



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**H.610**

(07/2003)

SERIE H: SISTEMAS AUDIOVISUALES Y  
MULTIMEDIOS

Servicios de banda ancha y de tríada multimedios –  
Servicios multimedios de banda ancha sobre VDSL

---

**VSDL de servicio completo – Arquitectura de  
sistema y del equipo en las instalaciones del  
cliente**

Recomendación UIT-T H.610

---

RECOMENDACIONES UIT-T DE LA SERIE H  
SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
SISTEMAS Y EQUIPOS TERMINALES PARA LOS SERVICIOS AUDIOVISUALES	H.300–H.399
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedia de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedia	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedia	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedia	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedia	H.560–H.569
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIOS	
<b>Servicios multimedia de banda ancha sobre VDSL</b>	<b>H.610–H.619</b>

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

## **Recomendación UIT-T H.610**

### **VDSL de servicio completo – Arquitectura de sistema y del equipo en las instalaciones del cliente**

#### **Resumen**

En esta Recomendación se especifica la arquitectura de sistema (SA) y la arquitectura del equipo en las instalaciones del cliente (CPE) para la entrega a un entorno doméstico de servicios de vídeo, datos y voz por una red de acceso VDSL, denominada red VDSL de servicio completo. La Recomendación especifica la arquitectura SA y CPE a alto nivel, independientemente del mecanismo de transporte de la capa física subyacente de banda ancha. En esta Recomendación VDSL aparece denominada tecnología de capa física; sin embargo, las especificaciones de arquitectura que se describen también podrían aplicarse a los CPE y las redes de acceso que emplean otras tecnologías de capa física de banda ancha.

En esta Recomendación se define una arquitectura que permite el suministro fiable de un paquete de servicios triple, con mínima intervención del usuario, que cumple los requisitos fundamentales de seguridad y acceso condicional al contenido y con un costo que permita la instalación en masa en el mercado.

#### **Orígenes**

La Recomendación UIT-T H.610 fue aprobada el 14 de julio de 2003 por la Comisión de Estudio 16 (2001-2004) 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.

© UIT 2004

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
2.1 Referencias normativas .....	1
2.2 Referencias informativas .....	2
3 Definiciones.....	3
4 Abreviaturas.....	5
5 Terminología .....	9
6 Modelo de referencia .....	10
6.1 Arquitecturas residenciales.....	10
6.2 Puntos de referencia centrales .....	12
7 Descripción general .....	12
7.1 Arquitectura de la red de acceso.....	12
7.2 Arquitectura de red principal.....	16
7.3 Entorno residencial .....	19
7.4 Nodos de servicio .....	20
7.5 Ingeniería IP .....	21
7.6 Puntos de demarcación .....	23
8 Requisitos ATM.....	24
8.1 Red de acceso .....	24
8.2 OLT .....	25
8.3 VTP/D.....	25
9 Conexiones y flujos de servicio.....	26
9.1 Conexión puente.....	27
9.2 Conexión PPPoE .....	27
9.3 Conexión encaminada traducida.....	28
9.4 Conexión encaminada no traducida.....	29
9.5 Conexión cambio de canal.....	30
9.6 Conexión de difusión digital .....	31
9.7 Conexión de gestión remota del VTP/D.....	33
9.8 Conexión BLES.....	33
10 Modelo funcional del VTP/D .....	33
10.1 Bloque ATM.....	34
10.2 Bloque DSL .....	34
10.3 Bloque encaminador .....	34
10.4 Bloque puente.....	36
10.5 Bloque difusión .....	38
10.6 Bloque de voz.....	39

	<b>Página</b>
10.7	Bloque gestión ..... 39
10.8	Bloque interconexión de red doméstica ..... 40
11	Implementación VTP/D básica ..... 40
12	Configuración IP de los CPE ..... 41
12.1	Escenarios estándar de procesamiento IP ..... 41
12.2	DHCP ..... 49
13	Servicio de datos ..... 50
14	Servicio de difusión ..... 50
14.1	Opciones de entrega ..... 50
14.2	Plan de direccionamiento IP de TV de difusión ..... 51
14.3	Transporte ..... 51
14.4	Señalización cambio de canal ..... 52
14.5	Modelo de información para la función cambio de canal dentro de la AN.... 55
15	Servicio VoD ..... 57
15.1	Gestión administrativa de VoD ..... 57
15.2	Ingeniería de red VoD ..... 58
15.3	Exploración de contenido VoD ..... 59
15.4	Establecimiento de sesión VoD ..... 59
15.5	Establecimiento de la conexión VoD ..... 60
16	Directrices para voz por DSL ..... 63
16.1	VoATM ..... 63
16.2	VoIP ..... 63
17	Gestión de la AN ..... 64
17.1	OLT ..... 64
17.2	ONU ..... 64
18	Gestión del VTP/D ..... 64
18.1	Modelo de gestión del VTP/D ..... 64
18.2	Métodos de configuración ..... 69
18.3	Secuencia de configuración VTP/D ..... 71
Anexo A – Formato del fichero de configuración ..... 74	
Anexo B – MIB SNMP para la función cambio de canal ..... 87	
B.1	Relación con otras MIB ..... 87
B.2	Definición de la MIB ..... 87
Apéndice I – Ejemplos de implementación del VTP ..... 96	
I.1	Procesamiento de protocolo ascendente ..... 96
I.2	Procesamiento de protocolo descendente ..... 98
Apéndice II – Función de traducción de IGMP v2 a DSMCC ..... 99	
Apéndice III – Soporte de canales de latencia dual VDSL ..... 100	

	<b>Página</b>
Apéndice IV – Configuraciones IP avanzadas.....	101
IV.1    Configuraciones avanzadas de procesamiento IP.....	101
Apéndice V – Gráficos de secuencias de mensajes .....	107
V.1    Inicialización del VTP .....	107
V.2    Inicialización del STB .....	108
V.3    Cambio de canal TV de difusión – IGMP entre el VTP y la AN.....	109
V.4    Cambio de canal de TV de difusión – DSM-CC entre el VTP y la AN.....	110
V.5    Varios STB zapeando TV de difusión – IGMP entre VTP y AN .....	111
V.6    Selección de la película VoD – Entrega multidifusión IP .....	113
V.7    Selección de la película VoD – Entrega unidifusión IP .....	115
V.8    Descarga remota de programas informáticos en el VTP .....	117
V.9    Navegación por Internet desde un terminal utilizando PPPoE.....	118
V.10   Navegación por Internet desde el VTP utilizando PPP .....	120
Apéndice VI – Descarga de ficheros FPD utilizando TFTP multidifusión .....	122
Apéndice VII – Configuración IP del FPD utilizando PPPoE y DHCP.....	125
Apéndice VIII – Conmutación de protección .....	127
Apéndice IX – Voz por DSL (VoDSL) .....	128
IX.1    BLES .....	128
IX.2    Voz sobre el IP (VoIP) .....	129
Apéndice X – Proceso IEEE para obtener OUI.....	131



## Recomendación UIT-T H.610

### VDSL de servicio completo – Arquitectura de sistema y del equipo en las instalaciones del cliente

#### 1 Alcance

En esta Recomendación se especifica la arquitectura de sistema (SA, *system architecture*) y la arquitectura del equipo en las instalaciones del cliente (CPE, *customer premises equipment*) para la entrega a un entorno doméstico de servicios de vídeo, datos y voz por una red de acceso VDSL, denominada red VDSL de servicio completo. La Recomendación especifica la arquitectura SA y CPE a alto nivel, independientemente del mecanismo de transporte de la capa física subyacente de banda ancha. En esta Recomendación VDSL aparece denominada tecnología de capa física; sin embargo, las especificaciones de arquitectura que se describen también podrían aplicarse a los CPE y las redes de acceso que emplean otras tecnologías de capa física de banda ancha.

En esta Recomendación se define una arquitectura que permite el suministro fiable de un paquete de servicios triple, con mínima intervención del usuario, que cumple los requisitos fundamentales de seguridad y acceso condicional al contenido y con un costo que permita la instalación en masa en el mercado.

Esta Recomendación se basa en la versión 4 del protocolo Internet (IPv4). La utilización del IPv6 queda en estudio.

#### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T acualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

##### 2.1 Referencias normativas

- [1] Recomendación UIT-T I.610 (1999), *Principios y funciones de operaciones y mantenimiento de la RDSI-BA*.
- [2] ATM Forum af-tm-0056.000 (1996), *Traffic Management 4.0*.
- [3] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.
- [4] IEEE Standard 802.1D (1998) | ISO/CEI 15802-3:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common Specifications – Media Access Control (MAC) bridges*.
- [5] Recomendación UIT-T H.611 (2003), *VDSL servicio completo – Aspectos de funcionamiento, administración, mantenimiento y prestación*.
- [6] IETF RFC 2684 (1999), *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.
- [7] IETF RFC 2516 (1999), *A method for transmitting PPP over Ethernet (PPPoE)*.
- [8] Recomendación UIT-T I.363.5 (1996), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la RDSI-BA: Capa de adaptación del modo de transferencia asíncrono tipo S*.

- [9] ATM Forum af-ilmi-0065.000 (1996), *ILMI Integrated Local Management Interface*.
- [10] ISO/CEI 13818-6:1998, Information technology – Generic coding of moving pictures and associated audio information – Part 6: Extensions for DSM-CC. See Chapter 10, U-N Switched Digital Broadcast – Channel Change Protocol, and Annex H (informative), Switched Digital Broadcast Service.
- [11] ATM Forum af-nm-0122.000 (1999), *Auto-configuration of PVCs*.
- [12] DSL Forum Technical Report TR-037 (2001), *Auto-configuration for the connection between the DSL broadband network termination (B-NT) and the network using ATM*.
- [13] Recomendación UIT-T J.82 (1996), *Transporte de señales de televisión con velocidad binaria constante MPEG 2 en la red digital de servicios integrados de banda ancha*.
- [14] IEEE Standard 802.3 (2002), *Information technology – Telecommunication and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.
- [15] Recomendación UIT-T I.361 (1999), *Especificación de la capa modo de transferencia asíncrono de la RDSI-BA*.
- [16] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.
- [17] IETF RFC 2364 (1998), *PPP Over AAL5*.
- [18] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.
- [19] IETF RFC 2453 (1998), *RIP Version 2*.
- [20] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)*.
- [21] IETF RFC 1877 (1995), *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*.
- [22] ETSI TR 101 290 v1.2.1 (2001), *Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems*.
- [23] IETF RFC 2326 (1998), *Real Time Streaming Protocol (RTSP)*.
- [24] IETF RFC 2279 (1998), *UTF-8, a transformation format of ISO 10646*.
- [25] IETF RFC 2863 (2000), *The Interfaces Group MIB*.
- [26] IETF RFC 2515 (1999), *Definitions of Managed Objects for ATM Management*.
- [27] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.
- [28] IETF RFC 3004 (2000), *The User Class Option for DHCP*.
- [29] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.
- [30] IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP)*.
- [31] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.
- [32] IETF RFC 1334 (1992), *PPP Authentication Protocols*.
- [33] IETF RFC 1994 (1996), *PPP Challenge Handshake Authentication Protocol (CHAP)*.

## 2.2 Referencias informativas

- [I-1] Recomendación UIT-T FS-VDSL Focus Group Technical Specification, Part 4 (2002), *Physical layer specification for interoperable VDSL systems*.

- [I-2] Recomendación UIT-T G.783 (2000), *Características de los bloques funcionales del equipo de la jerarquía digital síncrona.*
- [I-3] Recomendación UIT-T I.630 (1999), *Conmutación de protección del modo de transferencia asíncrono.*
- [I-4] Recomendaciones UIT-T de la serie H – Suplemento 3 (2003), *Requisitos de los operadores relativos a los servicios completos por líneas de abonado digital de velocidad muy alta en las Recomendaciones UIT-T H.610 y H.611.*
- [I-5] ATM Forum af-sig-0061.002 (2002), *ATM User Network Interface (UNI) Signalling Specification Version 4.1.*
- [I-6] Recomendación UIT-T I.363.2 (2000), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la RDSI-BA: Capa de adaptación del modo transferencia asíncrono tipo 2.*
- [I-7] IETF RFC 3350 (2003), *RTP: A transport protocol for real-time applications.*
- [I-8] ATM Forum af-vmoa-0145.000 (2000), *Loop Emulation Service Using AAL2.*
- [I-9] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.*
- [I-10] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP.*
- [I-11] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels.*
- [I-12] FIPS 180-1, *Secure hash standard.*
- [I-13] IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based internets: MIB-II.*

### 3 Definiciones

En esta Recomendación se definen los términos siguientes.

**3.1 red de acceso (AN, *access network*):** Incluye la ONU y la OLT. En el modelo de referencia, la AN se encuentra entre la U-R2 y los puntos de referencia V. El término AN se utiliza para describir la totalidad de capacidades de la OLT y de la ONU. Por ejemplo, si la red de acceso debe soportar un atributo  $x$ , la OLT, la ONU o ambas deben implementar el atributo  $x$ . Cuando haya un requisito que deba cumplir un determinado elemento de red, éste se indica.

**3.2 operador de red de acceso:** El operador AN explota el sistema de acceso físico, que abarca el dominio entre la U-R y el punto de referencia V del modelo de referencia del sistema (véase cláusula 6).

**3.3 proveedor de contenido:** El proveedor de contenido genera contenido, por ejemplo copias vídeo en diversos formatos digitales o analógicos. Se supone que el proveedor de servicios contrata al proveedor de contenido para ofrecer a sus abonados acceso al contenido de éste.

**3.4 operador de red principal:** El operador de red principal mantiene y gestiona la red principal que está más allá del punto de referencia V y de la interfaz física OLT.

**3.5 red de difusión digital:** Red multidifusión que se utiliza para distribuir tráfico punto a multipunto, como por ejemplo TV y radio digitales.

**3.6 sistema de gestión de elementos (EMS, *element management system*):** Sistema que permite la gestión de la AN.

**3.7 procesamiento funcional (FP, *functional processing*):** Punto donde se transforman o procesan señales.

- 3.8 procesamiento y decodificación funcionales (FPD, *functional processing and decoding*):** Punto donde se procesa vídeo, audio o datos de la capa aplicación.
- 3.9 red A/V interactiva:** Red unidifusión que se utiliza para entregar servicios de vídeo y audio punto a punto, por ejemplo VoD.
- 3.10 red Internet:** Red de datos de banda ancha en modo dúplex para la transmisión de servicios IP, normalmente servicios Internet.
- 3.11 interfuncionamiento con la red principal (IWCN, *interworking to core network*):** Toda función que es posible incluir en la OLT para interfuncionar con redes principales que no son ATM. Dada la variedad de tecnologías y configuraciones de red principal existentes, en esta Recomendación sólo se tratan los requisitos de la AN hasta el punto de referencia V.
- 3.12 M:** Punto de referencia entre la AN y el EMS.
- 3.13 red de distribución óptica (ODN, *optical distribution network*):** Medio de transmisión óptico que enlaza la OLT y las ONU, en ambos sentidos, entre los puntos de referencia S/R y R/S.
- 3.14 terminación de línea óptica (OLT, *optical line termination*):** Interfaz de red con varios nodos de servicio de múltiples ONU que están conectadas a través de la ODN.
- 3.15 unidad de red óptica (ONU, *optical network unit*):** Sirve de interfaz del lado usuario y está conectada con una OLT primaria a través de la ODN.
- 3.16 OTU-C:** Unidad de terminación óptica en la OLT.
- 3.17 OTU-R:** Unidad de terminación óptica en la ONU.
- 3.18 POTSc/ISDNc:** Interfaz de la RTPC con el divisor PS en el lado ONU.
- 3.19 POTSR/ISDNR:** Interfaz de los terminales de banda estrecha con el divisor PS en el lado de las instalaciones del cliente.
- 3.20 divisor POTS o RDSI (PS, *POTS or ISDN splitter*):** Divisor pasivo, que combina las señales de baja frecuencia (es decir, POTS o RDSI) y las señales de alta frecuencia (es decir, VDSL) en el lado ONU y en el lado de las instalaciones del cliente.
- 3.21 Q:** Punto de referencia para describir la interfaz con la red de gestión, normalmente para la configuración, mantenimiento y suministro del sistema.
- 3.22 R:** La salida (entrada) del FPD hacia (desde) el equipo residencial.
- 3.23 R/S:** Punto de referencia entre la ODN y la ONU.
- 3.24 modelo centralizado residencial:** En esta Recomendación significa la utilización de VTPD como unidad de decodificación.
- 3.25 modelo distribuido residencial:** En esta Recomendación significa la utilización de múltiples FPDs que están conectados al VTP a través de una LAN residencial.
- 3.26 red residencial:** Red digital utilizada en un entorno doméstico para la entrega de servicios FS-VDSL.
- 3.27 S/R:** Punto de referencia entre la OLT y la ODN. Puede tratarse de una interfaz óptica punto a punto o punto a multipunto.
- 3.28 operador de servicio:** El operador de servicio mantiene y gestiona los equipos físicos de uno o varios nodos de servicios que son interfaz con la red de acceso o con la red principal y proporcionan a los usuarios acceso a diversos servicios, por ejemplo servicios de datos, de difusión de vídeo, VoD y vocales.

- 3.29 proveedor de servicio:** El proveedor de servicio es la entidad que utiliza la plataforma física del operador de servicio para proporcionar acceso a diversos servicios, por ejemplo servicios de datos, de difusión de vídeo, VoD y vocales.
- 3.30 T<sub>CN</sub>:** La salida (entrada) de los puertos digitales del VTP/D hacia (desde) la red digital en las instalaciones del cliente.
- 3.31 terminal:** Entidad física que contiene un elemento FPD, por ejemplo un adaptador multimedios (STB, *set-top box*), un PC, teléfono IP.
- 3.32 U-C:** Punto de referencia entre los divisores, ubicados en la ONU, y la red de cobre.
- 3.33 U-C2:** Punto de referencia entre el divisor POTS o RDSI y la VTU-C.
- 3.34 U-R:** Lado red del PS ubicado en las instalaciones del cliente.
- 3.35 U-R2:** Entrada (salida) del lado red del módem VDSL.
- 3.36 V:** Punto de referencia entre la OLT y uno o varios nodos de servicio, ya sea directamente o a través de la red principal.
- 3.37 red de voz:** Red que puede entregar voz con calidad telefónica ordinaria y servicios de voz conmutados. Normalmente la red es una red TDM, como por ejemplo RTPC o RDSI, aunque también puede ser una red de voz por paquetes.
- 3.38 procesamiento de terminación VDSL (VTP, *VDSL termination processing*):** Unidad que realiza las funciones de terminación de módem VDSL y de protocolo. Los dispositivos que implementan las funciones VTP contienen una interfaz de capa 2 Ethernet con la red residencial.
- 3.39 VTP y decodificación (VTPD, *VTP and decoding*):** Unidad que realiza la función de decodificación de vídeo además de las funciones e interfaces VTP. Desde el punto de vista de la red de acceso, las funcionalidades e interfaces del elemento VTPD son idénticas a las del elemento VTP.
- 3.40 VTP/D:** En esta Recomendación se utiliza este término para referirse al VTP y al VTPD.
- 3.41 VTU-C:** Unidad de terminación VDSL (*VDSL termination unit*). Unidad de transmisión VDSL en la ONU.

#### 4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

A/V	Audio/Video
AAL	Capa de adaptación ATM ( <i>ATM adaptation layer</i> )
AIS	Señal de indicación de alarma ( <i>alarm indication signal</i> )
AN	Red de acceso ( <i>access network</i> )
ANSI	Instituto nacional de normas de los Estados Unidos ( <i>American National Standards Institute</i> )
API	Interfaz de programación de aplicaciones ( <i>application programming interface</i> )
ARP	Protocolo de resolución de direcciones ( <i>address resolution protocol</i> )
ATM	Modo de transferencia asíncrono ( <i>asynchronous transfer mode</i> )
BAS	Servidor de acceso de banda ancha ( <i>broadband access server</i> )
BER	Tasa de errores en los bits ( <i>bit error ratio</i> )
BLES	Servicio de emulación de bucle en banda ancha ( <i>broadband loop emulation service</i> )

BPID	ID del programa de difusión ( <i>broadcast program ID</i> )
CA	Acceso condicional ( <i>conditional access</i> )
CAC	Control de admisión de llamada ( <i>call admission control</i> )
CBR	Velocidad binaria constante ( <i>constant bit rate</i> )
CC	Comprobación de continuidad ( <i>continuity check</i> )
CCF MIM	Modelo de información de gestión de la función cambio de canal ( <i>channel change function management information model</i> )
CDV	Variación del retardo de célula ( <i>cell delay variation</i> )
CMIP	Protocolo común de información de gestión ( <i>common management information protocol</i> )
CO	Central ( <i>central office</i> )
CORBA	Arquitectura de intermediario de petición de objeto común ( <i>common object request broker architecture</i> )
CPE	Equipo en las instalaciones del cliente ( <i>customer premises equipment</i> )
CHAP	Protocolo de autenticación de invitación de toma de contacto ( <i>challenge handshake authentication protocol</i> )
DAVIC	Consejo audiovisual digital ( <i>digital audiovisual council</i> )
DBTV	Difusión digital de TV ( <i>digital broadcast TV</i> )
DHCP	Protocolo dinámico de configuración de anfitrión ( <i>dynamic host configuration protocol</i> )
DRM	Gestión de derechos digitales ( <i>digital rights management</i> )
DSL	Línea de abonado digital ( <i>digital subscriber line</i> )
DSM-CC	Medio de almacenamiento digital – Instrucción y control ( <i>digital storage media – command and control</i> )
DVB	Difusión de vídeo digital ( <i>digital video broadcasting</i> )
DVD	Disco versátil digital ( <i>digital versatile disc</i> )
EAS	Sistema de alarma de emergencia ( <i>emergency alert system</i> )
EMS	Sistema de gestión de elementos ( <i>element management system</i> )
EPD	Descarte de paquete anticipado ( <i>early packet discard</i> )
ER	Encaminador de borde ( <i>edge router</i> )
ETSI	Instituto Europeo de Normas de las Telecomunicaciones ( <i>European Telecommunications Standards Institute</i> )
FCC	Federal Communications Commission
FPD	Procesamiento y decodificación funcionales ( <i>functional processing and decoding</i> )
FSAN	Red de acceso a servicio completo ( <i>full service access network</i> )
FS-VDSL	VDSL de servicio completo ( <i>full service VDSL</i> )
FTP	Protocolo de transferencia de ficheros ( <i>file transfer protocol</i> )
HTML	Lenguaje de marcaje hipertexto ( <i>hyper text mark-up language</i> )
HTTP	Protocolo de transferencia de hipertexto ( <i>hyper text transfer protocol</i> )

HW	Soporte físico ( <i>hardware</i> )
IAD	Dispositivo de acceso integrado ( <i>integrated access device</i> )
ICMP	Protocolo de mensajes de control Internet ( <i>Internet control message protocol</i> )
IEEE	Institute of Electrical and Electronics Engineers
IETF	Grupo de tareas especiales de ingeniería en Internet ( <i>Internet engineering task force</i> )
IGMP	Protocolo de gestión del grupo Internet ( <i>Internet group management protocol</i> )
ILMI	Interfaz de gestión local integrada ( <i>integrated local management interface</i> )
IP	Protocolo Internet ( <i>Internet protocol</i> )
IPCP	Protocolo de control de protocolo Internet PPP ( <i>Internet protocol control protocol</i> )
IPv4	Protocolo Internet, versión 4 ( <i>Internet protocol version 4</i> )
IPv6	Protocolo Internet, versión 6 ( <i>Internet protocol version 6</i> )
IWCN	Interfuncionamiento con la red principal ( <i>interworking to core network</i> )
LAN	Red de área local ( <i>local area network</i> )
LCP	Protocolo de control de enlace ( <i>link control protocol</i> )
LT	Terminación de línea ( <i>line termination</i> )
MAC	Control de acceso a medios ( <i>medium access control</i> )
MCM	Modulación multiportadora ( <i>multi-carrier modulation</i> )
MIB	Base de información de gestión ( <i>management information base</i> )
MPEG	Grupo de expertos en imágenes en movimiento ( <i>moving picture experts group</i> )
NAPT	Traducción de direcciones de red y puertos ( <i>network address and port translation</i> )
NAT	Traducción de direcciones de red ( <i>network address translation</i> )
NSP	Proveedor de servicio de red ( <i>network service provider</i> )
NT	Terminación de red ( <i>network termination</i> )
OAM	Operación y gestión ( <i>operation and management</i> )
ODN	Red de distribución óptica ( <i>optical distribution network</i> )
OLT	Terminación de línea óptica ( <i>optical line termination</i> )
ONU	Unidad de red óptica ( <i>optical network unit</i> )
OSI	Interconexión de sistemas abiertos ( <i>open systems interconnection</i> )
OTU-C	Unidad de terminal óptico – Lado oficina central ( <i>optical terminal unit – central office side</i> )
OTU-R	Unidad de terminal óptico – Lado distante ( <i>optical terminal unit – remote side</i> )
PAP	Protocolo de autenticación de contraseña ( <i>password authentication protocol</i> )
PAT	Traducción de direcciones de puerto ( <i>port address translation</i> )
PBX	Centralita privada ( <i>private branch exchange</i> )
PCR	Velocidad de células de cresta ( <i>peak cell rate</i> )
POTS	Servicio telefónico ordinario ( <i>plain old telephone service</i> )

PPD	Descarte de paquetes parcial ( <i>partial packet discard</i> )
PPP	Protocolo punto a punto ( <i>point-to-point protocol</i> )
PPPoA	PPP por ATM ( <i>PPP over ATM</i> )
PPPoE	PPP por Ethernet ( <i>PPP over Ethernet</i> )
PPTP	Protocolo de tunelización punto a punto ( <i>point-to-point tunnelling protocol</i> )
PS	Divisor POTS o ISDN ( <i>POTS or ISDN splitter</i> )
PVC	Circuito virtual permanente ( <i>permanent virtual circuit</i> )
PVP	Trayecto virtual permanente ( <i>permanent virtual path</i> )
QoS	Calidad del servicio ( <i>quality of service</i> )
RDI	Indicación de defecto distante ( <i>remote defect indication</i> )
RDSI	Red digital de servicios integrados
RFC	Petición de comentarios (norma IETF) [ <i>request for comment (IETF standard)</i> ]
RIP	Protocolo de información de encaminamiento ( <i>routing information protocol</i> )
RPV	Red privada virtual
RTP	Protocolo en tiempo real ( <i>real time protocol</i> )
RTSP	Protocolo de trenes en tiempo real ( <i>real time streaming protocol</i> )
SAR	Segmentación y reensamblado ( <i>segmentation and reassembly</i> )
SCM	Modulación monoportadora ( <i>single carrier modulation</i> )
SCSI	Interfaz de pequeños sistemas de computadores ( <i>small computer system interface</i> )
SDH	Jerarquía digital síncrona ( <i>synchronous digital hierarchy</i> )
SDP	Protocolo de descripción de sesión ( <i>session description protocol</i> )
SIP	Protocolo de iniciación de sesión ( <i>session initiation protocol</i> )
SNMP	Protocolo simple de gestión de red ( <i>simple network management protocol</i> )
SONET	Red óptica síncrona ( <i>synchronous optical network</i> )
SPTS	Flujo de transporte de programa único ( <i>single program transport stream</i> )
STB	Adaptador multimedios ( <i>set top box</i> )
SVC	Circuito virtual conmutado ( <i>switched virtual circuit</i> )
SW	Soporte lógico ( <i>software</i> )
TDM	Multiplexación por división en el tiempo ( <i>time division multiplexing</i> )
TE	Equipo terminal ( <i>terminal equipment</i> )
TFTP	Protocolo de transferencia de ficheros trivial ( <i>trivial file transfer protocol</i> )
TM	Transmisión y multiplexación (Comité Técnico ETSI) [ <i>transmission and multiplexing (ETSI Technical Committee)</i> ]
UBR	Velocidad binaria no especificada ( <i>unspecified bit rate</i> )
UPC	Control de parámetros de utilización ( <i>usage parameter control</i> )
USB	Bus serial universal ( <i>universal serial bus</i> )

UTOPIA	Interfaz física de prueba universal y operacional para ATM ( <i>universal test and operational PHY interface for ATM</i> )
VBR	Velocidad binaria variable ( <i>variable bit rate</i> )
VBR-nRT	Velocidad binaria variable que no es en tiempo real ( <i>variable bit rate non-real time</i> )
VBR-RT	Velocidad binaria variable en tiempo real ( <i>variable bit rate real time</i> )
VC	Conexión virtual ( <i>virtual connection</i> )
VCI	Identificador del canal virtual ( <i>virtual channel identifier</i> )
VDSL	Línea de abonado digital de velocidad muy alta ( <i>very high bit rate digital subscriber line</i> )
VLAN	LAN virtual ( <i>virtual LAN</i> )
VoD	Vídeo a la carta ( <i>video-on-demand</i> )
VoDSL	Voz por DSL ( <i>voice over DSL</i> )
VoIP	Voz sobre el protocolo Internet ( <i>voice over IP</i> )
VP	Trayecto virtual ( <i>virtual path</i> )
VPI	Identificador de trayecto virtual ( <i>virtual path identifier</i> )
VTP	Procesamiento de terminación de VDSL ( <i>VDSL termination processing</i> )
VTP/D	VTP o VTPD
VTPD	Procesamiento y decodificación de terminación VDSL ( <i>VDSL termination processing and decoding</i> )
VTPD	VTP y decodificación ( <i>VTP and decoding</i> )
VTU-C	Unidad terminal VDSL – Oficina central ( <i>VDSL terminal unit – central office</i> )
VTU-R	Unidad terminal VDSL – Distante ( <i>VDSL terminal unit – remote</i> )

## 5 Terminología

En esta Recomendación los diferentes niveles de obligación se expresan del modo siguiente.

Obligación firme	La obligación firme se expresa con el futuro simple del verbo principal (futuro de mandato). En algunos casos también puede utilizarse otras expresiones con significado de obligación (como "tener que", "haber que") o el adjetivo "obligatorio".
Prohibición firme	La prohibición firme se expresa mediante la negación de la obligación firme.
Conveniencia	La conveniencia se expresa con el tiempo presente del verbo modal "deber" (debe) u otros verbos con significado de conveniencia (aconsejar, recomendar, ser conveniente) o mediante el adjetivo "recomendado". Expresa que hay que entender plenamente y sopesar las consecuencias que tendría la inobservancia de una determinada disposición, aunque en ciertas circunstancias puedan haber razones fundamentadas para ello.
Opción	La opción se expresa mediante el verbo "poder", otras expresiones que indican posibilidad o probabilidad (como "ser posible"), o los adjetivos "opcional" y "facultativo". Se utiliza cuando existe la posibilidad de elegir entre varias alternativas. La inclusión o no de una determinada opción no afectará a la compatibilidad.

## 6 Modelo de referencia

El modelo de referencia de la figura 1 sirve para definir claramente las interfaces y los puntos de referencia que se utilizan en un entorno FS-VDSL.

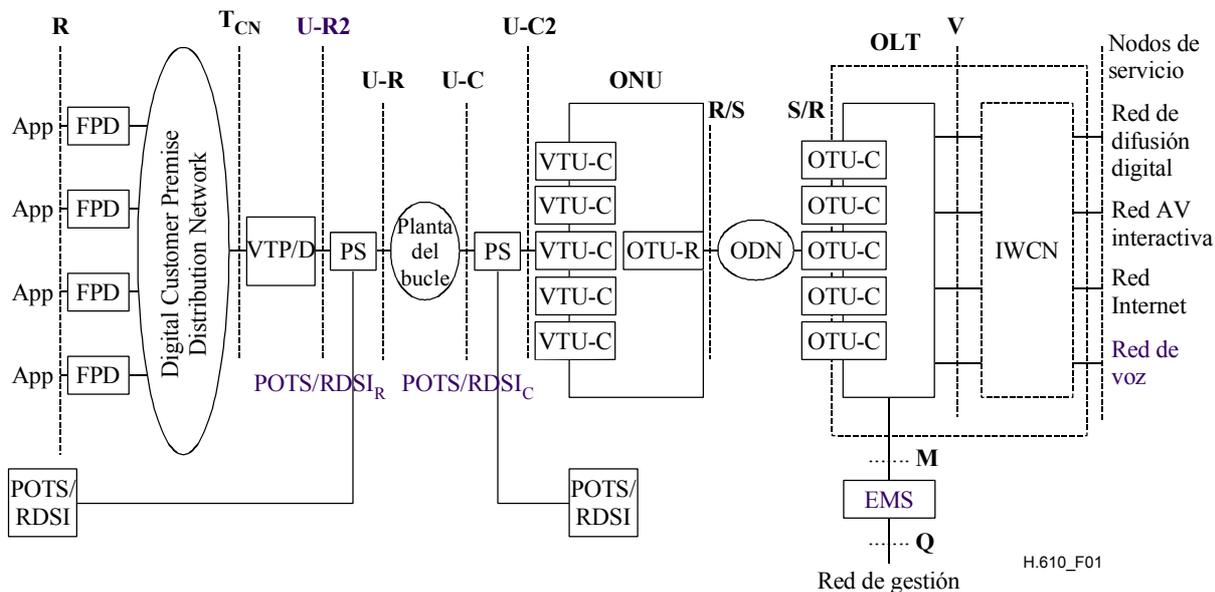
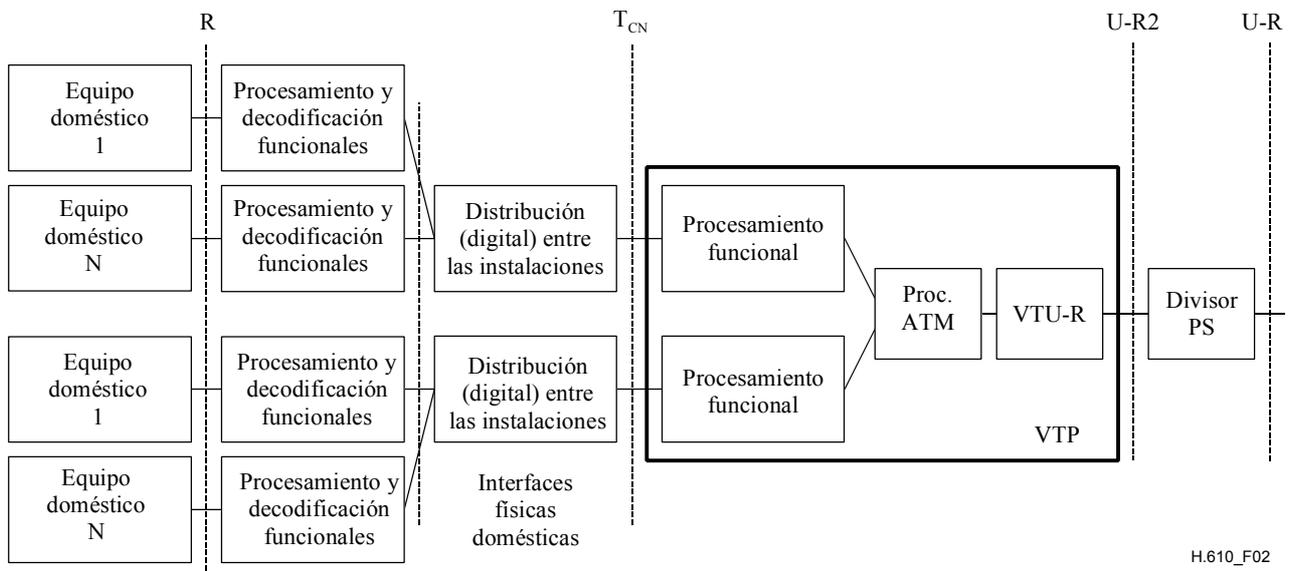


Figura 1/H.610 – Modelo de referencia FS-VDSL

### 6.1 Arquitecturas residenciales

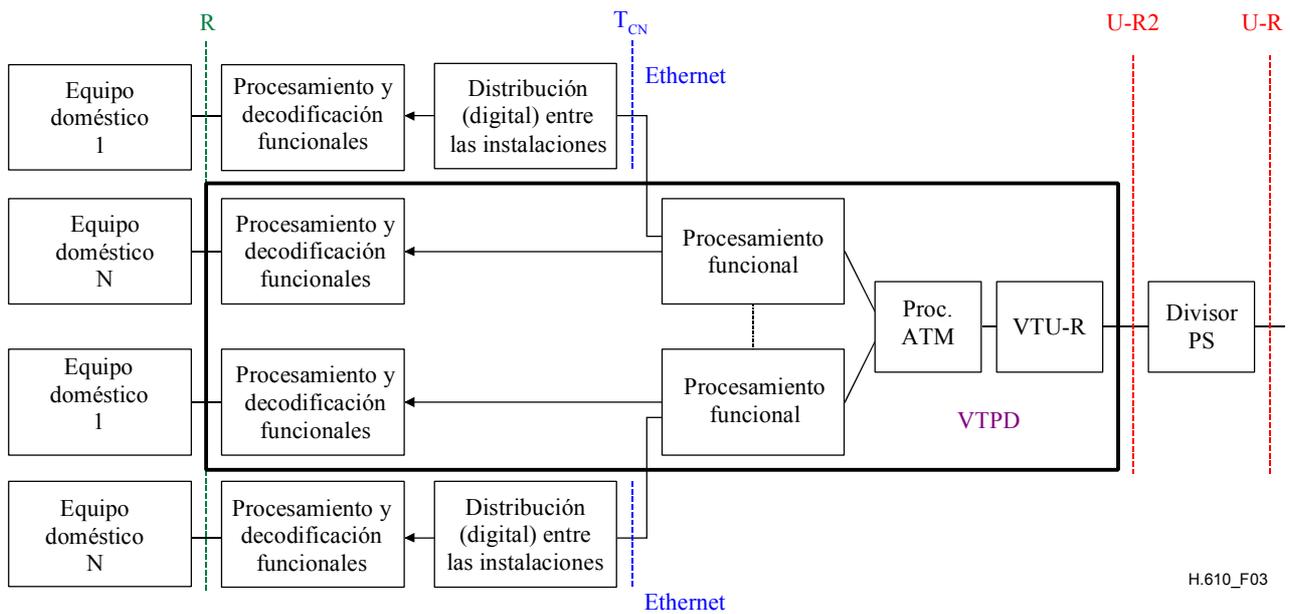
Las implementaciones físicas de los CPE FS-VDSL pueden consistir en un solo dispositivo que realice todo el procesamiento y la decodificación o en varios dispositivos en las instalaciones del cliente en los que esté distribuido el procesamiento y decodificación necesarios para el funcionamiento. Es posible combinar los elementos FP, FPD, VTP y VTPD para crear las dos arquitecturas posibles:

- **Arquitectura distribuida** en la que los diferentes elementos FPD están interconectados como se muestra en la figura 2. Estos elementos contienen los procesadores necesarios para el funcionamiento y posiblemente el propio equipo residencial. El VTP consta de un módem VDSL y un procesador de protocolo y funcional.
- **Arquitectura centralizada** en la que la mayor parte o todo el procesamiento y decodificación se realiza en una sola caja física denominada VTPD, según se muestra en la figura 3. En el interior de esta caja se lleva a cabo el procesamiento funcional y la distribución de señales digitales mediante buses.



**Figura 2/H.610 – Disposición del VTP correspondiente a una arquitectura CPE completamente distribuida**

Cuando la arquitectura de los CPE es una combinación de arquitecturas centralizadas y distribuidas, el VTPD tendrá que tener una interfaz T<sub>CN</sub> para conectar los componentes distribuidos.



**Figura 3/H.610 – Disposición del VTPD correspondiente a una arquitectura CPE centralizada con FP distribuidas opcionales**

## 6.2 Puntos de referencia centrales

Los puntos de referencia importantes de la arquitectura se describen en el cuadro 1.

**Cuadro 1/H.610 – Puntos de referencia importantes**

Punto de referencia	Ubicación
T <sub>CN</sub>	La entrada (salida) de los puertos digitales del VTP/D hacia (desde) la red digital en las instalaciones del cliente.
U-R2	Entrada del lado de red del módem DSL.
V	Punto de referencia ubicado entre la red de acceso ATM y cualquier función IWCN que conecta la red de acceso a la red principal.
M	Interfaz entre la OLT y el EMS.

### 6.2.1 Punto de referencia T<sub>CN</sub>

Los módulos de procesamiento de protocolo del VTP/D recibirán por el T<sub>CN</sub> una trama 802.3, definida en IEEE 802.3, cuyo campo tipo/longitud especifique el tipo de protocolo cliente MAC. Ahora bien, esto no significa que la red residencial utilice obligatoriamente la capa MAC 802.3 o una capa física Ethernet. Es posible utilizar diferentes tipos de MAC y capas físicas. En esta Recomendación se utiliza el término 'Ethernet', en el contexto de una capa en una pila de protocolos, para referirse a un formato de trama 802.3, según se ha definido antes.

### 6.2.2 Punto de referencia U-R2

En la interfaz U-R2, las capas de protocolo VTP/D serán las siguientes:

- La capa física será una capa DSL normalizada que transporte ATM.
- La capa ATM se implementará de conformidad con la subcláusula 8.3.
- La implementación de las capas superiores se hará de conformidad con la cláusula 9.

### 6.2.3 Punto de referencia V

Este punto de referencia está entre la AN ATM y cualquier función IWCN que conecta la AN con una red principal.

Este punto de referencia proporcionará una capa ATM de conformidad con la Rec. UIT-T I.361.

### 6.2.4 Punto de referencia M

Esta interfaz lógica hace posible la gestión a distancia de la OLT mediante el EMS, como se describe en la Rec. UIT-T H.611.

## 7 Descripción general

Esta cláusula describe la arquitectura general de las redes FS-VDSL y tiene carácter informativo. En esta cláusula no se define ningún requisito obligatorio. Esta arquitectura proporciona la infraestructura para la entrega de datos (normalmente acceso a Internet), vídeo (difusión y por demanda) y servicios vocales, como se describe en detalle en las Recomendaciones UIT-T de la serie H – Suplemento 3.

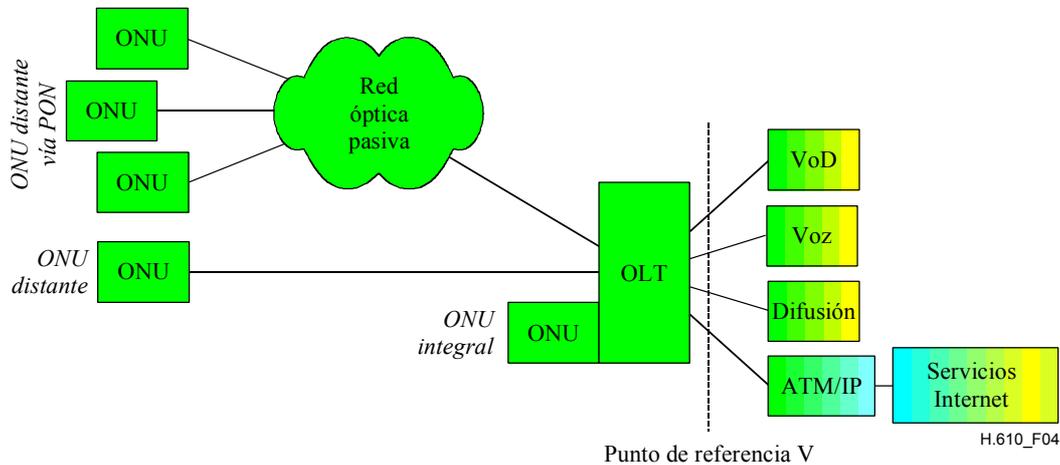
### 7.1 Arquitectura de la red de acceso

#### 7.1.1 Descripción general de la red de acceso

Esta Recomendación está concebida para redes de acceso basadas en DSL. La capa física puede ser VDSL, ADSL u otras tecnologías DSL existentes o futuras que cumplan los requisitos de servicio. La selección del tipo de DSL para una determinada implementación depende de las características

concretas del paquete de servicios, por ejemplo de los servicios que se ofrecen y la velocidad binaria necesaria.

En función de la topología de red, la red de acceso (AN, *access network*) puede estar formada por diversos equipos. Por ejemplo, los equipos CO pueden o no incluir tarjetas de línea DSL, y los enlaces físicos entre componentes AN pueden ser punto a punto o punto a multipunto. Asimismo, es posible tener una combinación de dos arquitecturas en la misma red. La figura 4 ilustra estas opciones de configuración básicas de la AN.

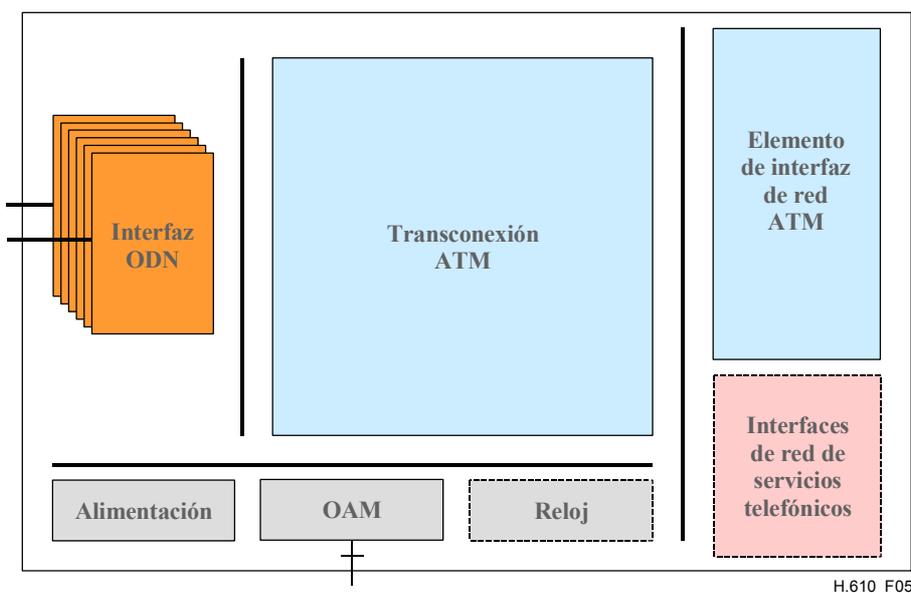


**Figura 4/H.610 – Posibles topologías de la red de acceso**

### 7.1.2 OLT

La función de la OLT es agrupar varias ONU. En el sentido ascendente, la OLT agrupa el tráfico ATM que procede de las ONU y que se dirige al punto de referencia V; en el sentido descendente realiza lo contrario, es decir demultiplexa el tráfico y lo distribuye a las ONU.

Los sistemas FS-VDSL pueden realizar las funciones de ONU y de OLT en una sola caja física. En el caso de un sistema ONU y OLT unificado, todos los elementos funcionales (descritos a continuación) de la OLT y la ONU están contenidos en una misma caja física.



**Figura 5/H.610 – Bloques funcionales de la OLT**

### **7.1.2.1 Elemento interfaz de red**

El elemento interfaz de red realiza las funciones de capa ATM y PHY que actúan como interfaz con la OLT y la red ATM. En el caso de que se utilicen redes principales que no son ATM, el elemento interfaz de red realiza la conversión de protocolo entre ATM y la tecnología de red principal utilizada. En una misma OLT pueden haber múltiples elementos interfaz de red que soporten transmisión ATM unidireccional o bidireccional.

### **7.1.2.2 Interfaces de red de servicio telefónico**

La OLT puede contener un elemento interfaz telefónica que permita la conexión de ésta con la red vocal, el cual hace las conversiones de protocolo necesarias. El elemento interfaz telefónica puede soportar transporte de voz TDM, ATM o IP y su correspondiente señalización.

