



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**T.123**

(05/99)

SERIE T: TERMINALES PARA SERVICIOS DE  
TELEMÁTICA

---

**Pilas de protocolos de datos específicos de la  
red para conferencias multimedios**

Recomendación UIT-T T.123

(Anteriormente Recomendación del CCITT)

---



## **RECOMENDACIÓN UIT-T T.123**

### **PILAS DE PROTOCOLOS DE DATOS ESPECÍFICOS DE LA RED PARA CONFERENCIAS MULTIMEDIOS**

#### **Resumen**

La presente Recomendación especifica los aspectos de red de los protocolos de datos de las Recomendaciones de la serie T.120 para conferencias multimedios. Las redes identificadas actualmente son: RDSI, RDCC, RDCP, RTPC, RDSI-BA y LAN. Se especifican perfiles de comunicación que proporcionan conexiones fiables punto a punto entre un terminal y una unidad de control multipunto, entre pares de terminales o entre pares de unidades de control multipunto (MCU). En algunos casos, una capa de protocolo inferior permite la multiplexión de señales audio y vídeo, además de las conexiones de datos. En otros casos, pueden establecerse por la misma red o una red diferente para transportar señales audio o vídeo.

Además, el anexo B especifica un protocolo que puede utilizarse para negociar servicios de conexión que van más allá de una transferencia de datos fiable. Este protocolo también permite la utilización de listas de direcciones de alias cuando se establece una conexión. Las listas de alias permitirán la creación y utilización de servicios por procuración para las comunicaciones T.120.

#### **Orígenes**

La Recomendación UIT-T T.123 ha sido revisada por la Comisión de Estudio 16 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.º 1 de la CMNT el 27 de mayo de 1999.

## 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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 N.º 1 de la CMNT.

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 *empresa de explotación reconocida (EER)* designa a toda persona, compañía, empresa u organización gubernamental que explote un servicio de correspondencia pública. Los términos *Administración*, *EER* y *correspondencia pública* están definidos en la *Constitución de la UIT (Ginebra, 1992)*.

## 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 2000

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

## ÍNDICE

### Página

1	Alcance .....	1
1.1	Redes identificadas .....	1
1.2	Señales audio y vídeo.....	1
1.3	Establecimiento de la comunicación RDSI.....	1
2	Referencias.....	1
3	Definiciones .....	5
4	Abreviaturas.....	6
5	Configuración multipunto.....	7
6	Configuración de perfiles.....	8
7	Perfiles básicos .....	10
7.1	Perfil básico RDSI .....	10
7.2	Perfil básico RDCC .....	11
7.3	Perfil básico RDCP.....	12
7.4	Perfil básico RTPC .....	12
7.5	Perfil básico RDSI-BA .....	13
7.6	Perfil básico LAN .....	14
8	Encabezamiento de paquete para delimitar unidades de datos en un tren de octetos .	16
9	Función de sincronización y convergencia .....	17
9.1	Visión de la SCF .....	17
9.2	Procedimientos de la SCF.....	18
9.3	Mensajes de la SCF.....	21
9.4	Parámetros de calidad de servicio.....	23
10	Parámetros y opciones de protocolo de la Recomendación Q.922 .....	24
11	Transparencia de la estructura de trama del enlace de datos para la transmisión arrítmica .....	25
12	Subcapa física formada por los canales MLP H.221 .....	26
13	Perfiles alternativos.....	28
13.1	Alternativa: RDSI basada en la Recomendación Q.922 .....	28
13.2	Alternativa: RDSI basada en la Recomendación T.90.....	29
13.3	Alternativa: RDSI basada en la Recomendación V.120 .....	30
13.4	Alternativa: RTPC basada en la Recomendación H.324 .....	30
13.5	Alternativa: RDSI-BA basada en la Recomendación H.222 .....	31
13.6	Alternativa: LAN basada en la transferencia de unidades de datos .....	32

Anexo A – Integración de señales multimedios organizadas conformea la Recomendación H.221 .....	34
Anexo B – Conexiones de transporte ampliadas.....	34
B.1 Alcance .....	34
B.2 Referencias normativas.....	34
B.3 Definiciones .....	35
B.4 Abreviaturas.....	35
B.5 Convenios .....	36
B.6 Sinopsis.....	36
B.6.1 Modelo de conexión de transporte ampliada.....	36
B.6.2 Servicios de transporte.....	38
B.6.3 Uso modificado de la Recomendación X.224 .....	38
B.6.4 Protocolo de negociación de la conexión .....	38
B.7 Conexiones de transporte ampliadas.....	39
B.7.1 Establecimiento de la conexión inicial .....	39
B.7.2 Restablecimiento de la conexión .....	42
B.7.3 Servicio de red no fiable .....	43
B.8 Perfiles ampliados.....	43
B.8.1 Transportes fiables.....	43
B.8.2 Transportes no fiables.....	48
B.9 Protocolo de negociación de la conexión (CNP, <i>connection negotiation protocol</i> )...	49
B.9.1 Sinopsis.....	49
B.9.2 Estructura de las TPDU del CNP .....	49
B.9.3 TPDU de control.....	50
B.9.4 TPDU de datos.....	54
B.9.5 Utilizar CNP en X.224.....	55
B.9.6 Definición ASN.1 .....	56
B.10 Protocolo de segmentación y reensamblado no fiable .....	59
B.10.1 Sinopsis.....	59
B.10.2 Estructura de las TPDU de SAR no fiables .....	59
Apéndice I – Establecimiento de la comunicación conferencia multimedios en la RDSI.....	62
I.1 Introducción .....	62
I.2 Requisitos básicos.....	62
I.3 Fase de conexión.....	63
I.4 Fase A (protocolo de canal D RDSI) .....	63
I.5 Fase B (protocolo H.242).....	63
I.6 Fase C (protocolo de la serie T.120).....	64

	<b>Página</b>
Apéndice II – Marco de seguridad de la GSS-API.....	67
II.1 Introducción .....	67
II.2 Tecnología de autenticación común (CAT, <i>common authentication technology</i> ) del IETF .....	67
II.2.1 IETF y grupo de trabajo CAT .....	67
II.2.2 Marco de seguridad de la GSS-API.....	67
II.2.3 SPNEGO.....	67
II.3 Marco de seguridad del anexo B/T.123 .....	67
II.3.1 GSS-API: Transporte de testigos GSS-API vía clase 0 de la X.224 o CNP..	68





## **Recomendación T.123**

# **PILAS DE PROTOCOLOS DE DATOS ESPECÍFICOS DE LA RED PARA CONFERENCIAS MULTIMEDIOS**

*(revisada en 1999)*

## **1 Alcance**

La presente Recomendación, que define pilas de protocolos comunes para terminales y MCU, especifica los aspectos de red de la sucesión de protocolos T.120, en forma de perfiles para cada red identificada. Cada perfil especifica un conjunto de protocolos que se extiende a la capa 4 del modelo de referencia OSI.

El fundamento de esta Recomendación es el siguiente: la conferencia audiográfica y visual está destinada a formar parte del repertorio de servicios de la RDSI. La teleconferencia a través de la RDSI implica la integración de múltiples medios (audio, vídeo y datos) en una conexión que puede estar compuesta por un cierto número de canales físicos. Sin embargo, la prestación de estos servicios no está limitada a la RDSI, y puede identificarse toda una serie de escenarios de red diferentes. Por ejemplo, una RDCC puede proporcionar un servicio similar al de la RDSI, aunque menos flexible, y la RTPC puede proporcionar un servicio, que aunque de calidad limitada, esté más fácilmente disponible. La teleconferencia puede también extenderse a la RDCP y a la RDSI-BA. Las LAN pueden proporcionar servicio de conferencia localmente dentro de una empresa o un medio de acceso a redes de área extensa.

### **1.1 Redes identificadas**

Se definen perfiles específicos de red para la RDSI, RDCC, RDCP y RTPC, conforme a la Recomendación F.710. El alcance de la presente Recomendación incluye también la RDSI-BA y la LAN.

### **1.2 Señales audio y vídeo**

El tratamiento de las señales audio y vídeo en una conferencia multimedia no forma parte de esta Recomendación, si se exceptúa la posibilidad de su transporte multiplexado por la misma conexión en algunos casos.

### **1.3 Establecimiento de la comunicación RDSI**

En el apéndice I figuran ejemplos de procedimientos de establecimiento de la comunicación RDSI para la teleconferencia audiográfica. Estos procedimientos ilustran:

- a) la utilización de los elementos de información RDSI;
- b) la coordinación del canal D y del canal B;
- c) las fases del establecimiento de la conexión;
- d) el interfuncionamiento con servicios telefónicos.

## **2 Referencias**

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta

Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

- Recomendación UIT-T F.702 (1996), *Servicios de conferencia multimedia*.
- Recomendación UIT-T H.221 (1997), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.
- Recomendación UIT-T H.222.0 (1995) | ISO/CEI 13818-1:1996, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas*.
- Recomendación UIT-T H.222.0 (1995)/enm.1 (1996) | ISO/CEI 13818-1:1996/enm.1:1997, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información audio asociada: Sistemas – Enmienda 1: Registro de identificador de derechos de autor*.
- Recomendación UIT-T H.222.0 (1995)/enm.2 (1996) | ISO/CEI 13818-1:1996/enm.2:1997, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información audio asociada: Sistemas – Enmienda 2: Registro de identificador de formato*.
- Recomendación UIT-T H.223 (1996), *Protocolo de multiplexación para comunicación multimedios a baja velocidad binaria*.
- Recomendación UIT-T H.230 (1997), *Señales de control e indicación con sincronismo de trama para sistemas audiovisuales*.
- Recomendación UIT-T H.231 (1997), *Unidades de control multipunto para sistemas audiovisuales que utilizan canales digitales de hasta 1920 kbit/s*.
- Recomendación UIT-T H.233 (1995), *Sistemas con confidencialidad para servicios audiovisuales*.
- Recomendación UIT-T H.242 (1997), *Sistema para el establecimiento de comunicaciones entre terminales audiovisuales con utilización de canales digitales de hasta 2 Mbit/s*.
- Recomendación UIT-T H.243 (1997), *Procedimientos para el establecimiento de comunicación entre tres o más terminales audiovisuales con utilización de canales digitales de hasta 1920 kbit/s*.
- Recomendación UIT-T H.310 (1998), *Sistemas y terminales de comunicación audiovisual en banda ancha*.
- Recomendación UIT-T H.320 (1997), *Sistemas y equipos terminales videotelefónicos de banda estrecha*.
- Recomendación UIT-T H.324 (1998), *Terminal para comunicación multimedios a baja velocidad binaria*.
- Recomendación UIT-T I.320 (1993), *Modelo de referencia de protocolo de la red digital de servicios integrados*.
- Recomendación CCITT I.321 (1991), *Modelo de referencia de protocolo RDSI-BA y su aplicación*.
- Recomendación UIT-T I.361 (1999), *Especificación de la capa modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha*.
- Recomendación UIT-T I.363.1 (1996), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha: Capa de adaptación del modo transferencia asíncrono tipo 1*.

- Recomendación UIT-T I.363.3 (1996), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha: Capa de adaptación del modo transferencia asíncrono tipo 3/4.*
- Recomendación UIT-T I.363.5 (1996), *Especificación de la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha: Capa de adaptación del modo transferencia asíncrono tipo 5.*
- Recomendación UIT-T I.365.1 (1993), *Subcapas de la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha: Subcapa de convergencia específica del servicio de retransmisión de tramas.*
- Recomendación UIT-T I.365.3 (1995), *Subcapas de la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha: Función de coordinación específica de servicio para proporcionar el servicio de transporte con conexión.*
- Recomendación UIT-T I.430 (1995), *Especificación de la capa 1 de la interfaz usuario-red básica.*
- Recomendación UIT-T I.431 (1993), *Especificación de la capa 1 de la interfaz usuario-red a velocidad primaria.*
- Recomendación UIT-T I.432.1 (1999), *Interfaz usuario-red de la red digital de servicios integrados de banda ancha (RDSI-BA) – Especificación de la capa física: Características generales.*
- Recomendación UIT-T I.432.2 (1999), *Interfaz usuario-red de la red digital de servicios integrados de banda ancha (RDSI-BA) – Especificación de la capa física: Explotación a 155 520 kbit/s y 622 080 kbit/s.*
- Recomendación UIT-T I.432.3 (1999), *Interfaz usuario-red de la red digital de servicios integrados de banda ancha (RDSI-BA) – Especificación de la capa física: Explotación a 1544 kbit/s y 2048 kbit/s.*
- Recomendación UIT-T I.432.4 (1999), *Interfaz usuario-red de la red digital de servicios integrados de banda ancha (RDSI-BA) – Especificación de la capa física: Operación a 51 840 kbit/s.*
- Recomendación UIT-T Q.920 (1993), *Aspectos generales de la capa enlace de datos de la interfaz usuario-red de la RDSI.*
- Recomendación UIT-T Q.921 (1997), *Interfaz usuario-red de la RDSI – Especificación de la capa de enlace de datos.*
- Recomendación UIT-T Q.921 bis (1993), *Serie de pruebas abstractas para la prueba de conformidad del procedimiento de acceso al enlace en el canal D.*
- Recomendación CCITT Q.922 (1992), *Especificación de la capa de enlace de datos de la RDSI para servicios portadores en modo trama.*
- Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de llamada básica.*
- Recomendación UIT-T Q.933 (1995), *Especificaciones de señalización para el control y la monitorización de la situación de conexiones virtuales conmutadas y permanentes en modo trama.*
- Recomendación UIT-T Q.2110 (1994), *Protocolo con conexión específico de servicio para la capa de adaptación del modo de transferencia asíncrono de la red digital de servicios integrados de banda ancha.*

- Recomendación UIT-T Q.2130 (1994), *Capa de adaptación del modo de transferencia asíncrono para señalización de la red digital de servicios integrados de banda ancha – Función de coordinación específica de servicio para el soporte de señalización en la interfaz usuario a red.*
- Recomendación UIT-T Q.2931 (1995), *Sistema de señalización digital de abonado N.º 2 – Especificación de la capa 3 de la interfaz usuario-red para el control de llamada/conexión básica.*
- Recomendación UIT-T Q.2931/enm.1 (1997), *Sistema de señalización digital de abonado N.º 2 – Especificación de la capa 3 a la interfaz usuario-red para el control de llamada/conexión básica.*
- Recomendación CCITT T.90 (1992), *Características y protocolos para terminales de servicios de telemática en la red digital de servicios integrados (RDSI).*
- Recomendación UIT-T T.120 (1996), *Protocolos de datos para conferencias multimedios.*
- Recomendación UIT-T T.122 (1998), *Servicio de comunicación multipunto – Definición de los servicios.*
- Recomendación UIT-T T.124 (1998), *Control genérico de conferencia.*
- Recomendación UIT-T T.125 (1998), *Especificación de protocolo del servicio de comunicación multipunto.*
- Recomendación UIT-T T.126 (1997), *Protocolo para imágenes fijas y anotaciones multipunto.*
- Recomendación UIT-T T.127 (1995), *Protocolo de transferencia multipunto de ficheros binarios.*
- Recomendación CCITT V.7 (1988), *Definiciones de términos relativos a la comunicación de datos por la red telefónica.*
- Recomendación UIT-T V.8 (1998), *Procedimientos para comenzar sesiones de transmisión de datos por la red telefónica pública conmutada.*
- Recomendación UIT-T V.8 bis (1996), *Procedimientos de identificación y selección, a través de la red telefónica pública conmutada y de circuitos arrendados de tipo telefónico punto a punto, de modos de funcionamiento comunes entre equipos de terminación del circuito de datos y entre equipos terminales de datos.*
- Recomendación UIT-T V.14 (1993), *Transmisión de caracteres arrítmicos por canales portadores síncronos.*
- Recomendación UIT-T V.34 (1998), *Módem que funciona a velocidades de señalización de datos de hasta 33 600 bit/s para uso en la red telefónica general conmutada y en circuitos arrendados punto a punto a dos hilos de tipo telefónico.*
- Recomendación UIT-T V.42 (1996), *Procedimientos de corrección de errores para los equipos de terminación del circuito de datos que utilizan la conversión de modo asíncrono a modo síncrono.*
- Recomendación CCITT V.42 bis (1990), *Procedimientos de compresión de datos para los equipos de terminación del circuito de datos (ETCD) que utilizan procedimientos de corrección de errores.*
- Recomendación UIT-T V.61 (1996), *Módem para voz y datos simultáneos que funciona a una velocidad de señalización de voz más datos de 4800 bit/s, con conmutación automática opcional a velocidades de señalización de hasta 14 400 bit/s para datos solamente,*

*destinado al uso en la red telefónica general conmutada y en circuitos arrendados de tipo telefónico punto a punto a dos hilos.*

- Recomendación UIT-T V.70 (1996), *Procedimientos para la transmisión simultánea de datos y señales vocales codificadas digitalmente por la red telefónica general conmutada y por circuitos arrendados punto a punto a dos hilos de tipo telefónico.*
- Recomendación UIT-T V.120 (1996), *Soporte proporcionado por una red digital de servicios integrados (RDSI) a equipos terminales de datos con interfaces del tipo serie V con multiplexión estadística.*
- Recomendación CCITT X.21 (1992), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para funcionamiento síncrono en redes públicas de datos.*
- Recomendación CCITT X.21 bis (1988), *Utilización, en las redes públicas de datos, de equipos terminales de datos diseñados para su conexión con módems síncronos de la serie V.*
- Recomendación UIT-T X.25 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados.*
- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación UIT-T X.213 (1995) | ISO/CEI 8348:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de red.*
- Recomendación UIT-T X.214 (1995) | ISO/CEI 8072:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de transporte.*
- Recomendación UIT-T X.224 (1995) | ISO/CEI 8073:1997, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo para proporcionar el servicio de transporte en modo con conexión.*
- ISO/CEI 3309:1993, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure.*
- ISO/CEI 7776:1995, *Information technology – Telecommunications and information exchange between systems – High-level data link control procedures – Description of the X.25 LAPB-compatible DTE data link procedures.*
- ISO/CEI 8208:1995, *Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment.*
- ISO/CEI TR 8802-1:1997, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 1: Overview of Local Area Network Standards.*

### **3 Definiciones**

En esta Recomendación se utilizan los siguientes términos definidos en la Recomendación F.701:

- Servicio de conferencia audiográfica.
- Unidad de control multipunto.

En esta Recomendación se utilizan los siguientes términos definidos en la Recomendación I.320:

- Plano de control.
- Plano de usuario.

En esta Recomendación se utiliza el siguiente término definido en la Recomendación Q.920:

- Identificador de conexión de enlace de datos.

En esta Recomendación se utiliza el siguiente término definido en la Recomendación Q.922:

- Función de sincronización y convergencia.

En esta Recomendación se utiliza el siguiente término definidos en la Recomendación V.7:

- Transmisión arrítmica.

En esta Recomendación se utiliza el siguiente término definidos en las Recomendaciones X.213 y X.214:

- Calidad de servicio.

#### **4 Abreviaturas**

En esta Recomendación se utilizan las siguientes siglas:

AAL	Capa de adaptación ATM ( <i>ATM adaptation layer</i> )
AL	Capa de adaptación ( <i>adaptation layer</i> )
ATM	Modo de transferencia asíncrono ( <i>asynchronous transfer mode</i> )
CPCS	Subcapa de convergencia de parte común ( <i>common part convergence sublayer</i> )
DCE	Equipo de terminación del circuito de datos ( <i>data circuit-terminating equipment</i> )
DLCI	Identificador de conexión de enlace de datos ( <i>data link connection identifier</i> )
DTE	Equipo terminal de datos ( <i>data terminal equipment</i> )
FCS	Secuencia de verificación de trama ( <i>frame check sequence</i> )
LAN	Red de área local ( <i>local area network</i> )
MCS	Servicio de comunicación multipunto ( <i>multipoint communication service</i> )
MCSAP	Punto de acceso al servicio MCS ( <i>MCS service access point</i> )
MCU	Unidad de control multipunto ( <i>multipoint control unit</i> )
NSAP	Punto de acceso al servicio de red ( <i>network service access point</i> )
OSI	Interconexión de sistemas abiertos ( <i>open systems interconnection</i> )
PDU	Unidad de datos de protocolo ( <i>protocol data unit</i> )
PES	Tren elemental empaquetado ( <i>packetized elementary stream</i> )
QoS	Calidad de servicio ( <i>quality of service</i> )
RDCC	Red de datos con conmutación de circuitos
RDCP	Red de datos con conmutación de paquetes
RDSI	Red digital de servicios integrados
RDSI-BA	Red digital de servicios integrados de banda ancha
RTPC	Red telefónica pública conmutada
SCF	Función de sincronización y convergencia ( <i>synchronization and convergence function</i> )

SDU	Unidad de datos de servicio ( <i>service data unit</i> )
TPDU	Unidad de datos de protocolo de transporte ( <i>transport protocol data unit</i> )
TSAP	Punto de acceso al servicio de transporte ( <i>transport service access point</i> )
VC	Canal virtual ( <i>virtual channel</i> )

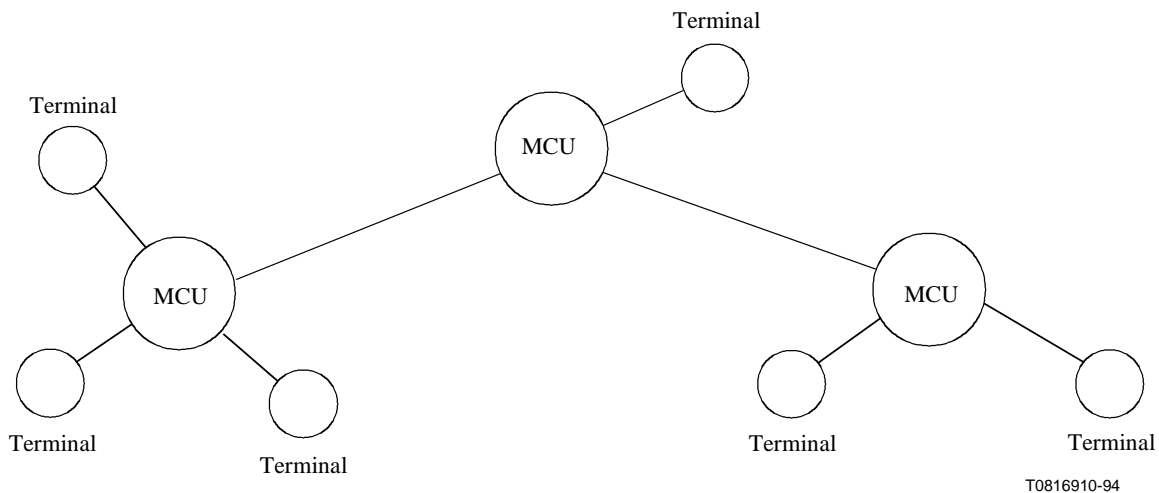
## 5 Configuración multipunto

La configuración multipunto se crea mediante conexiones punto a punto entre tres o más terminales y varias MCU. La figura 1 muestra una configuración típica donde los terminales están conectados en una configuración multipunto en estrella alrededor de cada MCU. Muestra también la manera de interconectar las MCU para formar conferencias de mayor magnitud.

