UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.112

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Anexo B
(03/2001)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Sistemas interactivos para distribución de televisión digital

---

Sistemas de transmisión para servicios interactivos de televisión por cable

Anexo B: Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia

Recomendación UIT-T J.112 – Anexo B

RECOMENDACIONES UIT-T DE LA SERIE J

REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	J.90–J.99
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	**J.110–J.129**
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159
IPCablecom	J.160–J.179
Varios	J.180–J.199
Aplicación para televisión digital interactiva	J.200–J.209

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T J.112

Sistemas de transmisión para servicios interactivos de televisión por cable

ANEXO B

Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia

Resumen

Este anexo define las especificaciones de interfaces de radiofrecuencia para sistemas de datos por cable de alta velocidad.

Se incluyen dos opciones en la tecnología de la capa física. Una opción se basa en la distribución en sentido descendente de la televisión multiprogramas empleada en Norteamérica, que utiliza una disposición de canales de 6 MHz y soporta transmisiones en sentido ascendente en la región entre 5 MHz y 42 MHz. La otra opción se basa en la distribución de televisión multiprogramas europea que, soporta transmisiones en sentido ascendente en la región entre 5 MHz y 65 MHz.

Orígenes

El anexo B a la Recomendación UIT-T J.112, preparado por la Comisión de Estudio 9 (2001-2004) del UIT-T, fue aprobado por el procedimiento de la Resolución 1 de la AMNT el 9 de marzo de 2001.

El anexo O "*Protección para la implementación de J.112, anexo B*", que era informativo cuando el anexo B de la Rec. J.112 fue aprobado en marzo de 2001, ha sido modificado en normativo por la enmienda 1 (02/2002) del anexo B de la Rec. UIT-T J.112.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

Página

Recomendación UIT-T J.112

Sistemas de transmisión para servicios interactivos de televisión por cable

ANEXO B

Especificaciones de interfaces de servicios de datos por cable:
Especificación de la interfaz de radiofrecuencia

B.1 Alcance y finalidad

B.1.1 Alcance

El presente anexo B define las especificaciones de interfaces de radiofrecuencia para sistemas de datos por cable de alta velocidad.

Existen diferencias entre los procedimientos de planificación del espectro del sistema de cable adoptados por las diferentes redes en el mundo. Por ello, se incluyen aquí dos opciones, igualmente prioritarias y no necesariamente interoperables, para la tecnología de la capa física. Una de estas opciones se basa en la distribución en sentido descendente de la televisión multiprogramas empleada en Norteamérica, que utiliza una disposición de canales de 6 MHz, y soporta transmisiones en sentido ascendente en la región entre 5 MHz y 42 MHz. La otra opción tecnológica se basa en la distribución de televisión multiprogramas europea, que soporta transmisiones en sentido ascendente en la región entre 5 MHz y 65 MHz. Aunque ambas opciones poseen el mismo estatus, la primera fue documentada antes que la segunda, que se introdujo después como una enmienda, con el resultado de que la estructura documental que no refleja esta igualdad de prioridades. La primera opción se define en B.4, B.6, B.7 y en B.C.1.1.1/anexo B.G, mientras que la segunda se define instituyendo el contenido de esas cláusulas por el del anexo B.N. De igual manera, las referencias [UIT-T J.83-B], [NCTA] y [SMS] se aplican solamente a la primera opción, y la referencia [EN 300 429] solamente a la segunda. La conformidad con el presente anexo B requiere solamente del acuerdo con lo estipulado en una de estas dos implementaciones, no con ambas. No se requiere que el equipo construido para una opción interopere con el equipo construido para la otra.

Estas tecnologías opcionales para la capa física permiten a los operadores tener cierta flexibilidad dentro de cualquier plan de frecuencias, así como en materia de requisitos de compatibilidad electromagnética (EMC, *electromagnetic compatibility*) y requisitos de seguridad que sean obligatorios para su zona de operación. Por ejemplo, la opción de transmisión en sentido descendente a 6 MHz, definida por B.4, B.G y B.7, podría ser utilizada dentro de un plan de frecuencias de 8 MHz. La conformidad con el plan de frecuencias y los requisitos de EMC no está cubierta por este anexo B y compete a la responsabilidad del operador. A este respecto, las referencias [FCC15], [FCC76] y [EIA 542] lo son para Norteamérica y las referencias [EN 50081-1], [EN 50082-1], [EN 50083-2], [EN 50083-7] y [EN 50083-10], lo son pertinentes para la Comunidad Europea.

Es preciso que la opción definida en B.4, B.6 y B.7, en el anexo B.G, y en B.C.1.1.1 sea retrocompatible con una versión anterior de esta tecnología [DOCSIS9], mientras que la opción del anexo B.N no fue incluida en [DOCSIS9] y por lo tanto no se requiere su retrocompatibilidad con versiones anteriores.

Cualquier referencia en el presente anexo B a la transmisión de televisión por el canal de ida que no sea coherente con la referencia [EN 300 429] queda fuera del alcance normativo, al ser dicha referencia la única norma utilizada en las aplicaciones europeas de distribución por cable de televisión multiprogramas.

Los requisitos de seguridad quedan fuera del alcance del presente anexo B. Las normas de seguridad para las aplicaciones europeas son publicadas por el CENELEC.

NOTA 1 – Las referencias [EN 60950] y [EN 50083-1] son ejemplos de normas de seguridad de productos del tipo CENELEC.

NOTA 2 – Véase la referencia [EG 201 212] para las categorías de seguridad de interfaces del CENELEC.

B.1.2 Convenios

A lo largo del presente anexo B, las palabras utilizadas para señalar la importancia de requisitos particulares son:

"DEBE(N)" Esta palabra, o el adjetivo "REQUERIDO", significa que el elemento es un requisito absoluto de este anexo B.

"NO DEBE(N)" Esta expresión significa que el elemento es una prohibición absoluta de este anexo B.

"DEBERÍA(N)" Esta palabra, o el adjetivo "RECOMENDADO", significa que, en determinadas circunstancias, pueden existir motivos válidos para hacer caso omiso de este elemento, pero que deberían tenerse en cuenta todas las explicaciones y ponderar cuidadosamente el caso antes de optar por una vía diferente.

"NO DEBERÍA(N)" Esta expresión significa que pueden existir motivos válidos en determinadas circunstancias en las que el comportamiento indicado sea aceptable o incluso de utilidad, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de implementar cualquier comportamiento descrito con esta etiqueta.

"PUEDE(N)" Esta palabra, o el adjetivo "OPCIONAL", significa que el elemento es verdaderamente opcional. Un vendedor puede optar por incluir el elemento porque así se exige en un determinado mercado o porque mejora el producto, por ejemplo; otro vendedor puede omitir el mismo elemento.

El resto del texto es descriptivo o explicativo.

B.1.3 Antecedentes

B.1.3.1 Objetivos del servicio

A los operadores de cable les interesa instalar sistemas de comunicaciones de datos, basados en paquetes de alta velocidad, en sistemas de televisión por cable, capaces de soportar una amplia gama de servicios. Entre los servicios objeto de atención por parte de los operadores de cable figuran el servicio de telefonía por paquetes, el servicio de videoconferencia, el servicio equivalente de retransmisión de tramas/T1, y muchos otros. Por ello, se ha decidido preparar una serie de especificaciones de interfaces que permitan definir, diseñar, desarrollar e instalar sistemas de datos por cable lo antes posible de manera uniforme, coherente, abierta, no patentada e interoperable con base en múltiples vendedores.

El servicio que se desea prestar permitirá la transferencia bidireccional transparente de tráfico de protocolo Internet (IP, *Internet protocol*), entre la cabecera del sistema de cable y las posiciones de los clientes, por una red de cable totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC, *hybrid-fiber/coax*). Esto se muestra en forma simplificada en la figura B.1-1.

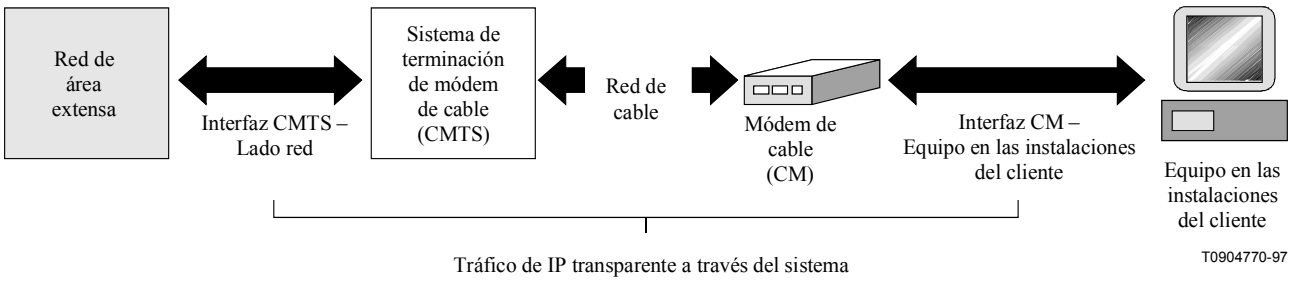


Figura B.1-1/J.112 – Tráfico de IP transparente a través del sistema de datos por cable

El trayecto de transmisión por el sistema de cable lo realiza en la cabecera un sistema de terminación de módem de cable (CMTS, *cable modem termination system*) y, en la posición de cada cliente, un módem de cable (CM, *cable modem*). En la cabecera (o centro de distribución), la interfaz con el sistema de datos por cable se denomina interfaz sistema de terminación de módem de cable – lado red (CMTS-NSI, *cable modem termination system – network side interface*) y se especifica en [DOCSIS3]. En las posiciones de los clientes, la interfaz se llama interfaz módem de cable – CPE (CMCI, *cable modem to CPE interface*) y se especifica en [DOCSIS4]. Lo que se pretende es que los operadores transfieran de manera transparente tráfico de IP entre estas interfaces incluyendo, pero sin limitarse a ello, diagramas DHCP, e ICMP y direccionamiento de grupo IP (radiodifusión y multidifusión).

B.1.3.2 Arquitectura de referencia

En la figura B.1-2 se muestra la arquitectura de referencia para los servicios e interfaces de datos por cable.

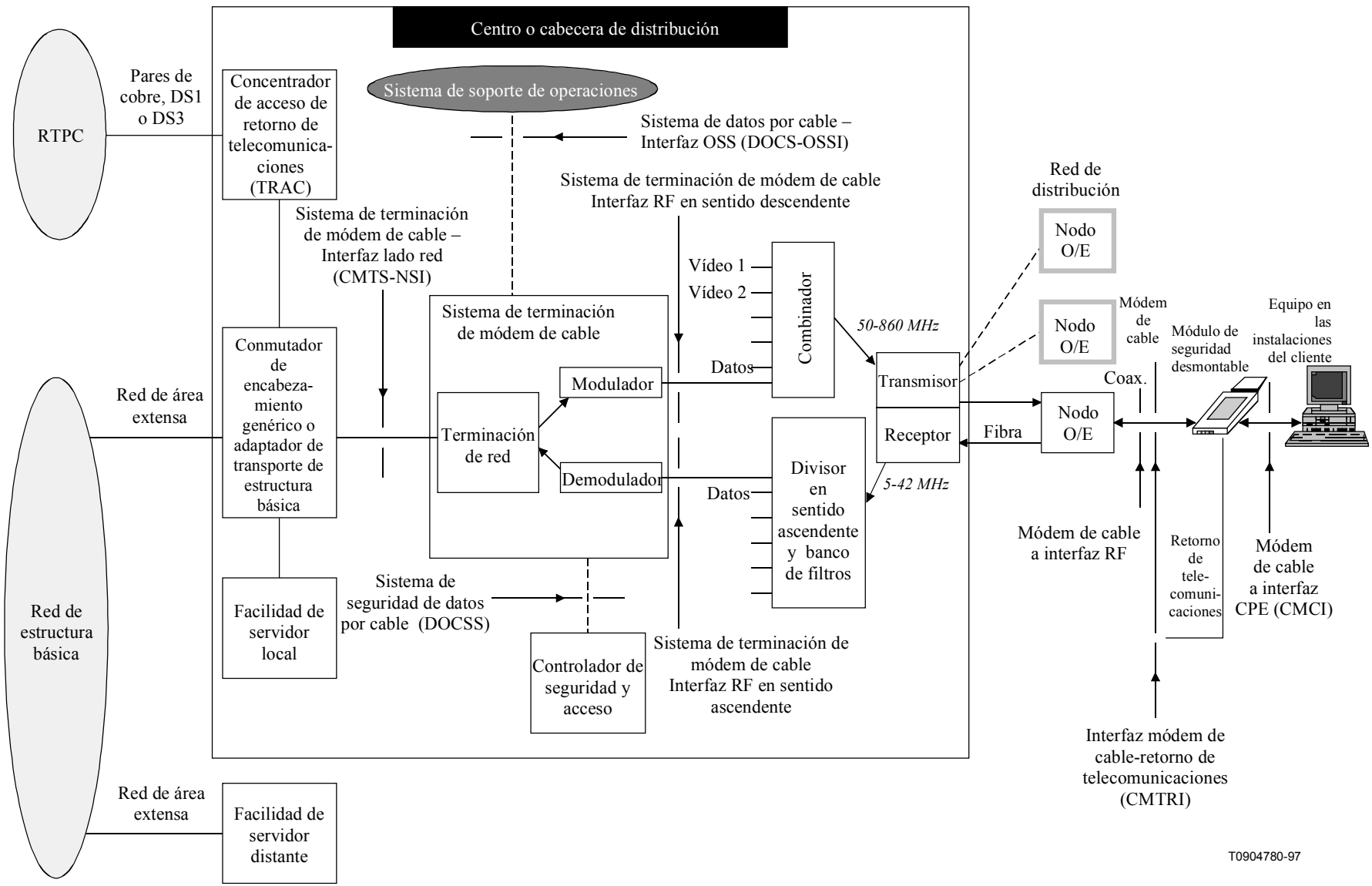


Figura B.1-2/J.112 – Arquitectura de referencia de datos por cable

B.1.3.3 Categorías de especificación de interfaz

La arquitectura de referencia básica de la figura B.1-2 entraña cuatro categorías de interfaz.

Interfaces de datos – Se trata de la CMCI [DOCSIS4] y la CMTS-NSI [DOCSIS3], lo que corresponde respectivamente a la interfaz módem de cable-equipo en las instalaciones del cliente (CPE, *customer premises equipment*) (por ejemplo, entre el computador del cliente y el módem del cable), y la interfaz sistema de terminación de módem de cable-lado red entre el sistema de terminación del módem del cable y la red de datos.

Interfaces de sistemas de soporte de operaciones – Se trata de las interfaces de la capa de gestión de elementos de red entre los elementos de red y el sistema de soporte de operaciones (OSS, *operations support system*) de alto nivel que soportan los procesos empresariales básicos, y están documentadas en [DOCSIS5].

Interfaz de retorno telefónico – CMTRI – Se trata de la interfaz entre el módem de cable y un trayecto de retorno telefónico para utilizar en los casos en que no se proporcione el trayecto de retorno o no esté disponible vía la red de cable, y está documentada en [DOCSIS6].

Interfaces RF – Las interfaces RF definidas en este anexo B son las siguientes:

- Interfaz entre el módem de cable y la red de cable.
- Interfaz entre el CMTS y la red de cable, en sentido descendente (tráfico hacia el cliente).
- Interfaz entre el CMTS y la red de cable, en sentido ascendente (tráfico procedente del cliente).

Requisitos de seguridad

La seguridad de datos por cable básica se define en [DOCSIS8].

NOTA – Esta arquitectura muestra solamente el plan de frecuencias norteamericano y no es normativa para las aplicaciones europeas. Para su aplicabilidad véase B.1.1.

B.1.3.3.1 Documentos de la interfaz de servicios de datos por cable

A continuación se da una lista de los documentos de la familia de especificaciones de interfaces de servicios de datos por cable. Para las actualizaciones, consúltese URL http://www.cablemodem.com.

Designación	Título
SP-CMCI	Especificación de la interfaz entre el módem del cable y el equipo en las instalaciones del cliente
SP-CMTS-NSI	Especificación de la interfaz entre el sistema de terminación del módem del cable y el lado red
SP-CMTRI	Especificación de la interfaz entre el módem del cable y el retorno telefónico
SP-OSSI	Especificación de la interfaz del sistema de soporte de operaciones
SP-RFI	Especificación de la interfaz de radiofrecuencia
SP-BPI+	Especificación de la interfaz Plus de privacidad básica

Claves para la designaciones

SP Especificación

TP Plan de pruebas – Un documento que incluye procedimientos de pruebas para validar la conformidad, interoperabilidad o idoneidad de una especificación.

TR Informe técnico (Proporciona un contexto a efectos de comprensión y aplicación de la especificación o ideas iniciales sobre posibles características futuras).

B.1.3.4 Declaración de compatibilidad

Esta cláusula se aplica solamente a la primera opción, tal como se define en B 1.1.

El presente anexo B especifica una interfaz, a la que se alude normalmente como DOCSIS 1.1, que es una extensión de la interfaz especificada en el [DOCSIS9], conocida como DOCSIS 1.0. Estas extensiones son completamente compatibles, tanto hacia adelante como hacia atrás, con la anterior versión de J.112 anexo B. Los CM conformes con la DOCSIS 1.1 deben interoperar sin problemas con los CMTS de la DOCSIS 1.0. Los CMTS conformes con la DOCSIS 1.1 DEBEN soportar sin incidencia alguna los CM del DOCSIS 1.0.

Véase el anexo B.G para más informaciones sobre interfuncionabilidad.

B.2 Referencias

Las siguientes Recomendaciones y otras referencias contienen disposiciones que, por referencia en el presente texto, constituyen disposiciones de este anexo B.

- Las referencias son específicas (es decir, identificadas por la fecha de publicación, el número de edición, el número de la versión, etc.) o no específicas.
- En el caso de una referencia específica, no se aplican las revisiones posteriores.
- En el caso de una referencia no específica se aplica la última versión.

[CableLabs1] CableLabs1, *Two-Way Cable Television System Characterization*, Cable Television Laboratories, Inc., 12 de abril de 1995.

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

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

[DOCSIS3] Data-Over-Cable Service Interface Specifications, Cable Modem Termination System – Network Side Interface Specification, SP-CMTS-NSII01-960702.

[DOCSIS4] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, SP-CMCI-I04-000714.

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

[DOCSIS6] Data-Over-Cable Service Interface Specifications, Cable Modem Telephony Return Interface Specification, SP-CMTRI-I01-970804.

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

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

[EIA 542] EIA Standard 542 (1997), *Cable Television Channel Identification Plan.*

[EN 50081-1] EN 50081-1, *Electromagnetic compatibility – Generic emission standard – Part 1: Residential, commercial and light industry.*

[EN 50082-1] EN 50082-1, *Electromagnetic compatibility – Generic immunity standard; Part 1: Residential, commercial and light industry.*

[EN 50083-2] EN 50083-2, *Cabled distribution systems for television and sound signals – Part 2: Electromagnetic compatibility for equipment.*

[EN 50083-7] EN 50083-7, *Cabled distribution systems for television and sound signals – Part 7: System performance.*

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

[EN 60950] EN 60950, *Safety of information technology equipment.*

[EN 50083-1] EN 50083-1, *Cabled distribution systems for television and sound signals – Part 1: Safety requirements.*

[EG 201 212] ETSI EG 201 212, *Electrical safety; Classification of interfaces for equipment to be connected to telecommunication networks.* (This document is also available from CENELEC as ROBT-002.)

[EN 300 429] ETSI EN 300 429, *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems.*

[FCC15] Code of Federal Regulations, Title 47, Part 15, *Radio frequency devices* (Octubre de 1998).

[FCC76] Code of Federal Regulations, Title 47, Part 76, *Cable televison service* (Octubre de 1998).

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

[IEEE 802.1Q] IEEE 802.1Q (1998), *IEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.*

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

[CEI-60169-24] CEI-60169-24 (1991), *Radio-frequency connectors – Part 24: Radio-frequency coaxial connectors with screw coupling, typically for use in 75 ohm cable distribution systems (Type F).*

[ISO 8825] ISO 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

[ISO/CEI 8802-2] ISO/CEI 8802-2:1994 (IEEE Std 802.2:1994), *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control.*

[ISO/CEI 8802-3] ISO/CEI 8802-3:1996 (IEEE Std 802.3:1996), *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical sublayer specifications.*

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

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

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

[UIT-T H.222.0] UIT-T H.222.0 (1995) | ISO/CEI 13818-1:1996, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas*.

[UIT-T J.83-B] UIT-T J.83 (1997) Anexo B, *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable*.

[UIT-T X.25] UIT-T X.25 (1993), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados*.

[UIT-T Z.100] UIT-T Z.100 (1999), *Lenguaje de especificación y descripción*.

[NCTA] NCTA Recommended Practices for Measurements on Cable Television Systems, *National Cable Television Association,* Washington DC, 2nd Edition, revised October, 1993.

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

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

[RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[RFC 826] IETF RFC 826 (1982), *Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet hardware.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[RFC 3046] RFC 3046 (2001), *DHCP Relay Agent Information Option.*

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

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

B.3 Definiciones y abreviaturas

B.3.1 Definiciones

En este anexo B se definen los términos siguientes.

B.3.1.1 flujo de servicio activo: Flujo de servicio admitido desde el CM hacia el CMTS, que está disponible para la transmisión de paquetes.

B.3.1.2 protocolo de resolución de direcciones (ARP, *address resolution protocol*): Protocolo del IETF para convertir direcciones de red en direcciones Ethernet de 48 bits.

B.3.1.3 flujo de servicio admitido: Flujo de servicio, ya sea previsto o señalado dinámicamente, que ha sido autorizado y para el cual se han reservado recursos pero que no está activo.

B.3.1.4 American National Standards Institute (ANSI): Organismo de normalización de Estados Unidos.

B.3.1.5 modo de transferencia asíncrono (ATM, *asynchronous transfer mode*): Protocolo para la transmisión de una diversidad de señales digitales que utilizan células uniformes de 53 octetos.

B.3.1.6 módulo de autorización: Módulo abstracto con el cual el CMTS puede ponerse en contacto para autorizar los flujos de servicio y los clasificadores. El módulo de autorización indica al CMTS si un CM demandante está autorizado a recibir los recursos que pide.

B.3.1.7 disponibilidad: En sistemas de televisión por cable, disponibilidad es la relación a largo plazo entre el tiempo efectivo de funcionamiento del canal de RF y el tiempo programado de funcionamiento del canal de RF (expresado como valor porcentual) y se basa en un supuesto con respecto a la tasa de errores en los bits (VER, *bit error rate*).

B.3.1.8 diagrama de atribución de anchuras de banda: El mensaje de gestión MAC que utiliza el CMTS para atribuir oportunidades de transmisión a los CM.

B.3.1.9 unidad de datos de protocolo puente (BPDU, *bridge protocol data unit*): Mensaje de protocolo de árbol abarcante, según se define en [RFC 1350].

B.3.1.10 dirección de difusión: Dirección de destino predefinida que indica el conjunto de todos los puntos de acceso del servicio de red de datos.

B.3.1.11 ráfaga de segundo con errores: Cualquier segundo con error que contiene al menos 100 errores.

B.3.1.12 módem de cable (CM, *cable modem*): Modulador-demodulador en las instalaciones del abonado a utilizar en comunicaciones de datos en un sistema de televisión por cable.

B.3.1.13 sistema de terminación de módem de cable (CMTS, *cable modem termination system*): Sistema de terminación, ubicado en la cabecera o centro de distribución de un sistema de televisión por cable, que proporciona una funcionalidad complementaria a los módems de cable para hacer posible la conectividad de datos en una red de área extensa.

B.3.1.14 sistema de terminación de módem de cable – interfaz del lado red (CMTS-NSI, *cable modem termination system – network side interface*): Interfaz, definida en [DOCSIS3], entre un CMTS y el equipo en su lado red.

B.3.1.15 interfaz módem de cable, equipo en las instalaciones del cliente (CMCI, *cable modem to CPE interface*): Interfaz, definida en [DOCSIS4], entre un módem de cable (CM) y un equipo en las instalaciones del cliente (CPE).

B.3.1.16 modulación por zumbido de portadora: Magnitud cresta a cresta de la distorsión de amplitud relativa al nivel de la señal portadora de RF debida a la frecuencia fundamental y a las armónicas de orden inferior de la frecuencia de alimentación.

B.3.1.17 relación portadora/ruido (C/N o CNR, *carrier-to-noise ratio*): Cuadrado de la relación entre el valor eficaz de la tensión de la portadora de RF con modulación digital y el valor eficaz de la tensión de ruido aleatorio continuo en la anchura de banda de medición definida. (Si no se especifica explícitamente, la anchura de banda de medición es la velocidad de símbolos de la modulación digital; para el vídeo es de 4 MHz.)

B.3.1.18 clasificador: Conjunto de criterios utilizados para el emparejamiento de paquetes, de acuerdo con los campos de paquetes de TCP, UDP, IP, LLC, y/o 802.1P/Q. Un clasificador hace corresponder cada paquete a un flujo de servicio. Un clasificador en sentido descendente es utilizado por el CMTS para asignar paquetes a los flujos de servicio en ese sentido. Un clasificador en sentido ascendente es usando por el CM para asignar paquetes a los flujos de servicio en el mismo sentido.

B.3.1.19 batido compuesto de segundo orden (CSO, *composite second order beat*): Cresta del nivel medio de productos de distorsión debidos a no linealidades de segundo orden en equipos de sistema por cable.

B.3.1.20 batido compuesto triple (CTB, *composite triple beat*): Cresta del nivel medio de los componentes de distorsión debidos a las no linealidades de tercer orden en equipos de sistemas por cable.

B.3.1.21 módem de cable controlado por un CPE (CCCM, *CPE controlled cable modem*): Véase la especificación de la interfaz entre un módem de cable y un equipo en las instalaciones del cliente (CMCI, *cable modem to customer premise equipment interface*) de DOCSIS.

B.3.1.22 modulación cruzada: Forma de distorsión de la señal de televisión en la que la modulación de uno o más canales de televisión afecta a otro u otros canales de televisión.

B.3.1.23 cliente: Véase usuario de extremo.

B.3.1.24 equipo en las instalaciones del cliente (CPE, *customer premises equipment*): Equipo en las instalaciones del usuario de extremo; PUEDE ser suministrado por el usuario de extremo o por el proveedor de servicio.

B.3.1.25 capa de enlace de datos: Capa 2 en la arquitectura de interconexión de sistemas abiertos (OSI); capa que proporciona servicios para transferir datos por el enlace de transmisión entre sistemas abiertos.

B.3.1.26 centro de distribución: Sitio en una red de televisión por cable que efectúa las funciones de cabecera para los clientes de su área inmediata, y que recibe parte o la totalidad de su material de programas de televisión de una cabecera principal ubicada en la misma área metropolitana o regional.

B.3.1.27 sentido ver; sentido descendente: En televisión por cable, sentido de transmisión de la cabecera al abonado.

B.3.1.28 cable de bajada: Cable coaxial que se conecta a una residencia o lugar de servicio desde un acoplador direccional (derivación) en el cable alimentador coaxial más cercano.

B.3.1.29 protocolo dinámico de configuración de ordenador principal (DHCP, *dynamic host configuration protocol*): Protocolo Internet utilizado para asignar direcciones de capa de red (IP).

B.3.1.30 gama dinámica: Relación entre la mayor potencia de señal que se puede transmitir por un sistema de transmisión analógico multicanal sin exceder la distorsión u otros límites de la calidad de funcionamiento, y la menor potencia de señal que se puede utilizar sin superar los límites de ruido, tasa de errores u otros límites de la calidad de funcionamiento.

B.3.1.31 Alliance de Industrias Electrónicas (EIA, *Electronic Industries Alliance*): Organización de participación voluntaria de fabricantes que, entre otras actividades, prepara y publica normas.

B.3.1.32 usuario de extremo: Persona, organización o sistema de telecomunicaciones que tiene acceso a la red para comunicarse a través de los servicios prestados por ésta.

B.3.1.33 notificación de cambio de ingeniería (ECN, *engineering change notice*): La etapa final en el procedimiento de cambio de las especificaciones.

B.3.1.34 orden de cambio de ingeniería (ECO, *engineering change order*): La segunda etapa en el procedimiento de cambio de las especificaciones. La DOCSIS sitúa ECO en la tabla EC del sitio Internet y la página de ECO (indicando la fecha límite de comentarios ECO). La DOCSIS publica un anuncio de ECO en las listas de correo del grupo de trabajo y de los anuncios DOCSIS (con una indicación de la fecha límite de comentarios ECO).

B.3.1.35 petición de cambio de ingeniería: (**ECR, *engineering change request***) La primera etapa en el procedimiento de cambio de las especificaciones. La DOCSIS produce un número de ECR, y lo sitúa a la tabla EC del sitio Internet y la página de ECR. La DOCSIS envía la ECR a la lista de correo del grupo de trabajo del área del tema (y al autor).

B.3.1.36 segundo con errores: Cualquier intervalo de un segundo que contiene al menos un bit erróneo.

B.3.1.37 subdivisión ampliada: Esquema de división de frecuencias que permite el tráfico bidireccional de un solo cable coaxial. Las señales del trayecto de retorno llegan a la cabecera con frecuencias comprendidas entre 5 y 42 MHz, y las señales del trayecto directo salen de la cabecera en 50 ó 54 MHz hasta el límite superior de frecuencias.

B.3.1.38 cable de alimentación: Cables coaxiales tendidos en las calles de la zona servida y que se conectan entre las derivaciones individuales que dan servicio a los ramales de cliente.

B.3.1.39 interfaz de datos distribuidos por fibra (FDDI, *fiber distributed data interface*): Norma LAN basada en fibras ópticas.

B.3.1.40 nodo de fibra: Punto de interfaz entre una troncal de fibra y la distribución coaxial.

B.3.1.41 canal de retorno: Sentido del flujo de la señal RF hacia la cabecera, lejos del abonado, equivalente al sentido descendente.

B.3.1.42 retardo de grupo: Diferencia en tiempo de transmisión entre la más alta y la más baja de varias frecuencias a través de un aparato, circuito o sistema.

B.3.1.43 tiempo de guarda: Tiempo mínimo atribuido entre ráfagas en sentido ascendente, referenciado desde el centro del símbolo del último símbolo de una ráfaga hasta el centro del símbolo del primer símbolo de la ráfaga siguiente. El tiempo de guarda debe ser igual a, al menos, la duración de cinco símbolos más el error máximo de temporización del sistema.

B.3.1.44 portadora relacionada con armónicas (HRC, *harmonic related carrier*): Método de separación de canales de televisión en un sistema de televisión por cable con incrementos exactos de 6 MHz, estando todas las frecuencias portadoras relacionadas armónicamente con una referencia común.

B.3.1.45 cabecera; extremo de cabecera: Ubicación central en la red de cable que se encarga de la introducción de señales de vídeo y otras señales de radiodifusión en sentido descendente. Véase también cabecera principal y centro de distribución.

B.3.1.46 encabezamiento: Información de control de protocolo ubicada al comienzo de una unidad de datos de protocolo.

B.3.1.47 alta frecuencia (HF, *high frequency*): Utilizada en el presente anexo B para referirse a la banda de subdivisión entera (5 a 30 MHz) y de subdivisión ampliada (5 a 42 MHz) utilizadas en comunicaciones por canal de retorno en la red de televisión por cable.

B.3.1.48 alto retorno: Esquema de división de frecuencia que permite el tráfico bidireccional por un solo cable coaxial. Las señales del canal de retorno se propagan hacia la cabecera por encima de la banda de paso en sentido descendente.

B.3.1.49 modulación por zumbido: Modulación no deseada de la portadora visual de televisión producida por la frecuencia fundamental o las armónicas de orden inferior de la frecuencia de la fuente de alimentación, de otras perturbaciones de baja frecuencia.

B.3.1.50 sistema híbrido de fibra óptica/cable coaxial (HFC, *hybrid fiber/coax*): Sistema bidireccional de transmisión con medios compartidos de banda ancha que utiliza troncales de fibra entre la cabecera y los nodos de fibra, y distribución coaxial desde los nodos de fibra a las posiciones de cliente.

B.3.1.51 portadoras incrementales relacionadas (IRC, *incremental related carriers*): Método de separación de canales de televisión NTSC en un sistema de televisión por cable en el que todos los canales, salvo el 5 y el 6, corresponden al plan de canales normalizados, utilizado para reducir distorsiones de batido triple compuesto.

B.3.1.52 Institute of Electrical and Electronic Engineers (IEEE): Organización de participación voluntaria que, entre otras actividades, patrocina comités de normalización y está acreditado por el American National Standards Institute.

B.3.1.53 Comisión Electrotécnica Internacional (CEI): Organismo de normas internacionales.

B.3.1.54 Organización Internacional de Normalización (ISO, *International Organization for Standardization*): Organismo de normas internacionales, conocido comúnmente como Organización Internacional de Normas.

B.3.1.55 protocolo de mensajes de control de Internet (ICMP, *Internet control message protocol*): Protocolo de capa de red de Internet.

B.3.1.56 grupo de tareas especiales de ingeniería en Internet (IETF, *Internet engineering task force*): Organismo responsable, entre otras cosas, de la elaboración de las normas utilizadas en Internet.

B.3.1.57 protocolo de gestión de grupos de Internet (IGMP, *Internet group management protocol*): Protocolo de capa de red que gestiona grupos de multidifusión en Internet.

B.3.1.58 ruido impulsivo: Ruido caracterizado por perturbaciones transitorias no superpuestas.

B.3.1.59 elemento de información (IE, *information element*): Los campos que componen un MAP y que definen concesiones individuales, concesiones diferidas, etc.

B.3.1.60 protocolo Internet (IP, *Internet protocol*): Protocolo de capa de red de Internet.

B.3.1.61 código de utilización de intervalos (IUC, *interval usage code*): Campo en MAP y UCD que sirve para unir perfiles de ráfaga a las concesiones.

B.3.1.62 latencia: Tiempo, expresado en cantidad de símbolos, que requiere un elemento de señal para pasar a través de un dispositivo.

B.3.1.63 capa: Subdivisión de la arquitectura de interconexión de sistemas abiertos (OSI), constituido por subsistemas del mismo rango.

B.3.1.64 red de área local (LAN, *local area network*): Red de datos no pública en la que se utiliza transmisión en serie para comunicaciones de datos directa entre estaciones de datos ubicadas en las instalaciones del usuario.

B.3.1.65 procedimiento de control de enlace lógico (LLC, *logical link control*): En una red de área local (LAN) o una red de área metropolitana (MAN), parte del protocolo que rige el ensamblado de tramas de capas de enlace de datos y su intercambio entre estaciones de datos, independientemente de cómo se comparte el medio de transmisión.

B.3.1.66 punto de acceso al servicio MAC (MSAP, *MAC service access point*): Véase B.8.1.2.2.

B.3.1.67 MAP: Véase diagrama de atribución de anchuras de banda.

B.3.1.68 cabecera principal: Cabecera que recopila material de programas televisivos de diversas fuentes, por satélite, microondas, fibra óptica y otros medios, y distribuye este material a los centros de distribución de la misma área metropolitana o regional. Una cabecera principal PUEDE realizar también funciones de centro de distribución para los clientes de su propia zona inmediata.

B.3.1.69 tiempo medio hasta el restablecimiento (MTTR, *mean time to repair*): En sistemas de televisión por cable, el MTTR es el tiempo medio transcurrido desde el momento en que se detecta la pérdida de funcionamiento de un canal de RF hasta el momento en que el funcionamiento de ese canal de RF está plenamente restablecido.

B.3.1.70 dirección de control de acceso a medios (MAC, *media access control*): Dirección de soporte físico "incorporada" de un dispositivo conectado a un medio compartido.

B.3.1.71 procedimiento de control de acceso a medios (MAC): En una subred, parte del protocolo que rige el acceso al medio de transmisión independientemente de las características físicas del medio, pero teniendo en cuenta los aspectos topológicos de la subred, a fin de permitir el intercambio de datos entre nodos. Entre los procedimientos MAC figuran la alineación de trama, la protección contra errores, y la adquisición del derecho a utilizar el medio de transmisión subyacente.

B.3.1.72 subcapa de control de acceso a medios (MAC): Parte de la capa de enlace de datos que soporta funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC).

B.3.1.73 microrreflexiones: Ecos en el trayecto de transmisión directo debidos a las desviaciones con respecto a las características ideales de amplitud y fase.

B.3.1.74 división media: Esquema de división de frecuencias que permite el tráfico bidireccional por un solo cable coaxial. Las señales de canal de retorno se propagan hacia la cabecera en 5 a 108 MHz, las señales de trayecto directo salen de la cabecera en frecuencias comprendidas entre 162 MHz y el límite superior de frecuencias. La banda de cruce díplex se halla entre 108 y 162 MHz.

B.3.1.75 miniintervalo de tiempo: Un "miniintervalo" de tiempo es un múltiplo entero de incrementos de 6,25 microsegundos. La relación entre miniintervalo, octetos y ticks de tiempo se describe en B.9.3.4.

B.3.1.76 grupo de expertos en imágenes en movimiento (MPEG, *moving picture experts group*): Organización de participación voluntaria que elabora normas sobre imágenes en movimiento digitales comprimidas y el audio asociado.

B.3.1.77 acceso multipunto: Acceso de usuario en el que una sola terminación de red soporta más de un equipo terminal.

B.3.1.78 conexión multipunto: Conexión entre más de dos terminaciones de red de datos.

B.3.1.79 National Cable Television Association (NCTA): Asociación de participación voluntaria de operadores de televisión por cable que, entre otras actividades, de directrices sobre medición y objetivos de sistemas de televisión por cable en Estados Unidos de América.

B.3.1.80 National Television Systems Committee (NTSC): Comité que definió la norma analógica de radiodifusión de la televisión en color en Estados Unidos de América.

B.3.1.81 capa de red: Capa 3 en arquitectura de interconexión de sistemas abiertos (OSI); capa que proporciona servicios para establecer un trayecto entre sistemas abiertos.

B.3.1.82 gestión de red: Funciones relacionadas con la gestión de los recursos de la capa de enlace de datos y la capa física y sus estaciones a través de la red de datos soportada por el sistema híbrido de fibra óptica/coaxial.

B.3.1.83 interconexión de sistemas abiertos (OSI, *open systems interconnection*): Marco de normas ISO para la comunicación entre sistemas diferentes fabricados por proveedores diferentes, en donde el proceso de comunicación se organiza en siete categorías situadas en una secuencia por capas basadas en su relación con el usuario. Cada capa utiliza la capa que se encuentra inmediatamente por debajo de ella y proporciona un servicio a la capa inmediatamente superior. Las capas 7 a 4 se refieren a la comunicación de extremo a extremo entre el origen y el destino del mensaje, y las capas 3 a 1, a las funciones de red.

B.3.1.84 identificador único de organización (OUI, *organizationally unique identifier*): Identificador de tres octetos asignado por el IEEE que se puede utilizar para generar direcciones MAC de LAN universales e identificadores de protocolo según [IEEE 802] a utilizar en aplicaciones de red de área local y metropolitana.

B.3.1.85 identificador de paquete (PID, *packet identifier*): Valor entero único utilizado para identificar flujos elementales de un programa en un flujo MPEG-2 uniprograma o multiprograma.

B.3.1.86 concesión parcial: Concesión que es menor que la petición correspondiente de anchura de banda del CM.

B.3.1.87 supresión de encabezamiento de cabida útil (PHS, *payloard header suppression*): Supresión del encabezamiento en un paquete de cabida útil (por ejemplo la supresión del encabezamiento Ethernet en los paquetes reenviados).

B.3.1.88 indicador de comienzo de unidad de cabida útil (PUSI, *payload unit start indicator*): Bandera en un encabezamiento MPEG. Un valor de 1 indica la presencia de un campo puntero en el primer octeto de la cabida útil.

B.3.1.89 capa física (PHY, *physical layer*): Capa 1 en la arquitectura de interconexión de sistemas abiertos (OSI); capa que proporciona servicios para transmitir bits o grupos de bits por un enlace de transmisión entre sistemas abiertos y sistemas que implican procedimientos eléctricos, mecánicos y de toma de contacto.

B.3.1.90 subcapa dependiente de los medios físicos (PMD, *physical media dependent*): Subcapa de la capa física que está relacionada con la transmisión de bits o grupos de bits por tipos particulares de enlaces de transmisión entre sistemas abiertos y sistemas que implican procedimientos eléctricos, mecánicos y de toma de contacto.

B.3.1.91 flujo de servicio primario: Todo CM tiene un flujo de servicio primario en sentido ascendente y un flujo de servicio primario en sentido descendente. Esos flujos aseguran que el CM es siempre gestionable y proporcionan una ruta por defecto para los paquetes reenviados que no son clasificados hacia ningún otro flujo de servicio.

B.3.1.92 información específica de programas (PSI, *programme-specific information*): En MPEG-2, datos normativos necesarios para la demultiplexación de flujos de transporte y la regeneración satisfactoria de programas.

B.3.1.93 flujo de programas: En el MPEG-2, un múltiplex de paquetes digitales de vídeo y audio de longitud variable procedentes de una o más fuentes de programas que tengan una base de tiempo común.

B.3.1.94 protocolo: Conjunto de reglas y formatos que determina el comportamiento de la comunicación de las entidades de capa en la actuación de las funciones de capa.

B.3.1.95 flujo de servicio aprovisionado: Flujo de servicio que ha sido aprovisionado como parte del proceso de registro, pero que no ha sido aún activado o admitido. Quizás requiera aún un intercambio de autorización con un módulo de política o con un servidor externo de seguridad antes de la admisión.

B.3.1.96 conjunto de parámetros QoS: Conjunto de codificaciones del flujo de servicio que describen los atributos de la calidad de servicio de un flujo de servicio o de una clase de servicio (véase B.C.2.2.5).

B.3.1.97 modulación de amplitud en cuadratura (QAM, *quadrature amplitude modulation*): Método de modulación de señales digitales sobre una señal portadora de radiofrecuencia que entraña la codificación en amplitud y en fase.

B.3.1.98 modulación por desplazamiento de fase cuaternaria (QPSK, *quadrature phase-shift keying*): Método de modulación de señales digitales sobre una señal portadora de radiofrecuencia que utiliza cuatro estados de fase para codificar dos bits digitales.

B.3.1.99 radiofrecuencia (RF): En sistemas de televisión por cable, se refiere a señales electromagnéticas generalmente en la gama 5 a 1000 MHz.

B.3.1.100 petición de comentarios (RFC, *request for comments*): Documento de carácter técnico del IETF; se puede acceder a estos documentos en el sitio http://www.rfc-editor.org/rfc-index.html de la World Wide Web.

B.3.1.101 pérdida de retorno: Parámetro que describe la atenuación de una señal de onda guiada (por ejemplo, a través de un cable coaxial) devuelta a una fuente por un dispositivo o medio resultante de las reflexiones de la señal generada por la fuente.

B.3.1.102 canal de retorno: Sentido del flujo de la señal hacia la cabecera, lejos del abonado, equivalente al sentido ascendente.

B.3.1.103 protocolo de información de encaminamiento (RIP, *routing information protocol*): Protocolo del IETF para el intercambio de información de encaminamiento sobre redes y subredes IP.

B.3.1.104 punto de acceso al servicio (SAP, *service access point*): Punto en el que una capa, o subcapa, presta servicios a la capa inmediatamente superior.

B.3.1.105 identificador de asociación de seguridad (SAID, *security association identifier)*: Identificador de seguridad de privacidad básica segura entre un CMTS y un CM.

B.3.1.106 unidad de datos de servicio (SDU, *service data unit*): Información que es entregada como una unidad entre puntos de acceso al servicio pares.

B.3.1.107 clase de servicio: Conjunto de atributos de programación y cola de espera, que el CMTS nombra y configura. Una clase de servicio se identifica con un nombre de clase de servicio. Una clase de servicio tiene un conjunto de parámetros QoS.

B.3.1.108 nombre de clase de servicios: Cadena ASCII mediante la cual puede hacerse referencia a una clase de servicio en los ficheros de configuración del módem y en los intercambios de protocolos.

B.3.1.109 flujo de servicio: Un servicio de transporte de capa MAC que: pProporciona transporte unidireccional de paquetes desde la entidad de servicio de capa superior hasta la RF; conforma, regula, y prioriza el tráfico de acuerdo con los parámetros de tráfico QoS definidos por el flujo.

B.3.1.110 identificador de flujo de servicio (SFID, *service flow identifier*): Identificador asignado por el CMTS al flujo de servicio (32 bits).

B.3.1.111 identificador de servicio (SID, *service identifier*): Identificador de flujo de servicio asignado por el CMTS (además del identificador de flujo de servicio) a un flujo de servicio en sentido ascendente activo o admitido (14 bits).

B.3.1.112 referencia de flujo de servicio: Parámetro de mensaje en los ficheros de configuración y en los mensajes de servicio dinámico MAC, que se usa para asociar clasificadores y otros objetos en el mensaje con codificaciones de flujo de servicio de un flujo de servicio pedido.

B.3.1.113 protocolo simple de gestión de red (SNMP, *simple network management protocol*): Protocolo de gestión de red del IETF.

B.3.1.114 sistema de gestión del espectro (SMS, *spectrum management system*): Sistema, definido en [SMS], para la gestión del espectro de cable de RF.

B.3.1.115 subcapa: División de una capa en el modelo de referencia de interconexión de sistemas abiertos (OSI).

B.3.1.116 subred: Las subredes se forman físicamente por la conexión de nodos adyacentes con enlaces de transmisión.

B.3.1.117 protocolo de acceso de subred (SNAP, *subnetwork access protocol*): Extensión del encabezamiento LLC para permitir el uso de redes IEEE tipo 802 como redes IP.

B.3.1.118 abonado: Véase usuario de extremo.

B.3.1.119 subdivisión: Esquema de división de frecuencia que permite el tráfico bidireccional por un solo cable. Las señales de trayecto de retorno acceden a la cabecera con frecuencias de 5 a 30 MHz (hasta 42 MHz en sistemas de subdivisión ampliada) Las señales de trayecto directo salen de la cabecera con frecuencias de 50 ó 54 MHz hasta el límite superior de frecuencia de la red de cable.

B.3.1.120 subsistema: Elemento en una división jerárquica de un sistema abierto que interactúa directamente con elementos en la división más alta siguiente o la siguiente división más baja de ese sistema abierto.

B.3.1.121 gestión de sistemas: Funciones de la capa de aplicación relacionadas con la gestión de diversos recursos de interconexión de sistemas abiertos (OSI) y su situación en todas las capas de la arquitectura OSI.

B.3.1.122 tick: Intervalo de tiempo de 6,25 microsegundos que sirve de referencia para la definición de miniintervalo de tiempo en sentido ascendente y tiempos de transmisión en sentido ascendente.

B.3.1.123 inclinación: Diferencia máxima en la ganancia de transmisión de un sistema de televisión por cable en una determinada anchura de banda (por lo general, la totalidad de la gama de frecuencias de funcionamiento directo).

B.3.1.124 retardo de tránsito: Diferencia de tiempo entre el instante en que el primer bit de una PDU cruza una frontera designada, y el instante en el que el último bit de la misma PDU cruza una segunda frontera designada.

B.3.1.125 protocolo de control de transmisión (TCP, *transmission control protocol*): Protocolo Internet de capa de transporte que asegura la entrega satisfactoria de extremo a extremo de paquetes de datos sin error.

B.3.1.126 subcapa de convergencia de transmisión: Subcapa de la capa física que proporciona una interfaz entre la capa de enlace de datos y la subcapa PMD.

B.3.1.127 enlace de transmisión: Unidad física de una subred que proporciona la conexión de transmisión entre nodos adyacentes.

B.3.1.128 medio de transmisión: Material por el que se pueden transportar señales de información; por ejemplo, fibras ópticas, cables coaxiales, y pares de alambres trenzados.

B.3.1.129 sistema de transmisión: Interfaz y medio de transmisión a través del cual las entidades de capa física pares transfieren bits.

B.3.1.130 relación transmisión activada/desactivada: En sistemas de acceso múltiple, relación entre las potencias de la señal enviada a la línea cuando se transmite y cuando no se transmite.

B.3.1.131 flujo de transporte: En el MPEG-2, método, basado en paquetes, de multiplexación de uno o más flujos digitales de vídeo y audio que tienen una o varias bases de tiempo independientes en un solo flujo.

B.3.1.132 protocolo de transferencia de ficheros trivial (TFTP, *trivial file-transfer protocol*): Protocolo Internet para la transferencia de ficheros sin el requisito de nombres de usuarios ni palabras clave que se utiliza típicamente para la telecarga automática de datos y soporte lógico.

B.3.1.133 cable troncal: Cable que transporta la señal desde la cabecera a grupos de abonados. El cable puede ser coaxial o de fibra óptica, dependiendo del diseño del sistema.

B.3.1.134 tipo/longitud/valor (TLV): Codificación de tres campos, en los que el primer campo indica el tipo de elemento, el segundo la longitud del elemento y el tercero el valor del elemento.

B.3.1.135 sentido ascendente; sentido hacia atrás: Sentido de transmisión de la posición de abonado hacia la cabecera.

B.3.1.136 descriptor de canal en sentido ascendente (UCD, *upstream channel descriptor*): El mensaje de gestión MAC utilizado para comunicar las características de la capa física en sentido ascendente a los módems de cable.

B.3.2 Abreviaturas

En este anexo se utilizan las siguientes siglas.

ANSI American National Standards Institute

ARP Protocolo de resolución de direcciones (*address resolution protocol)*

ATM Modo de transferencia asíncrono (*asynchronous transfer mode*)

BPDU Unidad de datos de protocolo puente (*bridge protocol data unit*)

CM Módem de cable (*cable modem*)

CMCI Interfaz módem de cable – CPE (*cable modem to CPE interface*)

CMTS Sistema de terminación de módem de cable (*cable modem termination system*)

CPE Equipo en las instalaciones del cliente (*customer premises equipment*)

CSO Batido de segundo orden compuesto (*composite second order beat*)

CTB Batido triple compuesto (*composite triple beat*)

DHCP Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)

EIA Alianza de industrias electrónicas (*electronic industries alliance*)

FDDI Interfaz de datos distribuidos por fibra (*fiber distributed data interface*)

HF Alta frecuencia (*high frequency*)

HFC Sistema híbrido de fibra óptica/cable coaxial (*hybrid-fiber/coax*)

HRC Portadora relacionada con armónicas (*harmonic related carrier*)

ICMP Protocolo de mensaje de control Internet (*Internet control message protocol*)

CEI Comisión Electrotécnica Internacional

IEEE Institute of Electrical and Electronic Engineers

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

IGMP Protocolo de gestión del grupo Internet (*Internet group management protocol*)

IP Protocolo Internet (*Internet protocol*)

IRC Portadoras relacionadas con incrementos (*incremental related carriers*)

ISO Organización Internacional de Normalización (*International Organization for Standardization*)

LAN Red de área local (*local area network*)

LLC Procedimiento de control de enlace lógico (*logical link control*)

MAC Control de acceso a medios (*media access control*)

MPEG Grupo de expertos en imágenes en movimiento (*moving picture experts group*)

MTTR Tiempo medio hasta el restablecimiento (*mean time to repair*)

NCTA National Cable Television Association

NTSC National Television Systems Committee

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

OUI Identificador único de organización (*organizationally unique identifier*)

PID Identificador de paquetes (*packet identifier*)

PMD Dependiente de los medios físicos (*physical media dependent*)

PSI Información específica de programa (*programme-specific information*)

PUSI Indicador de comienzo de unidad de carga útil (*payload unit start indicator*)

QAM Modulación de amplitud en cuadratura (*quadrature amplitude modulation*)

QPSK Modulación por desplazamiento de fase en cuadratura (*quadrature phase-shift keying*)

RF Radiofrecuencia

RFC Petición de comentarios (*request for comments*)

RIP Protocolo de información de encaminamiento (*routing information protocol*)

SAP Punto de acceso al servicio (*service access point*)

SDU Unidad de datos de servicio (*service data unit*)

SFID Identificador de flujo de servicio (*service flow identifier*)

SID Identificador de servicio (*service identifier*)

SMS Sistema de gestión del espectro (*spectrum management system*)

SNAP Protocolo de acceso de subred (*subnetwork access protocol*)

SNMP Protocolo simple de gestión de red (*simple network management protocol*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TFTP Protocolo de transferencia de ficheros trivial (*trivial file-transfer protocol*)

TLV Tipo/longitud/valor

UCD Descriptor de canal en sentido ascendente (*upstream channel descriptor*)

B.4 Hipótesis funcionales

En esta cláusula se describen las características del sistema de televisión por cable que se han de asumir a efectos del funcionamiento del sistema de datos por cable. No se trata de una descripción de los parámetros de la CMTS o del CM. El sistema de datos por cable interoperará con el entorno que aquí se describe.

Esta cláusula se aplica a la primera opción tecnológica descrita en B.1.1. Para la segunda opción, véase el anexo B.N.

Cuando una referencia a un plan de frecuencia o a la compatibilidad con otro servicio en esta cláusula entre en conflicto con un requisito legal para la zona de operación, este último tendrá la prioridad. Cualquier referencia a señales analógicas de NTSC en canales de 6 MHz no implica que tales señales estén presentes físicamente.

B.4.1 Red de acceso de banda ancha

Se supone red de acceso de banda ancha básicamente coaxial. Esto puede tomar la forma de una red totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC). La expresión genérica "red de cable" se emplea aquí para abarcar todos los casos.

Una red de cable utiliza un medio compartido, una arquitectura de árbol y ramas con transmisión analógica. Las características funcionales fundamentales cuya presencia se supone en el presente anexo B son las siguientes:

- transmisión bidireccional;
- separación óptica/eléctrica máxima entre el CMTS y el CM más distante de unos 160 km, aunque lo normal es que la separación máxima sea de unos 15 a 25 km;
- separación óptica/eléctrica diferencial máxima entre el CMTS y el módem más cercano y el más distante de unos 160 km, aunque lo normal es que este valor se reduzca a unos 25 km.

B.4.2 Hipótesis de los equipos

B.4.2.1 Plan de frecuencias

Se supone que, en el sentido descendente, el sistema de cable tiene una banda de paso con un borde inferior entre 50 MHz y 54 MHz y un borde superior que depende de la implementación, pero que varía normalmente entre 300 MHz y 864 MHz. Dentro de esa banda de paso se supone además que están presentes señales de televisión analógica NTSC en canales de 6 MHz de los planes de frecuencias normalizados HRC o IRC [EIA 542], así como otras señales digitales de banda estrecha y banda ancha.

En el sentido ascendente, el sistema de cable puede tener una banda de paso subdividida (5 MHz a 30 MHz) o subdividida ampliada (5 MHz a 40 MHz, o, 5 MHz a 42 MHz). Pueden estar presentes señales de televisión analógica NTSC en canales de 6 MHz, así como otras señales.

B.4.2.2 Compatibilidad con otros servicios

El CM y el CMTS DEBEN coexistir con los demás servicios en la red de cable. En particular:

a) DEBEN funcionar de manera satisfactoria en el espectro de cable asignado para el interfuncionamiento CMTS-CM mientras el resto del espectro del cable está ocupado por una combinación de señales de televisión y de otro tipo; y

b) NO DEBEN causar interferencia perjudicial a ningún otro servicio asignado a la red de cable en un espectro distinto del atribuido al CMTS.

Esto último se entiende como:

– degradación no medible (el más alto nivel de compatibilidad);

– ausencia de degradación por debajo del nivel perceptible de deterioro para todos los servicios (nivel de compatibilidad normal o medio); o

– ausencia de degradación por debajo de las normas mínimas aceptadas por la industria (por ejemplo, la FCC para los servicios de vídeo analógico) u otros proveedores de servicio (nivel mínimo de compatibilidad).

B.4.2.3 Repercusión del aislamiento de las averías en otros usuarios

Puesto que el sistema de datos por cable es un sistema punto a multipunto con medios compartidos, los procedimientos de aislamiento de averías deberían tener en cuenta la posible repercusión perjudicial de las averías y de los procedimientos de aislamiento de las mismas en muchos usuarios del servicio de datos por cable y de otros servicios.

Para la interpretación del impacto perjudicial, véase B.4.2.2.

B.4.2.4 Dispositivos terminales de sistema de cable

El CM DEBE cumplir con, y DEBERÍA superar, todas las reglamentaciones aplicables a los dispositivos de terminación de sistemas de cable y los equipos de cable preparados para el cliente, tal como se definen en [FCC15] y [FCC76] respectivamente. Ninguno de estos requisitos particulares puede ser utilizado para hacer menos estrictas algunas de las especificaciones contenidas en el presente anexo B.

B.4.3 Hipótesis de los canales de RF

El sistema de datos por cable, configurado con al menos un conjunto de parámetros de capa física definidos (por ejemplo, modulación, corrección de errores directa, velocidad de símbolos, etc.) de la gama de fijaciones de configuración descritas en el presente anexo B, DEBE ser interoperable en redes de cable cuyas características sean las definidas en esta cláusula, de tal manera que la corrección de errores directa permita el funcionamiento equivalente en un sistema de cable, con y sin las características de canal degradado descritas más adelante.

B.4.3.1 Transmisión en sentido descendente

Las características de la transmisión por canal de RF de la red de cable en sentido descendente se describen en el cuadro B.4-1. Las cifras indicadas suponen un valor de portadora igual a la potencia total media en una anchura de banda de canal de 6 MHz, a menos que se indique lo contrario. Para los niveles de degradación, los valores del cuadro B.4-1 suponen una potencia media en una anchura de banda en la cual los niveles de degradación se miden de manera estándar para un sistema de televisión por cable. Para los niveles de señales analógicas, las cifras del cuadro B.4-1 suponen potencia de cresta de la envolvente en una anchura de banda de canal de 6 MHz. Todas las condiciones se presentan de manera coincidente. Ninguna combinación de los parámetros siguientes superará ninguno de los límites de interfaz definidos en el presente anexo B.

Cuadro B.4-1/J.112 – Características supuestas de la transmisión por canal de RF en sentido descendente (véase la nota 1)

Parámetro	Valor
Gama de frecuencias	La gama normal de funcionamiento en el sentido descendente de un sistema de cable va de 50 MHz hasta incluso 860 MHz. Sin embargo, los valores de este cuadro se aplican solamente a frecuencias ≥ 88 MHz.
Separación de canales de RF (anchura de banda de diseño)	6 MHz
Retardo de tránsito del encabezamiento al cliente más distante	≤ 0,800 ms (normalmente, mucho menos)
Relación portadora/ruido en una banda de 6 MHz	No inferior a 35 dB (notas 2 y 3)
Relación portadora/distorsión de batido triple compuesto	No inferior a 41 dB (notas 2 y 3)
Relación portadora/distorsión de segundo orden compuesto	No inferior a 41 dB (notas 2 y 3)
Relación portadora/modulación cruzada	No inferior a 41 dB (notas 2 y 3)
Relación portadora/cualquier otra interferencia discreta (señales interferentes)	No inferior a 41 dB (notas 2 y 3)
Rizado de amplitud	3 dB dentro de la anchura de banda de diseño (nota 2)
Rizado de retardo de grupo en el espectro ocupado por el CMTS	75 ns dentro de la anchura de banda de diseño (nota 2)
Límite de las microrreflexiones para el eco dominante	–20 dBc @ ≤ 1,5 μs, –30 dBc @ >1,5 μs –10 dBc @ ≤ 0,5 μs, –15 dBc @ ≤ 1,0 μs (nota 2)
Modulación por zumbido de portadora	No superior a –26 dBc (5%) (nota 2)
Ruido en ráfagas	No superior a 25 μs a una frecuencia media de 10 Hz (nota 2)
Nivel máximo de portadora de vídeo analógico a la entrada del CM	17 dBmV
Número máximo de portadoras analógicas	121
NOTA 1 – La transmisión va del combinador de cabecera a la entrada del CM en la posición del cliente. NOTA 2 – Métodos de medición definidos en [NCTA] o [CableLabs2]. NOTA 3 – Medida relativa a la señal QAM que es igual al nivel de vídeo nominal en la planta.	

B.4.3.2 Transmisión en el sentido ascendente

En el cuadro B.4-2 se describen las características de la transmisión por canal de RF de la red de cable en sentido ascendente. Todas las condiciones se presentan de manera coincidente. Ninguna combinación de los parámetros siguientes superará ninguno de los límites de interfaz definidos en el presente anexo B.

Cuadro B.4-2/J.112 – Características supuestas de la transmisión por canal de RF en sentido ascendente (véase la nota 1)

Parámetro	Valor
Gama de frecuencias	5 MHz a 42 MHz borde a borde
Retardo de tránsito del CM más distante al CM o CMTS más cercano	≤ 0,800 ms (normalmente, mucho menos)
Relación portadora/interferencia más señal interferente (la suma de ruido, distorsión, distorsión de trayecto común y modulación cruzada y la suma de señales de interferencia discretas y de banda ancha, excluido el ruido impulsivo)	No inferior a 25 dB (nota 2)
Modulación por zumbido de portadora	No superior a –23 dBc (7,0%)
Ruido en ráfagas	No superior a 10 µs a una frecuencia media de 1 kHz para la mayoría de los casos (notas 3 y 4)
Rizado de amplitud 5 MHz a 42 MHz	0,5 dB/MHz
Rizado de retardo de grupo 5 MHz a 42 MHz	200 ns/MHz
Microrreflexiones, eco único	−10 dBc @ ≤ 0,5 µs −20 dBc @ ≤1,0 µs −30 dBc @ >1,0 µs
Variación de nivel de señal estacional y diurna	No superior a 14 dB de mínimo a máximo
NOTA 1 – La transmisión va de la entrada al CM en la posición del cliente a la cabecera. NOTA 2 – Se pueden utilizar técnicas de eliminación de las señales interferentes o de tolerancia a las mismas para garantizar el funcionamiento en presencia de señales interferentes discretas variables en el tiempo que podrían ser de hasta 10 dBc. Las relaciones se garantizan solamente dentro de los canales de portadora digital. NOTA 3 – Características de amplitud y frecuencia lo suficientemente fuertes como para enmascarar parcial o totalmente la portadora de datos. NOTA 4 – Niveles de ruido impulsivo más frecuentes a frecuencias más bajas (<15 MHz).	

B.4.3.2.1 Disponibilidad

La disponibilidad normal de las redes de cable suele ser superior al 99%.

B.4.4 Niveles de transmisión

Se pretende que el nivel de potencia nominal de la señal o señales del CMTS dentro de un canal de 6 MHz se encuentren en la gama de –10 dBc a –6 dBc con respecto al nivel de portadora de vídeo analógico, y que normalmente no supere a este último nivel. El nivel de potencia nominal de la señal o señales del CM en sentido ascendente deberá ser lo más bajo posible para conseguir el margen necesario por encima del ruido y la interferencia. Habitualmente se aplica una carga de potencia uniforme por unidad de anchura de banda al fijar los niveles de las señales en el sentido ascendente, con niveles específicos establecidos por el operador de red por cable para conseguir las relaciones requeridas de portadora/ruido y portadora/interferencia.

B.4.5 Inversión de frecuencia

No habrá inversión de frecuencia en el trayecto de transmisión en el sentido descendente ni en el sentido ascendente, es decir, un cambio positivo de frecuencia en la entrada a la red de cable dará lugar a un cambio positivo de frecuencia en la salida.

B.5 Protocolos de comunicación

Esta cláusula contiene una visión de conjunto de alto nivel de los protocolos de comunicación que deben ser utilizados en el sistema de datos por cable. En B.6, B.7 y B.8 se dan, respectivamente, las especificaciones detalladas de la subcapa dependiente de los medios físicos, de la subcapa de transmisión en sentido ascendente y de la subcapa de control de acceso a los medios.

B.5.1 Pila de protocolos

El CM y el CMTS funcionan como agentes retransmisores y también como sistemas de extremo (anfitriones). Las pilas de protocolos utilizadas en estos modos difieren entre sí como se indica más abajo.

La función principal del sistema de módem de cable consiste en transmitir paquetes de protocolo Internet (IP) transparentemente entre el encabezamiento y la ubicación del abonado. Algunas funciones de gestión dependen también del IP, por lo que la pila de protocolos en la red de cable es como se muestra en la figura B.5-1 (no se restringe por ello la generalidad de la transparencia del IP entre el encabezamiento y el cliente). Entre las funciones de gestión figuran, por ejemplo, la de soporte de la gestión de espectro y la de telecarga de soporte lógico.

B.5.1.1 CM y CMTS como anfitriones

Los CM y CMTS funcionarán como anfitriones de IP y LLC en los términos de [IEEE 802] para la comunicación por la red de cable. En la figura B.5-1 se muestra la pila de protocolos en las interfaces RF de CM y CMTS.

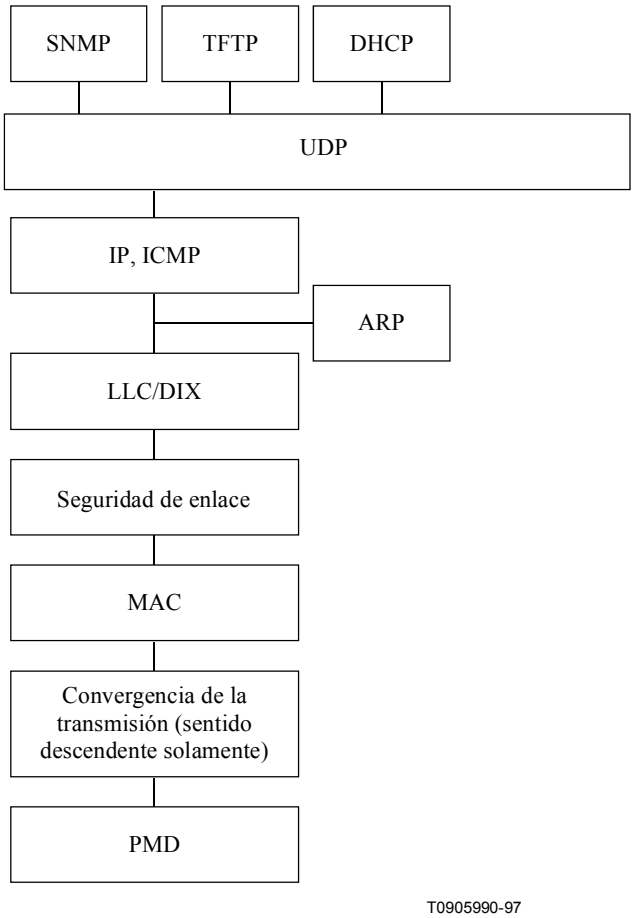


Figura B.5-1/J.112 – Pila de protocolos en la interfaz RF

El CM y el CMTS DEBEN funcionar como anfitriones de IP. Por ello, tanto el CM como el CMTS DEBEN soportar IP y ARP en la alineación de tramas de capa de enlace DIX (véase [DIX]). El CMTS NO DEBE transmitir tramas que sean menores que el octeto mínimo del DIX 64 por un canal en sentido descendiente (véase la nota). Sin embargo, el CM PUEDE transmitir tramas que sean menores que el octeto mínimo del DIX 64 por un canal en sentido ascendente.

NOTA – Excepto cuando es el resultado de una supresión de encabezamiento de cabida útil. Véase B.10.4.

El CM y el CMTS PUEDEN soportar también IP y ARP en la alineación de tramas SNAP [RFC 1042].

El CM y el CMTS DEBEN funcionar también como anfitriones de LLC. Por ello, tanto el CM como el CMTS DEBEN responder adecuadamente a las peticiones TEST y XID de conformidad con [ISO/CEI 8802-2].

B.5.1.2 Retransmisión de datos a través del CM y el CMTS

B.5.1.2.1 Consideraciones generales

La retransmisión de datos a través del CMTS PUEDE consistir en un puenteo transparente, o puede hacerse mediante la retransmisión de capa de red (encaminamiento, conmutación de IP) como se muestra en la figura B.5-2.

Salvo en el caso de PDU de paquetes de menos de 64 octetos que deben ser retransmitidas desde la RFI en sentido ascendente, un CMTS DEBE rellenar la PDU de paquetes y recalcular el CRC.

La retransmisión de datos a través del CM consiste en un puenteo transparente de capa de enlace, como se muestra en la figura B.5-2. Las reglas de la retransmisión son similares a las de [ISO/CEI 10038] con las modificaciones descritas en B.5.1.2.2 y B.5.1.2.3. De este modo es posible sustentar múltiples capas de red.

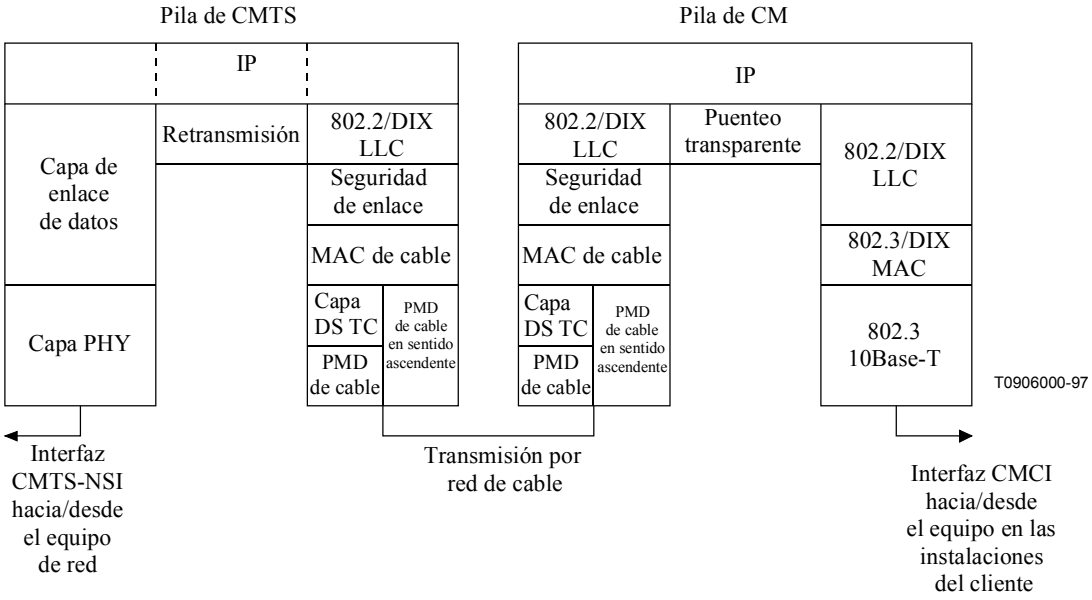


Figura B.5-2/J.112 – Retransmisión de datos a través del CM y el CMTS

La retransmisión de tráfico IP DEBE ser soportada. El soporte de otros protocolos de capa de red es OPCIONAL. La capacidad de restringir la capa de red a un único protocolo, por ejemplo el IP, es REQUERIDA.

El protocolo de árbol abarcante de IEEE 802.1D de [ISO/CEI 10038] con las modificaciones descritas en el anexo B.I PUEDE ser soportado por CM destinados a uso residencial. Los CM cuyo

uso previsto es de tipo comercial y los CMTS de puenteo DEBEN soportar esta versión de árbol abarcante. Los CMS y los CMTS DEBEN incluir la posibilidad de filtrar y desechar las BPDU de IEEE 802.1D.

En el presente anexo B se supone que los CM de uso residencial no se conectarán en una configuración que pudiera crear bucles de red tal como se muestra en la figura B.5-3.

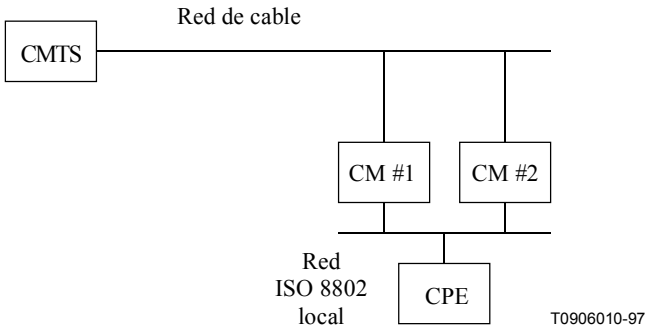


Figura B.5-3/J.112 – Ejemplo de condición para bucles de red

B.5.1.2.2 Reglas de retransmisión del CMTS

Si el CMTS utiliza retransmisión de capa de enlace, DEBE atenerse a las siguientes directrices de IEEE 802.1D de carácter general:

- Las tramas de capa de enlace NO DEBEN ser duplicadas.
- Las tramas que han prescrito (las que no han podido ser entregadas de manera puntual) DEBEN ser descartadas.
- Las tramas de capa de enlace, en un flujo de servicio dado (véase B.8.1.2.3), DEBEN ser entregadas en el orden en el que fueron recibidas.

Los mecanismos de aprendizaje y prescripción de las direcciones dependen del vendedor.

Si se utiliza retransmisión de capa de red, el CMTS debe atenerse a los requisitos del encaminador IETF [RFC 1812] con respecto a sus interfaces CMTS-RFI y CMTS-NSI.

Conceptualmente, el CMTS retransmite paquetes de datos en dos interfaces abstractas: entre la CMTS-RFI y la CMTS-NSI, y entre los canales en sentido ascendente y en sentido descendente. El CMTS PUEDE utilizar cualquier combinación de la semántica de capa de enlace (puenteo) y capa de red (encaminamiento) en cada una de esas interfaces. No es necesario emplear el mismo método en las dos interfaces.

La retransmisión entre los canales en sentido ascendente y en sentido descendente dentro de una capa MAC difiere con respecto a la retransmisión de LAN tradicional en que:

- Un canal único es símplex y no puede ser considerado como una interfaz completa para la mayoría de los fines de los protocolos (por ejemplo, el árbol abarcante de IEEE 802.1D, el protocolo de información de encaminamiento según [RFC 1058]).
- Los canales en sentido ascendente son básicamente canales punto a punto, mientras que los canales en sentido descendente son canales de medios compartidos.
- Puesto que se trata de una red pública, las decisiones de tipo político pueden invalidar la plena conectividad.

Por estos motivos, existe una entidad abstracta llamada retransmisor MAC en el CMTS para proporcionar conectividad entre estaciones dentro de un dominio MAC (véase B.5.2).

B.5.1.2.3 Reglas de retransmisión del CM

La retransmisión de datos a través del CM es un puenteo de capa de enlace con las reglas específicas que se indican a continuación.

B.5.1.2.3.1 Adquisición de direcciones MAC de dispositivos CPE

- El CM DEBE adquirir direcciones MAC de Ethernet de dispositivos CPE conectados, ya sea mediante el proceso de aprovisionamiento o bien aprendiéndolas, hasta alcanzar su número máximo de direcciones MAC de CPE (un valor que depende del dispositivo). Una vez que el CM haya adquirido su número máximo de dichas direcciones, las direcciones MAC de CPE recién descubiertas NO DEBEN reemplazar a las adquiridas previamente. El CM debe soportar la adquisición de por lo menos una dirección MAC de CPE.
- El CM DEBE permitir la configuración de direcciones CPE durante el proceso de aprovisionamiento (hasta su número máximo de direcciones CPE) para soportar configuraciones en las que el aprendizaje no resulta práctico o no se desea.
- Las direcciones proporcionadas durante el aprovisionamiento del CM DEBEN tener preferencia con respecto a las direcciones aprendidas.
- Las direcciones CPE NO DEBEN prescribir.
- Para permitir la modificación de direcciones MAC de usuario o el desplazamiento del CM, las direcciones no son retenidas en un almacenamiento no volátil. En una reposición de CM (por ejemplo, un ciclo de potencia), todas las direcciones aprendidas y aprovisionadas DEBEN ser descartadas.

B.5.1.2.3.2 Retransmisión

La retransmisión del CM en ambos sentidos DEBE atenerse a las siguientes directrices de IEEE 802.1D de carácter general:

- Las tramas de capa de enlace NO DEBEN ser duplicadas.
- Las tramas que han prescrito (las que no pueden ser entregadas de manera puntual) DEBEN ser descartadas.
- Las tramas de capa de enlace, en un flujo de servicio dado (véase B.8.1.2.3), DEBEN ser entregadas en el orden en el que fueron recibidas.

La retransmisión de red de cable a Ethernet DEBE seguir las reglas específicas que se indican a continuación:

- Las tramas dirigidas a destinos desconocidos NO DEBEN ser retransmitidas del puerto de cable al puerto Ethernet.
- Las tramas de radiodifusión DEBEN ser retransmitidas al puerto Ethernet, a menos que provengan de direcciones fuentes que sean aprovisonadas o aprendidas como dispositivos CPE soportados. En tal caso, NO DEBEN ser retransmitidas.
- La retransmisión de las tramas de multidifusión es controlada por parámetros fijados administrativamente por el servicio filtro de seguridad y por un algoritmo específico de seguimiento de la multidifusión (véase B.5.3.1). Las tramas de multidifusión NO DEBEN ser reenviadas a menos que ambos mecanismos así lo permitan.

La retransmisión de Ethernet a red de cable debe seguir las reglas específicas que se indican a continuación:

- Las tramas dirigidas a destinos desconocidos DEBEN ser retransmitidas desde el puerto Ethernet al puerto del cable.
- Las tramas de radiodifusión DEBEN ser retransmitidas al puerto del cable.

- Las tramas de multidifusión DEBEN ser retransmitidas al puerto del cable de acuerdo con las fijaciones de configuración de filtrado especificadas por las operaciones del operador de cable y los sistemas empresariales de soporte.
- Las tramas procedentes de direcciones de origen distintas de las aprovisionadas o aprendidas de dispositivos CPE sustentados NO DEBEN ser retransmitidas.
- Si un CM de usuario único ha aprendido una dirección MAC (véase B.5.1.2.3.1), NO DEBE retransmitir datos de una segunda fuente. Otras direcciones de origen CPE (no soportadas) del puerto Ethernet DEBEN ser aprendidas y esta información debe ser utilizada para filtrar tráfico local como en un puente de aprendizaje tradicional.
- Si un CM de usuario único ha adquirido una dirección MAC A como su dispositivo CPE soportado y ha aprendido B como un segundo dispositivo conectado al puerto Ethernet, DEBE filtrar cualquier tráfico de A a B.

B.5.2 Retransmisor MAC

El retransmisor MAC es una subcapa MAC que reside en el CMTS justo debajo de la interfaz del punto de acceso al servicio MAC (MSAP, *MAC service access point*), como se muestra en la figura B.5-4. Es responsable de la entrega de tramas en sentido ascendente a:

- uno o más canales en sentido descendente;
- la interfaz MSAP.

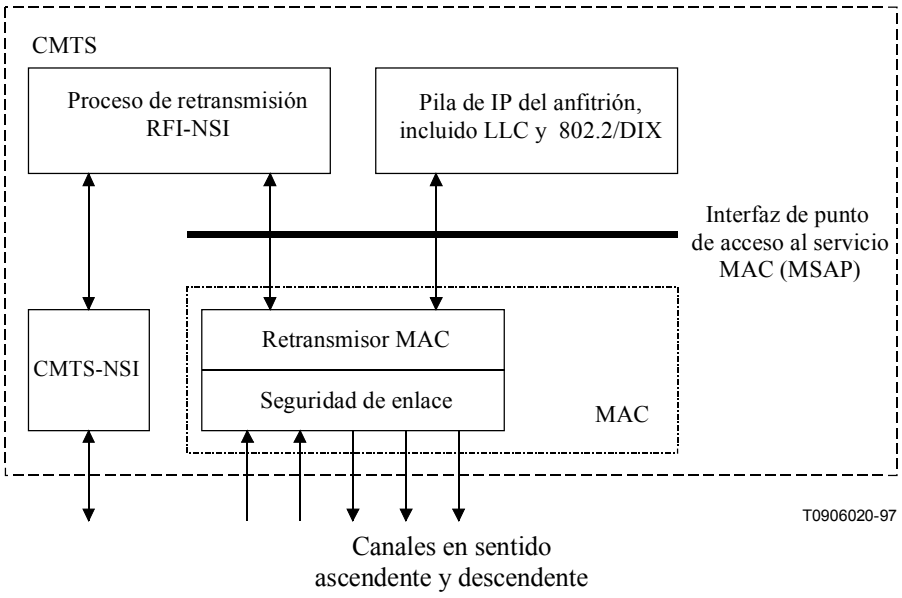


Figura B.5-4/J.112 – Retransmisor MAC

En la figura B.5-4, la subcapa LLC y las subcapas de seguridad de enlace de los canales en sentido ascendente y descendente por la red de cable terminan en el retransmisor MAC.

El usuario de la interfaz MSAP puede ser el proceso de retransmisión NSI-RFI o la pila de protocolos del anfitrión del CMTS.

La entrega de tramas puede basarse en la semántica de la capa de enlace de datos (puenteo), la semántica de la capa de red (encaminamiento) o en alguna combinación de las mismas. También se puede emplear semántica de capa superior (por ejemplo, los filtros aplicados a los números de puerto UDP). El CMTS DEBE proporcionar colectividad IP entre anfitriones conectados a módems de cable, y DEBE hacerlo de manera que se satisfagan las expectativas del equipo del cliente conectado

a Ethernet. Por ejemplo, el CMTS debe retransmitir paquetes ARP o facilitar un servicio ARP de apoderado. El retransmisor MAC del CMTS PUEDE prestar servicio para protocolos no IP.

Se señala que no hay ninguna exigencia en el sentido de que todos los canales en sentido ascendente y descendente se agreguen bajo un MSAP como se muestra más arriba. El vendedor podría optar simplemente por implementar múltiples MSAP, cada uno de ellos con un solo canal ascendente y descendente.

B.5.2.1 Reglas para la retransmisión de capa de enlace de datos

Los requisitos de esta cláusula son aplicables si el retransmisor MAC se implementa utilizando solamente semántica de capa de enlace de datos.

La entrega de tramas depende de la dirección de destino dentro de la trama. La manera de aprender la ubicación de cada dirección depende del vendedor, y PUEDE incluir:

- el aprendizaje y la prescripción de direcciones de origen al modo puenteo transparente;
- la selección a partir de los mensajes de petición de registro MAC;
- medios administrativos.

Si la dirección de destino de una trama es unidifundida, y esa dirección está asociada con un determinado canal en sentido descendente, la trama DEBE ser retransmitida a ese canal.

Los vendedores PUEDEN implementar extensiones, similares a direcciones estáticas en el puenteo de IEEE 802.1D/ISO 10038, que hagan que esas tramas sean filtradas o tratadas de alguna otra manera.

Si la dirección de destino de una trama es unidifundida, y se sabe que esa dirección reside en el otro lado (superior) de la interfaz MSAP, la trama DEBE ser entregada a la interfaz MSAP.

Si la dirección de destino es radiodifundida, multidifundida o desconocida, la trama DEBE ser entregada tanto al MSAP como a todos los canales en sentido descendente. (Con la excepción de las reglas de retransmisión de multidifusión de B.5.3.1.1.)

Todas las multidifusiones, incluidas las PDU de fuente de árbol abarcante de IEEE 802.1D/ISO 10038, DEBEN ser retransmitidas.

Las reglas de entrega son similares a las del puente o transparente:

- Las tramas NO DEBEN ser duplicadas.
- Las tramas que no puedan ser entregadas de manera puntual, DEBEN ser descartadas.
- La secuencia de verificación de trama DEBERÍA ser preservada en vez de ser regenerada.
- Las tramas, en un flujo de servicio dado (véase B.8.1.2.3), DEBEN ser entregadas en el orden en que fueron recibidas.

B.5.3 Capa de red

Como se ha indicado más arriba, el objetivo del sistema de datos por cable es transportar tráfico IP de manera transparente a través del sistema.

El protocolo de capa de red es la versión 4 del protocolo Internet (IP) definida en RFC 791, y en proceso de transformación en versión 6 del IP.

En el presente anexo B no se impone ningún requisito con respecto al reensamblado de paquetes IP.

B.5.3.1 Requisitos de gestión del IGMP

B.5.3.1.1 Reglas CMTS

- Si se utiliza el reenvío de la capa de enlace, el CMTS DEBE retransmitir todas las consultas sobre la pertenencia o no en calidad de miembro por todos los canales en sentido descendente, mediante la utilización del grupo multidifusión adecuado, 802.3 (por ejemplo,

01:00:5E: xx:xx:xx, donde xx:xx:xx son los 23 bits de orden inferior de la dirección de multidifusión, expresados en notación hexadecimal). Véase el [IMA].

- El CMTS DEBE reenviar la primera copia de los informes sobre pertenencia como miembro, solicitados y no solicitados, para cualquier grupo dado, recibidos en su interfaz RF en sentido ascendente, a todas sus interfaces RF en sentido descendente. Sin embargo, si la pertenencia se gestiona en base a cada interfaz RF en sentido descendente, los informes sobre pertenencia como miembro y los mensajes permiso de IGMP v2 sólo PUEDEN ser reenviados a la interfaz en sentido descendente a la que el CM del CPE que informa está conectado.
- El CMTS DEBERÍA suprimir la transmisión de informes adicionales sobre pertenencia como miembro (para cualquier grupo dado) en sentido descendente durante al menos el intervalo de respuesta a la consulta. Si el CMTS utiliza el reenvío de la capa de enlace de datos, DEBE también reenviar el informe sobre pertenencia a todas las interfaces apropiadas del lado de la red.
- El CMTS DEBERÍA suprimir la transmisión de tráfico en sentido descendente a cualquier grupo de multidifusión IP que no tenga abonados en esa interfaz RF en sentido descendente (a reserva de cualquier control administrativo).
- Si el CMTS efectúa el reenvío de la capa de red de paquetes multidifusión, DEBE implementar el tramo del encaminador del protocolo IGMP [RFC 2236] y DEBE actuar como el único consultante IGMP v2 en sus interfaces RF en sentido descendente.

B.5.3.1.2 Reglas CM

El CM DEBE soportar el IGMP, con las siguientes reglas especificas del cable. Los requisitos indicados a continuación se aplican a los CM que se ajustan a las reglas:

- El CM NO DEBE reenviar consultas sobre pertenencia como miembro desde su interfaz CPE hacia su interfaz RF.
- EL CM NO DEBE reenviar informes sobre pertenencia como miembro o permisos de IGMP v2, recibidos en su interfaz RF, a su interfaz CPE.
- El CM NO DEBE reenviar tráfico multidifusión desde su interfaz RF hacia su interfaz CPE, a menos que algún dispositivo en su interfaz CPE sea miembro de ese grupo multidifusión IP.
- El CM DEBE reenviar tráfico multidifusión desde su interfaz CPE hacia interfaz RF, a menos que sea prohibido por vía administrativa (por la configuración o por otro mecanismo).
- El CM DEBE reenviar tráfico para el grupo multidifusión TODOS ANFITRIONES, desde su interfaz RF hacia su interfaz CPE, a menos que sea prohibido por vía administrativa. El CPE DEBE ser considerado siempre como un miembro de este grupo.
- El CM DEBE reenviar consultas de grupo TODOS ANFITRIONES y consultas específicas de grupo que pasan filtros de permiso por su interfaz RF a su interfaz CPE, o DEBE implementar el tramo anfitrión del protocolo IGMP v2 [RFC 2236] en su interfaz RF para los CPE que tienen grupos activos, y NO DEBE actuar como un consultante en su interfaz RF. Si el CM implementa el tramo ANFITRIÓN del protocolo IGMP v2, debe actuar como un consultante IGMP v2 en su interfaz CPE. El CM NO DEBE requerir ninguna configuración específica para los valores del temporizador de multidifusión asociado y DEBE ser capaz de atenerse a los temporizadores especificados en esta cláusula. El CM PUEDE proporcionar control de configuración que omita los valores por defecto de esos temporizadores.
- El CM DEBE calcular el intervalo de consulta sobre pertenencia como miembro observando los tiempos de llegada de los mensajes de consulta al respecto. De manera formal: si $n < 2$,

MQI = 125, de no ser así, MQI = MAX (125, $MQ_n - MQ_{n-1}$), en donde MQI es el intervalo de consulta sobre pertenencia como miembro en segundos, n es el número de esas consultas observadas, y 'MQ_n' es el periodo de tiempo durante el cual la enésima consulta fue observada, aproximado al segundo más cercano.

- El paquete de consulta sobre pertenencia como miembro lleva el intervalo de respuesta a la consulta. El intervalo de respuesta a la consulta DEBE asumirse que es de 10 s, a menos que se fije de otra manera (o que se fije a 0) en el paquete de consulta sobre pertenencia .
- Como resultado de la recepción de un informe sobre pertenencia como miembro en su interfaz CPE, el CM DEBE empezar a reenviar tráfico para el grupo multidifusión IP apropiado. El CM DEBE dejar de reenviar tráfico multidifusión desde la RF hacia el lado CPE cuando no haya recibido un informe sobre pertenencia del CPE durante un tiempo mayor que el intervalo de pertenencia, que es igual a (2 × MQI) + QRI, donde MQI es el intervalo de consulta sobre pertenencia y QRI es el intervalo de respuesta a la consulta.
- Si el CM recibe un informe sobre pertenencia como miembro por su interfaz RF en sentido descendiente, para grupos activos de la interfaz CP del CM, dentro del intervalo de respuesta a la consulta, DEBE suprimir la transmisión por su interfaz RF en sentido ascendente de todos los informes sobre pertenencia recibidos por su interfaz CPE para este grupo.
- El CM PUEDE dejar de reenviar tráfico desde el RF hacia el CPE para un grupo multidifusión particular, antes de la expiración del intervalo de pertenencia (véase arriba), si puede determinar (por ejemplo, mediante un mensaje 'PERMISO' del IGMP y el intercambio apropiado de protocolos) que no existen dispositivos CPE abonados a este grupo en particular.
- El CM DEBE tratar los informes sobre pertenencia como miembro no solicitados (los 'JOIN' de IGMP) de su CPE como respuestas a una consulta sobre pertenencia recibidas por su interfaz RF. Al recibir un JOIN de su interfaz CPE, el CM DEBE arrancar un temporizador aleatorio, de acuerdo con el diagrama de estados del anfitrión (Host State Diagram), especificado en [RFC 2236], y DEBE utilizar un intervalo de respuesta a la consulta de 10 s, tal como se especifica más arriba. Como ya se ha dicho, si el CM recibe un informe sobre pertenencia como miembro por su interfaz RF en relación con este grupo durante el periodo de tiempo aleatorio, DEBE suprimir la transmisión de este Join por su interfaz RF en sentido ascendente. El CM DEBE suprimir todos los informes sobre pertenencia subsiguientes en relación con este grupo hasta el momento en que el CM reciba una consulta sobre pertenencia (general o específica del grupo) por su interfaz RF o se reciba un permiso IGMPv2 para este grupo procedente de la interfaz CPE.

Véase en el anexo B.L un ejemplo de diagrama de transición de estados de una aproximación a esos requisitos.

NOTA – Nada en esta cláusula impediría que un CM fuese configurado específicamente para no reenviar cierto tráfico de multidifusión, como resultado de una política de red.

B.5.4 Por encima de la capa de red

Los abonados podrán utilizar la capacidad de IP transparente como portador de servicios de capa superior. La utilización de estos servicios será transparente al CM.

Además del transporte de datos de usuarios, hay varias capacidades de gestión y explotación de red que dependen de la capa de red. Son las siguientes:

- SNMP (protocolo de gestión de red simple [RFC 1157]), que DEBE ser soportado para la gestión de red.
- TFTP (protocolo de transferencia de ficheros trivial [RFC 1350]), que DEBE ser soportado para la telecarga de soporte lógico e información de configuración, tal como fue modificado

por las opciones de intervalo de fin de temporización y de tamaño de transferencia del TFTP [RFC 2349];

- DHCP (protocolo dinámico de configuración de anfitrión [RFC 2131]), es un marco para pasar información de configuración a los anfitriones de una red TCP/IP que DEBE ser soportado.
- Un protocolo de hora del día [RFC 868], que DEBE ser soportado para obtener la hora del día.

B.5.5 Capa de enlace de datos

La capa de enlace de datos se divide en dos subcapas de acuerdo con [IEEE 802], y se añade la de seguridad de capa de enlace de conformidad con [DOCSIS8]. Las subcapas, empezando por la situada más arriba, son:

- la subcapa de control de enlace lógico (LLC, *logical link control*) (clase 1 solamente);
- la subcapa de seguridad de capa de enlace;
- la subcapa de control de acceso a medios (MAC, *media access control*).

B.5.5.1 Subcapa LLC

La subcapa LLC DEBE proporcionarse de acuerdo con [ISO/CEI 10039]. La resolución de direcciones DEBE utilizarse según lo definido en [RFC 826]. La definición del servicio MAC a LLC se especifica en [ISO/CEI 10039].

B.5.5.2 Subcapa de seguridad de capa de enlace

La seguridad de la capa de enlace DEBE proporcionarse de acuerdo con [DOCSIS8].

B.5.5.3 Subcapa MAC

La subcapa MAC define un transmisor único para cada canal en sentido descendente – el CMTS. Todos los CM están a la escucha de todas las tramas transmitidas por el canal en sentido descendente con el que están registrados y aceptan aquellas cuyo destino concuerda con el propio CM o los CPE alcanzados por conducto del puerto CMCI. Los CM sólo pueden comunicar con otros CM a través del CMTS.

El canal en sentido ascendente se caracteriza por muchos transmisores (CM) y un receptor (el CMTS). El tiempo en el canal ascendente se divide en intervalos, permitiendo el acceso múltiple por división en el tiempo en tics de tiempo regulados. El CMTS proporciona la referencia de tiempo y controla la utilización permitida de cada intervalo. Los intervalos pueden ser adjudicados para transmisiones por CM particulares o pueden competir por ellos todos los CM. Los CM pueden competir en la petición de tiempo de transmisión. En cierta medida, los CM pueden también competir en la transmisión de datos reales. En ambos casos, puede haber colisiones por lo que se llevan acabo reintentos.

En la cláusula B.8 se describen los mensajes de subcapa MAC procedentes del CMTS que dirigen el comportamiento de los CM en el canal en sentido ascendente, así como la mensajería de los CM a los CMTS.

B.5.5.3.1 Definición del servicio MAC

En el anexo B.E figura la definición del servicio de la subcapa MAC.

B.5.6 Capa física

La capa física (PHY) consta de dos subcapas:

- la subcapa de convergencia de transmisión (presente sólo en el sentido descendente);
- la subcapa dependiente de los medios físicos (PMD, *physical media dependent*).

B.5.6.1 Subcapa de convergencia de la transmisión en sentido descendente

La subcapa de convergencia de la transmisión en sentido descendente sólo existe en ese sentido. Hace posibles servicios adicionales en el tren de bits de la capa física. Estos servicios adicionales podrían incluir, por ejemplo, el vídeo digital. La definición de cualquiera de esos servicios queda fuera del alcance del presente anexo B.

Esta subcapa se define como una serie continua de paquetes MPEG [UIT-T H.222.0] de 188 octetos, cada uno de los cuales consta de un encabezamiento de 4 octetos seguido de 184 octetos de cabida útil. El encabezamiento identifica la cabida útil perteneciente al MAC de datos por cable. Otros valores del encabezamiento pueden indicar otras cabidas útiles. La combinación de cabidas útiles se hace de manera arbitraria y la controla el CMTS.

La subcapa de convergencia de la transmisión en sentido descendente se define en B.7.

B.5.6.2 Subcapa PMD

La subcapa dependiente del medio físico se define B.6.

B.5.6.2.1 Puntos de interfaz

En la subcapa PMD se definen tres puntos de interfaz RF:

a) salida en el sentido descendente en el CMTS;

b) entrada en el sentido ascendente en el CMTS;

c) entrada/salida del cable en el módem del cable.

Se necesitan interfaces separadas de salida en el sentido descendente y entrada en el sentido ascendente en el CMTS para compatibilidad con las configuraciones típicas de combinación y división de señales descendentes y ascendentes en las cabeceras.

B.6 Especificación de la subcapa dependiente de los medios físicos

Esta cláusula se aplica a la primera opción tecnológica a la que se hace referencia en B.1.1. Para la segunda opción, véase el anexo B.N.

Si cualquier referencia en esta cláusula a las emisiones espurias entrase en conflicto con cualquier requisito legal para la zona de operación, este último tendría prioridad.

B.6.1 Alcance

El presente anexo B define las características eléctricas y el protocolo de un módem de cable (CM) y un sistema de terminación de módem de cable (CMTS). Lo que se pretende con la misma es definir un CM y un CMTS que interfuncionen de tal manera que cualquier implementación de un CM pueda funcionar con cualquier CMTS. El presente anexo B no trata de inducir la puesta en aplicación de ninguna implementación en concreto.

B.6.2 Sentido ascendente

B.6.2.1 Visión de conjunto

La subcapa dependiente de los medios físicos (PMD) en el sentido ascendente utiliza un formato de modulación de ráfagas FDMA/TDMA, que proporciona cinco velocidades de símbolos y dos formatos de modulación (QPSK y 16QAM). El formato de modulación incluye la conformación de impulsos a efectos de eficacia espectral, tiene agilidad de frecuencia de portadora y su nivel de potencia de salida es seleccionable. El formato de la subcapa PMD consta de una ráfaga modulada de longitud variable con temporización precisa que comienza en puntos separados por múltiplos enteros de 6,25 μs (lo que representa 16 símbolos a la velocidad de datos más alta).

Cada ráfaga soporta modulación flexible, preámbulo, aleatorización de la cabida útil y codificación FEC programable.

Todos los parámetros de la transmisión en el sentido ascendente asociados con salidas de transmisión de ráfagas procedentes del CM pueden ser configurados por el CMTS mediante la mensajería MAC. Muchos de los parámetros son programables ráfaga por ráfaga.

La subcapa PMD puede soportar un modo de transmisión casi continua, en donde la rampa descendente de una ráfaga PUEDE superponerse con la rampa ascendente de la ráfaga siguiente, de tal manera que la envolvente transmitida nunca es cero. La temporización del sistema de las transmisiones TDMA desde los diversos CM DEBE hacerse de tal modo que el centro del último símbolo de una ráfaga y el centro del primer símbolo del preámbulo de la ráfaga que sigue inmediatamente estén separados por la duración de cinco símbolos como mínimo. El tiempo de guarda DEBE ser superior o igual a la duración de cinco símbolos más el error de temporización máximo. Al error de temporización contribuyen tanto el CM como el CMTS. El funcionamiento de la temporización del CM se especifica en B.6.2.7. El error de temporización máximo y el tiempo de guarda pueden variar con los CMTS de diferentes vendedores.

El modulador en sentido ascendente forma parte del módem del cable que hace interfaz con la red de cable. El modulador contiene la función de modulación de nivel eléctrico efectiva y la función de procesamiento de señales digitales; esta última proporciona la FEC, la agregación del preámbulo delantero, la correspondencia de símbolos y otros pasos del procesamiento. El presente anexo B se ha redactado con la idea de que las ráfagas se almacenen en memoria tampón en el tramo procesamiento de señal, y de que el tramo procesamiento de señal:

1) acepte el tren de información en base a una ráfaga en cada momento;

2) convierta dicho tren en una ráfaga completa de símbolos para el modulador; y

3) introduzca el tren de símbolos en ráfagas adecuadamente temporizadas en un modulador sin memoria en el momento exacto de la transmisión de la ráfaga.

El tramo sin memoria del modulador sólo efectúa la conformación de los impulsos y la conversión elevadora en cuadratura.

En el demodulador, al igual que en el modulador, hay dos componentes funcionales básicos: la función de demodulación y la función de procesamiento de señales. A diferencia del modulador, el demodulador reside en el CMTS y la especificación se establece teniendo en cuenta que habrá una función de demodulación (no necesariamente un demodulador físico real) por cada frecuencia de portadora que se utilice. La función de demodulación recibirá todas las ráfagas a una frecuencia determinada.

NOTA – El procedimiento de diseño de la unidad deberá tener en cuenta la naturaleza multicanal de la demodulación y del procesamiento de la señal que se ha de efectuar en la cabecera, y dividir/compartir la funcionalidad adecuadamente para influir de manera óptima en la aplicación multicanal. Lo apropiado podría ser un diseño de demodulador que soportara múltiples canales en una unidad demoduladora.

La función demodulación del demodulador acepta una señal de nivel variable centrada en torno al nivel de potencia pedido y efectúa la temporización de símbolos y la recuperación y seguimiento de la portadora, la adquisición de ráfagas y la demodulación. Además, la función demodulación proporciona una estimación de la temporización de las ráfagas con respecto a un borde de referencia, una estimación de la potencia de la señal recibida y una estimación de la relación señal/ruido, y puede llevar a cabo una ecualización adaptable para atenuar los efectos de:

a) los ecos del sistema de cables;

b) las señales interferentes de banda estrecha; y

c) el retardo de grupo.

La función procesamiento de señal del demodulador efectúa un procesamiento inverso al de la función procesamiento de señal del modulador. Se incluye en él la aceptación del tren de datos en ráfagas demoduladas, la decodificación, etc. y, posiblemente, la multiplexación de los datos procedentes de múltiples canales en un solo tren de salida. La función procesamiento de señal

proporciona también la señal de referencia de temporización con respecto al borde y de desbloqueo a los demoduladores para activar la adquisición de ráfagas de cada intervalo de ráfagas asignado. Además puede proporcionar una indicación de decodificación satisfactoria, error de decodificación o fallo de la decodificación por cada palabra de código y el número de símbolos Reed-Solomon corregidos en cada palabra de código. Para toda ráfaga en sentido ascendente, el CMTS tiene un conocimiento previo de su longitud en símbolos (véanse B.6.2.7 y B.6.2.11.1 y B.A.2).

B.6.2.2 Formatos de modulación

El modulador en sentido ascendente DEBE proporcionar tanto el formato de modulación QPSK como el 16QAM.

El demodulador en el sentido ascendente DEBE soportar el formato QPSK, el 16QAM o ambos formatos de modulación.

B.6.2.2.1 Velocidades de modulación

El modulador en sentido ascendente DEBE proporcionar QPSK a 160, 320, 640, 1280 y 2560 ksímb/s, y 16QAM a 160, 320, 640 1280 y 2560 ksímb/s.

Esta diversidad de velocidades de modulación, y la flexibilidad al fijar las frecuencias de la portadora en sentido ascendente, permite a los operadores ubicar operadoras en intervalos del esquema de señales interferentes de banda estrecha, como se analiza en el anexo B.G.

La velocidad de símbolos de cada canal en sentido ascendente se define en una mensaje MAC de descriptor de canal en sentido ascendente (UCD, *upstream channel descriptor*). Todos los CM que utilizan este canal en sentido ascendente DEBEN utilizar la velocidad de símbolos definida en las transmisiones en sentido ascendente.

B.6.2.2.2 Correspondencia de símbolos

El modo de modulación (QPSK o 16QAM) es programable. Los símbolos transmitidos en cada modo y la correspondencia entre los bits de entrada y la constelación I y Q DEBEN ser como se define en el cuadro B.6-1. En dicho cuadro, I_1 es el MSB del diagrama de símbolos, Q_1 es el LSB para QPSK, y Q_0 es el LSB para 16QAM. Q_1 e I_0 tienen posiciones de bits intermedias en 16QAM. El MSB DEBE ser el bit de los datos en serie con el que comienza el establecimiento de la correspondencia de símbolos.

Cuadro B.6-1/J.112 – Correspondencia de I/Q

Modo QAM	Definiciones de bit de entrada
QPSK	I_1 Q_1
16QAM	I_1 Q_1 I_0 Q_0

La correspondencia de símbolos de QPKS en sentido ascendente DEBE ser como se muestra en la figura B.6-1.

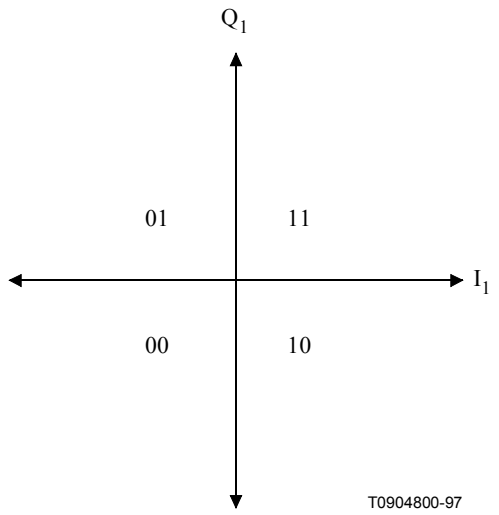


Figura B.6-1/J.112 – Correspondencia de símbolos de QPSK

La correspondencia de símbolos no invertidos de 16QAM (con codificación Gray) DEBE ser como se muestra en la figura B.6-2.

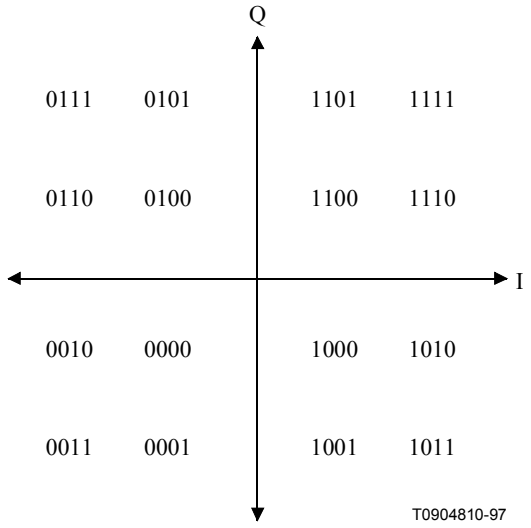


Figura B.6-2/J.112 – Correspondencia de símbolos con codificación Gray de 16QAM

La correspondencia de símbolos con codificación diferencial de 16QAM DEBE ser como se muestra en la figura B.6-3.

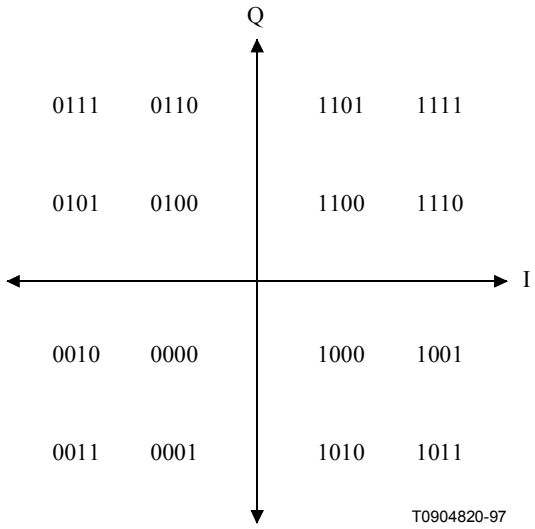


Figura B.6-3/J.112 – Correspondencia de símbolos con codificación diferencial de 16QAM

Si la codificación de cuadrante diferencial, está habilitada, el cuadrante de símbolos transmitido en un determinado momento se obtiene a partir del cuadrante de símbolos transmitido con anterioridad y de los bits de entrada en ese momento utilizando el cuadro B.6-2. Además, si tal es el caso, la subcapa PMD en sentido descendente DEBE aplicar estas reglas de codificación diferencial a todos los símbolos transmitidos (incluidos los que llevan bits de preámbulo).

Cuadro B.6-2/J.112 – Obtención del cuadrante de símbolos transmitidos actualmente

Bits de entrada actuales I(1) Q(1)	Cambio de fase del cuadrante	Bits más significativos del símbolo transmitido previamente	Bits más significativos del símbolo transmitido actualmente
00	0º	11	11
00	0º	01	01
00	0º	00	00
00	0º	10	10
01	90º	11	01
01	90º	01	00
01	90º	00	10
01	90º	10	11
11	180º	11	00
11	180º	01	10
11	180º	00	11
11	180º	10	01
10	270º	11	10
10	270º	01	11
10	270º	00	01
10	270º	10	00

B.6.2.2.3 Conformación del espectro

La subcapa PMD en sentido ascendente DEBE soportar una conformación Nyquist de raíz cuadrada de coseno alzado con factor del 25%.

El espectro ocupado NO DEBE exceder de las anchuras de canal que se muestran en el cuadro B.6-3.

Cuadro B.6-3/J.112 – Máxima anchura de canal

Velocidad de símbolos (ksímb/s)	Anchura de canal (kHz) (véase la nota)
160	200
320	400
640	800
1280	1600
2560	3200
NOTA – La anchura de canal es la anchura de banda de –30 dB.	

B.6.2.2.4 Agilidad y gama de las frecuencias en sentido ascendente

La subcapa PMD en sentido ascendente DEBE soportar el funcionamiento en la gama de frecuencias de 5 MHz a 42 MHz borde a borde.

Se DEBE soportar la resolución del desplazamiento de frecuencia con una gama de ± 32 kHz (incremento = 1 Hz; implementación dentro de ± 10 Hz).

B.6.2.2.5 Formato del espectro

El modulador en sentido ascendente DEBE funcionar con el formato $s(t) = I(t) \times \cos(\omega t) - Q(t) \times \text{sen}(\omega t)$, donde t representa el tiempo y ω indica la frecuencia angular.

B.6.2.3 Codificación FEC

B.6.2.3.1 Modos de codificación FEC

El modulador en sentido ascendente DEBE proporcionar las siguientes opciones: códigos Reed-Solomon en GF(256) con T = 1 a 10 o ausencia de codificación FEC.

DEBE soportarse el siguiente polinomio generador de Reed-Solomon:

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

donde el elemento primitivo alfa es 0x02 hex.

DEBE soportarse el siguiente polinomio primitivo de Reed-Solomon:

$$p(x) = x^8 + x^4 + x^3 + x^2 + x^1 + 1$$

El modulador en sentido ascendente DEBE proporcionar palabras de código con un tamaño comprendido entre un mínimo de 18 octetos (16 octetos de información [k] más dos octetos de paridad para corrección de errores T = 1) hasta un máximo de 255 octetos (octetos k más octetos de paridad). El tamaño de una palabra de código no codificada puede ser de hasta un mínimo de un octeto.

En el modo última palabra de código abreviada, el CM DEBE proporcionar la última palabra de código de una ráfaga abreviada a partir de la longitud asignada de k octetos de datos por palabra de código, según se describe en B.6.2.11.1.2.

El valor de T DEBE configurarse en respuesta al descriptor de canal en sentido ascendente del CMTS.

B.6.2.3.2 Orden de bit a símbolo FEC

La entrada en el codificador Reed-Solomon es lógicamente un tren de bits en serie proveniente de la capa MAC del CM, y se DEBE establecer la correspondencia entre el primer bit del tren y el MSB del primer símbolo Reed-Solomon que entra en el codificador. El MSB del primer símbolo que sale del codificador se DEBE hacer corresponder con el primer bit del tren de bits en serie introducido en el aleatorizador.

NOTA – El convenio MAC octeto a serie en sentido ascendente requiere que se establezca la correspondencia entre el LSB del octeto y el primer bit del tren de bits en serie, según B.8.2.1.3.

B.6.2.4 Aleatorizador

El modulador en sentido ascendente DEBE implementar un aleatorizador (véase la figura B.6-4) cuyo valor semilla de 15 bits DEBE ser programable de manera arbitraria.

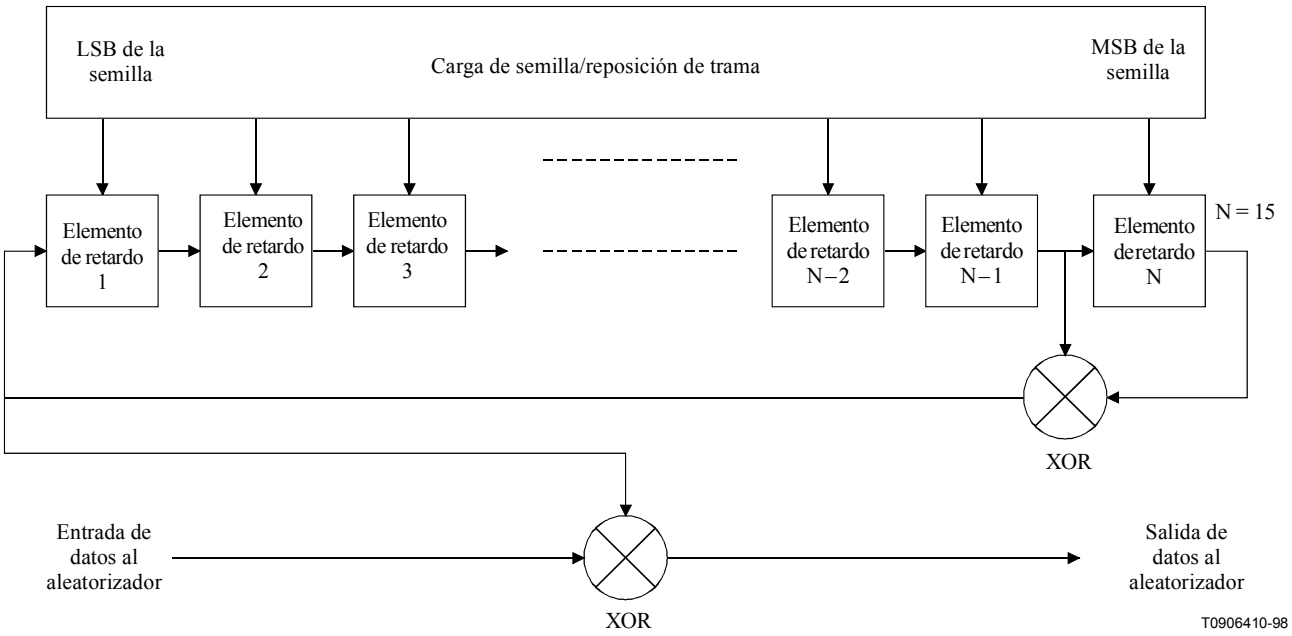


Figura B.6-4/J.112 – Estructura del aleatorizador

Al comienzo de cada ráfaga, se libera el registrador y se carga el valor semilla. El valor semilla se DEBE utilizar para calcular el bit del aleatorizador que se combina en un XOR (OR exclusivo) con el primer bit de los datos de cada ráfaga (que es el MSB del primer símbolo que sigue al último símbolo del preámbulo).

El valor semilla del aleatorizador DEBE configurarse en respuesta al descriptor de canal en sentido ascendente del CMTS.

El polinomio DEBE ser $x^{15} + x^{14} + 1$.

B.6.2.5 Agregación de preámbulo delantero

La subcapa PMD en sentido ascendente DEBE soportar un campo preámbulo de longitud variable que se sitúa delante de los datos una vez que éstos han sido aleatorizados y codificados según Reed-Solomon.

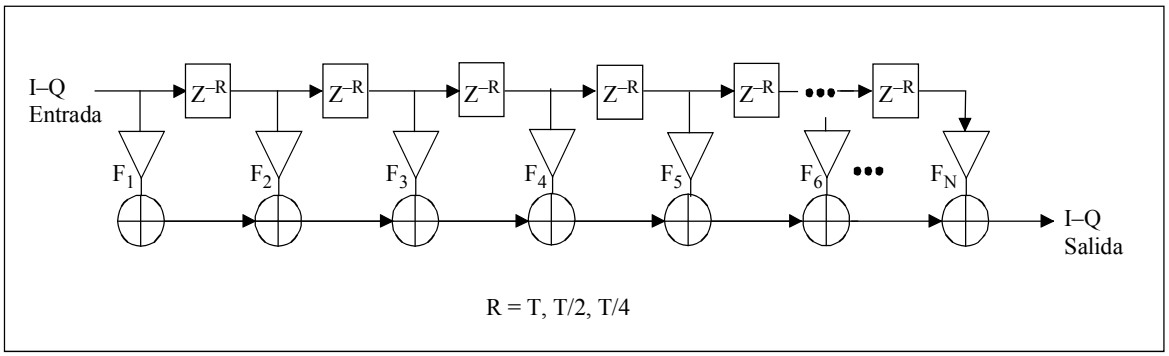
El primer bit del esquema de preámbulo es el primer bit que entra en el dispositivo de establecimiento de la correspondencia (véase la figura B.6-9), y es I_1 en el primer símbolo de la ráfaga (véase B.6.2.2.2). El primer bit del esquema de preámbulo es designado por el desplazamiento del valor del preámbulo como se describe en el cuadro B.8-19 de B.8.3.3.

El valor del preámbulo que se agrega delante DEBE ser programable y su longitud DEBE ser de 0, 2, 4, ..., ó 1024 bits para QPSK y 0, 4, 8, ..., ó 1024 bits para 16QAM. Con ello, la longitud máxima del preámbulo es de 512 símbolos QPSK o bien de 256 símbolos QAM.

La longitud y el valor del preámbulo DEBEN configurarse en respuesta al mensaje del descriptor de canal en sentido ascendente transmitido por el CMTS.

B.6.2.6 Ecualizador previo de transmisión

El CM DEBE configurar un ecualizador previo de transmisión de estructura de ecualizador lineal, tal como se muestra en la figura B.6-5, en respuesta a un mensaje de respuesta de alineación (RNG-RSP, *ranging response*) transmitido por el CMTS. El ecualizador previo DEBE aceptar una estructura de ecualizador con reparación de símbolos (T) con ocho derivaciones. El ecualizador previo PUEDE tener 1, 2 ó 4 muestras por símbolo, con una longitud de derivación superior a ocho símbolos.



T0910720-00

Figura B.6-5/J.112 – Estructura del ecualizador previo de transmisión

El mensaje MAC RNG-RSP (véase B.8.3.6.1) utiliza 16 bits por coeficiente en la notación de complemento a dos fraccional "s1.14" (bit de signo, bit de entero, punto binario y 14 bits fraccionales) para definir la información de ecualización de la transmisión del CM. El CM DEBE convolucionar los coeficientes enviados por el CMTS con los existentes para obtener los nuevos coeficientes.

En respuesta a una petición de alineación inicial y a peticiones de alineación periódicas, anteriores al registro del CM, cuando el CMTS envía los coeficientes del ecualizador previo, el CMTS DEBE calcularlos y enviarlos con una longitud de ecualizador de 8 y en formato de separación de símbolos. Tras el registro, el CMTS PUEDE utilizar un formato de ecualizador separado fraccionalmente (separación T/2 o T/4) que tenga una longitud de derivación mayor para poder adaptarse a las capacidades del ecualizador previo del CM, que el CMTS aprendió del campo capacidades del módem del mensaje REG-REQ. Para el uso adecuado del campo de capacidades del módem véase B.8.3.8.1.1.

Antes de efectuar una petición de alineación inicial y siempre que cambie la frecuencia de canal en sentido ascendiente o la velocidad de símbolo de canal en sentido ascendente, el CM DEBE inicializar los coeficientes del ecualizador previo con los valores correspondientes a una fijación por defecto en la que todos ellos son 0 excepto el coeficiente real de la primera derivación (F1). Durante la alineación inicial, el CM, y no el CMTS, DEBE compensar el retardo (desplazamiento de la

alineación) debido a un desplazamiento de la primera derivación a una nueva ubicación de la derivación principal de los coeficientes del ecualizador enviada por el CMTS. Los coeficientes del ecualizador previo se actualizan entonces mediante el proceso de alineación subsiguiente (mantenimiento de estación periódicos). El CMTS NO DEBE variar la ubicación de la derivación principal durante el mantenimiento de estación periódico. Los coeficientes del ecualizador pueden ser incluidos en cada mensaje RNG-RSP, pero normalmente sólo figuran cuando el CMTS encuentra que la respuesta de canal ha cambiado significativamente. La frecuencia de actualización de los coeficientes del ecualizador en el mensaje RNG-RSP la determina el CMTS.

El CM DEBE normalizar los coeficientes del ecualizador previo para poder garantizar un funcionamiento adecuado (es decir, sin desbordamientos ni recortes). El CM debe compensar además el cambio de la potencia de transmisión debido a la ganancia (o pérdida) de los nuevos coeficientes. Si la estructura del ecualizador CM implementa el mismo número de coeficientes que el de asignados en el mensaje RNG-RSP, el CM NO DEBE cambiar la ubicación de la derivación principal en el mensaje RNG-RSP. Si la estructura del ecualizador CM implementa un número de coeficientes diferente del de definidos en el mensaje RNG-RSP, el CM PUEDE variar la ubicación del valor de la derivación principal. Al hacer eso, el CM DEBE, de nuevo, ajustar su desplazamiento de alineación, además de cualquier otro ajuste en el mensaje RNG-RSP, en una cantidad que compense la variación de la ubicación de la derivación principal.

B.6.2.7 Perfiles de ráfagas

Las características de la transmisión se dividen en tres categorías:

a) parámetros de canal;

b) atributos de perfil de ráfaga; y

c) parámetros exclusivos del usuario.

Los parámetros de canal incluyen:

i) la velocidad de símbolos (cinco velocidades, desde 160 ksímb/s a 2,56 Msímb/s en pasos de octava);

ii) la frecuencia central (Hz); y

iii) la supercadena de preámbulo de 1024 bits.

La descripción de los parámetros de canal prosigue con más detalle en el cuadro B.8-18; esas características son compartidas por todos los usuarios en un canal determinado. La relación de los atributos de perfil de ráfaga figura en el cuadro B.6-4 y se describen con más detalle en el cuadro B.8-19; estos parámetros son los atributos compartidos correspondientes a un tipo de ráfaga. Los parámetros exclusivos del usuario pueden variar para cada usuario incluso cuando utilizan el mismo tipo de ráfaga por el mismo canal que otro usuario (por ejemplo, el nivel de potencia) y su relación figura en el cuadro B.6-5.

Cuadro B.6-4/J.112 – Parámetros de ráfagas de canal

Parámetro	Fijaciones de configuración
Modulación	QPSK, 16QAM
Codificación diferencial	Activa/inactiva
Longitud del preámbulo	0 a 1024 bits (véase B.6.2.5)
Desplazamiento de valor de preámbulo	0 a 1022
Corrección de errores FEC (T)	0 a 10 (0 implica la ausencia de FEC. El número de octeto de paridad de la palabra de código es $2^{*}T$)
Octetos de información de la palabra de código FEC(k)	Fija: 16 a 253 (suponiendo FEC activa) Abreviada: 16 a 253 (suponiendo FEC activa)
Semilla del aleatorizador	15 bits
Longitud de ráfaga máxima (miniintervalos de tiempo) (véase la nota)	0 a 255
Tiempo de guarda	5 a 255 símbolos
Longitud de última palabra de código	Fija, abreviada
Aleatorizador activo/inactivo	Activo/inactivo
NOTA – Una longitud de ráfaga de 0 miniintervalos de tiempo en el perfil del canal significa que la longitud de las ráfagas es variable en ese canal para ese tipo de ráfaga. La longitud de ráfaga, aunque no sea fija, la adjudica explícitamente el CMTS al CM en el MAP.	

Cuadro B.6-5/J.112 – Parámetros en ráfaga exclusivos de usuario

Parámetro	Fijaciones de configuración
Nivel de potencia (véase la nota)	+8 dBmV a +55 dBmV (16QAM) +8 dVmV a +58 dBmV (QPSK) 1 dB pasos
Frecuencia de desplazamiento (véase la nota)	Gama = ±32 kHz; incremento = 1 Hz; implementación ±10 Hz
Desplazamiento de la alineación	0 a $(2^{16} – 1)$, incrementos de 6,25 μs/64
Longitud de ráfaga (miniintervalos de tiempo) si es variable en este canal (cambia de ráfaga a ráfaga)	1 a 255 miniintervalos de tiempo
Coeficientes de ecualizador de transmisión (véase la nota) (módems avanzados solamente)	Hasta 64 coeficientes; 4 octetos por coeficiente: 2 reales y 2 complejos
NOTA – Los valores del cuadro son aplicables para este determinado canal y esta precisa velocidad de símbolos.	

El CM DEBE generar cada ráfaga en el momento apropiado indicado en las concesiones de miniintervalos de tiempo proporcionadas por los MAP del CMTS (véase B.8.3.4).

El CM DEBE admitir todos los perfiles de ráfaga indicados por el CMTS vía descriptores de ráfaga UCD (véase B.8.3.3) y originados subsiguientemente para transmisión en un MAP (véase B.8.3.4).

El CM DEBE implementar la frecuencia de desplazamiento con una aproximación de ±10 Hz.

El desplazamiento de alineación es la corrección de retardo aplicada por el CM al tiempo de trama en sentido ascendente del CMTS derivado en el CM. Es un avance equivalente aproximadamente al tiempo de propagación de ida y vuelta del CM con respecto CMTS, y es necesario para sincronizar las transmisiones en sentido ascendente en el esquema TDMA. El desplazamiento de alineación es

un avance equivalente aproximadamente al tiempo de propagación de ida y vuelta del CM con respecto al CMTS. El CMTS DEBE proporcionar al CM la corrección de este desplazamiento por realimentación, en base a la recepción satisfactoria de una o más ráfagas (es decir, resultado satisfactorio de cada una de las técnicas empleadas: corrección de errores y/o CRC), con una exactitud de 1/2 símbolo o mejor y una resolución de 1/64 del incremento de tics de trama (6,25 μs/64 = 0,09765625 μs = 1/4 de la duración de un símbolo de la velocidad de símbolos más elevada = 10,24 MHz^{-1}). El CMTS envía ajustes al CM, en donde un valor negativo significa que el desplazamiento de alineación se ha de disminuir, dando lugar a tiempos de transmisión posteriores en el CM. El CM DEBE implementar la corrección con una resolución equivalente a la duración de 1 símbolo como máximo (de la velocidad de símbolos utilizada para una ráfaga dada), y (aparte de un sesgo fijo) con una exactitud de ±0,25 μs más ±1/2 símbolo debido a la resolución. La exactitud de la temporización de ráfagas del CM de ±0,25 μs más ±1/2 símbolo está referida a los límites del miniintervalo de tiempo obtenible en el CM, en base a un procesamiento ideal de las señales de indicación de tiempo recibidas del CMTS.

El CM DEBE ser capaz de cambiar de perfiles de ráfagas sin que se requiera tiempo de reconfiguración entre ráfagas, salvo en el caso en que cambien los siguientes parámetros:

1) potencia de salida;
2) modulación;
3) velocidad de símbolos;
4) frecuencia de desplazamiento;
5) frecuencia de canal; y
6) desplazamiento de alineación.

Para velocidad de símbolos, frecuencia de desplazamiento y desplazamiento de alineación, el CM DEBE ser capaz de transmitir ráfagas consecutivas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente. El tiempo de reconfiguración máximo de 96 símbolos debe competir por el tiempo de rampa descendente de una ráfaga y el tiempo de rampa ascendente de la ráfaga siguiente así como el tiempo de retardo de transmisión total incluyendo el retardo de conducto y el retardo del ecualizador previo opcional. Para cambios de tipo de modulación, el CM DEBE ser capaz de transmitir ráfagas consecutivas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente. La potencia de salida transmitida, la velocidad de símbolos, la frecuencia de desplazamiento y el desplazamiento de alineación NO DEBEN cambiar mientras esté pendiente de transmisión más de −30 dB de la energía de cualquier símbolo de la ráfaga anterior, o si se ha transmitido más de –30 dB de la energía de cualquier símbolo de la ráfaga siguiente. La modulación NO DEBE cambiar mientras esté pendiente de transmisión más de –30 dB de la energía de cualquier símbolo de la ráfaga anterior, o si se ha transmitido más de –30 dB de la energía de cualquier símbolo de la ráfaga siguiente, EXCLUYENDO el efecto del ecualizador (si está presente en el CM). [Esto se ha de verificar cuando el ecualizador de transmisión no proporcione filtrado; sólo retardo, en todo caso. Se señala que si el CMTS tiene retroalimentación de decisión en su ecualizador, quizás necesite proporcionar más que el intervalo de 96 símbolos entre las ráfagas de tipo de modulación diferente que puede utilizar el CM; el CMTS tiene que decidir al respecto.] Ajustes por desplazamiento de alineación negativo harán que se viole el tiempo de guarda de los 96 símbolos. El CMTS tiene que garantizar que esto no ocurre permitiendo un tiempo de guarda adicional entre ráfagas que sea por lo menos igual al desplazamiento de alineación negativo.

Si se ha de cambiar la frecuencia del canal, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 100 ms entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

La frecuencia de canal del CM DEBE estabilizarse teniendo en cuenta los requisitos de ruido de fase y exactitud de B.6.2.10.5 y B.6.2.10.6 dentro de los 100 ms que siguen al comienzo del cambio.

Si la potencia de salida se va a cambiar en 1 dB o menos, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 5 µs entre el centro del último símbolos de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

Si la potencia de salida se va a cambiar en más de 1 dB, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 10 µs entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

La potencia de salida del CM DEBE estabilizarse a ±0,1 dB o menos de su nivel de potencia de salida final:

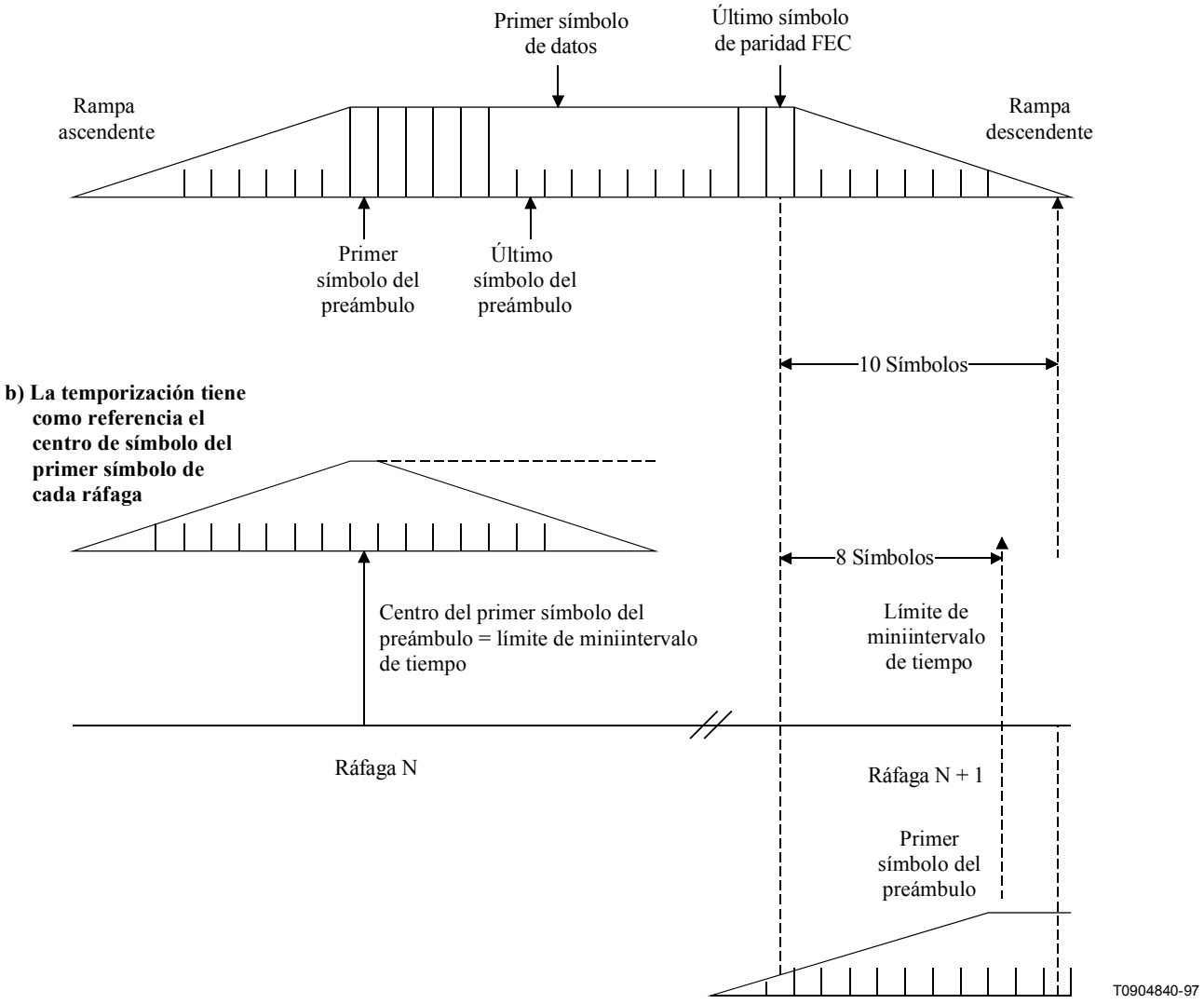
a) dentro de los 5 µs a partir del comienzo de un cambio de 1 dB o menos; y

b) dentro de los 10 µs a partir del comienzo de un cambio de más de 1 dB.

La potencia transmisión de salida DEBE mantenerse constante dentro de una ráfaga TDMA a menos de 0,1 dB (excluyendo la cantidad presente en teoría a causa de la conformación del impulso, y a la modulación de amplitud en caso de 16QAM).

B.6.2.8 Convenio de temporización de ráfagas

La figura B.6-6 ilustra la temporización de una ráfaga nominal.



NOTA – La rampa descendente de una ráfaga puede solapar la rampa ascendente de la ráfaga siguiente incluso cuando un transmisor tiene asignadas ambas ráfagas.

Figura B.6-6/J.112 – Temporización de ráfaga nominal

La figura B.6-7 indica la temporización de una ráfaga en el caso más desfavorable. En este caso, la ráfaga N llega con 1,5 símbolos de retardo y la ráfaga N + 1 llega con 1,5 símbolos de adelanto, pero se mantiene la separación de 5 símbolos; se muestra la banda de guarda de 8 símbolos.

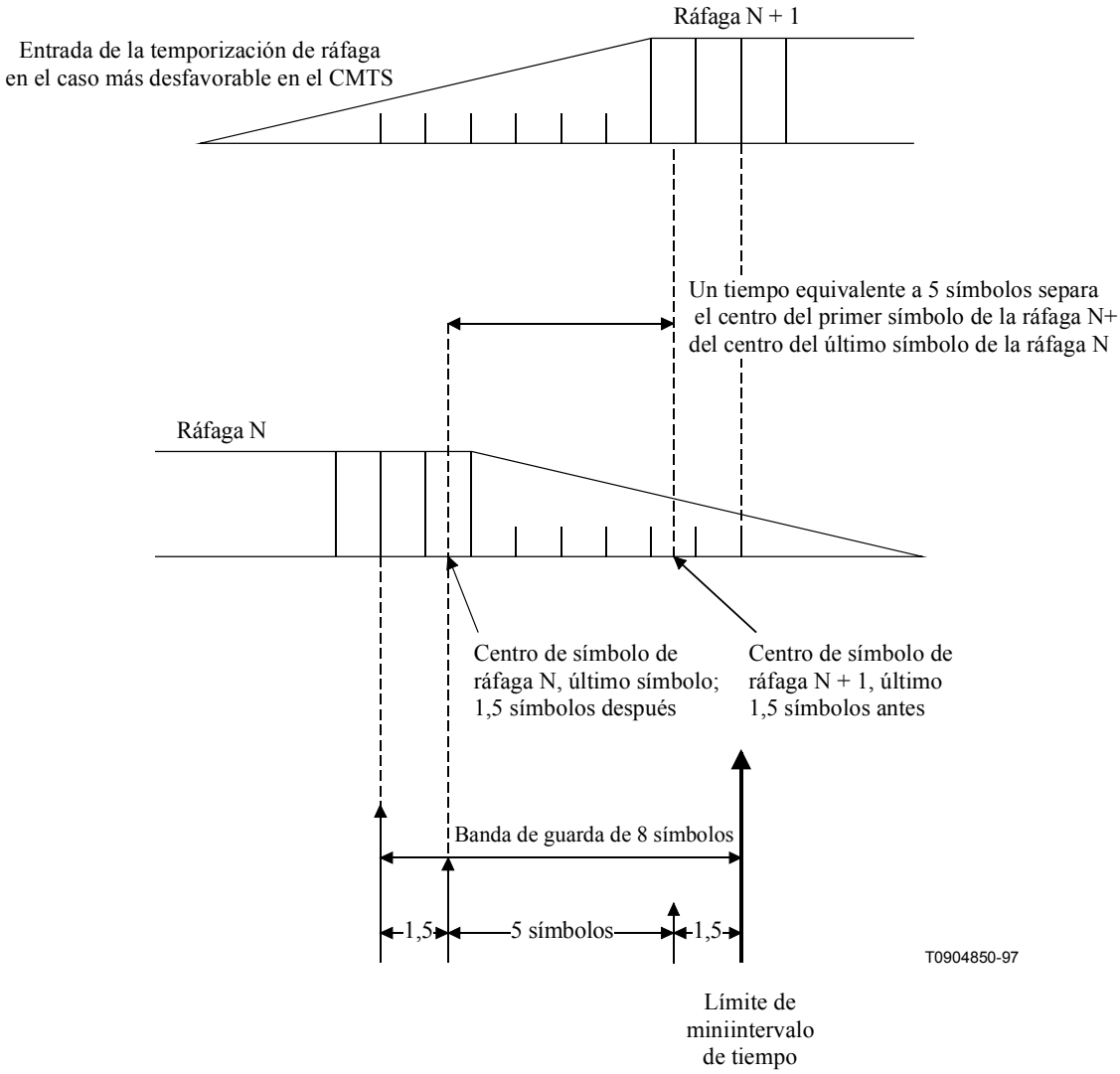


Figura B.6-7/J.112 – Temporización de ráfaga en el caso más desfavorable

Con una velocidad de símbolos de R_S, los símbolos se producen con una cadencia de uno cada $T_S = 1/R_S$ segundos. Las rampas ascendente y descendente representan la dispersión de un símbolo en el dominio temporal más allá del periodo de duración T_S debido al filtro de conformación de símbolos. Si sólo se transmitiera un símbolo, su duración sería superior a T_S porque la respuesta en impulsos del filtro de conformación es superior a T_S. La dispersión del primero y el último símbolos de una transmisión de ráfaga amplía efectivamente la duración de la ráfaga haciendo que sea superior a N $\times$ T_S, donde N es el número de símbolos de la ráfaga.

B.6.2.9 Requisitos con respecto a la potencia de la transmisión

La subcapa PMD en sentido ascendente DEBE soportar la variación de la cantidad de potencia de la transmisión. Se establecen requisitos con respecto a:

1) la gama de potencia de transmisión pedida;
2) el tamaño de los pasos de las peticiones de potencia; y
3) la exactitud (potencia de salida efectiva en comparación con la cantidad pedida) de la respuesta a la petición.

El mecanismo según el cual se efectúan los ajustes de potencia se define en B.11.2.4. Dichos ajustes DEBEN quedar dentro de las gamas de tolerancia que se describen a continuación.

B.6.2.9.1 Agilidad y gama de la potencia de salida

La potencia de transmisión de salida en la anchura de banda de diseño DEBE ser variable en la gama de +8 dBmV a 55 dBmV (16QAM), 58 dBmV (QPSK), en pasos de 1 dB.

La exactitud absoluta de la potencia transmitida DEBE ser de ±2 dB, y la del tamaño de los pasos, de ±0,4 dB, con un margen por histéresis al activar/desactivar un atenuador por etapas (por ejemplo, 20 dB) en cuyo caso el requisito de exactitud se rebaja a ±1,4 dB. Por ejemplo, el incremento efectivo de potencia resultante de una petición de que se aumente el nivel de potencia en 1 dB en la siguiente ráfaga transmitida de un CM DEBE estar entre 0,6 y 1,4 dB.

La resolución de un paso DEBE ser de 1 dB o menos. Cuando a un CM se le indique una resolución mayor de la que él puede implementar, DEBE redondear al tamaño de paso soportado más cercano. Si el paso indicado está a mitad de camino entre dos tamaños de paso soportados, el CM DEBE elegir el paso más pequeño. Por ejemplo, con una resolución de paso soportada de 1 dB, la indicación de variar en ±0,5 dB no provocaría variación alguna, mientras que una indicación de variación de ±0,75 dB daría lugar a una variación o paso de ±1 dB.

B.6.2.10 Requisitos de fidelidad

B.6.2.10.1 Emisiones espurias

El ruido y la potencia espuria NO DEBEN exceder de los niveles que se indican en los cuadros B.6-6, B.6-7 y B.6-8.

Cuadro B.6-6/J.112 – Emisiones espurias

Parámetro	Ráfaga transmisora	Entre ráfagas
Dentro de banda [entre las emisiones espurias dentro de banda figuran el ruido, la fuga de portadora, las líneas de reloj, los productos espurios de sintetizador y otros productos de transmisor no deseados. No se incluye la interferencia entre símbolos (ISI, *inter symbol interference*)]	–40 dBc	–72 dBc o –59 dBmV, lo que sea mayor
Banda adyacente	Véase el cuadro B.6-7	–72 dBc o –59 dBmV, lo que sea mayor
Tres bandas de frecuencia o menos relacionadas con la portadora (a modo de segundo armónico, si < 42 MHz)	–47 dBc	–72 dBc o –59 dBmV, lo que sea mayor
Bandas dentro de 5 a 42 MHz (excluyendo el canal asignado, los canales adyacentes y los canales relacionados con la portadora)	Véase el cuadro B.6-8	–72 dBc o –59 dBmV, lo que sea mayor
Límites de las emisiones espurias integradas en el CM (todas en 4 MHz, incluidos valores discretos) (nota 1)		
42 MHz a 54 MHz	máx (–40 dBc, –26 dBmV)	–26 dBmV
54 MHz a 60 MHz	–35 dBmV	–40 dBmV
60 MHz a 88 MHz	–40 dBmV	–40 dBmV
88 MHz a 860 MHz	–45 dBmV	máx (–45 dBmV, –40 dBc) (Nota 2)

Cuadro B.6-6/J.112 – Emisiones espurias

Parámetro	Ráfaga transmisora	Entre ráfagas
Límites de las emisiones espurias discretos en el CM (Nota 1)		
42 MHz a 54 MHz	máx (–50 dBc, –36 dBmV)	–36 dBmV
54 MHz a 88 MHz	–50 dBmV	–50 dBmV
88 MHz a 860 MHz	–50 dBmV	–50 dBmV
NOTA 1 – Estos límites de especificador excluyen una salida espuria discreta única relacionada con el canal recibido sintonizado; la salida espuria discreta única no DEBE ser superior a –40 dBmV.		
NOTA 2 – "dBc" se refiere al nivel de señal recibida en sentido descendente. Algunas salidas espurias son proporcionales al nivel de señal en recepción.		

Cuadro B.6-7/J.112 – Emisiones espurias en canal adyacente, relativas al nivel de potencia de ráfaga transmitido

Velocidad de símbolos de la portadora transmitida	Especificación en el intervalo	Intervalo de medición y distancia con respecto al borde de la portadora	Velocidad de símbolos de la portadora del canal adyacente
160 ksímb/s	–45 dBc	20 kHz a180 kHz	160 ksímb/s
	–45 dBc	40 kHz a 360 kHz	320 ksímb/s
	–45 dBc	80 kHz a 720 kHz	640 ksímb/s
	–42 dBc	160 kHz a 1440 kHz	1280 ksímb/s
	–39 dBc	320 kHz a 2880 kHz	2560 ksímb/s
Todas las demás velocidades de símbolos	–45 dBc	20 kHz a 180 kHz	160 ksímb/s
	–45 dBc	40 kHz a 360 kHz	320 ksímb/s
	–45 dBc	80 kHz a 720 kHz	640 ksímb/s
	–44 dBc	160 kHz a 1440 kHz	1280 ksímb/s
	–41 dBc	320 kHz a 2880 kHz	2560 ksímb/s

Cuadro B.6-8/J.112 – Emisiones espurias en 5 a 42 MHz, relativas al nivel de potencia de ráfaga transmitido

Posible velocidad de símbolos en este intervalo	Especificación en el intervalo	Intervalo de medición inicial y distancia con respecto al borde de la portadora
160 ksímb/s	–53 dBc	220 kHz a 380 kHz
320 ksímb/s	–50 dBc	240 kHz a 560 kHz
640 ksímb/s	–47 dBc	280 kHz a 920 kHz
1280 ksímb/s	–44 dBc	360 kHz a 1640 kHz
2560 ksímb/s	–41 dBc	520 kHz a 3080 kHz

En el cuadro B.6-6, las emisiones espurias dentro de banda incluyen el ruido, la fuga de portadora, las líneas de reloj, los productos espurios de sintetizador y otros productos de transmisor no deseados. No incluye ISI. La anchura de banda de medición de las emisiones espurias dentro de banda es igual a la velocidad de símbolos (por ejemplo, 160 kHz para 160 ksímb/s).

La anchura de banda de medición de las 3 (o menos) bandas de frecuencia relacionadas con la portadora (por debajo de 42 MHz) es de 160 kHz, con 3 bandas como máximo de 160 kHz, cada una de ellas con no más de –47 dBc, que se permite excluir de las especificaciones de "Bandas dentro de 5 MHz a 42 MHz de la ráfaga transmisora" del cuadro B.6-8.

La anchura de banda de medición es también de 160 kHz para las especificaciones entre ráfagas del cuadro B.6-6 por debajo de 42 MHz; las especificaciones de ráfagas transmisoras son aplicables durante los miniintervalos de tiempo concedidos al CM (cuando el CM utiliza la totalidad o una parte de la concesión), y durante un miniintervalo de tiempo antes y después de los miniintervalos de tiempo concedidos. (Se señala que un miniintervalo de tiempo puede ser tan breve como 32 símbolos, o 12,5 µs a la velocidad de 2,56 Msímb/s, o 200 µs a 160 ksímb/s.) Las especificaciones de ráfagas transmisoras se aplican salvo durante la utilización de una concesión de miniintervalos de tiempo, y durante el miniintervalo de tiempo anterior y el posterior a la concesión utilizada.

B.6.2.10.1.1 Emisiones espurias en canal adyacente

Las emisiones espurias procedentes de una portadora transmitida pueden producirse en un canal adyacente que pudiera estar ocupado por una portadora con las mismas o diferentes velocidades de símbolos. El cuadro B.6-7 contiene la relación de niveles de emisiones espurias en canal adyacente requeridos para todas las combinaciones de velocidades de símbolos de portadora transmitida y velocidades de símbolos de canal adyacente. La medición se efectúa en un intervalo de canal adyacente cuya anchura de banda y distancia con respecto a la portadora transmitida son las apropiadas en base a las velocidades de símbolos de la portadora transmitida y la portadora del canal adyacente.

B.6.2.10.1.2 Emisiones espurias en 5 a 42 MHz

Las emisiones espurias, distintas de las del canal adyacente o las emisiones relacionadas con la portadora e indicadas en el cuadro B.6-7, se pueden producir en intervalos que podrían estar ocupados por otras portadoras, con las mismas o diferentes velocidades de símbolos. Para acomodar estas velocidades de símbolos diferentes y anchuras de banda asociadas, las emisiones espurias se miden en un intervalo igual a la anchura de banda correspondiente a la velocidad de símbolos de la portadora que pudiera ser transmitida en ese intervalo. Ese intervalo es independiente de la velocidad con que se transmitan los símbolos en ese momento.

El cuadro B.6-8 contiene la relación de posibles velocidades de símbolos que pudieran ser transmitidas en un intervalo, el nivel de emisión espuria requerido en ese intervalo, y el nivel de medición inicial en que se han de empezar a medir las emisiones espurias. Las mediciones deberán comenzar en la distancia inicial y repetirse con distancias crecientes con respecto a la portadora hasta que se alcance el borde de la banda en sentido ascendente, 5 MHz o 42 MHz. Los intervalos de medición no deberán incluir emisiones relacionadas con la portadora.

B.6.2.10.2 Emisiones espurias durante los transitorios de activación/desactivación en ráfagas

Cada transmisor DEBE controlar las emisiones espurias, antes y durante la rampa ascendente y durante y después de la rampa descendente, con anterioridad y con posterioridad a una ráfaga en el esquema TDMA.

Las emisiones espurias de activación/desactivación, tales como las del cambio de tensión a la salida de un transmisor en sentido ascendente debido a la habilitación o inhabilitación de la transmisión, no DEBEN ser superiores a 100 mV, y ese paso incremental no DEBE disiparse antes de 2 µs siguiendo

un desarrollo de pendiente constante. Este requisito se aplica cuando el CM transmite a +55 dBmV o más; con niveles de transmisión reducidos, el cambio máximo de tensión DEBE disminuir con un factor de 2 para cada 6 dB de disminución del nivel de potencia a partir de +55 dBmV, hasta un cambio máximo de 7 mV a 31 dBmV y por debajo. Este requisito no es aplicable a los transitorios de activación y desactivación de potencia del CM.

B.6.2.10.3 Tasa de errores en los símbolos (SER)

La calidad de funcionamiento del modulador DEBE ser tal que su salida se encuentre a 0,5 dB o menos de la SER teórica en función de la relación C/N (es decir, E_s/N_o), para una SER tan baja como 10^{-6} sin codificación, para QPSK y 16QAM.

La degradación de la SER viene determinada por la varianza de conglomerado que provoca la forma de onda de transmisión a la salida de un filtro teórico de recepción de raíz cuadrada de coseno alzado. Incluye los efectos de la ISI, las emisiones espurias, el ruido de fase, y todas las demás degradaciones del transmisor.

La relación señal/ruido (SNR, *signal/noise ratio*) deberá medirse en un analizador de modulación que utilice filtro de recepción de raíz cuadrada de coseno alzado con alfa = 0,25. La SNR medida DEBE ser superior a 30 dB.

El CM DEBE ser capaz de obtener una SNR de agrupación de al menos 27 dB, en presencia de las microrreflexiones de canal definidas en el cuadro B.4-2. Puesto que el cuadro no pone límites al retardo del eco en el caso de −30 dBc, se supone a efectos de pruebas que la duración eco con esa magnitud es menor o igual que 1,5 μs.

B.6.2.10.4 Distorsión de filtro

En los requisitos que siguen se supone que cualquier ecualización previa queda inhabilitada.

B.6.2.10.4.1 Amplitud

La plantilla del espectro DEBE ser el espectro teórico de raíz cuadrada de coseno alzado con alfa = 0,25, dentro de las gamas que se indican en el cuadro B.6-9.

Cuadro B.6-9/J.112 – Amplitud de distorsión de filtro

Frecuencia	Gama de amplitudes	
	baja	alta
$f_c - 5\ R_s$	–	–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
$f_c + 5\ R_s/8$	–	–30 dB

Donde f_c es la frecuencia central, R_s es la velocidad de símbolos y la densidad espectral se mide con una anchura de banda de resolución de 10 kHz o menos.

B.6.2.10.4.2 Fase

$f_c - 5R_s/8$ Hz a $f_c + 5\ R_s/8$ Hz: la variación del retardo de grupo NO DEBE ser superior a 100 ns.

B.6.2.10.5 Ruido de fase de portadora

El ruido de fase integrado total del transmisor en sentido ascendente (incluido el ruido parásito discreto) DEBE ser inferior o igual a –43 dBc, teniendo en cuenta las regiones espectrales que se extienden de 1 kHz a 1,6 MHz por encima y por debajo de la portadora.

B.6.2.10.6 Exactitud de la frecuencia de canal

El CM DEBE implementar la frecuencia de canal asignada con una exactitud de ±50 partes por millón con una gama de temperaturas de 0° C a 40° C hasta cinco años después de la fecha de fabricación.

B.6.2.10.7 Exactitud de la velocidad de símbolos

El modulador en sentido ascendente DEBE proporcionar una exactitud absoluta de velocidad de símbolos de ±50 partes por millón con una gama de temperaturas de 0° C a 40° C hasta cinco años después de la fecha de fabricación.

B.6.2.10.8 Fluctuación de fase de la temporización de símbolos

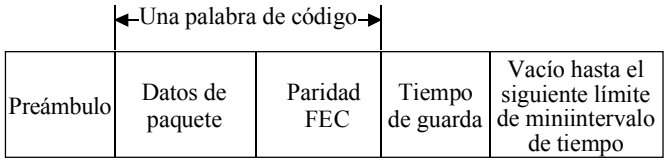
La fluctuación de fase cresta a cresta de los símbolos, referida al cruce de cero de símbolos, de la forma de onda transmitida, será inferior al 0,02 de la duración nominal de un símbolo durante un periodo de 2 s. En otras palabras, la diferencia entre la duración máxima y mínima de un símbolo durante el periodo de 2 s deberá ser inferior al 0,02 de la duración nominal de un símbolo para cada una de las cinco velocidades de símbolos en sentido ascendente.

El error de fase acumulado cresta a cresta, referido al momento del primer símbolo y descontado cualquier desplazamiento fijo de la frecuencia de símbolos, DEBE ser inferior al 0,04 de la duración nominal de un símbolo durante un periodo de 0,1 s. En otras palabras, la diferencia entre el error de fase acumulado máximo y mínimo durante el periodo de 0,1 s deberá ser inferior al 0,04 de la duración nominal de un símbolo para cada una de las cinco velocidades de símbolos en sentido ascendente. La eliminación de un desplazamiento fijo de la frecuencia de símbolos se ha de hacer utilizando la duración media de los símbolos calculada durante el periodo de 0,1 s.

B.6.2.11 Estructura de trama

La figura B.6-8 muestra dos ejemplos de estructura de trama; uno en el que la longitud de los paquetes es igual al número de octetos de información de una palabra de código, y otro en el que la longitud de los paquetes es superior al número de octetos de información de una palabra de código, pero inferior al de dos palabras de código. El ejemplo 1 ilustra el modo longitud de palabra de código fija, y el ejemplo 2, el modo última palabra de código abreviada. Ambos modos se definen en B.6.2.11.1.

Ejemplo 1 – Longitud de paquete = número de bytes de información de la palabra de código = k



Ejemplo 2 – Longitud de paquete = k + bytes de información restantes en la segunda palabra de código = $k + k' \leq k + k'' \leq 2k$ bytes

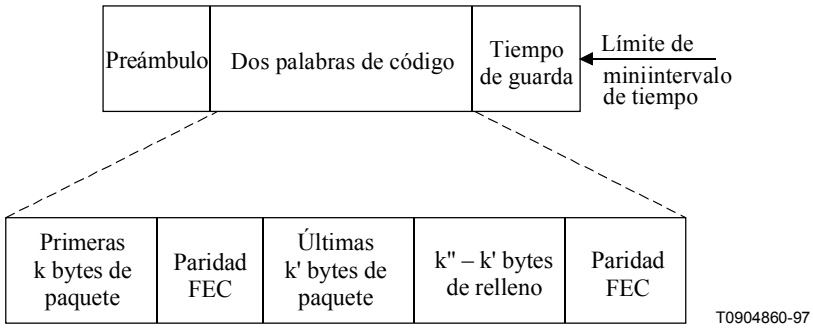


Figura B.6-8/J.112 – Ejemplo de estructura de trama con modo longitud de ráfagas

B.6.2.11.1 Longitud de palabra de código

Cuando FEC está habilitada, el CM funciona en modo palabra de código de longitud fija o en modo última palabra de código abreviada. El número mínimo de octetos de información en una palabra de código en cualquiera de los modos es 16. El modo última palabra de código abreviada sólo resulta ventajoso cuando el número de octetos en una palabra de código es superior al mínimo de 16 octetos.

Las descripciones que siguen son aplicables a una concesión de miniintervalos de tiempo atribuida tanto en regiones de competencia como de no competencia. (La atribución de miniintervalos de tiempo se examina en B.8.) La descripción tiene por objeto definir las reglas y los convenios que permitan a los CM pedir el número adecuado de miniintervalos de tiempo y que la capa PHY del CMTS sepa lo que cabe esperar con respecto a la alineación de trama FEC, tanto en el modo longitud de palabra de código fija como en el modo última palabra de código abreviada.

B.6.2.11.1.1 Longitud de palabra de código fija

Con las palabras de código de longitud fija, una vez codificados todos los datos, se rellenarán con octetos de valor cero si tal cosa hace falta para alcanzar los k octetos de datos asignados por palabra de código, y el relleno con octetos de valor cero DEBE continuar hasta que ya no puedan insertase más palabras de código de longitud fija antes del final del último miniintervalo de tiempo atribuido en la concesión, teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda.

B.6.2.11.1.2 Última palabra de código abreviada

Como se muestra en la figura B.6-8, k' es el número de octetos de información que quedan después de dividir los octetos de información de la ráfaga en palabras de código de longitud total (k octetos de datos en ráfaga). El valor de k' es inferior al de k. Suponiendo funcionamiento en modo última palabra de código abreviada, sea k'' el número de octetos de datos de la ráfaga más los octetos de relleno de valor cero de la última palabra de código abreviada. En el modo palabra de código abreviada, el CM DEBE codificar los octetos de datos de la ráfaga (incluido el encabezamiento MAC) utilizando el tamaño de palabra de código asignado (k octetos de información por palabra de código) hasta que:

1) todos los datos estén codificados; o

2) quede un resto de octetos de datos inferior a k.

Las últimas palabras de código abreviadas NO DEBERÁN tener menos de 16 octetos de información, y esto es algo que hay que tener en cuenta cuando los CM pidan miniintervalos de tiempo. En el modo última palabra de código abreviada, el CM se deberá llenar con datos de valor cero si es necesario hasta el final de la atribución del miniintervalo de tiempo, lo que la mayoría de las veces ocurrirá en el siguiente límite de un miniintervalo de tiempo, teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda. En muchos casos, sólo serán necesarios k'' – k' octetos de relleno de valor cero para llenar una atribución de miniintervalos de tiempo con $16 \leq k'' \leq k$ y $k' \leq k''$. No obstante, conviene tener en cuenta lo que sigue.

De manera más general, el CM DEBE rellenar datos con octetos de valor cero hasta que ya no puedan insertarse más palabras de código de longitud fija antes del final del último miniintervalo de tiempo atribuido en la concesión (teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda), y a continuación, si se puede, DEBE insertarse una última palabra de código abreviada de relleno con octetos de valor cero para que encaje en la atribución de miniintervalos de tiempo.

Si, tras rellenar con octetos de valor cero palabras de código adicionales de k octetos de información quedan menos 16 octetos en la concesión atribuida de miniintervalos de tiempo, teniendo en cuenta los símbolos de paridad y tiempo de guarda, el CM no deberá crear esta última palabra de código abreviada.

B.6.2.12 Requisitos del procesamiento de la señal

El orden de procesamiento de una señal para cada tipo de paquete en ráfaga DEBE ser compatible con la secuencia que se muestra en la figura B.6-9 y DEBE seguir el orden de los pasos que se indica en la figura B.6-10.

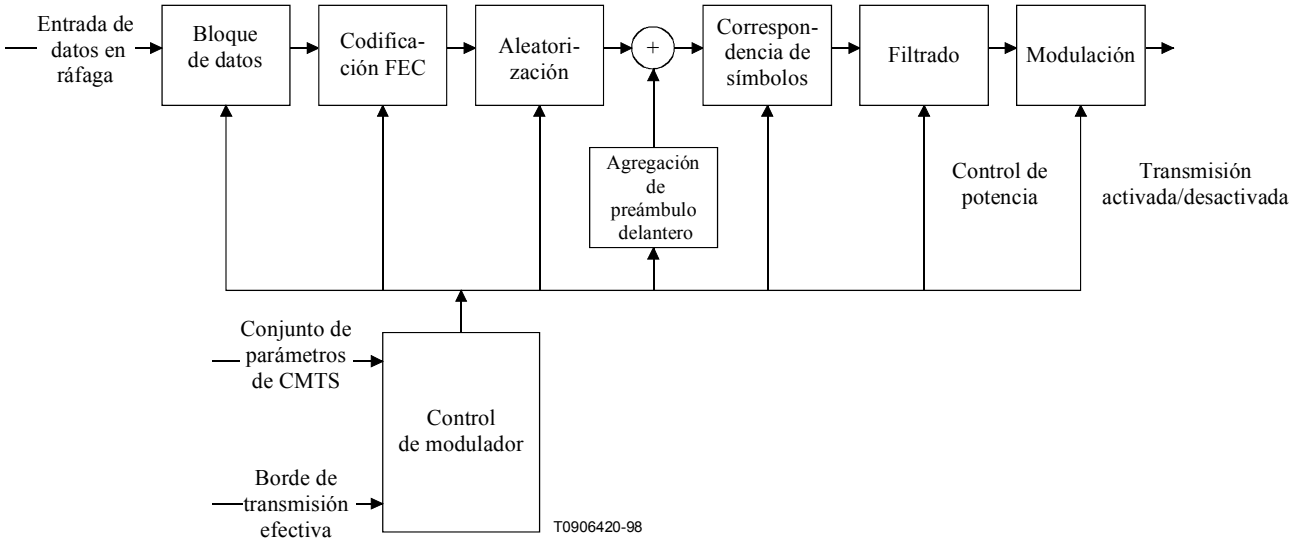


Figura B.6-9/J.112 – Secuencia de procesamiento de señal

	Entrada de tren de paquetes
	⇓
Bloques de datos	Separación de paquetes en bloques de información (= octetos de datos en una palabra de código)
	⇓
Codificación FEC	Codificación FEC (Reed-Solomon) de cada bloque de información, utilizando una palabra de código abreviada para el último bloque si es necesario. La FEC puede ser desactivada
	⇓
Aleatorización	Aleatorización (véase B.6.2.4)
	⇓
Agregación de preámbulo delantero	Símbolos de agregación de preámbulo delantero
	⇓
Correspondencia de símbolos	Correspondencia entre símbolos del tren de datos y símbolos del modulador
	⇓
Filtrado	Filtrado del tren de símbolos para conformación del espectro
	⇓
Modulación	Modulación en tiempos precisos (QPSK; 16QAM)
	⇓
	Salida de ráfagas de formas de onda RF

Figura B.6-10/J.112 – Procesamiento de la transmisión en sentido ascendente con TDMA

B.6.2.13 Características de la potencia de entrada en el demodulador en el sentido ascendente

La potencia de entrada total máxima en el demodulador en sentido ascendente NO DEBE exceder de 35 dBmV en la gama de frecuencias de funcionamiento de 5 MHz a 42 MHz.

El valor de la potencia que se trata de recibir en cada portadora DEBE estar entre los que se muestran en el cuadro B.6-10.

Cuadro B.6-10/J.112 – Gama máxima de potencia de recepción nominal pedida en cada portadora

Velocidad de símbolos (ksímb/s)	Gama máxima (dBmV)
160	–16 to +14
320	–13 to +17
640	–10 to +20
1280	–7 to +23
2560	–4 to +26

El demodulador DEBE ateniéndose a sus especificaciones definidas de calidad de funcionamiento con ráfagas recibidas dentro de un margen de ±6 dB con respecto a la potencia de recepción nominal pedida.

B.6.2.14 Salida eléctrica del CM en sentido ascendente

El CM DEBE producir como salida una señal modulada RF con las características que se indican en el cuadro B.6-11.

Cuadro B.6-11/J.112 – Salida eléctrica del CM

Parámetro	Valor
Frecuencia	5 MHz a 42 MHz borde a borde
Gama de niveles (un canal)	+8 dBmV a +55 dBmV (16QAM) +8 dBmV a +58 dBmV (QPSK)
Tipo de modulación	QPSK y 16QAM
Velocidad de símbolos (nominal)	160, 320, 640, 1280 y 2560 ksímb/s
Anchura de banda	200, 400, 800, 1600 y 3200 kHz
Impedancia de salida	75 ohmios
Pérdida de retorno de salida	> 6 dB (5 MHz a 42 MHz)
Conector	Conector F según CEI 60169-24 (común con la entrada)

B.6.3 Sentido descendente

B.6.3.1 Protocolo en sentido descendente

La subcapa PMD en sentido descendente DEBE atenerse a [UIT-T J.83-B] para aplicaciones vídeo de bajo retardo, con las excepciones a las que se refiere B.6.3.2.

NOTA – Cualquier referencia en el presente anexo B a la transmisión de televisión en el canal ver que no sea coherente con [EN 300 429], queda fuera del alcance normativo al ser [EN 300 429] utilizada solamente para la distribución de televisión digital multiprograma en las aplicaciones europeas. Véase B.1.1.

B.6.3.2 Intercalación escalable para soportar baja latencia

La subcapa PMD en el sentido descendente DEBE soportar un intercalador de profundidad variable con las características definidas en el cuadro B.6-12. Este cuadro contiene un subconjunto de los modos de intercalador que figuran en [UIT-T J.83-B].

Cuadro B.6-12/J.112 – Características del intercalador

I (Número de derivaciones)	J (Incremento)	Protección contra ráfagas 64QAM/256QAM	Latencia 64QAM/256QAM
8	16	5,9 µs/4,1 µs	0,22 ms/0,15 ms
16	8	12 µs/8,2 µs	0,48 ms/0,33 ms
32	4	24 µs/16 µs	0,98 ms/0,68 ms
64	2	47 µs/33 µs	2,0 ms/1,4 ms
128	1	95 µs/66 µs	4,0 ms/2,8 ms

La profundidad del intercalador, que se codifica en una palabra de control de 4 bits contenida en la cola de sincronismo de trama FEC, refleja siempre la intercalación en la trama que sigue inmediatamente. Además, se permiten errores mientras se vacía la memoria del intercalador después de que se haya indicado un cambio en la intercalación.

Véase [UIT-T J.83 B] a propósito de la especificación de bits de control requerida para indicar el modo de intercalación utilizado.

B.6.3.3 Plan de frecuencias en sentido descendente

El plan de frecuencias en sentido descendente deberá ser conforme a los planes de frecuencias de portadora relacionada con armónicas (HRC, *harmonic related carrier*), portadora relacionada con incrementos (IRC, *incremental related carrier*) o norteamericano normalizado (STD, *standard*) según [EIA 542]. Sin embargo, no es preciso el funcionamiento por debajo de una frecuencia central de 91 MHz.

B.6.3.4 Salida eléctrica del CMTS

El CMTS DEBE producir como salida una señal modulada RF con las características que se indican en el cuadro B.6-13.

Cuadro B.6-13/J.112 – Salida del CMTS

Parámetro	Valor
Frecuencia central (f_c)	91 MHz a 857 MHz ± 30 kHz (véase la nota)
Nivel	Ajustable en la gama de 50 dBmV a 61 dBmV
Tipo de modulación	64QAM y 256QAM
Velocidad de símbolos (nominal) 64QAM 256QAM	 5,056941 Msímb/s 5,360537 Msímb/s
Separación nominal de canales	6 MHz
Respuesta de frecuencia 64QAM 256QAM	 Conformación de raíz cuadrada de coseno alzado de ~18% Conformación de raíz cuadrada de coseno alzado de ~12%
Total de emisiones espurias discretas dentro de banda (f_c ± 3 MHz)	< –57 dBc
Emisiones espurias y ruido dentro de banda (f_c ± 3 MHz)	< –48 dBc. donde las emisiones espurias y el ruido del canal incluyen todas las emisiones espurias discretas, el ruido, la fuga de portadora, las líneas de reloj, los productos de sintetizador y otros productos del transmisor no deseados. Se excluye el ruido dentro de ±50 kHz de la portadora
Canal adyacente (f_c ± 3,0 MHz) a (f_c ± 3,75 MHz)	< –58 dBc en 750 kHz
Canal adyacente (f_c ± 3,75 MHz) a (f_c ± 9 MHz)	< –62 dBc en 5,25 MHz, excluyendo hasta tres señales espurias cada una de las cuales debe ser < –60 dBc cuando se mide en una banda de 10 kHz
Canal adyacente siguiente (f_c ± 9 MHz) a (f_c ± 15 MHz)	< –65 dBc en 6 MHz, excluyendo hasta tres señales espurias discretas. La potencia total de las derivaciones debe ser < –60 dBc cuando cada una de ellas se mide con una anchura de banda de 10 kHz
Otros canales (47 MHz a 1000 MHz)	< –12 dBmV en cada uno de los canales de 6 MHz, excluyendo hasta tres señales espurias discretas. La potencia total en las señales espurias debe ser < –60 dBc cuando cada una de ellas se mide con una anchura de banda de 10 kHz.

Cuadro B.6-13/J.112 – Salida del CMTS

Parámetro	Valor
Ruido de fase	1 kHz − 10 kHz: Potencia de ruido de doble banda lateral de −33 dBc 10 kHz − 50 kHz: Potencia de ruido de doble banda lateral de −51 dBc 50 kHz − 3 MHz: Potencia de ruido de doble banda lateral de −51 dBc
Impedancia de salida	75 ohmios
Pérdida de retorno de salida	> 14 dB dentro de un canal de salida de hasta 750 MHz; > 13 dB en un canal de salida por encima de 750 MHz
Conector	Conector F según [CEI 60169-24]
NOTA – ±30 kHz incluye un margen de 25 kHz para el mayor desplazamiento de frecuencia FCC que normalmente se acumula en los convertidores elevadores de frecuencia.	

B.6.3.5 Entrada eléctrica en el CM en sentido descendente

El CM DEBE ser capaz de aceptar y localizar una señal modulada RF ubicada en los canales definidos en [EIA 542] para la portadora relacionada con armónicas, (HRC), la portadora relacionada con incrementos (IRC), y el plan norteamericano de frecuencias. No se requiere el funcionamiento por debajo de una frecuencia central de 91 MHz. Las señales tendrán las características definidas en el cuadro B.6-14.

Cuadro B.6-14/J.112 – Entrada eléctrica en el CM

Parámetro	Valor
Frecuencia central	91 a 857 MHz ±30 kHz
Gama de niveles (un canal)	–15 dBmV a +15 dBmV
Tipo de modulación	64QAM y 256QAM
Velocidad de símbolos (nominal)	5,056941 Msímb/s (64QAM) y 5,360537 Msímb/s (256QAM)
Anchura de banda	6 MHz (conformación de raíz cuadrada de coseno alzado de 18% para 64QAM y conformación de raíz cuadrada de coseno alzado de 12% para 256QAM)
Potencia de entrada total (40-900 MHz)	< 30 dBmV
Impedancia de entrada (carga)	75 ohmios
Pérdida de retorno de entrada	> 6 dB (88 a 860 MHz)
Conector	Conector F según [CEI 60169-24] (común con la salida)

B.6.3.6 Características de VER de CM

La característica de tasa de errores en los bits de un CM DEBE ser tal como se describe en esta cláusula. Los requisitos son aplicables al modo de intercalación I = 128, J = 1.

B.6.3.6.1 64QAM

B.6.3.6.1.1 Característica de VER de CM con 64QAM

La pérdida de implementación de un CM DEBE ser tal que el CM tenga una VER después de la FEC inferior o igual a 10^{-8} cuando funciona con una relación portadora/ruido (E_s/N_o) de 23,5 dB o superior.

B.6.3.6.1.2 Característica de rechazo de imagen con 64QAM

La característica que se describe en B.6.3.6.1.1 DEBE cumplirse con una señal analógica o digital a +10 dBc en cualquier tramo de la banda RF distinto de los canales adyacentes.

B.6.3.6.1.3 Calidad del canal adyacente con 64QAM

La característica descrita en B.6.3.6.1.1 DEBE cumplirse con una señal digital a 0 dBc en los canales adyacentes.

La característica descrita en B.6.3.6.1 DEBE cumplirse con una señal analógica a +10 dBc en los canales adyacentes.

La calidad descrita en B.6.3.6.1.1, con un margen adicional de 0,2 dB, DEBE cumplirse con una señal digital a +10 dBc en los canales adyacentes.

B.6.3.6.2 256QAM

B.6.3.6.2.1 Característica de VER de CM con 256QAM

La pérdida de implementación de un CM DEBE ser tal que el CM tenga una VER después de la FEC inferior o igual a 10^{-8} cuando se funcione con una relación portadora/ruido (E_s/N_o) tal como se muestra a continuación.

Nivel de recepción de señal de entrada	**E_s/N_o**
desde –6 dBmV hasta +15 dBmV	30 dB o mayor
desde menos que –6 dBmV hasta –15 dBmV	33 dB o mayor

B.6.3.6.2.2 Característica de rechazo de imagen con 256QAM

La característica descrita en B.6.3.6.2.1 DEBE cumplirse con una señal analógica o digital a +10 dBc en cualquier tramo de la banda RF distinto de los canales adyacentes.

B.6.3.6.2.3 Calidad del canal adyacente con 256QAM

La característica descrita en B.6.3.6.2.1 DEBE cumplirse con una señal analógica o digital a 0 dBc en los canales adyacentes.

La característica descrita en B.6.3.6.2.1, con un margen adicional de 0,5 dB, DEBE cumplirse con una señal analógica a +10 dBc en los canales adyacentes.

La característica descrita en B.6.3.6.2.1, con un margen adicional de 1,0 dB, DEBE cumplirse con una señal digital a +10 dBc en los canales adyacentes.

B.6.3.7 Fluctuación de fase de la indicación de tiempo del CMTS

La fluctuación de fase de la indicación de tiempo del CMTS DEBE ser inferior a 500 ns, cresta a cresta, a la salida de la subcapa de convergencia de transmisión en sentido descendente. Dicha fluctuación está referida a una subcapa de convergencia de transmisión en sentido descendente teórica, que transfiere los datos del paquete MPEG a la subcapa dependiente de los medios físicos en sentido descendente, con un reloj perfectamente continuo y estable a la velocidad de datos del paquete MPEG. El procesamiento de la subcapa dependiente de los medios físicos en sentido

descendente NO DEBE ser considerado en la generación y transferencia de indicaciones de tiempo a la subcapa dependiente de los medios físicos en sentido descendente.

Así pues, cualesquiera dos indicaciones de tiempo N1 y N2 (N2 > N1), que fueron transferidas a la subcapa dependiente de los medios físicos en sentido descendente en los momentos T1 y T2 respectivamente, deben cumplir la siguiente relación:

$$\left|(N2-N1)/10240000-(T2-T1)\right|<500ns$$

La fluctuación de fase incluye imprecisiones en el valor de las indicaciones de tiempo y la fluctuación de fase en todos los relojes. Los 500 ns asignados para la fluctuación de fase a la salida de la subcapa de convergencia de transmisión en sentido descendente deben ser reducidos como consecuencia de cualquier fluctuación de fase que introduzca la subcapa dependiente de los medios físicos en sentido descendente.

Se prevé que el CM satisfaga los requisitos de exactitud de temporización de ráfaga de B.6.2.7 cuando las indicaciones de tiempo contengan esta fluctuación de fase de caso más desfavorable.

NOTA – La fluctuación de fase es el error (medido) con respecto al reloj maestro del CMTS. (El reloj maestro del CMTS es el reloj a 10,24 MHz utilizado para generar las indicaciones de tiempo.)

El reloj maestro a 10,24 MHz del CMTS DEBE tener una estabilidad de frecuencia de ≤ ±5 ppm (partes por millón), una velocidad de deriva de ≤ 10^{-8} por segundo y una fluctuación de borde de ≤ 10 ns cresta a cresta (±5 ns) en un rango de temperatura de 0º C a 40º C y hasta 10 años a partir de la fecha de manufactura. Los requisitos de velocidad de deriva y fluctuación de fase en el reloj maestro del CMTS entrañan el que la duración de dos segmentos adyacentes de 10 240 000 ciclos sea de 30 ns, 10 ns debidos a la fluctuación de fase mientras dura cada segmento y 10 ns debidos a la deriva de frecuencia. Se pueden deducir además otras duraciones del cómputo: 1 024 000 segmentos adyacentes, ≤ 21 ns; 1 024 000 segmentos de longitud separados por un segmento de 10 240 000 ciclos, ≤ 30 ns; 102 400 000 segmentos adyacentes, ≤ 120 ns. El reloj maestro del CMTS DEBE satisfacer esos límites de prueba en un 99%, o más, de las mediciones.

Las prescripciones del presente anexo B PUEDEN cumplirse también sincronizando el oscilador del reloj maestro del CMTS con una fuente externa de frecuencia de referencia. En tal caso, el reloj maestro interno del CMTS DEBE tener una exactitud de frecuencia de ±20 ppm en una gama de temperaturas de 0º C a 40º C y hasta 10 años después de la fecha de su fabricación, cuando no se haya conectado ninguna fuente de frecuencia de referencia. La velocidad de deriva y la fluctuación de fase de borde DEBEN ser tal como se ha especificado más arriba.

B.7 Subcapa de convergencia de la transmisión en sentido ascendente

Esta cláusula se aplica a la primera opción tecnológica, tal como se describe en B.1.1. Para la segunda opción, véase el anexo B.N.

B.7.1 Introducción

Para aumentar la solidez de la modulación, facilitar el que el equipo físico de recepción sea común para vídeo y datos y dejar abierta la posibilidad de una futura multiplexación de vídeo y datos en el tren de bits de la subcapa PMD definida en B.6, se interpone una subcapa entre la subcapa PMD en sentido descendente y la subcapa MAC de datos por cable.

El tren de bits en sentido descendente se define como una serie continua de paquetes MPEG [UIT-T H.222.0] de 188 octetos. Dichos paquetes constan de un encabezamiento de 4 octetos seguido de 184 octetos de cabida útil. El encabezamiento identifica la cabida útil como perteneciente al MAC de datos por cable. Otros valores del encabezamiento pueden indicar otras cabidas útiles. La combinación de cabidas útiles MAC y las de otros servicios es opcional y la controla el CMTS.

La figura B.7-1 ilustra la intercalación de bytes MAC de datos por cable (DOC, *data-over-cable*) con otra información digital (vídeo digital en el ejemplo mostrado).

Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital

Figura B.7-1/J.112 – Ejemplo de intercalación de paquetes MPEG en sentido ascendente

B.7.2 Formato de paquete MPEG

En la figura B.7-2 se muestra el formato de un paquete MPEG que lleva datos DOCSIS. El paquete consta de un encabezamiento MPEG de 4 octetos, un campo de puntero (no presente en todos los paquetes) y la cabida útil DOCSIS.

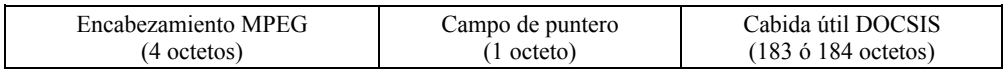


Figura B.7-2/J.112 – Formato de un paquete MPEG

B.7.3 Encabezamiento MPEG para datos por cable de DOCSIS

El formato del encabezamiento del flujo de transporte MPEG se define en 2.4/H.222.0. Los valores de campos particulares que distinguen a los trenes de datos por cable MAC se definen en el cuadro B.7-1. Los nombres de los campos proceden de la especificación de la UIT.

Cuadro B.7-1/J.112 – Formato de encabezamiento MPEG para paquetes de datos por cable de DOCSIS

Campo	Longitud (bits)	Descripción
octeto de sincronismo	8	0x47; octeto de sincronismo de paquete MPEG
indicador de error de transporte	1	Indica un error que se ha producido en la recepción del paquete. Este bit es repuesto a cero por el emisor, y puesto a uno cuando quiera que se produzca un error en la transmisión del paquete
indicador de comienzo de unidad de cabida útil	1	Un valor de uno indica la presencia de un campo de puntero como el primer octeto de la cabida útil (quinto octeto del paquete)
prioridad de transporte	1	Reservado; puesto a cero
PID	13	PID conocido de datos por cable de DOCSIS (0x1FFE)
control de aleatorización del transporte	2	Reservado; puesto a '00'
control de campo de adaptación	2	'01', la utilización del campo de adaptación NO ESTÁ PERMITIDA en el PID de DOCSIS
contador de continuidad	4	contador cíclico dentro de este PID

El encabezamiento MPEG consta de 4 octetos que inician el paquete MPEG de 188-octetos. El formato del encabezamiento a utilizar en un PID de datos por cable de DOCSIS está sometido a las restricciones que se muestran en el cuadro B.7-1. El formato del encabezamiento se atiene a la norma MPEG, pero su utilización está limitada en esta especificación para NO PERMITIR la inclusión de un campo de adaptación en los paquetes MPEG.

B.7.4 Cabida útil MPEG para datos por cable de DOCSIS

La porción de cabida útil MPEG del paquete MPEG llevará las tramas MAC de DOCSIS. El primer octeto de la cabida útil MPEG será un campo de puntero ('pointer_field') si se ha fijado el indicador de comienzo de unidad de cabida útil (payload_unit_start_indicator) (PUSI) del encabezamiento MPEG.

octeto de relleno (stuff_byte)

Este anexo B define un esquema de octetos de relleno que tienen un valor (0xFF) utilizado dentro de la cabida útil DOCSIS para llenar cualquier intervalo entre tramas MAC de DOCSIS. El valor se elige como valor no utilizado para el primer octeto de la trama MAC de DOCSIS. El octeto 'FC' del encabezamiento MAC se definirá de modo que nunca contenga ese valor. (FC_TYPE = '11' indica una trama específica del MAC, y FC_PARM = '11111' no se utiliza actualmente y, de acuerdo con este anexo B, se define como un valor ilegal para FC_PARM.)

campo de puntero (pointer_field)

El campo de puntero está presente como quinto octeto del paquete MPEG (quinto octeto tras el encabezamiento MPEG) cuando en el encabezamiento MPEG se ha fijado el PUSI a uno. La interpretación del campo de puntero es como sigue:

El campo de puntero contiene el número de octetos de este paquete que siguen inmediatamente a dicho campo que el decodificador del CM debe saltarse antes de buscar el comienzo de una trama MAC de DOCSIS. Un campo de puntero CM DEBE estar presente si es posible para empezar una trama MAC de DOCSIS de datos por cable en el paquete, y DEBE apuntar:

1) al comienzo de la primera trama MAC para empezar en el paquete; o
2) a cualquier octeto de relleno que preceda a la trama MAC.

B.7.5 Interacción con la subcapa MAC

Las tramas MAC pueden empezar en cualquier punto dentro de un paquete MPEG y pueden abarcar varios paquetes MPEG y, dentro de un paquete MPEG, pueden existir varias tramas MAC.

Las figuras que siguen muestran el formato de los paquetes MPEG que llevan tramas MAC de DOCSIS. En todos los casos, la bandera PUSI indica la presencia del campo de puntero como primer octeto de la cabida útil MPEG.

La figura B.7-3 muestra una trama MAC situada inmediatamente después del octeto pointer_field. En este caso, el campo de puntero es cero y el decodificador DOCSIS empezará la búsqueda de un octeto FC válido en el octeto que sigue inmediatamente al campo de puntero.

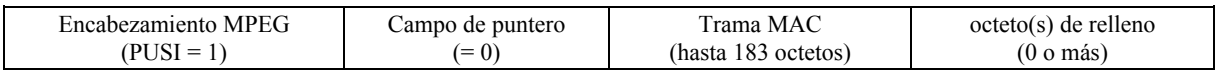


Figura B.7-3/J.112 – Formato de paquete cuando una trama MAC sigue inmediatamente al campo de puntero

La figura B.7-4 muestra el caso más general en el que una trama MAC va precedida por la cola de una trama MAC anterior y una secuencia de octetos de relleno. En este caso, el campo de puntero identifica todavía al primer octeto después de la cola de la trama # 1 octeto de relleno (un stuff_byte)

como la posición en la que el decodificador debería empezar la búsqueda de un valor FC de subcapa MAC legal. Este formato permite la operación de multiplexación en el CMTS para insertar inmediatamente una trama MAC que esté disponible para transmisión si dicha trama llega después de que se hayan transmitido el encabezamiento y el campo de puntero MPEG.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= M)	Cola de la trama MAC #1 (M octetos)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #2

Figura B.7-4/J.112 – Formato de paquete con trama MAC precedida por octetos de relleno

Para facilitar la multiplexación del tren de paquetes MPEG que lleva datos DOCSIS con otros datos con codificación MPEG, el CMTS NO DEBERÍA transmitir paquetes MPEG con el PID de DOCSIS que contienen solamente octetos de relleno en la zona de cabida útil. En su lugar, DEBERÍAN transmitirse paquetes nulos MPEG. Se señala que existen relaciones de temporización implícitas en la subcapa MAC de DOCSIS que también deben ser preservadas por cualquier operación de multiplexación MPEG.

La figura B.7-5 muestra que dentro del paquete MPEG pueden estar contenidas múltiples tramas MAC. Las tramas MAC pueden estar concatenadas una tras otra o separadas por una secuencia opcional de octetos de relleno.

EncabezamientoMPEG (PUSI = 1)	Campo de puntero (= 0)	Trama MAC #1	Trama MAC #2	octeto(s) de relleno (0 o más)	Trama MAC #3

Figura B.7-5/J.112 – Formato de paquete mostrando múltiples tramas MAC en un solo paquete

La figura B.7-6 muestra el caso en el que una trama MAC abarca múltiples paquetes MPEG. En este caso, el pointer_field de la trama subsiguiente apunta al octeto que sigue al último octeto de la cola de la primera trama.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= 0)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #1 (hasta 183 octetos)	
Encabezamiento MPEG (PUSI = 0)	Continuación de la trama MAC #1 (184 octetos)			
Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= M)	Cola de la trama MAC #1 (M octetos)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #2 (M octetos)

Figura B.7-6/J.112 – Formato de paquete cuando una trama MAC abarca múltiples paquetes

La subcapa de convergencia de transmisión debe funcionar en estrecha relación con la subcapa MAC para proporcionar una indicación de tiempo precisa que se ha de insertar en el mensaje de sincronización de tiempo (véanse B.8.3.2 y B.9.3).

B.7.6 Interacción con la capa física

El tren de paquetes MPEG-2 DEBE ser codificado de acuerdo con [UIT-T J.83-B], incluyendo la alineación de trama de transporte MPEG-2 que utiliza una suma de comprobación de paridad como se describe en [UIT-T J.83-B].

B.7.7 Sincronización y recuperación de encabezamiento MPEG

El tren de paquetes MPEG-2 DEBERÍA ser declarado "dentro de trama" (es decir, que se ha conseguido la alineación correcta de los paquetes) cuando se hayan recibido cinco sumas de comprobación de paridad correctas consecutivas, cada una de ellas a 188 octetos de la anterior.

El tren de paquetes MPEG-2 DEBERÍA ser declarado "fuera de trama", y debería iniciarse una búsqueda de alineación correcta de los paquetes, cuando se hayan recibido nueve sumas de comprobación de paridad incorrectas consecutivas.

En B.8 se describe en detalle el formato de las tramas MAC.

B.8 Especificación del control de acceso a medios

B.8.1 Introducción

B.8.1.1 Visión de conjunto

En esta cláusula se describe la versión 1.1 del protocolo MAC de DOCSIS. Algunos de los puntos más destacados del protocolo MAC son:

- Atribución de la anchura de banda controlada por el CMTS.
- Tren de miniintervalos de tiempo en sentido ascendente.
- Combinación dinámica de oportunidades de transmisión en sentido ascendente por contienda y reserva.
- Eficacia de la anchura de banda mediante el soporte de paquetes de longitud variable.
- Previsión de ampliaciones para el soporte futuro del ATM o de otras PDU de datos.
- Calidad de servicio que incluye:
  - soporte de la anchura de banda y latencia garantizadas;
  - clasificación de paquetes;
  - establecimiento del servicio dinámico.
- Previsión de ampliaciones a efectos de seguridad en la capa de enlace de datos.
- Soporte de una amplia gama de velocidades de datos.

B.8.1.2 Definiciones

B.8.1.2.1 Dominio de subcapa MAC

El dominio de subcapa MAC es un conjunto de canales en sentido ascendente y en sentido descendente para los que actúa un solo protocolo de atribución y gestión MAC. Entre sus vinculaciones figuran un CMTS y varios CM. El CMTS DEBE dar servicio a todos los canales en sentido ascendente y descendente. El CMTS DEBE verificar y descartar cualquier paquete recibido que tenga una dirección fuente MAC que no sea una dirección unidifusión MAC.

B.8.1.2.2 Punto de acceso al servicio MAC

Un punto de acceso al servicio MAC (MSAP) es un accesorio de un dominio de subcapa MAC. (Véase B.5.2.)

B.8.1.2.3 Flujos de servicio

El concepto de flujos de servicio es fundamental para la actuación del protocolo MAC. Los flujos de servicio proporcionan un mecanismo para la gestión de la calidad de servicio en sentido ascendente y descendente. Forman parte integrante, en particular, de la atribución de anchura de banda en sentido ascendente.

Un flujo de servicio define una correspondencia unidireccional particular entre un CM y el CMTS. Los identificadores ID de flujo de servicio en sentido ascendente activo tienen también un identificador de servicio asociado, o SID. La anchura de banda en sentido ascendente es atribuida a los SID, y por tanto a los CM, por el CMTS. Los ID de servicio proporcionan el mecanismo mediante el cual se implementa la calidad de servicio en sentido ascendente proporcionan.

El CMTS PUEDE asignar uno o más ID de flujo de servicio (SFID, *service flow ID*) a cada CM, la correspondencia con las clases de servicio de flujo requeridas por el CM. Dicha correspondencia puede ser negociada entre el CMTS y el CM durante el registro del CM, o a través del establecimiento de un servicio dinámico (véase B.11.4).

En una implementación de CM básica, se pueden utilizar dos flujos de servicio (uno en sentido ascendente, uno en sentido descendente), por ejemplo, para ofrecer el mejor servicio IP posible. Sin embargo, el concepto de flujo de servicio permite el desarrollo de CM más complejos, que soporten múltiples clases de servicio soportando al mismo tiempo que la interoperabilidad con módems más básicos. Con estos módems más complejos es posible que determinados flujos de servicio se configuren de tal manera que no puedan llevar todos los tipos de tráfico. Es decir, que pueden tener una limitación en cuanto al tamaño máximo de los paquetes o estar restringidos a las concesiones no solicitadas de tamaño pequeño y fijo. Es posible además que no convenga enviar otro tipo de datos en flujos de servicio utilizados para aplicaciones del tipo velocidad binaria constante (CBR, *constant bit rate*).

Aun en estos módems complejos, es preciso el poder enviar ciertos paquetes en sentido ascendente, necesarios para la gestión del MAC, la gestión SNMP, la gestión de claves, etc. Para que la red funcione adecuadamente, todos los CM DEBEN soportar al menos un flujo de servicio en sentido ascendente y uno en sentido descendente. Estos flujos de servicio DEBEN aprovisionarse siempre para que el CM pueda solicitar y enviar la mayor trama MAC no concatenada posible (véase B.8.2.2). Estos flujos de servicio se conocen como los flujos de servicio primarios en sentido ascendente y en sentido descendente. Al SID asignado al flujo de servicio primario en sentido ascendente se le denomina SID primario.

El SID primario DEBE asignarse siempre al primer flujo de servicio en sentido ascendente aprovisionado durante el proceso de registro (que puede ser o no el mismo SID temporal utilizado en el proceso de registro). Los flujos de servicio primarios DEBEN ser activados inmediatamente en el momento del registro. El SID primario DEBE ser utilizado siempre en el mantenimiento de la estación después del registro. Los flujos de servicio primarios PUEDEN ser utilizados para el tráfico. Todos los flujos de servicio de unidifusión DEBEN utilizar la asociación de seguridad definida por el flujo de servicio primario (véase [DOCSIS8]).

Todos los ID de flujo de servicio son únicos en el contexto de un solo dominio de subcapa MAC. La correspondencia entre un identificador de servicio de unidifusión y un flujo de servicio activo/admitido DEBE ser única en el contexto de un solo dominio de subcapa MAC. La longitud del ID de flujo de servicio es de 32 bits. La longitud del ID de servicio es 14 bits (aunque el ID de servicio se lleva a veces en los bits de orden inferior de un campo de 16 bits).

B.8.1.2.4 Intervalos en sentido ascendente, miniintervalos de tiempo e incrementos de 6,25 µs

La línea de tiempo de la transmisión en sentido ascendente es dividida en intervalos por el mecanismo de atribución de anchura de banda en sentido ascendente. Cada intervalo es un número entero de miniintervalos de tiempo. Un "miniintervalo de tiempo" es la unidad de granularidad para

las oportunidades de transmisiones en sentido ascendente. Esto no significa que una PDU cualquiera pueda ser transmitida de hecho en un solo miniintervalo de tiempo. Cada intervalo va etiquetado con un código de utilización que define tanto el tipo de tráfico que puede ser transmitido durante ese intervalo como la codificación de la modulación de la capa física. Un miniintervalo de tiempo es un múltiplo potencia de dos de 6,25 µs, es decir, 2, 4, 8, 16, 32, 64 ó 128 veces 6,25 µs. En B.9.3.4 se describe en detalle la relación entre miniintervalos de tiempo, octetos y tics de tiempo. Los valores del código de utilización se definen en el cuadro B.8-20 y los usos permitidos, en B.8.3. La vinculación de estos valores a los parámetros de capa física se define en el cuadro B.8-18.

B.8.1.2.5 Trama

Una trama es una unidad de datos intercambiada entre dos (o más) entidades en la capa de enlace de datos. Una trama MAC consta de un encabezamiento MAC (que comienza con un octeto de control de trama; véase la figura B.8-3), y puede incorporar células ATM o una PDU datos de longitud variable. La PDU de longitud variable incluye un par de direcciones de 48 bits, datos, y una suma CRC. En casos especiales, el encabezamiento MAC puede encapsular múltiples tramas MAC (véase B.8.2.5.5) en una sola trama MAC.

B.8.1.3 Utilización futura

En las diversas tramas MAC que se describen en el presente anexo B hay un cierto número de campos que se definen como "para utilización futura". Dichos campos NO DEBEN ser interpretados o utilizados en manera alguna por esta versión (1.1) del protocolo MAC.

B.8.2 Formatos de trama MAC

B.8.2.1 Formato de trama MAC genérica

La trama MAC es la unidad básica de transferencia entre subcapas MAC del CMTS y el módem de cable. Se utiliza la misma estructura básica tanto en el sentido ascendente como en el descendente. Las tramas MAC son de longitud variable. El término "trama" se utiliza en este contexto para indicar una unidad de información que se transfiere entre pares de subcapa MAC. No se ha de confundir con el término "alineación de trama" que indica algún tipo de relación de temporización fija.

Hay que considerar tres regiones diferentes, como se muestra en la figura B.8-1. Precediendo a la trama MAC se encuentra la tara de subcapa PMD (sentido ascendente) o bien un encabezamiento de convergencia de transmisión MPEG (sentido descendente). La primera parte de la trama MAC es el encabezamiento MAC. El encabezamiento MAC identifica de manera exclusiva el contenido de la trama MAC. Tras el encabezamiento se encuentra la región PDU datos opcional. En el encabezamiento MAC se indica el formato de la PDU datos y si está presente de manera uniforme.

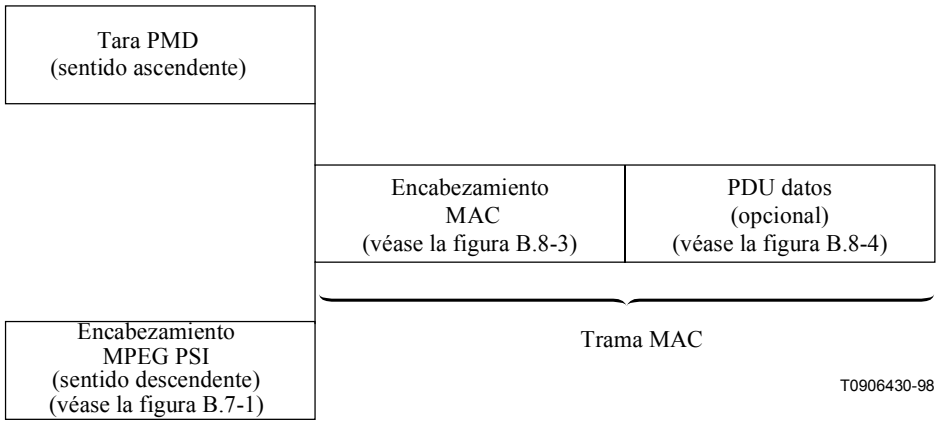


Figura B.8-1/J.112 – Formato de trama MAC genérica

B.8.2.1.1 Tara PMD

En el sentido ascendente, la capa PHY indica el comienzo de la trama MAC a la subcapa MAC. Desde el punto de vista de la subcapa MAC, sólo necesita saber cuál es la cantidad total de tara para tenerla en cuenta en el proceso de atribución de anchura de banda. Más información a este respecto figura en la cláusula del presente anexo B relativa a la subcapa PMD (véase B.6).

La tara FEC se extiende a lo largo de la trama MAC, y se supone que es transparente al tren de datos MAC. No es necesario que la subcapa MAC tenga en cuenta la tara cuando efectúe la atribución de anchura de banda. En la cláusula del presente anexo B relativa a la atribución de anchura de banda en sentido ascendente (véase B.9.1) hay más información sobre este tema.

B.8.2.1.2 Transporte de tramas MAC

En la figura B.8-2 se muestra el transporte de tramas MAC por la subcapa PMD para canales en sentido ascendente.

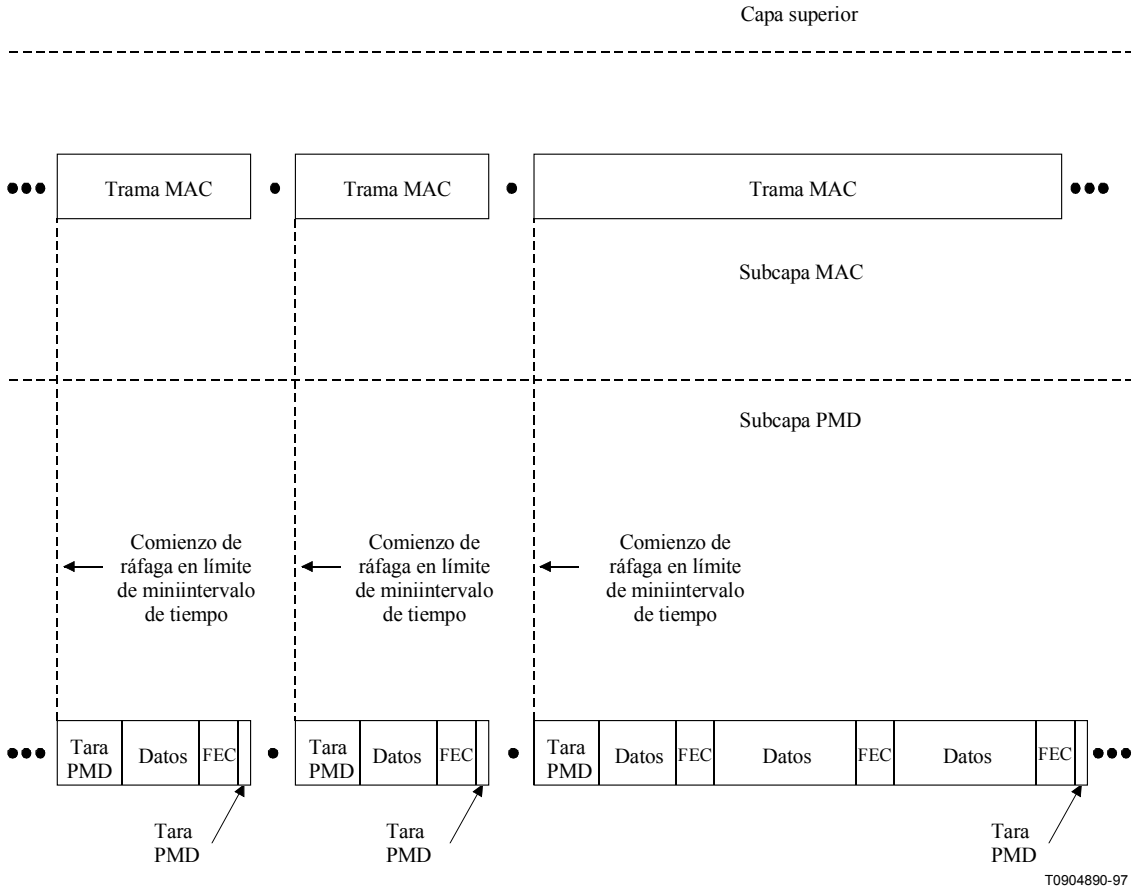


Figura B.8-2/J.112 – Convergencia MAC/PMD en sentido ascendente

La disposición por capas de tramas MAC en MPEG en el canal descendente se describe en B.7.

B.8.2.1.3 Orden de los bits y octetos

Dentro de un octeto, el bit menos significativo es el primero que se transmite por el conductor. De esta manera se sigue el convenio utilizado por Ethernet e [ISO/CEI 8802-3]. A esto se le llama a menudo orden en pequeña fila india de bits (véase la nota).

NOTA – Esto se aplica al canal en sentido ascendente solamente. Para el canal en sentido descendente, la subcapa de convergencia de transmisión MPEG presenta una interfaz de un octeto de ancha al MAC, por lo que la subcapa MAC no define el orden de los bits.

Dentro de la capa MAC, cuando las cantidades numéricas son representadas por más de un octeto (es decir, valores de 16 bits y de 32 bits), el octeto que contiene los bits más significativos es el primero que se transmite por el cable. A esto se le llama a veces orden en gran fila india de octeto.

En esta cláusula se sigue el convenio textual de que cuando se presentan campos de bits en cuadros, los bits más significativos son los situados en la parte superior del cuadro. Por ejemplo, en el cuadro B.8-2, FC_TYPE ocupa los dos bits más significativos y EHDR_ON ocupa el bit menos significativo.

B.8.2.1.3.1 Representación de número negativos

Los valores de enteros con signo DEBEN ser transmitidos y recibidos en formato de complemento a dos.

B.8.2.1.3.2 Campos de tipo-longitud-valor

Muchos mensajes MAC incorporan campos de tipo-longitud-valor (TLV, *type-length-value*). Los campos TLV son listas no ordenadas de tuplas de TLV. Algunos de los TLV están anidadas (véase el anexo B.C). Todos los campos de longitud TLV, con la excepción de EH-LEN (véase B.8.2.6), DEBEN ser superiores a cero. A menos que se especifique otra cosa, tipo y longitud son ambos iguales a un octeto.

Al utilizar esta codificación, pueden añadirse parámetros nuevos que algunos dispositivos no pueden interpretar. Un CM o CMTS que no reconozca un tipo de parámetro DEBE saltárselo y NO DEBE tratar el evento como una condición de error.

B.8.2.1.4 Formato de encabezamiento MAC

El formato del encabezamiento MAC DEBE ser como se muestra en la figura B.8-3.

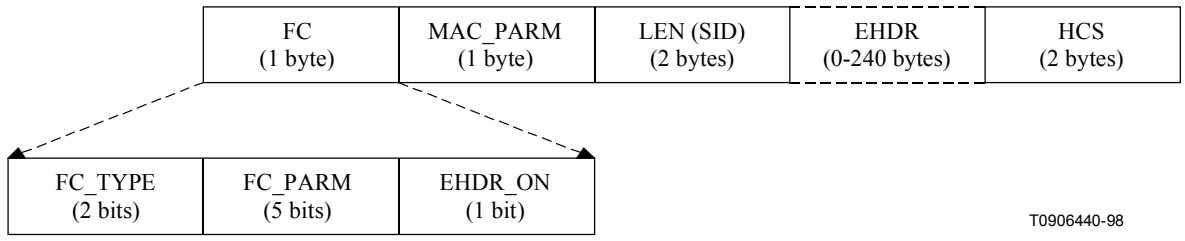


Figura B.8-3/J.112 – Formato de encabezamiento MAC

Todos los encabezamientos MAC DEBEN tener el formato general que se muestra en el cuadro B.8-1. El campo control de trama (FC, *frame control*) es el primer octeto e identifica de manera exclusiva el resto del contenido del encabezamiento MAC. El campo FC va seguido de 3 octetos de control MAC; un campo encabezamiento ampliado (EHDR, *extended header*) OPCIONAL; y una secuencia de verificación de encabezamiento (HCS, *header check sequence*) para garantizar la integridad del encabezamiento MAC.

Cuadro B.8-1/J.112 – Formato de encabezamiento MAC genérico

Campo encabeza-miento MAC	Utilización	Tamaño
FC	Control de trama: Identifica el tipo de encabezamiento MAC	8 bits
MAC_PARM	Campo parámetro cuya utilización depende del FC: si EHDR_ON = 1; utilizado para longitud de campo EHDR (ELEN) de otro modo, en caso de tramas concatenadas (véase el cuadro B.8-10), utilizado para cómputo de tramas MAC de otro modo (para peticiones solamente), indica el número de miniintervalos de tiempo y/o células ATM que se han perdido	8 bits
LEN (SID)	Longitud de la trama MAC: la longitud se define como la suma del número de octetos del encabezamiento ampliado (si está presente) y el número de octetos que siguen al campo HCS. (En caso de encabezamiento REQ, este campo es, en cambio, el ID de servicio)	16 bits
EHDR	Encabezamiento MAC ampliado (si está presente; tamaño variable)	0-240 octetos
HCS	Secuencia de verificación de encabezamiento MAC	2 octetos
	Longitud de un encabezamiento MAC	6 octetos + EHDR

El campo HCS es una CRC de 16 bits con la que se garantiza la integridad del encabezamiento MAC, incluso en un entorno de colisiones. La cobertura del campo HCS DEBE incluir el encabezamiento MAC en su totalidad, empezando con el campo FC e incluyendo cualquier campo EHDR que pueda estar presente. La HCS se calcula utilizando la CRC del CCITT ($x^{16} + x^{12} + x^5 + 1$) que se define en [UIT-T X.25].

El campo FC está constituido por el subcampo FC_TYPE, el subcampo FC_PARM y una bandera de indicación EHDR_ON. El formato del campo FC DEBE ser como se muestra en el cuadro B.8-2.

Cuadro B.8-2/J.112 – Formato de campo FC

Campo FC	Utilización	Tamaño
FC_TYPE	Campo tipo de control de trama MAC: 00: Encabezamiento MAC de PDU paquetes 01: Encabezamiento MAC de PDU con ATM 10: Encabezamiento MAC de PDU reservado 11: Encabezamiento específico de MAC	2 bits
FC_PARM	Bits de parámetro, utilización dependiente del FC_TYPE	5 bits
EHDR_ON	Cuando = 1, indica que el campo EHDR está presente Longitud de EHDR (ELEN) está determinada por el campo MAC_PARM	1 bit

El subcampo FC_TYPE está formado por los dos MSB del campo FC. Dichos bits DEBEN interpretarse siempre del mismo modo para indicar uno de los cuatro posibles formatos de trama MAC. Estos tipos son: encabezamiento MAC de PDU paquetes; encabezamiento MAC con células

ATM; encabezamiento MAC reservado para futuros tipos de PDU; o un encabezamiento MAC utilizado a efectos específicos del control MAC. En lo que queda de esta cláusula se expone con más detalle el significado de estos tipos.

Los cinco bits que siguen al subcampo FC_TYPE constituyen el subcampo FC_PARM. La utilización de estos bits depende del tipo de encabezamiento MAC. El LSB del campo FC es el indicador EHDR_ON. Si se fija este bit, está presente un encabezamiento ampliado (EHDR). El EHDR proporciona un mecanismo para hacer ampliable el encabezamiento MAC de manera interoperable.

El esquema de los octetos de relleno de la subcapa de convergencia de transmisión se define de modo que sea un valor de 0xFF. De esta manera se evita la utilización de valores de octetos de FC que tengan FC_TYPE = '11' y FC_PARM = '11111'.

El campo MAC_PARM del encabezamiento MAC sirve para diversos fines, dependiendo del campo FC. Si se fija el indicador EHDR_ON, el campo MAC_PARM DEBE ser utilizado como el de longitud del encabezamiento ampliado (ELEN). El campo EHDR PUEDE variar de 0 a 240 octetos. Si se trata de un encabezamiento MAC de concatenación, el campo MAC_PARM representa el número de tramas MAC (CNT) de la concatenación (véase B.8.2.5.5). Si se trata de un encabezamiento MAC de petición (REQ) (véase B.8.2.5.3), el campo MAC_PARM representa la cantidad de anchura de banda que se pide. En los demás casos, el campo MAC_PARM se reserva para utilización futura.

El tercer campo tiene dos posibles utilizaciones. En la mayoría de los casos, indica la longitud (LEN, *length*) de esta trama MAC. En un caso especial, el encabezamiento MAC de petición, se utiliza para indicar el ID de servicio del módem del cable ya que no hay ninguna PDU que siga al encabezamiento MAC.

El campo encabezamiento ampliado (EHDR) permite ampliaciones del formato de trama MAC. Se utiliza para implementar la seguridad del enlace de datos, así como que la fragmentación de trama, y se puede ampliar para añadir el soporte de otras funciones en versiones futuras. Las implementaciones iniciales DEBERÍAN transferir este campo al procesador. De esta manera será posible que las versiones futuras mejoradas del soporte lógico aprovechen esta capacidad (para más detalles, véase B.8.2.6, "Encabezamientos MAC ampliados").

B.8.2.1.5 PDU datos

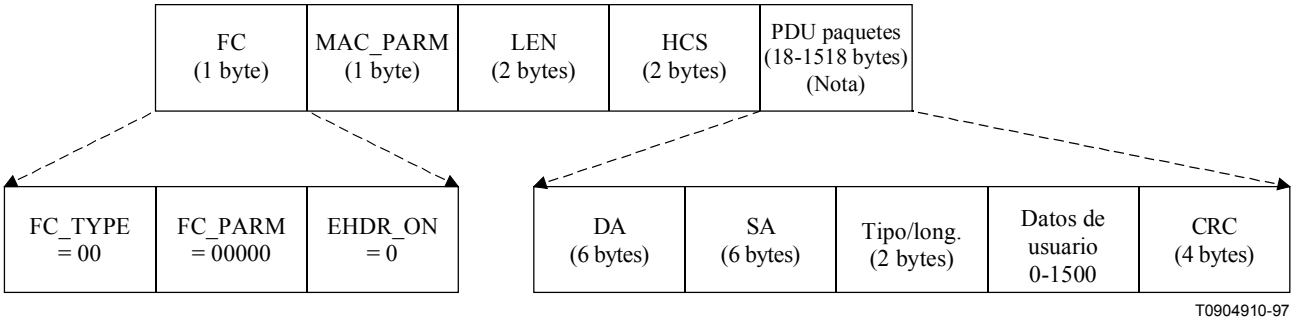
El encabezamiento MAC puede ir seguido de una PDU datos. El tipo y el formato de la PDU datos se definen en el campo control de trama (FC) del encabezamiento MAC. El campo FC define explícitamente una PDU datos por paquetes, una PDU datos con ATM, una trama específica MAC y un punto de código reservado (utilizado como mecanismo de escape para ampliaciones futuras). Todos los CM DEBEN utilizar la longitud del encabezamiento MAC para saltarse cualquier dato reservado.

B.8.2.2 Tramas MAC basadas en paquetes

B.8.2.2.1 Paquetes de longitud variable

La subcapa MAC DEBE soportar una PDU datos por paquetes de tipo Ethernet/[ISO/CEI 8802-3] de longitud variable. Se DEBE hacer que la PDU por paquetes pase a través de la red en su totalidad, incluyendo su CRC original. Al comienzo se agrega un encabezamiento MAC de paquetes único. El formato de trama sin encabezamiento ampliado DEBE ser como se muestra en la figura B.8-4 y en el cuadro B.8-3.

La excepción es el caso de supresión de encabezamiento de cabida útil. En este caso, todos los bytes salvo los suprimidos se DEBEN pasar a través de la red y la CRC abarca los bytes transmitidos efectivamente (véase B.8.2.6.3.1).



NOTA – El tamaño de las tramas se limita a 1518 bytes en ausencia de rotulación VLAN. Los equipos cooperantes que implementen la rotulación VLAN de IEEE 802.1Q PUEDEN utilizar un tamaño de trama de hasta 1522 bytes.

Figura B.8-4/J.112 – Formato de PDU paquetes de Ethernet 802.3

Cuadro B.8-3/J.112 – Formato de PDU paquetes

Campo	Utilización	Tamaño
FC	FC_TYPE = 00; encabezamiento MAC de paquetes FC_PARM[4:0] = 00000; los demás valores se reservan para utilización futura y se ignoran EHDR_ON = 0; si no hay encabezamiento ampliado, 1 si hay EHDR	8 bits
MAC_PARM	MAC_PARM = x; DEBE fijarse a 0 si no hay EHDR; de otro modo, se fija a la longitud del EHDR	8 bits
LEN	LEN = n + x; longitud de PDU paquetes en octetos + longitud de EHDR	16 bits
EHDR	Encabezamiento MAC ampliado, si está presente	0-240 octetos
HCS	Secuencia de verificación de encabezamiento MAC	16 octetos
Datos por paquetes	PDU paquetes: DA – Dirección de destino de 48 bits SA – Dirección de origen de 48 bits Tipo/longitud – Tipo Ethernet o campo de longitud [ISO/CEI 8802-3] de 16 bits Datos de usuario (longitud variable, 0−1500 octetos) CRC – CRC en PDU paquetes de 32 bits (como se define en Ethernet/[ISO/CEI 8802-3])	n octetos
	Longitud de trama MAC de paquetes	6 + x + n octetos

En determinadas circunstancias (véase el anexo B.M) puede ser necesario transmitir una trama MAC de PDU paquetes sin una PDU real. Esto se hace de tal manera que el encabezamiento ampliado pueda ser utilizado para llevar cierta información sobre el estado del flujo de servicio. Lo anterior podría ocurrir también como resultado de una PHS (véase B.8.2.6.3.1). Una trama así tendrá el campo longitud en el encabezamiento MAC igual a la longitud del encabezamiento ampliado y no tendrá datos de paquetes, ni tampoco, por tanto, CRC. Esto sólo puede ocurrir con tramas que sean transmitidas en sentido ascendente, ya que las tramas transmitidas en sentido descendente tienen siempre al menos los campos DA y SA de la PDU paquetes.

B.8.2.3 Tramas MAC de células ATM

El FC_TYPE 0x01 se reserva para una definición futura de las tramas MAC de células ATM. Este campo FC_TYPE en el encabezamiento MAC indica que una PDU con ATM está presente. Esta PDU DEBE ser descartado en silencio por las implementaciones MAC de la presente versión (DOCSYS 1.1) del anexo B. Implementaciones conformes con la versión 1.1 DEBEN utilizar el campo longitud para saltarse la PDU con ATM.

B.8.2.4 Tramas MAC de PDU reservada

La subcapa MAC proporciona un punto de código FC reservado que permite soportar futuros formatos de PDU (por definir). El campo FC del encabezamiento MAC indica que está presente una PDU reservada. Esta PDU DEBE ser descartada en silencio por las implementaciones MAC de la presente versión (DOCSYS 1.1) del anexo B. Las implementaciones conformes a la versión 1.1 DEBEN utilizar el campo longitud para saltarse la PDU reservada.

El formato de la PDU reservada sin encabezamiento ampliado DEBE ser como se muestra en la figura B.8-5 y en el cuadro B.8-4.

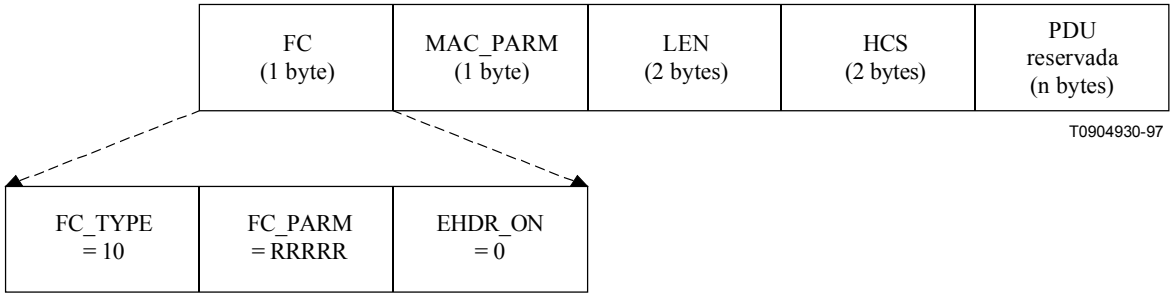


Figura B.8-5/J.112 – Formato de PDU reservada

Cuadro B.8-4/J.112 – Formato de PDU reservada

Campo	Utilización	Tamaño
FC	FC_TYPE = 10; encabezamiento MAC de PDU reservada FC_PARM[4:0]; reservado para utilización futura EHDR_ON = 0; en ausencia de encabezamiento ampliado, o 1 si hay un EHDR	8 bits
MAC_PARM	MAC_PARM = x; se DEBE fijar a 0 si no hay un EHDR; de otro modo se debe fijar a la longitud del EHDR	8 bits
LEN	LEN = n + x; longitud del mensaje de gestión MAC + la longitud del EHDR en octetos	16 bits
EHDR	Encabezamiento MAC ampliado, si está presente	0-240 octetos
HCS	Secuencia de verificación de encabezamiento MAC	16 octetos
Datos de usuario	PDU datos reservada	n octetos
	Longitud de una trama MAC de PDU reservada	6 + x + n octetos

B.8.2.5 Encabezamientos MAC específicos

Hay varios encabezamientos MAC que se utilizan para funciones muy específicas. Entre esas funciones figuran el soporte de la temporización en sentido descendente y la alineación en sentido ascendente, así como del ajuste de potencia, la petición de anchura de banda y la concatenación de múltiples tramas MAC.

El cuadro B.8-5 describe la utilización del FC-PARM dentro del encabezamiento MAC específico.

Cuadro B.8-5/J.112 – Encabezamientos y tramas MAC específicos

FC_PARM	Tipo de encabezamiento/trama
00000	Encabezamiento de temporización
00001	Encabezamiento MAC de gestión
00010	Trama de petición
00011	Encabezamiento de fragmentación
11100	Encabezamiento de concatenación

B.8.2.5.1 Encabezamiento de temporización

Se identifica un encabezamiento MAC específico para facilitar el soporte de la temporización y los ajustes requeridos. En el sentido descendente, este encabezamiento MAC DEBE ser utilizado para transportar la referencia de temporización global con la que se sincronizan todos los módems de cable. En el sentido ascendente, este encabezamiento MAC DEBE ser utilizado como parte del mensaje alineación que se necesita para la temporización del módem de un cable y los ajustes de potencia. El encabezamiento MAC de temporización va seguido de una PDU datos por paquetes. El formato DEBE ser como se muestra en la figura B.8-6 y en el cuadro B.8-6.

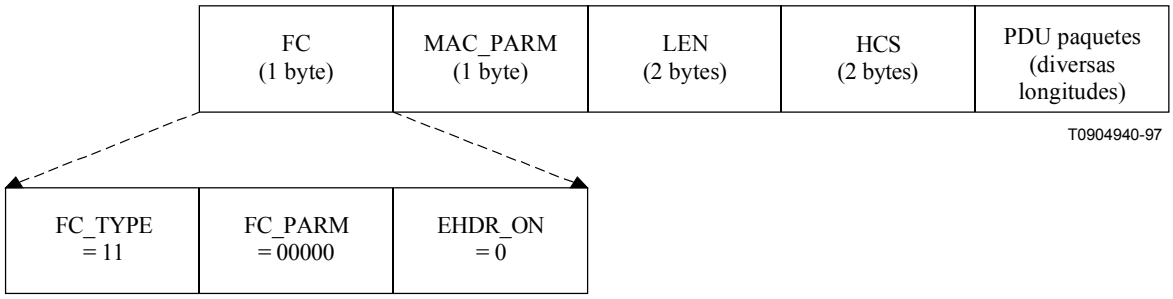


Figura B.8-6/J.112 – Encabezamiento MAC de temporización

Cuadro B.8-6/J.112 – Formato de encabezamiento MAC de temporización

Campo	Utilización	Tamaño
FC	FC_TYPE = 11; encabezamiento MAC específico FC_PARM[4:0] = 00000; encabezamiento MAC de temporización EHDR_ON = 0; encabezamiento ampliado prohibido para SYNC y RNG-REQ	8 bits
MAC_PARM	Reservado para utilización futura	8 bits
LEN	LEN = n; longitud de PDU paquetes en bytes	16 bits
EHDR	No está presente un encabezamiento MAC ampliado	0 bytes
HCS	Secuencia de verificación de encabezamiento MAC	2 bytes
Datos por paquetes	Mensaje de gestión MAC: mensaje SYNC (sentido descendente solamente) RNG-REQ (sentido ascendente solamente)	n bytes
	Longitud de trama MAC de mensaje temporización	6 + n bytes

B.8.2.5.2 Encabezamiento MAC de gestión

Se identifica un encabezamiento MAC específico para facilitar el soporte de los mensajes de gestión MAC requeridos. Este encabezamiento MAC DEBE ser utilizado para transportar todos los mensajes de gestión MAC (véase B.8-3). El formato DEBE ser como se muestra en la figura B.8-7 y en el cuadro B.8-7.

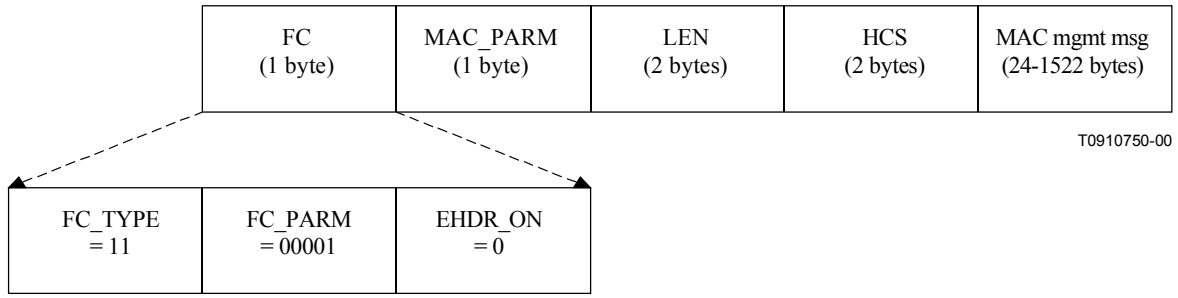


Figura B.8-7/J.112 – Encabezamiento MAC de gestión

Cuadro B.8-7/J.112 – Formato de encabezamiento MAC de gestión

Campo	Utilización	Tamaño
FC	FC_TYPE = 11; encabezamiento MAC específico FC_PARM[4:0] = 00001; Encabezamiento MAC de gestión EHDR_ON = 0 si no hay encabezamiento ampliado, 1 si hay un EHDR	8 bits
MAC_PARM	MAC_PARM = x; se DEBE fijar a 0 en ausencia de un EHDR; de otro modo se debe fijar a la longitud del EHDR	8 bits
LEN	LEN = n + x; longitud del mensaje de gestión MAC + longitud en octetos del EHDR	16 bits
EHDR	Encabezamiento MAC ampliado, si está presente	0-240 octetos
HCS	Secuencia de verificación de encabezamiento MAC	16 octetos
Datos por paquetes	Mensaje de gestión MAC	n octetos
	Longitud de trama MAC de gestión	6 +x +n octetos

B.8.2.5.3 Trama de petición

La trama de petición es el mecanismo básico que utiliza un módem de cable para pedir anchura de banda. Es el único aplicable en el sentido descendente. No DEBE haber ninguna PDU datos que siga a la trama de petición. El formato general de la petición DEBE ser como se muestra en la figura B.8-8 y en el cuadro B.8-8.

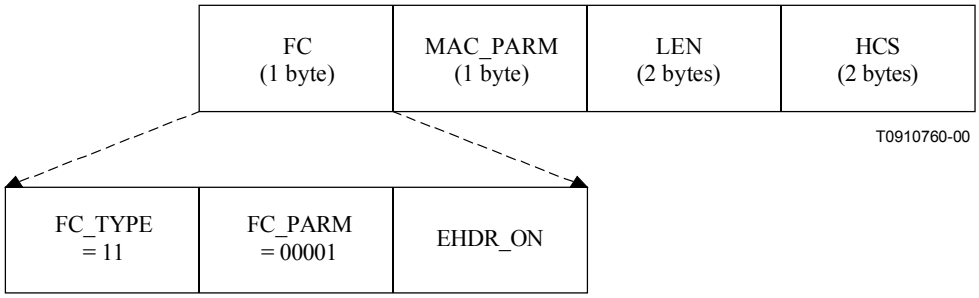


Figura B.8-8/J.112 – Formato de trama de petición

Cuadro B.8-8/J.112 – Formato de trama de petición (REQ)

Campo	Utilización	Tamaño
FC	FC_TYPE = 11; encabezamiento MAC específico FC_PARM[4:0] = 00010; encabezamiento MAC solamente; no sigue ninguna PDU datos EHDR_ON = 0 no se permite EHDR	8 bits
MAC_PARM	REQ, cantidad total de miniintervalos de tiempo pedidos	8 bits
SID	ID de servicio (0…0x1FFF)	16 bits
EHDR	No se permite encabezamiento MAC ampliado	0 octetos
HCS	Secuencia de verificación de encabezamiento MAC	2 octetos
	Longitud de un encabezamiento MAC de REQ	6 octetos

Puesto que la trama de petición no tiene ninguna PDU datos que le siga, no se necesita el campo LEN. El campo LEN DEBE ser sustituido por un SID. El SID DEBE identificar de manera exclusiva un flujo de servicio particular dentro de un CM.

La petición de anchura de banda, REQ, DEBE ser especificada en miniintervalos de tiempo. El campo REQ DEBE indicar la cantidad total actual de anchura de banda pedida para esta cola de espera de servicio, incluido un margen adecuado para la tara PHY.

B.8.2.5.4 Encabezamiento de fragmentación

El encabezamiento MAC de fragmentación proporciona el mecanismo básico con el que dividir una gran PDU MAC en componentes más pequeñas, que son transmitidas individualmente y reemsambladas a continuación en el CMTS. Por sus características, sólo es, aplicable en sentido ascendente. El formato general de el encabezamiento MAC de fragmentación DEBE ser tal como se muestra en la figura B.8-9.

Un CM conforme DEBE soportar fragmentación. Un CMTS conforme PUEDE soportar fragmentación. Para disminuir la carga del CMTS y reducir la tasa innecesaria, NO DEBEN encabezamientos de fragmentación utilizarse en tramas no fragmentadas.

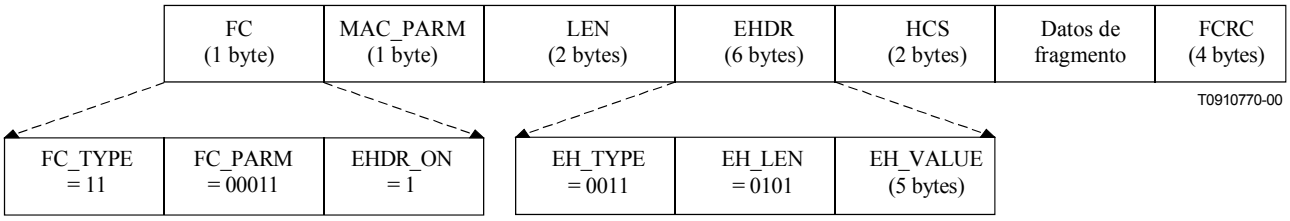


Figura B.8-9/J.112 – Formato de encabezamiento MAC de fragmentación

Cuadro B.8-9/J.112 – Formato de trama MAC de fragmentación (FRAG)

Campo	Utilización	Tamaño
FC	FC_TYPE = 11; encabezamiento MAC específico FC_PARM [4:0] = 00011; encabezamiento MAC de fragmentación EHDR_ON = 1; sigue EHDR de fragmentación	8 bits
MAC_PARM	ELEN = 6 octetos; longitud del EHDR de fragmentación	8 bits
LEN	LEN = longitud de cabida útil de fragmentos + longitud del EHDR+ longitud del FCRC	16 bits
EHDR	Véase B.8.2.6.2	6 octetos
HCS	Secuencia de verificación de encabezamiento MAC	2 octetos
Datos de fragmento	Cabida útil de fragmento; porción del total de la PDU MAC que se envía	n octetos
FCRC	CRC – CRC de 32 bits en cabida útil de datos de fragmento (tal como se define en Ethernet/ [ISO/CEI 8802-3])	4 octetos
	Longitud de trama MAC de fragmento	16 + n octetos

B.8.2.5.5 Encabezamiento de concatenación

Se define un encabezamiento MAC específico para hacer posible la concatenación de múltiples tramas MAC. Esto permite transferir una sola "ráfaga" MAC a través de la red. La tara PHY (véase la nota) y el encabezamiento MAC de concatenación sólo se producen una vez. La concatenación de múltiples tramas MAC DEBE ser como se muestra en figura B.8-10. La concatenación de tramas MAC múltiples es el único método mediante el cual el CM puede transmitir más de una trama MAC en una sola oportunidad de transmisión.

NOTA – Se incluye aquí el preámbulo, el tiempo de guarda, y posiblemente octetos de todo ceros en la última palabra de código. La tara del FEC se repite para cada palabra de código.

Un CM conforme DEBE soportar concatenación. Un CMTS conforme PUEDE soportar concatenación. La concatenación se aplica solamente al tráfico en sentido ascendente. La concatenación NO DEBE ser utilizada en el tráfico en sentido descendente.

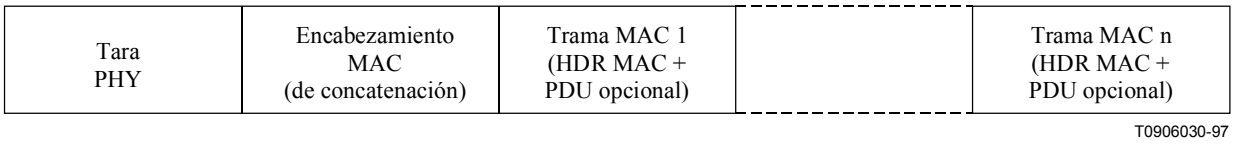


Figura B.8-10/J.112 – Concatenación de múltiples tramas MAC

Sólo un encabezamiento MAC de concatenación DEBE estar presente por "ráfaga" MAC. NO DEBE permitirse la concatenación anidada. Inmediatamente después del encabezamiento MAC de concatenación DEBE figurar el encabezamiento MAC de la primera trama MAC. La información del encabezamiento MAC indica la longitud de la primera trama MAC y sirve para encontrar el comienzo de la siguiente trama MAC. Cada trama MAC de una concatenación DEBE ser única y PUEDE ser de cualquier tipo. Esto significa que se pueden combinar tramas de PDU paquetes y tramas específicas de MAC. Sin embargo todas las tramas de una concatenación DEBEN ser asignadas al mismo flujo de servicio. Si el CMTS soporta concatenación, DEBE soportar las concatenaciones que contengan múltiples tipos de tramas, incluidas tramas de paquetes y específicas de MAC.

Las tramas MAC incorporadas PUEDEN ser dirigidas a destinos diferentes y DEBEN ser entregadas como si se transmitieran individualmente.

El formato del encabezamiento MAC de concatenación DEBE ser como se muestra en la figura B.8-11 y en el cuadro B.8-10.

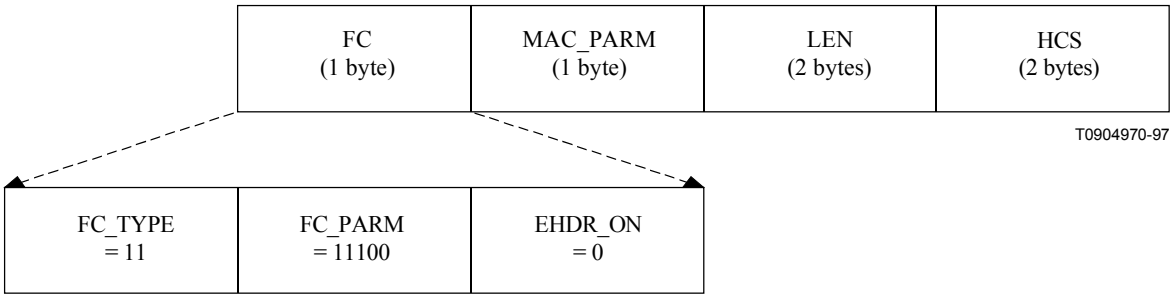


Figura B.8-11/J.112 – Formato de encabezamiento MAC de concatenación

Cuadro B.8-10/J.112 – Formato de trama MAC concatenada

Campo	Utilización	Tamaño
FC	FC_TYPE = 11; encabezamiento MAC específico FC_PARM[4:0] = 11100; encabezamiento MAC de concatenación EHDR_ON = 0; ningún EHDR con encabezamiento de concatenación	8 bits
MAC_PARM	CNT, número de tramas MAC en esta concatenación CNT = 0 indica número no especificado de tramas MAC	8 bits
LEN	LEN = x +…+ y; longitud de todas las tramas MAC siguientes en octetos	16 bits
EHDR	NO DEBE utilizarse encabezamiento MAC ampliado	0 octetos
HCS	Secuencia de verificación de encabezamiento MAC	2 octetos
Trama MAC 1	Primera trama MAC: encabezamiento MAC más PDU datos OPCIONAL	x octetos
Trama MAC n	Última trama MAC: encabezamiento MAC más PDU datos OPCIONAL	y octetos
	Longitud de trama MAC concatenada	6 + LEN octetos

El campo MAC_PARM del encabezamiento MAC de concatenación proporciona un conteo de las tramas MAC, por contraposición a la longitud EHDR o el número de REQ que se utilizan en otros encabezamientos MAC. Si el campo es distinto de cero, DEBE indicar el conteo total de tramas de MAC (CNT) en esta ráfaga de concatenación.

B.8.2.6 Encabezamientos MAC ampliados

Todos los encabezamientos MAC, excepto el de temporización, el de concatenación y el de trama de petición, tienen la posibilidad de definir un campo encabezamiento ampliado (EHDR). La presencia de un campo EHDR DEBE ser indicada por la bandera EHDR_ON en el campo FC que se fija. Cuando se fija este bit, se DEBE utilizar el campo MAC_PARM como el de longitud del EHDR (ELEN, *EHDR length*). El EHDR definido mínimo es de un octeto. La longitud máxima del EHDR es de 240 octetos.

Una combinación de CMTS y CM conforme DEBE soportar encabezamientos ampliados.

El formato de un encabezamiento MAC genérico con encabezamiento ampliado incluido DEBE ser como se muestra en la figura B.8-12 y en el cuadro B.8-11.

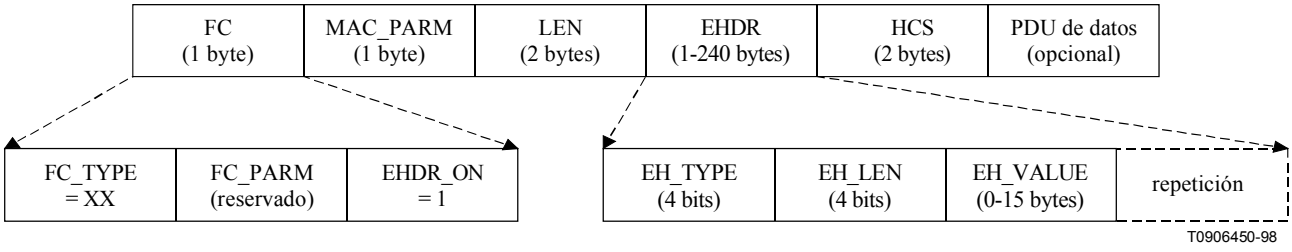


Figura B.8-12/J.112 – Formato de MAC ampliado

Cuadro B.8-11/J.112 – Formato de encabezamiento ampliado

Campo	Utilización	Tamaño
FC	FC_TYPE = XX; se aplica a todos los encabezamientos MAC FC_PARM[4:0] = XXXXX; depende de FC_TYPE EHDR_ON = 1; EHDR presente en este ejemplo	8 bits
MAC_PARM	ELEN = x; longitud de EHDR en octetos	8 bits
LEN	LEN = x + y; longitud de EHDR más PDU datos OPCIONAL en octetos	16 bits
EHDR	El encabezamiento MAC ampliado está presente en este ejemplo	x octetos
HCS	Secuencia de verificación de encabezamiento MAC	2 octetos
PDU	PDU datos OPCIONAL	y octetos
	Longitud de trama MAC con EHDR	6 + x + y octetos

Los encabezamientos ampliados NO DEBEN ser utilizados en un encabezamiento MAC de concatenación, pero PUEDEN ser incluidos como parte de los encabezamientos MAC dentro de la concatenación.

Los encabezamientos ampliados NO DEBEN ser utilizados en encabezamientos MAC de petición y temporización.

Puesto que el EHDR aumenta la longitud de la trama MAC el campo LEN DEBE incrementarse para incluir tanto la longitud de la PDU datos como la longitud del EHDR.

El campo EHDR consta de uno o más elementos EH. Cada elemento EH tiene un tamaño distinto. El primer octeto del elemento EH DEBE contener un campo tipo y un campo longitud. Los CM DEBEN utilizar esta longitud para saltarse cualquier elemento EH desconocido. El formato de un elemento EH DEBE ser como se muestra en el cuadro B.8-12.

Cuadro B.8-12/J.112 – Formato de elemento EH

Campo de elemento EH	Utilización	Tamaño
EH_TYPE	Campo tipo de elemento EH	4 bits
EH_LEN	Longitud de EH_VALUE	4 bits
EH_VALUE	Datos de elemento EH	0-15 octetos

Los tipos de elemento EH definidos en el cuadro B.8-13 DEBEN ser soportados. Los tipos reservado y ampliado no se definen en este punto y DEBEN ser ignorados.

Los diez primeros tipos de elemento EH tienen por objeto la transferencia unidireccional entre el módem del cable y el CMTS. Los cinco tipos de elemento EH siguientes son para utilización de extremo a extremo dentro de un dominio de subcapa MAC. Por eso, la información incorporada a los elementos 10-14 del EHDR en sentido ascendente DEBE agregarse también cuando se retransmite la información dentro de un dominio de subcapa MAC. El tipo de elemento EH final es un mecanismo de escape que permite disponer de más tipos y de valores más largos, y DEBE ser como se muestra en el cuadro B.8-13.

Cuadro B.8-13/J.112 – Tipo de encabezamiento ampliado

EH_TYPE	EH_LEN	EH_VALUE
0	0	Fijación de configuración nula: se puede utilizar para rellenar el encabezamiento ampliado. El EH_LEN DEBE ser cero, pero el ajuste de la configuración puede ser repetido
1	3	Petición: pedidos miniintervalos de tiempo (1 octeto); SID (2 octetos) [CM → CMTS]
2	2	Pedido acuse de recibo; SID (2 octetos) [CM → CMTS]
3 (= BP_UP)	4	Elemento EH de privacidad en sentido ascendente [DOCSIS8]
	5	Elemento EH de privacidad en sentido ascendente con fragmentación (véase la nota), [DOCSIS8] (véase B.8.2.7)
4 (= BP_DOWN)	4	Elemento EH de privacidad en sentido descendente [DOCSIS8]
5	1	Elemento EH de flujo de servicio; encabezamiento de supresión del encabezamiento de la cabida útil en sentido descendente
6	1	Elemento EH de flujo de servicio, encabezamiento de supresión del encabezamiento de la cabida útil en sentido ascendente
	2	Elemento EH de flujo de servicio; encabezamiento de supresión del encabezamiento de la cabida útil en sentido ascendente (1 octeto), encabezamiento de sincronización de concesión no solicitada (1 octeto)
7-9		Reservado
10-14		Reservado [CM ↔ CM]
15	XX	Elemento EH ampliado: EHX_TYPE (1 octeto), EHX_LEN (1 octeto), EH_VALUE (longitud determinada por EHX_LEN)
NOTA – Un elemento EH de privacidad en sentido ascendente con fragmentación DEBE aparecer solamente en el contexto de un encabezamiento MAC específico de fragmentación (véase B.8.2.5.4).		

B.8.2.6.1 Peticiones de porteo

Se pueden utilizar varios encabezamientos ampliados para pedir anchura de banda para transmisiones subsiguientes. Estas peticiones se conocen como "peticiones de porteo" o "peticiones de remolque". Son muy importantes a efectos de la calidad de funcionamiento porque no son objeto de contienda, como lo son las tramas de petición (véase B.9.4).

Las peticiones de anchura de banda adicional pueden incluirse en los elementos encabezamiento ampliado de petición, de privacidad en sentido ascendente y de privacidad en sentido ascendente con fragmentación.

B.8.2.6.2 Encabezamiento ampliado de fragmentación

Los paquetes fragmentados utilizan una combinación del encabezamiento MAC de fragmentación y una versión modificada del encabezamiento ampliado de privacidad en sentido ascendente. La subcláusula B.8.2.5.4 describe el encabezamiento de fragmentación MAC. El encabezamiento ampliado de privacidad en sentido ascendente con fragmentación, conocido también como el encabezamiento ampliado con fragmentación, DEBE ser tal como se muestra en el cuadro B.8-14.

Cuadro B.8-14/J.112 – Formato de encabezamiento ampliado de fragmentación

Campo de elemento EH	Utilización	Tamaño
EH_TYPE	Elemento EH de privacidad en sentido ascendente = 3	4 bits
EH_LEN	Longitud del EH_VALUE = 5	4 bits
EH_VALUE	Key_seq; la misma que en BP_UP	4 bits
	Ver = 1; número de versión de este EHDR	4 bits
	BPI_ENABLE Si BPI_ENABLE = 0, BPI inhabilitado Si BPI_ENABLE = 1, BPI habilitado	1 bit
	Bit de conmutación; tal como el BP_UP (véase la nota)	1 bit
	SID; identificador de servicio asociado con este fragmento	14 bits
	REQ; número de miniintervalos de tiempo para una petición de porteo	8 bits
	Reservado; se debe fijar a cero	2 bits
	First_Frag; se fija a uno para el primer fragmento solamente	1 bit
	Last_Frag; se fija a uno para el último fragmento solamente	1 bit
	Frag_seq; contador de secuencia de fragmentos, que es incrementado por cada fragmento	4 bits
NOTA – Véase [DOCSIS8].		

B.8.2.6.3 Encabezamiento ampliado de flujo de servicio

El elemento EH de un flujo de servicio se utiliza para potenciar las operaciones de dicho flujo. Puede estar compuesto por uno o dos octetos en el campo del EH_VALUE. El encabezamiento de supresión del encabezamiento de la cabida útil es el único octeto en un campo de un solo octeto o el primer octeto en un campo de dos octetos. El encabezamiento de sincronización de concesión no solicitada es el segundo octeto en un campo de dos octetos.

B.8.2.6.3.1 Encabezamiento de supresión de encabezamiento de cabida útil

En la supresión de encabezamiento de cabida útil (PHS, *payload header suppression*), la entidad emisora elimina una parte repetitiva de los encabezamientos de cabida útil, que viene después de la HCS, mientras que la entidad receptora la restablece. En el sentido ascendente, la entidad emisora es el CM y la entidad receptora es el CMTS. En el sentido descendente, la entidad emisora es el CMTS y la entidad receptora es el CM.

La supresión de encabezamiento de cabida útil proporciona, para cabidas útiles pequeñas, una eficiencia de anchura de banda incrementada sin necesidad de utilizar la compresión. La supresión de encabezamiento de cabida útil puede ser aprovisionada separadamente en el sentido ascendente y en el sentido descendente, y se hace referencia a la misma con un elemento encabezamiento ampliado.

Un CM conforme DEBE soportar la supresión de encabezamiento de cabida útil. Un CMTS conforme PUEDE soportar la supresión de encabezamiento de cabida útil.

Esto no implica que el CM deba ser capaz de determinar cuándo se ha de invocar la supresión de encabezamiento de cabida útil. El soporte de la supresión sólo se requiere en los casos en que se ha señalado explícitamente.

El subelemento encabezamiento ampliado de supresión de encabezamiento de cabida útil tiene el formato como en el cuadro B.8-15.

Cuadro B.8-15/J.112 – Formato del subelemento EHDR de supresión de encabezamiento de cabida útil

Campos del elemento EH	Utilización		Tamaño
EH_TYPE	EH_TYPE de flujo de servicio = 5 para el sentido descendente y EH_TYPE = 6 para el sentido ascendente		4 bits
EH_LEN	Longitud del EH_VALUE = 1		4 bits
EH_VALUE	0	Indica ausencia de supresión de encabezamiento de cabida útil en el paquete en curso.	8 bits
	1-255	Índice de supresión de encabezamiento de carga útil (PHSI)	

El índice de supresión de encabezamiento de cabida útil (PHSI) es único para cada SID en el sentido ascendente, y único para cada CM en el sentido descendente. La supresión de encabezamiento de cabida útil es inhabilitada si este elemento encabezamiento ampliado ha sido omitido o, si está incluido, con el valor del PHSI fijado a 0. El índice de supresión de encabezamiento de cabida útil (PHSI, *payload header suppression index*) hace referencia a la cadena de octetos suprimida, que se conoce como campo de supresión de encabezamiento de cabida útil (PHSF, *payload header suppression field*).

Aunque la señalización del PHS permite hasta 255 reglas de supresión de encabezamiento de cabida útil por flujo de servicio, el número exacta de reglas de PHS aceptadas por flujo de servicio depende de la implementación. De manera similar, la señalización del PHS permite tamaños de PHS de hasta 255 octetos, sin embargo, el tamaño máximo de PHS soportado depende de la implementación. Los efectos de interoperabilidad, el tamaño mínimo de PHS que DEBE ser soportado, es de 64 octetos para cualquier regla PHS soportada. Tal como ocurre con cualquier otro parámetro solicitado en una petición de servicio dinámica, una petición de DSx relacionada con el PHS puede ser rechazada por falta de recursos.

El campo supresión en sentido ascendente DEBE comenzar con el primer octeto tras la verificación de la suma del encabezamiento MAC. El campo supresión en sentido descendente DEBE comenzar con el decimotercer octeto tras la verificación de la suma del encabezamiento MAC. Esto permite que los SA y DA Ethernet estén disponibles para ser filtrados por el CM.

El funcionamiento de la privacidad básica (véase [DOCSIS8]) no se ve afectada por la utilización del PHS. Cuando la fragmentación está inactiva, la privacidad básica empieza la criptación y descriptación con el decimotercer octeto tras la verificación de la suma del encabezamiento MAC.

A menos que toda la PDU paquetes sea suprimida, la CRC de la PDU paquetes se transmite siempre y se DEBE calcular solamente en base a los octetos transmitidos. Los octetos que no son suprimidos NO se DEBEN incluir en el cálculo de la CRC.

B.8.2.6.3.2 Encabezamiento de sincronización de concesión no solicitada

El encabezamiento de sincronización de concesión no solicitada puede ser utilizado para pasar información de estatus, relacionada con la programación del flujo de servicio, entre el CM y el CMTS. Por lo general sólo se define para utilización en el sentido ascendente con servicios de programación de concesión no solicitada, y de concesión no solicitada con detección de actividad (véase B.10.2).

Este encabezamiento ampliado es similar al EHDR de supresión de cabida útil, excepto que el EH_LEN es 2, y el EH_VALUE tiene un octeto adicional, que incluye información relacionada con la sincronización de concesión no solicitada (véase el cuadro B.8-16). Para todos los demás tipos de programación de flujo de servicio, el campo NO DEBERÍA ser incluido en el elemento de encabezamiento ampliado generado por el CM. El CMTS PUEDE ignorar este campo.

Cuadro B.8-16/J.112 – Formato del subelemento EHDR de sincronización de concesión no solicitada

Campos del elemento EH	Utilización		Tamaño
EH_TYPE	EH_TYPE de flujo de servicio = 6		4 bits
EH_LEN	Longitud de EH_VALUE = 2		4 bits
EH_VALUE	0	Indica ausencia de supresión de encabezamiento de cabida útil en el paquete en curso	8 bits (presente)
	1-255	Índice de supresión de encabezamiento de cabida útil (PHSI)	
	Indicador de cola		1 bit
	Concesiones activas		7 bits

B.8.2.7 Tramas MAC fragmentadas

Cuando está habilitada la fragmentación (véase el cuadro B.8-13) se inicia en cualquier momento en que la longitud de la concesión sea menor que la longitud requerida. Esto ocurre normalmente porque el CMTS decide conceder una anchura de banda inferior a la pedida.

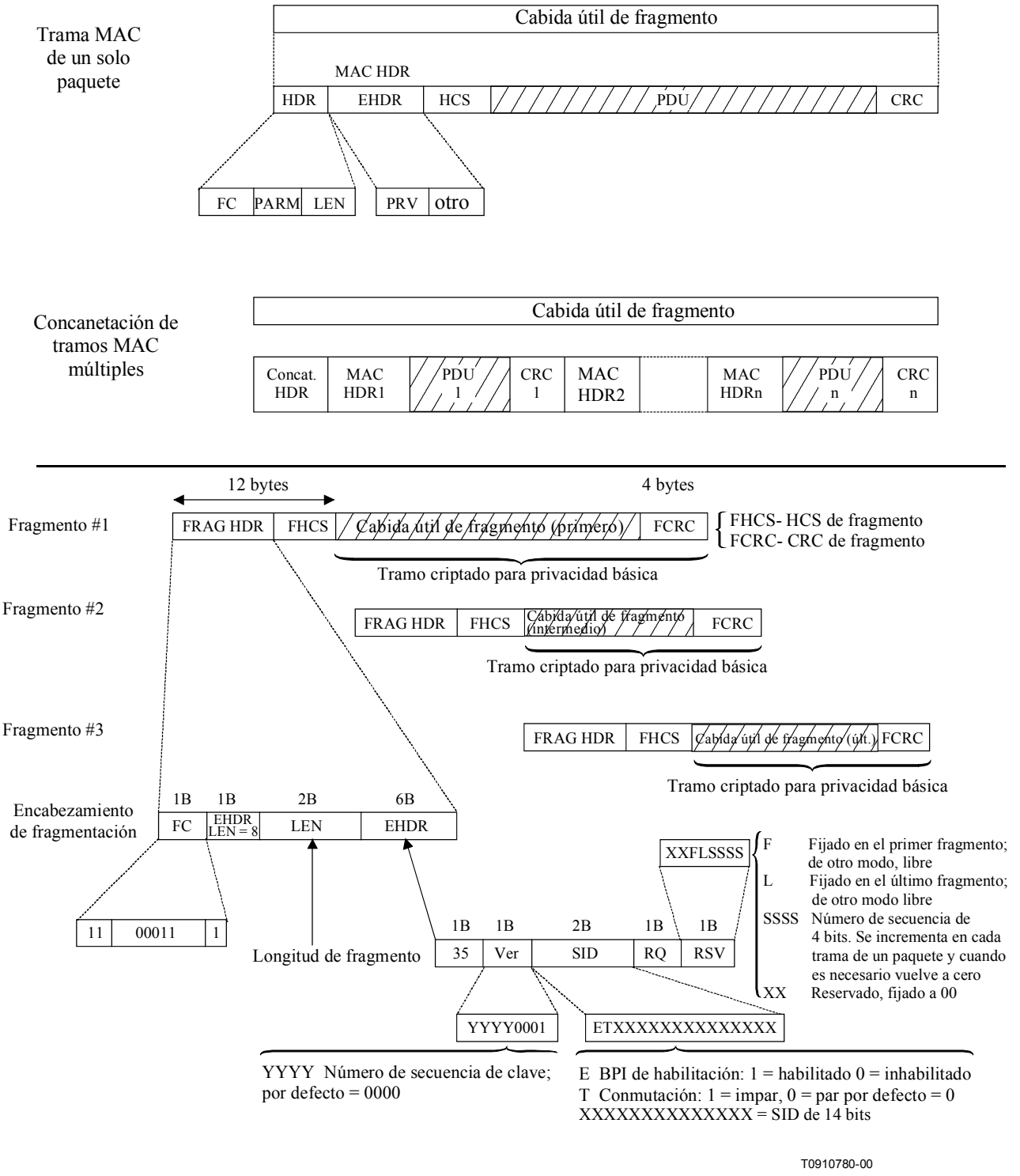


Figura B.8-13/J.112 – Detalles de la fragmentación

El MAC del CM calcula cuántos octetos de la trama original, incluida la tara por un encabezamiento de fragmentación y la CRC, pueden ser enviados en la concesión recibida. El MAC del CM genera un encabezamiento de fragmentación por cada fragmento. Las tramas fragmentadas utilizan el tipo de mensaje MAC (FC = 11). El campo parámetro de FC se fija a (00011), para poder identificar de manera exclusiva el encabezamiento de fragmentación de los otros tipos de mensaje MAC. En el último octeto del campo encabezamiento ampliado se utiliza un campo de secuencia de 4 bits para ayudar en el reensamblado y a detectar fragmentos perdidos o faltantes. El CM selecciona arbitrariamente un número de secuencia para el primer fragmento de una trama (véase la nota). Una

vez seleccionado, el CM DEBE incrementar el número de secuencia en una unidad por cada fragmento transmitido de esa trama. Existen dos banderas asociadas con el número de secuencia, F y L, en donde F se fija para indicar primer fragmento y L para indicar último fragmento. Ambas están libres para los fragmentos intermedios. El CMTS almacena el número de secuencia del primer fragmento (el bit F fijado) de cada trama. El CMTS DEBE verificar que el campo de secuencia del fragmento se incrementa (en una unidad) por cada fragmento de la trama.

NOTA – "Trama" se refiera siempre a tramas con una sola PDU paquetes o a tramas concatenadas.

El campo REQ del encabezamiento de fragmentación es utilizado por el protocolo de fragmentación para los fragmentos primero e intermedio (véase B.10.3). En el fragmento último, el campo REQ es interpretado como una petición de anchura de banda para una trama subsiguiente.

Los encabezamientos de fragmentación tienen un tamaño fijo y DEBEN contener un solo elemento de encabezamiento ampliado de fragmentación. El encabezamiento ampliado consiste en un elemento EH de privacidad ampliado en 1 octeto para hacer que la tara del fragmento sea exactamente de 16 octetos. Se utiliza un elemento EH de privacidad, tanto si el encabezamiento del paquete original tiene un elemento EH de privacidad como si no lo tiene. Si se utiliza privacidad, el número de secuencia de clave, la versión, el bit de habilitación, el bit de conmutación, y el SID del elemento EH del fragmento son los mismos que los del elemento EH del BP dentro de la trama MAC original. Si no se utiliza privacidad, si se utiliza el elemento EH de privacidad, pero el bit de habilitación está libre. El SID utilizado en el elemento EH del fragmento DEBE concordar con el SID utilizado en la concesión parcial que inició la fragmentación. El mismo encabezamiento ampliado debe ser utilizado para todos los fragmentos de un paquete. Se debe calcular una CRC aparte para cada fragmento (se señala que cada cabida útil de trama MAC contendrá, también, la CRC para ese paquete). La CRC de paquete de un paquete reensamblado PUEDE ser controlada por el CMTS aun cuando una FCRC abarque cada fragmento.

El CMTS DEBE garantizar que cualquier concesión fragmentaria que haga sea lo suficientemente grande como para retener al menos 17 octetos de datos de capa MAC. Con esto se pretende asegurar que la concesión es lo suficientemente grande como para acomodar la tara de fragmentación más 1 octeto de datos reales como mínimo. Es posible que el CMTS quiera fijar un límite incluso mayor, ya que los fragmentos pequeños son extremadamente ineficientes.

Cuando la fragmentación, está activa, la criptación y la descriptación de la privacidad básica empiezan con el primer octeto tras la verificación de la suma del encabezamiento MAC.

B.8.2.7.1 Consideraciones relativas a paquetes concatenados y fragmentación

Los mensajes de gestión MAC y los PDU datos pueden aparecer en la misma trama concatenada. Sin fragmentación, los mensajes de gestión MAC dentro de una trama concatenada estarían descriptados. Sin embargo, con fragmentación habilitada en la trama concatenada, esta trama es criptada en su totalidad en base al elemento de encabezamiento ampliado de privacidad. De esta manera, la privacidad básica puede encriptar cada fragmento sin examinar su contenido. En realidad, esto sólo se aplica cuando la privacidad básica ha sido habilitada.

Para asegurar la sincronización de la criptación, si la fragmentación, la concatenación y la privacidad básica están habilitadas, un CM NO DEBE concatenar mensajes de gestión MAC de BPKM. Así se garantiza el que los mensajes de gestión MAC de BPKM sean enviados siempre desencriptados.

B.8.2.8 Tratamiento de errores

La red de cable es un entorno potencialmente difícil, en el que es posible que se produzcan varias condiciones de error diferentes. En esta cláusula, y en B.11.5, se describen los procedimientos que es preciso aplicar cuando se produce una situación excepcional a nivel de alineación de trama MAC.

El tipo de error más elemental es el que se produce cuando falla la HCS en el encabezamiento MAC. Esto puede deberse al ruido en la red o quizás a colisiones en el canal en sentido ascendente. La recuperación de la alineación de trama en el canal de sentido descendente la lleva a cabo la subcapa de convergencia de transmisión MPEG. En el canal en sentido ascendente, la alineación de trama se recupera en cada ráfaga transmitida, por lo que la alineación de trama en una ráfaga es dependiente de la alineación de trama en las ráfagas anteriores. Por ello, los errores de alineación de trama en una ráfaga se tratan ignorando simplemente esa ráfaga; es decir, los errores son irrecuperables hasta la ráfaga siguiente.

Una segunda situación excepcional, aplicable sólo al sentido ascendente, se producen cuando el campo longitud está degradado y el MAC piensa que la trama tiene una longitud superior a la que realmente tiene. La sincronización se recuperará en el siguiente intervalo de datos en sentido ascendente válido.

LA HCS se DEBE verificar para cada transmisión MAC. Cuando se detecte una HCS errónea, se DEBE prescindir del encabezamiento MAC y de cualquier cabida útil.

En el caso de transmisiones de PDU paquetes, puede ser detectada una CRC con resultado negativo. Puesto que la CRC sólo abarca la PDU datos y la HCS abarca el encabezamiento MAC, este último se considera todavía válido. Así pues, DEBE prescindirse de la PDU paquetes, pero PUEDE utilizarse cualquier información pertinente del encabezamiento MAC (por ejemplo, información de petición de anchura de banda).

B.8.2.8.1 Recuperación tras error durante la fragmentación

El tratamiento de errores durante la fragmentación permite hacer algunas consideraciones especiales. Cada fragmento tiene su propio encabezamiento de fragmentación completo con un HCS y su propia FCRC. PUEDE haber otros encabezamientos MAC y otras CRC dentro de la cabida útil fragmentada. Sin embargo, sólo la HCS de encabezamiento de fragmento y la FCRC se utilizan para la detección de errores durante el reensamblado del fragmento.

Si la HCS de un fragmento falla, el CMTS DEBE descartar ese fragmento. Si la HCS pasa pero la FCRC falla, el CMTS DEBE descartar ese fragmento, pero PUEDE procesar cualesquiera peticiones del encabezamiento del fragmento. El CMTS DEBERÍA procesar cualquiera de esas peticiones si está realizando la fragmentación en modo porteo (véase B.10.3.2.2). Así se facilita la transmisión del resto de la trama tan rápido como sea posible.

Si un CMTS realiza la fragmentación en modo de concesiones múltiples (véase B.10.3.2.1) DEBERÍA completar todas las concesiones necesarias para satisfacer la petición original del CM, incluso si se pierde o se descarta un fragmento. Esto permite que el resto de la trama sea transmitido tan rápido como sea posible.

Si se pierde o se descarta cualquier fragmento de una trama MAC no concatenada, el CMTS DEBE descartar el resto de esa trama. Si se pierde o se descarta un fragmento de una trama MAC concatenada, el CMTS PUEDE reenviar cualesquiera tramas dentro de la concatenación que hayan sido recibidas correctamente o puede descartar todas las tramas de la concatenación.

Un CMTS DEBE terminar el reensamblado de fragmentos si se da cualquiera de las condiciones siguientes para cualquier fragmento de un SID determinado:

- el CMTS recibe un fragmento con el bit L fijado;
- el CMTS recibe un fragmento en sentido ascendente, distinto del primero, con el bit F fijado;
- el CMTS recibe una trama de PDU paquetes sin encabezamiento de fragmentación;
- el CMTS elimina el SID por cualquier motivo.

Además, el CMTS PUEDE terminar el reensamblado de fragmentos en base a criterios que dependen de la implementación, por ejemplo, el temporizado de reensamblado. Cuando un CMTS termina el reensamblado de fragmentos DEBE deshacerse (descartando o reenviando) de la(s) trama(s) reensamblada(s).

B.8.2.8.2 Códigos y mensajes de error

El anexo B.J contiene una lista de los códigos y mensajes de error de un CM y un CMTS. Cuando se informe de condiciones de error, estos códigos DEBEN ser utilizados tal como se indica en [DOCSIS5] y PUEDEN ser utilizados para informar sobre errores a través de interfaces específicas de los vendedores. Si se utilizan códigos de error, los mensajes de error PUEDEN ser reemplazado por otros mensajes descriptivos.

B.8.3 Mensajes de gestión MAC

B.8.3.1 Encabezamiento de mensaje de gestión MAC

Los mensajes de gestión MAC DEBEN estar encapsulados en una trama de información no numerada LLC según [ISO/CEI 8802-2], que a su vez se encapsula en la alineación de trama MAC de la red de cable, como se indica en la figura B.8-14. Dicha figura B.8-14 muestra los campos encabezamiento MAC y encabezamiento de los mensajes de gestión MAC que son comunes a todos los mensajes MAC.

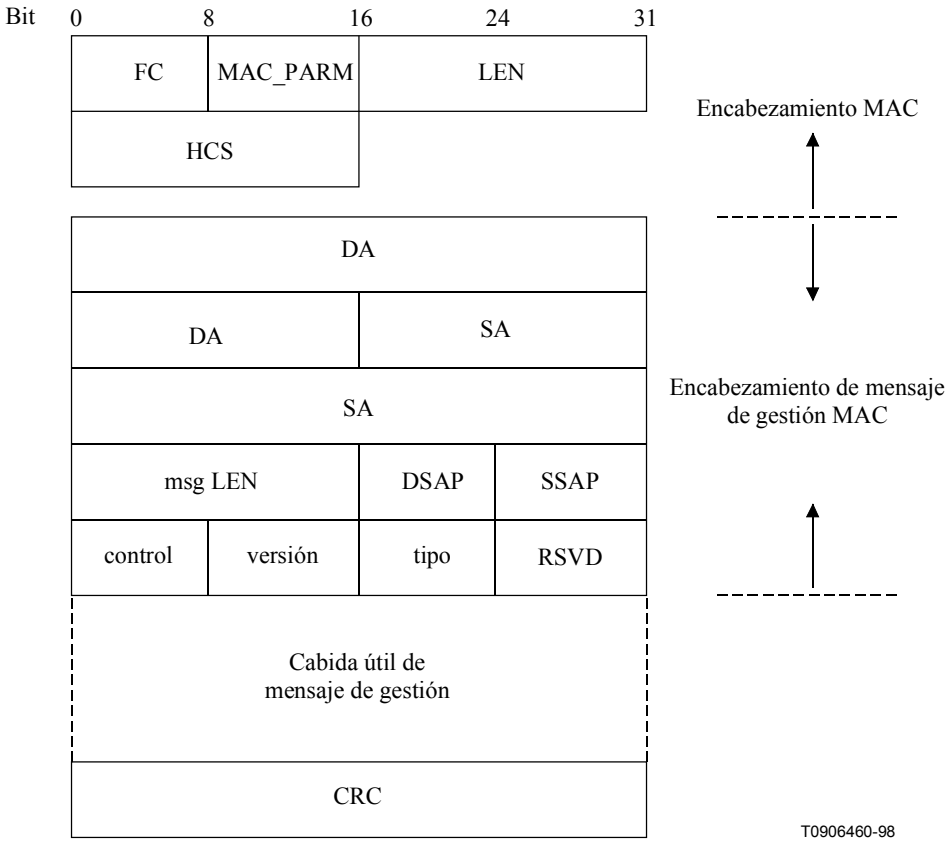


Figura B.8-14/J.112 – Campos encabezamiento MAC y encabezamiento de mensaje de gestión MAC

Los campos DEBEN ser como se define a continuación:

FC, MAC_PARM, LEN, HCS: Encabezamiento de trama MAC común; para más detalles, véase B.8.2.1.4. Todos los mensajes utilizan un encabezamiento especifico de MAC.

Dirección de destino (DA, *destination address*): Las tramas de gestión MAC se dirigirán a una dirección de unidifusión de CM específica o a la dirección de multidifusión de gestión del DOCSIS. Las direcciones de gestión MAC de DOCSIS se describen en el anexo B.A.

Dirección de origen (SA, *source address*): Dirección MAC del CM de origen o del sistema CMTS.

Longitud de mensaje: Longitud total del mensaje MAC de la DA a la CRC inclusive.

DSAP: SAP nulo de destino (00) de LLC definido por [ISO/CEI 8802-2].

SSAP: SAP nulo de origen (00) de LLC definido por [ISO/CEI 8802-2].

Control: Trama de información no numerada (03) LLC definida por [ISO/CEI 8802-2].

Versión y tipo: 1 octeto para cada uno. Véase el cuadro B.8-17.

Cuadro B.8-17/J.112 – Tipos de mensaje de gestión MAC

Valor del tipo	Versión	Nombre del mensaje	Descripción del mensaje
1	1	SYNC	Sincronización de temporización
2	1	UCD	Descriptor de canal en sentido ascendente
3	1	MAP	Atribución de anchura de banda en sentido ascendente
4	1	RNG-REQ	Petición de alineación
5	1	RNG-RSP	Respuesta de alineación
6	1	REG-REQ	Petición de registro
7	1	REG-RSP	Respuesta de registro
8	1	UCC-REQ	Petición de cambio de canal en sentido ascendente
9	1	UCC-RSP	Respuesta de cambio de canal en sentido ascendente
10	1	TRI-TCD	Descriptor de canal de telefonía [DOCSIS6]
11	1	TRI-TSI	Información de sistema de terminación [DOCSIS6]
12	1	BPKM-REQ	Petición de mensaje de clave de privacidad [DOCSIS8]
13	1	BPKM-RSP	Respuesta de mensaje de clave de privacidad [DOCSIS8]
14	2	REG-ACK	Acuse de recibo de registro
15	2	DSA-REQ	Petición dinámica de adición al servicio
16	2	DSA-RSP	Respuesta dinámica a la petición de adición
17	2	DSA-ACK	Acuse de recibo dinámico a la adición al servicio
18	2	DSC-REQ	Petición dinámica de cambio de servicio
19	2	DSC-RSP	Respuesta dinámica a la petición de cambio
20	2	DSC-ACK	Acuse de recibo dinámico al cambio de servicio
21	2	DSD-REQ	Petición dinámica de supresión del servicio
22	2	DSD-RSP	Respuesta dinámica a la supresión del servicio
23	2	DCC-REQ	Petición dinámica de cambio de canal
24	2	DCC-RSP	Respuesta dinámica a la petición de cambio decisivo
25	2	DCC-ACK	Acuse de recibo dinámico del cambio de canal

Cuadro B.8-17/J.112 – Tipos de mensaje de gestión MAC

Valor del tipo	Versión	Nombre del mensaje	Descripción del mensaje
26	2	DCI-REQ	Petición de identificación de la clase de dispositivo
27	2	DCI-RSP	Respuesta a la supresión de identificación de la clase de dispositivo
28	2	UP-DIS	Inhabilitar al transmisor en sentido ascendente
29-255			Reservado para utilización futura

RSVD: 1 octeto. Campo utilizado para alinear la cabida útil del mensaje en un límite de 32 bits. Fijado a 0 para la presente versión.

Cabida útil de mensaje de gestión: Longitud variable. Definida para cada mensaje de gestión específico.

CRC: Abarca el mensaje incluyendo los campos de encabezamiento (DA, SA, ...). Polinomio definido por [ISO/CEI 8802-3].

Un CMTS o un CM conforme DEBE soportar los tipos de mensaje de gestión MAC listados en el cuadro B.8-17, excepto los mensajes específicos para los dispositivos que pueden dar soporte al retorno para la telefonía.

B.8.3.2 Sincronización de tiempo (SYNC)

La sincronización de tiempo (SYNC) DEBE ser transmitida por el CMTS a intervalos periódicos para establecer la temporización de las subcapas MAC. Este mensaje DEBE utilizar un campo FC con encabezamiento específico FC_TYPE = MAC y encabezamiento MAC FC_PARM = temporización al que DEBE seguir una PDU paquetes con el formato que se muestra en la figura B.8-15.

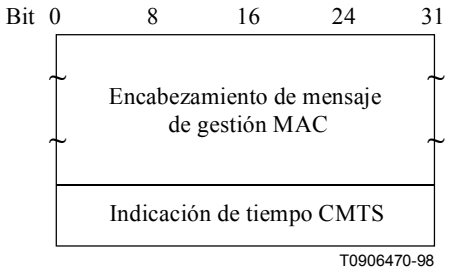


Figura B.8-15/J.112 – Formato de PDU paquetes que sigue al encabezamiento de temporización

Los parámetros serán como se define a continuación:

Indicación de tiempo de CMTS: El estado de conteo de un contador binario creciente de 32 bits sincronizado con el reloj maestro CMTS de 10,24 MHz.

La indicación de tiempo CMTS representa el estado de conteo en el instante en que el primer octeto (o un desplazamiento fijo de tiempo a partir del primer octeto) del mensaje de gestión MAC de sincronización de tiempo, se transfiere desde la subcapa de convergencia de transmisión en sentido descendente a la subcapa dependiente del medio físico en sentido descendente, como se describe en B.6.3.7. El CMTS NO DEBE permitir que un mensaje SYNC cruce el límite de un paquete MPEG (véase la nota).

NOTA – Como el mensaje SYNC se aplica a todos los canales en sentido ascendente dentro de este dominio MAC, se escogieron unidades que son independientes de la velocidad de símbolos de cualquier canal particular en sentido ascendente. Un tic de la base de tiempos representa la mitad del miniintervalo de tiempo más pequeño posible a la velocidad de símbolos más alta posible. Véase B.9.3.4 para las relaciones entre las unidades de tiempo.

B.8.3.3 Descriptor de canal en sentido ascendente (UCD, *upstream channel descriptor*)

El CMTS DEBE transmitir un descriptor de canal en sentido ascendente a intervalos periódicos para definir las características de un canal en sentido ascendente (véase la figura B.8-16). Por cada sentido ascendente activo DEBE transmitirse un mensaje separado.

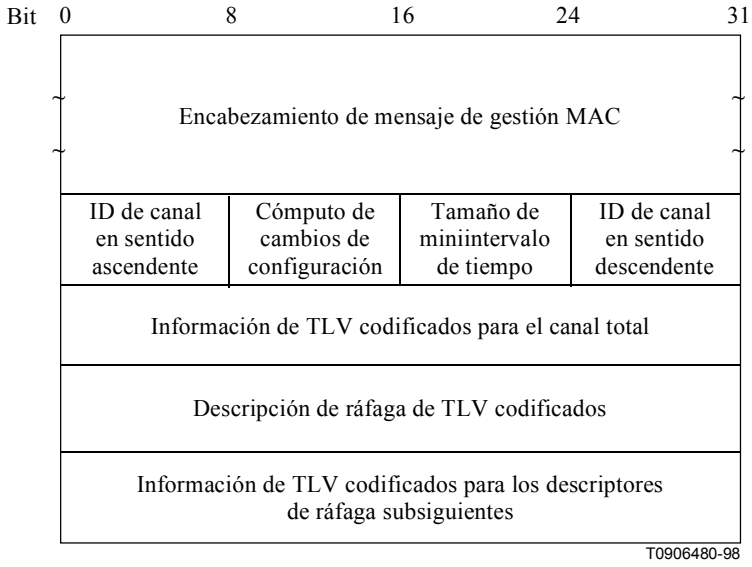


Figura B.8-16/J.112 – Descriptor de canal en sentido ascendente

Para facilitar la flexibilidad, los parámetros del mensaje que sigue al ID de canal DEBEN ser codificados en una forma de tipo/longitud/valor (TLV) en la que los campos tipo y longitud tengan cada uno de ellos una longitud de 1 octeto.

Un CMTS DEBE generar los UCD con el formato que se muestra en la figura B.8-16, incluyendo todos los parámetros que se indican a continuación:

Cuenta de cambios de configuración: Incrementada en una unidad (módulo: el tamaño del campo) por el CMTS cuando cambia cualquiera de los valores de este descriptor de canal. Si el valor de la cuenta en un UCD subsiguiente sigue siendo el mismo, el CM puede deducir rápidamente que los campos restantes no han cambiado, y desechar el resto del mensaje. A este valor se hace referencia también desde el MAP.

Tamaño de miniintervalo de tiempo: Tamaño T del miniintervalo de tiempo para este canal en sentido ascendente en unidades de tics de la base de tiempos de 6,25 µs. Los valores posibles son $T = 2^M$, M = 1, …, 7. Es decir, T = 2, 4, 8, 16, 32, 64 ó 128.

ID de canal en sentido ascendente: Identificador del canal en sentido ascendente al que se refiere este mensaje. Este identificador es elegido de manera arbitraria por el CMTS y sólo es exclusivo dentro del dominio de subcapa MAC.

NOTA – El ID canal en sentido ascendente = 0 se reserva para indicar el retorno de la telefonía [DOCSIS6].

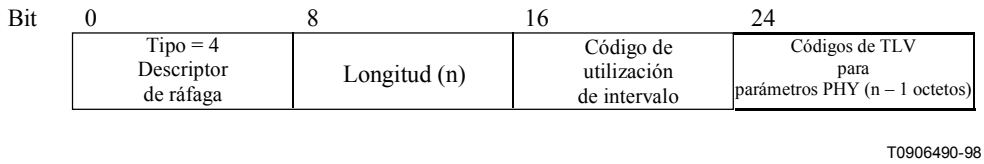
ID de canal en sentido descendente: Identificador del canal en sentido ascendente por el que se ha transmitido este mensaje. Este identificador es elegido de manera arbitraria por el CMTS y sólo es exclusivo dentro del dominio de subcapa MAC.

Todos los demás parámetros se codifican como tuplas de TLV. Los valores de tipo utilizados DEBEN ser los definidos, como parámetros de canal, en el cuadro B.8-18, y como atributos en ráfaga en sentido ascendente de capa física, en el cuadro B.8-19. Los parámetros que afectan a todo el canal (tipos 1 a 3 del cuadro B.8-18) DEBEN preceder a los descriptores de ráfaga (tipo 4).

Cuadro B.8-18/J.112 – Parámetros TLV de canal

Nombre	Tipo (1 octeto)	Longitud (1 octeto)	Valor (Longitud variable)
Velocidad de símbolos	1	1	Múltiplos de la velocidad básica de 160 ksímb/s. El valor es 1, 2, 4, 8 ó 16.
Frecuencia	2	4	Frecuencia central en sentido ascendente (Hz).
Esquema de preámbulo	3	1-128	Supercadena de preámbulo. Todos los valores del preámbulo específicos de la ráfaga se eligen como subcadenas de bits de esta cadena. El primer octeto del campo valor contiene los 8 primeros bits de la supercadena, con el primer bit de la supercadena de preámbulo en la posición MSB del primer octeto del campo valor, el octavo bit de la supercadena de preámbulo en la posición LSB del primer octeto del campo valor; el segundo octeto del campo valor contiene los segundos 8 bits de la supercadena, con el noveno bit de la supercadena en la posición MSB del segundo octeto y el decimosexto bit de la supercadena de preámbulo en la posición LSB del segundo octeto, y así sucesivamente.
Descriptor de ráfaga	4	n	Puede aparecer más de una vez; se describe más abajo.

Los descriptores de ráfagas son codificaciones de TLV compuestas por un código de utilización de intervalo en sentido ascendente, que definen, para cada tipo de intervalo de utilización en sentido ascendente, las características de la capa física que se han de utilizar durante ese intervalo. Los códigos de utilización de intervalo en sentido ascendente se definen en el mensaje MAP (véanse B.8.3.4 y el cuadro B.8-20). El formato del descriptor de ráfaga se muestra en la figura B.8-17.



Tipo 4 para descriptor de ráfaga.
Longitud Número de octetos en el objeto global, incluyendo los elementos IUC y TLV incorporados.
IUC Código de utilización de intervalo definido en el cuadro B.8-20. El IUC se codifica sobre los 4 bits menos significativos. Los 4 bits más significativos no se utilizan (=0).
Elementos TLV Parámetros TLV descritos en el cuadro B.8-19.

Figura B.8-17/J.117 – Codificación de nivel máximo para un descriptor de ráfaga

Se DEBE incluir un descriptor de ráfaga para cada código de utilización de intervalo que se va a utilizar en el MAP de atribución. El código de utilización de intervalo anterior debe ser uno de los valores del cuadro B.8-20.

Dentro de cada descriptor de ráfaga hay una lista no ordenada de atributos de capa física, codificados como valores de TLV. En el cuadro B.8-19 se muestran dichos valores.

Cuadro B.8-19/J.112 – Atributos de ráfaga de capa física en sentido ascendente

Nombre	Tipo (1 octeto)	Longitud (1 octeto)	Valor (Longitud variable)
Tipo de modulación	1	1	1 = QPSK, 2 = 16QAM
Codificación diferencial	2	1	1 = activa, 2 = inactiva
Longitud de preámbulo	3	2	Hasta 1024 bits. El valor debe ser un número entero de símbolos (un múltiplo de 2 para QPSK y de 4 para 16QAM).
Desplazamiento del valor del preámbulo	4	2	Identifica los bits que se van a utilizar para el valor del preámbulo. Se especifica como un desplazamiento de comienzo en el esquema del preámbulo (véase el cuadro B.8-18). Es decir, un valor de cero significa que el primer bit del preámbulo de este tipo de ráfaga es el valor del primer bit del esquema del preámbulo. Un valor de 100 significa que el preámbulo va a utilizar el bit 101 y los bits subsiguientes del esquema del preámbulo. Este valor debe ser un múltiplo del tamaño de los símbolos. El primer bit del esquema de preámbulo es el primer bit al que se aplica la correspondencia de símbolos (figura B.6-9), y es el bit I_1 del primer símbolo de la ráfaga (véase B.6.2.2.2).
Corrección de errores FEC (T octetos)	5	1	0 a 10 octetos (0 implica sin FEC. El número de octetos en la paridad de la palabra de código es 2*T.)
Octetos de información en la palabra de código de FEC (k)	6	1	Fija: 16 a 253 (suponiendo FEC activa) Abreviada: 16 a 253 (suponiendo FEC activa) (No se emplea si no se utiliza FEC, T=0.)

Cuadro B.8-19/J.112 – Atributos de ráfaga de capa física en sentido ascendente

Nombre	Tipo (1 octeto)	Longitud (1 octeto)	Valor (Longitud variable)
Semilla de aleatorizador	7	2	Valor de la semilla de 15 bits, justificado a la izquierda en el campo de dos octetos. El bit 15 es el MSB del primer octeto y el LSB del segundo octeto no se utiliza. (No se utiliza si el aleatorizador está desactivado.)
Tamaño máximo de ráfaga	8	1	Número máximo de miniintervalos de tiempo que pueden ser transmitidos durante una ráfaga de este tipo. La ausencia de esta fijación de configuración significa que el tamaño de la ráfaga está limitado en otro lugar. Cuando el tipo de intervalo es concesión de datos corta, este valor debe estar presente y ser mayor que cero. (Véase B.9.1.2.5.)
Duración del tiempo de guarda	9	1	Número de periodos de duración de un símbolo que deben transcurrir tras el final de esta ráfaga. (Aunque este valor se puede deducir de los parámetros de otra red y de los parámetros arquitecturales, se incluye aquí para asegurar que los CM y el CMTS utilizan todos ellos el mismo valor.)
Longitud de la última palabra de código	10	1	1 = fija; 2 = abreviada
Aleatorizador activo/inactivo	11	1	1 = activo; 2 = inactivo

B.8.3.3.1 Ejemplo de datos de TLV con codificación de UCD

En la figura B.8-18 se da un ejemplo de datos TLV con codificación de UCD.

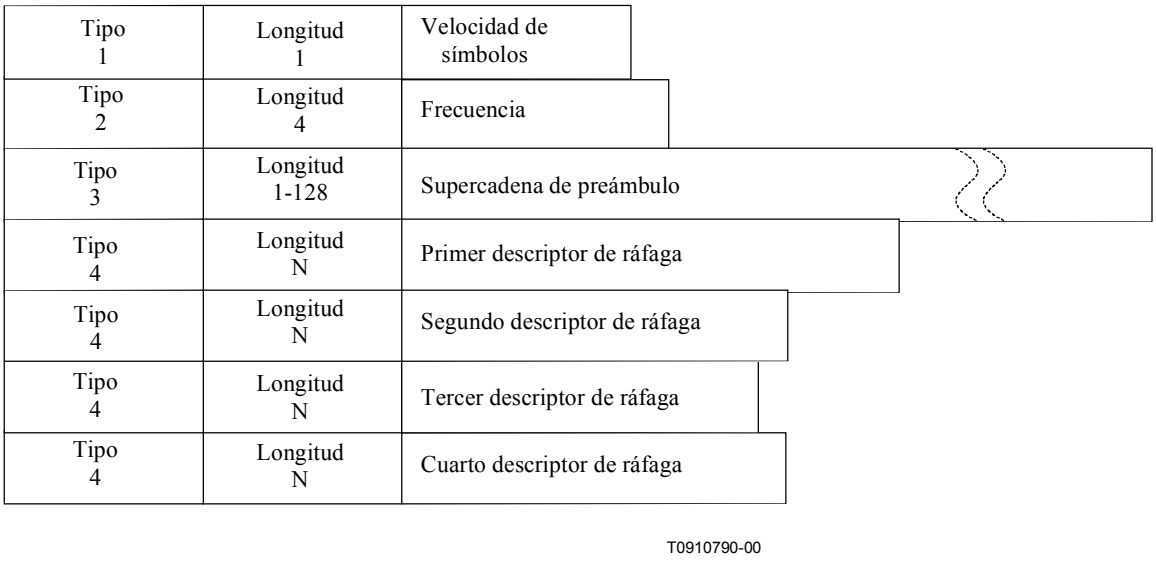


Figura B.8-18/J.112 – Ejemplo de datos de TLV con codificación de UCD

B.8.3.4 Diagrama de atribución de anchura de banda en sentido ascendente (MAP)

Un CMTS DEBE generar los MAP con el formato que se muestra en la figura B.8.19.

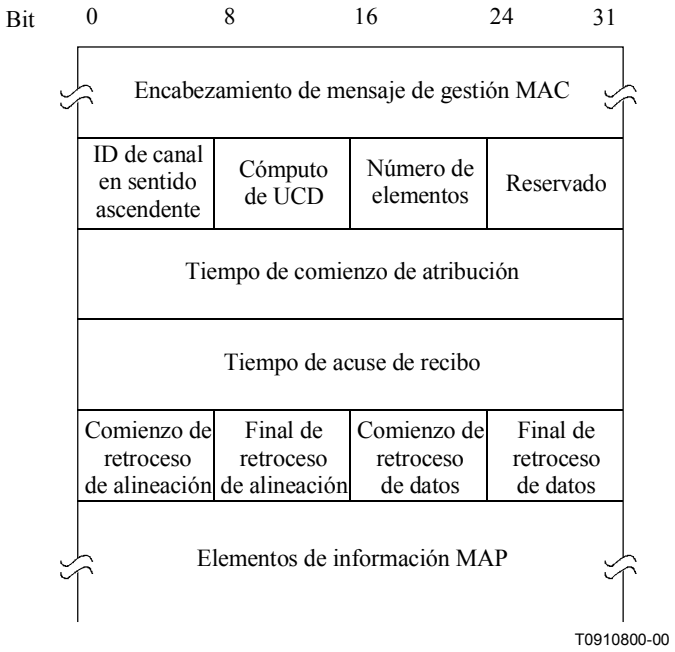


Figura B.8-19/J.112 – Formato de MAP

Los parámetros DEBEN ser como sigue:

ID de canal: Identificador del canal en sentido ascendente al que se refiere este mensaje.

Cuenta de UCD: Concuerda con el valor de la cuenta de cambios de configuración del UCD que describe los parámetros de ráfagas aplicables a este diagrama. Véase B.11.3.2.

Número de elementos: Número de elementos de información del diagrama.

Reservado: Campo reservado para alineación.

Tiempo de comienzo de atribución: Tiempo de comienzo efectivo a partir de la inicialización del CMTS (en miniintervalos de tiempo) para las asignaciones dentro de este diagrama.

Tiempo de acuse de recibo: Último tiempo, a partir de la inicialización del CMTS, (miniintervalos de tiempo) procesado en sentido ascendente. Este tiempo es utilizado por los CM a efectos de detección de colisiones. Véase B.9.4.

Comienzo de retroceso de alineación: Ventana de retroceso inicial para contienda de alineación inicial, expresada como una potencia de 2. Gama de valores: 0 a 15 (los bits de orden más alto deben estar sin utilizar y fijados a 0).

Final de retroceso de alineación: Ventana de retroceso final para contienda de alineación inicial, expresada como una potencia de 2. Gama de valores: 0 a 15 (los bits de orden más alto deben estar sin utilizar y fijados a 0).

Comienzo de retroceso de datos: Ventana de retroceso inicial para datos y peticiones por contienda, expresada como una potencia de 2. Gama de valores: 0 a 15 (los bits de orden más alto deben estar sin utilizar y fijados a 0).

Final de retroceso de datos: Ventana de retroceso final para datos y peticiones por contienda, expresada como una potencia de 2. Gama de valores: 0 a 15 (los bits de orden más alto deben estar sin utilizar y fijados a 0).

Elementos de información MAP: DEBEN tener el formato que se muestra en la figura B.8-20 y en el cuadro B.8-20. Los valores de los códigos de utilización de intervalo IUC, (*interval usage code)* se definen en el cuadro B.8-20 y se describen con detalle en B.9.1.2.

Se DEBEN de utilizar los bits inferiores (26 – M) del tiempo de comienzo de atribución y del tiempo de acuse de recibo, como los tiempos de comienzo de MAP y de acuse de recibo efectivos, donde M se da en B.8.3.3. La relación entre los contadores de tiempo de comienzo de atribución/acuse de recibo, y el contador de indicación de tiempo, se describe en B.9.4.

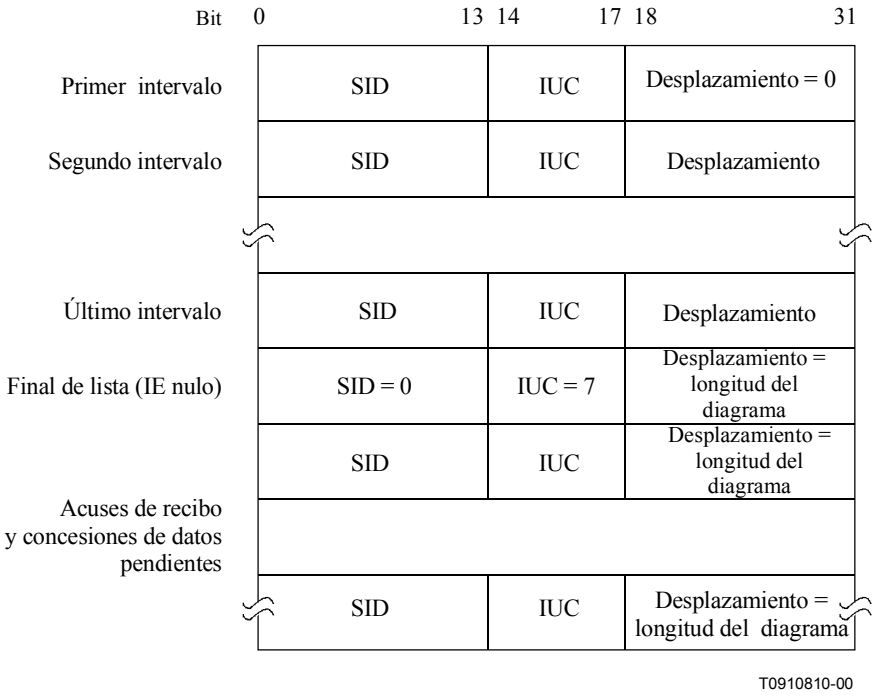


Figura B.8-20/J.112 – Estructura del elemento de información MAP

Cuadro B.8-20/J.112 – Elementos de información (IE) del MAP de atribución

Nombre del IE (Nota 1)	Código de utilización de intervalo (IUC) (4 bits)	SID (14 bits)	Desplazamiento de miniintervalo de tiempo (14 bits)
Petición	1	Cualquiera	Desplazamiento inicial de la región REQ
REQ/datos (véase en el anexo B.A la definición de multidifusión)	2	Multidifusión	Desplazamiento inicial de la región de datos IMMEDIATE. (Multidifusiones bien conocidas definen los intervalos de comienzo)
Mantenimiento inicial	3	Radiodifusión	Desplazamiento inicial de la región MAINT (utilizado en alineación inicial)
Mantenimiento de estación (Nota 2)	4	Unidifusión (Nota 3)	Desplazamiento inicial de la región MAINT (utilizado en alineación periódica)
Concesión de datos corta (Nota 4)	5	Unidifusión	Desplazamiento inicial de la asignación de concesión de datos Si la longitud deducida = 0, se trata de una concesión de datos pendiente
Concesión de datos larga	6	Unidifusión	Desplazamiento inicial de la asignación de concesión de datos Si la longitud deducida = 0, se trata de una concesión de datos pendiente
IE nulo	7	Cero	Desplazamiento final de la concesión previa. Se utiliza para limitar la longitud de la última atribución de intervalo efectiva
Acuse de recibo de datos	8	Unidifusión	CMTS lo fija a la longitud del mapa
Reservado	9-14	Cualquiera	Reservado
Ampliación	15	IUC ampliado	Número de palabras de 32 bits adicionales en este IE

NOTA 1 – Cada IE tiene 32 bits de los cuales los 14 bits más significativos representan el SID, los 4 bits del medio el IUC y los 14 bits de menor peso el desplazamiento de miniintervalo.

NOTA 2 – Aunque la distinción entre mantenimiento inicial y mantenimiento de estación es inequívoca a partir del tipo de ID de servicio, se utilizan códigos distintos para facilitar la configuración de la capa física (véanse en el cuadro B.8-19 las codificaciones de los descriptores de ráfagas).

NOTA 3 – El SID utilizado en el IE mantenimiento de estación DEBE ser un SID temporal, o el primer SID de registro (y quizás el único) que se asignó en el mensaje REG-RSP a un CM.

NOTA 4 – La distinción entre concesiones de datos largas y cortas está relacionada con la cantidad de datos que pueden transmitirse en la concesión. Un intervalo de concesión de datos corta PUEDE utilizar parámetros FEC que son apropiados para paquetes cortos mientras que una concesión de datos larga puede aprovechar las ventajas de una mayor eficacia en la codificación FEC.

B.8.3.5 Petición de alineación (RNG-REQ)

Un mensaje petición de alineación DEBE ser transmitido por un CM en la inicialización y periódicamente a petición del CMTS para determinar el retardo de red y solicitar el ajuste de potencia. Este mensaje DEBE utilizar un campo FC_TYPE = encabezamiento específico MAC y FC_PARM = encabezamiento MAC de temporización, al que DEBE seguir una PDU paquetes con el formato que se muestra en la figura B.8-21.

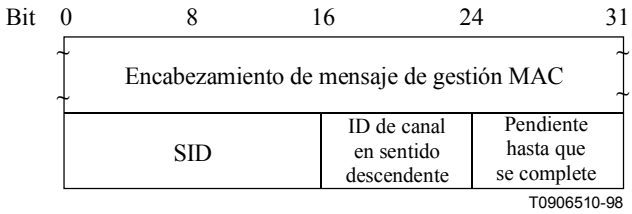


Figura B.8-21/J.112 – PDU paquetes que sigue al encabezamiento de temporización

Los parámetros DEBEN ser como sigue:

SID: Para mensajes RNG-REQ transmitidos en intervalos de mantenimiento inicial:

- SID de inicialización si el módem está tratando de incorporarse a la red.
- SID de inicialización si el módem no se ha registrado todavía y está cambiando los canales en sentido descendente (o tanto los canales en sentido descendente como ascendente) según lo indicado por un fichero de parámetros telecargado.
- SID temporal si el módem no se ha registrado todavía y está cambiando los canales en sentido ascendente (no los canales en sentido descendente) según lo indicado por un fichero de parámetros telecargado.
- SID de registro (asignado previamente en REG-RSP) si el módem se ha registrado y está cambiando los canales en sentido ascendente.

Para mensajes RNG-REQ transmitidos en intervalos de mantenimiento de estación:

- SID asignado.

Es un campo de 16 bits cuyos 14 bits más bajos definen el SID y cuyos bits 14 y 15 han de ser 0.

ID de canal en sentido ascendente: Identificador del canal en sentido descendente por el que el CM ha recibido el UCD que describe este sentido ascendente. Es un campo de 8 bits.

Pendiente hasta que se complete: Si es cero, se han aplicado todos los atributos de respuesta de alineación previos antes de transmitir esta petición. Si no es cero, se trata del tiempo estimado como necesario para completar la asimilación de los parámetros de alineación. Se señala que sólo se puede diferir la ecualización. Las unidades son centésimas de segundo (10 ms) sin signo.

B.8.3.6 Respuesta de alineación (RNG-RSP)

Un mensaje respuesta de alineación DEBE ser transmitido por un CMTS en respuesta al mensaje RNG-REQ recibido. Las máquinas de estados que describen el procedimiento de alineación se indican en B.11.2.4. En ese procedimiento cabe señalar, desde el punto de vista del CM, que la recepción de un mensaje respuesta de alineación carece de estado. En concreto, el CM DEBE estar preparado para recibir un mensaje de alineación en cualquier momento, no sólo tras un mensaje petición de alineación.

Para facilitar la flexibilidad, los parámetros del mensaje que siguen al ID de canal en sentido ascendente DEBEN ser codificados en una forma de tipo/longitud/valor (TLV). (Véase la figura B.8-22.)

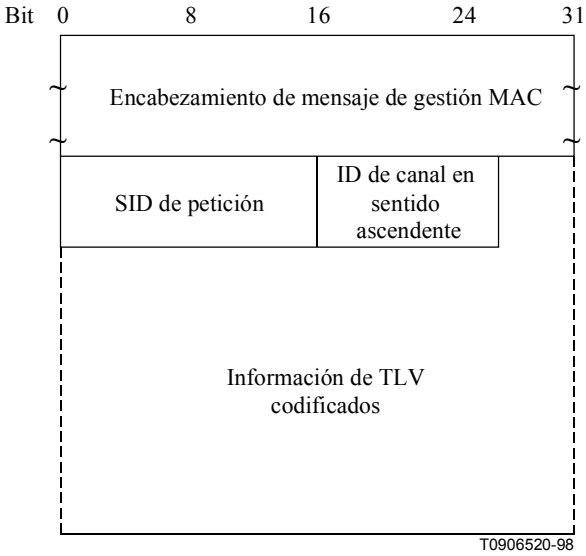


Figura B.8-22/J.112 – Respuesta de alineación

Un CMTS DEBE generar respuestas de alineación con el formato que se muestra en la figura B.8-22, incluyendo todos los parámetros que se indican a continuación:

SID: Si esta respuesta indica al módem que se desplace a un canal diferente, se trata del SID de inicialización. De no ser así, éste es el SID del mensaje RNG-REQ correspondiente al que se refiere esta respuesta, salvo si el RNG-REQ correspondiente fue una petición de alineación inicial especificando un SID de inicialización, en cuyo caso éste es el SID temporal asignado.

ID de canal en sentido ascendente: Identificador del canal en sentido ascendente por el que el CMTS ha recibido el mensaje RNG-REQ al que se refiere esta respuesta. Con la primera respuesta de alineación recibida por el CM durante la alineación inicial, el ID de canal puede ser diferente del ID del canal utilizado por el CM para transmitir la petición de alineación (véase el anexo B.H). Por eso el CM DEBE utilizar este ID de canal para el resto de sus transacciones, no el ID del canal con el que se inició la petición de alineación.

Todos los demás parámetros se codifican como tuplas TLV.

Situación de la alineación: Se utiliza para indicar si se reciben mensajes en sentido ascendente dentro de unos límites aceptables por el CMTS.

Información de ajuste de temporización: Tiempo en que se debe desplazar la transmisión de tramas de tal manera que las tramas lleguen al CMTS en el momento de los miniintervalos de tiempo previsto.

Información de ajuste de potencia: Especifica el cambio relativo del nivel de potencia de la transmisión que debe efectuar el CM para que las transmisiones lleguen al CMTS con la potencia deseada.

Información de ajuste de frecuencia: Especifica el cambio relativo de la frecuencia de transmisión que el CM debe efectuar para una mayor concordancia con el CMTS. (Se trata de un ajuste fino de frecuencia dentro de un canal, no una reasignación a un canal diferente.)

Información de ecualización de transmisor CM: Esta información proporciona los coeficientes de ecualización para el ecualizador previo.

Invalidación de frecuencia en sentido descendente: Parámetro opcional. La frecuencia con la que el módem debería rehacer la alineación inicial (véase B.8.3.6.3).

Invalidación de ID de canal en sentido ascendente: Parámetro opcional. El identificador del canal en sentido ascendente con el que el módem debería rehacer la alineación inicial (véase B.8.3.6.3).

B.8.3.6.1 Codificaciones

Los valores de tipo utilizados DEBEN ser los que se definen en el cuadro B.8-21 y en la figura B.8-23. Son valores únicos en el mensaje respuesta de alineación pero no en todo el conjunto de mensajes MAC. Los campos de tipo y longitud DEBEN tener una longitud de 1 octeto cada uno.

Cuadro B.8-21/J.112 – Codificaciones de mensajes de respuesta de alineación

Nombre	Tipo (1 octeto)	Longitud (1 octeto)	Valor (Longitud variable)
Ajuste de la temporización	1	4	Ajuste del desplazamiento de la temporización de transmisión (32 bits con signo, en unidades de 6,25 µs/64)
Ajuste del nivel de potencia	2	1	Ajuste del desplazamiento de la potencia de transmisión (8 bits con signo, en unidades de 1/4 dB)
Ajuste de la frecuencia de desplazamiento	3	2	Ajuste del desplazamiento de la frecuencia de transmisión (16 bits con signo, en unidades de Hz)
Ajuste de la ecualización de transmisión	4	n	Datos de ecualización de la transmisión (véanse los detalles más abajo)
Situación de la alineación	5	1	1 = continuación, 2 = aborto, 3 = éxito
Invalidación de frecuencia en sentido descendente	6	4	Frecuencia central del nuevo canal en sentido descendente en unidades de Hz
Invalidación de ID de canal en sentido ascendente	7	1	Identificador del nuevo canal en sentido ascendente
Reservado	8-255	n	Reservado para utilización futura

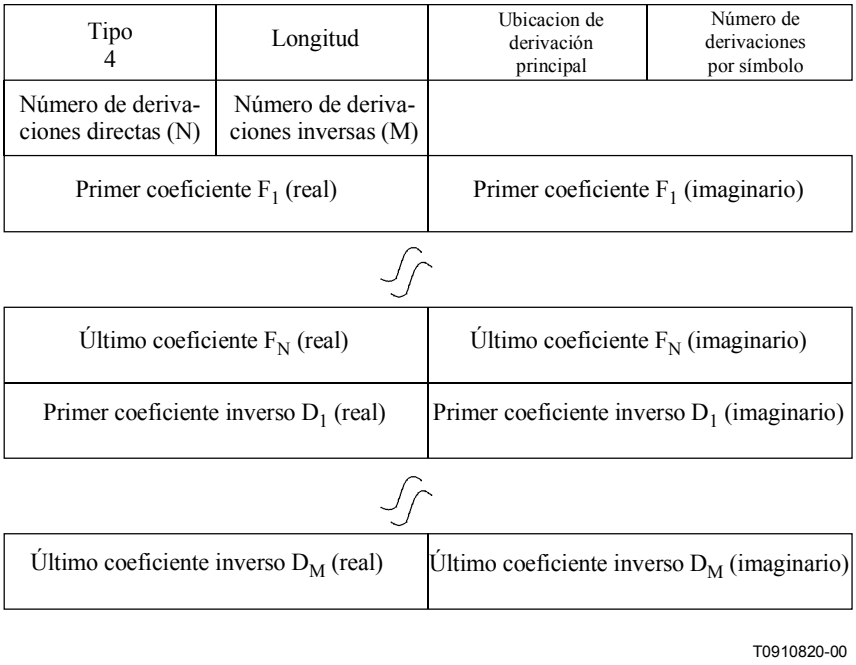


Figura B.8-23/J.112 – Coeficientes de ecualización de realimentación de decisión generalizada

El número de derivaciones de reenvío por símbolo DEBE ser 1, 2 ó 4. La ubicación de la derivación principal está referida a la derivación con retardo cero, entre 1 y N. Para un ecualizador con símbolos separados, el número de derivaciones de reenvío por campo de símbolo DEBE fijarse a "1". El número del campo (M) de derivaciones inversas debe fijarse a "0" para un ecualizador lineal. El número total de derivaciones PUEDE alinearse hasta 64. Cada derivación consta de una entrada en el cuadro de coeficiente real y coeficiente imaginario.

Si se necesitan más de 255 octetos para representar la información de ecualización, se PUEDEN utilizar elementos de tipo 4. Los datos DEBEN ser tratados como si fuesen octetos concatenados, es decir, el primer octeto después del campo de longitud del segundo elemento de tipo 4 se tratan como si siguiera inmediatamente al último octeto del primer elemento del tipo 4. (Véase la figura B.8-24.)

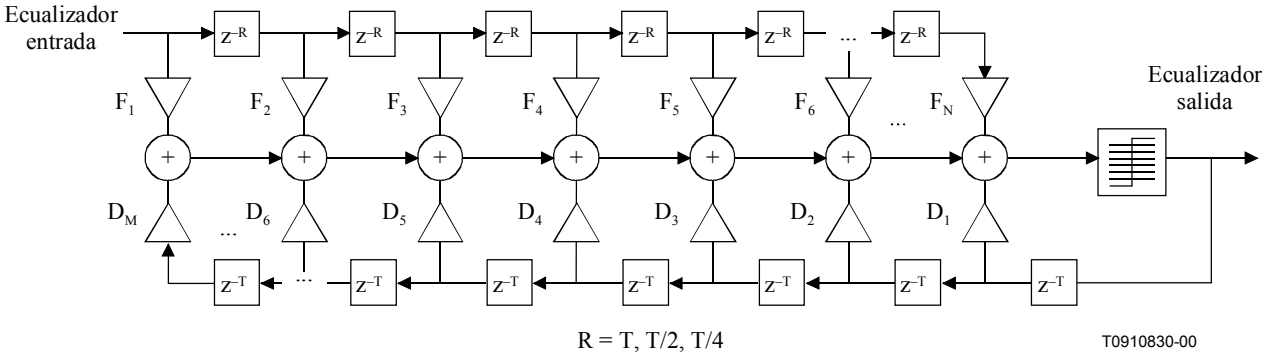


Figura B.8-24/J.112 – Definición de la ubicación de las derivaciones del ecualizador generalizado

B.8.3.6.2 Ejemplo de datos de TLV

En la figura B.8-25 se da un ejemplo de datos de TLV.

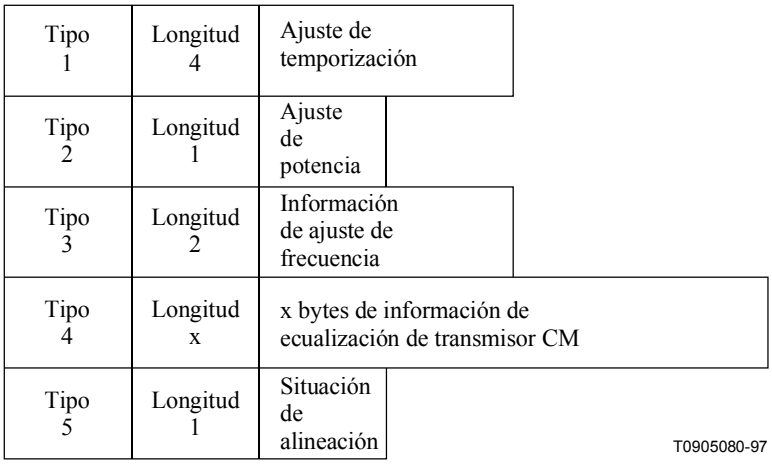


Figura B.8-25/J.112 – Ejemplo de datos de TLV

B.8.3.6.3 Invalidación de canales durante la alineación inicial

El mensaje RNG-RSP permite al CMTS indicar al módem que se desplace a un nuevo canal en sentido descendente y/o ascendente y que repita la alineación inicial. Sin embargo, el CMTS sólo puede hacer esto en respuesta a una petición de alineación inicial procedente de un módem que está tratando de incorporarse a la red, o en respuesta a cualquiera de las peticiones de alineación de unidifusión que se producen inmediatamente después de esta alineación inicial y hasta el momento en que el módem completa de manera satisfactoria la alineación periódica. Si en el mensaje RNG-RSP se especifica una invalidación de frecuencia en sentido descendente, el módem DEBE reinicializar su MAC (véase B.11.2) utilizando la alineación inicial con la frecuencia central en sentido descendente especificada como primer canal explorado. Para el canal en sentido ascendente, el módem puede seleccionar cualquier canal válido en base a los mensajes UCD recibidos.

Si en el mensaje RNG-RSP se especifica una invalidación de ID de canal en sentido ascendente, el módem DEBE reinicializar su MAC (véase B.11.2) utilizando la alineación inicial del canal del sentido ascendente especificado en el mensaje RNG-RSP y la misma frecuencia en sentido descendente en que se recibió dicho mensaje para su primer intento.

Si en el mensaje RNG-RSP están presentes tanto la invalidación de frecuencia en sentido descendente como la de ID de canal en sentido ascendente, el módem DEBE reinicializar su MAC (véase B.11.2) utilizando la alineación inicial con la frecuencia en sentido descendente y el ID de canal en sentido ascendente especificados para su primer intento.

Se señala que cuando un módem con un SID temporal asignado recibe la instrucción de que se desplace a un canal nuevo en sentido descendente y/o en sentido ascendente, el módem DEBE considerar que el SID temporal ha de ser revocado. El módem DEBE rehacer la alineación inicial utilizando el SID de inicialización.

Las fijaciones del fichero de configuración para ID de canal en sentido ascendente y frecuencia en sentido descendente son opcionales, pero si se especifican en el fichero de configuración, tienen precedencia respecto a los parámetros de respuesta de alineación. Cuando la alineación se concluye sólo están disponibles los mecanismos B.C.1.1.2, UCC-REQ y DCC-REQ para desplazar el módem a un nuevo canal en sentido ascendente, y sólo están disponibles el mecanismo B.C.1.1.1 y el mensaje DCC-REQ para desplazar el módem a un nuevo canal en sentido descendente.

B.8.3.7 Petición de registro (REG-REQ)

Un mensaje petición de registro, DEBE ser transmitido por un CM en la inicialización después de recibir un fichero de parámetros del CM.

Para facilitar la flexibilidad, los parámetros del mensaje que siguen al SID DEBEN ser codificados en forma de tipo/longitud/valor (TLV). (Véase la figura B.8-26.)

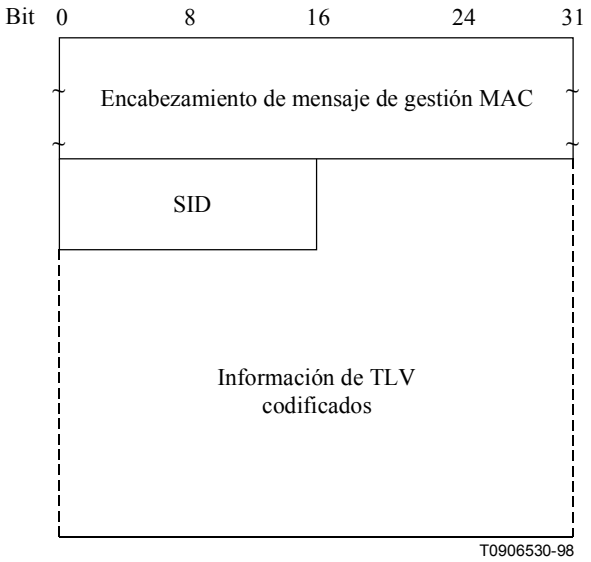


Figura B.8-26/J.112 – Petición de registro

Un CM DEBE generar peticiones de registro con el formato mostrado en la figura B.8-26, incluyendo los parámetros siguientes:

SID: SID temporal para este CM.

El resto de los parámetros se modifican como tuplas TLV tal como se define en el anexo B.C.

Las peticiones de registro pueden contener una diversidad de diferentes parámetros TLV, algunos de los cuales son fijados por el CM de acuerdo a su fichero de configuración y otros son generados por el mismo CM. Si se encuentran en el fichero de configuración, se DEBEN incluir en la petición de registro las siguientes fijaciones de configuración.

Fijaciones de fichero de configuración:

- fijación de configuración frecuencia en sentido descendente;
- fijación de configuración ID de canal en sentido ascendente;
- objeto de control de acceso a la red;
- fijación de configuración clasificación de paquetes en sentido ascendente;
- fijación de configuración clasificación de paquetes en sentido descendente;
- fijación de configuración clase de servicio;
- fijación de configuración flujo de servicio en sentido ascendente;
- fijación de configuración flujo de servicio en sentido descendente;
- fijación de configuración privacidad básica.
- número máximo de CPE;
- número máximo de clasificadores;
- fijación de configuración habilitación de privacía;

- supresión de encabezamiento de cabida útil;
- indicación de tiempo de servidor TFTP;
- dirección de módem suministrada por el servidor TFTP;
- fijación de configuración información específica del vendedor;
- fijación de configuración MIC de CM;
- fijación de configuración MIC de CMTS;

NOTA 1 – El CM DEBE reenviar las fijaciones de configuración específicas del vendedor al CMTS en el mismo orden en que se recibieron en el fichero de la configuración, para que se pueda llevar a cabo la verificación de la integridad de los mensajes.

En la petición de registro DEBE incluirse el siguiente parámetro de registro:

Parámetro específico de vendedor:

- Fijación de configuración ID de vendedor (ID de vendedor de CM).

En la petición de registro DEBE incluirse también el siguiente parámetro de registro.

- Codificaciones de las capacidades del módem.

NOTA 2 – El CM DEBE especificar todas las capacidades del módem en su petición de registro. El CMTS NO DEBE asumir ninguna capacidad del módem que esté definida pero no explícitamente indicada en la petición de registro del CM.

En la petición de registro PUEDE incluirse también el siguiente parámetro de registro.

- Dirección IP del módem.

Las siguientes fijaciones de configuración NO DEBEN ser reenviadas al CMTS en la petición de registro.

- nombre de fichero de la versión mejorada del soporte lógico;
- dirección IP en el servidor TFTP de la versión mejorada del soporte lógico;
- control de acceso a la escritura del SNMP;
- objeto MIB del SNMP;
- dirección MAC Ethernet del CPE;
- compendio HMAC;
- fijación de configuración de extremo;
- fijación de configuración de relleno;
- opción de las fijaciones telefónicas.

B.8.3.8 Respuesta de registro (REG-RSP)

Un mensaje respuesta de registro, DEBE ser transmitido por un CMTS en respuesta al mensaje REG-REQ recibido.

Para facilitar la flexibilidad, los parámetros del mensaje que siguen al campo de respuesta DEBEN codificarse con un formato TLV. (Véase la figura B.8-27.)

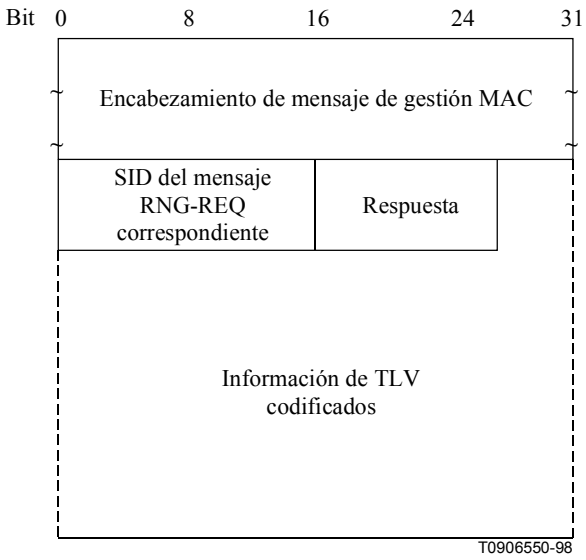


Figura B.8-27/J.112 – Formato de respuesta de registro

Un CMTS DEBE generar respuestas de registro con el formato mostrado en la figura B.8-27 incluyendo los dos parámetros que se indican a continuación:

SID del REG-REQ correspondiente SID del mensaje REG-REQ correspondiente al que se refiere esta REG respuesta. (Actúa como un identificador de transacción.)

Respuesta Mensaje REG-RSP hacia un módem que se registra como módem 1.0 (es decir, el mensaje REG-REQ contiene codificaciones de clase de servicio de DOCSSIS 1.0)

0 = correcto

1 = fallo de autenticación

2 = fallo de clase de servicio

Mensaje REG-RSP hacia un módem que se registra como módem 1.1 (es decir, el mensaje REG-REQ contiene codificaciones de flujo de servicio). Este campo DEBE contener uno de los códigos de confirmación mencionados en B.C.4 y en B.C.4.1.

NOTA 1 – Los fallos aplican a la petición de registro completa. Incluso si solamente una petición única de flujo de servicio o una clase de servicio de DOCSIS 1.0 no es válida o no es entregable, todo el registro se considera fallido.

Si el mensaje REG-REQ tiene éxito, y contiene parámetros de flujo de servicio, parámetros de clasificador, o parámetros de supresión de encabezamiento de cabida útil, el mensaje REG-RSP DEBE contener, para cada uno de estos:

Parámetros de clasificador Todos los parámetros de clasificador del mensaje correspondiente REG-REQ, más el identificador de clasificador asignado por el CMTS.

Parámetros de flujo de servicio	Todos los parámetros de flujo de servicio del mensaje REG-REQ, más el ID de flujo de servicio asignado por el CMTS. Todo flujo de servicio que contenga un nombre de clase de servicio que haya sido admitido/activado (véase la Nota 2), DEBE ser ampliado al conjunto completo de parámetros TLV que definen el flujo de servicio. Todo flujo de servicio en sentido ascendente que haya sido admitido/activado DEBE tener un identificador de servicio asignado por el CMTS. Un flujo de servicio que sólo haya sido aprovisionado incluirá solamente parámetros QoS que aparecen en el mensaje REG-REQ, más el ID del flujo de servicio asignado.
Parámetros de encabezamientos de cabida útil	Todos los parámetros de supresión del encabezamiento de cabida útil del mensaje REG-REQ, más el índice de supresión de encabezamiento de cabida útil asignados por el CMTS.

NOTA 2 – Los parámetros ActiveQosParamSet (conjunto de parámetros QoS activos) o AdmittedQosParamSet (conjunto de parámetros QoS admitidos) no son nulos.

Si el mensaje REG-REQ falla, y contiene parámetros de flujo de servicio, parámetros de clasificador, o parámetros de supresión de encabezamiento de cabida útil, y la respuesta no es alguno de los principales códigos de error de B.C.4.1, el mensaje REG-RSP DEBE contener al menos uno de los parámetros siguientes:

Conjunto de errores de clasificador	Se DEBE incluir un conjunto de errores de clasificador, una referencia de identificación de clasificador y una referencia de flujo de servicio al menos para un clasificador fallido en el mensaje REG-REQ correspondiente. Todo conjunto de errores de clasificador DEBE incluir al menos un parámetro de clasificador fallido específico del clasificador correspondiente.
Conjunto de errores de flujo de servicio	Se DEBE incluir un conjunto de errores de flujo de servicio y una referencia de identificación de flujo de servicio al menos por cada flujo de servicio fallido en el mensaje REG-REQ correspondiente. Todo conjunto de errores de flujo de servicio DEBE incluir al menos un parámetro QoS fallido específico del flujo de servicio correspondiente.
Conjunto de errores de supresión del encabezamiento de cabida útil	Se DEBE incluir un conjunto de errores tipo PHS, una referencia de identificación de flujo de servicio y un par de referencias de clasificador al menos para una regla PHS fallida en el mensaje REG-REQ correspondiente. Todo conjunto de errores tipo PHS DEBE incluir al menos un parámetro PHS fallido específico de la regla PHS fallida correspondiente.

La ampliación del nombre de clase de servicio ocurre siempre en el momento de la admisión. Por eso, si una petición de registro contiene una referencia de flujo de servicio y un nombre de clase de servicio para admisión/activación aplazada, la respuesta al registro NO DEBE incluir ningún parámetro QoS adicional excepto el identificador de flujo de servicio. (Véase B.10.1.3.)

Si la petición de registro correspondiente contiene parámetros TLV de clase de servicio de DOCSIS 1.0 (véase B.C.1.1.4), la respuesta de registro DEBE contener las siguientes tuplas TLV:

Datos de clase de servicio de DOCSIS 1.0	Devuelto cuando respuesta = correcto. Tupla ID de servicio/clase de servicio para cada clase de servicio concedida. Los ID de clase de servicio DEBEN ser los solicitados en el mensaje REG-REQ correspondiente.
Servicio no disponible	Devuelto cuando respuesta = fallo de clase de servicio. Si no se puede soportar una clase de servicio, se devuelve esta fijación de configuración en lugar de los datos de la clase de servicio.

El resto de los parámetros se codifican como tuplas TLV.

Capacidades del módem	La respuesta del CMTS a las capacidades del módem (si están presentes en la petición de registro).
Datos específicos del vendedor	Como se definen en el anexo B.C. – Fijación de la configuración ID del vendedor (ID del vendedor del CMTS) – Extensiones específicas del vendedor.

B.8.3.8.1 Codificaciones

Los valores de tipo utilizados DEBEN ser los que se muestran más adelante. Son valores únicos dentro del mensaje respuesta de registro, pero no en todo el conjunto de mensajes MAC. Los campos tipo y longitud DEBEN ser cada uno de 1 octeto.

B.8.3.8.1.1 Capacidades del módem

Este campo define la respuesta del CMTS al campo capacidades del módem en el mensaje petición de registro. El CMTS DEBE responder a cada una de las capacidades del módem para indicar si pueden ser utilizadas. Si el CMTS no reconoce una capacidad de módem, DEBE devolver el TLV con valor 0 ("inactiva") en el mensaje respuesta de registro.

Sólo las capacidades fijadas a "activada" en el mensaje REG-REQ pueden fijarse a "activa" en el REG-RSP ya que ésta es la toma de contacto que indica que se han negociado de manera satisfactoria. Las capacidades fijadas a "inactiva" en el mensaje REG-REQ también deben fijarse a "inactivas" en el mensaje REG-RSP.

Las codificaciones son como las definidas para el mensaje petición de registro.

B.8.3.8.1.2 Datos de clase de servicio de DOCSIS 1.0

En la respuesta de registro DEBE estar presente un parámetro de datos de clase de servicio de DOCSIS 1.0 por cada parámetro de clase de servicio de DOCSIS 1.0 (véase B.C.1.1.4) en la petición de registro.

Esta codificación define los parámetros asociados con una clase de servicio pedida. Es algo compleja en el sentido de que se compone de varios campos encapsulados de tipo/longitud/valor. Los campos encapsulados definen los parámetros de clase de servicio particulares para la clase de servicio en cuestión. Se señala los campos tipo definidos sólo son válidos dentro de la cadena encapsulada de fijaciones de configuración de datos de la clase de servicio. La fijación única de la configuración de datos de clase de servicio DEBE ser utilizada para definir los parámetros para una sola clase de servicio. Las definiciones de clases múltiples DEBEN utilizar conjuntos múltiples de fijación de la configuración de datos de clase de servicio.

Cada parámetro recibido de clase de servicio de DOCSIS 1.0 debe tener un ID de clase única en el rango 1 a 16. Si en el mensaje REG-REQ no está presente el ID de clase para ningún TLV de clase de servicio de DOCSIS 1.0, el CMTS DEBE enviar un mensaje REG-RSP con una respuesta de fallo de la clase de servicio y sin TLVs de clase de servicio de DOCSIS 1.0.

Tipo	Longitud	Valor
1	n	Datos codificados de clase de servicio

ID de clase

El valor de este campo DEBE especificar el identificador para la clase de servicio a la que se aplica la cadena encapsulada. Ésta DEBE ser de una clase solicitada en el mensaje REG-REQ asociado, si está presente.

Tipo	Longitud	Valor
1.1	1	Del mensaje REG-REQ

Gama válida

El ID de clase DEBE estar en la gama de 1 a 16.

ID de servicio

El valor de este campo DEBE especificar el SID asociado con esta clase de servicio.

Tipo	Longitud	Valor
1.2	2	SID

B.8.3.9 Acuse de recibo de registro (REG-ACK)

El CM DEBE transmitir un acuse de recibo de registro en respuesta a un mensaje REG-RSP procedente del CMTS. Confirma la aceptación en el CM de los parámetros QoS del flujo reportado por el CMTS en el mensaje REG-RSP. El formato de un mensaje REG-ACK DEBE ser como se muestra en la figura B.8-28.

NOTA – El acuse de recibo del registro es un mensaje DOCSIS 1.1. Véanse en el anexo B.G detalles sobre cuestiones relativas a la interoperabilidad del registro.

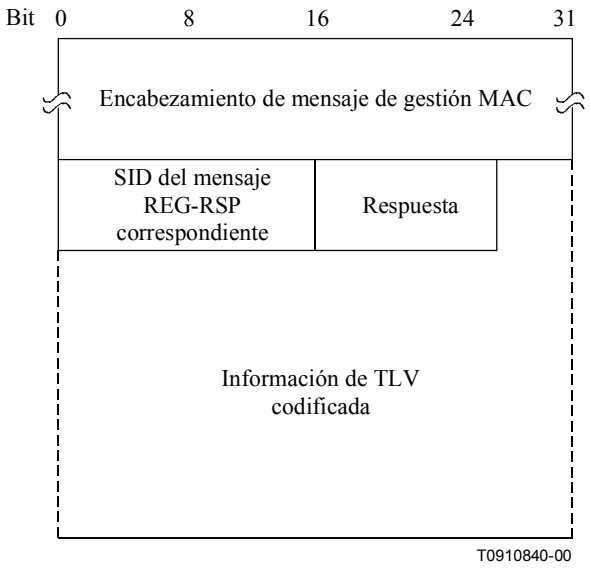


Figura B.8-28/J.112 – Acuse de recibo de registro

Los parámetros DEBEN ser como sigue:

SID del mensaje REG-RSP correspondiente SID del mensaje REG-RSP correspondiente al que se refiere este acuse de recibo. (Actúa como un identificador de transacción.)

Código de confirmación Código de confirmación apropiado (véase B.C.4) para la respuesta de registro completa correspondiente.

Se requiere que el CM transmita al CMTS en el mensaje REG-REQ (véase B.8.3.7), todos los clasificadores, flujos de servicio y reglas de supresión de encabezamiento de cabida útil aprovisionados. El CMTS los retornará con identificadores y nombres de clase de servicio ampliados, si están presentes, en el mensaje REG-RSP (véase B.8.3.8). Puesto que el CM quizás no pueda soportar uno o más de estos elementos aprovisionados, el mensaje REG-ACK incluye conjuntos de errores para todos los fallos relacionadas con el aprovisionamiento de estos elementos.

Si hubiera algunos fallos de elementos aprovisionados, el mensaje REG-ACK DEBE incluir los conjuntos de errores correspondientes a esos fallos. Se proporciona la identificación del conjunto de errores utilizando el ID de flujo de servicio y el ID de clasificador en el mensaje REG-RSP correspondiente. Si se omitió el ID de clasificador o SFID en el mensaje REG-RSP, el CM DEBE utilizar la referencia apropiada (referencia de clasificador, referencia de SF) en el mensaje REG-ACK.

Conjunto de errores de clasificador Se DEBEN incluir un conjunto de errores de clasificador y el par referencia/identificador de identificación de clasificador y referencia/identificador de flujo de servicio al menos para un clasificador fallido en el mensaje correspondiente REG-RSP. Todo conjunto de errores de clasificador DEBE incluir al menos un parámetro clasificador fallido específico del clasificador correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo REG-REQ/RSP.

Conjunto de errores de flujo de servicio Un conjunto de errores del flujo de servicio del mensaje REG-ACK codifica los datos específicos de los flujos de servicio fallidos en el mensaje REG-RSP. Se DEBEN incluir un conjunto de errores de flujo de servicio y una

referencia/identificador de identificación del flujo de servicio al menos para un parámetro QoS fallido de al menos un flujo de servicio fallido en el mensaje REG-RSP correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo REG-REQ/RSP.

Conjunto de errores de supresión de encabezamiento de cabida útil Se DEBEN incluir un conjunto de errores tipo PHS y un par referencia/identificador de identificación de flujo de servicio y referencia/identificador de clasificador al menos para una regla PHS fallida en el mensaje REG-RSP correspondiente. Todo conjunto de errores tipo PHS DEBE incluir al menos un PHS fallido específico de la regla PHS fallida. Este parámetro DEBE omitirse si tiene éxito el mensaje completo REG-REQ/RSP.

El acuse de recibo del flujo de servicio es necesario no solamente para la sincronización entre el CM y el CMTS, sino también para dar soporte a la utilización del nombre de clase de servicio. (Véase B.10.1.3.) Ya que el CM podría no conocer todos los parámetros de flujo de servicio asociados con un nombre de clase de servicio cuando se establece la petición de registro, puede ser necesario que el CM tenga que enviar un mensaje NAK tras una respuesta de registro si es que no cuenta con recursos suficientes para soportar este flujo de servicio.

B.8.3.10 Petición de cambio de canal en sentido ascendente (UCC-REQ)

Una petición de cambio de canal en sentido ascendente PUEDE ser transmitida por un CMTS para hacer que un CM cambie de canal en sentido ascendente por el que está transmitiendo. En la figura B.8-29 se muestra el formato de un mensaje UCC-REQ.

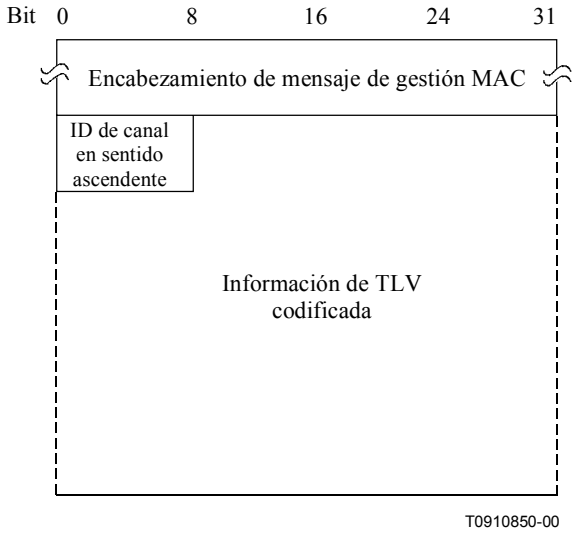


Figura B.8-29/J.112 – Petición de cambio de canal en sentido ascendente

Los parámetros DEBEN ser como sigue:

ID de canal en sentido ascendente Identificador del canal en sentido ascendente al que debe conmutar el CM para transmisiones en sentido ascendente. Es un campo de 8 bits.

El resto de los parámetros se codifican como tuplas TLV.

Técnica de alineación Direcciones para el tipo de alineación que el CM debe ejecutar una vez que se sincroniza con el nuevo canal en sentido ascendente.

B.8.3.10.1 Codificaciones

Los valores de tipo utilizados DEBEN ser los que se muestran más adelante. Son valores únicos dentro del mensaje de petición de cambio de canal en sentido ascendente, pero no en todo el conjunto de mensajes MAC. Los campos tipo y longitud DEBEN ser cada uno de 1 octeto.

B.8.3.10.1.1 Técnica de alineación

EL CMTS PUEDE incluir el parámetro TLV de la técnica de alineación en un mensaje UCC-REQ para indicar qué nivel de alineación debe ejecutar, si es que se requiere alguno. El CMTS puede tomar la decisión en base a su conocimiento de las diferencias entre los canales nuevos y antiguos en sentido ascendente.

Por ejemplo, algunas áreas del espectro en sentido ascendente a menudo se configuran en grupos. Un mensaje UCC-REQ hacia un canal adyacente dentro de un grupo podría no garantizar el realineamiento. Alternativamente, un mensaje UCC-REQ hacia un canal no adyacente podría requerir mantenimiento de estación mientras que un mensaje UCC-REQ desde uno hacia otro grupo de canales podría requerir mantenimiento inicial.

Tipo	Longitud	Valor
1	1	0 = Ejecutar mantenimiento inicial en el nuevo canal. 1 = Ejecutar sólo mantenimiento de estación en el nuevo canal. 2 = Ejecutar mantenimiento inicial o bien mantenimiento de estación en el nuevo canal (véase la Nota). 3 = Utilizar el nuevo canal directamente sin ejecutar mantenimiento inicial o de estación.

NOTA – Este valor autoriza a un CM a utilizar una región de mantenimiento inicial o de mantenimiento de estación, cualquiera que sea el que seleccione el CM. Este valor podría ser utilizado si hay incertidumbre respecto a cuándo el CM PUEDE ejecutar el UCC y por ello existe la posibilidad de que se omitan intervalos de tiempo de mantenimiento de estación.

Si este parámetro TLV está ausente, el CM DEBE ejecutar alineación con el mantenimiento inicial. Para la compatibilidad hacia atrás, el CMTS DEBE aceptar un CM que ignora esta tupla y ejecute el mantenimiento inicial.

Esta opción no debería ser utilizada en plantas físicas en donde las características de transmisión en sentido ascendente no sean coherentes.

B.8.3.11 Respuesta de cambio de canal en sentido ascendente (UCC-RSP)

Una respuesta de cambio de canal en sentido ascendente DEBE ser transmitida por un CM en respuesta a un mensaje petición de cambio de canal en sentido ascendente recibido para indicar que ha recibido y cumple con el mensaje UCC-REQ. En la figura B.8-30 se muestra el formato de un mensaje UCC-RSP.

Antes de empezar a conmutar a un nuevo canal en sentido ascendente, un CM DEBE transmitir un UCC-RSP por su canal existente en sentido ascendente. Un CM PUEDE ignorar un mensaje UCC-REQ mientras está efectuando un cambio de canal. Cuando un CM recibe un mensaje UCC-REQ pidiendo que cambie a un canal en sentido ascendente que ya está utilizando, el CM DEBE responder con un mensaje UCC-RSP por ese canal indicando que ya está utilizando el canal correcto.

Tras conmutar a un nuevo canal en sentido ascendente, un CM DEBE realinear utilizando la técnica de alineación en el mensaje UCC-REQ correspondiente, y a continuación debe proseguir sin efectuar de nuevo un registro. El procedimiento completo de cambio de canales se describe en B.11.3.3.

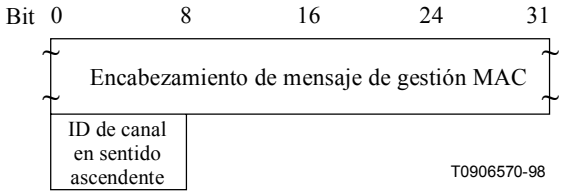


Figura B.8-30/J.112 – Respuesta de canal de cambio en sentido ascendente

Los parámetros DEBEN ser como sigue:

ID de canal en sentido ascendente Identificador del canal en sentido ascendente al que debe conmutar el CM para las transmisiones en sentido ascendente. DEBE ser el mismo ID de canal especificado en el mensaje UCC-REQ. DEBE ser un campo de 8 bits.

B.8.3.12 Petición de adición de servicio dinámica (DSA-REQ)

Un CM o un CMTS PUEDE enviar una petición de adición de servicio dinámica para crear un nuevo flujo de servicio. (Véase la figura B.8-31.)

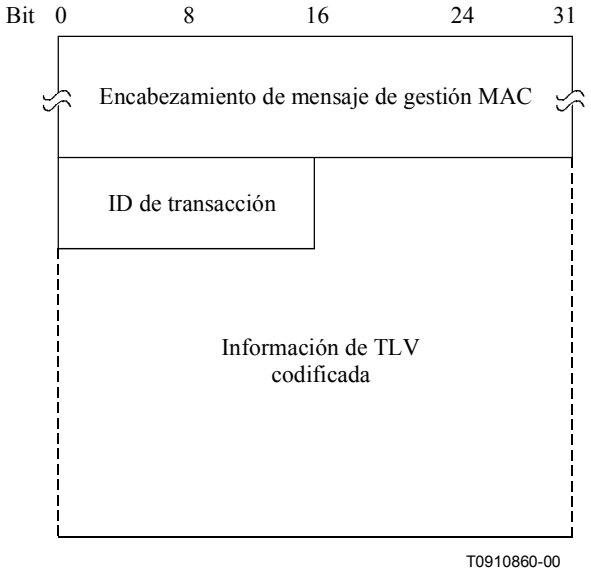


Figura B.8-31/J.112 – Petición de adición de servicio dinámica

Un CM o un CMTS DEBEN generar mensajes DSA-REQ con el formato mostrado en la figura B.8-31 incluyendo el siguiente parámetro:

ID de transacción Identificador único asignado por el emisor para esta transacción

El resto de los parámetros se codifica como las tuplas TLV definidas en el anexo B.C. Un mensaje DSA-REQ NO DEBE contener parámetros para más de un flujo de servicio en cada sentido, es decir, un mensaje DSA-REQ DEBE contener parámetros para un flujo de servicio único en sentido ascendente, o bien para un flujo de servicio único en sentido descendente, o para un flujo de servicio en sentido ascendente y uno en sentido descendente.

El mensaje DSA-REQ DEBE contener:

Parámetros de flujo de servicio Especificación de las características y de tráfico del flujo de servicio y de los requisitos de programación.

El mensaje DSA-REQ PUEDE contener parámetros de clasificador y parámetros de supresión de encabezamiento de cabida útil asociados con los flujos de servicio especificados en el mensaje:

Parámetros de clasificador Especificación de las reglas que se han de utilizar para clasificar paquetes dentro de un flujo de servicio específico.

Parámetros de supresión de encabezamiento de cabida útil Especificación de las reglas de supresión de encabezamiento de cabida útil que se han de utilizar con un clasificador asociado.

Si la privacidad está habilitada, el mensaje DSA-REQ DEBE contener:

Número de secuencia de clave El número de secuencia de clave de la clave Auth que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje del servicio dinámico (véase B.C.1.4.1).

B.8.3.12.1 Adición de servicio dinámica iniciada por el CM

Las peticiones DSA iniciadas por el CM DEBEN utilizar la referencia del flujo de servicio para asociar los clasificadores con los flujos de servicio. Los valores de la referencia del flujo de servicio son específicos del mensaje DSA; a cada flujo de servicio dentro de la petición DSA se le DEBE asignar una referencia única de flujo de servicio. No es preciso que el valor sea único con respecto a los otros flujos de servicio conocidos por el emisor.

La petición DSA iniciada por un CM DEBE utilizar la referencia del clasificador y la referencia del flujo de servicio para asociar los parámetros de supresión de encabezamiento de cabida útil con los clasificadores y flujos de servicio. Una petición DSA debe utilizar la referencia del flujo de servicio para asociar el clasificador con el flujo de servicio. Los valores de referencia del clasificador son específicos del mensaje DSA; a cada clasificador dentro de la petición DSA se le DEBE asignar una referencia única de clasificador.

Las peticiones DSA iniciadas por un CM PUEDEN utilizar el nombre de la clase de servicio (véase B.C.2.2.3.4) en lugar de algunos, o todos, los parámetros QoS.

B.8.3.12.2 Adición de servicio dinámica iniciada por un CMTS

Las peticiones DSA iniciadas por un CMTS DEBEN utilizar el ID del flujo de servicio para asociar los clasificadores con los flujos de servicio. Los indicadores de los flujos de servicio son únicos dentro del dominio MAC. Las peticiones DSA iniciadas por un CMTS para flujos de servicio en sentido ascendente DEBEN incluir también un ID de servicio.

Las peticiones DSA iniciadas por un CMTS que incluyen clasificadores DEBEN asignar un identificador único de clasificador por cada flujo de servicio.

Las peticiones DSA iniciadas por un CMTS para clases de servicio con nombre DEBEN incluir el conjunto de parámetros QoS asociados con esa clase de servicio.

B.8.3.13 Respuesta de adición de servicio dinámica (DSA-RSP)

Se DEBE generar una respuesta a la petición de adición al servicio dinámica tras la recepción de una petición DSA. El formato de un mensaje DSA-RSP DEBE ser como se muestra en la figura B.8-32.

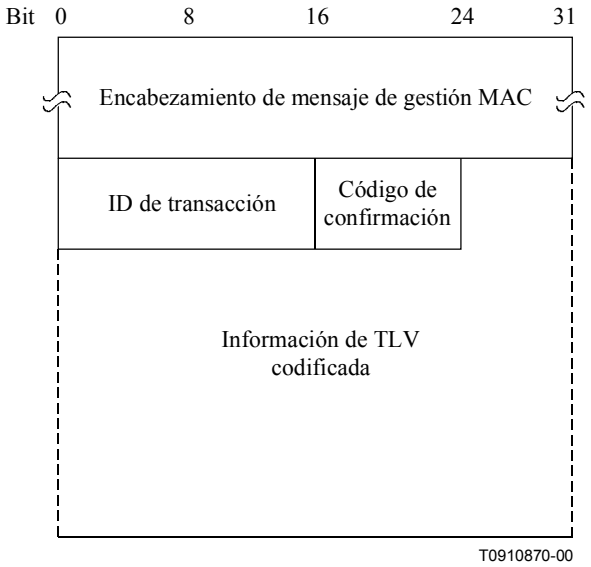


Figura B.8-32/J.112 – Respuesta de adición de servicio dinámica

Los parámetros DEBEN ser como sigue:

ID de transacción — ID de la transacción del mensaje DSA-REQ correspondiente.

Código de confirmación — El código de confirmación apropiado (véase B.C.4) para el mensaje de petición DSA completo correspondiente.

Los demás parámetros se codifican como los tuplas TLV definidas en el anexo B.C.

Si la transacción tiene éxito, el mensaje DSA-RSP PUEDE contener uno o más de los siguientes parámetros:

Parámetros de clasificador — Se DEBE incluir la especificación completa del clasificador en el mensaje DSA-RSP sólo si incluye un identificador de clasificador recién asignado. Si un clasificador pedido contiene una referencia de clasificador, el mensaje DSA-RSP DEBE contener un identificador de clasificador.

Parámetros de flujo de servicio — Se DEBE incluir la especificación completa del flujo de servicio en el mensaje DSA-RSP sólo si incluye un identificador de flujo de servicio recién asignado o si incluye un nombre ampliado de clase de servicio.

Parámetros de supresión de encabezamiento de cabida útil — Se DEBE incluir la especificación completa de los parámetros PHS en el mensaje DSA-RSP sólo si incluye un índice PHS recién asignado. Si está incluido, los parámetros PHS DEBEN contener un identificador de clasificador y un identificador de flujo de servicio.

Si la transacción no tiene éxito, y el código de confirmación no es uno de los códigos de error importante de B.C.4.2, el mensaje DSA-RSP DEBE contener al menos uno de los siguientes conjuntos de errores:

Conjunto de errores de flujo de servicio — Se DEBEN incluir un conjunto de errores de flujo de servicio y una referencia/identificador de identificación del flujo de servicio, al menos para un flujo de servicio fallido en el mensaje DSA-REQ correspondiente. Todo conjunto de errores de flujo de servicio DEBE incluir al menos un parámetro QoS fallido específico del flujo de servicio correspondiente. Este parámetro debe omitirse si tiene éxito el mensaje completo DSA-REQ.

Conjunto de errores de clasificador — Se DEBEN incluir un conjunto de errores del clasificador y el par de identificación referencia/identificador del clasificador y del flujo de servicio, al menos para un clasificador fallido en el mensaje DSA-REQ correspondiente. Todo conjunto de errores de clasificador DEBE incluir al menos un parámetro de clasificador fallido, del clasificador correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSA-REQ.

Conjunto de errores de supresión de encabezamiento de cabida útil — Se DEBEN incluir un conjunto de errores PHS y el par de identificación referencia/identificador del clasificador y del flujo de servicio, al menos para una regla PHS fallida en el mensaje DSA-REQ correspondiente. Todo conjunto de errores PHS DEBE incluir al menos un parámetro específico PHS fallido de la regla PHS fallida correspondiente. Este parámetro debe omitirse si tiene éxito el mensaje completo DSA-REQ.

Si la privacidad está habilitada, el mensaje DSA-RSP DEBE contener:

Número de secuencia de clave — El número de secuencia de clave de la clave Auth que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico (véase B.C.1.4.1).

B.8.3.13.1 Adición de servicio dinámica iniciada por un CM

La respuesta DSA del CMTS para flujos de servicio que se adicionan con éxito, DEBE contener un ID de flujo de servicio. La respuesta DSA para conjuntos de parámetros QoS admitidos con éxito o activos en sentido ascendente, debe contener también un ID de servicio.

Si la petición DSA correspondiente utiliza el nombre de clase de servicio (véase B.C.2.2.3.4) para pedir la adición del servicio, una respuesta DSA DEBE contener el conjunto de parámetros QoS asociado con la clase de servicio denominada. Si el nombre de la clase de servicio se utiliza junto con otros parámetros QoS en la petición DSA, el CMTS DEBE aceptar o rechazar la petición DSA utilizando los parámetros QoS explícitos en la petición DSA. Si estas codificaciones de flujo de servicio entran en conflicto con los atributos de clase de servicio, el CMTS DEBE utilizar los valores de la petición DSA como sus títulos de los de la clase de servicio.

Si la transacción tiene éxito, el CMTS DEBE asignar un identificador de clasificador a cada clasificador pedido y asignar un índice PHS a cada regla PHS solicitada. El CMTS DEBE utilizar la o las referencias originales del clasificador y la o las referencias del flujo de servicio para asociar los parámetros con éxito en el mensaje DSA-RSP.

Si la transacción no tiene éxito, el CMTS DEBE utilizar la o las referencias originales del clasificador y la o las referencias del flujo de servicio para identificar los parámetros fallidos en el mensaje DSA-RSP.

B.8.3.13.2 Adición al servicio dinámico iniciada por CMTS

Si la transacción no tiene éxito, el CM DEBE utilizar los identificadores de clasificador y los de flujo de servicio para identificar los parámetros fallidos en el mensaje DSA-RSP.

B.8.3.14 Mensaje de acuse de recibo – Adición al servicio dinámico (DSA-ACK)

El acuse de recibo de la adición al servicio dinámico DEBE ser generado en respuesta a la recepción de un mensaje DSA-RSP. El formato de un mensaje DSA-ACK DEBE ser como se muestra en la figura B.8-33.

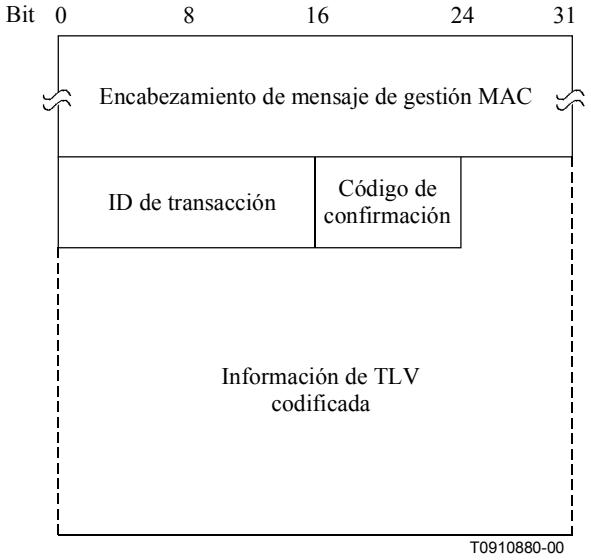


Figura B.8-33/J.112 – Adición al servicio dinámico – Acuse de recibo

Los parámetros DEBEN ser como sigue:

ID de transacción ID de la transacción del mensaje de respuesta DSA correspondiente.

Código de confirmación El código de confirmación apropiado (véase B.C.4) para el mensaje de respuesta DSA completo correspondiente.

NOTA – El código de confirmación se necesita sobre todo cuando se utiliza el nombre de clase de servicio (véase B.10.1.3) en el mensaje de petición DSA. En este caso, el mensaje de respuesta DSA puede contener parámetros de flujo de servicio que el CM no puede soportar (bien temporalmente o de conformidad con la configuración).

Los demás parámetros se codifican como tuplas TLV.

Conjunto de errores de flujo de servicio El conjunto de errores de flujo de servicio del mensaje DSA-ACK codifica los datos específicos de los flujos de servicio fallidos en el mensaje DSA-RSP. Se DEBEN incluir un conjunto de errores de flujo de servicio y una referencia/identificador de identificación del flujo de servicio, al menos para un parámetro QoS fallido de al menos un flujo de servicio fallido en el mensaje DSA-REQ correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSA-REQ.

Si la privacidad está habilitada, el mensaje DSA-ACK DEBE contener:

Número de secuencia de clave El número de secuencia de clave de la clave Auth, que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico (véase B.C.1.4.1).

B.8.3.15 Petición de cambio de servicio dinámico (DSC-REQ)

Un CM o un CMTS PUEDEN enviar una petición de cambio de servicio dinámico, para cambiar dinámicamente los parámetros de un flujo de servicio existente. Los DSC que cambian clasificadores DEBEN transportar el conjunto completo de parámetros TLV de clasificadores de ese nuevo clasificador.

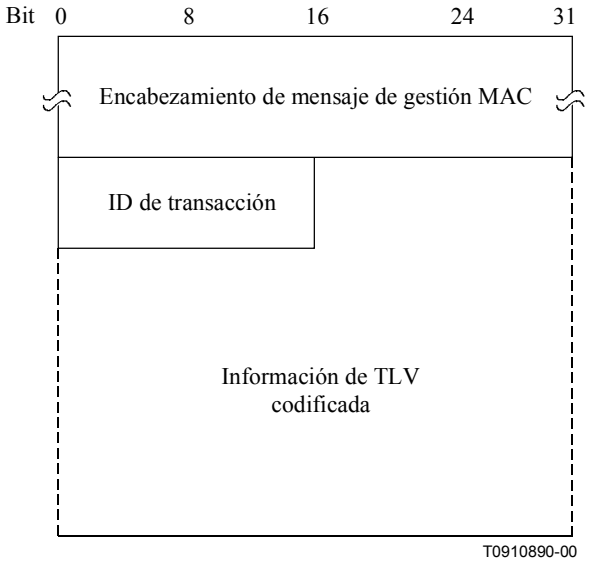


Figura B.8-34/J.112 – Petición de cambio de servicio dinámico

Un CM o un CMTS DEBEN generar mensajes DSC-REQ con el formato mostrado en la figura B.8-34, incluyendo los siguientes parámetros:

ID de transacción Identificador único asignado por el emisor para esta transacción.

Los demás parámetros se codifican como las tuplas TLV definida en el anexo B.C. Un mensaje DSC-REQ NO DEBE transportar parámetros para más de un flujo de servicio en cada sentido, es decir, un mensaje DSC-REQ DEBE contener parámetros para un flujo de servicio único en sentido ascendente, o bien para uno en sentido descendente o para un flujo de servicio en sentido ascendente y uno en sentido descendente. Un mensaje DSC-REQ DEBE contener al menos uno de los siguientes parámetros:

Parámetros de clasificador Especificación de las reglas que se han de utilizar para clasificar los paquetes dentro de un flujo de servicio específico. Esto incluye el parámetro TLV de acción de cambio de servicio dinámico que indica si este clasificador debe ser añadido, reemplazado o suprimido del flujo de servicio (véase B.C.2.1.3.7). Si están incluidos, los parámetros de clasificador DEBEN contener una referencia/identificador de clasificador y un identificador de flujo de servicio.

NOTA – Si el mensaje DSC-REQ es iniciado por un CM y el cambio se efectúa en un clasificador existente, se trata de un identificador de clasificador. Si el mensaje DSC-REQ es iniciado por un CM y el clasificador es un clasificador nuevo, se trata de una referencia de clasificador.

Parámetros de flujo de servicio Especificación de las características de tráfico nuevo del flujo de servicio y los requisitos de programación. Los conjuntos de parámetros de calidad de servicio admitidos y activos en este mensaje reemplazan a los conjuntos de parámetros de calidad de servicio admitidos y activos que emplea en ese momento el flujo de servicio. Si el mensaje DSC tiene éxito y contiene parámetros de flujo de servicio, pero no contiene conjuntos de reemplazo de los conjuntos de parámetros de calidad de servicio admitidos y activos, el o los conjuntos omitidos, se DEBEN fijar a nulo. Si están incluidos, los parámetros de flujo de servicio DEBEN contener un identificador de flujo de servicio.

Parámetros de supresión de encabezamiento de cabida útil Especificación de las reglas que se han de utilizar para la supresión del encabezamiento de la cabida útil, para suprimir los encabezamientos de cabida útil relacionados con un clasificador específico. Esto incluye el parámetro TLV de acción cambio de servicio dinámico que indica si la regla PHS se debe añadir, fijar o suprimir del flujo de servicio o si todas las reglas PHS del flujo de servicio especificado deben ser eliminadas (véase B.C.2.2.8.5). Si están incluidos, los parámetros PHS DEBEN contener una referencia/identificador de clasificador y un identificador de flujo de servicio, a menos que la acción de cambio de servicio dinámico sea "Eliminar todas las reglas PHS". Si la acción de cambio en el servicio dinámico es "Eliminar todas las reglas PHS", los parámetros PHS deben contener un identificador de flujo de servicio junto con la acción de cambio en el servicio dinámico, y en este caso no se requiere la presencia de otros parámetros PHS. Sin embargo, si están presentes otros parámetros PHS, en particular el índice de supresión de encabezamiento de cabida útil, DEBEN ser ignorados por el receptor del mensaje DSC-REQ.

Si la privacidad está habilitada, el mensaje DSC-REQ DEBE contener también:

Número de secuencia de clave El número de secuencia de clave de la clave Auth, que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico (véase B.C.1.4.1).

B.8.3.16 Respuesta de cambio de servicio dinámico (DSC-RSP)

La respuesta de cambio de servicio dinámico DEBE ser generada en respuesta a un mensaje DSC-REQ recibido. El formato de un mensaje DSC-RSP DEBE ser como el que se muestra en la figura B.8-35.

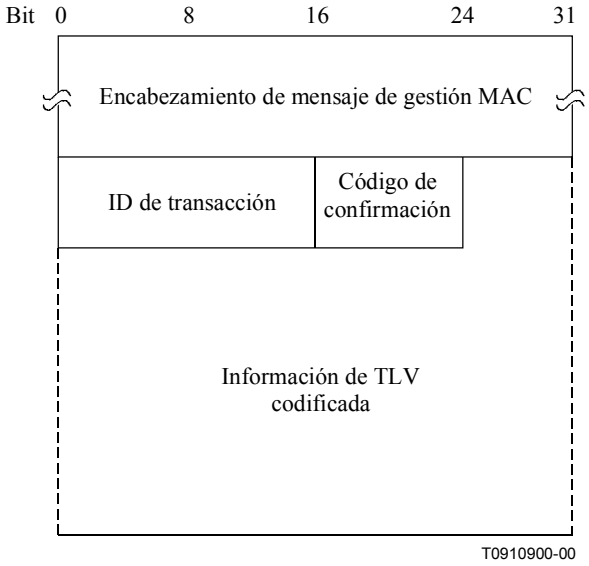


Figura B.8-35/J.112 – Respuesta de cambio de servicio dinámico

Los parámetros DEBEN ser como sigue:

ID de transacción ID de transacción del mensaje DSC-REQ correspondiente.

Código de confirmación El código de confirmación apropiado (véase B.C.4) para la petición DSC correspondiente.

Los demás parámetros se codifica como las tuplas TLV definidas en el anexo B.C.

Si la transacción tiene éxito, el mensaje DSC-RSP PUEDE contener uno o más de los siguientes parámetros:

Parámetros de clasificador Se DEBE incluir la especificación completa del clasificador en el mensaje DSC-RSP sólo si incluye un identificador de clasificador recién asignado. Si un clasificador pedido contiene una referencia de clasificador, el mensaje DSC-RSP DEBE contener un identificador de clasificador.

Parámetros de flujo de servicio — Se DEBE incluir la especificación completa del flujo de servicio en el mensaje DSC-RSP sólo si incluye un nombre de clase de servicio ampliado. Un SFID sólo puede ser asignado en un DSA, no en un DSC. Si un conjunto de parámetros de flujo de servicio contiene un conjunto de parámetros QoS admitidos en sentido ascendente y este flujo de servicio no tiene un SID asociado, el mensaje DSC-RSP DEBE incluir un SID. Si un conjunto de parámetros de flujo de servicio contiene un nombre de clase de servicio y un conjunto de parámetros QoS admitidos, el mensaje DSC-RSP DEBE incluir el conjunto de parámetros QoS correspondiente a la clase de servicio denominada. Si los parámetros QoS específicos estuviesen incluidos también en la petición de flujo de servicio con clase de servicio, estos parámetros QoS DEBEN estar incluidos en el mensaje DSC-RSP en lugar de cualesquiera otros parámetros QoS del mismo tipo de la clase de servicio denominada.

Parámetros de supresión de encabezamientos de cabida útil — Se DEBE incluir la especificación completa de los parámetros PHS En el mensaje DSC-RSP sólo si incluye el índice PHS recién asignado. Si lo incluye, los parámetros PHS DEBEN contener una referencia/identificador de clasificador y un identificador de flujo de servicio.

Si la transacción no tiene éxito, y el código de confirmación no es uno de los códigos de error importantes de B.C.4.2, el mensaje DSC-RSP DEBE contener al menos uno de los siguientes conjuntos de errores:

Conjunto de errores de clasificador — Se DEBEN incluir un conjunto de errores de clasificador y el par de identificación referencia/identificador del clasificador y del flujo de servicio, al menos para un clasificador fallido en el mensaje DSC-REQ correspondiente. Todo conjunto de errores de clasificador DEBE incluir al menos un parámetro de clasificador fallido del clasificador correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSC-REQ.

Conjunto de errores de flujo de servicio — Se DEBEN incluir un conjunto de errores de flujo de servicio y un ID de identificación de flujo de servicio, al menos para un flujo de servicio fallido en el mensaje DSC-REQ correspondiente. Todo conjunto de errores de flujo de servicio DEBE incluir al menos un parámetro QoS fallido específico del flujo de servicio correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSC-REQ.

Conjunto de errores de supresión de encabezamiento de cabida útil — Se DEBEN incluir un conjunto de errores tipo PHS y el par de identificación referencia/identificador del flujo de servicio y del clasificador, al menos para una regla PHS fallida en el mensaje DSC-REQ correspondiente, a menos que la acción de cambio de servicio dinámico sea "Eliminar todas las reglas PHS". Si la acción de cambio de servicio dinámico es "Eliminar todas las reglas PHS" los conjuntos de errores PHS DEBEN incluir un ID de identificación de flujo de servicio. Todo conjunto de errores PHS DEBE incluir al menos un parámetro PHS fallido específico de la regla PHS fallida correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSC-REQ.

Independientemente del éxito o fallo, si está habilitada la privacidad para el CM, el mensaje DSC-RSP DEBE contener:

Número de secuencia de clave — El número de secuencia de clave de la clave Auth, que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico (véase B.C.1.4.1).

B.8.3.17 Acuse de recibo de cambio de servicio dinámico (DSC-ACK)

El acuse de recibo de cambio de servicio dinámico DEBE ser generado en respuesta a la recepción de un mensaje DSC-RSP. El formato del mensaje DSC-ACK DEBE ser como se muestra en la figura B.8-36.

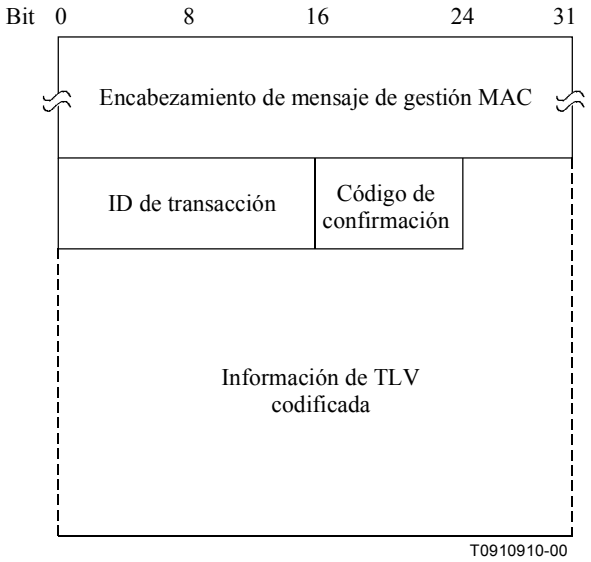


Figura B.8-36/J.112 – Acuse de recibo de cambio de servicio dinámico

Los parámetros DEBEN ser como sigue:

ID de transacción — ID de transacción del mensaje DSC-REQ correspondiente.

Código de confirmación — El código de confirmación apropiado (véase B.C.4) para la respuesta DSC completa correspondiente.

NOTA – El código de confirmación y el conjunto de errores de flujo de servicio se necesitan sobre todo cuando se utiliza un nombre de clase de servicio (véase B.10.1.3) en la petición DSC. En este caso, la respuesta DSC puede contener parámetros de flujo de servicio que el CM no puede soportar (ya sea temporalmente o de acuerdo con la configuración).

Los demás parámetros se codifican como tuplas TLV.

Conjunto de errores de flujo de servicio — El conjunto de errores de flujo de servicio del mensaje DSC-ACK codifica datos específicos de los flujos de servicio fallidos en el mensaje DSC-RSP. Se DEBEN incluir un conjunto de errores de flujo de servicio y un identificador de flujo de servicio, al menos para un parámetro QoS fallido de al menos un flujo de servicio fallido en el mensaje DSC-REQ correspondiente. Este parámetro DEBE omitirse si tiene éxito el mensaje completo DSC-REQ.

Si la privacidad está habilitada, el mensaje DSC-ACK DEBE contener:

Número de secuencia de clave — El número de secuencia de clave de la clave Auth, que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico (véase B.C.1.4.1).

B.8.3.18 Petición de supresión de servicio dinámica (DSD-REQ)

Un CM o un CMTS PUEDEN enviar una petición DSD para suprimir un flujo de servicio existente. El formato de una petición DSD DEBE ser como se muestra en la figura B.8-37.

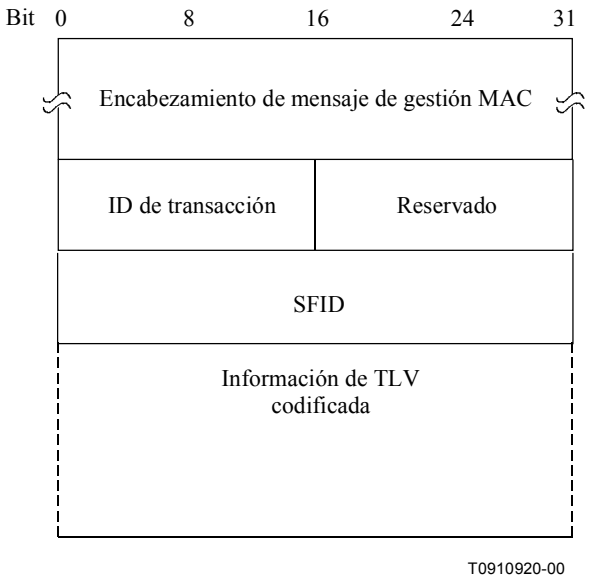


Figura B.8-37/J.112 – Petición de supresión de servicio dinámica

Los parámetros DEBEN ser como sigue:

Identificador de flujo de servicio El SFID que se ha de suprimir.

ID de transacción Identificador único para esta transacción asignado por el emisor.

Los demás parámetros se codifican como las tuplas TLV definidas en el anexo B.C.

Referencia de flujo de servicio El CM DEBE colocar la SFR en los mensajes DSD-REQ de una transacción local DSD si la transacción fue creada por la transición hacia el estado de supresión desde el estado local de adición. El CMTS DEBE colocar el SFR en los mensajes DSD-REQ de una transacción local DSD si la transacción fue creada por la transición hacia el estado de supresión desde el estado de adición distante. Véase la figura B.11-21.

Si la privacidad está habilitada, el mensaje DSD-REQ DEBE incluir:

Número de secuencia de clave El número de secuencia de la clave Auth, que se utiliza para calcular el compendio HMAC (véase B.C.1.4.3).

Compendio HMAC El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de servicio dinámico. (Véase B.C.1.4.1.)

B.8.3.19 Respuesta de supresión de servicio dinámica (DSD-RSP)

Se DEBE generar un mensaje DSD-RSP en respuesta a la recepción de un mensaje DSD-REQ. El formato de un mensaje DSD-RSP DEBE ser como se muestra en la figura B.8-38.

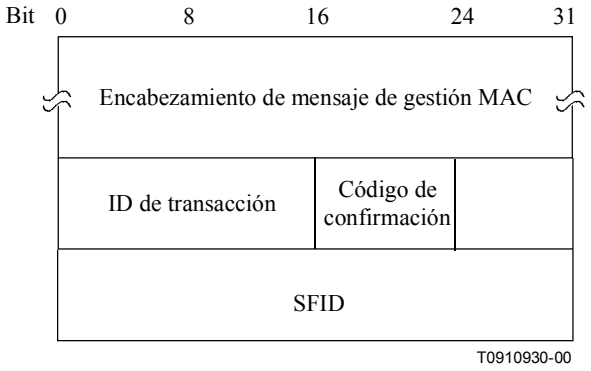


Figura B.8-38/J.112 – Respuesta de supresión de servicio dinámica (DSD-RSP)

Los parámetros DEBEN ser como sigue:

Identificador de flujo de servicio SFID desde el mensaje DSD-REQ al que se refiere este acuse de recibo.

ID de transacción ID de transacción desde el mensaje DSD-REQ correspondiente.

Código de confirmación El código de confirmación apropiado (véase B.C.4) para el mensaje de petición DSD correspondiente.

B.8.3.20 Petición de cambio de canal dinámico (DCC-REQ)

Un CMTS PUEDE transmitir una petición de cambio de canal dinámico para hacer que un CM con capacidad DCC cambie el canal en sentido ascendente por el cual está transmitiendo, un canal en sentido descendente por el cual está recibiendo, o ambos. (Véase la figura B.8-39.)

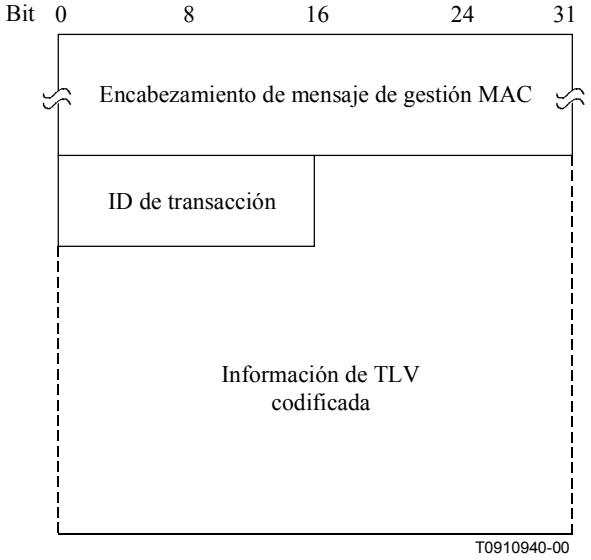


Figura B.8-39/J.112 – Petición de cambio de canal dinámico

Un CMTS DEBE generar un mensaje DCC-REQ con el formato mostrado en la figura B.8-39 incluyendo el siguiente parámetro:

ID de transacción — Un identificador único de 16 bits para esta transacción asignado por el emisor.

Los siguientes parámetros son opcionales y se codifican como tuplas TLV:

ID del canal en sentido ascendente — Identificador del canal en sentido ascendente al que debe conmutar el CM para transmisiones en sentido ascendente.

Parámetros en sentido descendente — La frecuencia del canal en sentido descendente a la que debe conmutar el CM para recepción en sentido descendente.

Técnica de inicialización — Direcciones para el tipo de inicialización, si existe alguna, las cuales deben ser ejecutadas por el CM una vez que se sincroniza con los nuevos canales.

Sustitución de UCD — Proporciona una copia del UCD para el nuevo canal. Este formato TLV ocurre una sola vez y contiene un UCD.

Sustitución de SAID — Un par de identificadores de asociación de seguridad (SAID, *security association identifiers*) que contienen el SAID en uso y el nuevo SAID para el nuevo canal. Este formato TLV ocurre una vez si el SAID requiere sustitución.

Sustitución del flujo de servicio — Un grupo de subformatos TLV que permite la sustitución en un flujo de servicio del identificador de flujo de servicio, identificador de servicio, identificador de clasificador, e índice de supresión de encabezamiento de cabida útil. Se repite este formato TLV para cada flujo de servicio que tenga parámetros que requieren sustitución.

Si la privacidad está habilitada, un mensaje DCC-REQ DEBE contener también:

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de cambio de canal dinámico (véase B.C.1.4.1).

B.8.3.20.1 Codificaciones

Los valores de tipo que se utilizan DEBEN ser los que se muestran más adelante. Estos mensajes son únicos dentro del mensaje de petición de cambio de canal dinámico, pero no en todo el conjunto de mensajes MAC.

Si un CM ejecuta un cambio de canal sin ejecutar una reinicialización (como se define en B.8.3.20.1.3), todas las variables de la configuración del CM permanecen constantes, con excepción de las variables de la configuración que explícitamente se cambian más adelante. El CM no estará al corriente de ningún cambio de configuración distinto de los que provocados por la instrucción DCC, por lo que es importante la coherencia al aprovisionar entre los canales antiguos y los nuevos.

B.8.3.20.1.1 ID de canal en sentido ascendente

Cuando está presente, este formato TLV especifica el nuevo ID de canal en sentido ascendente que DEBE utilizar el CM cuando ejecuta un cambio de canal dinámico. Se trata de una sustitución del ID del canal en uso en sentido ascendente. El CMTS DEBE asegurar que el ID de canal en sentido ascendente del nuevo canal es diferente del ID de canal en sentido ascendente del canal antiguo. El formato TLV DEBE estar incluido si se cambia el canal en sentido ascendente, aun si está incluido el TLV de sustitución de UCD.

Tipo	Longitud	Valor
1	1	0-255: ID de canal en sentido ascendente

Si este formato TLV está ausente, el CM NO DEBE cambiar su ID de canal en sentido ascendente. El CMTS PUEDE incluir este TLV. El CM DEBE cumplir con este TLV.

B.8.3.20.1.2 Parámetros en sentido descendente

Cuando está presente, este formato TLV especifica los parámetros de funcionamiento del nuevo canal en sentido descendente. El campo valor de este TLV contiene una serie de subtipos. El CMTS DEBE incluir todos los subtipos.

Tipo	Longitud	Valor
2	N	

Si este formato TLV está ausente, el CM NO DEBE cambiar sus parámetros de sentido descendente.

B.8.3.20.1.2.1 Frecuencia en sentido descendente

Este formato TLV especifica la nueva frecuencia de recepción que DEBE utilizar el CM cuando ejecuta un cambio de canal dinámico. Se trata de una sustitución de la frecuencia en uso del canal en sentido descendente. Es la frecuencia central en Hz del canal en sentido descendente y se almacena como un número binario de 32 bits. La frecuencia en sentido descendente DEBE ser un múltiplo de 62 500 Hz.

Tipo	Longitud	Valor
2.1	4	Frecuencia de recepción

El CMTS DEBE incluir este subformato TLV. El CM DEBE cumplir con este subformato TLV.

B.8.3.20.1.2.2 Tipo de modulación en sentido descendente

Este formato TLV especifica el tipo de modulación que se utiliza sobre el nuevo canal en sentido descendente.

Tipo	Longitud	Valor
2.2	1	0 = 64QAM 1 = 256QAM 2-255: reservado

El CMTS DEBERÍA incluir este subformato TLV. El CM DEBERÍA cumplir con este subformato TLV.

B.8.3.20.1.2.3 Velocidad de símbolos en sentido descendente

Este formato TLV especifica la velocidad de símbolos que se utiliza en el nuevo canal en sentido descendente.

Tipo	Longitud	Valor
2.3	1	0 = 5,056941 Msymb/s 1 = 5,360537 Msymb/s 2 = 6,952 Msymb/s 3-255: reservado

El CMTS DEBERÍA incluir este subformato TLV. El CM DEBERÍA cumplir con este subformato TLV.

B.8.3.20.1.2.4 Profundidad de intercalador en sentido descendente

Este formato TLV especifica los parámetros "I" y J del intercalador en sentido descendente.

Subtipo	Longitud	Valor
2.4	2	I: 0-255 J: 0-255

El CMTS DEBERÍA incluir este subformato TLV. El CM DEBERÍA cumplir con este subformato TLV.

B.8.3.20.1.2.5 Identificador de canal en sentido descendente

Este formato TLV especifica el identificador de canal en sentido descendente de 8 bits del nuevo canal en sentido descendente. El CMTS DEBE asegurar que el ID del canal en sentido descendente del nuevo canal es diferente del ID de canal en sentido descendente del canal antiguo.

Subtipo	Longitud	Valor
2.5	1	0-255: ID de canal en sentido descendente

El CMTS DEBERÍA incluir este subformato TLV. El CM DEBERÍA cumplir con este subformato TLV.

B.8.3.20.1.3 Técnica de inicialización

Cuando está presente este formato TLV permite al CMTS indicar al CM el nivel de reinicialización que DEBE ejecutar antes de que pueda comenzar las comunicaciones por los nuevos canales. El CMTS puede tomar esta decisión con base en su conocimiento de las diferencias entre los dominios MAC nuevo y antiguo y las características PHY de sus canales en sentido ascendente y en sentido descendente.

Típicamente, si el movimiento se produce entre canales en sentido ascendente y/o en sentido descendente dentro del mismo dominio MAC, pueden dejarse intactos los valores del perfil de conexión. Si el movimiento se produce entre diferentes dominios MAC, puede ejecutarse una inicialización completa.

Si no se requiere una reinicialización completa, quizás PUEDE requerirse a algún realineamiento. Por ejemplo, ciertas áreas del espectro en sentido ascendente se configuran a menudo en grupos. Un mensaje DCC-REQ hacia un canal adyacente en sentido ascendente dentro de un grupo puede que no garantice el realineamiento. Alternativamente, un mensaje DCC-REQ hacia un canal no adyacente en sentido ascendente podría requerir mantenimiento de estación mientras que un mensaje DCC-REQ desde uno hacia otro grupo de canales en sentido ascendente podría requerir

mantenimiento inicial. El realineamiento PUEDE requerirse también si existe alguna diferencia en los parámetros PHY entre los canales antiguo y nuevo.

Tipo	Longitud	Valor
3	1	0 = Reinicialización del MAC 1 = Ejecución del mantenimiento inicial por el nuevo canal antes del funcionamiento normal 2 = Ejecución del mantenimiento de estación por el nuevo canal antes del funcionamiento normal 3 = Ejecución del mantenimiento inicial o del mantenimiento de estación por el nuevo canal antes del funcionamiento normal 4 = Utilización directamente de los nuevos canales sin reinicialización o ejecución de mantenimiento inicial o de estación 5-255: reservados

En primer lugar el CM DEBE seleccionar los nuevos canales en sentido ascendente y sentido descendente en base al formato TLV de identificación del canal en sentido ascendente (véase B.8.3.20.1.1) y el formato TLV de la frecuencia en sentido descendente (véase B.8.3.20.1.2.1). A continuación el CM DEBE seguir las directrices de este formato TLV. Para la opción 0, el CM DEBE comenzar con el SID de inicialización. Para las opciones 1 a 4 el CM DEBE continuar utilizando el SID primario para alineación. Un TLV de sustitución de SID (véase B.8.3.20.1.7.2) puede especificar un nuevo SID primario para utilizarlo en el nuevo canal.

Opción 0: Esta opción indica al CM para que ejecute todas las operaciones asociadas con la inicialización del CM (véase B.11.2). Se incluyen aquí todos los eventos después de la adquisición de QAM, FEC, y el enganche MPEG en sentido descendente, y antes del funcionamiento normalizado (véase B.11.3), incluyendo la obtención de un UCD, la alineación, el establecimiento de la conectividad IP, el establecimiento de la hora del día, la transferencia de los parámetros operacionales, el registro, y la inicialización de la privacidad básica. Cuando se utiliza esta opción, los únicos formatos TLV relevantes en el mensaje DCC-REQ son el TLV de identificación del canal en sentido ascendente y el TLV de los parámetros en sentido descendente. Los demás formatos TLV de los mensajes DCC-REQ carecen de interés.

Opción 1: Si se especifica mantenimiento inicial, el funcionamiento por el nuevo canal podría ser retardado por varios intervalos de alineación (véase el anexo B.B).

Opción 2: Si se especifica mantenimiento de estación, el funcionamiento por el nuevo canal podría ser retardada por el valor de T4 (véase el anexo B.B).

Opción 3: Este valor autoriza a un CM a utilizar una región de mantenimiento inicial o mantenimiento de estación, cualquiera que sea lo que seleccione el CM. Este valor podría ser utilizado si hubiera incertidumbre respecto a cuándo el CM PUEDE ejecutar la instrucción DCC y existe, en consecuencia, la posibilidad de que pierda intervalos de tiempo de mantenimiento de estación.

Opción 4: Esta opción permite que la interrupción de servicio sea mínima y que el CM pueda continuar su funcionamiento normal tan pronto como alcanza la sincronización en el nuevo canal. La utilización prevista de esta opción es con un cambio casi perfecto de canal (véase B.11.4.5.3).

NOTA – Esta opción no debería ser utilizada en plantas físicas en las que las características de transmisión en sentido ascendente no son coherentes.

Si este formato TLV está ausente, el CM DEBE reinicializar el MAC. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.4 Sustitución de UCD

Cuando está presente, este formato TLV permite al CMTS enviar un mensaje descriptor de canal en sentido ascendente hacia el CM. Lo que se pretende es que este mensaje UCD se asocie con los nuevos canales en sentido ascendente y/o sentido descendente. El CM almacena los mensajes UCD en su memoria guardada, y los utiliza después de la sincronización con los nuevos canales.

Tipo	Longitud	Valor
4	n	UCD para el nuevo canal en sentido ascendente

Este formato TLV incluye todos los parámetros del mensaje UCD descritos en B.8.3.3 excepto por lo que se refiere al encabezamiento del mensaje de gestión MAC. El CMTS DEBE asegurar que la cuenta de cambios en el UCD concuerde con la cuenta de cambios en los UCD de los nuevos canales. El CMTS DEBE asegurar que el ID del canal en sentido ascendente del nuevo canal es diferente del ID del canal en sentido ascendente del canal antiguo.

Si el CM tiene que esperar la llegada de un mensaje UCD nuevo cuando se cambian los canales, el funcionamiento puede ser suspendido durante un cierto tiempo hasta el "intervalo UCD" (véase el anexo B.B) o un tiempo mayor, si el mensaje UCD se pierde.

El CMTS DEBERÍA incluir este formato TLV. El CM DEBERÍA cumplir con este formato TLV.

B.8.3.20.1.5 Sustitución de SYNC

Cuando está presente, este formato TLV permite al CMTS indicar al CM si tiene que esperar o no la llegada de un mensaje SYNC antes de proceder. El CMTS DEBE haber sincronizado las indicaciones de tiempo entre los canales antiguo y nuevo si indica al CM que no espere la llegada de un mensaje SYNC antes de transmitir por el nuevo canal. La sincronización de las indicaciones de tiempo implica el que se derivaban del mismo reloj y contienen el mismo valor.

Tipo	Longitud	Valor
5	1	0 = Adquisición del mensaje SYNC en el nuevo canal en sentido descendente antes de proceder 1 = Proceder sin antes obtener el mensaje SYNC 2-255: reservados

Si este formato TLV está ausente, el CM DEBE esperar la llegada de un mensaje SYNC por el nuevo canal antes de proceder. Si el CM tiene que esperar la llegada de un nuevo mensaje SYNC cuando se cambian los canales, el funcionamiento puede ser suspendido durante un cierto tiempo hasta el "intervalo SYNC" (véase anexo B.B) o un tiempo mayor, si el mensaje SYNC se pierde o no está sincronizado con los canales antiguos.

Un enfoque alternativo consiste en enviar mensajes SYNC más frecuentes (cada 10 ms por ejemplo), y pedir al CM que espere la llegada de un mensaje SYNC antes de proceder. Este enfoque conlleva una latencia ligeramente mayor, pero proporciona una verificación adicional para evitar que el CM transmita en un intervalo de tiempo incorrecto.

El CMTS DEBERÍA incluir este formato TLV. El CM DEBERÍA cumplir con este formato TLV.

B.8.3.20.1.6 Sustitución del identificador de asociación de seguridad (SAID)

Cuando está presente, este formato TLV permite al CMTS sustituir el identificador de asociación de seguridad (SAID) en el flujo de servicio en uso por nuevo identificador de asociación de seguridad. Las claves de privacidad básica asociadas con el SAID DEBEN seguir siendo las mismas. El CM no tiene que responder simultáneamente al SAID nuevo y antiguo.

Tipo	Longitud	Valor
6	4	SAID en uso (los 14 bits de orden inferior de un campo de 16 bits), SAID nuevo (los 14 bits de orden inferior de un campo de 16 bits)

Si este formato TLV está ausente, se retiene la asignación del identificador de asociación de seguridad en uso. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7 Sustituciones en flujos de servicio

Cuando está presente, este formato TLV permite al CMTS sustituir parámetros específicos dentro de los flujos de servicio en uso en la asignación de canal actual por nuevos parámetros para la asignación del nuevo canal. Se emplea un formato TLV para cada flujo de servicio que requiere cambios de parámetros. El CMTS PUEDE decidir hacer esto para facilitar el establecimiento de nuevas reservas de QoS en el nuevo canal antes de suprimir las reservas de QoS en el canal antiguo. El CM no tiene que responder simultáneamente a los flujos de servicio antiguo y nuevo.

Este formato TLV permite desplazar las asignaciones de recursos y servicios entre dos espacios de valor ID independiente y programar entidades cambiando los ID y los índices asociados. Los espacios de valor ID que pueden diferir entre los dos canales incluyen el identificador de flujo de servicio, el ID de servicio, el identificador de clasificador, y el índice de supresión de encabezamiento de cabida útil. Este formato TLV no permite cambios en los parámetros QoS del flujo de servicio, los parámetros de clasificador o los parámetros de las reglas PHS.

Los nombres de clase de servicio utilizados dentro del ID de flujo de servicio deben permanecer idénticos entre los canales antiguo y nuevo.

Tipo	Longitud	Valor
7	n	Lista de subtipos

Si este formato TLV está ausente para un flujo de servicio particular, se retienen el flujo de servicio en uso y sus atributos. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7.1 Sustitución del identificador de flujo de servicio

Este formato TLV permite al CMTS sustituir el identificador de flujo de servicio en uso (SFID) por un nuevo identificador de flujo de servicio. Véase B.C.2.2.3.2 para los detalles sobre la utilización de este parámetro.

Este formato TLV DEBE estar presente si se efectúa cualquier otra sustitución del subtipo del flujo de servicio. Si este formato TLV está incluido y el ID del flujo de servicio no cambia, se fijarán en el mismo valor el ID del flujo de servicio en uso y el del nuevo.

Subtipo	Longitud	Valor
7.1	8	ID del flujo de servicio en uso, ID del flujo de servicio nuevo

El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7.2 Sustitución de identificador de servicio

Cuando está presente, este formato TLV permite al CMTS sustituir el identificador de servicio (SID, *service identifier*) en el flujo de servicio en uso en sentido ascendente por un nuevo identificador de servicio. Véase B.C.2.2.3.3 para los detalles sobre la utilización de este parámetro.

Subtipo	Longitud	Valor
7.2	4	SID en uso (los 14 bits de orden inferior de un campo de 16 bits), SID nuevo (los 14 bits de orden inferior de un campo de 16 bits)

Si este formato TLV está ausente, se retienen las asignaciones del identificador de servicio en uso. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7.3 Sustitución de ID de clasificador

Cuando está presente, este formato TLV permite al CMTS sustituir el identificador de clasificador en uso por un nuevo identificador de clasificador. Se utiliza un TLV para cada par de identificadores de clasificador antiguo y nuevo que se van a sustituir dentro de este flujo de servicio. Véase B.C.2.1.3.2 para los detalles de la utilización de este parámetro.

Subtipo	Longitud	Valor
7.3	4	ID del clasificador en uso, ID del clasificador nuevo

Si este formato TLV está ausente, se retiene el identificador en uso. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7.4 Sustitución de índice de supresión de encabezamiento de cabida útil

Cuando está presente, este formato TLV permite al CMTS sustituir el índice de supresión de encabezamiento de cabida útil en uso (PHSI) por un nuevo índice de supresión de encabezamiento de cabida útil. Véase B.C.2.2.10.2 para los detalles sobre la utilización de este parámetro.

Subtipo	Longitud	Valor
7.4	2	PHSI en uso, PHSI nuevo

Si este formato TLV está ausente, se retiene el índice de supresión de encabezamiento de cabida útil en uso. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.20.1.7.5 Sustitución de referencia de tiempo de concesión no solicitada

Cuando está presente, este formato TLV permite al CMTS sustituir la referencia de tiempo de concesión no solicitada en uso por una nueva referencia de tiempo de concesión no solicitada. Véase B.C.2.2.6.11 para detalles sobre la utilización de este parámetro.

Este formato TLV es útil si los canales en sentido ascendente antiguo y nuevo utilizan bases de tiempo diferentes para sus indicaciones de tiempo. Este formato TLV también es de utilidad si la ventana de transmisión de concesión no solicitada se desplaza a un punto diferente en el tiempo. El cambio de este valor puede hacer que el funcionamiento exceda temporalmente la ventana de fluctuación de fase especificada en B.C.2.2.6.8.

Subtipo	Longitud	Valor
7.5	4	Nueva referencia

Si este formato TLV está ausente, se retiene la referencia de tiempo de concesión no solicitada en uso. El CMTS PUEDE incluir este formato TLV. El CM DEBE cumplir con este formato TLV.

B.8.3.21 Respuesta de cambio de canal dinámico (DCC-RSP)

Un CM PUEDE soportar un cambio de canal dinámico. Si el CM soporta el cambio de canal dinámico, un CM DEBE transmitir un mensaje de respuesta de cambio de canal dinámico en respuesta a la recepción de un mensaje de petición de cambio de canal dinámico para indicar que lo recibió y que está dando cumplimiento al mensaje DCC-REQ. El formato de un mensaje DCC-RSP DEBE ser como el que se muestra en la figura B.8-40.

Antes de comenzar a conmutar a un nuevo canal en sentido ascendente o en sentido descendente, un CM DEBE transmitir un mensaje DCC-RSP por su canal en uso en sentido ascendente. Cuando un CM recibe un mensaje DCC-REQ pidiendo que se conmute a un canal en sentido ascendente y/o en sentido descendente que ya está siendo utilizado, el CM DEBE responder con un mensaje DCC-RSP por ese canal indicando que ya se está utilizando el canal correcto.

Un CM PUEDE ignorar un mensaje DCC-REQ mientras se encuentra en el proceso de ejecución de un cambio de canal.

Después de la conmutación a un nuevo canal, si el MAC no es reinicializado según el formato TLV de inicialización DCC-REQ, opción 0, el CM DEBE enviar un mensaje DCC-RSP al CMTS. NO DEBE enviarse un mensaje DCC-RSP si el CM reinicializa su MAC.

En B.11.4.5 se describe el procedimiento completo de cambio de canales.

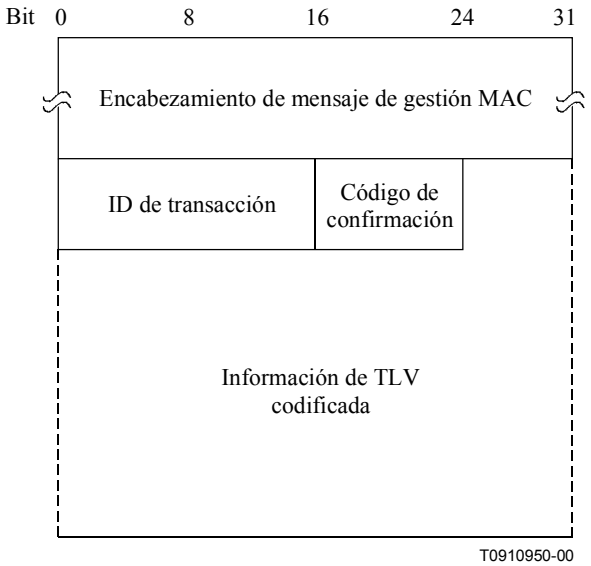


Figura B.8-40/J.112 – Respuesta de cambio de canal dinámico

Los parámetros DEBEN ser como sigue:

ID de la transacción Un ID de transacción de 16 bits del mensaje DCC-REQ correspondiente.

Código de confirmación Un código de confirmación de 8 bits como se describe en B.C.4.1.

Los siguientes parámetros son opcionales y se codifican como tuplas TLV.

Tiempo de salto del CM — Parámetros de temporización que describen cuándo tiene que hacer un salto el CM.

Independientemente del éxito o el fallo, si la privacidad está habilitada para el CM, el mensaje DCC-RSP DEBE contener:

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de cambio de canal dinámico (véase B.C.1.4.1).

B.8.3.21.1 Codificaciones

Los valores de tipo utilizados DEBEN ser los que se muestran más adelante. Estos valores son únicos dentro del mensaje de respuesta de cambio del canal dinámico, pero no en todo el conjunto de mensajes MAC.

B.8.3.21.1.1 Tiempo de salto de CM

Cuando está presente, este formato TLV permite al CM indicar al CMTS cuándo tiene previsto el CM efectuar su salto y desconectarse de la red. Con esta información, el CMTS PUEDE tomar medidas preventivas para minimizar o eliminar la pérdida de paquetes en el sentido descendente debido al cambio de canal.

Tipo	Longitud	Valor
1	n	

La referencia de tiempo y las unidades de tiempo de estos subformatos TLV se basan en la misma base de tiempo de 32 bits utilizada en el mensaje SYNC por el canal en uso en sentido descendente. Esta indicación de tiempo es incrementada por un reloj de 10,24 MHz.

El CM DEBERÍA incluir este formato TLV. El CMTS DEBERÍA cumplir con este formato TLV.

B.8.3.21.1.1.1 Longitud de salto

Este formato TLV indica al CMTS la longitud del salto desde el canal previo hasta el canal nuevo. Específicamente, representa el tiempo durante el cual el CM no podrá recibir datos en sentido descendente.

Tipo	Longitud	Valor
1	4	Longitud (en base a la indicación de tiempo)

El CM DEBE incluir este subformato TLV.

B.8.3.21.1.1.2 Tiempo de comienzo de salto

Cuando está presente, este formato TLV indica al CMTS el momento posterior en el que el CM tiene previsto efectuar el salto.

Subtipo	Longitud	Valor
2	8	Tiempo de comienzo (en base a la indicación de tiempo), exactitud de tiempo de comienzo (en base a la indicación de tiempo)

La base de tiempo de 32 bits, 10,24 MHz completa su ciclo cada 7 minutos aproximadamente. Si el valor del tiempo de comienzo es menor que la indicación de tiempo actual, el CMTS presupondrá que ha transcurrido un ciclo completo del contador de indicaciones de tiempo. La exactitud del tiempo de comienzo es una cantidad absoluta de tiempo antes y después de ese tiempo de comienzo.

La ventana de salto potencial es desde (tiempo de comienzo – exactitud) hasta (tiempo de comienzo + exactitud + longitud).

El CM DEBERÍA incluir este formato TLV.

B.8.3.22 Acuse de recibo de cambio de canal dinámico (DCC-ACK)

El acuse de recibo de cambio de canal dinámico DEBE ser transmitido por un CMTS en respuesta a la recepción de un mensaje de respuesta de cambio de canal dinámico por el nuevo canal con su código de confirmación fijado en llegada (1). El formato de un mensaje DCC-ACK DEBE ser como se muestra en la figura B.8-41.

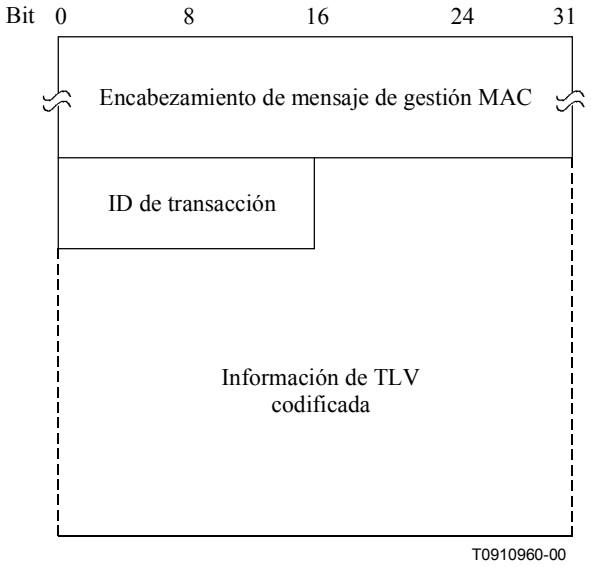


Figura B.8-41/J.112 – Acuse de recibo de cambio de canal dinámico

Los parámetros DEBEN ser como sigue:

ID de la transacción — Un ID de transacción de 16 bits del mensaje DCC-RSP correspondiente

Si la privacidad está habilitada, el mensaje DCC-ACK DEBE contener:

Compendio HMAC — El atributo del compendio HMAC es un compendio de mensajes en clave (para autenticar al emisor). El atributo del compendio HMAC DEBE ser el atributo final en la lista de atributos del mensaje de cambio de canal dinámico (véase B.C.1.4.1).

B.8.3.23 Petición de identificación de clase de dispositivo (DCI-REQ)

Un CM PUEDE implementar el mensaje DCI-REQ. Un CMTS DEBE implementar el mensaje DCI-REQ.

Cuando está implementado, un CM DEBE transmitir un mensaje DCI-REQ inmediatamente después de la recepción de una indicación completa de alineación procedente del CMTS. Un CM NO DEBE continuar con la inicialización hasta que se reciba el mensaje DCI-RSP procedente del CMTS. En el anexo B.B se da información sobre temporización transcurrida y reintentos.

El mensaje DCI-REQ DEBE tener el formato que se muestra en la figura B.8-42.

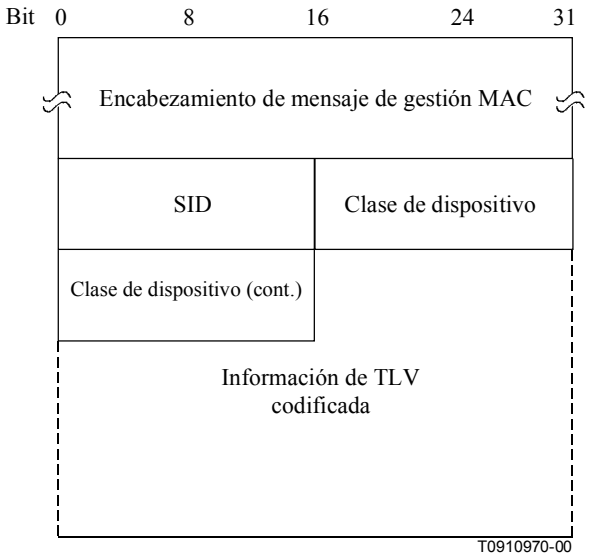


Figura B.8-42/J.112 – Petición de identificación de clase de dispositivo

Los parámetros DEBEN ser como sigue:

SID: El SID temporal asignado durante la alineación.

TLV de clase de dispositivo:

Subtipo	Longitud	Valor	
1	4	bit #0	módem de cable controlado del CPE (CCCM, CPE controlled cable modem)
		bits #1-31	reservados y se deben fijar a cero

Los bits se fijan a 1 para identificar el comportamiento de ese valor.

B.8.3.24 Respuesta de identificación de clase de dispositivo (DCI-RSP)

El CMTS DEBE transmitir un mensaje DCI-RSP en respuesta a la recepción de un mensaje DCI-REQ.

El mensaje DCI-RSP DEBE tener el formato que se muestra en la figura B.8-43.

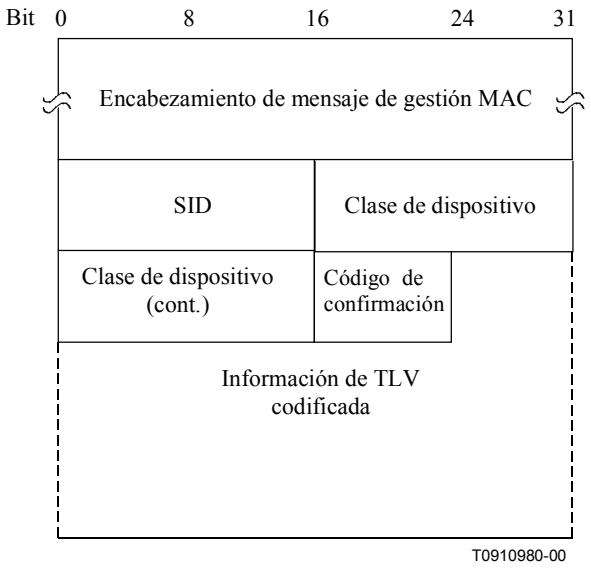


Figura B.8-43/J.112 – Respuesta de identificación de clase de dispositivo

Lo parámetros deben ser como sigue:

SID: El SID recibido en el mensaje DCI-REQ asociado.

TLV de clase de dispositivo: El formato TLV de clase de dispositivo recibido en el mensaje DCI-REQ asociado.

Código de confirmación: (véase B.C.4).

El CMTS DEBE utilizar sólo uno de los tres códigos de confirmación en el mensaje DCI-RSP.

Si la respuesta es rechazo-temporal (3), el CM DEBE reiniciar su contador de reintentos DCI-REQ desde cero y DEBE reenviar el mensaje DCI-REQ y esperar por el mensaje DCI-RSP antes de proceder.

Si la respuesta es rechazo-permanente (4), el CM DEBE abortar este intento de registro y DEBE comenzar la reexploración de un canal diferente en sentido descendente. El CM NO DEBE reintentar este canal hasta que haya intentado con todos los demás canales en sentido descendente de DOCSIS en la red.

Si la respuesta es éxito (0), el CM DEBE continuar con el registro.

El CMTS DEBE retener la información de la clase de dispositivo para su utilización en el proceso DHCP. El CMTS DEBE crear una tupla opción de agente DHCP 82 con la información de clase de dispositivo y DEBE insertar esta tupla en DHCPDISCOVER procedente del CM correspondiente antes de reenviar ese DHCPDISCOVER al servidor DHCP.

B.8.3.25 Mensaje de gestión MAC de inhabilitación de transmisor en sentido ascendente (UP-DIS)

El mensaje UP-DIS DEBE codificarse como sigue:

Encabezamiento de mensaje de gestión MAC

El mensaje UP-DIS se envía desde un CMTS a un CM y no existe una respuesta desde el CM transmitida de vuelta al CMTS.

El CMTS DEBE ser capaz de transmitir el mensaje UP-DIS. Los mecanismos para detectar e informar sobre situaciones en las que podría ser apropiada la transmisión de un mensaje UP-DIS dependen de la implementación. De forma similar, la señalización para activar la transmisión del mensaje UP-DIS queda fuera del alcance de este anexo B.

El CM PUEDE dar soporte al mensaje UP-DIS.

Si soporta el mensaje UP-DIS, el CM DEBE inhabilitar de manera autónoma su transmisor en sentido ascendente al recibir un mensaje UP-DIS independientemente de cualquier otro estado de transacción (véase B.11). Una vez inhabilitado el transmisor mediante el mensaje UP-DIS, el transmisor del CM en sentido ascendente sólo DEBE ser habilitado mediante la aplicación de ciclos de potencia al CM.

Puesto que el mecanismo UP-DIS del CM carece de estados, el CMTS DEBERÍA incorporar mecanismos para rastrear direcciones MAC inhabilitadas y reenviar un mensaje UP-DIS a los módems que disponen de ciclos de potencia e intentar registrarse de nuevo.

B.9 Operación del protocolo de control de acceso a los medios

B.9.1 Atribución de anchura de banda en sentido ascendente

El canal en sentido ascendente se modela como un tren de miniintervalos de tiempo. El CMTS DEBE generar la referencia de tiempo para identificar estos intervalos. También DEBE controlar el acceso a esos intervalos por los módems de cable. Por ejemplo, PUEDE conceder un cierto número de intervalos contiguos a un CM para que transmita una PDU datos. El CM DEBE temporizar su transmisión de tal manera que el CMTS la reciba en la referencia de tiempo especificada. En la presente cláusula se describen los elementos de protocolo utilizados en la petición, concesión y utilización de la anchura de banda en sentido ascendente. El mecanismo básico para la asignación de la gestión de anchura de banda es el MAP de atribución. Véase al respecto la figura B.9-1.

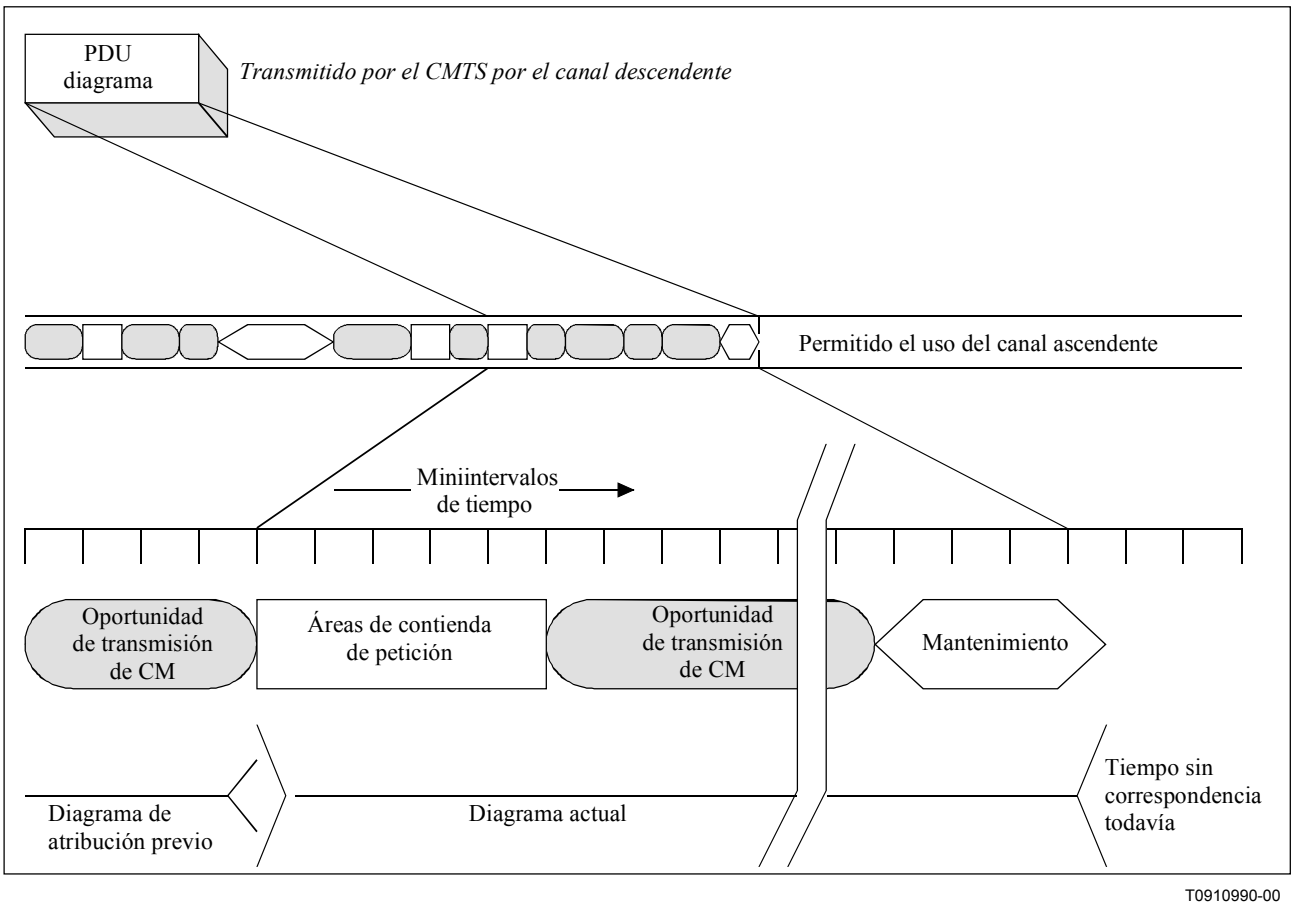


Figura B.9-1/J.112 – Diagrama de atribución

El MAP de atribución es un mensaje de gestión MAC transmitido por el CMTS por el canal en sentido descendente que describe, para algún intervalo, los usos a los que DEBEN aplicarse los miniintervalos de tiempo en sentido ascendente. Un diagrama determinado PUEDE indicar que algunos intervalos son concesiones para que determinadas estaciones transmitan datos por los mismos, otros intervalos están disponibles a efectos de transmisión por contienda, y otros intervalos constituyen una oportunidad para que nuevas estaciones se incorporen al enlace.

Los diferentes vendedores PUEDEN implementar en el CMTS muchos algoritmos de periodicidad diferentes; el presente anexo B no impone ningún algoritmo en concreto. Más bien, describe los elementos de protocolo con los que se pide y concede anchura de banda.

La atribución de la anchura de banda incluye los siguientes elementos básicos:

- Cada CM tiene uno o más identificadores de servicio cortos (SID, de 14 bits) así como una dirección de 48 bits.
- La anchura de banda en sentido ascendente se divide en un tren de miniintervalos de tiempo. Cada miniintervalo de tiempo se numera con respecto a una referencia principal contenida en el CMTS. La información de temporización se distribuye a los CM mediante paquetes SYNC.
- Los CM pueden emitir peticiones al CMTS de anchura de banda en sentido ascendente.

El CMTS DEBE transmitir unidades de datos de protocolo (PDU) diagrama de atribución por el canal en sentido descendente definiendo la utilización permitida de cada miniintervalo de tiempo. El diagrama se describe a continuación.

B.9.1.1 Mensaje de gestión MAC diagrama de atribución

El mapa de atribución es un mensaje de gestión MAC de longitud variable transmitido por el CMTS para definir oportunidades de transmisión por el canal en sentido ascendente. Incluye un encabezamiento de longitud fija seguido de un número variable de elementos de información (IE, *information element*) con el formato que se muestra en B.8.3.4. Cada elemento de información define la utilización permitida para una gama de miniintervalos de tiempo.

Se señala que tanto el CM como el CMTS deben comprender que los bits inferiores (26-M) de los tiempos de comienzo y acuse de recibo de la atribución se DEBEN utilizar como tiempos efectivos de comienzo y acuse de recibo del MAP, estando definido M en B.8.3.3. La relación entre los contadores de tiempo de comienzo/acuse de recibo de atribución y el contador de indicaciones de tiempo se describe con más detalle en B.9.3.4.

B.9.1.2 Elementos de información

Cada IE consta de un ID de servicio de 14 bits, un código de tipo de 4 bits y un desplazamiento de comienzo de 14 bits según se define en B.8.3.4. Puesto que todas las estaciones DEBEN explorar todos los IE, es fundamental que los IE sean cortos y tengan un formato relativamente fijo. Los IE del MAP están en orden estricto de desplazamiento de comienzo. En la mayoría de los casos la duración descrita por el IE se deduce a partir de la diferencia entre el desplazamiento de comienzo de un IE y el del siguiente IE. Por este motivo, un IE nulo DEBE terminar la lista. Véase el cuadro B.8-20.

Se definen cuatro tipos de ID de servicio:

1) 0x3FFF – Radiodifusión, para todas las estaciones.
2) 0x2000-0x3FFE – Multidifusión, objetivo definido administrativamente. Véase el anexo B.A;
3) 0x0001-0x1FFF – Unidifusión, para un CM determinado o un servicio determinado dentro de ese CM.
4) 0x0000 – Dirección nula, no está dirigido a ninguna estación.

Todos los elementos de información que se describen a continuación DEBEN ser soportados por todos los CM conformes. Los CMTS conformes PUEDEN utilizar cualquiera de estos elementos de información al crear diagramas de atribución de anchura de banda.

B.9.1.2.1 IE petición

El IE petición proporciona un intervalo en sentido ascendente en el que se PUEDEN efectuar peticiones de anchura de banda para transmisión de datos en sentido ascendente. El carácter de este IE cambia dependiendo de la clase de ID de servicio. Si se trata de difusión, es una invitación a que los CM contiendan por las peticiones. B.7.4 describe las oportunidades de transmisión por contienda que se pueden utilizar. Si se trata de unidifusión, es una invitación para que un determinado CM pida anchura de banda. Las unidifusiones PUEDEN ser utilizadas como parte de un sistema de planificación de calidad de servicio (véase B.10.2). Los paquetes transmitidos en este intervalo DEBEN utilizar el formato de trama MAC de petición (véase B.8.2.5.3).

En el anexo B.A se define un pequeño número de SID de petición de prioridad. Con ellos es posible limitar la contienda por IE de petición a flujos de servicio de determinada prioridad de tráfico (véase B.C.2.2.5.2).

B.9.1.2.2 IE petición/datos

El IE petición/datos proporciona un intervalo en sentido ascendente en el que se PUEDEN transmitir peticiones de anchura de banda o paquetes de datos cortos. Este IE se distingue del IE petición en que:

- Proporciona una manera de acuerdo con la cual los algoritmos de atribución PUEDEN facilitar la contienda por los datos "inmediatos" con cargas ligeras, y una manera según la cual esta oportunidad se puede retirar a medida que aumenta la carga de la red.
- Los ID de servicio de multidifusión se DEBEN utilizar para especificar la longitud máxima de los datos así como los puntos de comienzo aleatorio permitidos dentro del intervalo. Por ejemplo, un ID de multidifusión determinado puede especificar un máximo de paquetes de datos de 64 octetos, con oportunidades de transmisión cada cuarto intervalo.

En el anexo B.A se define un reducido número de ID de servicio de multidifusión conocidos. Se dispone de otros para los algoritmos específicos de los vendedores.

Puesto que los paquetes de datos transmitidos dentro de este intervalo pueden colisionar, el CMTS DEBE acusar recibo de cualquiera que se reciba de manera satisfactoria. El paquete de datos DEBE indicar en el encabezamiento MAC que se desea un acuse de recibo de datos (véase el cuadro B.8-13).

B.9.1.2.3 IE mantenimiento inicial

El IE mantenimiento inicial proporciona un intervalo en el que nuevas estaciones se pueden incorporar a la red. DEBE proporcionarse un intervalo largo, equivalente al retardo máximo de propagación de ida y retorno más el tiempo de transmisión del mensaje petición de alineación (RNG-REQ) (véase B.9.3.3), para permitir que nuevas estaciones efectúen la alineación inicial. Los paquetes transmitidos en este intervalo DEBEN utilizar el formato de mensaje de gestión MAC RNG-REQ (véase B.8.3.5).

B.9.1.2.4 IE mantenimiento de estación

El IE mantenimiento de estación proporciona un intervalo en el que se prevé que las estaciones efectúen algunas de las rutinas del mantenimiento de red, por ejemplo, la alineación o el ajuste de potencia. El CMTS PUEDE pedir que un CM particular efectúe alguna tarea relacionada con el mantenimiento de la red, tal como el ajuste periódico de la potencia de transmisión. En este caso, se unidifunde el IE mantenimiento de estación para proporcionar anchura de banda en sentido ascendente en la que llevar a cabo esa tarea. Los paquetes transmitidos en este intervalo DEBEN utilizar el formato de mensaje de gestión MAC RNG-REQ (véase B.8.3.5).

B.9.1.2.5 IE concesión de datos corta y larga

Los IE de concesión de datos corta y larga proporcionan una oportunidad para que un CM transmita una o más PDU en sentido ascendente. Estos IE se emiten en respuesta a una petición procedente de una estación, o a causa de una disposición administrativa por la que se atribuye cierta cantidad de anchura de banda a una estación determinada (véase más adelante el análisis de la clase de servicio). Estos IE se PUEDEN utilizar también con una longitud deducida de cero miniintervalos de tiempo (una concesión de longitud cero), para indicar que se ha recibido una petición y que está pendiente (una concesión de datos pendientes).

Las concesiones de datos cortas se utilizan con intervalos inferiores o iguales al tamaño máximo de una ráfaga para la utilización especificada en el descriptor de canal en sentido ascendente. Si en el UCD se definen perfiles de ráfagas de datos cortas, todas las concesiones de datos largas DEBEN ser para un número de miniintervalos de tiempo mayor que el máximo para datos cortos. La distinción entre concesiones de datos largas y cortas se puede aprovechar en la codificación de la corrección de errores directa de la capa física; de no ser así, no interesa en el proceso de atribución de anchura de banda.

Si este IE es una concesión de datos pendiente (una concesión de longitud cero), DEBE seguir al IE nulo. De esta manera, los módems de cable pueden procesar primero todas las atribuciones de intervalo efectivas, antes de explorar el diagrama en busca de concesiones de datos pendientes y acuses de recibo de datos.

B.9.1.2.6 IE acuse de recibo de datos

El IE de acuse de recibo de datos acusa la recepción de una PDU datos. El CM DEBE haber pedido este acuse de recibo dentro de la PDU datos (tal será normalmente el caso con las PDU transmitidas dentro de un intervalo de contienda para detectar colisiones).

Este IE DEBE seguir al IE nulo. De esta manera, los módems de cable pueden procesar primero todas las atribuciones de intervalo efectivas, antes de explorar el diagrama en busca de concesiones de datos pendientes y acuses de recibo de datos.

B.9.1.2.7 IE expansión

El IE expansión permite la ampliación, si se necesitan más de 16 puntos de código o 32 bits para IE futuros.

B.9.1.2.8 IE nulo

Un IE nulo termina todas las atribuciones efectivas de la lista de IE. Se utiliza para deducir la longitud del último intervalo. Todos los IE acuse de recibo de datos y todos los IE de concesión de datos pendiente (concesiones de datos de longitud deducida 0) deben seguir al IE nulo.

B.9.1.3 Peticiones

El tema de las peticiones se refiere al mecanismo utilizado por los CM para indicar a los CMTS que necesitan atribución de anchura de banda en sentido ascendente. Una petición PUEDE venir como una transmisión autónoma de trama de petición (véase B.8.2.5.3) o PUEDE venir como petición de porteo en el EHDR de otra transmisión de trama (véase B.8.2.6).

La trama de petición PUEDE ser transmitida durante cualquiera de los intervalos siguientes:

- IE petición;
- IE petición/datos;
- IE concesión datos corta;
- IE concesión de datos larga.

Una petición de porteo PUEDE estar contenida en los siguientes encabezamientos ampliados (EH, *extended header*):

- elemento EH de petición;
- elemento EH de privacidad en sentido ascendente;
- elemento EH de privacidad en sentido ascendente con fragmentación.

La petición DEBE incluir:

- el ID de servicio que efectúa la petición;
- el número de miniintervalos de tiempo pedidos.

El número de miniintervalos de tiempo pedidos DEBE ser el número total que desea el CM en el momento de la petición (incluida cualquier tara de capa física), sujeto a los límites UCD (véase la nota 1) y administrativos (véase la nota 2). El CM DEBE pedir un número de miniintervalos de tiempo correspondiente a una trama completa (véase la nota 3), a excepción del caso de la fragmentación en modo porteo (véase B.10.3.2.2).

La tara de capa física que se DEBE tener en cuenta en una petición incluye la banda de guarda, el preámbulo y la FEC, que dependerán del perfil de ráfaga.

NOTA 1 – El CM está limitado por el tamaño máximo de una ráfaga para el código de utilización de intervalo (IUC) de una concesión de datos larga en el UCD.

NOTA 2 – El CM está limitado por el tamaño máximo de ráfaga concatenada para el flujo de servicio (véase B.C.2.2.6.1).

NOTA 3 – Una trama es una trama MAC única o una trama MAC concatenada.

El CM DEBE tener una sola petición pendiente por vez para cada ID de servicio. Si el CMTS no responde inmediatamente con una concesión de datos, el CM puede determinar sin lugar a ambigüedad que su petición sigue pendiente porque el CMTS DEBE seguir emitiendo una concesión de datos pendiente en cada MAP mientras no sea satisfecha una petición.

En los MAP, los CMTS NO DEBEN realizar una concesión de datos superior a 255 miniintervalos de tiempo a ningún ID de servicio asignada. Así se pone un límite máximo al tamaño de concesión que el CM debe admitir.

B.9.1.4 Resumen de la utilización de las características de los elementos de información

En el cuadro B.9-1 se resumen los tipos de trama que puede transmitir el CM utilizando cada uno de los tipos de IE MAP que representan oportunidades de transmisión. Cuando en el cuadro se dice "DEBE" ello significa que, si procede, una implementación del CM conforme deberá poder transmitir ese tipo de trama en ese tipo de oportunidad. Cuando en el cuadro se dice "PUEDE" ello significa que una implementación del CM conforme no necesariamente deberá poder transmitir ese tipo de trama en ese tipo de oportunidad, pero que es legal que lo haga si procede. Cuando en la tabla se dice "NO DEBE", ello significa que una implementación del CM conforme jamás transmitirá ese tipo de trama en ese tipo de oportunidad.

Cuadro B.9-1/J.112 – Resumen de compatibilidad de características de IE

Elemento de información	Transmisión de trama de petición	Transmisión de trama MAC concatenada	Transmisión de trama MAC fragmentada	Transmisión de RNG-REQ	Transmisión de cualquier otra trama MAC
IE petición	DEBE	NO DEBE	NO DEBE	NO DEBE	NO DEBE
IE petición/datos	DEBE	PUEDE	NO DEBE	NO DEBE	PUEDE
IE mantenimiento inicial	NO DEBE	NO DEBE	NO DEBE	DEBE	NO DEBE
IE mantenimiento de estación	NO DEBE	NO DEBE	NO DEBE	DEBE	NO DEBE
IE concesión datos corta	PUEDE	DEBE	DEBE	NO DEBE	DEBE
IE concesión de datos larga	PUEDE	DEBE	DEBE	NO DEBE	DEBE

B.9.1.5 Transmisión del diagrama y temporización

El diagrama de atribución DEBE ser transmitido puntualmente para que se propague a través del cable físico y sea recibido y tratado por los CM receptores. En tal sentido, PUEDE ser transmitido bastante antes de su momento efectivo. Los componentes del retardo son:

- El retardo de propagación de ida y retorno en el caso más desfavorable – Puede ser específico de la red, pero del orden de cientos de microsegundos.
- Los retardos de espera en cola dentro del CMTS – Son específicos de la implementación.
- Los retardos de procesamiento dentro de los CM – Se DEBE permitir un tiempo mínimo de procesamiento por cada CM según lo especificado en el anexo B.B (tiempo de procesamiento de MAP del CM).
- La intercalación de la FEC de la capa PMD.

Con estas limitaciones, los vendedores pueden optar por minimizar el retardo de modo que sea mínima la latencia de acceso al canal en sentido ascendente.

El número de miniintervalos de tiempo descritos PUEDE variar de un diagrama a otro. Un diagrama PUEDE describir, como mínimo, un solo miniintervalo de tiempo. Esto significaría desaprovechar tanto la anchura de banda en sentido descendente como el tiempo de procesamiento dentro de los CM. Un diagrama PUEDE abarcar, como máximo, decenas de milisegundos. Un MAP generaría así una latencia en sentido ascendente más bien pobre. Los algoritmos de atribución PUEDEN variar el tamaño de los diagramas a lo largo del tiempo para conseguir un equilibrio entre utilización de la red y latencia en condiciones de carga de tráfico variable.

Un diagrama DEBE contener, como mínimo, dos elementos de información: uno para describir un intervalo y otro, un IE nulo, para terminar la lista. Un diagrama DEBE tener un contorno límite de, como máximo, 240 elementos de información. Los diagramas también están limitados en el sentido de que NO DEBEN describir más de 4096 miniintervalos de tiempo en el futuro. Esta última constricción tiene por objeto limitar el número de miniintervalos futuros cuyo seguimiento ha de efectuar cada uno de los CM. Un CM DEBE ser capaz de soportar múltiples diagramas de atribución pendientes. Incluso aunque varios MAP puedan estar pendientes, la suma del número de miniintervalos de tiempo que describen NO DEBE exceder de 4096.

Todos los diagramas juntos DEBEN describir cada uno de los miniintervalos de tiempo del canal en sentido ascendente. Si un CM no recibe el MAP que describe un determinado intervalo, NO DEBE transmitir durante ese intervalo.

B.9.1.6 Ejemplo de protocolo

Esta cláusula ilustra el intercambio entre el CM y el CMTS cuando el CM tiene datos para transmitir (figura B.9-2). Supóngase un CM dado que tiene una PDU datos disponible para transmisión.

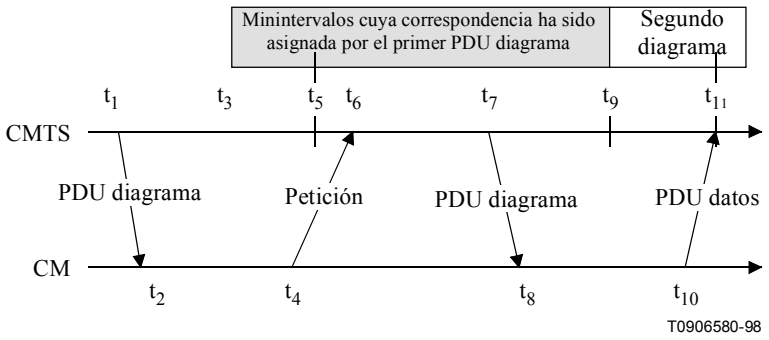


Figura B.9-2/J.112 – Ejemplo de protocolo

Descripción

1) En el instante t_1, el CMTS transmite un MAP cuyo momento de comienzo efectivo es t_3. Dentro de este MAP existe un IE petición que comenzará en t_5. La diferencia entre t_1 y t_3 se necesita en previsión del:
   - retardo de propagación en sentido descendente (incluyendo la intercalación de la FEC) para hacer posible que todos los CM reciban el diagrama de atribución;
   - tiempo de procesamiento en el CM (lo que permite que los CM analicen el MAP y lo conviertan en oportunidades de transmisión);
   - retardo de propagación en sentido ascendente (para que la transmisión de los primeros datos en sentido ascendente por parte de los CM comience puntualmente de modo que lleguen al CMTS en el instante t_3).

2) En el instante t_2, el CM recibe este MAP y lo explora buscando oportunidades de petición. Para minimizar las colisiones entre peticiones, calcula t_6 como un desplazamiento aleatorio en base al valor de comienzo de retroceso de datos del MAP más reciente (véase B.9.4 así como las definiciones SID de multidifusión de B.A.2).

3) En el instante t_4, el CM transmite una petición de tantos miniintervalos de tiempo como se necesiten para acomodar la PDU. El momento t_4 se elige en base al desplazamiento de alineación (véase B.9.3.3) de manera que la petición llegue al CMTS en el momento t_6.

4) En el instante t_6, el CMTS recibe la petición y la diagrama para dar servicio en el MAP siguiente. (La elección de las peticiones que se conceden dependerá de la clase de servicio solicitada, de las peticiones en contienda y del algoritmo utilizado por el CMTS.)

5) En el instante t_7, el CMTS transmite un MAP cuyo momento de comienzo efectivo es t_9. Dentro de este MAP comenzará, en t_{11}, una concesión de datos para el CM.

6) En el instante t_8, el CM recibe el MAP y lo explora buscando sus concesiones de datos.

7) En el instante t_{10}, el CM transmite su PDU datos de manera que llegue al CMTS en el intante t_{11}. El instante t_{10} se calcula a partir del desplazamiento de alineación, como en el paso 3).

Los pasos 1) y 2) no necesariamente contribuyen a la latencia de acceso si los CM mantienen de manera rutinaria una lista de oportunidades de petición.

En el paso 3), la petición puede colisionar con peticiones de otros CM, y perderse. El CMTS no detecta directamente la colisión. El CM determina que se ha producido una colisión (u otro fallo de recepción) cuando el siguiente MAP no incluye acuse de recibo de la petición. El CM DEBE efectuar entonces un algoritmo de retroceso e intentarlo de nuevo (véase B.9.4.1).

En el paso 4), el planificador del CMTS PUEDE no acomodar la petición dentro del MAP siguiente. Si tal cosa ocurre, DEBE replicar con una concesión de longitud cero en ese MAP o descartar la petición no haciendo ninguna concesión. DEBE seguir notificando esta concesión de longitud cero en todos los diagramas sucesivos hasta que la petición pueda ser concedida o sea descartada. Esto DEBE señalar al CM que la petición está todavía pendiente. Mientras el CM siga recibiendo una concesión de longitud cero, NO DEBE emitir peticiones nuevas para esa cola de servicio.

B.9.2 Soporte de múltiples canales

Los vendedores pueden optar por ofrecer diversas combinaciones de canales en sentido ascendente y descendente dentro de un punto de acceso al servicio MAC. El protocolo de atribución de anchura de banda en sentido ascendente permite que se gestionen múltiples canales en sentido ascendente por medio de uno o muchos canales en sentido descendente.

Si múltiples canales en sentido ascendente están asociados con un solo canal en sentido descendente, el CMTS DEBE enviar un diagrama de atribución por cada canal en sentido ascendente. El identificador de canal del MAP, junto con el mensaje descriptor de canal en sentido ascendente (véase B.8.3.3), DEBEN especificar a qué canal corresponde cada MAP. No existe requisito de que los diagramas se sincronicen en todos los canales. El anexo B.H proporciona un ejemplo.

Si múltiples canales en sentido descendente están asociados con un solo canal en sentido ascendente, el CMTS DEBE asegurar que el diagrama de atribución llega a todos los CM. Es decir, si algunos CM están conectados a un determinado canal en sentido descendente, el MAP DEBE ser transmitido por ese canal. Para ello, puede ser necesario transmitir múltiples copias del mismo MAP. El tiempo de comienzo de atribución en el encabezamiento del MAP DEBE remitir siempre a la referencia de SYNC en el canal en sentido descendente por el que se transmite.

Si múltiples canales en sentido descendente están asociados a múltiples canales en sentido ascendente, el CMTS puede necesitar transmitir múltiples copias de múltiples diagramas para garantizar tanto que se establece la correspondencia de todos los canales en sentido ascendente como que todos los CM reciben los diagramas que necesitan.

B.9.3 Temporización y sincronización

Uno de los mayores retos al diseñar un protocolo MAC para una red de cable consiste en compensar los grandes retardos que se producen. Dichos retardos son superiores en un orden de magnitud al de la duración de las ráfagas de transmisión en sentido ascendente. Para compensar esos retardos, el módem de cable DEBE ser capaz de temporizar sus transmisiones de manera precisa de modo que lleguen al CMTS al comienzo del miniintervalo de tiempo asignado.

A tal fin, se necesitan dos elementos de información por cada módem de cable, a saber:

- una referencia de temporización global enviada en sentido descendente desde el CMTS a todos los módems de cable;
- un desplazamiento de temporización, calculado durante un proceso de alineación, para cada módem de cable.

B.9.3.1 Referencia de temporización global

El CMTS DEBE crear una referencia de temporización global transmitiendo el mensaje de gestión MAC sincronización de tiempo (SYNC) en sentido descendente con una frecuencia nominal. El mensaje contiene una indicación de tiempo que identifica exactamente cuándo ha transmitido el CMTS el mensaje. Los módems de cable DEBEN comparar a continuación la hora en que realmente se recibió el mensaje con la indicación de tiempo y ajustar en consecuencia sus referencias de reloj local.

La subcapa de convergencia de transmisión DEBE funcionar en estrecha relación con la subcapa MAC para proporcionar una indicación de tiempo exacta al mensaje SYNC. Como se indica en B.9.3.3 relativa a la alineación, el modelo supone que los retardos de temporización a través del resto de la capa PHY DEBEN ser relativamente constantes. Cualquier variación de los retardos de la PHY DEBE ser tenida en cuenta en el tiempo de guarda de la tara de la PHY.

Se pretende que el intervalo nominal entre mensajes SYNC sea del orden de unas decenas de milisegundos. Esto impone una tara muy reducida en sentido descendente al tiempo que permite a los módems de cable adquirir rápidamente su sincronización de temporización global.

B.9.3.2 Adquisición de canal CM

Un módem de cable cualquiera NO DEBE utilizar el canal en sentido ascendente hasta que se haya sincronizado de manera satisfactoria en sentido descendente.

En primer lugar, el módem de cable DEBE establecer la sincronización de la subcapa PMD. Para ello es preciso que se haya enganchado en la frecuencia adecuada, que haya ecualizado el canal en sentido descendente, que haya recuperado cualquier alineación de trama de subcapa PMD y que la FEC sea operativa (véase B.11.2.2). En este punto, un tren de bits válido está siendo enviado a la subcapa de convergencia de transmisión. La subcapa de convergencia de transmisión efectúa su propia sincronización (véase B.7). Al detectar el PID de DOCSIS conocido, junto con un indicador de comienzo de unidad de cabida útil según [UIT-T H.222.0], entrega la trama MAC a la subcapa MAC.

La subcapa MAC DEBE buscar ahora los mensajes de gestión MAC sincronización de temporización (SYNC). El módem de cable alcanza la sincronización MAC una vez que ha recibido por lo menos dos mensajes SYNC y ha verificado que las tolerancias de su reloj se encuentren dentro de los límites especificados.

Un módem de cable permanece en "SYNC" mientras siga recibiendo de manera satisfactoria los mensajes SYNC. Si el intervalo SYNC perdida (véase el anexo B.B) transcurre sin un mensaje SYNC válido, el módem de cable NO DEBE utilizar el sentido ascendente y DEBE intentar restablecer la sincronización de nuevo.

B.9.3.3 Alineación

La alineación es el proceso de adquisición del desplazamiento de temporización correcto de tal manera que las transmisiones del módem del cable estén alineadas con el límite adecuado de miniintervalo de tiempo. Los retardos de temporización a través de la capa PHY DEBEN ser relativamente constantes. Cualquier variación de los retardos de la PHY DEBE ser tenida en cuenta en el tiempo de guarda de la tara PMD en sentido ascendente.

En primer lugar, un módem de cable DEBE sincronizarse con el canal en sentido descendente y aprender las características de canal en sentido ascendente mediante el mensaje de gestión MAC descriptor de canal en sentido ascendente. En este punto, el módem de cable DEBE explorar el mensaje MAP atribución de anchura de banda para encontrar una región de mantenimiento inicial. (Véase B.9.1.2.4.) El CMTS DEBE establecer una región de mantenimiento inicial suficientemente grande para tener en cuenta la variación de los retardos entre dos CM cualesquiera.

El módem de cable DEBE elaborar un mensaje petición de alineación para ser enviado en una región mantenimiento inicial. El campo SID DEBE fijarse al valor de CM no inicializado (cero).

Mediante el proceso de alineación se ajusta el desplazamiento de temporización de cada CM de modo que aparezca justo al lado del CMTS. El CM DEBE fijar su desplazamiento de temporización inicial en el valor del retardo fijo interno que equivale a poner este CM junto al CMTS. Dicho valor incluye los retardos introducidos por una implementación particular, y DEBE incluir la latencia de intercalación de la capa PHY en sentido descendente.

Cuando se produce la oportunidad de transmisión de mantenimiento inicial, el módem de cable DEBE enviar el mensaje petición de alineación. Así pues, el módem de cable envía el mensaje como si estuviese físicamente junto al CMTS.

Una vez que el CMTS ha recibido de manera satisfactoria el mensaje petición de alineación, DEBE devolver un mensaje respuesta de alineación dirigido al módem de cable de que se trate. Dentro del mensaje respuesta de alineación DEBE haber un SID asignado temporalmente a ese módem de cable hasta que haya completado el proceso de registro. El mensaje DEBE también contener información sobre ajuste del nivel de potencia de RF y ajuste de frecuencia de desplazamiento así como cualesquiera correcciones del desplazamiento de la temporización.

El módem de cable DEBE esperar ahora por una región de mantenimiento de estación individual asignada a su SID temporal. DEBE transmitir un mensaje petición de alineación en este momento utilizando el SID temporal junto con cualquier corrección del nivel de potencia y del desplazamiento de la temporización.

El CMTS DEBE devolver otro mensaje respuesta de alineación al módem del cable con cualquier ajuste fino de sintonización que se requiera. Los pasos de petición/respuesta de alineación DEBEN repetirse hasta que la respuesta contenga una notificación de alineación satisfactoria; de lo contrario, el CMTS interrumpirá la alineación. Una vez realizada con éxito la alineación, el módem del cable DEBE unirse al tráfico de datos normal en sentido ascendente. Véanse, en B.9, todos los detalles de la secuencia completa de inicialización. En B.11.2.4 se definen, en particular, las máquinas de estados y la aplicabilidad de los conteos de reintentos y los valores de temporizador para el proceso de alineación.

NOTA – El tipo de ráfaga que se ha de utilizar para cualquier transmisión viene definido por el código de utilización de intervalo (IUC). Cada IUC se hace corresponder con un tipo de ráfaga en el mensaje UCD.

B.9.3.4 Unidades de temporización y relaciones

El mensaje SYNC lleva una referencia de tiempo que se mide en tics de 6,25 ms. En el mensaje SYNC está presente además una resolución adicional de 6,25/64 ms para que el CM pueda efectuar el seguimiento del reloj del CMTS con un pequeño desplazamiento de fase. Estas unidades se eligieron como máximo común divisor de la duración de un miniintervalo en sentido ascendente en diversas modulaciones y velocidades de símbolos. Dado que esto se desliga de las características particulares de los canales en sentido ascendente, se puede utilizar una referencia de tiempo SYNC única para todos los canales en sentido ascendente asociados al canal en sentido descendente.

El MAP de atribución de anchura de banda utiliza unidades de tiempo de "miniintervalos de tiempo". Un miniintervalo de tiempo representa el tiempo en octetos que se necesita para transmitir un número fijo de octetos. Se calcula que el miniintervalo de tiempo representa el tiempo de 16 octetos, aunque podrían elegirse otros valores. El tamaño del miniintervalo de tiempo, expresado como un múltiplo de la referencia de tiempo SYNC, se lleva en el descriptor de canal en sentido ascendente. El ejemplo del cuadro B.9-2 relaciona miniintervalos de tiempo con tics de tiempo de SYNC.

Cuadro B.9-2/J.112 – Ejemplo de relación entre miniintervalos de tiempo y tics de tiempo

Parámetro	Ejemplo de valor
Tics de tiempo	6,25 ms
Octetos por miniintervalo de tiempo	16 (nominal, cuando se utiliza modulación QPSK)
Símbolos/octeto	4 (suponiendo QPSK)
Símbolos/segundo	2 560 000
Miniintervalos/segundo	40 000
Microsegundos/miniintervalo	25
Tics/miniintervalo	4

Se señala que la relación símbolos/octeto es una característica de una transmisión de ráfaga individual, no del canal. Un miniintervalo de tiempo podría representar, en este ejemplar, 16 ó 32 octetos, dependiendo de la modulación que se elija.

El "miniintervalo de tiempo" es la unidad de granularidad de las oportunidades de transmisión en sentido ascendente. Ello no significa que cualquier PDU pueda realmente ser transmitida en un solo miniintervalo de tiempo.

El MAP computa los miniintervalos de tiempo en un contador de 32 bits que cuenta hasta $(2^{32} - 1)$ y que a continuación retorna a cero. Los bits menos significativos (esto es, los bits 0 a 25 – M) del contador de miniintervalos de tiempo DEBEN concordar con los bits más significativos (esto es, desde el bit 6 + M al bit 31) del contador de indicaciones de tiempo SYNC. Es decir, el miniintervalo de tiempo N empieza en la referencia de indicación de tiempo $(N \times T \times 64)$, siendo $T = 2^M$ el multiplicador del UCD que define el miniintervalo de tiempo (esto es, el número de tics por miniintervalo de tiempo).

Los bits superiores no utilizados del contador de miniintervalos de tiempo de 32 bits (esto es, los bits 26 – M a 31) no los necesita el CM y PUEDEN ser ignorados.

NOTA – La restricción de que el multiplicador del UCD sea una potencia de dos tiene como consecuencia que el número de octetos por miniintervalo de tiempo deba también ser una potencia de dos.

B.9.4 Transmisión en sentido ascendente y resolución de contiendas

El CMTS controla las asignaciones en el canal en sentido ascendente a través del MAP y determina qué miniintervalos de tiempo son objeto de colisiones. El CMTS PUEDE permitir las colisiones en peticiones o en PDU datos.

En esta cláusula se presenta una visión general de la transmisión ascendente y la resolución de contiendas. Para simplificar se refiere a las decisiones tomadas por un CM; pero esto no es más que una herramienta pedagógica. Como un CM puede tener múltiples flujos de servicio ascendentes (cada uno con su propio SID), toma estas decisiones ya sea para cada cola de servicio o para cada SID. Véase en el anexo B.K un diagrama de transición de estados y más detalles.

B.9.4.1 Visión general de la resolución de contiendas

El método obligatorio de resolución de contiendas que DEBE ser soportado se basa en un retroceso exponencial binario truncado, con la ventana de retroceso inicial y la ventana de retroceso máxima controladas por el CMTS. Los valores se especifican como parte del mensaje MAC de atribución de anchura de banda (MAP) y representan un valor potencia de 2. Por ejemplo, un valor de 4 indica un ventana entre 0 y 15; un valor de 10 indica una ventana entre 0 y 1 023.

Cuando un CM tiene información para enviar y desea pasar al proceso de resolución de contiendas, pone su ventana de retroceso interna igual al principio del retroceso de datos definido en el MAP en vigor en ese momento.

NOTA 1 – El MAP en vigor en este momento es, de hecho, el MAP cuyo comienzo efectivo de atribución ya se ha producido pero que incluye IE que no se han producido.

El CM DEBE seleccionar de manera aleatoria un número dentro de su ventana de retroceso. Este valor aleatorio indica el número de oportunidades de transmisión por contienda que el CM DEBE diferir antes de proceder a la transmisión. Un CM DEBE considerar solamente aquellas oportunidades de transmisión por contienda para las que esta transmisión habría sido aceptable. Están definidas en el MAP por elementos de información (IE) petición o petición/datos.

NOTA 2 – Cada IE puede representar múltiples oportunidades de transmisión.

A título de ejemplo, considérese un CM cuya ventana de retroceso inicial es de 0 a 15 y que selecciona de manera aleatoria el número 11. El CM tiene que diferir un total de 11 oportunidades de transmisión por contienda. Si el primer IE petición disponible es para seis peticiones, el CM no utiliza la primera y tiene cinco oportunidades más para diferir. Si el siguiente IE petición es para dos peticiones, el CM tiene tres más para diferir. Si el tercer IE petición es para ocho peticiones, el CM transmite en la cuarta petición, después de diferir durante tres oportunidades más.

Después de una transmisión por contienda, el CM espera una concesión de datos (concesión de datos pendiente) o un acuse de recibo de datos en un MAP subsiguiente. Cuando recibe una u otra cosa, queda completa la resolución de la contienda. El CM determina que se perdió la transmisión por contienda cuando encuentra un MAP sin una concesión de datos (concesión de datos pendientes) o un acuse de recibo de datos dirigido a él con una hora de acuse de recibo más reciente que la de transmisión (véase la nota 3). El CM DEBE incrementar entonces su ventana de retroceso por un factor de dos, siempre que sea inferior a la ventana de retroceso máxima. El CM DEBE seleccionar de manera aleatoria un número dentro de su nueva ventana de retroceso y repetir el proceso de diferimiento descrito más arriba.

NOTA 3 – Los IE de acuse de recibo de datos tienen por objeto sólo la detección de colisiones y no están diseñados para proporcionar un transporte confiable (responsabilidad que cabe a capas superiores). Si se pierde un MAP o resulta dañado, un CM que esté esperando un acuse de recibo de datos DEBE suponer que su transmisión de datos por contienda fue exitosa y NO DEBE retransmitir el paquete de datos. Esto impide que el CM envíe innecesariamente paquetes de datos duplicados.

Este proceso de intentos sucesivos continúa hasta que se alcanza el número máximo de reintentos (16), en cuyo momento la PDU DEBE ser descartada.

NOTA 4 – El número máximo de reintentos es independiente de las ventanas de retroceso inicial y máxima definidas por el CMTS.

Si el CM recibe una petición de unidifusión o una concesión de datos en cualquier momento mientras está procediendo a diferir para este SID, DEBE detener el proceso de resolución de contiendas y utilizar la oportunidad de transmisión explícita.

El CMTS dispone de un alto grado de flexibilidad para controlar la resolución de contiendas. Por un lado, el CMTS puede optar por establecer el principio y el fin de retroceso de datos para emular un retroceso de estilo Ethernet con la simplicidad y el carácter distribuido que le son inherentes, pero también con sus características de equidad y eficacia. Esto se haría fijando principio de retroceso de datos = 0 y fin = 10 en el MAP. Por otra parte, el CMTS puede hacer que el principio y el fin del retroceso de datos sean idénticos y actualizar a menudo estos valores en el MAP, de manera tal que todos los módems de cable utilicen la misma, y es de esperar que óptima, ventana de retroceso.

B.9.4.2 Oportunidades de transmisión

Una oportunidad de transmisión se define como un miniintervalo de tiempo cualquiera en el que se puede permitir a un CM que comience una transmisión. Las oportunidades de transmisión se aplican normalmente a las oportunidades por contienda y se utilizan para calcular el grado de diferimiento apropiado en el proceso de resolución de contiendas.

El número de oportunidades de transmisión asociadas con un IE particular en una MAP depende del tamaño total de la región así como del tamaño permisible de una transmisión determinada. Supóngase, por ejemplo, que un IE petición define una región de 12 miniintervalos de tiempo. Si el UCD define un tamaño de ráfaga REQ que encaja en un solo miniintervalo de tiempo, hay 12 oportunidades de transmisión asociadas con este IE REQ, es decir, una por cada miniintervalo de tiempo. Si el UCD define un REQ que encaja en dos miniintervalos de tiempo, hay seis oportunidades de transmisión y puede empezar un REQ en miniintervalos alternos.

Supóngase, como segundo ejemplo, un IE petición/datos que define una región de 24 miniintervalos de tiempo. Si se envía con un SID de 0x3FF4 (véase el anexo B.A), el CM puede (eventualmente) comenzar una transmisión cada cuatro miniintervalos de tiempo; este IE contiene por tanto un total de seis oportunidades de transmisión (TX OP, *transmit opportunities*). De manera similar, un SID de 0x3FF6 implica cuatro oportunidades de transmisión; 0x3FF8 implica tres oportunidades de transmisión; y 0x3FFC implica dos oportunidades de transmisión.

Para un IE mantenimiento inicial, el CM DEBE empezar su transmisión en el primer miniintervalo de tiempo de la región, es decir, sólo tiene una oportunidad de transmisión. El resto de la región se utiliza para compensar los tiempos de propagación de ida y retorno ya que el CM todavía no ha sido alineado.

Los IE mantenimiento de estación, concesión de datos corta, concesión de datos larga y petición de unidifusión se envían por unidifusión por lo que no están normalmente asociados a oportunidades de transmisión por contienda. Representan una oportunidad de transmisión única especializada, o basada en reserva.

En resumen, véase el cuadro B.9-3.

Cuadro B.9-3/J.112 – Oportunidad de transmisión

Intervalo	Tipo de SID	Oportunidad de transmisión
Petición	Difusión	Número de miniintervalos de tiempo necesarios para una petición
Petición	Multidifusión	Número de miniintervalos de tiempo necesarios para una petición
Petición/datos	Difusión	No permitida
Petición/datos	Multidifusión conocida	Según definición de SID en el anexo B.A
Petición/datos	Multidifusión	Algoritmos específicos del vendedor
Mantenimiento inicial	Radiodifusión	Todo el intervalo es una sola oportunidad de transmisión

B.9.4.3 Utilización de la anchura de banda del CM

Las reglas que siguen rigen la respuesta que da un CM cuando procesa diagramas:

NOTA – Estos comportamientos normalizados pueden ser anulados por la política de petición/transmisión del CM (véase B.C.2.2.6.3).

1) Un CM DEBE utilizar primero cualquier concesión que se le haya asignado. A continuación, DEBE utilizar cualquier indicador de petición (REQ) de unidifusión dirigida a él. Por último, el CM DEBE utilizar el indicador de petición de radiodifusión/multidifusión siguiente que esté disponible, o los IE petición/datos, para los que es adecuado.
2) Un CM NO DEBE tener más que una petición pendiente en cualquier momento para un determinado ID de servicio.
3) Si un CM tiene una petición pendiente, NO DEBE utilizar los intervalos de contienda intermedios para ese ID de servicio.

B.9.5 Soporte de criptación de enlace de datos

Los procedimientos de soporte de la criptación de un enlace de datos se definen en [DOCSIS8]. La interacción entre la capa MAC y el sistema de seguridad se limita a los elementos que se definen más adelante.

B.9.5.1 Mensajes MAC

Los mensajes de gestión MAC (véase B.8.3) NO DEBEN ser criptados.

NOTA – A excepción de ciertos casos en los cuales esa trama está incluida en una ráfaga concatenada fragmentada en el canal en sentido ascendente. (Véase B.8.2.7.1.)

B.9.5.2 Alineación de trama

Cuando se aplica criptación a una PDU datos, se DEBEN seguir las reglas que se indican a continuación:

- El elemento EH de privacidad de [DOCSIS8] DEBE estar en el encabezamiento ampliado y DEBE ser el primer elemento EH del campo encabezamiento ampliado (EHDR).
- Los datos criptados se llevan transparentemente como PDU datos al MAC de cable.

B.10 Calidad de servicio y fragmentación

Este anexo B presenta varios conceptos nuevos relacionados con calidad de servicio (QoS, *quality of service*) que no están en [DOCSIS9]. Son los siguientes:

- clasificación de paquetes e identificación de flujo;
- planificación de la QoS de flujo de servicio;

- establecimiento de servicio dinámico;
- fragmentación;
- modelo de activación de dos fases.

B.10.1 Teoría del funcionamiento

Los distintos mecanismos del protocolo DOCSIS que se describen en el presente anexo B se pueden usar para el soporte de la calidad de servicio (QoS) tanto de tráfico ascendente como descendente por el CM y el CMTS. En la presente cláusula se presenta una visión general de los mecanismos de protocolo de QoS y el papel que desempeñan en la QoS de extremo a extremo.

Los requisitos de calidad de servicio incluyen:

- una función de configuración y registro para la configuración previa de **flujos de servicio** de QoS basados en CM y parámetros de tráfico;
- una función de señalización para establecer dinámicamente flujos de servicio habilitados para QoS y parámetros de tráfico;
- una función de conformación del tráfico y de control del tráfico para la gestión del tráfico basada en flujo de servicio, que se aplica al tráfico que llega de la interfaz de servicio de la capa superior y sale hacia la RF;
- utilización de parámetros de tráfico y de planificación de MAC para flujos de servicio ascendentes;
- utilización de parámetros de tráfico QoS para flujos de servicio descendentes;
- clasificación de los paquetes que llegan de la interfaz de servicio de la capa superior para un determinado flujo de servicio activo;
- agrupación de propiedades de flujo de servicio en **clases de servicio** con nombre, de modo tal que entidades de la capa superior y aplicaciones externas (tanto en el CM como en el CMTS) puedan pedir flujos de servicio con los parámetros de QoS deseados de una manera coherente en forma global.

La mejor manera de proporcionar una QoS mejorada consiste en clasificar los paquetes que atraviesan la interfaz MAC RF en un **flujo de servicio**. Un flujo de servicio es un flujo unidireccional de paquetes que proporcionan una determinada calidad de servicio. El CM y el CMTS proporcionan esta QoS conformando, controlando y priorizando el tráfico conforme al **conjunto de parámetros de QoS** definido para el flujo de servicio.

El objetivo principal de las características de calidad de servicio que aquí se definen es de definir el ordenamiento y la planificación en la interfaz de radiofrecuencia. Sin embargo, estas características deben a menudo funcionar de consuno con mecanismos que se encuentran más allá de la interfaz de RF para suministrar QoS de extremo a extremo o controlar el comportamiento de los módems de cable. Se permiten por ejemplo los siguientes comportamientos:

- Las políticas pueden ser definidas por las MIB de CM que sobreescriben el octeto de tipo de servicio (TOS, *type of service*). Dichas políticas están fuera del alcance de la especificación de la RFI. En la dirección ascendente, el CMTS controla el valor del octeto de TOS independientemente de cómo se obtenga o de quién lo escriba (el originador o la política de CM).
- La puesta en cola de paquetes de flujo de servicio en el CMTS en sentido descendente puede basarse en el octeto de TOS.
- Los flujos de servicio descendentes pueden ser reclasificados por el CM para proporcionar un servicio mejorado en la red del lado abonado.

Los flujos de servicio existen tanto en el sentido ascendente como en el descendente, y pueden existir sin de hecho ser activados para llevar tráfico. Los flujos de servicio tienen un **identificador de flujo de servicio** (SFID) de 32 bits asignado por el CMTS. Todos los flujos de servicio tienen un SFID; los flujos de servicio activos y admitidos también tienen un **identificador de servicio** (SID) de 14 bits.

En cada fichero de configuración deben estar definidos al menos dos flujos de servicio: uno para servicio ascendente y uno para servicio descendente. El primer flujo de servicio ascendente describe el **flujo de servicio ascendente primario** y es el flujo de servicio por defecto que se utiliza para tráfico sin otra clasificación, incluidos los mensajes de administración de MAC y las PDU datos. El primer flujo de servicio descendente describe el servicio al **flujo de servicio descendente primario**. Los flujos de servicio adicionales definidos en el fichero de configuración crean flujos de servicio que son proporcionados por los servicios de QoS.

Desde un punto de vista conceptual, a los paquetes entrantes se les hace concordar con un **clasificador** que determina a qué flujo de servicio de QoS se reenvía el paquete. El clasificador puede examinar el encabezamiento LLC del paquete, el encabezamiento IP/TCP/UDP del paquete o alguna combinación de ambos. Si el paquete coincide con alguno de los clasificadores, es reenviado al flujo de servicio indicado por el atributo SFID del clasificador. Si el paquete no coincide con un clasificador, es reenviado en el flujo de servicio primario.

B.10.1.1 Conceptos

B.10.1.1.1 Flujos de servicio

Un **flujo de servicio** es un servicio de transporte de capa MAC que provee el transporte unidireccional de paquetes ya sea a paquetes ascendentes transmitidos por el CM o a paquetes descendentes transmitidos por el CMTS (véase la nota 1). Un flujo de servicio se caracteriza por un conjunto de **parámetros de QoS** tales como latencia, fluctuación de fase, y garantías de caudal. A fin de normalizar el funcionamiento entre el CM y el CMTS, esos atributos contienen detalles sobre cómo pide el CM miniintervalos de tiempo ascendentes y el comportamiento esperado del planificador ascendente del CMTS.

NOTA 1 – Un flujo de servicio, tal como se define aquí, no tiene relación directa con el concepto de "flujo" según lo definió el Grupo de Trabajo de Servicios Integrados (intserv) del IETF [RFC 2212]. Un flujo intserv es un conjunto de paquetes que comparten puntos extremos de la capa de transporte. Varios flujos intserv pueden ser atendidos por un único flujo de servicio. Sin embargo, los clasificadores de un flujo de servicio PUEDEN basarse en criterios IEEE 802.1P/Q, por lo que NO PUEDEN en absoluto involucrar flujos intserv.

Los atributos siguientes caracterizan parcialmente al flujo de servicios (véase la nota 2):

- **ServiceFlowID** (identificador de flujo de servicio): existe para todos los flujos de servicio.
- **ServiceID** (identificador de servicio): existe sólo para flujos de servicio ascendentes admitidos o activos.
- **ProvisionedQosParamSet**: (conjunto de parámetros de QoS aprovisionado) define un conjunto de parámetros de QoS que aparece en el fichero de configuración y se presenta durante el registro. Esto PUEDE definir el límite inicial a las autorizaciones permitidas por el módulo de autorización. ProvisionedQosParamSet se define una vez creado el flujo de servicio por medio del registro (véase la nota 3).
- **AdmittedQosParamSet** (conjunto de parámetros de QoS admitido): define un conjunto de parámetros de QoS para los cuales el CMTS (y quizá el CM) están reservando recursos. El principal recurso a reservar es la anchura de banda, pero también cualquier otro recurso basado en memoria o en tiempo que sea necesario para activar el flujo subsiguientemente.
- **ActiveQosParamSet** (conjunto de parámetros de QoS activo): define un conjunto de parámetros de QoS que definen el servicio que de hecho se proporciona al flujo de servicio. Sólo un flujo de servicio activo puede retransmitir paquetes.

NOTA 2 – Algunos atributos se obtienen de la lista previa de atributos. El nombre de clase de servicio es un atributo de ProvisionedQosParamSet. El estado de activación del flujo de servicio lo determina el ActiveQosParamSet. Si ActiveQosParamSet es nulo, el flujo de servicio está inactivo.

NOTA 3 – ProvisionedQosParamSet es nulo cuando un flujo es creado dinámicamente.

Un flujo de servicio existe cuando el CMTS le asigna un ID de flujo de servicio (SFID). El SFID hace de identificador principal del flujo de servicio en el CM y el CMTS. Un flujo de servicio existente tiene al menos un SFID y un sentido asociado.

El **módulo de autorización** es una función lógica dentro del CMTS que aprueba o deniega cada cambio a los clasificadores y parámetros de QoS asociados a un flujo de servicio. Como tal, define una "envolvente" que limita los valores posibles de AdmittedQosParameterSet y ActiveQosParameterSet.

La relación entre los conjuntos de parámetros de QoS es la que se muestra en las figuras B.10-1 y B.10-2. ActiveQosParameterSet es siempre un subconjunto (véase la nota 4) de AdmittedQosParameterSet, el cual es siempre un subconjunto de la "envolvente" autorizada. En el modelo de autorización dinámica esta envolvente queda determinada por el módulo de autorización (etiquetado como AuthorizedQosParameterSet). En el modelo de autorización aprovisionada esta envolvente queda determinada por ProvisionedQosParameterSet. (Véase B.10.1.4 para más información sobre los modelos de autorización.)

NOTA 4 – Para afirmar que el conjunto A de parámetros de QoS es un subconjunto del conjunto B de parámetros de QoS, DEBE cumplirse lo siguiente para todo parámetro de QoS de A y B:

– si (un valor menor del parámetro de QoS indica menos recursos, por ejemplo, máxima velocidad de tráfico), A será un subconjunto de B si el parámetro de A es menor o igual al mismo parámetro de B;

– si (un valor mayor del parámetro de QoS indica menos recursos, por ejemplo, fluctuación de asignación tolerada), A será un subconjunto de B si el parámetro de A es mayor o igual al mismo parámetro de B;

– si (el parámetro de QoS especifica un intervalo periódico, por ejemplo, intervalo de concesión nominal), A será un subconjunto de B si el parámetro de A es un múltiplo entero del mismo parámetro de B:

– si (el parámetro de QoS no es cuantitativo, por ejemplo, tipo de planificación de flujo de servicio), A es un subconjunto de B si el parámetro de A es igual al mismo parámetro de B.

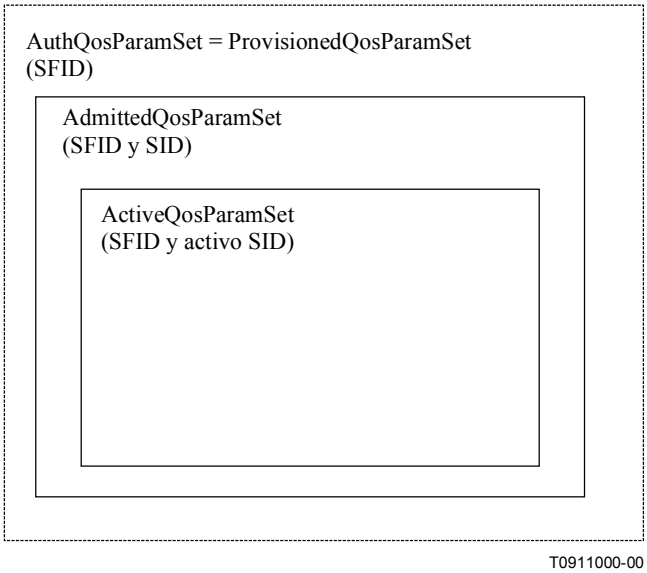


Figura B.10-1/J.112 – "Envolventes" del modelo de autorización aprovisionada

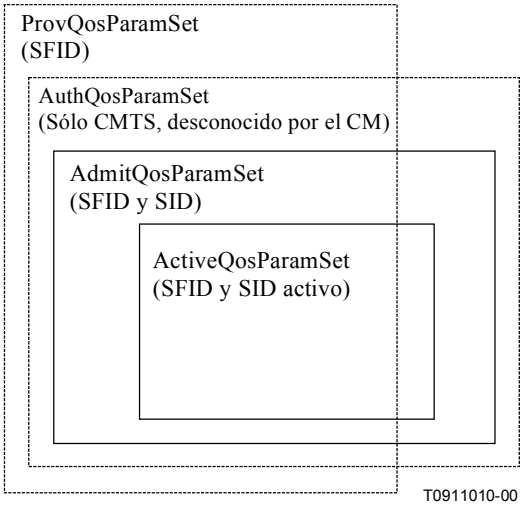


Figura B.10-2/J.112 – "Envolventes" del modelo de autorización dinámica

Resulta útil pensar en tres tipos de flujos de servicio:

- **Aprovisionado**: Este tipo de flujo de servicio se conoce a través del aprovisionamiento por medio del fichero de configuración; su AdmittedQosParamSet y su ActiveQosParamSet son ambos nulos. Un **flujo de servicio aprovisionado** puede o no tener clasificadores asociados. Si un flujo de servicio aprovisionado tiene clasificadores asociados, los clasificadores NO DEBEN ser utilizados para clasificar paquetes que se insertan en el flujo, independientemente del estado de activación del clasificador.
- **Admitido**: Este tipo de flujo de servicio tiene recursos reservados por el CMTS para su AdmittedQosParamSet, pero estos parámetros no están activos (su ActiveQosParamSet es nulo). Los **flujos de servicio admitidos** pueden haber sido aprovisionados, o pueden haber sido señalizados por algún otro mecanismo. Por lo general, los flujos de servicio admitidos tienen clasificadores asociados; sin embargo, los flujos de servicio admitidos pueden usar una clasificación basada en una política. Si los flujos de servicio admitidos tienen clasificadores asociados, los clasificadores NO DEBEN ser utilizados para clasificar paquetes que se insertan en el flujo, independientemente del estado de activación del clasificador.
- **Activo**: Este tipo de flujo de servicio tiene recursos concertados por el CMTS para su conjunto de parámetros de QoS (por ejemplo, está enviando activamente MAP que contienen concesiones no solicitadas para un flujo de servicio basado en UGS). Su ActiveQosParamSet es no nulo. Por lo general, los flujos de servicio activos tienen clasificadores asociados; sin embargo, los flujos de servicio activos pueden usar una clasificación basada en una política. Los flujos de servicio primarios pueden tener uno o más clasificadores asociados pero, además de cualquier paquete que concuerde con dichos clasificadores, todo paquete que no coincida con ningún clasificador será enviado por el flujo de servicio primario para ese sentido.

B.10.1.1.2 Clasificadores

Un **clasificador** es un conjunto de criterios concordantes aplicado a cada paquete que entra en la red de cable. Consiste en algunos criterio de concordancia de paquetes (por ejemplo, dirección IP de destino), una **prioridad de clasificador** y una referencia a un flujo de servicio. Si un paquete coincide con los criterios de concordancia de paquetes especificados, será enviado por el flujo de servicio al que se hace referencia.

Varios clasificadores pueden, todos ellos, referirse al mismo flujo de servicio. La prioridad de clasificador se utiliza para ordenar la aplicación de clasificadores a paquetes. Se hace necesario ordenar explícitamente ya que puede haber superposición entre los esquemas utilizados por los clasificadores. La prioridad no tiene por qué ser única, pero se debe tener cuidado dentro de una prioridad de clasificador para impedir la ambigüedad en la clasificación. (véase B.10.1.6.1.) Los **clasificadores descendentes** son aplicados por el CMTS a los paquetes que está transmitiendo, y los **clasificadores ascendentes** son aplicados en el CM y pueden ser aplicados en el CMTS para controlar la clasificación de los paquetes ascendentes. En la figura B.10-3 se ilustran los diagramas antes analizados.

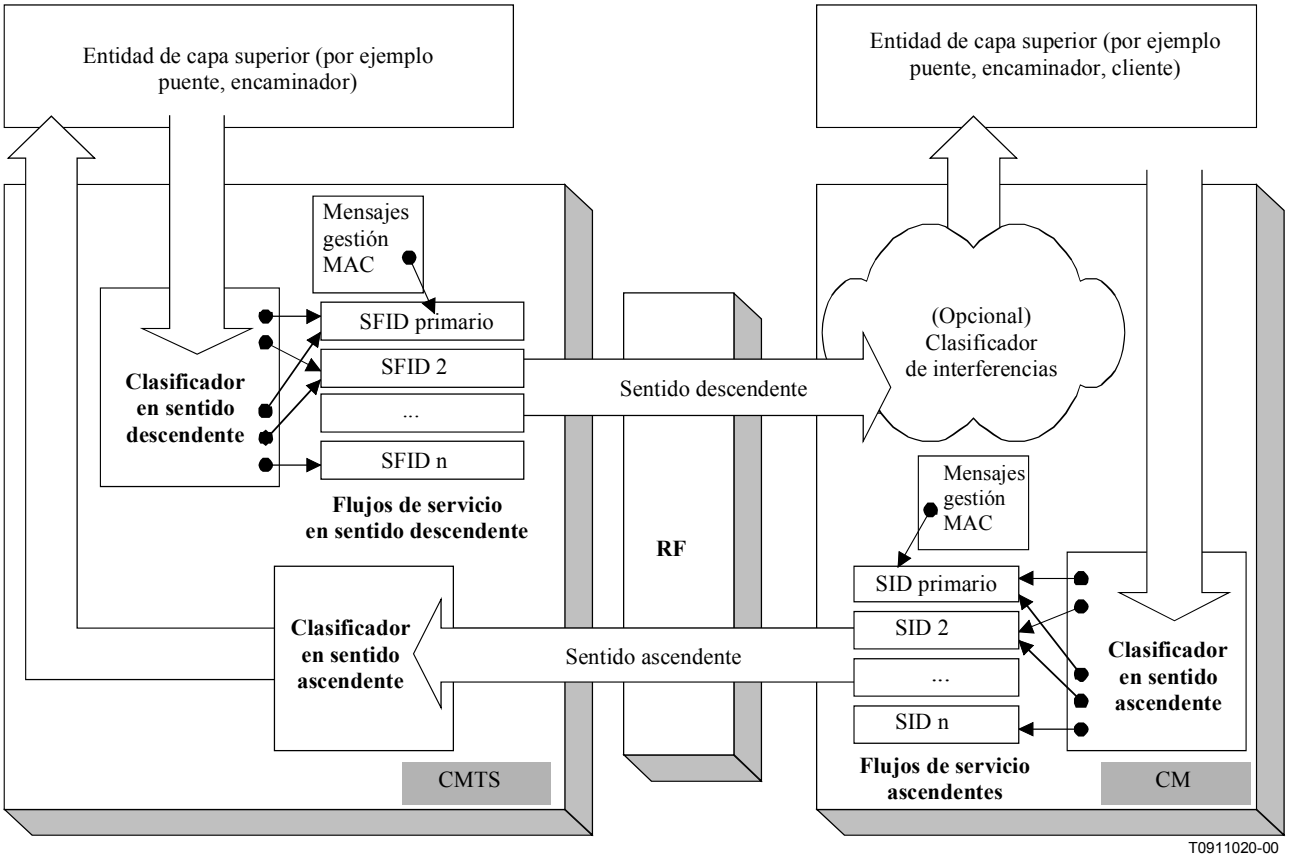


Figura B.10-3/J.112 – Clasificación dentro de la capa MAC

La clasificación de paquetes de CM y CMTS consta de múltiples clasificadores. Cada clasificador contiene un campo de prioridad que determina el orden de búsqueda de dicho clasificador. Se DEBE aplicar primero el clasificador de prioridad más elevada. Si se halla un clasificador en el que todos los parámetros concuerdan con el paquete, el clasificador DEBE retransmitir el paquete al correspondiente flujo de servicio. Si no se halla ningún clasificador en el que todos los parámetros concuerden con el paquete, el paquete es clasificado flujo de servicio primario.

La tabla de clasificación de paquetes contiene los campos que siguen:

- Prioridad – Determina el orden de búsqueda en la tabla. Los clasificadores de prioridad más alta se revisan antes que los clasificadores de prioridad más baja.
- Parámetros de clasificación IP – Cero o más de los parámetros de clasificación IP (gama/plantilla de TOS IP, protocolo IP, plantilla/dirección de origen IP, plantilla/dirección de destino IP, comienzo de puerto de origen TCP/UDP, final de puerto de origen TCP/UDP, comienzo de puerto de destino TCP/UDP, final de puerto de destino TCP/UDP).

- Parámetros de clasificación LLC – Cero o más de los parámetros de clasificación LLC (dirección de destino MAC, dirección de origen MAC, Ethertype/SAP).
- Parámetros IEEE 802.1P/Q – Cero o más de los parámetros de clasificación IEEE (gama de prioridades IEEE 802.1P, ID de VLAN IEEE 802.1Q).
- Identificador de flujo de servicio – Identificador de un flujo específico al que se ha de enviar este paquete.

Los clasificadores se pueden agregar a la tabla ya sea por medio de operaciones de gestión (fichero de configuración, registro) o por medio de operaciones dinámicas (señalización dinámica, interfaz de servicio de la subcapa MAC de DOCSIS). Las operaciones basadas en el SNMP pueden ver los clasificadores que se agregan por medio de operaciones dinámicas, pero no pueden modificar o eliminar clasificadores creados por operaciones dinámicas. El formato de los parámetros de la tabla de clasificación que se definen en el fichero de configuración, mensaje de registro o mensaje de señalización dinámica se encuentra en el anexo B.C.

Los atributos de clasificador incluyen un estado de activación (véase B.C.2.1.3.6). La configuración "inactivo" se puede usar para reservar recursos para un clasificador a activar más tarde. La activación efectiva del clasificador depende tanto de este atributo como del estado de su flujo de servicio. Si el flujo de servicio no está activo, no se utiliza el clasificador, independientemente de la configuración de este atributo.

B.10.1.2 Modelo de objeto

Los principales objetos de la arquitectura se representan mediante rectángulos con nombre en la figura B.10-4. Cada objeto tiene varios atributos; los nombres de los atributos que identifican al objeto de manera exclusiva están subrayados. Los atributos opcionales se denotan mediante paréntesis. La relación entre el número de objetos está marcada en cada extremo de la línea de asociación entre los objetos. Por ejemplo, un flujo de servicio puede estar asociado a un número de clasificadores comprendido entre 0 y 65 535, pero un clasificador está asociado exactamente a un flujo de servicio.

El flujo de servicio es el concepto central del protocolo MAC. Es identificado de manera exclusiva mediante un ID de flujo de servicio (SFID) de 32 bits que le asigna el CMTS. Los flujos de servicio pueden tener sentido ascendente o descendente. Un identificador de servicio (SID) de unidifusión es un índice de 14 bits asignado por el CMTS que está asociado a un, y sólo un, flujo de servicio ascendente admitido

En un caso típico, un paquete de datos de usuario saliente es enviado por un protocolo de capa superior (tal como el puente retransmisor de un CM) para la transmisión por la interfaz MAC de cable. El paquete se compara con un conjunto de clasificadores. El clasificador concordante para el paquete identifica el flujo de servicio correspondiente por medio del identificador de flujo de servicio (SFID). En el caso en que más de un clasificador concuerde con el paquete, se elige el clasificador de prioridad más elevada.

El clasificador que concuerda con un paquete puede estar asociado a una regla de supresión de encabezamiento de cabida útil (PHS). Una regla PHS proporciona detalles sobre cómo pueden ser omitidos los octetos de encabezamiento de una PDU paquetes, reemplazados por un índice de supresión de encabezamiento de cabida útil para su transmisión y luego regenerados en el extremo receptor. Las reglas PHS son indexadas por la combinación de {SFID, PHSI} (véase B.10.4). Cuando se elimina un flujo de servicio, todos los clasificadores y cualesquiera reglas de PHS asociadas que hacen referencia a dicho flujo DEBEN también ser eliminados.

La clase de servicio es un objeto opcional que PUEDE ser implementado en el CMTS. La referencia al mismo se hace por medio de un nombre ASCII cuyo objetivo es el aprovisionamiento. Una clase de servicio queda definida en el CMTS por el hecho de tener un conjunto de parámetros de QoS que le es particular. Los conjuntos de parámetros de QoS de un flujo de servicio pueden contener una

referencia al nombre de clase de servicio en forma de "macro" que selecciona todos los parámetros de QoS de la clase de servicio. Los conjuntos de parámetros de QoS del flujo de servicio pueden -a reserva de la autorización del CMTS- ampliar y hasta invalidar la configuración de parámetros de QoS de la clase de servicio. (Véase B.C.2.2.5.)

Si los mecanismos de control de capa superior ya han determinado que un paquete está asociado a una combinación determinada de prioridad/nombre de clase de servicio, dicha combinación asocia el paquete directamente con un determinado flujo de servicio (véase B.10.1.6.1). La capa superior puede también estar al tanto de los flujos de servicio particulares en la subcapa MAC, y puede haber asignado al paquete directamente a un flujo de servicio. En estos casos se considera que un paquete de datos de usuario está asociado directamente a un flujo de servicio según la selección realizada por la capa superior. En la figura B.10-4 se indica esto con la flecha de línea de puntos (véase el anexo B.E).

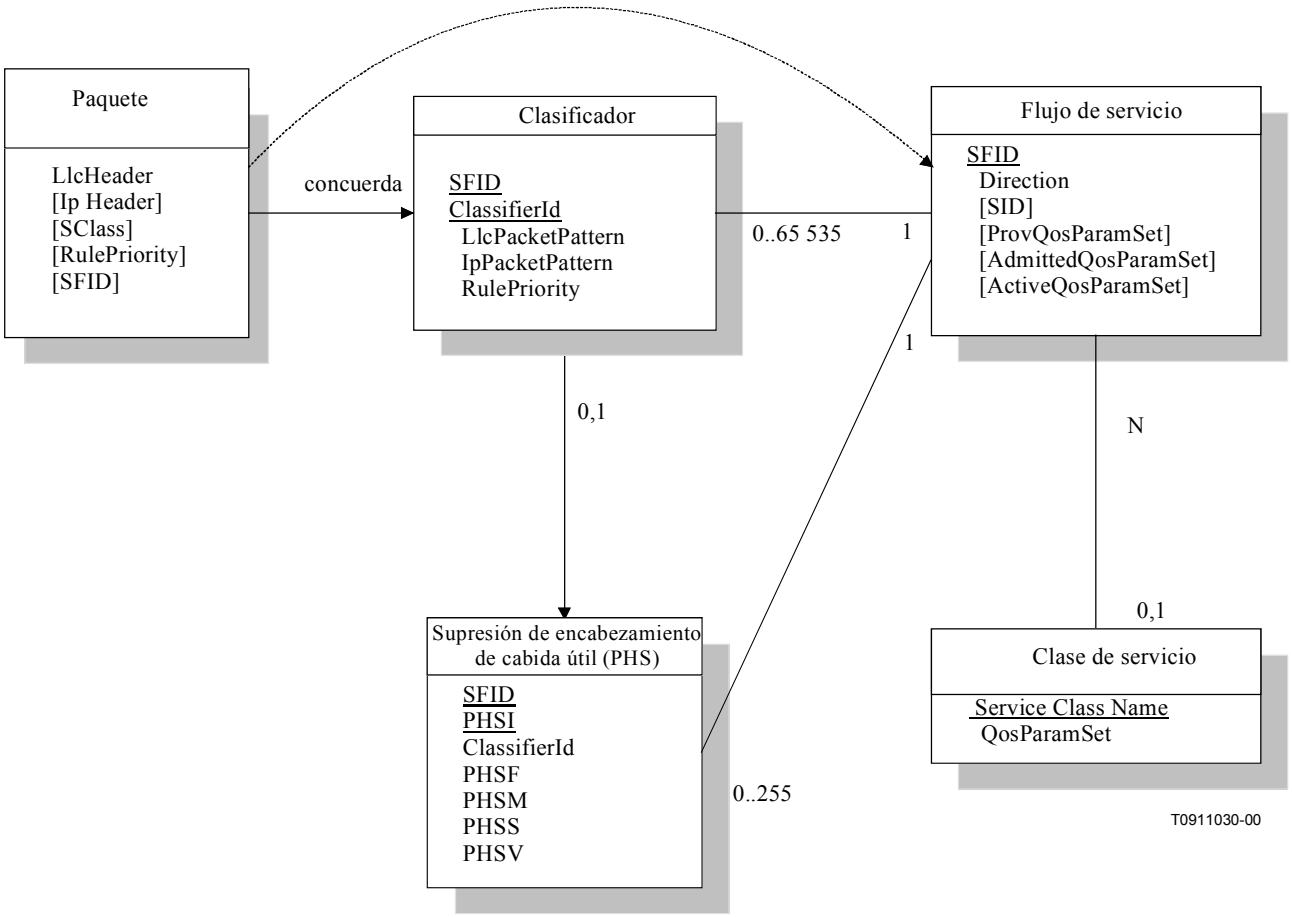


Figura B.10-4/J.112 – Modelo de objetos de la teoría del funcionamiento

B.10.1.3 Clases de servicio

Los atributos de QoS de un flujo de servicio se pueden especificar de dos maneras: sea definiendo explícitamente todos los atributos, o especificando implícitamente un **nombre de clase de servicio**. Un **nombre de clase de servicio** es una cadena que el CMTS asocia a un conjunto de parámetros de QoS. Se describe con más detalle a continuación.

La clase de servicio sirve a estos propósitos:

1) Permite a los operadores que así lo deseen trasladar la carga de la configuración de los flujos de servicio del servidor de aprovisionamiento al CMTS. Los operadores aprovisionan a los módems con el nombre de clase de servicio; la implementación del nombre se configura B.en la CMTS. Esto permite a los operadores modificar la implementación de un servicio dado para adaptarse a las circunstancias locales sin cambiar el aprovisionamiento de módems. Por ejemplo, es posible que algunos parámetros de planificación hayan de ser reajustados de manera diferente para que dos CMTS distintos proporcionen el mismo servicio. Otro ejemplo lo constituiría la posibilidad de cambiar los perfiles de servicio según la hora del día.

2) Permite a los vendedores de CMTS facilitar, si así lo deciden, la puesta en cola según la clase de manera que los flujos de servicio compitan dentro de su clase, y las clases compitan entre sí por la anchura de banda.

3) Permite a los protocolos de clase superior crear un flujo de servicio por su nombre de clase de servicio. Por ejemplo, la señalización de telefonía puede ordenar al CM la creación de una instancia de cualquier flujo de servicio aprovisionado disponible de la clase "G711".

4) Permite definir políticas de clasificación de paquetes que se refieran a una clase de servicio deseada sin tener que referirse a un ejemplar determinado de flujo de servicio de dicha clase.

NOTA – La clase de servicio es opcional: siempre puede proporcionarse una especificación completa de planificación de flujo; un flujo de servicio puede no pertenecer a clase de servicio alguna. Las implementaciones de CMTS PUEDEN tratar tales flujos "sin clase" de forma distinta a los flujos "con clase" con parámetros equivalentes.

El conjunto de parámetros de QoS de cualquier flujo de servicio PUEDE especificarse de alguna de estas tres maneras:

- incluyendo explícitamente todos los parámetros de tráfico;
- por referencia indirecta a un conjunto de parámetros de tráfico, para lo cual se especifica un nombre de clase de servicio;
- especificando un nombre de clase de servicio junto con los parámetros modificantes.

El nombre de clase de servicio se "expande" a su conjunto definido de parámetros cuando el CMTS admite con éxito el flujo de servicio. La expansión de la clase de servicio puede estar contenida en los siguientes mensajes originados en el CMTS: mensaje respuesta de registro, DSA-REQ, DSC-REQ, DSA-RSP y DSC-RSP. En todos estos casos, el CMTS DEBE incluir una codificación de flujo de servicio que incluya el nombre de clase de servicio y el conjunto de parámetros de QoS de la clase de servicio. Si una petición iniciada por CM contuviera cualesquiera parámetros de flujo de servicio suplementarios o de invalidación, una respuesta exitosa DEBE incluir también esos parámetros.

Cuando en una petición de admisión o activación se da un nombre de clase de servicio, el conjunto de parámetros de QoS devuelto puede cambiar de una activación a otra. Esto puede ocurrir por cambios administrativos introducidos en el conjunto de parámetros de QoS de clase de servicio en la CMTS. Si se cambia la definición de nombre de clase de servicio en el CMTS (por ejemplo, se modifica el conjunto de parámetros de QoS que tiene asociado), dicho cambio no tiene efecto alguno en los parámetros de QoS de los flujos de servicio existente y asociados a dicha clase de servicio. Un CMTS PUEDE iniciar transacciones DCS hacia flujos de servicio existentes que hacen referencia al nombre de clase de servicio para afectar a la definición modificada de clase de servicio.

Cuando un CM utilice el nombre de clase de servicio para especificar el conjunto de parámetros de QoS admitido, el conjunto ampliado de codificaciones de la tupla TLV (tipo/longitud/valor) del flujo de servicio será devuelto al CM en el mensaje de respuesta (REG-RSP, DSA-RSP, o DSC-RSP). La utilización del nombre de clase de servicio más adelante, en la petición de activación, puede fallar si ha cambiado la definición del nombre de clase de servicio y no están disponibles los nuevos recursos

requeridos. Así pues, el CM DEBERÍA pedir explícitamente el conjunto ampliado de la tupla TLV al mensaje de respuesta en su posterior petición de activación.

B.10.1.4 Autorización

Cualquier cambio de los parámetros de QoS de flujo de servicio DEBE ser aprobado por un módulo de autorización. Se incluyen aquí todos los mensajes REG-REQ o DSA-REQ para crear un nuevo flujo de servicio, y todos los mensajes DSC-REQ para modificar un conjunto de parámetros de QoS de un flujo de servicio existente. Tales cambios incluyen la solicitud de una decisión de control de admisión (por ejemplo, fijar el AdmittedQosParamSet) y la petición de una activación de un flujo de servicio (por ejemplo, fijar el ActiveQosParameterSet). Las peticiones de reducción a propósito de los recursos que han de ser admitidas o activadas también son verificadas por el módulo de autorización, al igual que las peticiones de adición o modificación de clasificadores.

En el modelo de autorización estática, el módulo de autorización recibe todos los mensajes de registro y almacena el estado aprovisionado de todos los flujos de servicio "diferidos". Se permitirán las peticiones de admisión y de activación de estos flujos de servicio aprovisionados siempre que el conjunto de parámetros de QoS admitido sea un subconjunto del conjunto de parámetros de QoS aprovisionado, y que el conjunto de parámetros de QoS activo sea un subconjunto del conjunto de parámetros de QoS admitido. Se rechazarán las peticiones de modificación del conjunto de parámetros de QoS aprovisionado, así como las peticiones de creación de nuevos flujos de servicio dinámicos. De esta manera se define un sistema estático en el que todos los servicios posibles son definidos en la configuración inicial de cada CM.

En el modelo de autorización dinámica, el módulo de autorización no sólo recibe todos los mensajes de registro sino que además se comunica a través de una interfaz separada con un servidor de políticas independiente. Este servidor puede dar aviso por adelantado al módulo de autorización sobre de próximas peticiones de admisión y de activación, y especifica la acción de autorización correcta a realizar en cuanto a esas peticiones. Las peticiones de admisión y de activación de un CM son verificadas a continuación por el módulo de autorización para asegurar que el ActiveQosParameterSet que se está solicitando es un subconjunto del conjunto proporcionado por el servidor de política. Se permiten las peticiones de admisión y de activación de un CM que son señalizadas por adelantado por el servidor de políticas externo. Las peticiones de admisión y de activación de un CM que no son señalizadas por adelantado por el servidor de políticas externo pueden dar lugar a una consulta en tiempo real al servidor de política o pueden ser rechazadas.

Durante el registro, el CM DEBE enviar al CMTS el conjunto autenticado de tuplas TLV obtenido de su fichero de configuración, el cual define el conjunto de parámetros de QoS aprovisionado. A su recepción y verificación en el CMTS, se pasan al módulo de autorización dentro del CMTS. El CMTS DEBE ser capaz de guardar el conjunto de parámetros de QoS aprovisionado y DEBE ser capaz de usar esta información para autorizar flujos dinámicos que constituyen un subconjunto del conjunto de parámetros de QoS provisionado. El CMTS DEBERÍA implementar mecanismos para invalidar este proceso de aprobación automatizado (como se describe en el modelo de autorización dinámico). Por ejemplo:

- rechazar todas las peticiones, hayan sido o no aprovisionadas por anticipado;
- definir una tabla interna con un mecanismo de política mejor pero inicializado por la información del fichero de la configuración;
- derivar todas las peticiones a un servidor de control externo.

B.10.1.5 Tipos de flujos de servicio

Resulta útil considerar tres tipos básicos de flujo de servicio. En esta cláusula se describen con más detalle estos tres tipos de flujo de servicio. Pero conviene señalar que hay más tipos que esos tres básicos. (Véase B.C.2.2.5.1.)

B.10.1.5.1 Flujos de servicio aprovisionados

Un flujo de servicio puede ser provisionado sin ser activado inmediatamente (a veces se le dice "diferido"). Es decir, que la descripción de cualquier flujo de servicio de esta naturaleza en el fichero de configuración TFTP (protocolo de transferencia de ficheros trivial, *trivial file transfer protocol*) contiene un atributo que provisiona pero difiere la activación y admisión (véase B.C.2.2.5.1). Durante el registro, el CMTS asigna un ID de flujo de servicio a ese flujo de servicio, pero no reserva recursos. El CMTS PUEDE también requerir, antes de la admisión, un intercambio con un módulo de políticas.

Como resultado de una acción externa que excede el alcance del presente anexo B (por ejemplo, [PKTCBL-MGCP]), el CM PUEDE optar por activar un flujo de servicio aprovisionado transfiriendo el ID de flujo de servicio y los conjuntos de parámetros de QoS asociados. El CM DEBE proporcionar además cualesquiera clasificadores que sean aplicables. Si se autoriza y hay recursos disponibles, el CMTS DEBE responder asignando una SID de unidifusión única para el flujo de servicio ascendente. El CMTS PUEDE desactivar el flujo de servicio, pero NO DEBERÍA eliminar el flujo de servicio durante el espacio de registro del CM.

Como resultado de una acción externa que excede el alcance del presente anexo B (por ejemplo, [PKTCBL-MGCP]), el CM PUEDE optar por activar un flujo de servicio transfiriendo el ID de flujo de servicio así como el SID y los conjuntos de parámetros de QoS asociados. La CMTS DEBE proporcionar además cualesquiera clasificadores que sean aplicables. El CMTS PUEDE desactivar el flujo de servicio, pero NO DEBERÍA eliminar el flujo de servicio durante el espacio de registro del CM. Un flujo de servicio provisionado PUEDE ser activado y desactivado muchas veces (por medio de intercambios de DSC). En todos los casos se DEBE utilizar el ID de flujo de servicio original al reactivar el flujo de servicio.

B.10.1.5.2 Flujos de servicio admitidos

Este protocolo contempla un modelo de activación de dos fases que se utiliza frecuentemente en aplicaciones de telefonía. En el modelo de activación de dos fases se "admiten" primero los recursos para una "llamada"; una vez completada la negociación de extremo a extremo (por ejemplo, la pasarela de la parte llamada genera un evento "descolgado"), se "activan" los recursos. Un modelo así de dos fases sirve para:

a) ahorrar recursos de red hasta que se haya establecido una conexión completa de extremo a extremo;

b) efectuar verificaciones de políticas y control de admisión de los recursos lo más rápido posible y, en particular, antes de informar al extremo lejano de la petición de conexión; y

c) evitar varias situaciones potenciales de robo de servicio.

Por ejemplo, si un servicio de capa superior estuviera utilizando un servicio de concesión no solicitada, y fuera posible añadir convenientemente flujos de capa superior incrementando el parámetro de QoS concesiones por intervalo, se podría aplicar el procedimiento que se indica a continuación. Cuando está pendiente el primer flujo de la capa superior, el CM emite una petición de DSA con el parámetro admitir concesiones por intervalo igual a uno, y el parámetro activar concesiones por intervalo igual a cero. Luego, cuando el flujo de la capa superior se torna activo, emite una petición de DSC con el ejemplar del parámetro activar concesiones por intervalo igual a uno. El control de admisión se llevó a cabo cuando se realizó la reserva, por lo que la posterior petición de DSC, con los parámetros de activar dentro del margen de la reserva previa, tiene el éxito garantizado. Los subsiguientes flujos de capa superior serían tratados de la misma manera. Si hubieran tres flujos de capa superior que estuvieran estableciendo conexiones con un flujo ya activo, el flujo de servicio tendría el parámetro concesiones admitidas por intervalo igual a cuatro, y el parámetro concesiones activas por intervalo igual a uno.

Una petición de activación de flujo de servicio cuando el nuevo ActiveQosParamSet sea un subconjunto de AdmittedQosParamSet y no se estén agregando clasificadores nuevos, DEBE ser admitida (excepto en el caso de fallo catastrófico). Una petición de admisión cuando AdmittedQosParamSet sea un subconjunto del AdmittedQosParamSet previo DEBE tener éxito siempre que ActiveQosParamSet siga siendo un subconjunto de AdmittedQosParameterSet.

Un flujo de servicio que tiene recursos asignados a su AdmittedQosParamSet pero cuyos recursos todavía no están completamente activados se encuentra en un estado transitorio. El CMTS que requiere la activación del flujo de servicio dentro de ese periodo DEBE imponer un valor de límite de tiempo. (Veáse B.C.2.2.5.8.) Si no se completa la activación del flujo de servicio dentro de este intervalo el CMTS deberá liberar los recursos asignados que exceden de los parámetros de QoS activos.

En algunas aplicaciones quizás sea necesaria o deseable una reserva de recursos a largo plazo. Por ejemplo, el poner una llamada telefónica en retención debería permitir asignar temporalmente cualesquiera recursos que se estén utilizando en la llamada con otros fines, pero dichos recursos deben estar disponibles para reanudar la llamada más tarde. AdmittedQosParamSet se mantiene como un "estado blando" en el CMTS; este estado debe ser renovado periódicamente para que se mantenga sin que el tiempo límite antes mencionado libere los recursos no activados. Esta renovación PUEDE ser señalizada con un mensaje periódico DSC-REQ con conjuntos de parámetros de QoS idénticos, o PUEDE ser señalizada por algún mecanismo interno dentro del CMTS que queda fuera del alcance del presente anexo B (por ejemplo, por parte del CMTS vigilando los mensajes de renovación RSVP). Cada vez que se le señalice una renovación al CMTS, el CMTS debe renovar el "estado blando".

B.10.1.5.3 Flujos de servicio activos

Un flujo de servicio con un conjunto de ActiveQosParameters no nulo se dice que es un flujo de servicio activo. Está realizando una petición (véase la nota) y recibiendo la concesión de anchura de banda para el transporte de paquetes de datos. Se puede convertir en activo un flujo de servicio admitido proporcionando un ActiveQosParameterSet, y señalizando los recursos realmente deseados en ese momento. Así se completa la segunda etapa del modelo de activación en dos fases (véase B.10.1.5.2).

NOTA – Conforme a su política de petición/transmisión (véase B.C.2.2.6.3).

Un flujo de servicio puede ser aprovisionado e inmediatamente activado. Tal es el caso de los flujos de servicio primarios. También es característico de los flujos de servicio en servicios de abono mensual, por ejemplo. Estos flujos de servicio se establecen en el momento del registro y DEBEN ser autorizados por el CMTS en base al MIC de CMTS. PUEDEN ser autorizados también por el módulo de autorización del CMTS.

Como alternativa, se puede crear un flujo de servicio creado dinámicamente y activarlo inmediatamente. En este caso se omite la activación en dos fases y el flujo de servicio está disponible para su utilización inmediata tras la autorización.

B.10.1.6 Flujos de servicio y clasificadores

El modelo básico consiste en que los clasificadores asocian los paquetes en exactamente un flujo de servicio. Las codificaciones de flujo de servicio proporcionan los parámetros de QoS para el tratamiento de dichos paquetes en la interfaz de RF. Estas codificaciones se describen en B.C.2.

En el sentido ascendente, el CM DEBE clasificar los paquetes ascendentes en flujos de servicio activos. El CMTS DEBE clasificar el tráfico descendente en flujos de servicio activos descendentes. DEBE haber un flujo de servicio descendente predeterminado para tráfico de radiodifusión y multidifusión que no esté clasificado de otra manera.

El CMTS controla paquetes en flujos de servicio ascendentes para asegurar la integridad de los parámetros de QoS y el valor TOS del paquete. Cuando la velocidad a la que se envían los paquetes es mayor que la velocidad controlada en el CMTS, el CMTS PUEDE prescindir de estos paquetes (véase B.C.2.2.5.3). Cuando el valor del octeto TOS no es correcto, el CMTS (en base a la política) DEBE controlar el tren de paquetes sobreescribiendo el octeto TOS (véase B.C.2.2.6.10).

Es posible que el CM no pueda retransmitir ciertos paquetes ascendentes por ciertos flujos de servicio. En particular, un flujo de servicio que esté utilizando un servicio de concesión no solicitada con fragmentación inhabilitada, no puede ser empleado para retransmitir paquetes mayores que el tamaño de la concesión. Si un paquete se clasifica según un flujo de servicio por el que no puede ser transmitido, el CM DEBE bien transmitir el paquete por el flujo de servicio primario, o bien descartar el paquete; dependiendo de la política de petición/transmisión del flujo de servicio de acuerdo con el cual se clasificó el paquete.

Los mensajes de gestión MAC sólo pueden encontrar su concordancia con un clasificador que contiene una codificación de parámetro "Ethertype/DSAP/MacType" de B.C.2.1.6.3 y cuando el campo "tipo" del encabezamiento de mensaje de gestión MAC (B.8.3.1) coincida con dicho parámetro. Como excepción, el SID primario DEBE ser usado para mantenimiento de estación tal como se especifica en B.8.1.2.3, aún cuando el clasificador coincida con el mensaje ascendente RNG-REQ de mantenimiento de estación. A falta de algún clasificador que concuerde con un mensaje de gestión MAC, DEBERÍA ser transmitido por el flujo de servicio primario. Fuera de los tipos de mensaje MAC excluidos de la clasificación en B.C.2.1.6.3, un CM o un CMTS PUEDEN retransmitir un mensaje MAC que no esté clasificado por cualquier flujo de servicio de una manera específica de la instalación o implementación.

Aunque los mensajes de gestión MAC están sujetos a clasificación, no se los considera parte de ningún flujo de servicio. La transmisión de los mensajes de gestión MAC NO DEBE influir en ninguno de los cálculos de QoS del flujo de servicio según el cual se clasifican. La entrega de los mensajes de gestión MAC está influida implícitamente por los atributos del flujo de servicio asociado.

B.10.1.6.1 Clasificación basada en políticas y clases de servicio

Como se señala en el anexo B.E, hay varias maneras de poner en cola los paquetes para transmisión en la interfaz de servicio MAC. En un extremo están las aplicaciones incorporadas que están estrechamente ligadas a una determinada regla de supresión de encabezamiento de cabida útil (véase B.10.4) y que preceden a una clasificación más general por parte del MAC. En el otro extremo están los paquetes de tránsito general, de los cuales no se sabe nada sino hasta que son analizados aplicando las reglas de clasificación MAC. Otra categoría útil es el tráfico al que aplica política una entidad perteneciente a una capa superior, siendo luego transferido al MAC para su ulterior clasificación según un determinado flujo de servicio.

La clasificación basada en políticas está, por lo general, fuera del alcance del presente anexo B. Un ejemplo podría ser docsDevFilterIpPolicyTable que se define en la MIB de dispositivos de cable [RFC 2669]. Tales políticas suelen durar más tiempo que los flujos de servicio individuales y los clasificadores de MAC, por lo cual es apropiado disponer los dos mecanismos en capas con una interfaz claramente definida entre políticas y clasificación de flujos de servicio MAC.

La interfaz entre las dos capas es la suma de los dos parámetros en la interfaz de petición de transmisión MAC. Los dos parámetros son un nombre de clase de servicio y una prioridad de regla, que se aplican para que concuerde el nombre de clase de servicio. La prioridad de política viene del mismo espacio de números que la prioridad de clasificador de paquetes de las reglas de concordancia de paquetes utilizadas por los clasificadores MAC. El algoritmo de clasificación MAC es ahora:

```
MAC_DATA.request(
    PDU,
    ServiceClassName,
    RulePriority)

TxServiceFlowID = FIND_FIRST_SERVICE_FLOW_ID (ServiceClassName)
SearchID = SEARCH_CLASSIFIER_TABLE (All Priority Levels)
IF (SearchID not NULL and Classifier.RulePriority >= MAC_DATA.RulePriority)
    TxServiceFlowID = SearchID

IF (TxServiceFlowID = NULL)
    TRANSMIT_PDU (PrimaryServiceFlowID)
ELSE
    TRANSMIT_PDU (TxServiceFlowID)
```

Mientras que prioridad de política compite con prioridad de clasificador de paquetes, y su selección podría teóricamente ser problemática, se estima que se elegirán gamas conocidas de prioridades para evitar la ambigüedad. En particular, los clasificadores agregados dinámicamente DEBEN usar la gama de prioridades 64-191. Los clasificadores creados como parte del registro, así como los clasificadores basados en políticas, utilizan de 0 a 255, pero DEBERÍAN evitar la gama dinámica.

La clasificación dentro de la subcapa MAC está destinada a simplemente asociar un paquete a un flujo de servicio. Si está previsto prescindir de un paquete, DEBE prescindir de él la entidad de capa superior en vez de ser entregado a la subcapa MAC.

B.10.1.7 Funcionamiento general

B.10.1.7.1 Funcionamiento estático

La configuración estática de los clasificadores y los flujos de servicio utiliza el proceso de registro. Un servidor de aprovisionamiento proporciona información de configuración al CM. El CM pasa esta información al CMTS en una petición de registro. El CMTS agrega información y replica con una respuesta de registro. El CM envía un acuse de recibo de registro para completar el proceso de registro. (Véase la figura B.10-5.)

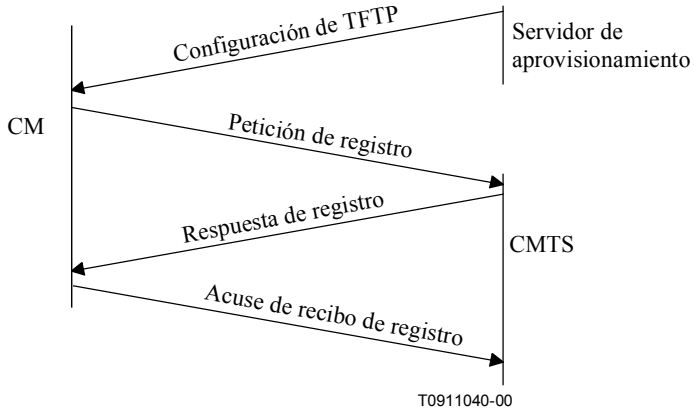


Figura B.10-5/J.112 – Flujo de mensaje de registro

Un fichero de configuración TFTP (véase el cuadro B.10-1) consiste en uno o más ejemplares de clasificadores y codificaciones de flujo de servicio. Los clasificadores se ordenan no muy estrictamente por "prioridad". Cada clasificador hace referencia a un flujo de servicio por medio de una "referencia a flujo de servicio". Varios clasificadores pueden referirse al mismo flujo de servicio.

Además, más de un clasificador pueden tener igual prioridad, y en este caso no queda definido el clasificador usado en concreto.

Cuadro B.10-1/J.112 – Contenido del fichero TFTP

Elementos	Referencia de punto a flujo de servicio	Referencia de flujo de servicio	ID de flujo de servicio
Clasificadores ascendentes Cada uno contiene una referencia de flujo de servicio (puntero)	1..n		
Clasificadores descendentes Cada uno contiene una referencia de flujo de servicio (puntero)	(n+1)..q		
Codificaciones de flujo de servicio Petición de activación inmediata, ascendente		1..m	Ninguno aún
Codificaciones de flujo de servicio Petición de aprovisionamiento para activación posterior, ascendente		(m+1)..n	Ninguno aún
Codificaciones de flujo de servicio Petición de activación inmediata, ascendente		(n+1)..p	Ninguno aún
Codificaciones de flujo de servicio Petición de aprovisionamiento para activación posterior, ascendente		(p+1)..q	Ninguno aún

Las codificaciones de flujo de servicio contienen sea una definición completa de atributos de servicio (omitiendo, si así se desea, los que pueden adquirir valores por defecto) o un nombre de clase de servicio. Un nombre de clase de servicio es una cadena ASCII conocida en el CMTS y que especifica en forma indirecta un conjunto de parámetros de QoS (véanse B.10.1.3 y B.C.2.2.3.4).

NOTA – En el momento del fichero de configuración TFTP las referencias de flujo de servicio existen tal como las define el servidor de aprovisionamiento. Los identificadores de flujo de servicio todavía no existen porque el CMTS no está al tanto de estas definiciones de flujo de servicio.

El paquete de petición de registro contiene clasificadores descendentes (si es que ha de ser activado inmediatamente) y todos los flujos (véase el cuadro B.10-2) de servicio inactivos. El fichero de configuración y, por ende, la petición de registro no contienen por lo general un clasificador descendente si la petición del correspondiente flujo de servicio es con activación diferida. Esto permite una vinculación posterior del clasificador, cuando se activa el flujo.

Cuadro B.10-2/J.112 – Contenidos de la petición de registro

Elementos	Referencia de punto a flujo de servicio	Referencia de flujo de servicio	ID de flujo de servicio
Clasificadores ascendentes Cada uno contiene una referencia de flujo de servicio (puntero)	1..n		
Clasificadores descendentes Cada uno contiene una referencia de flujo de servicio (puntero)	(n+1)..p		
Codificaciones de flujo de servicio Petición de activación inmediata, ascendente Puede especificar atributos explícitos o nombre de clase de servicio		1..m	Ninguno aún
Codificaciones de flujo de servicio Petición de aprovisionamiento para activación posterior, ascendente Atributos explícitos o nombre de clase de servicio		(m+1)..n	Ninguno aún
Codificaciones de flujo de servicio Petición de activación inmediata, descendente Atributos explícitos o nombre de servicio		(n+1)..p	Ninguno aún
Codificaciones de flujo de servicio Petición de aprovisionamiento para activación posterior, descendente Atributos explícitos o nombre de clase de servicio		(p+1)..q	Ninguno aún

La respuesta de registro fija los conjuntos de parámetros de QoS según el tipo de conjunto de parámetro de calidad de servicio en la petición de registro.

La respuesta de registro conserva los atributos de referencia de flujo de servicio de modo tal que la referencia de flujo de servicio puede ser asociada al SFIDy/o al SID. Véase el cuadro B.10-3.

Cuadro B.10-3/J.112 – Contenido de la respuesta de registro

Elementos	Referencia de flujo de servicio	Identificador de flujo de servicio	Identificador de servicio
Flujos de servicio ascendentes activos Atributos explícitos	1..m	SFID	SID
Flujos de servicio ascendentes aprovisionados Atributos explícitos	(m+1)..n	SFID	Aún no
Flujos de servicio descendentes activos Atributos explícitos	(n+1)..p	SFID	No aplicable
Flujos de servicio descendentes aprovisionados Atributos explícitos	(p+1)..q	SFID	No aplicable

El SFID es elegido por el CMTS para identificar un flujo de servicio, descendente o ascendente, que haya sido autorizado pero no activado. Una petición de DSC de un módem para que se admita o active un flujo de servicio aprovisionado contiene su SFID. Si se trata de un flujo descendente, se incluye también el clasificador descendente.

B.10.1.7.2 Creación de flujo de servicio dinámica iniciada por el CM

Los flujos de servicio pueden ser creados por el proceso de adición de servicio dinámica así como el proceso de registro previamente esbozado. La adición de servicio dinámica puede ser iniciada ya sea por el CM o por el CMTS, y se pueden crear uno o más flujos de servicio dinámicos ascendentes y/o descendentes. Se utiliza una toma de contacto de tres direcciones para crear flujos de servicio. El protocolo iniciado por el CM se muestra en la figura B.10-6 y se describe en detalle en B.11.4.2.1.

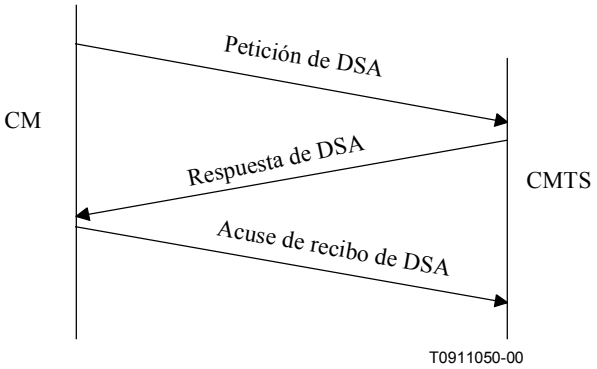


Figura B.10-6/J.112 – Flujo de mensaje de adición de servicio dinámica iniciada por el CM

Una petición de DSA procedente de un CM contiene referencia(s) de flujo de servicio, conjunto(s) de parámetros de QoS (marcados para admisión solamente o para admisión y activación) y los clasificadores que sean necesarios.

B.10.1.7.3 Creación de flujo de servicio dinámica iniciada por el CMTS

Una petición de DSA de un CMTS contiene uno o más identificadores de flujo de servicio para un flujo de servicio ascendente y/o un flujo de servicio descendente, posiblemente un SID, uno o más conjuntos de parámetros de QoS activos o admitidos, y cualesquiera clasificadores requeridos. El protocolo se muestra en la figura B.10-7 y se describe en detalle en B.11.4.2.2.

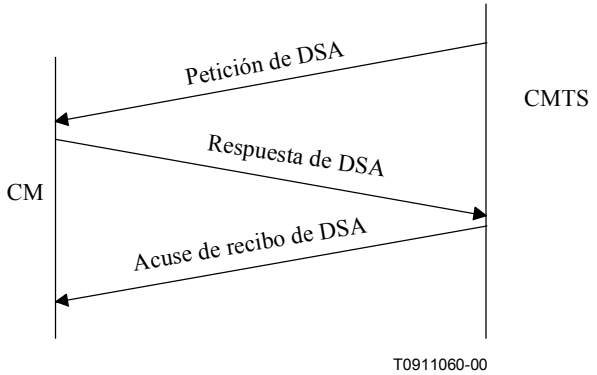


Figura B.10-7/J.112 – Flujo de mensaje de adición de servicio dinámica iniciada por el CMTS

B.10.1.7.4 Modificación y eliminación dinámicas de flujo de servicio

Además de los métodos previamente presentados para la creación de flujos de servicio, se definen protocolos para modificar y eliminar flujos de servicio. Véanse B.11.4.4 y B.11.4.3.

Los flujos de servicio, tanto aprovisionados como creados dinámicamente, son modificados por medio del mensaje DSC el cual puede cambiar los conjuntos de parámetros de QoS admitido y activo del flujo. El DSC también puede agregar, reemplazar o eliminar clasificadores y agregar reglas de PHS, agregar parámetros a las mismas o eliminarlas.

Una transacción DSC exitosa cambia los parámetros de QoS de un flujo de servicio reemplazando tanto el conjunto de parámetros de QoS admitido como el activo. Si el mensaje contiene sólo el conjunto admitido, el conjunto activo se fija a nulo y se desactiva el flujo. Si el mensaje no contiene ninguno de los conjuntos (se usa el valor "000" para el tipo de conjunto de parámetros de calidad de servicio, véase B.C.2.2.5.1), ambos conjuntos se fijan a nulo y se desadmite al flujo. Cuando el mensaje contiene ambos conjuntos de parámetros de QoS, se verifica primero el conjunto admitido y, de tener éxito el control de admisión, se comprueba el conjunto activo por comparación con el conjunto admitido del mensaje para asegurarse de que es un subconjunto (véase B.10.1.1.1). Si todas las verificaciones son exitosas, los conjuntos de parámetros de QoS del mensaje se convierten en los nuevos conjuntos de parámetros de QoS admitido y activo del flujo de servicio. Si falla cualquiera de las verificaciones, falla la transacción de DSC y los conjuntos de parámetros de QoS de flujo de servicio no se modifican.

B.10.2 Servicios de planificación de flujo de servicio ascendente

Las subcláusulas siguientes definen los servicios de planificación básicos de flujo de servicio y enumeran los parámetros de QoS asociados a cada servicio. En el anexo B.C se da una descripción en detalle de cada parámetro de QoS. En presente se analiza también cómo pueden combinarse estos servicios básicos y parámetros de QoS para formar nuevos servicios, por ejemplo, el servicio de velocidad de información concertada (CIR, *committed information rate*).

Los servicios de planificación están concebidos para mejorar la eficiencia del proceso de petición/concesión. Especificando un servicio de planificación y sus parámetros de QoS asociados, el CMTS puede prever las necesidades de caudal y latencia del tráfico en sentido ascendente, y proporcionar peticiones y/o concesiones en los momentos oportunos.

Cada servicio se adapta expresamente a un tipo específico de flujo de datos, según se describe a continuación. Los servicios básicos comprenden: servicio de concesión no solicitada (UGS, *unsolicited grant service*), servicio de interrogación secuencial en tiempo real (rtPS, *real-time polling service*), servicio de concesión no solicitada con detección de actividad (UGS-AD, *unsolicited grant service with activity detection*), servicio de interrogación secuencial no en tiempo real, (nrtPS, *non-real-time polling service*), y servicio de máximo esfuerzo (BE, *best effort*). En el cuadro B.10.4 se muestra la relación entre los servicios de planificación y los parámetros de QoS conexos.

B.10.2.1 Servicio de concesión no solicitada

El servicio de concesión no solicitada (UGS) está concebido para el soporte de flujos de servicio en tiempo real que generan paquetes de datos de tamaño fijo de forma periódica, por ejemplo, el protocolo de transmisión de la voz sobre el protocolo Internet (VoIP). Este servicio ofrece concesiones de tamaño fijo de forma periódica y en tiempo real, con lo cual se eliminan la tara y la latencia de las peticiones del CM y se asegura que las concesiones estarán disponibles para subvenir a las necesidades del flujo en tiempo real. El CMTS DEBE proporcionar al flujo de servicio concesiones de datos de tamaño fijo a intervalos periódicos. Para que este servicio funcione correctamente la política de petición/transmisión (véase B.C.2.2.6.3) DEBE ser tal que el CM tenga prohibido utilizar cualquier petición de contienda o de oportunidades de petición/datos, y el CMTS NO DEBE proporcionar oportunidad alguna de petición de unidifusión. La política de

petición/transmisión DEBE prohibir también las peticiones de porteo. Esto dará por resultado el que el CM utilice sólo concesiones de datos no solicitadas para la transmisión en sentido ascendente. Todos los demás bits de la política de petición/transmisión no interesan por lo que se refiere al funcionamiento básico del servicio de planificación, y deben fijarse conforme a la política de la red. Los parámetros clave de servicio son el tamaño de concesión no solicitada, el intervalo de concesión nominal, la fluctuación de fase de concesión tolerada y la política de petición/transmisión (véase el anexo B.M).

El encabezamiento de sincronización de concesión no solicitada (UGSH, *unsolicited grant synchronization header*) en el elemento EH de flujo de servicio (véase B.8.2.6.3.2) se utiliza para pasar información de estatus del CM al CMTS acerca del estado del flujo de servicio UGS. El bit más significativo del UGSH es el bit indicador de cola (QI, *queue indicator*). El CM DEBE fijar esta bandera cuando detecta que este flujo de servicio ha excedido su profundidad de cola de transmisión. Una vez que el CM detecta que la cola de transmisión del flujo de servicio ha vuelto a estar dentro de su límite, DEBE despejar la bandera QI. La bandera permite al CMTS compensar a largo plazo condiciones tales como diagramas perdidos o inadaptación de la velocidad de reloj emitiendo concesiones adicionales.

El CMTS NO DEBE atribuir más concesiones por intervalo de concesión nominal que el parámetro concesiones por intervalo del conjunto de parámetros de QoS activo, excepto cuando se haya fijado el bit de QI de UGSH. En tal caso el CMTS DEBERÍA asignar hasta un 1% adicional de anchura de banda para compensar la inadaptación de las velocidades de reloj. Si el CMTS concede anchura de banda adicional, DEBE limitar el número total de octetos que se reenvían por el flujo durante un intervalo de tiempo cualquiera a Max(T) tal como se describe en la expresión:

$$Max(T) = T \times (R \times 1{,}01) + 3B$$

donde:

Max(T)	el número máximo de octetos que se transmiten por el flujo durante el tiempo T (expresado en segundos),
R	(grant_size × grants_per_interval)/nominal_grant_interval, y
B	grant_size × grants_per_interval.

En servicio UGS se ignora el campo concesiones activas de UGSH. No hay cambios en el control del flujo de servicio ejercido por el CMTS.

B.10.2.2 Servicio de interrogación secuencial en tiempo real

El servicio de interrogación secuencial en tiempo real (rtPS) está concebido para el soporte de flujos de servicio en tiempo real que generan paquetes de datos de tamaño variable de forma periódica, por ejemplo, vídeo MPEG. El servicio ofrece oportunidades de petición de unidifusión periódicas y en tiempo real que cumplen con las necesidades en tiempo real del flujo y permiten al CM especificar el tamaño de la concesión deseada. Este servicio requiere una tara de petición mayor que el UGS pero es compatible con tamaños de concesión variables para obtener una eficiencia óptima del transporte de datos.

El CMTS DEBE proporcionar oportunidades periódicas de petición de unidifusión. Para que este servicio funcione correctamente la configuración de política de petición/transmisión (véase B.C.2.2.6.3) DEBERÍA ser tal que el CM tuviera prohibido utilizar cualquier oportunidad de petición de contienda o de petición/datos. La política de petición/transmisión también DEBERÍA prohibir las peticiones de porteo. El CMTS PUEDE emitir oportunidades de petición de unidifusión según lo prescribe este servicio, aún si hay una concesión pendiente. Esto dará como resultado el que el CM utilice sólo oportunidades de petición de unidifusión para obtener oportunidades de transmisión en sentido ascendente (el CM podría, con todo, utilizar también concesiones de datos no solicitadas para la transmisión en sentido ascendente). Todos los demás bits de la política de petición/transmisión no interesan por lo que se refiere al funcionamiento básico del servicio de

planificación, y deben fijarse conforme a la política de la red. Los parámetros clave de servicio son el intervalo de interrogación secuencial nominal, la fluctuación de fase de interrogación tolerada y la política de transmisión/petición.

B.10.2.3 Servicio de concesión no solicitada con detección de actividad

El servicio de concesión no solicitada con detección de actividad (UGS-AD) está concebido para el soporte de flujos UGS que pueden tornarse inactivos durante lapsos significativos de tiempo (es decir, decenas de milisegundos o incluso más), tales como el VoIP con supresión de silencios. El servicio proporciona concesiones no solicitadas cuando el flujo está activo e interrogaciones secuenciales de unidifusión cuando el flujo está inactivo. Así se combinan la tara baja y la latencia baja del UGS con la eficiencia del rtPS. Aunque USG-AD combina UGS con rtPS, no hay en ningún momento más que un solo servicio de planificación activo.

El CMTS DEBE proporcionar concesiones de unidifusión periódicas durante las cuales el flujo está activo, pero DEBE volver a proporcionar oportunidades de petición de unidifusión periódicas cuando el flujo esté inactivo. El CMTS puede detectar inactividad del flujo empleando concesiones no utilizadas. Sin embargo, el algoritmo para la detección del cambio de un flujo del estado activo al estado inactivo depende de la implementación del CMTS. Para que este servicio funcione correctamente, la configuración de la política de petición/transmisión (véase B.C.2.2.6.3) DEBE ser tal que el CM tenga prohibida la utilización de cualquier petición de contienda o de oportunidades de petición/datos. La política de petición/transmisión DEBE prohibir también las peticiones de porteo. Esto da como resultado que el CM utiliza sólo oportunidades de petición de unidifusión para obtener oportunidades de transmisión en sentido ascendente. Sin embargo, el CM utilizará también concesiones de datos no solicitadas para transmisiones en sentido ascendente. Todos los demás bits de la política de petición/transmisión no interesan por lo que se refiere al funcionamiento básico del servicio de planificación, y deben fijarse conforme a la política de la red. Los parámetros clave de servicio son el intervalo de interrogación secuencial nominal, la fluctuación de fase de interrogación secuencial tolerada, el intervalo de concesión nominal, la fluctuación de concesión tolerada, el tamaño de concesión no solicitada y la política de transmisión/petición.

En el servicio UGS-AD, cuando se reinicie el UGS tras un intervalo de rtPS, el CMTS DEBERÍA proporcionar concesiones adicionales en el primer (y/o segundo) intervalo de concesión de tal manera que el CM reciba en total una concesión por cada intervalo de concesión desde el momento en que el CM pidió que se reiniciara la UGS, y una concesión más. (Véase el anexo B.M). Puesto que el flujo de servicio es aprovisionado como un flujo UGS con intervalo de concesión y tamaño de concesión específicos, cuando se reinicia UGS el CM NO DEBE pedir una concesión de tamaño distinto que el flujo UGS ya aprovisionado. Al igual que para cualquier flujo de servicio, sólo se pueden solicitar cambios por medio de una instrucción DSC. Si la actividad reiniciada requiere más de una concesión por intervalo, el CM DEBE indicarlo en el campo concesiones activas del UGSH, comenzando por el primer paquete enviado.

El elemento encabezamiento ampliado de flujo de servicio permite al CM declarar dinámicamente cuántas concesiones por segundo se necesitan para soportar el número de flujos con actividad presente. En UGS-AD, el CM PUEDE usar el bit indicador de cola de UGSH. Los otros siete bits de UGSH definen el campo concesiones activas. Este campo define el número de concesiones dentro de un intervalo de concesión nominal que este flujo de servicio requiere en ese momento. Cuando se usa UGS-AD, el CM DEBE indicar el número de concesiones pedidas en este campo por intervalo de concesión nominal. El campo concesiones activas del UGSH se ignora con servicio UGS sin detección de actividad. Este campo permite al CM indicar al CMTS que ajuste dinámicamente el número de concesiones por intervalo que el flujo de servicio UGS está utilizando realmente. El CM NO DEBE pedir más que el número de concesiones por intervalo de ActiveQosParameterSet.

Si el CMTS atribuye anchura de banda adicional en respuesta al bit QI, DEBE usar la misma fórmula de limitación de la velocidad que UGS, pero la fórmula sólo se aplica a los periodos de estado estacionario cuando el CMTS ha ajustado las grants_per_interval para que concuerden con las active_grants pedidas por el CM.

Cuando el CM está recibiendo no solicitadas y no detecta actividad en el flujo de servicio, PUEDE enviar un paquete con el campo concesiones activas fijado a cero concesiones y a continuación cesar la transmisión. Puesto que quizás este paquete no sea recibido por el CMTS, el CM DEBE poder reiniciar la transmisión cuando el flujo de servicio pase de inactivo a activo, ya sea con peticiones secuenciadas o con concesiones no solicitadas.

B.10.2.4 Servicio de interrogación secuencial no en tiempo real

El servicio de interrogación secuencial no en tiempo real (nrtPS) está concebido para el soporte de flujos de servicio no en tiempo real que requieren concesiones de datos de tamaño variable de forma periódica, por ejemplo, FTP de gran anchura de banda. El servicio ofrece interrogaciones secuenciales de unidifusión de forma periódica, con lo que se asegura que el flujo recibe oportunidades de petición aún cuando la red esté congestionada. Es habitual que el CMTS interrogue secuencialmente a los SID de nrtPS a intervalos (periódicos o a periódicos) del orden de un segundo o menos.

El CMTS DEBE proporcionar oportunidades puntuales de petición de unidifusión. Para que este servicio funcione correctamente, la configuración de política de petición/transmisión (véase B.C.2.2.6.2) DEBERÍA ser tal que el CM pudiera utilizar oportunidades de petición de contienda. Esto dará como resultado que el CM utilice las oportunidades de petición de contienda así como las oportunidades de petición de unidifusión y las concesiones de datos no solicitadas. Todos los demás bits de la política de petición/transmisión no interesan por lo que se refiere al funcionamiento básico del servicio de planificación, y deben fijarse conforme a la política de la red. Los parámetros clave de servicio son el intervalo de interrogación nominal, la mínima velocidad de tráfico reservada, la máxima velocidad de tráfico continuo, la política de petición/transmisión y la prioridad de tráfico.

B.10.2.5 Servicio de máximo esfuerzo

La finalidad del servicio de máximo esfuerzo (BE) es la de proveer un servicio eficiente al tráfico del máximo esfuerzo. Para que este servicio funcione correctamente la configuración de la política de petición/transmisión DEBERÍA ser tal que el CM pudiera utilizar oportunidades de petición de contienda. Esto dará como resultado el que el CM utilice las oportunidades de petición de contienda así como las oportunidades de petición de unidifusión y las concesiones de datos no solicitadas. Todos los demás bits de la política de petición/transmisión no interesan por lo que se refieren al funcionamiento básico del servicio de planificación, y deben fijarse conforme a la política de la red. Los parámetros clave de servicio son la mínima velocidad de tráfico reservada, la máxima velocidad de tráfico continuo y la prioridad de tráfico.

B.10.2.6 Otros servicios

B.10.2.6.1 Velocidad de información concertada (CIR)

El servicio de velocidad de información concertada (CIR) se puede definir de varias maneras. Por ejemplo, podría configurarse utilizando un servicio de máximo esfuerzo con una mínima velocidad de tráfico reservada o un nrtPS con una mínima velocidad de tráfico reservada.

B.10.2.7 Aplicabilidad de parámetros a la planificación de servicio en sentido ascendente

En el cuadro B.10-4 se resume la relación entre los servicios de planificación y los parámetros clave de QoS. En el anexo B.C se da una descripción detallada de cada uno de los parámetros de QoS.

Cuadro B.10-4/J.112 – Aplicabilidad de parámetros a la planificación de servicio en sentido ascendente

Parámetro de flujo de servicio	Máximo esfuerzo	Interrogación secuencial no en tiempo real	Interrogación secuencial en tiempo real	Concesión no solicitada	Concesión no solicitada con detección de actividad
Varios					
• Prioridad de tráfico	Opcional Por defecto = 0	Opcional Por defecto = 0	N/A[a)]	N/A	N/A
• Ráfaga concatenada máxima	Opcional	Opcional	Opcional	N/A	N/A
• Tipo de servicio de planificación en sentido ascendente	Opcional Por defecto = 2	Obligatorio	Obligatorio	Obligatorio	Obligatorio
• Política de petición/transmisión	Opcional Por defecto = 0	Obligatorio	Obligatorio	Obligatorio	Obligatorio
Velocidad máxima					
• Máxima velocidad de tráfico continuo	Opcional Por defecto = 0	Opcional Por defecto = 0	Opcional Por defecto = 0	N/A	N/A
• Máxima ráfaga de tráfico	Opcional Por defecto = 1522	Opcional Por defecto = 1522	Opcional Por defecto = 1522	N/A	N/A
Velocidad mínima					
• Mínima velocidad de tráfico reservada	Opcional Por defecto = 0	Opcional Por defecto = 0	Opcional Por defecto = 0	N/A	N/A
• Tamaño de paquete mínimo supuesto	Opcional[c)]	Opcional[c)]	Opcional[c)]	Opcional[c)]	Opcional[c)]
Concesiones					
• Tamaño de concesión no solicitada	N/A	N/A	N/A	Obligatorio	Obligatorio
• Concesiones por intervalo	N/A	N/A	N/A	Obligatorio	Obligatorio
• Intervalo de concesión nominal	N/A	N/A	N/A	Obligatorio	Obligatorio
• Fluctuación de concesión tolerada	N/A	N/A	N/A	Obligatorio	Obligatorio

Cuadro B.10-4/J.112 – Aplicabilidad de parámetros a la planificación de servicio en sentido ascendente

Parámetro de flujo de servicio	Máximo esfuerzo	Interrogación secuencial no en tiempo real	Interrogación secuencial en tiempo real	Concesión no solicitada	Concesión no solicitada con detección de actividad
Interrogaciones secuenciales					
• Intervalo de interrogación secuencial nominal	N/A	Opcional[c)]	Obligatorio	N/A	Opcional[b)]
• Fluctuación de interrogación secuencial tolerada	N/A	N/A	Opcional[c)]	N/A	Opcional[c)]

a) N/A significa que no se aplica a este tipo de planificación de flujo de servicio. Si se incluye en una petición de flujo de servicio de este tipo de planificación de flujo de servicio, DEBE rechazarse esta petición.

b) El valor por defecto es el mismo que el intervalo de concesión nominal.

c) El valor por defecto es específico de cada CMTS.

B.10.2.8 Comportamiento de transmisión del CM

Para que estos servicios funcionen correctamente lo único que se pide al CM en lo que hace a su comportamiento de transmisión para un flujo de servicio es que siga las reglas establecidas en B.9.4.3 y la política de petición/transmisión especificada para el flujo de servicio.

B.10.3 Fragmentación

La fragmentación es una "capacidad de módem" del CM en sentido ascendente. El CMTS DEBE habilitar o inhabilitar esta capacidad módem por módem con TLV en la respuesta de registro. La base módem por módem es la que da la compatibilidad con los CM de DOCSIS 1.0. Una vez habilitada la fragmentación para un módem DOCSIS 1.1 se habilita la fragmentación para cada flujo de servicio por medio de la configuración de política de petición/transmisión. Cuando se habilita para un flujo de servicio, la fragmentación es iniciada por el CMTS al conceder anchura de banda a un determinado CM con un tamaño de concesión menor al de la petición correspondiente de anchura de banda del CM. Esto se conoce como **concesión parcial**.

B.10.3.1 Soporte de fragmentación de CM

La fragmentación es, en esencia, la encapsulación de una parte de la trama MAC dentro de un encabezamiento de fragmentación de tamaño fijo y una CRC de fragmento. Las PDU concatenadas así como las PDU únicas son encapsuladas de la misma manera. Si la privacidad básica está habilitada, se la aplica en cada fragmento, a diferencia de la trama MAC original completa.

El CM DEBE realizar la fragmentación según el diagrama de flujo de la figura B.10-8. La expresión "porción no transmitida del paquete" del diagrama de flujo se refiere a toda la trama MAC cuando no se ha iniciado ola fragmentación y al tramo no transmitido restante de la trama MAC original cuando se ha iniciado la fragmentación.

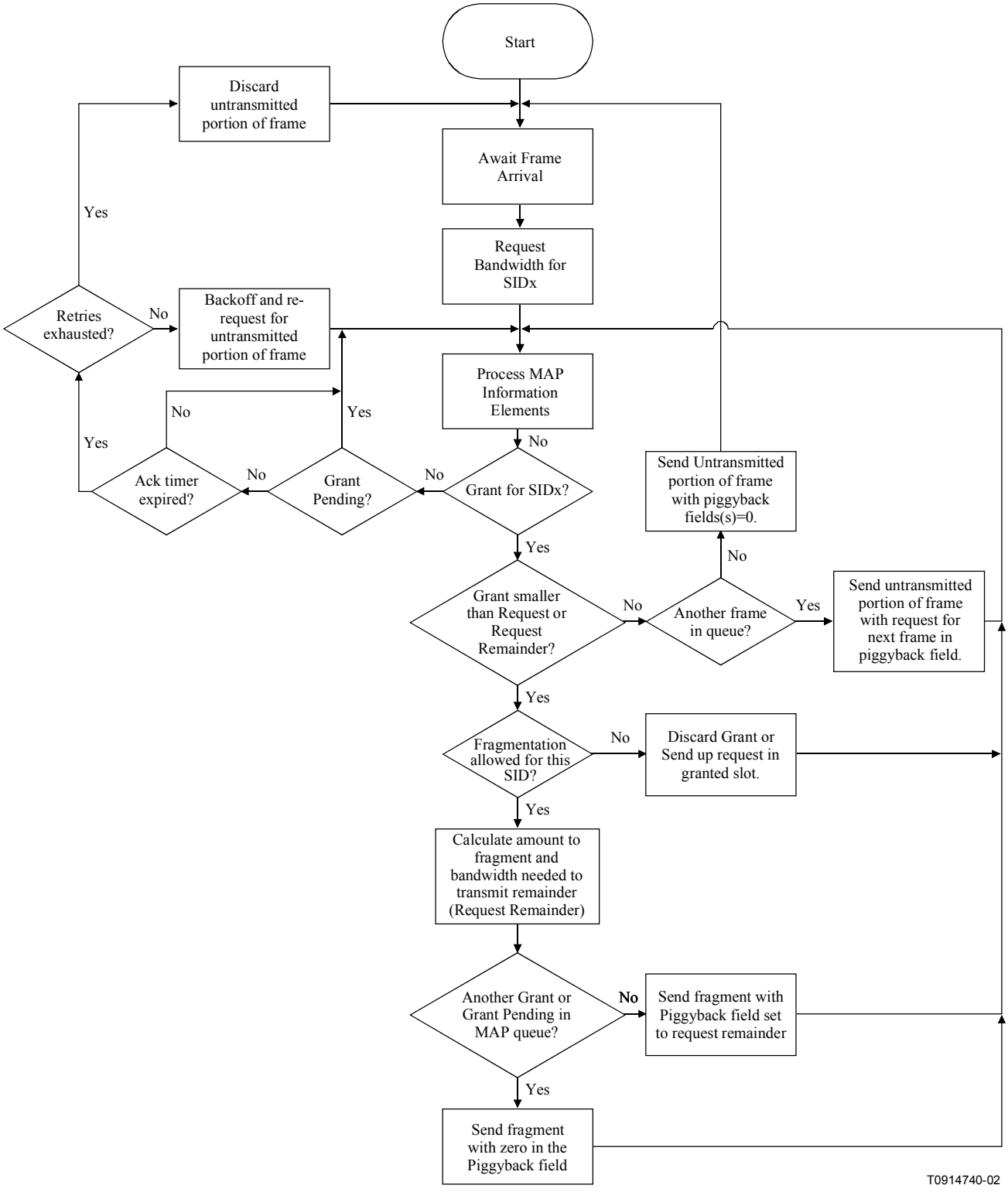


Figura B.10-8/J.112 – Diagrama de flujo de fragmentación de CM

B.10.3.1.1 Reglas de la fragmentación

1) Cada vez que se habilita la fragmentación y el tamaño de la concesión es menor que lo pedido, el CM DEBE llenar la concesión parcial que recibe con la máxima cantidad de datos (cabida útil fragmentada) posible, teniendo en cuenta la tara de fragmentación y la tara de capa física.
2) El CM DEBE enviar una petición de porteo siempre que no haya una concesión posterior o una concesión pendiente para ese SID en los diagramas de atribución recibidos en el CM.
3) Si el CM está fragmentando una trama, cualquier petición de porteo DEBE ser realizada en el tramo EHDR de BPI del encabezamiento del fragmento.
4) Al calcular las peticiones de anchura de banda para el resto de la trama (trama concatenada, si es que es concatenada) que ha sido fragmentado, el CM DEBE pedir suficiente anchura de banda como para transmitir el resto completo de la trama y además la tara del fragmento de 16 octetos así como toda la tara de capa física asociada.
5) Si el CM no recibe una concesión o una concesión pendiente dentro del tiempo ACK de envío de una petición, DEBE retroceder y volver a emitir una petición de la parte no transmitida de la trama hasta que se le conceda la anchura de banda o el CM exceda su umbral de reintentos.
6) Si el CM excede su umbral de reintentos mientras pide anchura de banda, descarta cualquier parte de la trama que no se haya transmitido previamente.
7) El CM DEBE fijar el bit F y liberar el bit L en el primer fragmento de una trama.
8) El CM DEBE liberar los bits F y L del encabezamiento de fragmento de cualesquiera fragmentos que estén entre el primero y el último fragmento de una trama.
9) El CM DEBE fijar el bit L y liberar el bit F del último fragmento de una trama.
10) El CM DEBE incrementar el número de secuencia de fragmento de forma secuencial para cada fragmento de una trama transmitida.
11) Si se ha de criptar una trama y la trama está fragmentada, se cripta la trama sólo en la capa del fragmento con criptación empezando inmediatamente después de la HCS del encabezamiento del fragmento y continuando hasta la CRC del fragmento.
12) Las tramas enviadas en regiones de datos inmediatos (petición/datos) NO DEBEN ser fragmentadas.

NOTA – "Trama" se refiere siempre sea a tramas con una única PDU de paquete o a tramas concatenadas.

B.10.3.2 Soporte de fragmentación de CMTS

En el CMTS el fragmento se procesa de manera similar a un paquete corriente, con la excepción de que el encriptado de la privacidad básica comienza justo después del encabezamiento de fragmentación en lugar de estar desplazado 12 octetos.

El CMTS tiene dos modos de efectuar la fragmentación. En el modo concesiones múltiples se supone que el CMTS retiene el estado de la fragmentación. Este modo permite al CMTS tener pendientes múltiples concesiones parciales para cualquier SID dado. En el modo porteo se supone que el CMTS NO retiene ningún estado de fragmentación. Sólo hay una concesión parcial pendiente, por lo cual el CM inserta la cantidad restante en el campo porteo del encabezamiento de fragmento. El tipo de modo que se está utilizando lo determina el CMTS. En todos los casos el CM trabaja con un conjunto coherente de reglas.

B.10.3.2.1 Modo concesión múltiple

Un CMTS PUEDE soportar el modo de concesiones múltiples para la realización de la fragmentación.

El modo concesión múltiple permite al CMTS dividir una petición en dos o más concesiones en un único diagrama de atribución o en varios diagramas sucesivos, y la tara adicional necesaria se calcula en las concesiones parciales restantes para satisfacer la petición. Si, en el modo concesiones múltiples, el CMTS no puede conceder el resto del diagrama de atribución actual (MAP) en curso, DEBE enviar al CM una concesión pendiente (concesión de longitud cero) en el MAP actual y en todos los MAP subsiguientes hasta que pueda conceder anchura de banda adicional. Si no hay ninguna concesión o concesión pendiente en los diagramas de atribución subsiguientes, el CM DEBE pedir de nuevo el resto. Este mecanismo de repetición de la petición es el mismo que se usa cuando un REQ normal no recibe una concesión o una concesión pendiente en el plazo de tiempo del ACK.

Si un CM recibe un IE concesión pendiente junto con una concesión de fragmento, NO DEBE portear una petición en el encabezamiento ampliado del fragmento transmitido en dicha concesión.

Si el CM deje pasar una concesión y repita la petición de la anchura de banda restante, el CMTS DEBE recuperarse sin abandonar la trama.

Debido a la falta de precisión del proceso de conversión de miniintervalo de tiempo en octetos, es posible que el CMTS no sea capaz de calcular exactamente el número de miniintervalos adicionales necesarios para la tara de fragmentación. Además, puesto que es posible que un CM deje pasar un diagrama de atribución con una concesión parcial y esté pidiendo por el envío de un fragmento no enviado en lugar de una nueva PDU, el CMTS no puede estar seguro de si el CM ya ha contabilizado o no la tara de fragmentación en una petición. Por ello, el CMTS DEBE asegurarse de que cualquier resto de cabida útil fragmentada tiene una longitud de al menos un miniintervalo más que el número de miniintervalos necesarios para dar cabida a la tara de un fragmento (16 octetos) más la tara de capa física que hace falta para transmitir un fragmento de tamaño mínimo. No hacer esto puede ser causa de que el CMTS emita una concesión innecesaria al haber completado la transmisión del resto de la cabida útil fragmentada utilizando la concesión parcial anterior. Esto puede hacer que el CM salga del sincronismo con el CTMS al comenzar, sin advertirlo, una nueva fragmentación. El CMTS debe también hacer frente al hecho de que, para determinados conjuntos de parámetros de capa física, el CM puede pedir un miniintervalo más que el tamaño máximo de una concesión de datos corta sin necesitar en realidad tantos miniintervalos. Así ocurre cuando el CM necesita llevar el tamaño de la petición más allá del límite de la concesión de datos corta. El CMTS precisa de una política para asegurar que la fragmentación de tales peticiones en modo concesión múltiple no lleva a concesiones fragmentarias innecesarias.

B.10.3.2.2 Modo de porteo

Un CMTS PUEDE soportar el modo porteo para la realización de la fragmentación.

Si el CMTS no coloca otra concesión parcial o una concesión pendiente en el diagrama de atribución (MAP) en el cual inicia la fragmentación de un SID, el CM DEBE portear automáticamente el resto. El CM calcula la parte de una trama que se puede enviar en la anchura de banda atribuida y forma un fragmento para enviarla. El CM utiliza el campo porteo del encabezamiento ampliado del fragmento para pedir la anchura de banda necesaria para transferir el resto de la trama. Puesto que el CMTS no indicó una concesión múltiple en el diagrama de atribución de anchura de banda del primer fragmento, el CM DEBE llevar la cuenta del resto que hay que enviar. La longitud de la petición para el resto de la trama original, incluyendo la tara de capa física y de fragmentación, es insertada en el octeto de petición de porteo del encabezamiento de fragmentación.

Si la HCS del fragmento es correcta, la petición porteada, de estar presente, se pasa al proceso de atribución de anchura de banda mientras que el fragmento en sí es puesto en cola para el reensamblado. Una vez reensamblada la trama MAC completa, se procesan los encabezamientos ampliados de no privacidad que existieran si la HCS del paquete es correcta y el paquete es reenviado al destino correcto.

B.10.3.3 Ejemplo de fragmentación

B.10.3.3.1 Fragmentación de un único paquete

Véase la figura B.10-8. Supóngase que se ha habilitado la fragmentación para un determinado SID.

1) (Petición de estado) – El CM desea transmitir un paquete de 1018 octetos. El CM calcula cuánta tara de capa física (POH, *physical layer overhead*) se necesita y pide el número apropiado de miniintervalos. El CM realiza una petición en una región de contienda. Ir al paso 2).

2) (Espera de la concesión) – El CM supervisa los MAP buscando una concesión o una concesión pendiente para este SID. Si el tiempo límite de ACK del CM se agota antes que el CM reciba una concesión o una concesión pendiente, el CM reintenta la petición del paquete hasta agotar el número permitido de reintentos. A continuación el CM abandona ese paquete. Ir al paso 3).

3) (Primer fragmento) – Antes del abandono del paso 2), el CM ve una concesión para este SID que es inferior al número pedido de miniintervalos. El CM calcula cuánta información MAC se puede enviar con el número concedido de miniintervalos utilizando el perfil de ráfaga especificado. En el ejemplo de la figura B.10-9, la primera concesión puede contener 900 octetos luego de restar la POH. Como la tara del fragmento (FRAG HDR, FHCS, y FCRC) es de 16 octetos, se pueden transportar 884 octetos en el fragmento. El CM crea un fragmento compuesto por el FRAG HDR, FHCS, 884 octetos del paquete original y una FCRC. El CM marca al fragmento como primero y se prepara para enviar el fragmento. Ir al paso 4).

4) (Primer fragmento, modo concesión múltiple) – El CM mira para ver si hay otras concesiones o concesiones pendientes en cola para este SID. Si es así, envía el fragmento con el campo porteo de FRAG HDR puesto a cero, y espera a que llegue el momento de la concesión subsiguiente. Ir al paso 6). Si no hay concesiones o concesiones pendientes, ir al paso 5).

5) (Primer fragmento, modo porteo) – Si no hay más concesiones o concesiones pendientes para este SID en este MAP, el CM calcula cuántos miniintervalos se necesitan para enviar el resto del paquete fragmentado, incluida la tara de fragmentación y la tara de capa física, e inserta esta cantidad en el campo porteo de FRAG HDR. El CM envía a continuación el fragmento y arranca su temporizador de ACK para la petición de porteo. En el ejemplo de la figura B.10-9 el CM envía en sentido ascendente una petición de miniintervalos suficientes para contener la POH y otros 150 octetos (1018 – 884 + 16). Ir al paso 6).

6) (Espera de concesión) – El CM está ahora esperando una concesión para el fragmento siguiente. Si el temporizador de ACK del CM expira mientras está esperando esta concesión, el CM deberá enviar una petición de miniintervalos suficientes para enviar el resto del paquete fragmentado, incluyendo la tara de fragmentación y la tara de capa física. Ir al paso 7).

7) (Recepción de la concesión del fragmento siguiente) – Antes de abandonar en el paso 6), el CM ve otra concesión para este SID. El CM comprueba que si el tamaño de la concesión es suficiente para contener el resto del paquete fragmentado, incluida la tara de fragmentación y la tara de capa física. Si es así, ir al paso 10). Si no, ir al paso 8).

8) (Fragmento intermedio, modo concesión múltiple) – Puesto que el resto del paquete (más la tara) no cabe en la concesión, el CM calcula la parte que sí cabrá. El CM encapsula esta parte del paquete como un fragmento intermedio. El CM busca luego cualesquiera otras concesiones o concesiones pendientes en cola para este SID. Si están presentes unas u otras, el CM envía el fragmento con el campo porteo de FRAG HDR puesto a cero, y espera a que llegue el momento de la concesión subsiguiente. Ir al paso 6). Si no hay concesiones o concesiones pendientes, ir al paso 9).

9) (Fragmento del medio, modo porteo) – El CM calcula cuántos miniintervalos se necesitan para enviar el resto del paquete fragmentado, incluida la tara de fragmentación y la tara de capa física, e inserta esta cantidad en el campo porteo de FRAG HDR. El CM envía a continuación el fragmento y arranca su temporizador de ACK para la petición de porteo. Ir al paso 6).

10) (Último fragmento) – El CM encapsula el resto del paquete como un último fragmento. Si no hay ningún otro paquete en cola o si hay otra concesión u otra concesión pendiente en cola para este SID, el CM pone un cero en el campo REQ de FRAG HDR. Si hay otro paquete en cola sin concesión o sin concesión pendiente, el CM calcula el número de miniintervalos necesarios para enviar el paquete siguiente y coloca este número en el campo REQ de FRAG HDR. El CM transmite luego este paquete. Ir al paso 11). En el ejemplo de la figura B.10-9 la concesión es lo suficientemente grande para contener los 150 octetos restantes más la POH.

11) (Funcionamiento normal) – El CM vuelve al funcionamiento normal de espera de concesiones y petición de paquetes. Si en algún momento se habilita la fragmentación y llega una concesión que es menor que la petición, el proceso de fragmentación empieza de nuevo en el paso 2).

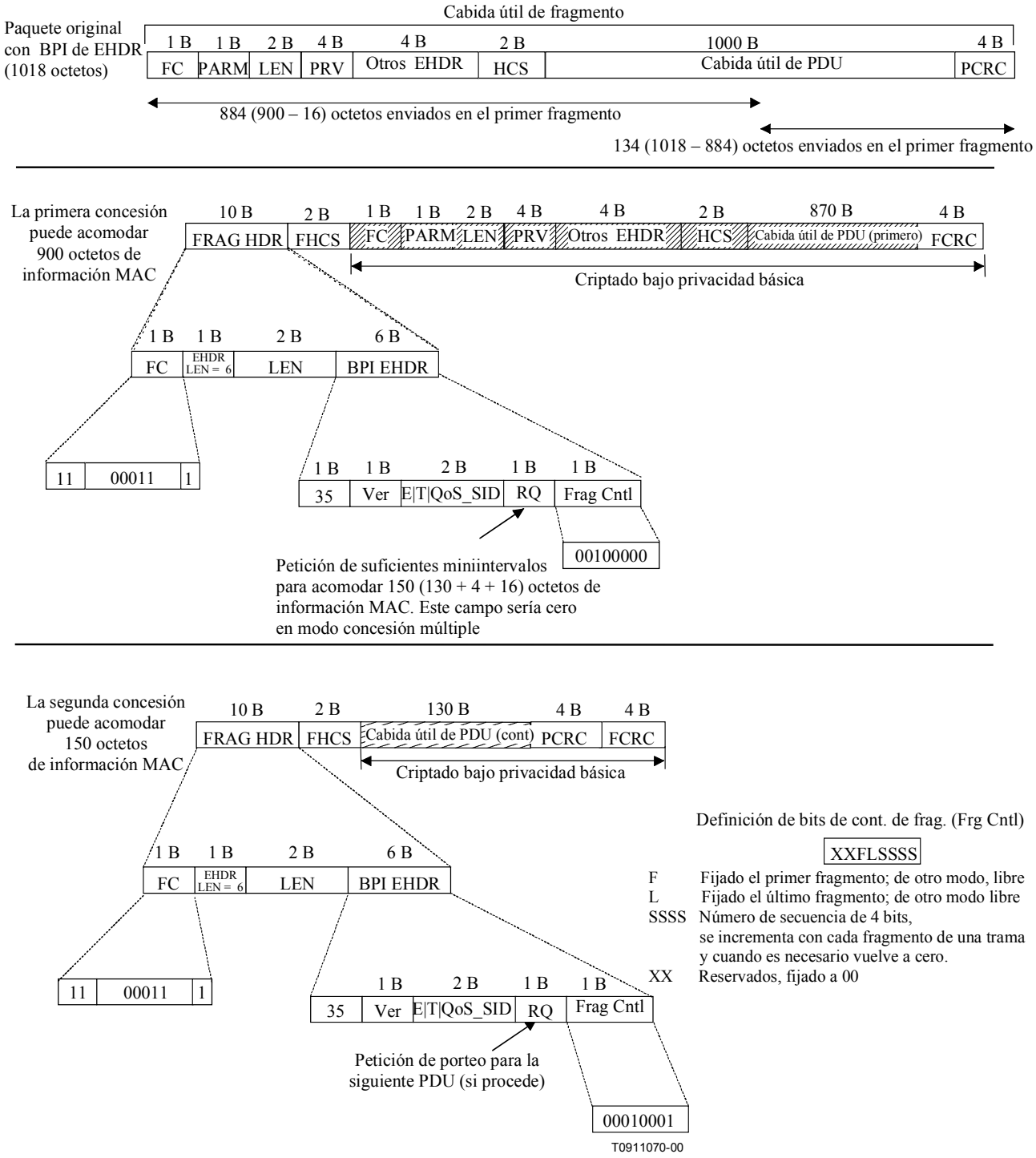


Figura B.10-9/J.112 – Ejemplo de fragmentación de un único paquete

B.10.3.3.2 Fragmentación de paquete concatenado

Una vez que el CM ha creado el paquete concatenado, le trata como una PDU única. En la figura B.10-10 se muestra un ejemplo de paquete concatenado dividido en tres fragmentos. Obsérvese que el paquete se fragmenta sin tomar en cuenta los límites de los paquetes dentro del paquete concatenado.

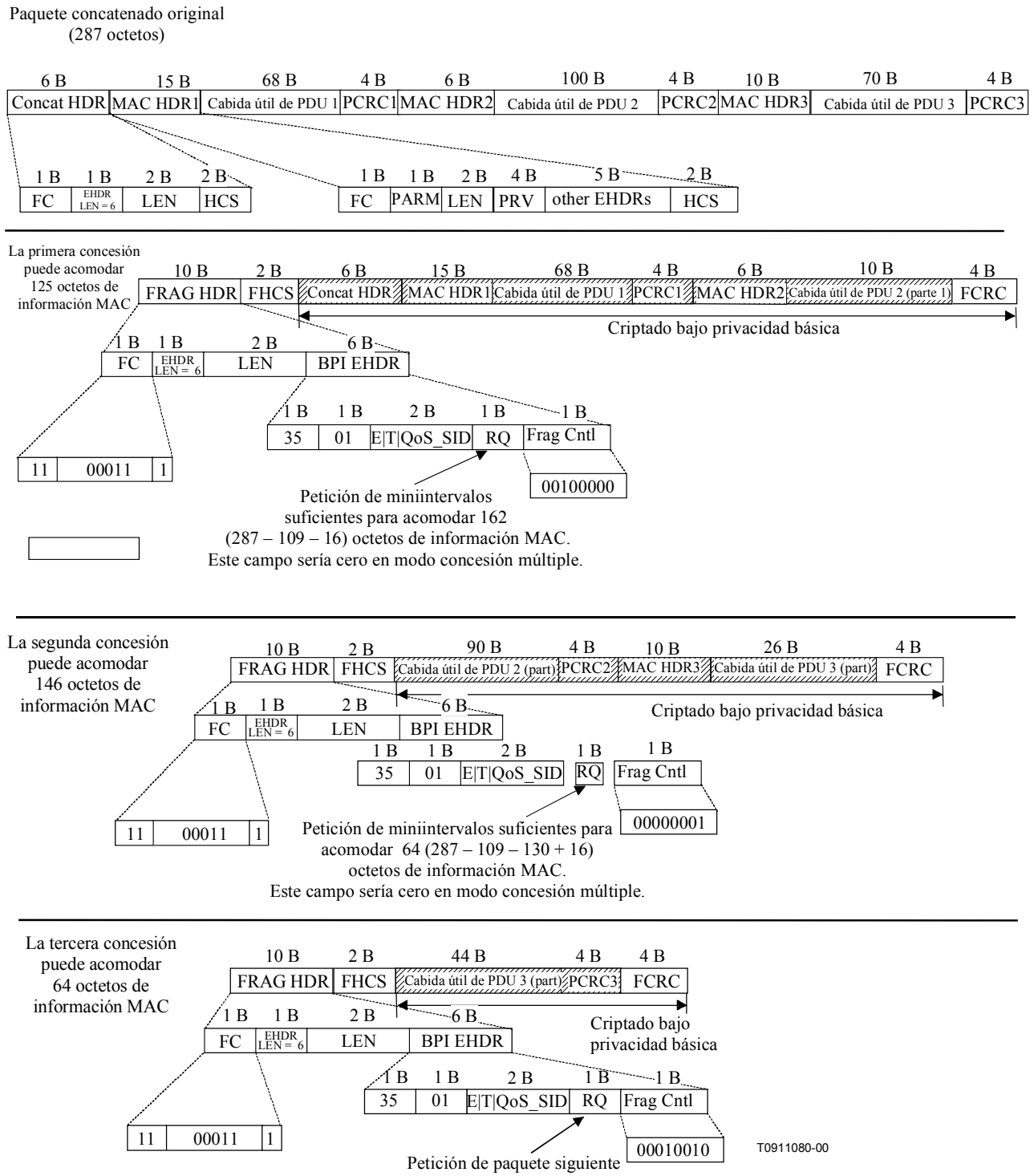


Figura B.10-10/J.112 – Ejemplo de paquete concatenado fragmentado

B.10.4 Supresión de encabezamiento de cabida útil

En la subcláusula B.10.4.1 (Visión de conjunto) se explican los principios de la supresión de encabezamiento de cabida útil. En las subcláusulas que siguen se explica la señalización de inicialización, funcionamiento y terminación. Para finalizar se presentan ejemplos específicos con trayectoria ascendente y descendente. Se utilizan las siguientes definiciones:

B.10.4-a PHS – *Supresión de encabezamiento de cabida útil*: Supresión de una cadena de octetos inicial en el emisor y restaurar la cadena de octetos en el destinatario.

B.10.4-b Regla PHS – *Regla de supresión de encabezamiento de cabida útil*: Conjunto de tuplas TLV aplicables a un determinado índice PHS.

B.10.4-c PHSF – *Campo supresión de encabezamiento de cabida útil*: Cadena de octetos que representan la parte encabezamiento de una PDU en la que uno o más octetos serán suprimidos (es decir, una instantánea del encabezamiento no comprimido de la PDU que incluye los octetos suprimidos y los no suprimidos).

B.10.4-d PHSI – *Índice de supresión de encabezamiento de cabida útil*: Un valor de 8 bits que hace referencia a la cadena de octetos suprimidos.

B.10.4-e PHSM – *Plantilla de supresión de encabezamiento de cabida útil*: Una plantilla (máscara) de bits que indica qué octetos del PHSF se suprimen y qué octetos no se suprimen.

B.10.4-f PHSS – *Tamaño de la supresión de encabezamiento de cabida útil*: Longitud en octetos del campo suprimido. Este valor es equivalente al número de octetos del PHSF y también al número de bits válidos en la PHSM.

B.10.4-g PHSV – *Verificación de la supresión de encabezamiento de cabida útil*: Bandera que indica a la entidad emisora que verifique todos los octetos que han de ser suprimidos.

B.10.4.1 Visión de conjunto

Cuando se trabaja con supresión de encabezamiento de cabida útil, la entidad emisora suprime una parte repetitiva de los encabezamientos de cabida útil que siguen al campo encabezamiento ampliado, mientras que la entidad receptora la restaura. En el sentido ascendente, la entidad emisora es el CM y la entidad receptora es el CMTS. En el sentido descendente la entidad emisora es el CMTS y la entidad receptora es el CM. El encabezamiento MAC ampliado contiene un índice de supresión de encabezamiento de cabida útil (PHSI) que hace referencia al campo de supresión de encabezamiento de cabida útil (PHSF).

Aunque se puede emplear PHS con cualquier tipo de flujo de servicio, ha sido concebido para su utilización con el tipo de planificación servicio de concesión no solicitada (UGS). UGS funciona con la mayor eficiencia con paquetes de longitud fija. PHS trabaja bien con UGS porque, a diferencia de otros sistemas de compresión de encabezamiento que a veces se utilizan con datos IP, PHS siempre suprime el mismo número de octetos en cada paquete. PHS generará siempre un encabezamiento de paquete comprimido y de longitud fija.

La entidad emisora utiliza clasificadores para atribuir paquetes a un flujo de servicio. El clasificador establece una correspondencia unívoca entre paquetes y su regla de supresión de encabezamiento de cabida útil asociada. La entidad receptora utiliza el identificador de servicio (SID) (véase la nota) y el PHSI para restaurar la PHSR.

Una vez que se conocen los campos PHSF y PHSS de una regla, se considera que la regla está "plenamente definida" y ninguno de sus campos puede ser modificado. Si se desea un funcionamiento modificado de la PHS para paquetes clasificados como pertenecientes al flujo, se debe eliminar la regla antigua del flujo de servicio e instalar una regla nueva.

Cuando se suprime un clasificador se DEBE suprimir también cualquier regla PHS asociada.

La PHS tiene una opción PHSV de verificación o no de la cabida útil antes de suprimirla. Tiene también una opción PHSM para permitir que determinados octetos no sean suprimidos. Esto se usa para enviar octetos que cambian, tales como números de secuencia IP, y suprimir de todos modos los octetos que no cambian.

Las reglas PHS son coherentes para todos los tipos de servicios de planificación. Las peticiones y concesiones de anchura de banda se especifican luego de haber tomado en cuenta la supresión. Para los servicios de concesión no solicitada se elige un tamaño de concesión con tupla TLV de tamaño

de concesión no solicitada. El paquete con su encabezamiento suprimido puede ser de tamaño igual o menor que la concesión.

El CMTS DEBE asignar todos los valores PHSI, al igual que asigna todos los valores SID. Tanto la entidad emisora como la receptora PUEDEN especificar el PHSF y el PHSS. Esta regla hace posibles los encabezamientos preconfigurados, o bien que protocolos de señalización de nivel más alto y que quedan fuera del alcance de este anexo B puedan establecer entradas de memoria. La PHS está pensada para servicio de unidifusión y no está definida para servicio de multidifusión.

Corresponde a la entidad de servicio de la capa más elevada generar una regla PHS que identifique de manera exclusiva al encabezamiento suprimido dentro del flujo de servicio. También es de la responsabilidad de esa entidad garantizar que las cadenas de octetos que se suprimen son constantes de un paquete a otro mientras dura el flujo de servicio activo.

B.10.4.2 Ejemplos de aplicación

- Un clasificador en un flujo de servicio en sentido ascendente que define de forma única un flujo de voz sobre el protocolo Internet (VoIP, *voice-over-IP*) especificando el tipo de protocolo de UDP, SA de IP, DA de IP, puerto de origen de UDP, puerto de destino de UDP, la referencia del flujo de servicio y un tamaño de PHS de 42 octetos. Una regla PHS hace referencia a este clasificador proporcionando un valor PHSI que identifica a este flujo de medio de VoIP. Para el caso del sentido ascendente, se verifican y suprimen 42 octetos de encabezamiento de cabida útil y se agrega a cada paquete en ese flujo de medios un encabezamiento ampliado de 2 octetos que contiene el PHSI.
- Un clasificador que identifica a los paquetes de un flujo de servicio, de los cuales el 90% concuerda con la PHSR. La verificación es habilitada. Esto puede aplicarse en una situación de compresión de paquetes en la que cada cierto tiempo se realizan reajustes de la compresión y se varía el encabezamiento. En este ejemplo, el algoritmo de programación permitiría una anchura de banda variable, y sólo al 90% de los paquetes se les suprimiría el encabezamiento. Puesto que la existencia del encabezamiento ampliado del PHSI indicará la elección realizada, una simple consulta del SID/PHSI en la entidad receptora dará siempre el resultado correcto.
- Un clasificador en un flujo de servicio en sentido ascendente que identifica a todos los paquetes IP especificando el Ethertype del IP, el ID del flujo de servicio, un PHSS de 14 octetos, y la no verificación por parte de la entidad emisora. En este ejemplo el CMTS ha decidido encaminar el paquete y sabe que no necesitará los primeros 14 octetos del encabezamiento Ethernet incluso aunque algunas partes, tales como la dirección de origen o la dirección de destino, puedan variar. El CM elimina 14 octetos de cada una de las tramas en sentido ascendente (encabezamiento Ethernet) sin verificar su contenido, y retransmite la trama al flujo de servicio.

B.10.4.3 Funcionamiento

A fin de aclarar el flujo de paquetes operativo, en la presente cláusula se describe una implementación. Las implementaciones particulares de CM y CMTS tienen libertad para efectuar la supresión de encabezamiento de cabida útil de cualquier manera, siempre que se respete el protocolo especificado en esta cláusula. En la figura B.10-11 se ilustra el procedimiento que se indica a continuación.

Se envía un paquete a la capa de servicio MAC del CM. El CM aplica su lista de reglas de clasificador. Si se encuentra una concordancia con la regla, ello resultará en un flujo de servicio ascendente, un SID y una regla PHS. La regla PHS proporciona PHSF, PHSI, PHSM, PHSS y PHSV. Si PHSV está fijado o no está presente, el CM comparará los octetos del encabezamiento del paquete con los octetos del PHSF que se han de suprimir según lo indicado por la PHSM. Si concuerdan, el CM suprimirá todos los octetos del campo supresión en sentido ascendente, a excepción de los octetos enmascarados por la PHSM. El CM insertará entonces el PHSI en el campo

PHS_Parm del elemento EH de flujo de servicio y pondrá el paquete en cola en el flujo de servicio en sentido ascendente.

Cuando el CMTS reciba el paquete, determinará el SID asociado ya sea por medios internos o a partir de otros elementos de encabezamientos ampliados tales como el encabezamiento ampliado de BPI. El CMTS utiliza el SID y el PHSI para buscar PHSF, PHSM y PHSS. Reensambla el paquete y continúa con el procesamiento normal de paquetes. El paquete reensamblado contendrá octetos del PHSF. Si la verificación estaba habilitada, los octetos del PHSF serán iguales a los octetos del encabezamiento original. Si la verificación no estaba habilitada no hay garantía alguna de que los octetos del PHSF concuerden con los octetos del encabezamiento original.

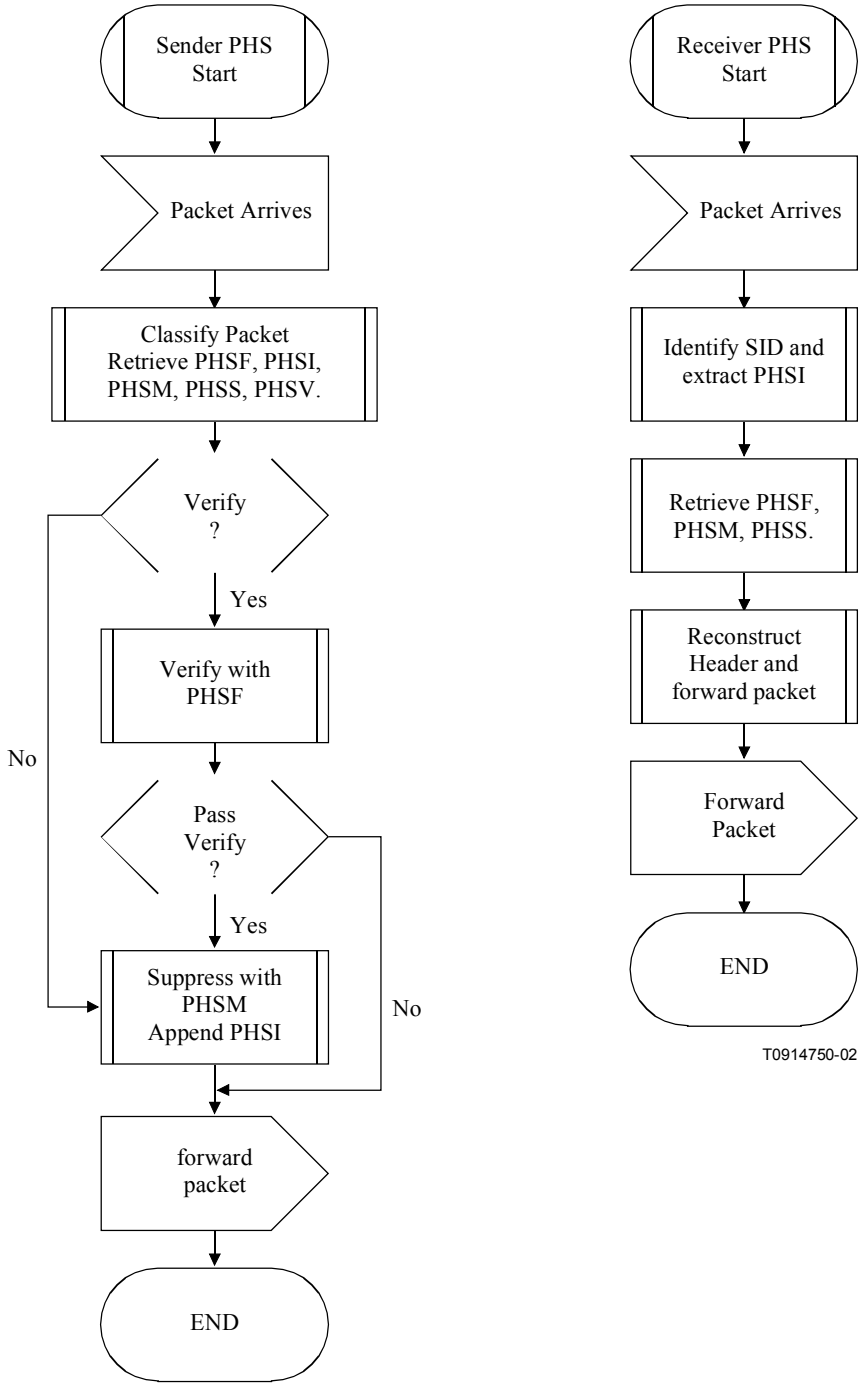


Figura B.10-11/J.112 – Operación de supresión de encabezamiento de cabida útil

En el flujo descendente se realiza una operación similar. El CMTS aplica su lista de clasificadores. Una concordancia con el clasificador resultará en un flujo de servicio descendente y una regla PHS. La regla PHS proporciona PHSF, PHSI, PHSM, PHSS, y PHSV. Si PHSV se fija a cero, o no está presente, el CMTS verificará el campo supresión en sentido descendente del paquete con el PHSF. Si concuerdan, el CMTS suprimirá todos los octetos del campo supresión en sentido descendente, a excepción de los octetos enmascarados por la PHSM. El CMTS insertará entonces el PHSI en el campo PHS_Parm del elemento EH de flujo de servicio y pondrá el paquete en cola en el flujo de servicio en sentido descendente.

El CM recibirá el paquete en base al filtrado de dirección de destino Ethernet. El CM utiliza entonces el PHSI para buscar PHSF, PHSM, y PHSS. El CM reensambla el paquete y continúa con el procesamiento normal de paquetes.

En la figura B.10-12 se muestra la supresión del paquete y su restauración cuando se utiliza enmascaramiento de PHS. El enmascaramiento sólo permite suprimir los octetos que no cambian. Se señala que PHSF y PHSM abarcan todo el campo supresión, incluidos los octetos suprimidos y los no suprimidos.

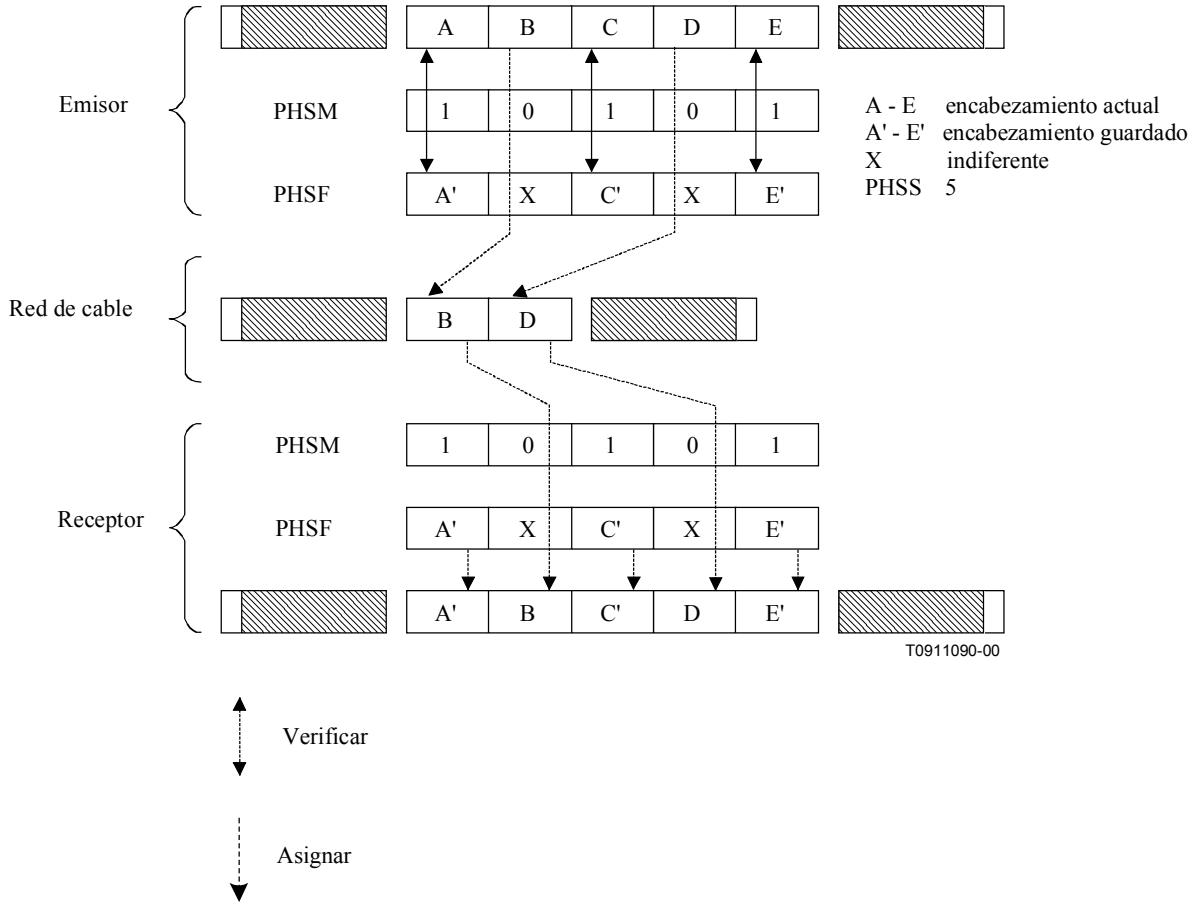


Figura B.10-12/J.112 – Supresión de encabezamiento de cabida útil con enmascaramiento

B.10.4.4 Señalización

La supresión de encabezamiento de cabida útil requiere la creación de tres objetos:

- Flujo de servicio.
- Clasificador.
- Regla de supresión de encabezamiento de cabida útil.

Estos tres objetos PUEDEN ser creados en flujos de mensaje separados o PUEDEN ser creados simultáneamente.

Las reglas PHS se crean con mensajes de registro, DSA o DSC. El CMTS DEBE definir el PHSI cuando se crea la regla PHS. Las reglas PHS se eliminan con mensajes DSA o DSC. El CM o el CMTS PUEDEN definir PHSS y PHSF.

En la figura B.10-13 se muestran dos maneras de señalizar la creación de una regla PHS.

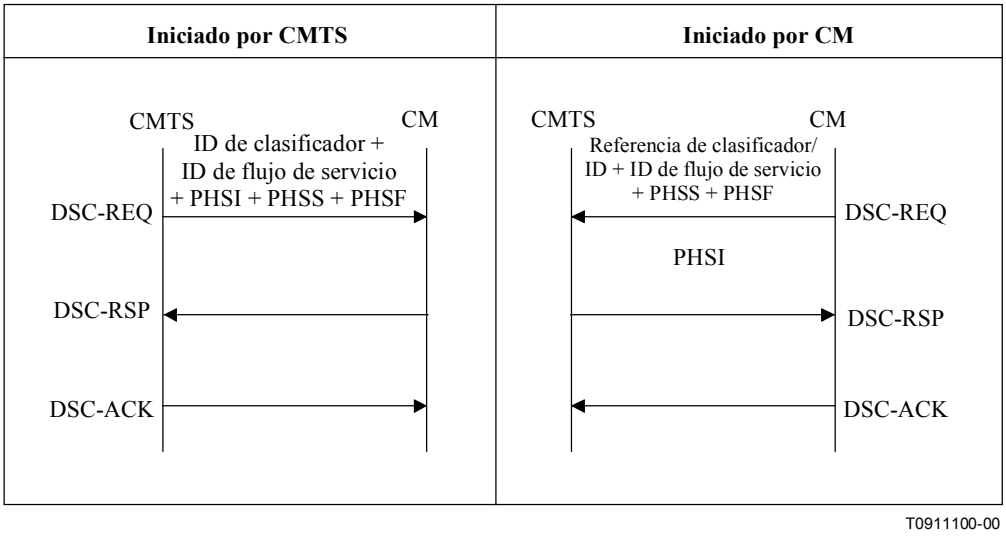


Figura B.10-13/J.112 – Ejemplo de señalización de supresión de encabezamiento de cabida útil

Es posible definir parcialmente una regla PHS (en particular, el tamaño de la regla) en el momento en que se crea un flujo de servicio.

Por ejemplo, es probable que cuando recién se aprovisiona un flujo de servicio, se conozca el tamaño del campo encabezamiento. Los valores de algunos elementos dentro del campo (por ejemplo, direcciones IP, números de puerto UDP, etc.) pueden no ser conocidos y se aprovisionarían en un DSC subsiguiente como parte de la activación del flujo de servicio (utilizando la acción DSC "Fijar regla PHS").

Una regla PHS estará parcialmente definida cuando los valores de los campos PHSF y PHSS sean ambos desconocidos. Una vez conocidos tanto PHSF como PHSS, se considera que la regla está plenamente definida y NO DEBE ser modificada por medio de la señalización DSC. Los campos PHSV y PHSM tienen valores por defecto; por lo tanto, no son necesarios para definir plenamente una regla PHS. Si PHSV y PHSM son desconocidos cuando se define plenamente la regla, se utilizan sus valores por defecto, y NO DEBEN ser modificados por medio de la señalización DSC.

Cada paso de la definición de la regla PHS, ya sea una petición de registro, DSA, o DSC, DEBE contener ID de flujo de servicio (o referencia), ID de clasificador (o referencia) a fin de identificar de modo unívoco la regla PHS que se define. Se utiliza un par constituido por un índice PHS y un ID de servicio para identificar de manera unívoca la regla PHS durante la transferencia de un paquete en sentido ascendente. Basta con un índice PHS para identificar de manera exclusiva la regla PHS utilizada en la transferencia de paquetes en sentido descendente.

B.10.4.5 Ejemplos de supresión de encabezamiento de cabida útil

B.10.4.5.1 Ejemplo en sentido ascendente

Se establece una clase de servicio con nombre de clase de servicio "G711-US-UGS-HS-42", destinada a tráfico VoIP en sentido ascendente conforme a UIT-T G.711 con servicio de concesión no solicitada. Cuando se agregan clasificadores al flujo, se incluye un valor PHSS de 42 que indica explícitamente que los primeros 42 octetos que siguen al encabezamiento ampliado MAC de todos los paquetes de dicho flujo deben ser verificados, suprimidos y restablecidos. En el presente ejemplo se configura la clase de servicio de modo tal que si un paquete cualquiera que no pasa la verificación, no se suprimirá su encabezamiento y será descartado ya que sobrepasará el tamaño de concesión no solicitada (véase B.C.2.2.6.3).

En la figura B.10-14 se muestra la encapsulación utilizada en el sentido ascendente, con y sin supresión de encabezamiento de cabida útil. Se usa una cabida útil RTP de voz por IP sin IPsec como ejemplo específico con el que mostrar la eficiencia.

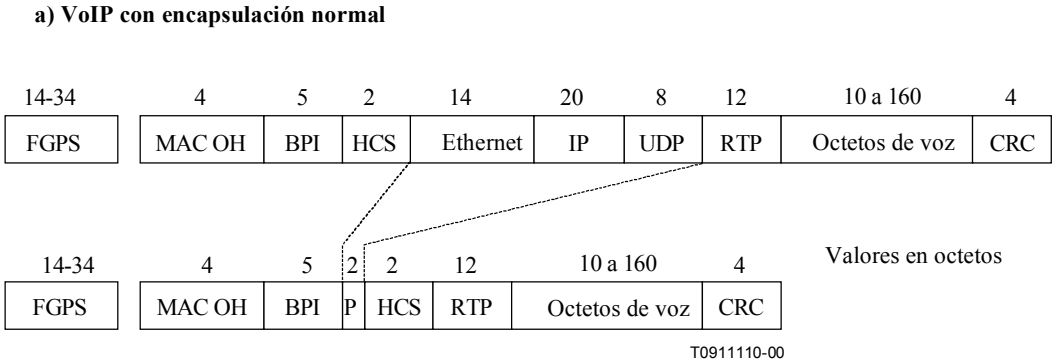


Figura B.10-14/J.112 – Ejemplo de supresión de encabezamiento de cabida útil en sentido ascendente

En la figura B.10-14a se muestra un paquete RTP normal transportado por un canal en sentido ascendente. El comienzo de la trama representa la tara de capa física (FGPS) de FEC, tiempo de guarda, el preámbulo y los octetos de relleno. Los octetos de relleno aparecen en la última palabra de código y cuando se establece la correspondencia entre bloques y miniintervalos. A continuación viene la tara de capa MAC, incluido el encabezamiento MAC de 6 octetos con un encabezamiento ampliado BPI de 5 octetos, el encabezamiento Ethernet de 14 octetos y los 4 octetos de la cola CRC de Ethernet. La cabida útil de VoIP utiliza un encabezamiento IP de 20 octetos, un encabezamiento UDP de 8 octetos y un encabezamiento RTP de 12 octetos. La cabida útil de voz es variable y depende del tiempo de muestreo y del algoritmo de compresión utilizado.

En la figura B.10-14b se muestra la misma cabida útil con supresión de encabezamiento de cabida útil habilitada. En el sentido ascendente la supresión de encabezamiento de cabida útil comienza con el primer octeto luego de la suma de verificación de encabezamiento MAC. Se han suprimido el encabezamiento Ethernet de 14 octetos, el encabezamiento IP de 20 octetos y el encabezamiento UDP de 8 octetos; al mismo tiempo, se ha agregado un encabezamiento ampliado PHS de 2 octetos, obteniéndose una reducción neta de 40 octetos. En el presente ejemplo de una conexión VoIP establecida, estos campos se mantienen constantes de un paquete a otro y son por lo demás redundantes.

B.10.4.5.2 Ejemplo en sentido descendente

Se establece una clase de servicio con el nombre de clase de servicio "G711-DS-HS-30", destinada a tráfico VoIP en sentido descendente conforme a UIT-T G.711. Cuando se agregan clasificadores al flujo de servicio, se incluye un valor PHSS de 30 que indica explícitamente que 30 octetos del encabezamiento de cabida útil de todos los paquetes deben ser procesados para realizar supresión y restauración según el PHSM. Si un paquete no pasa la verificación no se suprimirá su encabezamiento sino que será transmitido, sujeto a las reglas de conformación del tráfico vigentes para ese flujo de servicio.

En la figura B.10-15 se muestra la encapsulación en el sentido descendente, con y sin supresión de encabezamiento de cabida útil. Se usa una cabida útil RTP de Voz por IP sin IPsec como ejemplo específico con el que mostrar la eficiencia.

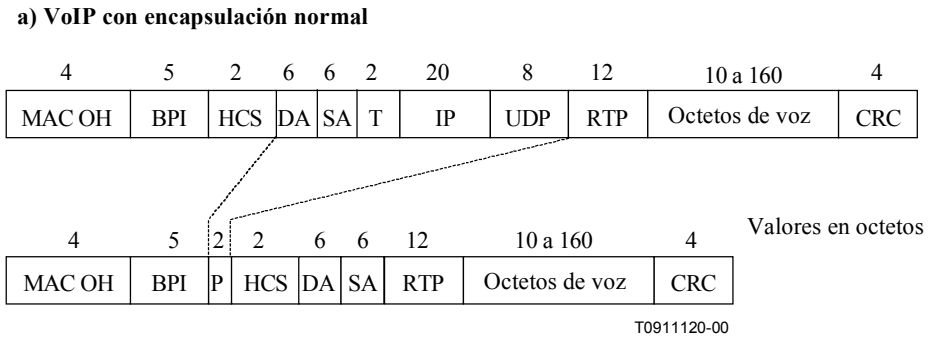


Figura B.10-15/J.112 – Ejemplo de supresión de encabezamiento de cabida útil en sentido descendente

En la figura B.10-15a se muestra un paquete RTP normal transportado por un canal en sentido descendente. La tara de capa 2 incluye el encabezamiento MAC de 6 octetos con un encabezamiento ampliado BPI de 5 octetos, el encabezamiento Ethernet de 14 octetos (dirección de destino de 6 octetos, dirección de origen de 6 octetos y campo EtherType de 2 octetos), y los 4 octetos de la cola CRC de Ethernet . La cabida útil de VoIP de capa 3 utiliza un encabezamiento IP de 20 octetos, un encabezamiento UDP de 8 octetos y un encabezamiento RTP de 12 octetos. La cabida útil de voz es variable y depende del tiempo de muestreo y del algoritmo de compresión utilizados.

En la figura B.10-15b se muestra la misma cabida útil con supresión de encabezamiento de cabida útil habilitada. En el sentido descendente, la supresión de encabezamiento de cabida útil comienza con el décimo tercer octeto luego de la suma de verificación de encabezamiento de MAC. Así se conserva la dirección de destino y la dirección de origen (ambas Ethernet) que son necesarias para que el CM pueda filtrar y recibir el paquete. Se han suprimido los 2 octetos restantes del encabezamiento Ethernet, el encabezamiento IP de 20 octetos y el encabezamiento UDP de 8 octetos; al mismo tiempo, se ha agregado un encabezamiento ampliado PHS de 2 octetos, obteniéndose una reducción neta de 28 octetos. En el presente ejemplo de una conexión VoIP establecida, estos campos se mantienen constantes de un paquete a otro y son por lo demás redundantes.

B.11 Interacción módem de cable – CMTS

Esta cláusula se refiere a los requisitos clave de la interacción entre un CM y un CMTS. La interacción puede dividirse en cinco categorías básicas: inicialización, autenticación, configuración, autorización y señalización.

B.11.1 Inicialización del CMTS

El mecanismo utilizado para la inicialización del CMTS (terminal local, telecarga de fichero, SNMP, etc.) se describe en [DOCSIS5]. DEBE satisfacer los siguientes criterios a efectos de interoperabilidad de los sistemas.

- El CMTS DEBE ser capaz de reiniciar y de trabajar en modo autónomo utilizando datos de la configuración retenidos en un almacenamiento no volátil.
- Si no se dispone de parámetros válidos del almacenamiento no volátil o de otro mecanismo, tal como el sistema de gestión del espectro (SMS, *spectrum management system*), el CMTS NO DEBE generar ningún mensaje en sentido descendente (ni siquiera el SYNC). De esta manera se impedirá que transmitan los CM.
- El CMTS DEBE proporcionar la información definida en B.8 a los CM para cada canal en sentido ascendente.

B.11.2 Inicialización del módem de cable

El procedimiento de inicialización de un módem de cable DEBE ser como se indica en la figura B.11-1. En ella se muestra el flujo global entre las etapas de inicialización en un CM. La figura no contiene ningún trayecto de error y su finalidad es simplemente dar una visión de conjunto del proceso. Las representaciones más detalladas de máquinas de estados finitos de las cláusulas individuales (incluyendo los trayectos de error) se muestran en las figuras subsiguientes. Los valores de temporización se definen en el anexo B.B.

El procedimiento de inicialización de un módem de cable y el de reinicialización de su MAC por parte del CM se puede subdividir en las fases siguientes:

- Exploración y sincronización en el sentido descendente.
- Obtención de parámetros en el sentido ascendente.
- Alineación y ajustes automáticos.
- Identificación de clase de dispositivo (opcional).
- Establecimiento de conectividad IP.
- Establecimiento de la hora del día.
- Transferencia de parámetros operativos.
- Registro.
- Inicialización de la privacidad básica, si CM está aprovisionado para ejecutar privacidad básica.

Cada CM contiene la siguiente información cuando sale de las instalaciones del fabricante:

- Una dirección MAC de 48 bits única [según IEEE 802] que es asignada durante el proceso de fabricación. Se utiliza para identificar el módem ante los diversos servidores de aprovisionamiento durante la inicialización.
- La información de seguridad definida en [DOCSIS8] (por ejemplo, el certificado X.509), utilizada para autenticar el CM al servidor de seguridad y autenticar las respuestas de los servidores de seguridad y aprovisionamiento.

La notación lenguaje de especificación y descripción (SDL, *specification and description language*) utilizada en las figuras que siguen se muestra en la figura B.11-2 (véase UIT-T Z.100).

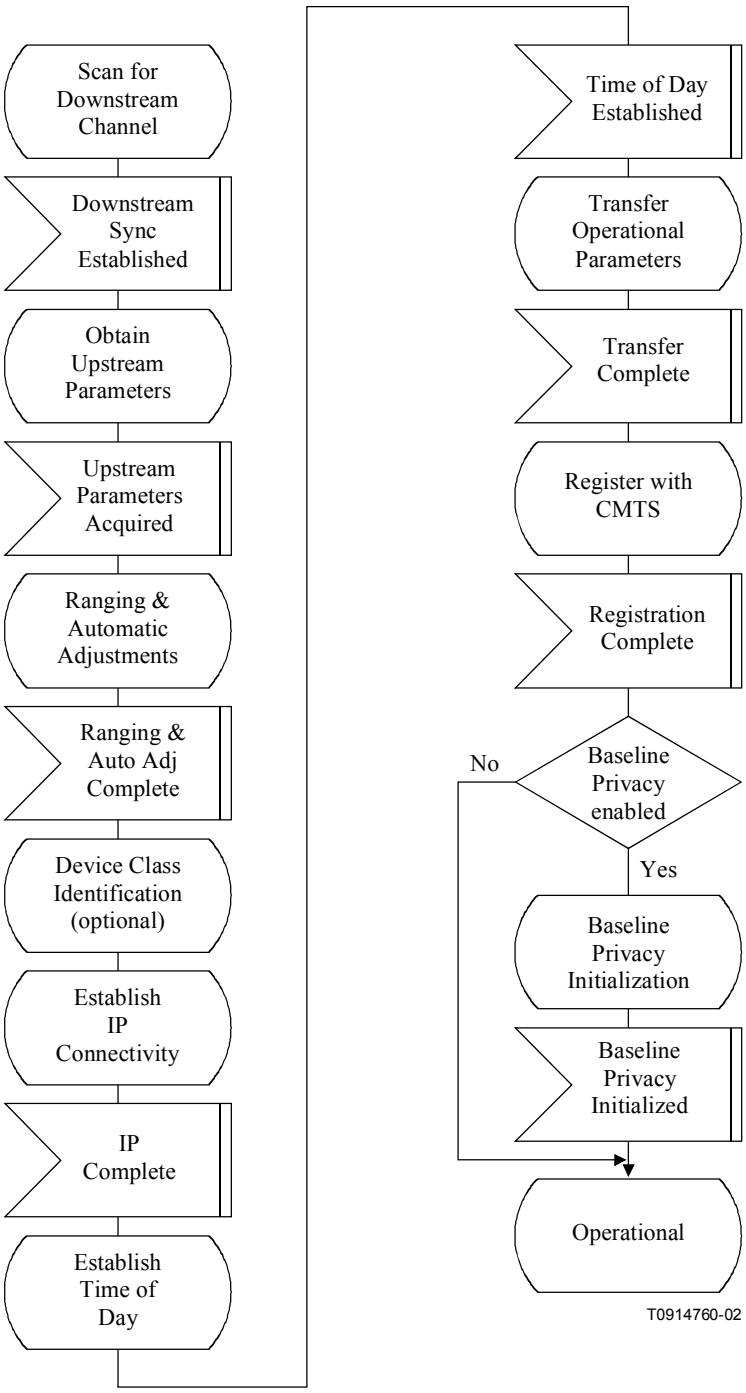


Figura B.11-1/J.112 – Visión de conjunto de la inicialización del CM

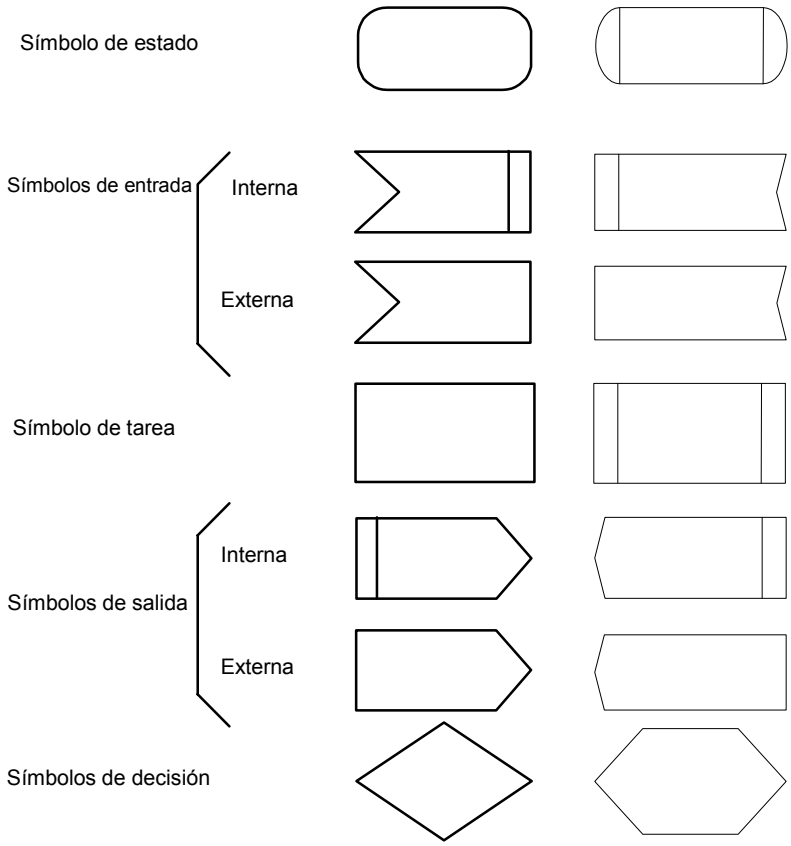


Figura B.11-2/J.112 – Notación SDL

B.11.2.1 Exploración y sincronización en el sentido descendente

Al producirse la inicialización, o tras una pérdida de señal, el módem de cable DEBE adquirir un canal en sentido descendente. El CM DEBE tener un almacenamiento no volátil en el que se almacenan los últimos parámetros operativos y DEBE intentar primero adquirir de nuevo este canal en sentido ascendente. Si no lo consigue, DEBE empezar a explorar de manera continua los canales de 6 MHz de la banda de frecuencias de funcionamiento en sentido descendente hasta que encuentre una señal en sentido descendente válida.

Se considera que una señal en sentido descendente es válida cuando el módem ha efectuado los siguientes pasos:

- Sincronización de la temporización de símbolos de QAM.
- Sincronización de la alineación de trama FEC.
- Sincronización del empaquetado MPEG.
- Reconocimiento de mensajes MAC en sentido descendente de SYNC.

Cuando el CM esté explorando, conviene que se dé al usuario una indicación al respecto.

B.11.2.2 Obtención de parámetros en el sentido ascendente

Véase la figura B.11-3. Después de la sincronización, el CM DEBE esperar por un mensaje descriptor de canal en sentido ascendente (UCD) del CMTS para recuperar un conjunto de parámetros de transmisión para un posible canal ascendente. Estos mensajes son transmitidos periódicamente desde el CMTS para todos los canales disponibles en sentido ascendente y son dirigidos a la dirección de radiodifusión MAC. El CM DEBE determinar si puede utilizar el canal en sentido ascendente a partir de los parámetros de descripción del canal.

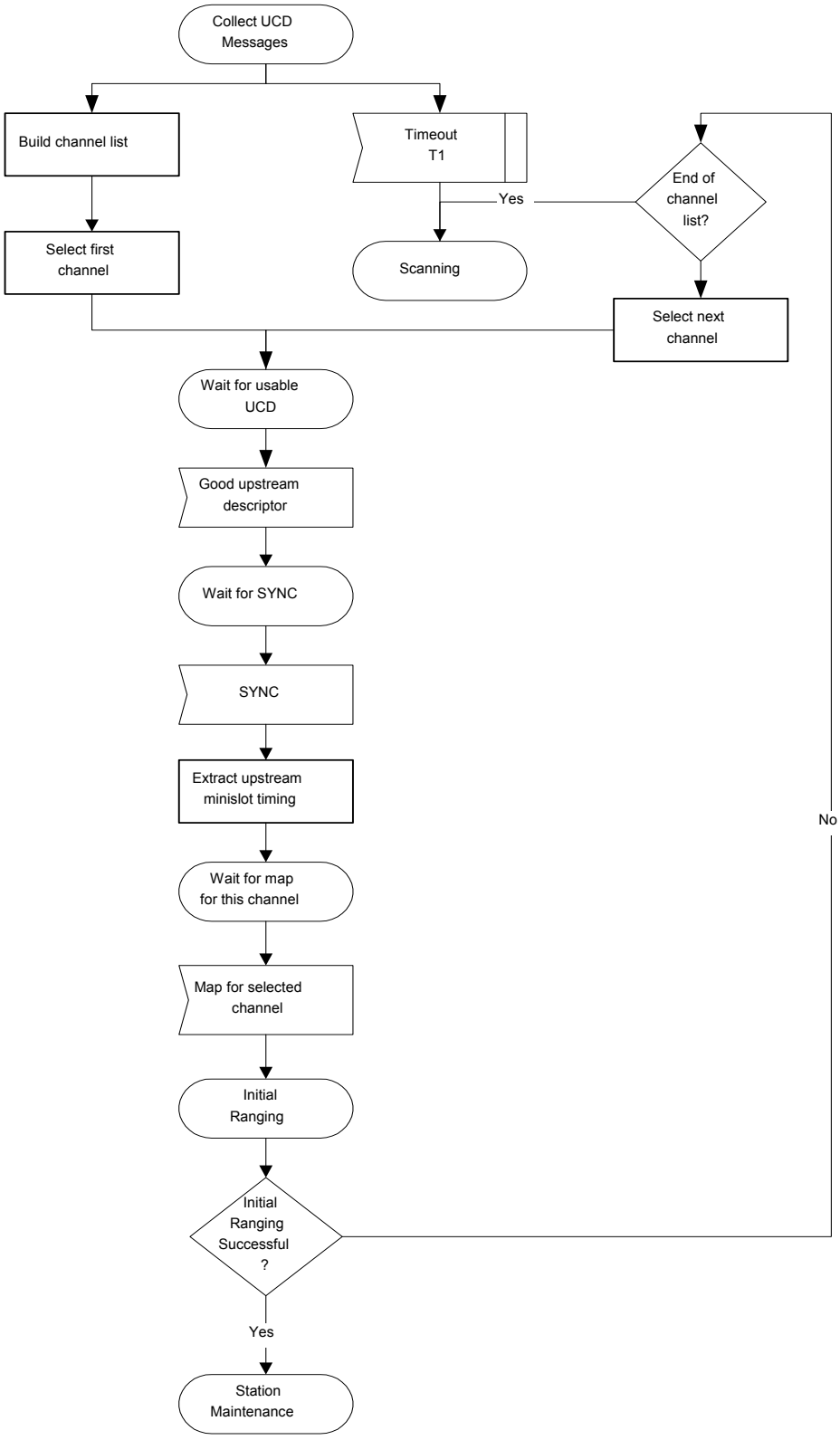


Figura B.11-3/J.112 – Obtención de parámetros en el sentido ascendente

El CM DEBE recopilar todos los UCD que son distintos de su campo ID de canal para construir un conjunto de ID de canal utilizable. Si no se encuentra ningún canal tras un periodo de temporización suficiente, el CM DEBE continuar explorando hasta encontrar otro canal en sentido descendente.

El CM DEBE determinar si puede utilizar el canal en sentido ascendente a partir de los parámetros de descripción del canal. Si el canal no es adecuado, el CM DEBE entonces intentar con el ID de canal siguiente hasta hallar un canal utilizable. Si el canal es adecuado, el CM DEBE extraer del UCD los parámetros para este sentido ascendente. A continuación DEBE esperar el siguiente mensaje SYNC (véase la nota) y extraer la indicación de tiempo del miniintervalo de tiempo en sentido ascendente de este mensaje. El CM DEBE esperar entonces un diagrama de atribución de anchura de banda para el canal seleccionado. Puede empezar a transmitir en sentido ascendente de acuerdo con el funcionamiento MAC y el mecanismo de atribución de anchura de banda.

NOTA – De manera alternativa, puesto que el mensaje SYNC se aplica a todos los canales en sentido ascendente, el CM puede haber adquirido ya una referencia de tiempo de los mensajes SYNC anteriores. Si tal es el caso, no necesita esperar por un nuevo SYNC.

El CM DEBE ejecutar una alineación inicial al menos una vez, según la figura B.11-6. Si la alineación inicial no tiene éxito, se selecciona el ID de canal siguiente y se reinicia el procedimiento a partir de la extracción del UCD. Cuando no hay más ID de canal con los que intentar, el CM DEBE seguir explorando para encontrar otro canal descendente.

B.11.2.3 Flujos de mensajes durante la exploración y la adquisición de parámetros en el sentido ascendente

El CMTS DEBE generar mensajes SYNC y UCD en el sentido descendente a intervalos periódicos dentro de las gamas definidas en el anexo B.B. Estos mensajes están dirigidos a todos los CM. Véase la figura B.11-4.

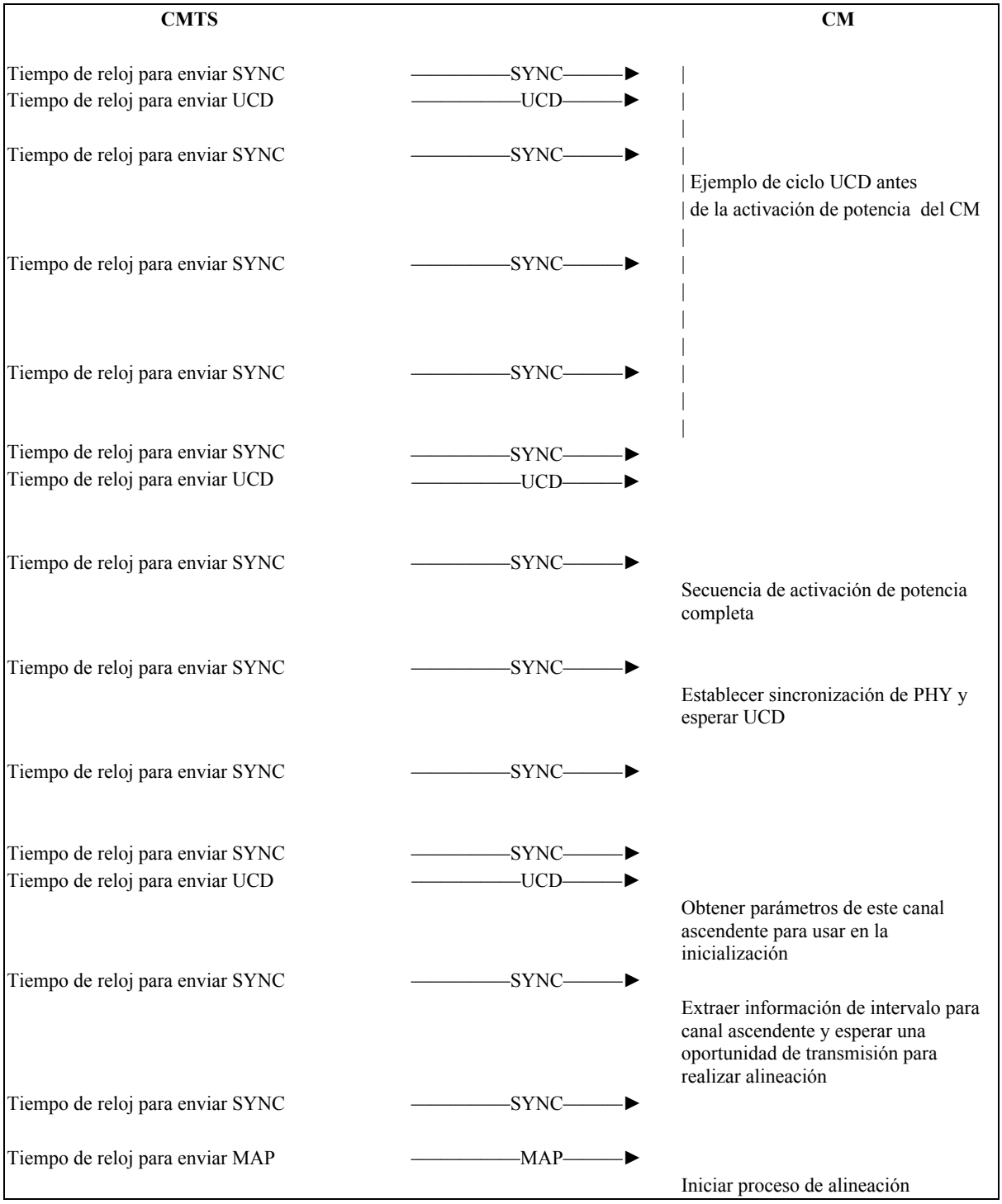


Figura B.11-4/J.112 – Flujos de mensajes durante la exploración y la adquisición de parámetros en el sentido ascendente

B.11.2.4 Alineación y ajustes automáticos

El proceso de alineación y ajuste se define por completo en B.8 y en las cláusulas que vienen a continuación. El diagrama de la secuencia de mensajes y las máquinas de estados finitos de las páginas que siguen definen el proceso de alineación y ajuste que DEBEN seguir los CM y CMTS conformes. Véanse las figuras B.11-5 a B.11-8.

NOTA – Los MAP se transmiten como se describe en B.8.

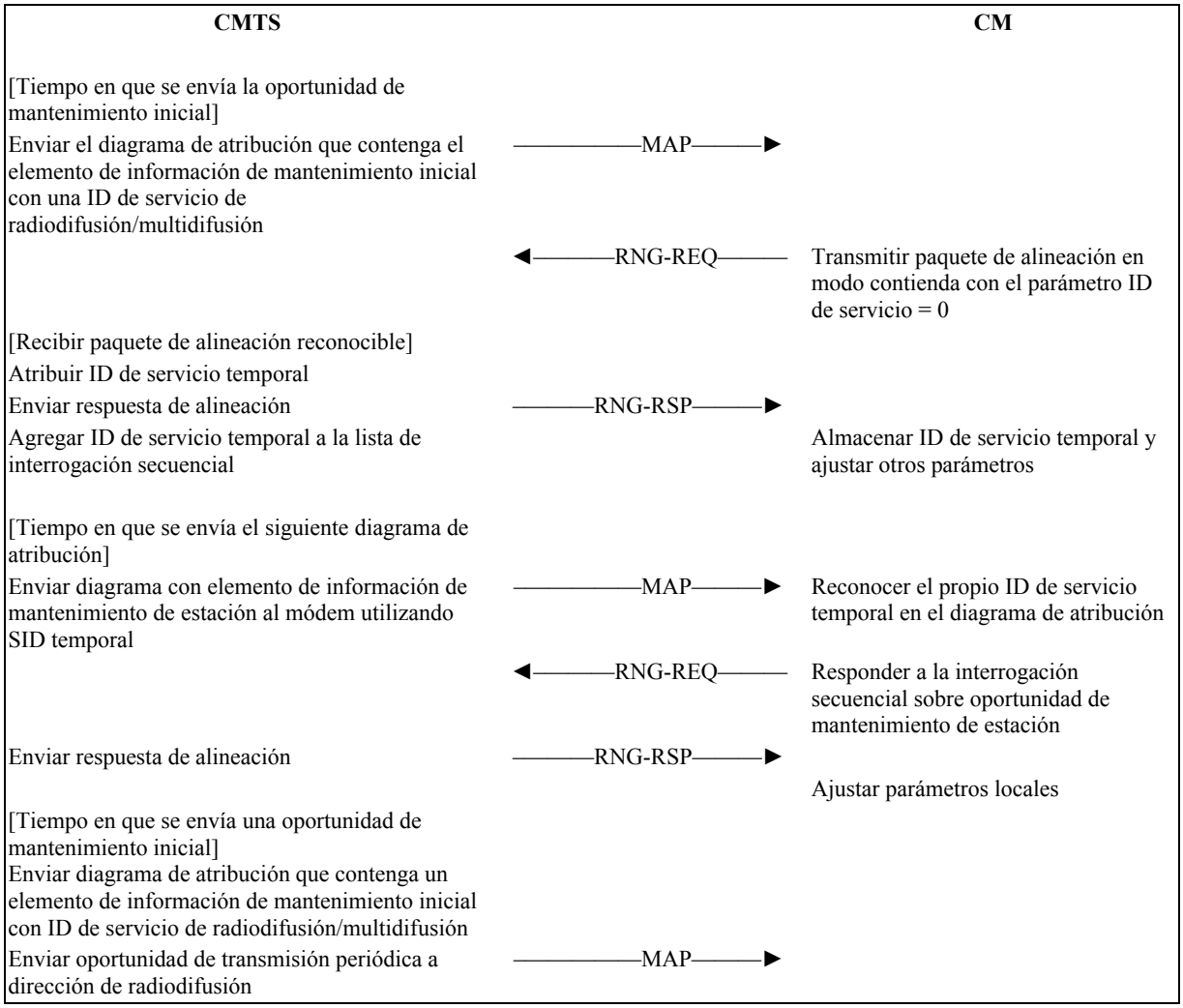
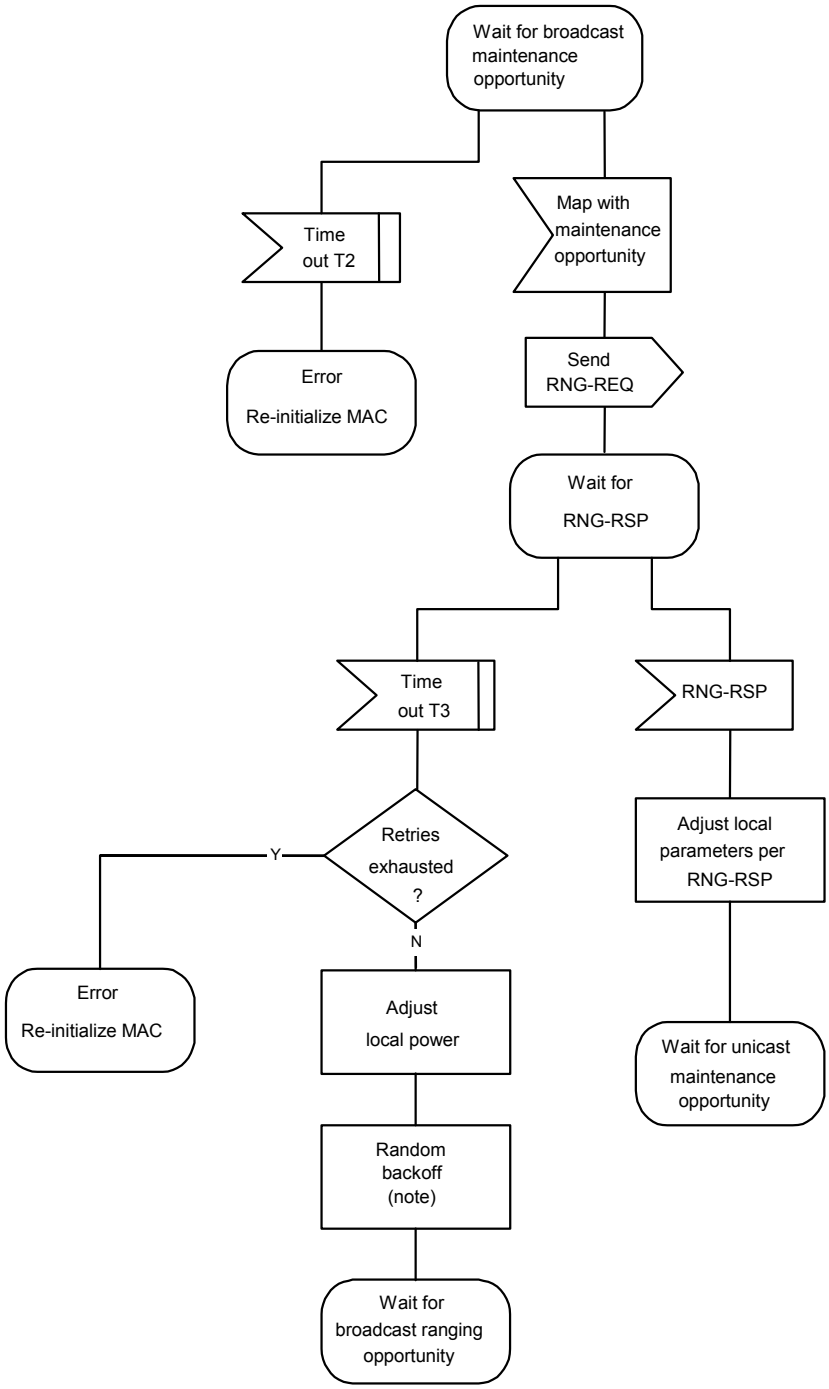


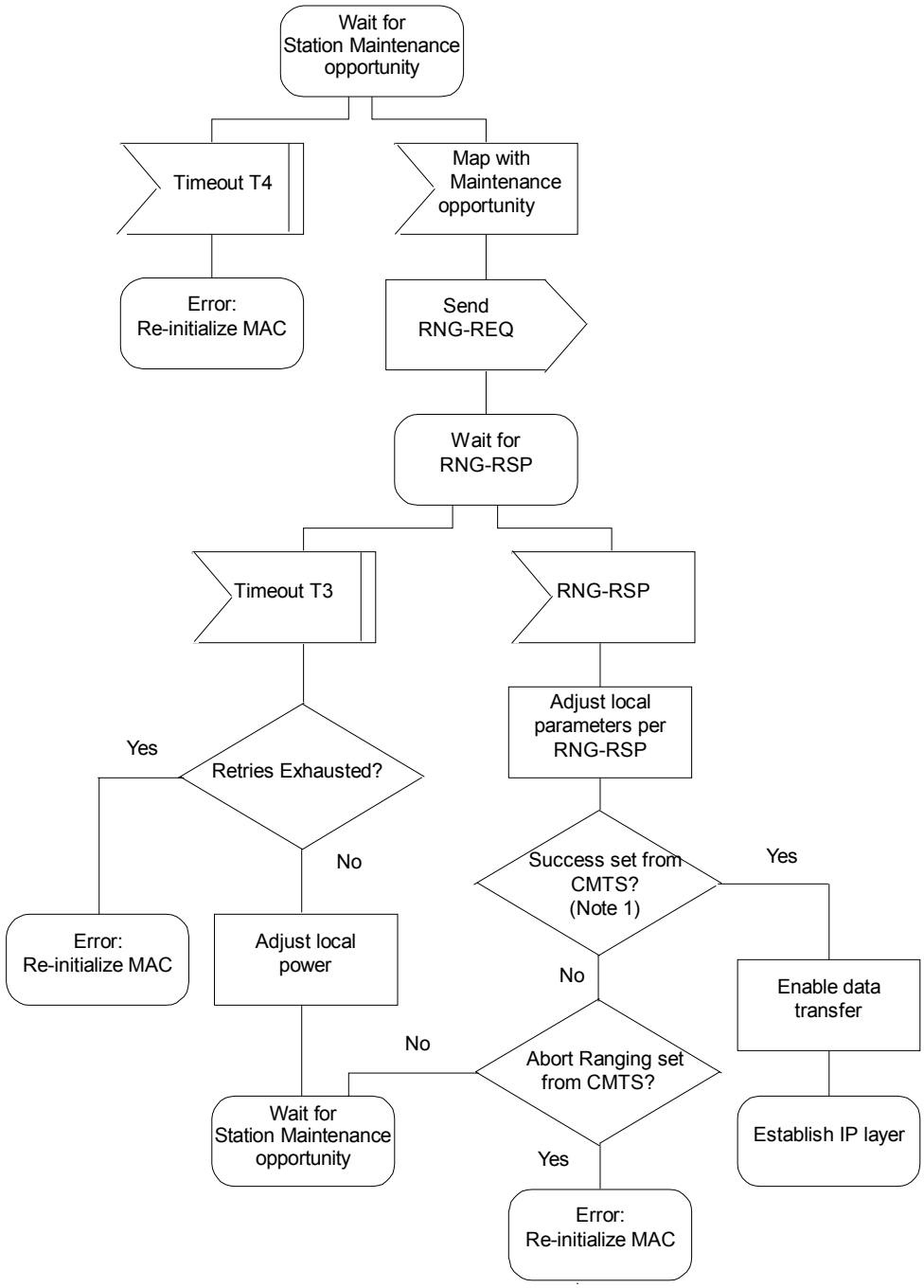
Figura B.11-5/J.112 – Procedimiento de alineación y ajuste automáticos

El CMTS DEBE dar al CM tiempo suficiente como para haber procesado la RNG-RSP previa (es decir, haber modificado los parámetros del transmisor) antes de enviar al CM una oportunidad de alineación específica. Esto se define en el anexo B.B como tiempo de respuesta de alineación del CM.



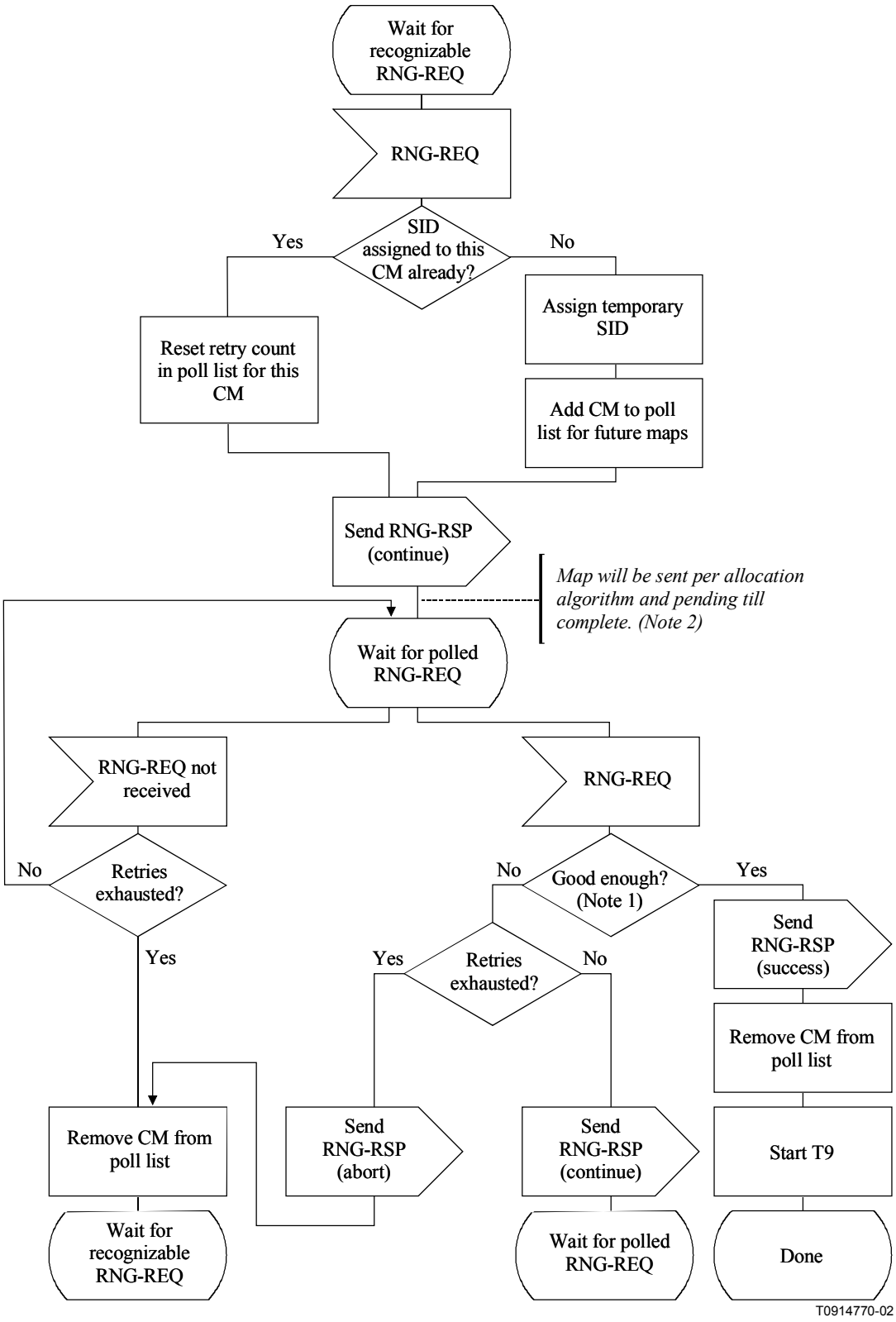
NOTA – La expiración de la temporización T3 se puede producir porque colisionaron los RNG-REQ de múltiples módems. Para evitar que estos módems repitan el bucle en formación cerrada, se necesita un retroceso aleatorio. Se trata de un retroceso sobre la ventana de alineación especificada en el diagrama de atribución. Las temporizaciones T3 también pueden ocurrir durante el funcionamiento en multicanal. En un sistema con múltiples canales ascendentes, el CM DEBE intentar la alineación inicial en cada canal ascendente adecuado antes de pasar al siguiente canal descendente disponible.

Figura B.11-6/J.112 – Alineación inicial – CM



NOTA – La petición de alineación está dentro de la tolerancia del CMTS.

Figura B.11-7/J.112 – Alineación inicial – CM *(fin)*



NOTA 1 – Significa que la alineación está dentro de la tolerancia del CMTS.

NOTA 2 – RNG-REQ pendiente hasta estar completo era no nulo, de acuerdo con lo cual el CMTS DEBERÍA retener la oportunidad de mantenimiento de estación a menos que se necesite, por ejemplo, para ajustar el nivel de potencia del CM. Si se ofrecen oportunidades antes de que expire "pendiente hasta estar completo", la prueba de "suficientemente bueno" que sigue a la recepción de un RNG-RSP NO DEBE juzgar la ecualización de transmisión del CM hasta que expire "pendiente hasta estar completo".

Figura B.11-8/J.112 – Alineación inicial – CMTS

B.11.2.4.1 Ajuste de parámetros de alineación

El ajuste de los parámetros locales (por ejemplo, la potencia de transmisión) en un CM como resultado de la recepción (o la no recepción) de un mensaje RNG-RSP se considera que depende de la implementación con las siguientes restricciones (véase B.8.3.6):

- todos los parámetros DEBEN estar en todo momento dentro de la gama aprobada;
- el ajuste de potencia DEBE empezar desde el valor mínimo a menos que se disponga de una potencia válida procedente de una almacenamiento no volátil, en cuyo caso se DEBE utilizar ésta como punto de comienzo;
- el ajuste de potencia DEBE ser susceptible de reducción o aumento en la cantidad especificada en respuesta a los mensajes RNG-RSP;
- si, durante la inicialización, se aumenta la potencia al valor máximo (sin tener respuesta del CMTS), DEBE replegarse hasta el mínimo;
- para que sea compatible con multicanal, el CM DEBE intentar la alineación inicial en cada canal ascendente adecuado antes de pasar al siguiente canal descendente disponible;
- para que sea compatible con multicanal, el CM DEBE usar el ID de canal ascendente de la respuesta de la gama, según se especifica en B.8.3.6 y en el anexo B.H.

B.11.2.5 Identificación de clase de dispositivo

Una vez completada la alineación y antes de establecer la conectividad IP, el CM identificarse a sí mismo al CMTS para la utilización en provisionamiento. Véase la figura B.11-9.

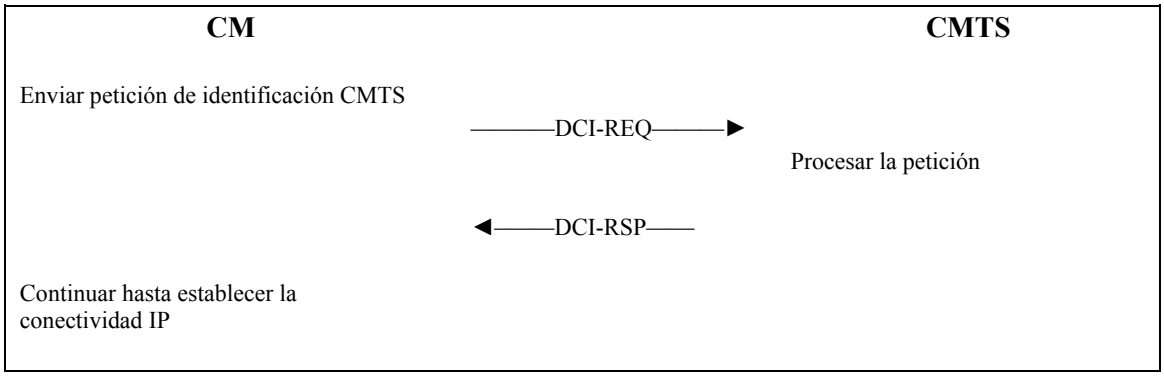


Figura B.11-9/J.112

Si se implementa, el CM DEBE usar un temporizador adaptable para la identificación de la clase de dispositivo basado en el retroceso exponencial binario, similar al utilizado para TFTP. Véase B.11.2.9 por más detalles.

B.11.2.6 Establecimiento de conectividad IP

En este punto, el CM DEBE invocar mecanismos DHCP [RFC 2131] para obtener una dirección IP y cualesquiera otros parámetros que necesite para establecer la conectividad IP (véase el anexo B.D). La respuesta DHCP DEBE contener el nombre de un fichero que contenga otros parámetros de la configuración. Véase la figura B.11-10.

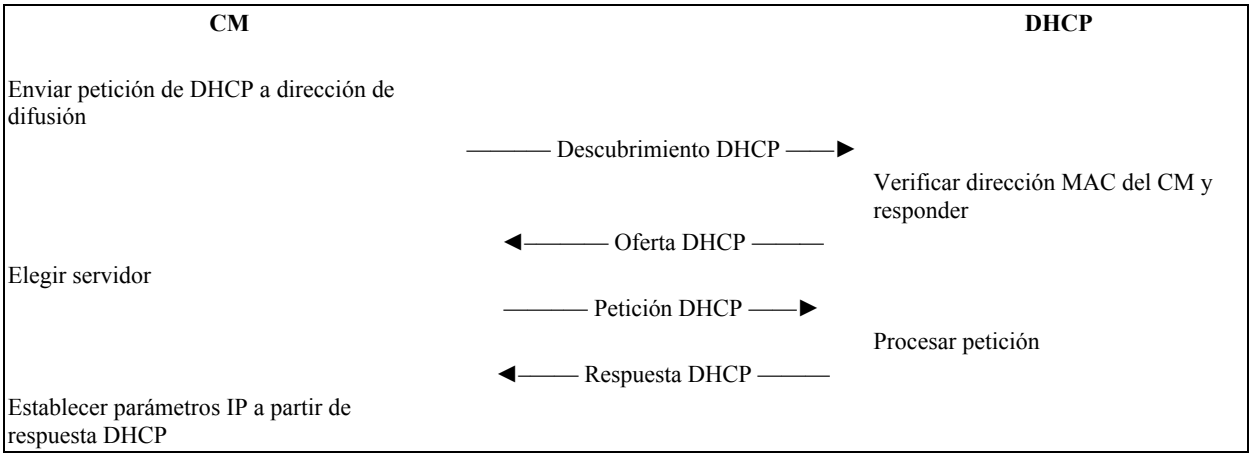


Figura B.11-10/J.112 – Establecimiento de conectividad IP

B.11.2.7 Establecimiento de la hora del día

El CM y el CMTS necesitan disponer de la fecha y la hora en curso. Esto es necesario para marcar la hora de los eventos registrados que pueden ser recuperados por el sistema de gestión. No es preciso que sean autenticadas y basta con que su exactitud sea de un segundo.

El protocolo según el cual se DEBE recuperar la hora del día será como se define en [RFC 868]. Véase la figura B.11-11. La petición y la respuesta DEBEN transferirse utilizando UDP. La hora recuperada del servidor (UTC) DEBE combinarse con el desplazamiento de tiempo recibido de la respuesta de DHCP para crear la hora local actual.

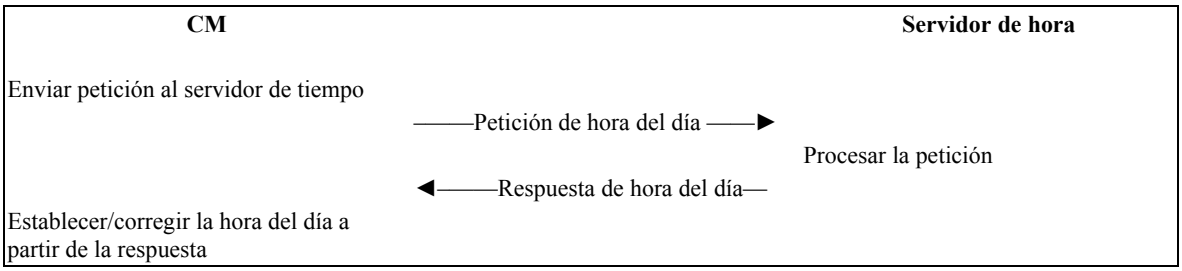


Figura B.11-11/J.112 – Establecimiento de la hora del día

El servidor DHCP puede ofrecer a un CM varias direcciones IP de servidor de hora del día con las que intentar. El CM DEBE intentar con todos los servidores de hora del día incluidos en la oferta de DHCP hasta establecer la hora local.

La consecución satisfactoria de la hora del día no es obligatoria para un registro exitoso, pero sí es necesaria para un funcionamiento continuo. Si un CM no logra establecer la hora del día antes del registro, DEBE registrar cronológicamente el fallo, generar una alerta dirigida a las facilidades de gestión y a continuación debe pasar a un estado operativo y reintentar periódicamente.

La temporización específica de las peticiones de hora del día depende de la implementación. Sin embargo, para cada uno de los servidores definidos, el CM NO DEBE superar tres peticiones de hora del día durante un periodo cualquiera de cinco minutos. Como mínimo, el CM DEBE emitir al menos una petición de hora del día por periodo de cinco minutos para cada servidor especificado hasta que se establezca la hora local.

B.11.2.8 Transferencia de parámetros operativos

Si la operación de DHCP es satisfactoria, el módem DEBE telecargar el fichero de parámetros utilizando el TFTP, como se muestra en la figura B.11-12. El servidor de parámetros de la configuración TFTP se especifica mediante el campo "siaddr" de la respuesta de DHCP. El CM DEBE usar un temporizador adaptable para TFTP basado en el retroceso exponencial binario. Véase [RFC 1123] y [RFC 2349].

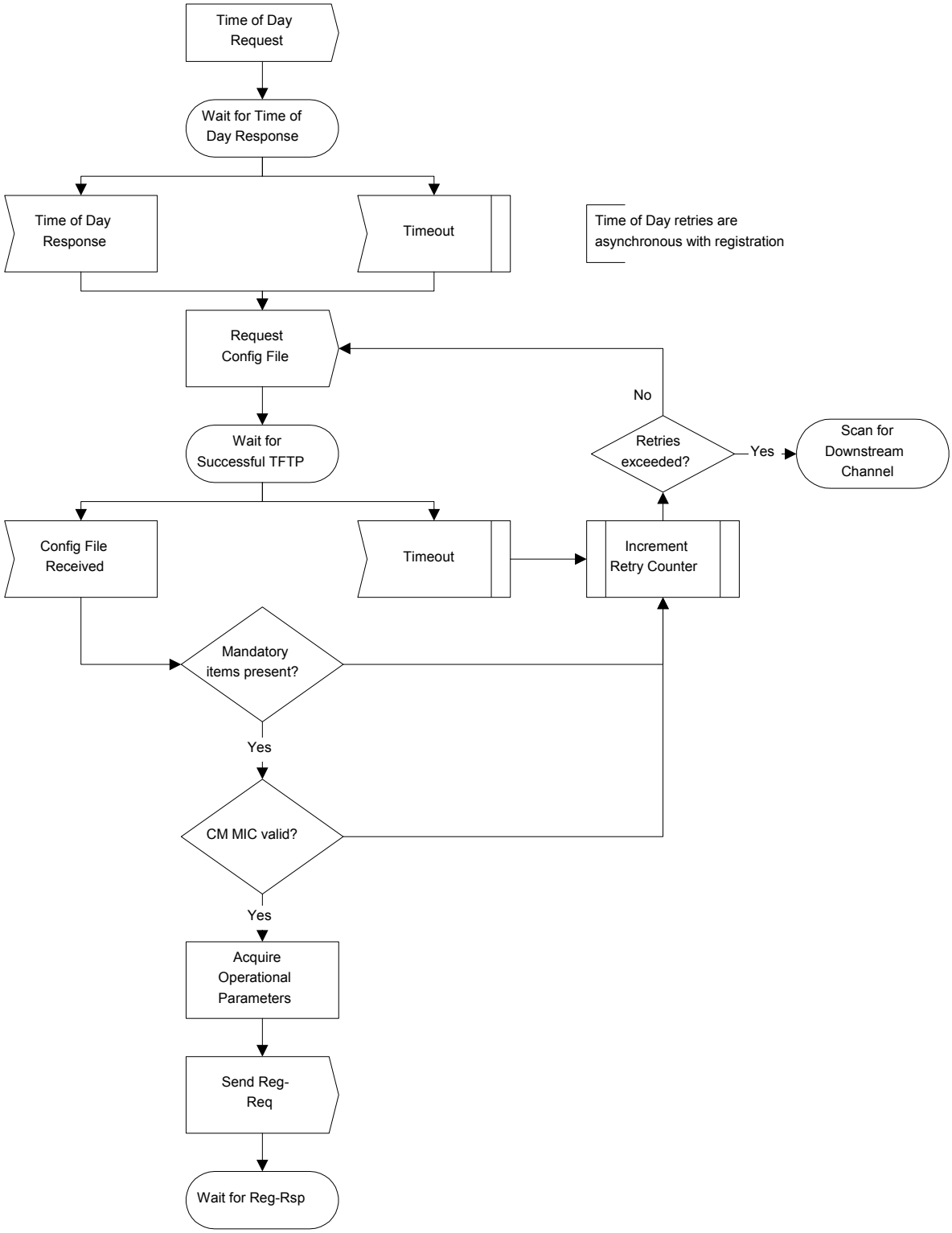


Figura B.11-12/J.112 – Registro – CM

Los campos de parámetros requeridos en la respuesta de DHCP y el formato y contenido del fichero de la configuración DEBEN ser como se define en el anexo B.D. Se señala que estos campos son el mínimo requerido a efectos de interoperabilidad.

Si un módem telecarga un fichero de configuración que contiene un canal ascendente y/o una frecuencia descendente diferente/s de lo que el módem está utilizando actualmente, el módem NO DEBE enviar un mensaje de petición de registro al CMTS. El módem DEBE rehacer la alineación inicial utilizando el canal ascendente configurado y/o la frecuencia descendente, conforme a B.8.3.6.3.

B.11.2.9 Registro

Un CM DEBE ser autorizado a retransmitir tráfico a la red una vez que haya sido inicializado y configurado. El CM está autorizado a reenviar tráfico a la red por medio del registro. Para registrarse en un CMTS, el CM DEBE retransmitir su clase de servicio configurada y cualesquiera otros parámetros operativos en el fichero de configuración (véase B.8.3.7) al CMTS como parte de su petición de registro. La figura B.11-12 muestra el procedimiento que DEBE seguir el CM.

Los parámetros de configuración telecargados al CM DEBEN incluir un objeto control de acceso a la red (véase B.C.1.1.3). Si se ha fijado a "no reenviar", el CM NO DEBE reenviar datos del CPE adjunto a la red; sin embargo, el CM DEBE responder a las peticiones de gestión de red. Esto permite configurar el CM de modo que sea gestionable, pero sin que retransmita datos. El CM NO DEBE enviar un REG-REQ si el fichero de configuración no tiene un objeto de control de acceso a red.

Una vez que el CM ha enviado una petición de registro al CMTS, DEBE esperar que una respuesta de registro lo autorice a reenviar tráfico a la red. La figura B.11-13 muestra el procedimiento de espera que DEBE seguir el CM.

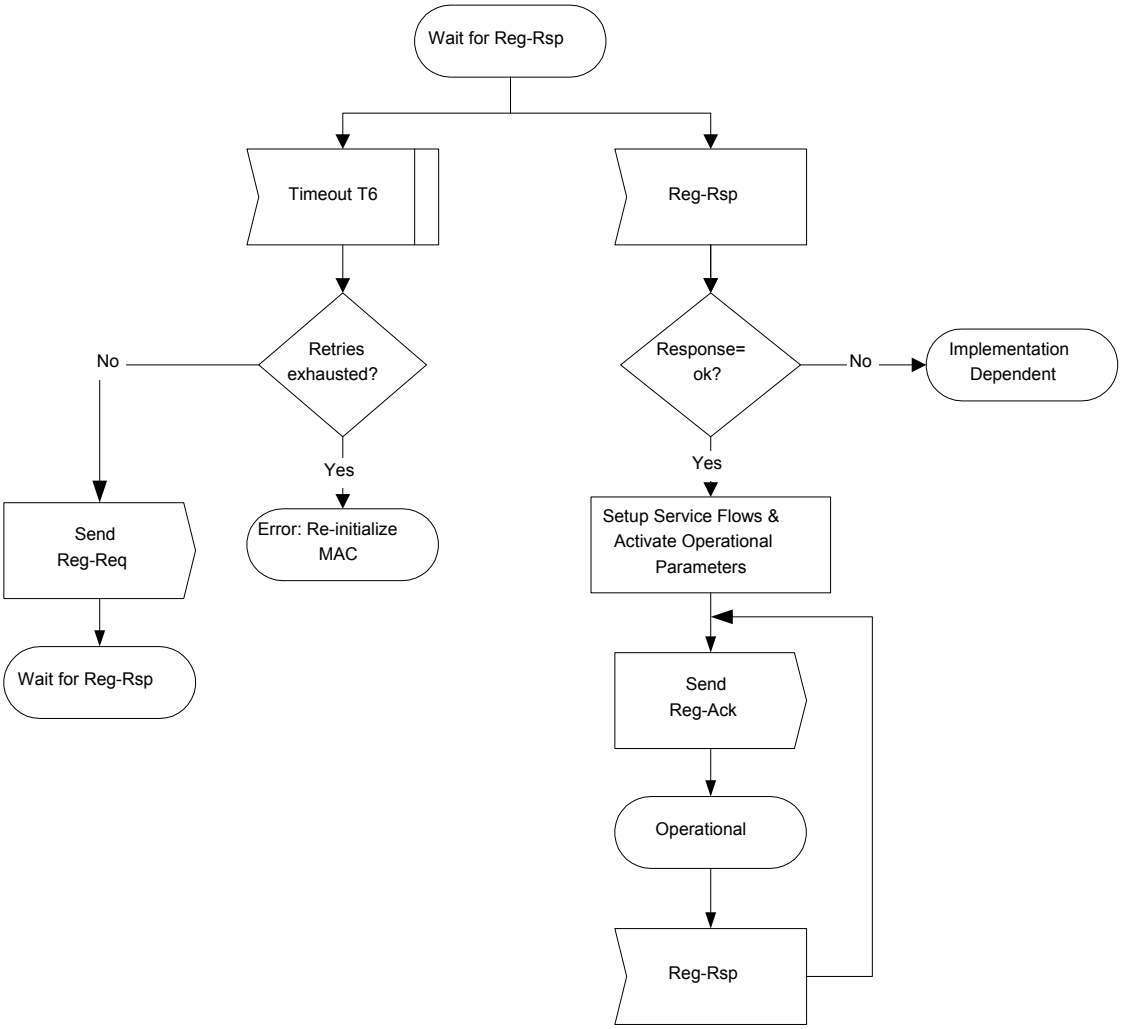


Figura B.11-13/J.112 – Espera de respuesta de registro – CM

El CMTS DEBE efectuar las siguientes operaciones para confirmar la autorización al CM (véase la figura B.11-14):

- Calcular un MIC conforme a B.D.3.1 y compararlo con el MIC de CMTS incluido en la petición de registro. Si el MIC no es válido, el CMTS DEBE responder con una falla de autorización.
- Si está presente, se debe verificar el campo indicación de tiempo del servidor TFTP. Si el CMTS detecta que la hora difiere de su hora local en más del tiempo de procesamiento de la configuración del CM (véase el anexo B.B), DEBE indicar un fallo de autenticación en la REG-RSP. El CMTS DEBERÍA también efectuar una inscripción en el registro indicando la dirección MAC del CM a partir del mensaje.
- Si está presente, se debe verificar el campo dirección del módem aprovisionado por servidor TFTP. Si la dirección del módem aprovisionado no concuerda con la dirección real del módem que efectúa la petición, el CMTS DEBE indicar una falla de autenticación en REG-RSP. El CMTS DEBERÍA también efectuar una inscripción en el registro indicando la dirección MAC del CM a partir del mensaje.
- Si la petición de registro contiene codificaciones de clase de servicio DOCSIS 1.0, se debe verificar la disponibilidad de la(s) clase(s) de servicio pedida(s). Si no puede proveer la(s) clase(s) de servicio, el CMTS DEBE responder con un fallo de clase de servicio y el(los) código(s) de respuesta de servicio no disponible correspondiente(s). (Véase B.C.1.3.4.)

- Si la petición de registro contiene codificaciones de flujo de servicio, se debe verificar la disponibilidad de la calidad de servicio pedida en el (los) flujo(s) de servicio provisionado(s). Si no puede proporcionar el (los) flujo(s) de servicio, el CMTS DEBE responder ya sea con indicación de rechazo temporal o el rechazo permanente (véase B.C.4) y la(s) correspondiente(s) respuesta(s) de flujo de servicio.
- Si la petición de registro contiene codificaciones de clase de servicio DOCSIS 1.0 y codificaciones de flujo de servicio, el CMTS DEBE responder con un fallo de clase de servicio y un código de respuesta de servicio no disponible fijado a "rechazo permanente" para todas las clases y todos los flujos de servicio DOCSIS 1.0 pedidos.
- Verificar la disponibilidad de cualquier capacidad de módem pedida. Si no puede o no desea proporcionar la capacidad de módem pedida, el CMTS DEBE "apagar" dicha capacidad de módem (véase B.8.3.8.1.1).
- Asignar un ID de flujo de servicio para cada clase de servicio soportada.
- Responder al módem en una respuesta de registro.
- Si la respuesta de registro contiene codificaciones de flujo de servicio, el CMTS DEBE esperar un acuse de registro según muestra la figura B.11-15. Si la petición de registro contiene codificaciones de clase de servicio DOCSIS 1.0, el CMTS NO DEBE esperar un acuse de recibo de registro.
- Si expira la temporización del temporizador T9, el CMTS DEBE retirar la asignación del SID temporal a ese CM y realizar algun aprovisionamiento para el proceso de prescripción de dicho SID.

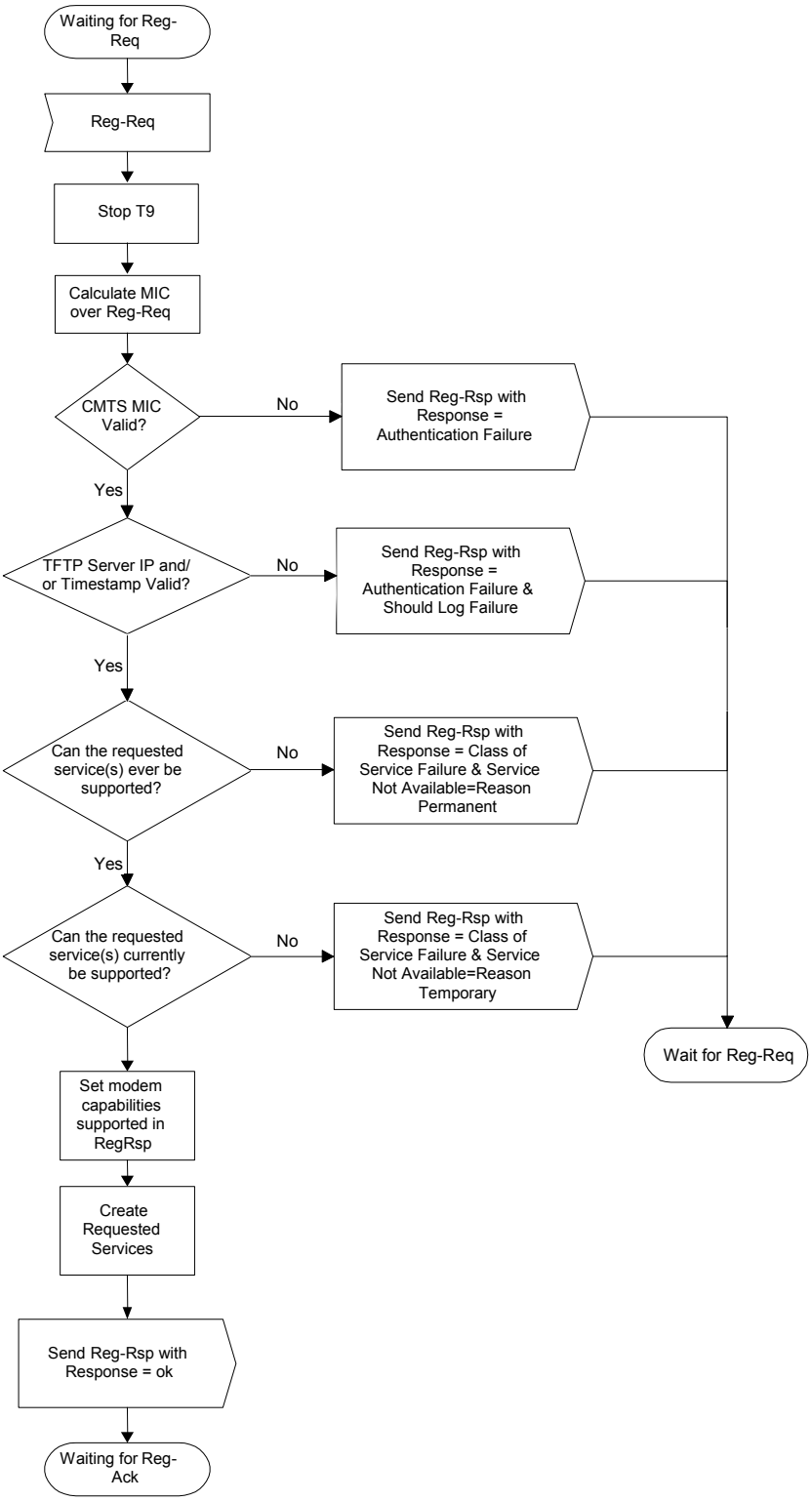


Figura B.11-14/J.112 – Registro – CMTS

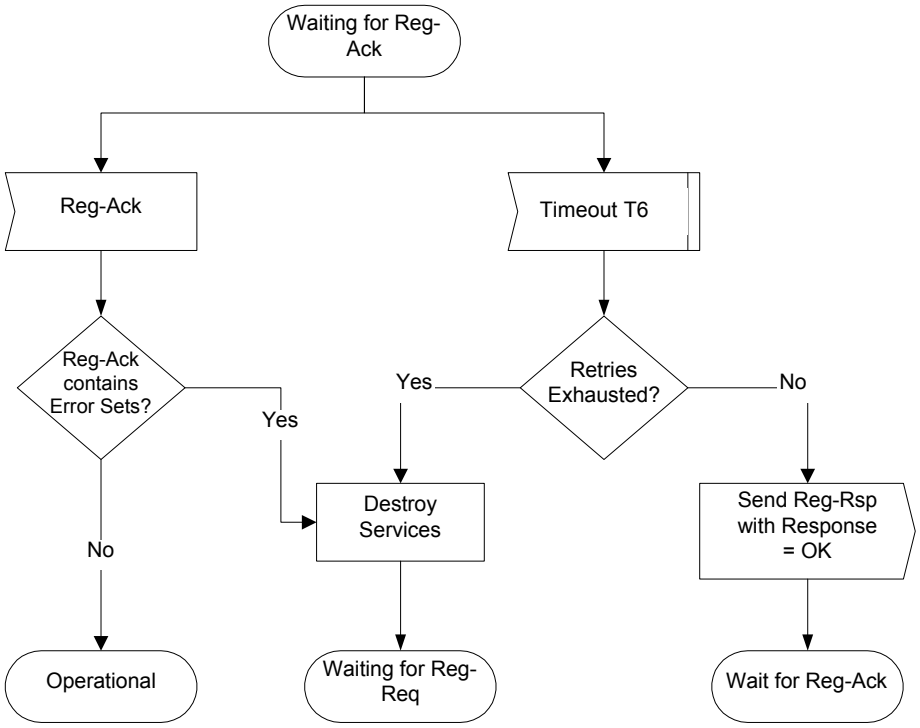


Figura B.11-15/J.112 – Acuse de registro – CMTS

B.11.2.10 Inicialización de privacidad básica

Tras el registro, si el CM es aprovisionado para ejecutar privacidad básica, el CM DEBE inicializar las operaciones de privacidad básica tal como se describe en [DOCSIS8]. Se aprovisiona un CM para que ejecute privacidad básica si su fichero de configuración incluye una fijación de configuración privacidad básica (véase B.C.3.2) y si el parámetro habilitar privacidad (véase B.C.1.1.16) está puesto para habilitar.

B.11.2.11 ID de servicio durante la inicialización del CM

Al completar el proceso de registro (véase B.11.2.9), se le habrán asignado al CM identificadores de flujo de servicio (SFID) conformes con su aprovisionamiento. Sin embargo, el CM tiene que concluir antes un cierto número de transacciones de protocolo (por ejemplo, alineación, DHCP, etc.), y requiere un ID de servicio temporal para completar esos pasos.

Al recibir una petición de alineación inicial, el CMTS DEBE atribuir un SID temporal y asignarlo al CM para que lo utilice en la inicialización. El CMTS PUEDE supervisar la utilización de ese SID y restringir el tráfico a lo que se necesite para la inicialización. DEBE informar al CM de esta asignación en la respuesta de alineación.

Al recibir una respuesta de alineación dirigida a él, el CM DEBE utilizar el SID temporal asignado para ulteriores peticiones de transmisión de inicialización hasta que se reciba la respuesta de registro.

Al recibir una instrucción respuesta de alineación de pasar a un nuevo ID de frecuencia en sentido descendente y/o canal en sentido ascendente, el CM DEBE considerar como revocada la asignación previamente realizada de cualquier SID temporal y DEBE obtener un nuevo SID temporal por vía de la alineación inicial.

Es posible que la respuesta de alineación se pierda tras la transmisión por el CMTS. El CM DEBE recuperar, mediante temporización y reemisión, su petición de alineación inicial. Puesto que el CM está identificado de manera exclusiva por la dirección de origen MAC en la petición de alineación, el CMTS PUEDE reutilizar inmediatamente el SID temporal asignado previamente. Si el CMTS asigna

un nuevo SID temporal, DEBE tomar algunas medidas para que prescriba el SID antiguo que no se utilizó (véase B.8.3.8).

Cuando asignan SFID aprovisionadas al recibir un mensaje petición de registro, el CMTS puede reutilizar el SID temporal, asignándolo a uno de los flujos de servicio solicitados. Si así lo hace, DEBE seguir autorizando mensajes de inicialización en ese SID, ya que el mensaje respuesta de registro podría perderse en tránsito. Si el CMTS asigna SID totalmente nuevos para el provisionamiento de clases de servicio, DEBE hacer que prescriba el SID temporal. El proceso de prescripción DEBE dar tiempo suficiente para que se complete el proceso de registro en el caso de que el mensaje respuesta de registro se pierda en tránsito.

B.11.2.12 Soporte de múltiples canales

Si en el sistema están presentes más de una señal en sentido descendente, el CM DEBE funcionar utilizando la primera señal en sentido descendente válida que encuentre en el proceso de exploración. Se le indicará, mediante los parámetros del fichero de la configuración (véase el anexo B.C), que desplace el funcionamiento a frecuencias en sentido descendente y/o ascendente diferentes si fuese necesario.

Los canales, tanto en sentido ascendente como descendente, DEBEN ser identificados cuando así se requiera en los mensajes de gestión MAC utilizando identificadores de canal.

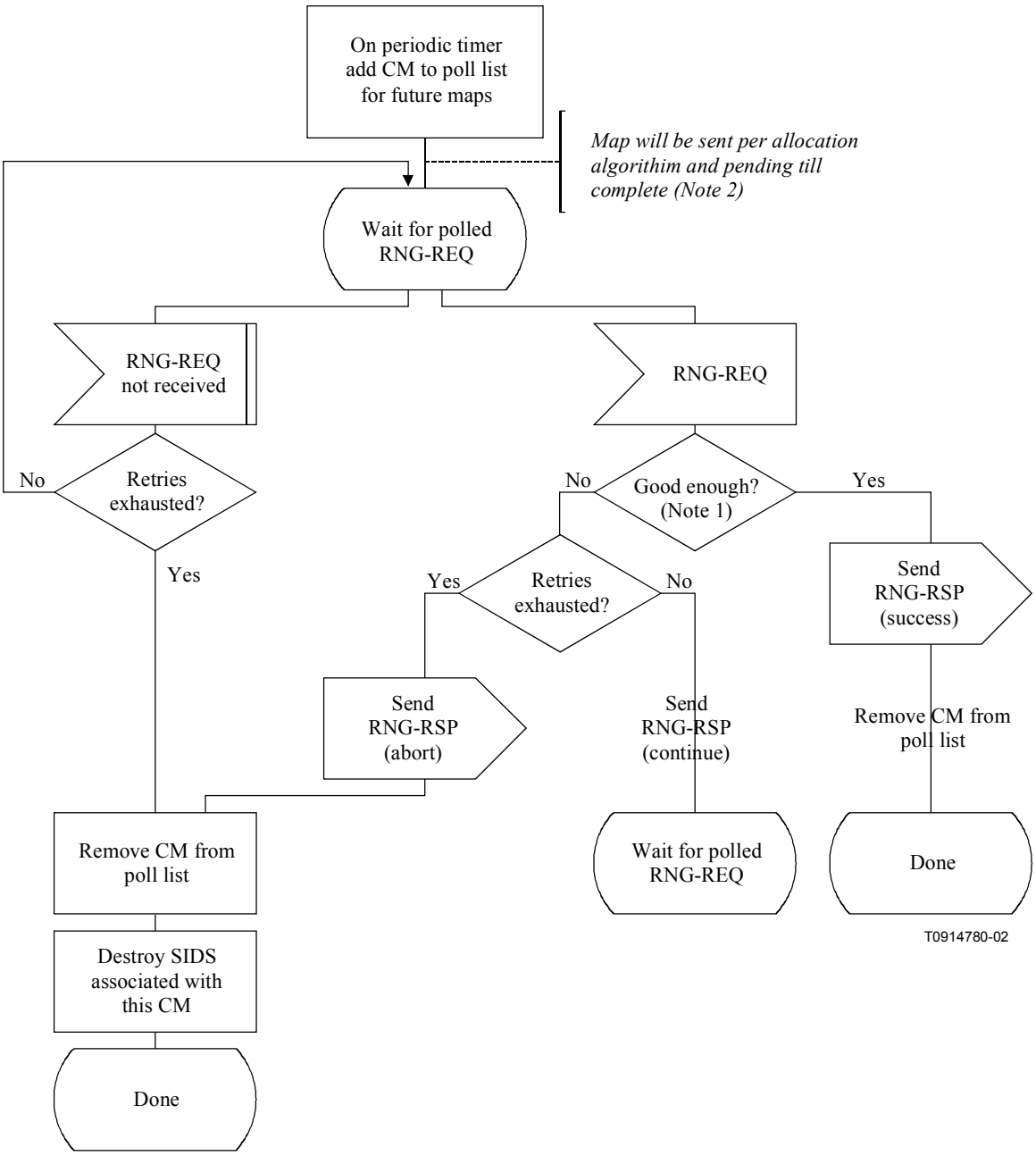
B.11.3 Funcionamiento normalizado

B.11.3.1 Ajuste periódico del nivel de señal

El CMTS DEBE proporcionar a cada CM una oportunidad de alineación periódica al menos cada T4 segundos. El CMTS DEBE enviar oportunidades de alineación periódica a intervalos lo suficientemente más breves que T4 como para que se pueda perder un diagrama de atribución de anchura de banda sin que expire la temporización del CM. La duración de este "subintervalo" depende del CMTS.

El CM DEBE reinicializar su capa MAC una vez que transcurran T4 segundos sin recibir una oportunidad de alineación periódica.

El ajuste remoto del nivel de la señal RF en el CM se efectúa mediante una función de mantenimiento periódico utilizando los mensajes MAC RNG-REQ y RNG-RSP. Se trata de algo similar a la alineación inicial y se muestra en las figuras B.11-16 y B.11-17. Tras la recepción de un RNG-RSP, el CM NO DEBE transmitir sino hasta que la señal RF haya sido ajustada de acuerdo con el RNG-RSP y se haya estabilizado (véase B.6).



NOTA 1 – Significa que la petición de alineación está dentro de la tolerancia del CMTS en lo que hace a ecualización de transmisión y potencia (si es que se soporta).

NOTA 2 – RNG-REQ pendiente hasta estar completo era no nulo, de acuerdo con lo cual el CMTS DEBERÍA retener la oportunidad de mantenimiento de estación a menos que sea necesario: por ejemplo, para ajustar el nivel de potencia del CM. Si se ofrecen oportunidades antes de que expire "pendiente hasta estar completo", la prueba de "suficientemente bueno" que sigue a la recepción de un RNG-RSP NO DEBE juzgar la ecualización de transmisión hasta que expire "pendiente hasta estar completo".

Figura B.11-16/J.112 – Alineación periódica – CMTS

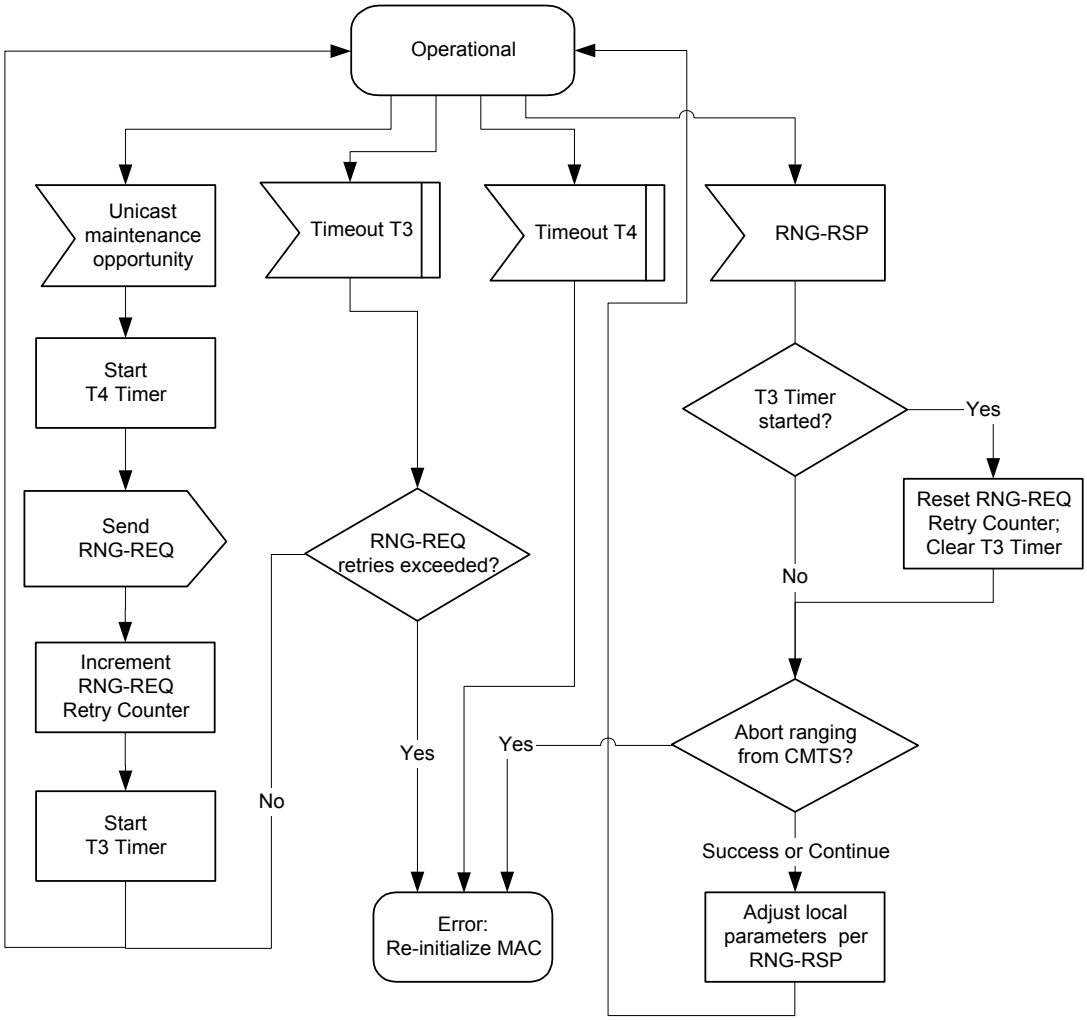


Figura B.11-17/J.112 – Alineación periódica – Visión del CM

B.11.3.2 Cambio de parámetros de ráfaga en sentido ascendente

Cuando el CMTS tenga que cambiar cualquiera de las características de una ráfaga en sentido ascendente, debe facilitar una transición ordenada de los valores antiguos a los valores nuevos por parte de todos los CM. Cada vez que el CMTS cambia alguno de los valores de ráfaga ascendente, DEBE anunciar los valores nuevos en un mensaje descriptor de canal en sentido ascendente, y el campo cuenta de cambios de la configuración DEBE incrementarse para indicar que ha cambiado un valor.

Después de transmitir uno o más mensajes UCD con el nuevo valor, el CMTS transmite un mensaje MAP con un conteo UCD que concuerde con el nuevo conteo de cambios de la configuración. El primer intervalo del MAP DEBE ser una concesión de datos de por lo menos 1 ms al ID de servicio nulo (cero). Es decir, el CMTS DEBE conceder 1 ms para que los módems de los cables cambien también sus parámetros de subcapa PMD de modo que concuerden con los nuevos. Este milisegundo se añade a otras restricciones de temporización MAP (véase B.9.1.5).

El CMTS NO DEBE transmitir ningún MAP con el conteo UCD antiguo después de transmitir el UCD nuevo.

El CM DEBE utilizar los parámetros del UCD correspondientes al "conteo UCD" del MAP para cualesquiera transmisiones que realice en respuesta a ese MAP. Si el CM no ha recibido, por el motivo que sea, el UCD correspondiente, no puede transmitir durante el intervalo descrito por ese MAP.

B.11.3.3 Cambio de canales en sentido ascendente

En cualquier momento después del registro, el CMTS puede ordenar al CM que cambie de canal en sentido ascendente, quizás para equilibrar el tráfico, evitar el ruido, o por otros diversos motivos que quedan fuera del alcance del presente anexo. La figura B.11-18 muestra el procedimiento que DEBE seguir el CMTS. La figura B.11-19 muestra el procedimiento correspondiente en el CM.

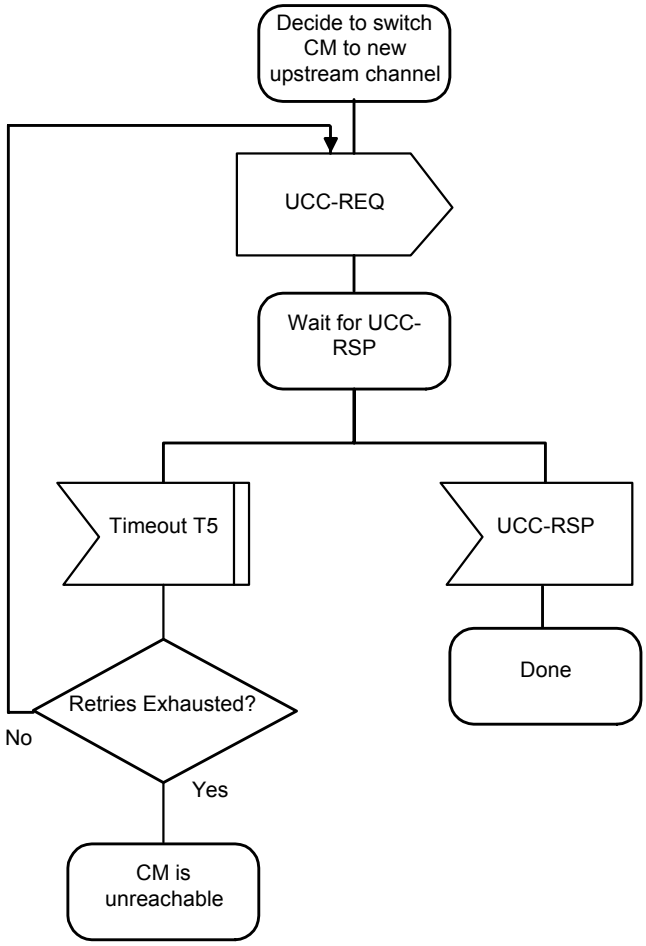


Figura B.11-18/J.112 – Cambio de canales en sentido ascendente: visión del CMTS

Se señala que si el CMTS intentara de nuevo el mensaje UCC-REQ, el CM podría haber cambiado ya los canales (si el UCC-RSP se hubiera perdido en el tránsito). En consecuencia, el CMTS DEBE estar a la escucha del mensaje UCC-RSP tanto en los canales antiguos como en los canales nuevos.

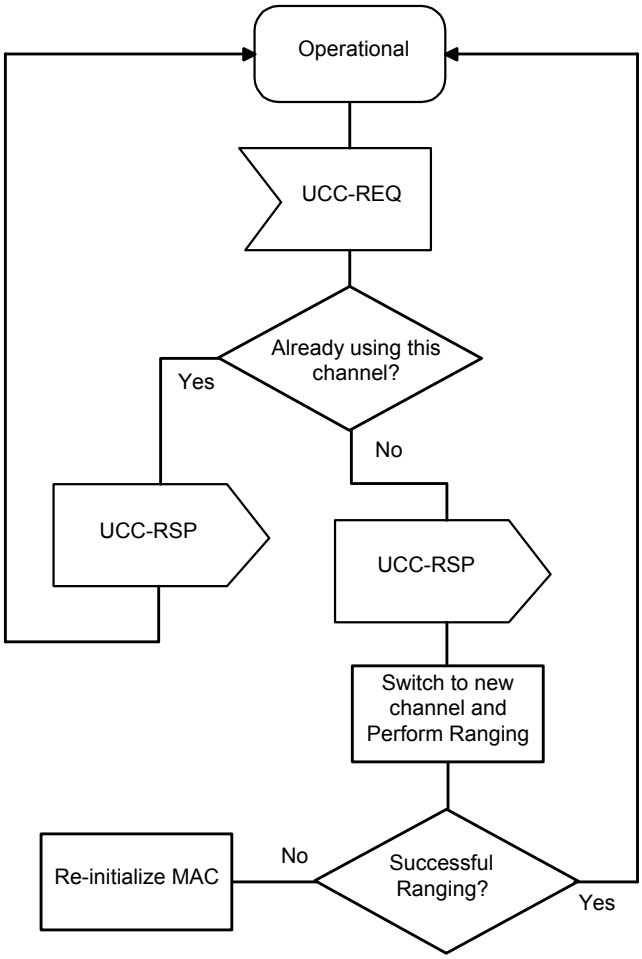


Figura B.11-19/J.112 – Cambio de canales en sentido ascendente – Visión del CM

Al sincronizar con el nuevo canal en sentido ascendente, el CM DEBE volver a alinear utilizando la tupla TLV de la técnica de alineación del mensaje UCC-REQ, si es que está presente. Si la tupla TLV no está presente en el mensaje UCC-REQ, el CM DEBE realizar mantenimiento inicial en el nuevo canal ascendente. (Véase B.8.3.10.1.1.)

Si el CM estableció con anterioridad la alineación en el nuevo canal, y si esa alineación en dicho canal sigue vigente (no ha transcurrido la temporización T4 desde la última alineación satisfactoria), el CM PUEDE utilizar información de alineación guardada y omitir la alineación.

El CM DEBERÍA guardar la información UCD de múltiples canales ascendentes para eliminar la espera del UCD correspondiente al nuevo canal ascendente.

El CM NO DEBE efectuar un registro nuevo, ya que su provisionamiento y dominio MAC siguen siendo válidos en el nuevo canal.

B.11.4 Servicio dinámico

Los flujos de servicio se pueden crear, cambiar o eliminar. Ello se logra a través de una serie de mensajes de gestión MAC denominados adición de servicio dinámica (DSA, *dynamic service addition*), cambio de servicio dinámico (DSC, *dynamic service change*) y eliminación de servicio dinámica (DSD, *dynamic service deletion*). Los mensajes DSA crean un nuevo flujo de servicio. Los mensajes DSC cambian un flujo de servicio existente. Los mensajes DSD eliminan un flujo de servicio existente. Esto se muestra en la figura B.11-20.

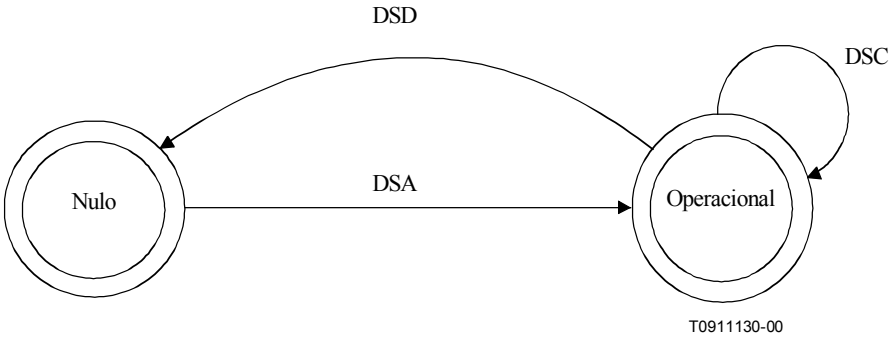


Figura B.11-20/J.112 – Visión general del flujo de servicio dinámico

El estado nulo implica la no existencia de un flujo de servicio que concuerde con la SFID y/o el TransactionID de un mensaje. Una vez que existe el flujo de servicio, será operacional y tendrá un SFID asignado. Funcionando en régimen permanente, un flujo de servicio reside en un estado nominal. Cuando se está produciendo el envío de mensajes de servicio dinámico, el flujo de servicio puede pasar por otros estados pero se mantiene operacional. Puesto que pueden existir múltiples flujos de servicio, pueden haber múltiples máquinas de estado activas, una por cada flujo de servicio. Los mensajes de servicio dinámico sólo afectan a aquellas máquinas de estado que concuerdan con el SFID y/o el TransactionID. Si se habilita la privacidad, tanto el CM como el CMTS DEBEN verificar el compendio HMAC de todos los mensajes de servicio dinámico antes de procesarlos y descartar cualquier mensaje que falle.

Los flujos de servicio creados en el momento del registro pasan al estado SF_operational sin una transacción DSA.

Los TransactionID son exclusivos para cada transacción, siendo seleccionados por el dispositivo iniciador (CM o CMTS). Para ayudar a evitar la ambigüedad y facilitar una comprobación sencilla, el espacio del número TransactionID se divide entre el CM y el CMTS. El CM DEBE seleccionar su TransactionID de la primera mitad del espacio de número (0x0000 a 0x7FFF). El CMTS DEBE seleccionar su TransactionID de la segunda mitad del espacio de número (0x8000 a 0xFFFF).

Cada secuencia de mensajes de servicio dinámico es una transacción única con un identificador de transacción único asociado. Las transacciones DSA/DSC consisten en una secuencia petición/respuesta/acuse de recibo. Las transacciones DSD consisten en una secuencia petición/respuesta. Los mensajes de respuesta DEBEN contener un código de confirmación "todo bien" a menos que se haya detectado alguna condición de excepción. Los mensajes de acuse de recibo DEBEN incluir el código de confirmación en la respuesta, a menos que surja una nueva condición de excepción. A continuación se muestra un diagrama de estados más detallado en el que se incluyen los estados de transición. Las acciones detalladas de cada transacción se indicarán en las subcláusulas que siguen.

B.11.4.1 Transiciones de estado de flujo de servicio dinámico

El diagrama de transición de estados de flujo de servicio dinámico es el diagrama de estado de nivel más alto, y controla el estado general del flujo de servicio. A medida que se necesita crea las transacciones, cada una de ellas representada por un diagrama de transición de estados de transacción, que hacen falta para proporcionar la señalización de DSA, DSC y DSD. Cada diagrama de transición de estados de transacción sólo se comunica con el diagrama progenitor de transición de estados de flujo de servicio dinámico. El diagrama de transición de estados de nivel superior filtra los mensajes de servicio dinámico y los pasa a la correspondiente transacción basándose en el identificador de flujo de servicio (SFID), número de referencia de flujo de servicio y TransactionID.

Hay seis tipos distintos de transacciones: iniciadas localmente o iniciadas remotamente, para cada uno de los mensajes DSA, DSC y DSD. La mayoría de las transacciones tienen tres estados básicos: pendiente, retención y eliminado. En el estado pendiente se entra típicamente luego de la creación; es donde la transacción está esperando una respuesta. En el estado de retención se entra típicamente una vez recibida la respuesta. El propósito de este estado es el permitir las retransmisiones en caso de un mensaje perdido, aún cuando la entidad local haya percibido que se ha completado la transacción. En el estado de eliminación se entra sólo si se está eliminando el flujo de servicio mientras se está procesando una transacción.

Los diagramas de flujo proporcionan una representación detallada de cada uno de los estados en los diagramas de transición de estados de transacción. Se muestran todas las transiciones válidas. Cualquier entrada que no se muestre debería ser tratada como una condición de error grave.

Con una sola excepción, estos diagramas de estado se aplican por igual al CMTS y al CM. En el estado local, cambiante de servicio de flujo dinámico, hay una sutil diferencia entre los comportamientos del CM y el CMTS. Esto se destaca en los diagramas de transición de estados y los diagramas de flujo detallados.

La variable "Num Xacts" del diagrama de transición de estados de flujo de servicio dinámico se incrementa cada vez que el diagrama de estados de nivel superior crea una transacción, y disminuye cada vez que se termina una transacción. Un flujo de servicio dinámico NO DEBE volver al estado nulo hasta que haya sido eliminado y todas las transacciones hayan terminado.

A continuación se identifican las entradas a los diagramas de estado.

Entradas al diagrama de transición de estados de flujo de servicio dinámico provenientes de entidades sin especificar, locales y de nivel superior:

- añadir;
- cambiar;
- eliminar.

Entradas al diagrama de transición de estados de flujo de servicio dinámico provenientes de diagramas de transición de estado de transacción DSx;

- DSA Succeeded (DSA Logrado)
- DSA Failed (DSA Fallido);
- DSA ACK Lost (DSA ACK Perdido);
- DSA Erred (DSA Errado);
- DSA Ended (DSA Terminado);
- DSC Succeeded (DSC Logrado);
- DSC Failed (DSC Fallido);
- DSC ACK Lost (DSA ACK Perdido);
- DSC Erred (DSC Errado);
- DSC Ended (DSC Terminado);
- DSD Succeeded (DSD Logrado);
- DSD Erred (DSD Errado);
- DSD Ended (DSD Terminado);

Entradas al diagrama de transición de estados de transacción DSx provenientes del diagrama de transición de estados de flujo de servicio dinámico:

- SF Add (SF Añadir);
- SF Change (SF Cambiar);

- SF Delete (SF Eliminar);
- SF Abort Add (SF Abortar Añadir);
- SF Change-Remote (SF Cambiar-Distante);
- SF Delete-Local (SF Eliminar-Local);
- SF Delete-Remote (SF Eliminar-Remoto);
- SF DSA-ACK Lost (SF DSA-ACK Perdido);
- SF-DSC-REQ Lost (SF-DSC-REQ Perdido);
- SF-DSC-ACK Lost (SF-DSC-ACK Perdido);
- SF DSD-REQ Lost (SF DSD-REQ Perdido);
- SF Changed (SF Cambiado);
- SF Deleted (SF Eliminado).

La creación de transacciones DSx por parte del diagrama de transición de estados de flujo de servicio dinámico se indica por medio de la notación

DSx-[Local | Remote] (initial_input),

donde initial_input (entrada inicial) puede ser SF Agregar, DSA-REQ, SF Cambiar, DSC-REQ, SF eliminar o DSD-REQ según sea el tipo de la transacción y el iniciador.

Véanse las figuras B.11-21 a B.11-27.

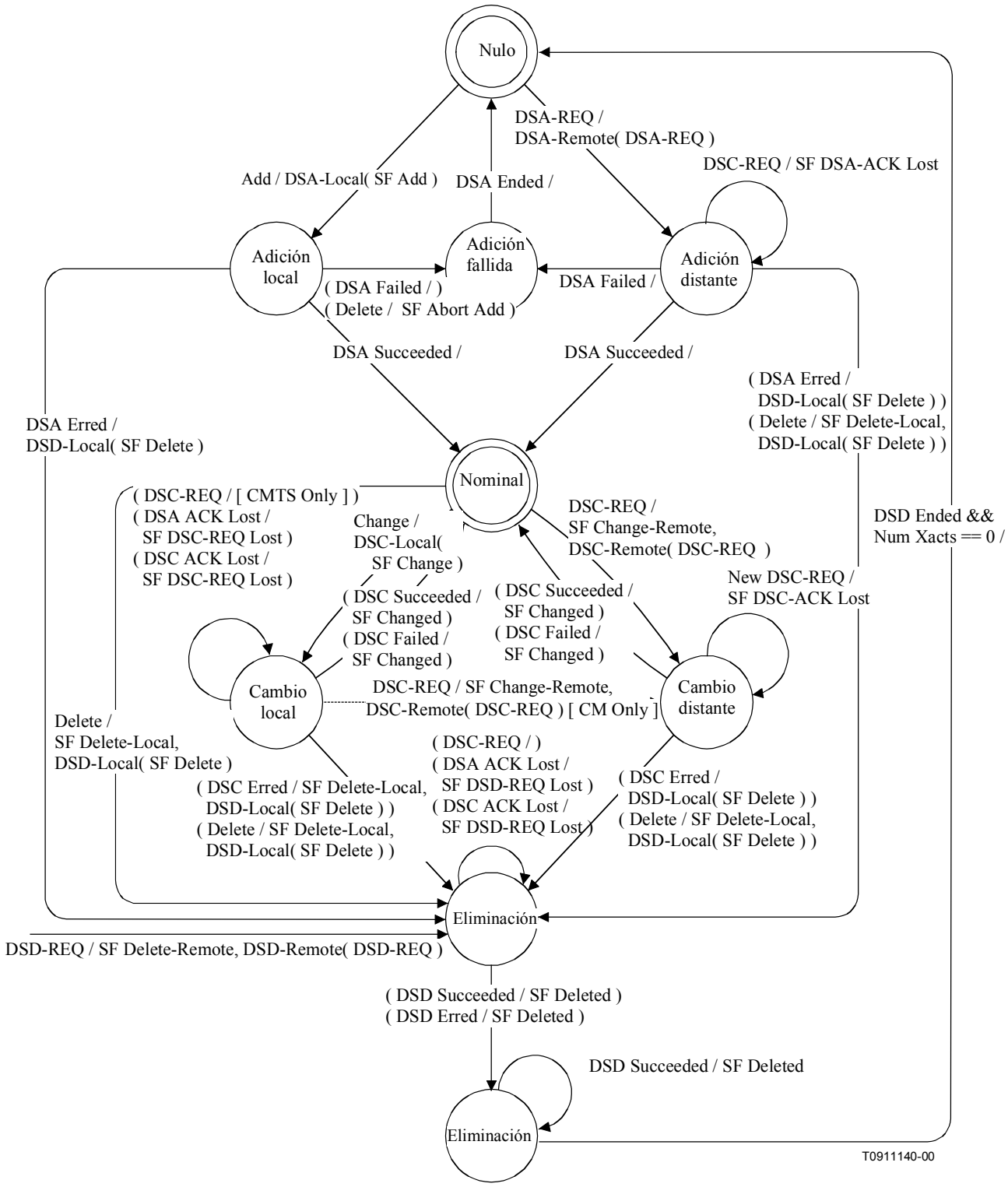


Figura B.11-21/J.112 – Diagrama de transiciones de estado de flujo de servicio dinámico

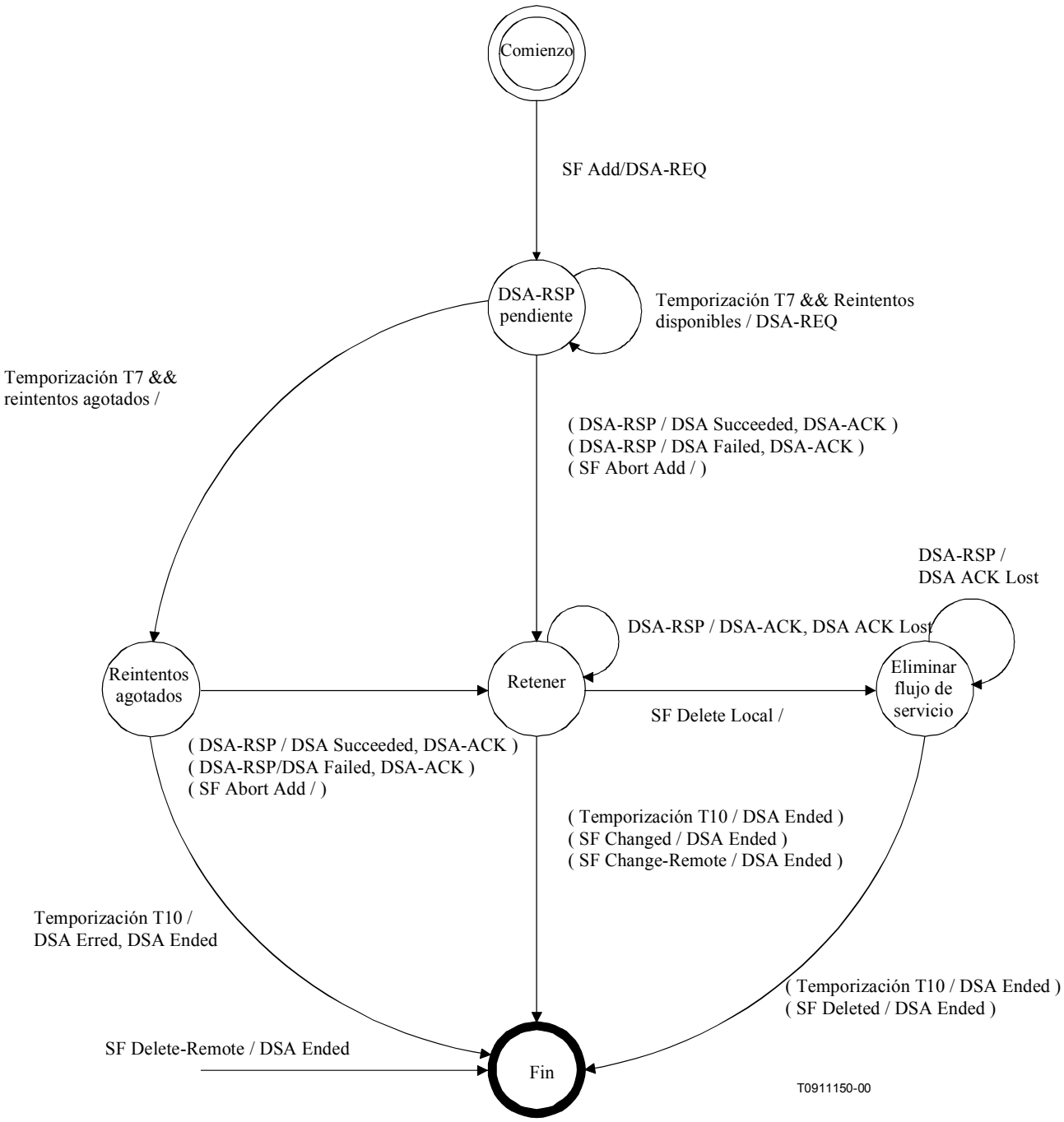


Figura B.11-22/J.112 – DSA – Diagrama de transición de estados de transacción iniciada localmente

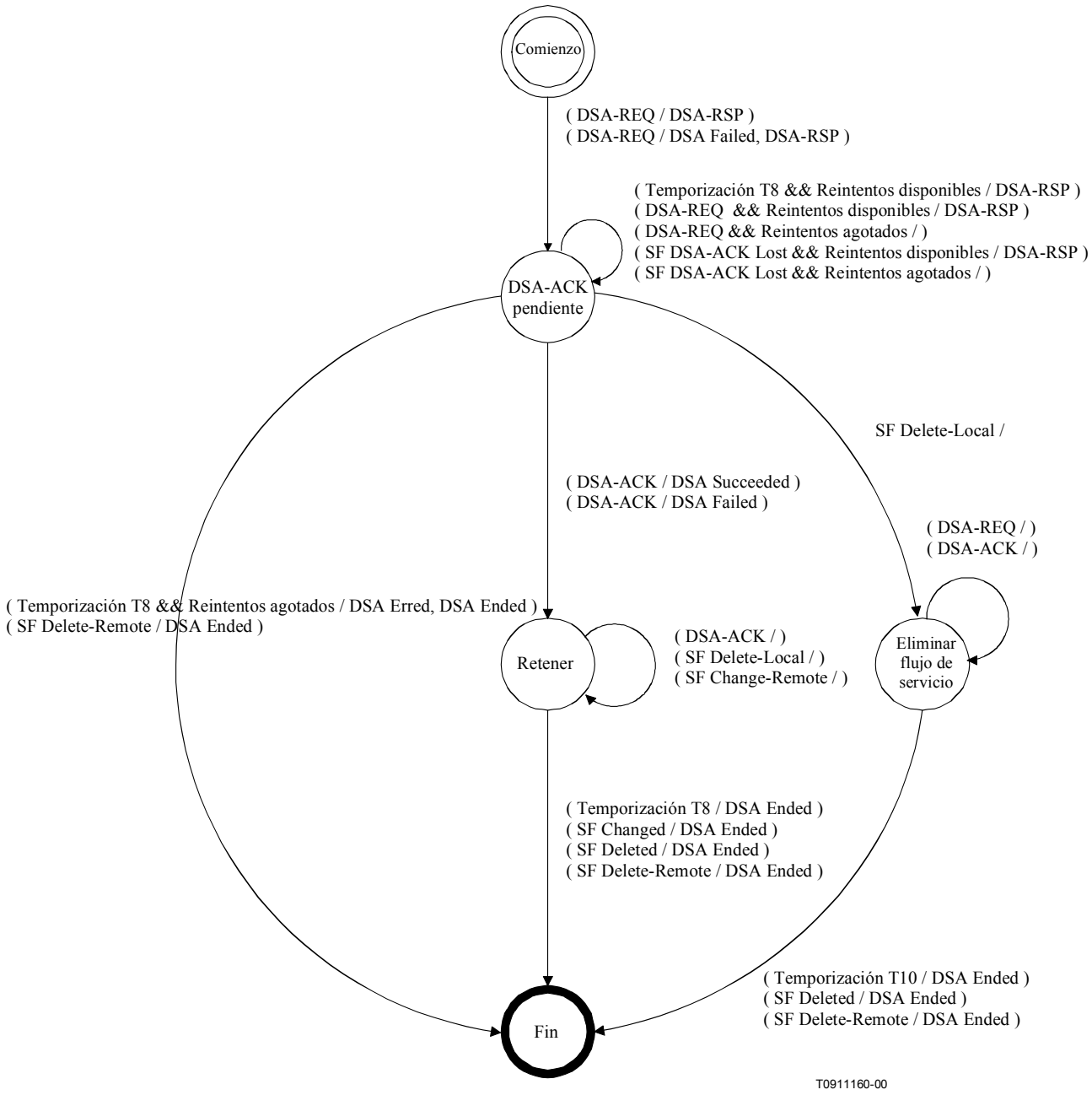


Figura B.11-23/J.112 – DSA – Diagrama de transición de estados de transacción iniciada a distancia

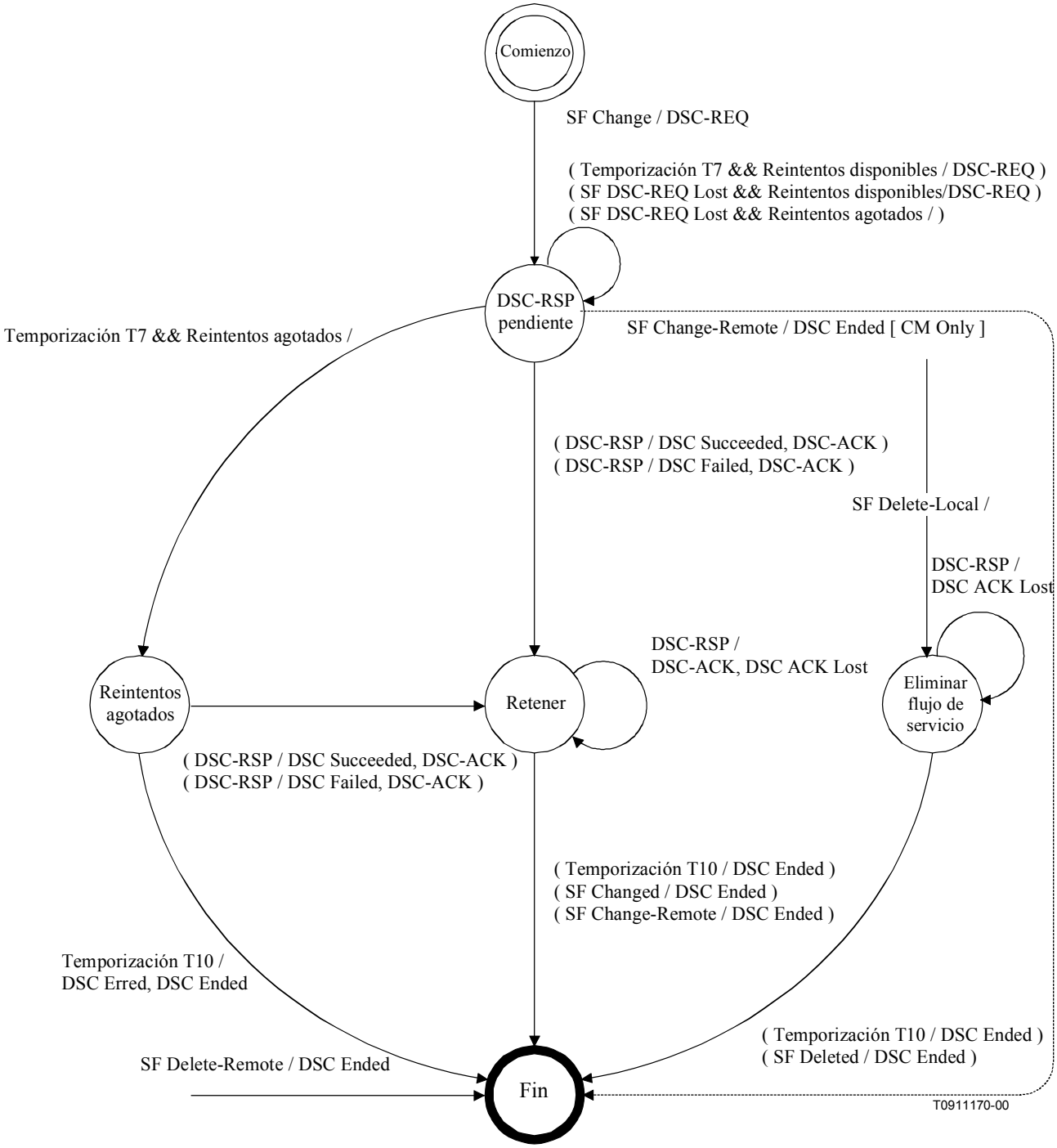


Figura B.11-24/J.112 – DSC – Diagrama de transición de estados de transacción iniciada localmente

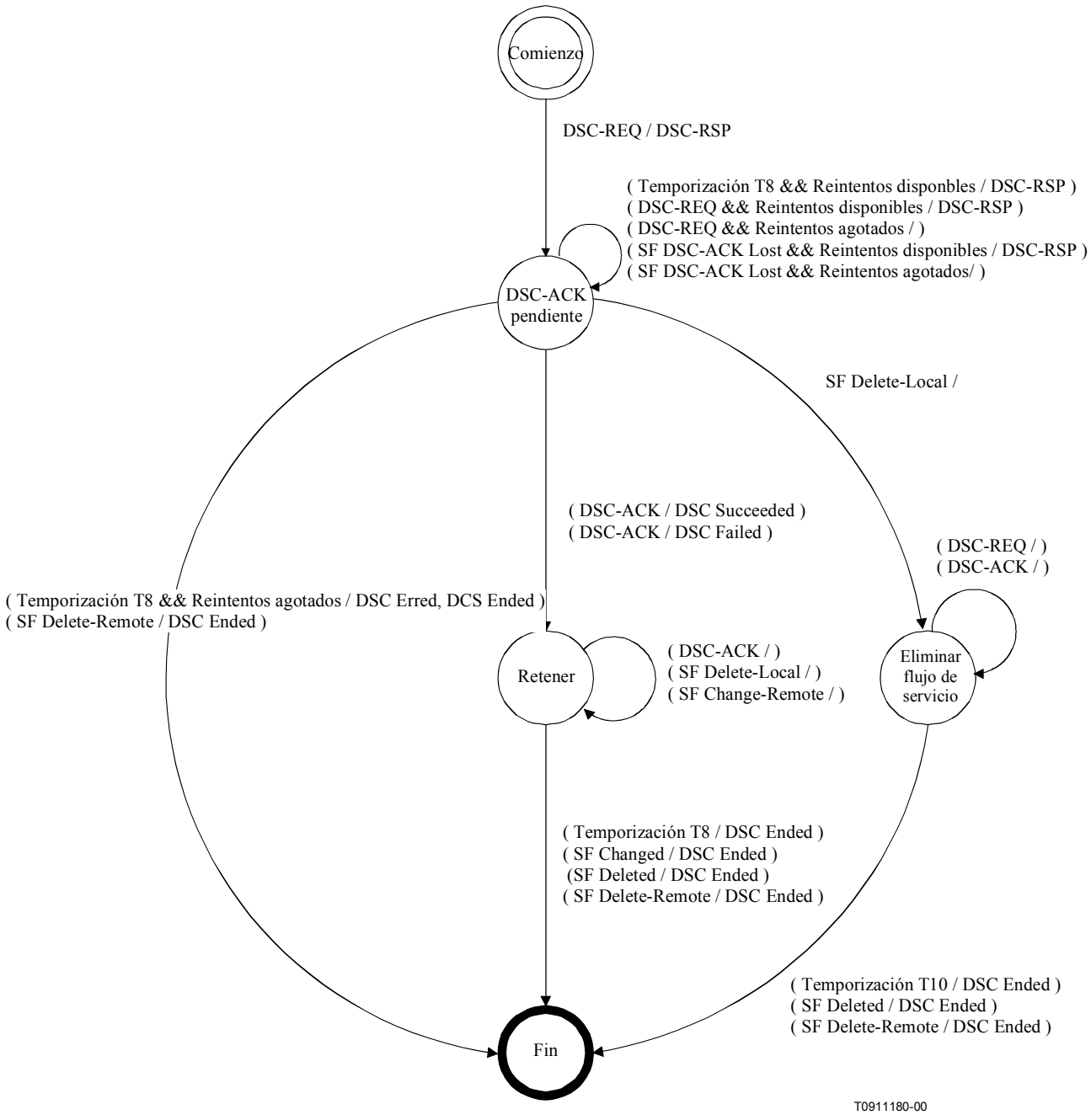


Figura B.11-25/J.112 – DSC – Diagrama de transición de estados de transacción iniciada a distancia

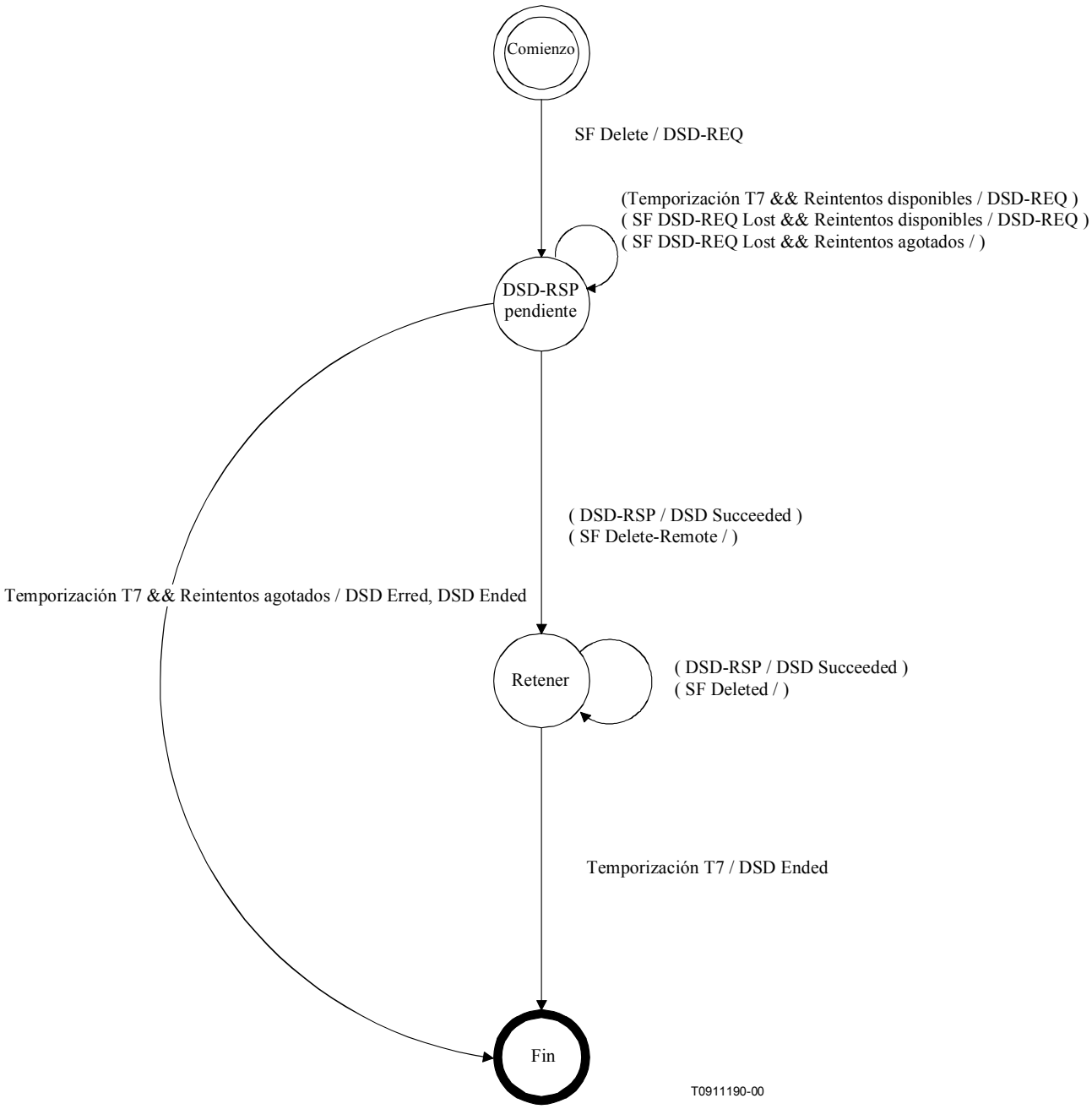


Figura B.11-26/J.112 – DSD – Diagrama de transición de estados de transacción iniciada localmente

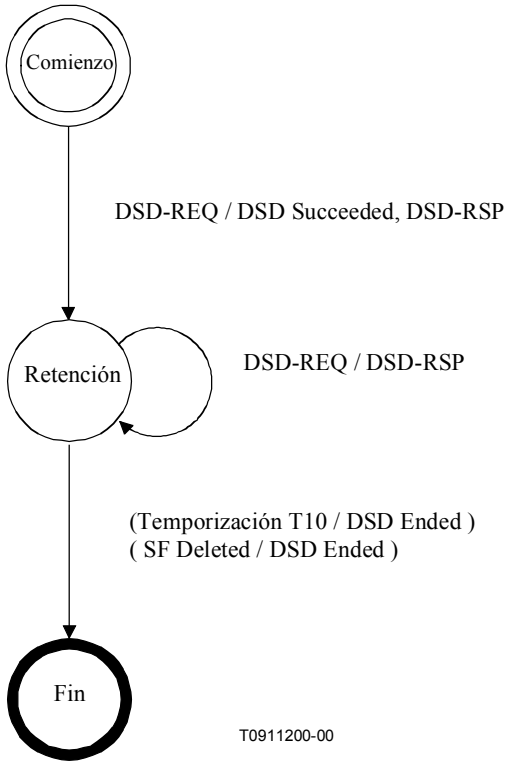


Figura B.11-27/J.112 – Eliminación dinámica (DSD) – Diagrama de transición de estados de transacción iniciada a distancia

B.11.4.2 Adición de servicio dinámico

B.11.4.2.1 Adición de servicio dinámica iniciada por el CM

Un CM que desea crear un flujo de servicio ascendente y/o descendente envía una petición al CMTS utilizando un mensaje de petición de adición de servicio dinámica (DSA-REQ, *dynamic service addition request message*). El CMTS verifica la autorización del CM para el (los) servicio(s) pedido(s) y si son soportados los requisitos de QoS, y genera una respuesta adecuada utilizando un mensaje de respuesta de adición de servicio dinámica (DSA-RSP, *dynamic service addition response message*). El CM concluye la transacción con un mensaje de acuse de recibo (DSA-ACK).

A fin de facilitar una respuesta de admisión en común, se pueden incluir en un único DSA-REQ un flujo de servicio ascendente y uno descendente. Ambos flujos de servicio son aceptados o rechazados de forma conjunta.

Véase la figura B.11-28.

CM		CMTS
Nuevo(s) flujo(s) de servicio necesario(s) Comprobar si hay recursos disponibles		
Enviar DSA-REQ	**——DSA-REQ——►**	**Recibir DSA-REQ** Verificar si el CM está autorizado para el (los) servicio(s) (véase la nota). Comprobar que se soporta QoS de flujo(s) de servicio Crear SFID(s) Si AdmittedQosParamSet ascendente es no nulo, crear SID. Si ActiveQosParamSet ascendente es no nulo, habilitar recepción de datos en nuevo flujo de servicio ascendente.
Recibir DSA-RSP Si ActiveQosParamSet es no nulo, habilitar transmisión y/o recepción de datos en nuevo(s) flujo(s) de servicio.	**◄——DSA-RSP——**	**Enviar DSA-RSP**
Enviar DSA-ACK	**——DSA-ACK——►**	**Recibir DSA-ACK** Si ActiveQosParamSet descendente es no nulo, habilitar transmisión de datos en nuevo flujo de servicio descendente
NOTA – La autorización puede producirse antes que el CMTS reciba el DSA-REQ. Los detalles de la señalización de CMTS para prever un DSA-REQ quedan más allá del alcance del presente anexo B.		

Figura B.11-28/J.112 – Adición de servicio dinámica iniciada por el CM

B.11.4.2.2 Adición de servicio dinámica iniciada por el CMTS

Un CMTS que desea establecer uno o más flujos de servicio dinámico ascendentes o descendentes con un CM realiza las siguientes operaciones. El CMTS verifica la autorización del CM de destino para la clase de servicio pedida y si son soportados los requisitos de QoS. Si el servicio es soportado, el CMTS genera nuevo(s) SFID con la clase de servicio pedida e informa al CM por medio de un mensaje de petición de adición de servicio dinámica (DSA-REQ). Si el CM comprueba que puede soportar el servicio, responde con un mensaje de respuesta de adición de servicio dinámica (DSA-RSP). El CMTS concluye la transacción enviando el mensaje de acuse de recibo (DSA-ACK).

Véase la figura B.11-29.

CM		CMTS
		Nuevo(s) flujo(s) de servicio requeridos para CM. Verificar que CM está autorizado para el (los) servicio(s) Comprobar que se soporte QoS de flujo(s) de servicio Crear SFID(s) Si AdmittedQosParamSet ascendente es no nulo, crear SID. Si ActiveQosParamSet ascendente es no nulo, habilitar recepción de datos en nuevo flujo de servicio ascendente
Recibir DSA-REQ Confirmar que CM puede soportar flujo(s) de servicio Añadir SFID descendente (si está presente) Habilitar recepción en cualquier nuevo flujo de servicio descendente	**◄—DSA-REQ—**	**Enviar DSA-REQ**
Enviar DSA-RSP	**—DSA-RSP—►**	**Recibir DSA-RSP** Habilitar transmisión y recepción de datos en nuevo(s) flujo(s) de servicio
Recibir DSA-ACK Habilitar transmisión en nuevo flujo de servicio ascendente	**◄—DSA-ACK—**	**Enviar DSA-ACK**

Figura B.11-29/J.112 – Adición de servicio dinámica iniciada por el CMTS

B.11.4.2.3 Diagramas de transiciones de estados de adición de servicio dinámica

Véanse las figuras B.11-30 a B.11-38.

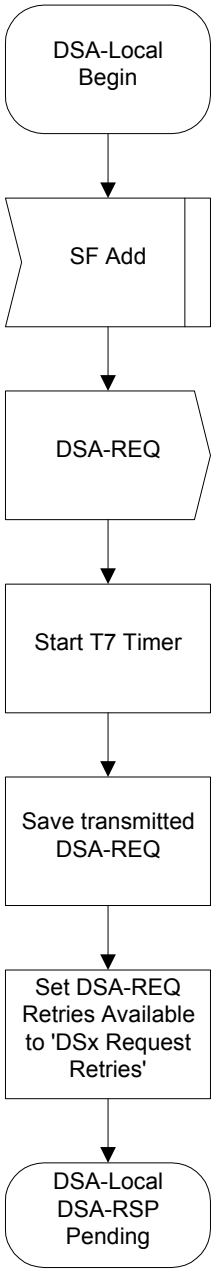


Figura B.11-30/J.112 – DSA – Diagrama de flujo de estados de comienzo de transacción iniciada localmente

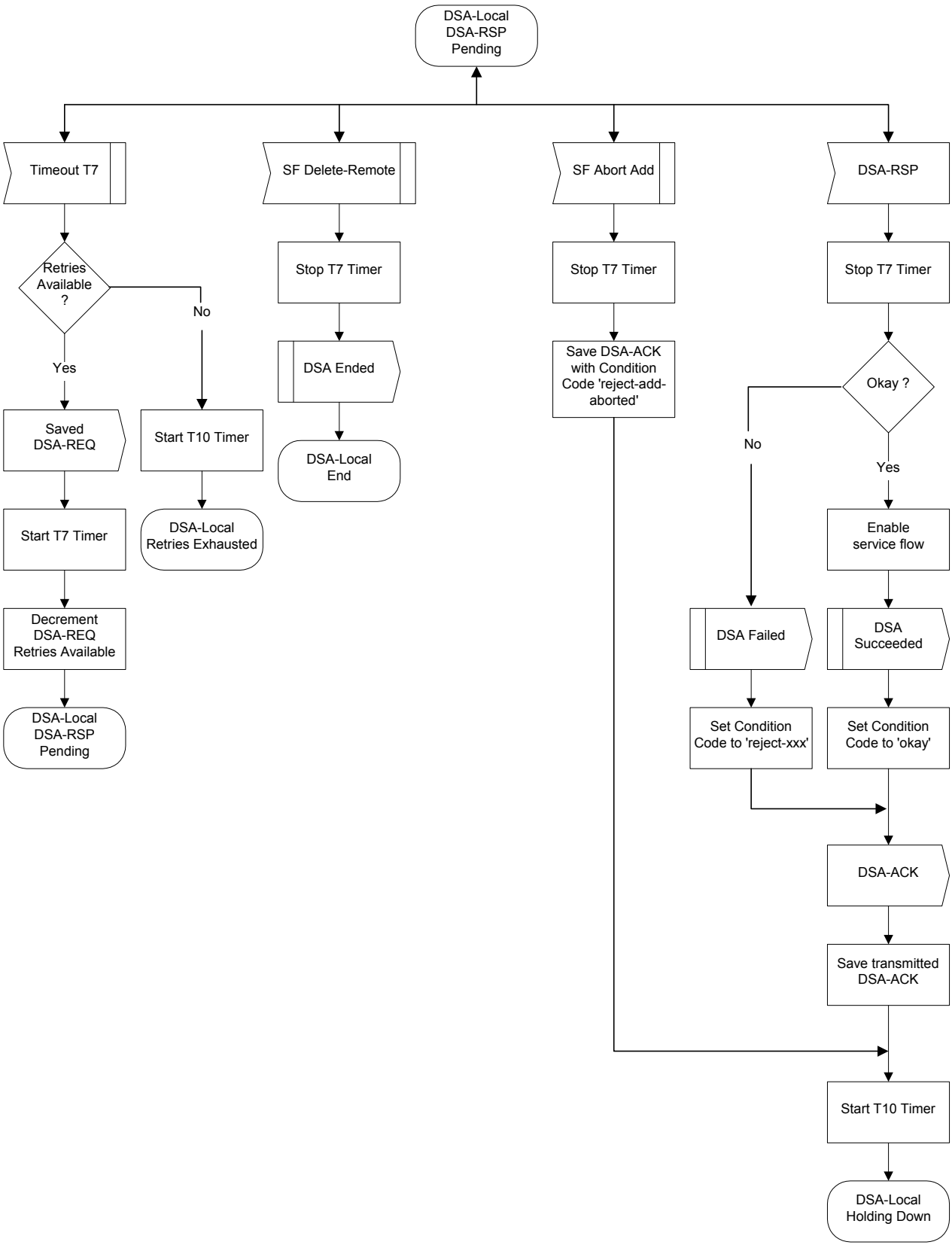


Figura B.11-31/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada localmente con DSA-RSP pendiente

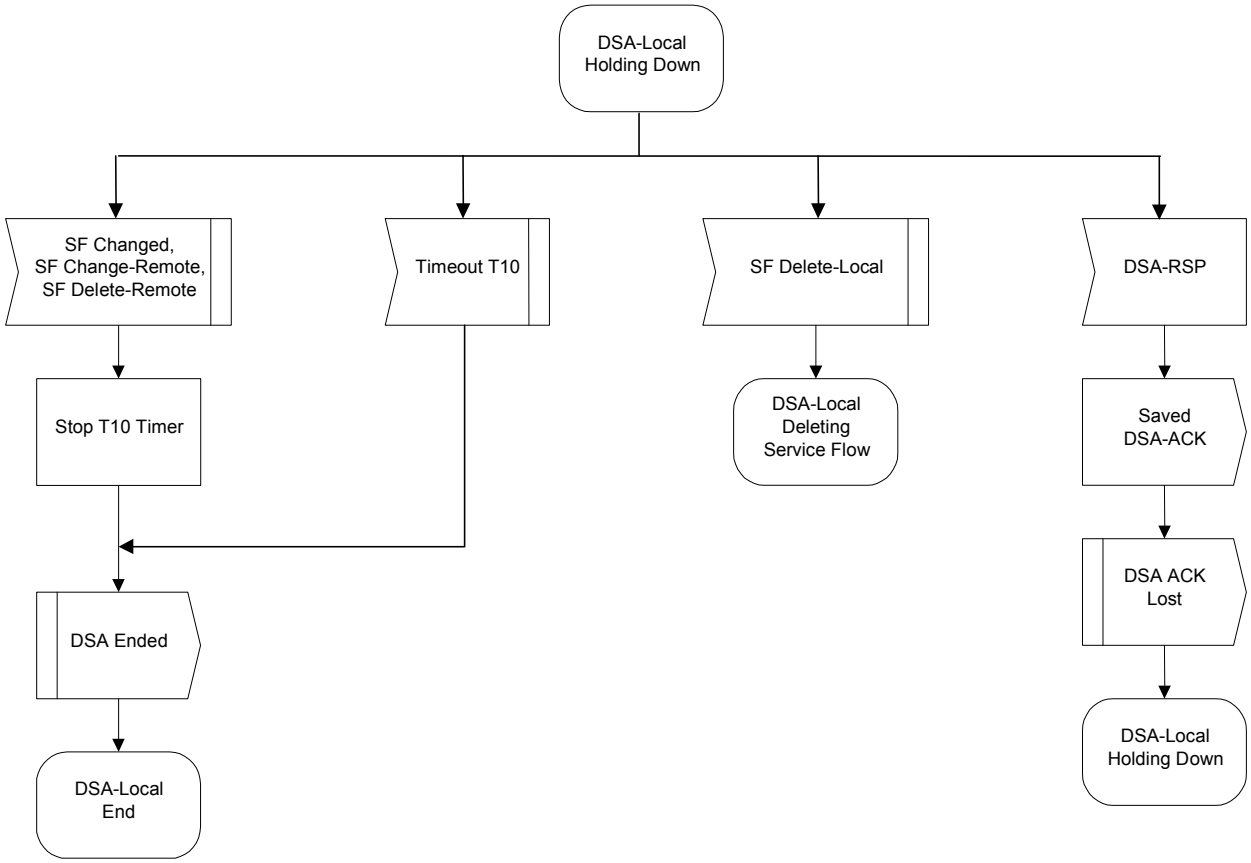


Figura B.11-32/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada localmente con retención

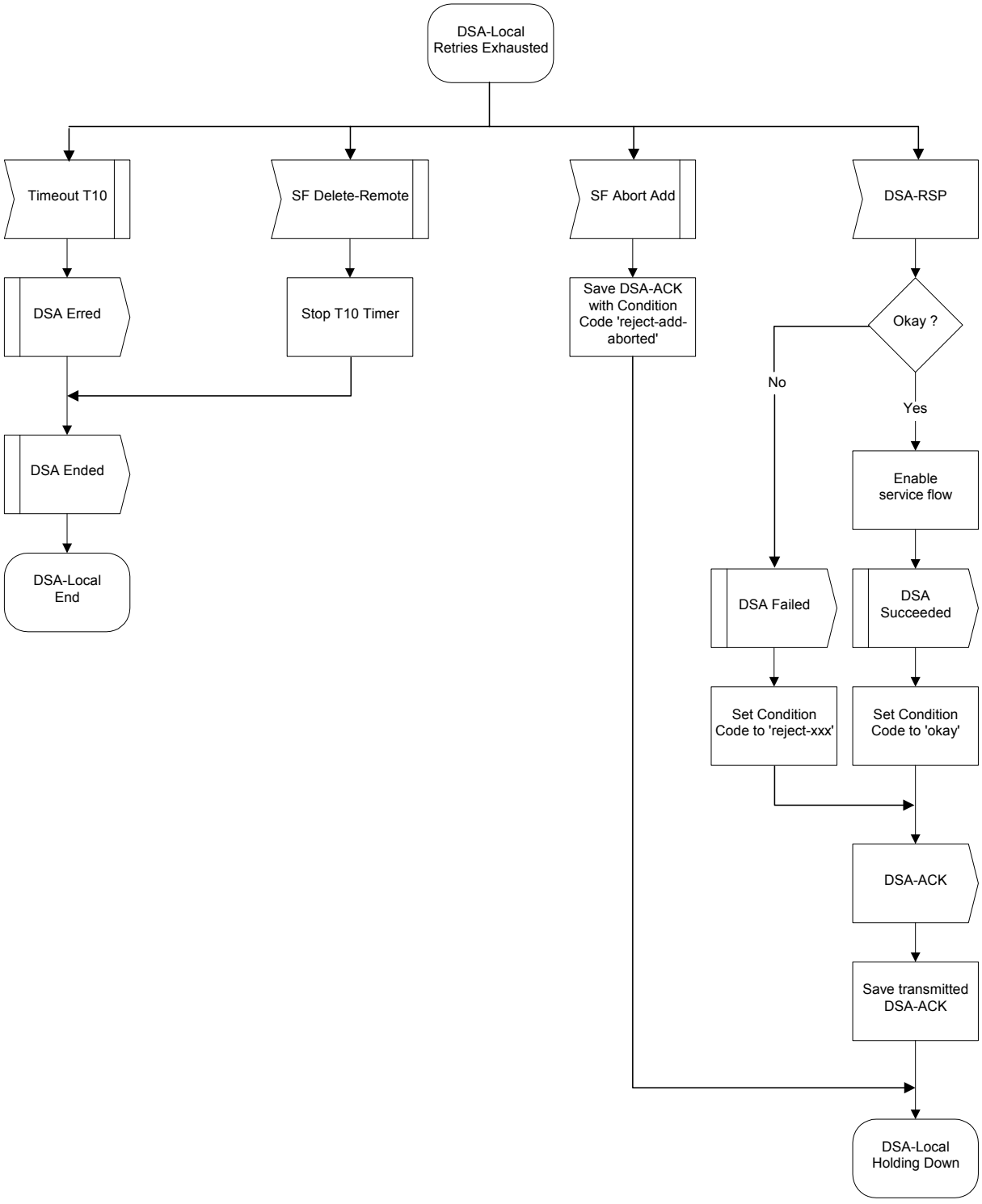


Figura B.11-33/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada localmente con reintentos agotados

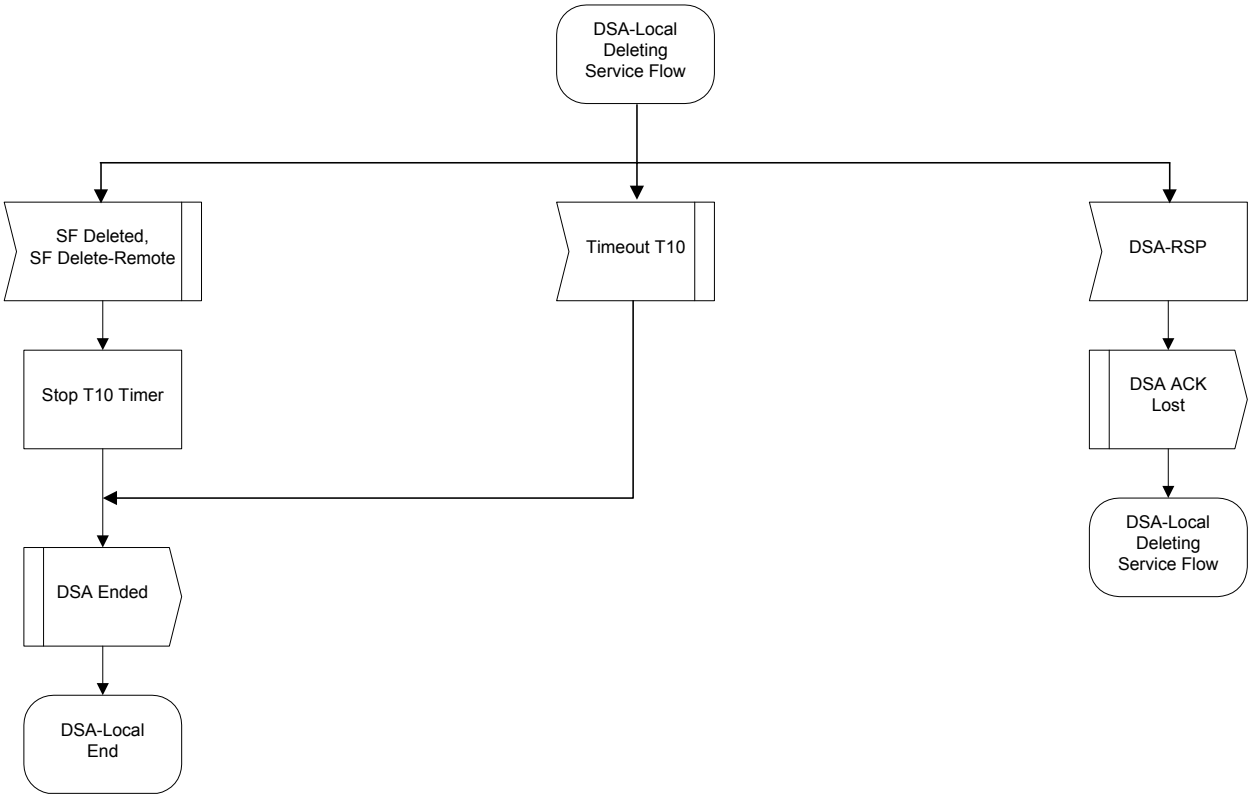


Figura B.11-34/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada localmente con eliminación de flujo de servicio

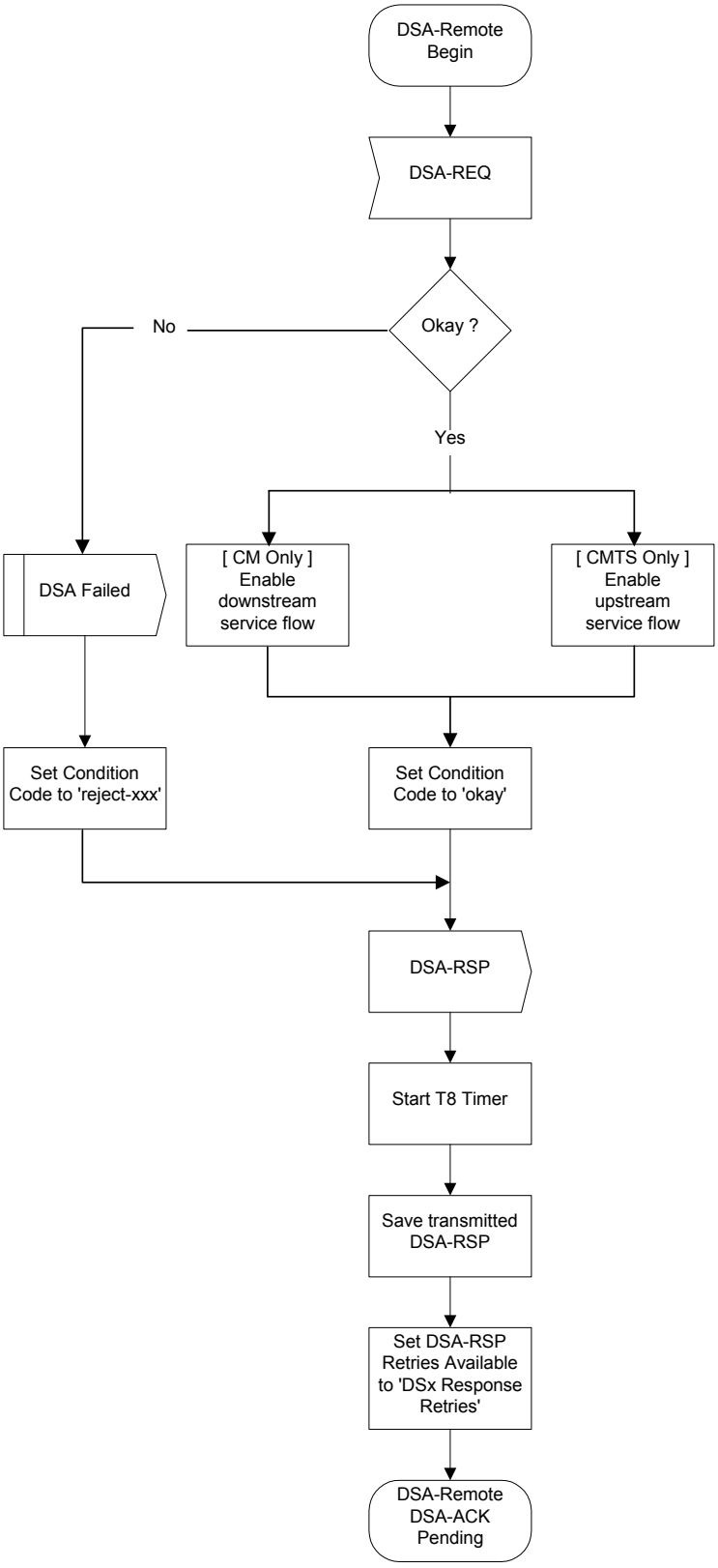


Figura B.11-35/J.112 – DSA – Diagrama de flujo de estados de comienzo de transacción iniciada a distancia

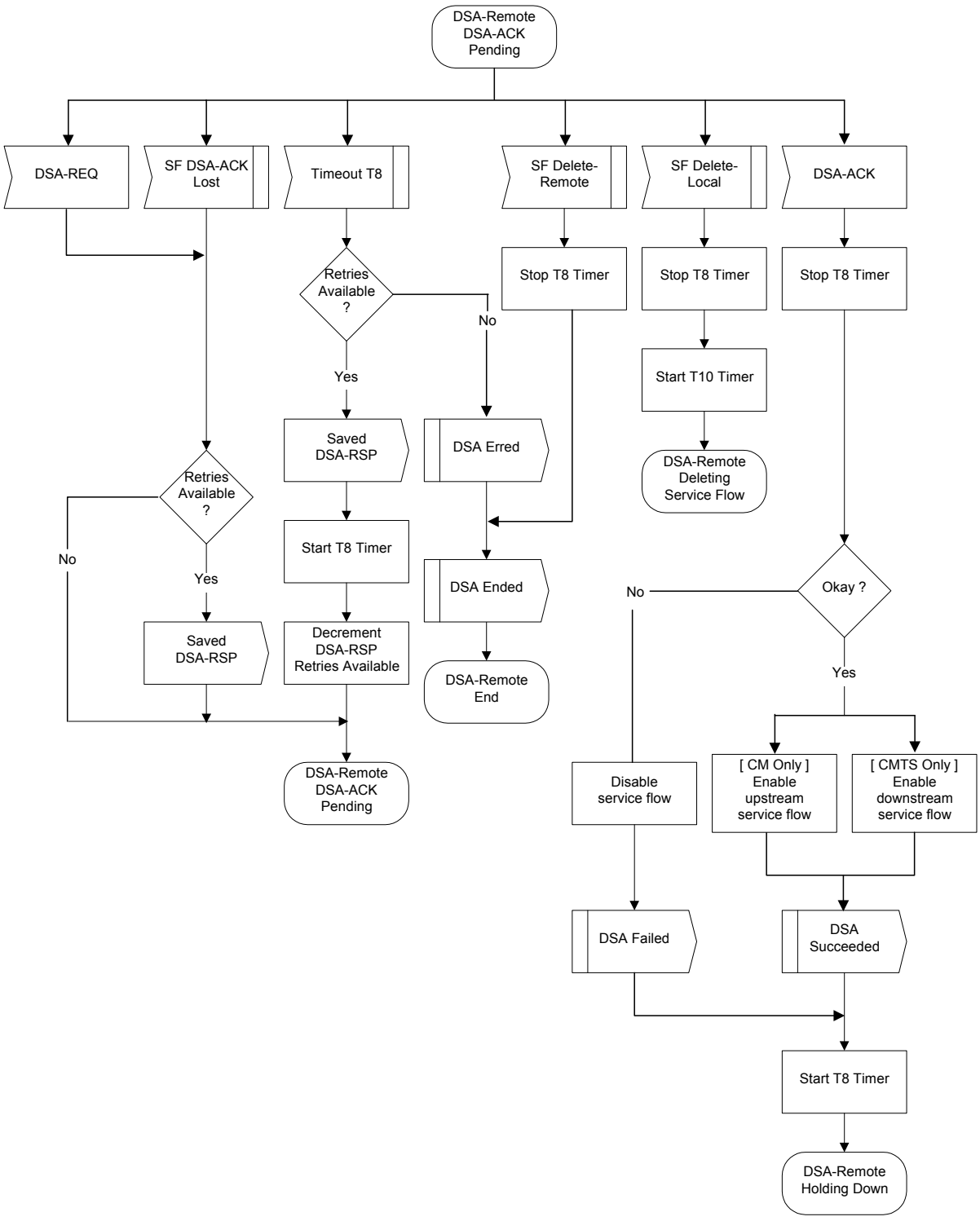


Figura B.11-36/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada a distancia con DSA-ACK pendiente

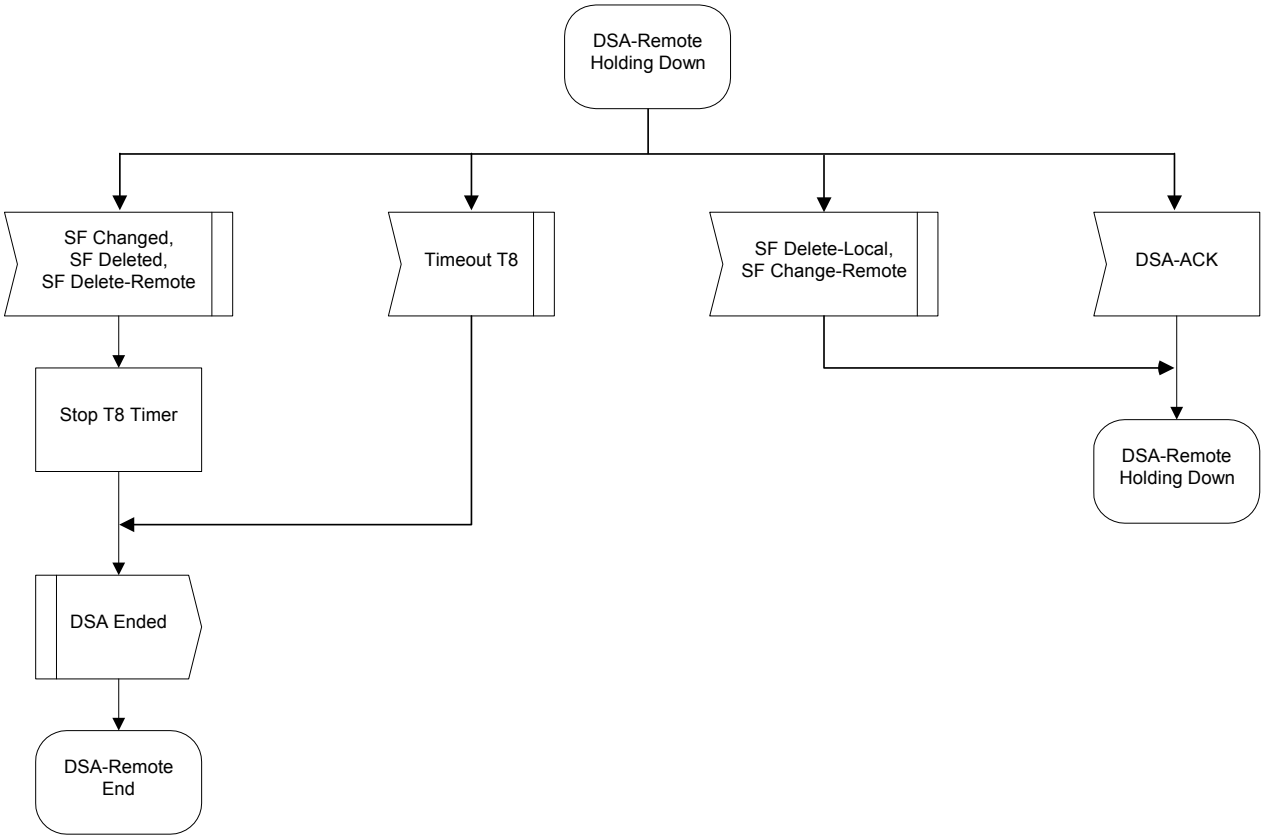


Figura B.11-37/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada a distancia con retención

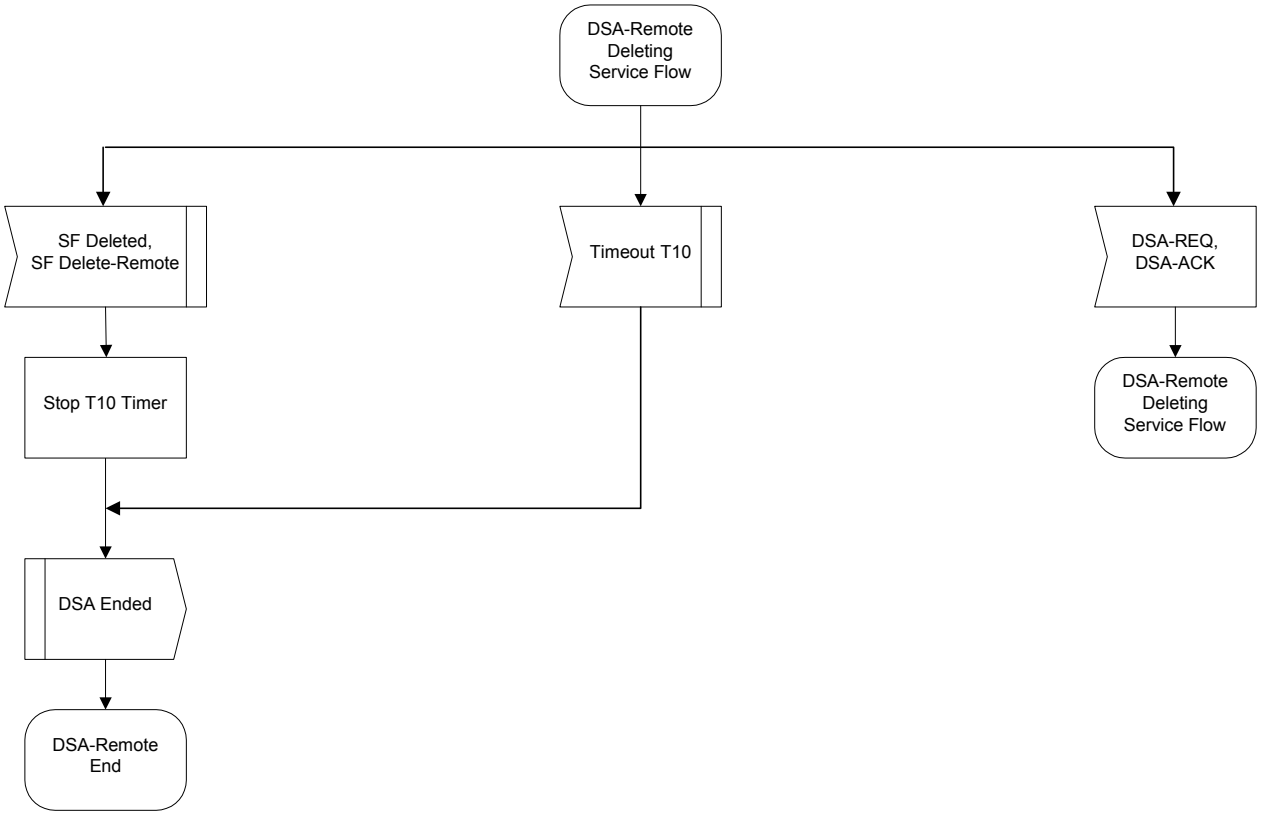


Figura B.11-38/J.112 – DSA – Diagrama de flujo de estados de transacción iniciada a distancia con eliminación de servicio

B.11.4.3 Cambio de servicio dinámico

El conjunto de mensajes de cambio de servicio dinámico (DSC) se utiliza para modificar los parámetros de flujo asociados a un flujo de servicio. En particular, DSC puede:

- modificar la especificación de flujo de servicio;
- agregar, eliminar o reemplazar un clasificador de flujo;
- agregar, eliminar o establecer elementos PHS.

Un único intercambio de mensajes DSC puede modificar los parámetros de un flujo de servicio en sentido descendente y/o un flujo de servicio en sentido ascendente.

Para impedir la pérdida de paquetes, se secuencia cualquier cambio de anchura de banda requerido entre el CM y el CMTS.

El CMTS controla la planificación tanto en sentido ascendente como descendente. La temporización de los cambios de la planificación es independiente del sentido Y también de si se trata de un incremento o una disminución de la anchura de banda. El CMTS cambia siempre la planificación al recibir una DSC-REQ (transacción iniciada por el CM) o un DSC-RSP (transacción iniciada por el CMTS).

El CMTS también controla el comportamiento de la transmisión en sentido descendente. El cambio en el comportamiento de la transmisión en sentido descendente coincide siempre con el cambio en la planificación en sentido descendente (es decir, el CMTS los controla a ambos y los modifica a ambos simultáneamente).

El CM controla el comportamiento de la transmisión en sentido ascendente. La temporización de los cambios del comportamiento de transmisión del CM es función de cuál dispositivo inició la transacción Y también de si el cambio es un "incremento" o una "disminución" de la anchura de banda.

Si se está reduciendo la anchura de banda del un flujo de servicio ascendente, el CM reduce primero la anchura de banda de su cabida útil, y luego el CMTS reduce la anchura de banda planificada para el flujo de servicio. Si se está incrementando la anchura de banda del un flujo de servicio ascendente, el CMTS incrementa primero la anchura de banda planificada para el flujo de servicio, y luego el CM incrementa la anchura de banda para su cabida útil.

Si los cambios de anchura de banda son complejos, es posible que al CM no le resulte evidente cuándo tiene que realizar los cambios de ancho de banda. Esta información se le puede señalizar al CM desde una entidad de capa superior. Análogamente, si la señalización DSC es iniciada por el CMTS, el CMTS PUEDE indicar al CM si debería instalar o suprimir clasificadores tras recibir la petición de DSC o si debería posponer esta instalación hasta recibir el acuse de recibo de DSC (véase B.C.2.1.8).

Cualquier flujo de servicio puede ser desactivado con una instrucción de cambio de servicio dinámico enviando un mensaje DSC-REQ, haciendo referencia al identificador de flujo de servicio, e incluyendo un ActiveQosParameterSet nulo. Sin embargo, si se desactiva el flujo de servicio primario de un CM, dicho CM queda eliminado del registro y DEBE volver a registrarse. Ha de tenerse cuidado, por tanto, antes de desactivar esos flujos de servicio. Si se desactiva un flujo de servicio que fue aprovisionado durante el registro, la información de aprovisionamiento de ese flujo de servicio DEBE mantenerse hasta que se vuelva a reactivar el flujo de servicio.

Un CM DEBE tener sólo una transacción DSC pendiente por cada flujo de servicio. Si el CM detecta una segunda transacción iniciada por el CMTS, DEBE abortar la transacción que inició y permitir que se complete la transacción iniciada por el CMTS.

Un CMTS DEBE tener sólo una transacción DSC pendiente por cada flujo de servicio. Si el CMTS detecta una segunda transacción iniciada por el CM, DEBE abortar la transacción que inició el CM y permitir que se complete la transacción iniciada por él mismo.

NOTA – Es probable que las aplicaciones actualmente previstas controlen un flujo de servicio ya sea mediante el CM o el CMTS, pero no mediante ambos. Por lo tanto, el caso de la iniciación simultánea de un DSC por el CM y el CMTS se considera como una condición de excepción y así se trata.

B.11.4.3.1 Cambio de servicio dinámico iniciado por el CM

Un CM que necesite cambiar la definición de un flujo de servicio, llevará a cabo las operaciones que se detallan a continuación (véase la figura B.11-39).

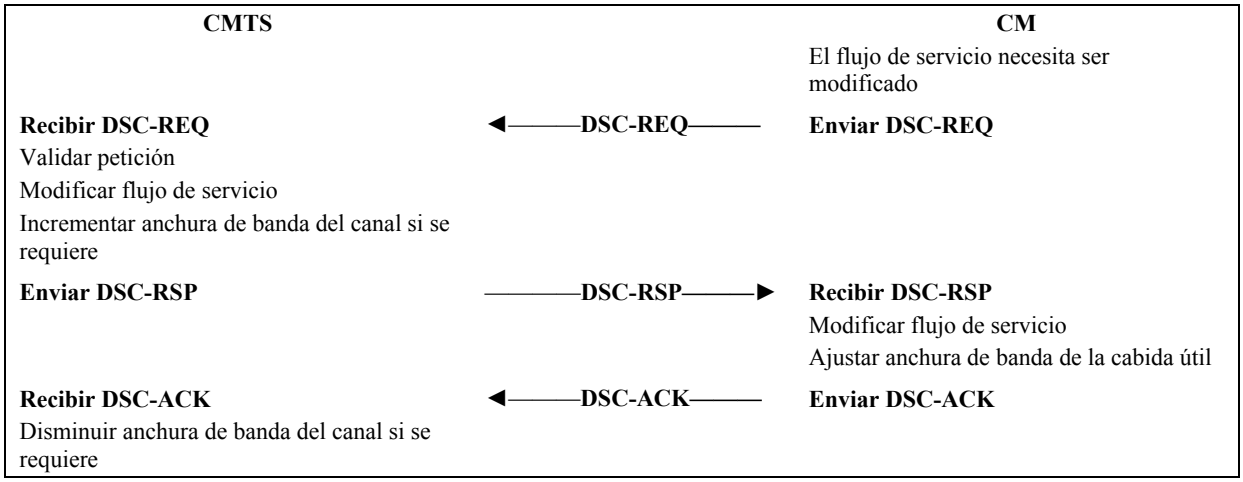


Figura B.11-39/J.112 – DSC iniciado por el CM

El CM informa al CMTS utilizando un mensaje de petición de cambio de servicio dinámico (DSC-REQ). El CMTS DEBE decidir si el flujo de servicio al que se hace referencia admite esta modificación. El CMTS DEBE responder con una respuesta de cambio de servicio dinámico (DSC-RSP) indicando la aceptación o el rechazo. El CM vuelve a configurar el flujo de servicio si procede, y a continuación DEBE responder con un acuse de recibo de cambio de servicio dinámico (DSC-ACK, *dynamic service change acknowledge*).

B.11.4.3.2 Cambio de servicio dinámico iniciado por el CMTS

Un CMTS que necesite cambiar la definición de un flujo de servicio, llevará a cabo las operaciones que se detallan a continuación (véase la figura B.11-40).

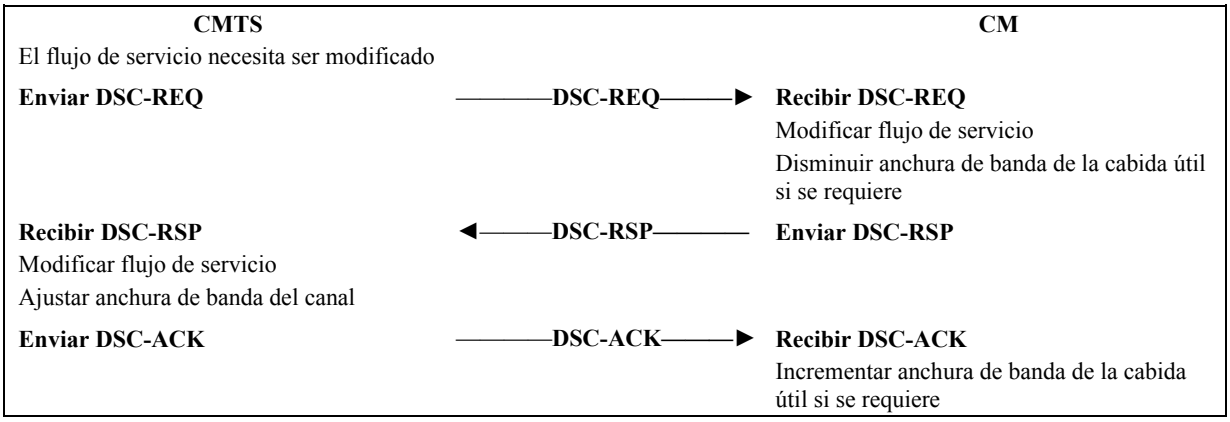


Figura B.11-40/J.112 – DSC iniciado por el CMTS

El CMTS DEBE decidir si el flujo de servicio al que se hace referencia soporta esta modificación. Si así es, el CMTS informa al CM utilizando un mensaje de petición de cambio de servicio dinámico (DSC-REQ, *dynamic service change request message*). El CM comprueba que puede admitir el cambio de servicio y DEBE responder con una respuesta de cambio de servicio dinámico (DSC-RSP, *dynamic service change response*) indicando la aceptación o el rechazo. El CMTS vuelve a configurar el flujo de servicio si procede, y a continuación DEBE responder con un acuse de recibo de cambio de servicio dinámico (DSC-ACK).

B.11.4.3.3 Diagramas de transiciones de estados de cambio de servicio dinámico

Véanse las figuras B.11-41 a B.11-49.

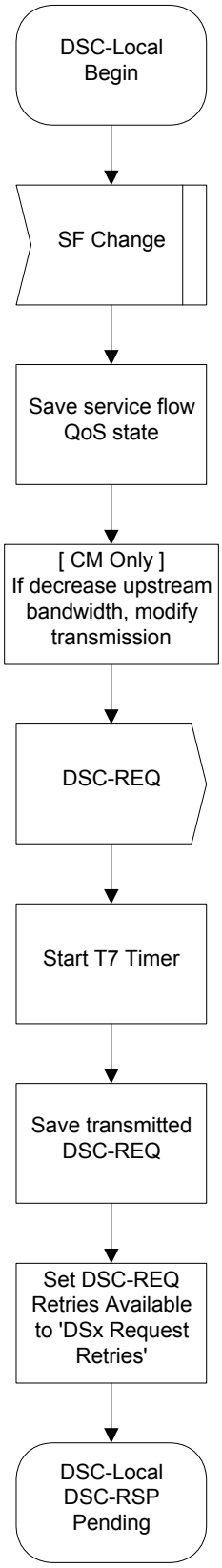


Figura B.11-41/J.112 – DSC – Diagrama de flujo de estados de comienzo de transacción iniciada localmente

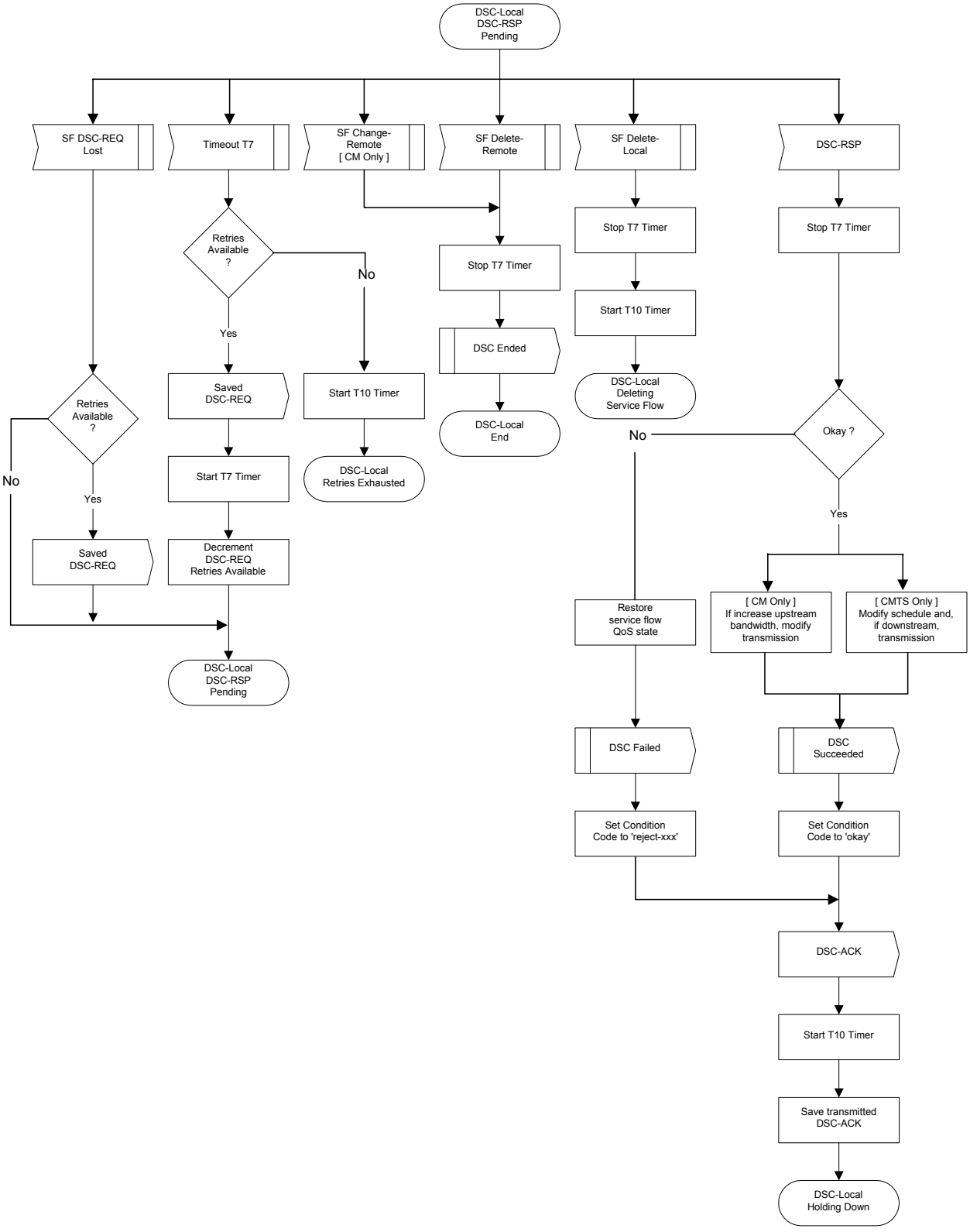


Figura B.11-42/J.112 – DSC – Diagrama de flujo de estados de transacción iniciada a distancia con DSC-RSP pendiente

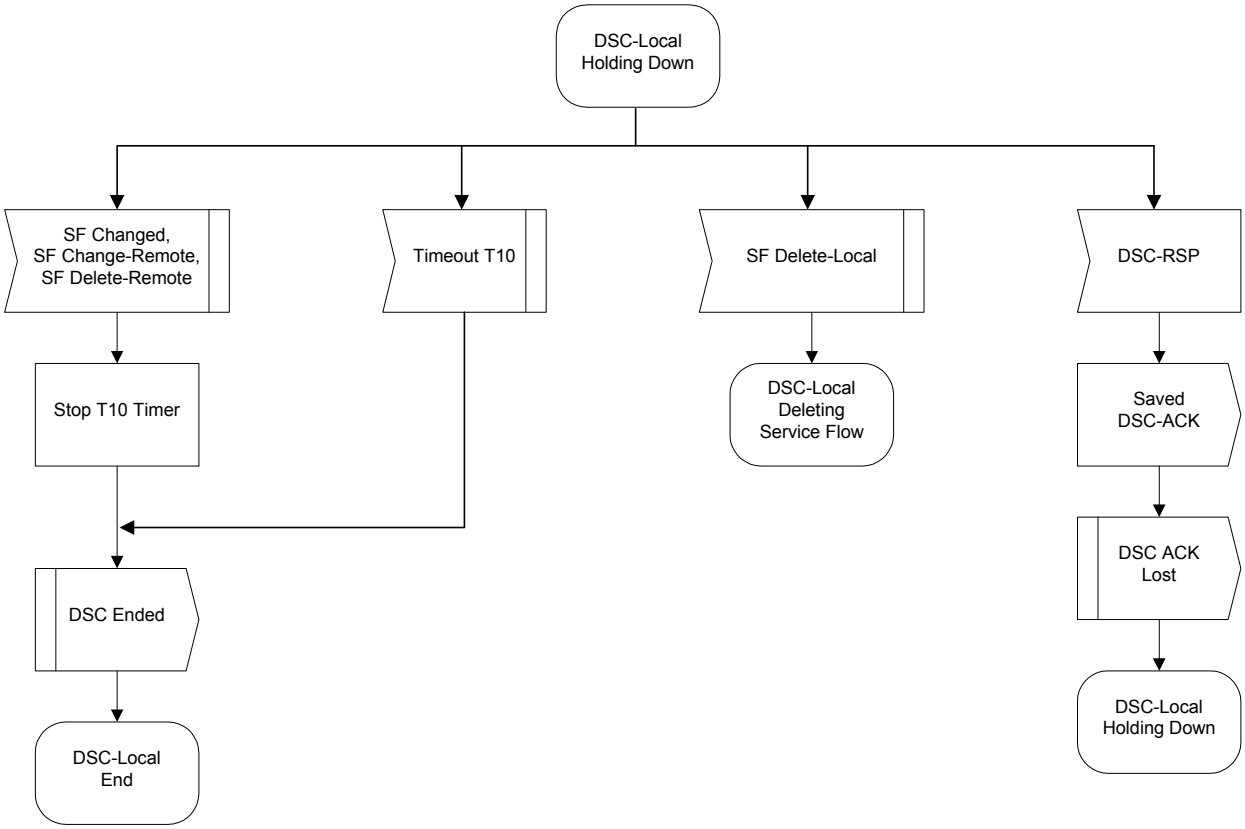


Figura B.11-43/J.112 – DSC – Diagrama de flujo de estados de transacción iniciada localmente con retención

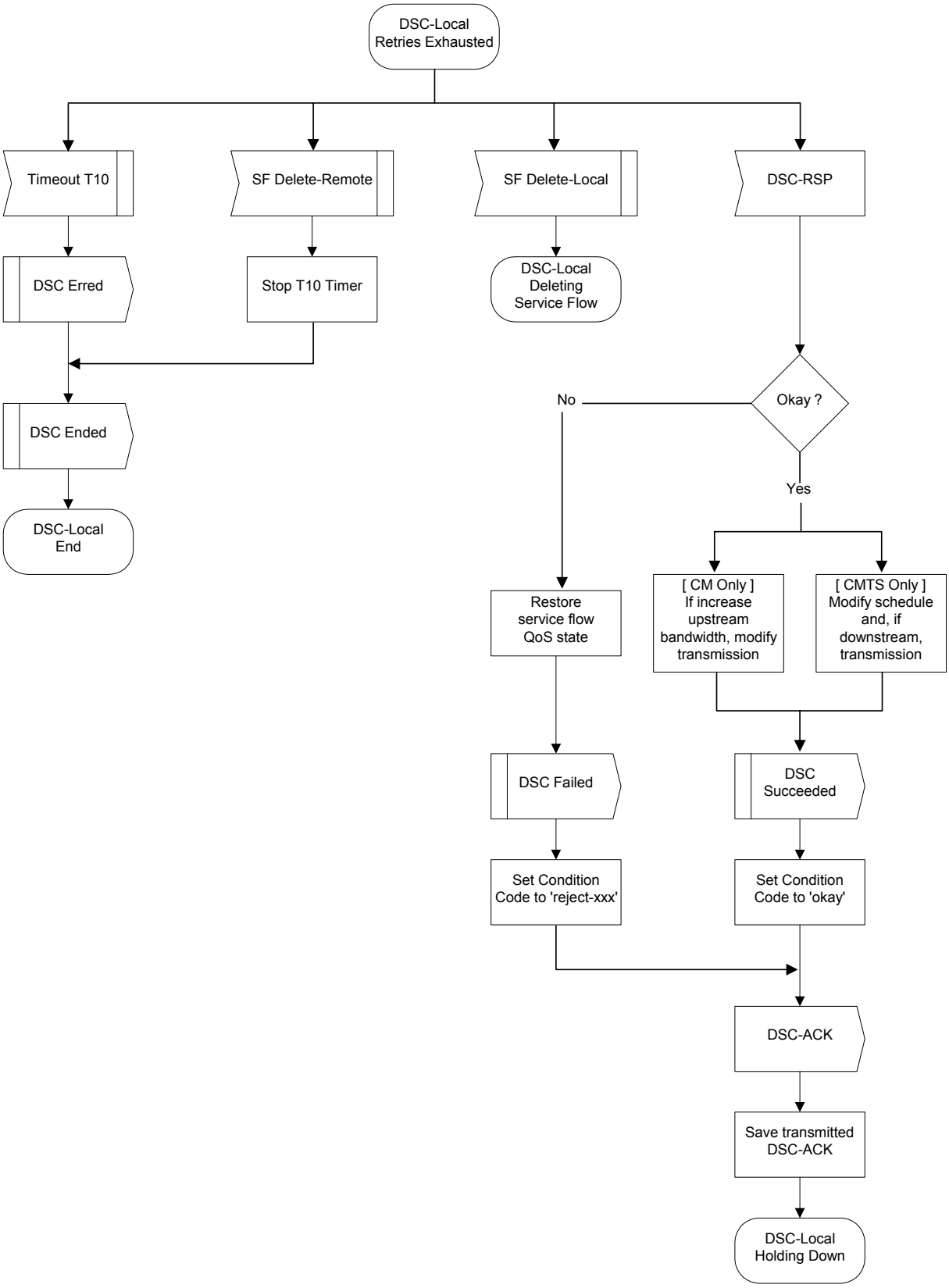


Figura B.11-44/J.112 – DSC – Diagrama de flujo de estados de transacción iniciada localmente con reintentos agotados

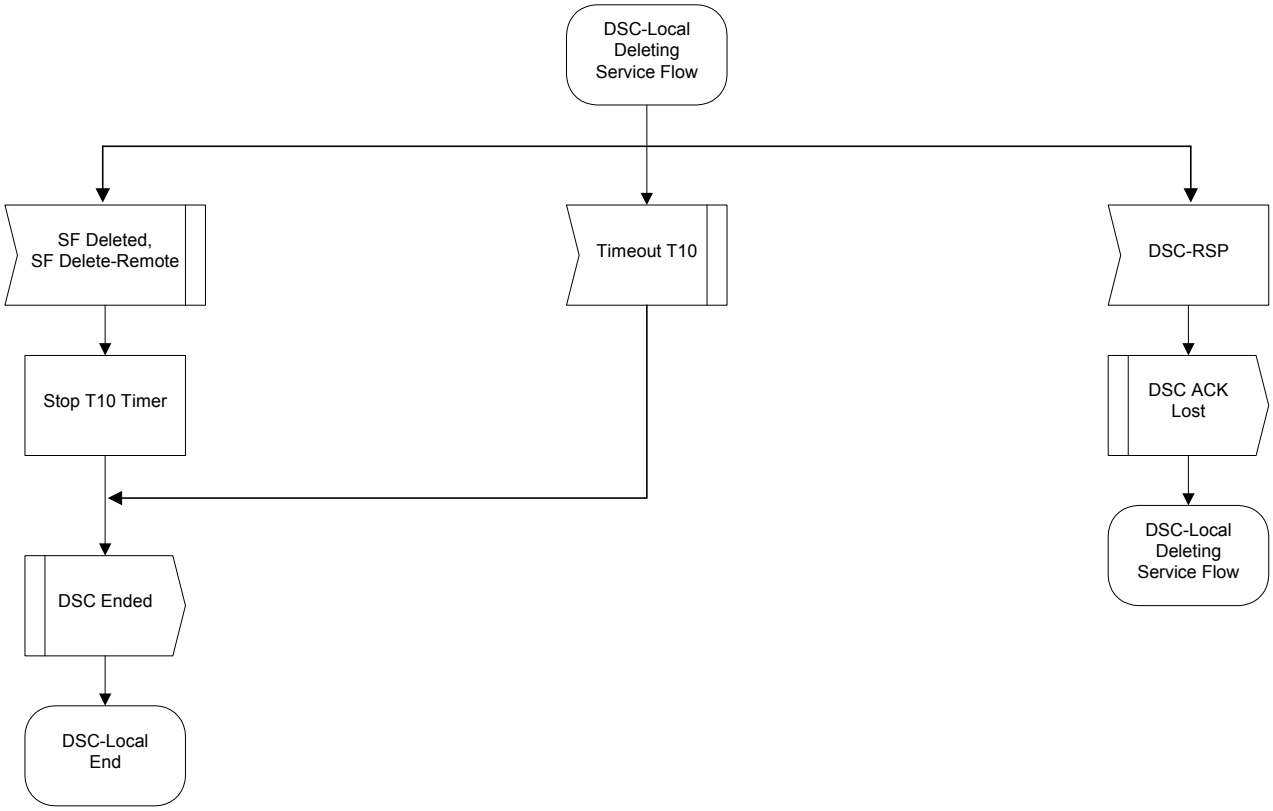


Figura B.11-45/J.112 – DSC – Diagrama de flujo de estados de servicio de transacción iniciada localmente con eliminación de flujo

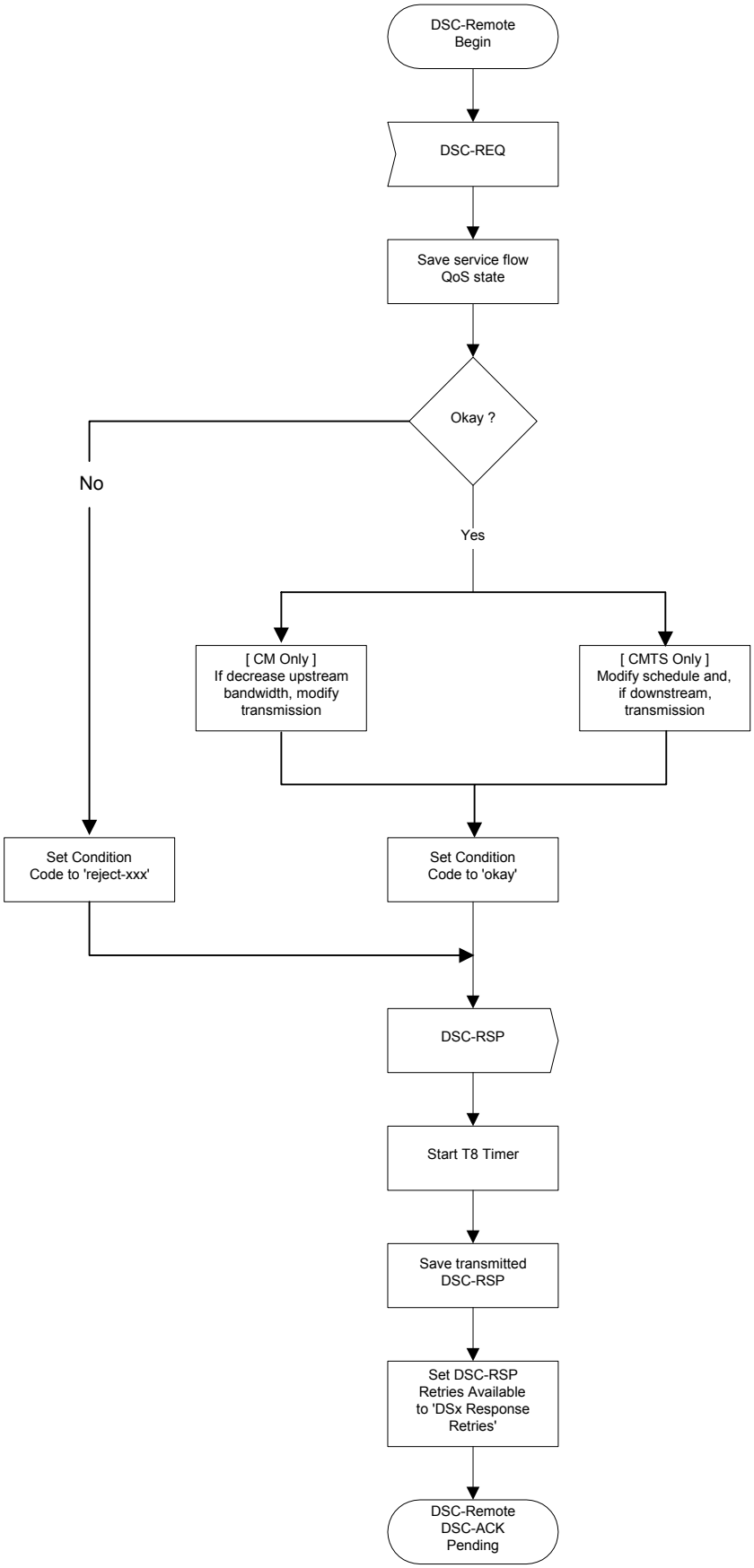


Figura B.11-46/J.112 – DSC – Diagrama de flujo de estados de comienzo de transacción iniciada a distancia

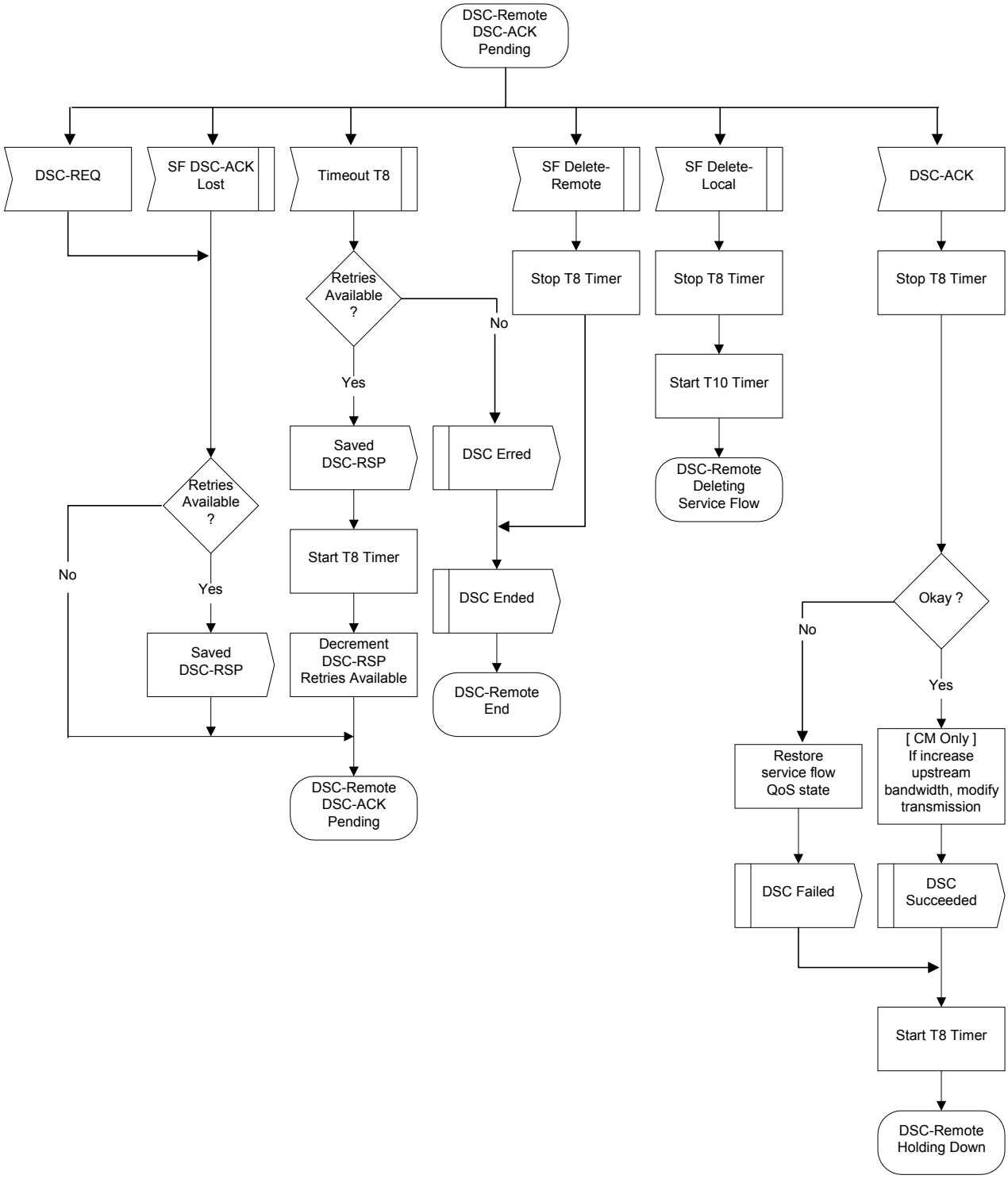


Figura B.11-47/J.112 – DSC – Diagrama de flujo de estado de transacción iniciada a distancia con DSC-ACK pendiente

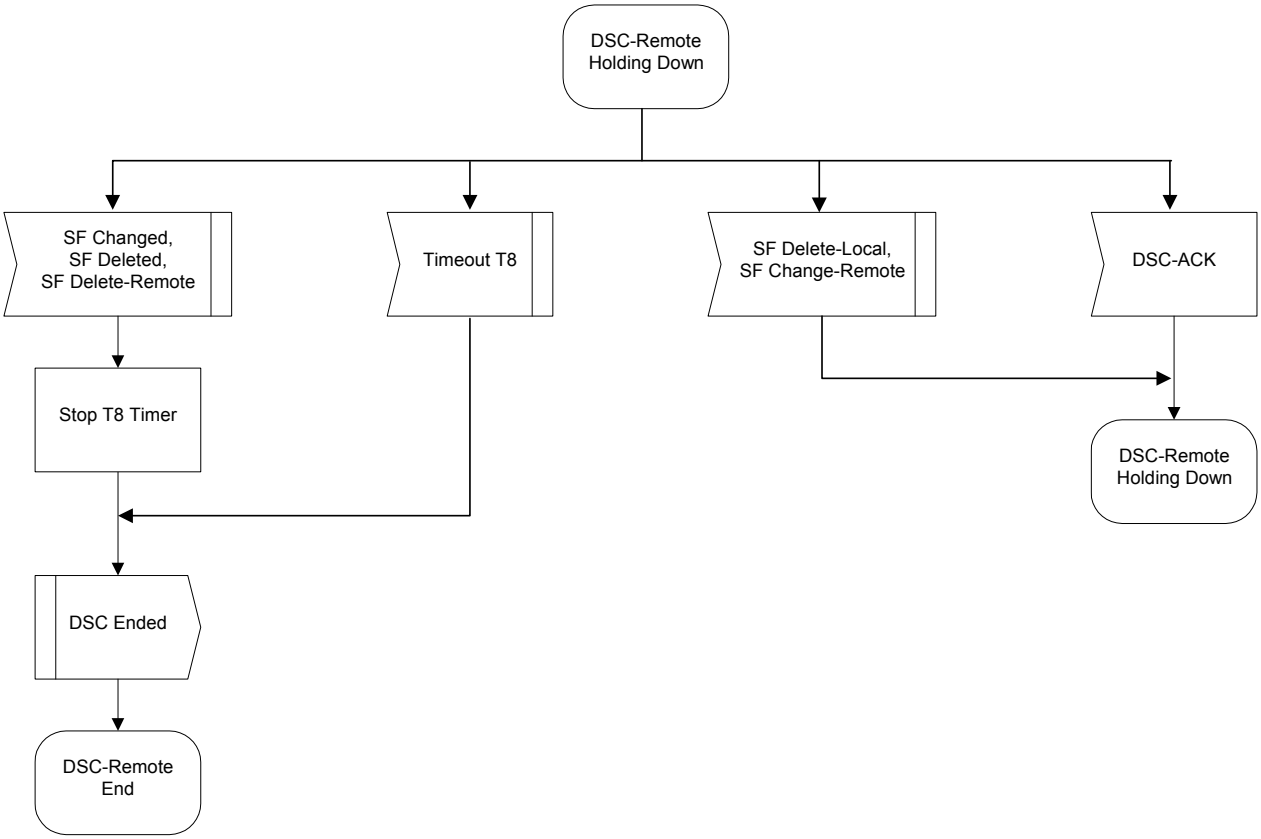


Figura B.11-48/J.112 – DSC – Diagrama de flujo de estados de transacción iniciada a distancia con retención

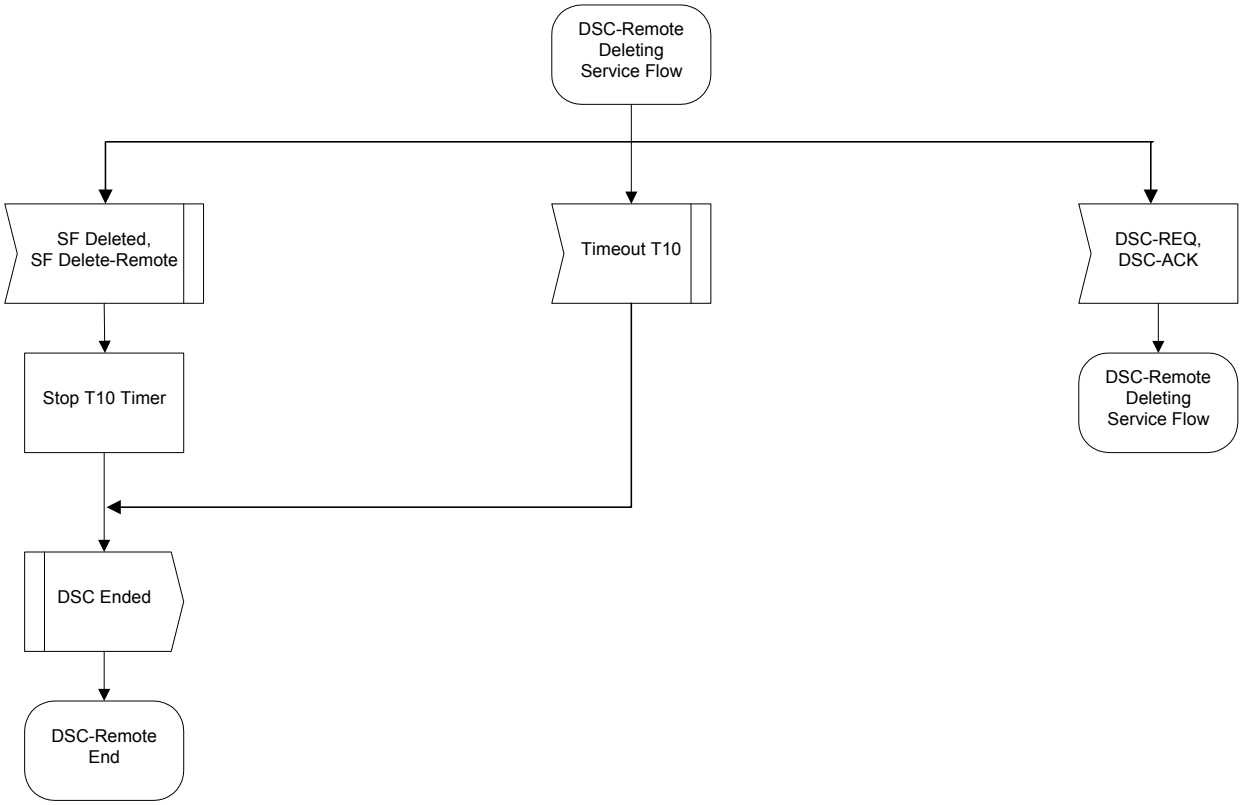


Figura B.11-49/J.112 – DSC – Diagrama de flujo de estados de transacción iniciada a distancia con eliminación de flujo de servicio

B.11.4.4 Eliminación de servicio dinámica

Cualquier flujo de servicio puede ser eliminado utilizando los mensajes de eliminación de servicio dinámica (DSD) Cuando se elimina un flujo de servicio se liberan todos los recursos asociados al mismo, incluidos los clasificadores y PHS. Sin embargo, si se elimina el flujo de servicio primario de un CM, dicho CM queda eliminado del registro y DEBE volver a registrarse. Asimismo, si se elimina un flujo de servicio que fue aprovisionado durante el registro, se pierde la información de aprovisionamiento de ese flujo de servicio hasta que el CM se registre nuevamente. Sin embargo, la eliminación de un flujo de servicio aprovisionado NO DEBE provocar un nuevo registro del CM. Ha de tenerse cuidado por tanto antes de eliminar esos flujos de servicio.

NOTA – A diferencia de los mensajes DSA y DSC, los mensajes DSD están limitados a un único flujo de servicio.

B.11.4.4.1 Eliminación de servicio dinámica iniciada por el CM

Un CM que desee eliminar un flujo de servicio genera una petición de eliminación hacia el CMTS utilizando un mensaje de petición de eliminación de servicio dinámica (DSD-REQ, *dynamic service deletion-request*). El CMTS suprime el flujo de servicio y genera una respuesta utilizando un mensaje de respuesta de eliminación de servicio dinámica (DSD-RSP, *dynamic service deletion-response*). Sólo se puede eliminar un flujo de servicio por cada petición de DSD. Véase la figura B.11-50.

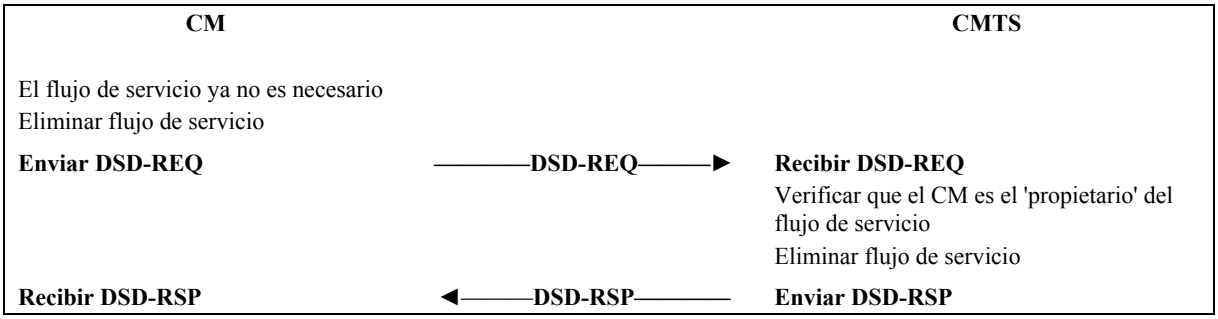


Figura B.11–50/J.112 – Eliminación de servicio dinámica iniciada por el CM

B.11.4.4.2 Eliminación de servicio dinámica iniciada por el CMTS

Un CMTS que desee eliminar un flujo de servicio dinámico genera una petición de eliminación hacia el CM asociado utilizando un mensaje de petición de eliminación de servicio dinámica (DSD-REQ). El CM suprime el flujo de servicio y genera una respuesta utilizando un mensaje de respuesta de eliminación de servicio dinámica (DSD-RSP). Sólo se puede eliminar un flujo de servicio por cada petición de DSD. Véase la figura B.11-51.

Figura B.11-51/J.112 – Eliminación de servicio dinámica iniciada por el CMTS

B.11.4.4.3 Diagramas de transiciones de estados de eliminación de servicio dinámica

Véanse las figuras B.11-52 a B.11-56.

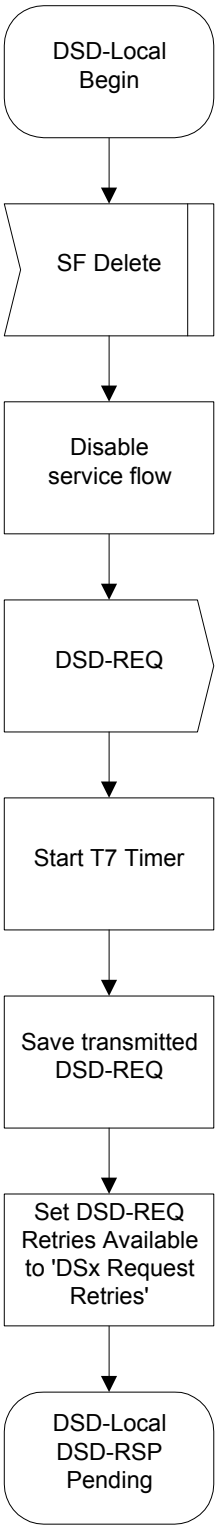


Figura B.11-52/J.112 – DSD – Diagrama de flujo de estados de comienzo de transacción iniciada localmente

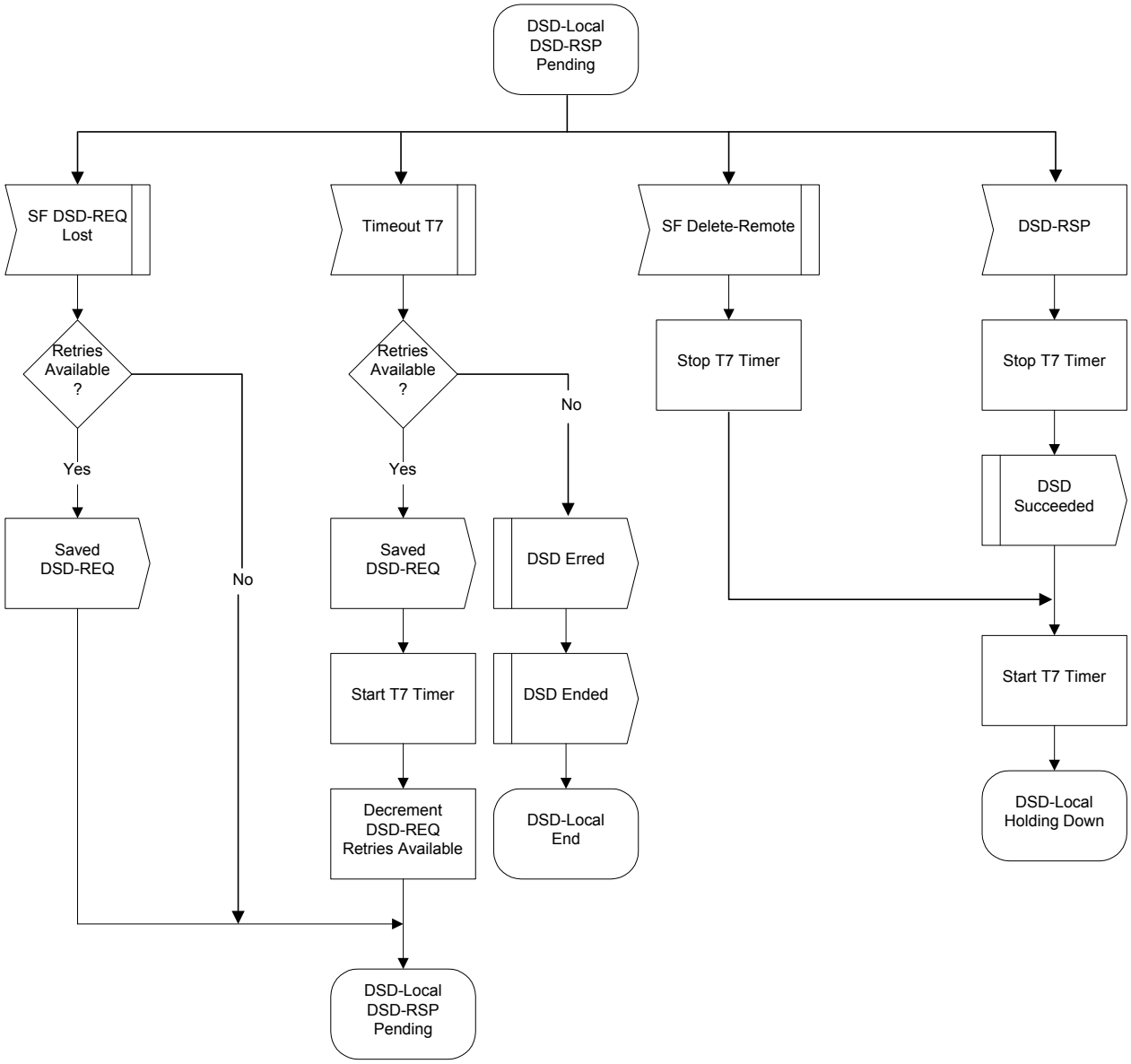


Figura B.11-53/J.112 – DSD – Diagrama de flujo de estado de transacción iniciada a distancia con DSD-RSP pendiente

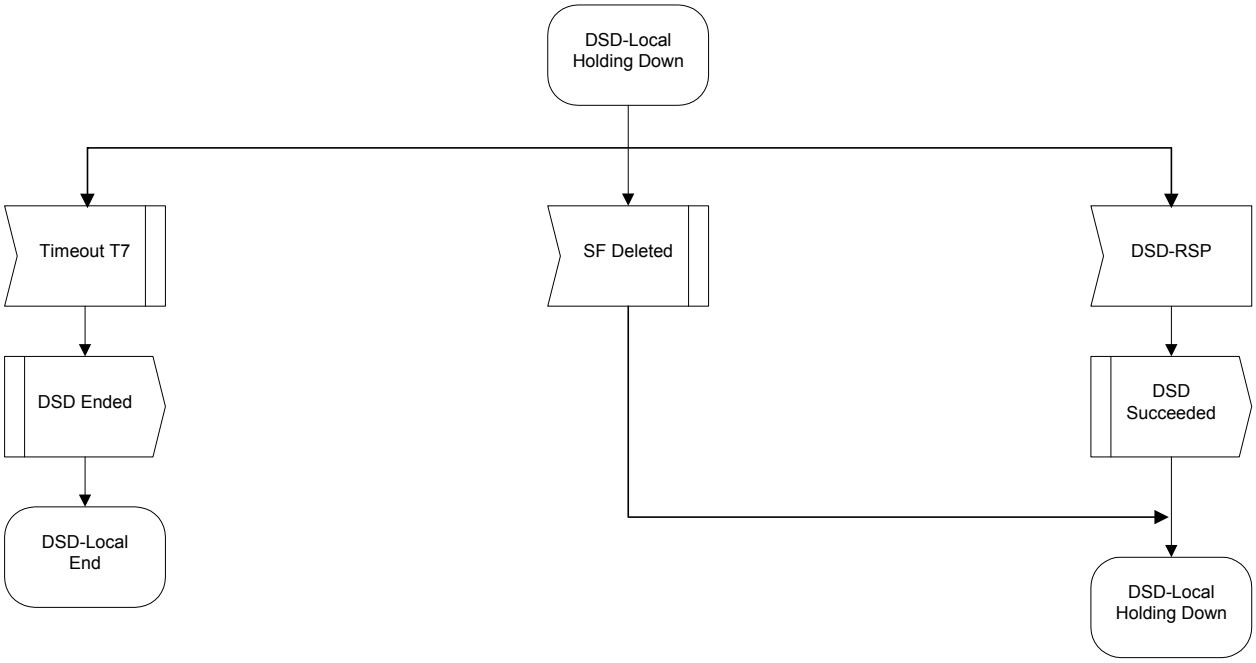


Figura 11-54/J.112 – DSD – Diagrama de flujo de estados de transacción iniciada localmente con retención

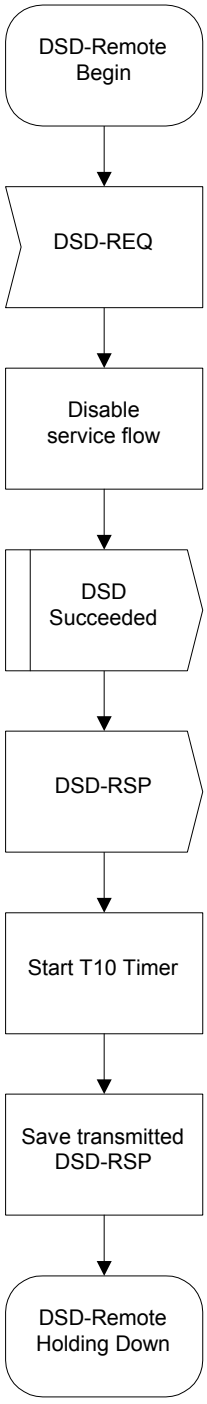


Figura 11-55/J.112 – DSD – Diagrama de flujo de estados de comienzo de transacción iniciada a distancia

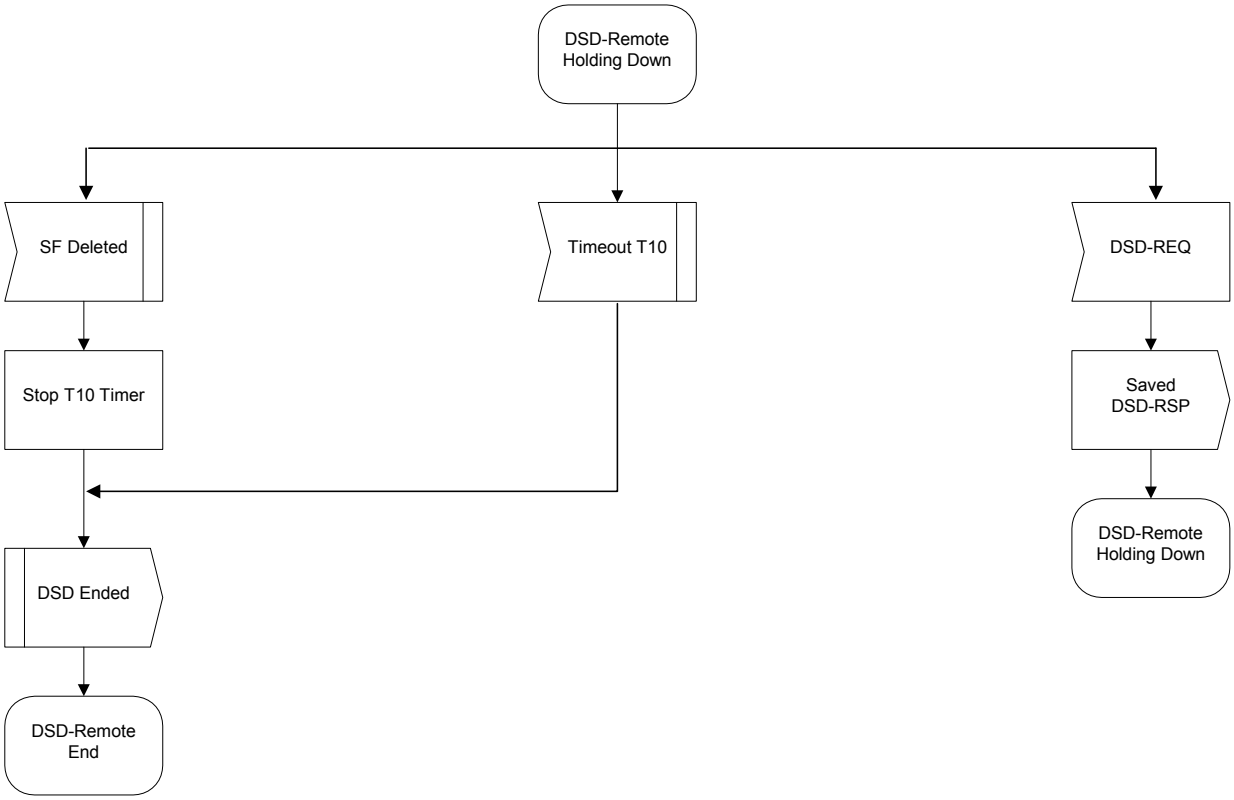


Figura 11-56/J.112 – DSD – Diagrama de flujo de estados de transacción iniciada a distancia con retención

B.11.4.5 Cambio dinámico de canales descendentes y/o ascendentes

B.11.4.5.1 Funcionamiento general del DCC

En cualquier momento después del registro, el CMTS PUEDE ordenar al CM que cambie su canal descendente y/o ascendente. Esto se puede hacer para equilibrar el tráfico, evitar el ruido, o por otros motivos que quedan fuera del alcance del presente anexo B. La figura B.11-58 muestra el procedimiento que DEBE seguir el CMTS. La figura B.11-60 muestra el procedimiento correspondiente que DEBE seguir un CM que soporte DCC.

La instrucción DCC se puede utilizar para cambiar sólo la frecuencia del canal ascendente, sólo la frecuencia del canal descendente, o tanto una como otra. Cuando sólo se cambia la frecuencia del canal ascendente o la del canal descendente, el cambio se realiza normalmente dentro de un dominio MAC. Cuando se modifican tanto la frecuencia del canal ascendente como la del canal descendente, el cambio puede ser dentro de un dominio MAC o entre dominios MAC.

El ID del canal descendente y el ID del canal ascendente DEBEN ambos ser únicos entre el canal antiguo y el nuevo. En este contexto, canal antiguo se refiere al canal o los canales en que estaba el CM antes del salto, y canal nuevo se refiere al canal o los canales en que está el CM luego del salto.

Al sincronizar con el nuevo canal ascendente y/o descendente, el CM DEBE utilizar la técnica especificada en la tupla TLV de técnica de inicialización del mensaje DCC-REQ, si es que está presente, para determinar si debe realizar una reinicialización, sólo una alineación, o ninguna de las dos cosas. Si esta tupla TLV no está presente en el mensaje de DCC-REQ, el CM DEBE reinicializar su MAC en la nueva asignación de canal, (véase B.11.2). Si se ha ordenado al CM que reinicialice, el CMTS NO DEBE esperar que en el nuevo canal se produzca un DCC-RSP.

Si el CM se está moviendo dentro de un dominio MAC, quizás no sea necesaria una reinicialización. Si el CM se está moviendo entre dominios MAC, quizás sea necesaria una reinicialización. La reinicialización, si se pide, se lleva a cabo con las nuevas asignaciones ascendentes y de canal. Incluye la obtención de los parámetros en sentido ascendente, el establecimiento de la conectividad IP, el establecimiento de la hora del día, la transferencia de los parámetros operativos, el registro, y la inicialización de la privacidad básica. Si se lleva a cabo la reinicialización, el CM NO DEBE enviar un DCC-RSP por el nuevo canal.

La decisión de volver a alinear se basa en el conocimiento que tiene el CMTS de cualquier diversidad de trayectos que pueda existir entre el canal antiguo y el nuevo, o de si ha cambiado alguno de los parámetros fundamentales del canal ascendente o el descendente, tales como velocidad de símbolos, tipo de modulación o tamaño de miniintervalo.

Cuando el mensaje DCC-REQ no conlleva una reinicialización o realineación, el objetivo de diseño del CM será habitualmente minimizar las perturbaciones del tráfico que ve el usuario final. Para lograr este objetivo, un CM PUEDE optar por seguir utilizando recursos de QoS (tales como concesiones de anchura de banda) en su canal actual tras recibir un DCC-REQ y antes de ejecutar de hecho el cambio de canal. El CM podría necesitar también este tiempo para vaciar colas de espera internas o para reposicionar máquinas de estados finitos antes de cambiar de canal.

El CM PUEDE continuar utilizando los recursos QoS del canal antiguo, incluida la transmisión y recepción de paquetes, luego de enviar un mensaje DCC-RSP (salida) y antes de realizar el cambio. El CM PUEDE utilizar los recursos QoS del canal nuevo, incluida la transmisión y recepción de paquetes, luego del cambio y antes de enviar un mensaje DCC-RSP (llegada). El CMTS NO DEBE usar el mensaje DCC-RSP (salida) para eliminar recursos QoS en el canal antiguo. El CMTS NO DEBE esperar un mensaje DCC-RSP (llegada) por el canal nuevo antes de permitir que se utilicen recursos QoS. Esta provisión sirve para hacer posible la afiliación del servicio de concesión no solicitada en el canal antiguo y en el nuevo con un mínimo de perturbaciones cuando se cambia de canal.

El CMTS DEBE retener los recursos QoS en el canal actual hasta que haya pasado un tiempo T13 después de haberse enviado el último DCC-REQ, o hasta que pueda confirmar internamente la presencia del CM en la nueva atribución de canal. El CM DEBE ejecutar la salida del canal antiguo y la llegada al nuevo canal, menos cualquier reinicialización que se haya ordenado, antes que expire T13. El CM PUEDE seguir utilizando recursos QoS en el canal actual luego de responder con DCC RSP y antes que expire T13.

Una vez que el CM cambia de canal, todas las peticiones de anchura de banda pendientes previas efectuadas por medio del IE petición o el IE petición/datos quedan invalidadas y el CM DEBE volver a pedir anchura de banda en el nuevo canal. En caso de un servicio de concesión no solicitada en el canal ascendente, las concesiones están implícitas con las reservas de QoS y no es necesario que sean solicitadas nuevamente.

B.11.4.5.2 Condiciones de excepción de DCC

Si un CM emite un mensaje de DSA-REQ o DSC-REQ pidiendo más recursos, y el CMTS necesita realizar un DCC para obtener dichos recursos, el CMTS rechazará la instrucción DSA o DSC sin atribuir recurso alguno al CM. El CMTS incluye un código de confirmación de "reject-temporary-DCC" (rechazo de DCC temporal, véase B.C.1.3.1) en el mensaje DSC-RSP para indicar que los nuevos recursos no estarán disponibles hasta que se reciba un DCC. El CMTS dará continuidad entonces a la transacción DSA o la DSC con una transacción DCC.

Después de cambiar a un nuevo canal y completar la transacción DCC, el CM reintenta la instrucción DSA o DSC. Si el CM no ha cambiado de canal luego de expirar T14, medido el tiempo desde el instante en que el CM recibió DSA-RSP o DSC-RSP del CMTS, el CM PUEDE reintentar la petición de recurso.

Si el CMTS necesita cambiar de canal para satisfacer una petición de recurso distinta de una instrucción de DSA o DSC iniciada por el CM, debería ejecutar primero la instrucción DCC y emitir luego una instrucción DSA o DSC.

Si un CMTS realiza un DCC sin reinicializar, el fichero de la configuración podría hacer que el CM volviera al canal original, lo que provocaría un bucle infinito. Para evitar esto, si la opción de provisionamiento por defecto del sistema es especificar el ID del canal ascendente y/o la frecuencia descendente, el CMTS NO DEBERÍA usar DCC-REQ sin la opción de reinicialización.

El CMTS NO DEBE emitir una instrucción DCC si el CMTS ha emitido previamente una instrucción DSA o DSC, y dicha instrucción está todavía pendiente. El CMTS NO DEBE emitir una instrucción DCC si el CMTS está todavía esperando un DSA-ACK o DSC-ACK de una instrucción DSA-REQ o DSC-REQ anterior iniciada por el CM.

El CMTS NO DEBE emitir una instrucción DSA o DSC si el CMTS ha emitido previamente una instrucción DCC, y dicha instrucción está todavía pendiente.

Si el CMTS emite una instrucción DCC-REQ y el CM emite simultáneamente una instrucción DSA-REQ o DSC-REQ, la instrucción del CMTS tiene prioridad. El CMTS responde con un código de confirmación de "reject-temporary" ("rechazo temporal, véase B.C.1.3.1). El CM continúa con la ejecución de la instrucción DCC.

Si el CM no logra establecer comunicaciones con un CMTS por el nuevo canal o los canales nuevos, DEBE volver al canal o los canales previos y reinicializar su MAC. La atribución previa de canales representa un buen punto de trabajo conocido, lo cual debería acelerar el proceso de reinicialización. Además, volver al canal previo proporciona un entorno operativo más robusto al CMTS para hallar un CM que no logra conectarse al canal o los canales nuevos.

Si el CMTS envía un mensaje DCC-REQ y no recibe un DCC-RSP dentro del plazo T11, DEBE retransmitir el DCC-REQ hasta un máximo de "Reintentos de DCC-REQ" (véase el anexo B.B) antes de declarar que la transacción ha fallado. Se señala que si el DCC-RSP se hubiera perdido en tránsito y el CMTS intentara de nuevo el mensaje DCC-REQ, el CM podría haber cambiado ya los canales descendentes.

Si el CM envía un mensaje DCC-RSP por el nuevo canal y no recibe un DCC-ACK del CMTS dentro del plazo T12, DEBE reintentar el DCC-RSP hasta un máximo de "Reintentos de DCC-ACK" (véase el anexo B.B).

Si el CM recibe una DCC-REQ con TLV ID de canal ascendente, si está presente, igual al ID de canal ascendente actual, y TLV frecuencia descendente, si está presente, es igual a la frecuencia descendente actual, entonces el CM DEBE considerar al mensaje DCC-REQ como una instrucción redundante. Los demás parámetros TLV de DCC-REQ NO DEBEN ser ejecutados, y el CM DEBE devolver un DCC-RSP, con un código de confirmación de "reject-already-there" ("rechazo ya está allí") al CMTS (véase B.C.4.1).

B.11.4.5.3 Cambio de canal casi imperceptible

Cuando el CMTS desea añadir nuevas reservas de QoS a un CM, quizás sea necesario desplazar ese CM a un nuevo canal ascendente y/o descendente para lograr dicho objetivos. Durante el cambio de canal conviene que se el número de interrupciones de los servicios de QoS existentes, tales como las sesiones de voz por IP o las transmisiones de vídeo continuas, sea mínimo. Este cambio de canal, casi imperceptible, es el objetivo de diseño primario de la instrucción DCC. El CMTS PUEDE sustentar un cambio de canal casi sin perturbaciones. El CM PUEDE soportar un cambio de canal casi sin perturbaciones.

Las acciones que se describen a continuación son procedimientos operativos recomendados, a utilizar para lograr un cambio de canal casi imperceptible. En la lista de acciones se supone que tanto el canal ascendente como el descendente están cambiando. Sería aplicable un subconjunto de la lista si cambiara sólo el canal descendente o el ascendente.

Para que sea posible un cambio de canal casi sin perturbaciones, se deben cumplir en la red las condiciones siguientes:

- Los parámetros de capa física de los nuevos canales ascendentes y descendentes no deberán cambiar al cambiar los canales ascendentes y descendentes antiguos. Se señala que un cambio en los parámetros en sentido descendente podría invalidar los parámetros de alineación.
- Los parámetros de alineación no deberán cambiar de los canales antiguos a los nuevos. Esto quizás requiera un cableado simétrico y unas condiciones de planta ajenas al CMTS.
- El CMTS deberá utilizar el mismo indicador de tiempo y mecanismo de SYNC para todos los canales descendentes.
- El encaminamiento de IP se deberá configurar de tal modo que el CM y sus CPE conectadas puedan seguir utilizando sus direcciones IP existentes. Así se evitará perturbar las sesiones de RTP u otras aplicaciones en curso.

Para lograr un cambio de canal casi sin perturbaciones, el CMTS:

- DEBERÍA duplicar todas las reservas de QoS pertinentes para el CM en las atribuciones de canal antiguas y nuevas antes de iniciar una instrucción DCC-REQ.
- DEBERÍA duplicar el flujo de paquetes en sentido descendente para el CM, en las atribuciones de canal antiguas y nuevas, antes de iniciar una instrucción DCC-REQ (para cambios de canal descendente).
- DEBERÍA transmitir mensajes MAP para el nuevo canal ascendente por el canal descendente antiguo durante al menos la duración de T13, si los canales descendentes antiguos y nuevos comparten la misma indicación de tiempo. (Se señala que si el CM no puede guardar los MAP para el nuevo canal ascendente mientras está en el canal descendente antiguo, el retardo de cambio de canal se verá incrementado en el lapso de tiempo que requiera la generación ulterior de los MAP. El CMTS DEBERÍA abstenerse por lo tanto de planificar MAP futuros más allá de lo que necesita.)
- DEBERÍA especificar los parámetros en sentido descendente y ascendente de los nuevos canales antes del cambio del CM.
- DEBERÍA especificar la no espera de un mensaje SYNC por el canal nuevo.
- DEBERÍA especificar la omisión de la inicialización (definida en B.11.2).
- DEBERÍA especificar la omisión del mantenimiento inicial y el mantenimiento de la estación.
- DEBERÍA gestionar las sustituciones de flujo de servicio entre antiguos y nuevos SID, SAID, ID de flujo de servicio, ID de clasificador, índices de supresión de encabezamiento de cabida útil, y referencias de tiempo de concesión no solicitada según se requiera. Los nombres de clase de servicio DEBERÍAN seguir siendo los mismos entre el o los canales antiguos y el o los nuevos.

Para lograr un cambio de canal casi sin perturbaciones, el CM:

- DEBERÍA replicar con estimaciones del tiempo de cambio del CM en el mensaje DCC-RSP.
- DEBERÍA estar a la escucha de, y guardar, los mensajes MAP por el antiguo canal descendente aplicables al nuevo canal ascendente. Esto DEBERÍA hacerse durante el plazo de tiempo de T13.

- DEBERÍA utilizar los parámetros en sentido descendente y el UCD en su memoria de la instrucción DCC para obligar a una convergencia PHY más rápida al realizar el cambio de canal.
- NO DEBERÍA esperar un mensaje SYNC luego de la convergencia PHY y antes de transmitir, si es que el CMTS le permite al CM hacerlo.
- DEBERÍA utilizar los MAP guardados en memoria, si están disponibles, para hacer posible un tiempo de arranque menor.
- DEBERÍA minimizar la perturbación del tráfico en cualquier sentido permitiendo que fluya en ambos sentidos hasta el momento previo al cambio, e inmediatamente después de producirse la resincronización con el o los canales nuevos.
- DEBERÍA poner en cola de espera los paquetes de datos entrantes que llegan durante el cambio, y transmitirlos después de que se produzca éste.
- DEBERÍA descartar luego del cambio los paquetes VoIP que hayan hecho que la cola de espera del servicio de petición no solicitada en sentido ascendente exceda de su límite; pero no más de lo necesario.

Las aplicaciones que se están ejecutando por el trayecto DOCSIS deberían soportar la pérdida de paquetes que se puede producir mientras el CM cambia de canal.

B.11.4.5.4 Ejemplo de funcionamiento

En la figura B.11-57 se muestra un ejemplo de utilización del DCC y su relación con otros mensajes MAC de DOCSIS. Este ejemplo describe, en particular, una situación en la que el CM intenta atribuir nuevos recursos con un mensaje DSA. El CMTS rechaza temporalmente la petición, le indica al CM que cambie de canal, y a continuación el CM vuelve a pedir los recursos. El ejemplo (sin incluir todas las condiciones de excepción) se describe a continuación. Véase B.11.2 por más detalles.

a) Se produce un evento, tal como la emisión por el CM de un mensaje DSA-REQ.

b) El CMTS decide que necesita cambiar de canales para atender esta petición de recursos. El CMTS responde con un mensaje DSA-RSP que incluye un código de confirmación de "reject-temporary-DCC" (rechazo temporal de DCC, véase B.C.1.3.1) en el mensaje DSC-RSP para indicar que los nuevos recursos no están disponibles hasta que se recibe un DCC. El CMTS rechaza ahora cualquier mensaje DSA o DSC ulterior hasta que se ejecuta la instrucción DCC.

c) El CMTS inicia las reservas de QoS en los nuevos canales ascendentes y/o descendentes. Las reservas de QoS incluyen la nueva asignación de recursos junto con todas las asignaciones de recursos actuales atribuidas al CM. En este ejemplo se cambian tanto el canal ascendente como el descendente.

d) Para facilitar un cambio de canal casi sin perturbaciones, y puesto que el CMTS no está seguro de exactamente cuándo ha de cambiar el CM de canal, el CMTS duplica el flujo de paquetes en sentido descendente por los canales descendentes antiguo y nuevo.

e) El CMTS envía una instrucción DCC-REQ al CM.

f) El CM envía un mensaje DCC-RSP (salida). El CM vacía entonces sus colas y máquinas de estados finitos, según corresponda, y cambia de canal.

g) Si hubo cambio de canal en sentido descendente, el CM se sincroniza con la temporización de símbolos de QAM, con la alineación de trama FEC y con la alineación MPEG.

h) Si se ha indicado al CM que efectúe una reinicialización, lo hace con la nueva asignación de canal ascendente y/o descendente. El CM sale del flujo de eventos que se describe aquí y entra en el flujo de eventos que se describe en la subcláusula B.11.2 comenzando por el reconocimiento de un mensaje SYNC en sentido descendente.

i) El CM busca un mensaje UCD, a menos que se le haya dado una copia.

j) El CM espera un mensaje SYNC en sentido descendente, a menos que se le haya indicado que no espere ninguno.

k) El CM recopila mensajes MAP, a menos que ya los tenga disponibles en su memoria de almacenamiento.

l) El CM realiza mantenimiento inicial y mantenimiento de estación, a menos que se le haya indicado que los omita.

m) El CM reanuda la transmisión de datos normal con su nueva atribución de recursos.

n) El CM envía un mensaje DCC-RSP (llegada) al CMTS.

o) El CMTS responde con un DCC-ACK.

p) El CMTS suprime las reservas de QoS de los canales antiguos. Si se duplicó el flujo de paquetes en sentido descendente, también se eliminará la duplicación de paquetes en el antiguo canal descendente.

q) El CM vuelve a emitir su instrucción DSA-REQ.

r) El CMTS reserva los recursos pedidos y responde con un mensaje DSA-RSP.

s) El CM termina con un mensaje DSA-ACK.

Véanse también las figuras B.11-58 a B.11-61.

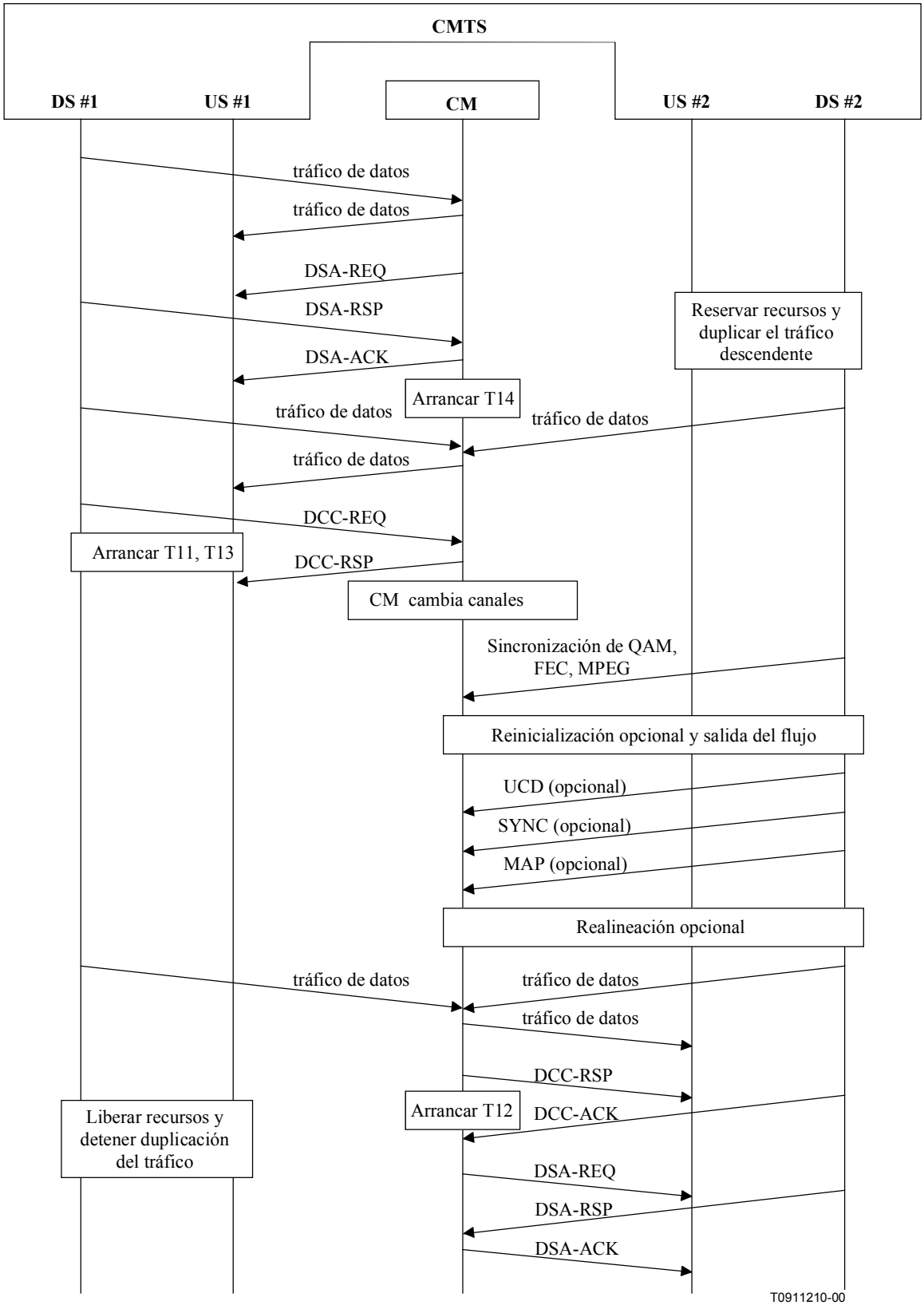


Figura B.11-57/J.112 – Ejemplo de flujo de operaciones de DCC

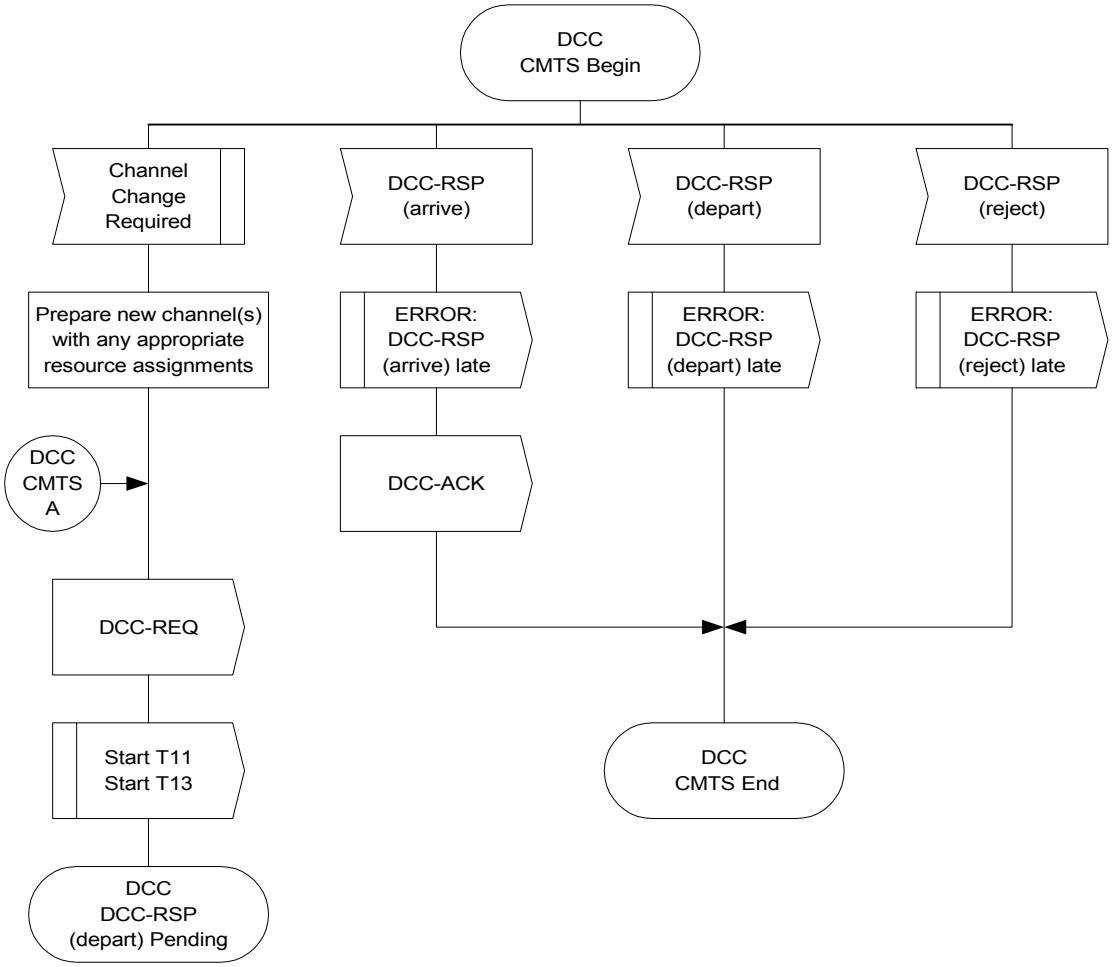


Figura B.11-58/J.112 – Cambio dinámico de canales: Visión del CMTS, 1ª parte

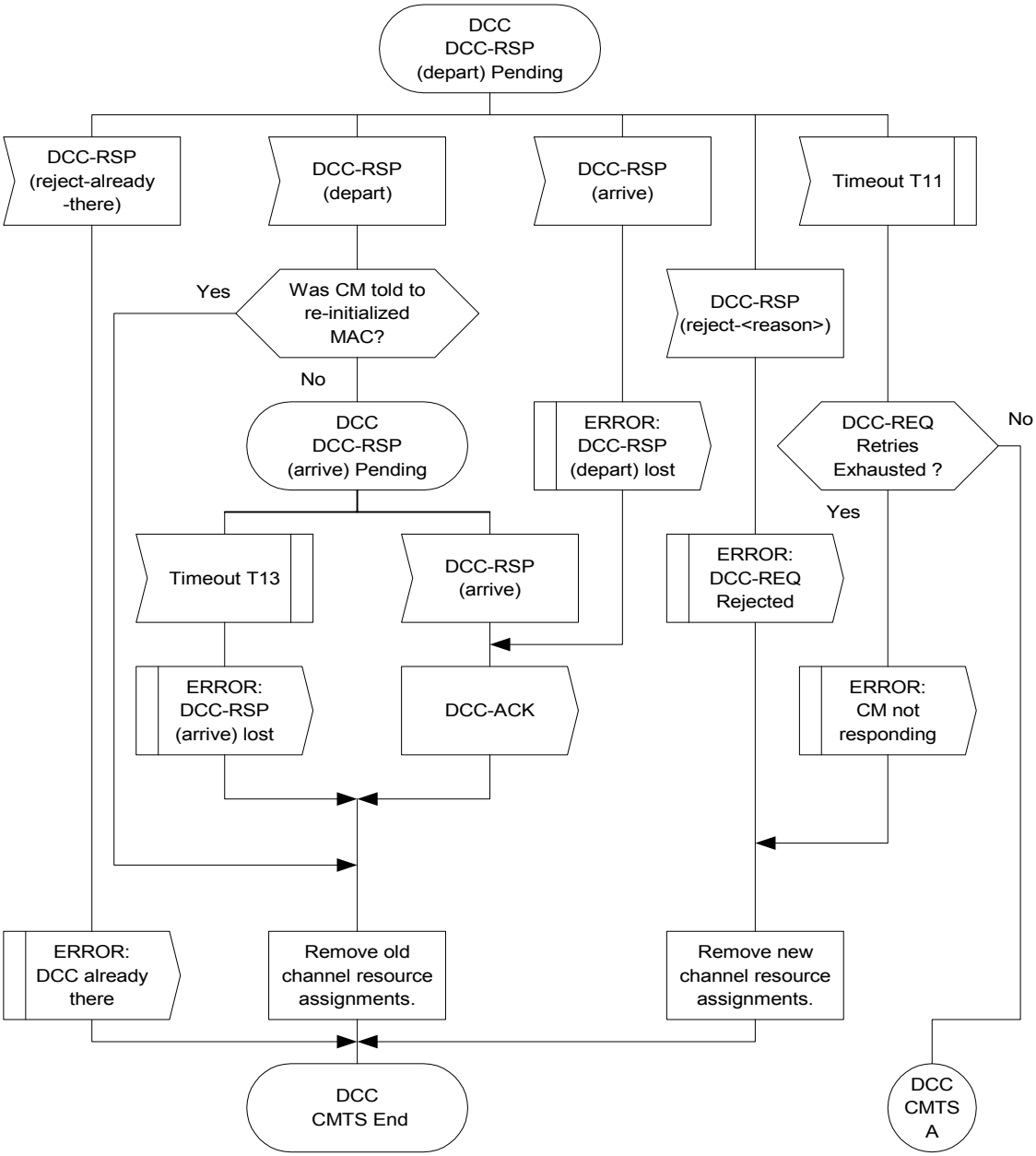
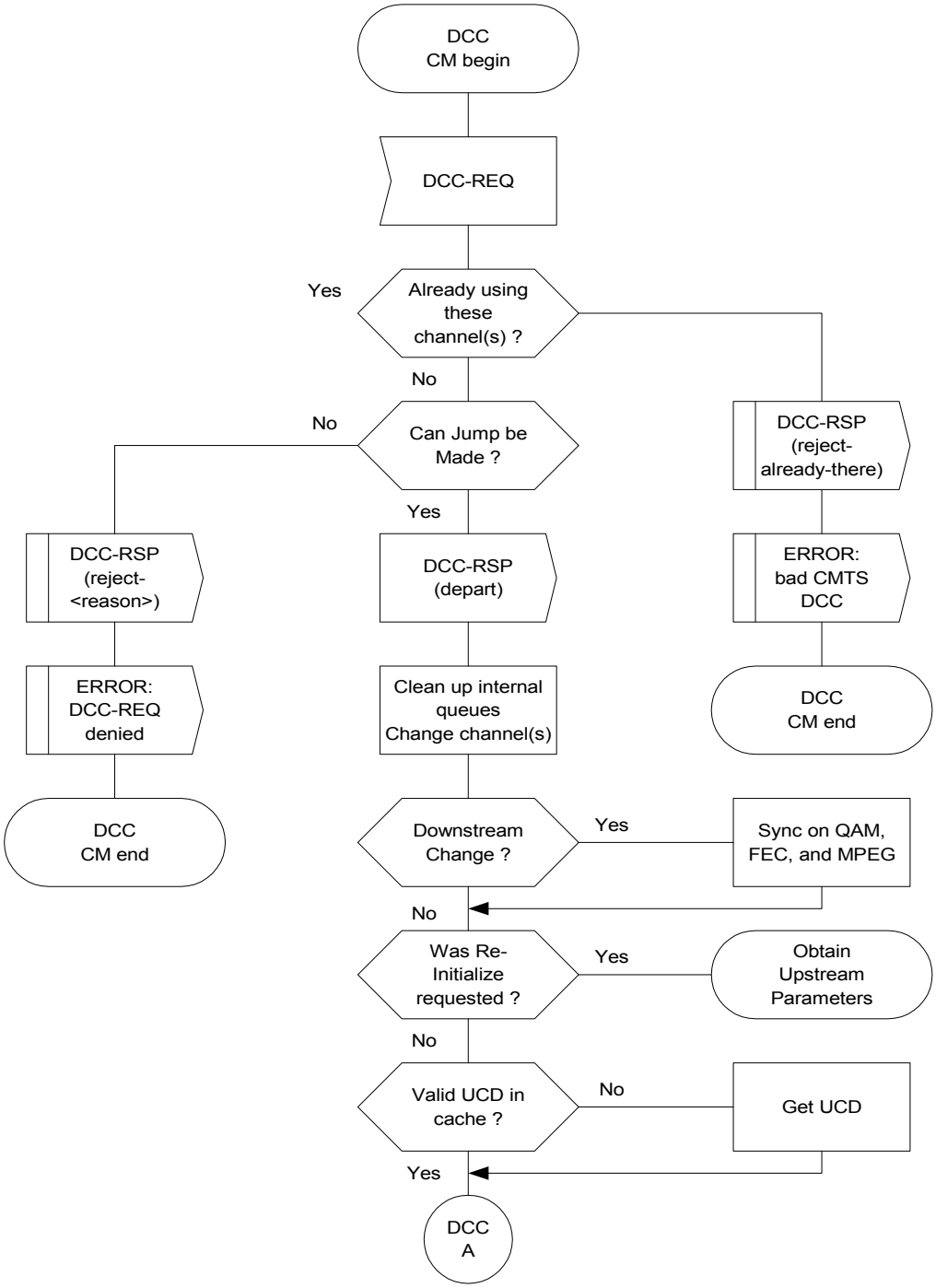


Figura B.11-59/J.112 – Cambio dinámico de canales: Visión del CMTS, 2ª parte



NOTA – El estado "obtener parámetros en sentido ascendente" se enlaza a la máquina de estados de la figura B.11-1.

Figura B.11-60/J.112 – Cambio dinámico de canales: Visión del CM, 1ª parte

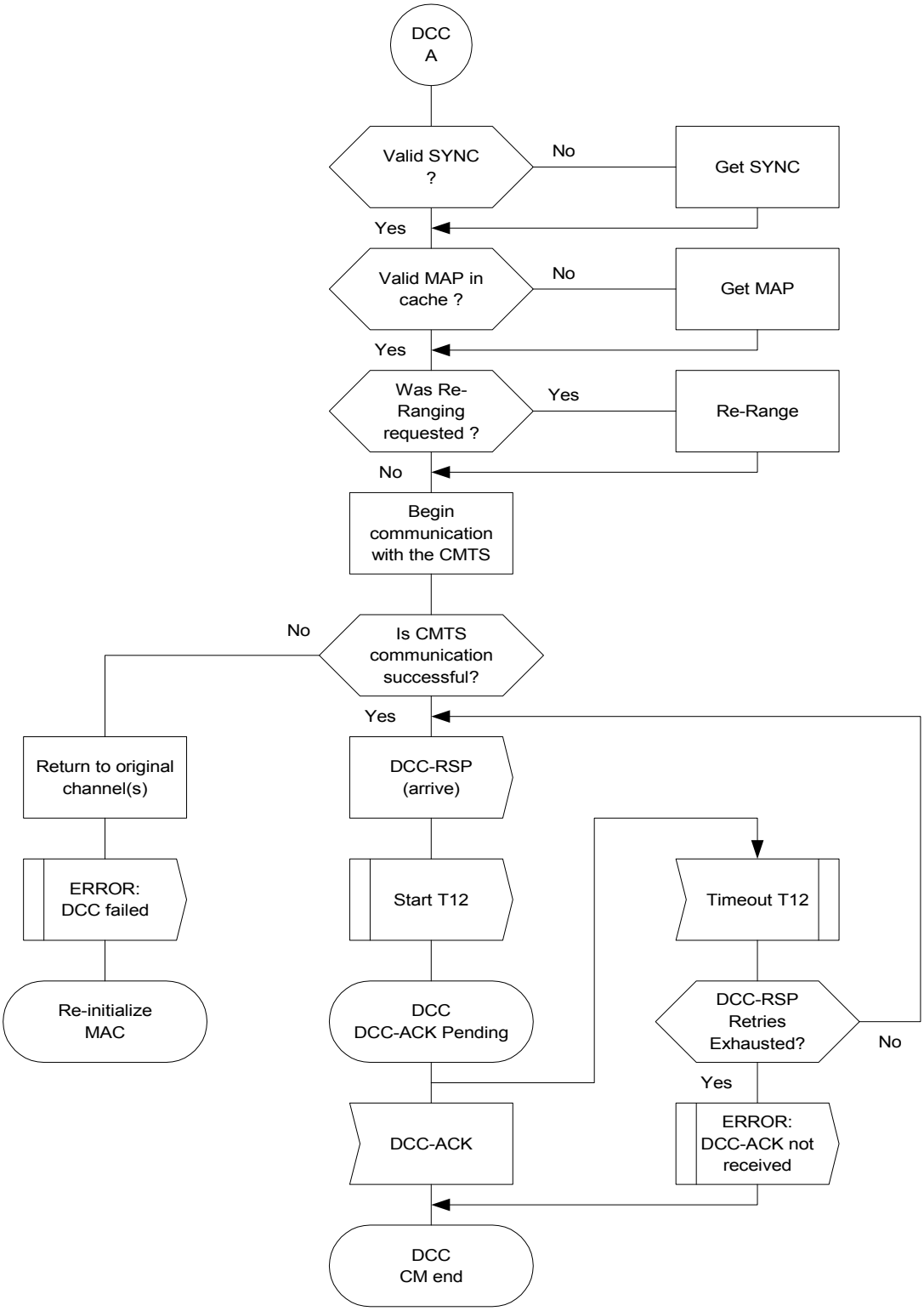


Figura B.11-61/J.112 – Cambio dinámico de canales: Visión del CM, 2ª parte

B.11.5 Detección de averías y recuperación

La detección de averías y la recuperación tienen lugar a múltiples niveles.

- A nivel de la capa física, se utiliza FEC para corregir errores donde sea posible. Véase, para más detalles, B.6.

- El protocolo MAC protege contra errores utilizando campos de sumas de comprobación tanto en el encabezamiento MAC como en los tramos de datos del paquete. Véase, para más detalles, B.8.
- Todos los mensajes de gestión MAC están protegidos con una CRC que abarca la totalidad del mensaje, como se define en B.8. Cualquier mensaje cuya CRC dé un resultado negativo DEBE ser descartada por el receptor.

El cuadro B.11-1 muestra el proceso de recuperación que DEBE aplicarse tras la pérdida de un tipo específico de mensaje MAC.

Cuadro B.11-1/J.112 – Proceso de recuperación ante pérdida de mensajes MAC específicos

Nombre del mensaje	Acción tras la pérdida del mensaje
SYNC	El CM puede perder mensajes SYNC durante una parte del intervalo SYNC de pérdida (*Lost SYNC* – véase el anexo B.B) antes de perder la sincronización con la red. Un CM que ha perdido la sincronización NO DEBE usar el canal ascendente y DEBE intentar restablecer la sincronización.
UCD	Durante su inicialización, el CM DEBE recibir un UCD utilizable (véase la nota) antes de transmitir en sentido ascendente. Cuando se está en el estado "obtener parámetros en sentido ascendente" del proceso de inicialización de un CM, si el CM no recibe un UCD utilizable dentro del periodo de temporización T1, dicho CM NO DEBE transmitir en sentido ascendente y DEBE explorar buscando otro canal descendente. Tras recibir un UCD utilizable, cada vez que el CM recibe un UCD no utilizable o un MAP con un contador de UCD que no concuerda con el campo cuenta de cambios de configuración del último UCD recibido, entonces el CM NO DEBE transmitir por la corriente ascendente y DEBE iniciar el temporizador T1. Si la temporización de T1 expira en estas circunstancias, el CM DEBE reposicionar y reinicializar su conexión MAC.
MAP	Un CM NO DEBE transmitir sin una atribución de anchura de banda en sentido ascendente válida. Si se pierde un MAP debido a un error, el CM NO DEBE transmitir durante el periodo abarcado por el MAP.
RNG-REQ RNG-RSP	Si un CM no recibe una respuesta de alineación válida durante un periodo de temporización definido después de transmitir una petición, se DEBE intentar de nuevo la petición un cierto número de veces (como se define en el anexo B.B). La no recepción de una respuesta de alineación válida después del número especificado de reintentos DEBE hacer que el módem reposicione y reinicialice su conexión MAC.
REG-REQ REG-RSP	Si un CM no recibe una respuesta de registro válida durante un periodo de temporización definido después de transmitir una petición, se intentará de nuevo la petición un cierto número de veces (como se define en el anexo B.B). La no recepción de una respuesta de registro válida después del número especificado de reintentos hará que el módem reposicione y reinicialice su conexión MAC.
UCC-REQ UCC-RSP	Si un CMTS no recibe una respuesta de cambio de canal en sentido ascendente válida dentro de un periodo de temporización definido después de transmitir una petición, se DEBE intentar de nuevo la petición un cierto número de veces (como se define en el anexo B.B). La no recepción de una respuesta válida después del número especificado de reintentos DEBE hacer que el CMTS considere al CM como no alcanzable.
NOTA – Un UCD utilizable es aquel que contiene perfiles legales que el módem puede comprender. El CM PUEDE también requerir que el contador de MAP recibidos del UCD concuerde con el campo cuenta de cambios de la configuración del último UCD recibido antes de considerar al UCD como utilizable.	

El anexo B.J contiene una lista de códigos de error con más información de utilidad acerca de los fallos en las capas PHY y MAC. Véase B.8.2.8 por más información.

La subcapa MAC considera que los mensajes de la capa de red y las capas superiores son paquetes de datos. Los mensajes son protegidos por el campo CRC del paquete de datos y cualquier paquete cuya CRC dé un resultado negativo es descartado. El retorno al funcionamiento normal tras la pérdida de estos paquetes se produce de acuerdo con el protocolo de capa superior.

B.11.5.1 Prevención de transmisiones no autorizadas

Un CM DEBERÍA incluir la manera de terminar una transmisión RF si detectara que su propia portadora ha permanecido activa de manera continua durante un periodo de tiempo superior al de la transmisión válida más larga posible.

B.12 Soporte de capacidades nuevas de módem de cable del futuro

B.12.1 Telecarga de soporte lógico operativo de módem de cable

Un CMTS DEBERÍA ofrecer la posibilidad de ser reprogramado localmente, mediante una operación a distancia consistente en la telecarga de soporte lógico a través de la red.

El dispositivo módem de cable DEBE ofrecer la posibilidad de ser reprogramado localmente mediante una operación a distancia consistente en la telecarga de soporte lógico por la red. Esta capacidad de telecarga de soporte lógico DEBE hacer posible el cambio de la funcionalidad del módem de cable sin que sea necesario que el personal del sistema de cable visite físicamente y configure de nuevo cada unidad. Se espera que esta capacidad de programación sobre el terreno se utilice para potenciar el soporte lógico del módem del cable y mejorar así la calidad de funcionamiento, acomodar nuevas funciones y prestaciones (por ejemplo, el soporte de clases de servicio mejoradas), corregir defectos de diseño encontrados en el soporte lógico y facilitar una vía de transición gradual a medida que evolucione la especificación de la interfaz de datos por cable.

El mecanismo utilizado para la telecarga DEBE ser la transferencia de ficheros TFTP. El mecanismo mediante el cual se aseguran y se autentican las transferencias figura en [DOCSIS8]. La transferencia DEBE ser iniciada de una de las dos maneras siguientes:

- Un gestor SNMP pide la mejora del CM;
- Si el nombre del fichero de mejora de soporte lógico del fichero de configuración del CM no concuerda con la configuración de soporte lógico actual del CM, el CM DEBE pedir el fichero especificado al servidor de soporte lógico por medio del TFTP.

La dirección IP de servidor de soporte lógico es un parámetro aparte. Si está presente, el CM DEBE intentar telecargar el fichero especificado desde este servidor. Si no está presente, el CM DEBE intentar telecargar el fichero especificado desde el servidor del fichero de la configuración.

El CM DEBE verificar que la configuración telecargada le resulta apropiada. Si la configuración es apropiada, el CM DEBE escribir la nueva configuración de soporte lógico en un almacenamiento no volátil. Una vez que concluya la transferencia del fichero, el CM DEBE reiniciarse a sí mismo con la nueva configuración de código.

Si el CM no puede completar la transferencia del fichero por cualquier motivo, DEBE seguir siendo capaz de aceptar nuevas telecargas de soporte lógico (sin interacción con el operador o el usuario), incluso si se interrumpe la potencia o la conectividad entre tentativas. El CM DEBE registrar en el fichero cronológico el fallo y PUEDE notificarlo de manera asíncrona al gestor de la red.

Tras la mejora del soporte lógico operativo, es posible que el CM necesite aplicar uno de los procedimientos descritos más arriba para cambiar los canales a fin de utilizar la funcionalidad perfeccionada.

Si el CM va a continuar funcionando con los mismos canales ascendente y descendente que antes de la mejora, DEBE ser capaz de interfuncionar con otros CM que pueden utilizar versiones anteriores del soporte lógico.

Cuando el soporte lógico haya sido mejorado para ajustarse a una nueva versión de la especificación, es fundamental que interfuncione con la versión anterior para hacer posible una transición gradual de las unidades de la red.

ANEXO B.A

Direcciones conocidas

B.A.1 Direcciones MAC

Las direcciones MAC aquí descritas se definen utilizando el convenio Ethernet/ISO/CEI 8802-3 conocido como pequeña fila india de bits.

Se DEBE utilizar la siguiente dirección de multidifusión para direccionar el conjunto de todas las subcapas MAC de CM; por ejemplo, cuando se transmiten las PDU diagrama de atribución.

01-E0-2F-00-00-01

La gama de direcciones,

01-E0-2F-00-00-03 a 01-E0-2F-00-00-0F

se reserva para definición futura. Las tramas dirigidas a cualquiera de esas direcciones NO DEBERÍAN ser reenviadas hacia afuera del dominio de subcapa MAC.

B.A.2 ID de servicio MAC

Los siguientes ID de servicio MAC tienen asignados significados. Los identificadores no incluidos en los siguientes subcláusulas están disponibles para asignación, ya sea por el CMTS o por vía administrativa.

B.A.2.1 ID de servicio de CM y de ningún CM

Estos ID de servicio se utilizan en los MAP para propósitos especiales o para indicar que cualquier CM puede responder en el intervalo correspondiente.

0x0000 No direccionado a ningún CM. Normalmente se utiliza cuando cambian los parámetros en ráfaga en sentido ascendente de manera que los CM tienen tiempo de ajustar sus moduladores antes de que entren en vigor las nuevas fijaciones en sentido ascendente.

0x3FFF Direccionado a todos los CM. Normalmente se utiliza para intervalos de petición de radiodifusión o intervalos de mantenimiento inicial.

B.A.2.2 ID conocidos de servicio "multidifusión"

Estos ID de servicio se utilizan solamente para IE de petición/datos. Indican que cualquier CM puede responder en un intervalo determinado, pero que debe limitar el tamaño de su transmisión a un número particular de miniintervalo de tiempo (como se indica mediante el SID particular de multidifusión asignado al intervalo).

0x3FF1-0x3FFE Direccionado a todos los CM. Disponible para pequeñas PDU datos, así como peticiones (utilizado solamente con IE petición/datos). El último dígito indica la longitud de trama y oportunidades de transmisión, como sigue.

- 0x3FF1 Dentro del intervalo especificado, una transmisión puede comenzar en cualquier miniintervalo de tiempo, y se debe ajustar dentro de un miniintervalo.
- 0x3FF2 Dentro del intervalo especificado, una transmisión puede comenzar en cualquier otro miniintervalo de tiempo, y se debe ajustar dentro de dos miniintervalos (por ejemplo, una estación puede iniciar la transmisión en el primer miniintervalo de tiempo del intervalo total, en el tercer miniintervalo, en el quinto, etc.).

0x3FF3 Dentro del intervalo especificado, una transmisión puede comenzar en cualquier tercer miniintervalo de tiempo, y se debe ajustar dentro de tres miniintervalos (por ejemplo, comienza en el primero, en el cuarto, en el séptimo, etc.).

0x3FF4 Comienza en el primero, en el quinto, en el noveno, etc.

0x3FFD Comienza en el primero, en el decimocuarto, en el vigésimo séptimo, etc.

0x3FFE Dentro del intervalo especificado, una transmisión puede comenzar en cualquier decimocuarto miniintervalo de tiempo, y se ha de ajustar dentro de 14 miniintervalos.

B.A.2.3 ID de servicio para petición de prioridad

Estos ID de servicio (0x3Exx) se reservan para los IE de petición (véase B.C.2.2.5.2).

- Si está fijado el bit 0x01, se puede pedir la prioridad cero.
- Si está fijado el bit 0x02, se puede pedir la prioridad uno.
- Si está fijado el bit 0x04, se puede pedir la prioridad dos.
- Si está fijado el bit 0x08, se puede pedir la prioridad tres.
- Si está fijado el bit 0x10, se puede pedir la prioridad cuatro.
- Si está fijado el bit 0x20, se puede pedir la prioridad cinco.
- Si está fijado el bit 0x40, se puede pedir la prioridad seis.
- Si está fijado el bit 0x80, se puede pedir la prioridad siete.

Los bits se pueden combinar como se desee mediante el programador CMTS en sentido ascendente para cualesquier IUC de petición.

B.A.3 PID MPEG

Todos los datos DOCSIS DEBEN ser transportados en paquetes MPEG-2 con el campo PID de encabezado fijado a 0x1FFE.

ANEXO B.B

Parámetros y constantes

Sistema	Nombre	Referencia de tiempo	Valor mínimo	Valor por defecto	Valor máximo
CMTS	Intervalo de sincronismo	Tiempo entre la transmisión de mensajes SYNC (véase B.8.3.2)			200 ms
CMTS	Intervalo UCD	Tiempo entre la transmisión de mensajes UCD (véase B.8.3.3)			2 s
CMTS	MAP máximo pendiente	Número de miniintervalos de tiempo que se permite a un CMTS trasladar al futuro (véase B.8.3.4)			4096 miniintervalos de tiempo
CMTS	Intervalo de alineación	Tiempo entre peticiones de alineación radiodifundidas (véase B.9.3.3)			2 s

Sistema	Nombre	Referencia de tiempo	Valor mínimo	Valor por defecto	Valor máximo
CM	Intervalo de sincronismo perdido	Tiempo transcurrido desde el último mensaje SYNC recibido antes que la sincronización se considere perdida			600 ms
CM	Nuevos intentos de alineación por contienda	Número de nuevos intentos de petición de alineación por contienda (véase B.11.2.4)	16		
CM, CMTS	Nuevos intentos de alineación por invitación	Número de nuevos intentos de petición de alineación por invitación (véase B.11.2.4)	16		
CM	Nuevos intentos de petición	Número de nuevos intentos de petición de atribución de anchura de banda	16		
CM CMTS	Nuevos intentos de petición/respuesta de registro	Número de nuevos intentos de petición/respuesta de registro	3		
CM	Nuevos intentos de datos	Número de nuevos intentos de transmisión inmediata de datos	16		
CMTS	Tiempo de procesamiento de MAP de CM	Tiempo transcurrido entre la recepción del último bit de un MAP en un CM y la efectividad de ese MAP (véase B.9.1.1)	200 µs		
CMTS	Tiempo de procesamiento de respuesta de alineación CM	Tiempo mínimo permitido a un CM tras la recepción de una respuesta de alineación antes de que conteste a una petición de alineación por invitación	1 ms		
CMTS	Configuración de CM	Tiempo máximo permitido a un CM tras la recepción de un fichero de configuración para que envíe una petición de registro a un CMTS	30 s		
CM	T1	Esperar temporización de UCD			5 × valor máximo del intervalo del UCD
CM	T2	Esperar temporización de alineación de radiodifusión			5 × intervalo de alineación
CM	T3	Espera de respuesta de alineación	50 ms	200 ms	200 ms

Sistema	Nombre	Referencia de tiempo	Valor mínimo	Valor por defecto	Valor máximo
CM	T4	Esperar oportunidad de alineación de unidifusión. Si el campo pendiente hasta compleción fue utilizado antes por este módem, el valor de ese campo se ha de añadir a este intervalo	30 s		35 s
CMTS	T5	Esperar respuesta de cambio de canal en sentido ascendente			2 s
CM CMTS	T6	Esperar REG-RSP y REG-ACK			3 s
CM, CMTS	Tamaño de miniintervalo de tiempo	Tamaño de miniintervalo de tiempo para transmisión en sentido ascendente. Debe ser una potencia de 2 (en unidades de tic de la base de tiempos)	32 tiempos de símbolo		
CM, CMTS	Tic de la base de tiempo	Unidad de temporización del sistema	6,25 µs		
CM, CMTS	Nuevos intentos de petición DSx	Número de nuevos intentos de temporización en las peticiones DSA/DSC/DSD	3		
CM, CMTS	Nuevos intentos de respuesta DSx	Número de nuevos intentos de temporización en las respuestas de DSA/DSC/DSD	3		
CM, CMTS	T7	Esperar temporización de respuestas DSA/DSC/DSD			1 s
CM, CMTS	T8	Esperar temporización de acuse de recibo DSA/DSC			300 ms
CM	Inicio del retroceso TFTP	Valor inicial del retroceso TFTP	1 s		
CM	Fin del retroceso TFTP	Valor último del retroceso TFTP	16 s		
CM	Nuevos intentos de petición TFTP	Número de nuevos intentos en petición TFTP	16		
CM	Nuevos intentos de telecarga TFTP	Número de nuevos intentos en telecargas completas TFTP	3		
CM	Espera TFTP	Espera entre secuencias de nuevo intento TFTP	10 min		
CM	Nuevos intentos ToD	Número de nuevos intentos por periodo de nuevo intento ToD	3		
CM	Periodo de nuevo intento ToD	Periodo de tiempo para nuevos intentos ToD	5 min		

Sistema	Nombre	Referencia de tiempo	Valor mínimo	Valor por defecto	Valor máximo
CMTS	T9	Temporización del registro, tiempo permitido entre el envío de un mensaje RNG-RSP (éxito) desde el CMTS al CM, y la recepción de un mensaje REG-REQ desde el mismo CM	15 min	15 min	
CM CMTS	T10	Esperar temporización del fin de transacción			3 s
CMTS	T11	Esperar respuesta de DCC por el canal antiguo			300 ms
CM	T12	Esperar acuse de recibo de DCC			300 ms
CMTS	T13	Tiempo máximo de retención de recursos QoS para DCC			1 s
CM	T14	Tiempo mínimo después de un rechazo-temp-DCC del DSx y el siguiente nuevo intento de la instrucción DSx	2 s		
CMTS	Nuevos intentos DCC-REQ	Número de nuevos intentos en petición dinámico de cambio de canal	3		
CM	Nuevos intentos DCC-RSP	Número de nuevos intentos en respuesta al cambio de canal, dinámico	3		
CM	Intervalo de pérdida de DCI-REQ	Tiempo desde el envío de un mensaje DCI-REQ y la no recepción de un mensaje DCI-RSP			2 s
CM	Nuevo intento de DCI-REQ	Número de nuevos intentos DCI-REQ antes de la reinicialización			16
CM	Inicio del retroceso DCI	Valor inicial del retroceso DCI	1 s		
CM	Fin del retroceso DCI	Valor último del retroceso DCI	16 s		

ANEXO B.C

Codificaciones comunes de interfaz de radiofrecuencia

B.C.1 Codificaciones para configuración y mensajes de capa MAC

Se DEBEN utilizar las siguientes codificaciones tipo/longitud/valor en el fichero de configuración (véase el anexo B.D), en las peticiones de registro CM y también en los mensajes de servicio dinámico. Todas las cantidades en multioctetos están en el orden de los octetos de la red, es decir, el octeto que contiene los bits más significativos es el primero que se transmite por el cable.

Las fijaciones de configuración siguientes DEBEN ser soportadas por todos los CM conformes con el presente anexo B.

B.C.1.1 Fijaciones de fichero de configuración y registro

Estas fijaciones se encuentran en el fichero de la configuración y, si están presentes, DEBEN ser reenviadas por el CM al CMTS en su petición de registro.

B.C.1.1.1 Fijación de la configuración frecuencia en sentido descendente

Se trata de la frecuencia de recepción que ha de utilizar por el CM. Representa una contraorden para el canal seleccionado durante la exploración. Es la frecuencia central en Hz del canal en sentido descendente almacenada como un número binario de 32 bits.

Tipo	Longitud	Valor
1	4	Frecuencia de recepción (rx)

Gama válida

La frecuencia de recepción DEBE ser un múltiplo de 62 500 Hz.

B.C.1.1.2 Fijación de la configuración ID del canal en sentido ascendente

Se trata del ID de canal en sentido ascendente que DEBE utilizar el CM. El CM DEBE estar a la escucha del canal descendente definido hasta que se encuentre un mensaje de descripción de canal ascendente con este ID. Representa una contraorden para el canal seleccionado durante la inicialización.

Tipo	Longitud	Valor
2	1	ID de canal

B.C.1.1.3 Objeto de control de acceso a red

Si el campo valor es 1, el CPE vinculado a este CM tiene permiso de acceso a la red, la base al provisionamiento del CM. Si el valor de este campo es 0, el CM NO DEBE reenviar tráfico del CPE vinculado a la red MAC, RF pero DEBE continuar aceptando y generando tráfico del propio CM. El valor de este campo no afecta al funcionamiento del flujo de servicio del CMTS ni al funcionamiento del reenvío de datos del CMTS.

Tipo	Longitud	Activado/desactivado
3	1	1 ó 0

NOTA – El propósito de "NACO = 0" es que el CM no reenvíe tráfico de cualquier CPE vinculado hacia la red de cable. (Un CPE es cualquier dispositivo cliente vinculado a ese CM, independientemente de cómo se implemente esa vinculación.) Sin embargo, con "NACO = 0", no se restringe el tráfico de gestión hacia el CM. De manera específica, con NACO desactivado, el CM sigue siendo gestionable, incluido el envío/la recepción de tráfico de gestión tal como (pero no limitado a ello):

- ARP: permite que el módem resuelva direcciones IP, pudiendo así responder a consultas o enviar trampas.
- DHCP: permite que el módem renueve su arriendo de dirección IP.
- ICMP: habilita la identificación de problemas de red con herramientas tales como "ping" y "traceroute".
- ToD: permite que el módem continúe la sincronización de su reloj después de la inicialización.

- TFTP: permite que el módem telecargue un nuevo fichero de configuración o una nueva configuración de soporte lógico.
- SYSLOG: permite que el módem informe de eventos de red.
- SNMP: permite la actividad de gestión.

En DOCSIS 1.1, con NACO desactivado, permanecen operacionales los flujos de servicio primarios del CM en sentido ascendente y sentido descendente sólo para el tráfico de gestión hacia y desde el CM. Con respecto al provisionamiento de DOCSIS 1.1, el CMTS debería ignorar el valor NACO y atribuir cualquier flujo de servicio que haya sido autorizado por el servidor de aprovisionamiento.

B.C.1.1.4 Fijación de la configuración clase de servicio DOCSIS 1.0

Este campo define los parámetros asociados con la clase de servicio DOCSIS 1.0. Cualquier CM que se registre con una fijación de configuración de clase de servicio DOCSIS 1.0 DEBE ser tratado como un CM de DOCSIS 1.0. Véase B.8.3.8.

Este campo define los parámetros asociados con una clase de servicio. Es algo complejo en el sentido de que está compuesto por varios campos tipo/longitud/valor encapsulados. Los campos encapsulados definen los parámetros particulares de clase de servicio de la clase de servicio en cuestión. Se señala que los campos tipo definidos sólo son válidos dentro de la cadena de fijaciones de configuración de clase de servicio encapsuladas. Se utiliza una sola fijación de configuración clase de servicio para definir los parámetros de una sola clase de servicio. Las definiciones de clases múltiples utilizan conjuntos múltiples de fijaciones de configuración clase de servicio.

Tipo	Longitud	Valor
4	n	

B.C.1.1.4.1 ID de clase

El valor de este campo especifica el identificador para la clase de servicio a la que es aplicable la cadena encapsulada.

Tipo	Longitud	Valor
4.1	1	

Gama válida

El ID de clase DEBE estar en la gama de 1 a 16.

B.C.1.1.4.2 Fijación de configuración velocidad máxima en sentido descendente

El valor de este campo especifica, para un módem de SID único, la velocidad máxima en bits por segundo en sentido descendente a la que se permite al CMTS reenviar hacia el CPE direcciones MAC de unidifusión que ha aprendido o que están configuradas como correspondientes al módem que se registra.

Para un módem de SID múltiples, el valor agregado de estos campos especifica la velocidad máxima en bits por segundo en sentido descendente a la que se permite al CMTS reenviar hacia el CPE direcciones MAC de unidifusión que ha aprendido o que están configuradas como correspondientes al módem que se registra.

Ésta es la velocidad cresta de datos para los datos de PDU paquetes (incluyendo las direcciones MAC de destino y la CRC) en un intervalo de un segundo. No incluye los paquetes MAC dirigidos hacia direcciones MAC de radiodifusión o multidifusión. El CMTS DEBE limitar el reenvío en sentido descendente a esta velocidad. El CMTS PUEDE retardar, en lugar de segregar, los paquetes que rebasen el límite.

Tipo	Longitud	Valor
4.2	4	

NOTA – Éste es un límite, no una garantía de que esta velocidad está disponible.

B.C.1.1.4.3 Fijación de configuración velocidad máxima en sentido ascendente

El valor de este campo especifica la velocidad máxima autorizada en bits por segundo en sentido ascendente a la que se permite al CM reenviar datos hacia la red de RF.

Ésta es la velocidad cresta de datos para los datos de PDU paquetes (incluyendo la dirección de destino y la CRC) en un intervalo de un segundo. El CM DEBE limitar todos los reenvíos en sentido ascendente (tanto por contienda como en base a reserva), para el SID correspondiente, para esta velocidad. El CM DEBE incluir los datos de PDU paquetes dirigidos hacia direcciones de radiodifusión o multidifusión cuando se calcula esta velocidad.

El CM DEBE hacer cumplir la velocidad máxima en sentido ascendente. NO DEBERÍA descartar tráfico en sentido ascendente debido simplemente a que excede esta velocidad.

El CMTS DEBE hacer cumplir este límite en todas las transmisiones de datos en sentido ascendente, incluyendo los datos enviados por contienda. El CMTS DEBERÍA generar una alarma si un módem excediera su velocidad autorizada.

Tipo	Longitud	Valor
4.3	4	

NOTA 1 – El propósito de este parámetro es que el CM efectúe la conformación del tráfico a la entrada de la red de RF y que el CMTS lleve a cabo la vigilancia del tráfico para asegurar que el CM no excede el límite.

El CMTS podría forzar el cumplimiento de este límite aplicando cualquiera de los métodos siguientes:

a) descartando las peticiones que excedan el límite;

b) aplazando (mediante concesiones de longitud cero) la concesión hasta que sea conforme al límite autorizado;

c) descartando los paquetes de datos que excedan el límite;

d) informando a un supervisor de vigilancia (por ejemplo, mediante el mecanismo de alarma) que pueda incapacitar los CM en deriva.

NOTA 2 – Éste es un límite, no es una garantía de que esta velocidad está disponible.

B.C.1.1.4.4 Fijación de configuración prioridad de canal en sentido ascendente

El valor del campo especifica la prioridad relativa asignada a esta clase de servicio para la transmisión de datos por el canal en sentido ascendente. Números más altos indican prioridad más elevada.

Tipo	Longitud	Valor
4.4	1	Frecuencia de recepción (rx)

Gama válida

$0 \rightarrow 7$

B.C.1.1.4.5 Fijación de configuración velocidad de datos de canal en sentido ascendente mínima garantizada

El valor del campo especifica la velocidad de datos en bit/s que se garantizará a esta clase de servicio en el canal en sentido ascendente.

Tipo	Longitud	Valor
4.5	4	

B.C.1.1.4.6 Fijación de configuración ráfaga de transmisión por canal en sentido ascendente máxima

El valor del campo especifica la ráfaga de transmisión máxima (en octetos) que se permite a esta clase de servicio por el canal ascendente. Un valor cero significa que no hay límite.

NOTA – Este valor no incluye ningún bit suplementario de capa física.

Tipo	Longitud	Valor
4.6	2	

B.C.1.1.4.7 Habilitación de privacidad en clase de servicio (CoS)

Esta fijación de configuración habilita/inhabilita la privacidad básica en una clase de servicio (CoS) aprovisionada. Véase DOCSIS8.

Tipo	Longitud	Habilitación/inhabilitación
4.7 (= CoS_BP_ENABLE)	1	1 ó 0

Cuadro B.C-1/J.112 – Ejemplo de codificación de clase de servicio DOCSIS 1.0

Tipo	Longitud	Valor (sub)tipo	Longitud	Valor	
4	28				**Fijación de configuración clase de servicio**
		1	1	1	Clase de servicio 1
		2	4	10 000 000	Velocidad máxima en sentido descendente de 10 Mbit/s
		3	4	300 000	Velocidad máxima en sentido ascendente de 300 kbit/s
		4	1	5	Prioridad de trayecto de retorno de 5
		5	4	64 000	64 kbit/s mínima garantizada
		6	2	1518	Ráfaga de transmisión máxima de 1518 octetos

Cuadro B.C-1/J.112 – Ejemplo de codificación de clase de servicio DOCSIS 1.0

Tipo	Longitud	Valor (sub)tipo	Longitud	Valor	
4	28				**Fijación de configuración clase de servicio**
		1	1	2	Clase de servicio 2
		2	4	5 000 000	Velocidad de ida máxima de 5 Mbit/s
		3	4	300 000	Velocidad de retorno máxima de 300 Mbit/s
		4	1	3	Prioridad de trayecto de retorno de 3
		5	4	32 000	32 kbit/s mínima garantizada
		6	2	1518	Ráfaga de transmisión máxima de 1518 octetos

B.C.1.1.5 Fijación de configuración verificación de integridad de mensaje (MIC, *message integrity check*) de CM

El campo valor contiene el código de verificación de la integridad del mensaje de CM. Dicho código se utiliza para detectar una modificación no autorizada o la degradación del fichero de la configuración.

Tipo	Longitud	Valor
6	16	d1, d2,…,d16

B.C.1.1.6 Fijación de configuración verificación de integridad de mensaje (MIC) de CMTS

El campo valor contiene el código de verificación de la integridad del mensaje del CMTS. Dicho código se utiliza para detectar una modificación no autorizada o la degradación del fichero de la configuración.

Tipo	Longitud	Valor
7	16	D1, d2,…,d16

B.C.1.1.7 Número máximo de CPE

Número máximo de CPE al que se puede conceder acceso a través de un CM durante un espacio CM. El espacio CM (véase B.5.1.2.3.1) es el tiempo entre el arranque y la reiniciación protegida del módem. El CM DEBE imponer el cumplimiento del número máximo de CPE.

NOTA 1 – Este parámetro no debe confundirse con el número de direcciones CPE que puede aprender un CM. Un módem puede aprender direcciones MAC Ethernet hasta su número máximo de sus direcciones CPE (véase B.5.1.2.3.1). El número máximo de CPE a los que se concede acceso a través del módem lo determina esta fijación de configuración.

Tipo	Longitud	Valor
18	1	

El CM DEBE interpretar este valor como un entero sin signo. La inexistencia de esta opción, o el valor 0, se DEBE interpretar como el valor por defecto de 1.

NOTA 2 – Esto representa un límite al número máximo de CPE a los que el CM concederá acceso. Las limitaciones de soporte físico de una determinada implementación de módem pueden requerir que el módem utilice un valor inferior.

B.C.1.1.8 Indicación de tiempo de servidor TFTP

Representa el tiempo o momento del envío del fichero de la configuración en segundos. La definición del tiempo está de acuerdo con [RFC 868].

Tipo	Longitud	Valor
19	4	Número de segundos desde 00:00 de 1 de enero de 1900

NOTA – El propósito de este parámetro es evitar que e hagan reproducciones con ficheros de configuración antiguos.

B.C.1.1.9 Dirección de módem aprovisionada por servidor TFTP

Se refiere a la dirección IP del módem que pide el fichero de la configuración.

Tipo	Longitud	Valor
20	4	Dirección IP

NOTA – El propósito de este parámetro es prevenir la simulación IP durante el registro.

B.C.1.1.10 Fijación de configuración clasificación de paquetes en sentido ascendente

Este campo define los parámetros asociados con una entrada de la lista de clasificación de tráfico en sentido ascendente. Véase B.C.2.1.1.

Tipo	Longitud	Valor
22	n	

B.C.1.1.11 Fijación de configuración clasificación de paquetes en sentido descendente

Este campo define los parámetros asociados con un clasificador en una lista de clasificación de tráfico en sentido descendente. Véase B.C.2.1.2.

Tipo	Longitud	Valor
23	n	

B.C.1.1.12 Codificaciones de flujo de servicio en sentido ascendente

Este campo define los parámetros asociados con la programación en sentido ascendente para un flujo de servicio. Véase B.C.2.2.1.

Tipo	Longitud	Valor
24	n	

B.C.1.1.13 Codificaciones de flujo de servicio en sentido descendente

Este campo define los parámetros asociados con la programación en sentido descendente para un flujo de servicio. Véase B.C.2.2.2.

Tipo	Longitud	Valor
25	n	

B.C.1.1.14 Supresión de encabezamiento de cabida útil

Este campo define los parámetros asociados con la supresión de encabezamiento de cabida útil.

Tipo	Longitud	Valor
26	n	

B.C.1.1.15 Número máximo de clasificadores

Se refiere al número máximo de clasificadores que el CM está autorizado a admitir.

Es necesario cuando se utiliza activación diferida porque el número de flujos de servicio aprovisionados puede ser alto y porque cada flujo de servicio podría soportar múltiples clasificadores. El aprovisionamiento representa el conjunto de flujos de servicio de entre los que puede seleccionar el CM, sin embargo, quizás convenga limitar el número de clasificadores admitidos de forma simultánea que se aplican a este conjunto. Este parámetro proporciona la capacidad de limitar el tamaño de ese conjunto.

Tipo	Longitud	Valor
28	2	Número máximo de clasificadores admitidos simultáneamente

El valor por defecto DEBE ser 0 a sin límite.

B.C.1.1.16 Habilitación de privacidad

Esta fijación de configuración habilita/inhabilita la privacidad básica en el flujo de servicio primario y en todos los demás flujos de servicio para este CM.

Tipo	Longitud	Valor
29	1	0: Inhabilitación 1: Habilitación

El valor por defecto de este parámetro DEBE ser 1 (privacidad habilitada).

B.C.1.1.17 Información específica del vendedor

La información específica del vendedor para módems de cable, si está presente, DEBE codificarse en el campo información específica del vendedor (VSIF, *vendor-specific information field*) (código 43) utilizando el campo ID de vendedor (véase B.C.1.3.2) para especificar qué tuplas TLV aplican a qué productos de los vendedores. El ID de vendedor DEBE ser la primera tupla TLV incorporada en el VSIF. Si la primera tupla TLV dentro del VSIF no es un ID de vendedor, la tupla TLV DEBE ser descartada.

Esta fijación de configuración PUEDE aparecer en múltiples ocasiones. El mismo ID de vendedor PUEDE aparecer en múltiples ocasiones. Esta fijación de configuración PUEDE estar anidada dentro de una fijación de configuración clasificación de paquetes, una fijación de configuración flujo de

servicio, o una respuesta de flujo de servicio. Sin embargo, NO DEBE haber más de una tupla TLV ID de vendedor dentro de un único VSIF.

Tipo	Longitud	Valor
43	n	Según la definición del vendedor

EJEMPLO:

Configuración con campos específicos del vendedor A y campos específicos del vendedor B:

VSIF (43) + n (número de octetos dentro de este VSIF)
8 (Tipo de ID de vendedor) + 3 (campo de longitud) + ID de vendedor del vendedor A
Tipo #1 específico del vendedor A + longitud del campo + valor #1
Tipo #2 específico del vendedor A + longitud del campo + valor #2

VSIF (43) + m (número de octetos dentro de este VSIF)
8 (tipo de ID de vendedor) + 3 (campo de longitud) + ID de vendedor del vendedor B
Tipo específico del vendedor B + longitud del campo + valor

B.C.1.1.18 Tupla TLV de gestión de abonado

La información de estas tuplas TLV no es utilizada por el CM; dicha información es utilizada, en cambio, por el CMTS para poblar la MIB de gestión de abonado de este CM.

Si están presentes en el fichero de configuración, el CM DEBE incluir estas tuplas TLV en los mensajes REG-REQ subsiguientes para que sean utilizadas por el CMTS a fin de poblar la MIB de gestión de abonado de este CM. Si están presentes en el fichero de configuración, el CM DEBE incluir estas tuplas TLV en el MIC del CMTS.

B.C.1.1.18.1 Control de gestión de abonado

Este campo de tres octetos proporciona información de control al CMTS para la base de información de gestión (MIB, *management information base*) de gestión del abonado. Los dos primeros octetos representan el número de direcciones IP autorizadas detrás del CM. El tercer octeto se utiliza para campos de control.

Tipo	Longitud	Valor
35	3	octeto 1, 2: docsSubMgtCpeControlMaxCpeIP (10 bits de orden inferior) octeto 3, bit 0: docsSubMgtCpeControlActive octeto 3, bit 1: docsSubMgtCpeControlLearnable octeto 3, bits 2-7: reservados, deben fijarse a cero

B.C.1.1.18.2 Cuadro IP del CPE de gestión de abonado

Este campo enumera las direcciones IP utilizadas para poblar el cuadro docsSubMgtCpeIpTable en la MIB de gestión de abonado dentro del CMTS.

Tipo	Longitud	Valor
36	n (múltiplo de 4)	Ipa1, Ipa2, Ipa3, Ipa4

B.C.1.1.18.3 Grupos de filtrado de gestión de abonado

La MIB de gestión del abonado permite que se asignen grupos de filtrado a un CM y al CPE conectado a ese CM. Incluye dos grupos de filtrado de CM, en sentido ascendente y en sentido descendente, y dos grupos de filtrado de CPE, en sentido ascendente y en sentido descendente. Estos

cuatro grupos de filtrado están codificados en el fichero de la configuración en una tupla TLV única como sigue:

Tipo	Longitud	Valor
37	8	octetos 1, 2: grupo de docsSubMgtSubFilterDownstream octetos 3, 4: grupo de docsSubMgtSubFilterUpstream octetos 5, 6: grupo de docsSubMgtCmFilterDownstream octetos 7, 8: grupo de docsSubMgtCmFilterUpstream

B.C.1.2 Fijaciones específicas de fichero de configuración

Estas fijaciones se encuentran solamente en el fichero de la configuración. Las fijaciones NO DEBEN ser reenviadas al CMTS en la petición de registro.

B.C.1.2.1 Marcador fin de datos

Es un marcador especial para la terminación de datos. No tiene campos de longitud ni valor.

Tipo		
255		

B.C.1.2.2 Fijación de configuración relleno

Esta fijación no tiene campos de longitud ni valor y solamente se utiliza a continuación del marcador fin de datos para rellenar el fichero hasta un número entero de palabras de 32 bits.

Tipo		
0		

B.C.1.2.3 Nombre de fichero de mejora de soporte lógico

Se trata del nombre de fichero del fichero de mejora de soporte lógico del CM. El nombre del fichero es un nombre de trayecto de directorio totalmente calificado. Se prevé que el fichero resida en un servidor TFTP identificado en una opción de fijación de configuración definida en B.D.2.2. Véase B.12.1.

Tipo	Longitud	Valor
9	n	Nombre de fichero

B.C.1.2.4 Control de acceso a la escritura del SNMP

Este objeto hace posible anular el acceso "fijado" del SNMP a objetos MIB individuales. Cada ejemplar de este objeto controla el acceso a todos los objetos MIB que pueden escribirse y con cuyo prefijo ID de objeto (OID), concuerda. Este objeto se puede repetir para inhabilitar el acceso a cualquier número de objetos MIB.

Tipo	Longitud	Valor
10	n	Prefijo OID más bandera de control

Donde n es el tamaño de la codificación, aplicando las reglas de codificación básica ASN.1 [ISO8025], del prefijo OID más un octeto para la bandera de control.

La bandera de control puede tomar los siguientes valores:

0: Permite el acceso a la escritura

1: Impide el acceso a la escritura

Se puede utilizar cualquier prefijo OID. Para controlar el acceso a todos los objetos MIB se puede utilizar el OID nulo 0.0. (El OID 1.3.6.1 tendrá el mismo efecto.)

Cuando están presentes y se superponen múltiples ejemplares de este objeto, tiene precedencia el prefijo más largo (más específico). Así por ejemplo:

someTable Impide el acceso a la escritura

someTable.1.3 Permite el acceso a la escritura

En este ejemplo se impide el acceso a todos los objetos de someTable salvo a las de someTable.1.3.

B.C.1.2.5 Objeto MIB del SNMP

Este objeto permite fijar objetos arbitrarios MIB del SNMP mediante el proceso de registro del TFTP.

Tipo	Longitud	Valor
11	n	Vinculación variable

donde el valor es una vinculación variable (VarBind) de SNMP definida en [RFC 1157]. La vinculación variable se codifica aplicando las reglas de codificación básica ASN.1, como si fuera parte de una petición de fijación de SNMP.

El módem de cable DEBE tratar este objeto como si fuera parte de una petición de fijación de SNMP teniendo en cuenta lo siguiente:

- la petición DEBE considerarse plenamente autorizada (no puede rehusar la petición por falta de privilegio);
- las disposiciones de control de la escritura del SNMP (véase la subcláusula anterior) no se aplican;
- el CM no genera ninguna respuesta SNMP.

Este objeto PUEDE repetirse con diferentes vinculaciones variables para "fijar" un cierto número de objetos MIB. Todas estas fijaciones DEBEN ser tratadas como si fueran simultáneas.

Cada vinculación variable DEBE limitarse a 255 octetos.

B.C.1.2.6 Dirección MAC de Ethernet de CPE

Este objeto configura el CM con la dirección MAC Ethernet de un dispositivo CPE (véase B.5.1.2.3.1). Este objeto se puede repetir para configurar cualquier número de direcciones de dispositivos CPE.

Tipo	Longitud	Valor
14	6	Dirección MAC de Ethernet de CPE

B.C.1.2.7 Servidor TFTP de mejora de soporte lógico

Se trata de la dirección IP del servidor TFTP en el que reside el fichero de mejora del soporte lógico para el CM. Véanse B.12.1 y B.C.1.2.3.

Tipo	Longitud	Valor
21	4	ip1, ip2, ip3, ip4

B.C.1.2.8 Valor de arranque SnmpV3

Los CM conformes DEBEN comprender las siguientes TLV y sus subelementos y ser capaces de arrancar el acceso SNMPv3 al CM independientemente de si los CM están funcionando en modo 1.0 o en modo 1.1.

Tipo	Longitud	Valor
34	n	Compuesto

Hasta cinco de estos objetos pueden estar incluidos en el fichero de la configuración. Cada uno de ellos da lugar a una fila adicional que se añade al cuadro usmDHKickstartTable y al cuadro usmUserTable y a un número público de agente generado para esas filas.

B.C.1.2.8.1 Nombre de la seguridad de arranque de SnmpV3

Tipo	Longitud	Valor
34.1	2-16	Nombre codificado de seguridad UTF8

Para el conjunto de caracteres ASCII, las codificaciones UTF8 y ASCII son idénticas. Normalmente, esto se especificará como uno de los usuarios USM integrados en Docsis, por ejemplo, "docsisManager", "docsisOperator", "docsisMonitor", "docsisUser". El nombre de seguridad NO termina en cero. Esto se indica en el cuadro usmDHKickStartTable como usmDHKickStartSecurityName y en el cuadro usmUserTable como usmUserName y usmUserSecurityName.

B.C.1.2.8.2 Número público del gestor de arranque de SnmpV3

Tipo	Longitud	Valor
34.2	n	Número público Diffie-Helman del gestor expresado como una cadena de octetos

Este número es el número público Diffie-Hellman derivado de un número aleatorio generado de forma privada (por el gestor u operador) y transformado de acuerdo con [RFC 2786]. Esto se indica en el cuadro usmDHKickStartTable como usmKickstartMgrPublic. Cuando se combina con el objeto notificado en la misma fila como usmKickstartMyPublicit puede ser utilizado para derivar las claves en la fila conexa del cuadro usmUserTable.

B.C.1.2.9 Certificado de verificación de código del fabricante

Se trata del certificado de verificación del código del fabricante (M-CVC, *manufacturer's code verification certificate*) para la telecarga segura del control lógico que se especifica en el anexo D de [DOCSIS8]. El fichero de configuración del CM DEBE contener este M-CVC y/o el C-CVC definidos en B.C.1.2.10 para permitir que el CM de conformidad con 1.1 efectúe la telecarga del fichero del código desde el servidor TFTP independientemente de que el CM esté aprovisionado para funcionar con BPI, con BPI+ o con ninguno de ellos. Véase el anexo D de [DOCSIS8] para más detalles.

Tipo	Longitud	Valor
32	n	CVC del fabricante (ASN.1 con codificación DER)

Si la longitud del M-CVC excede de 254 octetos, el M-CVC DEBE ser fragmentado en dos o más elementos sucesivos tipo 32. Cada fragmento, excepto el último DEBE tener una longitud de 254 octetos. El CM reconstruye el M-CVC concatenando los contenidos (Valor de los TLV) de elementos tipo 32 sucesivos en el orden en que aparecen en el fichero config. Por ejemplo, el primer octeto a continuación del campo de longitud del segundo elemento tipo 32 es tratado como si inmediatamente siguiera el último octeto del primer elemento tipo 32.

B.C.1.2.10 Certificado de verificación de código del co-firmante

Se trata del certificado de verificación del código del co-firmante (C-CVC, *co-signer's code verification certificate*) para la telecarga segura del control que se lógico especifica en el anexo D de [DOCSIS8]. El fichero de configuración del CM DEBE contener este C-CVC y/o el M-CVC definidos en B.C.1.2.9 para permitir que el CM de conformidad con 1.1 efectúe la telecarga del fichero del código desde el servidor TFTP independientemente de que el CM esté aprovisionado para funcionar con BPI, con BPI+, o con ninguno de ellos. Véase el anexo D de [DOCSIS8] para más detalles.

Tipo	Longitud	Valor
33	n	CVC del co-firmante (ASN.1 con codificación DER)

Si la longitud del C-CVC excede de 254 octetos, el C-CVC DEBE ser fragmentado en dos o más elementos sucesivos tipo 33. Cada fragmento, excepto el último, DEBE tener una longitud de 254 octetos. El CM reconstruye el C-CVC concatenando los contenidos (valor de las TLV) de elementos sucesivos tipo 33 en el orden en que aparecen en el fichero config. Por ejemplo, el primer octeto a continuación del campo de longitud del segundo elemento tipo 33 es tratado como si inmediatamente siguiera el último octeto del primer elemento tipo 33.

B.C.1.3 Codificaciones específicas de petición/respuesta de registro

Estas codificaciones no se encuentran en el fichero de la configuración, pero están incluidas en la petición de registro. Algunas codificaciones también son utilizadas en la respuesta de registro.

El CM DEBE incluir las codificaciones de las capacidades del módem en su petición de registro. Si están presentes en la petición de registro correspondiente, el CMTS DEBE incluir las capacidades del módem en la respuesta de registro.

B.C.1.3.1 Codificación de las capacidades del módem

El campo valor describe las capacidades de un módem particular, es decir, los límites, dependientes de la implementación, impuestos a las características particulares o al número de características que debe admitir el módem. Está compuesto por varios campos tipo/longitud/valor encapsulados. Los subtipos encapsulados definen las capacidades específicas del módem en cuestión. Se señala que los campos de subtipo definidos solamente son válidos dentro de la cadena de fijaciones de configuración de capacidades encapsuladas.

Tipo	Longitud	Valor
5	n	

Más adelante se describe el conjunto de posibles campos encapsulados.

B.C.1.3.1.1 Soporte de concatenación

Si el campo valor está fijado a "1", el CM pide soporte de concatenación desde el CMTS.

Tipo	Longitud	Valor
5.1	1	1 ó 0

B.C.1.3.1.2 Versión DOCSIS

Versión DOCSIS de este módem.

Tipo	Longitud	Valor
5.2	1	0: DOCSIS 1.0 1: DOCSIS 1.1 2 a 255: Reservados

Si esta tupla está ausente, el CMTS DEBE presuponer el funcionamiento DOCSIS 1.0. La ausencia de esta tupla o el valor "DOCSIS 1.0" no necesariamente significa que el CM soporta solamente funcionalidad DOCSIS 1.0, el CM PUEDE indicar que soporta otras capacidades individuales con otras codificaciones de capacidades del módem. (Véase B.G.3.)

B.C.1.3.1.3 Soporte de fragmentación

Si el campo valor está fijado a "1", el CM pide soporte de fragmentación desde el CMTS.

Tipo	Longitud	Valor
5.3	1	1 ó 0

B.C.1.3.1.4 Soporte de supresión de encabezamiento de cabida útil

Si el campo valor está fijado a "1", el CM pide soporte de supresión de encabezamiento de cabida útil desde el CMTS.

Tipo	Longitud	Valor
5.4	1	1 ó 0

B.C.1.3.1.5 Soporte del IGMP

Si el campo valor está fijado a "1", el CM soporta IGMP de conformidad con DOCSIS 1.1.

Tipo	Longitud	Valor
5.5	1	1 ó 0

B.C.1.3.1.6 Soporte de privacidad

El valor es el soporte de BPI del CM.

Tipo	Longitud	Valor
5.6	1	0 Soporte de BPI 1 Soporte de BPI Plus 2 a 255: Reservados

B.C.1.3.1.7 Soporte de SAID en sentido descendente

El campo muestra el número de SAID en sentido descendente que puede soportar el módem.

Tipo	Longitud	Valor
5.7	1	Número de SAID en sentido descendente que puede soportar el CM

Si el número de SAID es "0" significa que el módem sólo puede soportar 1 SAID.

B.C.1.3.1.8 Soporte de SID en sentido ascendente

El campo muestra el número de SID en sentido ascendente que puede soportar el módem.

Tipo	Longitud	Valor
5.8	1	Número de SID en sentido ascendente que puede soportar el CM

Si el número de SID es "0" significa que el módem sólo puede soportar 1 SID.

B.C.1.3.1.9 Soporte opcional de filtrado

El campo muestra el soporte opcional de filtrado en el módem.

Tipo	Longitud	Valor
5.9	1	Arreglo de soporte de filtrado de paquetes bit #0: filtrado 802.1P bit #1: filtrado 802.1Q bit #2-7: reservados, DEBE fijarse a cero

B.C.1.3.1.10 Derivaciones de ecualizador de transmisión por símbolo

Este campo muestra el número máximo de derivaciones previas al ecualizador por símbolo que soporta el CM.

NOTA – Todos los CM DEBEN soportar coeficientes de ecualización con reparación de símbolos. El soporte del CM de 2 ó 4 derivaciones por símbolo es opcional. Si falta esta tupla, ello significa que el CM soporta solamente coeficientes de ecualizador con reparación de símbolos.

Tipo	Longitud	Valor
5.10	1	1, 2 ó 4

B.C.1.3.1.11 Número de derivaciones de ecualizador de transmisión

Este campo muestra el número de derivaciones de ecualización que soporta el CM.

NOTA – Todos los CM DEBEN soportar una longitud de ecualizador de al menos 8 símbolos. El soporte del CM de hasta 64 derivaciones con separación de T, separación de T/2 o separación de T/4 es opcional. Si falta esta tupla ello significa que el CM soporta solamente una longitud de ecualizador de 8 derivaciones.

Tipo	Longitud	Valor
5.11	1	8 a 64

B.C.1.3.1.12 Soporte de DCC

El valor es el soporte de DCC del CM.

Tipo	Longitud	Valor
5.12	1	0 = DCC no es soportado 1 = DCC es soportado

B.C.1.3.2 Codificación de ID de vendedor

El campo valor contiene la identificación del vendedor especificada por el identificador único de organización de 3 octetos específico del vendedor de la dirección MAC del CM.

El ID de vendedor DEBE ser utilizado en una petición de registro, pero NO DEBE ser utilizado como un elemento independiente del fichero de la configuración. PUEDE ser utilizado como un subcampo del campo información específica del vendedor en un fichero de configuración. Cuando se utiliza como un subcampo del campo de información específica del vendedor, identifica el ID de vendedor de los CM que van a utilizar esta información. Cuando el ID de vendedor se utiliza en una petición de registro, es el ID de vendedor del CM que envía la petición.

Tipo	Longitud	Valor
8	3	v1, v2, v3

B.C.1.3.3 Dirección IP del módem

Para retrocompatibilidad con DOCSIS 1.0. Reemplazada por la dirección del módem aprovisionada por el servidor TFTP.

Tipo	Longitud	Valor
12	4	Dirección IP

B.C.1.3.4 Respuesta de servicio o servicios no disponibles

Esta fijación de configuración DEBE incluirse en el mensaje de respuesta de registro si el CMTS no puede o no desea conceder ninguna de las clases de servicio solicitadas que aparecen en la petición de registro. Aunque el valor sólo se aplica a la clase de servicio fallida, DEBE considerarse fallida la petición de registro en su totalidad (no se concede ninguna de las fijaciones de configuración clase de servicio).

Tipo	Longitud	Valor
13	3	ID de clase, tipo, código de confirmación

donde:

ID de clase identifica la clase de servicio de la petición que no está disponible.

Tipo es el objeto clase de servicio específico dentro de la clase que hace que la petición sea rechazada.

Código de confirmación: véase B.C.4.

B.C.1.4 Codificaciones específicas de mensaje de servicio dinámico

Estas codificaciones no se encuentran en el fichero de la configuración, ni en la señalización de petición/respuesta de registro. Solamente se encuentran en los mensajes DSA-REQ, DSA-RSP, DSA-ACK, DSC-REQ, DSC-RSP, DSC-ACK y DSD-REQ (véanse B.8.3.12 a B.8.3.18).

B.C.1.4.1 Compendio HMAC

La fijación compendio HMAC es un compendio de mensajes en clave. Si está habilitada la privacidad, el atributo compendio HMAC DEBE ser el atributo final en la lista de atributos de mensajes de servicio dinámico. El compendio de los mensajes se lleva a cabo teniendo en cuenta todos los parámetros del servicio dinámico (empezando inmediatamente después del encabezamiento del mensaje de gestión MAC y hasta, pero sin incluir, la fijación compendio HMAC), diferentes del compendio HMAC, en el orden en el cual aparecen dentro del paquete.

La inclusión del compendio en clave permite al receptor autenticar el mensaje. El algoritmo del compendio HMAC, y los requisitos de generación de claves en sentido ascendente y descendente, se documentan en [DOCSIS8].

Este parámetro contiene un troceado en clave que se utiliza para autenticar el mensaje. El algoritmo HMAC se define en [RFC 2104]. El algoritmo HMAC se especifica utilizando un algoritmo genérico con troceo criptográfico. La privacidad básica utiliza una versión particular de HMAC que emplea el algoritmo de troceado seguro (SHA-1, *secure hush algorithm*), definido en [SHA].

Más adelante se muestra un resumen del formato del atributo compendio HMAC. Los campos se transmiten de izquierda a derecha.

Tipo	Longitud	Valor
27	20	Un troceado SHA en clave de 160 bits (20 octetos)

B.C.1.4.2 Bloque de autorización

El bloque de autorización contiene una "insinuación" de autorización del CM al CMTS. Los datos específicos del contenido de esa "insinuación" quedan fuera del alcance del presente anexo B, pero incluyen [PKT-DQOS].

El bloque de autorización PUEDE estar presente en los mensajes DSA-REQ y DSC-REQ iniciados por un CM. Este parámetro NO DEBE estar presente en los mensajes DSA-RSP y DSC-RSP, ni en los mensajes DSA-REQ y DSC-REQ iniciados por un CMTS.

La información del bloque de autorización es aplicable al contenido completo del mensaje DSA-REQ o del mensaje DSC-REQ. Por eso, sólo PUEDE estar presente un único bloque de autorización por mensaje. El bloque de autorización, si está presente, DEBE pasarse al módulo de autorización en el CMTS. La información del bloque de autorización solamente es procesada por el módulo de autorización.

Tipo	Longitud	Valor
30	n	Secuencia de n octetos

B.C.1.4.3 Número de secuencia de clave

El valor muestra el número de secuencia de clave de la clave de autorización BPI+ que se utiliza para calcular el compendio HMAC en caso de que esté habilitada la privacidad.

Tipo	Longitud	Valor
31	1	Número de secuencia de clave de autorización (0 a 15)

B.C.2 Codificaciones relacionadas con calidad de servicio

B.C.2.1 Codificaciones de clasificación de paquetes

Las siguientes codificaciones de tipo/longitud/valor DEBEN ser utilizadas en el fichero de la configuración, los mensajes de registro y los mensajes de servicio dinámico para codificar los parámetros para la clasificación y la programación de los paquetes. Todas las cantidades en multioctetos están en el orden de los octetos de la red, es decir, el octeto que contiene los bits más significativos es el primero que se transmite por el cable.

Un clasificador DEBE contener al menos una codificación de B.C.2.1.5 "Codificaciones de clasificación de paquetes IP", de B.C.2.1.6 "Codificaciones de clasificación de paquetes LLC de Ethernet", o de B.C.2.1.7 "Codificaciones de clasificación de paquetes 802.1P/Q del IEEE".

Las siguientes fijaciones de configuración DEBEN ser soportadas por todos los CM que estén en conformidad con el presente anexo B.

B.C.2.1.1 Codificación de clasificación de paquetes en sentido ascendente

Este campo define los parámetros asociados con un clasificador en sentido ascendente.

Se señala que los mismos campos subtipo definidos son válidos tanto para la cadena de fijaciones de configuración clasificación de paquetes encapsulados en sentido ascendente como para la cadena de fijaciones en sentido descendente. Estos campos tipo no son válidos en otros contextos de codificación.

Tipo	Longitud	Valor
22	n	

B.C.2.1.2 Codificación de clasificación de paquetes en sentido descendente

Este campo define los parámetros asociados con un clasificador en sentido descendente.

Se señala que los mismos campos subtipo definidos son válidos tanto para la cadena de fijaciones de configuración clasificación de flujos encapsulados en sentido ascendente como para la cadena de fijaciones en sentido descendente. Los campos tipo no son válidos en otros contextos de codificación.

Tipo	Longitud	Valor
23	n	

B.C.2.1.3 Codificaciones de clasificador de paquetes en general

B.C.2.1.3.1 Referencia de clasificador

El valor del campo especifica una referencia para el clasificador. Este valor es único por mensaje de servicio dinámico, fichero de configuración, o mensaje de petición de registro.

Tipo	Longitud	Valor
[22/23].1	1	1-255

B.C.2.1.3.2 Identificador de clasificador

El valor del campo especifica un identificador para el clasificador. Este valor es único por flujo de servicio. El CMTS asigna el identificador del clasificador de paquetes.

Tipo	Longitud	Valor
[22/23].2	2	1-65 535

B.C.2.1.3.3 Referencia de flujo de servicio

El valor del campo especifica una referencia de flujo de servicio que identifica el flujo de servicio correspondiente.

Entre las tuplas TLV de clasificador de paquetes que aparecen en cualquier mensaje en el que el ID de flujo de servicio no es conocido (por ejemplo, mensajes DSA -REQ y REG-REQ iniciados por CM) DEBE figurar esta tupla TLV. En ninguna de las tuplas TLV de clasificador de paquetes que aparecen en un mensaje DSC-REQ y en los mensajes DSA-REQ iniciados por un CMTS DEBE estar especificada la referencia de flujo de servicio.

Tipo	Longitud	Valor
[22/23].3	2	1-65 535

B.C.2.1.3.4 Identificador de flujo de servicio

El valor de este campo especifica el ID de flujo de servicio que identifica el flujo de servicio correspondiente.

En las tuplas TLV de clasificador de paquetes en donde el ID de flujo de servicio no es conocido, esta tupla TLV NO DEBE estar incluida (por ejemplo, mensajes DSA-REQ y REG-REQ iniciados por un CM). En las tuplas TLV de clasificador de paquetes que aparecen en un mensaje DSC-REQ y en los mensajes DSA-REQ iniciados por un CMTS DEBE estar especificado el ID de flujo de servicio.

Tipo	Longitud	Valor
[22/23].4	4	1-4 294 967 295

B.C.2.1.3.5 Prioridad de regla

El valor del campo especifica la prioridad para el clasificador, que se utiliza para determinar el orden del clasificador. Un valor más alto indica prioridad más alta.

Los clasificadores que aparecen en los ficheros de configuración y los mensajes de registro PUEDEN tener prioridades comprendidas entre 0 y 255, con el valor 0 por defecto. Los clasificadores que aparecen en el mensaje DSA/DSC DEBEN tener prioridades comprendidas entre 64 y 191, con el valor 64 por defecto.

Tipo	Longitud	Valor
[22/23].5	1	

B.C.2.1.3.6 Estado de activación de clasificador

El valor de este campo especifica si el clasificador debería activarse en la selección de paquetes para el flujo de servicio. Normalmente se utiliza un clasificador inactivo con un AdmittedQosParameterSet para asegurar la disponibilidad de los recursos a efectos de su activación posterior. La activación del clasificador depende tanto de este atributo como del estado de su flujo de servicio. Si el flujo de servicio no está activo, no se utiliza el clasificador, independientemente de la fijación de este atributo.

Tipo	Longitud	Valor
[22/23].6	1	0: Inactivo 1: Activo

El valor por defecto es 1: activar el clasificador.

B.C.2.1.3.7 Acción de cambio de servicio dinámico

Cuando se recibe en una petición de cambio de servicio dinámico, este campo indica la acción que se debe tomar con este clasificador.

Tipo	Longitud	Valor
[22/23].7	1	0: DSC Añadir clasificador 1: DSC Sustituir clasificador 2: DSC Eliminar clasificador

B.C.2.1.4 Codificaciones de error de clasificador

Este campo define los parámetros asociados con errores de clasificador.

Tipo	Longitud	Valor
[22/23].8	n	

Una codificación de error de clasificador consta de un conjunto único de parámetros de error de clasificador definido por los siguiente parámetros individuales: parámetro con error, código de confirmación y mensaje de error.

La codificación de error de clasificador se devuelve en los mensajes REG-RSP, DSA-RSP y DSC-RSP para indicar el motivo de la respuesta negativa del receptor a una petición de establecimiento de clasificador en un mensaje REG-REQ, DSA-REQ o DSC-REQ.

En caso de fallo, los mensajes REG-RSP, DSA-RSP o DSC-RSP DEBEN incluir una codificación de error de clasificador para al menos un clasificador fallido solicitado en el mensaje REG-REQ, DSA-REQ o DSC-REQ. Una codificación de error de clasificador para el clasificador fallido DEBE incluir el código de confirmación y el parámetro con error y PUEDE incluir un mensaje de error. Si algunos conjuntos de clasificadores son rechazados pero otros en cambio son aceptados, las codificaciones de error de clasificador DEBEN ser incluidas solamente para los clasificadores rechazados. Cuando la transacción completa tiene éxito, el mensaje RSP o ACK NO DEBE incluir una codificación de error de clasificador.

Codificaciones de error de clasificador múltiples pueden aparecer en un mensaje REG-RSP, DSA-RSP o DSC-RSP, ya que múltiples parámetros de clasificador pueden tener errores. Un mensaje que incluso no tenga más que una sola codificación de error de clasificador NO DEBE contener ninguna otra codificación de clasificador de protocolo (por ejemplo, IP, 802.1P/Q).

Una codificación de error de clasificador NO DEBE aparecer en ningún mensaje REG-REQ, DSA-REQ o DSC-REQ.

B.C.2.1.4.1 Parámetro con error

El valor de este parámetro identifica el subtipo de un parámetro de clasificador solicitado con error en una petición de clasificador rechazada. Un conjunto de parámetros de error de clasificador DEBE tener exactamente una tupla TLV de parámetro con error dentro de una codificación de error de clasificador determinada.

Subtipo	Longitud	Valor
[22/23].8.1	n	Subtipo de codificación de clasificador con error

Si la longitud es 1, el valor es el subtipo de un solo nivel en donde se ha encontrado el error, por ejemplo 7 indica una acción de cambio no válida. Si la longitud es 2, el valor es el subtipo multinivel en donde se ha encontrado el error, por ejemplo "9-2" indica un valor de protocolo IP no válido.

B.C.2.1.4.2 Código de error

Este parámetro indica el estado de la petición. Un valor distinto de 0 corresponde al código de confirmación descrito en B.C.4. Un conjunto de parámetros de error de clasificador DEBE tener exactamente un código de error dentro de una codificación de error de clasificador determinada.

Subtipo	Longitud	Valor
[22/23].8.2	1	Código de confirmación

Un valor de okay (correcto) (0) indica que la petición de clasificador tuvo éxito. Puesto que un conjunto de parámetros de error de clasificador sólo es aplicable a parámetros con error, este valor NO DEBE ser utilizado.

B.C.2.1.4.3 Mensaje de error

Este subtipo es opcional en un conjunto de parámetros de error de clasificador. Si está presente, indica una cadena de texto se a de presentar en la consola del CM y/o en el fichero registro cronológico que describe con más detalle una petición de clasificador rechazada. Un conjunto de parámetros de error de clasificador PUEDE tener cero o un subtipo de mensaje de error dentro de una codificación de error de clasificador determinada.

Subtipo	Longitud	Valor
[22/23].8.3	n	Cadena de caracteres ASCII terminada en cero

NOTA – La longitud n incluye el cero de terminación.

El mensaje de codificación de clasificador completo DEBE tener una longitud total de menos de 256 caracteres.

B.C.2.1.5 Codificaciones de clasificación de paquetes IP

Este campo define los parámetros asociados con la clasificación del paquete IP.

Subtipo	Longitud	Valor
[22/23].9	n	

B.C.2.1.5.1 Gama y plantilla de tipo de servicio IP

Los valores del campo especifican los parámetros que concuerdan para la gama y la plantilla del octeto T = S de IP. Un paquete IP con el valor del octeto TOS de IP "ip-tos" concuerda con este parámetro si tos-low ≤ (ip-tos AND tos-mask) ≤ tos-high. Si este campo se omite, la comparación del octeto ToS del paquete IP para esta entrada es irrelevante.

Tipo	Longitud	Valor
[22/23].9.1	3	tos-bajo, tos-alto, tos-máscara

B.C.2.1.5.2 Protocolo IP

El valor del campo especifica el valor que concuerda para el campo protocolo IP [RFC 1700]. Si este parámetro se omite, la comparación del campo protocolo de encabezamiento IP para esta entrada es irrelevante.

Existen dos valores especiales del campo de protocolo IP: "256" que concuerda con tráfico con cualquier valor de protocolo IP, y "257" que concuerda tanto con tráfico TCP como UDP. Una entrada que incluya un valor de campo protocolo IP mayor que 257 DEBE invalidarse a efectos de comparaciones (es decir, ningún tráfico puede corresponder a esta entrada).

Tipo	Longitud	Valor
[22/23].9.2	2	prot1, prot2

Gama válida

0-257

B.C.2.1.5.3 Dirección de origen IP

El valor del campo especifica el valor que concuerda para la dirección de origen IP. Un paquete IP con dirección de origen IP "ip-src" concuerda a este parámetro si src = (ip-src AND smask), donde "smask" es el parámetro de B.C.2.1.5.4. Si este parámetro se omite, la comparación de la dirección de origen del paquete IP para esta entrada es irrelevante.

Tipo	Longitud	Valor
[22/23].9.3	4	src1, src2, src3, src4

B.C.2.1.5.4 Plantilla de origen IP

El valor del campo especifica el valor de la plantilla para la dirección de origen IP, como se describe en B.C.2.1.5.3. Si este parámetro se omite, la plantilla de origen IP por defecto es 255.255.255.255.

Tipo	Longitud	Valor
[22/23].9.4	4	smask1, smask2, smask3, smask4

B.C.2.1.5.5 Dirección de destino IP

El valor del campo especifica el valor que concuerda para la dirección de destino IP. Un paquete IP con dirección de destino IP "ip-dst" concuerda con este parámetro si dst = (ip-dst AND dmask), donde "dmask" es el parámetro de B.C.2.1.5.6. Si este parámetro se omite, entonces la comparación de la dirección de destino del paquete IP para esta entrada es irrelevante.

Tipo	Longitud	Valor
[22/23].9.5	4	dst1, dst2, dst3, dst4

B.C.2.1.5.6 Plantilla de destino IP

El valor del campo especifica el valor de la plantilla para la dirección de destino IP, como se describe en la dirección de destino IP. Si este parámetro se omite, la plantilla de destino IP por defecto es 255.255.255.255.

Tipo	Longitud	Valor
[22/23].9.6	4	dmask1, dmask2, dmask3, dmask4

B.C.2.1.5.7 Inicio de puerto de origen TCP/UDP

El valor del campo especifica el valor del puerto de origen del extremo inferior TCP/UDP. Un paquete IP con valor de puerto TCP/UDP "src-port" concuerda con este parámetro si sportlow ≤ src-port ≤ sporthigh. Si este parámetro se omite, el valor de sportlow por defecto es 0. Este parámetro es irrelevante para el tráfico IP no TCP/UDP.

Tipo	Longitud	Valor
[22/23].9.7	2	sportlow1, sportlow2

B.C.2.1.5.8 Extremo de puerto de origen TCP/UDP

El valor del campo especifica el valor de puerto de origen del extremo superior TCP/UDP. Un paquete IP con valor de puerto TCP/UDP "src-port" concuerda con este parámetro si sportlow ≤ src-port ≤ dsporthigh. Si este parámetro se omite, el valor de sporthigh por defecto es 65 535. Este parámetro es irrelevante para tráfico IP no TCP/UDP.

Tipo	Longitud	Valor
[22/23].9.8	2	sporthigh1, sporthigh2

B.C.2.1.5.9 Inicio de puerto de destino TCP/UDP

El valor del campo especifica el valor del puerto de destino del extremo inferior TCP/UDP. Un paquete IP con valor de puerto TCP/UDP "dst-port" concuerda con este parámetro si dportlow ≤ dst-port ≤ dporthigh. Si este parámetro se omite, el valor de dportlow por defecto es 0. Este parámetro es irrelevante para tráfico IP no TCP/UDP.

Tipo	Longitud	Valor
[22/23].9.9	2	dportlow1, dportlow2

B.C.2.1.5.10 Extremo de puerto de destino TCP/UDP

El valor del campo especifica el valor del puerto de destino del extremo superior TCP/UDP. Un paquete IP con valor de puerto TCP/UDP "dst-port" concuerda con este parámetro si dportlow ≤ dst-port ≤ dporthigh. Si este parámetro se omite, el valor de dporthigh por defecto es 65 535. Este parámetro es irrelevante para tráfico IP noTCP/UDP.

Tipo	Longitud	Valor
[22/23].9.10	2	dporthigh1, dporthigh2

B.C.2.1.6 Codificaciones de clasificación de paquetes LLC de Ethernet

Este campo define los parámetros asociados con la clasificación de paquetes LLC de Ethernet.

Tipo	Longitud	Valor
[22/23].10	n	

B.C.2.1.6.1 Dirección MAC de destino

Los valores del campo especifican los parámetros que concuerdan para la dirección MAC de destino. Un paquete Ethernet con dirección de destino MAC "etherdst" concuerda con este parámetro si dst = (etherdst AND msk). Si este parámetro se omite, entonces la comparación de la dirección MAC de destino de Ethernet para esta entrada es irrelevante.

Tipo	Longitud	Valor
[22/23].10.1	12	dst1, dst2, dst3, dst4, dst5, dst6, msk1, msk2, msk3, msk4, msk5, msk6

B.C.2.1.6.2 Dirección MAC de origen

El valor del campo especifica el valor que concuerda para la dirección MAC de origen. Si este parámetro se omite, la comparación de la dirección de la fuente MAC de Ethernet para esta entrada es irrelevante.

Tipo	Longitud	Valor
[22/23].10.2	6	src1, src2, src3, src4, src5, src6

B.C.2.1.6.3 Ethertype/DSAP/Tipo MAC

type, eprot1, y eprot2 indican el formato del ID del protocolo de capa 3 en el paquete Ethernet como sigue:

Si tipo = 0, la regla no utiliza el tipo de protocolo de capa 3 como un criterio de concordancia. Si tipo = 0, eprot1 y eprot2 se ignoran cuando se considera si un paquete concuerda con la regla actual.

Si tipo = 1, la regla aplica solamente a las tramas que contienen un valor Ethertype. Los valores Ethertype están contenidos en paquetes que utilizan la encapsulación DEC-Intel-Xerox (DIX, *DEC-Intel-Xerox*) o los formatos de encapsulación del protocolo de acceso a subred (SNAP) [RFC 1042]. Si tipo = 1, entonces eprot1, eprot2 determinan el valor de 16 bits de Ethertype con el que debe concordar el paquete con objeto de concordar con la regla.

Si tipo = 2, la regla aplica solamente a las tramas que utilizan el formato de encapsulación IEEE 802.2 con un servicio de destino (DSAP, *destination service*) diferente de 0xAA (el cual está reservado para SNAP). Si tipo = 2, los 8 bits inferiores de eprot1 y eprot2, DEBEN concordar con el octeto DSAP del paquete para coincidir con la regla.

Si tipo = 3, la regla aplica solamente a los mensajes de gestión MAC (campo FC 1100001x) con un campo "tipo" de su encabezamiento de mensaje de gestión MAC (B.8.3.1) entre los valores de eprot1 y eprot2, inclusive. Como excepción, NO DEBEN ser clasificados los siguientes tipos de mensajes de gestión MAC, que se transmiten siempre por el flujo de servicio primario:

Tipo 4: RNG_REQ
Tipo 6: REG_REQ
Tipo 7: REG_RSP
Tipo 14: REG_ACK

Si tipo = 4, la regla se considera como una regla "atrapa todos" que concuerda con todos los paquetes de PDU datos. La regla no concuerda con los mensajes de gestión MAC. En este caso se ignora el valor de eprot1 y eprot2.

Si la trama Ethernet contiene un encabezamiento rótulo IEEE 802.1P/Q (es decir, Ethertype 0x8100), este objeto se aplica al campo Ethertype incorporado dentro del encabezamiento IEEE 802.1P/Q.

Otros valores de tipo están reservados. Si esta tupla TLV se omite, la comparación de Ethertype o bien de DSAP 802.2 del IEEE, para esta regla es irrelevante.

Tipo	Longitud	Valor
[22/23].10.3	3	type, eprot1, eprot2

B.C.2.1.7 Codificaciones de clasificación de paquetes 802.1P/Q del IEEE

Este campo define los parámetros asociados con la clasificación del paquete 802.1P/Q del IEEE.

Tipo	Longitud	Valor
[22/23].11	n	

B.C.2.1.7.1 User_priority 802.1P del IEEE

Los valores del campo especifican los parámetros que concuerdan para los bits de prioridad de usuario 802.1P del IEEE. Un paquete Ethernet con valor "prioridad" de User_priority (prioridad de usuario) 802.1P del IEEE concuerda con estos parámetros si pri-low ≤ priority ≤ pri-high. Si este campo se omite, la comparación de los bits de prioridad de usuario 802.1P del IEEE para esta entrada es irrelevante.

Si este parámetro se especifica para una entrada, los paquetes Ethernet sin encapsulación 802.1Q del IEEE NO DEBEN concordar con esa entrada. Si este parámetro se especifica para una entrada en un CM que no soporta el reenvío de tráfico encapsulado 802.1Q, del IEEE esa entrada NO DEBE ser utilizada para ningún tráfico.

Tipo	Longitud	Valor
[22/23].11.1	2	pri-low, pri-high

Gama válida

0-7 para pri-low y pri-high.

B.C.2.1.7.2 VLAN_ID 802.1Q del IEEE

El valor del campo especifica el valor que concuerda para los bits del id_vlan 802.1Q del IEEE. Solamente los primeros 12 bits (es decir, los más significativos) del campo id_vlan especificado son significativos; los cuatro bits finales DEBEN ignorarse a efectos de la comparación. Si este campo se omite, la comparación de los bits id_vlan 802.1Q del IEEE para esta entrada es irrelevante.

Si este parámetro se especifica para una entrada, los paquetes Ethernet sin encapsulación 802.1Q del IEEE NO DEBEN concordar con esta entrada. Si este parámetro se especifica para una entrada en un CM que no soporta el reenvío de tráfico encapsulado 802.1Q del IEEE esta entrada NO DEBE ser utilizado para ningún tráfico.

Tipo	Longitud	Valor
[22/23].11.2	2	vlan_id1, vlan_id2

B.C.2.1.7.3 Parámetros de clasificador específico del vendedor

Estos parámetros permiten a los vendedores codificar los parámetros de clasificador específico del vendedor. El ID de vendedor DEBE ser la primera tupla TLV incorporada dentro de los parámetros de clasificador específico del vendedor. Si la primera tupla TLV dentro de los parámetros de clasificador específico del vendedor no es un ID de vendedor, DEBE descartarse la tupla TLV. (Véase B.C.1.1.17.)

Tipo	Longitud	Valor
[22/23].43	n	

B.C.2.1.8 Codificaciones de clasificación específica del sentido ascendente

B.C.2.1.8.1 Señal de activación de clasificador

Este campo DEBE ser utilizado solamente en los mensajes de cambio de servicio dinámico originados desde el CMTS y que afectan el conjunto de parámetros activo. No está presente en ningún otro tipo de mensajes de señalización de flujo de servicio.

Tipo	Longitud	Valor
[22/23].12	1	1 – Activar/Desactivar Clasificador en petición 2 – Activar/Desactivar Clasificador en acuse de recibo

Este campo indica al módem que cambie sus características de transmisión en sentido ascendente a fin de concordar con las del DSC ya sea inmediatamente después de recibir la petición DSC, o sólo después de recibir el mensaje DSC-ACK. En particular, señala el tiempo de activación o desactivación de cualesquiera clasificadores que se cambian como consecuencia de este intercambio DSC.

El valor por defecto es 2 para un aumente de anchura de banda. El valor por defecto es 1 para una disminución de anchura de banda. Si no está claro si se trata de aumento o disminución el valor por defecto es 2.

B.C.2.2 Codificaciones de flujo de servicio

Las siguientes codificaciones tipo/longitud/valor DEBEN ser utilizadas en el fichero de la configuración, los mensajes de registro y los mensajes de servicio dinámico para codificar los parámetros de los flujos de servicio. Todas las cantidades multioctetos están en el orden de los octetos de la red, es decir, el octeto que contiene los bits más significativos es el primero que se transmite por el cable.

Las siguientes fijaciones de configuración DEBEN ser soportadas por todos los CM que estén en conformidad con el presente anexo B.

B.C.2.2.1 Codificaciones de flujo de servicio en sentido ascendente

Este campo define los parámetros asociados con la programación en sentido ascendente para un flujo de servicio. Es algo complejo en el sentido de que consta de varios campos tipo/longitud/valor encapsulados.

Se señala que las cadenas de fijaciones de configuración flujo de servicio en sentido ascendente y en sentido descendente encapsuladas comparten el mismo plan de numeración del campo subtipo, debido a que muchos de los campos subtipo definidos son válidos para ambos tipos de fijaciones de configuración. Estos campos tipo no son válidos en otros contextos de codificación.

Tipo	Longitud	Valor
24	n	

B.C.2.2.2 Codificaciones de flujo de servicio en sentido descendente

Este campo define los parámetros asociados con la programación en sentido descendente para un flujo de servicio. Es algo complejo en el sentido de que consta de varios campos tipo/longitud/valor encapsulados.

Se señala que las cadenas de fijaciones de configuración clasificación de flujo en sentido ascendente y en sentido descendente encapsuladas comparten el mismo plan de numeración del campo subtipo, debido a que muchos de los campos subtipo definidos son válidos para ambos tipos de fijaciones de configuración excepto las codificaciones de flujo de servicio. Estos campos tipo no son válidos en otros contextos de codificación.

Tipo	Longitud	Valor
25	n	

B.C.2.2.3 Codificaciones de flujo de servicio general

B.C.2.2.3.1 Referencia de flujo de servicio

La referencia del flujo de servicio se utiliza para asociar una codificación de clasificador de paquetes con una codificación de flujo de servicio. La referencia de flujo de servicio se utiliza solamente para establecer un ID de flujo de servicio. Una vez que el flujo de servicio existe y tiene asignado un ID de flujo de servicio, la referencia del flujo de servicio NO DEBE continuar siendo utilizada. La referencia de flujo de servicio es única por fichero de configuración, intercambio de mensajes de registro, o intercambio de mensajes de adición a servicio dinámica.

Tipo	Longitud	Valor
[24/25].1	2	1-65 535

B.C.2.2.3.2 Identificador de flujo de servicio

El identificador de flujo de servicio es utilizado por el CMTS como la referencia primaria de un flujo de servicio. Solamente el CMTS puede emitir un identificador de flujo de servicio. Utiliza esta parametrización para emitir identificadores de flujo de servicio en peticiones DSA iniciadas por un CMTS y en su mensaje de respuesta REG/DSA a las peticiones REG/DSA iniciadas por un CM. El CM especifica el SFID de un flujo de servicio utilizando este parámetro en un mensaje DSC-REQ.

El fichero de la configuración NO DEBE contener este parámetro.

Tipo	Longitud	Valor
[24/25].2	4	1-4 294 967 295

B.C.2.2.3.3 Identificador de servicio

El valor de este campo especifica el identificador de servicio asignado por el CMTS a un flujo de servicio con un AdmittedQosParameterSet o un ActiveQosParameterSet no nulos. Esto se utiliza en el MAP de atribución de anchura de banda para asignar anchura de banda en sentido ascendente. Este campo DEBE estar presente en los mensajes DSA-REQ o DSC-REQ iniciados por un CMTS relacionados con el establecimiento de un flujo de servicio admitido o activo en sentido ascendente. Este campo DEBE estar presente también en los mensajes REG-RSP, DSA-RSP y DSC-RSP relacionados al establecimiento con éxito de un flujo de servicio admitido o activo en sentido ascendente.

Aun cuando un flujo de servicio haya sido admitido o activado con éxito (es decir, tiene un ID de servicio asignado) el ID de flujo de servicio DEBE ser utilizado para la señalización de mensajes DSx subsiguientes ya que representa el asa primaria de un flujo de servicio. Si un flujo de servicio ya no es admitido o no está activo (vía el mensaje DSC-REQ) su ID de servicio PUEDE ser reasignado por el CMTS.

Subtipo	Longitud	Valor
[24/25].3	2	SID (los 14 bits de orden inferior)

B.C.2.2.3.4 Nombre de clase de servicio

El valor del campo se refiere a una configuración de servicio de CMTS predefinida que se ha de utilizar para este flujo de servicio.

Tipo	Longitud	Valor
[24/25].4	2 a 16	Cadena de caracteres ASCII terminada en cero

NOTA – La longitud incluye el cero de terminación.

Cuando el nombre de clase de servicio se utiliza en una codificación de flujo de servicio, indica que todos los parámetros QoS no especificados del flujo de servicio han de ser proporcionados por el CMTS. Corresponde al operador armonizar la definición de los nombres de clase de servicio en el CMTS y en el fichero de la configuración.

B.C.2.2.4 Codificaciones de error de flujo de servicio

Este campo define los parámetros asociados con errores de flujo de servicio.

Tipo	Longitud	Valor
[24/25].5	n	

Una codificación de error de flujo de servicio consiste de un conjunto único de parámetros de error de flujo de servicio el cual está definido por los siguientes parámetros individuales: parámetro con error, código de confirmación y mensaje de error.

La codificación de error de flujo de servicio se devuelve en los mensajes REG-RSP, DSA-RSP y DSC-RSP para indicar el motivo de la respuesta negativa del receptor a una petición de establecimiento de flujo de servicio en un mensaje REG-REQ, DSA-REQ o DSC-REQ.

La codificación de error de flujo de servicio se devuelve en los mensajes REG-ACK, DSA-ACK y DSC-ACK para indicar el motivo de la respuesta negativa del receptor a la ampliación del nombre de clase de servicio en los mensajes REG-RSP, DSA-RSP o DSC-RSP correspondientes.

En caso de fallo, los mensajes REG-RSP, DSA-RSP o DSC-RSP DEBEN incluir una codificación de error de flujo de servicio al menos para un flujo de servicio fallido pedido en el mensaje REG-REQ, DSA-REQ o DSC-REQ. En caso de fallo, los mensajes REG-ACK, DSA-ACK o DSC-ACK DEBEN incluir una codificación de error de flujo de servicio al menos para una ampliación fallida de nombre de clase de servicio en los mensajes REG-RSP, DSA-RSP o DSC-RSP. Una codificación de error de flujo de servicio para el flujo de servicio fallido DEBE incluir el código de confirmación y el parámetro con error y PUEDE incluir un mensaje de error. Si algunos conjuntos de parámetros de flujo de servicio son rechazados pero otros conjuntos de parámetros de flujo de servicio son aceptados, las codificaciones de error de flujo de servicio DEBEN incluirse solamente para el flujo de servicio rechazado.

En caso de éxito de la transacción completa, el mensaje RSP o ACK NO DEBE incluir una codificación de error de flujo de servicio.

Codificaciones múltiples de error de flujo de servicio PUEDEN aparecer en los mensajes REG-RSP, DSA-RSP, DSC-RSP, REG-ACK, DSA-ACK o DSC-ACK, ya que múltiples parámetros de flujo de servicio pueden tener errores. Un mensaje que incluso no tenga más que una sola codificación de error de flujo de servicio NO DEBE contener ningún parámetro QoS.

Las codificaciones de error de flujo de servicio NO DEBEN aparecer en ningún mensaje REG-REQ, DSA-REQ o DSC-REQ.

B.C.2.2.4.1 Parámetro con error

El valor de este parámetro identifica el subtipo de un parámetro de flujo de servicio solicitado con error en una petición de flujo de servicio rechazada o en una respuesta de ampliación de nombre de clase de servicio. Un conjunto de parámetros de error de flujo de servicio DEBE tener exactamente una tupla TLV del parámetro con error dentro de una codificación de error de flujo de servicio determinada.

Subtipo	Longitud	Valor
[24/25].5.1	1	Subtipo con error de codificación de flujo de servicio

B.C.2.2.4.2 Código de error

Este parámetro indica el estado de la petición. Un valor distinto de 0 corresponde al código de confirmación descrito en B.C.4. Un conjunto de parámetros de error de flujo de servicio DEBE tener exactamente un código de error dentro de una codificación de flujo de servicio determinada.

Subtipo	Longitud	Valor
[24/25].5.2	1	Código de confirmación

Un valor de okay (correcto) (0) indica que la petición de flujo de servicio tuvo éxito. Puesto que un conjunto de parámetros de error de flujo de servicio sólo es aplicable a los parámetros con error, este valor NO DEBE ser utilizado.

B.C.2.2.4.3 Mensaje de error

Este subtipo es opcional en un conjunto de parámetros de error de flujo de servicio. Si está presente, indica una cadena de texto que se ha de presentar en la consola CM y/o en el fichero registro cronológico que describe con más a detalle una petición de flujo de servicio rechazada. Un conjunto

de parámetros de error de flujo de servicio PUEDE tener cero o un subtipo de mensaje de error dentro de una codificación de error de flujo de servicio determinada.

Subtipo	Longitud	Valor
[24/25].5.3	n	Cadena de caracteres ASCII terminada en cero

NOTA 1 – La longitud n incluye el cero de terminación.

NOTA 2 – El mensaje completo de codificación de flujo de servicio DEBE tener una longitud total de menos de 256 caracteres.

B.C.2.2.5 Codificaciones comunes de parámetros de calidad de servicio en sentido ascendente y descendente

Los parámetros restantes tipo 24 y 25 son parámetros QoS. Cualquier tipo de parámetro QoS dado DEBE aparecer cero o una veces por codificación de flujo de servicio.

B.C.2.2.5.1 Tipo conjunto de parámetros de calidad de servicio

Este parámetro DEBE aparecer dentro de cada codificación de flujo de servicio. Especifica la aplicación apropiada del conjunto de parámetros QoS: el conjunto aprovisionado, el conjunto admitido, y/o el conjunto activo. Cuando dos conjuntos de parámetros QoS son el mismo conjunto, PUEDE utilizarse un valor de múltiples bits de este parámetro para aplicar los parámetros QoS a más de un conjunto. Un sólo mensaje PUEDE contener múltiples conjuntos de parámetros QoS en codificaciones separadas de flujo de servicio tipo 24/25 para el mismo flujo de servicio. Esto permite la especificación de los conjuntos de parámetros QoS cuando sus parámetros son diferentes. El bit 0 es el LSB del campo valor.

Por cada flujo de servicio que aparece en un mensaje de petición de registro o respuesta de registro, DEBE haber una codificación de flujo de servicio que especifique un conjunto ProvisionedQosParameterSet. Esta codificación de flujo de servicio, u otra u otras codificaciones de flujo de servicio, PUEDEN especificar también un conjunto admitido y/o activo.

Cualquier codificación de flujo de servicio que aparezca en un mensaje de servicio dinámico NO DEBE especificar el conjunto ProvisionedQosParameterSet.

Tipo	Longitud	Valor
[24/25].6	1	Bit #0: Conjunto aprovisionado Bit #1: Conjunto admitido Bit #2: Conjunto activo

Cuadro B.C-2/J.112 – Valores utilizados en los mensajes REG-REQ y REG-RSP

Valor	Mensajes
001	Aplicar solamente al conjunto aprovisionado
011	Aplicar los conjuntos aprovisionado y admitido, y efectuar el control de admisión
101	Aplicar a los conjuntos aprovisionado y activo, efectuar el control de admisión en el conjunto admitido en codificación de flujo de servicio separada, y activar el flujo de servicio
111	Aplicar a los conjuntos aprovisionado, admitido y activo; efectuar el control de admisión y activar este flujo de servicio

Cuadro B.C-3/J.112 – Valores utilizados en los mensajes REG-REQ, REG-RSP y en los mensajes de servicio dinámico

Valor	Mensajes
010	Efectuar el control de admisión y aplicarlo al conjunto admitido
100	Verificar comparando con el conjunto admitido en una codificación de flujo de servicio separada, efectuar el control de admisión si se requiere, activar este flujo de servicio y aplicar al conjunto activo
110	Efectuar el control de admisión y activar este flujo de servicio, aplicar los parámetros tanto al conjunto admitido como al conjunto activo.

El valor 000 se utiliza solamente en los mensajes de cambio de servicio dinámico. Se utiliza para fijar a nulo los conjuntos activo y admitido (véase B.10.1.7.4).

Un CMTS DEBE tramitar una sola actualización de cada uno de los conjuntos de parámetros QoS activos y admitidos. NO se requiere capacidad de procesamiento de múltiples codificaciones de flujo de servicio que especifican el mismo conjunto de parámetros QoS; se deja como una función específica de vendedor. Si un mensaje DSA/DSC contiene múltiples actualizaciones de un sólo conjunto de parámetros QoS y el vendedor no admite eras actualizaciones, el CMTS DEBE responder con el código de error 2, rechazo de fijación de configuración no reconocida.

B.C.2.2.5.2 Prioridad de tráfico

El valor de este parámetro especifica la prioridad asignada a un flujo de servicio. Si se indican dos flujos de servicio idénticos en todos los parámetros QoS además de la prioridad, al flujo de servicio con la prioridad más alta DEBERÍA corresponderle menor demora y preferencia en cuanto al almacenamiento en memoria tampón. En el caso de flujos de servicio que no son idénticos, el parámetro de prioridad NO DEBERÍA tener precedencia respecto a ningún parámetro QoS de flujo de servicio contradictorio. El algoritmo específico para imponer la aplicación de este parámetro no es aquí obligatorio.

Para flujos de servicio en sentido ascendente, el CMTS DEBERÍA utilizar este parámetro cuando determina la precedencia en el servicio de petición y en la generación de concesiones, y el CM DEBE preferentemente seleccionar las oportunidades de petición de contención para los ID de servicio de petición de prioridad (véase B.A.2.3) en base a esta prioridad y a su política de petición/transmisión (véase B.C.2.2.6.3).

Tipo	Longitud	Valor
[24/25].7	1	0 a 7 (Los números más altos indican prioridad más alta)

NOTA – La prioridad por defecto es 0.

B.C.2.2.5.3 Velocidad de tráfico continua máxima

Este parámetro es el parámetro de velocidad R de un límite de velocidad basado en el "depósito testigo" de paquetes. R se expresa en bits por segundo, y DEBE tener en cuenta todas las PDU datos de la trama MAC del flujo de servicio desde el octeto que sigue a la HCS del encabezamiento MAC hasta el fin de la CRC (véase la nota 1). El número de octetos reenviados (en octetos) está limitado durante cualquier intervalo de tiempo T por Max(T), como se describe en la siguiente ecuación:

$$Max(T) = T \times (R/8) + B \qquad \text{(B.C.2.2.5.3-1)}$$

donde el parámetro B (en octetos) es la fijación de configuración ráfaga máxima de tráfico (véase B.C.2.2.5.4).

NOTA 1 – El tamaño de la cabida útil incluye toda PDU de una trama MAC concatenada.

NOTA 2 – Este parámetro no limita la velocidad instantánea del flujo de servicio.

NOTA 3 – El algoritmo específico para imponer la aplicación de este parámetro no es aquí obligatorio. Cualquier implementación que cumpla la ecuación anterior es conforme.

NOTA 4 – Si este parámetro se omite o se fija a cero, no hay un máximo de velocidad de tráfico impuesto de manera explícita. Este campo especifica sólo un límite, no una garantía de que estará esta velocidad está disponible.

B.C.2.2.5.3.1 Velocidad de tráfico continua máxima en sentido ascendente

Para un flujo de servicio en sentido ascendente, el CM NO DEBE solicitar anchura de banda que exceda el requisito de Max(T) de la ecuación (B.C.2.2.5.3-1) durante cualquier intervalo T ya que esto podría obligar al CMTS a llenar los MAP con concesiones diferidas.

El CM DEBE diferir los paquetes en sentido ascendente que contravengan la ecuación (B.C.2.2.5.3-1) y "configurar su velocidad" para satisfacer esa expresión, hasta un límite impuesto por las restricciones de almacenamiento en memoria tampón del vendedor.

El CMTS DEBE hacer cumplir la ecuación (B.C.2.2.5.3-1) en todas las transmisiones de datos en sentido ascendente, incluidos los datos enviados por contienda. El CMTS PUEDE considerar las concesiones no utilizadas en los cálculos que incluyen este parámetro. El CMTS PUEDE hacer cumplir este límite por cualquiera de los siguientes métodos:

a) descarte de las peticiones que excedan el límite;

b) aplazamiento (mediante concesiones de longitud cero) de la concesión hasta que tenga conformidad con el límite permitido, o

c) descarte de los paquetes de datos que excedan el límite.

Un CMTS DEBE informar de esta condición a un módulo de políticas. Si el CMTS actúa descartando paquetes o peticiones, DEBE permitir un margen de error entre los algoritmos del CM y del CMTS.

Tipo	Longitud	Valor
[24/25].8	4	R (en bits por segundo)

B.C.2.2.5.3.2 Velocidad de tráfico continua máxima en sentido descendente

Para un flujo de servicio en sentido descendente, este parámetro sólo es aplicable en el CMTS. El CMTS DEBE hacer cumplir la ecuación (B.C.2.2.5.3-1) en todas las transmisiones de datos en sentido descendente. El CMTS NO DEBE reenviar paquetes en sentido descendente que contravengan la ecuación (B.C.2.2.5.3-1) en cualquier intervalo T. El CMTS DEBERÍA "configurar la velocidad" del tráfico en sentido descendente poniendo en cola de espera los paquetes que lleguen excediendo el límite de la ecuación (B.C.2.2.5.3-1), y retardarlos hasta que la expresión pueda ser satisfecha.

No se pretende imponer el cumplimiento de este parámetro en el CM.

Tipo	Longitud	Valor
25.8	4	R (en bits por segundo)

B.C.2.2.5.4 Ráfaga máxima de tráfico

El valor de este parámetro especifica el tamaño B del depósito testigo (en octetos) para este flujo de servicio como se describe en la ecuación (B.C.2.2.5.3-1). Este valor se calcula desde el octeto que sigue a la HCS del encabezamiento MAC hasta el fin de la CRC (véase la nota 1).

NOTA 1 – El tamaño de la cabida útil incluye toda PDU de una trama MAC concatenada.

Si este parámetro se omite, el valor de B por defecto es de 1522 octetos. El valor mínimo de B bien es el total de los 1522 octetos o bien el valor del tamaño de ráfaga concatenada máxima, el mayor de ambos (véase B.C.2.2.6.1).

Tipo	Longitud	Valor
[24/25].9	4	B (octetos)

NOTA 2 – El algoritmo específico para imponer la aplicación de este parámetro no es aquí obligatorio. Cualquier implementación que cumpla la ecuación anterior es conforme.

B.C.2.2.5.5 Velocidad de tráfico reservada mínima

Este parámetro especifica la velocidad mínima en bits/s, reservada para este flujo de servicio. El CMTS DEBERÍA poder satisfacer las peticiones de anchura de banda para un flujo de servicio hasta su velocidad de tráfico reservada mínima. Si se pide menos anchura de banda que su velocidad de tráfico reservada mínima para un flujo de servicio, el CMTS PUEDE reatribuir el exceso de anchura de banda reservada a otros propósitos. La suma de las velocidades de tráfico reservadas mínimas de todos los flujos de servicio PUEDE superar la cantidad de anchura de banda disponible. El valor de este parámetro se calcula desde el octeto que sigue a la HCS del encabezamiento MAC hasta el fin de la CRC (véase la nota 1). Si este parámetro se omite, toma por defecto un valor de 0 bit/s (es decir, no se reserva anchura de banda para el flujo por defecto).

NOTA 1 – El tamaño de la cabida útil incluye toda PDU de una trama MAC concatenada.

Este campo sólo es aplicable en el CMTS y su aplicación DEBE ser impuesta por el CMTS.

Tipo	Longitud	Valor
[24/25].10	4	

NOTA 2 – El algoritmo específico para imponer la aplicación del valor especificado en este campo no es aquí obligatorio.

B.C.2.2.5.6 Tamaño supuesto de paquete de velocidad reservada mínima

El valor de este campo especifica un tamaño supuesto de paquete mínimo (en octetos) para el que se proporciona la velocidad de tráfico reservada mínima. Este parámetro se define en octetos y se especifica como los octetos que siguen a la HCS del encabezamiento MAC hasta el fin de la CRC (véase la nota). Si el flujo de servicio envía paquetes de un tamaño menor que el valor especificado, dichos paquetes serán tratados como si tuvieran el tamaño especificado en este parámetro para el cálculo de la velocidad de tráfico reservada mínima y para el cálculo del conteo de los octetos (es decir, los octetos transmitidos) que pueden ser utilizados finalmente a efectos de facturación.

NOTA – El tamaño de la cabida útil incluye toda PDU de una trama MAC concatenada.

El CMTS DEBE aplicar este parámetro a su algoritmo de velocidad de tráfico reservada mínima. Este parámetro es utilizado por el CMTS para estimar la tara por paquete de cada paquete del flujo de servicio.

Si este parámetro se omite, el valor por defecto depende de la implementación del CMTS.

Tipo	Longitud	Valor
[24/25].11	2	

B.C.2.2.5.7 Temporización de parámetros QoS activos

El valor de este parámetro especifica el tiempo máximo durante el cual los recursos permanecen sin ser utilizados en un flujo de servicio activo. Si no hay actividad en el flujo de servicio dentro de ese intervalo de tiempo, el CMTS DEBE cambiar a nulos los conjuntos de parámetros QoS activos y admitidos. El CMTS DEBE señalizar este cambio de recurso con un mensaje DSC-REQ enviado al CM.

Tipo	Longitud	Valor
[24/25].12	2	Segundos

La aplicación de este parámetro DEBE imponerse en el CMTS y NO DEBERÍA imponerse en el CM. El parámetro es procesado por el CMTS para cada conjunto de QoS contenido en los mensajes de registro y en los mensajes de servicio dinámico. Si se omite el parámetro, se supone el valor por defecto de 0 (es decir, temporización infinita) El valor especificado para el conjunto de QoS activo debe ser menor o igual que el valor correspondiente en el conjunto de QoS admitido, el cual debe ser menor o igual que el valor correspondiente en el conjunto de QoS aprovisionado/autorizado. Si el valor pedido es demasiado grande, el CMTS PUEDE rechazar el mensaje o responder con un valor menor que el solicitado. Si el mensaje de registro o de servicio dinámico es aceptado por el CMTS y el CM acuse recibo del mismo, el temporizador de la temporización de QoS activo se carga con el nuevo valor de temporización. El temporizador es activado si el mensaje activa el flujo de servicio asociado. El temporizador es desactivado si el mensaje fija el conjunto de QoS activo a nulo.

B.C.2.2.5.8 Temporización de parámetros QoS admitidos

El valor de este parámetro especifica el tiempo durante el cual el CMTS DEBE retener los recursos para el conjunto de parámetros QoS admitido de un flujo de servicio mientras exceden los de su conjunto de parámetros QoS activo. Si no hay mensaje DSC-REQ para activar el conjunto de parámetros QoS admitido dentro de ese intervalo de tiempo, y no hay DSC para renovar los conjuntos de parámetros QoS y reiniciar la temporización (véase B.10.1.5.2), se DEBEN liberar los recursos que están admitidos pero no activados, y retenidos solamente los recursos activos. El CMTS DEBE fijar el conjunto de parámetros QoS admitido igual al conjunto de parámetros QoS activo para el flujo de servicio e iniciar un intercambio de mensajes DSC-REQ con el CM para informarle del cambio.

Tipo	Longitud	Valor
[24/25].13	2	Segundos

La aplicación de este parámetro DEBE imponerse en el CMTS y NO DEBERÍA imponerse en el CM. El parámetro es procesado por el CMTS para cada conjunto de QoS contenido en los mensajes de registro y los mensajes de servicio dinámico. Si el parámetro se omite, se supone el valor por defecto de 200 s. Un valor de 0 significa que el flujo de servicio puede permanecer en el estado admitido durante un período de tiempo infinito y NO se le DEBE fijar ningún límite temporal por inactividad. Esto está sujeto, no obstante, a las políticas de control del CMTS. El valor especificado para el conjunto de QoS activo debe ser menor o igual que el valor correspondiente en el conjunto de QoS admitido, el cual debe ser menor que igual que el valor correspondiente en el conjunto de QoS aprovisionado/autorizado. Si el valor pedido es demasiado grande, el CMTS PUEDE rechazar el mensaje o responder con un valor menor que el solicitado. Si el mensaje de registro o de servicio dinámico que contiene este parámetro es aceptado por el CMTS y el CM acusa recibo del mismo, el temporizador de la temporización de QoS admitido se carga con el nuevo valor de temporización. El temporizador es activado si el mensaje admite recursos mayores que los del conjunto activo. El temporizador es desactivado si el mensaje fija el conjunto de QoS activo y el conjunto de QoS admitido iguales el uno al otro.

B.C.2.2.5.9 Parámetros QoS específicos de vendedor

Esto permite a los vendedores codificar los parámetros QoS específicos de vendedor. El ID de vendedor DEBE ser la primera tupla TLV incorporada dentro de los parámetros QoS específicos de vendedor. Si la primera tupla TLV dentro de los parámetros QoS específicos de vendedor no es un ID de vendedor, esa tupla DEBE ser descartada. (Véase B.C.1.1.17.)

Tipo	Longitud	Valor
[24/25].43	n	B (octetos)

B.C.2.2.6 Codificaciones de parámetros QoS específicas del sentido ascendente

B.C.2.2.6.1 Ráfaga máxima concatenada

El valor de este parámetro especifica la ráfaga máxima concatenada (en octetos) permitida para un flujo de servicio. Este parámetro se calcula desde octeto FC del encabezamiento MAC de concatenación hasta la última CRC de la trama concatenada MAC.

Un valor de 0 significa que no hay límite. El valor por defecto es 0.

Este campo sólo es aplicable en el CM. Si está definido, este parámetro DEBE hacerse cumplir en el CM.

NOTA 1 – Este valor no incluye ninguna tara de capa física.

Tipo	Longitud	Valor
24.14	2	

NOTA 2 – Aplica solamente a las ráfagas concatenadas. Es legal y, de hecho, puede ser útil para fijarlo más pequeño que el tamaño máximo de paquete Ethernet. Por supuesto también es legal fijarlo igual a o mayor que el tamaño máximo de paquete Ethernet.

B.C.2.2.6.2 Tipo de programación de flujo de servicio

El valor de este parámetro especifica qué servicio de programación en sentido ascendente se utiliza para las peticiones de transmisión en sentido ascendente y las transmisiones de paquetes. Si este parámetro se omite, se DEBE suponer servicio de mejor esfuerzo.

Este parámetro sólo es aplicable en el CMTS. Si está definido, este parámetro DEBE hacerse cumplir por el CMTS.

Tipo	Longitud	Valor
24.15	1	0: reservado 1: para no definido (que depende de la implementación del CMTS) (véase la nota) 2: para mejor esfuerzo 3: para servicio de interrogación secuencial no en tiempo real 4: para servicio de interrogación secuencial en tiempo real 5: para servicio de concesión no solicitado con detección de actividad 6: para servicio de concesión no solicitada 7 a 255: se reservan para uso futuro

NOTA – El tipo específico de servicio de programación dependiente de la implementación podría ser definido en el campo información específica de vendedor 24.43.

B.C.2.2.6.3 Política de petición/transmisión

El valor de este parámetro especifica qué oportunidades IUC utiliza el CM para las peticiones de transmisión en sentido ascendente y para las transmisiones de paquetes para este flujo de servicio, si las peticiones para este flujo de servicio pueden ser porteadas con datos o si los paquetes de datos transmitidos en este flujo de servicio pueden ser concatenados o fragmentados o se les puede suprimir sus encabezamientos de cabida útil. Para UGS, también especifica cómo tratar los paquetes que no encajan dentro de la concesión UGS. Véanse en B.10.2 los requisitos relativos a las fijaciones de los bits de este parámetro para cada tipo de programación de flujo de servicio.

Este parámetro se requiere para todos los tipos de programación de flujo de servicio excepto el de mejor esfuerzo. Si se omite en un conjunto de parámetros QoS de flujo de servicio de mejor esfuerzo, se debe utilizar el valor por defecto de 0. El bit #0 es el LSB del campo valor. Los bits se fijan a 1 para seleccionar el comportamiento que se define a continuación:

Tipo	Longitud	Valor
24.16	4	Bit 0: El flujo de servicio NO DEBE utilizar las oportunidades de petición de difusión tipo "todos los CM" Bit 1: El flujo de servicio NO DEBE utilizar oportunidades de petición multidifusión de petición de privacidad (véase B.A.2.3). Bit 2: El flujo de servicio NO DEBE utilizar oportunidades de petición/datos para peticiones. Bit 3: El flujo de servicio NO DEBE utilizar oportunidades de petición/datos para datos. Bit 4: El flujo de servicio NO DEBE portear peticiones con datos. Bit 5: El flujo de servicio NO DEBE concatenar datos. Bit 6: El flujo de servicio NO DEBE fragmentar datos. Bit 7: El flujo de servicio NO DEBE suprimir encabezamientos de cabida útil. Bit 8: (Nota 1) El flujo de servicio DEBE suprimir paquetes que no encajan en el tamaño de la concesión no solicitada (nota 2). El resto de los bits están reservados.

NOTA 1 – Este bit solamente es aplicable a los flujos de servicio con el tipo de programación de flujo de servicio de concesión no solicitada. Si este bit se fija en cualquier otro tipo de programación de flujo de servicio DEBE ignorarse.

NOTA 2 – Los paquetes correspondientes a un flujo de servicio de concesión no solicitada y que son más grandes que el tamaño de la concesión asociada con ese flujo de servicio son transmitidos normalmente en el flujo de servicio primario. Este parámetro invalida ese comportamiento por defecto.

NOTA 3 – Las concesiones de datos incluyen tanto concesiones de datos cortas como concesiones de datos largas.

B.C.2.2.6.4 Intervalo de interrogación secuencial nominal

El valor de este parámetro especifica el intervalo nominal (en unidades de microsegundos) entre oportunidades sucesivas de petición de unidifusión para este flujo de servicio por el canal en sentido ascendente. Este es el parámetro típico del servicio de interrogación secuencial en tiempo real y no en tiempo real.

El programa ideal de aplicación impuesta de este parámetro se define mediante un tiempo o instante de referencia t_0, y unos tiempos o instantes de interrogación secuencial deseados, $t_i = t_0 + i \times$ interval. Los tiempos efectivos de interrogación, t'_i, DEBEN estar en la gama $t_i \leq t'_i \leq t_i +$ fluctuación de fase, siendo la fluctuación de fase el valor especificado con esta tupla TLV, e "interval" el intervalo de interrogación secuencial nominal. La exactitud de los tiempos ideales de interrogación, secuencial, t_i, se mide en relación con el reloj maestro del CMTS utilizado para generar las indicaciones de tiempo (véase B.9.3).

Este campo sólo es aplicable al CMTS. Si está definido, este parámetro DEBE hacerse cumplir por el CMTS.

Tipo	Longitud	Valor
24.17	4	µs

B.C.2.2.6.5 Fluctuación tolerada de la interrogación secuencial

Los valores en este parámetro especifican la cantidad máxima de tiempo que puede retardarse el intervalo de petición de unidifusión con respecto al programa nominal periódico (medido en microsegundos) para este flujo de servicio.

El programa ideal de aplicación impuesta de este parámetro está definido por un tiempo o instantes de referencia, t_0, y unos tiempos o instantes deseados de interrogación secuencial, $t_i = t_0 + i \times$ interval. Los tiempos efectivos de interrogación, t'_i DEBEN estar en la gama $t_i \leq t'_i \leq t_i +$ fluctuación de fase, siendo la fluctuación de fase el valor especificado con esta tupla TLV e "interval" el intervalo de la interrogación secuencial nominal. La exactitud de los tiempos ideales de interrogación secuencial, t_i, se mide en relación con el reloj maestro del CMTS utilizado para generar las indicaciones de tiempo (véase B.9.3).

Este parámetro sólo es aplicable al CMTS. Si está definido, este parámetro representa un compromiso de servicio (o criterio de admisión) en el CMTS.

Tipo	Longitud	Valor
24.17	4	µs

B.C.2.2.6.6 Tamaño de concesión no solicitada

El valor de este parámetro especifica el tamaño de la concesión no solicitada en octetos. El tamaño de la concesión incluye las PDU datos de trama MAC completa desde el octeto de control de trama hasta el final de la trama MAC.

Este parámetro es aplicable al CMTS y DEBE hacerse cumplir en el CMTS.

Tipo	Longitud	Valor
24.19	2	µs

NOTA – Para UGS, este parámetro debería ser utilizado por el CMTS para calcular el tamaño de la concesión no solicitada en miniintervalos de tiempo.

B.C.2.2.6.7 Intervalo de concesión nominal

El valor de este parámetro especifica el intervalo nominal (en unidades de microsegundos) entre oportunidades sucesivas de concesión de datos para este flujo de servicio. Este parámetro se requiere para flujos de servicio de concesión no solicitada y de concesión no solicitada con detección de actividad.

El programa ideal de aplicación impuesta de este parámetro está definido por un tiempo o instante de referencia, t_0, y unos tiempos o instantes deseados de transmisión, $t_i = t_0 + i \times$ interval. Los tiempos efectivos de concesión, t'_i DEBEN estar en la gama $t_i \leq t'_i \leq t_i +$ fluctuación de fase, siendo el intervalo el valor especificado con esta tupla TLV, y la fluctuación de fase la fluctuación de concesión tolerada. Cuando se pidan múltiples concesiones por intervalo, todas las concesiones DEBEN estar dentro de este intervalo, por lo que DEBEN ser mantenidos por el CMTS el intervalo de concesión nominal y la fluctuación de concesión tolerada para todas las concesiones en este flujo de servicio. La exactitud de los tiempos ideales de concesión, t_i, se miden con relación al reloj maestro del CMTS utilizado para generar las indicaciones de tiempo (véase B.9.3).

Este campo es obligatorio para tipos de programación de concesión no solicitada y de concesión no solicitada con detección de actividad. Este campo sólo es aplicable en el CMTS y DEBE hacerse cumplir por el CMTS.

Tipo	Logitud	Valor
24.20	4	µs

B.C.2.2.6.8 Inestabilidad de concesión tolerada

Los valores en este parámetro especifican la cantidad máxima de tiempo que pueden retardarse las oportunidades de transmisión con respecto al programa nominal periódico (medido en microsegundos) para este flujo de servicio.

El programa ideal para la aplicación impuesta de este parámetro está definido por un tiempo o instante de referencia, t_0, y unos tiempos o instantes de deseados transmisión, $t_i = t_0 + i \times$ interval. Las oportunidades efectivas de transmisión t'_i DEBEN estar en la gama $t_i \leq t'_i \leq t_i +$ fluctuación de fase, siendo la fluctuación de fase el valor especificado con esta tupla TLV e interval nominal de la concesión. La exactitud de los tiempos ideales de concesión, t_i, se mide en relación con el reloj maestro del CMTS utilizado para generar las indicaciones de tiempo (véase B.9.3).

Este campo es obligatorio par tipos de programación de concesión no solicitada y de concesión no solicitada con detección de actividad. Este campo sólo es aplicable en el CMTS, y DEBE hacerse cumplir por el CMTS.

Tipo	Longitud	Valor
24.21	4	µs

B.C.2.2.6.9 Concesiones por intervalo

Para el servicio de concesión no solicitada, el valor de este parámetro indica el número efectivo de las concesiones de datos por intervalo de concesión nominal. Para el servicio de concesión no solicitada con detección de actividad, el valor de este parámetro indica el número máximo de concesiones activas por nominal de concesión intervalo. Tiene por objeto hacer posible la adición de sesiones a un flujo de servicio de concesión no solicitada existente mediante el mecanismo de cambio de servicio dinámico, sin repercutir negativamente en las sesiones existentes.

El programa ideal de aplicación impuesta de este parámetro está definido por un tiempo o instante de referencia, t_0, y unos tiempos o instantes deseados de transmisión, $t_1 = t_0 + i \times$ interval. Los tiempos efectivos de concesión en, t'_i DEBEN estar en la gama $t_i \leq t'_i \leq t_i +$ fluctuación de fase, siendo interval el intervalo de concesión nominal, y la fluctuación de fase la fluctuación de concesión tolerada. Cuando se pidan múltiples concesiones por intervalo, todas las concesiones DEBEN estar dentro de este intervalo, por lo que deben ser mantenidos por el CMTS el intervalo de concesión nominal y la fluctuación de concesión tolerada para todas las concesiones en este flujo de servicio.

Este campo es obligatorio para tipos de programación de concesión no solicitada y de concesión no solicitada con detección de actividad. Este campo sólo es aplicable al CMTS, y DEBE hacerse cumplir por el CMTS.

Tipo	Longitud	Valor
24.22	1	# de concesiones

Gama válida

0-7 para pri-low y pri-high.

B.C.2.2.6.10 Tipo IP de sobreescritura de servicio

El CMTS DEBE sobreescribir los paquetes IP con el valor del octeto ToS de IP "orig-ip-tos" con el valor "new-ip-tos", donde new-ip-tos = ((orig-ip-tos AND tos-and-mask) OR tos-or-mask). Si este parámetro se omite, el octeto ToS del paquete IP no se sobreescribe.

Este parámetro sólo es aplicable al CMTS. Si está definido, este parámetro DEBE hacerse cumplir por el CMTS.

Tipo	Longitud	Valor
24.23	2	tos-and-mask, tos-or-mask

B.C.2.2.6.11 Referencia de tiempo de concesión no solicitada

Para el servicio de concesión no solicitada y para el servicio de concesión no solicitada con detección de actividad, el valor de este parámetro especifica un tiempo o instante de referencia t_0 a partir del cual pueden derivarse los tiempos o instantes deseados de transmisión $t_i = t_0 + i \times$ interval, siendo interval el intervalo de concesión nominal (véase B.C.2.2.6.7). Este parámetro es aplicable sólo para mensajes transmitidos del CMTS al CM, y únicamente cuando se activa un flujo de servicio UGS o UGS-AD. En tales casos, este parámetro es obligatorio.

Tipo	Longitud	Valor
24.24	4	Indicación de tiempo de CMTS

Gama válida

0-4 294 967 295

La indicación de tiempo especificada en este parámetro representa un estado de conteo del reloj maestro de 10,24 MHz del CMTS. Puesto que siempre se activa un flujo de servicio UGS o UGS-AD antes de la transmisión de este parámetro hacia el módem, el tiempo de referencia t_0 será interpretado por el módem como el tiempo ideal de la siguiente concesión sólo si t_0 se encuentra a continuación del tiempo actual. Si t_0 precede al tiempo actual, el módem puede calcular el desplazamiento del tiempo actual con respecto al tiempo ideal de la siguiente concesión de acuerdo con:

$$\text{Intervalo del módulo} = \frac{\text{tiempo actual} - t_0}{10{,}24}$$

donde: el intervalo se da en unidades de microsegundos, el tiempo actual y t_0 se dan en unidades de 10,24 MHz

B.C.2.2.7 Codificaciones de parámetros QoS específicas del sentido descendente

B.C.2.2.7.1 Latencia en sentido descendente máxima

El valor de este parámetro especifica la latencia máxima entre la recepción de un paquete por el CMTS en su NSI y el reenvío del paquete a su interfaz RF.

Si está definido, este parámetro representa un compromiso de servicio (o criterio de admisión) en el CMTS y DEBE ser garantizado por el CMTS. Un CMTS no tiene que cumplir con este compromiso de servicio para flujos de servicio que exceden su velocidad mínima reservada en sentido descendente.

Tipo	Longitud	Valor
25.14	4	µs

B.C.2.2.8 Supresión de encabezamiento de cabida útil

Este campo define los parámetros asociados con la supresión de encabezamiento de cabida útil.

Tipo	Longitud	Valor
26	n	

La tupla TLV completa de supresión de encabezamiento de cabida útil DEBE tener una longitud de menos de 255 caracteres.

B.C.2.2.8.1 Referencia de clasificador

El valor del campo especifica una referencia de clasificador que identifica el clasificador correspondiente. (Véase B.C.2.1.3.1.)

Tipo	Longitud	Valor
26.1	1	1-255

B.C.2.2.8.2 Identificador de clasificador

El valor del campo especifica un identificador de clasificador que identifica el clasificador correspondiente. (Véase B.C.2.1.3.2.)

Tipo	Longitud	Valor
26.2	2	1-65 535

B.C.2.2.8.3 Referencia de flujo de servicio

El valor del campo especifica una referencia de flujo de servicio que identifica el flujo de servicio correspondiente. (Véase B.C.2.2.3.1.)

Tipo	Longitud	Valor
26.3	2	1-65 535

B.C.2.2.8.4 Identificador de flujo de servicio

El valor de este campo especifica el identificador de flujo de servicio que identifica el flujo de servicio al que se aplica la regla PHS.

Tipo	Longitud	Valor
26.4	4	1-4 294 967 295

B.C.2.2.8.5 Acción de cambio de servicio dinámico

Cuando se recibe en una petición de cambio de servicio dinámico, este parámetro indica la acción que DEBE efectuarse con esta cadena de octetos de supresión de encabezamiento de cabida útil.

Tipo	Longitud	Valor
26.5	1	0: Añadir regla PHS 1: Fijar regla PHS 2: Suprimir regla PHS 3: Suprimir todas las reglas PHS

La instrucción "Fijar regla PHS" se utiliza para añadir tuplas TLV específicas a una regla parcialmente definida de supresión de encabezamiento de cabida útil. Una regla PHS está parcialmente definida cuando los valores PHSF y PHSS son ambos desconocidos. Una regla PHS queda plenamente definida cuando los valores PHSF y PHSS son ambos conocidos. Una vez que una regla PHS está totalmente definida, la instrucción "Fijar regla PHS" NO DEBE ser utilizado para modificar tuplas TLV existentes.

La instrucción "Suprimir todas las reglas PHS" se utiliza para suprimir todas las reglas PHS de un flujo de servicio especificado. Véase en B.8.3.15 los detalles sobre los parámetros PHS requeridos para el mensaje DSC-REQ cuando se utiliza esta opción.

NOTA – El intento de añadir una regla PHS que ya existe constituye una condición de error.

B.C.2.2.9 Codificaciones de error de supresión de encabezamiento de cabida útil

Este campo define los parámetros asociados con los errores de supresión de encabezamiento de cabida útil.

Tipo	Longitud	Valor
26.6	n	

Una codificación de error de supresión de encabezamiento de cabida útil consiste en un conjunto único de parámetros de error de supresión de encabezamiento de cabida útil que se define mediante los siguientes parámetros individuales: parámetro con error, código de confirmación y mensaje de error.

La codificación de error de supresión de encabezamiento de cabida útil se devuelve en los mensajes REG-RSP, DSA-RSP y DSC-RSP para indicar el motivo de la respuesta negativa de un receptor a la petición de establecimiento de una regla de supresión de encabezamiento de cabida útil en un mensaje REG-REQ, DSA-REQ o DSC-REQ.

En caso de fallo, los mensajes REG-RSP, DSA-RSP, o DSC-RSP DEBEN incluir una codificación de error de supresión de encabezamiento de cabida útil al menos para una regla fallida de supresión de encabezamiento de cabida útil pedida en los mensajes REG-REQ, DSA-REQ o DSC-REQ. Una codificación de error de supresión de encabezamiento de cabida útil para la regla fallida de supresión de encabezamiento de cabida útil DEBE incluir el código de confirmación y el parámetro con error y

PUEDE incluir un mensaje de error. Si algunos conjuntos de reglas de supresión de encabezamiento de cabida útil son rechazados pero otros conjuntos de reglas de supresión de encabezamiento de cabida útil son aceptados, las codificaciones de error de supresión de encabezamiento de cabida útil DEBEN incluirse solamente para las reglas de supresión de encabezamiento de cabida útil rechazadas. En caso de éxito de la transacción completa, el mensaje RSP o ACK NO DEBE incluir una codificación de error de supresión de encabezamiento de cabida útil.

Las codificaciones múltiples de error de supresión de encabezamiento de cabida útil PUEDEN aparecer en los mensajes REG-RSP, DSA-RSP o DSC-RSP, ya que múltiples parámetros de supresión de encabezamiento de cabida útil pueden tener errores. Un mensaje que incluso no tenga más que una sola codificación única de error de supresión de encabezamiento de cabida útil NO DEBE contener ningún otro protocolo de codificaciones de supresión de encabezamiento de cabida útil (por ejemplo IP, IEEE 802.1P/Q).

Las codificaciones de error de supresión de encabezamiento de cabida útil NO DEBEN aparecer en ningún mensaje REG-REQ, DSA-REQ o DSC-REQ.

B.C.2.2.9.1 Parámetro con error

El valor de este parámetro identifica el subtipo de un parámetro de supresión de encabezamiento de cabida útil solicitado con error en una petición de supresión de encabezamiento de cabida útil rechazada. Un conjunto de parámetros de error de supresión de encabezamiento de cabida útil DEBE tener exactamente una tupla TLV del parámetro con error dentro de una codificación de error de supresión de encabezamiento de cabida útil determinada.

Tipo	Longitud	Valor
26.6.1	1	Codificación de supresión de encabezamiento de cabida útil subtipo con error

B.C.2.2.9.2 Código de error

Este parámetro indica el estado de la petición. Un valor distinto de 0 corresponde al código de confirmación descrito en B.C.4. Un conjunto de parámetros de error de supresión de encabezamiento de cabida útil DEBE tener exactamente un código de error dentro de una codificación de error de supresión de encabezamiento de cabida útil determinada.

Tipo	Longitud	Valor
26.6.2	1	Código de confirmación

Un valor de okay (correcto) (0) indica que la petición de supresión de encabezamiento de cabida útil tuvo éxito. Puesto que un conjunto de parámetros de error de supresión de encabezamiento de cabida útil sólo es aplicable a los parámetros con error, este valor NO DEBE ser utilizado.

B.C.2.2.9.3 Mensaje de error

Este subtipo es opcional en un conjunto de parámetros de error de supresión de encabezamiento de cabida útil. Si está presente, indica una cadena de texto que se ha de presentar en la consola CM y/o en el fichero registro cronológico que describe con más detalle una petición de supresión de encabezamiento de cabida útil rechazada. Un conjunto de parámetros de error de supresión de encabezamiento de cabida útil PUEDE tener cero o uno subtipos de mensaje de error dentro de una codificación de error de supresión de encabezamiento de cabida útil determinada.

Tipo	Longitud	Valor
26.6.3	n	Cadena de caracteres ASCII terminada en cero

- La longitud n incluye el cero de terminación.
- El mensaje completo de codificación de supresión de encabezamiento de cabida útil DEBE tener una longitud total de menos de 256 caracteres.

B.C.2.2.10 Codificaciones de regla de supresión de encabezamiento de cabida útil

B.C.2.2.10.1 Campo supresión de encabezamiento de cabida útil (PHSF)

El valor de este campo son los octetos de los encabezamientos que DEBEN ser suprimidos por la entidad emisora, y DEBEN ser restablecidos por la entidad de recepción. En el sentido ascendente, el PHSF corresponde a la cadena de octetos de PDU empezando con el primer octeto después de la suma de control del encabezamiento MAC. En el sentido descendente, el PHSF corresponde a la cadena de octetos de PDU empezando con el decimotercer octeto después de la suma de control del encabezamiento MAC. Esta cadena de octetos incluye tanto los octetos suprimidos como los no suprimidos del encabezamiento de PDU. El valor de los octetos no suprimidos dentro del PHSF depende de la implementación.

El orden de los octetos en el campo valor de la cadena de tuplas TLV del PHSF DEBE seguir la secuencia:

Sentido ascendente
MSB del valor PHSF = 1er octeto de la PDU
2^{o} MSB del valor PHSF = 2^{o} octeto de la PDU
...
n-ésimo octeto del PHSF (LSB del valor PHSF) = n-ésimo octeto de la PDU

Sentido descendente:

MSB del valor PHSF = 13^{o} octeto de la PDU
2^{o} MSB del valor PHSF = 14^{o} octeto de la PDU
...
n-ésimo octeto del PHSF (LSB del valor PHSF) = (n+13) ésimo octeto de la PDU

Tipo	Longitud	Valor
26.7	n	Cadena de octetos suprimidos

La longitud n DEBE ser siempre la misma que el valor para PHSS.

B.C.2.2.10.2 Índice de supresión de encabezamiento de cabida útil (PHSI)

El índice de supresión de encabezamiento de cabida útil (PHSI) tiene un valor entre 1 y 255 que hace referencia de forma exclusiva a la cadena de octetos suprimidos. El índice es único por flujo de servicio en sentido ascendente y único por CM en sentido descendente. Los valores de PHSI en sentido ascendente y sentido descendente son independientes entre sí.

Tipo	Longitud	Valor
26.8	1	Valor de índice

B.C.2.2.10.3 Plantilla de supresión de encabezamiento de cabida útil (PHSM, *payload header suppression mark*)

El valor de este campo se utiliza para interpretar los valores del campo supresión de encabezamiento de cabida útil. Se utiliza tanto en las entidades de envío como de recepción por el enlace. El PHSM

permite que campos tales como de los números de secuencia o sumas de control cuyo valor varía se excluyan de la supresión aunque se suprimen los octetos constantes en torno a ellos.

Tipo	Longitud	Valor
26.9	n	bit 0: 0 = no suprimir el primer octeto del campo supresión 1 = suprimir el primer octeto del campo supresión bit 1: 0 = no suprimir el segundo octeto del campo supresión 1 = suprimir el segundo octeto del campo supresión bit x: 0 = no suprimir el octeto (x+1) del campo supresión 1 = suprimir el octeto (x+1) del campo supresión

La longitud n representa el techo (PHSS/8). El bit 0 es el MSB del campo valor. El valor de cada bit secuencial del PHSM es un atributo del octeto secuencial correspondiente del PHSF.

Si el valor del bit es un "1" (y pasa la verificación o es inhabilitado), la entidad de envío DEBE suprimir el octeto, y la entidad de recepción DEBE restablecer el octeto a partir de su PHSF guardado en memoria. Si el valor bit es un "0", la entidad de envío NO DEBE suprimir el octeto, y la entidad de recepción DEBE restablecer el octeto utilizando el octeto siguiente del paquete.

Si esta tupla TLV no está incluida, la acción por defecto es suprimir todos los octetos.

B.C.2.2.10.4 Tamaño de supresión de encabezamiento de cabida útil (PHSS, *payload header suppression size*)

El valor de este campo es el número total de octetos del campo de supresión de encabezamiento de cabida útil (PHSF) para un flujo de servicio que utiliza supresión de encabezamiento de cabida útil.

Tipo	Longitud	Valor
26.10	1	Número de octetos de la cadena de supresión

Esta tupla TLV se utiliza cuando se está creando un flujo de servicio. Para todos los paquetes que se clasifican y asignan a un flujo de servicio con supresión de encabezamiento de cabida útil habilitada, la supresión DEBE efectuarse en el número especificado de octetos conforme indica el PHSS y de acuerdo al PHSM. Si esta tupla TLV está incluida en una definición de flujo de servicio con un valor de 0 octetos, se inhabilita la supresión de encabezamiento de cabida útil. Un valor diferente de cero indica que la supresión de encabezamiento de cabida útil está habilitada. Mientras no se conozca el valor de PHSS, la regla PHS se considera parcialmente definida, y la supresión no será efectuada. Una regla PHS queda plenamente definida cuando los valores PHSS y PHSF son ambos conocidos.

B.C.2.2.10.5 Verificación de la supresión de encabezamiento de cabida útil (PHSV, *payload header suppression verification*)

El valor de este campo indica a la entidad de envío si los contenidos del encabezamiento del paquete tienen que ser verificados o no antes de ejecutar la supresión. Si se habilita el PHSV, el transmisor DEBE comparar los octetos del encabezamiento del paquete con los octetos en el PHSF que van a ser suprimidos conforme lo indique el PHSM.

Tipo	Longitud	Valor
26.11	1	0: verificar 1: no verificar

Si esta tupla TLV no está incluida, el valor por defecto es verificar. Solamente el emisor DEBE verificar los octetos suprimidos. Si la verificación falla, el encabezamiento de cabida útil NO DEBE ser suprimido. (Véase B.10.4.3.)

B.C.2.2.10.6 Parámetros PHS específicos de vendedor

Estos parámetros permiten a los vendedores codificar los parámetros PHS específicos del vendedor. El ID de vendedor DEBE ser la primera tupla TLV incorporada dentro de los parámetros PHS específicos del vendedor. Si la primera tupla TLV dentro de los parámetros PHS específicos del vendedor no es un ID de vendedor, la tupla TLV DEBE ser descartada. (Véase B.C.1.1.17.)

Tipo	Longitud	Valor
26.420	n	

B.C.3 Codificaciones para otras interfaces

B.C.3.1 Opción de fijación telefónica

Esta fijación de configuración describe los parámetros que son específicos de los sistemas de retorno telefónico. Está compuesta de varios campos tipo/longitud/valor encapsulados. Véase [DOCSIS6].

Tipo	Longitud	Valor
15 (=TRI_CFG01)	n	

B.C.3.2 Opción de fijación de configuración privacidad básica

Esta fijación de configuración describe los parámetros que son específicos de la privacidad básica. Está compuesta de varios campos tipo/longitud/valor encapsulados. Véase [DOCSIS8].

Tipo	Longitud	Valor
17 (= BP_CFG)	n	

B.C.4 Código de confirmación

El código de confirmación (CC) proporciona un modo común de indicar los fallos en los mensajes de gestión MAC respuesta de registro, acuse de recibo de registro, respuesta de adición de servicio dinámica, acuse de recibo de adición de servicio dinámica, respuesta de supresión de servicio dinámica, de respuesta cambio de servicio dinámica y acuse de recibo de cambio de servicio dinámico. Los códigos de confirmación de esta cláusula son utilizados como códigos de confirmación de mensajes y como códigos de error en codificaciones de conjuntos de errores que pueden ser transportados en estos mensajes.

El código de confirmación es uno de los siguientes:

- okay/éxito(0);
- rechazo por otros motivos(1);
- rechazo-fijación-configuración-no reconocida(2);
- rechazo-temporal/rechazo-recurso(3);
- rechazo-permanente/rechazo-administrativo(4);
- rechazo-no-propietario(5);
- rechazo-flujo-servicio-no-encontrado(6);
- rechazo-flujo-servicio-existe(7);

– rechazo-parámetro-requerido-no-presente(8);
– rechazo-supresión-encabezamiento(9);
– rechazo-ID-transacción-desconocido(10);
– rechazo-fallo-autenticación(11);
– rechazo-adición-abortada(12);
– rechazo-múltiples-errores(13);
– rechazo-clasificador-no-encontrado(14);
– rechazo-clasificador-existe(15);
– rechazo-regla-PHS-no-encontrada(16);
– rechazo-regla-PHS-existe(17);
– rechazo-ID-referencia-duplicado-o-índice-en-mensaje(18);
– rechazo-múltiples-flujos-servicio-sentido-ascendente(19);
– rechazo-múltiples-flujos-servicio-sentido-descendente(20);
– rechazo-clasificador-para-otro-flujo-servicio(21);
– rechazo-PHS-para-otro-flujo-servicio(22);
– rechazo-parámetro-no-válido-para-contexto(23);
– rechazo-fallo-autorización(24);
– rechazo-temporal-DCC(25).

Los códigos de confirmación DEBEN ser utilizados de la siguiente manera:

- Okay o éxito(0) significa que el mensaje fue recibido con éxito.
- Rechazo-otros(1) se utilizan cuando no es aplicable ninguno de los otros códigos de motivo.
- Rechazo-fijación-configuración-no reconocida(2) se utiliza cuando una fijación de configuración no se reconoce o cuando su valor está fuera de la gama especificada.
- Rechazo-temporal(3), también conocido como rechazo-recurso, indica que la carga actual del CMTS o del CM impide la concesión de la petición, pero que la petición podría tener éxito en algún otro momento.
- Rechazo-permanente(4), también conocido como rechazo-administrativo, indica que, por motivos de política, configuración, o capacidades, la petición nunca sería concedida a menos de que el CMTS o el CM fueran reconfigurados manualmente o reemplazados.
- Rechazo-no-propietario(5) indica que el solicitante no está asociado con este flujo de servicio.
- Rechazo-flujo-servicio-no-encontrado(6) significa que el flujo de servicio indicado en la petición no existe.
- Rechazo-flujo-servicio-existe(7) indica que el flujo de servicio que se va a adicionar ya existe.
- Rechazo-parámetro-requerido-no-presente(8) indica que se ha omitido un parámetro requerido.
- Rechazo-supresión-encabezamiento(9) indica que la supresión de encabezamiento pedida no puede ser sustentada por algún motivo.
- Rechazo-id-transacción-desconocido(10) indica que la continuación de la transacción pedida no es válida porque el punto extremo de recepción no ve la transacción como "en proceso" (es decir, el mensaje es inesperado o está fuera de orden).

- Rechazo-fallo-autenticación(11) indica que la transacción pedida fue rechazada porque el mensaje contenía un compendio HMAC no válido.
- Rechazo-adición-abortada(12) indica que la adición de un flujo de servicio dinámico fue abortada por el iniciador de la adición del servicio dinámico.
- Rechazo múltiples-errores(13) se utiliza cuando se han detectado múltiples errores.
- Rechazo-clasificador-no-encontrado(14) se utiliza cuando la petición contiene un ID de clasificador no reconocido.
- Rechazo-clasificador-existe(15) indica que el ID de un clasificador que se va a añadir ya existe.
- Rechazo-regla-PHS-no-encontrada(16) indica que la petición contiene un par SFID/ID de clasificador para el que no existe una regla PHS.
- Rechazo-regla-PHS-existe(17) indica que la petición de añadir una regla PHS contiene un par SFID/ID de clasificador para el que ya existe una regla PHS.
- Rechazo-ID-referencia-duplicado-o-índice-en-mensaje(18) indica que la petición utilizó una SFR, una referencia de clasificador, un SFID, o un ID de clasificador dos veces de forma ilegal.
- Rechazo-múltiples-flujos-servicio-sentido-ascendente(19) se utiliza cuando una DSA/DSC contiene parámetros para más de un flujo en sentido ascendente.
- Rechazo-múltiples-flujos-servicio-sentido-descendente(20) se utiliza cuando un DSA/DSC contiene parámetros para más de un flujo en sentido descendente.
- Rechazo-clasificador-para-otro-flujo-servicio(21) se utiliza en un mensaje DSA-RSP cuando el mensaje DSA-REQ incluye parámetros de clasificador para un SF diferente del nuevo o los nuevos SF que van a ser añadidos por la DSA.
- Rechazo-PHS-para-otro-flujo-servicio(22) se utiliza en el mensaje DSA-RSP cuando el mensaje DSA-REQ incluye una regla PHS para un SF diferente del nuevo o los nuevos SF que van a ser añadidos por el DSA.
- Rechazo-parámetro-no-válido-para-contexto(23) indica que el parámetro suministrado no puede ser utilizado en la codificación en la que se incluyó, o que el valor de un parámetro no es válido para la codificación en la que fue incluido.
- Rechazo-fallo-autorización(24) indica que la transacción pedida fue rechazada por el módulo de autorización.
- Rechazo-temporal-DCC(25) indica que los recursos pedidos no están disponibles en los canales actuales en ese momento, y que el CM debería volver a pedirlos por nuevos canales después de completar un cambio de canal en respuesta a una instrucción DCC que enviará el CMTS. Si no se recibe DCC, el CM debe esperar durante un tiempo de al menos T14 antes de volver a pedir los recursos por los canales actuales.

B.C.4.1 Códigos de confirmación para cambio de canal dinámico

El CM puede devolver en el mensaje DCC-RSP un código de rechazo apropiado de B.C.1.3.1. Puede también devolver uno de los siguientes códigos de confirmación que son exclusivos del mensaje DCC-RSP.

- Salida (180).
- Llegada (181).
- Rechazo-ya-allí (182).

Los códigos de confirmación DEBEN ser utilizados de la siguiente manera:

- Salida (180) indica que el CM se halla en el canal antiguo y que está próximo a saltar al nuevo canal.

- Llegada (181) indica que el CM ha efectuado el salto y ha llegado al nuevo canal.
- Rechazo-ya-allí (182) indica que el CMTS ha pedido al CM que se desplace a un canal que ya está ocupado.

B.C.4.2 Códigos de confirmación para errores importantes

Estos códigos de confirmación DEBEN ser utilizados solamente como códigos de confirmación de mensaje en los mensajes REG-ACK, DSA-RSP, DSA-ACK, DSC-RSP, o DSC-ACK, o como el código de respuesta en los mensajes REG-RSP para CM 1.1. En general, los errores asociados con estos códigos de confirmación hacen imposible generar un conjunto de errores que pueda ser asociado de forma única con un conjunto de parámetros en los mensajes REG-REQ, DSA-REQ, o DSC-REQ, o bien generar un mensaje RSP completo.

– rechazo-error-flujo-servicio-importante(200);
– rechazo-error-clasificador-importante(201);
– rechazo-error-regla-PHS-importante(202);
– rechazo-múltiples-errores-importante(203);
– rechazo-mensaje-error-sintaxis(204);
– rechazo-error -flujo-servicio-primario(205);
– rechazo-mensaje-demasiado-grande(206);
– rechazo-capacidades-módem-no-válidas (207).

Los códigos de confirmación DEBEN ser utilizados de la siguiente manera:

- Rechazo-error-flujo-servicio-importante(200) indica que el mensaje REQ no tenía una SFR o un SFID en una codificación de flujo de servicio, y que los errores importantes del flujo de servicio eran los únicos errores importantes.
- Rechazo-error-clasificador-importante(201) indica que el mensaje REQ no tenía una referencia de clasificación, o no tenía ni un ID de clasificador ni un ID de flujo de servicio, y que los errores importantes del clasificador eran los únicos errores importantes.
- Rechazo-error-regla-PHS-importante(202) indica que el mensaje REQ no tenía una referencia/un identificador de flujo de servicio ni una referencia/un identificador de clasificador, y que los errores importantes de la regla PHS eran los únicos errores importantes.
- Rechazo-múltiples-errores-importantes(203) indica que el mensaje REQ contenía múltiples errores importantes de los tipos 200, 201 y 202.
- Rechazo-mensaje-error-sintaxis(204) indica que el mensaje REQ contenía error o errores de sintaxis (por ejemplo, un error de longitud de la tupla TLV) con el resultado de fallo del análisis sintáctico.
- Rechazo-error-flujo-servicio-primario(205) indica que un mensaje REG-REQ o REG-RSP no definió un flujo de servicio primario requerido, o que un flujo de servicio primario requerido no fue especificado como activo.
- Rechazo-mensaje-demasiado-grande(206) se utiliza cuando la longitud del mensaje que se necesita para responder excede el tamaño de mensaje permitido máximo.
- Rechazo-capacidades-módem-no-válidas(207) indica que el mensaje REG-REQ contenía una combinación no válida de capacidades de módem o capacidades de módem incoherentes con los servicios del mensaje REG-REQ.

ANEXO B.D

Especificación de la interfaz de configuración de CM

B.D.1 Direccionamiento IP de CM

B.D.1.1 Campos DHCP utilizados por el CM

En la petición DHCP desde el CM DEBEN estar presentes los campos siguientes y DEBEN fijarse como se describe a continuación:

- El tipo de soporte físico (htype, *hardware type*) que DEBE fijarse a 1 (Ethernet).
- La longitud del soporte físico (hlen, *hardware length*) que DEBE fijarse a 6.
- La dirección de soporte físico del cliente (chaddr) que DEBE fijarse en la dirección MAC de 48 bits asociada con la interfaz RF del CM.
- DEBE incluirse la opción "identificador de cliente", con el tipo de soporte físico fijado a 1, y el valor fijado a la misma dirección MAC de 48 bits que el campo chaddr.
- El código de opción 60 (identificador de clase de vendedor) – Para hacer posible la diferenciación entre peticiones CM de DOCSIS 1.1 y DOCSIS 1.0, un CM conforme DEBE enviar la siguiente cadena codificada ASCII en el código de opción 60: "docsis 1.1: xxxxxxx", donde xxxxx DEBE ser una representación ASCII de la codificación hexadecimal de las capacidades del módem (véase B.C.1.3.1). Por ejemplo, la codificación ASCII de los dos primeros formatos TLV (concatenación y versión de DOCSIS) de un módem DOCSIS 1.1 sería 05nn010101020101. Se señala que para un módem DOCSIS 1.1 se necesitan muchos más formatos TLV y que el campo "nn" contendrá la longitud de todos los TLV. En este ejemplo se muestran sólo dos formatos TLV para simplificar.
- DEBE incluirse la opción "lista de petición de parámetros". Los códigos de opción que DEBEN estar incluidos en la lista son:
  - Código de opción 1 (máscara de subred).
  - Código de opción 2 (desplazamiento de tiempo).
  - Código de opción 3 (opción encaminador).
  - Código de opción 4 (opción servidor de tiempo).
  - Código de opción 7 (opción servidor de registro cronológico).

En la respuesta DHCP devuelta al CM se prevé que estén presentes los campos siguientes. El CM DEBE configurarse a sí mismo en base a la respuesta DHCP.

- La dirección IP que será utilizada por el CM (yiaddr).
- La dirección IP del servidor TFTP a utilizar en la fase siguiente del proceso de instrucciones preliminares (siaddr).
- Si el servidor DHCP está en una red diferente (que requiere un agente de relevo), la dirección IP del agente de relevo (giaddr).

  NOTA – Esta dirección puede diferir de la dirección IP del encaminador del primer tramo.
- El nombre del fichero de configuración de CM que el CM leerá desde el servidor TFTP (fichero).
- La máscara de subred que será utilizada por el CM (máscara de subred, opción 1).
- El desplazamiento de tiempo del CM con respecto al tiempo universal codificado (UTC, *universal coordinated time*) (desplazamiento de tiempo, opción 2). El CM de empleo para calcular la hora local utilizada en los registros cronológicos de errores de indicación de tiempo.
- Una lista de las direcciones de uno o más encaminadores que serán utilizadas para reenviar el tráfico IP originado por el CM (opción encaminador, opción 3). No es preciso que el CM

utilice más de una dirección IP de encaminador para el reenvío pero al menos DEBE utilizar una.

- Una lista de los servidores de tiempo [RFC 868] de los que se puede obtener la hora corriente (opción servidor de tiempo, opción 4).
- Una lista de los servidores SYSLOG a los que se puede enviar información de registro cronológico (opción servidor de registro cronológico, opción 7); véase [DOCSIS5].

Para ayudar al servidor DHCP a diferenciar entre una petición de descubrimiento de CM y una petición de descubrimiento de LAN del lado CPE, un CMTS DEBE efectuar lo siguiente:

- El CMTS DEBE insertar la opción de información del agente de relevo DHCP, código de opción 82, en la petición de descubrimiento antes de reenviar el descubrimiento a un servidor DHCP. De manera específica, el CMTS DEBE incluir la dirección MAC de 48 bits de la interfaz del lado RF del CM generando o puenteando la petición de descubrimiento del DHCP en el campo subopción del ID distante del agente, código de subopción 2. El código de opción 82 DEBE ser formateado como sigue: 82 08 02 06 xx xx xx xx xx xx, donde "xx xx xx xx xx xx" se refieren a la dirección MAC lado RF del CM. La opción información de agente de relevo DHCP se describe con más detalle en [61].
- Si el CMTS es un encaminador, DEBE utilizar un campo giaddr para diferenciar entre CM y estación del lado CPE si se provisionan de modo que se hallen en subredes IP diferentes. El punteo de los CMTS DEBERÍA proporcionar también esta funcionalidad.
- Todos los CMTS DEBEN soportar la opción información de agente de relevo DHCP, [RFC 3046]. De manera específica, el CMTS DEBE incluir la dirección MAC de 48 bits de la interfaz del lado RF del CM generando o puenteando la petición de descubrimiento DHCP en el campo subopción del ID distante del agente antes de reenviar el descubrimiento a un servidor DHCP.
- Si el CMTS es un encaminador, DEBE utilizar un campo giaddr para diferenciar entre CM y estación del lado CPE si se aprovisionan de modo que se hallen en subredes IP diferentes. Los CMTS DEBERÍAN proporcionar también esta funcionalidad.

B.D.2 Configuración de CM

B.D.2.1 Formato de fichero de configuración binaria CM

Los datos de configuración específicos en CM DEBE estar contenidos en un fichero que es telecargado al CM por medio del TFTP. Se trata de un fichero binario con el mismo formato que el definido para datos de extensión de vendedor de DHCP [RFC 2132].

DEBE constar de un cierto números de fijaciones de configuración (1 por parámetro), cada una de ellas de la forma:

Tipo Longitud Valor

donde:

tipo es un identificador de octeto simple que define el parámetro;

longitud es un octeto simple que contiene la longitud del campo valor en octetos (no incluido los campos tipo y longitud); y

valor está comprendido entre 1 y 254 octetos que contienen el valor específico del parámetro.

Las fijaciones de configuración DEBEN figurar en el fichero directamente una a continuación de otra, constituyendo así un tren de octetos (sin marcadores de registro).

La fijaciones de configuración se dividen en tres tipos:

- fijaciones de configuración normalizadas que DEBEN estar presentes;

- fijaciones de configuración normalizadas que PUEDEN estar presentes;
- fijaciones de configuración específicas del vendedor.

Los CM DEBEN poder procesar todas las fijaciones de configuración normalizadas. Los CM DEBEN ignorar cualquier fijación de configuración presente en el fichero de configuración que no puedan interpretar. Para hacer posible una gestión uniforme de los CM que se atienen al presente anexo B, los CM conformes DEBEN soportar como mínimo un fichero de configuración de 8192 octetos.

La autenticación de la información de aprovisionamiento es suministrada por dos fijaciones de configuración verificación de integridad de mensaje (MIC), MIC de CM y MIC de CMTS.

- MIC de CM es un compendio que asegura que los datos enviados por el servidor de aprovisionamiento no se ha modificado en ruta. NO es un compendio autenticado (no incluye ningún secreto compartido).
- MIC de CMTS es un compendio utilizado para autenticar el servidor de aprovisionamiento al CMTS durante la operación de registro. Se toma de un número de campos uno de los cuales es un secreto compartido entre el CMTS y el servidor de aprovisionamiento.

La utilización de la MIC de CM permite al CMTS autenticar los datos de aprovisionamiento sin necesidad de recibir el fichero entero.

La estructura de fichero tiene por tanto, la forma que se muestra en la figura B.D-1:

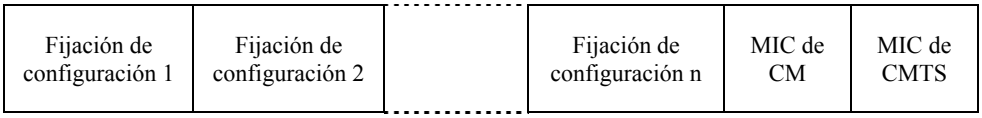


Figura B.D-1/J.112 – Formato de fichero de configuración binaria

B.D.2.2 Fijaciones de ficheros de configuración

Las siguientes fijaciones de configuración DEBEN estar incluidas en el fichero de la configuración y DEBEN ser soportadas por todos los CM. El CM NO DEBE enviar un mensaje REG-REQ basado en un fichero de configuración que carezca de los elementos obligatorios siguientes:

- Fijación de configuración acceso a la red.
- Fijación de configuración MIC de CM.
- Fijación de configuración MIC de CMTS.
- Fijación de configuración extremo.
- Fijación de configuración clase de servicio DOCSIS 1.0.

  NOTA – A un CM DOCSIS 1.0 se le debe proporcionar una configuración clase de servicio de DOCSIS 1.0. Un CM que se atenga al presente anexo B sólo se DEBERÍA aprovisionar con información de configuración clase de servicio de DOCSIS 1.0 si se ha de comportar como un CM de DOCSIS 1.0; de no ser así, se DEBE aprovisionar con fijaciones de configuración flujo de servicio.

o

- Fijación de configuración flujo de servicio en sentido ascendente.
- Fijación de configuración flujo de servicio en sentido descendente.

Las siguientes fijaciones de configuración PUEDEN estar incluidas en el fichero de la configuración y, si están presentes, DEBEN ser soportadas por todos los CM:

- Fijación de configuración frecuencias en sentido descendente.

- Fijación de configuración ID de canal en sentido ascendente.
- Fijación de configuración privacidad básica.
- Fijación de configuración nombre de fichero de mejora de soporte lógico.
- Fijación de clasificación de paquetes en sentido ascendente.
- Fijación de clasificación de paquetes en sentido descendente.
- Control de acceso a la escritura del SNMP.
- Objeto MIB del SNMP.
- Dirección IP del servidor del soporte lógico.
- Dirección MAC Ethernet del CPE.
- Número máximo de CPE.
- Número máximo de clasificadores.
- Fijación de configuración habilitación de privacidad.
- Supresión de encabezamiento de cabida útil.
- Indicación de tiempo de servidor TFTP.
- Dirección de módem suministrada por el servidor TFTP.
- Fijación de configuración relleno.

La siguiente configuración PUEDE estar incluida en el fichero de la configuración y, si está presente y es aplicable a este tipo de módem, DEBE ser reportada.

- Opción de fijaciones de telefonía.

La siguiente fijación de configuración PUEDE estar incluida en el fichero de la configuración y, si está presente, PUEDE ser soportada por CM.

- Fijación de configuración específica del vendedor.

Hay un límite al tamaño de las tramas de petición de registro y respuesta de registro (véase B.8.2.5.2). El fichero de la configuración no debe ser tan grande como para requerir que el CM o el CMTS excedan ese límite.

B.D.2.3 Creación de fichero de configuración

En las figuras B.D-2 a B.D-5 se muestra la secuencia de operaciones necesaria para la creación del fichero de la configuración.

1) Creación de las entradas tipo/longitud/valor (TLV) de todos los parámetros requeridos por el CM.

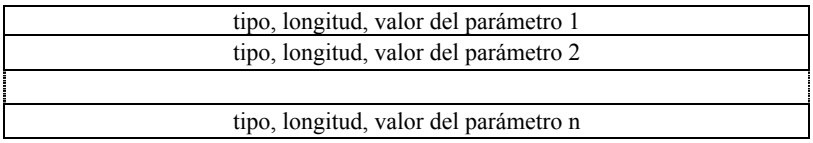


Figura B.D-2/J.112 – Creación de las entradas TLV de los parámetros requeridos por el CM

2) Cálculo de la fijación de la configuración verificación de integridad de mensaje (MIC) de CM como se define en B.D.2.3.1 y adición al fichero tras el último parámetro utilizando los valores de código y longitud definidos para este campo.

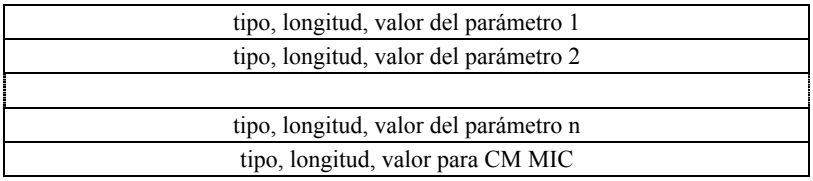


Figura B.D-3/J.112 – Adición de MIC de CM

3) Cálculo de la fijación de la configuración verificación de integridad de mensaje (MIC) de CMTS como se define en B.D.3.1 y adición de la misma al fichero tras la MIC de CM utilizando los valores de código y longitud definidos para este campo.

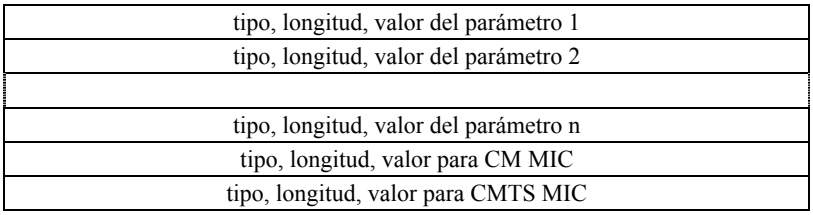


Figura B.D-4/J.112 – Adición de MIC de CMTS

4) Adición del marcador fin de datos.

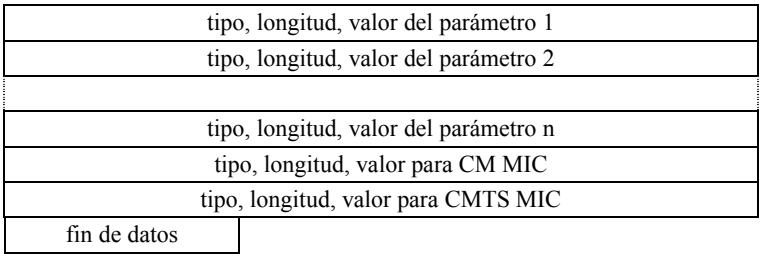


Figura B.D-5/J.112 – Adición de fin de datos

B.D.2.3.1 Cálculo de MIC de CM

La fijación de la configuración verificación de integridad de mensaje de CM se DEBE calcular obteniendo un compendio MD5 en los bytes de los campos fijación de configuración. Se calcula en los bytes de esas fijaciones tal como aparecen en la imagen TFTPed sin prestar atención al orden de TLV o al contenido. Hay dos excepciones a esa ignorancia deliberada del contenido:

1) Los bytes de TLV del propio MIC del CM se excluyen del cálculo. Se trata de los campos de tipo, longitud y valor.
2) Los bytes de TLV del MIC del CMTS se excluyen del cálculo. Se trata de los campos de tipo, longitud y valor.

Al recibir un fichero de configuración, el CM DEBE volver a calcular el compendio y compararlo con la fijación de configuración MIC de CM del fichero. Si los compendios no concuerdan, el fichero de la configuración DEBE ser descartado.

B.D.3 Verificación de la configuración

Es necesario verificar que el fichero de la configuración del CM procede de una fuente fiable. El CMTS y el servidor de la configuración comparten, por tanto, una cadena de autenticación que utilizan para verificar tramos de la configuración del CM en la petición de registro.

B.D.3.1 Cálculo de MIC de CMTS

La fijación de la configuración verificación de integridad de mensaje de CMTS se DEBE calcular obteniendo un compendio MD5 de los siguientes campos fijación de configuración, cuando están presentes en el fichero de la configuración, en el orden indicado.

- Fijación de configuración frecuencia en sentido descendente.
- Fijación de configuración ID de canal en sentido ascendente.
- Fijación de configuración acceso a la red.
- Fijación de configuración clase de servicio DOCSIS 1.0.
- Fijación de configuración ID de vendedor.
- Fijación de configuración privacidad básica.
- Fijación de configuración específica del vendedor.
- Fijación de configuración MIC de CM.
- Número máximo de CPE.
- Indicación de tiempo de servidor TFTP.
- Fijación de clasificación de paquetes en sentido ascendente.
- Fijación de clasificación de paquetes en sentido descendente.
- Fijación de configuración flujo de servicio en sentido ascendente.
- Fijación de configuración flujo de servicio en sentido descendente.
- Número máximo de clasificadores.
- Fijación de configuración habilitación de privacidad.
- Supresión de encabezamiento de cabida útil.
- Control de gestión de abonado.
- Cuadro IP de CPE de gestión de abonado.
- Grupos de filtro de gestión de abonado.

La lista anterior especifica el orden de las operaciones cuando se calcula el MIC de CMTS en los campos del tipo de fijación de la configuración. El CMTS DEBE calcular el MIC de CMTS en los formatos TLV del mismo tipo en el orden en que fueron recibidos. Dentro de los campos de tipo, el CMTS DEBE calcular el MIC de CMTS de los subtipos en el orden en que fueron recibidos. Para facilitar el cálculo correcto del MIC de CMTS por parte del CMTS, el CM NO DEBE reordenar los formatos TLV del fichero de la configuración del mismo tipo o los mismos subtipos de cualquier tipo dado en este mensaje de petición de registro.

Todos los campos fijación de configuración se DEBEN tratar como si fueran datos contiguos cuando se calcula el MIC de CM.

El compendio se DEBE añadir al fichero de la configuración como su propio campo fijación de configuración utilizando la codificación de configuración MIC de CMTS.

La cadena de autenticación es un secreto compartido entre el servidor de aprovisionamiento (que crea los ficheros de la configuración) y el CMTS. Permite al CMTS autenticar el aprovisionamiento del CM. La cadena de autenticación se ha de utilizar como la clave para el cálculo del compendio MIC de CMTS con clave que se indica en B.D.3.1.1.

El mecanismo de gestión del secreto compartido depende del operador del sistema.

Al recibir un fichero de configuración, el CM DEBE volver a enviar la MIC del CMTS como parte de la petición de registro (REG-REQ).

Al recibir un mensaje REG-REQ, el CMTS DEBE volver a calcular el compendio de los campos incluidos y la cadena de autenticación y compararlo con la fijación de configuración MIC de CMTS del fichero. Si los compendios no concuerdan, la petición de registro debe ser rechazada fijando el resultado fallo de la autenticación en el campo situación de la respuesta de registro.

B.D.3.1.1 Cálculo del compendio

El campo compendio MIC de CMTS DEBE calcularse utilizando el mecanismo HMAC-MD5 definido en [RFC 2104].

ANEXO B.E

Definición del servicio MAC

Este anexo B.E es de carácter informativo. Si hubiera alguna discrepancia entre el presente anexo y cualquier cláusula normativa del anexo B, la cláusula normativa tiene precedencia.

B.E.1 Visión general del servicio MAC

El MAC DOCSIS proporciona una interfaz de servicio protocolo a los servicios de capa superior. Ejemplos de servicios de capa superior son el puente DOCSIS, las aplicaciones incorporadas (por ejemplo, Packetcable/VOIP), una interfaz de ordenador principal (por ejemplo, un adaptador de NIC con gestor de NIDS) y encaminadores de capa 3 (por ejemplo, un encaminador IP).

La interfaz del servicio MAC define la estratificación por capas funcional entre el servicio de capa superior y el MAC. Define por tanto la funcionalidad del MAC proporcionado por los protocolos MAC subyacentes. Esta interfaz es una interfaz de protocolo, no una interfaz específica de la implementación.

La interfaz del servicio MAC proporciona los servicios de datos siguientes:

- un servicio MAC para la clasificación y transmisión de paquetes a flujos de servicio MAC;
- un servicio MAC para la recepción de paquetes procedentes de los flujos de servicio MAC. Los paquetes PUEDEN ser recibidos con los encabezamientos suprimidos;
- un servicio MAC para la transmisión y recepción de paquetes con los encabezamientos suprimidos. Los encabezamientos de los paquetes transmitidos se suprimen en base a las reglas de clasificadores concordantes. Los encabezamientos de los paquetes recibidos suprimidos se regeneran en base a un índice de encabezamiento de paquetes negociado entre el CM y el CMTS;
- un servicio MAC para la sincronización de la temporización de la concesión entre el MAC y el servicio de capa superior. Esta sincronización de reloj se necesita para aplicaciones tales como clientes Packetcable VOIP incorporados en las que el periodo de paquetización ha de ser sincronizado con la llegada de las concesiones programadas procedentes del CMTS;
- un servicio MAC para la sincronización del reloj de capa superior con el reloj maestro controlado por el CMTS.

Se señala la posibilidad de insertar un servicio de cortafuegos y supresión basado en el filtrado entre la capa MAC y el servicio de capa superior, pero dicho servicio no se modela en la presente definición del servicio MAC.

La interfaz del servicio MAC proporciona los servicios de control siguientes:

- un servicio MAC para que la capa superior se entere de la existencia de flujos de servicio aprovisionados y fijaciones de parámetros de tráfico QoS en el momento del registro;
- un servicio MAC para que la capa superior cree flujos de servicio. Utilizando este servicio, la capa superior inicia los conjuntos del parámetros QoS admitidos/activados, las reglas del clasificador, y los encabezamientos de supresión de paquetes para el flujo de servicio;
- un servicio MAC para que la capa superior suprima flujos de servicio;
- un servicio MAC para que la capa superior cambie flujos de servicio. Utilizando este servicio, la capa superior modifica los conjuntos de parámetros de QoS admitidos/activados, las reglas del clasificador y los encabezamientos de supresión de paquete;
- un servicio MAC para controlar la clasificación y la transmisión de unidades de datos de protocolo (PDU, *protocol data unit*) con encabezamientos suprimidos. Como máximo se define un encabezamiento suprimido único para una regla de clasificación única. El servicio de capa superior se encarga de especificar tanto la definición de los encabezamientos suprimidos (la inclusión de un comodín no entraña la supresión de campos) como la regla de clasificación única que discrimina cada encabezamiento. Además de definir las reglas de clasificación, el servicio MAC puede efectuar una comprobación completa de todos los bytes restantes del encabezamiento para evitar la generación de encabezamientos falsos si así está configurado por el servicio de capa superior.
- un servicio MAC para controlar en dos fases los recursos de tráfico QoS. La activación de las dos fases la lleva a cabo el servicio de capa superior siempre que tanto los parámetros QoS emitidos como los parámetros QoS activados figuren dentro de la petición de servicio apropiada. Tras recibir una indicación afirmativa, el servicio de capa superior sabe que el conjunto de parámetros QoS admitidos ha sido reservado por le CMTS, y que el conjunto de parámetros QoS activados ha sido activado por el CMTS. Salvo en caso de fallo catastrófico (por ejemplo, redimensionamiento de la anchura de banda de la capa PHY en sentido ascendente), estará garantizada la disponibilidad de los recursos admitidos para su activación, y estará garantizada la disponibilidad de los recursos activados para su utilización en la transmisión de paquetes.

Puede existir también una función de control para localizar un flujo de servicio no utilizado o un flujo de servicio identificado específico y vincularlo a un determinado servicio de capa superior. Los detalles de esa función no se especifican, y dependen de la implementación.

Pueden existir otras funciones de control en la interfaz del servicio MAC, por ejemplo, funciones que indaguen la situación de los flujos de servicio activos y los cuadros de clasificación de paquetes, o funciones del servicio MAC al servicio de una capa superior de manera que el servicio de capa superior pueda autorizar los flujos de servicio solicitados por el servicio de capa MAC par, pero dichas funciones no se modelan en la presente definición del servicio MAC.

Existen además otros servicios MAC no relacionados con flujos de servicio, por ejemplo, las funciones para el control de la dirección MAC del servicio MAC y las funciones de filtrado multidifusión SAID, pero dichas funciones no se modelan en la presente definición del servicio MAC.

B.E.1.1 Parámetros del servicio MAC

El servicio MAC utiliza los parámetros que se indican a continuación. Para una descripción completa de los parámetros, véase la sección relativa a la teoría del funcionamiento y otras secciones pertinentes del cuerpo principal de la especificación RFI.

- Parámetros de tráfico QoS de flujo de servicio

  Las primitivas activación de flujo de servicio y cambio de flujo de servicio MAC permiten proporcionar parámetros de tráfico QoS común, en sentido ascendente y en sentido descendente. Cuando se proporcionan tales parámetros, se anulan cualesquiera valores configurados para ellos en el momento del aprovisionamiento o en el momento en que el flujo de servicio fue creado por el servicio de capa superior.

- Parámetros de tráfico QoS activados/admitidos

  Si se utiliza la activación del flujo de servicio en dos fases, se controlan dos conjuntos completos de parámetros de tráfico QoS. Los parámetros QoS admitidos establecen los requisitos para que la reserva de los recursos sea autorizada por el CMTS. Los parámetros QoS activados establecen los requisitos para que la activación de los recursos sea autorizada por el CMTS. Los parámetros QoS admitidos pueden ser activados en un momento posterior por el servicio de capa superior. Los parámetros QoS activados PUEDEN ser utilizados inmediatamente por el servicio de capa superior.

- Reglas del filtro de clasificación del flujo de servicio

  Cero o más reglas del filtro de clasificación pueden ser proporcionadas para cada flujo de servicio controlado por el servicio de capa superior. Los clasificadores se identifican con un identificador de clasificador.

- Encabezamientos suprimidos PHS del flujo de servicio

  Cero o más cadenas de encabezamientos suprimidos PHS con sus correspondientes variables de control y plantilla de verificación PUEDEN ser definidas para cada flujo de servicio. Cuando se definen esos encabezamientos, se asocian en una relación biunívoca con reglas de clasificación específicas. Para regenerar paquetes con encabezamiento suprimido se negocia un índice de supresión del encabezamiento de la cabida útil entre el CM y CMTS.

B.E.2 Interfaz del servicio de datos MAC

Los servicios MAC se definen para la transmisión y recepción de datos hacia y desde flujos de servicio. Normalmente, un servicio de capa superior utilizará flujos de servicios para el establecimiento de la correspondencia entre diversas clases de tráfico y diferentes flujos de servicio. Se pueden definir las correspondencias con flujos de servicio para tráfico de baja prioridad, tráfico de alta prioridad y múltiples clases de tráfico especial, tales como el tráfico a velocidad binaria constante planificado mediante concesiones periódicas provenientes del CMTS en la capa MAC.

El servicio MAC proporciona las siguientes interfaces específicas del servicio de datos al servicio de capa superior. Representan una abstracción del servicio proporcionado y no implican ninguna implementación particular:

- MAC_DATA.request;
- MAC_DATA.indicate;
- MAC_GRANT_SYNCHRONIZE.indicate;
- MAC_CMTS_MASTER_CLOCK_SYNCHRONIZE.indicate.

B.E.2.1 MAC_DATA.request

Emitida por el servicio de capa inferior para pedir la clasificación y transmisión de una PDU formatada según IEEE 802.3 o DIX a la RF.

Parámetros

- PDU: PDU con codificación IEEE 802.3 o DIX incluyendo todos los campos de encabezamiento de capa 2 y FCS facultativo. PDU es el único parámetro obligatorio.
- Relleno: Se utiliza cuando la PDU tiene menos de 60 bytes y se desea mantener la transparencia [ISO/CEI 8802-3].

- ServiceFlowID (ID de flujo de servicio): Si se incluye, el servicio MAC elude la función de clasificación de paquetes y establece la correspondencia del paquete con el flujo de servicio específico indicado por el valor ServiceFlowID.
- ServiceClassName (nombre de clase de servicio), RulePriority (prioridad de regla): Si se incluye esta tupla, identifica el nombre de la clase de servicio de un flujo de servicio activo con el que se ha de establecer la correspondencia del paquete mientras no exista un clasificador con prioridad de regla superior a la prioridad de la regla suministrada.

Descripción de servicio ampliado

Transmisión de una PDU del servicio de capa superior a MAC/PHY. El único parámetro obligatorio es PDU. PDU contiene todos los encabezamientos de capa 2, los encabezamientos de capa 3, los datos y (facultativamente) la suma de comprobación de capa 2.

Si PDU es el único parámetro, el paquete se somete a la función de filtrado de clasificación de paquetes MAC para determinar cómo se establece la correspondencia del paquete con un flujo de servicio determinado. Los resultados de la operación clasificación de paquetes determinan en qué flujo de servicio se ha de transmitir el paquete y si el paquete deberá ser transmitido o no con los encabezamientos suprimidos.

Si se suministra el parámetro ServiceFlowID, se puede dirigir el paquete al flujo de servicio identificado de manera específica.

Si se suministra la tupla de parámetros ServiceClassName, RulePriority, el parámetro se dirige al primer flujo de servicio activo que concuerda con el nombre de la clase de servicio mientras no exista un clasificador con prioridad de regla superior a la prioridad de la regla suministrada. Este servicio es utilizado por los aplicadores de la política de capa superior para hacer posible la concordancia con cero o más reglas dinámicas para el tráfico seleccionado (por ejemplo, voz) mientras que el resto del tráfico se fuerza en un flujo de servicio dentro de la ServiceFlowClass (clase de flujo de servicios) denominada. Si no existe ningún flujo de servicio activo con el nombre de la clase de servicio, el servicio lleva a cabo una clasificación de paquetes normal.

En todos los casos, si no se encuentra concordancia con el clasificador, o si ninguna de las combinaciones de parámetros concuerda con un flujo de servicio específico, el paquete será dirigido al flujo de servicio primario.

El pseudo código siguiente describe el funcionamiento de la interfaz de servicio MAC_DATA.request pretendido:

```
MAC_DATA.request
        PDU
        [ServiceFlowID]
        [ServiceClassName, RulePriority]
```

FIND_FIRST_SERVICE_FLOW_ID (encontrar primero el ID de flujo de servicio) (ServiceClassName) devuelve ServiceFlowID del primer flujo de servicio cuyo ServiceClassName es igual al parámetro del procedimiento o NULL (nulo) si no se encuentra ningún flujo de servicio concordante.

SEARCH_CLASSIFIER_TABLE (buscar en la tabla del clasificador) (PriorityRange, gama de prioridades) busca todas las reglas dentro de la gama de prioridades especificada y devuelve el ServiceFlowID asociado con la regla o NULL si no se encuentra ninguna regla de clasificador.

```
TxServiceFlowID = NULL

IF (ServiceFlowID DEFINED)
        TxServiceFlowID = MAC_DATA.ServiceFlowID

ELSEIF(ServiceClassName DEFINED and RulePriority DEFINED)
        TxServiceFlowID = FIND_FIRST_SERVICE_FLOW_ID (ServiceClassName)
```

SearchID = SEARCH_CLASSIFIER_TABLE (All Priority Levels)
IF (SearchID not NULL and ClassifierRule.Priority >= MAC_DATA.RulePriority)
TxServiceFlowID = SearchID

ELSE [PDU only]
TxServiceFlow = SEARCH_CLASSIFIER_TABLE (All Priority Levels)

IF (TxServiceFlowID = NULL)
TRANSMIT_PDU (PrimaryServiceFlowID)
ELSE
TRANSMIT_PDU (TxServiceFlowID)

B.E.2.2 MAC_DATA.indicate

Emitido por el MAC para indicar la recepción de una PDU IEEE 802.3 o DIX para el servicio de capa superior procedente de la RF.

Parámetros

- PDU: PDU con codificación IEEE 802.3 o DIX incluyendo todos los campos de encabezamiento de capa 2 y FCS.

B.E.2.3 MAC_GRANT_SYNCHRONIZE.indicate

Emitida por le servicio MAC al servicio de capa superior para indicar la temporización de las capas llegadas de concesiones procedentes del CMTS. No se indica cómo deriva la capa superior, la latencia si es que existe alguna, entre la recepción de la indicación y la llegada efectiva de las concesiones (dentro de los límites de la fluctuación de fase de la concesión permitida) procedentes del CMTS. Cabe señalar que en las aplicaciones UGS, lo previsto es que el servicio de capa MAC aumente o disminuya el ritmo de las concesiones en base al número de concesiones por parámetro de tráfico QoS de cada intervalo. Cabe señalar además que, a medida que se aumenta o disminuye el número de concesiones por intervalo, así cambia la temporización de las llegadas de concesiones. Se señala también que, cuando se consigue la sincronización con el reloj maestro en sentido descendente del CMTS, dicha indicación sólo PUEDE ser requerida una vez por flujo de servicio activo. No se da ninguna indicación respecto a cómo se implementa esta función.

Parámetros

- ServicieFlowID (ID de flujo de servicios): Valor de identificador único para el flujo de servicio activo que, en concreto, recibe concesiones.

B.E.2.4 MAC_CMTS_MASTER_CLOCK_SYNCHRONIZE.indicate

Emitida por el servicio MAC al servicio de capa superior para indicar la temporización del reloj maestro del CMTS. No se da ninguna indicación respecto al número de veces que esta indicación es entregada por el servicio MAC al servicio de capa superior o a la frecuencia de esas entregas. No se da ninguna indicación respecto a cómo se implementa esta función.

Parámetros

- No se especifica ningún parámetro.

B.E.3 Interfaz de servicio del control MAC

Se define un conjunto de servicios MAC para el control de los flujos de servicio MAC y los clasificadores. Se señala que un servicio de capa superior puede utilizar estos servicios para proporcionar un constructivo de tráfico de capa superior, tal como "conexiones" o "subflujos" o "microflujos". Sin embargo, salvo por lo que se refiere a la capacidad de modificar clasificadores individuales, no se define ninguna semántica explícita para esos modelos de capa superior. El control de los parámetros de QoS del flujo de servicio MAC se especifica, por tanto, en el agregado.

El servicio MAC proporciona las funciones específicas de la interfaz del servicio de control que se indican a continuación al servicio de capa superior. Representan una abstracción del servicio proporcionado y no implican ninguna implementación particular:

– MAC_REGISTRATION_RESPONSE.indicate;
– MAC_CREATE_SERVICE_FLOW.request/response/indicate;
– MAC_DELETE_SERVICE_FLOW.request/response/indicate;
– MAC_CHANGE_SERVICE_FLOW.request/response/indicate.

B.E.3.1 MAC_REGISTRATION_RESPONSE.indicate

Emitida por el MAC DOSCSIS al servicio de capa superior para indicar el conjunto completo de flujos de servicio y parámetros de tráfico QoS del flujo de servicio que han sido aprovisionados y autorizados por la fase de registro de MAC. Los cambios subsiguientes en el estado de activación del flujo de servicio o adición y supresión de flujos de servicio se comunican al servicio de capa superior con indicaciones procedentes de otros servicios de control MAC.

Parámetros

- TLV de registro – Cualquiera y todos los formatos TLV que se necesitan para la definición de flujos de servicio y parámetros de flujo de servicio incluidos los parámetros QoS aprovisionados.

B.E.3.2 MAC_CREATE_SERVICE_FLOW.request

Emitida por el servicio de capa superior al MAC para pedir la creación de un nuevo flujo de servicio dentro del servicio MAC. Esta primitiva no se emite para flujos de servicio que ya están configurados y registrados, sino más bien para flujos de servicio creados dinámicamente. PUEDE definir también clasificadores para el flujo de servicio y suministrar parámetros QoS admitidos y activados. Esta función invoca la señalización DSA.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio específico que se crea.
- ServiceClassName (nombre de clase de servicio) – Nombre de la clase de flujo de servicio del flujo de servicio que se crea.
- Parámetros QoS admitidos – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Parámetros de QoS activados – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Reglas de supresión de encabezamiento de cabida útil del flujo de servicio – Cero o más reglas de PHS de cada flujo del servicio que es controlado por el servicio de capa superior.
- Reglas de filtro de clasificación de flujos de servicio – Cero o más reglas de filtro de clasificación de cada flujo de servicio que es controlado por el servicio de capa superior. Los clasificadores se identifican con un identificador de clasificador.

B.E.3.3 MAC_CREATE_SERVICE_FLOW.response

Emitida por el servicio MAC al servicio de capa superior para indicar el éxito o el fracaso de la petición de creación de un flujo de servicio.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio específico que se crea.
- ResponseCode (código de respuesta) – Código de éxito o fracaso.

B.E.3.4 MAC_CREATE_SERVICE_FLOW.indicate

Emitida por el servicio MAC para notificar al servicio de capa superior la creación de un nuevo flujo de servicio dentro del servicio MAC. Esta primitiva no se emite para flujos de servicio que han sido preconfigurados administrativamente, sino más bien para flujos de servicio definidos dinámicamente. En el presente anexo, la notificación tiene sólo carácter informativo.

Parámetros

- ServiceFlowID (ID de flujo de servicios) – Valor del identificador único del flujo de servicio específico que se crea.
- ServiceClassName (nombre de clase de servicio) – Nombre de la clase de flujo de servicio del flujo de servicio que se crea.
- Parámetros QoS admitidos – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Parámetros QoS activados – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Reglas de supresión de encabezamiento de cabida útil del flujo de servicio – Cero o más reglas de PHS de cada flujo de servicio que es controlado por el servicio de capa superior.
- Reglas de filtro de clasificación de flujos de servicio – Cero o más reglas de filtro de clasificación de cada flujo de servicio que es controlado por el servicio de capa superior. Los clasificadores se identifican mediante un identificador de clasificador.

B.E.3.5 MAC_DELETE_SERVICE_FLOW.request

Emitida por el servicio de capa superior al MAC para pedir la supresión de un flujo de servicio y todos los parámetros QoS, incluyendo todos los clasificadores y reglas de PHS. Esta función invoca la señalización DSD.

Parámetros

- ServiceFlowID (ID flujo de servicio) – Valor del identificador único opcional del flujo de servicio suprimido.

B.E.3.6 MAC_DELETE_SERVICE_FLOW.response

Emitida por el servicio MAC al servicio de capa superior para indicar el éxito o el fracaso de la petición de supresión de un flujo de servicio.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio específico que se suprime.
- ResponseCode (Código de respuesta) – Código de éxito o fracaso.

B.E.3.7 MAC_DELETE_SERVICE_FLOW.indicate

Emitida por servicio MAC para notificar al servicio de capa superior la supresión de un flujo de servicio dentro del servicio MAC.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificar único opcional del flujo de servicio suprimido.

B.E.3.8 MAC_CHANGE_SERVICE_FLOW.request

Emitida por el servicio de capa superior al MAC para pedir la introducción de modificaciones en un determinado flujo de servicio creado y adquirido. Esta función puede definir tanto el conjunto completo de clasificadores como los cambios incrementales de los clasificadores

(adición/eliminación). Esta función define el conjunto completo de parámetros QoS admitidos y activados para un flujo de servicio. Esta función invoca la señalización de capa MAC DSC.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio específico que se modifica.
- Cero o más reglas de clasificación de paquetes con la semántica de supresión/eliminación y LLC e IP y los parámetros IEEE 802.1P/Q.
- Parámetros QoS admitidos – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Parámetros QoS activados – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Reglas de supresión de encabezamiento de cabida útil del flujo de servicio – Cero o más reglas de PHS de cada flujo de servicio que es controlado por el servicio de capa superior.

B.E.3.9 MAC_CHANGE_SERVICE_FLOW.response

Emitida por el servicio MAC al servicio de capa superior para indicar el éxito o el fracaso de la petición de cambio de un flujo de servicio.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio específico que se libera.
- ResponseCode (código de respuesta) – Código de éxito o fracaso.

B.E.3.10 MAC_CHANGE_SERVICE_FLOW.indicate

Emitida por el servicio MAC DOSCIS para notificar al servicio de capa superior la petición de cambio de un flujo de servicio. En el presente anexo B, la notificación tiene sólo el carácter informativo y no se requiere confirmación antes de cambiar el flujo de servicio. Las indicaciones de cambio de flujo de servicio se generan en base a la señalización DSC. La señalización DSC puede tener su origen en eventos de cambio de flujo de servicio entre el servicio de capa superior par y su servicio MAC, o en fallos de recursos de red tales como el redimensionamiento de la anchura de banda disponible total en la capa PHY. No se especifica la manera de reaccionar del servicio de capa superior ante reducción forzada de los parámetros de tráfico QoS admitidos o reservados.

Parámetros

- ServiceFlowID (ID de flujo de servicio) – Valor del identificador único del flujo de servicio que se activa.
- Reglas de clasificación de paquetes con LLC, IP y parámetro IEEE 802.1P/Q, y con cero o más PHS_CLASSIFIER_IDENTIFIERs (identificadores de clasificador de supresión de encabezamiento de cabida útil).
- Parámetros QoS admitidos – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Parámetros QoS activados – Cero o más parámetros de tráfico en sentido ascendente, en sentido descendente y común del flujo de servicio.
- Reglas de supresión de encabezamiento de cabida útil del flujo de servicio – Cero o más reglas de PHS de cada flujo de servicio que es controlado por el servicio de capa superior.

B.E.4 Escenarios de utilización del servicio MAC

Las entidades de capa superior utilizan los servicio proporcionados por MAC para controlar flujos de servicio y para enviar y recibir paquetes de datos. Los escenarios siguientes exponen el reparto de funciones entre el servicio de capa superior y el servicio MAC.

B.E.4.1 Transmisión de PDU del servicio de capa superior al servicio de datos MAC

- El servicio de capa superior transmite las PDU vía el servicio MAC_DATA (datos de MAC).
- El servicio MAC_DATA clasifica las PDU transmitidas utilizando el cuadro de clasificación y transmite las PDU en el flujo de servicio apropiado. La función de clasificación puede provocar también la supresión del encabezamiento del paquete de acuerdo con una plantilla de supresión de encabezamiento incorporada a la regla de clasificación. El servicio de capa superior pueda eludir esa función de clasificación.
- El servicio MAC_DATA impone la aplicación de todos los parámetros de conformación del tráfico QoS en base al flujo de servicio.
- El servicio MAC_DATA transmite las PDU en la RF de DOCSIS según lo planificado por la capa MAC.

B.E.4.2 Recepción de PDU en el servicio de capa superior procedentes del servicio de datos MAC

- Las PDU se reciben de la RF de DOCSIS.
- Si se envía una PDU con encabezamiento suprimido, el encabezamiento es regenerado antes de que el paquete sea sometido a un procesamiento ulterior.
- En el CMTS, el servicio MAC_DATA clasifica las entradas de PDU procedentes de la RF utilizando el cuadro de clasificación y a continuación aplica sus normativas de conformación del tráfico QoS y valida el direccionamiento efectuado por el CM. En el CM no se requiera la clasificación de flujos de servicio por paquete para la entrada de tráfico procedente de la RF.
- El servicio de capa superior recibe las PDU del servicio MAC_DATA.indicate

B.E.4.3 Secuencia de muestra de los servicios de control MAC y datos MAC

Una posible secuencia orientada al CM de las funciones de los servicios MAC para la creación, adquisición, modificación y utilización subsiguiente de un flujo de servicio específico sería como sigue:

- MAC_REGISTER_RESPONSE.indicate

  Aprender cualquier flujo de servicio aprovisionado y sus parámetros de tráfico QoS aprovisionados.
- MAC_CREATE_SERVICE_FLOW.request/response

  Crear un nuevo flujo de servicio. Esta interfaz de servicio se utiliza si el flujo de servicio fue aprendido en tanto que flujo no aprovisionado por la interfaz de servicio MAC_REGISTER_RESPONSE. La creación de un flujo de servicio invoca señalización DSA.
- MAC_CHANGE_SERVICE_FLOW.request/response

  Definir conjuntos de parámetros QoS admitidos y activados, clasificadores y encabezamientos de supresión de paquetes. El cambio de un flujo de servicio invoca señalización DSC.
- MAC_DATA.request

  Enviar las PDU al servicio MAC para clasificación y transmisión.

- MAC_DATA.indication

  Recibir las PDU procedentes del servicio MAC
- MAC_DELETE_SERVICE_FLOW.request/response

  Suprimir flujo de servicio. Probablemente sólo se invoque para flujos de servicio creados dinámicamente, no flujos de servicio aprovisionados. La supresión de un flujo de servicio utiliza señalización DSD.

ANEXO B.F

Ejemplo de secuencia de preámbulo

(Este anexo es informativo)

B.F.1 Introducción

Se incluye una supercadena de preámbulo programable, de hasta 1024 bits de longitud, parte del perfil o los atributos a todo lo ancho del canal, común a todos los perfiles de ráfaga de canal (véanse B.8.3.3 y el cuadro B.8-18), pero teniendo cada perfil de ráfaga la capacidad de especificar la ubicación inicial dentro de esta secuencia de bits y la longitud del preámbulo (vénase B.8.3.3 y el cuadro B.8-19). El primer bit del esquema del preámbulo es designado por el desplazamiento del valor del preámbulo, como se describe en el cuadro B.8-19. El primer bit del esquema del preámbulo es el bit que accede en primer lugar al proceso de establecimiento de correspondencia de símbolos (véase la figura B.6-9), y es el bit I1 en el primer símbolo de la ráfaga (véase B.6.2.2.2). Si, por ejemplo, según el cuadro B.8-19, el valor del desplazamiento del preámbulo es 100, el bit 101 de la supercadena de preámbulo es el primero en acceder al proceso antes mencionado y el bit 102 es el segundo, y se establece su correspondencia con Q1 y así sucesivamente. En B.F.2 se da un ejemplo de supercadena de preámbulo con una longitud de 1024 bits.

B.F.2 Ejemplo de secuencia de preámbulo

Lo que sigue es un ejemplo de secuencia de preámbulo de 1024 bit:

Bits 1 a 128:

1100 1100 1111 0000 1111 1111 1100 0000 1111 0011 1111 0011 0011 0000 0000 1100
0011 0000 0011 1111 1111 1100 1100 1100 1111 0000 1111 0011 1111 0011 1100 1100

Bits 129 a 256:

0011 0000 1111 1100 0000 1100 1111 1111 0000 1100 1100 0000 1111 0000 0000 1100
0000 0000 1111 1111 1111 0011 0011 0011 1100 0011 1100 1111 1100 1111 0011 0000

Bits 257 a 384:

1100 0011 1111 0000 0011 0011 1111 1100 0011 0011 0000 0011 1100 0000 0011 0000
0000 1110 1101 0001 0001 1110 1110 0101 0010 0101 0010 0101 1110 1110 0010 1110

Bits 385 a 512:

0010 1110 1110 0010 0010 1110 1110 1110 1110 1110 0010 0010 0010 1110 1110 0010
1110 1110 1110 0010 1110 0010 1110 0010 0010 0010 0010 1110 0010 0010 1110 0010

Bits 513 a 640:

0010 0010 1110 1110 1110 1110 1110 1110 0010 1110 0010 1110 0010 1110 1110 0010
0010 1110 1110 0010 1110 1110 1110 0010 1110 1110 0010 1110 0010 0010 1110 0010

Bits 641 a 768:

0010 1110 1110 1110 0010 0010 0010 1110 0010 1110 1110 1110 1110 0010 0010 1110
0010 1110 0010 0010 0010 1110 1110 0010 0010 0010 0010 1110 0010 0010 0010 0010

Bits 769 a 896:

0010 1110 1110 1110 1110 1110 1110 0010 1110 0010 1110 0010 1110 1110 0010 0010
1110 1110 0010 1110 1110 1110 0010 1110 1110 0010 1110 0010 0010 1110 0010 0010

Bits 897 a 1024:

1110 1110 1110 0010 0010 0010 1110 0010 1110 1110 1110 1110 0010 0010 1110 0010
1110 0010 0010 0010 1110 1110 0010 0010 0010 0010 1110 0010 0010 0010 0010 1110

ANEXO B.G

Interoperabilidad versión 1.0/versión 1.1 de DOCSIS

B.G.1 Introducción

Este anexo B.G se aplica solamente a la primera opción definida en B.1.1

Al presente anexo B se hace referencia, de manera oficiosa, como DOCSIS 1.1. Es la segunda generación de DOCSIS 1.0 especificado en [DOCSIS9]. Los términos DOCSIS 1.1 y DOCSIS 1.0 se refieren a estas dos especificaciones diferentes.

La especificación DOCSIS 1.1 pretende sobre todo mejorar la funcionalidad QoS limitada de un sistema de acceso por cable basado en DOCSIS 1.0. Se han definido nuevos mensajes MAC para señalización de QoS dinámica, así como varias codificaciones de parámetros QoS nuevos en los mensajes MAC existentes. Un CMTS de DOCSIS 1.1 puede soportar mejor los requisitos de tráfico sensible al retardo/la fluctuación de fase en un CM de DOCSIS 1.1.

Además de soportar un amplio conjunto de características de QoS para los CM de DOCSIS 1.1, el CMTS de DOCSIS 1.1 debe ser retrocompatible con un CM de DOCSIS 1.0. Es preciso, por otra parte, que un CM 1.1 funcione como un CM 1.0 cuando interopere con un CMTS 1.0.

En el anexo B.G se describen las cuestiones relativas a la interoperabilidad y las soluciones de avenencia necesarias, cuando el operador desea soportar CM de DOCSIS 1.0 y de DOCSIS 1.1 en el mismo canal de acceso por cable.

B.G.2 Asuntos relativos a la interoperabilidad en general

Esta cláusula se refiere a asuntos relativos a la interoperabilidad DOCSIS 1.0/DOCSIS 1.1 en general, sin consecuencias en la calidad de funcionamiento cuando los CM funcionan de manera normal.

B.G.2.1 Aprovisionamiento

Los parámetros del fichero de configuración del TFTP para un CM de DOCSIS 1.1 son un superconjunto de los de un CM de DOCSIS 1.0. Los editores del fichero de configuración habrán de ser mejorados para incorporar el soporte de esos nuevos parámetros y del nuevo cálculo de la verificación de integridad de mensaje (MIC).

Si a un CM DOCSIS 1.1 se le aprovisiona un fichero de configuración de TFTP estilo DOCSIS 1.0, se DEBE registrar como un CM de DOCSIS 1.0 (aunque en REG-REQ todavía DEBE especificar "DOCSIS 1.1" en la capacidad del módem de la versión DOCSIS y PUEDE especificar las capacidades del módem 1.1 adicionales que soporta). Así pues, un CM de DOCSIS 1.1 puede ser aprovisionado de modo que funciones de manera continua en una red de DOCSIS 1.0 o una red de DOCSIS 1.1. Aunque está claro que un módem de DOCSIS 1.1 en una red de DOCSIS 1.0 sería incapaz de soportar cualquier característica específica de DOCSIS 1.1.

Por otro lado, los CM de DOCSIS 1.0 no reconocen (e ignoran) muchos de los formatos tipo/longitud/valor (TLV) nuevos de un fichero de configuración estilo DOCSIS 1.1, y no podrán registrarse de manera satisfactoria si se les aprovisiona un fichero de configuración DOCSIS 1.1. Para evitar cualquier inadaptación funcional, un CMTS de DOCSIS 1.1 DEBE rechazar toda petición de registro con parámetros de configuración específicos de DOCSIS 1.1 no sustentados por la codificación de capacidades del módem asociada en el mensaje REG-REQ (véase B.C.1.3.1).

B.G.2.2 Registro

El CMTS de DOCSIS 1.1 se ha diseñado de forma que maneje los formatos TLV de registro existentes de los CM de DOCSIS 1.0, así como los formatos TLV nuevos (a saber, los tipos 22 a 30) del CM de DOCSIS 1.1.

Hay una pequeña diferencia entre el procedimiento de mensajería relacionado con el registro cuando el CMTS de DOCSIS 1.1 responde a un CM de DOCSIS 1.1 y el procedimiento cuando responde a un CM de DOCSIS 1.0. Un CM de DOCSIS 1.1 podría configurarse para utilizar el nombre de clase de servicio definido de manera estática en el CMTS en vez de pedir explícitamente los parámetros de clase de servicio. Cuando el CMTS de DOCSIS 1.1 recibe esa petición de registro, codifica los parámetros reales de la clase de servicio en la respuesta de registro y espera el mensaje MAC de acuse de registro específico de DOCSIS 1.1 procedente del CM. Si las capacidades detalladas en el mensaje de respuesta de registro superan las que el CM es capaz de soportar, es preciso que el CM se lo indique al CMTS en el acuse de registro.

Cuando CM de DOCSIS 1.0 se registra con el mismo CMTS, la versión DOCSIS 1.0 por defecto es fácilmente identificada por la ausencia de la codificación de capacidades del módem "Versión de DOCSIS" en la petición de registro. La petición de registro procedente de un CM de DOCSIS 1.0 pide de manera explícita todos los parámetros de clase de servicio que no sean por defecto en la petición de registro según su información de aprovisionamiento. La ausencia de un nombre de clase de servicio hace innecesario que el CMTS de DOCSIS 1.1 especifique de manera explícita los parámetros de clase de servicio en la respuesta de registro utilizando los formatos TLV de DOCSIS 1.1. Cuando un CMTS de DOCSIS 1.1 reciba una petición de registro conteniendo codificaciones de clase de servicio de DOCSIS 1.0, responderá con la respuesta de registro estilo DOCSIS 1.0 habitual y no esperará el envío por el CM de un mensaje MAC de acuse de registro.

Otro asunto de importancia menor es que un CM de DOCSIS 1.0 pedirá una clase de servicio bidireccional (con parámetros en sentido ascendente/descendente) del CMTS utilizando una fijación de configuración clase de servicio.

Puesto que un CMTS de DOCSIS 1.1 funciona normalmente con clases de servicio unidireccionales, puede convertir fácilmente una fijación de configuración clase de servicio de DOCSIS 1.0 en una codificación de flujo de servicio de DOCSIS 1.1 para el establecimiento de clases de servicio unidireccionales en una implementación de QoS local. No obstante, en el caso de módems de DOCSIS 1.0, el CMTS de DOCSIS 1.1 DEBE continuar manteniendo el cuadro QoSProfile (perfil de QoS) (con parámetros de clase de servicio bidireccional) a efectos de la retrocompatibilidad con MIB de DOCSIS 1.0.

Así pues, si están adecuadamente aprovisionados, un CM de DOCSIS 1.0 y un CM de DOCSIS 1.1 pueden registrarse de manera satisfactoria con el mismo CMTS de DOCSIS 1.1. De manera similar,

un CM de DOCSIS 1.0 y un CM de DOCSIS 1.1 pueden registrarse de manera satisfactoria con el mismo CMTS de DOCSIS 1.0.

B.G.2.3 Establecimiento de servicio dinámico

Hay 8 mensajes MAC nuevos que se refieren al establecimiento de servicio dinámico. Un CM de DOCSIS 1.0 nunca los enviará a ningún CMTS ya que no son soportados. Un CM de DOCSIS 1.1 nunca los enviará a un CMTS de DOCSIS 1.0 porque:

a) para que el registro sea satisfactorio ha de ser aprovisionado como un CM de DOCSIS 1.0, y

b) cuando se aprovisiona como un CM de DOCSIS 1.0 actúa de manera idéntica.

Cuando un CM de DOCSIS 1.1 está conectado a un CMTS de DOCSIS 1.1, estos mensajes actúan según lo previsto.

B.G.2.4 Fragmentación

La fragmentación la inicia el CMTS. Por ello, un CMTS de DOCSIS 1.0 nunca iniciará una fragmentación ya que no sabe nada sobre la misma. Un CMTS de DOCSIS 1.1 sólo puede iniciar la fragmentación para los CM de DOCSIS 1.1. Un CMTS de DOCSIS 1.1 NO DEBE tratar de fragmentar transmisiones procedente de un CM de DOCSIS 1.0 que no haya indicado codificación de capacidades del módem para el soporte de la fragmentación con un valor de 1.

B.G.2.5 Soporte de la multidifusión

Es obligatorio que los CM de DOCSIS 1.0 soporten el reenvío del tráfico de multidifusión. Sin embargo, la especificación no dice nada sobre el soporte de IGMP. Así pues, el único mecanismo normalizado para el control de la multidifusión IP en los CM de DOCSIS 1.0 es mediante el SNMP y los filtros de paquetes. Los diseñadores de redes de DOCSIS 1.0 tendrán que hacer frente a estas limitaciones y esperar que no haya diferencias con respecto a los CM de DOCSIS 1.0 en una red de DOCSIS 1.1.

B.G.2.6 Cambio de canal en sentido ascendente (UCC, *upstream channel change*)

Un CMTS de DOCSIS 1.1 puede especificar el nivel de la realineación que se ha de efectuar cuando emite un mensaje UCC-Request (petición de UCC) al CM. Este parámetro de la técnica de realineación lo especifica el CMTS de DOCSIS 1.1 utilizando un formato TLV nuevo en el mensaje MAC UCC-Request.

Los CM de DOCSIS 1.1 que reconocen este nuevo TLV en el mensaje UCC-Request se pueden beneficiar realineando sólo al nivel especificado por ese formato TLV. Esto puede ayudar a reducir el tiempo de reinicialización, tras un UCC, del CM de DOCSIS 1.1 que lleva una llamada vocal. Un CMTS de DOCSIS 1.1 sabe cuál es el tipo de CM al que está emitiendo el UCC-Request. Se puede abstener de insertar este formato TLV de realineación en el UCC-Request para los CM de DOCSIS 1.0. Si un CMTS de DOCSIS 1.1 inserta este formato TLV de realineación en el UCC-Request, los CM de DOCSIS 1.0 que no reconozcan el TLV ignorarán su contenido y efectuarán la realineación DOCSIS 1.0 por defecto desde el principio (mantenimiento inicial). El CMTS de DOCSIS 1.1 acepta el procedimiento de alineación inicial por defecto desde cualquier módem que haya emitido el UCC-Request.

A los CM de DOCSIS 1.0 y DOCSIS 1.1 situados en el mismo canal en sentido ascendente se les puede pedir por tanto, individualmente, que cambien canales en sentido ascendente sin problema alguno de interoperabilidad causado por el TLV de realineación de estilo DOCSIS 1.1 en el mensaje UCC-Request.

B.G.3 Dispositivos híbridos

Algunos diseños de CM de DOCSIS 1.0 pueden facilitar el soporte de características DOCSIS 1.1 particulares mediante la mejora del soporte lógico. De manera similar, algunos CMTS de DOCSIS 1.0 PUEDEN soportar determinadas características de DOCSIS 1.1. Para facilitar estos

dispositivos "híbridos", la mayoría de las características de DOCSIS 1.1 se enumeran una a una en las capacidades del módem.

Los CM híbridos de DOCSIS 1.0 PUEDEN pedir características de DOCSIS 1.1 por medio de este mecanismo. Sin embargo, a menos que un CM se atenga por completo a DOCSIS 1.1 (es decir que no sea híbrido), NO DEBE enviar una capacidad de módem "versión DOCSIS" que indique cualquier cosa además de DOCSIS 1.0.

Si un CM híbrido pretende pedir capacidades 1.1 del CMTS durante el registro, DEBE enviar la cadena codificada ASCII en código de operación 60 de su petición DHCP, "docsis1.0:xxxxxxx", en donde xxxxx DEBE ser una representación ASCII de la codificación hexadecimal de las capacidades del módem (véanse B.C.1.3.1 y B.D.1.1). El servidor DHCP PUEDE utilizar esa información para determinar qué fichero de configuración ha de utilizar el CM.

Normalmente, un CMTS de DOCSIS 1.0 fijará todas las capacidades del módem desconocidas a "inactiva" en la respuesta de registro indicando que esas características no son soportadas y NO DEBEN ser utilizadas por el CM. Un CMTS híbrido de DOCSIS 1.0 PUEDE dejar las capacidades de módem soportadas fijadas a "activa" en la respuesta de registro. No obstante, a menos que un CMTS se atenga por completo a DOCSIS 1.1 (es decir, que no sea híbrido), aún DEBE fijar todas las capacidades del módem "versión DOCSIS" en DOCSIS 1.0.

Como siempre, cualquier capacidad del módem fijada en "inactiva" en la respuesta de registro debe ser considerada como no soportada por el CMTS y NO DEBE ser utilizada por el CM.

B.G.4 Interoperabilidad y funcionamiento

Esta cláusula se refiere al tema de las consecuencias que tiene el funcionamiento en la QoS de los CM de DOCSIS 1.1 cuando CM de DOCSIS 1.0 y DOCSIS 1.1 se aprovisionan de forma que compartan el mismo canal MAC en sentido ascendente.

Los CM de DOCSIS 1.0 no pueden fijar de manera explícita su procedimiento de petición (ni proporcionar parámetros de planificación) para los mecanismos de planificación de DOCSIS 1.1 avanzados, tales como el "servicio de concesión no solicitada" y el "servicio de interrogación secuencial en tiempo real". Por ello, los CM de DOCSIS 1.0 sólo recibirán el servicio "mejor esfuerzo escalonado" o "CIR" estáticamente configurado en el sentido ascendente. Los CM de DOCSIS 1.1 situados en el mismo canal en sentido ascendente pueden pedir de manera explícita flujos de servicio adicionales cuando así lo requieran, utilizando el mensaje MAC DSA-Request (petición de DSA) de DOCSIS 1.1. Los CM de DOCSIS 1.1 pueden aprovechar, por tanto, los mecanismos de planificación avanzados de un CMTS de DOCSIS 1.1 para su tráfico en tiempo real, además del servicio de planificación del mejor esfuerzo que comparten con los CM de DOCSIS 1.0 en el mismo canal ascendente.

El canal de acceso por cable en sentido ascendente de DOCSIS 1.1 lleva tramas MAC de longitud variable. A pesar de la longitud variable de las tramas MAC, el planificador de concesiones del CMTS de DOCSIS 1.1 es capaz, en teoría, de proporcionar un entorno similar al TDMA con fluctuación de fase cero para concesiones vocales en el sentido ascendente. Cuando el planificador de concesiones detecta que el plazo de tiempo de cualquier concesión vocal no va a ser respetado debido a la inserción de una concesión no vocal, fragmenta la concesión no vocal hasta el límite de la concesión vocal futura. De esta manera, las concesiones vocales ven un desplazamiento cero con respecto a la posición de la concesión periódica asignada.

Sin embargo, esa fragmentación de las concesiones podría no siempre ser posible, por ejemplo, cuando el CMTS soporta CM de DOCSIS 1.0 junto con CM de DOCSIS 1.1 en el mismo canal en sentido ascendente, ya que los CM de DOCSIS 1.0 no soportan la fragmentación. En el caso de un canal en sentido ascendente de versión de CM mixta, la fluctuación de fase de la concesión vocal más desfavorable vista por los CM de DOCSIS 1.1 ocurre cuando se da a un CM de DOCSIS 1.0 una concesión para una trama MAC de tamaño máximo no fragmentada justo antes del intervalo de concesión vocal designado del CM de DOCSIS 1.1.

La fluctuación de fase de concesión vocal máxima que sufren los CM de DOCSIS 1.1 es función de las características de la capa física del canal en sentido ascendente. Para canales en sentido ascendente a 10,24 Mbit/s y 5,12 Mbit/s, las consecuencias de tener CM fragmentadores y no fragmentadores en el mismo canal es casi imperceptible. En canales más pequeños, las ventajas de la fragmentación son mucho mayores y la fluctuación de fase inducida por CM de DOCSIS 1.0 no fragmentadores es mayor.

Así pues, redes diseñadas adecuadamente soportar voz incluso cuando se combinan CM de DOCSIS 1.0 y de DOCSIS 1.1.

ANEXO B.H

Múltiples canales en sentido ascendente

(Este anexo es informativo)

Si hubiera alguna discrepancia entre el presente anexo y cualquier cláusula normativa del anexo B, la cláusula normativa tiene precedencia.

En la subcláusula B.9.2 se describe el soporte de múltiples canales en sentido ascendente y en sentido descendente dentro de un dominio DOCSIS. La permutación que puede ver un CM en el segmento de cable al que está conectado incluye:

- sentido descendente único y sentido ascendente único por segmento de cable;
- sentido descendente único y sentidos ascendentes múltiples por segmento de cable;
- sentidos descendentes múltiples y sentido ascendente único por segmento de cable;
- sentidos descendentes múltiples y sentidos ascendentes múltiples por segmento de cable.

Una aplicación típica, que requerirá un canal en sentido ascendente y un canal en sentido descendente por CM, es el hojeo de la web. El hojeo de la web suele tener requisitos de anchura de banda asimétrica que concuerdan estrechamente con la anchura de banda asimétrica de DOCSIS.

Una aplicación típica, que requerirá acceso a uno de los múltiples canales en sentido ascendente por CM es la telefonía IP. La telefonía IP suele tener requisitos de anchura de banda simétrica. Si hay una gran concentración de CM en una zona geográfica, servidos todos ellos por el mismo nodo de fibra, quizás se necesite más de un canal en sentido ascendente para proporcionar anchura de banda suficiente y evitar el bloqueo de las llamadas.

Una aplicación típica, que requerirá acceso a uno de los múltiples canales en sentido descendente por CM es el vídeo continuo IP. El vídeo continuo IP suele tener requisitos de anchura de banda en sentido descendente extremadamente ancha. Si hay una gran concentración de CM en una zona geográfica, servidos todos ellos por el mismo nodo de fibra, quizás se necesite más de un canal en sentido descendente para proporcionar anchura de banda suficiente y entregar múltiples flujos de vídeo IP a múltiples CM.

Una aplicación típica, que requerirá múltiples canales en sentido descendente y múltiples canales en sentido ascendente es aquélla en la que se combinan las aplicaciones anteriores, y resulta más económico tener múltiples canales que subdividir físicamente la red HFC.

La función del CM en estos escenarios consistiría en poder desplazarse entre múltiples canales en sentido ascendente y en sentido descendente. La función del CMTS consistiría en gestionar la carga de tráfico dirigido a todos los CM, y equilibrar el tráfico entre múltiples canales en sentido ascendente y en sentido descendente desplazando dinámicamente los CM en base a sus necesidades de recursos y los recursos disponibles.

En el presente anexo B.H se hacen diversas consideraciones relativas a la implementación de estos casos. Se perfila, en concreto, la primera y la última aplicaciones. Con estos ejemplos se trata de ilustrar una topología y una implementación de esa topología.

B.H.1 Sentido descendente único y sentido ascendente único por segmento de cable

Esta cláusula presenta un ejemplo de canal en sentido descendente único y de cuatro canales en sentido ascendente. En la figura B.H-1, los cuatro canales en sentido ascendente se hallan en fibras separadas que da servicio a cuatro comunidades geográficas de módems. El CMTS tiene acceso al canal en sentido descendente y a los cuatro canales en sentido ascendente, mientras que cada CM tiene acceso al canal en sentido descendente y solamente a un canal en sentido ascendente.

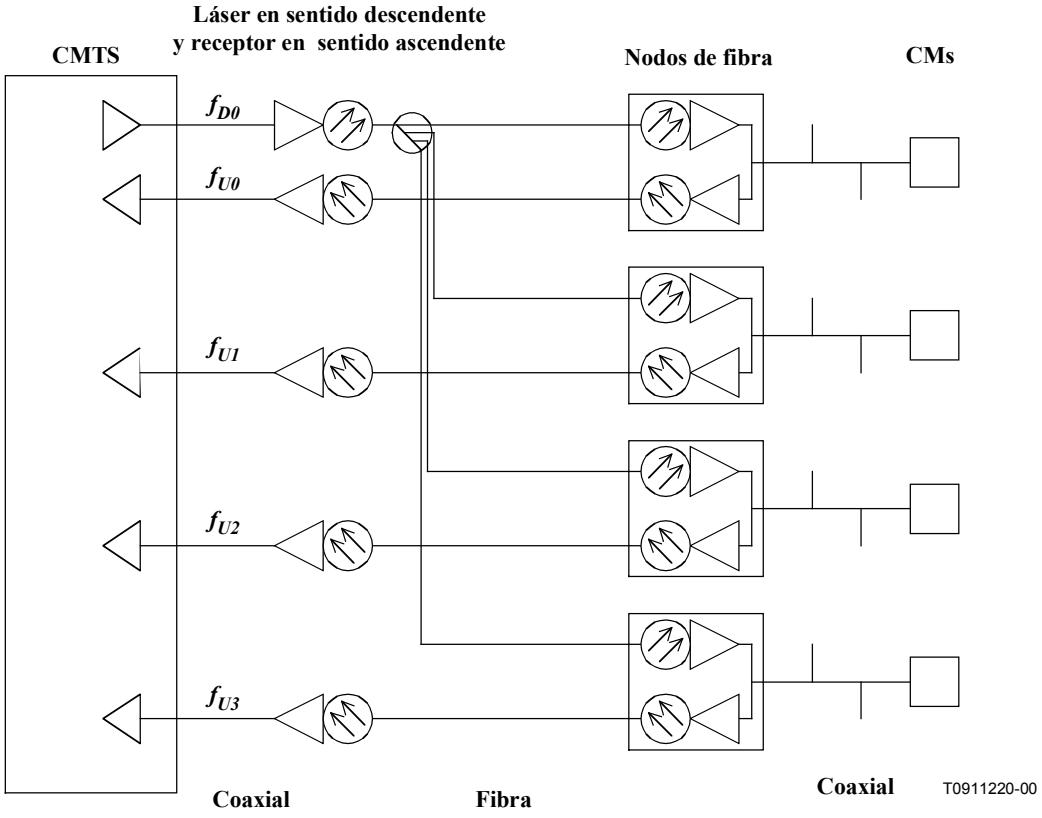


Figura B.H-1/J.112 – Canal en sentido descendente único y canal en sentido ascendente único por módem de cable

En esta topología, el CMTS transmite descriptores de canales en sentido ascendente (UCD) y los MAP de cada uno de los cuatro canales en sentido ascendente relacionados con el canal en sentido descendente compartido.

Desgraciadamente, los CM no pueden determinar a qué rama de la fibra está conectado cada uno de ellos porque no hay manera de llevar la información geográfica por el canal en sentido descendente compartido. En la inicialización, el CM elige aleatoriamente un UCD y su MAP correspondiente. El CM elige a continuación una oportunidad de mantenimiento inicial en ese canal y transmite una petición de alineación.

El CMTS recibirá la petición de alineación y redireccionará el CM al identificador de canal en el sentido ascendente apropiado especificando el ID de canal en sentido ascendente en la respuesta de alineación. El CM DEBE utilizar entonces el ID de canal de la respuesta de alineación, no el ID de canal con el que se inició la petición de alineación. Éste sólo hace falta en la primera respuesta de

alineación recibida por el CM. El CM DEBERÍA continuar el proceso de alineación normalmente y aguardar la llegada de los IE de mantenimiento de estación.

A partir de ese momento, el CM utilizará el MAP que corresponde a la rama de fibra a la que está conectado. Si el CM tuviera que rehacer en algún momento el mantenimiento inicial, podría empezar con su UCD previo conocido en vez de elegir uno al azar.

Esta tipología impone un cierto número de limitaciones:

- Todas las oportunidades de mantenimiento inicial de todos los nodos de fibra deben estar alineadas. Cuando el CM elige un UCD para utilizarlo y a continuación utiliza el MAP para ese canal, el CMTS debe estar preparado para recibir una petición de alineación en la oportunidad de mantenimiento inicial. Se señala que solamente los intervalos de inicialización deben estar alineados. Una vez que el CM esté alineado de manera satisfactoria en un canal en sentido ascendente, sus actividades sólo han de ser alineadas con otros usuarios en el mismo canal ascendente. En la figura B.H-1, la transmisión de datos ordinarios y las peticiones de anchura de banda se pueden producir de forma independiente los cuatro canales en sentido ascendente.
- Todos los canales en sentido ascendente de nodos diferentes deberán funcionar a la misma o las mismas frecuencias a menos que se sepa que no habrá repercusión alguna en ningún otro servicio en sentido ascendente como consecuencia de la transmisión por un CM de una petición de alineación a una frecuencia "errónea" durante una oportunidad de mantenimiento inicial. Si el CM eligiera de manera arbitraria un descriptor de canal en sentido ascendente, podría transmitir a la frecuencia errónea cuando el UCD seleccionado se aplicara a un canal en sentido ascendente de un nodo de fibra diferente, lo cual podría prolongar el mantenimiento inicial. No obstante, esta podría ser una solución de avenencia del sistema aceptable para mantener la gestión del espectro de manera independiente entre segmentos de cable.
- Todos los canales en sentido ascendente pueden funcionar con velocidades de símbolos diferentes. Sin embargo, existe un compromiso entre el tiempo que hace falta para adquirir los parámetros de alineación y la flexibilidad de la velocidad de símbolos por canal en sentido ascendente. Si las velocidades de símbolos no fuesen iguales, el CMTS sería incapaz de demodular la petición de alineación caso de ser transmitida con una velocidad de símbolos errónea para el receptor del canal en sentido ascendente de que se trate. El resultado sería que el CM llevaría a cabo un reintento tal como se indica en la especificación RFI y a continuación intentaría, eventualmente, otros canales en sentido ascendente asociados con el utilizado entonces en sentido descendente. Al aumentar la probabilidad de que se trate de alinear en múltiples canales aumenta el tiempo de inicialización del CM, pero la utilización de velocidades de símbolos diferentes en nodos de fibra diferentes redunda en una mayor flexibilidad al fijar el grado de mitigación del ruido en ráfagas.
- Todas las oportunidades de mantenimiento inicial en canales diferentes pueden utilizar características de ráfaga diferentes de manera que el CMTS pueda demodular la petición de alineación. Una vez más, se trata de un compromiso entre tiempo para lograr la alineación y un cierto grado de flexibilidad al fijar los parámetros de capa física entre diferentes canales en sentido ascendente. Si los parámetros de la ráfaga en sentido ascendente para el mantenimiento inicial no fuesen iguales, el CMTS sería incapaz de demodular la petición de alineación caso de haber sido transmitida con parámetros de ráfaga erróneos para el canal de que se trate. El resultado sería que el CM intentaría de nuevo la petición de alineación según lo indicado en la especificación de RFI y a continuación intentaría, eventualmente, otros canales en sentido ascendente asociados con el utilizado entonces en sentido descendente. Al aumentar la probabilidad de que se trate de alinear en múltiples canales aumenta el tiempo de inicialización del CM, pero la utilización parámetros de ráfaga diferentes para el mantenimiento inicial en nodos de fibra diferentes permite fijar los parámetros que convienen a las condiciones de la planta en un nodo específico.

B.H.2 Sentidos descendentes múltiples y sentidos ascendentes múltiples por segmento de canal

Esta cláusula presenta un conjunto más complejo de ejemplos de CM a los que dan servicio varios canales en sentido descendente y varios canales en sentido ascendente y en donde dichos canales, ascendentes y descendentes, forman parte de un dominio MAC. Se perfila la interacción de mantenimiento inicial, el funcionamiento normal y el cambio de canal dinámico, así como la repercusión de los múltiples canales en sentido descendente que utilizan indicaciones de tiempo sincronizadas o no sincronizadas.

Las indicaciones de tiempo sincronizadas se refieren a ambos trayectos en sentido descendente, que transmiten una indicación de tiempo derivada de la frecuencia de un reloj común y tienen bases de tiempo comunes. No es preciso que las indicaciones de tiempo de cada canal en sentido descendente se transmitan al mismo tiempo para que se consideren sincronizadas.

B.H.2.1 Topología

Supónganse dos canales en sentido descendente utilizados conjuntamente con cuatro canales en sentido ascendente, como se muestra en la figura B.H-2. En las tres topologías, hay dos comunidades geográficas de módems, servidas ambas por los dos mismos canales en sentido descendente. La diferencia entre las topologías se halla en su conectividad en sentido ascendente.

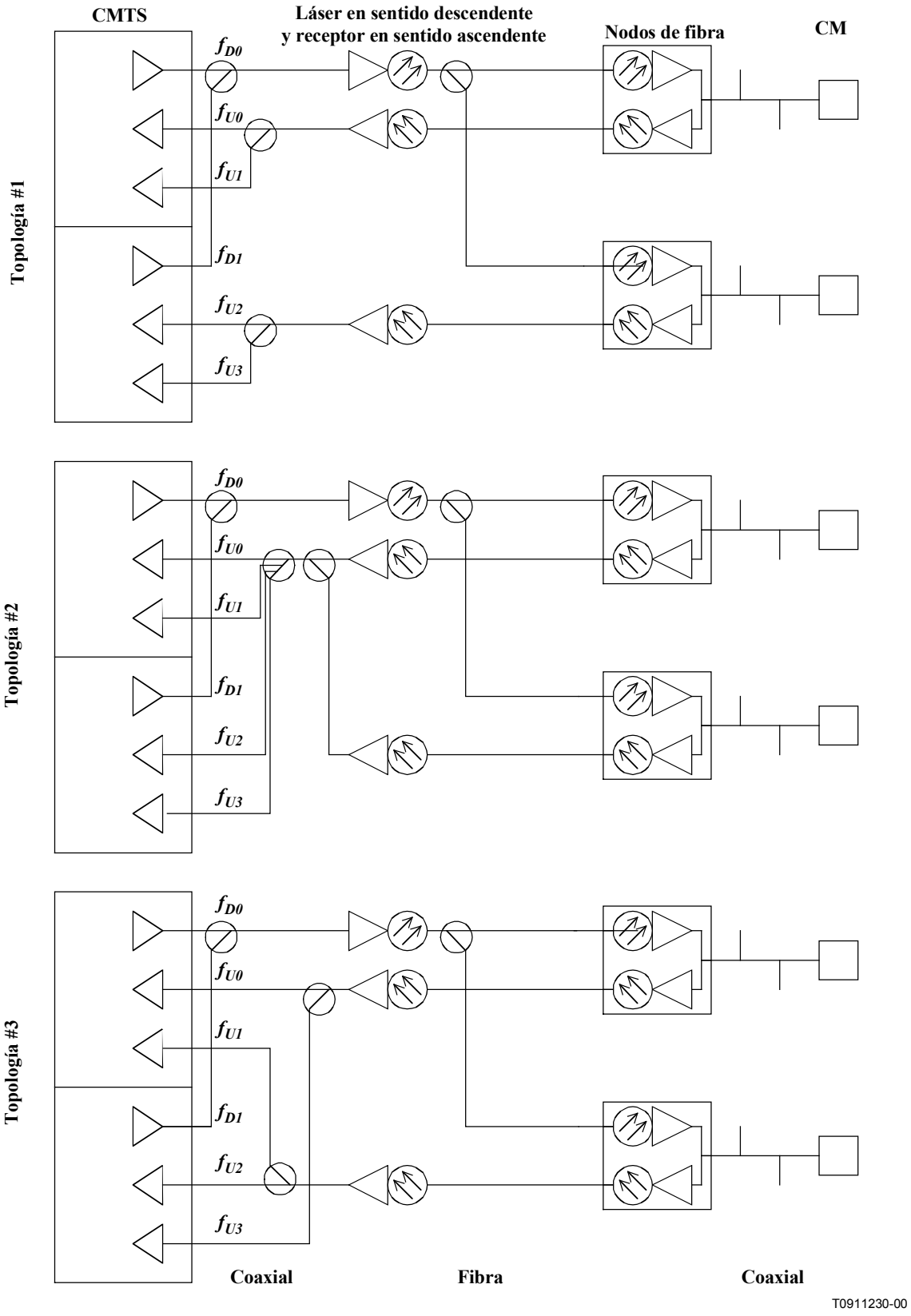


Figura B.H-2/J.112 – Múltiples canales en sentido descendente y múltiples canales en sentido ascendente por módem de cable

En la topología #1, el trayecto de retorno desde cada nodo de fibra se conecta a un conjunto especializado de receptores en sentido ascendente. Un CM verá ambos canales en sentido descendente, pero sólo un canal en sentido ascendente, que está asociado con uno de los dos canales en sentido descendente.

En la topología #2, el trayecto de retorno desde cada nodo de fibra se combina y a continuación se divide entre todos los receptores en sentido ascendente. Un CM verá ambos canales en sentido descendente y los cuatro canales en sentido ascendente utilizados con ambos canales en sentido descendente.

En la topología #3, el trayecto de retorno desde cada nodo de fibra se divide y a continuación se envía a múltiples receptores en sentido ascendente, cada uno de ellos asociado con un canal en sentido descendente diferente. Un CM verá ambos canales en sentido descendente, y un canal en sentido ascendente asociado con cada uno de los dos canales en sentido descendente.

La topología #1 es la que se utiliza normalmente. El desplazamiento entre canales en sentido descendente sólo puede producirse si las indicaciones de tiempo en ambos sentidos descendentes están sincronizadas. La topología #2 y la topología #3 sirven para compensar los canales en sentido descendente que tienen indicaciones de tiempo no sincronizadas, y permiten el desplazamiento entre canales en sentido descendente en tanto en cuanto los canales en sentido ascendente se cambien al mismo tiempo.

Los CM pueden recibir en una única frecuencia y transmitir en una única frecuencia.

B.H.2.2 Funcionamiento normal

El cuadro B.H-1 da la relación de mensajes MAC que contienen ID de canal.

Cuadro B.H-1/J.112 – Mensajes MAC con ID de canal

Mensajes MAC	ID de canal descendente	ID de canal ascendente
UCD	Sí	Sí
MAP	No	Sí
RNG-REQ	Sí	No
RNG-RSP	No	Sí
DCC-REQ	Sí	Sí

Con indicaciones de tiempo no sincronizadas:

- Puesto que la sincronización en sentido ascendente se basa en las indicaciones de tiempo en sentido descendente, cada canal en sentido ascendente debe estar asociado con la indicación de tiempo de uno de los canales en sentido descendente.
- Los canales en sentido descendente sólo deberán transmitir mensajes MAP y mensajes UCD que pertenezcan a sus canales en sentido ascendente asociados.

Con indicaciones de tiempo sincronizadas:

- Puesto que las sincronizaciones en sentido ascendente se puede obtener de cualquiera de los canales en sentido descendente, todos los canales en sentido ascendente pueden estar asociados con cualquiera de los canales en sentido descendente.

- Todos los MAP y los UCD de todos los canales en sentido ascendente deberán ser enviados por todos los canales en sentido descendente. Los mensajes UCD contienen un ID de canal en sentido descendente, de tal manera que el CMTS puede determinar con el mensaje RNG-REQ en qué canal en sentido descendente está el CM. Así pues, los mensajes UCD por cada canal en sentido descendente contendrán ID de canal en sentido descendente diferentes incluso aunque pudieran contener el mismo ID de canal en sentido ascendente.

B.H.2.3 Mantenimiento inicial

Cuando un CM efectúa mantenimiento inicial, se desconoce la topología y no se sabe si las indicaciones de tiempo de los canales en sentido descendente son coherentes entre sí. Por ello, el CM elige uno de los dos canales descendentes y cualquiera de los UCD enviados por ese canal descendente.

En ambos casos:

- Las frecuencias de canal en sentido ascendente dentro de un canal ascendente físico o canales ascendentes físicos combinados deben ser diferentes.
- Son aplicables las limitaciones especificadas en B.H.1.

B.H.2.4 Cambio de canal dinámico

Con indicaciones de tiempo no sincronizadas:

- Cuando se da un DCC-REQ, debe contener nuevos pares de frecuencias en sentido ascendente y en sentido descendente asociadas ambas con la misma indicación de tiempo.
- Cuando el CM se resincroniza con el nuevo canal en sentido descendente, debe permitir la resincronización de las indicaciones de tiempo sin realineación a menos que la instrucción DCC-REQ le indique que lo haga.
- La topología #1 soportará cambios de canal entre canales locales en sentido ascendente presentes dentro de un segmento de cable, pero no admitirá cambios entre canales en sentido descendente. Las topologías #2 y #3 admitirán cambios de canal en sentido ascendente y en sentido descendente en todos los canales dentro del nodo de fibra en tanto en cuanto el nuevo par de canales en sentido ascendente y en sentido descendente estén asociados con la misma indicación de tiempo.

Con indicaciones de tiempo sincronizadas:

- Los cambios de canal en sentido descendente y los cambios de canal en sentido ascendente son independientes entre sí.
- Las topologías #1, #2 y #3 soportarán cambios de canal entre todos los canales en sentido ascendente y todos los canales en sentido descendente presentes dentro del segmento de cable.

ANEXO B.I

Protocolo de árbol abarcante de datos por cable

Según la subcláusula B.5.1.2.1, es preciso utilizar el protocolo de árbol abarcante en los CM de uso comercial y en los CMTS de puenteo. Este anexo B.I describe cómo se adapta el protocolo de árbol abarcante IEEE 802.1D al funcionamiento de los sistemas de datos por cable.

B.I.1 Antecedentes

A menudo se utiliza un protocolo de árbol abarcante en una red puenteada para desactivar conexiones de red redundantes; es decir, para reducir una topología de red en malla arbitraria a una topología activa que es un árbol enraizado que abarca todos los segmentos de la red. El algoritmo y el protocolo de árbol abarcante no deberán confundirse con la propia función de retransmisión de datos; la retransmisión de datos puede aplicar reglas transparentes de aprendizaje del puenteo, o emplear cualquiera de otros varios mecanismos. Desactivando conexiones redundantes, el protocolo de árbol abarcante elimina los bucles topológicos, que de otra manera provocarían el que se retransmitieran para siempre los paquetes de datos de muchos tipos de dispositivos de retransmisión.

Se emplea un protocolo de árbol abarcante normalizado [IEEE 802.1D] en la mayoría de las redes de área local puenteadas. El destino previsto en principio para este protocolo eran las redes de área local privadas y requiere algunas modificaciones para utilizarlo con datos por cable.

B.I.2 Árbol abarcante público

Para utilizar un protocolo de árbol abarcante en una red de acceso público, tal como la de datos por cable, es preciso introducir algunas modificaciones en el proceso [IEEE 802.1D] básico. En primer lugar, el árbol abarcante público debe aislarse de cualesquiera redes de árbol abarcante privadas con las que esté conectado. Se trata con ello de proteger tanto la red de cable pública como cualquier red privada conectada. La figura B.I-1 ilustra la topología general.

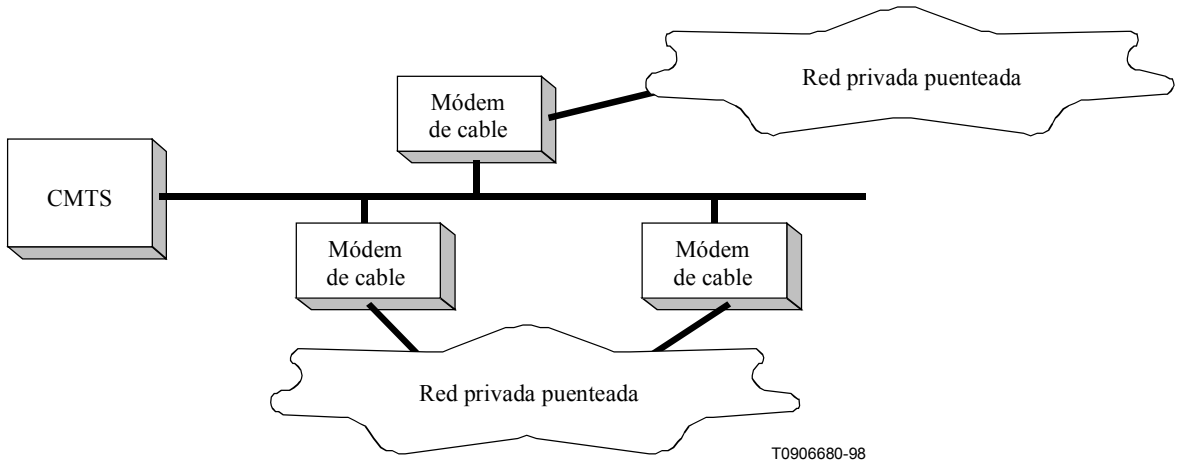


Figura B.I-1/J.112 – Topología de árbol abarcante

El cometido del protocolo de árbol abarcante público, con referencia a la figura B.I-1, es como sigue:

- Aislar las redes puenteadas privadas unas de otras. Si las dos redes privadas combinan sus árboles abarcantes, cada una de ellas está sujeta a las inestabilidades de la otra. Además, el árbol combinado puede exceder rebasar el diámetro de puenteo permisible máximo.
- Aislar la red pública de los árboles abarcantes de las redes privadas. La red pública no debe estar sujeta a las inestabilidades inducidas por las redes de los clientes ni ha de cambiar las características del árbol abarcante de las redes de los clientes.
- Inhabilitar uno de los dos enlaces redundantes que conectan con la red de cable, para evitar los bucles de reenvío. Esto deberá tener lugar en el módem de cable, más bien que en un puente cualquiera dentro de la red del cliente.

El protocolo de árbol abarcante debe atenerse además a la topología ilustrada en la figura B.I-2:

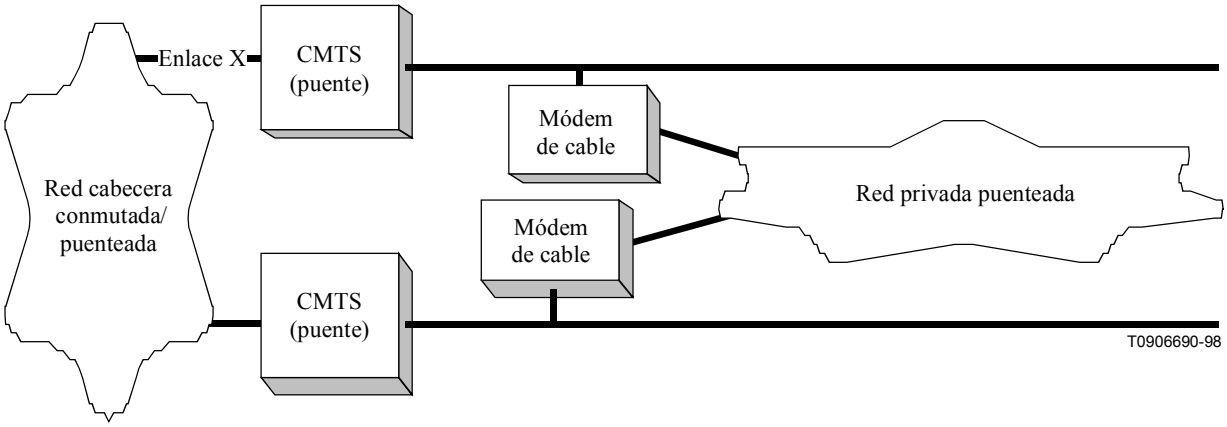


Figura B.I-2/J.112 – Árbol abarcante a través de los CMTS

En la figura B.I-2, en funcionamiento normal, el protocolo de árbol abarcante deberá desactivar un enlace en uno de los dos módems de cable. No deberá desviar tráfico a través de la red privada. Se señala que en algunas circunstancias, tales como la desactivación del enlace X, el árbol abarcante *desviará* tráfico hacia la red privada (aunque los límites impuestos a las direcciones MAC aprendidas probablemente representen un estrangulamiento del tráfico de tránsito). Si ese desvío no es conveniente, debe evitarse por medios externos al árbol abarcante; por ejemplo, utilizando encaminadores.

B.I.3 Detalles del protocolo de árbol abarcante público

El algoritmo y protocolo de árbol abarcante de datos por cable es idéntico al definido en [IEEE 802.1D], con las siguientes salvedades:

- Cuando se transmiten unidades de protocolo de puente de configuración (BPDU, *bridge protocol data units*), se usa la dirección de multidifusión de árbol abarcante de datos por cable 01-E0-2F-00-00-03 en vez de la definida en IEEE 802.1D. Estas BPDU serán retransmitidas en vez de calculadas de nuevo por puentes IEEE 802.1D ordinarios.
- Cuando se transmiten BPDU de configuración, se DEBE utilizar el encabezamiento SNAP AA-AA-03-00-E0-2F-73-74 en vez del encabezamiento LLC 42-42-03 empleado por IEEE 802.1D. Con ello se trata de diferenciar más aún estas BPDU de las utilizadas por los puentes IEEE 802.1D, en el caso de que algunos de esos puentes no identifiquen correctamente direcciones MAC de multidifusión (véase la nota).

  NOTA – Es probable que exista un cierto número de puentes de árbol abarcante instalados que se basen únicamente en los LSAP para distinguir paquetes 802.1D. Tales dispositivos no funcionarán correctamente si las BPDU de datos por cable utilizan también LSAP = 0x42.
- Se DEBE hacer caso omiso de las BPDU de IEEE 802.1D, que se descartan de manera silenciosa.
- Las PDU de notificación de cambio de topología (TCN, *topology change notification*) no DEBEN ser transmitidas (ni procesadas). Las TCN se utilizan en las redes IEEE para acelerar el envejecimiento de la base de datos de aprendizaje cuando la topología de la red pueda haber cambiado. Puesto que el mecanismo de aprendizaje de la red de cable difiere normalmente, este mensaje no es necesario y puede dar lugar a un desbordamiento innecesario.
- Los CMTS que funcionen a modo de puente deben participar en este protocolo y se les han de asignar prioridades superiores (probablemente sean raíces) a las de los módems de cable. A la interfaz NSI del CMTS se le DEBERÍA asignar un coste de puerto equivalente a una velocidad de enlace de por lo menos 100 Mbit/s. Estas dos condiciones juntas deberán asegurarse que:

1) la raíz es un CMTS; y

2) cualquier otro CMTS utilizará la red cabecera en vez de una red de cliente para alcanzar la raíz.

- El retransmisor MAC del CMTS DEBE retransmitir las BPDU de los canales en sentido ascendente a los canales en sentido descendente, con independencia de que el CMTS esté o no dando servicio como encaminador o como puente.

Se señala que los CM con este protocolo habilitado transmitirán BPDU por las redes de abonado para identificar otros CM en la misma red de abonado. Estas BPDU de árbol abarcante público serán transportadas transparentemente por cualquier red de abonado privada puenteada. De manera similar, los CMTS puenteantes transmitirán BPDU por la interfaz NSI así como por la interfaz RFI. La dirección de multidifusión y el encabezamiento SNAP definido más arriba se utilizan en todos los enlaces.

B.I.4 Parámetros y valores por defecto de árbol abarcante

La subcláusula B.4.10.2 de [IEEE 802.1D] especifica un cierto número de valores de parámetros recomendados. Deberán utilizarse dichos valores, con las excepciones que se indican a continuación.

Coste de trayecto

En [IEEE 802.1D], se utiliza la siguiente fórmula:

Coste de trayecto = 1000/Velocidad de LAN conectada en Mbit/s

Para los CM, esta fórmula se convierte en:

Coste de trayecto = 1000/(Velocidad de símbolos en sentido ascendente ∗ bits por símbolo para concesión de datos larga)

Es decir, el tipo de modulación (QPSK o 16QAM) del código de utilización de intervalo (IUC) de una concesión de datos larga se multiplica por la velocidad de símbolos en bruto para determinar el coste de trayecto nominal. El cuadro B.I-1 indica los valores obtenidos.

Cuadro B.I-17J.112 – Coste de trayecto de CM

Velocidad de símbolos	Coste de trayecto por defecto	
ksímb/s	QPSK	16QAM
160	3125	1563
320	1563	781
640	781	391
1280	391	195
2560	195	98

Para los CMTS, la fórmula es como sigue:

Coste de trayecto = 1000/(Velocidad de símbolos en sentido descendente ∗ bits por símbolo)

Prioridad de puente

La prioridad de puente de los CM DEBERÍA tomar por defecto el valor de 36 864 (0x9000). Con ello se pretende sesgar la red de modo que la raíz no tienda a estar en el CMTS. El CMTS DEBERÍA tomar por defecto el valor 32 768, según IEEE 802.1D.

Se señala que ambas recomendaciones afectan únicamente a las fijaciones *por defecto*. Estos parámetros, así como otros definidos en IEEE 802.1D, DEBERÍAN ser gestionables en toda su gama de valores mediante el objeto MIB puente ([RFC 1493]) o por otros medios.

ANEXO B.J

Códigos y mensajes de error

Se trata de códigos y mensajes de error de CM y CMTS (véase el cuadro B.J-1). Estos códigos de error pretenden emular la manera normalizada según la cual la RDSI informa de condiciones de error con independencia del fabricante del equipo.

Los errores notificados son pérdida de sincronización, UCD, MAP, REQ/RSP de alineación, UCC, registro, petición de servicio dinámico y fallos de DHCP/TFTP. En algunos casos hay un informe detallado del error y en otros se indica simplemente "fallo".

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
T00.0	**Sincronización de temporización SYNC**
T01.0	No se consigue la temporización de símbolos QAM/QPSK. ¿Situación de error? ¿# de reintentos?
T02.0	No se consigue alineación de trama FEC. ¿Situación de error? ¿Reintento #? ¿# de tramas erróneas?
T02.1	Conseguida alineación de trama FEC. No se consigue sincronización MPEG2. ¿# de reintentos?
T03.0	No se consigue alineación de trama MAC. ¿Situación de error? ¿Reintento #? ¿# de tramas erróneas?
T04.0	Falla recepción de trama SYNC MAC durante el periodo de temporización.
T05.0	Pérdida de sincronización (se pierden 5 seguidos, después de SYNC una vez).
U00.0	**Descriptor de canal en sentido ascendente UCD**
U01.0	No se reciben UCD. Temporización transcurrida.
U02.0	UCD no válido o canal no utilizable.
U03.0	UCD válido, PERO SYNC no recibido. TEMPORIZACIÓN TRANSCURRIDA.
U04.0	UCD, y SYNC válidos, NO MAPS para ESTE canal.
U05.0	UCD recibido con cuenta de cambios de configuración no válida o en desorden.
U06.0	Parámetros que afectan a todo el canal en sentido ascendente no fijados antes de descriptores de ráfaga.
M00.0	**Atribución de anchura de banda en sentido ascendente MAP**
M01.0	Perdida oportunidad de transmisión porque el MAP llegó demasiado tarde.
R00.0	**Petición de alineación RNG-REQ**
R01.0	NO se reciben multidifusiones de mantenimiento para oportunidades de alineación recibidas. Temporización de T2 transcurrida.
R04.0	Recibida respuesta a petición de mantenimiento de multidifusión, pero no recibidas oportunidades de mantenimiento unidifusión. Temporización de T4 transcurrida.
R101.0	No se reciben peticiones de alineación del CM INTERROGADO secuencialmente (interrogaciones generadas por el CMTS).
R102.0	Agotados reintentos para CM interrogado secuencialmente (notificación de dirección MAC). Después de 16 errores R101.0.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
R103.0	Incapaz de alinear CM satisfactoriamente (informe de dirección MAC). Reintentos agotados. NOTA – Este error difiere del R102.0 ya que pudo intentar, es decir, obtener REQ pero no alineó adecuadamente.
R104.0	No se recibe RNG-REQ periódico procedente del módem (SID X). SID de temporización transcurrida.
R00.0	**Respuesta de alineación RNG-RSP**
R02.0	No se recibe respuesta de alineación. Temporización de T3 transcurrida.
R03.0	Agotados reintentos de petición de alineación.
R05.0	Iniciada alineación de mantenimiento unidifusión sin recibir respuesta. Temporización de T3 transcurrida.
R06.0	Intentada alineación de mantenimiento unidifusión. Sin respuesta. Reintentos agotados.
R07.0	Alineación unidifusión recibe respuesta de aborto. MAC de reinicialización.
I00.0	**Petición de registro REG-REQ**
I04.0	Servicio no disponible. Motivo: otro.
I04.1	Servicio no disponible. Motivo: fijación de configuración no reconocida.
I04.2	Servicio no disponible. Motivo: indisponibilidad temporal.
I04.3	Servicio no disponible. Motivo: indisponibilidad permanente.
I05.0	Registro rechazado. Fallo de autenticación: MIC CMTS no válido.
I101.0	Encabezamiento MAC no válido.
I102.0	SID no válido, no utilizado.
I103.0	TLV requeridos en desorden.
I104.0	TLV requeridos no presentes.
I105.0	Formato de frecuencia en sentido descendente no válido.
I105.1	Frecuencia en sentido descendente no utilizada.
I105.2	Frecuencia en sentido descendente no válida, no es múltiplo de 62 500 Hz.
I106.0	Canal en sentido ascendente no válido, no asignado.
I106.1	Cambio del canal en sentido ascendente seguido de REQ de registro (RE-).
I107.0	Canal en sentido ascendente sobrecargado.
I108.0	Configuración acceso a la red tiene parámetro no válido.
I109.0	Configuración clase de servicio no válida.
I110.0	ID de clase de servicio no soportado.
I111.0	ID de clase de servicio no válido o fuera de gama.
I112.0	Formato de configuración velocidad binaria en sentido descendente máxima no válido.
I112.1	Fijación de configuración velocidad binaria en sentido descendente máxima no soportada.
I113.0	Formato de fijación de configuración velocidad binaria en sentido ascendente máxima no válido.
I113.1	Fijación de configuración velocidad binaria en sentido ascendente máxima no soportada.
I114.0	Formato de configuración prioridad en sentido ascendente no válido.
I114.1	Fijación de configuración prioridad en sentido ascendente fuera de gama.
I115.0	Formato de fijación de configuración velocidad binaria de canal en sentido ascendente mínima garantizada no válido.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
I115.1	Fijación de la configuración velocidad binaria de canales en sentido ascendente mínima garantizada excede de la velocidad binaria en sentido ascendente máxima.
I115.2	Fijación de configuración velocidad binaria de canal en sentido ascendente mínima garantizada fuera de gama.
I116.0	Formato de fijación de configuración ráfaga de transmisión por canal en sentido ascendente máxima no válido.
I116.1	Fijación de configuración ráfaga de transmisión por canal de sentido ascendente máxima fuera de gama.
I117.0	Formato de fijación de configuración capacidades del módem no válido.
I117.1	Fijación de configuración capacidades del módem
I200.0	**Petición de registro REG-REQ específico de la versión 1.1**
I201.0	Registro rechazado, motivo no especificado.
I201.1	Registro rechazado, fijación de configuración no reconocida.
I201.2	Registro rechazado, sin recurso temporalmente.
I201.3	Registro rechazado, rechazo administrativo permanente.
I201.4	Registro rechazado, parámetro requerido no presente.
I201.5	Registro rechazado, fijación supresión encabezamiento no soportada.
I201.6	Registro rechazado, errores múltiples.
I201.7	Registro rechazado, ID de referencia o índice en mensaje duplicado.
I201.8	Registro rechazado, parámetro no válido para el contexto.
I201.9	Registro rechazado, fallo de autorización.
I201.10	Registro rechazado, error de flujo de servicio importante.
I201.11	Registro rechazado, error de clasificador importante.
I201.12	Registro rechazado, error de regla PHS importante.
I201.13	Registro rechazado, múltiples errores importantes.
I201.14	Registro rechazado, error de sintaxis de mensaje.
I201.15	Registro rechazado, error de flujo de servicio primario
I201.16	Registro rechazado, mensaje demasiado grande.
I00.0	**Respuesta de registro RG-RSP**
I01.0	Formato de RESP de registro no válido o no reconocido
I02.0	RESP de registro no recibido.
I03.0	RESP de registro con SID erróneo.
I250.0	**Respuesta de registro REG-RESP específico de la versión 1.1**
I251.0	RSP de registro contiene parámetros de flujo de servicio que el CM no puede soportar.
I251.1	RSP de registro contiene parámetros de clasificador que el CM no puede soportar.
I251.2	RSP de registro contiene parámetros de PHS que el CM no puede soportar.
I251.3	Rechazado RSP de registro, motivo no especificado.
I251.4	Rechazado RSP de registro, error de sintaxis de mensaje.
I251.5	Rechazado RSP de registro, mensaje demasiado grande.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
I300.0	**Acuse de registro REG-ACK**
I301.0	Registro abortado, no REG-ACK.
I302.0	ACK de registro rechazado, motivo no especificado.
I303.0	ACK de registro rechazado, error de sintaxis de mensaje.
C00.0	**Petición de cambio de canal en sentido ascendente UCC-REQ**
C01.0	UCC-REQ recibido con ID de canal en sentido ascendente no válido o fuera de gama.
C02.0	UCC-REQ recibido incapaz de enviar UCC-RSP, ninguna oportunidad de transmitir.
C100.0	**Respuesta de cambio de canal en sentido ascendente UCC-RSP**
C101.0	UCC-RSP no recibido en ID de canal previo.
C102.0	UCC-RSP recibido con ID de canal no válido.
C103.0	UCC-RSP recibido con ID de canal no válido en canal nuevo.
D00.0	**Telecarga de configuración red de CM de DHCP y hora del día**
D01.0	Descubrimiento enviado sin oferta recibida, servidor DHCP no disponible.
D02.0	Petición enviada, sin respuesta.
D03.0	Información pedida no soportada.
D03.1	Respuesta DHCP no contiene todos los campos válidos como se describe en la especificación de RF del anexo B.D.
D04.0	Hora del día, no fijada o datos no válidos.
D04.1	Petición de hora del día enviada, respuesta no recibida.
D04.2	Respuesta de hora del día recibida pero datos/formato no válidos.
D05.0	Petición TFTP enviada, sin respuesta/sin servidor.
D06.0	Petición TFTP fallida, fichero de la configuración NO ENCONTRADO.
D07.0	TFTP fallido, paquetes DESORDENADOS.
D08.0	TFTP completo, pero verificación de la integridad fallida (MIC).
S00.0	**Peticiones de servicio dinámicas**
S01.0	Adición de servicio rechazada, motivo no especificado.
S01.1	Adición de servicio rechazada, fijación de configuración no reconocida.
S01.2	Adición de servicio rechazada, ausencia de recursos temporal.
S01.3	Adición de servicio rechazada, rechazo administrativo permanente.
S01.4	Adición de servicio rechazada, parámetro requerido no presente.
S01.5	Adición de servicio rechazada, fijación de supresión de encabezamiento no soportada.
S01.6	Adición de servicio rechazada, existe flujo de servicio.
S01.7	Adición de servicio rechazada, fallo de autenticación de HMAC.
S01.8	Adición de servicio rechazada, adición abortada.
S01.9	Adición de servicio rechazada, múltiples errores.
S01.10	Adición de servicio rechazada, clasificador no encontrado.
S01.11	Adición de servicio rechazada, existe clasificador.
S01.12	Adición de servicio rechazada, regla del PHS no encontrada.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
S01.13	Adición de servicio rechazada, regla del PHS existe.
S01.14	Adición de servicio rechazada, ID de referencia o índice en mensaje duplicado.
S01.15	Adición de servicio rechazada, múltiples flujos en sentido ascendente.
S01.16	Adición de servicio rechazada, múltiples flujos en sentido descendente.
S01.17	Adición de servicio rechazada, clasificador para otro flujo de servicio.
S01.18	Adición de servicio rechazada, regla de PHS para otro flujo de servicio.
S01.19	Adición de servicio rechazada, parámetro no válido para el contexto.
S01.20	Adición de servicio rechazada, fallo de autorización.
S01.21	Adición de servicio rechazada, error de flujo de servicio importante.
S01.22	Adición de servicio rechazada, error de clasificador importante.
S01.23	Adición de servicio rechazada, error de regla de PHS importante.
S01.24	Adición de servicio rechazada, múltiples errores importantes.
S01.25	Adición de servicio rechazada, error de sintaxis de mensaje.
S01.26	Adición de servicio rechazada, mensaje demasiado grande.
S01.27	Adición de servicio rechazada, DCC temporal.
S02.0	Cambio de servicio rechazado, motivo no especificado.
S02.1	Cambio de servicio rechazado, fijación de configuración no reconocida.
S02.2	Cambio de servicio rechazado, ausencia de recurso temporal.
S02.3	Cambio de servicio rechazado, rechazo administrativo permanente,
S02.4	Cambio de servicio rechazado, solicitante no es propietario de flujo de servicio.
S02.5	Cambio de servicio rechazado, flujo de servicio no encontrado.
S02.6	Cambio de servicio rechazado, parámetro requerido no está presente.
S02.7	Cambio de servicio rechazado, múltiples errores.
S02.8	Cambio de servicio rechazado, clasificador no encontrado.
S02.9	Cambio de servicio rechazado, existe clasificador.
S02.10	Cambio de servicio rechazado, regla de PHS no encontrada.
S02.11	Cambio de servicio rechazado, regla de PHS existe.
S02.12	Cambio de servicio rechazado, ID de referencia o índices en mensajes duplicado.
S02.13	Cambio de servicio rechazado, múltiples flujos en servicio ascendente.
S02.14	Cambio de servicio rechazado, múltiples flujos en sentido descendente.
S02.15	Cambio de servicio rechazado, clasificador para otro flujo de servicio.
S02.16	Cambio de servicio rechazado, regla de PHS para otro flujo de servicio.
S02.17	Cambio de servicio rechazado, parámetro no válido para el contexto.
S02.18	Cambio de servicio rechazado, fallo de autorización.
S02.19	Cambio de servicio rechazado, error de flujo de servicio importante.
S02.20	Cambio de servicio rechazado, error de clasificador importante.
S02.21	Cambio de servicio rechazado, error de regla de PHS importante.
S02.22	Cambio de servicio rechazado, múltiples errores importantes.
S02.23	Cambio de servicio rechazado, error de sintaxis de mensaje.
S02.24	Cambio de servicio rechazado, mensaje demasiado grande.
S02.25	Cambio de servicio rechazado, DCC temporal.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
S02.26	Cambio de servicio rechazado, fijación de supresión de encabezamiento no soportada.
S02.27	Cambio de servicio rechazado, fallo de autenticación de HMAC.
S03.0	Supresión de servicio rechazada, motivo no especificado.
S03.1	Supresión de servicio rechazada, solicitante no es propietario de flujo de servicio.
S03.2	Supresión de servicio rechazada, flujo de servicio no encontrado.
S03.3	Supresión de servicio rechazada, fallo de autenticación de HMAC.
S03.4	Supresión de servicio rechazada, error de sintaxis de mensaje.
S100.0	**Respuestas de servicio dinámicas**
S101.0	Respuesta de adición de servicio rechazada, ID de transacción no válido.
S101.1	Adición de servicio abortada, no RSP.
S101.2	Respuesta de adición de servicio rechazada, fallo de autenticación de HMAC.
S101.3	Respuesta de adición de servicio rechazada, error de sintaxis de mensaje.
S102.0	Respuesta de cambio de servicio rechazada, ID de transacción no válido.
S102.1	Cambio de servicio abortado, no RSP.
S102.2	Respuesta de cambio de servicio rechazada, fallo de autenticación de HMAC.
S102.3	Respuesta de cambio de servicio rechazada, error de sintaxis de mensaje.
S103.0	Respuesta de supresión de servicio rechazada, ID de transacción no válido.
S200.0	**Acuse de recibo de servicio dinámico**
S201.0	ACK de adición de servicio rechazado, ID de transacción no válido.
S201.1	Adición de servicio abortada, no ACK.
S201.2	ACK de adición de servicio rechazado, fallo de autenticación de HMAC.
S201.3	ACK de adición de servicio rechazado, error de sintaxis de mensaje.
S202.0	ACK de cambio de servicio rechazado, ID de transacción no válido.
S202.1	Cambio de servicio abortado, no ACK.
S202.2	ACK de cambio de servicio rechazado, fallo de autenticación de HMAC.
S202.3	ACK de cambio de servicio rechazado, error de sintaxis de mensaje.
C200.0	**Petición de cambio de canal dinámica**
C201.0	DCC rechazado ya presente.
C202.0	Partida de DCC antiguo.
C203.0	Llegada de DCC nuevo.
C204.0	DCC abortado, imposibilidad de conseguir nuevo canal en sentido descendente.
C205.0	DCC abortado, no UCD para nuevo canal en sentido ascendente.
C206.0	DCC abortado, imposibilidad de comunicar por el nuevo canal en sentido ascendente.
C207.0	DCC rechazado, motivo no especificado.
C208.0	DCC rechazo permanente, DCC no soportado.
C209.0	DCC rechazado, flujo de servicio no encontrado.
C210.0	DCC rechazado, parámetro requerido no está presente.
C211.0	DCC rechazado, fallo de autenticación.

Cuadro B.J-1/J.112 – Códigos de error para mensajes de gestión MAC

Código de Error	Mensaje de Error
C212.0	DCC rechazado, múltiples errores.
C213.0	DCC rechazado, clasificador encontrado.
C214.0	DCC rechazado, regla de PHS no encontrada.
C215.0	DCC rechazado, ID de referencia o índice en mensajes duplicado.
C216.0	DCC rechazado, parámetro no válido para el contexto.
C217.0	DCC rechazado, error de sintaxis de mensaje.
C218.0	DCC rechazado, mensaje demasiado grande.
C300.0	**Respuesta de cambio de canal dinámica**
C301.0	DCC-RSP no recibido por el canal antiguo
C302.0	DCC-RSP no recibido por el canal nuevo.
C303.0	DCC-RSP rechazado, motivo no especificado.
C304.0	DCC-RSP rechazado, ID de transacción desconocido.
C305.0	DCC-RSP rechazado, fallo de autenticación.
C306.0	DCC-RSP rechazado, error de sintaxis de mensaje.
C400.0	**Acuse de recibo de cambio de canal dinámico**
C401.0	DCC-ACK no recibido.
C402.0	DCC-ACK rechazado, motivo no especificado.
C403.0	DCC-ACK rechazado, ID de transacción desconocido.
C404.0	DCC-ACK rechazado, fallo de autenticación.
C405.0	DCC-ACK rechazado, error de sintaxis de mensaje.
B00.0	**Privacidad básica**
B01.0	Por determinar.

ANEXO B.K

Transmisión y resolución de contiendas DOCSIS

(Este anexo es informativo)

B.K.1 Introducción

La presente cláusula trata de aclarar cómo funcionan los algoritmos de transmisión y resolución de contiendas de DOCSIS. Se hacen en ella algunas simplificaciones de orden menor y se establecen algunas hipótesis, pero contribuirá de manera decisiva a aclarar este campo de la especificación.

En este ejemplo se hacen algunas simplificaciones:

- No se habla de manera explícita sobre llegadas de paquetes mientras se aplazan o se esperan las concesiones pendientes y no es muy preciso sobre el dimensionamiento del transporte en remolque o porteo.
- Gran parte de lo que aquí se indica en aplicable con concatenación, pero no se pretende tratar todas las sutilezas de esa situación.

En el ejemplo se establecen además algunas hipótesis:

- Se supone que una petición se adapta siempre a cualquier región de petición/datos.
- Cuando se envía una petición de porteo con un paquete de datos de contienda, la máquina de estados sólo verifica la concesión de la petición y supone que el acuse de datos del paquete de datos de la contienda fue suministrado por el CMTS.
- Se suponen probablemente algunas otras cosas, pero con lo anterior basta para asegurar los puntos básicos.

Véase la figura B.K-1.

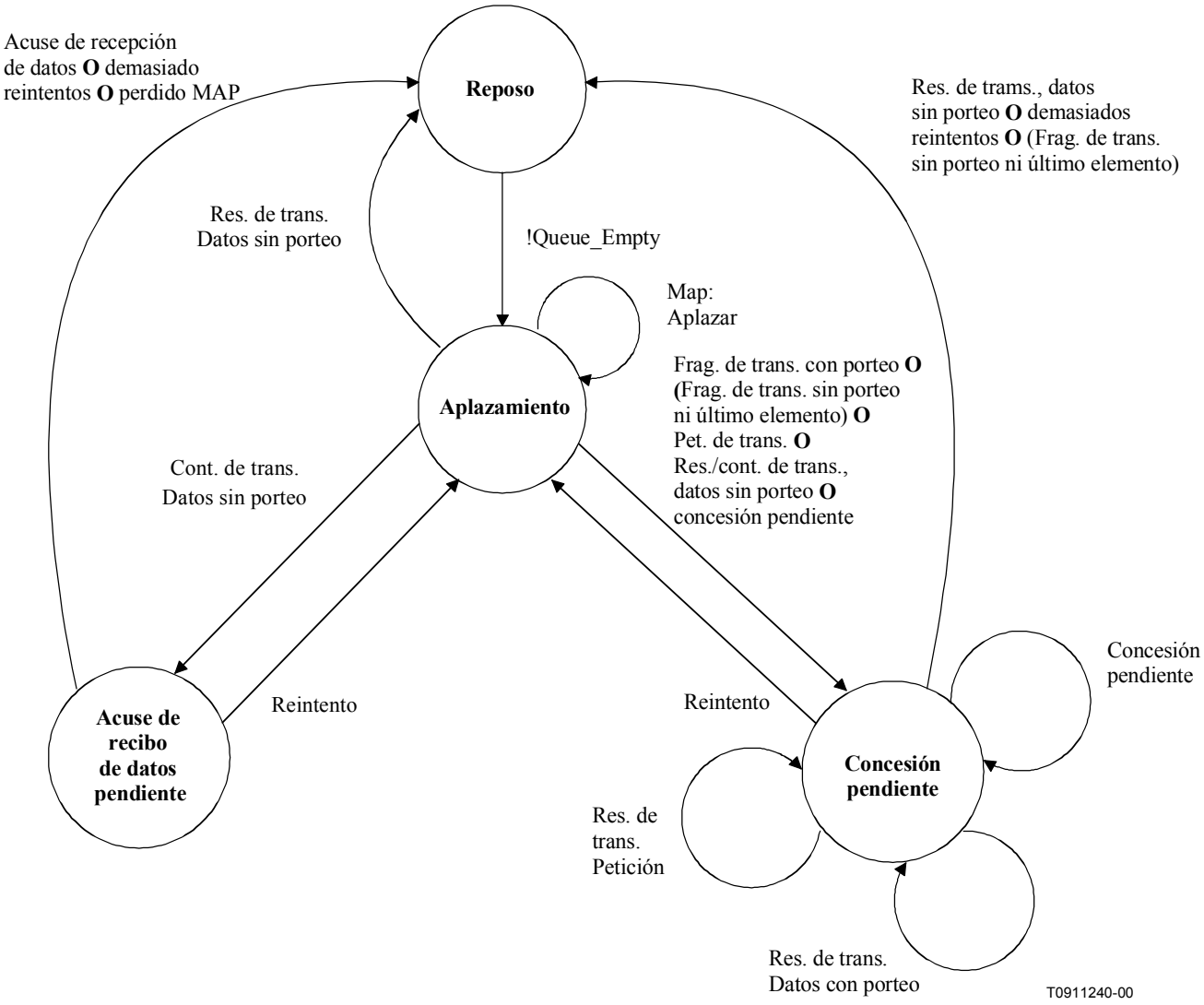


Figura B.K-1/J.112 – Diagrama de transición de estados de transmisión y aplazamiento

Definición de variables

Start	Campo comienzo de retroceso de datos desde Map "actualmente en vigor"
End	Campo final de retroceso de datos desde Map "actualmente en vigor"
Window	Ventana de retroceso actual
Random[n]	Generador de números aleatorios que selecciona un número entre 0 y n – 1
Defer (Aplazar)	Número de oportunidades de transmisión que hay que aplazar antes de transmitir
Retries	Número de transmisiones intentadas sin resolución
Tx_time	Hora de la transmisión de petición o petición/datos conservada
Ack_time	Campo hora de acuse de recibo del Map actual
Piggyback (Porteo)	Bandera fijada cuando se añade un "piggyback REQ" (mensaje de petición de porteo) a un paquete de transmisión
Queue_Empty	Bandera que se fija cuando la cola de datos para este SID está vacía
Lost_Map	Bandera que se fija cuando se pierde un MAP y se está en estado de acuse de recibo de datos pendiente
my_SID	ID de servicio de la cola que tiene un paquete para transmitir
pkt size (tamaño de paquete	Tamaño del paquete de datos incluyendo tara de capa física y MAC (así como porteo si se utiliza)
frag_size	Tamaño de fragmento
Tx_Mode	{Full_Pkt; First_Frag; Middle_Frag; Last_Frag}
min_frag	Tamaño de fragmento mínimo

Estado: Reposo (Idle) – En espera de un paquete para transmitir

```
Window = 0;
Retries = 0;
Wait for !Queue_Empty;        /* paquete disponible para transmitir */

CalcDefer();
go to Deferring
```

Estado: Pendiente acuse de recibo de datos (Data Ack Pending) – En espera de acuse de recibo de datos solamente

```
Wait for next Map;

if (Data Acknowledge SID == my_SID) /* ¡Éxito!, el CMTS recibió el paquete de
datos */
       go to state Idle;
else if (Ack_time > Tx_time)        /* !COLISIÓN!!! o paquete perdido o Map
                                       perdido */
       {
       if (Lost_Map)
          go to state Idle;         /* Suponer que se acusó recibo del paquete
                                       para evitar el envío de duplicados */

          else
             Retry();
       }

stay in state Data Ack Pending;
```

Estado: Concesión pendiente (Grant Pending) – En espera de una concesión

```
Wait for next Map;
while (Grant SID == my_SID)
       UtilizeGrant();
if (Ack_time > Tx_time)             /* !COLISIÓN!!!! o petición denegada/perdida
o Map */
       Retry();
stay in state Grant Pending
```

Estado: Aplazamiento (Deferring) – Determinar el momento oportuno para la transmisión y transmitir

```
if (Grant SID == my_SID)                  /* Concesión no solicitada */
       {
       UtilizeGrant();
       }
else if (unicast Request SID == my_SID)   /* Petición de unidifusión no
                                             solicitada */
       {
       transmit Request in reservation;
       Tx_time = time;

       go to state Grant Pending;
       }
else
       {
       for (each Request or Request/Data Transmit Opportunity)
          {
          if (Defer != 0)
             Defer = Defer - 1;                /* Mantener desplazamiento hasta
                                                  que Defer = 0 */
          else
             {
             if (Request/Data tx_op) and
             (Request/Data size >= pkt size)          /* Enviar datos en
                                                         contienda */
                {
                transmit data pkt in contention;
                Tx_time = time;
                if (Piggyback)
                  go to state Grant Pending;
                else
                  go to state Data Ack Pending;
                }
             else                          /* Enviar petición en contienda */
                {
                transmit Request in contention;
                Tx_time = time;
                go to state Grant Pending;
                }
             }
          }
       }

Wait for next Map;
stay in state Deferring
```

Función: CalcDefer() – Determinar el valor de Defer

```
if (Window < Start)
       Window = Start;

if (Window > End)
       Window = End;
Defer = Random[2^Window];
```

Función: UtilizeGrant() – Determinar el mejor empleo de una concesión

```
if (Grant size >= pkt size)         /* CM puede enviar un paquete completo */
       {
       transmit packet in reservation;
       Tx_time = time;
       Tx_mode = Full_pkt

       if (Piggyback)
          go to state Grant Pending
       else
          go to state Idle;
       }
else if (Grant size < min_frag && Grant Size > Request size)      /* No puede
enviar un fragmento, pero puede enviar una petición */
       {
       transmit Request in reservation;
       Tx_time = time;

       go to state Grant Pending;
       }
else if (Grant size == 0)                  /* Concesión pendiente */
       go to state Grant Pending;
else
       {
       while (pkt_size > 0 && Grant SID == my_SID)
          {

          if (Tx_mode == Full_Pkt)
             Tx_mode = First_frag;
          else
             Tx_mode = Middle_frag;
          pkt_size = pkt_size – frag_size;

          if (pkt_size == 0)
             Tx_mode = Last_frag;
          if (another Grant SID == my_SID)      /* Modo concesiones múltiples */
             piggyback_size = 0
          else
             piggyback_size = pkt_size          /* modo porteo */

          if (piggyback_size > 0)
             transmit fragment with piggyback request for remainder of packet in
reservation
          else
             transmit fragment in reservation;
          }

       go to state Grant Pending;
```

Función: Retry()

```
Retries = Retries + 1;
if (Retries > 16)
      {
      discard pkt, indicate exception condition
      go to state Idle;
      }

Window = Window + 1;

CalcDefer();

go to state Deferring;
```

ANEXO B.L

Ejemplo de IGMP

En la subcláusula B.5.3.1 se definen los requisitos para que un CMTS y un CM soporten la señalización IGMP. El presente anexo da más detalles sobre el soporte de IGMP por un CM.

El proceso definido PUEDE ser soportado por CM conformes. Véase la figura B.L-1.

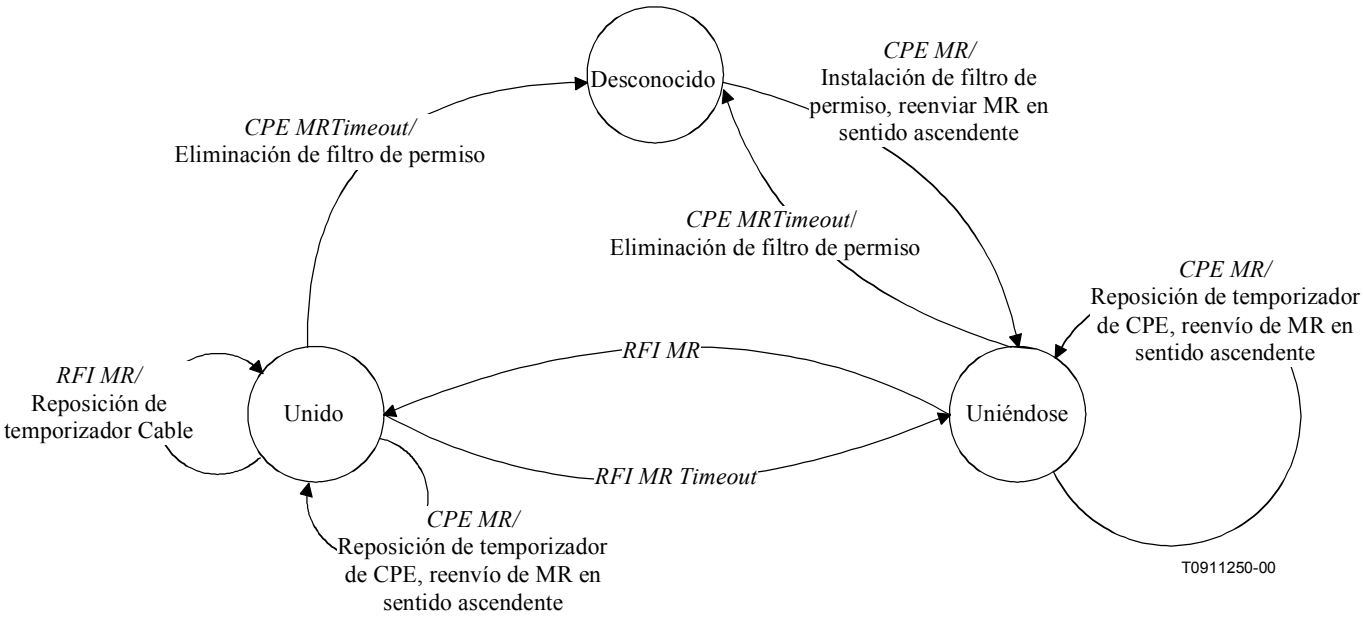


Figura B.L-1/J.112 – Soporte de IGMP-CM

B.L.1 Eventos de transición

Véase el cuadro B.L-1.

Cuadro B.L-1/J.112 – Tabla de eventos

Evento	Estado		
	1 Desconocido	**2 Uniéndose**	**3 Unido**
A) CpeMR	Uniéndose	Uniéndose	Unido
B) RFI MR		Unido	Unido
C) RFI MRTimeout			Uniéndose
D) CpeMRTimeout		Desconocido	Desconocido

1A

- Reenvío de informe de pertenencia como miembro (MR, *membership report*) en sentido ascendente.
- Arranque del temporizador CPE MR.
- Instalación de filtros de permiso multidifusión para el reenvío de tráfico multidifusión IP a la LAN del CPE.

2A

- Rearranque del temporizador CPE MR.
- Reenvío del MR en sentido ascendente.

3A

- Reposición del temporizador CPE, reenvío del MR en sentido ascendente.

2B

- Arranque del temporizador Cable MR.

3B

- Rearranque del temporizador Cable MR.

3C

- Parada del temporizador Cable MR.

2D

- Parada del temporizador CPE MR.
- Eliminación del filtro de permiso multidifusión para reenviar multidifusión IP al LAN del CPE.

3D

- Parada del temporizador CPE MR.
- Eliminación del filtro de permiso multidifusión para reenviar multidifusión IP al LAN del CPE.

ANEXO B.M

Servicios de concesión no solicitada

En el presente anexo B.M se examina la utilización prevista del servicio de concesión no solicitada (UGS) y el servicio de concesión no solicitada con detección de actividad (UGS-AD) y contiene ejemplos específicos.

B.M.1 Servicio de concesión no solicitada (UGS)

B.M.1.1 Introducción

El servicio de concesión no solicitada es un tipo de servicio de planificación de flujo en sentido ascendente que se utiliza para establecer la correspondencia entre tráfico a velocidad binaria constante (CBR, *constant bit rate*) y flujos de servicio. Puesto que el sentido ascendente es anchura de banda programada, un servicio CBR puede ser establecido por el CMTS programando un tren continuo de concesiones. Se denominan no solicitadas porque la anchura de banda está predeterminada, y no hay peticiones en curso.

Ejemplo clásico de aplicación CBR interesante es la de los paquetes del protocolo de transmisión de la voz sobre el protocolo Internet (VoIP). Es probable que existan además otras aplicaciones.

Los servicios de planificación de flujo en sentido ascendente están asociados con flujos de servicio, cada uno de los cuales está asociado con un ID de servicio (SID) único. Cada flujo de servicio puede tener múltiples clasificadores. Cada clasificador puede estar asociado con un tren de medios CBR único. Los clasificadores pueden ser añadidos a, y eliminados de, un flujo de servicio. Así pues, la semántica del UGS debe acomodar trenes de medios CBR únicos o múltiples por cada SID.

Para el análisis del presente anexo B.M, un subflujo se define como la salida de un clasificador. Puesto que una sesión de VoIP se identifica con un clasificador, un subflujo se refiere, en este contexto, a una sesión de VoIP.

B.M.1.2 Parámetros de la configuración

- Intervalo de concesión nominal.
- Tamaño de concesión no solicitada.
- Fluctuación de fase de concesión tolerada.
- Concesiones por intervalo.

En el anexo B.C se da una explicación de estos parámetros, así como sus valores por defecto.

B.M.1.3 Funcionamiento

Cuando se aprovisiona un flujo de servicio para el UGS, el intervalo de concesión nominal se elige igual al intervalo de paquetes de la aplicación CBR. Por ejemplo, aplicaciones VoIP con tamaños de paquete de 10 ms requerirán un intervalo de concesión nominal de 10 ms. El tamaño de la concesión se elige de manera que satisfaga los requisitos de anchura de banda de la aplicación CBR y está relacionado directamente con la longitud del paquete.

Cuando se asignan múltiples subflujos a un UGS, se emiten múltiples concesiones por intervalo. No hay una correspondencia explícita entre subflujos y concesiones. Múltiples concesiones por intervalo forman un grupo de concesiones en el que cualquier subflujo puede utilizar cualquier concesión.

En este ejemplo de funcionamiento se supone el caso de UGS por defecto de no concatenación y no fragmentación.

B.M.1.4 Fluctuación de fase

La figura B.M-1 muestra la relación entre el intervalo de concesión y la fluctuación de fase de concesión tolerada, y muestra un ejemplo de fluctuación de fase en subflujos.

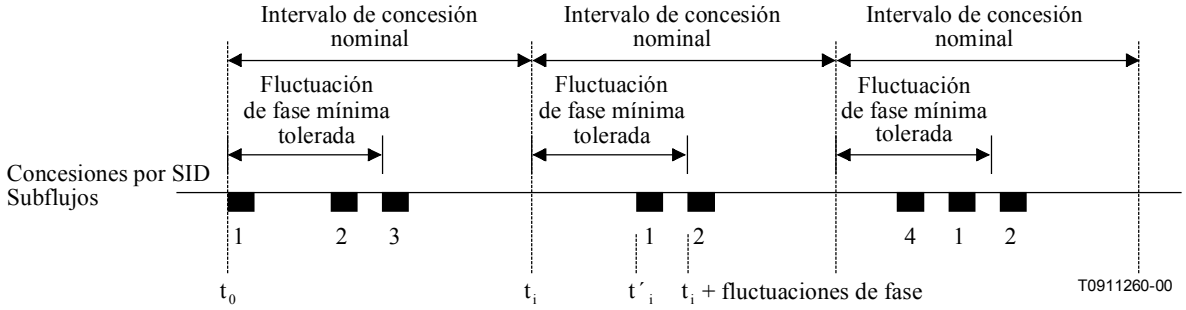


Figura B.M-1/J.112 – Ejemplo de fluctuación de fase con múltiples concesiones por SID

En el caso de una sola concesión por intervalo, la fluctuación de fase de concesión tolerada es la diferencia máxima entre el instante de concesión efectivo (t_i') y el instante de concesión nominal (t_i). En el caso de múltiples concesiones por intervalo, la fluctuación de fase de concesión tolerada es la diferencia máxima entre el instante efectivo de la última concesión en el grupo de concesiones y el instante de concesión nominal (t_i). Si la llegada de cualquier concesión se produce en el instante t_i', entonces $t_i \leq t_i' \leq t_i$ + fluctuación de fase.

La figura B.M-1 muestra cómo será sometido un subflujo a fluctuación de fase incluso aunque ninguna de las concesiones pueda desplazarse de su posición relativa. Durante el primer intervalo, se establecen tres sesiones VoIP, que caen en las tres concesiones. En el segundo intervalo, la sesión VoIP 3 ha sido retirada. Puesto que el CMTS no sabe que su flujo está asociado con cada concesión, decide eliminar la primera concesión. Las dos llamadas restantes se desplazan a las otras dos concesiones. En el tercer intervalo, se añade una nueva sesión VoIP 4 y una nueva concesión. La nueva llamada cae en la nueva concesión. El efecto neto consiste en que los subflujos se pueden desplazar dentro de su intervalo de fluctuación de fase.

La ventaja de un intervalo de fluctuación de fase pequeño es que la memoria tampón de las fluctuaciones de fase de recepción de VoIP se pueden mantener de tamaño reducido. La desventaja consiste en que impone una limitación de planificación al CMTS.

La frontera de un intervalo de concesión nominal es arbitraria y no se comunica entre el CMTS y el CM.

NOTA – Eventos de mayor trascendencia como la pérdida de un MAP, en sentido descendente, o los saltos de frecuencia de un canal en sentido ascendente, pueden hacer que la fluctuación de fase de los subflujos se produzca fuera de esta ventana de fluctuación de fase.

B.M.1.5 Asuntos relativos a la sincronización

Hay dos problemas relativos a la sincronización que se plantean cuando se transporta tráfico CBR, por ejemplo el de las sesiones VoIP, a través de una red. El primero consiste en la desadaptación de frecuencia entre el reloj fuente y el reloj destino. La aplicación VoIP gestiona esta situación, que, por otra parte, queda fuera del alcance del presente anexo B. El segundo problema es la desadaptación de frecuencia entre la fuente/los sumideros CBR y el canal portador que los lleva.

De manera específica, si el reloj que genera los paquetes VoIP hacia el canal en sentido ascendente no está sincronizado con el reloj del CMTS que proporciona el servicio UGS, es posible que los paquetes VoIP empiecen a acumularse en el CM. Esto podría ocurrir también si se perdiera un MAP, lo cual provocaría la acumulación de paquetes.

Cuando el CM detecta esta condición, confirma el indicador de cola del elemento EH del flujo de servicio. El CMTS responderá emitiendo una concesión adicional ocasional de manera que no se exceda el 1% de la anchura de banda aprovisionada. (Lo anterior corresponde a un máximo de una

concesión adicional cada cien concesiones.) El CMTS continuará suministrando esta anchura de banda adicional hasta que el CM deje sin efecto la confirmación de aquel bit.

En el sentido descendente se produce un problema similar. La fuente transmisora del extremo lejano puede no estar sincronizada en frecuencia con el reloj que dirige el CMTS. Por ello, la supervisión del CMTS DEBERÍA hacerse a una velocidad ligeramente superior a la de la velocidad aprovisionada exacta para tener en cuenta esa desadaptación y evitar la acumulación de retardos o la pérdida de paquetes en el CMTS.

B.M.2 Servicio de concesión no solicitada con detección de actividad (UGS-AD)

B.M.2.1 Introducción

El servicio de concesión no solicitada con detección de actividad (UGS-AD) es un tipo de servicio de planificación de flujo en sentido ascendente. Esta subcláusula describe una aplicación del UGS-AD que consiste en el soporte de la detección de actividad vocal (VAD, *voice activity detection*). La VAD se conoce también como supresión de silencio y es una técnica vocal en la que el códec transmisor envía muestras de voz solamente cuando hay una importante presencia de energía vocal. El códec receptor compensará los intervalos de silencio insertando silencio o ruido de confort igual al ruido de fondo percibido de la conversación.

La ventaja de la VAD es la reducción de la anchura de banda de red requerida para una conversación. Se estima que el 60% de una conversación oral es silencio. Eliminado ese silencio, la red podría dar curso a un volumen de tráfico notablemente mayor.

En este contexto, los subflujos se describirán como subflujos activos y subflujos inactivos. Ambos estados dentro de un estado de QoS de capa MAC conocido como estado activo.

B.M.2.2 Parámetros de configuración MAC

Los parámetros de la configuración son todos los parámetros del UGS normales, más:

- el intervalo de interrogación secuencial normal;
- la fluctuación de fase de interrogación secuencial tolerada.

En el anexo B.C se da una explicación de estos parámetros, así como sus valores por defecto.

B.M.2.3 Funcionamiento

Cuando no hay actividad, el CMTS envía peticiones secuenciadas al CM. Cuando hay actividad, el CMTS envía concesiones no solicitadas al CM. El CM indica el número de concesiones por intervalo que requiere en cada momento en el campo concesión activa del UGSH de cada paquete de cada concesión no solicita. El CM puede pedir hasta el máximo de concesiones activas por intervalo. El CM envía constantemente esta información de estado, por lo que no se requiere un acuse de recibo explícito procedente del CMTS.

La determinación de los niveles de actividad se deja que se decida en función de la implementación del CM. Opciones de la implementación son las siguientes:

- Hacer que el servicio de capa MAC proporcione un temporizador de actividad por clasificador. El servicio de capa MAC marcaría un subflujo como inactivo si dejaran de llegar los paquetes durante un cierto tiempo, y marcaría un subflujo como activo en el momento en que llegaran nuevos paquetes. El número de concesiones pedidas sería igual al número de subflujos activos.
- Disponer de una entidad de servicio de capa superior, tal como un cliente de medios incorporado, que indique actividad al servicio de capa MAC.

Cuando el CM recibe peticiones secuenciadas y detecta actividad, pide anchura de banda suficiente para una concesión por intervalo. Si la actividad es de más de un subflujo, el CM lo indicará en el campo concesión activa del UGSH empezando con el primer paquete que envía.

Cuando el CM reciba concesiones no solicitadas, detectará nueva actividad y pedirá una concesión más, por lo que habrá un retardo de tiempo antes de que reciba la nueva concesión. Durante ese retardo, los paquetes se pueden acumular en el CM. Cuando se añada la nueva concesión no solicitada, el CMTS enviará en ráfaga concesiones adicionales para eliminar la acumulación de paquetes..

Cuando el CM reciba concesiones no solicitadas, detectará inactividad en un subflujo y pedirá una concesión menos, por lo que habrá un retardo de tiempo antes de que se produzca la reducción de concesiones. Si se han acumulado paquetes en la cola de transmisiones en sentido ascendente, las concesiones adicionales reducirán o vaciarán la cola. Esto es lo apropiado porque mantiene baja la latencia del sistema. La ración entre subflujos y la concesión específica que obtiene cada uno de ellos variará también. Este efecto se manifiesta en forma de fluctuación de frecuencia baja que el extremo lejano debe gestionar.

Cuando el CM reciba concesiones no solicitadas y detecte ausencia de actividad en alguno de sus subflujos, enviará un paquete con el campo concesiones activas del UGSH fijado a cero concesiones, y a continuación cesará la transmisión. El CMTS conmutará del modo UGS al modo interrogación secuencial en tiempo real. Cuando se detecte de nuevo actividad, el CM enviará una petición en una de esas interrogaciones secuenciales para reanudar la entrega de concesiones no solicitadas. El CMTS ignora el tamaño de la petición y reanuda la atribución de concesiones tamaño concesión al CM.

No es necesario que el CMTS supervise separadamente la actividad de los paquetes porque ya lo hace el CM. En el caso más desfavorable, si el CMTS pierde el último paquete que indicara cero concesiones, el CMTS y el CM estarían de nuevo en sincronismo al comienzo del siguiente brote de palabras. Debido a este escenario, cuando el CM pasa de inactivo a activo, ha de poder reiniciar la transmisión con peticiones secuenciadas con concesiones no solicitadas.

B.M.2.4 Ejemplo

La figura B.M-2 muestra un ejemplo de una sola llamada vocal G.711 (64 kbit/s) con un tamaño de paquetes de 10 ms, y una memoria tampón de fluctuaciones de fase de recepción que requiere un mínimo de 20 ms de voz (por tanto, 2 paquetes) antes de comenzar la ejecución.

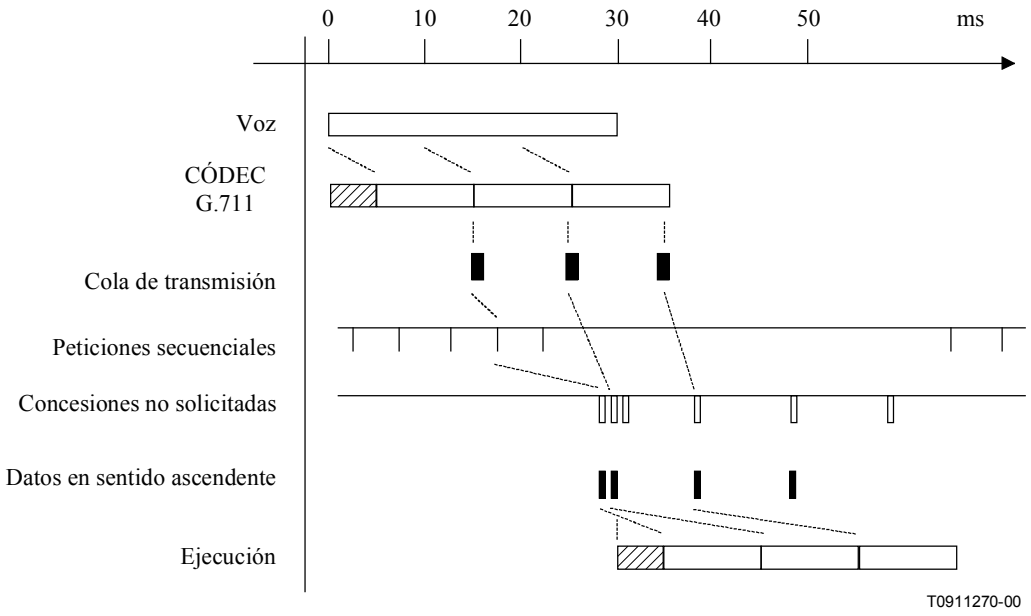


Figura B.M-2/J.112 – Arranque y parada de la VAD

Supóngase que la voz comienza en el instante cero. Tras un retardo de procesamiento nominal y un retardo de paquetización de 10 ms, el CÓDEC DSP genera paquetes de voz que se transfieren a continuación a la cola de transmisión en sentido ascendente. Seguidamente se utilizan peticiones secuenciadas lo que da como resultado el comienzo de las concesiones no solicitadas en algún momento posterior. Concesiones no solicitadas adicionales son emitidas inmediatamente para despejar la cola en sentido ascendente.

Esos paquetes atraviesan la red y llegan a la memoria tampón de fluctuaciones de fase de recepción. La memoria tampón de fluctuaciones de fase mínima de 20 ms se colma cuando llega el segundo paquete. Puesto que los paquetes llegan muy próximos, sólo se añade una latencia adicional de algunos milisegundos. Tras un retardo de procesamiento nominal, empieza la ejecución.

Cuando el brote de palabras termina, el CM envía un paquete restante sin cabida útil y con el campo concesiones activas del UGSH fijado a cero concesiones. En algún momento posterior, se para el UGS y comienza la interrogación secuencial en tiempo real.

B.M.2.5 Ráfaga de concesiones de brote de palabras

La ráfaga adicional de concesiones no solicitadas cuando un flujo pasa a estar activo se necesita porque la memoria tampón de fluctuaciones de fase en el CÓDEC receptor espera normalmente a tener una cantidad mínima de muestras vocales antes de empezar la ejecución. Cualquier retardo entre la llegada de esos paquetes iniciales se añadirá a la latencia final de la llamada telefónica. Así pues, cuanto antes reconozca el CMTS que el CM tiene paquetes para enviar y pueda vaciar la memoria tampón del CM, antes alcanzarán esos paquetes el receptor, y menor será la latencia en que se incurra en la llamada telefónica.

El problema de cuántas concesiones se deben enviar en ráfaga carece una solución precisa. Cuando el CM efectúa su petición de una concesión adicional es porque ya se ha acumulado un paquete de voz. El CM no tiene idea de cuántas concesiones adicionales ha de pedir ya que desconoce lo que tardará en llegar la respuesta del CMTS y, por tanto, cuántos paquetes puede acumular. El CMTS está mejor informado, aunque desconoce los requisitos de memoria tampón de fluctuación de fase del extremo lejano.

La solución consiste en que el CMTS elija un tamaño de ráfaga y que envíe en ráfaga esas concesiones muy próximas entre sí al comienzo del brote de palabras. Esto es lo que ocurre cuando se pasa de la interrogación en tiempo real al UGS, y cuando se aumenta el número de concesiones del UGS por intervalo.

En el cuadro B.M-1 se muestra la latencia de arranque típica que introducirá el tiempo de respuesta a una petición de concesión.

Cuadro B.M-1/J.112 – Ejemplo de tiempo de respuesta a una petición de concesión

	Variable	Ejemplo de valor	
1	Tiempo que transcurre desde la creación del paquete de voz hasta el momento en que el paquete de voz llega a la cola en sentido ascendente del CM.	0-1	ms
2	Tiempo que transcurre hasta que se recibe una petición secuenciada. El tiempo del caso más desfavorable es el intervalo de petición secuenciada.	0-5	ms
3	Tiempo de respuesta a la petición de concesión del CMTS. En este valor influyen la longitud del MAP y el número de MAP pendientes.	5-15	ms
4	Retardo de ida y retorno de la planta HFC incluido el retardo de intercalación en sentido descendente.	1-5	ms
	Total	**6-26**	**ms**

Este número variará de una implementación CMTS a otra, pero una cifra previsible de concesiones adicionales de acuerdo con el ejemplo anterior sería como en el cuadro B.M-2:

Cuadro B.M-2/J.112 – Ejemplo de concesiones adicionales para nuevos brotes de palabras

Intervalo del UGS	Concesiones adicionales para nuevos brotes de palabras
10 ms	2
20 ms	1
30 ms	0

Una vez más conviene señalar que el CMTS y CM no pueden, y no lo hacen, asociar subflujos individuales con concesiones individuales. Ello significa que cuando los subflujos actuales están activos y un nuevo subflujo pase a estar activo, el nuevo subflujo empezará inmediatamente a utilizar el grupo existente de concesiones. Esto reduce potencialmente la latencia de comienzo de nuevos brotes de palabras, pero aumenta la latencia de los otros subflujos. Cuando la ráfaga de concesiones llega, es compartida con todos los subflujos, y restaura o incluso reduce la latencia original. Se trata de un componente de la fluctuación de fase. Cuantos más subflujos estén activos, menos repercusiones tendrá la adición de un subflujo nuevo.

B.M.2.6 Consideraciones relativas a la admisión

Se señala que, al configurar el control de admisión del CMTS, se habrán de tener en cuenta los factores siguientes.

La VAD permite que el canal en sentido ascendente esté sobreaprovisionado. Por ejemplo, un canal en sentido ascendente que pudiera tratar normalmente 24 sesiones VoIP podría ser sobreprovisionado hasta 36 (50%) o incluso 48 (100%). Cuando hay sobreaprovisionamiento, existe la posibilidad estadística de que todas las sesiones VoIP en sentido ascendente pasen a estar activas. Al mismo tiempo, el CMTS podría ser incapaz de planificar todo el tráfico VoIP. Además, las ráfagas de concesiones de brotes de palabras se alargarían. Las implementaciones CM de la VAD deberían reconocer esta posibilidad, y fijar un límite al número de paquetes que dejarán que se acumulen en su cola.

La saturación ocasional del canal ascendente durante la VAD se puede eliminar estableciendo que el número máximo de sesiones VoIP permitidas sea inferior a la capacidad máxima del canal ascendente con todo el tráfico vocal (24 en el ejemplo anterior). La VAD haría que la utilización del canal cayera del 100% al 40% aproximadamente para voz, dejando el 60% restante para que lo utilizara el tráfico de datos y el tráfico de mantenimiento.

ANEXO B.N

Adiciones a la especificación europea

Este anexo B.N se aplica a la segunda opción tecnológica a la que se refiere B.1.1. Para la primera opción, véanse B.4, B.6 y B.7.

En el presente anexo B.N se describen las especificaciones de capa física requeridas para lo que se llama por lo general módems de cable EuroDOCSIS. Se trata de un anexo facultativo que de ninguna manera afecta a la certificación de América del Norte, módems DOCSIS 1.1.

Las cláusulas se han enumerado de tal manera que el sufijo después de B.N se refiera a la parte de la especificación que ha cambiado. En consecuencia, algunas cláusulas de este anexo carecen de texto, porque no ha sido preciso introducir ningún cambio.

B.N.1 Alcance

No ha hecho falta introducir ningún cambio.

B.N.2 Referencias

No ha hecho falta introducir ningún cambio.

B.N.3 Definiciones y abreviaturas

No ha hecho falta introducir ningún cambio.

B.N.4 Hipótesis funcionales

Esta cláusula define las características de las plantas de televisión por cable que se asumen a efectos del funcionamiento de un sistema de datos por cable. No se trata de una descripción de parámetros del CMTS o el CM. El sistema de datos por cable DEBE poder interfuncionar con el entorno que aquí se describe.

B.N.4.1 Red de acceso de banda ancha

Se supone una red de acceso de banda ancha básicamente coaxial, lo que puede tomar la forma de una red totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC). La expresión genérica "red de cable" se emplea aquí para abarcar todos los casos.

Una red de cable utiliza un medio compartido, una arquitectura de árbol y ramas con transmisión analógica. Las características funcionales fundamentales cuya presencia se supone en el presente anexo B.N son las siguientes:

- transmisión bidireccional;
- separación óptica/eléctrica máxima entre el CMTS y el terminal del cliente más distante de 160 km;
- separación óptica/eléctrica diferencial máxima entre el CMTS y el módem más cercano y el más distante de 160 km.

B.N.4.2 Hipótesis de los equipos

B.N.4.2.1 Plan de frecuencias

Se supone que, en el sentido descendente, el sistema de cable tiene una banda de paso con un borde inferior típico entre 47 y 87,5 MHz y un borde superior que depende de la implementación, pero que varía normalmente entre 300 y 862 MHz. Dentro de esa banda de paso se supone además que están presentes señales de televisión analógica PAL/SECAM en canales de 7/8 MHz, señales de radiofrecuencia modulada, y otras señales digitales de banda estrecha y banda ancha.

En el sentido ascendente, se supone que el sistema de cable tiene una banda de paso con un borde inferior a 5 MHz y un borde superior que depende la implementación, pero que varía normalmente entre 25 y 65 MHz.

B.N.4.2.2 Compatibilidad con otros servicios

El CM y el CMTS DEBEN coexistir con los demás servicios en la red de cable. En particular:

a) DEBEN funcionar de manera satisfactoria en el espectro de cable asignado para el interfuncionamiento CMTS-CM mientras el resto del espectro del cable está ocupado por una combinación de señales de televisión y de otro tipo; y

b) NO DEBEN causar interferencia perjudicial a ningún otro servicio asignado a la red de cable en un espectro distinto al atribuido al CM y al CMTS.

B.N.4.2.3 Repercusión del aislamiento de las averías en otros usuarios

Puesto que el sistema de datos por cable es un sistema punto a multipunto con medios compartidos, los procedimientos de aislamiento de averías deberían tener en cuenta la posible repercusión perjudicial de las averías y de los procedimientos de aislamiento de las mismas en muchos usuarios del servicio de datos por cable y de otros servicios.

Para la interpretación de la repercusión perjudicial, véase la anterior subcláusula B.N.4.2.2.

B.N.4.2.4 Dispositivos de terminal de sistema por cable

Véase B.1.

B.N.4.3 Hipótesis de los canales de RF

El sistema de datos por cable, configurado con al menos un conjunto de parámetros de capa física definidos (por ejemplo, modulación, corrección de errores directa, velocidad de símbolos, etc.) de la gama de fijaciones de configuración descritas en esta especificación, DEBE ser capaz de interfuncionar en redes por cable que tengan características definidas en esta cláusula de tal manera que la corrección de errores directa permita un funcionamiento equivalente en un sistema de cable con y sin las características de canal degradado que se describe más abajo.

B.N.4.3.1 Transmisión en sentido descendente

En el cuadro B.N-1 se describen las características de la transmisión por canal de RF de la red de cable en sentido descendente, asumidas a efectos de una capacidad de funcionamiento mínima. Se supone nivel de portadora de vídeo analógico nominal (potencia en la cresta de la envolvente) en una anchura de banda de canal de 7/8 MHz. Todas las características se presentan de manera coincidente.

Cuadro B.N-1/J.112 – Características supuestas de la transmisión por canal de RF en sentido descendente para señales de TV analógica y sonora

Parámetro	Valor
Gama de frecuencias	La gama normal de funcionamiento en sentido descendente de una sistema de cable va de 47 MHz hasta incluso 862 MHz. Sin embargo, la gama de funcionamiento para comunicación de datos es de 108 a 862 MHz. La utilización de frecuencias entre 108 y 136 MHz puede ser prohibida debido al reglamento nacional con respecto a la interferencia con frecuencias de navegación aeronáutica.
Separación de canales de RF (anchura de banda de diseño)	Se utilizan canales de 7/8 MHz, 8 MHz para comunicación de datos.
Retardo de tránsito del encabezamiento al cliente más distante	≤ 0,800 ms (normalmente, mucho menos).
Relación portadora/ruido en una banda de 8 MHz (nivel de vídeo analógico)	No inferior a 44 dB (nota 4).
Relación portadora/interferencia para potencia total (señales interferentes discretas y de banda ancha)	No inferior a 52 dB dentro de la anchura de banda de diseño.
Distorsión de batido triple compuesto para portadoras moduladas analógicas	No superior a −57 dBc dentro de la anchura de banda de diseño [nota 6 a)].
Distorsión de segundo orden compuesto para portadoras moduladas analógicas	No superior a −57 dBc dentro de la anchura de banda de diseño [nota 6 b)].
Nivel de modulación cruzada	Se está analizando.

Cuadro B.N-1/J.112 – Características supuestas de la transmisión por canal de RF en sentido descendente para señales de TV analógica y sonora

Parámetro	Valor
Rizado de amplitud	2,5 dB en 8 MHz.
Rizado de retardo de grupo en el espectro ocupado por el CMTS	100 ns en la gama de frecuencias de 0,5 MHz a 4,43 MHz.
Límite de las microrreflecciones para el eco dominante	–10 dBc @ ≤ 0,5 µs, –15 dBc @ ≤ 1,0 µs –20 dBc @ ≤ 1,5 µs, –30 dBc @ > 1,5 µs
Modulación por zumbido de portadora	No superior a –46 dBc (0,5 %).
Ruido en ráfagas	No superior a 25 µs a una frecuencia media de 10 Hz.
Variación del nivel de la señal estacional y diurna	8 dB.
Pendiente del nivel de la señal, 85 MHz a 862 MHz	12 dB.
Nivel máximo de portadora de vídeo analógico a la salida del sistema, incluida la variación de nivel de la señal anterior	77 dBµV [nota 6 c)].
Nivel más bajo de portadora de vídeo analógico a la salida del sistema, incluida la variación de la señal anterior	60 dBµV [nota 6 d)].
NOTA 1 – La transmisión va del combinador de cabecera a la entrada del CM en la posición del cliente. NOTA 2 – Para mediciones por encima de la banda de frecuencias de funcionamiento normales en el sentido descendente (excepto el zumbido), las degradaciones se refieren al nivel de portadora PAL/SECAM de frecuencia más alta. NOTA 3 – Para mediciones del zumbido por encima de la banda de frecuencias de funcionamiento normal en el sentido descendente, se envía una portadora de onda continua a la frecuencia de prueba del mismo nivel que la portadora PAL/SECAM de frecuencia más alta. NOTA 4 – Se supone aquí que la portadora digital funciona al nivel de la portadora de cresta analógica. Cuando la portadora digital funciona por debajo del nivel de portadora de cresta analógica, esta relación C/N puede ser inferior. NOTA 5 – Métodos de medición definidos en [CENELEC 50083-7]. NOTA 6 – Para sistemas SECAM son aplicables los valores siguientes: a) No superior a −52 dBc dentro de la anchura de banda de diseño. b) No superior a −52 dBc dentro de la anchura de banda de diseño. c) 74 dBµV. d) 57 dBµV.	

B.N.4.3.2 Transmisión en sentido ascendente

En el cuadro B.N-2 se describen las características de la transmisión por canal de RF de la red de cable en sentido ascendente, asumidas a efectos de una capacidad de funcionamiento mínima. Todas las condiciones se presentan de manera coincidente.

Cuadro B.N-2/J.112 – Características supuestas de la transmisión por canal RF en sentido ascendente

Parámetro	Valor
Gama de frecuencias	De 5 a 65 MHz borde a borde
Retardo de tránsito del CM más distante al CM o CMTS más cercano	≤ 0,800 ms (normalmente, mucho menos)
Relación portadora/ruido en canal activo	No inferior a 22 dB
Relación de potencia portadora/señal interferente (la suma de señales interferentes discretas y de banda ancha) en canal activo	No inferior a 22 dB (nota 2)
Relación portadora/señal interferencia (la suma de ruido, distorsión, distorsión de trayecto común y modulación cruzada) en canal activo	No inferior a 22 dB
Modulación por zumbido de portadora	No superior a –23 dBc (7,0 %)
Ruido en ráfagas	No superior a 10 µs a una frecuencia media de 1 kHz en la mayoría de los casos (notas 3 y 4)
Rizado de amplitud	5 MHz a 65 MHz: 2,5 dB en 2 MHz
Rizado de retardo de grupo	5 MHz a 65 MHz: 300 ns en 2 MHz
Microrreflexiones, eco único	–10 dBc @ ≤ 0,5 µs –20 dBc @ ≤ 1,0 µs –30 dBc @ > 1,0 µs
Variación de nivel de señal estacionaria y diurna	No superior a 12 dB de mínimo a máximo
NOTA 1 – La transmisión va de la entrada al CM en la posición del cliente a la cabecera. NOTA 2 – Se PUEDEN utilizar técnicas de eliminación de las señales interferentes o de tolerancia a las mismas para garantizar el funcionamiento en presencia de señales interferentes discretas variables en el tiempo que podrían ser hasta 0 dBc. NOTA 3 – Características de amplitud y frecuencia lo suficientemente fuertes como para enmascarar parcial o totalmente la portadora de datos NOTA 4 – Niveles de ruido impulsivo más frecuentes a frecuencias más bajas (<15 MHz).	

B.N.4.3.2.1 Disponibilidad

La disponibilidad normal de las redes de cable suele ser superior al 99%.

B.N.4.4 Niveles de transmisión

Se pretende que el nivel de potencia nominal de la señal o señales con QAM del CMTS dentro de un canal de 8 MHz se encuentre en la gama de –13 dBc a 0 dBc con respecto al nivel de portadora de vídeo analógico, y que normalmente no supere a este último nivel (por lo general entre –10 y –6 dBc para 64QAM, y entre –6 y –4 dBc para 256QAM). El nivel de potencia nominal de la señal o señales del CM en sentido ascendente deberá ser lo más bajo posible para conseguir el margen necesario por encima del ruido y la interferencia. Habitualmente se aplica una carga de potencia uniforme por unidad de anchura de banda al fijar los niveles de las señales en sentido ascendente, con niveles específicos establecidos por el operador de red por cable para conseguir las relaciones requeridas de portadora/ruido y portadora/interferencia.

B.N.4.5 Inversión de frecuencia

No habrá inversión de frecuencia en el trayecto de transmisión en el sentido descendente ni en el sentido ascendente, es decir, un cambio positivo de frecuencia en la entrada a la red por cable dará lugar a un cambio positivo de frecuencia en la salida.

B.N.5 Protocolos de comunicación

No ha hecho falta introducir ningún cambio.

B.N.6 Especificación de subcapa dependiente de los medios físicos

B.N.6.1 Alcance

Esta especificación define las características eléctricas y el protocolo de un módem de cable (CM) y un sistema de terminación de módem de cable (CMTS). Lo que se pretende con la misma es definir un CM y un CMTS que interfuncionen de tal manera que cualquier implementación de un CM pueda funcionar con cualquier CMTS. La presente especificación no trata de inducir la puesta en aplicación de ninguna implementación en concreto.

B.N.6.2 Sentido ascendente

B.N.6.2.1 Visión de conjunto

La subcapa dependiente de los medios físicos (PMD) en el sentido ascendente utiliza un formato de modulación de ráfagas FDMA/TDMA, que proporciona cinco velocidades de símbolos y dos formatos de modulación (QPSK y 16QAM). El formato de modulación incluye la conformación de impulsos a efectos de eficacia espectral, tiene agilidad de frecuencia de portadora y su nivel de potencia de salida es seleccionable. El formato de la subcapa PMD consta de una ráfaga modulada de longitud variable con temporización precisa que comienza en puntos separados por múltiplos enteros de 6,25 μs (lo que representa 16 símbolos a la velocidad de datos más alta).

Cada ráfaga soporta modulación flexible, preámbulo, aleatorización de la cabida útil y codificación FEC programable.

Todos los parámetros de la transmisión en el sentido ascendente asociados con salidas de transmisión de ráfagas procedentes del CM pueden ser configurados por el CMTS mediante la mensajería MAC. Muchos de los parámetros son programables ráfaga por ráfaga.

La subcapa PMD puede soportar un modo de transmisión casi continua, en donde la rampa descendente de una ráfaga PUEDE superponerse con la rampa ascendente de la ráfaga siguiente, de tal manera que la envolvente transmitida nunca es cero. La temporización del sistema de las transmisiones TDMA desde los diversos CM DEBE hacerse de tal modo que el centro del último símbolo de una ráfaga y el centro del primer símbolo del preámbulo de la ráfaga que sigue inmediatamente estén separados por la duración de cinco símbolos como mínimo. El tiempo de guarda DEBE ser superior o igual a la duración de cinco símbolos más el error de temporización máximo. Al error de temporización contribuyen tanto el CM como el CMTS. El funcionamiento de la temporización del CM se especifica en B.N.6.2.7, B.N.6.2.8, B.N.6.2.10 y B.N.6.3.7. El error de temporización máximo y el tiempo de guarda pueden variar con los CMTS de diferentes vendedores.

El modulador en sentido ascendente forma parte del módem del cable que hace interfaz con la red de cable. El modulador contiene la función de modulación de nivel eléctrico efectiva y la función de procesamiento de señales digitales; esta última proporciona la FEC, la agregación del preámbulo delantero, la correspondencia de símbolos y otros pasos del procesamiento. La presente especificación se ha redactado con la idea de que las ráfagas se almacenen en memoria tampón en el tramo procesamiento de señal, y de que el tramo procesamiento de señal:

1) acepte el tren de información en base a una ráfaga en cada momento;
2) convierta dicho tren en una ráfaga completa de símbolos para el modulador; y

3) introduzca el tren de símbolos en ráfagas adecuadamente temporizadas en un modulador sin memoria en el momento exacto de la transmisión de la ráfaga.

El tramo sin memoria del modulador sólo efectúa la conformación de los impulsos y la conversión elevadora en cuadratura.

En el demodulador, al igual que en el modulador, hay dos componentes funcionales básicos: la función de demodulación y la función de procesamiento de señales. A diferencia del modulador, el demodulador reside en el CMTS y la especificación se establece teniendo en cuenta que habrá una función de demodulación (no necesariamente un demodulador físico real) por cada frecuencia de portadora que se utilice. La función de demodulación recibirá todas las ráfagas a una frecuencia determinada.

NOTA – El procedimiento de diseño de la unidad deberá tener en cuenta la naturaleza multicanal de la demodulación y del procesamiento de la señal que se ha de efectuar en la cabecera, y dividir/compartir la funcionalidad adecuadamente para influir de manera óptima en la aplicación multicanal. Lo apropiado podría ser un diseño de demodulador que soportara múltiples canales en una unidad demoduladora.

La función de demodulación del demodulador acepta una señal de nivel variable centrada en torno al nivel de potencia pedido y efectúa la temporización de símbolos y la recuperación y seguimiento de la portadora, la adquisición de ráfagas y la demodulación. Además, la función de demodulación proporciona una estimación de la temporización de las ráfagas con respecto a un borde de referencia, una estimación de la potencia de la señal recibida y una estimación de la relación señal/ruido, y puede llevar a cabo una ecualización adaptable para atenuar los efectos de:

a) los ecos del sistema de cables;

b) las señales interferentes de banda estrecha; y

c) el retardo de grupo.

La función procesamiento de señal del demodulador efectúa un procesamiento inverso al de la función procesamiento de señal del modulador. Se incluye en él la aceptación del tren de datos en ráfagas demoduladas, la decodificación, etc. y, posiblemente, la multiplexación de los datos procedentes de múltiples canales en un solo tren de salida. La función procesamiento de señal proporciona también la señal de referencia de temporización con respecto al borde y de desbloqueo a los demoduladores para activar la adquisición de ráfagas de cada intervalo de ráfagas asignado. Además puede proporcionar una indicación de decodificación satisfactoria, error de decodificación o fallo de la decodificación por cada palabra de código y el número de símbolos Reed-Solomon corregidos en cada palabra de código. Para toda ráfaga en sentido ascendente, el CMTS tiene un conocimiento previo de su longitud en símbolos (véanse B.N.6.2.6, B.N.6.2.10.1 y B.A.2).

B.N.6.2.2 Formatos de modulación

El modulador en sentido ascendente DEBE proporcionar tanto el formato de modulación QPSK como 16QAM.

El demodulador en el sentido ascendente DEBE soportar los formatos de modulación QPSK y el 16QAM.

B.N.6.2.2.1 Velocidades de modulación

El modulador en sentido ascendente DEBE proporcionar QPSK a 160, 320, 640, 1280 y 2560 ksímb/s, y 16QAM a 160, 320, 640 1280 y 2560 ksímb/s.

Esta diversidad de velocidades de modulación, y la flexibilidad al fijar las frecuencias de la portadora en sentido ascendente, permite a los operadores ubicar operadoras en intervalos del esquema de señales interferentes de banda estrecha.

La velocidad de símbolos en sentido ascendente DEBE fijarse para cada frecuencia en sentido ascendente.

B.N.6.2.2.2 Correspondencia de símbolos

El modo de modulación (QPSK o 16QAM) es programable. Los símbolos transmitidos en cada modo y la correspondencia entre los bits de entrada y la constelación I y Q DEBEN ser como se define en el cuadro B.N-3. En dicho cuadro, I_1 es el MSB del diagrama de símbolos, Q_1 es el LSB para QPSK, y Q_0 es el LSB para 16QAM. Q_1 e I_0 tienen posiciones de bits intermedias en 16QAM. El MSB DEBE ser el bit de los datos en serie con el que comienza el establecimiento de la correspondencia de símbolos.

Cuadro B.N-3/J.112 – Correspondencia de I/Q

Modo QAM	Definiciones de bit de entrada
QPSK	I_1 Q_1
16QAM	I_1 Q_1 I_0 Q_0

La correspondencia de símbolos de QPKS en sentido ascendente DEBE ser como se muestra en la figura B.N-1.

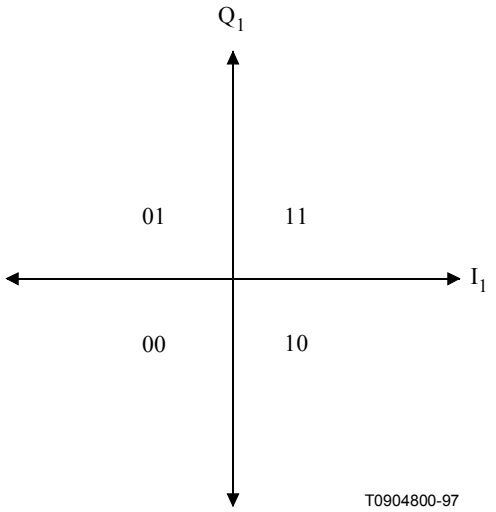


Figura B.N-1/J.112 – Correspondencia de símbolos de QPSK

La correspondencia de símbolos no invertidos de 16QAM (con codificación Gray) DEBE ser como se muestra en la figura B.N-2.

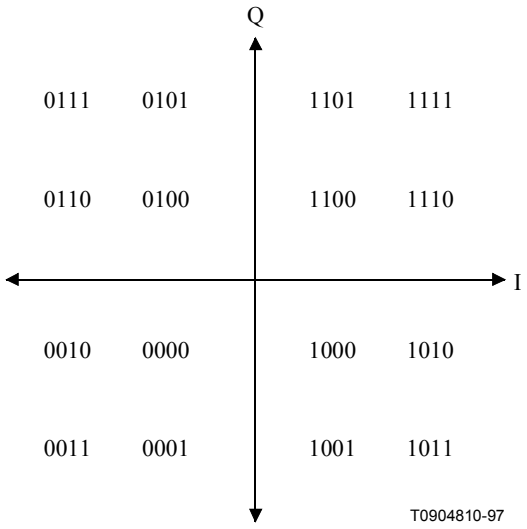


Figura B.N-2/J.112 – Correspondencia de símbolos con codificación Gray de 16QAM

La correspondencia de símbolos con codificación diferencial de 16QAM DEBE ser como se muestra en la figura B.N-3.

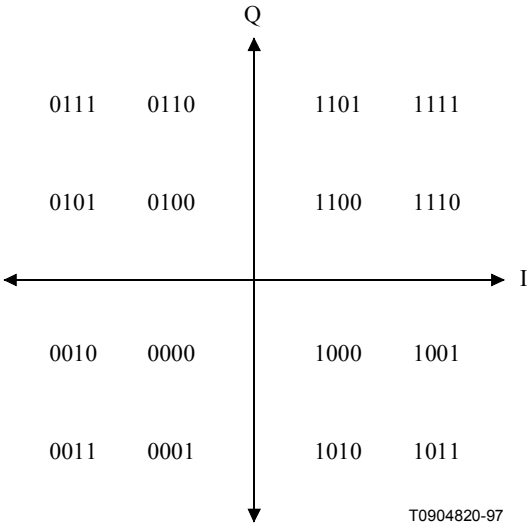


Figura B.N-3/J.112 – Correspondencia de símbolos con codificación diferencial de 16QAM

Si es posible la codificación de cuadrante diferencial, el cuadrante de símbolos transmitido en un determinado momento se obtiene a partir del cuadrante de símbolos transmitido con anterioridad y de los bits de entrada en ese momento utilizando el cuadro B.N-4.

Cuadro B.N-4/J.112 – Obtención del cuadrante de símbolos transmitidos actualmente

Bits de entrada actuales I(1) Q(1)	Cambio de fase del cuadrante	Bits más significativos del símbolo transmitido previamente	Bits más significativos del símbolo transmitido actualmente
00	0°	11	11
00	0°	01	01
00	0°	00	00
00	0°	10	10
01	90°	11	01
01	90°	01	00
01	90°	00	10
01	90°	10	11
11	180°	11	00
11	180°	01	10
11	180°	00	11
11	180°	10	01
10	270°	11	10
10	270°	01	11
10	270°	00	01
10	270°	10	00

B.N.6.2.2.3 Conformación del espectro

La subcapa PMD en sentido ascendente DEBE soportar una conformación Nyquist de raíz cuadrada de coseno alzado con factor del 25%. El espectro ocupado NO DEBE exceder de las anchuras de canal que se muestran en el cuadro B.N-5.

Cuadro B.N-5/J.112 – Máxima anchura de canal

Velocidad de símbolos (ksímb/s)	Anchura de canal (kHz) (véase la nota)
160	200
320	400
640	800
1280	1600
2560	3200
NOTA – La anchura de canal es la anchura de banda de –30 dB.	

B.N.6.2.2.4 Agilidad y gama de las frecuencias en sentido ascendente

La subcapa PMD en sentido ascendente DEBE soportar el funcionamiento en la gama de frecuencias de 5 a 65 MHz borde a borde.

Se DEBE soportar la resolución del desplazamiento de frecuencia con una gama de ±32 kHz (incremento = 1 Hz; implementación dentro de ±10 Hz).

B.N.6.2.2.5 Formato del espectro

El modulador en sentido ascendente DEBE funcionar con el formato $s(t) = I(t) \times \cos(\omega t) - Q(t) \times \text{sen}(\omega t)$, donde t representa el tiempo y ω indica la frecuencia angular.

B.N.6.2.3 Codificación FEC

B.N.6.2.3.1 Modos de codificación FEC

El modulador en sentido ascendente DEBE proporcionar las siguientes opciones: códigos Reed-Solomon en GF(256) con T = 1 a 10 o ausencia de codificación FEC.

DEBE soportarse el siguiente polinomio generador de Reed-Solomon:

$$g(x) = \left(x + \alpha^1\right)\left(x + \alpha^{2T-1}\right)$$

donde el elemento primitivo α es 0x02 hex.

DEBE soportarse el siguiente polinomio primitivo de Reed-Solomon:

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1$$

El modulador en sentido ascendente DEBE proporcionar palabras de código con un tamaño comprendido entre un mínimo de 18 octetos (16 octetos de información [k] más dos octetos de paridad para corrección de errores T = 1) hasta un máximo de 255 octetos (octetos k más octetos de paridad). El tamaño de una palabra de código no codificada puede ser de hasta un mínimo de un octeto.

En el modo última palabra de código abreviada, el CM DEBE proporcionar la última palabra de código de una ráfaga abreviada a partir de la longitud asignada de k octetos de datos por palabra de código, según se describe en B.N.6.10.1.2.

El valor de T DEBE configurarse en respuesta al descriptor de canal en sentido ascendente del CMTS.

B.N.6.2.3.2 Orden de bit a símbolo FEC

La entrada en el codificador Reed-Solomon es lógicamente un tren de bits en serie proveniente de la capa MAC del CM, y se DEBE establecer la correspondencia entre el primer bit del tren y el MSB del primer símbolo Reed-Solomon que entra en el codificador. El MSB del primer símbolo que sale del codificador se DEBE hacer corresponder con el primer bit del tren de bits en serie introducido en el aleatorizador.

Se señala que el convenio MAC octeto a serie en sentido ascendente requiere que se establezca la correspondencia entre el LSB del octeto y el primer bit del tren de bits en serie, según B.8.2.1.3.

B.N.6.2.4 Aleatorizador

El modulador en sentido ascendente DEBE implementar un aleatorizador (véase la figura B.N-4) cuyo valor semilla de 15 bits DEBE ser programable de manera arbitraria.

Al comienzo de cada ráfaga, se libera el registrador y se carga el valor semilla. El valor semilla se DEBE utilizar para calcular el bit del aleatorizador que se combina en un XOR (OR exclusivo) con el primer bit de los datos de cada ráfaga (que es el MSB del primer símbolo que sigue al último símbolo del preámbulo).

El valor semilla del aleatorizador DEBE configurarse en respuesta al descriptor de canal en sentido ascendente del CMTS.

El polinomio DEBE ser $x^{15} + x^{14} + 1$.

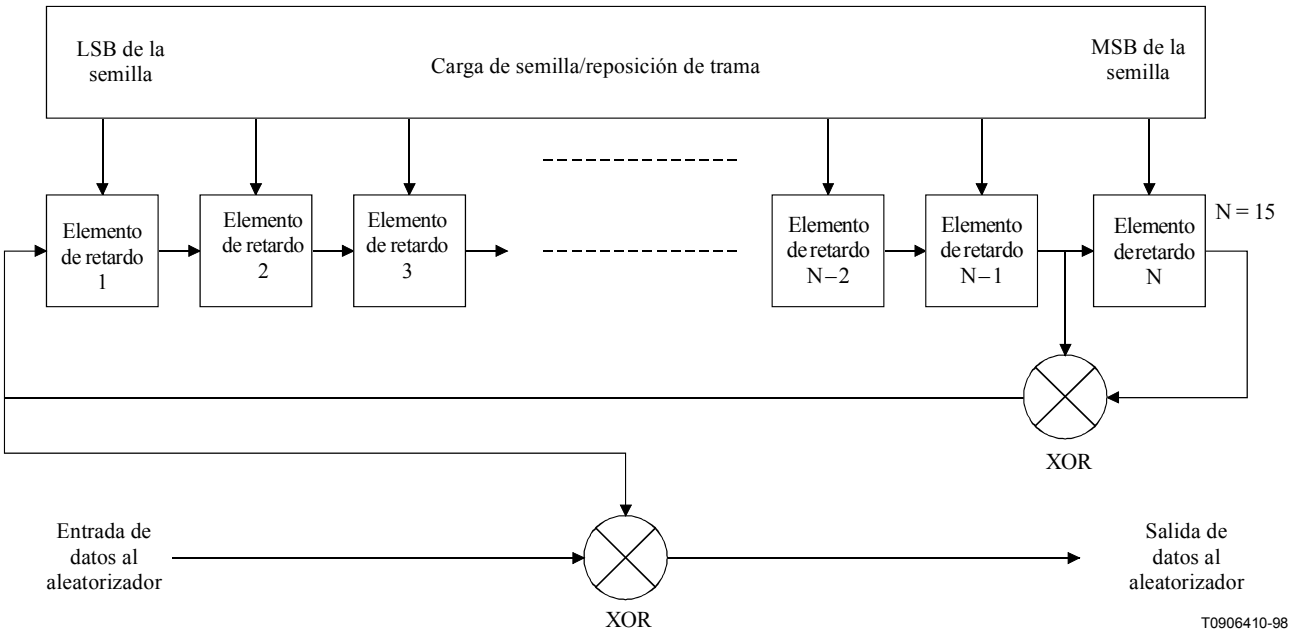


Figura B.N-4/J.112 – Estructura del aleatorizador

B.N.6.2.5 Agregación de preámbulo delantero

La subcapa PMD en sentido ascendente DEBE soportar un campo preámbulo de longitud variable que se sitúa delante de los datos una vez que éstos han sido aleatorizados y codificados según Reed-Solomon.

El primer bit del esquema de preámbulo es el primer bit que entra en el dispositivo de establecimiento de la correspondencia (véase la figura B.N-9), y es I_1 en el primer símbolo de la ráfaga (véase B.N.6.2.4). El primer bit del esquema de preámbulo es designado por el desplazamiento de valor de preámbulo como se describe en el cuadro B.8-19.

El valor del preámbulo que se agrega delante DEBE ser programable y su longitud DEBE ser de 0, 2, 4, ..., ó 1024 bits para QPSK y 0, 4, 8, ..., ó 1024 bits para 16QAM. Con ello, la longitud máxima del preámbulo es de 512 símbolos QPSK o bien de 256 símbolos QAM.

La longitud y el valor del preámbulo DEBEN configurarse en respuesta al mensaje del descriptor de canal en sentido ascendente transmitido por el CMTS.

B.N.6.2.6 Ecualizador previo de transmisión

El ecualizador previo de transmisión de una estructura de ecualizador lineal, como se muestra en la figura B.N-5, DEBE ser configurado por el CM en respuesta al mensaje respuesta de alineación (RNG-RSP, *ranging response*) transmitido por el CMTS. El ecualizador previo DEBE aceptar una estructura de ecualizador con separación de símbolos (T) con ocho derivaciones. El ecualizador previo PUEDE tener uno a cuatro muestras por símbolo, con una longitud de derivación superior a ocho símbolos.

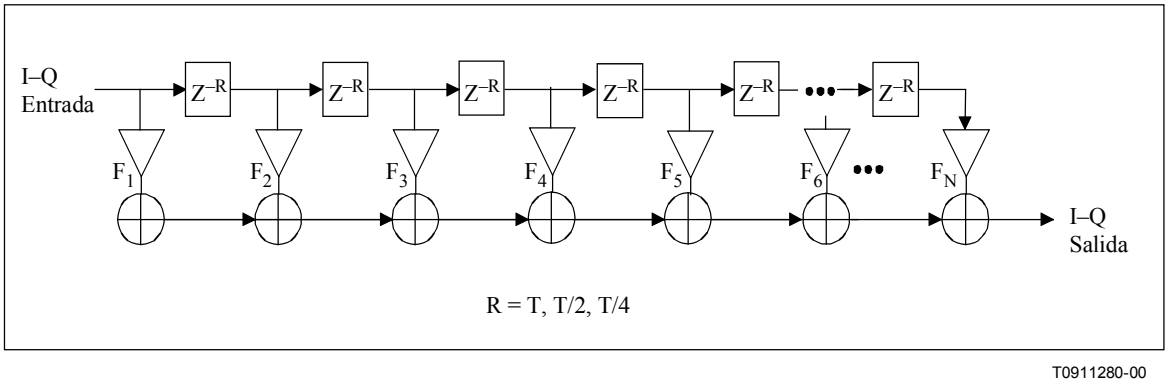


Figura B.N-5/J.112 – Estructura del ecualizador previo de transmisión

El mensaje MAC RNG-RSP (véase B.8.3.6.1) utiliza 16 bits por coeficiente en notación de complemento a dos fraccional: "s1.14" (bit de signo, bit de entero, punto binario y 14 bits fraccionales) para definir la información de ecualización de la transmisión del CM. El CM DEBE convolucionar los coeficientes enviados por el CMTS con los coeficientes existentes para obtener los coeficientes nuevos.

En respuesta a una petición de alineación inicial y a peticiones de alineación periódicas, anteriores al registro del CM, cuando el CMTS envía los coeficientes del ecualizador previo, DEBE calcularlos y enviarlos con una longitud de ecualizador de 8 y en formato de reparación de símbolos. Tras el registro, el CMTS PUEDE utilizar un formato de ecualizador separado fraccionalmente (separación T/2 o T/4) que tenga una longitud de derivación mayor para poder adaptarse a las capacidades del ecualizador previo del CM, que el CMTS aprendió del campo capacidades del módem del mensaje REG-REQ. Véase en B.8.3.8.1.1 la utilización apropiada del campo capacidades del módem.

Antes de efectuar una petición de alineación inicial y siempre que cambie la frecuencia o la velocidad de símbolos del canal ascendente, el CM DEBE inicializar los coeficientes del ecualizador previo con los valores correspondientes a una fijación por defecto en la que todos los coeficientes son 0 excepto el coeficiente real de la primera derivación (es decir, F_1). Durante la alineación inicial, el CM, y no el CMTS, DEBE compensar el retardo (desplazamiento de la alineación) debido a un desplazamiento desde la primera derivación a una nueva ubicación de la derivación principal de los coeficientes del ecualizador enviada por el CMTS. Los coeficientes del ecualizador previo se actualizan entonces mediante el proceso de alineación subsiguiente (mantenimiento de estación periódico). El CMTS NO DEBE variar la ubicación de la derivación principal durante el mantenimiento de estación periódico. Los coeficientes del ecualizador pueden ser incluidos en todos los mensajes RNG-RSP, pero normalmente sólo figuran cuando el CMTS encuentra que la respuesta del canal ha cambiado de forma significativa. La frecuencia de actualización de los coeficientes del ecualizador en el mensaje RNG-RSP la determina el CMTS.

El CM DEBE normalizar los coeficientes del ecualizador previo para garantizar un funcionamiento adecuado (es decir, sin desbordamientos ni recortes). El CM DEBE compensar además el cambio de la potencia de transmisión debido a la ganancia (o pérdida) de los nuevos coeficientes. Si la estructura del ecualizador CM implementa el mismo número de coeficientes que el de los asignados en el mensaje RNG-RSP, el CM NO DEBE cambiar la ubicación de la derivación principal en el mensaje RNG-RSP. Si la estructura del ecualizador CM implementa un número de coeficientes diferente del de los definidos en el mensaje RNG-RSP, el CM PUEDE variar la ubicación del valor de la derivación principal. Al hacer eso, el CM DEBE, de nuevo, ajustar su desplazamiento de alineación, además de cualquier otro ajuste en el mensaje RNG-RSP, en una cantidad que compense la variación de la ubicación de la derivación principal.

B.N.6.2.7 Perfiles de ráfagas

Las características de la transmisión se dividen en tres categorías:

a) parámetros de canal;

b) atributos de perfil de ráfaga; y

c) parámetros exclusivos del usuario.

Los parámetros de canal incluyen:

i) la velocidad de símbolos (cinco velocidades, desde 160 ksímb/s a 2,56 Msímb/s en pasos de octava);

ii) la frecuencia central (Hz); y

iii) la supercadena de preámbulo de 1024 bits.

La descripción de los parámetros de canal prosigue con más detalle en B.8.3.3, cuadro B.8-18; esas características son compartidas por todos los usuarios en un canal determinado. La relación de los atributos de perfil de ráfaga figura en el cuadro B.N-6 y se describen con más detalle en B.8.3.3, cuadro B.8-19; estos parámetros son los atributos compartidos correspondientes a un tipo de ráfaga. Los parámetros exclusivos del usuario pueden variar para cada usuario incluso cuando utilizan el mismo tipo de ráfaga por el mismo canal que otro usuario (por ejemplo, el nivel de potencia) y su relación figura en el cuadro B.N-7.

Cuadro B.N-6/J.112 – Atributos de perfil de ráfaga

Parámetro	Fijaciones de configuración
Modulación	QPSK, 16QAM
Codificación diferencial	Activa/inactiva
Longitud del preámbulo	0-1024 bits (véase B.N.6.2.5)
Desplazamiento de valor de preámbulo	0 a 1022
Corrección de errores FEC (octetos T)	0 a 10 (0 implica FEC inactiva)
Octetos de información de la palabra de código FEC(k)	Fija: 16 a 253 (suponiendo FEC activa) Abreviada: 16 a 253 (suponiendo FEC activa)
Semilla del aleatorizador	15 bits
Longitud de ráfaga máxima (miniintervalos de tiempo) (véase la nota)	0 a 255
Tiempo de guarda	5 a 255 símbolos
Longitud de última palabra de código	Fija, abreviada
Aleatorizador activo/inactivo	Activo/inactivo
NOTA – Una longitud de ráfaga de 0 miniintervalos de tiempo en el perfil del canal significa que la longitud de las ráfagas es variable en ese canal para ese tipo de ráfaga. La longitud de ráfaga, aunque no sea fija, la adjudica explícitamente el CMTS al CM en el MAP.	

Cuadro B.N-7/J.112 – Parámetros en ráfaga exclusivos de usuario

Parámetro	Fijaciones de configuración
Nivel de potencia (véase la nota)	+8 a +55 dBmV (16QAM) +8 a +58 dBmV (QPSK) 1 dB pasos
Frecuencia de desplazamiento (véase la nota)	Gama = ±32 kHz; incremento = 1 Hz; implementación ±10 Hz
Desplazamiento de la alineación	0 a (2^{16} – 1), incrementos de 6,25 µs/64
Longitud de ráfaga (miniintervalos de tiempo) si es variable en este canal (cambia de ráfaga a ráfaga)	1 a 255 miniintervalos de tiempo
Coeficientes de ecualizador de transmisión 1 (véase la nota) (módems avanzados solamente)	Hasta 64 coeficientes; 4 octetos por coeficiente: 2 reales y 2 complejos
NOTA – Los valores del cuadro son aplicables para este determinado canal y esta precisa velocidad de símbolos.	

El CM DEBE generar cada ráfaga en el momento apropiado indicado en las concesiones de miniintervalos de tiempo proporcionadas por los MAP del CMTS (véase B.8.3.4).

El CM DEBE soportar todos los perfiles de ráfaga indicados por el CMTS vía descriptores de ráfaga UCD (véase B.8.3.3) y originados subsiguientemente para transmisión en un MAP (véase B.8.3.4).

El CM DEBE implementar la frecuencia de desplazamiento con una aproximación de ±10 Hz.

El desplazamiento de alineación es la corrección de retardo aplicada por el CM al tiempo de trama en sentido ascendente del CMTS derivado en el CM, para sincronizar las transmisiones en sentido ascendente en el esquema TDMA. El desplazamiento de alineación es un avance equivalente aproximadamente al tiempo de propagación de ida y vuelta del CM con respecto al CMTS. El CMTS DEBE proporcionar al CM la corrección de este desplazamiento por realimentación, en base a la recepción satisfactoria de una o más ráfagas (es decir, resultado satisfactorio de cada una de las técnicas empleadas: corrección de errores y/o CRC), con una exactitud de 1/2 símbolo o mejor y una resolución de 1/64 del incremento de tics de trama (6,25 µs/64 = 0,09765625 µs = 1/4 de la duración de un símbolo de la velocidad de símbolos más elevada = 10,24 MHz^{-1}). El CMTS envía ajustes al CM, en donde un valor negativo significa que el desplazamiento de alineación se ha de disminuir, dando lugar a tiempos de transmisión posteriores en el CM. El CM DEBE implementar la corrección con una resolución equivalente a la duración de 1 símbolo como máximo (de la velocidad de símbolos utilizada para una ráfaga dada), y (aparte de un sesgo fijo) con una exactitud de ±0,25 µs más ±1/2 símbolo debido a la resolución. La exactitud de la temporización de ráfagas del CM de ±0,25 µs más ±1/2 símbolo está referida a los límites del miniintervalo de tiempo obtenible en el CM, en base a un procesamiento ideal de las señales de indicación de tiempo recibidas del CMTS.

El CM debe ser capaz de cambiar de perfiles de ráfagas sin que se requiera tiempo de reconfiguración entre ráfagas, salvo en el caso en que cambien los siguientes parámetros:

1) potencia de salida;
2) modulación;
3) velocidad de símbolos;
4) frecuencia de desplazamiento;
5) frecuencia de canal; y
6) desplazamiento de alineación.

Para velocidad de símbolos, frecuencia de desplazamiento y desplazamiento de alineación, el CM DEBE ser capaz de transmitir ráfagas consecutivas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente. El tiempo de reconfiguración máximo de 96 símbolos debe competir por el tiempo de rampa descendente de una ráfaga y el tiempo de rampa ascendente de la ráfaga siguiente así como el tiempo de retardo de transmisión total incluyendo el retardo de conducto y el retardo del ecualizador previo opcional. Para cambios de tipo de modulación, el CM DEBE ser capaz de transmitir ráfagas consecutivas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente. La potencia de salida transmitida, la velocidad de símbolos, la frecuencia de desplazamiento y el desplazamiento de alineación NO DEBEN cambiar mientras esté pendiente de transmisión más de -30 dB de la energía de cualquier símbolo de la ráfaga anterior, o si se ha transmitido más de –30 dB de la energía de cualquier símbolo de la ráfaga siguiente. La modulación NO DEBE cambiar mientras esté pendiente de transmisión más de –30 dB de la energía de cualquier símbolo de la ráfaga anterior, o si se ha transmitido más de –30 dB de la energía de cualquier símbolo de la ráfaga siguiente, EXCLUYENDO el efecto del ecualizador (si está presente en el CM). (Esto se ha de verificar cuando el ecualizador de transmisión no proporcione filtrado; sólo retardo, en todo caso. Se señala que si el CMTS tiene retroalimentación de decisión en su ecualizador, quizás necesite proporcionar más que el intervalo de 96 símbolos entre las ráfagas de tipo de modulación diferente que puede utilizar el CM; el CMTS tiene que decidir al respecto.) Ajustes por desplazamiento de alineación negativo harán que se viole el tiempo de guarda de los 96 símbolos. El CMTS tiene que garantizar que esto no ocurre permitiendo un tiempo de guarda adicional entre ráfagas que sea por lo menos igual al desplazamiento de alineación negativo.

Si se ha de cambiar la frecuencia del canal, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 100 ms entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

La frecuencia de canal del CM DEBE estabilizarse teniendo en cuenta los requisitos de ruido de fase y exactitud de B.N.6.9.5 y B.N.6.9.6 dentro de los 100 ms que siguen al comienzo del cambio.

Si la potencia de salida se va a cambiar en 1 dB o menos, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 5 μs entre el centro del último símbolos de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

Si la potencia de salida se va a cambiar en más de 1 dB, el CM DEBE ser capaz de implementar el cambio entre ráfagas en tanto en cuanto el CMTS atribuya por lo menos 96 símbolos más 10 μs entre el centro del último símbolo de una ráfaga y el centro del primer símbolo de la ráfaga siguiente.

La potencia de salida del CM DEBE estabilizarse a ±0,1 dB o menos de su nivel de potencia de salida final:

a) dentro de los 5 μs a partir del comienzo de un cambio de 1 dB o menos; y

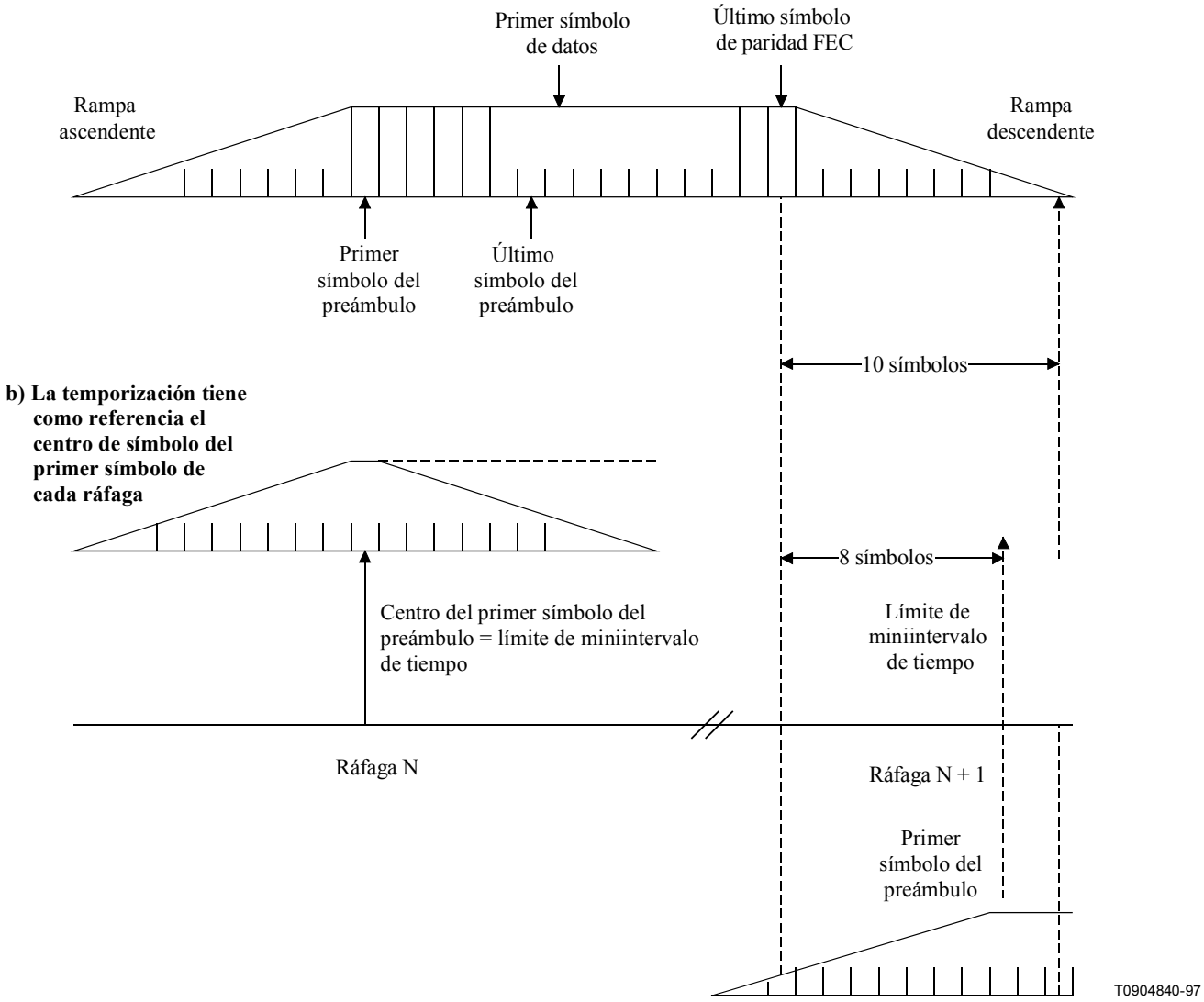
b) dentro de los 10 μs a partir del comienzo de un cambio de más de 1 dB.

La potencia transmisión de salida DEBE mantenerse constante dentro de una ráfaga TDMA a menos de 0,1 dB (excluyendo la cantidad presente en teoría a causa de la conformación del impulso, y a la modulación de amplitud en caso de 16QAM).

B.N.6.2.8 Convenio de temporización de ráfagas

La figura B.N-6 ilustra la temporización de una ráfaga nominal.

a) Perfil de ráfaga nominal (sin errores de temporización); se ilustra una banda de guarda de 8 símbolos; se ilustra una rampa ascendente y una rampa descendente de 10 símbolos.



NOTA – La rampa descendente de una ráfaga puede solapar la rampa ascendente de la ráfaga siguiente incluso cuando un transmisor tiene asignadas ambas ráfagas.

Figura B.N-6/J.112 – Temporización de ráfaga nominal

La figura B.N-7 indica la temporización de una ráfaga en el caso más desfavorable. En este caso, la ráfaga N llega con 1,5 símbolos de retardo y la ráfaga N + 1 llega con 1,5 símbolos de adelanto, pero se mantiene la separación de 5 símbolos; se muestra la banda de guarda de 8 símbolos.

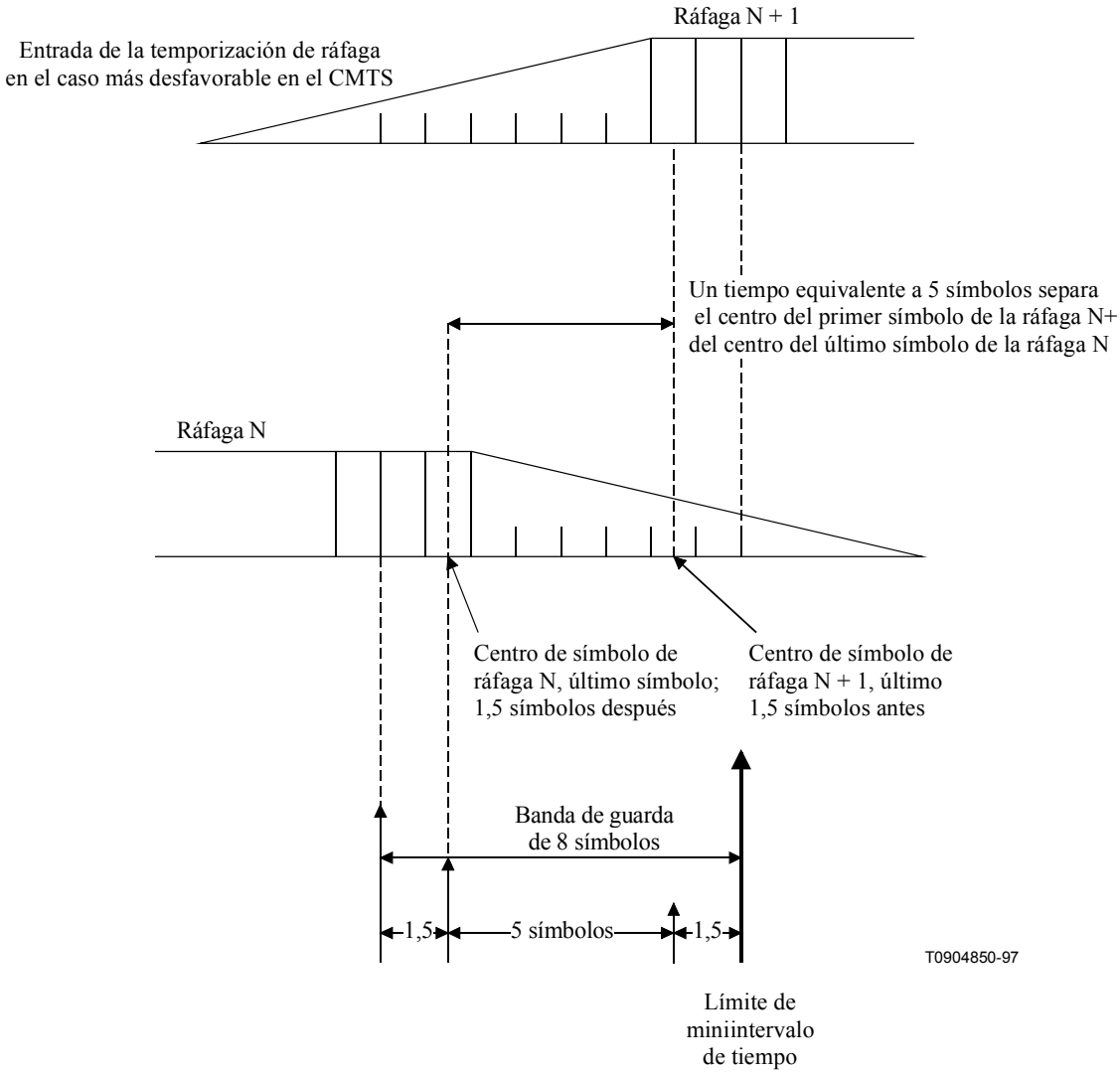


Figura B.N-7/J.112 – Temporización de ráfaga en el caso más desfavorable

Con una velocidad de símbolos de Rs, los símbolos se producen con una cadencia de uno cada Ts = 1/Rs segundos. Las rampas ascendente y descendente representan la dispersión de un símbolo en el dominio temporal más allá del periodo de duración Ts debido al filtro de conformación de símbolos. Si sólo se transmitiera un símbolo, su duración sería superior a Ts porque la respuesta en impulsos del filtro de conformación es superior a Ts. La dispersión del primero y el último símbolos de una transmisión de ráfaga amplía efectivamente la duración de la ráfaga haciendo que sea superior a N × Ts, donde N es el número de símbolos de la ráfaga.

B.N.6.2.9 Requisitos con respecto a la potencia de la transmisión

La subcapa PMD en sentido ascendente DEBE soportar la variación de la cantidad de potencia de la transmisión. Se establecen requisitos con respecto a:

1) la gama de potencia de transmisión pedida;
2) el tamaño de los pasos de las peticiones de potencia; y
3) la exactitud (potencia de salida efectiva en comparación con la cantidad pedida) de la respuesta a la petición.

El mecanismo según el cual se efectúan los ajustes de potencia se define en B.11.2.4. Dichos ajustes DEBEN quedar dentro de las gamas de tolerancia que se describen a continuación.

B.N.6.2.9.1 Agilidad y gama de la potencia de salida

La potencia de transmisión de salida en la anchura de banda de diseño DEBE ser variable en la gama de +8 dBmV a 55 dBmV (16QAM), 58 dBmV (QPSK), en pasos de 1 dB.

La exactitud absoluta de la potencia transmitida DEBE ser de ±2 dB, y la del tamaño de los pasos, de ±0,4 dB, con un margen por histéresis al activar/desactivar un atenuador por etapas (por ejemplo, 20 dB) en cuyo caso el requisito de exactitud se rebaja a ±1,4 dB. Por ejemplo, el incremento efectivo de potencia resultante de una petición de que se aumente el nivel de potencia en 1 dB en la siguiente ráfaga transmitida de un CM DEBE estar entre 0,6 y 1,4 dB.

La resolución de un paso DEBE ser de 1 dB o menos. Cuando a un CM se le indique una resolución mayor de la que él puede implementar, DEBE redondear al tamaño de paso soportado más cercano. Si el paso indicado está a mitad de camino entre dos tamaños de paso soportados, el CM DEBE elegir el paso más pequeño. Por ejemplo, con una resolución de paso soportada de 1 dB, la indicación de variar en ±0,5 dB no provocaría variación alguna, mientras que una indicación de variación de ±0,75 dB daría lugar a una variación o paso de ±1 dB.

B.N.6.2.10 Requisitos de fidelidad

B.N.6.2.10.1 Emisiones espurias

El ruido y la potencia espuria NO DEBEN exceder de los niveles que se indican en los cuadros B.N-8, B.N-9 y B.N-10.

En el cuadro B.N-8, las emisiones espurias dentro de banda incluyen el ruido, la fuga de portadora, las líneas de reloj, los productos espurios de sintetizador y otros productos de transmisor no deseados. No incluye ISI. La anchura de banda de medición de las emisiones no esenciales dentro de banda es igual a la velocidad de símbolos (por ejemplo, 160 kHz para 160 ksímb/s).

Cuadro B.N-8/J.112 – Emisiones no esenciales

Parámetro	Ráfaga transmisora	Entre ráfagas
Dentro de banda [entre las emisiones no esenciales dentro de banda figuran el ruido, la fuga de portadora, las líneas de reloj, los productos espurios de sintetizador y otros productos de transmisor no deseados. No se incluye la interferencia entre símbolos (ISI)]	–40 dBc	–72 dBc o 5 dBµV, lo que sea mayor
Banda adyacente	Véase el cuadro B.N-9	–72 dBc o 5 dBµV, lo que sea mayor
Tres bandas de frecuencia o menos relacionadas con la portadora (a modo de segundo armónico, si <65 MHz)	–47 dBc	–72 dBc o 5 dBµV, lo que sea mayor
Bandas dentro de 5 a 65 MHz (excluyendo el canal asignado, los canales adyacentes y los canales relacionados con la portadora)	Véase el cuadro B.N-10	–72 dBc o 5 dBµV, lo que sea mayor
Límites de las emisiones espurias integradas en el CM (todas en 250 kHz, incluidos valores discretos) 87,5 a 108 MHz	30 dBµV	5 dBµV

Cuadro B.N-8/J.112 – Emisiones no esenciales

Parámetro	Ráfaga transmisora	Entre ráfagas
Límites de las emisiones espurias integradas en el CM (todas en 4,75 MHz, incluidos valores discretos) (nota 1)		
65 a 87,5 MHz 108 a 136 MHz (nota 3) 136 a 862 MHz	máx –40 dBc, 34 dBµV 20 dBµV 15 dBµV	34 dBµV 15 dBµV máx (15 dBµV, –40 dBc) (Nota 2)
Límites des las emisiones espurias discretas en el CM (Nota 1)		
65 a 87,5 MHz 108 a 862 MHz	máx –50 dBc, –24 dBµV 10 dBµV	24 dBV 10 dBV
NOTA 1 – Estos límites de especificador excluyen una salida espuria discreta única relacionada con el canal recibido sintonizado; la salida espuria discreta única NO DEBE ser superior a 20 dBµV. NOTA 2 – dBc se refiere al nivel de señal recibida en sentido descendente. Algunas salidas espurias son proporcionales al nivel de señal recibida. NOTA 3 – Las frecuencias de 108 a 136 MHz pueden estar prohibidas debido a los reglamentos nacionales. NOTA 4 – Estos límites de especificador excluyen tres o menos salidas espurias discretas. Esas salidas espurias NO DEBEN ser superiores a 20 dBµV.		

La anchura de banda de medición de las 3 (o menos) bandas de frecuencia relacionadas con la portadora (por debajo de 65 MHz) es de 160 kHz, con 3 bandas como máximo de 160 kHz, cada una de ellas con no más de –47 dBc, que se permite excluir de las especificaciones de "Bandas dentro de 5 a 65 MHz de la ráfaga transmisora" del cuadro B.N-10.

La anchura de banda de medición es también de 160 kHz para las especificaciones entre ráfagas del cuadro B.N-8 por debajo de 65 MHz; las especificaciones de ráfagas transmisoras son aplicables durante los miniintervalos de tiempo concedidos al CM (cuando el CM utiliza la totalidad o una parte de la concesión), y durante un miniintervalo de tiempo antes y después de los miniintervalos de tiempo concedidos. (Se señala que un miniintervalo de tiempo puede ser tan breve como 32 símbolos, ó 12,5 µs a la velocidad de 2,56 Msímb/s, o 200 µs a 160 ksímb/s.) Las especificaciones de ráfagas transmisoras se aplican salvo durante la utilización de una concesión de miniintervalos de tiempo, y durante el miniintervalo de tiempo anterior y el posterior a la concesión utilizada.

B.N.6.2.10.1.1 Emisiones espurias en canal adyacente

Las emisiones no esenciales procedentes de una portadora transmitida pueden producirse en un canal adyacente que pudiera estar ocupado por una portadora con las mismas o diferentes velocidades de símbolos. El cuadro B.N-9 contiene la relación de niveles de emisiones espurias en canal adyacente requeridos para todas las combinaciones de velocidades de símbolos de portadora transmitida y velocidades de símbolos de canal adyacente. La medición se efectúa en un intervalo de canal adyacente cuya anchura de banda y distancia con respecto a la portadora transmitida son las apropiadas en base a las velocidades de símbolos de la portadora transmitida y la portadora del canal adyacente.

Cuadro B.N-9/J.112 – Emisiones no esenciales en canal adyacente

Velocidad de símbolos de la portadora transmitida	Especificación en el intervalo	Intervalo de medición y distancia con respecto al borde de la portadora	Velocidad de símbolos de la portadora del canal adyacente
160 ksímb/s	–45 dBc	20 a 180 kHz	160 ksímb/s
	–45 dBc	40 a 360 kHz	320 ksímb/s
	–45 dBc	80 a 720 kHz	640 ksímb/s
	–42 dBc	160 a 1440 kHz	1280 ksímb/s
	–39 dBc	320 a 2880 kHz	2560 ksímb/s
Todas las demás velocidades de símbolos	–45 dBc	20 a 180 kHz	160 ksímb/s
	–45 dBc	40 a 360 kHz	320 ksímb/s
	–45 dBc	80 a 720 kHz	640 ksímb/s
	–44 dBc	160 a 1440 kHz	1280 ksímb/s
	–41 dBc	320 a 2880 kHz	2560 ksímb/s

B.N.6.2.10.1.2 Emisiones espurias en 5 a 65 MHz

Las emisiones espurias, distintas de las del canal adyacente o las emisiones relacionadas con la portadora e indicadas más arriba, se pueden producir en intervalos que podrían estar ocupados por otras portadoras, con las mismas o diferentes velocidades de símbolos. Para acomodar estas velocidades de símbolos diferentes y anchuras de banda asociadas, las emisiones espurias se miden en un intervalo igual a la anchura de banda correspondiente a la velocidad de símbolos de la portadora que pudiera ser transmitida en ese intervalo. Ese intervalo es independiente de la velocidad con que se transmitan los símbolos en ese momento.

El cuadro B.N-10 contiene la relación de posibles velocidades de símbolos que pudieran ser transmitidas en un intervalo, el nivel de emisión espuria requerido en ese intervalo, y el nivel de medición inicial en que se han de empezar a medir las emisiones espurias. Las mediciones deberán comenzar en la distancia inicial y repetirse con distancias crecientes con respecto a la portadora hasta que se alcance el borde de la banda en sentido ascendente, 5 MHz o 65 MHz. Los intervalos de medición no deberán incluir emisiones relacionadas con la portadora.

Cuadro B.N-10/J.112 – Emisiones espurias en 5 a 65 MHz

Posible velocidad de símbolos en este intervalo	Especificación en el intervalo	Intervalo de medición inicial y distancia con respecto al borde de la portadora
160 ksímb/s	–53 dBc	220 a 380 kHz
320 ksímb/s	–50 dBc	240 a 560 kHz
640 ksímb/s	–47 dBc	280 a 920 kHz
1280 ksímb/s	–44 dBc	360 a 1640 kHz
2560 ksímb/s	–41 dBc	520 a 3080 kHz

B.N.6.2.10.2 Emisiones espurias durante los transitorios de activación/desactivación en ráfagas

Cada transmisor DEBE controlar las emisiones espurias, antes y durante la rampa ascendente y durante y después de la rampa descendente, con anterioridad y con posterioridad a una ráfaga en el esquema TDMA.

Las emisiones espurias de activación/desactivación, tales como las del cambio de tensión a la salida de un transmisor en sentido ascendente debido a la habilitación o inhabilitación de la transmisión, NO DEBEN ser superiores a 100 mV, y ese paso incremental NO DEBE disiparse antes de 2 μs siguiendo un desarrollo de pendiente constante. Este requisito se aplica cuando el CM transmite a +115 dBμV o más; con niveles de transmisión reducidos, el cambio máximo de tensión DEBE disminuir con un factor de 2 para cada 6 dB de disminución del nivel de potencia a partir de +115 dBμV, hasta un cambio máximo de 7 mV a 91 dBμV y por debajo. Este requisito no es aplicable a los transitorios de activación y desactivación de potencia del CM.

En el caso de transitorios de corriente continua inferiores a 7 mV no es preciso tener en cuenta la limitación de tasa de desarrollo de pendiente constante de 2 μs.

B.N.6.2.10.3 Tasa de errores en los símbolos (SER, *symbol error rate*)

La calidad de funcionamiento del modulador DEBE ser tal que su salida se encuentre a 0,5 dB o menos de la SER teórica en función de la relación C/N (es decir, E_s/N_o), para una SER tan baja como 10^{-6} sin codificación, para QPSK y 16QAM.

La degradación de la SER viene determinada por la varianza de conglomerado que provoca la forma de onda de transmisión a la salida de un filtro teórico de recepción de raíz cuadrada de coseno alzado. Incluye los efectos de la ISI, las emisiones espurias, el ruido de fase, y todas las demás degradaciones del transmisor.

La relación señal/ruido (SNR, *signal/noise ratio*) deberá medirse en un analizador de modulación que utilice filtro de recepción de raíz cuadrada de coseno alzado con alfa = 0,25. La SNR medida DEBE ser superior a 30 dB.

El CM DEBE ser capaz de conseguir una SNR de agrupación de al menos 27 dB en presencia de las microrreflexiones de canal definidas en el cuadro B.N-2. Puesto que el cuadro no pone límites al retardo del eco en el caso de −30 dBc, se supone a efectos de prueba que la duración del eco con esa magnitud es inferior o igual a 1,5 μs.

B.N.6.2.10.4 Distorsión de filtro

En los requisitos que siguen se supone que cualquier ecualización previa está inhabilitada.

B.N.6.2.10.4.1 Amplitud

La plantilla del espectro DEBE ser el espectro teórico de raíz cuadrada de coseno alzado con alfa = 0,25, dentro de las gamas que se indican a continuación:

f_c

$f_c - R_s/4\text{Hz}$ a $f_c + R_s/4\text{Hz}: -0{,}3$ dB a 0,3dB

$f_c - 3R_s/8\text{Hz}$ a $f_c - R_s/4\text{Hz}$, y $f_c + R_s/4\text{Hz}$ a $f_c + 3R_s/8\text{Hz}: -0{,}5$ dB a 0,3 dB

$f_c - R_s/2\text{Hz}$ y $f_c + \text{Rs}/2\text{Hz}: -3{,}5\text{dB}$ a $-2{,}5\text{dB}$

$f_c - 5R_s/8\text{Hz}$ y $f_c + 5R_s/8\text{Hz}$: no superior a -30 dB

donde f_c es la frecuencia central, R_s es la velocidad de símbolos y la densidad espectral se mide con una anchura de banda de resolución de 10 kHz o menos.

B.N.6.2.10.4.2 Fase

$f_c - 5R_s/8$ Hz a $f_c + 5R_s/8$ Hz: la variación del retardo de grupo NO DEBE ser superior a 100 ns.

B.N.6.2.10.5 Ruido de fase de portadora

El ruido de fase integrado total del transmisor en sentido ascendente (incluido el ruido espurio discreto) DEBE ser inferior o igual a –43 dBc, teniendo en cuenta las regiones espectrales que se extienden de 1 kHz a 1,6 MHz por encima y por debajo de la portadora.

B.N.6.2.10.6 Exactitud de la frecuencia de canal

El CM DEBE implementar la frecuencia de canal asignada con una exactitud de ±50 partes por millón con una gama de temperaturas de 0 a 40° C hasta cinco años después de la fecha de fabricación.

B.N.6.2.10.7 Exactitud de la velocidad de símbolos

El modulador en sentido ascendente DEBE proporcionar una exactitud absoluta de velocidad de símbolos de ±50 partes por millón con una gama de temperaturas de 0 a 40° C hasta cinco años después de la fecha de fabricación.

B.N.6.2.10.8 Fluctuación de fase de la temporización de símbolos

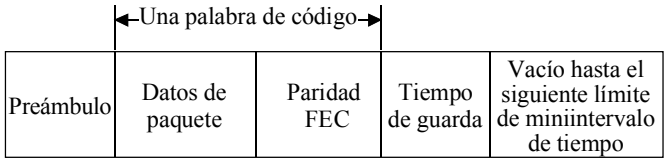
La fluctuación de fase cresta a cresta de los símbolos, referida al cruce de cero de símbolos, de la forma de onda transmitida, DEBE ser inferior al 0,02 de la duración nominal de un símbolo durante un periodo de 2 s. En otras palabras, la diferencia entre la duración máxima y mínima de un símbolo durante el periodo de 2 s deberá ser inferior al 0,02 de la duración nominal de un símbolo para cada una de las cinco velocidades de símbolos en sentido ascendente.

El error de fase acumulado cresta a cresta, referido al momento del primer símbolo y descontado cualquier desplazamiento fijo de la frecuencia de símbolos, DEBE ser inferior al 0,04 de la duración nominal de un símbolo durante un periodo de 0,1 s. En otras palabras, la diferencia entre el error de fase acumulado máximo y mínimo durante el periodo de 0,1 s deberá ser inferior al 0,04 de la duración nominal de un símbolo para cada una de las cinco velocidades de símbolos en sentido ascendente. La eliminación de un desplazamiento fijo de la frecuencia de símbolos se ha de hacer utilizando la duración media de los símbolos calculada durante el periodo de 0,1 s.

B.N.6.2.11 Estructura de trama

La figura B.N-8 muestra dos ejemplos de estructura de trama; uno en el que la longitud de los paquetes es igual al número de octetos de información de una palabra de código, y otro en el que la longitud de los paquetes es superior al número de octetos de información de una palabra de código, pero inferior al de dos palabras de código. El ejemplo 1 ilustra el modo longitud de palabra de código fija, y el ejemplo 2, el modo última palabra de código abreviada. Ambos modos se definen en B.N.6.11.1.

Ejemplo 1 – Longitud de paquete = número de bytes de información de la palabra de código = k



Ejemplo 2 – Longitud de paquete = k + bytes de información restantes en la segunda palabra de código = $k + k' \leq k + k'' \leq 2k$ bytes

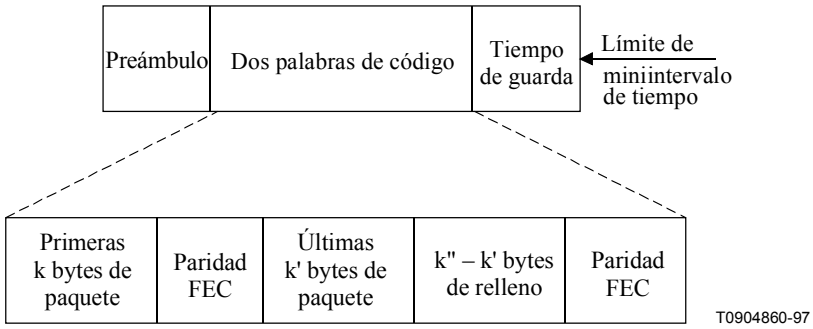


Figura B.N-8/J.112 – Ejemplo de estructura de trama con modo longitud de ráfagas flexible

B.N.6.2.11.1 Longitud de palabra de código

Cuando FEC está habilitada, el CM funciona en modo palabras de código de longitud fija o en modo última palabra de código abreviada. El número mínimo de octetos de información en una palabra de código en cualquiera de los modos es 16. El modo última palabra de código abreviada sólo resulta ventajoso cuando el número de octetos en una palabra de código es superior al mínimo de 16 bytes.

Las descripciones que siguen son aplicables a una concesión de miniintervalos de tiempo atribuida tanto en regiones de competencia como de no competencia. (La atribución de miniintervalos de tiempo se examina en B.8. La descripción tiene por objeto definir las reglas y los convenios que permitan a los CM pedir el número adecuado de miniintervalos de tiempo y que la capa PHY del CMTS sepa lo que cabe esperar con respecto a la alineación de trama FEC, tanto en el modo longitud de palabra de código fija como en el modo última palabra de código abreviada.

B.N.6.2.11.1.1 Longitud de palabra de código fija

Con las palabras de código de longitud fija, una vez codificados todos los datos, se rellenarán con octetos de valor cero si tal cosa hace falta para alcanzar los k octetos de datos asignados por palabra de código, y el relleno con octetos de valor cero DEBE continuar hasta que ya no puedan insertarse más palabras de código de longitud fija antes del final del último miniintervalo de tiempo atribuido en la concesión, teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda.

B.N.6.2.11.1.2 Última palabra de código abreviada

Como se muestra en la figura B.N-8, k' es el número de octetos de información que quedan después de dividir los octetos de información de la ráfaga en palabras de código de longitud total (k octetos de datos en ráfaga). El valor de k' es inferior al de k. Suponiendo funcionamiento en modo última palabra de código abreviada, sea k'' el número de octetos de datos de la ráfaga más los octetos de relleno de valor cero de la última palabra de código abreviada. En el modo palabra de código abreviada, el CM codificará los octetos de datos de la ráfaga (incluido el encabezamiento MAC) utilizando el tamaño de palabra de código asignado (k octetos de información por palabra de código) hasta que:

1) todos los datos estén codificados; o

2) quede un resto de octetos de datos inferior a k.

Las últimas palabras de código abreviadas no deberán tener menos de 16 octetos de información, y esto es algo que hay que tener en cuenta cuando los CM pidan miniintervalos de tiempo. En el modo última palabra de código abreviada, el CM se DEBE llenar con datos de valor cero si es necesario hasta el final de la atribución del miniintervalo de tiempo, lo que la mayoría de las veces ocurrirá en el siguiente límite de un miniintervalo de tiempo, teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda. En muchos casos, sólo serán necesarios k" – k' octetos de relleno de valor cero para llenar una atribución de miniintervalos de tiempo con $16 \leq k \leq k$ y $k' \leq k"$. No obstante, conviene tener en cuenta lo que sigue.

De manera más general, el CM DEBE rellenar datos con octetos de valor cero hasta que ya no puedan insertarse más palabras de código de longitud fija antes del final del último miniintervalo de tiempo atribuido en la concesión (teniendo en cuenta los símbolos de paridad FEC y de tiempo de guarda), y a continuación, si se puede, deberá insertarse una última palabra de código abreviada de relleno con octetos de valor cero para que encaje en la atribución de miniintervalos de tiempo.

Si, tras rellenar con octetos de valor cero palabras de código adicionales de k octetos de información quedan menos 16 octetos en la concesión atribuida de miniintervalos de tiempo, teniendo en cuenta los símbolos de paridad y tiempo de guarda, el CM no deberá crear esta última palabra de código abreviada.

B.N.6.2.12 Requisitos del procesamiento de la señal

El orden de procesamiento de una señal para cada tipo de paquete en ráfaga DEBE ser compatible con la secuencia que se muestra en la figura B.N-9 y DEBE seguir el orden de los pasos que se indica en la figura B.N-10.

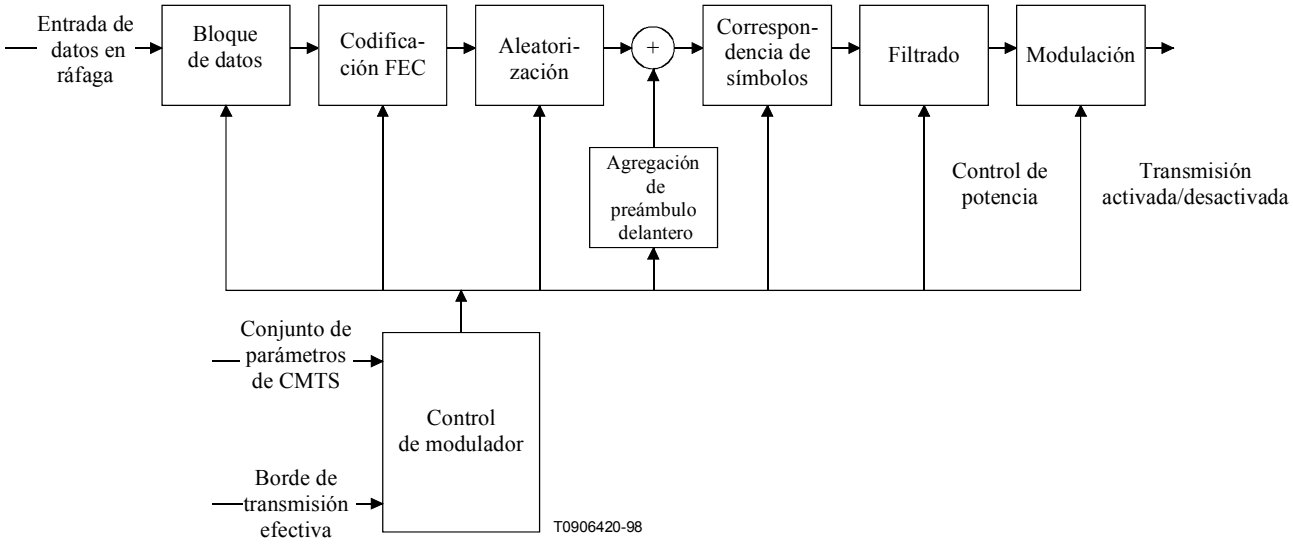


Figura B.N-9/J.112 – Secuencia de procesamiento de señal

	Entrada de tren de paquetes
	⇓
Bloques de datos	Separación de paquetes en bloques de información (= octetos de datos en una palabra de código)
	⇓
Codificación FEC	Codificación FEC (Reed-Solomon) de cada bloque de información, utilizando una palabra de código abreviada para el último bloque si es necesario. La FEC puede ser desactivada
	⇓
Aleatorización	Aleatorización (véase B.N.6.2.4)
	⇓
Agregación de preámbulo delantero	Símbolos de agregación de preámbulo delantero
	⇓
Correspondencia de símbolos	Correspondencia entre símbolos el tren de datos y símbolos del modulador
	⇓
Filtrado	Filtrado del tren de símbolos para conformación del espectro
	⇓
Modulación	Modulación en tiempos precisos (QPSK; 16QAM)
	⇓
	Salida de ráfagas de formas de onda RF

Figura B.N-10/J.112 – Procesamiento de la transmisión en sentido ascendente con TDMA

B.N.6.2.13 Características de la potencia de entrada en el demodulador en el sentido ascendente

La potencia de entrada total máxima en el demodulador en sentido ascendente NO DEBE exceder de 95 dBµV en la gama de frecuencias de funcionamiento de 5 a 65 MHz.

El valor de la potencia que se trata de recibir en cada portadora DEBE estar entre los que se muestran en el cuadro B.N-11.

El demodulador DEBE operar ateniéndose a sus especificaciones definidas de calidad de funcionamiento con ráfagas recibidas dentro de un margen de ±6 dB con respecto a la potencia de recepción nominal pedida.

Cuadro B.N-11/J.112 – Gama máxima de potencia de recepción nominal pedida en cada portadora

Velocidad de símbolos (ksímb/s)	Gama máxima (dBµV)
160	44 a 74
320	47 a 77
640	50 a 80
1280	53 a 83
2560	56 a 86

B.N.6.2.14 Salida eléctrica del CM en sentido ascendente

El CM DEBE producir como salida una señal modulada RF con las características que se indican en el cuadro B.N-12.

Cuadro B.N-12/J.112 – Salida eléctrica del CM

Parámetro	Valor
Frecuencia	5 a 65 MHz borde a borde
Gama de niveles (un canal)	+68 a +115 dBµV (16QAM) +68 a +118 dBµV (QPSK)
Tipo de modulación	QPSK y 16QAM
Velocidad de símbolos (nominal)	160, 320, 640, 1280 y 2560 ksímb/s
Anchura de banda	200, 400, 800, 1600 y 3200 kHz
Impedancia de salida	75 ohmios
Pérdida de retorno de salida	> 6 dB (5 a 65 MHz)
Conector	Conector F (común con la entrada)

B.N.6.3 Sentido descendente

B.N.6.3.1 Protocolo en sentido descendente

La subcapa PMD en sentido descendente DEBE atenerse a [EN 300 429].

B.N.6.3.2 Intercalación

La subcapa PMD en el sentido descendente DEBE soportar un intercalador con las características definidas en el cuadro B.N-13. El modo intercalador cumple por completo con [EN 300 429].

Cuadro B.N-13/J.112 – Características del intercalador

I (Número de derivaciones)	J (Incremento)	Protección contra ráfagas 64QAM/256QAM	Latencia 64QAM/256QAM
12	17	18 µs/14 µs	0,43 ms/0,32 ms

B.N.6.3.3 Plan de frecuencias en sentido descendente

El plan de frecuencias en sentido descendente incluirá todas las frecuencias centrales entre 112 y 858 MHz con incrementos de 250 kHz. El operador deberá decidir qué frecuencias utiliza para cumplir los requisitos de red y a escala nacional.

B.N.6.3.4 Salida eléctrica del CMTS

El CMTS DEBE producir como salida una señal modulada RF con las características que se indican en el cuadro B.N-14.

Cuadro B.N-14/J.112 – Salida del CMTS

Parámetro	Valor
Frecuencia central (f_c)	112 a 858 MHz ± 30 kHz
Nivel	Ajustable en la gama de 110 a 121 dBμV
Tipo de modulación	64QAM y 256QAM
Velocidad de símbolos (nominal) 64QAM 256QAM	 6,952 Msímb/s 6,952 Msímb/s
Separación nominal de canales	8 MHz
Repuesta de frecuencia 64QAM 256QAM	Conformación de raíz cuadrada de coseno alzado de ~15 % Conformación de raíz cuadrada de coseno alzado de ~15 %
Total de emisiones espurias discretas dentro de banda (f_c ± 4 MHz)	< –57 dBc
Emisiones espurias y ruido dentro de banda (f_c ± 4 MHz)	< –46,7 dBc; donde las emisiones espurias y el ruido del canal incluyen todas las emisiones espurias discretas, el ruido, la fuga de portadora, las líneas de reloj, los productos de sintetizador y otros productos del transmisor no deseados. Se excluye el ruido dentro de ±50 kHz de la portadora.
Canal adyacente (f_c ± 4,0 MHz) a (f_c ±4,75 MHz)	< –58 dBc en 750 kHz.
Canal adyacente (f_c ± 4,75 MHz) a (f_c ±12 MHz)	< –60,6 dBc en 7,25 MHz, excluyendo hasta tres señales espurias cada una de las cuales debe ser < –60 dBc cuando se mide en una banda de 10 kHz.
Canal adyacente siguiente (f_c ± 12 MHz) a (f_c ± 20 MHz)	Inferior a –63,7 dBc o 49,3 dBμV, lo que sea mayor, en 8 MHz, excluyendo hasta tres señales espurias discretas. La potencia total en las señales espurias debe ser < –60 dBc cuando cada una de ellas se mide con una anchura de banda de 10 kHz.
Otros canales (80 MHz a 1000 MHz)	< 49,3 dBμV en cada uno de los canales de 8 MHz, excluyendo hasta tres señales espurias discretas. La potencia total en las señales espurias debe ser < −60 dBc cuando cada una de ellas se mide con una anchura de banda de 10 kHz.
Ruido de fase	1 kHz-10 kHz: Potencia de ruido de doble banda lateral de –33 dBc 10 kHz-50 kHz: Potencia de ruido de doble banda lateral de –51 dBc 50 kHz-3 MHz: Potencia de ruido de doble banda lateral de –51 dBc
Impedancia de salida	75 ohms
Pérdida de retorno de salida	> 14 dB dentro de un canal de salida de hasta 750 MHz; > 13 dB en un canal de salida por encima de 750 MHz
Conector	Conector F según [CEI 60169-24]

B.N.6.3.5 Entrada eléctrica en el CM en sentido descendente

El CM DEBE aceptar una señal modulada RF con las características siguientes (véase el cuadro B.N-15).

Cuadro B.N-15/J.112 – Entrada eléctrica en el CM

Parámetro	Valor
Frecuencia central	112 a 858 MHz ± 30 kHz
Gama de niveles (un canal)	43 a 73 dBµV para 64QAM 47 a 77 dBµV para 256QAM
Tipo de modulación	64QAM y 256QAM
Velocidad de símbolos (nominal)	6,952 Msímb/s (64QAM) y 6,952 Msímb/s (256QAM)
Anchura de banda	8 MHz (conformación de raíz cuadrada de coseno alzado de 15% para 64QAM y conformación de raíz cuadrada de coseno alzado de 15% para 256QAM)
Potencia de entrada total (80-862 MHz)	< 90 dBµV
Impedancia de entrada (load)	75 ohms
Pérdida de retorno de entrada	> 6 dB (85 a 862 MHz)
Conector	Conector F según [CEI 60169-24] (común con la salida)

B.N.6.3.6 Características de BER de CM

La característica de tasa de errores en los bits de un CM DEBE ser tal como se describe en esta cláusula. Los requisitos son aplicables al modo de intercalación I = 12, J = 17.

B.N.6.3.6.1 64QAM

B.N.6.3.6.1.1 Característica de BER de CM con 64QAM

La pérdida de implementación de un CM DEBE ser tal que el CM tenga una BER después de la FEC inferior o igual a 10^{-8} cuando funciona con una relación portadora/ruido (E_s/N_o) de 25,5 dB o superior.

B.N.6.3.6.1.2 Característica de rechazo de imagen con 64QAM

La característica que se describe en B.N.7.6.1.1 DEBE cumplirse con una señal analógica o digital a +10 dBc en cualquier tramo de la banda RF distinto de los canales adyacentes.

B.N.6.3.6.1.3 Calidad del canal adyacente con 64QAM

La característica descrita en B.N.7.6.1.1 DEBE cumplirse con una señal digital a 0 dBc en los canales adyacentes.

La característica descrita en B.N.7.6.1.1 DEBE cumplirse con una señal analógica a +10 dBc en los canales adyacentes.

La calidad descrita en B.N.7.6.1.1, con un margen adicional de 0,2 dB, DEBE cumplirse con una señal digital a +10 dBc en los canales adyacentes.

B.N.6.3.6.2 256QAM

B.N.6.3.6.2.1 Característica de BER de CM con 256QAM

La pérdida de implementación de un CM DEBE ser tal que el CM tenga una BER después de la FEC inferior o igual a 10^{-8} cuando se funcione con una relación portadora/ruido (E_s/N_o) como se muestra en el cuadro B.N-16.

Cuadro B.N-16/J.112 – Característica de BER con 256QAM

Nivel de señal de recepción de entrada	Es/No
47 dBµV a 54 dBµV	34,5 dB
> 54 a +77 dBµV	31,5 dB

B.N.6.3.6.2.2 Característica de rechazo de imagen con 256QAM

La característica descrita en B.N.7.6.2.1 DEBE cumplirse con una señal analógica o digital a +10 dBc en cualquier tramo de la banda RF distinto de los canales adyacentes.

B.N.6.3.6.2.3 Calidad del canal adyacente con 256QAM

La característica descrita en B.N.7.6.2.1 DEBE cumplirse con una señal analógica o digital a 0 dBc en los canales adyacentes.

La característica descrita en B.N.7.6.2.1, con un margen adicional de 0,5 dB, DEBE cumplirse con una señal analógica a +10 dBc en los canales adyacentes.

La característica descrita en B.N.7.6.2.1, con un margen adicional de 1,0 dB, DEBE cumplirse con una señal digital a +10 dBc en los canales adyacentes.

B.N.6.3.6.2.4 Especificaciones adicionales para QAM

Para la modulación QAM le dan las especificaciones adicionales siguiente.

Parámetro	Especificaciones
Desplazamiento de fase I/Q	< 1,0 °
Diafonía I/Q	≤ –50 dB
Desequilibrio de amplitud I/Q	0,05 dB máx.
Asimetría de la temporización I/Q	< 3,0 ns

B.N.6.3.7 Fluctuación de fase de la indicación de tiempo del CMTS

La fluctuación de fase de la indicación tiempo del CMTS debe ser inferior a 500 ns, cresta a cresta, a la salida de la subcapa de convergencia de transmisión en sentido descendente. Dicha fluctuación de fase está referida a una subcapa de convergencia de transmisión en sentido descendente teórica, que transfiere los datos del paquete MPEG a la subcapa dependiente de los medios físicos en sentido descendente con un reloj perfectamente continuo y estable a la velocidad de datos del paquete MPEG. El procesamiento de la subcapa dependiente de los medios físicos en sentido descendente NO DEBE ser considerado en la generación y transferencia de indicaciones de tiempo a la subcapa dependiente de los medios físicos en sentido descendente.

Así pues, cualesquiera dos indicaciones de tiempo N1 y N2 (N2 > N1), que fueron transferidas a la subcapa dependiente de los medios físicos en sentido descendente en los momentos T1 y T2 respectivamente, deben cumplir la siguiente relación:

$$\left| \frac{N2 - N1}{10\,240\,000} - (T2 - T1) \right| < 500ns$$

La fluctuación de fase incluye imprecisiones en el valor de las indicaciones de tiempo y la fluctuación de fase en todos los relojes. Los 500 ns asignados para fluctuación de fase a la salida de la subcapa de convergencia de transmisión en sentido descendente deben ser reducidos como consecuencia de cualquier fluctuación de fase que introduzca la subcapa dependiente de los medios físicos en sentido descendente.

Se prevé que el CM satisfaga los requisitos de exactitud de temporización de ráfaga de B.N.6.6 cuando las indicaciones de tiempo contengan esta fluctuación de fase de caso más desfavorable.

NOTA – La fluctuación de fase es el error (medido) con respecto al reloj maestro del CMTS. (El reloj maestro del CMTS es el reloj a 10,24 MHz utilizado para generar las indicaciones de tiempo.)

El reloj maestro a 10,24 MHz del CMTS DEBE tener una estabilidad de frecuencia de ≤ ±5 ppm (partes por millón), una velocidad de deriva de $\leq 10^{-8}$ por segundo y una fluctuación de borde de ≤ 10 ns cresta a cresta (±5 ns). (Los requisitos de velocidad de deriva y fluctuación de fase en el reloj maestro del CMTS entrañan el que la duración de dos segmentos adyacentes de 10 240 000 ciclos sea de 30 ns, 10 ns debidos a la fluctuación de fase mientras dura cada segmento y 10 ns debidos a la deriva de frecuencia. Se pueden deducir además otras duraciones del cómputo: 1 024 000 segmentos adyacentes, ≤ 21 ns; 1 024 000 segmentos de longitud separados por un segmento de 10 240 000 ciclos, ≤ 30 ns; 102 400 000 segmentos adyacentes, ≤ 120 ns. El reloj maestro del CMTS DEBE satisfacer esos límites de prueba en un 99%, o más, de las mediciones.)

B.N.7 Subcapa de convergencia de la transmisión en sentido ascendente

B.N.7.1 Introducción

Para aumentar la solidez de la de modulación, facilitar el que el equipo físico de recepción sea común para vídeo y datos y dejar abierta la posibilidad de una futura multiplexación de vídeo y datos en el tren de bits de la subcapa PMD definida en B.N.6, se interpone una subcapa entre la subcapa PMD en sentido descendente y la subcapa MAC de datos por cable.

El tren de bits en sentido descendente se define como una serie continua de paquetes MPEG [UIT-T H.222.0] de 188 octetos. Dichos paquetes constan de un encabezamiento de 4 octetos seguido de 184 octetos de cabida útil. El encabezamiento identifica la cabida útil como perteneciente al MAC de datos por cable. Otros valores del encabezamiento pueden indicar otras cabidas útiles. La combinación de cabidas útiles MAC y las de otros servicios es opcional y la controla el CMTS.

La figura B.N-11 ilustra la intercalación de octetos MAC de datos por cable (DOC) con otra información digital (vídeo digital en el ejemplo mostrado).

Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = DOC	Cabida útil MAC de DOC
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital
Encabezamiento = vídeo	Cabida útil de vídeo digital

Figura B.N-11/J.112 – Ejemplo de intercalación de paquetes MPEG en sentido ascendente

B.N.7.2 Formato de paquete MPEG

En la figura B.N-12 se muestra el formato de un paquete MPEG que lleva datos EuroDOCSIS. El paquete consta de un encabezamiento MPEG de 4 octetos, un campo de puntero (no presente en todos los paquetes) y la cabida útil EuroDOCSIS.

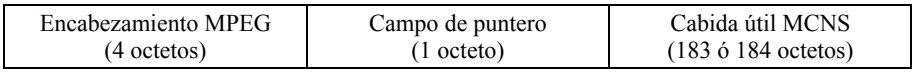


Figura B.N-12/J.112 – Formato de un paquete MPEG

B.N.7.3 Encabezamiento MPEG para datos por cable de MCNS

El formato del encabezamiento del flujo de transporte MPEG se define en 2.4/H.222.0. Los valores de campos particulares que distinguen a los trenes de datos por cable MAC se definen en el cuadro B.N-17. Los nombres de los campos proceden de UIT-T H.222.0.

El encabezamiento MPEG consta de 4 octetos que inician el paquete MPEG de 188-octetos. El formato del encabezamiento a utilizar en un PID de datos por cable de EuroDOCSIS está sometido a las restricciones que se muestran en el cuadro B.N-17. El formato del encabezamiento se atiene a la norma MPEG, pero su utilización está limitada en esta especificación para NO PERMITIR la inclusión de un campo de adaptación en los paquetes MPEG.

Cuadro B.N-17/J.112 – Formato de encabezamiento MPEG para paquetes de datos por cable de EuroDOCSIS

Campo	Longitud (bits)	Descripción
octeto de sincronismo	8	0x47; octeto de sincronismo de paquete MPEG
indicador de error de transporte	1	Indica un error que se ha producido en la recepción del paquete. Este bit es repuesto a cero por el emisor, y puesto a uno cuando quiera que se produzca un error en la transmisión del paquete
indicador de comienzo de unidad de cabida útil	1	Un valor de uno indica la presencia de un campo de puntero como el primer octeto de la cabida útil (quinto octeto del paquete)
prioridad de transporte	1	Reservado; puesto a cero
PID	13	PID conocido de datos por cable de EuroDOCSIS (0x1FFE)
control de aleatorización del transporte	2	Reservado; puesto a "00"
control de campo de adaptación	2	"01", la utilización del campo de adaptación NO ESTÁ PERMITIDA en el PID de EuroDOCSIS
contador de continuidad	4	contador cíclico dentro de este PID

B.N.7.4 Cabida útil MPEG para datos por cable de MCNS

La porción de cabida útil MPEG del paquete MPEG llevará las tramas MAC de EuroDOCSIS. El primer octeto de la cabida útil MPEG será un "campo de puntero" ("pointer_field") si se ha fijado el indicador de comienzo de unidad de cabida útil (payload_unit_start_indicator) (PUSI) del encabezamiento MPEG.

octeto de relleno (stuff_byte)

Este anexo B.N define un esquema de octetos de relleno que tienen un valor (0xFF) utilizado dentro de la cabida útil EuroDOCSIS para llenar cualquier intervalo entre tramas MAC de EuroDOCSIS. El valor se elige como valor no utilizado para el primer octeto de la trama MAC de EuroDOCSIS. El octeto "FC" del encabezamiento MAC se definirá de modo que nunca contenga ese valor. (FC_TYPE = "11" indica una trama específica del MAC, y FC_PARM = "11111" no se utiliza actualmente y, de acuerdo con esta especificación, se define como un valor ilegal para FC_PARM.)

campo de puntero (pointer_field)

El campo de puntero está presente como quinto octeto del paquete MPEG (quinto octeto tras el encabezamiento MPEG) cuando en el encabezamiento MPEG se ha fijado el PUSI a uno. La interpretación del campo de puntero es como sigue:

El campo de puntero contiene el número de octetos de este paquete que siguen inmediatamente a dicho campo que el decodificador del CM debe saltarse antes de buscar el comienzo de una trama MAC de EuroDOCSIS. Un campo de puntero CM DEBE estar presente si es posible para empezar una trama MAC de EuroDOCSIS de datos por cable en el paquete, y DEBE apuntar:

1) al comienzo de la primera trama MAC para empezar en el paquete; o
2) a cualquier octeto de relleno que preceda a la trama MAC.

B.N.7.5 Interacción con la subcapa MAC

Las tramas MAC pueden empezar en cualquier punto dentro de un paquete MPEG y pueden abarcar varios paquetes MPEG y, dentro de un paquete MPEG, pueden existir varias tramas MAC.

Las figuras que siguen muestran el formato de los paquetes MPEG que llevan tramas MAC de EuroDOCSIS. En todos los casos, la bandera PUSI indica la presencia del campo de puntero como primer octeto de la cabida útil MPEG.

La figura B.N-13 muestra una trama MAC situada inmediatamente después del octeto pointer_field. En este caso, el campo de puntero es 0 y el decodificador EuroDOCSIS empezará la búsqueda de un octeto FC válido en el octeto que sigue inmediatamente al campo de puntero.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= 0)	Trama MAC (hasta 183 octetos)	octeto(s) de relleno (0 o más)

Figura B.N-13/J.112 – Formato de paquete cuando una trama MAC sigue inmediatamente al campo de puntero

La figura B.N-14 muestra el caso más general en el que una trama MAC va precedida por la cola de una trama MAC anterior y una secuencia de octetos de relleno. En este caso, el campo de puntero identifica todavía al primer octeto después de la cola de la trama #1 octeto de relleno (un stuff_octeto) como la posición en la que el decodificador debería empezar la búsqueda de un valor FC de subcapa MAC legal. Este formato permite la operación de multiplexación en el CMTS para insertar inmediatamente una trama MAC que esté disponible para transmisión si dicha trama llega después de que se hayan transmitido el encabezamiento y el campo de puntero MPEG.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= M)	Cola de la trama MAC #1 (M octetos)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #2

Figura B.N-14/J.112 – Formato de paquete con trama MAC precedida por octetos de relleno

Para facilitar la multiplexación del tren de paquetes MPEG que lleva datos EuroDOCSIS con otros datos con codificación MPEG, el CMTS NO DEBERÍA transmitir paquetes MPEG con el PID de EuroDOCSIS que contienen solamente octetos de relleno en la zona de cabida útil. En su lugar, DEBERÍAN transmitirse paquetes nulos MPEG. Se señala que existen relaciones de temporización implícitas en la subcapa MAC de EuroDOCSIS que también deben ser preservadas por cualquier operación de multiplexación MPEG.

La figura B.N-15 muestra que dentro del paquete MPEG pueden estar contenidas múltiples tramas MAC. Las tramas MAC pueden estar concatenadas una tras otra o separadas por una secuencia opcional de octetos de relleno.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= 0)	Trama MAC #1	Trama MAC #2	octeto(s) de relleno (0 o más)	Trama MAC #3

Figura B.N-15/J.112 – Formato de paquete mostrando múltiples tramas MAC en un solo paquete

La figura B.N-16 muestra el caso en el que una trama MAC abarca múltiples paquetes MPEG. En este caso, el pointer_field de la trama subsiguiente apunta al octeto que sigue al último octeto de la cola de la primera trama.

Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= 0)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #1 (hasta 183 octetos)	
Encabezamiento MPEG (PUSI = 0)	Continuación de la trama MAC #1 (184 octetos)			
Encabezamiento MPEG (PUSI = 1)	Campo de puntero (= M)	Cola de la trama MAC #1 (M octetos)	octeto(s) de relleno (0 o más)	Comienzo de la trama MAC #2 (M octetos)

Figura B.N-16/J.112 – Formato de paquete cuando una trama MAC abarca múltiples paquetes

La subcapa de convergencia de transmisión debe funcionar en estrecha relación con la subcapa MAC para proporcionar una indicación de tiempo precisa que se ha de insertar en el mensaje de sincronización de tiempo (véanse B.8.3.2 y B.9.3).

B.N.7.6 Interacción con la capa física

El tren de paquetes MPEG-2 DEBE ser codificado de acuerdo con [EN 300 429].

B.N.7.7 Sincronización y recuperación de encabezamiento MPEG

El tren de paquetes MPEG-2 DEBERÍA ser declarado "dentro de trama" (es decir, que se ha conseguido la alineación correcta de los paquetes) cuando se hayan recibido cinco sumas de comprobación de paridad correctas consecutivas, cada una de ellas a 188 octetos de la anterior.

El tren de paquetes MPEG-2 DEBERÍA ser declarado "fuera de trama", y debería iniciarse una búsqueda de alineación correcta de los paquetes, cuando se hayan recibido nueve sumas de comprobación de paridad incorrectas consecutivas.

En B.8 se describe en detalle el formato de las tramas MAC.

ANEXO B.O[1]

Protección para la implementación de J.112, anexo B

B.O.1 Alcance

El presente anexo informativo contiene los servicios de privacidad de capa MAC (control de acceso a los medios) para comunicaciones CMTS-CM (sistema de terminación de módem de cable-módem de cable). Este anexo B.O (al que a menudo se hace referencia como interfaz de privacidad básica plus o BPI+) tiene los dos objetivos siguientes:

- proporcionar a los usuarios de módem de cable privacidad de datos en toda la red de cable, y
- proporcionar a los operadores de cable protección de los servicios, es decir, impedir que usuarios no autorizados accedan a los servicios MAC de RF (radiofrecuencia).

BPI+ permite un nivel de privacidad de los datos en toda la red por cable de medio compartido igual o mejor que el que proporcionan los servicios de acceso a red por línea especializada (módems analógicos o líneas de abonado digitales).

B.O.2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

Normativas

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

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

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

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

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

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

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

RFC 2459 IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile.*

[RSA 1] RSA Laboratories PKCS #1 (1993), *PKCS #1: RSA Encryption Standard,* Version 1.5.

---

[1] El anexo O "*Protección para implementación de J.112, anexo B*", que era informativo cuando el anexo B de la Rec. J.112 fue aprobado en marzo de 2001, ha sido modificado en normativo por la enmienda 1 (02/2002) de anexo B de la Rec. UIT-T J.112.

[RSA 2] RSA Laboratories, PKCS #1 (1999), *PKCS #1: RSA Cryptography Standard*, Version 2.0.

[UIT X.509] Recomendación UIT-T X.509 (1997), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco para certificados de cones públicos y de atributos*.

NOTA – La referencia a un documento en este anexo B.O no le da, en tanto que documento autónomo, categoría de Recomendación.

Informativas

[RFC 1750] IETF RFC 1750 (1994), Randomness Recommendations for Security.

[RFC 2202] IETF RFC 2202 (1997), Test cases for HMAC-MD5 and HMAC-SHA-1.

B.O.3 Convenios

A lo largo del presente anexo B.O, las palabras utilizadas para señalar la importancia de requisitos particulares se escriben con letras mayúsculas. Dichas palabras son:

"DEBE(N)" Esta palabra, o el adjetivo "REQUERIDO", significa que el elemento es un requisito absoluto de este anexo B.O.

"NO DEBE(N)" Esta expresión significa que el elemento es una prohibición absoluta de este anexo B.O.

"DEBERÍA(N)" Esta palabra, o el adjetivo "RECOMENDADO", significa que, en determinadas circunstancias pueden existir motivos válidos para hacer caso omiso de este elemento, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de optar por una vía diferente.

"NO DEBERÍA(N)" Esta expresión significa que pueden existir motivos válidos en determinadas circunstancias en las que el comportamiento indicado sea aceptable o incluso de utilidad, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de implementar cualquier comportamiento descrito con esta etiqueta.

"PUEDE(N)" Esta palabra, o el adjetivo "OPCIONAL", significa que el elemento es verdaderamente opcional. Un vendedor puede optar por incluir el elemento porque así se exige en un determinado mercado o porque mejora el producto, por ejemplo; otro vendedor puede omitir el mismo elemento.

B.O.4 Abreviaturas

En este anexo B.O se utilizan las siguientes siglas.

BPI+ Interfaz de privacidad básica plus (*baseline privacy interface plus*)

BPKM Gestión de claves de privacidad básica (*baseline privacy key management*)

CBC Encadenamiento de bloques cifrados (*cipher block chaining*)

CM Módem de cable (*cable modem*)

CMTS Sistema de terminación de módem de cable (*cable modem termination system*)

CRC Verificación por redundancia cíclica (*cyclic redundancy check*)

DES Norma de criptación de datos de los Estados Unidos (*US data encryption standard*)

HMAC Troceo con aplicación de clave para autenticación de mensaje (*keyed-hashing for message authentication*)

QoS Calidad de servicio (*quality of service*)

RSA Laboratorios RSA (*RSA laboratories*)

SA Asociación de seguridad (*security association*)

SAID Identificador de asociación de seguridad (*security association identifier*)

SID Identificador de servicio (*service identifier*)

TEK Clave de criptación de tráfico (*traffic encryption key*)

B.O.5 Antecedentes y visión de conjunto

A los operadores de cable les interesa instalar sistemas de comunicaciones por paquetes de alta velocidad en las redes de televisión por cable que permitan proporcionar una amplia variedad de servicios. Entre los servicios objeto de atención por parte de los operadores de cable figura el acceso a Internet a alta velocidad, el servicio de telefonía por paquetes, el servicio de videoconferencia, el servicio equivalente al de retransmisión de tramas, y muchos otros servicios.

El servicio cuya prestación se pretende permitirá la transferencia bidireccional transparente de tráfico de protocolo Internet (IP), entre la cabecera del sistema de cable y las posiciones de los clientes, por una red de televisión por cable totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC). Esto es lo que se muestra de forma simplificada en la figura B.O-1.

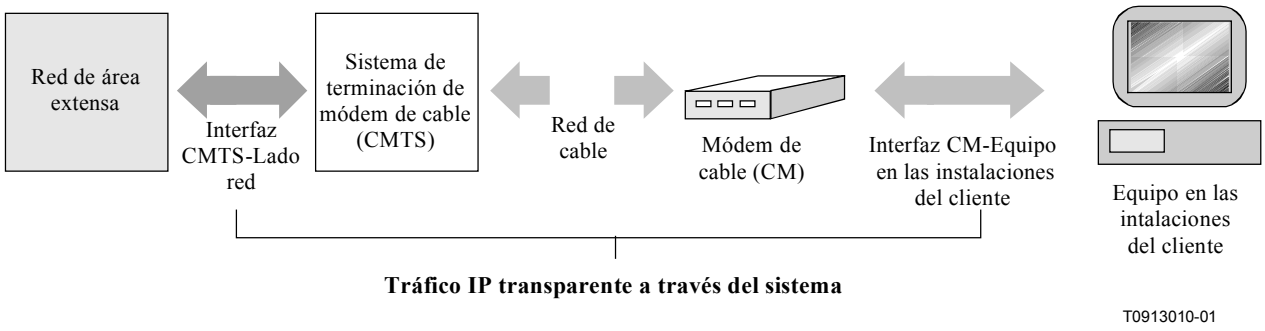


Figura B.O-1/J.112 – Tráfico IP transparente a través del sistema de datos por cable

El trayecto de transmisión por el sistema de cable se materializa en un CMTS en la cabecera, y en un CM en la posición de cada cliente. En la cabecera (o centro de distribución), la interfaz con el sistema de datos por cable se denomina interfaz sistema de terminación de módem de cable-lado red (CMTS-NSI). En las posiciones de los clientes, la interfaz se llama interfaz módem de cable-equipo en las instalaciones del cliente (CMCI). Lo que se pretende es que los operadores de cable transfieran de manera transparente tráfico IP entre esas interfaces incluyendo, pero sin limitarse a ello, diagramas DHCP, y direccionamiento de grupo IP (radiodifusión y multidifusión).

La interfaz de privacidad básica plus (BPI+) proporciona a los usuarios de módem de cable privacidad de datos en la red de cable. Lo hace criptando los flujos de tráfico entre CM y CMTS.

Además, BPI+ proporciona a los operadores de cable un alto grado de protección frente a quienes piratean el servicio. Los servicios de comunicaciones de datos MAC protegidos se dividen en tres categorías:

- servicios de datos IP del mejor esfuerzo y alta velocidad;
- servicios de datos con QoS (por ejemplo, velocidad binaria constante); y
- servicios de grupo de multidifusión IP.

Con BPI+, el CMTS protege contra los accesos no autorizados a esos servicios de transporte de datos implantando la criptación de los flujos de tráfico asociados a través de la red de cable. BPI+ emplea

un protocolo de gestión de clave de cliente/servidor autenticada en el que el CMTS, el servidor, controla la distribución del material de aplicación de claves a los CM clientes.

B.O.5.1 Visión general de la arquitectura

La privacidad básica plus tiene dos protocolos componentes:

- Un protocolo de encapsulación para la criptación de datos por paquetes a través de la red de cable. Dicho protocolo define:
  1) el formato de trama para el transporte de datos por paquetes encriptados dentro de las tramas MAC,
  2) un conjunto de series criptográficas soportadas, es decir, emparejamientos de algoritmos de criptación y autenticación de datos, y
  3) las reglas para la aplicación de esos algoritmos a los datos por paquetes de una trama MAC.
- Un protocolo de gestión de claves (gestión de claves de privacidad básica, o "BPKM") que permite la distribución segura de datos de aplicación de claves del CMTS a los CM: Mediante dicho protocolo de gestión de claves, el CM y el CMTS sincronizan los datos de aplicación de claves; además, el CMTS utiliza el protocolo para forzar el acceso condicional a los servicios de la red.

B.O.5.1.1 Criptación de datos por paquetes

Los servicios de criptación de BPI+ se definen como un conjunto de servicios ampliados dentro de la subcapa MAC. La información de encabezamiento de paquete específica de BPI+ se sitúa en el elemento encabezamiento ampliado de privacidad básica dentro del encabezamiento ampliado MAC.

En el momento en que se publica este anexo B.O, BPI+ soporta un solo algoritmo de criptación de datos por paquetes: el modo encadenamiento de bloques cifrados (CBC, *cipher block chaining*) del algoritmo norma de criptación de datos de Estados Unidos (DES, *US data encryption standard*) [FIPS 46-1] [FIPS 81]. BPI+ no empareja el CBC de DES con ningún algoritmo de autenticación de datos por paquetes. Algoritmos de criptación de datos adicionales pueden ser soportados en perfeccionamientos futuros de la especificación del protocolo BPI+, y esos algoritmos podrán ser emparejados con algoritmos de autenticación de datos.

BPI+ cripta los datos por paquetes de una trama MAC; el encabezamiento de la trama MAC no se cripta. Se DEBEN enviar mensajes de gestión MAC en claro para facilitar el registro, la alineación y el funcionamiento normal de la subcapa MAC[2].

La cláusula B.O.6 especifica el formato de las tramas MAC que llevan cabidas útiles de datos por paquetes criptados.

B.O.5.1.2 Protocolo de gestión de claves

Los CM utilizan el protocolo de gestión de claves de privacidad básica para obtener la autorización y el material de aplicación de claves de tráfico del CMTS, y soportar reautorizaciones y renovaciones periódicas de claves. El protocolo de gestión de claves utiliza certificados digitales X.509 [UIT-T X.509], RSA [RSA1, RSA2] (un algoritmo de criptación de claves públicas) y DES triple de dos claves para que los intercambios de claves entre CM y CMTS se produzcan de manera segura.

El protocolo de gestión de claves de privacidad básica se atiene al modo cliente/servidor, en el que el CM, un "cliente" BPKM, pide material de aplicación de claves, y el CMTS, un "servidor" BPKM, responde a esas peticiones, garantizándose que los CM clientes individuales sólo reciben el material

---

[2] Los encabezamientos MAC de las PDU de datos por paquetes y los mensajes de gestión MAC ajenos a BPI+ PUEDEN ser criptados cuando formen parte de un paquete concatenado fragmentado.

de aplicación de claves para el que están autorizados. El protocolo BPKM sólo utiliza mensajería de gestión MAC.

BPI+ utiliza criptografía de claves públicas para establecer un secreto compartido (es decir, una clave de autorización) entre CM y CMTS. El secreto compartido se emplea a continuación para asegurar los intercambios de claves de criptación de tráfico del protocolo BPKM subsiguientes. Este mecanismo de distribución de claves en dos etapas permite la renovación de claves de criptación de tráfico sin incurrir en laboriosas operaciones de complejo cálculo de claves públicas.

Un CMTS autentica un CM cliente durante el intercambio de autorización inicial. Cada CM lleva un certificado digital X.509 único expedido por el fabricante del CM. El certificado digital contiene la clave pública del CM junto con otra información de identificación, a saber, la dirección MAC del CM, el identificador ID del fabricante y el número de serie. Cuando se solicita una clave de autorización, el CM presenta su certificado digital a un CMTS. El CMTS verifica el certificado digital, y a continuación utiliza la clave pública verificada para criptar una clave de autorización, que envía seguidamente al CM solicitante.

El CMTS asocia la identidad autenticada de un módem de clave a un abonado de pago, y en consecuencia a los servicios de datos a los que el abonado está autorizado a acceder. Así pues, con el intercambio de clave de autorización, el CMTS establece la identidad autenticada de un CM cliente, y los servicios (es decir, las claves de criptación de tráfico específicas) a los que el CM está autorizado a acceder.

Puesto que el CMTS autentica los CM, puede proteger contra cualquier atacante que emplee un módem "clonado" (falsificado), fingiendo ser un módem de abonado legítimo. La utilización de los certificados X.509 impide que los módems clonados pasen credenciales falsas a un CMTS.

Los CM DEBEN tener pares de claves privada/pública RSA instaladas en fábrica o proporcionar un algoritmo interno para generar esos pares de claves de forma dinámica. Si un CM depende de un algoritmo interno para generar su par de claves RSA, DEBE generarlo antes de que se produzca su primera inicialización de privacidad básica, descrita en B.O.5.2.1. Los CM con pares de claves RSA instaladas en fábrica DEBEN tener también certificados X.509 instalados en fábrica. Los módems de cable que dependen de un algoritmo interno para generar un par de claves RSA DEBEN soportar un mecanismo de instalación del certificado X.509 expedido por el fabricante tras la generación de las claves.

En B.O.7 se define de forma detallada el protocolo BPKM.

B.O.5.1.3 Asociaciones de seguridad de BPI+

Una *asociación de seguridad* (SA, *security association*) de BPI+ es el conjunto de información de seguridad que comparten un CMTS y uno o más de sus CM clientes para hacer posible unas comunicaciones seguras a través de la red de cable. BPI+ define tres tipos de asociaciones de seguridad: *primario, estático* y *dinámico*. Una asociación de seguridad primaria está vinculada únicamente a un solo CM, y se establece cuando el CM completa el registro MAC. Las asociaciones de seguridad estáticas se aprovisionan dentro del CMTS. Las asociaciones de seguridad dinámicas se establecen y eliminan, sobre la marcha, en respuesta a la iniciación y terminación de flujos de tráfico (en sentido descendente) específicos. Tanto las SA estáticas como las dinámicas pueden ser compartidas por múltiples CM.

La información compartida de asociación de seguridad incluye las claves de criptación de tráfico y los vectores de inicialización del CBC. Para soportar, en perfeccionamientos futuros de BPI+, algoritmos alternativos de criptación y datos y autenticación de datos, los parámetros de asociación de seguridad de BPI+ incluyen un identificador de serie criptográfica que indica un emparejamiento particular de algoritmos de criptación de datos por paquetes y autenticación de datos por paquetes empleados por la asociación de seguridad. Al publicarse este anexo B.O, los únicos algoritmos de

criptación de datos por paquetes eran DES de 56 bits y DES de 40 bits, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos por paquetes[3].

BPI+ identifica las asociaciones de seguridad con un *identificador de asociación de seguridad (SAID)* de 14 bits.

Cada CM (BPI+ habilitada) establece una asociación de seguridad primaria con su CMTS. Todo el tráfico en sentido ascendente de un CM DEBE ser criptado en el marco de la asociación de seguridad primaria exclusiva del CM. El SAID correspondiente a la SA primaria de un CM DEBE ser igual al identificador de servicio (SID) primario del CM. Por otro lado, aunque normalmente el tráfico de unidifusión en sentido descendente dirigido al o a los dispositivos CPE, que se hallan detrás de un CM, son criptados de acuerdo con la asociación de seguridad primaria exclusiva del CM, flujos de tráfico de unidifusión en sentido descendente seleccionados pueden ser criptados de acuerdo con las SA estáticas o dinámicas. Es decir, tráfico en sentido descendente PUEDE ser criptado de conformidad con cualquiera de los tres tipos de SA. No obstante, un paquete de datos de multidifusión IP en sentido descendente está destinado por lo general a múltiples CM y, por tanto, lo más probable es que se cripte de conformidad con SA estáticas o dinámicas, a las que pueden acceder múltiples CM, al contrario que una SA primaria, que se circunscribe a un único CM.

Utilizando el protocolo BPKM, un CM pide a su CMTS el material de aplicación de claves de una SA. El CMTS garantiza que cada CM cliente sólo tenga acceso a las asociaciones de seguridad a las que está autorizado a acceder.

El material de aplicación de claves de una SA (por ejemplo, la clave DES y el vector de inicialización del CBC) tiene un tiempo de vida limitado. Cuando el CMTS entrega material de aplicación de claves de SA a un CM, le proporciona también el tiempo de vida restante de ese material. Corresponde al CM pedir material de aplicación de claves nuevo al CMTS antes de que expire en el CMTS el tiempo de vida del material de que dispone a la sazón el CM. El protocolo BKPM especifica cómo mantienen el CM y el CMTS la sincronización de la clave.

B.O.5.1.4 Identificadores de servicio (SID) de QoS e identificadores de asociación de seguridad (SAID) de BPI+

El elemento encabezamiento ampliado de BPI+ en tramas MAC en sentido descendente contiene el identificador de la asociación de seguridad (SAID) de BPI+ de acuerdo con el cual se cripta la trama en sentido descendente. Si la trama en sentido descendente es un paquete de unidifusión dirigido a un dispositivo CPE situado detrás de un determinado CM, será criptada normalmente de acuerdo con la SA primaria del CM, siendo entonces el SAID igual al SID primario del CM objetivo. Si la trama en sentido descendente es un paquete de multidifusión que se pretende que reciban múltiples CM, el elemento encabezamiento ampliado contendrá el SAID estático o dinámico del que se ha establecido la correspondencia con ese grupo de multidifusión. El SAID (primario, estático o dinámico), junto con otros campos de datos del elemento encabezamiento ampliado en sentido descendente, identifica a un módem receptor el conjunto particular de material de aplicación de claves que se requiere para descriptar el campo datos por paquetes encriptados de la trama MAC.

Puesto que todo el tráfico en sentido ascendente de un CM se cripta de conformidad con su SA primaria exclusiva, las tramas MAC en sentido ascendente, al contrario que las tramas MAC en sentido descendente, no necesitan llevar un SAID de BPI+ en sus encabezamientos ampliados; en cambio, el elemento EH de privacidad básica contiene el SID de QoS que identifica el flujo de servicio en sentido ascendente activo por el que se transporta la trama MAC.

---

[3] BPI+ cripta la CRC Ethernet/802.3 de una PDU paquete. Si bien esto equivale a un cierto grado de autenticación de datos, no representa una autenticación de datos segura desde el punto de vista criptográfico.

El elemento encabezamiento ampliado de privacidad básica sirve para múltiples fines en las tramas MAC de una PDU datos por paquetes en sentido ascendente. Además de identificar el material de aplicación de claves que, en concreto, se ha utilizado para criptar los datos por paquetes de una trama, proporciona un mecanismo para la emisión de peticiones de anchura de banda porteadas, y puede llevar datos de control de fragmentación. Estas dos últimas funciones están vinculadas a un SID de QoS particular y, por este motivo, los elementos encabezamiento ampliado de privacidad básica en sentido ascendente contienen un SID de QoS en vez de un SAID primario de BPI+, que se puede deducir del SID de QoS.

B.O.5.2 Visión de conjunto operativa

B.O.5.2.1 Inicialización de módem de cable

La Recomendación J.112 anexo B divide la inicialización del módem de cable en las fases siguientes:

- exploración del canal en sentido descendente y establecimiento de la sincronización con el CMTS;
- obtención de los parámetros de transmisión;
- realización de la alineación;
- establecimiento de la conectividad IP (DHCP);
- establecimiento de la hora del día;
- transferencia de los parámetros operativos (telecarga de ficheros de parámetros vía TFTP);
- registro en el CMTS.

El establecimiento de la privacidad básica sigue al registro en el CMTS.

Si un CM está en condiciones de aplicar privacidad básica, su fichero de parámetros, telecargado durante la transferencia de parámetros operativos, DEBE incluir fijaciones de configuración privacidad básica. En el anexo B.O.A se definen esas fijaciones de configuración adicionales.

Una vez completado el registro del CM, el CMTS asigna uno o más ID de servicio (SID) estático al CM que se registra en concordancia con el aprovisionamiento de clase de servicio estática del CM. El primer SID estático asignado durante el proceso de registro es el SID primario, y este SID servirá también como SAID primario de BPI+ del CM. Si un CM está configurado de modo que aplique privacidad básica, el registro en el CMTS va seguido inmediatamente por la inicialización de las funciones de seguridad de privacidad básica del CM.

La inicialización de la privacidad básica empieza con el envío por el CM al CMTS de una petición de autorización, conteniendo:

- datos que identifiquen el CM (por ejemplo, la dirección MAC);
- la clave pública RSA del CM;
- un certificado X.509 que demuestre la vinculación entre los datos que identifican el CM y la clave pública del CM;
- una lista de las capacidades de seguridad del CM (es decir, los emparejamientos particulares de algoritmos de criptación y autenticación que soporta el CM) y
- el SAID primario del CM (es decir, el SID primario).

Si el CMTS determina que el CM solicitante está autorizado para el SAID primario de la petición de autorización, contesta con una respuesta de autorización que contiene una clave de autorización, a partir de la cual el CM y el CMTS obtienen las claves necesarias para asegurar las peticiones subsiguientes de un CM de claves de criptación de tráfico y las respuestas del CMTS a esas peticiones. El CMTS cripta la clave de autorización con la clave pública del módem de cable receptor.

La respuesta de autorización contiene también una lista de descriptores de asociación de seguridad, que identifican las SA primaria y estáticas a las que el CM solicitante está autorizado a acceder. Cada descriptor de SA consta de un conjunto de parámetros de SA, incluidos el SAID, el tipo y la serie criptográfica. La lista contiene por lo menos una entrada: un descriptor que describe la asociación de seguridad primaria del CM. Otras entradas son opcionales, y describirían cualesquiera SA estáticas a las que el CM pudiera acceder.

Tras completar de manera satisfactoria la autenticación y obtener la autorización del CMTS, el módem de cable envía peticiones de clave al CMTS, solicitando claves de criptación de tráfico a utilizar con cada uno de sus SAID. Las peticiones de clave de tráfico de un CM se autentican aplicando un troceo con clave (el algoritmo HMAC [RFC 2104]); la clave de autenticación de mensajes se deduce de la clave de autorización obtenida durante el intercambio de autorización previo. El CMTS contesta con respuestas de clave, que contienen las claves de criptación de tráfico (TEK, *traffic encryption keys*); las TEK son DES triples criptadas con una clave de criptación de claves obtenida a partir de la clave de autorización. Al igual que las peticiones de clave, las respuestas de clave son autenticadas aplicando un troceo con clave, en el que la clave de autenticación de mensajes se deriva de la clave de autorización.

B.O.5.2.2 Mecanismo de actualización de clave de módem de cable

Las claves de criptación de tráfico que el CMTS proporciona a los CM clientes tienen un tiempo de vida limitado. El CMTS entrega el tiempo de vida restante de la clave, junto con el valor de la clave, en las respuestas de clave que envía a sus CM clientes. El CMTS controla cuáles son las claves vigentes eliminando las claves cuyo tiempo de vida haya expirado y generando nuevas claves. Corresponde a cada uno de los módems de cable asegurarse de que las claves que está utilizando concuerdan con las que utiliza el CMTS. Para ello, rastrean el momento en que está previsto que prescriba la clave de un determinado SAID y emiten una petición de clave nueva, la de la clave más reciente, antes de que se produzca esa prescripción.

Además, es preciso que los módems de cable renueven periódicamente la autorización del CMTS; como ocurre con las claves de criptación de tráfico, una clave de autorización tiene un tiempo de vida finito que el CMTS entrega al CM junto con el valor de la clave. Corresponde a cada módem de cable obtener una nueva autorización y una clave de autorización renovada (así como una lista actualizada de descriptores de SA) antes de que el CMTS haga que prescriba la clave de autorización vigente del CM.

La inicialización de la privacidad básica y la actualización de claves están implementadas dentro del protocolo de gestión de claves de privacidad básica, definido con detalle en B.O.7.

B.O.6 Formato de trama MAC

Cuando se funciona con BPI+ habilitada, el CM y el CMTS criptan las regiones PDU datos de las tramas MAC particulares que transmiten por la red de cable. La criptación de BPI+ se aplica a dos tipos específicos de tramas MAC:

- Tramas MAC de PDU datos por paquetes de longitud variable;
- Tramas MAC de fragmentación.

En cada uno de los dos casos, un elemento encabezamiento ampliado de privacidad básica del encabezamiento MAC identifica la asociación de seguridad y el material de aplicación de claves acompañante utilizado para criptar la PDU datos.

B.O.6.1 Formato de trama MAC de PDU datos por paquetes de longitud variable

La figura B.O.6-1 muestra el formato de una PDU datos por paquetes de longitud variable con un elemento encabezamiento ampliado (EH) de privacidad y cabida útil de PDU paquete criptada.

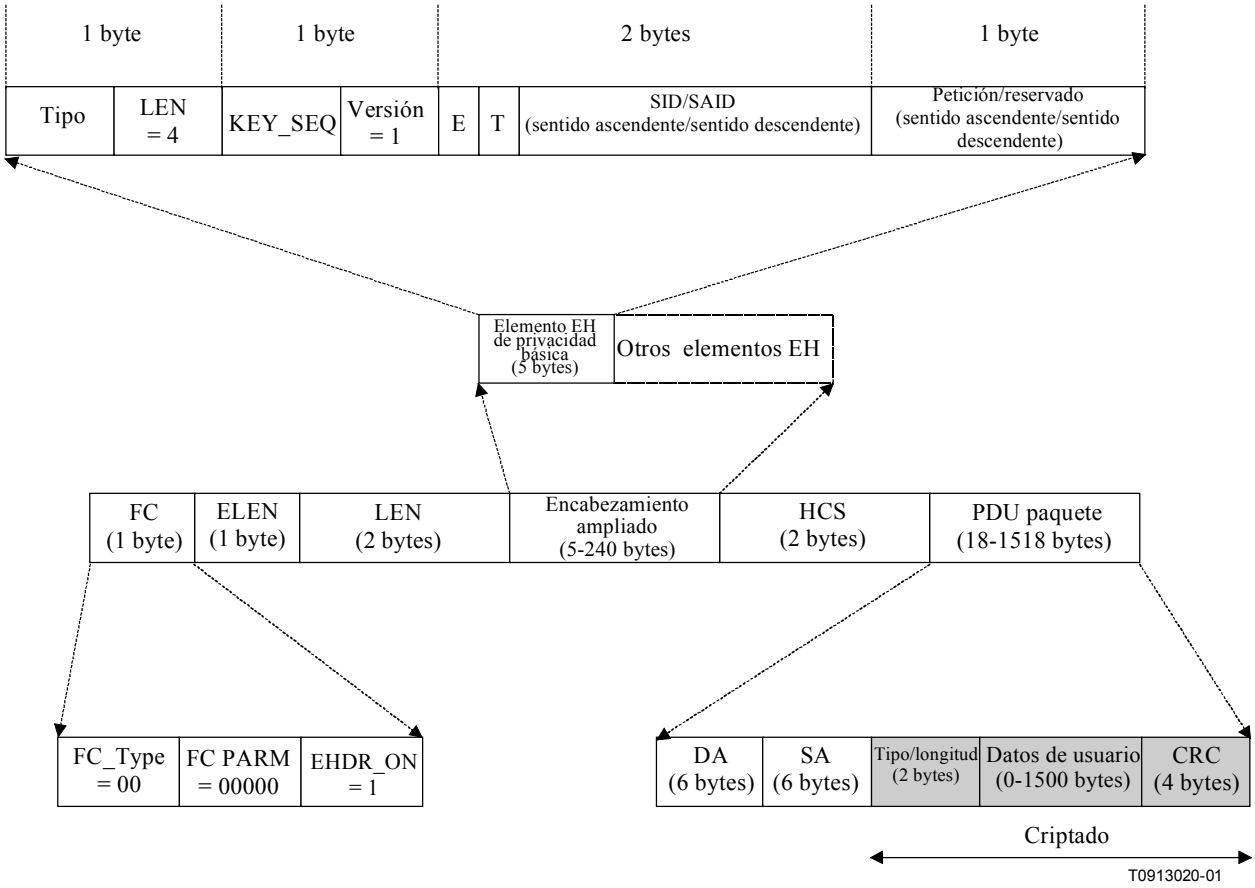


Figura B.O.6-1/J.112 – Formato de PDU datos por paquetes de longitud variable con elemento EH de privacidad

Los 12 primeros octetos de la PDU paquete, que contienen las direcciones de destino y origen (DA/SA, *destination address/source address*) Ethernet/802.3, no son criptados. La transmisión de las direcciones de origen y destino de una trama en claro da a los vendedores un mayor grado de flexibilidad a la hora de integrar la criptación/descriptación con la funcionalidad MAC; por ejemplo, los vendedores pueden optar libremente entre filtrado de DA/SA o de SID primero. La CRC Ethernet/802.3 de la PDU paquete es criptada.

El CMTS incluye el elemento EH de privacidad básica en todas las PDU datos por paquetes en sentido descendente que cripta en el marco de la privacidad básica plus. De manera similar, un CM incluye el elemento EH de privacidad básica en todas las PDU datos por paquetes en sentido descendente que cripta en el marco de la privacidad básica plus. Si en el encabezamiento MAC están presentes múltiples elementos encabezamiento ampliado, el elemento encabezamiento ampliado de privacidad básica DEBE ser el primero.

El elemento encabezamiento ampliado de privacidad emplea dos valores de tipo de elemento EH, BPI_UP y BPI_DOWN, a utilizar con las PDU datos por paquetes en sentido ascendente y en sentido descendente, respectivamente. La Recomendación J.112 anexo B define los valores de tipos de elemento EH específicos asignados a BPI_UP y BPI_DOWN.

Los 4 bits de orden superior del campo valor de un elemento encabezamiento ampliado de BPI+ contienen un número de secuencia de clave, KEY_SEQ. Se recuerda que el material de aplicación de claves asociado con un SAID de BPI+ tiene un tiempo de vida útil limitado, y que el CMTS renueva periódicamente el material de aplicación de claves de un SAID. El CMTS gestiona un número de secuencia de clave de 4 bits independientemente para de cada SAID y distribuye dicho número de secuencia de clave junto con el material de aplicación de claves del SAID entre los CM clientes. El

CMTS incrementa el número de secuencia de clave con cada nueva generación de material de aplicación de claves. El elemento EH de privacidad incluye este número de secuencia, junto con el SAID, para identificar la generación específica del material de aplicación de claves de ese SAID que está siendo utilizado para encriptar la PDU datos por paquetes adjunta. Puesto que se trata de una cantidad expresada con 4 bits, el número de secuencia retorna a 0 cuando llega a 15.

Comparando el número de secuencia de clave de una trama recibida con lo que se piensa que es el número de secuencia de clave "actual", un CM o un CMTS puede reconocer fácilmente una pérdida de sincronización de clave con su elemento par. Un CM DEBE mantener las dos generaciones más recientes de material de aplicación de claves para cada SAID de BPI+. Es preciso tener a mano esas dos generaciones más recientes para que el servicio permanezca ininterrumpido durante la transición de clave de un SAID.

Los 4 bits que siguen a KEY_SEQ contienen un número de versión de protocolo. Dicho número se fija a 1 en los encabezamientos MAC de PDU datos por paquetes de longitud variable.

Los dos bytes siguientes contienen los 2 bits de situación de encriptación y el SID/SAID de 14 bits (SID para tramas en sentido ascendente, SAID para tramas en sentido descendente). El bit de situación de criptación HABILITAR indica si la encriptación está habilitada o inhabilitada para esa PDU. Si el bit HABILITAR es 0, la PDU datos por paquetes no está encriptada y el elemento EH de privacidad básica DEBE ser ignorado (salvo en el caso de la petición de anchura de banda básica porteada opcional, véase más adelante). El bit BASCULAR DEBE concordar con el estado del bit menos significativo (LSB) de KEY_SEQ, el número de secuencia de clave.

El protocolo MAC define un elemento EH de petición para el porteo de una petición de anchura de banda en una transmisión de datos. La privacidad básica define un mecanismo adicional para el porteo de peticiones de anchura de banda: el último byte del elemento EH en sentido ascendente de privacidad básica (elemento EH tipo BPI_UP) lleva una petición de atribución de anchura de banda porteada opcional. Si hay una petición porteada, el bit representa el número de mini-intervalos solicitados. El SID de 14 bits dentro del elemento EH de privacidad básica en sentido ascendente identifica el ID de servicio al que se aplica la petición de anchura de banda. Si no hay petición porteada dentro del elemento EH de privacidad básica, el byte de petición se fija a 0. Una petición porteada dentro del elemento EH de privacidad básica DEBE ser procesada con independencia de la situación del bit HABILITAR.

En los paquetes en sentido descendente (elemento encabezamiento ampliado tipo BPI_DOWN), el cuarto y último byte está reservado y fijado a cero. (Véase el cuadro B.O.6-1.)

Cuadro B.O.6-1/J.112 – Resumen del contenido de los dos elementos EH de privacidad básica

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP	4	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Petición [porteo] (1 byte) [CM → CMTS] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SID definido como: bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada bit[14]: BASCULAR: 1..Clave impar; 0..Clave par bits[13:0]: ID de servicio. El campo petición contiene el número de miniintervalos solicitados para anchura de banda en sentido ascendente.
BPI__DOWN	4	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Reservado (1 byte) [CMTS → CM] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SAID definido como: bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada bit[14]: BASCULAR: 1..Clave impar; 0..Clave par bits[13:0]: ID de asociación de seguridad. Campo reservado fijado a 0.

En el caso de PDU datos por paquetes criptadas transmitidas en un intervalo de contienda de datos en sentido ascendente, el SID del elemento EH de privacidad básica DEBE identificar el SID de QoS; NO DEBE fijarse al ID de servicio de multidifusión del intervalo de contienda petición/datos.

B.O.6.2 Formato de trama MAC de fragmentación

Para soportar la fragmentación de tramas MAC en sentido ascendente, la Recomendación J.112 Anexo B v2 ha reconstruido el elemento EH de privacidad básica de modo que lleve campos control de criptación y control de fragmentación. Cuando desempeña este doble cometido, el elemento EH de privacidad básica (elemento EH tipo BPI_UP) se amplía en un byte, sirviendo el byte final como campo de control de la fragmentación. La figura B.O.6-2 muestra el formato de una trama MAC de fragmentación con una cabida útil de fragmentación criptada.

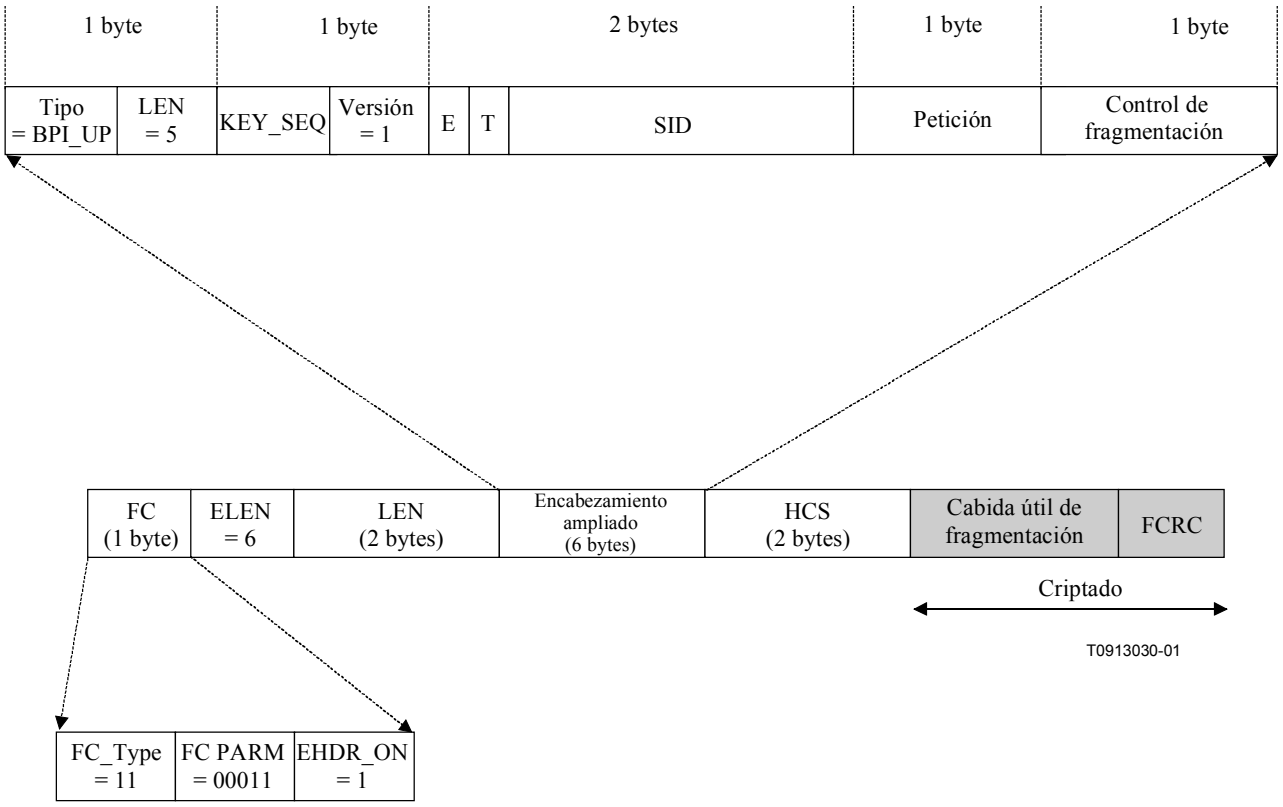


Figura B.O.6-2/J.112 – Formato de una trama MAC de fragmentación con una cabida útil criptada

Un FC_Type = 11 y un FC_PARM = 00011 identifican una trama MAC como trama de fragmentación. A diferencia de las tramas MAC de PDU datos por paquetes, las tramas MAC de fragmentación tienen un encabezamiento ampliado MAC de tamaño fijo (6 bytes) que contiene el elemento EH de privacidad básica "estirado".

El encabezamiento MAC de fragmentación va seguido por una cabida útil de fragmentos y una CRC de fragmentos. Cuando se aplica la criptación de privacidad básica a una trama MAC de fragmentación, se cripta la cabida útil de fragmentos en su totalidad junto con la CRC de fragmento. En otras palabras, al contrario que en la criptación de privacidad básica de las PDU datos por paquetes, no hay un desplazamiento de 12 bytes en la cabida útil antes de empezar la fragmentación[4].

El campo LEN del elemento EH de privacidad básica de las tramas MAC de fragmentación es de 5 bytes en vez de 4, con lo que se tiene en cuenta el campo control de fragmentación adicional de 1 byte. El campo KEY_SEQ, el campo VERSION, las banderas HABILITAR y BASCULAR y el campo SID son tal como serían en una trama MAC de PDU datos por paquetes en sentido ascendente. (Véase el cuadro B.O.6-2.)

[4] En el caso de tramas no fragmentadas, los primeros 12 bytes se dejan en claro para hacer posible un filtrado de DA/SA previo a la descriptación. Si las tramas están fragmentadas, el filtrado de DA/SA no puede tener lugar antes del reensamblado de paquetes; por tanto, no tiene sentido soportar el desplazamiento de la encriptación de 12 bytes en tramas MAC de fragmentación.

Cuadro B.O.6-2/J.112 – Contenido del elemento EH de privacidad básica de una trama MAC de fragmentación

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP	5	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Petición [porteo] (1 byte), Control de fragmentación (1 byte) [CM → CMTS] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SID definido como: Bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada Bit[14]: BASCULAR: 1..Clave impar; 0..Clave par Bit[13:0]: ID de servicio. El campo petición contiene el número de miniintervalos solicitados para anchura de banda en sentido ascendente. El campo control de fragmentación contiene información de control específica de la fragmentación; véase B.10 para más detalles.

El funcionamiento de la fragmentación invalida la BPI+ en el sentido de que el CM debe determinar primero si un paquete será o no fragmentado en base al tamaño de la concesión (el número de mini-intervalo que un CMTS concede a un CM en un MAP de atribución de anchura de banda en sentido ascendente). Si el paquete ha de ser fragmentado, la criptación de BPI+ DEBE producirse fragmento por fragmento, y no en la PDU como un todo; cada fragmento tendrá su propio encabezamiento de fragmentación y será criptado por separado. Si el paquete no ha de ser fragmentado, DEBE ser criptado como una sola unidad, con un encabezamiento de privacidad único.

B.O.6.3 Requisitos para la utilización de un elemento encabezamiento ampliado de privacidad básica en un encabezamiento MAC

Si BPI+ no está habilitada en un determinado flujo de tráfico en sentido descendente (por ejemplo, el tráfico de unidifusión de un CM o un determinado grupo de multidifusión IP), NO DEBERÍA ser utilizado el elemento encabezamiento ampliado de privacidad básica (BP, *baseline privacy*).

Si BPI+ no está habilitada para el tráfico de unidifusión de un CM, las tramas en sentido ascendente fragmentadas DEBEN utilizar aún el elemento encabezamiento ampliado de BP, con el bit HABILITAR criptación desactivado (0). Las peticiones de anchura de banda porteadas de las tramas fragmentadas DEBEN llevarse dentro de este elemento encabezamiento ampliado de BP.

Si BPI+ no está habilitada para el tráfico de unidifusión de un CM, las tramas en sentido ascendente fragmentadas PUEDEN utilizar el elemento encabezamiento ampliado de BP, con el bit HABILITAR criptación desactivado, para llevar peticiones de anchura de banda porteadas. De manera alternativa, las peticiones de anchura de banda porteadas de tramas en sentido ascendente no fragmentadas PUEDEN llevarse en un elemento encabezamiento ampliado PETICIÓN (EH_TYPE=1).

En el caso de tramas MAC que constan sólo de un encabezamiento MAC y EHDR opcional, la privacidad básica DEBE estar inhabilitada. Un EHDR de privacidad básica PUEDE estar presente en esas tramas, pero el bit de habilitación DEBE ser desactivado para inhabilitar la privacidad.

B.O.7 Protocolo de gestión de claves de privacidad básica (BPKM)

B.O.7.1 Modelos de estados

B.O.7.1.1 Introducción

El protocolo BPKM se especifica mediante dos modelos de estados separados pero independientes: un modelo de estados de autorización (la máquina de estados autorización) y un modelo de estados de clave de servicio operativa (la clave de criptación de tráfico, o máquina de estados TEK). En esta cláusula se definen ambos modelos de estados. Los modelos de estados sólo tienen una finalidad explicatoria, y no deben interpretarse en el sentido de que imponen una implementación determinada.

La autorización de un módem de cable, controlada por la máquina de estados autorización, es el proceso por el cual:

- El CMTS autentica la identidad de un CM cliente.
- El CMTS proporciona al CM autenticado una clave de autorización, de la que se deriva una clave de criptación de claves (KEK, *key encryption key*) y claves de autenticación de mensajes.
- El CMTS proporciona al CM autenticado las identidades (es decir, los SAID) y las propiedades de asociaciones de seguridad primarias y estáticas respecto a las que el CM está autorizado a obtener información sobre aplicación de claves.

La KEK es una clave de criptación DES triple de dos claves que utiliza el CMTS para criptar las claves de criptación de tráfico (TEK) que envía al módem. Las claves de criptación de tráfico se utilizan para criptar tráfico de datos de usuario. El CM y el CMTS utilizan claves de autenticación de mensajes para autenticar, vía compendio de mensajes con clave, las peticiones de clave y las respuestas que intercambian.

Tras conseguir la autorización inicial, el módem de cable solicita de manera periódica la reautorización, en el CMTS, reautorización gestionada también por la máquina de estados autorización del CM. Un CM DEBE mantener su situación de autorización en el CMTS para poder renovar las claves de criptación de tráfico que vayan prescribiendo. Las máquinas de estados TEK gestionan la renovación de las claves de criptación de tráfico.

Un módem de cable comienza el proceso de autorización enviando un mensaje información de autenticación a su CMTS. El mensaje información de autenticación contiene el certificado X.509 del fabricante del módem de cable. Se trata de un mensaje estrictamente informativo, es decir, el CMTS puede optar por ignorarlo; sin embargo, representa un mecanismo mediante el cual el CMTS se entera de los certificados de fabricante de sus CM clientes.

El módem de cable envía un mensaje petición de autorización a su CMTS inmediatamente después de enviar el mensaje información de autenticación. Es una petición de clave de autorización, así como de los SAID que identifican cualesquiera asociaciones de seguridad estáticas en las que el CM está autorizado a participar. La petición de autorización incluye:

- el ID del fabricante y el número de serie del módem de cable;
- la dirección MAC del módem de cable;
- la clave pública del módem de cable;
- un certificado X.509 expedido por el fabricante que vincula la clave pública del módem de cable al resto de su información identificadora;

- una descripción de los algoritmos criptográficos que soporta el módem de cable solicitante; las capacidades criptográficas de un CM se presentan al CMTS como una lista de identificadores de series criptográficas, cada una de las cuales indica un determinado emparejamiento de los algoritmos de criptación de datos por paquetes y autenticación de datos por paquetes que admite el CM;
- el SAID primario del módem de cable, que es igual al SID primario del CM. El SID primario es el primer SID estático que el CMTS asigna a un CM durante el registro MAC de RF.

En respuesta a un mensaje petición de autorización, un CMTS valida la entidad del CM solicitante, determina el algoritmo de criptación y el soporte de protocolos que comparte con el CM, activa una clave de autorización para el CM, la cripta con la clave pública del módem de cable y la devuelve al CM en un mensaje respuesta de autorización. La respuesta de autorización incluye:

- una clave de autorización criptada con la clave pública del CM;
- un número de secuencia de clave de 4 bits, utilizado para distinguir entre generaciones sucesivas de claves de autorización;
- el tiempo de vida de una clave;
- las identidades (es decir, los SAID) y las propiedades de la única asociación de seguridad primaria y las cero o más asociaciones de seguridad estáticas respecto a las que el CM está autorizado a obtener información sobre aplicación de claves.

Si bien la respuesta de autorización PUEDE identificar SA estáticas además de la SA primaria cuyo SAID concuerda con el SID de mejor esfuerzo del CM solicitante, NO DEBE identificar en cambio ninguna SA dinámica.

El CMTS determinará, al responder a la petición de autorización de un CM, si el módem de cable solicitante, cuya identidad se puede verificar mediante el certificado digital X.509, está autorizado para servicios de unidifusión básicos, y a qué otros servicios prestados estáticamente (es decir, los SAID estáticos) está abonado el usuario del módem de cable. Se señala que los servicios protegidos que un CMTS pone a disposición de un CM cliente pueden depender de las series criptográficas particulares cuyo soporte comparten el CM y el CMTS.

Tras conseguir la autorización, el CM pone en marcha una máquina de estados TEK distinta por cada SAID identificado en el mensaje respuesta de autorización. Cada máquina de estados TEK que funciona dentro del CM es responsable de la gestión del material de aplicación de claves asociado con su correspondiente SAID. Las máquinas de estados TEK envían periódicamente mensajes de petición de clave al CMTS, solicitando la renovación del material de aplicación de claves para sus SAID respectivos. Una petición de clave incluye:

- información de identificación exclusiva del módem de cable, consistente en el ID del fabricante, el número de serie, la dirección MAC y la clave pública RSA;
- el SAID cuyo material de aplicación de claves se está solicitando;
- un compendio de mensajes con clave HMAC, con el que se autentica la petición de clave.

El CMTS responde a una petición de clave con un mensaje respuesta de clave que contiene el material de aplicación de claves activo del CMTS para un SAID específico. Dicho material incluye:

- la clave de criptación de tráfico criptada según DES triple;
- un vector de inicialización del CBC;
- un número de secuencia de clave;
- el tiempo de vida restante de una clave;
- un mensaje con clave HMAC, con el que se autentica la respuesta de clave.

La clave de criptación de tráfico (TEK) de la respuesta de clave se cripta según DES triple (criptación-descriptación-criptación o modo EDE), utilizando una clave de criptación de claves (KEK) de DES triple de dos claves derivada de la clave de autorización.

Se señala que el CMTS mantiene en todo momento dos conjuntos activos de material de aplicación de claves por cada SAID. Los tiempos de vida de las dos generaciones se superponen de tal manera que cada generación pasa a estar activa a mitad de la vida activa de su predecesora y prescribe a mitad de la de su sucesora. Un CMTS incluye en sus respuestas de clave las *dos* generaciones activas de material de aplicación de claves de un SAID.

La respuesta de clave proporciona al solicitante, además de la TEK y el vector de inicialización del CBC, el resto del tiempo de vida de cada uno de los dos conjuntos de material de aplicación de claves. El CM receptor utiliza esos tiempos de vida restantes para estimar cuándo invalidará el CMTS una TEK determinada y, por tanto, para cuándo ha de programar futuras peticiones de clave de tal manera que sus peticiones y recepciones de nuevo material de aplicación de claves se produzcan antes de que el CMTS haga que prescriba el material de ese tipo de claves que a la sazón retiene el CM.

El funcionamiento del algoritmo de programación de peticiones de clave de la máquina de estados TEK, combinado con el procedimiento del CMTS de actualización y utilización del material de aplicación de claves de un SAID (véase B.O.9), asegura que el CM podrá intercambiar continuamente tráfico criptado con el CMTS.

Un CM DEBE renovar periódicamente su clave de autorización reenviando una petición de autorización al CMTS. La reautorización es idéntica a la autorización con la salvedad de que el CM no envía mensajes información de autenticación durante los ciclos de reautorización. En la descripción de la máquina de estados autorización de B.O.7.1.2 se indica claramente cuándo se envían los mensajes información de autenticación.

Para evitar interrupciones del servicio durante la reautorización, se superponen los tiempos de vida de las generaciones sucesivas de claves de autorización del CM. Tanto el CM como el CMTS DEBEN poder soportar hasta dos claves de autorización activas simultáneamente durante esos periodos de transición. El funcionamiento del algoritmo de programación de peticiones de autorización de la máquina de estados autorización, junto con el procedimiento del CMTS de actualización y utilización de las claves de autorización de un CM cliente (véase B.O.9), asegura que los CM podrán renovar la información de aplicación de claves TEK sin interrupción mientras transcurren los periodos de reautorización del CM.

Una máquina de estados TEK permanece activa siempre que:

- el CM esté autorizado para funcionar en el dominio de seguridad del CMTS; es decir, tiene una clave de autorización válida, y
- el CM esté autorizado para participar en esa asociación de seguridad particular; es decir, el CMTS continúa proporcionando material de aplicación de claves renovado durante los ciclos de nueva aplicación de clave.

La máquina de estados autorización progenitora detiene todas sus máquinas de estados TEK vástagos cuando el CM recibe del CMTS un rechazo de autorización durante un ciclo de reautorización. Se pueden arrancar o detener máquinas de estados TEK específicas durante un ciclo de reautorización si las autorizaciones de SAID estático de un CM cambian durante reautorizaciones sucesivas.

La comunicación entre máquinas de estados autorización y TEK se produce mediante el traspaso de eventos y la mensajería de protocolos. La máquina de estados autorización genera eventos (esto es, los eventos parada, autorizado, autorización pendiente y autorización completa) a los que se dirigen sus máquinas de estados TEK vástagos. Las máquinas de estados TEK no trabajan con eventos de su máquina de estados autorización progenitora. La máquina de estados TEK afecta a la máquina de estados autorización indirectamente por los mensajes que un CMTS envía en respuesta a las

peticiones de un módem: un CMTS PUEDE responder a las peticiones de clave de una máquina TEK con una respuesta de fallo (es decir, mensaje de autorización no válida) que será tratada por la máquina de estados autorización.

B.O.7.1.1.1 Comentario preliminar sobre las asociaciones de seguridad dinámicas y el establecimiento de la correspondencia de las SA dinámicas

En la cláusula B.O.5.1.3 se presentan las SA dinámicas y se menciona la manera según la cual un CMTS puede establecer o eliminar una SA dinámica en respuesta a la iniciación o terminación de flujos de tráfico en sentido descendente (por ejemplo, el tráfico de un determinado grupo de multidifusión IP). Para que un CM utilice una máquina de estados TEK a fin de obtener el material de aplicación de claves de una asociación de seguridad dinámica, el CM ha de conocer cuál es el valor del SAID correspondiente. El CMTS, sin embargo, no manifiesta a los CM clientes de forma voluntaria la existencia de las SA dinámicas; por el contrario, corresponde a los CM pedir al CMTS las correspondencias entre identificadores de flujo de tráfico (por ejemplo, una dirección de multidifusión IP) y SAID dinámicos.

La BPI+ define el intercambio de mensajes mediante el cual un CM se entera del establecimiento de la correspondencia entre un flujo de tráfico en sentido descendente y una SA dinámica (todo el tráfico en sentido ascendente se cripta de conformidad con la SA primaria del CM). Una máquina de estados establecimiento de correspondencia de SA especifica cómo gestionan los módems de cable la transmisión de esos mensajes de petición de establecimiento de correspondencia. En la actualidad, sólo los servicios de gestión de multidifusión IP de la Recomendación J.112 anexo B utilizan este mecanismo. En el futuro, nuevos servicios pueden emplear SA dinámicas de BPI+.

La máquina de estados autorización controla el establecimiento y la terminación de las máquinas de estados TEK asociadas con la SA primaria y cualesquiera SA estáticas; no controla, sin embargo, el establecimiento y la terminación de las máquinas de estados TEK asociadas con SA dinámicas. Los CM DEBEN implementar la lógica necesaria para establecer y terminar la máquina de estados TEK de una SA dinámica. De todos modos, la presente especificación de interfaz no especifica cómo deberían gestionar los CM sus máquinas de estados TEK de SA dinámica.

La descripción completa del modelo de estados establecimiento de correspondencia de SA se pospone hasta B.O.8.

B.O.7.1.1.2 Selección de capacidades de seguridad

Como parte de su intercambio de autorización BPI+, el CM proporciona al CMTS una lista de todas las series criptográficas (emparejamiento de algoritmos de criptación de datos y de autenticación de datos) que soporta el CM. El CMTS selecciona de esa lista una sola serie criptográfica para emplearla con la SA primaria del CM solicitante. La respuesta de autorización que el CMTS devuelve al CM incluye un descriptor de SA primaria que, entre otras cosas, identifica la serie criptográfica que el CMTS seleccionó para utilizarla con la SA primaria del CM. Un CMTS DEBE rechazar la petición de autorización si determina que ninguna de la series criptográficas ofrecidas es satisfactoria.

La respuesta de autorización contiene también una lista facultativa de descriptores de SA estáticas; cada descriptor de SA estática identifica la serie criptográfica empleada dentro de la SA. La selección de la serie criptográfica de una SA estática se lleva a cabo normalmente con independencia de las capacidades criptográficas del CM solicitante. Un CMTS PUEDE incluir en su respuesta de autorización descriptores de SA estáticas que identifiquen series criptográficas que el CM solicitante no soporta. Si tal es el caso, el CM NO DEBE arrancar las máquinas de estados TEK para SA estáticas cuyas series criptográficas no soporta.

El marco de selección anterior se incorporó en BPI+ para soportar perfeccionamientos futuros del soporte físico basado en la Recomendación J.112 anexo B y del protocolo BPI+. En el momento de publicarse el presente anexo B.O, los únicos algoritmos de criptación de datos por paquetes

soportados eran DES de 56 bits y DES de 40 bits, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos por paquetes.

B.O.7.1.2 Máquina de estados autorización

La máquina de estados autorización consta de seis estados y ocho eventos distintos (incluida la recepción de mensajes) que pueden provocar transiciones de estados. La máquina de estados finitos (FSM, *finite state machine*) autorización se presenta más adelante con formato gráfico, como un modelo de flujos de estados (figura B.O.7-1) y con formato tabular, como una matriz de transiciones de estados (cuadro B.O.7-1).

El diagrama de flujos de estados muestra los mensajes de protocolo transmitidos y los eventos internos generados para cada una de las transiciones de estados del modelo; sin embargo, el diagrama no indica acciones internas adicionales, tales como la detención o el arranque de temporizadores, que acompañan a las transiciones de estados específicas. La matriz de transiciones de estados que se adjunta es una descripción detallada de las acciones específicas que se efectúan junto con cada transición de estado; la matriz de transiciones de estados DEBE ser utilizada como la especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

En el diagrama de flujos de la máquina de estados autorización que se muestra en la figura B.O.7-1 se han aplicado las reglas de representación siguientes:

- Los óvalos representan estados.
- Los eventos están en letra *cursiva*.
- Los mensajes están en letra de tipo normal.
- Las transiciones de estados (es decir, las líneas entre estados) se han etiquetado con <lo que provoca la transición>/<mensajes y eventos provocados por la transición>. Así pues "*temporización*/petición autoriz." significa que el estado ha recibido un evento "temporización" y ha enviado un mensaje petición de autorización ("petición autoriz."). Si hay múltiples eventos o mensajes antes de "/" separados por una coma, *cualquiera de ellos* puede provocar una transición. Si hay múltiples eventos o mensajes tras la barra inclinada, *todas* las acciones especificadas deben acompañar a la transición.

La matriz de transiciones de estados de autorización presentada en el cuadro B.O.7-1 contiene siete máquinas de estados autorización en la fila superior y ocho eventos de máquina de autorización (incluidas las recepciones de mensajes) en la columna situada más a la izquierda. Cualquier casilla de la matriz representa una combinación específica de estado y evento, mostrándose dentro de la casilla el estado siguiente (el estado al que se transita). Por ejemplo, la casilla 4-B representa la recepción de un mensaje respuesta de autorización (respuesta autoriz.) cuando se está en el estado espera de autorización (espera autoriz.). Dentro de la casilla 4-B figura el nombre del estado siguiente, "autorizado". Así pues, cuando la máquina de estados autorización de un CM está en el estado espera de autorización y se recibe el mensaje respuesta de autorización, la máquina de estados autorización pasa al estado autorizado. Junto con esta transición de estado deben llevarse a cabo varias acciones, que se describen en la relación de acciones de protocolo que figura bajo el epígrafe 4-B de B.O.7.1.2.5.

Una célula sombreada en la matriz de transiciones de estados significa que el evento de que se trate no puede o no debe ocurrir dentro de ese estado, y que si el evento se produce, la máquina de estados DEBE ignorarlo. Por ejemplo, si llega un mensaje respuesta de autorización cuando se está en el estado autorizado, dicho mensaje debería ser ignorado (casilla 4-C). El CM PUEDE, no obstante, en respuesta a un evento inapropiado, registrar cronológicamente su ocurrencia, generar un evento SNMP o efectuar cualquier otra acción definida por el vendedor. Ahora bien, esas acciones no se especifican dentro del contexto de la máquina de estados autorización, que simplemente ignora los eventos improcedentes.

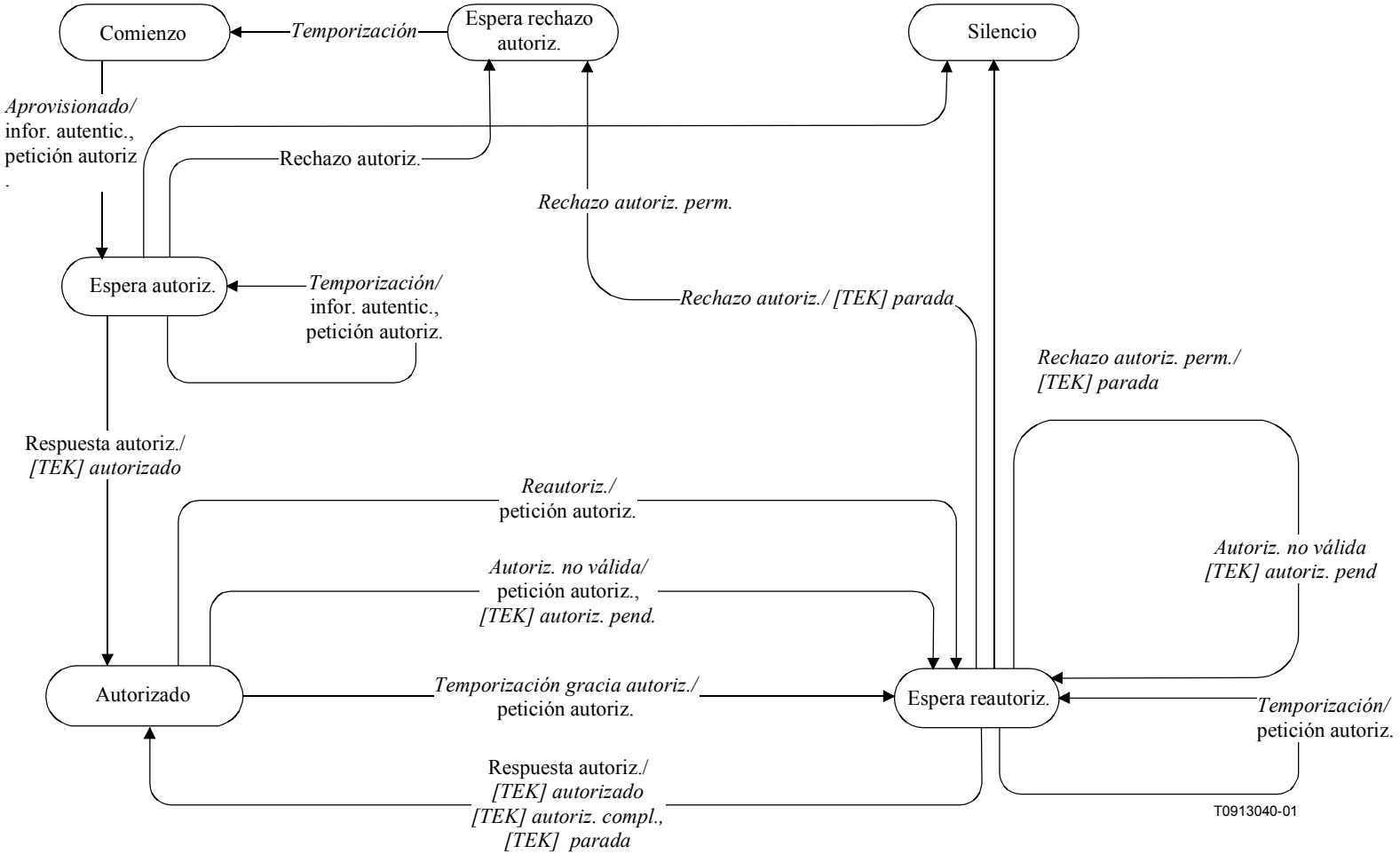


Figura B.O.7-1/J.112 – Diagrama de flujos de la máquina de estados autorización

Cuadro B.O.7-1/J.112 – Matriz de transición de estados de FSM autorización

Estado *Evento o mensaje recibido*	**(A) Comienzo**	**(B) Espera autoriz.**	**(C) Autorizado**	**(D) Espera reautoriz.**	**(E) Espera rechazo autoriz.**	**(F) Silencio**
(1) Aprovisionado	Espera autoriz.					
(2) Rechazo autoriz.		Espera rechazo autoriz.		Espera rechazo autoriz.		
(3) Rechazo autoriz. perm.		Silencio		Silencio		
(4) Respuesta autoriz.		Autorizado		Autorizado		
(5) Temporización		Espera autoriz.		Espera reautoriz.	Comienzo	
(6) Temporización gracia autoriz.			Espera reautoriz.			
(7) Autoriz. no válida			Espera reautoriz.	Espera reautoriz.		
(8) Reautoriz.			Espera reautoriz.			

B.O.7.1.2.1 Estados

B.O.7.1.2.1.1 Comienzo

Éste es el estado inicial de la máquina de estados finitos (FSM). No hay ningún recurso asignado a la FSM, ni utilizado por la misma, en este estado; por ejemplo, todos los temporizadores están desactivados, y no está programado ningún procesamiento.

B.O.7.1.2.1.2 Espera de autorización (espera autoriz.)

El CM ha recibido el evento "aprovisionado" que indica que ha completado el registro MAC de RF en el CMTS. En respuesta a la recepción del evento, el CM ha enviado un mensaje información de autenticación y un mensaje petición de autorización al CMTS y está esperando la respuesta.

B.O.7.1.2.1.3 Autorizado

El CM ha recibido un mensaje respuesta de autorización que contiene una lista de SAID válidos para ese CM. En este momento, el módem tiene una clave de autorización y una lista de SAID válidos. La transición a este estado provoca la creación de una FSM TEK para cada uno de los SAID de privacidad habilitada del CM.

B.O.7.1.2.1.4 Espera de reautorización (espera reautoriz.)

El CM tiene una petición de reautorización pendiente. El CM estaba a punto de agotar el tiempo de su autorización actual o había recibido una indicación (un mensaje autorización no válida del CMTS) de que su autorización ya no era válida. El CM envió un mensaje petición de autorización al CMTS y está esperando la respuesta.

B.O.7.1.2.1.5 Espera de rechazo de autorización (espera rechazo autoriz.)

El CM recibió un mensaje rechazo de autorización en respuesta a su última petición de autorización. El código de error del rechazo de autorización indicaba que el error no era de carácter permanente. En respuesta a la recepción de este mensaje de rechazo, el CM fijó un temporizador y transitó al estado espera de rechazo de autorización. El CM permanece en este estado hasta que expira el temporizador.

B.O.7.1.2.1.6 Silencio

El CM recibió un mensaje rechazo de autorización en respuesta a su última petición de autorización. El código de error del rechazo de autorización indicaba que el error era de carácter permanente. Esto provocó la transición al estado silencio, en el que al CM no se le permite pasar tráfico CPE, pero puede responder a peticiones de gestión SNMP que lleguen procedentes de toda la red de cable.

B.O.7.1.2.2 Mensajes

Los formatos de los mensajes se definen con detalle en B.O.7.2.

B.O.7.1.2.2.1 Petición de autorización (petición autoriz.)

Petición de una clave de autorización y de una lista de SAID autorizados. Enviado del CM al CMTS.

B.O.7.1.2.2.2 Respuesta de autorización (respuesta autoriz.)

Recepción de una clave de autorización y de una lista SAID autorizados y estáticos. Enviado del CMTS al CM. La clave de autorización es criptada con la clave pública del CM.

B.O.7.1.2.2.3 Rechazo de autorización (rechazo autoriz.)

La tentativa de autorización es rechazada. Enviado del CMTS al CM.

B.O.7.1.2.2.4 Autorización no válida (autoriz. no válida)

El CMTS puede enviar un mensaje autorización no válida a un CM cliente como:

- una indicación no solicitada, o
- la respuesta a un mensaje recibido de ese CM.

En cualquier caso, el mensaje autorización no válida ordena al CM receptor que obtenga una nueva autorización de su CMTS.

El CMTS responde a una petición de clave con un mensaje autorización no válida:

1) si no reconoce que el CM está siendo autorizado (es decir, no hay ninguna clave de autorización válida asociada con el módem de cable); o
2) falla la verificación del compendio de mensajes con clave de la petición de clave (en el atributo compendio de HMAC).

Se señala que el evento autorización no válida, al que se hace referencia en el diagrama de flujos de estados y en la matriz de transiciones de estados, significa la recepción de un mensaje autorización no válida o un evento generado internamente.

B.O.7.1.2.2.5 Información de autenticación (infor. autentic.)

El mensaje información de autenticación contiene el certificado X.509 del fabricante del módem. Es un mensaje estrictamente informativo que el CM envía al CMTS; con él, un CMTS PUEDE

enterarse dinámicamente del certificado del fabricante de los CM clientes. De manera alternativa, el CMTS PUEDE requerir una configuración fuera de banda de su lista de certificados de fabricante.

B.O.7.1.2.3 Eventos

B.O.7.1.2.3.1 Aprovisionado

La máquina de estados autorización genera este evento tras pasar al estado comienzo si el MAC de RF ha completado la inicialización, es decir, el registro en el CMTS. Si la inicialización del MAC de RF no se ha completado, el CM envía un evento aprovisionado a la FSM autorización tras completar el registro en el CMTS. El evento aprovisionado hace que el CM inicie el proceso de obtención de su clave de autorización y sus TEK.

B.O.7.1.2.3.2 Temporización

Ha concluido la temporización de un temporizador de retransmisión o espera. Por lo general se reenvía una petición.

B.O.7.1.2.3.3 Temporización de gracia de autorización (temporización gracia autoriz.)

Ha concluido la temporización del temporizador de periodo de gracia de autorización. Este temporizador fija una duración de tiempo configurable (el tiempo de gracia de autorización) antes de que la autorización en curso prescriba según lo previsto, indicando al CM que obtenga una nueva autorización antes de que su autorización prescriba efectivamente. El tiempo de gracia de autorización se especifica en una fijación de configuración dentro del fichero de parámetros telecargado vía TFTP.

B.O.7.1.2.3.4 Reautorización (reautoriz.)

El conjunto de SAID estáticos autorizados del CM puede haber cambiado. Este evento se genera en respuesta a un conjunto del SNMP, que tiene por objeto activar un ciclo de reautorización.

B.O.7.1.2.3.5 Autorización no válida (autoriz. no válida)

Este evento puede ser generado internamente por el CM cuando se produce el fallo de autenticación de un mensaje respuesta de clave, rechazo de clave o TEK no válida, o generado externamente por la recepción de un mensaje autorización no válida, enviado del CMTS al CM. Un CMTS responde a una petición de clave con un mensaje autorización no válida si falla la verificación del código de autenticación de mensajes de la petición. Ambos casos indican que el CMTS y el CM han perdido la sincronización de la clave de autorización.

Un CMTS PUEDE enviar también a un CM un mensaje autorización no válida no solicitado, forzando un evento autorización no válida.

B.O.7.1.2.3.6 Rechazo de autorización permanente (rechazo autoriz. perm.)

El CM recibe un mensaje rechazo de autorización en respuesta a un mensaje petición de autorización. El código de error del rechazo de autorización indica que el error es de carácter permanente. Lo que se interpreta como error permanente está sujeto al control administrativo dentro del CMTS. Entre los errores de procesamiento de una petición de autorización que pueden interpretarse como condiciones de error permanente figuran los siguientes:

- fabricante desconocido (no tiene certificado de CA del expedidor del certificado de CM),
- signatura o firma no válida en un certificado de CM,
- se produce un fallo en el análisis sintáctico de la ASN.1,
- incoherencias entre los datos del certificado y los datos de los atributos BPKM acompañantes,

- capacidades de seguridad incompatibles.

Cuando un CM recibe un mensaje rechazo de autorización indicando condición de fallo permanente, la máquina de estados autorización pasa al estado silencio en el que no se permite al CM pasar tráfico CPE, pero puede responder a las peticiones de gestión SNMP recibidas a través de la interfaz de la red de cable. Los CM DEBEN emitir una trampa SNMP tras pasar al estado silencio.

B.O.7.1.2.3.7 Rechazo de autorización (rechazo autoriz.)

El CM recibe un mensaje rechazo de autorización en respuesta a un mensaje petición de autorización. El código de error del rechazo de autorización no indica que el fallo se deba a una condición de error permanente. Como resultado de ello, la máquina de estados autorización del CM fija un temporizador de espera y transita al estado espera de rechazo de autorización. El CM permanece en este estado hasta que expire el temporizador, en cuyo momento volverá a intentar la autorización.

NOTA – Los eventos que siguen son enviados por la máquina de estados autorización a la máquina de estados TEK.

B.O.7.1.2.3.8 [TEK] Parada

Enviado por la FSM autorización a una FSM TEK activa (no estado COMIENZO) para terminar la FSM TEK y retirar el material de aplicación de claves del SAID correspondiente del cuadro de claves del CM.

B.O.7.1.2.3.9 [TEK] Autorizado

Enviado por la FSM autorización a una FSM TEK no activa (estado COMIENZO), pero válida.

B.O.7.1.2.3.10 [TEK] Autorización pendiente (autoriz. pend.)

Enviado por la FSM autorización a una FSM TEK específica para poner la FSM TEK en un estado de espera hasta que la FSM autorización pueda completar su operación de reautorización.

B.O.7.1.2.3.11 [TEK] Autorización completa (autoriz. compl.)

Enviado por la FSM autorización a una FSM TEK en los estados espera de reautorización operativa (espera reautoriz. oper.) o espera de reautorización de nueva aplicación de la clave (espera reautoriz. nueva aplic. clave) para eliminar el estado de espera iniciado por un evento autorización pendiente de la FSM TEK.

B.O.7.1.2.4 Parámetros

Todos los valores de los parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo B.O.A: Extensiones de fichero de configuración TFTP).

B.O.7.1.2.4.1 Temporización de espera de autorización (temporización espera autoriz.)

Periodo de temporización entre envíos de mensajes petición autorización desde el estado espera de autorización. Véase B.O.A.1.1.1.1.

B.O.7.1.2.4.2 Temporización de espera de reautorización (temporización espera reautoriz.)

Periodo de temporización entre envíos de mensajes petición de autorización desde el estado espera de reautorización. Véase B.O.A.1.1.1.2.

B.O.7.1.2.4.3 Tiempo de gracia de autorización (temporización gracia autoriz.)

Periodo de tiempo en que el CM se adelanta a la prescripción prevista de la autorización, comenzando la reautorización. Véase B.O.A.1.1.1.3.

B.O.7.1.2.4.4 Temporización de espera de rechazo de autorización (temporización espera rechazo autoriz.)

Periodo de tiempo que la FSM autorización de un CM permanece en el estado espera de rechazo de autorización antes de transitar al estado comienzo. Véase B.O.A.1.1.1.7.

B.O.7.1.2.5 Acciones

Las acciones efectuadas en asociación con transiciones de estados se indican mediante <evento/mensaje recibido> → <estado> en lo que sigue:

1-A Comienzo (*Aprovisionado*) → Espera autoriz.

- enviar mensaje información de autenticación a CMTS;
- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de autorización.

2-B Espera autoriz. (*Rechazo autoriz.*) → Espera rechazo autoriz.

- detener temporizador de reintento de petición de autorización;
- fijar un temporizador de espera a temporización de espera de rechazo de autorización.

2-D Espera reautoriz. (*Rechazo autoriz.*) → Espera rechazo autoriz.

- detener temporizador de reintento de petición de autorización;
- generar eventos parada de FSM TEK para todas las máquinas de estados TEK activas;
- fijar un temporizador de espera a temporización de espera de rechazo de autorización.

3-B Espera autoriz. (*Rechazo autoriz. perm.*) → Silencio

- detener temporizador de reintento de petición de autorización;
- inhabilitar todo reenvío de tráfico CPE.

3-D Espera reautoriz. (*Rechazo autoriz. perm.*) → Silencio

- detener temporizador de reintento de petición de autorización;
- generar eventos parada de FSM TEK para todas las máquinas de estados TEK activas;
- inhabilitar todo reenvío de tráfico CPE.

4-B Espera autoriz. (*Respuesta autoriz.*) → Autorizado

- detener temporizador de reintento de petición de autorización;
- descriptar y registrar la clave de autorización entregada con el mensaje respuesta de autorización;
- arrancar las FSM TEK de todos los SAID indicados en la respuesta de autorización (siempre que el CM soporte la serie criptográfica asociada con cada SAID) y emitir un evento autorizado de FSM TEK por cada una de las FSM TEK nuevas;
- fijar el temporizador de tiempo de gracia de autorización para que arranque "tiempo de gracia de autorización" segundos antes de que se produzca la prescripción prevista de la clave de autorización suministrada.

4-D Espera reautoriz. (*Respuesta autoriz.*) → Autorizado

- detener temporizador de reintento de petición de autorización;
- descriptar y registrar la clave de autorización entregada con el mensaje respuesta de autorización;

- arrancar las FSM TEK correspondientes a cualesquiera SAID recién autorizados indicados en la respuesta de autorización (siempre que el CM soporte la serie criptográfica asociada con cada SAID nuevo) y emitir un evento autorizado de FSM TEK por cada una de las FSM TEK nuevas;
- generar eventos autorización completa de FSM TEK para cualesquiera FSM TEK activas a la sazón cuyos SAID correspondientes estén indicados en la respuesta de autorización;
- generar eventos parada de FSM TEK para cualesquiera FSM TEK activas a la sazón cuyos SAID correspondientes no estén indicados en la respuesta de autorización;
- fijar el temporizador de tiempo de gracia de autorización para que arranque "tiempo de gracia de autorización" segundos antes de que se produzca la prescripción programada de la clave de autorización suministrada.

5-B Espera autoriz. (*Temporización*) → Espera autoriz.

- enviar mensaje información de autenticación a CMTS;
- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de autorización.

5-D Espera reautoriz. (*Temporización*) → Espera reautoriz.

- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

5-E Espera rechazo autoriz. (*Temporización*) → Comienzo

- ninguna acción de protocolo asociada con la transición de estado.

6-C Autorizado (*Temporización de tiempo de gracia de autoriz.*) → Espera reautoriz.

- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

7-C Autorizado (*Autoriz. no válida*) → Espera reautoriz.

- detener temporizador de tiempo de gracia de autorización;
- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización;
- si el evento autorización no válida está asociado con una determinada FSM TEK, generar un evento autorización pendiente de FSM TEK para la máquina de estados TEK responsable del evento autorización no válida (es decir, la FSM TEK que generó el evento, o envió el mensaje petición de clave al que el CMTS respondió con un mensaje autorización no válida).

7-D Espera reautoriz. (*Autoriz. no válida*) → Espera reautoriz.

- si el evento autorización no válida está asociado con una determinada FSM TEK, generar un evento autorización pendiente de FSM TEK para la máquina de estados TEK responsable del evento autorización no válida (es decir, la FSM TEK que generó el evento, o envió el mensaje petición de clave al que el CMTS respondió con un mensaje autorización no válida).

8-C Autorizado (*Reautoriz.*) → Espera reautoriz.

- detener temporizador de tiempo de gracia de autorización;
- enviar mensaje de petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

B.O.7.1.3 Máquinas de estados TEK1

La máquina de estados TEK consta de seis estados y nueve eventos (incluida la recepción de mensajes) que pueden provocar transiciones de estados. Al igual que la máquina de estados autorización, la máquina de estados TEK se presenta en un diagrama de flujos de estados y una matriz de transiciones de estados y como ocurrió con la máquina de estados autorización, la matriz de transiciones de estados DEBE ser utilizada como especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

Los estados sombreados de la figura B.O.7-2 (operativo, espera de nueva aplicación de clave y espera de reautorización de nueva aplicación de clave) tienen material de aplicación de claves válido y se puede pasar tráfico criptado.

La máquina de estados autorización arranca una máquina de estados TEK independiente por cada uno de sus SAID autorizados.

Como se mencionó en B.O.7.1.1, el CMTS mantiene dos TEK activas por cada SAID. El CMTS incluye en sus respuestas de clave esas TEK junto con el tiempo de vida restante de las mismas. El CMTS cripta tráfico en sentido descendente con la más antigua de las dos TEK y descripta tráfico en sentido ascendente con la TEK más antigua o más reciente, dependiendo de cuál de las dos claves está utilizando el CM en ese momento. El CM cripta tráfico en sentido ascendente con la más reciente de sus dos TEK y descripta tráfico en sentido descendente con la TEK más antigua o más reciente, dependiendo de cuál de las dos claves está utilizando el CMTS en ese momento. Véanse en B.O.9 los detalles de los requisitos de utilización de claves por parte del CM y el CMTS.

Mediante el funcionamiento de una máquina de estados TEK, el CM intenta guardar sus copias de las TEK de un SAID sincronizadas con las de su CMTS. Una máquina de estados TEK emite peticiones de clave para renovar copias del material de aplicación de claves de su SAID poco después del momento de prescripción prevista de la más antigua de sus dos TEK y antes de que prescriba su TEK más reciente. Para acomodar la oblicuidad de reloj del CM/CMTS y otros retardos de procesamiento de sistemas y transmisiones, el CM programa sus peticiones de clave con un número configurable de segundos antes de que se produzca la prescripción estimada de la TEK más reciente en el CMTS. Al recibir la respuesta de clave, el CM DEBE actualizar siempre sus registros con los parámetros de TEK de ambas TEK contenidos en el mensaje respuesta de clave. La figura B.O.7-2 ilustra la programación por parte del CM de sus renovaciones de clave junto con su gestión de las TEK activas de una SA de BPI+.

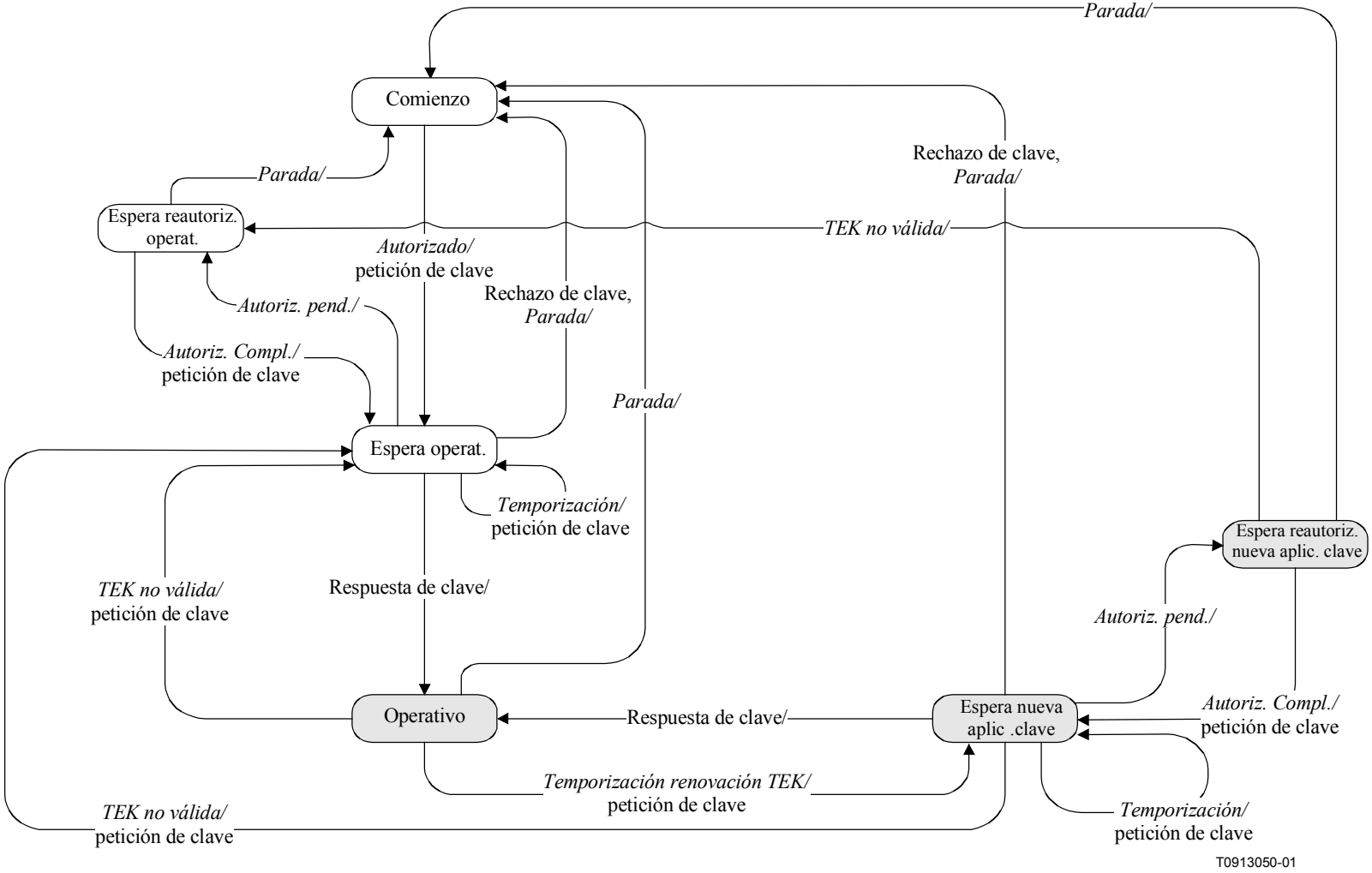


Figura B.O.7-2/J.112 – Diagrama de flujos de máquina de estados TEK

Cuadro B.O.7-2/J.112 – Matriz de transiciones de estados de FSM TEK

Estado *Evento o mensaje recibido*	**(A) Comienzo**	**(B) Espera operat.**	**(C) Espera reautoriz. operat.**	**(D) Operat.**	**(E) Espera nueva aplic. clave**	**(F) Espera reautoriz. nueva aplic. clave**
(1) Parada		Comienzo	Comienzo	Comienzo	Comienzo	Comienzo
(2) Autorizado	Espera operat.					
(3) Autoriz. pend.		Espera reautoriz. operat.			Espera reautoriz. nueva aplic. clave	
(4) Autoriz. compl.			Espera operat.			Espera nueva aplic. clave
(5) TEK no válida				Espera operat.	Espera operat.	Espera reautoriz. operat.
(6) Temporización		Espera operat.			Espera nueva aplic. clave	
(7) Temporización renovación TEK				Espera nueva aplic. clave		
(8) Respuesta clave		Operativo			Operativo	
(9) Rechazo clave		Comienzo			Comienzo	

B.O.7.1.3.1 Estados

B.O.7.1.3.1.1 Comienzo

Éste es el estado inicial de la FSM. No hay ningún recurso asignado a la FSM, ni inutilizado por la misma, en este estado; por ejemplo, todos los temporizadores están desactivados y no está programado ningún procesamiento.

B.O.7.1.3.1.2 Espera operativa (espera operat.)

La máquina de estados TEK ha enviado su petición inicial (petición de clave) de material de aplicación de claves para su SAID (clave de criptación de tráfico y vector de inicialización del CBC), y está esperando la respuesta del CMTS.

B.O.7.1.3.1.3 Espera de reautorización operativa (espera reautoriz. operat.)

Es el estado de espera en que se coloca la máquina de estados TEK si no tiene material de aplicación de claves válido mientras que la máquina de estados autorización está en medio de un ciclo de reautorización.

B.O.7.1.3.1.4 Operativo

El CM tiene material de aplicación de claves válido para el SAID.

B.O.7.1.3.1.5 Espera de nueva aplicación de clave

La temporización del temporizador de renovación de TEK ha expirado y el CM ha pedido una actualización de clave para este SAID. Se señala que la más reciente de sus dos TEK no ha prescrito y puede ser utilizada todavía para criptación y descriptación de tráfico de datos.

B.O.7.1.3.1.6 Espera de autorización de nueva aplicación de clave (espera autoriz. nueva aplic. clave)

Es el estado de espera en que se coloca la máquina de estados TEK si tiene material de aplicación de claves de tráfico válido, tiene pendiente una petición de material de aplicación de claves más reciente y la máquina de estados autorización inicia un ciclo de reautorización.

B.O.7.1.3.2 Mensajes

Los formatos de los mensajes se definen en detalle en B.O.7.2.

B.O.7.1.3.2.1 Petición de clave

Petición de una TEK para este SAID. Enviado por el CM al CMTS y autenticado con un compendio de mensajes con clave. La clave de autenticación de mensajes se obtiene a partir de la clave de autorización.

B.O.7.1.3.2.2 Respuesta de clave

Respuesta del CMTS que lleva los dos conjuntos activos de material de aplicación de claves de tráfico para este SAID. Enviado por el CMTS al CM, incluye las claves de criptación de tráfico del SAID, DES triple criptada con una clave de criptación de claves obtenida a partir de la clave de autorización. El mensaje respuesta de clave es autenticado con un compendio de mensajes con clave; la clave de autenticación se obtiene a partir de la clave de autorización.

B.O.7.1.3.2.3 Rechazo de clave

Respuesta del CMTS al CM para indicar que este SAID ya no es válido y no se va a enviar ninguna clave. El mensaje rechazo de clave es autenticado con un compendio de mensajes con clave; la clave de autenticación se obtiene a partir de la clave de autorización.

B.O.7.1.3.2.4 TEK no válida

El CMTS envía a un CM este mensaje si determina que el CM ha criptado una PDU datos por paquetes en sentido ascendente con una TEK no válida; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete recibido, está fuera de la gama conocida de números de secuencia válidos del CMTS para ese SAID.

B.O.7.1.3.3 Eventos

B.O.7.1.3.3.1 Parada

Enviado por la FSM autorización a una FSM TEK activa (no estado comienzo) para terminar la FSM TEK y retirar el material de aplicación de claves del SAID correspondiente del cuadro de claves del CM. Véase B.O.7.1.2.3.8.

B.O.7.1.3.3.2 Autorizado

Enviado por la FSM autorización a una FSM TEK no activa (estado comienzo) para notificar a la FSM TEK la autorización exitosa. Véase B.O.7.1.2.3.9.

B.O.7.1.3.3.3 Autorización pendiente (autoriz. pend.)

Enviado por la FSM autorización a una FSM TEK para poner la FSM TEK en un estado de espera mientras que la FSM autorización completa la reautorización. Véase B.O.7.1.2.3.10.

B.O.7.1.3.3.4 Autorización completa (autoriz. compl.)

Enviado por la FSM autorización a una FSM TEK en los estados espera de reautorización operativa o espera de reautorización de nueva aplicación de clave para eliminar el estado de espera iniciado por un evento autorización pendiente previo. Véase B.O.7.1.2.3.11.

B.O.7.1.3.3.5 TEK no válida

Este evento puede ser provocado por la lógica de descriptación de paquetes de datos de un CM, o por la recepción de un mensaje TEK no válida procedente del CMTS.

La lógica de descriptación de paquetes de datos de un CM provoca un evento TEK no válida si reconoce pérdida de sincronización de clave TEK entre él mismo y el CMTS criptador; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete en sentido descendente recibido, está fuera de la gama de números de secuencia conocidos del CM para ese SAID.

Un CMTS envía a un CM un mensaje TEK no válida, provocando un evento TEK no válida dentro del CM, si la lógica de descriptación del CMTS reconoce pérdida de sincronización de clave TEK entre él mismo y el CM.

B.O.7.1.3.3.6 Temporización

Temporización de un temporizador de reintentos. Por lo general, se retransmite la petición particular.

B.O.7.1.3.3.7 Temporización de renovación de TEK

Ha concluido la temporización del temporizador de renovación TEK. Este evento de temporizador ordena a la máquina de estados TEK que emita una nueva petición de clave para renovar su material de aplicación de claves. El temporizador de la renovación se fija de manera que haga posible una duración de tiempo configurable (tiempo de gracia de TEK) antes de que prescriba la TEK más reciente que retiene a la sazón el CM. Esto se configura mediante el CMTS para que ocurra tras la prescripción programada de la más antigua de las dos TEK.

B.O.7.1.3.4 Parámetros

Todos los valores de parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo B.O.A: Extensiones de fichero de configuración TFTP).

B.O.7.1.3.4.1 Temporización de espera operativa

Periodo de temporización entre envíos de mensajes petición de clave desde el estado espera operativa. Véase B.O.A.1.1.1.4.

B.O.7.1.3.4.2 Temporización de espera de nueva aplicación de clave

Periodo de temporización entre envíos de mensajes petición de clave desde el estado espera de nueva aplicación de clave. Véase B.O.A.1.1.1.5.

B.O.7.1.3.4.3 Tiempo de gracia de TEK

Periodo de tiempo, en segundos, en que el CM se adelanta a la prescripción estimada de una TEK, comenzando una nueva aplicación de clave para una nueva TEK.

El tiempo de gracia de TEK se especifica en una fijación de configuración dentro del fichero de parámetros telecargado vía TFTP, y es el mismo en todos los SAID. Véase B.O.A.1.1.1.6.

B.O.7.1.3.5 Acciones

1-B Espera operat. (*Parada*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK.

1-C Espera reautoriz. operat. (*Parada*) → Comienzo

- terminar FSM TEK.

1-D Operativo (*Parada*) → Comienzo

- detener temporizador de renovación de TEK, que es el temporizador fijado para que arranque "tiempo de gracia de TEK" segundos antes de que se produzca la prescripción prevista de la TEK;
- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

1-E Espera de nueva aplicación de clave (*Parada*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

1-F Espera reautoriz. nueva aplic. clave (*Parada*) → Comienzo

- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

2-A Comienzo (*Autorizado*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

3-B Espera operat. (*Autoriz. pend.*) → Espera reautoriz. operat.

- detener temporizador de reintento de petición de clave.

3-E Espera nueva aplic. clave (*Autoriz. pend.*) → Espera reautoriz. nueva aplic. clave

- detener temporizador de reintento de petición de clave.

4-C Espera reautoriz. operat. (*Autoriz. compl.*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

4-F Espera reautoriz. nueva aplic. clave (*Autoriz. compl.*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

5-D Operativo (*TEK no válida*) → Espera operat.

- detener temporizador de renovación de TEK;
- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa;
- retirar material de aplicación de claves de SAID de cuadro de claves.

5-E Espera de nueva aplic. clave (*TEK no válida*) → Espera operat.

- detener temporizador de reintento de petición de clave;
- enviar mensaje de petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa;
- retirar material de aplicación de claves de SAID de cuadro de claves.

5-F Espera reautoriz. nueva aplic. clave (*TEK no válida*) → Espera reautoriz. operat.

- retirar material de aplicación de claves de SAID de cuadro de claves.

6-B Espera operat. (*Temporización*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

6-E Espera nueva aplic. clave (*Temporización*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

7-D Operativo (*Temporización de tiempo de gracia de TEK*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

8-B Espera operat. (*Respuesta de clave*) → Operativo

NOTA 1 – La respuesta de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- procesar contenido de mensaje respuesta de clave e incorporar nuevo material de aplicación de claves en base de datos de claves;
- fijar temporizador de renovación de TEK para que arranque "tiempo de gracia de TEK" segundos antes de la prescripción prevista de la clave.

8-E Espera nueva aplic. clave (*Respuesta de clave*) → Operativo

NOTA 2 – La respuesta de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- procesar contenido de mensaje respuesta de clave e incorporar nuevo material de aplicación de claves en base de datos de claves;
- fijar temporizador de renovación de TEK para que se arranque "tiempo de gracia de TEK" segundos antes de la prescripción prevista de la clave.

9-B Espera operat. (*Rechazo de clave*) → Comienzo

NOTA 3 – El rechazo de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK.

9-E Espera nueva aplic. clave (*Rechazo de clave*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK;
- retirar material de aplicación de claves de SAID de cuadro de claves.

B.O.7.2 Formatos de mensajes de gestión de claves[5]

La gestión de claves de privacidad básica emplea dos tipos de mensajes MAC: BPKM-REQ y BPKM-RSP. La Recomendación J.112 anexo B define los valores de tipo específico asignados a los mismos (véase el cuadro B.O.7.3).

---

[5] Los formatos de los mensajes del protocolo de gestión de claves de privacidad básica se modelan de acuerdo con los del protocolo servicio de usuario de marcación directa de extensiones para autenticación a distancia (RADIUS, *remote authentification dial in user service*), definido en RFC 2058, y un protocolo de seguimiento de las normas Internet. BPKM, al igual que RADIUS, se atiene a un modelo cliente/servidor. A diferencia de RADIUS, BPKM no se aplicará a UDP/IP. Los mensajes BPKM se encapsulan dentro de los mensajes de gestión MAC de RF.

Cuadro B.O.7-3/J.112 – Mensajes MAC de gestión de claves de privacidad básica

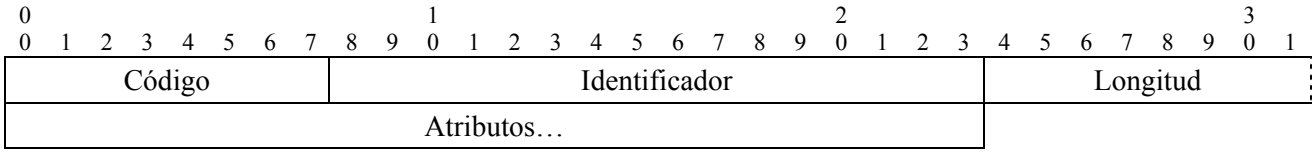
Valor de tipo	Nombre del mensaje	Descripción del mensaje
Véase el anexo B a la Rec. J.112	BPKM-REQ	Petición de gestión de clave de privacidad [CM → CMTS]
Véase el anexo B a la Rec. J.112	BPKM-RSP	Respuesta de gestión de clave de privacidad [CMTS → CM]

Si bien estos dos tipos de mensaje de gestión MAC distinguen entre peticiones (CM a CMTS) y respuestas (CMTS a CM) de BPKM, en los propios mensajes BPKM se codifica información más detallada a propósito del contenido de los mismos. Así se mantiene una separación clara entre funciones de gestión de privacidad y atribución de anchura de banda en sentido ascendente MAC de RF, temporización y sincronización (principales responsabilidades de la gestión MAC de RF).

B.O.7.2.1 Formatos de paquetes

En el campo cabida útil de mensaje de gestión de un mensaje de gestión MAC se encapsula exactamente un mensaje BPKM.

A continuación se muestra de forma resumida el formato de un mensaje BPKM. Los campos se transmiten de izquierda a derecha.



Código

El campo código es de un octeto, e identifica el tipo de paquete BPKM. Si se recibiera un paquete con un campo código no válido, DEBERÍA ser descartado en silencio.

Los códigos BPKM (decimales) se asignan como sigue en el cuadro B.O.7-4.

Cuadro B.O.7-4/J.112 – Códigos de mensajes de gestión de claves de privacidad básica

Código	Tipo de mensaje BPKM	Nombre de mensaje de gestión MAC
0-3	Reservado	–
4	Petición de autorización	BPKM-REQ
5	Respuesta de autorización	BPKM-RSP
6	Rechazo de autorización	BPKM-RSP
7	Petición de clave	BPKM-REQ
8	Respuesta de clave	BPKM-RSP
9	Rechazo de clave	BPKM-RSP
10	Autorización no válida	BPKM-RSP
11	TEK no válida	BPKM-RSP
12	Información de autenticación	BPKM-REQ
13	Petición de relación de correspondencia	BPKM-REQ
14	Respuesta de relación de correspondencia	BPKM-RSP
15	Rechazo de relación de correspondencia	BPKM-RSP
16-255	Reservado	–

Identificador

El campo identificador es de un octeto. Un CM utiliza el identificador para que concuerden las respuestas de un CMTS con las peticiones del CM.

El CM DEBE cambiar (por ejemplo, incrementar, volviendo a 0 tras llegar a 255) el campo identificador cuando emita un mensaje BPKM nuevo. Un mensaje "nuevo" es una petición de autorización, petición de clave, o petición de relación de correspondencia de SA que no sea una retransmisión enviada en respuesta a un evento temporización. Para las retransmisiones, el campo identificador DEBE permanecer inalterado.

El campo identificador de los mensajes información de autenticación, que son informativos y no efectúan ninguna mensajería de respuesta, PUEDE fijarse a cero.

El campo identificador del mensaje de respuesta BPKM de un CMTS DEBE concordar con el campo identificador del mensaje de petición BPKM al que responde el CMTS. El campo identificador de mensajes TEK no válida, no enviados en respuesta a peticiones BPKM, DEBE fijarse a cero. El campo identificador de mensajes autorización no válida no solicitados DEBE fijarse a cero.

Al recibir un mensaje de respuesta BPKM, el CM asocia el mensaje con una máquina de estados determinada (la máquina de estados autorización en el caso de respuestas de autorización, rechazos de autorización y autorizaciones no válidas; una máquina de estados TEK particular en el caso de respuestas de clave, rechazos de clave y TEK no válidas; una máquina de estados establecimiento de correspondencia de SA particular en el caso de respuestas de relación de correspondencia de SA y rechazos de relación de correspondencia de SA).

Un CM PUEDE efectuar el seguimiento del identificador de su petición de autorización más reciente y pendiente. El CM PUEDE descartar en silencio las respuestas de autorización y los rechazos de autorización cuyos campos identificador no concuerden con los de las peticiones pendientes.

Un CM PUEDE efectuar el seguimiento del identificador de su petición de clave más reciente y pendiente. El CM PUEDE descartar en silencio las peticiones de clave y los rechazos de clave cuyos campos identificador no concuerden con los de las peticiones pendientes.

Un CM PUEDE efectuar el seguimiento del identificador de su petición de relación de correspondencia de SA más reciente y pendiente. El CM PUEDE descartar en silencio las respuestas de relación de correspondencia de SA y los rechazos de relación de correspondencia de SA cuyos campos identificador no concuerden con los de las peticiones pendientes.

Longitud

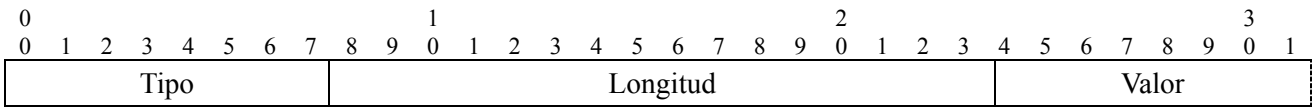
El campo longitud es de dos octetos. Indica la longitud de los campos atributo en octetos. El campo longitud no incluye los campos código, identificador y longitud. Los octetos fuera de la gama del campo longitud DEBEN ser tratados como relleno e ignorados en recepción. Si el paquete fuese más corto que lo que indica el campo longitud, DEBERÍA ser descartado en silencio. La longitud mínima es 0 y la máxima es 1490.

Atributos

Los atributos BPKM llevan los datos específicos de autenticación, autorización y gestión de las claves intercambiadas entre el cliente y el servidor. Cada tipo de paquete BPKM tiene su propio conjunto de atributos requeridos y opcionales. A menos que se indique de manera explícita, no hay ningún requisito respecto al orden de los atributos dentro de un mensaje BPKM.

El final de la lista de atributos viene indicada por la longitud del paquete BPKM.

Los atributos se codifican en forma tipo/longitud/valor (TLV), como se muestra seguidamente. Los campos se transmiten de izquierda a derecha.



A continuación se describen los formatos de los paquetes de cada mensaje BPKM. Las descripciones dan la relación de atributos BPKM contenidos dentro de cada tipo de mensaje BPKM. Los propios atributos se describen en B.O.7.2.2. Los atributos desconocidos DEBEN ser ignorados en recepción, y se pasarán por alto cuando se explore buscando atributos reconocidos.

El CMTS DEBE descartar en silencio todas las peticiones que no contengan TODOS los atributos requeridos. El CM DEBE descartar en silencio todas las respuestas que no contengan TODOS los atributos requeridos.

B.O.7.2.1.1 Petición de autorización (petición autoriz.)

Código: 4

Atributos:

Cuadro B.O.7-5/J.112 – Atributos de petición de autorización

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
CM-Certificate	Contiene el certificado de usuario X.509 del CM
Security-Capabilities	Describe la petición de capacidades de seguridad del CM solicitante
SAID	SAID primario del CM igual al SID primario

El atributo CM-Identification (identificación de CM) contiene un conjunto de datos que identifican el módem de cable solicitante al CMTS. Se señala que el CMTS utiliza, con toda probabilidad, un solo elemento del atributo CM-Identification (por ejemplo, la dirección MAC de CM) como un asa del CM. Aunque podría seleccionarse un elemento específico para incorporarlo en el mensaje petición de autorización, la inclusión del atributo CM-Identification a efectos de identificación del cliente proporciona a los vendedores un mayor grado de flexibilidad a la hora de diseñar el sistema de cabecera.

El atributo CM-Certificate (certificado de CM) contiene un certificado X.509 de CM expedido por el fabricante del CM. El certificado X.509 del CM es un certificado de clave pública que vincula la información de identificación del CM a su clave pública RSA de manera verificable. El certificado X.509 va firmado digitalmente por el fabricante del CM, y esa firma (signatura) puede ser verificada por un CMTS que conozca la clave pública del fabricante. La clave pública del fabricante se pone en un certificado expedido por la autoridad de certificación (CA, *certification authority*), conforme a X.509, que a su vez va firmado por una autoridad de certificación de nivel superior.

El atributo Security-Capabilities (capacidades de seguridad) es un atributo compuesto que describe las capacidades de seguridad del módem de cable solicitante. Se incluyen aquí el algoritmo o los algoritmos de criptación de datos por paquetes que soporta un CM y el algoritmo o los algoritmos de autenticación de datos por paquetes soportados (de los que actualmente no hay ninguno) y la versión del protocolo de privacidad básica soportado (de las que actualmente hay una: la versión 1 para BPI+).

Un atributo SAID contiene el identificador de asociación de seguridad de privacidad básica, o SAID. En este caso, el SAID proporcionado es el SAID primario de BPI+ del CM, que es igual al SID primario asignado al módem de cable durante el registro MAC de RF.

B.O.7.2.1.2 Respuesta de autorización (respuesta autoriz.)

Enviado por el CMTS al CM cliente en respuesta a una petición de autorización, el mensaje respuesta de autorización contiene una clave de autorización, el tiempo de vida de la misma, su número de secuencia y una lista de descriptores de SA que identifican las asociaciones de seguridad primaria y estáticas a las que el módem de cable solicitante está autorizado a acceder y sus propiedades particulares (por ejemplo, tipo, serie criptográfica, etc.). La clave de autorización DEBE ser criptada con la clave pública del CM. La lista de descriptores de SA DEBE incluir un descriptor para el SAID de BPI+ primario notificado al CMTS en la petición de autorización correspondiente. La lista de descriptores de SA PUEDE incluir descriptores de SAID estáticos a los que el CM está autorizado a acceder.

Código: 5

Atributos:

Cuadro B.O.7-6/J.112 – Atributos de respuesta de autorización

Atributo	Contenido
AUTH-Key	Clave de autorización (AUTH), criptada con la clave pública del CM cliente objetivo
Key-Lifetime	Tiempo de vida de la clave de autorización
Key-Sequence-Number	Número de secuencia de clave de autorización
SA-Descriptor (uno o más)	Cada atributo compuesto descriptor de SA especifica un SAID y propiedades adicionales de la SA

B.O.7.2.1.3 Rechazo de autorización (rechazo autoriz.)

El CMTS responde a la petición de autorización de un CM con un mensaje rechazo de autorización si el CMTS rechaza la petición de autorización del CM.

Código: 6

Atributos:

Cuadro B.O.7-7/J.112 – Atributos de rechazo de autorización

Atributo	Contenido
Error-Code	Código de error que identifica el motivo del rechazo de la petición de autorización
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de la petición de autorización

Los atributos Error-Code (código de error) y Display-String (cadena de presentación) describen al CM solicitante el motivo del fallo de la autorización.

B.O.7.2.1.4 Petición de clave

Código: 7

Atributos:

Cuadro B.O.7-8/J.112 – Atributos de petición de clave

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de la petición de clave. El compendio de mensajes se efectúa con el encabezamiento del paquete y todos los atributos de la petición de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al CMTS autenticar el mensaje petición de clave. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase B.O.10.

B.O.7.2.1.5 Respuesta de clave

Código: 8

Atributos:

Cuadro B.O.7-9/J.112 – Atributos de respuesta de clave

Atributo	Contenido
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
TEK-Parameters	Generación "más antigua" de parámetros de clave pertinentes para el SAID
TEK-Parameters	Generación "más reciente" de parámetros de clave pertinentes para el SAID
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo TEK-Parameters (parámetros de TEK) es un atributo compuesto que contiene todo el material de aplicación de claves correspondiente a una generación particular de la TEK de un SAID. Se incluyen aquí la TEK, el tiempo de vida restante de la TEK, su número de secuencia de clave y el vector de inicialización del CBC. La TEK es encriptada. Véanse los detalles en B.O.7.2.2.13.

El CMTS mantiene en todo momento dos conjuntos de generaciones activas de material de aplicación de claves por cada SAID. (Un conjunto de material de aplicación de claves incluye la TEK y su vector de inicialización del CBC correspondiente.) Un conjunto corresponde a la generación "más antigua" de material de aplicación de claves y el otro a la generación "más reciente" de dicho material. La generación más reciente tiene un número de secuencia de clave superior en una unidad (módulo 16) al de la generación más antigua. La cláusula B.O.9.1 especifica los requisitos del

CMTS a efectos de mantenimiento y utilización de las dos generaciones activas de material de aplicación de claves de un SAID.

El CMTS entrega a un CM cliente ambas generaciones de material de aplicación de claves activo. Por ello, el mensaje respuesta de clave contiene dos atributos TEK-Parameters, cada uno de los cuales contiene el material de aplicación de claves de uno de los dos conjuntos activos de material de aplicación de claves del SAID.

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de la respuesta de clave. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código de BPKM) y todos los atributos de la respuesta de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje respuesta de clave y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase B.O.10.

B.O.7.2.1.6 Rechazo de clave

La recepción de un rechazo de clave indica que el CM cliente receptor ya no está autorizado para un SAID particular.

Código: 9

Atributos:

Cuadro B.O.7-10/J.112 – Atributos de rechazo de clave

Atributo	Contenido
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
Error-Code	Código de error que identifica el motivo del rechazo de la petición de clave
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de la clave
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos del rechazo de clave. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código de BPKM) y todos los atributos del rechazo de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje rechazo de clave y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase B.O.10.

B.O.7.2.1.7 Autorización no válida

El CMTS puede enviar un mensaje autorización no válida a un CM cliente, como:

- una indicación no solicitada, o
- una respuesta a un mensaje recibido de ese CM.

En cualquiera de ambos casos, el mensaje autorización no válida ordena al CM receptor que se ponga en contacto con su CMTS para obtener una nueva autorización.

El CMTS envía un mensaje autorización no válida en respuesta a una petición de clave si:

1) el CMTS no reconoce que el CM está autorizado (es decir, no hay ninguna clave de autorización válida asociada con el módem de cable solicitante); o

2) falla la verificación del compendio de mensajes con clave de la petición de clave (en el atributo HMAC-Digest), lo que indica una pérdida de sincronización de claves de autorización entre el CM y el CMTS.

Código: 10

Atributos:

Cuadro B.O.7-11/J.112 – Atributos de autorización no válida

Atributo	Contenido
Error-Code	Código de error que identifica el motivo de la autorización no válida
Display-String (opcional)	Cadena de presentación que describe la condición de fallo

B.O.7.2.1.8 TEK no válida

El CMTS envía un mensaje TEK no válida a un CM cliente si el CMTS determina que el CM ha criptado una PDU datos por paquetes en sentido ascendente con una TEK no válida; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete recibido, está fuera de la gama de números de secuencia válidos y conocidos del CMTS para ese SAID.

Código: 11

Atributos:

Cuadro B.O.7-12/J.112 – Atributos de TEK no válida

Atributo	Contenidos
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
Error-Code	Código de error que identifica el motivo del mensaje TEK no válida
Display-String (opcional)	Cadena de presentación que contiene información definida por el vendedor
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de TEK no válida. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código BPKM) y todos los atributos de TEK no válida, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje TEK no válida y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autorización del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase B.O.10.

B.O.7.2.1.9 Información de autenticación (infor. autentic.)

El mensaje información de autenticación contiene un solo atributo CA-Certificate (certificado de CA), con un certificado de CA X.509 para el fabricante del CM. El certificado de usuario X.509 del CM DEBE haber sido expedido por la autoridad de certificación (CA) identificada por el certificado de CA X.509. Todos los certificados de CA X.509 DEBEN ser expedidos por una autoridad de certificación raíz.

Los mensajes información de autenticación son de carácter estrictamente informativo: mientras que el CM DEBE transmitir mensajes información de autenticación según lo indicado por el modelo estados de autenticación (véase B.O.7.1.2), el CMTS PUEDE ignorarlos.

Código: 12

Atributos:

Cuadro B.O.7-13/J.112 – Atributos de información de autenticación

Atributo	Contenido
CA-Certificate	Certificado de fabricante de la CA que expide el certificado de CM

El atributo CA-Certificate (certificado de CA) contiene un certificado de CA X.509 de la CA que expidió el certificado de usuario X.509 del CM. La autoridad de certificación expide estos certificados de CA a fabricantes de CM certificados.

B.O.7.2.1.10 Petición de relación de correspondencia de SA (petición Map)

Un CM envía peticiones de relación de correspondencia de SA a su CMTS solicitando que se establezca la correspondencia entre un determinado flujo de tráfico en sentido descendente y una SA de BPI+. En la cláusula B.O.8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 13

Atributos:

Cuadro B.O.7-14/J.112 – Atributos de petición de relación de correspondencia de SA

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que el CM pide el establecimiento de correspondencia de una SA

B.O.7.2.1.11 Respuesta de relación de correspondencia de SA (respuesta Map)

Un CMTS envía una respuesta de relación de correspondencia de SA como respuesta positiva a la petición de relación de correspondencia de SA de un CM cliente. El mensaje respuesta de relación de correspondencia de SA informa al CM del establecimiento de la correspondencia entre una dirección indagada y una SA de BPI+. En la cláusula B.O.8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 14

Atributos:

Cuadro B.O.7-15/J.112 – Atributos de respuesta de relación de correspondencia de SA

Atributo	Contenido
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que el CM pide el establecimiento de correspondencia de una SA
SA-Descriptor	Atributo compuesto descriptor de SA que especifica el SAID de la SA cuya correspondencia se ha establecido y otras propiedades

B.O.7.2.1.12 Rechazo de relación de correspondencia de SAID (rechazo Map)

Un CMTS envía un rechazo de relación de correspondencia de SA como respuesta negativa a la petición de relación de correspondencia de SA de un CM cliente. El mensaje rechazo de relación de correspondencia de SA informa al CM de que:

1) el flujo de tráfico en sentido descendente identificado en el atributo SA-Query (indagación de SA) no está siendo criptado; o
2) el CM solicitante no está autorizado para recibir ese tráfico.

El contenido de un atributo de código de error distingue entre los dos casos. En la cláusula B.O.8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 15

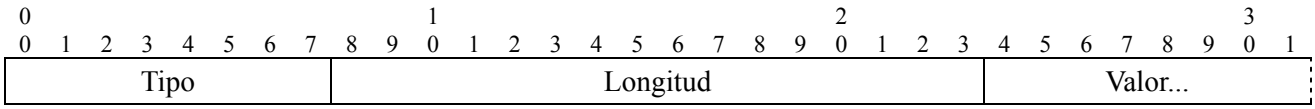
Atributos:

Cuadro B.O.7-16/J.112 – Atributos de rechazo de relación de correspondencia de SA

Atributo	Contenido
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que CM pide el establecimiento de correspondencia de una SA
Error-Code	Código de error que identifica el motivo del rechazo de la petición de relación de correspondencia de SA
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de relación de correspondencia

B.O.7.2.2 Atributos de BPKM

A continuación se muestra de forma resumida el formato de los atributos. Los campos se transmiten de la izquierda a derecha.



Tipo

El campo tipo es de 1 octeto. Los valores del campo tipo de BPKM se especifican más adelante. Se señala que en la especificación de la privacidad básica se definen valores de tipo entre 0 y 127; los valores entre 128 y 255 corresponden a tipos de atributo asignados por el vendedor.

Un servidor BPKM DEBE ignorar aquellos atributos cuyo tipo sea desconocido.

Un cliente BPKM DEBE ignorar aquellos atributos cuyo tipo sea desconocido.

El cliente y el servidor BPKM (es decir, CM y CMTS) PUEDEN registrar cronológicamente la recepción de tipos de atributo desconocidos.

Cuadro B.O.7-17/J.112 – Tipos de atributo de BPKM

Tipo	Atributo de BPKM
0	Reservado
1	Serial-Number (número de serie)
2	Manufacturer-ID (ID de fabricante)
3	MAC-Address (dirección MAC)
4	RSA-Public-Key (clave pública RSA)
5	CM-Identification (identificación de CM)
6	Display-String (cadena de presentación)
7	AUTH-KEY (clave de autorización)
8	TEK
9	Key-Lifetime (tiempo de vida de la clave)
10	Key-Sequence-Number (número de secuencia de clave)
11	HMAC-Digest (compendio de HMAC)
12	SAID
13	TEK-Parameters (parámetros de TEK)
14	SA-Flag OBSOLETED, atributo OBSOLETO
15	CBC-IV (vector de inicialización de CBC)
16	Error-Code (código de error)
17	CA-Certificate (certificado de CA)
18	CM-Certificate (certificado de CM)
19	Security-Capabilities (capacidades de seguridad)
20	Cryptographic-Suite (serie criptográfica)
21	Cryptographic-Suite-List (lista de series criptográficas)
22	BPI-Version (versión de BPI)
23	SA-Descriptor (descriptor de SA)
24	SA-Type (tipo de SA)
25	SA-Query (indagación de SA)
26	SA-Query-Type (tipo de indagación de SA)
27	IP-Address (dirección IP)
28-126	Reservado
127	Vendor-Defined (definido por el vendedor)
128-255	Vendor-assigned attribute types (tipos de atributo asignados por el vendedor)

Longitud

El campo longitud es de 2 octetos e indica la longitud del campo valor de este atributo, en octetos. El campo longitud no incluye los campos tipo y longitud[6]. La longitud mínima del atributo es 0, la longitud máxima es 1487.

Los paquetes que contengan atributos con longitudes no válidas DEBERÍAN ser descartados en silencio.

Valor

El campo valor es de 0 o más octetos y contiene información específica del atributo. El formato y la longitud del campo valor vienen determinados por los campos tipo y longitud. Todas las cantidades enteras de multioctetos están en el orden de bytes de la red, es decir, el octeto que contiene los bits más significativos es el primero que se transmite por el cable.

Se señala que no es preciso terminar una "cadena" con un NULO de ASCII porque el atributo ya tiene un campo longitud.

El formato del campo valor corresponde a uno de los cinco tipos de datos que se indican a continuación.

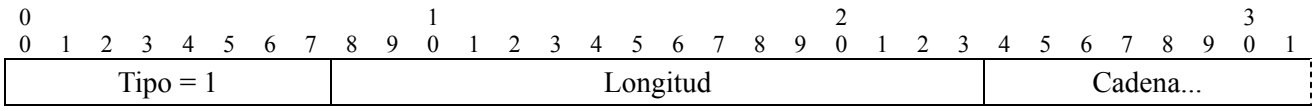
Cuadro B.O.7-18/J.112 – Tipos de datos de valor de atributo

string	0-1487 octetos
uint8	entero sin signo de 8 bits
uint16	entero sin signo de 16 bits
uint32	entero sin signo de 32 bits
compound	conjunto de atributos

B.O.7.2.2.1 Número de serie

Este atributo indica el número de serie asignado por el fabricante a un dispositivo módem de cable.

A continuación se muestra de forma resumida el formato del atributo Serial-Number (número de serie). Los campos se transmiten de izquierda a derecha.



Tipo

1 para Serial-Number

Longitud

≥ 0 y ≤ 255

---

[6] Se señala que esto es coherente con la codificación de la tupla TLV empleada en los elementos encabezamiento ampliado de MAC de RF, y con la codificación de la tupla TLV empleada para fijaciones de configuración del fichero de configuraciones del CM. La codificación de TLV de BPKM difiere de la utilizada por el protocolo RADIUS, en el que se basa la estructura de mensaje básica de BPKM: el campo longitud de los atributos RADIUS incluye los campos tipo y longitud, así como el campo valor de un atributo.

Cadena

El campo cadena es de 0 o más octetos y contiene un número de serie asignado por el fabricante.

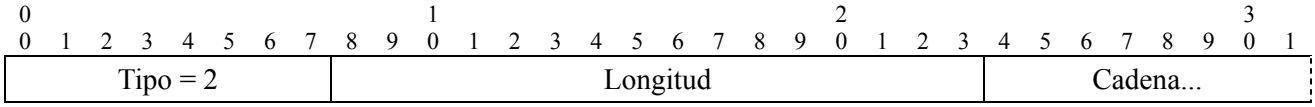
El número de serie asignado por el fabricante DEBE ser codificado de acuerdo con la codificación de caracteres de ISO 8859-1. Los caracteres empleados DEBEN limitarse a los siguientes:

- `A-Z (0x41-0x5A)`
- `a-z (0x61-0x7A)`
- `0-9 (0x30-0x39)`
- `"-" (0xD2)`

B.O.7.2.2.2 ID de fabricante

Este atributo identifica al fabricante. El identificador tiene una longitud de 3 octetos y contiene el identificador único de organización (OUI, *organizationally unique identifier*) de 3 octetos asignado a las organizaciones solicitantes por el IEEE [IEEE1]. Los dos primeros bits de la cadena de 3 octetos se fijan a cero.

A continuación se muestra de forma resumida el formato del atributo Manufacturer-ID (ID de fabricante). Los campos se transmiten de izquierda a derecha.



Tipo

2 para Manufacturer-ID

Longitud

3

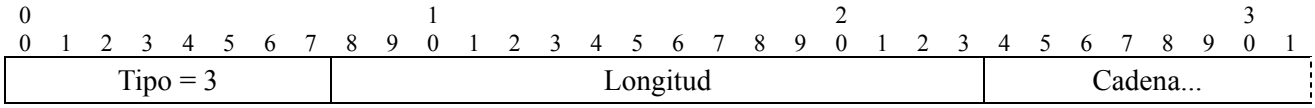
Cadena

El campo cadena es de 3 octetos y contiene un OUI del IEEE.

B.O.7.2.2.3 Dirección MAC

Este atributo identifica la dirección MAC del IEEE asignada al CM. Garantizada su unicidad, lo probable es que se utilice como asa/índice de módem de cable en el CMTS.

A continuación se muestra de forma resumida el formato del atributo MAC-Address (dirección MAC). Los campos se transmiten de izquierda a derecha.



Tipo

3 para MAC-Address

Longitud

6

Cadena

El campo cadena contiene una dirección MAC de 6 octetos.

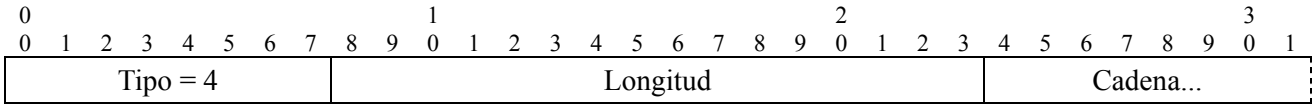
B.O.7.2.2.4 Clave pública RSA

Este atributo es un atributo cadena que contiene un tipo ASN.1 de clave pública RSA codificada según las reglas de codificación distinguida (DER, *distinguished encoding rules*), de acuerdo con lo definido en la norma de criptación de los laboratorios RSA PKCS#1 v2.0 [RSA2].

Según especifica la norma PKCS #1 v2.0, una clave pública RSA está formada por un módulo público RSA y un exponente público RSA; el tipo de clave pública RSA incluye ambas cosas como tipos ENTEROS codificados según DER.

La norma PKCS #1 v2.0 establece que el exponente público RSA puede ser normalizado en aplicaciones específicas, y sugiere valores de 3 ó 65537 (F4). La privacidad básica plus normaliza en F4 para un exponente público y emplea un módulo de 1024 bits (la privacidad básica empleaba un módulo de 768 bits). Para poder adaptar a BPI+ el soporte lógico de equipos construidos de acuerdo con una versión preliminar de la presente especificación, las implementaciones BPI+ DEBEN soportar un módulo de 768 bits.

A continuación se muestra de forma resumida el formato del atributo Public-Key (clave pública). Los campos se transmiten de izquierda a derecha.



Tipo

4 para RSA-Public-Key

Longitud

106 ó 140 (longitud de codificación DER, utilizando F4 como exponente público y un módulo de 768 bits o 1024 bits, respectivamente).

Cadena

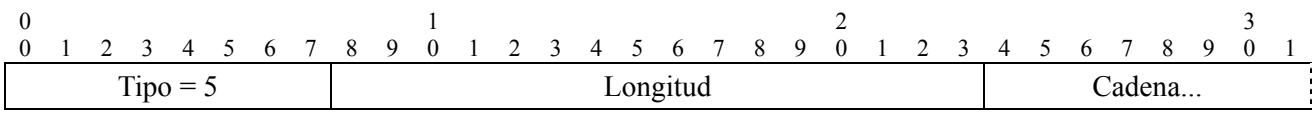
Clave pública RSA codificada según DER tipo ASN.1.

B.O.7.2.2.5 Identificación de CM

Este atributo es un atributo compuesto, formado por un conjunto de subatributos. Los subatributos contienen información que se puede utilizar para identificar de manera exclusiva un módem de cable. Entre los subatributos DEBEN figurar los siguientes:

- Serial-Number (número de serie).
- Manufacturer-ID (ID de fabricante).
- MAC-Address (dirección MAC).
- RSA-Public-Key (clave pública RSA).

El atributo CM-Identification (identificación de CM) PUEDE contener también atributos facultativos definidos por el vendedor.



Tipo

5

Longitud

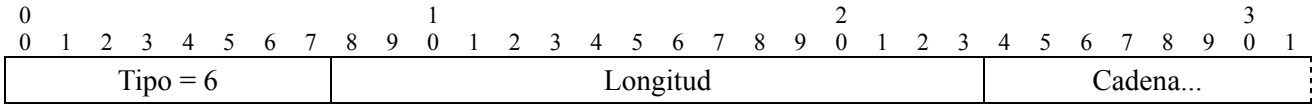
≥ 126

B.O.7.2.2.6 Cadena de presentación

Descripción

Este atributo contiene un mensaje textual. Su utilización típica consiste en explicar una respuesta de fallo, y podría ser registrado cronológicamente por el receptor para su recuperación posterior por un gestor SNMP. Las cadenas de presentación NO DEBEN tener una longitud superior a 128 bytes.

A continuación se muestra de forma resumida el formato del atributo Display-String (cadena de presentación). Los campos se transmiten de izquierda a derecha.



Tipo

6 para Display String

Longitud

≥ 0 y ≤ 128

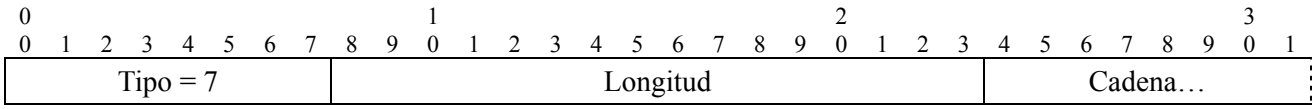
Cadena

Una cadena de caracteres. No se requiere que la cadena de caracteres termine con NULO; el campo longitud identifica siempre el final de la cadena.

B.O.7.2.2.7 Clave de autorización

El atributo Authorization Key (clave de autorización) es una cantidad de 20 bytes, de la que se obtienen una clave de encriptación de claves y dos claves de autenticación de mensajes (una para peticiones en sentido ascendente y otra para respuestas en sentido descendente).

Este atributo contiene una cantidad de 96 ó 128 octetos que a su vez contienen la clave de autorización criptada según RSA con la clave pública RSA de 768 bits o 1024 bits del CM. El texto cifrado producido por el algoritmo RSA tendrá la longitud del módulo RSA, es decir, 96 ó 128 octetos.



Tipo

7 para AUTH-Key

Longitud

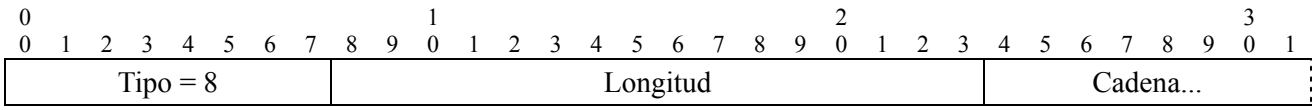
96 ó 128

Cadena

Cantidad de 96 ó 128 octetos que representa una clave de autorización criptada según RSA.

B.O.7.2.2.8 TEK

Este atributo contiene una cantidad de 8 octetos que es una clave DES TEK, criptada con una clave de criptación de claves obtenida a partir de la clave de autorización. Las claves TEK se encriptan utilizando el modo criptación-descriptación-criptación (EDE, *encrypt-decrypt-encrypt*) de DES triple de dos claves. Para los detalles, véase B.O.10.



Tipo

8 para TEK

Longitud

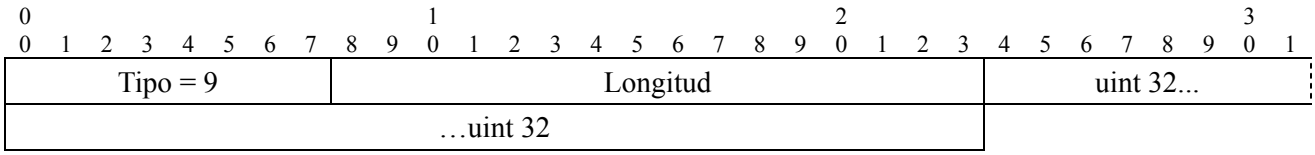
8

Cadena

Cantidad de 64 bits que representa una clave de criptación de tráfico encriptada (modo EDE de DES triple de dos claves).

B.O.7.2.2.9 Vida útil de clave

El atributo Key-Lifetime (tiempo de vida de clave) contiene el tiempo de vida, en segundos, de una clave de autorización o TEK. Es una cantidad sin signo de 32 bits que representa el número de segundos restantes durante los cuales la clave asociada será válida.



Tipo

9 para Key-Lifetime

Longitud

4

uint32

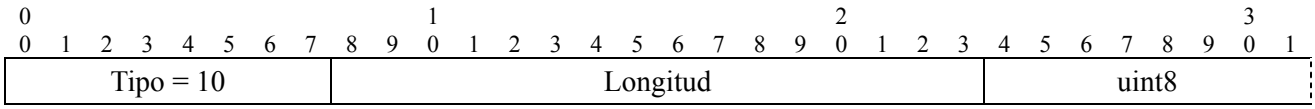
Cantidad de 32 bits que representa el tiempo de vida de la clave

Un tiempo de vida de clave de cero indica que no es válida la clave de autorización o la clave de encriptación de tráfico correspondiente.

B.O.7.2.2.10 Número de secuencia de clave

Este atributo contiene un número de secuencia de 4 bits para una TEK o una clave de autorización. La cantidad de 4 bits, no obstante, se almacena en un único octeto, con los 4 bits de orden superior fijados a 0.

A continuación se muestra de forma resumida el formato del atributo Key-Sequence-Number (número de secuencia de clave). Los campos se transmiten de izquierda a derecha.



Tipo

10 para Key-Sequence-Number

Longitud

1

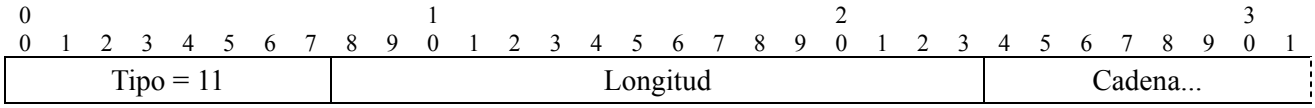
uint8

Número de secuencia de 4 bits

B.O.7.2.2.11 Compendio de HMAC

Este atributo contiene un troceo con clave utilizado para la autenticación de mensajes. El algoritmo HMAC se define en [RFC 2104] y se especifica utilizando un algoritmo de troceo criptográfico genérico. La privacidad básica utiliza una versión particular de HMAC que emplea el algoritmo de troceo seguro (SHA-1, *secure hash algorithm*-1), definido en [FIPS 180-1].

A continuación se muestra de forma resumida el formato del atributo HMAC-Digest (compendio de HMAC). Los campos se transmiten de izquierda a derecha.



Tipo

11 para HMAC-Digest

Longitud

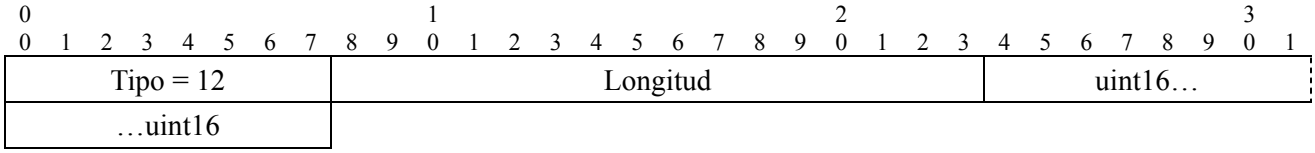
20 octetos

Cadena

Un troceo SHA con clave de 160 bits (20 octetos).

B.O.7.2.2.12 SAID

Este atributo contiene un identificador (ID) de asociación de seguridad (SAID) de 14 bits utilizado por privacidad básica plus como identificador de la asociación de seguridad. Los dos bits de orden superior se fijan a cero. Se señala que el SAID primario de BPI+ de un CM es igual al SID primario de ese CM.



Tipo

12 para SAID

Longitud

2

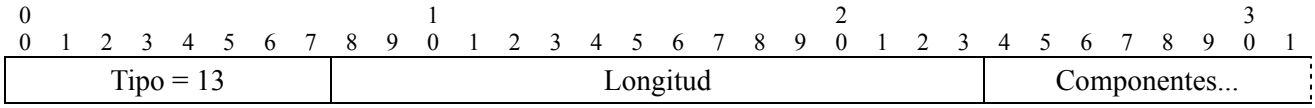
uint16

Cantidad de 16 bits que representa un SAID

B.O.7.2.2.13 Parámetros de TEK

Este atributo es un atributo compuesto, formado por un conjunto de subatributos. Los subatributos representan todos los parámetros de seguridad pertinentes para la generación particular de la TEK de un SAID.

A continuación se muestra de forma resumida el formato del atributo TEK-Parameters (parámetros de TEK). Los campos se transmiten de izquierda a derecha.



Tipo

13 para TEK-Parameters

Longitud

33

Componentes

El campo componentes contiene los subatributos que se indican a continuación:

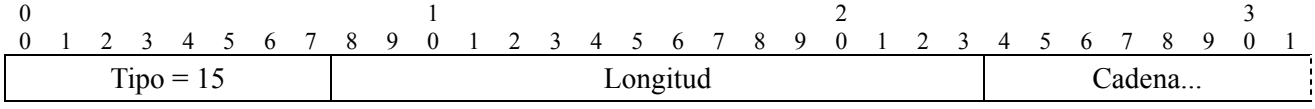
Cuadro B.O.7-19/J.112 – Subatributos de parámetros de TEK

Atributo	Contenido
TEK	TEK, criptada con la KEK (modo EDE de DES triple de dos claves)
Key-Lifetime	Tiempo de vida restante de la TEK
Key-Sequence-Number	Número de secuencia de TEK
CBC-IV	Vector de inicialización de encadenamiento de bloques cifrados (CBC)

B.O.7.2.2.14 Vector de inicialización de CBC

Este atributo contiene un valor de 64 bits (8 octetos) que especifica un vector de inicialización de encadenamiento de bloques cifrados (CBC).

A continuación se muestra de forma resumida el formato del atributo CBC-IV (vector de inicialización de CBC). Los campos se transmiten de izquierda a derecha.



Tipo

15 para CBC-IV

Longitud

8 octetos

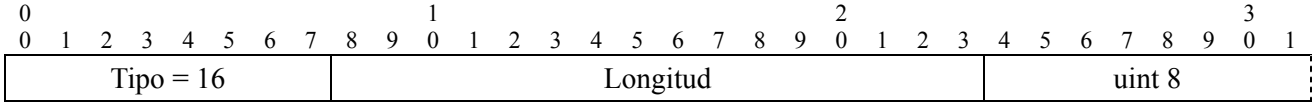
Cadena

Una cantidad de 64 bits que representa un vector de inicialización de CBC de DES.

B.O.7.2.2.15 Código de error

Este atributo contiene un código de error de un octeto que proporciona más información sobre un rechazo de autorización, un rechazo de clave, una autorización no válida o una TEK no válida.

A continuación se muestra de forma resumida el formato del atributo Error-Code (código de error). Los campos se transmiten de izquierda a derecha.



Tipo

16 para Error-Code

Longitud

1

uint8

código de error de 1 octeto

Un CMTS DEBE incluir el atributo Error-Code en todos los mensajes rechazo de autorización, autorización no válida, rechazo de clave y TEK no válida. El cuadro B.O.7-20 da la relación de valores de código a utilizar con este atributo. El CMTS PUEDE emplear los códigos de error distintos de cero (1-8) que se indican más abajo; PUEDE, no obstante, devolver un valor de código de cero (0). Los valores de código de error distintos de los definidos en el cuadro B.O.7-20 DEBEN ser ignorados. Si se devuelve un valor de código de cero, no se envía información de fallo adicional al CM; por motivos de seguridad, puede que esto sea lo conveniente.

Cuadro B.O.7-20/J.112 – Valores de código del atributo código de error

Código de error	Mensaje	Descripción
0	Todos	Sin información
1	Rechazo de autorización, autorización no válida	CM no autorizado
2	Rechazo de autorización, rechazo de clave	SAID no autorizado
3	Autorización no válida	No solicitado
4	Autorización no válida, TEK no válida	Número de secuencia de clave no válida
5	Autorización no válida	Fallo de autenticación de mensaje (petición de clave)
6	Rechazo de autorización	Fallo de autorización permanente
7	Rechazo de relación de correspondencia	No autorizado para el flujo de tráfico en sentido descendente solicitado
8	Rechazo de relación de correspondencia	Correspondencia entre flujo de tráfico en sentido descendente y SAID de BPI+ no establecida
9	Rechazo de autorización	Hora del día no adquirida

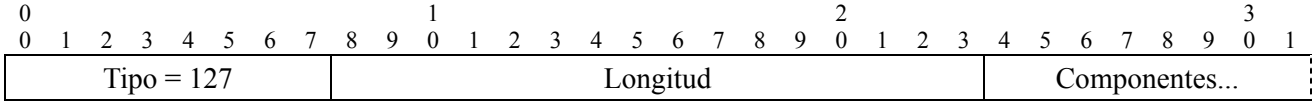
El código de error 6, fallo de autorización permanente, se utiliza para indicar un cierto número de condiciones de error diferentes que afectan al intercambio de autorización BPKM. Entre ellas figuran las siguientes:

- Fabricante desconocido; es decir, el CMTS no tiene el certificado de CA perteneciente al expedidor de un certificado de CM.
- El certificado de CM tiene una signatura o firma no válida.
- Fallo del análisis sintáctico de la ASN.1 durante la verificación de un certificado de CM.
- El certificado de CM está en la lista actualizada permanentemente ("lista caliente").
- Incoherencias entre los datos de un certificado y los datos de los atributos BPKM acompañantes.
- El CM y el CMTS tienen capacidades de seguridad incompatibles.

Su propiedad común consiste en que la condición de fallo se considera permanente: cualquier nueva tentativa de autorización seguiría dando como resultado rechazos de autorización. Los detalles sobre el motivo de un fallo de autorización permanente PUEDEN ser notificados al CM en un atributo cadena de presentación opcional que puede acompañar al atributo código de error en los mensajes rechazo de autorización. El CMTS DEBERÍA proporcionar la capacidad de decidir administrativamente si se envían o no detalles adicionales al CM. El CMTS PUEDE registrar cronológicamente estos fallos de autorización, o incluso atraparlos a continuación para un gestor SNMP.

B.O.7.2.2.16 Definido por el vendedor

El atributo Vendor-Defined (definido por el vendedor) es un atributo compuesto cuyo primer subatributo DEBE ser el atributo ID de fabricante. El o los atributos subsiguientes son definidos por el usuario, con valores de tipo asignados por el vendedor identificado por el atributo ID de fabricante previo.



Tipo

127 para Vendor-Defined

Longitud

≥ 6

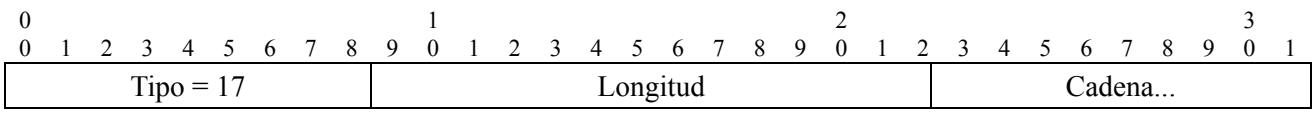
Componentes

El primer subatributo DEBE ser el ID de fabricante. Los atributos subsiguientes pueden incluir tipos universales (es decir, definidos dentro del presente anexo B.O), y tipos definidos por el vendedor, específicos del vendedor identificado en el subatributo ID de fabricante precedente.

B.O.7.2.2.17 Certificado de CA

Este atributo es un atributo cadena que contiene un certificado de CA X.509, definido en [UIT-T X.509].

A continuación se muestra de forma resumida el formato del atributo CA-Certificate (certificado de CA). Los campos se transmiten de izquierda a derecha.



Tipo

17 para CA-Certificate

Longitud

Variable. La longitud NO DEBE hacer que el mensaje de gestión MAC resultante exceda del tamaño máximo permitido.

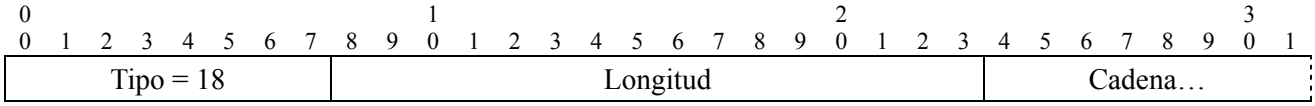
Cadena

Certificado de CA X.509 (ASN.1 con codificación según DER).

B.O.7.2.2.18 Certificado de CM

Este atributo es un atributo cadena que contiene el certificado de usuario X.509 de un módem de cable, definido en [UIT-T X.509].

A continuación se muestra de forma resumida el formato del atributo CM-Certificate (certificado de CM). Los campos se transmiten de izquierda a derecha.



Tipo

18 para CM-Certificate

Longitud

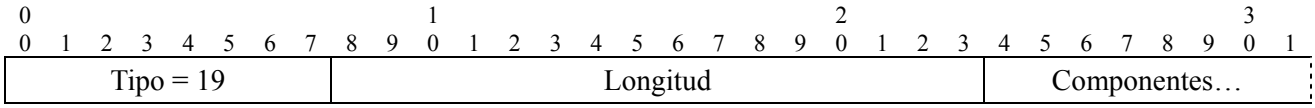
Variable. La longitud NO DEBE hacer que el mensaje de gestión MAC resultante exceda del tamaño máximo permitido.

Cadena

Certificado de usuario X.509 (ASN.1 con codificación según DER).

B.O.7.2.2.19 Capacidades de seguridad

El atributo Security-Capabilities (capacidades de seguridad) es un atributo compuesto cuyos subatributos identifican la versión de BPI+ que soporta un CM y la serie o series criptográficas que soporta.



Tipo

19 para Security-Capabilities

Longitud

≥ 9

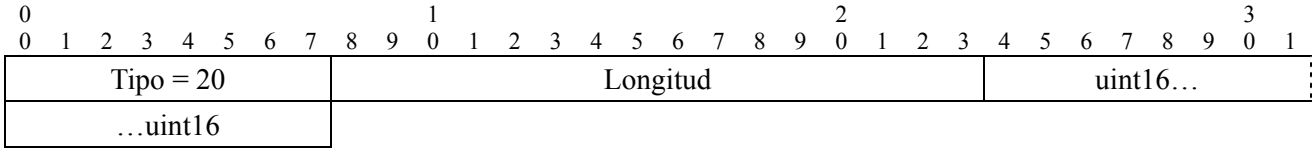
Componentes

El campo componentes contiene los subatributos que se indican a continuación:

Cuadro B.O.7-21/J.112 – Subatributos de capacidades de seguridad

Atributo	Contenido
Cryptographic-Suite-List	Lista de series criptográficas soportadas
BPI-Version	Versión de BPI+ soportada

B.O.7.2.2.20 Serie criptográfica



Tipo

20 para Criptographic-Suite

Longitud

2

Unit16

Un entero de 16 bits que identifica el emparejamiento de un algoritmo de criptación de datos (codificado en el byte situado más a la izquierda y más significativo) con un algoritmo de autenticación de datos (codificado en el byte situado más a la derecha y menos significativo). En la actualidad, DES de 56 bits y DES de 40 bits son los únicos algoritmos especificados para utilizar dentro de la seguridad, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos.

Cuadro B.O.7-22/J.112 – Identificadores de algoritmo de encriptación de datos

Valor	Descripción
0	Reservado
1	Modo CBC, DES de 56 bits
2	Modo CBC, DES de 40 bits
3-255	Reservado

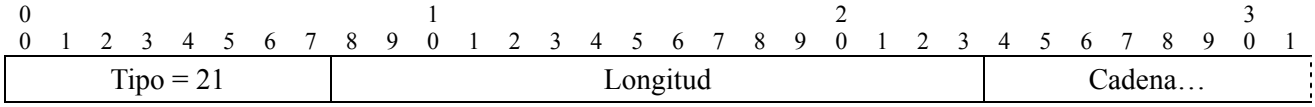
Cuadro B.O.7-23/J.112 – Identificadores de algoritmo de autenticación de datos

Valor	Descripción
0	Sin autenticación de datos
1-255	Reservado

Cuadro B.O.7-24/J.112 – Valores del atributo serie criptográfica

Valor	Descripción
256 (0x0100 hex)	Modo CBC, DES de 56 bits y sin autenticación de datos
512 (0x0200 hex)	Modo CBC, DES de 40 bits y sin autenticación de datos
Todos los demás valores	Reservado

B.O.7.2.2.21 Lista de series criptográficas



Tipo

21 para Cryptographic-Suite-List

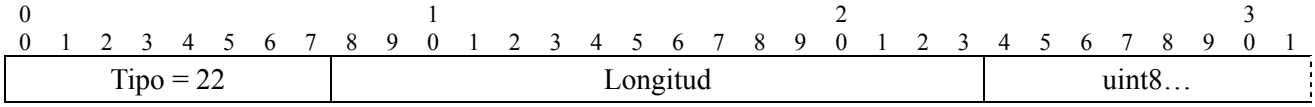
Longitud

2 × n, siendo n el número de series criptográficas indicadas

Uint8

Una lista de pares de bytes que identifica un conjunto de series criptográficas. Cada par de bytes representa una serie criptográfica soportada, con una codificación idéntica a la del campo valor del atributo serie criptográfica (B.O.7.2.2.20). El CMTS NO DEBE interpretar el orden relativo de los pares de bytes de la lista como preferencias del CM entre las series criptográficas que soporta.

B.O.7.2.2.22 Versión de BPI



Tipo

22 para BPI-Version

Longitud

1

Uint8

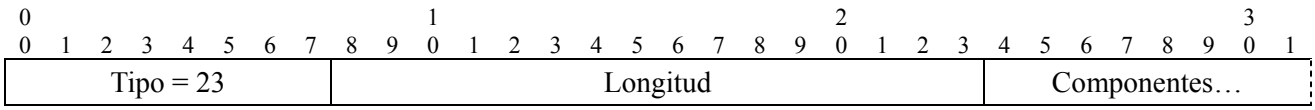
Un código de 1 octeto que identifica una versión de la seguridad de privacidad básica.

Cuadro B.O.7-25/J.112 – Valores del atributo versión de BPI

Valor	Descripción
0	Reservado
1	BPI+
2-255	Reservado

B.O.7.2.2.23 Descriptor de SA

El atributo SA-Descriptor (descriptor de SA) es un atributo compuesto cuyos subatributos describen las propiedades de una asociación de seguridad de BPI+. Esas propiedades incluyen el SAID, el tipo de SA y la serie criptográfica empleada dentro de la SA.



Tipo

23 para SA-Descriptor

Longitud

14

Componentes

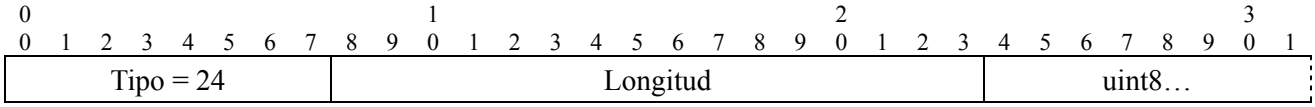
El campo componentes contiene los subatributos que se indican a continuación:

Cuadro B.O.7-26/J.112 – Subatributos de descriptor de SA

Atributo	Contenido
SAID	ID de asociación de seguridad
SA-Type	Tipo de SA
Cryptographic-Suite	Emparejamiento de algoritmos de criptación de datos y autenticación de datos empleados dentro de la SA

B.O.7.2.2.24 Tipo de SA

Identifica el tipo de SA. La BPI+ define tres tipos de SA: primario, estático y dinámico.



Tipo

24 para SA-Type

Longitud

1

Uint8

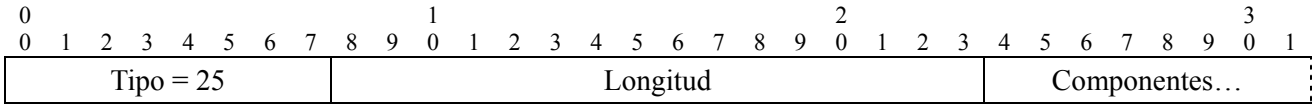
Un código de 1 octeto que identifica el valor del atributo SA-Type (tipo de SA) definido en el cuadro B.O.7-27.

Cuadro B.O.7-27/J.112 – Valores del atributo tipo de SA

Valor	Descripción
0	Primario
1	Estático
2	Dinámico
3-127	Reservado
128-255	Específico del vendedor

B.O.7.2.2.25 Indagación de SA

Se trata de un atributo compuesto utilizado en la petición de relación de correspondencia de SA para especificar los argumentos de indagación del establecimiento de la correspondencia. Los argumentos de la indagación incluyen el tipo de indagación y cualesquiera atributos de direccionamiento propios de ese tipo de indagación: los atributos de direccionamiento que identifican un determinado flujo de tráfico en sentido descendente para el que se pide el establecimiento de la correspondencia de una SA. En la actualidad, el único tipo de indagación especificado es multidifusión IP, y el argumento de direccionamiento asociado con ese tipo es una dirección de grupo IP.



Tipo

25 para SA-Query

Longitud

11

Componentes

El campo componentes contiene los subatributos que se indican a continuación:

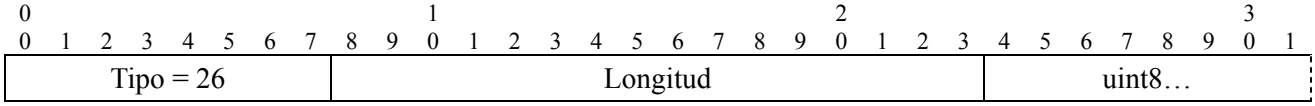
Cuadro B.O.7-28/J.112 – Subatributos de indagación de SA

Atributo	Contenido
SA-Query-Type	Tipo de indagación
IP-Address	Se requiere si tipo de indagación de SA = multidifusión IP; contiene una dirección de grupo IP de la que se pide el establecimiento de la correspondencia de SA

B.O.7.2.2.26 Tipo de indagación de SA

Este atributo identifica una dirección IP utilizada para identificar un flujo de tráfico IP criptado. Se emplea, por ejemplo, para especificar una dirección de grupo de multidifusión IP.

A continuación se muestra de forma resumida el formato del atributo SA-Query-Type (tipo de indagación de SA). Los campos se transmiten de izquierda a derecha.



Tipo

26 para SA-Query-Type

Longitud

1

Uint8

Un código de 1 octeto que identifica el valor del atributo tipo de indagación de SA definido en el cuadro B.O.7-29.

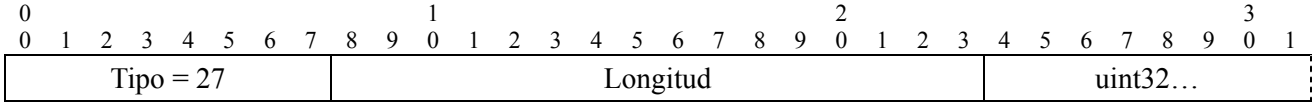
Cuadro B.O.7-29/J.112 – Valores del atributo tipo de indagación de SA

Valor	Descripción
0	Reservado
1	Multidifusión IP
2-127	Reservado
128-255	Específico del vendedor

B.O.7.2.2.27 Dirección IP

Este atributo identifica la dirección IP utilizada para identificar un flujo de tráfico IP criptado. Se emplea, por ejemplo, para especificar una dirección de grupo de multidifusión IP.

A continuación se muestra de forma resumida el formato del atributo IP-Address (dirección IP). Los campos se transmiten de izquierda a derecha.



Tipo

27 para IP-Address

Longitud

4

Uint32

Contiene el entero sin signo de 32 bits (en el orden de los bytes de la red) que representa una dirección IP.

B.O.8 Establecimiento de correspondencia de SA dinámica

B.O.8.1 Introducción

Las asociaciones de seguridad dinámicas (SA dinámicas) de BPI+, presentadas en B.O.5.1.3, son las SA que un CMTS establece y elimina, dinámicamente, en respuesta a su habilitación e inhabilitación de flujos específicos de tráfico en sentido descendente. Dichos flujos de tráfico pueden ser iniciados por las acciones de:

- un dispositivo CPE (equipo en las instalaciones del cliente) conectado a uno de los CM clientes del CMTS;
- un servidor de aplicación ubicado en la cabecera;
- un sistema de soporte de operaciones, u
- otros mecanismos no especificados.

Con independencia de lo que provoque el establecimiento de una SA dinámica dentro del CMTS, los CM clientes necesitan un mecanismo de aprendizaje del establecimiento de la correspondencia entre un determinado flujo de tráfico en sentido descendente protegido por BPI+ y la asociación de seguridad de BPI+ asignada dinámicamente de ese flujo (y el correspondiente SAID de esa SA).

La máquina de estados establecimiento de correspondencia de SA, definida en esta cláusula, especifica la manera según la cual los módems de cable indagan un CMTS para el establecimiento de la correspondencia entre flujos de tráfico en sentido descendente y SA dinámicas. La máquina de estados controla la transmisión de los mensajes petición de relación de correspondencia de SA a un CMTS.

La Recomendación J.112 anexo B especifica actualmente SA dinámicas para un solo tipo de servicio: el de criptación del tráfico de multidifusión IP en sentido descendente, restringiendo de este modo el acceso a dicho tráfico. Un CMTS puede establecer o eliminar SA dinámicas en respuesta a los cambios que se produzcan en cuanto a la pertenencia o no al grupo IP de dispositivos CPE en sentido descendente. Los mecanismos de gestión IGMP de dicho anexo pueden provocar el establecimiento de SA dinámicas en el CMTS. Esos mismos mecanismos DEBEN activar en el CM mensajes petición de relación de correspondencia BPI+ que indaguen el CMTS para el establecimiento de la correspondencia entre una dirección de grupo de multidifusión IP y una SA.

El mecanismo de establecimiento de la correspondencia de una SA de BPI+ PUEDE hacer corresponder un grupo de multidifusión IP con una SA estática, o incluso con una SA primaria de un determinado CM; la respuesta de un CMTS a una petición de establecimiento de correspondencia puede contener cualquiera de los tres tipos de SA. El mecanismo de establecimiento de correspondencia de SA, no obstante, es el único mecanismo mediante el cual un CM puede enterarse de la identidad de las SA dinámicas.

En la cláusula B.O.8.4 se examina con más detalle el uso particular del mecanismo de establecimiento de la correspondencia de una SA como soporte de dicho establecimiento entre tráfico de multidifusión IP y SA dinámicas. En las dos cláusulas que siguen, sin embargo, la atención se centra en el mecanismo más general de establecimiento de correspondencia de SA.

Se señala que en futuros perfeccionamientos de las especificaciones del servicio se pueden definir aplicaciones adicionales de las SA dinámicas.

B.O.8.2 Teoría de funcionamiento

La BPI+ define tres mensajes BPKM nuevos para soportar la indagación por los CM de los establecimientos de correspondencia de SA, a saber, el mensaje de petición de relación de correspondencia de SA, el de respuesta de relación de correspondencia de SA y el de rechazo de relación de correspondencia de SA. Un CM envía una petición de relación de correspondencia a su CMTS solicitando el establecimiento de la correspondencia entre un flujo en sentido descendente conocido y una SA. La petición de relación de correspondencia lleva atributos de datos BPI+ que identifican el CM solicitante y el flujo de tráfico en sentido descendente del que se pide el establecimiento de la correspondencia con la SA.

El CMTS puede responder a una petición de relación de correspondencia con:

- una respuesta de relación de correspondencia, que proporciona al CM el establecimiento de correspondencia de SA solicitado, o
- un rechazo de relación de correspondencia, que señala al CM que:
  1) no está autorizado a recibir el flujo de tráfico identificado en la petición de relación de correspondencia; o
  2) no se ha establecido la correspondencia entre el flujo de tráfico solicitado y una SA de BPI+.

Si el CM no recibe ninguna de las respuestas anteriores dentro de un periodo de tiempo de reintento configurable, envía de nuevo la petición de relación de correspondencia. Si no se recibe ninguna respuesta después de un número máximo configurable de reintentos, el CM deja de intentarlo.

Si el CM recibe un rechazo de relación de correspondencia, cesa toda tentativa ulterior de obtener el establecimiento de la correspondencia. En caso de que exista correspondencia entre el acceso al flujo de tráfico en sentido descendente y una SA de BPI+, y el CM solicitante no esté autorizado a acceder a esa SA, se denegará el acceso al CM y a su dispositivo CPE conectado, porque el CM no puede obtener el material de aplicación de claves necesario para descriptar los flujos de tráfico en sentido descendente criptados de conformidad con esa SA. Si el flujo de tráfico solicitado no está criptado (es decir, no existe correspondencia entre dicho flujo y una SA), el tráfico no encriptado será simplemente reenviado al dispositivo CPE conectado.

Si el CM recibe una respuesta de relación de correspondencia que identifica la SA de BPI+ asociada con el flujo de tráfico en sentido descendente solicitado, activa una máquina de estados TEK para la SA, siempre que:

1) el CM no esté utilizando ya una máquina de estados TEK para esa SA; y
2) el CM admita la serie criptográfica identificada en la respuesta de relación de correspondencia junto con el valor del ID de asociación de seguridad (SAID).

El CM puede estar utilizando ya una máquina de estados TEK si la SA, cuya correspondencia se ha establecido, es:

- una SA dinámica de la que se ha establecido la correspondencia con otro flujo de tráfico protegido y a la que el CM ya tiene acceso;
- la SA primaria del CM solicitante; o
- una SA estática de la que el CM ha tenido conocimiento en una respuesta de autorización recibida previamente.

Se señala que un CMTS puede asignar múltiples flujos de tráfico a la misma SA. Si se está criptando más de un flujo de tráfico descendente de conformidad con la misma SA dinámica, puede ocurrir que un CM esté ya utilizando una máquina de estados TEK para la SA identificada en la respuesta de relación de correspondencia. Se señala además que la correspondencia de la SA devuelta en la respuesta de relación de correspondencia no necesariamente ha de ser una SA dinámica: se puede hacer corresponder el flujo de tráfico solicitado con la SA primaria o una SA estática del CM.

La respuesta de relación de correspondencia incluye un atributo descriptor de SA que identifica tanto un SAID como la serie criptográfica empleada dentro de la SA. Como ocurre con las SA estáticas, la selección de una serie criptográfica de una SA dinámica se hace normalmente con independencia de las capacidades criptográficas del CM solicitante. Así pues, un CMTS PUEDE responder a una petición de relación de correspondencia con una SA (estática o dinámica) que emplea una serie criptográfica que el CM no soporta. El CM NO DEBE arrancar máquinas de estado TEK para SA estáticas o dinámicas cuyas series criptográficas no soporta. (No obstante, una SA primaria debe emplear una serie criptográfica soportada por el CM al que pertenece la SA.)

La máquina de estados TEK controla la recuperación del material de aplicación de claves de la SA cuya correspondencia se ha establecido. El CM enviará peticiones de clave para la SA; el CMTS puede responder a esas peticiones de clave con:

- un mensaje respuesta de clave, proporcionando al CM el material de aplicación de claves solicitado,
- un mensaje rechazo de clave, señalando al CM que no tiene autorización para el SAID solicitado y cuya correspondencia se ha establecido,
- un mensaje autorización no válida, señalando al CM que ha fallado la autenticación del mensaje petición de clave.

La recepción de un mensaje rechazo de clave fuerza la terminación de la máquina de estados TEK.

Se señala que el CMTS puede comunicarle a un CM cliente que no está autorizado a acceder a un determinado flujo de tráfico de una de las maneras siguientes: respondiendo a una petición de relación de correspondencia con un rechazo de correspondencia, o respondiendo a una petición de clave con un rechazo de clave. Depende de la implementación el que un CMTS compruebe o no la situación de autorización de un CM antes de responder a una petición de relación de correspondencia. Si la comprobación se efectúa durante el intercambio para el establecimiento de la correspondencia, se evitará que el CM ponga en marcha innecesariamente una máquina de estados TEK y envíe un mensaje petición de clave correspondiente a un SAID para el que no está autorizado.

B.O.8.3 Modelo de estados de establecimiento de correspondencia de SA

El modelo de estados de establecimiento de correspondencia de SA especifica el mecanismo por el cual un CM se entera del establecimiento de la correspondencia entre un flujo de tráfico y una SA dinámica.

Se arranca una máquina de estados cuando, dentro del CM, un evento externo al modelo de estados de establecimiento de correspondencia de SA, hace necesario el establecimiento de la correspondencia entre un flujo de tráfico y una SA (por ejemplo, cuando un CM instala los filtros de permiso para un grupo de multidifusión IP como resultado de los mecanismos de gestión IGMP

del CM). El evento externo genera un evento "Map" (relación de correspondencia) interno en la máquina de estados establecimiento de correspondencia de SA.

La máquina de estados termina si el CM no recibe una respuesta después de efectuar el número máximo de reintentos, o cuando el CM determina que ya no necesita el material de aplicación de claves de la SA cuya correspondencia se ha establecido. En este último caso, un evento externo genera un evento "Unmap" (terminación de relación de correspondencia) interno en la máquina de estados establecimiento de correspondencia de SA, forzando su terminación. Así pues, la máquina de estados puede ser utilizada no sólo para obtener la información requerida de establecimiento de correspondencia, sino también para efectuar el seguimiento del periodo de tiempo durante el cual una aplicación externa que utiliza el mecanismo de establecimiento de correspondencia de la SA (por ejemplo, la gestión IGMP) requiere ese establecimiento de correspondencia. La vinculación de un evento "Unmap" a un evento externo, y por tanto la implementación del evento Unmap es OPCIONAL.

Al igual que con las máquinas de estados TEK y autorización BIP+, la máquina de estados establecimiento de correspondencia de SA se presenta en formato gráfico, como un modelo de flujos de estados (figura B.O.8-1), y en formato tabular, como una matriz de transiciones de estados (cuadro B.O.8-1). Y al igual que las máquinas de estados definidas previamente, la matriz de transiciones de estados DEBE ser utilizada como la especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

Si, mediante el mecanismo de establecimiento de correspondencia de SA, un CM se entera de que necesita acceso al material de aplicación de claves de una SA dinámica, debe establecer una máquina de estados TEK para esa SA dinámica. Aunque que la máquina de estados autorización controla el establecimiento y la terminación de las máquinas de estados TEK asociadas con el SAID primario y cualesquiera SAID estáticos, no controla en cambio el establecimiento y la terminación de máquinas de estados TEK asociadas con SA dinámicas. Los CM DEBEN implementar la lógica necesaria para establecer y terminar máquinas de estados TEK para las SA dinámicas de las que se ha tenido conocimiento a través del mecanismo de establecimiento de correspondencia de SA. La especificación BIP+, no obstante, no define cómo deberían gestionar los CM las máquinas de estados TEK de sus SA dinámicas.

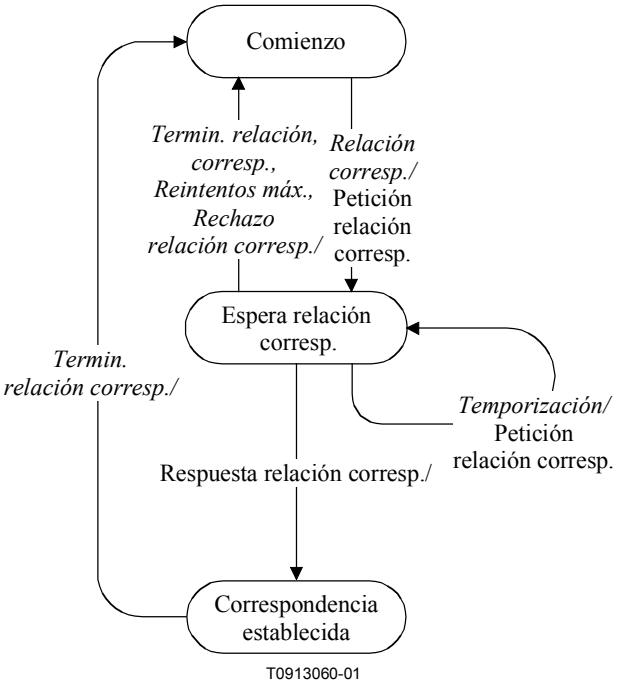


Figura B.O.8-1/J.112 – Diagrama de flujos de máquina de estados establecimiento de correspondencia de SA

Cuadro B.O.8-1/J.112 – Matriz de transición de estado de SAID dinámico

Estado *Evento o mensaje recibido*	**(A)** **Comienzo**	**(B)** **Espera relación corresp.**	**(C)** **Correspondencia establecida**
(1) *Relación corresp.*	Espera relación corresp.		
(2) *Termin. relación corresp.*		Comienzo	Comienzo
(3) *Respuesta relación corresp*.		Correspondencia establecida	
(4) *Rechazo relación corresp.*		Comienzo	
(5) *Temporización*		Espera relación corresp.	
(6) *Reintentos máx*.		Comienzo	

B.O.8.3.1 Estados

B.O.8.3.1.1 Comienzo

Es el estado inicial de la máquina de estados finitos.

B.O.8.3.1.2 Espera relación corresp.

El CM ha enviado al CMTS una petición de relación de correspondencia y está esperando la respuesta.

B.O.8.3.1.3 Correspondencia establecida

El CM ha recibido una respuesta de relación de correspondencia y se ha enterado de la petición de establecimiento de correspondencia de SA solicitada.

B.O.8.3.2 Mensajes

B.O.8.3.2.1 Petición de relación de correspondencia de SA (petición relación corresp.)

Enviado por el CM al CMTS para pedir el establecimiento de la correspondencia de una SA.

B.O.8.3.2.2 Respuesta de relación de correspondencia de SA (respuesta relación corresp.)

Respuesta positiva del CMTS a la petición de relación de correspondencia que contiene el establecimiento de correspondencia de SA solicitado.

B.O.8.3.2.3 Rechazo de relación de correspondencia de SA (rechazo relación corresp.)

Respuesta negativa del CMTS a la petición de relación de correspondencia del CM; señala al CM que:

1) no está autorizado a acceder al flujo de tráfico identificado en la petición de relación de correspondencia; o
2) no se ha establecido la correspondencia entre el flujo de tráfico solicitado y una SA de BPI+.

B.O.8.3.3 Eventos

B.O.8.3.3.1 Relación de correspondencia

Este evento provoca el arranque de la máquina de estados establecimiento de correspondencia de SA. El evento relación de correspondencia está vinculado a un evento de CM ajeno al protocolo BPI+.

B.O.8.3.3.2 Terminación de relación de correspondencia

Este evento provoca la terminación de la máquina de estados establecimiento de correspondencia de SA. El evento terminación de relación de correspondencia está vinculado a un evento de CM ajeno al protocolo BPI+. La implementación del evento Unmap es OPCIONAL.

B.O.8.3.3.3 Respuesta de relación de correspondencia

El módem de cable recibe un mensaje respuesta de relación de correspondencia de SA.

B.O.8.3.3.4 Rechazo de relación de correspondencia

El módem de cable recibe un mensaje rechazo de relación de correspondencia de SA.

B.O.8.3.3.5 Temporización

El módem de cable ha agotado su temporización esperando la respuesta a un mensaje petición de relación de correspondencia de SA pendiente.

B.O.8.3.3.6 Reintentos máximos

El módem de cable ha efectuado el número máximo de reintentos y no ha recibido ninguna respuesta.

B.O.8.3.4 Parámetros

Todos los valores de parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo B.O.A: Extensiones de fichero de configuración TFTP).

B.O.8.3.4.1 Temporización de espera de relación de correspondencia de SA

Es el periodo de temporización entre envíos de mensajes petición de relación de correspondencia de SA desde el estado espera de SA. Véase B.O.A.1.1.1.8.

B.O.8.3.4.2 Reintentos máximos de relación de correspondencia de SA

Número máximo de veces que el CM intenta la petición de relación de correspondencia de SA antes de dejar de intentarlo.

B.O.8.3.5 Acciones

Las acciones efectuadas en asociación con transiciones de estados se indican mediante <evento/mensaje recibido> → <estado> en lo que sigue:

1-A Comienzo (*Relación corresp.*) →Espera de relación de correspondencia

- enviar petición de relación de correspondencia de SA;
- fijar temporizador de reintentos de petición de relación de correspondencia a temporización de espera de relación de correspondencia de SA;
- fijar contador de reintentos de relación de correspondencia a 0.

2-B Espera de relación de correspondencia (*Termin. establ. corresp.*) → Comienzo

- detener temporizador de reintentos de petición de relación de correspondencia;
- terminar máquina de estados establecimiento de correspondencia de SA.

2-C Correspondencia establecida (*Termin. relación corresp.*) → Comienzo

- terminar máquina de estados establecimiento de correspondencia de SA.

3-B Espera de relación de correspondencia (*Respuesta relación corresp.*) → Correspondencia establecida

- detener temporizador de reintentos de petición de relación de correspondencia (Map).

4-B Espera de relación de correspondencia (*Rechazo relación corresp.*) → Comienzo

- detener temporizador de reintentos de petición de relación de correspondencia (Map);
- terminar máquina de estados establecimiento de correspondencia de SA.

5-B Espera de relación de correspondencia (*Temporización*) → Espera de relación de correspondencia

- enviar petición de relación de correspondencia;
- fijar temporizador de reintentos de petición de relación de correspondencia a temporización de espera de relación de correspondencia de SA;
- incrementar contador de reintentos de relación de correspondencia;
- si contador de reintentos de relación de correspondencia > reintentos máximos de relación de correspondencia de SA, generar evento reintentos máximos.

6-B Espera de relación de correspondencia (*Reintentos máx.*) → Comienzo

- terminar máquina de estados establecimiento de correspondencia de SA.

B.O.8.4 Tráfico de multidifusión IP y SA dinámicas

La Recomendación J.112 anexo B especifica las reglas para la gestión del tráfico IGMP en el CM y el CMTS. Dichas reglas se han concebido con miras a controlar el flujo de tráfico de multidifusión IP a través de la red de cable y a través de la interfaz CM/CPE de tal manera que:

- un CMTS sólo reenvíe tráfico en sentido descendente asociado con un grupo de multidifusión IP si un dispositivo CPE, conectado a uno de los CM clientes del CMTS, es miembro de ese grupo, y
- un CM sólo reenvíe, a través de su interfaz CPE, tráfico en sentido descendente asociado con un grupo de multidifusión IP si un dispositivo CPE conectado es miembro de ese grupo.

BPI+, funcionando en combinación con la interfaz RFI de la Recomendación J.112 anexo B, controla el acceso a los flujos de tráfico de multidifusión IP criptándolos y controlando la distribución del material de aplicación de claves de multidifusión requerido para descriptar los flujos.

Un CMTS puede establecer la correspondencia entre flujos de multidifusión en sentido ascendente y cualquiera de las tres clases de asociaciones de seguridad de BIP+: primaria, estática o dinámica. Si se establece la correspondencia entre el tráfico de un grupo de multidifusión IP y una SA primaria, sólo el único CM perteneciente a esa SA puede acceder a ese grupo. Si se establece la correspondencia con una SA estática o dinámica, múltiples CM pueden acceder a ese grupo, si bien un CMTS puede limitar una SA estática o dinámica a un solo CM.

Cuando un CM conforme a la Recomendación J.112 anexo B habilita el reenvío en sentido descendente de un grupo de multidifusión IP (en respuesta a la recepción de un informe de pertenencia como miembro en su interfaz CPE), el CM DEBE determinar si el tráfico en sentido ascendente del grupo de multidifusión IP está criptado y el SAID de BPI+ está asociado con el flujo de multidifusión criptado en sentido descendente. Una vez que el CM tiene el SAID asociado, puede activar el funcionamiento de una máquina de estados TEK para recuperar el material de aplicación de claves de la SA.

El CM utiliza el mecanismo de establecimiento de correspondencia de SA de BPI+ para pedir a su CMTS el establecimiento de la correspondencia de la SA para un grupo de multidifusión IP al que acaba de unirse. El evento relación de correspondencia de la máquina de estados establecimiento de correspondencia de SA se activa por la habilitación del reenvío de RF a CPE del grupo de multidifusión IP en el CM. Una respuesta de relación de correspondencia de SA informa al CM de que se ha establecido la correspondencia entre el grupo al que se ha unido y una SA de BPI+. Si se establece la correspondencia entre el grupo y la SA primaria del CM, el CM ya tiene el material de aplicación de claves requerido. Si se establece la correspondencia entre el grupo y una SA estática o

dinámica, el CM determina si ya está utilizando una máquina de estados TEK para esa SA; en caso negativo, arranca una.

La máquina de estados establecimiento de correspondencia de SA define un evento terminación de relación de correspondencia OPCIONAL que termina la máquina de estados establecimiento de correspondencia de SA y PUEDE ser utilizado para indicar al CM que ya no necesita el material de aplicación de claves de la SA cuya correspondencia se ha establecido. En caso de establecimiento de correspondencia entre tráfico de multidifusión IP y una SA, el evento terminación de relación de correspondencia podría indicar que el CM ha eliminado todos los filtros de permiso de multidifusión IP asociados con grupos de multidifusión IP cuya correspondencia con la SA en cuestión se ha establecido. Así pues, la máquina de estados establecimiento de correspondencia SA PUEDE ser utilizada para rastrear la necesidad de un CM de mantener material de aplicación de claves para una SA dinámica a la que se ha hecho corresponder con uno o más grupos de multidifusión IP.

Las máquinas de estados TEK correspondientes a SAID primarios y estáticos se paran de acuerdo con las condiciones de terminación definidas en las máquinas de estados autorización y TEK.

B.O.9 Utilización de claves

B.O.9.1 CMTS

Tras completar el registro MAC, el CM inicia un intercambio de autorización con su CMTS. La primera recepción por el CMTS de un mensaje petición de autorización procedente del CM no autorizado inicia la activación de una nueva clave de autorización (AK, *authorization key*), que el CMTS envía al CM solicitante en un mensaje respuesta de autorización. Esta AK permanecerá activa hasta que prescriba de acuerdo con su tiempo de vida predefinido, el *tiempo de vida de clave de autorización*, que es un parámetro de la configuración del sistema CMTS (véase B.O.A.2).

El CMTS DEBE utilizar material de aplicación de claves obtenido a partir de la clave de autorización del CM para:

- verificar el compendio de HMAC en peticiones de clave recibidas de ese CM,
- criptar (DES triple de dos claves modo EDE) la TEK en las respuestas de clave que envíe al CM (TEK es un subatributo del atributo parámetros de TEK de una respuesta de clave),
- calcular el compendio de HMAC que escribe en los mensajes respuesta de clave, rechazo de clave y TEK no válida que envía al CM.

El CMTS debe estar siempre preparado para enviar una AK a un CM cuando se le pida. EL CMTS DEBE poder soportar hasta dos AK activas simultáneamente para cada CM cliente. El CMTS tiene dos AK activas durante el periodo de transición de clave de autorización; las dos claves activas tienen unos tiempos de vida que se superponen.

El periodo de transición de una clave de autorización empieza cuando el CMTS recibe una petición de autorización procedente de un CM y sólo tiene una AK activa para ese CM. En respuesta a la petición de autorización, el CMTS activa una segunda AK, que envía al CM solicitante en una respuesta de autorización. El CMTS DEBE fijar el tiempo de vida activa de esta segunda AK de modo que sea el tiempo de vida activa restante de la primera AK, más el *tiempo de vida de clave de autorización* predefinida; de este modo, la segunda clave, la "más reciente", permanecerá activa durante un periodo de *tiempo de vida activa de clave de autorización*, tras la prescripción de la primera, la clave "más antigua". El periodo de transición de clave finalizará al prescribir la clave más antigua. Esto es lo que se describe en la mitad superior de la figura B.O.9-1.

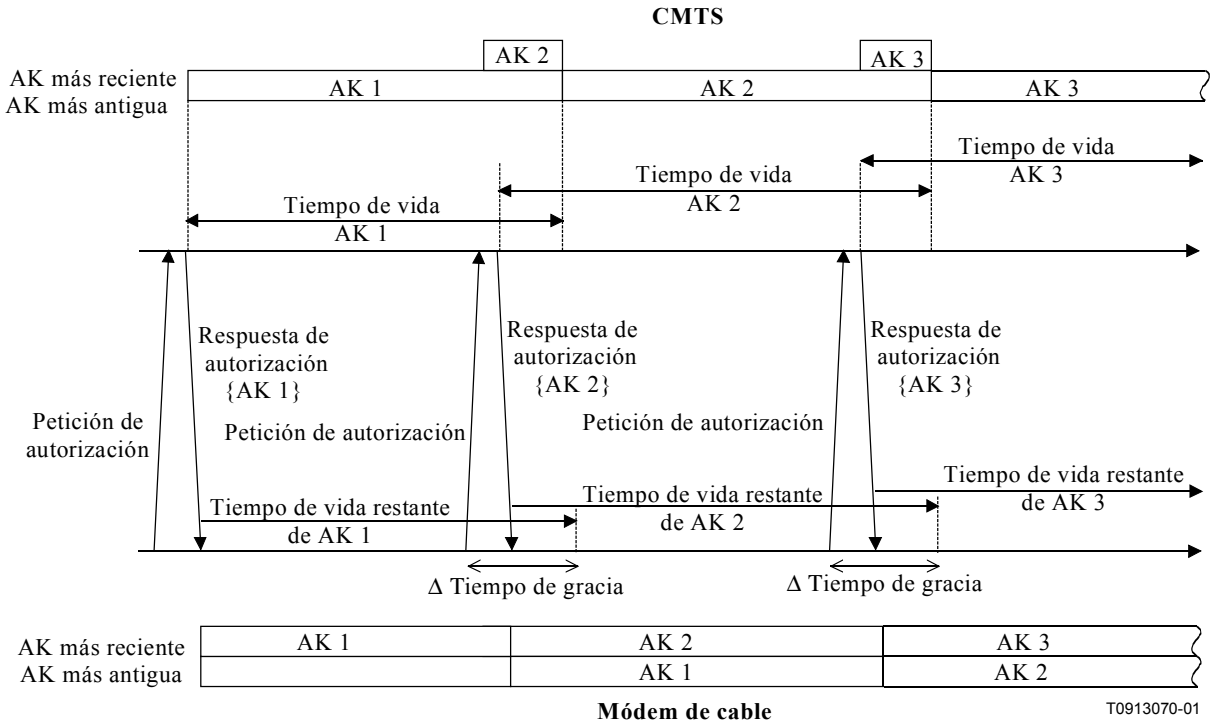


Figura B.O.9-1/J.112 – Gestión de clave de autorización en CMTS y CM

El tiempo de vida de la clave de autorización que un CMTS notifica en una respuesta de autorización DEBE reflejar, de manera tan precisa como permita la implementación, los tiempos de vida restantes de las AK en el momento en que se envía el mensaje de respuesta.

Mientras el CMTS esté en medio del periodo de transición de clave de autorización de un CM, y esté reteniendo por tanto dos claves de autorización activas para ese CM, responderá a las peticiones de autorización con la más reciente de las dos claves activas. Una vez que prescriba la clave más antigua, una petición de autorización provocará la activación de una AK nueva, y el comienzo de un nuevo periodo de transición de clave.

Si la reautorización de un CM no se produce antes de que prescriba su AK más reciente, el CMTS retendrá claves de autorización no activas para ese CM y considerará al CM *no autorizado*. Un CMTS DEBE retirar de sus cuadros de claves todas las TEK asociadas con la SA primaria de un CM no autorizado.

Un CMTS DEBE utilizar la clave o las claves de autorización activas de un CM para verificar el compendio de HMAC en las peticiones de clave recibidas del CM. Si un CMTS recibe una petición de clave durante un periodo de transición de AK, y el número de secuencia de clave de la AK acompañante indica que la petición fue autenticada con la más reciente de las dos AK, el CMTS identifica esto como un *reconocimiento implícito* de que el CM ha obtenido la más reciente de las dos AK activas.

Un CMTS DEBE utilizar una AK activa cuando calcule compendios de HMAC en mensajes respuesta de clave, rechazo de clave y TEK no válida, y cuando cripte la TEK en mensajes respuesta de clave. Cuando envíe mensajes respuesta de clave, rechazo de clave o TEK no válida dentro de un periodo de transición de clave (es decir, cuando estén disponibles dos AK activas), si se ha acusado recibo implícitamente de la clave más reciente, el CMTS DEBE utilizar la más reciente de las dos AK activas; si no se ha acusado recibo de la clave más reciente, el CMTS DEBE utilizar la más antigua de las dos AK activas.

La mitad superior de la figura B.O.9-1 ilustra la estrategia del CMTS a propósito de su utilización de claves de autorización.

El CMTS DEBE mantener dos conjuntos de claves de criptación de tráfico activas (y sus vectores de inicialización de CBC asociados) por cada SAID. Corresponden a dos generaciones sucesivas de material de aplicación de claves, y sus tiempos de vida se superponen. La TEK más reciente DEBE tener un número de secuencia de clave superior en una unidad (módulo 16) al de la TEK más antigua. Cada TEK pasa a estar activa a mitad del tiempo de vida de su predecesora, y prescribe a mitad del tiempo de vida útil de su sucesora. Una vez concluido el tiempo de vida de una TEK, la TEK pasa a estar inactiva y NO DEBE ser ya utilizada.

El CMTS transita entre las dos TEK activas de manera diferente, dependiendo de si la TEK se utiliza para tráfico en sentido descendente o ascendente. Para cada uno de sus SAID, el CMTS DEBE transitar entre TEK activas de acuerdo con las reglas siguientes:

- El CMTS DEBE utilizar la más antigua de las dos TEK activas para criptar tráfico en sentido descendente. Al prescribir la TEK más antigua, el CMTS DEBE pasar a utilizar inmediatamente la TEK más reciente a efectos de criptación.
- Para descriptar tráfico en sentido ascendente, se define un periodo de transición que empieza una vez que el CMTS ha enviado la TEK más reciente a un CM dentro de un mensaje respuesta de clave. El periodo de transición en sentido ascendente empieza a partir del momento en que el CMTS envía la TEK más reciente en un mensaje respuesta de clave y concluye una vez que prescribe la TEK más antigua. Durante el periodo de transición, el CMTS DEBE ser capaz de descriptar tramas en sentido ascendente utilizando cualquiera de las TEK, la más antigua o la más reciente.

Se señala que el CMTS cripta con una TEK determinada sólo durante la segunda mitad del tiempo de vida total de esa TEK. El CMTS puede, no obstante, descriptar con una TEK durante todo el tiempo de vida de la misma.

El campo KEY_SEQ del elemento EH de privacidad básica identifica con cuál de las dos TEK se criptan los datos por paquetes de la trama en sentido ascendente. El bit BASCULAR del elemento EH de privacidad, que es igual al bit menos significativo del campo KEY_SEQ, puede ser utilizado por el CMTS para identificar la TEK con la que se ha criptado.

La mitad superior de la figura B.O.9-2 ilustra la gestión que este CMTS lleva a cabo de las TEK de una asociación de seguridad de BPI+.

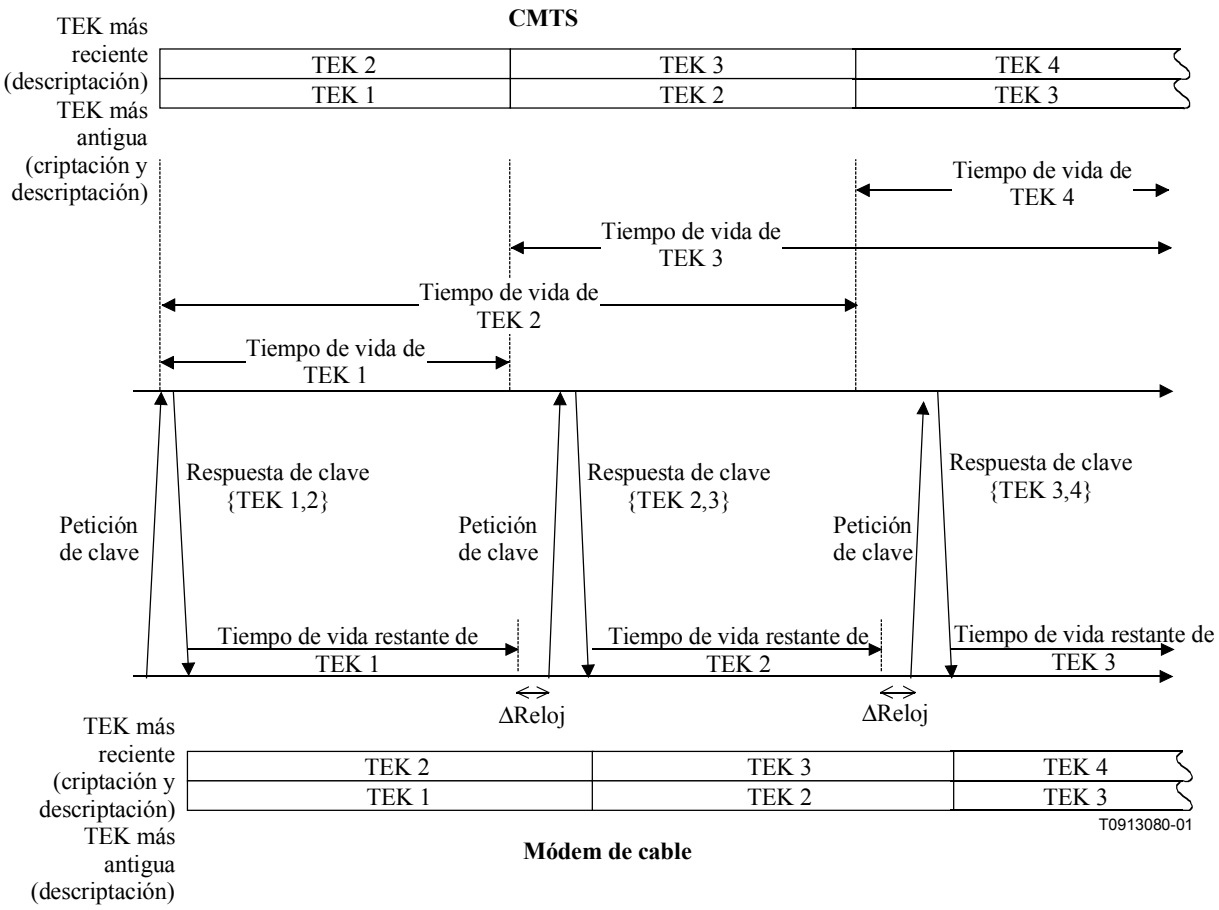


Figura B.O.9-2/J.112 – Gestión de TEK en CMTS y CM

El CMTS se encarga del mantenimiento de la información de aplicación de claves tanto para los SAID primarios como para los SAID de multidifusión de la forma antes indicada. El protocolo de gestión de claves de privacidad básica definido en este anexo B.O describe un mecanismo para sincronización de esa información de aplicación de claves entre un CMTS y sus CM clientes. Corresponde al CM actualizar sus claves de manera puntual; el CMTS transitará a una nueva clave de encriptación en sentido descendente con independencia de si un CM cliente ha recuperado una copia de esa TEK.

Las respuestas de clave enviadas por un CMTS contienen parámetros de TEK (la propia TEK, un tiempo de vida de clave, un número de secuencia de clave y un vector de inicialización de CBC) para las dos TEK activas. Los tiempos de vida de clave de los que informa el CMTS en un mensaje respuesta de clave DEBEN reflejar, de la manera más precisa que permita la implementación, los tiempos de vida restantes de esas TEK y el momento en que se envía el mensaje respuesta de clave.

B.O.9.2 Módem de cable

El CM se encarga de mantener la autorización recibida de su CMTS y de mantener una clave de autorización activa. Un CM DEBE estar preparado para utilizar sus dos AK obtenidas más recientemente.

Las claves de autorización (AK) tienen un tiempo de vida limitado y han de ser renovadas periódicamente. Un CM renueva su clave de autorización reenviando una petición de autorización dirigida al CMTS. La máquina de estados autorización (B.O.7.1.2) gestiona la programación de las peticiones de autorización para renovar las AK.

La máquina de estados autorización de un CM programa el comienzo de una reautorización con un plazo de tiempo configurable (el tiempo de gracia de autorización) antes de que prescriba según lo previsto la AK más reciente del CM. El tiempo de gracia de autorización se configura de forma que el CM disponga de un periodo de reintentos de autorización suficientemente largo, en previsión de los posibles retardos del sistema, y que disponga asimismo de un plazo de tiempo adecuado para completar de manera satisfactoria el intercambio de autorización antes de que prescriba su AK más reciente.

Se señala que el CMTS no precisa conocer el tiempo de gracia de autorización. El CMTS, no obstante, sigue atentamente el tiempo de vida de las claves de autorización y DEBE desactivarlas una vez que hayan prescrito.

Un módem de cable DEBE utilizar la más nueva de sus dos claves de autorización más recientes cuando calcule los compendios de HMAC que adjunta a las peticiones de clave. DEBE poder utilizar cualquiera de las dos AK más recientes para autenticar mensajes respuesta de clave, rechazo de clave o TEK no válida, y descriptar la TEK criptada de un mensaje respuesta de clave. El CM utiliza el número de secuencia de clave de AK acompañante para determinar cuál de las dos AK utiliza.

La mitad inferior de la figura B.O.9-1 ilustra el mantenimiento y la utilización por parte de un CM de sus claves de autorización.

Un CM DEBE poder mantener dos conjuntos sucesivos de material de aplicación de claves de tráfico por cada SAID autorizado. Con el funcionamiento de sus máquinas de estados TEK, el CM trata de mantener siempre los dos conjuntos más recientes de material de aplicación de claves de tráfico de un SAID.

Para cada uno de sus SAID autorizados, el módem de cable:

- DEBE utilizar la más reciente de sus TEK para criptar tráfico en sentido ascendente recién recibido. El tráfico ya puesto en cola de espera PUEDE utilizar cualquiera de las TEK (sin orden específico) durante un breve periodo de tiempo que abarque la transición de la clave antigua a la clave nueva.
- DEBE poder descriptar tráfico en sentido descendente criptado con cualquiera de las TEK.

El campo KEY_SEQ del elemento EH de privacidad básica identifica el número de secuencia de clave de la TEK utilizada para criptar los datos por paquetes de una PDU. El bit BASCULAR del elemento EH de privacidad, que es igual al bit menos significativo del campo KEY_SEQ, sirve para distinguir entre dos generaciones de claves sucesivas.

B.O.9.3 Autenticación de peticiones de servicio dinámico de la Recomendación J.112 anexo B

Si un CM conforme a la Recomendación J.112 anexo B se configura para utilizar BPI+, la interfaz RFI de dicho anexo requiere que el CM y el CMTS incluyan compendios de HMAC en todas las peticiones de adición de servicio dinámico (DSA-REQ), peticiones de cambio de servicio dinámico (DSC-REQ) y peticiones de supresión de servicio dinámico (DSD-REQ) que se envíen el uno al otro.

Esos compendios de HMAC de servicio dinámico se manipulan con claves de autenticación de mensajes de BPI+, es decir, las claves de autenticación de mensajes obtenidas a partir de la clave de autorización de BPI+. Los CM y los CMTS DEBEN utilizar las claves de autenticación de mensajes vigentes cuando generen y validen los compendios de HMAC contenidos en peticiones de servicio dinámico.

B.O.10 Métodos criptográficos

Esta cláusula especifica los algoritmos criptográficos y los tamaños de clave que utiliza BPI+.

B.O.10.1 Criptación de datos por paquetes

La privacidad básica plus DEBE utilizar el modo encadenamiento de bloques cifrados (CBC) del algoritmo norma de criptación de datos (DES) de Estados Unidos [FIPS 46, FIPS 46-1, FIPS 74, FIPS 81] para criptar las tramas PDU datos por paquetes de MAC de RF del campo datos por paquetes y los campos cabida útil de fragmentación y CRC de fragmentación de las tramas de fragmentación MAC.

Las implementaciones BPI+ que utilizan soporte físico conforme a la Recomendación J.112 anexo B (la configuración soporte físico/soporte lógico predominante) DEBEN soportar tanto la clave DES de 40 bits como la clave DES de 56 bits. El funcionamiento con DES de 56 bits se RECOMIENDA ENCARECIDAMENTE.

BPI+ soporta la clave DES de 40 bits sobre todo para hacer posible la interoperabilidad con un soporte físico de la versión inicial de ese anexo, a 40 bits, perfeccionado para utilizar BPI+. La clave DES de 40 bits es idéntica a la de 56 bits, con la salvedad de que 16 bits de la clave DES de 56 bits se fijan a valores fijos y conocidos. Un CM o CMTS que utilice DES de 40 bits DEBE enmascarar (a cero) los 16 bits situados más a la izquierda de cualquier clave DES de 56 bits antes de ejecutar las operaciones de criptación/descriptación. Se señala que los bits enmascarados son los 16 bits situados más a la izquierda que estarían presentes DESPUÉS de eliminar todos los bits octavos de la TEK de 64 bits (es decir, los llamados bits de paridad). El soporte físico conforme a la Recomendación J.112 anexo B v2 de aquel anexo y el conforme Recomendación J.112 anexo B v1 a 56 bits que utilice BPI+ PUEDEN implementar el enmascaramiento de la clave DES de 40 bits en el soporte lógico.

El CBC DEBE ser inicializado con un vector de inicialización proporcionado, junto con otro material de aplicación de cables de SAID, en la respuesta de clave de un CMTS. El encadenamiento se lleva a cabo de bloque a bloque dentro de una trama y se reinicializa trama por trama para que el sistema sea más robusto frente a posibles pérdidas de tramas.

Se DEBE utilizar el procesamiento de bloques de terminación residuales para criptar el bloque final del texto en claro cuando tenga menos de 64 bits. Dado un bloque final con n bits, siendo n inferior a 64, el penúltimo bloque de texto cifrado se cripta de acuerdo con DES una segunda vez, utilizando el modo ECB, y a los n bits menos significativos del resultado se les aplica un operador lógico OR exclusivo con los n bits finales de la cabida útil para generar el bloque de texto cifrado final corto. Para que el receptor descripte este último bloque, la clave DES del receptor encripta el penúltimo bloque de texto cifrado, utilizando el modo ECB, y se aplican operadores lógicos OR exclusivos a los n bits situados más a la izquierda con el bloque de texto cifrado final corto para recuperar el bloque de texto en claro final corto. El procedimiento de criptación se describe en la figura 9.4 de [SCHNEIER].

En el caso especial de que el texto en claro de la trama que ha de ser criptado sea inferior a 64 bits, el vector de inicialización DEBE ser criptado de acuerdo con DES, y a los n bits situados más a la izquierda del texto cifrado resultante, correspondientes al número de bits de la cabida útil, se les DEBE aplicar el operador lógico OR exclusivo con los n bits de la cabida útil para generar el bloque de texto cifrado corto[7].

---

[7] Este método de criptación de cabidas útiles cortas es susceptible de sufrir agresiones: la aplicación del operador lógico OR exclusivo a dos conjuntos de texto cifrado criptado de la manera anterior con el mismo conjunto de material de aplicación de claves dará como resultado el OR exclusivo de los conjuntos correspondientes de texto en claro. En el caso de tramas PDU datos por paquetes, sin embargo, esta cuestión no se plantea porque todas las tramas que lleven datos de usuario protegidos contendrán por lo menos 20 bytes de encabezamiento IP. En el caso de tramas de fragmentación, es posible una trama corta que lleve menos de 8 bytes (64 bits) de texto cifrado; no obstante, los cuatro bytes finales serían la CRC de fragmentación criptada, y los tres o menos bytes antes de la CRC de fragmentación criptada serían la CRC de datos por paquetes criptada.

B.O.10.2 Criptación de TEK

El CMTS cripta el campo valor de TEK de los mensajes respuesta de clave que envía a los CM clientes. Este campo se cripta utilizando DES triple de dos claves en el modo criptación-descriptación-criptación (EDE) [SCHNEIER]:

criptación: $C = E_{k1}[Dk_2[E_{k1}[P]]]$

descriptación: $P = Dk_1[Ek_2[D_{k1}[C]]]$

P = TEK de 64 bits de texto en claro

C = TEK de 64 bits de texto cifrado

k1 = los 64 bits situados más a la izquierda de la KEK de 128 bits

k2 = los 64 bits situados más a la derecha de la KEK de 128 bits

E[ ] = criptación según el modo ECB (libro de códigos electrónicos) de DES de 56 bits

D[ ] = descriptación ECB de DES de 56 bits

En la cláusula B.O.10.4 se describe la manera de obtener la KEK a partir de la clave de autorización.

B.O.10.3 Algoritmo compendio de HMAC

El troceo con clave empleado por el atributo compendio de HMAC DEBE utilizar el método de autenticación de mensajes HMAC [RFC 2104] con el algoritmo de troceo SHA-1 [FIPS 180-1].

Las claves de autenticación de mensajes en sentido ascendente y en sentido descendente se obtienen a partir de la clave de autorización (para los detalles, véase B.O.10.4).

B.O.10.4 Obtención de las TEK, las KEK y las claves de autenticación de mensajes

El CMTS genera claves de autenticación, TEK (claves de criptación de tráfico) e IV (vectores de inicialización). Se DEBE utilizar un generador de números aleatorios o seudoaleatorios para generar claves de autorización y TEK. También se PUEDE utilizar un generador aleatorio o seudoaleatorio para generar vectores de inicialización; con independencia de cómo se generan, los IV DEBEN ser impredecibles. [RFC 1750] contiene prácticas recomendadas para la generación de números aleatorios a utilizar en los sistemas criptográficos.

[FIPS 81] define claves DES como cantidades de 8 octetos (64 bits) en las que los siete bits más significativos (es decir, los siete bits situados más a la izquierda) de cada octeto son los bits independientes de una clave DES, y el bit menos significativo (es decir, el bit situado más a la derecha) de cada octeto es un bit de paridad que se calcula teniendo en cuenta los siete bits independientes precedentes y se ajusta de manera que el octeto tenga paridad impar.

El material de aplicación de claves para DES triple de dos claves consta de dos claves DES diferentes (únicas).

BPKM no requiere paridad impar. El protocolo BPKM genera y distribuye claves DES de 8 octetos de paridad arbitraria, y precisa que las implementaciones ignoren el valor del bit menos significativo de cada octeto.

De una clave de autorización común se obtienen una clave de criptación de claves (KEK) y dos claves de autenticación de mensajes. A continuación se expone la manera de obtener estas claves:

KEK es la clave de criptación de claves utilizada para criptar claves de criptación de tráfico.

HMAC_KEY_U es la clave de autenticación de mensajes utilizada en mensajes, petición de clave en sentido ascendente.

HMAC_KEY_D es la clave de autenticación de mensajes utilizada en mensajes respuesta de clave, rechazo de clave y TEK no válida.

SHA(x|y) denota el resultado de aplicar la función SHA a las cadenas de bits concatenados x e y.

Truncate(x,n) denota el resultado de truncar x a sus n bits situados más a la izquierda.

```
KEK = Truncate(SHA( K_PAD | AUTH_KEY ), 128)

HMAC_KEY_U = SHA( H_PAD_U | AUTH_KEY )

HMAC_KEY_D = SHA( H_PAD_D | AUTH_KEY )
```

Cada_PAD_ es una cadena de 512 bits:

```
K_PAD = 0x53 repetido 64 veces.

H_PAD_U = 0x5C repetido 64 veces.

H_PAD_D = 0x3A repetido 64 veces.
```

B.O.10.5 Criptación de clave de autorización con clave pública

Las claves de autorización de los mensajes respuesta de autorización DEBEN ser criptadas con una clave pública RSA, utilizando la clave pública del módem de cable. BPI+ utiliza F4 (65537 decimal, o de manera equivalente, 010001 hexadecimal) como su exponente público y una longitud de módulo de 1024 bits. BPI+ emplea el esquema de encriptación RSAES-OAEP especificado en la versión 2.0 de la norma PKCS #1 [RSA 2]. El esquema RSAES-OAEP requiere la selección de una función de troceo, una función de generación de máscaras y una cadena de parámetros de codificación. Cuando se cripta la clave de autorización se DEBEN utilizar las selecciones por defecto especificadas en [RSA 2]. Dichas selecciones por defecto son: SHA-1 para la función de troceo, MGF1 con SHA-1 para la función de generación de máscaras y cadena vacía para la cadena de parámetros de codificación.

B.O.10.6 Signaturas digitales

BPI+ emplea el algoritmo signatura RSA [RSA 2] con SHA-1 [FIPS186] para sus tres tipos de certificado.

Al igual que con sus claves de criptación RSA, BPI+ utiliza F4 (65537 decimal, 010001 hexadecimal) como exponente público para su operación de firma. La CA raíz empleará una longitud de módulo de 2048 bits (256 octetos) para firmar los certificados de CA de fabricante que expide. Las CA de fabricante DEBEN emplear longitudes de módulo de clave de signatura de al menos 1024 bits, y no superiores a 2048 bits.

B.O.10.7 Soporte de algoritmos alternativos

La especificación actual relativa a BPI+ requiere la utilización de DES de 56 bits para criptar datos por paquetes, DES triple de dos claves para encriptar claves de encriptación de tráfico, RSA de 1024 bits para criptar claves de autorización y RSA de 1024 a 2048 bits para firmar certificados X.509 de BPI+. Las longitudes de clave y los algoritmos elegidos, si bien parecen apropiados para los tipos de amenazas y las capacidades de los soportes lógicos que se consideran actualmente, pueden ser inadecuados en el futuro.

Existe, por ejemplo, un consenso general en el sentido de que DES se está acercando al final de su utilidad práctica en tanto que norma industrial para la criptación simétrica. NIST contempla actualmente el desarrollo y la adopción de un nuevo algoritmo de criptación normalizado, al que se hace referencia habitualmente como norma de criptación avanzada, o AES (*advanced encryption standard*). Dada la naturaleza de los servicios de seguridad cuyo soporte se demanda a BPI+ (privacidad básica a un nivel superior o igual al posible con conductores especializados, y acceso condicional a los servicios de transporte de datos RF) así como la política de gestión de claves de manera flexible del protocolo (es decir, fijación del tiempo de vida de las claves), los proveedores de servicios basados en la Recomendación J.112 anexo B tendrán motivos para seguir confiando en DES durante, por lo menos, los cinco próximos años. No obstante, en algún momento futuro, los

módems de cable de la Recomendación J.112 anexo B habrán de adoptar un algoritmo de encriptación de tráfico más potente, posiblemente el AES.

La adopción de un algoritmo nuevo para la criptación de datos por paquetes no exigirá el rediseño de BPI+. La utilización coherente del protocolo de codificación de tipo/longitud/valor de los atributos BPKM, los elementos encabezamiento ampliado de encabezamiento MAC y la selección de capacidades de seguridad en el intercambio de autorización garantiza la posibilidad de ampliar el protocolo BPI+. De hecho, los cambios que se introduzcan en cualquier algoritmo criptográfico de BPI+, o las longitudes de claves asociadas, no repercutirán en forma alguna en la estructura general ni en el funcionamiento del protocolo.

B.O.11 Protección física de claves en el CM y el CMTS

BPI+ requiere que los CM y los CMTS mantengan las claves de encriptación de tráfico y las claves de autorización de CM en su memoria. Un CM DEBE mantener también en memoria permanente, no borrable, un par de claves RSA. Tanto los CM como los CMTS DEBEN impedir el acceso físico no autorizado a este material de aplicación de claves.

El nivel de protección física del material de aplicación de claves que BPI+ exige de los CM y los CMTS se especifica en términos de los niveles de seguridad definidos en FIPS PUBS 140-1 y los requisitos de seguridad para módulos criptográficos de la norma [FIPS 140-1]. En particular, los CM y los CMTS DEBEN satisfacer los requisitos del nivel 1 de seguridad de FIPS PUBS 140-1.

El nivel de seguridad 1 de FIPS PUBS 140-1 exige una protección física mínima mediante la utilización de recintos con calidad de producción. Para los requisitos formales, el lector deberá acudir al documento FIPS PUBS; no obstante, a continuación se da un resumen de esos requisitos.

De acuerdo con la clasificación FIPS PUBS 140-1 de las "materializaciones físicas" de los módulos criptográficos, los CMTS y los CM externos son *módulos criptográficos autónomos de múltiples microplaquetas*. FIPS PUBS 140-1 especifica los requisitos siguientes del nivel 1 de seguridad para módulos autónomos de múltiples microplaquetas:

- Las microplaquetas deberán tener calidad de producción, lo que incluye técnicas de pasivación estándar (es decir, aplicación de una pintura sellante sobre la circuitería de las microplaquetas para protegerla contra el deterioro debido al medio ambiente y daños físicos de otro tipo).
- La circuitería deberá implementarse dentro del módulo como una agrupación de múltiples microplaquetas de calidad de producción (es decir, una placa de circuitos impresos integrados, un sustrato cerámico, etc.).
- El módulo deberá estar contenido por completo dentro de un recinto de calidad de producción, metálico o de plástico duro, que puede tener puertas o tapas desmontables.

B.O.12 Perfil y gestión de certificados X.509 de BPI+

BPI+ deberá emplear certificados digitales de la versión 3 de la Recomendación X.509 para autenticar intercambios de clave entre CM y CMTS. La Recomendación X.509 es una norma de uso general; el perfil del certificado de BPI+, que aquí se describe, especifica además el contenido de los campos definidos del certificado. El perfil del certificado define también la jerarquía de confianza establecida para la gestión y validación de certificados BPI+.

Salvo que se indique otra cosa en las cláusulas que siguen, los certificados de BPI+ DEBEN estar en conformidad con las normas PKIX del IETF [RFC 2459]. La utilización de certificados X.509 de la Recomendación J.112 anexo B está, no obstante, mucho más circunscrita que la de PKIX. El perfil del certificado X.509 de la norma PKIX del IETF está orientado al soporte de un mecanismo de distribución de claves, independiente de la aplicación y basado en el certificado, a través de la Internet pública. El perfil del certificado X.509 de la norma PKIX debe admitir una amplia gama de entornos de comunicación, aplicaciones y relaciones de confianza.

Por el contrario, la utilización por parte de BPI+ de certificados digitales se limita a la salvaguarda de los operadores de cable contra la piratería de los servicios de comunicaciones de datos imponiendo un acceso condicional a las claves de criptación de tráfico. Los servicios de comunicaciones protegidos se dividen en tres categorías:

- servicios de datos IP a alta velocidad y del mejor esfuerzo;
- servicios de datos a velocidad primaria constante con recargo; y
- acceso a grupos de multidifusión IP con recargo.

Así pues, si bien el protocolo BPI+ se apoya de manera notable en trabajos realizados respecto al perfil del certificado X.509 de la norma PKIX del IETF, el perfil X.509 de BPI+ se utiliza mucho más.

El perfil del certificado X.509 de BPI+ procede además, en buena medida, de la norma transacción electrónica segura (SET, *secure electronic transaction*) [SET Book 2]. Tanto la organización global de la presente cláusula como parte de su contenido reflejan esa norma.

B.O.12.1 Visión general de la arquitectura de gestión de certificados BPI+

La arquitectura de gestión de certificados BPI+, mostrada en la figura B.O.12-1, consta de una jerarquía de confianza de tres niveles que soporta tres tipos de certificados de la versión 3 de la Recomendación X.509.

- un certificado único, auto-firmado, de la autoridad de certificación (CA) raíz;
- certificados de CA de fabricante;
- certificados de CM.

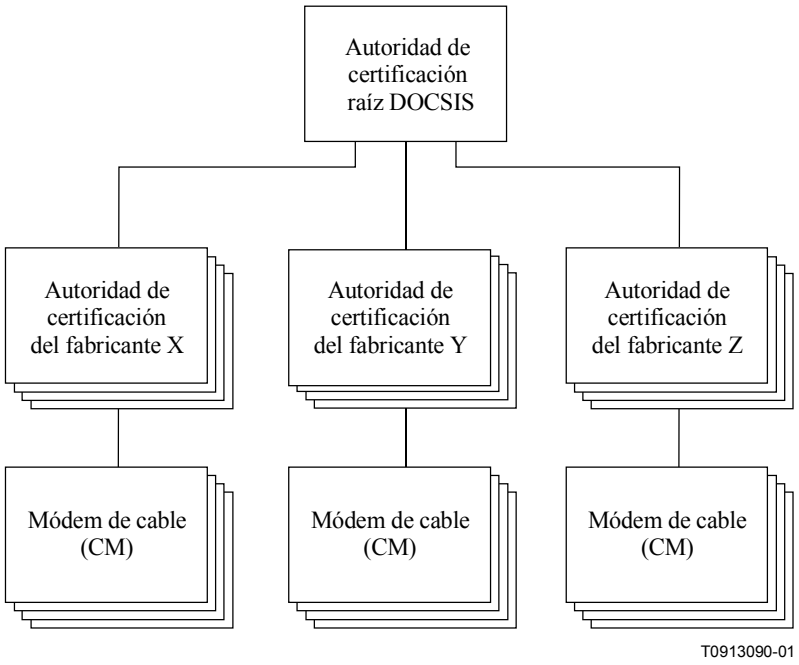


Figura B.O.12-1/J.112 – Arquitectura de gestión de certificados

La autoridad de certificación raíz actúa como la CA raíz. La CA raíz expide certificados a las CA subordinadas mantenidas por los fabricantes. Las CA de los fabricantes expiden certificados a las entidades finales de módem de cable. Se señala que un solo fabricante puede mantener múltiples CA (por ejemplo, una CA diferente por cada planta de fabricación).

La CA raíz deberá mantenerse bajo estrictos controles físicos. Sólo se accederá a ella de vez en cuando para expedir nuevos certificados de CA de fabricante. La organización responsable de la

certificación se encargará del mantenimiento de la CA raíz. La CA raíz generará y distribuirá entre los operadores de cable una lista de revocación de certificados (CRL, *certificate revocation list*) en la que se identifiquen los certificados de fabricante revocados. La manera de distribuir los CRL entre los operadores de cable queda fuera del alcance de la especificación BPI+.

La organización que mantenga la CA raíz deberá definir un protocolo de certificados generados por fabricantes para la CA de fabricante solicitante. La especificación de este protocolo, sin embargo, queda fuera del alcance de la especificación BPI+.

Los fabricantes serán responsables del mantenimiento de su propia CA, desde la que expedirán certificados de CM. Un solo fabricante puede mantener múltiples CA de fabricante. El protocolo para solicitar certificados de una CA de fabricante y distribuir los certificados resultantes entre los módems de cable receptores será un procedimiento interno del fabricante, y queda por tanto fuera del alcance de la especificación de BPI+. Una CA de fabricante PUEDE generar y distribuir listas de revocación de certificados (CRL) entre los operadores de cable; la manera en que se lleva a cabo esa distribución queda fuera del alcance de la especificación de BPI+.

B.O.12.2 Formato de certificado

En esta cláusula se describe el formato del certificado de la versión 3 de la Recomendación X.509 y las extensiones de certificados que se utilizan en BPI+.

El cuadro B.O.12-1 presenta de forma resumida los campos básicos de un certificado versión 3 de X.509.

Cuadro B.O.12-1/J.112 – Campos básicos de un certificado X.509

Campo de versión 3 de X.509	Descripción
tbsCertificate.version	Indica la versión del certificado X.509. Se fija siempre a v3 (valor de 2)
tbsCertificate.serialNumber	Entero único que la CA expedidora asigna al certificado
tbsCertificate.signature	OID y parámetros opcionales que definen el algoritmo utilizado para firmar el certificado. Este campo DEBE contener el mismo identificador de algoritmo que el campo signatureAlgorithm que figura más adelante
tbsCertificate.issuer	Nombre distinguido de la CA que expidió el certificado
tbsCertificate.validity	Especifica cuándo pasa a estar activo el certificado y cuándo prescribe
tbsCertificate.subject	Nombre distinguido que identifica la entidad cuya clave pública se certifica en el campo información de clave pública del asunto
tbsCertificate .subjectPublicKeyInfo	Campo que contiene el material de la clave pública (clave pública y parámetros) y el identificador del algoritmo con el que se utiliza la clave
tbsCertificate .issuerUniqueID	Campo opcional que permite reutilizar nombres de expedidores a lo largo del tiempo
tbsCertificate .subjectUnique ID	Campo opcional que permite reutilizar nombres de asuntos a lo largo del tiempo
tbsCertificate.extensions	Datos de la extensión
signatureAlgorithm	OID y parámetros opcionales que definen el algoritmo utilizado para firmar el certificado. Este campo DEBE contener el mismo identificador de algoritmo que el campo signatura de tbsCertificate
signatureValue	Signatura digital calculada con el tbsCertificate codificado según las DER de la ASN.1

Todos los certificados y los CRL que se describen en este anexo B.O DEBEN estar firmados con el algoritmo de signatura (firma) RSA utilizando SHA-1 como función de troceo unidireccional. El algoritmo de signatura RSA se describe en PKCS #1 [RSA 1]; SHA-1 se describe en [FIPS 180-1]. Se trata sólo de un ejemplo de cómo BPI+ restringe los valores de los campos básicos del certificado X.509. A continuación se describen todas estas restricciones.

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

Los certificados de módem de cable no serán renovables, y, deben tener por tanto, un periodo de validez superior al tiempo de vida operativa del módem de cable. Un certificado de CA de fabricante DEBE ser válido durante 5 años a partir de la fecha de su expedición y reexpedido cada 2 a 3 años. El certificado de CA raíz debe ser válido durante 30 años a partir de la fecha en que la CA raíz empieza a actuar, y reexpedido antes de que prescriba.

En la presente especificación se supone que el tiempo de vida operativa de un módem de cable no superará los 20 años. El periodo de validez de un certificado de módem de cable DEBE empezar con los datos de fabricación del equipo; el periodo de validez DEBERÍA extenderse durante al menos 20 años a partir de la fecha de fabricación.

Los periodos de validez DEBEN ser codificados como tiempo UTCT (UTCTime). Los valores de tiempo UTCT DEBEN expresarse como tiempo medio de Greenwich (Zulu) y DEBEN incluir los segundos (es decir, los tiempos son YYMMDDHHMMSSZ), incluso cuando el número de segundos sea cero. El campo año (YY) DEBE interpretarse como sigue:

- cuando YY sea superior o igual a 50, el año se interpretará como 19YY;
- cuando YY sea inferior a 50, el año se interpretará como 20YY.

B.O.12.2.2 tbsCertificate.serialNumber

Los números de serie de certificados de módem de cable firmados por un expedidor particular DEBEN ser asignados por el fabricante en orden creciente. Así por ejemplo, si el campo tbsCertificate.validity.notBefore de un certificado es mayor que el campo tbsCertificate.validity.notBefore de otro certificado, el número de serie del primer certificado debe ser superior al número de serie del segundo certificado. El fabricante NO DEBERÍA imponer o asumir una relación entre el número de serie del certificado y el número de serie del módem para el que se expide el certificado.

B.O.12.2.3 tbsCertificate.signature y signatureAlgorithm

Todos los certificados y las CRL que se describen en esta especificación DEBEN ser firmados con el algoritmo de signatura RSA, utilizando SHA-1 como función de troceo unidireccional. El algoritmo de signatura RSA se describe en PKCS #1 [RSA 1]; SHA-1 se describe en [FIPS 180-1].

El ID de objeto (OID, *object ID*) de la ASN.1 utilizado para identificar el algoritmo de signatura "SHA-1 con RSA" es:

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
```

Cuando el OID sha-1WithRSAEncryption aparece dentro del AlgorithmIdentifier (identificador de algoritmo) tipo ASN.1, como es el caso tanto en tbsCertificate.signature como en signatureAlgorithm, el componente parámetros de ese tipo es el tipo NULO de ASN.1.

B.O.12.2.4 tbsCertificate.issuer y tbsCertificate.subject

Los nombres X.509 son SECUENCIAS de RelativeDistinguishedNames (nombres distinguidos relativos), que a su vez son CONJUNTOS de AttributeTypeAndValue (tipo y valor de atributo). AttributeTypeAndValue es una SECUENCIA de un AttributeType (tipo de atributo) (un IDENTIFICADOR DE OBJETO) y un AttributeValue (valor de atributo). El valor del atributo countryName (nombre de país) DEBE ser una PrintableString (cadena imprimible) de 2 caracteres,

tomada de la norma ISO 3166; todos los demás AttributeValues (valores de atributo) DEBEN ser codificados como T.61/TeletexString (cadena de teletexto) o como cadenas de caracteres PrintableString. Se DEBE utilizar la codificación PrintableString si la cadena de caracteres sólo contiene caracteres del conjunto PrintableString. De manera específica:

```
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
'()+,-./:=? y espacio.
```

Se DEBE utilizar la T.61/TeletexString si la cadena de caracteres contiene otros caracteres.

Los OID que se indican a continuación se necesitan para definir nombres de expedidor y asunto en certificados BPI+:

```
id-at OBJECT IDENTIFIER    ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-commonName     OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName    OBJECT IDENTIFIER ::= {id-at 6}
id-at-localityName   OBJECT IDENTIFIER ::= {id-at 7}
id-at-stateOrProvinceName  OBJECT IDENTIFIER ::= {id-at 8}
id-at-organizationName           OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName     OBJECT IDENTIFIER ::= {id-at 11}
```

En las subcláusulas que siguen se describe el formato del campo nombre del asunto de cada tipo de certificado de BPI+. El campo nombre del expedidor de un certificado concuerda con el campo nombre del asunto del certificado que se expide. Cualquier certificado transmitido por un CM en un mensaje información de autorización o petición de autorización DEBE tener campos de nombre que se atengan al formato indicado. Un CMTS PUEDE decidir aceptar certificados que tienen campos de nombre no conformes con el formato indicado.

Por lo general, los certificados X.509 soportan un conjunto no estricto de reglas para determinar si el nombre del expedidor de un certificado concuerda con el nombre del asunto de otro. Las reglas permiten incluso que dos campos de nombre se puedan declarar concordantes incluso si de una comparación binaria de ambos campos no se deduce esa concordancia. [RFC 2459] recomienda que las autoridades certificadoras limiten la codificación de campos de nombre para que una implementación pueda declarar concordancia o discrepancia utilizando una comparación binaria simple, y BPI+ sigue esa recomendación. En consecuencia, el campo tbsCertificate.issuer codificado según las DER de un certificado BPI+ DEBE concordar exactamente con el campo tbsCertificate.subject codificado según las DER del certificado de su expedidor. Una implementación PUEDE comparar un nombre de expedidor con un nombre de asunto efectuando una comparación binaria de los campos tbsCertificate.issuer y tbsCertificate.subject codificadas según las DER.

B.O.12.2.4.1 Certificado raíz

countryName=EE.UU.

organizationName=Especificaciones de la interfaz del servicio de datos por cable

organizationalUnitName=Módems de cable

commonName=Autoridad de certificación raíz del módem de cable según la Recomendación J.112 anexo B.

Los atributos countryName (nombre de país), organizationName (nombre de organización), organizationalUnitName (nombre de unidad organizacional) y commonName (nombre común) DEBEN ser incluidos y DEBEN tener los valores mostrados. Otros valores no están permitidos y NO DEBEN ser incluidos.

B.O.12.2.4.2 Certificado de fabricante

countryName=<país del fabricante>

[stateOrProvinceName=< estado/provincia>]

[localityName=<ciudad>]

organizationName=<nombre de la empresa>

organizationalUnitName= la Recomendación J.112 anexo B

[organizationalUnitName=<ubicación de la fábrica>]

commonName=<nombre de la empresa> autoridad de certificación raíz del módem de cable

Los atributos countryName, organizationName y commonName DEBEN ser incluidos y DEBEN tener los valores mostrados.

El atributo organizationalUnitName que tiene el valor "Recomendación J.112 anexo B" DEBE ser incluido.

El atributo organizationalUnitName que representa la ubicación de la fábrica DEBERÍA ser incluido. Si se incluye, DEBE estar precedido por el atributo organizationalUnitName con el valor "Recomendación J.112 anexo B".

Los atributos stateOrProvinceName (nombre del estado o la provincia) y localityName (nombre de la localidad) PUEDEN ser incluidas.

Otros atributos no están permitidos y NO DEBEN ser incluidos.

B.O.12.2.4.3 Certificado de módem de cable

countryName=<país del fabricante>

organizationName=<nombre de la empresa>

organizationalUnitName=<ubicación de la fábrica>

commonName=<número de serie>

commonName=<dirección MAC>

Para distinguir entre dos commonNames (nombres comunes), el commonName que representa el "número de serie" DEBE preceder al commonName que representa la "dirección MAC". La utilización del campo número de serie está en desuso. Si se utiliza, el número de serie DEBE ser un identificador de módem de cable único, pero PUEDE ser diferente del número de serie codificado en los atributos BPKM. La dirección MAC del certificado de CM DEBE ser la misma que la dirección MAC de los atributos BPKM.

Los caracteres empleados en la representación PrintableString (cadena imprimible) de los números de serie de CM DEBEN estar limitados al subconjunto de caracteres siguiente:

- `A-Z (0x41-0x5A)`
- `a-z (0x61-0x7A)`
- `0-9 (0x30-0x39)`
- `"-" (0x2D)`

La dirección MAC se expresa mediante seis pares de dígitos hexadecimales separados por el signo dos puntos (:), por ejemplo, "00:60:21:A5:0A:23". Los caracteres hexadecimales alfanuméricos (A-F) DEBEN representarse mediante letras mayúsculas.

El organizationalUnitName (nombre de la unidad organizacional) de un certificado de módem de cable, que describe la ubicación del fabricante del módem, DEBERÍA ser el mismo que el organizationalUnitName del nombre del expedidor que describe la ubicación de una fábrica.

Los atributos countryName, organizationName, organizationalUnitName y commonName (dirección MAC) DEBEN ser incluidos. El atributo commonName (número de serie) PUEDE ser incluido. Otros atributos no están permitidos y NO DEBEN ser incluidos.

B.O.12.2.5 tbsCertificate.subjectPublicKeyInfo

El campo tbsCertificate.subjectPublicKeyInfo contiene la clave pública y el identificador del algoritmo de la clave pública. La clave pública RSA del certificado de CM DEBE ser la misma que la clave pública RSA de los atributos BPKM.

El campo tbsCertificate.subjectPublicKeyInfo.algorithm es una estructura AlgorithmIdentifier (identificador de algoritmo). El algoritmo del AlgorithemIdentifier DEBE ser una encriptación RSA, identificada por el siguiente OID:

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
     rsadsi(113549) pkcs(1) 1}
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}
```

El campo de parámetros del AlgorithmIdentifier DEBE tener NULO tipo ASN.1.

La clave pública RSA deberá codificarse utilizando la RSAPublicKey tipo ASN.1:

```
RSAPublicKey ::= SEQUENCE {
      modulus           INTEGER, -- n
      publicExponent    INTEGER, -- e -- }
```

donde modulus es el módulo n, y publicExponent es el exponente público e. La RSAPublicKey (clave pública RSA) codificada según las DER es el valor de la CADENA DE BITS tbsCertificate.subjectPublicKeyInfo.subjectPublicKey.

B.O.12.2.6 tbsCertificate.issuerUniqueID y tbsCertificate.subjectUniqueID

Los campos issuerUniqueID (ID único de expedidor) y subjectUniqueID (ID único de asunto) DEBEN ser omitidos para los tres tipos de certificado BIP+.

B.O.12.2.7 tbsCertificate.extensions

No se exige que los certificados BPI+ incluyan extensión alguna; esto es así incluso si las extensiones son obligatorias según [RFC 2459]. Los certificados de BPI+ PUEDEN incluir las extensiones que se describen en las subcláusulas que siguen. Las extensiones incluidas en certificados BPI+ DEBEN ser conformes a [RFC 2459].

B.O.12.2.7.1 Certificados de módem de cable

Los certificados de módem de cable PUEDEN contener extensiones no críticas; NO DEBEN contener extensiones críticas. Si está presente la extensión KeyUsage (utilización de clave), los bits keyAgreement (acuerdo de clave) y keyEncipherment (cifrado de clave) DEBEN ser activados, los bits keyCertSign (signo de certificado de clave) y cRLSign (signo de CRL) DEBEN ser desactivados, y todos los demás bits DEBERÍAN ser desactivados.

B.O.12.2.7.2 Certificados raíz y de fabricante

Los certificados raíz y de fabricante PUEDEN contener la extensión limitaciones básicas. Si se incluye, la extensión limitaciones básicas PUEDE aparecer como una extensión crítica o como una extensión no crítica.

Los certificados raíz y de fabricante PUEDEN contener extensiones no críticas; NO DEBEN contener extensiones críticas distintas de, quizás, la extensión limitaciones básicas.

Si la extensión KeyUsage está presente en un certificado raíz o de fabricante, se DEBE activar el bit keyCertSign y se DEBERÍAN desactivar todos los demás bits.

B.O.12.2.8 signatureValue

En los tres tipos de certificado de BPI+, el signatureValue (valor de signatura), contiene la signatura (firma) RSA (con SHA-1) calculada en el certificado tbsCertificate codificado según las DER de la ASN.1. Este último certificado se utiliza como entrada en la función signatura RSA. El valor de signatura (firma) resultante se codifica de acuerdo con la ASN.1 como una CADENA DE BITS y se incluye en el campo signatureValue del certificado.

B.O.12.3 Almacenamiento y gestión de certificados de módem de cable en el CM

Los certificados de CM expedidos por los fabricantes DEBEN almacenarse en memoria permanente y no borrable de los CM. Los CM que tienen pares de claves privada/pública RSA instaladas en fábrica DEBEN tener también certificados de CM instalados en fábrica. Los CM que dependen de algoritmos internos para generar un par de claves RSA DEBEN disponer de un mecanismo que permita instalar el certificado de CM expedido por el fabricante tras la generación de las claves.

La clave pública de la autoridad de certificación (CA) raíz (RSA) se DEBE situar en la memoria no volátil del CM. (El CM utiliza la CA raíz para verificar las signaturas digitales incorporadas en los perfeccionamientos del soporte lógico telecargado vía TFTP. En el anexo B.O.B se analiza la utilización de signaturas (firmas) de código para verificar los perfeccionamientos del soporte lógico operativo).

El certificado de CA de la CA del fabricante que firmó el certificado del CM, DEBE ser almacenado en la memoria no volátil del módem de cable. El módem de cable DEBE ser capaz de actualizar o sustituir el certificado de CA del fabricante vía fichero de telecarga de código (véase el anexo B.O.B). El certificado de CA del fabricante PUEDE ser incorporado en el soporte lógico del CM.

Si el certificado de CA del fabricante se incorpora en el soporte lógico del CM, cuando un fabricante expida certificados de CM con múltiples certificados de CA, la memoria del CM deberá incluir TODOS esos certificados de CA de fabricante. El certificado de CA del fabricante específico instalado por el CM (es decir, anunciado en los mensajes información de autenticación y devuelto por el objeto base de información de gestión (MIB), será el que identifique al expedidor del certificado de CM de ese módem.

B.O.12.4 Procesamiento y gestión de certificados en el CMTS

BPKM emplea certificados digitales para permitir a los CMTS verificar la vinculación entre la identidad de un CM (codificado en los nombres del asunto de un certificado digital X.509) y su clave pública. El CMTS hace esto validando el trayecto o la cadena de certificación del certificado del CM. Dicho trayecto constará normalmente de tres certificados encadenados: empezando con el certificado del CM, el trayecto lleva al certificado de la CA del fabricante que expidió el certificado del CM y termina en el certificado auto-firmado de la CA raíz (figura B.O.12-2). Validación de la cadena significa que se verifica la signatura o firma del certificado de la CA del fabricante con la clave pública de la CA raíz y que se verifica a continuación la signatura del certificado del CM con la clave pública de la CA del fabricante.

Figura B.O.12-2/J.112 – Cadena de certificación de CM

BPI+ requiere que los CMTS soporten controles administrativos que permitan al operador anular una validación de cadena de certificación especificando si una CA de fabricante o un certificado de CM puede ser o no fiduciado. Se ha de dar una descripción detallada de esos controles administrativos sobre la gestión de certificados del CMTS en un documento OSS asociado. La presente cláusula especifica el modelo de gestión para el ejercicio de esos controles, así como el proceso que lleva a cabo un CMTS para evaluar la validez de un certificado de CM, y verificar así la vinculación entre la identidad del CM y su clave pública.

B.O.12.4.1 Modelo de gestión de certificados del CMTS

El CMTS mantiene copias de certificados de CA raíz, CA de fabricante y de módem de cable, que obtiene mediante aprovisionamiento o mensajería BPKM. Se DEBE marcar el estado en que se halla cada uno de los certificados de los que el CMTS tiene conocimiento, y que puede ser uno de los cuatro siguientes: no fiduciado, fiduciado, encadenado o raíz. Sólo el certificado de la CA raíz (un certificado auto-firmado que contiene la clave pública fiduciada de la CA raíz) DEBE ser marcado como raíz. Sin embargo, un CMTS PUEDE admitir múltiples certificados de CA raíz. Los certificados raíz DEBEN ser aprovisionados dentro de un CMTS.

Un CMTS tiene conocimiento de los certificados de CA de fabricante a través de la interfaz de aprovisionamiento del CMTS o por la recepción y procesamiento de mensajes información de autenticación de los CM clientes. Con independencia de cómo obtiene un CMTS su certificado de CA de fabricante, el CMTS DEBE marcarlos como no fiduciados, fiduciados o encadenados. Si un certificado de CA de fabricante no está auto-firmado, el CMTS la marca como encadenado. El CMTS, no obstante, DEBE soportar controles administrativos que permitan a un operador anular la marcación de encadenado y especificar que un determinado certificado de CA de fabricante es fiduciado o no fiduciado.

Si un certificado de CA de fabricante está auto-firmado, el CMTS lo marca como fiduciado o no fiduciado, de acuerdo con la política del CMTS controlada administrativamente. Un certificado de CA de fabricante auto-firmado cuya signatura (firma) no pueda ser verificada DEBE ser marcado como no fiduciado. La fiduciación por parte de los CMTS de certificados de CA de fabricante auto-firmados DEBE ser configurable. La fiduciación por defecto de certificados de CA de

fabricante auto-firmados NO SE RECOMIENDA en sistemas operativos comerciales; la fiduciación por defecto debería utilizarse como soporte de la certificación y de otros modos de prueba. El CMTS DEBE marcar el certificado de CM como encadenado a menos que lo invalide el control administrativo del CMTS.

Un CMTS obtiene copias de certificados de módem de cable en las peticiones de autorización que recibe de los CM clientes. Los certificados de módem de cable DEBEN ser expedidos por una autoridad de certificación (CA) de fabricante; así pues, a no ser que los invalide el control administrativo del CMTS, los certificados de CM serán marcados por el CMTS como encadenados. Un operador puede, como parte del proceso de aprovisionamiento del módem, especificar que el certificado de un CM determinado se marque como no fiduciado o fiduciado.

B.O.12.4.2 Validación de certificados

El CMTS valida los trayectos de certificación de CA de fabricante y los certificados de CM aplicando los criterios que se indican a continuación. Se señala que los criterios son iterativos y requieren que un CMTS valide el trayecto de certificación de un certificado de CA de fabricante encadenado antes de que pueda validar el trayecto de certificación de un certificado de CM expedido por esa CA de fabricante.

El CMTS marca los certificados de CA de fabricante y de módem de cable como válidos o no válidos si sus trayectos de certificación son válidos o no válidos, respectivamente. Los certificados fiduciados son válidos, incluso si el momento en que se examinan no está dentro de su periodo de validez. Los certificados no fiduciados no son válidos.

Un certificado encadenado es válido si:

1) el certificado se encadena con un certificado raíz, fiduciado o válido; y
2) la signatura o firma del certificado puede ser verificada con la clave pública del expedidor; y
3) el momento en que se analiza queda dentro del periodo de validez de cada certificado encadenado o raíz dentro de la cadena de certificación (se señala que BPI+ no requiere la superposición de los periodos de validez, es decir, no hace falta que todo el periodo de validez de un certificado quede dentro del periodo de validez de su certificado de emisión); y
4) el certificado no está en una lista actualizada permanentemente (hot lis) de certificados de CM y CA de fabricante (véase B.O.12.4.4);
5) en el caso de un certificado de CM, la dirección MAC del CM codificada en su campo tbsCertificate.subject y la clave pública RSA codificada en su campo tbsCertificate.subjectPublicKeyInfo concuerdan con la dirección MAC del CM y la clave pública RSA codificada en los atributos BPKM de la petición de autorización; y
6) en el caso de un certificado de CM, si la extensión KeyUsage (utilización de clave) está presente, se activan los bits keyAgreement (acuerdo de clave) y keyEncipherment (cifrado de clave) y se desactivan los bits keyCertSign (signo de certificación de clave) y cRLSign (signo de CRL), todos los demás bits DEBERÍAN desactivarse; en el caso de un certificado de CA de fabricante, si está presente la extensión KeyUsage, se activa el bit keyCertSign, todos los demás bits DEBERÍAN desactivarse.

El criterio 3) anterior se tiene en cuenta o se ignora según decida el control administrativo.

Si se HABILITA la comprobación del periodo de validez y el CMTS no ha adquirido la hora del día, se DEBE devolver un mensaje de rechazo de autorización (no permanente) en respuesta a una petición de autorización de estilo BPI+.

Si un certificado encadenado no cumple ninguno de los criterios de validez anteriores, se identifica como no válido.

Si un CMTS marca un certificado de CM como no fiduciado o no válido, el CMTS DEBE rechazar las peticiones de autorización del CM correspondiente.

B.O.12.4.3 Huellas dactilares de un certificado

Las huellas dactilares son funciones de troceo unidireccional resistente a la colisión (por ejemplo SHA-1) de certificados. Representan una manera consistente de identificación de los certificados. Un CMTS PUEDE guardar huellas dactilares de los certificados de CM y CA de fabricante que retiene o que ha validado. Utilizando las huellas dactilares, un CMTS puede guardar en memoria (cache) los resultados de una operación de validación anterior: contrastando la huella dactilar de un certificado recién ofrecido con una huella dactilar guardada en memoria, puede determinar rápidamente la validez del certificado de que se trate.

B.O.12.4.4 Listas de certificados de CA de fabricante y de CM actualizados permanentemente

Cuando el CMTS encadena certificados de validación, no es preciso que compruebe la situación de revocación o no de un certificado (es decir, la presencia o no del certificado en una CRL actualizada). El CMTS, no obstante, DEBE ser capaz de mantener *listas actualizadas permanentemente* de certificados de CA de fabricante y de CM conocidos, no fiduciados. Los certificados de esas listas calientes pueden incluir certificados revocados por sus expedidores; sin embargo, también pueden incluir certificados válidos que la EMPRESA DEL CABLE que explota el CMTS decide marcar como "no fiduciados".

La definición de los procedimientos y protocolos para el mantenimiento de listas calientes de certificados de CA de fabricante y certificados de CM de un CMTS queda fuera del alcance de la especificación BPI+.

ANEXO B.O.A

Extensiones de fichero de configuración TFTP

Todos los valores de parámetros de configuración de privacidad básica de un CM se especifican en el fichero de configuración telecargado vía TFTP por el CM durante la inicialización MAC de RF. Los campos de fijación de la configuración de privacidad básica se incluyen tanto en los cálculos de MIC del CM como de MIC del CMTS, y en las peticiones de registro de un CM. Para el orden en que se incluyen los campos de fijación de configuración de privacidad básica en el compendio MD5 de MIC del CMTS, véase la Recomendación J.112 anexo B.

B.O.A.1 Codificaciones

Las codificaciones de tipo/longitud/valor que siguen para fijaciones de configuración privacidad básica DEBEN ser utilizadas tanto en el fichero de la configuración y en las peticiones de registro de CM MAC de RF. Todas las cantidades multioctectos están en el orden de bytes de la red, es decir, el octeto que contiene los bits más significativo es el primero que se transmite por el cable.

B.O.A.1.1 Fijación de configuración privacidad básica

La fijación de configuración habilitación de privacidad de la RFI 1.1 (Recomendación J.112 anexo B) controla si la privacidad básica está habilitada o inhabilitada en un CM. Si la privacidad básica está habilitada, la fijación de configuración privacidad básica DEBE estar también presente. La fijación de configuración privacidad básica PUEDE estar presente si la privacidad básica está inhabilitada. El parámetro habilitación de privacidad separado permite a un operador inhabilitar o rehabilitar la privacidad básica haciendo bascular el valor de un solo parámetro de la configuración, es decir, sin que sea preciso eliminar o reinsertar el conjunto mayor de parámetros de la configuración privacidad básica.

Este campo define los parámetros asociados con el funcionamiento de la privacidad básica. Se compone de un cierto número de campos tipo/longitud/valor encapsulados. Los campos tipos definidos sólo son válidos dentro de la cadena de fijaciones de la configuración privacidad básica encapsuladas.

Tipo	Longitud	Valor
BP_CFG	n	

El anexo B a la Recomendación J.112 define el valor específico de BP_CFG.

B.O.A.1.1.1 Codificaciones de privacidad básica internas

B.O.A.1.1.1.1 Temporización de espera de autorización

El valor de este campo especifica el intervalo de retransmisión, en segundos, de mensajes petición de autorización desde el estado espera de autorización.

Subtipo	Longitud	Valor
1	4	

Gama válida: 1-30

B.O.A.1.1.1.2 Temporización de espera de reautorización

El valor de este campo especifica el intervalo de retransmisión, en segundos, de mensajes petición de autorización desde el estado espera de autorización.

Subtipo	Longitud	Valor
2	4	

Gama válida: 1-30

B.O.A.1.1.1.3 Tiempo de gracia de autorización

El valor de este campo especifica el periodo de gracia para la reautorización, en segundos.

Subtipo	Longitud	Valor
3	4	

Gama válida: 1-6 047 999

B.O.A.1.1.1.4 Temporización de espera operativa

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de clave desde el estado espera operativa.

Subtipo	Longitud	Valor
4	4	

Gama válida: 1-10

B.O.A.1.1.1.5 Temporización de espera de nueva aplicación de clave

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de clave desde el estado espera de nueva aplicación de clave.

Subtipo	Longitud	Valor
5	4	

Gama válida: 1-10

B.O.A.1.1.1.6 Tiempo de gracia de TEK

El valor de este campo especifica el periodo de gracia, en segundos, de nueva aplicación de la TEK.

Subtipo	Longitud	Valor
6	4	

Gama válida: 1-302 399

B.O.A.1.1.1.7 Temporización de espera de rechazo de autorización

El valor de este campo especifica la duración de la espera, en segundos, de un CM en el estado espera de rechazo de autorización después de recibir un rechazo de autorización.

Tipo	Longitud	Valor
7	4	

Gama válida: 1-600

B.O.A.1.1.1.8 Temporización de espera de relación de correspondencia de SA

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de relación de correspondencia de SA desde el estado espera de establecimiento de correspondencia.

Tipo	Longitud	Valor
8	4	

Gama válida: 1-10

B.O.A.1.1.1.9 Reintentos máximos de relación de correspondencia de SA

El valor de este campo especifica el número máximo de reintentos de petición de relación de correspondencia (Map) permitido.

Tipo	Longitud	Valor
9	4	

Gama válida: 0-10

B.O.A.2 Directrices sobre parámetros

A continuación se dan gamas y valores recomendados para los diversos parámetros de configuración y parámetros operativos de la privacidad básica. Esas gamas y esos valores por defecto pueden cambiar a medida que los proveedores de servicios adquieran experiencia en la aplicación de la privacidad básica.

Cuadro B.O.A-1/J.112 – Gamas operativas recomendadas para parámetros de configuración de BPI

Sistema	Nombre	Descripción	Valor mínimo	Valor por defecto	Valor máximo
CMTS	Tiempo de vida de autorización	Tiempo de vida, en segundos, que el CMTS asigna a una clave de autorización nueva	1 día (86 400 s)	7 días (604 800 s)	70 días (6 048 000 s)
CMTS	Tiempo de vida de TEK	Tiempo de vida, en segundos, que el CMTS asigna a una TEK nueva	30 min (1800 s)	12 horas (43 200 s)	7 días (604 800 s)
CM	Temporización de espera de autorización	Intervalo de retransmisión de petición de autorización desde el estado espera de autorización	2 s	10 s	30 s
CM	Temporización de espera de reautorización	Intervalo de retransmisión de petición de autorización desde el estado espera de reautorización	2 s	10 s	30 s
CM	Tiempo de gracia de autorización	Tiempo de adelanto del comienzo de la reautorización por el CM respecto a la autorización	5 min (300 s)	10 min (600 s)	35 días (3 024 000 s)
CM	Temporización de espera operativa	Intervalo de retransmisión de petición de clave desde el estado espera operativa	1 s	1 s	10 s
CM	Temporización de espera de nueva aplicación de clave	Intervalo de retransmisión de petición de clave desde el estado espera de nueva aplicación de clave	1 s	1 s	10 s
CM	Tiempo de gracia de TEK	Tiempo de adelanto del comienzo de la nueva aplicación de clave por el CM respecto a la prescripción de la TEK	5 min (300 s)	1 hora (3600 s)	3,5 días (302 399 s)
CM	Espera de rechazo de autorización	Plazo de tiempo antes de reenviar una petición de autorización tras recibir un rechazo de autorización	10 s	60 s	10 min (600 s)

Cuadro B.O.A-1/J.112 – Gamas operativas recomendadas para parámetros de configuración de BPI

Sistema	Nombre	Descripción	Valor mínimo	Valor por defecto	Valor máximo
CM	Temporización de espera de relación de correspondencia de SA	Intervalo de retransmisión de petición de relación de correspondencia desde el estado espera de establecimiento de correspondencia	1 s	1 s	10 s
CM	Reintentos máximos de relación de correspondencia de SA	Número máximo de veces que el CM intenta la petición de relación de correspondencia de SA antes de abandonar	0	4	10

La gama válida (frente a la gama operativa recomendada) de tiempos de vida de autorización y TEK es como sigue:

- Gama válida de tiempo de vida de autorización: 1 a 6 048 000 segundos.
- Gama válida de tiempo de vida de TEK: 1 a 604 800 segundos.

Se señala que las gamas válidas definidas para cada uno de los parámetros de la configuración de BPI se extienden por debajo de las gamas operativas recomendadas. A efectos de prueba de protocolos, resulta útil aplicar el protocolo BPI con valores de temporizador muy por debajo del extremo inferior de las gamas operativas recomendadas. Los valores de temporizador más reducidos "aceleran" el reloj de la BPI, provocando la ocurrencia de eventos de máquina de estados de protocolo BPI mucho más rápidamente de lo que sería el caso con una configuración "operativa". Si bien no es preciso diseñar las implementaciones BPI para que funcionen eficazmente a ese ritmo acelerado de BPI, la implementación del protocolo DEBERÍA funcionar de manera correcta con esas temporizaciones más breves. El cuadro B.O.A-2 contiene una lista de valores de parámetros reducidos que probablemente se empleen en pruebas de conformidad de protocolos y certificación.

Cuadro B.O.A-2/J.112 – Valores de parámetros de BPI reducidos para pruebas de protocolos

Tiempo de vida de autorización	5 min (300 s)
Tiempo de vida de TEK	3 min (180 s)
Tiempo de gracia de autorización	1 min (60 s)
Tiempo de gracia de TEK	1 min (60 s)

El tiempo de gracia de TEK DEBE ser inferior a la mitad del tiempo de vida de la TEK.

ANEXO B.O.B

Verificación de soporte lógico operativo telecargado

B.O.B.1 Introducción

El sistema módem de cable soporta la telecarga a distancia de un código en los módems de cable de red. El origen y la integridad del código telecargado son importantes a efectos del funcionamiento y la seguridad globales del sistema de módem de cable.

El módulo de telecarga de soporte lógico constituye un objetivo atractivo para cualquier atacante. Si un atacante fuese capaz de organizar un ataque escalable contra el módulo de telecarga de soporte lógico, podría incluso instalar un código que inhabilitara todos los CM dentro de un dominio, o provocar una perturbación del servicio de gran magnitud. Para impedir esos ataques, habrá que interponer diversas barreras de seguridad entre el atacante y su objetivo.

B.O.B.2 Visión de conjunto

Los requisitos definidos en esta cláusula se refieren a los objetivos de seguridad primaria del proceso de telecarga de códigos:

- El CM deberá tener alguna manera de autenticar que el originador de cualquier código telecargado es una fuente conocida y fiduciada.
- El CM deberá disponer de alguna manera de verificar que el código telecargado no ha sido alterado desde la forma original en la que lo proporcionó la fuente fiduciada.
- El proceso deberá tratar de simplificar los requisitos de manejo de ficheros de código de operador de cable y proporcionar los mecanismos que permitan al operador de cable mejorar o rebajar la categoría de la versión del código de los módems de cable de su red.
- El proceso debe permitir además que un operador de cable tenga la posibilidad de establecer y controlar sus propias políticas de primera mano, con respecto a:
  a) los ficheros de código que serán aceptados por los módems de cable dentro de su dominio de red, y
  b) los controles de seguridad que definen la seguridad del proceso en su red.
- Los módems de cable han de poder desplazarse libremente entre sistemas controlados por diferentes organizaciones de operador de cable.

El presente anexo B.O.B se circunscribe a esos requisitos de seguridad primaria de los sistemas, pero tiene en cuenta que en algunos casos quizás sea conveniente una mayor seguridad. Los recelos de algunos operadores de cable o fabricantes de módems de cable pueden tener como resultado un cierto grado de seguridad adicional en relación con la distribución e instalación de códigos en un módem de cable o en otro elemento de red DOCSIS. La presente especificación no restringe la utilización de otras formas de protección, en tanto no contravengan los objetivos y las directrices que en ella se exponen.

Para proteger y verificar de manera satisfactoria la telecarga de códigos se requieren múltiples niveles de protección.

- El fabricante del código del CM aplica siempre una signatura o firma digital al fichero de código; signatura que es verificada con una cadena de certificación que llega hasta la raíz. La signatura del fabricante autentica la fuente y la integridad del fichero de códigos al CM. En dicho fichero se incluyen parámetros de control adicionales para controlar el acceso al CM.
- Si bien el fabricante debe firmar siempre sus ficheros de código, un operador de cable puede aplicar posteriormente su signatura o firma de código, además de la del fabricante. El CM debe verificar ambas signaturas con una cadena de certificados que llegue hasta la raíz antes de aceptar un fichero de código.
- Los mecanismos OSS de aprovisionamiento y control del CM son de gran importancia para que la ejecución del proceso se lleve a cabo de manera adecuada. La capacidad de mejorar la categoría del código de un CM se habilita durante el proceso de aprovisionamiento y registro. Las telecargas de códigos se inician durante el proceso de aprovisionamiento y registro; o pueden ser iniciadas en funcionamiento normal mediantge una instrucción SNMP.

El fichero de código se construye utilizando una estructura conforme a la norma PKCS #7 que haya sido definida en un formato específico para utilizarla con módems de cable. En la estructura PKCS #7 debe estar incluido lo siguiente:

- La configuración de código: la configuración del código de mejora.
- La signatura de verificación de código (CVS, *code verification signature*): la signatura digital en la configuración del código y cualesquiera otros atributos autenticados definidos en la estructura PKCS #7.
- El certificado de verificación de código (CVC, *code verification certificate*): una estructura de certificado conforme a X.509 que se utiliza para entregar y validar la clave pública de verificación de código que verificará la signatura en la configuración del código. La autoridad de certificación, una parte fiduciada cuya clave pública ya está almacenada en el módem de cable, firma el certificado. El certificado X.509 se define con un formato específico para utilizarlo con módems de cable.

La figura B.O.B-1 muestra los pasos básicos requeridos para la firma de una configuración de código cuando el fichero de código lo firma sólo el fabricante del CM, y cuando el fichero de códigos es firmado por el fabricante del CM y co-firmado por un operador de cable.

En el sistema, cada módem de cable recibirá una clave pública fiduciada de la autoridad de certificación raíz. El fabricante del código elaborará el fichero de código firmando la configuración de código mediante una estructura de signatura digital de la norma PKCS #7 con un certificado X.509. El fichero de código se envía a continuación al operador de cable. El operador de cable, que posee una clave pública raíz, DEBERÍA verificar que el fichero de código procede de un fabricante fiduciado y no ha sido modificado. En este punto, el operador de cable tiene la opción de cargar el fichero de código en el servidor TFTP tal como está, o de añadir su firma y el CVC del operador de cable al fichero de código. Durante el proceso de mejora del código, el CM accederá al fichero de código desde el servidor TFTP y verificará la configuración del código antes de instalarlo.

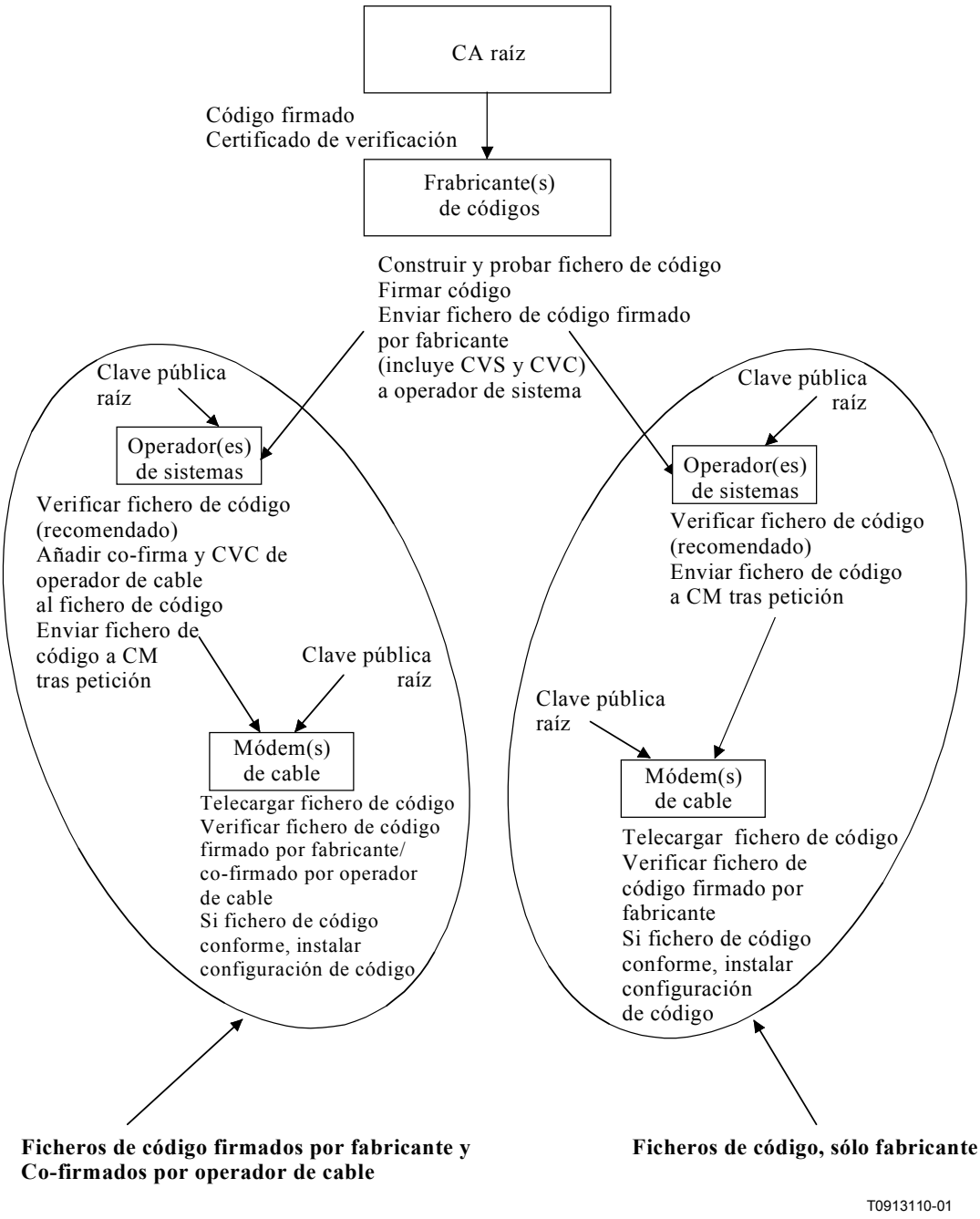


Figura B.O.B-1/J.112 – Jerarquía de validación de código típica

B.O.B.3 Requisitos de mejora de código

En las subcláusulas que siguen se definen los requisitos para el soporte del proceso de verificación de mejora de códigos. Todas las mejoras de código DEBEN ser preparadas y verificadas como se define en la presente especificación. Todos los módem de cable certificados DEBEN verificar las mejoras de código de acuerdo con esta especificación, con independencia de si funcionan o no según un modo conforme a la versión 2 de la Recomendación J.112. Todos los módem de cable certificados conformes a lo prescrito en el anexo B.1.1 a dicha Recomendación DEBEN verificar las mejoras de código de acuerdo con la presente especificación con independencia de si la privacidad básica está habilitada o inhabilitada.

B.O.B.3.1 Requisitos de fichero de código

Se utiliza un solo fichero para encapsular el código del módem de cable. El fichero de código es un mensaje datos firmado de la norma PKCS #7 que incluye:

1) la signatura de verificación de código (CVS) del fabricante;
2) el certificado de verificación de código (CVC) del fabricante firmado por la autoridad de certificación (CA) raíz;
3) la configuración del código (compatible con el módem de cable de destino) a modo de contenido firmado;
4) facultativamente, cuando el operador de cable firma también el fichero del código:
   a) la CVS del operador del cable;
   b) el CVC del operador del cable firmado por la CA raíz.

El fichero de código DEBE cumplir la especificación PKCS #7 y DEBE ser codificado de acuerdo con las reglas de codificación distinguida (DER). El fichero de código DEBE concordar con la estructura que se muestra en el cuadro B.O.B-1. En el apéndice B.O.I se presenta un ejemplo.

Cuadro B.O.B-1/J.112 – Estructura de fichero de código

Fichero de código	Descripción
`PKCS #7 Digital Signature{`	
`SignedData()`	Incluye CVS y CVC X.509
`}`	
`SignedContent{`	
`Content`	`Datos ::= CADENA DE OCTETOS` (configuración de código mejorada)
`}`	

Si al telecargar el certificado de un fabricante, el fabricante no incorpora el certificado en la configuración de código efectiva, el campo SignedContent (contenido firmado) del fichero de código PUEDE ser definido como se muestra en el cuadro B.O.B-2. En este caso, los certificados de CA de fabricante están contenidos en el campo MfgCerts (certificados de fabricante) y separados de la configuración de código efectiva del módem de cable en el campo CodeImage (configuración de código).

Así es posible distinguir claramente la configuración de código de los otros parámetros del fichero de telecarga del código. También es posible, de esta manera, cambiar los certificados de CA de fabricante o parámetros de SignedData (datos firmados) del fichero de telecarga de código sin perturbar o modificar la configuración de código que recibirá el módem de cable. Con ello se puede verificar que la configuración de código no ha cambiado incluso aunque sí lo haya hecho el fichero de telecarga de código debido a un cambio en los certificados de CA de fabricante o los parámetros de SignedData.

Cuadro B.O.B-2/J.112 – Estructura de fichero de código opcional

Fichero de código	Descripción
`PKCS#7 Digital Signature{`	
`Signed Data()`	Incluye CVS y CVC X.509
}	
`SignedContent{`	
`MfgCerts()`	Uno o más certificados de fabricante codificados según DER cada uno de ellos formateado de acuerdo con el formato TLV del certificado de CA definido en B.O.7.2.2.17.
`CodeImage()`	`Datos ::= CADENA DE OCTETOS` (configuración de código mejorada)
}	

B.O.B.3.1.1 Datos firmados de la norma PKCS #7

La información contenida en el fichero de mejora de soporte lógico será del tipo datos firmados de PKCS #7, como se muestra más adelante. Aun manteniendo la conformidad con PKCS #7, se ha restringido el formato de la estructura utilizada por el anexo B a la Recomendación J.112, para facilitar el procesamiento que lleva a cabo un CM a fin de validar la signatura. Los datos firmados de la norma PKCS #7 (PKCS #7 Signed Data) DEBEN concordar con la estructura mostrada en el cuadro B.O.B-3.

Cuadro B.O.B-3/J.112 – Datos firmados de la norma PKCS #7

Campo de PKCS #7	Descripción
Signed Data {	
version	Versión = 1
digestAlgorithmIdentifiers	SHA-1
contentInfo	
contentType	Datos (el fichero de mejora sigue la estructura de PKCS #7)
certificates {	Certificado de verificación de código (CVC)
mfgCVC	REQUERIDO para todos los ficheros de código
Cable OperatorCVC	OPCIONAL; requerido para co-firmas de operadores de cable
} end certificates	
SignerInfo{	
MfgSignerInfo {	REQUERIDO para todos los ficheros de código
version	Versión = 1
issuerAndSerialNumber	Del certificado del firmante
issuerName	Nombre distinguido del expedidor del certificado
countryName	Estados Unidos
organizationName	Certificado de CableLabs
organizationUnitName	Anexo B a la Recomendación J.112

Cuadro B.O.B-3/J.112 – Datos firmados de la norma PKCS #7

Campo de PKCS #7	Descripción
commonName	Autoridad de certificación raíz del anexo B a la Recomendación J.112
certificateSerialNumber	De CVC; entero, 8 octetos
digestAlgorithm	SHA-1
authenticatedAttributes	
signingTime	utcTime (GMT), YYMMDDhhmmssZ
contentType	Datos; tipo del contenido de la configuración del código
messageDigest	Compendio del contenido más atributos autenticados
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end mfg signer info	
MsoSignerInfo {	OPCIONAL; requerido para co-firmas de operadores de cable
version	Versión = 1
issuerAndSerialNumber	Del certificado del firmante
issuerName	Nombre distinguido del expedidor del certificado
countryName	Estados Unidos
organizationName	Certificado de CableLabs
organizationUnitName	Anexo B a la Recomendación J.112
commonName	Autoridad de certificación raíz del anexo B a la Recomendación J.112
certificateSerialNumber	De CVC; entero, 8 octetos
digestAlgorithm	SHA-1
authenticatedAttributes	
signingTime	utcTime (GMT), YYMMDDhhmmssZ
contentType	Datos; tipo del contenido de la configuración del código
messageDigest	Compendio del contenido más atributos autenticados
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end Cable Operator signer info	
} end signer info	
} end signed data	

B.O.B.3.1.1.1 Claves de firma de código

La signatura o firma digital de la norma PKCS #7 utiliza el algoritmo de encriptación RSA [RSA 2] con SHA-1 [FIPS 186]. El módulo de la clave RSA para la firma del código tiene una longitud de 1024 bits, 1536 bits o 2048 bits. El CM DEBE ser capaz de verificar las signaturas de fichero de código firmadas utilizando cualquiera de esos tamaños de módulo. El exponente público es F4 (65537 decimal).

B.O.B.3.1.1.2 Formato de certificado de verificación de código

El formato utilizado para el CVC es conforme a X.509 (véase el cuadro B.O.B-4). Sin embargo, en este caso, se ha restringido el formato de la estructura X.509 para facilitar el procesamiento que lleva a cabo un CM a fin de validar el certificado y extraer la clave pública utilizada para verificar la CVS. El CVC DEBE ser codificado de acuerdo con las DER.

El CVC requiere también que se añada el ID de finalidad de la clave para la "firma del código" dentro del campo utilización de clave ampliada.

```
   -- extended key usage extension OID and syntax
   id-ce-exKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
   ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPuposeID ::= OBJECT IDENTIFIER
```

El CVC DEBE contener un campo extensión, y solamente uno, a saber, el campo extensión de utilización de clave ampliada. La extensión de utilización de clave ampliada DEBE ser marcada como crítica. La extensión de utilización de clave DEBE contener el OID finalidad del código para la firma del código. Si la extensión de utilización de clave ampliada no está presente, o no está marcada como crítica, o incluye cualquier OID de finalidad de la clave distinto del, o además del, ID de finalidad de la firma del código, el CM DEBE detener el proceso de validación y descartar el CVC.

```
   -- extended key purpose OIDs
   id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }
```

Cuadro B.O.B-4/J.112 – Certificado de verificación de código conforme a la Recomendación X.509

Campo del certificado X.509	Descripción
Certificate {	
tbsCertificate	
version	v3(2)
serialNumber	Entero, 8 octetos
signature	SHA-1 con RSA, parámetros nulos
issuer	
countryName	Estados Unidos
organizationName	Certificado de CableLabs
organizationUnitName	Anexo B a la Recomendación J.112
commonName	Autoridad de certificación raíz del anexo B a la Recomendación J.112
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<país de la empresa del asunto>
organizationName	<agente co-firmante del código del asunto>
organizationalUnitName	anexo B a la Recomendación J.112
commonName	Certificado de verificación de código

Cuadro B.O.B-4/J.112 – Certificado de verificación de código conforme a la Recomendación X.509

Campo del certificado X.509	Descripción
subjectPublicKeyInfo	
algorithm	Criptación RSA, parámetros nulos
subjectKey	Módulo de 1024 bits, 1536 bits, o 2048 bits
extensions	
extKeyUsage	
critical	Verdad
keypurposeId	ID de finalidad de la clave para la firma del código
signatureAlgorithm	SHA-1 con RSA, parámetros nulos
signature Value	Módulo de 1024-bits
} end certificate	

B.O.B.3.1.1.3 Revocación de certificado

Esta especificación no requiere o define la utilización de listas de revocación de certificados (CRL, *certificate revocation list*). No se exige al módem de cable que soporte las CRL. Quizá los operadores de cable deseen definir y utilizar las CRL fuera de la red HFC para ayudar en la gestión de los ficheros de código que les proporcionan los fabricantes.

Sin embargo, hay un método de revocación de certificados basado en la fecha de comienzo de la validez de los mismos (que se describe en la subcláusula B.O.B.3.3.2.2). Dicho método requiere que se entregue al módem un CVC puesto al día de cable con una fecha de comienzo de validez actualizada. Una vez que el CVC ha sido validado satisfactoriamente, el tiempo de comienzo de validez de la Recomendación X.509 actualizará el valor que a la sazón tiene cvcAccessStart (comienzo de acceso a CVC) del CM.

Para acelerar la entrega de un CVC actualizado sin necesidad de que el módem de cable procese una mejora de código, el CVC PUEDE ser entregado en el fichero de configuración del CM o en una base de información de gestión (MIB) del SNMP. El formato de un CVC es el mismo tanto si está en un fichero de código como en un fichero de configuración o en una MIB de SNMP.

B.O.B.3.1.2 Contenido firmado

El campo contenido firmado del fichero de código es la configuración de código final en un formato compatible con el módem de cable de destino. De conformidad con los requisitos de la signatura o firma de la norma PKCS #7, el contenido del código se escribe como si fueran datos, es decir, una cadena de octetos simple. El formato de la configuración de código final no se especifica aquí y será definido por cada fabricante de acuerdo con sus requisitos.

Cada fabricante DEBERÍA elaborar su código con mecanismos adicionales que permitan verificar si una configuración de código de mejora es compatible con el módem de cable de destino. El CM NO DEBERÍA instalar la configuración de código mejorado a menos que se haya verificado la compatibilidad de la configuración de código con el CM.

B.O.B.3.2 Controles de acceso a fichero de código

Además de los controles criptográficos proporcionados por la signatura digital y el certificado X.509, en el fichero de código se incluyen valores de control especiales para que el módem de cable efectúe una comprobación antes de validar una configuración de código. Las

condiciones impuestas a los valores de esos parámetros de control DEBEN ser satisfechas antes de que el CM valide el CVC o la CVS y acepte la configuración de código.

B.O.B.3.2.1 Nombres de organización de asunto

El módem de cable reconocerá, en cualquier momento, hasta dos nombres que considere un agente firmante de código fiduciado en el campo asunto del CVC de un fichero de código. Se incluyen aquí:

- El fabricante del módem de cable: el nombre de fabricante del campo asunto del CVC del fabricante DEBE concordar exactamente con el nombre de fabricante almacenado por el fabricante en la memoria no volátil del CM. El CVC de un fabricante se DEBE incluir siempre en el fichero de código.
- Un agente co-firmante: el fabricante permite que otra organización fiducida co-firme ficheros de códigos destinados a sus módems de cable. En la mayoría de los casos, se trata del operador de cable que controla en esos momentos el dominio de explotación del módem de cable. El nombre de la organización del agente co-firmante se comunica al módem de cable vía un CVC del co-firmante en el fichero de configuración cuando se inicializa el proceso de verificación de código del módem de cable. El nombre de organización del co-firmante que figura en el campo asunto del CVC del co-firmante DEBE coincidir exactamente con el nombre de organización del co-firmante recibido previamente en el CVC de inicialización del co-firmante y almacenado por el CM.

El CM PUEDE comparar nombres de organización utilizando una comparación binaria.

B.O.B.3.2.2 Controles variables con el tiempo

Para ayudar en el proceso de mejora de código, el CM DEBE mantener dos conjuntos de valores de tiempo UTC asociados con cada agente firmante de código. Un conjunto de valores DEBE estar siempre almacenado y mantenido para el fabricante del módem de cable. Mientras el módem de cable tiene asignado un agente co-firmante del código, DEBE almacenar y mantener también un conjunto aparte de valores de tiempo para el agente co-firmante.

Estos valores se utilizan para controlar el acceso del fichero de código al módem de cable, controlando individualmente la validez de la CVS y el CVC. Los valores son:

codeAccessStart: un valor de tiempo UTC de 12 bytes referencia al tiempo medio de Greenwich (GMT, *Greenwich mean time*).

cvcAccessStart: un valor de tiempo UTC de 12 bytes con referencia al GMT.

Los valores de UTCTime (tiempo UTC) en el CVC DEBEN expresarse como tiempo medio de Greenwich (GMT) y DEBEN incluir segundos. Es decir, DEBEN expresarse en la forma siguiente: YYMMDDhhmmssZ. El campo año (YY) DEBE interpretarse como sigue:

- Cuando YY sea superior o igual a 50, el año se interpretará como 19YY.
- Cuando YY sea inferior a 50, el año se interpretará como 20YY.

Estos valores estarán siempre referidos al tiempo medio de Greenwich (GMT), por lo que el carácter final de ASCII (Z) se puede eliminar cuando sean almacenados por el CM como codeAccessStart y cvcAccessStart. El CM DEBE mantener cada uno de estos valores de tiempo en un formato que contenga información de tiempo y exactitud equivalentes al formato UTV de 12 caracteres (es decir, YYMMDDhhmmss). El CM DEBE comparar con precisión esos valores almacenados con los valores de tiempo UTC que le hayan sido entregados en un CVC. Estos requisitos se analizan más adelante en la presente especificación.

B.O.B.3.3 Inicialización de mejora de código de módem de cable

Para que el módem de cable pueda mejorar un código, deberá ser inicializado convenientemente. Su fabricante es quien lo inicializa por primera vez. Cada vez que un módem de cable se registre en una red de módem de cable, DEBE comprobar su estado de inicialización en ese momento con

respecto a las necesidades operativas de la red de que se trate. Quizá sea necesario que el módem de cable se reinicialice al registrarse; sobre todo si se traslada de una red a otra.

B.O.B.3.3.1 Inicialización de fabricante

Corresponde al fabricante instalar correctamente la versión de código inicial en el CM.

Para ayudar a la verificación de la mejora del código, se DEBEN cargar valores de los parámetros que se indican a continuación en la memoria no volátil del CM:

1) organizationName (nombre de organización) del fabricante del CM;
2) valores de control variables con el tiempo del fabricante:
    a) valor de inicialización del codeAccessStart (comienzo de acceso a código);
    b) valor de inicialización de cvcAccessStart (comienzo de acceso a CVC).

El nombre de organización del fabricante del módem DEBE estar siempre presente en el módem de cable. El organizationName (nombre de organización) del fabricante del módem de cable PUEDE ser almacenado en la configuración de código de los módems de cable. En condiciones normales, el organizationName del fabricante NO DEBERÍA cambiar, pero la presente especificación no impide que un fabricante cambie la forma de almacenar en el CM su organizationName. El nombre del fabricante utilizado para mejorar el código no necesariamente es el mismo nombre que se utiliza en el certificado del fabricante.

Los valores de control variables con el tiempo, codeAccessStart y cvcAccessStart, DEBEN ser inicializados en un tiempo UTC compatible con el tiempo de comienzo de validez del CVC más reciente del fabricante. Estos valores variables con el tiempo serán actualizados periódicamente en funcionamiento normal vía los CVC de fabricante recibidos y verificados por el módem de cable.

Al principio, el módem de cable no reconocerá a un agente co-firmante.

B.O.B.3.3.2 Inicialización de red

El método de inicialización y obtención de ficheros de telecarga de código de CM se define en el [Recomendación J.112 anexo B]. Para ayudar a la verificación del código, se utiliza el fichero de configuración como medio autenticado en el que inicializar el proceso de verificación del código. En el fichero de configuración de módem de cable, el módem de cable recibe fijaciones de configuración pertinentes a la verificación de mejora de código. Dichas fijaciones NO DEBEN ser utilizadas sino hasta que el CMTS haya registrado el CM de manera satisfactoria.

El fichero de configuración DEBERÍA incluir siempre el CVC más actualizado aplicable al módem de cable de destino; pero cuando el fichero de configuración se utiliza para iniciar una mejora de código, DEBE incluir un certificado de verificación de código (CVC) para inicializar el módem de cable de modo que acepte ficheros de código de acuerdo con la presente especificación. Con independencia de si se requiere o no una mejora de código, un CVC del fichero de configuración DEBE ser procesado por el módem de cable.

Un fichero de configuración PUEDE contener:

- ningún CVC;
- un CVC de fabricante solamente;
- un CVC de co-firmante (operador de cable) solamente;
- tanto un CVC de fabricante como un CVC de co-firmante.

Antes de que el CM ponga a punto su capacidad de mejorar ficheros de código en la red, DEBE recibir un CVC válido en un fichero de configuración y registrarse de manera satisfactoria en el CMTS. Además, cuando el fichero de configuración del módem de cable no contiene un CVC válido, y su capacidad de mejorar ficheros de código ha sido inhabilitada, el CM DEBE rechazar cualquier información que figure en un CVC entregado subsiguientemente vía SNMP.

Cuando el fichero de configuración del módem de cable contiene solamente un CVC de fabricante válido, el módem de cable sólo requerirá una signatura del fabricante en los ficheros de código. En este caso, el CM NO DEBE aceptar ficheros de código que hayan sido co-firmados.

Cuando el fichero de configuración del módem de cable contiene el CVC de un co-firmante, se utiliza para inicializar el módem de cable con un agente co-firmante. Una vez validado, el nombre de organizationName del asunto del CVC pasará a ser el agente co-firmante del código asignado al módem de cable. Para que un CM acepte subsiguientemente una configuración de código, el co-firmante, además del fabricante del módem de cable, DEBE haber firmado el fichero de código.

El nombre de organización del fabricante del módem de cable y los valores de control variables con el tiempo del fabricante DEBEN estar siempre presentes en el módem de cable. Si se inicializa el módem de cable para aceptar un código co-firmado por un agente co-firmante adicional, el nombre de la organización y sus correspondientes valores de control variables con el tiempo DEBEN ser almacenados y mantenidos mientras sean operativos. Se DEBE asignar espacio en la memoria del módem de cable para los valores de control del co-firmante siguientes:

1) organizationName (nombre de organización) del agente co-firmante;
2) valores de control variables con el tiempo del co-firmante:
    a) cvcAccessStart (comienzo de acceso a CVC);
    b) codeAccessStart (comienzo de acceso a código).

El conjunto de estos valores del fabricante se DEBE almacenar en la memoria no volátil del CM y no deberá perderse cuando se elimine la alimentación de energía eléctrica del CM. Cuando se asigna un co-firmante al CM, el CVC del co-firmante está siempre en el fichero de configuración. Por tanto, puesto que los valores de control del co-firmante se recibirán siempre en el fichero de configuración, no es preciso que el CM almacene valores de control variables con el tiempo del co-firmante en memoria no volátil; y no hace falta retener los valores cuando se pierda la alimentación de energía eléctrica del CM y se ponga en marcha un proceso de reiniciación de la misma.

B.O.B.3.3.2.1 Procesamiento de CVC de fichero de configuración

Cuando se incluye un CVC en el fichero de configuración, el CM DEBE verificar el CVC antes de aceptar cualquiera de las fijaciones de mejora de código que contiene. Al recibir el CVC en el fichero de configuración, el CM DEBE efectuar los pasos de validación y procedimiento que se indican a continuación. Si cualquiera de las comprobaciones de verificación siguientes falla, el CM DEBE detener inmediatamente el proceso de verificación del CM y registrar cronológicamente el error, si procede. Si el fichero de configuración del CM no incluye un CVC cuya validación sea ratificadora, el CM NO DEBE efectuar telecargas de ficheros de código de mejora, ya sean provocadas por el fichero de configuración de CM o vía una MIB de SNMP. Además, si los ficheros de configuración del CM no incluyen un CVC que se valide adecuadamente, no es necesario que el CM procese un CVC entregado a continuación por conducto de una MIB de SNMP, y NO DEBE aceptar información procedente de un CVC entregado seguidamente por ese mismo conducto.

Al recibir el CVC en un fichero de configuración, y después de que el CM se haya registrado de manera satisfactoria en el CMTS, el CM DEBE:

1) Verificar que la extensión utilización de clave ampliada figura en el CVC tal como se define en B.O.B.3.1.1.2.
2) Comprobar el nombre de organización de asunto del CVC:
    a) SI el organizationName (nombre de organización) es idéntico al nombre del fabricante del módem de cable, se trata ENTONCES del CVC del fabricante. En este caso, el CM DEBE verificar que el tiempo de comienzo de la validez del CVC del fabricante es superior o igual al valor de cvcAccessStart (comienzo de acceso a CVC) del fabricante retenido a la sazón en el CM.

b) SI el organizationName es idéntico al agente co-firmante de código actual del módem de cable, se trata ENTONCES del CVC del co-firmante actual y el CM DEBE verificar que el tiempo de comienzo de la validez es superior o igual al valor de cvcAccessStart del co-firmante retenido a la sazón en el CM.

c) SI el organizationName no es idéntico al nombre del fabricante o del agente co-firmante del código actual, una vez que el CVC haya sido validado (y se haya completado el registro), este nombre de organización de asunto pasará a ser ENTONCES el nuevo agente co-firmante de código del CM. El CM NO DEBE aceptar un fichero de código a menos que haya sido firmado por el fabricante, y co-firmado por este agente co-firmante de código.

3) Validar la signatura o firma del certificado utilizando la clave raíz retenida por el CM. La verificación de la signatura del CM autenticará la fuente y validará la confianza en los parámetros del CVC.

4) Actualizar los valores de cvcAccessStart y codeAccessStart actuales del CM correspondientes al organizationName de asunto del CVC (es decir, el fabricante o el agente co-firmante del código) con el valor de tiempo de comienzo de validez del CVC validado. El CM DEBERÍA descartar cualquier remanente del CVC.

B.O.B.3.3.2.2 Procesamiento de CVC del SNMP

El CM DEBE procesar los CVC entregados por el SNMP cuando esté habilitado para mejorar ficheros de código; de otro modo, todos los CVC entregados vía SNMP DEBEN ser rechazados. Cuando se valide el CVC entregado vía SNMP, el CM DEBE efectuar los pasos de validación y procedimientos que se indican a continuación. Si cualquiera de las comprobaciones de verificación siguientes falla, el CM DEBE detener inmediatamente el proceso de verificación del CVC, registrar cronológicamente el error, si procede, y eliminar todos los remanentes del proceso hasta ese paso.

El CM DEBE:

1) Verificar que la extensión utilización de clave ampliada figura en el CVC tal como se define en B.O.B.3.1.1.2.

2) Comprobar el nombre de organización de asunto del CVC.

Si el CVC es un CVC de fabricante (tipo 32):

a) SI el organizationName (nombre de organización) es idéntico al nombre del fabricante, del módem, se trata ENTONCES del CVC del fabricante. En este caso, el CM DEBE verificar que el tiempo de comienzo de la validez del CVC del fabricante es superior o igual al valor de cvcAccessStart (comienzo de acceso a CVC) del fabricante retenido a la sazón en el CM.

b) SI el organizationName no es idéntico al nombre del fabricante del módem, este CVC DEBE ser rechazado ENTONCES y el error debe ser registrado cronológicamente.

Si el CVC es un CVC de co-firmante (tipo 33):

a) SI el organizationName es idéntico al agente co-firmante de código actual del módem de cable, se trata ENTONCES del CVC del co-firmante actual y el CM DEBE verificar que el tiempo de comienzo de la validez es superior o igual al valor de cvcAccessStart del co-firmante retenido a la sazón en el CM.

b) SI el organizationName no es idéntico al nombre del agente co-firmante de código actual, una vez que el CVC haya sido validado (y se haya completado el registro), este nombre de organización de asunto pasará a ser ENTONCES el nuevo agente co-firmante de código del CM. El CM NO DEBE aceptar un fichero de código a menos que haya sido firmado por el fabricante, y co-firmado por este agente co-firmante de código.

3) Validar la signatura o firma del certificado utilizando la clave raíz retenida por el CM. La verificación de la signatura autenticará el certificado y confirmará la confianza en el tiempo de comienzo de validez del CVC.

4) Actualizar los valores de cvcAccessStart y codeAccessStart actuales del asunto con el valor de tiempo de comienzo de validez del CVC validado. Todos los parámetros del certificado, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados.

B.O.B.3.4 Requisitos de firma de código

Cuando se firmen ficheros de código, DEBEN seguirse los procedimientos que se indican a continuación.

B.O.B.3.4.1 Requisitos de autoridad de certificación (CA)

Además del certificado de fabricante expedido a un fabricante, que se describe con anterioridad en el presente anexo B.O, la CA raíz expedirá certificados de firma de código llamados certificados de verificación de código (CVC).

El certificado de verificación de código (CVC) lo proporciona la CA y se firma con la clave raíz (DRK). Los CVC firmados por la CA DEBEN ser exactamente tal como se especifica en B.O.B.3.1.1.2 y utilizados solamente como respaldo de las signaturas de código de módem de cable. La CA no DEBE firmar ningún CVC a menos que sea idéntico al formato especificado en esa cláusula. Antes de firmar un CVC, la CA DEBE verificar que el agente que firma el código es auténtico y es un agente válido a tal fin.

La CA será responsable del registro de nombres de agentes firmantes de código autorizados. Entre los agentes firmantes de código figuran los fabricantes de CM y los operadores de cable que co-firmarán las configuraciones de código de módem de cable. Corresponde a la CA garantizar que el nombre de organización de cada agente firmante de código es diferente. Cuando se asignan nombres de organización para co-firmantes de código se DEBEN aplicar las directrices que siguen:

- El nombre de organización utilizado para identificarse como el agente co-firmante de código en un CVC DEBE ser asignado por una CA.
- El nombre DEBE ser una cadena imprimible de ocho dígitos hexadecimales que distinga de manera exclusiva a un agente firmante de código de todos los demás.
- Cada dígito hexadecimal del nombre DEBE elegirse del conjunto de caracteres 0-9 (0x30-0x39) o A-F (0x41-0x46).
- La cadena formada por ocho dígitos 0 no está permitida y NO DEBE ser utilizada en un CVC.

Para conservar espacio de almacenamiento, el CM PUEDE representar internamente el nombre del agente co-firmante de código en un formato alternativo en tanto en cuanto se mantenga toda la información y el formato original pueda ser reproducido; por ejemplo, un entero no cero de 32 bits, con un valor entero de 0 representando la ausencia de agente firmante de código.

B.O.B.3.4.2 Requisitos de fabricación

Para firmar sus ficheros de código, el fabricante DEBE obtener un CVC válido de la CA. Todas las configuraciones de código de fabricante proporcionadas a un operador de cable para la mejora a distancia de un CM de una red HFC conforme a la Recomendación J.112 anexo B DEBEN ser firmadas de acuerdo con los requisitos definidos en la presente especificación.

Cuando el fabricante firma un fichero de código, PUEDE optar por no actualizar el valor de signingTime (tiempo de firma) de la norma PKCS #7 en la información de firma del fabricante. Esta especificación requiere que el valor de signingTime de PKCS #7 sea igual o superior al tiempo de comienzo de validez del CVC. Si el fabricante utiliza un signingTime igual al tiempo de

comienzo de validez del CVC cuando firma una serie de ficheros de código, esos ficheros pueden ser utilizados y reutilizados. De esta manera, un operador de cable puede utilizar el fichero de código para aumentar o rebajar la categoría de la versión del código de los módems de cable de aquel fabricante. Esos ficheros de código serán válidos hasta que se genere un nuevo CVC y sea recibido por el módem de cable. Se recomienda que el fabricante firme sus ficheros de código de esta manera cuando su política de seguridad así lo permita (véase § B.O.B.4, Consideraciones relativas a la seguridad).

B.O.B.3.4.3 Requisitos de operador de cable

Un operador de cable recibirá ficheros de código de mejora de soporte lógico procedentes del fabricante. Utilizando la clave pública raíz, el operador de cable deberá confirmar que esa configuración de código ha sido elaborada por el fabricante fiduciado. El operador de cable puede verificar de nuevo el fichero de código, en cualquier momento, repitiendo el proceso.

El operador de cable tiene la opción de co-firmar la configuración de código destinada a un módem de cable de su red. Para ello, el operador co-firma el contenido del fichero de acuerdo con la norma de signatura PKCS #7, e incluye su CVC co-firmado. La Recomendación J.112 anexo B no requiere que un operador de cable co-firme ficheros de código; pero cuando el operador de cable sigue todas las reglas definidas en la presente especificación para la preparación de un fichero de código, el módem de cable DEBE aceptarlo.

Todas las configuraciones de código telecargadas en un CM a través de la red HFC de aquel anexo DEBEN ser firmadas de acuerdo con los requisitos definidos en esta especificación.

B.O.B.3.5 Requisitos de verificación de código

NO DEBE instalarse un código de mejora a menos que se compruebe que el código está fiduciado de acuerdo con el proceso de verificación descrito en la presente especificación.

El CM DEBE poder procesar una signatura o firma digital de la norma PKCS #7 y un certificado X.509 según lo definido en esta especificación. No es preciso que el CM soporta la gama completa de las especificaciones PKCS #7 y X.509.

B.O.B.3.5.1 Pasos de la verificación de código de módem de cable

Cuando el CM telecarga un código, DEBE efectuar los pasos que se describen en esta cláusula. Si falla cualquiera de las comprobaciones de verificación, el CM DEBE detener inmediatamente el proceso de telecarga, registrar cronológicamente el error, si procede, eliminar todos los remanentes del proceso hasta ese paso, y continuar funcionando con el código existente.

1) El CM DEBE validar la información de signatura o firma del fabricante verificando que:
   a) el valor de signingTime (tiempo de firma) de PKCS #7 es igual o superior al valor de codeAccessStart (comienzo de acceso a código) retenido a la sazón en el CM;
   b) el valor de signingTime de PKCS #7 es igual o superior al tiempo de comienzo de validez del CVC del fabricante;
   c) el valor de signingTime de PKCS #7 es menor o igual que el tiempo de final de validez del CVC del fabricante.
2) El CM DEBE validar el CVC del fabricante verificando que:
   a) el organizationName (nombre de organización) del asunto del CVC es idéntico al nombre del fabricante almacenado a la sazón en la memoria del CM;
   b) el tiempo de comienzo de validez del CVC es igual o superior al valor de cvcAccessStart (comienzo de acceso a CVC) retenido a la sazón en el CM;
   c) la extensión utilización de clave ampliada figura en el CVC tal como se define en B.O.B.3.1.1.2.

3) El CM DEBE validar la signatura o firma del certificado utilizando la clave raíz retenida por el CM. La verificación de la signatura autenticará la fuente de la clave de verificación de código (CVK, *code verification key*) pública y confirmará la confianza en la clave.

4) El CM DEBE verificar la signatura o firma de fichero de código del fabricante:

   a) una vez que se haya establecido la confianza en la CVK del fabricante, los parámetros del certificado restantes, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados;

   b) si la signatura no pasa la prueba de verificación, todos los componentes del fichero de código (incluida la configuración de código), y cualesquiera valores obtenidos a partir del proceso de verificación DEBEN ser rechazados y DEBERÍAN ser descartados inmediatamente.

5) Si la signatura del fabricante pasa la prueba de verificación y se requiere la signatura del agente co-firmante:

   a) el CM DEBE validar la información de la signatura del co-firmante verificando que:

      i) la información de signatura del co-firmante está incluida en el fichero de código;

      ii) el valor de signingTime (tiempo de firma) de la norma PKCS #7 es igual o superior al valor de codeAccessStart (comienzo de acceso a código) correspondiente retenido a la sazón en el CM;

      iii) el valor de signingTime de PKCS #7 es igual o superior al tiempo de comienzo de validez del CVC correspondiente;

      iv) el valor de signingTime de PKCS #7 es menor o igual que el tiempo de final de validez del CVC correspondiente;

   b) el CM DEBE validar el CVC del co-firmante, verificando que:

      i) el organizationName (nombre de organización) del asunto del CVC es idéntico al nombre de organización del co-firmante almacenado a la sazón en la memoria del CM;

      ii) el tiempo de comienzo de validez del CVC es igual o superior al valor de cvcAccessStart (comienzo de acceso a CVC) retenido a la sazón en el CM para el organizationName del asunto correspondiente;

      iii) la extensión utilización de clave ampliada figura en el CVC tal como se define en la subcláusula B.O.B.3.1.1.2;

   c) el CM DEBE validar la signatura o firma del certificado utilizando la clave raíz retenida por el CM. La verificación de la signatura autenticará la fuente de la clave de verificación de código (CVK) pública del co-firmante y confirmará la confianza en la clave. Una vez establecida la confianza en la CVK del co-firmante, los parámetros del certificado restantes, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados;

   d) el CM DEBE verificar la signatura de fichero de código del co-firmante.

   Si la signatura no pasa la prueba de verificación, todos los componentes del fichero de código (incluida la configuración de código), y cualesquiera valores obtenidos a partir del proceso de verificación DEBEN ser rechazados y DEBERÍAN ser descartados inmediatamente.

6) Si se verifica la signatura del fabricante, y facultativamente la del co-firmante, pasa la prueba de verificación, la configuración de código puede ser fiduciada y la instalación puede proseguir. Antes de instalar la configuración de código, todos los demás componentes del fichero de código y cualesquiera valores obtenidos a partir del proceso de verificación, excepto los valores de signingTime de PKCS #7 y el tiempo de comienzo de validez del CVC, DEBERÍAN ser descartados inmediatamente.

7) El CM puede mejorar su soporte lógico instalando el fichero de código de acuerdo con la [Recomendación J.112 anexo B v1].

8) Si la instalación del código no tiene éxito, el CM DEBE rechazar los valores de signingTime de PKCS #7 y los valores de tiempo de comienzo de validez del CVC que acaba de recibir en el fichero de código. Deberán seguirse los pasos indicados en la [Recomendación J.112 anexo B v1] para el tratamiento de esta condición de fallo.

9) Cuando la instalación del código tiene éxito, el CM DEBE actualizar los controles variables con el tiempo del fabricante con los valores obtenidos de la información de signatura del fabricante y el CVC:

   a) actualizar el valor actual de codeAccessStart con el valor de signingTime de PKCS #7;

   b) actualizar el valor actual de cvcAccessStart con el valor de comienzo de validez del CVC.

10) Cuando la instalación del código tiene éxito, SI el fichero está co-firmado, el CM DEBE actualizar los controles variables con el tiempo del co-firmante con los valores obtenidos de la información de signatura del co-firmante y el CVC:

   a) actualizar el valor actual de codeAccessStart con el valor de signingTime de PKCS #7;

   b) actualizar el valor actual de cvcAccessStart con el valor de comienzo de validez del CVC.

B.O.B.3.6 Interoperabilidad de la Recomendación J.112 anexo B 1.0

Los módems de cable de la Recomendación J.112 anexo B v2 DEBEN verificar las mejoras de código de acuerdo con esta especificación incluso cuando funcionen con un entorno que se atiene a la Recomendación J.112 anexo B v1.

Los ficheros de configuración de la Recomendación J.112 anexo B v1 destinados a módems de cable de la Recomendación J.112 anexo B v2 DEBEN soportar los requisitos de fichero de configuración definidos en la presente especificación.

Los módems de cable de la Recomendación J.112 anexo B.1.1 DEBEN recibir ficheros de código conformes a la Recomendación J.112 anexo B v2. Los ficheros de mejora pasan a través del sistema de la Recomendación J.112 anexo B v1 inalterados, y no precisarán modificación alguna de los requisitos de tratamiento de ficheros de código de la Recomendación J.112 anexo B v1.

En un entorno conforme a esa Recomendación J.112 anexo B.1.0 en donde módems de clave de la Recomendación J.112 anexo B v2 están recibiendo ficheros de mejora de código, el gestor SNMP DEBERÍA admitir las bases de información de gestión (MIB) definidas para la verificación de códigos de la Recomendación J.112 anexo B v2. La disponibilidad de esta capacidad MIB es muy importante a efectos del funcionamiento y la seguridad adecuados del proceso de mejora de códigos de la mencionada Recomendación J.112 anexo B v2.

B.O.B.3.7 Códigos de error

Se definen códigos de error para reflejar posibles estados de fallo durante el proceso de verificación del código.

1) Controles de ficheros de código inadecuado:

   a) El organizationName (nombre de organización) del asunto del CVC del fabricante no concuerda con el nombre de fabricante del CM.

   b) El organizationName del asunto del CVC para el agente co-firmante del código no concuerda con el agente co-firmante de código actual del CM.

   c) El valor de signingTime (tiempo de firma) de PKCS #7 del fabricante es inferior al valor de codeAccessStart (comienzo de acceso a código) retenido a la sazón en el CM.

d) El valor de tiempo de comienzo de validez de PKCS #7 del fabricante es inferior al valor de cvcAccessStart (comienzo de acceso a CVC) retenido a la sazón en el CM.

e) El tiempo de comienzo de validez del CVC del fabricante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.

f) El valor de signingTime de PKCS #7 del fabricante es inferior al tiempo de comienzo de validez del CVC.

g) Extensión utilización de cable ampliada faltante o inapropiada en el CVC del fabricante.

h) El valor de signingTime de PKCS #7 del co-firmante es inferior al valor de codeAccessStart retenido a la sazón en el CM.

i) El valor de tiempo de comienzo de validez de PKCS #7 del co-firmante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.

j) El tiempo de comienzo de validez del CVC del co-firmante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.

k) El valor de signingTime de PKCS #7 del co-firmante es inferior al tiempo de comienzo de validez del CVC.

l) Extensión utilización de clave ampliada faltante o inapropiada en el CVC del co-firmante.

2) Fallo de validación de CVC del fabricante del fichero de código.

3) Fallo de validación de CVS del fabricante del fichero de código.

4) Fallo de validación de CVC del co-firmante del fichero de código.

5) Fallo de validación de CVS del co-firmante del fichero de código.

6) Formato de CVC de fichero de configuración inapropiado:

– Atributo de utilización de clave faltante o inapropiado.

7) Fallo de validación de CVC de fichero de configuración.

8) Formato de CVC de SNMP inapropiado:

a) El organizationName del asunto del CVC para el fabricante no concuerda con el nombre del fabricante del CM.

b) El organizationName del asunto del CVC para el agente co-firmante del código no concuerda con el agente co-firmante de código actual del CM.

c) El tiempo de comienzo de validez del CVC es inferior o igual al valor de cvcAccessStart del asunto correspondiente retenido a la sazón en el CM.

d) Atributo de utilización de clave faltante o inapropiado.

9) Fallo de validación de CVC de SNMP.

B.O.B.4 Consideraciones relativas a la seguridad (informativo)

La protección dada a las claves privadas constituye un factor fundamental para el mantenimiento de la seguridad. Los usuarios autorizados a firmar códigos, tales como los fabricantes y operadores a los que la autoridad de certificación (CA) ha enviado certificados de verificación de firma de código (CVC), deben proteger sus claves privadas. Un atacante con acceso a la clave privada de un usuario firmante de código autorizado puede crear, a su capricho, ficheros de código potencialmente aceptables por un gran número de módems de cable (CM).

La defensa contra ese tipo de ataques consiste en que el operador revoque el certificado cuya clave privada de firma de código asociada ha sido descubierta por el atacante. Para revocar un certificado, el operador debe entregar a cada CM afectado un CVC actualizado con un tiempo de comienzo de validez más reciente que el del certificado o los certificados que se revocan. El CVC nuevo puede ser entregado por conducto de cualquiera de los mecanismos soportados: fichero de configuración,

fichero de código o MIB de SNMP. El CVC nuevo revoca implícitamente todos los certificados cuyo tiempo de comienzo de validez es anterior al del CVC nuevo.

Para reducir la vulnerabilidad a este tipo de ataques, es importante que los operadores actualicen periódicamente el CVC de cada CM, con una frecuencia comparable a la de sus actualizaciones de la lista de revocación de certificados (CRL), si se dispusiera de una. Las actualizaciones periódicas ayudan a controlar el intervalo de tiempo durante el cual un atacante puede utilizar una clave de firma de código comprometida. Con independencia de si se está en el ciclo de actualización de los CVC, éstos deberían actualizarse también cuando se sospeche que una clave de firma de código ha quedado comprometida. Para actualizar un CVC, el usuario necesita otro CVC expedido por la CA cuyo tiempo de comienzo de validez sea posterior al del CVC del CM. Esto significa que la CA raíz debe enviar periódicamente CVC nuevos a todos los fabricantes y operadores firmantes de códigos autorizados, para facilitar la actualización de los CVC. Es probable que DOCSIS establezca una estrategia respecto al programa de expedición de nuevos CVC, y seguramente los operadores deseen coordinar sus políticas de actualización con ese programa.

Cuando un CM está tratando de registrarse en la red por primera vez, o se ha estado fuera de línea durante un cierto periodo de tiempo, es importante que reciba una CVC fiduciado tan pronto como sea posible. Así se da al CM la oportunidad de recibir el CVC más actualizado de que se disponga y se le impide el acceso a los CVC que tuvieron que ser revocados desde la última inicialización del CM. La primera oportunidad que tiene el CM de recibir un CVC fiduciado está en su fichero de configuración. Si el fichero de configuración no incluye un CVC válido, el CM no pedirá o no podrá mejorar a distancia ficheros de código. Además, el CM no aceptará los CVC entregados subsiguientemente vía una MIB de SNMP.

Para reducir la posibilidad de que un CM reciba un fichero de código anterior como consecuencia de un ataque de tipo reproducción, los ficheros de código incluyen un valor de tiempo de firma en la estructura PKCS #7 que se puede utilizar para indicar el momento en que se firmó la configuración de código. Cuando el CM recibe un fichero de código cuyo tiempo de firma es posterior al tiempo de firma que hubiera recibido en último lugar, actualizará su memoria interna con ese valor. El CM no aceptará ficheros de código con un tiempo de firma anteriores al valor almacenado internamente. Para mejorar la categoría de un CM con un fichero de código nuevo sin denegar el acceso a ficheros de código pasados, el firmante puede optar por no actualizar el tiempo de firma. De esta manera, múltiples ficheros de código con el mismo tiempo de firma de código permiten a un operador rebajar de categoría libremente la configuración de código de un CM a una versión anterior (es decir, hasta que el CVC sea actualizado). Esta manera de actuar presenta varias ventajas para el operador, pero esas ventajas deberían ponderarse frente a la posibilidad de un ataque del tipo reproducción de fichero de código.

Sin un mecanismo fiable que permita retornar a una versión de código buena y conocida, cualquier esquema de actualización de códigos, incluido el de la presente especificación, tiene el inconveniente de que una sola actualización impuesta y exitosa de una configuración de código no válida por parte de un CM puede inutilizar el CM. Incluso peor, una configuración de código no válida puede provocar que el CM se comporte de forma dañina y perjudicial para la red. Ese CM no sería reparable, en tales condiciones, por medio de una actualización de código a distancia, ya que la configuración de código no válida no admite el esquema de actualización.

APÉNDICE B.O.I

Ejemplos de mensajes, certificados y PDU

Este apéndice presenta ejemplos numéricos que pueden ser de utilidad para los implementadores de la presente especificación. Los ejemplos se desarrollan a través de un intercambio de claves típico: información de autorización, petición de autorización, respuesta de autorización, petición de clave y

respuesta de clave. En cada paso se dan detalles sobre los cálculos criptográficos, y se incluyen ejemplos de certificados. Los ejemplos incluyen asimismo varias PDU paquete, criptadas utilizando el material de aplicación de claves obtenido en el intercambio de claves del ejemplo.

El presente apéndice es de carácter informativo solamente y no forma parte de la especificación.

B.O.I.1 Notación

En el ejemplo que sigue, los paquetes se representan como trenes de octetos, cada octeto en notación hexadecimal, a veces con una anotación de texto. El orden de transmisión de los octetos es de izquierda a derecha y de arriba abajo. Considérese, por ejemplo la representación siguiente de un paquete:

00 01 02 03	Descripción #1
04 05	
06 07 08	Descripción #2

El paquete consta de 9 octetos, representados en notación hexadecimal como "00", "01", ..., "08". El octeto representado por "00" es el que se transmite primero, y el octeto representado por "08" se transmite el último.

En el análisis de los ejemplos, los valores enteros se representan en notación hexadecimal utilizando un prefijo "0x" o en notación decimal sin prefijo. Por ejemplo, la notación hexadecimal 0x12345 y la notación decimal 74565 representan el mismo valor entero. Todos los valores enteros son valores no negativos. Así por ejemplo, 0xff representa el entero que tiene el valor 255, es decir, un valor no negativo.

El protocolo BPKM genera y distribuye claves DES de 8 octetos y claves DES triple de 16 octetos, sin corregir el bit menos significativo de cada octeto para paridad. Las implementaciones extraen una clave de 56 bits de una clave de 8 octetos y una clave de 112 bits de una clave de 16 octetos ignorando el valor del bit menos significativo de cada octeto. En los ejemplos que aquí se dan, las claves se representan sin corrección de paridad.

B.O.I.2 Información de autorización

El CM envía el mensaje información de autorización siguiente:

0c 02 94	Encabezamiento de información de autorización
11 02 91	Encabezamiento de certificado de CA
30 82 02 8d 30 82 01 f6 . . . 81 87 19 61 72 20 19 1e	Certificado de CA

El campo código tiene el valor 0x0c, lo que identifica esto como un mensaje información de autenticación. El campo longitud tiene el valor 0x294 (660), que es el número de octetos que siguen al campo longitud.

El único atributo es el certificado de CA. A continuación se dan detalles del certificado.

B.O.I.2.1 Detalles del certificado de CA

Los campos del certificado de CA del mensaje información de autorización anterior se descomponen como sigue:

30 82 02 8d	encabezamiento de certificado
30 82 01 f6	encabezamiento de tbsCertificate
a0 03 02 01 02	versión
02 08 01 02 03 04 05 06 07 08	número de serie
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	signatura
30 81 88	encabezamiento de expedidor
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común
30 1e	encabezamiento de validez
17 0d 39 39 30 31 32 30 31 36 30 35 30 30 5a	no antes
17 0d 34 39 31 32 33 31 32 33 35 39 35 35 5a	no después
30 81 88	encabezamiento de asunto
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común
30 81 9f	encabezamiento de información de clave pública de asunto
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	tipo de algoritmo de clave pública
03 81 8d 00 30 81 89	encabezamiento de clave pública

02 81 81 00 af d1 86 c8 17 45 02 bc e5 59 b4 15 ac 95 87 7b 89 f5 8b f8 3b 8a 8b ef 67 cf 9e 00 47 d5 f1 06 42 55 36 a1 d1 8c dc cb 81 bb 31 8d 35 f7 6d 11 a0 91 9b 31 3d b9 71 38 46 15 c8 81 c4 51 06 7b d7 8a 70 be c1 28 0d 78 80 3c 44 a6 5e 35 5f 6e 46 2f 80 41 28 78 63 6c 86 cc d0 b3 58 ca bc 07 d5 19 3e 8a a2 1c 7e ff 0d 16 2b 0f bd a5 5e 60 93 64 09 80 24 76 ed e4 a9 e3 81 26 0c de 8a 89	módulo de clave pública
02 03 01 00 01	exponente de clave pública
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	algoritmo de signatura
03 81 81 00 81 4d db 31 e2 31 d2 6c f5 21 29 93 4a ce cb 6c fb 8b fc 3d ef 4b e8 4a 8a db f7 d8 e3 70 1d 3c ff ba 71 70 c4 82 24 9f 12 b5 d4 3e 3a 4d 20 64 2f ab 8b 05 27 9a 34 24 33 24 d4 7e bc 41 07 34 7a a6 51 12 29 55 e7 9b 5b e5 6b 79 bb 31 04 2f d1 c6 d3 7f 32 a2 b5 cc 99 23 09 97 1a 21 44 fa 25 3b f4 4b d6 00 cf e9 1b a9 be 9b 88 f8 90 fd 59 77 80 41 7d cb ca bf 81 87 19 61 72 20 19 1e	valor de signatura

Algunos de los campos de este ejemplo son los mismos en todos los certificados de CA. Dichos campos son:

- versión: v3
- signatura: SHA-1 con RSA, parámetros nulos
- primer nombre de unidad organizacional del asunto: "J.112 anexo B".
- tipo de algoritmo de clave pública: encriptación RSA, parámetros nulos
- exponente de clave pública: entero de 3 octetos de valor 0x10001
- algoritmo de signatura: SHA-1 con RSA, parámetros nulos

Este es un ejemplo de certificado de CA auto-firmado. El nombre del expedidor y los nombres del asunto son idénticos. En este ejemplo, los campos nombre concordantes son:

- nombre de país: "US"
- nombre de organización: "Nortel"
- primer nombre de unidad organizacional: "J.112 Annex B"
- segundo nombre de unidad organizacional: "Building 1, Andover MA"
- nombre común: "Nortel Cable Modem Root Certificate Authority"

Los otros campos son ejemplos de valores. Algunos de éstos son:

- número de serie: entero de 8 octetos cuyo valor es 0x0102030405060708. Otros certificados de CA pueden utilizar una longitud diferente.
- no antes: 1999-01-20 16:05:00 GMT
- no después: 2049-12-31 23:59:55 GMT
- módulo de clave pública: entero de 1024 bits cuyo valor es 0x00afd1...8a89. Otros certificados de CA pueden utilizar una longitud de entero de 1024 a 2048 bits, inclusive.
- valor de signatura: cadena de bits de 1024 bits de longitud que representa el valor entero 0x00814d...191e. Otros certificados de CA pueden utilizar una cadena de bits de longitud 1024 a 2048 bits, inclusive; la longitud concuerda con la del módulo del expedidor. La signatura se calcula en la porción del certificado que comienza con el encabezamiento de tbsCertificate y termina con el exponente de clave pública, inclusive.

B.O.I.3 Petición de autorización

El CM envía la petición de autorización siguiente:

04 72 03 40	Encabezamiento de petición de autorización
05 00 ad	Encabezamiento de identificación de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Número de serie
02 00 03 00 00 ca	ID de fabricante
03 00 06 00 00 ca 01 04 01	Dirección MAC
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clave pública RSA
12 02 7a	Encabezamiento de certificado de CM
30 82 02 76 30 82 01 df . . . 19 c9 f1 dc 30 b8 d3 d5	Certificado de CM
13 00 0b	Encabezamiento de capacidades de seguridad
15 00 04 01 00 02 00	Lista de series criptográficas
16 00 01 01	Versión de BPI
0c 00 02 22 60	SAID

El campo código tiene el valor 0x04, lo que identifica esto como un paquete petición de autorización. El campo identificador tiene el valor 0x72; se trata de un valor de ejemplo. El campo longitud tiene el valor 0x0340 (832), que es el número de octetos que siguen al campo longitud.

El primer atributo es la identificación de CM. Es un atributo compuesto formado por los subatributos siguientes: número de serie, ID de fabricante, dirección MAC y clave pública RSA. Se muestran ejemplos de valores de estos tres subatributos.

La clave pública RSA se codifica según las DER y es similar al ejemplo de la subcláusula 2.2 de [RSA 3]. El módulo es un entero de 1024 bits que se representa utilizando 0x81 (129) octetos. En este ejemplo, el valor del módulo es:

```
0x00e0e06c8d ... caeed631.
```

Se señala que 0x00 es el octeto más significativo del módulo y 0x31 el menos significativo. El exponente es un entero formado por 3 octetos y cuyo valor es 0x010001.

El atributo siguiente es el certificado de CM. Más adelante se dan detalles del certificado. Se señala que algunos campos del certificado de CM deben concordar con subatributos de la identificación de CM; esos subatributos son la dirección MAC y la clave pública RSA.

El siguiente atributo es el atributo capacidades de seguridad. Es un atributo compuesto formado por la lista de series criptográficas y la versión de BPI. En este ejemplo se indican dos series

criptográficas: DES de 56 bits sin autenticación y DES de 40 bits sin autenticación. La versión de BPI es BPI+.

El atributo final es el SAID primario del CM, cuyo valor es igual a su SID primario. En este ejemplo, el SAID primario tiene el valor 0x2260.

B.O.I.3.1 Detalles del certificado de CM

Los campos del certificado de CM del mensaje información de autorización anterior se descomponen como sigue:

30 82 02 76	encabezamiento de certificado
30 82 01 df	encabezamiento de tbsCertificate
a0 03 02 01 02	versión
02 08 01 01 01 01 01 01 01 01	número de serie
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	signatura
30 81 88	encabezamiento de expedidor
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común
30 1e	encabezamiento de validez
17 0d 39 39 30 33 32 33 31 36 35 38 33 34 5a	no antes
17 0d 34 39 31 32 33 31 32 33 35 39 35 30 5a	no después
30 72	encabezamiento de asunto
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 15 30 13 06 03 55 04 03 13 0c 30 30 30 30 30 30 31 32 33 34 35 36	nombre común (número de serie)
31 1a 30 18 06 03 55 04 03 13 11 30 30 3a 30 30 3a 43 41 3a 30 31 3a 30 34 3a 30 31	nombre común (dirección MAC)
30 81 9f	encabezamiento de información de clave pública de asunto

30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	tipo de algoritmo de clave pública
03 81 8d 00 30 81 89	encabezamiento de clave pública
02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31	módulo de clave pública
02 03 01 00 01	exponente de clave pública
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	algoritmo de signatura
03 81 81 00 19 b0 2b e5 2c 37 4a af 34 cb c9 59 62 68 88 05 8a 91 5b d4 c6 fa 2e 19 ab 98 42 33 68 9d fc e4 76 23 84 8d 4a be ff bf 34 cf e0 fb 93 96 01 8b 89 d9 86 42 5e cf 6d e6 68 2e 44 99 56 6a cc f1 2c b9 5b 30 21 08 22 f5 11 b1 38 ba 6e b5 62 f0 3a dc f1 2e c4 61 95 2f 16 c8 27 63 b6 e8 69 a6 1c e1 4f 1a 8c 65 cb 57 5e 13 ce db 7f 27 f9 c1 6e bf 2f 75 77 9e a9 87 19 c9 f1 dc 30 b8 d3 d5	valor de signatura

Algunos de los campos de este ejemplo son los mismos en todos los certificados de CM.

Dichos campos son:

- versión: v3
- signatura: SHA-1 con RSA, parámetros nulos
- primer nombre de unidad organizacional del expedidor: " J.112 annex B"
- tipo de algoritmo de clave pública: criptación RSA, parámetros nulos
- exponente de clave pública: entero de 3 octetos de valor 0x10001
- algoritmo de signatura: SHA-1 con RSA, parámetros nulos.

El nombre del expedidor del certificado de CM concuerda con el nombre del asunto del certificado de CA. En este ejemplo, los campos nombre de expedidor concordantes son:

- nombre de país: "US"
- nombre de organización: "Nortel"
- primer nombre de unidad organizacional: "J.112 Annex B"
- segundo nombre de unidad organizacional: "Building 1, Andover MA"
- nombre común: "Nortel Cable Modem Root Certificate Authority".

Los otros campos son ejemplos de valores. Algunos de éstos son:

- número de serie: entero de 8 octetos de valor 0x0101010101010101. Otros certificados de CM pueden utilizar una longitud diferente
- no antes: 1999-03-23 16:58:34 GMT
- no después: 2049-12-31 23.59.50 GMT
- nombre de país del asunto: "US"
- nombre de organización del asunto: "Nortel"
- nombre de unidad organizacional del asunto: "Building 1, Andover MA"

- nombre común del asunto (número de serie): "000000123456". Otros certificados de CM pueden utilizar una cadena de longitud diferente. El valor concuerda con el atributo número de serie del mensaje petición de autorización
- segundo nombre común del asunto (dirección MAC): "00:00:CA:01:04:01". Todos los certificados de CM utilizan una cadena de esta longitud. El valor concuerda con el atributo dirección MAC del mensaje petición de autorización
- módulo de clave pública: entero de 1024 bits de longitud y valor 0x00e0e0 ... d631. Otros certificados de CM pueden utilizar un entero de longitud 768 o 1024 bits
- valor de signatura: cadena de bits de 1024 bits de longitud que representa el valor entero 0x0019b0 ... d3d5. Otros certificados de CM pueden utilizar una cadena de bits de 1024 a 2048 bits de longitud, inclusive; la longitud concuerda con la del módulo del expedidor. La signatura se calcula en la porción del certificado que comienza con el encabezamiento de tbsCertificate y termina con el exponente de clave pública, inclusive.

B.O.I.4 Respuesta de autorización

El CMTS envía la respuesta de autorización siguiente:

05 72 00 9f	Encabezamiento de respuesta de autorización
07 00 80 a2 cb ad c8 34 27 71 47 06 d5 10 0c 07 94 90 bf e6 44 1b 0c 90 0d b4 ed 9c 39 aa 05 a0 c1 ef 54 4b cc fb 3a 7a 22 81 c0 dc c6 6e 39 a4 91 1c ba bf b0 ed 47 10 f2 f4 13 f9 09 33 c6 ae a3 45 67 c8 38 0f c3 9a 12 be d5 27 27 39 77 fb 98 03 39 50 39 99 f5 b6 ad b5 85 f9 16 d0 ff c6 2a ff 9f 38 73 6f 35 44 21 ad 9e e1 a5 91 4d 34 06 1d bb c9 b6 8f 8a 17 9e be c6 c9 40 eb 81 f0 62 d8 18	Clave de autorización
09 00 04 00 09 3a 80	Tiempo de vida de la clave
0a 00 01 07	Número de secuencia de clave
17 00 0e	Encabezamiento de descriptor de SA
0c 00 02 22 60	SAID
18 00 01 00	Tipo de SA
14 00 02 01 00	Serie criptográfica

El campo código tiene el valor 0x05, lo que identifica esto como un paquete respuesta de autorización. El campo identificador tiene el valor 0x72, que concuerda con el campo identificador de la petición de autorización. El campo longitud tiene el valor 0x009f (159), que es el número de octetos que siguen al campo longitud.

El primer atributo es la clave de autorización. Este atributo contiene una clave de autorización que ha sido criptada según RSA utilizando la clave pública del mensaje petición de autorización. La clave de autorización criptada según RSA es un entero formado por 0x80 (128) octetos. En este ejemplo, el valor de la clave de autorización criptada según RSA es:

0xa2cbadc8 ... f062d818.

Se señala que 0xa2 es el octeto más significativo de la clave de autorización con criptación RSA y 0x18 es el octeto menos significativo. Más adelante se dan detalles relativos al cálculo de la criptación RSA.

El segundo atributo es el tiempo de vida de la clave. En este ejemplo, su valor es 0x00093a80 (604800) segundos, o 7 días.

El tercer atributo es el número de secuencia de clave. En este ejemplo, su valor es 0x07.

Los atributos restantes son descriptores de SA. Cada descriptor de SA es un atributo compuesto formado por los subatributos siguientes: SAID, tipo de SA y serie criptográfica. En este ejemplo se incluye sólo un descriptor de SA, correspondiente al SAID de la petición de autorización. El tipo de SA es primario, y la serie criptográfica es DES de 56 bits sin autenticación.

El CM y el CMTS obtienen, cada uno de ellos, una clave de criptación de claves y dos claves de autenticación de mensajes a partir de la clave de autorización, utilizando el proceso de troceo. Más adelante se dan detalles a propósito de los cálculos del troceo. Los valores de las claves de este ejemplo son como sigue:

Clave de autorización	4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Clave de encriptación de claves	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62
Clave de autenticación de mensajes, sentido ascendente	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Clave de autenticación de mensajes, sentido descendente	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

B.O.I.4.1 Detalles de la criptación según RSA

El CMTS genera una clave de autorización aleatoria de 20 octetos. En este ejemplo, el valor de la clave de autorización es:

```
4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
```

La clave de autorización se cripta utilizando el esquema RSAES-OAEP de [RSA2]. En esta cláusula se dan detalles del esquema aplicado en el presente ejemplo. El esquema utiliza una función generadora de máscaras (MGF, *mask-generation function*) que se basa en el troceo; en una cláusula posterior se dan detalles al respecto.

La clave de autorización se inserta en un bloque DB de 107 octetos:

```
DB =

da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 60 18 90 af d8 07 09 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 01 42 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0
bc ob 75
```

Para formar DB la clave de autorización se prologa con un octeto de valor 1, y el resultado se coloca en los 21 últimos octetos del bloque. Los 20 primeros octetos del bloque son el resultado de efectuar una operación de troceo en una cadena de longitud 0; estos 20 octetos tienen el mismo valor en cada respuesta de autorización y no son exclusivos del presente ejemplo. Los 66 octetos restantes del bloque se fijan a 0.

El CMTS genera una cadena aleatoria de 20 octetos llamada SEED (semilla). La SEED se genera de manera independiente para cada respuesta de autorización. En este ejemplo, la SEED tiene el valor siguiente:

```
SEED =


ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d
```

La SEED es la entrada a la MGF para generar DB_MASK, un bloque de 107 octetos:

```
DB_MASK =

de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 db 13 7b a6 3b 37 ac 86 06 7c b5
ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17
23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76
c 3f 6e ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c ca 04 a1 af
c7 c4 62
```

A DB y DB_MASK se les aplica conjuntamente el operador lógico OR exclusivo para producir MASKED_DB, que tiene 107 octetos:

```
MASKED_DB =

04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5
ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17
23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76
cc 3f 6e ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f
7b cf 17
```

MASKED_DB la entrada a la MGF para generar SEED_MASK, un bloque de 20 octetos:

```
SEED_MASK =


b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82
```

A SEED y SEED_MASK se les aplica conjuntamente el operador lógico OR exclusivo para producir MASKED_SEED, que tiene 20 octetos:

```
MASKED_SEED =


19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef
```

MASKED_SEED y MASKED_DB están concatenadas, y el resultado se prologa con un solo octeto de valor 0. Con ello se obtiene un bloque de 128 octetos llamado EM:

```
EM =


00 19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef 04 29 6a b7 1f
a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e
01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1
4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99
3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

Para efectuar la criptación según RSA, EM se interpreta como el valor entero:

0x00192a5e32 ... 5f7bcf17.

Se señala que 0x00 es el octeto más significativo y 0x17 es el octeto menos significativo.

La criptación RSA se efectúa como la operación $Y = M^E$ módulo N, donde:

M es el valor entero del bloque EM (0x00192a5e32 ... 5f7bcf17); E es el valor entero del exponente de la clave pública RSA (0x010001); N es el valor entero del módulo de la clave pública RSA (oxe0e06c8d ... caeed631), e Y es el valor entero de la clave de autorización criptada según RSA (0xa2cbadc8 ... f062d818).

B.O.I.4.2 Detalles de la descriptación según RSA

El cuadro que figura a continuación contiene la lista de parámetros de clave privada que concuerdan con los de la clave pública RSA en el mensaje petición de autorización del ejemplo:

Parámetro	Propiedad	Valor
D (exponente privado)	M^{DE} módulo N = M	6b 1f 1d 36 ec 77 7b 15 a9 c6 30 27 71 ae 92 62 3a 9f 67 47 d8 00 9d ca 0 0b f9 a6 0d be 54 3d 5a 6e be 25 25 bc d9 67 da 7b 80 5f a1 c6 75 67 dd 84 ba 4b 16 26 ba e9 fd 61 ab cd 49 e0 18 47 37 9f 56 08 2d d9 16 81 ff 7d d0 7e 01 8f d4 84 d3 e8 eb 27 48 c3 6c dc a9 01 b7 e5 24 28 d1 6c 67 03 a7 63 fb fa 79 d8 08 6a e1 de 3d 12 7a 36 20 25 01 d1 08 11 0c cd 80 44 3c fd c5 c4 db d1
P (factor primo)	N = PQ	f1 6b dd 2f dd d8 df 80 30 e6 9c d3 4e 46 5e 9f 42 62 b1 66 86 57 1b ca 87 9c cf fd 1c b6 26 76 95 35 bf 0b fb 51 af 0f 46 1c 5e cb 82 a0 83 bf 46 c9 3b d6 4e 7a 5d bf 03 05 69 27 31 6d 65 bd
Q (factor primo)	N = PQ	ee 74 cb a3 d0 90 2d 8a e9 e7 10 dd b4 65 2e 91 22 09 52 72 ab bd 32 31 4e d7 d0 2b 4b 13 57 20 6b f9 a4 57 b1 47 59 67 86 a6 8c 2c c1 f3 8b ba 8a 6b b1 62 5d 43 5a 71 db d0 33 43 97 99 17 85
D_p (exponente del CRT)	D_p = D módulo (P – 1)	a6 35 dc d2 57 aa 38 35 c9 74 fc 03 7e a0 74 04 b1 6f c1 33 14 ca 64 17 cb c5 ea 6c 18 98 4f 62 d4 d7 6b f0 93 d6 68 ef db 15 2d 2e 6f 80 93 33 dd 48 2e 2a 1d 5d a1 ad 20 27 59 7d e2 49 af 01
D_q (exponente del CRT)	D_q = D módulo (Q – 1)	cf f1 9c 30 33 cd b7 59 7f 96 57 f7 ee bb 99 bb 48 a2 36 7a f7 57 1a f1 32 df 32 92 be 7a 94 2d 1a db ed bb e7 45 e0 2a 4e 9a e8 7c 93 7a 4e 2c 93 4f 4c b6 09 bc 95 9f da df 9a 04 e4 ab c5 7d
U_p (Constante del CRT)	PU_p módulo Q = 1	08 17 0c 11 bc aa 2f 96 80 8b 31 95 6d 2e b8 3c ee 2e 05 88 ab 9e fc 53 24 c4 04 b8 7e 1d 01 db 2d f2 2c 06 b0 cd 04 6b 1c 14 d8 d0 4f c9 a0 ae 1b c9 80 88 be 42 0a 52 4a ef 62 3c 8b dd c5 37

Cada valor del cuadro representa los octetos de un entero, mostrándose en primer lugar el octeto más significativo. Por ejemplo, el exponente privado D tiene el valor entero:

0x6b1f1d36 ... c5c4dbd1.

El CM puede descriptar la clave de autorización utilizando o no el teorema del resto chino (CRT, *chinese remainder theorem*). La descriptación con el CRT es más complicada, pero puede resultar una operación más rápida.

Para descriptar sin utilizar el CRT, el CM efectúa la operación $M = Y^D$ módulo N. D es el exponente privado del cuadro, e Y y N se describen en la cláusula precedente. El valor resultante concuerda con el valor de M de la cláusula precedente, es decir, es el valor entero del bloque EM formado por el CMTS. El CM decodifica la clave de autorización a partir del EM invirtiendo el procedimiento utilizado por el CMTS para formar el EM, como se describe en [RSA2].

Para descriptar utilizando el CRT, el CM calcula primero dos cantidades intermedias:

$$A = Y^{Dp} \mathrm{mod}\ P$$

$$B = Y^{Dq} \mathrm{mod}\ Q$$

P y Q son los factores primos del módulo, y D_p y D_q son exponentes privados relacionados con esos factores, todos ellos con los valores mostrados en el cuadro. El CM calcula el valor de M de la manera siguiente:

$$M = A + ((B - A)U_p \text{ módulo } Q)P$$

U_p es una constante derivada de los factores primos, cuyo valor se muestra en el cuadro. El valor resultante de M concuerda con el valor que se hubiera calculado utilizando la fórmula $M = Y^D$ módulo N.

B.O.I.4.3 Detalles del troceo

La clave de autorización se trocea utilizando el algoritmo SHA-1 [FIPS 180-1] para producir la clave de criptación de claves (KEK), la clave de autenticación de mensajes para el sentido ascendente y la clave de autenticación de mensajes para el sentido descendente.

En el análisis que aquí se hace se representa un cálculo de troceo utilizando un cuadro que muestra la entrada a la función de troceo y el valor de troceo resultante. A continuación se muestra, para referencia, un cuadro que describe el ejemplo del apéndice B de [FIPS 180-1]:

Entrada al troceo	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
Valor del troceo	84 98 3e 44 1c 3b d2 6e ba ae 4a a1 f9 51 29 e5 e5 46 70 f1

B.O.I.4.3.1 KEK

La KEK se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62 b0 df e6 3b

La entrada es el octeto 0x53, repetido 64 veces, seguido por los 20 octetos de la clave de autorización. El orden en que los octetos de la clave de autorización son compendiados es el mismo en que aparecen en el bloque de criptación EM.

El valor del troceo tiene una longitud de 20 bytes. Los 16 primeros bytes son la KEK.

B.O.I.4.3.2 Claves de autenticación de mensajes

La clave de autenticación de mensajes en sentido ascendente se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7

La entrada es el octeto 0x5c, repetido 64 veces, seguido por los 20 octetos de la clave de autorización. El orden en que los octetos de la clave de autorización son compendiados es el mismo que en el cálculo de la KEK.

El valor del troceo tiene una longitud de 20 octetos. Los 20 octetos forman la clave de autenticación de mensajes en sentido ascendente.

La clave de autenticación de mensajes en sentido descendente se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

Esto es similar al cálculo en el caso del sentido ascendente, con la salvedad de que el valor 0x3a sustituye al valor 0x5c.

B.O.I.4.3.3 Función de generación de máscaras

La función de generación de máscaras (MGF) se construye a partir de las operaciones de troceo de SHA-1. Cada operación de troceo genera 20 octetos de datos de máscara. El número de operaciones de troceo efectuadas depende del tamaño de la máscara que se necesite.

La cantidad SEED_MASK se forma aplicando la MGF a MASKED_DB. Puesto que SEED_MASK tiene una longitud de 20 octetos, sólo se necesita una función de troceo:

Entrada al troceo	04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17 00 00 00 00
Valor del troceo	b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82

Los datos de entrada a la operación de troceo son el MASKED_DB de 107 octetos seguido por 4 octetos de valor 0. La salida de la operación de troceo es el valor de SEED_MASK.

La cantidad DB_MASK se forma aplicando la MGF a SEED. Puesto que DB_MASK tiene una longitud de 107 octetos, hacen falta seis operaciones de troceo:

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 00
Valor del troceo	de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 bd 13 7b a6 3b

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 01
Valor del troceo	37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 02
Valor del troceo	a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 03
Valor del troceo	9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 04
Valor del troceo	6e ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 05
Valor del troceo	ca 04 a1 af c7 c4 62 3a df 6f 33 ec e2 cd 2c 7f b7 7e 48 19

Los datos de entrada a cada operación de troceo son los 20 octetos de SEED seguidos por un valor de cuatro octetos. El valor de cuatro octetos cuenta los valores enteros 0, 1, 2, 3, 4, 5 en operaciones de troceo sucesivas. Las salidas de las seis operaciones de troceo se concatenan en un resultado de 120 octetos, y los primeros 107 octetos del resultado constituyen DB_MASK.

B.O.I.5 Petición de clave

El CM envía la petición de clave siguiente:

07 73 00 d0	Encabezamiento de petición de clave
05 00 ad	Encabezamiento de identificación de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Número de serie
02 00 03 25 53 41	ID de fabricante

03 00 06 00 00 ca 01 04 01	Dirección MAC
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clave pública RSA
0a 00 01 07	Número de secuencia de clave
0c 00 02 22 60	SAID
0b 00 14 86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e	Compendio de HMAC

El campo código tiene el valor 0x07, lo que identifica esto como un paquete petición de clave. El campo identificador tiene el valor 0x73; se trata de un valor de ejemplo, obtenido incrementando el valor del identificador de la petición de autorización. El campo longitud tiene el valor 0x00d0 (208), que es el número de octetos que siguen al campo longitud.

El primer atributo es la identificación de CM. Es un atributo compuesto, idéntico al de la petición de autorización.

El segundo atributo es el número de secuencia de clave, que identifica la clave de autorización. El valor es idéntico al de la respuesta de autorización.

El tercer atributo es el SAID para el que se está pidiendo una clave. Este valor de SAID estaba contenido en la respuesta de autorización.

El atributo final es el compendio de HMAC. El compendio consta de 20 octetos. Se calcula utilizando la clave de autenticación de mensajes en sentido ascendente. El compendio se efectúa con todos los octetos del paquete petición de clave, excluyendo los 23 octetos del propio atributo compendio de HMAC. A continuación se dan detalles del cálculo del compendio.

B.O.I.5.1 Detalles del compendio de HMAC

El compendio de HMAC se calcula utilizando el método de autenticación de HMAC definido en [RFC 2104], con SHA-1 como función de troceo. En [RFC 2202] se presentan ejemplos de cálculo de HMAC utilizando SHA-1.

En el análisis que aquí se hace se representa un cálculo de HMAC utilizando un cuadro que muestra la clave, la entrada a la función HMAC y el compendio de HMAC resultante. A continuación se muestra, para referencia, un cuadro que describe el caso de prueba #2 de los ejemplos de HMAC-SHA-1 en [RFC 2202]:

Clave	4a 65 66 65
Entrada a HMAC	77 68 61 74 20 64 6f 20 79 61 20 77 61 6e 74 20 66 6f 72 20 6e 6f 74 68 69 6e 67 3f
Compendio de HMAC	ef fc df 6a e5 eb 2f a2 d2 74 16 d5 f1 84 df 9c 25 9a 7c 79

El compendio de HMAC del paquete petición de clave se computa aplicando el cálculo de HMAC siguiente:

Clave	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Entrada a HMAC	07 73 00 d0 05 00 ad 01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36 02 00 03 25 53 41 03 00 06 00 00 ca 01 04 01 04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01 0a 00 01 07 0c 00 02 22 60
Compendio de HMAC	86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e

La clave es la clave de autenticación de mensajes en sentido ascendente. La entrada consta de todos los octetos del paquete petición de clave, excluyendo el atributo compendio de HMAC. Los octetos del compendio son el contenido del atributo compendio de HMAC.

B.O.I.6 Respuesta de clave

El CMTS envía la respuesta de clave siguiente:

08 73 00 68	Encabezamiento de respuesta de clave
0a 00 01 07	Número de secuencia de clave (clave de autorización)
0c 00 02 22 60	SAID
0d 00 21	Encabezamiento de parámetros de TEK
08 00 08 b6 4d 54 8c 3f 6b 25 69	Clave de TEK
09 00 04 00 00 a8 c0	Tiempo de vida de la clave
0a 00 01 02	Número de secuencia de clave (TEK)
0f 00 08 81 0e 52 8e 1c 5f da 1a	IV CBC DES
0d 00 21	Encabezamiento de parámetros de TEK
08 00 08 5e bd 03 aa 5e d5 e2 94	Clave TEK
09 00 04 00 01 51 80	Tiempo de vida de la clave
0a 00 01 03	Número de secuencia de clave (TEK)
0f 00 08 25 35 67 c3 09 21 8c 2c	IV CBC DES
0b 00 14 a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02	Compendio de HMAC

El campo código tiene el valor 0x08, lo que identifica esto como un paquete respuesta de clave. El identificador tiene el valor 0x73, que concuerda con el valor de la petición de clave. El campo longitud tiene el valor 0x68 (104), que es el número de octetos que siguen al campo longitud.

El atributo número de secuencia de clave identifica la clave de autorización. Concuerda con el valor de la petición de clave.

El atributo SAID identifica el SAID para el que se está suministrando una TEK. Concuerda con el valor de la petición de clave.

Se incluyen dos atributos parámetros de TEK, el primero para la generación más antigua de parámetros de clave y el segundo para la más reciente. Cada atributo parámetros de TEK es un atributo compuesto formado por los subatributos siguientes: clave TEK, tiempo de vida de la clave, número de secuencia de clave y vector de inicialización (IV) de encadenamiento de bloques cifrados (CBC) de DES.

La clave TEK consta de 8 octetos. Contiene la TEK, criptada utilizando ECB de DES triple con la KEK obtenida a partir de la clave de autorización. Más adelante se dan detalles sobre el cálculo de ECB de DES triple.

El subatributo tiempo de vida de la clave se refiere a la TEK. En este ejemplo, el valor para la TEK más antigua es 0x0000a8c0 (43200) segundos, o 12 horas, y el valor para la TEK más reciente es 0x00015180 (86400) segundos, o 24 horas.

El subatributo número de secuencia de clave identifica la TEK. En este ejemplo, el valor para la TEK más antigua es 0x02, y el valor para la TEK más reciente es 0x03.

El subatributo IV CBC DES (vector de inicialización del encadenamiento de bloques cifrados de la norma DES) consta de 8 octetos. Especifica el vector de inicialización que se ha de utilizar con la TEK.

El atributo final es el compendio de HMAC. Consta de 20 octetos. Se calcula de manera similar a la de la respuesta de clave, con la salvedad de que se utiliza la clave de autenticación de mensajes en sentido descendente en vez de la clave en sentido ascendente. Más adelante se dan detalles sobre el cálculo de HMAC.

Una vez que el CM ha procesado el paquete respuesta de clave, el CM y el CMTS comparten dos generaciones de TEK e IV. Los valores de estos parámetros para el presente ejemplo son como sigue:

TEK más antigua	e6 60 0f d8 85 2e f5 ab
IV más antiguo	81 0e 52 8e 1c 5f da 1a
TEK más reciente	b1 d7 4f c9 64 68 f7 58
IV más reciente	25 35 67 c3 09 21 8c 2c

B.O.I.6.1 Detalles de la criptación de EK

El CMTS genera una TEK aleatoria de 8 octetos. En este ejemplo, el valor de la TEK es:

```
e6 60 0f d8 85 2e f5 ab.
```

Ésta es la primera TEK del mensaje respuesta de clave.

La TEK se cripta utilizando encriptación DES-ECB triple. La clave de criptación es la KEK:

```
76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62.
```

La criptación DES-ECB triple se describe aquí en términos de varias iteraciones de criptación o descriptación DES-ECB. DES-ECB se define en [FIPS 81].

En el análisis que aquí se hace se representa una operación de criptación o descriptación DES-ECB utilizando un cuadro que muestra la clave, la entrada y la salida. A continuación se muestran, para referencia, los cuadros que describen el ejemplo del cuadro B1 de [FIPS 81]:

Modo	Criptación ECB
Clave	01 23 45 67 89 ab cd ef
Entrada a DES	4e 6f 77 20 69 73 20 74
Salida de DES	3f a4 0e 8a 98 4d 48 15

Modo	Descriptación ECB
Clave	01 23 45 67 89 ab cd ef
Entrada a DES	3f a4 0e 8a 98 4d 48 15
Salida de DES	4e 6f 77 20 69 73 20 74

NOTA – En [FIP 81] se pide que el bit menos significativo de cada octeto de la clave se ajuste de manera que el octeto tenga paridad impar. Esto es evidente en la clave del ejemplo anterior. El protocolo BPKM no precisa paridad impar. BPKM genera y distribuye claves DES de 8 octetos de paridad arbitraria, y requiere que las implementaciones ignoren el valor del bit menos significativo de cada octeto.

La TEK se cripta según DES-ECB triple utilizando las tres operaciones DES-ECB siguientes:

Modo	Criptación ECB
Clave	76 b4 d4 2f 14 98 59 6a
Entrada a DES	e6 60 0f d8 85 2e f5 ab
Salida de DES	c3 94 31 f5 8d f9 1d bf

Modo	Descriptación ECB
Clave	ab fe 72 94 15 7c 7d 62
Entrada a DES	c3 94 31 f5 8d f9 1d bf
Salida de DES	44 b0 94 4e ab 04 4c 23

Modo	Criptación ECB
Clave	76 b4 d4 2f 14 98 59 6a
Entrada a DES	44 b0 94 4e ab 04 4c 23
Salida de DES	b6 4d 54 8c 3f 6b 25 69

La primera y tercera operaciones son criptación DES-ECB; la clave para cada una de ellas son los ocho primeros octetos de la KEK. La segunda operación es descriptación DES-ECB; la clave son los últimos ocho octetos de la KEK. La entrada a la primera operación es la TEK que ha de ser criptada. La entrada a la segunda operación es la salida de la primera, y la entrada a la tercera es la salida de la segunda. La salida de la tercera operación es la TEK criptada; esto se lleva en el subatributo clave TEK del mensaje respuesta de clave.

B.O.I.6.2 Detalles del HMAC

El compendio de HMAC del paquete respuesta de clave se calcula aplicando un método similar al del paquete petición de clave. La clave es la clave de autenticación de mensajes en sentido descendente. A continuación se indican los detalles del cálculo de HMAC:

Clave	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd
Entrada a HMAC	08 73 00 68 0a 00 01 07 0c 00 02 22 60 0d 00 21 08 00 08 b6 4d 54 8c 3f 6b 25 69 09 00 04 00 00 a8 c0 0a 00 01 02 0f 00 08 81 0e 52 8e 1c 5f da 1a 0d 00 21 08 00 08 5e bd 03 aa 5e d5 e2 94 09 00 04 00 01 51 80 0a 00 01 03 0f 00 08 25 35 67 c3 09 21 8c 2c
Compendio de HMAC	a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02

B.O.I.7 Criptación de PDU paquete

Los 12 primeros octetos de la PDU paquete, que contienen las direcciones de destino y origen (DA/SA, *destination and source addresses*) Ethernet/802.3, no son criptados. Los restantes octetos de la PDU paquete se criptan utilizando el modo DES-CBC con un tratamiento especial de los bloques de terminación residuales que tienen menos de 64 bits. La combinación DES-CBC y procesamiento de bloques residuales garantiza el que la criptación no cambie la longitud del paquete. La clave de criptación es la TEK correspondiente al número de secuencia de clave del encabezamiento ampliado de privacidad del paquete.

La especificación describe el procesamiento del bloque residual como sigue:

"Dado un bloque final que tiene n bits, siendo n inferior a 64, el penúltimo bloque de texto cifrado se cripta aplicando DES una segunda vez, el modo ECB, y a los n bits menos significativos del resultado se les aplica el operador lógico OR exclusivo con los n bits finales de la cabida útil para generar el bloque cifrado final corto. ... En el caso especial de que la cabida útil de la PDU datos por paquetes sea inferior a 64 bits, el vector de inicialización se cripta aplicando DES, y a los n bits situados más a la izquierda del texto cifrado resultante, correspondientes al número de bits de la cabida útil, se les aplica el operador lógico OR exclusivo con los n bits de la cabida útil para generar el bloque cifrado corto."

Una descripción alternativa de este procedimiento, que equivale a la descripción de la especificación, es como sigue:

Dado un bloque final que tiene n bits, siendo n inferior a 64, se añaden bits de relleno a los n bits hasta formar un bloque de 64 bits agregando 64-n bits de un valor cualquiera a la derecha de los n bits de la cabida útil. El bloque resultante se cripta según DES utilizando el modo CFB64, en donde el penúltimo bloque de texto cifrado actúa como vector de inicialización de la operación CFB64. Los n bits situados más a la izquierda del texto cifrado resultante se utilizan como bloque cifrado corto. ... En el caso especial de que la cabida útil de la PDU datos por paquetes sea inferior a 64 bits, el procedimiento es el mismo que para un bloque final corto, con el vector de inicialización proporcionado sirviendo como vector de inicialización de la operación DES-CFB64.

La descripción alternativa produce el mismo texto cifrado que la descripción de la especificación. En la descripción alternativa, no obstante, no se menciona la combinación de criptación ECB con la aplicación de un operador lógico OR exclusivo. Estas operaciones son operaciones internas de CFB64, al igual que lo son de CBC. La descripción alternativa conviene aquí porque permite que el procesamiento del bloque residual se ilustre utilizando ejemplos de CFB64 de [FIPS 81].

La PDU paquete incluye la dirección de destino (DA), la dirección de origen (SA) y los campos tipo/longitud. En los ejemplos que se presentan aquí no se hace ningún esfuerzo por utilizar valores correctos para esos campos. Como resultado de ello, los ejemplos no son paquetes válidos, adecuados para la transmisión. El propósito de los ejemplos es ilustrar los detalles de la criptación solamente.

En estos ejemplos, la TEK y el IV se toman del ejemplo de paquete respuesta de clave descrito más arriba.

B.O.I.7.1 CBC solamente

Cuando el número de octetos que se han de criptar es un múltiplo de 8, el modo de criptación es el DES-CBC definido en [FIPS 81]. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

En el análisis que aquí se hace se representa una criptación DES-CBC utilizando un cuadro que muestra la clave, el IV, la entrada de texto en claro y la salida de texto cifrado. A continuación se muestra, para referencia, un cuadro que describe el ejemplo del cuadro C1 de [FIPS 81]:

Modo	CBC
Clave	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Texto en claro	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Texto cifrado	e5 c7 cd de 87 2b f2 7c 43 e9 34 00 8c 38 9c 0f

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b
CRC	88 41 65 06

La criptación DES-CBC se efectúa como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 88 41 65 06
Texto cifrado	0d da 5a cb d0 5e 55 67 9f 04 d1 b6 41 3d 4e ed

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	0d da
Datos de usuario	5a cb d0 5e 55 67 9f 04 d1 b6
CRC	41 3d 4e ed

B.O.I.7.2 CBC con procesamiento de bloque residual

Cuando el número de octetos que se han de criptar es superior a 8 y no es un múltiplo de 8, el modo de criptación es una combinación de DES-CBC y DES-CFB64.

La criptación empieza en el modo DES-CBC. El modo DES-CBC se utiliza para procesar todos los bloques DES completos que estén presentes. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

Después de la criptación DES-CBC, hay 1 a 7 octetos que no han sido criptados. Estos octetos se criptan utilizando el modo DES-CFB64. El modo DES-CFB64 es "el modo realimentación de cifrado de 64 bits", definido en [FIPS 81]. La clave de criptación está en el paquete respuesta de clave. El vector de inicialización (IV) son los 8 últimos octetos del texto cifrado producido por el procesamiento DES-CBC.

En el análisis que aquí se hace se representa una criptación DES-CFB64 utilizando un cuadro que muestra la clave, el IV, la entrada de texto en claro y la salida de texto cifrado. A continuación se presenta, para referencia, un cuadro que describe el ejemplo del cuadro D3 [FIPS 81]:

Modo	CFB64
Clave	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Texto en claro	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Texto cifrado	f3 09 62 49 c7 f4 6e 51 a6 9e 83 9b 1a 92 f7 84

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

El número total de octetos que se han de criptar es 19. Los 16 primeros octetos se procesan utilizando criptación DES-CBC, y los 3 últimos octetos utilizando criptación DES-CFB64.

La criptación DES-CBD se efectúa como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Texto cifrado	0d da 5a cb d0 5e 55 67 51 47 46 86 8a 71 e5 77

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	51 47 46 86 8a 71 e5 77
Texto en claro	d2 d1 9f 00 00 00 00 00
Texto cifrado	ef ac 88 e8 ee 80 33 14

La clave es la misma que se utiliza para la operación criptación DES-CBC. El IV son los 8 últimos octetos del texto cifrado generado por la operación DES-CBC.

Se señala que se han agregado 5 octetos de valor 0 a los 3 octetos de texto en claro. Los valores de estos octetos de texto en claro agregados no afectan a los valores de los tres primeros octetos de texto cifrado, que son los únicos octetos de texto cifrado que interesan. Se pueden utilizar cualesquiera otros valores en vez de 0 para los octetos de texto en claro agregados.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/Longitud	0d da
Datos de usuario	5a cb d0 5e 55 67 51 47 46 86 8a 71 e5
CRC	77 ef ac 88

B.O.I.7.3 Trama runt

Cuando el número de octetos que se han de criptar es inferior a 8, el modo de criptación es DES-CFB64. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02
CRC	88 ee 59 7e

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto claro	00 01 02 88 ee 59 7e 00
Texto cifrado	17 86 a8 03 a0 85 75 01

Se señala que se ha agregado 1 octeto de valor 0 a los 7 octetos de texto en claro. El valor de este octeto de texto en claro agregado no afecta a los valores de los 7 primeros octetos de texto cifrado,

que son los únicos octetos de texto cifrado que interesan. Se puede utilizar cualquier otro valor en vez de 0 para el octeto de texto en claro agregado.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	17 86
Datos de usuario	a8
CRC	03 a0 85 75

B.O.I.7.4 Clave de 40 bits

El protocolo BPKM genera y distribuye siempre claves DES de 56 bits. Cuando se requiere criptación de 40 bits, la clave DES de 56 bits se convierte, dentro de una implementación, en una clave de 40 bits enmascarando (a cero) 16 de los 56 bits de una TEK.

La TEK tiene 8 octetos, cada uno de los cuales contiene 7 bits de clave y 1 bit de paridad. El procedimiento de conversión de una TEK en una clave de 40 bits es como sigue:

- los dos primeros octetos de la TEK se fijan a 0;
- los dos bits más significativos del tercer octeto de la TEK se fijan a 0;
- los cinco octetos restantes de la TEK permanecen inalterados.

Por ejemplo, si la TEK distribuida por el protocolo BPKM es:

```
ff ff ff ff ff ff ff ff,
```

la conversión a 40 bits genera la TEK

```
00 00 3f ff ff ff ff ff.
```

Excepto por lo que se refiere a esta conversión del valor de la TEK, el procedimiento de criptación de 40 bits de una PDU paquete es idéntico al caso de criptación de 40 bits.

Para ilustrar la criptación de 40 bits, se repite aquí un ejemplo previo de PDU paquete, con la TEK convertida a 40 bits.

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

El número total de octetos que se han de criptar es 19. Los 16 primeros octetos se procesan utilizando criptación DES-CBC, y los tres últimos octetos utilizando criptación DES-CFB64.

La criptación DES-CBD se efectúa como sigue:

Modo	CBC
Clave	00 00 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Texto cifrado	44 c8 4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e 86

La clave es la TEK llevada en el mensaje respuesta de clave, convertida en una clave de 40 bits. El IV es tal como se lleva en el mensaje respuesta de clave.

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	00 00 0f d8 85 2e f5 ab
IV	dc 64 8f b0 dc 1e 1e 86
Texto en claro	d2 d1 9f 00 00 00 00 00
Texto cifrado	f1 42 aa a3 e4 9b eb 29

La clave es la misma que se utiliza para la operación criptación DES-CBC. El IV son los últimos 8 octetos del texto cifrado generado por la operación DES-CBC.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/Longitud	44 c8
Datos de usuario	4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e
CRC	86 f1 42 aa

B.O.I.8 Criptación de PDU paquete con supresión de encabezamiento de cabida útil

Estos ejemplos muestran cómo se efectúa la criptación de una PDU paquete cuando se aplica supresión de encabezamiento de cabida útil (PHS). El ejemplo utiliza la cabida útil del protocolo de transmisión de la voz por Internet con RTP. En los ejemplos que aquí se presentan no se hace ningún esfuerzo por utilizar valores correctos para los campos de la PDU paquete. Como resultado de ello, los ejemplos no son paquetes válidos, adecuados para la transmisión. El objetivo de los ejemplos es ilustrar los detalles de la criptación solamente.

B.O.I.8.1 Sentido descendente

Supóngase que la PDU paquete, después de la PHS y antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	31 32 33 34 35 36 37 38 39 3a
CRC	93 86 b3 b9

La PHS ha suprimido los campostipo/longitud que, de otro modo, estarían incluidos en el encabezamiento Ethernet/802.3. Los datos de usuario consisten en el encabezamiento de RTP y los datos de voz. La criptación se aplica empezando con el primer octeto del encabezamiento de RTP y terminando con el último octeto de la CRC, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	21 22 23 24 25 26 27 28 29 2a 2b 2c 31 32 33 34 35 36 37 38 39 3a 93 86
Texto cifrado	b4 55 da c8 39 1e 0c ed 15 cf b5 79 0a c3 24 5e cf 0f 52 c0 69 f5 f6 6e

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	cf 0f 52 c0 69 f5 f6 6e
Texto en claro	b3 b9 00 00 00 00 00 00
Texto cifrado	3e 31 de ea 96 6a 88 6b

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Encabezamiento de RTP	b4 55 da c8 39 1e 0c ed 15 cf b5 79
Datos de voz	0a c3 24 5e cf 0f 52 c0 69 f5
CRC	f6 6e 3e 31

B.O.I.8.2 Sentido ascendente

Supóngase que la PDU paquete, después de la PHS y antes de la criptación, es como sigue:

Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	31 32 33 34 35 36 37 38 39 3a
CRC	65 cf fe 89

La PHS ha suprimido la DA, la SA y los campos tipo/longitud que, de otro modo, estarían incluidos en el encabezamiento Ethernet/802.3. Los datos de usuario consisten en el encabezamiento de RTP y los datos de voz. Los primeros 12 octetos de los datos de usuario no son criptados. La criptación se aplica empezando con el primer octeto de los datos de voz y terminando con el último octeto de la CRC, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	31 32 33 34 35 36 37 38
Texto cifrado	d6 88 87 66 1f 66 04 79

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	d6 88 87 66 1f 66 04 79
Texto en claro	39 3a 65 cf fe 89 00 00
Texto cifrado	c0 07 20 8e 3b 0b b1 b9

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	d6 88 87 66 1f 66 04 79 c0 07
CRC	20 8e 3b 0b

B.O.I.9 Criptación de paquete fragmentado

Cuando se fragmenta un paquete, cada fragmento se cripta independientemente utilizando DES-CBC con procesamiento del bloque residual. La TEK y el IV de cada fragmento son los mismos TEK e IV utilizados para criptar una PDU paquete no fragmentado. Se criptan todos los octetos de un fragmento, incluidos los 12 octetos que llevan las direcciones de destino y origen (DA/SA) Ethernet/802.3 de la PDU paquete.

En el ejemplo que aquí se presenta, no se hace ningún esfuerzo por utilizar valores significativos de los campos del paquete. Como resultado de ello, el ejemplo no es un paquete válido, adecuado para la transmisión. El objetivo del ejemplo es ilustrar los detalles de la criptación solamente.

En este ejemplo, la TEK y el IV se toman del ejemplo de paquete respuesta de clave descrito anteriormente.

Supóngase que el paquete se divide en dos fragmentos, como sigue:

Cabida útil del fragmento 1	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03 04 05
CRC del fragmento 1	b4 2b 6d d4

Cabida útil del fragmento 2	06 07 08 09 0a 0b 0c 0d
CRC del fragmento 2	48 34 45 36

El primer fragmento se cripta utilizando DES-CBC y DES-CFB64, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03
Texto cifrado	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	c8 1a 67 4e 26 0c 20 c5
Texto en claro	04 05 b4 2b 6d d4 00 00
Texto cifrado	56 6d 5c 58 2f 56 dc 39

El primer fragmento, después de la criptación, tiene el aspecto siguiente:

Cabida útil del fragmento 1	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5 56 6d
CRC del fragmento 1	5c 58 2f 56

El segundo fragmento se cripta utilizando DES-CBC y DES-CFB64, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	06 07 08 09 0a 0b 0c 0d
Texto cifrado	d8 55 0f 59 9d 19 d9 c6

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	d8 55 0f 59 9d 19 d9 c6
Texto en claro	48 34 45 36 00 00 00 00
Texto cifrado	b4 5f 3e 95 0e e4 d7 df

El segundo fragmento, después de la criptación, tiene el aspecto siguiente:

Cabida útil del fragmento 2	d8 55 0f 59 9d 19 d9 c6
CRC de fragmento 2	b4 5f 3e 95

APÉNDICE B.O.II

Interoperabilidad BPI/BPI+

La privacidad básica plus constituye un perfeccionamiento de los requisitos originales de la privacidad básica que habían sido desarrollados en algunas áreas nacionales para utilizar con la Recomendación J.112 anexo B v1. Aunque la especificación original nunca se presentó al UIT-T, se ha implementado en determinadas zonas. El presente apéndice contiene orientaciones al respecto dirigidas a fabricantes y operadores. La especificación ha introducido las mejoras necesarias para aumentar la seguridad del sistema y tener en cuenta los recelos derivados de la especificación original a propósito de la calidad de funcionamiento. La arquitectura y el diseño originales de la privacidad básica se han mantenido donde ha sido posible.

La evolución de las características de la Recomendación J.112 anexo B v2 y de la privacidad básica plus no tenía por objeto la obsolescencia inmediata de los sistemas de la Recomendación J.112 anexo B v1, ni que dejara de utilizarse la privacidad básica. La transición de los sistemas de módem de cable hacia la conformidad con la Recomendación J.112 anexo B v2 puede hacerse de forma escalonada. Mientras tanto, las unidades de privacidad básica de la Recomendación J.112 anexo B v1 y las de privacidad básica plus de la Recomendación J.112 anexo B v2 pueden coexistir dentro de un sistema de módem de cable.

B.O.II.1 Interoperabilidad de la Recomendación J.112 anexo B v1/v2

Los requisitos de interoperabilidad BPI/BPI+ son un subconjunto de los requisitos de interoperabilidad global de la Recomendación J.112 anexo B v1/v2 definidos en el apéndice G de [la Recomendación J.112 anexo B]. Deberán cumplirse los requisitos de interoperabilidad relativos a aprovisionamiento y registro definidos por [la Recomendación J.112 anexo B].

B.O.II.2 Requisitos de interoperabilidad BPI/BPI+

Los requisitos de interoperabilidad BPI/BPI+ se resumen en el cuadro que sigue. Un sistema de privacidad básica plus DEBERÍA ser retrocompatible con la privacidad básica de acuerdo con ese cuadro. Hay cuatro capacidades unidad definidas aquí a partir de la especificación de la privacidad básica y soportadas por estos requisitos de interoperabilidad.

1) Sistema de terminación de módem de cable

a) CMTS BPI: privacidad básica con DES de 56 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits.

b) CMTS BPI – 40 bits: privacidad básica con DES de 40 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits. DES sólo puede funcionar en el modo 40 bits.

2) Módem de cable

a) CM BPI: privacidad básica con DES de 56 bits, y un módulo de clave pública de 768 bits o 1024 bits.

b) CM BPI – 40 bits: privacidad básica con DES de 40 bits, y un módulo de clave pública de 768 bits o 1024 bits. DES sólo puede funcionar en el modo 40 bits.

Como se define en esta especificación, la privacidad básica plus introduce dos tipos de unidad adicionales.

- CMTS BPI+: privacidad básica plus con DES de 56 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits.
- CM BPI+: privacidad básica plus con DES de 56 bits, y un módulo de clave pública de 1024 bits.

Los requisitos para la interoperabilidad BPI/BPI+ son como sigue:

Un CMTS DEBE aceptar claves públicas con un módulo tanto de 768 bits como de 1024 bits procedente de un CM durante la autorización.

De acuerdo con los requisitos de interoperabilidad de [la Recomendación J.112 anexo B] y la presente especificación, un CMTS con privacidad básica plus DEBE ser capaz de replegarse a un modo de funcionamiento compatible con la privacidad básica.

Cuando un CMTS con privacidad básica plus funcione en un sistema con un CM que sólo tiene capacidad de privacidad básica, el CMTS DEBE replegarse a un modo de funcionamiento compatible con la privacidad básica para las comunicaciones con ese CM.

Cuando un CMTS con privacidad básica plus funcione en un sistema que admite módems de cable (CM) tanto de BPI como de BPI+, el servidor TFTP DEBE incluir ficheros de configuración de la

Recomendación J.112 anexo B v1 y J.112 anexo B v2 para entregar las fijaciones apropiadas de BPI o BPI+ a cada CM.

De acuerdo con los requisitos de interoperabilidad de [la Recomendación J.112 anexo B] y esta especificación, un CM con privacidad básica plus DEBE ser capaz de replegarse a un modo de funcionamiento compatible con la privacidad básica antes de intentar la autorización.

Cuando un CM con privacidad básica plus funcione en un sistema con un CMTS que sólo tiene capacidad de privacidad básica, el CM DEBE replegarse a un modo de funcionamiento con privacidad básica para comunicar con el CMTS.

Cuadro B.O.II-1/J.112 – Matriz de interoperabilidad BPI/BPI+

	CM BPI	**CM BPI -40 bits**	**CM BPI+**
CMTS BPI	Configuración BPI nacional. Módulo RSA de 768 ó 1024 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	El CM se repliega al modo BPI con módulo RSA de 1024 bits
CMTS BPI 40 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	Módulo RSA de 768 ó 1024 bits. Toda la compatibilidad a 40 bits manejada por microplaquetas MAC	El CM se repliega al modo BPI con módulo RSA de 1024 bits. El soporte lógico del CMTS pone a cero bits de TEK hasta la norma de 40 bits
CMTS BPI+	El CMTS se repliega al modo BPI. Módulo RSA de 768 ó 1024 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	Configuración BPI+ completa. Módulo RSA de 1024 bits

B.O.II.3 Consideraciones relativas al modo exportación DES de 40 bits de BPI

La especificación de la privacidad básica plus es retrocompatible con el modo exportación DES de 40 bits de privacidad básica. La carga de la conformidad se sitúa en el CMTS. No todos los vendedores de equipos necesitarán funcionar alguna vez en sistemas con unidades BPI con capacidad de DES de 40 bits. Por ello, la conformidad se deja a criterio de cada fabricante de CMTS. Un CMTS DEBERÍA soportar la retrocompatibilidad con la privacidad básica de DES de 40 bits. Si la soporta, DEBE hacerlo de acuerdo con la presente especificación.

a) Cuando un CMTS envía o recibe datos criptados que circulan entre él mismo y un CM que utiliza DES de 40 bits, el CMTS DEBE poner a cero los bits apropiados de sus TEK antes de criptar o descriptar los datos de tráfico correspondientes. Los bits apropiados de la TEK DEBEN ser puestos a cero de acuerdo con el requisito de TEK de 40 bits de la privacidad básica.

b) Cuando se ha de pasar tráfico criptado entre un CMTS con capacidad de DES de 40 bits solamente y un CM con capacidad de DES de 56 bits, el CMTS DEBE proporcionar una TEK conforme de 40 bits en el mensaje respuesta de clave enviado al CM.

El método que utiliza un CMTS para reconocer los CM de un sistema con capacidad de DES de 56 bits o sólo DES de 40 bits se deja que lo decida cada operador de sistema y cada vendedor de CMTS, de la forma que se acomode lo mejor posible a su propia situación. Una manera de obtener esta información sería conseguirla de los vendedores de CM, en base a los números de serie de los CM, las direcciones MAC, las fechas de fabricación o algún otro mecanismo que permita

efectuar el seguimiento del dispositivo. Una vez recogida la información, debería incorporarse a la base de datos del CMTS de información almacenada en cada uno de los CM.

Una manera alternativa de obtener esa información es mediante una base de información de gestión (MIB) de BPI definida a tal fin.

B.O.II.4 Funcionamiento del sistema

B.O.II.4.1 CMTS con capacidad BPI

Un CMTS con capacidad BPI aprovisionará siempre los módems de cable (CM) utilizando ficheros de configuración TFTP según la Recomendación J.112 anexo B v1 y fijaciones de configuración de BPI. Los CM tanto de BPI como de BPI+ recibirán las fijaciones BPI y cada CM sólo tratará de registrarse como un CM de la versión 1 de aquel anexo con capacidad de BPI. Si un CM indica una capacidad de módem BPI+ en la petición de registro, el CMTS responderá con esa capacidad eliminada y forzará la compatibilidad del CM con BPI.

B.O.II.4.2 CMTS con capacidad BPI+

Un CMTS con capacidad BPI+ de la Recomendación J.112 anexo B v2 DEBE poder funcionar en modos compatibles con BPI y con BPI+ y ajustarse de acuerdo con la capacidad de cada CM cliente. Cuando el CMTS tiene capacidad BPI+ y el sistema soporta simultáneamente módems de cable (CM) de BPI y BPI+, DEBEN estar disponibles los ficheros de configuración tanto de la Recomendación J.112 anexo B v1 como de J.112 anexo B v2 de aquel anexo para la entrega de fijaciones de configuración BPI+ y BPI a los CM apropiados. Un CM con capacidad BPI recibirá un fichero de configuración de la Recomendación J.112 anexo B v1 con fijaciones BPI. A continuación se registrará con capacidad de módem BPI.

APÉNDICE B.O.III

Bibliografía

[IEEE1] IEEE Std 802-1990*, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture,*.diciembre de 1990.

[RSA3] RSA Laboratories, *Some Examples of the PKCS Standards,* RSA Data Security, Inc., Redwood City, CA, 1 de noviembre de 1993.

[SCHNEIER] SCHNEIER (B.), *Applied Cryptography*, Second Edition, *John Wiley*, New York 1996.

[SET Book 2] *SET Secure Electronic Transaction Specification –Book 2: Programmer's Guide*, Version 1.0, 31 de mayo de 1997.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2002