INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.112

Annex C

(02/2002)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Interactive systems for digital television distribution

Transmission systems for interactive cable television services

Annex C: Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique

ITU-T Recommendation J.112 – Annex C

ITU-T J-SERIES RECOMMENDATIONS

CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

General Recommendations	J.1–J.9
General specifications for analogue sound-programme transmission	J.10–J.19
Performance characteristics of analogue sound-programme circuits	J.20–J.29
Equipment and lines used for analogue sound-programme circuits	J.30–J.39
Digital encoders for analogue sound-programme signals	J.40–J.49
Digital transmission of sound-programme signals	J.50–J.59
Circuits for analogue television transmission	J.60–J.69
Analogue television transmission over metallic lines and interconnection with radio-relay links	J.70–J.79
Digital transmission of television signals	J.80–J.89
Ancillary digital services for television transmission	J.90–J.99
Operational requirements and methods for television transmission	J.100–J.109
Interactive systems for digital television distribution	**J.110–J.129**
Transport of MPEG-2 signals on packetised networks	J.130–J.139
Measurement of the quality of service	J.140–J.149
Digital television distribution through local subscriber networks	J.150–J.159
IPCablecom	J.160–J.179
Miscellaneous	J.180–J.199
Application for Interactive Digital Television	J.200–J.209

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation J.112

Transmission systems for interactive cable television services

Annex C

Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique

Summary

This annex includes descriptions of 256-QAM for downstream and 16-QAM for upstream in Physical Layer. These modulation functions enable cable television networks to transmit high speed programme data and IP Packets as well. However, the most significant change of this revised annex is an enhancement of MAC Layer the descriptions for QoS oriented services such as Voice over IP, Video over IP. The enhancement includes Extension of MAC Frame Format, Extension for QoS Control Function, Payload Header Suppression and Multicast Extension.

Source

Annex C to ITU-T Recommendation J.112 was revised by ITU-T Study Group 9 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 February 2002.

Keywords

must, must not, should, should not, may

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Page

ITU-T Recommendation J.112

Transmission systems for interactive cable television services

Annex C

Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique

C.1 Scope

C.1.1 General Scope

This annex describes the radio-frequency interface specifications for high-speed data-over-cable systems.

Since successful standardization of J.112 Cable Modem in ITU-T in 1998, intensive efforts have been taken to develop a new version of cable modem for realization of QoS-controled services over Cable television networks that carry IP traffic between external network and cable modems transparently. This revised Annex C describes interface specification for a new version of cable modem for the realization of services mentioned above.

Extension of MAC Frame Format describes Fragmentation MAC Header that divides and re-constructs Protocol Data Unit in up-stream, Concatenation MAC Header for improvement of cable modem through-put, and Piggy-back request for next reservation information. Extension for QoS Control Function includes descriptions for scheduling function between Cable Modem Termination System and Cable Modem to guarantee bandwidth and latency, for packet recognition function, and for dynamic addition/ deletion functions for QoS guaranteed services. Payload Header Suppression improves bandwidth usage efficiency by suppressing repeated header information in each IP Packet. Multicast Extension is a filtering function of Multicast Packets by IGMP (Internet Group Management Protocol) to control Multicast Packets between CMTS and cable modem.

C.1.2 Background

C.1.2.1 Service Goals

Cable operators are interested in deploying high-speed packet-based communications systems on cable television systems that are capable of supporting a wide variety of services. Services under consideration by cable operators include packet telephony service, video conferencing service, T1/frame relay equivalent service, and many others. It has been decided to prepare a series of interface specifications that will permit the early definition, design, development and deployment of data-over-cable systems on a uniform, consistent, open, non-proprietary, multi-vendor interoperable basis.

The intended service will allow transparent bidirectional transfer of Internet Protocol (IP) traffic, between the cable system headend and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network. This is shown in simplified form in Figure C.1-1.

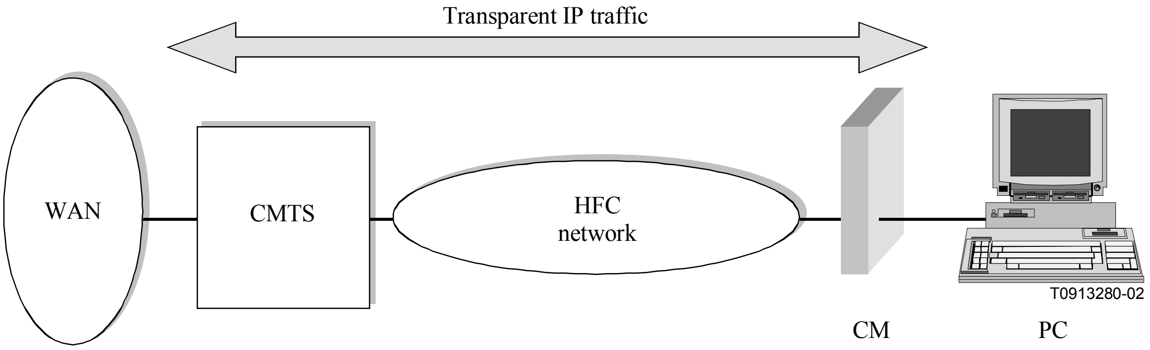


Figure C.1-1/J.112 – Transparent IP traffic through HFC network

The transmission path over the cable system is realized at the headend by a Cable Modem Termination System (CMTS), and at each customer location by a Cable Modem (CM). The intent is for operators to transparently transfer IP traffic between WAN and PC in customer premises, including but not limited to datagrams, DHCP, ICMP, and IP Group addressing (broadcast and multicast).

C.1.2.2 Reference Architecture

The reference architecture for the data-over-cable services and interfaces is shown in Figure C.1-2.

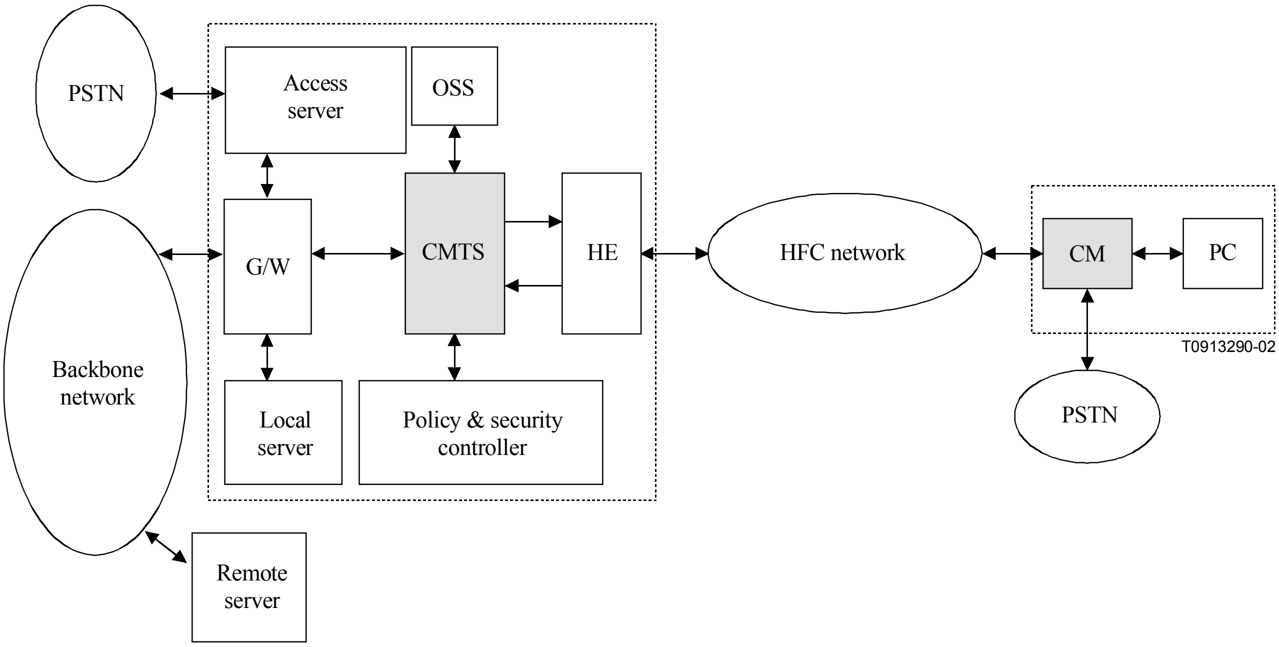


Figure C.1-2/J.112 – Data-over-cable reference architecture

C.1.2.3 Statement of Compatibility

This clause applies only to the first option as defined in C.1.1.

This annex specifies an interface, commonly referred to as Revised Annex C (2002), which is an extension of the interface specified in Previous Annex C (1998). These extensions are entirely backwards and forwards compatible with the Previous Annex C (1998). Revised Annex C (2002) compliant CMs have to interoperate seamlessly with Previous Annex C CMTSs. Revised Annex C compliant CMTSs MUST seamlessly support Previous Annex C CMs.

Refer to Annex G for further interoperability information.

C.2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this annex.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[CableLabs1] CableLabs1 (April 12, 1995), *Two-Way Cable Television System Characterization, Cable Television Laboratories, Inc.*

[CableLabs2] CableLabs2 (November, 1994), *Digital Transmission Characterization of Cable Television Systems, Cable Television Laboratories, Inc.*

[DIX] DIX (1982), *Ethernet Protocol Version 2.0, Digital, Intel, Xerox.*

[FCC15] Code of Federal Regulations, Title 47, Part 15, (October, 1998).

[FCC76] Code of Federal Regulations, Title 47, Part 76, (October, 1998).

[ID-DHCP] ID-DHCP: Patrick, M., DHCP Relay Agent Information Option, IETF DHC Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-dhc-agent-options-10.txt, (work in progress).

[IEEE802] IEEE 802 (1990), *Local and Metropolitan Area Networks: Overview and Architecture.*

[IEEE802.1Q] IEEE 802.1Q (1996), *IEEE Draft Standard 802.1Q/D4 Draft Standard for Virtual Bridged Local Area Networks.*

[IMA] Internet Assigned Numbers Authority, Internet Multicast Addresses, http://www.isi.edu/in-notes/iana/assignments/multicast-addresses.

[ISO-169-24] ISO-169-24 F connector, female, indoor.

[ISO8025] ISO 8025:1987, *Information processing systems – Open Systems Interconnection – Specification of the Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

[ISO/IEC8802-2] ISO/IEC 8802-2:1998 (IEEE 802.2 (1998)), *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control.*

[ISO/IEC8802-3] ISO/IEC 8802-3:2000 (IEEE 802.3 (2000)): *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.*

[ISO/IEC10038] ISO/IEC 10038:1993 (ANSI/IEEE 802.1D (1993)), *Information technology – Telecommunications and information exchange between systems – Local area networks – Media access control (MAC) bridges.*

[ISO/IEC10039] ISO/IEC 10039:1991, *Information technology – Open Systems Interconnection – Local area networks – Medium Access Control (MAC) service definition.*

[ISO/IEC15802-1] ISO/IEC 15802-1:1995, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 1: Medium Access Control (MAC) service definition.*

[ITU-T H.222.0] ITU-T Recommendation H.222.0 (2000) | ISO/IEC 13818-1:2000, *Information technology – Generic coding of moving pictures and associated audio information: Systems.*

[ITU-T J.83-C] ITU-T Recommendation J.83 (1997), Annex C, *Digital multi-programme systems for television, sound and data services for cable distribution.*

[ITU-T X.25] ITU-T Recommendation X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*

[ITU-T Z.100] ITU-T Recommendation Z.100 (2002), *CCITT Specification and description language (SDL).*

[RFC 791] IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification.*

[RFC 826] IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol-or-Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware.*

[RFC 868] IETF RFC 868 (1983), *Time Protocol.*

[RFC 1042] IETF RFC 1042 (1988), *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks.*

[RFC 1058] IETF RFC 1058 (1988), *Routing Information Protocol.*

[RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support.*

[RFC 1157] IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP).*

[RFC 1350] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2).*

[RFC 1493] IETF RFC 1493 (1993), *Definitions of Managed Objects for Bridges.* (Obsoletes RFC 1286).

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

[RFC 1700] IETF RFC 1700 (1994), *Assigned Numbers.*

[RFC 1812] IETF RFC 1812 (1995), Baker, F., *Requirements for IP Version 4 Routers.*

[RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication.*

[RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*

[RFC 2132] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions.*

[RFC 2210] IETF RFC 2210 (1997), *The Use of RSVP with the IETF Integrated Services.*

[RFC 2211] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service.*

[RFC 2212] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.

[RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

[RFC 2349] IETF RFC 2349 (1998), *TFTP Timeout Interval and Transfer Size Options*.

[RFC 2669] IETF RFC 2669 (1999), *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*.

[RFC 2786] IETF RFC 2786 (2000), *Diffie-Helman USM Key Management Information Base and Textual Convention*.

[RFC 3046] IETF RFC 3046 (2001), *DHCP relay agent information option.*

[SHA] NIST, FIPS PUB 180-1 (1995), *Secure Hash Standard*.

[SMS] *The Spectrum Management Application (SMA) and the Common Spectrum Management Interface (csmi)*, Time Warner Cable, December 24, 1995.

C.3 Definitions and Abbreviations

C.3.1 Definitions

This annex defines the following terms:

C.3.1.1 active service flow: Admitted Service Flow from the CM to the CMTS which is available for packet transmission.

C.3.1.2 Address Resolution Protocol (ARP): Protocol of the IETF for converting network addresses to 48 bit Ethernet addresses.

C.3.1.3 admitted service flow: Service Flow, either provisioned or dynamically signalled, which is authorized and for which resources have been reserved but is not active.

C.3.1.4 Asynchronous Transfer Mode (ATM): Protocol for the transmission of a variety of digital signals using uniform 53-byte cells.

C.3.1.5 authorization module: Authorization module is an abstract module that the CMTS can contact to authorize Service Flows and Classifiers. The authorization module tells the CMTS whether the requesting CM is authorized for the resources it is requesting.

C.3.1.6 availability: In cable television systems, availability is the long-term ratio of the actual RF channel operation time to scheduled RF channel operation time (expressed as a percent value) and is based on a bit error rate (BER) assumption.

C.3.1.7 bandwidth allocation map: The MAC Management Message that the CMTS uses to allocate transmission opportunities to CMs.

C.3.1.8 Bridge Protocol Data Unit (BPDU): Spanning tree protocol messages as defined in [RFC 1350].

C.3.1.9 broadcast addresses: Predefined destination address that denotes the set of all data network service access points.

C.3.1.10 burst error second: Any Errored Second containing at least 100 errors.

C.3.1.11 Cable Modem (CM): Modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.

C.3.1.12 Cable Modem Termination System (CMTS): Cable modem termination system, located at the cable television system headend or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.

C.3.1.13 Cable Modem Termination System – Network Side Interface (CMTS-NSI): The interface, defined in "DataOver-Cable Service Interface Specifications, Cable Modem Termination System Network Side Interface Specification, SP-CMTS-NSI-I01-960702", between a CMTS and the equipment on its network side.

C.3.1.14 Cable Modem to CPE Interface (CMCI): The interface between a CM and CPE.

C.3.1.15 carrier hum modulation: The peak-to-peak magnitude of the amplitude distortion relative to the RF carrier signal level due to the fundamental and low-order harmonics of the power-supply frequency.

C.3.1.16 Carrier-to-Noise Ratio (C/N or CNR): The square of the ratio of the root mean square (rms) of the voltage of the digitally-modulated RF carrier to the rms of the continuous random noise voltage in the defined measurement bandwidth. (If not specified explicitly, the measurement bandwidth is the symbol rate of the digital modulation; for video it is 4 MHz).

C.3.1.17 classifier: Set of criteria used for packet matching according to TCP, UDP, IP, LLC, and/or 802.1P/Q packet fields. A classifier maps each packet to a Service Flow. A Downstream Classifier is used by the CMTS to assign packets to downstream service flows. An Upstream Classifier is used by the CM to assign packets to upstream service flows.

C.3.1.18 Composite Second Order Beat (CSO): The peak of the average level of distortion products due to second-order non-linearities in cable system equipment.

C.3.1.19 Composite Triple Beat (CTB): The peak of the average level of distortion components due to third-order non-linearities in cable system equipment.

C.3.1.20 cross-modulation: Form of television signal distortion where modulation from one or more television channels is imposed on another channel or channels.

C.3.1.21 customer: See End User (C.3.1.29).

C.3.1.22 Customer Premises Equipment (CPE): Equipment at the end user's premises; MAY be provided by the end user or the service provider.

C.3.1.23 data link layer: Layer 2 in the Open System Interconnection (OSI) architecture; the layer that provides services to transfer data over the transmission link between open systems.

C.3.1.24 distribution hub: Location in a cable television network which performs the functions of a Headend for customers in its immediate area, and which receives some or all of its television program material from a Master Headend in the same metropolitan or regional area.

C.3.1.25 downstream: In cable television, the direction of transmission from the headend to the subscriber.

C.3.1.26 drop cable: Coaxial cable that connects to a residence or service location from a directional coupler (tap) on the nearest coaxial feeder cable.

C.3.1.27 Dynamic Host Configuration Protocol (DHCP): Internet protocol used for assigning network-layer (IP) addresses.

C.3.1.28 dynamic range: The ratio between the greatest signal power that can be transmitted over a multichannel analog transmission system without exceeding distortion or other performance limits, and the least signal power that can be utilized without exceeding noise, error rate or other performance limits.

C.3.1.29 end user: Human being, organization, or telecommunication system that accesses the network in order to communicate via the services provided by the network.

C.3.1.30 errored second: Any 1-second interval containing at least one bit error.

C.3.1.31 feeder cable: Coaxial cables that run along streets within the served area and connect between the individual taps which serve the customer drops.

C.3.1.32 Fiber Distributed Data Interface (FDDI): Fiber-based LAN standard.

C.3.1.33 fiber node: Point of interface between a fiber trunk and the coaxial distribution.

C.3.1.34 forward channel: The direction of RF signal flow away from the headend toward the end user; equivalent to Downstream.

C.3.1.35 group delay: The difference in transmission time between the highest and lowest of several frequencies through a device, circuit or system.

C.3.1.36 guard time: Minimum time allocated between bursts in the upstream referenced from the symbol center of the last symbol of a burst to the symbol center of the first symbol of the following burst. The guard time be at least the duration of five symbols plus the maximum system timing error.

C.3.1.37 Harmonic Related Carrier (HRC): Method of spacing television channels on a cable television system in exact 6 MHz increments, with all carrier frequencies harmonically related to a common reference.

C.3.1.38 headend: The central location on the cable network that is responsible for injecting broadcast video and other signals in the downstream direction. See also Master Headend, Distribution Hub.

C.3.1.39 header: Protocol control information located at the beginning of a protocol data unit.

C.3.1.40 High Frequency (HF): Used in this annex to refer to the entire subsplit (5 MHz to 30 MHz) and extended subsplit (5 MHz to 42 MHz) band used in reverse channel communications over the cable television network.

C.3.1.41 high return: Frequency division scheme that allows bi-directional traffic on a single coaxial cable. Reverse channel signals propagate to the headend above the downstream passband.

C.3.1.42 hum modulation: Undesired modulation of the television visual carrier by the fundamental or low-order harmonics of the power supply frequency, or other low-frequency disturbances.

C.3.1.43 Hybrid Fiber/Coax (HFC) system: Broadband bidirectional shared-media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.

C.3.1.44 Incremental Related Carriers (IRC): Method of spacing NTSC television channels on a cable television system in which all channels except 5 and 6 correspond to the standard channel plan, used to reduce composite triple beat distortions.

C.3.1.45 Institute of Electrical and Electronic Engineers (IEEE): Voluntary organization which, among other things, sponsors standards committees and is accredited by the American National Standards Institute.

C.3.1.46 International Electrotechnical Commission (IEC): International standards body.

C.3.1.47 International Organization for Standardization (ISO): International standards body, commonly known as the International Standards Organization.

C.3.1.48 Internet Control Message Protocol (ICMP): Internet network-layer protocol.

C.3.1.49 Internet Engineering Task Force (IETF): Body responsible, among other things, for developing standards used in the Internet.

C.3.1.50 Internet Group Management Protocol (IGMP): Network-layer protocol for managing multicast groups on the Internet.

C.3.1.51 impulse noise: Noise characterized by non-overlapping transient disturbances.

C.3.1.52 information element: The fields that make up a MAP and define individual grants, deferred grants, etc.

C.3.1.53 Internet Protocol (IP): Internet network-layer protocol.

C.3.1.54 interval usage code (IUC): Field in MAPs and UCDs to link burst profiles to grants.

C.3.1.55 latency: The time, expressed in quantity of symbols, taken for a signal element to pass through a device.

C.3.1.56 layer: Subdivision of the Open System Interconnection (OSI) architecture, constituted by subsystems of the same rank.

C.3.1.57 Local Area Network (LAN): Non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

C.3.1.58 Logical Link Control (LLC) procedure: In a local area network (LAN) or a Metropolitan Area Network (MAN), that part of the protocol that governs the assembling of data link layer frames and their exchange between data stations, independent of how the transmission medium is shared.

C.3.1.59 master headend: Headend which collects television program material from various sources by satellite, microwave, fiber and other means, and distributes this material to Distribution Hubs in the same metropolitan or regional area. A Master Headend MAY also perform the functions of a Distribution Hub for customers in its own immediate area.

C.3.1.60 Mean Time to Repair (MTTR): In cable television systems, the MTTR is the average elapsed time from the moment a loss of RF channel operation is detected up to the moment the RF channel operation is fully restored.

C.3.1.61 Media Access Control (MAC) address: The "built-in" hardware address of a device connected to a shared medium.

C.3.1.62 Media Access Control (MAC) procedure: In a subnetwork, that part of the protocol that governs access to the transmission medium independent of the physical characteristics of the medium, but taking into account the topological aspects of the subnetworks, in order to enable the exchange of data between nodes. MAC procedures include framing, error protection, and acquiring the right to use the underlying transmission medium.

C.3.1.63 Media Access Control (MAC) sublayer: The part of the data link layer that supports topology-dependent functions and uses the services of the Physical Layer to provide services to the logical link control (LLC) sublayer.

C.3.1.64 micro-reflections: Echoes in the forward transmission path due to departures from ideal amplitude and phase characteristics.

C.3.1.65 mid split: Frequency division scheme that allows bidirectional traffic on a single coaxial cable. Reverse channel signals propagate to the headend. Forward path signals go from the headend.

C.3.1.66 mini-slot: "Mini-slot" is an integer multiple of 64/9.216 microsecond increments. The relationship between mini-slots, bytes and time ticks is described in C.9.3.4.

C.3.1.67 Moving Picture Experts Group (MPEG): Voluntary body which develops standards for digital compressed moving pictures and associated audio.

C.3.1.68 multipoint access: User access in which more than one terminal equipment is supported by a single network termination.

C.3.1.69 multipoint connection: Connection among more than two data network terminations.

C.3.1.70 National Cable Television Association (NCTA): Voluntary association of cable television operators which, among other things, provides guidance on measurements and objectives for cable television systems in the USA.

C.3.1.71 National Television Systems Committee (NTSC): Committee which defined the analog color television broadcast standard used today in North America.

C.3.1.72 network layer: Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.

C.3.1.73 network management: The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

C.3.1.74 Open Systems Interconnection (OSI): Framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

C.3.1.75 Organizationally Unique Identifier (OUI): 3-octet IEEE assigned identifier that can be used to generate Universal LAN MAC addresses and Protocol Identifiers per [IEEE802] for use in Local and Metropolitan Area Network applications.

C.3.1.76 Packet Identifier (PID): Unique integer value used to identify elementary streams of a program in a single- or multi-program MPEG-2 stream.

C.3.1.77 partial grant: Grant that is smaller than the corresponding bandwidth request from the CM.

C.3.1.78 payload header suppression: The suppression of the header in a payload packet. (e.g. the suppression of the Ethernet header in forwarded packets).

C.3.1.79 Payload Unit Start Indicator (PUSI): Flag in an MPEG header. A value of 1 indicates the presence of a pointer field as the first byte of the payload.

C.3.1.80 physical (PHY) layer: Layer 1 in the Open System Interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical and handshaking procedures.

C.3.1.81 Physical Media Dependent (PMD) sublayer: Sublayer of the Physical Layer which is concerned with transmitting bits or groups of bits over particular types of transmission link between open systems and which entails electrical, mechanical and handshaking procedures.

C.3.1.82 primary service flow: All CMs have a Primary Upstream Service Flow and a Primary Downstream Service Flow. They ensure that the CM is always manageable and they provide a default path for forwarded packets that are not classified to any other Service Flow.

C.3.1.83 Program-Specific Information (PSI): In MPEG-2, normative data necessary for the demultiplexing of Transport Streams and the successful regeneration of programs.

C.3.1.84 program stream: In MPEG-2, a multiplex of variable-length digital video and audio packets from one or more program sources having a common time-base.

C.3.1.85 protocol: Set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions.

C.3.1.86 provisioned service flow: Service Flow that has been provisioned as part of the Registration process, but has not yet been activated or admitted. It may still require an authorization exchange with a policy module or external policy server prior to admission.

C.3.1.87 QoS parameter set: The set of Service Flow Encodings that describe the Quality of Service attributes of a Service Flow or a Service Class. (Refer to C.C.2.2.5.)

C.3.1.88 Quadrature Amplitude Modulation (QAM): Method of modulating digital signals onto a radio-frequency carrier signal involving both amplitude and phase coding.

C.3.1.89 Quadrature Phase-Shift Keying (QPSK): Method of modulating digital signals onto a radio-frequency carrier signal using four phase states to code two digital bits.

C.3.1.90 Radio Frequency (RF): In cable television systems, this refers to electromagnetic signals in the range 5 to 1000 MHz.

C.3.1.91 Request For Comments (RFC): Technical policy document of the IETF; these documents can be accessed on the World Wide Web at http://ds.internic.net/ds/rfcindex.html.

C.3.1.92 return loss: The parameter describing the attenuation of a guided wave signal (e.g., via a coaxial cable) returned to a source by a device or medium resulting from reflections of the signal generated by the source.

C.3.1.93 reverse channel: The direction of signal flow towards the headend, away from the subscriber; equivalent to Upstream.

C.3.1.94 Routing Information Protocol (RIP): Protocol of the IETF for exchanging routing information about IP networks and subnets.

C.3.1.95 Service Access Point (SAP): The point at which services are provided by one layer, or sublayer to the layer immediately above it.

C.3.1.96 security association identifier: Baseline Privacy security identifier between a CMTS and a CM.

C.3.1.97 Service Data Unit (SDU): Information that is delivered as a unit between peer service access points.

C.3.1.98 service class: Set of queuing and scheduling attributes that is named and that is configured at the CMTS. A Service Class is identified by a Service Class Name. A Service Class has an associated QoS Parameter Set.

C.3.1.99 service class name: ASCII string by which a Service Class may be referenced in modem configuration files and protocol exchanges.

C.3.1.100 service flow: A MAC-layer transport service which: Provides unidirectional transport of packets from the upper layer service entity to the RF; Shapes, polices, and prioritizes traffic according to QoS traffic parameters defined for the Flow.

C.3.1.101 Service Flow Identifier (SFID): Identifier assigned to a service flow by the CMTS. (32 bits).

C.3.1.102 Service Identifier (SID): Service Flow Identifier assigned by the CMTS (in addition to a Service Flow Identifier) to an Active or Admitted Upstream Service Flow. (14 bits).

C.3.1.103 service flow reference: Message parameter in Configuration Files and Dynamic Service MAC messages used to associate Classifiers and other objects in the message with the Service Flow Encodings of a requested Service Flow.

C.3.1.104 Simple Network Management Protocol (SNMP): Network management protocol of the IETF.

C.3.1.105 Spectrum Management System (SMS): System, defined in [SMS], for managing the RF cable spectrum.

C.3.1.106 sublayer: Subdivision of a layer in the Open System Interconnection (OSI) reference model.

C.3.1.107 subnetwork: Subnetworks are physically formed by connecting adjacent nodes with transmission links.

C.3.1.108 Subnetwork Access Protocol (SNAP): Extension of the LLC header to accommodate the use of 802-type networks as IP networks.

C.3.1.109 subscriber: See end User (C.3.1.29).

C.3.1.110 subsystem: Element in a hierarchical division of an Open System that interacts directly with elements in the next higher division or the next lower division of that open system.

C.3.1.111 systems management: Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.

C.3.1.112 tick: 6.9444…. microsecond time intervals that are the reference for upstream mini-slot definition and upstream transmission times.

C.3.1.113 tilt: Maximum difference in transmission gain of a cable television system over a given bandwidth (typically the entire forward operating frequency range).

C.3.1.114 transit delay: The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

C.3.1.115 Transmission Control Protocol (TCP): Transport-layer Internet protocol which ensures successful end-to-end delivery of data packets without error.

C.3.1.116 transmission convergence sublayer: Sublayer of the Physical Layer that provides an interface between the Data Link Layer and the PMD Sublayer.

C.3.1.117 transmission link: The physical unit of a subnetwork that provides the transmission connection between adjacent nodes.

C.3.1.118 transmission medium: The material on which information signals may be carried; e.g., optical fiber, coaxial cable, and twisted-wire pairs.

C.3.1.119 transmission system: The interface and transmission medium through which peer physical layer entities transfer bits.

C.3.1.120 transmit on/off ratio: In multiple-access systems, the ratio between the signal powers sent to line when transmitting and when not transmitting.

C.3.1.121 transport stream: In MPEG-2, a packet-based method of multiplexing one or more digital video and audio streams having one or more independent time bases into a single stream.

C.3.1.122 Trivial File-Transfer Protocol (TFTP): Internet protocol for transferring files without the requirement for user names and passwords that is typically used for automatic downloads of data and software.

C.3.1.123 trunk cable: Cables that carry the signal from the headend to groups of subscribers. The cables can be either coaxial or fiber depending on the design of the system.

C.3.1.124 Type/Length/Value (TLV): Encoding of three fields, in which the first field indicates the type of element, the second the length of the element, and the third field the value.

C.3.1.125 upstream: The direction from the subscriber location toward the headend.

C.3.1.126 Upstream Channel Descriptor (UCD): The MAC Management Message used to communicate the characteristics of the upstream physical layer to the cable modems.

C.3.2 Abbreviations

This annex uses the following abbreviations:

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BPDU	Bridge Protocol Data Unit
BPKM	Baseline Privacy Key Management
CM	Cable Modem
CMCI	Cable Modem to CPE Interface
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CSO	Composite Second Order Beat
CTB	Composite Triple Beat
DHCP	Dynamic Host Configuration Protocol
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSD	Dynamic Service Deletion
EIA	Electronic Industries Association
FDDI	Fiber Distributed Data Interface
HF	High Frequency
HFC	Hybrid-Fiber/Coax
HRC	Harmonic Related Carrier
ICMP	Internet Control Message Protocol
IE	Information Element
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRC	Incremental Related Carriers
ISO	International Organization for Standardization
IUC	Interval Usage Code
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAP	Bandwidth Allocation Map
MPEG	Moving Picture Experts Group

MSAP	MAC Service Access Point
MTTR	Mean Time to Repair
NCTA	National Cable Television Association
NTSC	National Television Systems Committee
OSI	Open System Interconnection
OUI	Organizationally Unique Identifier
PHS	Payload Header Supression
PHY	Physical (PHY) Layer
PID	Packet Identifier
PMD	Physical Media Dependent
PSI	Program-Specific Information
PUSI	Payload Unit Start Indicator
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
RF	Radio Frequency
RFC	Request For Comments
RIP	Routing Information Protocol
SAID	Security Association Identifier
SAP	Service Access Point
SDU	Service Data Unit
SFID	Service Flow Identifier
SID	Service Identifier
SMS	Spectrum Management System
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File-Transfer Protocol
TLV	Type/Length/Value
UCD	Upstream Channel Descriptor

C.3.3 Conventions

If this annex is implemented, the key words "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of this annex.

The key words indicating a certain level of significance of a particular requirements that are used throughout this annex are summarized below.

"MUST" This word or the adjective "REQUIRED" means that the item is an absolute requirement of this annex.

"MUST NOT" This phrase means that the item is an absolute prohibition of this annex.

"SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY" This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

C.4 Functional assumptions

This clause describes the characteristics of cable television plant to be assumed for the purpose of operating a data-over-cable system. It is not a description of CMTS or CM parameters. The data-over-cable system shall be interoperable within the environment described in this clause.

Whenever any reference in this clause to frequency plans or compatibility with other services conflicts with any legal requirement for the area of operation, the latter shall take precedence. Any reference to NTSC analogue signals in 6 MHz channels does not imply that such signals are physically present.

C.4.1 Broadband access network

A coaxial-based broadband access network is assumed. This MAY take the form of either an all-coax or hybrid- fiber/coax (HFC) network. The generic term "cable network" is used here to cover all cases.

A cable network uses a shared-medium, tree-and-branch architecture with analog transmission. The key functional characteristics assumed in this annex are the following:

- two-way transmission;
- maximum optical/electrical spacing between the CMTS and the most distant CM of 160 km, although typical maximum separation may be 16 to 24 km;
- a maximum differential optical/electrical spacing between the CMTS and the closest and most distant modems of 160 km, although this would typically be limited to 24 km.

C.4.2 Equipment assumptions

C.4.2.1 Frequency plan

In the downstream direction, the cable system is assumed to have a passband with a lower edge 70 MHz and an upper edge that is implementation-dependent but is typically in the range of 350 MHz to 770 MHz. Within that passband, NTSC analog television signals in 6 MHz channels are assumed to be present on the standard, Japan frequency plans, as well as other narrowband and wideband digital signals.

In the upstream direction, the cable system MAY have a subsplit (10 MHz to 55 MHz) passband. NTSC analog television signals in 6 MHz channels MAY be present, as well as other signals.

C.4.2.2 Compatibility with other services

The CM and CMTS MUST coexist with the other services on the cable network. In particular:

a) they MUST be interoperable in the cable spectrum assigned for CMTS-CM interoperation while the balance of the cable spectrum is occupied by any combination of television and other signals; and

b) they MUST NOT cause harmful interference to any other services that are assigned to the cable network in spectrum outside of that allocated to the CMTS.

The latter is understood as:

- no measurable degradation (highest level of compatibility);
- no degradation below the perceptible level of impairments for all services (standard or medium level of compatibility); or
- no degradation below the minimal standards accepted by the industry or other service provider (minimal level of compatibility).

C.4.2.3 Fault isolation impact on other users

As the data-over-cable system is a shared media, point-to-multipoint system, fault isolation procedures SHOULD take into account the potential harmful impact of faults and fault isolation procedures on numerous users of the data-over-cable and other services.

For the interpretation of harmful impact, see C.4.2.2.

C.4.3 RF channel assumptions

The data-over-cable system, configured with at least one set of defined physical layer parameters (e.g., modulation, forward error correction, symbol rate, etc.) from the range of configuration settings described in this annex, MUST be interoperable on cable networks having characteristics defined in this subclause in such a manner that the forward error correction provides for equivalent operation in a cable system both with and without the impaired channel characteristics described below.

C.4.3.1 Transmission downstream

The RF channel transmission characteristics of the cable network in the downstream direction are described in Table C.4-1.

Table C.4-1/J.112 – Assumed downstream RF channel transmission characteristics (see Note 1)

Parameter	Value
Frequency range	Cable system normal downstream operating range is from 90 MHz to as high as 770 MHz.
RF channel spacing (design bandwidth)	6 MHz
Transit delay from headend to most distant customer	≤ 0.800 ms (typically much less)
Carrier-to-noise ratio in a 6 MHz band	Not less than 26 dBrms(@5.274 MHz) for 64-QAM Not less than 33 dBrms(@5.274 MHz) for 256-QAM (Note 2)
Carrier-to-Composite triple beat distortion ratio	Not less than 40 dBrms for 64-QAM Not less than 51 dBrms for 256-QAM (Note 2)
Carrier-to-any other discrete interference (ingress)	Not less than 26 dBrms for 64-QAM Not less than 33 dBrms for 256-QAM (Note 2)
Amplitude ripple	3 dB within the design bandwidth
Micro reflections bound for dominant echo	Figure C.4-1
Maximum analog video carrier level at the CM input	85 dBμVpeak
Maximum number of carriers	111 (770 MHz System)
NOTE 1 – Transmission is from the headend combiner to the CM input at the customer location. NOTE 2 – Measured relative to a QAM signal level (rms) that is −10 dB for 64-QAM, −4 dB for 256-QAM to the nominal video level (peak) in the plant.	

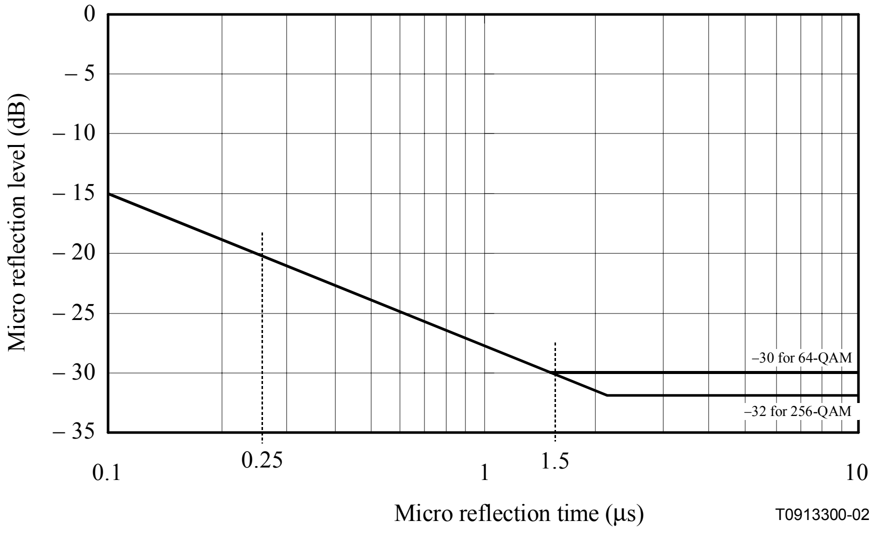


Figure C.4-1/J.112 – Micro reflections bound for dominant echo

C.4.3.2 Transmission upstream

The RF channel transmission characteristics of the cable network in the upstream direction are described in Table C.4-2. All conditions are present concurrently. No combination of the following parameters will exceed any stated interface limit defined elsewhere in this annex.

Table C.4-2/J.112 – Assumed upstream RF channel transmission characteristics (see Note 1)

Parameter	Value
Frequency range	10 MHz to 55 MHz edge to edge
Transit delay from the most distant CM to the nearest CM or CMTS	≤ 0.800 ms (typically much less)
Carrier-to-interference plus ingress (the sum of noise, distortion, common path distortion and cross modulation and the sum of discrete and broadband ingress signals, impulse noise excluded) ratio	Not less than 25 dB (Note 2)
Carrier hum modulation	Not greater than −23 dBc (7.0%)
Burst noise	Not longer than 10 μs at a 1 kHz average rate for most cases (Notes 3 and 4)
Amplitude ripple 10 MHz to 55 MHz:	0.5 dB/MHz
Group delay ripple 10 MHz to 55 MHz:	200 ns/MHz
Micro reflections – single echo	−10 dB @ ≤ 0.5 μs −20 dB @ ≤ 1.0 μs −30 dB @ > 1.0 μs
Seasonal and diurnal reverse gain (loss) variation	Not greater than 14 dB min to max

NOTE 1 – Transmission is from the CM output at the customer location to the headend.

NOTE 2 – Ingress avoidance or tolerance techniques may be used to ensure operation in the presence of time varying discrete ingress signals that could be as high as 10 dBc. The ratios are guaranteed only within the digital carrier channels.

NOTE 3 – Amplitude and frequency characteristics sufficiently strong to partially or wholly mask the data carrier.

NOTE 4 – Impulse noise levels more prevalent at lower frequencies (< 15 MHz).

C.4.4 Transmission levels

The nominal power level of the downstream CMTS signal(s) within a 6 MHz channel is targeted to be in the range −10 dBc to −6 dBc relative to analog video carrier level and will normally not exceed analog video carrier level. The 256-QAM downstream carrier level SHOULD be carefully chosen from two reasons. One is to avoid any interference to the adjacent analog video carrier, the other is to maintain required carrier-to-noise ratio. Normally the 256-QAM downstream signal MAY NOT be allocated to any channels that are adjacent to analog video carrier.

The nominal power level of the upstream CM signal(s) will be as low as possible to achieve the required margin above noise and interference. Uniform power loading per unit bandwidth is commonly followed in setting upstream signal levels, with specific levels established by the cable network operator to achieve the required carrier-to-noise and carrier-to-interference ratios.

C.4.5 Frequency inversion

There will be no frequency inversion in the transmission path in either the downstream or upstream directions, i.e., a positive change in frequency at the input to the cable network will result in a positive change in frequency at the output.

C.5 Communication protocols

This clause provides a high level overview of the communication protocols that must be used in the data-over-cable system. Detailed specifications for the physical media dependent, downstream transmission, and media access control sublayers are provided in clauses C.6, C.7 and C.8, respectively.

C.5.1 Protocol stack

The CM and CMTS operate as forwarding agents and also as end systems (hosts). The protocol stacks used in these modes differ as shown below.

The principal function of the cable modem system is to transmit Internet Protocol (IP) packets transparently between the headend and the subscriber location. Certain management functions also ride on IP, so that the protocol stack on the cable network is as shown in Figure C.5-1 (this does not restrict the generality of IP transparency between the headend and the customer). These management functions include, for example, supporting spectrum management functions and the downloading of software.

C.5.1.1 CM and CMTS as hosts

CMs and CMTSs will operate as IP and LLC hosts in terms of [IEEE802] for communication over the cable network. The protocol stack at the CM and CMTS RF interfaces is shown in Figure C.5-1.

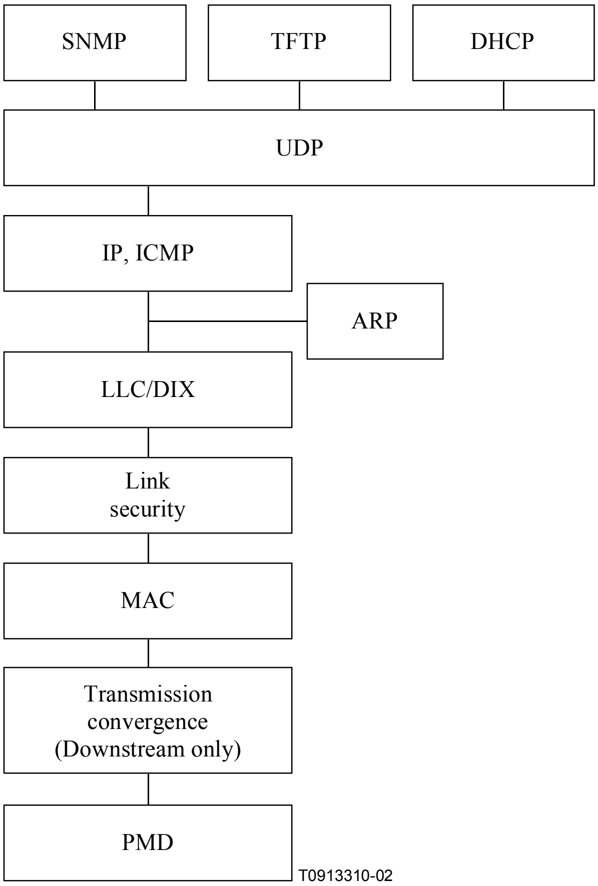


Figure C.5-1/J.112 – Protocol stack on the RF interface

The CM and CMTS MUST function as IP hosts. As such, the CM and CMTS MUST support IP and ARP over DIX link layer framing (see [DIX]). The CMTS MUST NOT transmit frames that are smaller than the DIX 64 byte minimum on a downstream channel (see Note). However, the CM MAY transmit frames that are smaller than the DIX 64 byte minimum on an upstream channel.

NOTE – Except as a result of Payload Header Suppression. Refer to C.10.4.

The CM and CMTS MAY also support IP and ARP over SNAP framing [RFC 1042].

The CM and CMTS also MUST function as LLC hosts. As such, the CM and CMTS MUST respond appropriately to TEST and XID requests per [ISO/IEC8802-2].

C.5.1.2 Data forwarding through the CM and CMTS

C.5.1.2.1 General

Data forwarding through the CMTS MAY be transparent bridging or MAY employ network layer forwarding (routing, IP switching) as shown in Figure C.5-2.

With the exception that for packet PDUs less than 64 bytes to be forwarded from the upstream RFI, a CMTS MUST pad out the packet PDU and recompute the CRC.

Data forwarding through the CM is link layer transparent bridging, as shown in Figure C.5-2. Forwarding rules are similar to [ISO/IEC10038] with the modifications described in clauses C.5.1.2.2 and C.5.1.2.3. This allows the support of multiple network layers.

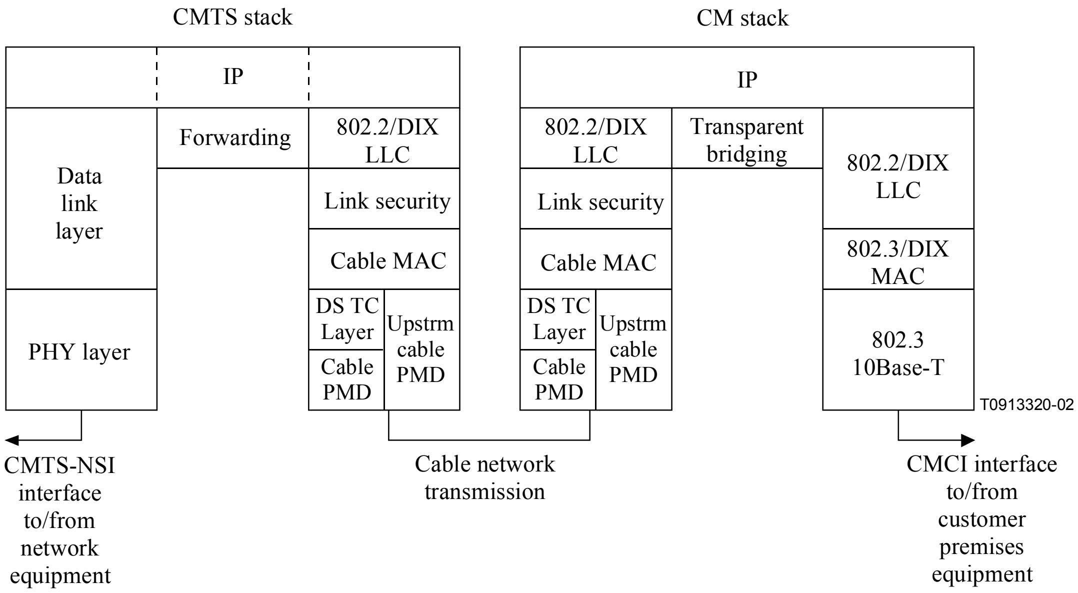


Figure C.5-2/J.112 – Data forwarding through the CM and CMTS

Forwarding of IP traffic MUST be supported. Other network layer protocols MAY be supported. The ability to restrict the network layer to a single protocol such as IP MUST be supported.

The IEEE 802.1D spanning tree protocol of [ISO/IEC10038] with the modifications described in Annex C.I MAY be supported by CMs intended for residential use. CMs intended for commercial use MUST support this version of spanning tree. CMs and CMTSs MUST include the ability to filter (and disregard) IEEE 802.1D BPDUs.

This annex assumes that CMs intended for residential use will not be connected in a configuration which would create network loops such as that shown in Figure C.5-3.

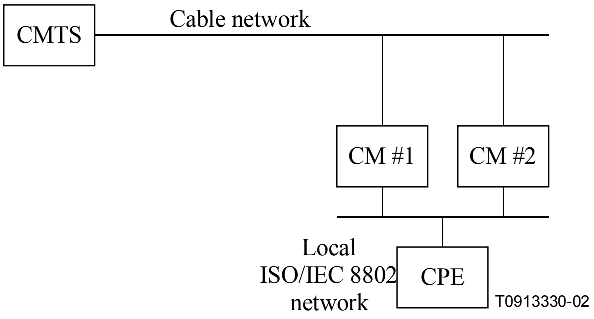


Figure C.5-3/J.112 – Example condition for network loops

C.5.1.2.2 CMTS forwarding rules

At the CMTS, if link layer forwarding is used, then it MUST conform to the following general IEEE 802.1D guidelines:

- link layer frames MUST NOT be duplicated;
- stale frames (those that cannot be delivered in a timely fashion) MUST be discarded;
- link layer frames, on a given Service Flow (refer to C.8.1.2.3), MUST be delivered in the order they are received.

The address learning and aging mechanisms used are vendor dependent.

If network layer forwarding is used, then the CMTS conform to IETF Router Requirements [RFC 1812] with respect to its CMTS-RFI and CMTS-NSI interfaces.

Conceptually, the CMTS forwards data packets at two abstract interfaces: between the CMTS-RFI and the CMTS-NSI, and between the upstream and downstream channels. The CMTS MAY use any combination of link layer (bridging) and network layer (routing) semantics at each of these interfaces. The methods used at the two interfaces need not be the same.

Forwarding between the upstream and downstream channels within a MAC layer differs from traditional LAN forwarding in that:

- a single channel is simplex, and cannot be considered a complete interface for most protocol (e.g., IEEE 802.1D spanning tree, Routing Information Protocol per [RFC 1058]) purposes;
- upstream channels are essentially point-to-point, whereas downstream channels are shared media;
- policy decisions may override full connectivity.

For these reasons, an abstract entity called the MAC Forwarder exists within the CMTS to provide connectivity between stations within a MAC domain (see C.5.2).

C.5.1.2.3 CM forwarding rules

Data forwarding through the CM is link layer bridging with the following specific rules.

C.5.1.2.3.1 CPE MAC address acquisition

- The CM MUST acquire Ethernet MAC addresses of connected CPE devices, either from the provisioning process or from learning, until the CM acquires its maximum number of CPE MAC addresses (a device dependent value). Once the CM acquires its maximum number of CPE MAC addresses, then newly discovered CPE MAC addresses MUST NOT replace previously acquired addresses. The CM must support acquisition of at least one CPE MAC address.

- The CM MUST allow configuration of CPE addresses during the provisioning process (up to its maximum number of CPE addresses) to support configurations in which learning is not practical nor desired.
- Addresses provided during the CM provisioning MUST take precedence over learned addresses.
- CPE addresses MUST NOT be aged out.
- In order to allow modification of user MAC addresses or movement of the CM, addresses are not retained in non volatile storage. On a CM reset (e.g. power cycle), all provisioned and learned addresses MUST be discarded.

C.5.1.2.3.2 Forwarding

CM forwarding in both directions MUST conform to the following general IEEE 802.1D guidelines:

- link layer frames MUST NOT be duplicated;
- stale frames (those that cannot be delivered in a timely fashion) MUST be discarded;
- link layer frames, on a given Service Flow (refer to C.8.1.2.3), MUST be delivered in the order they are received.

Cable Network to Ethernet forwarding MUST follow the following specific rules:

- frames addressed to unknown destinations MUST NOT be forwarded from the cable port to the Ethernet port;
- broadcast frames MUST be forwarded to the Ethernet port, unless they are from source addresses which are provisioned or learned as supported CPE devices, in which case they MUST NOT be forwarded;
- the forwarding of multicast is controlled by administratively set parameters for the policy filter service and by a specific multicast tracking algorithm (refer to C.5.3.1). Multicast frames MUST NOT be forwarded unless both mechanisms are in a permissive state.

Ethernet to Cable Network forwarding MUST follow the following specific rules:

- frames addressed to unknown destinations MUST be forwarded from the Ethernet port to the cable port;
- broadcast frames MUST be forwarded to the cable port;
- multicast frames MUST be forwarded to the cable port in accordance with filtering configuration settings specified by the cable operator's operations and business support systems;
- frames from source addresses other than those provisioned or learned as supported CPE devices MUST NOT be forwarded;
- if a single user CM has acquired a MAC address (see C.5.1.2.3.1), it MUST NOT forward data from a second source. Other (non supported) CPE source addresses MUST be learned from the Ethernet port and this information used to filter local traffic as in a traditional learning bridge;
- if a single user CM has acquired MAC address A as its supported CPE device and learned B as a second device connected to the Ethernet port, it MUST filter any traffic from A to B.

C.5.2 The MAC forwarder

The MAC Forwarder is a MAC sublayer that resides on the CMTS just below the MAC service access point (MSAP) interface, as shown in Figure C.5-4. It is responsible for delivering upstream frames to:

- one or more downstream channels;

- the MSAP interface.

In Figure C.5-4, the LLC sublayer and link security sublayers of the upstream and downstream channels on the cable network terminate at the MAC Forwarder.

The MSAP interface user may be the NSI-RFI Forwarding process or the CMTS's host protocol stack.

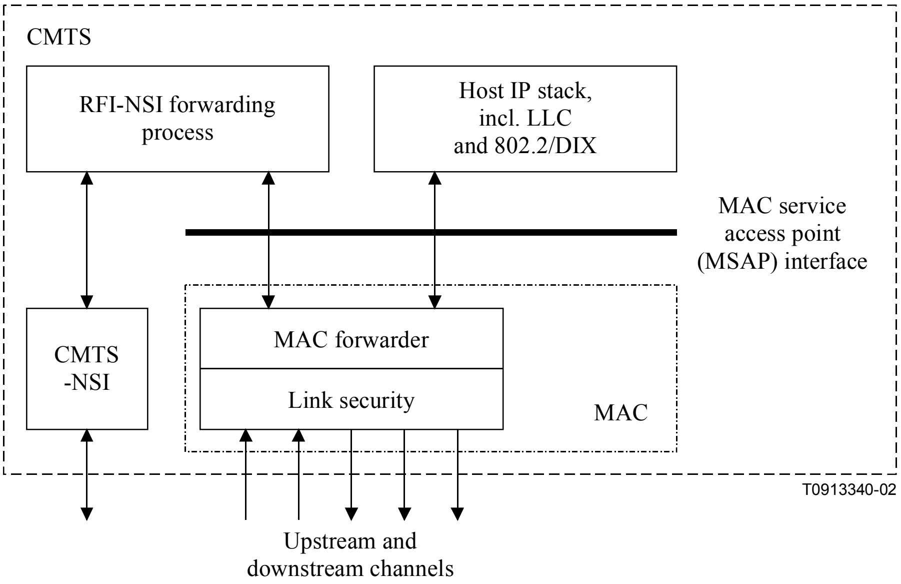

CMTS
RFI-NSI forwarding process
Host IP stack, incl. LLC and 802.2/DIX
MAC service access point (MSAP) interface
CMTS -NSI
MAC forwarder
Link security
MAC
T0913340-02
Upstream and downstream channels

Figure C.5-4/J.112 – MAC forwarder

Delivery of frames may be based on data link layer (bridging) semantics, network layer (routing) semantics, or some combination. Higher layer semantics may also be employed (e.g., filters on UDP port numbers). The CMTS MUST provide IP connectivity between hosts attached to cable modems, and MUST do so in a way that meets the expectations of Ethernet attached customer equipment. For example, the CMTS must either forward ARP packets or it must facilitate a proxy ARP service. The CMTS MAC Forwarder MAY provide service for non IP protocols.

Note that there is no requirement that all upstream and downstream channels be aggregated under one MSAP as shown above. The vendor could just as well choose to implement multiple MSAPs, each with a single upstream and downstream channel.

C.5.2.1 Rules for data link layer forwarding

If the MAC Forwarder is implemented using only data link layer semantics, then the requirements in this clause apply.

Delivery of frames is dependent on the Destination Address within the frame. The means of learning the location of each address is vendor dependent, and MAY include:

- transparent bridging like source address learning and aging;
- gleaning from MAC Registration Request messages;
- administrative means.

If the destination address of a frame is unicast, and that address is associated with a particular downstream channel, then the frame MUST be forwarded to that channel.

Vendors MAY implement extensions, similar to static addresses in IEEE 802.1D/ISO/IEC 10038 bridging, that cause such frames to be filtered or handled in some other manner.

If the destination address of a frame is unicast, and that address is known to reside on the other (upper) side of the MSAP interface, then the frame MUST be delivered to the MSAP interface.

If the destination address is broadcast, multicast, or unknown, the frame MUST be delivered to both the MSAP and to all downstream channels. (With the exception of the C.5.3.1.1 multicast forwarding rules).

All multicasts, including IEEE 802.1D/ISO/IEC 10038 Spanning Tree Bridge BPDU's, MUST be forwarded.

Delivery rules are similar to those for transparent bridging:

- frames MUST NOT be duplicated;
- frames that cannot be delivered in a timely fashion MUST be discarded;
- the Frame Check Sequence SHOULD be preserved rather than regenerated;
- frames, on a given Service Flow (refer to C.8.1.2.3), MUST be delivered in the order they are received.

C.5.3 Network layer

As stated above, the purpose of the data-over-cable system is to transport IP traffic transparently through the system.

The Network Layer protocol is the Internet Protocol (IP) version 4, as defined in RFC 791, and migrating to IP version 6.

This annex imposes no requirements for reassembly of IP packets.

C.5.3.1 Requirements for IGMP management

C.5.3.1.1 CMTS rules

- If link layer forwarding is used, the CMTS MUST forward all Membership Queries on all downstream channels using the appropriate 802.3 multicast group (e.g. 01:00:5E:xx:xx:xx where xx:xx:xx are the low order 23 bits of the multicast address expressed in hex notation). Refer to [IMA].
- The CMTS MUST forward the first copy of Solicited and Unsolicited Membership Reports for any given group received on its upstream RF interface to all of its downstream RF interfaces. However, if membership is managed on a per downstream RF interface basis, Membership Reports and IGMPv2 Leave messages MAY be forwarded only on the downstream interface to which the reporting CPE's CM is connected.
- The CMTS SHOULD suppress the transmission of additional Membership Reports (for any given group) downstream for at least the Query Response Interval. If the CMTS uses data link layer forwarding, it MUST also forward the Membership Report out all appropriate Network Side Interfaces.
- The CMTS SHOULD suppress the downstream transmission of traffic to any IP multicast group that does not have subscribers on that downstream RF interface (subject to any administrative controls).
- If the CMTS performs network layer forwarding of multicast packets, it MUST implement the router portion of the IGMP protocol [RFC 2236] and MUST act as the only IGMPv2 Querier on its downstream RF interfaces.

C.5.3.1.2 CM rules

The CM MUST support IGMP with the following cable specific rules. The following requirements apply to conformant CMs:

- The CM MUST NOT forward Membership Queries from its CPE interface to its RF interface.
- The CM MUST NOT forward Membership Reports or IGMPv2 Leaves received on its RF interface to its CPE interface.
- The CM MUST NOT forward multicast traffic from its RF interface to its CPE interface unless a device on its CPE interface is a member of that IP multicast group.
- The CM MUST forward multicast traffic from its CPE interface to its RF interface unless administratively (via configuration or other mechanism) prohibited.
- The CM MUST forward traffic for the ALL HOSTS multicast group from its RF interface to its CPE interface unless administratively prohibited. The CPE MUST always be considered a member of this group.
- The CM MUST forward ALL HOSTS Group Queries and Group Specific Queries that pass permit filters on its RF interface to its CPE interface or the CM MUST implement the Host portion of the IGMPv2 protocol [RFC 2236] on its RF interface for CPEs with active groups and MUST NOT act as a Querier on its RF interface. If the CM implements the Host portion of the IGMPv2 protocol, it MUST act as an IGMPv2 Querier on its CPE interface. The CM MUST NOT require any specific configuration for the associated multicast timer values and MUST be capable of adhering to the timers specified in this clause. The CM MAY provide configuration control that overrides the default values of these timers.
- The CM MUST derive the Membership Query Interval by looking at the inter arrival times of the Membership Query messages. Formally: If $n < 2$, MQI = 125 else MQI = MAX (125, $MQ_n - MQ_{n-1}$), where MQI is the Membership Query Interval in seconds, n is the number of Membership Queries seen, and 'MQ_n' is the epoch time at which the nth Membership Query was seen to the nearest second.
- The Query Response Interval is carried in the Membership Query packet. The Query Response Interval MUST be assumed to be 10 s if not otherwise set (or set to 0) in the Membership Query packet.
- As a result of receiving a Membership Report on its CPE interface, the CM MUST begin forwarding traffic for the appropriate IP multicast group. The CM MUST stop forwarding multicast traffic from the RF to the CPE side whenever the CM has not received a Membership Report from the CPE side for more than the Membership Interval, which is $(2 \times \text{MQI}) + \text{QRI}$, where MQI is the Membership Query Interval and QRI is the Query Response Interval.
- If the CM has received a Membership Report on its downstream RF interface for groups active on the CM's CPE interface within the Query Response Interval, it MUST suppress transmission on its upstream RF interface of all Membership Reports received on its CPE interface for that group.
- The CM MAY stop forwarding traffic from the RF to the CPE side for a particular multicast group prior to the expiration of the Membership Interval (see above) if it can determine (for example, via an IGMP 'LEAVE' message and the appropriate protocol exchange) that there are no CPE devices subscribed to that particular group.

- The CM MUST treat Unsolicited Membership Reports (IGMP 'JOIN's) from CPE as responses to a Membership Query received on its RF interface. Upon receipt of a JOIN from its CPE interface, the CM MUST start a random timer according to the Host State Diagram, specified in [RFC 2236], and MUST use a Query Response Interval of 10 s, as specified above. As specified above, if the CM receives a Membership Report on its RF interface for this group during this random time period, it MUST suppress transmission of this Join on its upstream RF interface. The CM MUST suppress all subsequent Membership Reports for this group until such time as the CM receives a Membership Query (General or Specific to this Group) on its RF interface or a IGMPv2 Leave is received for this group from the CPE interface.

Refer to Annex C.L for a state transition diagram example of an approach to these requirements.

NOTE – Nothing in this clause would prohibit the CM from being specifically configured to not forward certain multicast traffic as a matter of network policy.

C.5.4 Above the network layer

The subscribers will be able to use the transparent IP capability as a bearer for higher layer services. Use of these services will be transparent to the CM.

In addition to the transport of user data, there are several network management and operation capabilities which depend upon the Network Layer. These include:

- SNMP (Simple Network Management Protocol, [RFC 1157]), MUST be supported for network management;
- TFTP (Trivial File Transfer Protocol, [RFC 1350]), a file transfer protocol, MUST be supported for downloading software and configuration information, as modified by TFTP Timeout Interval and Transfer Size Options [RFC 2349];
- DHCP (Dynamic Host Configuration Protocol, [RFC 2131]), a framework for passing configuration information to hosts on a TCP/IP network, MUST be supported;
- Time of Day Protocol [RFC 868], MUST be supported to obtain the time of day.

C.5.5 Data link layer

The Data Link Layer is divided into sublayers in accordance with [IEEE802] with the addition of Link Layer security. The sublayers, from the top, are:

- Logical Link Control (LLC) sublayer (Class 1 only);
- Link Layer Security sublayer;
- Media Access Control (MAC) sublayer.

C.5.5.1 LLC sublayer

The LLC sublayer MUST be provided in accordance with [ISO/IEC10039]. Address resolution MUST be used as defined in [RFC 826]. The MAC-to-LLC service definition is specified in [ISO/IEC10039].

C.5.5.2 Link layer security sublayer

Link layer security MUST be provided in accordance with "Data-Over-Cable Service Interface Specifications, Baseline Privacy Interface Specification, SP-BPI-I03-010829", or MAY be provided in accordance with "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I05-000714".

C.5.5.3 MAC sublayer

The MAC sublayer defines a single transmitter for each downstream channel – the CMTS. All CMs listen to all frames transmitted on the downstream channel upon which they are registered and accept those where the destinations match the CM itself or CPEs reached via the CMCI port. CMs can communicate with other CMs only through the CMTS.

The upstream channel is characterized by many transmitters (CMs) and one receiver (the CMTS). Time in the upstream channel is slotted, providing for Time Division Multiple Access at regulated time ticks. The CMTS provides the time reference and controls the allowed usage for each interval. Intervals may be granted for transmissions by particular CMs, or for contention by all CMs. CMs may contend to request transmission time. To a limited extent, CMs may also contend to transmit actual data. In both cases, collisions can occur and retries are used.

Clause C.8 describes the MAC sublayer messages from the CMTS which direct the behavior of the CMs on the upstream channel, as well as messaging from the CMs to the CMTS.

C.5.6 Physical layer

The Physical (PHY) layer is comprised of two sublayers:

- Transmission Convergence sublayer (present in the downstream direction only);
- Physical Media Dependent (PMD) sublayer.

C.5.6.1 Downstream transmission convergence sublayer

The Downstream Transmission Convergence sublayer exists in the downstream direction only. It provides an opportunity for additional services over the physical layer bitstream. These additional services might include, for example, digital video. Definition of any such additional services is beyond the scope of this annex.

This sublayer is defined as a continuous series of 188 byte MPEG, [ITU-T H.222.0] packets, each consisting of a 4 byte header followed by 184 bytes of payload. The header identifies the payload as belonging to the data-over-cable MAC. Other values of the header may indicate other payloads. The mixture of payloads is arbitrary and controlled by the CMTS.

The Downstream Transmission Convergence sublayer is defined in clause C.7.

C.5.6.2 PMD sublayer

The Physical Media Dependent sublayer is defined in clause C.6.

C.5.6.2.1 Interface points

Three RF interface points are defined at the PMD sublayer:

1) downstream output on the CMTS;
2) upstream input on the CMTS;
3) cable in/out at the cable modem.

Separate downstream output and upstream input interfaces on the CMTS are required for compatibility with typical downstream and upstream signal combining and splitting arrangements in headends.

C.6 Physical layer specification

C.6.1 Upstream

C.6.1.1 Modulation method

QPSK and 16-QAM modulation method MUST be applied for upstream channel. Choice of QPSK or 16-QAM MUST be programmable.

C.6.1.2 Signal constellation diagram and phase shift rule

In Table C.6-1, I_n is in-phase component, while Q_n denotes quadrant component. I_1 means the MSB (Most Significant Bit) of the symbol map. Q_1 is the LSB (Least Significant Bit) for QPSK, and Q_0 is the LSB for 16-QAM. Q_1 and I_0 have intermediate bit positions in 16-QAM.

Table C.6-1/J.112 – Definition of I_n and Q_n

Modulation Method	Input Bit Definitions
QPSK	I_1 Q_1
16-QAM	I_1 Q_1 I_0 Q_0

The modulation mode (QPSK or 16-QAM) is programmable. CM and CMTS MUST provide differential-coded QPSK, non inverted (Gray-coded) 16-QAM and differential-coded 16-QAM. Figure C.6-1 shows the signal constellation diagram for QPSK modulation in general form, and Table C.6-2 provides the phase shift rule of differential-coding. Figure C.6-2 shows the signal constellation diagram for Gray-coded 16-QAM, and Figure C.6-3 depicts the diagram for differential-coded 16-QAM.

Table C.6-3 shows the phase shift rule of differential-coding for differential-coded 16-QAM.

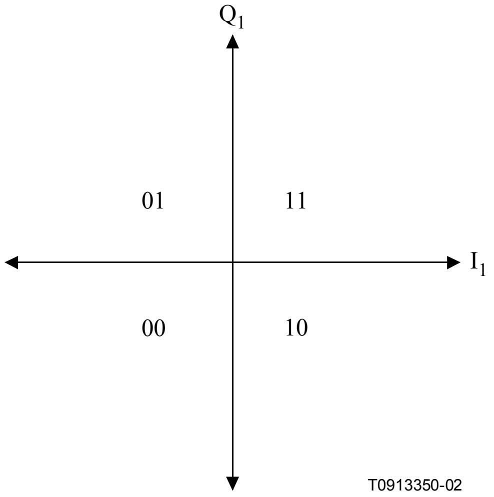


Figure C.6-1/J.112 – QPSK signal constellation diagram

Table C.6-2/J.112 – Phase shift rule for differential-coded QPSK

Input I_1 Q_1	Phase shift output
0 0	0 degree
0 1	+90 degrees
1 1	+180 degrees
1 0	+270 degrees

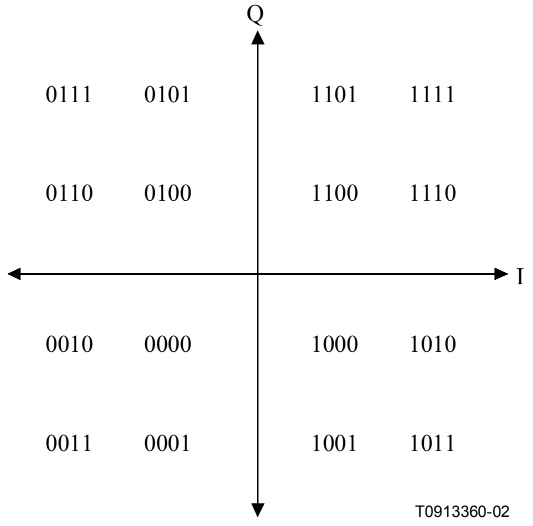


Figure C.6-2/J.112 – 16-QAM gray coded signal constellation diagram

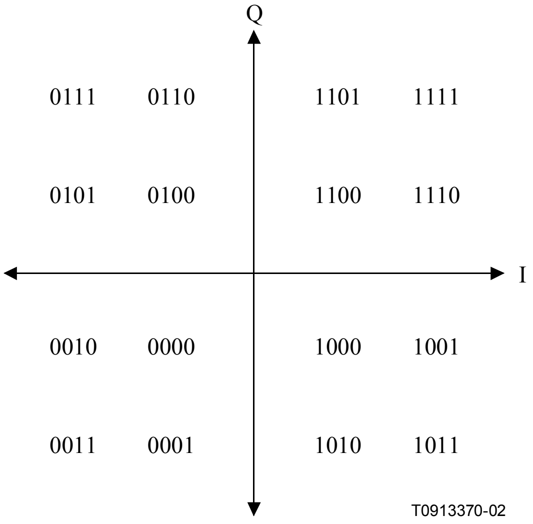


Figure C.6-3/J.112 – 16-QAM differential coded signal constellation diagram

Table C.6-3/J.112 – Phase shift rule for differential-coded 16-QAM

Input I_1 Q_1	Phase shift output
0 0	0 degree
0 1	+90 degrees
1 1	+180 degrees
1 0	+270 degrees

C.6.1.3 Symbol rate, bandwidth and roll off

In some countries, the upstream channel has been used to transmit several 6 MHz video signals. In order to utilize the limited bandwidth efficiently, the bandwidth of the upstream channel is strongly recommended to be integer-divided value of 6 MHz or 6 MHz/n.

The value "n" shall be carefully chosen to form a series of integer-related upstream bandwidths. Appropriate Roll Off value should be selected from the viewpoint of effective band separation and manufacturing. Furthermore, the preferable symbol rate should be multiples of 8 kHz, for synchronization with external transmission lines if required. The resulting values of "n" should be 2, 4, 8, 16 and 32. The Roll Off factor should be 25%.

Table C.6-4 summarizes Integer n, Bandwidth and Symbol Rate. The upstream channel MUST support all symbol rates shown below.

Table C.6-4/J.112 – Integer n, bandwidth and symbol rate

Integer n	6 MHz/n Bandwidth (kHz)	Symbol rate (ksym/s)
2	3000.0	2304
4	1500.0	1152
8	750.0	576
16	375.0	288
32	187.5	144

C.6.1.4 Frequency range

The upstream channel MUST support a 10 MHz to 55 MHz frequency range edge to edge.

C.6.1.5 Error correction

Error correction functionality SHOULD be considered for the noise environment in the cable television network.

A Reed-Solomon Code SHOULD be implemented as an error correction function for the upstream modulator.

The original Reed-Solomon code over GF (256) is defined as follows:

- Primitive polynomial: $p(X) = X^8 + X^4 + X^3 + X^2 + 1$
- Generator polynomial: $g(X) = (X + \alpha^0)(X + \alpha^1)$----------$(X + \alpha^{2T-1})$

where T is error correcting capability of a Reed-Solomon code and α is 02H and one of roots of equation $p(X) = 0$.

C.6.1.6 Randomization

The upstream modulator SHOULD provide a randomization function. The polynomial MUST be $X^{15} + X^{14} + 1$.

C.6.1.7 Transmission signal level

The transmitting signal level at CM Output connector MUST be adjustable over the range +68 to +118 dBµV for QPSK, +68 to +115 dBµV for 16-QAM. Level adjustment step MUST be 1dB.

C.6.1.8 Receiving signal level

The operational receiving signal level at CMTS Input connector MUST satisfy the values in Table C.6-5.

In the case that transmission level control is applied, signals can be received within a part of the range mentioned below.

Table C.6-5/J.112 – Symbol rate and nominal receive level

Symbol rate (ksym/s)	**Nominal receive level (dBµV)**
144	+44 to +72
288	+47 to +75
576	+50 to +78
1152	+53 to +81
2304	+56 to +84

C.6.1.9 Transmission spurious

The noise and spurious power MUST NOT exceed the values shown in Table C.6-6.

Table C.6-6/J.112 – Noise and spurious powers

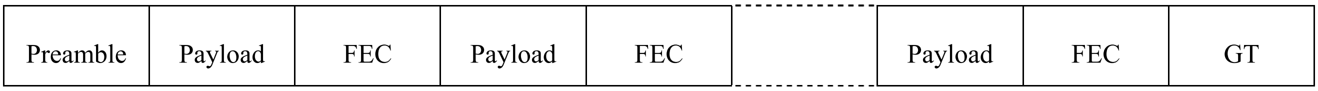
Frequency	**Active period**	**Inactive period**
10 to 55 MHz, Inband	Less than –40 dBc	Less than +25 dBµV
10 to 55 MHz, Outband including adjacent band, carrier-related band and other noise powers within 10 to 55 MHz	Less than –45 dBc	
55 to 70 MHz	Less than –45dBc	
70 to 90 MHz	Less than +35 dBµV	
90 to 770 MHz	Less than +25 dBµV	

C.6.1.10 Bit error rate

Bit error rate of the upstream signal MUST be less than 10^{-6} without error correction when operating at CNR (Nyquist bandwidth) of 16 dBrms for QPSK, or at CNR of 23 dBrms for 16-QAM.

C.6.1.11 Frame structure

The frame structure MUST have the following general format (see Figure C.6-4). Actual length in bits MUST be defined in the data link layer protocol specifications.



GT Guard Time

FEC Forward Error Correction

Figure C.6-4/J.112 – Frame structure

C.6.1.12 Channel frequency accuracy

Channel frequency accuracy MUST be within ± 50 ppm over a temperature range of 0 to 40 degrees C.

C.6.1.13 Symbol rate accuracy

Symbol rate accuracy MUST be within ± 50 ppm over a temperature range of 0 to 40 degrees C.

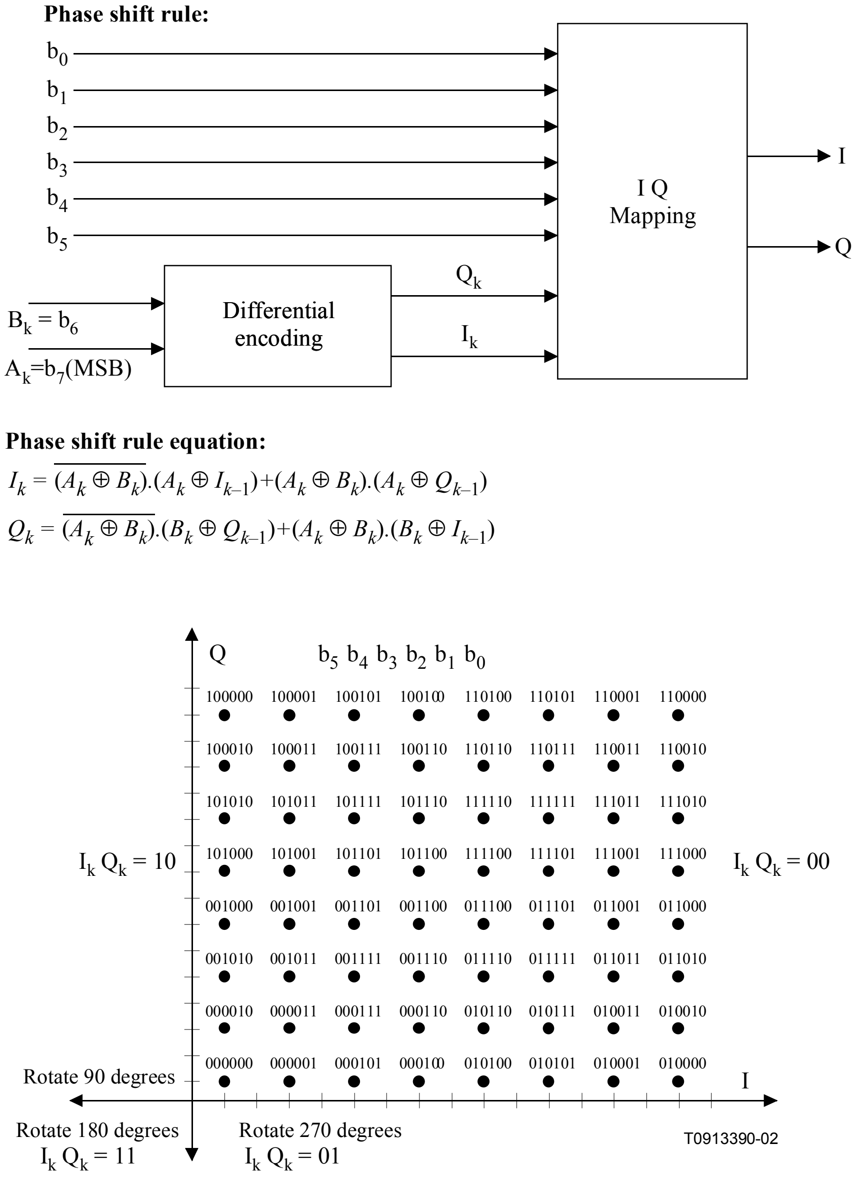
C.6.2 Downstream

C.6.2.1 Modulation method

The modulation method MUST be 64-QAM and 256-QAM for downstream.

C.6.2.2 Signal constellation diagram and phase shift rule

The signal constellation diagram and phase shift rule for 64-QAM MUST be compliant with Annex C/J.83. 256-QAM Signal Constellation Diagram MUST be compliant with Figure C.6-5, when the interleave depth I = 12 is selected. In case that the interleave depth I = 34 or 204 is selected, the signal constellation diagram and phase shift rule MUST be as shown in Figure C.6-6.



Phase shift rule equation:

$$I_k = \overline{(A_k \oplus B_k)}.(A_k \oplus I_{k-1})+(A_k \oplus B_k).(A_k \oplus Q_{k-1})$$

$$Q_k = \overline{(A_k \oplus B_k)}.(B_k \oplus Q_{k-1})+(A_k \oplus B_k).(B_k \oplus I_{k-1})$$

100000	100001	100101	100100	110100	110101	110001	110000
100010	100011	100111	100110	110110	110111	110011	110010
101010	101011	101111	101110	111110	111111	111011	111010
101000	101001	101101	101100	111100	111101	111001	111000
001000	001001	001101	001100	011100	011101	011001	011000
001010	001011	001111	001110	011110	011111	011011	011010
000010	000011	000111	000110	010110	010111	010011	010010
000000	000001	000101	000100	010100	010101	010001	010000

Figure C.6-5/J.112 – 256-QAM signal constellation diagram and phase shift rule (I = 12)

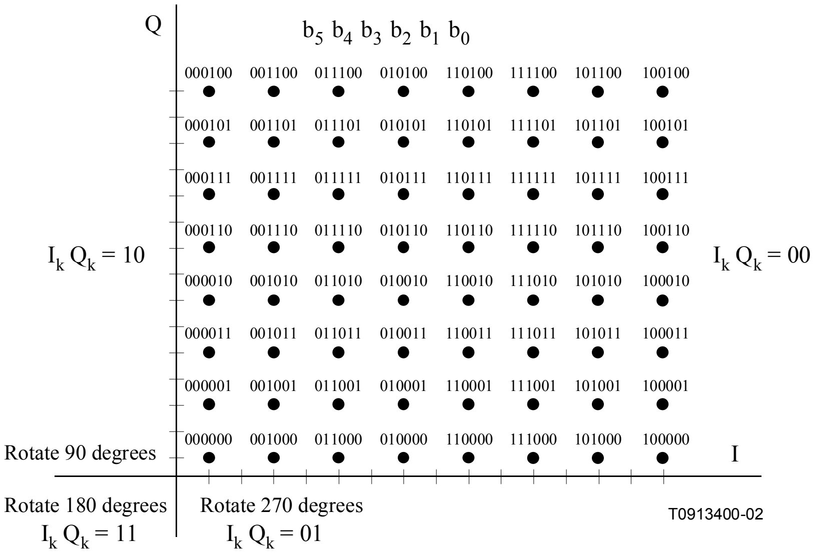


Figure C.6-6/J.112 – 256-QAM signal constellation diagram and phase shift rule (I = 34 or 204)

C.6.2.3 Symbol rate, bandwidth and roll off

The symbol rate MUST be 5.274 Msym/s. Bandwidth MUST be 6 MHz. The roll off factor MUST be 13%. Other parameters related to symbol rate, bandwidth and roll off SHOULD be compliant with Annex C/J.83.

C.6.2.4 Frequency range

The downstream channel MUST support a 90 MHz to 770 MHz frequency range edge to edge.

C.6.2.5 Frame structure

The frame structure SHOULD be compliant with Annex C/J.83.

C.6.2.6 Error correction

Error correction functionality SHOULD be considered for the noise environment in the cable television network. Code length and information byte length MUST be in accordance with Annex C/J.83.

The original Reed-Solomon code is defined as follows:

- Primitive polynomial: $p(X) = X^8 + X^4 + X^3 + X^2 + 1$
- Generator polynomial: $g(X) = (X + \alpha^0)(X + \alpha^1)$----------$(X + \alpha^{2T-1})$

where T is error correcting capability of a Reed-Solomon code and α is 02H and one of roots of equation $p(X) = 0$.

C.6.2.7 Randomization

A randomization function MUST be provided. The generator polynomial MUST be compliant with Annex C/J.83.

C.6.2.8 Interleave

The interleave method for 64-QAM MUST be compliant with Annex C/J.83. The interleave method for 256-QAM is equal to Annex C/J.83 except for interleave depth values. The interleave depth I = 12 MUST be applied. The interleave depth I = 34 or 204 MAY be selected for optional use. Table C.6-7 shows the interleaver characteristics at 5.274 Msym/s.

Table C.6-7/J.112 – Interleaver characteristics (@5.274 Msym/s)

I (Number of taps)	12	34	204
M (Increment)	17	6	1
Burst protection 64-QAM/256-QAM	24 µs/18 µs	–/51 µs	–/300 µs
Latency 64-QAM/256-QAM	0.57 ms/0.43 ms	–/1.28 ms	–/7.85 ms

C.6.2.9 Transmission signal level

The transmission signal level at CMTS Output connector MUST be adjustable over the range of +100 to +120 dBµVrms.

C.6.2.10 Receiving signal level

CM MUST be able to operate at the level within a range of +45 to +75 dBµVrms for 64-QAM, +51 to +81 dBµVrms for 256-QAM at CM Input connector.

C.6.2.11 Transmission spurious

Transmission spurious level at CMTS Output connector MUST be less than –55 dBc over the range of 90 MHz to 770 MHz.

C.6.2.12 Bit error rate

Bit error rate MUST be less than 10^{-8} at CNR (Nyquist bandwidth) of 26 dBrms for 64-QAM, at CNR of 33 dBrms for 256-QAM with error correction.

C.6.2.13 Channel frequency accuracy

Channel frequency accuracy MUST be within ± 20 ppm over a temperature range of 0 to 40° C.

C.6.2.14 Symbol rate accuracy

Symbol rate accuracy MUST be within ± 20 ppm over a temperature range of 0 to 40° C.

C.6.2.15 Impedance, return loss and connector

Impedance, Return Loss and Connector at CM In/Output, CMTS Output and CMTS Input MUST meet the requirements shown in Table C.6-8.

Table C.6-8/J.112 – Impedance, return loss and connector type

	Impedance	Return loss	Connector type
CM In/Output	75 Ω	More than 6 dB 10-55 and 90-770 MHz	F-type, Female
CMTS Output	75 Ω	More than 14 dB 90-770 MHz	F-type, Female
CMTS Input	75 Ω	More than 6 dB 10-55 MHz	F- type, Female

C.7 Downstream transmission convergence sublayer

This clause applies to the technology option referred to in C.1.1.

C.7.1 Introduction

In order to improve demodulation robustness, facilitate common receiving hardware for both video and data, and provide an opportunity for the possible future multiplexing of video and data over the PMD sublayer bitstream defined in clause C.6, a sublayer is interposed between the downstream PMD sublayer and the Data-Over-Cable MAC sublayer.

The downstream bitstream is defined as a continuous series of 188-byte MPEG [ITU-T H.222.0] packets. These packets consist of a 4-byte header followed by 184 bytes of payload. The header identifies the payload as belonging to the Data-Over-Cable MAC. Other values of the header MAY indicate other payloads. The mixture of MAC payloads and those of other services is optional and is controlled by the CMTS.

Figure C.7-1 illustrates the interleaving of Data-Over-Cable (DOC) MAC bytes with other digital information (digital video in the example shown).

Header = DOC	DOC MAC payload
Header = video	Digital video payload
Header = video	Digital video payload
Header = DOC	DOC MAC payload
Header = video	Digital video payload
Header = DOC	DOC MAC payload
Header = video	Digital video payload
Header = video	Digital video payload
Header = video	Digital video payload

Figure C.7-1/J.112 – Example of interleaving MPEG packets in downstream

C.7.2 MPEG packet format

The format of an MPEG Packet carrying Annex C/J.112 data is shown in Figure C.7-2. The packet consists of a 4-byte MPEG Header, a pointer_field (not present in all packets) and the Annex C/J.112 Payload.

MPEG Header (4 bytes)	pointer_field (1 byte)	Payload (183 or 184 bytes)

Figure C.7-2/J.112 – Format of an MPEG packet

C.7.3 MPEG header for Annex C/J.112 data-over-cable

The format of the MPEG Transport Stream header is defined in 2.4/H.222.0 [ITU-T H.222.0]. The particular field values that distinguish Data-Over-Cable MAC streams are defined in Table C.7-1. Field names are from the ITU specification.

The MPEG Header consists of 4 bytes that begin the 188-byte MPEG Packet. The format of the header for use on an Annex C/J.112 Data-Over-Cable PID is restricted to that shown in Table C.7-1. The header format conforms to the MPEG standard, but its use is restricted in this annex to NOT ALLOW inclusion of an adaptation_field in the MPEG packets.

Table C.7-1/J.112 – MPEG header format for Annex C/J.112 data-over-cable packets

Field	Length (bits)	Description
sync_byte	8	0x47; MPEG Packet Sync byte
transport_error_indicator	1	Indicates an error has occurred in the reception of the packet. This bit is reset to zero by the sender, and set to one whenever an error occurs in transmission of the packet
payload_unit_start_indicator	1	A value of one indicates the presence of a pointer_field as the first byte of the payload (fifth byte of the packet)
transport_priority	1	Reserved; set to zero
PID	13	Annex C/J.112 Data-Over-Cable well-known PID (0x1FFE)
transport_scrambling_control	2	Reserved, set to '00'
adaptation_field_control	2	'01'; use of the adaptation_field is NOT ALLOWED on the Annex C/J.112 PID
continuity_counter	4	cyclic counter within this PID

C.7.4 MPEG payload for Annex C/J.112 data-over-cable

The MPEG payload portion of the MPEG packet will carry the Annex C/J.112 MAC frames. The first byte of the MPEG payload will be a 'pointer_field' if the payload_unit_start_indicator (PUSI) of the MPEG header is set.

stuff_byte

This annex defines a stuff_byte pattern having a value (0xFF) that is used within the Annex C/J.112 payload to fill any gaps between the Annex C/J.112 MAC frames. This value is chosen as an unused value for the first byte of the Annex C/J.112 MAC frame. The 'FC' byte of the MAC Header will be defined to never contain this value. (FC_TYPE = '11' indicates a MAC-specific frame, and FC_PARM = '11111' is not currently used and, according to this annex, is defined as an illegal value for FC_PARM.)

pointer_field

The pointer_field is present as the fifth byte of the MPEG packet (first byte following the MPEG header) whenever the PUSI is set to one in the MPEG header. The interpretation of the pointer_field is as follows:

The pointer_field contains the number of bytes in this packet that immediately follow the pointer_field that the CM decoder must skip past before looking for the beginning of an Annex C/J.112 MAC Frame. A pointer field MUST be present if it is possible to begin a Data-Over-Cable MAC Frame in the packet, and MUST point to either:

1) the beginning of the first MAC frame to start in the packet; or

2) to any stuff_byte preceding the MAC frame.

C.7.5 Interaction with the MAC sublayer

MAC frames may begin anywhere within an MPEG packet, MAC frames may span MPEG packets, and several MAC frames may exist within an MPEG packet.

The following figures show the format of the MPEG packets that carry Annex C/J.112 MAC frames. In all cases, the PUSI flag indicates the presence of the pointer_field as the first byte of the MPEG payload.

Figure C.7-3 shows a MAC frame that is positioned immediately after the pointer_field byte. In this case, pointer_field is zero, and the Annex C/J.112 decoder will begin searching for a valid FC byte at the byte immediately following the pointer_field.

MPEG Header (PUSI =1)	pointer_field (= 0)	MAC Frame (up to 183 bytes)	stuff_byte(s) (0 or more)

Figure C.7-3/J.112 – Packet format where a MAC frame immediately follows the pointer_field

Figure C.7-4 shows the more general case where a MAC Frame is preceded by the tail of a previous MAC Frame and a sequence of stuffing bytes. In this case, the pointer_field still identifies the first byte after the tail of Frame #1 (a stuff_byte) as the position where the decoder should begin searching for a legal MAC sublayer FC value. This format allows the multiplexing operation in the CMTS to immediately insert a MAC frame that is available for transmission if that frame arrives after the MPEG header and pointer_field have been transmitted.

In order to facilitate multiplexing of the MPEG packet stream carrying Annex C/J.112 data with other MPEG-encoded data, the CMTS SHOULD NOT transmit MPEG packets with the Annex C/J.112 PID which contain only stuff_bytes in the payload area. MPEG null packets SHOULD be transmitted instead. Note that there are timing relationships implicit in the Annex C/J.112 MAC sublayer which must also be preserved by any MPEG multiplexing operation.

MPEG Header (PUSI =1)	pointer_field (= M)	Tail of MAC Frame #1 (M bytes)	stuff_byte(s) (0 or more)	Start of MAC Frame #2

Figure C.7-4/J.112 – Packet format with MAC frame preceded by stuffing bytes

Figure C.7-5 shows that multiple MAC frames may be contained within the MPEG packet. The MAC frames may be concatenated one after the other or be separated by an optional sequence of stuffing bytes.

MPEG Header (PUSI =1)	pointer_field (= 0)	MAC Frame #1	MAC Frame #2	stuff_byte(s) (0 or more)	MAC Frame #3

Figure C.7-5/J.112 – Packet format showing multiple MAC frames in a single packet

Figure C.7-6 shows the case where a MAC frame spans multiple MPEG packets. In this case, the pointer_field of the succeeding frame points to the byte following the last byte of the tail of the first frame.

<table>
<tr><td>MPEG Header
(PUSI = 1)</td><td>pointer_field
(= 0)</td><td>stuff_bytes
(0 or more)</td><td colspan="3">Start of MAC Frame #1
(up to 183 bytes)</td></tr>
<tr><td>MPEG Header
(PUSI = 0)</td><td colspan="5">Continuation of MAC Frame #1
(184 bytes)</td></tr>
<tr><td>MPEG Header
(PUSI = 1)</td><td>pointer_field
(= M)</td><td>Tail of MAC Frame #1
(M bytes)</td><td>stuff_bytes
(0 or more)</td><td colspan="2">Start of MAC Frame #2
(M bytes)</td></tr>
</table>

Figure C.7-6/J.112 – Packet format where a MAC frame spans multiple packets

The Transmission Convergence sublayer MUST operate closely with the MAC sublayer in providing an accurate timestamp to be inserted into the Time Synchronization message (refer to C.8.3.2 and C.9.3).

C.7.6 Interaction with the physical layer

The MPEG-2 packet stream MUST be encoded according to [ITU-T J.83-C].

C.7.7 MPEG header synchronization and recovery

The MPEG-2 packet stream SHOULD be declared "in frame" (i.e., correct packet alignment has been achieved) when five consecutive correct parity checksums, each 188 bytes from the previous one, have been received.

The MPEG-2 packet stream SHOULD be declared "out of frame," and a search for correct packet alignment started, when nine consecutive incorrect parity checksums are received.

The format of MAC frames is described in detail in clause C.8.