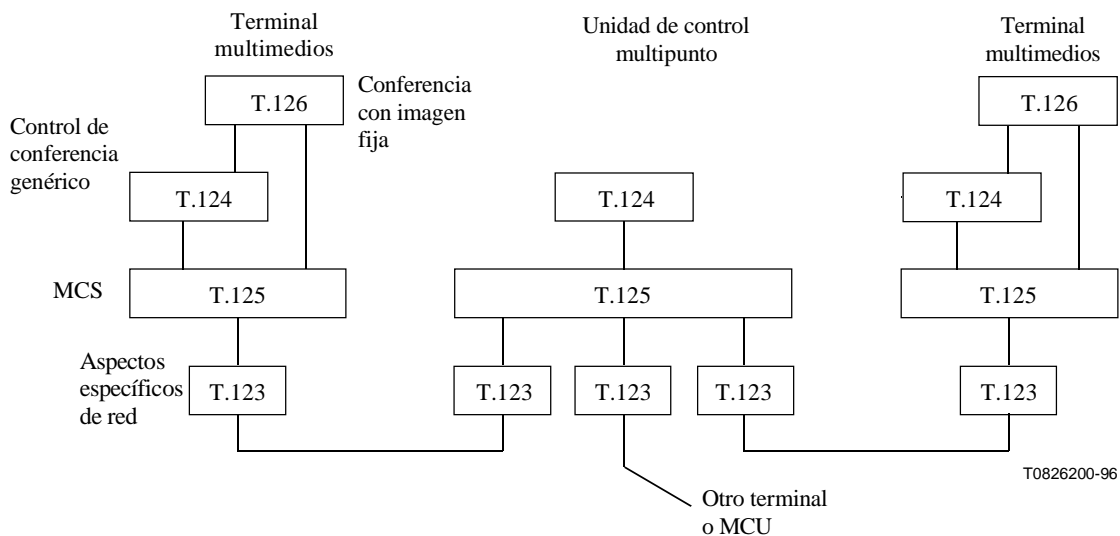
La figura 2 muestra la organización de la sucesión de protocolos T.120. Esta Recomendación define los protocolos específicos de la red en cualquier conexión directa entre un terminal y una MCU, entre dos terminales o entre dos MCU.

Las conexiones punto a punto a una única MCU no necesitan tener perfiles de comunicación idénticos. El funcionamiento de la capa de protocolo MCS soporta la comunicación a través de diferentes redes.

Si dos terminales carecen de un perfil común, no pueden conectarse directamente entre sí. En ese caso, una MCU puede servir de intermediario haciendo posible la comunicación. Éste es un ejemplo especial de configuración multipunto.



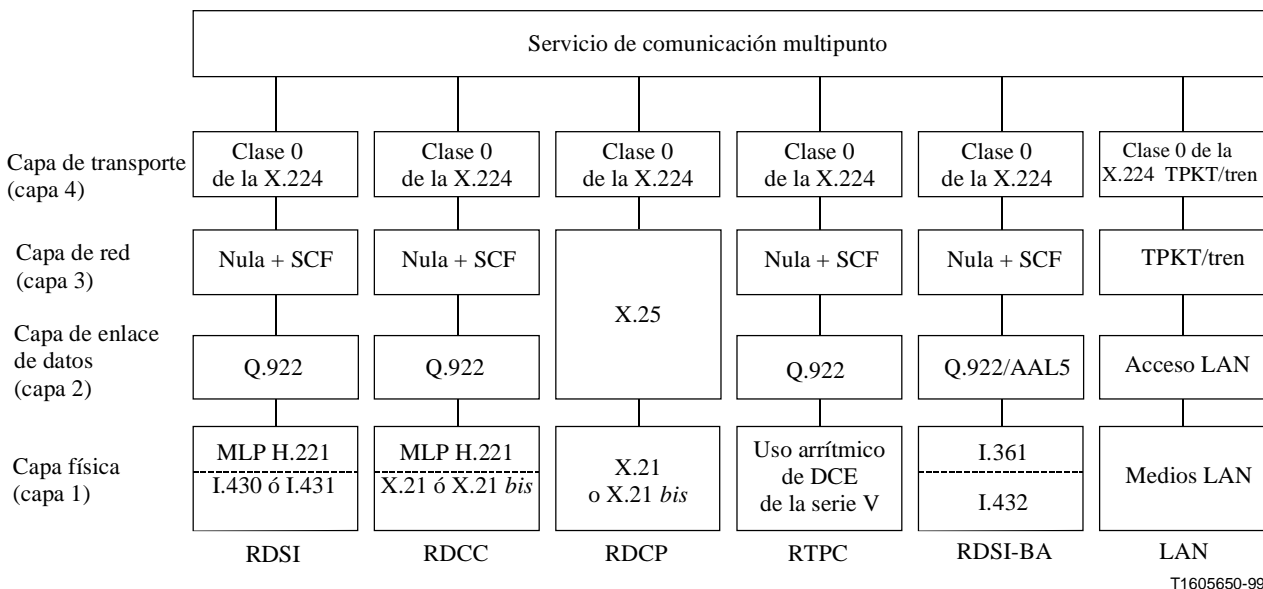
**Figura 1/T.123 – Configuración multipunto típica**



**Figura 2/T.123 – Organización de la sucesión de protocolos T.120**

## 6 Configuración de perfiles

La estructura general de los perfiles específicos de la red se muestra en la figura 3. Los perfiles se definen en detalle en las cláusulas que siguen.



**Figura 3/T.123 – Estructura general de los perfiles en el modo básico**

NOTA 1 – La utilización de la Recomendación Q.922 en la RDSI no implica la utilización de un servicio portador con retransmisión de tramas. La Recomendación Q.922 se utiliza para potenciar la calidad de servicio proporcionada por la capa física de una RDSI, RDCC, RTPC, o RDSI-BA. Esta Recomendación explota los mecanismos de recuperación tras errores del modo de funcionamiento con acuse de recibo multitrama Q.922 de uno o más enlaces de datos sobre una conexión punto a punto proporcionada por la red correspondiente.

El servicio que el MCS requiere de las capas inferiores es la transferencia fiable, secuencial y de flujo controlado de unidades de datos de tamaño ilimitado. Una conexión MCS se compone de una a



cuatro conexiones de transporte. El número depende de cuántas prioridades de transferencia de datos MCS se implementen por separado.

Se derivan múltiples conexiones de transporte de una conexión punto a punto sobre una red específica mediante multiplexión en alguna capa de protocolo inferior. Esto ocurre en la capa 2 en aquellos casos en los que se utiliza la Recomendación Q.922 y en la capa 3 cuando se utiliza la Recomendación X.25 o un protocolo LAN.

La figura 4 muestra la posición de un proveedor MCS en el modelo de referencia OSI. Un proveedor MCS intercambia unidades de datos de protocolo MCS con proveedores MCS distantes. A tal fin, utiliza servicios de capa de transporte. Un proveedor MCS se comunica con usuarios MCS a través de un MCSAP por medio de las primitivas MCS definidas en la Recomendación T.122.

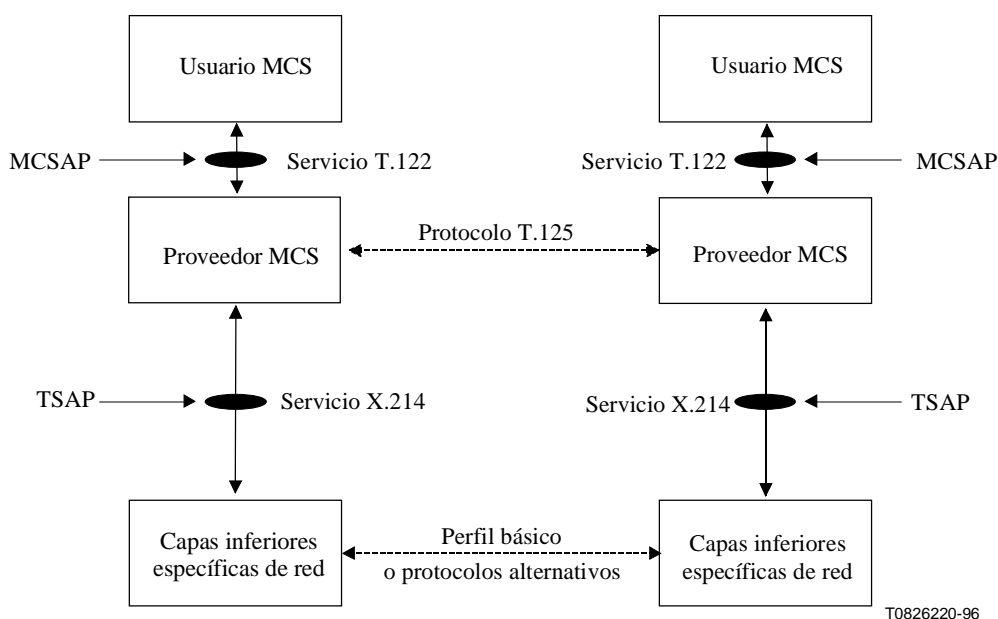
Para simplificar la información de dirección que ha de ser suministrada cuando se establece una conexión MCS, se recomienda que los terminales y las MCU se administren para los perfiles en modo básico, de modo que los selectores de NSAP y TSAP nulos seleccionen un proveedor de MCS en el sistema de destino.

Esto no excluye la posibilidad de que pueda ser necesario que un selector concreto comunique con un proveedor MCS en un contexto determinado. Este caso puede darse, por ejemplo, si la conexión de datos ha de asociarse con una conexión audio o vídeo establecida independientemente. Puede también darse si la conexión MCS ha de incorporarse a una conferencia albergada en una partición de una gran MCU. Idealmente, el selector concreto a utilizar se comunicará dinámicamente mediante algún intercambio previo.

NOTA 2 – Un selector de NSAP puede aparecer en la parte específica de dominio de una dirección NSAP. El formato de éste no está normalizado.

NOTA 3 – En cada uno de los perfiles aquí especificados, el protocolo de transporte es la Recomendación X.224. Transporta selectores de TSAP como parámetros TSAP-ID de las TPDU de establecimiento de la conexión.

NOTA 4 – El anexo B especifica los perfiles que se utilizarán cuando se establezcan conexiones de transporte ampliadas T.120.



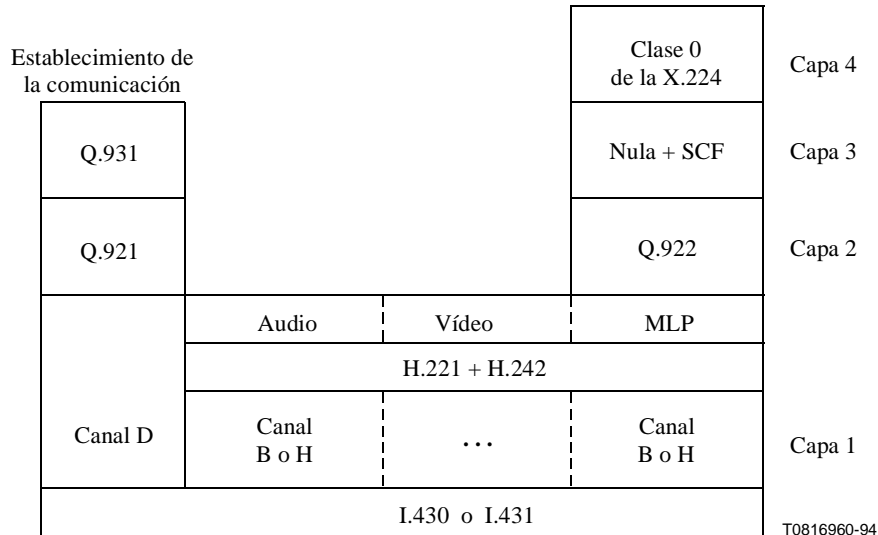
**Figura 4/T.123 – Posición de un proveedor MCS en el modelo de referencia OSI**

## 7 Perfiles básicos

Cuando los protocolos de establecimiento de la comunicación o el audio o el vídeo se muestran en los perfiles que siguen, es sólo para ayudar a la comprensión. Son una parte normativa de esta Recomendación.

### 7.1 Perfil básico RDSI

La figura 5 define el perfil básico RDSI.



**Figura 5/T.123 – Perfil básico RDSI**

#### Capa 4

- X.224.
- Clase 0 preferida, sin clase alternativa.
- El tamaño máximo de la TPDU no debe rebasar el parámetro N201 de la capa 2.

#### Capa 3

- Plano de usuario: nulo (sin protocolo adicional durante la transferencia de datos).
- Plano de control: SCF como se especifica en la cláusula 9.

#### Capa 2

- Q.922.
- Parámetros y opciones de protocolo como se especifica en la cláusula 10, parámetros y opciones de protocolo de la Recomendación Q.922.

#### Capa 1

Subcapa formada por los canales MLP de la Recomendación H.221:

- Como se especifica en la cláusula 12, subcapa física formada por los canales MLP H.221.

Subcapa formada por la RDSI:

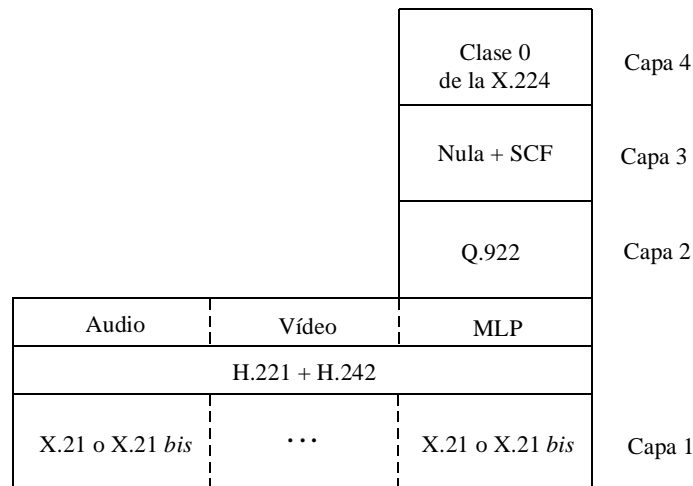
- 1 a 6 canales B, o 1 a 5 canales H0, o 1 canal H1.
- Información digital sin restricciones, opcionalmente con tonos y anuncios.

- Los canales B se pueden adaptar en velocidad a 56 kbit/s para redes con restricciones.
- El canal D se utiliza sólo para señalización de red, no para datos de usuario.

NOTA – Esta Recomendación no especifica el establecimiento de la comunicación en la RDSI (si bien se ilustran casos posibles en el apéndice I). La SCF mostrada sólo funciona en el canal MLP, después de establecida la comunicación en la RDSI y conmutada al modo H.242.

## 7.2 Perfil básico RDCC

La figura 6 define el perfil básico RDCC. Las capas por encima de H.221 son idénticas a las del perfil básico RDSI.



T0816970-94

**Figura 6/T.123 – Perfil básico RDCC**

### Capa 4

- Como se especifica en 7.1, perfil básico RDSI.

### Capa 3

- Como se especifica en 7.1, perfil básico RDSI.

### Capa 2

- Como se especifica en 7.1, perfil básico RDSI.

### Capa 1

Subcapa formada por canales MLP de la Recomendación H.221:

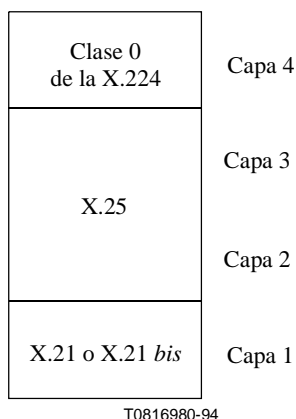
- Como se especifica en la cláusula 12, subcapa física formada por los canales MLP H.221.

Subcapa formada por la RDCC:

- X.21 o X.21 bis para cada conexión de circuito conmutado.
- Las velocidades binarias deben ser un múltiplo uniforme de 64 kbit/s o 56 kbit/s.

### 7.3 Perfil básico RDCP

La figura 7 define el perfil básico RDCP



**Figura 7/T.123 – Perfil básico RDCP**

#### Capa 4

- X.224.
- Clase 0 preferida, sin clase alternativa.

#### Capa 3

- Servicio de llamada virtual de la X.25.

#### Capa 2

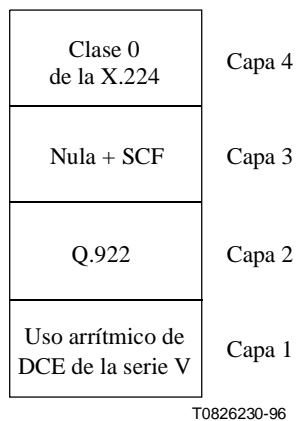
- Procedimiento de enlace único LAPB de la X.25.

#### Capa 1

- X.21 o X.21 bis.

### 7.4 Perfil básico RTPC

La figura 8 define el perfil básico RTPC. Las capas por encima de Q.922 son idénticas a las del perfil básico RDSI.



**Figura 8/T.123 – Perfil básico RTPC**

#### Capa 4

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 3

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 2

- Q.922.
- Parámetros y opciones de protocolo como se especifican en la cláusula 10, parámetros y opciones de protocolo de la Recomendación Q.922.
- Transparencia de trama modificada basada en ISO/CEI 3309, como se especifica en la cláusula 11, transparencia de la estructura de trama del enlace de datos para la transmisión arrítmica.

#### Capa 1

- Transmisión arrítmica por el DTE.
- Cuando se usa V.14: un bit de arranque, un bit de parada, ocho bits de datos, sin paridad.
- Se puede emplear cualquier módem compatible de DCE de la serie V que funcione por la RTPC.
- El DTE y el DCE pueden ser funciones lógicas que no estén físicamente separadas, si el equipo integrado puede producir las mismas señales transmitidas.
- La elección de DCE de la serie V es sin restricciones e incluye, por ejemplo, módems V.34, V.61 y V.70, con uso opcional de V.42 y V.42 *bis*. La selección de un modo operativo compatible puede ser asistida por V.8 o V.8 *bis*.

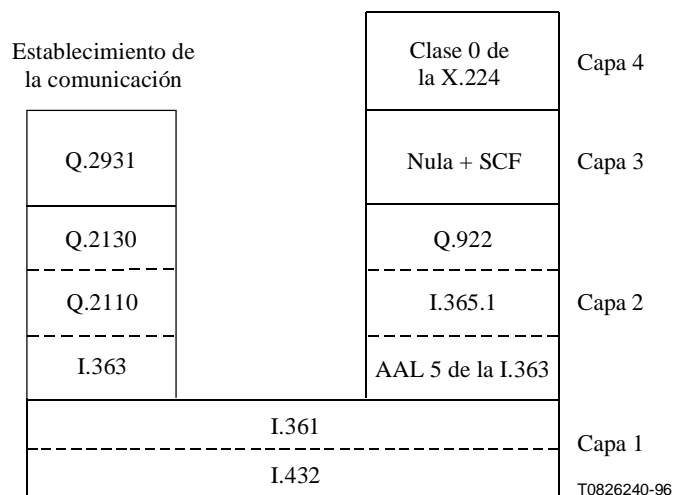
NOTA 1 – Si se activa la función de control de errores de V.42, deben fijarse los parámetros del sistema para evitar una interacción adversa con la operación de corrección de errores de Q.922. Elementos importantes son el temporizador de acuse de recibo, máximo número de octetos en un campo de información, y las condiciones de reenvío de datos.

NOTA 2 – La eficacia de la compresión de datos V.42 *bis* variará dependiendo del volumen de los datos de aplicación intercambiados en una conferencia que ha sido ya comprimida por otros medios.

NOTA 3 – Los DCE V.70, si se les comunica que se está empleando este perfil, pueden negociar entre sí el uso de técnicas potenciadas, como la tunelización UNERM para T.120, mientras el servicio proporcionado en la interfaz DTE sigue siendo transmisión arrítmica.

### 7.5 Perfil básico RDSI-BA

La figura 9 define el perfil básico RDSI-BA. Las capas por encima de Q.922 son idénticas a las del perfil básico RDSI.



**Figura 9/T.123 – Perfil básico RDSI-BA**

*Capa 4*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 3*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 2*

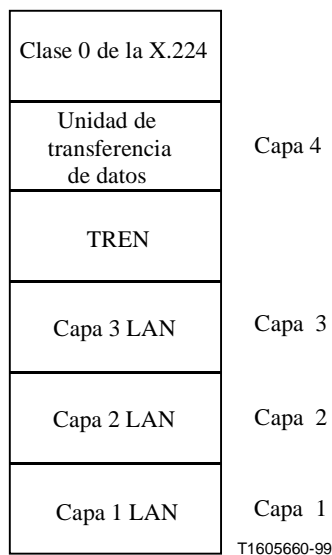
- Q.922.
- Parámetros y opciones de protocolo como se especifica en la cláusula 10, parámetros y opciones de protocolo de la Recomendación Q.922.
- Estructura de PDU definida en la figura 3/I.365.1 (sin utilización de banderas, transparencia, o FCS)
- Octetos PDU transportados como una CPCS-SDU utilizando AAL tipo 5.

*Capa 1*

- Canal virtual ATM.

**7.6 Perfil básico LAN**

La figura 10 define el perfil básico LAN.



**Figura 10/T.123 – Perfil básico LAN**

*Capa 4*

- Clase 0 X.224 preferida, sin clase alternativa.
- TPDU tamaño 65531 por defecto, pero pueden negociarse valores menores.
- Encabezamiento de paquete TPKT para delimitar las TPDU como se especifica en la cláusula 8, encabezamiento de paquete para delimitar unidades de datos en un tren de octetos.

NOTA 1 – Se requiere TPKT porque un servicio de trenes de octetos no marca cuándo se producen fronteras de unidades de datos.

- Transferencia de trenes de octetos con las características siguientes:
  - a) Servicio con conexión preservando la secuencia de octetos.
  - b) Frontera entre unidades de datos *no* mantenida como parte de la transferencia.
  - c) Tasa de errores residual suficientemente baja para utilizar como un servicio de red de tipo A.
  - d) Mecanismo de control de flujo para ejercer presión posterior sobre un transmisor.

NOTA 2 – A continuación se especifica un protocolo para la transferencia de trenes de octetos que es un ejemplo de lo anterior:

- a) RFC 793, Transmission control protocol.
- b) Por defecto, número de puerto de destino 1503 por RFC 1700, Assigned numbers, pero pueden utilizarse otros.

*Capa 3*

- Ordinariamente, RFC 791, 792, 919, 922, 950, 1112, protocolo Internet.

*Capa 2*

- Ordinariamente subcapas de control de enlace lógico y acceso al medio ISO/CEI 8802.

*Capa 1*

- Ordinariamente, medio físico ISO/CEI 8802.

## 8 Encabezamiento de paquete para delimitar unidades de datos en un tren de octetos

La Recomendación X.224 espera información a recibir y transmitir en unidades discretas denominadas unidades de datos del servicio de red (NSDU, *network service data unit*), que pueden ser una secuencia arbitraria de octetos. Aunque otras clases del protocolo de transporte pueden combinar más de una TPDU dentro de una sola NSDU, la clase 0 de la X.224 no utiliza esta facilidad. Por tanto, en el contexto de las pilas de protocolos T.123, una TPDU puede ser identificada con su NSDU subyacente.

Una diferencia fundamental entre el servicio de red esperado por la Recomendación X.224 y un servicio de transferencia de trenes de octetos, cuyas características se indican en 7.6, es que el segundo transporta una secuencia continua de octetos sin fronteras explícitas entre grupos relacionados de octetos.

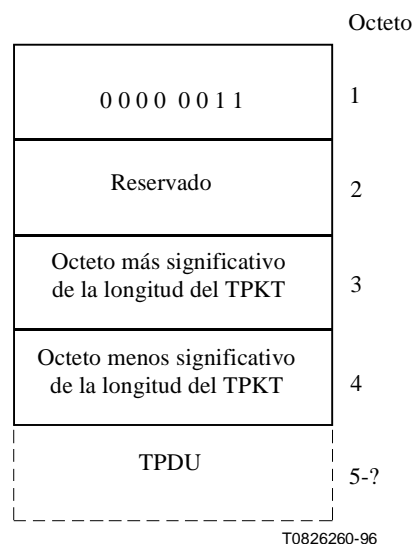
Esta cláusula especifica una capa de protocolo distinta para subsanar la discrepancia y satisface las necesidades de la Recomendación X.224. Define un formato de paquetes simple cuyo fin es delimitar las TPDU. Cada paquete, denominado un TPKT, es una unidad compuesta por un número entero de octetos, de longitud variable.

Un TPKT consta de dos partes: un encabezamiento de paquete seguido de una TPDU. El formato del encabezamiento de paquete es constante, independientemente del tipo de TPDU. El encabezamiento de paquete consta de cuatro octetos como se muestra en la figura 11.

El octeto 1 es un número de versión, con el valor binario 0000 0011. El octeto 2 queda en estudio. Los octetos 3 y 4 son la codificación binaria de 16 bits sin signo de la longitud del TPKT. Ésta es la longitud del paquete completo en octetos, incluido el encabezamiento de paquete y la TPDU.

Como una TPDU de la Recomendación X.224 ocupa al menos tres octetos, el valor mínimo de la longitud de TPKT es 7. El valor máximo es 65535. Esto permite un tamaño máximo de TPDU de 65531 octetos.

NOTA – La descripción de la capa de protocolo TPKT es conforme con RFC 1006, *ISO transport service on top of the TCP*.