### **7.1.2.3 Transconexión ATM**

Este bloque realiza la transconexión VP/VC hacia las interfaces adecuadas, y desde éstas. Además de una capa ATM, este bloque debe proporcionar funciones de protocolo de capa superiores como por ejemplo el procesamiento cambio de canal, el control de acceso y la gestión.

### **7.1.2.4 Interfaz de red de distribución óptica (ODN)**

Este bloque realiza las funciones de capa ATM y PHY de la interfaz de la OLT que conecta la OLT con las ONU a través de la ODN. La tecnología de capa física puede ser conforme a las diversas normas de transmisión óptica o puede ser específico del fabricante.

### **7.1.2.5 Bloque OAM**

El bloque OAM realiza las funciones de operación, administración y gestión de la AN vía la interfaz M.

### **7.1.2.6 Bloque de alimentación**

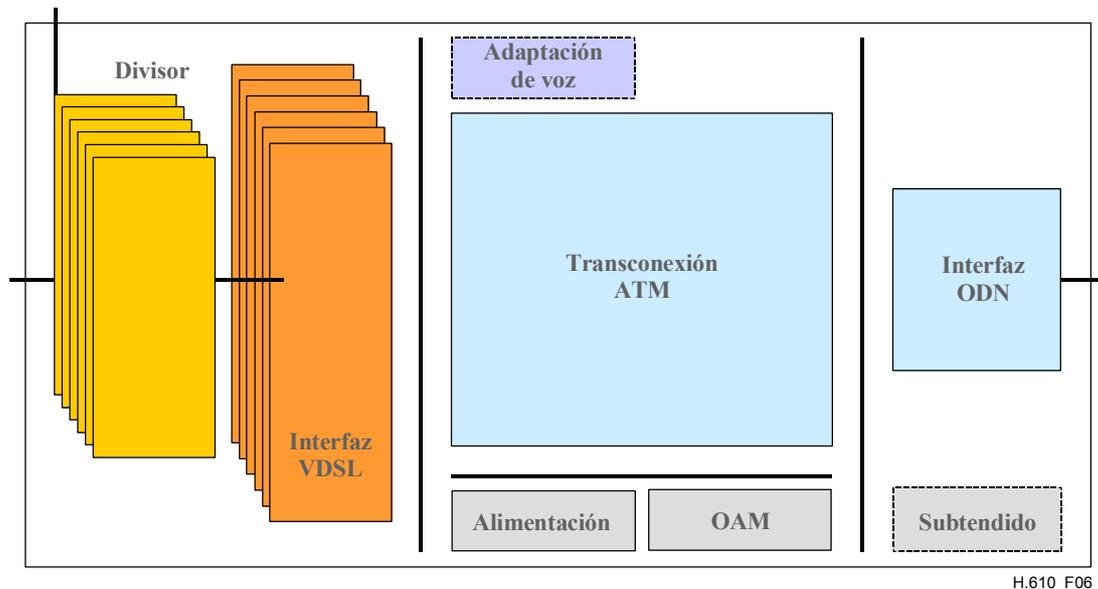
El bloque de alimentación suministra la tensión y la corriente necesarias para todos los circuitos electrónicos de la OLT. No es obligatorio que la OLT, que normalmente se encuentra en la central, tenga una batería de reserva.

### **7.1.2.7 Bloque reloj**

En función de la implementación de los demás bloques, es posible que haya una interfaz de reloj externo.

## **7.1.3 ONU**

La ONU actúa como una transconexión ATM entre las líneas DSL y la ODN.



**Figura 6/H.610 – Bloques funcionales de la ONU**

### 7.1.3.1 Interfaz ODN

Este bloque realiza las funciones de capa ATM y PHY en la interfaz que conecta la ONU a la OLT a través de la ODN.

### 7.1.3.2 Adaptación de voz

La ONU puede contener un elemento adaptación de voz que realiza la conversión de señales de voz en la banda base a voz por paquetes, voz por ATM o voz por IP.

### 7.1.3.3 Transconexión ATM

Este bloque realiza la transconexión VP/VC desde las interfaces adecuadas o hacia las mismas. Este bloque puede realizar funciones de protocolo de capas superiores, por ejemplo el procesamiento cambio de canal.

### 7.1.3.4 Interfaces VDSL

La interfaz VDSL realiza la función de la VTU-C. Además realiza la terminación de funciones de capa PHY VDSL y soporta el transporte ATM por líneas de cobre.

### 7.1.3.5 Divisor POTS/RDSI

En el sentido ascendente, el divisor POTS realiza la separación de capa PHY de la frecuencia portadora POTS/RDSI y de la frecuencia portadora VDSL. En el sentido descendente el divisor POTS/RDSI combina la portadora PHY POTS/RDSI y la portadora PHY VDSL en frecuencias portadoras separadas por la misma derivación de cobre.

### 7.1.3.6 Bloque OAM

El bloque OAM permite la operación, administración y gestión de la ONU, en particular de las derivaciones DSL. Las funciones OAM se realizan mediante una conexión ATM dentro de la banda.

### 7.1.3.7 Bloque alimentación

El bloque alimentación suministra la tensión y la corriente necesarias para todos los circuitos electrónicos de la ONU. Dado que la ONU puede estar instalada en el exterior, es posible que este bloque también suministre potencia a los ventiladores de refrigeración y a los sistemas de circuitos

de la batería de reserva. Además, el bloque de potencia ONU puede suministrar alimentación a los sensores medioambientales o circuitos de alarma externos, si los hubiere.

Normalmente, los sistemas de alimentación de la ONU están formados por componentes locales, distantes y de reserva.

### 7.1.3.8 Subtendido

La ONU puede incluir un bloque de subtendido que conecte otras ONU secundarias.

## 7.2 Arquitectura de red principal

En cada instalación concreta, es posible que la AN esté conectada a nodos de servicio mediante redes principales de diferentes topologías y tecnologías. La red principal se utiliza para que la interconexión de la AN a los diversos nodos de servicio sea flexible. Las capacidades que ofrece la red principal son las siguientes:

- Ancho de banda suficiente para soportar el tráfico entre la AN y los nodos de servicio.
- QoS adecuada para los diferentes servicios.
- Encaminamiento/conmutación de tráfico entre la AN y los nodos de servicio.
- Multidifusión de tráfico de difusión en los puntos más óptimos de la red principal.
- Control de admisión cuando se produce una concentración de ancho de banda dentro de la red principal.
- Interfuncionamiento de tecnologías de red principal híbridas (por ejemplo, ATM a IP).
- Si se permite la interconexión a redes terceras, se deben proporcionar los puntos homólogos adecuados.

En las siguientes subcláusulas se describen los posibles escenarios de instalación.

### 7.2.1 Red de acceso ATM

En muchas instalaciones de red, los nodos de servicio están centralizados, por ejemplo en un centro de operaciones de red, y por consiguiente, se necesita una red principal para conectar la OLT a los nodos de servicio. Como la OLT funciona como una transconexión ATM, es posible conectarla con una red ATM obteniéndose un transporte ATM totalmente compatible de VC ATM y VP ATM. En una red principal ATM no es obligatorio el interfuncionamiento de protocolo entre el punto de referencia V y la red principal. Este tipo de instalación se ilustra en la figura 7.

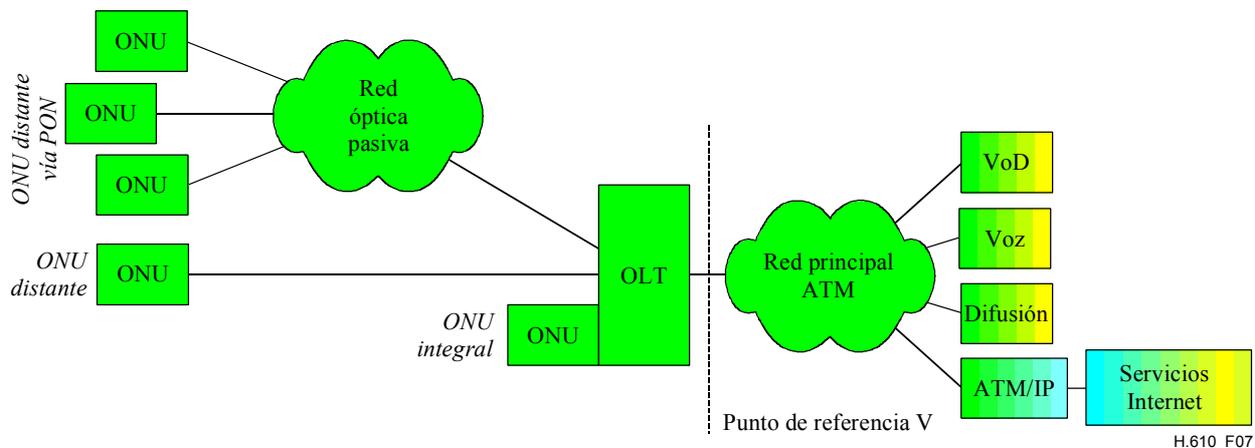
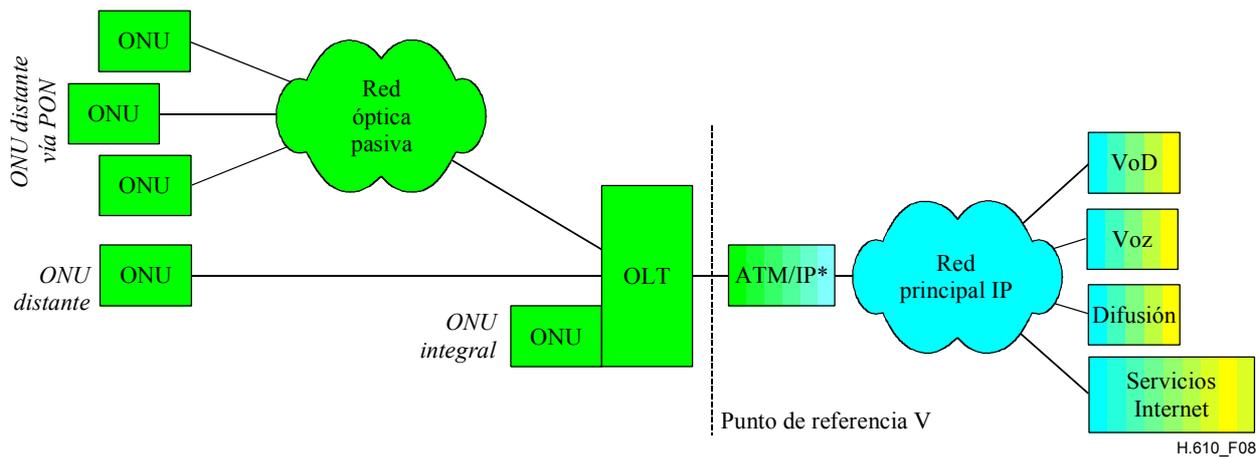


Figura 7/H.610 – Red principal ATM

## 7.2.2 Red principal IP

En esta Recomendación se describe la arquitectura IP para cada uno de los servicios FS-VDSL obligatorios, y para algunos de estos servicios se especifica además una solución AMT pura. Es decir, aunque la AN esté basada en el protocolo ATM, los protocolos que utilizan los puntos extremo (es decir los nodos de servicio y los equipos residenciales) para suministrar los servicios son del tipo IP. Esto significa que en muchas instalaciones el tráfico que atraviesa el punto de referencia V es 100% de PDU IP. Por consiguiente es posible terminar la capa ATM en el punto de referencia V y conectar las OLT a los nodos de servicio mediante una red IP. Este caso se ilustra en la figura 8.



\* El nodo de servicio local ATM/IP puede estar implementado en el mismo equipo que la OLT.

**Figura 8/H.610 – Red principal IP**

Este tipo de instalación presenta algunas dificultades técnicas, la mayoría de las cuales tienen que ver con mantener las características QoS coherentes en las dos redes.

## 7.2.3 Otros escenarios de red principal

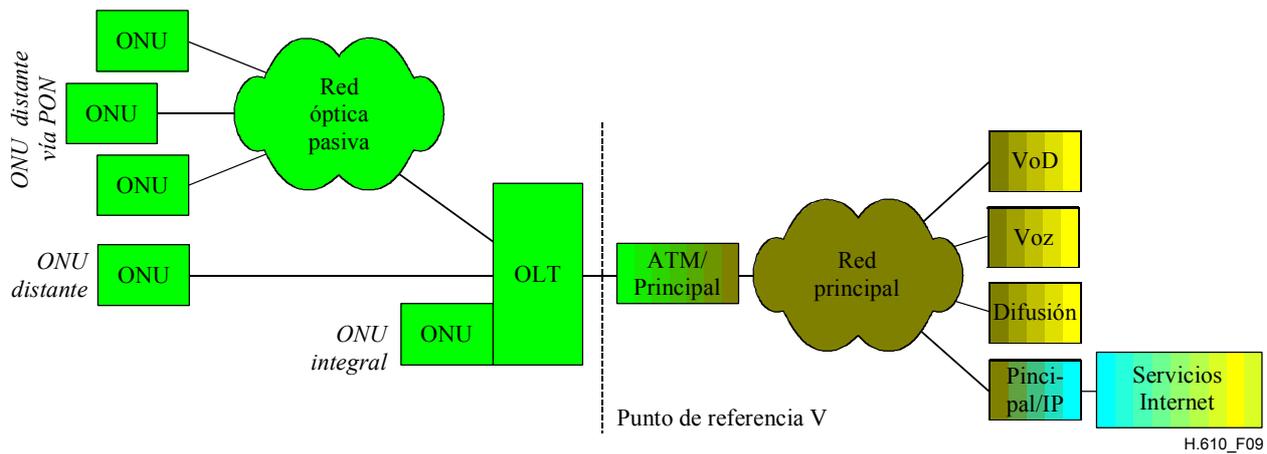
Esta Recomendación no se limita a las redes principales de tecnología ATM o IP. También son posibles otros protocolos y tecnologías de red, por ejemplo SONET/SDH, Ethernet y MPLS. Dado que la OLT es un dispositivo ATM, es obligatorio el interfuncionamiento entre la OLT y la red principal. Hay tres posibles maneras de lograr el interfuncionamiento.

Una primera forma consiste en encapsular y multiplexar una o más VC ATM en el punto de referencia V dentro de una entidad de transporte conforme de la red principal. En este caso, la red principal es en realidad una red de capa 1. La red principal debe transportar el paquete de VC de modo que, cuando se elimine el encapsulado, sea posible regenerar la VC ATM con todas las características de la VC original.

Una segunda posibilidad es emular la VC ATM con la entidad de transporte de la red. En este caso, la red principal es una red de capa 2 como la ATM. Esta emulación se debe realizar de manera que todas las características de la conexión sean idénticas a las de la VC original.

Por último, la terminación de las VC ATM y el transporte de capa superiores de manera transparente. En este caso, la red principal es en realidad una red de capa 3. Esta solución sólo debería tenerse en consideración cuando el protocolo de capa 3 es IP, en cuyo caso se reduce al de la red principal IP del caso anterior.

Este tipo de instalación se ilustra en la figura 9. Se supone que el nodo de servicio realiza también las funciones de terminación del protocolo de red principal y de pila de protocolo de servicios.

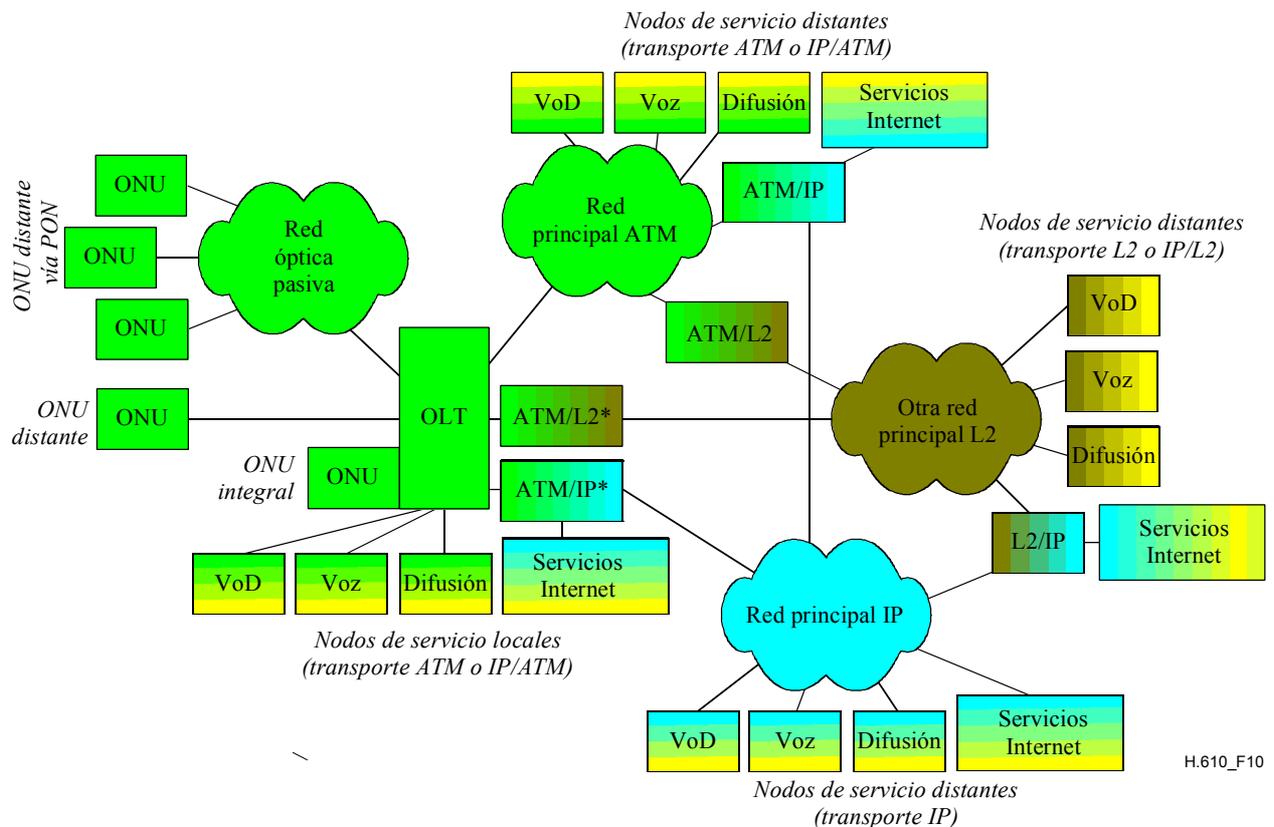


\* El nodo de servicio local ATM/Principal puede estar implementado en el mismo equipo que la OLT.

**Figura 9/H.610 – Otra posible red principal**

### 7.2.4 Red principal híbrida

Muchos operadores de red utilizan más de un escenario de red principal, lo cual se debe probablemente a la evolución de las redes y a que se siguen utilizando equipos de generaciones anteriores junto con equipos de nuevas generaciones. Los escenarios de instalación descritos anteriormente no son los únicos y se pueden combinar de muy diversas maneras, muchas de las cuales se muestran en la figura 10.



\* El nodo de servicio local ATM/IP y/o ATM/L2 puede estar implementado en el mismo equipo que la OLT (en cuyo caso la interfaz ATM es interna al equipo).

**Figura 10/H.610 – Red principal híbrida**

### 7.3 Entorno residencial

En un entorno de instalaciones de cliente FS-VDSL pueden haber los siguientes tipos de funcionalidades.

- Un divisor de servicio que separe las señales eléctricas DSL de las de los demás servicios de baja frecuencia (por ejemplo POTS o RDSI). En la figura 1 se muestra el divisor PS entre las interfaces UR y UR2.
- Un módem VDSL en las instalaciones de cliente, VTU-R (véase [1]). La función VTU-R está contenida en un elemento VTP o VTPD.
- Procesamiento de protocolo e interfaces de distribución en la vivienda, que forman parte de la función VTP.
- Unidades de decodificación MPEG para la visualización de vídeo de difusión y VoD, que forman parte de las funciones VTPD y FPD.
- PC y otros dispositivos IP de las instalaciones del cliente conectados a servicios de datos IP, que están abarcados por las funciones FP y FPD.
- Dispositivos locales analógicos o digitales que están conectados a servicios VoATM o VoIP, que también están abarcados por las funciones FPD.
- Equipos domésticos, como por ejemplo aparatos de televisión que son el destino último de la información audio/vídeo procesada y decodificada. En el cuadro 2 figuran ejemplos de la interfaz entre la FPD y los equipos domésticos.

**Cuadro 2/H.610 – Ejemplos de interfaces entre equipos domésticos y FPD**

Cable coaxial (vídeo compuesto modulado en RF)
S-Vídeo
Vídeo Compuesto
Componente de Vídeo
SCART
Dolby Digital/AC-3
L/R Stereo
Línea telefónica
Ethernet
USB
IEEE 1394
Audio analógico de 5 canales
SCSI
LPDT paralelo
RS-232 serie
Bluetooth
Emisor IR (para el control de dispositivos controlados por infrarrojos)
IEEE 802.11b
HomeRF

Como se observa en la lista anterior, la categoría FP abarca funciones muy diversas. En el cuadro 3 se dan ejemplos de funciones FP y FPD.

### Cuadro 3/H.610 – Ejemplo de procesamiento funcional

Decodificación de vídeo MPEG-1 ó 2
Decodificación de vídeo MPEG-4
Vídeo H.323
Decodificación de audio MPEG/MP3
Dolby digital (AC-3/AAC)
Descriptación y desaleatorización
Procesamiento de acceso condicionado
Procesamiento de gestión de permisos
Procesamiento de aplicaciones
Programas intermedios
Procesamiento de datos IP
Control y gestión a distancia
RF
IR
MIC de 64 kbit/s para servicios vocales conexos

#### 7.4 Nodos de servicio

En la figura 11 se muestra una descripción esquemática de los nodos de servicio en un sistema FS-VDSL.

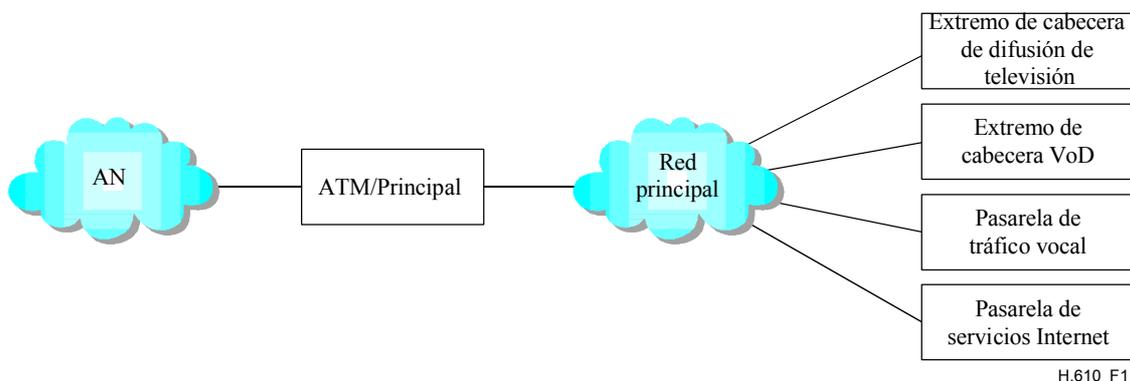


Figura 11/H.610 – Nodos de servicio FS-VDSL

##### 7.4.1 Extremo de cabecera de difusión de televisión

El sistema de extremo de cabecera recibe secuencias de vídeo en diversos formatos, los reformatea y encapsula, actúa como interfaz con la red principal y transmite la señal vídeo por la red principal hacia la red de acceso. En esta Recomendación no se especifican restricciones sobre los mecanismos de adquisición de vídeo aplicables al sistema de extremo de cabecera.

##### 7.4.2 Extremo de cabecera VoD

El extremo de cabecera VoD está formado por múltiples elementos, entre los que se cuentan:

- Gestión administrativa, en particular gestión de activos, gestión de abonados, gestión de sesiones y gestión de derechos digitales (DRM, *digital rights management*).
- Una "granja de servidores" con el contenido digital.
- Instalaciones de redes de transporte y de acceso que garantizan la QoS.

- Soporte lógico de aplicación de servidor atractivas para soportar el servicio VoD.

### 7.4.3 Pasarela de tráfico vocal

La pasarela de tráfico vocal realiza las funciones interfaz necesarias para el tráfico vocal modulado digitalmente desde la red de acceso ATM a la RTPC/RDSI tradicional, y viceversa. La función de pasarela de voz puede realizarse con un sólo dispositivo o mediante múltiples dispositivos (por ejemplo, pasarelas de medios, pasarelas de señalización y controladores de pasarelas de medios).

Las principales funciones de la pasarela son:

- Terminación de los circuitos locales TDM que son la interfaz con la RTPC/RDSI.
- Terminación de la señalización RTPC/RDSI.
- Control de llamada y de portador.
- Terminación AAL 2 y (de)multiplexación (todas las conexiones vocales de una VTP/D pasan a través de una sola VC ATM) en el caso de BLES.
- (De)multiplexación de VoIP (es posible concentrar múltiples conexiones vocales en una sola dirección IP) en el caso de VoIP.
- Funciones de tratamiento de la voz (por ejemplo, creación de paquetes, compresión, cancelación de ecos, supresión de ecos, supresión de silencios, generación de ruido de confort, tonos y anuncios).
- Terminación de la señalización del FPD a la pasarela.
- Conectividad a la RTPC/RDSI mediante una interfaz abierta.
- Soporte V5.2 para ETSI y soporte GR-303 para ANSI.

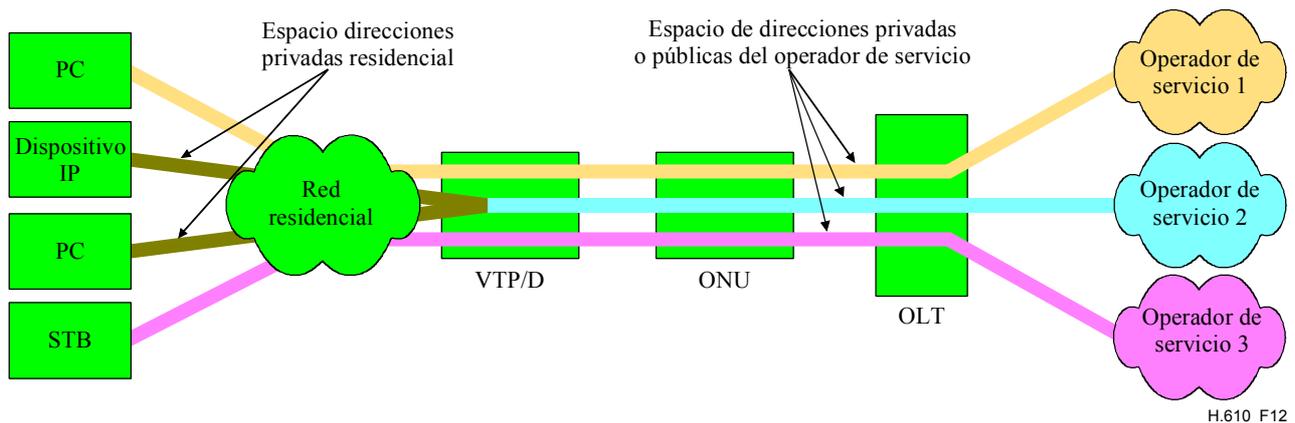
### 7.5 Ingeniería IP

Para facilitar múltiples servicios a determinados abonados mediante múltiples operadores de servicio, quizá sea necesario que coexistan simultáneamente diversos planes de direccionamiento IP en la red residencial del abonado. Los operadores de red y/o los operadores de servicio deben proporcionar las directrices para garantizar la coherencia de todos los planes de direccionamiento IP. Esto significa, entre otras cosas, garantizar que todas las subredes a las que se pueda acceder simultáneamente mediante un determinado VTP/D no tengan gamas de direcciones IP conflictivas.

El plan de ingeniería IP se establece de acuerdo con las siguientes restricciones, que podrían aplicarse a un sistema FS-VDSL.

- Habida cuenta de lo limitado del espacio de direcciones público IPv4, y la naturaleza "ininterrumpida" de este servicio, es preferible que la utilización de direcciones públicas sea mínima.
- En el caso de aplicaciones sensibles a NAT, por ejemplo juegos punto a punto y voz por IP, es posible utilizar espacios de direccionamiento privados o públicos.
- Probablemente, el cliente realizará múltiples conexiones lógicas a múltiples redes dentro del entorno de red residencial.
- Un proveedor de servicio o de red que suministre equipos residenciales, por ejemplo STB y equipos Internet, necesitará comunicarse con esos dispositivos, para, por ejemplo, la actualización, la reconfiguración o la instalación de éstos.

La figura 12 ilustra los planes de direccionamiento considerados:



**Figura 12/H.610 – Planes de direccionamiento de red**

Pueden haber simultáneamente hasta cuatro planes de direccionamiento IP distintos:

- Plan de direccionamiento VTP/D T<sub>CN</sub>.
- Plan de direccionamiento VTP/D U-R2.
- Plan de direccionamiento del operador de servicio basado en sesión de terminal.
- Plan de direccionamiento del operador de servicio no basado en sesión de terminal.

#### 7.5.1 Plan de direccionamiento VTP/D T<sub>CN</sub>

El VTP/D atribuye direcciones IP privadas a los terminales designados a través de su servidor DHCP IETF RFC 2131. También es posible implementar este plan mediante una configuración IP estática. Sin embargo, no se recomienda esta opción.

#### 7.5.2 Plan de direccionamiento VTP/D U-R2

El operador de servicio utiliza los métodos indicados a continuación para asignar una dirección IP al VTP/D. Es posible que diferentes operadores de servicio asignen simultáneamente varias direcciones IP a un solo VTP/D para distintas interfaces IP. En ese caso, la función de encaminamiento del VTP/D debe gestionar el reenvío correcto de paquetes IP a la interfaz IP adecuada.

- Basada en la sesión – El VTP/D inicia una sesión PPP con el encaminador limítrofe del operador de servicio.
- No basada en sesión – El VTP/D obtiene la dirección IP del servidor DHCP/BOOTP del operador de servicio.
- Configuración estática – Aunque es posible, no se recomienda la configuración estática.

#### 7.5.3 Plan de direccionamiento del operador de servicio basado en sesión de terminal

El terminal inicia una sesión PPPoE con el nodo de servicio de datos del operador de servicio. Varios terminales residenciales pueden utilizar este plan simultáneamente para conectarse al mismo o a diferentes operadores de servicio.

#### 7.5.4 Plan de direccionamiento del operador de servicio no basado en sesión de terminal

El operador de servicio asigna direcciones IP a los terminales residenciales utilizando uno de los siguientes métodos:

- Configuración dinámica – El servidor DHCP del operador de servicio asigna las direcciones IP del terminal.

- Configuración estática – Aunque es posible, no se recomienda la configuración estática.

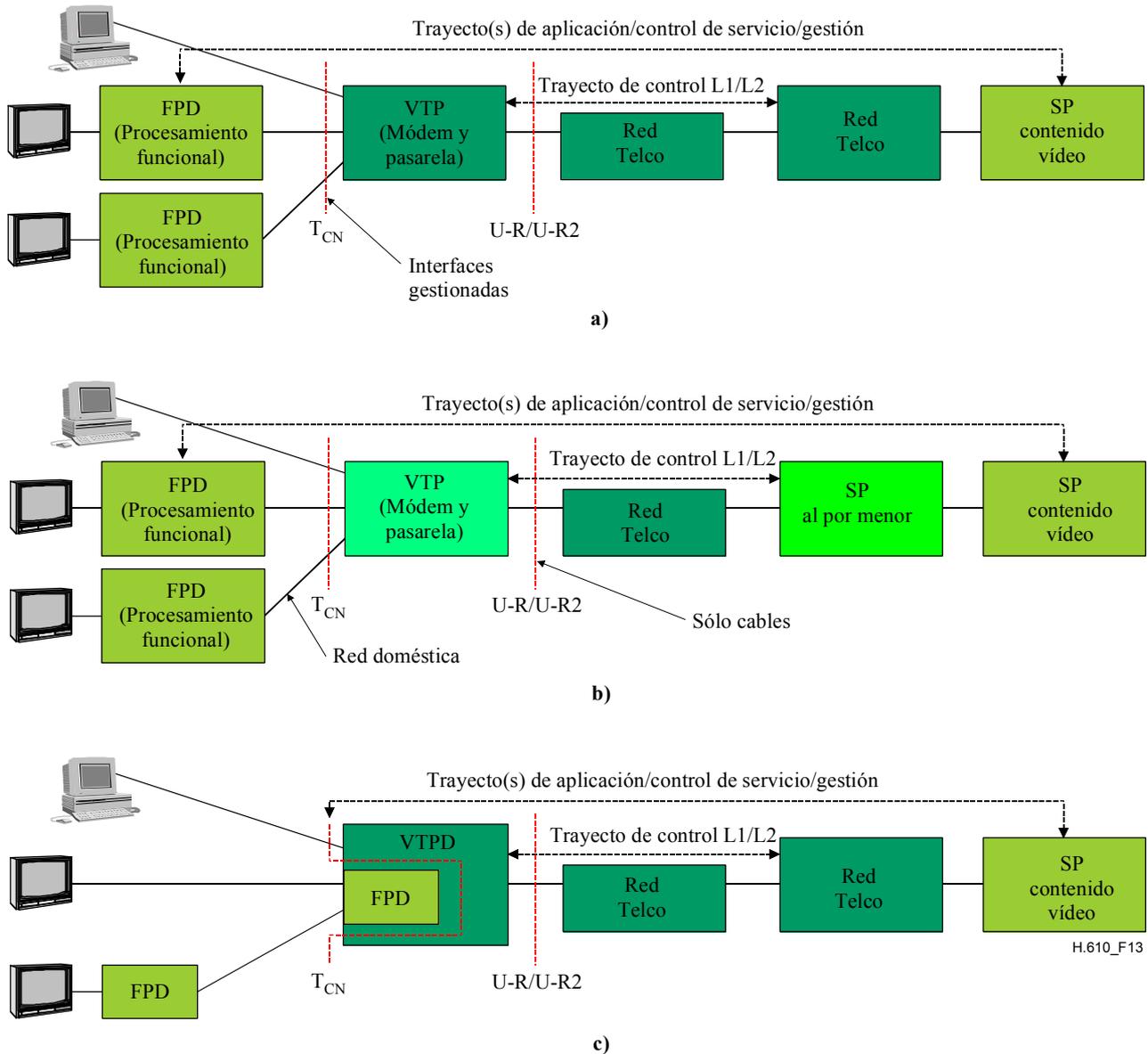
Varios terminales residenciales pueden utilizar simultáneamente este plan para conectarse al mismo o a diferentes operadores de servicio.

#### **7.5.5 Política de direccionamiento IP utilizando DHCP**

En un sistema FS-VDSL pueden haber varios servidores de DHCP funcionando simultáneamente. Para garantizar que a los mensajes DHCP responde el servidor DHCP correcto, los sistemas conformes FS-VDSL deben cumplir ciertas restricciones en el lado red residencial y en el lado operador de servicio necesarios para lograr la integridad del plan de redireccionamiento. Este asunto se trata con mayor detalle en 10.3.4.

#### **7.6 Puntos de demarcación**

Es posible que algunos proveedores proporcionen los equipos CPE residenciales como parte de su oferta de servicios. Esta situación se ilustra en la figura 13 partes a) y c). Otra posibilidad es que los proveedores de red proporcionen un servicio al punto de diferenciación U-R o U-R2 y, por consiguiente, las funciones VTP o VTPD las proporcionen los proveedores de servicio. El caso de VTP se muestra en la parte b) de la figura 13. La interfaz U-R2 incluye el cableado desde la interfaz U-R del divisor hasta el conector VTP. Es posible que el proveedor controle la QoS y la gestión hasta la interfaz  $T_{CN}$  o incluso hasta la interfaz R, en función de la implementación. El control de entrega de servicio residencial se extiende hasta el FPD. Los puntos de marcación pueden variar en función del operador de red y de la reglamentación.



- a) El VTP se controla desde el dominio de red y las ofertas de servicios son interfaces gestionadas.  
 b) El VTP lo controla el proveedor de servicio (SP).  
 c) En lugar del VTP como en (a) se muestra un VTPD.

**Figura 13/H.610 – Modelo de referencia que muestra soluciones comerciales**

## 8 Requisitos ATM

En la siguiente subcláusula se describen los requisitos funcionales ATM de la OLT, la ONU y el VTP/D.

La capa física DSL soportará el transporte ATM.

### 8.1 Red de acceso

- La AN soportará la transconexión de conexiones de trayecto virtual (VP) ATM.
- La AN soportará transconexión de conexiones de canal virtual (VC) ATM.
- La AN soportará la terminación de conexiones VC de funciones específicas, por ejemplo cambio de canal de TV, gestión, etc.

- La AN será capaz de actuar como un punto extremo OAM ATM, como se describe en la Rec. UIT-T I.610 [1], para conexiones VC y VP (es decir, F5 y F4, respectivamente) que terminan en ella.
- La AN será capaz de actuar como un punto de segmento OAM para conexiones VC o VP que están transconectadas a través de ella.
- La AN soportará conexiones ATM punto a multipunto mediante las cuales se duplican las secuencias TV de difusión de acuerdo con la función de cambio de canal.
- La AN soportará el control de tráfico (es decir, UPC) de conexiones de usuario, como se describe en la especificación de gestión de tráfico del foro ATM, versión 4.0 [2].
- La AN soportará las siguientes categorías de servicio ATM: CBR, VBR-RT, VBR-nRT, UBR definidas en ATM Forum Specification af-tm-0056.000 [2].
- La AN soportará el descarte de tramas (es decir, EPD, PPD) por conexión designado por el tráfico AAL 5.
- La AN podrá soportar conexiones virtuales conmutadas (SVC, *switched virtual connections*).
- Si la AN soporta SVC, tendrá que soportar la señalización de la interfaz de red de usuario (UNI, *user network interface*) ATM Forum Specification af-sig-0061.002 [I-5].

### 8.1.1 Soporte de OAM F4 y F5

Los siguientes requisitos se aplican a la implementación OAM especificada en la Rec. UIT-T I.610 [1]. Obsérvese que el funcionamiento de la red de acceso en una determinada conexión debe ser acorde con su función configurada para esa conexión (por ejemplo, punto extremo, punto de segmento, etc.).

- La AN responderá a bucles OAM.
- La AN generará mensajes de indicación de defectos (por ejemplo, AIS, RDI).
- La AN debe informar a los bloques OAM de los mensajes de indicación de defectos detectados.
- La AN debe funcionar como un punto sumidero de comprobación de continuidad (CC, *continuity check*).

## 8.2 OLT

La OLT debe soportar la formación de conexiones VP hacia la red (es decir, en el punto de referencia V).

### 8.2.1 Soporte de OAM F4 y F5

Los siguientes requisitos se aplican a la implementación OAM descrita en la Rec. UIT-T I.610 [1]:

- La OLT debe ser capaz de funcionar como un punto de origen de comprobación de continuidad (CC) hacia la red de acceso.
- La OLT debería ser capaz de generar células de bucle (LB, *loop-back cells*) hacia la red de acceso.

## 8.3 VTP/D

Los siguientes requisitos son obligatorios para el punto de referencia U-R2:

- El VTP/D soportará la capa 5 de adaptación ATM (de acuerdo con la Rec. UIT-T I.363.5 [8]) y la función de segmentación y reensamblado (SAR, *segmentation and reassembly*) ATM.

- El VTP/D que soporte el servicio voz por ATM (VoATM) soportará a tal efecto la capa 2 de adaptación ATM (de acuerdo con la Rec. UIT-T I.363.2 [I-6]).
- El VTP/D soportará la terminación de conexiones permanentes de trayecto virtual (PVP, *permanent virtual path*).
- El VTP/D soportará la terminación de conexiones permanentes de circuito virtual (PVC, *permanent virtual circuit*).
- El VTP/D soportará conexiones de circuito virtual conmutados (SVC).
- El VTP/D que soporte SVC será conforme con ATM Forum Specification af-sig-0061.002 [I-5].
- El VTP/D soportará al menos los tipos de tráfico CBR, VBR-nRT y UBR, definidos en [2]. El VTP/D será capaz de dar forma a estos tipos de tráfico en el sentido ascendente (es decir hacia la red). El VTP/D soportará el servicio UBR con una determinada PCR.
- El VTP/D soportará la puesta en cola y planificación de células ATM en el sentido ascendente.
- El VTP/D soportará el descarte por paquetes de PDU AAL 5, a saber, no transmitirá a la red tramas AAL 5 incompletas.

### 8.3.1 Soporte OAM F4 y F5

Los siguientes requisitos se aplican a la implementación OAM descrita en la Rec. UIT-T I.610 [1]:

- El VTP/D soportará flujos OAM ATM de los niveles F4 y F5.
- El VTP/D soportará OAM ATM de extremo a extremo.
- El VTP/D soportará función de bucle OAM ATM.
- El VTP/D soportará indicaciones de defectos OAM ATM, es decir, AIS y RDI.
- El VTP/D soportará función de sumidero de comprobación de continuidad (CC) OAM ATM. La activación y desactivación podrá realizarse enviando una célula de activación/desactivación o mediante gestión distante (por ejemplo, RGT).
- El VTP/D podrá soportar la función de información hacia atrás (BR) de supervisión de calidad de funcionamiento (PM) OAM ATM.
- El VTP/D debe ser capaz de recibir células AIS por conexiones punto a multipunto. En ese caso el VTP/D entrará en un estado de defecto como se describe para la conexión punto a punto (excepto para la transmisión de células).

## 9 Conexiones y flujos de servicio

Es posible que cada servicio requiera características de conexión diferentes. A continuación el tipo de conexión ATM queda determinada por el procesamiento de control de capa superior que le corresponde en los puntos extremos. Las redes de servicio completo soportarán simultáneamente los siguientes tipos de conexión, que se definen en las siguientes subcláusulas.

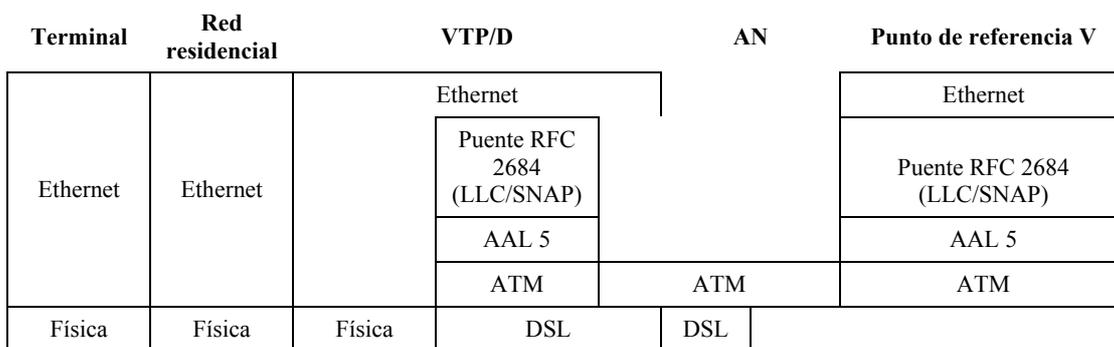
- Conexión puente (subcláusula 9.1).
- Conexión PPPoE (subcláusula 9.2).
- Conexión encaminada traducida (subcláusula 9.3).
- Conexión encaminada no traducida (subcláusula 9.4).
- Conexión cambio de canal (subcláusula 9.5).
- Conexión difusión digital (subcláusula 9.6).
- Conexión de gestión remota del VTP/D (subcláusula 9.7).
- Conexión BLES (subcláusula 9.8).

Estas conexiones se inician en el VTP/D y pueden llegar hasta el punto de referencia V. El tráfico que se transmite y recibe en los puntos extremos por un determinado tipo de conexión se denomina respectivamente *flujo*, por ejemplo, flujo puente o flujo PPPoE. Aunque los cuatro primeros tipos de conexión en la lista anterior son genéricos, en el sentido de que se pueden utilizar para transportar una gran variedad de servicios, los últimos tres tipos de conexión son específicos de una función o servicio.

### 9.1 Conexión puente

Este tipo de conexión soporta el puenteo de tramas Ethernet entre la red residencial y un nodo de servicio. En un mismo VTP/D se pueden iniciar múltiples conexiones puente, de modo que los diferentes servicios puedan utilizar simultáneamente conexiones distintas. Cada una de ellas se identifica como una **Conexión puente**. La red tendrá capacidad para soportar múltiples conexiones puente por una misma línea DSL. El flujo direccional de PDU recibidas y transmitidas en la conexión puente se conoce como **flujo puente**.

Los dos puntos puente garantizarán la seguridad, para lo cual impedirán explícitamente el reenvío de una VC a otra VC. La encapsulación Ethernet en el punto de referencia V y la interfaz U-R2 serán conformes con el modo puente RFC 2684 que utiliza LLC/SNAP sin FCS, como se describe en IETF RFC 2684.



**Figura 14/H.610 – Pila de protocolo de la conexión puente**

### 9.2 Conexión PPPoE

Este tipo de conexión soporta el transporte de tráfico PPPoE entre terminales residenciales designados y un nodo de servicio. En la misma VC ATM se pueden establecer múltiples sesiones PPPoE. El flujo bidireccional de PDU recibidas y transmitidas por la conexión PPPoE se denomina **flujo PPPoE**.

La implementación PPPoE en el terminal y en el nodo de servicio será conforme con RFC 2516 [7]. La red tendrá que ser capaz de soportar una conexión PPPoE por línea DSL.

El encapsulado en U-R2 y en el punto de referencia V de la conexión PPPoE será conforme con el modo puente de RFC 2684 que utiliza LLC/SNAP sin FCS. En la figura 15 se muestra el procesamiento del protocolo de extremo a extremo correspondiente a una conexión PPPoE.

Terminal	Red residencial	VTP/D	AN	Punto de referencia V
IP				IP
PPP				PPP
PPPoE		Función filtrado		PPPoE
Ethernet	Ethernet	Ethernet		Ethernet
		Puente RFC 2684 (LLC/SNAP)		Puente RFC 2684 (LLC/SNAP)
		AAL 5		AAL 5
		ATM	ATM	ATM
Física	Física	Física	DSL	DSL

**Figura 15/H.610 – Pila de protocolo de la conexión PPPoE**

### 9.3 Conexión encaminada traducida

Este tipo de conexión permite que múltiples dispositivos extremo compartan una misma dirección IP para acceder a la red pública. Esta conexión soporta una conexión encaminada entre el VTP/D y un nodo de servicio. La dirección IP de los terminales residenciales se corresponden utilizando una función NAT (traducción de direcciones de red IETF RFC 3022 [16]) que se aplica a las direcciones IP del VTP asignadas por el operador de servicio. La correspondiente traducción de direcciones de puerto (PAT, *port address translation*) permite hacer corresponder una sola dirección IP de una sola interfaz de un encaminador en múltiples direcciones IP (privadas) de las otras interfaces. La red tendrá la capacidad de soportar una conexión encaminada traducida por línea DSL.

El VTP/D y el nodo de servicio que termina la VC ATM soportarán el PPP como se define en RFC 1661. El transporte PPP se puede realizar mediante PPPoA de conformidad con RFC 2364 [17] utilizando para ello la opción de encapsulado de multiplexación VC, o mediante PPPoE de conformidad con RFC 2516 utilizando en ese caso el modo puente RFC 2684 que utiliza LLC/SNAP sin FCS.