C.8 Media access control specification

C.8.1 Introduction

C.8.1.1 Overview

This clause describes revised Annex C/J.112 MAC protocol. Some of the MAC protocol highlights include:

- Bandwidth allocation controlled by CMTS;
- A stream of mini-slots in the upstream;
- Dynamic mix of contention- and reservation-based upstream transmit opportunities;
- Bandwidth efficiency through support of variable-length packets;
- Extensions provided for future support of ATM or other Data PDU;
- Quality-of-service including:
  - Support for Bandwidth and Latency Guarantees;
  - Packet Classification;
  - Dynamic Service Establishment;
- Extensions provided for security at the data link layer;
- Support for a wide range of data rates.

C.8.1.2 Definitions

C.8.1.2.1 MAC-sublayer domain

A MAC-sublayer domain is a collection of upstream and downstream channels for which a single MAC Allocation and Management protocol operates. Its attachments include one CMTS and some number of CMs. The CMTS MUST service all of the upstream and downstream channels; each CM MAY access one or more upstream and downstream channels. The CMTS MUST police and discard any packets received that have a source MAC address that is not a unicast MAC address.

C.8.1.2.2 MAC service access point

A MAC Service Access Point (MSAP) is an attachment to a MAC-sublayer domain. (Refer to C.5.2.)

C.8.1.2.3 Service flows

The concept of Service Flows 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 bandwidth allocation.

A Service Flow ID defines a particular unidirectional mapping between a CM and the CMTS. Active Upstream Service Flow IDs also have associated Service IDs or SIDs. Upstream bandwidth is allocated to SIDs, and hence to CMs, by the CMTS. Service IDs provide the mechanism by which upstream Quality of Service is implemented.

The CMTS MAY assign one or more Service Flow IDs (SFIDs) to each CM, corresponding to the Service Flows required by the CM. This mapping can be negotiated between the CMTS and the CM during CM registration or via dynamic service establishment (refer to C.11.4).

In a basic CM implementation, two Service Flows (one upstream, one downstream) could be used, for example, to offer best-effort IP service. However, the Service Flow concept allows for more complex CMs to be developed with support for multiple service classes while supporting interoperability with more basic modems. With these more complex modems, it is possible that certain Service Flows will be configured in such a way that they cannot carry all types of traffic. That is, they may have a maximum packet size limitation or be restricted to small fixed size unsolicited grants. Furthermore, it might not be appropriate to send other kinds of data on Service Flows that are being used for Constant Bit Rate (CBR)-type applications.

Even in these complex modems, it is necessary to be able to send certain upstream packets needed for MAC management, SNMP management, key management, etc. For the network to function properly, all CMs MUST support at least one upstream and one downstream Service Flow. These Service Flows MUST always be provisioned to allow the CM to request and to send the largest possible unconcatenated MAC frame (refer to C.8.2.2). These Service Flows are referred to as the upstream and downstream Primary Service Flows. The SID assigned to the upstream Primary Service Flow is referred to as the Primary SID.

The Primary SID MUST always be assigned to the first provisioned upstream Service Flow during the registration process (which may or may not be the same temporary SID used for the registration process). The Primary Service Flows MUST be immediately activated at registration time. The Primary SID MUST always be used for station maintenance after registration. The Primary Service Flows MAY be used for traffic. All unicast Service Flows MAY use the security association defined for the Primary Service Flow.

All Service Flow IDs are unique within a single MAC-sublayer domain. The mapping of a unicast Service Identifier to an active/admitted Service Flow MUST be unique within a single MAC-sublayer domain. The length of the Service Flow ID is 32 bits. The length of the Service ID is 14 bits (although the Service ID is sometimes carried in the low-order bits of a 16 bit field).

C.8.1.2.4 Upstream intervals, mini-slots and 6.94-microsecond increments

The upstream transmission time-line is divided into intervals by the upstream bandwidth allocation mechanism. Each interval is an integral number of mini-slots. A "mini-slot" is the unit of granularity for upstream transmission opportunities. There is no implication that any PDU can actually be transmitted in a single mini-slot. Each interval is labeled with a usage code which defines both the type of traffic that can be transmitted during that interval and the physical-layer modulation encoding. A mini-slot is a power-of-two multiple of 6.94 µs increments, i.e., 2, 4, 8, 16, 32, 64, or 128 times 6.94 µs. The relationship between mini-slots, bytes, and time ticks is described further in C.9.3.4. The usage code values are defined in Table C.8-20 and allowed use is defined in C.8.3. The binding of these values to physical-layer parameters is defined in Table C.8-18.

C.8.1.2.5 Frame

A frame is a unit of data exchanged between two (or more) entities at the Data Link Layer. A MAC frame consists of a MAC Header (beginning with a Frame Control byte; see Figure C.8-3), and may incorporate a variable-length data PDU. The variable-length PDU includes a pair of 48 bit addresses, data, and a CRC. In special cases, the MAC Header may encapsulate multiple MAC frames (see C.8.2.5.5) into a single MAC frame.

C.8.1.3 Future use

A number of fields are defined as being "for future use" or Reserved in the various MAC frames described in this annex. These fields MUST NOT be interpreted or used in any manner by this version (revised Annex C/J.112) of the MAC protocol.

C.8.2 MAC frame formats

C.8.2.1 Generic MAC frame format

A MAC frame is the basic unit of transfer between MAC sublayers at the CMTS and the cable modem. The same basic structure is used in both the upstream and downstream directions. MAC frames are variable in length. The term "frame" is used in this context to indicate a unit of information that is passed between MAC sublayer peers. This is not to be confused with the term "framing" that indicates some fixed timing relationship.

There are three distinct regions to consider, as shown in Figure C.8-1. Preceding the MAC frame is either PMD sublayer overhead (upstream) or an MPEG transmission convergence header (downstream). The first part of the MAC frame is the MAC Header. The MAC Header uniquely identifies the contents of the MAC frame. Following the header is the optional Data PDU region. The format of the Data PDU and whether it is even present is described in the MAC Header.

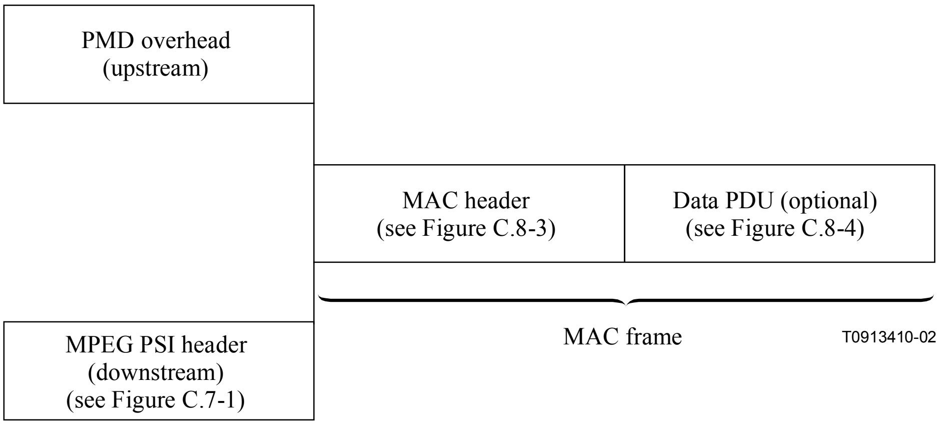


Figure C.8-1/J.112 – Generic MAC frame format

C.8.2.1.1 PMD Overhead

In the upstream direction, the PHY layer indicates the start of the MAC frame to the MAC sublayer. From the MAC sublayer's perspective, it only needs to know the total amount of overhead so it can account for it in the Bandwidth Allocation process. More information on this may be found in the PMD Sublayer clause (clause C.6).

The FEC overhead is spread throughout the MAC frame and is assumed to be transparent to the MAC data stream. The MAC sublayer does need to be able to account for the overhead when doing Bandwidth Allocation. More information on this may be found in the Upstream Bandwidth Allocation clause (refer to C.9.1).

C.8.2.1.2 MAC Frame Transport

The transport of MAC frames by the PMD sublayer for upstream channels is shown in Figure C.8-2.

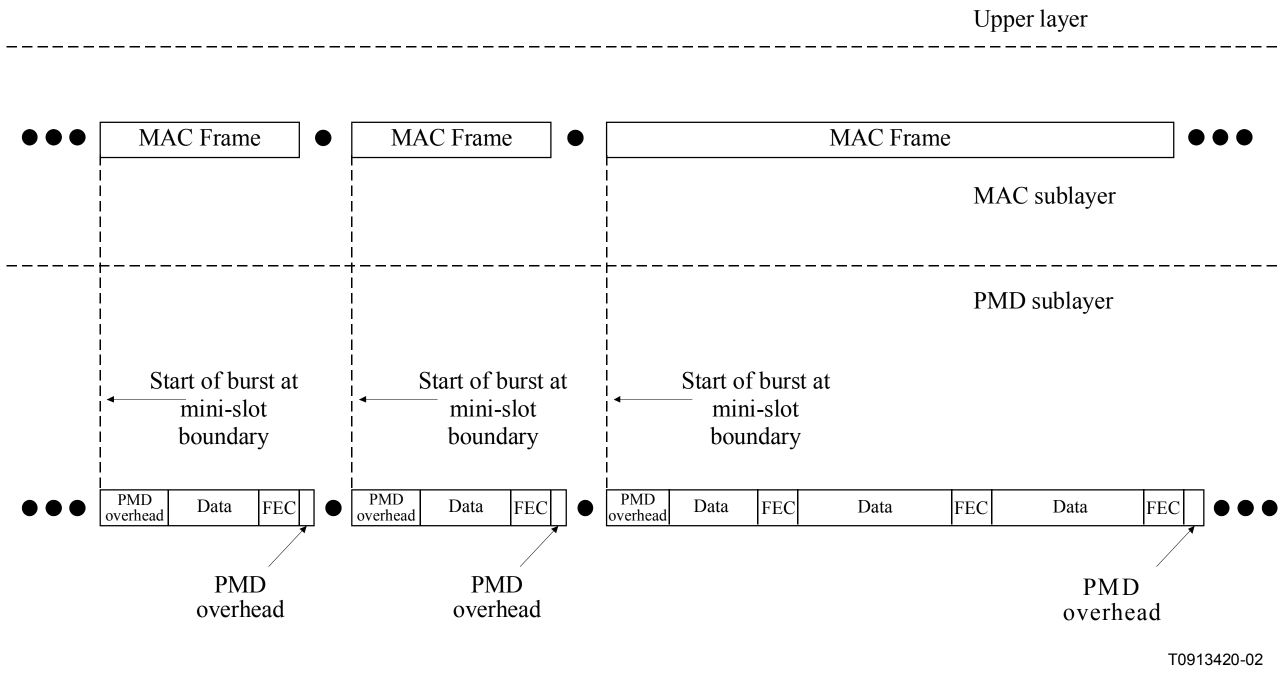


Figure C.8-2/J.112 – Upstream MAC/PMD Convergence

The layering of MAC frames over MPEG in the downstream channel is described in clause C.7.

C.8.2.1.3 Ordering of bits and octets

Within an octet, the least-significant bit is the first transmitted on the wire. This follows the convention used by Ethernet and [ISO/IEC8802-3]. This is often called bit-little-endian order (see Note).

NOTE – This applies to the upstream channel only. For the downstream channel, the MPEG transmission convergence sublayer presents an octet-wide interface to the MAC, so the MAC sublayer does not define the bit order.

Within the MAC layer, when numeric quantities are represented by more than one octet (i.e., 16 bit and 32 bit values), the octet containing the most-significant bits is the first transmitted on the wire. This is sometimes called byte-big-endian order.

This clause follows the textual convention that when bit-fields are presented in tables, the most-significant bits are topmost in the table. For example, in Table C.8-2, FC_TYPE occupies the two most-significant bits and EHDR_ON occupies the least-significant bit.

C.8.2.1.3.1 Representing negative numbers

Signed integer values MUST be transmitted and received in two's complement format.

C.8.2.1.3.2 Type-length-value fields

Many MAC messages incorporate Type-Length-Value (TLV) fields. TLV fields are unordered lists of TLV-tuples. Some TLV's are nested (see Annex C.C). All TLV Length fields, except for EH-LEN (see C.8.2.6) MUST be greater than zero. Unless otherwise specified, Type is one byte and Length is one byte.

Using this encoding, new parameters may be added which some devices cannot interpret. A CM or CMTS which does not recognize a parameter type MUST skip over this parameter and MUST NOT treat the event as an error condition.

C.8.2.1.4 MAC header format

The MAC Header format MUST be as shown in Figure C.8-3.

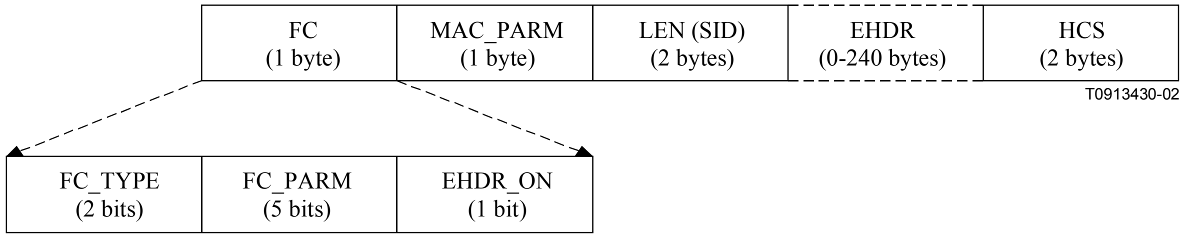


Figure C.8-3/J.112 – MAC header format

All MAC Headers MUST have the general format as shown in Table C.8-1. The Frame Control (FC) field is the first byte and uniquely identifies the rest of the contents within the MAC Header. The FC field is followed by 3 bytes of MAC control; an OPTIONAL Extended Header field (EHDR); plus a Header Check Sequence (HCS) to ensure the integrity of the MAC Header.

Table C.8-1/J.112 – Generic MAC header format

MAC header field	Usage	Size
FC	Frame Control: Identifies type of MAC Header	8 bits
MAC_PARM	Parameter field whose use is dependent on FC: if EHDR_ON = 1; used for EHDR field length (ELEN) else if for concatenated frames (see Table C.8-10) used for MAC frame count else (for Requests only) indicates the number of mini-slots requested	8 bits
LEN (SID)	The length of the MAC frame. The length is defined to be the sum of the number of bytes in the extended header (if present) and the number of bytes following the HCS field. (For a REQ Header, this field is the Service ID instead)	16 bits
EHDR	Extended MAC Header (where present; variable size)	0-240 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a MAC Header	6 bytes + EHDR

The HCS field is a 16 bit CRC that ensures the integrity of the MAC Header, even in a collision environment. The HCS field coverage MUST include the entire MAC Header, starting with the FC field and including any EHDR field that may be present. The HCS is calculated using CRC-ITU-T ($x^{16}+x^{12}x^{5}+1$) as defined in [ITU-T X.25].

The FC field is broken down into the FC_TYPE subfield, FC_PARM subfield and an EHDR_ON indication flag. The format of the FC field MUST be as shown in Table C.8-2.

Table C.8-2/J.112 – FC field format

FC field	Usage	Size
FC_TYPE	MAC Frame Control Type field: 00: Packet PDU MAC Header 01: ATM PDU MAC Header 10: Reserved PDU MAC Header 11: MAC Specific Header	2 bits
FC_PARM	Parameter bits, use dependent on FC_TYPE.	5 bits
EHDR_ON	When = 1, indicates that EHDR field is present. Length of EHDR (ELEN) determined by MAC_PARM field	1 bit

The FC_TYPE subfield is the two MSBs of the FC field. These bits MUST always be interpreted in the same manner to indicate one of four possible MAC frame formats. These types include: MAC Header with Packet PDU; MAC Header with ATM cells; MAC Header reserved for future PDU types; or a MAC Header used for specific MAC control purposes. These types are spelled out in more detail in the remainder of this clause.

The five bits following the FC_TYPE subfield is the FC_PARM subfield. The use of these bits are dependent on the type of MAC Header. The LSB of the FC field is the EHDR_ON indicator. If this bit is set, then an Extended Header (EHDR) is present. The EHDR provides a mechanism to allow the MAC Header to be extensible in an inter-operable manner.

The Transmission Convergence Sublayer stuff-byte pattern is defined to be a value of 0xFF. This precludes the use of FC byte values which have FC_TYPE = '11' and FC_PARM = '11111'.

The MAC_PARM field of the MAC Header serves several purposes depending on the FC field. If the EHDR_ON indicator is set, then the MAC_PARM field MUST be used as the Extended Header length (ELEN). The EHDR field may vary from 0 to 240 bytes. If this is a concatenation MAC Header, then the MAC_PARM field represents the number of MAC frames (CNT) in the concatenation (see C.8.2.5.5). If this is a Request MAC Header (REQ) (see C.8.2.5.3), then the MAC_PARM field represents the amount of bandwidth being requested. In all other cases, the MAC_PARM field is reserved for future use.

The third field has two possible uses. In most cases, it indicates the length (LEN) of this MAC frame. In one special case, the Request MAC Header, it is used to indicate the cable modem's Service ID since no PDU follows the MAC Header.

The Extended Header (EHDR) field provides extensions to the MAC frame format. It is used to implement data link security as well as frame fragmentation, and can be extended to add support for additional functions in future releases. Initial implementations SHOULD pass this field to the processor. This will allow future software upgrades to take advantage of this capability. (Refer to C.8.2.6, "Extended MAC Headers", for details.)

C.8.2.1.5 Data PDU

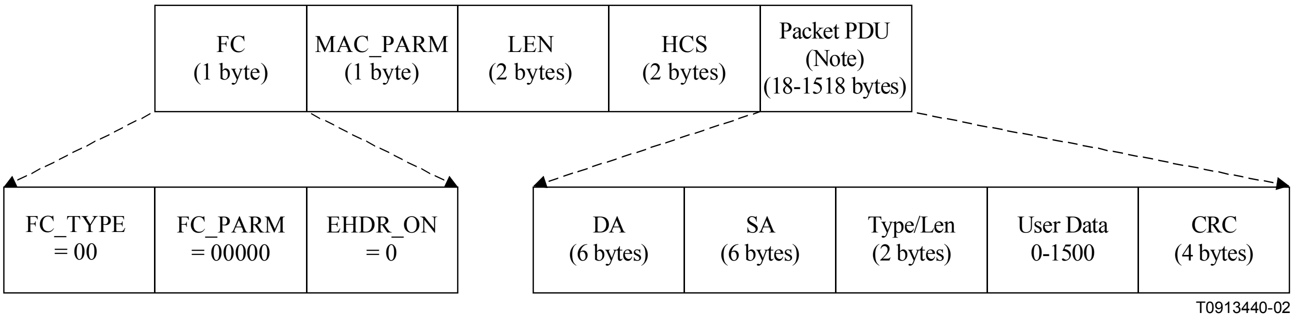
The MAC Header may be followed by a Data PDU. The type and format of the Data PDU is defined in the Frame Control field of the MAC Header. The FC field explicitly defines a Packet Data PDU, an ATM Data PDU, a MAC-Specific Frame and a reserved code point (used as an escape mechanism for future extensions). All CMs MUST use the length in the MAC Header to skip over any reserved data.

C.8.2.2 Packet-based MAC frames

C.8.2.2.1 Variable-length packets

The MAC sublayer MUST support a variable-length Ethernet/[ISO/IEC8802-3] type Packet Data PDU. Normally, the Packet PDU MUST be passed across the network in its entirety, including its original CRC. A unique Packet MAC Header is appended to the beginning. The frame format without an Extended header MUST be as shown in Figure C.8-4 and Table C.8-3.

The one exception is the case of Payload Header Suppression. In this case, all bytes except those suppressed MUST be passed across the network and the CRC covers only those bytes actually transmitted. (Refer to C.8.2.6.3.1.)



NOTE – Frame size is limited to 1518 bytes in the absence of VLAN tagging. Cooperating devices which implement IEEE 802.1Q VLAN tagging MAY use a frame size up to 1522 bytes.

Figure C.8-4/J.112 – Ethernet/802.3 packet PDU format

Table C.8-3/J.112 – Packet PDU format

Field	Usage	Size
FC	FC_TYPE = 00; Packet MAC Header FC_PARM[4:0] = 00000; other values reserved for future use and ignored EHDR_ON = 0 if there is no extended header, 1 if there is an EHDR	8 bits
MAC_PARM	MAC_PARM = x; MUST be set to zero if there is no EHDR; Otherwise set to length of EHDR	8 bits
LEN	LEN = n+x; length of Packet PDU in bytes + length of EHDR	16 bits
EHDR	Extended MAC Header, if present	0-240 bytes
HCS	MAC Header Check Sequence	16 bits
Packet Data	Packet PDU: DA – 48 bit Destination Address SA – 48 bit Source Address Type/Len – 16 bit Ethernet Type or [ISO/IEC8802-3] Length Field User Data (variable length, 0 – 1500 bytes) CRC – 32-bit CRC over packet PDU (as defined in Ethernet/[ISO/IEC8802-3])	n bytes
	Length of Packet MAC frame	6 + x + n bytes

Under certain circumstances (see Annex C.M) it may be necessary to transmit a packet PDU MAC frame without an actual PDU. This is done so that the extended header can be used to carry certain information about the state of the service flow. This could also happen as a result of PHS (see C.8.2.6.3.1). Such a frame will have the length field in MAC header set to the length of the extended header and will have no packet data, and therefore no CRC. This can only happen with frames transmitted on the upstream as frames transmitted on the downstream always have at least the DA and SA fields of the packet PDU.

C.8.2.3 ATM cell MAC frames

The FC_TYPE 0x01 is reserved for future definition of ATM Cell MAC Frames. This FC_TYPE field in the MAC Header indicates that an ATM PDU is present. This PDU MUST be silently discarded by MAC implementations of this version (revised Annex C/J.112) of the specification. Compliant revised Annex C/J.112 implementations MUST use the length field to skip over the ATM PDU.

C.8.2.4 Reserved PDU MAC frames

The MAC sublayer provides a reserved FC code point to allow for support of future (to be defined) PDU formats. The FC field of the MAC Header indicates that a Reserved PDU is present. This PDU MUST be silently discarded by MAC implementations of this version (revised Annex C/J.112) of the specification. Compliant revised Annex C/J.112 implementations MUST use the length field to skip over the Reserved PDU.

The format of the Reserved PDU without an extended header MUST be as shown in Figure C.8-5 and Table C.8-4.

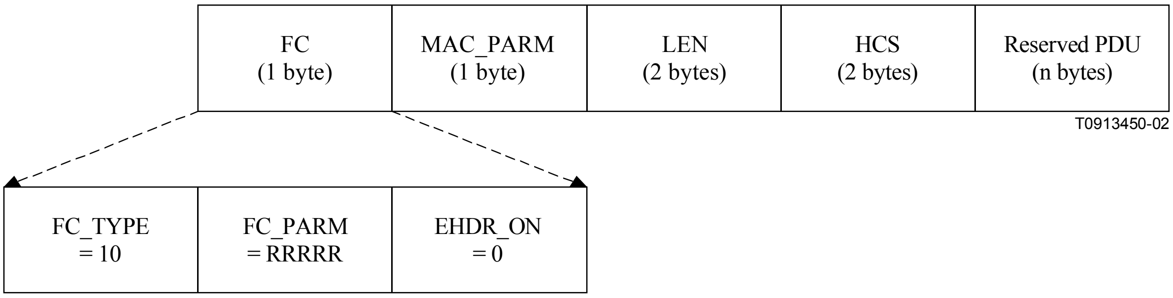


Figure C.8-5/J.112 – Reserved PDU format

Table C.8-4/J.112 – Reserved PDU format

Field	Usage	Size
FC	FC_TYPE = 10; Reserved PDU MAC Header FC_PARM[4:0]; reserved for future use EHDR_ON = 0 if there is no extended header, 1 if there is an EHDR	8 bits
MAC_PARM	MAC_PARM = x; MUST be set to zero if there is no EHDR; Otherwise set to length of EHDR	8 bits
LEN	LEN = n + x; length of Reserved PDU + length of EHDR in bytes	16 bits
EHDR	Extended MAC Header, if present	0-240 bytes
HCS	MAC Header Check Sequence	16 bits
User Data	Reserved Data PDU	n bytes
	Length of Reserved PDU MAC frame	6 + x + n bytes

C.8.2.5 MAC-specific headers

There are several MAC Headers which are used for very specific functions. These functions include support for downstream timing and upstream ranging/power adjust, requesting bandwidth, fragmentation and concatenating multiple MAC frames.

Table C.8-5 describes FC_PARM usage within the MAC Specific Header.

Table C.8-5/J.112 – MAC-Specific Headers and Frames

FC_PARM	Header/Frame Type
00000	Timing Header
00001	MAC Management Header
00010	Request Frame
00011	Fragmentation Header
11100	Concatenation Header

C.8.2.5.1 Timing header

A specific MAC Header is identified to help support the timing and adjustments required. In the downstream, this MAC Header MUST be used to transport the Global Timing Reference to which all cable modems synchronize. In the upstream, this MAC Header MUST be used as part of the Ranging message needed for a cable modem's timing and power adjustments. The Timing MAC Header is followed by a Packet Data PDU. The format MUST be as shown in Figure C.8-6 and Table C.8-6.

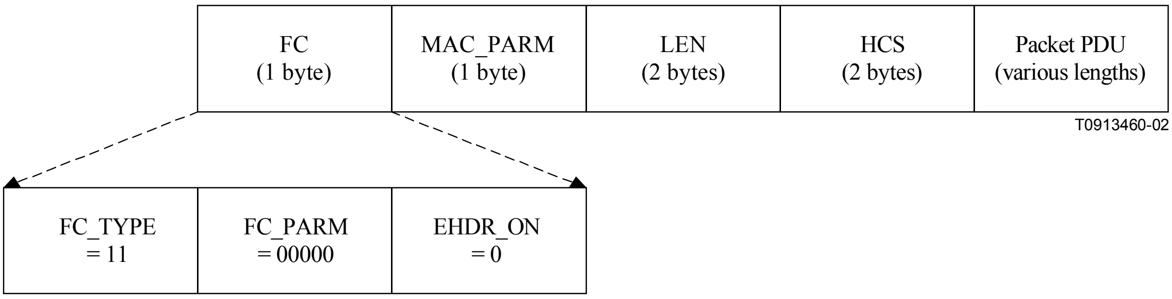


Figure C.8-6/J.112 – Timing MAC Header

Table C.8-6/J.112 – Timing MAC Header Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC Specific Header FC_PARM[4:0] = 00000; Timing MAC Header EHDR_ON = 0; Extended header prohibited for SYNC and RNG-REQ	8 bits
MAC_PARM	Reserved for future use	8 bits
LEN	LEN = n; Length of Packet PDU in bytes	16 bits
EHDR	Extended MAC Header not present	0 bytes
HCS	MAC Header Check Sequence	2 bytes
Packet Data	MAC Management message: SYNC message (downstream only) RNG-REQ (upstream only)	n bytes
	Length of Timing Message MAC frame	6 + n bytes

C.8.2.5.2 MAC Management Header

A specific MAC Header is identified to help support the MAC management messages required. This MAC Header MUST be used to transport all MAC management messages (refer to C.8.3). The format MUST be as shown Figure C.8-7 and Table C.8-7.

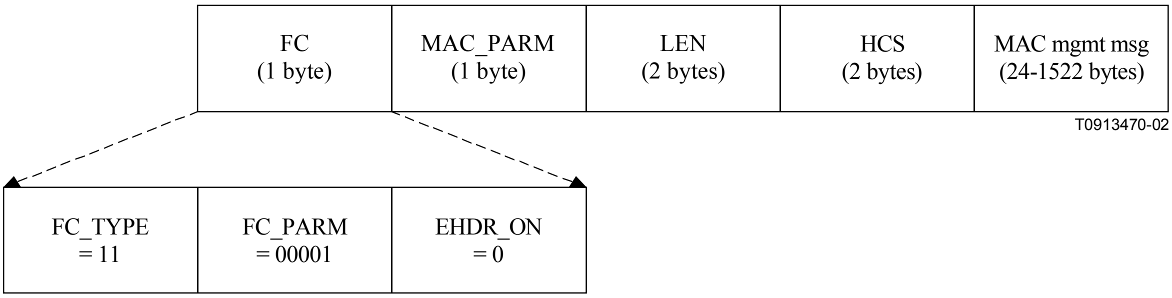


Figure C.8-7/J.112 – Management MAC header

Table C.8-7/J.112 – MAC management format

Field	Usage	Size
FC	FC_TYPE = 11; MAC Specific Header FC_PARM[4:0] = 00001; Management MAC Header EHDR_ON = 0 if there is no extended header, 1 if there is an EHDR	8 bits
MAC_PARM	MAC_PARM = x; MUST be set to zero if there is no EHDR; Otherwise set to length of EHDR	8 bits
LEN	LEN = n + x; length of MAC management message + length of EHDR in bytes	16 bits
EHDR	Extended MAC Header, if present	0-240 bytes
HCS	MAC Header Check Sequence	16 bits
Packet Data	MAC management message	n bytes
	Length of Packet MAC frame	6 + x + n bytes

C.8.2.5.3 Request frame

The Request Frame is the basic mechanism that a cable modem uses to request bandwidth. As such, it is only applicable in the upstream. There MUST be no Data PDUs following the Request Frame. The general format of the Request MUST be as shown in Figure C.8-8 and Table C.8-8.

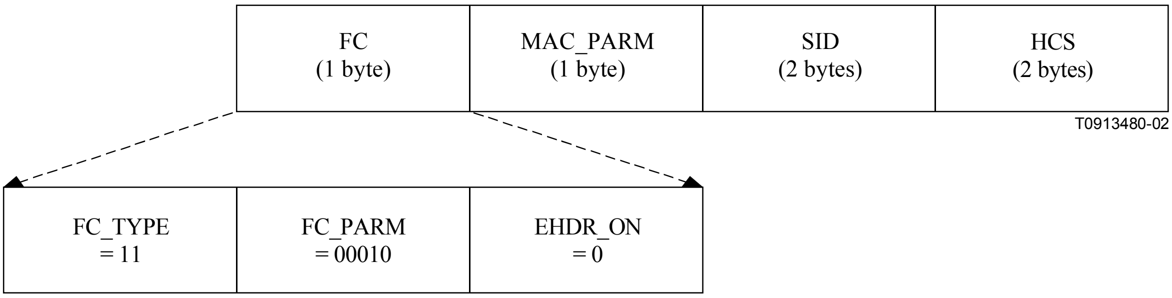


Figure C.8-8/J.112 – Request frame format

Table C.8-8/J.112 – Request frame (REQ) format

Field	Usage	Size

FC	FC_TYPE = 11; MAC-Specific Header
	FC_PARM[4:0] = 00010; MAC Header only; no data PDU following
	EHDR_ON = 0; No EHDR allowed
		8 bits

MAC_PARM	REQ, total number of minislots requested	8 bits
SID	Service ID (0...0x1FFF)	16 bits
EHDR	Extended MAC Header not allowed	0 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a REQ MAC Header	6 bytes

Because the Request Frame does not have a Data PDU following it, the LEN field is not needed. The LEN field MUST be replaced with an SID. The SID MUST uniquely identify a particular Service Flow within a given CM.

The bandwidth request, REQ, MUST be specified in mini-slots. The REQ field MUST indicate the current total amount of bandwidth requested for this service queue including appropriate allowance for the PHY overhead.

C.8.2.5.4 Fragmentation header

The Fragmentation MAC Header provides the basic mechanism to split a larger MAC PDU into smaller pieces that are transmitted individually and then re-assembled at the CMTS. As such, it is only applicable in the upstream. The general format of the Fragmentation MAC Header MUST be as shown in Figure C.8-9.

A compliant CM MUST support fragmentation. A compliant CMTS MAY support fragmentation. To decrease the burden on the CMTS and to reduce unnecessary overhead, fragmentation headers MUST NOT be used on unfragmented frames.

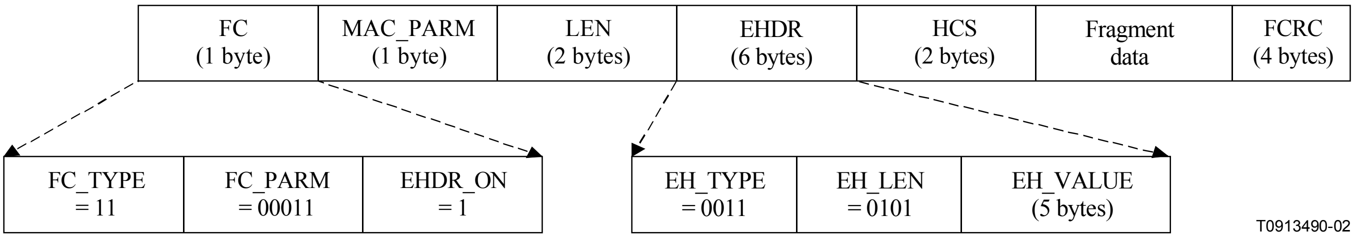


Figure C.8-9/J.112 – Fragmentation MAC header format

Table C.8-9/J.112 – Fragmentation MAC frame (FRAG) format

Field	Usage	Size

FC	FC_TYPE = 11; MAC-Specific Header
	FC_PARM[4:0] = 00011; Fragmentation MAC Header
	EHDR_ON = 1; Fragmentation EHDR follows
		8 bits

MAC_PARM	ELEN = 6 bytes; length of Fragmentation EHDR	8 bits
LEN	LEN = length of fragment payload + EHDR length + FCRC length	16 bits
EHDR	Refer to C.8.2.6.2	6 bytes
HCS	MAC Header Check Sequence	2 bytes
Fragment Data	Fragment payload; portion of total MAC PDU being sent	n bytes
FCRC	CRC – 32 bit CRC over Fragment Data payload (as defined in Ethernet/[ISO/IEC8802-3])	4 bytes
	Length of a MAC Fragment Frame	16 + n bytes

C.8.2.5.5 Concatenation header

A Specific MAC Header is defined to allow multiple MAC frames to be concatenated. This allows a single MAC "burst" to be transferred across the network. The PHY overhead (see Note) and the Concatenation MAC Header only occur once. Concatenation of multiple MAC frames MUST be as shown in Figure C.8-10. Concatenation of multiple MAC frames is the only method by which the CM can transmit more than one MAC frame in a single transmit opportunity.

NOTE – This includes the preamble, guard time, and possibly zero-fill bytes in the last codeword. The FEC overhead recurs for each codeword.

A compliant CM MUST support concatenation. A compliant CMTS MAY support concatenation. Concatenation only applies to upstream traffic. Concatenation MUST NOT be used on downstream traffic.

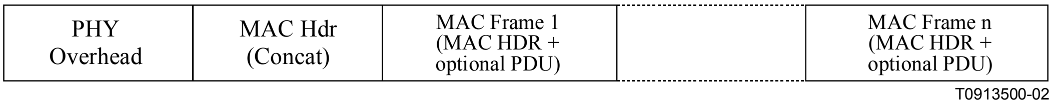

PHY Overhead
MAC Hdr (Concat)
MAC Frame 1 (MAC HDR + optional PDU)
MAC Frame n (MAC HDR + optional PDU)
T0913500-02

Figure C.8-10/J.112 – Concatenation of Multiple MAC Frames

Only one Concatenation MAC Header MUST be present per MAC "burst." Nested concatenation MUST NOT be allowed. Immediately following the Concatenation MAC Header MUST be the MAC Header of the first MAC frame. Information within the MAC Header indicates the length of the first MAC Frame and provides a means to find the start of the next MAC Frame. Each MAC frame within a concatenation MUST be unique and MAY be of any type. This means that Packet and MAC-specific Frames MAY be mixed together. However, all frames in a concatenation MUST be assigned to the same Service Flow. If the CMTS supports concatenation, it MUST support concatenations containing multiple frame types, including both Packet and MAC-specific Frames.

The embedded MAC frames MAY be addressed to different destinations and MUST be delivered as if they were transmitted individually.

The format of the Concatenation MAC Header MUST be as shown in Figure C.8-11 and Table C.8-10.

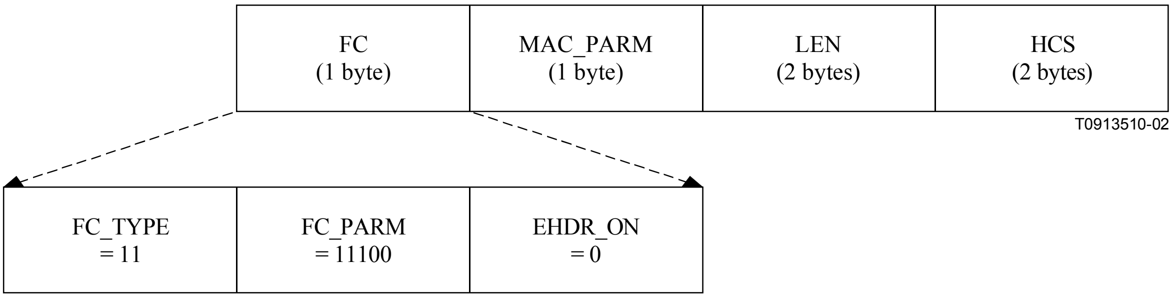


Figure C.8-11/J.112 – Concatenation MAC header format

Table C.8-10/J.112 – Concatenated MAC frame format

Field	Usage	Size

FC	FC_TYPE = 11; MAC Specific Header
	FC_PARM[4:0] = 11100; Concatenation MAC Header
	EHDR_ON = 0; No EHDR with Concatenation Header
		8 bits

MAC_PARM	CNT, number of MAC frames in this concatenation CNT = 0 indicates unspecified number of MAC frames	8 bits
LEN	LEN = x +... + y; length of all following MAC frames in bytes	16 bits
EHDR	Extended MAC Header MUST NOT be used	0 bytes
HCS	MAC Header Check Sequence	2 bytes
MAC frame 1	First MAC frame: MAC Header plus OPTIONAL data PDU	x bytes
MAC frame n	Last MAC frame: MAC Header plus OPTIONAL data PDU	y bytes
	Length of Concatenated MAC frame	6 + LEN bytes

The MAC_PARM field in the Concatenation MAC header provides a count of MAC frames as opposed to EHDR length or REQ amount as used in other MAC headers. If the field is non-zero, then it MUST indicate the total count of MAC Frames (CNT) in this concatenantion burst.

C.8.2.6 Extended MAC Headers

Every MAC Header, except the Timing, Concatenation MAC Header and Request Frame, has the capability of defining an Extended Header field (EHDR). The presence of an EHDR field MUST be indicated by the EHDR_ON flag in the FC field being set. Whenever this bit is set, then the MAC_PARM field MUST be used as the EHDR length (ELEN). The minimum defined EHDR is 1 byte. The maximum EHDR length is 240 bytes.

A compliant CMTS & CM MUST support extended headers.

The format of a generic MAC Header with an Extended Header included MUST be as shown in Figure C.8-12 and Table C.8-11.

Extended Headers MUST NOT be used in a Concatenation MAC Header, but MAY be included as part of the MAC Headers within the concatenation.

Extended Headers MUST NOT be used in Request Frames and Timing MAC Headers.

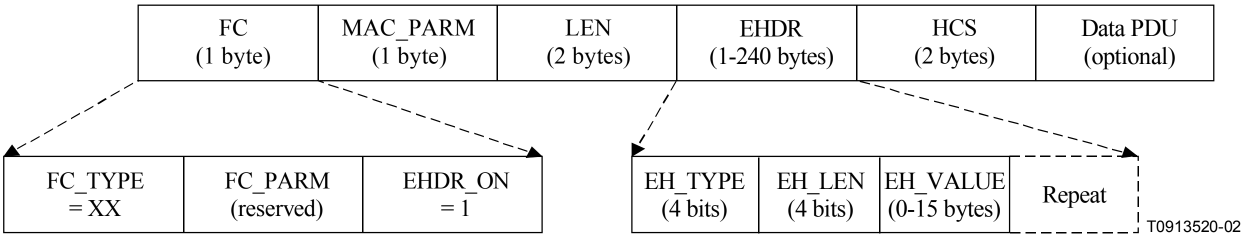


Figure C.8-12/J.112 – Extended MAC format

Table C.8-11/J.112 – Example extended header format

Field	Usage	Size

FC	FC_TYPE = XX; Applies to all MAC Headers
	FC_PARM[4:0] = XXXXX; dependent on FC_TYPE
	EHDR_ON = 1; EHDR present this example
		8 bits

MAC_PARM	ELEN = x; length of EHDR in bytes	8 bits
LEN	LEN = x + y; length of EHDR plus OPTIONAL data PDU in bytes	16 bits
EHDR	Extended MAC Header present this example	x bytes
HCS	MAC Header Check Sequence	2 bytes
PDU	OPTIONAL data PDU	y bytes
	Length of MAC frame with EHDR	6 + x + y bytes

Since the EHDR increases the length of the MAC frame, the LEN field MUST be increased to include both the length of the Data PDU and the length of the EHDR.

The EHDR field consists of one or more EH elements. Each EH element is variable sized. The first byte of the EH element MUST contain a type and a length field. Every CM MUST use this length to skip over any unknown EH elements. The format of an EH element MUST be as shown in Table C.8-12.

Table C.8-12/J.112 – EH element format

EH element fields	Usage	Size
EH_TYPE	EH element Type Field	4 bits
EH_LEN	Length of EH_VALUE	4 bits
EH_VALUE	EH element data	0-15 bytes

The types of EH element defined in Table C.8-13 MUST be supported. Reserved and extended types are undefined at this point and MUST be ignored.

The first ten EH element types are intended for one-way transfer between the cable modem and the CMTS. The next five EH element types are for end-to-end usage within a MAC-sublayer domain. Thus, the information attached to EHDR elements 10-14 on the upstream MUST also be attached when the information is forwarded within a MAC-sublayer domain. The final EH element type is an escape mechanism that allows for more types and longer values, and MUST be as shown in Table C.8-13.

Table C.8-13/J.112 – Extended header types

EH_TYPE	EH_LEN	EH_VALUE
0	0	Null configuration setting; may be used to pad the extended header. The EH_LEN MUST be zero, but the configuration setting may be repeated.
1	3	Request: mini-slots requested (1 byte); SID (2 bytes) [CM → CMTS]
2	2	Acknowledgment requested; SID (2 bytes) [CM → CMTS]
3 (= BP_UP)	4	Upstream Privacy EH Element
	5	Upstream Privacy with Fragmentation (see Note) EH Element
4 (= BP_DOWN)	4	Downstream Privacy EH Element
5	1	Service Flow EH Element; Payload Header Suppression Header Downstream
6	1	Service Flow EH Element; Payload Header Suppression Header Upstream
	2	Service Flow EH Element; Payload Header Suppression Header Upstream (1 byte), Unsolicited Grant Synchronization Header (1 byte)
7-9		Reserved
10 – 14		Reserved [CM ↔ CM]
15	XX	Extended EH Element: EHX_TYPE (1 byte), EHX_LEN (1 byte), EH_VALUE (length determined by EHX_LEN)
NOTE – An Upstream Privacy with Fragmentation EH Element MUST only occur within a Fragmentation MAC-Specific Header (refer to C.8.2.5.4).		

C.8.2.6.1 Piggyback requests

Several Extended Headers can be used to request bandwidth for subsequent transmissions. These requests are generically referred to as "piggyback requests". They are extremely valuable for performance because they are not subject to contention as Request Frames generally are. (Refer to C.9.4.)

Requests for additional bandwidth can be included in Request, Upstream Privacy and Upstream Privacy with Fragmentation Extended Header elements.

C.8.2.6.2 Fragmentation extended header

Fragmented packets use a combination of the Fragmentation MAC header and a modified version of the Upstream Privacy Extended header. Clause C.8.2.5.4 describes the Fragmentation MAC header. The Upstream Privacy Extended Header with Fragmentation, also known as the Fragmentation Extended Header, MUST be as shown in Table C.8-14.

Table C.8-14/J.112 – Fragmentation extended header format

EH element fields	Usage	Size
EH_TYPE	Upstream Privacy EH element = 3	4 bits
EH_LEN	Length of EH_VALUE = 5	4 bits
EH_VALUE	Key_seq; same as in BP_UP	4 bits
	Ver = 1; version number for this EHDR	4 bits
	BPI_ENABLE If BPI_ENABLE = 0, BPI disabled If BPI_ENABLE = 1, BPI enabled	1 bit
	Toggle bit; same as in BP_UP	1 bit
	SID; Service ID associated with this fragment	14 bits
	REQ; number of mini-slots for a piggyback request	8 bits
	Reserved; must be set to zero	2 bits
	First_Frag; set to one for first fragment only	1 bit
	Last_Frag; set to one for last fragment only	1 bit
	Frag_seq; fragment sequence count, incremented for each fragment.	4 bits

C.8.2.6.3 Service flow extended header

The Service Flow EH Element is used to enhance Service Flow operations. It may consist of one or two bytes in the EH_VALUE field. The Payload Header Suppression Header is the only byte in a one byte field or the first byte in a two byte field. The Unsolicited Grant Synchronization Header is the second byte in a two byte field.

C.8.2.6.3.1 Payload header suppression header

In Payload Header Suppression (PHS), a repetitive portion of the payload headers following the HCS is suppressed by the sending entity and restored by the receiving entity. In the upstream, the sending entity is the CM and the receiving entity is the CMTS. In the downstream, the sending entity is the CMTS and the receiving entity is the CM.

For small payloads, Payload Header Suppression provides increased bandwidth efficiency without having to use compression. Payload Header Suppression may be separately provisioned in the upstream and downstream, and is referenced with an extended header element.

A compliant CM MUST support Payload Header Suppression. A compliant CMTS MAY support Payload Header Suppression.

This is not intended to imply that the CM must be capable of determining when to invoke Payload Header Suppression. Payload Header Suppression support is only required for the explicitly signalled case.

The Payload Header Suppression Extended Header subelement has the following format:

Table C.8-15/J.112 – Payload header suppression EHDR subelement format

EH element fields	Usage		Size
EH_TYPE	Service Flow EH_TYPE = 5 for downstream and EH_TYPE = 6 for upstream		4 bits
EH_LEN	Length of EH_VALUE = 1		4 bits
EH_VALUE	0	Indicates no payload header suppression on current packet.	8 bits
	1-255	Payload Header Suppression Index (PHSI)	

The Payload Header Suppression Index is unique per SID in the upstream and unique per CM in the downstream. Payload Header Suppression is disabled if this Extended Header element is omitted or, if included, with the PHSI value set to 0. The Payload Header Suppression Index (PHSI) references the suppressed byte string known as a Payload Header Suppression Field (PHSF).

While PHS Signalling allows for up to 255 Payload Header Suppression Rules per Service Flow, the exact number of PHS rules supported per Service Flow is implementation dependent. Similarly, PHS Signalling allows for PHS Sizes of up to 255 bytes, however, the maximum PHS Size supported is implementation dependent. For interoperability, the minimum PHS Size that MUST be supported is 64 bytes for any PHS rule supported. As with any other parameter requested in a Dynamic Service Request, a PHS-related DSx request can be denied because of a lack of resources.

The Upstream Suppression Field MUST begin with the first byte following the MAC Header Checksum. The Downstream Suppression Field MUST begin with the thirteenth byte following the MAC Header Checksum. This allows the Ethernet SA and DA to be available for filtering by the CM.

The operation of Baseline Privacy is not affected by the use of PHS. When Fragmentation is inactive, Baseline Privacy begins encryption and decryption with the thirteenth byte following the MAC Header checksum.

Unless the entire Packet PDU is suppressed, the Packet PDU CRC is always transmitted, and MUST be calculated only on the bytes transmitted. The bytes that are suppressed MUST NOT be included in the CRC calculation.

C.8.2.6.3.2 Unsolicited grant synchronization header

The Unsolicited Grant Synchronization Header may be used to pass status information regarding Service Flow scheduling between the CM and CMTS. It is currently only defined for use in the upstream with Unsolicited Grant and Unsolicited Grant with Activity Detection scheduling services. (Refer to C.10.2.)

This extended header is similar to the Payload Suppression EHDR except that the EH_LEN is 2, and the EH_VALUE has one additional byte which includes information related to Unsolicited Grant Synchronization. For all other Service Flow Scheduling Types, the field SHOULD NOT be included in the Extended Header Element generated by the CM. The CMTS MAY ignore this field.

Table C.8-16/J.112 – Unsolicited grant synchronization EHDR subelement format

EH element fields	Usage		Size
EH_TYPE	Service Flow EH_TYPE = 6		4 bits
EH_LEN	Length of EH_VALUE = 2		4 bits
EH_VALUE	0	Indicates no payload header suppression on current packet.	8 bits (always present)
	1-255	Payload Header Suppression Index (PHSI)	
	Queue Indicator		1 bit
	Active Grants		7 bits

C.8.2.7 Fragmented MAC frames

When enabled, fragmentation is initiated any time the grant length is less than the requested length. This normally occurs because the CMTS chooses to grant less than the requested bandwidth.

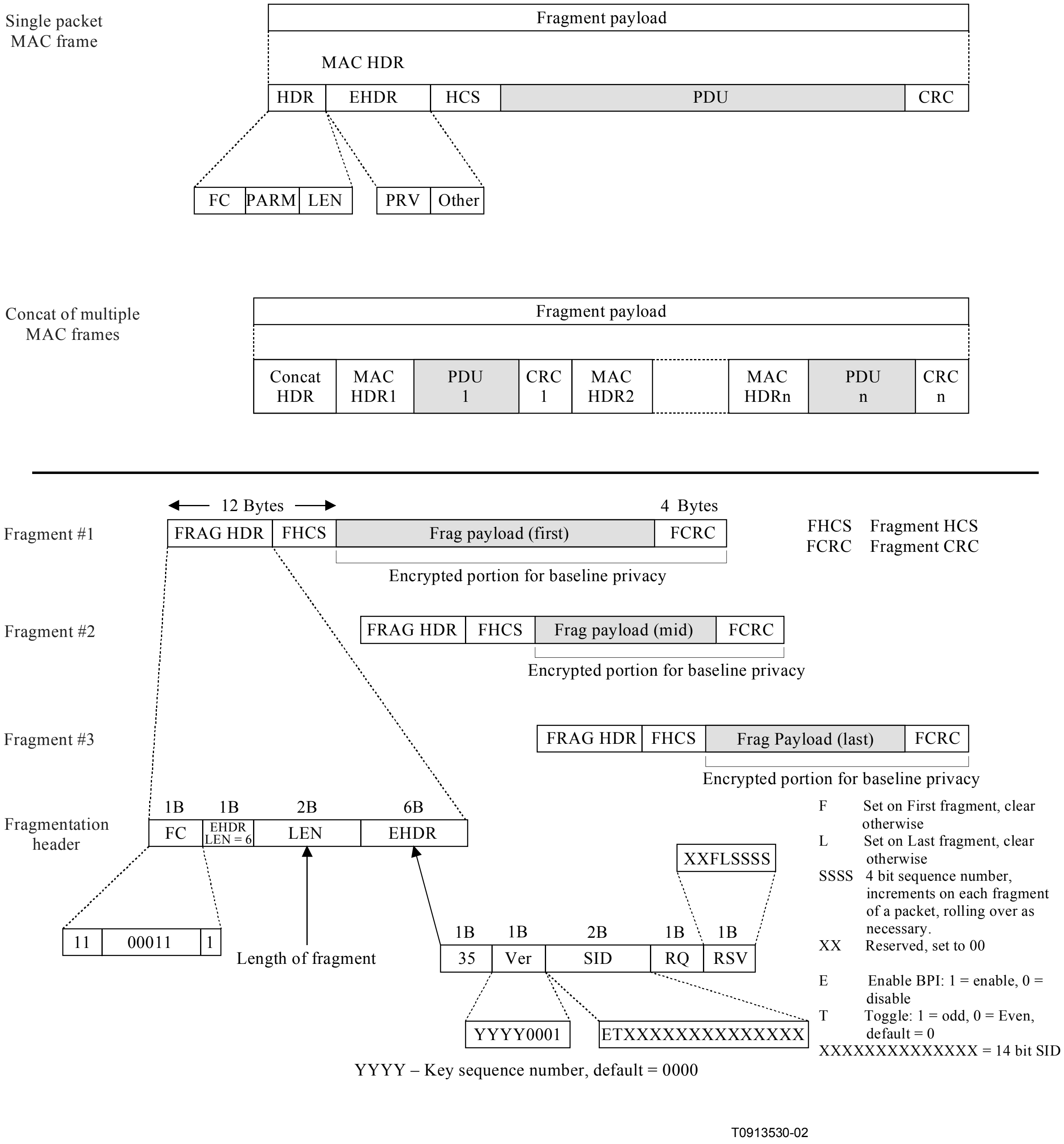


Figure C.8-13/J.112 – Fragmentation details

The CM MAC calculates how many bytes of the original frame, including overhead for a fragmentation header and CRC, can be sent in the received grant. The CM MAC generates a fragmentation header for each fragment. Fragmented frames use the MAC Message type (FC = 11). The FC parameter field is set to (00011), in order to uniquely identify the fragmentation header from other MAC Message types. A four bit sequence field is used in the last byte of the Extended Header field to aid in reassembly and to detect dropped or missing fragments. The CM arbitrarily selects a sequence number for the first fragment of a frame (see Note). Once the sequence number is selected for the first fragment, the CM MUST increment the sequence number by one for each fragment transmitted for that frame. There are two flags associated with the sequence number, F and L, where F is set to indicate the first fragment and L is set to indicate the last fragment. Both are cleared for middle fragments. The CMTS stores the sequence number of the first fragment (F bit set) of each frame. The CMTS MUST verify that the fragment sequence field increments (by one) for each fragment of the frame.

NOTE – "Frame" always refers to either frames with a single Packet PDU or concatenated frame.

The REQ field in the fragmentation header is used by the fragmentation protocol for First and Middle fragments (refer to C.10.3). For the Last fragment, the REQ field is interpreted as a request for bandwidth for a subsequent frame.

Fragmentation headers are fixed size and MUST contain only a Fragmentation extended header element. The extended header consists of a Privacy EH element extended by one byte to make the fragment overhead an even 16 bytes. A Privacy EH element is used whether the original packet header contained a Privacy EH element or not. If privacy is in use, Key Sequence number, Version, Enable bit, Toggle bit and SID in the fragment EH element are the same with those of BP EH element inside the original MAC frame. If privacy is not in use, the Privacy EH element is used but the enable bit is cleared. The SID used in the fragment EH element MUST match the SID used in the Partial Grant that initiated the fragmentation. The same extended header must be used for all fragments of a packet. A separate CRC must be calculated for each fragment (note that each MAC frame payload will also contain the CRC for that packet). A packet CRC of a reassembled packet MAY be checked by the CMTS even though an FCRC covers each fragment.

The CMTS MUST make certain that any fragmentary grant it makes is large enough to hold at least 17 bytes of MAC layer data. This is to ensure that the grant is large enough to accommodate fragmentation overhead plus at least 1 byte of actual data. The CMTS may want to enforce an even higher limit as small fragments are extremely inefficient.

When Fragmentation is active, Baseline Privacy encryption and decryption begin with the first byte following the MAC Header checksum.

C.8.2.7.1 Considerations for concatenated packets and fragmentation

MAC Management Messages and Data PDUs can occur in the same concatenated frame. Without fragmentation, the MAC Management Messages within a concatenated frame would be unencrypted. However, with fragmentation enabled on the concatenated frame, the entire concatenated frame is encrypted based on the Privacy Extended Header Element. This allows Baseline Privacy to encrypt each fragment without examining its contents. Clearly, this only applies when Baseline Privacy is enabled.

To ensure encryption synchronization, if fragmentation, concatenation and Baseline Privacy are all enabled, a CM MUST NOT concatenate BPKM MAC Management messages. This ensures that BPKM MAC Management messages are always sent unencrypted.

C.8.2.8 Error-handling

The cable network is a potentially harsh environment that can cause several different error conditions to occur. This clause, together with C.11.5, describes the procedures that are required when an exception occurs at the MAC framing level.

The most obvious type of error occurs when the HCS on the MAC Header fails. This can be a result of noise on the network or possibly by collisions in the upstream channel. Framing recovery on the downstream channel is performed by the MPEG transmission convergence sublayer. In the upstream channel, framing is recovered on each transmitted burst, such that framing on one burst is independent of framing on prior bursts. Hence, framing errors within a burst are handled by simply ignoring that burst; i.e., errors are unrecoverable until the next burst.

A second exception, which applies only to the upstream, occurs when the Length field is corrupted and the MAC thinks the frame is longer or shorter than it actually is. Synchronization will recover at the next valid upstream data interval.

For every MAC transmission, the HCS MUST be verified. When a bad HCS is detected, the MAC Header and any payload MUST be dropped.

For Packet PDU transmissions, a bad CRC may be detected. Since the CRC only covers the Data PDU and the HCS covers the MAC Header; the MAC Header is still considered valid. Thus, the Packet PDU MUST be dropped, but any pertinent information in the MAC Header (e.g., bandwidth request information) MAY be used.

C.8.2.8.1 Error recovery during fragmentation

There are some special error handling considerations for fragmentation. Each fragment has its own fragmentation header complete with an HCS and its own FCRC. There MAY be other MAC headers and CRCs within the fragmented payload. However, only the HCS of the fragment header and the FCRC are used for error detection during fragment reassembly.

If the HCS for a fragment fails, the CMTS MUST discard that fragment. If the HCS passes but the FCRC fails, the CMTS MUST discard that fragment, but MAY process any requests in the fragment header. The CMTS SHOULD process such a request if it is performing fragmentation in Piggyback Mode. (Refer to C.10.3.2.2.) This allows the remainder of the frame to be transmitted as quickly as possible.

If a CMTS is performing fragmentation in Multiple Grant Mode (refer to C.10.3.2.1) it SHOULD complete all the grants necessary to fulfill the CM's original request even if a fragment is lost or discarded. This allows the remainder of the frame to be transmitted as quickly as possible.

If any fragment of a non-concatenated MAC frame is lost or discarded the CMTS MUST discard the rest of that frame. If a fragment of a concatenated MAC frame is lost or discarded the CMTS MAY forward any frames within the concatenation that have been received correctly, or it MAY discard all the frames in the concatenation.

A CMTS MUST terminate fragment reassembly if any of the following occurs for any fragment on a given SID:

- the CMTS receives a fragment with the L bit set;
- the CMTS receives an upstream fragment, other than the first one, with the F bit set;
- the CMTS receives a packet PDU frame with no fragmentation header;
- the CMTS deletes the SID for any reason.

In addition, the CMTS MAY terminate fragment reassembly based on implementation-dependent criteria such as a reassembly timer. When a CMTS terminates fragment reassembly it MUST dispose of (either by discarding or forwarding) the reassembled frame(s).

C.8.2.8.2 Error codes and messages

Annex C.J lists CM and CMTS error codes and messages. When reporting error conditions, these codes MAY be used as indicated in "Data-Over-Cable Service Interface Specifications, 1.1 Operations Support System Interface Specification, SP-OSSIv1.1-I02-000714" and MAY be used for reporting errors via vendor-specific interfaces. If the error codes are used, the error messages MAY be replaced by other descriptive messages.

C.8.3 MAC management messages

C.8.3.1 MAC management message header

MAC Management Messages MUST be encapsulated in an LLC unnumbered information frame per [ISO/IEC8802-2], which in turn is encapsulated within the cable network MAC framing, as shown in Figure C.8-14. Figure C.8-14 shows the MAC Header and the MAC Management Message Header fields which are common across all MAC Management Messages.

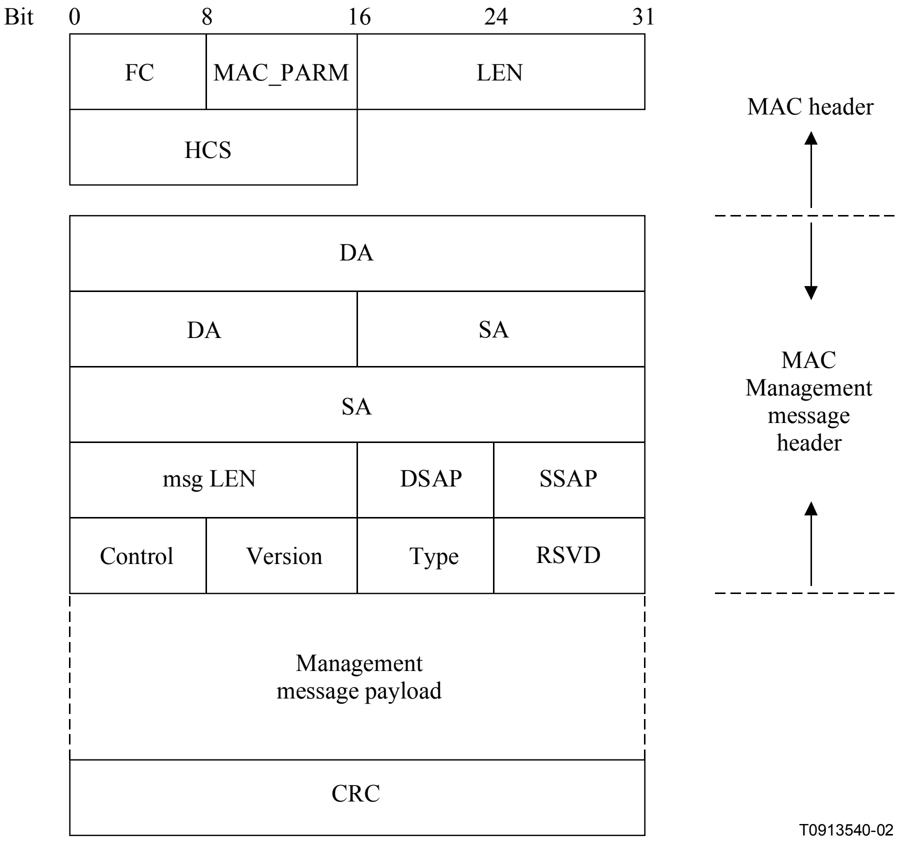


Figure C.8-14/J.112 – MAC header and MAC management message header fields

The fields MUST be as defined below.

FC, MAC_PARM, LEN, HCS: Common MAC frame header-refer to subclause C.8.2.1.4 for details. All messages use a MAC-specific header.

Destination Address (DA): MAC management frames will be addressed to a specific CM unicast address or to the Annex C/J.112 management multicast address. These MAC management addresses are described in Annex C.A.

Source Address (SA): The MAC address of the source CM or CMTS system.

Msg Length: Length of the MAC message from DSAP to the end of the payload.

DSAP: The LLC null destination SAP (00) as defined by [ISO/IEC8802-2].

SSAP: The LLC null source SAP (00) as defined by [ISO/IEC8802-2].

Control: Unnumbered information frame (03) as defined by [ISO/IEC8802-2].

Version and Type: Each 1 octet. Refer to Table C.8-17.

Table C.8-17/J.112 – MAC management message types

Type value	Version	Message name	Message description
1	1	SYNC	Timing Synchronization
2	1	UCD	Upstream Channel Descriptor
3	1	MAP	Upstream Bandwidth Allocation
4	1	RNG-REQ	Ranging Request
5	1	RNG-RSP	Ranging Response
6	1	REG-REQ	Registration Request
7	1	REG-RSP	Registration Response
8	1	UCC-REQ	Upstream Channel Change Request
9	1	UCC-RSP	Upstream Channel Change Response
10	1	TRI-TCD	Telephony Channel Descriptor
11	1	TRI-TSI	Termination System Information
12	1	BPKM-REQ	Privacy Key Management Request
13	1	BPKM-RSP	Privacy Key Management Response
14	2	REG-ACK	Registration Acknowledge
15	2	DSA-REQ	Dynamic Service Addition Request
16	2	DSA-RSP	Dynamic Service Addition Response
17	2	DSA-ACK	Dynamic Service Addition Acknowledge
18	2	DSC-REQ	Dynamic Service Change Request
19	2	DSC-RSP	Dynamic Service Change Response
20	2	DSC-ACK	Dynamic Service Change Acknowledge
21	2	DSD-REQ	Dynamic Service Deletion Request
22	2	DSD-RSP	Dynamic Service Deletion Response
23	2	DCC-REQ	Dynamic Channel Change Request
24	2	DCC-RSP	Dynamic Channel Change Response
25	2	DCC-ACK	Dynamic Channel Change Acknowledge
26	2	DCI-REQ	Device Class Identification Request
27	2	DCI-RSP	Device Class Identification Response
28	2	UP-DIS	Upstream Transmitter Disable
29-255			Reserved for future use

RSVD: 1 octet. This field is used to align the message payload on a 32 bit boundary. Set to 0 for this version.

Management Message Payload: Variable length. As defined for each specific management message.

CRC: Covers message including header fields (DA, SA,...). Polynomial defined by [ISO/IEC8802-3].

A compliant CMTS or CM MUST support the MAC management message types listed in Table C.8-17, except messages specific to Telephony Return devices, Digital Certificated devices, CPE Controled devices and DCC supported devices which MAY be supported.

C.8.3.2 Time synchronization (SYNC)

Time Synchronization (SYNC) MUST be transmitted by CMTS at a periodic interval to establish MAC sublayer timing. This message MUST use an FC field with FC_TYPE = MAC Specific Header and FC_PARM = Timing MAC Header. This MUST be followed by a Packet PDU in the format shown in Figure C.8-15.

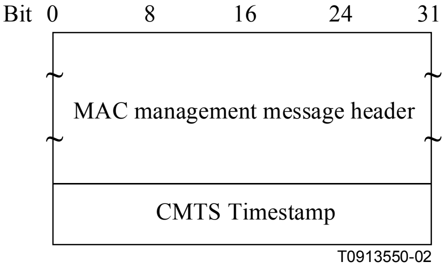


Figure C.8-15/J.112 – Format of packet PDU following the timing header

The parameters shall be as defined below.

CMTS Timestamp: The count state of an incrementing 32 bit binary counter clocked with the CMTS 9.216 MHz master clock.

The CMTS timestamp represents the count state at the instant that the first byte (or a fixed time offset from the first byte) of the Time Synchronization MAC Management Message is transferred from the Downstream Transmission Convergence Sublayer to the Downstream Physical Media Dependent Sublayer as described in C.6.3.7. The CMTS MUST NOT allow a SYNC message to cross an MPEG packet boundary (see Note).

NOTE – Since the SYNC message applies to all upstream channels within this MAC domain, units were chosen to be independent of the symbol rate of any particular upstream channel. A timebase tick represents one half the smallest possible mini-slot at the highest possible symbol rate. See C.9.3.4 for time-unit relationships.

C.8.3.3 Upstream Channel Descriptor (UCD)

An Upstream Channel Descriptor MUST be transmitted by the CMTS at a periodic interval to define the characteristics of an upstream channel (Figure C.8-16). A separate message MUST be transmitted for each active upstream.

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

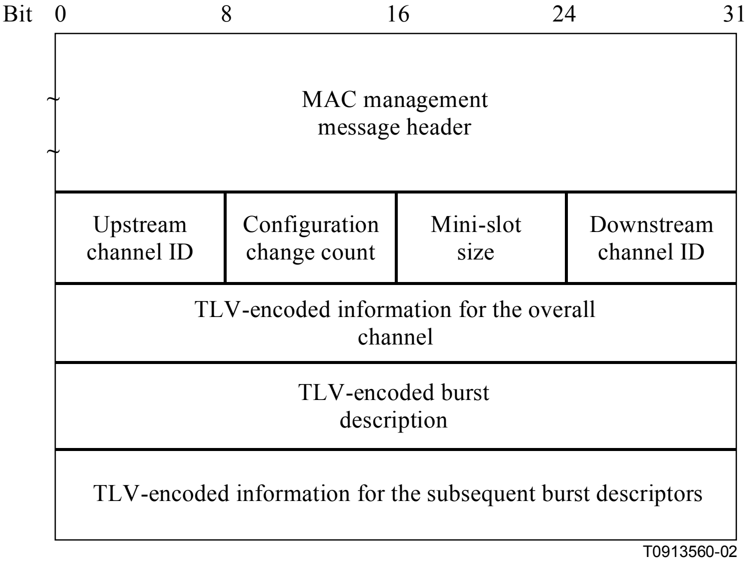

Bit 0 8 16 24 31
MAC management message header
Upstream channel ID
Configuration change count
Mini-slot size
Downstream channel ID
TLV-encoded information for the overall channel
TLV-encoded burst description
TLV-encoded information for the subsequent burst descriptors
T0913560-02

Figure C.8-16/J.112 – Upstream channel descriptor

A CMTS MUST generate UCDs in the format shown in Figure C.8-16, including all of the following parameters:

Configuration Change Count: Incremented by one (modulo the field size) by the CMTS whenever any of the values of this channel descriptor change. If the value of this count in a subsequent UCD remains the same, the CM 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 MAP.

Mini-Slot Size: The size T of the Mini-Slot for this upstream channel in units of the Timebase Tick of 6.94 µs. Allowable values are $T = 2^M$, M = 1,...7. That is, T = 2, 4, 8, 16, 32, 64 or 128.

Upstream Channel ID: The identifier of the upstream channel to which this message refers. This identifier is arbitrarily chosen by the CMTS and is only unique within the MAC-Sublayer domain.

NOTE – Upstream Channel ID = 0 is reserved to indicate telephony return.

Downstream Channel ID: The identifier of the downstream channel on which this message has been transmitted. This identifier is arbitrarily chosen by the CMTS and is only unique within the MAC-Sublayer domain.

All other parameters are coded as TLV tuples. The type values used MUST be those defined in Table C.8-18, for channel parameters, and Table C.8-19, for upstream physical layer burst attributes. Channel-wide parameters (types 1-3 in Table C.8-18) MUST precede burst descriptors (type 4 below).

Table C.8-18/J.112 – Channel TLV parameters

Name	Type (1 byte)	Length (1 byte)	Value (Variable length)
Symbol rate	1	1	Multiples of base rate of 144 ksym/s. (Value is 1, 2, 4, 8, or 16.)
Frequency	2	4	Upstream center frequency (Hz)
Preamble pattern	3	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.
Burst descriptor	4	N	May appear more than once; described below.

Burst Descriptors are composed of an upstream Interval Usage Code, followed by TLV encodings that define, for each type of upstream usage interval, the physical-layer characteristics that are to be used during that interval. The upstream interval usage codes are defined in the MAP message (see C.8.3.4 and Table C.8-20). The format of the Burst Descriptor is shown in Figure C.8-17.

Bit 0	8	16	24
Type = 4 burst descriptor	Length (n)	Internal usage code	TLV codes for PHY parameters (n-1)

Type	4 for Burst Descriptor
Lenght	The number of bytes in the overall object, including the IUC and the embedded TLV items.
IUC	Interval Usage code defined in Table C.8-20. The IUC is coded on the 4 less significant bits. The 4 most significant bits are unused (= 0).
TLV items	TLV parameters described in Table C.8-19.

Figure C.8-17/J.112 – Top-level encoding for a burst descriptor

A Burst Descriptor MUST be included for each Interval Usage Code that is to be used in the allocation MAP. The Interval Usage Code MUST be one of the values from Table C.8-20.

Within each Burst Descriptor is an unordered list of Physical-layer attributes, encoded as TLV values. These attributes are shown in Table C.8-19.

Table C.8-19/J.112 – Upstream physical-layer burst attributes

Name	Type (1 byte)	Length (1 byte)	Value (variable length)
Modulation type	1	1	1 = QPSK, 2 = 16-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 16-QAM)

Name	Type (1 byte)	Length (1 byte)	Value (variable length)
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 C.8-18). 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.
FEC error correction (T)	5	1	0-10 (0 implies no FEC. The number of codeword parity bytes is 2 × T)
FEC codeword information bytes (k)	6	1	Fixed: 16 to 253 (assuming FEC on) Shortened: 16 to 253 (assuming FEC on) (Not used if no FEC, T = 0)
Scrambler seed	7	2	The 15 bit seed value left justified in the 2 byte field. Bit 15 is the MSB of the first byte and the LSB of the second byte is not used. (Not used if scrambler is off)
Maximum burst size	8	1	The maximum number of mini-slots that can be transmitted during this burst type. Absence of this configuration setting implies that the burst size is limited elsewhere. When the interval type is Short Data Grant this value MUST be present and greater than zero. (See C.9.1.2.5.)
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 CMs and CMTS all use the same value.)
Last codeword length	10	1	1 = fixed; 2 = shortened
Scrambler on/off	11	1	1 = on; 2 = off

C.8.3.3.1 Example of UCD encoded TLV data

An example of UCD encoded TLV data is given in Figure C.8-18.

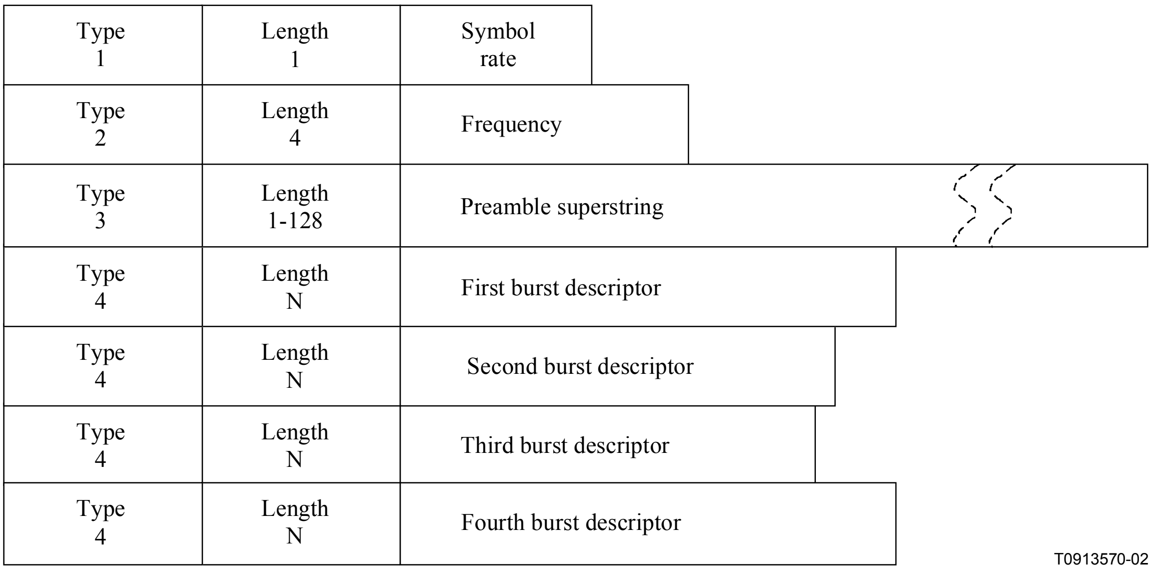


Figure C.8-18/J.112 – Example of UCD encoded TLV data

C.8.3.4 Upstream bandwidth allocation map (MAP)

A CMTS MUST generate MAPs in the format shown in Figure C.8-19.

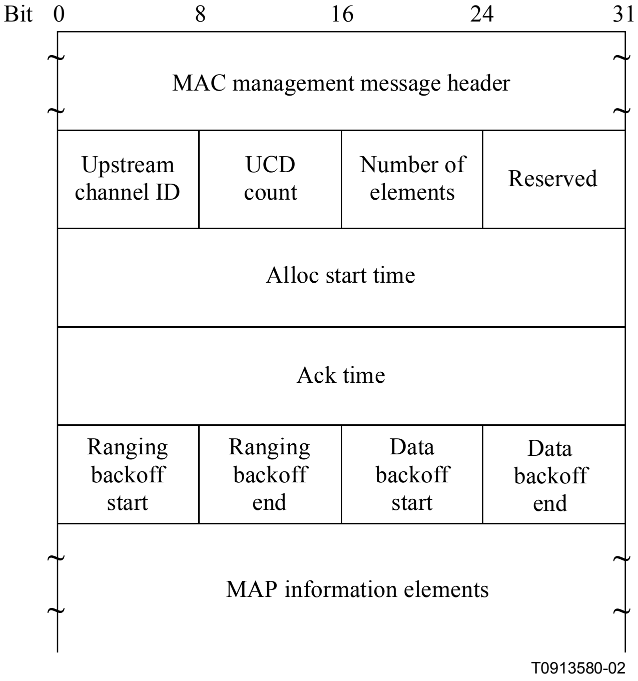


Figure C.8-19/J.112 – MAP format

The parameters MUST be as follows:

Upstream Channel ID: The identifier of the upstream channel to which this message refers.

UCD Count: Matches the value of the Configuration Change Count of the UCD which describes the burst parameters which apply to this map. See C.11.3.2.

Number Elements: Number of information elements in the map.

Reserved: Reserved field for alignment.

Alloc Start Time: Effective start time from CMTS initialization (in mini-slots) for assignments within this map.

Ack Time: Latest time, from CMTS initialization, (mini-slots) processed in upstream. This time is used by the CMs for collision detection purposes. See C.9.4.

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

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

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

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

MAP Information Elements: MUST be in the format defined in Figure C.8-20 and Table C.8-20. Values for IUCs are defined in Table C.8-20 and are described in detail in C.9.1.2.

That the lower (26-M) bits of the Alloc Start Time and Ack Time MUST be used as the effective MAP start and ack times where M is given in C.8.3.3. The relationship between the Alloc Start/Ack time counters and the timestamp counter is described in C.9.4.

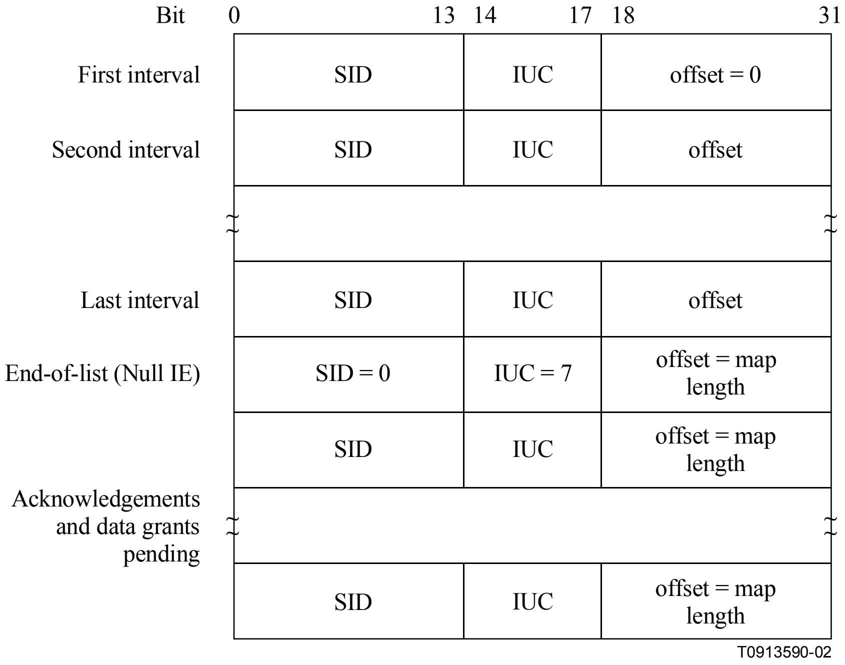


Figure C.8-20/J.112 – MAP information element structure

Table C.8-20/J.112 – Allocation MAP information elements (IE)

IE name (Note 1)	Interval usage code (IUC) (4 bits)	SID (14 bits)	Mini-slot offset (14 bits)
Request	1	Any	Starting offset of REQ region
REQ/Data (refer to Annex C.A for multicast definition)	2	Multicast	Starting offset of IMMEDIATE Data region (well-known multicasts define start intervals)
Initial Maintenance	3	Broadcast	Starting offset of MAINT region (used in Initial Ranging)
Station Maintenance (Note 2)	4	unicast (Note 3)	Starting offset of MAINT region (used in Periodic Ranging)
Short Data Grant (Note 4)	5	unicast	Starting offset of Data Grant assignment; If inferred length = 0, then it is a Data Grant pending
Long Data Grant	6	unicast	Starting offset of Data Grant assignment; If inferred length = 0, then it is a Data Grant Pending
Null IE	7	zero	Ending offset of the previous grant. Used to bound the length of the last actual interval allocation
Data Ack	8	unicast	CMTS sets to map length
Reserved	9-14	any	Reserved
Expansion	15	expanded IUC	# of additional 32 bit words in this IE

NOTE 1 – Each IE is a 32 bit quantity, of which the most significant 14 bits represent the SID, the middle 4 bits the IUC, and the low-order 14 bits the mini-slot offset.

NOTE 2 – Although the distinction between Initial Maintenance and Station Maintenance is unambiguous from the Service ID type, separate codes are used to ease physical-layer configuration (see burst descriptor encodings, Table C.8-19).

NOTE 3 – The SID used in the Station Maintenance IE MUST be a Temporary SID, or the first Registration SID (and MAYbe the only one) that was assigned in the REG-RSP message to a CM.

NOTE 4 – The distinction between long and short data grants is related to the amount of data that can be transmitted in the grant. A short data grant interval MAY use FEC parameters that are appropriate to short packets while a long data grant may be able to take advantage of greater FEC coding efficiency.

C.8.3.5 Ranging request (RNG-REQ)

A Ranging Request MUST be transmitted by a CM at initialization and periodically on request from CMTS to determine network delay and request power adjustment. This message MUST use an FC_TYPE = MAC Specific Header and FC_PARM = Timing MAC Header. This MUST be followed by a Packet PDU in the format shown in Figure C.8-21.

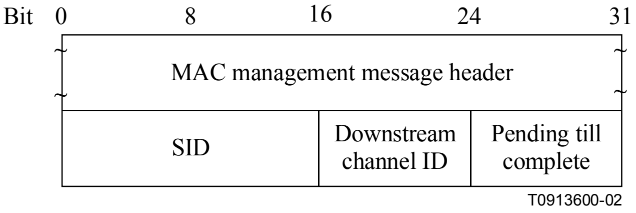


Figure C.8-21/J.112 – Packet PDU following the timing header

Parameters MUST be as follows:

SID: For RNG-REQ messages transmitted in Initial Maintenance intervals:

- Initialization SID if modem is attempting to join the network.
- Initialization SID if modem has not yet registered and is changing downstream (or both downstream and upstream) channels as directed by a downloaded parameter file.
- Temporary SID if modem has not yet registered and is changing upstream (not downstream) channels as directed by a downloaded parameter file.
- Registration SID (previously assigned in REG-RSP) if modem is registered and is changing upstream channels.

For RNG-REQ messages transmitted in Station Maintenance intervals:

- Assigned SID.

This is a 16 bit field of which the lower 14 bits define the SID with bits 14, 15 defined to be 0.

Downstream Channel ID: The identifier of the downstream channel on which the CM received the UCD which described this upstream. This is an 8 bit field.

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

C.8.3.6 Ranging response (RNG-RSP)

A Ranging Response MUST be transmitted by a CMTS in response to received RNG-REQ. The state machines describing the ranging procedure appear in C.11.2.4. In that procedure it may be noted that, from the point of view of the CM, reception of a Ranging Response is stateless. In particular, the CM MUST be prepared to receive a Ranging Response at any time, not just following a Ranging Request.

To provide for flexibility, the message parameters following the Upstream Channel ID MUST be encoded in a type/length/value (TLV) form.

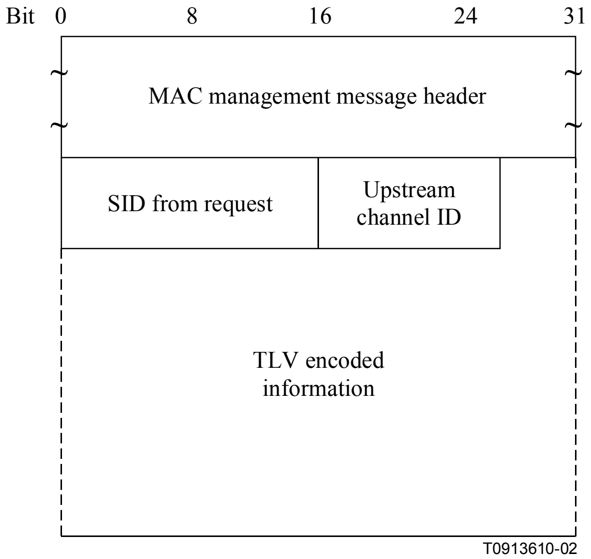


Figure C.8-22/J.112 – Ranging response

A CMTS MUST generate Ranging Responses in the form shown in Figure C.8-22, including all of the following parameters:

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

Upstream Channel ID: The identifier of the upstream channel on which the CMTS received the RNG-REQ to which this response refers. On the first ranging response received by the CM during initial ranging, this channel ID may be different from the channel ID the CM used to transmit the range. Thus, the CM MUST use this channel ID for the rest of its transactions, not the channel ID it initiated the range request from.

All other parameters are coded as TLV tuples.

Ranging Status: Used to indicate whether upstream messages are received within acceptable limits by CMTS.

Timing Adjust Information: The time by which to offset frame transmission so that frames arrive at the expected mini-slot time at the CMTS.

Power Adjust Information: Specifies the relative change in transmission power level that the CM is to make in order that transmissions arrive at the CMTS at the desired power.

Frequency Adjust Information: Specifies the relative change in transmission frequency that the CM is to make in order to better match the CMTS. (This is fine-frequency adjustment within a channel, not reassignment to a different channel.)

CM Transmitter Equalization Information: This provides the equalization coefficients for the pre-equalizer.

Downstream Frequency Override: An optional parameter. The downstream frequency with which the modem redo initial ranging (see C.8.3.6.3).

Upstream Channel ID Override: An optional parameter. The identifier of the upstream channel with which the modem redo initial ranging (see C.8.3.6.3).

C.8.3.6.1 Encodings

The type values used MUST be those defined in Table C.8-21 and Figure C.8-23. These are unique within the ranging response message but not across the entire MAC message set. The type and length fields MUST each be 1 octet in length.

Table C.8-21/J.112 – Ranging response message encodings

Name	Type (1 byte)	Length (1 byte)	Value (variable length)
Timing Adjust	1	4	TX timing offset adjustment (signed 32 bits, units of (6.94 µs/64)
Power Level Adjust	2	1	TX Power offset adjustment (signed 8 bits, 1/4 dB units)
Offset Frequency Adjust	3	2	TX frequency offset adjustment (signed 16 bits, Hz units)
Transmit Equalization Adjust	4	n	TX equalization data (see details below)
Ranging Status	5	1	1 = continue, 2 = abort, 3 = success
Downstream frequency override	6	4	Center frequency of new downstream channel in Hz
Upstream channel ID override	7	1	Identifier of the new upstream channel.
Reserved	8-255	n	Reserved for future use

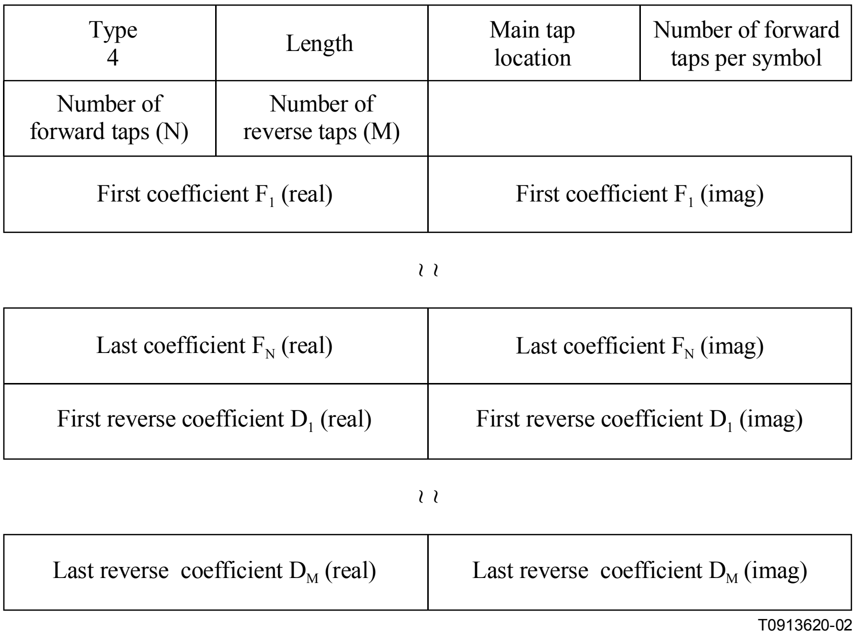

Type
4
Length
Main tap location
Number of forward taps per symbol
Number of forward taps (N)
Number of reverse taps (M)
First coefficient F_1 (real)
First coefficient F_1 (imag)
Last coefficient F_N (real)
Last coefficient F_N (imag)
First reverse coefficient D_1 (real)
First reverse coefficient D_1 (imag)
Last reverse coefficient D_M (real)
Last reverse coefficient D_M (imag)
T0913620-02

Figure C.8-23/J.112 – Generalized decision feedback equalization coefficients

The number of forward taps per symbol MUST be either 1, 2 or 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 MUST be set to "1". The number of reverse taps (M) field MUST 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 MUST 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.

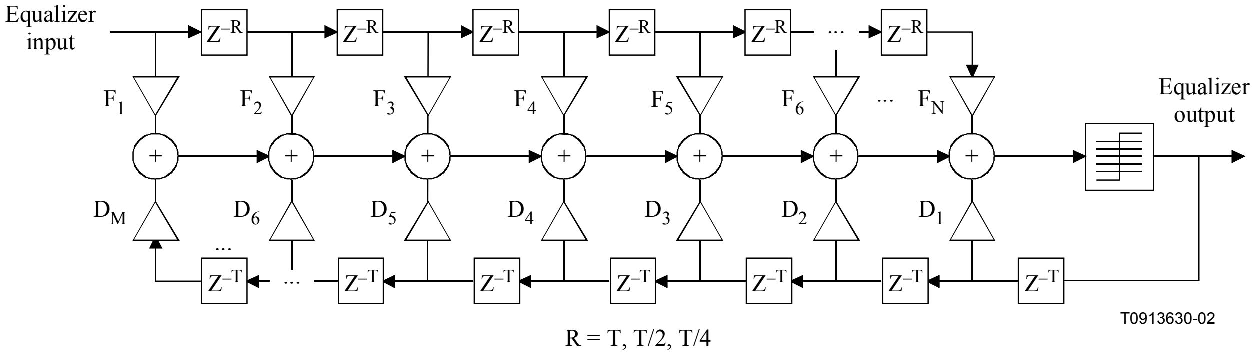


Figure C.8-24/J.112 – Generalized equalizer tap location definition

C.8.3.6.2 Example of TLV Data

An example of TLV data is given in Figure C.8-25.

Type 1	Length 4	Timing adjust
Type 2	Length 1	Power adjust
Type 3	Length 2	Frequency adjust information
Type 4	Length x	x bytes of CM transmitter equalization information
Type 5	Length 1	Ranging status

Figure C.8-25/J.112 – Example of TLV data

C.8.3.6.3 Overriding channels during initial ranging

The RNG-RSP message allows the CMTS to instruct the modem to move to a new downstream and/or upstream channel and to repeat initial ranging. However, the CMTS may do this only in response to an initial ranging request from a modem that is attempting to join the network, or in response to any of the unicast ranging requests that take place immediately after this initial ranging and up to the point where the modem successfully completes periodic ranging. If a downstream frequency override is specified in the RNG-RSP, the modem MUST reinitialize its MAC (see C.11.2) using initial ranging with the specified downstream center frequency as the first scanned channel. For the upstream channel, the modem may select any valid channel based on received UCD messages.

If an upstream channel ID override is specified in the RNG-RSP, the modem MUST reinitialize its MAC (see C.11.2) using initial ranging with the upstream channel specified in the RNG-RSP for its first attempt and the same downstream frequency on which the RNG-RSP was received.

If both downstream frequency and upstream channel ID overrides are present in the RNG-RSP, the modem MUST reinitialize its MAC (see C.11.2) using initial ranging with the specified downstream frequency and upstream channel ID for its first attempt.

Note that when a modem with an assigned temporary SID is instructed to move to a new downstream and/or upstream channel and to redo initial ranging, the modem MUST consider the temporary SID to be deassigned. The modem MUST redo initial ranging using the Initialization SID.

Configuration file settings for upstream channel ID and downstream frequency are optional, but if specified in the config file they take precedence over the ranging response parameters. Once ranging is complete, only the C.C.1.1.2, UCC-REQ, and DCC-REQ mechanisms are available for moving the modem to a new upstream channel, and only the C.C.1.1.1 mechanism and DCC-REQ is available for moving the modem to a new downstream channel.

C.8.3.7 Registration request (REG-REQ)

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

To provide for flexibility, the message parameters following the SID MUST be encoded in a type/length/value form.