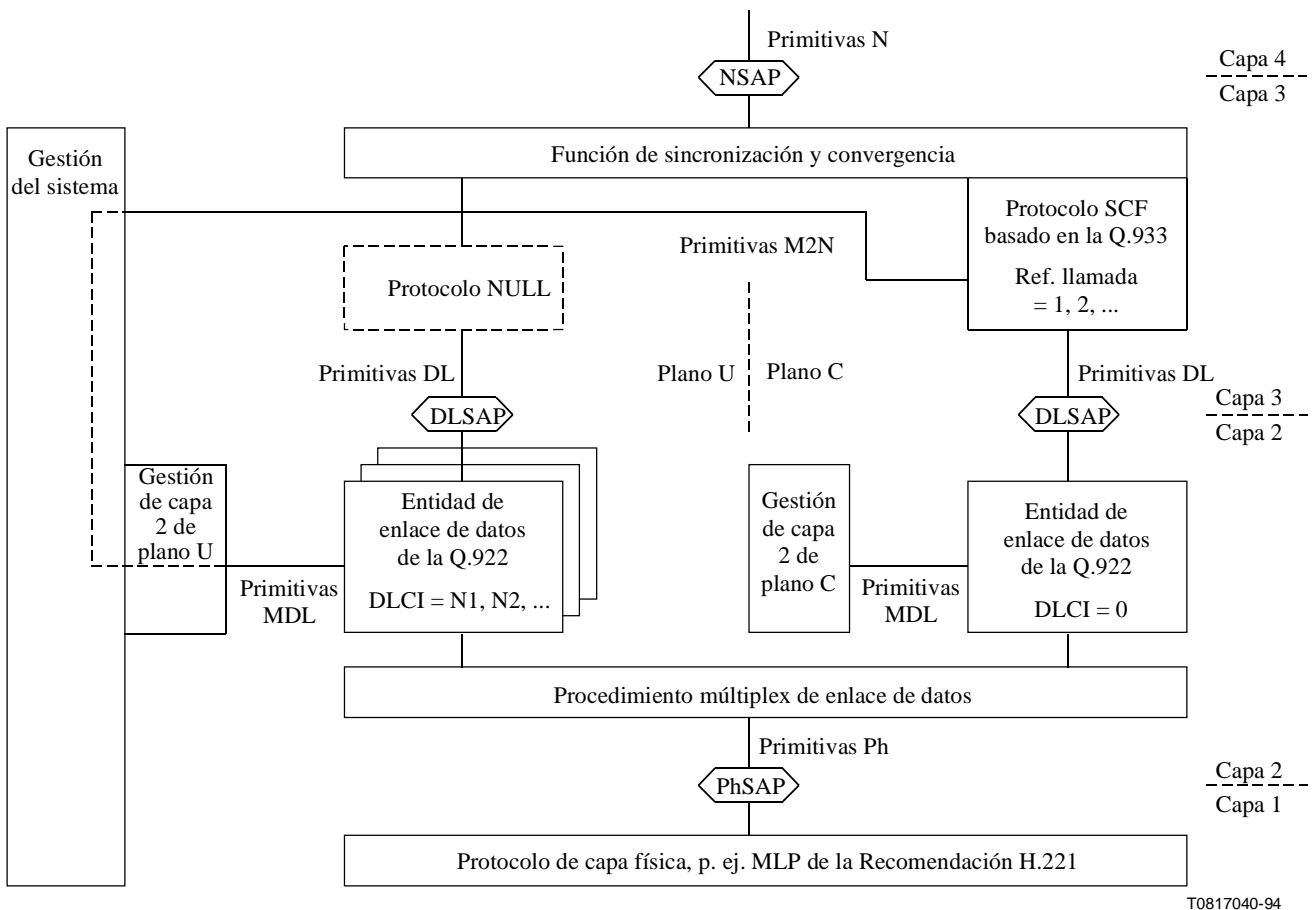
**Figura 11/T.123 – Formato del encabezamiento de paquete de un TPKT**



## 9 Función de sincronización y convergencia

### 9.1 Visión de la SCF

La SCF reside en la capa de red de cada perfil de comunicación cuya capa de enlace de datos se especifica en la Recomendación Q.922. Coordina el establecimiento y la liberación de la conexión entre el plano de control y el plano de usuario como se describe en la cláusula 4/Q.922. El propósito de la SCF es proporcionar servicios de red a la capa de transporte. En la figura 12 se ilustra el modelo arquitectural de la SCF.



**Figura 12/T.123 – Modelo arquitectural de la SCF**

En el cuadro 1 se enumeran los servicios de red requeridos por el protocolo de transporte de la Recomendación X.224. Este cuadro se deriva del cuadro 2/X.224 con exclusión de las características opcionales y de las primitivas N-REINICIACIÓN (en razón de que, conforme al cuadro A.3/X.224, N-REINICIACIÓN nunca se solicita, y cualquier indicación de la misma puede ser convertida a N-DESCONEXIÓN).

**Cuadro 1/T.123 – Servicios de red requeridos por la Recomendación X.224**

<b>Primitivas</b>	<b>Parámetros</b>
Petición N-CONEXIÓN Indicación N-CONEXIÓN	Dirección llamada Dirección llamante Conjunto de parámetros de QoS
Respuesta N-CONEXIÓN Confirmación N-CONEXIÓN	Dirección contestadora Conjunto de parámetros de QoS
Petición N-DATOS Indicación N-DATOS	Datos de usuario NS
Petición N-DESCONEXIÓN Indicación N-DESCONEXIÓN	

La SCF introduce las primitivas N-CONEXIÓN y N-DESCONEXIÓN. Durante la transferencia de datos permanece inactiva y la primitiva N-DATOS se pone en correspondencia directa con DL-DATOS sin protocolo adicional. Esto requiere que la capa de transporte limite el tamaño de sus TPDU a una trama I de la Recomendación Q.922.

La Recomendación Q.922 soporta múltiples conexiones de enlace de datos distinguidas por un DLCI. La SCF, actuando a través de la gestión de capa 2, controla las asignaciones de DLCI. Se comunica con una SCF par enviando y recibiendo mensajes conforme a la Recomendación Q.933 por el DLCI 0, que está reservado para señalización dentro del canal. El DLCI 0 sirve al plano de control, que soporta el control de la SCF. Otros DLCI sirven al plano de usuario, que soporta la transferencia de datos.

Los procedimientos de la SCF se basan en los especificados en la Recomendación Q.933, donde se define el caso A que trata del acceso del circuito conmutado a un manejador de trama distante y el caso B que trata del acceso integrado a un manejador de trama local. La utilización por la SCF de mensajes Q.933 se puede considerar un nuevo caso C que trata del acceso de circuitos conmutados directamente a otro usuario de red. Este nuevo caso C no utiliza DLCI para distinguir conexiones a destinos diferentes. Utiliza DLCI para distinguir conexiones múltiples entre los dos mismos puntos extremos. Cada una de estas conexiones puede tener una calidad de servicio diferente.

La secuencia de acciones para obtener un circuito físico entre dos usuarios puede variar con el perfil de la comunicación y con otras circunstancias. Un circuito se puede establecer sin la ayuda de SCF antes de las primeras primitivas de petición e indicación N-CONEXIÓN. Cuando finalmente se invocan estas primitivas, las direcciones llamada y llamante se pueden omitir o ignorar. Alternativamente, la petición N-CONEXIÓN puede iniciar eventos y se pueden requerir direcciones de red para el encaminamiento del circuito.

## **9.2 Procedimientos de la SCF**

La SCF actuará como usuario de red si tiene que actuar para el caso A de retransmisión de trama de la Recomendación Q.933. Se comportará como si estuviera conectada en forma semipermanente a un manejador de trama distante, aun cuando la velocidad binaria atribuida al circuito físico puede no ser exactamente una velocidad de transferencia de información RDSI.

La única excepción es 5.6/Q.933 referente a las colisiones entre los DLCI. Para mantener una relación simétrica entre dos usuarios de red, la SCF no debe dar preferencia a ninguna dirección como entrante. Por el contrario, resolverá colisiones forzando nuevas selecciones de DLCI en ambos lados, como se especifica en detalle más adelante.

La SCF deberá cumplir los requisitos adicionales establecidos en el resto de esta subcláusula.

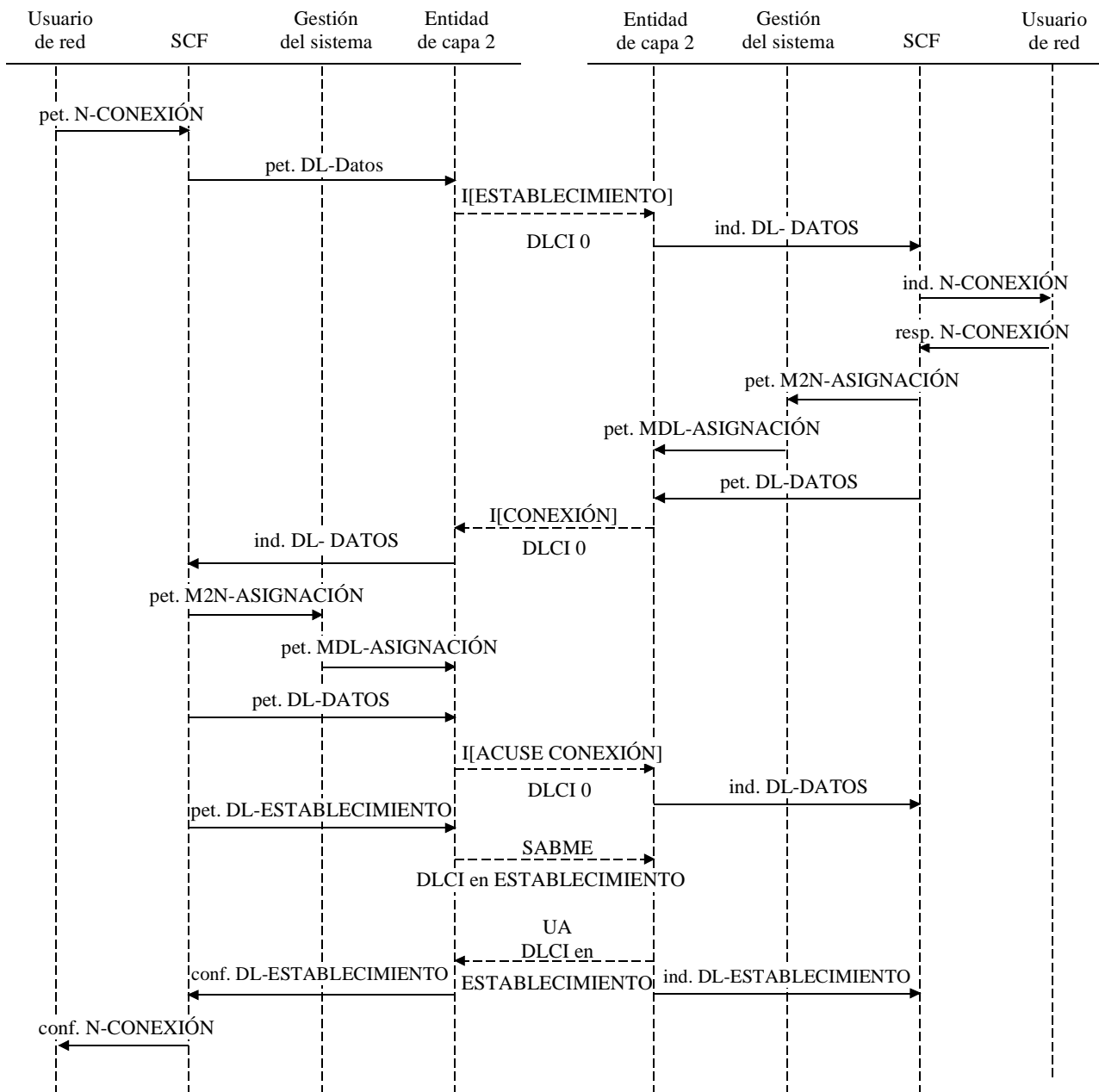
Tan pronto como se activa un circuito físico dúplex, la SCF asignará y establecerá un DLCI 0 para servir al plano de control. El DLCI 0 transportará mensajes de la Recomendación Q.933 en tramas I

de la Recomendación Q.922. Si se restablece DLCI 0, lo que indica un error de protocolo, la SCF hará que se libere. Si se libera DLCI 0, la SCF eliminará todos los demás DLCI asignados al circuito físico e indicará que sus enlaces de datos están desconectados. La SCF puede entonces intentar establecer DLCI 0 nuevamente y reinicializar de nuevo la señalización de la Recomendación Q.933.

Como respuesta positiva a ESTABLECIMIENTO, la SCF transmitirá CONEXIÓN, y esto será contestado por ACUSE DE CONEXIÓN. En esta situación no tiene utilidad transmitir AVISO, LLAMADA EN CURSO, o PROGRESIÓN. Si se reciben estos mensajes, pueden ser ignorados.

La respuesta negativa a ESTABLECIMIENTO será LIBERACIÓN COMPLETA. Ésta es la manera más sencilla de liberar una llamada activa. En esta situación no tiene utilidad transmitir DESCONEXIÓN, ESTADO, o INDAGACIÓN DE ESTADO. Si se reciben estos mensajes, pueden estimular la transmisión de LIBERACIÓN COMPLETA. Si se recibe LIBERACIÓN durante la mayoría de los estados de llamada especificados en la Recomendación Q.933, por ejemplo, mientras la llamada está activa pero no mientras se espera una respuesta a ESTABLECIMIENTO o LIBERACIÓN, causará la transmisión de LIBERACIÓN COMPLETA. Aunque una indicación LIBERACIÓN COMPLETA no esperada se considera un error de la secuencia de mensajes, con ella se consigue el efecto pretendido de forzar al receptor a liberar una comunicación.

La figura 13 muestra los mensajes intercambiados y las primitivas invocadas durante una primitiva N-CONEXIÓN satisfactoria. En esta figura se supone que ya está establecido DLCI 0 como resultado del intercambio SABME y UA cuando el circuito físico fue activado.



T0817050-94

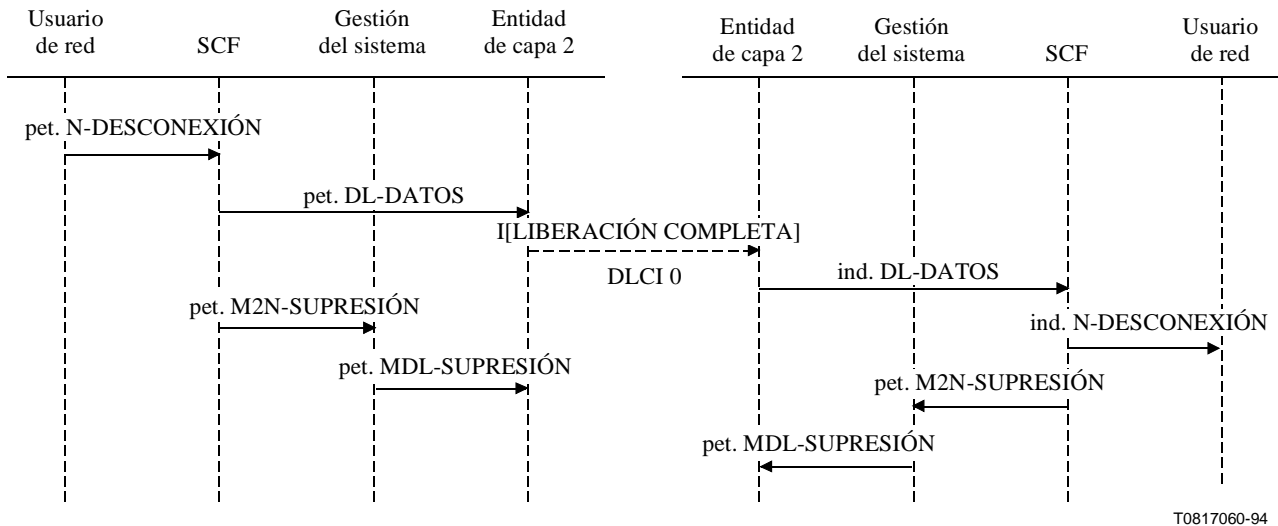
**Figura 13/T.123 – Secuencia de acciones para N-CONEXIÓN**

La SCF empleará valores de referencia de llamada (variables de 1 a 127 en cada lado) de un octeto y valores de DLCI (constituidos por 10 bits) de dos octetos. Los DLCI se seleccionarán aleatoriamente dentro de la gama atribuida por la Recomendación Q.922 para soportar la información de usuario, a saber, de 16 a 991 inclusive.

Una SCF que procese una petición N-CONEXIÓN propondrá un valor DLCI preferido en ESTABLECIMIENTO. Una SCF que reciba ESTABLECIMIENTO examinará el valor DLCI que contiene. Si el valor DLCI ya está asignado, se trata de un error. Si la SCF de recepción ha propuesto el mismo valor DLCI en un ESTABLECIMIENTO no respondido, contestará LIBERACIÓN COMPLETA con número de causa 44 *circuito/canal solicitado no disponible*. De otro modo aceptará el valor DLCI recibido. Su respuesta al mensaje ESTABLECIMIENTO dependerá entonces de la consideración de otros parámetros y de la voluntad del usuario de red. Si la respuesta es positiva, se devolverá el mismo valor DLCI en el mensaje CONEXIÓN; si es negativa, se devolverá un número de causa distinto de 44 en LIBERACIÓN COMPLETA. Una SCF que reciba una

respuesta LIBERACIÓN COMPLETA con número de causa 44 volverá a intentar su ESTABLECIMIENTO fallido con un nuevo valor DLCI seleccionado aleatoriamente. Si el número de intentos fuera excesivo, la SCF podrá optar por reactivar su generador de números aleatorios. Una SCF que reciba una respuesta de LIBERACIÓN COMPLETA con un número de causa distinto de 44 indicará por medio de N-DESCONEXIÓN que la petición N-CONEXIÓN ha fallado.

La figura 14 muestra los mensajes intercambiados y las primitivas invocadas tras una petición N-DESCONEXIÓN solicitada por el usuario. Nótese que no se requiere la petición DL-LIBERACIÓN ni la transmisión de DESC, ya que MDL-SUPRESIÓN de cada lado repone adecuadamente el estado del DLCI afectado.



**Figura 14/T.123 – Secuencia de acciones para N-DESCONEXIÓN**

Para evitar una condición de competitividad, la SCF debería demorar la reutilización de su referencia de llamada liberada para una nueva llamada si inició N-DESCONEXIÓN, por la razón de que si ambos lados desconectan y el llamante reconecta utilizando el mismo valor de referencia de llamada, una LIBERACIÓN COMPLETA en tránsito para la vieja llamada podría ser interpretada erróneamente como un fallo de la nueva llamada. La probabilidad de que esto ocurra se reduce al mínimo si la SCF elige a continuación su valor de referencia de llamada menos recientemente utilizada. En la práctica, puede bastar una asignación en serie de valores (incrementando en uno cada vez). Otra posibilidad es que la SCF decida emplear un procedimiento de desconexión más complicado, transmitiendo LIBERACIÓN y esperando LIBERACIÓN o LIBERACIÓN COMPLETA.

Un error no recuperado en la transferencia de datos en un DLCI viene indicado por DL-ESTABLECIMIENTO o DL-LIBERACIÓN, dependiendo del éxito de la reposición del enlace de datos. Cualquiera de estas primitivas hará que N-DESCONEXIÓN comience con una indicación en lugar de una petición, seguida por las acciones restantes de la figura 14. La excepción se produce si el DLCI 0 se ve afectado; esto tiene las consecuencias más severas especificadas anteriormente.

### 9.3 Mensajes de la SCF

Los elementos de información aparecen en un orden fijo, como se indica en los cuadros 2 a 5. Los del tipo M son obligatorios en la Recomendación Q.933 o son necesarios como parte de la especificación de la SCF. Los de tipo O son opcionales. Los elementos de información que no se indican aquí, no deben ser transmitidos y, si se reciben, pueden ser ignorados.

NOTA 1 – Si los selectores de NSAP para un proveedor de MCS se administran para ser nulos, como se recomienda en la cláusula 6, no resulta conveniente transportar elementos de información de subdirección como parte de los mensajes ESTABLECIMIENTO y CONEXIÓN. Sin embargo, pueden necesitarse selectores específicos para llegar a un proveedor de MCS en un contexto determinado. Su posible utilización como soporte de protocolos, distintos de los de la Recomendación T.125, que comparten el mismo circuito físico queda en estudio.

NOTA 2 – La codificación binaria preferida de una dirección de NSAP se especifica en A.8.3.1/X.213.

**Cuadro 2/T.123 – Contenido del mensaje ESTABLECIMIENTO**

<b>Elemento de información</b>	<b>Tipo</b>	<b>Notas</b>
Discriminador de protocolo	M	
Referencia de llamada	M	
Tipo de mensaje	M	
Capacidad portadora	M	Recomendación Q.922
DLCI	M	Preferido
Retardo de tránsito de extremo a extremo	O	Acumulativo, solicitado, máximo
Parámetros del núcleo de la capa de enlace	O	N201, caudal(es), mínimo(s)
Parámetros del protocolo de la capa de enlace	O	k, T200
Prioridad de la Recomendación X.213	O	Prioridad de datos, la menor aceptable
Subdirección de la parte llamante	O	Dirección NSAP
Subdirección de la parte llamada	O	Dirección NSAP

**Cuadro 3/T.123 – Contenido del mensaje CONEXIÓN**

<b>Elemento de información</b>	<b>Tipo</b>	<b>Notas</b>
Discriminador de protocolo	M	
Referencia de llamada	M	
Tipo de mensaje	M	
DLCI	M	Exclusiva
Retardo de tránsito de extremo a extremo	O	Acumulativo
Parámetros del núcleo de la capa de enlace	O	N201, caudal(es)
Parámetros del protocolo de la capa de enlace	O	k, T200
Subdirección conectada	O	Dirección NSAP
Prioridad de la Recomendación X.213	O	Prioridad de datos

**Cuadro 4/T.123 – Contenido del mensaje ACUSE CONEXIÓN**

<b>Elemento de información</b>	<b>Tipo</b>
Discriminador de protocolo	M
Referencia de llamada	M
Tipo de mensaje	M

**Cuadro 5/T.123 – Contenido del mensaje LIBERACIÓN COMPLETA**

<b>Elemento de información</b>	<b>Tipo</b>
Discriminador de protocolo	M
Referencia de llamada	M
Tipo de mensaje	M
Causa	M

#### **9.4 Parámetros de calidad de servicio**

Las características importantes de la transferencia de datos son el caudal, el retardo de tránsito y la prioridad, que forman parte del conjunto de parámetros QoS de N-CONEXIÓN. Los parámetros QoS están separados pero pueden influir en la elección de los parámetros de protocolo. La SCF puede llevar parámetros de ambas clases utilizando elementos de información opcionales en ESTABLECIMIENTO Y CONEXIÓN.

Las negociaciones de los parámetros se efectuarán de acuerdo con las reglas establecidas en 5.1.3.3/Q.933 y 5.2.3.3/Q.933.

Los parámetros de sistema de la Recomendación Q.922 que pueden ser negociados son: k, N201 y T200. Su valor será el mismo para ambos sentidos de la transferencia. Si estos parámetros no están expresamente señalizados, tomarán los valores por defecto indicados en la cláusula 10 siguiente.

Si los parámetros QoS no están expresamente señalizados, las cualidades correspondientes quedan indeterminadas y pueden tomar cualquier valor que sea conveniente a los proveedores de servicio.

Los parámetros QoS y de protocolo en CONEXIÓN, complementados por algún valor por defecto, constituirán los valores finales para el DLCI asignado. La SCF pasará estos valores a la entidad de capa 2 subyacente por medio de M2N-ASIGNACIÓN, que emerge del plano de gestión como MDL-ASIGNACIÓN. Esto está de acuerdo con 4.1.1.5/Q.922 y 4.1.1.10/Q.922, que indican que en estas primitivas pueden incluirse parámetros facultativos adicionales.

Los parámetros QoS y de protocolo de DLCI 0 no están expresamente señalizados. Los parámetros QoS serán implícitamente iguales o superiores que los de cualquier otro DLCI. Los parámetros de protocolo k, N201 y T200 para DLCI 0 tomarán los valores por defecto.

