Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.290

(11/2006)

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

Módems de cable

Arquitectura básica del decodificador multimedia de la próxima generación

Recomendación UIT-T J.290

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.290

Arquitectura básica del decodificador multimedia de la próxima generación

Resumen

En esta Recomendación se describe una funcionalidad arquitectónica básica del decodificador multimedia de la próxima generación que los operadores y los fabricantes de equipos PUEDEN utilizar en sus decisiones de inversión relativas a la red y productos conexos. Esta arquitectura define una plataforma eficiente en términos de costes que dispone de la capacidad y flexibilidad necesarias para permitir el crecimiento de los servicios de vídeo a la carta, televisión digital de alta definición y conexión a redes gestionadas en el hogar de una amplia gama de dispositivos que están a disposición de los consumidores, así como futuros servicios multimedia basados en el protocolo Internet (IP), incluyendo voz sobre IP, videotelefonía y juegos con participación de varios jugadores. El objetivo de esta Recomendación es proporcionar funcionalidades básicas que puedan utilizarse en entornos de red específicos. DEBERÍA observarse que la parte correspondiente a la red en el hogar de esta arquitectura está basada en la Rec. UIT-T J.190. En una implementación real de las funcionalidades de la arquitectura del decodificador multimedia de la próxima generación (NG-STB-A), esta Recomendación DEBE utilizarse conjuntamente con la Rec. UIT-T J.292 o la Rec. UIT-T J.291 relativas a la disponibilidad de la red de acceso.

Orígenes

La Recomendación UIT-T J.290 fue aprobada el 29 de noviembre de 2006 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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 no 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 en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T J.290

Arquitectura básica del decodificador multimedia de la próxima generación

1 Alcance

En esta Recomendación se describe una funcionalidad arquitectónica básica del decodificador multimedia de la próxima generación que los operadores y los fabricantes de equipos PUEDEN utilizar en sus decisiones de inversión relativas a la red y productos conexos. Esta arquitectura define una plataforma eficiente en términos de costes que dispone de la capacidad y flexibilidad necesarias para permitir el crecimiento de los servicios de vídeo a la carta, televisión digital de alta definición y conexión a redes gestionadas en el hogar de una amplia gama de dispositivos que están a disposición de los consumidores, así como futuros servicios multimedia basados en el protocolo Internet (IP, *Internet protocol*), incluyendo voz sobre IP, videotelefonía y juegos con participación de varios jugadores. El objetivo de esta Recomendación es proporcionar funcionalidades básicas que puedan servir utilizarse en entornos de red específicos. DEBERÍA observarse que la parte correspondiente a la red en el hogar de esta arquitectura está basada en la Rec. UIT-T J.190. En una implementación real de las funcionalidades de la arquitectura del decodificador multimedia de la próxima generación (NG-STB-A, *next generation STB architecture*), esta Recomendación DEBE utilizarse conjuntamente con la Rec. UIT-T J.292 o la Rec. UIT-T J.291 relativas a la disponibilidad de la red de acceso.

2 Referencias

Ninguna.

3 Definiciones

En esta Recomendación se definen los términos siguientes:

3.1 dominio de servicio autorizado (ASD, *authorized service domain*): Los dispositivos de este dominio pueden autenticarse por sí mismos y permiten aplicar derechos sobre la utilización de contenidos tal como defina el operador de red.

3.2 identificador de aplicación: Este campo se refiere a un identificador (ID) numérico para una aplicación que se ejecuta en el decodificador multimedia.

3.3 dominio de salida autorizado (AOD, *authorized output domain*): Los dispositivos de este dominio se conectan al ASD mediante interfaces de salida aprobadas por el operador.

3.4 dominio de mejor esfuerzo (BED, *best effort domain*): Dispositivos y segmentos de capa física que no cumplen los requisitos de ASD, AOD o GSD. Los dispositivos de este dominio no requieren la protección de contenidos o una calidad de servicio garantizada.

3.5 identificador del sistema de acceso condicional (CA_system_ID): Este campo indica el tipo de sistema de acceso condicional (CA) aplicable a los flujos asociados ECM y/o EMM. Este identificador CA_system_ID puede ser utilizado como un identificador de cliente DSG en modo avanzado DSG.

3.6 cliente DSG: El cliente DSG (pasarela del decodificador multimedia DOCSIS) termina el túnel DSG y recibe el contenido del servidor DSG.

3.7 mensajes de control de derecho a prestaciones (ECM, *entitlement control message*): Un mensaje de control de derecho a prestaciones (ECM) es un mensaje criptado que contiene criterios de acceso a varios niveles de servicio y una palabra de control (CW, *control word*).

3.8 servicios de portal integrado: Elemento de servicios de portal (PS) que no utiliza una interfaz separada para la conexión con un dispositivo de decodificador multimedia.

3.9 decodificador multimedia integrado: Un decodificador multimedia integrado es una entidad funcional de aplicación de servicio integrada. Incluye el cliente o clientes DSG, un controlador de cliente DSG, un procesador integrado para el entorno de aplicación y un módulo integrado o sustituible para el acceso condicional.

3.10 mensajes de gestión de derecho a prestaciones (EMM, *entitlement management message*): Un mensaje de gestión de derecho a prestaciones (EMM) contiene los datos de autorización reales y se envía de forma segura a cada dispositivo CPE.

3.11 dominio de servicio garantizado (GSD, *guaranteed service domain*): Los dispositivos del dominio de servicio garantizado (GSD) pueden recibir servicios de contenido sensibles a la calidad de servicio tales como VoIP, juegos interactivos con varios jugadores y videotelefonía IP.

3.12 dispositivo de acceso en el hogar (HA, *home access*): Agrupación de elementos lógicos utilizados para conseguir el acceso HFC a una o varias redes IPCable2Home.

3.13 dispositivo puente en el hogar (HB, *home bridge*): Grupo de elementos lógicos utilizados para conectar en modo puente varias redes IPCable2Home.

3.14 dispositivo del cliente en el hogar (HC, *home client*): Grupo de elementos lógicos utilizados para proporcionar funcionalidades a aplicaciones de cliente.

3.15 dispositivo IP de LAN: Un dispositivo IP de red de área local (LAN) es representativo de un dispositivo IP típico que previsiblemente reside en redes domésticas y que se supone que incluye una pila TCP/IP y un cliente DHCP.

3.16 servicios de portal (PS, *portal services*): Elemento funcional que proporciona las funciones de gestión y traducción entre la red HFC y la red del hogar.

3.17 unidireccional: Esta expresión implica que el trayecto descendente (de la red al abonado) está en funcionamiento, y que el trayecto ascendente (del abonado a la red) no lo está. Ello puede deberse a que el trayecto ascendente no esté disponible, el dispositivo del decodificador multimedia no esté registrado o que el dispositivo del decodificador multimedia no permita el modo de funcionamiento bidireccional.

3.18 conjunto de parámetros de calidad de servicios: Conjunto de codificación de flujos de servicio que describe los atributos de calidad de servicio de una flujo de servicio o una clase de servicio.

3.19 pasarela residencial: Dispositivo que permite las funcionalidades de interconexión entre la red de acceso y la red del hogar tal como se describe en la Rec. UIT-T J.190.

NOTA – En un futuro próximo DEBERÍA tenerse en cuenta la forma de aplicar la funcionalidad de pasarela residencial J.190 a las diversas redes.

3.20 clase de servicio: Conjunto de atributos de disposición en cola y de programación del tratamiento de los datos que recibe una denominación concreta y que se configura en el equipo situado en la cabecera de la red. Una clase de servicio se identifica mediante un nombre de clase de servicio. Una clase de servicio tiene un conjunto de parámetros de calidad de servicio (QoS) asociados.

3.21 controlador de decodificador multimedia: Sistema informático responsable de la gestión de los dispositivos del decodificador multimedia en un sistema de cable. Gestiona los dispositivos del decodificador multimedia y los mensajes de información enviados a través del canal fuera de banda.

3.22 dispositivo de decodificador multimedia: Receptor que contiene integradas tanto una función de servicios de portal (PS) para la conectividad de la red del hogar como un decodificador multimedia.

3.23 bidireccional: Esta expresión implica que tanto el trayecto descendente como el trayecto ascendente están en funcionamiento.

3.24 dirección MAC bien conocida: Hace referencia a la dirección MAC del cliente en el dispositivo del decodificador multimedia. Esta dirección MAC ha sido asignada por el fabricante del sistema de acceso condicional al dispositivo del decodificador multimedia.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

AES Norma de criptación avanzada (*advanced encryption standard*)

API Interfaz de programación de aplicaciones (*application programming interface*)

ASD Dominio de servicio autorizado (*authorized service domain*)

BED Dominio de mejor esfuerzo (*best effort domain*)

BP Punto frontera (de IPCable2Home) (*boundary point*)

CA Acceso condicional (*conditional access*)

CAS Sistema de acceso condicional (*conditional access system*)

CBC Concatenación de bloques cifrados (*cipher block chaining*)

CE Dispositivo electrónico (*consumer electronics*)

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

Codec Codificador/decodificador

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

CSA Algoritmo de aleatorización común (*common scrambling algorithm*)

CSP Procesador de seguridad configurable (*configurable security processor*)

CW Palabra de control (*control word*)

DES Norma de criptación de datos (*data encryption standard*)

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

DiffServ Arquitectura de servicios diferenciados para tráfico en la red (*differentiated services architecture for network traffic*)

DLNA Alianza de red para la vida digital (*digital living network alliance*)

DRM Gestión de derechos digitales (*digital rights management*)

DSCP Punto de código de servicio diferenciado (*Diffserv code point*)

DSL Línea de abonado digital (*digital subscriber line*)

DTCP Protección de contenidos con transmisión digital (*digital transmission content protection*)

DTV Televisión digital (*digital TV*)

DVB Difusión de vídeo digital (*digital video broadcast*)

DVI Interfaz de vídeo digital (*digital video interface*)

DVR Grabación de vídeo digital (*digital video recording*)

ECB Libro de código electrónico (*electronic code book*)

ECM Mensaje de control de derecho a prestaciones (*entitlement control message*)

EMM Mensaje de gestión de derecho a prestaciones (*entitlement management message*)

EPG Guía electrónica de programas (*electronic program guide*)

FIPS Norma federal de procesamiento de la información (*federal information processing standards*)

FTTH Fibra a la vivienda (*fibre to the home*)

GigE Gigabit Ethernet

GSD Dominio de servicio garantizado (*guaranteed service domain*)

HDCP Protección de contenidos digitales de gran anchura de banda (*high-bandwidth digital content protection*)

HDMI Interfaz multimedia de alta definición (*high definition multimedia interface*)

HDTV Televisión de alta definición (*high definition TV*)

HFC Híbrido fibra coaxial (*hybrid fibre coaxial*)

ID Identificador

IP Protocolo Internet (*Internet protocol*)

Layer 3 Capa de red en la pila OSI; capa protegida por la barrera cortafuegos en la que se basa el encaminamiento IP

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

MGCP Protocolo de control de la pasarela de medios (*media gateway control protocol*)

MIB Base de información de gestión (*management information base*)

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

MPTS Flujo de transporte multiprograma (*multiple program transport stream*)

MTA Adaptador de terminal de medios (*multimedia terminal adapter*)

NAT Traducción de dirección de red (*network address translation*)

NCS Señalización de llamada de red (*network call signalling*)

NE Elemento de red (*network element*)

NG-STB-A Arquitectura del decodificador multimedia de la próxima generación (*next generation STB architecture*)

NIU Unidad de interfaz de red (*network interface unit*)

OCAP OpenCable Applications Platform

OEM Fabricante de equipo original (*original equipment manufacturer*)

OSS Sistema de soporte de operaciones (*operations support system*)

PC Computador personal (*personal computer*)

PHY Capa física (*physical layer*)

PID Identificador de paquetes (*packet identifier*)

PS Servicios de portal (*portal services*)

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

QoS Calidad de servicio (*quality of service*)

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

RAN Red de área regional (*regional area network*)

RMS Sistema de gestión de derechos (*rights management system*)

RSA Sistema criptográfico de clave pública desarrollado por Rivest, Shamir, Adleman; asimismo empresa del mismo nombre que comercializa tecnología de clave pública

RSVP Protocolo de reserva de recursos (*resource reservation protocol*)

RTP Protocolo en tiempo real (*real time protocol*)

RTSP Protocolo de flujos en tiempo real (*real time streaming protocol*)

SCTE Sociedad de ingenieros de telecomunicaciones por cable (*society of cable telecommunications engineers*)

SD Digital seguro (*secure digital*)

SHA-1 Algoritmo de troceo seguro 1 (*secure hash algorithm 1*)

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

SOC Sistema en un chip (*system-on-chip*)

SPTS Flujo de transporte de programa único (*single program transport stream*)

STB Decodificador multimedia (*set-top box*)

SVD Dispositivo de vídeo de abonado (*subscriber video device*)

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

TOS Tipo de servicio (*type of service*) (también punto de código DiffServ, DSCP)

TS Flujo de transporte (*transport stream*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

UI Interfaz de usuario (*user interface*)

UPnP Disponible sin preparativos (*universal plug and play*)

USB Bus serial universal (*universal serial bus*)

VLAN Red de área local virtual (*virtual local area network*)

VoD Vídeo a la carta (*video-on-demand*)

VoIP Voz sobre IP (*voice over IP*)

XML Lenguaje de marcaje extensible (*extensible markup language*)

5 Convenios

En esta Recomendación, las palabras utilizadas para señalar la importancia de determinados requisitos se escriben en MAYÚSCULAS. Dichas palabras son las siguientes:

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

"NO DEBE(N)" Esta expresión significa que el elemento es una prohibición absoluta de esta Recomendación.

"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.

6 Arquitectura multimedia integrada

Se presentan a continuación atributos clave de la NG-STB-A para una *arquitectura multimedia integrada*:

– *Capacidad ampliada*: Proporciona capacidad ampliada que no restringe la introducción de nuevos servicios. Permite al operador de cable disponer de opciones para una utilización más eficiente del espectro mediante conversión de canales analógicos en servicios de vídeo con compresión digital; algoritmos de compresión avanzados; esquemas de modulación más avanzados; gestión integrada de los recursos espectrales en la cabecera y vídeo digital conmutado.

– *Transición a un entorno completamente digital*: Soporta la transición a servicios completamente digitales al tiempo que permite mantener de una forma económica la televisión y los dispositivos VCR analógicos.

– *Acceso condicional flexible y seguro (CA)*: Implementa el acceso condicional mediante hardware interno (el procesador de seguridad configurable, (CSP, *configurable security processor)* de la NG-STB-A) que puede ser configurado o actualizado a distancia mediante descargas de software. Permite utilizar varios sistemas de CA, incluyendo sistemas de CA preexistentes o nuevos, propietarios o no propietarios, permitiendo así la integración del CPE de varios suministradores. Proporciona flexibilidad a un precio inferior que si se utilizan CA físicamente removibles. Al mismo tiempo, las redes de cable pueden continuar soportando un esquema de seguridad físicamente diferenciado mediante tarjetas de seguridad.

– *Soporte de la distribución al por menor*: Facilita la venta al por menor de dispositivos de vídeo de abonado (SVD, *subscriber video devices*) que permiten la activación por el propio usuario mediante una configuración a distancia realizada por el operador a fin de garantizar la compatibilidad con cualquier sistema de cable NG-STB-A.

– *Red segura en el hogar*: Permite utilizar tecnologías y sistemas normalizados de red en el hogar, sistemas de gestión de derechos digitales (DRM, *digital rights management*), y la ubicuidad del protocolo Internet (IP) para la distribución de contenidos en el hogar. Permite a los operadores de red ofrecer servicios de red multimedia en el hogar gestionados desde la cabecera. Soporta la utilización de sistemas de entretenimiento simultáneos en varias habitaciones (multiestancia) que utilizan dispositivos de almacenamiento en el hogar que

sirven contenidos a los dispositivos domésticos conectados en red tanto de gama alta como de gama baja. Integra servicios multimedia entre dispositivos basados en decodificador multimedia de vídeo y computadoras personales de datos.

– *Canales autenticados bidireccionales seguros*: Todos los CPE de la próxima generación permiten canales de comunicación autenticados bidireccionales seguros entre la cabecera de red y CPE. Ello aumenta la seguridad respecto a la que puede conseguirse en sistemas unidireccionales. Dichos canales se utilizan para la gestión de claves de acceso condicionales renovables, gestión a distancia de los CPE, actualización de firmware descargable, datos para aplicaciones interactivas privadas y reconfiguración de algoritmos de criptación.

– *Opciones de transporte flexible*: Permite el transporte de vídeo en modo difusión, multidifusión y/o unidifusión IP.

– *CPE equipados para normas futuras de transmisión y de compresión*: Permite futuros aumentos de la capacidad efectiva de los sistemas con inversiones incrementales mínimas sin que inversiones anteriormente realizadas en CPE queden inutilizables, tanto si las inversiones las realizan los operadores o los consumidores en el mercado al por menor.

– *Entorno de aplicaciones bien definidas en el CPE*: Incluye la capacidad necesaria para que el software de integración de sistemas (middleware) de la plataforma de aplicaciones basadas en las Recomendaciones UIT-T de la serie J.200 permita utilizar aplicaciones descargables, se mantenga la capacidad de creación rápida de servicios, así como las posibilidades de innovación y de desarrollo de nuevos modelos de negocio a fin de que las Recomendaciones UIT-T de la serie J.200 puedan ejecutarse en todos los SVD, siempre que existan condiciones de licencia razonables. Proporciona los ahorros de coste propios de una plataforma normalizada sin afectar a la capacidad de innovación de los operadores de cable en relación con las interfaces de usuario y el diseño del aspecto y percepción de los servicios.

– *Prestación rápida de nuevos servicios*: Permite la autoinstalación y la prestación rápida de nuevos servicios mediante la auto detección, la gestión a distancia y las capacidades de configuración a distancia de los CPE que sean conformes con la NG-STB-A.

– *Gestión mejorada de recursos mediante interfaces abiertas en la cabecera*: La reestructuración de los elementos de red de la cabecera con interfaces abiertas permite un uso más eficiente de los recursos del sistema, aumentando efectivamente la capacidad utilizable del sistema y la flexibilidad del mismo, reduciendo los costes y aumentando el número de suministradores de componentes de la cabecera, al tiempo que se garantiza la capacidad de interconexión.

6.1 Descripción de la arquitectura de referencia

La arquitectura de referencia se define mediante un conjunto de elementos de red utilizados para satisfacer necesidades específicas. Estos elementos de red funcionan dentro de los principales segmentos de red que incluyen la oficina técnica de apoyo, la cabecera, la planta externa y las facilidades en domicilio del cliente, tal como se representa en la figura 1.

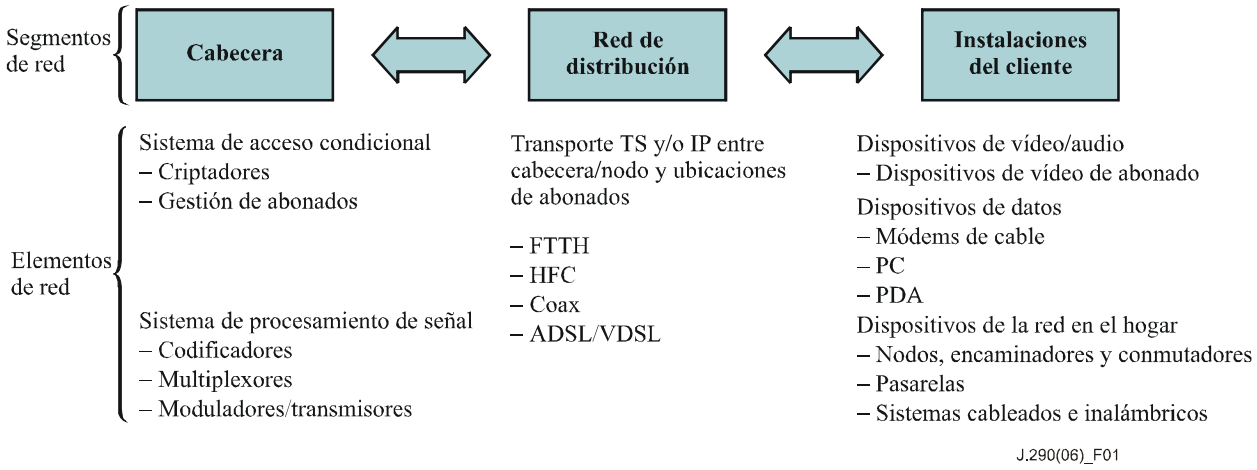


Figura 1 – Principales segmentos y elementos de red

6.2 Atributos de una arquitectura multimedia integrada

6.2.1 Arquitectura de los servicios de vídeo

Un CPE que sea conforme con la NG-STB-A tendrá como mínimo, los atributos siguientes.

– *Acceso condicional*: Utiliza un sistema de acceso condicional (CA) interno reconfigurable basado en una combinación de hardware para la descriptación (CSP) e intercambio de claves definido por software. Permite la descriptación de múltiples flujos para DVR, capacidades para la inserción de publicidad local y otras aplicaciones que requieran varias señales.

– *Transporte de vídeo*: Se permiten dos modos:

  • modo no IP (MPEG básico sobre QAM);

  • modo IP (MPEG encapsulado en IP).

– *Soporte de las aplicaciones de los dispositivos de vídeo*: Todos los CPE de vídeo disponen de los recursos mínimos necesarios (es decir, memoria y capacidad de procesamiento) para soportar [b-UIT-T J.200], [b-UIT-T J.201] y [b-UIT-T J.202].

– *Códecs de vídeo*: Permite la decodificación de H.262 (vídeo MPEG-2) y de códecs avanzados, H.264 (AVC MPEG-4) y, opcionalmente, VC-1. El dispositivo de cliente DEBE poder conmutar de forma casi instantánea entre un códec avanzado que se encuentre activo y un códec MPEG-2.

– *Códecs de audio*: Permite la decodificación de AAC MPEG o Dolby Digital.

6.2.2 Arquitectura IP multimedia

– *Protocolo Internet*: Se selecciona IP como capa portadora básica para todos los servicios multimedia de la red del hogar.

– *QoS (calidad de servicio) de la red IP en el hogar*: {Texto informativo: Plan para cumplir UPnP (norma para la disponibilidad sin preparativos) a fin de permitir la gestión, aprovisionamiento y observación del servicio para dispositivos UPnP de las redes en el hogar.}

– *IPv6*: En dispositivos "todo IP" conectados puede emplearse tanto IPv4 como IPv6, con el objetivo de que finalmente se haga una migración a IPv6.

6.2.3 Red del hogar

– *Dominios de red del hogar*: Se definen dominios de red del hogar en función del nivel de servicio y de protección de los contenidos.

  • Dominio de servicio garantizado (GSD, *guaranteed service domain*): calidad de servicio (QoS) gestionada desde la cabecera hasta el dispositivo extremo.

  • Dominio de servicio autorizado (ASD, *authorized service domain*): los contenidos pueden transferirse a dispositivos receptores que disponen de sistemas certificados, con DRM autenticado por la red del operador o de acceso condicional.

  • Dominio autorizado de salida (OAD, *output authorized domain*): los contenidos pueden transferirse a través de una interfaz de derechos gestionados desde el ASD a dispositivos con DRM no autenticado por el operador.

  • Dominio del mejor esfuerzo (BED, *best effort domain*): dispositivos conectados externos a GSD, ASD o OAD.

  El CPE PUEDE estar ubicado en cualquiera de dichos dominios o en varios dominios cuando hay solapamientos entre ellos.

– *Puerto USB-2 y/o Ethernet*: Proporciona una conexión universal de los CPE a las redes del hogar. Puede utilizarse cualquier capa física que pueda transportar tráfico IP de forma transparente (por ejemplo, cables CAT5 para Ethernet) mediante un adaptador entre el puerto USB y la capa física específica.

– *Compartición de aplicaciones*: Permite el uso compartido de aplicaciones entre dispositivos de la serie J.200, así como dispositivos que no pertenecen a dichas series que residen en uno o más dominios de red del hogar definidos en la cláusula 6.5.1; por ejemplo, un PC con un cliente compatible con la NG-STB-A. Las siguientes son ejemplos de aplicaciones: el acceso distante al contenido de un DVR, los juegos con varios participantes y el gestor de información personal (por ejemplo, calendario familiar, libro de direcciones, reloj despertador).

6.2.4 Inserción de programas

– *Inserción de programas*: Las técnicas de inserción de programas, tales como la Rec. UIT-T J.181 (Inserción de programas digitales) permiten responder a la necesidad que tienen los operadores de una distribución flexible de programas. Se dispone asimismo de capacidad para unir dos flujos criptados diferentes, por ejemplo, para sustituir un contenido criptado de un flujo difundido por un contenido criptado que previamente ha sido almacenado temporalmente en el disco duro local.

6.2.5 Segmento de red: en instalaciones del cliente

– *Dispositivos de vídeo del abonado (SVD, subscriber video devices)*: Los SVD son dispositivos de vídeo que satisfacen la NG-STB-A, y que incluye un sintonizador tal como un decodificador o una unidad de adaptación de medios o televisores digitales independientes (DTV). Un SVD básico (de gama baja) se define con funcionalidades NG-STB-A mínimas necesarias. Los SVD de gama alta incluyen varias opciones de configuración a discreción de los fabricantes, operadores de red y comerciantes minoristas. En el cuadro 1 se muestran funciones SVD básicas y ejemplos de diversas opciones.

Cuadro 1 – Funcionalidades básica y ampliada de los SVD

Funcionalidad básica de los SVD	Ejemplos de funciones opcionales de los SVD
• Soporte para múltiples modos de transporte. • Soporte para la decodificación MPEG-2 (con definición normal y alta) y H.264. • Conectividad en la red del hogar como cliente. • CA descargable. • Capacidad del middleware para la serie J.200. • Salida de definición normal. • Salida de vídeo de alta definición. • Interfaces de salida digital con protección contra copia. • Mando a distancia universal OEM con capacidad para controlar el SVD y la TV preexistente. • Opcionalmente, modulación QAM J.83 en sentido descendente. • Incluye puertos USB-2 y/o Ethernet de propósito general para la conectividad de la red del hogar y la eventual conexión de periféricos no especificados.	• Interfaces digitales con protección contra copia (por ejemplo, HDMI, DVI). • Función de pasarela integrada (cliente, servidor y gestión de direcciones IP) entre las redes de acceso y del hogar. • Funcionalidad de DVR básico. • Códec VC-1.

– *Gestión de derechos*: Los dispositivos CPE respetan y protegen los derechos de los titulares de los contenidos cuando utilizan contenidos de alto valor.

6.2.6 Segmento de red: cabecera de la red

- *Gestión de recursos de calidad de servicio (QoS) y de sesión*: Define la estructura lógica y los flujos de procesos con QoS (peticiones, concesiones y garantía de servicio). Coordina y es conforme con los procesos de QoS de la cabecera asociados con todos los recursos de la cabecera, la planta externa y red del hogar.
- *Interfaces OSS/BSS*: Define el modelo de las interfaces con los sistemas de facturación de apoyo, el sistema soporte de las operaciones (OSS, *operations support system*), y el sistema soporte del negocio (BSS, *business support system*).

6.3 Arquitectura de los servicios de vídeo

Las características comunes de la arquitectura de los servicios de vídeo incluyen lo siguiente:

- **Seguridad**: el procesador de seguridad configurable gestiona las funciones de acceso condicional (CA), protección contra copia, soporte para servicios por demanda seguros, descargas seguras y gestión de derechos digitales (DRM) en el hogar.
- **Protección contra copia**: mecanismo de protección contra copia para la distribución de contenidos a través de salidas protegidas.
- **Descargas de firmware**: permiten la configuración del dispositivo.
- **Transporte de vídeo**: se soporta tanto el modo no IP (MPEG básico sobre QAM) como el modo IP (MPEG encapsulado en IP).
- **Códecs de vídeo**: se soportan los códecs H.262 (vídeo MPEG-2) y H.264 (AVC MPEG-4) así como, opcionalmente, el códec SMPTE 421M (VC-1).

- **Entorno software de cliente de vídeo**: soporta el middleware de la serie J.200 en todos los dispositivos de red de la próxima generación que permiten la descarga de aplicaciones, además de ofrecer flexibilidad para soportar aplicaciones a través de los sistemas basados en la cabecera de la red.
- **Descarga segura de software**: soporta la instalación y actualización de aplicaciones software, programas de gestión de dispositivos (controladores), kernels e implementaciones del middleware de la serie J.200.

6.3.1 Seguridad

Un SVD incluirá un procesador de seguridad configurable (CSP) interno de la próxima generación para la gestión de aspectos de seguridad relacionados con los servicios. Los elementos de seguridad pueden clasificarse de la forma siguiente, existiendo un cierto solapamiento entre ellos:

- Autenticación y gestión del dispositivo.
- Acceso condicional (CA) a servicios entre la cabecera de red y el equipo de cliente.
- Descarga segura de actualizaciones del firmware y aplicaciones descargables.
- Protección contra copia.
- Seguridad del dominio de servicio autorizado (ASD).
- DRM en los dispositivos de una o más redes del hogar en el dominio de servicio autorizado.
- Puente de seguridad entre CA y DRM según se define en la Rec. UIT-T J.197.

El modelo de seguridad de la próxima generación incluye tres subsistemas:

1) *criptación/descriptación de contenido y de clave*, basado en hardware pero que puede ser reconfigurado a distancia;
2) *gestión de claves*, parcialmente basado en software y, por tanto, redefinible mediante la descarga segura del sistema de acceso condicional;
3) *autenticación*, parcialmente basado en software y, por tanto, actualizable mediante la descarga segura del sistema de CA.

Estos subsistemas permiten la gestión por parte del operador de los siguientes aspectos del CA:

- Reconfiguración a distancia de la máquina de descriptación para permitir varios algoritmos de aleatorización predefinidos, incluidos algoritmos de CA comunes preexistentes y nuevos algoritmos de CA.
- Descarga inicial y actualización definidos por software del mecanismo de intercambio de claves del CA.

En el modelo de referencia CSP, el contenido PUEDE permanecer seguro gracias a una norma abierta, un sistema CA/DRM no propietario y/o un sistema CA/DRM propietario (preexistente o no).

La "máquina de descriptación flexible" del CSP puede configurarse para soportar varios algoritmos, tal como se muestra en la figura 2. Es suficientemente flexible como para permitir que la configuración mediante instrucciones a distancia sea compatible con los algoritmos de criptación utilizados por el sistema de CA, así como con el sistema o sistemas de protección de contenidos. Los mensajes de derecho a prestaciones y de control se codifican y distribuyen a través de canales dentro y fuera de banda hasta el CPE de vídeo de forma que el CSP pueda recuperar las claves de forma segura; a este procedimiento se le denomina aplicación de gestión de claves de acceso condicional definida por firmware.

Los aspectos de seguridad del CSP se protegen gracias a la integración en un sistema construido sobre un chip (SOC, *system-on-chip*) que incluye una máquina de descriptación configurable y un microcontrolador para la gestión de claves. El SOC incluye el CSP y los elementos del

decodificador de forma que ni el vídeo abierto (no protegido) ni el vídeo comprimido abandonan en ningún momento el SOC. El vídeo digital abierto se protegerá entre el CSP y los elementos del decodificador del SOC utilizando técnicas de función de troceado simple o técnicas criptográficas rápidas.

El CSP se estructurará para evitar incurrir en obligaciones derivadas de regalías debidas a sistemas CA/DRM que permanezcan inactivos. Es previsible que los derechos de propiedad intelectual (IPR, *intellectual property rights*) asociados a un sistema CA/DRM no se aplique hasta que dicho sistema CA/DRM sea activado por el operador.

En la figura 2 se muestran varios algoritmos posibles. Los algoritmos permitidos serán seleccionados en última instancia cuando se desarrollen las especificaciones. Para soportar la transición desde el sistema CA preexistente, el equipo de cliente DEBE tener la capacidad de funcionar tanto en un entorno simulcrypt como multicrypt. En caso de que se active el modo simulcrypt, el CSP permitirá el uso compartido de claves en el CPE.

El CSP utilizará tecnologías que permitan la descriptación de flujos de transporte seguros normalizados propietarios o no propietario basados en variantes tales como DES, 3-DES, CSA y algoritmos de criptación AES y Multi2.

El CSP podrá generar firmas digitales seguras en sistemas hardware resistentes a la manipulación, sin desproteger las claves privadas o el procesamiento de generación de las claves de troceado y la criptación. La red de la próxima generación podrá firmar digitalmente mensajes utilizados para la autenticación y garantizar la integridad mediante una función de troceado segura.

Cada CSP de un dispositivo CPE se identificará con un ID específico. A los efectos de serialización privada, cada uno puede incluir un identificador unívoco conocido como ID semilla privado. Este ID semilla se utiliza para generar la clave única que permite descriptar los derechos a prestaciones de dicho CPE. El CPE podrá cambiar el ID semilla a otro valor único mediante una instrucción segura desde la cabecera de la red. La clave de criptación se generaría entonces utilizando el nuevo ID semilla como un componente de la clave. También puede utilizarse una clave asimétrica para descriptar la clave de categoría enviada en el mensaje de gestión de derecho a prestaciones (EMM, *entitlement management message*).

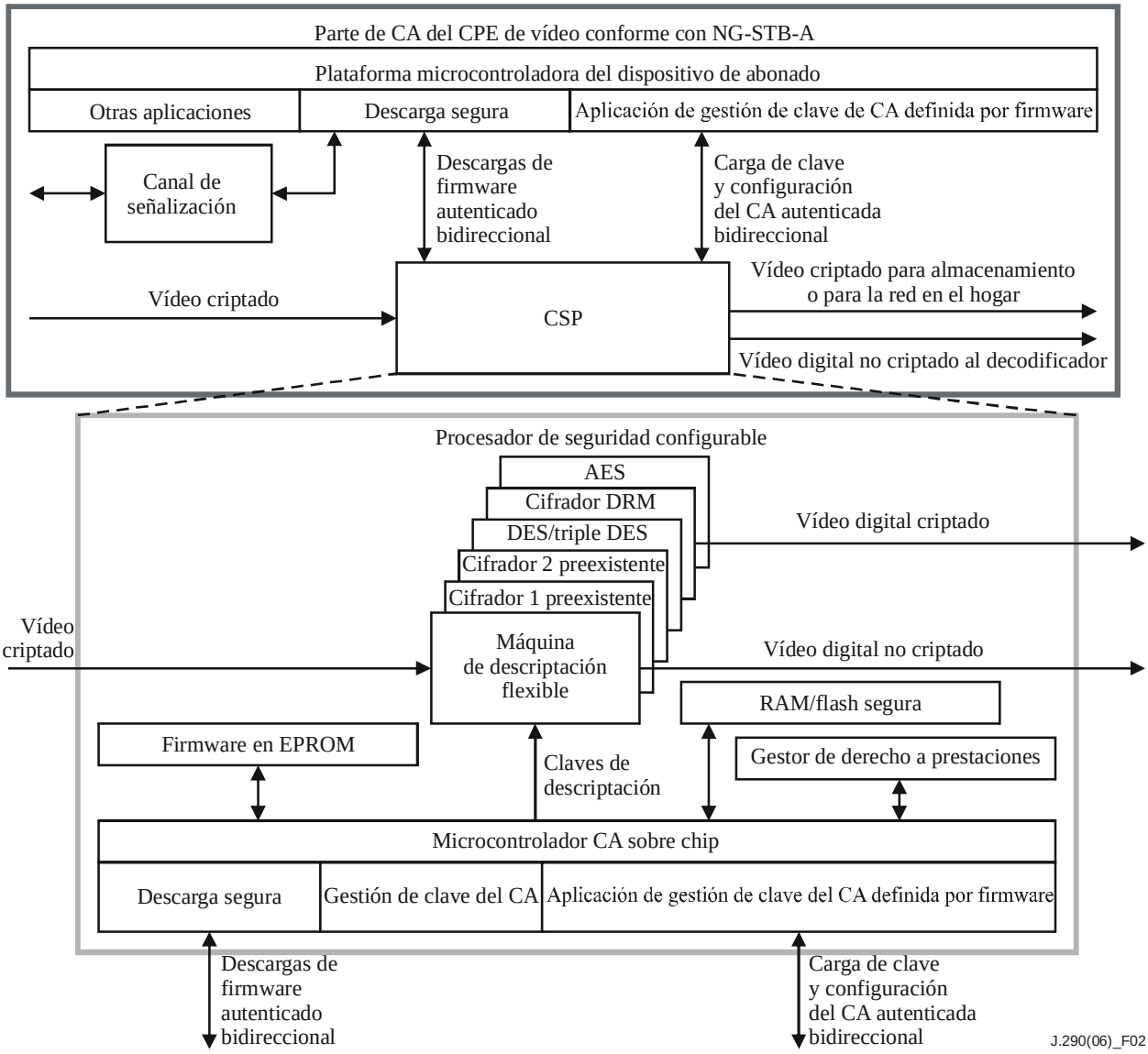


Figura 2 – Ejemplo de diagrama de bloques de seguridad

6.3.1.1 Soporte de múltiples flujos

Los CSP tendrán capacidad para descriptar y volver a criptar simultáneamente varios flujos de contenidos. Es previsible que los distintos CSP tengan capacidad para procesar un número diferente de flujos en función de las capacidades de los CPE asociados, pero todos los CSP tendrán la capacidad de procesar un número mínimo de flujos simultáneamente. Los CSP DEBERÍAN permitir los siguientes escenarios de múltiples flujos:

- *Ver y grabar*: capacidad de poder visualizar, por disponer de dos sintonizadores, un flujo criptado 'en directo' al tiempo que se graba otro en un disco duro simultáneamente. Es muy probable que ello requiera que el CSP suprima para ambos flujos la criptación del sistema de acceso condicional de red y aplique a ambos flujos simultáneamente una criptación local en el disco duro.

- *Servidor DVR*: dispositivo DVR con varios sintonizadores y un disco duro que ofrece servicio a otros dispositivos en el hogar que no tienen disco duro distribuyendo el material grabado a través de la red del hogar. Un servidor DVR puede soportar varios flujos que se graban y se reproducen de forma concurrente, por ejemplo, distribuyendo flujos simultáneamente a varios dispositivos del hogar y grabando al mismo tiempo varios programas. El CSP del dispositivo DVR PUEDE disponer de la facilidad de ver y grabar al tiempo que distribuye flujos criptados enviados desde el disco duro a dispositivos distantes en un escenario de DVR multiestancia.

Los CSP PUEDEN soportar varios flujos utilizando varios núcleos CSP, aumentando el caudal de un único núcleo, o aplicando ambos procedimientos.

6.3.1.2 Acceso condicional

La arquitectura NG-STB-A prevé que el operador de cable pueda elegir entre varias opciones de acceso condicional (CA), permitiendo que el operador de red utilice un CA propietario así como cualquier nuevo sistema de CA normalizado. El CSP de cada CPE puede configurarse para ejecutar el CA específico elegido por el operador de cable.

Puesto que la elección del CA puede realizarse en cualquier momento bajo el control de una instrucción de la cabecera de la red, un sistema equipado con un CSP puede migrar sin problemas de un CA a otro. El CSP será compatible con tarjetas de seguridad. En los dispositivos de abonado con interfaces para tarjetas de seguridad, el CSP DEBERÍA ser la opción por defecto en caso de que no se instale una tarjeta de seguridad.

6.3.1.2.1 Actualización del software de acceso condicional

Determinados aspectos relativos a algoritmos, intercambio de claves, gestión de claves y protocolos criptográficos, se implementan en software o en firmware actualizable en el CSP. La actualización del software es un aspecto importante de un sistema de seguridad robusto y es deseable que esté disponible en los sistemas de la próxima generación. Por motivos de coste, es conveniente utilizar actualización de software en lugar de actualización de hardware en tantas situaciones como sea posible.

La NG-STB-A no soporta un sistema de CA "basado exclusivamente en software" en el que las funciones criptográficas se realicen en un procesador de propósito general. Los elementos de seguridad basados en hardware constituyen una parte necesaria de un sistema de seguridad que sea realmente efectivo para contenidos de alto valor. Los elementos basados en software y hardware específico son complementarios y PUEDEN proporcionar una seguridad adicional con respecto a las soluciones basadas exclusivamente en software o en hardware.

6.3.1.2.2 Actualización del hardware de acceso condicional

Aunque la actualización del software es más eficiente en términos de coste, y operacionalmente más fácil de implementar, es deseable disponer en el CSP de un cierto nivel de actualización del hardware de la tecnología de gestión de claves y de descriptación de transporte.

La actualización del hardware de la tecnología de gestión de claves y de la descriptación de transporte puede conseguirse de varias formas utilizando hardware removible que soporte los requisitos de anchura de banda de los flujos de transporte. Por ejemplo, para dispositivos NG-STB-A que soporten una interfaz de tarjeta de seguridad con capacidad para varios flujos, la inserción de una tarjeta de seguridad permitiría una actualización completa. Alternativamente, si la seguridad del dispositivo se viera comprometida podría utilizarse un puerto de comunicación, por ejemplo, USB 2.0, destinado a alojar un nuevo dispositivo para una actualización completa del hardware.

6.3.2 Protección contra copia

Si un dispositivo NG-STB-A utiliza una tarjeta de seguridad, la interfaz implementará capacidad para actualización y configuración. También se tendrán en cuenta métodos adicionales de protección contra copia de la próxima generación.

6.3.3 Descargas de firmware y/o software

Se asume que los SVD soportan tres tipos de descargas seguras de firmware:

- Firmware de control general que controla la interfaz de usuario, el funcionamiento del dispositivo y que permite determinadas aplicaciones (por ejemplo, VoD, EPG, Recomendaciones UIT-T de la serie J.200).
- Firmware interno para la gestión y comunicación con el CSP.
- Mensajes altamente seguros destinados a ser transferidos al CSP, que reconfiguran el hardware y/o instalan un firmware de gestión de claves de acceso condicional en el CSP.

Las descargas seguras se codifican para la transmisión hasta el SVD a través de un canal seguro. Todos los trayectos de señal para descarga segura requieren intercambios autenticados bidireccionales, asumiéndose además que los trayectos de señal físicamente accesibles entre bloques de la figura 2 están criptados.

6.3.4 Transporte de vídeo

Los flujos digitales de vídeo y audio normalmente se transportan sobre flujos de transporte MPEG-2. Tanto el flujo de transporte de programa único (SPTS, *single program transport stream*) como los flujos de transporte multiprograma (MPTS, *multiple program transport streams*) PUEDEN entregarse en varios segmentos del sistema. La información específica del programa MPEG-2 y la información de servicio (J.94 SI) se utilizan en la capa de transporte MPEG.

6.3.4.1 Red troncal

El transporte troncal de audio/vídeo (difusión a la carta) se basa normalmente en transporte MPEG-2 sobre el protocolo de datagramas de usuario (UDP)/IP transportado sobre Gigabit Ethernet. PUEDEN utilizarse tanto SPTS como MPTS. Un ejemplo de SPTS es el flujo de vídeo a la carta en la salida Gigabit Ethernet del servidor de flujos. Son ejemplos de MPTS los flujos en difusión multiplexados desde un multiplexor. El encapsulamiento IP en la red troncal termina normalmente en el borde de la red (en el QAM o el CMTS).

Las redes troncales futuras PUEDEN utilizar el protocolo RTP u otros protocolos para recuperar la sincronización afectada por la variación de fase o el retardo de la red. La utilización de un encabezamiento adicional, como por ejemplo RTP, PUEDE permitir que el paquete transporte información específica adicional de vídeo, tal como el identificador de sesión de VoD o el identificador del programa.

6.3.4.2 Desde el borde de la red hasta la instalación del cliente

La arquitectura de referencia NG-STB-A prevé dos medios alternativos para el transporte de datos entre el borde de la cabecera y la instalación del cliente. Los datos de vídeo se comprimen mediante MPEG-2 o alguno de los métodos de codificación avanzados descritos a continuación. Los datos de audio estarán codificados en MPEG-1 capa 3, o en algún otro esquema de codificación de audio. Los dos métodos de transporte posibles son los siguientes:

- **Básico: transporte MPEG-2 sobre QAM**

  La utilización de flujos de transporte multiprograma (MPTS) MPEG-2 sobre QAM es el método convencional actualmente utilizado en los sistemas digitales por cable. Con el objetivo de mantener la retrocompatibilidad, el dispositivo de vídeo de abonado digital (SVD), o el equipo de cliente de vídeo de la próxima generación, deberán procesar el

transporte de MPEG-2 sobre QAM tanto para aplicaciones de difusión como de vídeo a la carta. La cabida útil del flujo de transporte PUEDE ser audio o vídeo MPEG-2 o un flujo comprimido empleando un códec avanzado.

- **Mejorado: Vídeo sobre IP**

  En este enfoque, el vídeo se transporta sobre IP y se entrega sobre varios medios tales como FTTH, DSL, HFC o cables coaxiales. Ello permitirá en el futuro establecer servicios tales como flujos de medios basados en IP dirigidos a los SVD digitales. El audio y vídeo PUEDEN transportarse en cualquiera de los formatos siguientes:

  – Paquetes de transporte MPEG-2 sobre IP.

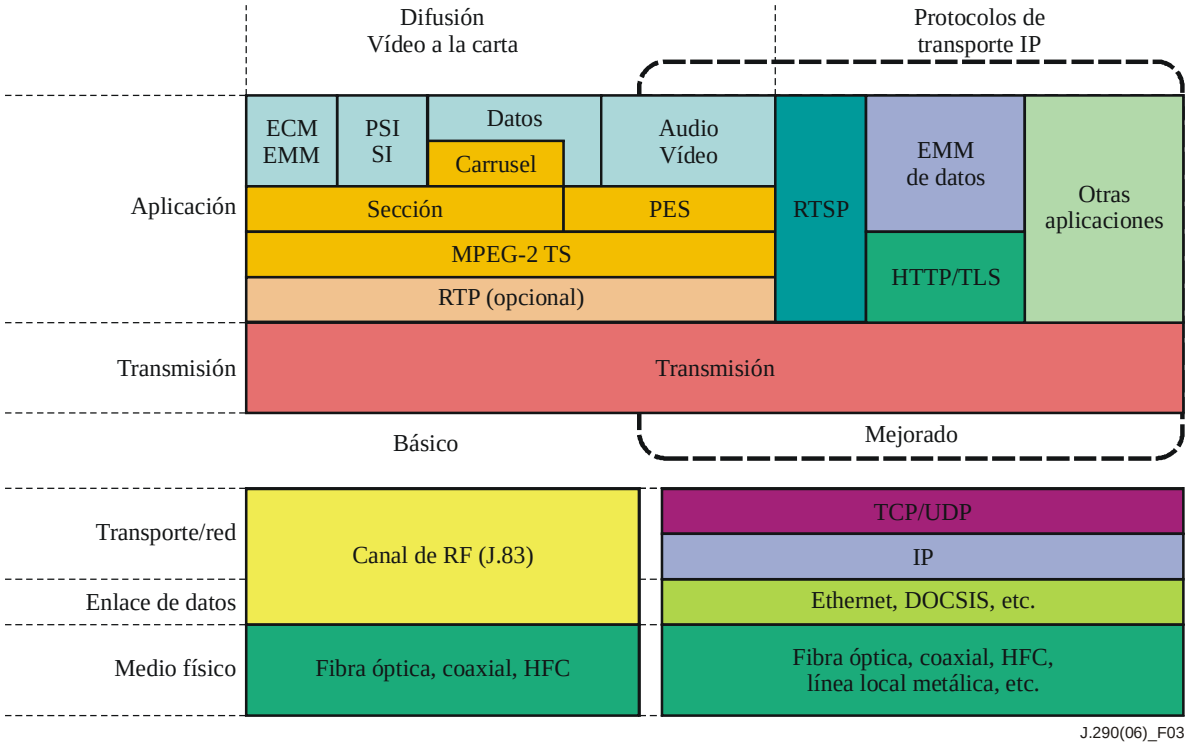
  – Paquetes de transporte MPEG-2 en cabidas útiles del protocolo RTP sobre IP.

  – Cabidas útiles RTP (o de otro protocolo IP en tiempo real) sobre IP.

El CPE receptor DEBERÍA poder procesar flujos distribuidos en cualquiera de los tres formatos anteriores.

Además, tanto datos como EMM PUEDEN ser transportados sobre HTTP con TLS. Para las aplicaciones de VoD, PUEDE utilizarse RTSP para el control de sesión. El CPE receptor DEBERÍA asimismo soportar dichos protocolos. Para aplicaciones de VoD, se utiliza RTSP para el control de sesión, mediante SETUP, PLAY, PAUSE, TEARDOWN.

Es necesario que el terminal de abonado soporte dos métodos de transporte, básico y mejorado. En la figura 3 se muestran formas de transporte de vídeo alternativas basadas en ambos métodos de transporte.



NOTA – Es necesario utilizar TCP para la transmisión de RTSP y HTTP/TLS.

Figura 3 – Enfoques alternativos de transporte de vídeo

6.3.5 Códec de vídeo

Los sistemas de cable NG-STB-A distribuirán los contenidos de vídeo en cualquiera de los dos formatos comprimidos: en MPEG-2 (para definición normal o de alta definición), tal como se hace en los sistemas actuales, y en un formato de compresión avanzado. La elección entre MPEG-2 u otro procedimiento avanzado se hará para cada programa o para cada servicio (incluyendo la conmutación en función del contenido, programa o publicidad). Por lo tanto, el SVD DEBE poder conmutar rápidamente para decodificar contenidos en MPEG-2 y contenidos comprimidos mediante un método avanzado. La transición entre la codificación de MPEG-2 y la decodificación de códec avanzados, DEBE realizarse de forma imperceptible para el espectador, tal como actualmente ocurre en la transición entre programas MPEG-2.

El formato de compresión avanzado será H.264 (MPEG-4 Parte 10, codificación avanzada de vídeo) y, opcionalmente, VC-1.

El operador elegirá el formato de compresión avanzada a utilizar. No es previsible que un operador utilice en su red los dos formatos de codificación avanzada simultáneamente. Por lo tanto, lo normal sería que el SVD pueda decodificar simultáneamente MPEG-2 y uno de los sistemas de codificación avanzada, así como que pueda detectar cuál es el códec avanzado que necesita aplicar en el sistema al que está conectado, y configurar su software adecuadamente durante la fase de carga. Ello puede requerir la descarga del firmware adecuado o la activación del firmware residente más conveniente.

Es previsible que los aspectos residentes pero no utilizados del códec avanzado (es decir, estructura hardware o código firmware) no infringirán los derechos de propiedad intelectual (IPR) asociados a dicho códec. Los IPR no se aplicarán salvo que el operador active el códec avanzado. Este requisito es necesario para que los suministradores de los SVD que sean conformes con NG-STB-A de carácter OEM, así como los operadores de cable que desplieguen dichos dispositivos, no se vean obligados a pagar regalías por IPR salvo que realmente utilicen los algoritmos alternativos de codificación avanzada.

Además de las técnicas de codificación avanzadas de vídeo, se considerarán esquemas de codificación avanzada de audio que conlleven mejoras significativas en relación con la codificación de audio actualmente utilizada.

6.3.6 Entorno software del cliente de vídeo

Todos los SVD que sean conformes con la NG-STB-A dispondrán de memoria y recursos de procesado suficientes para poder ejecutar el middleware de las Recomendaciones UIT-T de la serie J.200. El middleware PUEDE estar residente o ser descargado en el dispositivo. El objetivo es que dicho middleware se ejecute en los SVD sujeto a la negociación de unos términos de licencia razonables. Las Recomendaciones UIT-T de la serie J.200 proporcionan un entorno consistente para aplicaciones tanto de carácter no direccional como direccional. Las primeras (aplicaciones no direccionales) son independientes de los canales de programación, como por ejemplo, un juego, y las segundas (canales direccionales) están ligadas a canales de programación específicos, como por ejemplo un enlace que mediante un clic permitan rebobinar una película que está siendo visionada.

Las Recomendaciones UIT-T de la serie J.200 incluyen un conjunto de API para el componente middleware de la solución software. También especifican un conjunto de ficheros de petición de permisos, una imagen código firmada digitalmente y una aplicación de supervisión para diversos aspectos de seguridad y acceso competitivo a recursos.

La figura 4 describe la arquitectura del software de un CPE de vídeo basado en las Recomendaciones UIT-T de la serie J.200.

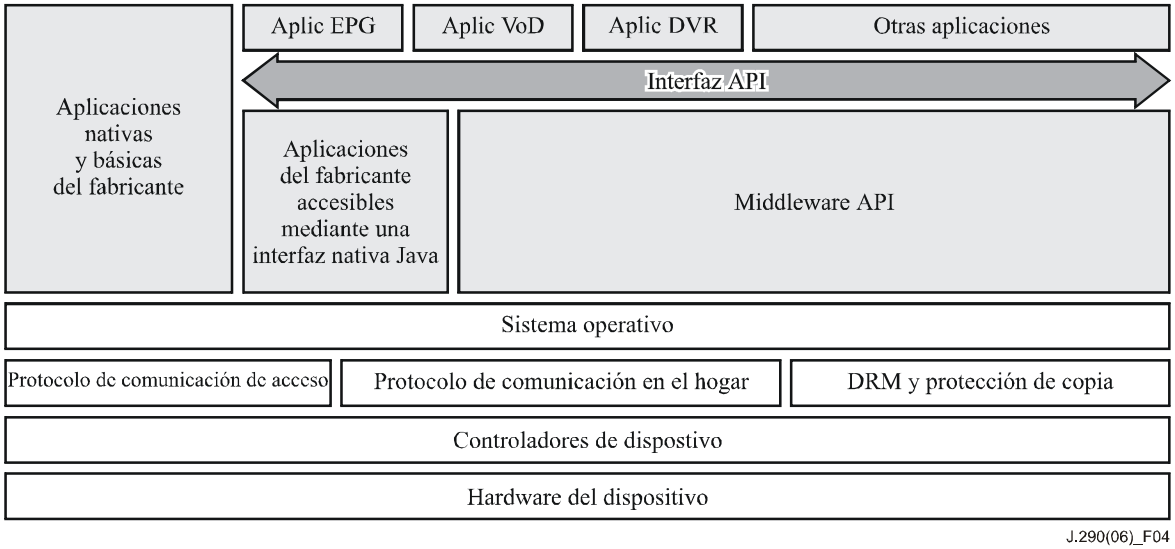


Figura 4 – Arquitectura software de un CPE de vídeo

El modelo de referencia identifica dos categorías de aplicaciones nativas que probablemente el fabricante del dispositivo incluya en sus productos. Las aplicaciones del fabricante descritas como "nativas y básicas" tendrán acceso directo al sistema operativo, obviando la capa de middleware de las Recomendaciones UIT-T de la serie J.200 para tener una interfaz directa con el anfitrión y la interfaz de usuario; ello puede servir para permitir, por ejemplo, que el usuario pueda seleccionar entre la programación del sistema de cable o la programación radiodifundida. La otra categoría de aplicaciones del fabricante se denomina "accesible mediante interfaz nativa Java" (JNI, *Java native interface*). Estas aplicaciones son también suministradas por el fabricante y están directamente relacionadas con la capa middleware de las Recomendaciones UIT-T de la serie J.200.

La situación por defecto a las Recomendaciones UIT-T de la serie J.200 sería que dichas aplicaciones pasaran a través de la interfaz del anfitrión y del usuario; no obstante, las Recomendaciones UIT-T de la serie J.200 tendrían la capacidad de modificar dicha situación por defecto o incluso sustituir la aplicación OEM con una nueva aplicación, por ejemplo, que sea descargada por el usuario final y esté por encima de las Recomendaciones UIT-T de la serie J.200. Un ejemplo de aplicaciones nativas por defecto es el control de volumen de sonido en un receptor de televisión digital (DTV). Normalmente, las Recomendaciones UIT-T de la serie J.200 permitirían que la aplicación del fabricante mantuviera el control, pero en caso de un aviso de emergencia (EA, *emergency alert*), la aplicación aviso de emergencia del operador, que se ejecuta sobre el middleware de las Recomendaciones UIT-T de la serie J.200, tomaría el control del nivel del control del volumen de sonido.

Las aplicaciones descargables se ejecutan en el entorno del middleware de las Recomendaciones UIT-T de la serie J.200. Entre las aplicaciones que un operador de red PUEDE descargar es previsible que se encuentre un conjunto básico de aplicaciones esenciales: guía electrónica de programas (EPG, *electronic program guide*), vídeo a la carta (VoD, *video-on-demand*) y otras aplicaciones del servicio por cable, como son las aplicaciones prestadas desde la cabecera. Con esta última opción, la interfaz de salida del usuario se visualiza como una imagen de vídeo estática creada en la cabecera y que se reproduce en el equipo de cliente, o bien, alternativamente, PUEDE implementarse como un flujo de vídeo unidifusión si la anchura de banda lo permite, que puede incluir componentes en movimiento. La utilización de la interfaz de entrada del usuario implica transmitir las interacciones entre usuario y mando a distancia hasta la

cabecera a fin de comunicar una selección del menú o una selección hecha sobre la pantalla mediante el cursor.

{Texto informativo: Además de la API de la serie J.200, DEBERÍAN ser aplicables las API basadas en Internet, como html, java y flash para aplicaciones bastante sencillas. Estas API DEBERÍAN estar sujetas a la negociación de unas condiciones razonables para la concesión de la licencia. Ulteriormente podrán añadirse los estudios actualmente en curso destinados a definir las relaciones entre los formatos de contenidos, por ejemplo, de HTML o FLASH con la arquitectura J.200.}

Es previsible que existan diferencias entre dispositivos CPE en términos de aplicaciones y capacidades soportadas. Por ejemplo, los dispositivos de gama alta soportarán algunas aplicaciones, tales como DVR, que no existen en los CPE de gama baja.

6.3.6.1 Mejoras de seguridad

El software de cliente de la próxima generación será un componente crítico en la arquitectura global de seguridad del sistema. Dado que la seguridad del sistema en la fase de autenticación durante la carga del sistema, la autenticación del controlador del dispositivo y la seguridad del kernel del sistema no están incluidas en la especificación de las Recomendaciones UIT-T de la serie J.200, y dado que ello conlleva un riesgo de seguridad, es importante que los restantes requisitos de seguridad para la solución completa de software de cliente de la próxima generación sean especificadas. La solución propuesta incluye un cargador de arranque confiable y no modificable, que sea la base para todas las descargas y actualizaciones de software. También incluye la autenticación de todos los elementos de software, incluida la implementación de las Recomendaciones UIT-T de la serie J.200, el kernel del sistema, los controladores de dispositivos, las aplicaciones de las Recomendaciones UIT-T de la serie J.200 y el software restante utilizado durante la fase de arranque y durante las descargas. Además, incluye tecnología kernel confiable que crea un entorno de confianza para la conmutación entre contextos. Toda la seguridad del software de cliente proporcionado por el operador de cable en el CPE DEBERÍA estar vinculada al esquema de confianza del sistema de acceso condicional en lugar de crear otro modelo de confianza autónomo y diferente.

6.3.6.2 Interfaz de usuario avanzada

Las Recomendaciones UIT-T de la serie J.200 y las aplicaciones basadas en la cabecera del sistema de cable pueden utilizarse conjuntamente con otros elementos de la arquitectura NG-STB-A a fin de disponer de interfaces de usuario avanzadas para nuevos servicios. Dado que la arquitectura de red de la próxima generación permitirá una variedad mucho mayor de servicios y la rápida introducción de nuevos servicios, será un factor importante disponer de interfaces de usuario intuitivas, convenientes y de fácil aprendizaje.

El modelo de referencia NG-STB-A tiene por objeto soportar nuevos conceptos de la interfaz de usuario software y hardware adicionales a los que se desarrollan sobre la base de los mandos y teclados a distancia básicos, tales como:

- controles a distancia avanzados con nuevos dispositivos de entrada, como por ejemplo, superficies táctiles, dispositivos de apuntamiento y teclados definidos por software;
- controles a distancia u otros dispositivos auxiliares con pantallas adicionales a la pantalla principal que permitan visualizar a una o a varias personas que se encuentren en la misma habitación mensajes, páginas web, navegación en general, información de ayuda o de control;
- dispositivos de entrada/salida atípicos, como por ejemplo, realimentadores de esfuerzo de controles de juegos, dispositivos de vibración asociados al contenido de programas y generadores de efectos especiales con efectos de sonido tridimensionales.

A fin de soportar dichas facilidades, se define un puerto de ampliación normalizado (véase la cláusula 7) que pueda ser utilizado para la conexión de dispositivos externos con un dispositivo de interfaz de usuario avanzada externa.

6.4 Arquitectura de servicios multimedia basados en IP

Los servicios multimedia del núcleo IP incluyen servicios de datos de alta velocidad y telefonía basada en VoIP. Es previsible que los proveedores de servicios por cable aumenten sus ofertas multimedia basadas en IP de servicios interactivos para incluir, entre otros ejemplos representativos, los servicios siguientes: la compartición y representación de fotografías de alta calidad, la videoconferencia y la videotelefonía con movimiento completo, la mejora de presencia para medios de comunicaciones emergentes, la compartición de aplicaciones y herramientas colaborativas así como juegos con varios participantes en línea. La arquitectura de servicios multimedia basados en IP de la próxima generación constituirá una plataforma que permitirá una gran variedad de aplicaciones con una amplia gama de equipos de cliente y un conjunto más rico de servicios.

Muchos servicios multimedia basados en IP son sensibles al retardo de la red, a la variación de fase y al caudal; la arquitectura NG-STB-A permite el tratamiento de la calidad de servicio (QoS) extremo a extremo para tráfico de datos asociado a servicios multimedia basados en IP accesibles desde dispositivos en los dominios de la red del hogar. Además de ofrecer calidad de servicio, permite la prestación y supervisión de servicios, la gestión de los derechos digitales y las funciones necesarias para atravesar dominios con funciones de traducción de red (NAT).

Los servicios multimedia basados en IP se cursan a través de canales IP transparentes:

i) entre la cabecera de cable y el cliente; y

ii) dentro de los dominios en la red del hogar, incluyendo contenidos protegidos (dominio de servicio autorizado, ASD) y calidad de servicio gestionada (dominio de servicio garantizado, GSD).

La arquitectura NG-STB-A no define las capas de red física, pero puede incluir redes del hogar con o sin cable coaxial, por ejemplo, con cableado CAT5, HomePlug o inalámbrico. Aunque la NG-STB-A para distintos tipos de servicios podría soportar cualquier capa física, existe en general preferencia por capas físicas (PHY) que soporten QoS y dispongan de capacidad para varios canales de alta definición.

Los potenciales puntos extremos de servicios multimedia basados en IP pueden incluir dispositivos de abonado de las Recomendaciones UIT-T de la serie J.200 conectados a la red coaxial, computadoras personales que compartan una conexión de datos de alta velocidad DOCSIS sobre la red del hogar y dispositivos inalámbricos personales con funciones de movilidad y que sean de utilidad en el hogar. A continuación se enumeran un conjunto prospectivo de aplicaciones multimedia basadas en IP que utilizan ese tipo de CPE:

- Computadoras personales ubicadas en la red de datos IP del hogar configuradas como servidores de medios y a las que acceden los equipos de vídeo de abonado en la red IP del hogar para presentaciones de alta fidelidad de música, vídeo o imágenes estáticas.
- Consolas de juegos que disponen de interfaces con los equipos de vídeo y las redes de datos de acceso y del hogar, y que permiten participar en sesiones de juegos en línea con varios jugadores.
- Terminales de videotelefonía y dispositivos de comunicaciones móviles o inalámbricas que disponen de facilidades de red con calidad de servicio mejorada, al tiempo que comparten infraestructura con otros servicios del hogar.
- Equipos domésticos para el acceso a Internet que permitan visualizar la identidad del llamante, el registro de las llamadas y la recuperación de mensajes en dispositivos de vídeo y en computadoras personales del cliente.

La arquitectura NG-STB-A soportará ampliaciones de la red de cable que permitirán a los operadores de cable establecer acuerdos y/o competir con proveedores de servicios de voz y de datos por medios inalámbricos mediante la oferta de servicios tales como:

- Servicios de mensajería unificada que integren servicios fijos y de servicios móviles basados en numeración universal, correo electrónico de voz, facsímil, desvío de llamadas de voz, correo electrónico, mensajería multimedia y redes privadas virtuales.
- Movilidad IP e itinerancia entre servicios basados en módem de cable y en redes públicas WiFi.
- Despliegue de puntos de acceso en la planta externa para facilitar servicios WiFi u otra cobertura utilizando tecnología inalámbrica en ubicaciones públicas.

6.4.1 Transporte

Los servicios multimedia se prestarán mediante IPv4, en modo unidifusión y en modo multidifusión. Será necesario utilizar posteriormente IPv6 para garantizar las capacidades futuras de la NG-STB-A conforme se conecten a la red un número cada vez mayor de dispositivos.

Las redes de área regional estarán basadas en IP, siendo previsible que el transporte se haga mediante tecnologías Gigabit Ethernet, por ejemplo, 1GigE y 10GigE. Probablemente se comparta una infraestructura de red de área regional que sea compartida por las arquitecturas de los servicios de vídeo y los servicios multimedia basados en IP.

El plan asociado a la NG-STB-A no prescribe las capas físicas (PHY) de la red de datos del hogar. Sin embargo, cualquier capa física adecuada DEBE satisfacer dos requisitos:

- La capa física (PHY) DEBE ser transparente a nivel IP para los servicios en todos los dominios de la red del hogar.
- En el caso de servicios con QoS en el dominio de red del hogar, la PHY DEBE poder ser gestionada con criterios de calidad de servicio.

Los abonados PUEDEN seleccionar alguna de posibles opciones que son transparentes a nivel IP. No obstante, las combinaciones PHY/MAC que puedan ser gestionadas con criterios de QoS por los protocolos NG-STB-A ofrecerán al usuario una mejor experiencia. Asimismo, no todas las opciones a nivel de PHY soportarán aplicaciones de gran anchura de banda tales como flujos con varios canales de alta definición. Los siguientes son ejemplos de capa PHY transparente a nivel IP que puede ser utilizada en los sistemas NG-STB-A: líneas telefónicas basadas en sistemas inalámbricos WiFi 802.11a/b/g, utilización del cableado de la instalación eléctrica, cable coaxial y cable trenzado (CAT 5).

6.4.2 Calidad de servicio extremo a extremo

La experiencia global de un usuario dependerá del tratamiento extremo a extremo que reciba el tráfico del servicio de red en cuestión. En consecuencia, es importante analizar detenidamente las fronteras entre los segmentos de red para garantizar una adecuada coordinación en la gestión de la calidad global de la sesión.

Un posible enfoque en el contexto de una red multimedia de la próxima generación es diferenciar tres segmentos de red en sentido amplio: la red de área regional (RAN, *regional area network*), definida como el núcleo de red que la red de acceso; la red de acceso, definida como el segmento de red HFC que conecta el CMTS y el módem de cable (CM, *cable modem*); y, finalmente, la red del hogar, definida en sentido amplio como la topología de red (agnóstica en relación con la capa física) que existe en el hogar más allá del CM.

La arquitectura NG-STB-A hace referencia a los mecanismos desarrollados al amparo de los proyectos IPCablecom e IPCable2Home. El proyecto IPCablecom Multimedia (IPCMM) se centra en el segmento de acceso, mientras que IPCable2Home se centra en el segmento de red del hogar. Además, la NG-STB-A define un puente o pasarela entre la red coaxial en el hogar (típicamente una

extensión de la acometida coaxial a los equipos de TV u otros dispositivos de vídeo en el hogar), y las redes de datos en el hogar (típicamente propiedad del abonado y frecuentemente diferente a coaxial, que permite aplicaciones basadas en computadoras personales).

6.4.2.1 Calidad de servicio en la red de área regional

Muchas redes de área regional (RAN) se encuentran en un proceso de maduración con el objetivo de poder diferenciar trayectos (utilizando métricas de calidad asociadas) en base al marcado de paquetes. IPCablecom Multimedia soporta sobre la RAN las estrategias basadas en DiffServ que permiten al operador de red asociar un punto de código DiffServ (DSCP, *DiffServ code point*) a cada flujo de servicio en sentido ascendente. Todos los paquetes de dicho flujo serán marcados con dicho DSCP antes de acceder a la RAN. Igualmente, IPCablecom Multimedia tiene capacidad para distinguir los flujos del tráfico entrante descendente recibidos de la RAN y acomodar dicho tráfico en el flujo de servicio adecuado en función de las marcas DSCP (así como mediante mecanismos convencionales de direcciones de origen y terminación IP y de capa MAC). La correspondiente arquitectura se describe en la Rec. UIT-T J.174.

Aunque las arquitecturas de red externas a las RAN quedan fuera del campo de aplicación del proyecto NG-STB-A, se reconoce la existencia de potenciales beneficios derivados de acuerdos para el intercambio de tráfico de contenidos y servicios que vayan más allá de los actuales acuerdos de intercambio de tráfico de datos de alta velocidad. Por ejemplo, mantener las llamadas de VoIP "dentro de la red" ("on-net") puede generar ahorros significativos. Ese es particularmente el caso en las zonas geográficas donde los operadores de cable tienen RAN adyacentes. Dichos acuerdos de intercambio de tráfico pueden incluir interfaces hardware, protocolos y sistemas de "liquidación" adecuados.

6.4.2.2 Calidad de servicio en la red de acceso

El prerrequisito fundamental en términos de calidad de servicio (QoS) en la red de acceso es la capacidad de gestionar la anchura de banda para el tráfico con prioridades.

Un posible enfoque para dicha gestión es garantizar la anchura de banda requerida para los servicios especificados sobre los segmentos de acceso, asignando permanentemente parte de la anchura de banda disponible al tráfico con prioridad. El tráfico se diferencia mediante las marcas de QoS de los paquetes, que se cursan por los trayectos asignados individualmente. El método de encolamiento con prioridad es también una solución efectiva para garantizar la QoS en la red de acceso.

El tráfico priorizado recibe la correspondiente prioridad para utilizar la anchura de banda, evitando así retardos de red y degradación de la variación de fase y del caudal.

Aunque en la especificación IPCablecom Multimedia, Rec. UIT-T J.179, se han identificado varios elementos de red e interfaces clave, no se ha definido un protocolo para el establecimiento de la sesión. La arquitectura NG-STB-A reconoce la predominancia del protocolo SIP en muchas de las aplicaciones multimedia actuales. Uno de los objetivos de dicha arquitectura es soportar una amplia variedad de aplicaciones y mecanismos de establecimiento de sesión conexos. La NG-STB-A permitirá implícitamente la utilización del protocolo SIP, además de otros mecanismos de establecimiento de sesión específicos de cada aplicación.

6.4.2.3 Calidad de servicio en la red del hogar

Las especificaciones de IPCable2Home tienen por objetivo proporcionar una arquitectura basada en el protocolo Internet (IP) para los servicios sobre redes gestionadas del hogar.

La arquitectura de red del hogar NG-STB-A está en pare definida mediante determinados aspectos [b-UIT-T J.192] sobre IPCable2Home. No obstante, la versión actual de [b-UIT-T J.192] sólo incluye QoS con prioridad a través de la red en el hogar para dispositivos que incluyen el software de punto frontera de QoS de IPCable2Home. {Texto informativo: A fin de permitir íntegramente los objetivos de QoS de NG-STB-A, [b-UIT-T J.192] deberá ampliarse para proporcionar un

control de QoS parametrizada mediante mecanismos de puente entre UPnP e IPCablecom Multimedia.}

Las capacidades de QoS PUEDEN o NO ser ofrecidas al cliente final en función de las tecnologías de capa 2 utilizadas y la ubicación del cliente en la red. Desde una perspectiva de QoS, el cliente puede residir en uno de los dos dominios de la red en el hogar, a saber, el dominio de servicio garantizado (GSD) o fuera del GSD. Cuando un cliente reside en el GSD, tiene a su disposición capacidades de QoS para establecer no sólo QoS dentro de la red del hogar, sino también para establecer un puente entre la QoS dentro del hogar y la red de acceso a fin de poder aplicar QoS extremo a extremo. En el caso de clientes que están fuera del GSD, éstos no disponen de QoS en el hogar; sin embargo, el cliente PUEDE disponer de QoS en el acceso y en la RAN mediante señalización a nivel de aplicación. Este tipo de cliente suele ser un dispositivo preexistente que no discierne niveles de QoS, pero que puede beneficiarse de la aplicación de QoS a nivel de acceso.

Para establecer un puente entre la red de acceso y las redes del hogar, un dispositivo IPCable2Home puede aprovechar los mecanismos de clasificación de paquetes de DOCSIS 1.1 y utilizarlos en IPCablecom Multimedia. Es posible identificar y transmitir paquetes salientes del segmento de red en el hogar en función de varias características, incluyendo las direcciones y puertos de origen y terminación a nivel IP y de capa MAC, el marcado DiffServ/ToS y las etiquetas VLAN 802.1q.

Actualmente, IPCable2Home 1.1 [b-UIT-T J.192] ha adoptado un esquema de marcado de paquetes y de encolamiento con prioridad basado en 802.1q. {Texto informativo: Es previsible que ulteriormente se produzca un alineamiento entre las capacidades QoS de IPCable2Home y las definidas mediante UPnP.}

En el caso de dispositivos que residen en el GSD, los enlaces existentes en la red en el hogar entre la pasarela y el dispositivo GSD deben soportar QoS paramétrica. {Texto informativo: Además, el dispositivo cliente, ha de ser conforme con los requisitos del punto frontera de calidad IPCable2Home (que son un superconjunto de los requisitos de los dispositivos UPnP).}

NG-STB-A proporcionará interfaces a nivel de aplicación que permitan a los servicios clientes solicitar recursos de anchura de banda y de contenidos. El segmento de red específico en el que residan dichos recursos determinará la interfaz a la que se accederá. Es deseable mantener un lenguaje común para simplificar los requisitos de la aplicación. {Texto informativo: Entre los ejemplos de dichas interfaces PUEDEN estar IPCablecom Multimedia con extensiones SOAP/XML, IPCable2Home con QoS UPnP y ampliaciones de aplicaciones de red del hogar de las Recomendaciones UIT-T de la serie J.200.} Estas mejoras proporcionarán un mecanismo normalizado para la interfaz de aplicación.

6.4.3 IPv6

A fin de soportar los previsibles despliegues a gran escala, será necesario que los clientes de la red puedan utilizar IPv6. Este requisito es necesario para garantizar la recuperación de las inversiones de capital realizadas y garantizar que el espacio de direccionamiento sea suficientemente grande para permitir una amplia difusión de los servicios de telemetría así como de otros servicios asociados a mercados más reducidos. Aunque aún no se han definido estrategias de coexistencia y de transición a IPv6, la utilización de IPv6 puede interpretarse como una mejora del software. Por lo tanto, no DEBERÍAN ser necesarias mejoras de hardware para poder utilizar IPv6 en dispositivos conformes con NG-STB-A (esto PUEDE o NO ser cierto para dispositivos preexistentes).

6.4.4 Seguridad y privacidad

A fin de proporcionar un servicio de telemetría, es imperativo considerar la privacidad y, por tanto, la seguridad de los datos de usuario. La arquitectura NG-STB-A proporcionará mecanismos para permitir que un punto extremo autentique una petición y que asegure su respuesta a dicha petición. Las características siguientes son necesarias para una telemetría segura y otras aplicaciones de control:

- todos los puntos extremos tendrán identidades que han sido definidas en fábrica;
- se mantendrán mecanismos criptográficos seguros (tales como AES, 3DES) en todos los elementos de ajuste, pasarelas, de red y de cliente; y
- todas las comunicaciones de gestión (XML, SNMP) podrán ser realizadas con seguridad.

6.5 Arquitectura de la red del hogar

En esta cláusula se hace referencia a la "red del hogar" dentro del ámbito y entre las posibles redes que existirán en un hogar.

Aunque muchos hogares tienen hoy en día una o más redes, éstas no están por lo general bien integradas con el sistema de cable y proporcionan un soporte limitado para servicios multimedia (por ejemplo, distribución en modo mejor esfuerzo de vídeo de baja calidad frente a la distribución garantizada de vídeo de alta definición). La presencia en el hogar de servicios proporcionados por el operador de cable y de contenidos permitirá que participen en los mismos un número mayor de dispositivos, así como nuevas oportunidades para nuevos servicios y modelos de negocio.

La arquitectura de red de la próxima generación incluirá una arquitectura completa de red del hogar que permita la transferencia sin discontinuidades del tráfico entre dispositivos situados en el lado de la planta externa de cable (por ejemplo, DOCSIS, MPEG-TS) y las diversas tecnologías/segmentos de red del hogar. Uno de dichos modelos incluye las Recomendaciones UIT-T de la serie J.200 en los dispositivos cliente y servidor (por ejemplo, un SVD de gama baja que se comunica con un SVD de gama alta). {Texto informativo: Además, la NG-STB-A también PUEDE definir interfaces de aplicación, tales como una interfaz de usuario (UI) distante UPnP, que serían independientes del sistema operativo y del middleware en determinados dispositivos.}

Los siguientes son ejemplos de servicios y aplicaciones que soportaría dicha arquitectura de red en el hogar:

- Un dispositivo de vídeo de abonado de gama baja (SVD) podría acceder a un SVD de gama alta que funcione como grabador de vídeo digital (DVR, *digital video recorder*) en la red coaxial con el objetivo de visualizar contenidos almacenados en el disco duro del SVD de gama alta. Por lo tanto, el SVD de gama baja accedería a la función de aplicación DVR del dispositivo de gama alta sin el coste de tener que disponer de un disco duro adicional pudiendo disfrutar así de la capacidad de visionar de forma unificada el contenido almacenado en varias ubicaciones del hogar.
- Un SVD de gama baja con memoria y potencia de procesamiento limitadas podría acceder a aplicaciones basadas en Recomendaciones UIT-T de la serie J.200 ejecutadas sobre SVD de gama alta y disponer de las aplicaciones como si la aplicación residiera en el SVD de gama baja.
- Un SVD en la red coaxial en el hogar podría acceder a vídeos o contenidos multimedia residentes en una computadora personal no ubicada en la red coaxial en el hogar, o viceversa.
- El tráfico de mensajes podría pasar entre la red coaxial del hogar y la red no coaxial a fin de permitir aplicaciones tales como la visualización de la identidad del llamante sobre una TV conectada a un SVD, o la visualización del resumen de la bandeja de mensajes de entrada en una TV conectada a un SVD.

El tráfico más exigente en la red del hogar en términos de anchura de banda probablemente sea la TV de alta definición (HDTV, *high definition TV*). Son preferibles las capas físicas (PHY) que proporcionen capacidad para varios canales de HDTV en tiempo real, tanto dentro como entre las diversas tecnologías y segmentos de la red en el hogar.

El proyecto IPCable2Home ha definido un elemento pasarela para la red del hogar que actúa como puente entre la red DOCSIS del operador de cable y la red o redes del abonado en el hogar. Esta pasarela se ha diseñado para ser aprovisionada y gestionada de forma segura y, adicionalmente, para poder priorizar paquetes transferidos entre los segmentos DOCSIS y de la red en el hogar. La arquitectura de red del hogar de la próxima generación complementará los elementos principales definidos en el proyecto IPCable2Home con las consideraciones necesarias para el transporte de contenidos de alta calidad (por ejemplo, contenidos que requieren la gestión de derechos y obligaciones estrictas de QoS) dentro de cada red y entre redes, a fin de gestionar varios segmentos LAN y para la admisión de dispositivos clientes en la red.

6.5.1 Elementos y dominios de la arquitectura general

Un elemento pasarela amplía la funcionalidad de los servicio de portal (PS) de IPCable2Home. Este elemento pasarela adapta el segmento o segmentos de la red del hogar a la red de la capa MAC y, posiblemente MPEG-TS; su funcionalidad incluye la transferencia entre y dentro de segmentos y tecnologías de la red del hogar. La pasarela PUEDE presentar muchas implementaciones físicas, desde ser módems xDSL o módems de cable integrados, hasta combinaciones de módems/NAT, o implementaciones de SVD de gama alta.

Tal como se muestra en la figura 5, la pasarela puede soportar varias tecnologías de transporte que permitan que el tráfico se transfiera sin discontinuidades en las instalaciones del cliente en un entorno IP agnóstico respecto al transporte. El tráfico de la red del hogar PUEDE incluir varias combinaciones de contenidos, control de contenidos, navegación y compartición de aplicaciones que permitan la interacción entre datos, videos o servicios multimedia basados en IP.

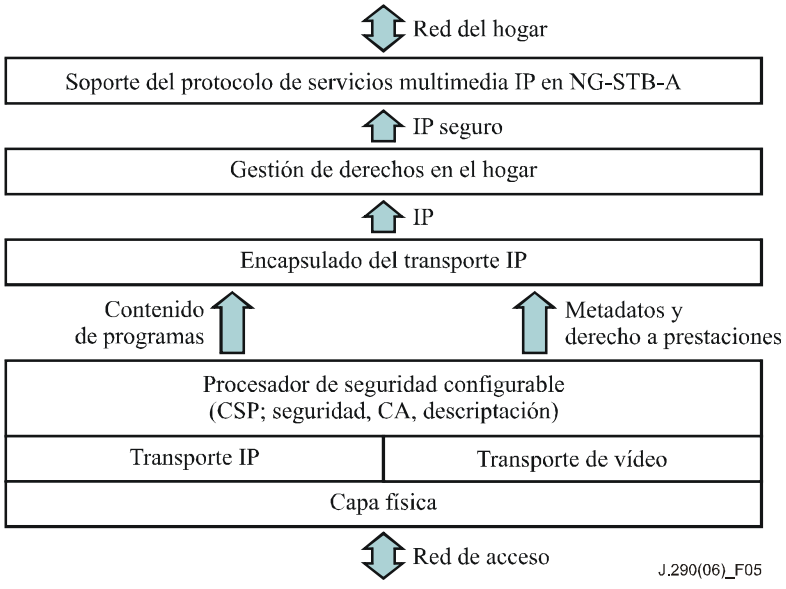


Figura 5 – Arquitectura de comunicaciones de la pasarela

Las diversas tecnologías de red del hogar no están especificadas a nivel de la capa de control de acceso al medio (MAC, *media access control*) ni de la capa física. Son candidatas a constituir dichas capas cualquier capa conocida o futura que soporte el protocolo Internet a alta velocidad. {Texto informativo: Entre los ejemplos de tales capas cabe señalar Ethernet sobre CAT5, HomePlug para la utilización del cableado eléctrico, Home PNA, MoCA y 802.11a/b/g/n.}. Es

previsible que en numerosos hogares se utilicen múltiples tecnologías de red del hogar para satisfacer una amplia gama de necesidades.

Se asume que los diversos segmentos de red del hogar están basados en IP; además de permitir aplicaciones de datos de alta velocidad, IP permite una capa de interoperabilidad normalizada y de carácter ubicuo, válida a través de múltiples tecnologías de red y dispositivos.

Tal como se muestra en la figura 6, en la arquitectura de comunicaciones de la red del hogar existen dominios funcionales que se modifican mediante la gestión de la QoS y en términos de gestión de derechos (protección de los contenidos).

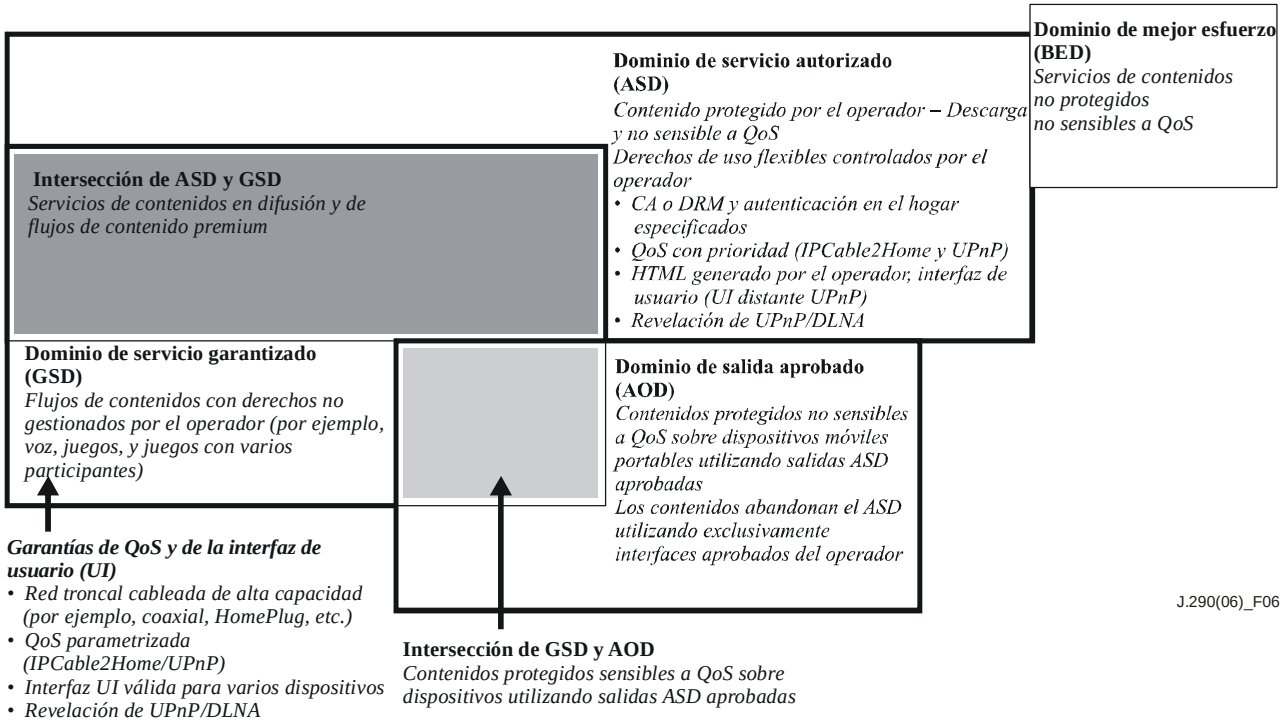


Figura 6 – Dominios de la red del hogar – Visión general

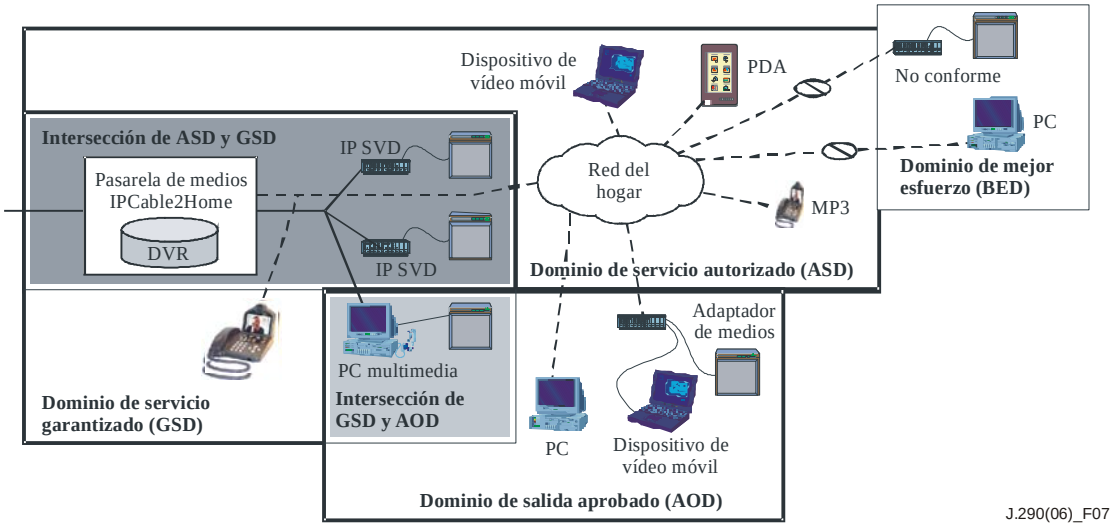


Figura 7 – Dominios de la red del hogar – Ejemplos

Dominio de servicio garantizado (GSD)

Si las garantías de QoS pueden mantenerse desde la cabecera de red hasta el cliente, se considera que éste forma parte del dominio de servicio garantizado.

A fin de ofrecer una QoS garantizada, el cliente DEBE permitir la utilización de la pertinente señalización de QoS: la tecnología de red del hogar a la que el cliente esté conectado DEBE proporcionar garantías asociadas a los parámetros de QoS necesarios, tales como anchura de banda, variación de fase y retardo, y DEBE tener capacidad suficiente para transportar varios flujos de alta definición. {Texto informativo: Las tecnologías cableadas basadas en coaxial (MoCA), las asociadas a las líneas eléctricas (HomePlug) y a la línea telefónica (HPNA 2.0) son ejemplos de tecnologías que en el futuro tratarán de satisfacer estos requisitos.}

{Texto informativo: La pasarela del hogar DEBE soportar la adecuada señalización de la QoS y los medios necesarios para establecer un puente entre la QoS en el hogar y la QoS en la red de acceso, y DEBE implementar la funcionalidad de QoS de IPCable2Home, mientras que el dispositivo del cliente DEBE implementar la QoS UPnP. La funcionalidad de QoS de IPCable2Home es un superconjunto de la QoS UPnP.} Por lo tanto, un cliente dado PUEDE estar en el GSD cuando esté conectado a un segmento de la red del hogar y no estar en el GSD cuando esté conectado a otro segmento. Igualmente, un segmento dado puede tener algunos clientes que se encuentren en el GSD y otros que no lo estén en base al nivel de QoS soportado por cada dispositivo de cliente y aplicación.

{Texto informativo: Todos los dispositivos y el contenido almacenado en este dominio pueden ser detectados empleando un mecanismo que emplea UPnP/DLNA (*digital living network alliance*, anteriormente denominado *digital home working group* o DHWG). La pasarela en el hogar actúa como servidor de detección centralizado para la LAN del hogar. El operador de cable puede acceder a esta información a través de una interfaz MIB definida de conformidad con IPCable2Home.}

Los dispositivos que se encuentren en el GSD podrán recibir servicios de contenidos sensibles a la QoS, tales como VoIP, juegos interactivos con varios participantes y videotelefonía IP. Este contenido PUEDE o no incluir protección de contenidos de terceros basada en DRM.

Dominio de servicio autorizado (ASD)

Los dispositivos presentes en este dominio pueden autenticarse y permitir la utilización de derechos sobre contenidos, tal como defina el operador de red. Este segmento incluye dispositivos que son conformes con la gestión de derechos digitales en el hogar especificada más adelante.

No es necesario proporcionar QoS a los dispositivos en el ADS. {Texto informativo: Sin embargo, los dispositivos de cliente PUEDEN soportar QoS basada en prioridad y, por tanto, DEBERÍAN implementar la señalización QoS UPnP.} La tecnología de red del hogar DEBERÍA soportar QoS basada en prioridad, particularmente en segmentos en los que circulan flujos sensibles al retardo y a la anchura de banda.

{Texto informativo: Todos los dispositivos y los contenidos almacenados en este dominio pueden detectarse utilizando mecanismos de detección definidos de acuerdo con UPnP/DLNA.}

Los dispositivos presentes en el ASD podrán recibir servicios de contenidos no sensibles a la QoS, tales como música, vídeo que no sea en tiempo real o vídeo de baja velocidad.

Dominio de salida aprobado (AOD)

Los dispositivos de este dominio están conectados al ASD mediante interfaces de salida aprobadas por el operador. Cuando el contenido fluye desde el ASD al AOD, las reglas de utilización del operador traspasan la interfaz. Actualmente, 5C sobre 1394 y DHCP sobre DVI (o la interfaz multimedia de alta definición, HDMI, *high definition multimedia interface*) son interfaces de salida digital normalizados en los despliegues de cable realizados en Norteamérica. Por ejemplo, una interfaz que PUEDE llegar a ser establecida es una interfaz de DRM que permita la comunicación

de contenidos y reglas de utilización a sistemas DRM de terceros, distintos del sistema DRM del operador.

Un operador renuncia al control directo del contenido una vez que éste pasa al AOD. Ésta es una diferencia fundamental entre ASD y AOD.

Un dispositivo PUEDE recibir contenidos desde el ASD a través de una interfaz adecuada. No es obligado que el dispositivo satisfaga ningún otro requisito relativo a la QoS o la detección de dispositivos. No obstante, algunos dispositivos del AOD podrán participar en el dominio de servicio garantizado (GSD) en la medida que éste esté relacionado con la detección de dispositivos y la QoS. Todos los dispositivos del AOD podrán recibir contenidos no sensibles a la QoS que tengan restricciones de utilización impuestas por el operador en función de la interfaz de salida aprobada.

Los medios que pueden retirarse, tales como DVD regrabables, tarjetas de tipo flash y discos CD-R se encuentran típicamente en el AOD.

Dominio de mejor esfuerzo (BED)

Los dispositivos y segmentos de capa física que no sean conformes con los requisitos de los tres dominios anteriores PUEDEN ser detectados y participar en servicios que no requieran la protección de los contenidos ni una calidad de servicio garantizada.

Intersección de GSD y ASD

Los dominios GSD y ASD son independientes; un dispositivo puede no pertenecer a ninguno, pertenecer a uno de ellos o a ambos. Los dispositivos que pertenecen a ambos pueden disponer de garantías de QoS, autenticarse por sí mismos y soportar los DRM en el hogar. Dichos dispositivos representen un nivel superior de cumplimiento y PUEDEN recibir contenidos de alto valor con restricciones de utilización impuestas por el operador.

Intersección de GSD y AOD

Los dominios GSD y AOD son independientes; un dispositivo puede no pertenecer a ninguno, pertenecer a uno de ellos o pertenecer a ambos. Los dispositivos que pertenecen a ambos pueden proporcionar garantías de QoS para los contenidos que fluyan desde ASD a AOD sobre interfaces aprobadas. Dichos dispositivos podrán recibir contenidos protegidos y sensibles a QoS con restricciones de uso impuestas por el operador en función de la interfaz aprobada.

Exclusividad de ASD y AOD

Los dominios ASD y AOD son mutuamente excluyentes. Un dispositivo puede pertenecer al ASD, al AOD o a ninguno de ellos.

El cuadro 2 resume los requisitos funcionales asociados a dispositivos en diferentes dominios.

Cuadro 2 – Requisitos funcionales de los distintos dominios y servicios ofrecidos

Funcio-nalidad[a)]	ASD – Derechos de uso flexibles controlado por el operador de red	GSD – Garantías de QoS, interfaz de usuario consistente	AOD	ASD+GSD	AOD+GSD	BED
Seguridad	Autenticación más CA o DRM del hogar basados en CSP NG-STB-A	Ninguna	Seguridad de la interfaz de salida aprobada	Autenticación y CA o DRM del hogar	Seguridad de la interfaz de salida aprobada	Ninguna
QoS	QoS con prioridades (QoS UPnP) – **Opcional**	QoS parametrizada (IPCable2Home o UPnP)	Ninguna	QoS parametrizada (IPCable2Home o UPnP)	QoS parametrizada (IPCable2Home o UPnP)	Ninguna
UI consistente	Deseable	Sí	Ninguna	Sí	Sí	Ninguna
Gestión	IPCable2Home PS[b)] (para la pasarela) o IPCable2Home BP[c)] (para el cliente) – **Opcional**	PS IPCable2Home (para la pasarela) o BP IPCable2Home (para el cliente)	Control de salida seleccionable	IPCable2Home PS (para la pasarela) o IPCable2Home BP (para el cliente)	IPCable2Home PS (para la pasarela) o IPCable2Home BP (para el cliente)	Control de salida seleccionable
Detección	UPnP/DLNA	UPnP /DLNA	Ninguna	UPnP /DLNA	UPnP /DLNA	Ninguna
Servicios	Contenido protegido no sensible a la QoS con total flexibilidad para establecer los derechos de utilización	Servicios de contenidos no protegidos sensibles a la QoS por ejemplo, juegos interactivos, voz y videotelefonía	Servicios de contenidos protegidos no sensibles a la QoS con flexibilidad limitada para establecer los derechos de utilización	Servicios de contenidos de alto valor con total flexibilidad para establecer los derechos de utilización	Servicios de contenidos protegidos sensibles a la QoS con flexibilidad limitada para establecer los derechos de utilización	Contenido no protegido no sensibles a la QoS

a) En este cuadro se asume que todos los dispositivos de estos dominios tienen una interfaz de red del hogar.

b) PS IPCable2Home incluye la funcionalidad de punto de control UPnP.

c) BP IPCable2Home es un superconjunto de la QoS UPnP y otras funcionalidades UPnP.

d) Todas las descripciones UPnP y DLNA del cuadro 2 son meramente informativas.

Si no está disponible la gestión de la red del hogar NG-STB-A, los dispositivos CPE conformes con NG-STB-A-DEBERÍAN estar diseñados para seguir funcionando, aunque posiblemente a un nivel reducido. Los dispositivos programables PUEDEN ser conformes con dicha arquitectura cuando ejecuten determinadas aplicaciones y no serlo cuando ejecuten otras aplicaciones.

La estructura NG-STB-A propuesta anticipa la ejecución de clientes seguros y compatibles sobre PC de forma que los contenidos gestionados con derechos puedan intercambiarse entre los SVD y los PC. Un ejemplo de dicha aplicación puede ser ver un vídeo de un PC a partir de un DVR incluido en un SVD. Alternativamente, un PC puede asumir el papel de servidor de vídeo o de música que permita el acceso de un SVD a su contenido. Por ejemplo, un PC puede servir como un contestador automático avanzado o también se podría visualizar la información del llamante en la pantalla de TV.

6.5.2 Gestión de derechos digitales

El contenido se distribuye a cada SVD del dominio de servicio autorizado utilizando el sistema de acceso condicional (CA) gestionado por la cabecera. Cada SVD utiliza un protocolo de comunicación entre pares (*peer-to-peer*) con la protección contra copia que proporciona el sistema

de gestión de derechos digitales (DRM) de la red del hogar. El plan de NG-STB-A asume que cada dispositivo incluye clientes seguros que pueden autenticarse mutuamente entre sí mediante firmas digitales o una tecnología de intercambio de claves normalizada. El CSP PUEDE proporcionar capacidades de puente entre el CA de la red de cable y la DRM de la red del hogar.

En la arquitectura para el hogar NG-STB-A propuesta, un SVD de la red puede tener acceso a características y contenidos de otro dispositivo que se encuentre en las redes del GSD o del ASD. Utilizando algoritmos normalizados para la criptación de contenidos en el sistema de gestión de derechos (RMS, *rights management system*), el RMS soportará la grabación de varios flujos de vídeo, su visualización en tiempo real y múltiples sesiones de visionado.

El sistema de gestión de derechos de NG-STB-A podrá traducir los estados del derecho a prestaciones y la protección contra copia a la red del hogar. El sistema de gestión de derechos de NG-STB-A utilizará nuevos conceptos y tecnologías en el área de la gestión de claves cuando funcione con sistemas preexistentes que utilicen criterios de compartición o reconfiguración de claves. Las claves y los derechos a prestaciones PUEDEN traducirse a partir de la información de control de copia (CCI, *copy control information*) del flujo de vídeo, a saber, los ECM y los EMM, para que puedan ser cargados directamente en las máquinas de descriptación sin quedar desprotegidos en la máquina de descriptación de contenidos del dispositivo de la red del hogar.

En el sistema de gestión de derechos del hogar propuesto en la arquitectura NG-STB-A, un fichero de derechos que contenga criterios de acceso a varios niveles de servicio y una clave de descriptación de contenido, estará normalmente firmado y criptado. La clave del contenido sería la clave a utilizar para descriptar el contenido, cuyo cambio PUEDE ser necesario con una periodicidad variable. Las restricciones a los derechos de utilización y a la protección contra copia serán descriptados y verificados en el CPE en comparación con los criterios de acceso del cliente a fin de otorgar la autorización pertinente. Si se concede la autorización, el elemento de acceso condicional (CA) genera la clave de contenidos, que se utiliza para descriptar el contenido en el dispositivo CPE sito en la red del hogar.

El sistema de gestión de derechos de la NG-STB-A realizará todos los procesos de generación de clave, criptado, descriptado, y algoritmos de firma digital e intercambio de claves dentro de hardware y software resistentes a la manipulación, diseñados para evitar la modificación o la revelación y análisis no autorizado del proceso, los parámetros de seguridad críticos y las claves privadas.

6.5.2.1 Vinculación entre CA y DRM

El acceso condicional (CA) de la red será responsable de gestionar el sistema de gestión de derechos de la NG-STB-A. Todos los DRM de terceras partes DEBEN ser previamente aprobados como salida aceptable antes de que el sistema de gestión de derechos de la NG-STB-A traspase derechos y contenidos. La DRM de terceros se tratará como parte del dominio de salida aprobado (AOD), tal como se ha definido anteriormente. Para soportar cualquier sistema de DRM de terceros no asociado con el CA de la red, se utiliza el sistema de gestión de derechos de la NG-STB-A para traducir los derechos al sistema DRM del tercero. Además, el sistema de gestión de derechos de la NG-STB-A se utilizará para autenticar cualquier dispositivo de DRM de terceros antes de compartir información sobre contenidos y derechos. El CSP soportará este proceso de traspaso.

6.5.3 Fuentes de contenido y clientes

La arquitectura de la red del hogar se especifica para contribuir a una interoperabilidad sin discontinuidades entre fuentes de contenido y clientes. Los repositorios de contenidos (es decir, bibliotecas de música, fotos y vídeo) que existen en clientes en red PUEDEN ser detectados, catalogados y retransmitidos en flujos a otros dispositivos de la red del hogar, e incluso opcionalmente ser ofrecidos a dispositivos autorizados fuera de la red del hogar.

Un objetivo clave de la arquitectura de red del hogar es la disponibilidad de una plataforma de red del hogar para el consumidor que sea conveniente, y no esté sobrecargada, al tiempo que se mantenga la integridad del contenido protegido (restringido) en el dominio de servicio autorizado (ASD). En este marco se incluyen varios supuestos clave:

- Todo el transporte de contenidos entre dispositivos conectados a la red del hogar se realiza en IP (protocolo Internet).
- La arquitectura de red transportará muchos tipos distintos de medios, incluyendo vídeo, audio, medios "estáticos" (por ejemplo, archivos JPEG) y datos.
- La arquitectura de red permitirá al mismo tiempo contenidos y servicios protegidos y ofrecidos por el operador de red, contenidos protegidos originados en fuentes alternativas (por ejemplo, una solución DRM de un tercero para música) y contenidos no protegidos (con independencia de la fuente).

Aunque PUEDEN existir varias arquitecturas de red del hogar que satisfagan los objetivos perseguidos, DEBEN tenerse en cuenta una serie de aspectos técnicos importantes:

- Sólo dispositivos autorizados (es decir, certificados) PUEDEN formar parte del ASD.
- La arquitectura DEBE soportar la transmisión y almacenamiento de contenidos distribuidos por el operador de red y de contenidos que distribuye el otro agente.
- El contenido protegido distribuido por el operador de red PUEDE ser almacenado y consumido en el ASD.
- El contenido protegido distribuido por el operador de red sólo PUEDE abandonar el dominio ASD a través de interfaces de salida aprobados.
- El contenido protegido y que no distribuye el operador de red PUEDE ser consumido y almacenado en el ASD.
- Si los enlaces de comunicación con la red de cable se interrumpen, la arquitectura de red del hogar DEBERÍA seguir funcionando durante un cierto periodo de tiempo cuya duración establece el operador de cable.

6.6 Publicidad digital avanzada

La NG-STB-A soportará la inserción de programas y tecnologías de reproducción en varios medios, tanto la inserción de publicidad por medios analógicos como digitales, permitiendo una amplia variedad de modelos[1] de publicidad avanzada, tales como:

- Publicidad digital sobre digital.
- Publicidad selectiva y dirigida.
- Publicidad interactiva (en todos los servicios).
- Publicidad en DVR:
  - Forma larga: contenidos distribuidos y almacenados localmente en el DVR.
  - Sustitución: refresco de contenidos publicitarios previamente grabados en el DVR.
  - DVR en red: refresco de contenidos publicitarios previamente grabados en un DVR en red (nDVR).

[1] La publicidad digital avanzada puede ser un servicio atractivo para operadores de servicios que desean ampliar sus estructuras de negocio. Es necesario armonizar los esquemas de negocio entre los operadores de servicio y los difusores.

- Publicidad en VoD:
  - Publicidad durante la selección de contenidos de VoD: contenido publicitario intersticial y contenido publicitario enviado cuando el usuario solicita un programa de VoD ("bumper ad").
  - Inserción publicitaria local en VoD: inserción de publicidad local en contenidos de VoD soportados por la publicidad.
  - VoD publicitario de un anunciante.
- Recopilación de datos a través de todos los servicios publicitarios para incluir contenidos sincronizados.
- Inserción de publicidad nacional, regional y local en todos los puntos de la red de cable, así como de fuentes externas a dicha red, como por ejemplo, de Internet.

7 Equipo en las instalaciones del cliente (CPE)

Esta cláusula de la NG-STB-A describe los elementos esenciales de los dispositivos CPE de vídeo y no de vídeo conformes con la NG-STB-A. Las variaciones y combinaciones innovadoras de dichos elementos que desarrollen los fabricantes serán de gran utilidad. El objetivo de la NG-STB-A es ofrecer a los fabricantes de equipos una plataforma con las menores limitaciones posibles.

7.1 Visión general

El segmento de red en las instalaciones del cliente conlleva numerosas oportunidades y desafíos para los fabricantes de electrónica de consumo, para los distribuidores de equipos de cliente y para la reglamentación, siendo éste el segmento objeto de las mayores inversiones, dado el gran número de dispositivos. Los CPE tendrán capacidades diversas. Por ejemplo, las opciones incluyen que se puedan soportar los servicios pasarela en la red de datos del hogar y la grabación de vídeo digital (DVR). El cuadro 3 resume las características y atributos clave de una amplia gama de dispositivos CPE conformes con la NG-STB-A.

Cuadro 3 – Visión general de las características de los CPE

	SVD básico	**SVD ampliado (no pasarela)**	**SVD ampliado (pasarela)**	**Cliente de medios**
Soporte de procesador de seguridad configurable (CSP)	✓	✓	✓	✓
Funciones de SVD ampliadas distintas a pasarela (por ejemplo, DVR, tarjeta de seguridad, visualización)		✓	✓	A definir
Pasarela de la red del hogar (servicios de portal IPCable2Home, punto de control UPnP)			✓	
Cliente de la red del hogar (punto frontera de IPCable2Home, señalización UPnP, QoS UPnP)	✓	✓		✓
Capacidades de la serie J.200	✓	✓	✓	Opcional
Anfitrión con USB 2.0 y/o Ethernet	✓	✓	✓	✓
NOTA – Todas las descripciones de UPnP del cuadro 3 son informativas.				

7.2 Dispositivos de vídeo de abonado (SVD)

Los dispositivos de vídeo de abonado (SVD) incluyen desde dispositivos con capacidades mínimas esenciales hasta dispositivos que proporcionan un conjunto más rico de capacidades.

Este equipo puede ser suministrado por el operador o por los suministradores de equipos de electrónica de consumo al por menor. Los SVD funcionan como decodificador multimedia. Algunos SVD pueden incluir receptores de TV digitales bidireccionales.

Estos dispositivos se denominan SVD porque cada uno proporciona funcionalidades adicionales a las de un decodificador multimedia convencional, como por ejemplo, un sistema de acceso condicional reconfigurable mediante un CSP, funcionalidad de códec de vídeo avanzado, opciones de transporte de múltiples señales de vídeo y de conexiones en red a la red del hogar. Cada SVD puede acceder a recursos o proporcionar recursos a otros dispositivos de la red. En otras palabras, todos los SVD PUEDEN actuar como fuente o como destino de contenidos en la red del hogar. Por lo tanto, a través de la red del hogar, el dispositivo de gama más baja puede disponer de algunas de las capacidades y prestaciones del dispositivo de gama más alta. Un sistema que sea conforme con esta Recomendación proporciona protección contra copia y el intercambio gestionado de derechos sobre contenidos ente cualquiera de los SVD de la red del hogar.

La figura 8 ilustra la capacidad del SVD para establecer conexiones con otros SVD y con otros dispositivos compatibles.

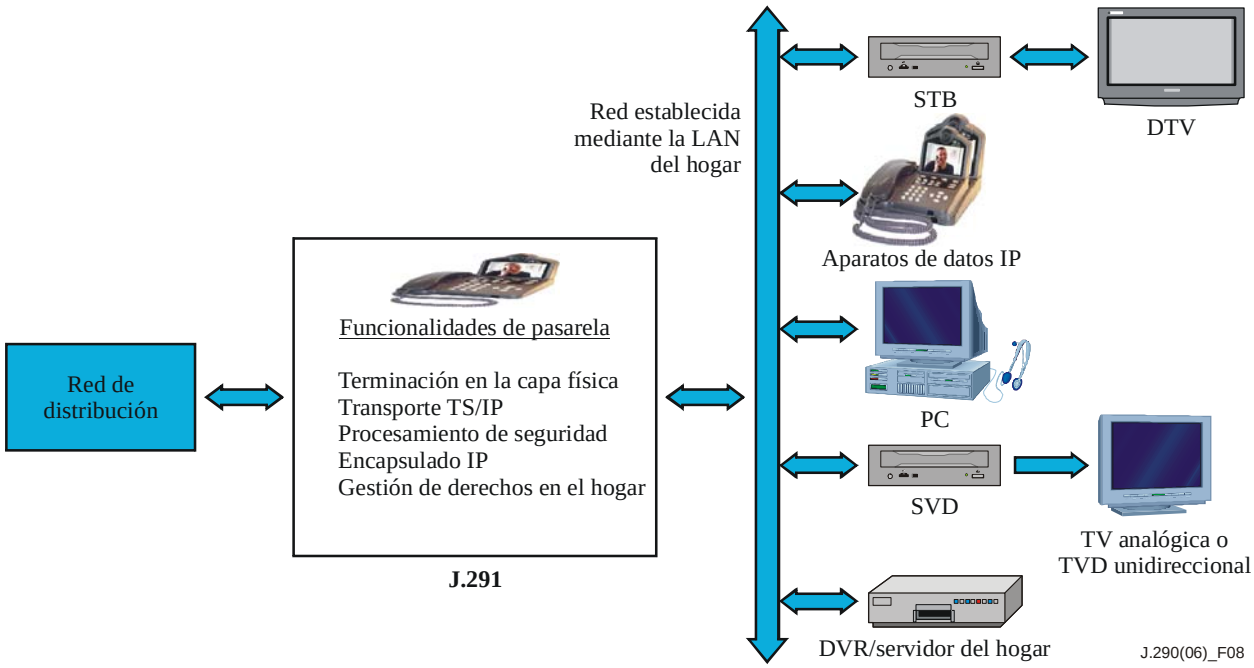


Figura 8 – Ejemplos de despliegue de CPE para abonados con redes de datos del hogar basadas en IP (con un sistema de DRM del hogar)

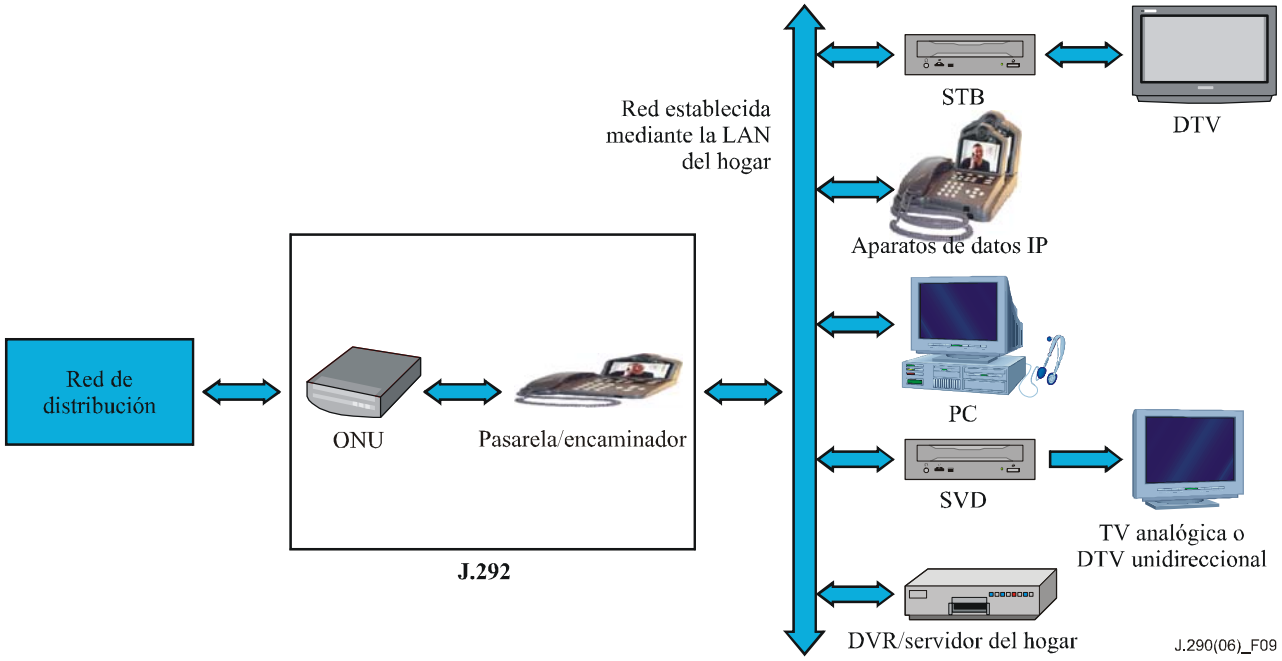


Figura 9 – Ejemplos de despliegue de equipos de cliente (CPE) para abonados con redes de datos del hogar basadas en IP

La función principal de los SVD es la distribución de vídeos de entretenimiento. Existen otros dispositivos adicionales que PUEDEN ofrecer comunicaciones de vídeo y que PUEDEN ser conectados en red con otros SVD, tal como los dispositivos de videoconferencia y otros basados en IP. Estos dispositivos serán definidos por el mercado, no incluyéndose información de los mismos en esta Recomendación.

El SVD básico incluye las funcionalidades siguientes:

- Ser íntegramente digital, con decodificación de vídeo digital normalizada (MPEG-2 y códec avanzado).
- Dispositivo autónomo (no funciona como TV).
- Capacidad para servicios unidireccionales y bidireccionales.
- Capacidad para los servicios de la serie J.200 – se pretende que los SVD ejecuten el middleware de las serie J.200, siempre que exista un régimen razonable de licencias de uso de la tecnología de la serie J.200.
- Compatibilidad con el modelo de seguridad, tal como se ha descrito anteriormente, con CSP interno.
- El vídeo PUEDE entregarse en forma de paquetes de transporte MPEG sobre QAM o sobre una red IP. Además, el vídeo PUEDE distribuirse sobre la red del hogar.
- Soporte de MPEG-2 y de los códecs de vídeo avanzado antes descritos.
- Soporte de codificación de audio, BC (ISO/CEI 13818-3) y/o audio AAC (ISO/CEI 13818-7).
- El puerto USB 2.0 y/o Ethernet (100BASE-TX) permite el funcionamiento básico en red en el hogar. A dicho puerto pueden añadirse otros adaptadores de red para permitir la funcionalidad de capa PHY/MAC para distintas arquitecturas de red del hogar (por ejemplo, WiFi, CAT5).
- El SVD básico es un dispositivo del dominio de servicio autorizado y garantizado, tal como se ha definido anteriormente.

- {Texto informativo: El dispositivo funcionará como un cliente en de la red del hogar, con funciones de punto frontera IPCable2Home, con señalización UPnP y QoS UPnP.}
- Disponibilidad de un puerto de expansión (tipo a determinar) que soporte la actualización del hardware del mecanismo de seguridad interno.
- Salida de vídeo proporcionada por un puerto de vídeo compuesto en RF, una salida de vídeo de alta definición o una interfaz de vídeo digital aprobada.

Los SVD básicos PUEDEN ser de ayuda en la transición a una situación de servicios completamente digitales. Utilizados para este fin, los SVD básicos permitirán que los abonados que tengan TV analógicas y otros dispositivos analógicos (por ejemplo, VCR) continúen recibiendo los servicios actuales de forma tan transparente como sea posible, aunque los antiguos canales analógicos hayan sido reasignados para transportar señales comprimidas digitalmente.

La figura 10 ilustra las funciones de los SVD básicos.

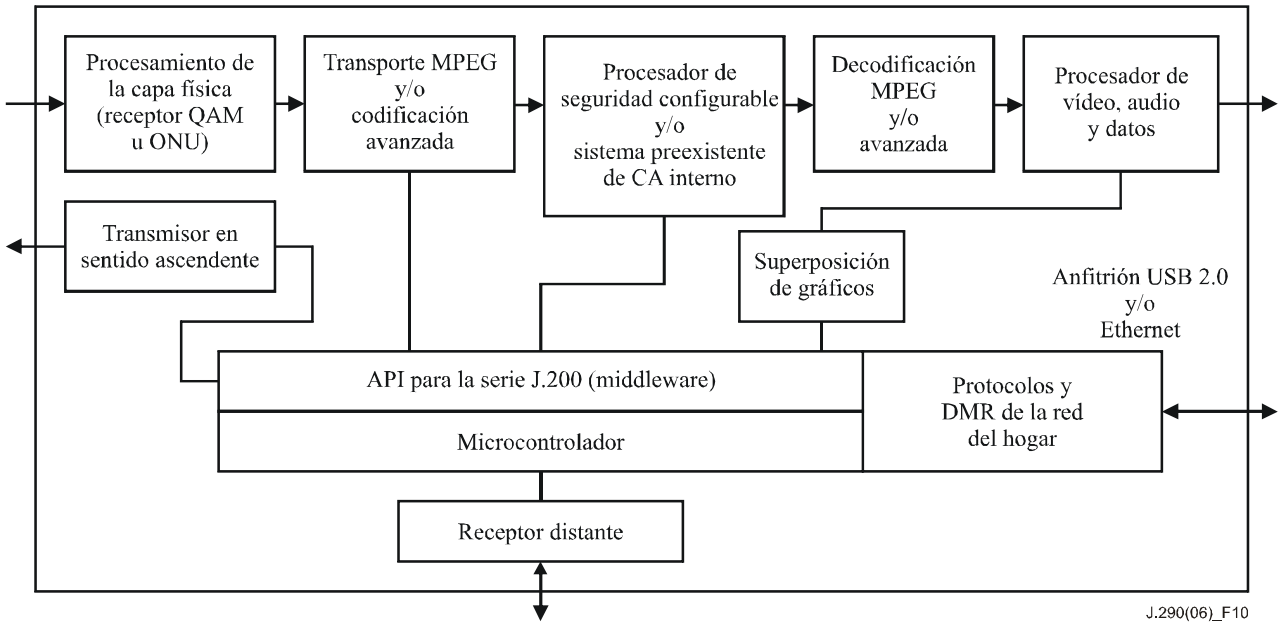


Figura 10 – Funciones del SVD básico

Los suministradores de SVD PUEDEN proporcionar funciones adicionales en dispositivos de gama alta. Por ejemplo, se PUEDEN ofrecer las funcionalidades siguientes:

- Señales de vídeo de alta definición, incluyendo las salidas digitales autorizadas siguientes: DVI (o HDMI) con HDCP y 1394 con DTCP.
- Recepción y procesamiento de múltiples programas de vídeo.
- Funcionalidad de DVR, incluyendo al almacenamiento interno y externo.
- {Texto informativo: Funcionalidad de pasarela, que requiere que el dispositivo soporte los servicios de portal y que funcione como un punto de control UPnP.} Además, los dispositivos con funcionalidad de pasarela podrán habilitar e inhabilitar esta característica para evitar conflictos cuando se instalen varias pasarelas en la misma red.
- Tarjetas de seguridad.
- Equipamiento para la conectividad en red (por ejemplo, WiFi, CAT5). Esta prestación es adicional a la básica del puerto USB-2 y el soporte de la red asociada.
- Pantalla asociada para que el SVD pueda funcionar como una TV digital (TVD) bidireccional.

Aunque según esta Recomendación no es necesario que disponga de un sintonizador analógico, un SVD que incluya dicha característica debe cumplir los requisitos aplicables a los dispositivos de televisión digital que incluyan TV analógica.

La figura 11 muestra las funciones de un SVD con características adicionales que pueden encontrarse en SVD de gama alta.

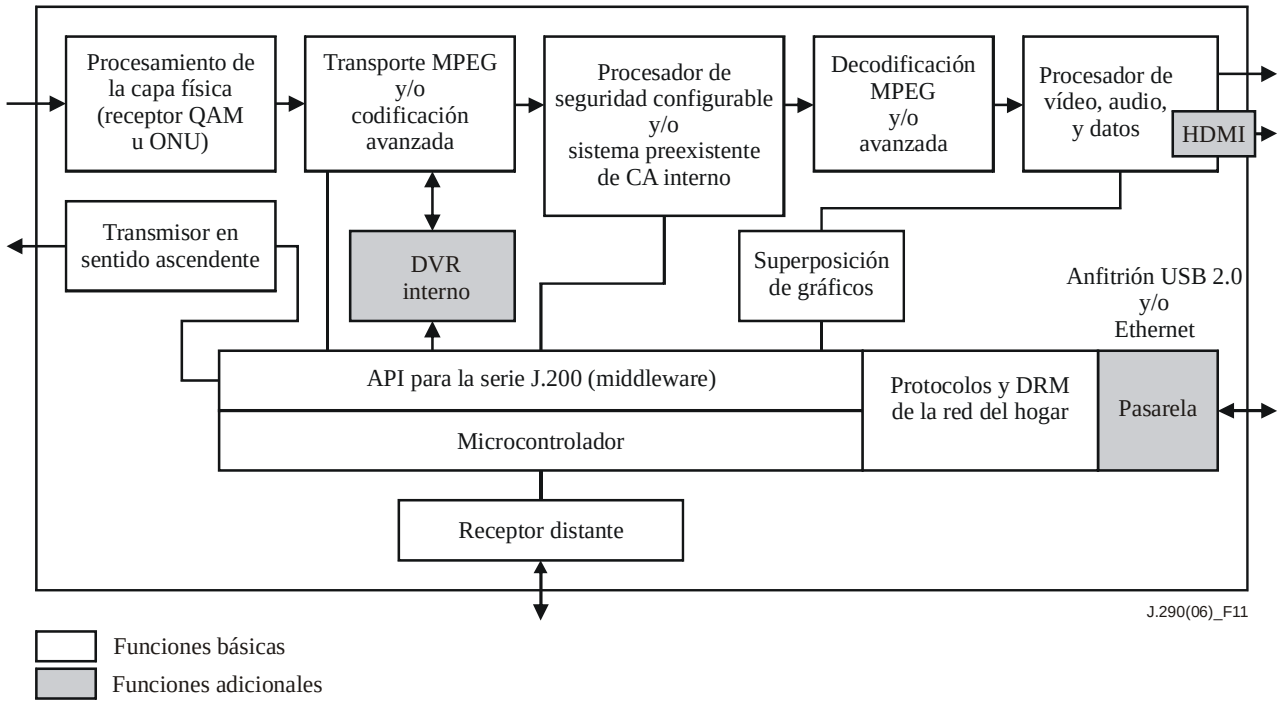


Figura 11 – Funciones de SVD con posibles ampliaciones

Todos los SVD deberán satisfacer la protección de contenidos y otras reglas pertinentes que garanticen que los servicios distribuidos en los dominios garantizado y autorizado se distribuyan tal como desea el operador de cable.

7.3 Otros dispositivos de equipos en las instalaciones del cliente (CPE)

El plan de la NG-STB-A describe ejemplos de CPE de red de la próxima generación adicionales a las opciones de los SVD.

7.3.1 Cliente de medios de vídeo

El cliente de medios de vídeo es un dispositivo "sin sintonizador" diseñado específicamente para conectarse a otros SVD de la red del hogar al objeto de recibir contenidos de vídeo. PUEDE proporcionar un entorno rico en aplicaciones gracias al middleware y a diversas aplicaciones incorporadas en el equipo, o PUEDE presentar, en lugar de ello, una "interfaz de usuario distante" controlada por el SVD que le ofrece los contenidos.

Algunas de las características básicas del cliente de medios son las siguientes:

- Sólo digital, con definición normal.
- DRM del hogar, tal como proporciona el CSP.
- Soporte del cliente en red del hogar.
- PUEDE funcionar como dispositivo ASD o como dispositivo GSD/ASD.
- Soporte de códec MPEG-2 y avanzado.

- Dispositivo de control a distancia universal o control a distancia con comunicación con el dispositivo fuente.
- USB 2.0 para la conectividad en red.

Las características opcionales del cliente de medios incluye:

- Vídeo de alta definición con salidas digitales aprobadas asociadas.

7.3.2 CPE sin vídeo

Dada la proliferación de nuevos servicios de vídeo, datos y multimedia, y la creciente convergencia entre dichos servicios, es previsible que se desarrollen nuevos CPE de la próxima generación que no incluyan vídeo y que se conecten directa e indirectamente a la red de cable.

Los fabricantes de dispositivos ya están incorporando múltiples funciones a los módem de cable, tales como combinaciones de barreras cortafuegos para encaminadores de capa 3, concentradores de datos, adaptadores de terminal multimedia (MTA) para telefonía, y facilidades de transporte en la red del hogar (por ejemplo, WiFi, HPNA, HomePlug, etc.), siendo previsible que los futuros módems de cable y otros dispositivos de abonado integren algunas funciones de la próxima generación. Las funciones de la red de la próxima generación candidatas para una integración creativa en los CPE incluyen redes del hogar dentro de y entre los dominios de servicios autorizados y garantizados, y funciones IPCable2Home que permitan la gestión y visibilidad de los dispositivos de abonado desde la cabecera de la red.

Ejemplo de CPE sin vídeo: pasarela multifunción

Los elementos esenciales de este dispositivo están actualmente disponibles, e incluye un módem de cable, una barrera cortafuego del encaminador de capa 3 y un MTA para telefonía. Una versión de la próxima generación de este dispositivo añadiría capacidades IPCable2Home para permitir la visibilidad y gestión a distancia desde la cabecera de la red. También se incluirían protocolos de la red del hogar y el CPE de la red de datos del hogar. Dicho dispositivo también incluiría la posibilidad de actuar en modo puente para permitir la interacción entre los SVD que sean compatibles con los protocolos de la red del hogar y los CPE en la red de datos del hogar. Dicho dispositivo soportaría aplicaciones tales como:

- Permitir que los PC con un puente adecuado utilicen la red coaxial para acceder a servicios de datos de alta velocidad.
- Permitir que los PC o servidores que sean propiedad de los consumidores y están ubicados en la red coaxial o de datos del hogar, se comuniquen mediante mensajes visualizables o mensajes de control con los SVD.
- Habilitar que el MTA para telefonía envíe mensajes sobre la ID del llamante (u otros mensajes) a los SVD.
- Permitir que los SVD accedan a información de facturación o de servicio relativa a los servicios de datos/multimedia interactivos de los abonados.

8 Seguridad

8.1 Elemento hardware de seguridad

El elemento hardware procesador de seguridad configurable (CSP) de la próxima generación podrá utilizar diversos algoritmos normalizados para la criptación del flujo de transporte en la cabecera y su descriptación en el CPE. A continuación se enumeran ejemplos de algoritmos normalizados que eventualmente PUEDEN ser soportados por el CSP.

- Norma de criptación de datos DES (*data encryption standard*) – ECB (*electronic code book*), CBC (*cipher block chaining*) y otros modos basados en bloques de datos residuales (Federal Information Processing standard, FIPS 46-2).

- Triple DES – ECB, CBC, y otros modos basados en bloques de datos residuales (FIPS 46-2). Ello incluye la criptación con clave doble y clave triple.
- Norma de criptación avanzada (AES, *advanced encryption standard*) (Rijndael).
- DVB – Algoritmo común de aleatorización (CSA, *common scrambling algorithm*).
- Multi2 (ISO/CEI 9979).

El elemento hardware CSP será configurable ("actualizable") y utilizará tecnologías para poder descriptar al menos los cinco tipos siguientes de flujos de transporte seguros:

1) Triple DES – permitiendo como mínimo ECB y CBC, así como los modos con dos y con tres claves.
2) DVB-CSA – tal como se define para DVB.
3) AES – utilizando una nueva arquitectura de clave normalizada con ECM, EMM, unidad semilla y la metodología de ID de unidad normalizadas.
4) B-CAS – tal como se define en ARIB, que será soportada por las tarjetas de seguridad.

Obsérvese que el CSP se definirá de forma que los proveedores de semiconductores no tengan que disponer de licencias para algunos de los sistemas de seguridad a fin de incluir la funcionalidad CSP en sus productos. El CSP se definirá de modo que los dispositivos semiconductores que sean conformes puedan ejecutar los algoritmos adecuados que sean descargables sobre el CSP cuando se conecten a la red de cable o que sean suministrados mediante la propia tarjeta de seguridad.

8.2 Autenticación

Los componentes hardware del CSP podrán almacenar de forma segura y ejecutar firmas digitales utilizando varios tamaños de claves RSA (por ejemplo, 1024, 2048 y 4096 bits) en registros hardware. Los componentes de la próxima generación podrán generar de forma segura firmas digitales en hardware resistente a la manipulación sin poner por ello en riesgo las claves privadas o los procesos necesarios para generar las funciones de troceo y la criptación. La red de la próxima generación podrá firmar digitalmente mensajes utilizados para la autenticación y garantizar la integridad utilizando una función de troceo segura de tipo SHA-1.

8.3 Claves de criptación de clave

El hardware CSP podrá almacenar de forma segura claves de criptación de clave para sistemas criptográficos simétricos o preferentemente asimétricos. La capacidad de utilizar parejas de claves para transportar claves criptadas entre dispositivos CPE y a los dispositivos de la cabecera de cable es muy deseable.

8.4 Dirección de la unidad

Cada CSP que utilice un dispositivo CPE será identificado unívocamente mediante un ID único. Este ID se utiliza para direccionar cada dispositivo CPE de forma que dicho dispositivo CPE pueda recibir los correspondientes derechos a prestaciones. En algunas implementaciones, PUEDE utilizarse como ID una dirección MAC. El ID de unidad también podrá proporcionarse mediante una tarjeta de seguridad.

8.5 Resistencia a la manipulación

El CSP se diseñará para satisfacer la seguridad FIPS-140 de nivel 2 en la mayoría de las áreas, existiendo algunas áreas (tales como reconfiguración hardware y actualizaciones software) que requieran seguridad FIPS 140-2 de nivel 3, resistente a la manipulación de conformidad con ciertos criterios, tales como FIPS-140 de nivel 2 o nivel 3. También utilizará las últimas tecnologías disponibles en materia de resistencia a la manipulación (por ejemplo, distribución del plano de

energía y fragmentación de células) a fin de evitar el análisis microscópico y los ataques de supresión.

8.6 Gestión de claves

La jerarquía de claves incluye múltiples claves tal como se ilustra en la figura 12. Además, en la figura 13 se muestra un esquema de descriptación en el que se utiliza la tarjeta de seguridad.

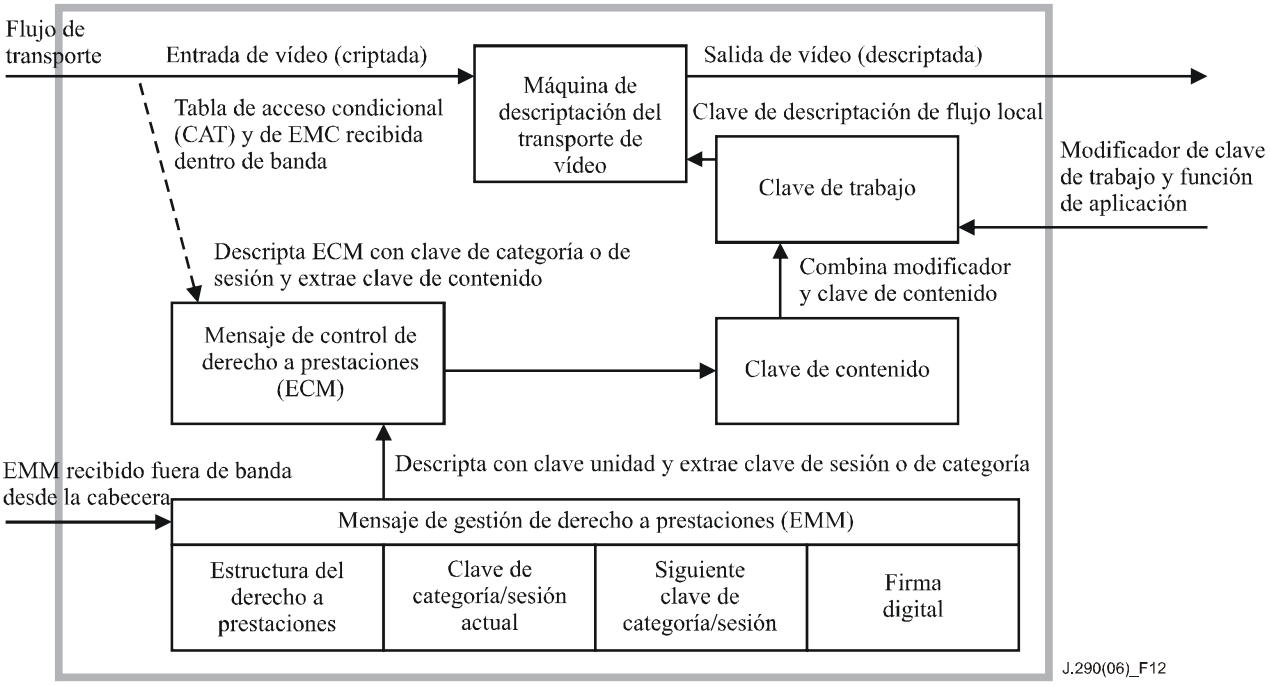


Figura 12 – Jerarquía de claves

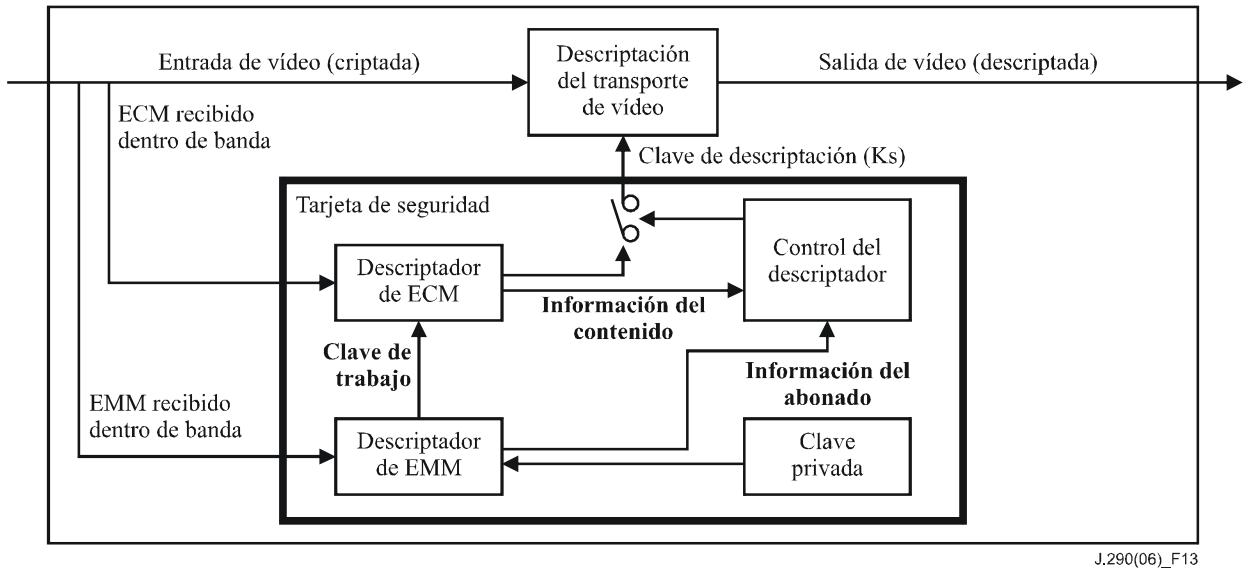


Figura 13 – Flujo de señales utilizado por la tarjeta de seguridad

El software y hardware del CSP DEBERÍA ser diseñado para poder utilizar nuevos conceptos y tecnologías en el área de gestión de claves, al tiempo que pueda funcionar con sistemas preexistentes empleando claves compartidas o criterios de reconfiguración. El módulo CSP soportará los esquemas siguientes:

1) las claves descriptadas extraídas en el CPE del flujo de vídeo y de los ECM y EMM se cargarán directamente en las máquinas de descriptación sin pasar por interfaces externas, incluidos los descriptadores de transporte;

2) los ECM y EMM se extraen del flujo de transporte (dentro de banda) y se transfieren directamente al dispositivo tarjeta de seguridad, donde se decodifica la clave de trabajo y se calcula la clave de descriptación de flujo.

8.6.1 Mensajes de control del derecho a prestaciones (ECM, *entitlement control messages*)

Un ECM es un mensaje criptado que contiene criterios de acceso a varios niveles de servicio y una palabra de control (CW, *control word*). La palabra de control es la clave semilla que se utiliza y se modifica para descriptar los flujos de vídeo y que puede ser modificada con una periodicidad variables o convertida en una "clave de trabajo". El ECM se descripta y verifica en el CPE confrontándolo con el criterio de acceso a fin de conceder la autorización. Si se concede, la CW se libera, se convierte en una clave de trabajo y se utiliza para descriptar el contenido en el dispositivo CPE.

8.6.2 Mensajes de gestión del derecho a prestaciones (EMM, *entitlement management messages*)

Los mensajes criptados se crean en la cabecera y se envían al CPE de la próxima generación de conformidad con determinados criterios de acceso a los contenidos por parte de dicho dispositivo. El EMM contiene los datos para la autorización, que se envían con un método seguro a cada dispositivo CPE. El EMM está dirigido a un único dispositivo CPE y está criptado también de forma unívoca de forma que el dispositivo pueda descriptar y validar los derechos a prestaciones. El CSP soportará los mecanismos y formatos del derecho a prestaciones DigiCipher II, PowerKey, NDS, Nagravision, NCAS y B-CAS.

8.7 Protección contra copia

Si un dispositivo de la arquitectura de red de la próxima generación utiliza una tarjeta de seguridad, la interfaz implementará la actualización y configuración de conformidad con SCTE-41. Además de soportar los requisitos actuales de los flujos de transporte SCTE-41, el CSP podrá descriptar los tres tipos siguientes de árboles de flujos de transporte seguros normalizados. A continuación se enumeran algunos ejemplos:

1) Protección contra copia – DES (tal como se define en SCTE-41, con la opción adicional de utilizar el modo CBC DES además del modo EBC).

2) Triple DES – soportando, como mínimo, ECB y CBC.

3) AES – utilizando una nueva arquitectura de clave normalizada con ECM, EMM, claves de criptación de claves y la metodología de ID de unidad normalizadas.

4) Multi2 – incluyendo ECB y OFB.

9 Arquitectura de red de la cabecera

Los beneficios derivados de la integración de la cabecera, lo cual resulta consistente con la versión de la NG-STB como elemento multimedia integrado, son entre otros los siguientes:

- Utilizar de forma más eficiente los recursos del sistema.

- Facilitar el interfuncionamiento de elementos de red suministrados por diversos fabricantes a fin de permitir un entorno de competencia más abierto y ampliar la vida útil de servicio de la base instalada, proporcionando flexibilidad para la introducción de nuevos servicios y escalabilidad para acomodar una gama de tamaños del sistema.
- Proporcionar una plataforma para la innovación y la creación rápida de servicios.

9.1 Arquitectura de distribución de la red de la cabecera

En la figura 14 se describe la arquitectura global de distribución de la red de la cabecera.

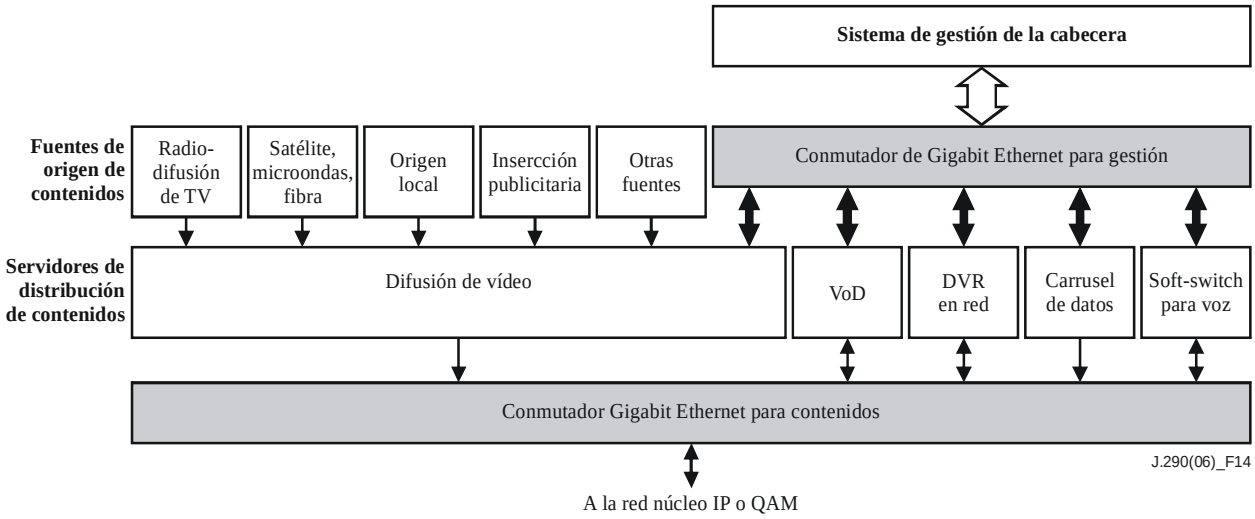


Figura 14 – Arquitectura de distribución de la cabecera de la red

Las características fundamentales de la arquitectura de la red de la cabecera de la próxima generación incluyen:

- Permitir la distribución de tráfico de vídeo y tráfico genérico de datagramas IP sobre una misma infraestructura de red de la cabecera.
- Gestionar las aplicaciones para todos los servicios mediante sistemas de gestión de sesión y de recursos, con capacidad para funcionar de forma autónoma en el caso de fallo de las comunicaciones con los sistemas de la oficina de apoyo.
- Controlar de manera diferenciada los servidores de la cabecera de forma que las aplicaciones de operación de red y de gestión de recursos de terceros puedan gestionar la cabecera como un sistema integrado, en lugar de hacerlo como subsistemas autónomos específicos por servicio.
  - *Conmutador Gigabit Ethernet para contenidos*: El conmutador Gigabit Ethernet estará bajo el control de un gestor de recursos de red para la distribución de contenidos y garantizará que cualquier servidor pueda conmutar datos de cualquier fuente de contenidos y que se pueda conmutar fácilmente entre servidores de contenidos.
  - *Sistema de gestión de sesión y de recursos*: Los gestores de aplicaciones, gestores de sesión y gestores de recursos tendrán funcionalidades que permitan al operador controlar y supervisar la carga de tráfico, las necesidades de QoS y los derechos a prestaciones de los abonados.
  - *Conmutador Ethernet o Gigabit Ethernet para la gestión*: El conmutador dispondrá de una interfaz normalizada en el plano de gestión mediante un conmutador Ethernet o Gigabit Ethernet de forma que cada servicio pueda ser controlado y gestionado por sistemas de gestión de IT externos mediante APIs abiertas.

- El protocolo Internet (IP) se utiliza para transportar los mensajes de control y gestión por la red hasta el CPE. Es previsible que el conjunto de protocolos de señalización para servicios de vídeo incluya DSM-CC (*digital storage media – command and control*), RTSP, SIP, NCS/MGCP y, potencialmente, protocolos de "servicios web" basados en XML, tales como SOAP.

9.2 Arquitectura de gestión de sesión y recursos

Para conseguir una gestión común de los recursos para todos los servicios y aplicaciones, es necesario disponer de un marco para la gestión de la sesión y los recursos, tal como se muestra en la figura 15.

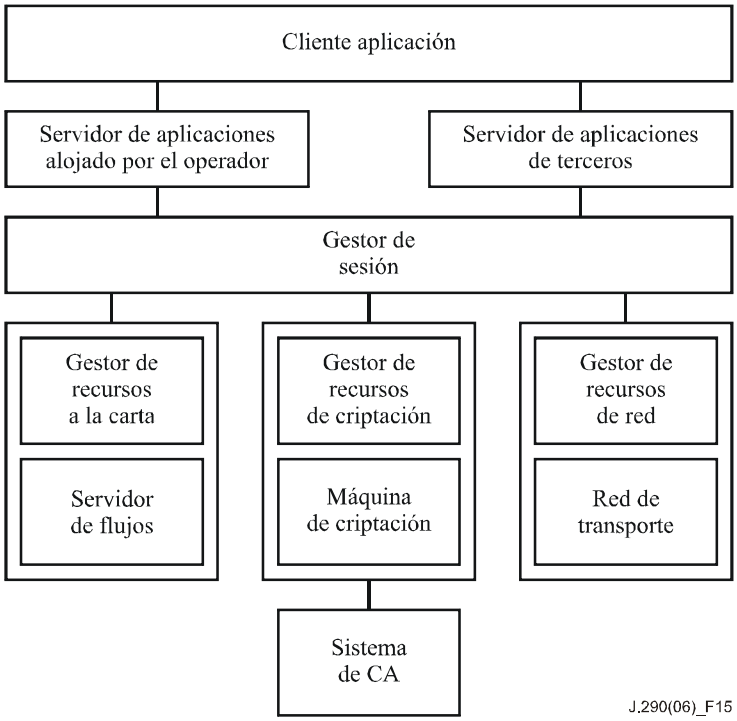


Figura 15 – Marco de gestión de sesión y recursos

Para aumentar la eficiencia de la utilización de los recursos, una cabecera de la próxima generación utiliza una arquitectura de gestión de recursos basada en la sesión. La creación de dicha arquitectura debe mantener un estricto control de los recursos a fin de asegurar su uso eficiente. En un intento de proporcionar un marco genérico, la función de gestión de sesiones y recursos se divide en tres dominios: gestión de aplicación, gestión de sesión y gestión de recursos. Cada uno de dichos dominios se analiza en detalle en las cláusulas siguientes.

9.2.1 Gestor de aplicación

El gestor de aplicación juega un papel de coordinación que implica la señalización de la aplicación así como la interacción con el marco de gestión de recursos de la cabecera por medio del gestor de sesión. En la mayoría de los casos, es previsible que el gestor de aplicación sea propiedad del operador de servicios y esté operado por él. No obstante, PUEDE haber casos en los que el gestor de aplicación quede de hecho fuera del control del operador de servicios. Son ejemplos de gestores de aplicación del operador, los servicios de VoD (vídeo a la carta) y de telefonía. Son ejemplos de gestores de aplicación de terceros, los servicios de flujos de audio o de vídeo y los juegos.

En un sistema de VoD es responsabilidad del gestor de sesión, más que del gestor de aplicación, mantener y gestionar el ciclo de vida. En tales casos, el cliente puede establecer una sesión con un gestor de sesión directamente o utilizando un representante (*proxy*) del mismo a través del gestor de aplicación. Puesto que el gestor de aplicación no necesita gestionar la sesión, esta arquitectura permite que diferentes aplicaciones utilicen el mismo gestor de sesión para una variedad de servicios por demanda.

En el caso de servicios y aplicaciones basados en IP, una implementación típica integra el gestor de sesión en el servidor de aplicaciones, aunque ambos PUEDEN residir en la misma caja física, se considera que están separados lógicamente.

9.2.2 Gestor de sesión

El papel del gestor de sesión es actuar como intermediario en nombre del gestor de aplicación ante las peticiones de recursos de la cabecera. Aunque un gestor de aplicación sólo conoce las necesidades de QoS de la sesión, el gestor de sesión ha de saber cómo traducir dichas necesidades de QoS en recursos del sistema, así como identificar recursos no asociados a QoS que PUEDEN ser necesarios para la sesión (por ejemplo, recursos para la criptación o recursos del servidor).

Es importante señalar que PUEDEN existir varios ejemplares de un gestor de sesión en una cabecera dada y que cada gestor de sesión puede comunicarse con un conjunto de gestores de recursos. El conjunto de gestores de recursos con los que se comunica un gestor de sesión viene determinado por las aplicaciones para las que el gestor de sesión debe manejar las peticiones de recursos. Dicha arquitectura permite una introducción más rápida de nuevos servicios al no requerir un 'super' gestor de sesión que deba ser actualizado cada vez que se prueba un nuevo servicio. Se prevé que un gestor de aplicación dado se comunique con un único gestor de sesión salvo cuando se implementen gestores de sesión redundantes. Los gestores de sesión no necesitan soportar todos los tipos de sesiones; de hecho, es previsible que se desplieguen gestores de sesión diferenciados para diferentes tipos de sesiones; por ejemplo, para VoD y para difusión conmutada.

El gestor de sesión no tomará decisiones de la política basadas en el negocio. En lugar de ello, coordinará las necesidades de recursos para la aplicación, en el supuesto de que las peticiones provengan de un dispositivo válido y de un abonado con autorización para solicitar dichos servicios. PUEDE tomar decisiones de política basadas en los recursos en función del estado actual de los recursos del sistema.

9.2.3 Gestor de recursos

El gestor de recursos se ocupa esencialmente de la asignación de los recursos necesarios para satisfacer una petición de sesión. Cada recurso de la cabecera tendrá asociado (de forma lógica) un gestor de recursos, cuya misión es hacer un seguimiento del consumo de recursos y asignar nuevos recursos conforme sean necesarios. Los siguientes son ejemplos de gestores de recursos:

- Gestor de recursos por demanda – Recursos del servidor de flujos.
- Gestor de recursos de criptación – Recursos de la criptación de flujos.
- Gestor de recursos de red – Recursos de la red IP conmutada.

Para una mejor comprensión del marco de la gestión de sesión y gestión de recursos, se presenta la siguiente descripción:

- Un servicio VoD se desarrolla de acuerdo con el flujo siguiente: el cliente inicia la sesión haciendo una petición de VoD al gestor de aplicaciones. Cuando éste recibe la petición, la reenvía al gestor de sesión apropiado, que negocia con varios gestores de recursos a fin de obtener los recursos correspondientes. Éstos PUEDEN incluir (no necesariamente en cualquier orden) recursos del servidor, recursos de red, recursos de encriptación y recursos de borde de red.

10 Calidad de servicio

La calidad de servicio puede conseguirse dimensionando ampliamente la red para que todos los paquetes consigan una calidad de servicio suficiente a fin de conseguir una adecuada prestación del servicio para aplicaciones sensibles a la QoS. Este enfoque es relativamente sencillo y es económicamente viable en muchas redes de banda ancha. Las prestaciones de este sistema son razonables, particularmente si el usuario está dispuesto a que en ocasiones exista una cierta degradación. Sin embargo, en el caso de redes de banda estrecha, más típicas de empresas y oficinas locales, los costes de la anchura de banda pueden ser sustanciales y el sobredimensionado difícil de justificar. En general, las redes requieren los factores siguientes para establecer una QoS extremo a extremo a fin de soportar tanto servicios para los que el tiempo es un factor crítico como servicios de vídeo de alta calidad.

- Retardo.
- Variación de fase.
- Pérdida de paquetes.
- Anchura de banda.

Las funciones de QoS incluidas en encaminadores o conmutadores DEBEN controlar dichos factores clave y transmitir los paquetes al tramo de red siguiente. En esta situación, se han desarrollado dos filosofías distintas para satisfacer los requisitos.

10.1 IntServ y DiffServ

Los primeros desarrollos utilizaban la filosofía denominada "IntServ" (integración de servicios) para la reserva de recursos de red. En este modelo, las aplicaciones utilizaban el protocolo de reserva de recursos (RSVP, *resource reservation protocol*) para solicitar y reservar recursos a través de la red. Aunque los mecanismos IntServ funcionan correctamente, pronto fue evidente que en una red de banda ancha típica de un proveedor de servicio de gran tamaño, los encaminadores del núcleo de red deberían aceptar, mantener y deshacer miles o posiblemente decenas de miles de reservas.

El segundo, y actualmente aceptado, enfoque es el denominado "DiffServ" o de servicios diferenciados. En el modelo DiffServ, los paquetes se marcan de acuerdo con el tipo de servicio que precisan. Como consecuencia de dichas marcas, los encaminadores y conmutadores utilizan varias estrategias de disposición en cola para conseguir adaptar las prestaciones a los requisitos. En la capa IP, las marcas de puntos de código de servicios diferenciados (DSCP) utilizan 6 bits de la cabecera de cada paquete IP. En la capa MAC, pueden utilizarse VLAN IEEE 802.1Q e IEEE 802.1D para transportar esencialmente la misma información.

10.2 Calidad de servicio extremo a extremo y servicios

Teniendo en cuenta los servicios que DEBERÍA ofrecer una STB de la próxima generación, el mecanismo de QoS DEBE satisfacer los requisitos tanto de servicios de vídeo de alta calidad como de servicios para los que la temporización resulta crítica, como es el caso de la VoIP. Para ello, el mecanismo de QoS garantizada definido en la cláusula 6.5.1 DEBE implementarse de forma que lo lleve a cabo.

La prestación de un mecanismo de QoS garantizada difiere de una red a otra en las áreas de aplicación del servicio y en las estructuras de las sesiones. En esta Recomendación se diferencian tres tipos de QoS: QoS por sesión, QoS basada en anchura de banda previamente aprovisionada y QoS basada en la prioridad. La definición de cada tipo de QoS es la siguiente:

- QoS por sesión: es necesario que la señalización establezca las rutas con QoS. Se asegura cada vez que se activa el servicio y la anchura de banda se libera cuando se desactiva el servicio.

- QoS basada en anchura de banda previamente aprovisionada: la señalización no es siempre necesaria para el establecimiento de rutas con QoS. El tipo de QoS es lo que determina la reserva la anchura de banda requerida, con independencia del tipo de tráfico o su presencia.
- QoS basada en la prioridad: en ciertos casos, la QoS basada en prioridad puede satisfacer los requisitos de QoS garantizada mediante el sobredimensionado de la anchura de banda, tal como se define en la cláusula 6.5.1. Dicho sobredimensionado es suficiente para satisfacer las limitaciones de anchura de banda y en la mayoría de los casos también las relativas a variación de fase y retardo, siempre que se mantenga estrictamente la prioridad de los paquetes sin interrupciones debido a limitaciones de anchura de banda o del procesador.

Obsérvese que en esta Recomendación, la palabra servicio hace referencia al servicio desde la perspectiva del usuario, y no significa que se haga referencia a un ISP o a un operador de telecomunicaciones.

El cuadro 4 muestra servicios típicos y la QoS requerida para la arquitectura independiente del medio (MI, *media independent*) (Rec. UIT-T J.292) y para la arquitectura de cable (Rec. UIT-T J.291).

Los requisitos para cada servicio DEBERÍAN hacer referencia a la Rec. UIT-T J.193 (2004). En cuanto a la relación entre servicio y QoS, véase el apéndice I.

Cuadro 4 – Servicios típicos y QoS requerida

Servicio	Arquitectura MI	Arquitectura de cable
Difusión de TV	Anchura de banda previamente aprovisionada	Anchura de banda previamente aprovisionada
VoD	Por sesión	Por sesión
VoIP	Por sesión	Por sesión
Video telefonía	Por sesión	Por sesión
Internet	Mejor esfuerzo	Mejor esfuerzo

En el cuadro 5 se muestra una relación entre el tipo de QoS, la señalización y la asignación de anchura de banda. En este caso, señalización significa todas las transacciones de señales para el establecimiento de una sesión entre los dispositivos concernidos.

Cuadro 5 – Relaciones entre tipo de QoS, señalización y asignación de anchura de banda

Tipo de QoS	Señalización	Asignación de anchura de banda
QoS basada en sesión	Aplicable	La genera la sesión, reserva anchura de banda.
QoS basada en anchura de banda previamente aprovisionada	No Aplicable	Anchura de banda fija.
QoS con prioridad	No Aplicable	Disposición de cola con prioridad, independientemente de la anchura de banda. Opcional para la QoS de tipo DiffServ, tiene aspecto de anchura de banda.

10.3 Requisitos del puente de QoS

Tal como se muestra en la figura 16, es necesario que exista una correspondencia lógica entre los mecanismos de QoS del segmento A (red de acceso) y del segmento B (red del hogar), que normalmente difieren entre sí. El puente de QoS permite la comunicación entre ellos y su entidad lógica DEBERÍA implementarse en un dispositivo de acceso a la red del hogar (HA, *home access*), o pasarela residencial, de conformidad con la Rec. UIT-T J.190.

10.3.1 Objetivo del puente de QoS

El objetivo del puente de QoS es establecer una ruta con QoS extremo a extremo, hacer corresponder lógicamente el mecanismo de QoS entre el segmento A y el segmento B y proporcionar una interfaz de QoS unificada a los dispositivos terminales ocultando los diversos mecanismos de QoS aplicados en el segmento A.

10.3.2 Requisitos funcionales del puente de QoS

- *Dónde se implementa*

  La función puente de QoS DEBERÍA implementarse en un dispositivo HA tal como se especifica en la Rec. UIT-T J.190, o en un punto de interfaz de los distintos mecanismos de QoS definidos en otra arquitectura de QoS.

- *Dirección de la señalización de QoS*

  1) Al menos una función de puente de QoS direccional DEBE intercambiar señalización de QoS desde el segmento A al segmento B. También es necesario un puente de QoS bidireccional cuando se requiere que el control de la QoS se haga desde el dispositivo terminal final al servidor de aplicación. En la figura 16 se muestra un aspecto del puente de QoS.

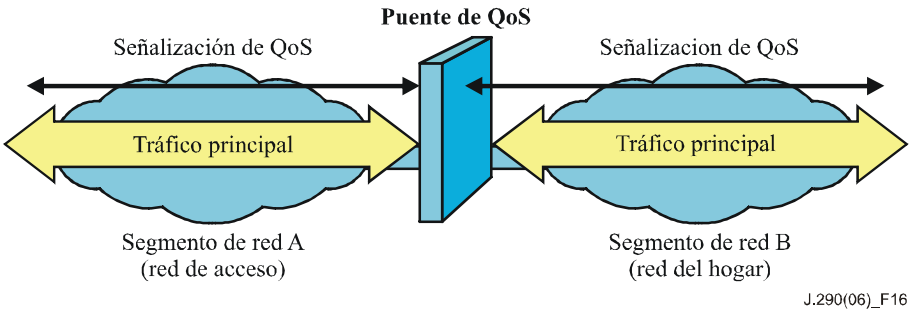


Figura 16 – Aspecto del puente de QoS

Un puente de QoS, a diferencia de un puente de capa 2, DEBERÍA estar situado en la zona (segmento A/B de la figura 16) donde las distintas redes presentan interfaces, y DEBERÍA proporcionar las subfunciones siguientes:

a) Iniciar, retransmitir y terminar la señalización de QoS de cada segmento.

b) Marcar y volver a marcar el tráfico de la señal principal.

c) Conformar el tráfico de la señal principal.

2) El puente de QoS DEBERÍA notificar a los dispositivos terminales su indisponibilidad para realizar las funciones de puente de QoS en caso de que el segmento A (red de acceso) no disponga de funciones de QoS en sentido ascendente.

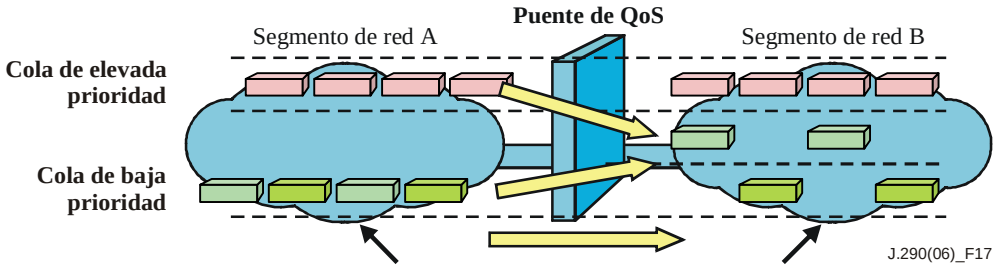
- *Gestión*

  1) El puente de QoS DEBERÍA garantizar que la política de QoS del operador funcione con la política de QoS del segmento B (red del hogar), que posiblemente sea provista por un usuario final. Un usuario final PUEDE proporcionar una función de gestión de política para el segmento B.

  2) El puente de QoS DEBERÍA notificar a ambas partes cualquier desalineación que pueda producirse entre las políticas de QoS de los segmentos A y B.

- *Función de puente*

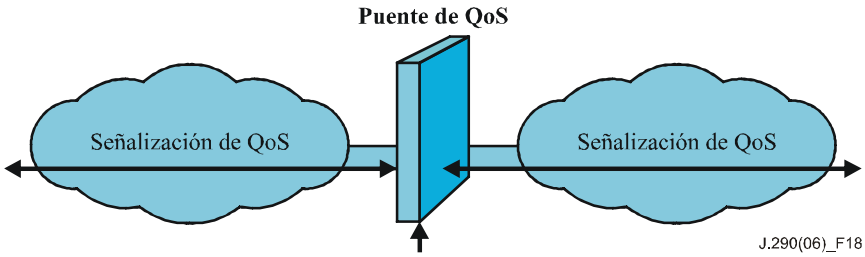
  1) El puente de QoS DEBERÍA mantener la prioridad de la clase de QoS en los segmentos A y B, así como proporcionar las tablas de correspondencia para las clases de QoS de ambos segmentos. En la figura 17 se muestra un aspecto de la correspondencia de clase de QoS.



Correspondencia de clases de QoS a través del puente de QoS, manteniendo la clase de QoS del tráfico principal en cada segmento de red

Figura 17 – Aspecto de la correspondencia entre clases de QoS

  2) El puente de QoS DEBERÍA disponer de funciones para la iniciación, retransmisión y terminación de la señalización de QoS en los segmentos A y B. En la figura 18 se muestra la gestión de la señalización de QoS.



Activación, retransmisión y terminación de señalización QoS en cada segmento (por ejemplo, UPnP y RSVP)

Figure 18 – Gestión de la señalización de QoS

- *Establecimiento de la política*

Aunque la provisión de QoS extremo a extremo y los requisitos del puente de QoS se describen en cláusulas anteriores, es necesario disponer de un mecanismo de prioridad de los paquetes para controlar realmente la QoS. En la figura 19 se muestra un ejemplo de flujo de procesos de QoS.

1) Clasificación:

   Clasifica las etiquetas de QoS en base a la verificación y establecimiento de los paquetes. En este caso, establecimiento significa determinar la etiqueta de tipo de servicio (TOS), el número de puerto UDP, el protocolo y la dirección IP, etc.

2) Función de política:

   Discrimina los paquetes concordantes comparando la velocidad del tráfico recibido y el elemento de política aprovisionado. En este caso, el elemento de política es una entidad que realiza la función de política, más específicamente ello significa aplicar las tablas de función de política proporcionadas por el operador o el cliente.

3) Marcado:

   Juzga si el paquete concuerda, si éste debe ser transmitido en base a los parámetros establecidos, si debe ser marcado con la prioridad siguiente inferior o si debe ser descartado.

4) Disposición en cola y programación:

   Determina la cola de salida donde debe situarse el paquete en función de la etiqueta de QoS. Cada cola se procesa entonces de acuerdo con el peso otorgado a la misma.

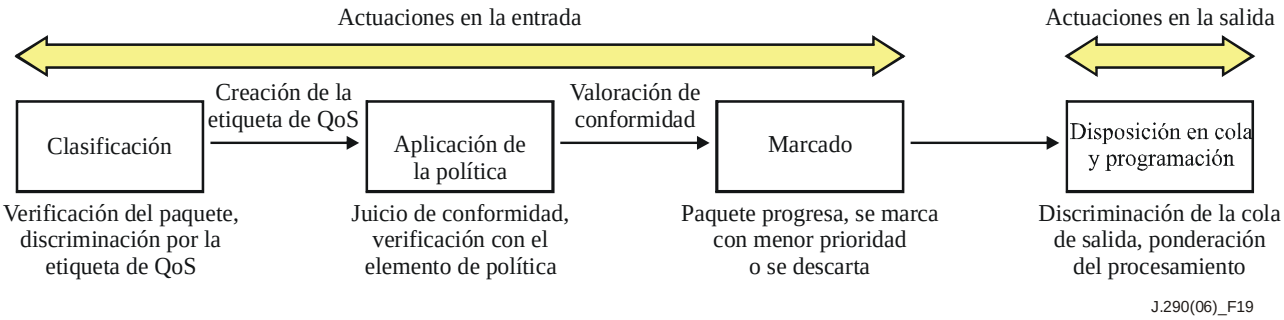


Figura 19 – Ejemplo del flujo del proceso de QoS

La priorización de los paquetes DEBERÍA permitir el establecimiento de una precedencia IP en virtud del mecanismo de QoS DiffServ, que utiliza el punto de código de servicio diferenciado (DSCP) y/o la clase de servicio (CoS, *class of service*) definida en IEEE 802.1Q. En la figura 20 se ilustra la prioridad en disposición en cola entre el núcleo de red y la red de acceso. La política de disposición en cola DEBE proporcionarse con una prioridad basada en el tipo de servicio (ToS, *type of service*), que constituye un procesamiento previo a la asignación de anchura de banda. Para una información más detallada sobre las prioridades de la QoS, DEBERÍA hacerse referencia a la cláusula 9/J.292.

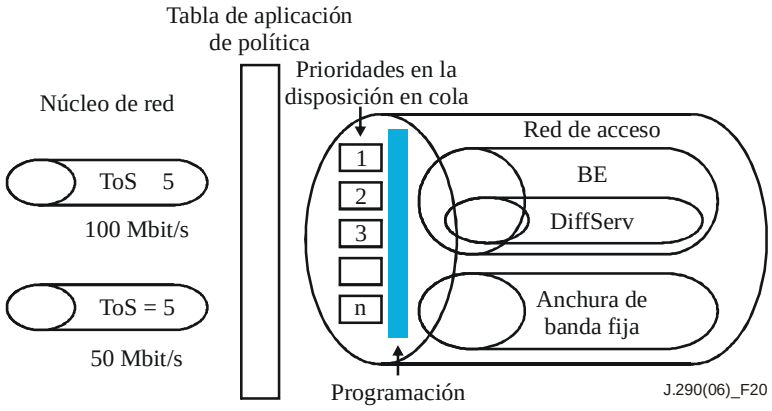


Figura 20 – Aspecto de la prioridad en la disposición en cola entre el núcleo de red y la red de acceso

Apéndice I

Relación entre el tipo de servicio independiente del medio (MI) y el tipo de QoS

(Este apéndice no es parte integrante de esta Recomendación)

Este apéndice es un suplemento al cuadro 4 de la cláusula 10. El cuadro I.1 ilustra la relación entre el servicio de tipo de servicio independiente del medio (MI) y el tipo de QoS para servicios de calidad garantizada. Este cuadro muestra una combinación deseable entre servicio y tipo de QoS y no excluye otras posibles combinaciones.

Cuadro I.1 – Relación entre el tipo de servicio independiente del medio (MI) y el tipo de QoS

	Anchura de banda previamente aprovisionada	**Basada en sesión**	**DiffServ**	**Mejor esfuerzo**
Difusión de TV	✓			
VoD	✓	✓		
VoIP	✓	✓		
Vídeo telefonía	✓	✓	✓	✓
Teléfono sobre PC				✓

El cuadro I.2 ilustra la relación entre el servicio de tipo cable y el tipo de QoS para servicios de calidad garantizada. Este cuadro representa una combinación deseable entre servicio y tipo de QoS y no excluye otras posibles combinaciones.

Cuadro I.2 – Relación entre el tipo de servicio de cable y el tipo de QoS

	Anchura de banda previamente aprovisionada	**Basada en sesión**	**DiffServ**	**Mejor esfuerzo**
Difusión de TV	✓			
VoD		✓		
VoIP		✓		
Vídeo telefonía		✓	✓	✓
Teléfono sobre PC				✓

Bibliografía

[b-UIT-T J.112] Recomendación UIT-T J.112 (1998), *Sistemas de transmisión para servicios interactivos de televisión por cable*.

[b-UIT-T J.122] Recomendación UIT-T J.122 (2002), *Sistemas de transmisión de segunda generación para los servicios interactivos de televisión por cable - Módems de cable para protocolo IP*.

[b-UIT-T J.125] Recomendación UIT-T J.125 (2004), *Privacidad de enlace para la implementación de módems de cable*.

[b-UIT-T J.126] Recomendación UIT-T J.126 (2004), *Especificación de dispositivos módem de cable incorporados*.

[b-UIT-T J.192] Recomendación UIT-T J.192 (2005), *Pasarela residencial para soportar la entrega de servicios de datos por cable*.

[b-UIT-T J.200] Recomendación UIT-T J.200 (2001), *Núcleo común a escala mundial – Entorno de aplicación de los servicios de televisión interactiva digital*.

[b-UIT-T J.201] Recomendación UIT-T J.201 (2004), *Armonización del formato de contenido declarativo para aplicaciones de televisión interactiva*.

[b-UIT-T J.202] Recomendación UIT-T J.202 (2005), *Armonización de los formatos de contenidos de procedimiento para las aplicaciones de televisión interactiva*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007