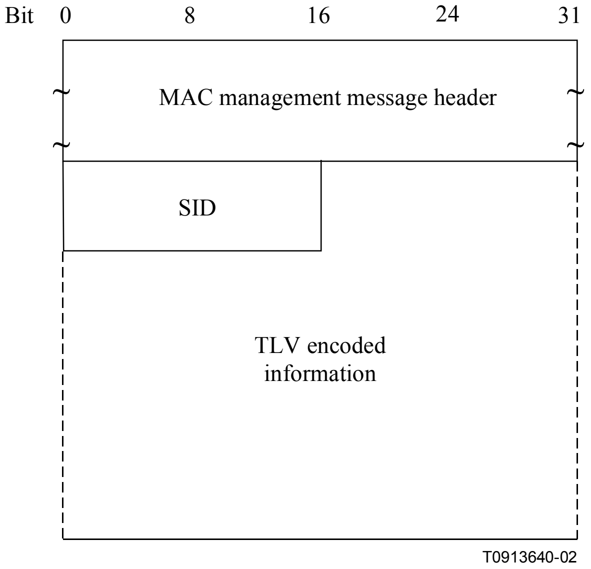


Figure C.8-26/J.112 – Registration request

A CM MUST generate Registration Requests in the form shown in Figure C.8-26, including the following parameters:

SID: Temporary SID for this CM.

All other parameters are coded as TLV tuples as defined in Annex C.C.

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

Configuration File Settings:

- Downstream Frequency Configuration Setting;
- Upstream Channel ID Configuration Setting;
- Network Access Control Object;
- Upstream Packet Classification Configuration Setting;
- Downstream Packet Classification Configuration Setting;

- Class of Service Configuration Setting;
- Upstream Service Flow Configuration Setting;
- Downstream Service Flow Configuration Setting;
- Baseline Privacy Configuration Setting;
- Maximum Number of CPEs;
- Maximum Number of Classifiers;
- Privacy Enable Configuration Setting;
- Payload Header Suppression;
- TFTP Server Timestamp;
- TFTP Server Provisioned Modem Address;
- Vendor-Specific Information Configuration Setting;
- CM MIC Configuration Setting;
- CMTS MIC Configuration Setting.

NOTE 1 – The CM MUST forward the vendor specific configuration settings to the CMTS 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 MUST be included in the Registration Request.

Vendor Specific Parameter:

- Vendor ID Configuration Setting (Vendor ID of CM).

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

- Modem Capabilities Encodings.

NOTE 2 – The CM MUST specify all of its Modem Capabilities in its Registration Request. The CMTS MUST NOT assume any Modem Capability which is defined but not explicitly indicated in the CM's Registration Request.

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

- Modem IP Address.

The following Configuration Settings MUST NOT be forwarded to the CMTS in the Registration Request.

- Software Upgrade Filename;
- Software Upgrade TFTP Server IP Address;
- SNMP Write-Access Control;
- SNMP MIB Object;
- CPE Ethernet MAC Address;
- HMAC Digest;
- End Configuration Setting;
- Pad Configuration Setting;
- Telephone Settings Option.

C.8.3.8 Registration response (REG-RSP)

A Registration response MUST be transmitted by CMTS in response to received REG-REQ.

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

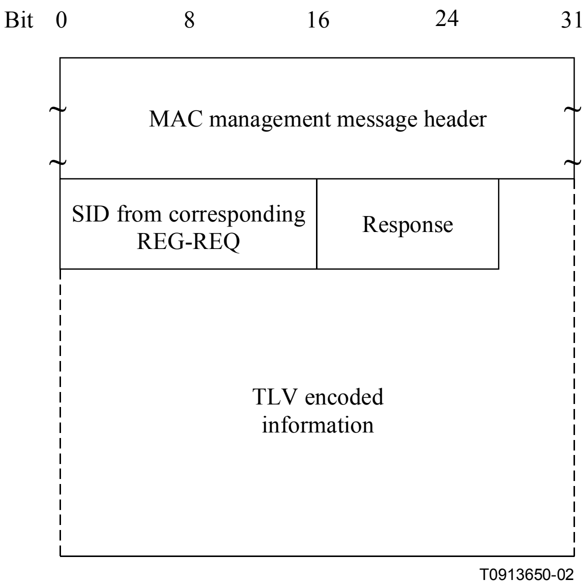


Figure C.8-27/J.112 – Registration response format

A CMTS MUST generate Registration Responses in the form shown in Figure C.8-27, including both of the following parameters:

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

Response: For REG-RSP to a modem registering as a previous Annex C/J.112 modem (i.e., REG-REQ contains previous Annex C/J.112 Class of Service Encodings)

0 = Okay

1 = Authentication Failure

2 = Class of Service Failure

For REG-RSP to a modem registering as a revised Annex C/J.112 modem (i.e., REG-REQ contains Service Flow Encodings), this field MUST contain one of the Confirmation Codes in clauses C.C.4 and C.C.4.1.

NOTE 1 – Failures apply to the entire Registration Request. Even if only a single requested Service Flow or previous Annex C/J.112 Service Class is invalid or undeliverable the entire registration is failed.

If the REG-REQ was successful, and contained Service Flow Parameters, Classifier Parameters, or Payload Header Suppression Parameters, the REG-RSP MUST contain, for each of these:

Classifier Parameters: All of the Classifier Parameters from the corresponding REG-REQ, plus the Classifier Identifier assigned by the CMTS.

Service Flow Parameters: All the Service Flow Parameters from the REG-REQ, plus the Service Flow ID assigned by the CMTS. Every Service Flow that contained a Service Class Name that was admitted/activated (see Note 2) MUST be expanded into the full set of TLVs defining the Service Flow. Every upstream Service Flow that was admitted/activated MUST have a Service Identifier assigned by the CMTS. 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.

Payload Header Suppression Parameters: All the Payload Header Suppression Parameters from the REG-REQ, plus the Payload Header Suppression Index assigned by the CMTS.

NOTE 2 – The ActiveQoSParamSet or AdmittedQoSParamSet is non-null.

If the REG-REQ failed, and contained Service Flow Parameters, Classifier Parameters, or Payload Header Suppression Parameters, and the Response is not one of the major error codes in C.C.4.1, the REG-RSP MUST contain at least one of the following:

Classifier Error Set: A Classifier Error Set and identifying Classifier Reference and Service Flow Reference MUST be included for at least one failed Classifier in the corresponding REG-REQ. Every Classifier Error Set MUST include at least one specific failed Classifier Parameter of the corresponding Classifier.

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

Payload Header Suppression Error Set: A PHS Error Set and identifying Service Flow Reference and Classifier Reference pair MUST be included for at least one failed PHS Rule in the corresponding REG-REQ. Every PHS Error Set MUST include at least one specific failed PHS Parameter of the corresponding failed PHS Rule.

Service Class Name expansion always occurs at admission time. Thus, if a Registration-Request contains a Service Flow Reference and a Service Class Name for deferred admission/activation, the Registration-Response MUST NOT include any additional QoS Parameters except the Service Flow Identifier. (Refer to C.10.1.3.)

If the corresponding Registration Request contains previous Annex C/J.112 Service Class TLV's (refer to C.C.1.1.4), the Registration Response MUST contain the following TLV tuples:

Previous Annex C/J.112 Service Class Data: Returned when Response = Okay. Service ID/service class tuple for each class of service granted. Service class IDs MUST be those requested in the corresponding REG-REQ.

Service Not Available: Returned when Response = Class of Service Failure. If a service class cannot be supported, this configuration setting is returned in place of the service class data.

All other parameters are coded TLV tuples.

Modem Capabilities: The CMTS response to the capabilities of the modem (if present in the Registration Request).

Vendor-Specific Data: As defined in Annex C.C.

– Vendor ID Configuration Setting (vendor ID of CMTS)

– Vendor-specific extensions.

C.8.3.8.1 Encodings

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

C.8.3.8.1.1 Modem capabilities

This field defines the CMTS response to the modem capability field in the Registration Request. The CMTS MUST respond to each modem capability to indicate whether they may be used. If the CMTS does not recognize a modem capability, it MUST return the TLV with the value zero ("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. Capabilities set to "off" in the REG-REQ MUST also be set to "off" in the REG-RSP.

Encodings are as defined for the Registration Request.

C.8.3.8.1.2 Previous Annex C/J.112 service class data

A previous Annex C/J.112 Service Class Data parameter MUST be present in the Registration Response for each previous Annex C/J.112 Class of Service parameter (refer to C.C.1.1.4) in the Registration Request.

This encoding defines the parameters associated with a requested class of service. It is somewhat complex in that it is composed from a number of encapsulated type/length/value fields. The encapsulated fields define the particular class of service parameters for the class of service in question. Note that the type fields defined are only valid within the encapsulated service class data configuration setting string. A single service class data configuration setting MUST be used to define the parameters for a single service class. Multiple class definitions MUST use multiple service class data configuration setting sets.

Each received previous Annex C/J.112 Class of Service parameter must have a unique Class ID in the range 1 to16. If no Class ID was present for any single previous Annex C/J.112 Class-of-Service TLV in the REG-REQ, the CMTS MUST send a REG-RSP with a class-of-service failure response and no previous Annex C/J.112 Class-of-Service TLVs.

Type	Length	Value
1	n	Encoded service class data

Class ID

The value of the field MUST specify the identifier for the class of service to which the encapsulated string applies. This MUST be a class which was requested in the associated REG-REQ, if present.

Type	Length	Value
1.1	1	from REG-REQ

Valid Range

The class ID MUST be in the range 1 to 16.

Service ID

The value of the field MUST specify the SID associated with this service class.

Type	Length	Value
1.2	2	SID

C.8.3.9 Registration acknowledge (REG-ACK)

A Registration Acknowledge MUST be transmitted by the CM in response to a REG-RSP from the CMTS. It confirms acceptance by the CM of the QoS parameters of the flow as reported by the CMTS in it REG-RSP. The format of a REG-ACK MUST be as shown in Figure C.8-28.

NOTE – The Registration-Acknowledge is a revised Annex C/J.112 message. Refer to Annex C.G for details of registration interoperability issues.

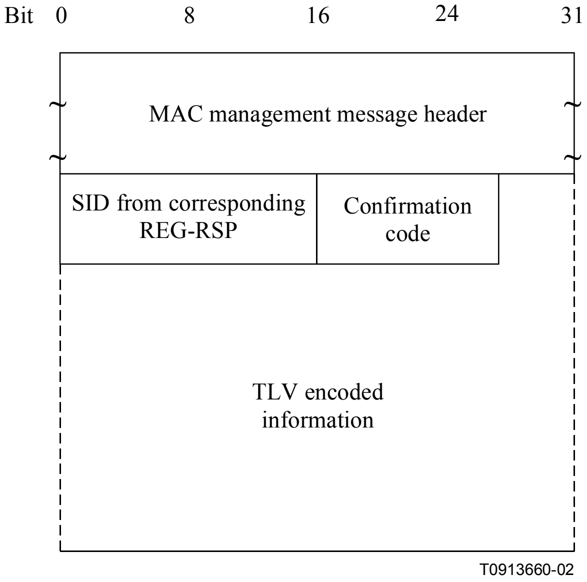


Figure C.8-28/J.112 – Registration Acknowledgment

The parameter MUST be as follows:

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

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the entire corresponding Registration Response.

The CM is required to send all provisioned Classifiers, Service Flows and Payload Header Suppression Rules to the CMTS in the REG-REQ (see C.8.3.7). The CMTS will return them with Identifiers, expanding Service Class Names if present, in the REG-RSP (see C.8.3.8). Since the CM may be unable to support one or more of these provisioned items, the REG-ACK includes Error Sets for all failures related to these provisioned items.

If there were any failures of provisioned items, the REG-ACK MUST include the Error Sets corresponding to those failures. The Error Set identification is provided by using Service Flow ID and Classifier ID from corresponding REG-RSP. If a Classifier ID or SFID was omitted in the REG-RSP, the CM MUST use the appropriate Reference (Classifier Reference, SF Reference) in the REG-ACK.

Classifier Error Set: A Classifier Error Set and identifying Classifier Reference/Identifier and Service Flow Reference/Identifier pair MUST be included for at least one failed Classifier in the corresponding REG-RSP. Every Classifier Error Set MUST include at least one specific failed Classifier Parameter of the corresponding Classifier. This parameter MUST be omitted if the entire REG-REQ/RSP is successful.

Service Flow Error Set: A Service Flow Error Set of the REG-ACK message encodes specifics of failed Service Flows in the REG-RSP message. A Service Flow Error Set and identifying Service Flow Reference/Identifier MUST be included for at least one failed QoS Parameter of at least one failed Service Flow in the corresponding REG-RSP message. This parameter MUST be omitted if the entire REG-REQ/RSP is successful.

Payload Header Suppression Error Set: A PHS Error Set and identifying Service flow Reference/Identifier and Classifier Reference/Identifier pair MUST be included for at least one failed PHS Rule in the corresponding REG-RSP. Every PHS Error Set MUST include at least one specific failed PHS of the failed PHS Rule. This parameter MUST be omitted if the entire REG-REQ/RSP is successful.

Per Service Flow acknowledgment is necessary not just for synchronization between the CM and CMTS, but also to support use of the Service Class Name. (Refer to C.10.1.3.) Since the CM 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 CM to NAK a Registration Response if it has insufficient resources to actually support this Service Flow.

C.8.3.10 Upstream channel change request (UCC-REQ)

An Upstream Channel Change Request MAY be transmitted by a CMTS to cause a CM to change the upstream channel on which it is transmitting. The format of an UCC-REQ message is shown in Figure C.8-29.

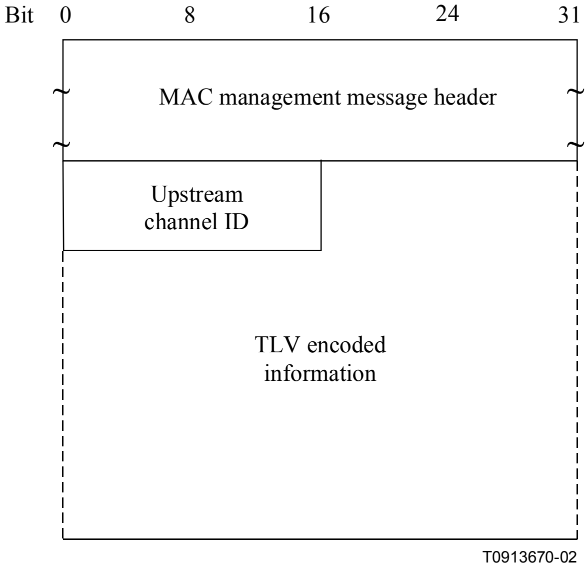


Figure C.8-29/J.112 – Upstream Channel Change Request

Parameters MUST be as follows:

Upstream Channel ID: The identifier of the upstream channel to which the CM is to switch for upstream transmissions. This is an 8 bit field.

All other parameters are coded as TLV tuples.

Ranging Technique: Directions for the type of ranging that the CM perform once synchronized to the new upstream channel.

C.8.3.10.1 Encodings

The type values used MUST be those shown below. These are unique within the Upstream Channel Change Request message, but not across the entire MAC message set. The type and length fields MUST each be 1 octet.

C.8.3.10.1.1 Ranging technique

The CMTS MAY include the Ranging Technique TLV in a UCC-REQ message to indicate what level of reranging, if any, to perform. The CMTS can make this decision based upon its knowledge of the differences between the old and new upstream channels.

For example, areas of upstream spectrum are often configured in groups. A UCC-REQ to an adjacent channel within a group may not warrant reranging. Alternatively, a UCC-REQ to a non-adjacent channel might require station maintenance whereas a UCC-REQ from one channel group to another might require initial maintenance.

Type	Length	Value
1	1	0 = Perform initial maintenance on new channel. 1 = Perform only station maintenance on new channel. 2 = Perform either initial maintenance or station maintenance on new channel (see Note). 3 = Use the new channel directly without performing initial or station maintenance.

NOTE – This value authorizes a CM to use an initial maintenance or station maintenance region, which ever the CM selects. This value might be used when there is uncertainty when the CM MAY execute the UCC and thus a chance that it might miss station maintenance slots.

If this TLV is absent, the CM MUST perform ranging with initial maintenance. For backwards compatibility, the CMTS MUST accept a CM which ignores this tuple and performs initial maintenance.

This option not be used in physical plants where upstream transmission characteristics are not consistent.

C.8.3.11 Upstream channel change response (UCC-RSP)

An Upstream Channel Change Response MUST be transmitted by a CM in response to a received Upstream Channel Change Request message to indicate that it has received and is complying with the UCC-REQ. The format of an UCC-RSP message is shown in Figure C.8-30.

Before it begins to switch to a new upstream channel, a CM MUST transmit a UCC-RSP on its existing upstream channel. A CM MAY ignore an UCC-REQ message while it is in the process of performing a channel change. When a CM receives a UCC-REQ message requesting that it switch to an upstream channel that it is already using, the CM MUST respond with a UCC-RSP message on that channel indicating that it is already using the correct channel.

After switching to a new upstream channel, a CM MUST re-range using the Ranging Technique in the corresponding UCC-REQ, and then MUST proceed without re-performing registration. The full procedure for changing channels is described in C.11.3.3.

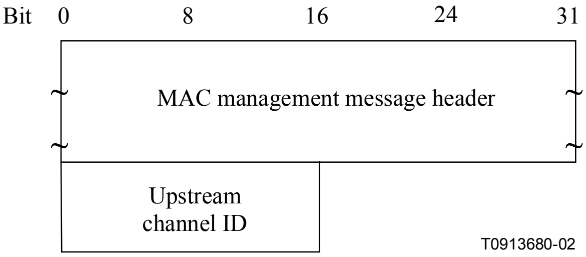


Figure C.8-30/J.112 – Upstream channel change response

Parameters MUST be as follows:

Upstream Channel ID: The identifier of the upstream channel to which the CM is to switch for upstream transmissions. This MUST be the same Channel ID specified in the UCC-REQ message. This MUST be an 8-bit field.

C.8.3.12 Dynamic service addition-request (DSA-REQ)

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

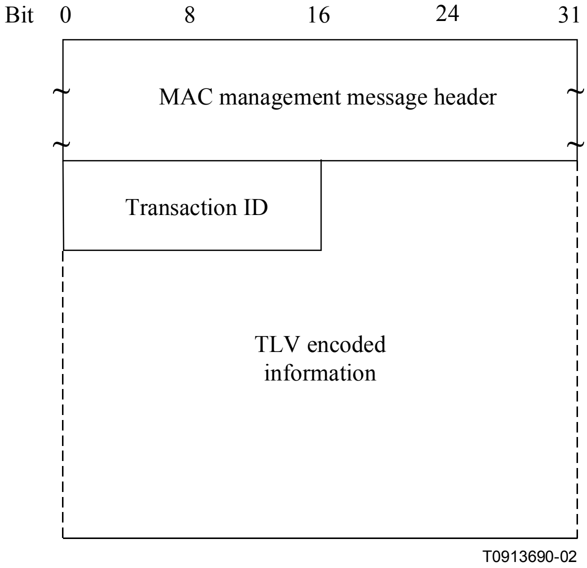


Figure C.8-31/J.112 – Dynamic service addition-request

A CM or CMTS MUST generate DSA-REQ messages in the form shown in Figure C.8-31 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 Annex C.C. A DSA-REQ message MUST NOT contain parameters for more than one Service Flow in each direction, i.e., a DSA-REQ message MUST contain parameters for either a single upstream Service Flow, or for a single downstream Service Flow, or for one upstream and one downstream Service Flow.

The DSA-REQ message MUST contain:

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

The DSA-REQ message MAY contain classifier parameters and payload header suppression parameters associated with the Service Flows specified in the message:

Classifier Parameters: Specification of the rules to be used to classify packets into a specific Service Flow.

Payload Header Suppression Parameters: Specification of the payload header suppression rules to be used with an associated classifier.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.12.1 CM-initiated dynamic service addition

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

CM-initiated DSA-Request MUST use the Classifier Reference and Service Flow Reference to link Payload Header Suppression Parameters to Classifiers and Service Flows. A DSA-request MUST use the Service Flow Reference to link Classifier to Service Flow. Values of the Classifier Reference are local to the DSA message; each Classifier within the DSA-request MUST be assigned a unique Classifier Reference.

CM-initiated DSA-Requests MAY use the Service Class Name (refer to C.C.2.2.3.4) in place of some, or all, of the QoS Parameters.

C.8.3.12.2 CMTS-initiated dynamic service addition

CMTS-initiated DSA-Requests MUST use the Service Flow ID to link Classifiers to Service Flows. Service Flow Identifiers are unique within the MAC domain. CMTS-initiated DSA-Requests for Upstream Service Flows MUST also include a Service ID.

CMTS-initiated DSA-Requests which include Classifiers, MUST assign a unique Classifier Identifier on a per Service Flow basis.

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

C.8.3.13 Dynamic service addition-response (DSA-RSP)

A Dynamic Service Addition Response MUST be generated in response to a received DSA-Request. The format of a DSA-RSP MUST be as shown in Figure C.8-32.

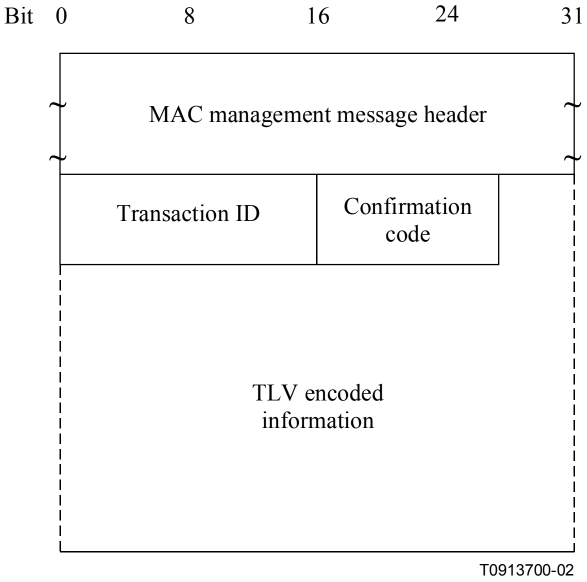


Figure C.8-32/J.112 – Dynamic Service Addition – Response

Parameters MUST be as follows:

Transaction ID: Transaction ID from corresponding DSA-REQ.

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the entire corresponding DSA-Request.

All other parameters are coded as TLV tuples as defined in Annex C.C.

If the transaction is successful, the DSA-RSP MAY contain one or more of the following:

Classifier Parameters: The complete specification of the Classifier MUST be included in the DSA-RSP only if it includes a newly assigned Classifier Identifier. If a requested Classifier contained a Classifier Reference, the DSA-RSP MUST contain a Classifier Identifier.

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

Payload Header Suppression Parameters: The complete specification of the PHS Parameters MUST be included in the DSA-RSP only if it includes a newly assigned PHS Index. If included, the PHS Parameters MUST contain a Classifier Identifier and a Service Flow Identifier.

If the transaction is unsuccessful, and the Confirmation Code is not one of the major error codes in C.C.4.2, the DSA-RSP MUST contain at least one of the following:

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

Classifier Error Set: A Classifier Error Set and identifying Classifier Reference/Identifier and Service Flow Reference/Identifier pair MUST be included for at least one failed Classifier in the corresponding DSA-REQ. Every Classifier Error Set MUST include at least one specific failed Classifier Parameter of the corresponding Classifier. This parameter MUST be omitted if the entire DSA-REQ is successful.

Payload Header Suppression Error Set: A PHS Error Set and identifying Classifier Reference/Identifier and Service Flow Reference/Identifier pair MUST be included for at least one failed PHS Rule in the corresponding DSA-REQ. Every PHS Error Set MUST include at least one specific failed PHS Parameter of the corresponding failed PHS Rule. This parameter MUST be omitted if the entire DSA-REQ is successful.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.13.1 CM-initiated dynamic service addition

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

If the corresponding DSA-Request uses the Service Class Name (refer to C.C.2.2.3.4) to request service addition, a DSA-Response MUST contain the QoS Parameter Set associated with the named Service Class. If the Service Class Name is used in conjunction with other QoS Parameters in the DSA-Request, the CMTS MUST accept or reject the DSA-Request using the explicit QoS Parameters in the DSA-Request. If these Service Flow Encodings conflict with the Service Class attributes, the CMTS MUST use the DSA-Request values as overrides for those of the Service Class.

If the transaction is successful, the CMTS MUST assign a Classifier Identifier to each requested Classifier and a PHS Index to each requested PHS Rule. The CMTS MUST use the original

Classifier Reference(s) and Service Flow Reference(s) to link the successful parameters in the DSA-RSP.

If the transaction is unsuccessful, the CMTS MUST use the original Classifier Reference(s) and Service Flow Reference(s) to identify the failed parameters in the DSA-RSP.

C.8.3.13.2 CMTS-initiated dynamic service addition

If the transaction is unsuccessful, the CM MUST use the Classifier Identifier(s) and Service Flow Identifier(s) to identify the failed parameters in the DSA-RSP.

C.8.3.14 Dynamic service addition-acknowledge (DSA-ACK)

A Dynamic Service Addition Acknowledge MUST be generated in response to a received DSA-RSP. The format of a DSA-ACK MUST be as shown in Figure C.8-33.

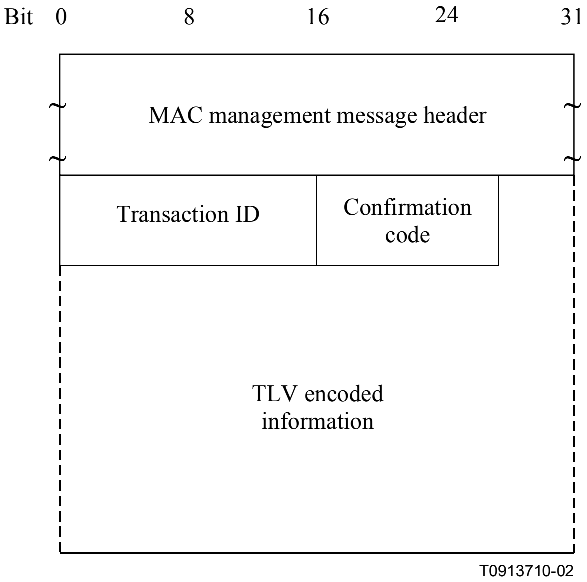


Figure C.8-33/J.112 – Dynamic service addition-acknowledge

Parameters MUST be as follows:

Transaction ID: Transaction ID from corresponding DSA-Response.

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the entire corresponding DSA-Response.

NOTE – The confirmation code is necessary particularly when a Service Class Name (refer to C.10.1.3) is used in the DSA-Request. In this case, the DSA-Response could contain Service Flow parameters that the CM is unable to support (either temporarily or as configured).

All other parameters are coded TLV tuples.

Service Flow Error Set: The Service Flow Error Set of the DSA-ACK message encodes specifics of failed Service Flows in the DSA-RSP message. A Service Flow Error Set and identifying Service Flow Reference/Identifier MUST be included for at least one failed QoS Parameter of at least one failed Service Flow in the corresponding DSA-REQ. This parameter MUST be omitted if the entire DSA-REQ is successful.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.15 Dynamic Service Change-Request (DSC-REQ)

A Dynamic Service Change Request MAY be sent by a CM or CMTS to dynamically change the parameters of an existing Service Flow. DSCs changing classifiers MUST carry the entire classifier TLV set for that new classifier.

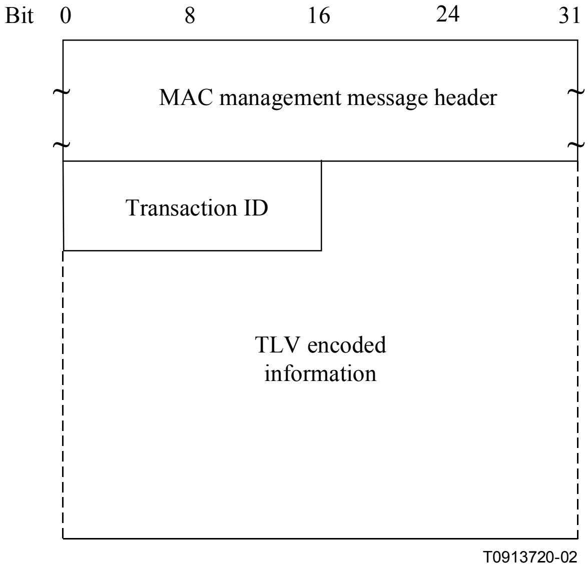


Figure C.8-34/J.112 – Dynamic Service Change-request

A CM or CMTS MUST generate DSC-REQ messages in the form shown in Figure C.8-34 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 Annex C.C. A DSC-REQ message MUST NOT carry parameters for more than one Service Flow in each direction, i.e., a DSC-REQ message MUST contain parameters for either a single upstream Service Flow, or for a single downstream Service Flow, or for one upstream and one downstream Service Flow. A DSC-REQ MUST contain at least one of the following:

Classifier Parameters: Specification of the rules to be used to classify packets into a specific service flow – this includes the Dynamic Service Change Action TLV which indicates whether this Classifier be added, replaced or deleted from the Service Flow (refer to C.C.2.1.3.7). If included, the Classifier Parameters MUST contain a Classifier Reference/Identifier and a Service Flow Identifier.

NOTE – If the DSC-REQ is CM-initiated and this is a change to an existing Classifier then this is a Classifier Identifier. If the DSC-REQ is CM-initiated and this is a new Classifier then this is a Classifier Reference.

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

Payload Header Suppression Parameters: Specification of the rules to be used for Payload Header Suppression to suppress payload headers related to a specific Classifier – this includes the Dynamic Service Change Action TLV which indicates whether this PHS Rule be added, set or deleted from the Service Flow or whether all the PHS Rules for the Service Flow specified be deleted (refer to C.C.2.2.8.5). If included, the PHS Parameters MUST contain a Classifier Reference/Identifier and a Service Flow Identifier, unless the Dynamic Service Change Action is "Delete all PHS Rules". If the Dynamic Service Change Action is "Delete all PHS Rules", the PHS Parameters MUST contain a Service Flow Identifier along with the Dynamic Service Change Action, and no other PHS parameters need be present in this case. However, if other PHS parameters are present, in particular Payload Header Suppression Index, they MUST be ignored by the receiver of the DSC-REQ message.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.16 Dynamic Service Change-Response (DSC-RSP)

A Dynamic Service Change Response MUST be generated in response to a received DSC-REQ. The format of a DSC-RSP MUST be as shown in Figure C.8-35.

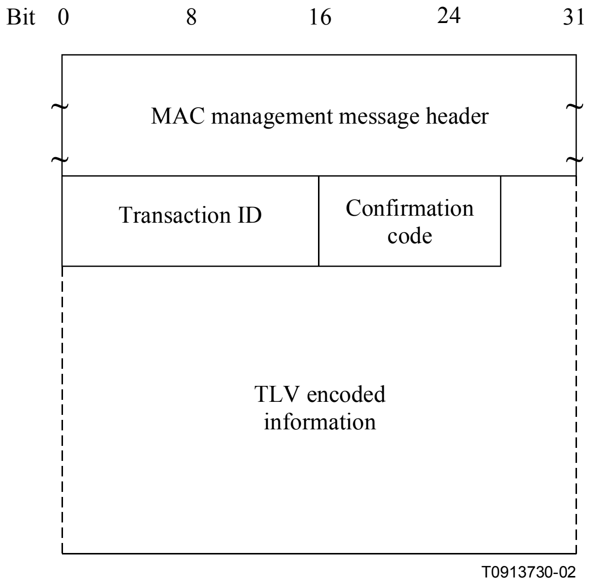


Figure C.8-35/J.112 – Dynamic Service Change-Response

Parameters MUST be as follows:

Transaction ID: Transaction ID from corresponding DSC-REQ

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the corresponding DSC-Request.

All other parameters are coded as TLV tuples as defined in Annex C.C.

If the transaction is successful, the DSC-RSP MAY contain one or more of the following:

Classifier Parameters: The complete specification of the Classifier MUST be included in the DSC-RSP only if it includes a newly assigned Classifier Identifier. If a requested Classifier contained a Classifier Reference, the DSC-RSP MUST contain a Classifier Identifier.

Service Flow Parameters: The complete specification of the Service Flow MUST be included in the DSC-RSP only if it includes an expanded Service Class Name. An SFID can only be assigned in a DSA, not in a DSC. If a Service Flow Parameter set contained an upstream Admitted QoS Parameter Set and this Service Flow does not have an associated SID, the DSC-RSP MUST include a SID. If a Service Flow Parameter set contained a Service Class Name and an Admitted QoS Parameter Set, the DSC-RSP MUST include the QoS Parameter Set corresponding to the named Service Class. If specific QoS Parameters were also included in the classed Service Flow request, these QoS Parameters MUST be included in the DSC-RSP instead of any QoS Parameters of the same type of the named Service Class.

Payload Header Suppression Parameters: The complete specification of the PHS Parameters MUST be included in the DSC-RSP only if it includes a newly assigned PHS Index. If included, the PHS Parameters MUST contain a Classifier Reference/Identifier and a Service Flow Identifier.

If the transaction is unsuccessful, and the Confirmation Code is not one of the major error codes in C.C.4.2, the DSC-RSP MUST contain at least one of the following:

Classifier Error Set: A Classifier Error Set and identifying Classifier Reference/Identifier and Service Flow Reference/Identifier pair MUST be included for at least one failed Classifier in the corresponding DSC-REQ. Every Classifier Error Set MUST include at least one specific failed Classifier Parameter of the corresponding Classifier. This parameter MUST be omitted if the entire DSC-REQ is successful.

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

Payload Header Suppression Error Set: A PHS Error Set and identifying Service Flow Reference/Identifier and Classifier Reference/Identifier pair MUST be included for at least one failed PHS Rule in the corresponding DSC-REQ, unless the Dynamic Service Change Action is "Delete all PHS Rules". If the Dynamic Service Change Action is "Delete all PHS Rules" the PHS Error Set(s) MUST include an identifying Service Flow ID. Every PHS Error Set MUST include at least one specific failed PHS Parameter of the corresponding failed PHS Rule. This parameter MUST be omitted if the entire DSC-REQ is successful.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.17 Dynamic Service Change-Acknowledge (DSC-ACK)

A Dynamic Service Change Acknowledge MUST be generated in response to a received DSC-RSP. The format of a DSC-ACK MUST be as shown in Figure C.8-36.

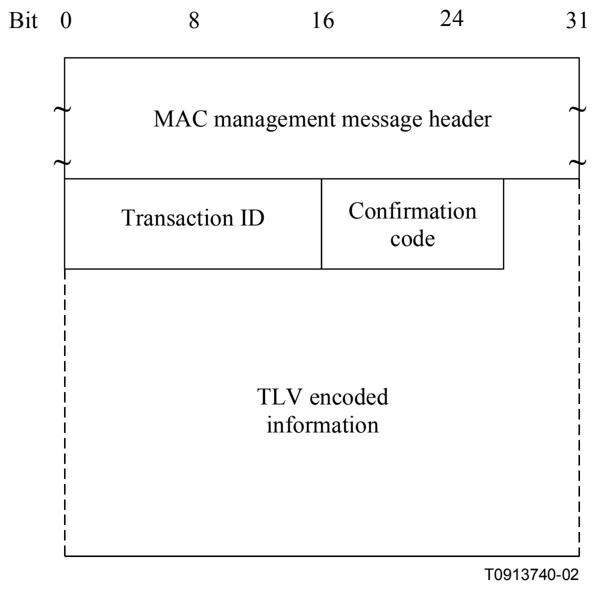


Figure C.8-36/J.112 – Dynamic Service Change-Acknowledge

Parameters MUST be as follows:

Transaction ID: Transaction ID from the corresponding DSC-REQ.

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the entire corresponding DSC-Response.

NOTE – The Confirmation Code and Service Flow Error Set are necessary particularly when a Service Class Name is (refer to C.10.1.3) used in the DSC-Request. In this case, the DSC-Response could contain Service Flow parameters that the CM is unable to support (either temporarily or as configured).

All other parameters are coded TLV tuples.

Service Flow Error Set: The Service Flow Error Set of the DSC-ACK message encodes specifics of failed Service Flows in the DSC-RSP message. A Service Flow Error Set and identifying Service Flow Identifier MUST be included for at least one failed QoS Parameter of at least one failed Service Flow in the corresponding DSC-REQ. This parameter MUST be omitted if the entire DSC-REQ is successful.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.18 Dynamic Service Deletion-Request (DSD-REQ)

A DSD-Request MAY be sent by a CM or CMTS to delete an existing Service Flow. The format of a DSD-Request MUST be as shown in Figure C.8-37.

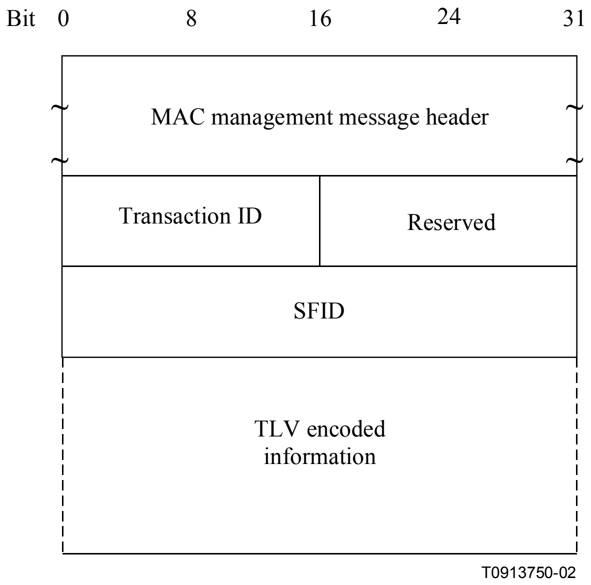


Figure C.8-37/J.112 – Dynamic Service Deletion-Request

Parameters MUST be as follows:

Service Flow Identifier: The SFID to be deleted.

Transaction ID: Unique identifier for this transaction assigned by the sender.

All other parameters are coded as TLV tuples as defined in Annex C.C.

Service Flow Reference: The CM MUST put the SFR in the DSD-REQs of a DSD-Local transaction if the transaction was created by the transition to the Deleted state from the Adding Local state. The CMTS MUST put the SFR in the DSD-REQs of a DSD-Local transaction if the transaction was created by the transition to the Deleted state from the Adding Remote state. Refer to Figure C.11-21.

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

Key Sequence Number: The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest. (Refer to C.C.1.4.3.)

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.19 Dynamic Service Deletion-Response (DSD-RSP)

A DSD-RSP MUST be generated in response to a received DSD-REQ. The format of a DSD-RSP MUST be as shown in Figure C.8-38.

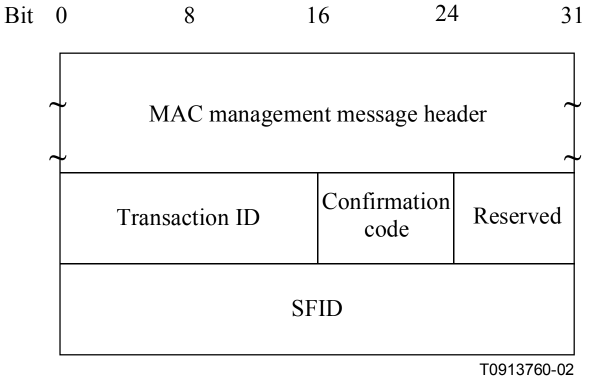


Figure C.8-38/J.112 – Dynamic Service Deletion-Response

Parameters MUST be as follows:

Service Flow Identifier: SFID from the DSD-REQ to which this acknowledgment refers.

Transaction ID: Transaction ID from corresponding DSD-REQ.

Confirmation Code: The appropriate Confirmation Code (refer to clause C.C.4) for the corresponding DSD-Request.

C.8.3.20 Dynamic Channel Change-Request (DCC-REQ)

A Dynamic Channel Change Request MAY be transmitted by a CMTS to cause a DCC-capable CM to change the upstream channel on which it is transmitting, the downstream channel it is receiving, or both.

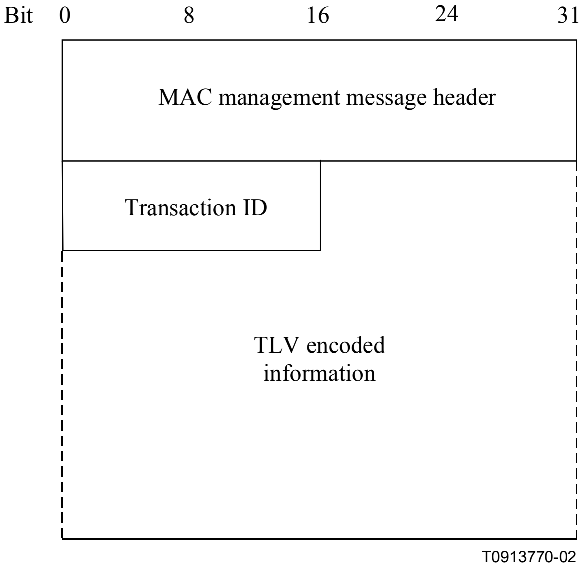


Figure C.8-39/J.112 – Dynamic Channel Change-Request

A CMTS MUST generate DCC-REQ message in the form shown in Figure C.8-39 including the following parameter:

Transaction ID: A 16 bit unique identifier for this transaction assigned by the sender.

The following parameters are optional and are coded as TLV tuples:

Upstream Channel ID: The identifier of the upstream channel to which the CM is to switch for upstream transmissions.

Downstream Parameters: The frequency of the downstream channel to which the CM is to switch for downstream reception.

Initialization Technique: Directions for the type of initialization, if any, that the CM perform once synchronized to the new channel(s).

UCD Substitution: Provides a copy of the UCD for the new channel. This TLV occurs once and contains one UCD.

SAID Substitution: A pair of Security Association Identifiers (SAID) which contain the current SAID and the new SAID for the new channel. This TLV occurs once if the SAID requires substitution.

Service Flow Substitution: A group of sub-TLVs which allows substitution in a Service Flow of the Service Flow Identifier, Service Identifier, Classifier Identifier, and the Payload Header Suppression Index. This TLV is repeated for every Service Flow which has parameters requiring substitution.

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

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Channel Change message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.20.1 Encodings

The type values used MUST be those shown below. These are unique within the Dynamic Channel Change Request message, but not across the entire MAC message set.

If a CM performs a channel change without performing a reinitialization (as defined in C.8.3.20.1.3), then all the configuration variables of the CM MUST remain constant, with the exception of the configuration variables which are explicitly changed below. The CM will not be aware of any configuration changes other than the ones that have been supplied in the DCC command, so consistency in provisioning between the old and new channels is important.

C.8.3.20.1.1 Upstream channel ID

When present, this TLV specifies the new upstream channel ID that the CM MUST use when performing a Dynamic Channel Change. It is an override for the current upstream channel ID. The CMTS MUST ensure that the Upstream Channel ID for the new channel is different than the Upstream Channel ID for the old channel. This TLV MUST be included if the upstream channel is changed, even if the UCD substitution TLV is included.

Type	Length	Value
1	1	0-255: Upstream Channel ID

If this TLV is missing, the CM MUST NOT change its upstream channel ID. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.2 Downstream Parameters

When present, this TLV specifies the operating parameters of the new downstream channel. The value field of this TLV contain a series of subtypes. The CMTS MUST include all subtypes.

Type	Length	Value
2	N	

If this TLV is missing, the CM MUST NOT change its downstream parameters.

C.8.3.20.1.2.1 Downstream Frequency

This TLV specifies the new receive frequency that the CM MUST use when performing a Dynamic Channel Change. It is an override for the current downstream channel frequency. This is the center frequency of the downstream channel in Hz and is stored as a 32-bit binary number. The downstream frequency MUST be a multiple of 62 500 Hz.

Type	Length	Value
2.1	4	Rx Frequency

The CMTS MUST include this sub-TLV. The CM MUST observe this sub-TLV.

C.8.3.20.1.2.2 Downstream Modulation Type

This TLV specifies the modulation type that is used on the new downstream channel.

Type	Length	Value
2.2	1	0 = 64-QAM 1 = 256-QAM 2-255: reserved

The CMTS SHOULD include this sub-TLV. The CM SHOULD observe this sub-TLV.

C.8.3.20.1.2.3 Downstream symbol rate

This TLV specifies the symbol rate that is used on the new downstream channel.

Type	Length	Value
2.3	1	0 = 5.274 Msym/sec 1-255: reserved

The CMTS SHOULD include this sub-TLV. The CM SHOULD observe this sub-TLV.

C.8.3.20.1.2.4 Downstream interleaver depth

This TLV specifies the parameters "I" and J of the downstream interleaver.

Subtype	Length	Value
2.4	2	I: 12 J: 17

The CMTS SHOULD include this sub-TLV. The CM SHOULD observe this sub-TLV.

C.8.3.20.1.2.5 Downstream Channel Identifier

This TLV specifies the 8 bit downstream channel identifier of the new downstream channel. The CMTS MUST ensure that the Downstream Channel ID for the new channel is different than the Downstream Channel ID for the old channel.

Subtype	Length	Value
2.5	1	0-255: Downstream Channel ID

The CMTS SHOULD include this sub-TLV. The CM SHOULD observe this sub-TLV.

C.8.3.20.1.3 Initialization technique

When present, this TLV allows the CMTS to direct the CM as to what level of reinitialization, if any, it MUST perform before it can commence communications on the new channel(s). The CMTS can make this decision based upon its knowledge of the differences between the old and new MAC domains and the PHY characteristics of their upstream and downstream channels.

Typically, if the move is between upstream and/or downstream channels within the same MAC domain, then the connection profile values may be left intact. If the move is between different MAC domains, then a complete initialization may be performed.

If a complete reinitialization is not required, some reranging MAY still be required. For example, areas of upstream spectrum are often configured in groups. A DCC-REQ to an adjacent upstream channel within a group may not warrant reranging. Alternatively, a DCC-REQ to a non-adjacent upstream channel might require station maintenance whereas a DCC-REQ from one upstream channel group to another might require initial maintenance. Reranging MAY also be required if there is any difference in the PHY parameters between the old and new channels.

Type	Length	Value
3	1	0 = Reinitialize the MAC 1 = Perform initial maintenance on new channel before normal operation. 2 = Perform station maintenance on new channel before normal operation. 3 = Perform either initial maintenance or station maintenance on new channelbefore normal operation. 4 = Use the new channel(s) directly without re-initializing or performing initialor station maintenance 5-255: reserved

The CM MUST first select the new upstream and downstream channels based upon the Upstream Channel ID TLV (refer to C.8.3.20.1.1) and the Downstream Frequency TLV (refer to C.8.3.20.1.2.1). Then the CM MUST follow the directives of this TLV. For option 0, the CM MUST begin with the Initialization SID. For options 1 to 4 the CM MUST continue to use the primary SID for ranging. A SID Substitution TLV (see C.8.3.20.1.7.2) may specify a new primary SID for use on the new channel.

Option 0: This option directs the CM to perform all the operations associated with initializing the CM (refer to C.11.2). This includes all the events after acquiring downstream QAM, FEC, and MPEG lock and before Standard Operation (refer to C.11.3), including obtaining a UCD, ranging, establishing IP connectivity, establishing time of day, transfer of operational parameters, registration, and baseline privacy initialization. When this option is used, the only other TLVs in DCC-REQ that are relevant are the Upstream Channel ID TLV and the Downstream Parameters TLV. All other DCC-REQ TLVs are irrelevant.

Option 1: If initial maintenance is specified, operation on the new channel could be delayed by several Ranging Intervals (see Annex C.B).

Option 2: If station maintenance is specified, operation on the new channel could be delayed by the value of T4 (see Annex C.B).

Option 3: This value authorizes a CM to use an initial maintenance or station maintenance region, which ever the CM selects. This value might be used when there is uncertainty when the CM MAY execute the DCC command and thus a chance that it might miss station maintenance slots.

Option 4: This option provides for the least interruption of service, and the CM may continue its normal operation as soon as it has achieved synchronization on the new channel. This option is intended for use with a near-seamless channel change (refer to C.11.4.5.3).

NOTE – This option not be used in physical plants where upstream transmission characteristics are not consistent.

If this TLV is absent, the CM MUST reinitialize the MAC. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.4 UCD substitution

When present, this TLV allows the CMTS to send an Upstream Channel Descriptor message to the CM. This UCD message is intended to be associated with the new upstream and/or downstream channel(s). The CM stores this UCD messages in its cache, and uses it after synchronizing to the new channel(s).

Type	Length	Value
4	N	UCD for the new upstream channel

This TLV includes all parameters for the UCD message as described in C.8.3.3 except for the MAC Management Message Header. The CMTS MUST ensure that the change count in the UCD matches the change count in the UCDs of the new channel(s). The CMTS MUST ensure that the Upstream Channel ID for the new channel is different than the Upstream Channel ID for the old channel.

If the CM has to wait for a new UCD message when changing channels, then operation may be suspended for a time up to the "UCD Interval" (see Annex C.B) or longer, if the UCD message is lost.

The CMTS SHOULD include this TLV. The CM SHOULD observe this TLV.

C.8.3.20.1.5 SYNC substitution

When present, this TLV allows the CMTS to inform the CM to wait or not wait for a SYNC message before proceeding. The CMTS MUST have synchronized timestamps between the old and new channel(s) if it instructs the CM to not wait for a SYNC message before transmitting on the new channel. Synchronized timestamps implies that the timestamps are derived from the same clock and contain the same value.

Type	Length	Value
5	1	0 = acquire SYNC message on the new downstream channel before proceeding 1 = proceed without first obtaining the SYNC message 2-255: reserved

If this TLV is absent, the CM MUST wait for a SYNC message on the new channel before proceeding. If the CM has to wait for a new SYNC message when changing channels, then operation may be suspended for a time up to the "SYNC Interval" (see Annex C.B) or longer, if the SYNC message is lost or is not synchronized with the old channel(s).

An alternative approach is to send SYNC messages more frequently (every 10 ms for example), and continue to require the CM to wait for a SYNC message before proceeding. This approach has the slightly more latency, but provides an additional check to prevent the CM from transmitting at an incorrect time interval.

The CMTS SHOULD include this TLV. The CM SHOULD observe this TLV.

C.8.3.20.1.6 Security Association Identifier (SAID) substitution

When present, this TLV allows the CMTS to replace the Security Association Identifier (SAID) in the current Service Flow with a new Security Association Identifier. The baseline privacy keys associated with the SAID MUST remain the same. The CM does not have to simultaneously respond to the old and new SAID.

Type	Length	Value
6	4	Current SAID (lower order 14 bits of a 16 bits field), new SAID (lower order 14 bits of a 16 bits field).

If this TLV is absent, the current Security Association Identifier assignment is retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7 Service flow substitutions

When present, this TLV allows the CMTS to replace specific parameters within the current Service Flows on the current channel assignment with new parameters for the new channel assignment. One TLV is used for each Service Flow that requires changes in parameters. The CMTS MAY choose to do this to help facilitate setting up new QoS reservations on the new channel before deleting QoS reservations on the old channel. The CM does not have to simultaneously respond to the old and new Service Flows.

This TLV allows resource assignments and services to be moved between two independent ID value spaces and scheduling entities by changing the associated IDs and indexes. ID value spaces that may differ between the two channels include the Service Flow Identifier, the Service ID, the Classifier Identifier, and the Payload Header Suppression Index. This TLV does not allow changes to Service Flow QoS parameters, classifier parameters, or PHS rule parameters.

The Service Class Names used within the Service Flow ID remain identical between the old and new channels.

Type	Length	Value
7	N	List of subtypes

If this TLV is absent for a particular Service Flow, then current Service Flow and its attributes are retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7.1 Service flow identifier substitution

This TLV allows the CMTS to replace the current Service Flow Identifier (SFID) with a new Service Flow Identifier. Refer to C.C.2.2.3.2 for details on the usage of this parameter.

This TLV MUST be present if any other Service Flow subtype substitutions are made. If this TLV is included and the Service Flow ID is not changing, then the current and new Service Flow ID will be set to the same value.

Subtype	Length	Value
7.1	8	Current Service Flow ID, new Service Flow ID

The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7.2 Service identifier substitution

When present, this TLV allows the CMTS to replace the Service Identifier (SID) in the current upstream Service Flow with a new Service Identifier. Refer to C.C.2.2.3.3 for details on the usage of this parameter.

Subtype	Length	Value
7.2	4	Current SID (lower order 14 bits of a 16 bits field), new SID (lower order 14 bits of a 16 bits field).

If this TLV is absent, the current Service Identifier assignments are retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7.3 Classifier ID substitution

When present, this TLV allows the CMTS to replace the current Classifier Identifier with a new Classifier Identifier. One TLV is used for each pair of old and new Classifier Identifier that are to be substituted within this Service Flow. Refer to C.C.2.1.3.2 for details on the usage of this parameter.

Subtype	Length	Value
7.3	4	Current Classifier ID, new Classifier ID

If this TLV is absent, the current Classifier Identifier is retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7.4 Payload header suppression index substitution

When present, this TLV allows the CMTS to replace the current Payload Header Suppression Index (PHSI) with a new Payload Header Suppression Index. Refer to C.C.2.2.10.2 for details on the usage of this parameter.

Subtype	Length	Value
7.4	2	Current PHSI, new PHSI

If this TLV is absent, the current Payload Header Suppression Index is retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.20.1.7.5 Unsolicited grant time reference substitution

When present, this TLV allows the CMTS to replace the current Unsolicited Grant Time Reference with a new Unsolicited Grant Time Reference. Refer to C.C.2.2.6.11 for details on the usage of this parameter.

This TLV is useful if the old and new upstream use different time bases for their time stamps. This TLV is also useful if the Unsolicited Grant transmission window is moved to a different point in time. Changing this value may cause operation to temporarily exceed the jitter window specified by C.C.2.2.6.8.

Subtype	Length	Value
7.5	4	New reference

If this TLV is absent, the current Unsolicited Grant Time Reference is retained. The CMTS MAY include this TLV. The CM MUST observe this TLV.

C.8.3.21 Dynamic Channel Change-Response (DCC-RSP)

A CM MAY support Dynamic Channel Change. If the CM supports Dynamic Channel Change, a Dynamic Channel Change Response MUST be transmitted by a CM in response to a received Dynamic Channel Change Request message to indicate that it has received and is complying with the DCC-REQ. The format of a DCC- RSP message MUST be as shown in Figure C.8-40.

Before it begins to switch to a new upstream or downstream channel, a CM MUST transmit a DCC-RSP on its existing upstream channel. When a CM receives a DCC-REQ message requesting that it switch to an upstream and/or downstream channel that it is already using, the CM MUST respond with a DCC-RSP message on that channel indicating that it is already using the correct channel.

A CM MAY ignore a DCC-REQ message while it is in the process of performing a channel change.

After switching to a new channel, if the MAC was not reinitialized per DCC-REQ Initialization TLV, option 0, the CM MUST send a DCC-RSP message to the CMTS. A DCC-RSP MUST NOT be sent if the CM reinitializes its MAC.

The full procedure for changing channels is described in C.11.4.5.

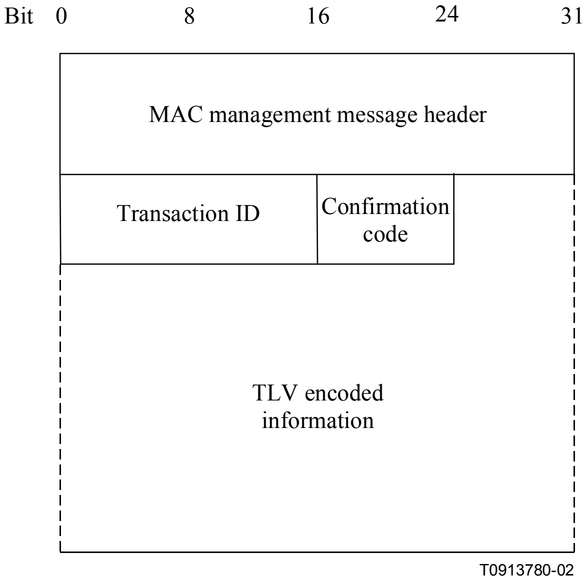


Figure C.8-40/J.112 – Dynamic Channel Change-Response

Parameters MUST be as follows:

Transaction ID: A 16 bit Transaction ID from corresponding DCC-REQ.

Confirmation Code: An 8 bit Confirmation Code as described in C.C.4.1.

The following parameters are optional and are coded as TLV tuples.

CM Jump Time: Timing parameters describing when the CM will make the jump.

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

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Channel Change message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.21.1 Encodings

The type values used MUST be those shown below. These are unique within the Dynamic Channel Change Response message, but not across the entire MAC message set.

C.8.3.21.1.1 CM jump time

When present, this TLV allows the CM to indicate to the CMTS when the CM plans to perform its jump and be disconnected from the network. With this information, the CMTS MAY take preventative measures to minimize or to eliminate packet drops in the downstream due to the channel change.

Type	Length	Value
1	N	

The time reference and units of time for these sub-TLVs is based upon the same 32 bit time base used in the SYNC message on the current downstream channel. This timestamp is incremented by a 9.216 MHz clock

The CM SHOULD include this TLV. The CMTS SHOULD observe this TLV.

C.8.3.21.1.1.1 Length of jump

This TLV indicates to the CMTS the length of the jump from the previous channel to the new channel. Specifically, it represents the length of time that the CM will not be able to receive data in the downstream.

Subtype	Length	Value
1	4	Length (based upon timestamp)

The CM MUST include this sub-TLV.

C.8.3.21.1.1.2 Start time of jump

When present, this TLV indicates to the CMTS the time in the future that the CM is planning on making the jump.

Subtype	Length	Value
2	8	Start time (based upon timestamp), accuracy of start time (based upon timestamp)

The 32 bit, 9.216 MHz time base rolls over approximately every 7 minutes. If the value of the start time is less than the current timestamp, the CMTS will assume one roll-over of the timestamp counter has elapsed. The accuracy of the start time is an absolute amount of time before and after the start time.

The potential jump window is from (start time – accuracy) to (start time + accuracy + length).

The CM SHOULD include this TLV.

C.8.3.22 Dynamic Channel Change-Acknowledge (DCC-ACK)

A Dynamic Channel Change Acknowledge MUST be transmitted by a CMTS in response to a received Dynamic Channel Change Response message on the new channel with its Confirmation Code set to arrive (1). The format of a DCC-ACK message MUST be as shown in Figure C.8-41.

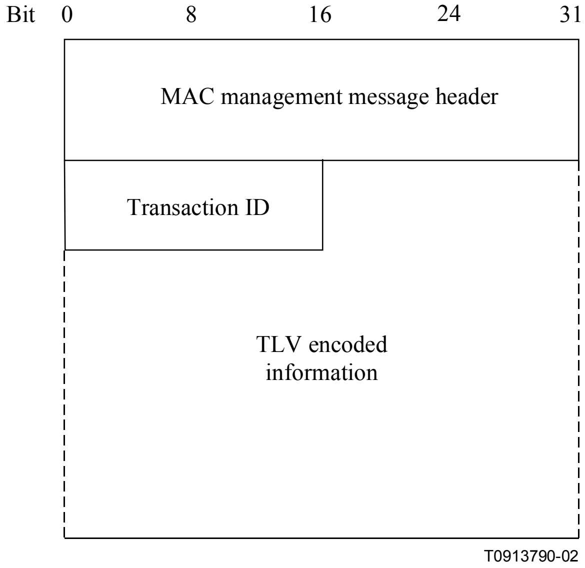


Figure C.8-41/J.112 – Dynamic Channel Change-Acknowledge

Parameters MUST be as follows:

Transaction ID: A 16 bit Transaction ID from corresponding DCC-RSP

If Privacy is enabled, the DCC-ACK message MUST contain:

HMAC-Digest: The HMAC-Digest Attribute is a keyed message digest (to authenticate the sender). The HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Channel Change message's Attribute list. (Refer to C.C.1.4.1.)

C.8.3.23 Device Class Identification-Request (DCI-REQ)

A CM MAY support the DCI-REQ message. A CMTS MUST support the DCI-REQ message.

When implemented, a CM MUST transmit a DCI-REQ immediately following receipt of a ranging complete indication from the CMTS. A CM MUST NOT continue with initialization until a DCI-RSP message is received from the CMTS. Timeout and retry information is provided in Annex C.C.

The DCI-REQ MUST be formatted as shown in Figure C.8-42.

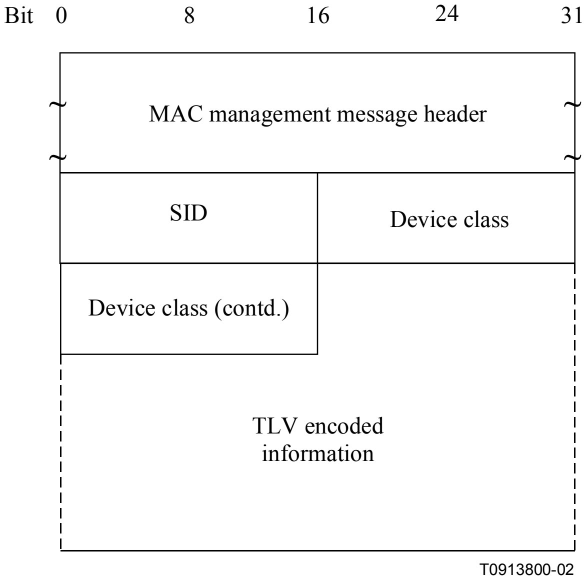


Figure C.8-42/J.112 – Device Class Identification-Request

Parameters MUST be as follows:

SID: The temporary SID assigned during Ranging.

Device Class TLV:

Type	Length	Value
1	4	Bit #0 CPE Controlled Cable Modem (CCCM) Bits #1-31 reserved and must be set to zero

Bits are set to 1 to identify the behavior of that value.

C.8.3.24 Device Class Identification-Response (DCI-RSP)

A DCI-RSP MUST be transmitted by a CMTS in response to a received DCI-REQ.

The DCI-RSP MUST be formatted as shown in Figure C.8-43.

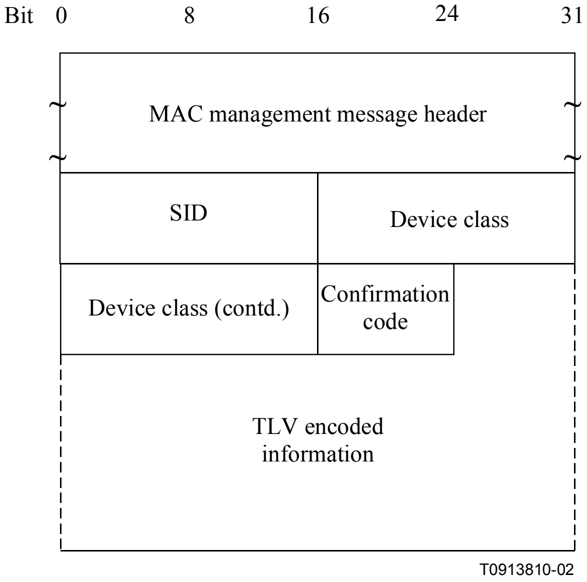


Figure C.8-43/J.112 – Device Class Identification-Response

Parameters MUST be as follows:

SID: The SID received in the associated DCI-REQ.

Device Class TLV: The device class TLV as received in the associated DCI-REQ.

Confirmation Code (refer to clause C.C.4):

The CMTS MUST use only one of 3 confirmation codes in the DCI-RSP.

If the response is reject-temporary (3), the CM MUST reset its DCI-REQ retry counter to zero and MUST resend the DCI-REQ and wait for the DCI-RSP before proceeding.

If the response is reject-permanent (4), the CM MUST abort this registration attempt and MUST begin rescanning for a different downstream channel. The CM MUST NOT retry this channel until it has tried all other Annex C/J.112 downstream channels on the network.

If the response is success (0), the CM MUST continue with registration.

The CMTS MUST retain the device class information for use in the DHCP Process. The CMTS MUST create a DHCP Agent Option 82 tuple with the device class information and MUST insert this tuple in the DHCPDISCOVER from the corresponding CM before forwarding that DHCPDISCOVER to the DHCP server.

C.8.3.25 Upstream Transmitter-Disable (UP-DIS) MAC management message

The UP-DIS MUST be coded as follows:

MAC management message header

UP-DIS is sent from a CMTS to a CM and there is no response from the CM transmitted back to the CMTS.

The CMTS MAY be capable of transmitting the UP-DIS message. Mechanisms for detecting and reporting situations where the transmission of an UP-DIS message might be appropriate are implementation dependent. Similarly, Signalling to trigger the transmission of the UP-DIS message is outside the scope of this annex.

The CM MAY support the UP-DIS message.

If supported, the CM MUST autonomously disable its upstream transmitter upon receipt of an UP-DIS message regardless of any other transaction state (refer to clause C.11). Once disabled via UP-DIS, the CM upstream transmitter MUST only be re-enabled by power cycling the CM.

Since the UP-DIS mechanism at the CM is stateless, the CMTS SHOULD incorporate mechanisms to track disabled MAC addresses and resend an UP-DIS message to modems that are powered cycled and attempt to reregister.

C.9 Media access control protocol operation

C.9.1 Upstream bandwidth allocation

The upstream channel is modeled as a stream of mini-slots. The CMTS MUST generate the time reference for identifying these slots. It MUST also control access to these slots by the cable modems. For example, it MAY grant some number of contiguous slots to a CM for it to transmit a data PDU. The CM MUST time its transmission so that the CMTS receives it in the time reference specified. This clause describes the elements of protocol used in requesting, granting, and using upstream bandwidth. The basic mechanism for assigning bandwidth management is the allocation MAP. Please refer to Figure C.9-1.

The allocation MAP is a MAC Management message transmitted by the CMTS on the downstream channel which describes, for some interval, the uses to which the upstream mini-slots MUST be put. A given MAP MAY describe some slots as grants for particular stations to transmit data in, other slots as available for contention transmission, and other slots as an opportunity for new stations to join the link.

Many different scheduling algorithms MAY be implemented in the CMTS by different vendors; the present annex does not mandate a particular algorithm. Instead, it describes the protocol elements by which bandwidth is requested and granted.

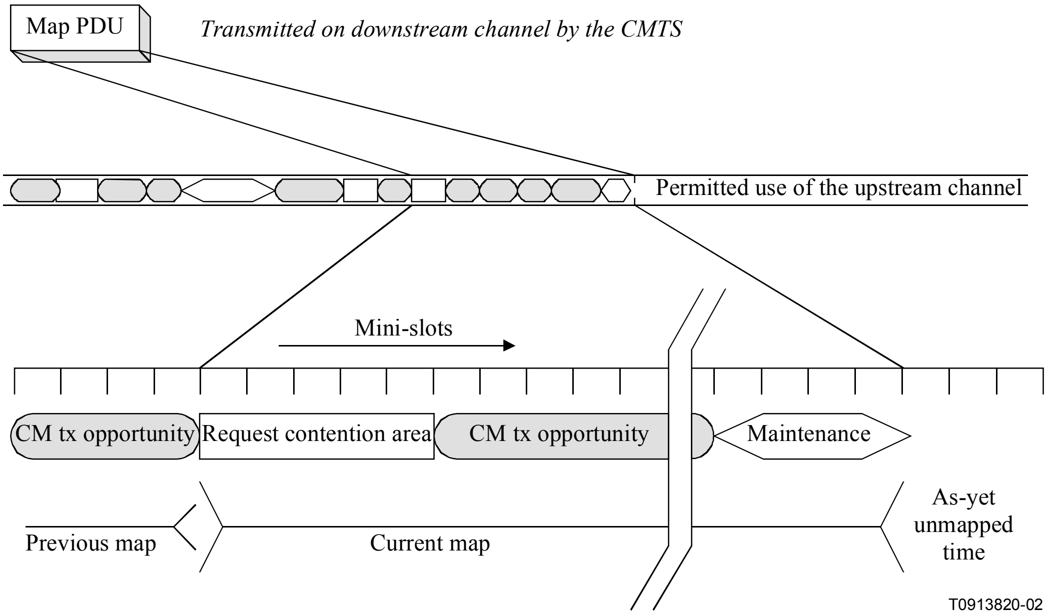


Figure C.9-1/J.112 – Allocation map

The bandwidth allocation includes the following basic elements:

- Each CM has one or more short (14 bit) service identifiers (SIDs) as well as a 48 bit address.
- Upstream bandwidth is divided into a stream of mini-slots. Each mini-slot is numbered relative to a master reference maintained by the CMTS. The clocking information is distributed to the CMs by means of SYNC packets.
- CMs may issue requests to the CMTS for upstream bandwidth.

The CMTS MUST transmit allocation MAP PDUs on the downstream channel defining the allowed usage of each mini-slot. The MAP is described below.

C.9.1.1 The allocation map MAC management message

The allocation MAP is a varying-length MAC Management message that is transmitted by the CMTS to define transmission opportunities on the upstream channel. It includes a fixed-length header followed by a variable number of information elements (IEs) in the format shown in C.8.3.4. Each information element defines the allowed usage for a range of mini-slots.

Note that it be understood by both CM and CMTS that the lower (26-M) bits of alloc start and ack times MUST be used as the effective MAP start and ack times, where M is defined in C.8.3.3. The relationship between alloc start/ack time counters and the timestamp counter is further described in C.9.3.4.

C.9.1.2 Information Elements

Each IE consists of a 14 bit Service ID, a 4 bit type code, and a 14 bit starting offset as defined in C.8.3.4. Since all stations MUST scan all IEs, it is critical that IEs be short and relatively fixed format. IEs within the MAP are strictly ordered by starting offset. For most purposes, the duration described by the IE is inferred by the difference between the IE's starting offset and that of the following IE. For this reason, a Null IE MUST terminate the list. Refer to Table C.8-20.

Four types of Service IDs are defined:

1) 0x3FFF – broadcast, intended for all stations;
2) 0x2000-0x3FFE – multicast, purpose is defined administratively. Refer to Annex C.A;
3) 0x0001-0x1FFF – unicast, intended for a particular CM or a particular service within that CM;
4) 0x0000 – null address, addressed to no station.

All of the Information Elements defined below MUST be supported by conformant CMs. Conformant CMTSs MAY use any of these Information Elements when creating Bandwidth Allocation Maps.

C.9.1.2.1 The request IE

The Request IE provides an upstream interval in which requests MAY be made for bandwidth for upstream data transmission. The character of this IE changes depending on the class of Service ID. If broadcast, this is an invitation for CMs to contend for requests. Clause C.7.4 describes which contention transmit opportunity may be used. If unicast, this is an invitation for a particular CM to request bandwidth. Unicasts MAY be used as part of a Quality of Service scheduling scheme (refer to C.10.2). Packets transmitted in this interval MUST use the Request MAC Frame format (refer to C.8.2.5.3).

A small number of Priority Request SIDs are defined in Annex C.A. These allow contention for Request IEs to be limited to service flows of a given Traffic Priority (refer to C.C.2.2.5.2).

C.9.1.2.2 The request/data IE

The Request/Data IE provides an upstream interval in which requests for bandwidth or short data packets MAY be transmitted. This IE is distinguished from the Request IE in that:

- It provides a means by which allocation algorithms MAY provide for "immediate" data contention under light loads, and a means by which this opportunity can be withdrawn as network loading increases.
- Multicast Service IDs MUST be used to specify maximum data length, as well as allowed random starting points within the interval. For example, a particular multicast ID may specify a maximum of 64-byte data packets, with transmit opportunities every fourth slot.

A small number of well-known multicast Service IDs are defined in Annex C.A. Others are available for vendor-specific algorithms.

Since data packets transmitted within this interval may collide, the CMTS MUST acknowledge any that are successfully received. The data packet MUST indicate in the MAC Header that a data acknowledgment is desired (see Table C.8-13).

C.9.1.2.3 The initial maintenance IE

The Initial Maintenance IE provides an interval in which new stations may join the network. A long interval, equivalent to the maximum round-trip propagation delay plus the transmission time of the Ranging Request (RNG-REQ) message (see C.9.3.3), MUST be provided to allow new stations to perform initial ranging. Packets transmitted in this interval MUST use the RNG-REQ MAC Management message format (refer to C.8.3.5).

C.9.1.2.4 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 CMTS MAY request that a particular CM perform some task related to network maintenance, such as periodic transmit power adjustment. In this case, the Station Maintenance IE is unicast to provide upstream bandwidth in which to perform this task. Packets transmitted in this interval MUST use the RNG-REQ MAC Management message format (see C.8.3.5).

C.9.1.2.5 Short and long data grant IEs

The Short and Long Data Grant IEs provide an opportunity for a CM 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 below). These IEs MAY also be used with an inferred length of zero mini slots (a zero length grant), to indicate that a request has been received and is pending (a Data Grant Pending).

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

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

C.9.1.2.6 Data acknowledge IE

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

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

C.9.1.2.7 Expansion IE

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

C.9.1.2.8 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.

C.9.1.3 Requests

Requests refer to the mechanism that CMs use to indicate to the CMTS that it needs upstream bandwidth allocation. A Request MAY come as a stand-alone Request Frame transmission (refer to C.8.2.5.3) or it MAY come as a piggyback request in the EHDR of another Frame transmission (refer to C.8.2.6).

The Request Frame MAY be transmitted during any of the following intervals:

- Request IE;
- Request/Data IE;

- Short Data Grant IE;
- Long Data Grant IE.

A piggyback request MAY be contained in the following Extended Headers:

- Request EH element;
- Upstream Privacy EH element;
- Upstream Privacy EH element with Fragmentation.

The request MUST include:

- The Service ID making the request;
- The number of mini-slots requested.

The number of mini-slots requested MUST be the total number that are desired by the CM at the time of the request (including any physical layer overhead), subject to UCD (see Note 1) and administrative limits (see Note 2). The CM MUST request a number of mini-slots corresponding to one complete frame (see Note 3), except in the case of fragmentation in Piggyback Mode (refer to C.10.3.2.2).

Physical layer overhead that MUST be accounted for in a request includes: guard band, preamble, and FEC which are dependent on the burst profile.

NOTE 1 – The CM is limited by the Maximum Burst size for the Long Data Grant IUC in the UCD.

NOTE 2 – The CM is limited by the Maximum Concatenated Burst for the Service Flow (refer to C.C.2.2.6.1).

NOTE 3 – A frame is a single MAC frame or a concatenated MAC frame.

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

In MAPs, the CMTS MUST NOT make a data grant greater than 255 mini-slots to any assigned Service ID. This puts an upper bound on the grant size the CM has to support.

C.9.1.4 Information element feature usage summary

Table C.9-1 summarizes what types of frames the CM can transmit using each of the MAP IE types that represent transmit opportunities. A "MUST" entry in the table means that, if appropriate, a compliant CM implementation has to be able to transmit that type of frame in that type of opportunity. A "MAY" entry means that compliant CM implementation does not have to be able to transmit that type of frame in that type of opportunity but that it is legal for it to do so, if appropriate. A "MUST NOT" entry means that a compliant CM will never transmit that type of frame in that type of opportunity.

Table C.9-1/J.112 – IE feature compatibility summary

Information element	Transmit request frame	Transmit concatenated MAC frame	Transmit fragmented MAC frame	Transmit RNG-REQ	Transmit any other MAC frame
Request IE	MUST	MUST NOT	MUST NOT	MUST NOT	MUST NOT
Request/Data IE	MUST	MAY	MUST NOT	MUST NOT	MAY
Initial Maintenance IE	MUST NOT	MUST NOT	MUST NOT	MUST	MUST NOT
Station Maintenance IE	MUST NOT	MUST NOT	MUST NOT	MUST	MUST NOT
Short Data Grant IE	MAY	MUST	MUST	MUST NOT	MUST
Long Data Grant IE	MAY	MUST	MUST	MUST NOT	MUST

C.9.1.5 Map transmission and timing

The allocation MAP MUST be transmitted in time to propagate across the physical cable and be received and handled by the receiving CMs. As such, it MAY be transmitted considerably earlier than its effective time. The components of the delay are:

- Worst-case round-trip propagation delay – may be network-specific, but on the order of hundreds of microseconds.
- Queuing delays within the CMTS – implementation-specific.
- Processing delays within the CMs – MUST allow a minimum processing time by each CM as specified in Annex C.B (CM MAP Processing Time).
- PMD-layer FEC interleaving.

Within these constraints, vendors may wish to minimize this delay so as to minimize latency of access to the upstream channel.

The number of mini-slots described MAY vary from MAP to MAP. At minimum, a MAP MAY describe a single mini-slot. This would be wasteful in both downstream bandwidth and in processing time within the CMs. At maximum, a MAP MAY stretch to tens of milliseconds. Such a MAP would provide poor upstream latency. Allocation algorithms MAY vary the size of the maps over time to provide a balance of network utilization and latency under varying traffic loads.

At minimum, a MAP MUST contain two Information Elements: one to describe an interval and a null IE to terminate the list. At a maximum, a MAP MUST be bounded by a limit of 240 information elements. Maps are also bounded in that they MUST NOT describe more than 4096 mini-slots into the future. The latter limit is intended to bound the number of future mini-slots that each CM is required to track. A CM MUST be able to support multiple outstanding MAPs. Even though multiple MAPs may be outstanding, the sum of the number of mini-slots they describe MUST NOT exceed 4096.

The set of all maps, taken together, MUST describe every mini-slot in the upstream channel. If a CM fails to receive a MAP describing a particular interval, it MUST NOT transmit during that interval.

C.9.1.6 Protocol example

This clause illustrates the interchange between the CM and the CMTS when the CM has data to transmit (Figure C.9-2). Suppose a given CM has a data PDU available for transmission.

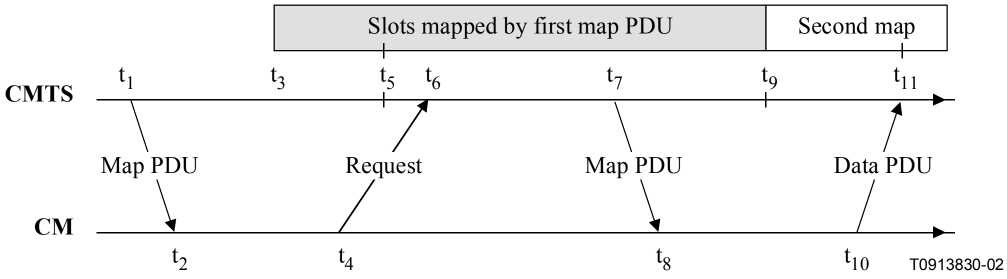


Figure C.9-2/J.112 – Protocol example

Description

1) At time t_1, the CMTS transmits a MAP whose effective starting time is t_3. Within this MAP is a Request IE which will start at t_5. The difference between t_1 and t_3 is needed to allow for:
   - Downstream propagation delay (including FEC interleaving) to allow all CMs to receive the Map.
   - Processing time at the CM (allows the CMs to parse the Map and translate it into transmission opportunities).
   - Upstream propagation delay (to allow the CM's transmission of the first upstream data to begin in time to arrive at the CMTS at time t_3).
2) At t_2, the CM receives this MAP and scans it for request opportunities. In order to minimize request collisions, it calculates t_6 as a random offset based on the Data Backoff Start value in the most recent Map (see C.9.4, also the multicast SID definitions in clause C.A.2).
3) At t_4, the CM transmits a request for as many mini-slots as needed to accommodate the PDU. Time t_4 is chosen based on the ranging offset (see C.9.3.3) so that the request will arrive at the CMTS at t_6.
4) At t_6, the CMTS receives the request and schedules it for service in the next MAP. (The choice of which requests to grant will vary with the class of service requested, any competing requests, and the algorithm used by the CMTS.)
5) At t_7, the CMTS transmits a MAP whose effective starting time is t_9. Within this MAP, a data grant for the CM will start at t_{11}.
6) At t_8, the CM receives the MAP and scans for its data grant.
7) At t_{10}, the CM transmits its data PDU so that it will arrive at the CMTS at t_{11}. Time t_{10} is calculated from the ranging offset as in step 3).

Steps 1) and 2) need not contribute to access latency if CMs routinely maintain a list of request opportunities.

At Step 3), the request may collide with requests from other CMs and be lost. The CMTS does not directly detect the collision. The CM determines that a collision (or other reception failure) occurred when the next MAP fails to include acknowledgment of the request. The CM MUST then perform a back-off algorithm and retry (refer to C.9.4.1).

At Step 4), the CMTS scheduler MAY fail to accommodate the request within the next MAP. If so, it MUST reply with a zero-length grant in that MAP or discard the request by giving no grant at all. It MUST continue to report this zero-length grant in all succeeding maps until the request can be granted or is discarded. This MUST signal to the CM that the request is still pending. So long as the CM is receiving a zero-length grant, it MUST NOT issue new requests for that service queue.

C.9.2 Support for multiple channels

Vendors may choose to offer various combinations of upstream and downstream channels within one MAC service access point. The upstream bandwidth allocation protocol allows for multiple upstream channels to be managed via one or many downstream channels.

If multiple upstream channels are associated with a single downstream channel, then the CMTS MUST send one allocation MAP per upstream channel. The MAP's channel identifier, taken with the Upstream Channel Descriptor Message (see C.8.3.3), MUST specify to which channel each MAP applies. There is no requirement that the maps be synchronized across channels.

If multiple downstream channels are associated with a single upstream channel, the CMTS MUST ensure that the allocation MAP reaches all CMs. That is, if some CMs are attached to a particular downstream channel, then the MAP MUST be transmitted on that channel. This may necessitate that multiple copies of the same MAP be transmitted. The Alloc Start Time in the MAP header MUST always relate to the SYNC reference on the downstream channel on which it is transmitted.

If multiple downstream channels are associated with multiple upstream channels, the CMTS may need to transmit multiple copies of multiple maps to ensure both that all upstream channels are mapped and that all CMs have received their needed maps.

C.9.3 Timing and synchronization

One of the major challenges in designing a MAC protocol for a cable network is compensating for the large delays involved. These delays are an order of magnitude larger than the transmission burst time in the upstream. To compensate for these delays, the cable modem MUST be able to time its transmissions precisely to arrive at the CMTS at the start of the assigned mini-slot.

To accomplish this, two pieces of information are needed by each cable modem:

- a global timing reference sent downstream from the CMTS to all cable modems;
- a timing offset, calculated during a ranging process, for each cable modem.

C.9.3.1 Global timing reference

The CMTS MUST create a global timing reference by transmitting the Time Synchronization (SYNC) MAC management message downstream at a nominal frequency. The message contains a timestamp that exactly identifies when the CMTS transmitted the message. Cable modems MUST then compare the actual time the message was received with the timestamp and adjust their local clock references accordingly.

The Transmission Convergence sublayer MUST operate closely with the MAC sublayer to provide an accurate timestamp for the SYNC message. As mentioned in the Ranging clause below (C.9.3.3), the model assumes that the timing delays through the remainder of the PHY layer MUST be relatively constant. Any variation in the PHY delays MUST be accounted for in the guard time of the PHY overhead.

It is intended that the nominal interval between SYNC messages be tens of milliseconds. This imposes very little downstream overhead while letting cable modems acquire their global timing synchronization quickly.

C.9.3.2 CM channel acquisition

Any cable modem MUST NOT use the upstream channel until it has successfully synchronized to the downstream.

First, the cable modem MUST establish PMD sublayer synchronization. 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 C.11.2.2). At this point, a valid bit stream is being sent to the transmission convergence sublayer. The transmission convergence sublayer performs its own synchronization (see clause C.7). On detecting the well-known Annex C/J.112 PID, along with a payload unit start indicator per [ITU-T H.222.0], it delivers the MAC frame to the MAC sublayer.

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

A cable modem remains in "SYNC" as long as it continues to successfully receive the SYNC messages. If the Lost SYNC Interval (refer to Annex C.B) has elapsed without a valid SYNC message, a cable modem MUST NOT use the upstream and MUST try to reestablish synchronization again.

C.9.3.3 Ranging

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

First, a cable modem MUST synchronize to the downstream and learn the upstream channel characteristics through the Upstream Channel Descriptor MAC management message. At this point, the cable modem MUST scan the Bandwidth Allocation MAP message to find an Initial Maintenance Region. Refer to C.9.1.2.4. The CMTS MUST make an Initial Maintenance region large enough to account for the variation in delays between any two CMs.

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

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

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

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

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

The CMTS MUST return another Ranging Response message to the cable modem with any additional fine tuning required. The ranging request/response steps MUST be repeated until the response contains a Ranging Successful notification or the CMTS aborts ranging. Once successfully ranged, the cable modem MUST join normal data traffic in the upstream. See clause C.9 for complete details on the entire initialization sequence. In particular, state machines and the applicability of retry counts and timer values for the ranging process are defined in C.11.2.4.

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

C.9.3.4 Timing units and relationships

The SYNC message conveys a time reference that is measured in 6.94 µs ticks. Additional resolution of 6.94/64 µs is also present in the SYNC message to allow the CM to track the CMTS clock with a small phase offset. These units were chosen as the greatest-common-divisor of the upstream mini-slot time across various modulations and symbol rates. As this is decoupled from particular upstream channel characteristics, a single SYNC time reference may be used for all upstream channels associated with the downstream channel.

The bandwidth allocation MAP uses time units of "mini-slots." A mini-slot represents the byte-time needed for transmission of a fixed number of bytes. The mini-slot is expected to represent 16 byte-times, although other values could be chosen. The size of the mini-slot, expressed as a multiple of the SYNC time reference, is carried in the Upstream Channel Descriptor. The example in Table C.9-2 relates mini-slots to the SYNC time ticks:

Table C.9-2/J.112 – Example relating mini-slots to time ticks

Parameter	Example Value
Time tick	6.94 µs
Bytes per mini-slot	16 (nominal, when using QPSK modulation)
Symbols/byte	4 (assuming QPSK)
Symbols/second	2 304 000
Mini-slots/second	36 000
Microseconds/mini-slot	$1/36\,000 \times 10^6$
Ticks/mini-slot	4

Note that the symbols/byte is a characteristic of an individual burst transmission, not of the channel. A mini-slot in this instance could represent either 16 or 32 bytes, depending on the modulation choice.

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

The MAP counts mini-slots in a 32 bit counter that normally counts to $(2^{32} – 1)$ and then wraps back to zero. The least-significant bits (i.e., bit 0 to bit 25 – M) of the mini-slot counter MUST match the most-significant bits (i.e., bit 6 + M to bit 31) of the SYNC timestamp counter. That is, mini-slot N begins at timestamp reference $(N \times T \times 64)$, where $T = 2^M$ is the UCD multiplier that defines the mini-slot (i.e., the number of timeticks per mini-slot).

The unused upper bits of the 32 bit mini-slot counter (i.e., bit 26 – M to bit 31) are not needed by the CM and MAY be ignored.

NOTE – The constraint that the UCD multiplier be a power of two has the consequence that the number of bytes per mini-slot must also be a power of two.

C.9.4 Upstream transmission and contention resolution

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

This clause provides an overview of upstream transmission and contention resolution. For simplicity, it refers to the decisions a CM makes, however, this is just a pedagogical tool. Since a CM can have multiple upstream Service Flows (each with its own SID) it makes these decisions on a per service queue or per SID basis. Refer to Annex C.K for a state transition diagram and more detail.

C.9.4.1 Contention resolution overview

The mandatory method of contention resolution which MUST be supported is based on a truncated binary exponential back-off, with the initial back-off window and the maximum back-off window controlled by the CMTS. The values are specified as part of the Bandwidth Allocation Map (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 CM 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 MAP currently in effect.

NOTE 1 – The MAP currently in effect is the MAP whose allocation start time has occurred but which includes IEs that have not occurred.

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

NOTE 2 – Each IE can represent multiple transmission opportunities.

As an example, consider a CM whose initial back-off window is 0 to 15 and it randomly selects the number 11. The CM must defer a total of 11 contention transmission opportunities. If the first available Request IE is for 6 requests, the CM does not use this and has 5 more opportunities to defer. If the next Request IE is for 2 requests, the CM has 3 more to defer. If the third Request IE is for 8 requests, the CM transmits on the fourth request, after deferring for 3 more opportunities.

After a contention transmission, the CM waits for a Data Grant (Data Grant Pending) or Data Acknowledge in a subsequent MAP. Once either is received, the contention resolution is complete. The CM determines that the contention transmission was lost when it finds a MAP without a Data Grant (Data Grant Pending) or Data Acknowledge for it and with an Ack time more recent than the time of transmission (see Note 3). The CM MUST now increase its back-off window by a factor of two, as long as it is less than the maximum back-off window. The CM MUST randomly select a number within its new back-off window and repeat the deferring process described above.

NOTE 3 – Data Acknowledge IEs are intended for collision detection only and is not designed for providing reliable transport (that is the responsibility of higher layers). If a MAP is lost or damaged, a CM waiting for a Data Acknowledge MUST assume that its contention data transmission was successful and MUST NOT retransmit the data packet. This prevents the CM from sending duplicate packets unnecessarily.

This retry process continues until the maximum number of retries (16) has been reached, at which time the PDU MUST be discarded.

NOTE 4 – The maximum number of retries is independent of the initial and maximum back-off windows that are defined by the CMTS.

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

The CMTS has much flexibility in controlling the contention resolution. At one extreme, the CMTS 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 MAP. At the other end, the CMTS may make the Data Backoff Start and End identical and frequently update these values in the MAP so all cable modems are using the same, and hopefully optimal, back-off window.

C.9.4.2 Transmit opportunities

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

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

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

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

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

In summary:

Table C.9-3/J.112 – Transmit opportunity

Interval	SID Type	Transmit opportunity
Request	Broadcast	No. of mini-slots required for a Request
Request	Multicast	No. of mini-slots required for a Request
Request/Data	Broadcast	Not allowed
Request/Data	Well-known Multicast	As defined by SID in Annex C.A
Request/Data	Multicast	Vendor specific algorithms
Initial Maintenance	Broadcast	Entire interval is a single TX OPP.

C.9.4.3 CM bandwidth utilization

The following rules govern the response a CM makes when processing maps.

NOTE – These standard behaviors can be overridden by the CM's Request/Transmission Policy (refer to C.C.2.2.6.3):

1) a CM MUST first use any Grants assigned to it. Next, the CM MUST use any unicast REQ for it. Finally, the CM MUST use the next available broadcast/multicast REQ or REQ/Data IEs for which it is eligible;

2) a CM MUST NOT have more than one Request outstanding at a time for a particular Service ID;

3) if a CM has a Request pending, it MUST NOT use intervening contention intervals for that Service ID.

C.9.5 Data link encryption support

The procedures to support data link encryption are defined in "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I05-000714". The interaction between the MAC layer and the security system is limited to the items defined below.

C.9.5.1 MAC messages

MAC Management Messages (C.8.3) MUST NOT be encrypted.

NOTE – Except for certain cases where such a frame is included in a fragmented concatenated burst on the upstream. (Refer to C.8.2.7.1.)

C.9.5.2 Framing

The following rules MUST be followed when encryption is applied to a data PDU:

- Privacy EH element MUST be in the extended header and MUST be the first EH element of the Extended Header field (EHDR).
- Encrypted data are carried as Data PDUs to the Cable MAC transparently.

C.10 Quality of Service & fragmentation

This annex introduces several new Quality of Service (QoS)-related concepts not present in Previous Annex C/J.112. These include:

- Packet Classification & Flow Identification;
- Service Flow QoS Scheduling;
- Dynamic Service Establishment;
- Fragmentation;
- Two-Phase Activation Model.

C.10.1 Theory of operation

The various Annex C/J.112 protocol mechanisms described in this annex can be used to support Quality of Service (QoS) for both upstream and downstream traffic through the CM and the CMTS. This clause 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 configuration and registration function for pre-configuring CM-based QoS Service Flows and traffic parameters;
- a Signalling function for dynamically establishing QoS-enabled Service Flows and traffic parameters;
- a traffic-shaping and traffic-policing function for Service Flow-based traffic management, performed on traffic arriving from the upper layer service interface and outbound to the RF;
- utilization of MAC scheduling and traffic parameters for upstream Service Flows;
- utilization of QoS traffic parameters for downstream Service Flows;
- classification of packets arriving from the upper layer service interface to a specific active Service Flow;
- grouping of Service Flow properties into named Service Classes, so upper layer entities and external applications (at both the CM and CMTS) can request Service Flows with desired QoS parameters in a globally consistent way.

The principal mechanism for providing enhanced QoS is to classify packets traversing the RF MAC interface into a Service Flow. A Service Flow is a unidirectional flow of packets that is provided a particular Quality of Service. The CM and CMTS provide this QoS by shaping, policing, and prioritizing traffic according to the QoS Parameter Set defined for the Service Flow.

The primary purpose of the Quality of Service features defined here is to define transmission ordering and scheduling on the Radio Frequency Interface. However, these features often need to work in conjunction with mechanisms beyond the RF interface in order to provide end-to-end QoS or to police the behavior of cable modems. For example, the following behaviors are permitted:

- Policies may be defined by CM MIBs which overwrite the TOS byte. Such policies are outside the scope of the RFI specification. In the upstream direction the CMTS polices the TOS byte setting regardless of how the TOS byte is derived or by whom it is written (originator or CM policy).
- The queuing of Service Flow packets at the CMTS in the downstream direction may be based on the TOS byte.
- Downstream Service Flows can be reclassified by the CM to provide enhanced service onto the subscriber-side network.

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 CMTS. All Service Flows have an SFID; active and admitted upstream Service Flows also have a 14 bit Service Identifier (SID).

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, including both MAC Management messages and Data PDUs. 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.