Una entidad de capa 2 puede incluir o no prioridad de datos como un parámetro QoS. En caso afirmativo, la prioridad relativa de los DLCI determinará el orden en que se da servicio a las peticiones de datos de usuario puestos en cola para transmisión, suponiendo que sus respectivos estados de protocolo están igualmente preparados. Los DLCI de la misma prioridad deben ser tratados imparcialmente.

La SCF expresará prioridades de datos utilizando la codificación del valor del elemento de información *prioridad de la Recomendación X.213* (que concuerda con la codificación de la capa paquete de la Recomendación X.25). La prioridad más baja será 0 y la más alta 14, como máximo. Las prioridades solicitadas se negociarán en el sentido descendente de la gama de valores que la entidad capa 2 subyacente puede implementar claramente, comenzando por 0.

## 10 Parámetros y opciones de protocolo de la Recomendación Q.922

El formato del campo de dirección será de dos octetos (DLCI de 10 bits).

Se reservan tres bits del campo de dirección para utilizarlos con el servicio de retransmisión de trama: notificación de congestión explícita hacia adelante (FECN, *forward explicit congestion notification*), notificación de congestión explícita hacia atrás (BECN, *backward explicit congestion notification*), e indicador de elegibilidad de descarte (DE, *discard eligibility*). El transmisor pondrá estos bits a 0 y el receptor los ignorará.

La transferencia de información se efectuará en tramas I que utilizan los procedimientos de la operación de acuse de trama múltiple.

Los tipos de trama UI y XID no se transmitirán.

Los parámetros del sistema están asociados con cada una de las conexiones de enlace de datos. Sus valores se deben fijar teniendo en cuenta las características del circuito físico subyacente. En el cuadro 6 se especifican los valores por defecto.

**Cuadro 6/T.123 – Valores por defecto de los parámetros del sistema de enlace de datos**

Parámetro del sistema	Valor por defecto	Descripción del parámetro
K	40	Número máximo de tramas I pendientes
N200	10	Número máximo de retransmisiones
N201	260	Número máximo de octetos en un campo de información
T200	1,5 s	Temporizador de retransmisión
T203	30 s	Temporizador de reposo

Los valores de k, N201 y T200 pueden ser negociados por la SCF especificada en la cláusula 9. Los valores de N200 y de T203 no necesitan ser comunicados del transmisor al receptor y se pueden fijar localmente en cada lado.

El valor de k por defecto es el máximo indicado en 5.9.4/Q.922 (para una velocidad de enlace de 1536-1920 Mbit/s). Este es también el valor indicado en el apéndice VI/T.90, independiente de la velocidad de enlace, para caudal óptimo con un tamaño de paquete de 256 octetos.

Un valor demasiado grande de k es mejor que un valor demasiado pequeño. Un receptor de la Q.922 no necesita aceptar una ventana completa de tramas I si las memorias tampón son insuficientes; puede fijar la condición *receptor propio ocupado* en algún punto intermedio. Además, un transmisor de la Recomendación Q.922 se puede autolimitar voluntariamente a un número más pequeño de tramas I pendientes; no está obligado a llenar la ventana a la capacidad máxima. Por otra parte, si k se fija en un valor pequeño y la ventana se llena con demasiada rapidez, se requerirá la interrupción del transmisor, ya que el caudal y la respuesta pueden resultar perjudicados.

En el apéndice I/Q.933 se presenta un procedimiento para negociar el valor de k utilizando una fórmula en la que figura el tamaño de la trama de datos en octetos.

Los implementadores deben considerar la posibilidad de limitar dinámicamente el tamaño de la trama a un valor más pequeño que el que permite el parámetro N201 del sistema. Quizá esto requiera la coordinación con la capa de transporte que forma las TPDU. Puede que convenga limitar el tiempo de transmisión en serie para el caso más desfavorable de datos de prioridad inferior, de tal modo que los datos de prioridad superior recién puestos en cola puedan ser servidos rápidamente. Se ha propuesto un retardo máximo de 60 ms.

También puede considerarse la opción alternativa de abortar una transmisión de baja prioridad que ya esté en curso.

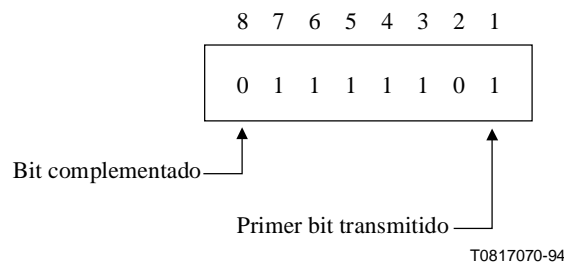


## 11 Transparencia de la estructura de trama del enlace de datos para la transmisión arrítmica

Puesto que la transmisión arrítmica está organizada como una secuencia de octetos, conviene utilizar un esquema de relleno de octetos para la transparencia de la estructura de trama del enlace de datos. Esta es una alternativa reconocida al esquema de relleno de bits (inserción de un bit 0 después de cada secuencia de cinco bits 1 contiguos), adecuada para la transmisión síncrona. De esta manera la aplicación de la Recomendación Q.922 para el perfil RTPC resulta más eficaz y sencilla, especialmente cuando se utiliza el puerto serie de un computador personal típico.

En el caso de la RTPC, no se aplicará 2.6/Q.922 que define la transparencia de la estructura de trama por referencia a la Recomendación Q.921. En su lugar se aplicará el siguiente procedimiento tomado de 4.5.2 de ISO/CEI 3309:

El octeto de escape de control es un identificador de transparencia que identifica un octeto que ocurre dentro de una trama a la que se aplica el siguiente procedimiento de transparencia. En la figura 15 se muestra la codificación del octeto de escape.



**Figura 15/T.123 – Octeto de escape de control para transparencia arrítmica**

El transmisor examinará el contenido de la trama entre las secuencias de bandera de apertura y de cierre que incluyen los campos de dirección, control y FCS, y, tras la compleción del cálculo de la FCS:

- complementará el sexto bit del octeto, en cuanto ocurra la bandera o un octeto de escape de control; y
- insertará un octeto de escape de control inmediatamente antes del octeto resultante de lo anterior, antes de la transmisión.

El transmisor puede incluir, opcionalmente, otros valores de octeto en el procedimiento de transparencia.

El receptor examinará el contenido de la trama entre los dos octetos de bandera y, en cuanto reciba un octeto de escape de control y antes del cálculo de la FCS:

- descartará el octeto de escape de control; y
- restablecerá el octeto inmediatamente siguiente complementando su sexto bit.

Una trama que termina con un octeto de escape de control seguido de una bandera de cierre no es válida y será ignorada por el receptor (aborto de trama).

NOTA – Este procedimiento no excluye la aparición de ningún carácter determinado dentro del tren de datos transmitido. En el caso de DTE y DCE separados, el control de flujo entre ellos mediante caracteres de instrucción (XON/XOFF) debe desactivarse, ya que no puede distinguirse de la transmisión de DTE a DTE de los mismos caracteres. Para la presente Recomendación, en este caso el control de flujo es una función del protocolo Q.922.

## **12 Subcapa física formada por los canales MLP H.221**

La utilización de los canales MLP y H-MLP H.221 se efectuará conforme a lo especificado en las Recomendaciones H.221, H.230, H.233, H.242 y H.243 para la integración de señales multimedios:

- Para determinar un modo de funcionamiento compatible, se aplica la secuencia A de intercambio de capacidad de la Recomendación H.242.
- Todos los sistemas que admiten protocolos multicapa (MLP) declararán por lo menos la capacidad común MLP-6,4k.
- Pueden declararse también otras velocidades binarias de MLP y H-MLP definidas en la Recomendación H.221.
- Para establecer o cambiar el modo, se aplica la secuencia B de conmutación de modo de la Recomendación H.242.
- Tras recibir una instrucción de apertura de MLP o H-MLP conforme a la Recomendación H.221, el sistema actuará para asegurar que al menos uno de estos protocolos está abierto en el sentido opuesto, de modo que pueda tener lugar la comunicación en dúplex.
- Las velocidades binarias de MLP y H-MLP no necesitan ser las mismas en ambos sentidos de transmisión, salvo que expresamente se exija simetría.
- La instrucción MCS (instrucción multipunto de transmisión simétrica de datos) de la Recomendación H.230 se aplica al MLP y al H-MLP, requiriendo que las velocidades binarias de salida se fijen igual que las de entrada.

Como se propone en 9.2/H.242, si tanto el MLP como el H-MLP están activos, se combinarán sus respectivas velocidades binarias para formar un solo tren de bits en serie. Las posiciones de los bits se enumerarán horizontalmente a lo largo de la trama H.221 sincronizada de los canales inicial y adicional, como se ilustra en los cuadros 7 a 9.

Las instrucciones de la Recomendación H.221 para fijar la velocidad de MLP o de H-MLP no interrumpirán la continuidad lógica del tren de bits serie combinado. La entrada o salida de bits continuará simplemente en la próxima submultitrama a una velocidad modificada. El funcionamiento de los protocolos de capa superior no será perturbado a menos que la velocidad binaria se reduzca demasiado durante un largo periodo de tiempo.

En particular, MLP o H-MLP, o ambos, pueden desactivarse temporalmente en el proceso de reordenar las velocidades de datos de un multiplex multimedios. Esta causa no es en sí suficiente para desconectar involuntariamente enlaces de datos Q.922. Esta acción sólo se ejercerá, en ausencia de errores detectados de protocolo, al recibo de la instrucción H.221 T.120-off.

**Cuadro 7/T.123 – Posiciones de bits para MLP-6,4k,  
restringido, con encriptación activa**

Canal inicial							
1	2	3	4	5	6	7	8
						FAS	1
							1
							1
						BAS	1
							1
						ECS	1
							1
						M1	1
						M2	1
						•	1
						•	1
						M55	1
						M56	1
FAS Señal de alineación de trama ( <i>frame alignment signal</i> ) BAS Señal de asignación de velocidad binaria ( <i>bit-rate allocation signal</i> ) ECS Señal de control de encriptación ( <i>encryption control signal</i> )							

**Cuadro 8/T.123 – Posiciones de bits para MLP-6,4k más H-MLP-62,4k**

Canal inicial								Canal adicional							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
								M1	M2	M3	M4	M5	M6	M7	
							FAS	M8	•	•	•	•	•	M14	FAS
								•	•	•	•	•	•	•	
							BAS	•	•	•	•	•	•	•	BAS
								M106	•	•	•	•	•	M112	
							M113	M114	•	•	•	•	•	M120	M121
							•	•	•	•	•	•	•	•	•
							•	•	•	•	•	•	•	•	•
							M680	•	•	•	•	•	•	•	M688

**Cuadro 9/T.123 – Posiciones de bits para H-MLP-128k en un canal H0**

Intervalo de tiempo 1	Intervalo de tiempo 2	Intervalo de tiempo 3	Intervalo de tiempo 4	Intervalo de tiempo 5	Intervalo de tiempo 6
	M1    • • •    M8	M9    • • •    M16			
	M17   • • •    •	•       • • •    M32			
	•       • • •    •	•       • • •    •			
	•       • • •    •	•       • • •    •			
	M1265 • • •    •	•       • • •    M1280			

### 13 Perfiles alternativos

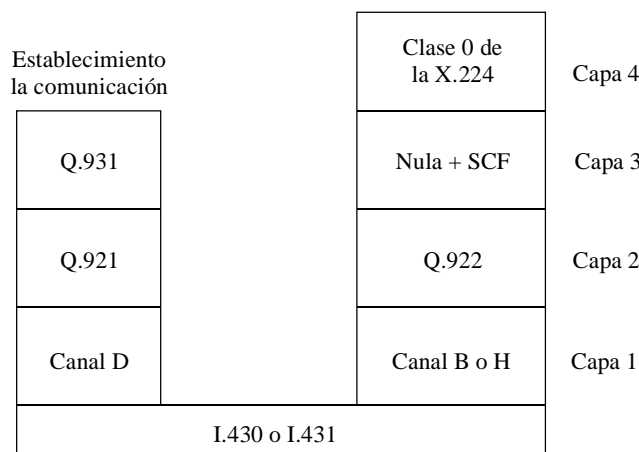
Estas alternativas están concebidas para permitir conexiones punto a punto entre terminales o MCU en circunstancias especiales. Su uso puede especificarse en la Recomendación del sistema para un determinado servicio o puede acordarse bilateralmente.

El conjunto de perfiles alternativos no es completo y no pretende ser una lista exhaustiva de todas las posibilidades.

No se ofrecen aquí procedimientos por los que los terminales puedan descubrir el hecho de que pueden compartir un perfil común, ni se adopta disposición alguna para la negociación, en el caso de que compartan más de uno. La codificación de los elementos de información de control de llamada Q.931 o Q.2931 puede restringir el conjunto de perfiles que pueden considerarse, pero no puede garantizar un resultado exitoso. Estos problemas son parte de una concesión más amplia, que puede decidir hacer referencia a esta Recomendación.

#### 13.1 Alternativa: RDSI basada en la Recomendación Q.922

La figura 16 define un perfil alternativo para la RDSI basada en la Recomendación Q.922. Cuando no se requiere vídeo y puede asignársele al audio su propio canal, resulta una pila de protocolos menos costosa de implementar que la H.221. Las capas por encima del canal B o H son idénticas al perfil básico RDSI.



T0826270-96

**Figura 16/T.123 – Perfil alternativo para la RDSI basada en la Recomendación Q.922**

*Capa 4*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 3*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 2*

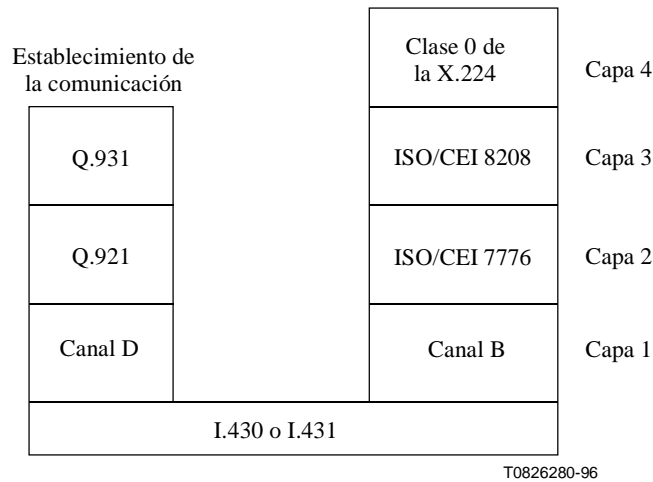
- Como se especifica en 7.1, perfil básico RDSI.

*Capa 1*

- Un canal B, un canal H0 o un canal H1.
- Algunas redes pueden también ofrecer canales de velocidad binaria intermedia.

**13.2 Alternativa: RDSI basada en la Recomendación T.90**

La figura 17 define un perfil alternativo para la RDSI basada en la Recomendación T.90. Aunque menos eficaz que Q.922, la pila de protocolos X.25 es más familiar como un componente de terminales telemáticos.



**Figura 17/T.123 – Perfil alternativo para la RDSI basada en la Recomendación T.90**

*Capa 4*

- X.224.
- Clase 0 preferida, sin clase alternativa.

*Capa 3*

- Comunicación DTE-DTE como se especifica en la cláusula 2/T.90.

*Capa 2*

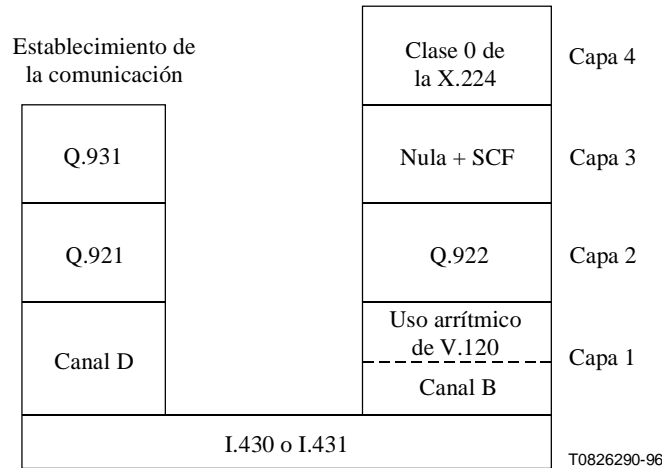
- Comunicación DTE-DTE como se especifica en la cláusula 2/T.90.

*Capa 1*

- Comunicación DTE-DTE como se especifica en la cláusula 2/T.90.

### 13.3 Alternativa: RDSI basada en la Recomendación V.120

La figura 18 define un perfil alternativo para una RDSI basada en la Recomendación V.120. Esta pila de protocolos da un acceso típico por computador personal a velocidades de la RDSI mediante un adaptador de terminal común. Las capas por encima de la adaptación de terminal son idénticas al perfil básico de la RTPC.



**Figura 18/T.123 – Perfil alternativo para la RDSI basada en la Recomendación V.120**

#### Capa 4

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 3

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 2

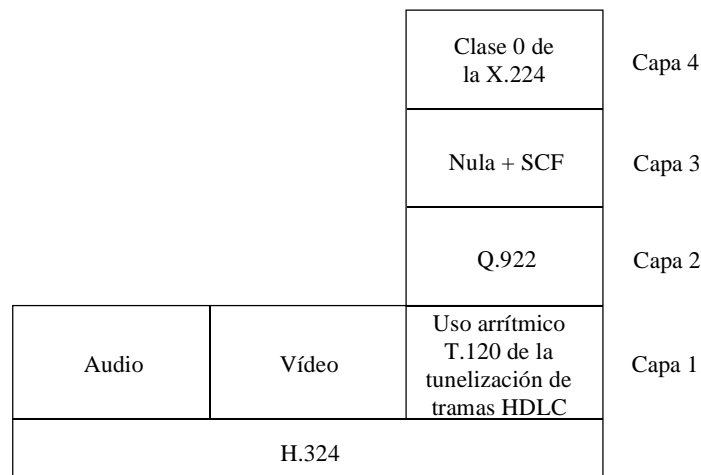
- Como se especifica en 7.4, perfil básico RDSI.

#### Capa 1

- Transmisión arrítmica por el DTE.
- DCE como se especifica en el funcionamiento en modo asíncrono V.120.
- El DTE y el DCE pueden ser funciones lógicas que no estén físicamente separadas, si el equipo integrado puede producir las mismas señales transmitidas.

### 13.4 Alternativa: RTPC basada en la Recomendación H.324

La figura 19 define un perfil alternativo para una RTPC basada en la Recomendación H.324. Esto permite una amplia instalación de la conferencia de datos en unión del videoteléfono de la RTPC. La correspondencia de tramas Q.922 a AL-SDU es una mejor utilización de una anchura de banda escasa que otras posibles disposiciones de tramas. Las capas por encima de la adaptación son idénticas al perfil básico RTPC.



T0826300-96

**Figura 19/T.123 – Perfil alternativo para una RTPC basada en la Recomendación H.324**

*Capa 4*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 3*

- Como se especifica en 7.1, perfil básico RDSI.

*Capa 2*

- Como se especifica en 7.4, perfil básico RDSI.

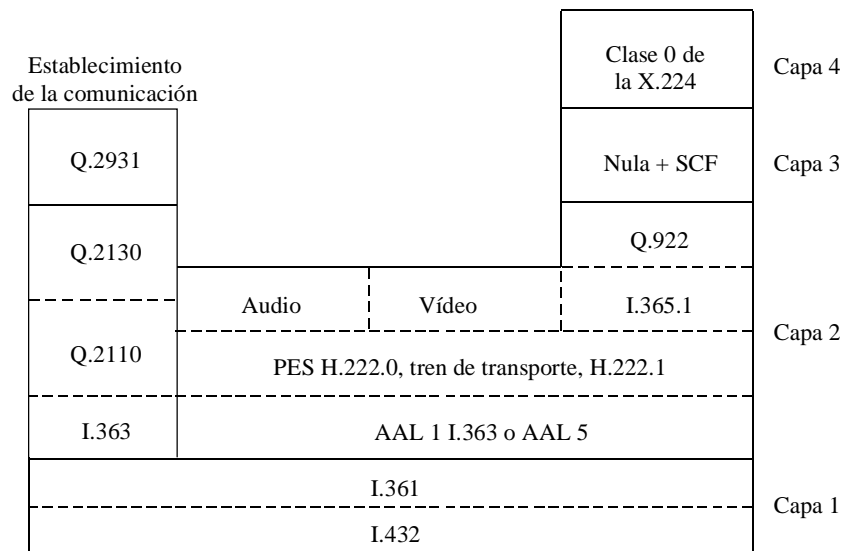
*Capa 1*

- Transmisión arrítmica por el DTE.
- DCE como se especifica en la tunelización de tramas HDLC H.324 para la Recomendación T.120.
- El DTE y el DCE pueden ser funciones lógicas que no estén físicamente separadas, si el equipo integrado puede producir las mismas señales transmitidas.

NOTA – El efecto neto es que el contenido de una trama Q.922, incluida FCS pero sin tramas ni transparencia, es transportado como una AL-SDU utilizando AL1 con alineación de trama por un canal lógico H.223 abierto para la aplicación de datos T.120.

**13.5 Alternativa: RDSI-BA basada en la Recomendación H.222**

La figura 20 define un perfil alternativo para una RDSI-BA basada en la Recomendación H.222. Esta pila de protocolos multiplexa audio, vídeo y datos junto con un único canal virtual ATM. Las capas por encima de Q.922 son idénticas al perfil básico RDSI.



T0826310-96

**Figura 20/T.123 – Perfil alternativo para la RDSI-BA basada en la Recomendación H.222**

#### Capa 4

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 3

- Como se especifica en 7.1, perfil básico RDSI.

#### Capa 2

- Q.922.
- Parámetros y opciones de protocolo como se especifican en la cláusula 10, parámetros y opciones de protocolo de la Recomendación Q.922.
- Estructura de trama modificada: sin utilización de banderas ni transparencia.
- Cada trama (octetos de dirección a través de FCS) transportada como los bytes de datos de un paquete PES en el tren elemental de datos definido en la Recomendación H.222.1 para el subcanal T.120 de tipo de protocolo.
- Transmisión de trenes de transporte como se especifica en la Recomendación H.222.1.

NOTA – El indicador de comienzo de unidad de cabida útil clasifica cada paquete de tren de transporte que contiene sea el primer segmento o un segmento de continuación de un paquete PES. Si un segmento es menor que el tamaño máximo, la diferencia es absorbida por bytes de relleno antes de que el encabezamiento de paquete PES hasta un total de 188 bytes.

#### Capa 1

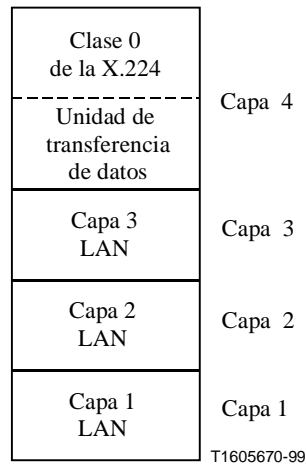
- Canal virtual ATM.

### 13.6 Alternativa: LAN basada en la transferencia de unidades de datos

La figura 21 define un perfil alternativo para una LAN basada en la transferencia de unidades de datos. Alineando las TPDU con unidades de datos de la LAN subyacente, dicha pila de protocolos puede eliminar alguna gestión de memoria tampón. Aunque su característica de segmentación no puede añadir nada a lo que ya ofrece la LAN, X.224 se recomienda para mayor uniformidad y como base para futuras mejoras.



NOTA – No se nombra aquí ningún protocolo LAN, porque los servicios comercialmente importantes son más conocidos mediante sus interfaces de programación de aplicaciones. Los protocolos que soportan un servicio pueden ser no revelados ni documentados.



**Figura 21/T.123 – Perfil alternativo para la LAN basado en la transferencia de unidades de datos**

*Capa 4*

- Clase 0 X.224 preferida, sin clase alternativa.
- El tamaño máximo de TPDU no superará la máxima unidad de datos LAN.
- Transferencia de unidades de datos con las características siguientes:
  - a) Servicio orientado a la conexión que preserva la secuencia de octetos.
  - b) Límite entre unidades de datos mantenido como parte de la transferencia.
  - c) Tasa de errores residual suficientemente baja para utilizarla como un servicio de red de tipo A.
  - d) Mecanismo de control de flujo para ejercer presión posterior sobre un transmisor.