El flujo bidireccional de PDU recibidas y transmitidas por la conexión encaminada traducida se denomina flujo encaminado traducido. En las figuras 16 y 17 se muestra el procesamiento del protocolo de extremo a extremo correspondiente a una conexión encaminada traducida.

Terminal	Red residencial	VTP/D	AN	Punto de referencia V
IP		IP		IP
Ethernet	Ethernet	Ethernet	NAT/PAT	IP
				PPP
				RFC 2364 (VC mux)
				AAL 5
		ATM	ATM	ATM
Física	Física	Física	DSL	DSL

**Figura 16/H.610 – Pila de protocolo de la conexión encaminada traducida con PPPoA**

Terminal	Red residencial	VTP/D			AN	Punto de referencia V
IP		IP	NAT/PAT	IP		IP
Ethernet	Ethernet	Ethernet		PPP		PPP
				RFC 2516		RFC 2516
				Ethernet		Ethernet
				Puente RFC 2684 (LLC/SNAP)		Puente RFC 2684 (LLC/SNAP)
				AAL 5		AAL 5
ATM		ATM	ATM			
Física	Física	Física		DSL	DSL	

**Figura 17/H.610 – Pila del protocolo de la conexión encaminada traducida con PPPoE**

#### 9.4 Conexión encaminada no traducida

Este tipo de conexión soporta una conexión encaminada entre el VTP/D y el nodo de servicio. Cada conexión de este tipo se denomina **conexión encaminada no traducida**. La red soportará múltiples conexiones de este tipo por una misma línea DSL. El flujo bidireccional de PDU recibidas y transmitidas por esta conexión se denomina **flujo encaminado no traducido**.

Existen diversos tipos de conexiones encaminadas no traducidas. Éstas se identifican de acuerdo con el encapsulado IP: IP por ATM, PPPoA o PPPoE.

##### 9.4.1 IP por ATM

IP por ATM se realiza mediante conexiones de modo encaminado RFC 2684. Tanto el VTP/D como el nodo de servicio que termina la capa ATM soportarán el modo encaminado RFC 2684 mediante LLC/SNAP. A diferencia de los otros tipos de conexiones encaminadas no traducidas, este método encapsulado no soporta la autenticación inherente de usuario. En la figura 18 se muestra el procesamiento del protocolo de extremo a extremo correspondiente a una conexión encaminada IP por ATM.

Terminal	Red residencial	VTP/D		AN	Punto de referencia V
IP		IP			IP
Ethernet	Ethernet	Ethernet	Ruta RFC 2684 (LLC/SNAP)		Ruta RFC 2684 (LLC/SNAP)
			AAL 5		AAL 5
			ATM		ATM
Física	Física	Física	DSL	DSL	

**Figura 18/H.610 – Conexión IP por ATM**

##### 9.4.2 PPPoA encaminada no traducida

Este tipo de conexión soporta el encaminamiento de tráfico de datos desde las terminales residenciales y hacia las mismas en una conexión PPP establecida entre el VTP/D y el nodo de servicio.

Para soportar este tipo de conexión, el VTP/D y el nodo de servicio que termina la VC ATM soportarán PPPoA, de conformidad con RFC 2364 que utiliza la opción de encapsulado de multiplexación VC. En la figura 19 se muestra el procesamiento de protocolo de extremo a extremo correspondiente a una conexión PPPoA encaminada no traducida.

Terminal	Red residencial	VTP/D		AN	Punto de referencia V
IP		IP			IP
Ethernet	Ethernet	Ethernet	PPP	ATM	PPP
			RFC 2364 (VC mux)		RFC 2364 (VC mux)
			AAL 5		AAL 5
			ATM		ATM
Física	Física	Física	DSL	DSL	

**Figura 19/H.610 – Pila de protocolo de la conexión PPPoA encaminada no traducida**

### 9.4.3 PPPoE encaminada no traducida

Este tipo de conexión soporta el encaminamiento de tráfico de datos hacia terminales residenciales y desde los mismos por una conexión PPPoE establecida entre el VTP/D y el nodo de servicio.

Para soportar este tipo de conexión el VTP/D y el nodo de servicio que termina la VC ATM soportará PPPoE, de conformidad con RFC 2516 que utiliza la opción de encapsulado LLC/SNAP sin FCS. En la figura 20 se muestra el procesamiento del protocolo de extremo a extremo correspondiente a una conexión PPPoE encaminada no traducida.

Terminal	Red residencial	VTP/D		AN	Punto de referencia V
IP		IP	IP		IP
Ethernet	Ethernet	Ethernet	PPP	ATM	PPP
			RFC 2516		RFC 2516
			Ethernet		Ethernet
			Puente RFC 2684 (LLC/SNAP)		Puente RFC 2684 (LLC/SNAP)
			AAL 5		AAL 5
			ATM		ATM
Física	Física	Física	DSL	DSL	

**Figura 20/H.610 – Pila de protocolo de conexión PPPoE encaminada no traducida**

### 9.5 Conexión cambio de canal

Este tipo de conexión soporta mensajería de cambio de canal entre el VTP/D y la red de acceso. Los mensajes de cambio de canal por esta conexión serán IGMPv2 RFC 2236 [18] o DSM-CC ISO/CEI 13818-6 [10].

La conexión cambio de canal utilizará una VC ATM dedicada entre el VTP/D y la red de acceso. El flujo bidireccional de PDU recibidas y transmitidas por esta conexión se denomina **flujo cambio de canal**.

La red soportará una conexión cambio de canal por línea DSL.

### 9.5.1 Utilización de IGMPv2

Cuando se utiliza IGMPv2, el encapsulado de la conexión cambio de canal será conforme con el modo encaminado RFC 2684 que utiliza LLC/SNAP. En la figura 21 se describe el procesamiento del protocolo de extremo a extremo correspondiente a una conexión cambio de canal basada en IGMP.

Terminal	Red residencial	VTP		AN
IGMPv2		IGMP Proxy		IGMPv2
IP		IP		IP
Ethernet	Ethernet	Ethernet	Puente RFC 2684 (LLC/SNAP)	Puente RFC 2684 (LLC/SNAP)
			AAL 5	AAL 5
			ATM	ATM
Física	Física	Física	DSL	DSL

**Figura 21/H.610 – Pila de protocolo de extremo a extremo IGMP**

### 9.5.2 Utilización de DSM-CC

En la figura 22 se muestra el procesamiento de protocolo de extremo a extremo correspondiente a una conexión cambio de canal basada en DSM-CC. Obsérvese que en la figura se indica que el VTP realiza la traducción IGMP a DSM-CC. La DSM-CC se encapsula directamente sobre la AAL 5 (es decir multiplexación VC).

Terminal	Red residencial	VTP		AN
IGMPv2		IGMPv2/DSM-CC		DSM-CC
IP		IP		
Ethernet	Ethernet	Ethernet	AAL 5	AAL 5
			ATM	ATM
			DSL	DSL
Física	Física	Física	DSL	DSL

**Figura 22/H.610 – Pila del protocolo IGMP a DSM-CC**

## 9.6 Conexión de difusión digital

Este tipo de conexión soporta la distribución unidireccional de información de difusión digital. La conexión se implementa como un enlace VC hoja punto a multipunto, la cual se puede conectar dinámicamente a una raíz punto a multipunto en la red de acceso. La red tendrá la capacidad de soportar múltiples de esas conexiones por una misma línea DSL. El flujo unidireccional de PDU recibidas por esta conexión se denomina **flujo de difusión digital**. Son posibles dos métodos de entrega de difusión digital, MPEG-2 por AAL 5 y MPEG-2 por UDP/IP/Ethernet por AAL 5. En ambos casos, la red mapea un solo SPTS MPEG-2 en una sola conexión ATM punto a multipunto.

### 9.6.1 MPEG-2 por UDP/IP/Ethernet por AAL 5

En este método, la secuencia de transporte (TS) MPEG-2 se encapsula en UDP, IP y Ethernet y se transporta por AAL 5 utilizando una cabecera LLC/SNAP sin FCS, de acuerdo con RFC 2684. En

la figura 23 se muestra el correspondiente procesamiento del protocolo de extremo a extremo. Obsérvese que en caso de un VTPD sólo son aplicables las tres columnas que están más a la derecha de la figura 23 (la capa IP y las capas superiores que aparecen en la columna terminal se procesan en el VTPD).

Terminal	Red residencial	VTP	AN	Punto de referencia V
Un solo programa				Un solo programa
MPEG-2 TS				MPEG-2 TS
UDP				UDP
IP				IP
Ethernet	Ethernet	Ethernet		Ethernet
			Puente RFC 2684 LLC/SNAP	Puente RFC 2684 LLC/SNAP
			AAL 5	AAL 5
		ATM	ATM punto a multipunto	ATM
Física	Física	Física	DSL	DSL

**Figura 23/H.610 – MPEG2 por UDP/IP/Ethernet por AAL 5**

### 9.6.2 MPEG-2 por AAL 5

En este método, la MPEG-2 TS se transporta directamente por AAL 5 de acuerdo con la cláusula 8/J.82 [13]. En la figura 24 se muestra el correspondiente procesamiento del protocolo de extremo a extremo. Obsérvese que en el caso de un VTPD sólo son aplicables las tres columnas que están más a la derecha de la figura 24 (el MPEG-2 TS y las capas superiores que aparecen en la columna terminal se procesan en el VTPD).

Terminal	Red residencial	VTP	AN	Punto de referencia V
Un solo programa				Un solo programa
MPEG-2 TS				MPEG-2 TS
UDP		UDP		AAL 5
IP		IP		AAL 5
Ethernet	Ethernet	Ethernet	ATM	ATM punto a multipunto
Física	Física	Física	DSL	DSL

**Figura 24/H.610 – MPEG-2 por AAL 5**

### 9.6.3 Futuros métodos de entrega basados en IP

La AN y el VTP serán transparentes a la cabida útil de las PDU IP recibidas por la conexión de difusión digital. De este modo se podrán utilizar en el futuro otros métodos de entrega basados en IP, por ejemplo RTP IETF RFC 3350 [I-7], y MPEG-4, para lo cual bastará con actualizar únicamente los puntos extremo (es decir, el codificador y el decodificador).

## 9.7 Conexión de gestión remota del VTP/D

Este tipo de conexión soporta el flujo de tráfico bidireccional entre el VTP/D y los agentes de gestión en la red. Se utiliza para la gestión y configuración remota del VTP/D. La red tendrá la capacidad de soportar una conexión de gestión remota del VTP/D por línea DSL.

El flujo bidireccional de PDU recibidas y transmitidas por esta conexión se denomina **flujo de gestión remota del VTP/D**. En la figura 25 se muestra el procesamiento de control de extremo a extremo correspondiente a la conexión de gestión remota del VTP/D.

El VTP/D utilizará DHCP IETF RFC 2131 [3] para extraer dinámicamente la configuración IP de esta conexión.

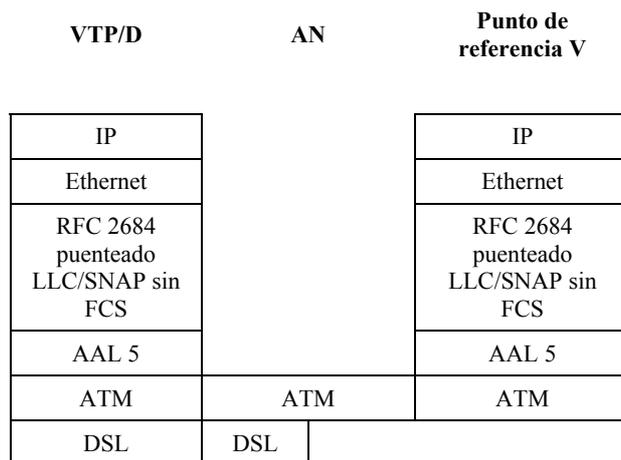


Figura 25/H.610 – Conexión de gestión remota del VTP/D

## 9.8 Conexión BLES

Este tipo de conexión soporta tráfico de voz por ATM entre el VTP/D y la pasarela de voz designada. El flujo bidireccional de PDU recibidas y transmitidas por esta conexión se denomina **flujo BLES**. La implementación del VTP/D y de la pasarela de voz debe ser acorde con af-vmoa-0145.000 [I-8]. En la figura 26 se muestra el procesamiento del protocolo correspondiente a este flujo.

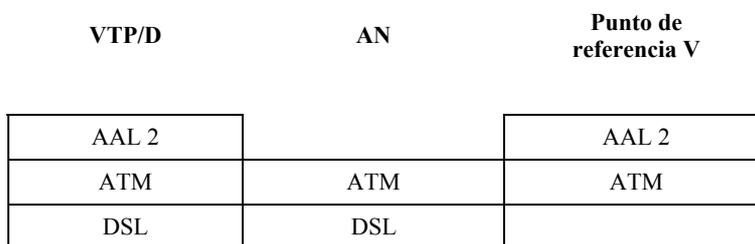


Figura 26/H.610 – Conexión BLES

## 10 Modelo funcional del VTP/D

Esta cláusula especifica los bloques funcionales correspondientes a las capacidades del VTP/D. Un VTP/D real es una implementación de varios de estos bloques funcionales. La selección de los bloques funcionales para una determinada implementación dependerá de los flujos que necesite soportar el VTP/D. En la cláusula 11 se especifican los bloques funcionales necesarios para un VTP/D básico. Son posibles otras implementaciones de VTP/D, para lo cual se seleccionarán otros

bloques funcionales. En cualquier caso, los bloques funcionales elegidos deberán cumplir la especificación que se describe en esta cláusula.

En esta cláusula se utilizan los siguientes términos:

- Ascendente – se refiere al flujo de datos desde la T<sub>CN</sub> hacia la interfaz U-R2.
- Descendente – se refiere al flujo de datos desde la U-R2 a la interfaz T<sub>CN</sub>.
- Flujo encaminado – término que abarca el flujo encaminado traducido y el no traducido.
- Flujo puenteado – término que abarca los flujos "puente" y "PPPoE".
- VC encaminadas – VC ATM que transportan flujos encaminados.
- VC puenteadas – VC ATM que transportan flujos puenteados.
- Tramas encaminadas – tramas Ethernet que llegan a la interfaz T<sub>CN</sub> que transportan un flujo encaminado en la red residencial y que por consiguiente, en el sentido ascendente, son PDU con cabecera MAC Ethernet que contienen como dirección de destino la dirección MAC T<sub>CN</sub> VTP/D y una dirección de destino IP unidifusión.
- Tramas puenteadas – tramas Ethernet que llegan a la interfaz T<sub>CN</sub> y que transportan un flujo puente en la red residencial.

### 10.1 Bloque ATM

El bloque *ATM* realiza las funciones de capa ATM y AAL, como se describe en 8.3.

### 10.2 Bloque DSL

El bloque *DSL* implementa la capa física en la interfaz UR-2.

### 10.3 Bloque encaminador

El bloque encaminador se ocupa de dos flujos de paquetes, el flujo encaminado traducido y el flujo encaminado no traducido. En la interfaz UR-2 el flujo traducido utiliza la conexión encaminada traducida y el flujo no traducido utiliza las conexiones encaminadas no traducidas. El bloque encaminador soportará al menos una conexión encaminada traducida y 4 conexiones encaminadas no traducidas.

#### 10.3.1 Flujo encaminado traducido

Este tipo de flujo de paquetes transporta paquetes que necesitan la traducción de direcciones de red (NAT, *network address translation*) y la traducción de direcciones de puerto (PAT) dentro del VTP/D. La traducción consiste en convertir los dominios de direcciones IP de la interfaz T<sub>CN</sub> en las direcciones IP de la interfaz U-R2. Obsérvese que los servicios vídeo no deben utilizar este flujo a causa de las consecuencias que esto tendría en la fluctuación de fase y en implementación. En el cuadro 4 se describe cómo se procesa este flujo en el VTP/D.

**Cuadro 4/H.610 – Flujo encaminado traducido**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	Los paquetes IP destinados a la conexión encaminada traducida se harán pasar por una función de encaminamiento y también por funciones de traducción de direcciones de red (NAT) y de traducción de direcciones de puerto (PAT), de acuerdo con RFC 3022.
<b>Salida ascendente</b>	Paquetes encaminados cuya dirección de destino IP cumpla los criterios de encaminamiento de la conexión NAT.
	Si el VTP/D soporta una función de retransmisión IGMP (por ejemplo, para habilitar la unión de secuencias multidifusión de Internet) y delimita la conexión encaminada traducida, la salida podrá incluir mensajes IGMP con una dirección de clase D que no pertenece al dominio de servicio de medios de difusión (TV).
	Si se soporta el reenvío en sentido ascendente de PDU multidifusión IP y está limitado a la conexión encaminada traducida, la salida podrá contener unidades PDU multidifusión IP con una dirección de destino de clase D que no pertenece al dominio de servicios de medios de difusión (TV).
<b>Entrada descendente</b>	Paquetes IP recibidos por la conexión encaminada traducida, cuyas direcciones origen y destino son direcciones IP públicas, y cuyas direcciones de destino IP corresponden a la dirección IP pública del VTP asignada por la función NAT.
<b>Procesamiento funcional descendente</b>	Paquetes recibidos por la conexión encaminada traducida se encaminarán a la red residencial después de pasar por las funciones NAT y PAT.
<b>Salida descendente</b>	Trama Ethernet que contiene la dirección MAC, determinada por la correspondencia NAT de la cabecera IP entrante en las direcciones IP locales, las cuales se convierten después a direcciones MAC mediante la función encaminamiento.

### 10.3.2 Flujo encaminado no traducido

Este tipo de flujo de paquetes transporta paquetes que requieren encaminamiento IPv4 sin NAT dentro del VTP/D. Como se describe en 9.4, existen tres formas de encapsular este flujo para la interfaz UR-2, a saber, PPPoA, PPPoE e IPoA. Ahora bien, en todos los casos el flujo recibe el mismo procesamiento de capa 3, como se describe en el cuadro 5.

**Cuadro 5/H.610 – Flujo encaminado no traducido**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	A los paquetes entrantes se les aplicará una función de encaminamiento. Cada conexión encaminada define una interfaz de encaminado distinta.
<b>Salida ascendente</b>	Paquetes encaminados cuya dirección de destino IP cumpla los criterios de encaminamiento de una determinada conexión encaminada no traducida.
	Si el VTP/D soporta la función de retransmisión IGMP (por ejemplo para habilitar la unión de secuencias de multidifusión Internet) está limitada a una de las conexiones encaminadas no traducidas, la salida podrá incluir mensajes IGMP con una dirección de clase D que no pertenece al dominio de servicios de medios de difusión (TV).
	Si se soporta el reenvío ascendente de PDU multidifusión IP y está limitado a una de las conexiones encaminadas no traducidas, la salida podrá contener unidades PDU multidifusión IP con dirección de destino de clase D que no pertenece al dominio de servicios de medios de difusión (TV).
<b>Entrada descendente</b>	Conexiones encaminadas no traducidas que transportan paquetes IP.
<b>Procesamiento funcional descendente</b>	Función de encaminamiento.
<b>Salida descendente</b>	Tramas Ethernet que contienen la dirección MAC que se resuelve mediante la función encaminamiento.

### 10.3.3 Función encaminamiento

El bloque encaminador soportará el encaminamiento estático, a saber, una tabla de encaminamiento que sólo se puede modificar mediante un canal de gestión.

El bloque encaminador soportará el encaminamiento dinámico, para lo cual utilizará el RIPv2 RFC 2453 [19].

### 10.3.4 DHCP

El bloque encaminador implementará un servidor DHCP RFC 2131 [3] para la red residencial.

La red residencial no debe contener otros servidores DHCP aparte del que figura en el VTP.

El servidor DHCP del VTP/D debe hacer caso omiso de los mensajes DHCPDISCOVER y DHCPREQUEST que transporten opciones de identificador de clase de usuario o identificador de clase de fabricantes (números 77 y 60 respectivamente) de la sintaxis descrita en 12.2.

## 10.4 Bloque puente

El bloque puente gestiona dos flujos de paquetes, el flujo puente y el flujo PPPoE. En la interfaz UR-2, el flujo puente utiliza las conexiones puente y el flujo PPPoE utiliza la conexión PPPoE. El bloque puente soportará al menos una conexión PPPoE y 4 conexiones puente.

### 10.4.1 Flujo puente

Este flujo transporta tramas que necesitan el puenteo IEEE 802.1D [4] dentro del bloque puente. Las tramas en sentido ascendente y descendente se reenvían de acuerdo con una tabla de direcciones MAC de puente de aprendizaje. Cada conexión puente define un puerto puente distinto. A continuación se describe cómo se procesa este flujo en el VTP/D.

**Cuadro 6/H.610 – Flujo de puente**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	Se aplicará a las tramas entrantes una función de puenteo, como se define en IEEE 802.1D. Sólo es obligatoria la funcionalidad puente de autoaprendizaje ([4] subcláusulas 7.7 – 7.9).
<b>Salida ascendente</b>	Tramas cuya dirección MAC de destino cumplan los criterios de puenteo de la VC de salida y tramas cuya dirección MAC de destino no corresponda a la dirección MAC del VTP (en la interfaz T <sub>CN</sub> ) y que no contengan un mensaje IGMP con dirección de clase D asignada al servicio de medios de difusión (TV) y que no transporte un PPPoE de tipo Ethernet (siempre que el filtro PPPoE esté activado).
<b>Entrada descendente</b>	Conexiones puente que transportan tramas Ethernet.
<b>Procesamiento funcional descendente</b>	Las tramas Ethernet válidas se puentean a la red residencial. No se permite el puenteo entre dos VC.
<b>Salida descendente</b>	Tramas Ethernet.

### 10.4.2 Flujo PPPoE

Este flujo transporta únicamente tramas PPPoE RFC 2516 [7]. Las tramas ascendentes que se reciben a través del punto de referencia T<sub>CN</sub> se filtran hacia una VC dedicada si y sólo si tienen uno de los tipos Ethernet PPPoE (0x8863 ó 0x8864).

**Cuadro 7/H.610 – Flujo PPPoE**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	Filtrado de tramas PPPoE.
<b>Salida ascendente</b>	Tramas que transportan PPPoE Ethertype (0x8863 ó 0x8864) y cuyas direcciones MAC de destino no es la dirección MAC del VTP.
<b>Entrada descendente</b>	La conexión PPPoE que transporta tramas Ethernet.
<b>Procesamiento funcional descendente</b>	Ninguno.
<b>Salida descendente</b>	Tramas Ethernet.

### 10.4.3 Filtrado

El bloque puente soportará el filtrado PPPoE. El filtro PPPoE se activará a distancia o estará preconfigurado (por ejemplo por el fabricante). En el caso de que se soporte ILMI, el filtro PPPoE se activará a distancia vinculando el flujo PPPoE a un PVC ATM (véase la cláusula 18).

## 10.5 Bloque difusión

El bloque difusión gestiona dos tipos de paquetes, el flujo de difusión y el flujo cambio de canal. En la interfaz UR-2 el flujo de difusión utiliza conexiones de difusión digital y el flujo de canal utiliza la conexión cambio de canal. El bloque difusión soportará una sola conexión de canal y al menos 4 conexiones difusión. La implementación del bloque difusión queda determinada por el método de entrega de difusión elegido, entrega por IP o por ATM. El cuadro 8 describe los aspectos de la implementación de los dos métodos de entrega de difusión posibles.

**Cuadro 8/H.610 – Compatibilidad de difusión**

Método de entrega	Encapsulado de secuencias de difusión	Protocolo cambio de canal entre el VTP/D y la AN	Posibles arquitecturas CPE	Repercusiones sobre el VTP
Basado en IP	MPEG/UDP/IP/Ethernet/AAL 5	IGMPv2	Distribuido	–
			Centralizado	–
Basado en ATM	MPEG/AAL 5	DSM-CC	Distribuido	El VTP convertirá IGMPv2 a DSM-CC. El VTP también adaptará MPEG/AAL 5 a MPEG/UDP/IP/Ethernet
			Centralizado	–

En el caso de que se implemente el modelo distribuido residencial, y que la entrega esté basada en ATM, el VTP realizará el reencapsulado IP, para lograr la conformidad con la pila de protocolo descrita en 9.6.1, en el punto de emisión de secuencias de la señal vídeo a la red residencial. La dirección de clase D que se utilizará se obtiene de la indicación BPID en la mensajería DSM-CC. Dado que el encapsulado UDP necesita un número de puerto UDP, éste será el 1970.

### 10.5.1 Flujo difusión

Es un flujo unidireccional que transporta todos los paquetes relacionados con el contenido de difusión (por ejemplo audio, vídeo) en el sentido descendente.

**Cuadro 9/H.610 – Flujo difusión**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	Bloqueo de todos los paquetes.
<b>Salida ascendente</b>	Ninguna.
<b>Entrada descendente</b>	Conexiones difusión que transportan TS MPEG-2.
<b>Procesamiento funcional descendente (en el VTP)</b>	<i>Entrega basada en ATM:</i> La cabida útil de una o varias tramas AAL 5 se encapsula como un único paquete multidifusión IP en una sola trama Ethernet.
	<i>Entrega basada en IP:</i> El único procesamiento obligatorio es la supresión de la cabecera LLC/SNAP.
<b>Salida descendente</b>	Tramas Ethernet que transportan paquetes multidifusión IP.

### 10.5.2 Flujo cambio de canal

El VTP/D implementará un 'servidor intermediario (proxy) de cambio de canal', a saber, una función de servidor IGMP (es decir un encaminador) hacia la interfaz T<sub>CN</sub> y una función cliente IGMP o DSM-CC hacia la interfaz U-R2.

**Cuadro 10/H.610 – Flujo cambio de canal**

<b>Entrada ascendente</b>	Tramas Ethernet.
<b>Procesamiento funcional ascendente</b>	Servidor intermediario de cambio de canal. Esta función acepta tramas que contienen mensajes IGMP con una dirección de clase D asignada al servicio de medios de difusión (TV). La función de servidor intermediario de cambio de canal genera los correspondientes mensajes de cambio de canal hacia la red de acceso. En el caso de una entrega ATM, se realiza la conversión del protocolo IGMP al DSM-CC.
<b>Salida ascendente</b>	<b>Entrega basada en ATM:</b> mensajes DSM-CC.
	<b>Entrega basada en IP:</b> mensajes IGMPv2.
<b>Entrada descendente</b>	PDU recibidas por la conexión cambio de canal.
<b>Procesamiento funcional descendente (en el VTP)</b>	<b>Entrega basada en ATM:</b> máquina de estados del servidor intermediario de cambio de canal (cliente DSM-CC y encaminador IGMP).
	<b>Entrega basada en IP:</b> máquina de estados del servidor intermediario IGMPv2.
<b>Salida descendente</b>	Tramas Ethernet que contienen consultas IGMP.

### 10.6 Bloque de voz

Este bloque funcional es obligatorio si se desea soportar el servicio VoATM. El bloque de voz gestiona el flujo BLES que transporta PDU de voz por ATM (es decir células AAL 2), como se describe en el cuadro 11. El bloque de voz soportará al menos una conexión BLES.

**Cuadro 11/H.610 – Flujo BLES**

<b>Entrada ascendente</b>	Señal de voz analógica
<b>Procesamiento funcional ascendente</b>	Generación de flujo BLES.
<b>Salida ascendente</b>	Células AAL 2 que transportan señales telefónicas.
<b>Entrada descendente</b>	Células AAL 2 que transportan señales telefónicas.
<b>Procesamiento funcional descendente</b>	Terminación del flujo BLES.
<b>Salida descendente</b>	Señal de voz analógica.

### 10.7 Bloque gestión

El bloque gestión se encarga del flujo de gestión remota del VTP/D que permite gestionar la configuración del VTP/D. Este bloque se encarga además de la gestión local del VTP.

El bloque de gestión soportará las funciones descritas en la cláusula 18.

### 10.7.1 Configuración IP

El VTP/D implementará un cliente DHCP RFC 2131 [3] que permita la configuración dinámica de los parámetros IP de la interfaz de gestión. El VTP/D soportará las opciones DHCP 66 (nombre de servidor TFTP) y 67 (nombre Bootfile) descritas en RFC 2132 [27], que permiten la extracción de ubicaciones y nombres de ficheros que contienen información de configuración específicas del VTP/D (además de la posibilidad de recibir estos parámetros en los campos 'sname' y 'file').

### 10.7.2 Descarga de ficheros remota

El VTP/D implementará un cliente TFTP, como se define en RFC 1350 [20]. Esta capacidad permite la actualización de programas informáticos/configuración del fabricante y descarga de ficheros de configuración al VTP/D.

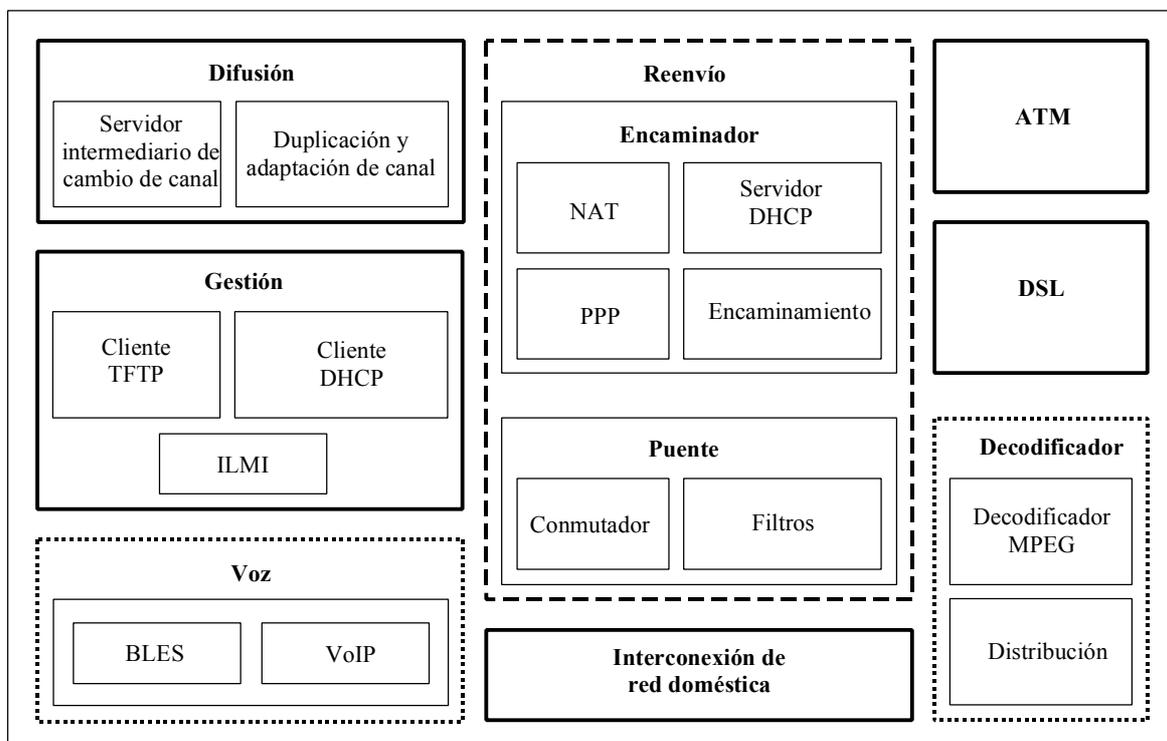
### 10.8 Bloque interconexión de red doméstica

El bloque interconexión de red doméstica realiza la función de adaptación entre la interfaz T<sub>CN</sub> y la red residencial física.

## 11 Implementación VTP/D básica

En esta cláusula se describe la implementación de un VTP/D básico. Esta implementación consiste en una solución multiservicios que proporciona servicios de TV de difusión, VoD, acceso a Internet y, como opción, servicios locales.

En la figura 27 se muestran los bloques funcionales VTP/D necesarios para la implementación del VTP/D básico. Los bloques obligatorios están marcados con una línea continua y los opcionales con una línea de puntos. Las líneas discontinuas indican que es obligatorio implementar al menos uno de los bloques que contiene. El bloque *decodificador* sólo es obligatorio para los VTP/D que gestionan la decodificación MPEG y la distribución de contenidos A/V decodificados a diferentes TV.



H.610\_F27

Figura 27/H.610 – Bloques funcionales VTP

El bloque reenvío está formado por el bloque encaminador y el bloque puente. El VTP/D de base implementará al menos uno de estos bloques. Cuando se implementa el bloque encaminador se considera que el VTP/D es un dispositivo de capa 3, mientras que cuando se implementa el bloque puente se le considera como un dispositivo de capa 2. Es posible que la implementación del VTP/D de base tenga ambos bloques, en cuyo caso se le considerará como un dispositivo híbrido.

## **12 Configuración IP de los CPE**

Se prevé que la mayoría de las instalaciones constarán de una sola subred IP de la red residencial y una sola ruta externa (traducida o no). Estos escenarios se denominan escenarios estándar.

Sin embargo, esta especificación de la funcionalidad de procesamiento IP también permite una gran variedad de escenarios de interconexión de red IP. Cuando los escenarios tengan más de una subred IP en la red residencial y/o más de una ruta saliente, se denominan escenarios avanzados.

Es posible lograr la configuración completamente automática de escenarios estándar y avanzados mediante la utilización de valores por defecto y/o protocolos de configuración normalizados, por ejemplo, DHCP y PPP, no siendo necesaria configuración de gestión alguna. Ahora bien, son posibles otras configuraciones mediante la utilización de gestión distante y/o interfaces de gestión local que permiten la configuración explícita de los parámetros de interconexión de red IP.

El soporte de escenarios estándar es obligatorio. El soporte de escenarios avanzados es opcional. En el apéndice IV se describen los escenarios avanzados.

En esta cláusula se supone que la implementación del VTP/D contiene un bloque encaminador. En esta cláusula se utiliza el término PPP para referirse a PPPoA o PPPoE.

### **12.1 Escenarios estándar de procesamiento IP**

Gracias al procesamiento IP en el VTP/D la red residencial puede funcionar como una subred IP. En esta subred, el VTP/D actúa como la pasarela por defecto de la subred IP y además proporciona la función de servidor DHCP, el cual atribuye direcciones IP y otra información de configuración de cliente IP al cliente IP en los FPD.

El VTP/D soporta automáticamente varios mecanismos de direccionamiento diferentes de la subred IP, que será uno de los siguientes escenarios:

- Un espacio exclusivo de direcciones privadas de la red residencial, por ejemplo, 192.168.0.0.
- Una subred de un espacio de direcciones encaminables externamente. La red residencial puede ser una subred de:
  - La Internet pública que utiliza una subred del espacio de direcciones públicas (registrado a nivel mundial).
  - Una red privada más grande que utiliza espacio de direcciones privadas, por ejemplo, espacio de direcciones privadas 10.0.0.0.

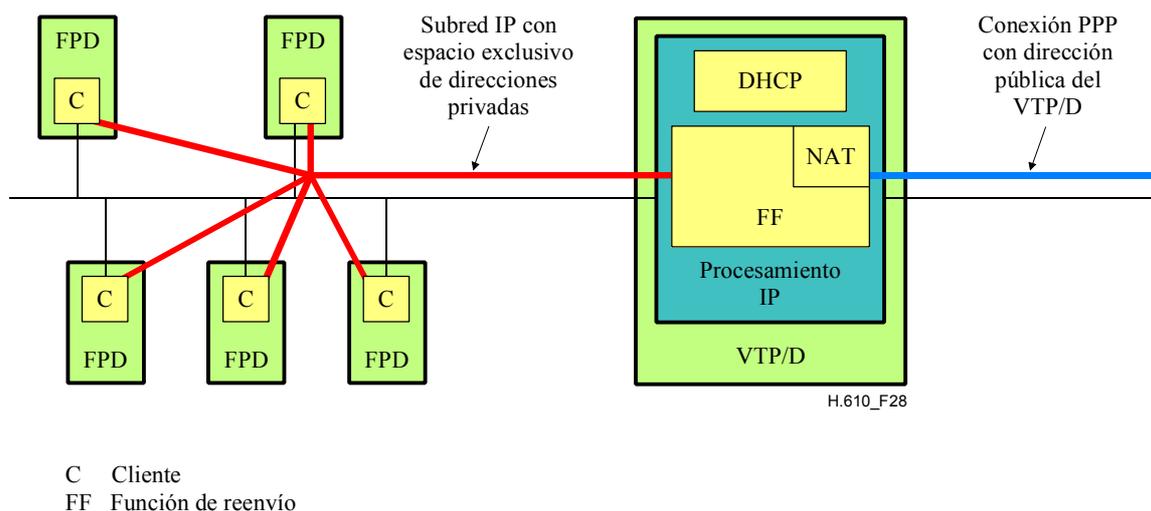
La interconexión de red IP dentro de la subred IP de la red doméstica se logra mediante capacidades de capa MAC Ethernet, en las que se realiza la correspondencia de direcciones IP en direcciones MAC mediante un ARP utilizado de manera usual.

La interconexión más allá de esta subred IP se logra utilizando una función de reenvío IP en el VTP/D, que mantiene rutas de reenvío. Éstas son las reglas que utiliza la función de reenvío IP para decidir hacia dónde enviar los paquetes IP. En el caso de un escenario estándar, es decir con una sola subred IP y un sola ruta saliente, la función de reenvío es la solución trivial que se basa en una sola ruta por defecto. Si la subred IP utiliza un espacio exclusivo de direcciones privadas, los paquetes se pasan a través de la función NAT/PAT dentro de la función de reenvío IP.

La subred IP en la red residencial puede ser de dos tipos, en función del espacio de direcciones utilizado. En el primer tipo se utiliza un espacio exclusivo de direcciones privadas. En el segundo la subred IP es una subred de un espacio de direcciones más amplio, que puede ser privado o público.

### 12.1.1 Configuración por defecto del espacio exclusivo de direcciones privadas

La configuración de este escenario estándar se muestra en la figura 28. La red residencial utiliza un espacio exclusivo de direcciones privadas (cuyo valor por defecto es 192.168.0.0/24) y dado que esta gama de direcciones se conoce independientemente de la conexión a la red más amplia, es posible configurar los parámetros de subred IP y los parámetros del servidor DHCP antes de que se cree o se configure la conexión a la red.



**Figura 28/H.610 – Escenario de procesamiento IP estándar con espacio exclusivo de direcciones privadas**

#### 12.1.1.1 Secuencia de acciones de configuración por defecto

Esta secuencia de acciones de configuración por defecto se pone en marcha automáticamente al encender el VTP/D. La secuencia es la siguiente:

- Se configura la interfaz de red residencial VTP/D, el servidor DHCP y otros parámetros de procesamiento IP con los parámetros de la subred IP por defecto con el direccionamiento privado exclusivo que se describe a continuación.
- Suponiendo que la conexión es una conexión de ruta traducida, se inicia una sesión PPP sobre la VC ATM con los parámetros PPP por defecto que se describen a continuación.
- Se utiliza como dirección del VTP/D la dirección atribuida a la PPP correspondiente a la subred IP. La conexión PPP se configura con una interfaz de capa 2 de la ruta por defecto de la función reenvío. La función NAT/PAT se crea dentro de la función de reenvío IP como parte de su ruta por defecto y se configura con los parámetros por defecto descritos a continuación.

#### 12.1.1.2 Configuración por defecto de la subred IP del servidor DHCP

La configuración por defecto es que la subred IP en la red residencial utilice la gama de direcciones privadas 192.168.0.0/24.

Los parámetros que definen la subred de direcciones privadas residencial figuran en el cuadro 12 junto con sus valores por defecto y/o calculados. La tercera columna indica otros posibles métodos de configuración para ese parámetro.

El cuadro 13 define los parámetros del servidor DHCP para los computadores centrales (hosts) de configuración dentro de la subred.

**Cuadro 12/H.610 – Parámetros de subred por defecto para una subred IP con espacio exclusivo de direcciones privadas**

Parámetro	Valor por defecto	Otra posible configuración
Máscara de subred (m.m.m.m)	Estático – 255.255.255.0	Valor estático a través de la interfaz de gestión
Dirección de subred (x.x.x.x)	Estático – 192.168.0.0	Valor estático a través de la interfaz de gestión
Pasarela por defecto	Calculado – 192.168.0.1	No – se calcula mediante x.x.x.x y m.m.m.m + 0.0.0.1
Dirección de difusión	Calculado – 192.168.0.255	No – se calcula mediante x.x.x.x y m.m.m.m + no m.m.m.m
Dirección del servidor DNS primario	Calculado – Extensión IPCP RFC 1332 de acuerdo con la RFC 1877 del nodo de servicio (véase parámetro PPP <i>infra</i> )	Valor estático a través de la interfaz de gestión o bien el VTP puede implementar una función de retransmisión y/o de almacenamiento en caché DNS
Dirección de servidor DNS secundario	Calculado – Extensión IPCP de acuerdo con RFC 1877 del nodo de servicio (véase parámetro PPP <i>infra</i> )	Valor estático a través de la interfaz de gestión
Resolución de direcciones dentro de la subred	ARP	–
Dirección del VTP/D dentro de la subred	192.168.0.1	No – se calcula mediante x.x.x.x y m.m.m.m + 0.0.0.1

**Cuadro 13/H.610 – Parámetros del servidor DHCP por defecto para una subred IP con espacio exclusivo de direcciones privadas**

Parámetro	Valor por defecto	Otra posible configuración
Máscara de subred	Copiado de los parámetros de subred	No
Gama de atribución de direcciones	Estático – 192.168.0.16 a 192.168.0.239	Valores estáticos a través de la interfaz de gestión
Pasarela por defecto	Copiado de los parámetros de subred	No
Dirección de difusión	Copiado de los parámetros de subred	No
Dirección de servidor DNS primario	Copiado de los parámetros de subred	No
Dirección de servidor DNS secundario	Copiado de los parámetros de subred	No

### 12.1.1.3 Configuración de la conexión externa por defecto

Los parámetros por defecto que figuran en el cuadro 14 se utilizan para configurar la conexión externa a la subred IP y para negociar los parámetros con el encaminador de borde en la red.

**Cuadro 14/H.610 – Parámetros por defecto de la conexión externa a la subred IP con espacio exclusivo de direcciones privadas**

Parámetro	Valor por defecto	Otra posible configuración
Encapsulado	PPP	No
Velocidad de mantenimiento de la conexión de LCP	Estático – 1 minuto	Valor estático a través de la interfaz de gestión
Autenticación	PAP RFC 1334	CHAP RFC 1994
Dirección del VTP IPCP facilitada por el VTP	0.0.0.0	Configuración estática utilizando la interfaz de gestión
Dirección del VTP IPCP facilitada por el nodo de servicio	Acepta dirección x.x.x.x facilitada	Ignora dirección
Dirección del nodo de servicio IPCP facilitada por el nodo de servicio	Hace caso omiso de la dirección (el enlace PPP es la ruta por defecto)	No
Dirección del nodo de servicio IPCP facilitada por el VTP	No facilita dirección alguna	No
Dirección del servidor DNS primario IPCP facilitada por el nodo de servicio	Acepta dirección x.x.x.x facilitada	Hace caso omiso de la dirección
Dirección del servidor DNS secundario IPCP facilitada por el nodo de servicio	Acepta dirección x.x.x.x facilitada	Hace caso omiso de la dirección

### 12.1.1.4 Configuración por defecto de la función reenvío IP

Las rutas en la función de reenvío IP son las correspondientes a la función de reenvío trivial. Las rutas principales salientes son la red residencial y la conexión externa, que es la ruta por defecto. Esta ruta por defecto también incluye la función NAT/PAT. Además de estas rutas, el VTP/D debe implementar una ruta en bucle. Las rutas por defecto se muestran en el cuadro 15. Los parámetros por defecto de la función NAT/PAT figuran en el cuadro 16.

**Cuadro 15/H.610 – Parámetros por defecto de la función de reenvío IP de una subred IP con espacio exclusivo de direcciones privadas**

Gama de direcciones de destino		Enmascarado	Interfaz de capa 2 saliente
Dirección de destino	Máscara de subred		
x.x.x.x (calculada a partir de los parámetros de subred)	s.s.s.s (calculada a partir de los parámetros de subred)	No	Interfaz de la red residencial, por ejemplo, eth0
127.0.0.0	255.0.0.0	No	VTP/D – ruta en bucle
Ruta por defecto		Sí	Conexión externa, por ejemplo, ppp0

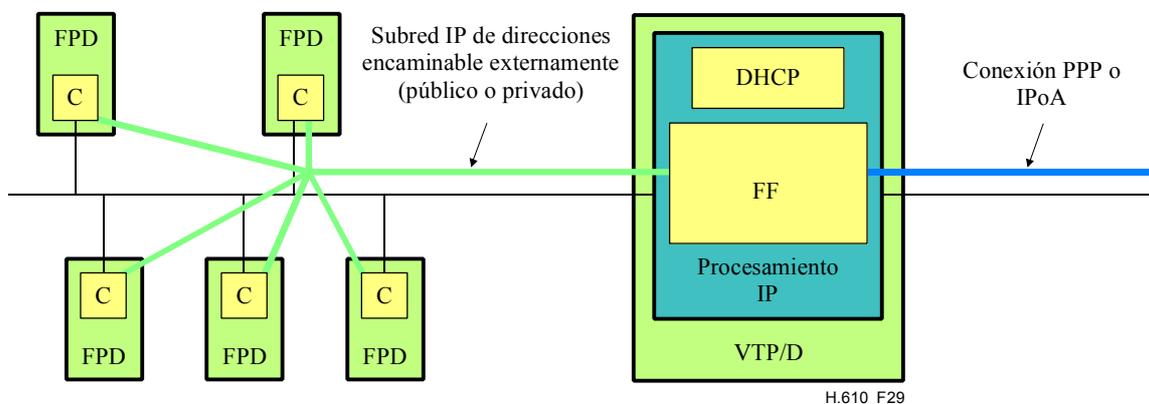
**Cuadro 16/H.610 – Parámetros NAT/PAT por defecto de una subred con espacio exclusivo de direcciones privadas**

Parámetro	Valor por defecto	Otra posible configuración
Valores del puerto abierto en sentido ascendente	Todos los puertos abiertos	Todos los puertos cerrados excepto aquellos abiertos por la configuración estática mediante la interfaz de gestión local o distante, mediante un protocolo dinámico, por ejemplo, UPnP, o por una solución específica del fabricante.
Correspondencia del puerto en direcciones locales, en sentido descendente	Ninguna correspondencia de ningún valor del puerto	Correspondencia de un valor de puerto a una dirección IP privada de la red residencial mediante una correspondencia configurada estadísticamente a través de una interfaz de gestión local o remota, mediante un protocolo dinámico, por ejemplo, UPnP, o mediante una solución específica del fabricante.
Retransmisión del protocolo de aplicación NAT	FTP, ICMP	El fabricante puede añadir otras configuraciones y/o se pueden configurar dinámicamente mediante, por ejemplo, UPnP.

### 12.1.2 Configuración por defecto del escenario estándar con espacio de direcciones encaminable externamente

La configuración de este escenario estándar se muestra en la figura 29. En este escenario estándar, la red asigna la gama de direcciones por defecto mediante un encaminador de borde, utilizando para ello PPP o DHCP. (Obsérvese que la transacción DHCP tiene lugar entre el VTP/D como cliente DHCP y el encaminador de borde como servidor DHCP.)

Como la gama de direcciones no se conoce hasta que no se haya establecido la conexión externa, la creación y configuración de la subred IP se producirá después del establecimiento de la conexión externa.



C Cliente  
FF Función de reenvío

**Figura 29/H.610 – Escenarios de procesamiento IP estándar con espacio de direcciones encaminable externamente**

### 12.1.2.1 Secuencia de acciones para la configuración por defecto

El VTP/D inicia la configuración por defecto después del establecimiento de una conexión encaminada no traducida externa.