Conceptually, incoming packets are matched to a Classifier that determines to which QoS Service Flow the packet is forwarded. The Classifier can examine the LLC header of the packet, the IP/TCP/UDP header of the packet or some combination of the two. If the packet matches one of the Classifiers, it is forwarded to the Service Flow indicated by the SFID attribute of the Classifier. If the packet is not matched to a Classifier, it is forwarded on the Primary Service Flow.

C.10.1.1 Concepts

C.10.1.1.1 Service Flows

A Service Flow is a MAC-layer transport service that provides unidirectional transport of packets either to upstream packets transmitted by the CM or to downstream packets transmitted by the CMTS (see Note 1). A Service Flow is characterized by a set of QoS Parameters such as latency, jitter, and throughput assurances. In order to standardize operation between the CM and CMTS, these attributes include details of how the CM requests upstream mini-slots and the expected behavior of the CMTS upstream scheduler.

NOTE 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. However, the Classifiers for a Service Flow MAY be based on IEEE 802.1P/Q criteria, and so MAY NOT involve intserv flows at all.

A Service Flow is partially characterized by the following attributes (see Note 2):

- **ServiceFlowID**: exists for all service flows.
- **ServiceID**: only exists for admitted or active upstream service flows.
- **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 (see Note 3).

- **AdmittedQosParamSet**: defines a set of QoS parameters for which the CMTS (and possibly the CM) 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.
- **ActiveQosParamSet**: defines set of QoS parameters defining the service actually being provided to the Service Flow. Only an Active Service Flow may forward packets.

NOTE 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.

NOTE 3 – The ProvisionedQoSParamSet is null when a flow is created dynamically.

A Service Flow exists when the CMTS assigns a Service Flow ID (SFID) to it. The SFID serves as the principal identifier in the CM and CMTS for the Service Flow. A Service Flow which exists has at least an SFID, and an associated Direction.

The Authorization Module is a logical function within the CMTS 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 Figures C.10-1 and C.10-2. The ActiveQoSParameterSet is always a subset (see Note 4) of the AdmittedQoSParameterSet which is always a subset of the authorized "envelope." In the dynamic authorization model, this envelope is determined by the Authorization Module (labeled as the AuthorizedQoSParameterSet). In the provisioned authorization model, this envelope is determined by the ProvisionedQoSParameterSet. (Refer to C.10.1.4 for further information on the authorization models.)

NOTE 4 – To say that QoS Parameter Set A is a subset of QoS Parameter Set B the following MUST be true for all QoS Parameters in A and B:

- if (a smaller QoS parameter value indicates less resources, e.g. Maximum Traffic Rate), A is a subset of B if the parameter in A 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.

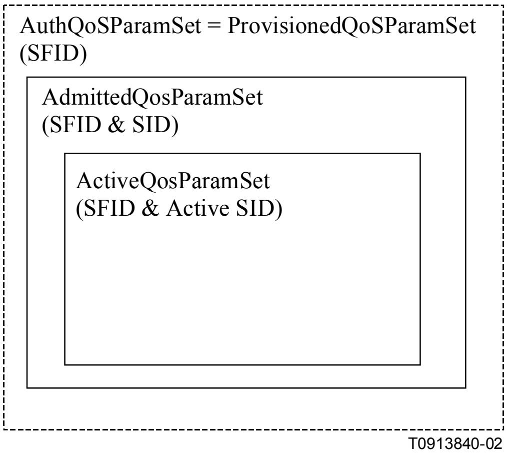


Figure C.10-1/J.112 – Provisioned authorization model "Envelopes"

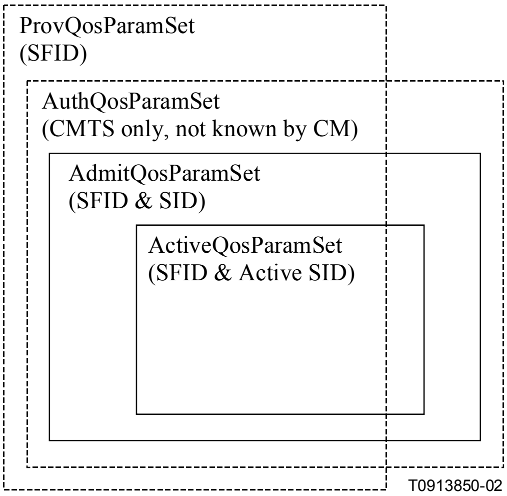


Figure C.10-2/J.112 – Dynamic authorization model "Envelopes"

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

- **Provisioned**: this type of Service Flow is known via provisioning through the configuration file, its AdmittedQoSParamSet and ActiveQoSParamSet are both null. A Provisioned Service Flow may or may not have associated Classifiers. If a Provisioned Service Flow has associated Classifiers, the Classifiers MUST NOT be used to classify packets onto the flow, regardless of the Classifier's Activation State.
- **Admitted**: this type of Service Flow has resources reserved by the CMTS 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. Generally, Admitted Service Flows have associated Classifiers, however, it is possible for Admitted Service Flows to use policy-based classification. If Admitted Service Flows have associated Classifiers, the classifiers MUST NOT be used to classify packets onto the flow, regardless of the classifier's activation state.
- **Active**: this type of Service Flow has resources committed by the CMTS 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. Generally, Active Service Flows have associated Classifiers, however, it is possible for Active Service Flows to use policy-based classification. Primary Service Flows may have associated Classifiers(s), but in

addition to any packets matching such Classifiers, all packets that fail to match any Classifier will be sent on the Primary Service Flow for that direction.

C.10.1.1.2 Classifiers

A Classifier is a set of matching criteria applied to each packet entering the cable network. It consists of some packet matching criteria (destination IP address, for example), a classifier priority, and a reference to a service flow. If a packet matches the specified packet matching criteria, it is then delivered on the referenced service flow.

Several Classifiers may all refer to the same Service Flow. The classifier priority is used for ordering the application of Classifiers to packets. Explicit ordering is necessary because the patterns used by Classifiers may overlap. The priority need not be unique, but care must be taken within a classifier priority to prevent ambiguity in classification. (Refer to C.10.1.6.1.) Downstream Classifiers are applied by the CMTS to packets it is transmitting, and Upstream Classifiers are applied at the CM and may be applied at the CMTS to police the classification of upstream packets. Figure C.10-3 illustrates the mappings discussed above.

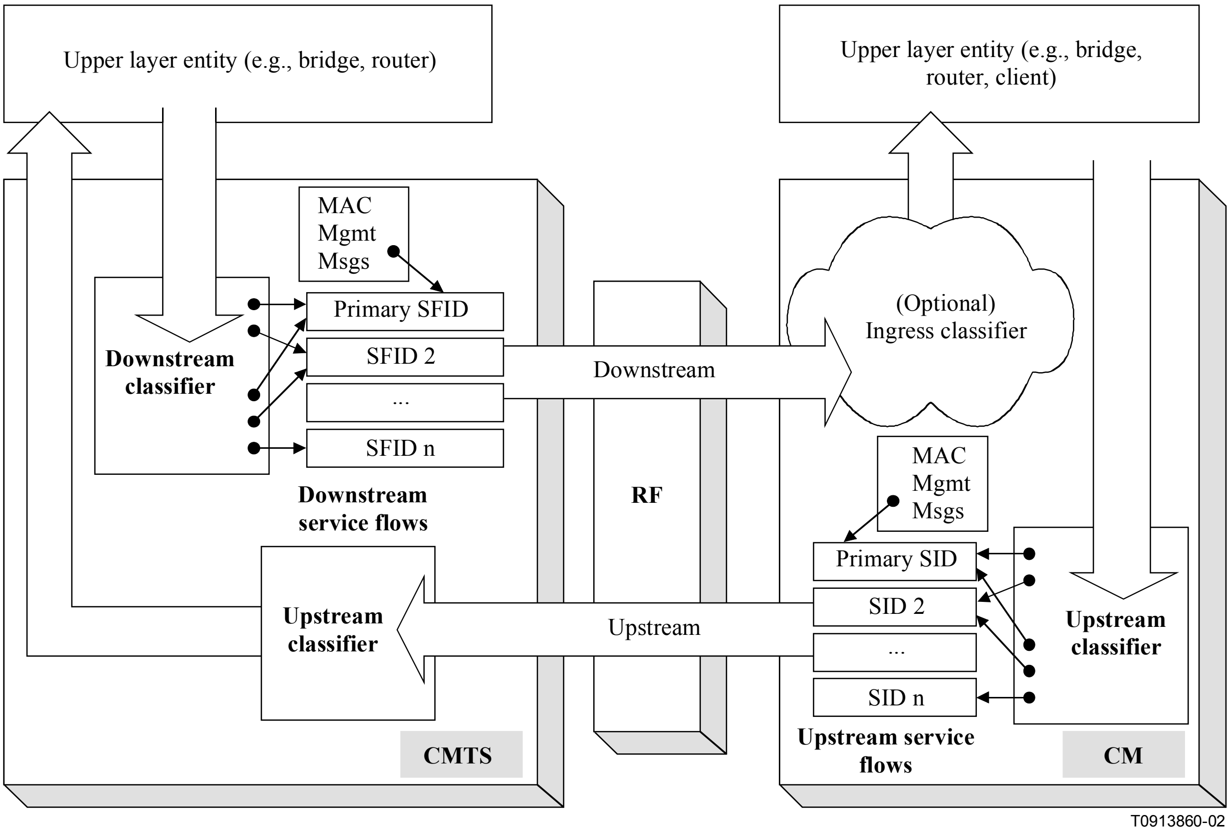


Figure C.10-3/J.112 – Classification within the MAC layer

CM and CMTS Packet Classification consists of multiple Classifiers. Each Classifier contains a priority field which determines the search order for the Classifier. The highest priority Classifier MUST be applied first. If a Classifier is found in which all parameters match the packet, the Classifier MUST forward the packet to the corresponding Service Flow. If no Classifier is found in which all parameters match the packet then the packet is classified to the Primary Service Flow.

The packet classification table contains the following fields:

- Priority – determines the search order for the table. Higher priority Classifiers are searched before lower priority Classifiers.

- IP Classification Parameters – zero or more of the IP classification parameters (IP TOS Range/Mask, IP Protocol, IP Source Address/Mask, IP Destination Address/Mask, TCP/UDP Source Port Start, TCP/UDP Source Port End, TCP/UDP Destination Port Start, TCP/UCP Destination Port End).
- LLC Classification Parameters – zero or more of the LLC classification parameters (Destination MAC Address, Source MAC Address, Ethertype/SAP).
- IEEE 802.1P/Q Parameters – zero or more of the IEEE classification parameters (IEEE 802.1P Priority Range, IEEE 802.1Q VLAN ID).
- Service Flow Identifier – identifier of a specific flow to which this packet is to be directed.

Classifiers can be added to the table either via management operations (configuration file, registration) or via dynamic operations (dynamic Signalling, Annex C/J.112 MAC sublayer service interface). SNMP-based operations can view Classifiers that are added via dynamic operations, but can not modify or delete Classifiers that are created by dynamic operations. The format for classification table parameters defined in the configuration file, registration message, or dynamic Signalling message is contained in Annex C.C.

Classifier attributes include an activation state (see C.C.2.1.3.6). The "inactive" setting may be used to reserve resources for a classifier which is to be activated later. The actual activation of the classifier depends both on this attribute and on the state of its service flow. If the service flow is not active then the classifier is not used, regardless of the setting of this attribute.

C.10.1.2 Object model

The major objects of the architecture are represented by named rectangles in Figure C.10-4. Each object has a number of attributes; the attribute names which uniquely identify the object are underlined. Optional attributes are denoted with brackets. The relationship between the number of objects is marked at each end of the association line between the objects. For example, a Service Flow may be associated with from 0 to 65 535 Classifiers, but a Classifier is associated with exactly one Service flow.

The Service Flow is the central concept of the MAC protocol. It is uniquely identified by a 32 bit Service Flow ID (SFID) assigned by the CMTS. Service Flows may be in either the upstream or downstream direction. A unicast Service Identifier (SID) is a 14 bit index, assigned by the CMTS, which is associated with one and only one Admitted Upstream Service Flow.

Typically, an outgoing user data Packet is submitted by an upper layer protocol (such as the forwarding bridge of a CM) for transmission on the Cable MAC interface. The packet is compared against a set of Classifiers. The matching Classifier for the Packet identifies the corresponding Service Flow via the Service Flow ID (SFID). In the case where more than one Classifier matches the packet, the highest Priority Classifier is chosen.

The Classifier matching a packet may be associated with a Payload Header Suppression Rule. A PHS Rule provides details on how header bytes of a Packet PDU can be omitted, replaced with a Payload Header Suppression Index for transmission and subsequently regenerated at the receiving end. PHS Rules are indexed by the combination of (SFID, PHSI) (refer to C.10.4). When a Service Flow is deleted, all Classifiers and any associated PHS Rules referencing it MUST also be deleted.

The Service Class is an optional object that MAY be implemented at the CMTS. It is referenced by an ASCII name which is intended for provisioning purposes. A Service Class is defined in the CMTS 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 CMTS. (Refer to C.C.2.2.5.)

If a Packet has already been determined by upper layer policy mechanisms to be associated with a particular Service Class Name/Priority combination, that combination associates the packet with a particular Service Flow directly (refer to C.10.1.6.1). The upper layer may also be aware of the particular Service Flows in the MAC Sublayer, and may have assigned the Packet directly to a Service Flow. In these cases, a user data Packet is considered to be directly associated with a Service Flow as selected by the upper layer. This is depicted with the dashed arrow in Figure C.10-4.

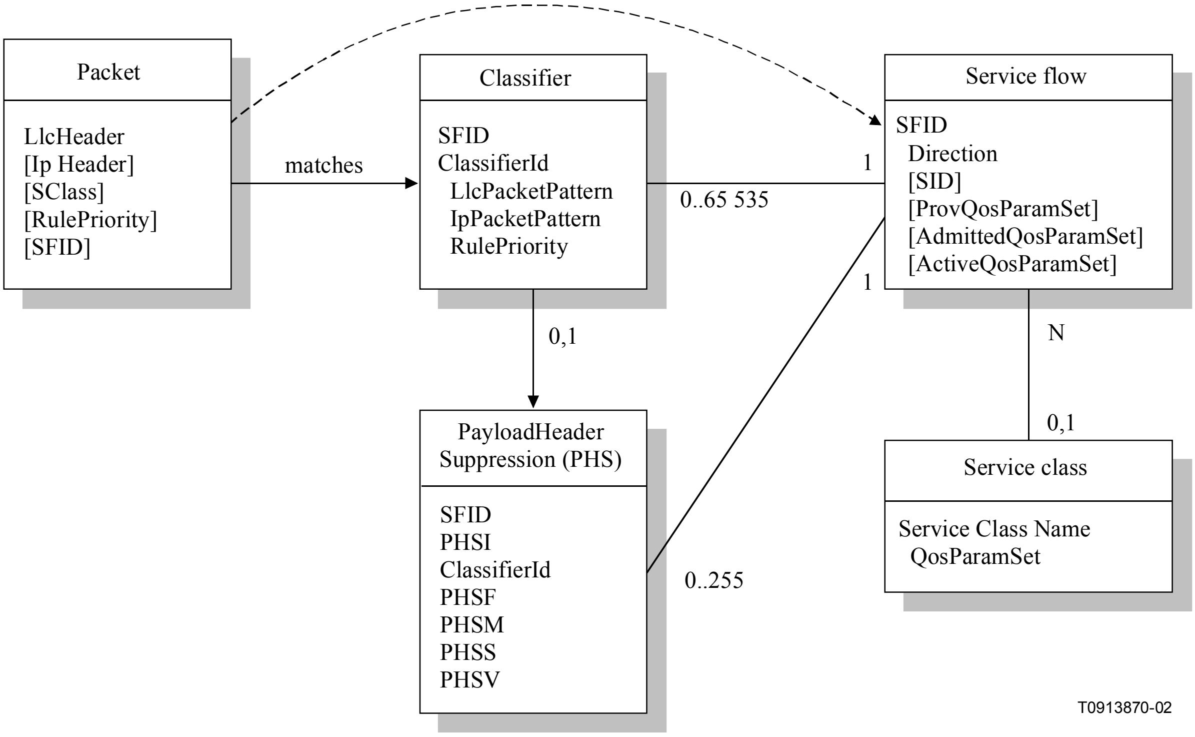


Figure C.10-4/J.112 – Theory of operation object model

C.10.1.3 Service classes

The QoS attributes of a Service Flow may be specified in two ways: either by explicitly defining all attributes, or implicitly by specifying a Service Class Name. A Service Class Name is a string which the CMTS associates with a QoS Parameter Set. It is described further below.

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 CMTS. Operators provision the modems with the Service Class Name; the implementation of the name is configured at the CMTS. 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 CMTSs to provide the same service. As another example, service profiles could be changed by time of day.

2) It allows CMTS 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 Signalling may direct the CM to instantiate any available Provisioned Service Flow of class "G711".

4) It allows packet classification policies to be defined which refer to a desired service class, without having to refer to a particular service flow instance of that class.

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. CMTS 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:

- by explicitly including all traffic parameters;
- by indirectly referring to a set of traffic parameters by specifying a Service Class Name;
- 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 CMTS successfully admits the Service Flow. The Service Class expansion can be contained in the following CMTS-originated messages: Registration Response, DSA-REQ, DSC-REQ, DSA-RSP and DSC-RSP. In all of these cases, the CMTS MUST include a Service Flow Encoding that includes the Service Class Name and the QoS Parameter Set of the Service Class. If a CM-initiated request contained any supplemental or overriding Service Flow parameters, a successful response MUST also include these parameters.

When a Service Class name is given in an admission or activation request, 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 CMTS. If the definition of a Service Class Name is changed at the CMTS (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 CMTS MAY initiate DSC transactions to existing Service Flows which reference the Service Class Name to affect the changed Service Class definition.

When a CM 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 CM 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 CM SHOULD explicitly request the expanded set of TLVs from the response message in its later activation request.

C.10.1.4 Authorization

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

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

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 CM 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 CM that are signalled in advance by the external policy server are permitted. Admission and activation requests from a CM 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 CM MUST send to the CMTS the authenticated set of TLVs derived from its configuration file which defines the Provisioned QoS Parameter Set. Upon receipt and verification at the CMTS, these are handed to the Authorization Module within the CMTS. The CMTS MUST be capable of caching the Provisioned QoS Parameter Set, and MUST be able to use this information to authorize dynamic flows which are a subset of the Provisioned QoS Parameter Set. The CMTS SHOULD implement mechanisms for overriding this automated approval process (such as described in the dynamic authorization model). For example:

- deny all requests whether or not they have been preprovisioned;
- define an internal table with a richer policy mechanism but seeded by the configuration file information;
- refer all requests to an external policy server.

C.10.1.5 Types of Service Flows

It is useful to think about three basic types of Service Flows. This clause 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 C.C.2.2.5.1.)

C.10.1.5.1 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 C.C.2.2.5.1). During Registration, the CMTS assigns a Service Flow ID for such a service flow but does not reserve resources. The CMTS MAY also require an exchange with a policy module prior to admission.

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

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

C.10.1.5.2 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 following 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 CM 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 AdmittedQoS-ParamSet and no new classifiers are being added MUST be allowed (except in the case of catastrophic failure). An admission request where the AdmittedQoSParamSet is a subset of the previous AdmittedQoSParamSet, so long as the ActiveQoSParamSet remains a subset of the AdmittedQoSParameterSet, MUST succeed.

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

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 allows 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 CMTS; this state must be refreshed periodically for it to be maintained without the above timeout releasing the non-activated resources. This refresh MAY be signalled with a periodic DSC-REQ message with identical QoS Parameter Sets, or MAY be signalled by some internal mechanism within the CMTS outside of the scope of this annex (e.g. by the CMTS monitoring RSVP refresh messages). Every time a refresh is signalled to the CMTS, the CMTS MUST refresh the "soft state".

C.10.1.5.3 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 (see Note) and being granted bandwidth for transport of data packets. An admitted Service Flow may be made active by providing an ActiveQoSParameterSet, Signalling the resources actually desired at the current time. This completes the second stage of the two-phase activation model (refer to C.10.1.5.2).

NOTE – According to its Request/Transmission Policy (refer to C.C.2.2.6.3).

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

C.10.1.6 Service flows and classifiers

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

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

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

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

MAC Management messages may only be matched by a classifier that contains a C.C.2.1.6.3 "Ethertype/DSAP/MacType" parameter encoding and when the "type" field of the MAC Management Message Header (C.8.3.1) matches that parameter. One exception is that the Primary SID MUST be used for station maintenance, as specified in C.8.1.2.3, even if a classifier matches the upstream RNG-REQ message of station maintenance. In the absence of any classifier matching a MAC Management message, it SHOULD be transmitted on the Primary Service Flow. Other than those MAC message types precluded from classification in C.C.2.1.6.3, a CM or CMTS MAY forward an otherwise unclassified MAC message on any Service Flow in an implementation-specific manner.

Although MAC Management messages are subject to classification, they are not considered part of any service flow. Transmission of MAC Management messages MUST NOT influence any QoS calculations of the Service Flow to which they are classified. Delivery of MAC Management messages is implicitly influenced by the attributes of the associated service flow.

C.10.1.6.1 Policy-based classification and service classes

There are a variety of ways in which packets may be enqueued for transmission at the MAC Service Interface. At one extreme are embedded applications that are tightly bound to a particular Payload Header Suppression Rule (refer to C.10.4) and which forego more general classification by the MAC. At the other extreme are general transit packets of which nothing is known until they are parsed by the MAC Classification rules. Another useful category is traffic to which policies are applied by a higher-layer entity and then passed to the MAC for further classification to a particular service flow.

Policy-based classification is, in general, beyond the scope of this annex. One example might be the docsDevFilterIpPolicyTable defined in the Cable Device MIB, [RFC 2669]. Such policies may tend to be longer-lived than individual service flows and MAC classifiers and so it is appropriate to layer the two mechanisms, with a well-defined interface between policies and MAC Service Flow Classification.

The interface between the two layers is the addition of two parameters at the MAC transmission request interface. The two parameters are a Service Class Name and a Rule Priority that is applied to matching the service class name. The Policy Priority is from the same number space as the

Packet Classifier Priority of the packet-matching rules used by MAC classifiers. The MAC Classification algorithm is now:

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

While Policy Priority competes with Packet Classifier Priority and its choice might in theory be problematic, it is anticipated that well-known ranges of priorities will be chosen to avoid ambiguity. In particular, dynamically-added classifiers MUST use the priority range 64-191. Classifiers created as part of registration, as well as policy-based classifiers, may use zero through 255, but SHOULD avoid the dynamic range.

Classification within the MAC sublayer is intended to simply associate a packet with a service flow. If a packet is intended to be dropped it MUST be dropped by the higher-layer entity and not delivered to the MAC sublayer.

C.10.1.7 General operation

C.10.1.7.1 Static operation

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

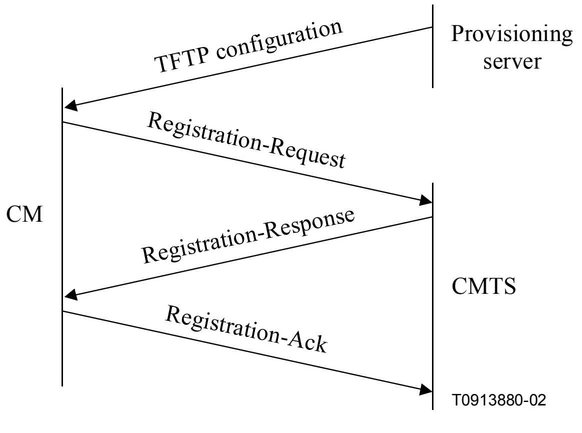


Figure C.10-5/J.112 – Registration message flow

A TFTP configuration file consists of one or more instances of Classifiers and Service Flow Encodings. Classifiers are loosely ordered by "priority". Each Classifier refers to a Service Flow via a "service flow reference". Several Classifiers may refer to the same Service Flow. Additionally, more than one Classifier may have the same priority, and in this case, the particular classifier used is not defined.

Table C.10-1/J.112 – TFTP file contents

Items	Point to service flow reference	Service flow reference	Service flow ID
Upstream Classifiers Each containing a Service Flow Reference (pointer)	1..n		
Downstream Classifiers Each containing a Service Flow Reference (pointer)	(n+1)..q		
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 CMTS and which indirectly specifies a set of QoS Parameters (refer to C.10.1.3 and C.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 CMTS 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 C.10-2/J.112 – Registration request contents

Items	Point to service flow reference	Service flow reference	Service flow ID
Upstream Classifiers Each containing a Service Flow Reference (pointer)	1..n		
Downstream Classifiers Each containing a Service Flow Reference (pointer)	(n+1)..p		
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 C.10-3/J.112 – 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	None 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 CMTS to identify a downstream or upstream service Flow that has been authorized but not activated. A DSC-Request from a modem to admit or activate a Provisioned Service Flow contains its SFID. If it is a downstream Flow then the Downstream Classifier is also included.

C.10.1.7.2 Dynamic service flow creation – CM 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 CM or the CMTS, and may create one upstream and/or one downstream dynamic Service Flow(s). A three-way handshake is used to create Service Flows. The CM-initiated protocol is illustrated in Figure C.10-6 and described in detail in C.11.4.2.1.

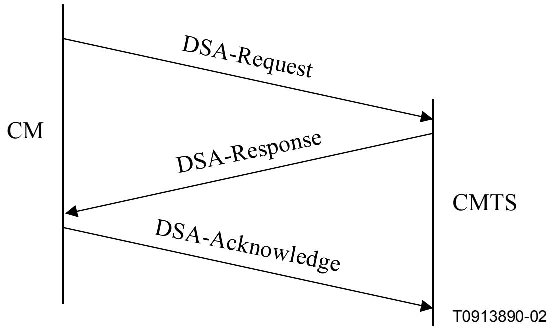


Figure C.10-6/J.112 – Dynamic service addition message flow – CM initiated

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

C.10.1.7.3 Dynamic service flow creation – CMTS initiated

A DSA-Request from a CMTS contains Service Flow Identifier(s) for one upstream and/or one downstream Service Flow, possibly a SID, set(s) of active or admitted QoS Parameters, and any required Classifier(s). The protocol is as illustrated in Figure C.10-7 and is described in detail in C.11.4.2.2.

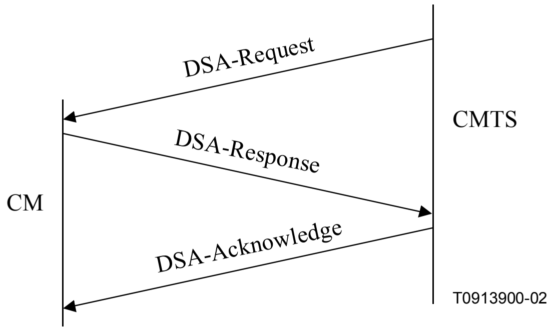


Figure C.10-7/J.112 – Dynamic service addition message flow – CMTS initiated

C.10.1.7.4 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 C.11.4.4 and C.11.4.3.

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. The DSC can also add, replace, or delete classifiers, and add, add parameters to, or delete PHS rules.

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 C.C.2.2.5.1) 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 subset (see C.10.1.1.1). 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.

C.10.2 Upstream service flow scheduling services

The following clauses 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 Annex C.C. The clause also discusses how these basic services and QoS parameters can be combined to form new services, such as, Committed Information Rate (CIR) service.

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

Each service is tailored to a specific type of data flow as described below. The basic services comprise: Unsolicited Grant Service (UGS), Real-Time Polling Service (rtPS), Unsolicited Grant Service with Activity Detection (UGS-AD), Non-Real-Time Polling Service (nrtPS) and Best Effort (BE) service. Table C.10.4 shows the relationship between the scheduling services and the related QoS parameters.

C.10.2.1 Unsolicited Grant Service

The Unsolicited Grant Service (UGS) is designed to support real-time service flows that generate fixed size data packets on a periodic basis, such as Voice over IP. The service offers fixed size grants on a real-time periodic basis, which eliminate the overhead and latency of CM requests and assure that grants will be available to meet the flow's real-time needs. The CMTS MUST provide fixed size data grants at periodic intervals to the Service Flow. In order for this service to work correctly, the Request/Transmission Policy (refer to C.C.2.2.6.3) setting MUST be such that the CM is prohibited from using any contention request or request/data opportunities and the CMTS SHOULD NOT provide any unicast request opportunities. The Request/Transmission Policy MUST also prohibit piggyback requests. This will result in the CM only using unsolicited data grants for upstream transmission. All other bits of the Request/Transmission Policy are not relevant to the fundamental operation of this scheduling service and should be set according to network policy. The key service parameters are the Unsolicited Grant Size, the Nominal Grant interval, the Tolerated Grant Jitter and the Request/Transmission Policy (refer to Annex C.M).

The Unsolicited Grant Synchronization Header (UGSH) in the Service Flow EH Element (refer to C.8.2.6.3.2) is used to pass status information from the CM to the CMTS regarding the state of the UGS Service Flow. The most significant bit of the UGSH is the Queue Indicator (QI) bit. The CM MUST set this flag once it detects that this Service Flow has exceeded its transmit queue depth. Once the CM detects that the Service Flow's transmit queue is back within limits, it MUST clear the QI flag. The flag allows the CMTS to provide for long term compensation for conditions such as lost maps or clock rate mismatch's by issuing additional grants.

The CMTS MUST NOT allocate more grants per Nominal Grant Interval than the Grants Per Interval parameter of the Active QoS Parameter Set, excluding the case when the QI bit of the UGSH is set. In this case, the CMTS SHOULD grant up to 1% additional bandwidth for clock rate mismatch compensation. If the CMTS grants additional bandwidth, it MUST limit the total number of bytes forwarded on the flow during any time interval to Max(T), as described in the expression:

$$Max(T) = T \times (R \times 1.01) + 3B$$

where:

Max(T) is the maximum number of bytes transmitted on the flow over a time *T* (in units of seconds),

R = (grant_size × grants_per_interval)/nominal_grant_interval, and

B = grant_size × grants_per_interval.

The active grants field of the UGSH is ignored with UGS service. The CMTS policing of the Service Flow remains unchanged.

C.10.2.2 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 CM 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 CMTS MUST provide periodic unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (refer to C.C.2.2.6.3) SHOULD be such that the CM is prohibited from using any contention request or request/data opportunities. The Request/Transmission Policy SHOULD also prohibit piggyback requests. The CMTS MAY issue unicast request opportunities as prescribed by this service even if a grant is pending. This will result in the CM using only unicast request opportunities in order to obtain upstream transmission opportunites (the CM 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 parameters are the Nominal Polling Interval, the Tolerated Poll Jitter and the Request/Transmission Policy.

C.10.2.3 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 CMTS MUST provide periodic unicast grants, when the flow is active, but MUST revert to providing periodic unicast request opportunities when the flow is inactive. The CMTS 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 CMTS implementation. In order for this service to work correctly, the Request/Transmission Policy setting (refer to C.C.2.2.6.3) MUST be such that the CM is prohibited from using any contention request or request/data opportunities. The Request/Transmission Policy MUST also prohibit piggyback requests. This results in the CM using only unicast request opportunities in order to obtain upstream transmission opportunities. However, the CM 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 CMTS SHOULD provide additional grants in the first (and/or second) grant interval such that the CM receives a total of one grant for each grant interval from the time the CM requested restart of UGS, plus one additional grant. (Refer to Annex C.M.) Because the Service Flow is provisioned as a UGS flow with a specific grant interval and grant size, when restarting UGS, the CM MUST NOT request a different sized grant than the already provisioned UGS flow. As with any Service Flow, changes can only be requested with a DSC command. If the restarted activity requires more than one grant per interval, the CM MUST indicate this in the Active Grants field of the UGSH beginning with the first packet sent.

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

If the CMTS allocates additional bandwidth in response to the QI bit, it MUST use the same rate limiting formula as UGS, but the formula only applies to steady state periods where the CMTS has adjusted the grants_per_interval to match the active_grants requested by the CM.

When the CM is receiving unsolicited grants and it detects no activity on the Service Flow, it MAY send one packet with the Active Grants field set to zero grants and then cease transmission. Because this packet may not be received by the CMTS, when the Service Flow goes from inactive to active the CM MUST be able to restart transmission with either polled requests or unsolicited grants.

C.10.2.4 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 CMTS typically polls nrtPS SIDs on an (periodic or non-periodic) interval on the order of one second or less.

The CMTS MUST provide timely unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (refer to C.C.2.2.6.2) SHOULD be such that the CM is allowed to use contention request opportunities. This will result in the CM 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 network policy. The key service parameters are Nominal Polling Interval, Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Request/Transmission Policy and Traffic Priority.

C.10.2.5 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 CM is allowed to use contention request opportunities. This will result in the CM 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 parameters are the Minimum Reserved Traffic Rate, the Maximum Sustained Traffic Rate, and the Traffic Priority.

C.10.2.6 Other services

C.10.2.6.1 Committed Information Rate (CIR)

A Committed Information Rate (CIR) service can be defined a number of different ways. For example, it could be configured by using a Best Effort service with a Minimum Reserved Traffic Rate or a nrtPS with a Minimum Reserved Traffic Rate.

C.10.2.7 Parameter applicability for upstream service sheduling

Table C.10-4 summarizes the relationship between the scheduling services and key QoS parameters. A detailed description of each QoS parameter is provided in Annex C.C.

Table C.10-4/J.112 – Parameter applicability for upstream service scheduling

Service flow parameter	Best effort	Non-real time polling	Real-time polling	Unsolicited grant	Unsolicited grant with activity det.
Miscellaneous					
• Traffic Priority	Optional Default = 0	Optional Default = 0	N/A (Note 1)	N/A	N/A
• Max Concatenated Burst	Optional	Optional	Optional	N/A	N/A
• Upstream Scheduling Service Type	Optional Default = 2	Mandatory	Mandatory	Mandatory	Mandatory
• Request/Transmission Policy	Optional Default = 0	Mandatory	Mandatory	Mandatory	Mandatory
Maximum Rate					
• Max Sustained Traffic Rate	Optional Default = 0	Optional Default = 0	Optional Default = 0	N/A	N/A
• Max Traffic Burst	Optional Dflt = 1522	Optional Dflt = 1522	Optional Dflt = 1522	N/A	N/A
Minimum Rate					
• Min Reserved Traffic Rate	Optional Default = 0	Optional Default = 0	Optional Default = 0	N/A	N/A
• Assumed Minimum... Packet Size	Optional (Note 3)	Optional (Note 3)	Optional (Note 3)	Optional (Note 3)	Optional (Note 3)
Grants					
• Unsolicited Grant Size	N/A	N/A	N/A	Mandatory	Mandatory
• Grants per interval	N/A	N/A	N/A	Mandatory	Mandatory
• Nominal Grant Interval	N/A	N/A	N/A	Mandatory	Mandatory
• Tolerated Grant Jitter	N/A	N/A	N/A	Mandatory	Mandatory

Polls					
• Nominal Polling Interval	N/A	Optional (Note 3)	Mandatory	N/A	Optional (Note 2)
• Tolerated Poll Jitter	N/A	N/A	Optional (Note 3)	N/A	Optional (Note 3)
NOTE 1 – N/A means not applicable to this service flow scheduling type. If included in a request for a service flow of this service flow scheduling type, this request MUST be denied. NOTE 2 – Default is same as Nominal Grant Interval. NOTE 3 – Default is CMTS specific.					

C.10.2.8 CM transmit behavior

In order for these services to function correctly, all that is required of the CM with regard to its transmit behavior for a service flow, is for it to follow the rules specified in C.9.4.3 and the Request/Transmission Policy specified for the service flow.

C.10.3 Fragmentation

Fragmentation is an upstream CM "modem capability". The CMTS MUST enable or disable this capability on a per-modem basis with a TLV in the Registration Response. The per-modem basis provides compatibility with Previous Annex C/J.112 CMs. Once fragmentation is enabled for a Revised Annex C/J.112 modem, fragmentation is enabled on a per-Service Flow basis via the Request/Transmission Policy Configuration Settings. When enabled for a Service Flow, fragmentation is initiated by the CMTS when it grants bandwidth to a particular CM with a grant size that is smaller than the corresponding bandwidth request from the CM. This is known as a Partial Grant.

C.10.3.1 CM fragmentation support

Fragmentation is essentially encapsulation of a portion of a MAC Frame within a fixed size fragmentation header and a fragment CRC. Concatenated PDUs, as well as single PDUs, are encapsulated in the same manner. Baseline Privacy, if enabled, is performed on each fragment as opposed to the complete original MAC frame.

The CM MUST perform fragmentation according to the flow diagram in Figure C.10-8. The phrase "untransmitted portion of packet" in the flow diagram refers to the entire MAC frame when fragmentation has not been initiated and to the remaining untransmitted portion of the original MAC frame when fragmentation has been initiated.

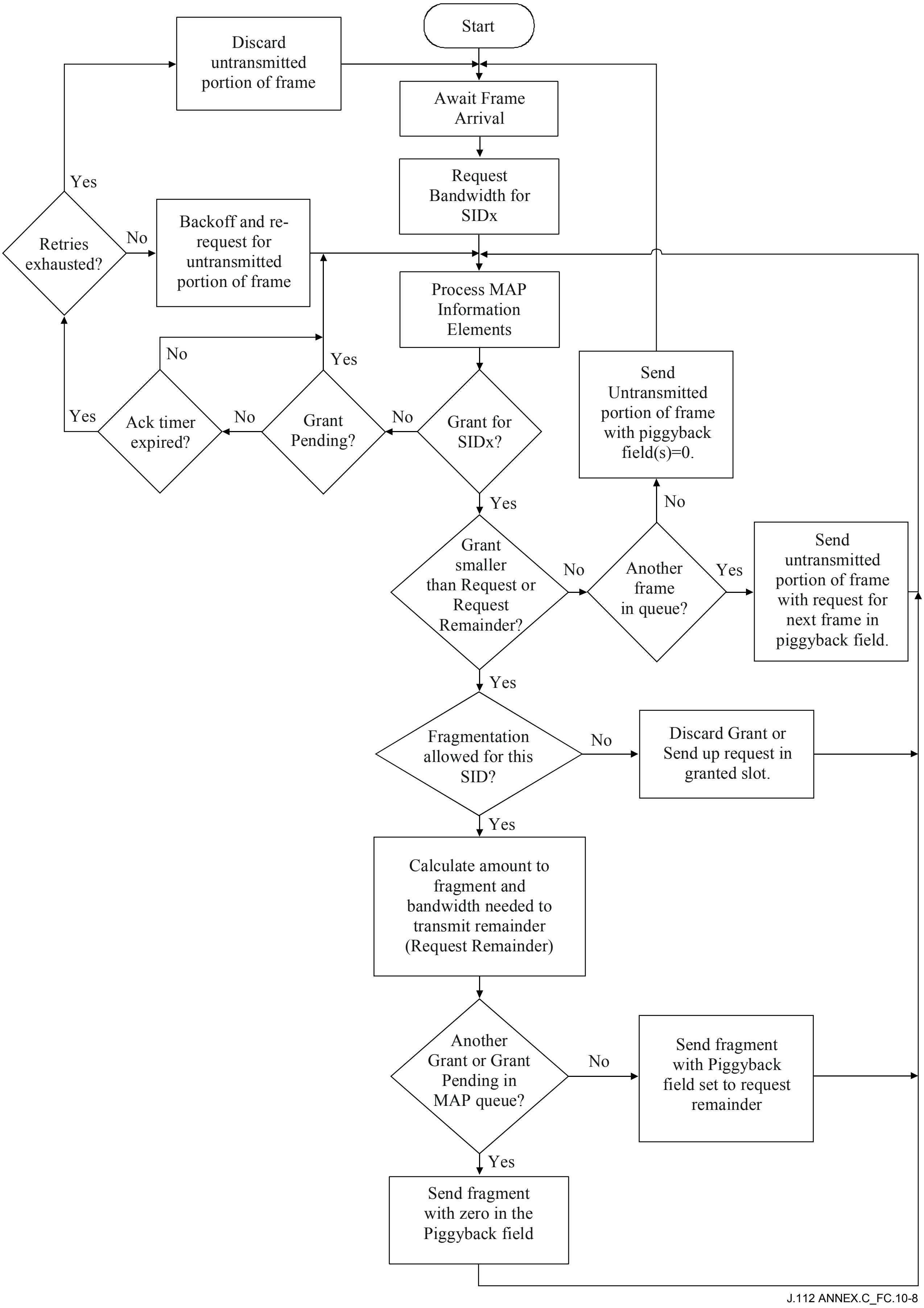

Start
Discard untransmitted portion of frame
Await Frame Arrival
Request Bandwidth for SIDx
Yes
Retries exhausted?
No
Backoff and re-request for untransmitted portion of frame
Process MAP Information Elements
No
Yes
Send Untransmitted portion of frame with piggyback field(s)=0.
Yes
Ack timer expired?
No
Grant Pending?
No
Grant for SIDx?
Yes
No
Grant smaller than Request or Request Remainder?
No
Another frame in queue?
Yes
Send untransmitted portion of frame with request for next frame in piggyback field.
Yes
Fragmentation allowed for this SID?
No
Discard Grant or Send up request in granted slot.
Yes
Calculate amount to fragment and bandwidth needed to transmit remainder (Request Remainder)
Another Grant or Grant Pending in MAP queue?
No
Send fragment with Piggyback field set to request remainder
Yes
Send fragment with zero in the Piggyback field
J.112 ANNEX.C_FC.10-8

Figure C.10-8/J.112 – CM Fragmentation flowchart

C.10.3.1.1 Fragmentation rules

1) Any time fragmentation is enabled and the grant size is smaller than the request, the CM MUST fill the partial grant it receives with the maximum amount of data (fragment payload) possible accounting for fragmentation overhead and physical layer overhead.

2) The CM MUST send up a piggyback request any time there is no later grant or grant pending for that SID in MAPs that have been received at the CM.

3) If the CM is fragmenting a frame, any piggyback request MUST be made in the BPI EHDR portion of the fragment header.

4) In calculating bandwidth requests for the remainder of the frame (concatenated frame, if concatenated) that has been fragmented, the CM MUST request enough bandwidth to transmit the entire remainder of the frame plus the 16-byte fragment overhead and all associated physical layer overhead.

5) If the CM does not receive a grant or grant pending within the ACK time of sending a request, the CM MUST backoff and re-request for the untransmitted portion of the frame until the bandwidth is granted or the CM exceeds its retry threshold.

6) If the CM exceeds its retry threshold while requesting bandwidth, the CM discards whatever portion of the frame was not previously transmitted.

7) The CM MUST set the F bit and clear the L bit in the first fragment of a frame.

8) The CM MUST clear the F and L bits in the fragment header for any fragments that occur between the first and last fragments of a frame.

9) The CM MUST set the L bit and clear the F bit in the last fragment of a frame.

10) The CM MUST increment the fragment sequence number sequentially for each fragment of a frame transmitted.

11) If a frame is to be encrypted and the frame is fragmented, the frame is encrypted only at the fragment layer with encryption beginning immediately after the fragment header HCS and continuing through the fragment CRC.

12) Frames sent in immediate data (request/data) regions MUST NOT be fragmented.

NOTE – "Frame" always refers to either frames with a single Packet PDU or concatenated frames.

C.10.3.2 CMTS fragmentation support

At the CMTS, the fragment is processed similarly to an ordinary packet with the exception that the baseline privacy encryption starts just after the fragmentation header as opposed to being offset by 12 bytes.

The CMTS has two modes it can use to perform fragmentation. The Multiple Grant Mode assumes that the CMTS retains the state of the fragmentation. This mode allows the CMTS to have multiple partial grants outstanding for any given SID. The Piggybacking Mode assumes the CMTS does NOT retain any fragmentation state. Only one partial grant is outstanding, so that the CM inserts the remaining amount into the Piggyback field of the fragment header. The type of mode being used is determined by the CMTS. In all cases, the CM operates with a consistent set of rules.

C.10.3.2.1 Multiple grant mode

A CMTS MAY support Multiple Grant Mode for performing fragmentation.

Multiple Grant Mode allows the CMTS to break a request up into two or more grants in a single or over successive maps and it calculates the additional overhead required in the remaining partial grants to satisfy the request. In Multiple Grant Mode, if the CMTS cannot grant the remainder in the current MAP, it MUST send a grant pending (zero length grant) in the current MAP and all subsequent MAPs to the CM until it can grant additional bandwidth. If there is no grant or grant pending in subsequent maps, the CM MUST re-request for the remainder. This re-request mechanism is the same as that used when a normal REQ does not receive a grant or grant pending within the ACK time.

If a CM receives a grant pending IE along with a fragment grant, it MUST NOT piggyback a request in the extended header of the fragment transmitted in that grant.

In the case where the CM misses a grant and re-requests the remaining bandwidth, the CMTS MUST recover without dropping the frame.

Due to the imprecision of the mini-slot to byte conversion process, the CMTS may not be able to calculate exactly the number of extra mini-slots needed to allow for fragmentation overhead. Also, because it is possible for a CM to have missed a map with a partial grant, and thus to be requesting to send an unsent fragment rather than a new PDU, the CMTS can not be certain whether the CM has already accounted for fragmentation overhead in a request. Therefore, the CMTS MUST make sure that any fragment payload remainder is at least one mini-slot greater than the number of mini-slots needed to contain the overhead for a fragment (16 bytes) plus the physical layer overhead necessary to transmit a minimum sized fragment. Failure to do this may cause the CMTS to issue a grant that is not needed as the CM has completed transmission of the fragment payload remainder using the previous partial grant. This may cause the CM to get out of sync with the CMTS by inadvertently starting a new fragmentation. Also the CMTS needs to deal with the fact that with certain sets of physical layer parameters, the CM may request one more mini-slot than the maximum size of a short data grant, but not actually need that many mini-slots. This happens in the case where the CM needs to push the request size beyond the short data grant limit. The CMTS needs a policy to ensure that fragmenting such requests in multiple grant mode does not lead to unneeded fragmentary grants.

C.10.3.2.2 Piggyback mode

A CMTS MAY support Piggyback Mode for performing fragmentation.

If the CMTS does not put another partial grant or a grant pending in the MAP in which it initiates fragmentation on a SID, the CM MUST automatically piggyback for the remainder. The CM calculates how much of a frame can be sent in the granted bandwidth and forms a fragment to send it. The CM utilizes the piggyback field in the fragment extended header to request the bandwidth necessary to transfer the remainder of the frame. Since the CMTS did not indicate a multiple grant in the first fragment MAP, the CM MUST keep track of the remainder to send. The request length, including physical-layer and fragmentation overhead, for the remainder of the original frame is inserted into the piggyback request byte in the fragmentation header.

If the fragment HCS is correct, the piggybacked request, if present, is passed on to the bandwidth allocation process while the fragment itself is enqueued for reassembly. Once the complete MAC Frame is reassembled, any non-privacy extended headers are processed if the packet HCS is correct, and the packet is forwarded to the appropriate destination.

C.10.3.3 Fragmentation example

C.10.3.3.1 Single packet fragmentation

Refer to Figure C.10-8. Assume that fragmentation has been enabled for a given SID.

1) (Requesting State) – CM wants to transmit a 1018 byte packet. CM calculates how much physical layer overhead (POH) is required and requests the appropriate number of minislots. CM makes a request in a contention region. Go to step 2).

2) (Waiting for Grant) – CM monitors MAPs for a grant or grant pending for this SID. If the CM's ACK time expires before the CM receives a grant or grant pending, the CM retries requesting for the packet until the retry count is exhausted – then the CM gives up on that packet. Go to step 3).

3) (First Fragment) – Prior to giving up in step 2), the CM sees a grant for this SID that is less than the requested number of minislots. The CM calculates how much MAC information can be sent in the granted number of minislots using the specified burst profile. In the example in Figure C.10-9, the first grant can hold 900 bytes after subtracting the POH. Since the fragment overhead (FRAG HDR, FHCS, and FCRC) is 16 bytes, 884 bytes of the original packet can be carried in the fragment. The CM creates a fragment composed of the FRAG HDR, FHCS, 884 bytes of the original packet, and an FCRC. The CM marks the fragment as first and prepares to send the fragment. Go to step 4).

4) (First Fragment, multiple grant mode) – CM looks to see if there are any other grants or grant pendings enqueued for this SID. If so, the CM sends the fragment with the piggyback field in the FRAG HDR set to zero and awaits the time of the subsequent grant to roll around. Go to step 6). If there are not any grants or grant pendings, go to step 5).

5) (First Fragment, piggyback mode) – If there are no other grants or grant pendings for this SID in this MAP, the CM calculates how many mini-slots are required to send the remainder of the fragmented packet, including the fragmentation overhead, and physical layer overhead, and inserts this amount into the piggyback field of the FRAG HDR. The CM then sends the fragment and starts its ACK timer for the piggyback request. In the example in Figure C.10-9, the CM sends up a request for enough minislots to hold the POH plus 150 bytes (1018 – 884 + 16). Go to step 6).

6) (Waiting for Grant) – The CM is now waiting for a grant for the next fragment. If the CM's ACK timer expires while waiting on this grant, the CM send up a request for enough mini-slots to send the remainder of the fragmented packet, including the fragmentation overhead, and physical layer overhead. Go to step 7).

7) (Receives next fragment grant) – Prior to giving up in step 6), the CM sees another grant for this SID. The CM checks to see if the grant size is large enough to hold the remainder of the fragmented packet, including the fragmentation overhead and physical layer overhead. If so, go to step 10). If not, go to step 8).

8) (Middle Fragment, multiple grant mode) – Since the remainder of the packet (plus overhead) will not fit in the grant, the CM calculates what portion will fit. The CM encapsulates this portion of the packet as a middle fragment. The CM then looks for any other grants or grant pendings enqueued for this SID. If either are present, the CM sends the fragment with the piggyback field in the FRAG HDR set to zero and awaits the time of the subsequent grant to roll around. Go to step 6). If there are not any grants or grant pendings, go to step 9).

9) (Middle Fragment, piggyback mode) – The CM calculates how many minislots are required to send the remainder of the fragmented packet, including the fragmentation overhead and physical layer overhead, and inserts this amount into the piggyback field of the FRAG HDR. The CM then sends the fragment and starts its ACK timer for the piggyback request. Go to step 6).

10) (Last Fragment) – The CM encapsulates the remainder of the packet as a last fragment. If there is no other packet enqueued, or there is a another grant or a grant pending enqueued for this SID, the CM places a zero in the REQ field of the FRAG HDR. If there is another packet enqueued with no grant or grant pending, the CM calculates the number of minislots required to send the next packet and places this number in the REQ field in the FRAG HDR. The CM then transmits the packet. Go to step 11). In the example in Figure C.10-9, the grant is large enough to hold the remaining 150 bytes plus POH.

11) (Normal operation) – The CM then returns the normal operation of waiting for grants and requesting for packets. If at any time fragmentation is enabled and a grant arrives that is smaller than the request, the fragmentation process starts again as in step 2).

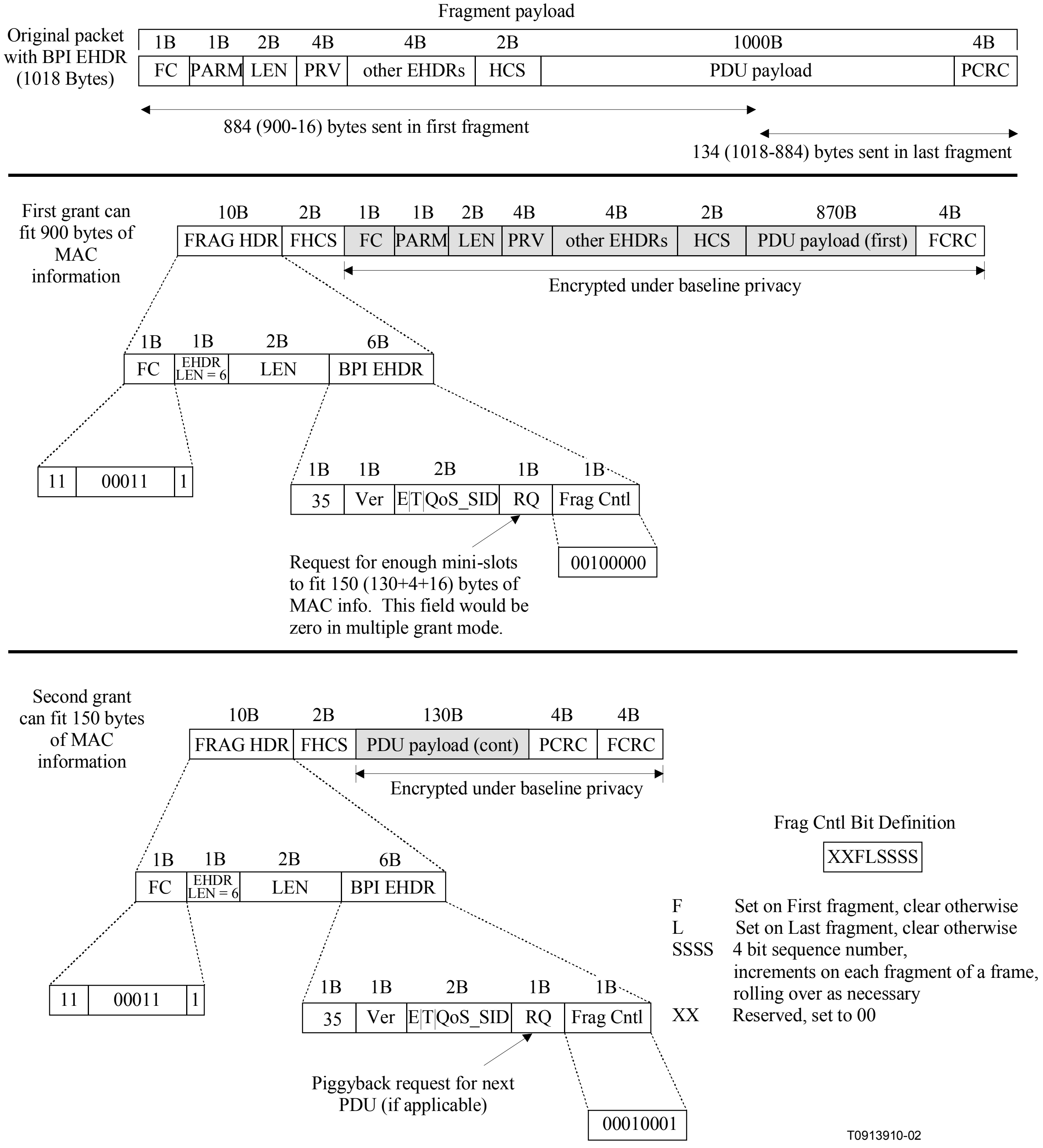

Fragment payload
Original packet with BPI EHDR (1018 Bytes)
1B 1B 2B 4B 4B 2B 1000B 4B
FC PARM LEN PRV other EHDRs HCS PDU payload PCRC
884 (900-16) bytes sent in first fragment
134 (1018-884) bytes sent in last fragment
First grant can fit 900 bytes of MAC information
10B 2B 1B 1B 2B 4B 4B 2B 870B 4B
FRAG HDR FHCS FC PARM LEN PRV other EHDRs HCS PDU payload (first) FCRC
Encrypted under baseline privacy
1B 1B 2B 6B
FC EHDR LEN = 6 LEN BPI EHDR
11 00011 1
1B 1B 2B 1B 1B
35 Ver E T QoS_SID RQ Frag Cntl
00100000
Request for enough mini-slots to fit 150 (130+4+16) bytes of MAC info. This field would be zero in multiple grant mode.
Second grant can fit 150 bytes of MAC information
10B 2B 130B 4B 4B
FRAG HDR FHCS PDU payload (cont) PCRC FCRC
Encrypted under baseline privacy
1B 1B 2B 6B
FC EHDR LEN = 6 LEN BPI EHDR
11 00011 1
1B 1B 2B 1B 1B
35 Ver E T QoS_SID RQ Frag Cntl
00010001
Piggyback request for next PDU (if applicable)
Frag Cntl Bit Definition
XXFLSSSS
F Set on First fragment, clear otherwise
L Set on Last fragment, clear otherwise
SSSS 4 bit sequence number, increments on each fragment of a frame, rolling over as necessary
XX Reserved, set to 00
T0913910-02

Figure C.10-9/J.112 – Example of fragmenting a single packet

C.10.3.3.2 Concatenated packet fragmentation

After the CM creates the concatenated packet, the CM treats the concatenated packet as a single PDU. Figure C.10-10 shows an example of a concatenated packet broken into 3 fragments. Note that the packet is fragmented without regard to the packet boundaries within the concatenated packet.

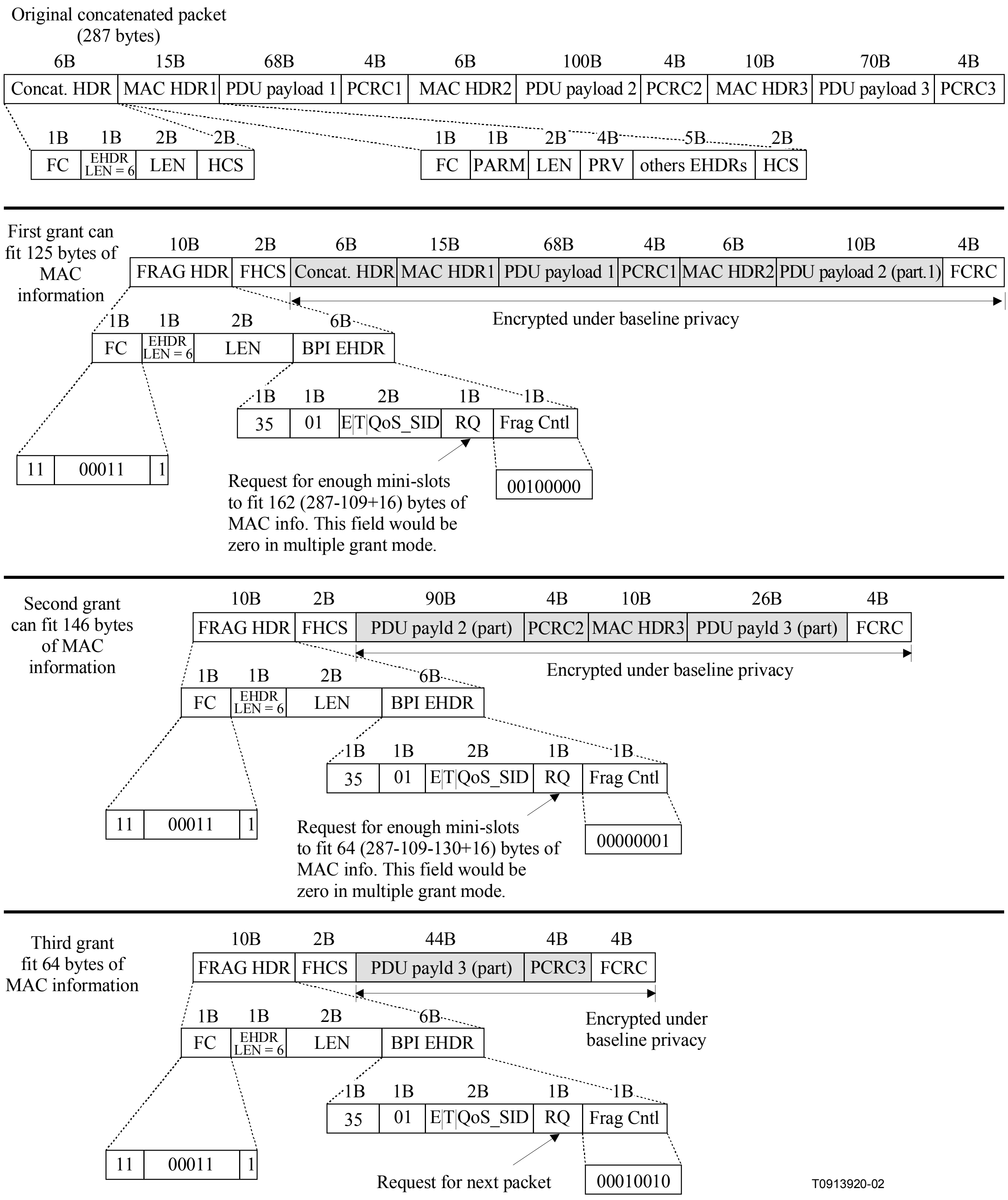


Figure C.10-10/J.112 – Fragmented concatenated packet example

C.10.4 Payload header suppression

The overview clause (C.10.4.1) explains the principles of Payload Header Suppression. The subsequent clauses explain the Signalling for initialization, operation, and termination. Finally, specific upstream and downstream examples are given. The following definitions are used:

Table C.10-5/J.112 – Payload header suppression definitions

PHS	Payload Header Suppression	Suppressing an initial byte string at the sender and restoring the byte string at the receiver.
PHS Rule	Payload Header Suppression Rule	A set of TLV's that apply to a specific PHS Index.
PHSF	Payload Header Suppression Field	A string of bytes representing the header portion of a PDU in which one or more bytes will be suppressed (i.e., a snapshot of the uncompressed PDU header inclusive of suppressed and unsuppressed bytes).
PHSI	Payload Header Suppression Index	An 8 bit value which references the suppressed byte string.
PHSM	Payload Header Suppression Mask	A bit mask which indicates which bytes in the PHSF to suppress, and which bytes to not suppress.
PHSS	Payload Header Suppression Size	The length of the Suppressed Field in bytes. This value is equivalent to the number of bytes in the PHSF and also the number of valid bits in the PHSM.
PHSV	Payload Header Suppression Verify	A flag which tells the sending entity to verify all bytes which are to be suppressed.

C.10.4.1 Overview

In Payload Header Suppression, a repetitive portion of the payload headers following the Extended Header field is suppressed by the sending entity and restored by the receiving entity. In the upstream, the sending entity is the CM and the receiving entity is the CMTS. In the downstream, the sending entity is the CMTS and the receiving entity is the CM. The MAC Extended Header contains a Payload Header Suppression Index (PHSI) which references the Payload Header Suppression Field (PHSF).

Although PHS may be used with any Service Flow Type, it has been designed for use with the Unsolicited Grant Service (UGS) Scheduling Type. UGS works most efficiently with packets of a fixed length. PHS works well with UGS because, unlike other header compression schemes sometimes used with IP data, PHS always suppresses the same number of bytes in each packet. PHS will always produce a fixed length compressed packet header.

The sending entity uses Classifiers to map packets into a Service Flow. The Classifier uniquely maps packets to its associated Payload Header Suppression Rule. The receiving entity uses the Service Identifier (SID) and the PHSI to restore the PHSR.

Once the PHSF and PHSS fields of a rule are known, the rule is considered "fully defined" and none of its fields can be changed. If modified PHS operation is desired for packets classified to the flow, the old rule must be removed from the Service Flow, and a new rule must be installed.

When a classifier is deleted, any associated PHS rule MUST also be deleted.

PHS has a PHSV option to verify or not verify the payload before suppressing it. PHS also has a PHSM option to allow select bytes not to be suppressed. This is used for sending bytes which change such as IP sequence numbers, and still suppressing bytes which do not change.

PHS rules are consistent for all scheduling service types. Requests and grants of bandwidth are specified after suppression has been accounted for. For Unsolicited Grant Services, the grant size is chosen with the Unsolicited Grant Size TLV. The packet with its header suppressed may be equal to, or less than, the grant size.

The CMTS MUST assign all PHSI values just as it assigns all SID values. Either the sending or the receiving entity MAY specify the PHSF and PHSS. This provision allows for preconfigured headers, or for higher level Signalling protocols outside the scope of this annex to establish cache entries. PHS is intended for unicast service, and is not defined for multicast service.

It is the responsibility of the higher-layer service entity to generate a PHS Rule which uniquely identifies the suppressed header within the Service Flow. It is also the responsibility of the higher-layer service entity to guarantee that the byte strings being suppressed are constant from packet to packet for the duration of the Active Service Flow.

C.10.4.2 Example applications

- A Classifier on an upstream Service Flow which uniquely defines a Voice-over-IP (VoIP) flow by specifying Protocol Type of UDP, IP SA, IP DA, UDP Source Port, UDP Destination Port, the Service Flow Reference, and a PHS Size of 42 bytes. A PHS Rule references this Classifier providing a PHSI value which identifies this VoIP media flow. For the upstream case, 42 bytes of payload header are verified and suppressed, and a 2 byte extended header containing the PHSI is added to every packet in that media flow.
- A Classifier which identifies the packets in a Service Flow, of which 90% match the PHSR. Verification is enabled. This may apply in a packet compression situation where, every so often, compression resets are done and the header varies. In this example, the scheduling algorithm would allow variable bandwidth, and only 90% of the packets might get their headers suppressed. Since the existence of the PHSI extended header will indicate the choice made, the simple SID/PHSI lookup at the receiving entity will always yield the correct result.
- A Classifier on an upstream Service Flow which identifies all IP packets by specifying Ethertype of IP, the Service Flow ID, a PHSS of 14 bytes, and no verification by the sending entity. In this example, the CMTS has decided to route the packet, and knows that it will not require the first 14 bytes of the Ethernet header, even though some parts such as the Source Address or Destination Address may vary. The CM removes 14 bytes from each upstream frame (Ethernet Header) without verifying their contents and forwards the frame to the Service Flow.

C.10.4.3 Operation

To clarify operational packet flow, this clause describes one potential implementation. CM and CMTS implementations are free to implement Payload Header Suppression in any manner as long as the protocol specified in this clause is followed. Figure C.10-11 illustrates the following procedure.

A packet is submitted to the CM MAC Service Layer. The CM applies its list of Classifier rules. A match of the rule will result in an Upstream Service Flow, SID, and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the CM will compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM. If they match, the CM will suppress all the bytes in the Upstream Suppression Field except the bytes masked by PHSM. The CM will then insert the PHSI into the PHS_Parm field of the Service Flow EH Element, and queue the packet on the Upstream Service Flow.

When the packet is received by the CMTS, the CMTS will determine the associated SID either by internal means or from other Extended Headers elements such as the BPI Extended Header. The CMTS uses the SID and the PHSI to look up PHSF, PHSM, and PHSS. The CMTS reassembles the packet and then proceeds with normal packet processing. The reassembled packet will contain bytes from the PHSF. If verification was enabled, then the PHSF bytes will equal the original header byes. If verification was not enabled, then there is no guarantee that the PHSF bytes will match the original header bytes.

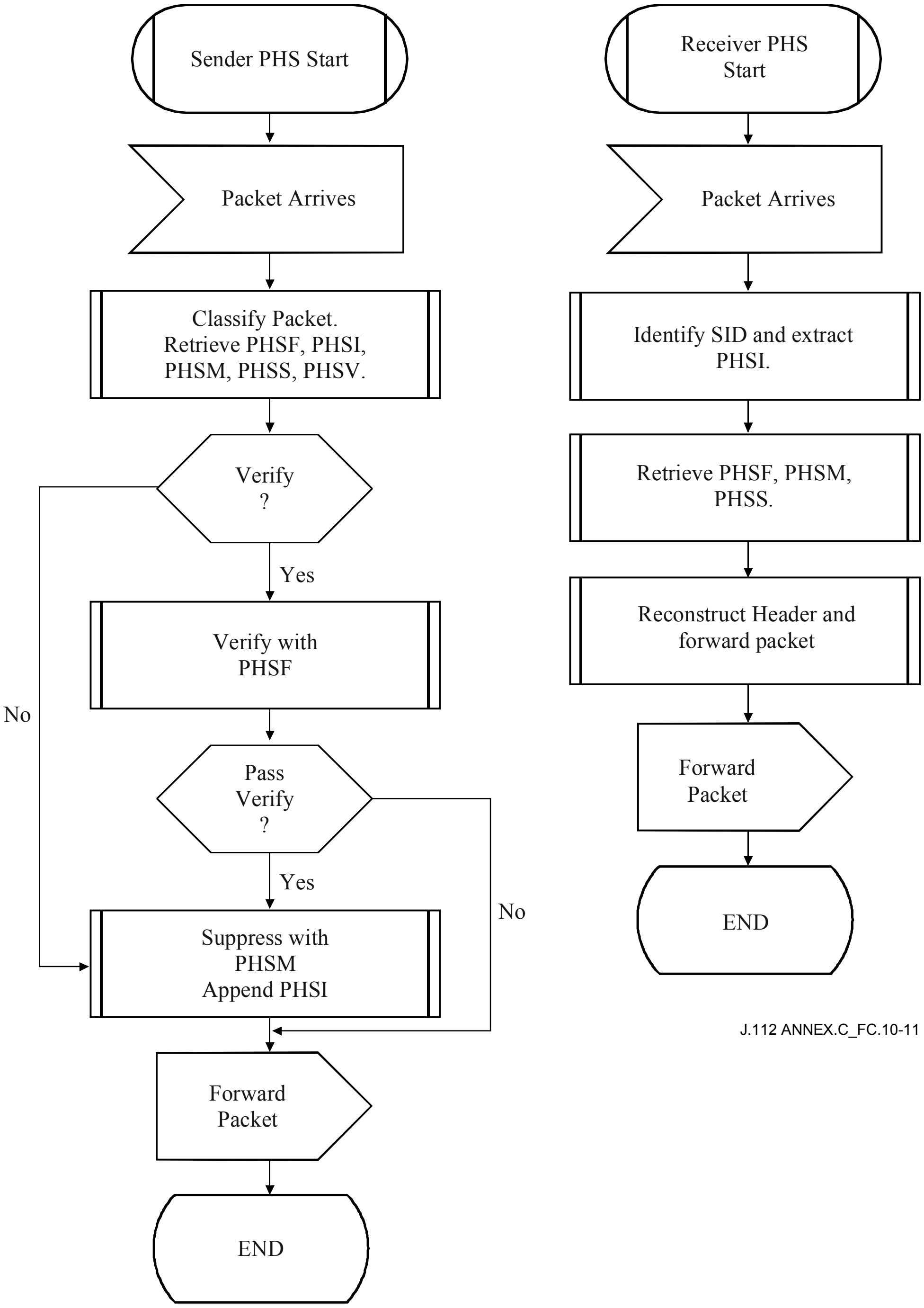

Sender PHS Start
Packet Arrives
Classify Packet. Retrieve PHSF, PHSI, PHSM, PHSS, PHSV.
Verify ?
Yes
Verify with PHSF
No
Pass Verify ?
Yes
No
Suppress with PHSM Append PHSI
Forward Packet
END
Receiver PHS Start
Packet Arrives
Identify SID and extract PHSI.
Retrieve PHSF, PHSM, PHSS.
Reconstruct Header and forward packet
Forward Packet
END
J.112 ANNEX.C_FC.10-11

Figure C.10-11/J.112 – Payload header suppression operation

A similar operation occurs in the downstream. The CMTS applies its list of Classifiers. A match of the Classifier will result in a Downstream Service Flow and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set to zero, or is not present, the CMTS will verify the Downstream Suppression Field in the packet with the PHSF. If they match, the CMTS will suppress all the bytes in the Downstream Suppression Field except the bytes masked by PHSM. The CMTS will then insert the PHSI into the PHS_Parm field of the Service Flow EH Element, and queue the packet on the Downstream Service Flow.

The CM will receive the packet based upon the Ethernet Destination Address filtering. The CM then uses the PHSI to lookup PHSF, PHSM, and PHSS. The CM reassembles the packet and then proceeds with normal packet processing.

Figure C.10-12 demonstrates packet suppression and restoration when using PHS masking. Masking allows only bytes which do not change to be suppressed. Note that the PHSF and PHSM span the entire Suppression Field, including suppressed and unsuppressed bytes.

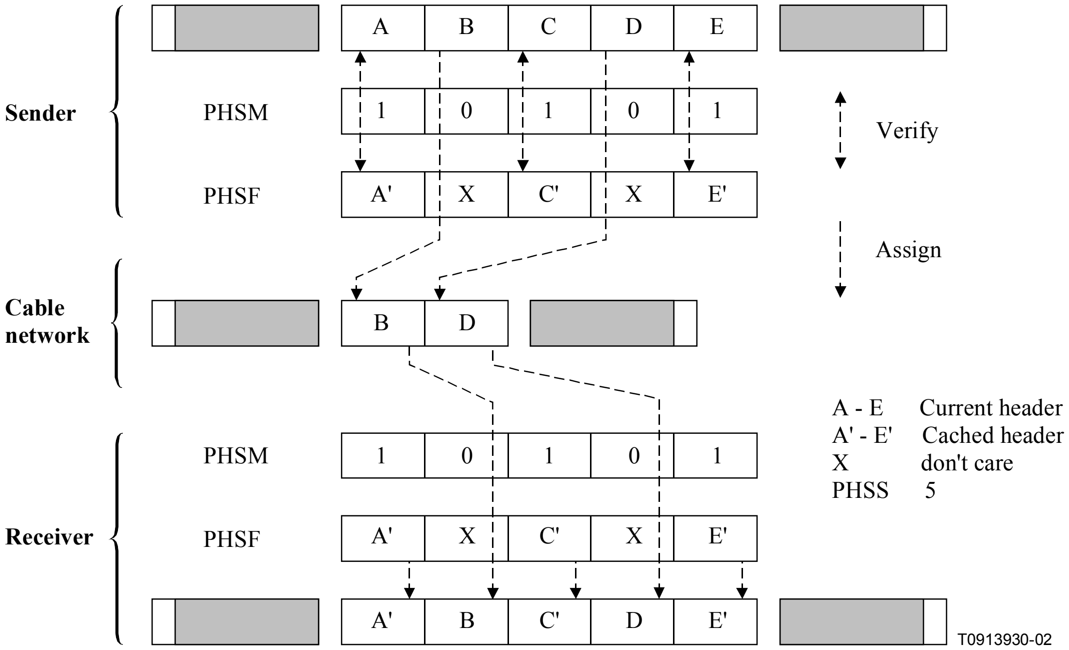


Figure C.10-12/J.112 – Payload header suppression with masking

C.10.4.4 Signalling

Payload Header Suppression requires the creation of three objects:

- Service Flow;
- Classifier;
- Payload Header Suppression Rule.

These three objects MAY be created in separate message flows, or MAY be created simultaneously.

PHS Rules are created with Registration, DSA, or DSC messages. The CMTS MUST define the PHSI when the PHS Rule is created. PHS Rules are deleted with the DSC or DSD messages. The CM or CMTS MAY define the PHSS and PHSF.

Figure C.10-13 shows the two ways to signal the creation of a PHS Rule.

It is possible to partially define a PHS rule (in particular the size of the rule) at the time a Service Flow is created.

As an example, it is likely that when a Service Flow is first provisioned the size of the header field to be suppressed will be known. The values of some items within the field (e.g., IP addresses, UDP port numbers, etc.) may not be known and would be provided in a subsequent DSC as part of the activation of the Service Flow (using the "Set PHS Rule" DSC Action).

A PHS rule is partially defined when the PHSF and PHSS field values are not both known. Once both PHSF and PHSS are known, the rule is considered fully defined, and MUST NOT be modified via DSC Signalling. PHSV and PHSM fields have default values, thus are not required to fully define a PHS rule. If PHSV and PHSM are not known when the rule becomes fully defined, their default values are used, and MUST NOT be modified via DSC Signalling.

Each step of the PHS rule definition, whether it is a registration request, DSA or a DSC, MUST contain Service Flow ID (or reference), Classifier ID (or reference) to uniquely identify the PHS rule being defined. A PHS Index and Service ID pair is used to uniquely identify the PHS rule during upstream packet transfer. A PHS Index is enough to uniquely identify the PHS rule used in downstream packet transfer.

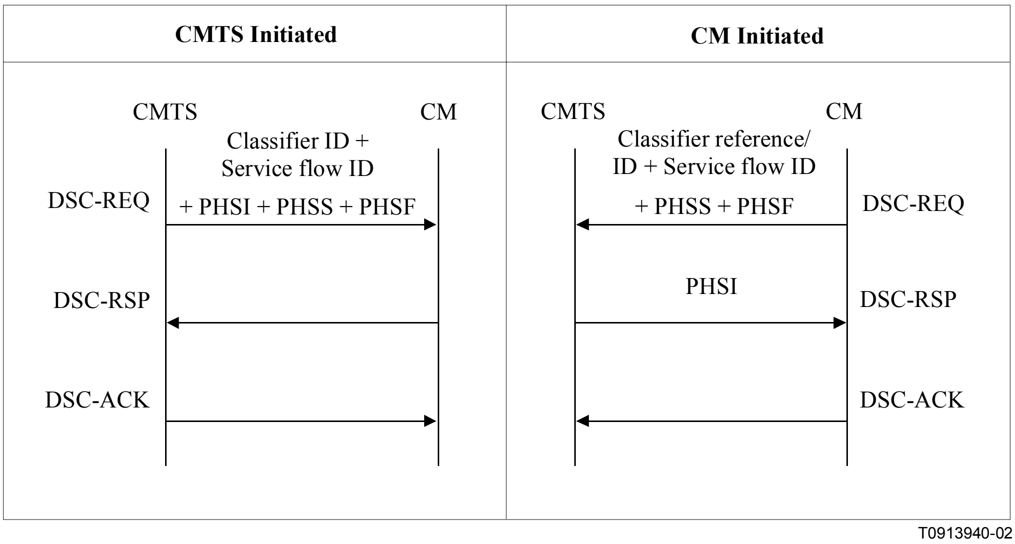

CMTS Initiated
CM Initiated
CMTS
CM
Classifier ID + Service flow ID + PHSI + PHSS + PHSF
DSC-REQ
DSC-RSP
DSC-ACK
CMTS
CM
Classifier reference/ ID + Service flow ID + PHSS + PHSF
DSC-REQ
PHSI
DSC-RSP
DSC-ACK
T0913940-02

Figure C.10-13/J.112 – Payload header suppression signalling example

C.10.4.5 Payload header suppression examples

C.10.4.5.1 Upstream example

A Service Class with the Service Class Name of "G711-US-UGS-HS-42" is established which is intended for G.711 VoIP traffic in the upstream with Unsolicited Grant Service. When Classifiers are added to the flow, a PHSS value of 42 is included which explicitly states that the first 42 bytes following the MAC Extended Header on all packets in that flow must be verified, suppressed and restored. In this example, the Service Class is configured such that any packet which does not verify correctly will not have its header suppressed and will be discarded since it will exceed the Unsolicited Grant Size (refer to C.C.2.2.6.3).

Figure C.10-14 shows the encapsulation used in the upstream with and without Payload Header Suppression. An RTP Voice over IP Payload without IPsec is used as a specific example to demonstrate efficiency.

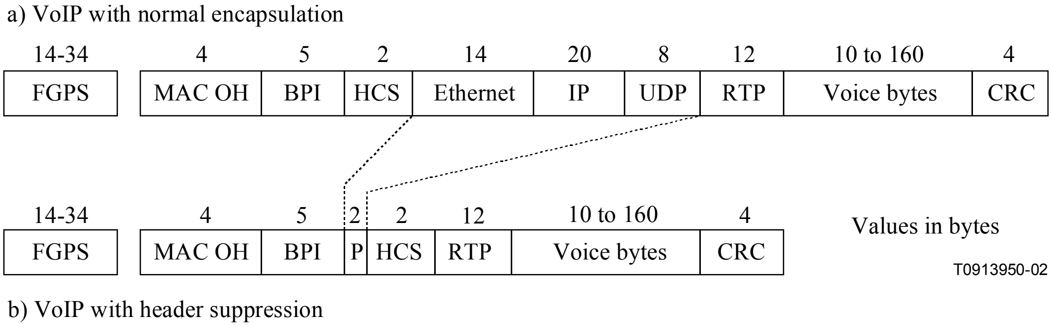


Figure C.10-14/J.112 – Upstream payload header suppression example

Figure C.10-14a) shows a normal RTP packet carried on an upstream channel. The beginning of the frame represents the physical layer overhead (FGPS) of FEC, guard time, preamble, and stuffing bytes. Stuffing bytes occur in the last code word and when mapping blocks to minislots. Next is the MAC layer overhead including the 6 byte MAC header with a 5 byte BPI Extended Header, the

14 byte Ethernet Header, and the 4 byte Ethernet CRC trailer. The VoIP payload uses a 20 byte IP header, an 8 byte UDP header, and a 12 byte RTP header. The voice payload is variable and depends upon the sample time and the compression algorithm used.

Figure C.10-14b) shows the same payload with Payload Header Suppression enabled. In the upstream, Payload Header Suppression begins with the first byte after the MAC Header Checksum. The 14 byte Ethernet header, the 20 byte IP header, and the 8 byte UDP header have been suppressed, and a 2 byte PHS Extended Header element has been added, for a net reduction of 40 bytes. In this example of an established VoIP connection, these fields remain constant from packet to packet, and are otherwise redundant.

C.10.4.5.2 Downstream example

A Service Class with the Service Class Name of "G711-DS-HS-30" is established which is intended for G.711 VoIP traffic in the downstream. When Classifiers are added to the Service Flow, a PHSS value of 30 is included which explicitly indicates that 30 bytes of the payload header on all packets must be processed for suppression and restoration according to the PHSM. Any packet which does not verify correctly will not have its header suppressed but will be transmitted subject to the traffic shaping rules in place for that Service Flow.

Figure C.10-15 shows the encapsulation used in the downstream with and without Payload Header Suppression. An RTP Voice over IP Payload without IPsec is used as a specific example to demonstrate efficiency.

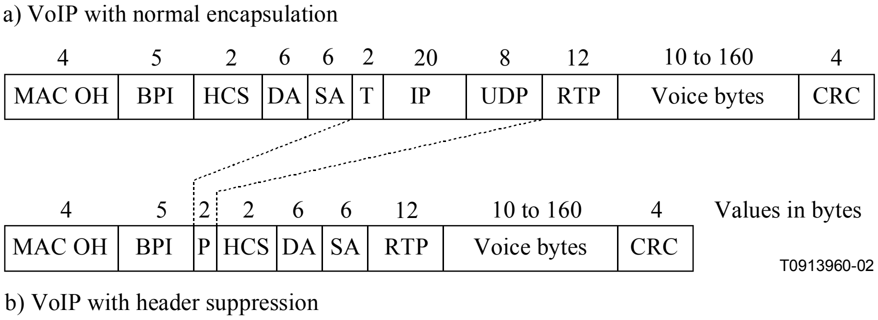


Figure C.10-15/J.112 – Downstream payload header suppression example

Figure C.10-15a) shows a normal RTP packet carried on a downstream channel. The Layer 2 overhead includes the 6 byte MAC header with a 5 byte BPI Extended Header, the 14 byte Ethernet Header (6 byte Destination Address, 6 byte Source Address, and 2 byte EtherType field), and the 4 byte Ethernet CRC trailer. The Layer 3 VoIP payload uses a 20 byte IP header, an 8 byte UDP header, and a 12 byte RTP header. The voice payload is variable and depends upon the sample time and the compression algorithm used.

Figure C.10-15b) shows the same payload with Payload Header Suppression enabled. In the downstream, Payload Header Suppression begins with the thirteenth byte after the MAC Header Checksum. This retains the Ethernet Destination Address and Source Address which is required so that the CM may filter and receive the packet. The remaining 2 bytes of the Ethernet Header, the 20 byte IP header, and the 8 byte UDP header have been suppressed, and a 2 byte PHS Extended Header element has been added, for a net reduction of 28 bytes. In this example of an established VoIP connection, these fields remain constant from packet to packet, and are thus redundant.

C.11 Cable modem – CMTS interaction

This clause covers the key requirements for the interaction between a CM and a CMTS. The interaction can be broken down into five basic categories: initialization, authentication, configuration, authorization, and Signalling.

C.11.1 CMTS initialization

The mechanism utilized for CMTS initialization (local terminal, file download, SNMP, etc.) MUST meet the following criteria for system interoperability.

- The CMTS MUST be able to reboot and operate in a stand-alone mode using configuration data retained in non-volatile storage.
- If valid parameters are not available from non-volatile storage or via another mechanism, the CMTS MUST NOT generate any downstream messages (including SYNC). This will prevent CMs from transmitting.
- The CMTS MUST provide the information defined in clause C.8 to CMs for each upstream channel.

C.11.2 Cable modem initialization

The procedure for initialization of a cable modem MUST be as shown in Figure C.11-1. This figure shows the overall flow between the stages of initialization in a CM. 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 clauses (including error paths) are shown in the subsequent figures. Timeout values are defined in Annex C.C.

The procedure for initializing a cable modem and for a CM to reinitialize its MAC can be divided into the following phases:

- Scanning and synchronization to downstream;
- Obtain upstream parameters;
- Ranging and automatic adjustments;
- Device Class Identification (optional);
- Establish IP connectivity;
- Establish time of day;
- Transfer operational parameters;
- Registration;
- Baseline Privacy initialization, if CM is provisioned to run Baseline Privacy.

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

- A unique [IEEE802] 48 bit MAC address which is assigned during the manufacturing process. This is used to identify the modem to the various provisioning servers during initialization.

The Specification and Description Language (SDL) notation used in the following figures is shown in Figure C.11-2 (refer to [ITU-T Z.100]).

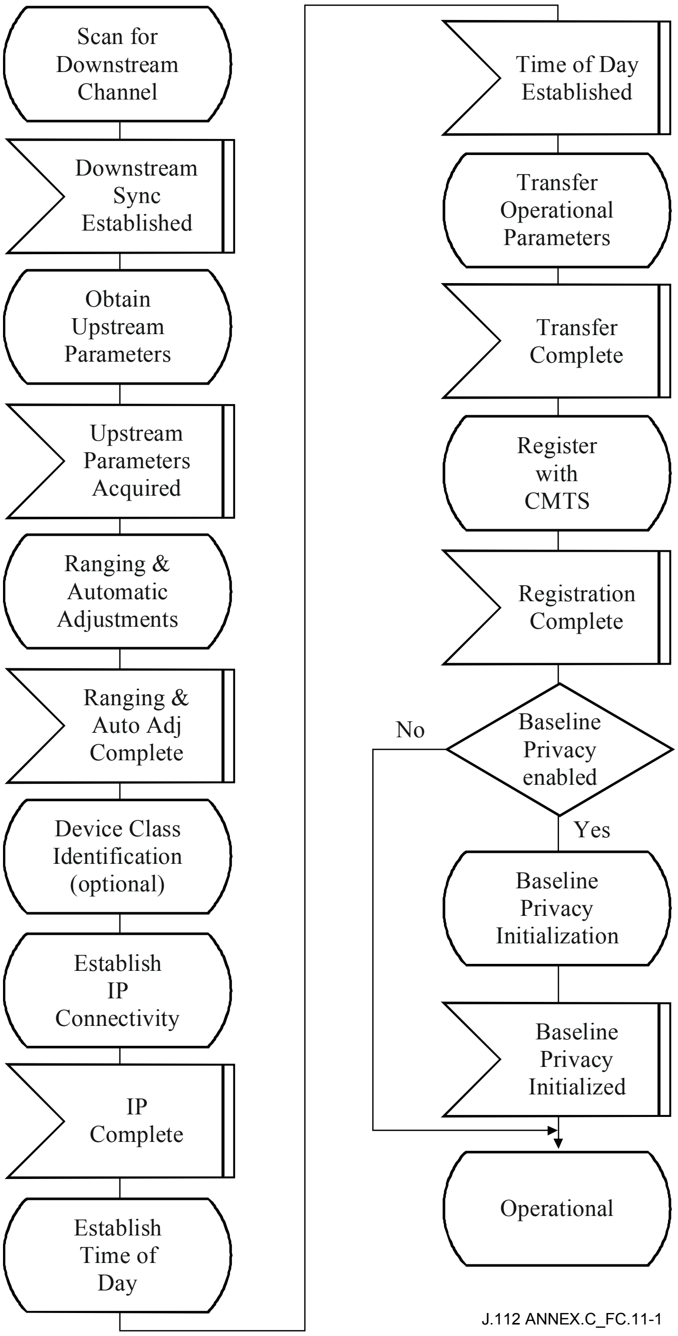

Scan for Downstream Channel
Downstream Sync Established
Obtain Upstream Parameters
Upstream Parameters Acquired
Ranging & Automatic Adjustments
Ranging & Auto Adj Complete
Device Class Identification (optional)
Establish IP Connectivity
IP Complete
Establish Time of Day
Time of Day Established
Transfer Operational Parameters
Transfer Complete
Register with CMTS
Registration Complete
Baseline Privacy enabled
No
Yes
Baseline Privacy Initialization
Baseline Privacy Initialized
Operational
J.112 ANNEX.C_FC.11-1

Figure C.11-1/J.112 – CM initialization overview

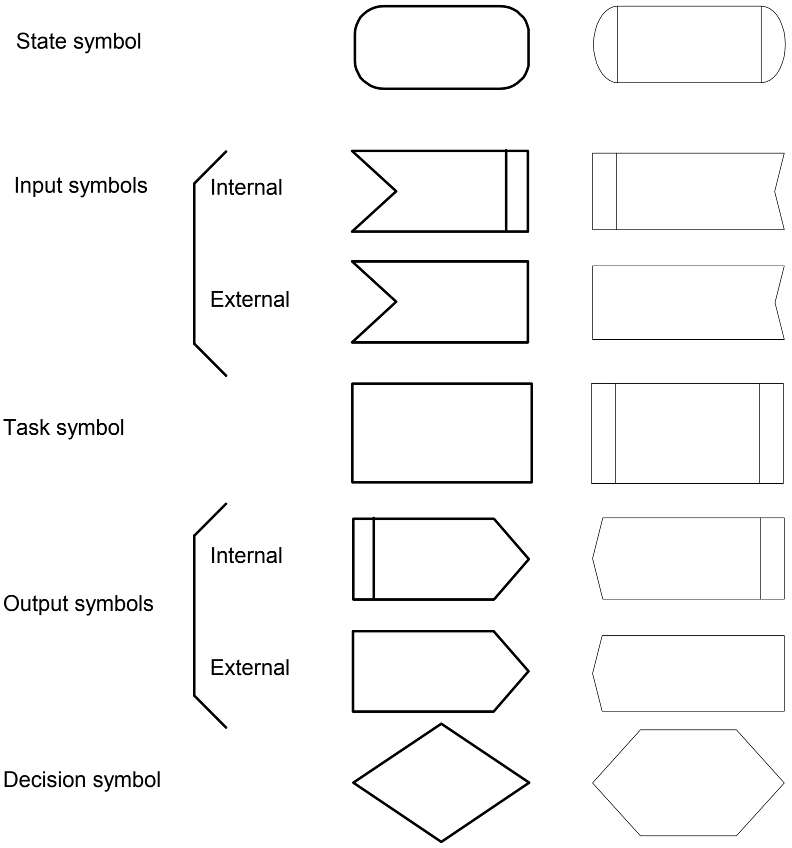


Figure C.11-2/J.112 – SDL notation

C.11.2.1 Scanning and synchronization to downstream

On initialization or after signal loss, the cable modem MUST acquire a downstream channel. The CM MUST have non-volatile storage in which the last operational parameters are stored and MUST first try to re-acquire this downstream channel. If this fails, it MUST begin to continuously scan the 6 MHz 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 modem has achieved the following steps:

- synchronization of the QAM symbol timing;
- synchronization of the FEC framing;
- synchronization of the MPEG packetization;
- recognition of SYNC downstream MAC messages.

While scanning, it is desirable to give an indication to the user that the CM is doing so.

C.11.2.2 Obtain upstream parameters

Refer to Figure C.11-3. After synchronization, the CM MUST wait for an upstream channel descriptor message (UCD) from the CMTS in order to retrieve a set of transmission parameters for a possible upstream channel. These messages are transmitted periodically from the CMTS for all available upstream channels and are addressed to the MAC broadcast address. The CM MUST determine whether it can use the upstream channel from the channel description parameters.

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

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

NOTE – Alternatively, since the SYNC message applies to all upstream channels, the CM may have already acquired a time reference from previous SYNC messages. If so, it need not wait for a new SYNC.

The CM MUST perform initial ranging at least once per Figure C.11-6. If initial ranging is not successful, then the next channel ID is selected, and the procedure restarted from UCD extraction. When there are no more channel IDs to try, then the CM MUST continue scanning to find another downstream channel.