NOTA 1 – NetBIOS Extended User Interface (NetBEUI), NetWare Sequenced Packet Exchange (SPX), y AppleTalk Data Stream Protocol (ADSP) son ejemplos de lo anterior.

NOTA 2 – En el caso de SPX y ADSP las fronteras de unidades de datos se marcan fijando un bit de fin de mensaje.

*Capa 3*

- Ejemplos ordinarios son NetWare Internetwork Packet eXchange (IPX) y Apple Datagram Delivery Protocol (DDP).

*Capa 2*

- Ordinariamente, subcapas de control de enlace lógico y de acceso al medio ISO/CEI 8802.

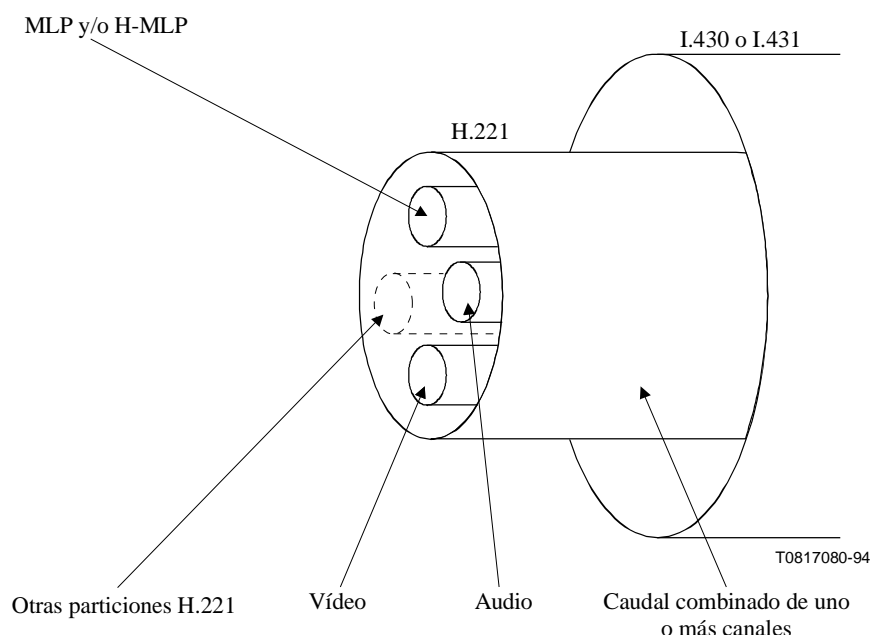
*Capa 1*

- Ordinariamente, medio físico ISO/CEI 8802.

## ANEXO A

### Integración de señales multimedia organizadas conforme a la Recomendación H.221

La figura A.1 ilustra cómo se combina el caudal de uno o más canales digitales y las particiones subsiguientes de la velocidad de transferencia total en atribuciones de velocidad binaria para cada medio, según la Recomendación H.221.



**Figura A.1/T.123 – Integración de señales multimedia organizadas conforme a la Recomendación H.221**

## ANEXO B

### Conexiones de transporte ampliadas

#### B.1 Alcance

Este anexo define un procedimiento y un protocolo que permitirán conexiones de transporte para que una conferencia T.120 negocie la disponibilidad de servicio de transporte ampliados. Estos servicios pueden incluir utilización de protocolos de seguridad, protocolos de transporte, niveles de fiabilidad para la transferencia de datos y soporte de alias de dirección. Esta negociación está destinada a proporcionar compatibilidad hacia atrás de las pilas de transporte T.123 que sólo soportan conexiones de transporte básicas.

#### B.2 Referencias normativas

- Recomendación UIT-T H.225.0 (1998), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes.*

- Recomendación UIT-T X.234 (1994) | ISO/CEI 8602:1995, *Tecnología de la información – Protocolo para proporcionar el servicio de transporte en modo sin conexión de interconexión de sistemas abiertos.*
- Recomendación UIT-T X.234 (1994)/enm.1 (1995) | ISO/CEI 8602:1995/enm.1:1996, *Tecnología de la información – Protocolo para proporcionar el servicio de transporte en modo sin conexión de interconexión de sistemas abiertos – Enmienda 1: Adición de la capacidad multidifusión en modo sin conexión.*
- Recomendación UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Tecnología de la información – Intercambio de telecomunicaciones e información entre sistemas – Protocolo de seguridad de la capa de transporte.*
- Recomendación UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica.*
- Recomendación UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Tecnología de la información – Notación de sintaxis abstracta uno – Especificación de objetos de información.*
- Recomendación UIT-T X.691 (1997) | ISO/CEI 8825-2:1998, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno – Especificación de las reglas de codificación compactada.*

### B.3 Definiciones

**B.3.1 pila de transporte básica:** Pila de transporte que no soporta los procedimientos ni el protocolo definidos en este anexo, pero que cumple no obstante la Recomendación T.123.

**B.3.2 pila de transporte ampliada:** Pila de transporte T.123 que soporta los procedimientos y el protocolo definidos en este anexo.

**B.3.3 conexión de red:** Conexión entre dos nodos T.120 que utiliza un conjunto de protocolos específico.

**B.3.4 protocolo fiable:** Protocolo que garantiza que los datos llegarán a su destino completos, incorruptos y en el orden en el que se transmitieron. TCP es un ejemplo de protocolo no fiable.

**B.3.5 conexión de transporte:** Conexión lógica entre dos nodos T.120 que utiliza una o más conexiones de red.

**B.3.6 protocolo no fiable:** Protocolo que no garantiza que los datos llegarán a su destino completos, incorruptos y en el orden en el que se transmitieron. UDP es un ejemplo de protocolo no fiable.

### B.4 Abreviaturas

CNP	Protocolo de negociación de la conexión ( <i>connection negotiation protocol</i> )
CNPPDU	Unidad de datos de protocolo del protocolo de negociación de la conexión ( <i>connection negotiation protocol – protocol data unit</i> )
IP	Protocolo Internet ( <i>Internet protocol</i> )
IPSec	Seguridad del protocolo Internet ( <i>Internet protocol security</i> )
MAP	Protocolo de adaptación multidifusión ( <i>multicast adaptation protocol</i> ) (definido en el anexo A/T.125)
MCS	Servicio de comunicación multipunto ( <i>multipoint communication service</i> )
NSDU	Unidad de datos del servicio de red ( <i>network service data unit</i> )
PDU	Unidad de datos de protocolo ( <i>protocol data unit</i> )

SAR	Segmentación y reensamblado ( <i>segmentation and reassembly</i> )
SSL	Capa de zócalos seguros ( <i>secure sockets layer</i> )
TCP	Protocolo de control de la transmisión ( <i>transmission control protocol</i> )
TLS	Seguridad del nivel de transporte ( <i>transport layer security</i> ) (protocolo, definido por IETF Internet draft)
TLSP	Protocolo de seguridad del nivel de transporte ( <i>transport layer security protocol</i> ) (definido por la Recomendación UIT-T X.274)
TPDU	Unidad de datos de protocolo de transporte ( <i>transport protocol data unit</i> )
TSDU	Unidad de datos de servicio de transporte ( <i>transport service data unit</i> )
UDP	Protocolo de datagrama de usuario ( <i>user datagram protocol</i> )

## B.5 Convenios

- En este anexo los verbos en futuro (traducción de "shall") indican un requisito obligatorio, mientras que en condicional ("should") indican un procedimiento o característica sugeridos pero opcionales. El término poder (may) se refiere a un desarrollo opcional sin expresar una preferencia.
- A menos que se especifique otra cosa, se utilizará la codificación PER de variantes alineadas de ASN.1 en toda la ASN.1 especificada en este anexo.
- Los bits de un octeto se enumeran de 1 a 8, siendo el bit 1 el bit de orden más bajo.
- Los octetos de una TPDU se enumeran a partir de 1 y aumentando en el orden en el que se ponen en una NSDU.
- Todos los mensajes y campos de mensaje X.224 van en *CURSIVAS MAYÚSCULAS*.
- Todos los elementos ASN.1 y elementos de estructura de octetos del CNP van en **negritas**.

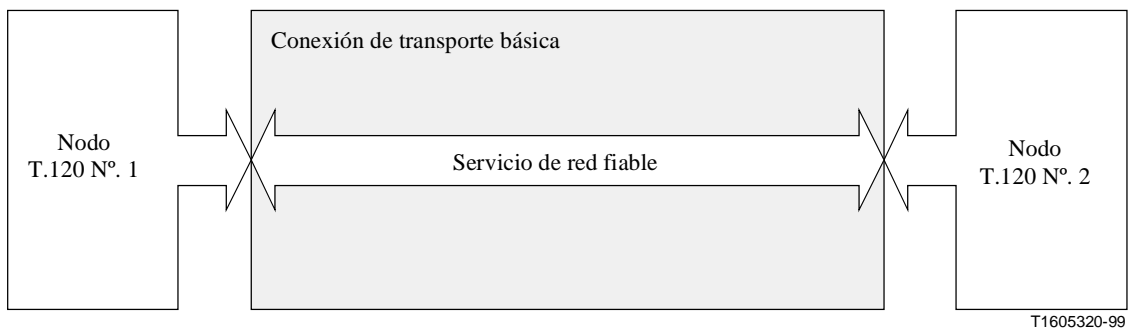
## B.6 Sinopsis

El servicio de transporte básico T.123 se limita a la transferencia totalmente fiable de datos entre nodos. Se ha determinado la necesidad de servicios de transporte no soportados en las pilas de transporte básicas. Entre estos servicios están la seguridad, la transferencia de datos no fiable y el direccionamiento por alias.

Como el protocolo X.224 no puede ampliarse arbitrariamente, estos servicios no pueden añadirse simplemente a la definición de la Recomendación T.123 de una conexión de transporte básica, pero manteniendo la compatibilidad hacia atrás. En respuesta a este problema, los procedimientos y el protocolo de este anexo definen una conexión de transporte ampliada con servicios que pueden negociarse y ampliarse.

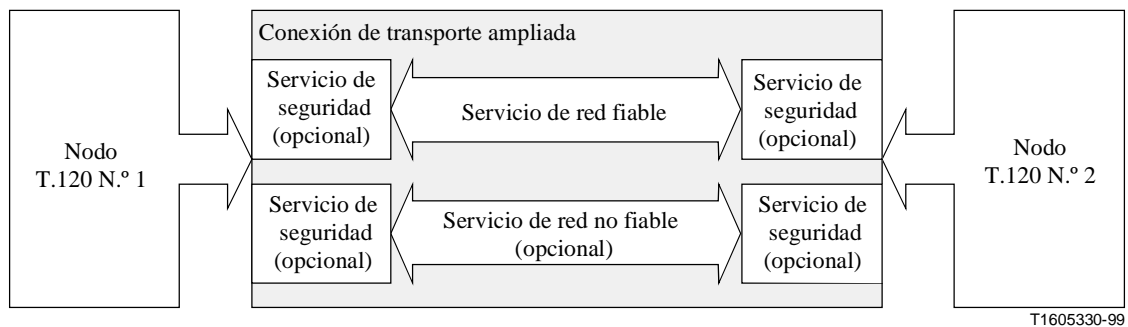
### B.6.1 Modelo de conexión de transporte ampliada

El modelo de conexión de transporte básica T.123 se muestra en la figura B.1. Las conexiones de este tipo proporcionan un servicio de comunicación entre nodos T.120 utilizando una única conexión de red fiable. La dirección de red específica del nodo llamado debe ser conocida para que se establezca una conexión de este tipo. Además, ni los servicios de seguridad ni los servicios de transferencia no fiable de datos pueden proporcionarse con este tipo de conexión.



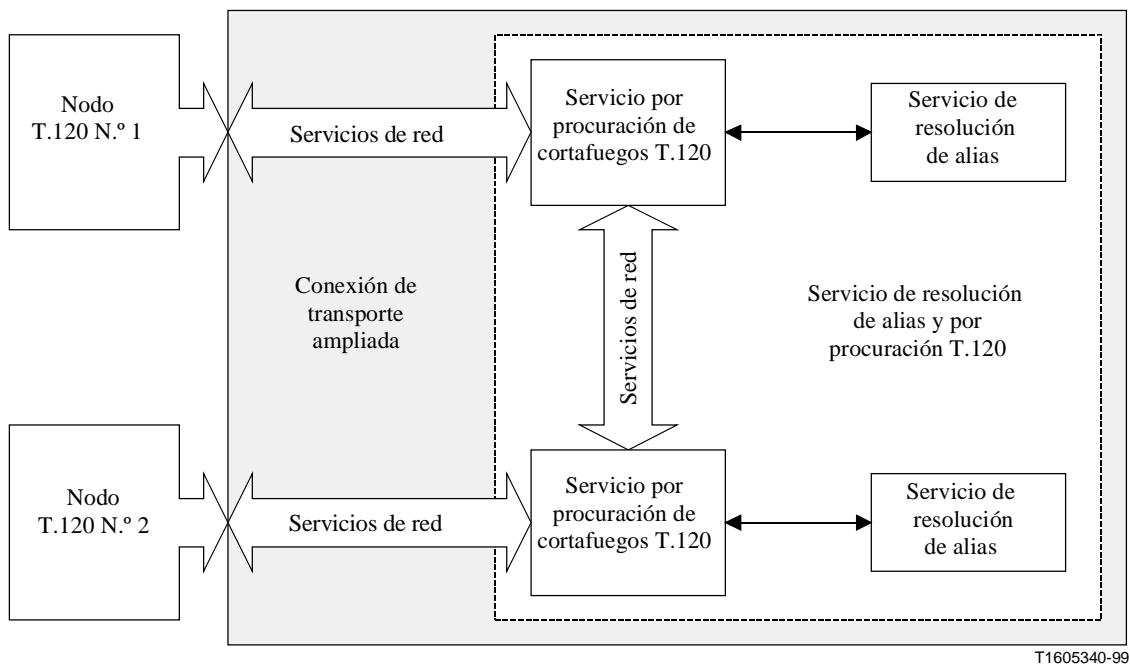
**Figura B.1/T.123 – Modelo de conexión de transporte básica**

Para añadir servicios ampliados a los transportes T.123, se define un nuevo modelo de conexión. Este modelo se muestra en la figura B.2. En este modelo, una conexión de transporte consta de uno o más servicios de red, lógicamente vinculados. Estos servicios pueden incluir transferencia fiable y no fiable de datos así como servicios de seguridad para datos transmitidos. Este modelo es funcionalmente equivalente al modelo básico cuando se omiten todos los servicios opcionales.



**Figura B.2/T.123 – Modelo de conexión de transporte ampliada**

Además de los servicios de seguridad y fiabilidad, este anexo especifica un método para utilizar una lista de direcciones de alias para establecer conexiones de transporte ampliadas. Estos alias pueden ser utilizados con una serie de fines, como son los servicios por procuración, de pasarela y de redireccionamiento de llamada para comunicaciones T.120. En la figura B.3 se muestra un ejemplo de este tipo de conexión de transporte ampliada.



**Figura B.3/T.123 – Ejemplo de conexión de transporte ampliada por procuración T.120**

### B.6.2 Servicios de transporte

Aunque una variedad de servicios de transporte pueden negociarse utilizando los procedimientos y el protocolo de este anexo, la especificación exacta de muchos de estos servicios cae fuera del alcance de esta Recomendación. En particular, las definiciones de los servicios de pasarelas y por procuración T.120 quedan en estudio.

Debe también señalarse que muchos servicios de seguridad están implícitamente definidos en este anexo. Cuando no se especifica otra cosa, los mecanismos utilizados para proporcionar y controlar estos servicios (por ejemplo, obtención de certificados e intercambio de claves fuera de banda) se dejan a criterio de los implementadores.

### B.6.3 Uso modificado de la Recomendación X.224

La Recomendación T.123 establece el uso del protocolo de clase 0 X.224 para las conexiones básicas. Es conveniente que el establecimiento de la conexión ampliada siga siendo compatible con el establecimiento de la conexión básica. Para lograr este objetivo, la información para las negociaciones de la conexión ampliada se encapsulará dentro de las TPDU *PETICIÓN DE CONEXIÓN (CR) CONFIRMACIÓN DE CONEXIÓN (CC)* y *PETICIÓN DE DESCONEXIÓN (DR)* de la Recomendación X.224. Los detalles de este procedimiento se indican en B.7 Conexiones de transporte ampliadas.

### B.6.4 Protocolo de negociación de la conexión

Este anexo define el protocolo que se utilizará para establecer conexiones de transporte ampliadas. El protocolo de negociación de la conexión (CNP, *connection negotiation protocol*) está diseñado para su encapsulación en el X.224 o para su uso para protocolo independiente por una conexión de red fiable. Para permitir la ampliación del protocolo, CNP se define utilizando ASN.1 para su control de las PDU. Los detalles del CNP se indican en B.9 Protocolo de negociación de la conexión (CNP).

## B.7 Conexiones de transporte ampliadas

La finalidad de esta subcláusula es definir el procedimiento para establecer conexiones de transporte ampliadas. Este procedimiento de conexión ampliada está destinado a permitir que un nodo T.120 establezca una conexión de transporte con otro nodo T.120 sin conocimiento anterior de la aptitud del modo ganado para soportar conexiones de transporte ampliadas.

### B.7.1 Establecimiento de la conexión inicial

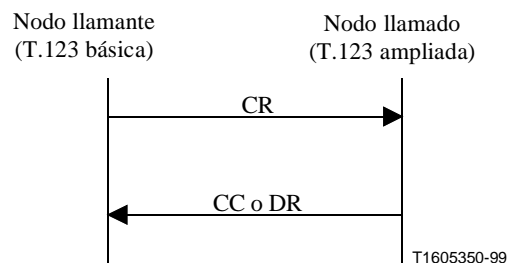
La Recomendación X.224 define el campo *SELECTOR DE TRANSPORTE* como un campo opcional de longitud variable en la parte variable de sus encabezamientos de PDU. Como se define en 6.5.5/X.224, "indica los puntos de acceso al servicio de transporte llamante y llamado". Este campo opcional no es utilizado por la X.224, ni por la T.123 básica. Esta subcláusula define su utilización en los nodos T.120 para soportar conexiones de transporte ampliadas.

Los nodos que soportan conexiones de transporte ampliadas soportarán el uso del campo *SELECTOR DE TRANSPORTE* en la *TPDU PETICIÓN DE CONEXIÓN (CR)* y en la *TPDU CONFIRMACIÓN DE CONEXIÓN (CC)* X.224. Se soportará también la parte variable de la *TPDU PETICIÓN DE DESCONEXIÓN (DR)*. El campo *SELECTOR DE TRANSPORTE* de la *CR-TPDU*, *CC-TPDU* y la parte variable de la *DR-TPDU* contendrá las CNP PDU especificadas en B.9 Protocolo de negociación de la conexión (CNP). En todos los casos se respetará el límite de 128 octetos fijado por la X.224 para la *CR-TPDU* y la *DR-TPDU*.

Los nodos T.120 que soportan conexiones de transporte ampliadas soportarán los siguientes modelos de llamada.

#### B.7.1.1 Establecimiento de llamada desde un transporte básico

Este modelo de llamada se utiliza cuando un nodo T.120 que soporta sólo conexiones básicas trata de conectarse a un nodo que soporta conexiones ampliadas. Véase la figura B.4.

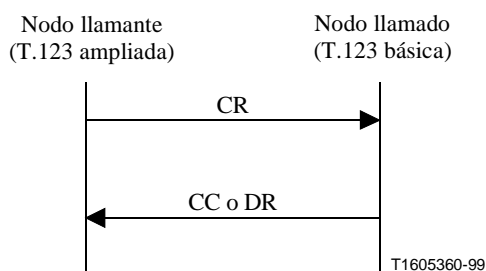


**Figura B.4/T.123 – Llamada de T.123 básica a T.123 ampliada**

Este modelo es señalado en el nodo llamado cuando se recibe una *CR-TPDU* que no contiene un campo *SELECTOR DE TRANSPORTE*. En este caso, el nodo llamado responderá con arreglo al establecimiento de conexión definido para las conexiones T.123 básicas. Una respuesta de *CC-TPDU* no contendrá un campo *SELECTOR DE TRANSPORTE*. Una respuesta de *DR-TPDU* no contendrá la parte variable del encabezamiento de PDU. Si se acepta la conexión, el nodo llamado tratará la conexión como una conexión básica.

#### B.7.1.2 Establecimiento de llamada a un transporte básico

Este modelo de llamada se utiliza cuando un nodo T.120 que soporta conexiones ampliadas trata de conectarse a un modo que soporta sólo conexiones básicas. Véase la figura B.5.

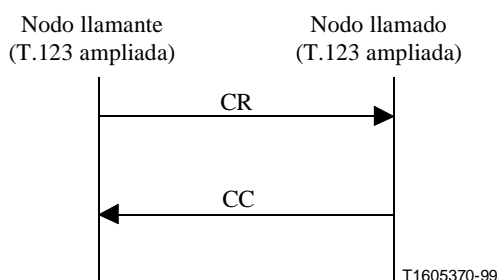


**Figura B.5/T.123 – Llamada de T.123 ampliada a T.123 básica**

En este modelo, el nodo llamante colocará un campo *SELECTOR DE TRANSPORTE* en la *CR-TPDU*. El nodo básico ignorará el campo y responderá con una *CC-TPDU* sin un campo *SELECTOR DE TRANSPORTE* o una *DR-TPD* sin una parte variable. Este modelo de llamada es señalado al nodo de transporte cuando se recibe la *TPDU* de respuesta y no contiene el campo opcional apropiado. Si se acepta la conexión, el nodo llamante tratará la conexión como una conexión básica.

### B.7.1.3 Establecimiento de llamada utilizando la conexión de red inicial

El modelo de llamada se utiliza cuando un nodo T.120 que soporta conexiones ampliadas intenta conectarse a un nodo que también soporta conexiones ampliadas. En este caso, el nodo llamado determina que los servicios disponibles con la conexión de red existentes son suficientes y se acepta la conexión T.120. Véase la figura B.6.



**Figura B.6/T.123 – Llamada entre nodos de T.123 ampliada –  
Seleccionada conexión de red existente**

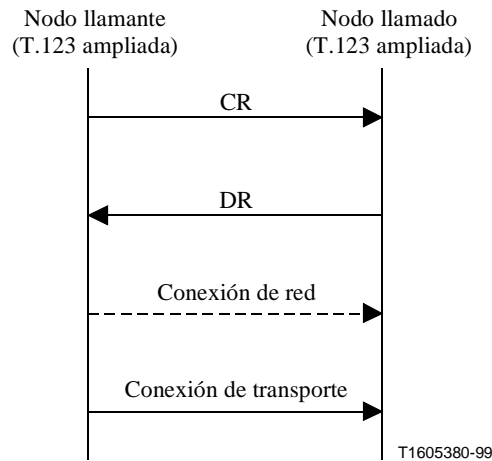
En este modelo, el nodo llamante colocará un campo *SELECTOR DE TRANSPORTE* en la *CR-TPDU*. El nodo llamado examinará este campo para determinar si ha de mantenerse la conexión de red existente. Si es así, responderá con una *CC-TPDU* que contiene un campo *SELECTOR DE TRANSPORTE*. Este modelo de llamada es señalado en el nodo llamante cuando recibe la *CC-TPDU* que contiene el campo opcional.

Adviértase que pueden producirse cambios de protocolo de transporte negociados después de que el intercambio de *PDU* inicial esté completo, a condición de que se mantenga la conexión de red existente. Los cambios en el protocolo de transporte se producirán como si la conexión de red fuese de creación reciente. Los procedimientos de conexión ordinarios para el protocolo de transporte negociados se producirán por la conexión de red existente.



#### B.7.1.4 Establecimiento de llamada por reconexión de la red

Este modelo de llamada se utiliza cuando un nodo T.120 que soporta conexiones ampliadas intenta conectarse a un nodo que también soporta conexiones ampliadas. En este caso, el nodo llamado determina que los servicios disponibles con la conexión de red existente son insuficientes para la conexión T.120. Se rechaza el intento de conexión, pero se devuelve al llamante información suficiente para permitir una reconexión exitosa. Véase la figura B.7.



