quantities where the seven most significant bits (i.e., seven left-most bits) of each octet are the independent bits of a DES key, and the least significant bit (i.e., right-most bit) of each octet is a parity bit computed on the preceding seven independent bits and adjusted so that the octet has odd parity.

The keying material for two-key triple DES consists of two distinct (single) DES keys.

[1] This method of encrypting short payloads is vulnerable to attack: EXORing two sets of ciphertext encrypted in the above manner under the same set of keying material will yield the EXOR of the corresponding sets of plaintext. Further investigation is required.

PKM does not require odd parity. The PKM protocol generates and distributes 8-octet DES keys of arbitrary parity, and it requires that implementations ignore the value of the least significant bit of each octet.

A key encryption key (KEK) and two message authentication keys are derived from a common Authorization Key. The following defines how these keys are derived:

KEK is the Key Encryption Key used to encrypt Traffic Encryption Keys.

HMAC_KEY_U is the message authentication key used in upstream Key Requests

HMAC_KEY_D is the message authentication key used in downstream Key Replies, Key Rejects and TEK Invalids.

SHA(x|y) denotes the result of applying the SHA function to the concatenated bit strings x and y.

Truncate(x,n) denotes the result of truncating x to its left-most n bits.

```
KEK = Truncate(SHA( K_PAD | AUTH_KEY ), 128)

HMAC_KEY_U = SHA( H_PAD_U | AUTH_KEY )

HMAC_KEY_D = SHA( H_PAD_D | AUTH_KEY )
```

Each _PAD_ is a 512 bit string:

K_PAD = 0x53 repeated 64 times.

H_PAD_U = 0x5C repeated 64 times.

H_PAD_D = 0x3A repeated 64 times.

7.6.5 Public-Key Encryption of Authorization Key

Authorization keys in Authorization Reply messages shall be RSA public-key encrypted, using the CPE's public key. The protocol uses F4 (65537 decimal, or equivalently, 010001 hexadecimal) as its public exponent and a modulus length of 1024 bits. The protocol employs the RSAES-OAEP encryption scheme specified in version 2.0 of the PKCS#1 standard [RSA3]. RSAES-OAEP requires the selection of: a hash function; a mask-generation function; and an encoding parameter string. The default selections specified in [RSA3] shall be used when encrypting the authorization key. These default selections are: SHA-1 for the hash function; MGF1 with SHA-1 for the mask-generation function; and the empty string for the encoding parameter string.

7.6.6 Digital Signatures

The Protocol employs the RSA Signature Algorithm [RSA3] with SHA-1 [FIPS186] for all three of its certificate types.

As with its RSA encryption keys, Privacy uses F4 (65537 decimal, 010001 hexadecimal) as the public exponent for its signing operation. The external authority Root CA will employ a modulus length of 2048 bits (256 octets) for signing the Manufacturer CA certificates it issues. Manufacturer CAs shall employ signature key modulus lengths of at least 1024 bits, and no greater than 2048 bits.

7.6.7 Supporting Alternative Algorithms

The current specification requires the use of 56-bit DES for encrypting packet data, two-key triple DES for encrypting traffic encryption keys, 1024-bit RSA for encrypting Authorization keys, and 1024-to-2048-bit RSA for signing Privacy X.509 certificates. The choice of key lengths and algorithms, while appropriate for current threat models and hardware capabilities, may be inappropriate in the future.

For example, it is generally agreed that DES is approaching the end of its practical usefulness as the industry standard for symmetric encryption. NIST is currently overseeing the development and adoption of a new standard encryption algorithm, commonly referred to as the Advanced Encryption Standard, or AES. Given the nature of the security services, the protocol is being asked to support (basic privacy at a level better than or equal to that possible over dedicated wires, and conditional access to RF data transport services) as well as the protocol's flexible key management policy (i.e., setting of key lifetimes), service providers will be justified in the continued reliance on DES for, at least, the next five years. Nevertheless, at some future date, CPEs will need to adopt a stronger traffic encryption algorithm, possibly AES.

7.7 TFTP Configuration File Extensions

All of a CPE's Privacy configuration parameter values are specified in the configuration file TFTP-downloaded by the CPE during RF MAC initialization. Privacy configuration setting fields are included in both the CPE MIC and BS MIC calculations, and in a CPE's registration requests.

7.7.1 Privacy Configuration Setting Encodings

The following type/length/value encodings for Privacy configuration settings shall be used in both the configuration file and in MAC CPE registration requests.

The Privacy Enable configuration setting controls whether Privacy is enabled or disabled in a CPE. If Privacy is enabled, the Privacy Configuration Setting shall also be present. The Privacy Configuration setting may be present if Privacy is disabled. The separate Privacy Enable parameter allows an operator to disable or re-enable Privacy by toggling a single configuration parameter, thus not requiring the removal or re-insertion of the larger set of Privacy Configuration parameters.

This field defines the parameters associated with Privacy operation. It is composed of a number of encapsulated type/length/value fields. The type fields defined are only valid within the encapsulated Baseline Privacy configuration setting string.

type	length	value
P_CFG	n	

7.7.1.1 Internal Baseline Privacy Encodings

7.7.1.1.1 Authorize Wait Timeout

The value of the field specifies retransmission interval, in seconds, of Authorization Request messages from the Authorize Wait state.

sub-type	length	value
1	4	

Valid Range: 1 - 30

Reauthorize Wait Timeout

The value of the field specifies retransmission interval, in seconds, of Authorization Request messages from the Authorize Wait state.

sub-type	length	value
2	4	

Valid Range: 1 - 30

7.7.1.1.2 Authorization Grace Time

The value of this field specifies the grace period for re-authorization, in seconds.

sub-type	length	value
3	4	

Valid Range: 1 - 6,047,999

7.7.1.1.3 Operational Wait Timeout

The value of this field specifies the retransmission interval, in seconds, of Key Requests from the Operational Wait state.

sub-type	length	value
4	4	

Valid Range: 1 - 10

7.7.1.1.4 Rekey Wait Timeout

The value of this field specifies the retransmission interval, in seconds, of Key Requests from the Rekey Wait state.

sub-type	length	value
5	4	

Valid Range: 1 - 10

7.7.1.1.5 TEK Grace Time

The value of this field specifies grace period, in seconds, for rekeying the TEK.

sub-type	length	value
6	4	

Valid Range: 1 - 302399

7.7.1.1.6 Authorize Reject Wait Timeout

The value of this field specifies how long a CPE waits (seconds) in the Authorize Reject Wait state after receiving an Authorization Reject.

sub-type	length	value
7	4	

Valid Range: 1 - 600

7.7.1.1.7 SA Map Wait Timeout

The value of this field specifies the retransmission interval, in seconds, of SA Map Requests from the Map Wait state.

sub-type	length	value
8	4	

Valid Range: 1 - 10

7.7.1.1.8 SA Map Max Retries

The value of this field specifies the maximum number of Map Request retries allowed.

sub-type	length	value
9	4	

Valid Range: 0 - 10

7.7.1.2 Parameter Guidelines

Below are recommended ranges and values for Privacy’s various configuration and operational parameters. These ranges and default values may change as service providers gain operational experience running Privacy.

Table 58—Recommended Operational Ranges for Privacy Configuration Parameters

System	Name	Description	Minimum Value	Default Value	Maximum Value
BS	Authorization Lifetime	Lifetime, in seconds, BS assigns to new Authorization Key	1 day (86,400 sec.)	7 days (604,800 sec.)	70 days (6,048000 sec.)
BS	TEK Lifetime	Lifetime, in seconds, BS assigns to new TEK	30 min. (1800 sec.)	12 hours (43,200 sec.)	7 days (604,800 sec.)
CPE	Authorize Wait Timeout	Auth Req retransmission interval from Auth Wait state	2 sec.	10 sec.	30 sec.
CPE	Reauthorize Wait Timeout	Auth Req retransmission interval from Reauth Wait state	2 sec.	10 sec.	30 sec.
CPE	Authorization Grace Time	Time prior to Authorization expiration CPE begins re-authorization	5 min. (300 sec.)	10 min. (600 sec.)	35 days (3,024,000 sec).
CPE	Operational Wait Timeout	Key Req retransmission interval from Op Wait state	1 sec.	1 sec.	10 sec.
CPE	Rekey Wait Timeout	Key Req retransmission interval from Rekey Wait state	1 sec.	1 sec.	10 sec.
CPE	TEK Grace Time	Time prior to TEK expiration CPE begins rekeying	5 min. (300 sec)	1 hour (3,600 sec.)	3.5 days (302,399 sec)
CPE	Authorize Reject Wait	Delay before re-sending Auth Request after receiving Auth Reject	10 sec.	60 sec.	10 min. (600 sec.)
CPE	SA Map Wait Timeout	Map Request retransmission interval from Map Wait state	1 sec.	1 sec.	10 sec.
CPE	SA Map Max Retries	Maximum number of times CPE retries SA Map Request before giving up	0	4	10

The valid range (vs. recommended operational range) for Authorization and TEK lifetimes are:

a) Authorization Lifetime Valid Range: 1 - 6,048,000 seconds
b) TEK Lifetime Valid Range: 1 - 604,800 seconds

Note that valid ranges defined for each of Privacy’s configuration parameters extend below the recommended operational ranges. For the purposes of protocol testing, it is useful to run the privacy protocol with timer values well below the low end of the recommended operational ranges. The shorter timer values "speed up" prviacy’s clock, causing privacy protocol state machine events to occur far more rapidly than they would under an "operational" configuration. While privacy implementations need not be designed to operate efficiently at this accelerated privacy pace, the protocol implementation should operate correctly under these shorter timer values. Table 59 provides a list of shortened parameter values which are likely to be employed in protocol conformance and certification testing.

Table 59—Shortened Privacy Parameter Values for Protocol Testing

Authorization Lifetime	**5 min. (300 sec.)**
TEK Lifetime	3 min. (180 sec.)
Authorization Grace Time	1 min. (60 sec.)
TEK Grace time	1 min. (60 sec.)

The TEK Grace Time shall be less than half the TEK lifetime.