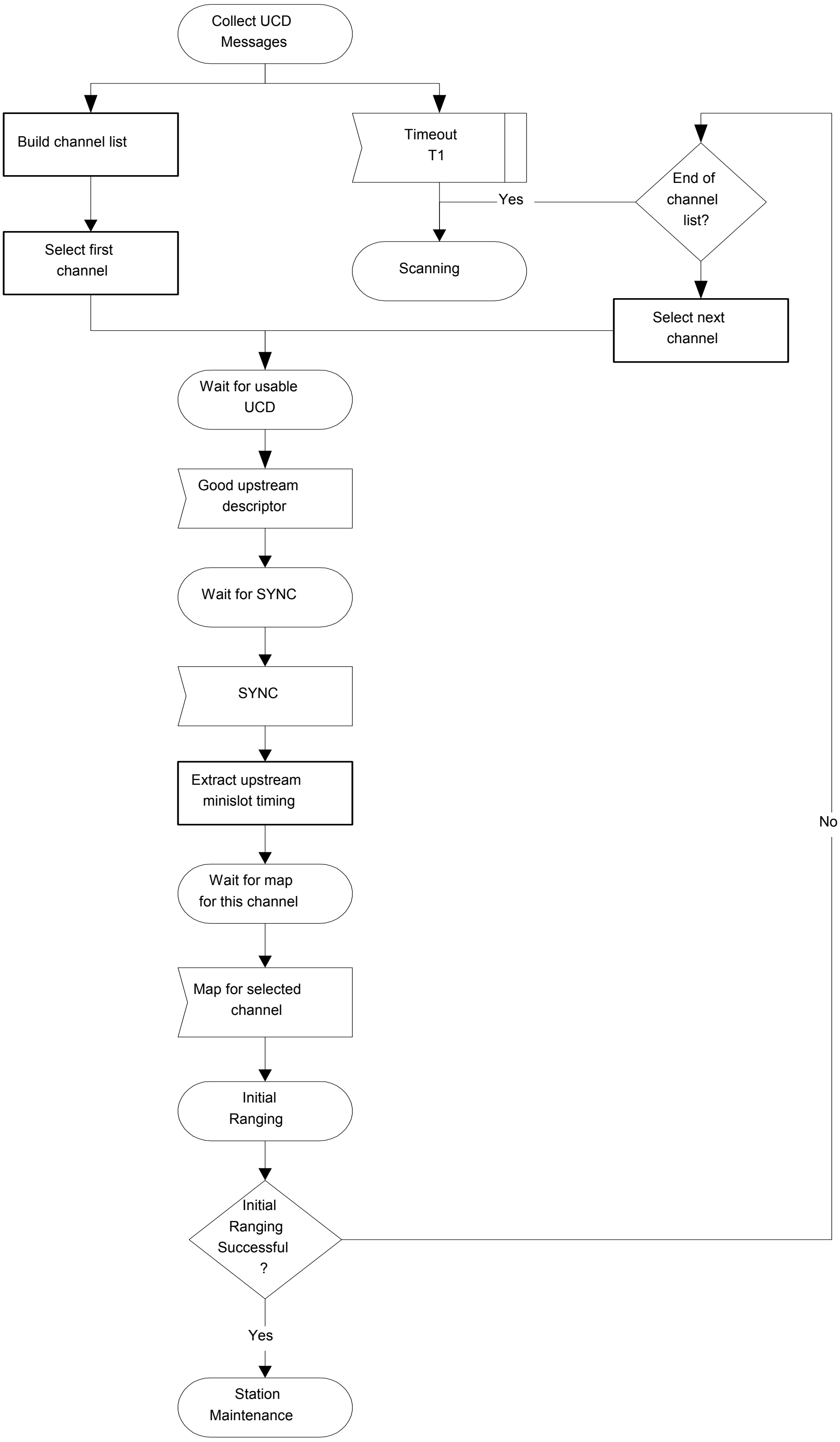


Figure C.11-3/J.112 – Obtaining upstream parameters

C.11.2.3 Message flows during scanning and upstream parameter acquisition

The CMTS MUST generate SYNC and UCD messages on the downstream at periodic intervals within the ranges defined in Annex C.C. These messages are addressed to all CMs. Refer to Figure C.11-4.

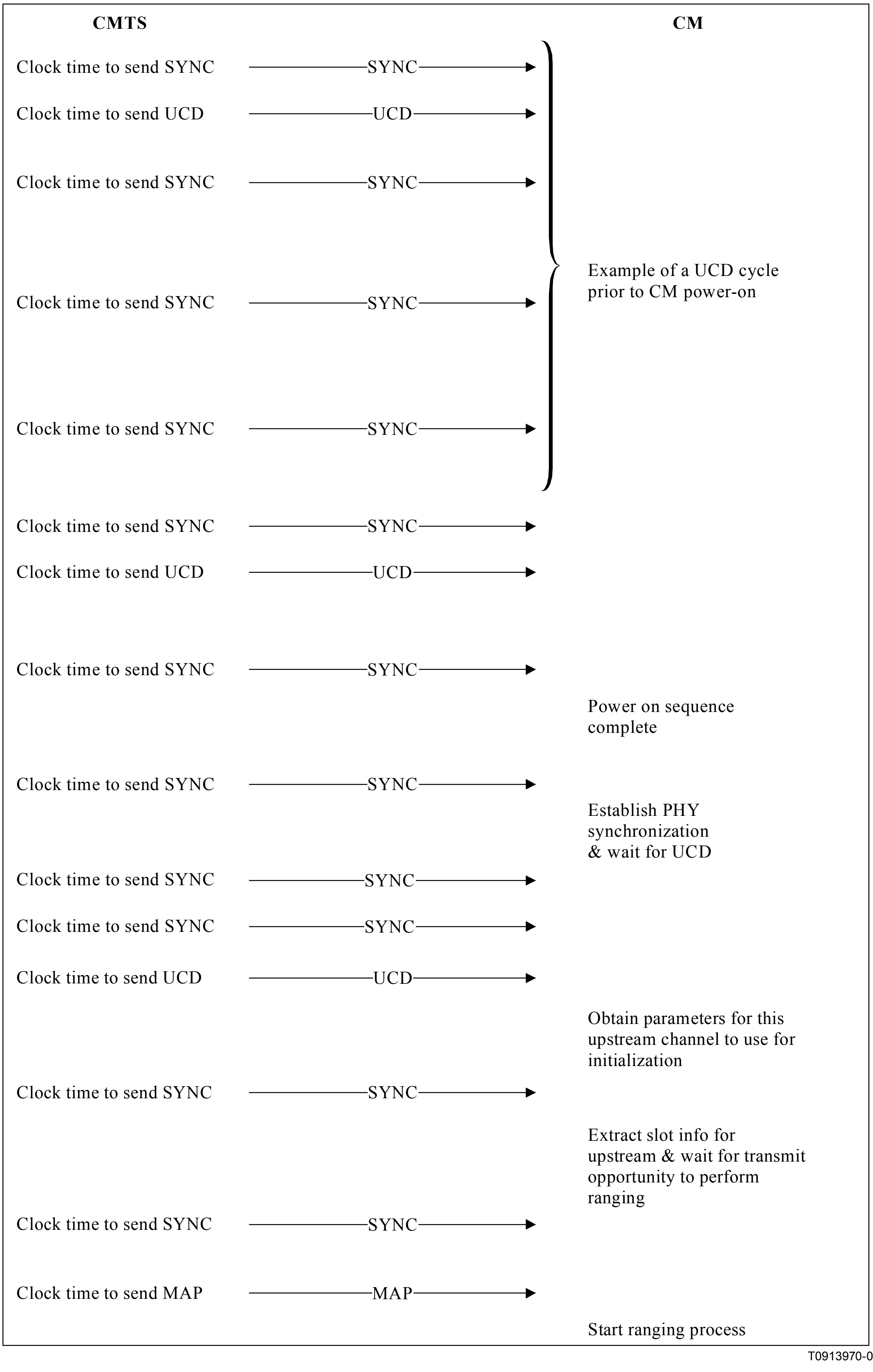


Figure C.11-4/J.112 – Message flows during scanning and upstream parameter acquisition

C.11.2.4 Ranging and automatic adjustments

The ranging and adjustment process is fully defined in clause C.8 and in the following clauses. The message sequence chart and the finite state machines on the following pages define the ranging and adjustment process which MUST be followed by compliant CMs and CMTSs. Refer to Figures C.11-5 through C.11-8.

NOTE – MAPs are transmitted as described in clause C.8.

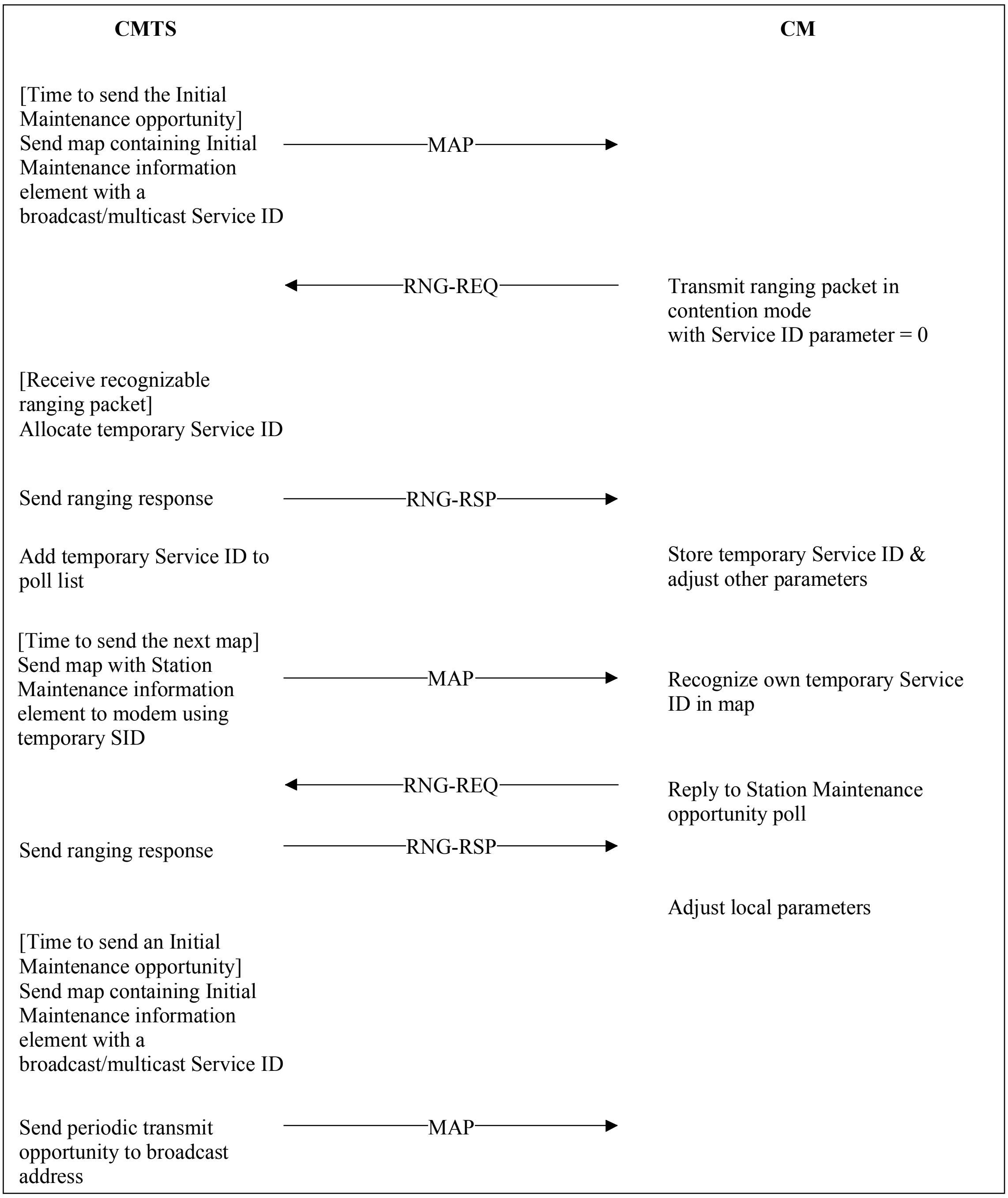
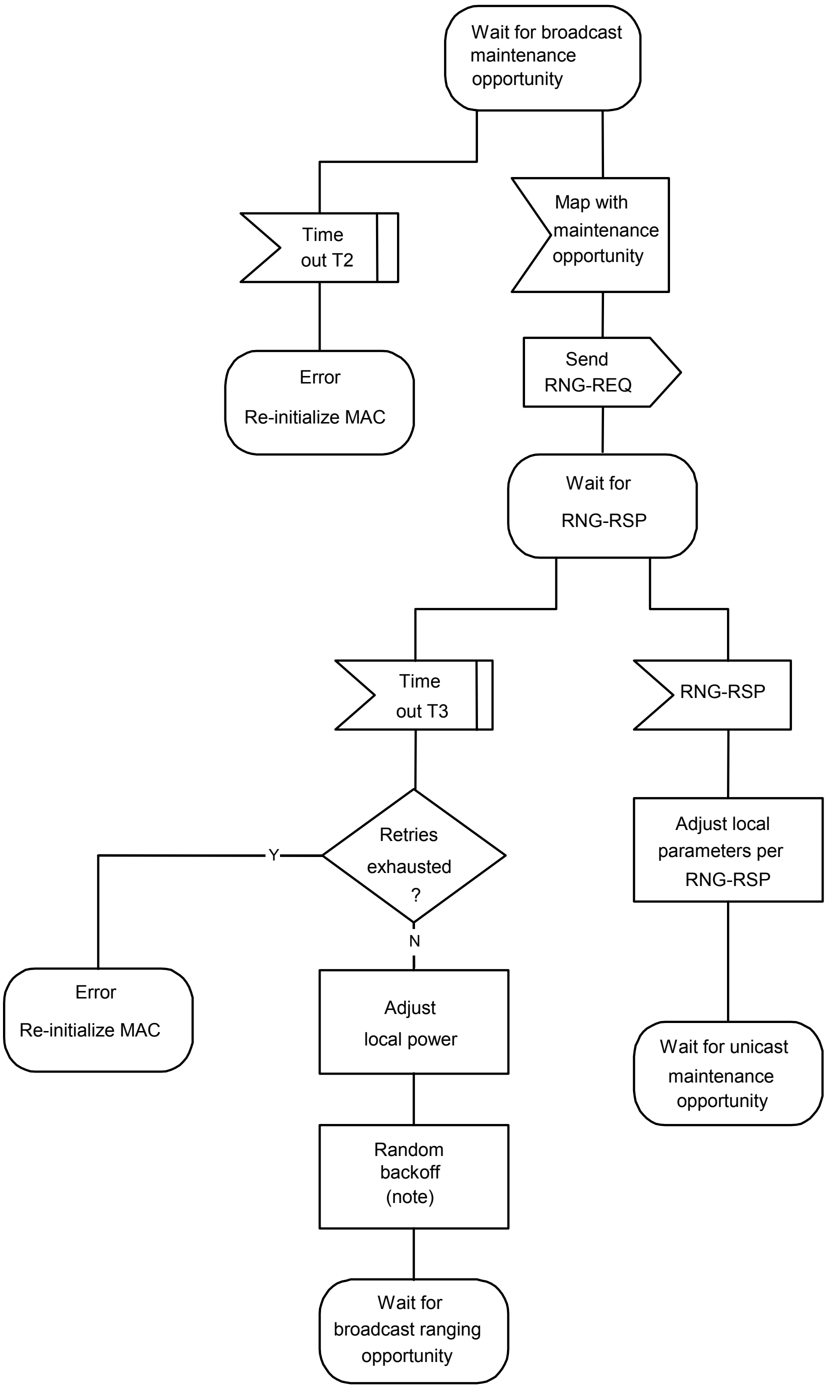

CMTS
CM
[Time to send the Initial Maintenance opportunity] Send map containing Initial Maintenance information element with a broadcast/multicast Service ID
MAP
RNG-REQ
Transmit ranging packet in contention mode with Service ID parameter = 0
[Receive recognizable ranging packet] Allocate temporary Service ID
Send ranging response
RNG-RSP
Add temporary Service ID to poll list
Store temporary Service ID & adjust other parameters
[Time to send the next map] Send map with Station Maintenance information element to modem using temporary SID
MAP
Recognize own temporary Service ID in map
RNG-REQ
Reply to Station Maintenance opportunity poll
Send ranging response
RNG-RSP
Adjust local parameters
[Time to send an Initial Maintenance opportunity] Send map containing Initial Maintenance information element with a broadcast/multicast Service ID
Send periodic transmit opportunity to broadcast address
MAP
T0913980-02

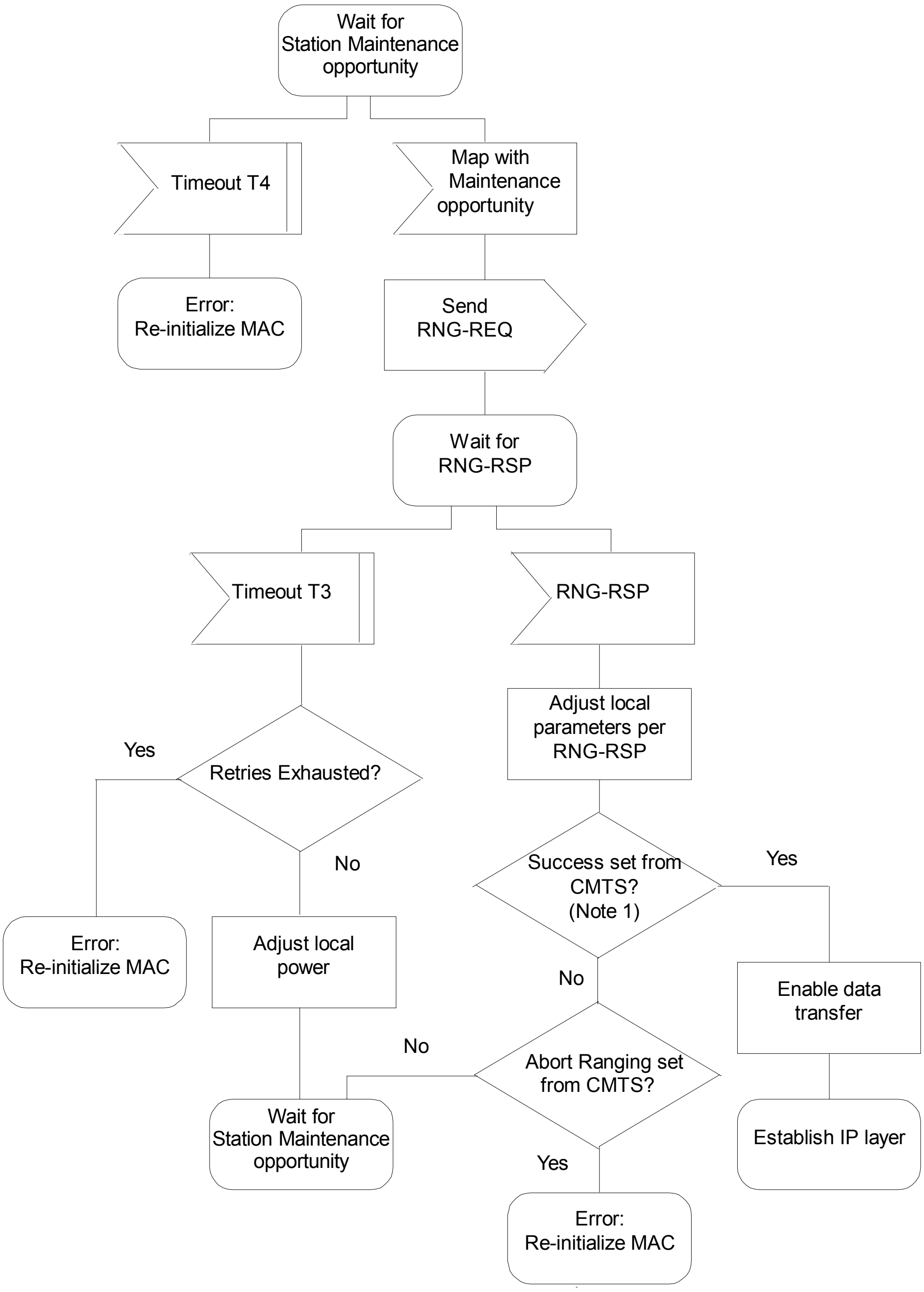
Figure C.11-5/J.112 – Ranging and automatic adjustments procedure

The CMTS MUST allow the CM sufficient time to have processed the previous RNG-RSP (i.e., to modify the transmitter parameters) before sending the CM a specific ranging opportunity. This is defined as CM Ranging Response Time in Annex C.C.


Wait for broadcast maintenance opportunity
Time out T2
Map with maintenance 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

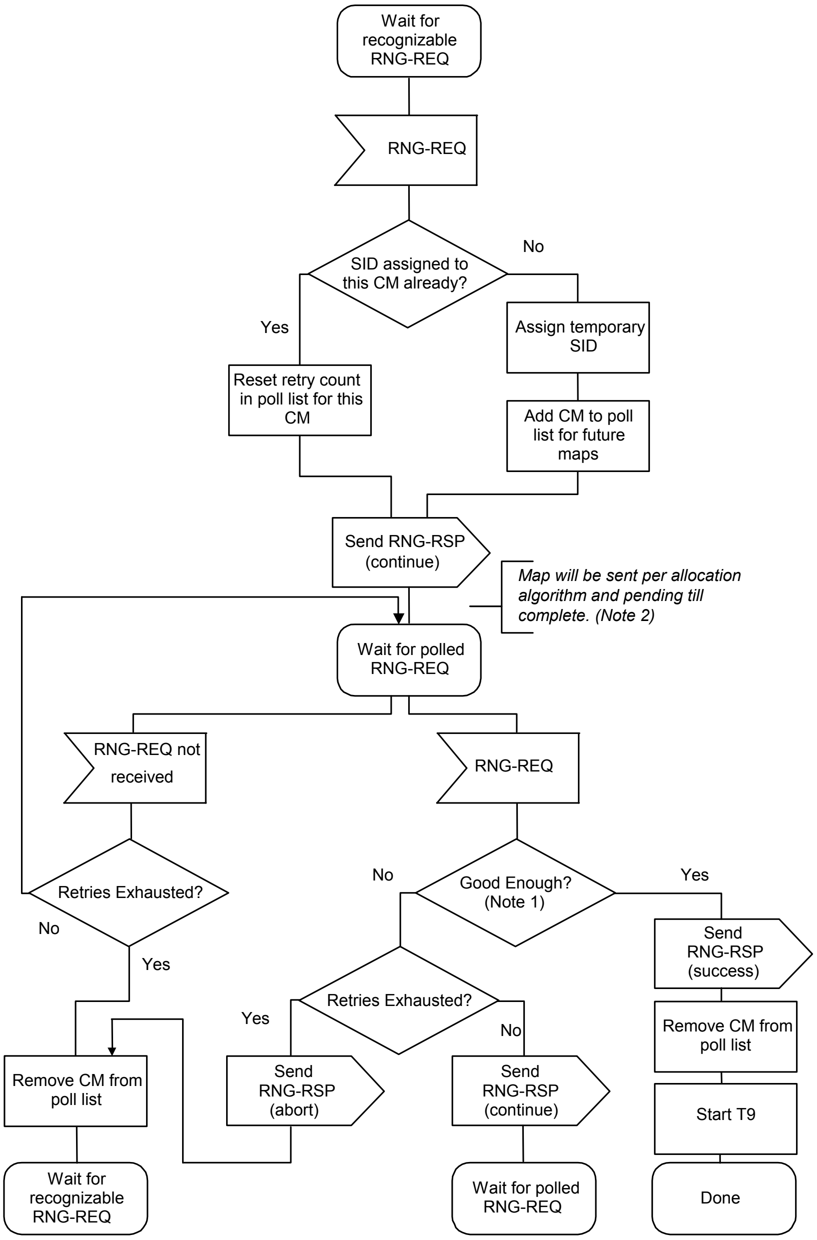
NOTE – Timeout T3 may occur because the RNG-REQs from multiple modems collided. To avoid these modems repeating the loop in lockstep, a random backoff is required. This is a backoff over the ranging window specified in the MAP. T3 timeouts can also occur during multi-channel operation. On a system with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

Figure C.11-6/J.112 – Initial ranging – CM



NOTE – Ranging Request is within the tolerance of the CMTS.

Figure C.11-7/J.112 – Initial ranging – CM (concluded)



NOTE 1 – Means ranging is within the tolerable limits of the CMTS.

NOTE 2 – RNG-REQ pending-till-complete was nonzero, the CMTS SHOULD hold off the station maintenance opportunity accordingly unless needed, for example, to adjust the CM's power level. If opportunities are offered prior to the pending-till-complete expiry, the "good-enough" test which follows receipt of a RNG-RSP MUST NOT judge the CM's transmit equalization until pending-till-complete expires.

Figure C.11-8/J.112 – Initial ranging – CMTS

C.11.2.4.1 Ranging parameter adjustment

Adjustment of local parameters (e.g., transmit power) in a CM as a result of the receipt (or non-receipt) of an RNG-RSP is considered to be implementation-dependent with the following restrictions (refer to C.8.3.6):

- all parameters MUST be within the approved range at all times;
- power adjustment MUST start from the minimum value unless a valid power is available from non-volatile storage, in which case this MUST be used as a starting point;

- power adjustment MUST be capable of being reduced or increased by the specified amount in response to RNG-RSP messages;
- if, during initialization, power is increased to the maximum value (without a response from the CMTS) it MUST wrap back to the minimum;
- for multi-channel support, the CM MUST attempt initial ranging on every suitable upstream channel before moving to the next available downstream channel;
- for multi-channel support, the CM MUST use the upstream channel ID of the range response as specified in C.8.3.

C.11.2.5 Device class identification

After Ranging is complete and before establishing IP connectivity, the CM MAY identify itself to the CMTS for use in provisioning. Refer to Figure C.11-9.

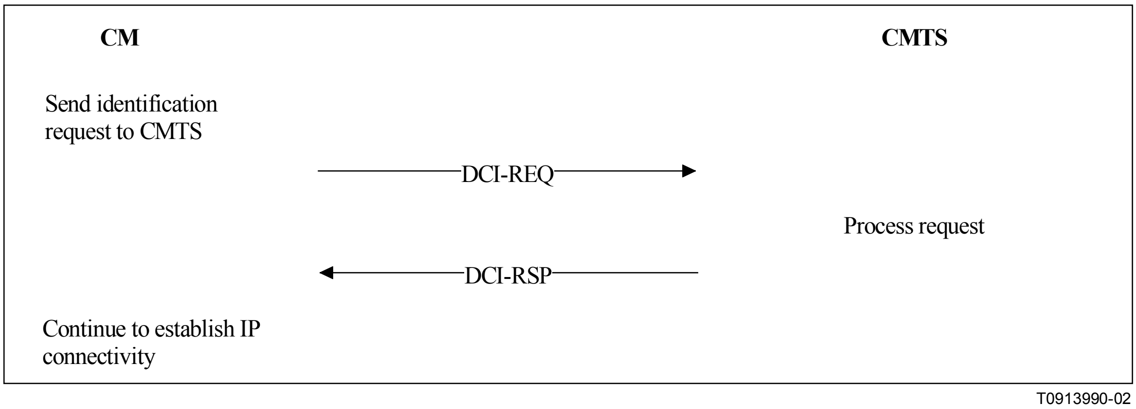

CM
CMTS
Send identification request to CMTS
DCI-REQ
Process request
DCI-RSP
Continue to establish IP connectivity
T0913990-02

Figure C.11-9/J.112 – Device class identification

If implemented, the CM MUST use an adaptive timeout for device class identification based on binary exponential backoff, similar to that used for TFTP. Refer to C.11.2.9 for details.

C.11.2.6 Establish IP connectivity

At this point, the CM MUST invoke DHCP mechanisms [RFC 2131] in order to obtain an IP address and any other parameters needed to establish IP connectivity (refer to Annex C.D). The DHCP response MUST contain the name of a file which contains further configuration parameters. Refer to Figure C.11-10.

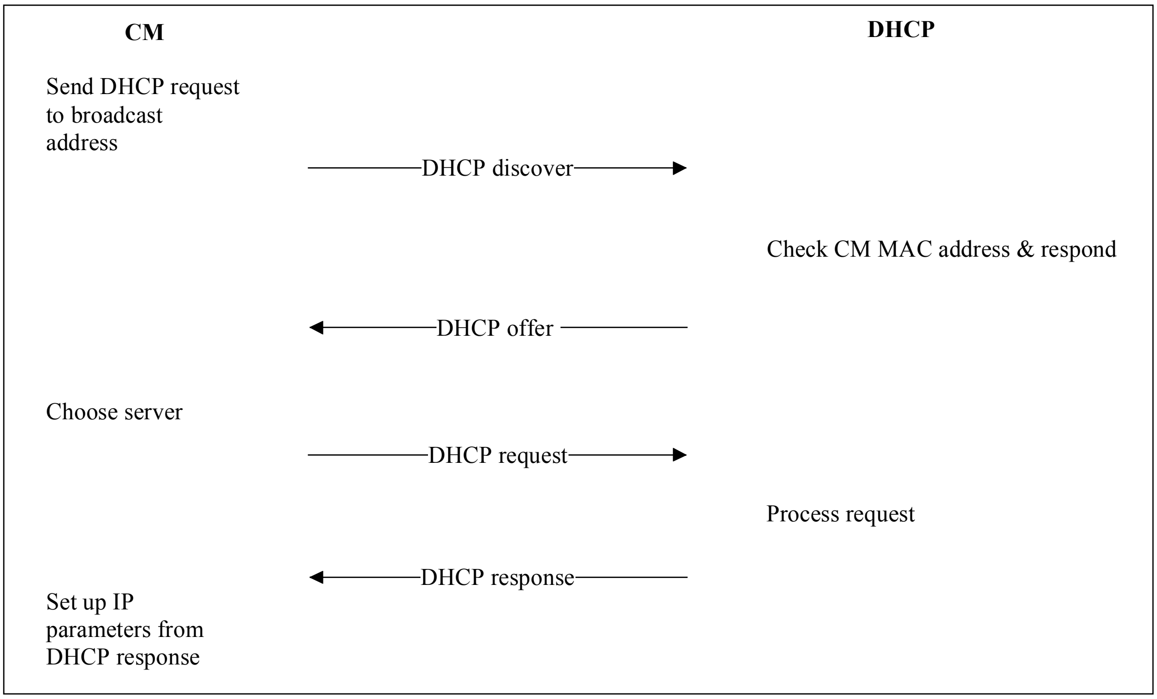

CM
DHCP
Send DHCP request to broadcast address
DHCP discover
Check CM MAC address & respond
DHCP offer
Choose server
DHCP request
Process request
DHCP response
Set up IP parameters from DHCP response
T0914000-02

Figure C.11-10/J.112 – Establishing IP Connectivity

C.11.2.7 Establish time of day

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

The protocol by which the time of day MUST be retrieved is defined in [RFC 868]. Refer to Figure C.11-11. The request and response MUST be transferred using UDP. The time retrieved from the server (UTC) MUST be combined with the time offset received from the DHCP response to create the current local time.

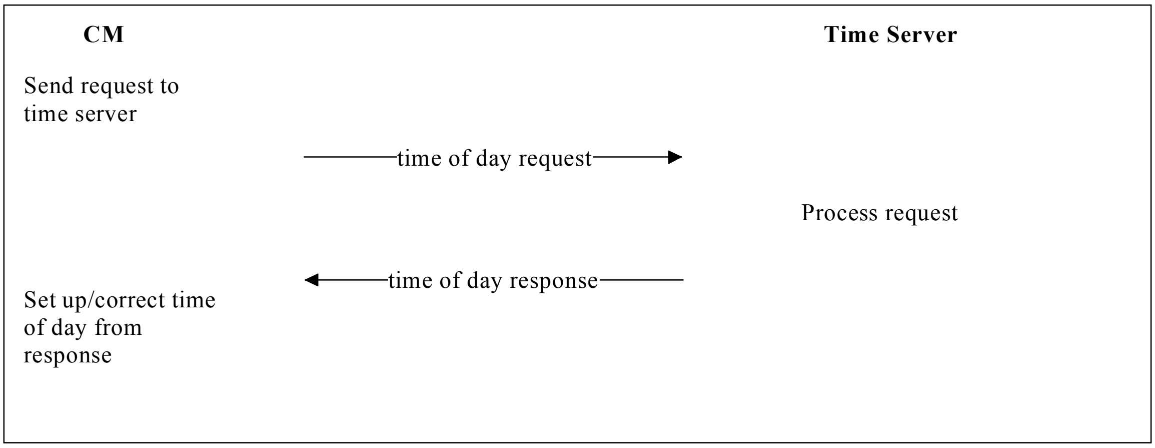


Figure C.11-11/J.112 – Establishing time of day

The DHCP server may offer a CM multiple Time of Day server IP addresses to attempt. The CM MUST attempt all Time of Day servers included in the DHCP offer until local time is established.

Successfully acquiring the Time of Day is not mandatory for a successful registration, but it is necessary for ongoing operation. If a CM is unable to establish time of day before registration it MUST log the failure, generate an alert to management facilities, then proceed to an operational state and retry periodically.

The specific timeout for Time of Day Requests is implementation-dependent. However, for each server defined, the CM MUST NOT exceed more than 3 Time of Day requests in any 5 minute period. At minimum, the CM MUST issue at least 1 Time of Day request per 5 minute period for each server specified until local time is established.

C.11.2.8 Transfer operational parameters

After DHCP is successful, the modem MUST download the parameter file using TFTP, as shown in Figure C.11-12. The TFTP configuration parameter server is specified by the "siaddr" field of the DHCP response. The CM MUST use an adaptive timeout for TFTP based on binary exponential backoff. Refer to [RFC 1123] and [RFC 2349].

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

If a modem downloads a configuration file containing an upstream channel and/or downstream frequency different from what the modem is currently using, the modem MUST NOT send a Registration Request message to the CMTS. The modem MUST redo initial ranging using the configured upstream channel and/or downstream frequency per C.8.3.6.3.

C.11.2.9 Registration

A CM MUST be authorized to forward traffic into the network once it is initialized and configured. The CM is authorized to forward traffic into the network via registration. To register with a CMTS, the CM MUST forward its configured class of service and any other operational parameters in the configuration file (refer to C.8.3.7) to the CMTS as part of a Registration Request. Figure C.11-12 shows the procedure that MUST be followed by the CM.

The configuration parameters downloaded to the CM MUST include a network access control object (see C.C.1.1.3). If this is set to "no forwarding," the CM MUST NOT forward data from attached CPE to the network, yet the CM MUST respond to network management requests. This allows the CM to be configured in a mode in which it is manageable but will not forward data. The CM MUST NOT send a REG-REQ if the configuration file lacks a network access control object.

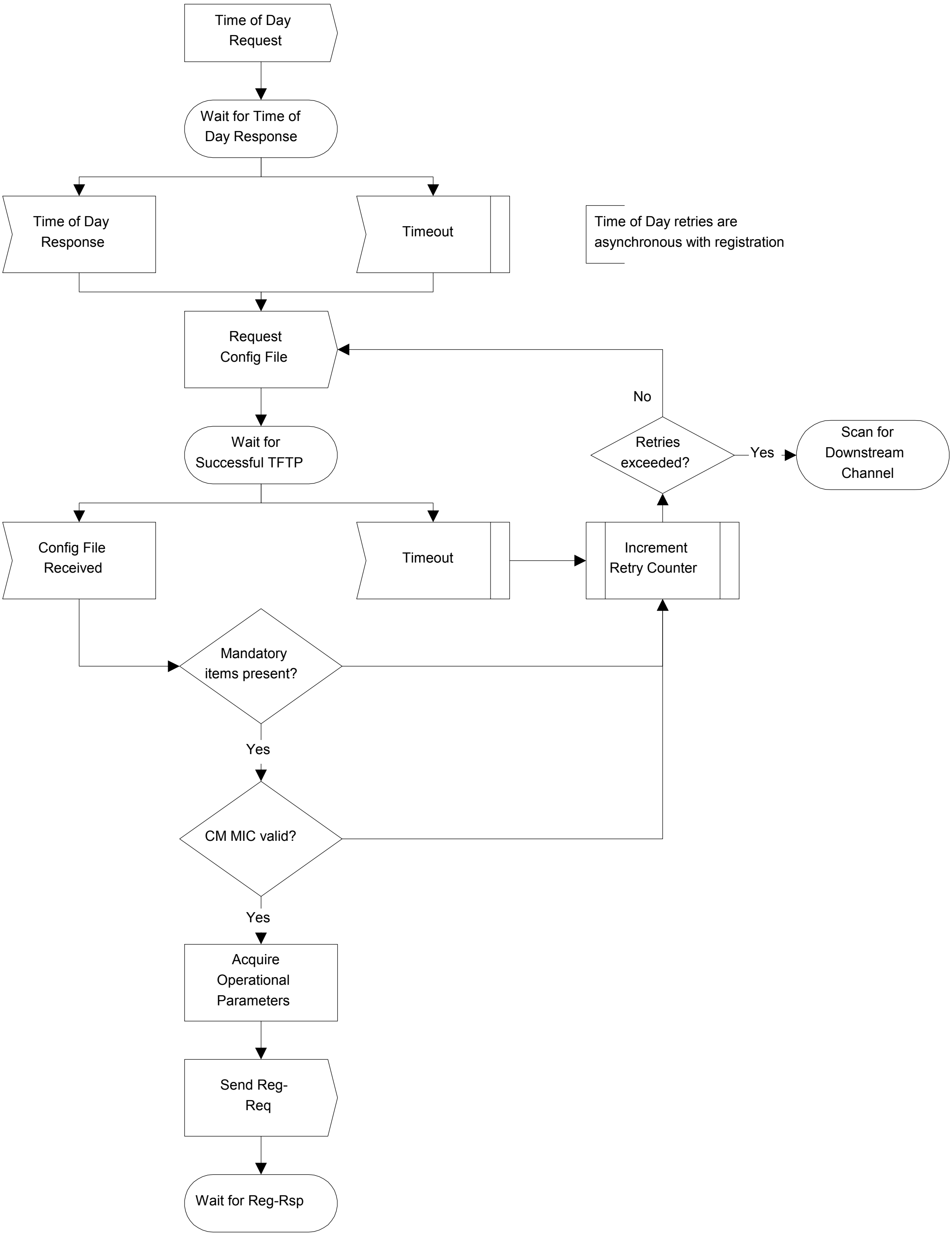


Figure C.11-12/J.112 – Registration – CM

Once the CM has sent a Registration Request to the CMTS it MUST wait for a Registration Response to authorize it to forward traffic to the network. Figure C.11-13 shows the waiting procedure that MUST be followed by the CM.

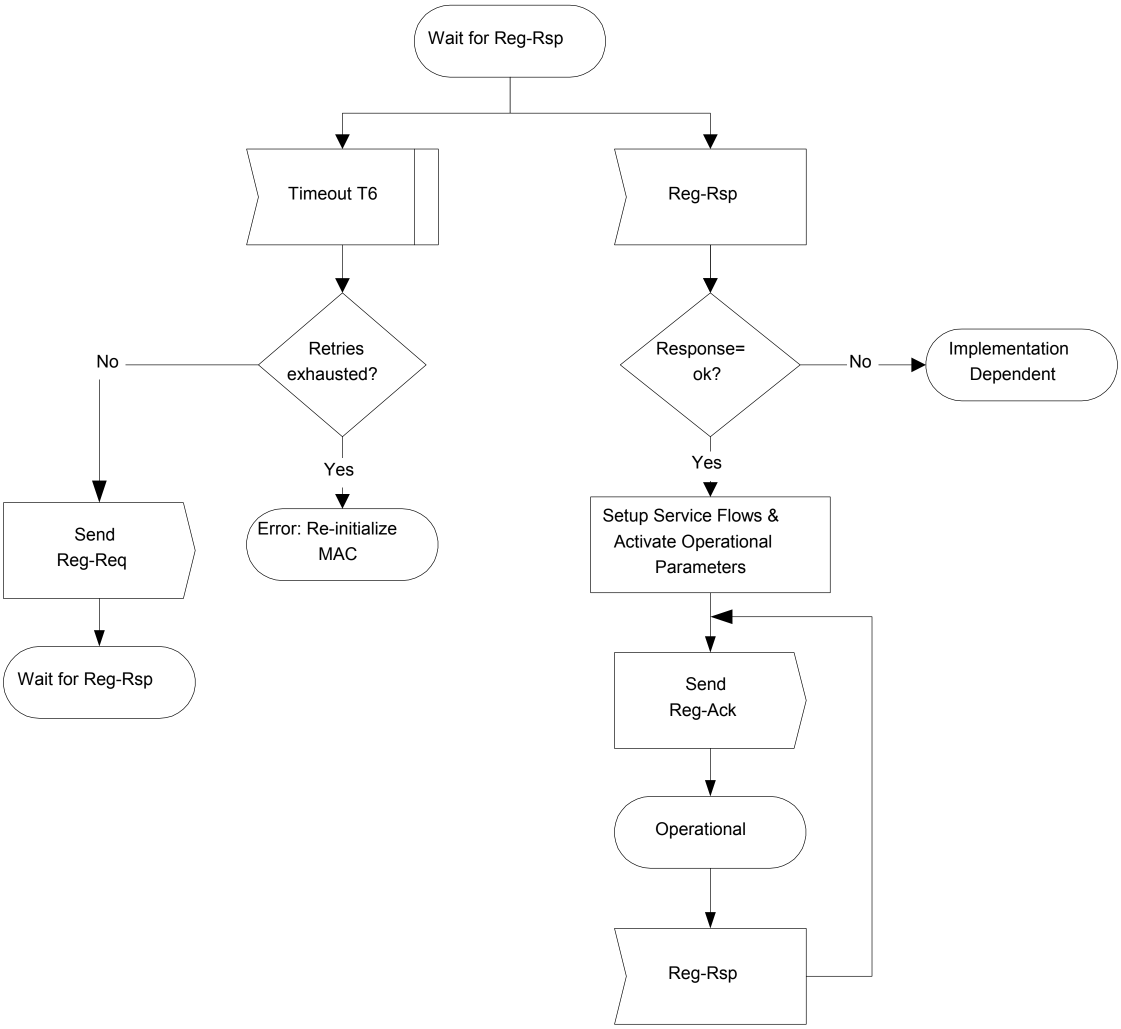


Figure C.11-13/J.112 – Wait for registration response – CM

The CMTS MUST perform the following operations to confirm the CM authorization (refer to Figure C.11-14):

- Calculate a MIC per C.D.3.1 and compare it to the CMTS MIC included in the Registration Request. If the MIC is invalid, the CMTS MUST respond with an Authorization Failure.
- If present, check the TFTP Server Timestamp field. If the CMTS detects that the time is different from its local time by more than CM Configuration Processing Time (refer to Annex C.B), the CMTS MUST indicate authentication failure in the REG-RSP. The CMTS SHOULD also make a log entry stating the CM MAC address from the message.
- If present, check the TFTP Server Provisioned Modem Address field. If the Provisioned Modem Address does not match the requesting modem's actual address, the CMTS MUST indicate authentication failure in the REG-RSP. The CMTS SHOULD also make a log entry stating the CM MAC address from the message.
- If the Registration Request contains Previous Annex C/J.112 Class of Service encodings, verify the availability of the class(es) of service requested. If unable to provide the class(es) of service, the CMTS MUST respond with a Class of Service Failure and the appropriate Service Not Available response code(s). (Refer to C.C.1.3.4.)
- 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 CMTS MUST respond with either a reject-temporary or a reject-permanent (see clause C.C.4) and the appropriate Service Flow Response(s).

- If the Registration Request contains Previous Annex C/J.112 Class of Service encodings and Service Flow encodings, the CMTS MUST respond with a Class of Service Failure and a Service Not Available response code set to 'reject-permanent' for all Previous Annex C/J.112 Classes and Service Flows requested.
- Verify the availability of any Modem Capabilities requested. If unable or unwilling to provide the Modem Capability requested, the CMTS MUST turn that Modem Capability 'off' (refer to C.8.3.8.1.1).
- Assign a Service Flow ID for each class of service supported.
- Reply to the modem in a Registration Response.
- If the Registration Request contains Service Flow encodings, the CMTS MUST wait for a Registration Acknowledgment as shown in Figure C.11-15. If the Registration Request contains Previous Annex C/J.112 Class of Service encodings, the CMTS MUST NOT wait for a Registration Acknowledgment.
- If timer T9 expires, the CMTS MUST both de-assign the temporary SID from that CM and make some provision for aging out that SID.

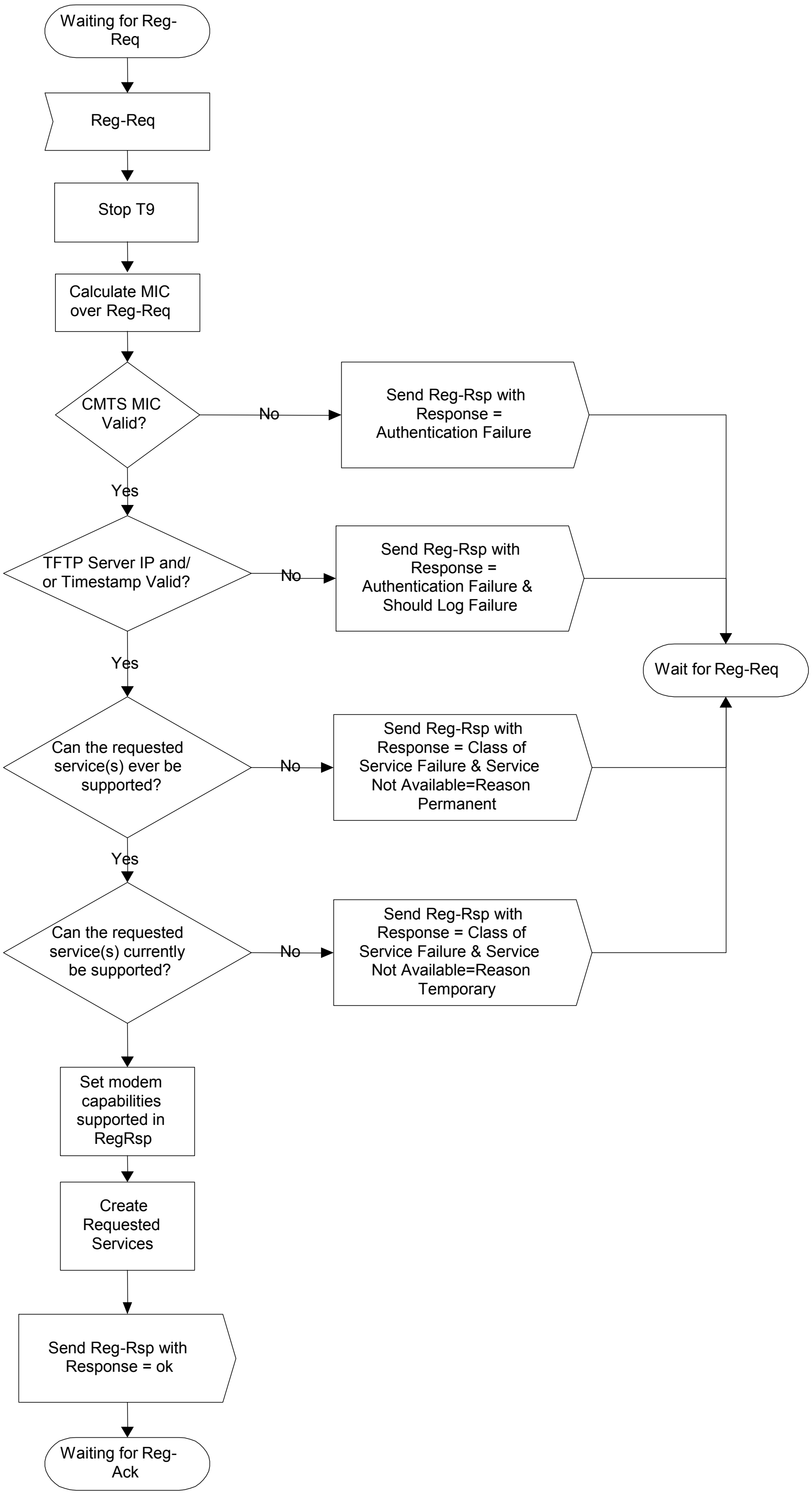

Waiting for Reg-Req
Reg-Req
Stop T9
Calculate MIC over Reg-Req
CMTS MIC Valid?
No
Send Reg-Rsp with Response = Authentication Failure
Yes
TFTP Server IP and/ or Timestamp Valid?
No
Send Reg-Rsp with Response = Authentication Failure & Should Log Failure
Wait for Reg-Req
Yes
Can the requested service(s) 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 C.11-14/J.112 – Registration – CMTS

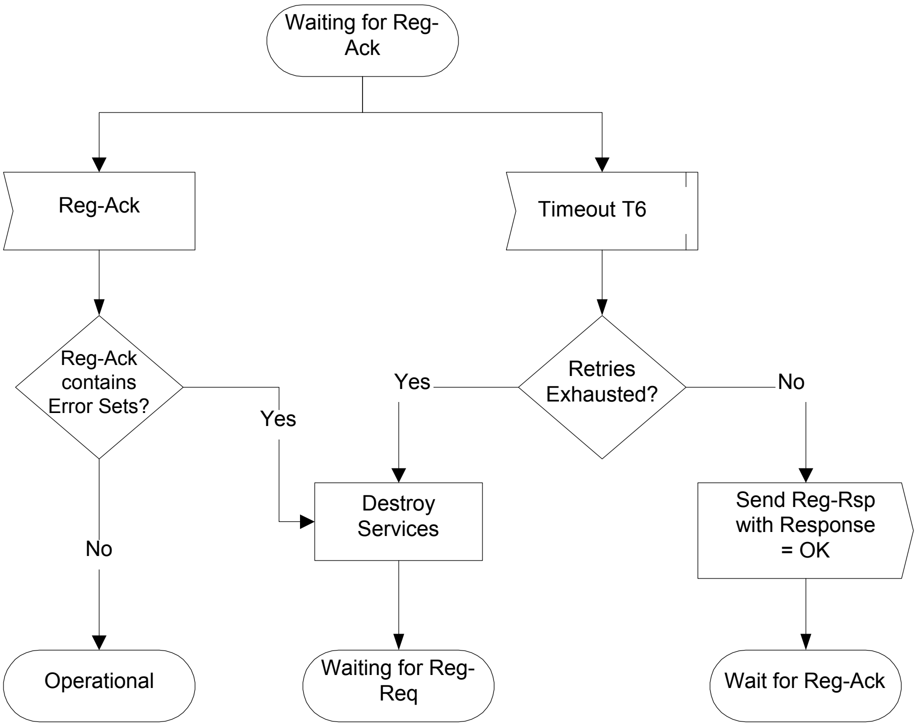


Figure C.11-15/J.112 – Registration acknowledgment – CMTS

C.11.2.10 Baseline privacy initialization

Following registration, if the CM is provisioned to run Baseline Privacy, the CM MAY initialize Baseline Privacy operations, as described in "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I05-000714". A CM is provisioned to run Baseline Privacy if its configuration file includes a Baseline Privacy Configuration Setting (C.C.3.2) and if the Privacy Enable parameter (C.C.1.1.16) is set to enable.

C.11.2.11 Service IDs During CM Initialization

After completion of the Registration process (C.11.2.9), the CM will have been assigned Service Flow IDs (SFIDs) to match its provisioning. However, the CM must complete a number of protocol transactions prior to that time (e.g., Ranging, DHCP, etc.), and requires a temporary Service ID in order to complete those steps.

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

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

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

It is possible that the Ranging Response may be lost after transmission by the CMTS. The CM MUST recover by timing out and re-issuing its Initial Ranging Request. Since the CM is uniquely identified by the source MAC address in the Ranging Request, the CMTS MAY immediately reuse the temporary SID previously assigned. If the CMTS assigns a new temporary SID, it MUST make some provision for aging out the old SID that went unused (see C.8.3.8).

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

C.11.2.12 Multiple-channel support

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

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

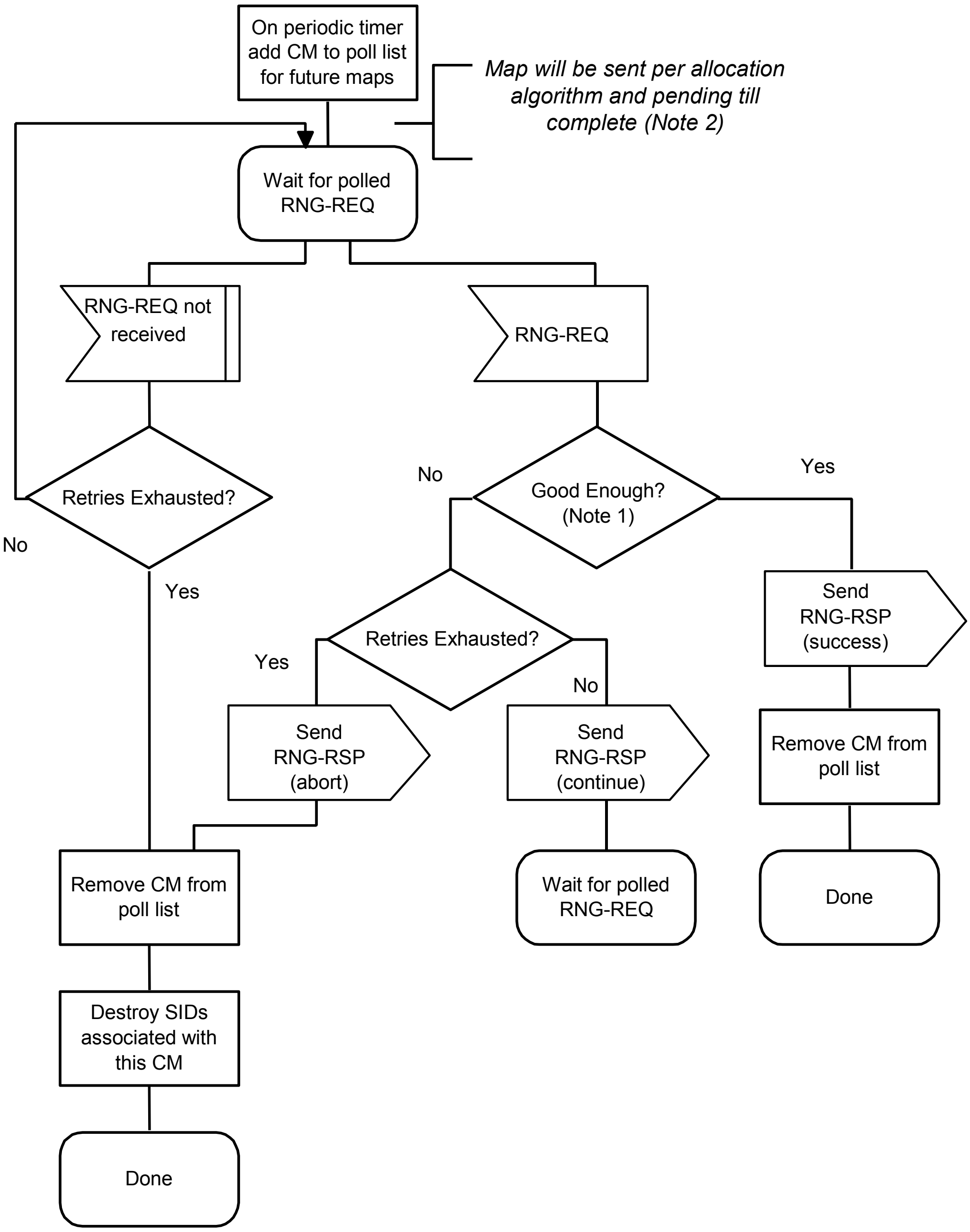
C.11.3 Standard operation

C.11.3.1 Periodic signal level adjustment

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

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

Remote RF signal level adjustment at the CM 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 Figures C.11-16 and C.11-17. On receiving a RNG-RSP, the CM MUST NOT transmit until the RF signal has been adjusted in accordance with the RNG-RSP and has stabilized (refer to clause C.6).



NOTE 1 – Means Ranging Request is within the tolerance limits of the CMTS for power and transmit equalization (if supported).

NOTE 2 – RNG-REQ pending-till-complete was nonzero, the CMTS SHOULD hold off the station maintenance opportunity accordingly unless needed, for example, to adjust the CM's power level. If opportunities are offered prior to the pending-till-complete expiry, the "good-enough" test which follows receipt of a RNG-RSP MUST NOT judge the CM's transmit equalization until pending-till-complete expires.

Figure C.11-16/J.112 – Periodic Ranging – CMTS

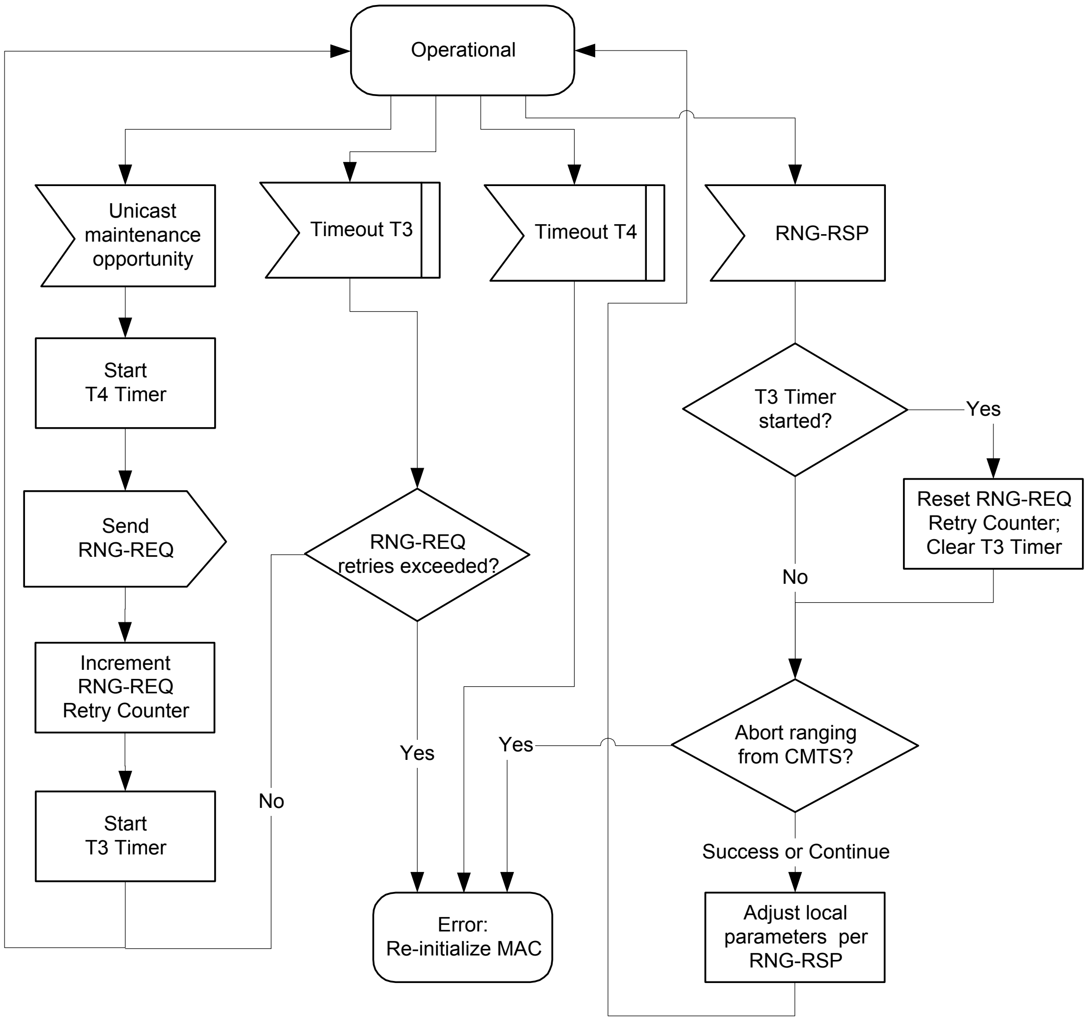


Figure C.11-17/J.112 – Periodic ranging – CM view

C.11.3.2 Changing upstream burst parameters

Whenever the CMTS is to change any of the upstream burst characteristics, it must provide for an orderly transition from the old values to the new values by all CMs. Whenever the CMTS is to change any of the upstream burst values, it MUST announce the new values in an Upstream Channel Descriptor message, and the Configuration Change Count field MUST be incremented to indicate that a value has changed.

After transmitting one or more UCD messages with the new value, the CMTS transmits a MAP message with a UCD Count matching the new Configuration Change Count. The first interval in the MAP MUST be a data grant of at least 1 ms to the null Service ID (zero). That is, the CMTS MUST allow one millisecond for cable modems to change their PMD sublayer parameters to match the new set. This millisecond is in addition to other MAP timing constraints (see C.9.1.5).

The CMTS MUST NOT transmit MAPs with the old UCD Count after transmitting the new UCD.

The CM MUST use the parameters from the UCD corresponding to the MAP's "UCD Count" for any transmissions it makes in response to that MAP. If the CM has, for any reason, not received the corresponding UCD, it cannot transmit during the interval described by that MAP.

C.11.3.3 Changing upstream channels

At any time after registration, the CMTS may direct the CM to change its upstream channel. This may be done for traffic balancing, noise avoidance, or any of a number of other reasons which are beyond the scope of this annex. Figure C.11-18 shows the procedure that MUST be followed by the CMTS. Figure C.11-19 shows the corresponding procedure at the CM.

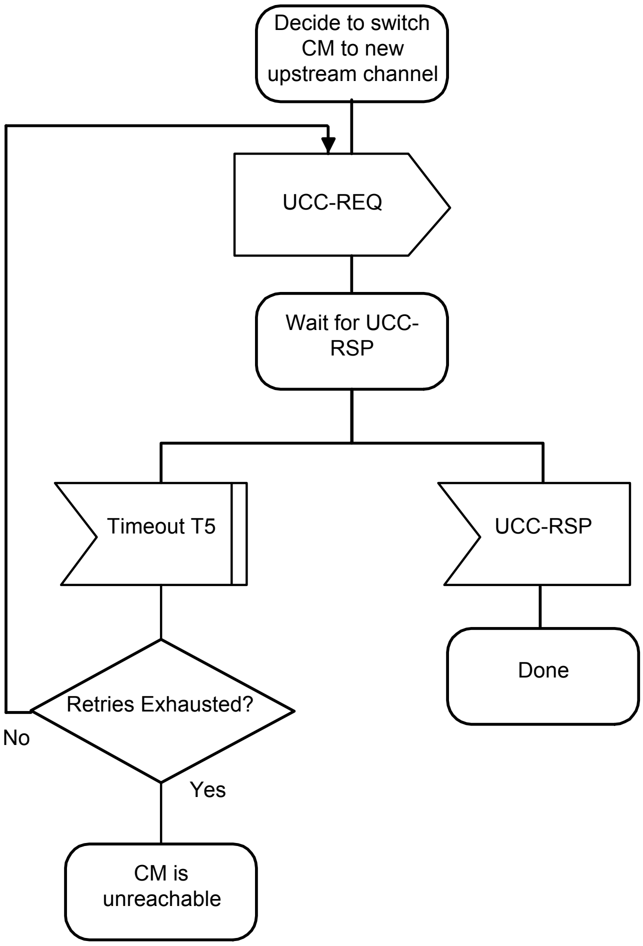


Figure C.11-18/J.112 – Changing upstream channels: CMTS view

Note that if the CMTS retries the UCC-REQ, the CM may have already changed channels (if the UCC-RSP was lost in transit). Consequently, the CMTS MUST listen for the UCC-RSP on both the old and the new channels.

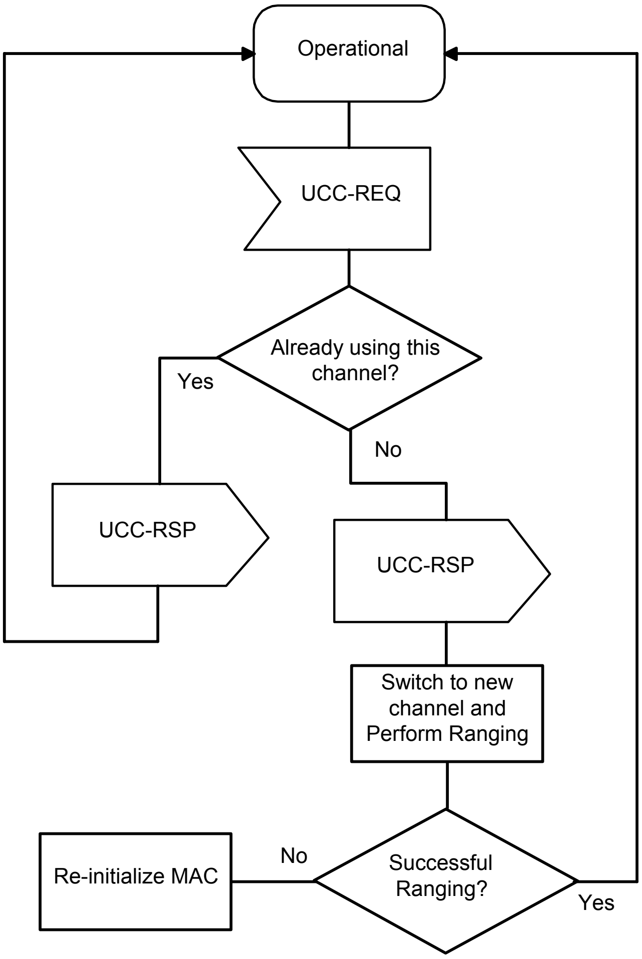


Figure C.11-19/J.112 – Changing upstream channels: CM view

Upon synchronizing with the new upstream channel, the CM MUST re-range using the technique specified in the UCC-REQ Ranging Technique TLV, if present. If this TLV is not present in the UCC-REQ, the CM MUST perform initial maintenance on the new upstream channel. (Refer to C.8.3.10.1.1.)

If the CM has previously established ranging on the new channel, and if that ranging on that channel is still current (T4 has not elapsed since the last successful ranging), then the CM MAY use cached ranging information and omit ranging.

The CM SHOULD cache UCD information from multiple upstream channels to eliminate waiting for a UCD corresponding to the new upstream channel.

The CM MUST NOT perform reregistration, since its provisioning and MAC domain remain valid on the new channel.

C.11.4 Dynamic service

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 C.11-20.

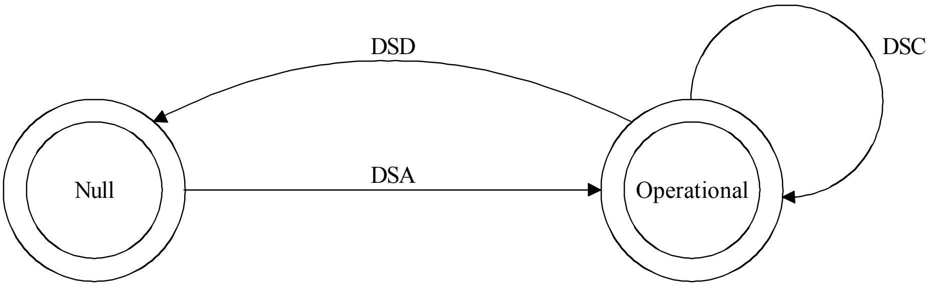


Figure C.11-20/J.112 – Dynamic service flow overview

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

Service Flows created at registration time effectively enter the SF_operational state without a DSA transaction.

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

Each dynamic service message sequence is a unique transaction with an associated unique transaction identifier. The DSA/DSC transactions consist of a request/response/acknowledge sequence. The DSD transactions consist of a request/response sequence. The response messages MUST contain a confirmation code of okay unless some exception condition was detected. The acknowledge messages MUST include 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 clauses.

C.11.4.1 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 Signalling. 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 CMTS and CM. In the Dynamic Service Flow Changing-Local state, there is a subtle difference in the CM and CMTS behaviors. This is called out in the state transition and detailed flow diagrams.

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

The inputs for the state diagrams are identified below.

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

- add;
- change;
- delete.

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

- DSA Succeeded;
- DSA Failed;
- DSA ACK Lost;
- DSA Erred;
- DSA Ended;
- DSC Succeeded;
- DSC Failed;

DSC ACK Lost;

- DSC Erred;
- DSC Ended;
- DSD Succeeded;
- DSD Erred;
- DSD Ended.

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

- SF Add;
- SF Change;
- SF Delete;
- SF Abort Add;
- SF Change-Remote;

- SF Delete-Local;
- SF Delete-Remote;
- SF DSA-ACK Lost;
- SF-DSC-REQ Lost;
- SF-DSC-ACK Lost;
- SF DSD-REQ Lost;
- SF Changed;
- 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.

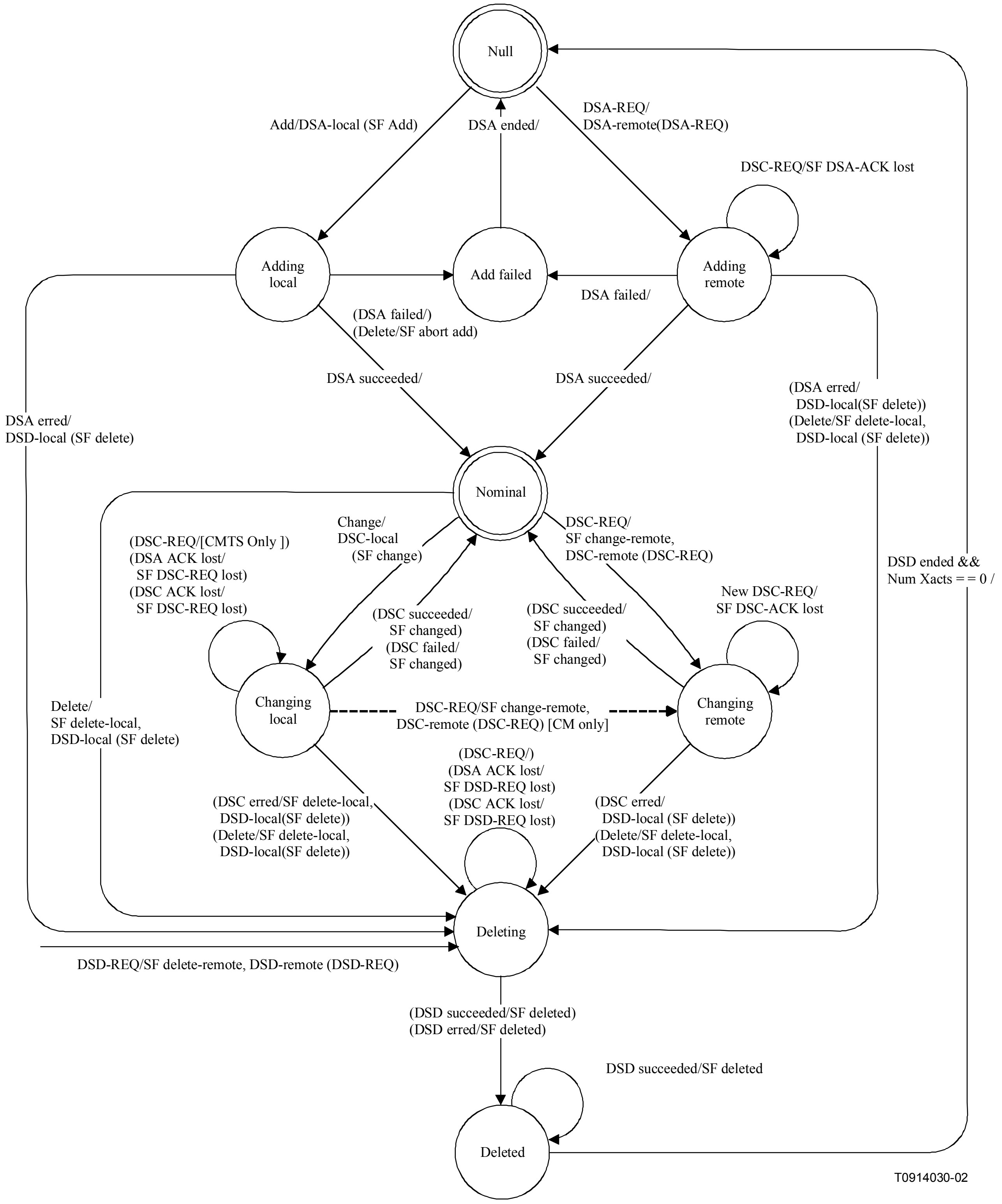


Figure C.11-21/J.112 – Dynamic service flow state transition diagram

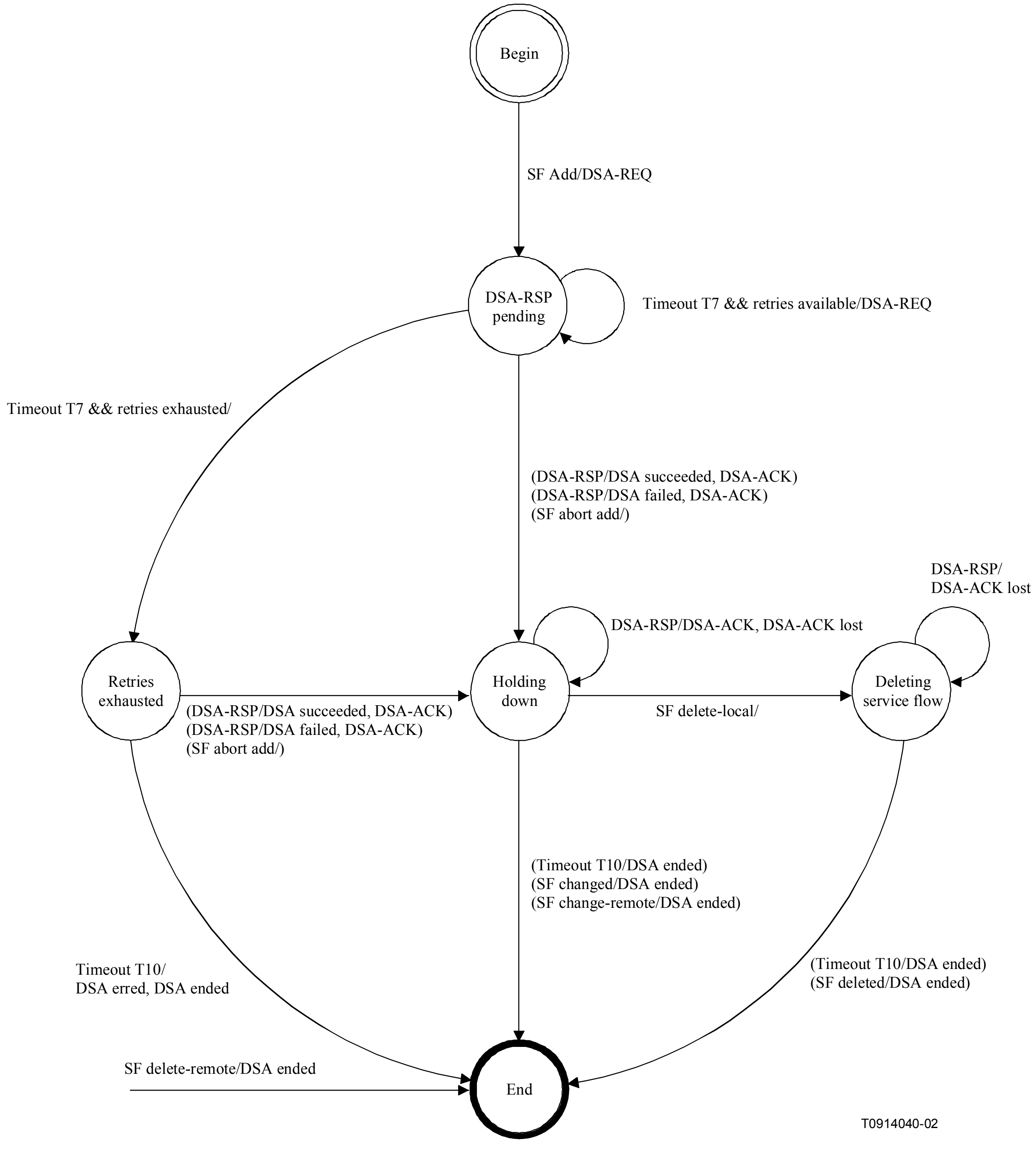


Figure C.11-22/J.112 – DSA – Locally initiated transaction state transition diagram

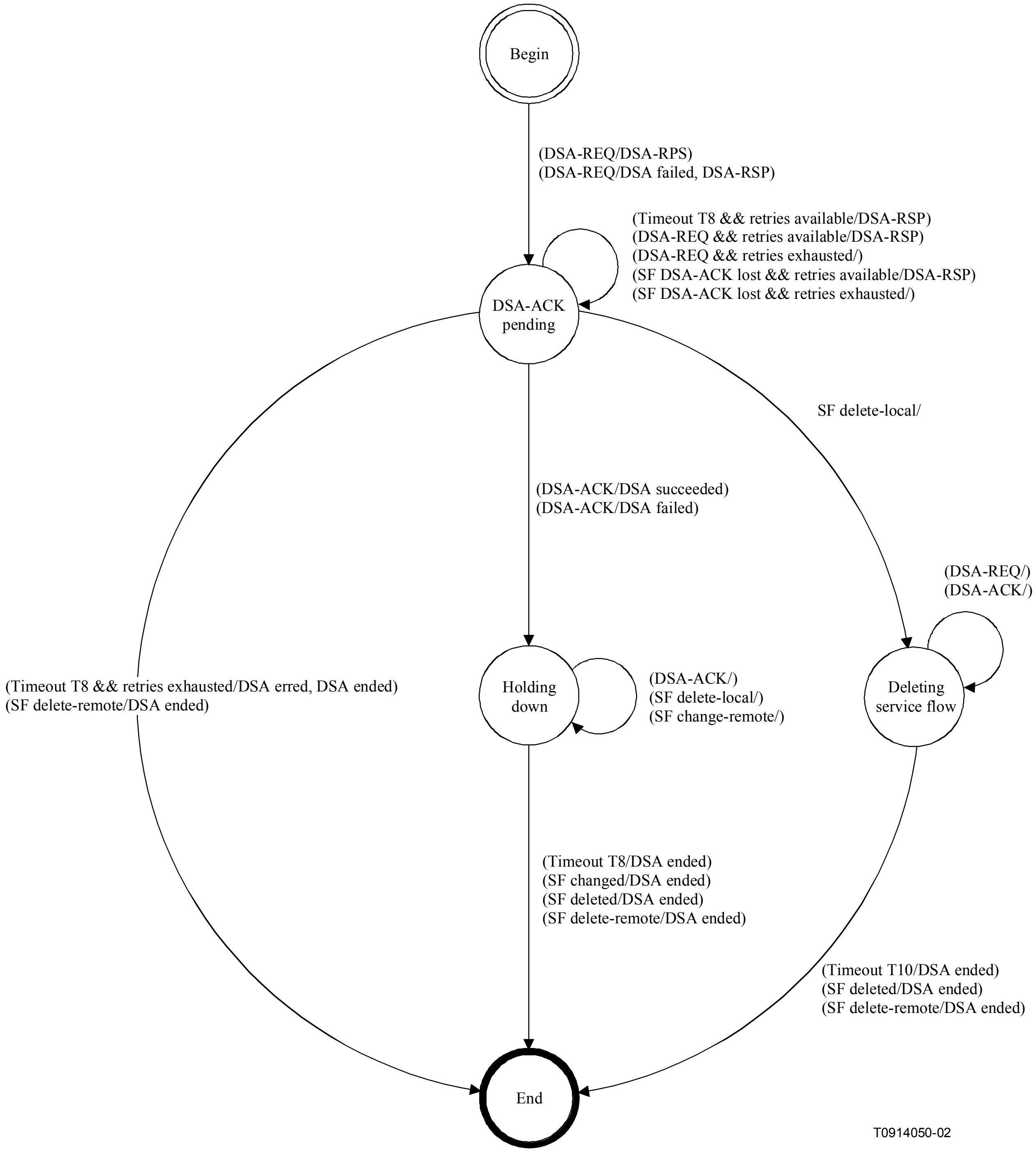

Begin
(DSA-REQ/DSA-RPS)
(DSA-REQ/DSA failed, DSA-RSP)
(Timeout T8 && retries available/DSA-RSP)
(DSA-REQ && retries available/DSA-RSP)
(DSA-REQ && retries exhausted/)
(SF DSA-ACK lost && retries available/DSA-RSP)
(SF DSA-ACK lost && retries exhausted/)
DSA-ACK pending
SF delete-local/
(DSA-ACK/DSA succeeded)
(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
T0914050-02

Figure C.11-23/J.112 – DSA – Remotely initiated transaction state transition diagram

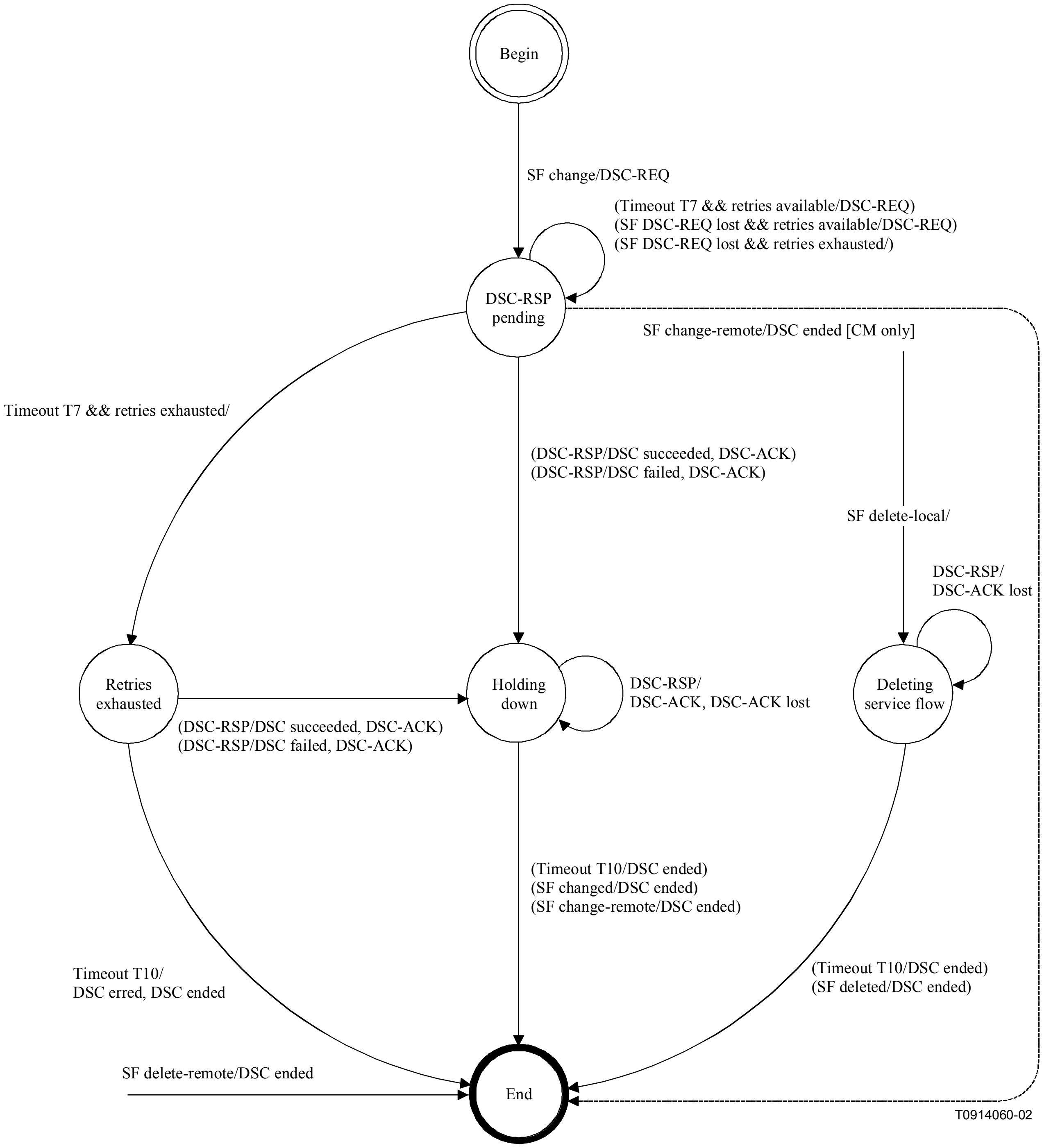

Begin
SF change/DSC-REQ
(Timeout T7 && retries available/DSC-REQ)
(SF DSC-REQ lost && retries available/DSC-REQ)
(SF DSC-REQ lost && retries exhausted/)
DSC-RSP pending
SF change-remote/DSC ended [CM only]
Timeout T7 && retries exhausted/
(DSC-RSP/DSC succeeded, DSC-ACK)
(DSC-RSP/DSC failed, DSC-ACK)
SF delete-local/
DSC-RSP/
DSC-ACK lost
Retries exhausted
Holding down
DSC-RSP/
DSC-ACK, DSC-ACK lost
Deleting service flow
(DSC-RSP/DSC succeeded, DSC-ACK)
(DSC-RSP/DSC failed, DSC-ACK)
(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
T0914060-02

Figure C.11-24/J.112 – DSC – Locally initiated transaction state transition diagram

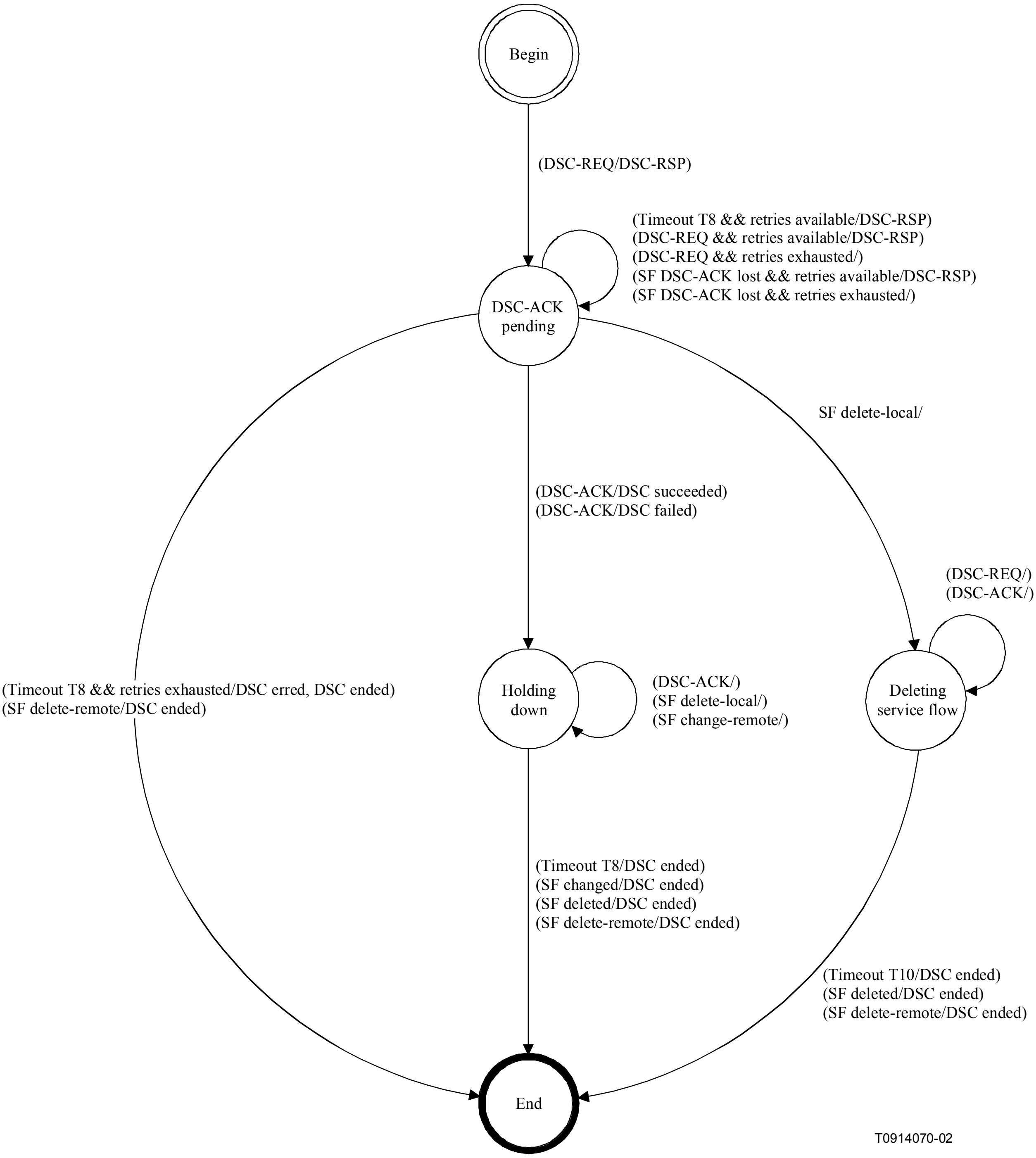

Begin
(DSC-REQ/DSC-RSP)
(Timeout T8 && retries available/DSC-RSP)
(DSC-REQ && retries available/DSC-RSP)
(DSC-REQ && retries exhausted/)
(SF DSC-ACK lost && retries available/DSC-RSP)
(SF DSC-ACK lost && retries exhausted/)
DSC-ACK pending
SF delete-local/
(DSC-ACK/DSC succeeded)
(DSC-ACK/DSC failed)
(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
T0914070-02

Figure C.11-25/J.112 – DSC – Remotely initiated transaction state transition diagram

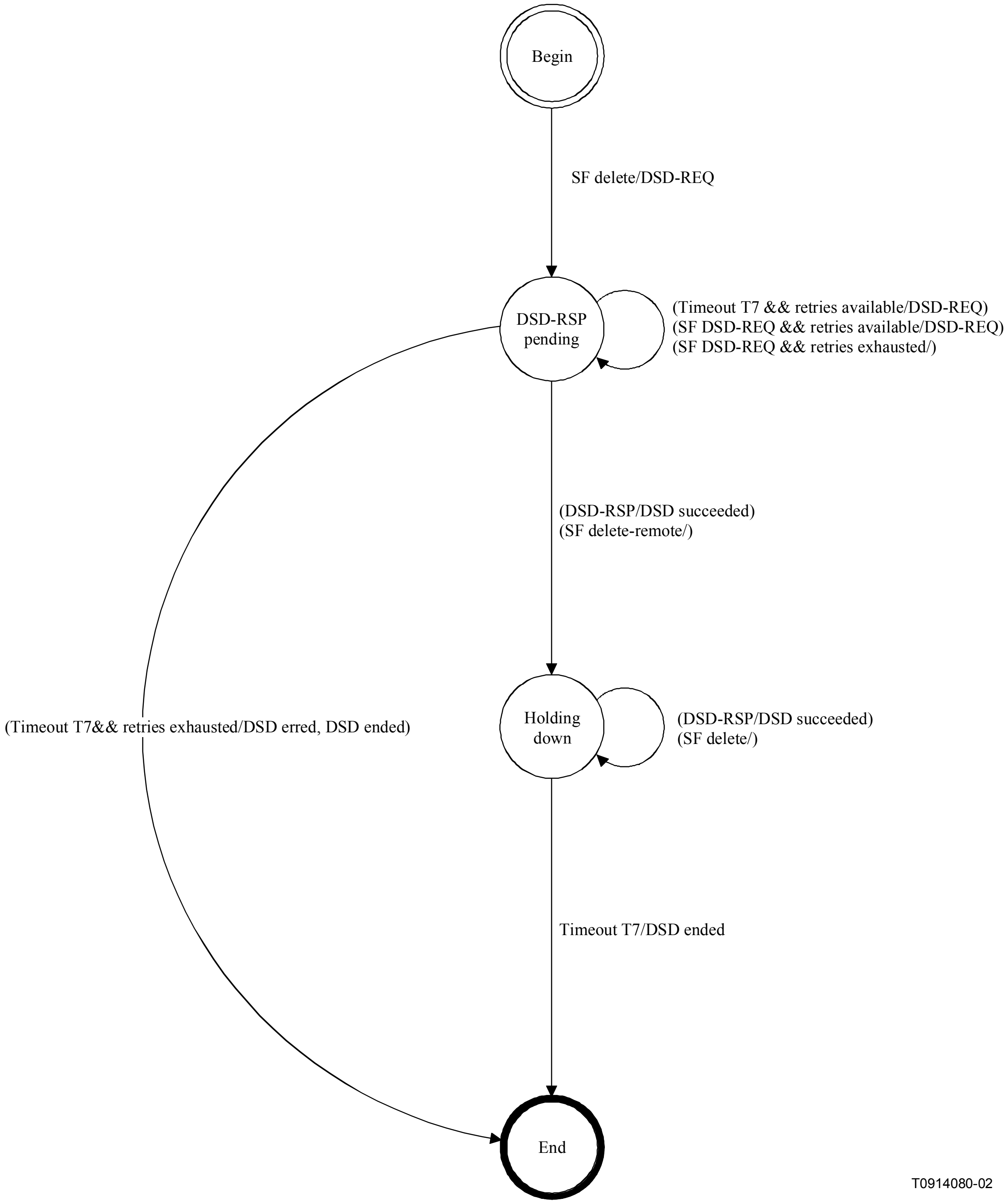

Begin
SF delete/DSD-REQ
DSD-RSP pending
(Timeout T7 && retries available/DSD-REQ)
(SF DSD-REQ && retries available/DSD-REQ)
(SF DSD-REQ && retries exhausted/)
(DSD-RSP/DSD succeeded)
(SF delete-remote/)
(Timeout T7&& retries exhausted/DSD erred, DSD ended)
Holding down
(DSD-RSP/DSD succeeded)
(SF delete/)
Timeout T7/DSD ended
End
T0914080-02

Figure C.11-26/J.112 – DSD – Locally initiated transaction state transition diagram

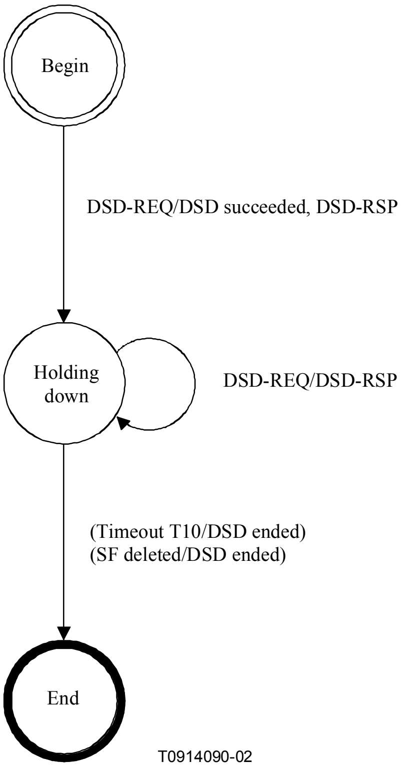


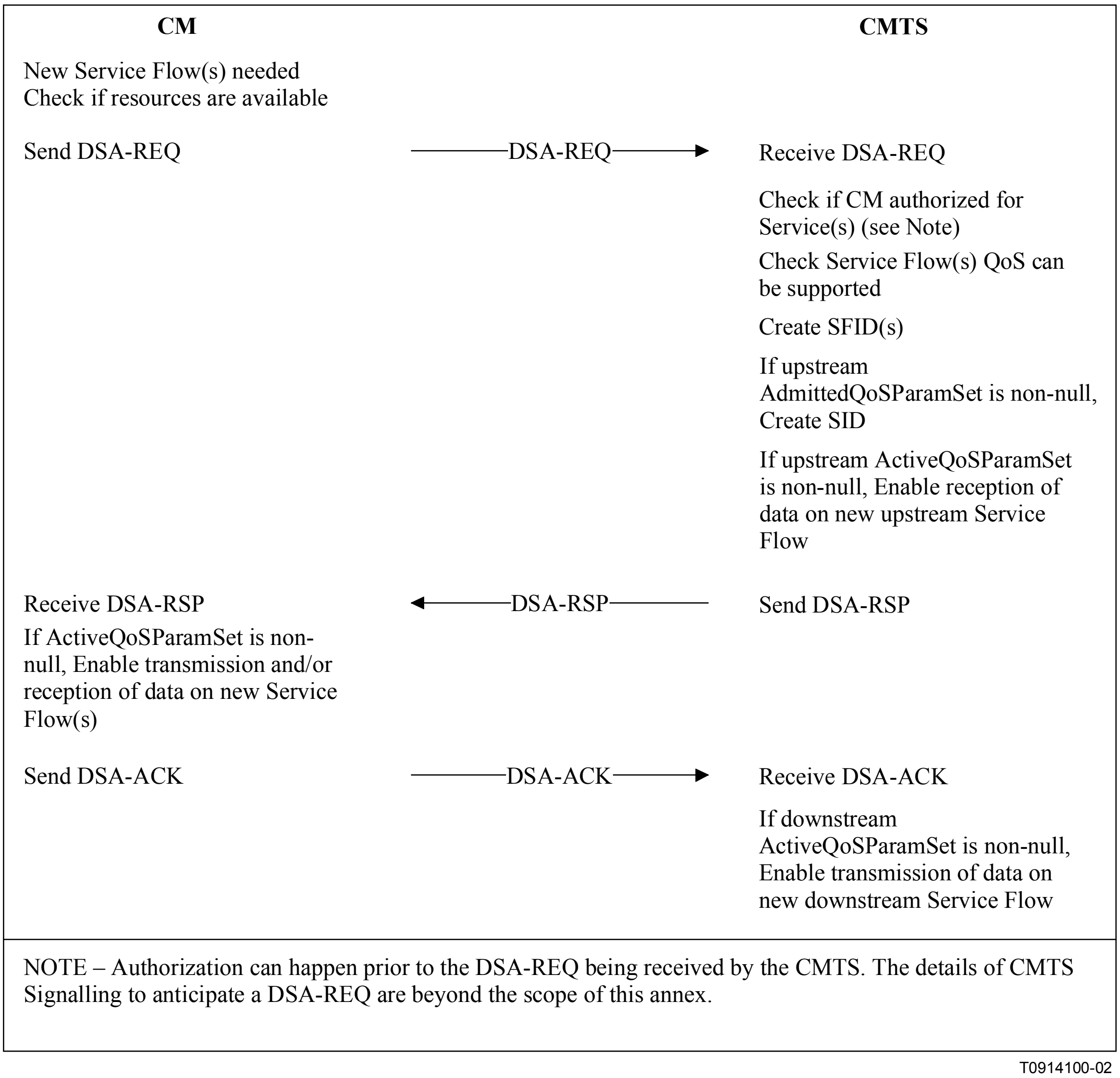
Figure C.11-27/J.112 – Dynamic Deletion (DSD) – Remotely initiated transaction state transition diagram

C.11.4.2 Dynamic service addition

C.11.4.2.1 CM initiated dynamic service addition

A CM wishing to create an upstream and/or a downstream Service Flow sends a request to the CMTS using a dynamic service addition request message (DSA-REQ). The CMTS checks the CM'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 CM 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.

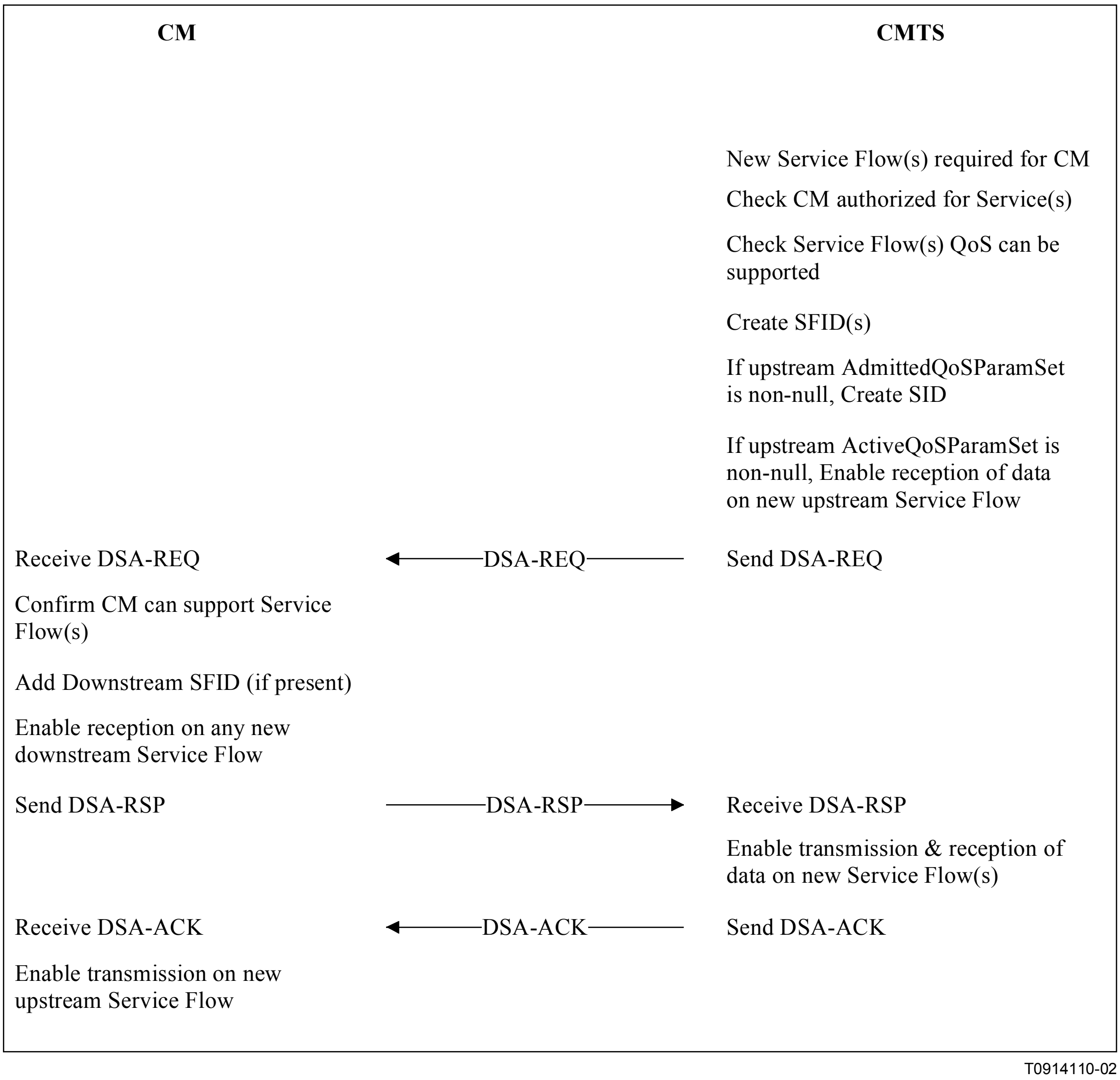

CM
CMTS
New Service Flow(s) needed
Check if resources are available
Send DSA-REQ
DSA-REQ
Receive DSA-REQ
Check if CM authorized for Service(s) (see Note)
Check Service Flow(s) QoS can be supported
Create SFID(s)
If upstream AdmittedQoSParamSet is non-null, Create SID
If upstream ActiveQoSParamSet is 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
T0914100-02

NOTE – Authorization can happen prior to the DSA-REQ being received by the CMTS. The details of CMTS Signalling to anticipate a DSA-REQ are beyond the scope of this annex.

Figure C.11-28/J.112 – Dynamic service addition initiated from CM

C.11.4.2.2 CMTS initiated dynamic service addition

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



CM		CMTS
		New Service Flow(s) required for CM
		Check CM authorized for Service(s)
		Check Service Flow(s) QoS can be supported
		Create SFID(s)
		If upstream AdmittedQoSParamSet is non-null, Create SID
		If upstream ActiveQoSParamSet is non-null, Enable reception of data on new upstream Service Flow
Receive DSA-REQ	◄——DSA-REQ——	Send DSA-REQ
Confirm CM 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		

T0914110-02

Figure C.11-29/J.112 – Dynamic service addition initiated from CMTS

C.11.4.2.3 Dynamic service addition state transition diagrams

See Figures C.11-30 to C.11-38.

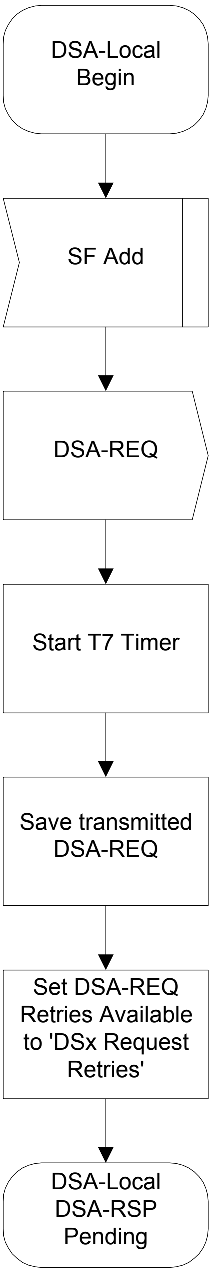

DSA-Local Begin
SF Add
DSA-REQ
Start T7 Timer
Save transmitted DSA-REQ
Set DSA-REQ Retries Available to 'DSx Request Retries'
DSA-Local DSA-RSP Pending

Figure C.11-30/J.112 – DSA – Locally initiated transaction begin state flow diagram

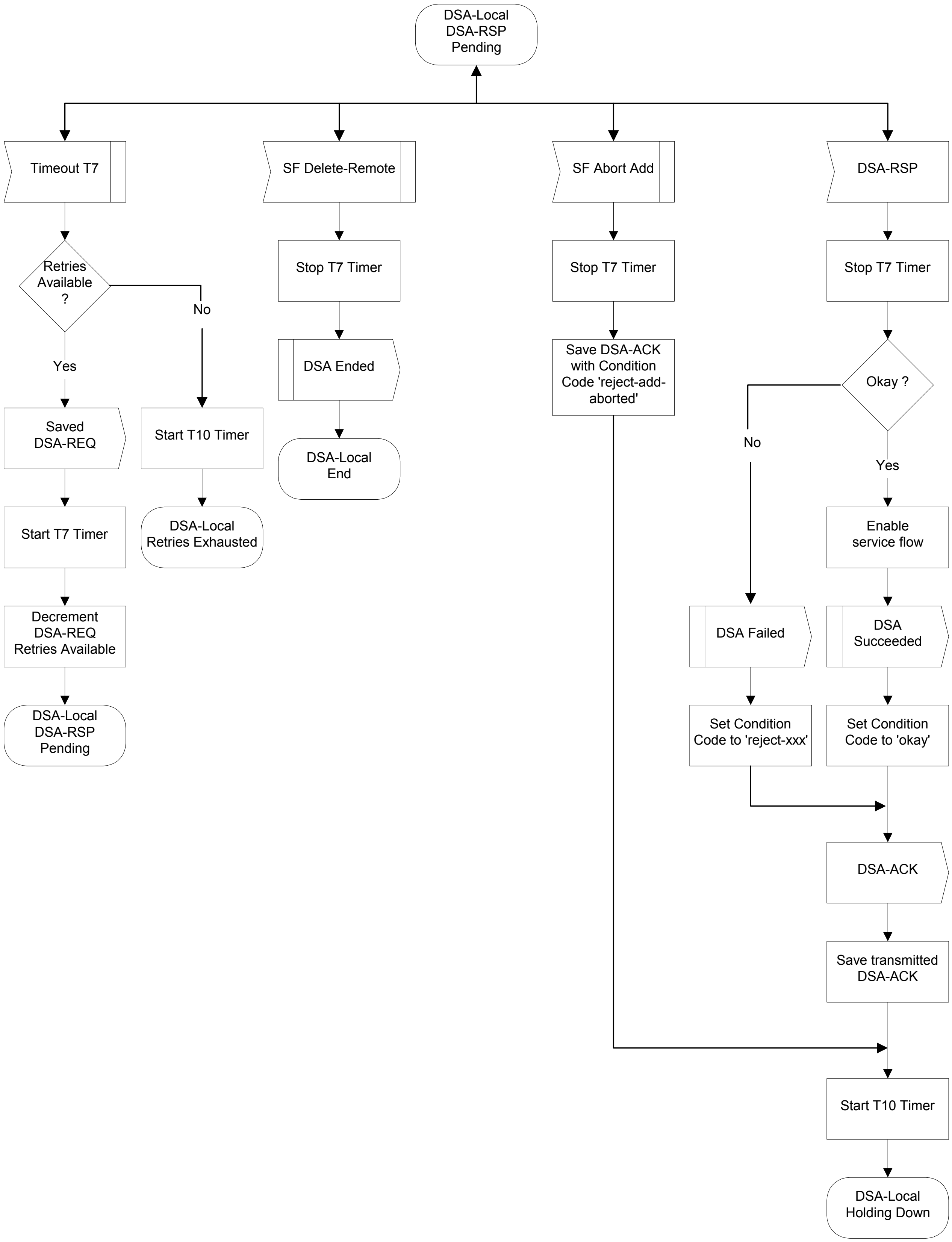


Figure C.11-31/J.112 – DSA – Locally initiated transaction DSA-RSP pending state flow diagram

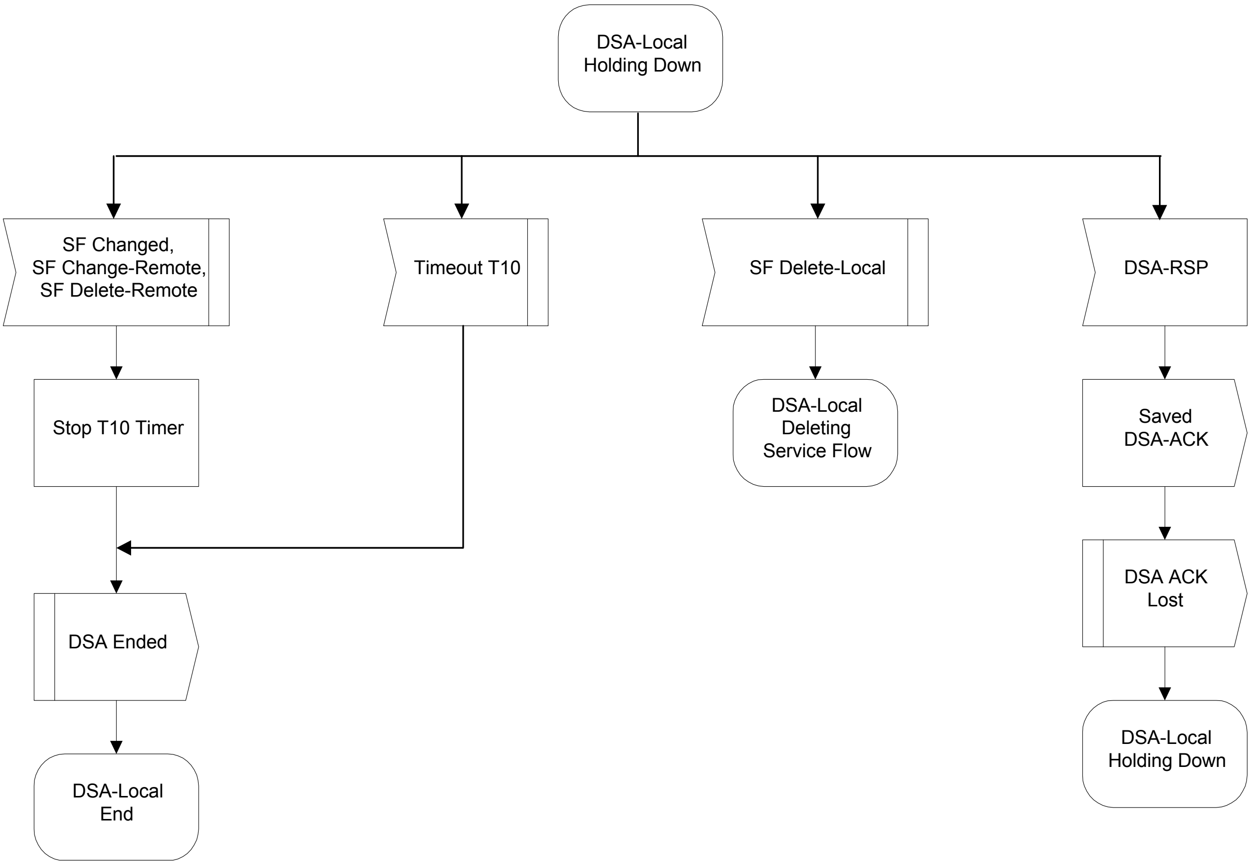


Figure C.11-32/J.112 – DSA – Locally initiated transaction holding state flow diagram

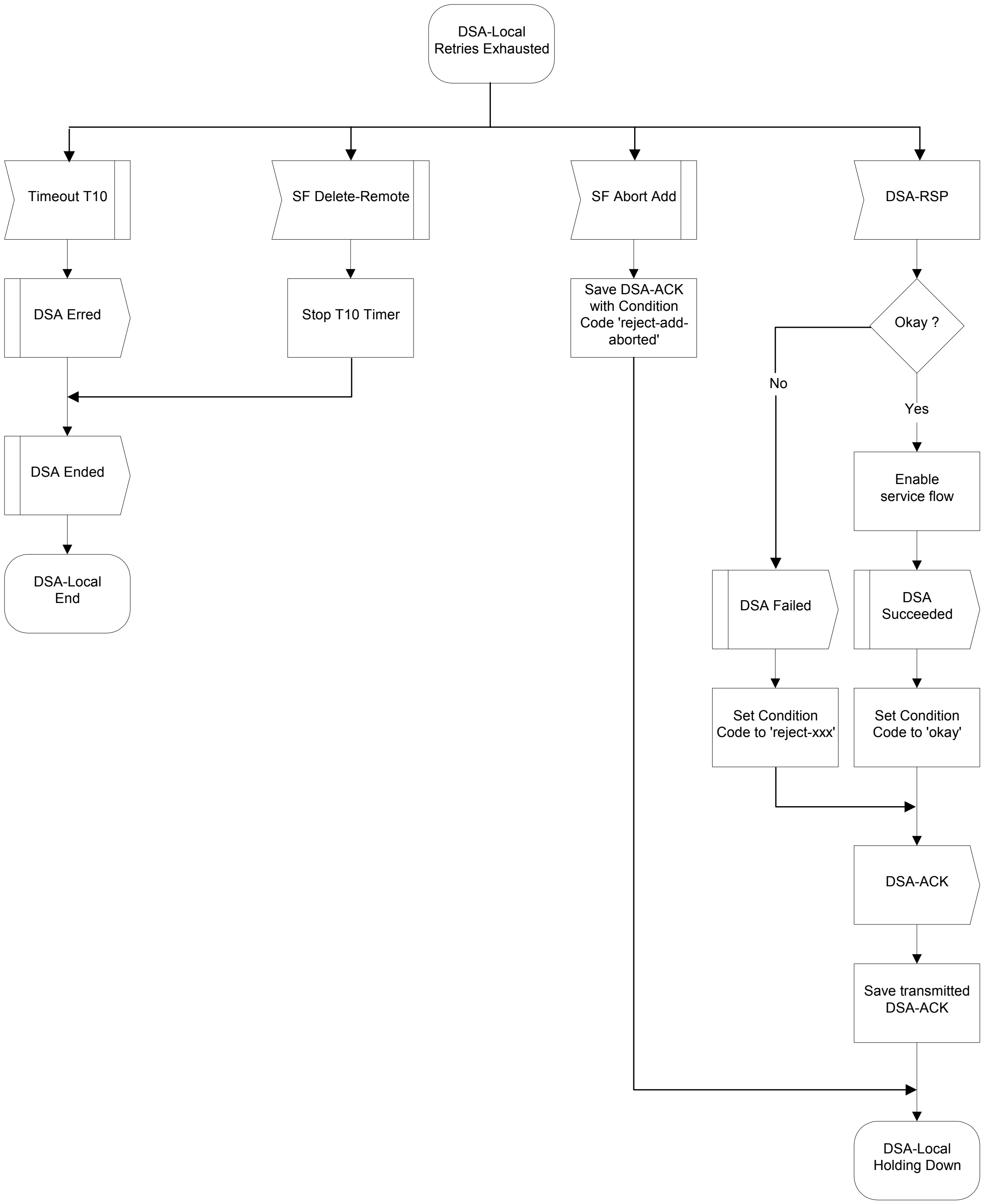


Figure C.11-33/J.112 – DSA – Locally initiated transaction retries exhausted state flow diagram

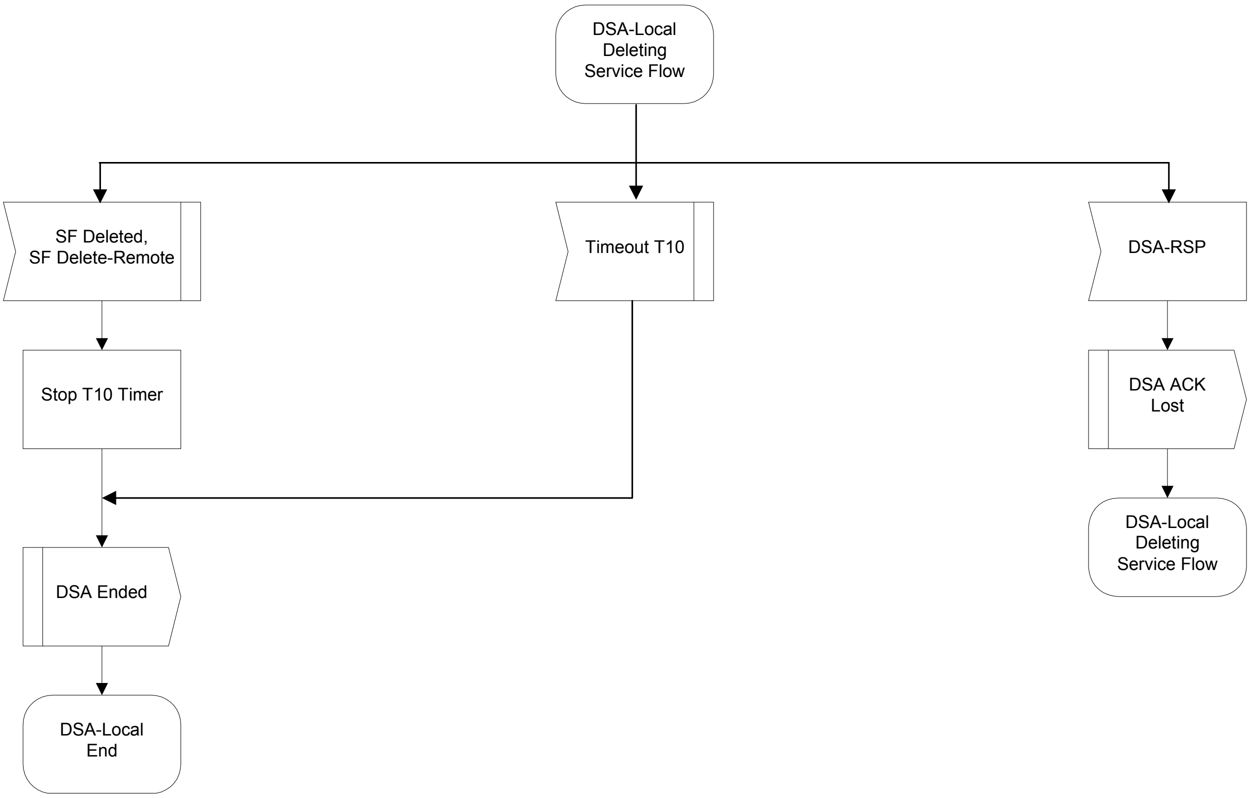

DSA-Local Deleting Service Flow
SF Deleted, SF Delete-Remote
Timeout T10
DSA-RSP
Stop T10 Timer
DSA ACK Lost
DSA-Local Deleting Service Flow
DSA Ended
DSA-Local End

Figure C.11-34/J.112 – DSA – Locally initiated transaction deleting service flow state flow diagram

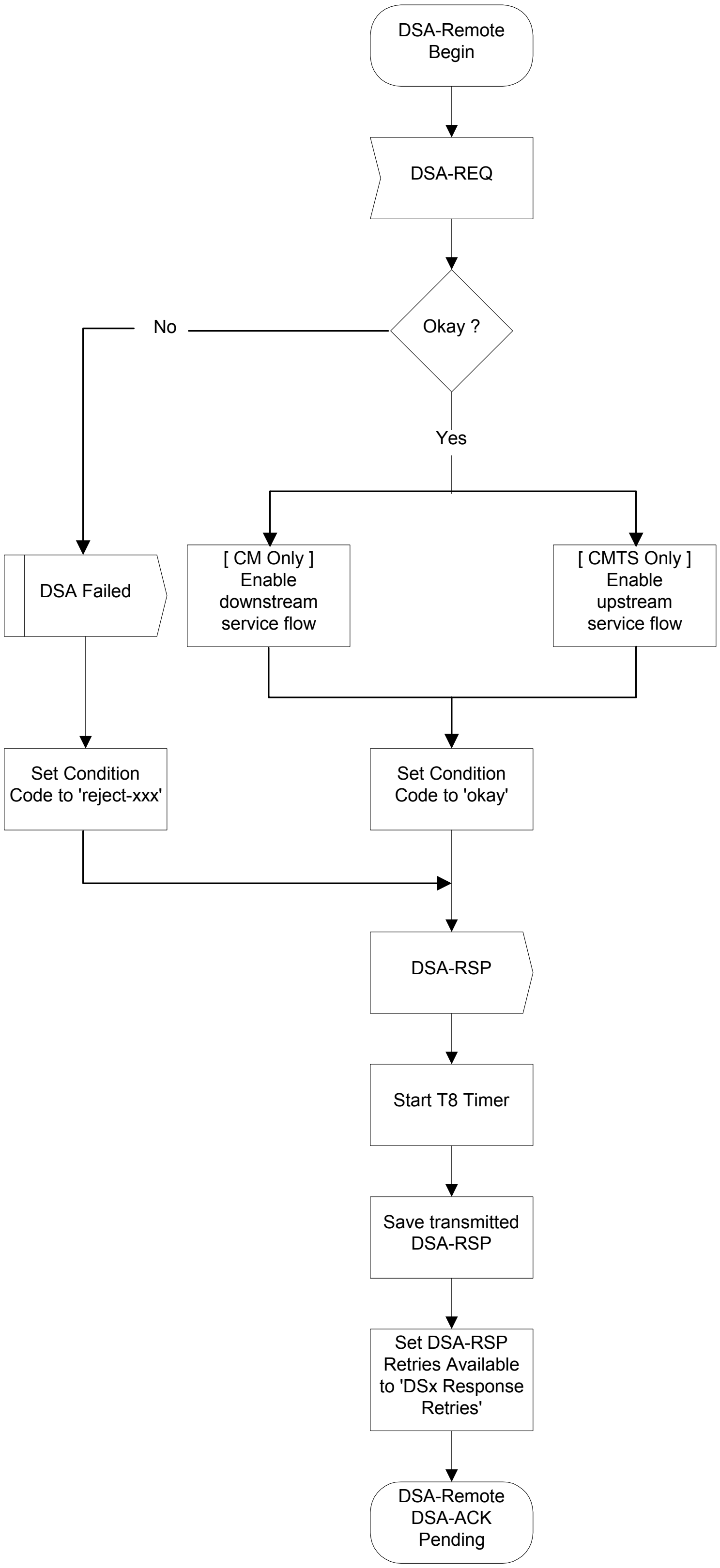

DSA-Remote Begin
DSA-REQ
Okay ?
No
Yes
DSA Failed
[CM Only] Enable downstream service flow
[CMTS Only] Enable upstream service flow
Set Condition Code to 'reject-xxx'
Set Condition Code to 'okay'
DSA-RSP
Start T8 Timer
Save transmitted DSA-RSP
Set DSA-RSP Retries Available to 'DSx Response Retries'
DSA-Remote DSA-ACK Pending

Figure C.11-35/J.112 – DSA – Remotely initiated transaction begin state flow diagram

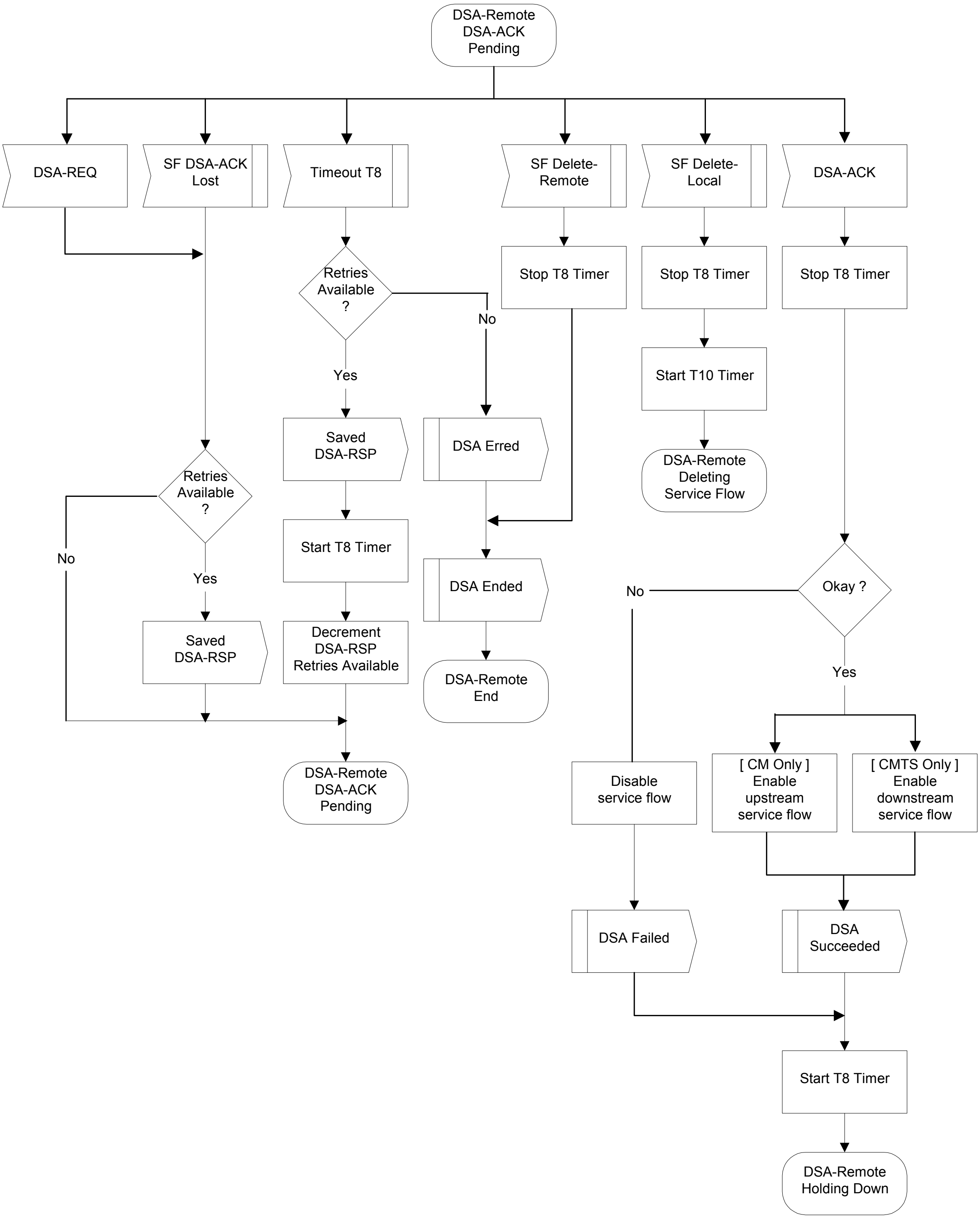


Figure C.11-36/J.112 – DSA – Remotely initiated transaction DSA-ACK pending state flow diagram

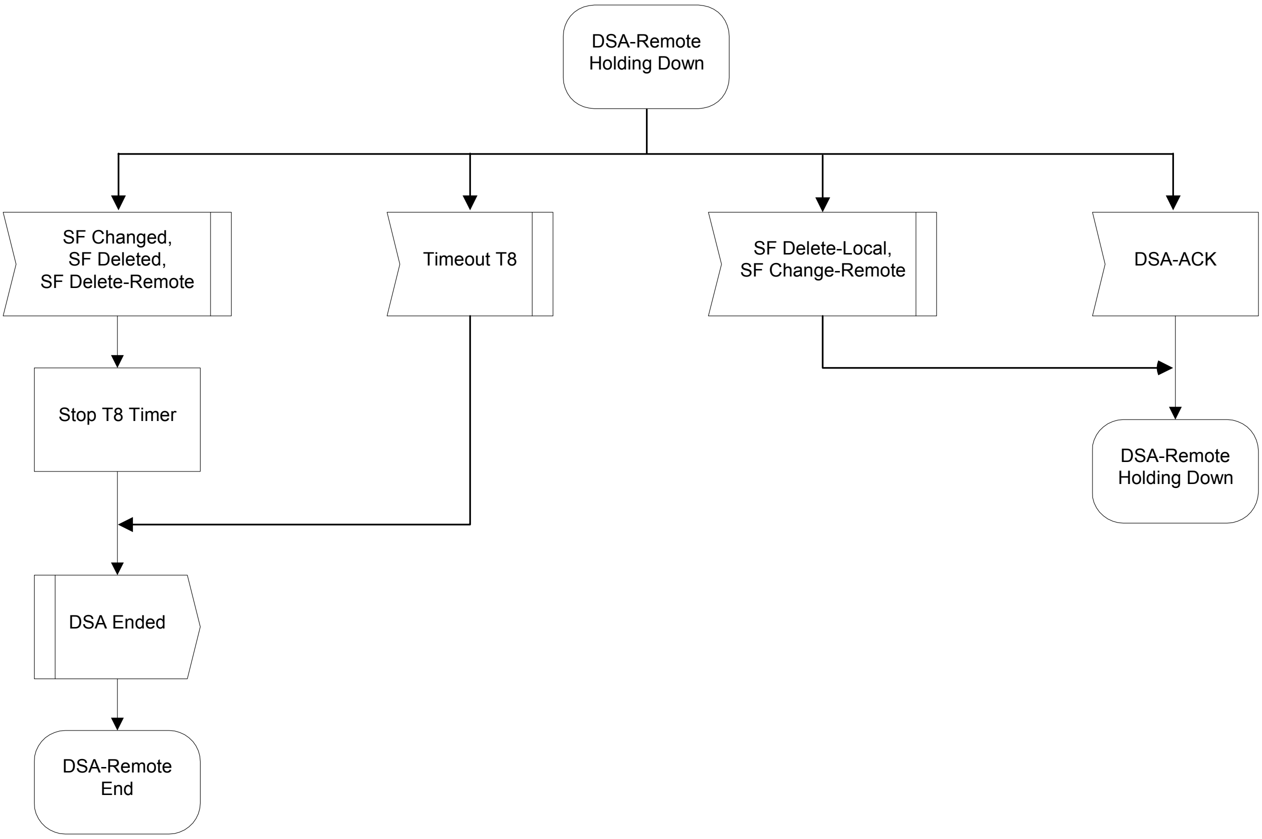


Figure C.11-37/J.112 – DSA – Remotely initiated transaction holding down state flow diagram

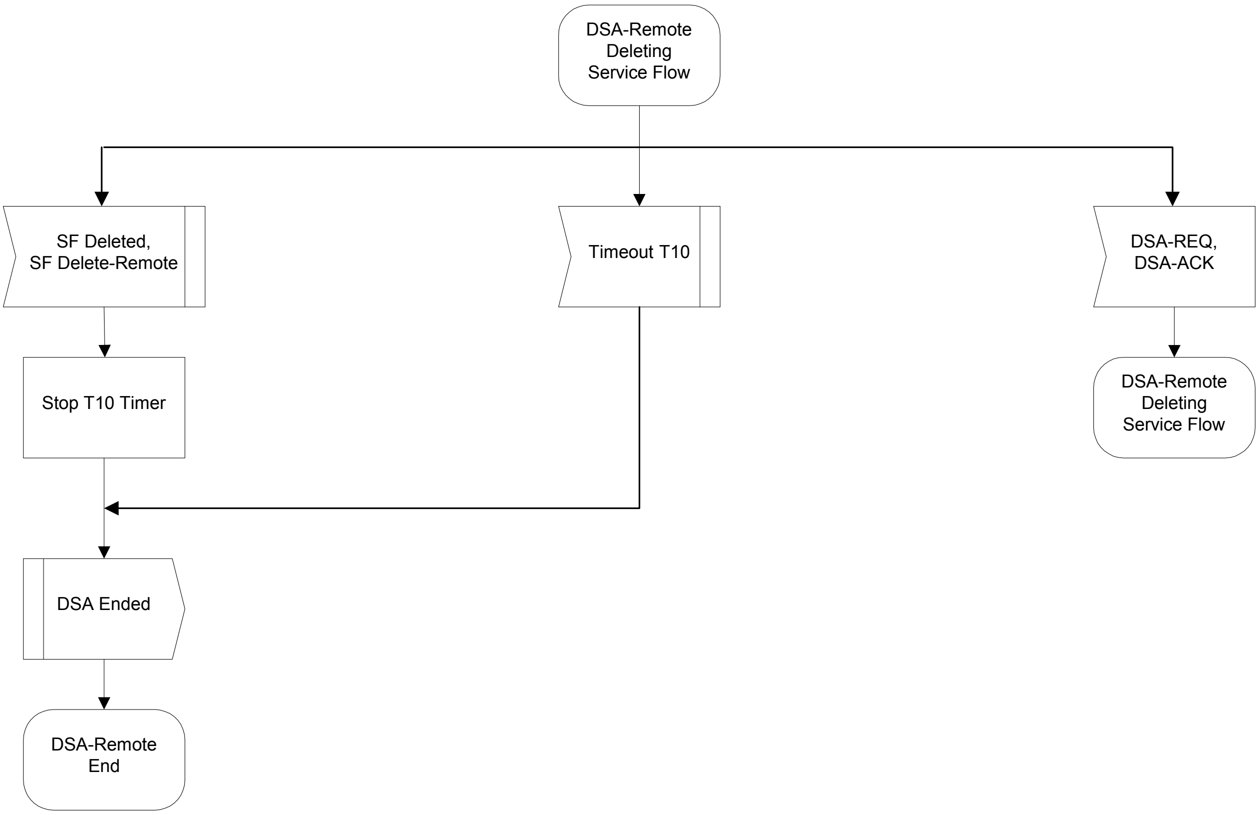

DSA-Remote Deleting Service Flow
SF Deleted, SF Delete-Remote
Timeout T10
DSA-REQ, DSA-ACK
Stop T10 Timer
DSA-Remote Deleting Service Flow
DSA Ended
DSA-Remote End

Figure C.11-38/J.112 – DSA – Remotely initiated transaction deleting service state flow diagram

C.11.4.3 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;
- add, Delete or Replace a Flow Classifier;
- add, Delete or Set PHS elements.

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

To prevent packet loss, any required bandwidth change is sequenced between the CM and CMTS.

The CMTS 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 CMTS always changes scheduling on receipt of a DSC-REQ (CM initiated transaction) or DSC-RSP (CMTS initiated transaction).

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

The CM controls the upstream transmit behavior. The timing of CM 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 CM reduces its payload bandwidth first and then the CMTS reduces the bandwidth scheduled for the Service Flow. If an upstream Service Flow's bandwidth is being increased, the CMTS increases the bandwidth scheduled for the Service Flow first and then the CM increases its payload bandwidth.

If the bandwidth changes are complex, it may not be obvious to the CM when to effect the bandwidth changes. This information may be signalled to the CM from a higher layer entity. Similarly, if the DSC Signalling is initiated by the CMTS, the CMTS MAY indicate to the CM whether it install or remove Classifiers upon receiving the DSC-Request or whether it postpone this installation until receiving the DSC-Ack (refer to C.C.2.1.8).

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 CM is deactivated that CM is de-registered and MUST reregister. Therefore, care should be taken before deactivating such Service Flows. If a Service Flow that was provisioned during registration is deactivated, the provisioning information for that Service Flow MUST be maintained until the Service Flow is reactivated.

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

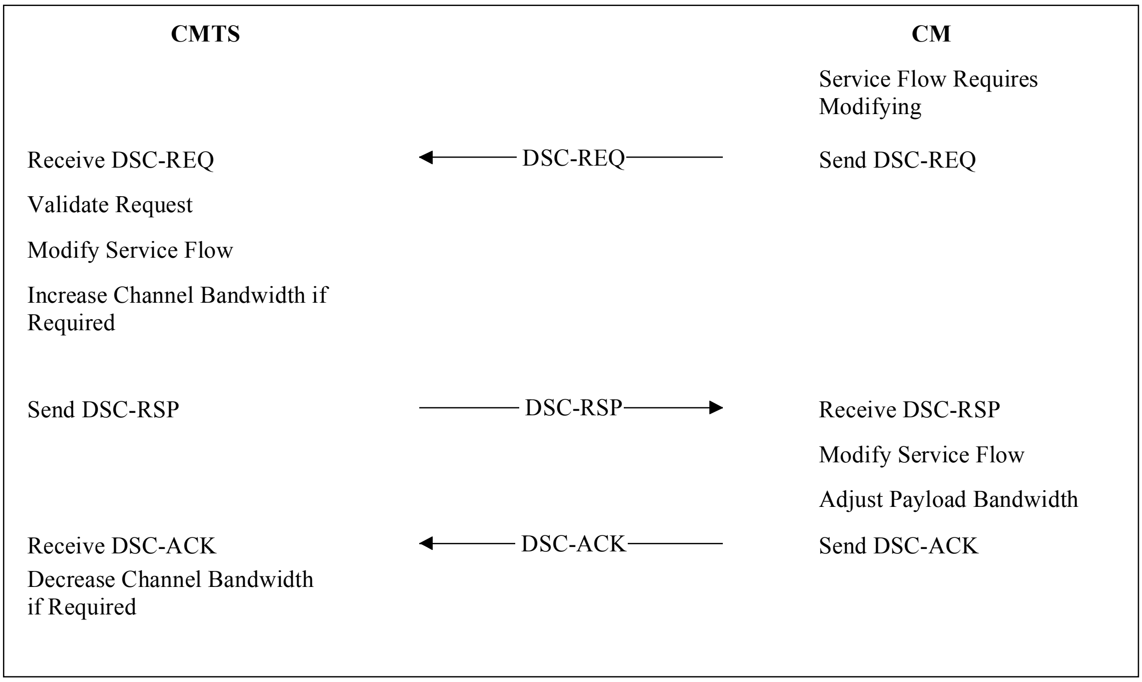
A CMTS MUST have only one DSC transaction outstanding per Service Flow. If it detects a second transaction initiated by the CM, the CMTS MUST abort the transaction the CM initiated and allow the CMTS initiated transaction to complete.

NOTE – Currently anticipated applications would probably control a Service Flow through either the CM or CMTS, and not both. Therefore the case of a DSC being initiated simultaneously by the CM and CMTS is considered as an exception condition and treated as one.

C.11.4.3.1 CM-initiated dynamic service change

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

The CM informs the CMTS using a Dynamic Service Change Request message (DSC-REQ). The CMTS MUST decide if the referenced Service Flow can support this modification. The CMTS MUST respond with a Dynamic Service Change Response (DSC-RSP) indicating acceptance or rejection. The CM reconfigures the Service Flow if appropriate, and then MUST respond with a Dynamic Service Change Acknowledge (DSC-ACK).



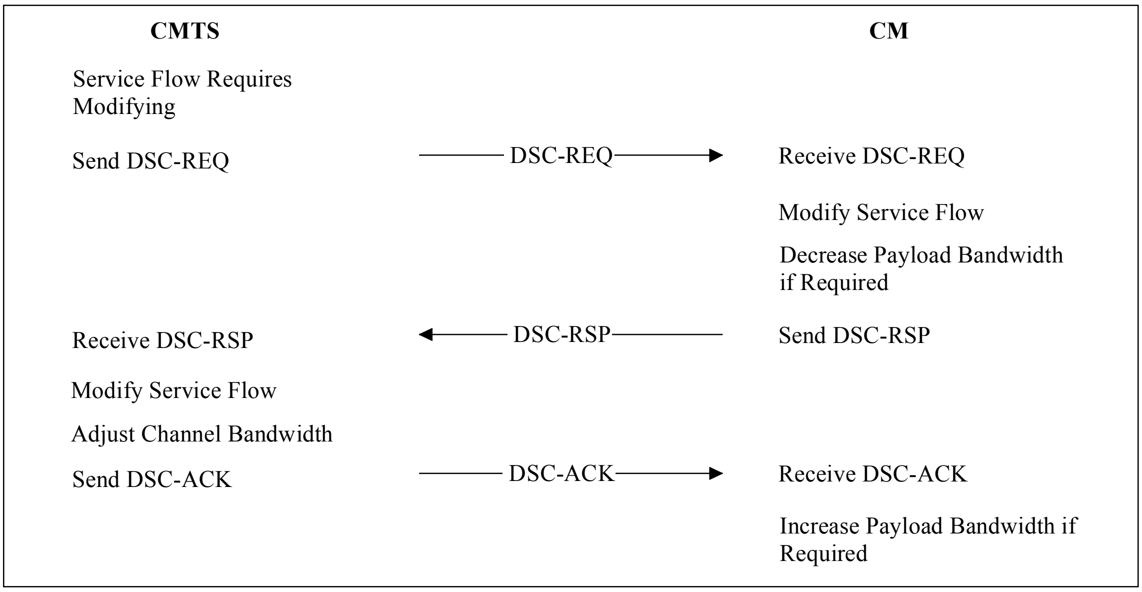
T0914120-02

Figure C.11-39/J.112 – CM-initiated DSC

C.11.4.3.2 CMTS-initiated dynamic service change

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

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



T0914130-02

Figure C.11-40/J.112 – CMTS-initiated DSC

C.11.4.3.3 Dynamic service change state transition diagrams

See Figures C.11-41 to C.11-49.

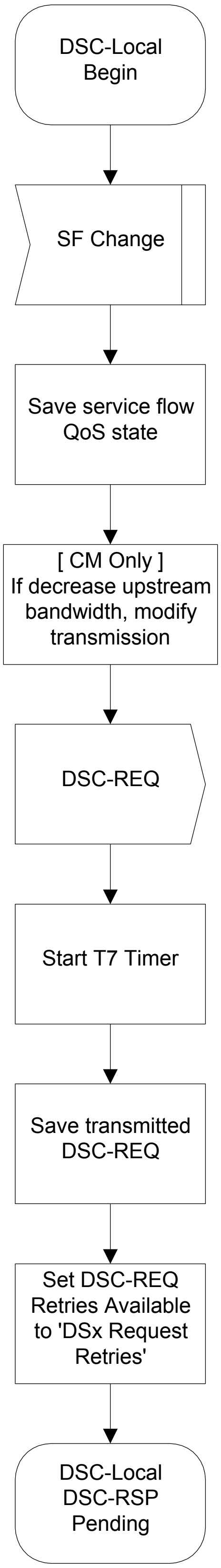

DSC-Local Begin
SF Change
Save service flow QoS state
[CM Only] If decrease upstream bandwidth, modify transmission
DSC-REQ
Start T7 Timer
Save transmitted DSC-REQ
Set DSC-REQ Retries Available to 'DSx Request Retries'
DSC-Local DSC-RSP Pending

Figure C.11-41/J.112 – DSC – Locally initiated transaction begin state flow diagram

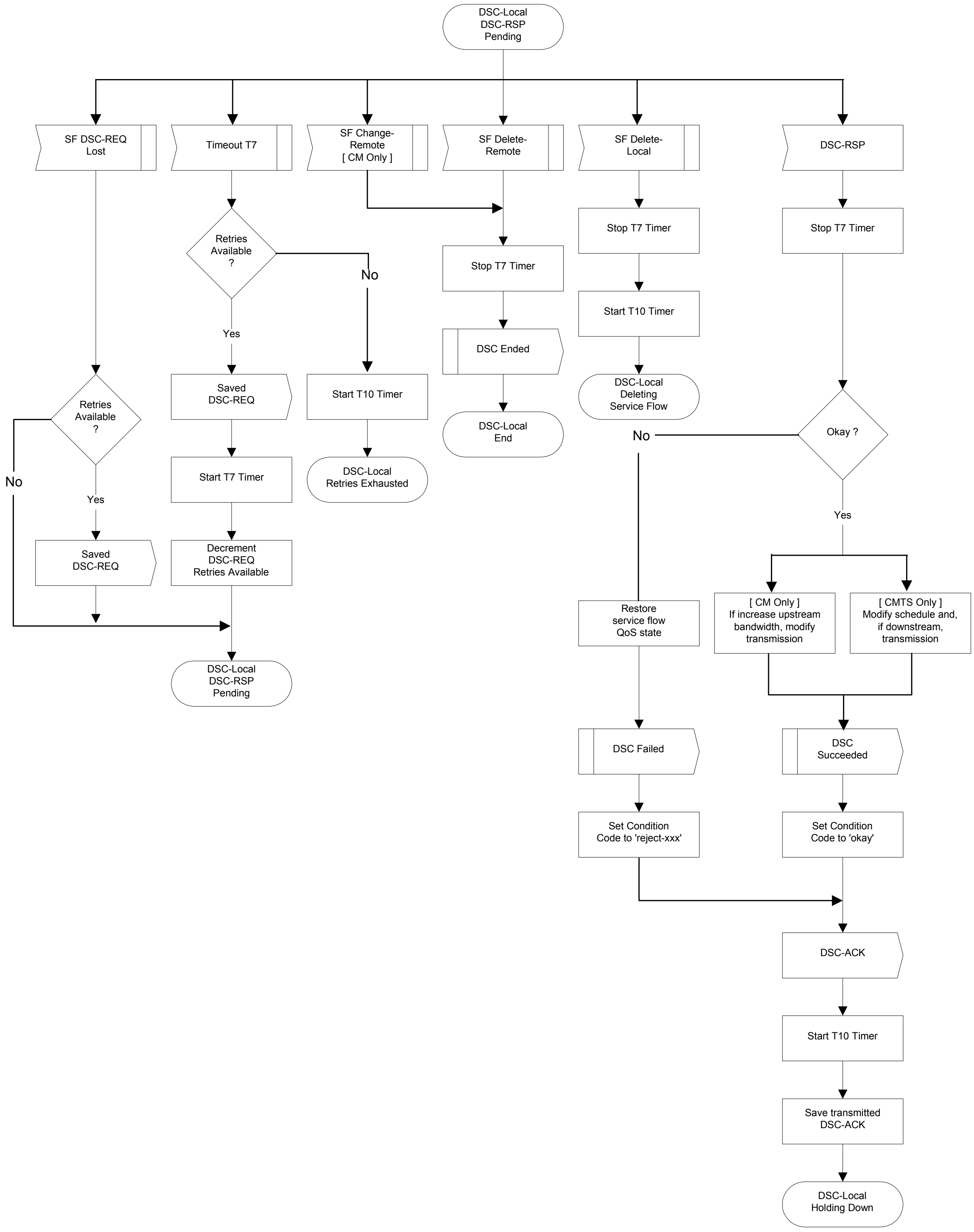


Figure C.11-42/J.112 – DSC – Locally initiated transaction DSC-RSP pending state flow diagram

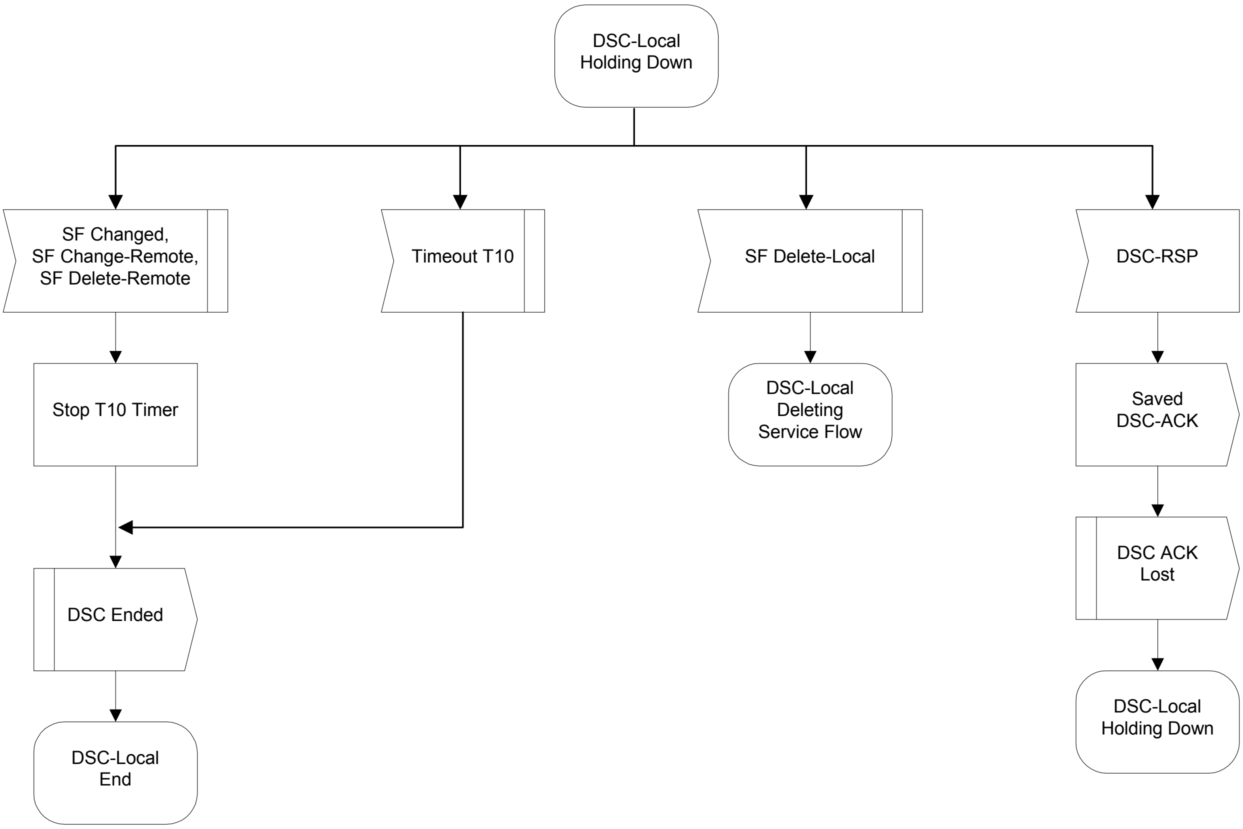


Figure C.11-43/J.112 – DSC – Locally initiated transaction holding down state flow diagram

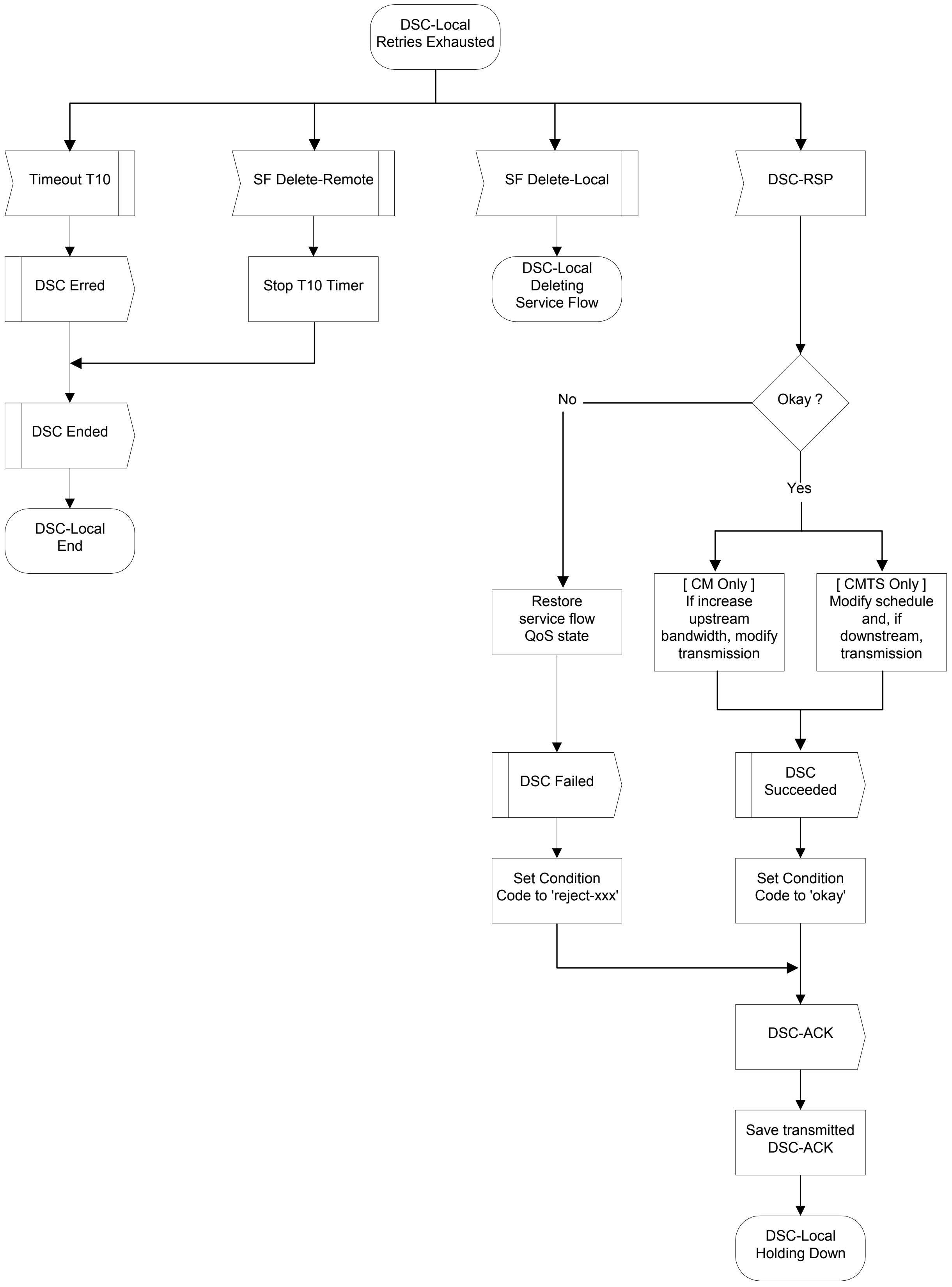

DSC-Local Retries Exhausted
Timeout T10
SF Delete-Remote
SF Delete-Local
DSC-RSP
DSC Erred
Stop T10 Timer
DSC-Local Deleting Service Flow
DSC Ended
DSC-Local End
Okay ?
No
Yes
Restore service flow QoS state
[CM Only] If increase upstream bandwidth, modify transmission
[CMTS Only] Modify schedule and, 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 C.11-44/J.112 – DSC – Locally initiated transaction retries exhausted state flow diagram

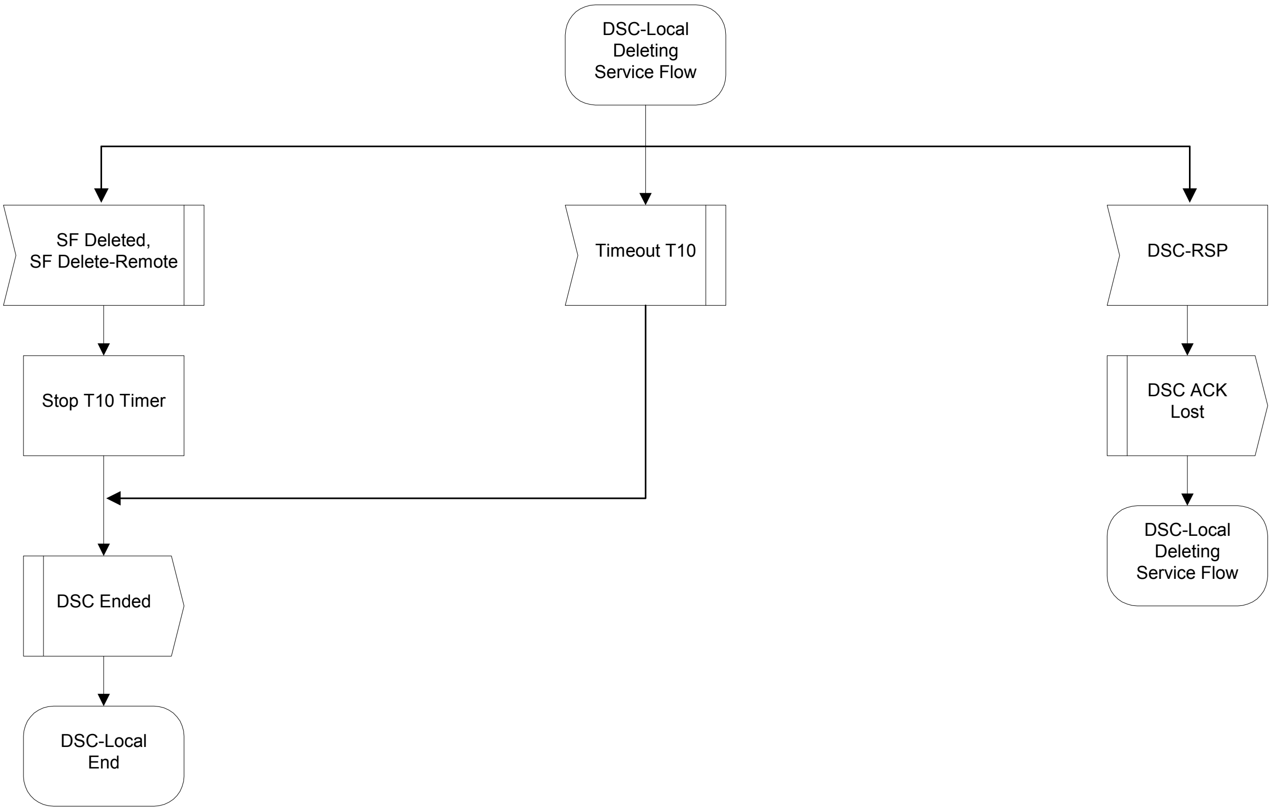

DSC-Local Deleting Service Flow
SF Deleted, SF Delete-Remote
Timeout T10
DSC-RSP
Stop T10 Timer
DSC ACK Lost
DSC-Local Deleting Service Flow
DSC Ended
DSC-Local End

Figure C.11-45/J.112 – DSC – Locally initiated transaction deleting service flow state flow diagram

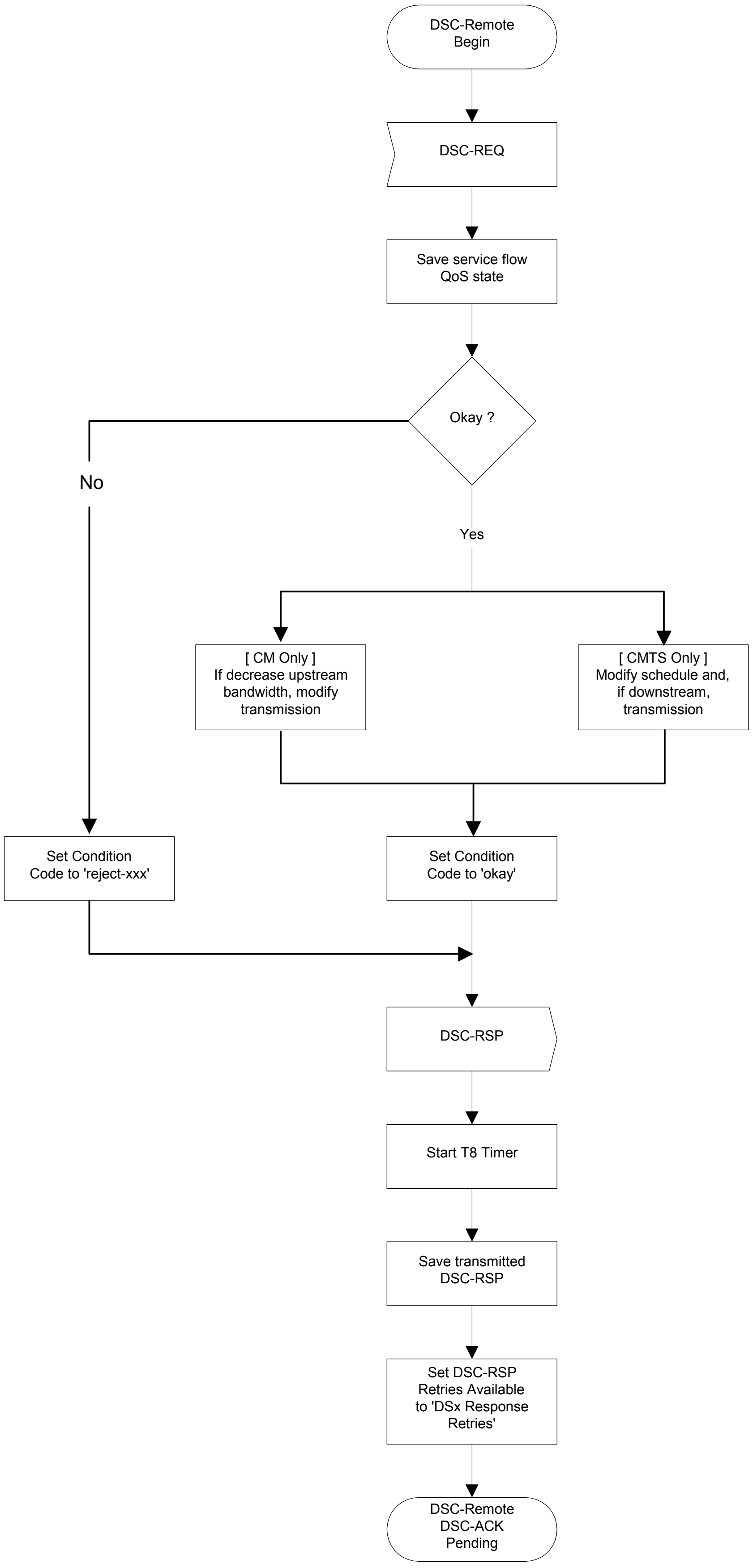


Figure C.11-46/J.112 – DSC – Remotely initiated transaction begin state flow diagram

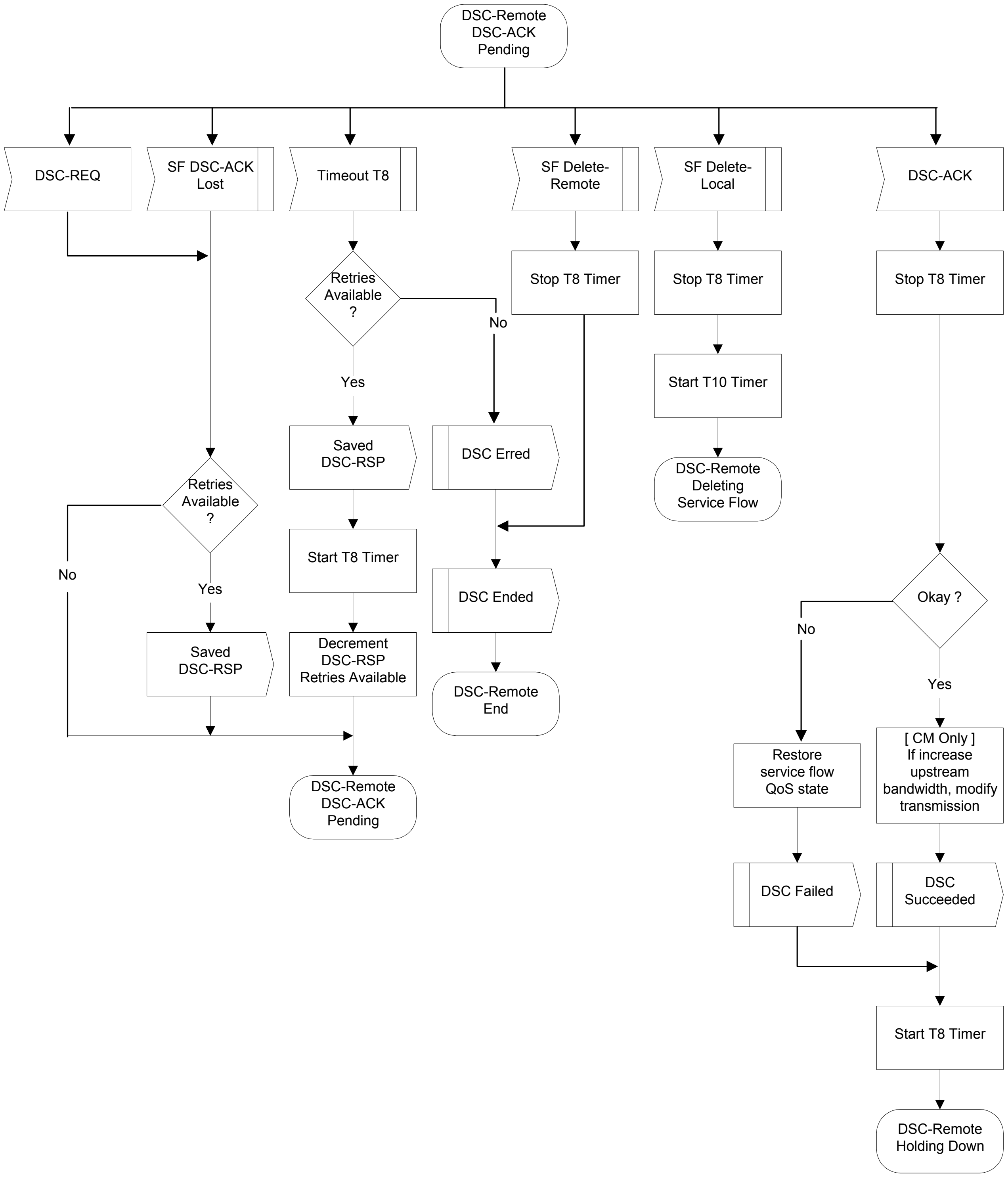


Figure C.11-47/J.112 – DSC – Remotely initiated transaction DSC-ACK pending state flow diagram

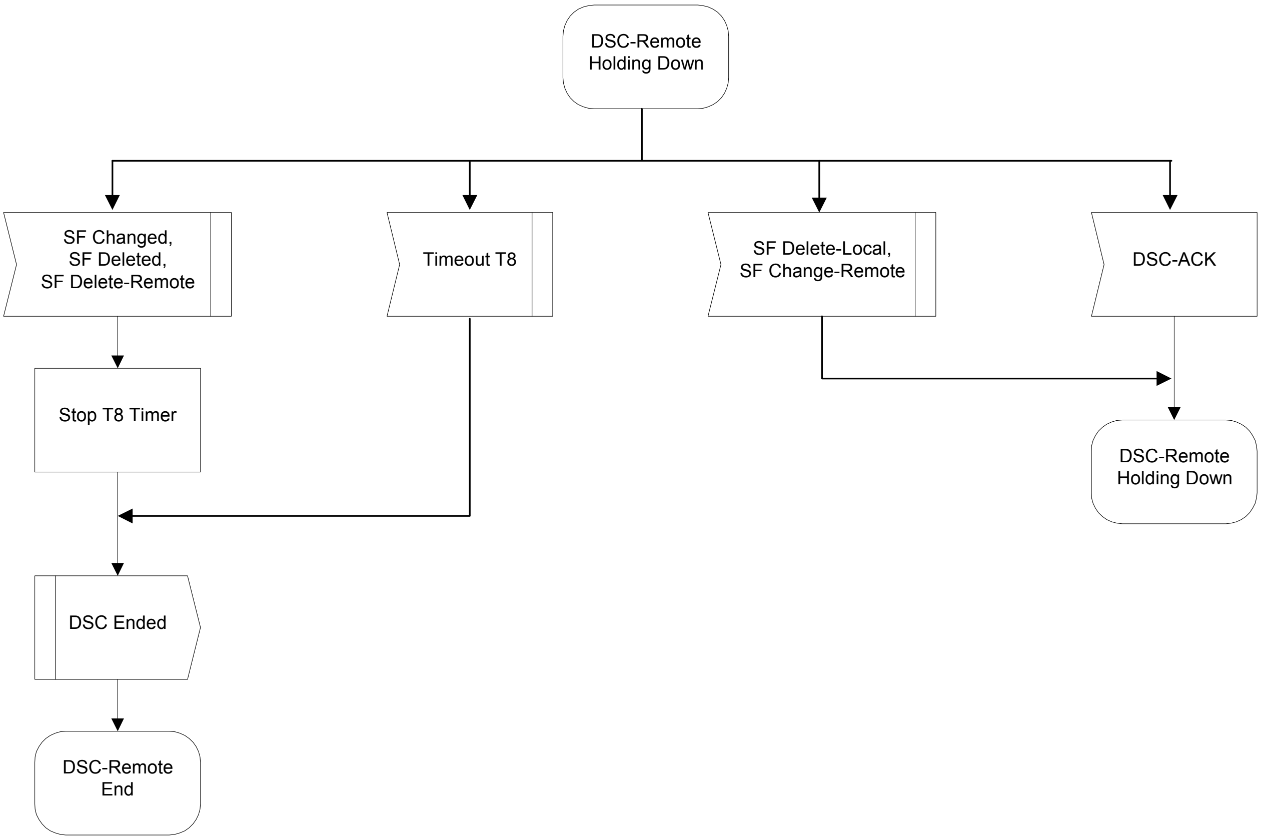


Figure C.11-48/J.112 – DSC – Remotely initiated transaction holding down state flow diagram

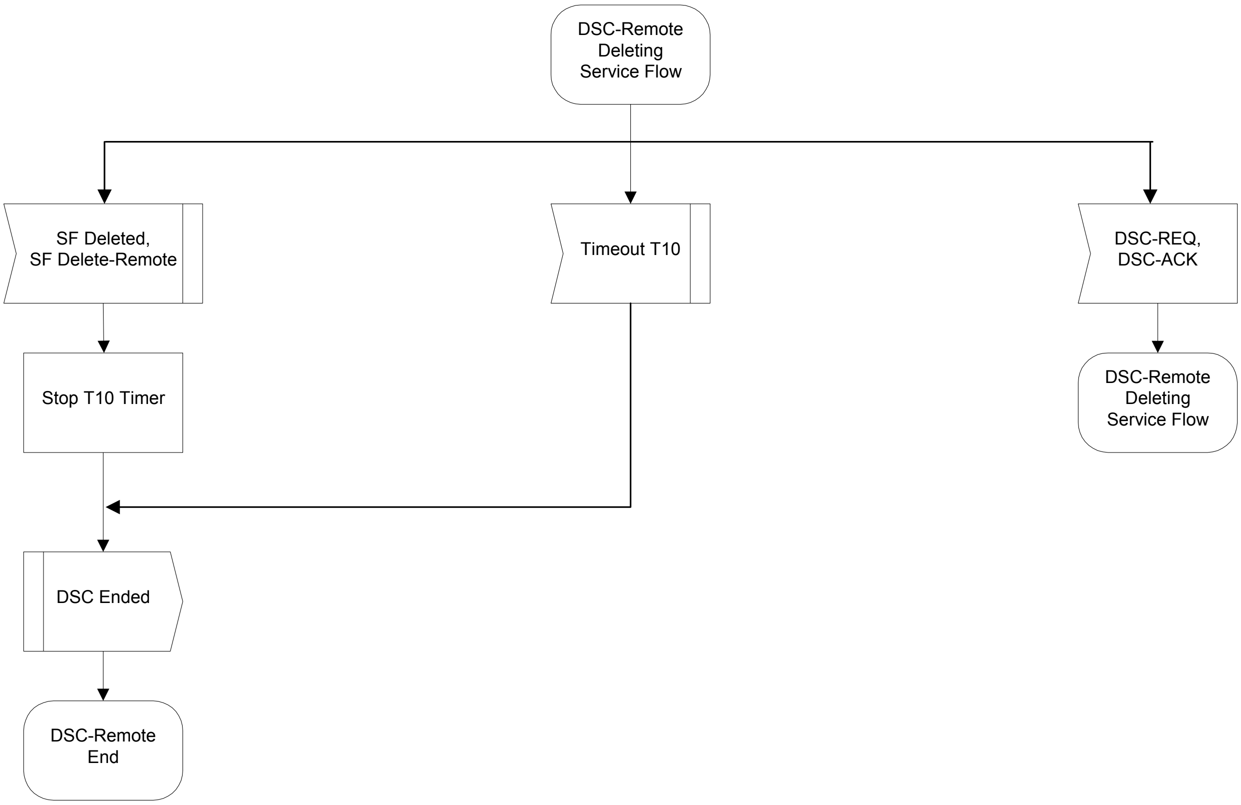


Figure C.11-49/J.112 – DSC – Remotely initiated transaction deleting service flow state flow diagram

C.11.4.4 Dynamic service deletion

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, including classifiers and PHS. However, if a Primary Service Flow of a CM is deleted, that CM is deregistered and MUST reregister. Also, if a Service Flow that was provisioned during registration is deleted, the provisioning information for that Service Flow is lost until the CM reregisters. However, the deletion of a provisioned Service Flow MUST NOT cause a CM to reregister. Therefore, care be taken before deleting such Service Flows.

NOTE – Unlike DSA and DSC messages, DSD messages are limited to only a single Service Flow.

C.11.4.4.1 CM initiated dynamic service deletion

A CM wishing to delete a Service Flow generates a delete request to the CMTS using a Dynamic Service Deletion-Request message (DSD-REQ). The CMTS 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.

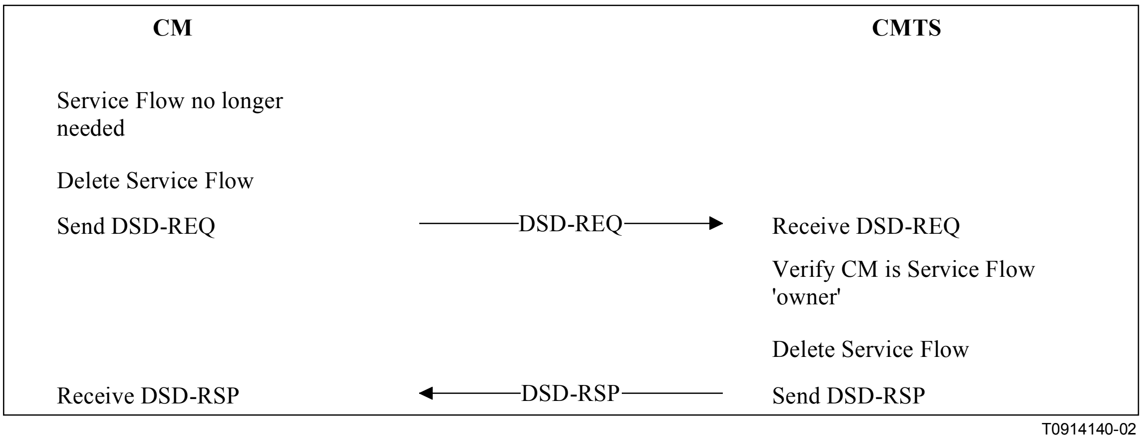


Figure C.11-50/J.112 – Dynamic service deletion initiated from CM

C.11.4.4.2 CMTS initiated dynamic service deletion

A CMTS wishing to delete a dynamic Service Flow generates a delete request to the associated CM using a Dynamic Service Deletion-Request message (DSD-REQ). The CM 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.

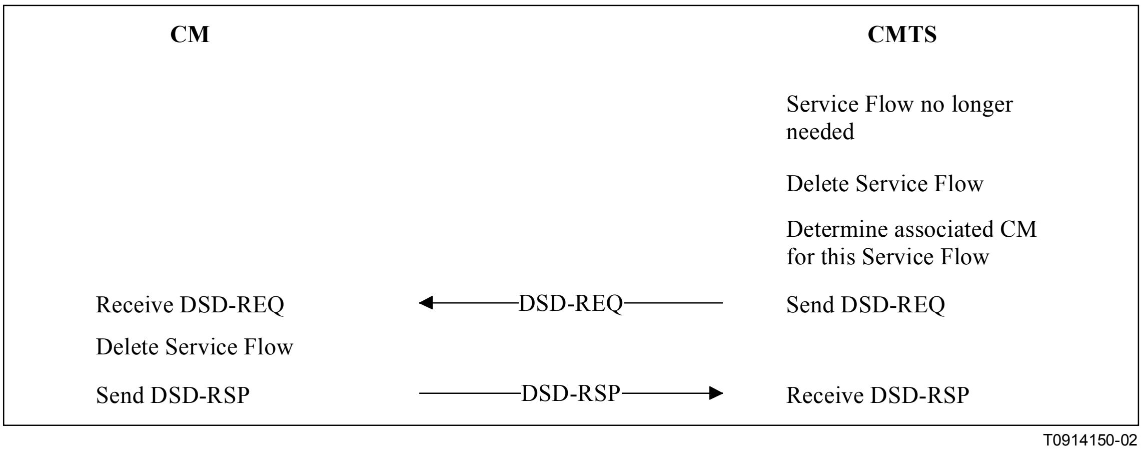


Figure C.11-51/J.112 – Dynamic service deletion initiated from CMTS

C.11.4.4.3 Dynamic service deletion state transition diagrams

See Figures C.11-52 to C.11-56.

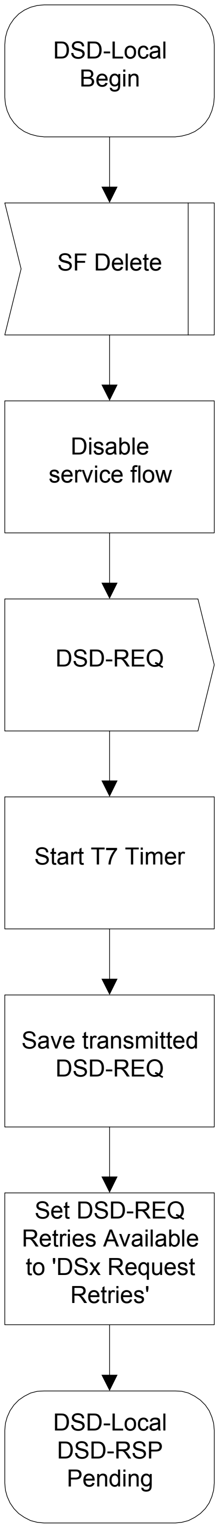


Figure C.11-52/J.112 – DSD – Locally initiated transaction begin state flow diagram

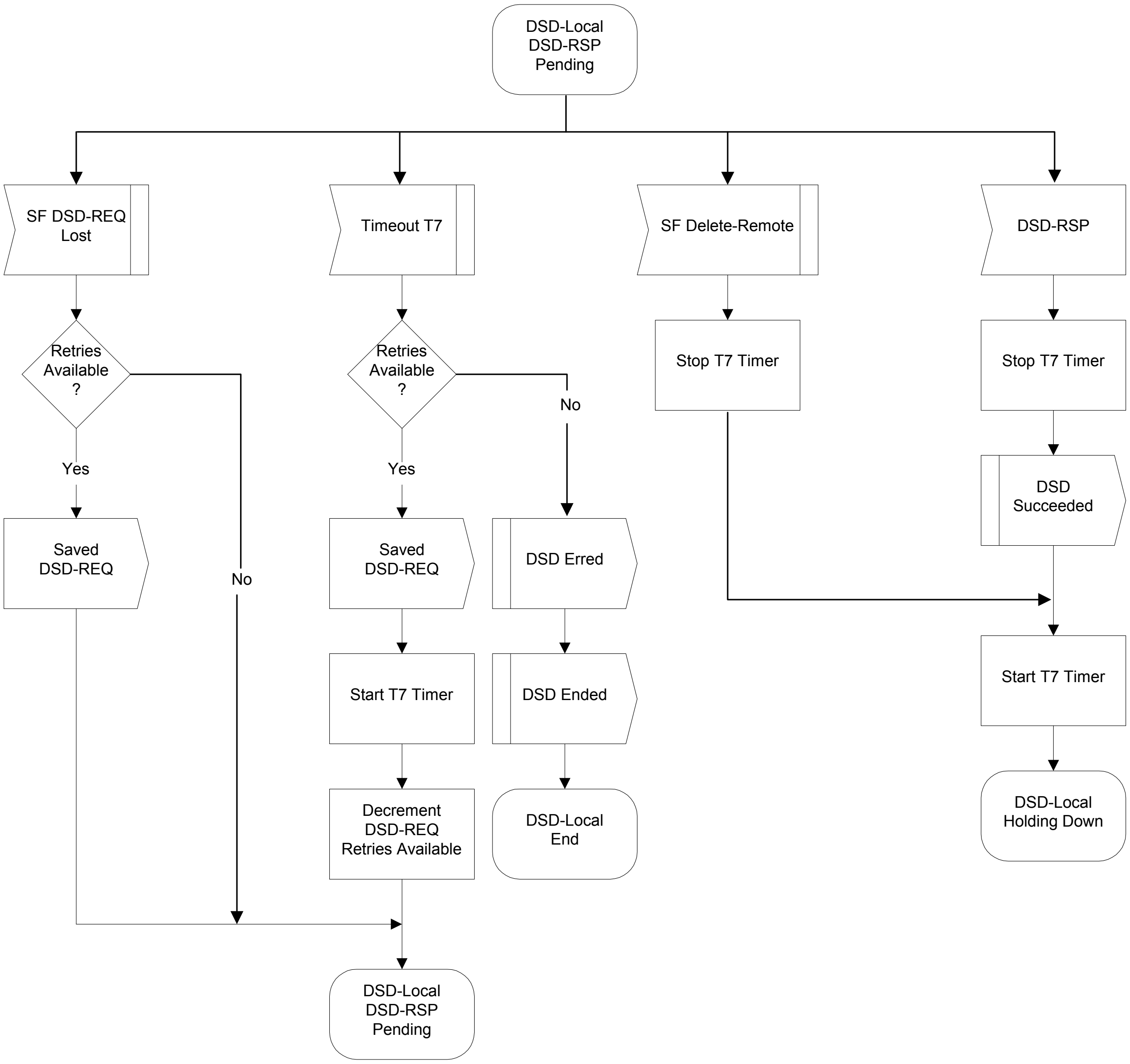


Figure C.11-53/J.112 – DSD – Locally initiated transaction DSD-RSP pending state flow diagram

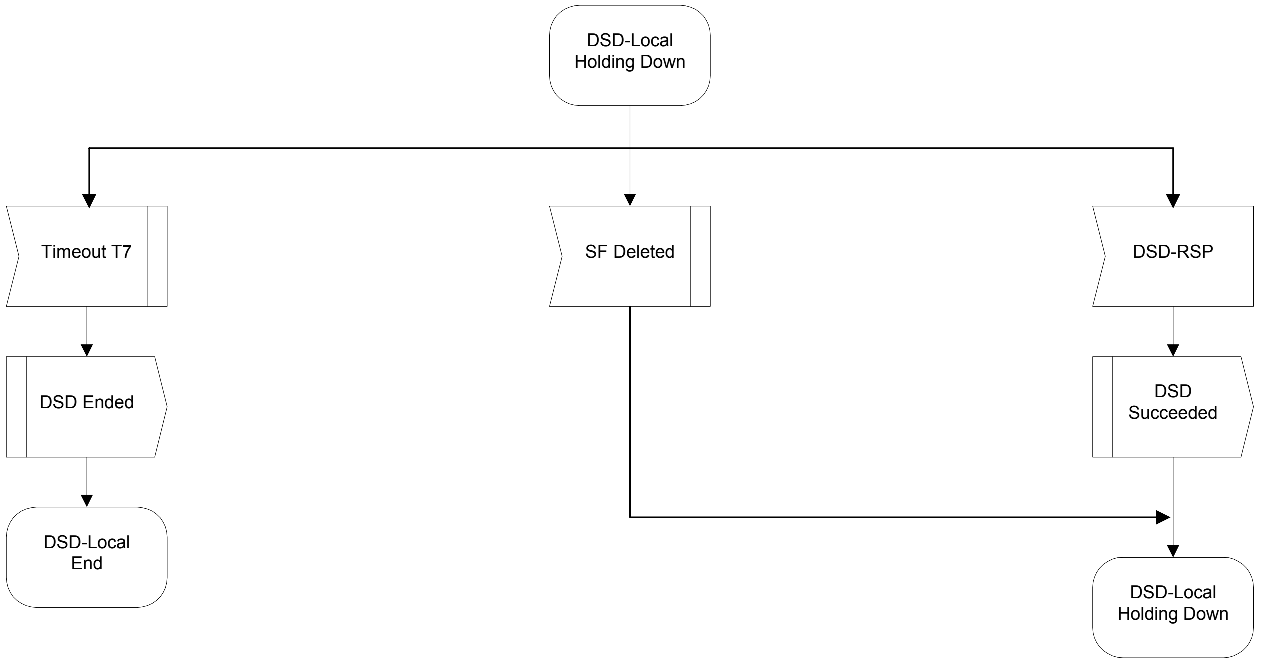


Figure C.11-54/J.112 – DSD – Locally initiated transaction holding down state flow diagram

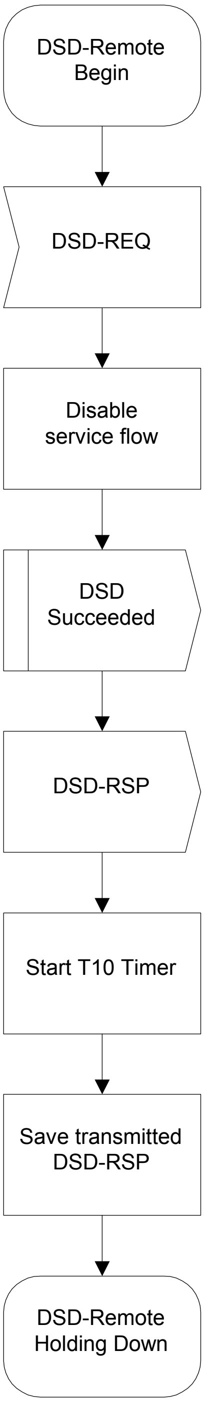


Figure C.11-55/J.112 – DSD – Remotely initiated transaction begin state flow diagram

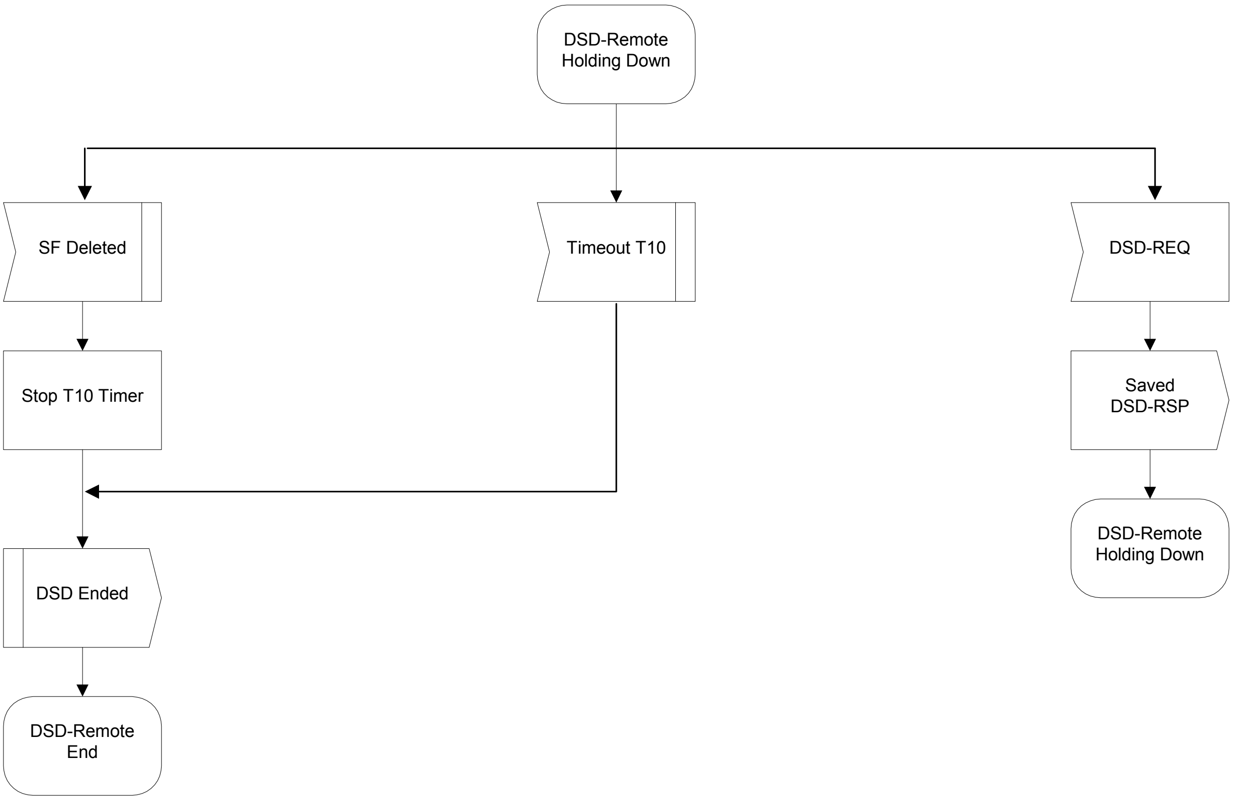


Figure C.11-56/J.112 – DSD – Remotely initiated transaction holding down state flow diagram

C.11.4.5 Dynamically changing downstream and/or upstream channels

C.11.4.5.1 DCC general operation

At any time after registration, the CMTS MAY direct the CM to change its downstream and/or upstream channel. This may be done for traffic balancing, noise avoidance, or other reasons which are beyond the scope of this annex. Figure C.11-58 shows the procedure that MUST be followed by the CMTS. Figure C.11-60 shows the corresponding procedure that MUST be followed by a DCC-capable CM.

The DCC command can be used to change only the upstream frequency, only the downstream frequency, or both the upstream and downstream frequencies. When only the upstream or only the downstream frequency is changed, the change is typically within a MAC domain. When both the upstream and downstream frequencies are changed, the change may be within a MAC domain, or between MAC domains.

The Downstream Channel ID and the Upstream Channel ID MUST both be unique between the old and new channels. In this context, the old channel refers to the channel(s) that the CM was on before the jump, and the new channel refers to the channel(s) that the CM is on after the jump.

Upon synchronizing with the new upstream and/or downstream channel, the CM MUST use the technique specified in the DCC-REQ Initialization Technique TLV, if present, to determine if it perform reinitialization, only ranging, or neither. If this TLV is not present in DCC-REQ, the CM MUST reinitialize its MAC on the new channel assignment. (Refer to C.11.2.) If the CM has been instructed to reinitialize, then the CMTS MUST NOT wait for a DCC-RSP to occur on the new channel.

If the CM is being moved within a MAC domain, then a reinitialization may not be required. If the CM is being moved between MAC domains, then a reinitialization may be required. Reinitializing, if requested, is done with the new upstream and downstream channel assignments. It includes obtaining upstream parameters, establishing IP connectivity, establishing time of day, transferring operational parameters, registering, and initializing baseline privacy. If reinitialization is performed, the CM MUST NOT send a DCC-RSP on the new channel.

The decision to rerange is based upon the CMTS's knowledge of any path diversity that may exist between the old and new channels, or if any of the fundamental parameters of the upstream or downstream channel such as symbol rate, modulation type, or mini-slot size have changed.

When DCC-REQ does not involve reinitialization or reranging, the design goal of the CM will typically be to minimize the disruption of traffic to the end user. To achieve this goal, a CM MAY choose to continue to use QoS resources (such as bandwidth grants) on its current channel after receiving a DCC-REQ and before actually executing the channel change. The CM might also need this time to flush internal queues or reset state machines prior to changing channels.

The CM MAY continue to use QoS resources on the old channel, including the transmission and reception of packets, after sending a DCC-RSP (depart) message and prior to the actual jump. The CM MAY use QoS resources on the new channel, including the transmission and reception of packets, after the jump and prior to sending a DCC-RSP (arrive) message. The CMTS MUST NOT use the DCC-RSP (depart) message to remove QoS resources on the old channel. The CMTS MUST NOT wait for a DCC-RSP (arrive) message on the new channel before allowing QoS resources to be used. This provision is to allow the Unsolicited Grant Service to be used on the old and new channel with a minimum amount of disruption when changing channels.

The CMTS MUST hold the QoS resources on the current channel until a time of T13 has passed after the last DCC-REQ that was sent, or until it can internally confirm the presence of the CM on the new channel assignment. The CM MUST execute the departure from the old channel and the arriving at the new channel, less any commanded reinitialization, before the expiry of T13. The CM MAY continue to use QoS resources on the current channel after responding with DCC-RSP and before the expiry of T13.

Once the CM changes channels, all previous outstanding bandwidth requests made via the Request IE or Request/Data IE are invalidated, and the CM MUST rerequest bandwidth on the new channel. In the case of Unsolicited Grant Service in the upstream, the grants are implicit with the QoS reservations, and do not need to be rerequested.

C.11.4.5.2 DCC exception conditions

If a CM issues a DSA-REQ or DSC-REQ for more resources, and the CMTS needs to do a DCC to obtain those resources, the CMTS will reject the DSA or DSC command without allocating any resources to the CM. The CMTS includes a confirmation code of "reject-temporary-DCC" (refer to C.C.4) in the DSC-RSP message to indicate that the new resources will not be available until a DCC is received. The CMTS will then follow the DSA or DSC transaction with a DCC transaction.

After the CM jumps to a new channel and completes the DCC transaction, the CM retries the DSA or DSC command. If the CM has not changed channels after the expiry of T14, as measured from the time that the CM received DSA-RSP or DSC-RSP from the CMTS, then the CM MAY retry the resource request.

If the CMTS needs to change channels in order to satisfy a resource request other than a CM initiated DSA or DSC command, then the CMTS should execute the DCC command first, and then issue a DSA or DSC command.

If a CMTS does a DCC with reinitialize, the config file could cause the CM to come back to the original channel. This would cause an infinite loop. To prevent this, if the provisioning system default is to specify the upstream channel ID and/or the downstream frequency, then the CMTS SHOULD NOT use DCC-REQ with the reinitialize option.

The CMTS MUST NOT issue a DCC command if the CMTS has previously issued a DSA, or DSC command, and that command is still outstanding. The CMTS MUST NOT issue a DCC command if the CMTS is still waiting for a DSA-ACK or DSC-ACK from a previous CM initiated DSA-REQ or DSC-REQ command.

The CMTS MUST NOT issue a DSA or DSC command if the CMTS has previously issued a DCC command, and that command is still outstanding.

If the CMTS issues a DCC-REQ command and the CM simultaneously issues a DSA-REQ or DSC-REQ then the CMTS command takes priority. The CMTS responds with a confirmation code of "reject-temporary" (refer to C.C.4). The CM proceeds with executing the DCC command.

If the CM is unable to achieve communications with a CMTS on the new channel(s), it MUST return to the previous channel(s) and reinitialize its MAC. The previous channel assignment represents a known good operating point which should speed up the reinitialization process. Also, returning to the previous channel provides a more robust operational environment for the CMTS to find a CM that fails to connect on the new channel(s).

If the CMTS sends a DCC-REQ and does not receive a DCC-RSP within time T11, it MUST retransmit the DCC-REQ up to a maximum of "DCC-REQ Retries" (Annex C.B) before declaring the transaction a failure. Note that if the DCC-RSP was lost in transit and the CMTS retries the DCC-REQ, the CM may have already changed downstream channels.

If the CM sends a DCC-RSP on the new channel and does not receive a DCC-ACK from the CMTS within time T12, it MUST retry the DCC-RSP up to a maximum of "DCC-ACK Retries" (Annex C.B).

If the CM receives a DCC-REQ with the Upstream Channel ID TLV, if present, equal to the current Upstream Channel ID, and the Downstream Frequency TLV, if present, is equal to the current downstream frequency, then the CM MUST consider the DCC-REQ as a redundant command. The remaining DCC-REQ TLV parameters MUST NOT be executed, and the CM MUST return a DCC-RSP, with a confirmation code of "reject-already-there", to the CMTS (refer to C.C.4.1).

C.11.4.5.3 Near-seamless channel change

When the CMTS wishes to add new QoS reservations to a CM, it may be necessary to move that CM to a new upstream and/or downstream channel to achieve that goal. During that changing of channels, it is desirable to provide the minimum of interruption to existing QoS services such as voice over IP or video streaming sessions. This near-seamless channel change is the primary design goal of the DCC command. The CMTS MAY support a near-seamless channel change. The CM MAY support a near-seamless channel change.

The actions below are recommended operating procedures to implement a near-seamless channel change. The list assumes both the upstream and downstream channels are changing. A subset of the list would apply if only the upstream or downstream channel changed.

To support a near-seamless channel change, the following conditions apply in the network:

- The physical layer parameters for the new upstream and downstream channels do not change with the old upstream and downstream channels. Note that a change in downstream parameters could invalidate the ranging parameters.
- The ranging parameters not change between the old and new channels. This may require symmetrical cabling and plant conditions which are external to the CMTS.
- The CMTS use the same time stamp and SYNC mechanism for all downstream channels.
- IP routing be configured so that the CM and its attached CPEs can continue to use their existing IP addresses. This will avoid disruption to RTP sessions or other in progress applications.

To achieve a near-seamless channel change, the CMTS:

- SHOULD duplicate all the relevant QoS reservations for the CM on the old and new channel assignments before initiating a DCC-REQ.
- SHOULD duplicate downstream packet flow for the CM on the old and new channel assignments before initiating a DCC-REQ (for downstream channel changes).
- SHOULD transmit MAP messages for the new upstream channel on the old downstream channel for at least the duration of T13, if the old and new downstream channels share the same timestamp. (Note that if the CM cannot cache MAPs for the new upstream while on the old downstream channel, then the channel change delay will be increased by the amount of time into the future that MAPs are generated. Thus, the CMTS SHOULD refrain from scheduling MAPs farther into the future than it needs to.)
- SHOULD specify the downstream and upstream parameters of the new channels prior to the CM jumping.
- SHOULD specify to not wait for a SYNC message on the new channel.
- SHOULD specify to skip initialization (as defined in C.11.2).
- SHOULD specify to skip initial maintenance and station maintenance.
- SHOULD manage service flow substitutions between old and new SIDs, SAID, Service Flow IDs, Classifier IDs, Payload Header Suppression Indexes, and Unsolicited Grant Time Reference as required. Service Class Names SHOULD remain the same between the old and new channel(s).

To achieve a near-seamless channel change, the CM:

- SHOULD reply with estimates for CM Jump Time in the DCC-RSP message.
- SHOULD listen for and cache MAP messages on the old downstream that apply to the new upstream. This SHOULD be done during time T13.
- SHOULD use the downstream parameters and the UCD in its cache from the DCC command to force a quicker PHY convergence when jumping.
- SHOULD NOT wait for a SYNC message after PHY convergence and before transmitting, if the CMTS permits the CM to do so.
- SHOULD use the cached MAP, if available, to allow a quicker start-up time.
- SHOULD minimize the disruption of traffic in either direction by allowing traffic to continue to flow in both directions up to the moment prior to the jump and then immediately after resynchronization to the new channel(s) has happened.
- SHOULD queue incoming data packets that arrive during the jump, and transmit them after the jump.
- SHOULD discard VoIP packets after the jump that have caused the upstream Unsolicited Grant Service queue to exceed its limit, but no more than necessary.

Applications that are running over the Annex C/J.112 path should be able to cope with the loss of packets that may occur during the time that the CM changes channels.

C.11.4.5.4 Example operation

Figure C.11-18 shows an example of the use of DCC and its relation to the other Annex C/J.112 MAC messages. In particular, this example describes a scenario where the CM attempts to allocated new resources with a DSA message. The CMTS temporarily rejects the request, tells the CM to change channels, and then the CM rerequests the resources. This example (not including all exception conditions) is described below. Refer to C.11.2 for more detail.

a) An event occurs, such as the CM issuing a DSA-REQ message.

b) The CMTS decides that it needs to change channels in order to service this resource request. The CMTS responds with a DSA-RSP message which includes a confirmation code of "reject-temporary-DCC" (refer to C.C.4) in the DSC-RSP message to indicate that the new resources are not available until a DCC is received. The CMTS now rejects any further DSA or DSC messages until the DCC command is executed.

c) The CMTS initiates QoS reservations on the new upstream and/or downstream channels. The QoS reservations include the new resource assignments along with all the current resource assignments assigned to the CM. In this example, both the upstream and downstream channels are changed.

d) To facilitate a near-seamless channel change, since the CMTS is not sure exactly when the CM will switch channels, the CMTS duplicates the downstream packet flow on the old and new downstream channels.

e) The CMTS issues a DCC-REQ command to the CM.

f) The CM sends a DCC-RSP (depart). The CM then cleans up its queues and state machines as appropriate and changes channels.

g) If there was a downstream channel change, the CM synchronizes to the QAM symbol timing, synchronizes the FEC framing, and synchronizes with the MPEG framing.

h) If the CM has been instructed to reinitialization, it does so with the new upstream and/or downstream channel assignment. The CM exits from the flow of events described here, and enters the flow of events described in C.11.2 starting with the recognition of a downstream SYNC message.

i) The CM searches for a UCD message unless it has been supplied with a copy.

j) The CM waits for a downstream SYNC message unless it has been instructed not to wait for one.

k) The CM collects MAP messages unless it already has them available in its cache.

l) The CM performs initial maintenance and station maintenance unless it has been instructed to skip them.

m) The CM resumes normal data transmission with its new resource assignment.

n) The CM sends a DCC-RSP (arrive) message to the CMTS.

o) The CMTS responds with a DCC-ACK.

p) The CMTS removes the QoS reservations from the old channels. If the downstream packet flow was duplicated, the packet duplication would also be removed on the old downstream channel.

q) The CM re-issues its DSA-REQ command.

r) The CMTS reserves the requested resources and responds with a DSA-RSP.

s) The CM finishes with a DSA-ACK.

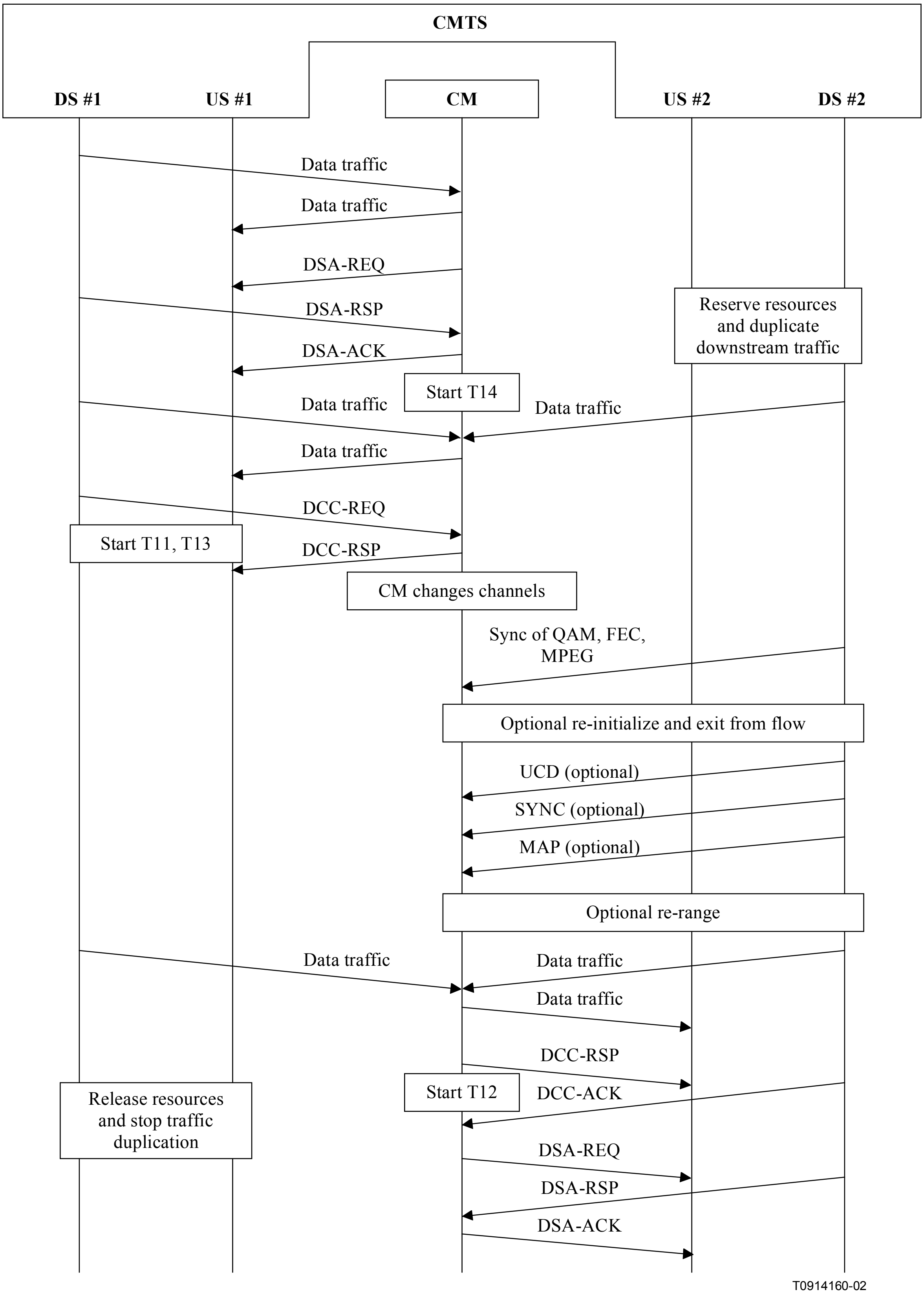


Figure C.11-57/J.112 – DCC example operational flow

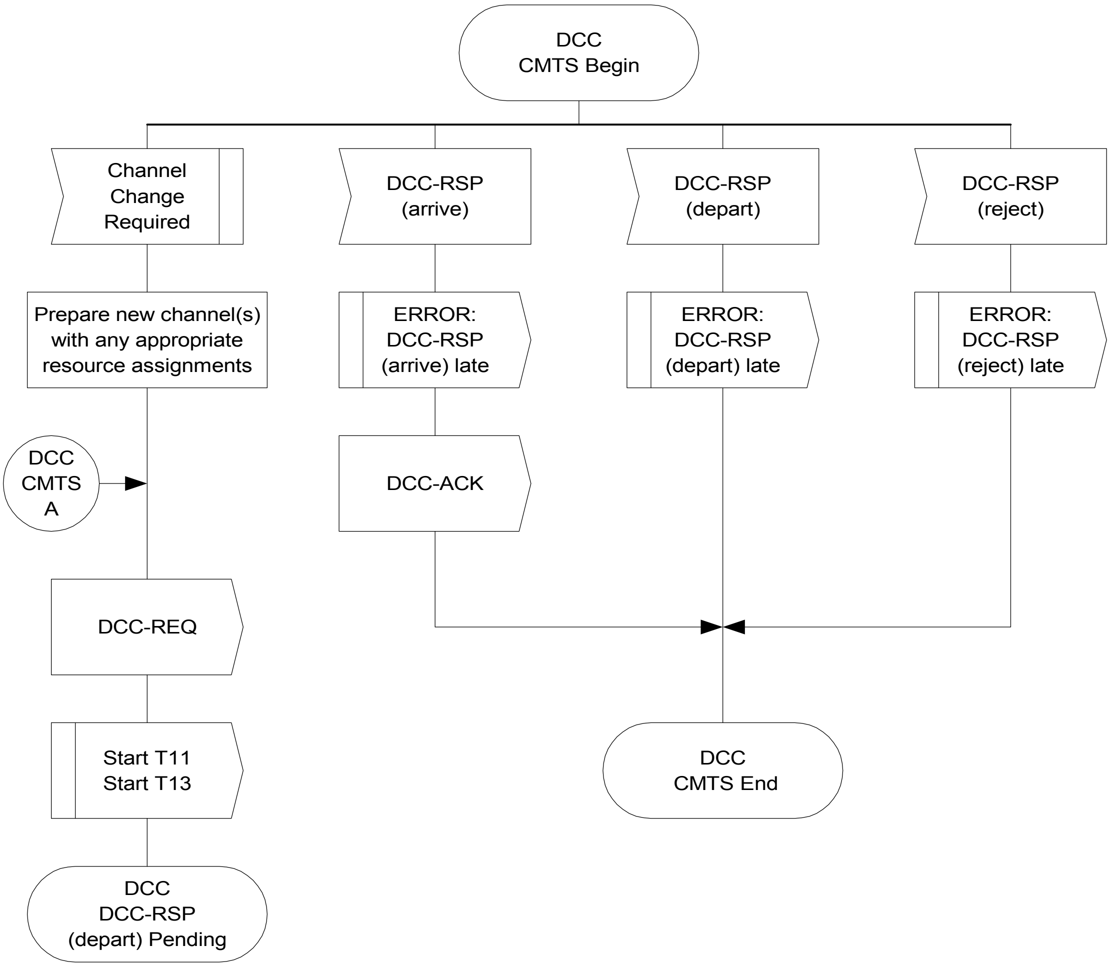


Figure C.11-58/J.112 – Dynamically changing channels: CMTS view, Part 1

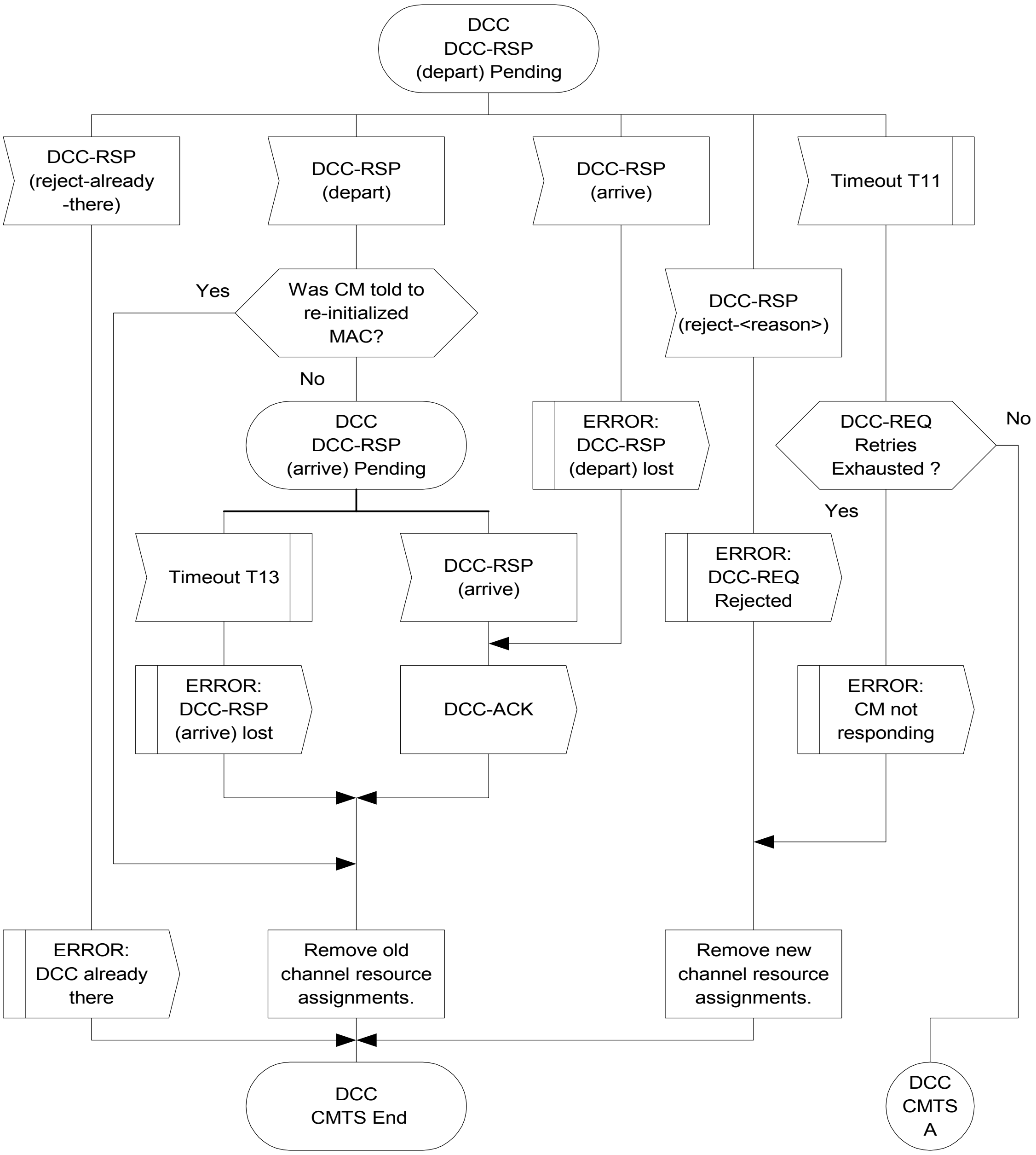
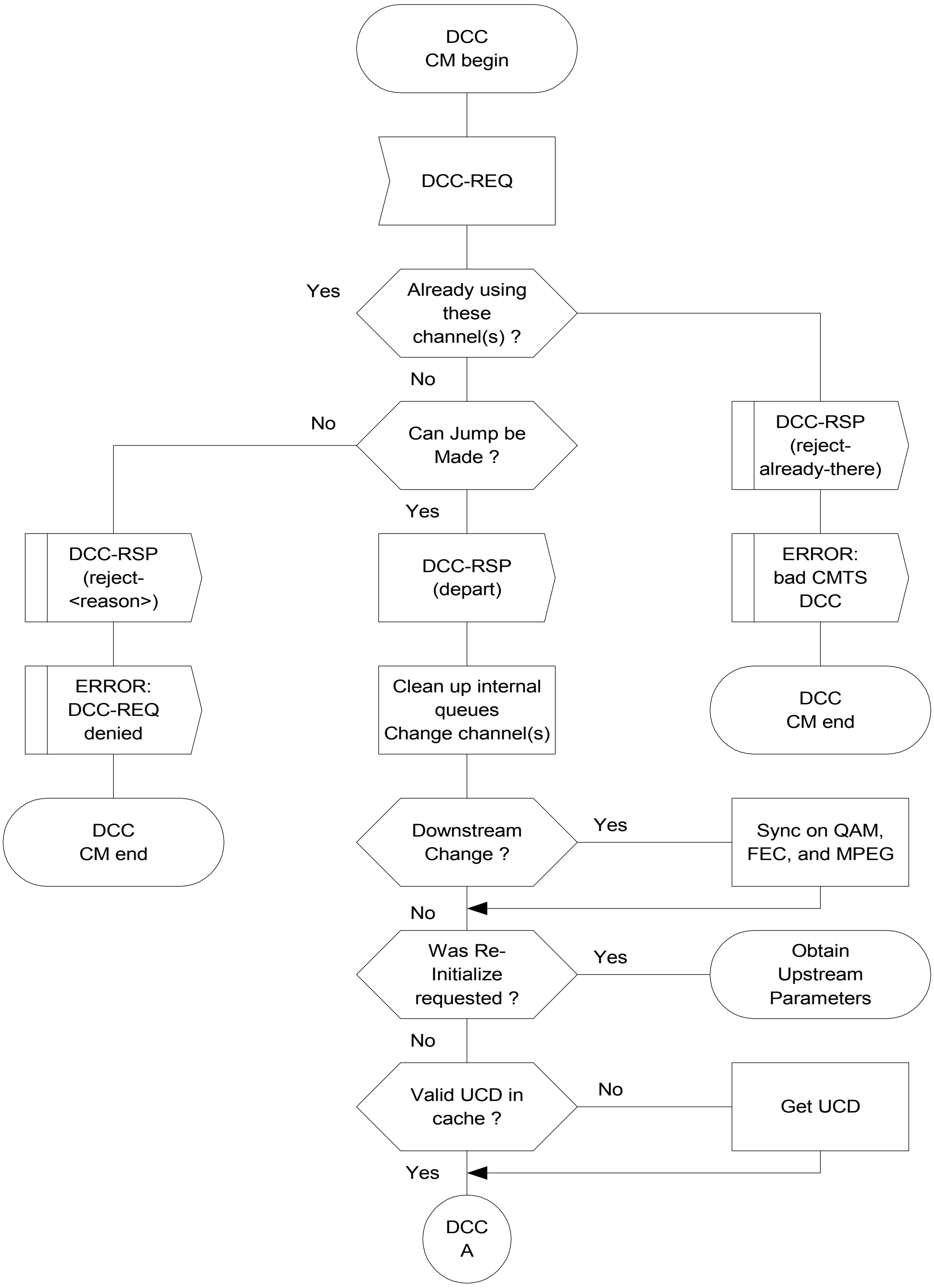


Figure C.11-59/J.112 – Dynamically changing channels: CMTS view, Part 2


DCC
CM begin
DCC-REQ
Yes
Already using these channel(s) ?
No
No
Can Jump be Made ?
Yes
DCC-RSP (reject-already-there)
DCC-RSP (reject-<reason>)
DCC-RSP (depart)
ERROR: bad CMTS DCC
ERROR: DCC-REQ denied
Clean up internal queues Change channel(s)
DCC CM end
DCC CM end
Downstream Change ?
Yes
Sync on QAM, FEC, and MPEG
No
Was Re-Initialize requested ?
Yes
Obtain Upstream Parameters
No
Valid UCD in cache ?
No
Get UCD
Yes
DCC A

NOTE – The state "Obtain Upstream Parameters" links to the state machine in Figure C.11-1.

Figure C.11-60/J.112 – Dynamically changing channels: CM view, Part 1

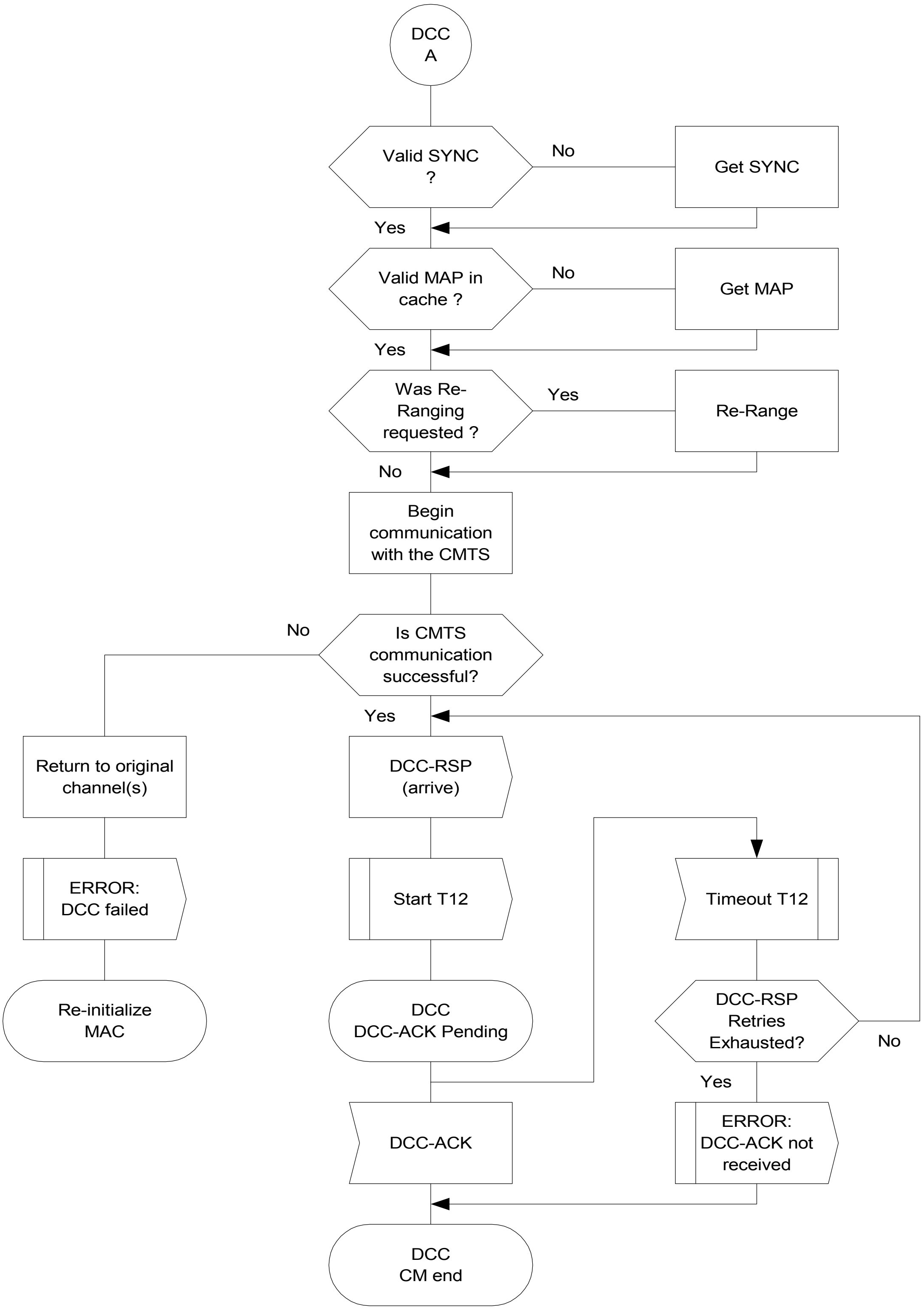


Figure C.11-61/J.112 – Dynamically changing channels: CM view, Part 2

C.11.5 Fault detection and recovery

Fault detection and recovery occurs at multiple levels.

- At the physical level, FEC is used to correct errors where possible – refer to clause C.6 for details.

- The MAC protocol protects against errors through the use of checksum fields across both the MAC Header and the data portions of the packet – refer to clause C.8 for details.
- All MAC management messages are protected with a CRC covering the entire message, as defined in clause C.8. Any message with a bad CRC MUST be discarded by the receiver.

Table C.11-1 shows the recovery process that MUST be taken following the loss of a specific type of MAC message.

Annex C.J contains a list of error codes with more useful information as to the failure of the PHY and MAC layers. Refer to C.8.2.8 for additional information.

Table C.11-1/J.112 – Recovery process on loss of specific MAC messages

Message name	Action following message loss
SYNC	The CM can lose SYNC messages for a period of the Lost SYNC interval (see Annex C.B) before it has lost synchronization with the network. A CM that has lost synchronization MUST NOT use the upstream and MUST try to reestablish synchronization.
UCD	During CM initialization the CM MUST receive a usable (see Note) UCD before transmitting on the upstream. When in the "Obtain Upstream Parameters" state of CM initialization process, if the CM does not receive a usable UCD within the T1 timeout period, the CM MUST NOT transmit on the upstream and MUST scan for another downstream channel. After receiving a usable UCD, whenever the CM receives an unusable UCD or a MAP with a UCD Count that does not match the Configuration Change Count of the last UCD received, the CM MUST NOT transmit on the upstream and MUST start the T1 timer. If the T1 timer expires under these circumstances, the CM MUST reset and reinitialize its MAC connection.
MAP	A CM MUST NOT transmit without a valid upstream bandwidth allocation. If a MAP is missed due to error, the CM MUST NOT transmit for the period covered by the MAP.
RNG-REQ RNG-RSP	If a CM fails to receive a valid ranging response within a defined timeout period after transmitting a request, the request MUST be retried a number of times (as defined in Annex C.B). Failure to receive a valid ranging response after the requisite number of attempts MUST cause the modem to reset and reinitialize its MAC connection.
REG-REQ REG-RSP	If a CM fails to receive a valid registration response within a defined timeout period after transmitting a request, the request will be retried a number of times (as defined in Annex C.B). Failure to receive a valid registration response after the requisite number of attempts will cause the modem to reset and reinitialize its MAC connection.
UCC-REQ UCC-RSP	If a CMTS fails to receive a valid upstream channel change response within a defined timeout period after transmitting a request, the request MUST be retried a number of times (as defined in Annex C.B). Failure to receive a valid response after the requisite number of attempts MUST cause the CMTS to consider the CM as unreachable.
NOTE – A usable UCD is one that contains legal profiles that the modem can understand. The CM MAY also require that the UCD Count of the MAPs received match the Configuration Change Count field of the last received UCD before it considers the UCD as usable.	

Messages at the network layer and above are considered to be data packets by the MAC Sublayer. These are protected by the CRC field of the data packet and any packets with bad CRCs are discarded. Recovery from these lost packets is in accordance with the upper layer protocol.

C.11.5.1 Prevention of unauthorized transmissions

A CM SHOULD include a means for terminating RF transmission if it detects that its own carrier has been on continuously for longer than the longest possible valid transmission.

C.12 Supporting future new cable modem capabilities

C.12.1 Downloading cable modem operating software

A CMTS SHOULD be capable of being remotely reprogrammed in the field via a software download via the network.

The cable modem MUST be capable of being remotely reprogrammed in the field via a software download over the network. This software download capability MUST allow the functionality of the cable modem to be changed without requiring that cable system personnel physically revisit and reconfigure each unit. It is expected that this field programmability will be used to upgrade cable modem software to improve performance, accommodate new functions and features (such as enhanced class of service support), correct any design deficiencies discovered in the software, and to allow a migration path as the Data-Over-Cable Interface Specification evolves.

The mechanism used for download MUST be TFTP file transfer. The transfer MUST be initiated in one of two ways:

- an SNMP manager requests the CM to upgrade;
- if the Software Upgrade File Name in the CM's configuration file does not match the current software image of the CM, the CM MUST request the specified file via TFTP from the Software Server.

The Software Server IP Address is a separate parameter. If present, the CM MUST attempt to download the specified file from this server. If not present, the CM MUST attempt to download the specified file from the configuration file server.

The CM MUST verify that the downloaded image is appropriate for itself. If the image is appropriate, the CM MUST write the new software image to non-volatile storage. Once the file transfer is completed successfully, the CM MUST restart itself with the new code image.

If the CM is unable to complete the file transfer for any reason, it MUST remain capable of accepting new software downloads (without operator or user interaction), even if power or connectivity is interrupted between attempts. The CM MUST log the failure and MAY report it asynchronously to the network manager.

Following upgrade of the operational software, the CM MAY need to follow one of the procedures described above in order to change channels to use the enhanced functionality.

If the CM is to continue to operate in the same upstream and downstream channels as before the upgrade, then it MUST be capable of inter-working with other CMs which may be running previous releases of software.

Where software has been upgraded to meet a new version of the specification, then it is critical that it MUST inter-work with the previous version in order to allow a gradual transition of units on the network.

Annex C.A

Well-known addresses

C.A.1 MAC Addresses

MAC addresses described here are defined using the Ethernet/ISO/IEC8802-3 convention as bit-little-endian.

The following multicast address MUST be used to address the set of all CM MAC sublayers; for example, when transmitting Allocation Map PDUs.

01-E0-2F-00-00-01

The address range,

01-E0-2F-00-00-03 through 01-E0-2F-00-00-0F

is reserved for future definition. Frames addressed to any of these addresses SHOULD NOT be forwarded out of the MAC-sublayer domain.

C.A.2 MAC service IDs

The following MAC Service IDs have assigned meanings. Those not included in the following subclauses are available for assignment, either by the CMTS or administratively.

C.A.2.1 CMs and no CM service IDs

These Service IDs are used in MAPs for special purposes or to indicate that any CM can respond in the corresponding interval.

0x0000 Addressed to no CM. Typically used when changing upstream burst parameters so that CMs have time to adjust their modulators before the new upstream settings are in effect.

0x3FFF Addressed to all CMs. Typically used for broadcast Request intervals or Initial Maintenance intervals.

C.A.2.2 Well-known "Multicast" service IDs

These Service IDs are only used for Request/Data IE's. They indicate that any CM can respond in a given interval, but that it must limit the size of its transmission to a particular number of mini-slots (as indicated by the particular multicast SID assigned to the interval).

0x3FF1-0x3FFE Addressed to all CMs. Available for small data PDUs, as well as requests (used only with request/data IEs). The last digit indicates the frame length and transmission opportunities as follows:

0x3FF1 Within the interval specified, a transmission may start at any mini-slot, and must fit within one mini-slot.

0x3FF2 Within the interval specified, a transmission may start at every other mini-slot, and must fit within two mini-slots (e.g., a station may start transmission on the first mini-slot within the interval, the third mini-slot, the fifth, etc.).

0x3FF3 Within the interval specified, a transmission MAY start at any third mini-slot, and must fit within three mini-slots (e.g., starts at first, fourth, seventh, etc.).

0x3FF4 Starts at first, fifth, ninth, etc.

0x3FFD Starts at first, fourteenth (14th), twenty-seventh (27th), etc.

0x3FFE Within the interval specified, a transmission may start at any 14th mini-slot, and must fit within 14 mini-slots.

C.A.2.3 Priority request service IDs

These Service IDs (0x3Exx) are reserved for Request IEs (refer to C.C.2.2.5.2).

– 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.

Bits can be combined as desired by the CMTS upstream scheduler for any Request IUCs.

C.A.3 MPEG PID

All Annex C/J.112 data MUST be carried in MPEG-2 packets with the header PID field set to 0x1FFE.

Annex C.B

Parameters and constants

System	Name	Time reference	Minimum value	Default value	Maximum value
CMTS	Sync Interval	Nominal time between transmission of SYNC messages (see C.8.3.2).			200 ms
CMTS	UCD Interval	Time between transmission of UCD messages (see C.8.3.3).			2 s
CMTS	Max MAP Pending	The number of mini-slots that a CMTS is allowed to map into the future (see C.8.3.4).			4096 mini-slot times
CMTS	Ranging Interval	Time between transmission of broadcast Ranging requests (see C.9.3.3).			2 s
CM	Lost Sync Interval	Time since last received Sync message before synchronization is considered lost.			600 ms
CM	Contention Ranging Retries	Number of retries on contention Ranging Requests (see C.11.2.4).	16		

System	Name	Time reference	Minimum value	Default value	Maximum value
CM, CMTS	Invited Ranging Retries	Number of retries on inviting Ranging Requests (see C.11.2.4).		16	
CM	Request Retries	Number of retries on bandwidth allocation requests.		16	
CM CMTS	Registration Request/Response Retries	Number of retries on registration requests/responses.		3	
CM	Data Retries	Number of retries on immediate data transmission.		16	
CMTS	CM MAP processing time	Time provided between arrival of the last bit of a MAP at a CM and effectiveness of that MAP (see C.9.1.1).	200 µs		
CMTS	CM Ranging Response processing time	Minimum time allowed for a CM following receipt of a ranging response before it is expected to reply to an invited ranging request.	1 ms		
CMTS	CM Configuration	The maximum time allowed for a CM, following receipt of a configuration file, to send a Registration Request to a CMTS.	30 s		
CM	T1	Wait for UCD timeout.			5 × UCD interval maximum value
CM	T2	Wait for broadcast ranging timeout.			5 × ranging interval
CM	T3	Wait for ranging response.	50 ms	200 ms	200 ms
CM	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 s		35 s
CMTS	T5	Wait for Upstream Channel Change response.			2 s
CM CMTS	T6	Wait for REG-RSP and REG-ACK.			3 s
CM CMTS	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		
CM CMTS	Timebase Tick	System timing unit.		6.94 µs	

System	Name	Time reference	Minimum value	Default value	Maximum value
CM CMTS	DSx Request Retries	Number of Timeout retries on DSA/DSC/DSD Requests.	3		
CM CMTS	DSx Response Retries	Number of Timeout retries on DSA/DSC/DSD Responses.	3		
CM CMTS	T7	Wait for DSA/DSC/DSD Response timeout.			1 s
CM CMTS	T8	Wait for DSA/DSC Acknowledge timeout.			300 ms
CM	TFTP Backoff Start	Initial value for TFTP backoff.	1 s		
CM	TFTP Backoff End	Last value for TFTP backoff.	16 s		
CM	TFTP Request Retries	Number of retries on TFTP request.	16		
CM	TFTP Download Retries	Number of retries on entire TFTP downloads.	3		
CM	TFTP Wait	The wait between TFTP retry sequences.	10 min		
CM	ToD Retries	Number of retries per ToD Retry Period.	3		
CM	ToD Retry Period	Time period for ToD retries.	5 min		
CMTS	T9	Registration Timeout, the time allowed between the CMTS sending a RNG-RSP (success) to a CM, and receiving a REG-REQ from that same CM.	15 min	15 min	
CM CMTS	T10	Wait for Transaction End timeout.			3 s
CMTS	T11	Wait for a DCC Response on the old channel.			300 ms
CM	T12	Wait for a DCC Acknowledge.			300 ms
CMTS	T13	Maximum holding time for QOS resources for DCC.			1 s
CM	T14	Minimum time after a DSx reject-temp-DCC and the next retry of DSx command.	2 s		
CMTS	DCC-REQ Retries	Number of retries on Dynamic Channel Change Request.	3		
CM	DCC-RSP Retries	Number of retries on Dynamic Channel Change Response.	3		
CM	Lost DCI-REQ interval	Time from sending DCI-REQ and not receiving a DCI-RSP.			2 s
CM	DCI-REQ retry	Number of retries of DCI-REQ before rebooting.			16
CM	DCI Backoff start	Initial value for DCI backoff.	1 s		
CM	DCI Backoff end	Last value for DCI backoff.	16 s		

Annex C.C

Common radio frequency interface encodings

C.C.1 Encodings for configuration and MAC-layer messaging

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

The following configuration settings MUST be supported by all CMs which are compliant with this annex.

C.C.1.1 Configuration file and registration settings

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

C.C.1.1.1 Downstream frequency configuration setting

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

Type	Length	Value
1	4	Rx Frequency

Valid Range

The receive frequency MUST be a multiple of 62 500 Hz.

C.C.1.1.2 Upstream channel ID configuration setting

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

Type	Length	Value
2	1	Channel ID

C.C.1.1.3 Network access control object

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

Type	Length	On/Off
3	1	1 or 0

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

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

In revised Annex C/J.112, with NACO off, the primary upstream and primary downstream service flows of the CM remain operational only for management traffic to and from the CM. With respect to revised Annex C/J.112 provisioning, a CMTS should ignore the NACO value and allocate any service flows that have been authorized by the provisioning server.

C.C.1.1.4 Previous Annex C/J.112 Class of Service Configuration Setting

This field defines the parameters associated with a previous Annex C/J.112 class of service. Any CM registering with a previous Annex C/J.112 Class of Service Configuration Setting MUST be treated as a previous Annex C/J.112 CM. Refer to C.8.3.8.

This field defines the parameters associated with a class of service. It is somewhat complex in that is composed from a number of encapsulated type/length/value fields. The encapsulated fields define the particular class of service parameters for the class of service in question. Note that the type fields defined are only valid within the encapsulated class of service configuration setting string. A single class of service configuration setting is used to define the parameters for a single service class. Multiple class definitions use multiple class of service configuration setting sets.

Type	Length	Value
4	N	

C.C.1.1.4.1 Class ID

The value of the field specifies the identifier for the class of service to which the encapsulated string applies.

Type	Length	Value
4.1	1	

Valid Range

The class ID MUST be in the range 1 to 16.

C.C.1.1.4.2 Maximum downstream rate configuration setting

For a single SID modem, the value of this field specifies the maximum downstream rate in bits per second that the CMTS is permitted to forward to CPE unicast MAC addresses learned or configured as mapping to the registering modem.

For a multiple SID modem, the aggregate value of these fields specifies the maximum downstream rate in bits per second that the CMTS is permitted to forward to CPE unicast MAC addresses learned or configured as mapping to the registering modem.

This is the peak data rate for Packet PDU Data (including destination MAC address and the CRC) over a one-second interval. This does not include MAC packets addressed to broadcast or multicast MAC addresses. The CMTS MUST limit downstream forwarding to this rate. The CMTS MAY delay, rather than drop, over-limit packets.

Type	Length	Value
4.2	4	

NOTE – This is a limit, not a guarantee that this rate is available.

C.C.1.1.4.3 Maximum upstream rate configuration setting

The value of this field specifies the maximum upstream rate in bits per second that the CM is permitted to forward to the RF Network.

This is the peak data rate for Packet PDU Data (including destination address and the CRC) over a one-second interval. The CM MUST limit all upstream forwarding (both contention and reservation-based), for the corresponding SID, to this rate. The CM MUST include Packet PDU Data packets addressed to broadcast or multicast addresses when calculating this rate.

The CM MUST enforce the maximum upstream rate. It SHOULD NOT discard upstream traffic simply because it exceeds this rate.

The CMTS MUST enforce this limit on all upstream data transmissions, including data sent in contention. The CMTS SHOULD generate an alarm if a modem exceeds its allowable rate.

Type	Length	Value
4.3	4	

NOTE – The purpose of this parameter is for the CM to perform traffic shaping at the input to the RF network and for the CMTS to perform traffic policing to ensure that the CM does not exceed this limit.

The CMTS could 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;

c) discarding over-limit data packets;

d) reporting to a policy monitor (for example, using the alarm mechanism) that is capable of incapacitating errant CMs.

NOTE – This is a limit, not a guarantee that this rate is available.

C.C.1.1.4.4 Upstream channel priority configuration setting

The value of the field specifies the relative priority assigned to this service class for data transmission in the upstream channel. Higher numbers indicate higher priority.

Type	Length	Value
4.4	1	Rx Frequency

Valid Range

$0 \rightarrow 7$

C.C.1.1.4.5 Guaranteed minimum upstream channel data rate configuration setting

The value of the field specifies the data rate in bit/s which will be guaranteed to this service class on the upstream channel.

Type	Length	Value
4.5	4	

C.C.1.1.4.6 Maximum upstream channel transmit burst configuration setting

The value of the field specifies the maximum transmit burst (in bytes) which this service class is allowed on the upstream channel. A value of zero means there is no limit.

NOTE – This value does not include any physical layer overhead.

Type	Length	Value
4.6	2	

C.C.1.1.4.7 Class-of-Service privacy enable

This configuration setting enables/disables Baseline Privacy on a provisioned CoS.

Type	Length	Enable/Disable
4.7 (= CoS_BP_ENABLE)	1	1 or 0

Table C.C-1/J.112 – Sample previous annex C/J.112 Class of Service encoding

Type	Length	Value (sub)type	Length	Value	
4	28				**Class of service configuration setting**
		1	1	1	Service class 1
		2	4	10 000 000	Max. downstream rate of 10 Mbit/s
		3	4	300 000	Max. upstream rate of 300 kbit/s
		4	1	5	Return path priority of 5
		5	4	64 000	Min guaranteed 64 kbit/s
		6	2	1518	Max. Tx burst of 1518 bytes
4	28				**Class of service configuration setting**
		1	1	2	Service class 2
		2	4	5 000 000	Max. forward rate of 5 Mbit/s
		3	4	300 000	Max. return rate of 300 Mbit/s
		4	1	3	Return path priority of 3
		5	4	32 000	Min guaranteed 32 kbit/s
		6	2	1518	Max. Tx burst of 1518 bytes

C.C.1.1.5 CM Message Integrity Check (MIC) configuration setting

The value field contains the CM 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

C.C.1.1.6 CMTS Message Integrity Check (MIC) configuration setting

The value field contains the CMTS 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

C.C.1.1.7 Maximum number of CPEs

The maximum number of CPEs that can be granted access through a CM during a CM epoch. The CM epoch is (from C.5.1.2.3.1) the time between startup and hard reset of the modem. The maximum number of CPE's MUST be enforced by the CM.

NOTE – This parameter should not be confused with the number of CPE addresses a CM may learn. A modem may learn Ethernet MAC addresses up to its maximum number of CPE addresses (from C.5.1.2.3.1). The maximum number of CPEs that are granted access through the modem is governed by this configuration setting.

Type	Length	Value
18	1	

The CM MUST interpret this value as an unsigned integer. The non-existence of this option, or the value 0, MUST be interpreted as the default value of 1.

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

C.C.1.1.8 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.

C.C.1.1.9 TFTP server provisioned modem address

The IP Address of the modem requesting the configuration file.

Type	Length	Value
20	4	IP Address

NOTE – The purpose of this parameter is to prevent IP spoofing during registration.

C.C.1.1.10 Upstream packet classification configuration setting

This field defines the parameters associated with one entry in an upstream traffic classification list. Refer to C.C.2.1.1.

Type	Length	Value
22	n	

C.C.1.1.11 Downstream packet classification configuration setting

This field defines the parameters associated with one Classifier in an downstream traffic classification list. Refer to C.C.2.1.2.

Type	Length	Value
23	n	

C.C.1.1.12 Upstream service flow encodings

This field defines the parameters associated with upstream scheduling for one Service Flow. Refer to C.C.2.2.1.

Type	Length	Value
24	n	

C.C.1.1.13 Downstream service flow encodings

This field defines the parameters associated with downstream scheduling for one Service Flow. Refer to C.C.2.2.2.

Type	Length	Value
25	n	

C.C.1.1.14 Payload header suppression

This field defines the parameters associated with Payload Header Suppression.

Type	Length	Value
26	n	

C.C.1.1.15 Maximum number of classifiers

This is the maximum number of Classifiers that the CM is allowed to have admitted.

This is necessary when using deferred activation since the number of provisioned Service Flows may be high and since each Service Flow might support multiple Classifiers. Provisioning represents the set of Service Flows the CM can choose between, however, it may still be desirable to limit the number of simultaneously admitted Classifiers applied to this set. This parameter provides the ability to limit the size of that set.

Type	Length	Value
28	2	Maximum number of simultaneous admitted classifiers

The default value MUST be 0 = no limit.

C.C.1.1.16 Privacy enable

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

Type	Length	Value
29	1	0: Disable 1: Enable

The default value of this parameter MUST be 0 (privacy disabled).

C.C.1.1.17 Vendor-specific information

Vendor-specific information for cable modems, if present, MUST be encoded in the vendor specific information field (VSIF) (code 43) using the Vendor ID field (C.C.1.3.2) to specify which TLV tuples apply to which vendors products. The Vendor ID MUST be the first TLV embedded inside VSIF. If the first TLV inside VSIF is not a Vendor ID, then the TLV MUST be discarded.

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

Type	Length	Value
43	n	per vendor definition

EXAMPLE:

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

VSIF (43) + n (number of bytes inside this VSIF)

8 (Vendor ID Type) + 3 (length field) + Vendor ID of Vendor A

Vendor A Specific Type #1 + length of the field + Value #1

Vendor A Specific Type #2 + length of the field + Value #2

VSIF (43) + m (number of bytes inside this VSIF)

8 (Vendor ID Type) + 3 (length field) + Vendor ID of Vendor B

Vendor B Specific Type + length of the field + Value

C.C.1.1.18 Subscriber management TLVs

The information in these TLVs is not used by the CM; rather, the information is used by the CMTS to populate the Subscriber Management MIB for this CM.

If present in the configuration file, the CM MUST include these TLVs in the subsequent REG-REQ to be used by the CMTS to populate the Subscriber Management MIB for this CM. If present in the configuration file, the CM MUST include these TLVs in the CMTS MIC.

C.C.1.1.18.1 Subscriber management control

This three byte field provides control information to the CMTS for the Subscriber Management MIB. The first two bytes represent the number of IP addresses permitted behind the CM. The third byte is used for control fields.

Type	Length	Value
35	3	Byte 1, 2 docsSubMgtCpeControlMaxCpeIP (low order 10 bits) Byte 3, bit 0: docsSubMgtCpeControlActive Byte 3, bit 1: docsSubMgtCpeControlLearnable Byte 3, bits 2-7: reserved, must be set to zero

C.C.1.1.18.2 Subscriber management CPE IP table

This field lists the IP Addresses used to populate docsSubMgtCpeIpTable in the Subscriber Management MIB at the CMTS.

Type	Length	Value
36	n (multiple of 4)	Ipa1, Ipa2, Ipa3, Ipa4

C.C.1.1.18.3 Subscriber management filter groups

The Subscriber Management MIB allows filter groups to be assigned to a CM and CPE attached to that CM. These include two CM filter groups, upstream and downstream, and two CPE filter groups, upstream and downstream. These four filter groups are encoded in the configuration file in a single TLV as follows:

Type	Length	Value
37	8	Bytes 1, 2: docsSubMgtSubFilterDownstream group Bytes 3, 4: docsSubMgtSubFilterUpstream group Bytes 5, 6: docsSubMgtCmFilterDownstream group Bytes 7, 8: docsSubMgtCmFilterUpstream group

C.C.1.2 Configuration-file-specific settings

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

C.C.1.2.1 End-of-data marker

This is a special marker for end of data.

It has no length or value fields.

Type	Length	Value
255		

C.C.1.2.2 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	Length	Value
0		

C.C.1.2.3 Software upgrade filename

The filename of the software upgrade file for the CM. 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 C.D.2.2. See C.12.1.

Type	Length	Value
9	n	Filename

C.C.1.2.4 SNMP write-access control

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

Type	Length	Value
10	n	OID prefix plus control flag

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

The control flag may take values:

0: Allow write-access;

1: Disallow write-access.

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

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

someTable	disallow write-access
someTable 1.3	allow write-access

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

C.C.1.2.5 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 cable modem MUST treat this object as if it were part of an SNMP Set Request with the following caveats:

- It MUST treat the request as fully authorized (it cannot refuse the request for lack of privilege);
- SNMP Write-Control provisions (see C.C.1.2.4) do not apply;
- No SNMP response is generated by the CM.

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

Each VarBind MUST be limited to 255 bytes.

C.C.1.2.6 CPE ethernet MAC address

This object configures the CM with the Ethernet MAC address of a CPE device (see C.5.1.2.3.1). This object may be repeated to configure any number of CPE device addresses.

Type	Length	Value
14	6	Ethernet MAC Address of CPE

C.C.1.2.7 Software upgrade TFTP server

The IP address of the TFTP server, on which the software upgrade file for the CM resides. See C.12.1 and C.C.1.2.3.

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

C.C.1.2.8 SnmpV3 kickstart value

Compliant CMs MAY understand the following TLV and its subelements and be able to kickstart SNMPv3 access to the CM regardless of whether the CMs are operating in Previous Annex C/J.112 mode or Revised Annex C/J.112 mode.

Type	Length	Value
34	n	Composite

Up to 5 of these objects may be included in the configuration file. Each results in an additional row being added to the usmDHKickstartTable and the usmUserTable and results in an agent public number being generated for those rows.

C.C.1.2.8.1 SnmpV3 kickstart security name

Type	Length	Value
34.1	2-16	UTF8 Encoded security name

For the ASCII character set, the UTF8 and the ASCII encodings are identical. Normally, this will be specified as one of the built-in USM users. The security name is NOT zero terminated. This is reported in the usmDHKickStartTable as usmDHKickStartSecurityName and in the usmUserTable as usmUserName and usmUserSecurityName.

C.C.1.2.8.2 SnmpV3 kickstart manager public number

Type	Length	Value
34.2	n	Manager's Diffie-Helman public number expressed as an octet string

This number is the Diffie-Helman public number derived from a privately (by the manager or operator) generated random number and transformed according to [RFC 2786]. This is reported in the usmDHKickStartTable as usmKickstartMgrPublic. When combined with the object reported in the same row as usmKickstartMyPublicit, it can be used to derive the keys in the related row in the usmUserTable.

C.C.1.2.9 Manufacturer code verification certificate

The Manufacturer's Code Verification Certificate (M-CVC) for Secure Software Downloading specified by Appendix D of SP-BPI+-I05-000714. The CM config file MAY contain this M-CVC and/or C-CVC defined in C.C.1.2.10 in order to allow the Revised Annex C/J.112 compliant CM to download the code file from TFTP server when the CM is provisioned to run with BPI+.

Type	Length	Value
32	n	Manufacturer CVC (DER-encoded ASN.1)

If the length of the M-CVC exceeds 254 bytes, the M-CVC MUST be fragmented into two or more successive Type 32 elements. Each fragment, except the last, MUST be 254 bytes in length. The CM reconstructs the M-CVC by concatenating the contents (Value of the TLV) of successive Type 32 elements in the order in which they appear in the config file. For example, the first byte following the length field of the second Type 32 element is treated as if it immediately follows the last byte of the first Type 32 element.

C.C.1.2.10 Co-signer code verification certificate

The Co-signer's Code Verification Certificate (C-CVC) for Secure Software Downloading specified by Appendix D of SP-BPI+-I05-000714. The CM config file MAY contain this C-CVC and/or M-CVC defined in C.C.1.2.9 in order to allow the Revised Annex C/J.112 compliant CM to download the code file from TFTP server when the CM is provisioned to run with BPI+.

Type	Length	Value
33	n	Co-signer CVC (DER-encoded ASN.1)

If the length of the C-CVC exceeds 254 bytes, the C-CVC MUST be fragmented into two or more successive Type 33 elements. Each fragment, except the last, MUST be 254 bytes in length. The CM reconstructs the C-CVC by concatenating the contents (Value of the TLV) of successive Type 33 elements in the order in which they appear in the config file. For example, the first byte following the length field of the second Type 33 element is treated as if it immediately follows the last byte of the first Type 33 element.

C.C.1.3 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 CM MUST include Modem Capabilities Encodings in its Registration Request. If present in the corresponding Registration Request, the CMTS MUST include Modem Capabilities in the Registration Response.

C.C.1.3.1 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 subtypes define the specific capabilities for the modem in question. Note that the subtype 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.

C.C.1.3.1.1 Concatenation support

If the value field is a 1 the CM requests concatenation support from the CMTS.

Type	Length	Value
5.1	1	1 or 0

C.C.1.3.1.2 Annex C/J.112 version

Annex C/J.112 version of this modem.

Type	Length	Value
5.2	1	0: PRE_C(Previous Annex C/J.112) 1: REV_C(Revised Annex C/J.112) 2-255: Reserved

If this tuple is absent, the CMTS MUST assume previous Annex C/J.112 operation. The absence of this tuple or the value 'Previous Annex C/J.112' does not necessarily mean the CM only supports previous Annex C/J.112 functionality; the CM MAY indicate it supports other individual capabilities with other Modem Capability Encodings. (Refer to clause C.G.3.)

C.C.1.3.1.3 Fragmentation support

If the value field is a 1 the CM requests fragmentation support from the CMTS.

Type	Length	Value
5.3	1	1 or 0

C.C.1.3.1.4 Payload header suppression support

If the value field is a 1 the CM requests payload header suppression support from the CMTS.

Type	Length	Value
5.4	1	1 or 0

C.C.1.3.1.5 IGMP support

If the value field is a 1 the CM supports revised Annex C/J.112-compliant IGMP.

Type	Length	Value
5.5	1	1 or 0

C.C.1.3.1.6 Privacy support

The value is the BPI support of the CM.

Type	Length	Value
5.6	1	0 BPI Support 1 BPI Plus Support(option) 2-255 Reserved

C.C.1.3.1.7 Downstream SAID support

The field shows the number of Downstream SAIDs the modem can support.

Type	Length	Value
5.7	1	Number of Downstream SAIDs the CM can support

If the number of SAIDs is 0 that means the Modem can support only 1 SAID.

C.C.1.3.1.8 Upstream SID support

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

Type	Length	Value
5.8	1	Number of Upstream SIDs the CM can support

If the number of SIDs is 0 that means the Modem can support only 1 SID.

C.C.1.3.1.9 Optional filtering support

The fields show the optional filtering support in the modem.

Type	Length	Value
5.9	1	Packet Filtering Support Array bit #0: 802.1P filtering bit #1: 802.1Q filtering bit #2-7: reserved, MUST be set to zero

C.C.1.3.1.10 Transmit equalizer taps per symbol

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

NOTE – All CMs MUST support symbol-spaced equalizer coefficients. CM support of 2 or 4 taps per symbol is optional. If this tuple is missing, it is implied that the CM only supports symbol spaced equalizer coefficients.

Type	Length	Value
5.10	1	1, 2 or 4

C.C.1.3.1.11 Number of transmit equalizer taps

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

NOTE – All CMs MUST support an equalizer length of at least 8 symbols. CM 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 CM only supports an equalizer length of 8 taps.

Type	Length	Value
5.11	1	8 to 64

C.C.1.3.1.12 DCC support

The value is the DCC support of the CM.

Type	Length	Value
5.12	1	0 = DCC is not supported 1 = DCC is supported

C.C.1.3.2 Vendor ID encoding

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

The Vendor ID MUST be used in a Registration Request, but MUST NOT be used as a stand-alone configuration file element. It MAY be used as a subfield of the Vendor Specific Information Field in a configuration file. When used as a subfield of the Vendor Specific Information field, this identifies the Vendor ID of the CMs 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 CM sending the request.

Type	Length	Value
8	3	v1, v2, v3

C.C.1.3.3 Modem IP address

For backwards compatibility with previous Annex C/J.112. Replaced by "TFTP Server Provisioned Modem Address".

Type	Length	Value
12	4	IP Adress

C.C.1.3.4 Service(s) not available response

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

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

Where:

Class ID is the class-of-service class from the request which is not available;

Type is the specific class-of-service object within the class which caused the request to be rejected;

Confirmation Code: Refer to clause C.C.4.

C.C.1.4 Dynamic-service-message-specific encodings

These encodings are not found in the configuration file, nor in the Registration Request/Response Signalling. They are only found in DSA-REQ, DSA-RSP, DSA-ACK, DSC-REQ, DSC-RSP, DSC-ACK, and DSD-REQ messages (C.8.3.12 through C.8.3.18).

C.C.1.4.1 HMAC-digest

The HMAC-Digest setting is a keyed message digest. If privacy is enabled, the HMAC-Digest Attribute MUST be the final Attribute in the Dynamic Service message's Attribute list. The message digest is performed over 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 "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I05-000714".

This parameter contains a keyed hash used for message authentication. The HMAC algorithm is defined in [RFC 2104]. 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

C.C.1.4.2 Authorization block

The Authorization Block contains an authorization "hint" from the CM to the CMTS. The specifics of the contents of this "hint" are beyond the scope of this annex, but include "PacketCable Specifications, Dynamic Quality of Service Specification, PKT-SP-DQOS-I01-991201".

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

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

Type	Length	Value
30	n	Sequence of n octets

C.C.1.4.3 Key sequence number

The value shows the key sequence number of the BPI+ Authorization Key which is used to calculate the HMAC-Digest in case that the Privacy is enabled.

Type	Length	Value
31	1	Auth Key Sequence Number (0-15)

C.C.2 Quality-of-Service-related encodings

C.C.2.1 Packet classification encodings

The following type/length/value encodings MUST be used in both the configuration file, registration messages, and Dynamic Service messages to encode parameters for packet classification and scheduling. 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.

A classifier MUST contain at least one encoding from C.C.2.1.5 "IP packet classification encodings", C.C.2.1.6 "Ethernet LLC packet classification encodings", or C.C.2.1.7 "IEEE 802.1P/Q packet classification encodings".

The following configuration settings MUST be supported by all CMs which are compliant with this annex.

C.C.2.1.1 Upstream packet classification encoding

This field defines the parameters associated with an upstream Classifier.

Note that the same subtype fields defined are valid for both the encapsulated upstream and downstream packet classification configuration setting string. These type fields are not valid in other encoding contexts.

Type	Length	Value
22	n	

C.C.2.1.2 Downstream packet classification encoding

This field defines the parameters associated with a downstream Classifier.

Note that the same subtype fields defined are valid for both the encapsulated upstream and downstream flow classification configuration setting string. These type fields are not valid in other encoding contexts.

Type	Length	Value
23	n	

C.C.2.1.3 General packet classifier encodings

C.C.2.1.3.1 Classifier reference

The value of the field specifies a reference for the Classifier. This value is unique per Dynamic Service message, configuration file, or Registration Request message.

Type	Length	Value
[22/23].1	1	1-255

C.C.2.1.3.2 Classifier identifier

The value of the field specifies an identifier for the Classifier. This value is unique per Service Flow. The CMTS assigns the Packet Classifier Identifier.

Type	Length	Value
[22/23].2	2	1-65 535

C.C.2.1.3.3 Service flow reference

The value of the field specifies a Service Flow Reference that identifies the corresponding Service Flow.

In all Packet Classifier TLVs that occur in any message where the Service Flow ID is not known (e.g. CM- initiated DSA-REQ and REG-REQ) this TLV MUST be included. In all Packet Classifier TLVs that occur in a DSC-REQ and CMTS-initiated DSA-REQ messages the Service Flow Reference MUST NOT be specified.

Type	Length	Value
[22/23].3	2	1-65 535

C.C.2.1.3.4 Service flow identifier

The value of this field specifies the Service Flow ID that identifies the corresponding Service Flow.

In Packet Classifier TLVs where the Service Flow ID is not known, and this TLV MUST NOT be included (e.g. CM-initiated DSA-REQ and REG-REQ). In Packet Classifier TLVs that occur in a DSC-REQ and CMTS- initiated DSA-REQ message, the Service Flow ID MUST be specified.

Type	Length	Value
[22/23].4	4	1-4 294 967 295

C.C.2.1.3.5 Rule priority

The value of the field specifies the priority for the Classifier, which is used for determining the order of the Classifier. A higher value indicates higher priority.

Classifiers that appear in Configuration files and Registration messages MAY have priorities in the range 0 to 255 with the default value 0. Classifiers that appear in DSA/DSC message MUST have priorities in the range 64 to 191, with the default value 64.

Type	Length	Value
[22/23].5	1	

C.C.2.1.3.6 Classifier activation state

The value of this field specifies whether this classifier should become active in selecting packets for the Service Flow. An inactive Classifier is typically used with an AdmittedQoSParameterSet to ensure resources are available for later activation. The actual activation of the classifier depends both on this attribute and on the state of its service flow. If the service flow is not active then the classifier is not used, regardless of the setting of this attribute.

Type	Length	Value
[22/23].6	1	0: Inactive 1: Active

The default value is 1: activate the classifier.

C.C.2.1.3.7 Dynamic service change action

When received in a Dynamic Service Change Request, this indicates the action that should be taken with this classifier.

Type	Length	Value
[22/23].7	1	0: DSC Add Classifier 1: DSC Replace Classifier 2: DSC Delete Classifier

C.C.2.1.4 Classifier error encodings

This field defines the parameters associated with Classifier Errors.

Type	Length	Value
[22/23].8	n	

A Classifier Error Encoding consists of a single Classifier Error Parameter Set which is defined by the following individual parameters: Errored Parameter, Confirmation Code and Error Message.

The Classifier Error Encoding is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the reason for the recipient's negative response to a Classifier establishment request in a REG-REQ, DSA-REQ or DSC-REQ message.

On failure, the REG-RSP, DSA-RSP or DSC-RSP MUST include one Classifier Error Encoding for at least one failed Classifier requested in the REG-REQ, DSA-REQ or DSC-REQ message. A Classifier Error Encoding for the failed Classifier MUST include the Confirmation Code and Errored Parameter and MAY include an Error Message. If some Classifier Sets are rejected but other Classifier Sets are accepted, then Classifier Error Encodings MUST be included for only the rejected Classifiers. On success of the entire transaction, the RSP or ACK message MUST NOT include a Classifier Error Encoding.

Multiple Classifier Error Encodings may appear in a REG-RSP, DSA-RSP or DSC-RSP message, since multiple Classifier parameters may be in error. A message with even a single Classifier Error Encoding MUST NOT contain any other protocol Classifier Encodings (e.g. IP, IEEE 802.1P/Q).

A Classifier Error Encoding MUST NOT appear in any REG-REQ, DSA-REQ or DSC-REQ messages.

C.C.2.1.4.1 Errored parameter

The value of this parameter identifies the subtype of a requested Classifier parameter in error in a rejected Classifier request. A Classifier Error Parameter Set MUST have exactly one Errored Parameter TLV within a given Classifier Error Encoding.

Type	Length	Value
[22/23].8.1	n	Classifier Encoding Subtype in Error

If the length is one, then the value is the single-level subtype where the error was found, e.g. "7" indicates an invalid Change Action. If the length is two, then the value is the multi-level subtype where there error was found e.g. "9-2" indicates an invalid IP Protocol value.

C.C.2.1.4.2 Error code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in clause C.C.4. A Classifier Error Parameter Set MUST have exactly one Error Code within a given Classifier Error Encoding.

Type	Length	Value
[22/23].8.2	1	Confirmation code

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

C.C.2.1.4.3 Error message

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

Subtype	Length	Value
[22/23].8.3	n	Zero-terminated string of ASCII characters

NOTE – The length n includes the terminating zero.

The entire Classifier Encoding message MUST have a total length of less than 256 characters.

C.C.2.1.5 IP packet classification encodings

This field defines the parameters associated with IP packet classification.

Type	Length	Value
[22/23].9	n	

C.C.2.1.5.1 IP Type of Service range and mask

The values of the field specify the matching parameters for the IP ToS byte range and mask. An IP packet with IP ToS byte value "ip-tos" matches this parameter if tos-low ≤ (ip-tos AND tos-mask) ≤ tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.

Type	Length	Value
[22/23].9.1	3	tos-low, tos-high, tos-mask

C.C.2.1.5.2 IP protocol

The value of the field specifies the matching value for the IP Protocol field [RFC 1700]. If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

There are two special IP Protocol field values: "256" matches traffic with any IP Protocol value, and "257" matches both TCP and UDP traffic. An entry that includes an IP Protocol field value greater than 257 MUST be invalidated for comparisons (i.e. no traffic can match this entry).

Type	Length	Value
[22/23].9.2	2	prot1, prot2

Valid Range

0-257

C.C.2.1.5.3 IP source address

The value of the field specifies the matching value for the IP source address. An IP packet with IP source address "ip-src" matches this parameter if src = (ip-src AND smask), where "smask" is the parameter from C.C.2.1.5.4. If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.

Type	Length	Value
[22/23].9.3	4	src1, src2, src3, src4

C.C.2.1.5.4 IP source mask

The value of the field specifies the mask value for the IP source address, as described in C.C.2.1.5.3. If this parameter is omitted, then the default IP source mask is 255.255.255.255.

Type	Length	Value
[22/23].9.4	4	smask1, smask2, smask3, smask4

C.C.2.1.5.5 IP destination address

The value of the field specifies the matching value for the IP destination address. An IP packet with IP destination address "ip-dst" matches this parameter if dst = (ip-dst AND dmask), where "dmask" is the parameter from C.C.2.1.5.6. If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.

Type	Length	Value
[22/23].9.5	4	dst1, dst2, dst3, dst4

C.C.2.1.5.6 IP destination mask

The value of the field specifies the mask value for the IP destination address, as described in IP Destination Address. If this parameter is omitted, then the default IP destination mask is 255.255.255.255.

Type	Length	Value
[22/23].9.6	4	dmask1, dmask2, dmask3, dmask4

C.C.2.1.5.7 TCP/UDP source port start

The value of the field specifies the low-end TCP/UDP source port value. An IP packet with TCP/UDP port value "src-port" matches this parameter if sportlow ≤ src-port ≤ sporthigh. If this parameter is omitted, then the default value of sportlow is 0. This parameter is irrelevant for non-TCP/UDP IP traffic.

Type	Length	Value
[22/23].9.7	2	sportlow1, sportlow2

C.C.2.1.5.8 TCP/UDP source port end

The value of the field specifies the high-end TCP/UDP source port value. An IP packet with TCP/UDP port value "src-port" matches this parameter if sportlow ≤ src-port ≤ sporthigh. If this parameter is omitted, then the default value of sporthigh is 65 535. This parameter is irrelevant for non-TCP/UDP IP traffic.

Type	Length	Value
[22/23].9.8	2	sporthigh1, sporthigh2

C.C.2.1.5.9 TCP/UDP destination port start

The value of the field specifies the low-end TCP/UDP destination port value. An IP packet with TCP/UDP port value "dst-port" matches this parameter if dportlow ≤ dst-port ≤ dporthigh. If this parameter is omitted, then the default value of dportlow is 0. This parameter is irrelevant for non-TCP/UDP IP traffic.

Type	Length	Value
[22/23].9.9	2	dportlow1, dportlow2

C.C.2.1.5.10 TCP/UDP destination port end

The value of the field specifies the high-end TCP/UDP destination port value. An IP packet with TCP/UDP port value "dst-port" matches this parameter if dportlow ≤ dst-port ≤ dporthigh. If this parameter is omitted, then the default value of dporthigh is 65 535. This parameter is irrelevant for non-TCP/UDP IP traffic.

Type	Length	Value
[22/23].9.10	2	dporthigh1, dporthigh2

C.C.2.1.6 Ethernet LLC packet classification encodings

This field defines the parameters associated with Ethernet LLC packet classification.

Type	Length	Value
[22/23].10	n	

C.C.2.1.6.1 Destination MAC address

The values of the field specifies the matching parameters for the MAC destination address. An Ethernet packet with MAC destination address "etherdst" matches this parameter if dst = (etherdst AND msk). If this parameter is omitted, then comparison of the Ethernet MAC destination address for this entry is irrelevant.

Type	Length	Value
[22/23].10.1	12	dst1, dst2, dst3, dst4, dst5, dst6, msk1, msk2, msk3, msk4, msk5, msk6

C.C.2.1.6.2 Source MAC address

The value of the field specifies the matching value for the MAC source address. If this parameter is omitted, then comparison of the Ethernet MAC source address for this entry is irrelevant.

Type	Length	Value
[22/23].10.2	6	src1, src2, src3, src4, src5, src6

C.C.2.1.6.3 Ethertype/DSAP/MacType

type, eprot1, and eprot2 indicate the format of the layer 3 protocol ID in the Ethernet packet as follows:

If type = 0, the rule does not use the layer 3 protocol type as a matching criteria. If type = 0, eprot1, eprot2 are ignored when considering whether a packet matches the current rule.

If type = 1, the rule applies only to frames which contain an Ethertype value. Ethertype values are contained in packets using the DEC-Intel-Xerox (DIX) encapsulation or the [RFC 1042] Sub-Network Access Protocol (SNAP) encapsulation formats. If type = 1, then eprot1, eprot2 gives the 16 bit value of the Ethertype that the packet must match in order to match the rule

If type = 2, the rule applies only to frames using the IEEE 802.2 encapsulation format with a Destination Service (DSAP) other than 0xAA (which is reserved for SNAP). If type = 2, the lower 8 bits of the eprot1, eprot2, MUST match the DSAP byte of the packet in order to match the rule.

If type = 3, the rule applies only to MAC Management Messages (FC field 1100001x) with a "type" field of its MAC Management Message header (C.8.3.1) between the values of eprot1 and eprot2, inclusive. As exceptions, the following MAC Management message types MUST NOT be classified, and are always transmitted on the primary service flow:

Type 4: RNG_REQ

Type 6: REG_REQ

Type 7: REG_RSP

Type 14: REG_ACK

If type = 4, the rule is considered a "catch-all" rule that matches all Data PDU packets. The rule does not match MAC Management Messages. The value of eprot1 and eprot2 are ignored in this case.

If the Ethernet frame contains an IEEE 802.1P/Q Tag header (i.e., Ethertype 0x8100), this object applies to the embedded Ethertype field within the IEEE 802.1P/Q header.

Other values of type are reserved. If this TLV is omitted, then comparison of either the Ethertype or IEEE 802.2 DSAP for this rule is irrelevant.

Type	Length	Value
[22/23].10.3	3	type, eprot1, eprot2

C.C.2.1.7 IEEE 802.1P/Q packet classification encodings

This field defines the parameters associated with IEEE 802.1P/Q packet classification.

Type	Length	Value
[22/23].11	n	

C.C.2.1.7.1 IEEE 802.1P User_Priority

The values of the field specify the matching parameters for the IEEE 802.1P user_priority bits. An Ethernet packet with IEEE 802.1P user_priority value "priority" matches these parameters if pri-low ≤ priority ≤ pri- high. If this field is omitted, then comparison of the IEEE 802.1P user_priority bits for this entry is irrelevant.

If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation MUST NOT match this entry. If this parameter is specified for an entry on a CM that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry MUST NOT be used for any traffic.

Type	Length	Value
[22/23].11.1	2	pri-low, pri-high

Valid Range

0-7 for pri-low and pri-high.

C.C.2.1.7.2 IEEE 802.1Q VLAN_ID

The value of the field specify the matching value for the IEEE 802.1Q vlan_id bits. Only the first (i.e. most-significant) 12 bits of the specified vlan_id field are significant; the final four bits MUST be ignored for comparison. If this field is omitted, then comparison of the IEEE 802.1Q vlan_id bits for this entry is irrelevant.

If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation MUST NOT match this entry. If this parameter is specified for an entry on a CM that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry MUST NOT be used for any traffic.

Type	Length	Value
[22/23].11.2	2	vlan_id1, vlan_id2

C.C.2.1.7.3 Vendor-specific classifier parameters

This allows vendors to encode vendor-specific Classifier parameters. The Vendor ID MUST be the first TLV embedded inside Vendor-Specific Classifier Parameters. If the first TLV inside Vendor-Specific Classifier Parameters is not a Vendor ID, then the TLV MUST be discarded. (Refer to C.C.1.1.17.)

Type	Length	Value
[22/23].43	n	

C.C.2.1.8 Upstream-specific classification encodings

C.C.2.1.8.1 Classifier activation signal

This field MUST only be used in Dynamic Service Change messages that originate from the CMTS and which affect the Active parameter set. It is not present in any other Service Flow Signalling messages.

Type	Length	Value
22.12	1	1: Activate/Deactivate Classifier on Request 2: Activate/Deactivate Classifier on Ack

This field directs the modem to change its upstream transmission characteristics to match those in the DSC either immediately on receiving the DSC-Request, or only after receiving the DSC-Ack. In particular, it signals the time of (de-)activation of any classifiers which are changed by this DSC exchange.

The default value is 2 for a bandwidth increase. The default value is 1 for a bandwidth decrease. If increase or decrease is ambiguous, then the default value is 2.

C.C.2.2 Service flow encodings

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

The following configuration settings MUST be supported by all CMs which are compliant with this annex.

C.C.2.2.1 Upstream service flow encodings

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

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

Type	Length	Value
24	n	

C.C.2.2.2 Downstream service flow encodings

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

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

Type	Length	Value
25	n	

C.C.2.2.3 General service flow encodings

C.C.2.2.3.1 Service flow reference

The Service Flow Reference is used to associate a packet classifier encoding with a Service Flow encoding. A Service Flow Reference is only used to establish a Service Flow ID. Once the Service Flow exists and has an assigned Service Flow ID, the Service Flow Reference MUST no longer be used. The Service Flow Reference is unique per configuration file, Registration message exchange, or Dynamic Service Add message exchange.

Type	Length	Value
[24/25].1	2	1-65 535

C.C.2.2.3.2 Service flow identifier

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

The configuration file MUST NOT contain this parameter.

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

C.C.2.2.3.3 Service identifier

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

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

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

C.C.2.2.3.4 Service class name

The value of the field refers to a predefined CMTS 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 CMTS. It is up to the operator to synchronize the definition of Service Class Names in the CMTS and in the configuration file.

C.C.2.2.4 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 Encoding consists of a single Service Flow Error Parameter Set which is defined by the following individual parameters: Errored Parameter, Confirmation Code, and Error Message.

The Service Flow Error Encoding is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the reason for the recipient's negative response to a Service Flow establishment request in a REG-REQ, DSA-REQ or DSC-REQ message.

The Service Flow Error Encoding is returned in REG-ACK, DSA-ACK and DSC-ACK messages to indicate the reason for the recipient's negative response to the expansion of a Service Class Name in a corresponding REG-RSP, DSA-RSP or DSC-RSP.

On failure, the REG-RSP, DSA-RSP or DSC-RSP MUST include one Service Flow Error Encoding for at least one failed Service Flow requested in the REG-REQ, DSA-REQ or DSC-REQ message. On failure, the REG-ACK, DSA-ACK or DSC-ACK MUST include one Service Flow Error Encoding for at least one failed Service Class Name expansion in the REG-RSP, DSA-RSP or DSC-RSP message. A Service Flow Error Encoding for the failed Service Flow MUST include the

Confirmation Code and Errored Parameter and MAY include an Error Message. If some Service Flow Parameter Sets are rejected but other Service Flow Parameter Sets are accepted, then Service Flow Error Encodings MUST be included for only the rejected Service Flow.

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

Multiple Service Flow Error Encodings 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 Encoding MUST NOT contain any QoS Parameters.

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

C.C.2.2.4.1 Errored parameter

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

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

C.C.2.2.4.2 Error code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in clause C.C.4. A Service Flow Error Parameter Set MUST have exactly one Error Code within a given Service Flow Encoding.

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

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

C.C.2.2.4.3 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 CM 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 Error Encoding.

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

NOTE 1 – The length n includes the terminating zero.

NOTE 2 – The entire Service Flow Encoding message MUST have a total length of less than 256 characters.

C.C.2.2.5 Common upstream and downstream Quality-of-Service parameter encodings

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

C.C.2.2.5.1 Quality of Service parameter set type

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

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

Any Service Flow Encoding that appears in a Dynamic Service Message MUST NOT specify the ProvisionedQoSParameterSet.

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

Table C.C-2/J.112 – 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 on Admitted set in separate Service Flow Encoding, and activate the Service flow
111	Apply to Provisioned, Admitted, and Active sets; perform admission control and activate this Service Flow

Table C.C-3/J.112 – Values ised in REG-REQ, REG-RSP and dynamic service messages

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

The value 000 is used only in Dynamic Service Change messages. It is used to set the Active and Admitted sets to Null (see C.10.1.7.4).

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

C.C.2.2.5.2 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 CMTS SHOULD use this parameter when determining precedence in request service and grant generation, and the CM MUST preferentially select contention Request opportunities for Priority Request Service IDs (refer to C.A.2.3) based on this priority and its Request/Transmission Policy (refer to C.C.2.2.6.3).

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

NOTE – The default priority is 0.

C.C.2.2.5.3 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 (see Note 1). The number of bytes forwarded (in bytes) is limited during any time interval T by Max(T), as described in the expression:

$$\text{Max}(T) = T \times (R/8) + B, \qquad \text{(C.C.2.2.5.3-1)}$$

where the parameter B (in bytes) is the Maximum Traffic Burst Configuration Setting (refer to C.C.2.2.5.4).

NOTE 1 – The payload size includes every PDU in a Concatenated MAC Frame.

NOTE 2 – This parameter does not limit the instantaneous rate of the Service Flow.

NOTE 3 – The specific algorithm for enforcing this parameter is not mandated here. Any implementation which satisfies the above equation is conformant.

NOTE 4 – 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.

C.C.2.2.5.3.1 Upstream maximum sustained traffic rate

For an upstream Service Flow, the CM MUST NOT request bandwidth exceeding the Max(T) requirement in Equation (C.C.2.2.5.3-1) during any interval T because this could force the CMTS to fill MAPs with deferred grants.

The CM MUST defer upstream packets that violate Equation (C.C.2.2.5.3-1) and "rate shape" them to meet the expression, up to a limit as implemented by vendor buffering restrictions.

The CMTS MUST enforce Equation (C.C.2.2.5.3-1) on all upstream data transmissions, including data sent in contention. The CMTS MAY consider unused grants in calculations involving this parameter. The CMTS 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 CMTS MUST report this condition to a policy module. If the CMTS is policing by discarding either packets or requests, the CMTS MUST allow a margin of error between the CM and CMTS algorithms.

Type	Length	Value
[24/25].8	4	R (in bits per second)

C.C.2.2.5.3.2 Downstream maximum sustained traffic rate

For a downstream Service Flow, this parameter is only applicable at the CMTS. The CMTS MUST enforce Equation (C.C.2.2.5.3-1) on all downstream data transmissions. The CMTS MUST NOT forward downstream packets that violates Equation (C.C.2.2.5.3-1) in any interval T. The CMTS SHOULD "rate shape" the downstream traffic by enqueuing packets arriving in excess of Equation (C.C.2.2.5.3-1), and delay them until the expression can be met.

This parameter is not intended for enforcement on the CM.

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

C.C.2.2.5.4 Maximum traffic burst

The value of this parameter specifies the token bucket size B (in bytes) for this Service Flow as described in Equation (C.C.2.2.5.3-1). This value is calculated from the byte following the MAC header HCS to the end of the CRC (see Note 1).

NOTE 1 – The payload size includes every PDU in a Concatenated MAC Frame.

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 C.C.2.2.6.1).

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

NOTE 2 – The specific algorithm for enforcing this parameter is not mandated here. Any implementation which satisfies the above equation is conformant.

C.C.2.2.5.5 Minimum reserved traffic rate

This parameter specifies the minimum rate, in bits/s, reserved for this Service Flow. The CMTS 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 CMTS MAY reallocate the excess reserved bandwidth for other purposes. The aggregate Minimum Reserved Traffic Rate of all Service Flows MAY exceed the amount of available bandwidth. This value of this parameter is calculated from the byte following the MAC header HCS to the end of the CRC (see Note 1). If this parameter is omitted, then it defaults to a value of 0 bit/s (i.e., no bandwidth is reserved for the flow by default).

NOTE 1 – The payload size includes every PDU in a Concatenated MAC Frame.

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

Type	Length	Value
[24/25].10	4	

NOTE 2 – The specific algorithm for enforcing the value specified in this field is not mandated here.

C.C.2.2.5.6 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 (see Note). 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.

NOTE – The payload size includes every PDU in a Concatenated MAC Frame.

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

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

Type	Length	Value
[24/25].11	2	

C.C.2.2.5.7 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 CMTS MUST change the active and admitted QoS Parameter Sets to null. The CMTS MUST signal this resource change with a DSC-REQ to the CM.

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

This parameter MUST be enforced at the CMTS and SHOULD NOT be enforced at the CM. The parameter is processed by the CMTS for every QoS set contained in Registration messages and Dynamic Service messages. If the parameter is omitted, the default of 0 (i.e. infinite timeout) is assumed. The value specified for the active QoS set must be less than or equal to the corresponding value in the admitted QoS set which must be less than or equal to the corresponding value in the provisioned/authorized QoS set. If the requested value is too large, the CMTS MAY reject the message or respond with a value less than that requested. If the Registration or Dynamic Service message is accepted by the CMTS and acknowledged by the CM, the Active MQoS Timeout timer is loaded with the new value of the timeout. The timer is activated if the message activates the associated Service Flow. The timer is deactivated if the message sets the active QoS set to null.

C.C.2.2.5.8 Timeout for admitted QoS parameters

The value of this parameter specifies the duration that the CMTS MUST hold resources for a Service Flow's Admitted QoS Parameter Set while they are in excess of its Active QoS Parameter Set. If there is no DSC-REQ to activate the Admitted QoS Parameter Set within this time interval, and there is no DSC to refresh the QoS parameter sets and restart the timeout (see C.10.1.5.2), the resources that are admitted but not activated MUST be released, and only the active resources retained. The CMTS MUST set the Admitted QoS Parameter Set equal to the Active QoS Parameter Set for the Service Flow and initiate a DSC-REQ exchange with the CM to inform it of the change.

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

This parameter MUST be enforced at the CMTS and SHOULD NOT be enforced at the CM. The parameter is processed by the CMTS for every QoS set contained in Registration messages and Dynamic Service messages. If the parameter is omitted, the default of 200 s is assumed. A value of 0 means that the Service Flow can remain in the admitted state for an infinite amount of time and MUST NOT be timed out due to inactivity. However, this is subject to policy control by the CMTS. The value specified for the active QoS set must be less than or equal to the corresponding value in the admitted QoS set which must be less than or equal to the corresponding value in the provisioned/authorized QoS set. If the requested value is too large, the CMTS MAY reject the message or respond with a value less than that requested. If the Registration or Dynamic Service message containing this parameter is accepted by the CMTS and acknowledged by the CM, the Admitted QoS Timeout timer is loaded with the new value of the timeout. The timer is activated if the message admits resources greater than the active set. The timer is deactivated if the message sets the active QoS set and admitted QoS set equal to each other.

C.C.2.2.5.9 Vendor-specific QoS parameters

This allows vendors to encode Vendor-Specific QoS parameters. The Vendor ID MUST be the first TLV embedded inside Vendor-Specific QoS Parameters. If the first TLV inside Vendor-Specific QoS Parameters is not a Vendor ID, then the TLV MUST be discarded. (Refer to C.C.1.1.17.)

Type	Length	Value
[24/25].43	n	B (bytes)

C.C.2.2.6 Upstream-specific QoS parameter encodings

C.C.2.2.6.1 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 CM. If defined, this parameter MUST be enforced at the CM.

NOTE 1 – This value does not include any physical layer overhead.

Type	Length	Value
24.14	2	

NOTE 2 – 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.

C.C.2.2.6.2 Service flow scheduling type

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

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

Type	Length	Value
24.15	1	0 Reserved 1 for Undefined (CMTS implementation-dependent) (see Note) 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

NOTE – The specific implementation dependent scheduling service type could be defined in the 24.43 Vendor-Specific Information Field.

C.C.2.2.6.3 Request/transmission policy

The value of this parameter specifies which IUC opportunities the CM 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 C.10.2 for requirements related to settings of the bits of this parameter for each Service Flow Scheduling Type.

This parameter is required for all Service Flow Scheduling Types except Best Effort. If omitted in a Best Effort Service Flow QoS parameter Set, the default value of zero MUST be used. Bit #0 is the LSB of the Value field. Bits are set to 1 to select the behavior defined below:

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

NOTE 1 – This bit only applies to Service Flows with the Unsolicited Grant Service Flow Scheduling Type, if this bit is set on any other Service Flow Scheduling type it MUST be ignored.

NOTE 2 – 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.

NOTE 3 – Data grants include both short and long data grants.

C.C.2.2.6.4 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 $t_i = t_0 + i \times \text{interval}$. The actual poll times, t'_i MUST be in the range $t_i \le t'_i \le t_i + \text{jitter}$, where interval is the value specified with this TLV, and jitter is Tolerated Poll Jitter. The accuracy of the ideal poll times, t_i, are measured relative to the CMTS Master Clock used to generate timestamps (refer to C.9.3).

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

Type	Length	Value
24.17	4	µs

C.C.2.2.6.5 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 $t_i = t_0 + i \times$ interval. The actual poll, t'_i MUST be in the range $t_i \leq t'_i \leq t_i$ + 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 CMTS Master Clock used to generate timestamps (refer to C.9.3).

This parameter is only applicable at the CMTS. If defined, this parameter represents a service commitment (or admission criteria) at the CMTS.

Type	Length	Value
24.18	4	µs

C.C.2.2.6.6 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 CMTS and MUST be enforced at the CMTS.

Type	Length	Value
24.19	2	µs

NOTE – For UGS, this parameter should be used by the CMTS to compute the size of the unsolicited grant in minislots.

C.C.2.2.6.7 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 $t_i = t_0 + i \times$ interval. The actual grant times, t'_i MUST be in the range $t_i \leq t'_i \leq t_i$ + jitter, where interval is the value specified with this TLV, and jitter is the Tolerated Grant Jitter. When multiple grants per interval are requested, all grants MUST be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter MUST be maintained by the CMTS for all grants in this Service Flow. The accuracy of the ideal grant times, t_i, are measured relative to the CMTS Master Clock used to generate timestamps (refer to C.9.3).

This field is mandatory for Unsolicited Grant and Unsolicited Grant with Activity Detection Scheduling Types. This field is only applicable at the CMTS, and MUST be enforced by the CMTS.

Type	Length	Value
24.20	4	µs

C.C.2.2.6.8 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 $t_i = t_0 + i \times$ interval. The actual transmission opportunities, t'_i MUST be in the range $t_i \leq t'_i \leq t_i$ + 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 CMTS Master Clock used to generate timestamps (refer to C.9.3).

This field is mandatory for Unsolicited Grant and Unsolicited Grant with Activity Detection Scheduling Types. This field is only applicable at the CMTS, and MUST be enforced by the CMTS.

Type	Length	Value
24.21	4	µs

C.C.2.2.6.9 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 $t_i = t_0 + i \times$ interval. The actual grant times, t'_i MUST be in the range $t_i \leq t'_i \leq t_i$ + jitter, where interval is the Nominal Grant Interval, and jitter is the Tolerated Grant Jitter. When multiple grants per interval are requested, all grants MUST be within this interval, thus the Nominal Grant Interval and Tolerated Grant Jitter MUST be maintained by the CMTS 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 CMTS, and MUST be enforced by the CMTS.

Type	Length	Value
24.22	1	# of grants

Valid Range

0-7 for pri-low and pri-high.

C.C.2.2.6.10 IP type of Service overwrite

The CMTS MUST overwrite IP packets with IP ToS byte value "orig-ip-tos" with the value "new-ip-tos", where new-ip-tos = ((orig-ip-tos AND tos-and-mask) OR tos-or-mask). If this parameter is omitted, then the IP packet ToS byte is not overwritten.

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

Type	Length	Value
24.23	2	Tos-and-mask, tos-or-mask

C.C.2.2.6.11 Unsolicited grant time reference

For Unsolicited Grant Service and Unsolicited Grant Service with Activity Detection, the value of this parameter specifies a reference time t_0 from which can be derived the desired transmission times $t_i = t_0 + i \times$ interval, where interval is the Nominal Grant Interval (refer to C.C.2.2.6.7). This parameter is applicable only for messages transmitted from the CMTS to the CM, and only when a UGS or UGS-AD service flow is being made active. In such cases this is a mandatory parameter.

Type	Length	Value
24.24	4	CMTS Timestamp

Valid Range

0-4 294 967 295

The timestamp specified in this parameter represents a count state of the CMTS 9.216 MHz master clock. Since a UGS or UGS-AD service flow is always activated before transmission of this parameter to the modem, the reference time t_0 is to be interpreted by the modem as the ideal time of the next grant only if t_0 follows the current time. If t_0 precedes the current time, the modem can calculate the offset from the current time to the ideal time of the next grant according to:

interval: (((current time – t_0)/9.216) modulus interval)

where: interval is in units of microseconds, current time and t_0 are in 9.216 MHz units

C.C.2.2.7 Downstream-specific QoS parameter encodings

C.C.2.2.7.1 Maximum downstream latency

The value of this parameter specifies the maximum latency between the reception of a packet by the CMTS 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 CMTS and MUST be guaranteed by the CMTS. A CMTS does not have to meet this service commitment for Service Flows that exceed their minimum downstream reserved rate.

Type	Length	Value
24.14	4	μs

C.C.2.2.8 Payload header suppression

This field defines the parameters associated with Payload Header Suppression.

Type	Length	Value
26	n	

The entire Payload Header Suppression TLV MUST have a length of less than 255 characters.

C.C.2.2.8.1 Classifier reference

The value of the field specifies a Classifier Reference that identifies the corresponding Classifier. (Refer to C.C.2.1.3.1.)

Type	Length	Value
26.1	1	1-255

C.C.2.2.8.2 Classifier identifier

The value of the field specifies a Classifier Identifier that identifies the corresponding Classifier. (Refer to C.C.2.1.3.2.)

Type	Length	Value
26.2	2	1-65 535

C.C.2.2.8.3 Service flow reference

The value of the field specifies a Service Flow Reference that identifies the corresponding Service Flow. (Refer to C.C.2.2.3.1.)

Type	Length	Value
26.3	2	1-65 535

C.C.2.2.8.4 Service flow identifier

The value of this field specifies the Service Flow Identifier that identifies the Service Flow to which the PHS rule applies.

Type	Length	Value
26.4	4	1-4 294 967 295

C.C.2.2.8.5 Dynamic service change action

When received in a Dynamic Service Change Request, this indicates the action that MUST be taken with this payload header suppression byte string.

Type	Length	Value
26.5	1	0: Add PHS Rule 1: Set PHS Rule 2: Delete PHS Rule 3: Delete all PHS Rules

The "Set PHS Rule" command is used to add specific TLVs to a partially defined payload header suppression rule. A PHS rule is partially defined when the PHSF and PHSS values are not both known. A PHS rule becomes fully defined when the PHSF and PHSS values are both known. Once a PHS rule is fully defined, "Set PHS Rule" MUST NOT be used to modify existing TLVs.

The "Delete all PHS Rules" command is used to delete all PHS Rules for a specified Service Flow. See C.8.3.15 for details on DSC-REQ required PHS parameters when using this option.

NOTE – An attempt to Add a PHS Rule which already exists is an error condition.

C.C.2.2.9 Payload header suppression error encodings

This field defines the parameters associated with Payload Header Suppression Errors.

Type	Length	Value
26.6	n	

A Payload Header Suppression Error Encoding consists of a single Payload Header Suppression Error Parameter Set which is defined by the following individual parameters: Errored Parameter, Confirmation Code and Error Message.

The Payload Header Suppression Error Encoding is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the reason for the recipient's negative response to a Payload Header Suppression Rule establishment request in a REG-REQ, DSA-REQ or DSC-REQ message.

On failure, the REG-RSP, DSA-RSP, or DSC-RSP MUST include one Payload Header Suppression Error Encoding for at least one failed Payload Header Suppression Rule requested in the REG-REQ, DSA-REQ or DSC-REQ message. A Payload Header Suppression Error Encoding for the failed Payload Header Suppression Rule MUST include the Confirmation Code and Errored Parameter and MAY include an Error Message. If some Payload Header Suppression Rule Sets are rejected but other Payload Header Suppression Rule Sets are accepted, then Payload Header Suppression Error Encodings MUST be included for only the rejected Payload Header Suppression Rules. On success of the entire transaction, the RSP or ACK message MUST NOT include a Payload Header Suppression Error Encoding.

Multiple Payload Header Suppression Error Encodings MAY appear in a REG-RSP, DSA-RSP or DSC-RSP message, since multiple Payload Header Suppression parameters may be in error. A message with even a single Payload Header Suppression Error Encoding MUST NOT contain any other protocol Payload Header Suppression Encodings (e.g. IP, 802.1P/Q).

A Payload Header Suppression Error Encodings MUST NOT appear in any REG-REQ, DSA-REQ or DSC-REQ messages.

C.C.2.2.9.1 Errored parameter

The value of this parameter identifies the subtype of a requested Payload Header Suppression parameter in error in a rejected Payload Header Suppression request. A Payload Header Suppression Error Parameter Set MUST have exactly one Errored Parameter TLV within a given Payload Header Suppression Error Encoding.

Type	Length	Value
26.6.1	1	Payload Header Suppression Encoding Subtype in Error

C.C.2.2.9.2 Error code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in C.C.4. A Payload Header Suppression Error Parameter Set MUST have exactly one Error Code within a given Payload Header Suppression Error Encoding.

Type	Length	Value
26.6.2	1	Confirmation code

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

C.C.2.2.9.3 Error message

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

Type	Length	Value
26.6.3	n	Zero-terminated string of ASCII characters

- The length n includes the terminating zero.

- The entire Payload Header Suppression Encoding message MUST have a total length of less than 256 characters.

C.C.2.2.10 Payload header suppression rule encodings

C.C.2.2.10.1 Payload Header Suppression Field (PHSF)

The value of this field are the bytes of the headers which MUST be suppressed by the sending entity, and MUST be restored by the receiving entity. In the upstream, the PHSF corresponds to the string of PDU bytes starting with the first byte after the MAC Header Checksum. For the downstream, the PHSF corresponds to the string of PDU bytes starting with the 13th byte after the MAC Header Checksum. This string of bytes is inclusive of both suppressed and unsuppressed bytes of the PDU header. The value of the unsuppressed bytes within the PHSF is implementation dependent.

The ordering of the bytes in the value field of the PHSF TLV string MUST follow the sequence:

Upstream:

MSB of PHSF value = 1st byte of PDU
2nd MSB of PHSF value = 2nd byte of PDU
...
nth byte of PHSF (LSB of PHSF value) = nth byte of PDU

Downstream:

MSB of PHSF value = 13th byte of PDU
2nd MSB of PHSF value = 14th byte of PDU
...
nth byte of PHSF (LSB of PHSF value) = (n+13)th byte of PDU

Type	Length	Value
26.7	n	String of bytes suppressed

The length n MUST always be the same as the value for PHSS.

C.C.2.2.10.2 Payload Header Suppression Index (PHSI)

The Payload Header Suppression Index (PHSI) has a value between 1 and 255 which uniquely references the suppressed byte string. The Index is unique per Service Flow in the upstream direction and unique per CM in the downstream direction. The upstream and downstream PHSI values are independent of each other.

Type	Length	Value
26.8	1	Index value

C.C.2.2.10.3 Payload Header Suppression Mask (PHSM)

The value of this field is used to interpret the values in the Payload Header Suppression Field. It is used at both the sending and receiving entities on the link. The PHSM allows fields such as sequence numbers or checksums which vary in value to be excluded from suppression with the constant bytes around them suppressed.

Type	Length	Value
26.9	n	Bit 0: 0 = Do not suppress first byte of the suppression field 1 = Suppress first byte of the suppression field Bit 1: 0 = Do not suppress second byte of the suppression field 1 = Suppress second byte of the suppression field Bit x: 0 = Do not suppress (x+1) byte of the suppression field 1 = Suppress (x+1) byte of the suppression field

The length n is ceiling (PHSS/8). Bit 0 is the MSB of the Value field. The value of each sequential bit in the PHSM is an attribute for the corresponding sequential byte in the PHSF.

If the bit value is a "1" (and verification passes or is disabled), the sending entity MUST suppress the byte, and the receiving entity MUST restore the byte from its cached PHSF. If the bit value is a "0", the sending entity MUST NOT suppress the byte, and the receiving entity MUST restore the byte by using the next byte in the packet.

If this TLV is not included, the default is to suppress all bytes.

C.C.2.2.10.4 Payload Header Suppression Size (PHSS)

The value of this field is the total number of bytes in the Payload Header Suppression Field (PHSF) for a Service Flow that uses Payload Header Suppression.

Type	Length	Value
26.10	1	Number of bytes in the suppression string

This TLV is used when a Service Flow is being created. For all packets that get classified and assigned to a Service Flow with Payload Header Suppression enabled, suppression MUST be performed over the specified number of bytes as indicated by the PHSS and according to the PHSM. If this TLV is included in a Service Flow definition with a value of 0 bytes, then Payload Header Suppression is disabled. A non-zero value indicates Payload Header Suppression is enabled. Until the PHSS value is known, the PHS rule is considered partially defined, and suppression will not be performed. A PHS rule becomes fully defined when both PHSS and PHSF are known.

C.C.2.2.10.5 Payload Header Suppression Verification (PHSV)

The value of this field indicates to the sending entity whether or not the packet header contents are to be verified prior to performing suppression. If PHSV is enabled, the sender MUST compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM.

Type	Length	Value
26.11	1	0: Verify 1: Do not verify

If this TLV is not included, the default is to verify. Only the sender MUST verify suppressed bytes. If verification fails, the Payload Header MUST NOT be suppressed. (Refer to C.10.4.3.)

C.C.2.2.10.6 Vendor specific PHS parameters

This allows vendors to encode vendor-specific PHS parameters. The Vendor ID MUST be the first TLV embedded inside Vendor Specific PHS Parameters. If the first TLV inside Vendor Specific PHS Parameters is not a Vendor ID, then the TLV MUST be discarded. (Refer to C.C.1.1.17.)

Type	Length	Value
26.420	n	

C.C.3 Encodings for other interfaces

C.C.3.1 Telephone settings option

This configuration setting describes parameters which are specific to telephone return systems. It is composed from a number of encapsulated type/length/value fields.

Type	Length	Value
15 (= TRI_CFG01)	n	

C.C.3.2 Baseline privacy configuration settings option

This configuration setting describes parameters which are specific to Baseline Privacy. It is composed from a number of encapsulated type/length/value fields.

Type	Length	Value
17 (= BP_CFG)	n	

C.C.4 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. The confirmation codes in this clause are used both as message Confirmation Codes and as Error Codes in Error Set Encodings which may be carried in these 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)
- reject-multiple-errors(13)
- reject-classifier-not-found(14)
- reject-classifier-exists(15)
- reject-PHS-rule-not-found(16)
- reject-PHS-rule-exists(17)
- reject-duplicate-reference-ID-or-index-in-message(18)
- reject-multiple-upstream-service-flows(19)
- reject-multiple-downstream-service-flows(20)
- reject-classifier-for-another-service-flow(21)
- reject-PHS-for-another-service-flow(22)
- reject-parameter-invalid-for-context(23)
- reject-authorization-failure(24)
- reject-temporary-DCC(25)

The Confirmation Codes MUST be used in the following way:

- Okay or success(0) means the message was received and successful.
- Reject-other(1) is used when none of the other reason codes apply.
- Reject-unrecognized-configuration setting(2) is used when a configuration setting is not recognized or when its value is outside of the specified range.
- Reject-temporary(3), also known as reject-resource, indicates that the current loading of the CMTS or CM prevents granting the request, but that the request might succeed at another time.
- Reject-permanent(4), also known as reject-admin, indicates that, for policy, configuration, or capabilities reasons, the request would never be granted unless the CMTS or CM were manually reconfigured or replaced.
- Reject-not-owner(5) the requester is not associated with this service flow.
- Reject-service-flow-not-found(6) the Service Flow indicated in the request does not exist.
- Reject-service-flow-exists(7) the Service Flow to be added already exists.
- Reject-required-parameter-not-present(8) a required parameter has been omitted.
- Reject-header-suppression(9) the requested header suppression cannot be supported for whatever reason.
- Reject-unknown-transaction-id(10) the requested transaction continuation is invalid because the receiving end-point does not view the transaction as being 'in process' (i.e. the message is unexpected or out of order).
- Reject-authentication-failure(11) the requested transaction was rejected because the message contained an invalid HMAC-digest.
- Reject-add-aborted(12) the addition of a dynamic service flow was aborted by the initiator of the Dynamic Service Addition.
- Reject-multiple errors(13) is used when multiple errors have been detected.
- Reject-classifier-not-found(14) is used when the request contains an unrecognized classifier ID.
- Reject-classifier-exists(15) indicates that the ID of a classifier to be added already exists.

- Reject-PHS-rule-not-found(16) indicates that the request contains an SFID/classifier ID pair for which no PHS rule exists.
- Reject-PHS-rule-exists(17) indicates that the request to add a PHS rule contains an SFID/classifier ID pair for which a PHS rule already exists.
- Reject-duplicate-reference-ID-or-index-in-message(18) indicates that the request used an SFR, classifier reference, SFID, or classifier ID twice in an illegal way.
- Reject-multiple-upstream-service-flows(19) is used when DSA/DSC contains parameters for more than one upstream flow.
- Reject-multiple-downstream-service-flows(20) is used when DSA/DSC contains parameters for more than one downstream flow.
- Reject-classifier-for-another-service-flow(21) is used in DSA-RSP when the DSA-REQ includes classifier parameters for a SF other than the new SF(s) being added by the DSA.
- Reject-PHS-for-another-service-flow(22) is used in DSA-RSP when the DSA-REQ includes a PHS rule for a SF other than the new SF(s) being added by the DSA.
- Reject-parameter-invalid-for-context(23) indicates that the parameter supplied cannot be used in the encoding in which it was included, or that the value of a parameter is invalid for the encoding in which it was included.
- Reject-authorization-failure(24) the requested transaction was rejected by the authorization module.
- Reject-temporary-DCC(25) indicates that the requested resources are not available on the current channels at this time, and the CM should re-request them on new channels after completing a channel change in response to a DCC command which the CMTS will send. If no DCC is received, the CM must wait for a time of at least T14 before re-requesting the resources on the current channels.

C.C.4.1 Confirmation codes for dynamic channel change

The CM may return in the DCC-RSP message an appropriate rejection code from C.C.1.3.1. It may also return one of the following Confirmation Codes which are unique to DCC-RSP.

- Depart(180).
- Arrive(181).
- Reject-already-there(182).

The Confirmation Codes MUST be used in the following way:

- Depart(180) indicates the CM is on the old channel and is about to perform the jump to the new channel.
- Arrive(181) indicates the CM has performed the jump and has arrived at the new channel.
- Reject-already-there(182) indicates that the CMTS has asked the CM to move to a channel that it is already occupying.

C.C.4.2 Confirmation codes for major errors

These confirmation codes MUST be used only as message Confirmation Codes in REG-ACK, DSA-RSP, DSA-ACK, DSC-RSP, or DSC-ACK messages, or as the Response code in REG-RSP messages for Revised Annex C/J.112 CMs. In general, the errors associated with these confirmation codes make it impossible either to generate an error set that can be uniquely associated with a parameter set in the REG-REQ, DSA-REQ, or DSC-REQ message, or to generate a full RSP message.

– reject-major-service-flow-error(200)

– reject-major-classifier-error(201)

– reject-major-PHS-rule-error(202)

– reject-multiple-major-errors(203)

– reject-message-syntax-error(204)

– reject-primary-service-flow-error(205)

– reject-message-too-big(206)

– reject-invalid-modem-capabilities(207)

The Confirmation Codes MUST be used only in the following way:

- Reject-major-service-flow-error(200) indicates that the REQ message did not have either a SFR or SFID in a service flow encoding, and that service flow major errors were the only major errors.
- Reject-major-classifier-error(201) indicates that the REQ message did not have a classifier reference, or did not have both a classifier ID and a Service Flow ID, and that classifier major errors were the only major errors.
- Reject-major-PHS-rule-error(202) indicates that the REQ message did not have a Service Flow Reference/Identifier nor a Classifier Reference/Identifier, and that PHS rule major errors were the only major errors.
- Reject-multiple-major-errors(203) indicates that the REQ message contained multiple major errors of types 200, 201, 202.
- Reject-message-syntax-error(204) indicates that the REQ message contained syntax error(s) (e.g., a TLV length error) resulting in parsing failure.
- Reject-primary-service-flow-error(205) indicates that a REG-REQ or REG-RSP message did not define a required primary Service Flow, or a required primary Service Flow was not specified active.
- Reject-message-too-big(206) is used when the length of the message needed to respond exceeds the maximum allowed message size.
- Reject-invalid-modem-capabilities(207) indicates that the REG-REQ contained either that in invalid combination of modem capabilities or modem capabilities that are inconsistent with the services in the REG-REQ.

Annex C.D

CM configuration interface specification

C.D.1 CM IP addressing

C.D.1.1 DHCP fields used by the CM

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

- The hardware type (htype) MUST be set to 1 (Ethernet).
- The hardware length (hlen) MUST be set to 6.
- The client hardware address (chaddr) MUST be set to the 48 bit MAC address associated with the RF interface of the CM.

- The "client identifier" option MUST be included, with the hardware type set to 1, and the value set to the same 48 bit MAC address as the chaddr field.
- Option code 60 (Vendor Class Identifier) – to allow for the differentiation between Revised Annex C/J.112(rev_c) and Previous Annex C/J.112(pre_c) CM requests, a compliant CM MUST send the following ASCII coded string in Option code 60, "rev_c:xxxxxxx". Where xxxxx MUST be an ASCII representation of the hexadecimal encoding of the Modem Capabilities, refer to C.C.1.3.1. For example, the ASCII encoding for the first two TLVs (concatenation and Annex C/J.112 Version) of a Revised Annex C/J.112 modem would be 05nn010101020101. Note that many more TLVs are required for a Revised Annex C/J.112 modem and the field "nn" will contain the length of all the TLVs. This example shows only two TLVs for simplicity.
- The "parameter request list" option MUST be included. The option codes that MUST be included in the list are:
  - Option code 1 (Subnet Mask);
  - Option code 2 (Time Offset);
  - Option code 3 (Router Option);
  - Option code 4 (Time Server Option);
  - Option code 7 (Log Server Option).

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

- The IP address to be used by the CM (yiaddr).
- The IP address of the TFTP server for use in the next phase of the bootstrap process (siaddr).
- 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.
- The name of the CM configuration file to be read from the TFTP server by the CM (file).
- The subnet mask to be used by the CM (Subnet Mask, option 1).
- The time offset of the CM from Universal Coordinated Time (UTC) (Time Offset, option 2). This is used by the CM to calculate the local time for use in time-stamping error logs.
- A list of addresses of one or more routers to be used for forwarding CM-originated IP traffic (Router Option, option 3). The CM is not required to use more than one router IP address for forwarding, but MUST use at least one.
- A list of [RFC 868] time-servers from which the current time may be obtained (Time Server Option, option 4).

To assist the DHCP server in differentiating a CM discovery request from a CPE side LAN discovery request, a CMTS MUST implement the following:

- The CMTS insert the DHCP relay agent information option, Option code 82, in the discovery request before relaying the discovery to a DHCP server. Specifically the CMTS shall include the 48 bit MAC address of the RF side interface of the CM generating or bridging the DHCP discovery request in the agent remote ID sub-option field, sub-option code 2. The option code 82 shall be formatted as follows: 82 08 02 06 xx xx xx xx xx xx, where "xx xx xx xx xx xx" refers to the CM's RF side MAC address. The DHCP relay agent information option is further described in [RFC 3046].

- If the CMTS is a router, it shall use a giaddr field to differentiate between CM and CPE side station if they are provisioned to be in different IP subnets. Bridging CMTSs should also provide this functionality.
- All CMTSs MUST support the DHCP relay agent information option, [ID-DHCP]. Specifically, the CMTS MUST include the 48 bit MAC address of the RF side interface of the CM generating or bridging the DHCP discovery request in the agent remote ID sub-option field before relaying the discovery to a DHCP server.
- If the CMTS is a router, it MUST use a giaddr field to differentiate between CM and CPE side station if they are provisioned to be in different IP subnets. CMTSs SHOULD also provide this functionality.

C.D.2 CM Configuration

C.D.2.1 CM binary configuration file format

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

It MUST 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 MUST follow each other directly in the file, which is a stream of octets (no record markers).

Configuration settings are divided into three types:

- standard configuration settings which MUST be present;
- standard configuration settings which MAY be present;
- vendor-specific configuration settings.

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

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

- CM 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).
- CMTS MIC is a digest used to authenticate the provisioning server to the CMTS during registration. It is taken over a number of fields one of which is a shared secret between the CMTS and the provisioning server.

Use of the CM MIC allows the CMTS to authenticate the provisioning data without needing to receive the entire file.

Thus the file structure is of the form shown in Figure C.D-1:

Configuration Setting 1	Configuration Setting 2		Configuration Setting n	CM MIC	CMTS MIC

Figure C.D-1/J.112 – Binary configuration file format

C.D.2.2 Configuration file settings

The following configuration settings MUST be included in the configuration file and MUST be supported by all CMs. The CM MUST NOT send a REG-REQ based on a configuration file that lacks these mandatory items.

- Network Access Configuration Setting;
- CM MIC Configuration Setting;
- CMTS MIC Configuration Setting;
- End Configuration Setting;
- Previous Annex C/J.112 Class of Service Configuration Setting.

NOTE – A Previous Annex C/J.112 CM MUST be provided with a Previous Annex C/J.112 Class of Service Configuration. A CM conformant with the present annex SHOULD only be provisioned with Previous Annex C/J.112 Class of Service Configuration information if it is to behave as a Previous Annex C/J.112 CM, otherwise it MUST be provisioned with Service Flow Configuration Settings.

or

- Upstream Service Flow Configuration Setting;
- Downstream Service Flow Configuration Setting.

The following configuration settings MAY be included in the configuration file and if present, MUST be supported by all CMs.

- Downstream Frequency Configuration Setting;
- Upstream Channel ID Configuration Setting;
- Baseline Privacy Configuration Setting;
- Software Upgrade Filename Configuration Setting;
- Upstream Packet Classification Setting;
- Downstream Packet Classification Setting;
- SNMP Write-Access Control;
- SNMP MIB Object;
- Software Server IP Address;
- CPE Ethernet MAC Address;
- Maximum Number of CPEs;
- Maximum Number of Classifiers;
- Privacy Enable Configuration Setting;
- Payload Header Suppression;
- TFTP Server Timestamp;
- TFTP Server Provisioned Modem Address;

- Pad Configuration Setting.

The following configurations MAY be included in the configuration file and if present, and applicable to this type of modem, MUST be supported.

- Telephone Settings Option.

The following configuration settings MAY be included in the configuration file and if present, MAY be supported by a CM.

- Vendor-Specific Configuration Settings.

There is a limit on the size of registration request and registration response frames (see C.8.2.5.2). The configuration file should not be so large as to require the CM or CMTS to exceed that limit.

C.D.2.3 Configuration file creation

The sequence of operations required to create the configuration file is as shown in Figure C.D-2 through Figure C.D-5.

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

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

Figure C.D-2/J.112 – Create TLV entries for parameters required by the CM

2) Calculate the CM message integrity check (MIC) configuration setting as defined in C.D.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 CM MIC

Figure C.D-3/J.112 – Add CM MIC

3) Calculate the CMTS message integrity check (MIC) configuration setting as defined in C.D.3.1 and add to the file following the CM MIC 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 CM MIC
type, length, value for CMTS MIC

Figure C.D-4/J.112 – Add CMTS MIC

4) 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 CM MIC
type, length, value for CMTS MIC
end-of-data marker

Figure C.D-5/J.112 – Add end-of-data marker

C.D.2.3.1 CM MIC calculation

The CM message integrity check configuration setting MUST 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 CM MIC TLV itself are omitted from the calculation. This includes the type, length, and value fields.

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

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

C.D.3 Configuration verification

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

C.D.3.1 CMTS MIC calculation

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

- Downstream Frequency Configuration Setting;
- Upstream Channel ID Configuration Setting;
- Network Access Configuration Setting;
- Previous Annex C/J.112 Class of Service Configuration Setting;
- Baseline Privacy Configuration Setting;
- Vendor-Specific Configuration Settings;
- CM MIC Configuration Setting;
- Maximum Number of CPEs;
- TFTP Server Timestamp;
- TFTP Server Provisioned Modem Address;
- Upstream Packet Classification Setting;
- Downstream Packet Classification Setting;

- Upstream Service Flow Configuration Setting;
- Downstream Service Flow Configuration Setting;
- Maximum Number of Classifiers;
- Privacy Enable Configuration Setting;
- Payload Header Suppression;
- Subscriber Management Control;
- Subscriber Management CPE IP Table;
- Subscriber Management Filter Groups.

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

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

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

The authentication string is a shared secret between the provisioning server (which creates the configuration files) and the CMTS. It allows the CMTS to authenticate the CM provisioning. The authentication string is to be used as the key for calculating the keyed CMTS MIC digest as stated in C.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 CM MUST forward the CMTS MIC as part of the registration request (REG-REQ).

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

C.D.3.1.1 Digest calculation

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

Annex C.E
(Void)

Annex C.F
(Void)

Annex C.G

Previous/Revised Annex C/J.112 Interoperability

C.G.1 Introduction

This annex applies only to the first option as defined in C.1.1.

In this annex, the terms "Annex C-P" and "Annex C-R" refer to the Previous Annex C/J.112 and the Revised Annex C/J.112 respectively.

The Annex C-R specification, primarily aims at enhancing the limited QoS functionality of an Annex C-P-based cable access system. New MAC messages have been defined for dynamic QoS Signalling, and several new QoS parameter encodings have been defined in the existing MAC messages. An Annex C-R CMTS can better support the requirements of delay/jitter sensitive traffic on an Annex C-R CM.

Besides supporting a rich set of QoS features for Annex C-R CMs, the Annex C-R CMTS must be backwards compatible with an Annex C-P CM. Furthermore, it is necessary for an Annex C-R CM to function like an Annex C-P CM when interoperating with an Annex C-P CMTS.

This annex describes the interoperability issues and trade-offs involved, when the operator wishes to support Annex C-P as well as Annex C-R CMs on the same cable access channel.

C.G.2 General interoperability issues

This clause addresses the general Annex C-P/Annex C-R interoperability issues that do not impact the performance during normal operation of the CMs.

C.G.2.1 Provisioning

The parameters of the TFTP config file for an Annex C-R CM, are a superset of those for an Annex C-P CM. Configuration file editors will have to be enhanced to incorporate support for these new parameters and the new MIC calculation.

If an Annex C-R CM is provisioned with an Annex C-P style TFTP configuration file, it MUST register like an Annex C-P CM (although in the REG-REQ it MUST still specify "Annex C-R" in the Annex C/J.112 Version Modem Capability and MAY specify additional revised Annex C/J.112 Modem Capabilities that it supports). Thus, an Annex C-R CM can be provisioned to work seamlessly on either an Annex C-P or an Annex C-R network. Although, clearly, an Annex C-R modem on an Annex C-P network would be unable to support any Annex C-R-specific features.

On the other hand, Annex C-P CMs do not recognize (and ignore) many of the new TLVs in an Annex C-R style config file, and will be unable to register successfully if provisioned with an Annex C-R configuration file. To prevent any functionality mismatches, an Annex C-R CMTS MUST reject any Registration Request with Annex C-R-specific configuration parameters that are not supported by the associated Modem Capabilities encoding in the REG-REQ (see C.C.1.3.1).

C.G.2.2 Registration

An Annex C-R CMTS is designed to handle the existing registration TLVs from Annex C-P CMs as well as the new TLVs (namely, types 22 to 30) from the Annex C-R CM.

There is a slight difference in the Registration-related messaging procedure when the Annex C-R CMTS is responding to an Annex C-R CM as opposed to Annex C-P CM. An Annex C-R CM could be configured to use the Service Class Name which is statically defined at the CMTS instead of asking for the service class parameters explicitly. When such a Registration-Request is received by the Annex C-R CMTS, it encodes the actual parameters of that service class in the Registration-Response and expects the Annex C-R specific Registration-Acknowledge MAC message from the CM. If the detailed capabilities in the Registration-Response message exceed those the CM is capable of supporting, the CM is required to indicate this to the CMTS in its Registration-Acknowledge.

When an Annex C-P CM registers with the same CMTS, the default Annex C-P version is easily identified by the absence of the "Annex C/J.112 Version" Modem Capabilities encoding in the Registration-Request. The Registration-Request from Annex C-P CM explicitly requests all non-default service class parameters in the Registration-Request per its provisioning information. Absence of a Service Class Name eliminates the need for the Annex C-R CMTS to explicitly specify the service class parameters in the Registration-Response using Annex C-R TLVs. When an Annex C-R CMTS receives a Registration-Request containing Annex C-P Class of Service Encodings, it will respond with the regular Annex C-P-style Registration-Response and not expect the CM to send the Registration-Acknowledge MAC message.

Another minor issues is that an Annex C-P CM will request for a bidirectional (with Upstream/Downstream parameters) service class from the CMTS using a Class-of-Service Configuration Setting.

Since Annex C-R CMTS typically operates with unidirectional service classes, it can easily translate an Annex C-P Class-of-Service Configuration Setting into Annex C-R Service Flow Encodings for setting up unidirectional service classes in local QoS implementation. However, for Annex C-P modems, the Annex C-R CMTS MUST continue to maintain the QoSProfile table (with bidirectional Class parameters) for backward compatibility with Annex C-P MIB.

Thus, if properly provisioned, an Annex C-P and an Annex C-R CM can successfully register with the same Annex C-R CMTS. Likewise, an Annex C-P and an Annex C-R CM can successfully register with the same Annex C-P CMTS.

C.G.2.3 Dynamic service establishment

There are 8 new MAC messages that relate to Dynamic Service Establishment. An Annex C-P CM will never send them to any CMTS since they are unsupported. An Annex C-R CM will never send them to an Annex C-P CMTS because:

a) to register successfully it has to be provisioned as an Annex C-P CM and

b) when provisioned as an Annex C-P CM it acts identically.

When an Annex C-R CM is connected to an Annex C-R CMTS, these messages work as expected.

C.G.2.4 Fragmentation

Fragmentation is initiated by the CMTS. Thus, an Annex C-P CMTS will never initiate fragmentation since it knows nothing about it. An Annex C-R CMTS can only initiate fragmentation for Annex C-R CMs. An Annex C-R CMTS MUST NOT attempt to fragment transmissions from an Annex C-P CM that has not indicated a Modem Capabilities encoding for Fragmentation Support with a value of 1.

C.G.2.5 Multicast support

It is mandatory for Annex C-P CM's to support forwarding of multicast traffic. However, the specification is silent on IGMP support. Thus, the only standard mechanism for controlling IP-multicast on Annex C-P CMs is through SNMP and packet filters. Designers of Annex C-P networks will have to deal with these limitations and expect no difference from Annex C-P CM's on an Annex C-R network.

C.G.2.6 Upstream channel change

An Annex C-R CMTS is capable of specifying the level of reranging to be performed when it issues an UCC-Request to the CM. This reranging technique parameter is specified by the Annex C-R CMTS using a new TLV in the UCC-Request MAC message.

Annex C-R CMs that recognize this new TLV in the UCC-Request can benefit by only reranging to the level specified by this TLV. This can help in reducing the reinitialization time following a UCC, for the Annex C-R CM carrying a voice call. An Annex C-R CMTS is aware of the type of CM to which it is issuing the UCC-Request. It can refrain from inserting this reranging TLV in the UCC-Request for Annex C-P CMs. If an Annex C-R CMTS inserts this reranging TLV in the UCC-Request, the Annex C-P CMs which do not recognize this TLV will ignore its contents and perform the default Annex C-P reranging from start (Initial-Maintenance). The Annex C-R CMTS accepts default initial ranging procedure from any modem issuing the UCC-Request.

Thus Annex C-P and Annex C-R CMs on the same upstream channel can be individually requested to change upstream channels without any interoperability issues caused by the Annex C-R style reranging TLV in the UCC-request.

C.G.3 Hybrid devices

Some Annex C-P CM designs may be capable of supporting individual Annex C-R features via a software upgrade. Similarly, some Annex C-P CMTSs MAY be capable of supporting individual Annex C-R features. To facilitate these "hybrid" devices, the majority of Annex C-R features are individually enumerated in the Modem Capabilities.

Annex C-P hybrid CMs MAY request Annex C-R features via this mechanism. However, unless a CM is fully Annex C-R compliant (i.e. not a hybrid), it MUST NOT send an "Annex C/J.112 Version" Modem Capability which indicates anything besides Annex C-P.

If a hybrid CM intends to request such Annex C-R capabilities from the CMTS during registration, it MUST send the ASCII coded string in Option code 60 of its DHCP request, "pre_c:xxxxxxx". Where xxxxx MUST be an ASCII representation of the hexadecimal encoding of the Modem Capabilities, refer to C.C.1.3.1 and C.D.1.1. The DHCP server MAY use such information to determine what configuration file the CM is to use.

Normally, an Annex C-P CMTS would set all unknown Modem Capabilities to 'Off' in the Registration Response indicating that these features are unsupported and MUST NOT be used by the CM. An Annex C-P hybrid CMTS's MAY leave supported Modem Capabilities set to 'On' in the Registration Response. However, unless a CMTS is fully Annex C-R compliant (i.e. not a hybrid), it MUST still set all "Annex C/J.112 Version" Modem Capabilities to Annex C-P.

As always, any Modem Capability set to 'Off' in the Registration Response must be viewed as unsupported by the CMTS and MUST NOT be used by the CM.

C.G.4 Interoperability and Performance

This clause addresses the issue of performance impact on the QoS for Annex C-R CMs when Annex C-P and Annex C-R CMs are provisioned to share the same upstream MAC channel.

The Annex C-P CMs lack the ability to explicitly set their request policy (or provide scheduling parameters) for the advanced Annex C-R scheduling mechanisms like "Unsolicited Grant Service" and "Real-Time Polling Service". Thus, Annex C-P CMs will only receive statically configured "Tiered Best Effort" or "CIR" service on the upstream. The Annex C-R CMs on the same upstream channel can explicitly request for additional Service Flows when required, using the Annex C-R DSA-Request MAC message. Thus, Annex C-R CMs can benefit from the advanced scheduling mechanisms of an Annex C-R CMTS for their real-time traffic, besides the best-effort scheduling service they share with the Annex C-P CMs on the same upstream channel.

The Annex C-R upstream cable access channel carries variable-length MAC frames. In spite of the variable-length nature of the MAC frames, the Annex C-R CMTS grant scheduler is theoretically capable of providing a zero jitter TDMA-like environment for voice grants on the Upstream. Whenever the grant scheduler detects that the deadline of any future voice grant will be violated by the insertion of a non-voice grant, it fragments the non-voice grant up to the future voice grant boundary. Thus the voice grants see a zero shift from the assigned periodic grant position.

However, such grant fragmentation might not always be possible when the CMTS supports Annex C-P CMs along with Annex C-R CMs on the same Upstream channel since Annex C-P CM do not support fragmentation. For a mixed CM version upstream channel, the worst case voice grant jitter seen by the Annex C-R CMs, is when an Annex C-P CM is given a grant for an unfragmented maximum sized MAC frame just before the designated voice grant slot of the Annex C-R CM.

The maximum Voice grant jitter experienced by the Annex C-R CMs is a function of the physical layer characteristics of the Upstream Channel. For 9.216 Mbit/s and 4.608 Mbit/s upstream channels, the impact of having fragmenting and non-fragmenting CM's on the same channel is almost undetectable. On smaller channels, the benefit of fragmentation is far greater and the jitter induced by non-fragmenting Annex C-P CMs is greater.

Thus, properly engineered networks can support voice even when mixing Annex C-P and Annex C-R CMs.

Annex C.H
(Void)

Annex C.I

The data-over-cable spanning tree protocol

Clause C.5.1.2.1 requires the use of the spanning tree protocol on CMs that are intended for commercial use and on bridging CMTSs. This annex describes how the IEEE 802.1D spanning tree protocol is adapted to work for data-over-cable systems.

C.I.1 Background

A spanning tree protocol is frequently employed in a bridged network in order to deactivate redundant network connections; i.e., to reduce an arbitrary network mesh topology to an active topology that is a rooted tree that spans all of the network segments. The spanning tree algorithm and protocol should not be confused with the data-forwarding function itself; data forwarding may follow transparent learning bridge rules, or may employ any of several other mechanisms. By deactivating redundant connections, the spanning tree protocol eliminates topological loops, which would otherwise cause data packets to be forwarded forever for many kinds of forwarding devices.

A standard spanning tree protocol [IEEE802.1D] is employed in most bridged local area networks. This protocol was intended for private LAN use and requires some modification for cable data use.

C.I.2 Public spanning tree

To use a spanning tree protocol in a public-access network such as data-over-cable, several modifications are needed to the basic [IEEE802.1D] process. Primarily, the public spanning tree must be isolated from any private spanning tree networks to which it is connected. This is to protect both the public cable network and any attached private networks. Figure C.I-1 illustrates the general topology.

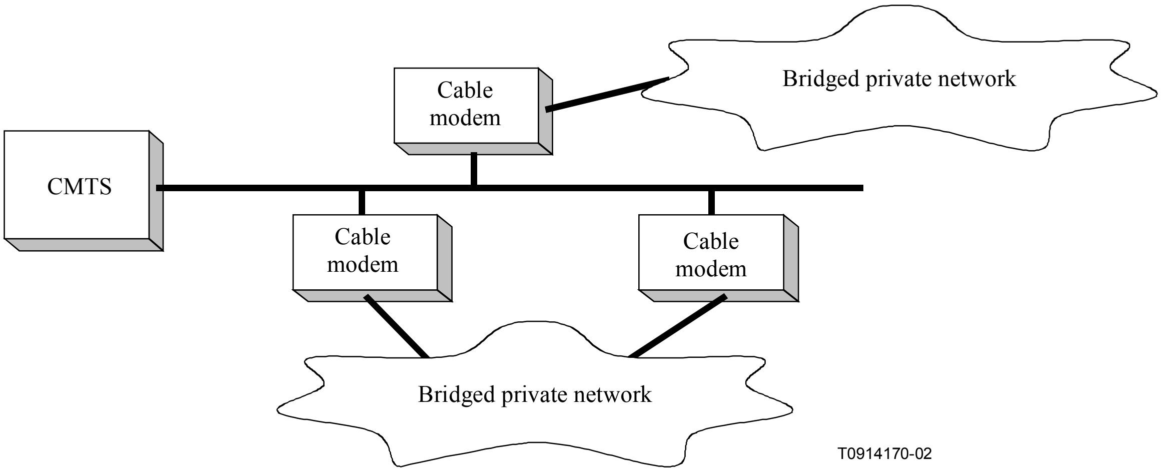


Figure C.I-1/J.112 – Spanning tree topology

The task for the public spanning tree protocol, with reference to Figure C.I-1, is to:

- Isolate the private bridged networks from each other. If the two private networks merge spanning trees then each is subject to instabilities in the other's network. Also, the combined tree may exceed the maximum allowable bridging diameter.
- Isolate the public network from the private networks' spanning trees. The public network must not be subject to instabilities induced by customers' networks; nor should it change the spanning tree characteristics of the customers' networks.
- Disable one of the two redundant links into the cable network, so as to prevent forwarding loops. This should occur at the cable modem, rather than at an arbitrary bridge within the customer's network.

The spanning tree protocol must also serve the topology illustrated in Figure C.I-2.

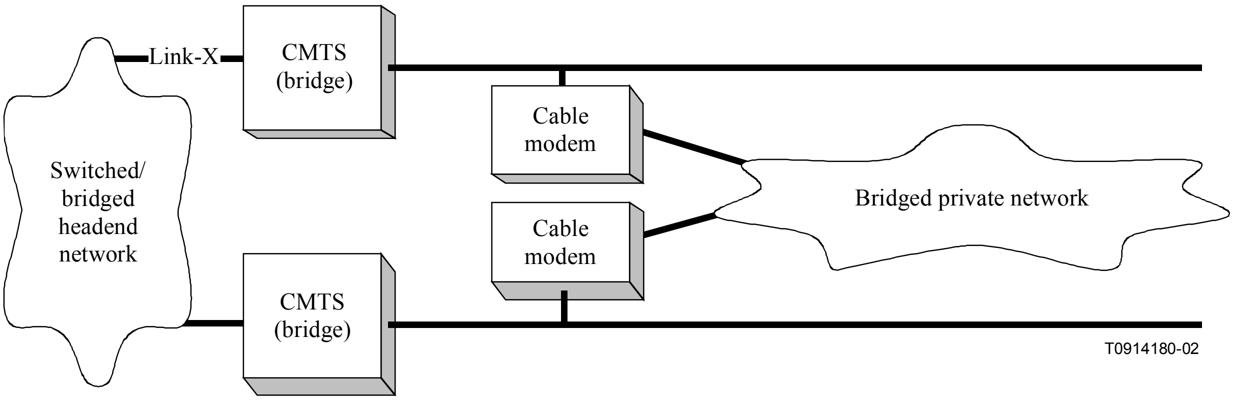


Figure C.I-2/J.112 – Spanning tree across CMTSs

In Figure C.I-2, in normal operation the spanning tree protocol should deactivate a link at one of the two cable modems. It should not divert traffic across the private network. Note that in some circumstances, such as deactivation of Link-X, spanning tree will divert traffic onto the private network (although limits on learned MAC addresses will probably throttle most transit traffic). If this diversion is undesirable, then it must be prevented by means external to spanning tree; for example, by using routers.

C.I.3 Public spanning tree protocol details

The Data-over-Cable Spanning Tree algorithm and protocol is identical to that defined in [IEEE 802.1D], with the following exceptions:

- When transmitting Configuration Bridge Protocol Data Units (BPDUs), the Data-over-Cable Spanning Tree Multicast Address 01-E0-2F-00-00-03 MUST be used rather than that defined in IEEE 802.1D. These BPDUs will be forwarded rather than recalculated by ordinary IEEE 802.1D bridges.
- When transmitting Configuration BPDUs, the SNAP header AA-AA-03-00-E0-2F-73-74 MUST be used rather than the LLC 42-42-03 header employed by IEEE 802.1D. This is to further differentiate these BPDUs from those used by IEEE 802.1D bridges, in the event that some of those bridges do not correctly identify multicast MAC addresses (see Note).

  NOTE – It is likely that there are a number of spanning tree bridges deployed which rely solely on the LSAPs to distinguish IEEE 802.1D packets. Such devices would not operate correctly if the data-over-cable BPDUs also used LSAP = 0x42.
- IEEE 802.1D BPDUs MUST be ignored and silently discarded.
- Topology Change Notification (TCN) PDUs MUST NOT be transmitted (or processed). TCNs are used in IEEE networks to accelerate the aging of the learning database when the network topology may have changed. Since the learning mechanism within the cable network typically differs, this message is unnecessary and may result in unnecessary flooding.
- CMTSs operating as bridges must participate in this protocol and must be assigned higher priorities (more likely to be root) than cable modems. The NSI interface on the CMTS SHOULD be assigned a port cost equivalent to a link speed of at least 100 Mbit/s. These two conditions, taken together, should ensure that:

  1) a CMTS is the root; and

  2) any other CMTS will use the head-end network rather than a customer network to reach the root.

- The MAC Forwarder of the CMTS MUST forward BPDUs from upstream to downstream channels, whether or not the CMTS is serving as a router or a bridge.

Note that CMs with this protocol enabled will transmit BPDUs onto subscriber networks in order to identify other CMs on the same subscriber network. These public spanning tree BPDUs will be carried transparently over any bridged private subscriber network. Similarly, bridging CMTSs will transmit BPDUs on the NSI as well as on the RFI interface. The multicast address and SNAP header defined above are used on all links.

C.I.4 Spanning tree parameters and defaults

Clause 4.10.2 of [IEEE802.1D] specifies a number of recommended parameter values. Those values should be used, with the exceptions listed below:

Path Cost

In [IEEE802.1D], the following formula is used:

Path_Cost = 1000/Attached_LAN_speed_in_Mbit/s

For CMs, this formula is adapted as:

Path_Cost = 1000/(Upstream_symbol_rate × bits_per_symbol_for_long_data_grant)

That is, the modulation type (QPSK or 16-QAM) for the Long Data Grant IUC is multiplied by the raw symbol rate to determine the nominal path cost. Table C.I-1 provides the derived values.

Table C.I-1/J.112 – CM path cost

Symbol Rate	Default path cost	
ksym/s	QPSK	16-QAM
144	3472	1736
288	1736	868
576	868	434
1152	434	217
2304	217	109

For CMTSs, this formula is:

Path_Cost = 1000/(Downstream_symbol_rate × bits_per_symbol)

Bridge Priority

The Bridge Priority for CMs SHOULD default to 36 864 (0x9000). This is to bias the network so that the root will tend to be at the CMTS. The CMTS SHOULD default to 32 768, as per IEEE 802.1D.

Note that both of these recommendations affect only the default settings. These parameters, as well as others defined in IEEE 802.1D, SHOULD be manageable throughout their entire range through the Bridge MIB ([RFC 1493]) or other means.

Annex C.J

Error codes and messages

These are CM and CMTS error codes and messages. These error codes are meant to emulate the standard fashion that ISDN reports error conditions regardless of the vendor producing the equipment.

The errors reported are Sync loss, UCD, MAP, Ranging REQ/RSP, UCC, registration, dynamic service request, and DHCP/TFTP failures. In some cases, there is detailed error reports in others, error codes are simply "it failed."

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
T00.0	**SYNC Timing Synchronization**
T01.0	Failed to acquire QAM/QPSK symbol timing. Error stats? Retry #'s?
T02.0	Failed to acquire FEC framing. Error stats? Retry #'s? # of bad frames?
T02.1	Acquired FEC framing. Failed to acquire MPEG2 Sync. Retry #'s?
T03.0	Failed to acquire MAC framing. Error stats? Retry #'s? # of bad frames?
T04.0	Failed to Receive MAC SYNC frame within time-out period.
T05.0	Loss of Sync. (Missed 5 in a row, after having SYNC'd at one time)
U00.0	**UCD Upstream Channel Descriptor**
U01.0	No UCDs Received. Time-out.
U02.0	UCD invalid or channel unusable.
U03.0	UCD valid, BUT no SYNC received. TIMED OUT.
U04.0	UCD, & SYNC valid, NO MAPs for THIS Channel.
U05.0	UCD received with invalid or out of order Configuration Change Count.
U06.0	US Channel wide parameters not set before Burst Descriptors.
M00.0	**MAP Upstream Bandwidth Allocation**
M01.0	A transmit opportunity was missed because the MAP arrived too late.
R00.0	**RNG-REQ Ranging Request**
R01.0	NO Maintenance Broadcasts for Ranging opportunities Received T2 time-out.
R04.0	Received Response to Broadcast Maintenance Request, But no Unicast Maintenance opportunities received. T4 time-out.
R101.0	No Ranging Requests received from POLLED CM (CMTS generated polls).
R102.0	Retries exhausted for polled CM (report MAC address). After 16 R101.0 errors.
R103.0	Unable to Successfully Range CM (report MAC address) Retries Exhausted. NOTE – This is different from R102.0 in that it was able to try, i.e. got REQs but failed to Range properly.
R104.0	Failed to receive Periodic RNG-REQ from modem (SID X), timing-out SID.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
R00.0	**RNG-RSP Ranging Response**
R02.0	No Ranging Response received, T3 time-out.
R03.0	Ranging Request Retries exhausted.
R05.0	Started Unicast Maintenance Ranging no Response received. T3 time-out.
R06.0	Unicast Maintenance Ranging attempted. No Response. Retries exhausted.
R07.0	Unicast Ranging Received Abort Response. Reinitializing MAC.
I00.0	**REG-REQ Registration Request**
I04.0	Service not available. Reason: Other.
I04.1	Service not available. Reason: Unrecognized configuration setting.
I04.2	Service not available. Reason: Temporarily unavailable.
I04.3	Service not available. Reason: Permanent.
I05.0	Registration rejected authentication failure: CMTS MIC invalid.
I101.0	Invalid MAC header.
I102.0	Invalid SID, not in use.
I103.0	Required TLVs out of order.
I104.0	Required TLVs not present.
I105.0	Down Stream Frequency format invalid.
I105.1	Down Stream Frequency not in use.
I105.2	Down Stream Frequency invalid, not a multiple of 62 500 Hz.
I106.0	Up Stream Channel invalid, unassigned.
I106.1	Up Stream Channel Change followed with (RE-)Registration REQ.
I107.0	Up Stream Channel overloaded.
I108.0	Network Access configuration has invalid parameter.
I109.0	Class of Service configuration is invalid.
I110.0	Class of Service ID unsupported.
I111.0	Class of Service ID invalid or out of range.
I112.0	Max Down Stream Bit Rate configuration is invalid format.
I112.1	Max Down Stream Bit Rate configuration setting is unsupported.
I113.0	Max Up Stream Bit Rate configuration setting invalid format.
I113.1	Max Up Stream Bit Rate configuration setting unsupported.
I114.0	Up Stream Priority configuration invalid format.
I114.1	Up Stream Priority configuration setting out of range.
I115.0	Guaranteed Min Up Stream Channel Bit Rate configuration setting invalid format.
I115.1	Guaranteed Min Up Stream Channel Bit Rate configuration setting exceeds Max Up Stream Bit Rate.
I115.2	Guaranteed Min Up Stream Channel Bit Rate configuration setting out of range.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
I116.0	Max Up Stream Channel Transmit Burst configuration setting invalid format.
I116.1	Max Up Stream Channel Transmit Burst configuration setting out of range.
I117.0	Modem Capabilities configuration setting invalid format.
I117.1	Modem Capabilities configuration setting out of range.
I200.0	**Revised Annex C/J.112 Specific REG-REQ Registration Request**
I201.0	Registration rejected unspecified reason.
I201.1	Registration rejected unrecognized configuration setting.
I201.2	Registration rejected temporary no resource.
I201.3	Registration rejected permanent administrative.
I201.4	Registration rejected required parameter not present.
I201.5	Registration Rejected header suppression setting not supported.
I201.6	Registration rejected multiple errors.
I201.7	Registration rejected duplicate reference-ID or index in message.
I201.8	Registration rejected parameter invalid for context.
I201.9	Registration rejected authorization failure.
I201.10	Registration rejected major service flow error.
I201.11	Registration rejected major classifier error.
I201.12	Registration rejected major PHS rule error.
I201.13	Registration rejected multiple major errors.
I201.14	Registration rejected message syntax error.
I201.15	Registration rejected primary service flow error.
I201.16	Registration rejected message too big.
I00.0	**REG-RSP Registration Response**
I01.0	Registration RESP invalid format or not recognized.
I02.0	Registration RESP not received.
I03.0	Registration RESP with bad SID.
I250.0	**Revised Annex C/J.112 Specific REG-RSP Registration Response**
I251.0	Registration RSP contains service flow parameters that CM cannot support.
I251.1	Registration RSP contains classifier parameters that CM cannot support.
I251.2	Registration RSP contains PHS parameters that CM cannot support.
I251.3	Registration RSP rejected unspecified reason.
I251.4	Registration RSP rejected message syntax error.
I251.5	Registration RSP rejected message too big.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
I300.0	**REG-ACK Registration Acknowledgement**
I301.0	Registration aborted no REG-ACK.
I302.0	Registration ACK rejected unspecified reason.
I303.0	Registration ACK rejected message syntax error.
C00.0	**UCC-REQ Upstream Channel Change Request**
C01.0	UCC-REQ received with invalid or out of range US channel ID.
C02.0	UCC-REQ received unable to send UCC-RSP, no TX opportunity.
C100.0	**UCC-RSP Upstream Channel Change Response**
C101.0	UCC-RSP not received on previous channel ID.
C102.0	UCC-RSP received with invalid channel ID.
C103.0	UCC-RSP received with invalid channel ID on new channel.
D00.0	**DHCP CM Net Configuration download and Time of Day**
D01.0	Discover sent, no Offer received, No available DHCP Server.
D02.0	Request sent, no Response.
D03.0	Requested Info not supported.
D03.1	DHCP response doesn't contain ALL the valid fields as described in the RF spec. Annex C.D
D04.0	Time of Day, none set or invalid data.
D04.1	Time of Day Request sent no Response received.
D04.2	Time of Day Response received but invalid data/format.
D05.0	TFTP Request sent, No Response/No Server.
D06.0	TFTP Request Failed, configuration file NOT FOUND.
D07.0	TFTP Failed, OUT OF ORDER packets.
D08.0	TFTP complete, but failed Integrity Check (MIC).
S00.0	**Dynamic Service Requests**
S01.0	Service add rejected unspecified reason.
S01.1	Service add rejected unrecognized configuration setting.
S01.2	Service add rejected temporary no resource.
S01.3	Service add rejected permanent administrative.
S01.4	Service add rejected required parameter not present.
S01.5	Service add rejected header suppression setting not supported.
S01.6	Service add rejected service flow exists.
S01.7	Service add rejected HMAC authentication failure.
S01.8	Service add rejected add aborted.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
S01.9	Service add rejected multiple errors.
S01.10	Service add rejected classifier not found.
S01.11	Service add rejected classifier exists.
S01.12	Service add rejected PHS rule not found.
S01.13	Service add rejected PHS rule exists.
S01.14	Service add rejected duplicate reference-ID or index in message.
S01.15	Service add rejected multiple upstream flows.
S01.16	Service add rejected multiple downstream flows.
S01.17	Service add rejected classifier for another service flow
S01.18	Service add rejected PHS rule for another service flow.
S01.19	Service add rejected parameter invalid for context.
S01.20	Service add rejected authorization failure.
S01.21	Service add rejected major service flow error.
S01.22	Service add rejected major classifier error.
S01.23	Service add rejected major PHS rule error.
S01.24	Service add rejected multiple major errors.
S01.25	Service add rejected message syntax error.
S01.26	Service add rejected message too big.
S01.27	Service add rejected temporary DCC.
S02.0	**Service change rejected unspecified reason**
S02.1	Service change rejected unrecognized configuration setting.
S02.2	Service change rejected temporary no resource.
S02.3	Service change rejected permanent administrative.
S02.4	Service change rejected requestor not owner of service flow.
S02.5	Service change rejected service flow not found.
S02.6	Service change rejected required parameter not present.
S02.7	Service change rejected multiple errors
S02.8	Service change rejected classifier not found.
S02.9	Service change rejected classifier exists.
S02.10	Service change rejected PHS rule not found.
S02.11	Service change rejected PHS rule exists.
S02.12	Service change rejected duplicate reference-ID or index in message.
S02.13	Service change rejected multiple upstream flows.
S02.14	Service change rejected multiple downstream flows.
S02.15	Service change rejected classifier for another service flow.
S02.16	Service change rejected PHS rule for another service flow.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
S02.17	Service change rejected parameter invalid for context.
S02.18	Service change rejected authorization failure.
S02.19	Service change rejected major service flow error.
S02.20	Service change rejected major classifier error.
S02.21	Service change rejected major PHS rule error.
S02.22	Service change rejected multiple major errors.
S02.23	Service change rejected message syntax error.
S02.24	Service change rejected message too big.
S02.25	Service change rejected temporary DCC.
S02.26	Service change rejected header suppression setting not supported.
S02.27	Service change rejected HMAC authentication failure.
S03.0	**Service delete rejected unspecified reason**
S03.1	Service delete rejected requestor not owner of service flow.
S03.2	Service delete rejected service flow not found.
S03.3	Service delete rejected HMAC authentication failure.
S03.4	Service delete rejected message syntax error.
S100.0	**Dynamic Service Responses**
S101.0	Service add response rejected invalid transaction ID.
S101.1	Service add aborted no RSP.
S101.2	Service add response rejected HMAC authentication failure.
S101.3	Service add response rejected message syntax error.
S102.0	Service change response rejected invalid transaction ID.
S102.1	Service change aborted no RSP.
S102.2	Service change response rejected HMAC authentication failure.
S102.3	Service change response rejected message syntax error.
S103.0	Service delete response rejected invalid transaction ID.
S200.0	**Dynamic Service Acknowledgements**
S201.0	Service add ACK rejected invalid transaction ID.
S201.1	Service add aborted no ACK.
S201.2	Service add ACK rejected HMAC authentication failure.
S201.3	Service add ACK rejected message syntax error.
S202.0	Service change ACK rejected invalid transaction ID.
S202.1	Service change aborted no ACK.
S202.2	Service change ACK rejected HMAC authentication failure.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
S202.3	Service change ACK rejected message syntax error.
C200.0	**Dynamic Channel Change Request**
C201.0	DCC rejected already there.
C202.0	DCC depart old.
C203.0	DCC arrive new.
C204.0	DCC aborted unable to acquire new downstream channel.
C205.0	DCC aborted no UCD for new upstream channel.
C206.0	DCC aborted unable to communicate on new upstream channel.
C207.0	DCC rejected unspecified reason.
C208.0	DCC rejected permanent – DCC not supported.
C209.0	DCC rejected service flow not found.
C210.0	DCC rejected required parameter not present.
C211.0	DCC rejected authentication failure.
C212.0	DCC rejected multiple errors.
C213.0	DCC rejected classifier not found.
C214.0	DCC rejected PHS rule not found.
C215.0	DCC rejected duplicate reference-ID or index in message.
C216.0	DCC rejected parameter invalid for context.
C217.0	DCC rejected message syntax error.
C218.0	DCC rejected message too big.
C300.0	**Dynamic Channel Change Response**
C301.0	DCC-RSP not received on old channel.
C302.0	DCC-RSP not received on new channel.
C303.0	DCC-RSP rejected unspecified reason.
C304.0	DCC-RSP rejected unknown transaction ID.
C305.0	DCC-RSP rejected authentication failure.
C306.0	DCC-RSP rejected message syntax error.
C400.0	**Dynamic Channel Change Acknowledgement**
C401.0	DCC-ACK not received.
C402.0	DCC-ACK rejected unspecified reason.
C403.0	DCC-ACK rejected unknown transaction ID.
C404.0	DCC-ACK rejected authentication failure.
C405.0	DCC-ACK rejected message syntax error.

Table C.J-1/J.112 – Error codes for MAC management messages

Error code	Error message
B00.0	**Baseline Privacy**
B01.0	TBD

Annex C.K

Annex C/J.112 Transmission and contention resolution

C.K.1 Introduction

This clause attempts to clarify how the Annex C/J.112 transmission and contention resolution algorithms work. It has a few minor simplifications and a few assumptions, but should definitely help clarify this area of the specification.

This example has a few simplifications:

- It does not explicitly talk about packet arrivals while deferring or waiting for pending grants and is vague about sizing piggyback requests.
- Much of this applies with concatenation, but it does not attempt to address all the subtleties of that situation.

It also has a few assumptions:

- It assumes that a Request always fits in any Request/Data region.
- When a piggyback request is sent with a contention data packet, the state machine only checks for the Grant to the Request and assumes the Data Ack for the contention data packet was supplied by CMTS.
- It probably assumes a few other things, but should be sufficient to get the basic point across.

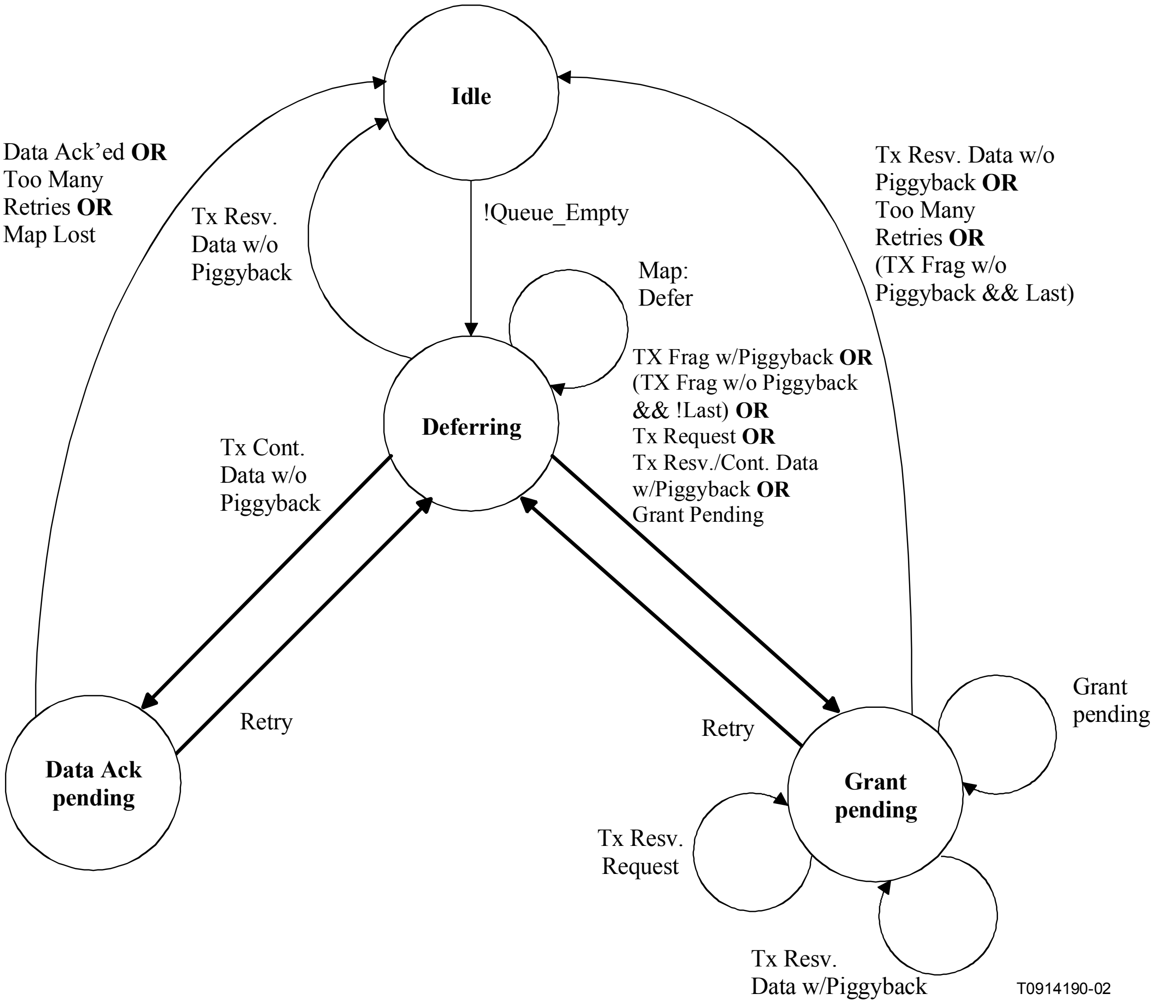

Idle
Data Ack'ed OR Too Many Retries OR Map Lost
Tx Resv. Data w/o Piggyback
!Queue_Empty
Map: Defer
Tx Resv. Data w/o Piggyback OR Too Many Retries OR (TX Frag w/o Piggyback && Last)
TX Frag w/Piggyback OR (TX Frag w/o Piggyback && !Last) OR Tx Request OR Tx Resv./Cont. Data w/Piggyback OR Grant Pending
Deferring
Tx Cont. Data w/o Piggyback
Retry
Retry
Grant pending
Data Ack pending
Grant pending
Tx Resv. Request
Tx Resv. Data w/Piggyback
T0914190-02

Figure C.K-1/J.112 – Transmission and deference state transition diagram

Variable Definitions

```
Start        =  Data Backoff Start field from Map "currently in effect"
End          =  Data Backoff End field from Map "currently in effect"
Window       =  Current backoff window
Random[n]    =  Random number generator that selects a number between 0 and n-1
Defer        =  Number of Transmit Opportunities to defer before transmitting
Retries      =  Number of transmissions attempted without resolution
Tx_time      =  Saved time of when Request or Request/Data was transmitted
Ack_time     =  Ack Time field from current Map
Piggyback    =  Flag set whenever a piggyback REQ is added to a transmit pkt
Queue_Empty  =  Flag set whenever the data queue for this SID is empty
Lost_Map     =  Flag set whenever a MAP is lost & we're in state Data Ack
                Pending
my_SID       =  Service ID of the queue that has a packet to transmit
pkt size     =  Data packet size including MAC and physical layer overhead
                (including piggyback if used)
frag_size    =  Size of the fragment
Tx_Mode      =  {Full_Pkt; First_Frag; Middle_Frag; Last_Frag}
min_frag     =  Size of the minimum fragment
```

State: Idle – Waiting for a Packet to Transmit

```
Window = 0;
Retries = 0;
Wait for !Queue_Empty;  /* Packet available to transmit */
CalcDefer();
```

```
go to Deferring
```

State: Data Ack Pending – Waiting for Data Ack only

```
Wait for next Map;

if (Data Acknowledge SID == my_SID)   /* Success! CMTS received data packet */
     go to state Idle;
else if (Ack_time > Tx_time)      /* COLLISION!!! or Pkt Lost or Map Lost */
     {
     if (Lost_Map)
       go to state Idle;
     /* Assume pkt was ack'ed to avoid sending duplicates */
     else
       Retry();
     }
stay in state Data Ack Pending;
```

State: Grant Pending – Waiting for a Grant

```
Wait for next Map;
while (Grant SID == my_SID)
     UtilizeGrant();
if (Ack_time > Tx_time)
     /* COLLISION!!!!! or Request denied/lost or Map Lost */
     Retry();
stay in state Grant Pending
```

State: Deferring – Determine Proper Transmission Timing & Transmit

```
if (Grant SID == my_SID)              /* Unsolicited Grant */
     {
     UtilizeGrant();
     }
else if (unicast Request SID == my_SID)    /* Unsolicited Unicast Request */
     {
     transmit Request in reservation;
     Tx_time = time;
     go to state Grant Pending;
     }
else
     {
     for (each Request or Request/Data Transmit Opportunity)
       {
       if (Defer != 0)
          Defer = Defer - 1;          /* Keep deferring until Defer = 0 */
       else
          {
          if (Request/Data tx_op) and     /* tsc_op = transmission opportunity */
          (Request/Data size >= pkt size)       /* Send data in contention */
           {
           transmit data pkt in contention;
           Tx_time = time;
           if (Piggyback)
              go to state Grant Pending;
           else
              go to state Data Ack Pending;
           }
          else               /* Send Request in contention */
           {
           transmit Request in contention;
           Tx_time = time;
           go to state Grant Pending;
          }
        }
       }
     }

Wait for next Map;
stay in state Deferring
```

Function: CalcDefer() – Determine Defer Amount

```
if (Window < Start)
     Window = Start;

if (Window > End)
     Window = End;

Defer = Random[2^Window];
```

Function: UtilizeGrant() – Determine Best Use of a Grant

```
if (Grant size >= pkt size)             /* CM can send full pkt */
     {
     transmit packet in reservation;
     Tx_time = time;
     Tx_mode = Full_pkt

     if (Piggyback)
       go to state Grant Pending
     else
       go to state Idle;
     }
else if (Grant size < min_frag && Grant Size > Request size)      /* Can't send
fragment, but can send a Request */
     {
     transmit Request in reservation;
     Tx_time = time;

     go to state Grant Pending;
     }
else if (Grant size == 0)               /* Grant Pending */
     go to state Grant Pending;
     else
     {
     while (pkt_size > 0 && Grant SID == my_SID)
       {


       if (Tx_mode == Full_Pkt)
          Tx_mode = First_frag;
       else
          Tx_mode = Middle_frag;
       pkt_size = pkt_size – frag_size;

       if (pkt_size == 0)
          Tx_mode = Last_frag;
       if (another Grant SID == my_SID)         /* multiple grant mode */
          piggyback_size = 0
       else
          piggyback_size = pkt_size          /* piggyback mode */

       if (piggyback_size > 0)
          transmit fragment with piggyback request for remainder of packet in
reservation
       else
```

```
          transmit fragment in reservation;
        }

     go to state Grant Pending;
```

Function: Retry()

```
Retries = Retries + 1;
if (Retries > 16)
     {
     discard pkt, indicate exception condition
     go to state Idle;
     }

Window = Window + 1;

CalcDefer();

go to state Deferring;
```

Annex C.L

IGMP example

Clause C.5.3.1 defines the requirements for CMTS and CM support of IGMP Signalling. This annex provides further details on CM support for IGMP.

The process defined MAY be supported by compliant CMs. Refer to Figure C.L-1.

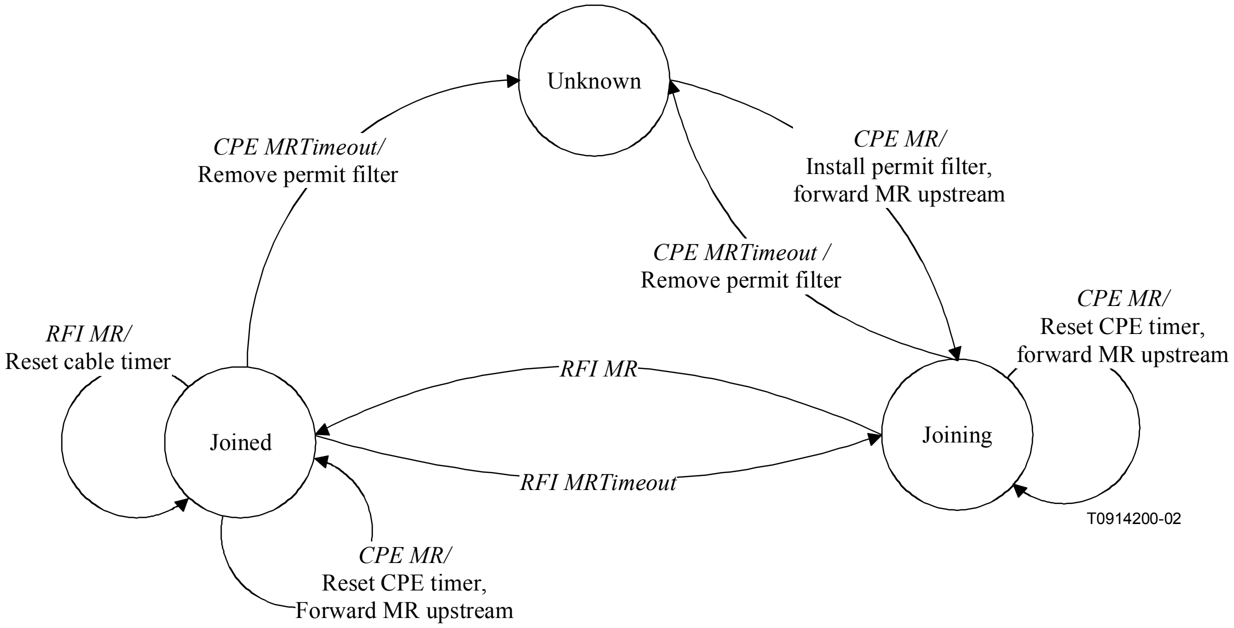


Figure C.L-1/J.112 – IGMP support – CM

C.L.1 Transition events

See Table C.L-1.

Table C.L-1/J.112 – Event table

Event	State		
	1. Unknown	**2. Joining**	**3. Joined**
A) CpeMR	Joining	Joining	Joined
B) RFI MR		Joined	Joined
C) RFI MRTimeout			Joining
D) CpeMRTimeout		Unknown	Unknown

1A

- Forward Membership Report (MR) Upstream.
- Start CPE MR Timer.
- Install Permit Multicast Filters for forwarding IP multicast traffic to the CPE LAN.

2A

- Restart CPE MR timer.
- Forward MR upstream.

3A

- Reset CPE timer, forward MR upstream.

2B

- Start Cable MR timer.

3B

- Restart Cable MR timer.

3C

- Stop Cable MR timer.

2D

- Stop CPE MR timer.
- Remove Permit Multicast Filter for forwarding IP multicast to the CPE LAN.

3D

- Stop CPE MR timer.
- Remove Permit Multicast Filter for forwarding IP multicast to the CPE LAN.

Annex C.M

Unsolicited grant services

This annex discusses the intended use of the Unsolicited Grant Service (UGS) and Unsolicited Grant Service with Activity Detection (UGS-AD) and includes specific examples.

C.M.1 Unsolicited grant service (UGS)

C.M.1.1 Introduction

Unsolicited Grant Service is an Upstream Flow Scheduling Service Type that is used for mapping constant bit rate (CBR) traffic onto Service Flows. Since the upstream is scheduled bandwidth, a CBR service can be established by the CMTS scheduling a steady stream of grants. These are referred to as unsolicited because the bandwidth is predetermined, and there are no ongoing requests being made.

The classic example of a CBR application of interest is Voice over Internet Protocol (VoIP) packets. Other applications are likely to exist as well.

Upstream Flow Scheduling Services are associated with Service Flows, each of which is associated with a single Service ID (SID). Each Service Flow may have multiple Classifiers. Each Classifier may be associated with a unique CBR media stream. Classifiers may be added and removed from a Service Flow. Thus, the semantics of UGS must accommodate single or multiple CBR media streams per SID.

For the discussion within this annex, a Subflow will be defined as the output of a Classifier. Since a VoIP session is identified with a Classifier, a Subflow in this context refers to a VoIP session.

C.M.1.2 Configuration parameters

- Nominal Grant Interval.
- Unsolicited Grant Size.
- Tolerated Grant Jitter.
- Grants per Interval.

Explanation of these parameters and their default values are provided in Annex C.C.

C.M.1.3 Operation

When a Service Flow is provisioned for UGS, the Nominal Grant Interval is chosen to equal the packet interval of the CBR application. For example, VoIP applications with 10 ms packet sizes will require a Nominal Grant Interval of 10 ms. The size of the grant is chosen to satisfy the bandwidth requirements of the CBR application and relates directly to the length of the packet.

When multiple Subflows are assigned to a UGS service, multiple grants per interval are issued. There is no explicit mapping of Subflows to grants. The multiple grants per interval form a pool of grants in which any subflow can use any grant.

The default UGS case of no concatenation and no fragmentation is assumed in this operational example.

C.M.1.4 Jitter

Figure C.M-1 shows the relationship between Grant Interval and Tolerated Grant Jitter, and shows an example of jitter on subflows.

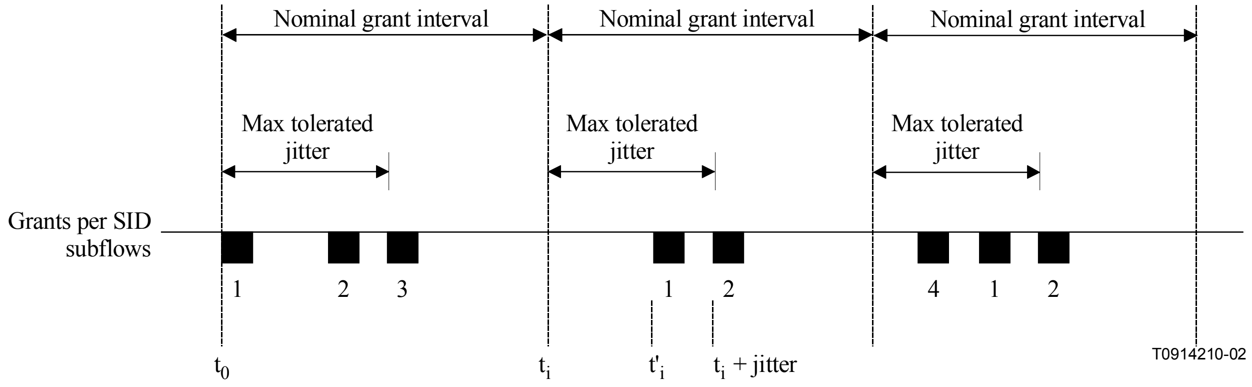


Figure C.M-1/J.112 – Example jitter with multiple grants per SID

For only one Grant per Interval, the Tolerated Grant Jitter is the maximum difference between the actual grant time (t_i') and the nominal grant time (t_i). For multiple Grants per Interval, the Tolerated Grant Jitter is the maximum difference between the actual time of the last grant in the group of grants and the nominal grant time (t_i). If the arrival of any grant is at t_i', then $t_i \leq t_i' \leq t_i + \text{jitter}$.

Figure C.M-1 demonstrates how a Subflow will be jittered even though the individual grants may not move from their relative position. During the first interval, three VoIP sessions are established, and they happen fall on the three grants. In the second interval, VoIP session 3 has been torn down. Since the CMTS does not know which Subflow is associated with which grant, it decides to remove the first grant. The remaining two calls shift to the other two grants. In the third interval, a new VoIP session 4 and a new grant have been added. The new call happens to fall on the new grant. The net effect is that the Subflows may move around within their jitter interval.

The advantage of a small jitter interval is that the VoIP receive jitter buffer may be kept small. The disadvantage is that this places a scheduling constraint on the CMTS.

The boundary of a Nominal Grant Interval is arbitrary and is not communicated between the CMTS and the CM.

NOTE – More dramatic events like the loss of a downstream MAP, or the frequency hopping of an upstream may cause subflows to jitter outside of this jitter window.

C.M.1.5 Synchronization isues

There are two synchronization problems that occur when carrying CBR traffic such as VoIP sessions across a network. The first is a frequency mismatch between the source clock and the destination clock. This is managed by the VoIP application, and is beyond the scope of this annex. The second is the frequency mismatch between the CBR source/sinks, and the bearer channel that carries them.

Specifically, if the clock that generates the VoIP packets towards the upstream is not synchronized with the clock at the CMTS which is providing the UGS service, the VoIP packets may begin to accumulate in the CM. This could also occur if a MAP was lost, causing packets to accumulate.

When the CM detects this condition, it asserts the Queue Indicator in the Service Flow EH Element. The CMTS will respond by issuing an occasional extra grant so as to not exceed 1% of the provisioned bandwidth. (This corresponds to a maximum of one extra grant every one hundred grants.) The CMTS will continue to supply this extra bandwidth until the CM desserts this bit.

A similar problem occurs in the downstream. The far end transmitting source may not be frequency synchronized to the clock which drives the CMTS. Thus the CMTS SHOULD police at a rate slightly higher than the exact provisioned rate to allow for this mismatch and to prevent delay buildup or packet drops at the CMTS.

C.M.2 Unsolicited Grant Service with Activity Detection (UGS-AD)

C.M.2.1 Introduction

Unsolicited Grant Service with Activity Detection (UGS-AD) is an Upstream Flow Scheduling Service Type. This clause describes one application of UGS-AD which is the support for Voice Activity Detection (VAD). VAD is also known as Silence Suppression and is a voice technique in which the transmitting CODEC sends voice samples only when there is significant voice energy present. The receiving CODEC will compensate for the silence intervals by inserting silence or comfort noise equal to the perceived background noise of the conversation.

The advantage of VAD is the reduction of network bandwidth required for a conversation. It is estimated that 60% of a voice conversation is silence. With that silence removed, that would allow a network to handle substantially more traffic.

Subflows in this context will be described as active and inactive. Both of these states of within the MAC Layer QOS state known as Active.

C.M.2.2 MAC configuration parameters

The configuration parameters include all of the normal UGS parameters, plus:

- Nominal Polling Interval.
- Tolerated Poll Jitter.

An explanation of these parameters and their default values is provided in Annex C.C.

C.M.2.3 Operation

When there is no activity, the CMTS sends polled requests to the CM. When there is activity, the CMTS sends Unsolicited Grants to the CM. The CM indicates the number of grants per interval which it currently requires in the active grant field of the UGSH in each packet of each Unsolicited Grant. The CM may request up to the maximum active Grants per Interval. The CM constantly sends this state information so that no explicit acknowledgment is required from the CMTS.

It is left to the implementation of the CM to determine activity levels. Implementation options include:

- Having the MAC layer service provide an activity timer per Classifier. The MAC layer service would mark a Subflow inactive if packets stopped arriving for a certain time, and mark a Subflow active the moment a new packet arrived. The number of Grants requested would equal the number of active Subflows.
- Having a higher layer service entity such as an embedded media client which indicates activity to the MAC layer service.

When the CM is receiving polled requests and it detects activity the CM requests enough bandwidth for one Grant per Interval. If activity is for more than one Subflow, the CM will indicate this in the active grant field of the UGSH beginning with the first packet it sends.

When the CM is receiving Unsolicited Grants, then detects new activity and asks for one more grant, there will be a delay in time before it receives the new grant. During that delay, packets may build up at the CM. When the new Unsolicited Grant is added, the CMTS will burst extra Grants to clear out the packet buildup.

When the CM is receiving Unsolicited Grants, then detects inactivity on a Subflow and asks for one less grant, there will be a delay in time before the reduction in Grants occurs. If there has been any build up of packets in the upstream transmit queue, the extra grants will reduce, or empty the queue. This is fine, and keeps system latency low. The relationship of which Subflow is getting which specific grant will also change. This effect appears as low frequency jitter that the far end must manage.

When the CM is receiving Unsolicited Grants and detects no activity on any of its Subflows, it will send one packet with the active grants field of the UGSH set to zero grants, and then cease transmission. The CMTS will switch from UGS mode to Real Time Polling mode. When activity is again detected, the CM sends a request in one of these polls to resume delivery of Unsolicited Grants. The CMTS ignores the size of the request and resumes allocating Grant Size grants to the CM.

It is not necessary for the CMTS to separately monitor packet activity since the CM does this already. Worst case, if the CMTS misses the last packet which indicated zero grants, the CMTS and CM would be back in sync at the beginning of the next talk spurt. Because of this scenario, when the CM goes from inactive to active, the CM must be able to restart transmission with either Polled Requests or Unsolicited Grants.

C.M.2.4 Example

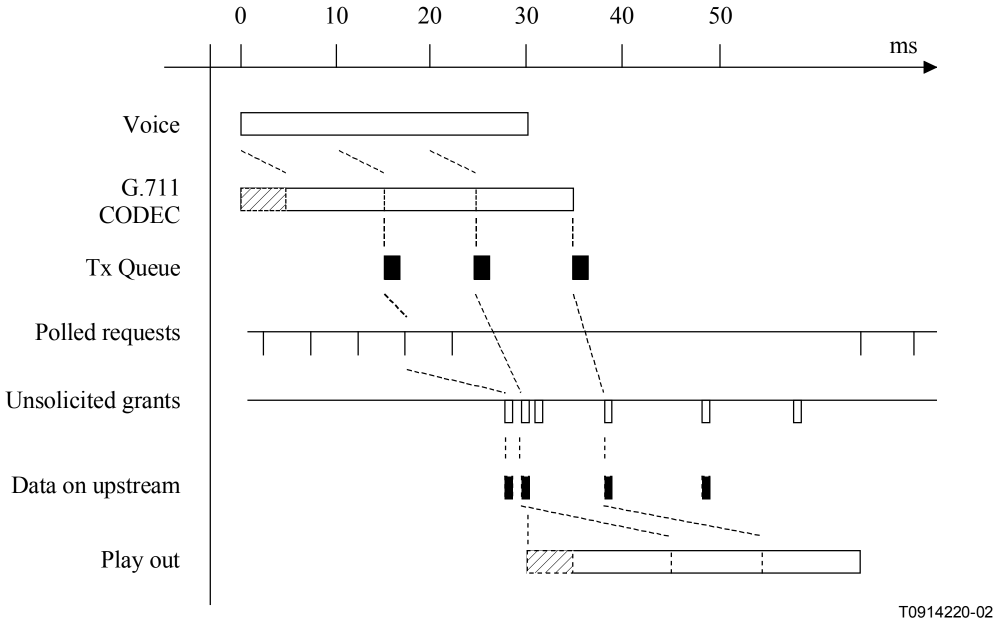


Figure C.M-2/J.112 – VAD start-up and stop

Figure C.M-2 shows an example of a single G.711 (64 kbit/s) voice call with a packet size of 10 ms, and a receive jitter buffer that requires a minimum of 20 ms of voice (thus 2 packets) before it will begin playout.

Assume voice begins at time zero. After a nominal processing delay and a 10 ms packetization delay, the DSP CODEC generates voice packets which are then transferred to the upstream transmit queue. The next Polled Request is used which results in the start of the Unsolicited Grants some time later. Additional Unsolicited Grants are immediately issued to clear out the upstream queue.

These packets traverse the network and arrive at the receive jitter buffer. The 20 ms minimum jitter buffer is met when the second packet arrives. Because the packets arrived close together, only an additional few milliseconds of latency has been added. After a nominal processing delay, playout begins.

When the voice spurt ends, the CM sends one remaining packet with no payload and with the active grants field of the UGSH set to zero grants. Some time later, UGS stops, and Real Time Polling begins.

C.M.2.5 Talk spurt grant burst

The extra burst of Unsolicited Grants when a flow becomes active is necessary because the jitter buffer at the receiving CODEC typically waits to have a minimum amount of voice samples before beginning the playout. Any delay between the arrival of these initial packets will add to the final latency of the phone call. Thus, the sooner the CMTS recognizes that the CM has packets to send and can empty the CM's buffer, the sooner those packets will reach the receiver, and the lower the latency that will be incurred in the phone call.

It is an indeterminate problem as to how many grants must be burst. When the CM makes its request for an additional grant, one voice packet has already accumulated. The CM has no idea how many extra grants to request as it has no idea of the round trip response time it will receive from the CMTS, and thus how many packets may accumulate. The CMTS has a better idea, although it does not know the far end jitter buffer requirements.

The solution is for the CMTS to choose the burst size, and burst these grants close together at the beginning of the talk spurt. This occurs when moving from Real Time Polling to UGS, and when increasing the number of UGS Grants per Interval.

A typical start-up latency that will be introduced by the Request to Grant response time is shown in Table C.M-1.

Table C.M-1/J.112 – Example request to grant response time

Variable		Example value	
1	The time taken from when the voice packet was created to the time that voice packet arrives in the CM upstream queue.	0-1	ms
2	The time until a polled request is received. The worst case time is the Polled Request Interval.	0-5	ms
3	The Request-Grant response time of the CMTS. This value is affected by MAP length and the number of outstanding MAPS.	5-15	ms
4	The round trip delay of the HFC plant including the downstream interleaving delay.	1-5	ms
	Total	**6-26**	**ms**

This number will vary between CMTS implementations, but a reasonable number of extra grants to expect from the example above would be:

Table C.M-2/J.112 – Example extra grants for new talk spurts

UGS interval	Extra grants for new talk spurts
10 ms	2
20 ms	1
30 ms	0

Once again it is worth noting that the CMTS and CM cannot and do not associate individual Subflows with individual grants. That means that, when current Subflows are active and a new Subflow becomes active, the new Subflow will immediately begin to use the existing pool of grants. This potentially reduces the start-up latency of new talk spurts, but increases the latency of the other Subflows. When the burst of grants arrives, it is shared with all the Subflows, and restores, or even reduces, the original latency. This is a jitter component. The more Subflows that are active, the less impact that adding a new Subflow has.

C.M.2.6 Admission considerations

Note that when configuring the CMTS admission control, the following factors must be taken into account.

VAD allows the upstream to be over provisioned. For example, an upstream that might normally handle 24 VoIP sessions might be over provisioned as high as 36 (50%) or even 48 (100%). Whenever there is over provisioning, there exists the statistical possibility that all upstream VoIP sessions may become active. At that time, the CMTS may be unable to schedule all the VoIP traffic. Additionally, the talk spurt grant bursts would be stretched out. CM implementations of VAD should recognize this possibility, and set a limit as to how many packets they will allow to accumulate on its queue.

Occasional saturation of the upstream during VAD can be eliminated by provisioning the maximum number of permitted VoIP sessions to be less than the maximum capacity of the upstream with all voice traffic (24 in the previous example). VAD would cause the channel usage to drop from 100% to around 40% for voice, allowing the remaining 60% to be used for data and maintenance traffic.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2003