**Figura B.7/T.123 – Llamada entre nodos de T.123 ampliada – Seleccionada reconexión**

En este modelo, el nodo llamante colocará un campo *SELECTOR DE TRANSPORTE* en la *CR-TPDU*. El nodo llamado examinará el campo. Si el nodo llamado determina que los servicios de conexión de red existentes no son suficientes, puede necesitarse una nueva conexión de red. En este caso, el nodo llamado responderá con un *DR-TPDU* que contiene una parte variable.

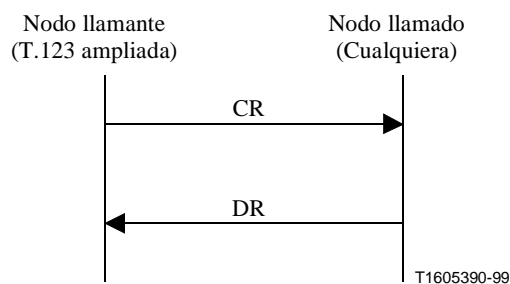
Este modelo de llamada se señala en el nodo llamante cuando recibe la *DR-TPDU* que contiene el campo opcional.

Tras recibir la *DR-TPDU* que contiene el campo opcional, el nodo llamante cerrará la conexión de red existente. El llamante creará entonces una nueva conexión de red utilizando los protocolos, servicios y direcciones devueltos en la parte variable de *DR-TPDU*. En B.9.5.2, Procedimientos de reconexión se dan detalles del procedimiento de reconexión.

Adviértase que este procedimiento de reconexión puede producirse más de una vez en el establecimiento de una única conexión de transporte, si se estima necesario establecer los servicios de transporte necesarios.

#### B.7.1.5 Denegación de la conexión

Este modelo de llamada se utiliza cuando un nodo T.120 que soporta conexiones ampliadas intenta conectarse a cualquier nodo que no desea aceptar la conexión. Véase la figura B.8.



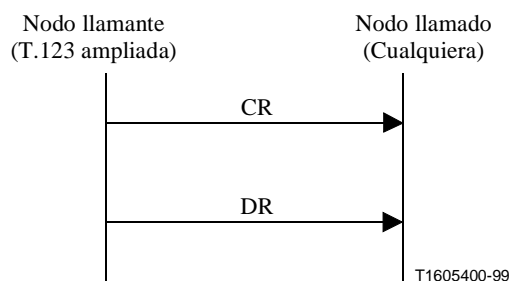
**Figura B.8/T.123 – Denegación de la llamada**

En este modelo, el nodo llamante colocará un campo *SELECTOR DE TRANSPORTE* en la *CR-TPDU*. El nodo llamado puede examinar el campo. Si el nodo llamado determina que ha de denegarse la conexión de transporte, el llamante responderá con una *DR-TPDU* que no contiene una parte variable. Este modelo de llamada es señalado en el nodo llamante cuando recibe la *DR-TPDU* sin el campo opcional.

Los motivos para denegar una conexión se dejan a criterio de los implementadores. Pueden ser incompatibilidad de la seguridad, límites de conexión excedidos, o otras violaciones de la política local.

#### **B.7.1.6 Intento de conexión abandonado**

Este modelo de llamada se utiliza cuando un nodo T.120 que soporta conexiones ampliadas intenta conectarse con cualquier nodo y el nodo llamante decide abandonar el intento de llamada antes de completarse la conexión. Véase la figura B.9.



**Figura B.9/T.123 – Intento de llamada abandonado**

En este modelo, el nodo llamante colocará un campo *SELECTOR DE TRANSPORTE* en la *CR-TPDU*. Si el nodo llamante decide abandonar el intento de llamada antes de recibir una *CC-TPDU* o *DR-TPDU*, enviará entonces un *DR-TPDU* que contiene una parte variable. Este modelo de llamada es señalada en el nodo llamado cuando recibe la *DR-TPDU* que contiene el campo opcional.

Los motivos para denegar una conexión se dejan a criterio de los implementadores. Pueden ser un plazo expirado en un intento de conexión u otras violaciones de la política local.

#### **B.7.2 Restablecimiento de la conexión**

Cuando un nodo llamante en respuesta una *CR-TPDU* recibe una *DR-TPDU* que contiene la parte variable de la PDU, indica que los servicios de red existentes no son adecuados para el conjunto de servicios de transporte seleccionados por el nodo llamante. En este caso, el nodo llamante cerrará inmediatamente la conexión de red asociada con la llamada intentada.

Después de cerrada la conexión de red, el nodo llamante creará una conexión de red que proporcione los servicios (por ejemplo, seguridad) indicados en la parte variable de la *DR-TPDU*. Una vez establecida la nueva conexión de red, se seguirá normalmente el procedimiento de conexión ordinario para los protocolos de transporte seleccionados.

Un caso en el que puede producirse reconexión se presenta si las listas de parámetros deseados son demasiado grandes para enviarlas en el límite de 128 octetos de los tamaños de PDU impuestos por la Recomendación X.224. En este caso, el nodo llamante debe negociar la utilización del CNP como protocolo de transporte a utilizar. En la **ConnectRequestPDU** subsiguiente, no se aplica el límite de 128 octetos, y pueden incluirse listas de parámetros deseados.

Adviértase que puede ser necesario restablecer la conexión de red varias veces para establecer la conexión de transporte final.

### B.7.3 Servicio de red no fiable

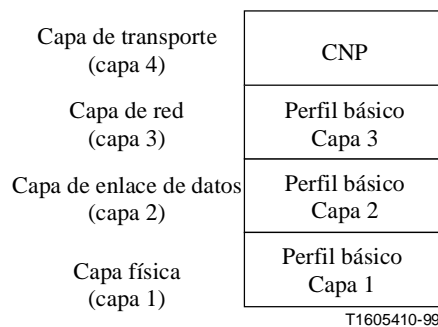
Si una conexión de transporte debe proporcionar un servicio de transmisión de datos no fiable, será negociado por el mismo intercambio de CNP que establece el servicio de transmisión de datos fiable final. El servicio de datos no fiable para la conexión T.120 se considerará establecido sólo después de haberse establecido el servicio de transmisión de datos fiable.

## B.8 Perfiles ampliados

### B.8.1 Transportes fiables

#### B.8.1.1 Perfil ampliado CNP

La figura B.10 define el perfil ampliado CNP para servicio de transporte fiable. Este perfil es idéntico a cualquiera de los perfiles básicos o alternativos definidos en esta Recomendación, salvo que la capa CNP sustituye a la capa clase 0 X.224.



**Figura B.10/T.123 – Perfil ampliado utilizando CNP para servicio de transporte fiable**

#### Capa 4

- CNP

#### Capa 3

- Como se especifica en perfiles básicos o alternativos T.123.

#### Capa 2

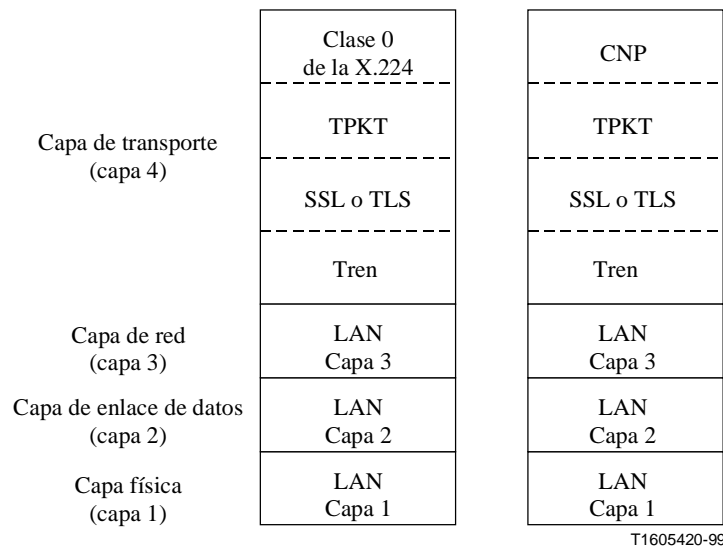
- Como se especifica en perfiles básicos o alternativos T.123.

### Capa 1

- Como se especifica en perfiles básicos o alternativos T.123.

### B.8.1.2 Perfiles ampliados SSL/TLS

La figura B.11 define los perfiles ampliados para añadir servicios de seguridad a la Recomendación T.123 utilizando SSL o TLS. Estos perfiles son idénticos a los perfiles LAN básicos, alternativos o ampliados, salvo que SSL o TLS se añade a la capa de transporte entre la capa TPKT y la capa de tren.



**Figura B.11/T.123 – Perfiles ampliados utilizando SSL o TLS para servicios de seguridad**

### Capa 4

- Clase 0 de la X.224 o CNP para servicio de transporte fiable.
- Encabezamiento de paquete TPKT para delimitar las TPDU, como se especifica en la cláusula 8, encabezamiento de paquete para delimitar unidades de datos en un tren de octetos.

NOTA 1 – Se requiere TPKT porque un servicio de trenes de octetos no marca cuándo se producen fronteras de unidades de datos.

- SSL o TLS
- Transferencia de trenes de octetos con las características siguientes:
  - a) Servicio con conexión preservando la secuencia de octetos.
  - b) Tasa de errores residual suficientemente baja para utilizar como un servicio de red de tipo A.
  - c) Mecanismo de control de flujo para ejercer presión posterior sobre un transmisor.

NOTA 2 – A continuación se especifica un protocolo para la transferencia de trenes de octetos que es un ejemplo de lo anterior:

- a) RFC 793, *Transmission control protocol*.
- b) Por defecto, número de puerto de destino 1503 por RFC 1700, *Assigned numbers*, pero pueden utilizarse otros.

### Capa 3

- Ordinariamente, RFC 791, 792, 919, 922, 950, 1112, protocolo Internet.

### Capa 2

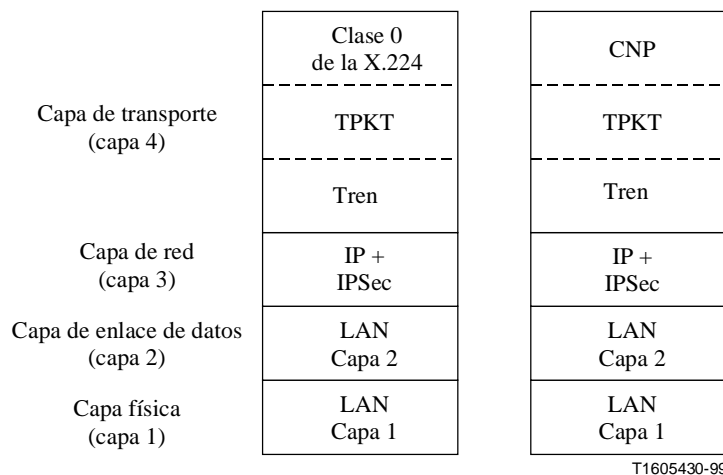
- Ordinariamente, subcapas de control de enlace lógico y acceso al medio ISO/CEI 8802.

### Capa 1

- Ordinariamente, medio físico ISO/CEI 8802.

#### B.8.1.3 Perfiles ampliados IPSec

La figura B.12 define los perfiles ampliados para añadir servicios de seguridad a la Recomendación T.123 utilizando IPSec. Estos perfiles son idénticos a los perfiles LAN básicos, alternativos o ampliados, salvo que se añade IPSec a la capa de enlace de datos.



**Figura B.12/T.123 – Perfiles ampliados utilizando IPSec para servicios de seguridad**

### Capa 4

- Clase 0 de la X.224 o CNP para servicio de transporte fiable.
- Encabezamiento de paquete TPK para delimitar las TPDU, como se especifica en la cláusula 8, encabezamiento de paquete para delimitar unidades de datos en un tren de octetos.

NOTA 1 – Se requiere TPKT porque un servicio de trenes de octetos no marca cuándo se producen fronteras de unidades de datos.

- Transferencia de trenes de octetos con las características siguientes:
  - a) Servicio con conexión preservando la secuencia de octetos.
  - b) Tasa de errores residual suficientemente baja para utilizar como un servicio de red de tipo A.
  - c) Mecanismo de control de flujo para ejercer presión posterior sobre un transmisor.

NOTA 2 – A continuación se especifica un protocolo por capas para la transferencia de trenes de octetos que es un ejemplo de lo anterior:

- a) RFC 793, *Transmission control protocol*.
- b) Por defecto, número de puerto de destino 1503 por RFC 1700, *Assigned numbers*, pero pueden utilizarse otros.

### Capa 3

- Ordinariamente, RFC 791, 792, 919, 922, 950, 1112, protocolo Internet.
- IPSec.

### Capa 2

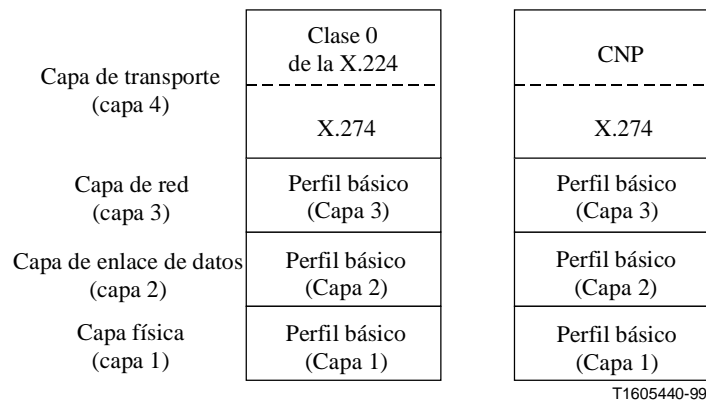
- Ordinariamente, subcapas de control de enlace lógico y acceso al medio ISO/CEI 8802.

### Capa 1

- Ordinariamente, medio físico ISO/CEI 8802.

#### B.8.1.4 Perfiles ampliados X.274

La figura B.13 define los perfiles ampliados para añadir servicios de seguridad a la Recomendación T.123 utilizando X.274. Estos perfiles son idénticos a cualquiera de los perfiles básicos o alternativos, o al perfil ampliado de B.8.1.1 Perfil ampliado CNP, salvo que se añade X.274 a la capa de transporte que sigue inmediatamente a las capas CNP o clase 0 de la X.224.



**Figura B.13/T.123 – Perfiles ampliados utilizando X.274 para servicios de seguridad**

### Capa 4

- Clase 0 de la X.224 o CNP para servicio de transporte fiable.
- X.274 para servicio de seguridad.

### Capa 3

- Como se especifica en perfiles básicos o alternativos T.123.

### Capa 2

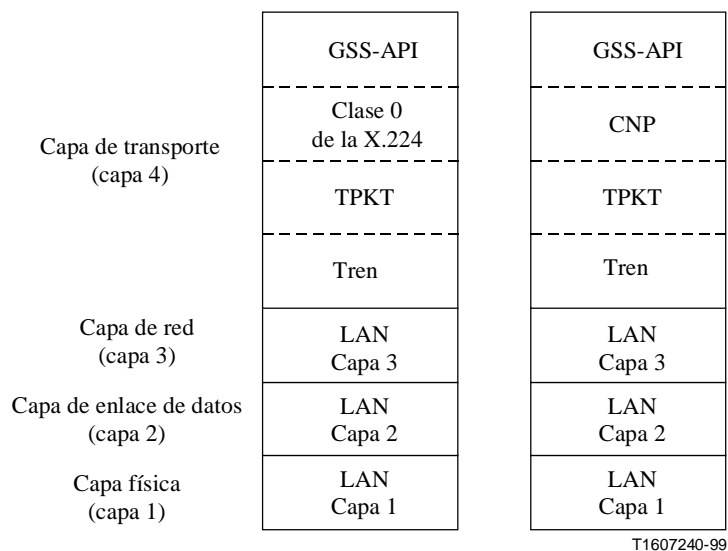
- Como se especifica en perfiles básicos o alternativos T.123.

### Capa 1

- Como se especifica en perfiles básicos o alternativos T.123.

#### B.8.1.5 Perfiles ampliados GSS-API

La figura B.14 define los perfiles ampliados para añadir servicios de seguridad a la Recomendación T.123 utilizando el marco de seguridad GSS-API del IETF. Todos estos perfiles son idénticos a los perfiles LAN básicos, alternativos o ampliados, salvo que se añade paso del testigo GSS-API a la capa de transporte que está por encima de las capas clase 0 de la X.224 o CNP.



**Figura B.14/T.123 – Perfiles ampliados utilizando GSS-API para servicios de seguridad**

#### Capa 4

- Intercambio de testigos GSS-API.
- Clase 0 de la X.224 o CNP para servicio de transporte fiable.
- Encabezamiento de paquete TPKT para delimitar las TPDU, como se especifica en la cláusula 8, encabezamiento de paquete para delimitar unidades de datos en un tren de octetos.

NOTA 1 – Se requiere TPKT porque un servicio de trenes de octetos no marca cuándo se producen fronteras de unidades de datos.

- Transferencia de trenes de octetos con las características siguientes:
  - a) Secuencia de conexión preservando la secuencia de octetos.
  - b) Frontera entre unidades de datos *no* mantenida como parte de la transferencia.
  - c) Tasa de errores residual suficientemente baja para utilizar como un servicio de red de tipo A.
  - d) Mecanismo de control de flujo para ejercer presión posterior sobre un transmisor.

NOTA 2 – A continuación se especifica un protocolo para la transferencia de trenes de octetos que es un ejemplo de lo anterior:

- a) RFC 793, *Transmission control protocol*
- b) Por defecto, número de puerto de destino 1503 por RFC 1700, *Assigned numbers*, pero pueden utilizarse otros.

#### Capa 3

- Ordinariamente, RFC 791, 792, 919, 922, 950, 1112, protocolo Internet.

#### Capa 2

- Ordinariamente, subcapas de control de enlace y acceso al medio ISO/CEI 8802.

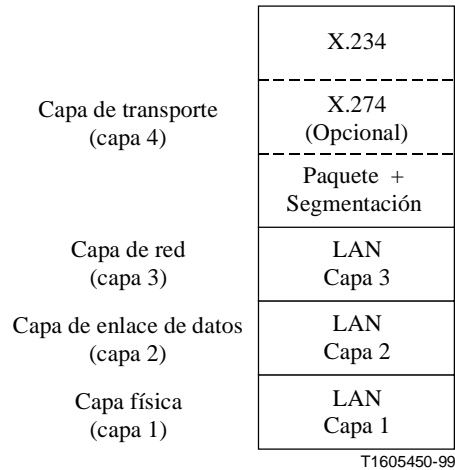
#### Capa 1

- Ordinariamente, medio físico ISO/CEI 8802.

## B.8.2 Transportes no fiables

### B.8.2.1 Perfil LAN no fiable

La figura B.15 define el perfil ampliado para añadir servicios de transporte no fiables a la Recomendación T.123 por conexiones LAN. Las capas 1, 2 y 3 son idénticas a cualquiera de los perfiles LAN básicos o alternativos.



**Figura B.15/T.123 – Perfil LAN no fiable**

#### Capa 4

- X.234, modo sin conexión.
- X.274 (opcionalmente negociado por CNP).
- Transferencia de datos paquetizada no fiable con segmentación.

NOTA – El Protocolo de datagrama de usuario (UDP, *user datagram protocol*) es un ejemplo ordinario de lo anterior.

#### Capa 3

- Como se especifica en perfiles LAN básicos T.123.

#### Capa 2

- Como se especifica en perfiles LAN básicos T.123.

#### Capa 1

- Como se especifica en perfiles LAN básicos T.123.



### B.8.2.2 Perfil RTPC no fiable

Véase la figura B.16.

	Perfil fiable básico o ampliado	Perfil no fiable
Capa de transporte (capa 4)	Clase 0 de la X.224 o CNP	X.234
		X.274 (Opcional)
		Segmentación y reensamblado
Capa de red (capa 3)	Nula + SCF	
Capa de enlace de datos (capa 2)	Q.922	
Capa física (capa 1)	Uso arrítmico del DCE de la serie V	

T1605460-99

**Figura B.16/T.123 – Perfil RTPC no fiable**

#### Capa 4

- X.234, modo sin conexión.
- X.274 (opcional, negociado por CNP).
- Protocolo de segmentación y reensamblado no fiable definido en B.10, protocolo de segmentación y reensamblado no fiable.

#### Capa 3

- Como se especifica en perfil RTPC básico T.123.

#### Capa 2

- Q.922, utilizando información no numerada (UI, *unnumbered information*).

#### Capa 1

- Como se especifica en perfil RTPC básico T.123.

## B.9 Protocolo de negociación de la conexión (CNP, *connection negotiation protocol*)

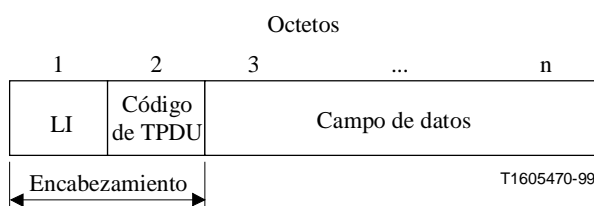
### B.9.1 Sinopsis

Las PDU definidas en este protocolo se basan en sus homólogas X.224/clase 0. X.224 y CNP proporcionan las TPDU petición de conexión, confirmación de conexión, petición de desconexión, datos y error. Además, CNP proporciona una **NonStandardPDU** para la ampliabilidad del protocolo.

### B.9.2 Estructura de las TPDU del CNP

Todas las unidades de datos de protocolo de transporte (TPDU, *transport protocol data unit*) del CNP contendrán un número entero de octetos. Cuando se utilizan octetos consecutivos para representar un número binario, el número de octeto más bajo tendrá el valor más significativo. Las entidades de transporte del CNP respetarán los convenios de orden de los bits y los octetos, permitiendo así que se produzca la comunicación.

La figura B.17 ilustra la estructura de las TPDU del CNP.



**Figura B.17/T.123 – Estructura de las TPDU generales del CNP**

Las TPDU del CNP contendrán, en el orden siguiente:

- El encabezamiento, que comprende:
  - a) el campo indicador de longitud (LI, *length indicator*);
  - b) el código de TPDU.
- El campo de datos.

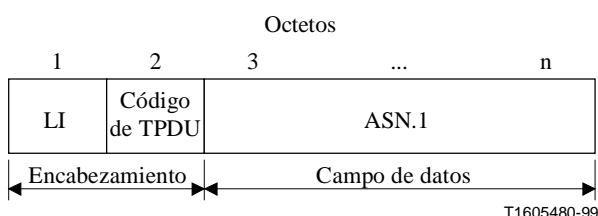
Las TPDU del CNP se dividen en dos categorías: de control y de datos. Los valores de los campos de encabezamiento de cada uno de estos tipos de TPDU se dan en el cuadro B.1. El campo de datos de las TPDU de control contendrá una estructura ASN.1 como la definida en B.9.3, TPDU de control. El campo de datos de las TPDU de datos contendrá estructuras de octetos como las definidas en B.9.4, TPDU de datos.

**Cuadro B.1/T.123 – Valores de los campos de TPDU del CNP**

TPDU	Tipo	LI	Código de TPDU	Campo de datos
Petición de conexión	Control	0000 0001	0100 0111	ASN.1
Confirmación de conexión	Control	0000 0001	0100 0111	ASN.1
Petición de desconexión	Control	0000 0001	0100 0111	ASN.1
Error	Control	0000 0001	0100 0111	ASN.1
No normalizada	Control	0000 0001	0100 0111	ASN.1
Datos	Datos	0000 0001	0100 0110	Estructuras de octetos

### B.9.3 TPDU de control

La estructura de una TPDU de control del CNP se ilustra en la figura B.18.



**Figura B.18/T.123 – Estructura de las TPDU de control del CNP**

Todas las TPDU del CNP utilizarán los siguientes valores de octetos de los campos de encabezamiento.

**LI** 0000 0001

**Código de TPDU** 0100 0111

El campo de datos para estas TPDU constará de una única estructura **CNPControlPDU**, que se define en B.9.6, definición ASN.1. Se dan a continuación descripciones de componentes de esta estructura.

### B.9.3.1 Elementos de información comunes

Las partes de la ASN.1 para el CNP se obtuvieron de otras fuentes, que se describen a continuación:

- 1) **Priority** se obtuvo del anexo A/T.125 (1998) – *Especificación de protocolo del servicio de comunicación multipunto*.
- 2) **H221NonStandard**, **NonStandardIdentifier**, **NonStandardParameter** y **AliasAddress** (así como sus subtipos requeridos tales como **TransportAddress** y **PartyNumber**) se obtuvieron de la Recomendación H.225.0 (1998) – *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

**ReliableTransportProtocol** – especifica un único protocolo de transporte fiable y las condiciones en las que puede utilizarse. Esta estructura contiene los siguientes elementos:

- **type**: especifica CNP, X.224, MAP o un protocolo no normalizado.
- **maxTPDUSize**: el máximo tamaño soportado (en octetos) de una TPDU, incluido el encabezamiento.
- **nonStandardParameters**: información no definida en esta Recomendación (por ejemplo, datos propietarios)

**ReliableSecurityProtocol** – especifica un único protocolo de seguridad para uso con transferencia de datos fiable. Este valor especificará uno de los siguientes:

- Ninguno.
- TLS.
- SSL.
- IPSec (con IKE o gestión manual de claves).
- X.274 (con o sin soporte ID de SA).
- GSS-API.
- Física<sup>1</sup>.
- Un protocolo no normalizado.

**UnreliableTransportProtocol** – especifica un protocolo de transporte no fiable y las condiciones en las que puede utilizarse. Esta estructura contiene los siguientes elementos:

- **type** – especifica un protocolo X.234 o un protocolo no normalizado.
- **maxTPDUSize** – el tamaño máximo soportado de una TPDU, incluido el encabezamiento.

---

<sup>1</sup> Indica que existe una conexión físicamente segura entre los nodos conectantes para comunicaciones fiables. Determinar si existe o no esta condición cae fuera del alcance de esta Recomendación y es competencia de los implementadores. Adviértase que esta condición debe proponerse y también aceptarse durante el establecimiento de la conexión para que se considere en vigor.

- **sourceAddress** – dirección de red a utilizar en unión de este protocolo. Ésta es la dirección que el emisor de la estructuras **UnreliableTransportProtocol** utilizará para recibir datos no fiables para que se negocie la conexión.
- **sourceTSAP** – TSAP a utilizar en unión de este protocolo. El emisor de la estructura **UnreliableTransportProtocol** puede utilizar este identificador para distinguir entre datos para esta conexión y datos de otras conexiones cuando se reciben ambos en la misma dirección de red.
- **nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

**UnreliableSecurityProtocol** – especifica un único protocolo de seguridad para uso con transferencia de datos no fiable. Este valor especificará uno de los siguientes:

- Ninguno.
- IPSec (con IKE o gestión manual de claves).
- X.274 (con o sin soporte ID de SA).
- Física<sup>2</sup>.
- Un protocolo no normalizado.

### B.9.3.2 Petición de conexión

**protocolIdentifier** – la versión del protocolo CNP soportada por el llamante.

**reconnectRequested** – cuando un nodo llamado recibe una petición de conexión con este campo puesto a *verdadero*, responderá con una petición de desconexión. Este campo debe ser puesto a *verdadero* por el nodo llamante en una petición de conexión encapsulada X.224 cuando la información de conexión completa no cumpla las constricciones de tamaño de una *CR-TPDU*. En este caso CNP debe negociarse para su reconexión de manera que pueda intercambiarse el conjunto completo de información de conexión.

**priority** – prioridad de los datos a enviar por esta conexión de transporte. Si se omite, esta conexión se utilizará para transferir todas las prioridades de datos.

**reliableTransportProtocols** – lista de los protocolos de transporte fiables soportados por el nodo llamante, por orden de preferencia. Si se omite, seguirá utilizándose el protocolo existente.

**reliableSecurityProtocols** – lista de los protocolos de seguridad fiables soportados por el nodo llamante, por orden de preferencia. La omisión de este campo indica que el llamante no soporta protocolos de seguridad fiables.

**unreliableTransportProtocols** – lista de los protocolos de transporte no fiables soportados por el nodo llamante, por orden de preferencia. La omisión de este campo indica que el llamante no soporta la transferencia de datos no fiable.

**unreliableSecurityProtocols** – lista de los protocolos de seguridad no fiables soportados por el nodo llamante, por orden de preferencia. La omisión de este campo indica que el llamante no soporta protocolos de seguridad no fiables.

**destinationAddress** – lista secuencial de alias de transporte para el establecimiento de la conexión.

**nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

---

<sup>2</sup> Indica que existe una conexión físicamente segura entre los nodos conectantes para comunicaciones fiables. Determinar si existe o no esta condición cae fuera del alcance de esta Recomendación y es competencia de los implementadores. Adviértase que esta condición debe proponerse y también aceptarse durante el establecimiento de la conexión para que se considere en vigor.

### B.9.3.3 Confirmación de conexión

**protocolIdentifier** – la versión del protocolo CNP a utilizar por esta conexión de transporte.

**reliableTransportProtocol** – el protocolo de transporte fiable a utilizar por esta conexión de transporte. Si se omite, seguirá utilizándose el protocolo existente (por ejemplo, X.224 o CNP).

**reliableSecurityProtocol** – el protocolo de seguridad fiable a utilizar por esta conexión de transporte. La omisión de este campo indica que esta conexión no utilizará un protocolo de seguridad fiable.

**unreliableTransportProtocol** – el protocolo de transporte no fiable a utilizar por esta conexión de transporte. La omisión de este campo indica que esta conexión no soportará una transferencia de datos no fiable.

**unreliableSecurityProtocol** – el protocolo de seguridad no fiable a utilizar por esta conexión de transporte. La omisión de este campo indica que esta conexión no utilizará un protocolo de seguridad no fiable.

**nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

### B.9.3.4 Petición de desconexión

**disconnectReason** – motivo de la desconexión. Este campo puede tener los valores siguientes:

- **unacceptableVersion** – en respuesta a una petición de conexión, indica que la versión del CNP utilizada en la petición de conexión no es aceptable.
- **incompatibleParameters** – en respuesta a una petición de conexión, no se encontró ningún conjunto común aceptable de parámetros de conexión válidos.
- **securityDenied** – indica que las políticas de seguridad locales no permiten que se establezca la conexión<sup>3</sup> ni continuar la operación si ya está establecida.
- **destinationUnreachable** – en respuesta a una petición de conexión, indica que el nodo llamado no puede completar la conexión que especificó el llamante.
- **userRejected** – en respuesta a una petición de conexión, indica que el intento de conexión fue rechazado a un nivel por encima del transporte.
- **userInitiated** – después de establecida una conexión, indica que la desconexión se solicitó a un nivel por encima del transporte.
- **protocolError** – indica que se produjo un error fatal mientras se procesaba una TPDU.
- **unspecifiedFailure** – se produjo un error no específico.
- **routeToAlternate** – en respuesta a una petición de conexión, indica que se desea la conexión, pero el llamante debe intentar reconectar utilizando la información de los campos restantes.
- **nonStandardDisconnectReason** – motivo no definido en esta Recomendación (por ejemplo, un motivo propietario).

**reliableTransportProtocol** – el protocolo de transporte fiable a utilizar por esta conexión de transporte. Si se omite, seguirá utilizándose X.224. Este campo es válido sólo si **disconnectReason** era **routeToAlternate**.

---

<sup>3</sup> Es aceptable emitir una *DR-TPDU* sin el campo opcional (que se describe en B.7.1.5 denegación de la conexión), si el nodo llamado no desea revelar la razón para rechazar un intento de conexión.

**reliableSecurityProtocol** – el protocolo de seguridad fiable a utilizar después de la reconexión. La omisión de este campo indica que no se utilizará un protocolo de seguridad fiable después de la reconexión. Este campo es válido sólo si **disconnectReason** era **routeToAlternate**.

**unreliableTransportProtocol** – el protocolo de transporte no fiable a utilizar después de la reconexión. La omisión de este campo indica que la transferencia de datos fiable no se soportará después de la reconexión. Este campo es válido sólo si **disconnectReason** era **routeToAlternate**.

**unreliableSecurityProtocol** – el protocolo de transporte no fiable a utilizar por esta conexión de transporte. La omisión de este campo indica que esta conexión no utilizará un protocolo de transporte no fiable. Este campo es válido sólo si **disconnectReason** era **routeToAlternate**.

**destinationAddress** – lista secuencial de los alias de transporte a utilizar por el llamante para establecer la conexión. Este campo es válido sólo si **disconnectReason** era **routeToAlternate**.

**nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

### B.9.3.5 Error

**rejectCause** – el motivo de la PDU fue rechazado. Este campo puede tener los valores siguientes:

- **unrecognizedPDU** – indica que la PDU no se decodificó en una forma reconocible.
- **invalidParameter** – indica que la PDU contenía uno o más valores de parámetros inválidos.
- **causeUnspecified** – causa no específica.
- **nonStandardRejectCause** – causa no definida en esta Recomendación (por ejemplo, una causa propietaria).

**rejectedPDU** – la PDU rechazada

**nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

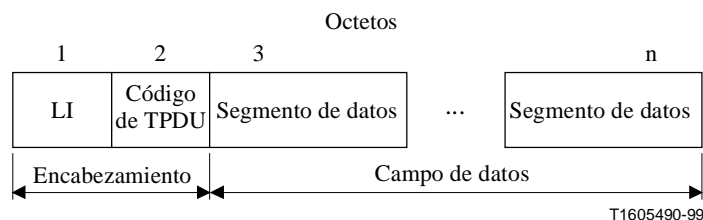
### B.9.3.6 PDU no normalizada

**nonStandardParameters** – información no definida en esta Recomendación (por ejemplo, datos propietarios).

## B.9.4 TPDU de datos

### B.9.4.1 Estructura

La estructura de una TPDU de datos del CNP se ilustra en la figura B.19.



**Figura B.19/T.123 – Estructura de TPDU de datos del CNP**

Todas las TPDU del CNP utilizarán los siguientes valores de octetos de los campos de encabezamiento:

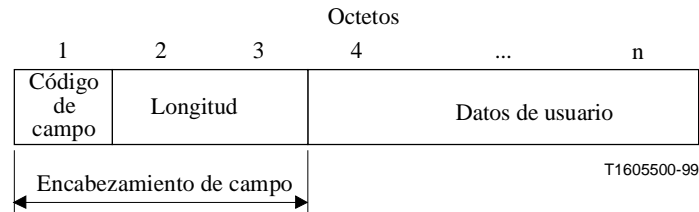
**LI** 0000 0001

**Código de TPDU** 0100 0110

El campo de datos para una TPDU de datos constará de uno o más segmentos de datos, que se describen a continuación.

### B.9.4.2 Segmentos de datos

La estructura de un segmento de datos se muestra en la figura B.20.



**Figura B.20/T.123 – Estructura de un segmento de datos**

Un segmento de datos es una estructura de octetos compuesta de un encabezamiento de campo de longitud fija y un número variable de octetos de datos de usuario.

En un segmento de datos se requieren los parámetros siguientes:

**a) Código de campo (octeto 1)**

Longitud de parámetro: un octeto

Valor de parámetro: 000y zzzz

y indica si éste es el segmento final de un paquete de datos de usuario. Poner y al valor 1 indica un segmento final.

zzzz es un valor binario igual a la prioridad MCS de los datos.

**b) Longitud (octetos 2 y 3)**

Longitud de parámetro: dos octetos

Valor de parámetro: valor binario que indica el número de octetos de datos de usuario, con un valor máximo de 65530.

**c) Datos de usuario (octetos 4 a longitud + 4)**

Longitud de parámetro: octetos de **longitud**

Valor de parámetro: octetos de datos de usuario

## B.9.5 Utilizar CNP en X.224

### B.9.5.1 Encapsulamiento de TPDU

Durante los procedimientos de conexión descritos en B.7.1, establecimiento de la conexión inicial de este anexo, se utilizarán TPDU X.224 para encapsular TPDU de CNP como sigue:

- El campo *SELECTOR DE TRANSPORTE* en una *CR-TPDU* contendrá una **TPDU de petición de conexión**.
- El campo *SELECTOR DE TRANSPORTE* en una *CC-TPDU* contendrá una **TPDU de confirmación de conexión**.

- La parte variable de una *DR-TPDU* contendrá una **TPDU de petición de desconexión** o una **TPDU de error**.

### B.9.5.2 Procedimientos de reconexión

- Si el protocolo de transporte fiable indicado en una **TPDU de confirmación de conexión** es X.224, ambos lados pueden inmediatamente enviar una *TPDU DE DATOS (DT)*, o cualquier otra PDU X.224 válida.
- Si el protocolo de transporte fiable indicado en una **TPDU de confirmación de conexión** es CNP, ambos lados pueden inmediatamente enviar una **TPDU de datos**, o cualquier otra PDU de CNP.
- Si el protocolo de transporte fiable indicado en una **TPDU de confirmación de conexión** no es X.224 ni CNP, el nodo llamante y el nodo llamado seguirán el procedimiento de establecimiento de conexión completo para el protocolo seleccionado (es decir, el llamante emitirá la PDU de petición de conexión apropiada).

### B.9.6 Definición ASN.1

```

--*****
--*   ASN.1 Definition for CNP Control PDUs
--*****

```

CNP-PROTOCOL {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

```

--
-- Imported Definitions
--

```

**IMPORTS**

```

    NonStandardParameter,
    TransportAddress,
    AliasAddress

```

**FROM H323-MESSAGES**

```

    -- H.225.0 Version 2
    -- {itu-t (0) recommendation (0) h (8) 2250 version (0) 2}

```

**Priority**

**FROM MAP-PROTOCOL;**

```

    -- T.125 Annex A Version 1

```

**ProtocolIdentifier ::= OBJECT IDENTIFIER**

```

    -- shall be set to
    -- {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

```

```

--
-- Service Negotiation Types
--

```

**TPDUSize ::= INTEGER (128..65535)**

**ReliableTransportProtocolType ::= CHOICE**

```

{
    cnp                NULL,
    x224               NULL,
    map                NULL,
    nonStandardTransportProtocol NonStandardParameter,
    ...
}

```



```

ReliableTransportProtocol ::= SEQUENCE
{
  type                ReliableTransportProtocolType,
  maxTPDUSize        TPDUSize,
  nonStandardParameters SEQUENCE OF NonStandardParameter OPTIONAL,
  ...
}

```

```

ReliableSecurityProtocol ::= CHOICE
{
  none                NULL,
  tls                 NULL,
  ssl                 NULL,
  ipsecIKEKeyManagement NULL,
  ipsecManualKeyManagement NULL,
  x274WithoutSAID    NULL,
  x274WithSAID       X274WithSAIDInfo,
  gssApi              NULL,
  physical            NULL,
  nonStandardSecurityProtocol NonStandardParameter,
  ...
}

```

```

UnreliableTransportProtocolType ::= CHOICE
{
  x234                NULL,
  nonStandardTransportProtocol NonStandardParameter,
  ...
}

```

```

UnreliableTransportProtocol ::= SEQUENCE
{
  type                UnreliableTransportProtocolType,
  maxTPDUSize        TPDUSize,
  sourceAddress       TransportAddress,
  sourceTSAP         OCTET STRING OPTIONAL,
  nonStandardParameters SEQUENCE OF NonStandardParameter OPTIONAL,
  ...
}

```

```

UnreliableSecurityProtocol ::= CHOICE
{
  none                NULL,
  ipsecIKEKeyManagement NULL,
  ipsecManualKeyManagement NULL,
  x274WithoutSAID    NULL,
  x274WithSAID       X274WithSAIDInfo,
  physical            NULL,
  nonStandardSecurityProtocol NonStandardParameter,
  ...
}

```

```

X274WithSAIDInfo ::= SEQUENCE
{
  localSAID           OCTET STRING,
  peerSAID            OCTET STRING,
  ...
}

```

```

--
-- CNP Control PDU Types
--

```

**ConnectRequestPDU ::= SEQUENCE**

```
{
  protocolIdentifier          ProtocolIdentifier,
  reconnectRequested          BOOLEAN,
  priority                    Priority OPTIONAL,
  reliableTransportProtocols SEQUENCE OF ReliableTransportProtocol OPTIONAL,
  reliableSecurityProtocols  SEQUENCE OF ReliableSecurityProtocol OPTIONAL,
  unreliableTransportProtocols SEQUENCE OF UnreliableTransportProtocol OPTIONAL,
  unreliableSecurityProtocols SEQUENCE OF UnreliableSecurityProtocol OPTIONAL,
  destinationAddress         SEQUENCE OF AliasAddress OPTIONAL,
  nonStandardParameters      SEQUENCE OF NonStandardParameter OPTIONAL,
  ...
}
```

**ConnectConfirmPDU ::= SEQUENCE**

```
{
  protocolIdentifier          ProtocolIdentifier,
  reliableTransportProtocol  ReliableTransportProtocol OPTIONAL,
  reliableSecurityProtocol   ReliableSecurityProtocol OPTIONAL,
  unreliableTransportProtocol UnreliableTransportProtocol OPTIONAL,
  unreliableSecurityProtocol UnreliableSecurityProtocol OPTIONAL,
  nonStandardParameters      SEQUENCE OF NonStandardParameter OPTIONAL,
  ...
}
```

**DisconnectReason ::= CHOICE**

```
{
  unacceptableVersion      NULL,
  incompatibleParameters   NULL,
  securityDenied           NULL,
  destinationUnreachable   NULL,
  userRejected             NULL,
  userInitiated            NULL,
  protocolError            NULL,
  unspecifiedFailure       NULL,
  routeToAlternate         NULL,
  nonStandardDisconnectReason NonStandardParameter,
  ...
}
```

**DisconnectRequestPDU ::= SEQUENCE**

```
{
  disconnectReason          DisconnectReason,
  reliableTransportProtocol ReliableTransportProtocol OPTIONAL,
  reliableSecurityProtocol  ReliableSecurityProtocol OPTIONAL,
  unreliableTransportProtocol UnreliableTransportProtocol OPTIONAL,
  unreliableSecurityProtocol UnreliableSecurityProtocol OPTIONAL,
  destinationAddress        SEQUENCE OF AliasAddress OPTIONAL,
  nonStandardParameters     SEQUENCE OF NonStandardParameter OPTIONAL,
  ...
}
```

**RejectCause ::= CHOICE**

```
{
  unrecognizedPDU          NULL,
  invalidParameter         NULL,
  causeUnspecified         NULL,
  nonStandardRejectCause   NonStandardParameter,
  ...
}
```

```

ErrorPDU ::= SEQUENCE
{
    rejectCause          RejectCause,
    rejectedPDU          OCTET STRING,
    nonStandardParameters SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

NonStandardPDU ::= SEQUENCE
{
    nonStandardParameters SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

CNPControlPDU ::= CHOICE
{
    connectRequest      ConnectRequestPDU,
    connectConfirm      ConnectConfirmPDU,
    disconnectRequest   DisconnectRequestPDU,
    error               ErrorPDU,
    nonStandardCNPPDU  NonStandardPDU,
    ...
}

END

```

## B.10 Protocolo de segmentación y reensamblado no fiable

### B.10.1 Sinopsis

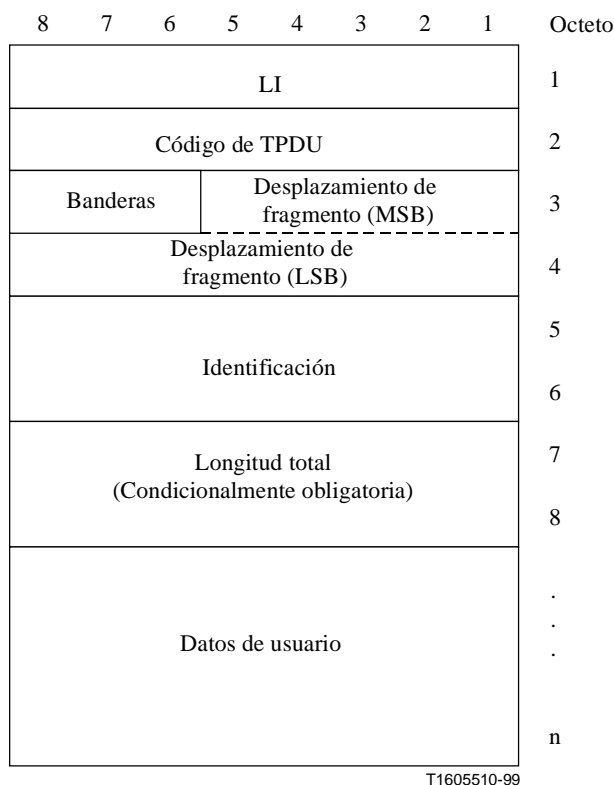
Este protocolo estaba destinado a su utilización por conexiones no fiables en modo paquete y se basa en las funciones de segmentación y reensamblado (SAR) descritas en RFC 791, *Internet Protocol*. El protocolo define una única PDU que permitirá a un emisor segmentar una TSDU en una o más TPDU suficientemente pequeñas para ser transmitidas por una capa de red inferior de tamaño limitado. En el receptor, los segmentos de TPDU pueden reensamblarse para proporcionar la TSDU original completa a una capa de red superior. Aunque este protocolo no supone una entrega ordenada o garantizada de paquetes, supone que los paquetes recibidos están incorruptos.

### B.10.2 Estructura de las TPDU de SAR no fiables

Todas las unidades de datos de protocolo de transporte (TPDU) de SAR no fiables contendrán un número entero de octetos. Cuando se utilizan octetos consecutivos para representar un número binario, el número de octeto inferior tendrá el valor más significativo. Las entidades de transporte de SAR no fiables respetarán los convenios de orden de los octetos, permitiendo así que tenga lugar la comunicación.

Adviértase que los aspectos que intervienen en la reordenación por el receptor de los fragmentos desordenados queda a criterio de los implementadores.

La estructura de una TPDU de SAR no fiable se muestra en la figura B.21.



**Figura B.21/T.123 – Estructura de TPDU de SAR no fiable**

Las TPDU de SAR no fiable contendrán, en el orden siguiente:

- El encabezamiento, que comprende:
  - a) El campo de indicador de longitud (LI)
  - b) El código de TPDU
  - c) El campo de banderas
  - d) El campo de desplazamiento de fragmento
  - e) El campo de identificación
  - f) Condicionamente, un campo de longitud total
- El campo de datos de usuario

#### **B.10.2.1 Campo de indicador de longitud**

Longitud del campo: un octeto

Valor del campo: valor binario que indica la longitud de encabezamiento en octetos, incluidos los campos opcionales, pero excluidos el campo indicador de longitud y los datos de usuario.

#### **B.10.2.2 Código de TPDU**

Longitud del campo: un octeto

Valor del campo: el valor binario: 0100 0110

### **B.10.2.3 Campo de banderas**

Longitud del campo:	3 bits
Valor del campo:	Bit 8: reservado, debe ponerse a cero
	Bit 7: reservado, debe ponerse a cero
	Bit 6: bandera de más fragmentos (MF, <i>more fragments</i> )
	0 = Último fragmento de TSDU
	1 = Siguen más fragmentos de TSDU

### **B.10.2.4 Campo de desplazamiento de fragmento**

Longitud del campo:	13 bits
Valor del campo:	valor binario que indica a qué lugar de la TSDU reensamblada pertenece este fragmento. El desplazamiento de fragmento se mide en unidades de 8 octetos. El desplazamiento del primer fragmento es cero. El bit 5 del octeto 3 representa el bit más significativo de este valor.

### **B.10.2.5 Campo de identificación**

Longitud del campo:	dos octetos
Valor del campo:	valor binario que identifica fragmentos comunes de un datagrama. Este valor no asignado será cero para la primera TSDU enviada a través de una conexión y aumentará en 1 para cada TSDU sucesiva.

### **B.10.2.6 Campo de longitud total (condicionalmente obligatorio)**

Longitud del campo:	dos octetos
Valor del campo:	valor binario que indica la longitud total de la TSDU, medida en octetos. Este valor se incluirá con el primer fragmento de cualquier TSDU segmentada en múltiples fragmentos. El valor puede incluirse con cualquiera de los otros fragmentos o con todos ellos.

### **B.10.2.7 Campo de datos de usuario**

Longitud del campo:	variable
Valor del campo:	octetos de datos de usuario

### **Bibliografía**

- IETF RFC 2078 (enero de 1997), *Generic Security Service Application Program Interface*.

## APÉNDICE I

### Establecimiento de la comunicación conferencia multimedios en la RDSI

#### I.1 Introducción

Los terminales de conferencia multimedios (MMC, *multimedia conference*), actualmente en proceso de normalización en el UIT-T, están destinados a funcionar en la RDSI. Sin embargo, diversos terminales de diferentes tipos, tales como el teléfono, el facsímil del grupo 4, los videoteléfonos y los sistemas de teleconferencia, están también conectados a la RDSI.