Si la conexión encaminada no traducida utiliza PPP, la secuencia es la siguiente:

- Se inicia una sesión PPP por esta conexión, de modo que los parámetros PPP sean los parámetros por defecto que se describen a continuación.
- Se configura la interfaz de red residencial VTP/D, el servidor DHCP y otros parámetros de procesamiento IP con los valores de los parámetros de la subred IP por defecto como se describe a continuación (que se obtienen de la negociación IPCP).
- Se configura la conexión PPP como una interfaz de capa 2 de la ruta por defecto de la función reenvío.

Si la conexión encaminada no traducida es IPoA, la secuencia de acciones es la siguiente:

- Se inicia una detección DHCP a través de la conexión IPoA.
- Se configura la interfaz de red residencial VTP/D, el servidor DHCP, y otros parámetros de procesamiento IP con los parámetros de la subred IP por defecto como se describe a continuación (que se obtienen de la negociación DHCP).
- Se configura la conexión IPoA como una interfaz de capa 2 de la ruta por defecto de la función reenvío.

### 12.1.2.2 Configuración por defecto de la conexión externa

Si la conexión externa a la subred IP utiliza PPP, los parámetros por defecto se muestran en el cuadro 17; si, por el contrario, la conexión externa utiliza IPoA los parámetros por defecto figuran en el cuadro 18. Estos parámetros se utilizan para configurar la conexión externa y para la negociación con el encaminador de borde.

**Cuadro 17/H.610 – Parámetros por defecto de la conexión PPPoA externa a una subred IP con espacio de direcciones encaminables externamente**

Parámetro	Valor por defecto	Otra posible configuración
Encapsulado	PPP	No
Velocidad LCP activa RFC 1661	Estático – 1 minuto	Valor estático a través de la interfaz de gestión
Autenticación	PAP	CHAP
Dirección VTP IPCP facilitada por el VTP	0.0.0.0	Configuración estática mediante la interfaz de gestión
Dirección VTP IPCP facilitada por el nodo de servicio	Acepta la dirección x.x.x.x facilitada	Hace caso omiso de la dirección
Dirección del nodo de servicio IPCP facilitada por el nodo de servicio	Hace caso omiso de la dirección (el enlace PPP es la ruta por defecto)	No
Dirección del nodo de servicio IPCP facilitada por el VTP	No facilita la dirección	No
Dirección del servidor DNS primario IPCP facilitada por el nodo de servicio	Acepta la dirección x.x.x.x facilitada	Hace caso omiso de la dirección
Dirección del servidor DNS secundario IPCP facilitada por el nodo de servicio	Acepta la dirección x.x.x.x facilitada	Hace caso omiso de la dirección

**Cuadro 18/H.610 – Parámetros por defecto de la conexión IPoA externa a la subred IP con espacio de direcciones encaminable externamente**

Parámetro	Valor por defecto	Reconfiguración
Encapsulado	IPoA (modo de encaminamiento RFC 2684 con LLC/SNAP)	No
Protocolo de configuración	DHCP	Ninguna – es decir protocolo de configuración
Protocolo de encaminamiento	Ninguno	Habilitación del RIPv2 opcional

### 12.1.2.3 Configuración por defecto de la subred IP y del servidor DHCP

El valor por defecto de esta gama de direcciones se obtiene a partir de los parámetros negociados con el encaminador de borde por la conexión externa.

Cuando la conexión externa utiliza PPP, la obtención por defecto de las gamas de direcciones cumple las siguientes reglas.

- Cuando la componente IPCP del PPP pueda atribuir una máscara de subred, ésta se debe utilizar para la subred.
- Si el IPCP no atribuye una máscara de subred, la subred debe suponer una máscara de subred igual a 255.255.255.248.

NOTA – Esto exige que el encaminador de borde y los servidores RADIUS también conozcan este convenio y que están configurados en consecuencia.

Cuando la conexión externa utiliza IPoA, la obtención por defecto de la gama de direcciones cumple la siguiente regla:

- La subred IP debe utilizar la dirección IP y la máscara de subred atribuida por DHCP.

En el cuadro 19 se muestran los parámetros que definen la subred IP junto con sus valores por defecto y/o derivados. La tercera columna especifica otros métodos de configuración posibles para este parámetro. El cuadro 20 define los parámetros del servidor DHCP en el VTP/D correspondiente a la subred IP.

**Cuadro 19/H.610 – Parámetros por defecto de la subred IP con espacio de direcciones encaminable externamente**

Parámetro	Valor por defecto	Otra posible configuración
Máscara de subred (m.m.m.m)	Obtenido a partir de los parámetros de configuración de una conexión externa o valor por defecto estático (255.255.255.248) – véase <i>supra</i>	Valor estático mediante la interfaz de gestión
Dirección de subred (x.x.x.x)	Obtenido a partir de los parámetros de configuración de una conexión externa – x.x.x.x y m.m.m.m	Valor estático mediante la interfaz de gestión
Pasarela por defecto	Obtenido – x.x.x.x y m.m.m.m + 0.0.0.1	No
Dirección de difusión	Obtenido – x.x.x.x y m.m.m.m + no m.m.m.m	No

**Cuadro 19/H.610 – Parámetros por defecto de la subred IP  
con espacio de direcciones encaminable externamente**

<b>Parámetro</b>	<b>Valor por defecto</b>	<b>Otra posible configuración</b>
Dirección del servidor DNS primario	Obtenido a partir de los parámetros de configuración de la conexión externa	Valor estático mediante la interfaz de gestión o bien el VTP puede implementar una función de retransmisión y/o almacenamiento en caché DNS
Dirección del servidor DNS secundario	Obtenido a partir de los parámetros de configuración de la conexión externa	Valor estático mediante la interfaz de gestión
Resolución de direcciones dentro de la subred	ARP	–
Dirección VTP	Obtenido – x.x.x.x y m.m.m.m + 0.0.0.1	No

**Cuadro 20/H.610 – Parámetros por defecto del servidor DHCP de la subred IP  
con espacio de direcciones encaminable externamente**

<b>Parámetro</b>	<b>Valor por defecto</b>	<b>Reconfiguración</b>
Máscara de subred (m.m.m.m)	Copiado de los parámetros de subred	No
Gama atribución de direcciones	Obtenido – la gama máxima estaría entre x.x.x.x y m.m.m.m + 0.0.0.2 a x.x.x.x y m.m.m.m + no m.m.m.m – 0.0.0.1	Valores estáticos a través de la interfaz gestión
Pasarela por defecto	Copiado de los parámetros de subred	No
Dirección de difusión	Copiado de los parámetros de subred	No
Dirección de servidor DNS primario	Copiado de los parámetros de subred	No
Dirección de servidor DNS secundario	Copiado de los parámetros de subred	No

#### **12.1.2.4 Configuración por defecto de la función de reenvío IP**

Las rutas en la función de reenvío IP son las de una función de reenvío trivial. Las rutas salientes principales son la red residencial y la conexión externa, siendo esta última la ruta por defecto. Además de estas rutas, el VTP/D debe implementar una ruta en bucle. En el cuadro 21 se muestran las rutas por defecto.

**Cuadro 21/H.610 – Parámetros por defecto de la función reenvío IP para una subred IP con espacio de direcciones encaminable externamente**

Gama de direcciones de destino		Enmascaramiento	Interfaz de capa 2 saliente
Dirección de destino	Máscara de subred		
x.x.x.x (obtenida a partir de los parámetros de subred)	s.s.s.s (obtenida a partir de los parámetros de subred)	No	Interfaz de red residencial, por ejemplo, eth0
127.0.0.0	255.0.0.0	No	Ruta en bucle – VTP/D
Ruta por defecto		No	Conexión externa, por ejemplo, ppp0 o ipoa0

## 12.2 DHCP

Los mensajes DHCPDISCOVER y DHCPREQUEST, enviados por terminales conformes FS-VDSL incluirán una opción de identificador de clase de fabricante (subcláusula 9.13 de IETF RFC 2132 [27]) que especifica el tipo de terminal. El valor de esta opción se interpretará como una cadena de caracteres UTF-8 IETF RFC 2279 [24] con el formato de 4 campos siguiente.

**<FSVDSL><Tipo de servicio><ID del fabricante><Número de modelo>**

- **<FSVDSL>** es la cadena de seis caracteres constante "FSVDSL" seguido del carácter punto ('.').
- **<Tipo de servicio>** es una cadena de longitud variable que indica el servicio que soporta el terminal. Este campo contendrá un solo carácter punto que estará al final de la cadena.
- **<ID del fabricante>** es una cadena de longitud variable que identifica unívocamente al fabricante. Se recomienda que este campo se codifique como el OUI identificador único de organización atribuido al fabricante por el IEEE. Este campo contendrá un solo carácter punto, que será el último. En el apéndice X se indica el procedimiento vigente para obtener un OUI de IEEE.
- **<Número de modelo>** es una cadena de longitud variable que identifica unívocamente el tipo de terminal de entre todos los modelos del fabricante. Los números de modelo los atribuirá y publicará el fabricante de terminal.

Cuando el terminal no utilice la opción de identificador de clase de fabricante, se utilizará en su lugar la opción clase de usuario IETF RFC 3004 [28], con la misma sintaxis definida antes. Esta opción también se utilizará cuando el terminal tenga que indicar múltiples tipos de servicio.

El servidor DHCP en la red debe estar configurado de manera que sólo responda a mensajes DHCP cuya identificación tenga una sintaxis válida, como se describe a continuación. De lo contrario, el servidor DHCP debe descartar el mensaje y no responder al mismo. De esta manera es posible, por ejemplo, configurar el servidor DHCP para responder a terminales que solicitan parámetros IP de un determinado servicio o a terminales de un determinado fabricante o modelo.

El servidor DHCP en el VTP/D debe hacer caso omiso de los mensajes DHCPDISCOVER y DHCPREQUEST que transporten opciones de identificador de clase de usuario o identificador de clase de fabricante de la sintaxis anterior, a fin de permitir controlar el direccionamiento IP para servicios avanzados desde la red (es decir, el operador de servicio).

A continuación se definen los tipos de servicios básicos para la utilización de terminales FS-VDSL (aunque es posible utilizar otros tipos):

- "VOICE" – para servicios de voz derivados.
- "VIDEO" – para servicios de difusión digital y VoD.

- "DATA" – para servicios de datos únicamente.

### **13 Servicio de datos**

El servicio de datos se proporcionará mediante una o varias de las siguientes conexiones:

- Conexión puente, según se describe en 9.1 correspondiente al flujo puente, descrito en 10.4.1.
- Conexión PPPoE, como se describe en 9.2, correspondiente con el flujo PPPoE, descrito en 10.4.2.
- Conexión de ruta no traducida, como se describe en 9.4 correspondiente al flujo encaminado no traducido, descrito en 10.3.2.
- Conexión de ruta traducida, como se describe en 9.3, correspondiente al flujo de encaminamiento traducido, descrito en 10.3.1.

La respectiva configuración IP será conforme con la cláusula 12.

### **14 Servicio de difusión**

En esta cláusula se describe la especificación técnica para la entrega de TV de difusión y otros servicios de difusión, por ejemplo difusión de radio, por la red FS-VDSL. Por TV de difusión se entiende el acceso por parte del usuario secuencias a emisiones vídeo que se ofrecen en una programación de difusión. Se prevé que la experiencia del usuario en lo tocante a TV de difusión FS-VDSL sea similar a la del servicio ofrecido vía satélite o por un operador de cable.

#### **14.1 Opciones de entrega**

El contenido A/V se encapsulará en MPEG2-TS independientemente de la técnica de codificación utilizada (por ejemplo, MPEG-2, MPEG-4).

Antes de la transmisión de contenido A/V por el punto de referencia V, se realizará el encapsulado adecuado. Hay dos posibles opciones de entrega, "entrega ATM" y "entrega IP", como se describe en 10.5. La elección de una u otra opción de entrega determina el encapsulado MPEG2-TS y el protocolo de cambio de canal del VTP/D a la AN.

En las dos opciones es obligatorio que el contenido A/V se transmita en una SPTS. El transporte de contenido A/V en la AN será el mismo independientemente de la opción de encapsulado elegida.

Los métodos de encapsulado son independientes de la PCR.

##### **14.1.1 Entrega ATM**

La entrega ATM de flujo de transporte MPEG-2 se encapsulará como se describe en 9.6.2 y el protocolo de cambio de canal será DSM-CC.

En el lanzamiento de servicios DBTV en el extremo de cabecera, el encapsulado será de dos paquetes de flujo de transporte MPEG por PDU AAL 5 en el punto de referencia V.

##### **14.1.2 Entrega IP**

En la entrega IP el flujo de transporte MPEG-2 se encapsulará como se describe en 9.6.1 y el protocolo de cambio de canal será IGMPv2.

En el lanzamiento de servicios DBTV en el extremo de cabecera, el encapsulado será de siete paquetes de flujo de transporte MPEG por paquete IP en una PDU AAL 5 cuando se utiliza MPEG-2/IP/ATM en el punto de referencia V.

## **14.2 Plan de direccionamiento IP de TV de difusión**

En el caso de entrega IP, cada flujo de difusión que se recibe en el punto de referencia V tendrá una única dirección de destino IP de clase D.

En el caso de entrega ATM y un entorno residencial distribuido, el encapsulado multidifusión IP se realiza sólo en el VTP. La asignación de direcciones IP de clase D en este caso se describe en 10.5 y 14.4.1.

La subred IP de clase D por defecto atribuida a la emisión de flujo de difusión será 239.192.0.0/14.

## **14.3 Transporte**

### **14.3.1 Duplicación de canales y transconexión ATM**

La OLT duplicará los flujos de difusión entrantes (canales), y la ONTU podrá replicar, para todos los usuarios que accedan simultáneamente al mismo canal, de modo que la AN reciba una sola vez cada canal de difusión. La duplicación de canales se realiza utilizando una conexión punto a multipunto ATM distinta para cada canal. La petición de cambio de canal por un usuario causa la transconexión del enlace VC del lado usuario con la raíz punto a multipunto adecuada.

### **14.3.2 Criptación**

La AN y la red residencial funcionarán de manera transparente a la implementación de acceso condicional basado en la criptación.

### **14.3.3 Canal administrativo**

El canal administrativo incluye toda la mensajería y los flujos de datos entre el FPD y la plataforma de gestión del servicio de difusión. La mensajería administrativa puede consistir en archivos de arranque STB, actualización de soporte lógico, datos de guía de programación electrónica, etc. Este canal administrativo utilizará una conexión puente, una PPPoE o una conexión encaminada o no traducida.

### **14.3.4 Objetivos de desempeño de la calidad del servicio DBTV**

Para proporcionar la capacidad de recuperación de errores necesaria para la entrega fiable de contenido MPEG-2 a velocidad muy alta, en la arquitectura propuesta DBTV FS-VDSL se supone que se garantiza la entrega de paquetes, el orden secuencial de paquetes correcto, y que están limitadas la variación del retardo de paquetes y la fluctuación de fase de la referencia de reloj de programa. El diseño de red de la red principal y de la AN tendrá en cuenta estas restricciones.

Si bien la medición de la variación del retardo de célula (CDV, *cell delay variation*) es adecuada para medir la calidad de funcionamiento de fluctuación de la red de acceso ATM, es mucho más importante controlar el valor de la fluctuación de la referencia de reloj de programa en la entrega de servicios vídeo transportados dentro de flujos de transporte MPEG-2. La CDV contribuye a la fluctuación de la referencia de reloj de programa del servicio entregado, como se indica a continuación. En la cláusula 5.3.2 y en el anexo I de ETSI TR 101 290 figuran una definición detallada de la fluctuación de la referencia de reloj de programa y técnicas de medición de esa fluctuación.

#### **14.3.4.1 Extremo de cabecera**

El extremo de cabecera (junto con la contribución de toda red principal que intervenga) no causará una variación de más de 5 ms en la fluctuación de la referencia de reloj de programa en la entrega de paquetes SPTS MPEG, medida en el punto de referencia V.

#### **14.3.4.2 Red de acceso (AN)**

La configuración y dimensionamiento de la AN entre el punto de referencia V y la interfaz U-R2 soportará una variación de retardo de célula de cresta a cresta inferior a 2 ms, como se define en

ATM Forum Specification af-tm-0056.000. La suma de la tasa de errores en las células y la tasa de células perdidas será inferior a  $10^{-8}$ .

#### **14.3.4.3 VTP y red residencial**

La red residencial no causará una fluctuación de referencia de reloj de programa mayor que 5 ms en la entrega de paquetes SPTS MPEG. Es tanto conveniente como posible que el VTP/D suprima la 'fluctuación posicional' que se produce al ubicar la referencia de reloj de programa en la trama IP o en la célula ATM, para lo cual se utiliza la velocidad de bit media del flujo y la posición de la referencia de reloj de programa que transporta el paquete de flujo de transporte MPEG.

NOTA – La 'fluctuación posicional' de la referencia de reloj de programa aumenta al disminuir la velocidad de bits del flujo (que permiten MPEG-4 y otras compresiones de marca).

#### **14.3.4.4 FPD**

El FPD tolerará una fluctuación de la referencia de reloj de programa de al menos 12 ms. En la relación de  $10^{-8}$  indicada en 14.3.4.2 se supone que la FPD contiene algún tipo de recuperación de errores. Los resultados dependen de lo "sofisticado" que sea el decodificador MPEG-2 en el FPD. Para facilitar la cancelación de errores que puede haber en el FPD, los paquetes con errores deben pasarse por el decodificador MPEG-2 y marcarse como tales.

### **14.4 Señalización cambio de canal**

#### **14.4.1 Uso de IGMPv2 y DSM-CC para el control del cambio de canal**

La utilización de la entrega ATM en el caso del modelo residencial distribuido exige una traducción IGMPv2 a DSM-CC en el VTP. Esta traducción implica que el VTP implementa máquinas de estado IGMP y DSM-CC, y que las direcciones de clase D se convierten a BPID (ID de programa de difusión utilizados en la señalización CCP DSM-CC). La utilización de planes de numeración idénticos para las direcciones clase D y los BPID hacen innecesaria la traducción calculada. Para mayor información sobre la traducción de IGMPv2 a DSM-CC véase apéndice II.

#### **14.4.2 IGMPv2 de extremo a extremo para el control del cambio de canal de difusión**

El protocolo IGMP no fue creado en un principio para utilizarlo como protocolo de cambio de canal, y algunos de los valores por defecto de temporizadores, etc. podrían ser inaceptables para esta aplicación. En esta subcláusula se sugiere y se describe una serie de modificaciones de los valores por defecto y otros valores de temporizador por defecto para optimizar la calidad de funcionamiento.

En general, los tiempos de cambio de canal dependen de varios parámetros:

- *Procesamiento de instrucciones*  
El intervalo de tiempo entre la acción de control remoto y la transmisión del mensaje conexo.
- *Tiempo de transmisión de la red*  
El intervalo de tiempo entre la transmisión del mensaje conexo y la recepción del primer paquete multidifusión del canal solicitado.
- *Retardo de capa STB*  
El tiempo que necesita la pila IP del adaptador multimedios (STB, *set top box*) para procesar los paquetes entrantes y entregar el contenido al decodificador MPEG.
- *Retardo de la memoria intermedia de fluctuación STB*  
El tiempo que transcurre hasta que la memoria intermedia de fluctuación STB alcanza el máximo de su capacidad antes de reenviar la señal de vídeo a la función decodificador.

- *Retardo del decodificador MPEG*

El intervalo de tiempo correspondiente al proceso de decodificación.

En esta Recomendación, sólo se trata el tiempo de transmisión de la red, y se fija como objetivo que éste sea inferior a 500 ms.

La reducción de los parámetros del temporizador por defecto implica la aceleración del proceso que regula las operaciones de llegada a un canal y abandono de un canal, lo que resulta en la reducción del tiempo de cambio de canal. A continuación se indican los valores del temporizador recomendados.

En adelante, los mensajes de informe IGMPv2 no solicitados se denominarán *llegada* y los mensajes de desunión IGMPv2 se denominarán *abandono*.

### **Intervalo LastMemberQuery**

El intervalo *LastMemberQuery* es el tiempo máximo permitido que tarda el adaptador multimedia (STB) en responder a las solicitudes específicas de grupo que el VTP envía tras la recepción de un mensaje abandono. Dado que el tiempo necesario para eliminar un canal cuando no lo tiene sintonizado ningún STB es igual a tres veces el valor de *LastMemberQuery*, de modo que cuando más pequeño sea el valor más rápida sea la liberación de los recursos no utilizados.

Valor por defecto RFC 2236: 1 s

Valor recomendado: 100 ms

### **Número LastMemberQuery**

El *LastMemberCount* es el número de consultas específicas del grupo que se envía antes de que el VTP suponga que no hay miembros locales.

Valor por defecto del RFC 2236: 2

Valor recomendado: 1

### **Intervalo UnsolicitedReport**

Cuando un STB llega a un grupo multidifusión, debe inmediatamente transmitir un informe no solicitado de los miembros para ese grupo. Para contemplar la posibilidad de que el informe del miembro inicial no se pierda o se estropee, RFC 2236 recomienda que se repita una o dos veces con una diferencia breve (intervalo de informe no solicitado).

Valor por defecto RFC 2236: 10 s

Valor recomendado: 100 ms

Los FPD y los VTP deben soportar valores recomendados, e interfundionarán con los demás equipos utilizando estos valores. Ahora bien, la utilización de los valores recomendados no es obligatoria. Los parámetros para los que no se recomienda optimización alguna tendrán los valores por defecto indicados en RFC 2236.

#### **14.4.2.1 Requisitos del STB**

El STB implementará el procesamiento de computador principal RFC 2236, en particular cumplirá los siguientes requisitos adicionales:

- Cada vez que se abandona un canal el STB enviará un mensaje abandono.
- Durante un cambio de canal, el mensaje abandono siempre se enviará antes que el mensaje llegada, salvo cuando se reciban múltiples canales (por ejemplo, para imagen dentro de imagen).

- Durante un cambio de canal el STB enviará un mensaje llegada después de que haya pasado un tiempo *joinDelay* desde que se envió el mensaje abandono para garantizar que se mantiene el orden de los mensajes abandono y llegada cuando estos mensajes se envían del VTP/D a la AN.
- El valor de *joinDelay* debe ser configurable. El valor recomendado es 100 ms.
- El STB será capaz de responder a consultas específicas con un tiempo de respuesta máximo de 100 ms.
- El STB debe generar 2 (ó 3) informes no solicitados en el intervalo *UnsolicitedReport*.

#### 14.4.2.2 Requisitos del VTP

El VTP implementará el proceso consultor RFC 2236 en la interfaz de red residencial y retransmitirá peticiones IGMPv2 (mensajes llegada y abandono) a la red de acceso. Cuando se recibe un mensaje informe destinado a un canal que no tiene miembros, el VTP retransmitirá este mensaje a la OLT. El VTP enviará un solo mensaje abandono cada vez que se suprima un canal recibido de su lista de miembros de grupos multidifusión. El VTP también cumplirá las siguientes optimizaciones:

- El VTP debe ser capaz de generar consultas específicas con un tiempo de respuesta máximo de 100 ms.
- El VTP debe ser capaz de poner a 1 el *LastMemberQuery*.

#### 14.4.2.3 Requisitos de la AN

Tras recibir un mensaje llegada, la AN conectará el canal solicitado al puerto DSL adecuado y, al recibir un mensaje abandono lo desconectará.

Debido a los requisitos aplicables al VTP, no es necesario que la AN implemente el mecanismo "consulta específica" descrita en la cláusula 3 de RFC 2236. La AN implementará el mecanismo "consulta general" para recuperarse de mensajes abandono perdidos. Este último proceso podrá iniciarse periódicamente (de acuerdo con RFC 2236) o activarse por un determinado evento.

#### 14.4.3 Direcciones fuente IP utilizadas en mensajes IGMP

La dirección destino IP de los paquetes IP que transportan mensajes IGMP es una dirección multidifusión, que indica el grupo al que se llega o se abandona, o una dirección multidifusión predefinida (todos los encaminadores/todas las direcciones de sistemas).

Dado que la asignación de la dirección de red residencial del STB y del VTP/D pueden estar gestionadas por distintas entidades, que se traduce en direcciones IP que pertenecen a distintas subredes, y teniendo en cuenta que:

- La conexión cambio de canal especificada FS-VDSL no se extiende más allá del punto de referencia V, aunque en cambio se termina en la AN.
- Se prevé de que todos los canales de difusión se reciban por la OLT. Ahora bien, para la ampliación de esta Recomendación en el futuro, la señalización entre la AN y la red principal para la obtención dinámica de canales de difusión, se basa en protocolos normalizados y no simplemente en el reenvío de mensajes IGMP generados por el VTP/D.

Se aplica lo siguiente:

- Se permite que el FPD, el VTP/D y la AN utilicen cualquier dirección IP de origen para mensajería IGMP.
- El FPD, el VTP/D y la AN procesarán mensajes IGMP independientemente de su dirección IP de origen.

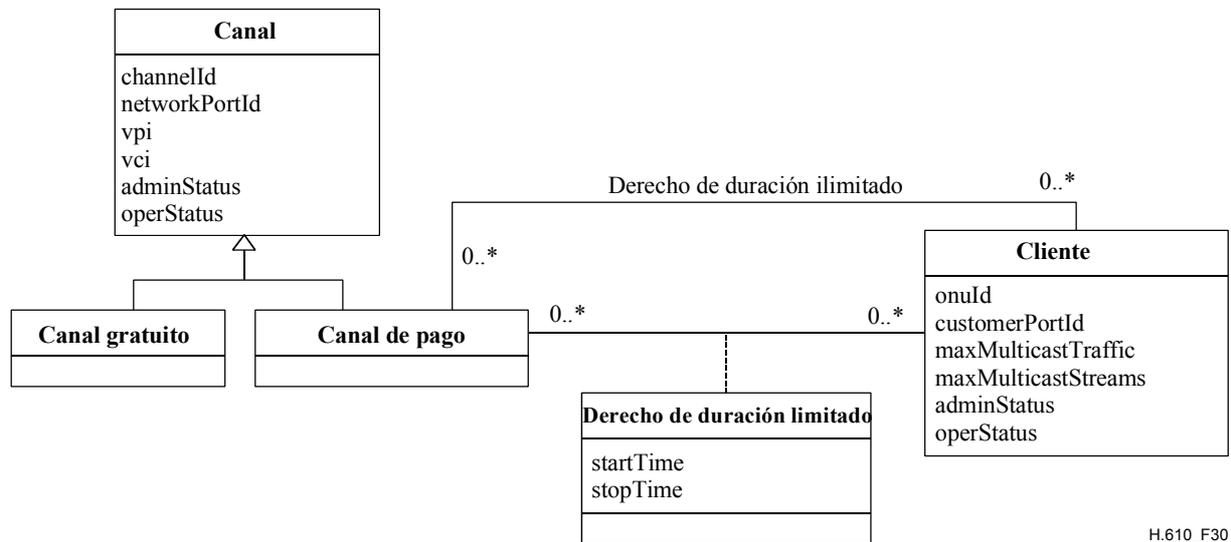
## 14.5 Modelo de información para la función cambio de canal dentro de la AN

Esta cláusula se aplica exclusivamente a la interfaz M. Las funciones que a continuación se definen se aplican en la entrega de servicios de ocio de difusión [el término 'servicio de ocio de difusión' incluye la TV/radio de difusión, vídeo de pago (PPV, *pay-per-view*) y VoD, en el caso de que se utilicen flujos multidifusión IP].

- Cambio de canal.
- Control de admisión de conexión (CAC, *connection admission control*).
- Acceso condicional (CA, *conditional access*).

Para realizar estas funciones, es necesario comunicar a la AN la información de gestión adicional. En la figura 30 se muestra el modelo de información de gestión que se implementará en la AN. Este modelo se denomina modelo de información de gestión de la función cambio de canal (CCF MIM, *channel change function management information model*). En la figura 30 se describen los objetos, atributos, relaciones y operaciones necesarias que se han de mantener. El CCF MIM se puede utilizar para obtener una base de información de gestión (MIB, *management information base*) SNMP adecuada para la AN, a la que se pueda acceder a través de la interfaz M. La MIB SNMP se define en el anexo B.

A continuación se describen las partes del modelo de información utilizado por cada función.



H.610\_F30

Figura 30/H.610 – Modelo de información de gestión de la función cambio de canal

### 14.5.1 Cambio de canal

La función cambio de canal utiliza la información contenida en los objetos 'Canal' (Channel) y 'Cliente' (Customer).

El objeto **Canal** define cada canal de ocio de difusión y su correspondiente channelId, que puede ser una dirección multidifusión IP o un ID de programa de difusión DSM-CC. Además, define los valores de networkPortId, VPI y VCI en el punto de referencia V.

El objeto **Cliente** se utiliza para describir cada UNI DSL (interfaz usuario-red) en una ONU que está adjunta a un cliente que recibe servicios de ocio de difusión. Los atributos que la identifican son el onuId y el customerPortId. Si la ONU está integrada en la OLT o la función cambio de canal se realiza en la ONU, el onuId no es aplicable.

Los dos objetos tienen dos atributos de estado de gestión: adminStatus y operStatus. El adminStatus define el estado deseado del correspondiente objeto. El operStatus define el estado real del

correspondiente objeto. El sistema de gestión manipula el atributo `adminStatus`, pero no el atributo `operStatus`.

Los objetos Canal y Cliente contienen toda la información necesaria para realizar la transconexión punto a multipunto ATM, a saber, la correspondencia entre el `channelId` recibido en el mensaje cambio de canal y la conexión ATM.

### 14.5.2 Control de admisión de conexión (CAC)

El objeto Cliente define los atributos `maxMulticastStreams` y `maxMulticastTraffic`. `maxMulticastStreams` especifica el máximo número de flujos separados que se pueden activar simultáneamente a través del enlace DSL del Cliente. `MaxMulticastTraffic` especifica el volumen máximo de tráfico atribuido a los servicios de difusión. El ancho de banda del canal se puede obtener de la información del punto de duplicación ATM almacenada en la OLT/ONU y que forma parte de la información VCC ATM. Esta información no forma parte del CCF MIM, aunque debe ser accesible por la entidad de gestión CCF MIM.

Los sistemas de gestión pueden utilizar `maxMulticastStreams` para controlar el número de ejemplares de servicios de ocio de difusión que puede recibir simultáneamente un cliente. La función CAC puede utilizar `maxMulticastTraffic` para comparar el ancho de banda disponible con el ancho del canal al que se va a pasar.

### 14.5.3 Acceso condicional en la AN

Para poder realizar el acceso condicional el modelo necesita soportar lo siguiente:

- La distinción entre los canales que requieren acceso condicional y los que no.
- El concepto de derechos de duración limitada e ilimitada.
- El número máximo de ejemplares de un servicio de ocio de difusión que puede tener activas un cliente.

No es necesario aplicar el acceso condicional a los canales gratuitos ("Free-to-air"), el modelo de las cuales utiliza el objeto canal gratuito (Free Channel). A los canales de pago (Premium) sí es necesario aplicarles acceso condicional y su modelo utiliza el objeto canal de pago (Premium Channel). Los objetos canal gratuito y canal de pago son formas especializadas del objeto Canal y por consiguiente heredan los atributos y operaciones de dicho objeto.

Los derechos a los canales de pago se modelan mediante dos tipos de relaciones entre los objetos Cliente y canal de pago. La relación derecho de duración ilimitada (Untimed Entitlement) describe el derecho concedido a un cliente para ver un canal de pago por un tiempo indefinido o hasta que se revoque ese derecho, para lo cual se suprime la relación con el canal de pago. También existe la relación derecho de duración limitada (Timed Entitlement) que describe un derecho concedido a un cliente para ver un canal de pago por un tiempo finito. Como la relación derecho de duración limitada tiene propiedades que no pertenecen al objeto canal de pago o al objeto Cliente, se define una clase de correspondencia para tenerlo en cuenta en el modelo y que se denomina objeto derecho de duración limitada. Este objeto especifica un intervalo de tiempo (`startTime` y `stopTime`) durante el cual el cliente tiene derecho a ver el canal de pago. Después de este intervalo de tiempo, la AN destruye automáticamente el objeto derecho de duración limitada y su correspondiente relación. La relación derecho de duración limitada es necesaria para soportar los servicios de PPV y VoD multidifusión. El cliente sólo puede tener derecho de duración ilimitada o de duración limitada para un determinado canal de pago, pero no ambos.

Para cumplir la precisión de temporización de los derechos de duración limitada, la AN estará sincronizada con la entidad que concede el derecho. La manera en que se logra esta sincronización no forma parte de los propósitos de esta Recomendación.

La relación duración ilimitada, la relación de duración limitada y el atributo `maxMulticastStreams` del objeto Cliente proporcionan toda la información necesaria para realizar la función acceso

condicional (CA) en la AN. Mediante la manipulación de estas relaciones de atributos el sistema de gestión puede conceder y revocar derechos de duración limitada o ilimitada de un determinado canal de pago y limitar el número de ejemplares de un servicio de ocio de difusión que el cliente puede obtener simultáneamente.

## 15 Servicio VoD

En esta cláusula se definen los requisitos del servicio vídeo a la carta (VoD, *video-on-demand*) en un sistema FS-VDSL. El servicio VoD es un servicio a la carta que entrega contenidos multimedia, por ejemplo vídeo, audio y juegos<sup>1</sup>. El servicio VoD requiere una calidad del servicio y una anchura de banda garantizada. Este servicio entrega vídeo de calidad de difusión y permite funciones interactivas como "pausa" y "avance rápido".

Normalmente las implementaciones del servicio VoD necesitan:

- gestión administrativa;
- una "granja de servidores" donde se almacena el contenido;
- instalaciones de transporte y de AN que puedan garantizar la QoS;
- soporte lógico de aplicación servidor-cliente que sean atractivos para los usuarios;
- coordinación de los recursos de red fundamentales entre los proveedores de servicio VoD y el operador de red.

El sistema FS-VDSL proporcionará la capacidad de entregar múltiples sesiones VoD por línea DSL.

### 15.1 Gestión administrativa de VoD

Las funciones de gestión administrativa VoD son: gestión de contenido, gestión de abonados, gestión de sesiones y gestión de derechos digitales.

La figura 31 ilustra los componentes administrativos. El contenido y sus correspondientes metadatos llegan al gestor de contenido, el cual los ubica en los servidores ("distribución de contenido") y alimenta el "directorio de contenido" con la información de programación y precios.

El contenido puede almacenarse criptado en el servidor de vídeo, en cuyo caso la información sobre derechos se ubicará en el gestor de derechos digitales desde el gestor de contenido cuando se cargue el contenido. Al establecer la sesión, el cliente y el gestor de sesión se comunicarán con el gestor de derechos digitales para determinar la información sobre derechos y comunicársela al cliente; el gestor de derechos digitales comunicará con el servidor de vídeo para aplicar las claves de criptación adecuadas.

El gestor de abonados creará cuentas de usuario y mantendrá el estado de las cuentas existentes. Al final de un ciclo de facturación, el gestor de abonados enviará las facturas al sistema de asistencia a la clientela. El gestor de contenido recopilará la información sobre compras.

El cliente selecciona el contenido que desea comprar del directorio de contenido. Cuando un cliente desea ver un contenido VoD se llama al establecimiento de sesión y de conexión, como se describe a continuación.

---

<sup>1</sup> Los servicios "VoD" también pueden entregar contenidos que no son vídeo. Ahora bien, dado que ésta es la principal aplicación y que además los requisitos más estrictos de anchura de banda y QoS son los que se derivan del transporte de vídeo, el término "VoD" se utiliza en esta Recomendación sin más aclaraciones o explicaciones.

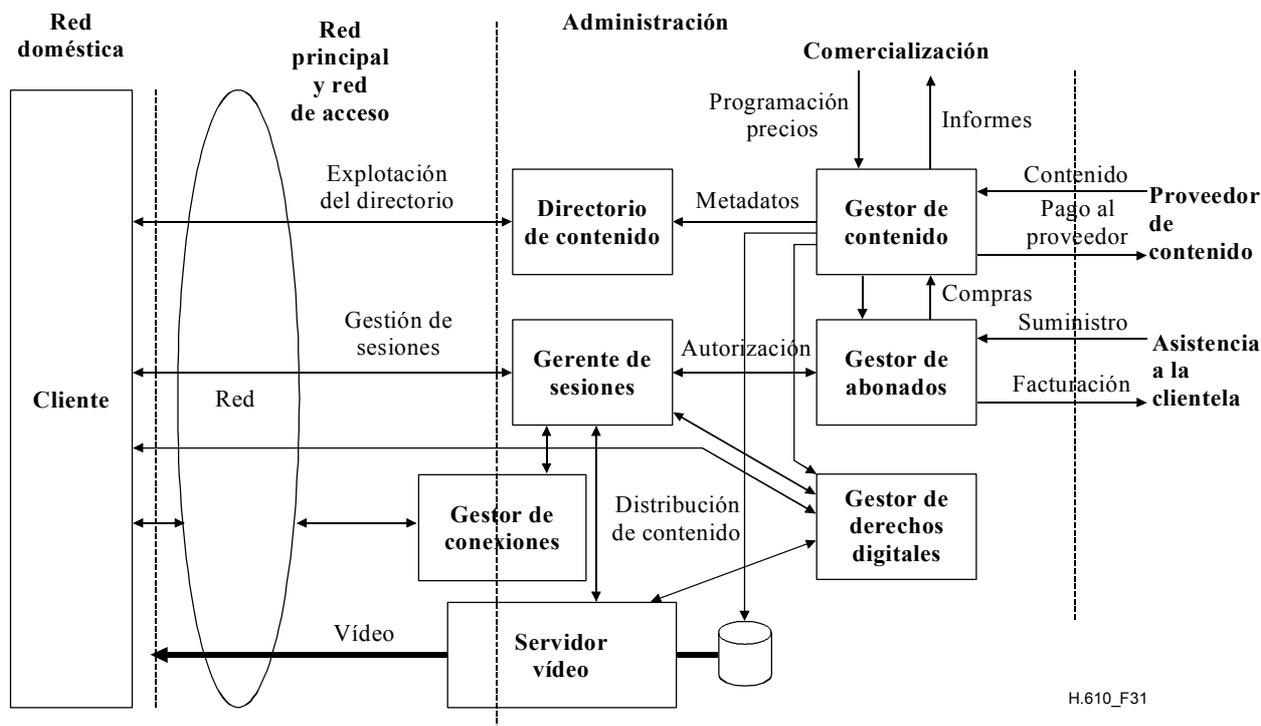


Figura 31/H.610 – Gestión administrativa de VoD

## 15.2 Ingeniería de red VoD

### 15.2.1 Granjas de servidores VoD centralizadas y distribuidas

Los equipos del servidor VoD pueden estar "centralizados", de modo que los servidores VoD proporcionan contenido a un gran número de usuarios desde un único lugar, o bien pueden estar "distribuidos" lo que significa que existen varios sitios que contienen menos servidores, los cuales a su vez proporcionan contenido a un número inferior de usuarios.

### 15.2.2 Tráfico administrativo bidireccional

El FPD será capaz de explorar el directorio, interactuar con el extremo de cabecera DRM y realizar establecimiento de sesiones VoD y de control de flujo. Se utilizarán protocolos IP para comunicarse con los servidores de aplicaciones VoD.

Para el tráfico administrativo VoD se proporcionarán conexiones punteadas, PPPoE, o encaminadas no traducidas, como se describe en la cláusula 9. Los servidores de aplicación que soportan estas funciones pueden estar en una red físicamente separada de la Internet pública y de los servicios de datos.

Este tráfico administrativo bidireccional debe compartir la conexión con el canal administrativo del servicio de difusión definido en 14.3.3.

### 15.2.3 Tráfico de vídeo unidireccional

La capacidad de transporte unidireccional transportará el contenido VoD desde el servidor de vídeo al VTP/D.

El tráfico administrativo puede estar multiplexado con el tráfico de vídeo descendente (por ejemplo, mediante señalización "dentro de la banda"). Sin embargo es posible que esto introduzca fluctuación MPEG y complique el diseño del servidor VoD.

El tráfico administrativo debe utilizar señalización "fuera de la banda". Esta solución permite que el operador de red haga las optimizaciones necesarias para la naturaleza unidireccional y la QoS del tráfico de vídeo.

Existen tres soluciones para la gestión del ancho de banda y la ingeniería de red de la red de transporte VoD.

- Ancho de banda preestablecido de este extremo a extremo (por ejemplo en el servidor de vídeo y en el VTP/D).
- Ancho de banda preestablecido en la red principal, y concentración en la red de acceso.
- Concentración en la red principal y en la red de acceso.

También son posibles otras variantes. La solución adoptada influye en los procedimientos de establecimiento de la conexión, que se describe en 15.5.

#### **15.2.4 Requisitos de QoS para el tráfico de vídeo VoD**

La red de transporte no permitirá la pérdida indebida de paquetes, no introducirá una excesiva fluctuación de paquetes ni permitirá la reordenación de paquetes. Las necesidades de QoS detalladas para el servicio VoD son idénticas a las del servicio de difusión (véase 14.3.4).

#### **15.2.5 Encapsulado del tráfico de vídeo VoD**

Las posibles opciones de encapsulado de flujo de vídeo son idénticas a las del servicio de difusión, descritas en 9.6.1 y 9.6.2.

### **15.3 Exploración de contenido VoD**

El abonado podrá explorar el directorio de contenido para comprar el contenido que desee. Para ello se utilizará el canal administrativo bidireccional descrito en 15.2.2.

Si bien no se especifica cómo se gestiona el directorio de contenido o cómo se realiza la exploración de éste, es posible utilizar técnicas como HTML.

Una vez que el usuario ha realizado su selección, el directorio de contenido proporcionará el identificador para el contenido VoD (por ejemplo, un URI RTSP) y quizá información adicional, por ejemplo información sobre QoS, tasa y formato de codificación, y la dirección IP del servidor de gestión de sesión que puede proporcionar el contenido deseado.

### **15.4 Establecimiento de sesión VoD**

La señalización de gestión de sesión tendrá lugar entre la aplicación FPD y la entidad de gestión de sesión VoD. Se utilizará el protocolo de gestión de sesión RTSP RFC 2326.

El mensaje RTSP SETUP (ESTABLECIMIENTO RTSP) contendrá los siguientes campos:

- Se proporcionará un identificador único del EPD. La sintaxis semántica del identificador no está definida, aunque podría ser un número de serie, un Id MACC o Id Smart Card.
- Se proporcionará un identificador del contenido deseado. Esta información vendrá del directorio de contenido.

El mensaje RTSP SETUP puede contener los siguientes campos:

- Un identificador de gestor de sesión VoD. El gestor de sesión VoD puede identificarse mediante la dirección IP o el nombre de su computador central en la información que figure en el directorio de contenido.
- Un identificador de OLT o identificador de zona de servicio para especificar con más detalle la ubicación física del FPD.
- Información sobre la QoS, por ejemplo la tasa de codificación deseada.

Antes de que se pueda admitir una sesión, el gestor de sesiones comprueba normalmente una serie de reglas comerciales: si el usuario tiene permiso, acceso, crédito; si el contenido se puede comprar, si hay suficientes recursos en el servidor. Si el usuario puede comprar la película, el gestor de conexiones realiza los cálculos del ancho de banda necesario y llama a los procedimientos establecimiento de conexión para determinar si hay suficientes recursos de red.

Es posible llamar a la gestión de derechos digitales en ese momento para conceder al usuario los derechos necesarios y proporcionarle la clave y la información de acceso al FPD para la descripción.

El mensaje RTSP SETUP REPLY (RESPUESTA AL ESTABLECIMIENTO RTSP) puede contener los siguientes campos:

- Información sobre la conexión y la QoS. Esta información podría incluir la dirección multidifusión de clase D o BroadcastProgramId (identificador del programa de difusión) DSM-CC.
- Derechos DRM o información clave.

Una vez establecida la conexión, el usuario puede utilizar el control de secuencias RTSP de la sesión para iniciar, hacer una pausa o reproducir la película.

Cuando el cliente ha terminado de ver la película, liberará la sesión mediante la instrucción RTSP TEARDOWN, mediante la cual se liberan tanto los recursos de sesión como de conexión. El servidor puede, además, liberar la sesión si lo considera necesario.

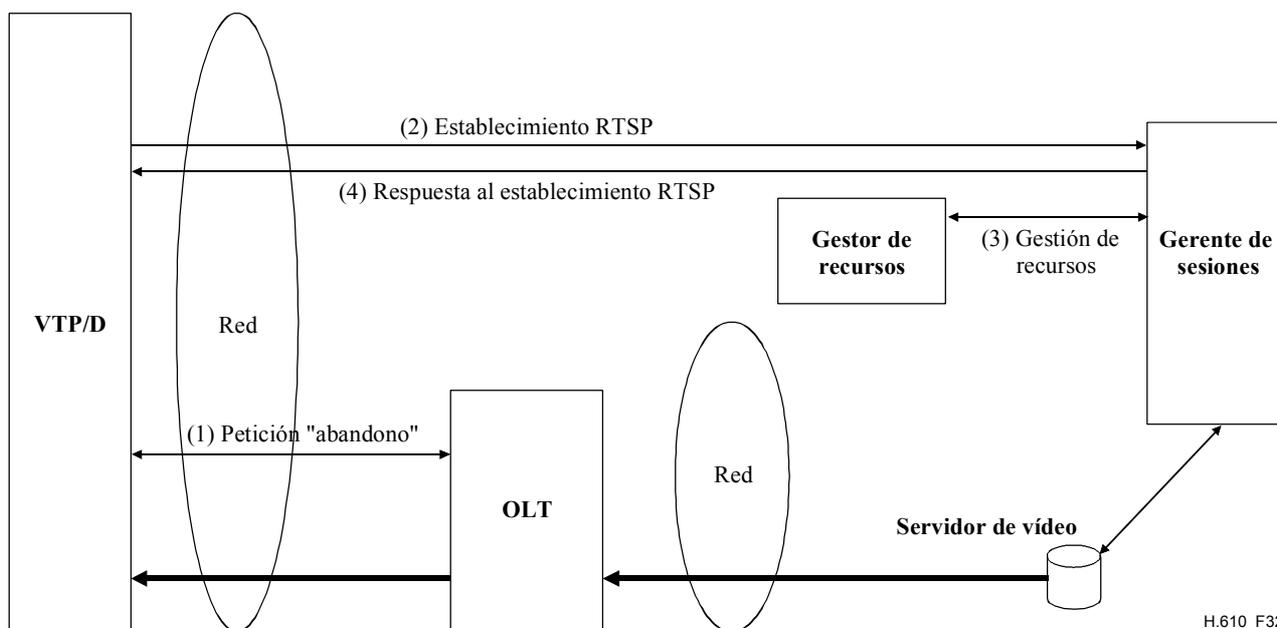
## **15.5 Establecimiento de la conexión VoD**

En esta cláusula se describe los procedimientos de establecimiento de conexión. En el primer caso que se describe a continuación el ancho de banda entre el servidor VoD y el cliente VTP/D está preestablecido de antemano y los procedimientos de establecimiento de conexión no son necesarios. La otra posibilidad es que el ancho de banda no esté establecido entre el VTP/D y el servidor, en cuyo caso se llamará a los procedimientos de establecimiento de conexión en el momento de establecer la sesión.

### **15.5.1 Ancho de banda preestablecido de extremo a extremo**

Esta subcláusula describe el caso en que el ancho de banda entre el servidor VoD y el VTP/D está preestablecido.

En ese caso, el ancho de banda está normalmente "sobredimensionado" en la AN y sobre la línea DSL; el ancho de banda del abonado se comparte entre el servicio de vídeo de difusión y los datos. El programa informático del FPD y las componentes VoD administrativas garantizarán que el ancho de banda total del abonado se distribuya correctamente entre los diferentes servicios. En el momento de establecer una sesión, sólo es necesario la atribución de recursos en el servidor VoD; la red principal y la AN no están al corriente de la sesión.



H.610\_F32

**Figura 32/H.610 – Establecimiento de sesión VoD – ancho de banda preestablecido de extremo a extremo**

La figura 32 ilustra el flujo de mensajes para establecer una sesión VoD.

Paso 1. El cliente "abandona" un canal de difusión existente para liberar el ancho de banda necesario para el canal VoD.

Paso 2. Se lleva a cabo la señalización de la sesión VoD entre el FPD y el gestor de sesiones.

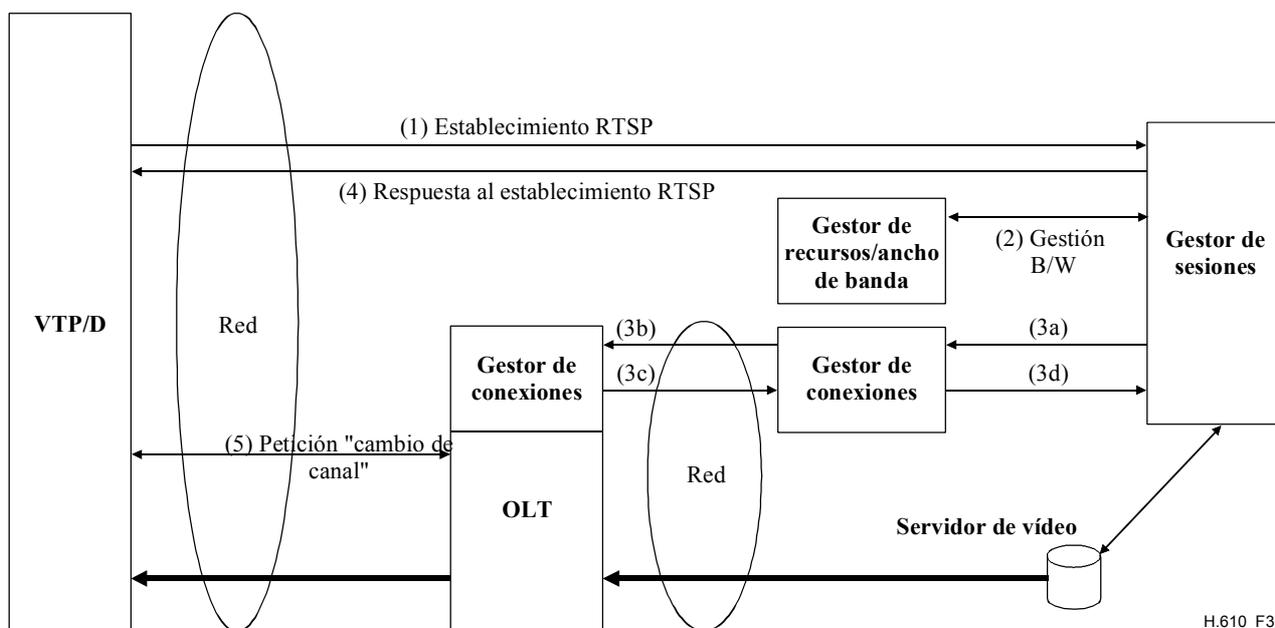
Paso 3. Se atribuirán recursos del servidor VoD. En el diagrama anterior, el gestor de sesiones llama al gestor de recursos. Como mínimo, el gestor de recursos necesita identificar y atribuir los recursos del servidor de vídeo adecuados, por ejemplo el puerto de salida. Para ello, quizá necesite conocer la identidad del VTP/D (o de la OLT) y también el contenido vídeo deseado.

Paso 4. Se envía de vuelta al VTP/D la información sobre recursos de conexión y de confirmación (por ejemplo, el "canal" VoD).

### **15.5.2 Embotellamiento del ancho de banda en la red de transporte**

Esta subcláusula describe el caso en que el ancho de banda entre el servidor VoD y el VTP/D no está preestablecido. Por consiguiente, los procedimientos de establecimiento de conexión son obligatorios.

En la figura 33 se proporciona una descripción general de la sesión VoD y de los procedimientos de establecimiento de conexión.



**Figura 33/H.610 – Establecimiento de sesión VoD – concentración en la red de acceso**

Paso 1. Se lleva a cabo la señalización de la sesión VoD entre el FPD y el gestor de sesiones.

Pasos 2 y 3a. Es obligatoria la asignación de recursos de servidor VoD y de ancho de banda red. El gestor de sesiones llama al gestor de recursos y al gestor de conexiones para establecer una conexión desde el servidor de vídeo al FPD. Es posible realizar la gestión del ancho de banda necesario como parte de la señalización de conexión (es decir mediante el gestor de conexiones) o bien que sea una función del gestor de recursos.

Paso 3b. Se utilizan procedimientos de establecimiento de conexión para reservar el ancho de banda de la conexión vídeo descendente. La entidad de establecimiento de conexión en el gestor de sesiones mapeará la identidad VTP/D en la OLT de la AN para determinar la ruta de la conexión. Sólo hay unos pocos métodos posibles para extraer la ubicación de la OLT de la identificación VTP/D o FPD.

- Configuración local del id OLT en la FPD.
- De manera implícita, mediante mecanismos de asignación de direcciones IP (por ejemplo servidor DHCP o RADIUS). Un posible convenio es asignar una gama de direcciones IP a una OLT.
- Otros mecanismos de configuración.

Si en la red de acceso se utilizan procedimientos de control de acceso, los procedimientos de establecimiento de conexión crearán la conexión con los permisos necesarios.

Pasos 3c, 3d y 4. Una vez que los procedimientos de establecimiento de conexión han negociado satisfactoriamente una conexión, se envía de vuelta al FPD la confirmación y la información de recursos de conexión (por ejemplo el "canal" VoD).

Paso 5 (recomendado). El FPD utiliza los procedimientos de cambio de canal para sintonizar el "canal" deseado. Mediante la utilización de señalización explícita del VTP/D a la AN, el VTP/D puede conmutar de servicios VoD a servicios de difusión, lo que le permite a la AN gestionar explícitamente el ancho de banda entre los dos servicios. Obsérvese que la utilización de direccionamiento clase D (es decir direcciones IP multidifusión) simplifica la señalización.

### **15.5.3 Requisitos del protocolo de establecimiento de conexión**

El protocolo de establecimiento de conexión debe realizarse fuera de banda.

El protocolo de establecimiento de conexión debe iniciarlo el servidor, dado que la señalización iniciada por el servidor es más segura que la iniciada por el FPD.

El protocolo de establecimiento de conexión debe ser un "estado inalterable". Esta solución crea un trayecto bien definido para garantizar la QoS durante toda la sesión. Las conexiones de estado inalterable también eliminan la necesidad del tráfico "de mantenimiento" para cada conexión. Por ejemplo, el RSVP RFC 2205 [I-9], es un protocolo "de estado alterable" que no se recomienda como solución a largo plazo.

### **15.5.4 Opciones del protocolo de establecimiento de conexión**

La selección del protocolo de establecimiento de conexión depende de la red de transporte.

Para las redes de transporte IP, puede utilizarse el RSVP-TE RFC 3209 [I-11] o el CR-LDP RFC 3212 [I-10].

Para redes de transporte ATM, puede utilizarse el SVC o el "PVC alterable" (conexiones establecidas en el plano de gestión).

En el caso de los SVC ATM, la señalización puede ser de extremo a extremo, y terminar en el VTP/D (en cuyo caso el VTP/D necesita una pila de señalización ATM y la AN tiene que actuar como un conmutador ATM).

Otra posibilidad es terminar, la señalización ATM en la red de acceso y complementarse con señalización de cambio de canal desde el FPD.

### **15.5.5 Asignación de direcciones IP para VoD descendente**

Si hay una capa IP, es posible utilizar direcciones IP unidifusión o multidifusión (por ejemplo, clase D), si bien se recomienda direcciones IP multidifusión.

El motivo de utilizar direcciones de clase D para flujos VoD es que permite que el VTP/D conmute fácilmente entre trenes VoD y trenes de vídeo de difusión (por ejemplo, mediante señalización de cambio de canal) y permite que la OLT participe en la gestión del ancho de banda.

## **16 Directrices para voz por DSL**

Para proporcionar voz por DSL se utilizará VoATM o VoIP. En el apéndice IX figuran las directrices informativas sobre las implementaciones de voz por DSL.

### **16.1 VoATM**

VoATM se proporcionará mediante BLES, de acuerdo con 9.8 y 10.6.

### **16.2 VoIP**

Es posible establecer la conectividad IP subyacente mediante una de las opciones siguientes:

- Una conexión puente, como se describe en 9.1 y 10.4.1.
- Una conexión PPPoE, como se describe en 9.2 y 10.4.2.
- Una conexión encaminada no traducida, como se describe en 9.4 y 10.3.2.
- Una conexión encaminada traducida, como se describe en 9.3 y 10.3.1.

## 17 Gestión de la AN

### 17.1 OLT

Las funciones OAM de la AN se realizarán mediante la OLT vía la interfaz M (véase la figura 1). La operación y gestión distantes de la AN será posible a través de una conexión dentro de banda al bloque OAM, y quizá también mediante una conexión fuera de banda. La interfaz M puede ser específica del fabricante. Ahora bien, se debe soportar un protocolo de gestión aceptado por la industria (por ejemplo, SNMP, CORBA, CMIP) para los sistemas de gestión específicos del operador que accedan directamente al bloque OAM.

La MIB de control de acceso del servicio de radiodifusión digital se describe en 14.5.3 y en el anexo B.

La gestión de la OLT será conforme con la Rec. UIT-T H.611 [5].

### 17.2 ONU

El bloque OAM permite el control de funcionamiento y gestión de la ONU, incluidas las derivaciones DSL. La operación se realizará mediante una conexión dentro de banda.

La gestión de la ONU será conforme con la Rec. UIT-T H.611 [5].

## 18 Gestión del VTP/D

### 18.1 Modelo de gestión del VTP/D

El modelo de gestión del VTP/D consta de clases y atributos que puede ser necesario configurar dentro del VTP/D. El modelo de gestión se expresa utilizando el lenguaje de modelado unificado (UML, *unified modelling language*). Las zonas sombreadas en la figura 34 indican la relación del modelo de gestión con los bloques del modelo funcional VTP/D definidos en la cláusula 10. Las clases con un contorno punteado no se describen en esta Especificación y sólo se muestran para completar el diagrama.

El **VTP/D** contiene un máximo de dos **interfaces DSL** (es decir, trayecto rápido y/o entrelazado) para la interconexión a una red de acceso y una o varias **interfaces Ethernet** para la interconexión a la red residencial.

La interfaz DSL contienen una o varias **PVC ATM** (conexiones virtuales permanentes). Si la PVC ATM utiliza AAL 2 o AAL 5, se asigna a la PVC el **Descriptor AAL 5** o **Descriptor AAL 2** que corresponda. A cada PVC se le asigna el transporte de un tipo particular de flujo que se define en la cláusula 9. Esto se indica mediante la relación de herencia con respecto a la clase flujo. La clase flujo puede tener atributos asociados para proporcionar los parámetros de configuración relacionados con ese flujo PVC ATM. En algunos casos la clase flujo puede estar vacía y sólo existe para indicar el tipo de flujo transportado por la PVC ATM. Las siguientes relaciones adicionales se indican en términos de aspecto de gestión de flujos.

- El **flujo encaminado** puede ser del tipo **PPP** o **IPoA**, y puede ser traducido o no traducido.
- El **flujo puenteado** puede que no tenga **filtros puente** asociados, o puede tener varios, para soportar el filtrado de paquetes recibidos por el flujo. Por ejemplo, un filtro basado en un paquete que es un paquete PPPoE.

El VTP/D tiene un **servidor DHCP**, que se utiliza para atribuir direcciones IP a los terminales de la red residencial.

La **ruta IP** es una entrada de reenvío utilizada para encaminamiento IP. Cada ruta IP está asociada a un flujo encaminado para el encaminamiento del paquete hacia la AN o una interfaz Ethernet para el encaminamiento hacia la red residencial. A un mismo flujo encaminado pueden hacer referencia



**Cuadro 22/H.610 – Clase ATM PVC**

<b>Atributo</b>	<b>Valor</b>	<b>Observación</b>
Interfaz DSL	Rápido, entrelazado	–
VPI	0-255	–
VCI	32-65535	–
Función F5	Punto extremo, segmento, ambos, ninguno	Véase la Rec. UIT-T I.610
Función F4	Punto extremo, segmento, ambos, ninguno	Véase la Rec. UIT-T I.610
F4ccsink	Activado, desactivado	–
F5ccsink	Activado, desactivado	–
Tipo de encapsulado	LLC/SNAP, VCMUX	–
Tipo AAL	AAL 2, AAL 5	–
Categoría de servicio ATM	CBR, UBR, VBRrt, VBRnrt	–
Velocidad de célula de cresta	Todos (células/s)	–
Velocidad de célula sostenible	Todos (células/s)	Para el servicio VBR solamente
Tamaño máximo de ráfaga	Todos (células/s)	Para el servicio VBR solamente

**18.1.2 Clase difusión**

Los atributos que se describen en el cuadro 23 corresponden a la gestión de configuración de la función servicio de difusión digital del VTP/D.

**Cuadro 23/H.610 – Clase difusión**

<b>Atributo</b>	<b>Valor</b>	<b>Observación</b>
Intervalo de consulta del último miembro IGMP	1-100 (múltiplos de 100 ms)	Véase 14.4.2
Número de consultas del último miembro IGMP	1-10	Véase 14.4.2
Intervalo de información no solicitada IGMP	1-100 (múltiplo de 100 ms)	Véase 14.4.2
Dirección IP de TV de difusión	Todos (dirección IP de clase D)	Véase 14.2
Máscara IP de TV de difusión	Todos (dirección IP)	Véase 14.2
Protocolo de cambio de canal	IGMPv2, DSMCC	Véase 9.5
Encapsulado MPEG	MPEG2AAL5, MPEG2UDP	–

### 18.1.3 Clase flujo puentado

En el cuadro 24 se describen los atributos correspondientes a la gestión de configuración de una clase flujo puentado.

**Cuadro 24/H.610 – Clase Flujo Puentado**

Atributo	Valor	Observación
Rotulado VLAN	Activado, desactivado	–
Rótulo VLAN por defecto	Todos (entero)	–

### 18.1.4 Filtro puente

En el cuadro 25 figuran los atributos relacionados con la gestión de configuración del filtro puente.

**Cuadro 25/H.610 – Filtro puente**

Atributo	Valor	Observación
Filtro	Activado, desactivado	–
Puerto puente	Una referencia a un puerto puente	–

### 18.1.5 Clase PPP

En el cuadro 26 figuran los atributos correspondientes a la gestión de configuración de la clase PPP.

**Cuadro 26/H.610 – Clase PPP**

Atributo	Valor	Observación
Tipo PPP	PPPoA, PPPoE	–
Rótulo nombre del servicio PPPoE	Cualquiera (texto)	Véase RFC 2516. No es aplicable si el tipo PPP es "PPPoA"
Rótulo nombre AC PPPoE	Cualquiera (texto)	Véase RFC 2516. No es aplicable si el tipo PPP es "PPPoA"
Protocolo de autenticación por defecto PPP	Ninguno, CHAP, PAP	–
Intervalo de petición de eco LCP	Cualquiera (segundos)	–
Nombre de usuario PPP	Cualquiera (texto)	–
Contraseña PPP	Cualquiera (texto)	–

### 18.1.6 Clase IPoA

En el cuadro 27 figuran los atributos correspondientes a la gestión de configuración de una clase IPoA.

**Cuadro 27/H.610 – Clase IPoA**

Atributo	Valor	Observación
Configuración IP	Dinámico, estático	Si el valor es dinámico la configuración se realiza mediante DHCP y se utilizan los dos parámetros DHCP siguientes en los mensajes DHCP.
Opción Identificador de clase de fabricante DHCP	Cualquiera (texto)	Véase 12.2
Opción Clase de usuario DHCP	Cualquiera (texto)	Véase 12.2
RIP v2	Activado, desactivado	–

**18.1.7 Clase ruta IP**

En el cuadro 28 figuran los atributos correspondientes a la gestión de configuración de una clase ruta IP.

**Cuadro 28/H.610 – Clase ruta IP**

Atributo	Valor	Observación
Dirección de destino IP	Cualquiera (dirección IP)	–
Máscara de subred de destino IP	Cualquiera (dirección IP)	–
Interfaz	Se refiere a una clase PPP o a una clase IPoA o a una interfaz IP en la red residencial.	–
Métrica	Cualquiera (entero)	–

**18.1.8 Clase NAT**

En el cuadro 29 figuran los atributos correspondientes a la gestión de configuración de la clase NAT.

**Cuadro 29/H.610 – Clase NAT**

Atributo	Valor	Observación
Tipo de puerto descendente	UDP, TCP	–
Número de puerto descendente	1-65535	–
Dirección IP de destino	Toda dirección IP en la red residencial (dirección IP)	–
Identificador de puerto PPP	Referencia a un puerto PPP	–

### 18.1.9 Clase servidor DHCP

En el cuadro 30 figuran los atributos correspondientes a la gestión de configuración del servidor DHCP.

**Cuadro 30/H.610 – Clase servidor DHCP**

Atributo	Valor	Observación
Dirección de subred	Cualquiera (dirección IP)	–
Máscara de subred	Cualquiera (dirección IP)	–
Fuente de direcciones IP	Cualquiera dentro de la subred definida antes (dirección IP)	–
DNS primario	Cualquiera (dirección IP)	–
DNS secundario	Cualquiera (dirección IP)	–
Retransmisión DNS	Activado, desactivado	Es necesario cuando los campos DNS primario y secundario no están completados y no se pueden atribuir a terminales en la red residencial.

## 18.2 Métodos de configuración

A continuación se describen las posibles formas de configurar un VTP/D. Cada tipo de escenario podrá tener la configuración que mejor se adapte a sus necesidades. Además, en algunos tipos de escenarios es posible que se necesiten varios métodos de configuración. Evidentemente, los métodos de configuración propuestos son el resultado de un compromiso entre el nivel de flexibilidad y la dificultad (es decir, complejidad y gastos de estructura) correspondientes a la configuración. A no ser que se especifique explícitamente lo contrario es posible utilizar un método para proporcionar todas las capas de configuración VTP/D.

### 18.2.1 Configuración preestablecida

El VTP/D será capaz de arrancar y funcionar con una configuración preestablecida. Por ello se entiende tanto la configuración establecida por el fabricante para la primera instalación o la configuración dinámica almacenada en una memoria no volátil de la unidad antes de la última vez que se reinicializó. Este atributo permite que el VTP/D funcione en un entorno estático donde la red no soporta mecanismos dinámicos de configuración. Para facilitar la compatibilidad en las primeras etapas de las instalaciones FS-VDSL, se define una configuración FS-VDSL ATM por defecto. El valor de la configuración ATM por defecto se especifica en el cuadro 31.

### 18.2.2 ILMI

La ILMI ATM Forum Specification af-ilmi-0065.0000 es una herramienta dedicada y limitada a la configuración de capa ATM. La ILMI puede definir conexiones ATM y asociar cada una de ellas con parámetros de capa ATM fundamentales, por ejemplo clase de tráfico, descriptor de tráfico, tipo AAL, encapsulado, e incluso tipo de servicio. Dado que en esta Recomendación se tratan principalmente las VC permanentes, el VTP/D soportará las extensiones ILMI del Foro ATM y del

Foro DSL aplicables a PVC, como se describe en Specification af-nm-0122.000 y TRF 037. La ILMI utiliza una conexión VC predefinida (es decir, 0,16) entre el VTP/D y la red de acceso.

La asociación entre una PVC y el procesamiento funcional específico (es decir, el flujo de tráfico) se logra mediante el campo ILMI MIB atmfAtmServiceName, que forma parte del objeto tipo de servicio. A continuación se numeran los nombres de servicio FS-VDSL que representan los ocho tipos de conexión descritos en la cláusula 9 (en el mismo orden).

- FS-VDSL-BRIDGE
- FS-VDSL-PPPOEFILTER
- FS-VDSL-TRANSROUTE
- FS-VDSL-NONTRANSROUTE
- FS-VDSL-CHANNELCHANGE
- FS-VDSL-BROADCAST
- FS-VDSL-RMMANAGE
- FS-VDSL-BLES

Además, se definen unos pocos valores de subnombres de servicio para definir más precisamente el servicio. Para ello se utiliza el atmfAtmServiceSubName, que forma parte del objeto tipo de servicio en la ILMI MIB.

- DSMCC – sólo es pertinente para el flujo FS-VDSL-CHANNELCHANGE.
- IGMPv2 – sólo es pertinente para el flujo FS-VDSL-CHANNELCHANGE.
- MPEG2AAL5 – indica que se utiliza el encapsulado MPEG2 por AAL 5 (es decir, entrega basada en ATM). Sólo es pertinente para el flujo FS-VDSL-BROADCAST.
- MPEG2UDP – indica que se utiliza el encapsulado MPEG2 por UDP (es decir, entrega basada en IP). Sólo es pertinente para el flujo FS-VDSL-BROADCAST.

### **18.2.3 Canal de gestión a distancia**

Cada VTP/D dispone de una VC ATM dedicada para la gestión a distancia, como se define en 9.7 y 10.7. Los métodos de configuración que a continuación se describen puede utilizarse por esta conexión.

#### **18.2.3.1 SNMP**

Es posible utilizar SNMPv2 IETF RFC 3416 para gestionar y configurar a distancia el VTP/D. El SNMP es un protocolo de gestión a escala completa muy conocido y adecuado para entornos de gestión muy dinámicos. Este protocolo permite configurar y consultar el valor de objetos específicos dentro de un gran conjunto de tablas de base de datos. Asimismo, permite a las entidades gestionadas iniciar notificaciones (es decir, mensajes de alerta SNMP) hacia los sistemas de gestión que indican condiciones de avería. Las operaciones SNMP se basan en la información común sobre la organización interna de las tablas de las bases de datos, denominados SNMP MIB, que contienen las entidades gestionadas.

En esta Recomendación no se define un SNMP MIB para el VTP/D. Así pues, en la medida de lo posible, la implementación SNMP para el VTP/D debe utilizar los MIB normalizados existentes, por ejemplo MIB II IETF RFC 1213 [I-13] para la interfaz básica y definición de sistema, la MIB Interfaz IETF RFC 2863 [25] para la definición de interfaces lógicas y físicas y la MIB AToM IETF RFC 2515 [26] para las definiciones de capa ATM.

### **18.2.3.2 Fichero de configuración**

A diferencia del SNMP, este método no pretende realizar una configuración paso a paso sino realizar una gran cantidad de operaciones de configuración de una sola vez. El fichero de configuración se descarga al VTP/D mediante TFTP.

En el anexo A se especifica el formato del fichero de configuración FS-VDSL. El formato se basa en definiciones TLV (tipo, longitud, valor) e incluye todos los parámetros necesarios para la configuración básica del VTP/D. Asimismo el formato ofrece la posibilidad a los fabricantes de ampliar la configuración básica con atributos específicos del fabricante.

### **18.2.3.3 Otros métodos**

Es posible utilizar otros métodos, por ejemplo la gestión local, como se describe en la Rec. UIT-T H.611 [5].

## **18.3 Secuencia de configuración VTP/D**

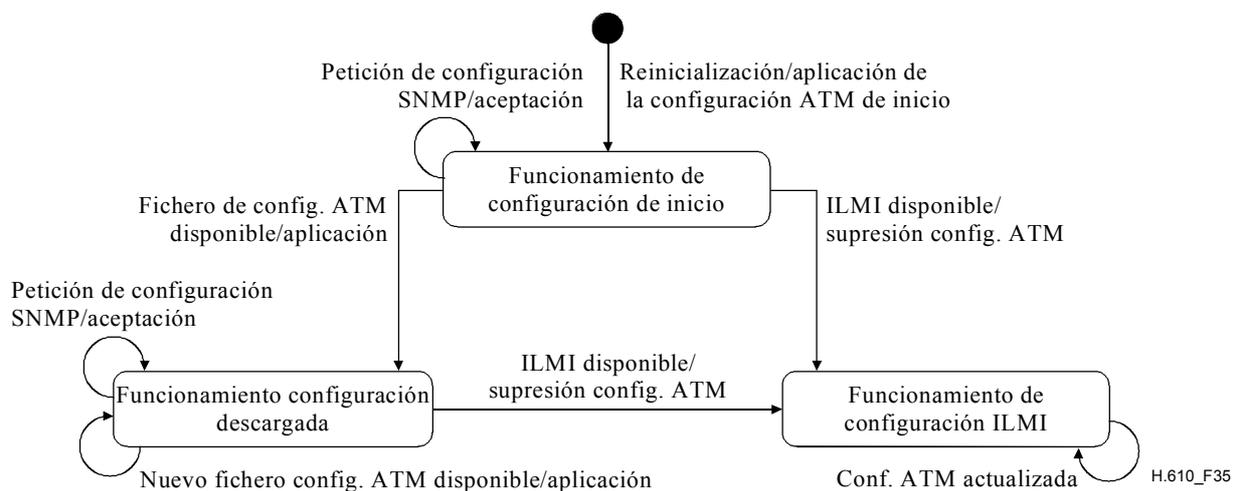
Una manera sencilla de configurar el VTP/D es por orden ascendente de las capas de la pila de protocolos. A saber, en primer lugar se configura la capa física, DSL. En segundo lugar se configura ATM. En tercer lugar la capa Ethernet y el IP, y por último los servicios (por ejemplo difusión digital). Ahora bien, esta secuencia no se puede utilizar cuando se emplea un canal de gestión a distancia para la configuración (por ejemplo SNMP, fichero, etc.) dado que la configuración IP de la conexión de gestión a distancia del VTP/D (es decir DHCP) concluirá después de llamar a una transferencia de ficheros o a una transacción SNMP. Esto hace absolutamente necesario que siempre haya una conexión de gestión a distancia por defecto.

Otro asunto relativo a la secuencia de configuración es el orden de precedencia entre las diversas tareas de gestión que se pueden configurar en la misma capa de protocolo. En la siguiente subcláusula se explica este asunto con respecto a la capa ATM.

### **18.3.1 Secuencia de configuración ATM**

Dado que es posible que haya múltiples procesos de gestión funcionando simultáneamente en el VTP/D y que cada uno de ellos puede utilizarse para configurar los parámetros ATM del VTP/D, se utilizará la máquina de estados que se describe en la figura 35 para evitar conflictos en la configuración de la capa ATM. Esta máquina de estados especifica que la configuración basada en ILMI puede sustituirse por la configuración ATM basada en el flujo de gestión a distancia durante el funcionamiento del VTP/D. En cambio, lo contrario no es cierto, es decir una vez establecida la conectividad ILMI el VTP/D nunca aceptará la configuración ATM a través de del canal de gestión a distancia, aun cuando se pierda la conectividad ILMI. La única manera de forzar al VTP/D para obtener una nueva configuración ATM a través del canal de gestión es reiniciando el VTP/D.

Obsérvese además que, si se utiliza ILMI o se descarga un fichero de configuración, la interfaz de gestión local se deshabilitará para la configuración de capa ATM.



**Figura 35/H.610 – Máquina de estados de la configuración de capa ATM del VTP/D**

Los estados y las transiciones de estado son los siguientes.

**Estado inicial:** Representa el VTP/D en estado fundamental. Sólo es posible la transición a partir de este estado.

- *Reinicialización:* Se reinicializa el VTP/D. Esto causa que se aplique la configuración de inicio. La configuración de inicio puede ser la última configuración que estaba funcionando (si la había); en el caso de un primer inicio, se utilizará la configuración por defecto descrita en el cuadro 31. El VTP/D pasa al estado funcionamiento de configuración de inicio.

**Estado funcionamiento de configuración de inicio:** Ese estado representa una capa ATM funcionando, la cual se configuró mediante una configuración de inicio. En este estado es posible manipular las capas superiores correspondientes con todas las VCC configuradas y disponibles. Existen tres posibles transiciones desde este estado.

- *ILMI disponible:* Si se establece la conectividad ILMI, se suprime la configuración ATM existente y el VTP/D pasa al estado de funcionamiento de configuración ILMI.
- *Fichero de configuración ATM disponible:* Si se descarga el fichero de configuración ATM por el flujo de gestión a distancia, se aplica esta configuración (sobrescribiendo la configuración existente) y el VTP/D pasa al estado de funcionamiento de configuración descargada.
- *Petición de configuración SNMP:* Si se recibe una solicitud de configuración SNMP, ésta se aceptará de acuerdo con el protocolo y las reglas SNMP del VTP/D MIB. El VTP/D no cambiará de estado.

**Estado funcionamiento de configuración ILMI:** Este estado representa una capa ATM configurada mediante ILMI. En este estado es posible manipular las capas superiores correspondientes a todas las VCC configuradas y disponibles. Una vez el VTP/D está en este estado, no es posible utilizar el canal de gestión a distancia para configurar la capa ATM, aun cuando se pierda la conectividad ILMI. La ILMI tiene muchos estados, sólo se muestra uno de ellos para aclarar que la ILMI se puede utilizar para actualizar la configuración de capa ATM una vez está en este estado.

**Estado funcionamiento de configuración descargada:** Este estado representa una capa ATM configurada mediante un fichero de configuración recibido a través del flujo de gestión a distancia. En este estado es posible manipular las capas superiores correspondientes a todas las VCC configuradas y disponibles. Existen tres posibles transiciones desde este estado.

- *Petición de configuración SNMP:* Si se recibe una petición de configuración SNMP, ésta se aceptará de acuerdo con el protocolo y las reglas SNMP de la MIB VTP/D. El VTP/D no cambia de estado.
- *Nuevo fichero de configuración ATM disponible:* Si se descarga un nuevo fichero de configuración ATM a través del flujo de gestión a distancia, se aplicará esta configuración (sobrescribiendo la configuración existente) y el VTP/D no cambiará de estado.
- *ILMI disponible:* Si establece la conectividad ILMI, se suprime la configuración ATM existente y el VTP/D pasa al estado de funcionamiento de configuración ILMI.

**Cuadro 31/H.610 – Configuración ATM por defecto**

Tipo de conexión	Descriptor de tráfico ATM	Notas
Difusión	VPI/VCI = 1/33 Tipo de tráfico: CBR uni-d	Los valores por defecto sólo son necesarios para el cambio de canal basado en IGMP.
Difusión	VPI/VCI = 1/34 Tipo de tráfico: CBR uni-d	Los valores por defecto sólo son necesarios para el cambio de canal basado en IGMP.
Difusión	VPI/VCI = 1/35 Tipo de tráfico: CBR uni-d	Los valores por defecto sólo son necesarios para el cambio de canal basado en IGMP.
Difusión	VPI/VCI = 1/36 Tipo de tráfico: CBR uni-d	Reservado para tráfico que no es vídeo. Los valores por defecto sólo son necesarios para el cambio de canal basado en IGMP.
Cambio de canal	VPI/VCI = 1/32 Tipo de tráfico: CBR bi-d sym PCR = 42 células/s	–
Punteada	VPI/VCI = 0/32 Tipo de tráfico: UBR bi-d	–
Punteada	VPI/VCI = 0/33 Tipo de tráfico: UBR bi-d	–
Punteada	VPI/VCI = 0/34 Tipo de tráfico: UBR bi-d	–
Punteada	VPI/VCI = 0/35 Tipo de tráfico: UBR bi-d	–
PPPoE	VPI/VCI = 0/62 Tipo de tráfico: UBR bi-d	–
Encaminada no traducida	VPI/VCI = 0/42 Tipo de tráfico: UBR bi-d	–
Encaminada no traducida	VPI/VCI = 0/43 Tipo de tráfico: UBR bi-d	–
Encaminada no traducida	VPI/VCI = 0/44 Tipo de tráfico: UBR bi-d	–

**Cuadro 31/H.610 – Configuración ATM por defecto**

<b>Tipo de conexión</b>	<b>Descriptor de tráfico ATM</b>	<b>Notas</b>
Encaminada no traducida	VPI/VCI = 0/45 Tipo de tráfico: UBR bi-d	–
Encaminada traducida	VPI/VCI = 0/63 Tipo de tráfico: UBR bi-d	–
BLES	VPI/VCI = 0/40 Tipo de tráfico: CBR bi-d sym No se especifica valor por defecto PCR.	Esta VC es opcional.
Canal ILMI	(VPI/VCI = 0/16 bi-d sym)	–
Canal de gestión a distancia	VPI/VCI = 0/50 Tipo de tráfico: VBRnrt bi-d sym PCR = 100 células/s SCR = 50 células/s MBS = 50 células	–
NOTA – bi-d = conexión bidireccional, uni-d = conexión unidireccional, sym = parámetros ancho de banda simétricos.		

## Anexo A

### Formato del fichero de configuración

En este anexo se define el formato y la utilización del fichero de configuración del VTP/D. Éste se puede utilizar para configurar el VTP/D desde un sistema de gestión remota a través de una conexión de gestión remota.

El formato del fichero de configuración será TLV (tipo, longitud, valor). Los tipos y subtipos TLV correspondientes a la configuración básica del VTP/D se describen en el cuadro A.1. Se permiten las extensiones de marca registrada de las siguientes definiciones mediante la utilización de un tipo TLV especial (127).

El fichero de configuración se considera una secuencia de octetos, siendo el bit menos significativo el bit 1 y el más significativo el bit 8.

El fichero de configuración cumplirá las siguientes reglas generales:

- 1) Los campos tipo TLV y SubTLV tendrán una longitud de 1 byte.
- 2) Los campos longitud TLV y longitud SubTLV tendrán una longitud de 1 byte.
- 3) Si el fichero de configuración no contiene un tipo TLV, se aplicará el valor por defecto del parámetro especificado por ese tipo TLV.
- 4) Cada definición TLV sólo puede contener un ejemplar de un cierto subtipo TLV.
- 5) Los subtipos TLV en un TLV se ordenan por orden ascendente de subtipo TLV.
- 6) No todos los SubTLV de un cierto tipo TLV son obligatorios; ciertas combinaciones pueden carecer de sentido. Ahora bien, la única directriz que se da es la utilización del sentido común.

- 7) Se pueden repetir las definiciones TLV para definir más entidades del mismo tipo.
- 8) Los parámetros se configuran en el orden en que aparecen en el fichero de configuración.
- 9) Los valores de los subtipos TLV *index* (índice) serán distintos para cada tipo TLV.
- 10) Los valores de TLV o sub-TLV no identificados se desestimarán sin reacción alguna.

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas
Relleno			0	N.A.			N.A.	Este TLV especial no contiene los campos longitud ni valor. Se utiliza para rellenar el fichero con un número entero de palabras, si fuera necesario. Su posición es después del campo fin de datos (TLV tipo = 255)
Descriptor de tráfico ATM			1	Variable (suma de campos sub TLV)			Composición de sub TLV	Este TLV se repite una vez por cada definición de descriptor de tráfico ATM
	<i>Índice</i>				1	1	Cualquiera	
	<i>Clase tráfico ATM</i>				2	1	0..3 (0 = CBR, 1 = UBR, 2 = VBRrt, 3 = VBRnrt)	
	<i>PCR</i>	<i>[Células/s]</i>			3	1..3	Cualquiera	
	<i>SCR</i>	<i>[Células/s]</i>			4	1..3	Cualquiera	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas
	<i>MBS</i>	<i>[Células]</i>			5	1, 2	Cualquiera	
Puerto ATM			2	Variable (suma de campos sub TLV)			Composición de sub TLV	Este TLV se repite una vez por cada puerto ATM
	<i>Índice</i>				1	1	Cualquiera	
	<i>Trayecto</i>				2	1	0, 1 (0 = Rápido, 1 = Entrelazado)	
	<i>VPI</i>				3	1, 2	0..4095	
	<i>VCI</i>				4	1, 2	0..65535	
	<i>Descriptor tráfico ATM</i>				5	1	Cualquiera	
	<i>F4 ccsink</i>				6	1	0, 1 (0 = deshabilitado, 1 = habilitado)	
	<i>F5 ccsink</i>				7	1	0, 1 (0 = deshabilitado, 1 = habilitado)	
	<i>Tipo AAL</i>				8	1	2, 5	
	<i>Encapsulado</i>				9	1	0, 1 (0 = VCMUX, 1 = LLC/SNAP)	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

<b>Nombre</b>	<b>Subnombre</b>	<b>Unidades</b>	<b>Valor del rótulo tipo TLV</b>	<b>Valor del rótulo longitud TLV</b>	<b>Valor del rótulo tipo SubTLV</b>	<b>Valor del rótulo longitud SubTLV</b>	<b>Valor del rótulo (Sub)TLV</b>	<b>Notas</b>
	<i>Protocolo</i>				10	1	0..3 (0 = Ethernet, 1 = IPoA, 2 = PPPoA, 3 = PPPoE)	
	<i>Tipo de Conexión</i>				11	1	0..7 (0 = Puente, 1 = PPPoE, 2 = Ruta traducida, 3 = Ruta no traducida, 4 = Cambio de canal, 5 = Gestión, 6 = Difusión, 7 = BLES)	
	<i>Subtipo conexión</i>				12	1	0..3 (0 = DSM-CC, 1 = IGMPv2, 2 = MPEG2AAL5, 3 = MPEG2UDP)	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas	
Puerto del encaminador			3	Variable (suma de campos sub TLV)			Composición de sub TLV		Este TLV se repite una vez por cada definición de puerto del encaminador
	<i>Índice</i>				1	1	Cualquiera		
	<i>Índice del puerto ATM</i>				2	1	Cualquiera		
	<i>Configuración IP</i>				3	1	0, 1 (0 = Estático, 1 = Dinámico)		
	<i>Dirección IP estática</i>				4	4	Cualquiera		
	<i>Máscara IP estática</i>				5	4	Cualquiera		
	<i>Protocolo de autenticación PPP por defecto</i>				6	1	0..2 (0 = Ninguno, 1 = PAP, 2 = CHAP)		
	<i>Intervalo para el eco LCP</i>	<i>[segundos]</i>			7	1	Cualquiera		
	<i>Dirección IPCP VTP facilitada por el VTP</i>				8	4	Cualquiera		

**Cuadro A.1/H.610 – Formato del fichero de configuración**

<b>Nombre</b>	<b>Subnombre</b>	<b>Unidades</b>	<b>Valor del rótulo tipo TLV</b>	<b>Valor del rótulo longitud TLV</b>	<b>Valor del rótulo tipo SubTLV</b>	<b>Valor del rótulo longitud SubTLV</b>	<b>Valor del rótulo (Sub)TLV</b>	<b>Notas</b>	
	<i>ID usuario PPP</i>				9	Cualquiera	Texto cualquiera	Texto codifi- cado UTF-8 IETF RFC 2279 [24]	
	<i>Contraseña PPP</i>				10	Cualquiera	Texto cualquiera	Texto codifi- cado UTF-8 IETF RFC 2279 [4]	
	<i>Nombre del servicio PPPoE</i>				11	Cualquiera	Texto cualquiera	Texto codifi- cado UTF-8 IETF RFC 2279 [4]	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas		
	<i>Nombre del concentrador de acceso PPPoE</i>					12	Cualquiera	Texto cualquiera	Texto codifi- cado UTF-8 IETF RFC 2279 [4]	
	<i>Activación NAT/PAT</i>					13	1	0, 1 (0 = Deshabilitado, 1 = Habilitado)		
	<i>Activación RIP</i>					14	1	0, 1 (0 = Deshabilitado, 1 = Habilitado)		
	<i>Tamaño MTU</i>					15	1, 2	0..1500		
Correspon- dencia del puerto descen- dente NAT/PAT en dirección local			4	Variable (suma de campos sub TLV)				Composición de sub TLV	Este TLV se repite una vez por cada correspondencia puerto-dirección	
	<i>Número de puerto descendente</i>					1	1, 2	Cualquiera		
	<i>Dirección IP local</i>					2	4	Cualquiera		

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas
Puerto puente			5	Variable (suma de campos sub TLV)			Composición de sub TLVs	Este TLV se repite una vez por cada definición de puerto puente
	<i>Índice del puerto ATM</i>				1	1	Cualquiera	
	<i>Filtrado</i>				2	1	0, 1 (0 = Ninguno, 1 = PPPoE)	
Encamina- miento	<i>Rotulado VLAN</i>				3	1	0, 1 (0 = Deshabilitado, 1 = Habilitado)	Este TLV se repite una vez por cada definición de ruta estática
	<i>Rótulo VLAN por defecto</i>				4	4	Cualquiera	
	<i>Dirección de destino</i>				1	4	Cualquiera	
	<i>Máscara de destino</i>				2	4	Cualquiera	Los sub TLV 3 y 4 son mutuamente exclusivos
	<i>Dirección del siguiente salto</i>				3	4	Cualquiera	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

<b>Nombre</b>	<b>Subnombre</b>	<b>Unidades</b>	<b>Valor del rótulo tipo TLV</b>	<b>Valor del rótulo longitud TLV</b>	<b>Valor del rótulo tipo SubTLV</b>	<b>Valor del rótulo longitud SubTLV</b>	<b>Valor del rótulo (Sub)TLV</b>	<b>Notas</b>
	<i>Índice del puerto encaminador</i>				4	1	Cualquiera	
	<i>Métrica</i>				5	1	Cualquiera	
Servidor DHCP			7	Variable (suma de campos sub TLV)			Composición de sub TLV	
	<i>Dirección de subred</i>				1	4	Cualquiera	
	<i>Máscara de subred</i>				2	4	Cualquiera	
	<i>Dirección IP agrupación de base</i>				3	4	Cualquiera	
	<i>Número de direcciones IP de agrupación</i>				4	1, 2	Cualquiera	
	<i>Activación de retransmisión DNS</i>				5	1	0, 1 (0 = Deshabilitado, 1 = Habilitado)	
	<i>DNS primario</i>				6	4	Cualquiera	
	<i>DNS secundario</i>				7	4	Cualquiera	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

<b>Nombre</b>	<b>Subnombre</b>	<b>Unidades</b>	<b>Valor del rótulo tipo TLV</b>	<b>Valor del rótulo longitud TLV</b>	<b>Valor del rótulo tipo SubTLV</b>	<b>Valor del rótulo longitud SubTLV</b>	<b>Valor del rótulo (Sub)TLV</b>	<b>Notas</b>
Mecanismo cambio de canal			8	Variable (suma de campos sub TLV)			Composición de sub TLV	
	<i>Protocolo cambio de canal</i>				1	1	0, 1 (0 = DSM-CC, 1 = IGMPv2)	
	<i>Intervalo de consulta del último miembro</i>	<i>[1/10 segundos]</i>			2	1	Cualquiera	
	<i>Número de consultas último miembro</i>				3	1	Cualquiera	
	<i>Intervalo de informe no solicitado</i>	<i>[1/10 segundos]</i>			4	1	Cualquiera	
	<i>Subred IP de clase D de canales difusión</i>				5	4	Cualquiera	
	<i>Máscara IP de clase D de canales difusión</i>				6	4	Cualquiera	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

Nombre	Subnombre	Unidades	Valor del rótulo tipo TLV	Valor del rótulo longitud TLV	Valor del rótulo tipo SubTLV	Valor del rótulo longitud SubTLV	Valor del rótulo (Sub)TLV	Notas	
Opciones específicas del fabricante			127	Variable (suma de campos sub TLV)			Composición de sub TLV		Este TLV se repite una vez por cada atributo específico del fabricante. Puede incluirse como un subTLV de TLV de tipos 1 a 8
	<i>Código del fabricante</i>				1	6	Cualquiera	Identificador único del fabricante asignador por IEEE (véase apéndice X); si no lo hubiere se utilizará este sub TLV	
	<i>Opción 1 del fabricante</i>				2	Específico del fabricante	Específico del fabricante		
	<i>Opción n del fabricante</i>				n + 1	Específico del fabricante	Específico del fabricante	$n \leq 254$	

**Cuadro A.1/H.610 – Formato del fichero de configuración**

<b>Nombre</b>	<b>Subnombre</b>	<b>Unidades</b>	<b>Valor del rótulo tipo TLV</b>	<b>Valor del rótulo longitud TLV</b>	<b>Valor del rótulo tipo SubTLV</b>	<b>Valor del rótulo longitud SubTLV</b>	<b>Valor del rótulo (Sub)TLV</b>	<b>Notas</b>
Comprobación de integridad del fichero de configuración			254	20			Cualquiera	El campo valor es el valor de troceo de 160-bit SHA FIPS 180-1 de todos los bytes anteriores del fichero de configuración. Se puede poner al final del marcador Fin de datos (TLV tipo = 255)
Marcador Fin de datos			255	N.A.			N.A.	Este TLV es especial y no tiene los campos Longitud y Valor. Se pone al final del fichero, antes de los campos de relleno (TLV tipo = 0).

## Anexo B

### MIB SNMP para la función cambio de canal

En este anexo se define la base de información de gestión (MIB) SNMP IETF RFC 3416 [29] que utiliza SMIV2 para gestionar la configuración de la función cambio de canal (CCF) contenida en la OLT/ONU. La MIB conoce el modelo de información de gestión (MIM) CCF definido en 14.5.

#### B.1 Relación con otras MIB

La MIB CCF contiene referencias a las siguientes MIB SNMP.

- La interfaz MIB IETF RFC 2863, que utiliza la OLT para describir el punto de referencia V y las interfaces S-R definidas en el modelo de referencia del sistema FS-VDSL. La channelTable hace referencia a la interfaz V y la customerTable hace referencia a la interfaz S-R.
- La MIB ATM IETF RFC 2515, que utiliza OLT para describir los puntos de duplicación de VCC ATM para la difusión de servicios de ocio en el punto de referencia V. La channelTable hace referencia a la VCC ATM para que la función CAC pueda verificar el ancho de banda necesario para un determinado canal de difusión.

#### B.2 Definición de la MIB

```
-- MIB for configuration management of the Channel Change Function
-- residing in the OLT/ONU.

CHANNEL-CHANGE-MIB DEFINITIONS ::= BEGIN
  IMPORTS
    RowStatus
      FROM SNMPv2-TC
    enterprises, MODULE-IDENTITY, OBJECT-TYPE, IPAddress
      FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
      FROM SNMPv2-CONF
    InterfaceIndex, InterfaceIndexOrZero
      FROM IF-MIB;

  channelChangeMib          MODULE-IDENTITY
    LAST-UPDATED            "200205121638Z"
    ORGANIZATION            "FS VDSL Architecture Experts Group"
    CONTACT-INFO
      "FS-VDSL Secretariat
      -- editor's note: enter correct address in here
      Email: teresa.marsico@fs-vdsl.net"
    DESCRIPTION
      "This module defines a MIB for managing the Channel
      Change Control Function within an OLT/ONU."
    ::= { fsVdsl 1 }

  fsan OBJECT IDENTIFIER ::= { enterprises 18479 }
  fsVdsl OBJECT IDENTIFIER ::= { fsan 1 }

  channelChangeMibObjects OBJECT IDENTIFIER ::= { channelChangeMib 1 }
  channelChangeMibNotifications OBJECT IDENTIFIER ::= { channelChangeMib 2 }

  -----
  --
  -- The Channel Table

  channelTable OBJECT-TYPE
    SYNTAX                SEQUENCE OF ChannelEntry
    MAX-ACCESS            not-accessible
    STATUS                current
```

```

DESCRIPTION
    "This defines the channels and associated ATM replication points (ATM VCCs) within
    the OLT/ONU. Note that the channel table supports both IP multicast addresses and
    DSM-CC program IDs as a means of channel lookup."
 ::= { channelChangeMibObjects 1 }

channelEntry OBJECT-TYPE
    SYNTAX                ChannelEntry
    MAX-ACCESS             not-accessible
    STATUS                 current
    DESCRIPTION
        "An entry in the channelTable represents a single channel."
    INDEX                 { channelId }
    ::= { channelTable 1 }

ChannelEntry ::= SEQUENCE {
    channelId              IpAddress,
    entitlementIndex       Integer32,
    networkPortId         InterfaceIndex,
    vpi                   Integer32,
    vci                   Integer32,
    channelAdminStatus     INTEGER,
    channelRowStatus      RowStatus
}

channelId OBJECT-TYPE
    SYNTAX                IpAddress
    MAX-ACCESS             not-accessible
    STATUS                 current
    DESCRIPTION
        "The channelId shall be a Class D IP address allocated to the multicast channel
        regardless of whether the channel is delivering video over UDP/IP multicast or
        AAL5. Where DSM-CC is used as the channel change protocol, this is also the DSM-CC
        Broadcast Program ID (BPID). This facilitates transparent mapping between the IGMP
        and DSM-CC channel change protocols."
    ::= { channelEntry 1 }

entitlementIndex OBJECT-TYPE
    SYNTAX                Integer32 ( 0 .. 4095 )
    MAX-ACCESS             read-create
    STATUS                 current
    DESCRIPTION
        "The value of this object is the key for performing conditional access. The value
        zero (0) is reserved and is allocated to a channel which is free and does not
        require conditional access to be performed. Note that a maximum of 4095 channels
        can be supported by this MIB."
    ::= { channelEntry 2 }

networkPortId OBJECT-TYPE
    SYNTAX                InterfaceIndex
    MAX-ACCESS             read-create
    STATUS                 current
    DESCRIPTION
        "The value of this object shall be equal to the ifIndex of the network interface
        in the OLT/ONU carrying the multicast channels. This is so that this object along
        with the vpi and vci objects below can be used as an index into the OLT's/ONU's
        ifTable to gather more information about the replication point(ATM VCC) such as
        peak bandwidth."
    ::= { channelEntry 3 }

vpi OBJECT-TYPE
    SYNTAX                Integer32 ( 0 .. 255 )
    MAX-ACCESS             read-create
    STATUS                 current
    DESCRIPTION
        "The value of this object is equal to the VPI allocated to
        the replication point (ATM VCC) in the OLT/ONU for this channel."
    ::= { channelEntry 4 }

vci OBJECT-TYPE
    SYNTAX                Integer32 ( 32 .. 65535 )
    MAX-ACCESS             read-create
    STATUS                 current
    DESCRIPTION
        "The value of this object is equal to the VCI allocated to
        the replication point (ATM VCC) in the OLT/ONU for this channel."

```

```

 ::= { channelEntry 5 }

channelAdminStatus OBJECT-TYPE
  SYNTAX          INTEGER {
                    locked ( 1 ),
                    unlocked ( 2 ),
                    shuttingDown ( 3 )
                  }
  MAX-ACCESS      read-create
  STATUS          current
  DESCRIPTION
    "This object is used to control the management state of this channel. When this
    object is set to locked(1) all existing customers connected to this channel shall
    be immediately disconnected and further join requests to this channel should be
    rejected. If this object is set to shuttingDown(3), no further join requests
    should be accepted for this channel; when all existing customers have disconnected
    from this channel the value of this object moves to locked(1)."
```

```

 ::= { channelEntry 7 }

channelRowStatus OBJECT-TYPE
  SYNTAX          RowStatus {
                    active ( 1 ),
                    notInService ( 2 ),
                    notReady ( 3 ),
                    createAndGo ( 4 ),
                    createAndWait ( 5 ),
                    destroy ( 6 )
                  }
  MAX-ACCESS      read-create
  STATUS          current
  DESCRIPTION
    "This object is used to manage row creation and deletion. When the
    channelAdminStatus is locked(1) the value of this object should be
    notInService(2). When the channelAdminStatus is unlocked(2) the value of this
    objects should be active(1) or notReady (3). When the value of channelAdminStatus
    is shuttingDown(3), the value of this object should be active(1)."
```

```

 ::= { channelEntry 8 }

-----
--
-- The Customer Table

customerTable OBJECT-TYPE
  SYNTAX          SEQUENCE OF CustomerEntry
  MAX-ACCESS      not-accessible
  STATUS          current
  DESCRIPTION
    "This defines the customers for broadcast entertainment
    services."
  ::= { channelChangeMibObjects 2 }

customerEntry OBJECT-TYPE
  SYNTAX          CustomerEntry
  MAX-ACCESS      not-accessible
  STATUS          current
  DESCRIPTION
    "An entry in the customerTable represents a single customer."
  INDEX          { onuId, customerPortId }
  ::= { customerTable 1 }

CustomerEntry ::= SEQUENCE {
  onuId           InterfaceIndexOrZero,
  customerPortId  InterfaceIndex,
  maxMulticastTraffic  Integer32,
  maxMulticastStreams  Integer32,
  untimedEntitlements1  OCTET STRING,
  untimedEntitlements2  OCTET STRING,
  grantEntitlement      IpAddress,
  revokeEntitlement     IpAddress,
  customerAdminStatus  INTEGER,
  customerRowStatus    RowStatus
}

onuId OBJECT-TYPE
  SYNTAX          InterfaceIndexOrZero
  MAX-ACCESS      not-accessible
  STATUS          current

```

```

DESCRIPTION
    "Describes uniquely the ONU to which the customer is attached. The value of this
    object shall be the ifIndex of the interface in the OLT that connects to the
    associated ONU. If the OLT/ONU are integrated then the value of this object shall
    be zero (0)."
```

```

 ::= { customerEntry 1 }

customerPortId OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Describes uniquely the port within the ONU/OLT to which the customer is attached.
        The value of this object shall be the ifIndex of the port to which the customer is
        attached."
```

```

 ::= { customerEntry 2 }

maxMulticastTraffic OBJECT-TYPE
    SYNTAX          Integer32
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object defines the maximum amount of bandwidth in kilobit/s allocated to
        broadcast entertainment services. The value shall be an integer multiple of 10kbps
        and shall not exceed the DSL line rate."
```

```

 ::= { customerEntry 3 }

maxMulticastStreams OBJECT-TYPE
    SYNTAX          Integer32
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object defines the maximum number of multicast streams that can be active
        simultaneously across a DSL UNI. A value of zero (0) is used to indicate that this
        object shall not be used as part of any decision making process for a channel
        change request."
```

```

 ::= { customerEntry 4 }

untimedEntitlements1 OBJECT-TYPE
    SYNTAX          OCTET STRING ( SIZE ( 0 .. 256 ) )
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is used as a bitmap to store untimed entitlements to premium
        channels. Note that the first bit of the first octet is reserved. Bits 1 to 2047
        correspond to entitlements for channels with entitlementIndex between 1 and 2047,
        respectively. In order to entitlement channel with entitlementIndex x, the value
        of bit x in this bitmap shall be 1. In order to revoke entitlement to channel with
        entitlementIndex y, the value of bit y in this bitmap shall be 0."
```

```

 ::= { customerEntry 5 }

untimedEntitlements2 OBJECT-TYPE
    SYNTAX          OCTET STRING ( SIZE ( 0 .. 256 ) )
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "In order to support a greater number of channels this object is used in the same
        way as untimedEntitlements1 but bits 0 to 2048 correspond to entitlements for
        channels with entitlementIndex between 2048 and 4095, respectively. The index into
        this bitmap is entitlementIndex - 2048."
```

```

 ::= { customerEntry 6 }

grantEntitlement OBJECT-TYPE
    SYNTAX          IpAddress
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "When granting entitlements to a single channel for many customers SNMP Setting
        the untimedEntitlement1/2 object leads to lots of management traffic due to the
        size of the untimedEntitlement1/2 object. In this situation it is much more
        bandwidth efficient to use this object. To grant an entitlement, the value of this
        object is SET to the channelId of the Channel for which entitlement is being
        granted to this customer. When this object is SET, the OLT/ONU shall automatically
        update the associated bit in the untimedEntitlement1/2 object to 1."
```

```

 ::= { customerEntry 7 }

revokeEntitlement OBJECT-TYPE
    SYNTAX          IPAddress
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "When revoking entitlements to a single channel for many customers SNMP Setting
        the untimedEntitlement1/2 object leads to lots of management traffic due to the
        size of the untimedEntitlement1/2 object. In this situation it is much more
        bandwidth efficient to use this object. To revoke an entitlement, the value of
        this object is SET to the channelId of the Channel for which entitlement is being
        revoked for this customer. When this object is SET, the OLT/ONU shall
        automatically update the associated bit in the untimedEntitlement1/2 object to
        zero (0)."
```

```

 ::= { customerEntry 8 }

customerAdminStatus OBJECT-TYPE
    SYNTAX          INTEGER {
                    locked ( 1 ),
                    unlocked ( 2 ),
                    shuttingDown ( 3 )
                    }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is used to control the management state of this customer. When this
        object is set to locked(1) all existing channels being delivered to this customer
        shall be immediately disconnected and further join requests from this customer
        shall be rejected. If this object is set to shuttingDown(3), no further join
        requests should be accepted from this customer; when all existing channels have
        been disconnected from this customer the value of this object moves to locked(1)."
```

```

 ::= { customerEntry 9 }

customerRowStatus OBJECT-TYPE
    SYNTAX          RowStatus {active ( 1 ),
                               notInService ( 2 ),
                               notReady ( 3 ),
                               createAndGo ( 4 ),
                               createAndWait ( 5 ),
                               destroy ( 6 )
                               }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is used to manage row creation and deletion. When the
        channelAdminStatus is locked(1) the value of this object should be
        notInService(2). When the channelAdminStatus is unlocked(2) the value of this
        objects should be active(1) or notReady (3). When the value of channelAdminStatus
        is shuttingDown(3), the value of this object should be active(1)."
```

```

 ::= { customerEntry 10 }

-----
--
-- The Timed Entitlement Table

timedEntitlementTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF TimedEntitlementEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "This table is used to store entitlements to channels that
        have a relatively short duration, such as PPV channels."
    ::= { channelChangeMibObjects 3 }

timedEntitlementEntry OBJECT-TYPE
    SYNTAX          TimedEntitlementEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry corresponds to timed entitlement for a single
        channel identified by the channelId. The same entry may
        be applicable to one or more customers as defined by
        the customerTimeEntitlementTable."
    INDEX          { timedEntitlementId }
    ::= { timedEntitlementTable 1 }

```

```

TimedEntitlementEntry ::= SEQUENCE {
    timedEntitlementId          Integer32,
    timedEntitlementChannelId IpAddress,
    startTime                   OCTET STRING,
    stopTime                    OCTET STRING,
    entitlementRowStatus        RowStatus
}

timedEntitlementId OBJECT-TYPE
    SYNTAX          Integer32 ( 0 .. 65535 )
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "Describes uniquely a timed entitlement."
    ::= { timedEntitlementEntry 1 }

timedEntitlementChannelId OBJECT-TYPE
    SYNTAX          IpAddress
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This has the value of the channelId of the channelEntry
        for which this timedEntitlementEntry is for."
    ::= { timedEntitlementEntry 2 }

startTime OBJECT-TYPE
    SYNTAX          OCTET STRING ( SIZE ( 0..16 ) )
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This is the time, expressed in UTC, from which time
        the channel is allowed to be viewed. When this time is
        less than or equal to the current time, the bit in the
        untimedEntitlement1/2 object corresponding to the channel
        for which this timedEntitlementEntry relates is set to 1."
    ::= { timedEntitlementEntry 3 }

stopTime OBJECT-TYPE
    SYNTAX          OCTET STRING ( SIZE ( 0..16 ) )
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This is the time, expressed in UTC, after which time
        the channel is not allowed to be viewed. When this time is
        less than the current time, the bit in the
        untimedEntitlement1/2 object corresponding to the channel
        for which this timedEntitlementEntry relates is set to
        zero (0). Once this is done this timedEntitlementEntry
        shall also be removed from this table in order to stop this
        table growing indefinitely. Note that the information may
        be archived by the management system for audit purposes."
    ::= { timedEntitlementEntry 4 }

entitlementRowStatus OBJECT-TYPE
    SYNTAX          RowStatus {active ( 1 ),
                                notInService ( 2 ),
                                notReady ( 3 ),
                                createAndGo ( 4 ),
                                createAndWait ( 5 ),
                                destroy ( 6 )
                                }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is used to manage row creation and deletion."
    ::= { timedEntitlementEntry 5 }

-----
--
-- The Customer Timed Entitlement Table

customerTimedEntitlementTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF CustomerTimedEntitlementEntry
    MAX-ACCESS      not-accessible
    STATUS          current

```

```

DESCRIPTION
    "This table defines the timed entitlements used by a
    customer as defined by the associated
    timedEntitlementEntry."
 ::= { channelChangeMibObjects 4 }

customerTimedEntitlementEntry OBJECT-TYPE
    SYNTAX CustomerTimedEntitlementEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry corresponds to a timed entitlement for a customer."
    INDEX { onuId, customerPortId, custTimedEntitlementId }
    ::= { customerTimedEntitlementTable 1 }

CustomerTimedEntitlementEntry ::= SEQUENCE {
    onuId InterfaceIndexOrZero,
    customerPortId InterfaceIndex,
    custTimedEntitlementId Integer32,
    custTimedEntitlementRowStatus RowStatus
}

onuId OBJECT-TYPE
    SYNTAX InterfaceIndexOrZero
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Describes uniquely the ONU to which the customer is
        attached. The value of
        this object shall be the ifIndex of the interface in the OLT that connects to the
        associated ONU. If the OLT/ONU are integrated then the value of this object shall
        be zero (0)."
    ::= { customerTimedEntitlementEntry 1 }

customerPortId OBJECT-TYPE
    SYNTAX InterfaceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Describes uniquely the port within the ONU/OLT to which the customer is
        attached.
        The value of this object shall be the ifIndex of the port to which the customer is
        attached."
    ::= { customerTimedEntitlementEntry 2 }

custTimedEntitlementId OBJECT-TYPE
    SYNTAX Integer32 ( 0..65535 )
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "This has the value of the timedEntitlementId for the
        timedEntitlementEntry that defined the timed entitlement
        to a channel for this customer."
    ::= { customerTimedEntitlementEntry 3 }

custTimedEntitlementRowStatus OBJECT-TYPE
    SYNTAX RowStatus {active ( 1 ),
        notInService ( 2 ),
        notReady ( 3 ),
        createAndGo ( 4 ),
        createAndWait ( 5 ),
        destroy ( 6 )
        }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "This object is used to manage row creation and deletion."
    ::= { customerTimedEntitlementEntry 4 }

-----
--
-- Channel Change Function traps

channelChangeMibNotificationPrefix OBJECT IDENTIFIER
    ::= { channelChangeMibNotifications 0 }

channelChangeCAFailed NOTIFICATION-TYPE
    OBJECTS { rejectedOnuId, rejectedCustomerPortId }
    STATUS current

```

```

DESCRIPTION
    "This trap is generated when conditional access fails for a
    requested channel change. The trap identifies the customer
    that issued the request."
 ::= { channelChangeMibNotificationPrefix 1 }

rejectedOnuId OBJECT-TYPE
    SYNTAX          InterfaceIndexOrZero
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "Identifies the ONU from which the rejected channel change
        request originated."
 ::= { channelChangeMibObjects 5 }

rejectedCustomerPortId OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "Identifies the DSL portfrom which the rejected channel
        change request originated."
 ::= { channelChangeMibObjects 6 }

caFailedNotificationStatus OBJECT-TYPE
    SYNTAX          INTEGER { enabled ( 1 ),
                             disabled ( 2 )
                             }
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object is used to enable and disable the sending of
        the channelChangeCAFailed trap."
 ::= { channelChangeMibObjects 7 }

-- -----
--
-- Conformance Information

channelChangeMibConformance OBJECT IDENTIFIER
 ::= { channelChangeMib 3 }

channelChangeMibCompliances OBJECT IDENTIFIER
 ::= { channelChangeMibConformance 1 }

channelChangeMibGroups OBJECT IDENTIFIER
 ::= { channelChangeMibConformance 2 }

-- compliance statements

channelChangeMibCompliance MODULE-COMPLIANCE
    STATUS          current
    DESCRIPTION
        "The compliance statement for SNMP entities that support
        the channel change function as specified in FS-VDSL SA
        specification.

        For a system to conform to this MIB it shall also implement:

        - ifTable from RFC 2863 to define the physical interfaces."

    MODULE -- this module
    MANDATORY-GROUPS {
        channelChangeBasicGroup
    }

    -- conditionally mandatory groups listed below, where the
    -- condition is given in the DESCRIPTION clause of the group.

    GROUP          channelChangeCACGroup
    DESCRIPTION
        "This group is mandatory if a Channel Change Function
        implements Connection Admission Control (CAC) for channel
        change requests."

    GROUP          channelChangeBasicCAGroup

```

```

DESCRIPTION
    "This group is mandatory if a Channel Change Function
    implements conditional access (CA) for up to 2047 channels
    and supports only untimed entitlements."

GROUP          channelChangeCA4095ChannelsGroup
DESCRIPTION
    "This group is mandatory if a Channel Change Function
    implements conditional access (CA) for up to 4095 channels."

GROUP          channelChangeCATimedEntitlementsGroup
DESCRIPTION
    "This group is mandatory if a Channel Change Function
    implements CA based on timed entitlements."

GROUP          channelChangeCANotificationsGroup
DESCRIPTION
    "This group is optional if CA is implemented by the Channel
    Change Function."

 ::= { channelChangeMibCompliances 1 }

-- Units of Conformance

channelChangeBasicGroup      OBJECT-GROUP
OBJECTS {
    channelId,
    networkPortId,
    vpi,
    vci,
    channelAdminStatus,
    channelRowStatus,
    onuId,
    customerPortId
}
STATUS      current
DESCRIPTION
    "A collection of objects required as a minimum to manage
    the Channel Change Control function."
 ::= { channelChangeMibGroups 1 }

channelChangeCACGroup        OBJECT-GROUP
OBJECTS {
    maxMulticastTraffic
}
STATUS      current
DESCRIPTION
    "A collection of objects required to support CAC."
 ::= { channelChangeMibGroups 2 }

channelChangeBasicCAGroup    OBJECT-GROUP
OBJECTS {
    maxMulticastStreams,
    entitlementIndex,
    untimedEntitlements1,
    grantEntitlement,
    revokeEntitlement,
    rejectedOnuId,
    rejectedCustomerPortId,
    caFailedNotificationStatus
}
STATUS      current
DESCRIPTION
    "A collection of objects required to support CA with only
    untimed entitlements. This group is sufficient to support
    conditional access for up to 2047 channels."
 ::= { channelChangeMibGroups 3 }

channelChangeCA4095ChannelsGroup  OBJECT-GROUP
OBJECTS {
    untimedEntitlements2
}
STATUS      current
DESCRIPTION
    "This group is required in addition to the
    channelChangeBasicCAGroup to support CA for up to 4095
    channels."
 ::= { channelChangeMibGroups 4 }

```

```

channelChangeCATimedEntitlementsGroup      OBJECT-GROUP
OBJECTS {
    timedEntitlementID,
    timedEntitlementChannelId,
    startTime,
    stopTime,
    entitlementRowStatus,
    custTimedEntitlementId,
    custTimedEntitlementRowStatus
}
STATUS      current
DESCRIPTION
    "This group is required in addition to the
channelChangeBasicCAGroup, and if applicable the
channelChangeCA4095ChannelsGroup, to support timed
entitlements."
 ::= { channelChangeMibGroups 5 }

channelChangeCANotificationsGroup      NOTIFICATION-GROUP
NOTIFICATIONS {
    channelChangeCAFailed
}
STATUS      current
DESCRIPTION
    "This group contains the notification used to inform
management that a conditional access request failed. This
group is optional if CA is implemented by the Channel
Change Function."
 ::= { channelChangeMibGroups 6 }

END

```

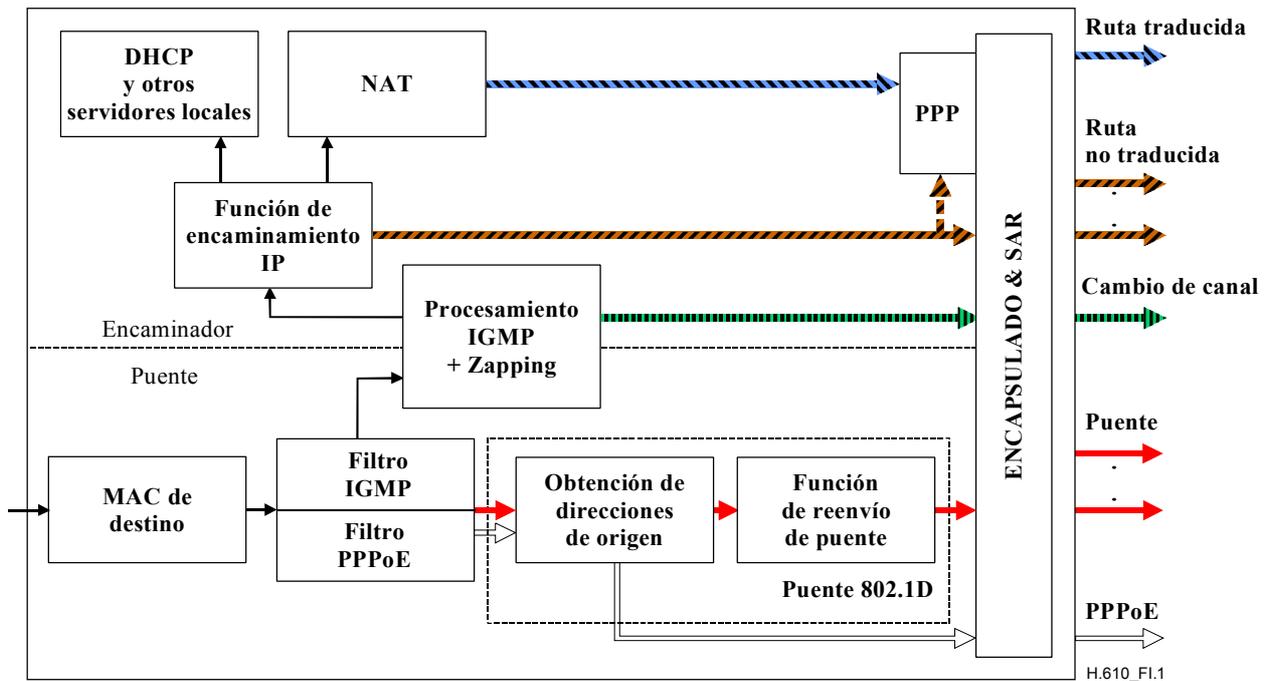
## Apéndice I

### Ejemplos de implementación del VTP

En este apéndice se da un ejemplo de implementación del VTP.

#### I.1 Procesamiento de protocolo ascendente

En la figura I.1 se describe el procesamiento de protocolo del tráfico ascendente que realiza un VTP. La parte izquierda indica la red residencial, la interfaz T<sub>CN</sub>. Se supone que el VTP está conectado a la red residencial en modo promiscuo, a saber, cada trama que se transmite por la red residencial la recibe el VTP. La parte derecha de la figura indica el lado de la red de acceso, la interfaz UR. Cuando aparece una sola flecha con nombre indica que se trata de una sola conexión VC ATM. Cuando aparecen más de una flecha sin nombre significa que pueden haber varias VC del mismo tipo.



**Figura I.1/H.610 – Procesamiento del protocolo ascendente del VTP**

Hay dos bloques comunes a todos los flujos de tráfico. El primero es el bloque encapsulado y SAR, que realiza el encapsulado RFC 2684, el procesamiento de subcapa AAL y la segmentación ATM. El segundo es la capa ATM, que realiza la puesta en cola y formación de células priorizadas.

El procesamiento de una trama entrante comienza en la capa 2. El primer paso es inspeccionar la dirección MAC de destino de la trama. Si ésta es idéntica a la dirección MAC del VTP, la trama se transfiere directamente al procesamiento de capa 3. De lo contrario, se trata de una trama difusión/multidifusión o una trama unidifusión que se ha de puentear. La función del siguiente módulo de capa 2, el filtro PPPoE, es separar tramas PPPoE y puenteadas que atraviesan el mismo encaminador o BRAS en diferentes VC ATM. Obsérvese que si las VC PPPoE y puenteadas terminan en encaminadores o BRAS diferentes, prácticamente se puede lograr la misma función de filtrado mediante la propia función puente. El módulo de filtrado PPPoE inspecciona el campo Ethertype de la trama recibida. Si se detecta una trama PPPoE (es decir, Ethertype = 0x8863 ó 0x8864), ésta se filtra y se entrega para la transmisión del tráfico PPPoE por la VC ATM dedicada a tal fin.

Asimismo, en esta etapa los mensajes IGMP de dirección de clase D asignados al servicio de medios de difusión (TV) se pasan al bloque de procesamiento IGMP y se transmiten los correspondientes mensajes cambio de canal (IGMP o DSM-CC) a la red de acceso por una VC dedicada a tal fin. Todas las demás tramas multidifusión IGMP o difusión distinta de PPPoE se reenvían al IP (capa 3) y a la función de reenvío puente. La obtención de la dirección MAC de origen se aplica a todas las tramas excepto a aquellas que el filtro IGMP ha desviado hacia el bloque de procesamiento IGMP. El bloque de reenvío puente realiza el reenvío de decisiones de acuerdo con las tablas puente de obtención (según un puente 802.1D normalizado).

Los paquetes reenviados a la función de encaminamiento IP causan una búsqueda en la tabla de encaminamiento. Se supone que la tabla de encaminamiento consiste en una correspondencia entre cada VC ATM encaminada y al menos una subred IP distinta (o computador central). La pasarela por defecto se configura para que sea la conexión encaminada traducida (si estuviera activa). Por consiguiente, aunque la conexión encaminada traducida se puede utilizar para la comunicación Internet, las VC encaminadas no traducidas sólo pueden utilizarse para la comunicación con intranet (es decir, redes o subredes específicas). El tráfico local, por ejemplo peticiones DHCP que

transportan la propia dirección IP del VTP o una dirección difusión, se filtran y se envían al procesamiento de protocolo local. Los paquetes encaminados hacia la pasarela por defecto pasan en primer lugar por el bloque NAT. La dirección IP pública que se utiliza para NAT se recibe durante el protocolo de control IP (IPCP), el cual es una parte normalizada del conjunto PPP.

En la figura no aparecen los flujos de gestión y BLES, y tampoco se describen en este ejemplo.

## I.2 Procesamiento de protocolo descendente

En la figura I.2 se describe el procesamiento de protocolo que se realiza en el sentido descendente. El primer bloque es el bloque encapsulado y SAR, que realiza el reensamblado ATM, el procesamiento de subcapa AAL y el desencapsulado RFC 684. Las VC ATM y el servicio TV difusión sólo son importantes en el sentido descendente, dado que son unidireccionales (es decir, son VC ATM punto multipunto). Las tramas que reciben las VC de difusión digital se envían directamente al controlador MAC para su transmisión. Las tramas que proceden de la VC PPPoE se reenvían al bloque de reenvío puente (es decir, esto es necesario cuando hay múltiples puertos físicos libres hacia la red residencial). Las tramas procedentes de VC puenteadas se pasan primeramente a través de la función puente (es decir, reenvío y obtención) y luego se envían para su transmisión. De los paquetes encaminados se encarga la función de encaminamiento IP (por ejemplo, ARP, etc.) y luego se reenvían al controlador MAC. Este mismo tratamiento reciben los paquetes generados localmente, por ejemplo respuestas DHCP. El bloque PPP se encarga de las sesiones PPP que funcionan por las conexiones encaminadas. Los paquetes en la salida del bloque PPP se envían a la función de encaminamiento directamente o a través del bloque NAT, el cual realiza la traducción de direcciones de red y de puerto.

En la figura no aparecen los flujos de gestión y BLES, y tampoco se describen en este ejemplo.

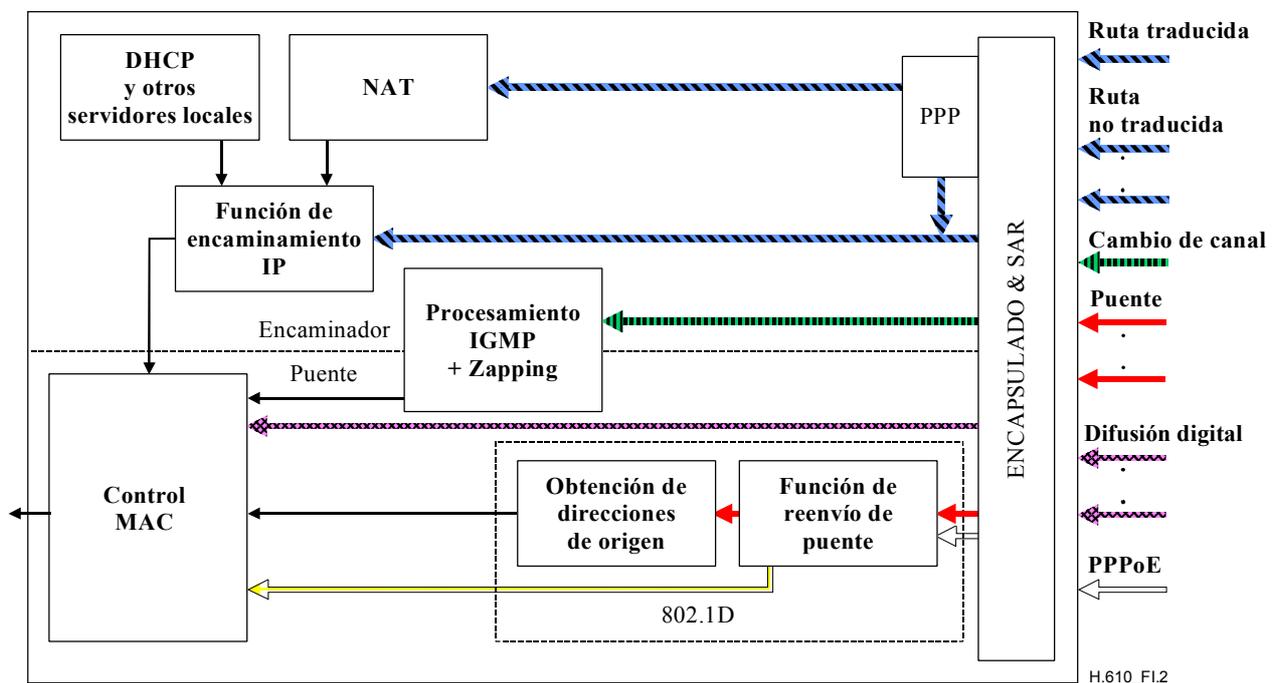
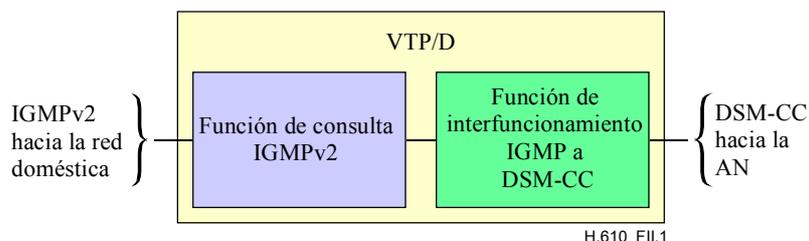


Figura I.2/H.610 – Procesamiento de protocolo en sentido descendente del VTP

## Apéndice II

### Función de traducción de IGMP v2 a DSMCC

En este apéndice se describe cómo se puede lograr el interfuncionamiento del VTP/D con los dos protocolos cambio de canal, IGMPv2 y DSM-CC. El interfuncionamiento podría realizarse por una función de interfuncionamiento IGMPv2-DSM-CC contenida en el VTP/D, como se describe en la figura II.1 siguiente.



**Figura II.1/H.610 – Arquitectura funcional cambio de canal DSM-CC del VTP/D**

En la siguiente discusión se supone que todos los mensajes IGMPv2 que procesa el bloque consulta IGMPv2 están relacionadas con el servicio de difusión digital.

La función consulta IGMPv2 supervisa el estado de cada canal multidifusión activo, como se define en la cláusula 14. De este modo se logra determinar si el canal multidifusión tiene algún miembro.

Dentro del DSM-CC es posible utilizar un solo mensaje para cambiar a un miembro de un canal multidifusión a otro. Al utilizar un solo mensaje la AN proporciona un cambio de canal más rápido y por consiguiente es posible reducir el tiempo total que se tarda en cambiar de canal. Además, puede mejorar el caudal total de cambio de canal y la calidad de funcionamiento de la AN. Ahora bien, el IGMPv2 utiliza dos mensajes para cambiar de canal, un mensaje abandono IGMP seguido de un mensaje llegada IGMP. Por consiguiente, la función interfuncionamiento necesita realizar lo siguiente para explotar la utilización de un solo mensaje DSM-CC.

- Al recibir un mensaje abandono IGMP, se inicia el temporizador "Join\_Anticipation". El valor por defecto de este temporizador puede ser de 200 ms.
- Si se recibe un mensaje llegada cuando todavía está funcionando el temporizador "Join\_Anticipation", éste se cancela. Seguidamente se genera un mensaje ProgramSelect DSM-CC que especifica la identidad de la sesión correspondiente con el antiguo canal y el nuevo Id del programa de difusión (BPID) necesario. Obsérvese que este funcionamiento no es óptimo cuando se transmiten simultáneamente múltiples trenes multimedios al mismo VTP/D.
- Si se recibe un mensaje llegada cuando el temporizador no está funcionando, se envía un mensaje ProgramSelect DSM-CC que especifica el Id de la nueva sesión y el BPID del canal que se solicita.
- Si el temporizador "Join\_Anticipation" expira, se envía un mensaje ProgramSelect DSM-CC que especifica el Id de la sesión correspondiente al canal que ya no se solicita y un BPID igual a "0".

NOTA – El BPID se determina a partir de la dirección multidifusión de clase D IP.

La optimización descrita *supra* permite la recepción simultánea de múltiples trenes de difusión digital.

## Apéndice III

### Soporte de canales de latencia dual VDSL

La capa física VDSL soporta los canales de latencia dual, conocidos comúnmente como el canal rápido y el canal entrelazado. El canal "rápido" tiene una baja latencia (normalmente 2 ms) pero su tasa de errores en los bits (BER, *bit error ratio*) es mayor, que puede deberse al ruido de impulso, en comparación con el canal "entrelazado". En cambio, el canal "entrelazado" tiene una mayor latencia (normalmente decenas de milisegundos) y una BER menor que puede deberse al ruido impulso. Esto se debe a que el canal entrelazado soporta el entrelazado de bloques y la corrección de errores en recepción de la cabida útil.

Es posible configurar la profundidad de entrelazado del canal entrelazado. La profundidad de entrelazado es directamente proporcional al retardo. Así pues, cuanto mayor sea la profundidad de entrelazado mayor será el retardo.

Normalmente el ancho de banda que se asigna a cada canal de latencia se determina estadísticamente. Las normas VDSL soportan la "redistribución dinámica de velocidad" (DRR, *dynamic rate re-partitioning*) que asigna dinámicamente el ancho de banda correspondiente a cada trayecto de latencia entre los dos canales de latencia. Sin embargo el DRR no se utiliza comúnmente debido a su complejidad.

Si se soportan los canales de latencia dual, el cuadro III.1 proporciona una posible correspondencia de aplicaciones en el canal de latencia dual VDSL. La selección entre un canal de latencia u otro presenta claramente un equilibrio entre el retardo y la tasa de errores en los bits.

**Cuadro III.1/H.610 – Correspondencia típica de aplicaciones a los canales de latencia dual VDSL**

Aplicación	Sensibilidad al retardo	Sensibilidad a la tasa de errores en los bits (BER)	Canal de latencia dual VDSL
Voz	Sí (nota 1)	No (nota 2)	Canal rápido preferiblemente.
Cambio de canal	Sí	Sí	Ninguno de los canales es el ideal. Se tiene que lograr un equilibrio entre el retardo y la tasa de errores en los bits.
Vídeo a la carta	No	Sí	Canal entrelazado, preferiblemente.
TV difusión	No	Sí	Canal entrelazado, preferiblemente.
Datos	No	No	Los dos canales son adecuados. Si los datos utilizan la categoría de servicio UBR, resulta ventajoso para el tráfico de datos compartir el mismo canal de latencia que el tráfico TV VoD/difusión para permitir que el servicio de datos utilice el ancho de banda libre de tráfico de TV VoD/difusión.

**Cuadro III.1/H.610 – Correspondencia típica de aplicaciones  
a los canales de latencia dual VDSL**

<b>Aplicación</b>	<b>Sensibilidad al retardo</b>	<b>Sensibilidad a la tasa de errores en los bits (BER)</b>	<b>Canal de latencia dual VDSL</b>
Juegos	Sí	Sí	Ningún canal es adecuado. Se tiene que encontrar un equilibrio entre el retardo y la tasa de errores en los bits.
<p>NOTA 1 – Comúnmente se tolera un retardo de 150 ms entre el habla y la escucha sin que haya una degradación de la calidad, si se utilizan técnicas de cancelación de ecos. El retardo que introduce el entrelazado es sólo uno de los aspectos que contribuyen al retardo general entre el habla y la escucha. Otras fuentes de retardo son el codificador de voz, el decodificador de voz, el retardo de empaquetado, el retardo de puesta en cola, etc.</p> <p>NOTA 2 – En función del códec de voz seleccionado.</p>			

El módem VDSL contenido en la ONU, o el VTP/D, no distingue entre las aplicaciones que transporta cada VCC ATM. El VTP/D y la ONU podrán utilizar el VPI ATM o los valores de las cabeceras de células ATM VPI/VCI correspondientes a la conexión ATM para hacer corresponder la cabida útil en el canal rápido o en el entrelazado VDSL.

Si se utiliza la correspondencia VPI ATM, se recomienda asignar por separado los VP ATM entrelazado y rápido. El tráfico correspondiente con el VP ATM se transporta por el canal entrelazado VDSL, mientras que el tráfico correspondiente al VP ATM rápido se transporta por el canal rápido VDSL. Se asigna una determinada VCC ATM al VP entrelazado o al rápido. Esta asignación debe depender de la naturaleza del tráfico de la aplicación que se transporta por ese VCC (véase el cuadro 1) (por ejemplo, las VCC de TV ATM de difusión que suelen transportar canales TV de difusión separados podrían utilizar el VP ATM entrelazado).

Si se utiliza la correspondencia VPI/VCI ATM, las VCC ATM separadas se asignan al canal entrelazado o al rápido VDSL en función del tráfico de aplicación que transporte esa VC (véase el cuadro *supra*).

Cabe observar que el soporte de canales de latencia dual aumenta la complejidad, dado que se ha de gestionar el ancho de banda entre los dos canales de latencia, y por consiguiente el soporte de esta capacidad puede traducirse en un aumento de los costos. Los operadores deben evaluar objetivamente los beneficios que se derivan de introducir la latencia dual en comparación con el aumento de la complejidad y de los costos. Obsérvese que no es obligatorio que el VTP/D o la ONU soporte más de un canal de latencia.

## Apéndice IV

### Configuraciones IP avanzadas

En este apéndice se describen configuraciones avanzadas de red residencial y se complementa lo descrito en la cláusula 12.

#### IV.1 Configuraciones avanzadas de procesamiento IP

Si el VTP/D tiene más de una conexión encaminada externa y/o hay más de una subred IP en la red residencial, el procesamiento IP ya no puede configurarse como una de las configuraciones

estándar. En esta subcláusula se describe la configuración por defecto de casos avanzados, que puede abarcar una gran variedad de situaciones de interconexión de redes IP.

El principio general en el que se basan los casos avanzados es que las configuraciones por defecto de cualesquiera conexiones externas adicionales y cualquier subred IP adicional siguen las mismas reglas básicas que en los casos estándar. La mayoría de las configuraciones específicas de los casos avanzados se establecen en los parámetros que se negocian a través de las conexiones externas y de las rutas que se añaden a la función de reenvío IP.

Estas configuraciones por defecto de la función de reenvío IP funcionan esencialmente del modo siguiente.

- Si sólo hay una red IP, cada conexión externa adicional da lugar a al menos una ruta adicional en la tabla de reenvío.
- Si hay más de una subred IP, la función de reenvío IP utiliza el concepto de encaminadores virtuales para separar las rutas en la tabla de reenvío de modo que cada ruta está relacionada únicamente con una subred IP.

NOTA – Para ello es necesario que cada conexión externa esté relacionada unívocamente con una subred IP.

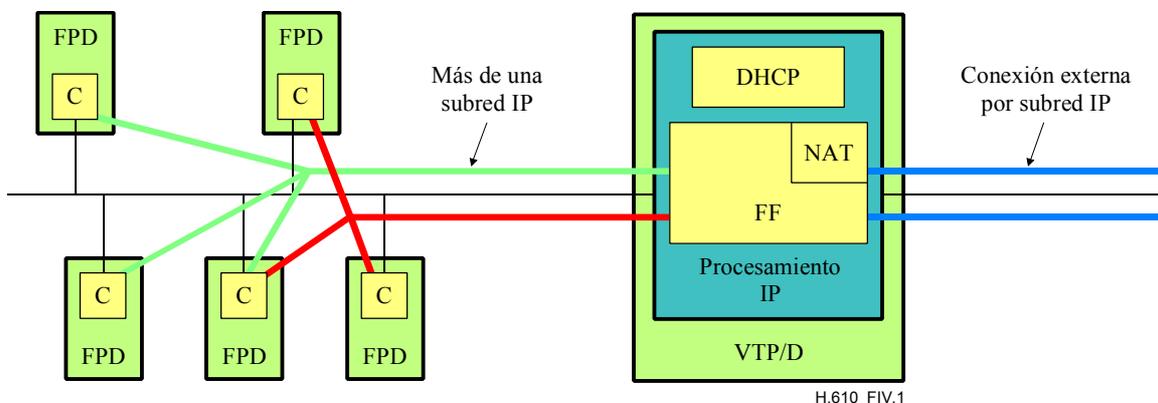
En aras de la claridad, en primer lugar se describe la configuración por defecto correspondiente a la visión de una subred IP, dado que ésta introduce el procedimiento correspondiente a los encaminadores virtuales. En la descripción de la configuración por defecto correspondiente a la adición de conexiones externas, es posible considerar el caso en el que sólo hay una subred IP como un caso especial en el que no son necesarios los encaminadores virtuales.

#### IV.1.1 Adición de una subred IP adicional

Esta configuración avanzada se ilustra en la figura IV.1 *infra*.

En esta configuración, el funcionamiento de las subredes IP existentes no varía por la creación de una nueva subred IP. Cada subred IP es en realidad totalmente independiente de las demás subredes IP.

Por consiguiente, cada subred IP se considera, desde el punto de vista de la configuración por defecto, como un caso estándar excepto que la condición determinante para crear una subred adicional no puede estar completamente automatizada y necesita un estímulo externo. Si bien podría realizarse una interpretación inteligente de los parámetros negociados por la conexión externa mediante PPP o DHCP, se prevé que la condición determinante procederá en última instancia de la interfaz de gestión.



C Cliente  
FF Función de reenvío

**Figura IV.1/H.610 – Configuración avanzada – adición de una subred IP**

La función de reenvío IP consta de un conjunto ortogonal de reglas de reenvío basadas en las gamas de direcciones de destino IP. Cada regla se denomina una ruta y el conjunto total de rutas se denomina tabla de reenvío.

En el encaminamiento virtual cada ruta pertenece a un encaminador virtual. Los paquetes que entran a la función de reenvío se identifican como pertenecientes a un encaminador virtual sobre la base de uno o más parámetros; sin embargo en esta Recomendación se basa únicamente en las interfaces de capa 2 entrantes y/o en la gama de direcciones de origen IP.

El ID del encaminador virtual apunta a un conjunto de listas de control de acceso; cada una de estas listas de control de acceso es una gama de direcciones de origen definida como direcciones origen s.s.s.s y una máscara de subred m.m.m.m o una interfaz de capa 2 entrante, por ejemplo ppp0, ppp1, ipoa0, eth1, etc.

La creación de una lista de control de acceso por defecto se hace de manera que la subred IP se identifica a una encaminador virtual mediante su gama de direcciones de origen (obtenidas a partir de los parámetros de subred IP) mientras que la conexión externa se identifica por su interfaz de capa 2 entrante.

El funcionamiento lógico de la función de reenvío IP en el encaminamiento virtual es el siguiente:

- El paquete entrante se compara con la lista de control de acceso para determinar el encaminamiento virtual.
- Las rutas que pertenecen al encaminador virtual se comprueban en orden, y cuando se encuentra una correspondencia, se pasa al puerto de salida especificado en la tabla de reenvío.
- Si no se encuentra una correspondencia en las rutas que pertenecen al encaminador virtual, el paquete se pasa al puerto definido como la ruta por defecto del encaminador virtual.

El cuadro IV.1 muestra el ejemplo de la tabla de reenvío que resulta de añadir una subred IP encaminable externamente a una configuración estándar con una subred IP con espacio exclusivo de direcciones privadas y en el cuadro IV.2 se muestra las listas de control de acceso correspondientes a cada encaminador virtual.

**Cuadro IV.1/H.610 – Ejemplo de tabla de reenvío de una subred IP añadida a una configuración estándar con espacio exclusivo de direcciones privadas**

ID del encaminador virtual	Gama de direcciones de destino		Enmascarado	Interfaz de capa 2 saliente
	Dirección de destino	Máscara de subred		
0	192.168.0.0	255.255.255.0	No	Interfaz de red residencial, por ejemplo, eth0
0	127.0.0.0	255.0.0.0	No	VTP/D – ruta en bucle
0	Ruta por defecto		Sí	Conexión externa encaminada traducida, por ejemplo, ppp0
1	x.x.x.x (obtenido a partir de IPCP o DHCP)	s.s.s.s (valor por defecto u obtenido a partir de IPCP o DHCP)	No	Interfaz de red residencial, por ejemplo, eth1

**Cuadro IV.1/H.610 – Ejemplo de tabla de reenvío de una subred IP añadida a una configuración estándar con espacio exclusivo de direcciones privadas**

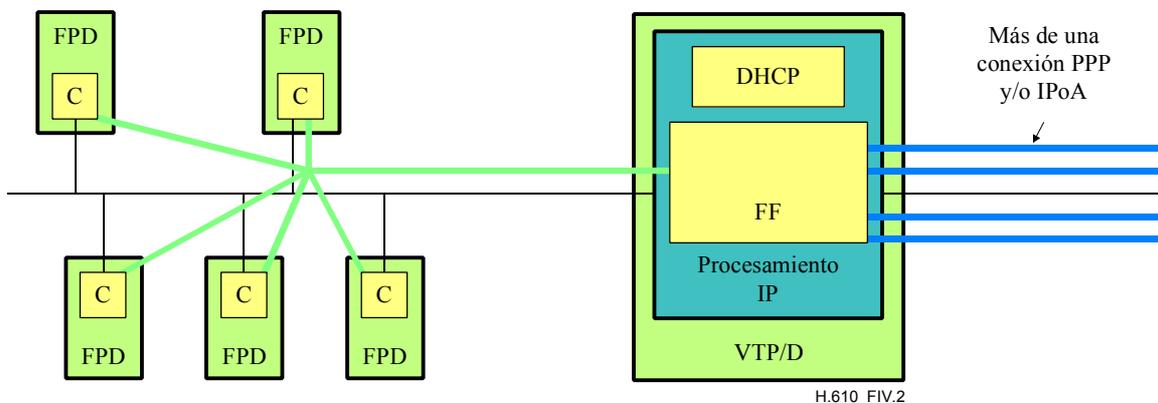
ID del encaminador virtual	Gama de direcciones de destino		Enmascarado	Interfaz de capa 2 saliente
	Dirección de destino	Máscara de subred		
1	127.0.0.0	255.0.0.0	No	VTP/D – ruta en bucle
1	Ruta por defecto		No	Conexión externa encaminada no traducida, por ejemplo, ppp1 o ipoa0

**Cuadro IV.2/H.610 – Ejemplo de listas de control de acceso con subred IP añadida a una configuración estándar con espacio exclusivo de direcciones privadas**

Gama de direcciones de origen		Interfaz de capa 2 entrante	ID del encaminador virtual
Dirección de origen	Máscara de subred		
192.168.0.0	255.255.255.0		0
		Conexión externa encaminada traducida, por ejemplo, ppp0	0
x.x.x.x (obtenida a partir de IPCP o DHCP)	s.s.s.s (valor por defecto u obtenido a partir de IPCP o DHCP)		1
		Conexión externa encaminada no traducida, por ejemplo, ppp1 o ipoa0	1

#### IV.1.2 Adición de una conexión externa adicional a una subred IP

El primer caso que hay que considerar es la adición de conexiones adicionales a una configuración estándar de subred IP. Esta situación se ilustra en la figura IV.2 *infra*.



C Cliente  
FF Función reenvío

**Figura IV.2/H.610 – Adición de conexiones a una subred IP**

Cuando la subred IP utiliza un espacio de direcciones encaminables externamente, es necesario añadir una nueva ruta a la tabla de reenvío cuando se añade una conexión externa adicional. De este modo los paquetes pueden pasar a través de esta conexión, cuando corresponda, hacia las direcciones alcanzables desde el extremo lejano. Cuando la conexión utiliza PPP, la configuración por defecto es que esta ruta se calcule a partir de la dirección del extremo lejano pasada al extremo lejano. Si al IPCP no se le puede pasar una máscara de subred, esta máscara se debe obtener a partir de la clase de la dirección de extremo lejano pasada (es decir 255.0.0.0 para una dirección de clase A, 255.255.0.0 para una dirección de clase B y 255.255.255.0 para una dirección de clase C).

La adición de conexiones adicionales a una subred con espacio exclusivo de direcciones privadas merece una atención especial. La manera en que estas conexiones se consideran depende del espacio de direcciones del otro extremo de la conexión.

- Si el espacio de direcciones del otro extremo de la conexión es otra subred con el mismo espacio exclusivo de direcciones (por ejemplo 192.168.1.0/24), la ruta correspondiente se puede añadir a la tabla de reenvío como se describió antes (sin que sea necesario el enmascaramiento adicional con NAT/PAT).
- Si el espacio de direcciones del otro extremo de la conexión es un espacio de direcciones distinto al de la subred IP o a la dirección en el extremo de la conexión normalizada (por ejemplo, 10.0.0.0 cuando la conexión normalizada está conectada a la Internet pública), la función de reenvío se puede configurar con una ruta (por ejemplo, 10.0.0.0 máscara de subred 255.0.0.0) para este espacio de direcciones mediante el enmascaramiento con NAT/PAT (separado del NAT/PAT utilizado para el espacio de direcciones de la Internet pública).
- Si el espacio de direcciones en el extremo de la conexión es el mismo que al final de la conexión estándar, la función de reenvío necesita definir una ruta adecuada para esa conexión. Cuando la conexión utiliza PPP, esta ruta se calcula a partir de la dirección pasada desde el otro extremo. Si al IPCP no se le puede pasar una máscara de subred, la máscara debe obtenerse a partir de la clase de la dirección que se le ha pasado. La ruta necesita utilizar el enmascarado con NAT/PAT.

En el cuadro IV.3 figuran las consecuencias de las reglas anteriores para la adición de conexiones PPP externas a los parámetros PPP y la negociación con el extremo lejano.

**Cuadro IV.3/H.610 – Parámetros de configuración por defecto de una conexión PPP subsiguiente a una subred IP**

<b>Parámetro</b>	<b>Valor por defecto</b>	<b>Otra posible configuración</b>
Encapsulado	PPP	No
Velocidad de mantenimiento activo LCP	Estático – 1 minuto	Valor estático mediante la interfaz de gestión
Autenticación	PAP	CHAP
Dirección IPCP del VTP facilitada por VTP	Obtenido – x.x.x.x (es decir dirección de la subred)	Configuración estática mediante la interfaz de gestión
Dirección IPCP del VTP facilitada por ER	Dirección desconocida	Acepta la dirección x.x.x.x facilitada
Dirección IPCP del ER facilitada por ER	Utiliza dirección para alimentar la tabla de reenvío	Dirección desconocida
Dirección IPCP del ER facilitada por VTP	No facilita dirección	No

**Cuadro IV.3/H.610 – Parámetros de configuración por defecto de una conexión PPP subsiguiente a una subred IP**

Parámetro	Valor por defecto	Otra posible configuración
Dirección IPCP del servidor DNS primario facilitada por ER	Dirección desconocida	Acepta la dirección x.x.x.x facilitada
Dirección IPCP del servidor DNS secundario facilitada por ER	Dirección desconocida	Acepta la dirección x.x.x.x facilitada

En el cuadro IV.4 se muestra un ejemplo de cuadro de reenvío. Este ejemplo corresponde al caso en el que la subred IP tiene un espacio de direcciones encaminables externamente, la conexión externa utiliza PPP y su IPCP pasa una dirección de subred.

**Cuadro IV.4/H.610 – Parámetros por defecto de la función de reenvío IP después de añadir una conexión externa PPP a una subred IP con espacio de direcciones encaminables externamente**

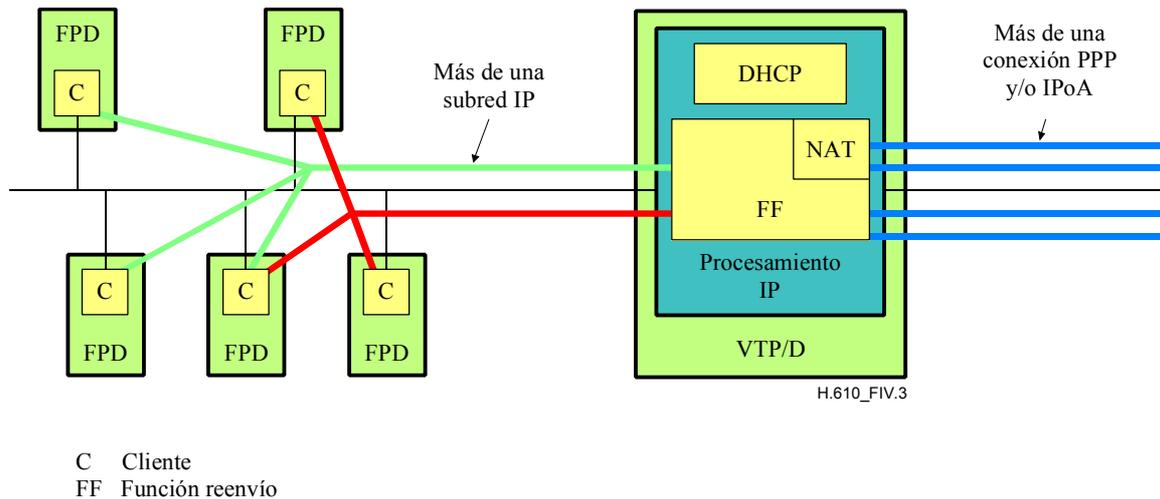
Gama de direcciones de destino		Enmascarado	Interfaz de capa 2 saliente
Dirección de destino	Máscara de subred		
x.x.x.x (obtenido a partir de los parámetros de subred)	s.s.s.s (obtenido a partir de los parámetros de subred)	No	Interfaz de red residencial, por ejemplo, eth0
y.y.y.y (obtenido a partir de la dirección pasada por IPCP por una conexión adicional)	y.y.y.y (parámetro pasado por IPCP por una conexión adicional)	No	Conexión externa adicional, por ejemplo, ppp1
127.0.0.0	255.0.0.0	No	VTP/D – ruta en bucle
Ruta por defecto		No	Conexión externa, por ejemplo, ppp0 o ipoa0

Si se utiliza IPoA para la conexión adicional a una subred IP, el valor por defecto es que no se añaden automáticamente nuevas entradas al cuadro de reenvío y todas las adiciones se añaden utilizando la configuración estática mediante la interfaz de gestión. Los parámetros por defecto de la conexión adicional que utiliza IPoA se describen en el cuadro IV.5.

**Cuadro IV.5/H.610 – Parámetros de una subsiguiente conexión IPoA a una subred**

Parámetro	Valor por defecto	Reconfiguración
Encapsulado	IPoA (Modo de encaminamiento RFC 2684)	No
Protocolo de configuración	Ninguno	No
Protocolo de encaminamiento	Encaminamiento estático	Habilitación de RIPv2 opcional

Como la figura IV.3 *infra* ilustra, se pueden dar otros escenarios cuando hay más de una subred IP.



**Figura IV.3/H.610 – Adición de conexiones a una subred IP cuando hay más de una subred IP**

Estos casos se pueden describir como múltiples ejemplares del escenario mostrado en la figura IV.1, dado que las subredes IP se mantienen completamente separadas utilizando encaminadores virtuales, para lo cual se utilizarán las reglas para la creación de subredes adicionales.

## Apéndice V

### Gráficos de secuencias de mensajes

En este apéndice se describe un conjunto de ejemplos de gráficos de frecuencias de mensajes (MSC, *message sequence charts*) que describen casos típicos que han de soportar el VTP y la red FS-VDSL.

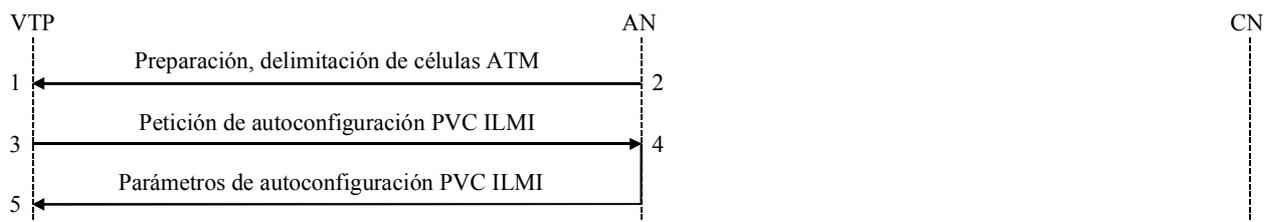
En cada MSC se incluyen anotaciones que describen los procedimientos de alto nivel y ayudan a comprenderlos.

#### V.1 Inicialización del VTP

Este escenario describe el flujo que se produce cuando el VTP se inicializa en frío, por ejemplo cuando se prende el VTP o éste se inicializa debido a un mal funcionamiento.

##### Condiciones previas:

Ninguna.



H.610\_FV.1

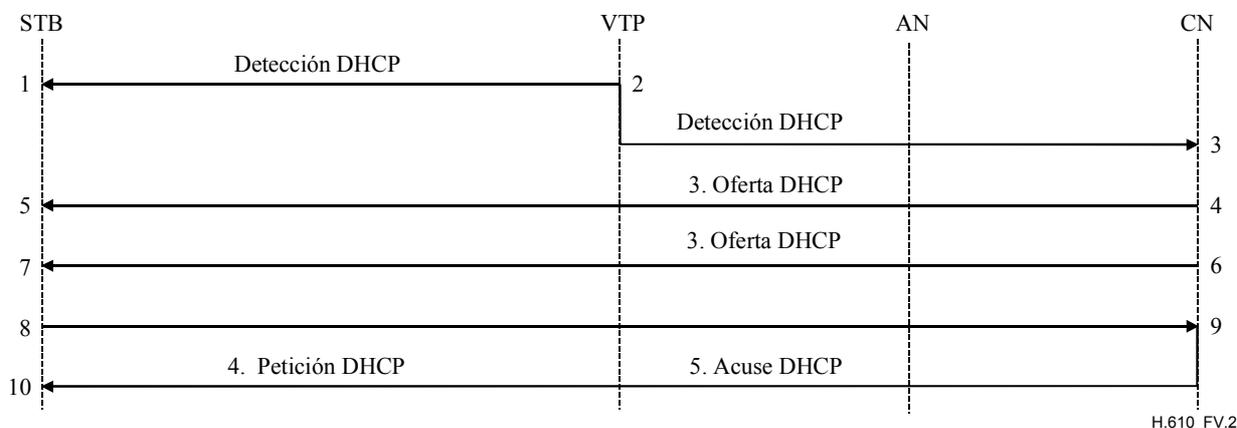
- 1 Se prende y reinicializa el VTP. El VTP se prepara para lo cual negocia y se pone de acuerdo sobre los parámetros de capa física VDSL, por ejemplo el ancho de banda en sentido ascendente y descendente. Una vez el VTP y la AN están preparados, comprueban la delimitación de células ATM para confirmar que pueden intercambiar células ATM por la interfaz VDSL.
- 2 La AN se prepara, como se describe en el apartado 1.
- 3 El VTP realiza una petición de autoconfiguración VPC ILMI (interfaz de gestión local integrada) por la VCI de valor habitual "16". Gracias a esta petición, el VTP puede determinar las VC ATM que se han configurado y su correspondiente descriptor de tráfico para cada una de estas VC.
- 4 La AN responde con los parámetros de configuración de la VC ATM. Para mayor información véase Specification af-ilm-0065.00.
- 5 El VTP guarda los parámetros de configuración ATM que identifican las VCC ATM que se han establecido y sus correspondientes descriptores de tráfico.

## V.2 Inicialización del STB

Este escenario describe la inicialización del adaptador multimedia (STB), por ejemplo cuando se prende el STB o se reinicializa debido a un mal funcionamiento del mismo.

### Condiciones previas:

Ninguna.



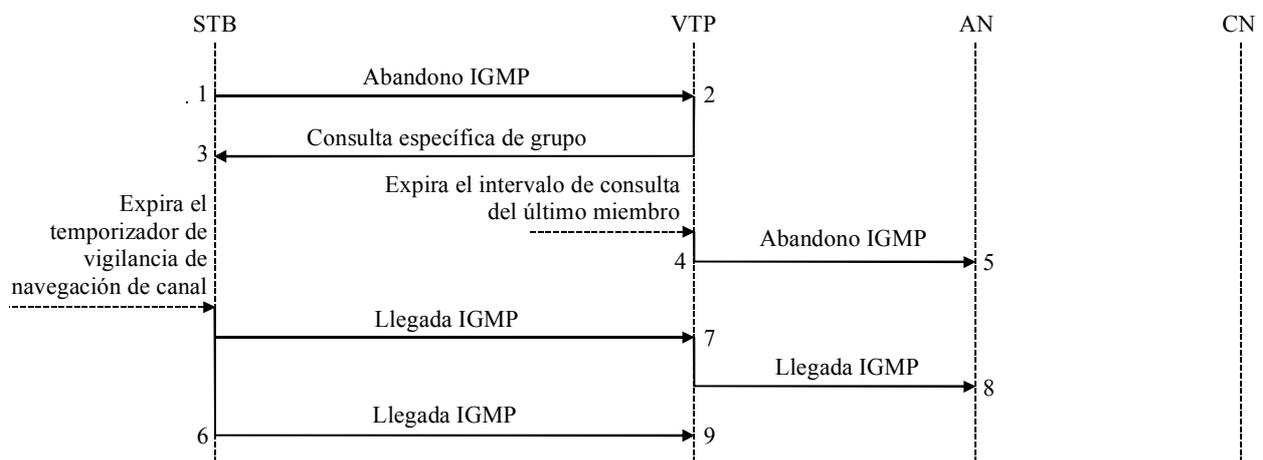
- 1 El STB solicita a la red una dirección IP y otros parámetros de configuración. El paquete de detección DHCP contiene la dirección de difusión IP de destino (255.255.255.255) y la cadena "FS-VDLS STB" de servicio identificador de clase de fabricante.
- 2 El servidor DHCP ubicado en el VTP hace caso omiso del paquete de detección DHCP dado que, como se describe en 10.3.4, está configurado para hacer caso omiso de paquetes DHCP que contengan identificador de clase de fabricante. *Si el VTP está funcionando en modo puente, el paquete de detección DHCP se envía a todas las VC ATM puenteadas.*
- 3 Uno o varios servidores DHCP reciben y procesan la detección DHCP.
- 4, 6 Uno o varios servidores DHCP ubicados en la red principal responden con una oferta DHCP que incluye una dirección IP disponible. La red principal quizá incluya un agente de retransmisión DHCP para retransmitir los paquetes DHCP de difusión a los servidores DHCP necesarios, lo cual mejora la escalabilidad y la seguridad.
- 5, 7 El STB elige un servidor DHCP adecuado de la lista de los que han respondido con una oferta DHCP.
- 8 El STB selecciona un servidor DHCP de la lista de peticiones de oferta DHCP que ha recibido. Para ello envía un paquete de petición DHCP con la dirección de difusión IP de destino (255.255.255.255) e incluye la dirección del servidor elegido en el campo "dirección IP del servidor" del paquete DHCP, en el que incluirá además la cadena de servicio de identificador de clase de fabricante como se describe en 10.3.4. La razón por la que se difunde la petición es para que se pueda notificar a los servidores DHC que no han sido elegidos. *Si el VTP está funcionando en modo puente, el paquete petición DHCP se envía a todas las VC ATM puenteadas.*
- 9 El servidor elegido reconoce su dirección IP en el campo "dirección IP del servidor" del paquete de petición DHCP y responde con un acuse DHCP que contiene los siguientes parámetros de configuración: dirección IP, máscara de subred, pasarela por defecto, servidores DNS primario y secundario.
- 10 El STB guarda los parámetros de configuración recibidos durante el periodo de usufructo. El STB puede utilizar estos parámetros para realizar algunas de las siguientes tareas:
  - Descargar programas informáticos mediante, por ejemplo, TFTP/FTP.
  - Seleccionar el canal TV y VoD de difusión como se describe en los últimos diagramas MSC.
  - Navegar por Internet.

### V.3 Cambio de canal TV de difusión – IGMP entre el VTP y la AN

En este escenario se describe el flujo cuando el usuario cambia de canal de TV y el protocolo de cambio de canal entre el VT y la AN es IGMP.

#### Condiciones previas:

- El VTP y el STB se han inicializado satisfactoriamente.
- El STB está recibiendo un canal TV de difusión.



H.610\_FV.3

- 1 El usuario de extremo está viendo un canal TV de difusión y selecciona otro canal TV de difusión. El STB solicita la desconexión de las secuencias TV de difusión seleccionadas antes. Para ello emite un mensaje abandono IGMP que contiene la dirección multidifusión IP del canal del que se va a desconectar. Además el STB inicia un "temporizador de control de zapping" para prevenir la generación innecesaria de mensajes de llegada IGMP en caso de que el usuario esté zapeando.
- NOTA 1 – El funcionamiento y valor de este temporizador depende de la aplicación y queda fuera del alcance de esta Recomendación.
- 2 Después de recibir un mensaje "abandono IGMP" el VTP comprueba si hay otros STB que quieren recibir el canal multidifusión, para lo cual envía una consulta específica de grupo IGMP y pone en marcha un temporizador de intervalo "lastmemberquery" (consulta al último miembro).
- 3 Todos los STB que no son miembros del grupo multidifusión especificado en el mensaje hacen caso omiso de la consulta específica de grupo.
- 4 Expira el temporizador de intervalo "lastmemberquery" y el VTP genera un mensaje abandono IGMP dirigido a la AN en el que especifica que el grupo de multidifusión no tiene ningún miembro.
- 5 Tras recibir el mensaje "abandono IGMP" la red de acceso deja de enviar al VTP secuencias del canal multidifusión especificado.
- 6 Después de la expiración del temporizador "Control de zapping" el STB genera un mensaje de llegada IGMP, en el que se indica el canal multidifusión que ha seleccionado el usuario de extremo. El STB permite generar un segundo mensaje IGMP para el caso en que se pierda el primero (como se indica en la variable robustez en IETF RFC 2236).
- 7 Tras recibir el mensaje de llegada IGMP, el VTP comprueba si hay algún miembro que pertenezca al grupo multidifusión especificado en dicho mensaje. Como no hay miembros, el mensaje llegada IGMP se reenvía a la red de acceso.
- 8 Después de recibir el mensaje llegada IGMP, la red de acceso comprueba si la derivación DSL tiene el derecho de unirse al grupo multidifusión seleccionado. Esto sólo es posible cuando la AN incorpora acceso condicional. En ese caso se asegurará de que la derivación DSL tiene capacidad suficiente para el canal especificado, en cuyo caso se adjuntará una VC ATM de TV de difusión gratuita a la fuente multidifusión especificada en el mensaje llegada IGMP. Esto causará el reenvío de secuencias de difusión al VTP.
- 9 El VTP hace caso omiso del segundo mensaje llegada IGMP, pues ya existe un miembro del grupo multidifusión especificado en dicho mensaje (que fue resultado del primer mensaje).

NOTA 2 – El VTP filtra mensajes IGMP recibidos por la interfaz  $T_{CN}$  que concuerdan con alguna dirección multidifusión correspondiente a la secuencia TV de difusión.

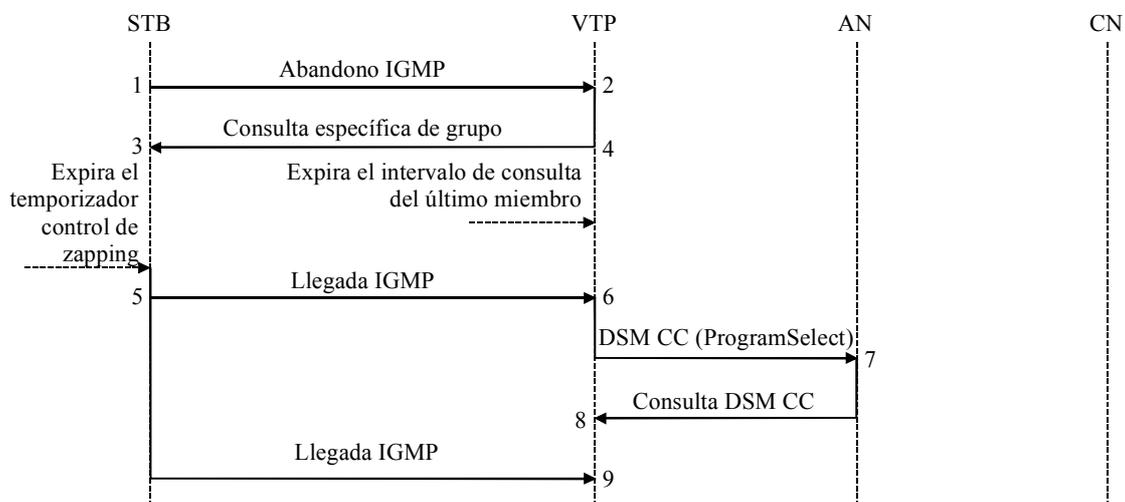
NOTA 3 – Los mensajes IGMP que se envían entre el VTP y la AN se transportan por una VCC ATM de cambio de canal dedicada a este fin.

#### V.4 Cambio de canal de TV de difusión – DSM-CC entre el VTP y la AN

Este escenario describe el flujo cuando el usuario cambia de canal de TV y el protocolo de cambio de canal utilizado entre el VTP y la AN es el protocolo de DSM-CC.

##### Condiciones previas:

- El VTP y el STB se han inicializado satisfactoriamente.
- El STB está recibiendo un canal TV de difusión.



H.610\_FV.4

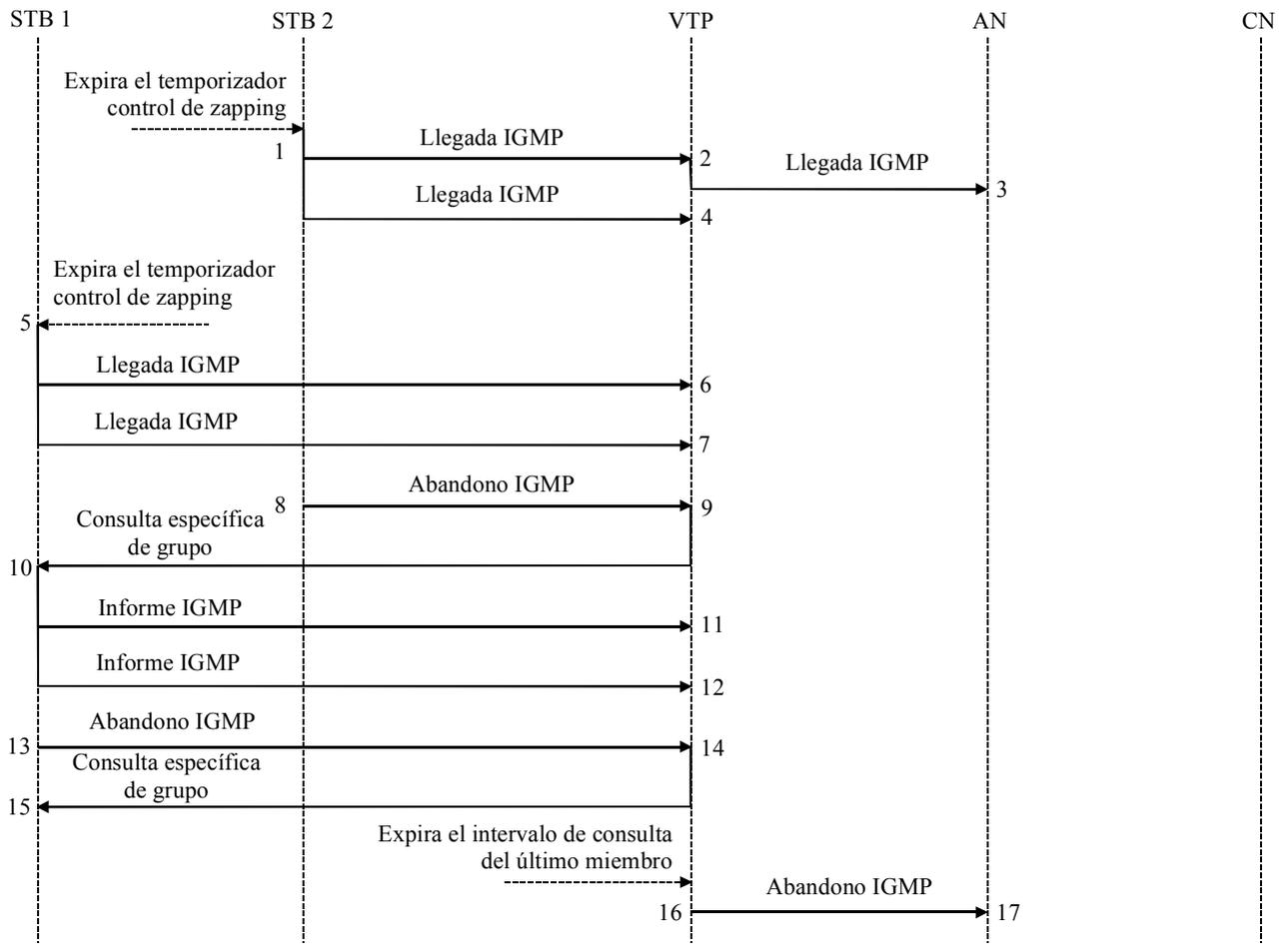
- 1 De acuerdo con el paso 1 de la secuencia V.3.
  - 2 De acuerdo con el paso 2 de la secuencia V.3.
  - 3 De acuerdo con el paso 3 de la secuencia V.3.
  - 4 Expira el temporizador de intervalo "lastmemberquery" y el VTP inicia el temporizador "JoinAnticipation", de manera que es posible enviar un único mensaje DSM-CC para realizar una operación "move" (activación). La operación "move" desconecta la VC ATM de difusión de su grupo multidifusión existente y la conecta al nuevo grupo multidifusión. De este modo se logra optimizar el funcionamiento de la AN.  
Para lograr esta optimización el temporizador "JoinAnticipation" debe ser de duración mayor que el temporizador "control de zapping" incorporado en el STB.
  - 5 De acuerdo con el paso 6 de la secuencia V.3.
  - 6 Después de recibir el primer mensaje llegada IGMP el VTP comprueba si hay algún miembro existente correspondiente al grupo multidifusión que especifica dicho mensaje. Dado que no hay ninguno, se cancela el temporizador "JoinAnticipation" y se envía el mensaje DSM CC (ProgramSelect) a la red de acceso que contiene el Id de programa de difusión (BPID) y a la entidad de sesión correspondiente al canal anterior que se estaba viendo.  
El BPID es una copia de la dirección multidifusión recibida en el mensaje llegada IGMP.
  - 7 Tras recibir el mensaje DSM CC (ProgramSelect) la red de acceso desconecta la VC ATM de TV de difusión del grupo multidifusión anterior. Si la red de acceso soporta el acceso condicional, se comprueba si la derivación VDSL tiene derecho a ver el VPID solicitado. Por último conecta la VC de TV de difusión a la nueva fuente multidifusión especificado por el BPID.  
Esto da lugar al reenvío de secuencias multidifusión solicitadas al VTP. Además, la AN envía un mensaje DSM CC ACK (acuse) en el que indica la VC ATM que se utilizará para entregar el Id del programa de difusión (BPID).
  - 8 El VTP observa que la AN comienza a reenviar las secuencias de difusión. El VTP reconoce además la VC que se utilizará para entregar el BPID.  
*El VTP necesita conocer esta información cuando se utiliza el transporte MPEG2/AAL5, de manera que el VTP pueda insertar la dirección de clase multidifusión IP adecuada en las secuencias que envíe por la interfaz T<sub>CN</sub>.*
  - 9 De acuerdo con el paso 9 de la secuencia V.3.
- NOTA 1 – El VTP filtra los mensajes IGMP que reciba por la interfaz T<sub>CN</sub> que concuerden con alguna de las direcciones multidifusión correspondientes a las secuencias TV de difusión.
- NOTA 2 – Los mensajes DSCM CC enviados entre el VTP y la AN se transportan por una VCC ATM de cambio de canal dedicada para este fin.

## V.5 Varios STB zapeando TV de difusión – IGMP entre VTP y AN

Este escenario describe el caso en el que dos STB dentro de la misma red residencial están viendo el mismo canal de TV. Esta secuencia ilustra la optimización IGMP que realiza el VTP.

### Condiciones previas:

- El VTP, el STB 1 y el STB 2 se han inicializado satisfactoriamente.
- El STB 1 y el STB 2 todavía no están recibiendo ningún canal de TV de difusión.



H.610\_FV.5

- 1 El usuario de extremo 2 selecciona un canal TV de difusión y comienza a contar el temporizador "control de zapping".  
Tras expirar este temporizador, el STB 2 genera un mensaje llegada IGMP que especifica la dirección del grupo multidifusión que el usuario ha seleccionado. El STB 2 también genera un segundo IGMP por si se pierde el primero (de acuerdo con la variable robustez especificada en RFC2236).
- 2 De acuerdo con el paso 7 de la secuencia V.3.
- 3 De acuerdo con el paso 8 de la secuencia V.3.
- 4 De acuerdo con el paso 9 de la secuencia V.3.
- 5 El usuario de extremo 1 selecciona el mismo canal de TV de difusión que el usuario de extremo 2 y comienza a contar el temporizador "control de zapping".  
Tras la expiración de este temporizador, el STB 1 genera un mensaje llegada IGMP en el que especifica el grupo multidifusión, que es el mismo que el especificado por el STB 2. El STB 1 genera además un segundo mensaje IGMP por si se pierde el primero (de acuerdo con la variable robustez especificada en RFC 2236).
- 6 El VTP determina que ya existe un miembro (es decir, el STB 2) del mismo grupo multidifusión. Por consiguiente no se envía el mensaje llegada IGMP a la AN.
- 7 De acuerdo con el paso 6 de la secuencia V.3.
- 8 El usuario de extremo 2/STB2 se desconecta del canal TV de difusión. El STB2 envía un mensaje abandono IGMP al VTP indicándole de esta manera que el grupo de multidifusión ya no se necesita.
- 9 El VTP realiza una consulta específica de grupo e inicia el temporizador de intervalo "lastmemberquery" para comprobar si otro STB pide ser miembro del grupo de multidifusión.
- 10 El STB 1 determina que todavía se necesita el canal multidifusión especificado por la consulta específica de grupo. Genera un informe y envía otro informe por si se pierde el primero (como se indica en la variable robustez de RFC 2236).
- 11 El VTP observa que el miembro del grupo multidifusión todavía se necesita.
- 12 El VTP hace caso omiso del mensaje llegada IGMP, puesto que ya hay un miembro del grupo multidifusión.
- 13 El usuario de extremo 1/STB1 se desconecta del canal TV de difusión. El STB1 envía un mensaje abandono IGMP al VTP indicándole el grupo multidifusión que ya no se necesita.
- 14 Tras recibir el mensaje "abandono IGMP" el VTP comprueba si todavía hay otros STB interesados en recibir el canal multidifusión, para lo cual realiza una consulta específica de grupo IGMP e inicia el temporizador de intervalo "lastmemberquery".
- 15 Todos los STB hacen caso omiso de la consulta específica de grupo, dado que ninguno de ellos son miembros del grupo multidifusión especificado en el mensaje.
- 16 Expira el temporizador de intervalo "lastmemberquery" y el VTP envía un mensaje abandono IGMP a la AN especificándole que el grupo multidifusión ya no tiene miembros.
- 17 Tras recibir el mensaje "abandono IGMP" la red de acceso deja de enviar al VTP las secuencias del canal multidifusión especificado.

NOTA 1 – El VTP filtra todos los mensajes IGMP recibidos por la interfaz  $T_{CN}$  que concuerdan con algunas de las direcciones multidifusión correspondientes a la secuencia de TV de difusión.

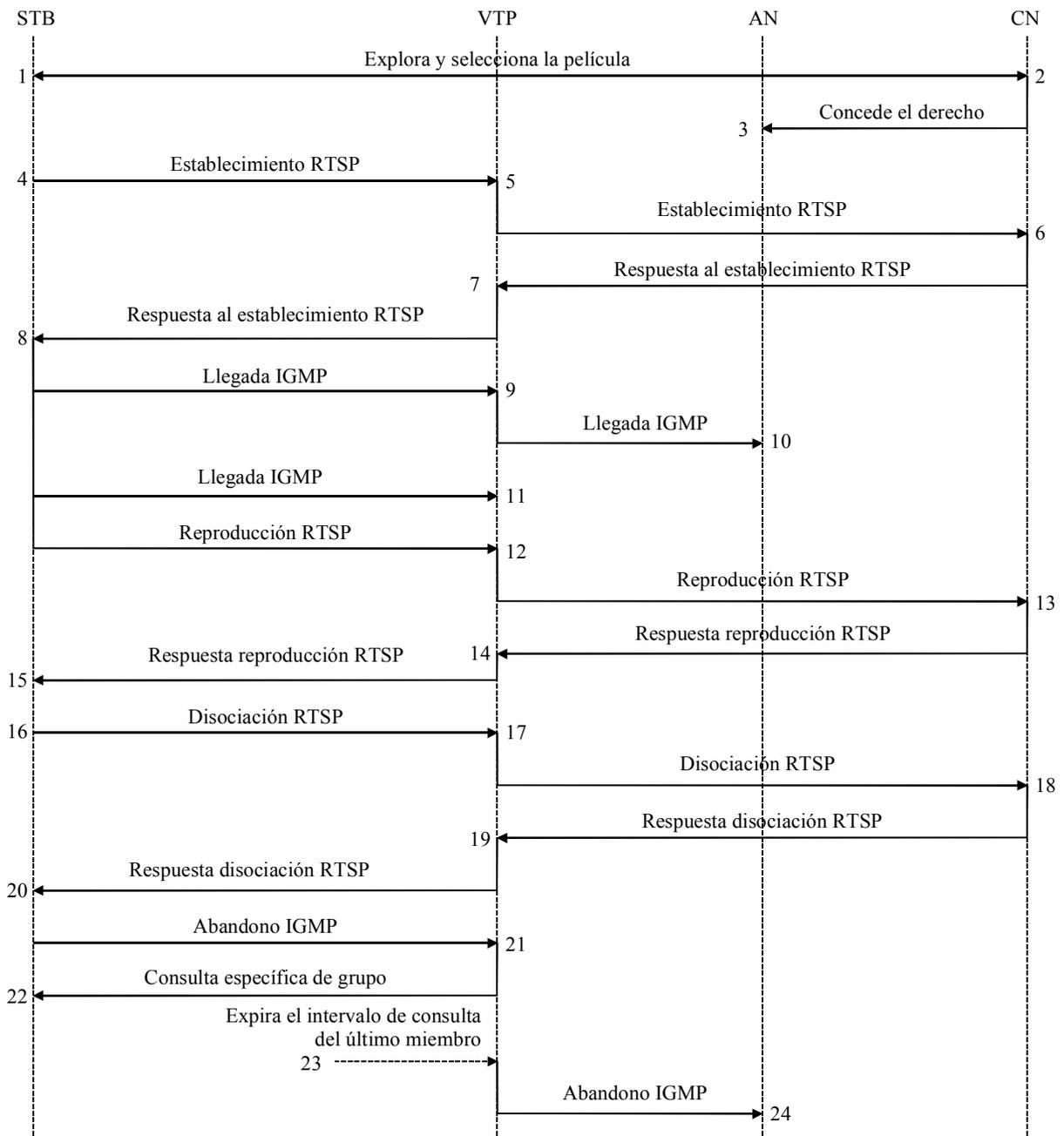
NOTA 2 – Los mensajes IGMP enviados entre la VTP y la AN se transportan por una VCC ATM de cambio de canal dedicada para esa función.

## V.6 Selección de la película VoD – Entrega multidifusión IP

En este escenario se describe el flujo de mensajes cuando el usuario selecciona una película VoD que se entrega mediante multidifusión IP. La película se termina de transmitir cuando el usuario lo decide o cuando la película llega a su fin.

### Condiciones previas:

- El VTP y el STB se han inicializado satisfactoriamente.
- El STB todavía no está recibiendo ninguna película VoD.



H.610\_FV.6

- 1 El usuario de extremo explora el directorio de contenido y selecciona una película VoD.
- 2 El gestor de TV de la red principal autentica el usuario, acepta la compra y devuelve un URI válido para la película al STB. Si la AN dispone de acceso condicional, se concede a la AN el derecho para la película VoD seleccionada.
- 3 La AN concede al cliente acceso a la dirección multidifusión especificada.
- 4 El STB envía un mensaje SETUP (ESTABLECIMIENTO) RTSP en el que especifica el indicador de recursos unificado de la película seleccionada.
- 5 El VTP reenvía a la AN la petición.
- 6 El servidor VoD realiza el control de admisión de conexión para garantizar que hay suficiente ancho de banda para el canal VoD. En caso necesario, se realiza el establecimiento de la conexión. Se atribuyen y reservan los recursos adecuados para reproducir la película VoD seleccionada. Seguidamente se envía una respuesta al ESTABLECIMIENTO RTSP que contiene la dirección de grupo multidifusión que se utilizará para la película VoD.
- 7 El VTP reenvía a la red residencial la solicitud.
- 8 El STB genera un mensaje llegada IGMP en el que especifica una copia de la dirección del grupo multidifusión recibida correspondiente a la película VoD seleccionada. Asimismo, el STB genera un segundo mensaje IGMP por si se perdiera el primero (según lo especificado por la variable robustez de la RFC 2236).  
Además el STB también envía una solicitud reproducción RTSP para informar al servidor VoD de que empiece a reproducir la película VoD.
- 9 El VTP determina que no hay miembros del mismo grupo multidifusión y reenvía el mensaje llegada IGMP a la AN.
- 10 De acuerdo con el paso 8 de la secuencia V.3.
- 11 De acuerdo con el paso 9 de la secuencia V.3.
- 12 El VTP reenvía a la AN la petición.
- 13 El servidor VoD inicia la reproducción de la película solicitada antes, para lo cual utiliza la dirección de grupo multidifusión especificada anteriormente en la respuesta reproducción RTSP.
- 14 El VTP reenvía a la red residencial la petición.
- 15 El STB se da cuenta de que la película VoD ya se ha empezado a reproducir.
- 16 La película ha terminado o el usuario la ha parado. A consecuencia de ello, el STB envía una petición disociación RTSP.
- 17 El VTP reenvía a AN la petición.
- 18 El servidor VoD para la reproducción de la película VoD, libera los recursos y desasocia las conexiones que fueron establecidas dinámicamente. Por último, envía una respuesta disociación RTSP.
- 19 El VTP reenvía a la red residencial la petición.
- 20 El STB envía al VTP un mensaje abandono IGMP en el que indica la dirección de grupo multidifusión que ya no necesita.
- 21 Tras recibir el mensaje "abandono IGMP" el VTP comprueba si hay otros STB que siguen interesados en recibir el canal multidifusión, para lo cual envía una consulta específica de grupo IGMP e inicia el temporizador de intervalo "lastmemberquery".
- 22 Todos los STB hacen caso omiso de la consulta específica de grupo, dado que ninguno de ellos es miembro del grupo multidifusión especificado en el mensaje.
- 23 Expira el temporizador de intervalo "lastmemberquery" y el VTP envía a la AN un mensaje abandono IGMP en el que se especifica que el grupo multidifusión ya no tiene miembros.
- 24 Tras recibir el mensaje "abandono IGMP" la red de acceso para de enviar al VTP secuencias del canal multidifusión especificado.

NOTA 1 – El VTP puede enviar los mensajes RTSP por una VC ATM puente, encaminada o PPPoE, en función de la arquitectura de red. El tipo de VC ATM que se utilice no afecta a la secuencia descrita antes.

NOTA 2 – La AN no intercepta ningún mensaje RTSP, los cuales simplemente se reenvían de manera transparente, dado que la AN realiza la retransmisión de células ATM.

NOTA 3 – El VTP filtra los mensajes IGMP recibidos por la interfaz  $T_{CN}$  que concuerden con alguna de las direcciones multidifusión correspondientes a la secuencia TV/VoD de difusión.

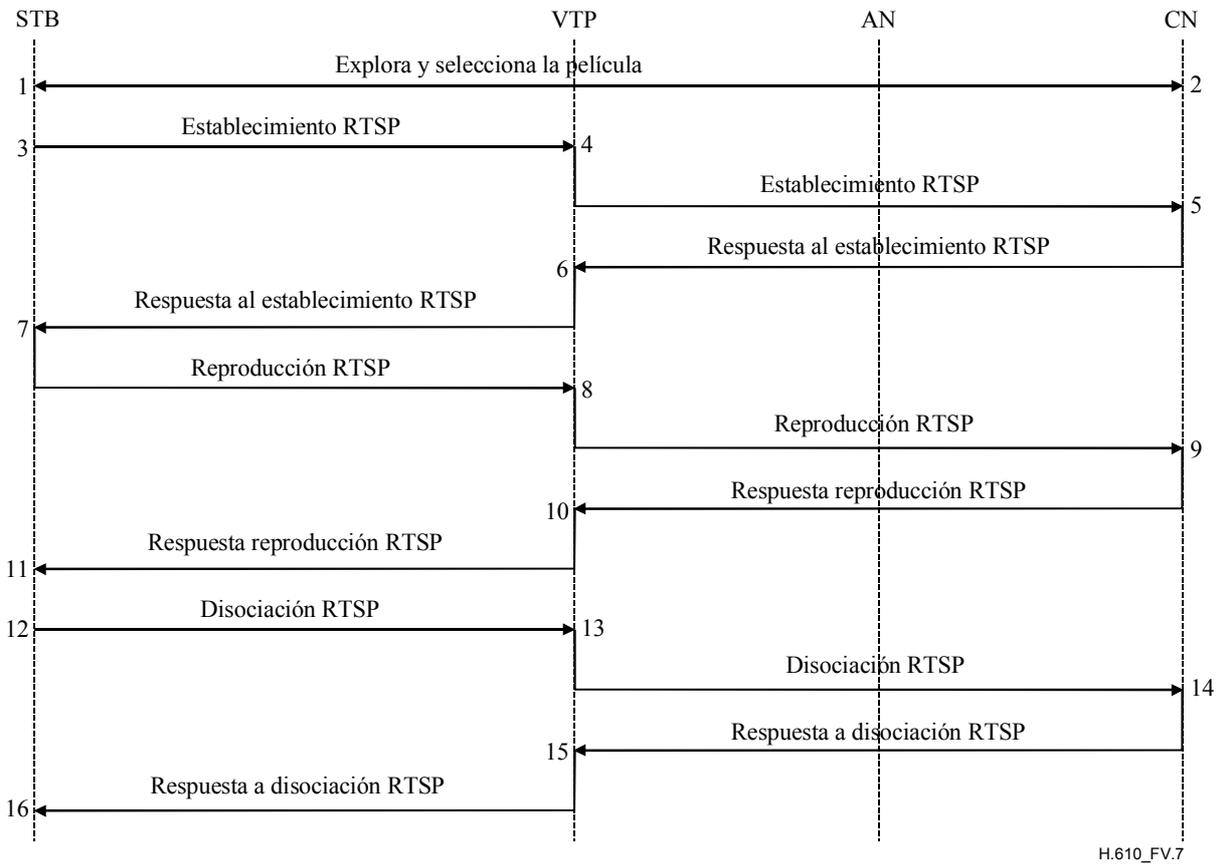
NOTA 4 – Los mensajes IGMP enviados entre el VTP y AN se transportan por una VCC ATM de cambio de canal dedicada para este fin.

## V.7 Selección de la película VoD – Entrega unidifusión IP

En este escenario se describe el flujo de mensajes cuando el usuario selecciona una película VoD y ésta se entrega utilizando unidifusión IP. La película termina cuando el usuario lo desea o cuando la película llega su fin.

### Condiciones previas:

- El VTP y el STB se han inicializado satisfactoriamente.
- El STB todavía no está recibiendo una película VoD.



- 1 El usuario de extremo explora el directorio de contenido y selecciona una película VoD.
- 2 El gestor TV de la red principal autentica al usuario, acepta la compra y devuelve al STB una URI válida para la película.
- 3 El STB envía un mensaje establecimiento RTSP en el que especifica el indicador de recursos unificado de la película seleccionada.
- 4 El VTP reenvía a la AN la petición.
- 5 El servidor VoD realiza el control de admisión de la conexión para garantizar que hay suficiente ancho de banda para el canal VoD. En caso necesario, se realiza el establecimiento de la conexión. Se atribuyen y reservan los recursos adecuados para reproducir la película VoD seleccionada. Seguidamente envía una respuesta al establecimiento RTSP.
- 6 El VTP reenvía a la red residencial la petición.
- 7 El STB envía una respuesta reproducción RTSP para informar al servidor VoD de que inicie la reproducción de la película VoD.
- 8 El VTP reenvía a la AN la petición.
- 9 El servidor VoD inicia la emisión de secuencias de la película utilizando la dirección IP multidifusión del STB y genera una respuesta reproducción RTSP.  
Las secuencias de la película VoD se envían al VTP utilizando un flujo puente, encaminado o PPPoE.
- 10 El VTP reenvía a la red residencial la petición.
- 11 El STB observa que el servidor VoD ha comenzado a emitir las secuencias de la película VoD.
- 12 La película VoD ha llegado a su fin o el usuario la ha parado. Como consecuencia de ello, el STB envía una petición disociación RTSP.
- 13 El VTP reenvía a la AN la petición.
- 14 El servidor VoD detiene la emisión de secuencias de la película VoD, libera los recursos y disocia las conexiones que fueron establecidas dinámicamente. Por último, envía una respuesta disociación RTSP.
- 15 El VTP reenvía a la red residencial la petición.
- 16 El STB observa que el servidor VoD ha dado fin satisfactoriamente a la película VoD.

NOTA 1 – El VTP puede enviar y/o recibir los mensajes RTSP y las secuencias de la película VoD a través de una VC ATM puente, encaminada o PPPoE. La elección depende de la arquitectura de red. El tipo de VC ATM que se utilice no afecta al orden secuencial descrito antes.

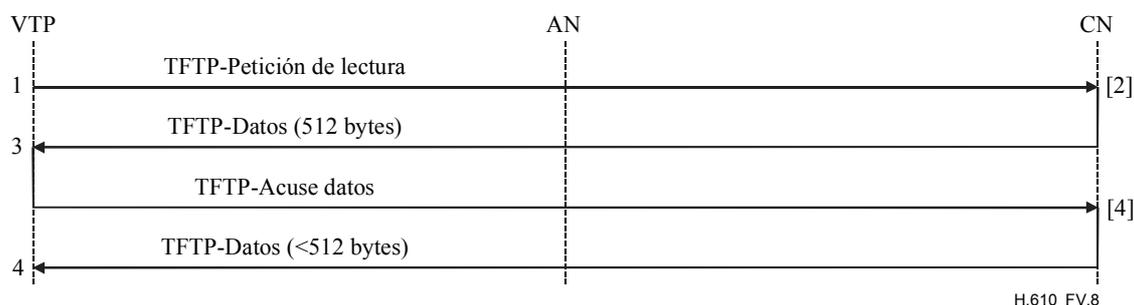
NOTA 2 – La AN no intercepta los mensajes RTSP o las secuencias de video VoD, por el contrario los reenvía de manera transparente dado que la AN realiza la retransmisión de células ATM.

## V.8 Descarga remota de programas informáticos en el VTP

El siguiente diagrama describe la actualización remota de los programas informáticos del VTP. Para descargar un fichero de la red principal, el VTP utiliza TFTP. La descarga puede iniciarse autónomamente por el VTP, por ejemplo tras reiniciarse, o por el sistema de gestión remota.

### Condiciones previas:

- El VTP se ha reinicializado satisfactoriamente.
- Se ha establecido una conectividad IP del canal de gestión remota.



- 1 El VTP solicita la descarga de una nueva versión de un programa informático. Para ello se emite una petición de lectura TFTP (RRQ).
- 2 El sistema de gestión a distancia de la red principal acusa recibo de la petición para lo cual envía los primeros 512 bytes del fichero.
- 3 El VTP acusa la petición para el cual envía el paquete de acuse de datos TFTP y almacena los bytes recibidos.
- 4 El sistema de gestión distancia de la red principal envía los bytes restantes del fichero y cuando el número de bytes sea <512, se produce el cierre de la sesión TFTP.
- 5 El VTP añade los bytes recibidos a los que había recibido antes y marca el final de la sesión. En ese momento, el VTP está preparado para utilizar la nueva imagen del programa informático descargado.

NOTA 1 – El VTP recibe mensajes TFTP por la VC que ha designado la gestión a distancia.

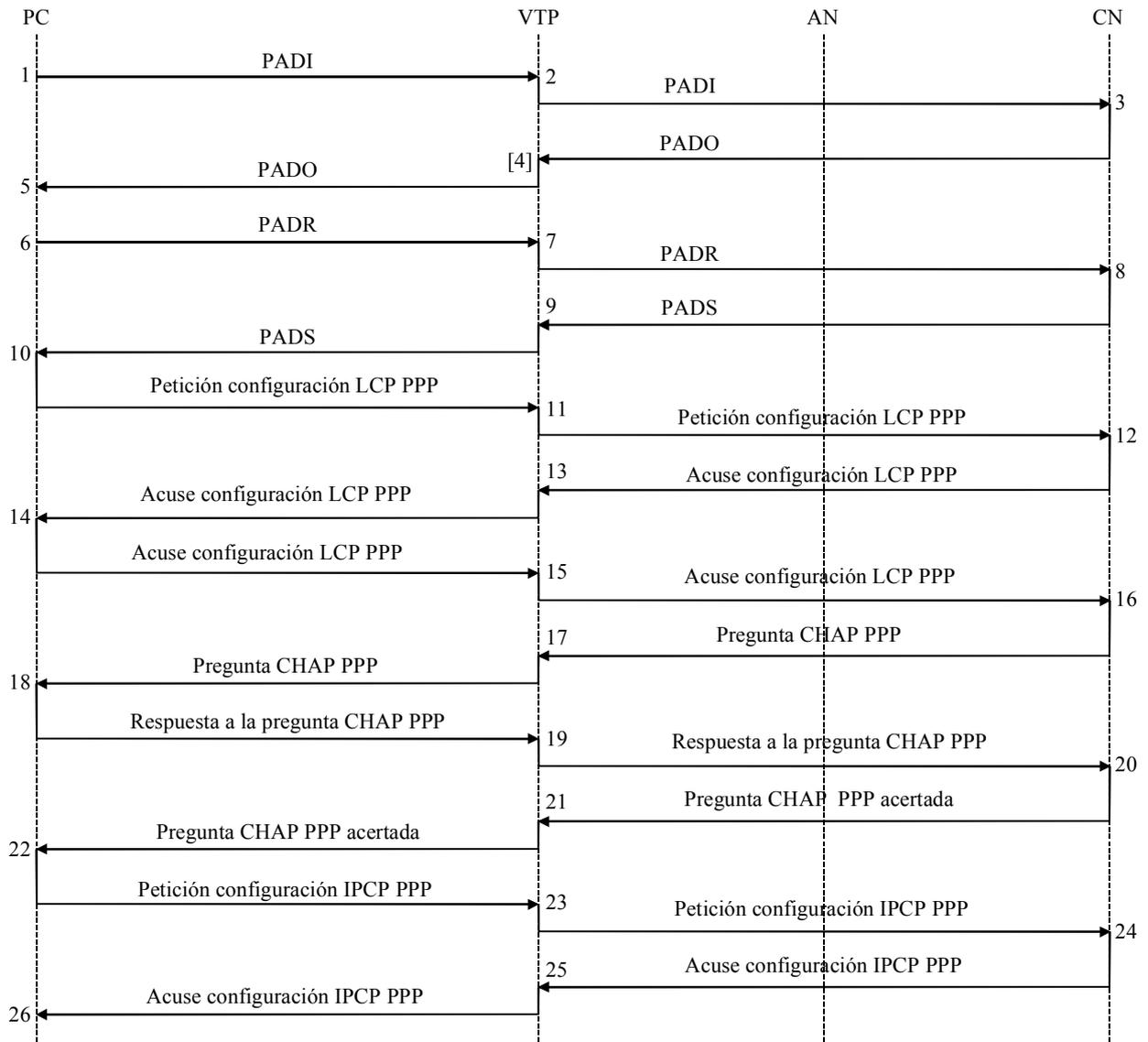
NOTA 2 – La AN no intercepta ninguno de los mensajes TFTP, sino que simplemente los reenvía de manera transparente, dado que la AN realiza la retransmisión de células ATM.

## **V.9 Navegación por Internet desde un terminal utilizando PPPoE**

El siguiente diagrama describe la situación en el que un computador personal (PC) inicia una sesión PPPoE para conectarse a la red con objeto de realizar tareas como la navegación por la web y el acceso al correo electrónico.

### **Condiciones previas:**

- El VTP se ha reinicializado satisfactoriamente.



H.610\_FV.9

- 1 El PC inicia una sesión PPPoE, para lo cual envía un paquete PADI que contiene el conjunto de direcciones Ethernet de destino para la difusión. El paquete PADI también puede contener información adicional como el nombre del servicio.
- 2 El VTP reenvía a la AN la petición.
- 3 El encaminador de borde de la red principal (CN) que puede servir la petición PADI responde con un paquete PADO. El paquete PADO contiene la dirección Ethernet de destino del PC, tal como se recibió en la PADI.
- 4 El VTP reenvía a la red residencial la petición.
- 5 Como ya se difundió la PADI, es posible recibir uno o varios paquetes PADO. Por consiguiente, el PC pone en marcha un temporizador de guarda que le permite esperar las respuestas de otros encaminadores de borde.
- 6 Después de la expiración del temporizador de guarda el PC elige a qué paquete PADO va a responder. Los criterios de selección pueden basarse en, por ejemplo, el nombre del encaminador de borde. El PC genera un paquete PADR que contiene las direcciones Ethernet de destino del encaminador de borde seleccionado.
- 7 El VTP reenvía a la AN la petición.
- 8 El encaminador de borde responde con un paquete PADS que indica que está preparado para iniciar la sesión PPP. Además, atribuye una identidad de sesión PPPoE única.
- 9 El VTP reenvía a la red residencial la petición.
- 10 El PC se da cuenta de que se ha establecido satisfactoriamente la sesión PPPoE. Para iniciar la sesión PPPoE, envía una petición de configuración LCP PPP.
- 11 El VTP reenvía a la AN la petición.
- 12 El encaminador de borde especifica los parámetros de enlace que se utilizarán en la sesión PPPoE y los incluye en el mensaje acuse (ACK) de configuración LCP PPP.
- 13 El VTP reenvía a la red residencial la petición.
- 14 El PC observa los parámetros de configuración del enlace y envía un acuse de configuración al LCP PPP.
- 15 El VTP reenvía a la AN la petición.
- 16 El encaminador de borde trata de realizar la autenticación segura del PC, para lo cual envía un paquete pregunta CHAP PPP.
- 17 El VTP reenvía a la red residencial la petición.
- 18 El PC cripta el nombre de usuario y la contraseña y lo incluye en la respuesta a la pregunta PPP.
- 19 El VTP reenvía a la AN la petición.
- 20 El encaminador de borde valida el nombre de usuario y la contraseña criptados y si son válidos envía un mensaje pregunta CHAP PPP acertada.
- 21 El VTP reenvía a la red residencial la petición.
- 22 El PC se da cuenta de que la autenticación es válida y envía una petición de configuración IPCP PPP por la que solicita los parámetros de configuración IP, por ejemplo la dirección IP del PC, y de los servidores DNS primario y secundario.
- 23 El VTP reenvía a la AN la petición.
- 24 El encaminador de borde envía un mensaje de acuse de configuración IPCP PPP en el que especifica los parámetros de configuración IP solicitados.
- 25 El VTP reenvía a la red residencial la petición.
- 26 El PC toma nota de los parámetros de configuración IP. Se establece la sesión PPP que se puede utilizar para la navegación por Internet.

NOTA 1 – Los mensajes PPPoE se pueden filtrar mediante un filtro PPPoE y enviarse por una VC ATM designada exclusivamente para la PPPoE. Otra posibilidad es que los mensajes PPPoE se puenteen y se envíen por una VC ATM puente. La selección depende de la arquitectura de red y no debe afectar al orden secuencial descrito antes.

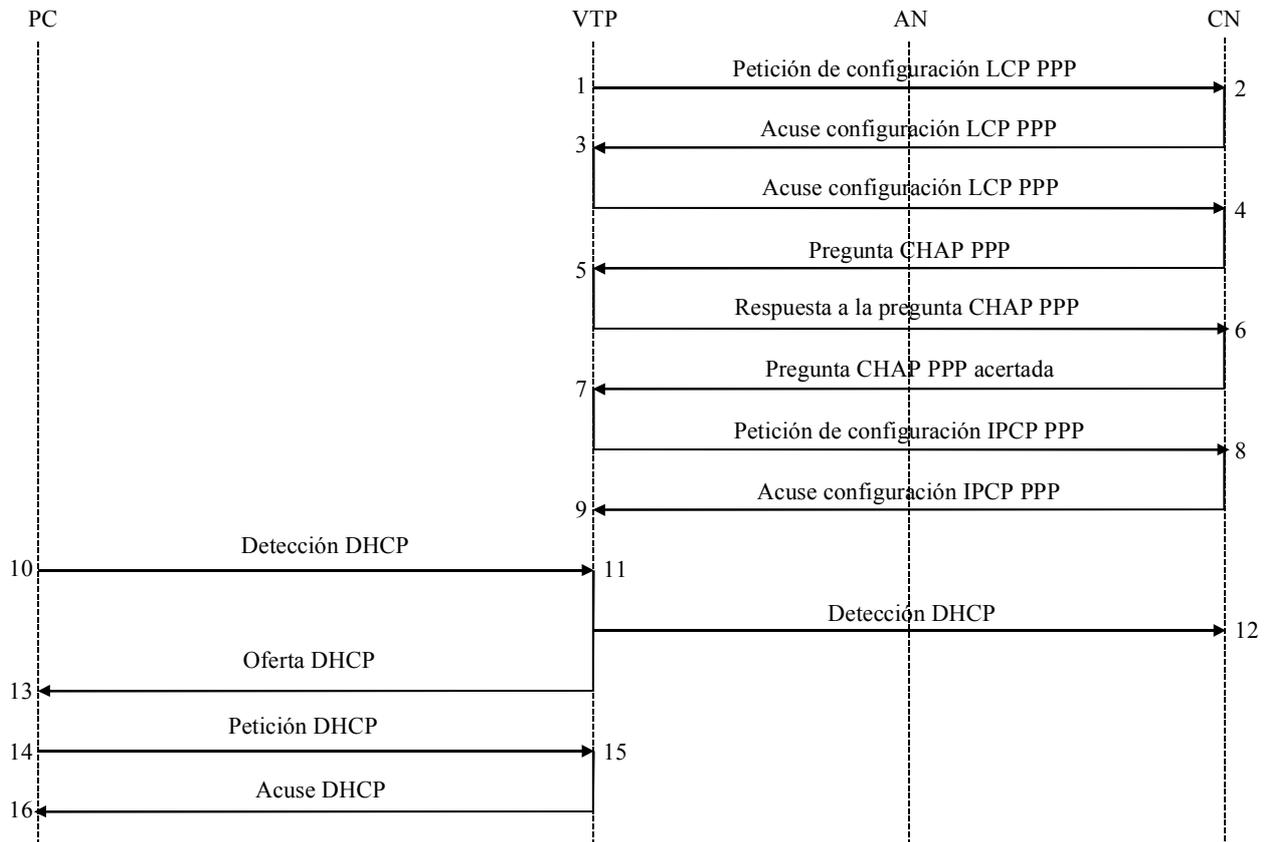
NOTA 2 – La AN no intercepta los mensajes PPPoE, por el contrario los reenvía de manera transparente, dado que está realizando la retransmisión de células ATM.

## **V.10 Navegación por Internet desde el VTP utilizando PPP**

El diagrama siguiente describe el caso en el que VTP inicia una sesión PPP y funciona como un servidor intermedio para el computador personal (PC) dentro de la red residencial. El servidor DHCP de la red residencial está ubicado dentro del VTP/D.

### **Condiciones previas:**

- El VTP se ha reinicializado satisfactoriamente.



H.610\_FV.10

- 1 El VTP inicia una sesión PPP para lo cual envía una petición de configuración LCP PPP.
- 2 El encaminador de borde, que normalmente es un BRAS de la red principal (CN) especifica los parámetros de enlace que se utilizarán para la sesión PPP y los incluye en el mensaje acuse de configuración LCP PPP.
- 3 El VTP toma nota de los parámetros de configuración del enlace y envía un acuse de configuración LCP PPP.
- 4 El encaminador de borde trata de autenticar al VTP de manera segura para lo cual envía un paquete pregunta CHAP PPP.
- 5 El VTP cripta el nombre de usuario y la contraseña y los incluye en la respuesta a la pregunta PPP.
- 6 El encaminador de borde valida el nombre de usuario y la contraseña criptados y si son válidos envía un mensaje pregunta CHAP PPP acertada.
- 7 El VTP se da cuenta de que la autenticación ha sido satisfactoria y envía una petición de configuración IPCP PPP mediante la cual solicita los parámetros de configuración del protocolo IP, por ejemplo la dirección IP del PC y los servidores DNS primario y secundario.
- 8 El encaminador de borde envía un acuse de configuración IPCP PPP que especifica los parámetros de configuración IP solicitados.
- 9 El VTP toma nota de los parámetros de configuración IP. Se establece la sesión PPP, la cual se puede compartir entre los equipos residenciales para la navegación por Internet, etc.
- 10 El PC envía al VTP una petición en la que solicita la dirección IP y otros parámetros de configuración, por ejemplo la pasarela por defecto, y las direcciones de los servidores DNS primario y secundario. El paquete de detección DHCP contiene la dirección de difusión IP de destino (255.255.255.255).
- 11 El servidor DHCP que se encuentra en el VTP procesa el paquete de difusión de detección DHCP. El servidor DHCP responde con un paquete oferta DHCP que incluye la dirección IP disponible.  
*Si el VTP también está puenteando, el paquete de difusión de detección DHCP también se envía a las VC ATM puente. De lo contrario no se envía ningún paquete detección DHCP a la AN.*
- 12 La retransmisión o el servidor DHCP ubicados en la red principal se configuran para hacer caso omiso de los paquetes de detección DHCP que no contengan el atributo identificador de clase de fabricante.
- 13 El PC se da cuenta de que el servidor DHCP ha respondido y pone en funcionamiento un temporizador de guarda que mide el tiempo durante el cual otros servidores DHCP pueden responder al paquete de detección DHCP que fue difundido.
- 14 El PC selecciona el servidor DHCP que ha respondido para lo cual envía el paquete de petición DHCP a la dirección IP de destino (255.255.255.255 ) e incluye la dirección del servidor seleccionado en el campo "dirección IP del servidor" del paquete DHCP. El paquete de petición DHCP se difunde para informar a los servidores DHCP que han respondido y que no han sido seleccionados.  
*Si el VTP también está puenteando, el paquete de difusión de detección DHCP también se envía a las VC ATM puente. De lo contrario no se envía ningún paquete detección DHCP a la AN.*
- 15 El servidor DHCP del VTP reconoce su dirección IP en el campo "dirección IP del servidor" del paquete de petición DHCP y responde con un acuse DHCP que contiene los siguientes parámetros de configuración: dirección IP, máscara de subred, pasarela por defecto, direcciones de los servidores DNS primario y secundario (asignados por PPP).
- 16 El PC registra los parámetros recibidos para la duración del periodo de usufructo. El PC está ahora preparado para navegar por Internet.  
*Los demás paquetes IP utilizados para la navegación por Internet se procesan mediante al función NAT VTP y se envían por la conexión encaminada traducida.*  
La función NAT VTP permite a diversos equipos residenciales (por ejemplo ordenadores personales) compartir acceso a Internet, para lo cual utilizan la dirección IP asignada por el proceso PPP cuando envían paquetes por la interfaz U-R2.

NOTA – La AN no intercepta los mensajes PPP, por el contrario los reenvía de modo transparente dado que la AN está realizando la retransmisión de células ATM.

## Apéndice VI

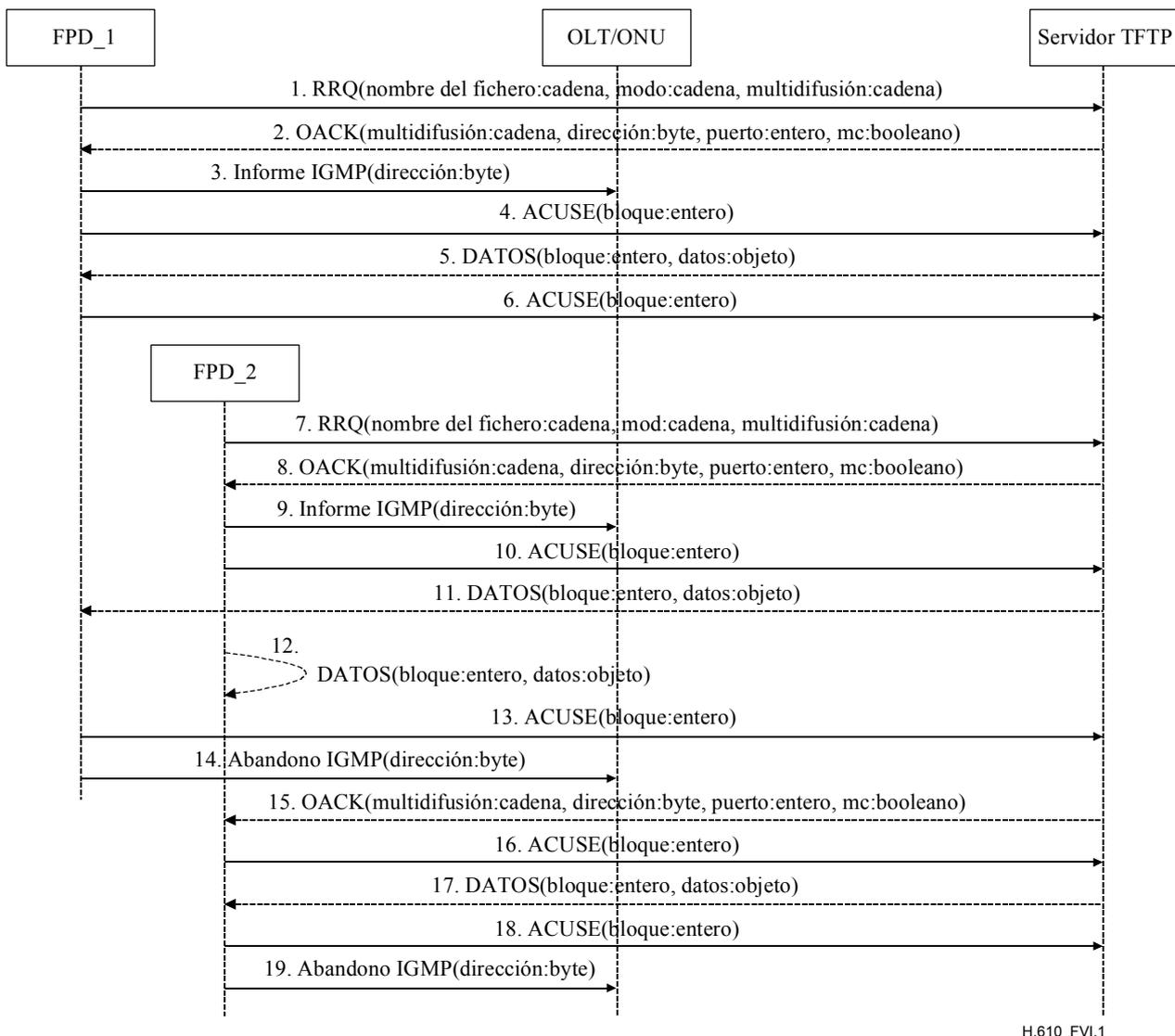
### Descarga de ficheros FPD utilizando TFTP multidifusión

Después de haberse establecido la conexión IP, los FPD que soportan servicios vídeo pueden descargar programas informáticos, metadatos e información de configuración adicional por la red. De este modo se garantiza que después de reinicializar el FPD, éste tiene la última versión de los programas informáticos y de los datos para las aplicaciones vídeo. Durante la fase de establecimiento de la conexión IP, se le pasa al FPD (mediante DHCP) el nombre del fichero y la ubicación del mismo que contiene el programa informático del FPD. El FPD tiene a su disposición varios mecanismos para descargar este fichero:

- Protocolo de transferencia de ficheros trivial multidifusión (M-TFTP) – El TFTP normalizado se define en RFC 1350 y la opción multidifusión se define en RFC 2090. Entre los dos describen un mecanismo óptimo para la transferencia de ficheros con una distribución uno a muchos. Se trata de un protocolo petición-respuesta que utiliza multidifusión IP para la transmisión de datos.
- Protocolo de distribución de ficheros coherente (CFDP). Este protocolo se define en RFC 1235 y tiene una arquitectura similar a la del M-TFTP.
- Carrusel de ficheros de propiedad – Este mecanismo sería similar al carrusel de objetos DSM-CC definidos por DAVIC. Se trata de un mecanismo que saca datos a la red sin que lo haya solicitado ningún FPD. No existe ninguna norma que defina un carrusel de este tipo para las redes FS-VDSL.

El TFTP unidifusión se utiliza mucho para la descarga de ficheros en los equipos y en las instalaciones del cliente actualmente instalados y ya existe infraestructura de red para esta solución. Por consiguiente, lo más fácil sería actualizar poco a poco el mecanismo de transferencia de ficheros, para hacerlo más escalable, siendo el M-TFTP el más adecuado de entre los anteriores. La elección de un único mecanismo que se aplique a múltiples FPD, dará lugar a una mayor compatibilidad en un entorno de múltiples fabricantes de FPD.

En este apéndice se describe como se puede utilizar el M-TFTP para descargar los programas informáticos del FPD antes de que éste se reinicialice. Este protocolo se puede asimismo utilizar después de la reinicialización para descargar metadatos e información de configuración necesarias para aplicaciones de TV por IP. En la figura VI.1 se muestra un ejemplo típico de utilización del M-TFTP, en el que dos FPD descargan simultáneamente un fichero que consta de  $2 \times 512$  Byte bloques.



H.610\_FVI.1

**Figura VI.1/H.610 – Descarga de ficheros TFTP multidifusión**

La descripción paso a paso es la siguiente:

El FPD\_1 envía una petición de lectura (RRQ) del archivo que se especificó durante la fase de establecimiento de la conexión IP mediante DHCP. La RRQ solicita el modo de transferencia de ficheros de octeto y contiene la opción multidifusión.

El servidor TFTP reconoce y soporta el modo octeto de transferencia de ficheros y la opción multidifusión y por consiguiente envía un acuse de opción (OACK) en el que especifica la dirección multidifusión, el número de puerto y mc = 1 indica que el FPD\_1 es el cliente maestro, responsable de acusar los paquetes de datos TFTP.

El FPD\_1 pasa a formar parte del grupo multidifusión especificado en el OACK mediante el mensaje de informe IGMPv2 OLT/ONU e inicia la escucha del grupo multidifusión y el número de puerto para los paquetes TFTP.

El FPD\_1 envía un ACUSE (ACK) con el parámetro bloque puesto a cero (0). De este modo especifica que el servidor TFTP que está solicitando el bloque uno (1).

El servidor TFTP envía un paquete DATOS (DATA) que contiene el bloque número 1.

El FPD\_1 envía un ACUSE (ACK) con el parámetro bloque puesto a uno (1). De este modo indica al servidor TFTP que está solicitando el bloque (2).

El FPD\_2 envía un RRQ para el mismo nombre de archivo especificado durante la fase de establecimiento de la conectividad IP mediante DHCP. LA RRQ contiene la opción multidifusión.

Dado que ese fichero ya se está transfiriendo al FPD\_1, el servidor TFTP envía un OACK en la que especifica la misma dirección multidifusión y número de puerto que para el FPD\_1, pero con  $mc = 0$ , lo que indica que el cliente maestro es otro FPD y que el FPD\_2 no debe enviar respuestas de acuse a los paquetes DATOS (DATA) que reciba.

El FPD\_2 pasa a formar parte del grupo multidifusión especificado en el OACK mediante un mensaje de informe IGMPv2 e inicia la escucha de ese grupo multidifusión y ese número de puerto de paquetes TFTP.

El FPD\_2 acusa el OACK con un ACK con el parámetro bloque puesto a cero (0).

El servidor TFTP envía el paquete de DATOS que contiene el bloque número 2, en respuesta al paso 6.

El FPD\_2 también recibe este paquete de DATOS porque está escuchando el mismo grupo multidifusión y número de puerto que el FPD\_1.

El FPD\_1 envía un ACK con el parámetro bloque puesto a (2). De este modo indica al servidor TFTP que el FPD\_1 ha terminado de recibir el fichero.

El FPD\_1 envía el grupo multidifusión especificado por el OACK mediante un mensaje abandono IGMPv2.

El servidor TFTP envía un OACK al FPD\_2 con los mismos parámetros especificados en el paso 8 pero con  $mc = 1$ , lo que indica que el FPD\_2 es ahora el cliente maestro y que debe empezar a enviar ACUSES (ACK) en respuesta a los paquetes de DATOS (DATA).

El FPD\_2 envía un ACK con el parámetro bloque puesto a cero (0). De este modo indica al servidor TFTP que está solicitando el bloque uno (1).

El servidor TFTP envía un paquete de DATOS que contiene el bloque número 1.

El FPD\_2, después de haber recibido el bloque dos (2), envía un ACK con el parámetro bloque puesto a dos (2). De este modo indica al servidor TFTP que el FPD\_2 ha completado la recepción del fichero.

El FPD\_2 abandona el grupo multidifusión especificado en el OACK mediante un mensaje abandono IGMPv2.

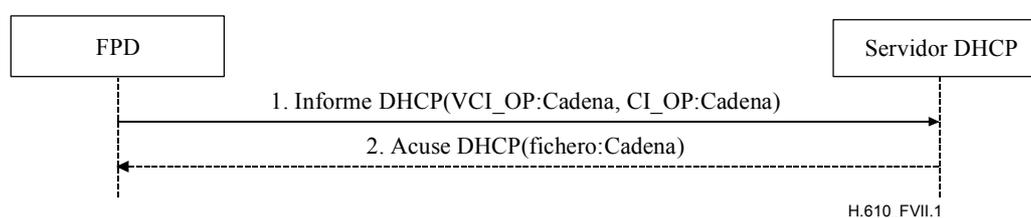
## Apéndice VII

### Configuración IP del FPD utilizando PPPoE y DHCP

Cuando un FDP soporta servicios vídeo (es decir, un adaptador multimedio) lo primero que necesita tras la inicialización es obtener una dirección IP, una pasarela por defecto y un DNS para poder obtener la conectividad IP por la red del proveedor de servicios vídeo. Para obtener dicha conectividad IP, los FPD utilizan principalmente el protocolo dinámico de configuración de anfitrión (DHCP, *dynamic host configuration protocol*). El uso exclusivo del DHCP para realizar esta tarea y las opciones DHCP necesarias con su correspondiente nomenclatura se definen en la parte normativa de esta Recomendación.

Ahora bien, en un entorno de red donde ya existen servicios Internet DSL de banda ancha instalados, es posible que ya haya una infraestructura de establecimiento de conectividad IP basada en el protocolo punto a punto (PPP). En ese caso, sería rentable poder reutilizar la misma infraestructura para la conectividad IP del FPD, y utilizar el DHCP sólo para la configuración adicional que está más allá de las capacidades que ofrece el PPP. En la parte normativa de esta Recomendación no se contempla este caso, y por esta razón en este apéndice se indica cómo puede utilizarse el PPPoE en el FPD para obtener la conectividad IP a la red del proveedor de servicios vídeo y, posteriormente, utilizar el DHCP para obtener los demás parámetros de configuración.

La primera fase, a saber, el establecimiento de una configuración IP básica mediante PPPoE se describe en el apéndice V (escenario 9). Una vez se han establecido la sesión PPPoE y el enlace PPP, se termina la fase de establecimiento de la conectividad IP. La siguiente fase consiste en recuperar el nombre del archivo y la ubicación del programa informático del FPD. Para ello se utilizan los mensajes informe DHCP que envía el FPD al servidor DHCP que está ubicado en la red del proveedor de servicios vídeo, tal como se muestra en la figura VII.1. Los pasos necesarios son los siguientes:



**Figura VII.1/H.610 – Informe DHCP para la obtención del nombre del archivo del programa informático del FPD**

Una vez terminada la fase de establecimiento de la conectividad IP, el FPD envía mediante el PPP un mensaje de informe DHCP. El mensaje informe DHCP se envía a la dirección Ethernet de difusión. Además de los parámetros normalizados, el mensaje informe DHCP contiene las opciones DHCP descritas en 10.3.4.

El servidor de DHCP que recibe el mensaje informe de DHCP, responde con un mensaje ACK DHCP que contiene los parámetros de configuración del FPD adecuados, pero sólo en caso de que esté encargado del CLIENT\_TYPE como figura en el mensaje informe. De lo contrario, el servidor DHCP descarta el mensaje informe DHCP sin admitir ninguna respuesta. El mensaje ACK DHCP también contiene la dirección IP del servidor TFTP (cuando se utiliza este protocolo para la descarga de ficheros) en el parámetro *sname*, y el nombre del directorio completo, en el parámetro *file* del mensaje DHCP, los cuales apuntan, respectivamente, a la ubicación y al nombre del fichero del programa informático<sup>2</sup> del FPD del tipo CLIENT\_TYPE. El servidor DHCP no atribuye una nueva dirección, comprueba si hay una vinculación existente, escribe el *yiaddr* o incluye los parámetros de tiempo de usufructo en el mensaje ACK DHCP, ya que todos estos aspectos fueron manipulados por el BAS durante la fase de establecimiento de la conectividad IP PPP. De esta manera se lleva a cabo completamente la obtención de la ubicación y el nombre del fichero del

<sup>2</sup> Obsérvese que el DHCP normalizado sólo permite facilitar en el mensaje DHCP el nombre del fichero. Éste contiene el nombre del fichero del programa informático necesario para la reinicialización del FPD. Cuando el FPD necesita otros ficheros, por ejemplo metadatos, debe ser el propio programa informático el que contenga las opciones adecuadas DHCP específicas del fabricante que permitan al FPD descargar a continuación esos ficheros adicionales después de la reinicialización. De este modo la implementación DHCP básica es lo más simple y normalizada posible, y a la vez permite una gran flexibilidad a los fabricantes de programas informáticos del FPD a la hora de implementar sus propias extensiones.

programa informático del FPD utilizando DHCP, y queda totalmente contemplado el caso en el que se utiliza PPPoE y DHCP para el establecimiento de la conectividad IP del FPD.

## Apéndice VIII

### Conmutación de protección

Para reducir al mínimo las interrupciones de los servicios básicos (por ejemplo, TV y voz de difusión) cuando se produce un fallo en la interfaz, el sistema FS-VDSL puede proporcionar soporte para la conmutación "rápida" de protección. La conmutación de protección se debe producir dentro de los 10 milisegundos siguientes a la detección del fallo, para que la interrupción del servicio sea mínima. Hay varios dominios de la arquitectura de sistema que pueden protegerse. Esos dominios protegidos y el correspondiente esquema de protección utilizado dependen enormemente de la topología de red y del control del operador de red o de servicio.

En la siguiente lista figura un ejemplo de esquemas de conmutación rápida de protección que se utilizan comúnmente.

- Protección de la sección del multiplexor (MSP) SDH/SONET – En este esquema se utilizan dos conjuntos de rutas diferentes, un enlace principal y otro de protección. El tráfico circula por el enlace principal cuando no hay averías, y pasa completamente al enlace de protección cuando se produce una avería en el enlace principal. Los dos enlaces, el de protección y el principal, terminan en el mismo punto extremo de la red, de manera que las funciones puente (encargada de la transmisión de tráfico) y selector (encargada de la recepción de tráfico) se pueden coordinar en los dos extremos del enlace (para mayor información véase la Rec. UIT-T G.783 [I-2]).
- Conmutación de protección ATM – En este esquema se utilizan también dos conjuntos de rutas diferentes de manera similar al esquema MSP SDH/SONET. Sin embargo, como la protección se produce en la capa ATM, sólo se utilizan conexiones de trayecto virtual (VPC, *virtual path connections*) y conexiones de canal virtual (VCC, *virtual channel connections*) que es necesario proteger. De este modo se consigue economizar ancho de banda, dado que el enlace de protección sólo necesita tener un ancho de banda suficiente para transportar las VPC y las VCC protegidas (para mayor información véase la Rec. UIT-T I.630 [I-3]).
- Reencaminamiento rápido MPLS – Este esquema requiere el establecimiento de dos trayectos conmutado por etiquetas (LSP, *label switch paths*) diferentes entre los conmutadores de origen y de destino, a fin de proporcionar un dominio de protección entre los dos conmutadores. En caso de que se produzca un fallo en una interfaz, el conmutador de origen se encarga de redirigir el tráfico mediante el LSP alternativo al conmutador de destino.

Los dominios del sistema FS-VDSL que quizá pueda ser necesario proteger son los siguientes:

- La interfaz ODN entre la OLT y la ONU – Dado que la interfaz ODN representa una interfaz cerrada, resulta conveniente un esquema de protección normalizado o de marca registrada.
- El punto de referencia V desde la OLT – Para esta interfaz son adecuados el esquema de conmutación MSP SDH/SONET o el esquema de conmutación de protección ATM.

Red principal – El esquema de protección adoptado depende de la tecnología de red principal (por ejemplo, ATM, IP). Por consiguiente, son posibles la conmutación de protección MSP SDH/SONET o la ATM o el reencaminamiento rápido MPLS.

## Apéndice IX

### Voz por DSL (VoDSL)

Por VoDSL se entiende el transporte de voz emulada digitalmente por la arquitectura de acceso DSL simultáneamente con el transporte de datos. El VoDSL soporta el acceso por parte del usuario a los servicios de telecomunicaciones en la banda vocal mediante los terminales existentes (por ejemplo, teléfono tradicional, fax) utilizando al mismo tiempo las nuevas tecnologías de acceso de datos basadas en hilos de cobre (es decir, DSL). En algunos casos los servicios VoDSL se ofrecen a través de dispositivos basados en datos, como PC multimedia y teléfonos Ethernet o teléfonos VoIP, etc. En este apéndice se describen los aspectos generales de tecnologías VoDSL normalizadas especificadas por diferentes organismos, como por ejemplo el foro ATM, el foro DSL, IETF, la CE 15/16 del UIT-T y la ETSI.

Las características del VoDSL son las siguientes:

- Servicios de voz emulados digitalmente mediante una función de pasarela de voz por paquetes en el VTP/D y una función de voz por paquetes en la red principal, denominados "servicios de voz conexos". En el VTP/D, las interfaces telefónicas analógicas se denominan "líneas de voz conexas". Normalmente, estas líneas no soportan servicios permanentes (es decir, no disponen de una oficina central).
- Se ofrecen simultáneamente servicios VoDSL y servicios de datos (por ejemplo, acceso a Internet, transferencia de ficheros).
- Como normalmente el VTP/D VoDSL ofrece múltiples interfaces de servicio, se denomina dispositivo de acceso integrado (IAD, *integrated access device*).
- La calidad de la voz que puede soportar VoDSL es idéntica a la de otras formas de telefonía digital, como RDSI. Además, no aparecen los problemas de las líneas analógicas ya que el transporte es digital. Es posible utilizar la modulación por impulsos codificados, por ejemplo MIC o G.711, cuando sea necesario. Ahora bien, también es posible utilizar algoritmos de compresión que utilizan menos ancho de banda, por ejemplo MICDA o G.726, sin que se aprecie una pérdida de la calidad de la voz. Asimismo, cabe observar que VoDSL utiliza técnicas de cancelación de ecos.

A continuación se describen dos arquitecturas diferentes de voz por DSL. En la primera, la capa de adaptación ATM es la AAL 2 para el transporte de servicios de voz tradicional hasta el punto interfaz con la red pública, y se denomina BLES af-vmoa-0145.000 [I-8]. La segunda arquitectura se basa en el IP para el transporte de paquetes de voz y se conoce como voz por IP.

Algunos de los criterios que se pueden tomar en consideración para elegir entre una u otra arquitectura son los siguientes:

- La medida en que la red de voz principal (TDM) va a evolucionar hacia una red completamente por paquetes.
- La posibilidad de introducir pasarelas entre la red de voz y la red de datos.
- La integración de los servicios de voz existentes (en particular los servicios de valor añadido).
- La medida en que se desean mejorar los servicios de datos con terminales de voz.

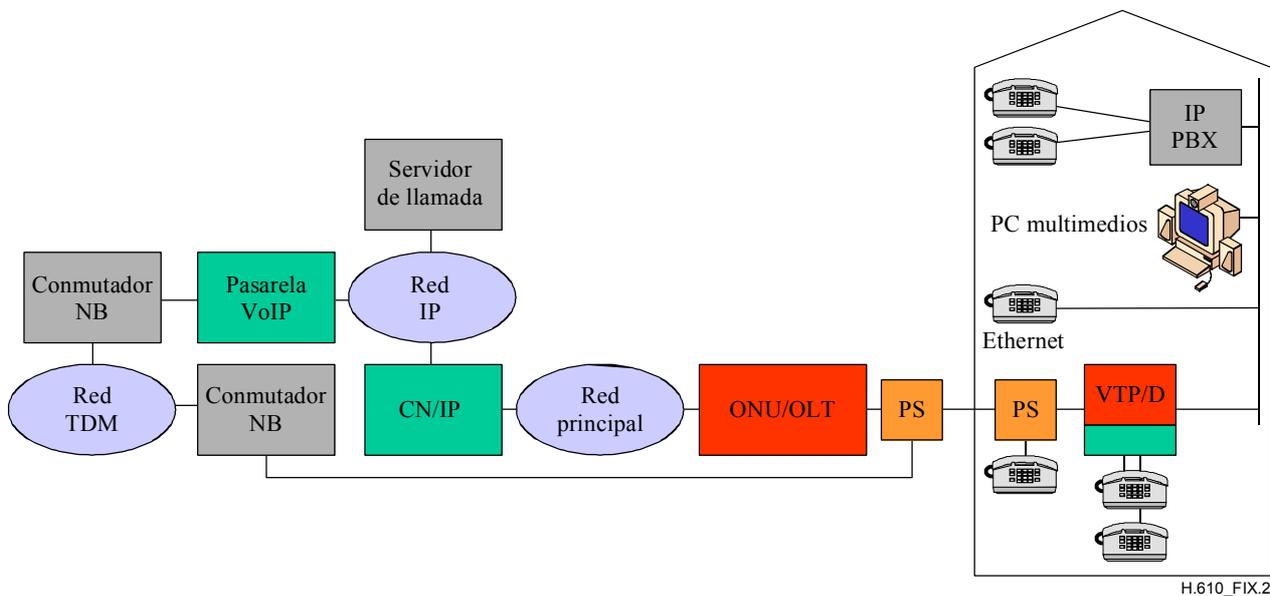
#### IX.1 BLES

El servicio de emulación de bucle (LES, *loop emulation service*) fue creado por el foro ATM y lo adoptó el foro DSL. En el contexto de VoDSL, aparece denominado algunas veces como servicio de emulación de bucle en banda ancha (BLES, *broadband loop emulation service*). El modo de transferencia del BLES es ATM/AAL 2. La unión de la señal digital de datos y de la señal digital de



Los elementos de red que tradicionalmente se utilizan para la implementación de VoIP son los siguientes:

- Instalaciones del cliente:
  - PC multimedia que tiene instalados y en funcionamiento programas informáticos de VoIP. Análogamente, el STB podría evolucionar para soportar VoIP.
  - Un VTP/D que dispone de interfaces telefónicas analógicas tradicionales e incluye la funcionalidad de VoIP. A este dispositivo se le podría denominar IAD.
  - Terminal de sólo voz VoIP, por ejemplo, un teléfono Ethernet, que está conectado a una LAN residencial o de la empresa.
  - PBX LAN que conecta terminales telefónicas tradicionales y proporciona paquetización y servicios PBX.
  - Otra posibilidad es que se proporcione una funcionalidad de control local de llamada, por ejemplo un controlador de acceso o un servidor intermedio SIP, y también un servidor local o incorporado en el IAD VDSL o PBX LAN.
- Red principal:
  - Pasarela VoIP que convierte voz por paquetes que hace de interfaz con la red TDM.
  - VoIP que conoce los encaminadores NAT.
  - Controlador de llamada que realiza el control de llamada de los dispositivos VoIP en la red. En función de la arquitectura y los protocolos utilizados, el controlador de llamada podrá denominarse como servidor intermedio SIP, controlador de acceso H.323 o controlador de pasarela de medios.



**Figura IX.2/H.610 – Elementos de red VoIP**

La combinación de voz y datos se produce en el dominio de las instalaciones del cliente. La segregación puede hacerse en la red principal, donde está la interfaz de la señal de voz con la red TDM, o bien, no se hace la segregación, en caso de que el VoIP se transporte de extremo a extremo.

Se aplican los siguientes principios para VoIP:

- Para implementar el VoIP, se puede añadir la funcionalidad VoIP en las instalaciones del cliente, y añadir al control de llamada VoIP y la pasarela VoIP en el punto de interfaz con la red TDM tradicional.

- En el grupo VTP/D, una función de conversión VoIP convierte el tráfico procedente de las interfaces de usuario en la banda vocal analógicas tradicionales a VoIP y viceversa. La conversión VoIP consiste, entre otras cosas, en la compresión de la voz, la paquetización, el encapsulado RTP y la señalización VoIP, por ejemplo, H.323, SIP o H.248. Esta funcionalidad puede incorporarse en el VTP/D o estar en un dispositivo independiente, como por ejemplo un adaptador VoIP o un PBX LAN. Además, es posible implementar el VoIP mediante un programa informático en un dispositivo de datos multifunción, como por ejemplo un PC multimedia o un STB.
- En el VTP/D, deben proporcionarse capacidades QoS para garantizar que se pierden pocos paquetes y que se produce muy poco retraso del tráfico VoIP. Esto se puede implementar de diferentes maneras, por ejemplo mecanismos Ethernet, IP o QoS ATM.
- Si el tráfico VoIP se encamina mediante una conexión encaminada traducida en el VTP/D, se prevé que éste conozca IP y proporcione los tratamientos VoIP necesarios.
- El tráfico de voz IP puede direccionarse, mediante la red de acceso DSL, a un proveedor de servicios de voz por IP dedicado a la red de voz por IP, que está diseñado para proporcionar la QoS basada en IP necesaria para los servicios de voz, o la Internet pública, que actualmente no dispone de capacidades QoS para los servicios de voz de calidad.
- En la red principal, la voz IP por paquetes se convierte a las interfaces tradicionales (es decir RDSI/NNI RTPC) mediante pasarelas de medios y pasarelas de señalización. La principales funciones de estas pasarelas son la terminación de circuitos de voz TDM, la (de)multiplexación VoIP, la función de tratamiento de voz, por ejemplo compresión y cancelación de ecos, la interfaz con el control de llamada y la conectividad a una o varias centrales telefónicas tradicionales mediante una interfaz NNI. No obstante, es posible proporcionar VoIP de extremo a extremo, en cuyo caso no es necesaria la conversión de tráfico de voz basado en IP a tráfico TDM tradicional.
- La funciones de control de llamada son, entre otras, la traducción de direcciones (por ejemplo, de números de teléfono a nombres de computadores centrales, direcciones de correo electrónico y/o direcciones IP), el establecimiento de sesión mediante procedimiento de establecimiento de llamada (por ejemplo, configuración, alerta, conexión, desconexión), la gestión de sesiones mediante dispositivos que conocen VoIP intermedios, por ejemplo, pasarelas y encaminadores NAT, la función de interfaz con servicios administrativos, por ejemplo red inteligente, facturación, etc., y el control de recursos de red.

## **Apéndice X**

### **Proceso IEEE para obtener OUI**

Los números OUI los gestiona la organización IEEE. La solicitud de OUI puede presentarse en el sitio web de IEEE (<http://standards.ieee.org>), mediante el siguiente URL, <http://standards.ieee.org/regauth/oui/forms/>





## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
<b>Serie H</b>	<b>Sistemas audiovisuales y multimedios</b>
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación