INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.112
Annex B
Implementor's Guide
(April 2003)

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

Implementor's Guide for

ITU-T Recommendation J.112 Annex B:
Data-over-cable service interface specifications: Radio-frequency interface specification

Implementors' Guide to Recommendation J.112 – Annex B

Summary:

This Implementor's Guide has been approved by the Study Group as a basis for a future Amendment to Recommendation J.112 Annex B (03/01) and J.112 Annex B Amendment 1 (02/02). This Implementor's Guide will be superceded by that future Amendment.

All proposed text changes are indicated in this document by color coding of text. Unchanged text appears normally. Proposed deleted text appears in ~~red strikethrough~~, new text appears in blue double underline, and where text has been moved from one location to another, the "moved from" text is in ~~green strikethrough~~, whereas the "moved to" location appears in green double underline. Comments and instructions to the editors are highlighted in yellow.

Editor's Notes:
This document was produced electronically using comparison software. All minor changes such as US spelling vs. European, smart quotes vs. straight quotes, differences in hyphens, and changing "subclause" to "section" should be ignored.

The source documents, and additional details regarding the document comparison, can be found on the final page of this guide.

For purposes of retaining smaller file size and page count of this document, of all figures being replaced, only the new versions are shown in this document, that is, the original figures are not shown.

Contact: Greg White
Cable Television Laboratories, Inc.
United State of America

Tel: +1 303-661-9100
Fax: +1 303-661-9199
Email: g.white @cablelabs.com

B.1.3.2 Reference architecture [move Note text from below Figure 1-2 to above figure]

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

NOTE – This architecture illustrates the North American frequency plans only and is not normative for European applications. Refer to Subclause B.1.1 for applicability.

FIGURE **1-2**

B.1.3.3 Categories of interface specification [edit text as indicated below]

The basic reference architecture of Figure 1-2 involves ~~three~~five categories of interface.

~~NOTE – This architecture illustrates the North American frequency plans only and is not normative for European applications. Refer to subclause B.1.1 for applicability.~~

B.2 References

[update references as indicated below]

~~[DOCSIS5] DOCSIS5: "Data-Over-Cable Service Interface Specifications, 1.1 Operations Support System Interface Specification, SP-OSSIv1.1-I02-000714".~~

~~[DOCSIS8] DOCSIS8: "Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I05-000714".~~

~~[DOCSIS9] DOCSIS9: "Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFI-I06-000630".~~

[EN 300 429] ETSI EN 300 429 V1.2.1: "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems", April 1998.

[EN 50083-1] CENELEC EN 50083-1: "1993, Cabled distribution systems for television, sound and interactive multimedia signals, Part 1: Safety requirements".

[EN 50083-2] CENELEC EN 50083-2: 1995, "Cabled distribution systems for television, sound and interactive multimedia signals, Part 2: Electromagnetic compatibility for equipment".

[EN 50083-7] CENELEC EN 50083-7: ~~"Cabled distribution systems~~"Cable networks for television ~~and~~signals, sound signals~~;~~ and interactive services, Part 7: System performance".

[EN 50083-10] CENELEC EN 50083-10: "Cable networks for television signals, sound signals and interactive services, Part 10: System performance of return paths".

[EN 60950] CENELEC EN 60950: "Safety of information technology equipment".

~~[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).~~

[IGMP] Fenner W., IGMP-based Multicast Forwarding ("IGMP Proxying"), magma-igmp-proxy-00.txt, (work in progress).

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

[PKTCBL-MGCP] PKTCBL-MGCP: "PacketCable Specifications, Network-Based Call Signalling Protocol Specification, PKT-SP-EC-MGCP-I02-991201".

[J162] ITU-T Recommendation J.162 - Network call signalling protocol for the delivery of time critical services over cable television networks using cable modems (03/01)

[PKT-DQOS] PKT-DQOS: "PacketCable Specifications, Dynamic Quality of Service Specification, PKT-SP-DQOS-I01-991201".

[J163] ITU-T Recommendation J. 163 - Dynamic quality of service for the provision of real-time services over cable television networks using cable modems. (03/01)

[RFC-1493] Definitions of Managed Objects for Bridges. E. Decker, P. Langille, A. Rijsinghani, &and K. McCloghrie. July 1993. (Obsoletes RFC 1286)".

[RFC 1700] IETF RFC 1700 (October 1994): Assigned Numbers. J. Reynolds, J. Postel.

[RFC-3046] Patrick, M., DHCP Relay Agent Information Option, IETF RFC-3046, January, 2001.

[SCTE1] SCTE 22-1 2002, DOCSIS 1.0, Radio Frequency Interface Standard.

[SCTE2] SCTE 22-2 2002, DOCSIS 1.0, Baseline Privacy Interface Standard.

[SCTE3] SCTE 23-3 2003, DOCSIS 1.1 Operations Support System Interface Standard.

[X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002: "Information Technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[Editor's Notes: Replace all [DOCSIS5] references globally with [SCTE3];
replace all [DOCSIS8] with Annex B.O of this document, with the exception noted in B.C.1.1.4.7
replace all [DOCSIS9] with [SCTE1]

B.3.1 Definitions [edit text as indicated below]

Bridge Protocol Data Unit (BDU):

Spanning tree protocol messages as defined in [RFC 1350][ISO/IEC10038].

Guard Band~~Time~~
Minimum time allocated between bursts in the upstream referenced from the symbol centre of the last symbol of a burst to the symbol centre of the first symbol of the following burst. The guard ~~time~~band should be at least the duration of five symbols plus the maximum system timing error.

Guard Time
The term guard time is similar to the guard band, except that it is measured from the end of the last symbol of one burst to the beginning of the first symbol of the preamble of an immediately following burst. Thus, the guard time is equal to the guard band – 1.

B.4 Functional assumptions

[edit 1st paragraph as indicated]

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~~MUST be interoperable within the environment described in this clause.

B.5.1.2.1 General

[add new paragraph after figure 5-3]

Although provisions exist in this specification for frames to be passed from a higher-layer entity to be forwarded by the cable modem, these frames MUST be treated identically to frames arriving at the CPE port. In particular, all of the forwarding rules defined in subclause B.5.1.2.3 MUST apply to these frames.

B.5.1.2.3.2 Forwarding

[edit text in this subclause as follows]

CM forwarding in both directions MUST conform to the following general 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, MUST be delivered in the order that they are received on a given Service Flow (refer to subclause B.8.1.2.~~3~~.5) ~~MUST be delivered in the order that they are received~~. In the upstream direction, the CM may perform one or more frame/packet processing functions on frames received from the CMCI prior to classifying them to a Service Flow. In the downstream direction, the CM may perform one or more frame/packet processing functions on frames received from the HFC prior to transmitting them on the CMCI. Example processing functions include: DOCSIS protocol filtering as specified in [DOCSIS5] subclause B.6.3, a policy-based filtering service as described in Subclause B.10.1.6.1 and Annex E, and priority-based queuing to support 802.1P/Q services.

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

- Frames addressed to unknown destinations MUST NOT be forwarded from the cable port to the ~~Ethernet port~~CPE ports.
- Broadcast frames MUST be forwarded to the ~~Ethernet port~~CPE ports, 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 subclause B.5.3.1). Multicast frames MUST NOT be forwarded unless both mechanisms are in a permissive state.

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

- Frames addressed to unknown destinations MUST be forwarded from ~~the Ethernet port~~all CPE ports 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 subclause B.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~~all CPE ports 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.~~
- Frames addressed to destination addresses that are learned from all CPE ports MUST be filtered as local traffic.

B.5.3.1 Requirements for IGMP Management

[add new text and subclause (previously empty), renumber subsequent subclauses appropriately as follows]

There are two basic modes of IGMP capability that are applicable to a DOCSIS 1.1 device (CMTS and CM). The first mode is a *passive* operation in which the device selectively forwards IGMP based upon the known state of multicast session activity on the subscriber side (an example of this is described in Annex L). In *passive* mode, the device derives its IGMP timers based on the rules specified in subclause B.5.3.1.1 of the RFI. The second mode is an *active* operation in which the device terminates and initiates IGMP based upon the known state of multicast session activity on the subscriber side. One example of the latter, active, mode is commonly referred to as an IGMP-Proxy implementation side (as described in [ID-IGMP]). A more complete example of an active IGMP device is that of a Multicast Router.

Active and Passive IGMP devices MUST support IGMPv2 [RFC-2236]

B.5.3.1.1 IGMP Timer Requirements

The following IGMP timer requirements apply only when the device (CMTS / CM) is operating in passive IGMP mode:

- The device MUST NOT require any specific configuration for the associated multicast timer values and MUST be capable of adhering to the timers specified in this subclause.
- The device MAY provide configuration control that overrides the default values of these timers.
- The device 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, MQn- MQn-1), where MQI is the Membership Query Interval in seconds, n is the number of Membership Queries seen, and MQn 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 seconds if not otherwise set (or set to 0) in the Membership Query packet.

B.~~5.3.1.1~~5.3.1.2 CMTS Rules

- If link layer forwarding of multicast packets 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 IGMP v2 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~~support Active IGMP ~~protocol [RFC 2236] and MUST act as the only IGMP v2 Querier on its downstream RF interfaces~~mode.
- If link-layer forwarding of multicast packets is used, the CMTS SHOULD support Passive IGMP mode and MAY support Active IGMP mode.

B.~~5.3.1.2~~5.3.1.3 CM Rules

The CM MUST support IGMP with the ~~following~~ cable -specific rules specified in this subclause.

The CM MUST implement the passive IGMP mode. Additionally, the CM MAY implement the active IGMP mode. If the CM implements the active IGMP mode, the CM MUST support a capability to switch between modes.

Multicast Forwarding Requirements

The following requirements apply to ~~conformant CMs~~both passive and active modes of IGMP operations:

- The CM MUST NOT forward Membership Queries from its CPE interface to its RF interface.
- The CM MUST NOT forward Membership Reports or IGMP v2 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.
- 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 * MQI) + QRI, where MQI is the Membership Query Interval and QRI is the Query Response Interval.
- 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 following requirements apply only when the CM is operating in passive IGMP mode:

- 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. In particular, the CM MUST forward ALL-HOSTS Group Queries that pass permit filters on its RF interface to its CPE interface. ~~or the~~
- Upon receiving a Membership Report on its CPE interface, the CM MUST start a random timer between 0 and 3 seconds. During this time period, the CM MUST discard any additional Membership Reports received in its CPE interface for the associated multicast group. If the CM receives a Membership Report on its HFC interface for the associated multicast group, the CM MUST discard the Membership Report received on its CPE interface. If the random timer expires without the reception of a Membership Report on the CMs HFC interface, the CM MUST transmit the Membership Report received on its CPE interface.

The following requirements apply only when the CM is operating in active IGMP mode:

- The CM MUST implement the Host portion of the IGMP v2 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 IGMP v2 protocol, it~~ The CM MUST act as an IGMP v2 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 subclause. 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 * MQI) + 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~~ such 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 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.
  - The CM MUST treat Unsolicited Membership Reports (IGMP 'JOIN's) from its CPE interface as ~~responses~~a response to a Membership Query received on its RF interface. Upon receipt of ~~a~~this unsolicited 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~~3 seconds. 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 IGMP v2 Leave is received for this group from the CPE interface.~~

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

B.5.4 Above the Network Layer
[edit 2nd bullet, add two paragraphs following last bullet]

- TFTP (Trivial File Transfer Protocol, [RFC -1350]), a file transfer protocol, MUST be supported for downloading operational software and configuration information, as modified by TFTP Timeout Interval and Transfer Size Options [RFC -2349].

- Time of Day Protocol [RFC 868], MUST be supported to obtain the time of day.

DHCP, TFTP, and ToD client messages generated by the CM MUST only be sent via the RF Interface. DHCP, TFTP and ToD client messages include DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE, DHCPINFORM, TFTP-RRQ, TFTP-ACK, and ToD request.

The CM's DHCP, TFTP, and ToD client MUST ignore DHCP, TFTP, and ToD server messages received on the CMCI port. DHCP, TFTP, and ToD server messages include: DHCPOFFER, DHCPACK, DHCPNAK, TFTP-DATA, and ToD time message.

B.6.2.1 Overview
[edit text as shown and add sentence at the end of the 4th paragraph]

The PMD sublayer can support a near -continuous mode of transmission, wherein ramp -down of one burst MAY overlap the ramp -up of the following burst, so that the transmitted envelope is never zero. The system timing of the TDMA transmissions from the various CMs MUST provide that the centre of the last symbol of one burst and the centre of the first symbol of the preamble of an immediately following burst are separated by at least the duration of five symbols. The guard ~~time~~band MUST be greater than or equal to the duration of five symbols plus the maximum timing error. Timing error is contributed by both the CM and CMTS. CM timing performance is specified in subclause B.6.2.7. Maximum timing error and guard ~~time~~band may vary with CMTSs from different vendors. The term guard time is similar to the guard band, except that it is measured from the end of the last symbol of one burst to the beginning of the first symbol of the preamble of an immediately following burst. Thus, the guard time is equal to the guard band - 1.

B.6.2.6 Transmit pre-equalizer
[4th and 5th paragraph]

Prior to making an initial ranging request and whenever the upstream channel frequency or upstream channel symbol rate changes, the CM MUST initialize the coefficients of the pre-equalizer to a default setting in which all coefficients are zero except the real coefficient of the first tap (*i.e.* F1). During initial ranging, the CM, not the CMTS, MUST compensate for the delay (ranging offset) due to a shift from the first tap to a new main tap location of the equalizer coefficients sent by the CMTS. The pre-equalizer coefficients are then updated though the subsequent ranging process (periodic station maintenance). The CMTS MUST ~~NOT~~not move the main tap location during periodic station maintenance. Equalizer coefficients may be included in every RNG-RSP message, but typically they only occur when the CMTS determines the channel response has significantly changed. The frequency of equalizer coefficient updates in the RNG-RSP message is determined by the CMTS.

The CM MUST normalize the pre-equalizer coefficients in order to guarantee proper operation (such as not to overflow or clip). The CM MUST ~~also compensate for the~~NOT change ~~in~~its commanded output transmit power due to ~~the~~a gain ~~(~~or loss~~)~~ of the new coefficients. The actual output transmit power is subject to the power accuracy requirements defined in Subclause B.6.2.9.1. If the CM equalizer structure implements the same number of coefficients as assigned in the RNG-RSP message, then the CM MUST ~~NOT~~not change the location of the main tap in the RNG-RSP message. If the CM equalizer structure implements a different number of coefficients than defined in the RNG-RSP message, the CM MAY shift the location of the main tap value. Again, in doing so, the CM MUST adjust its ranging offset, in addition to any adjustment in the RNG-RSP message, by an amount that compensates for the movement of the main tap location.

B.6.2.7 Burst profiles
[add new text after the 4th paragraph following Table 6-5]

…Negative ranging offset adjustments will cause the 96 symbol guard to be violated. To assure that this does not happen, the CMTS MUST allow extra guard time between bursts that is at least equal to the amount of negative ranging offset.

To provide backward interoperability with DOCSIS 1.0 and 1.1 equipment, when making a symbol rate change the CM MUST employ the following timing offsets when changing symbol rates. The offsets in the table correspond to the contribution of DOCSIS 1.0 and 1.1 legacy upstream receivers to changes in latency when making symbol rate changes. The timing offset to apply is the difference between the entry in the table corresponding to the new symbol rate and the entry corresponding to the original symbol rate. The offsets are referenced to the center of the first symbol in the burst, which is the reference point for burst timing as stated in Subclause B.6.2.8. Specification of these offsets is needed so that CMs apply uniform adjustments to their ranging offsets and so that CMTSes can appropriately handle CMs that apply these offsets when making symbol rate changes.

Symbol Rate	Timing Offset (in units of 1/64 time ticks referenced to 2.56 Msps)
2.56 Msps	0 (reference)
1.28 Msps	24
0.64 Msps	72
0.32 Msps	168
0.16 Msps	360

As an example, suppose a CM is on an upstream channel operating at 1.28 Msps. Now, suppose the UCD message from the CMTS changes the symbol rate of the channel to 0.32 Msps. The CM applies an additional timing offset of 168 - 24 = 144 to its ranging offset to compensate for this symbol rate change. The value of 144 is positive, and thus, the CM will add to its ranging offset so that it effectively transmits earlier by 144 units of 1/64 time ticks.

Furthermore, in changing symbol rates, if a CM has its own contribution to a change in latency, the CM MUST also compensate for this CM-specific latency difference. This is in addition to the offset applied from the values in the table above, which result from legacy CMTS upstream receiver contributions to changes in latency. The requirements for CM burst timing accuracy found earlier in this subclause, referenced to the symbol rate that is the lower of the original and the new symbol rate, apply after the symbol rate change with the required timing offsets above considered.

A CMTS that does not apply the same internal physical delay offsets as the legacy DOCSIS upstream CMTS receiver implementation is capable of receiving a CM burst after a symbol rate change in any of the following ways but is not limited necessarily to only these ways:

a) The CMTS may implement the internal physical delay offset, as specified in the above table.

b) The CMTS may implement an internal timing compensation based on the expected offset in the above table.

c) The CMTS may increase the guard time.

d) The CMTS may send an unsolicited RNG-RSP to each CM to adjust the delay offset. As discussed in subclause B.8.3.6, the CM is expected to be capable of adjusting its timing offset at any time with the accuracy specified within this subclause.

If Channel Frequency is to be changed, then the CM MUST be able to implement the change between bursts as long as the CMTS allocates at least 96 symbols plus 100 ms between the last symbol centre of one burst and the first symbol of the following burst.

B.6.2.10.1 Spurious emissions
[edit 3rd paragraph]

The measurement bandwidth for the 3 (or fewer) Carrier Related Frequency Bands (below 42 MHz) is 160 kHz, with up to three 160 kHz bands, each with no more than –47 dBc, allowed to be excluded from the Bands within 5 MHz-to 42 MHz Transmitting Burst specs of Table 6-8. Carrier-related spurious emissions include all products whose frequency is a function of the carrier frequency of the upstream transmission, such as but not limited to carrier harmonics.

B.6.2.10.4.1 Amplitude

[edit frequency in column 1, row 1 and 4 of Table 6-9]

TABLE 6-9

Filter amplitude distortion

Frequency	Amplitude range	
	low	high
f_c - $5R_s$/8	-	–30 dB
f_c - R_s/2	–3.5 dB	–2.5 dB
f_c - 3 R_s/8 to f_c - R_s/4	–0.5 dB	+0.3 dB
f_c - R_s/4 to f_c + R_s /4	–0.3 dB	+0.3 dB
f_c + R_s/4 to f_c + 3 R_s/8	–0.5 dB	+0.3 dB
f_c + R_s/2	–3.5 dB	–2.5 dB
f_c + $5R_s$/8	-	–30 dB

B.6.3.7 CMTS timestamp jitter

[edit as shown below]

The CMTS timestamp jitter ~~must~~MUST be less than 500 ns peak-to-peak at the output of the Downstream Transmission Convergence Sublayer. This jitter is relative to an ideal Downstream Transmission Convergence Sublayer that transfers the MPEG packet data to the Downstream Physical Media Dependent Sublayer with a perfectly continuous and smooth clock at the MPEG packet data rate. Downstream Physical Media Dependent Sublayer processing MUST NOT be considered in timestamp generation and transfer to the Downstream Physical Media Dependent Sublayer.

Thus, any two timestamps N1 and N2 (N2 > N1) which were transferred to the Downstream Physical Media Dependent Sublayer at times T1 and T2 respectively must satisfy the following relationship:

$$| (N2 - N1)/~~10240000~~f_{CMTS} - (T2 - T1) | < 500 ~~ns~~ x10^{-9}$$

In the equation, the value of (N2-N1) is assumed to account for the effect of rollover of the timebase counter, and T1 and T2 represent time in seconds. f_{CMTS} is the actual frequency of the CMTS master timebase and may include a fixed frequency offset from the nominal frequency of 10.24 MHz. This frequency offset is bounded by a requirement further below in this subclause.

The jitter includes inaccuracy in timestamp value and the jitter in all clocks. The 500 ns allocated for jitter at the Downstream Transmission Convergence Sublayer output ~~must~~MUST be reduced by any jitter that is introduced by the Downstream Physical Media Dependent Sublayer.

B.8.2.2.1 Variable-length packets

[Edit the following 3 tables as indicated]

TABLE 8-3

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	x (0 - 240) bytes
HCS	MAC Header Check Sequence	16 bits
Packet ~~data~~Data Packet PDU:	~~Packet PDU:~~DA - 48 bit Destination address SA - 48 bit Source address Type/LEN - 16 bit Ethernet type or [ISO8802-3] length field User Data (variable length, 0 - 1500 bytes) CRC - 32-bit CRC over packet PDU (as defined in Ethernet/[ISO8802-3])	n bytes
	Length of Packet MAC frame	6 + x + n bytes

TABLE 8-4

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	x (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

TABLE 8-7

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	x (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

B.8.2.7 Fragmented MAC Frames
[edit 5th paragraph]

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, the following fields~~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~~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.

B.8.2.8.1 Error Recovery During Fragmentation
[edit 1st paragraph]

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~~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.

B.8.3.5 Ranging Request (RNG-REQ)
[edit SID parameter following Figure 8-21]

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 upstream, downstream, ~~(~~or both upstream and 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~~Primary 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~~ Temporary SID if during or before registration.
- Primary SID if after registration.

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

TABLE 8-21

Ranging Response Message Encodings

Name	Type (1 byte)	Length (1 byte)	Value (Variable Length)
Timing Adjust	1	4	TX timing offset adjustment (signed 32 -bit, units of (6.25 ~~micros~~microsec/64))
Power Level Adjust	2	1	TX Power offset adjustment (signed 8 -bit, 1/4 -dB units)
Offset Frequency Adjust	3	2	TX frequency offset adjustment (signed 16 -bit, 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	Centre 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

B.8.3.6.3 Overriding Channels ~~During Initial Ranging~~Prior to Registration
[edit subclause title, and last paragraph]

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.1.1.2, UCC-REQ, and DCC-REQ mechanisms are available for moving the modem to a new upstream channel, and only the C.1.1.1 ~~mechanism~~ and DCC-REQ ~~is~~mechanisms are available for moving the modem to a new downstream channel.

B.8.3.7 Registration Request (REG-REQ)
[modify paragraphs and bullet lists as shown below]

A Registration Request MUST be transmitted by a CM at initialization after receipt of a CM parameter file~~.~~, except as outlined in subclauses B.11.2.8 and B.11.2.9.

Configuration File Settings:

- All configuration settings included in the CMTS MIC calculation as specified in Subclause B.D.3.1~~Downstream Frequency~~
- ~~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.

[…]

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~~;~~
- SNMPv3 Kickstart Value
- CPE Ethernet MAC Address~~;~~
- HMAC Digest~~;~~
- End Configuration Setting~~;~~
- Pad Configuration Setting~~;~~
- Telephone Settings Option~~.~~
- SNMPv3 Notification Receiver

A Registration Acknowledge MUST be transmitted by the CM in response to a REG-RSP from the CMTS~~.~~ with a confirmation code of ok (0). 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 8-28.

B.8.3.10 Upstream Channel Change Request (UCC-REQ)

[delete text (after Figure 8-29) as shown below]

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 should perform once synchronized to the new upstream channel.~~

~~B.8.3.10.1 Upstream Channel ID Encodings~~

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

~~*B.*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 re-ranging, if any, to perform. The CMTS can make this decision based upon its knowledge of the differences between the old and new1nnels.~~

~~For example, areas of upstream spectrum are often configured in groups. A UCC-REQ to an adjacent channel within a group may not warrant re-ranging. 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 - channel to which the CM is to switch for upstream transmissions. 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 should not be used in physical plants where upstream transmission characteristics are not consistent.is an 8-bit field.~~

B.8.3.11 Upstream Channel Change Response (UCC-RSP)

[edit 3rd paragraph]

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

B.8.3.13 Dynamic Service Addition - Response (DSA-RSP)

[edit text as shown below]

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.~~ The CMTS MUST include the complete specification of the Classifier in the DSA-RSP, including a newly assigned Classifier Identifier. The CM MUST NOT include the specification of the Classifier in the DSA-RSP.
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.~~ The CMTS MUST include the complete specification of the Service Flow in the DSA-RSP, including a newly assigned Service Flow Identifier and an expanded service class name if applicable. The CM MUST NOT include the specification of the Service Flow in the DSA-RSP.
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.~~ The CMTS MUST include the complete specification of

the PHS Parameters in the DSA-RSP, including a newly assigned PHS Index, a Classifier Identifier and a Service Flow Identifier. The CM MUST NOT include the specification of the PHS Parameters.

If the transaction is unsuccessful due to Service Flow Parameters, Classifier Parameters, or Payload Header Suppression Parameters, and the Confirmation Code is not one of the major error codes in subclause B.C.4.2, the DSA-RSP MUST contain at least one of the following:

B.8.3.14 Dynamic Service Addition ~~-~~ = Acknowledge (DSA-ACK)

(edits as shown below]

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

B.8.3.16 Dynamic Service Change - Response (DSC-RSP)

[edits follow figure 8-35]

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.~~ The CMTS MUST include the complete specification of the Classifier in the DSC-RSP, including a newly assigned Classifier Identifier for new Classifiers. The CM MUST NOT include the specification of the Classifier in the DSC-RSP.

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.~~ The CMTS MUST include the complete specification of the Service Flow in the DSC-RSP, including an expanded service class name if applicable. The CMTS MUST include a SID in the DSC-RSP if a Service Flow Parameter Set contained an upstream Admitted QoS Parameter Set and this Service Flow does not have an associated SID. If a Service Flow Parameter set contained a Service Class Name and an Admitted QoS Parameter Set, the CMTS MUST include the QoS Parameter Set corresponding to the named Service Class in the DSC-RSP. If specific QoS Parameters were also included in the classed Service Flow request, the CMTS MUST include these QoS Parameters in the DSC-RSP instead of any QoS Parameters of the same type of the named Service Class. The CM MUST NOT include the specification of the Service Flow in the DSC-RSP.

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.~~ The CMTS MUST include the complete specification of the PHS Parameters in the DSC-

RSP, including a newly assigned PHS Index for new PHS rules, a Classifier Identifier and a Service Flow Identifier. The CM MUST NOT include the specification of the PHS Parameters.

If the transaction is unsuccessful due to Service Flow Parameters, Classifier Parameters, or Payload Header Suppression Parameters, and the Confirmation Code is not one of the major error codes in subclause B.C.4.2, the DSC-RSP MUST contain at least one of the following:

B.8.3.18 Dynamic Service Deletion - Request (DSD-REQ)
(edits as shown below]

A DSD-Request MAY be sent by a CM or CMTS to delete ~~An~~a single existing Upstream Service Flow and/or a single existing Downstream Service Flow. The format of a DSD-Request MUST be as shown in Figure 8-37.

Parameters MUST be as follows:

Service Flow Identifier	~~The SFID to be deleted.~~ If this value is non-zero it is the SFID of a single Upstream or single Downstream Service Flow to be deleted. If this value is zero the Service Flow(s) to be deleted will be identified by SFID(s) in the TLV's. If this value is non-zero then any SFIDs included in the TLV's MUST be ignored.
Transaction ID	Unique identifier for this transaction assigned by the sender.

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

Service Flow ~~Reference~~ **Identifier**	~~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 11-21.~~ The SFID(s) to be deleted, which MUST be encoded per C.2.2.3.2. The Service Flow Identifier TLV MUST be the only Service Flow Encoding sub-TLV used.

B.8.3.20 Dynamic Channel Change - Request (DCC-REQ)
(edits as shown below]

A CMTS MUST generate DCC-REQ message in the form shown in Figure 8-39 including the following parameter:

UCD Substitution	Provides a copy of the UCD for the new channel. ~~This TLV occurs once and contains one UCD.~~

If Privacy is enabled, a DCC-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 Annex C.1.4.3)

B.8.3.20.1.2.6 SYNC Substitution

[Add new section, text moved from 8.3.20.1.5]

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
2.6	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 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 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.

B.8.3.20.1.3 Initialization Technique

[edit 3rd paragraph]

If a complete re-initialization is not required, some re-ranging ~~MAY~~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 re-ranging. 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. Re-ranging ~~MAY~~may also be required if there is any difference in the PHY parameters between the old and new channels.

B.8.3.20.1.4 UCD Substitution

[edit 3rd and 4th paragraph]

If the length of the UCD exceeds 254 bytes, the UCD MUST be fragmented into two or more successive Type 4 elements. Each fragment, except the last, MUST be 254 bytes in length. The CM reconstructs the UCD Substitution by concatenating the contents (Value of the TLV) of successive Type 4 elements in the order in which they appear in the DCC-REQ message. For example, the first byte following the length field of the second Type 4 element is treated as if it immediately follows the last byte of the first Type 4 element.

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 B) or longer, if the UCD message is lost.

B.8.3.20.1.5 ~~SYNC Substitution~~

[move entire text in this subclause to B.8.3.20.1.2.6 and renumber subsequent subclauses]

~~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 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.

B.8.3.20.1.6 B.8.3.20.1.5 *Security Association Identifier (SAID) Substitution*

When present, this TLV allows the CMTS to replace the Security Association Identifier (SAID) in the

---

B.8.3.20.1.7B.8.3.20.1.6 *Service Flow Substitutions*

[edit section as indicated]

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 MAYmay 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, and 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 should remain identical between the old and

B.8.3.20.1.7.1B.8.3.20.1.6.1 *Service Flow Identifier Substitution*

The CMTS MAYMUST include this Sub-TLV. The CM MUST observe this Sub-TLV.

B.8.3.20.1.7.2B.8.3.20.1.6.2 *Service Identifier Substitution*

B.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 subclause B.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.~~

~~*B*.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 subclause B.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.~~

~~B.8.3.20.1.7.5~~*B.8.3.20.1.6.3* *Unsolicited Grant Time Reference Substitution*

B.8.3.20.1.7 CMTS MAC Address

[Add new text as indicated below]

When present, this TLV allows the current CMTS to send the MAC address of the destination CMTS corresponding to the target downstream frequency. This TLV MUST be specified if the CM is changing downstream channels and UCD substitution is specified or if the CM is changing downstream channels and using initialization technique 4, use the new channel(s) directly.

Type	Length	Value
8	6	MAC Address of Destination CMTS

The CMTS SHOULD include the CMTS MAC address TLV. The CM SHOULD observe the CMTS MAC address TLV.

B.8.3.21 Dynamic Channel Change ~~-~~= Response (DCC-RSP)

[Edit text as indicated]

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 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~~/~~ downstream channel that it is already using or requesting that it switch to only an upstream 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.

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

Key Sequence Number The key sequence number of the Auth Key, which is used to calculate the HMAC-Digest (refer to Annex 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 Channel Change message's Attribute list. (Refer to subclause B.C.1.4.1)

B.8.3.22 Dynamic Channel Change ~~-~~= Acknowledge (DCC-ACK)

[Add text as indicated]

If Privacy is enabled, the DCC-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 Annex 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 Channel Change message's Attribute list. (Refer to subclause B.C.1.4.1)

B.8.3.23 Device Class Identification Request (DCI-REQ)

[Edit text as indicated]

A CM MAY ~~implement the DCI-REQ message. A CMTS MUST~~ implement the DCI-REQ message.

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~~

This is a 32-bit field where individual bits represent individual attributes of the CM. Bit #0 is the LSB of the field. Bits are set to 1 to ~~identify~~ select the ~~Behaviour of that value~~ attributes defined below.

bit #0 CPE Controlled Cable Modem (CCCM)

bits #1-31 reserved and must be set to zero

B.8.3.25 Upstream Transmitter Disable (UP-DIS) MAC Management Message

[Edit text as indicated]

~~The UP-DIS MUST be coded as follows:~~

~~MAC Management Message Header~~

The UP-DIS message provides additional functionality to permanently or temporarily disable the modem, as well as to disable the modem for a specified period of time. It is used to control the admission of certain modem types and groups to the network as early as immediately before registration. It can also be used for network troubleshooting, disabling the modems that violate network policies, or for avoiding request floods in a large network, when the CMTS goes on-line.

This message is stateless and can be issued by the CMTS at any time. The UP-DIS message ~~UP-Dis~~ is sent from a CMTS to a CM ~~and~~, there is no response from the CM transmitted back to the CMTS. UP-DIS messages may be unicast, in which case the destination address in the MAC header is the address of the selected CM, or multicast, in which case the destination address is a well-known MAC multicast address (see Annex A for details on well-known addresses).

The CMTS MUST be capable of transmitting the UP-DIS message. The CMTS can transmit UP-DIS messages either as a result of a triggering event detected by CMTS internally, or in response to a remote management command. Mechanisms for setting up, detecting, and reporting situations where the transmission of an UP-DIS message might be appropriate, are implementation dependent. Similarly, Signalling, which remotely instructs CMTS to ~~trigger the transmission~~transmit of the UP-DIS message, is outside the scope of this specification. One of the possible implementations may be SNMP command sent to CMTS over network.

~~The CM MAY~~CMs SHOULD support the UP-DIS message for easier network management.

~~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 B.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 and the CMs do not retain disabled status after power cycle, the CMTS ~~SHOULD~~MAY incorporate mechanisms to track disabled CMs by their MAC addresses ~~and~~. CMTS would resend an UP-DIS message as appropriate to the modems that ~~are powered~~were permanently disabled by the network operator, and then power cycled ~~and~~by the user to attempt to re-register. However, the same function may also be implemented by provisioning infrastructure on modem registration, and therefore if CMTS is unable to track disabled modems autonomously, it SHOULD be able to send UP-DIS in response to external command.

The UP-DIS message MUST be formatted as shown in Figure 8-44.

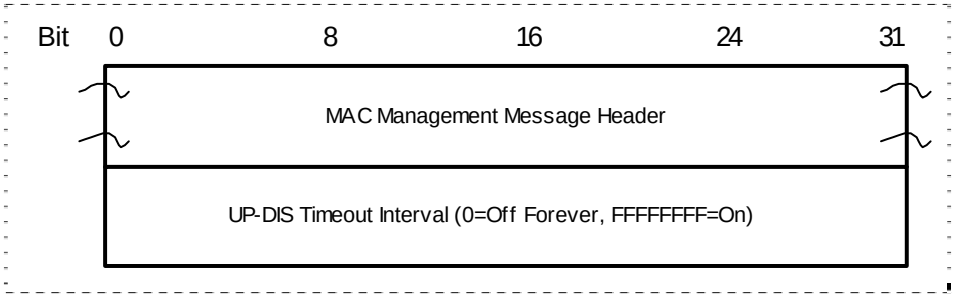


Figure 8-44. UP-DIS message format

The only parameter is UP-DIS Timeout Interval, which MUST be encoded as follows.

UP-DIS Timeout Interval: A 32-bit, unsigned integer representing the disable timeout interval in milliseconds. There are two special values defined:

00000000 permanently disables the upstream of the modem, as described below.

FFFFFFFF remotely reinitializes the MAC, which resumes the normal operation of the modem.

The CM MUST autonomously disable its upstream transmitter immediately upon receipt of an UP-DIS message with UP-DIS Timeout Interval = 0, regardless of any other transaction state (refer to subclause B.9), or the state of its control program. The modem stops all transmissions, but continues to listen to the MAC messages sent in the downstream. Once disabled, the CM upstream transmitter MUST only be re-enabled by power cycling the CM, or by an UP-DIS message with UP-DIS Timeout Interval = FFFFFFFF. All other UP-DIS messages MUST be ignored when the upstream is disabled.

If supported, the CM MUST autonomously reset its upstream transmitter upon receipt of an UP-DIS message with UP-DIS Timeout Interval = FFFFFFFF, regardless of any other transaction state (refer to Subclause B.9), or the state of its

control program. Resetting allows the modem to resume transmissions.

Additional, non-zero timeout values in the UP-DIS message SHOULD be supported. If supported, the CM MUST autonomously disable its upstream transmitter immediately upon receipt of an UP-DIS message with UP-DIS Timeout Interval T > 0 for a period of T milliseconds, regardless of any other transaction state (refer to Subclause B.9), or the state of its control program. Although the timeout T is specified in milliseconds, the CM MAY extend the specified timeout by up to 100 msec. When timeout expires, the CM SHOULD reinitialize MAC as appropriate, starting with the initial ranging process and registration, because there is no guarantee that the CMTS has not de-registered it. In the disabled state, all other UP-DIS messages MUST be ignored, except for an UP-DIS message with UP-DIS Timeout Interval = FFFFFFFF or 00000000.

B.9.1.3 Requests
[edit text at the end of the subclause as indicated below]

The request MUST include:

- The Service ID making the request~~;~~
- The number of mini-slots requested~~.~~

The CM MUST request the number of mini-slots ~~requested MUST be~~needed to transmit an entire frame, or a fragment containing the ~~total number~~entire remaining portion of a frame that ~~are desired~~a previous grant has caused to be fragmented. The frame may be a single MAC frame, or a MAC frame that has been formed by the ~~CM at the time~~concatenation of ~~the~~multiple MAC frames (see subclause B.8.2.5.5). The request ~~(including any~~from the CM MUST be large enough to accommodate the entire necessary physical layer overhead~~), subject to UCD~~ (see ~~NOTE~~Subclause ~~1~~B.6.2) ~~and administrative limits (see NOTE 2)~~for transmitting the MAC frame or fragment. The CM MUST NOT make a request ~~a number of mini-slots corresponding to one complete frame (see NOTE 3), except~~that would violate the limits on data grant sizes in the ~~case of fragmentation in Piggyback Mode (refer to subclause B.10.3.2.2).~~UCD message (see Subclause B.10.3.3) or any limits established by QOS parameters associated with the Service Flow.

~~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 subclause B.C.2.2.6.1).~~

~~NOTE 3 – A frame is a single MAC frame or a concatenated MAC frame.~~

B.9.3.1 Global Timing Reference
[edit 2nd paragraph]

The Transmission Convergence sublayer ~~MUST~~must operate closely with the MAC sublayer to provide an accurate timestamp for the SYNC message. As mentioned in the Ranging subclause below (subclause B.9.3.3), the model assumes that the timing delays through the remainder of the PHY layer MUST be relatively constant with the exception of the timing offsets specified in subclause 8.3.7 related to symbol rate changes to accommodate a legacy DOCSIS upstream receiver implementation. Any variation in the PHY delays MUST be accounted for in the guard time of the PHY overhead.

B.9.3.3 Ranging [edit 1st paragraph]

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 with the

exception of the timing offsets specified in subclause B.8.3.7 related to symbol rate changes to accommodate a legacy DOCSIS upstream receiver implementation. Any variation in the PHY delays MUST be accounted for in the guard time of the upstream PMD overhead.

B.10.1.1.2 Classifiers [paragraph following figure]

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~~that has at least one relevant parameter and all relevant parameters match the packet, the Classifier MUST forward the packet to the corresponding Service Flow (irrelevant parameters have no impact on packet classification decisions). If ~~no~~a Classifier ~~is found in which~~contains no relevant parameters for a given packet (i.e., all parameters ~~match the packet~~are irrelevant), then ~~the~~that packet ~~is~~cannot match the Classifier, and the Classifier MUST NOT forward the packet to the corresponding Service Flow. If a packet does not match any Classifier and as a result has not been classified to any other flow, then it MUST be classified to the Primary Service Flow.

B.10.1.2 Object Model [edit 5th paragraph as follows]

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~~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 subclause B.C.2.2.5.)

B.10.1.5.1 Provisioned Service Flows

[update 2 cross reference from [PKTCBL-MGCP] to [J.162]

B.10.3.1.1 Fragmentation Rules [edit item #3 as follows]

3) If the CM is fragmenting a frame, any piggyback request for the next fragment MUST be made in the BPI EHDR portion of the fragment header. Any piggyback request for a subsequent frame SHOULD be made in the BPI EHDR portion of the last fragment, but MAY be made in one of the extended headers inside the original frame. However, the same request MUST NOT be made in more than one place. Because the CMTS could ignore a request inside the original frame, making the request in the original frame may cause a loss of the request.

B.10.3.2.2 Piggyback Mode [edit 3rd paragraph]

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~~ and it has been determined that the ~~packet~~ HCS is correct~~, and~~ , the ~~packet is forwarded to~~CMTS processes the ~~appropriate destination~~frame as though it had been received unfragmented except that the CMTS MUST ignore the decryption related portion of any privacy EHDRs. However, the bandwidth requests in privacy EHDRs and request EHDRs of such frame SHOULD be processed, but they MAY be ignored also.

B.10.4.3 Operation [edit 2nd paragraph]

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 to zero, or is 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.

[delete Figure 10-13 in 10.4.4, insert new figure in subclause B.10.4.5]

~~FIGURE 10-13~~

~~**Payload Header Suppression Signalling Example**~~

B.10.4.5 Payload Header Suppression Example

[Update figure as indicated]

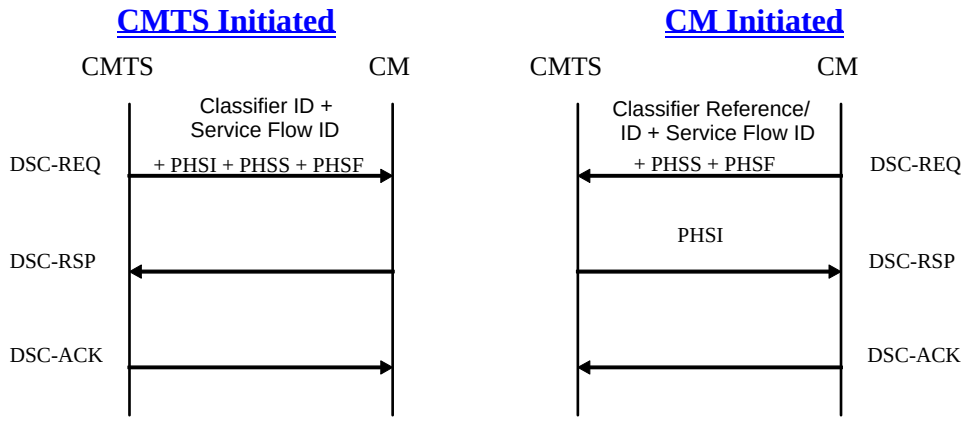


Figure 10-13. Payload Header Suppression Signaling Examples

B.11.2.1 Scanning and Synchronization to Downstream
[edit first paragraph, add new paragraph at the end of the subclause]

On initialization or ~~after signal loss~~a "Reinitialize MAC" operation, 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.

While scanning, it is desirable to give an indication to the user that the CM is doing so.

In order to support redundant CMTS architectures, when a CM in the Operational state detects that the downstream signal is invalid (*i.e.*, does not meet the four criteria above), the CM MUST NOT immediately perform a Reinitialize MAC operation. It must instead attempt to re-establish synchronization on the current downstream channel (see subclause B.11.5). Such re-establishment attempts MUST continue until the operation of Periodic Ranging as specified in Figure 11-17 of subclause 11.3.1 calls for a "Re-initialize MAC" operation after the expiration of Timeout T4 or 16

expirations of Timeout T3. Figure 11-17 shows the procedure that MUST be followed by a cable modem during standard operation.

B.11.2.4 Ranging and Automatic Adjustments

[Replace Figure 11-8 with the following]

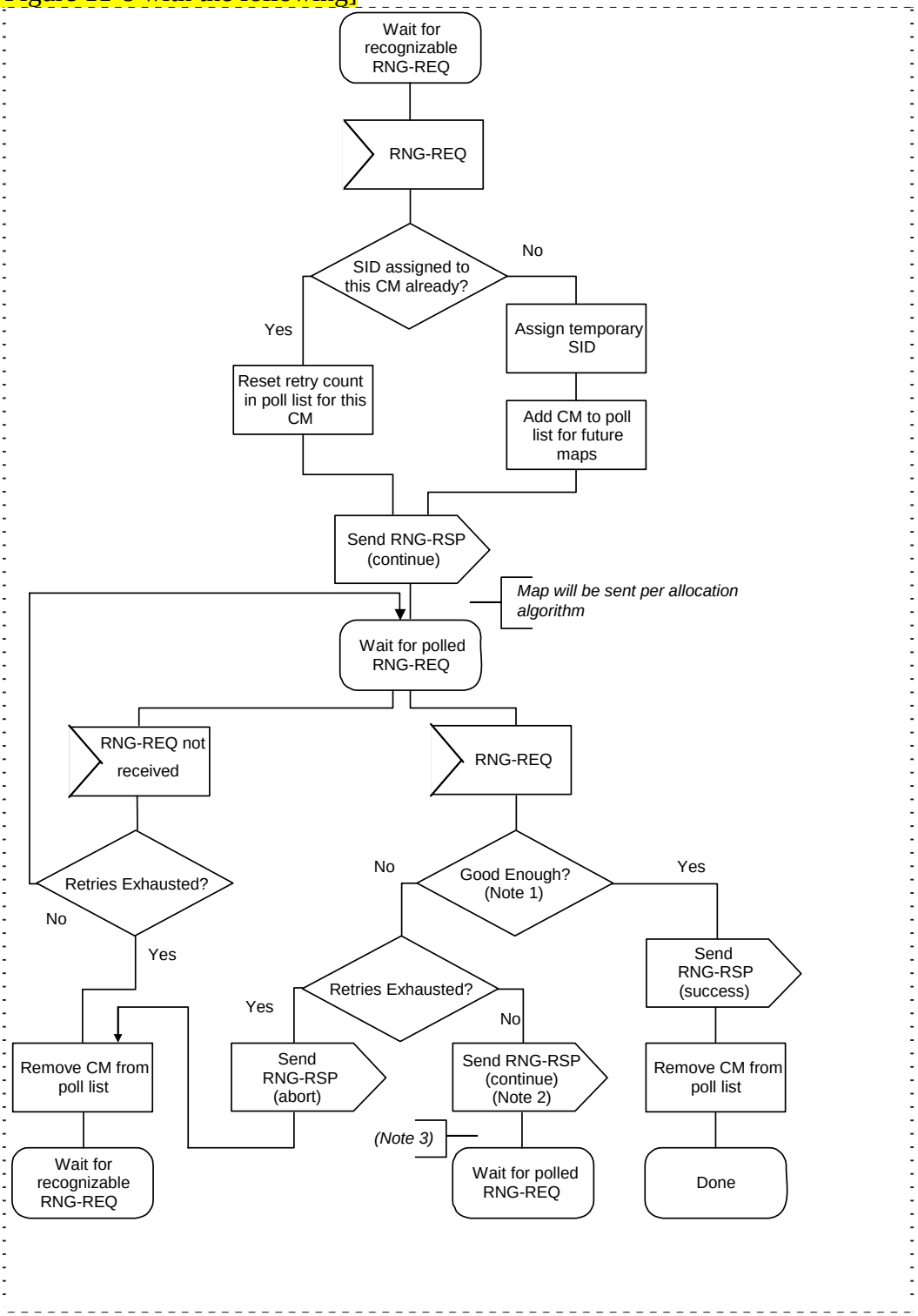


Figure 11-8. Initial Ranging - CMTS

NOTE 1. Means pending-till-complete was zero and ranging is within the tolerable limits of the CMTS.

NOTE 2. If pending-till-complete is nonzero, the CMTS MUST NOT send new Pre-Equalization Coefficients in the corresponding RNG-RSP. However, the CMTS MAY adjust other ranging parameters in the RNG-RSP message.

NOTE 3. If the RNG-REQ pending-till-complete was nonzero, the CMTS MAY schedule additional station maintenance opportunities during the pending-till-complete period in order to adjust ranging parameters other than the equalizer.

B.11.2.5 Device Class Identification

[update internal cross-reference]

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 subclause B.~~11.2.~~ 11.2.8 for details.

B.11.2.8 Transfer Operational Parameters

[edits to 3rd paragraph]

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 subclause B.8.3.6.3. The modem MAY reject the configuration file in the case of size limit errors (refer to Subclause B.D.2.1).

B.11.2.9 Registration

[edits as shown below]

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 subclause B.8.3.7) to the CMTS as part of a Registration Request. The CM MUST perform the following operations before registration (refer to Figure 11-12~~ shows the procedure that MUST be followed by the CM.~~):

- Check the mandatory items in the configuration file (refer to Subclause D.2.2). The CM MUST reject the configuration file if it lacks any mandatory items.
- Calculate a MIC per Subclause B.D.2.3.1 and compare it to the CM MIC included in the configuration file. If the MIC is invalid, the CM MUST reject the configuration file.
- If the configuration file contains TLV-11 encoding, the CM MUST follow the configuration process defined in [DOCS5] Subclause B.3.4. The CM MUST reject the configuration file in the case of TLV-11 processing failure.

The configuration parameters downloaded to the CM MUST include a network access control object (see subclause B.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.~~

[modify only 1st and 10th bullets which follow the text]

The CMTS MUST perform the following operations to confirm the CM authorization (refer to Figure 11-14):

- Calculate a MIC per Subclause B.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~~Authentication Failure.
- If the Registration Request contains Service Flow encodings, and the REG-RSP was sent with a confirmation code of ok (0), the CMTS MUST wait for a Registration Acknowledgment as shown in Figure 11-~~15.~~14. If the

Registration Request contains DOCSIS 1.0 Class of Service encodings, the CMTS MUST NOT wait for a Registration Acknowledgment.

B.11.2.10 Baseline Privacy Initialization

[modify paragraph as follows]

Following registration, if the CM is provisioned to run Baseline Privacy, the CM MUST initialize Baseline Privacy operations, as described in ~~[DOCSIS8]~~ Annex B.O. A CM is provisioned to run Baseline Privacy if ~~its~~the Privacy Enable TLV (Subclause B.C.1.1.16) in the DOCSIS 1.1-style configuration file ~~includes a~~is explicitly/implicitly set to enable or the Baseline Privacy Configuration Setting (subclause B.C.3.2) is contained in the DOCSIS 1.0-style configuration file as specified in subclauses B.O.A.1.1 and ~~if the Privacy Enable parameter (subclause C.1.1.16)~~B.O.II.2. Note that the Secure Software Download is ~~set~~required regardless of whether the CM is provisioned to ~~enable~~run Baseline Privacy or not as specified in Annex B.O..

B.11.3.1 Periodic Signal Level Adjustment

[replace figure 11-16 and notes with the following]

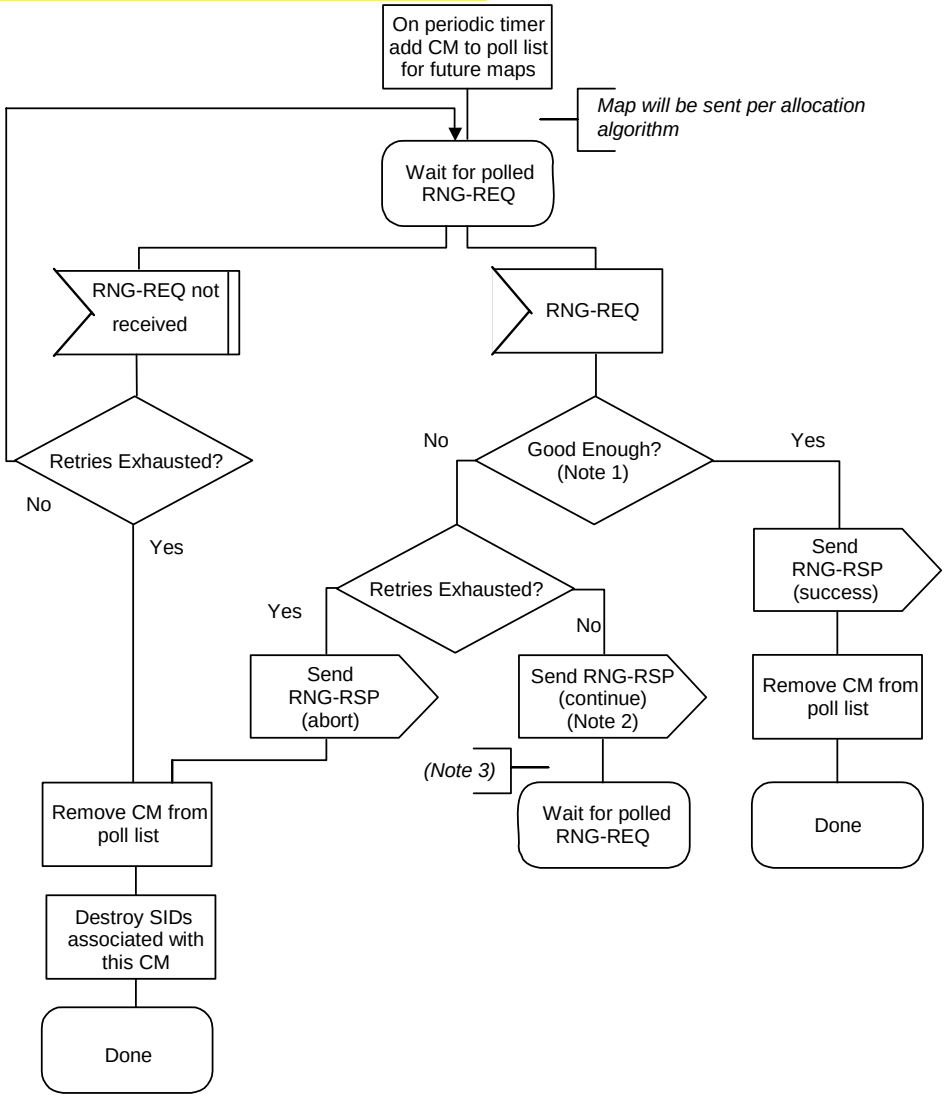


FIGURE 11-16
Periodic Ranging - CMTS

Notes to Figure 11-16:

1. Means pending-till-complete was zero and ranging is within the tolerable limits of the CMTS.
2. If pending-till-complete is nonzero, the CMTS MUST NOT send new Pre-Equalization Coefficients in the corresponding RNG-RSP. However, the CMTS MAY adjust other ranging parameters in the RNG-RSP message.
3. If the RNG-REQ pending-till-complete was nonzero, the CMTS MAY schedule additional station maintenance opportunities during the pending-till-complete period in order to adjust ranging parameters other than the equalizer.

[edit paragraph immediately following Figure 11-19 as follows:]

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 subclause 8.3.10.1.1.)~~

B.11.4 Dynamic Service

[Edit text as indicated]

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~~a single existing Upstream and/or a single existing Downstream Service Flow. This is illustrated in Figure 11-20.

B.11.4.1 Dynamic Service Flow State Transitions

[add new paragraph after 1st, edit bullet list]

If a single Dynamic Service message affects a pair of service flows, a single transaction is initiated which communicates with both parent Dynamic Service Flow State Transition Diagrams. In this case, both service flows MUST remain locked in the same state until they receive the DSx Succeeded or DSx Failed input from the DSx Transaction State Transition Diagram. During that "lock interval", if a message is received which refers to only one of the two service flows, it MUST be treated as if it refers to both service flows, so that both service flows stay in the same state. If a DSD-REQ message is received during the lock interval which refers to only one of the two service flows, the device MUST handle the event normally, by sending the SF Delete-Remote to the ongoing DSx Transaction and by initiating a DSD-Remote transaction, and in addition, it MUST initiate a DSD-Local transaction to delete the second service flow of the locked pair.

B.11.4.3 Dynamic Service Change

[edits begin in second paragraph following the bullet list as shown]

To prevent packet loss, any required bandwidth change ~~is~~must be sequenced between the application generating the data and the bandwidth parameters of the Service Flow carrying the data. Because MAC messages can be lost, the timing of Service Flow parameter changes can vary, and it occurs at different times in the CM and CMTS. Applications should reduce their transmitted data bandwidth before initiating a DSC to reduce the Service Flow bandwidth, and should not increase their transmitted data bandwidth until after the completion of a DSC increasing the Service Flow bandwidth.

The CMTS controls both upstream and downstream scheduling. Scheduling is based on data transmission requests and is subject to the limits contained in the current Service Flow parameters at the CMTS. The timing of Service Flow parameter changes, and any consequent scheduling changes, is independent of both direction ~~AND~~and whether ~~it~~there is an increase or decrease in bandwidth. The CMTS always changes ~~scheduling~~Service Flow parameters on receipt of a DSC-REQ (CM -initiated transaction) or DSC-RSP (CMTS -initiated transaction).

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

The CM controls the upstream transmit ~~behaviour~~requests, subject to limits contained in the current Service Flow parameters at the CM. The timing of Service Flow parameter changes in the CM, and any consequent CM transmit ~~behaviour~~request behavior changes, is a function of which device initiated the transaction~~ AND whether the change is an "increase" or "decrease" in bandwidth~~. For a CM-initiated DSC-REQ, the Service Flow parameters are changed on receipt of the DSC-RSP from the CMTS. For a CMTS-initiated DSC-REQ, the Service Flow parameters are changed on receipt of the DSC-REQ from the CMTS.

~~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 should posinstall or remove Classifiers upon receiving the DSC-Request or whether it should postpone this installation until receiving the DSC-Ack (refer to subclause C.2.1.8).~~

B.11.4.3.1 CM-Initiated Dynamic Service Change

[delete rows in Figure as shown]

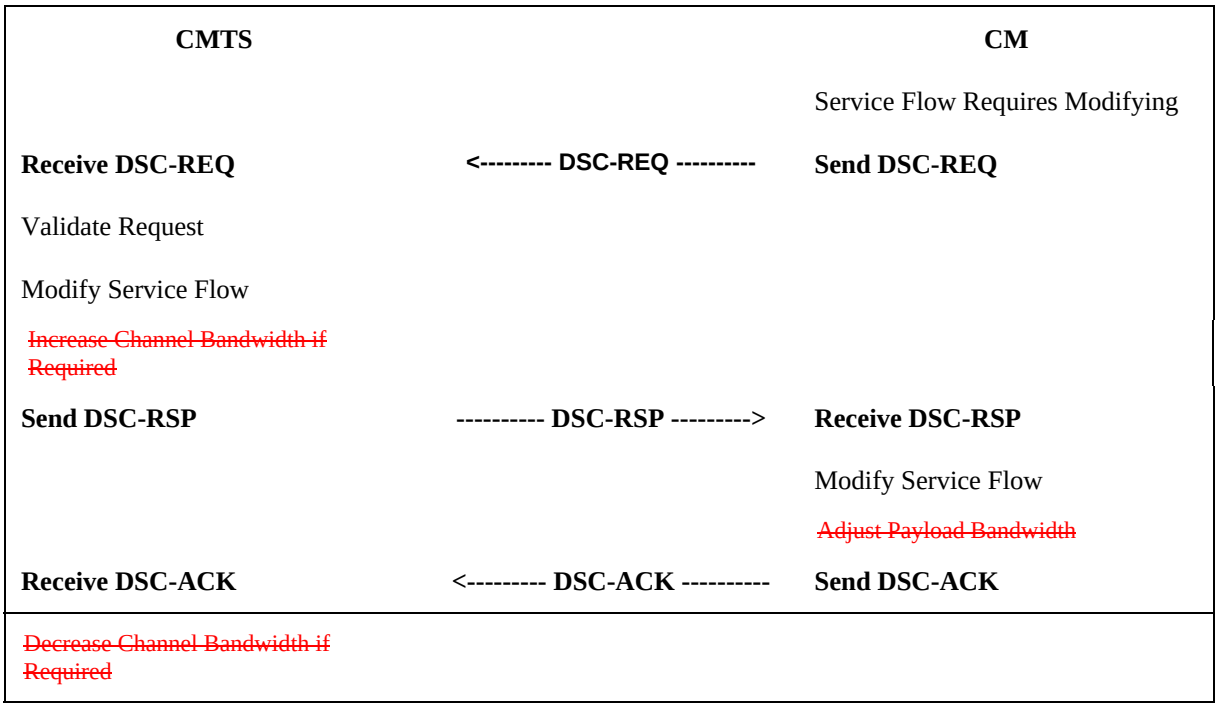


FIGURE 11-39. CM-Initiated DSC

B.11.4.3.2 CMTS-Initiated Dynamic Service Change

[delete rows in Figure as shown]

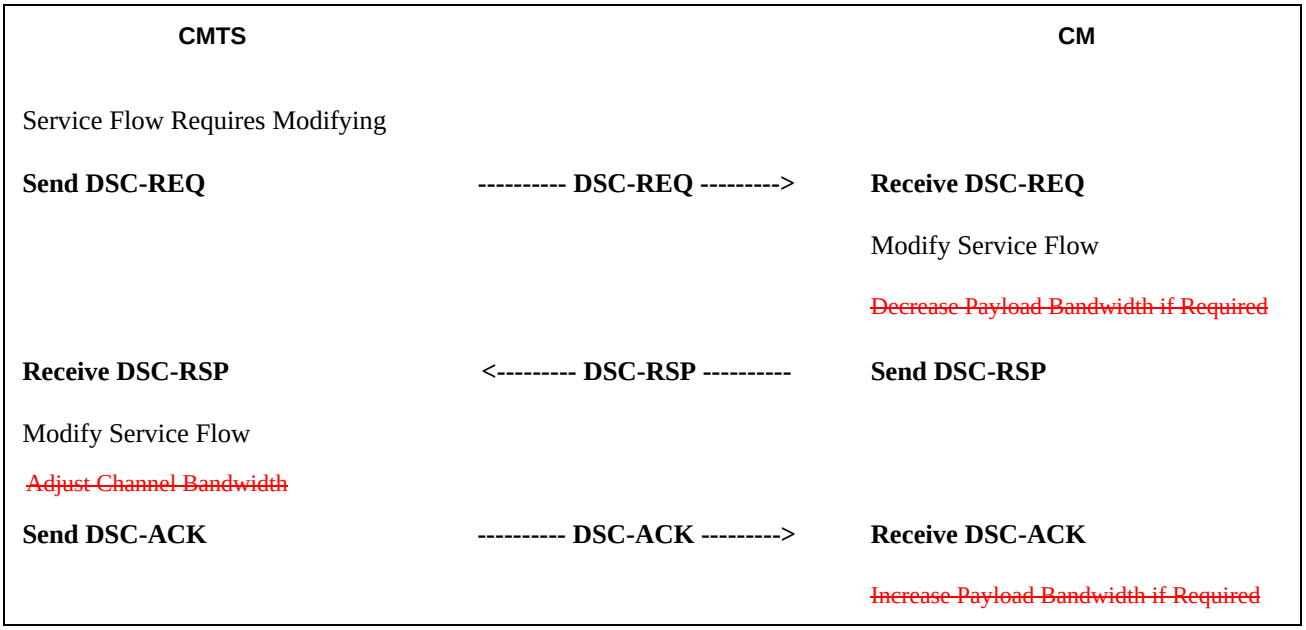


FIGURE 11-40–CMTS-Initiated DSC

B.11.4.4 Dynamic Service Deletion

[delete note at end of subclause]

~~NOTE—Unlike DSA and DSC messages, DSD messages are limited to only a single Service Flow.~~

B.11.4.4.1 CM Initiated Dynamic Service Deletion

A CM wishing to delete ~~a~~an upstream and/or a downstream Service Flow generates a delete request to the CMTS using a Dynamic Service Deletion-Request message (DSD-REQ). The CMTS removes the Service Flow(s) and generates a response using a Dynamic Service Deletion-Response message (DSD-RSP). Only one upstream and/or one downstream Service Flow can be deleted per DSD-Request.

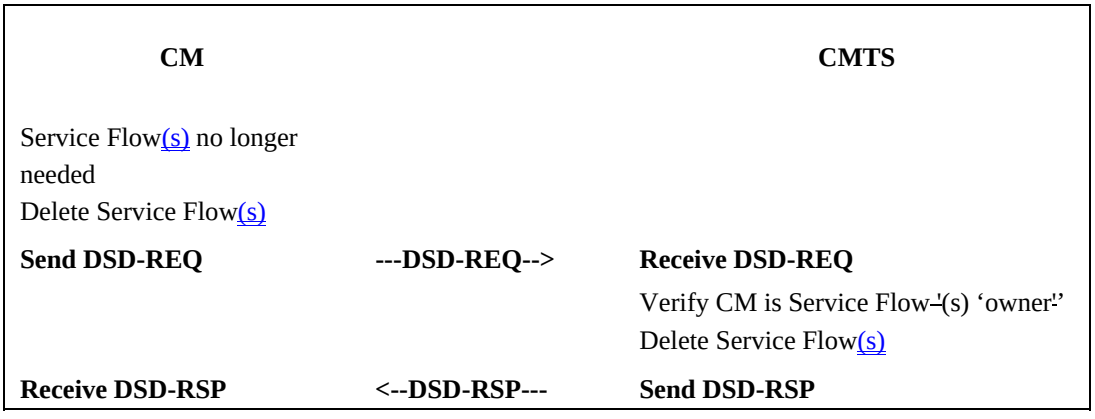


FIGURE 11–50 Dynamic Service Deletion Initiated from CM

B.11.4.4.2 CMTS Initiated Dynamic Service Deletion

[modify paragraph and Fig 11-51]

A CMTS wishing to delete ~~a~~an upstream and/or a downstream 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(s) and generates a response using a Dynamic Service Deletion-Response message (DSD-RSP). Only one upstream and/or one downstream Service Flow can be deleted per DSD-Request.

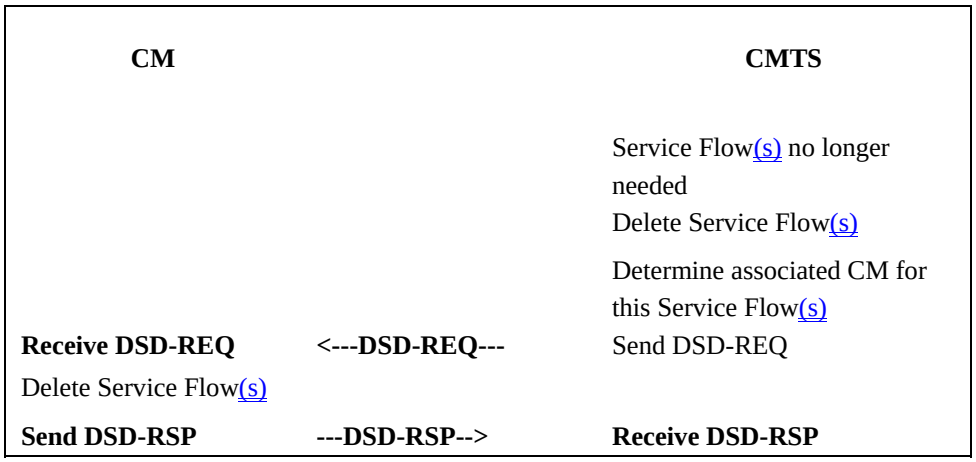


FIGURE 11-51 Dynamic Service Deletion initiated from CMTS

B.11.4.5.1 DCC General Operation

[edits to 1st, 3rd, 9th paragraph, insert new text after 9th paragraph and before last one in subclause]

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 specification. Figure 11-58 ~~shows~~and Figure 11-59 show the procedure that MUST be followed by the CMTS. Figure 11-~~60~~62 shows the corresponding procedure that MUST be followed by a ~~DCC-capable~~ CM.

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.

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 arriving at the new channel, less any commanded re-initialization,~~ before the expiry of T13. The CM MAY continue to use QoS resources on the ~~current~~old channel after responding with DCC-RSP and before the expiry of T13.

If the CM is commanded to perform initial or station maintenance or to use the channel directly, the destination CMTS MUST hold the QoS resources on the new channel until a time of T15 has passed after the last DCC-REQ was sent if the CM has not yet been detected on the new channel. If the CM is commanded to re-initialize the MAC, then QoS resources are not reserved on the destination CMTS, and T15 does not apply.

The T15 timer represents the maximum time period for the CM to complete the move to the destination CMTS, and is based on the TLV encodings (i.e., initialization technique TLV, UCD substitution TLV, and SYNC substitution TLV) included in the DCC-REQ message and the local configuration of the destination CMTS (UCD transmit interval, SYNC

interval, etc.).

The destination CMTS SHOULD calculate and limit T15 based on internal policy according to the guidelines in Subclause 11.4.5.1.1.

If initialization technique of initial ranging is utilized and if the CM arrives after T15 has passed, attempting to use resources on the new channel that have been removed (ranging or requesting bandwidth on a SID that has been deleted), the CMTS MUST send a Ranging Abort to the CM in order to cause the DCC transaction to fail.

When a CM is moved between DS channels on different IP subnets using initialization techniques other than re-initialize the MAC, a network connectivity issue may occur because no DHCP process is indicated as part of the DCC operation. The CM MAY implement a vendor-specific feature to deal with this situation. The CMTS SHOULD take this issue into account when sending a DCC-REQ and SHOULD direct the CM to use the appropriate initialization technique TLV to ensure no IP connectivity loss as a result of DCC.

B.11.4.5.1.1 Derivation of T15 Timer

The maximum value noted for the T15 timer denotes the maximum amount of time that the CMTS should reserve resources on the new channel. This value is not to be used to represent acceptable performance.

The equation below describes the method for calculating the value of T15.

T15 = CmJumpTime + CmRxTargetUcd + CmRxDsSync + CmtsRxRngReq

Each of the variables in the equation calculating the T15 timer is explained in the table below.

Variable	Explanation and Value
CmJumpTime	This is the CM's indication to the CMTS of when it intends to start the jump and how long it will take to jump. For a downstream change, it includes the time for the CM to synchronize to the downstream parameters on the destination channel, such as QAM symbol timing, FEC framing, and MPEG framing. It incorporates CM housecleaning on the old channel. It also incorporates one T11 period for the CM to process and receive the DCC-REQ message. This optional value is computed by CM and returned in DCC-RSP (depart). If CM does not specify the Jump Time TLVs, then the destination CMTS assumes that the value is 1.3 seconds. This recognizes the fact that the CM may continue to use the old channel until the expiry of the T13 timer. If CM specifies the Jump Time TLVs, then the destination CMTS uses the specified value.
CmRxTargetUcd	This variable represents the time for the CM to acquire UCD parameters for the target upstream channel. The value of this variable is two CMTS UCD timer periods.
CmRxDsSync	This variable represents the time for the CM to acquire a downstream SYNC message. The value of this variable is two CMTS SYNC timer periods.
CmtsRxRngReq	This variable represents the time for the CM to receive and use a ranging opportunity, and for the CMTS to receive and process the RNG-REQ. For the initialization technique of use directly, this value is two times the CMTS time period between unicast ranging opportunities plus 20 - 40 milliseconds for MAP and RNG-REQ transmission time and CMTS RNG-REQ processing time. For the initialization technique of station maintenance, this value is two times the CMTS time period between unicast ranging opportunities plus 20 - 40 milliseconds for MAP and RNG-REQ transmission time and CMTS RNG-REQ processing time. For the initialization technique of initial maintenance, this value is 30 seconds. Because the variables involved in initial maintenance are not strictly under the control of the CMTS, the computation of this factor is uncertain.

The maximum value assigned to the T15 timer denotes the maximum amount of time that the CMTS should reserve resources on the new channel. The minimum value of the T15 timer is two seconds; this was derived by doubling the value of the T13 timer. The maximum value of the T15 timer is 35 seconds.

B.11.4.5.2 DCC Exception Conditions

[edit 2nd-to-last paragraph in subclause]

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~~RSP Retries" (Annex B).

B.11.4.5.3 DCC Performance

[add new section; renumber subsequent subclauses]

The purpose of a DCC is to move the CM to a new upstream and/or downstream channel with little interruption of service. There are many factors that affect the performance of a DCC transaction including CM housecleaning, initialization technique, and the number of TLV hints given by the current CMTS in the DCC-REQ message. Each of these factors is individually discussed in the table below.

The DCC transaction is defined from the perspective of both the CM and the CMTS for the discussion on performance in the following table. From the perspective of the CM, the DCC transaction begins when the CM receives the DCC-REQ message from the CMTS and completes when the CM receives the DCC-ACK message from the CMTS. From the perspective of the CMTS, the DCC transaction begins when the CMTS sends the DCC-REQ message to the CM and completes when the CMTS receives the DCC-RSP (arrive) message from the CM.

TLV Type	Value	Explanation
Initialization Technique	Absent or 0 Reinitialize MAC	There are no performance requirements in this case. The CM will arrive on the destination CMTS after initialization occurs.
	1 Initial Maintenance	There are low performance expectations in this case because many factors affect the performance, such as collisions and ranging backoff. The CM should arrive on the destination CMTS as quickly as possible.
	2 Station Maintenance	The DCC transaction SHOULD complete within 1.5 seconds after the start of jump if the UCD substitution TLV and the downstream parameter TLVs are supplied. The DCC transaction SHOULD complete within the sum of CM jump time, two UCD intervals, and two ranging intervals if the current CMTS supplies no TLV hints in the DCC-REQ message.
	3 Initial or Station Maintenance	The CMTS does not know which ranging technique the CM will utilize. The CM should arrive on the destination CMTS as quickly as possible.
	4 Use Channel Directly	The DCC transaction SHOULD complete within one second after the start of jump if the UCD substitution TLV and the downstream parameter TLVs are supplied. The DCC transaction SHOULD occur within the sum of CM jump time and two UCD intervals if the current CMTS supplies no TLV hints in the DCC-REQ message.
DS Parameter		The CMTS SHOULD include the downstream parameter TLVs for station maintenance and use directly initialization techniques that are expected to occur quickly.
UCD Substitution		The CMTS SHOULD include the UCD substitution TLV for station maintenance and use directly initialization techniques that are expected to occur quickly.

SYNC Substitution		The CMTS SHOULD include the SYNC substitution TLV for station maintenance and use directly initialization techniques that are expected to occur quickly.
CM Jump Time		The length of jump TLV SHOULD be less than one second for downstream channel changes that include the downstream parameter TLVs or for upstream only channel changes.

When the DCC-REQ does not contain UCD Substitution TLVs and/or specifies an Initialization Technique of Initial Maintenance, Station Maintenance, or use directly, the destination CMTS SHOULD increase the probability that the CM will arrive quickly by using the CM Jump Time TLVs specified in the DCC-RSP (depart) to adjust the transmission of UCDs and ranging opportunities such that they coincide with the time when CM has estimated that it will arrive, and SHOULD increase the frequency of UCDs and/or ranging opportunities during this period.

B.11.4.5.4 Near-Seamless Channel Change
[renumber subclause, modify last bullet as shown]

- 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).

B.~~11.4.5.4~~11.4.5.5 Example Operation
[renumber subclause]

***B.11.4.5.5.1* Example Signaling**
[update cross reference in 1st paragraph]

Figure 11-~~18~~57 shows an example of the use of DCC and its relation to the other DOCSIS 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 re-requests the resources. This example (not including all exception conditions) is described below. Refer to subclause 11.2 for more detail.

[add new text, new subclauses, and graphics immediately following Figure 11-57 as follows]

Figure 11-57. DCC Example Operational Flow

The states for the old and new CMTSes are shown as separate flow diagrams, since the old and new CMTS may be different. If the CMTSes are the same (e.g., the same MAC domain), then the CMTS will need to run both sets of state machines concurrently.

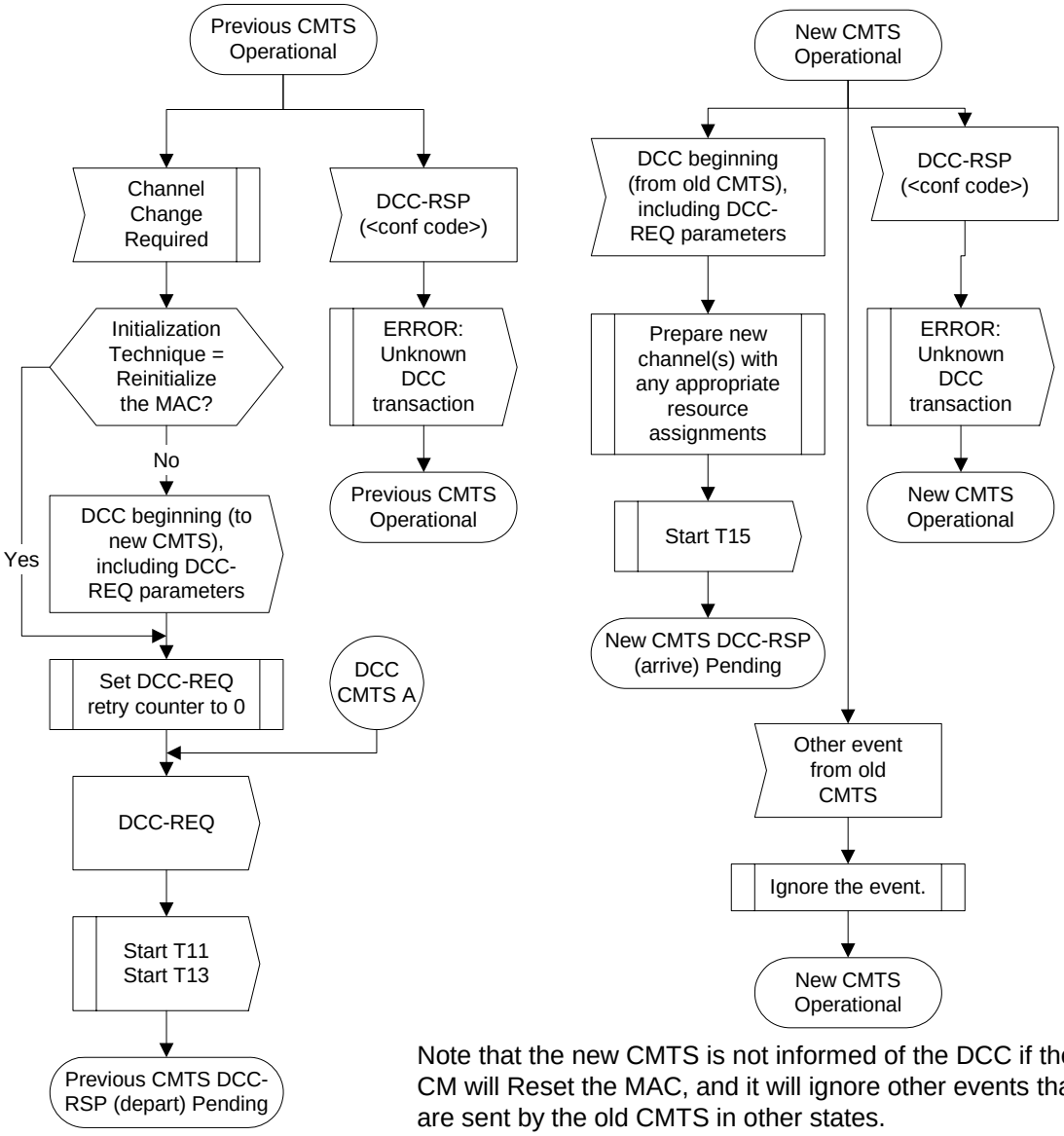
The flow diagrams show points where explicit signaling between the old and new CMTS is desirable, especially for near-seamless operation. The mechanism for this signaling is beyond the scope of this specification.

Note that the flow diagrams for both old and new CMTSs have been carefully crafted to handle many error conditions, such as:

- If the CM does not respond to the DCC-REQ (or responds with a reject conf code) and does not move, then it will be allowed to remain on the old channel. Resources on the new channel will be released (old CMTS signals DCC aborted to the new CMTS).
- If the CM DCC-RSP (depart) is lost, but the CM moves and arrives on the new CMTS, the new CMTS will signal that the CM has arrived to the old CMTS, allowing it to remove resources.

- If the CM DCC-RSP (depart) is received and the CM DCC-RSP (arrive) is lost, but the new CMTS otherwise detects the presence of the CM, the DCC transaction is considered successful, and the CM is allowed to remain on the new channel.
- If the CM DCC-RSP (depart) and (arrive) are lost, but the new CMTS otherwise detects the presence of the CM, the new CMTS will signal that the CM has arrived to the old CMTS, allowing it to remove resources, and the CM is allowed to remain on the new channel.
- If the CM DCC-RSP (depart) is received, but the CM never arrives, the new CMTS will detect this and remove resources after T15 expires.
- If the CM DCC-RSP (depart) is lost and the CM never arrives, the old CMTS will signal DCC aborted to the new CMTS, allowing it to remove resources. The old CMTS will use a different mechanism outside the scope of the DCC flow diagrams (such as ranging timeout) to remove resources on the old channels.
- If the CMTS DCC-ACK is lost and the DCC-RSP retry counter is expired, the CM will log an error and continue to the operational state.

There is a race condition that is not addressed in the flow diagrams; if the CM DCC-RSP (depart) is lost, the old CMTS will signal DCC aborted to the new CMTS. If the CM is in the process of moving, but has not yet arrived, the new CMTS will remove resources. This will prevent the CM from arriving successfully, unless it is able to complete the jump and arrive in approximately 1.2 seconds (3 retries of the DCC-REQ).



Note that the new CMTS is not informed of the DCC if the CM will Reset the MAC, and it will ignore other events that are sent by the old CMTS in other states.

Figure 11-58. Dynamically Changing Channels: CMTS View Part 1

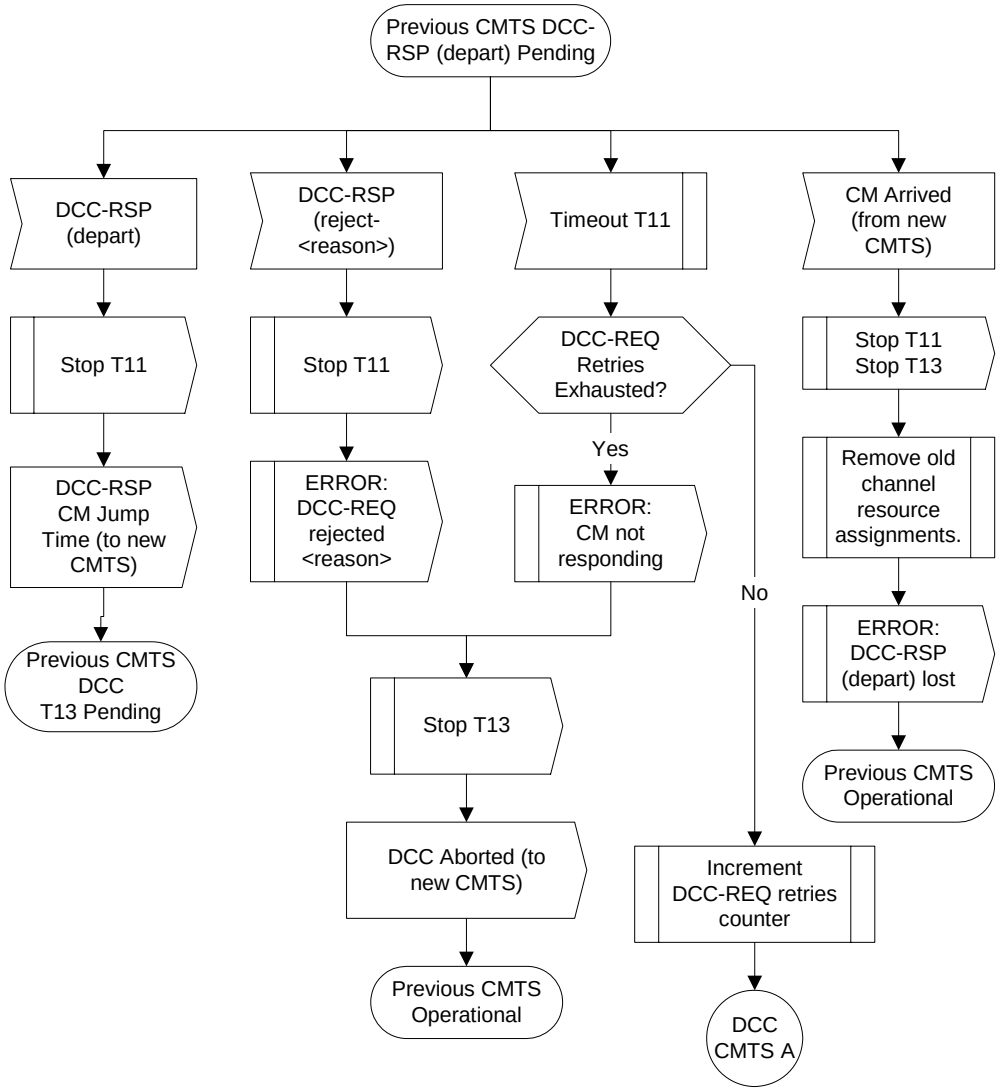


Figure 11-59. Dynamically Changing Channels: CMTS View Part 2

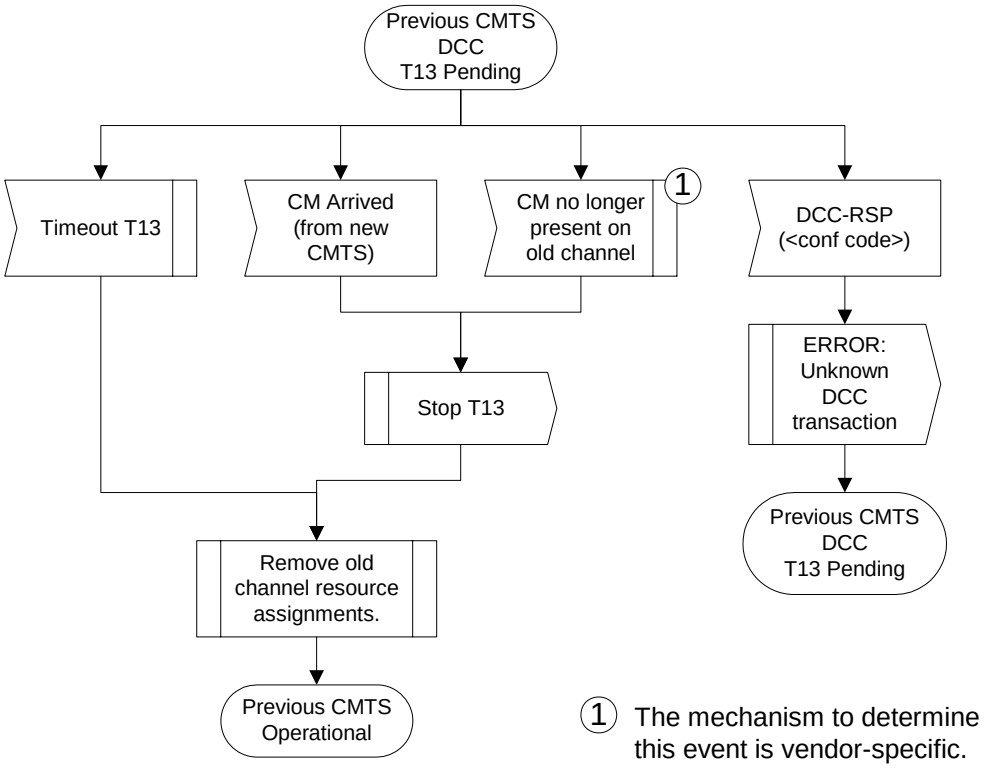


Figure 11-60. Dynamically Changing Channels: CMTS View Part 3

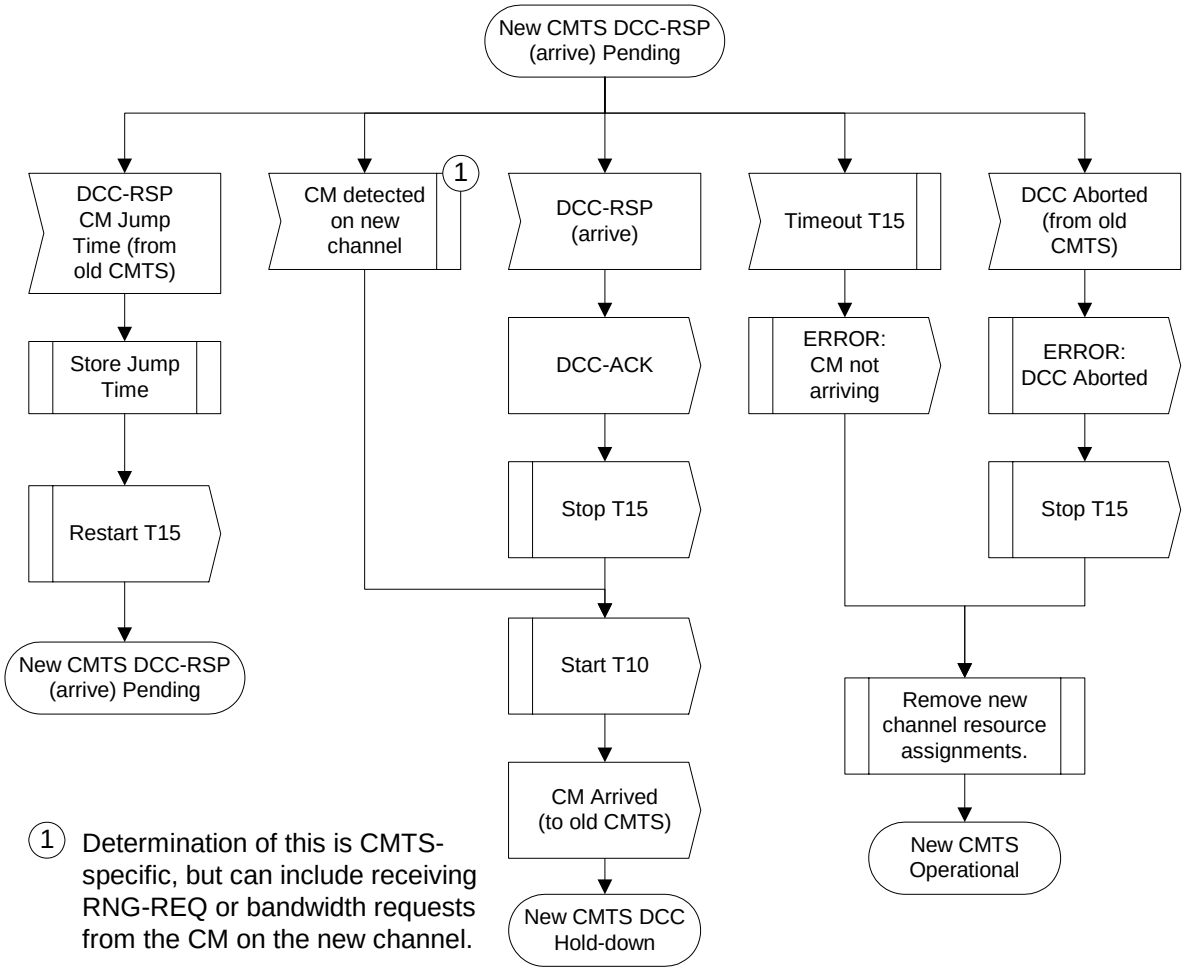


Figure 11-61 Dynamically Changing Channels: CMTS View Part 4

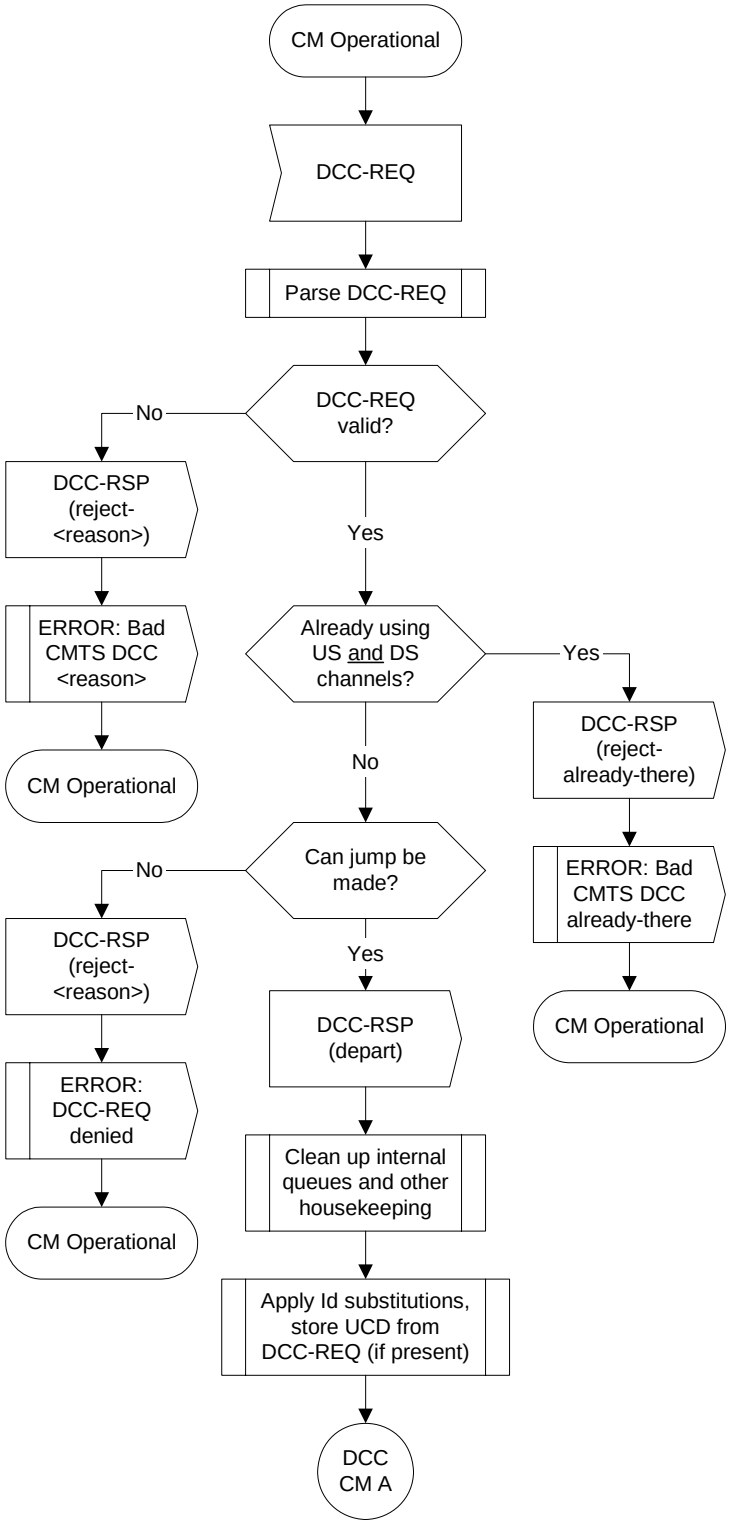


Figure 11-62. Dynamically Changing Channels: CM View Part 1[1]

[1]The state "Obtain Upstream Parameters" links to the state machine in Figure 11-1.

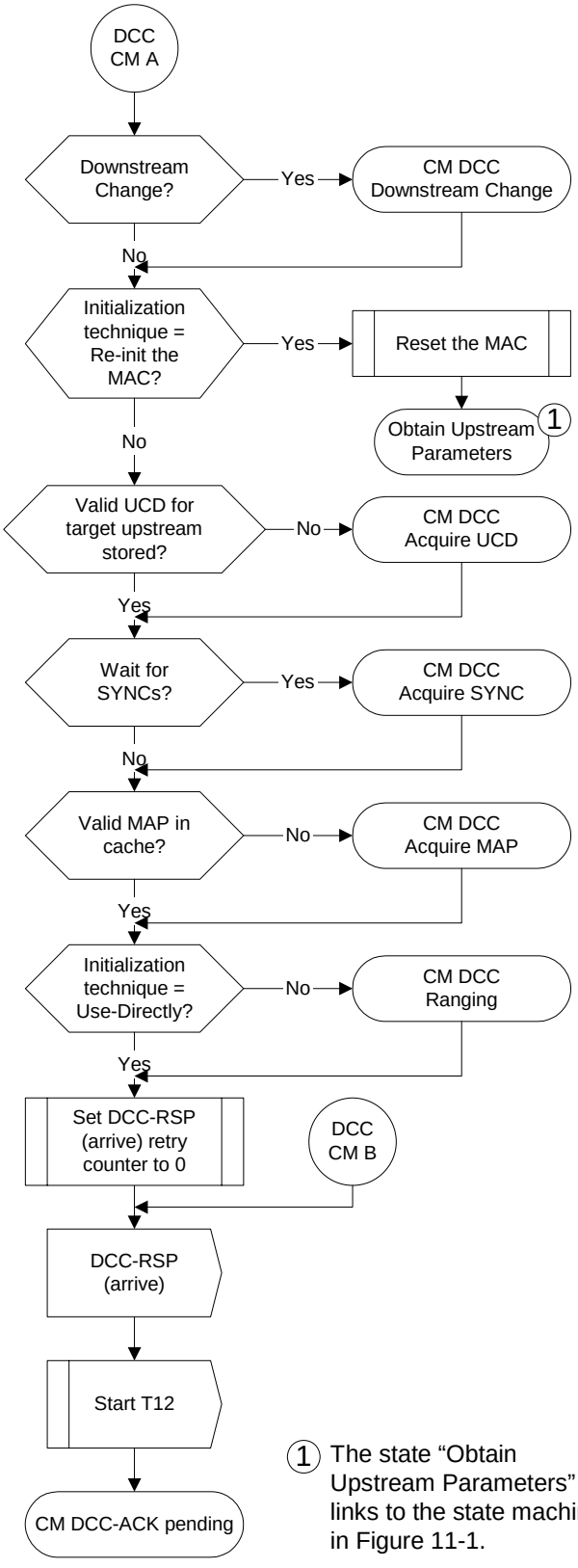


Figure 11-63. Dynamically Changing Channels: CM View Part 2

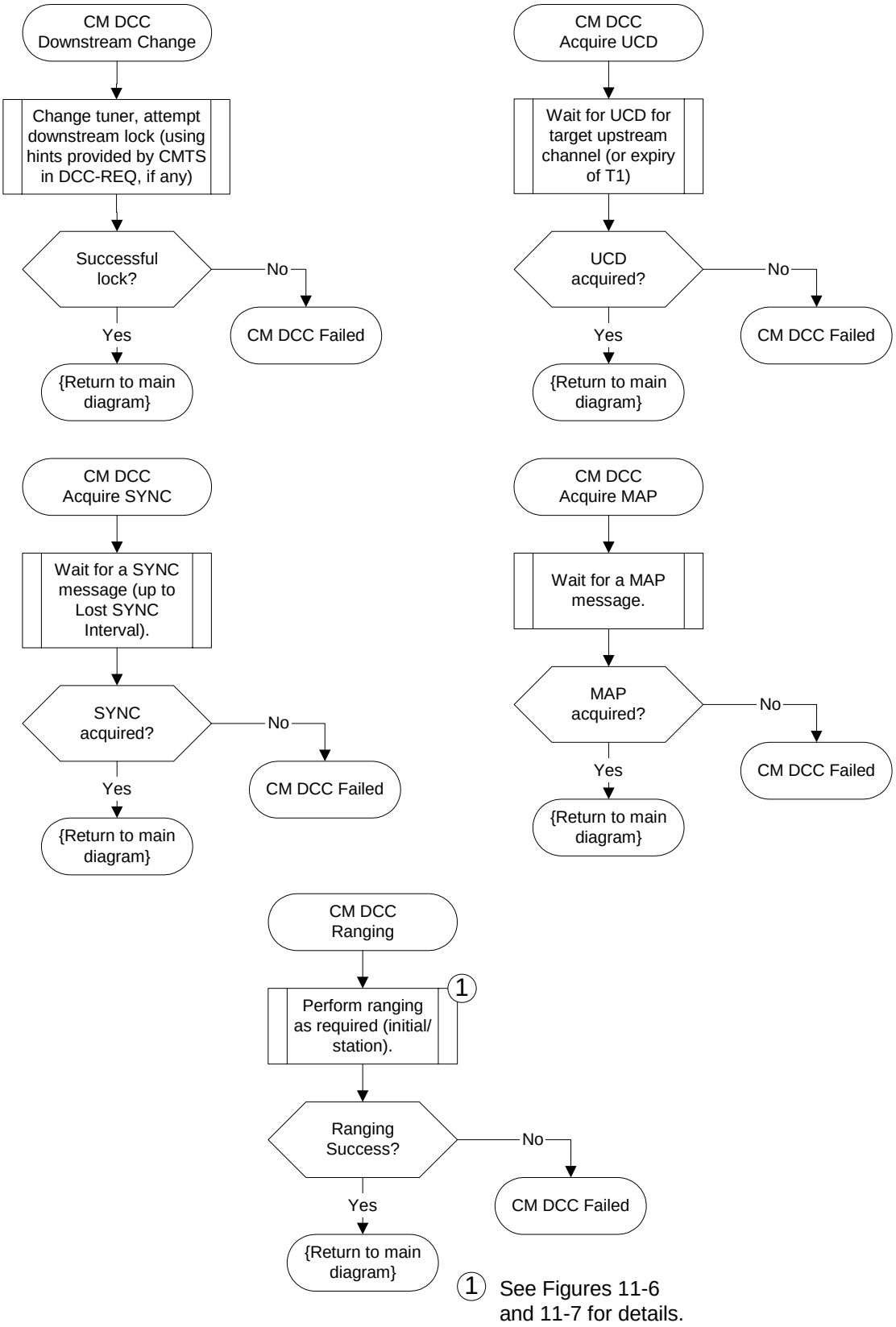


Figure 11-64. Dynamically Changing Channels: CM View Part 3

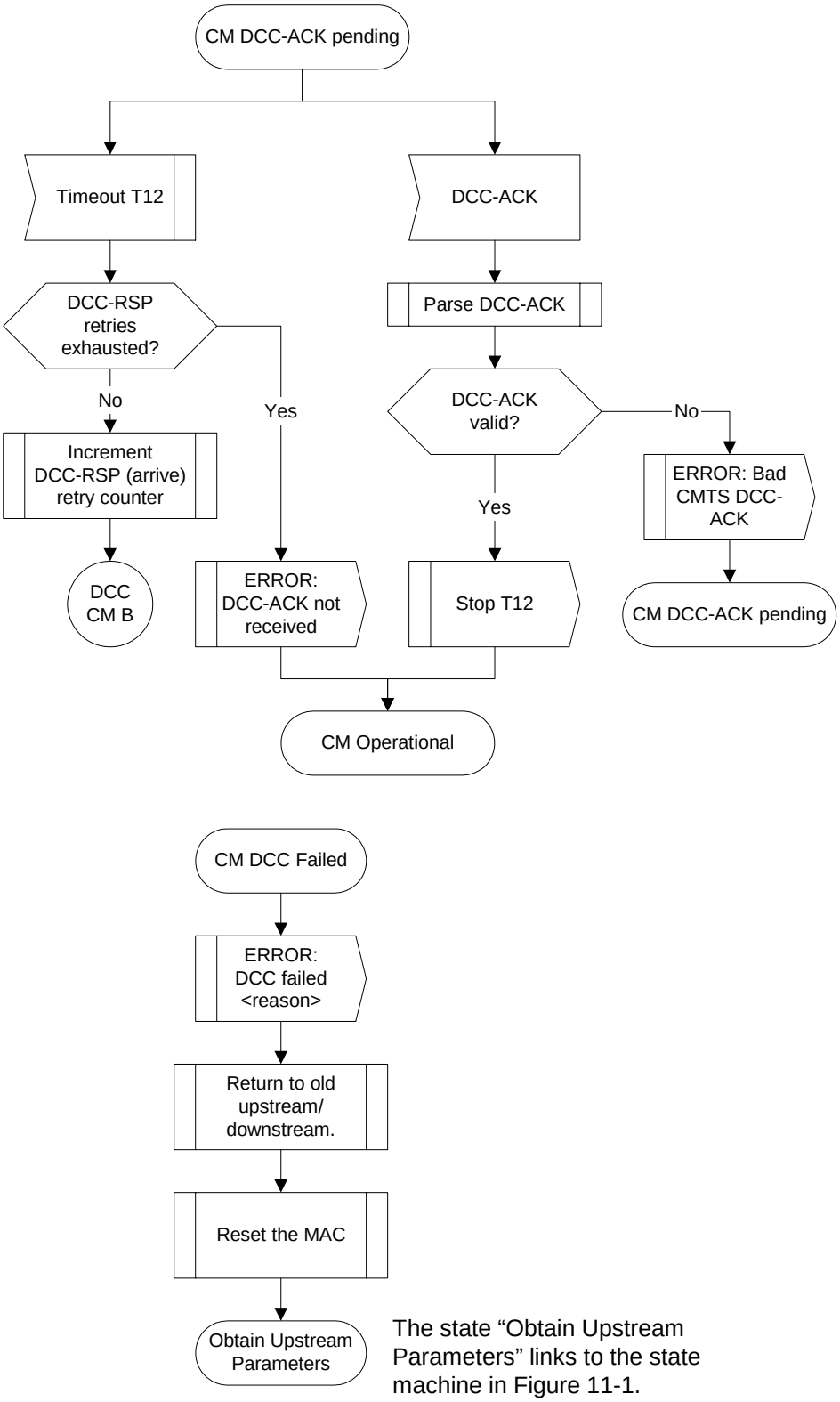


Figure 11-65. Dynamically Changing Channels: CM View Part 4

B.11.4.5.5.2 Example Timing

B.11.4.5.5.2.1 Upstream and Downstream Change – Use Channel Directly: CMTS Supplies All TLV Hints

In this example, the current CMTS sends a DCC-REQ message requesting that the CM switch both upstream and downstream channels. The DCC-REQ message includes the UCD substitution TLV, the SYNC substitution TLV, the downstream parameter TLVs, and the initialization technique TLV of 4 (use channel directly). The CM does not include the CM jump time TLV in the DCC-RSP.

The destination CMTS has the following local parameters:

UCD interval – 1 sec.
SYNC interval – 10 msec.
Unicast ranging interval – 1 sec.

The destination CMTS calculates the T15 timer value. The definition of the formula used in determining T15 is shown below. The variables used in calculating T15 are explained in the table below.

T15 = CmJumpTime + CmRxTargetUcd + CmRxDsSync + CmtsRxRngReq
T15 = 1.3 sec. + 2 sec. + 20 msec. + (2.02 sec.) = 5.34 sec.

Variable	Value	Explanation
CmJumpTime	1.3 sec.	Since the CM did not include the optional jump time TLV, the CMTS will use the default value of 1.3 seconds.
CmRxTargetUcd	2 sec.	Although UCD substitution settings are specified in the DCC-REQ, the CMTS does not know that the CM implements this TLV.
CmRxDsSync	20 msec.	Although SYNC substitution settings are specified in the DCC-REQ, the CMTS does not know that the CM implements this TLV.
CmtsRxRngReq	2.02 sec = 2 * (1 sec.) + 20 msec.	Two times the CMTS time period between unicast ranging opportunities plus 20 - 40 milliseconds for MAP and RNG-REQ transmission time and CMTS RNG-REQ processing time.

The CM synchronizes to the downstream parameters on the new channel, applies the UCD supplied in the DCC-REQ, collects MAP messages on the new channel, and resumes normal data transmission on the destination channels. This occurs within the recommended performance of 1 second.

B.11.4.5.5.2.2 Upstream and Downstream Change - Station maintenance: CMTS Supplies No TLV Hints

In this example, the current CMTS sends a DCC-REQ message requesting that the CM switch both upstream and downstream channels. The DCC-REQ message includes the initialization technique TLV of 2 (perform station maintenance). The CM does not include the CM jump time TLV in the DCC-RSP.

The destination CMTS has the following local parameters:

UCD interval – 1 sec.
SYNC interval – 10 msec.
Unicast ranging interval – 1 sec.

The destination CMTS starts scheduling the CM immediately after it receives the DCC-RSP (depart). The destination

CMTS calculates the T15 timer value. The definition of the formula used in determining T15 is shown below. The variables used in calculating T15 are explained in the table below.

T15 = CmJumpTime + CmRxTargetUcd + CmRxDsSync + CmtsRxRngReq
T15 = 1.3 sec. + 2 sec. + 20 msec. + (2.02 sec.) = 5.34 sec.

Variable	Value	Explanation
CmJumpTime	1.3 sec.	Since the CM did not include the optional jump time TLV, the CMTS will use the default value of 1.3 seconds.
CmRxTargetUcd	2 sec.	Two CMTS UCD timer periods.
CmRxDsSync	20 msec.	Two CMTS SYNC timer periods.
CmtsRxRngReq	2.02 sec = 2 * (1 sec.) + 20 msec.	Two times the CMTS time period between unicast ranging opportunities plus 20 - 40 milliseconds for MAP and RNG-REQ transmission time and CMTS RNG-REQ processing time.

The CM should synchronize to the downstream parameters on the new channel, search for and apply a UCD message on the destination channel, wait for a downstream SYNC on the destination channel, collect MAP messages on the destination channel, perform station maintenance on the destination channel, and resume normal data transmission on the destination channels.

These events occur in less than two seconds; this is within the acceptable performance criteria. The DCC transaction occurred within the recommended four second sum of CM jump time, two UCD intervals, and two ranging intervals (0 + 2 sec. + 2 sec. = 4 sec.).

B.A.1 MAC Addresses

MAC addresses described here are defined using the Ethernet/ISO~~/IEC~~8802-3 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~~02 through 01-E0-2F-00-00-0F

B.A.2.1 All CMs and No CM Service IDs

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. This is also the "Initialization SID" used by the CM during initial ranging."

B.A.2.2 Well-Known "Multicast" Service IDs

[edit 4th Service ID, add ellipsis between 5th and 6th ID]

0x3FF3	Within the interval specified, a transmission ~~MAY~~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.

B.A.2.3 Priority Request Service IDs
[update cross-reference only]

These Service IDs (0x3Exx) are reserved for Request IEs (refer to subclause C.~~2.2.5.2~~2.2.5.1).

B.C.1.1.4.7 Class-of-Service Privacy Enable
[update cross-reference only]

This configuration setting enables/disables Baseline Privacy on a provisioned CoS. See ~~DOCSIS8~~SCTE2.

B.C.1.1.15 Maximum Number of Classifiers
[edits as shown below]

This is the maximum number of Classifiers associated with admitted or active upstream Service Flows that the CM is allowed to have ~~admitted~~. Both active and inactive Classifiers are included in the count.

This is ~~necessary~~useful when using deferred activation ~~since the~~of provisioned resources. 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~~. The CMTS can control the QoS resources committed to the CM by limiting the number of Service Flows that are admitted. However, it may still be desirable to limit the number of ~~simultaneously admitted~~ Classifiers ~~applied to this set~~associated with the committed QoS resources. This parameter provides ~~the ability to~~that limit ~~the size of that set.~~.

Type	Length	Value
28	2	Maximum number of ~~simultaneous admitted classifiers~~ active and inactive Classifiers associated with admitted or active upstream Service Flows

The default value MUST be 0 – no limit.

B.C.1.1.16 Privacy Enable
[edits as shown below]

This configuration setting enables/disables Baseline Privacy on the Primary Service Flow and all other Service Flows for this CM. If a DOCSIS 1.1 CM receives this setting in a configuration file, the CM is required to forward this setting as part of the registration request (REG-REQ) as specified in Subclause B.6.3.7 regardless of whether the configuration file is DOCSIS 1.1-style or not while this setting is usually contained only in a DOCSIS 1.1-style configuration file with DOCSIS 1.1 Service Flow TLVs.

[Add the following new subclauses]

B.C.1.2.11 SNMPv3 Notification Receiver

This TLV specifies a Network Management Station that will receive notifications from the modem when it is in Coexistence mode.

Type	Length	Value
38	n	Composite

B.C.1.2.11.1 SNMPv3 Notification Receiver IP Address

This sub-TLV specifies the IP address of the notification receiver.

Type	Length	Value
38.1	4	ip1, ip2, ip3, ip4

If TLV 38.1 is not present, the CM MUST consider this a configuration failure, and the CM MUST NOT proceed with CM registration.

B.C.1.2.11.2 SNMPv3 Notification Receiver UDP Port Number

This sub-TLV specifies the Port number on the notification receiver to receive the notifications.

Type	Length	Value
38.2	2	UDP port number

If not present, the default value 162 is used.

B.C.1.2.11.3 SNMPv3 Notification Receiver Trap Type

This sub-TLV specifies the type of trap to send.

Type	Length	Value
38.3	2	1 : SNMP v1 trap in an SNMP v1 packet
		2 : SNMP v2c trap in an SNMP v2c packet
		3 : SNMP inform in an SNMP v2c packet
		4 : SNMP v2c trap in an SNMP v3 packet
		5 : SNMP inform in an SNMP v3 packet

If TLV 38.3 is not present, the CM MUST consider this a configuration failure, and the CM MUST NOT proceed with CM registration.

B.C.1.2.11.4 SNMPv3 Notification Receiver Timeout

This sub-TLV specifies the round trip timeout used to wait before sending a retry of an inform notification if sender does not get an acknowledgement from the receiver.

Type	Length	Value
38.4	2	time in milliseconds

If not present, the default value of 15000 milliseconds is used. This corresponds to the default value of 1500 hundredths of a second defined for the snmpTargetAddrTimeout MIB object (see Annex P of [DOCSIS5] and [RFC-2573]).

B.C.1.2.11.5 SNMPv3 Notification Receiver Retries

Defines the number times to retry an Inform after the first Inform transmission.

Type	Length	Value
38.5	2	number of retries

If not present, the default value of 3 retries is used.

SNMPv3 Notification Receiver Retries must be in the range of 0 to 255.

B.C.1.2.11.6 Notification Receiver Filtering Parameters

This sub-TLV specifies the OID of the snmpTrapOID value that is the root of the MIB subtree that defines all of the notifications to be sent to the Notification Receiver.

Type	Length	Value
38.6	n	Object Identifier ASN.1

The encoding of this TLV value field starts with the ASN.1 Universal type 6 (Object Identifier) byte, then the ASN.1 length field, then the ASN.1 encoded object identifier components. If this Sub-TLV is not present, the notification receiver will receive all notifications generated by the SNMP agent.

B.C.1.2.11.7 Notification Receiver Security Name

This sub-TLV specifies v3 Security Name to use when sending a SNMP V3 Notification.

Type	Length	Value
38.7	2-16	UTF8 Encoded security name

When Trap of Type value field is set to 1, 2, or 3, this value field SHOULD not be interpreted (has no meaning) and Informs messages will be sent with community string “public”. In the case of Trap of Type 4 or 5, two situations happen:

- If this TLV is not supplied, the V3 Notification will be sent in the noAuthNoPriv security level using the security name “@config”.
- If TLV-38 is supplied in configuration file, the value field MUST be the Security Name specified in a TLV Type 34 as part of the DH Kickstart procedure. The notifications will be sent using the Authentication and Privacy Keys calculated by the modem during the DH Kickstart procedure.

For detailed implementation refer to subclause B.3.6, Config File Element - docsisV3NotificationReceiver, of

[DOCSIS5].

B.C.1.3 Registration-Request/Response-Specific Encodings
[edits as shown below]

These encodings are not found in the configuration file, but are included in the Registration Request and option 60 of the DHCP request. Some encodings are also used in the Registration Response.

The CM MUST include all Modem Capabilities Encodings that are subject to negotiation with the CMTS in its Registration Request. ~~If present~~Modem Capabilities Encodings that are not subject to negotiation with the CMTS are explicitly stated in the ~~corresponding Registration Request,~~description of the particular modem capability. The CMTS MUST include Modem Capabilities in the Registration Response.

B.C.1.3.1 Modem Capabilities Encoding
[edits as shown below]

The set of possible encapsulated fields is described below.

All these capabilities are to be included in both the registration request and option 60 of the DHCP request unless the description of the capability explicitly prohibits this.

B.C.1.3.1.1 Concatenation Support
[edits as shown below]

If the value field is a 1 the CM requests concatenation support from the CMTS.

Type	Length	~~Value~~ On / Off
5.1	1	1 or 0

B.C.1.3.1.5 IGMP Support
[add note as shown below]

Type	Length	Value
5.5	1	1 or 0

Note: This CM capability is not subject to negotiation with the CMTS. The CM MUST include this capability in the DHCP request, but MUST NOT include this capability in the registration request. If a CMTS does receive this capability with in a registration request it MUST return the capability with the same value in the registration response.

B.C.1.3.1.7 Downstream SAID Support
[edits as shown below]

~~The~~This field shows the number of Downstream SAIDs the modem can support.

B.C.1.3.1.8 Upstream SID Support
[edits as shown below]

~~The~~This field shows the number of Upstream SIDs the modem can support.

Type Length Value

B.C.1.3.1.9 Optional Filtering Support

~~The fields~~This field shows 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

Note: This CM capability is not subject to negotiation with the CMTS. The CM MUST include this capability in the DHCP request, but MUST NOT include this capability in the registration request. If a CMTS does receive this capability with in a registration request it MUST return the capability with the same value in the registration response.

B.C.1.4.2 Authorization Block
[Edit text as indicated]

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 the present document, but include [~~PKT-DQOS~~J163].

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

B.C.2.1 Packet Classification Encodings
[Modify 3rd paragraph and delete text as indicated]

The following configuration settings MUST be supported by all CMs which are compliant with the present document. All CMTSs MUST support classification of downstream packets based on IP header fields (subclause B.C.2.1.5).

~~**B.C.2.1.8**~~

~~**Upstream-Specific Classification Encodings**~~

~~**B.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.~~

B.C.2.2.3.2 Service Flow Identifier

[Edit text as indicated]

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. Both the CM and CMTS MAY use this TLV to encode Service Flow IDs in a DSD-REQ.

~~*B. C.2.2.5.1*~~ B.C.2.2.3.5 Quality of Service Parameter Set Type

[Move the entire existing section C.2.2.5.1 to section C.2.2.3.5, modify the first sentence of the first paragraph as follows; renumber subsequent subclauses as shown].

This parameter MUST appear within every Service Flow Encoding, with the exception of Service Flow Encodings in the DSD-REQ where the Quality of Service Parameter Set Type has no value.

~~B.C.2.2.5.2~~ *B.C.2.2.5.1* *Traffic Priority*

~~*B.C.2.2.5.3*~~ B *C.2.2.5.2* *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:

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

where the parameter B (in bytes) is the Maximum Traffic Burst Configuration Setting (refer to subclause B.C.2.2.~~5.4~~5.3).

B.C.~~2.2.5.3.1~~2.2.5.2.1 *Upstream Maximum Sustained Traffic Rate*

B.C.~~2.2.5.3.2~~2.2.5.2.2 *Downstream Maximum Sustained Traffic Rate*

B.C.~~2.2.5.4~~2.2.5.3 *Maximum Traffic Burst* ***[in addition to renumbering clause, edit 3rd and 4th paragraphs as follows]***

The minimum value of B is 1522 bytes. If this parameter is omitted, ~~then~~ the default ~~B is 1 522 bytes. The minimum~~

~~value of B is the larger of 1 522~~value for B is 3044 bytes ~~or~~. This parameter has no effect unless a non-zero value has been provided for the Maximum Sustained Traffic Rate parameter.

For an upstream service flow, if B is sufficiently less than the ~~value of~~ Maximum Concatenated Burst ~~Size (refer to subclause B.C.2.2.6.1).~~parameter, then enforcement of the rate limit equation will limit the maximum size of a concatenated burst.

B.C.~~2.2.5.5~~2.2.5.4 Minimum Reserved Traffic Rate

B.C.~~2.2.5.6~~2.2.5.5 Assumed Minimum Reserved Rate Packet Size

B.C.~~2.2.5.7~~2.2.5.6 Timeout for Active QoS Parameters

B.C.~~2.2.5.8~~2.2.5.7 Timeout for Admitted QoS Parameters

B.C.~~2.2.5.9~~2.2.5.8 Vendor Specific QoS Parameters

B.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~~If this parameter is omitted the default value is ~~0.~~1522.

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.

Note: The maximum size of a concatenated burst can also be limited by the enforcement of a rate limit, if the Maximum Traffic Burst parameter is small enough, and by limits on the size of data grants in the UCD message.

B.C.4 Confirmation Code

[Edit text as indicated]

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 and Dynamic Channel Change-Response 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.

The Confirmation Codes MUST be used in the following way: [change in 12th bullet only]

- Reject-authentication-failure(11) the requested transaction was rejected because the message contained an invalid HMAC-digest, CMTS-MIC, provisioned IP address, or timestamp.

B.D.1.1 DHCP Fields Used by the CM

[Edit text as indicated]

The following fields are expected in the DHCP response returned to the CM. Fields identified as critical MUST be present in the DHCP response, and fields identified as non-critical SHOULD be present. The CM MUST configure itself ~~based on~~with the critical fields from the DHCP response, and, if present, with the non-critical fields.

- The IP address to be used by the CM (yiaddr) (critical).
- The IP address of the TFTP server for use in the next phase of the bootstrap process (siaddr) (critical).
- 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 (non-critical).
- The name of the CM configuration file to be read from the TFTP server by the CM (file) (critical).
- The subnet mask to be used by the CM (Subnet Mask, option 1) (non-critical).
- 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 (non-critical).
- 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 (non-critical).
- A list of [RFC -868] time-servers from which the current time may be obtained (Time Server Option, option 4) (non-critical).
- A list of SYSLOG servers to which logging information may be sent (Log Server Option, option 7); see [DOCSIS5] (non-critical).

If a critical field is missing or is invalid in the DHCP response during initialisation, the CM MUST log an error and reinitialise its MAC and continue channel scanning.

If a non-critical field is missing or is invalid in the DHCP response during initialisation, the CM MUST log a warning, ignore the field and go operational, with the following considerations:

- If the subnet mask is missing or is invalid, the CM MUST use the default for the IP of Class A, B or C as defined in [RFC-791].
- If the time server is missing or is invalid, the CM MUST initialise the time for the events to Jan 1, 1970, 0h00.

If the IP address field is missing or is invalid in the DHCP response during renew or rebind, the CM MUST log an error and reinitialise its MAC and continue channel scanning.

If any other critical or non-critical field is missing or is invalid in the DHCP response during renew or rebind, the CM MUST log a warning, ignore the field and stay operational.

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 MUST 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 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, sub-option code 2. The option code 82 MUST be formatted as follows:~~
  ~~82 08 02 06 xx xx xx xx xx xx, where "xx xx xx xx xx xx" refers to before relaying the CM's RF side MAC address. The discovery to a DHCP relay agent information option is further described in [61]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. Bridging CMTSs SHOULD also provide this~~

~~functionality.~~

- All CMTSs MUST support the DHCP relay agent information option, ~~[ID-DHCP]~~ [RFC-3046]. 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. Bridging CMTSs SHOULD also provide this functionality.

B.D.2.2 Configuration File Settings

[update Note in 1st bullet list as shown]

- DOCSIS 1.0 Class of Service Configuration Setting~~.~~

  NOTE – A DOCSIS 1.0 CM ~~MUST~~must be provided with a DOCSIS 1.0 Class of Service Configuration. A CM conformant with the present document SHOULD only be provisioned with DOCSIS 1.0 Class of Service Configuration information if it is to behave as a DOCSIS 1.0 CM, otherwise it ~~MUST~~should be provisioned with Service Flow Configuration Settings.

[add 18th bullet to 2nd list in subclause – follows "Pad Configuration Setting"]

- SNMPv3 Notification Receiver

B.E.1 MAC Service Overview

[modify text in 2nd bullet]

The following data services are provided by the MAC service interface:

- a MAC service exists for classifying and transmitting packets to MAC service flows~~;~~.
- a-MAC service exists for receiving packets from MAC service flows. Packets ~~MAY~~may be received with suppressed headers~~;~~.

B.E.1.1 MAC Service Parameters

[edit paragraphs as shown]

- Active/Admitted QoS Traffic Parameters

  If two-phase service flow activation is being used, then two complete sets of QoS Traffic Parameters are controlled. The admitted QoS Parameters state the requirements for reservation of resources to be authorized by the CMTS. The ~~actived~~activated QoS Parameters state the requirements for activation of resources to be authorized by the CMTS. Admitted QoS parameters may be activated at a future time by the upper layer service. Activated QoS parameters ~~MAY~~may be used immediately by the upper layer service.

- Service Flow PHS Suppressed Headers

  Zero or more PHS suppressed header strings with their associated verification control and mask variables ~~MAY~~may be defined for each service flow. When such headers are defined, they are associated 1-to-1 with specific classification rules. In order to regenerate packets with suppressed headers a payload header suppression index is negotiated between the CM and CMTS.

B.E.2.3 MAC_GRANT_SYNCHRONIZE.indicate
[edit second to last sentence in 1st paragraph as shown]

It should also be noted that when synchronization is achieved with the CMTS downstream master clock, this indication ~~MAY~~may only be required once per active service flow. No implication is given as to how this function is implemented.

B.E.3.2 MAC_CREATE_SERVICE_FLOW.request
[edit 1st paragraph as shown]

Issued by the upper-layer service to the MAC to request the creation of a new service flow within the MAC service. This primitive is not issued for service flows that are configured and registered, but rather for dynamically created service flows. This primitive ~~MAY~~may also define classifiers for the service flow and supply admitted and activated QoS parameters. This function invokes DSA Signalling.

B.E.3.5 MAC_DELETE_SERVICE_FLOW.request
[edit bullet as shown]

Parameters:

- ServiceFlowID(s) - ~~optional~~ unique identifier value(s) for the deleted service flow(s).

B.E.3.6 MAC_DELETE_SERVICE_FLOW.response
[delete ServiceFlowID bullet as shown]

Parameters:

~~- ServiceFlowID - unique identifier value for the specific service flow being deleted.~~

- ResponseCode - success or failure code~~.~~

B.E.3.7 MAC_DELETE_SERVICE_FLOW.indicate
[edit bullet as shown]

Parameters:

- ServiceFlowID(s) - ~~optional~~ unique identifier value(s) for the deleted service flow(s).

B.G.2.1 Provisioning
[add new 2nd and 4th paragraph, modify 3rd paragraph]

The parameters of the TFTP config file for a DOCSIS 1.1 CM, are a superset of those for a DOCSIS 1.0 CM. Configuration file editors will have to be enhanced to incorporate support for these new parameters and the new MIC calculation.

A TFTP configuration file containing DOCSIS 1.0 Class of Service TLVs is considered a “DOCSIS 1.0-style” configuration file. A TFTP configuration file containing DOCSIS 1.1 Service Flow TLVs is considered a “DOCSIS 1.1-style” configuration file. A TFTP configuration file containing both Class of Service and Service Flow TLVs will be

rejected by the CMTS (see subclause B.9.2.9).

If a DOCSIS 1.1 CM is provisioned with a DOCSIS 1.0 ~~style TFTP configuration file it MUST register~~-style TFTP configuration file, like a DOCSIS 1.0 CM, it MUST NOT respond to REG-RSP with REG-ACK (although in the REG-REQ it MUST still specify "DOCSIS v1.1" in the DOCSIS Version Modem Capability and MAY specify ~~additional~~ 1.1 Modem Capabilities that it ~~supports~~can support when registered like a DOCSIS 1.0 CM). Thus, a DOCSIS 1.1 CM can be provisioned to work seamlessly on either a DOCSIS 1.0 or a DOCSIS 1.1 network. ~~Although, clearly, a DOCSIS 1.1 modem on a DOCSIS 1.0 network would be unable to support any DOCSIS 1.1 specific features.~~

If a DOCSIS 1.1 CM supports certain 1.1 capabilities when registered like a DOCSIS 1.0 CM (as indicated by the Modem Capabilities Encoding), those features MUST function according to the requirements defined in the DOCSIS 1.1 specifications.

B.G.3 Hybrid Devices

[change in 1st paragraph, add new 4th paragraph + Table]

Some DOCSIS 1.0 CM designs may be capable of supporting individual DOCSIS 1.1 features via a software upgrade. Similarly, some DOCSIS 1.0 CMTS's ~~MAY~~may be capable of supporting individual DOCSIS 1.1 features. To facilitate these "hybrid" devices, the majority of DOCSIS 1.1 features are individually enumerated in the Modem Capabilities.

If a hybrid CM intends to request such 1.1 capabilities from the CMTS during registration, it MUST send the ASCII coded string in Option code 60 of its DHCP request, "docsis1.0:xxxxxxx". Where xxxxx MUST be an ASCII representation of the hexadecimal encoding of the Modem Capabilities, refer to-subclauses B.C.1.3.1 and B.D.1.1. The DHCP server MAY use such information to determine what configuration file the CM is to use.

In order to control the hybrid operation of modems, if a DOCSIS 1.1 CMTS receives a 1.0-style Registration Request message from a CM, the CMTS MUST, by default, force the modem to operate in a “pure” 1.0 mode with respect to certain features by disabling those features via the Modem Capabilities Encoding in the Registration Response. Specifically, the CMTS MUST support the six default values given in square brackets in Table G-1. The CMTS MAY provide switches, as indicated in Table G-1, for the operator to selectively allow certain hybrid features to be enabled.

Table G-1. Hybrid Mode Controls

	Concatenation Support	Fragmentation Support	Privacy Support
1.0 CM	allow/[deny]	allow/[deny]	allow BPI+/[force BPI]
1.1 CM in 1.0 mode	allow/[deny]	allow/[deny]	allow BPI+/[force BPI]

Annex J Error Codes and Messages

[Insert new first paragraph, delete remaining text as indicated]

To avoid redundancy, the error codes and messages are combined with and listed in [SCTE3] . Please refer to that document for a complete list of 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 other error codes are simply "it failed".~~

~~TABLE J-1~~

~~**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.
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. Re-initializing 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.
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.
I200.0	**Version 1.1 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	**Version 1.1 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.
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 describe in the RF spec. Annex 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.
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.
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.
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.~~
~~**B00.0**~~	~~**Baseline Privacy**~~
~~B01.0~~	~~TBD~~

B.K.1 Introduction

[add 2nd bullet]

This clause attempts to clarify how the DOCSIS 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:

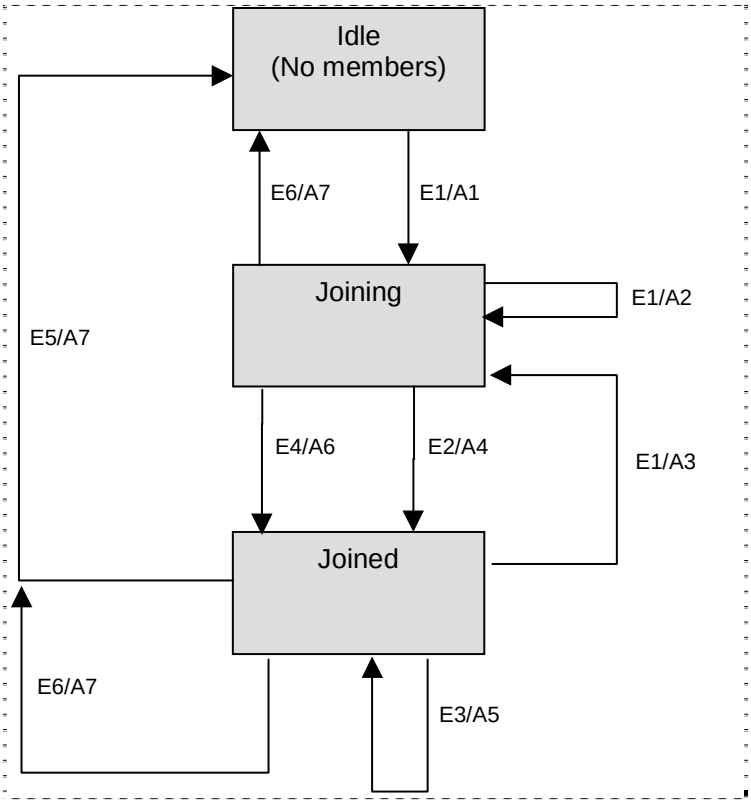
- It does-not explicitly talk about packet arrivals while deferring or waiting for pending grants and is vague about sizing piggyback requests.
- The CM sends a Piggyback Request for the next frame in the last fragment and not inside one of the headers of the original frame.

Annex B.L IGMP Example

[edit first paragraph as shown, replace current Figure L-1 with new Figure and update figure caption, delete table and following text, replace with text as indicated]

Subclause B.5.3.1defines the requirements for CMTS and CM support of IGMP Signalling. This annex provides ~~further details on~~an example CM ~~support~~passive-mode state machine for ~~IGMP~~maintaining membership of a single multicast group.

~~The process defined MAY be supported by compliant CMs. Refer to Figure L-1.~~



FIGURE

L-1 **IGMP Support – CM passive mode**

~~TABLE L-1~~

~~**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~~

~~L.1 Transition Events~~

~~**1A**~~

- ~~Forward Membership Report (MR) Upstream.~~
- ~~Start~~

- ~~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.~~

Events

E1: MR received on CPE I/f
E2: M1 timer expired
E3: MQ received on RF I/f
E4: MR received on RF I/f
E5: M2 timer expired
E6: Auth Failure
Note: SA-MAP response returns an error code of 7 - “not authorized for requested downstream traffic flow”

Actions

A1: MQI= 125 sec; QRI = 10 sec; Start M1 timer with random value between 0 and 3 sec; start M2 timer = 2*MQI+QRI; start TEK machine, if necessary; add multicast addr to multicast filter
Note: If the multicast traffic is encrypted, then a TEK machine needs to be started to decrypt the encrypted multicast packets. To determine whether the multicast is encrypted, the CM makes a SA-MAP request to the CMTS to get the associated SAID of the multicast group address. If the SA-MAP response returns an SAID, then a TEK machine is started. No TEK machine is necessary, if the SA-MAP response indicates that the multicast traffic is not encrypted. The SA-MAP response may also indicate that the CM is not authorized to receive this multicast traffic. In which case, the CM terminates the multicast state machine and stops forwarding the multicast traffic.

A2: discard MR packet

A3: reset M2 timer = 2*MQI+QRI; start M1 timer with random value between 0 and 3 sec

A4: transmit MR on RF I/f; set I = current time

A5: recompute MQI = MAX(125, current time – I); set I = current time, forward MQ on CPE i/f

A6: cancel M1 timer

A7: delete multicast addr from multicast filter

B.N.6.2.1 Overview

[edit 4th paragraph as shown]

The PMD sublayer can support a near-continuous mode of transmission, wherein ramp-down of one burst MAY overlap the ramp-up of the following burst, so that the transmitted envelope is never zero. The system timing of the TDMA transmissions from the various CMs MUST provide that the centre of the last symbol of one burst and the centre of the first symbol of the preamble of an immediately following burst are separated by at least the duration of five symbols. The guard ~~time~~band MUST be greater than or equal to the duration of five symbols plus the maximum timing error. Timing error is contributed by both the CM and CMTS. CM timing performance is specified in subclauses N.6.2.7, N.6.2.8, N.6.2.10 and N.6.3.7. Maximum timing error and guard ~~time~~band may vary with CMTSs from different vendors. The term guard time is similar to the guard band, except that it is measured from the end of the last symbol of one burst to the beginning of the first symbol of the preamble of an immediately following burst. Thus, the guard time is equal to the guard band – 1.

B.O.1.0 Scope

[Modify the first sentence of this subclause to make it agree with Amendment 1 to Annex B.]

This ~~informative, optional~~ normative Annex providesMAC layer privacy services for CMTS – CM communications. …

B.O.2.0 References

[Update the following normative references.]

J.122 ITU-T Recommendation J.122 Second generation transmission systems for interactive cable television services - IP cable modems, (12/02).

~~RFC2459 R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, January 1999.~~

RFC3280 R. Housley, W. Ford, W. Polk, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC3280, April 2002.

SCTE DSS-02-06 DOCSIS 1.1 Operations Support System Interface, 2002

ANSI/SCTE 79-2 2002 (formerly DSS 02-07) DOCS 2.0 Operations Support System Interface

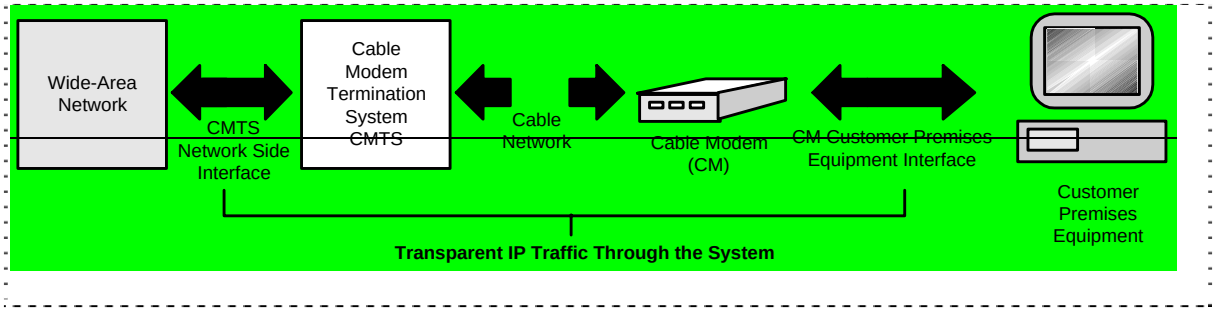
X.509 ITU-T Recommendation X.509 ~~(1997 E)~~: Information Technology - Open Systems Interconnection - The Directory: ~~Authentication Framework, June 1977~~ Public-key and attribute certificate frameworks, (03/2000)

B.O.5.0 Background and Overview

[Remove redundant text found in B.1.3.1]

~~Cable operators are interested in deploying high-speed packet-based communications systems on cable television networks that are capable of supporting a wide variety of services. Services under consideration by cable operators include high-speed Internet access, packet telephony service, video conferencing service, frame relay equivalent service and many others.~~

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



~~Figure 1-1. Transparent IP Traffic Through the Data-Over-Cable System~~

~~The transmission path over the cable system is realized at the headend by a CMTS, and at each customer location by a CM. At the headend (or hub), the interface to the data-over-cable system is~~

~~called the Cable Modem Termination System - Network-Side Interface (CMTS-NSI)). At the customer locations, the interface is called the cable-modem-to-customer-premise-equipment interface (CMCI). The intent is for the cable operators to transparently transfer IP traffic between these interfaces, including but not limited to datagrams, DHCP, ICMP, and IP Group addressing (broadcast and multicast).~~

B.O.5.1.4 QoS SIDs and BPI+ SAIDs

[Edit the second paragraph as indicated below.]

Since all of a CM's upstream traffic is encrypted under its unique Primary SA, upstream MAC Frames, unlike downstream MAC Frames, need not carry a BPI+ SAID in their extended headers; instead, the Baseline Privacy EH element ~~contains the QoS SID identifying the Active Upstream Service Flow over which the MAC Frame is transported~~ MAY contain any valid QoS SID assigned to the CM.

B.O.5.2.1 Cable Modem Initialization

[Edit the 3rd paragraph as indicated.]

If a CM is to run Baseline Privacy, ~~its parameter file, downloaded during the transfer of operational parameters,~~the Privacy Enable setting (type 29) in the DOCSIS 1.1/2.0 style (see B.G.2.1 and J.122 respectively) configuration file, MUST ~~include~~be explicitly/implicitly set to enable, regardless of the presence of the Baseline Privacy Configuration Settings (type 17). In other words, Baseline Privacy Configuration Settings do not need to be present in the configuration file in order to run Baseline Privacy. These additional configuration settings are defined in Appendix B.O.A.

B.O.6.3 Requirements on Usage of BP Extended Header Element in MAC Header

[Edit the 3rd paragraph as indicated.]

If BPI+ is not enabled for a CM's unicast traffic, ~~unfragmented~~fragmented upstream frames ~~MAY~~MUST still use the BP Extended Header element, but with the Encryption ENABLE bit turned off~~, to carry~~ (0). This way the BP Extended Header can still be used for piggybacked bandwidth requests according to fragmentation rules described in this document or J.122~~. Alternatively, unfragmented upstream frames' piggybacked bandwidth requests MAY be carried in a REQUEST Extended Header element (EH_TYPE=1)~~.

B.O.7.1.2.1.4 Reauthorize Wait (Reauth Wait)

[Edit word indicated.]

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

B.O.7.1.2.1.6 Silent

[Edit text as indicated.]

The CM received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated the error was of a permanent nature. This triggers a transition to the Silent state. In the Silent state, ~~where~~ the CM ~~is not permitted to~~MUST NOT pass CPE traffic, but ~~is~~MUST be able to respond to SNMP management requests arriving from across the cable network. CMTS MAY forward any IP traffic without encryption.

B.O.7.1.2.3.6 Permanent Authorization Reject (Perm Auth Reject)

[Edit noted statements and add paragraph after bulleted list as indicated.]

BPI+'s associated OSS document provides a description of the particular CMTS MIB objects which control the actions a CMTS takes in the event any of the above error conditions occur.

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

B.O.7.1.2.4.2 ~~Reauthorization~~Reauthorize Wait Timeout (Reauth Wait Timeout)

[Edit section title as indicated above.]

B.O.7.1.3 TEK State Machine

[Edit noted statements and add text as indicated.]

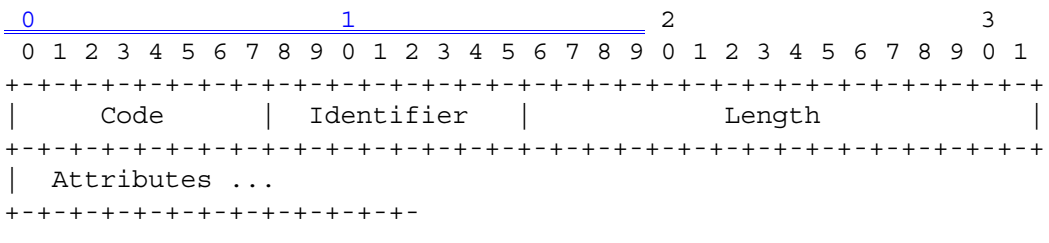
Through operation of a TEK state machine, the CM attempts to keep its copies of a SAID's TEKs synchronized with those of its CMTS. A TEK state machine issues Key Requests to refresh copies of its SAID's keying material ~~soon~~ after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for CM/CMTS clock skew and other system processing and transmission delays, the CM schedules its Key Requests a configurable number of seconds (*i.e.*, "TEK Grace Time") before the newer TEK's estimated expiration in the CMTS. With the receipt of the Key Reply, the CM MUST always update its records with the TEK Parameters from both TEKs contained in the Key Reply Message. Figure 9-2 illustrates the CM's scheduling of its key refreshes in conjunction with its management of a BPI+ SA's active TEK's.

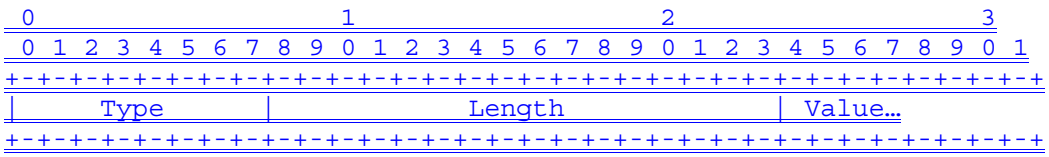
B.O.7.1.~~4.5~~3.5 Actions

[Correct subclause numbering as indicated above.]

B.O.7.2.1 Packet Formats

[Edit noted statements (first numeric row indicates increments of 10 and MUST BE placed exactly as depicted and applies to all attributes in B.O.7) and add text as indicated.]





~~B.O.7.2.1.12 SAID Map Reject (Map Reject)~~

[delete entire section]

~~A CMTS sends SA Map Reject as a negative response to a client CM's SA Map Request. The SA Map Reject informs the CM that either (1) downstream traffic flow identified in the SA-Query Attribute is not being encrypted or (2) the requesting CM is not authorized to receive that traffic. The contents of an error code attribute distinguishes between the two cases. Section 8 describes the SA Mapping state model which uses the message.~~

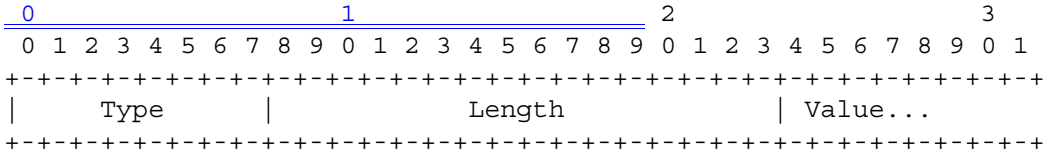
~~Code: 15~~

~~Attributes:~~

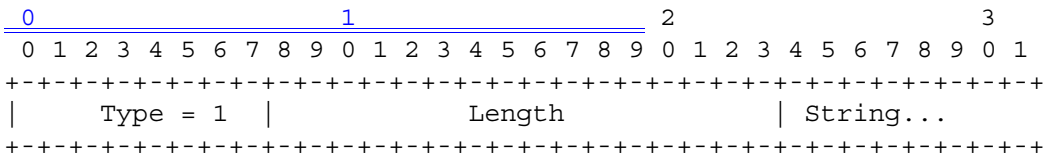
~~Table 7-16. SA MAP Reject Attributes~~

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

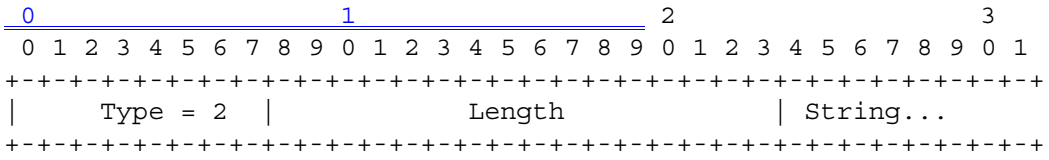
B.O.7.2.2 BPKM Attributes



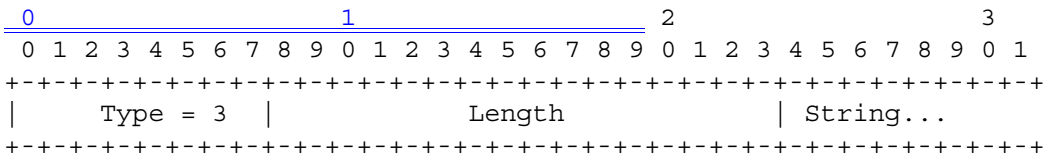
B.O.7.2.2.1 Serial-Number



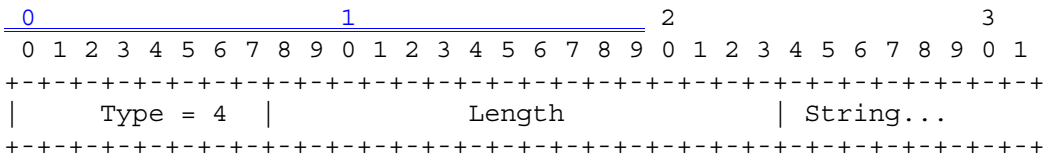
B.O.7.2.2.2 Manufacturer-ID



B.O.7.2.2.3 MAC-Address



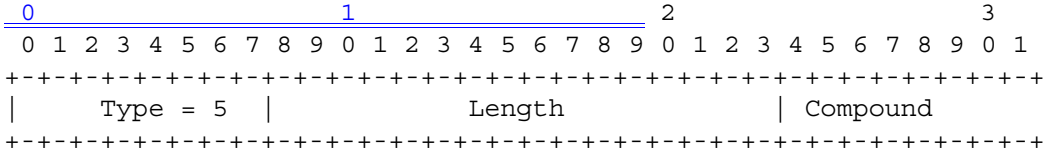
B.O.7.2.2.4 RSA-Public-Key



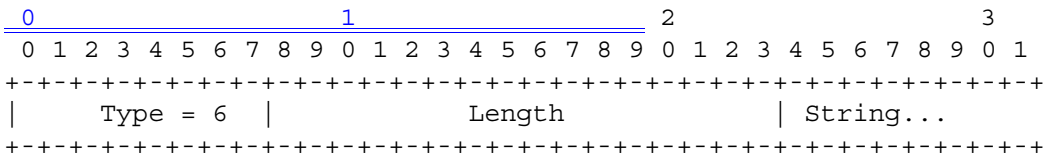
Length

~~106~~106, 140, or ~~140~~270 (length of DER-encoding, using F4 as the public exponent, and a 768-bit ~~or~~, 1024-bit, or 2048-bit public modulus, respectively) ~~17~~

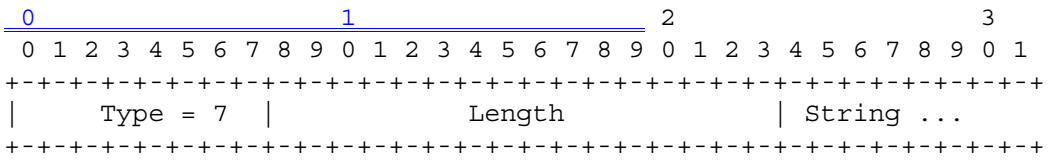
B.O.7.2.2.5 CM-Identification



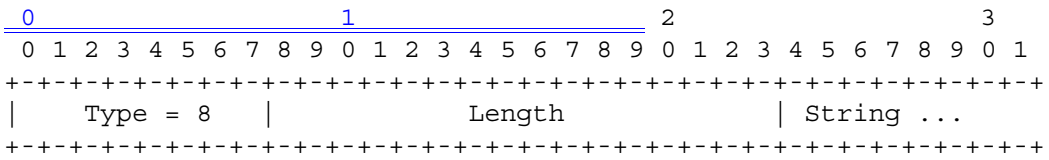
B.O.7.2.2.6 Display-String



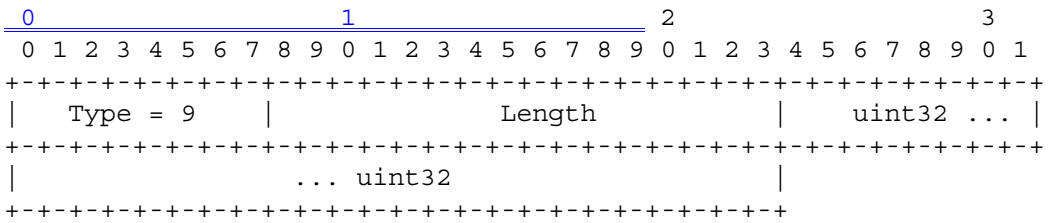
B.O.7.2.2.7 AUTH-Key



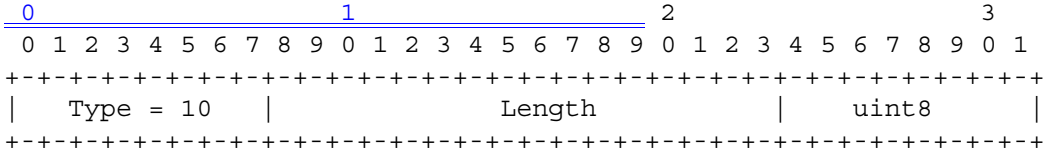
B.O.7.2.2.8 TEK



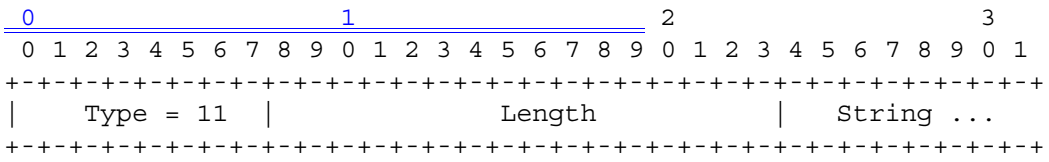
B.O.7.2.2.9 Key-Lifetime



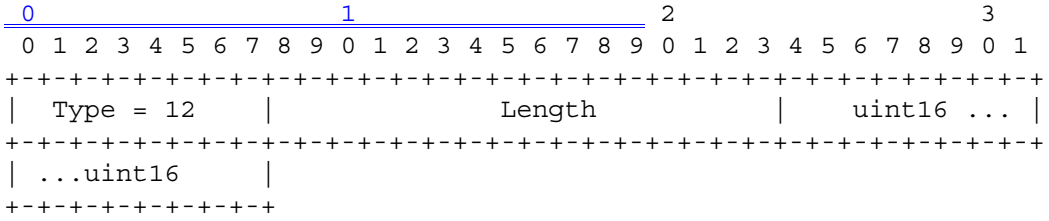
B.O.7.2.2.10 Key-Sequence-Number



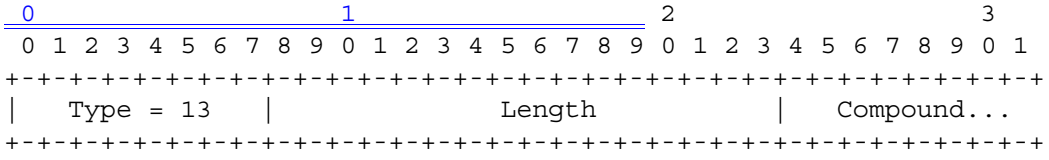
B.O.7.2.2.11 HMAC-Digest



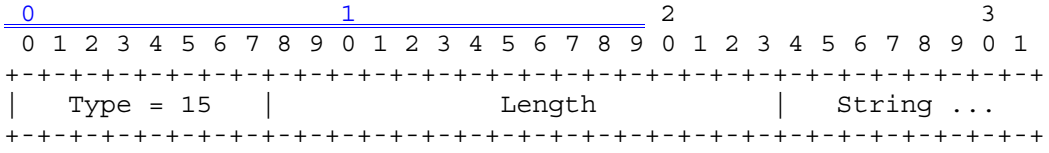
B.O.7.2.2.12 SAID



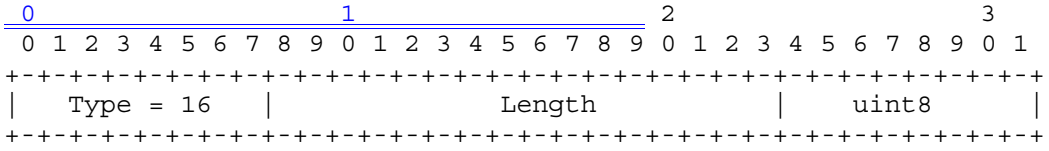
B.O.7.2.2.13 TEK-Parameters



B.O.7.2.2.14 CBC-IV



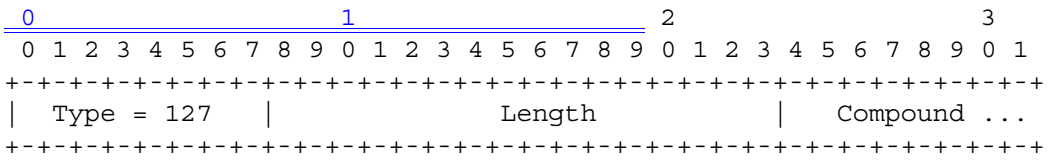
B.O.7.2.2.15 Error-Code



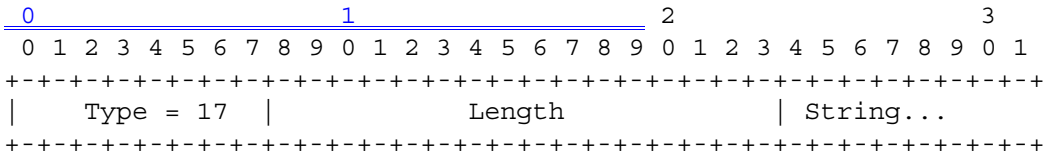
[Edit noted statements and add text as indicated.]

A CMTS MUST include the Error-Code Attribute in all Authorization Reject, Authorization Invalid, Key Reject ~~and~~, TEK Invalid, and SA-MAP Reject messages. Table 4-20 lists code values for use with this Attribute. The CMTS MUST employ the nonzero error codes list below for SA-MAP Reject messages. The CMTS MAY employ the nonzero error codes ~~(1-8)~~ listed below for the other BPI+ message types; it MAY, however, return a code value of zero (0). Error code values other than those defined in Table 7-20 MUST be ignored. Returning a code value of zero sends no additional failure information to the CM; for security reasons, this may be desirable.

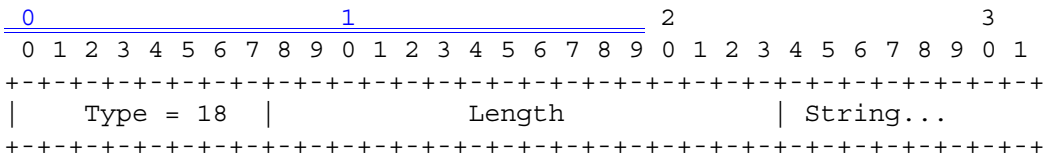
B.O.7.2.2.16 Vendor-Defined



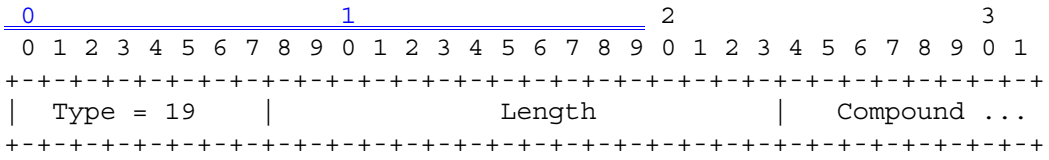
B.O.7.2.2.17 CA-Certificate



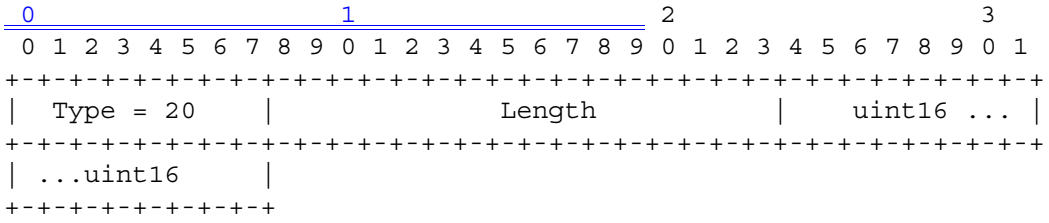
B.O.7.2.2.18 CM-Certificate



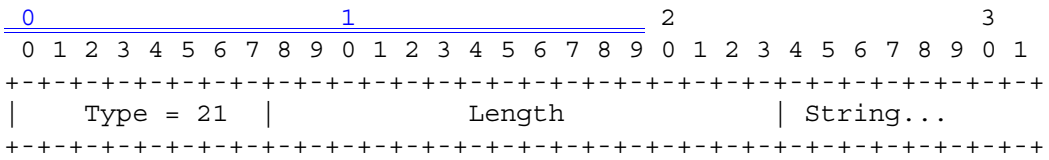
B.O.7.2.2.19 Security-Capabilities



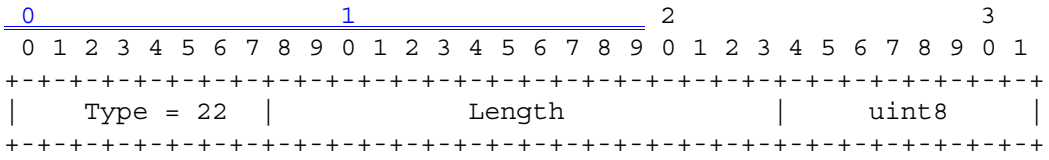
B.O.7.2.2.20 Cryptographic-Suite



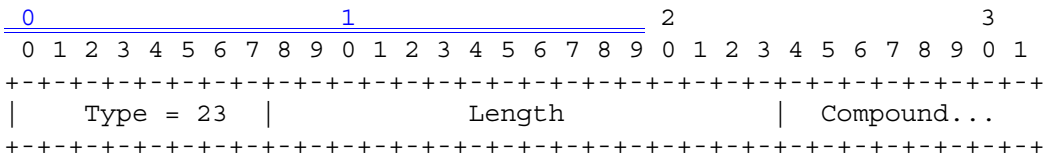
B.O.7.2.2.21 Cryptographic-Suite-List



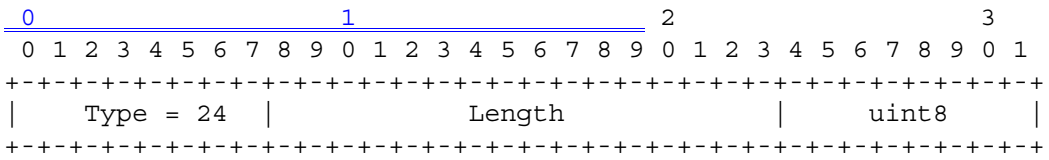
B.O.7.2.2.22 BPI-Version



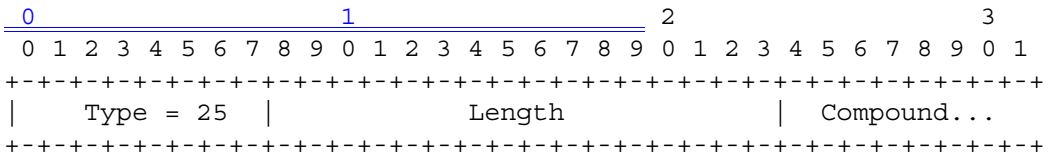
B.O.7.2.2.23 SA-Descriptor



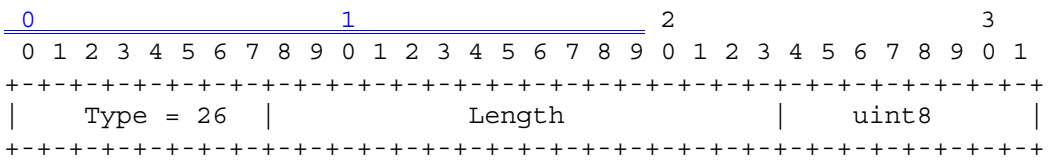
B.O.7.2.2.24 SA-Type



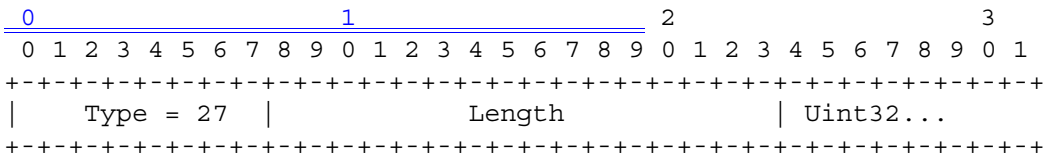
B.O.7.2.2.25 SA-Query



B.O.7.2.2.26 SA-Query-Type



B.O.7.2.2.27 IP-Address



B.O.7.2.2.28 Download-Parameters

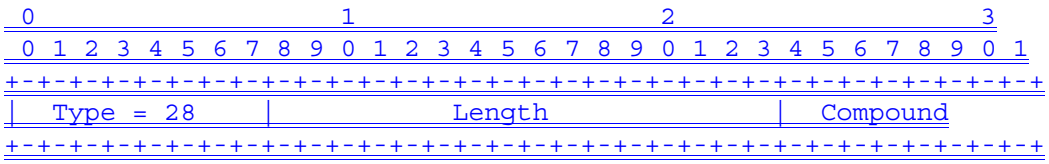
[Add entire new section.]

Description

This attribute is used in the CM Code File defined in the section B.3.1. This attribute is a compound attribute, consisting of a collection of sub-attributes.

Sub-attribute MAY include one or both of the following attribute(s) in this order.

- RSA-Public-Key (zero or one)
- CA-Certificate (zero, one or more)



Type

28

Length

>=0

B.O.8.2 Theory of Operation

[Edit text in 4th and 7th paragraphs as indicated.]

If the CM receives a Map Reject, it ceases all further attempts to obtain the mapping. In the case where access to the downstream traffic flow is mapped to a BPI+ SA, and the requesting CM is not authorized access for that SA, the CM and its attached CPE device will be denied access because the CM cannot obtain keying material needed to decrypt the downstream traffic flows encrypted under that SA. E.g., the user may be requesting a premium service that he or she is not subscribed to. In the case where the requested traffic flow is not encrypted (i.e., it is not mapped to a SA), the unencrypted traffic will simply be forwarded to the attached CPE device. E.g., the CM makes an SA-MAP request for the All-Hosts multicast address. Since multicast packets addressed to the All-Hosts multicast address are necessary for the proper operation of IGMP, there is no need to encrypt these packets.

Note that a CMTS ~~can~~MAY assign multiple traffic flows (i.e., IP multicast addresses) to the same SA. If more than one downstream traffic flow is being encrypted under the same Dynamic SA, a CM may already be running a TEK state machine for the SA identified in the Map Reply. Note also that the SA mapping returned in the Map Reply need not be

a Dynamic SA: the requested traffic flow may be mapped to the CM's Primary SA or a Static SA.

B.O.9.2 Cable Modem

[Edit 4th paragraph as indicated below and replace Figure 9-2.]

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

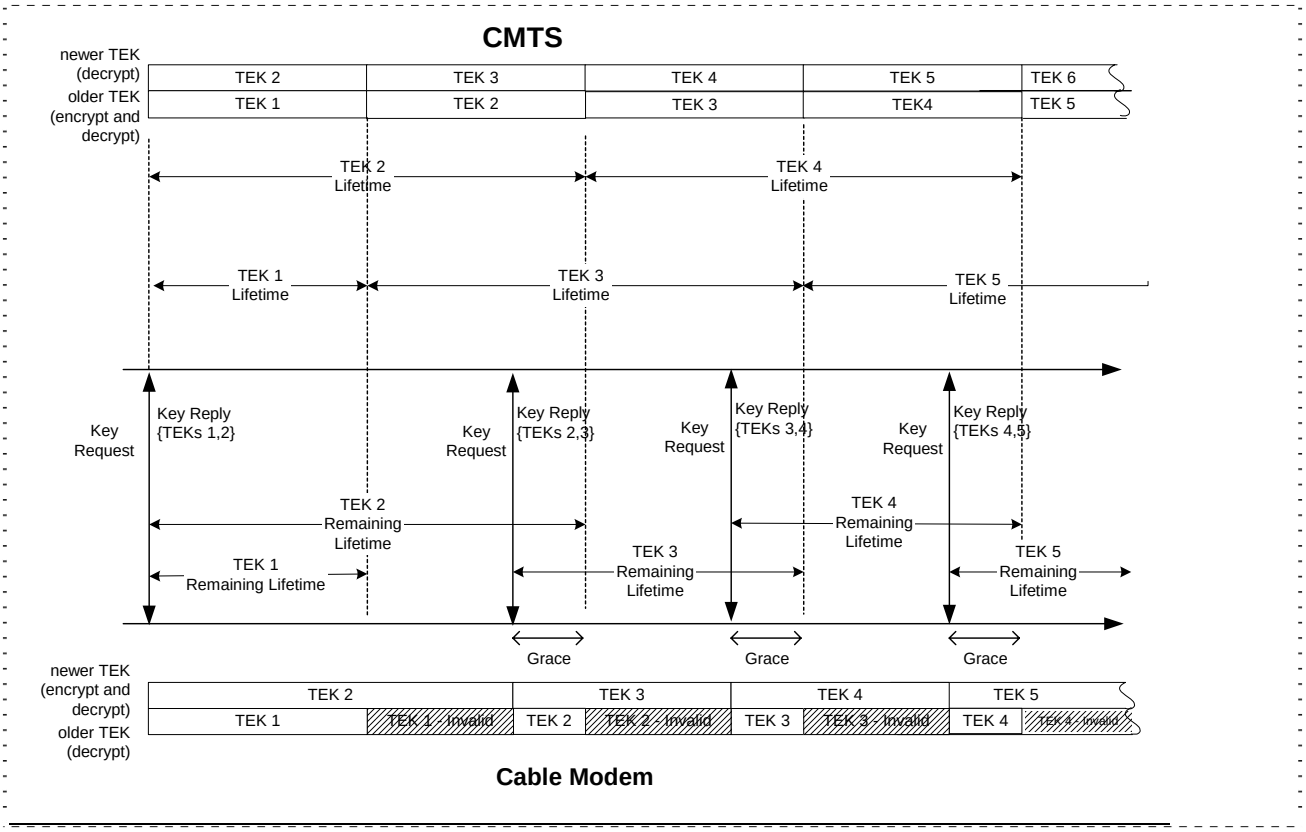


Figure 9-2. TEK Management in CMTS and CM

B.O.10.1 Packet Data Encryption

[Edit 2nd and 3rd paragraph as indicated.]

BPI+ implementations running on J.112 Annex B hardware (the predominant hardware/software configuration) MUST support ~~both 40~~56-bit DES and ~~56~~MAY support 40-bit DES. ~~Operation with 56-bit DES is STRONGLY RECOMMENDED.~~

BPI+ supports 40-bit DES principally to permit interoperability with 40-bit J.112 Annex B initial version hardware upgraded to run BPI+. 40-bit DES is identical to 56-bit DES, with the exception that 16 bits of the 56-bit DES key are set to known, fixed values. ~~A~~If a CM or CMTS is running the optional 40-bit DES, it MUST mask off (to zero) the sixteen left-most bits of any 56-bit DES key prior to running encryption/decryption operations. Note that the masked bits are the sixteen left-most bits that would be present AFTER the removal of every eighth bit from the 64-bit TEK (i.e., the so-called parity bits). J.112 Annex B v2 and 56-bit J.112 Annex B v1 hardware running BPI+ MAY implement 40-bit DES key masking in software.

B.O.10.5 Public-Key Encryption of Authorization Key

[Add two paragraphs of new text after the first paragraph.]

Note that Baseline Privacy [DOCSIS2] employed the encryption scheme described in version 1.5 of the PKCS #1 standard [RSA1]. This is the same scheme as RSAES-PKCS1-v1_5 in [RSA3]. In order to maintain backwards compatibility, CMs and CMTSs MUST revert to RSAES-PKCS1-v1_5 for encrypting the authorization key when falling back to BPI.

The Baseline Privacy [DOCSIS2] protocol, whose support is required in J.112 Annex B v1 CMs, specifies an modulus length of 768 bits for its RSA keys. In order to enable software upgrades of J.112 Annex B v1 CM hardware to BPI+, the BPI+ protocol MUST support 768-bit as well as 1024-bit modulus lengths. J.112 Annex B v2 CMs, however, MUST employ RSA keys having a 1024-bit modulus length. To support interoperability with the upgraded v1 CMs, a J.112 Annex B v2 CMTS's BPI+ implementation MUST support 768-bit as well as 1024-bit modulus lengths.

B.O.11 Physical Protection of Keys in the CM and CMTS

[Add text at the end of the section as indicated.]

An internal CM would be classified as a FIPS PUBS 140-1 *multiple-chip embedded cryptographic module*; the Security Level 1 requirements for these devices are the two first bullets listed above.

B.O.12.1 BPI+ Certificate Management Architecture Overview

[Insert new paragraph just prior to Figure 12-1.]

Currently, the Root Certificate Authority also serves as the root CA to issue the Code Verification Certificate (CVC) for the Secure Software Downloading specified in Annex D to this annex. However, there is no security reason to require the same root CA to issue both the Manufacturer CA Certificate and the CVC. Therefore, the CVC may be issued by the different root Certificate Authority in the future.

B.O.12.2.1 tbsCertificate.validity.notBefore and tbsCertificate.validity.notAfter

[Edit text as indicated]

Cable Modem certificates will not be renewable, and, thus, must have a validity period greater than the operational lifetime of the cable modem. A Manufacturer CA certificate MUST be valid from the issuance date for ~~5 years~~a period defined by [SCTE DSS 02-06] or [ANSI/SCTE 79-2] and re-issued ~~every 2 to 3 years~~in a period defined by [SCTE DSS 02-06] or [ANSI/SCTE 79-2]. The Root CA certificate MUST be valid from the date when the Root CA starts operating for a period ~~of 30 years~~defined by the [SCTE DSS 02-06] or [ANSI/SCTE 79-2] and re-issued ~~before it expires~~in a period defined by [SCTE DSS 02-06] or [ANSI/SCTE 79-2].

B.O.12.2.2 tbsCertificate.serialNumber

[Edit first paragraph and add new second paragraph as indicated.]

~~Serial numbers for Cable Modem certificates signed by a particular issuer MUST be assigned by the manufacturer in increasing order. Thus, if the tbsCertificate.validity.notBefore field of one certificate is greater than the tbsCertificate.validity.notBefore field of another certificate, then the~~

~~serial number of the first certificate must be greater than the serial number of the second certificate.~~ The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer. The Manufacturer SHOULD NOT impose or assume a relationship between the serial number of the certificate and the serial number of the modem to which the certificate is issued.

Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conformant CAs MUST NOT use serialNumber values longer than 20 octets.

Note: Certificate users in the J.112-B v2 system MUST be prepared to handle certificates that may already have negative, or zero, serial numbers, to ensure backwards compatibility.

B.O.12.2.4 tbsCertificate.issuer and tbsCertificate.subject

[update the reference in the last paragraph of this subclause as follows:]

[RFC~~2459~~3280]

B.O.12.2.4.1 Root Certificate

[edits as shown.]

countryName=US
organizationName=Data ~~OverCableService~~Over Cable Service Interface Specifications
organizationalUnitName=Cable Modems
commonName=~~J.112 Annex B~~DOCSIS Cable Modem Root Certificate Authority

---

B.O.12.2.4.2 Manufacturer Certificate

[edits as shown.]

countryName=<Country of Manufacturer>
[stateOrProvinceName=<state/province>]
[localityName=<City>]
organizationName=<Company Name>
organizationalUnitName=~~J.112 ANNEX B~~DOCSIS
[organizationalUnitName=<Manufacturing Location>]
commonName=<Company Name> [<Serial Identifier>] Cable Modem Root Certificate Authority [<Serial Identifier>]

The countryName, organizationName, and commonName attributes MUST be included and MUST have the values shown.

The commonName MAY contain a serial identifier (e.g., 1, 2, ONE, TWO, A, B, I, II, etc.) to identify different Manufacturer CAs deployed by the same Manufacturers with the same Company Name.

The organizationalUnitName having the value ~~"J.112 Annex B"~~"DOCSIS" MUST be included.

The organizationalUnitName representing manufacturing location SHOULD be included. If included, it MUST be preceded by the organizationalUnitName having value ~~"J.112 ANNEX B."~~"DOCSIS."

B.O.12.2.7 tbsCertificate.extensions

[Edit the paragraph as shown.]

~~BPI+~~Cable Modem certificates and Manufacturer CA certificates are not required to include any extensions; this is true even for extensions mandated by [RFC~~2459~~3280]. ~~BPI+~~Cable Modem certificates ~~MAY~~and Manufacturer CA certificates may include extensions as described in sections B.O.12.2.7.1 and B.O.12.2.7.2, respectively. The section B.O.12.2.7.3 specifies the ~~following subsections~~requirements on the extensions of Root CA certificate. Extensions included in BPI+ certificates MUST conform to [RFC~~2459~~3280].

B.O.12.2.7.1 Cable Modem Certificates

[Edit and add text as indicated.]

Cable Modem certificates MAY contain ~~non-critical~~noncritical extensions; they MUST NOT contain critical extensions. If the KeyUsage extension is present, the ~~keyAgreement~~digitalSignature and keyEncipherment bits MUST be turned on, keyCertSign and cRLSign bits MUST be turned off, and all other bits SHOULD be turned off. The basicConstraints extension MAY appear as a non-critical extension in cable modem certificates.

B.O.12.2.7.2 ~~Root and~~ Manufacturer CA Certificates

[edit and add text to this subclause as indicated below.]

~~Root and~~Manufacturer CA certificates MAY contain the Basic Constraints extension and/or the Key Usage extension. If included, ~~the Basic Constraints extension~~these extensions MAY appear as a critical extension or as a ~~non-critical~~noncritical extension.

~~Root and~~Manufacturer CA certificates MAY contain ~~non-critical~~noncritical extensions; they MUST NOT contain critical extensions other than, possibly, the Basic Constraints extension and the Key Usage extension.

If the ~~KeyUsage~~Key Usage extension is present in a ~~Root or~~Manufacturer CA certificate, the keyCertSign bit MUST be turned on, cRLSign bit MAY be turned on, and all other bits SHOULD be turned off.

If the Basic Constraints extension is present, the cA MUST be set to TRUE and the pathLenConstraint MUST be set to 0.

B.O.12.2.7.3 Root CA Certificate

[Insert new subclause]

Root CA certificate MUST contain the Basic Constraints extension and the Key Usage extension as critical extensions.

Root CA certificate MAY contain noncritical extensions; they MUST NOT contain critical extensions other than the Basic Constraints extension and the Key Usage extension.

For the KeyUsage extension, the keyCertSign bit MUST be turned on, cRLSign bit MAY be turned on, and all other bits SHOULD be turned off.

For the Basic Constraints extension, the cA MUST be set to TRUE and the pathLenConstraint MUST be set to 1.

B.O.12.3 Cable Modem Certificates Storage and Management in the CM

[Edit the 2nd paragraph as indicated.]

The ~~Root~~root CA~~'s (RSA)~~ public key for the CVC verification, which the CM uses to verify the Code Verification Certificate (CVC) for the Secure Software Download defined in Annex B.O.D of this document, MUST be placed into the CM's non-volatile memory. ~~(The CM uses the Root CA to verify digital signatures attached to tftp-downloaded software upgrades Appendix D discusses the use of code signatures to verify optional software upgrades.)~~ While the Root CA for the cable modem certificate chain currently issues the CVC, a different root CA may issue the CVC in the future. Therefore, the CM MUST NOT use the root CA public key for the CVC verification embedded in the CM's non-volatile memory in order to verify the cable modem certificate chain.

B.O.12.4 Certificate Processing and Management in the CMTS

[Edit the paragraph immediately following Figure 12-2 as indicated.]

BPI+ requires that CMTSs support administrative controls that allow the operator to override certification chain validation by specifying a Manufacturer CA or CM Certificate to be trusted or untrusted. A detailed description of these administrative controls on CMTS certificate management is ~~to be~~ provided in ~~an~~BPI+'s associated OSS document. This section specifies the management model for the exercise of these controls, as well as the processing a CMTS undertakes to assess a CM Certificate's validity, and thus verify the binding between the CM's identity and its public key.

B.O.12.4.1 CMTS Certificate Management Model

[Edit the 1st paragraph as indicated.]

The CMTS maintains copies of Root CA, Manufacturer CA and Cable Modem Certificates, which it obtains through either provisioning or BPKM messaging. Each certificate a CMTS learns of MUST be marked as being in one of four states: Untrusted, Trusted, Chained or Root. Only the Root CA Certificate (a self-signed certificate containing the Root CA's trusted public key) MUST be marked as Root. However, a CMTS MAY support multiple Root CA Certificates. Root ~~certificates~~Certificate(s) MUST be provisioned within a CMTS and the CMTS MUST support the function to show the entire Root Certificate(s) and/or its thumbprint so that the operator can verify the Root Certificate(s).

B.O.12.4.2 Certificate Validation

[Edit and add text as indicated.]

6. in the case of a CM Certificate, if the KeyUsage extension is present, the digitalSignature and/or keyAgreement ~~and~~bits are turned on, the keyEncipherment ~~bits~~bit ~~are~~is turned on, and the keyCertSign~~,~~ and cRLSign bits are off~~, and all other bits SHOULD be off~~; in the case of a Manufacturer CA Certificate, if the KeyUsage extension is present, the keyCertSign bit is turned on~~, and all other bits SHOULD be off~~.

B.O.A.1 Encodings

[Edit and add text as indicated.]

The following type/length/value encodings MUST be used for any Baseline Privacy configuration settings ~~MUST be used~~ included in ~~both~~ the configuration file ~~and~~. The Baseline Privacy configuration settings in the RF MAC CM registration requests MUST be the same as those included in the configuration file. 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.

B.O. A.1.1 Baseline Privacy Configuration Setting

[Edit the 1st paragraph as follows.]

The combination of RFI 1.1's Privacy Enable configuration setting (~~J112 ANNEX B~~B.C.1.1.16) and the Privacy Support Modem Capability Setting (B.C.1.3.1.6) controls whether Baseline Privacy Plus is enabled or disabled in a CM. ~~If Baseline Privacy is enabled, the Baseline Privacy Configuration Setting MUST also be present.~~ If the operator intends to provision a CM to operate in BPI+ mode using the default BPI Configuration Parameter(s) specified in the Table A-1, the corresponding Baseline Privacy Configuration subsetting(s) in the configuration file MAY be omitted. If the configuration file does not contain all the necessary BPI+ parameters, the CM MUST use the default value(s) specified in the Table A-1 for the missing parameter(s). On the other hand, if the operator intends to provision a CM to operate in BPI+ mode using the BPI Configuration Parameter(s) different from the default value(s) in the Table A-1, the corresponding Configuration subsetting(s) MUST be present. The Baseline Privacy Configuration setting MAY be present if Baseline Privacy Plus is disabled. The separate Privacy Enable parameter allows an operator to disable or re-enable Baseline Privacy by toggling a single configuration parameter, thus not requiring the removal or re-insertion of the larger set of Baseline Privacy Configuration parameters.

B.O.A.2 Parameter Guidelines

[Edit and add text as indicated in rows 6-8 in the table.]

Table A-1. Recommended Operational Ranges for BPI Configuration Parameters

System	Name	Description	Minimum Value	Default Value	Maximum Value
CMTS	Authorization Lifetime	Lifetime, in seconds, CMTS assigns to new Authorization Key	1 day (86,400 sec.)	7 days (604,800 sec.)	70 days (6,048000 sec.)
CMTS	TEK Lifetime	Lifetime, in seconds, CMTS assigns to new TEK	30 min. (1800 sec.)	12 hours (43,200 sec.)	7 days (604,800 sec.)
CM	Authorize Wait Timeout	Auth Req retransmission interval from Auth Wait state	2 sec.	10 sec.	30 sec.
CM	Reauthorize Wait Timeout	Auth Req retransmission interval from Reauth Wait state	2 sec.	10 sec.	30 sec.
CM	Authorization Grace Time	Time prior to Authorization expiration CM begins re-authorization	5 min. (300 sec.)	10 min. (600 sec.)	35 days (3,024,000 sec).
CM	Operational Wait Timeout	Key Req retransmission interval from Op Wait state	1 sec.	~~1~~10 sec.	10 sec.
CM	Rekey Wait Timeout	Key Req retransmission interval from Rekey Wait state	1 sec.	~~1~~10 sec.	10 sec.
CM	TEK Grace Time	Time prior to newer TEK expiration CM begins rekeying	5 min. (300 sec)	1 hour (3,600 sec.)	3.5 days (302,399 sec)
CM	Authorize Reject Wait	Delay before re-sending Auth Request after receiving Auth Reject	10 sec.	60 sec.	10 min. (600 sec.)

B.O.B.2 Overview

[Edit and add two bullet list items to the end of the first bullet list; add a new paragraph just prior to Figure Annex B-1, and replace Figure Annex B-1]

- Root CA Public Key (optional): an updated Root CA Public Key that replaces the Root CA Public Key currently stored in the CM.
- Manufacturer Certificate(s) (optional): One or more X.509 compliant Manufacturer Certificate(s) that replaces the Manufacturer Certificates currently stored in the CM.

While the Root CA for the cable modem certificate chain currently serves as the Root CA for the Secure Software Download, the different Root CA may be used in the future. Therefore, the CM MUST NOT assume that the Manufacturer CVC and Co-signer CVC are issued by the Root CA for the cable modem certificate chain.

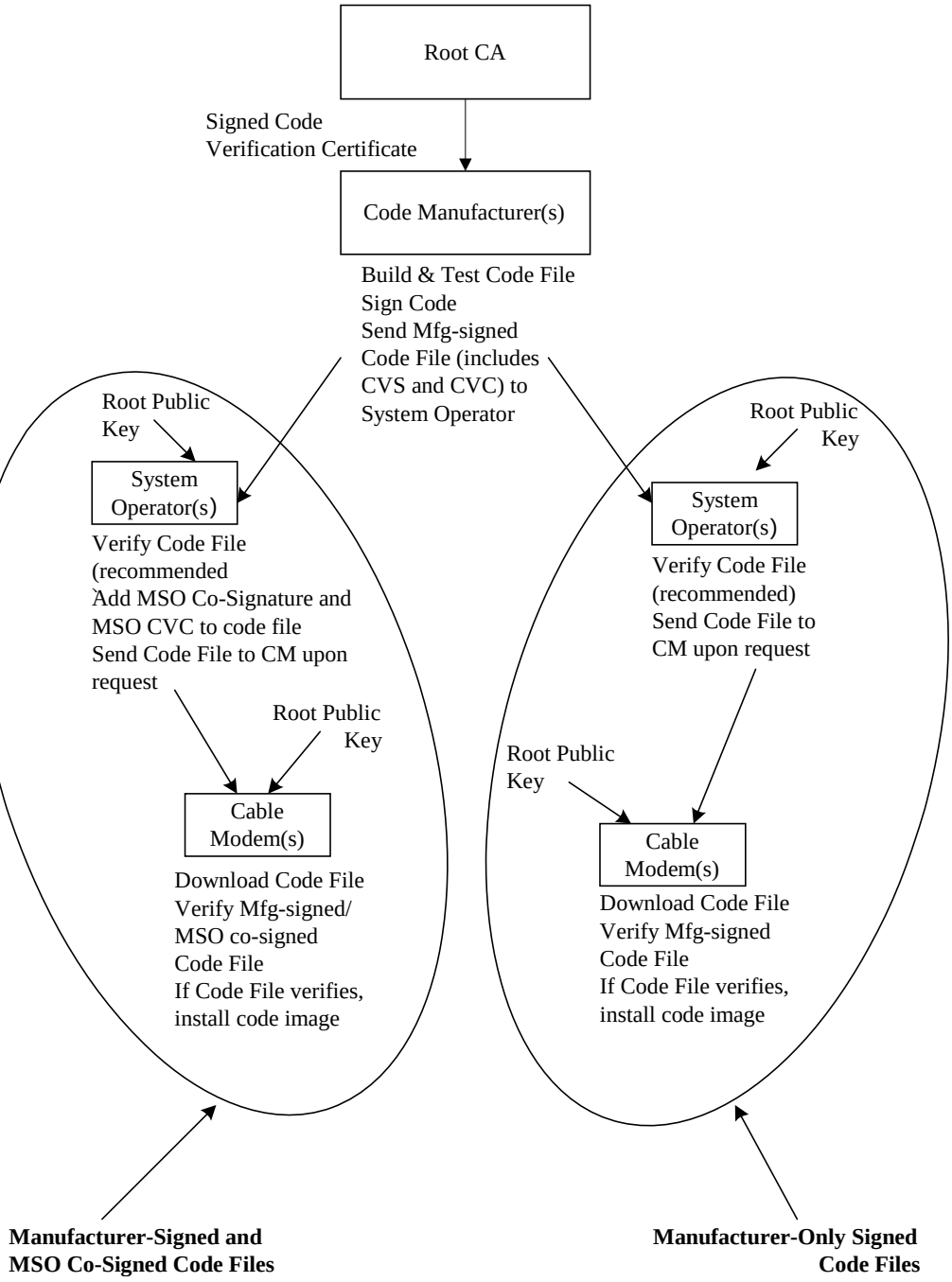


Figure Annex B-1. Typical Code Validation Hierarchy

B.O.B.3 Code Upgrade Requirements [edits as indicated.]

The following sections define requirements in support of the code upgrade verification process. All code upgrades MUST be prepared and verified as defined in this specification. All certified cable modems MUST verify code upgrades according to this specification, regardless of whether it is operating in a ~~J.112v 2 or J.112v2~~, J.112v 1, J.112v 2, or J.122, compliant mode. All J.112 Annex B ~~1.1~~v 2 and J.122 certified cable modems MUST verify code upgrades according to this specification regardless of whether Baseline Privacy is enabled or disabled.

B.O.B.3.1 Code File Requirements

[Edit and add text as indicated, delete entire Table Annex-B-2.]

5. optional Root CA Public Key for the CVC verification

6. optional Manufacturer Certificate(s)

The code file MUST comply with ~~the~~ [PKCS#7 ~~specification~~] and MUST be DER encoded. The code file MUST match the structure shown in Table B-1. An example is shown in Appendix I.

Table Annex-B-1. Code File Structure

Code File	Description
PKCS#7 Digital Signature{	
ContentInfo	
contentType	SignedData
SignedData()	~~Includes~~EXPLICIT signed-data content value; includes CVS and X.509 CVC
}	
SignedContent{	
~~Content~~ DownloadParameters {	~~Data ::=OCTET STRING (upgrade code image~~Mandatory TLV format (Type 28) defined in the section 7.2.2.28. (Length is zero if there is no sub-TLVs.)
RootCAPublicKey()	Optional TLV for the Root CA Public Key for CVC Verification, formatted according to the RSA-Public-Key TLV format (Type 4) defined in the section 7.2.2.4.
MfgCerts()	Optional TLV for one or more DER-encoded Manufacturer Certificate(s) each formatted according to the CA-Certificate TLV format (Type 17) defined in the section 7.2.2.17.
}	
CodeImage()	Upgrade code image
}	

~~If when downloading a manufacturer certificate, a manufacturer does not embed the certificate in the actual code image, the SignedContent field of the code file MAY be defined as shown in Table B-2. In this case,~~ If when downloading the Root CA Public Key and/or the Manufacturer Certificate as a part of the CM Code File, the Root CA Public Key and/or the Manufacturer CA Certificates ~~are~~MAY be contained in the RootCAPublicKey field and/or the MfgCerts field as specified in the Table Annex B-1 respectively, and separated from the actual cable modem code image contained in the CodeImage field.

This makes it possible to clearly discriminate the code image from other parameters in the code download file. This makes it possible to change the Root CA Public Key, the Manufacturer CA Certificates or SignedData parameters in the code download file without disrupting or changing the code image that the cable modem will receive. This allows one to verify that the code image has not changed even though the code download file changed because of a change in the Root CA Public Key, the Manufacturer CA Certificates or SignedData parameters.

~~Table Annex B-2. Optional Code File Structure~~

~~Code File~~	~~Description~~
~~PKCS#7 Digital Signature{~~	
~~Signed Data()~~	~~Includes CVS and X.509 CVC~~
~~}~~	
~~SignedContent{~~	
~~MfgCerts()~~	~~One or more DER-encoded Manufacturer Certificates each formatted according to the CA Certificate TLV format defined in section 4.2.2.17.~~
~~CodeImage()~~	~~Data ::= OCTET STRING (upgrade code image)~~
~~}~~	

B.O.B.3.1.1 PKCS#7 Signed Data

[edit the text as indicated below, note the correct renumbering of the Table reference (Annex B-3 to Table Annex-B-2).]

The software upgrade file will contain the information in a PKCS#7 Signed Data content type as shown below. Though maintaining compliance to [PKCS#~~7~~,7], the structure used by J.112 Annex B has been restricted in format to ease the processing a CM does to validate the signature. The PKCS#7 Signed Data MUST be DER encoded and exactly match the structure shown in Table B-~~3.~~2 except for any change in order required to DER encode (*e.g.*, the ordering of SET OF attributes). The CM SHOULD reject the PKCS#7 signature if the PKCS#7 Signed Data does not match the DER encoded structure represented in Table B-2.

B.O.B.3.1.1.1 Code Signing Keys

[Renumber table, replace text as indicated, and reformat column one (note: formatting (spacing) must be changed as shown.]

Table Annex B-~~3.~~2. PKCS#7 Signed Data

PKCS#7 Field	Description
Signed Data {	
version	version = 1
digestAlgorithmIdentifiers	SHA-1
contentInfo	
contentType	data (~~upgrade file follows~~SignedContent is concatenated at the end of the PKCS#7 structure)
certificates {	Code Verification Certification (CVC)
mfgCVC	REQUIRED for all code files
~~CableOperatorCVC~~msoCVC	OPTIONAL; required for Cable Operator co-signatures
} *end certificates*	
SignerInfo{	
MfgSignerInfo {	REQUIRED for all code files
version	version = 1
issuerAndSerialNumber	from the signer's certificate
issuerName	distinguished name of the certificate issuer
~~c~~CountryName	US
organizationalName	~~CableLabs Certified~~Data Over Cable Service Interface Specifications
organizationalUnitName	~~J.112 Annex B~~Cable Modems
commonName	~~J.112 Annex B~~DOCSIS Cable Modem Root Certificate Authority
certificateSerialNumber	from CVC; Integer, ~~8~~ size (1..20) octets
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	data; contentType of signedContent

signingTime	UTCTime (GMT), YYMMDDhhmmssZ
~~contentType~~	~~data; contentType of code image content~~
messageDigest	digest of the content ~~plus authenticated attributes~~as defined in [PKCS#7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end mfg signer info*	
MsoSignerInfo {	OPTIONAL; required for MSO co-signatures
version	version =1
issuerAndSerialNumber	from the ~~singer~~'signer'’s certificate
issuerName	distinguished name of the certificate issuer
~~c~~CountryName	US
organizationalName	~~CableLabs Certified~~Data Over Cable Service Interface Specifications
organizationalUnitName	~~J.112 Annex B~~Cable Modems
commonName	DOCSIS Cable Modem Root Certificate Authority
certificateSerialNumber	from CVC; Integer, ~~8~~ size (1..20) octets
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	data; contentType of signedContent
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
~~contentType~~	~~data; contentType of code image content~~
messageDigest	digest of the content ~~plus authenticated attributes~~as defined in [PKCS#7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end* ~~Cable Operator~~*mso signer info*	
} *end signer info*	
} *end signed data*	

B.O.B.3.1.1.2 Code Verification Certificate Format

[Edit and add text as indicated.]

The format used for the CVC is X.509 compliant. However, in this case, the X.509 structure has been restricted to ease the processing a CM does to validate the certificate and extract the public key used to verify the CVS. The CVC MUST be DER encoded~~.~~ and exactly match the structure shown in Table B-3 except for any change in order required to DER encode (*e.g.*, the ordering of SET OF attributes). The CM SHOULD reject the CVC if it does not match the DER encoded structure represented in Table B-3.

[Renumber table, replace text as indicated, and reformat column one (note: formatting (spacing) must be changed as shown.]

Table B-~~4.~~3. X.509 Compliant Code Verification Certificate

X.509 Certificate Field	Description
Certificate {	
tbsCertificate	
version	v3(2)
serialNumber	~~integer, 8~~ Integer, size (1..20) octets
signature	SHA-1 with RSA, null parameters
issuer	
countryName	US
organizationName	~~Cablelabs Certified~~Data Over Cable Service Interface Specifications
organizationalName	~~J.112 Annex B~~Cable Modems

commonName	~~J.112 Annex B~~DOCSIS Cable Modem Root Certificate Authority
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<country of subject company>
organizationName	<subject code-signing agent>
organizationalUnitName	J.112 Annex B
commonName	Code Verification Certificate
subjectPublicKeyInfo	
algorithm	RSA encryption, null parameters
subjectPublicKey	1024-bit, 1536-bit, or 2048-bit modulus
extensions	
extKeyUsage	
critical	true
keypurposeId	id-kp-codeSigning
signatureAlgorithm	SHA-1 with RSA, null parameters
signature Value	~~1024-bit modulus~~
} *end certificate*	

B.O.B.3.1.2 Signed Content

[Break existing first paragraph into two separate paragraphs. Add two new paragraphs at the end of the section.]

The signed content field of the code file ~~is the~~contains the code image and the download parameters field, which possibly contains two additional optional items - a DOCSIS Root CA Public key and Manufacturer Certificate.

The final code image is in a format compatible with the destination cable modem. In support of the PKCS#7 signature requirements, the code content is typed as data; *i.e.*, a simple octet string. The format of the final code image is not specified here and will be defined by each manufacturer according to their requirements.

Each manufacturer SHOULD build their code with additional mechanisms that verify an upgrade code image is compatible with the destination cable modem. The CM SHOULD NOT install the upgraded code image unless the code image has been verified as being compatible with the CM.

If included in the signed content field, the DOCSIS Root CA Public key is intended to replace the DOCSIS Root CA Public key currently stored in the CM. If the code download and installation specified in section B.3.5.1 is successful, then the CM MUST replace its currently stored DOCSIS Root CA Public key with the DOCSIS Root CA Public key received in the signed content field. This new DOCSIS Root CA Public key will then be used for subsequent CVC verification.

If included in the signed content field, the Manufacturer Certificate(s) is intended to replace the Manufacturer Certificate(s) currently stored in the CM. If the code download and installation specified in section B.3.5.1 is successful, then the CM MUST replace its currently stored Manufacturer Certificate(s) with the Manufacturer Certificate(s) received in the signed content field. The new Manufacturer Certificate(s) will then be sent to the CMTS during the subsequent BPI+ initialization.

B.O.B.3.2.2 Time Varying Controls

[Add the following paragraph at the end of the section.]

The values of codeAccessStart and cvcAccessStart corresponding to the cable modem's manufacturer MUST NOT decrease. The value of codeAccessStart and cvcAccessStart corresponding to the co-signing agent MUST NOT decrease as long as the co-signing agent does not change and the CM maintains that co-signer's time-varying control values.

B.O.B.3.3.2 Network Initialization

[Edit the last paragraph of the section.]

The manufacturer's set of these values MUST be stored in the CM's non-volatile memory and not lost when the CM's main power source is removed or during a CM reboot process. When a co-signer is assigned to the CM, the co-signer's set of these values MUST be stored in the CM's memory. The CM MAY retain these values in non-volatile memory that will not be lost when the CM's main power source is removed or during a CM reboot process. However, when assigning a CM a co-signing agent, the CVC is always in the configuration file. Therefore, ~~because the co-signer's control values will always be received in the configuration file, the CM~~ the CM will always receive the co-signer's control values during the initialization phase and is not required to store the co-signer's time-varying control values ~~in non-volatile memory; and is not required to retain the values~~ when main power is lost ~~and the CM goes through a power-up~~ or during a reboot process.

B.O.B.3.3.2.1 Processing the Configuration File CVC

[Edit step #2-4 as indicated.]

2. Check the CVC subject organization name~~:~~.

   If the CVC is a Manufacturer's CVC (Type 32) then:

   a. IF, the organizationName is identical to the cable modem's manufacturer name, THEN this is the manufacturer's CVC. In this case, the CM MUST verify that the manufacturer's CVC validity start time is greater-than or equal-to the ~~manufacturer~~manfacturer's cvcAccessStart value currently held in the CM.

   b) IF, the organizationName is not identical to the cable modem's manufacturer name, THEN this CVC MUST be rejected and the error logged.

   If the CVC is a Co-signer's CVC (Type 33) then:

   ~~b.~~a. IF, the organizationName is identical to the cable modem's current code co-signing agent, THEN this is the current co-signer's CVC and the CM MUST verify that the validity start time is greater-than or equal-to the co-signer's cvcAccessStart value currently held in the CM.

   ~~c.~~b. IF, the organizationName is not identical to ~~cable modem's manufacturer or~~the current code co-signing agent name, THEN after the CVC has been validated (and registration is complete) this subject organization name will become the CM's new code co-signing agent. The CM MUST NOT accept a code file unless it has been signed by the manufacturer, and co-signed by this code co-signing agent.

3. Validate the certificate signature using the root key held by the CM. Verification of the CVC signature will authenticate the source and validate trust in the CVC parameters.

4. Update the CM's current value of cvcAccessStart ~~and codeAccessStart values~~ corresponding to the CVC's subject organizationName (*i.e.*, manufacturer or code co-signing agent) with the validity start time value from the validated CVC. If the validity start time value is greater than the CM's current value of codeAccessStart, update the CM's codeAccessStart value with the validity start time value. The CM SHOULD discard any remnants of the CVC.

B.O.B.3.3.2.2 Processing the SNMP CVC

[Edit step #2-4 as indicated.]

2. Check the CVC subject organization name.

~~If the CVC is a Manufacturer's CVC (Type 32) then:~~

a. IF, the organizationName is identical to the cable modem's manufacturer name, THEN this is the manufacturer's CVC. In this case, the CM MUST verify that the manufacturer's CVC validity start time is greater-than ~~or equal-to~~ the manufacturer's cvcAccessStart value currently held in the CM.

b. IF, the organizationName is ~~not~~ identical to the cable modem's ~~manufacturer name, THEN this CVC MUST be rejected and the error logged.~~ current code co-signing agent, THEN this is a current co-signer's CVC and the validity start time MUST be greater-than the co-signer's cvcAccess Start value currently held in the CM.

~~If the CVC is a Co-signer's CVC (Type 33) then:~~

~~a. IF, the organizationName is identical to the cable modem's current code co-signing agent, THEN this is the current co-signer's CVC and the CM MUST verify that the validity start time is greater-than or equal-to the co-signer's cvcAccessStart value currently held in the CM.~~

~~b.~~c. IF, the organizationName is not identical to ~~current code co-signing agent name. THEN after the CVC has been validated (and registration is complete) this subject organization name will become the CM's new code co-signing agent. The CM MUST NOT accept a code file unless it has been signed by the manufacturer, and co-signed by this code co-signing agent~~ cable modem's manufacturer or current code co-signing agent name, THEN the CM MUST immediately reject this CVC.

3. Validate the certificate signature using the root key held by the CM. Verification of the signature will authenticate the certificate and confirm trust in the CVC's validity start time.

4. Update the current value of the subject's cvcAccessStart ~~and codeAccessStart~~ values with the validated CVC's validity start time value. If the validity start time value is greater than the CM's current value of codeAccessStart, update the CM's codeAccessStart value with the validity start value. All certificate parameters EXCEPT for the validity start time are no longer needed and SHOULD be discarded.

B.O.B.3.4.1 Certificate Authority (CA) Requirements

[Move text from the end of this section to the end of B.O.3.4.2]

~~To conserve storage space, the CM MAY internally represent the code co-signing agent's name in an alternate format as long as all information is maintained and the original format can be reproduced; e.g., as a 32-bit nonzero integer, with an integer value of 0 representing the absence of a code-signing agent.~~

B.O.B.3.4.2 Manufacturing Requirements

[Text moved from B.O.3.4.1 to the end of this section]

To conserve storage space, the CM MAY internally represent the code co-signing agent's name in an alternate format as long as all information is maintained and the original format can be reproduced; e.g., as a 32-bit nonzero integer, with an integer value of 0 representing the absence of a code-signing agent.

B.O.B.3.5.1 Cable Modem Code Verification Steps

[Edit first paragraph as indicated; Edit steps 3-5 as indicated.]

When downloading code the CM MUST perform the ~~steps as~~verification checks presented in this section. If any of the verification checks fail, or if any section of the code file is rejected due to invalid formatting, the CM MUST immediately halt the download process, log the error if applicable, remove all remnants of the process to that step, and continue to operate with its existing code. The verification checks can be made in any order, as long as all of the applicable checks presented in this section are made.

3. The CM MUST validate the certificate signature using the root key held by the CM. Verification of the signature will authenticate the source of the public code verification key (CVK) and confirm trust in the key. Once trust has been established in the manufacturer's CVK, the remaining certificate parameters EXCEPT for the validity start time are no longer needed and SHOULD be discarded.

4. The CM MUST verify the manufacturer's code file signature.

~~a. Once trust has been established in the manufacturer's CVK, the remaining certificate parameters EXCEPT for the validity start time are no longer needed and SHOULD be discarded.~~

a. The CM MUST perform a new SHA-1 hash over the SignedContent. If the value of the messageDigest doesn't match the new hash, the CM MUST consider the signature on the code file as invalid.

b. If the signature does not verify, all components of the code file (including the code image), and any values derived from the verification process MUST be rejected and SHOULD be immediately discarded.

5. If the manufacturer signature verifies and a co-signing agent signature is required~~.~~:

a. The CM MUST validate the co-signer's signature information by verifying that:

i) the co-signer's signature information is included in the code file~~.~~

ii) the PKCS#7 signingTime value is equal-to or greater-than the corresponding codeAccessStart value currently held in the CM~~.~~

iii) the PKCS#7 signingTime value is equal-to or greater-than the corresponding CVC validity start time~~.~~

iv) the PKCS#7 signingTime value is less-than or equal-to the corresponding CVC validity end time~~.~~

b. The CM MUST validate the co-signer's CVC, by verifying that:

i) the CVC subject organizationName is identical to the co-signer's organization name currently stored in the CM~~.~~'s memory~~.~~

ii) the CVC validity start time is equal-to or greater-than the cvcAccessStart value currently held in the CM for the corresponding subject organizationName~~.~~

iii) the extended key usage extension is in the CVC as defined in section II.3.1.1.2.

c. The CM MUST validate the certificate signature using the root key held by the CM. Verification of the signature will authenticate the source of the co-signer's public code verification key (CVK) and confirm trust in the key. Once trust has been established in the co-signer's CVK, the remaining certificate parameters EXCEPT for the validity start time are no longer needed and SHOULD be discarded.

d. The CM MUST verify the co-signer's code file signature.

e. The CM MUST perform a new SHA-1 hash over the SignedContent. If the value of the messageDigest doesn't match the new hash, the CM MUST consider the signature on the code file as invalid.

~~e.~~ f. If the signature does not verify, all components of the code file (including the code image), and any values derived from the verification process MUST be rejected and SHOULD be immediately discarded.

B.O.B.3.7 Error Codes

[Edit and add text as indicated.]

Error codes are defined to reflect the failure states possible during the code verification process. Description and usage guidelines for these error codes can be found in ~~[TBD~~Annex H of [SCTE DSS-02-06] or Annex G of [ANSI/SCTE 79-2 2002].

B.O.I.2 ~~Authorization~~Authentication Info

[Edit and add text as indicated including the section title.]

The CM sends the following ~~Authorization~~Authentication Info message:

0c 01 02 94	Auth Info header
11 02 91	CA Certificate header
30 82 02 8d 30 82 01 f6 . . . 81 87 19 61 72 20 19 1e	CA Certificate

B.O.I.2.1 CA Certificate details
[edits as indicated.]

Some of the fields in this example are the same in all CA certificates. These fields are:

- version: v3
- signature: SHA-1 with RSA, null parameters
- subject first organizational unit name: ~~"J.112 Annex B"~~"DOCSIS"
- public key algorithm type: RSA encryption, null parameters
- public key exponent: 3-octet integer, value 0x10001
- signature algorithm: SHA-1 with RSA, null parameters

This is an example of a self-signed CA certificate. The issuer name and the subject names are identical. In this example, the matching name fields are:

- country name: "US"
- organization name: "Nortel"
- first organizational unit name: ~~"J.112 Annex B"~~"DOCSIS"
- second organizational unit name: "Building 1, Andover MA"
- common name: "Nortel Cable Modem Root Certificate Authority"

B.O.I.3.1 CM Certificate details

[Edit text in the 12th row, second column as follows; edit bullet lists as indicated.]

~~validityheader~~validity header

Some of the fields in this example are the same for all CM Certificates. These fields are:

- version: v3
- signature: SHA-1 with RSA, null parameters
- issuer first organizational unit name: ~~"J.112 Annex B"~~"DOCSIS"
- public key algorithm type: RSA encryption, null parameters
- public key exponent: 3-octet integer, value 0x10001
- signature algorithm: SHA-1 with RSA, null parameters

The issuer name of the CM certificate matches the subject name of the CA certificate. In this example, the matching issuer-name fields are:

- country name: "US"
- organization name: "Nortel"
- first organizational unit name: ~~"J.112 Annex B"~~"DOCSIS"
- second organizational unit name: "Building 1, Andover MA"
- common name: "Nortel Cable Modem Root Certificate Authority"

B.O.I.6.1 ~~EK~~TEK encryption details

[Edit section title as indicated.]

B.O.II.2 BPI/BPI+ Interoperability Requirements

[Edits begin at step #2, modify text as indicated.]

2. Cable Modem:

a. CM BPI: Baseline Privacy with 56-bit DES, and either a 768 or 1024 bit public key modulus.

b. CM BPI – 40bit: Baseline Privacy with 40-bit DES, and either a 768 or 1024 bit public key modulus. DES can only operate in 40-bit mode.

As defined in this specification, Baseline Privacy Plus introduces two additional unit types.

1. CMTS BPI+: Baseline Privacy Plus with 56-bit DES, and will accept both a 768 and 1024 bit public key modulus.

~~•~~ 2. CM BPI+: Baseline Privacy Plus with 56-bit DES, and a 1024 bit public key modulus.

The CMTS and the CM negotiate the BPI/BPI+ compatible mode using the Privacy Support Modem Capability TLV (type 5.6) in the REG-REQ and REG-RSP messages. The requirements for BPI/BPI+ interoperability are:

a. A CMTS MUST accept public keys with a modulus of both 768 and 1024 bits from a CM during authorization.

~~According to the interoperability requirements of [J.112 Annex B] and this specification, a CMTS with Baseline Privacy Plus MUST be capable of falling back into a Baseline Privacy compatible mode of operation.~~

b. If a CM with Baseline Privacy Plus (CM BPI+) is provisioned with a DOCSIS 1.0 style configuration file, the CM sets the Privacy Support Modem Capability TLV (type 5.6) to either BPI Support (0) or BPI+ Support (1) depending on its capability in that situation (cf. [DOCSIS1], section G.2.1, or [DOCSIS9], Section G.1.1).

c. When a CMTS with Baseline Privacy Plus (CMTS BPI+) ~~is operating in a system with a CM that has only Baseline Privacy capability~~ receives the Privacy Support Modem Capability TLV set to BPI Support (type 5.6, value 0) or no type 5.6 TLV in the REG-REQ message from the CM, the CMTS MUST fall back into a Baseline Privacy compatible mode of operation [DOCSIS2] for communications with that CM.

d. When a CMTS with Baseline Privacy Plus is operating in a system that supports both BPI and BPI+ CMs, the TFTP server MUST include ~~both J.112 Annex B v1 and J.112 Annex B v2 configuration files to deliver the appropriate BPI or BPI+ settings to each CM.~~ the following two kinds of configuration files:

- Configuration file with all of the BPI parameters (type 17.1 through 17.7) for the CMs provisioned to operate in BPI mode, and
- Configuration file with all of or a part of the BPI+ parameters for the CMs provisioned to operate in BPI+ mode.

~~According to the interoperability requirements of [J.112 Annex B] and this specification, a CM with~~

~~Baseline Privacy Plus MUST be capable of falling back into a Baseline Privacy compatible mode of operation before attempting authorization.~~

e) When a CM with Baseline Privacy Plus (CM BPI+) ~~is operating in a system with a CMTS that has only Baseline Privacy capability, it~~ receives the Privacy Support Modem Capability TLV set to BPI Support (type 5.6, value 0) or no type 5.6 TLV in the REG-RSP message from the CMTS, the CM MUST fall back into a Baseline Privacy mode of operation [DOCSIS2] to communicate with the CMTS.

Note that, as specified in Appendix I to Annex O of this document, the DOCSIS 1.1 CM always verifies downloaded operational software as specified in Appendix I regardless of the Privacy Support setting (type 5.6) in the REG-RSP message and the Privacy Enable setting (type 4.7 or 29) in the CM configuration file.

Table Appendix II-1. BPI/BPI+ Interoperability Matrix

	CM BPI	**CM BPI – 40bit**	**CM BPI+**
CMTS BPI	Domestic BPI configuration. 768 or 1024-bit RSA modulus.	768 or 1024 bit RSA modulus. CMTS software zeros TEK bits to 40-bit standard	CM falls back into BPI mode with 1024-bit RSA modulus
CMTS BPI-40bit	768 or 1024 bit RSA modulus. CMTS software zeros TEK bits to 40-bit standard	768 or 1024 bit RSA modulus. All 40-bit compatibility handled by MAC chips.	CM falls back into BPI mode with 1024-bit RSA modulus. CMTS software zeros TEK bits to 40-bit standard
CMTS BPI+	CMTS falls back into BPI mode. 768 or 1024-bit RSA modulus.	768 or 1024 bit RSA modulus. CMTS software zeros TEK bits to 40-bit standard	Full BPI+ mode or BPI mode depending on configuration file and CMTS setting. 1024-bit RSA modulus.

Document comparison done by DeltaView on Monday, October 28, 2002 10:09:55

Input:	
Document 1	Rec_J.112-AnnexB-(2001).doc
Document 2	SP-RFIv1.1-I09-020830.doc
Rendering set	Standard

Document comparison done by DeltaView on Monday, November 04, 2002 08:45:58

Input:	
Document 1	Rec_J.112-AnnexB.O-(2001).doc
Document 2	SP-BPI+-I09-020830.doc
Rendering set	Standard

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Inserted cell	
Deleted cell	

Moved cell	