Los siguientes casos se derivan de la Recomendación Q.931, que suministra mayor información y describe otras posibilidades. Se debe prestar atención a la codificación de los elementos de información para BC, LLC y HLC, porque son importantes para el interfuncionamiento.

En el cuadro I.1 se presentan valores que pueden ser utilizados en un mensaje ESTABLECIMIENTO. El terminal del lado llamado debe también aceptar otros valores de los elementos de información para BC, LLC, y HLC. Los ajustes alternativos incluyen la información digital sin restricciones con tonos y anuncios (UDI-TA, *unrestricted digital information with tones and announcements*), adaptación de la velocidad a 56 kbit/s para redes con restricciones, BC/HLC doble y ausencia de LLC. Cuando se utiliza HLC, el usuario debe configurar la aceptación de la llamada para permitir utilizar telefonía a 7 kHz, videotelefonía o telefonía a 3,1 kHz.

**Cuadro I.1/T.123 – Fijación de los parámetros originados en el mensaje ESTABLECIMIENTO**

Elemento de información	BC	LLC	HLC
Capacidad de transferencia de información	Información digital sin restricciones	Información digital sin restricciones	
Modo de transferencia	Circuito	Circuito	
Velocidad de transferencia de la información	64 kbit/s	64 kbit/s	
Protocolo de capa 1 de información de usuario		H.221	
Identificación de características de capa alta			AC <sup>a)</sup>
<sup>a)</sup> AC Teleconferencia audiográfica. VC (videoconferencia), VP (videoteléfono) y AV (audiovisual) son aceptables en el caso del lado llamado.			

#### I.2 Requisitos básicos

Han de reunirse fundamentalmente las siguientes condiciones:

- 1) Un terminal MMC tiene la función I/F RDSI dentro del mismo, y se conecta directamente a la RDSI en un punto S(T).
- 2) Un terminal MMC desea intercomunicar con los siguientes terminales:
  - a) terminal MMC;
  - b) videoteléfono, teleconferencia, con soporte de la estructura de trama H.221;a) y b) antes citados se denominarán juntos terminales AV (audiovisuales) en lo sucesivo.

La intercomunicación entre terminales MMC y teléfonos es la demanda fundamental, pero cada lado utiliza diferentes servicios RDSI (por ejemplo, MMC: información digital sin restricciones, teléfono: conversación), por lo que este tipo de intercomunicación sería difícil, sin utilizar secuencias especiales, como se muestra en las figuras I.2 e I.3.

- 3) Esta descripción corresponde únicamente a la conexión punto a punto. La descripción de la secuencia se muestra en la figura I.1.

### **I.3 Fase de conexión**

El procedimiento de conexión puede dividirse en las tres fases siguientes:

- 1) Fase A (protocolo de canal D RDSI) – Utilizando el protocolo de señalización de canal D (véase la Recomendación Q.931), un terminal MMC efectúa el control de llamada de forma que se establece un canal B RDSI, para la comunicación con un terminal AV.
- 2) Fase B (protocolo H.242) – Un terminal MMC basado en la Recomendación H.221 establece la alineación de trama y decide el modo de comunicación basado en la secuencia H.242 (modo MMC/modo conversación), y establece el trayecto MLP.
- 3) Fase C (protocolo de la serie T.120) – En el caso de que ambos terminales tengan funcionalidad MMC y decidan comunicar por el modo MMC, se inicia el protocolo MMC T.120 y se decide la función de comunicación final en detalle, lo que conduce al comienzo de la comunicación real.

### **I.4 Fase A (protocolo de canal D RDSI)**

Al efectuar control de llamada basado en la Recomendación Q.931 (protocolo de señalización de canal D), han de fijarse los parámetros especificados en el cuadro I.1 en el mensaje ESTABLECIMIENTO en el lado origen. En la presente Recomendación, no obstante, el cuadro I.1 muestra sólo los elementos de información de:

- 1) capacidad portadora (BC, *bearer capability*);
- 2) capacidad de capa baja (LLC, *low layer capability*);
- 3) capacidad de capa alta (HLC, *high layer capability*),

todos los cuales son necesarios para reconocer la capacidad de comunicación de los otros terminales.

Un terminal MMC en el lado llamante debe fijar los parámetros antes citados en el mensaje ESTABLECIMIENTO para su envío, aunque en el lado llamado debe comprobar los parámetros de manera que estime la posibilidad de comunicación. Si juzga posible comunicar, puede aceptar la llamada y conectarse a un canal B. A continuación un terminal MMC empieza a intercomunicar con un terminal audiovisual, que puede ser otro terminal MMC u otro tipo de terminal audiovisual tal como un videoteléfono.

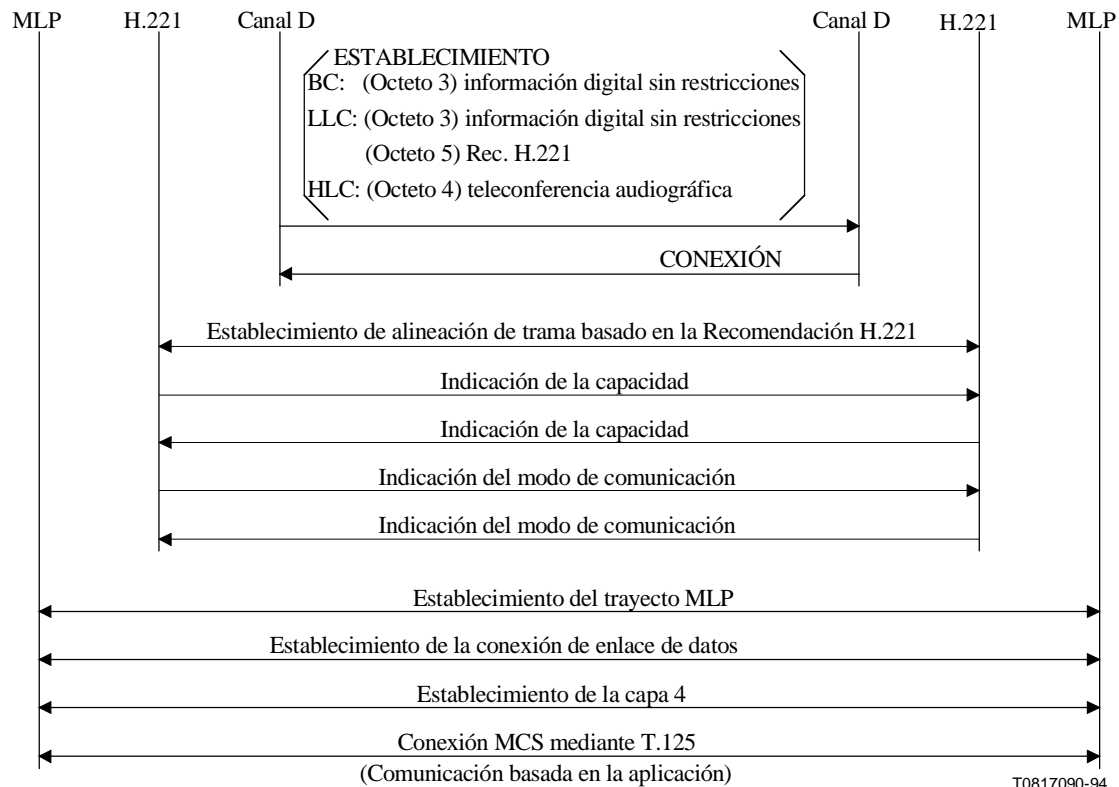
### **I.5 Fase B (protocolo H.242)**

Tras conectarse al canal B, deben efectuarse los siguientes procedimientos basados en la Recomendación H.242:

- 1) Alineación de trama conforme a la Recomendación H.221 es el modo. Luego utilizando BAS, se ejecuta la secuencia de intercambio de capacidad en modo MIC de 7 bits (modo 0F).
- 2) Después de que cada lado haya reconocido la capacidad del otro, ellos deciden su propio modo de comunicación, incluido el modo común. Es decir, cuando ambos están seguros de tener capacidad MLP, se establece el trayecto MLP y se inicia el protocolo T.120, lo que conduce a la fase C.
- 3) En el caso de que un lado no tenga capacidad MLP, la comunicación de ambos se limita a audio y posiblemente vídeo (por ejemplo, si un lado es una MMC y el otro un videoteléfono).

## I.6 Fase C (protocolo de la serie T.120)

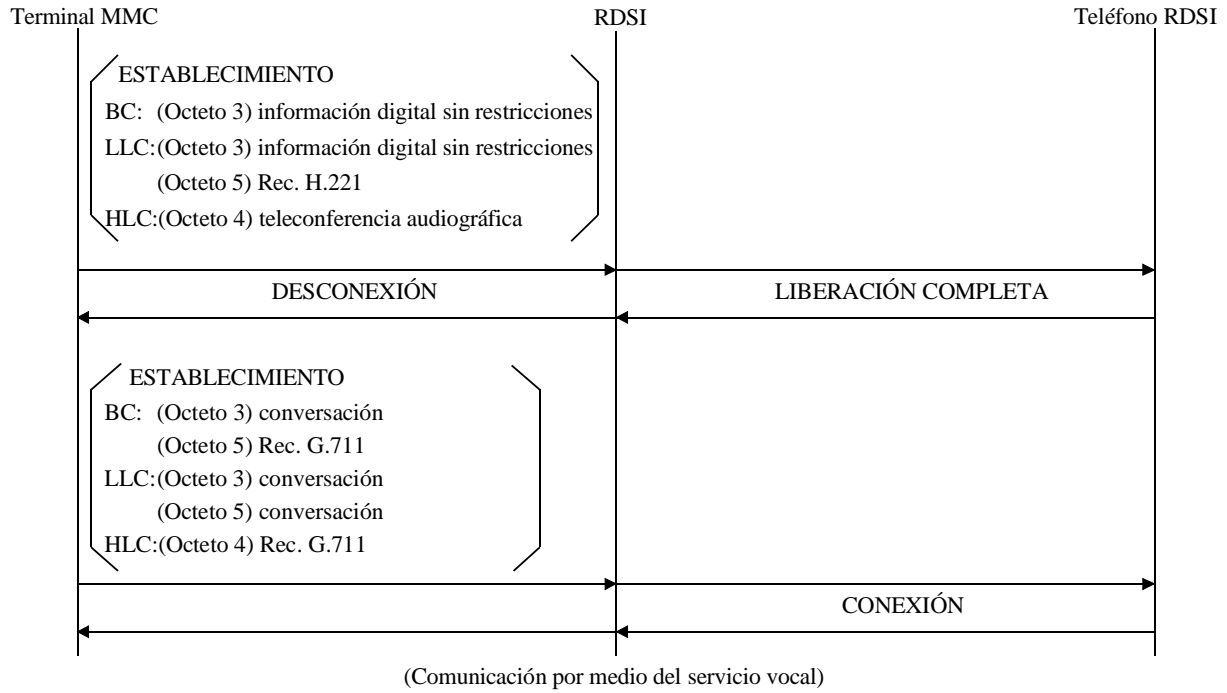
- 1) Establecer una conexión de enlace de datos por el trayecto MLP.
- 2) Establecer la capa 4.
- 3) Después de que los canales se hayan establecido con arreglo a la Recomendación T.125, las negociaciones, a fin de reconocer las funciones de cada una de las partes en relación con la MMC y la información necesaria para la conferencia, se intercambian por control de conferencia genérica mediante la lista de aplicaciones.



**Figura I.1/T.123 – Secuencia de establecimiento de la comunicación para terminales MMC**



1) Llamada desde un terminal MMC a un teléfono RDSI



2) Llamada desde un teléfono RDSI a un terminal MMC

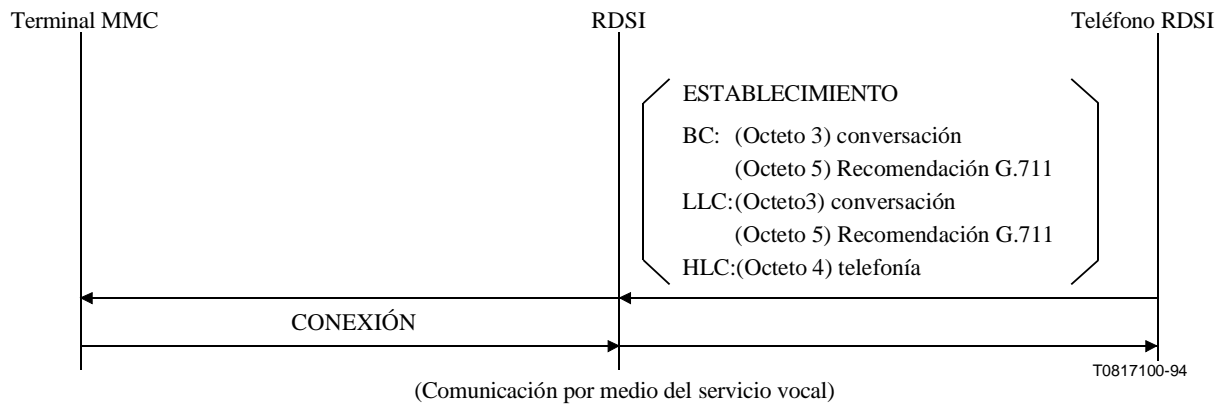
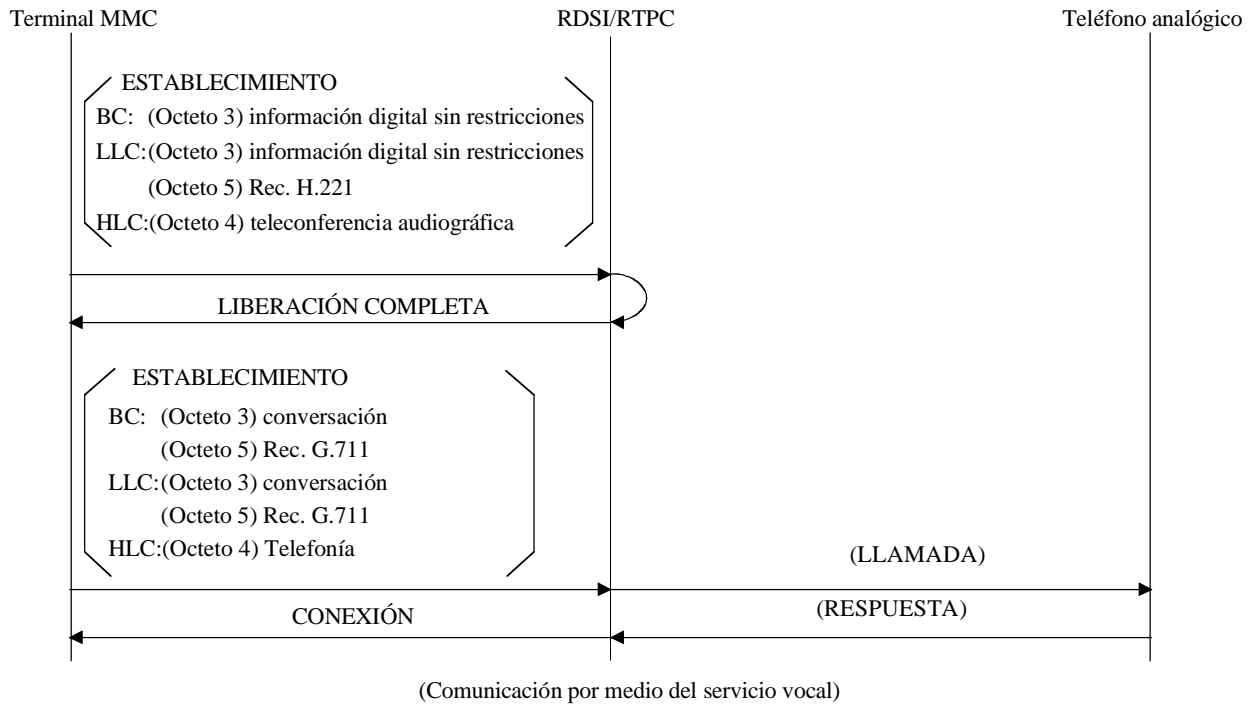
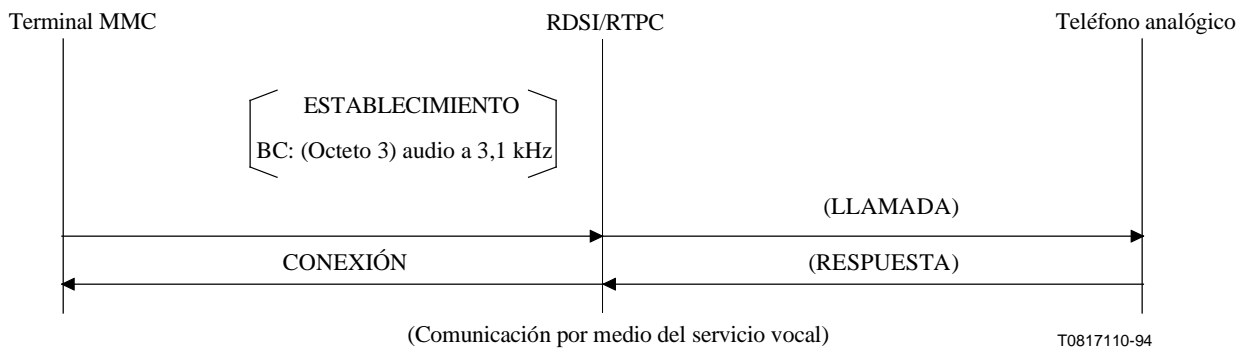


Figura I.2/T.123 – Secuencias de intercomunicación para terminal MMC y teléfono RDSI

**3) Llamada desde un terminal MMC a un teléfono analógico**



**4) Llamada desde un teléfono analógico a un terminal MMC**



T0817110-94

**Figura I.3/T.123 – Secuencias de intercomunicación para terminal MMC y teléfono analógico**

## APÉNDICE II

### Marco de seguridad de la GSS-API

#### II.1 Introducción

Este apéndice contiene información general sobre el marco de seguridad definido por la interfaz de programación de aplicación del servicio de seguridad genérica (GSS-API, *generic security service-application programming interface*) en el anexo B.

#### II.2 Tecnología de autenticación común (CAT, *common authentication technology*) del IETF

Esta subcláusula contiene referencias generales sobre diversas iniciativas de seguridad en el IETF en relación con la GSS-API.

##### II.2.1 IETF y grupo de trabajo CAT

El Grupo de Tareas sobre Ingeniería Internet (IETF) – ha centralizado su trabajo de seguridad dentro de un marco que ahora se utiliza ordinariamente a través de todos los protocolos IETF. RFC 1511, norma titulada "Common Authentication Technology Overview", expone estos trabajos y su objetivo.

##### II.2.2 Marco de seguridad de la GSS-API

El marco de seguridad del grupo de trabajo CAT está constituido por la GSS-API en RFC 1508. GSS-API es una API que produce un conjunto bien definido de estructuras de datos para comunicación por un canal fiable entre dos entidades negociadoras. RFC 2078, *Generic Security*, explica el mecanismo del marco de seguridad.

##### II.2.3 SPNEGO

La negociación del contexto de seguridad de la GSS-API puede ser problemática. Es posible soportar múltiples mecanismos de seguridad en la GSS-API. Sin embargo, no hay ningún medio de identificar para qué mecanismo de seguridad se necesita un testigo opaco. En efecto, al recibir el primer testigo, una aplicación llamante de la GSS-API debe intentar la validación del testigo para cada mecanismo de seguridad instalado, hasta que se produzca éxito (o fallo definitivo). Este método llegará inequívocamente a la conclusión correcta, pero carece de eficacia. Para optimizar el uso de la GSS-API, el grupo de trabajo CAT está definiendo un mecanismo de seguridad que permite una negociación simple. El mecanismo de negociación GSS-API simple y protegido, o SPNEGO, es la serie de normas RFC 2478.

#### II.3 Marco de seguridad del anexo B/T.123

El anexo B define implícitamente un marco de seguridad para la Recomendación T.120. Suponiendo el caso de transmisión fiable, el marco tiene las siguientes características.

Una lista de protocolos de seguridad fiables conocidos. Esta lista es ampliable y permite la inclusión de protocolos no normalizados (por ejemplo, protocolos no incluidos en la lista).

Nodos que soportan conexiones de transporte ampliadas puede seleccionar y hacer uso de un determinado protocolo de seguridad. Pueden ambos soportar, mediante un simple mecanismo de negociación de capacidad que utilice los modelos de llamada especificados en la B.7.

El llamante transmite un conjunto de protocolos de seguridad fiables que puede soportar en la ConnectRequestPDU del CNP.

El llamado puede señalar que los servicios disponibles con cada conexión de red en curso son suficientes o insuficientes para el protocolo de seguridad deseado (utilizando respectivamente una DisconnectRequestPDU del CNP o una ConnectConfirmPDU del CNP, respectivamente). En uno u

otro caso, el llamado transmite el protocolo de seguridad fiable simple que ha elegido utilizar (que debe ser un elemento del conjunto anunciado por el llamante).

En el caso de servicios suficientes, la conexión T.120 procede a utilizar la conexión de red existente (que puede incluir cambios de protocolo de transporte negociados).

En el caso de servicios insuficientes, el llamante cierra la conexión de red existente y crea una nueva conexión de red que proporciona los servicios indicados por el llamado en la DisconnectRequestPDU del CNP.

En todos los perfiles ampliados definidos en el anexo B, la seguridad es implícitamente un servicio que existe por debajo de la capa clase 0 de la X.224 o CNP. Sin embargo, nada impide que pueda negociarse que se prohíba a un perfil no normalizado proveer servicios (incluido el de seguridad) por encima de las capas clase 0 de la X.224 o CNP.

### **II.3.1 GSS-API: Transporte de testigos GSS-API vía clase 0 de la X.224 o CNP**

El marco de seguridad GSS-API implementa un proceso por el que un mecanismo de seguridad crea testigos opacos para la comunicación mediante un mecanismo fiable (o sea, transporte) entre dos entidades negociadoras. Este proceso está en curso para todas las comunicaciones entre las entidades, por lo que abarca una sesión entera. Incluye no sólo la fase de establecimiento de un contexto de seguridad donde pueden elegirse los mecanismos de seguridad y las credenciales intercambiadas, sino también algún intercambio posterior de datos criptados.

Un uso común del marco de seguridad GSS-API es para la aplicación de invocación para gestionar la seguridad de una sesión en lo que respecta a la política de seguridad que puede proyectarse localmente para la aplicación. Por ejemplo, la aplicación puede decidir qué protocolos de seguridad anunciar y qué credenciales seleccionar.

Naturalmente son posibles otros usos de la GSS-API. Por ejemplo, el servicio de red de un sistema operativo puede establecer su propio contexto de seguridad entre dos puntos extremos. Dado que la existencia de este contexto de seguridad puede o no ser conocida para una aplicación de invocación de nivel más alto, la aplicación puede no saber si necesita gestionar o no la seguridad de su sesión (por ejemplo, puede invocarse seguridad IP por el servicio de interconexión de redes, pero su invocación es probablemente transparente a una aplicación de nivel más alto que utilice TCP/IP). Aún si no sabe de otro contexto de seguridad, la aplicación puede desear de todos modos gestionar su propia seguridad de la sesión.

Por consiguiente, el uso más probable del marco de seguridad GSS-API en la serie de Recomendaciones T.120 es cuando una aplicación T.120 desea gestionar directamente la seguridad de una sesión. Se plantea entonces de forma natural la cuestión de dónde debe la aplicación T.120 decidir establecer el tren de testigos GSS-API dentro de la sesión T.120.

Considerando que la GSS-API no se preocupa sobre el mecanismo de comunicación para su tren de testigos, el anexo B especifica un esquema que señala el marco de seguridad de la GSS-API como protocolo de seguridad fiable dentro del CNP, y, en un perfil ampliado, dispone el tren de testigos GSS-API por encima del componente de clase 0 de la X.224 de la capa 4 (o dispone el tren por encima del CNP en el caso de que CNP sustituya a la clase 0 de la X.224).

## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión 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
<b>Serie T</b>	<b>Terminales para servicios de telemática</b>
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación