



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

T.127

(08/95)

TERMINALES PARA SERVICIOS DE TELEMÁTICA

**PROTOCOLO DE TRANSFERENCIA
MULTIPUNTO DE FICHEROS BINARIOS**

Recomendación UIT-T T.127

(Anteriormente «Recomendación del CCITT»)

PREFACIO

El UIT-T (Sector de Normalización de las Telecomunicaciones) es un órgano permanente de la Unión Internacional de Telecomunicaciones (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 (Helsinki, 1 al 12 de marzo de 1993).

La Recomendación UIT-T T.127 ha sido preparada por la Comisión de Estudio 8 (1993-1996) del UIT-T y fue aprobada por el procedimiento de la Resolución N.º 1 el 11 de agosto de 1995.

NOTA

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

© UIT 1996

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

		<i>Página</i>
1	Alcance.....	1
2	Referencias normativas	1
3	Definiciones	2
4	Abreviaturas	3
5	Introducción a la transferencia multipunto de ficheros	3
6	Transferencia multipunto de datos – Visión de conjunto.....	4
	6.1 Modelo de sistema T.127.....	6
	6.2 Compresión.....	7
	6.3 Prioridad	7
	6.4 Entrega previa de ficheros	8
7	Aplicación MBFT básica	8
8	Descripción de funcionamiento.....	9
	8.1 Aplicación de usuario transferencia de ficheros	9
	8.2 Gestor de recursos de aplicación transferencia de ficheros	9
	8.3 Elemento de servicio de aplicación transferencia de ficheros	9
	8.4 Recursos MBFT.....	10
	8.4.1 Inicialización de MBFT	11
	8.4.2 Modo estático.....	13
	8.4.3 Modo multidifusión	14
	8.4.4 Modo privado.....	18
	8.4.5 Formación de las claves de registro	19
	8.5 Capacidades MBFT	19
	8.6 Soporte de transferencias de ficheros adicionales concurrentes	21
	8.6.1 Canales multidifusión	21
	8.6.2 Canales privados	21
	8.7 Transferencia de ficheros selectiva.....	23
	8.8 Abandono de una sesión MBFT	24
	8.9 Intercambio de ficheros	25
	8.9.1 Operación invocada por el transmisor	25
	8.9.2 Operación invocada por el receptor	29
	8.10 Listado de directorio distante.....	30
	8.11 Comportamiento en modo conducido.....	32
	8.11.1 APE de fichero par presente en el nodo conductor	32
	8.11.2 Ausencia de APE de fichero pares en el nodo conductor	34
	8.12 Aborto de una transferencia de fichero.....	34
	8.13 Diagnóstico	35
	8.14 Operaciones no normalizadas	36
9	Definiciones de PDU MBFT.....	36
10	Uso del servicio de comunicación multipunto	43
	10.1 Uso de los servicios de transmisión de datos MCS	43
	10.2 Atribución de canales	44
	10.3 Atribución de testigos	45
	10.4 Servicios MCS	46

	<i>Página</i>
11 Uso del control de conferencia genérico	46
11.1 Identificadores de recurso	46
Anexo A – Asignación de testigos y canales estáticos	49
Anexo B – Asignaciones de identificadores de objeto	50
Apéndice I – Ejemplos de transferencia de ficheros	50
Apéndice II – Atributos MBFT	56

RESUMEN

Esta Recomendación define un protocolo para sustentar el intercambio de datos de ficheros binarios dentro de un entorno interactivo de conferencia o trabajo en grupo en el que se aplican las Recomendaciones de la serie T.120. Proporciona mecanismos de soporte para la distribución simultánea de ficheros múltiples, la distribución selectiva de ficheros a un subconjunto de participantes y la extracción de ficheros desde posiciones distantes. También se ha previsto el acceso distante al directorio.

PROTOCOLO DE TRANSFERENCIA MULTIPUNTO DE FICHEROS BINARIOS

(Ginebra, 1995)

1 Alcance

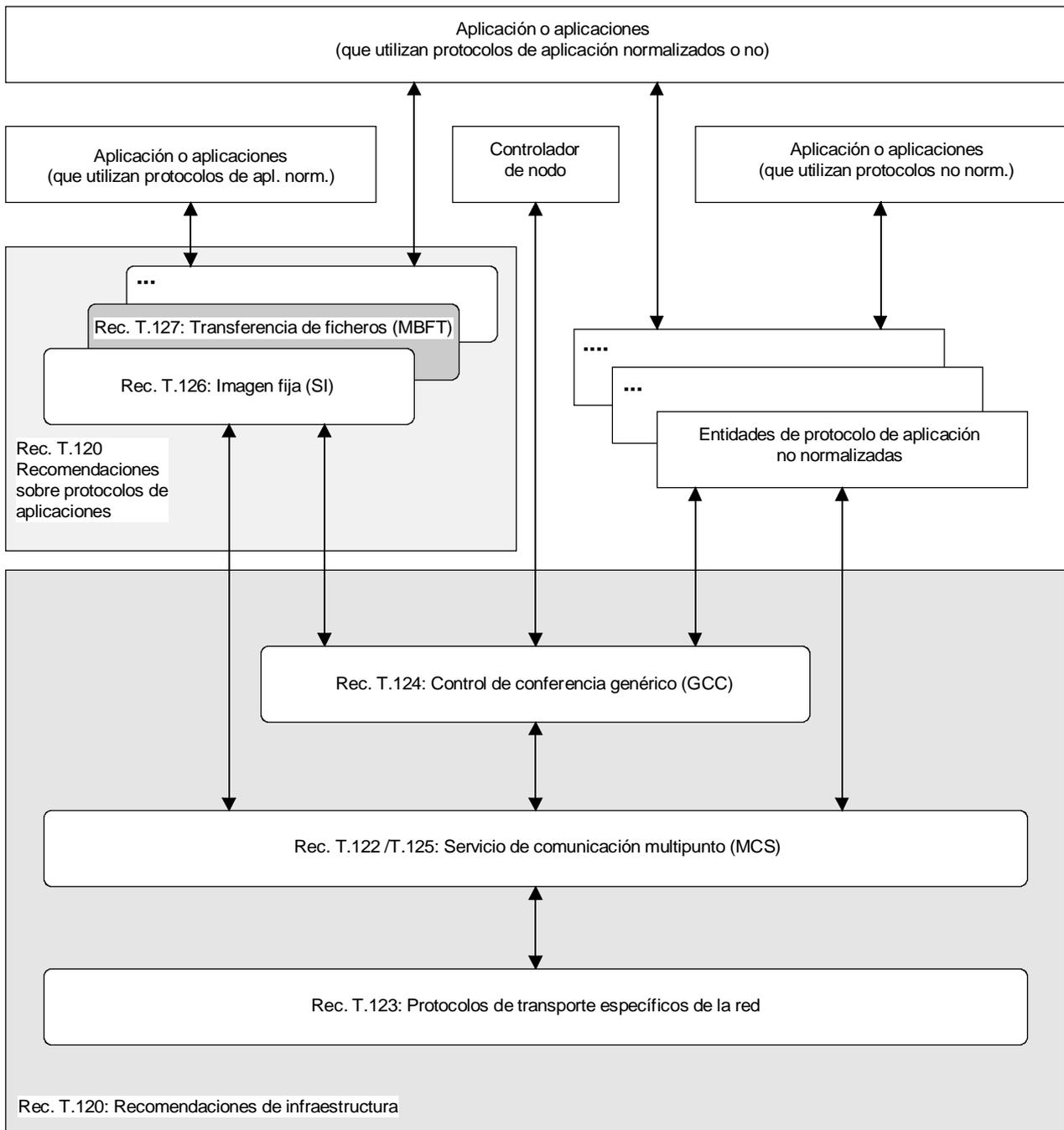
Esta Recomendación define un protocolo para sustentar el intercambio de datos de ficheros binarios dentro de un entorno interactivo de conferencia o trabajo en grupo en el que se aplican las Recomendaciones de la serie T.120. Proporciona mecanismos que facilitan la distribución y extracción de uno o más ficheros simultáneamente utilizando las primitivas que aporta la Recomendación T.122 (Servicio de comunicación multipunto). La Recomendación T.127 tiene por finalidad ofrecer un protocolo versátil y ligero que proporcione la funcionalidad esencial para permitir el interfuncionamiento entre aplicaciones que requieran una capacidad básica de transferencia de ficheros, y posee además flexibilidad para satisfacer las demandas de aplicaciones más sofisticadas. Véase la Figura 1.

2 Referencias normativas

Las siguientes Recomendaciones y demás referencias contienen disposiciones que, mediante la referencia hecha en este texto, constituyen disposiciones de la presente Recomendación. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se incita a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar la edición más reciente de las Recomendaciones y otras referencias citadas a continuación. Regularmente se publica una lista de las Recomendaciones UIT-T vigentes.

- Recomendación del CCITT T.35 (1991), *Procedimiento para la asignación de códigos definidos por el CCITT para facilidades no normalizadas*.
- Recomendación UIT-T T.120¹⁾, *Protocolos de datos para conferencia multimedia*.
- Recomendación UIT-T T.122 (1993), *Servicio de comunicación multipunto para la definición de los servicios de conferencia audiográfica y de conferencia audiovisual*.
- Recomendación UIT-T T.123 (1994), *Pilas de protocolos para aplicaciones de teleconferencia audiográficas y audiovisuales*.
- Recomendación UIT-T T.124 (1995), *Control genérico de conferencia*.
- Recomendación UIT-T T.125 (1994), *Especificación de protocolo del servicio de comunicación multipunto*.
- Recomendación T.434 del CCITT (1992), *Formato de transferencia de ficheros binarios en los servicios telemáticos*.
- Recomendación UIT-T H.221 (1993), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.
- Recomendación UIT-T X.680 (1994), *Tecnología de la información – Notación de sintaxis abstracta uno (ASN.1): Especificación de la notación básica*.
- Recomendación UIT-T X.691 (1995), *Tecnología de la información – Reglas de codificación en notación de sintaxis abstracta uno – Especificación de las reglas de codificación paquetizada*.
- Recomendación V.42 bis del CCITT (1990), *Procedimientos de compresión de datos para los equipos de terminación del circuito de datos (EDCE) que utilizan procedimientos de corrección de errores*.
- ISO/CEI 3309:(1993), *Information technology – Telecommunications and information exchange between systems – High-Level Data Link Control (HDLC) procedures – Frame structure*.
- ISO 8571-2:(1988), *Information processing systems – Open Systems Interconnection – File Transfer, Access and Management (FTAM) – Part 2: Virtual filestore definitions*.

¹⁾ Actualmente en estado de proyecto.



T0820070-95/d01

FIGURA 1/T.127
Alcance de la Recomendación T.127

3 Definiciones

A los efectos de la presente Recomendación, son aplicables las definiciones siguientes:

3.1 canal de datos con acuse de recibo: Un canal MCS por el cual se distribuyen ficheros. Los participantes tienen la facultad de rechazar los ficheros ofrecidos por un canal de datos con acuse de recibo. Un canal con acuse de recibo puede ser *exclusivo* (cuando solamente el creador del canal puede enviar ficheros por él) o *compartido* (cuando puede enviar ficheros cualquier participante).

- 3.2 canal de datos de difusión:** Un canal MCS por el cual se distribuyen ficheros. Los participantes deben recibir todos los ficheros distribuidos por el canal, descartando localmente los datos que no sean necesarios.
- 3.3 canal de control:** Un canal MCS utilizado para la gestión de las transacciones de ficheros.
- 3.4 atributos de fichero:** El nombre y otras propiedades identificables de un fichero.
- 3.5 PETICIÓN-FICHERO:** El testigo utilizado para asegurar que hay como máximo una petición de fichero pendiente en el canal de control de la sesión CONTROL-MBFT.
- 3.6 PETICIÓN-FICHERO(p):** El testigo utilizado para asegurar que hay como máximo una petición de fichero pendiente en el canal de control de la subsesión CONTROL-MBFT(p).
- 3.7 TRANSMISIÓN-FICHERO:** El testigo utilizado para asegurar que no hay más de una transferencia de fichero en curso en el canal de datos de difusión de la sesión DATOS-MBFT.
- 3.8 TRANSMISIÓN-FICHERO(p):** El testigo utilizado para asegurar que no hay más de una transferencia de fichero en curso en el canal de datos de difusión de la subsesión DATOS-MBFT(p).
- 3.9 TRANSMISIÓN-FICHERO(n):** El testigo utilizado para asegurar que no hay más de una transferencia de fichero en curso en el canal de datos con acuse de recibo DATOS-MBFT(n).
- 3.10 CONTROL-MBFT:** El canal de control de la sesión.
- 3.11 CONTROL-MBFT(p):** Un canal de control de la subsesión cuyo identificador de canal MCS es p.
- 3.12 DATOS-MBFT:** El canal de datos de difusión de la sesión.
- 3.13 DATOS-MBFT(p):** Un canal de datos de difusión de subsesión cuyo identificador de canal MCS es p.
- 3.14 DATOS-MBFT(n):** Un canal de datos con acuse de recibo cuyo identificador de canal MCS es n.
- 3.15 capacidad no normalizada:** Una capacidad que cae fuera del ámbito de esta Recomendación. Las capacidades no normalizadas deben ser negociadas antes de la utilización.
- 3.16 sesión:** Un conjunto de entidades de protocolo de aplicación pares (del mismo rango).
- 3.17 capacidad normalizada:** Una capacidad que se define dentro del ámbito de esta especificación pero no es necesaria para todas las realizaciones MBFT. Las capacidades normalizadas deben ser negociadas antes de la utilización.
- 3.18 subsesión:** Un subgrupo de entidades de protocolo de aplicación pares comprendidas en una sesión.

4 Abreviaturas

A los fines de esta Recomendación, se utilizan las abreviaturas siguientes:

ARM	Gestor de recursos de aplicación (<i>application resource manager</i>)
APE	Entidad de protocolo de aplicación (<i>application protocol entity</i>)
ASE	Elemento de servicio de aplicación (<i>application service element</i>)
GCC	Control de conferencia genérico (<i>generic conference control</i>)
GCCSAP	Punto de acceso al servicio GCC (<i>GCC service access point</i>)
MBFT	Transferencia multipunto de ficheros binarios (<i>multipoint binary file transfer</i>)
MCS	Servicio de comunicación multipunto (<i>multipoint communication service</i>)
MCSAP	Punto de acceso del servicio MCS (<i>MCS service access point</i>)
PDU	Unidad de datos de protocolo (<i>protocol data unit</i>)

5 Introducción a la transferencia multipunto de ficheros

Con el fin de sustentar actividades de grupo tales como las reuniones, conferencias u otras en las que intervienen participantes separados físicamente, se plantea la necesidad de reunir dos o más ubicaciones. El término comunicación multipunto describe simplemente la interconexión de múltiples terminales. La transferencia multipunto de ficheros

binarios (MBFT) permite el intercambio interactivo de ficheros entre participantes comprendidos en un entorno multipuntual, merced al servicio de comunicación multipunto (MCS), implícito e independiente de la red.

En concreto, esta Recomendación proporciona mecanismos flexibles y eficientes para dar soporte a:

- distribución simultánea de múltiples ficheros;
- difusión de ficheros a todos los participantes en una conferencia;
- distribución selectiva de ficheros a un subconjunto de participantes;
- extracción de ficheros de posiciones distantes;
- retransmisión parcial de ficheros tras una interrupción;
- acceso distante al directorio.

6 Transferencia multipunto de datos – Visión de conjunto

La Recomendación T.127 emplea una arquitectura de canal de control o de datos que facilita la transferencia simultánea de uno o más ficheros binarios. Permite difundir ficheros a todos los participantes en una conferencia, o bien dirigirlos con carácter selectivo a un subconjunto de posiciones a manera de transferencia privada. No se impone restricción alguna sobre el tipo de datos transmitidos.

Dos tipos de canales se utilizan en esta Recomendación: *canales de control* y *canales de datos*. Los canales de control sirven para gestionar todos los aspectos de la transferencia de ficheros (oferta de ficheros, petición de ficheros), mientras que los canales de datos se utilizan exclusivamente para la transferencia de ficheros de datos. Por cada canal de datos sólo puede transmitirse un fichero a la vez, pero es posible valerse de canales de datos adicionales para permitir la distribución simultánea de múltiples ficheros. El número de canales de datos en uso en un momento dado depende del número de transferencias de ficheros que se encuentren entonces en curso.

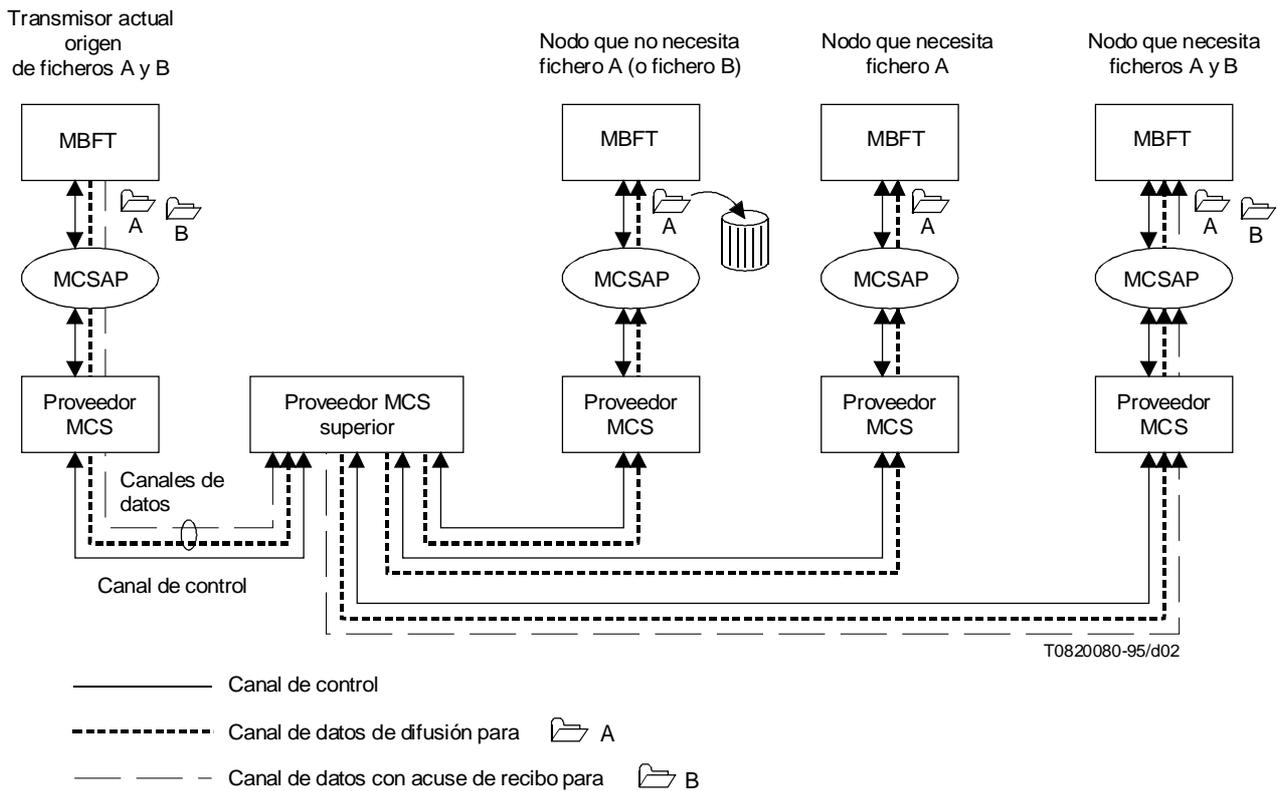
Un grupo de aplicaciones de transferencia que se comunican todas entre sí se consideran participantes en una misma *sesión* de transferencia de ficheros. Cada *sesión* de transferencia requiere un canal de control único y uno o más canales de datos para la distribución de ficheros a todas las aplicaciones participantes.

La Recomendación T.127 considera dos tipos de canales de datos: los de *difusión* y los de *acuse de recibo*. Si un transmisor desea imponer que todos los nodos reciban un fichero que ofrece, deberá utilizar el canal de datos de difusión. Todos los nodos deberán seguir incorporados al canal de datos de difusión mientras dure la sesión de transferencia de ficheros, y están obligados a recibir todos los ficheros que por dicho canal se distribuyan; si alguno de los ficheros no fuere necesario, los receptores deberán descartarlo. Si un transmisor desea conceder a otros nodos la facultad de rechazar un fichero, deberá ofrecer dicho fichero por un canal de datos con acuse de recibo. En este caso, cada nodo debe hacer saber al transmisor si necesita esos datos o no, y solamente se incorporarán al canal de datos los que desean el fichero ofrecido. El empleo de canales de datos con acuse de recibo permite efectuar múltiples transferencias de ficheros concurrentes.

Deberán utilizarse canales de datos con acuse de recibo cuando el transmisor considere que uno o más de los parámetros del encabezamiento del fichero son esenciales para el funcionamiento de la aplicación. Por ejemplo, la aplicación puede requerir un nombre de ruta de acceso para que los receptores lo conserven como referencia futura. Los parámetros esenciales se identifican al ofrecerse el fichero para su distribución; los nodos que no sean capaces de admitir todos esos parámetros deberán rechazar el fichero.

El creador de un canal de datos con acuse de recibo puede disponer que éste sea *exclusivo* (sólo su creador podrá enviar ficheros por él) o *compartido* (podrá enviar ficheros cualquier participante).

Las transacciones de ficheros por el canal de difusión no requieren ningún procedimiento de toma de contacto entre el transmisor y los receptores, ya que los nodos están obligados a recibir todos los ficheros que por ese canal se distribuyan. Esto reduce al mínimo el periodo de latencia al principio de las transferencias de ficheros en las transacciones por el canal de datos de difusión. Las transacciones por el canal de datos con acuse de recibo incurren en cierta latencia al iniciarse la transferencia, pero pueden alcanzar una mejor calidad de funcionamiento global evitando la distribución de datos a posiciones que no los necesitan, particularmente si tales posiciones se ubican sobre enlaces de escasa anchura de banda. La elección del canal queda a discreción del transmisor y puede depender de la aplicación, tamaño del fichero, configuración de la red y número de participantes en la conferencia. Véase la Figura 2.



NOTAS

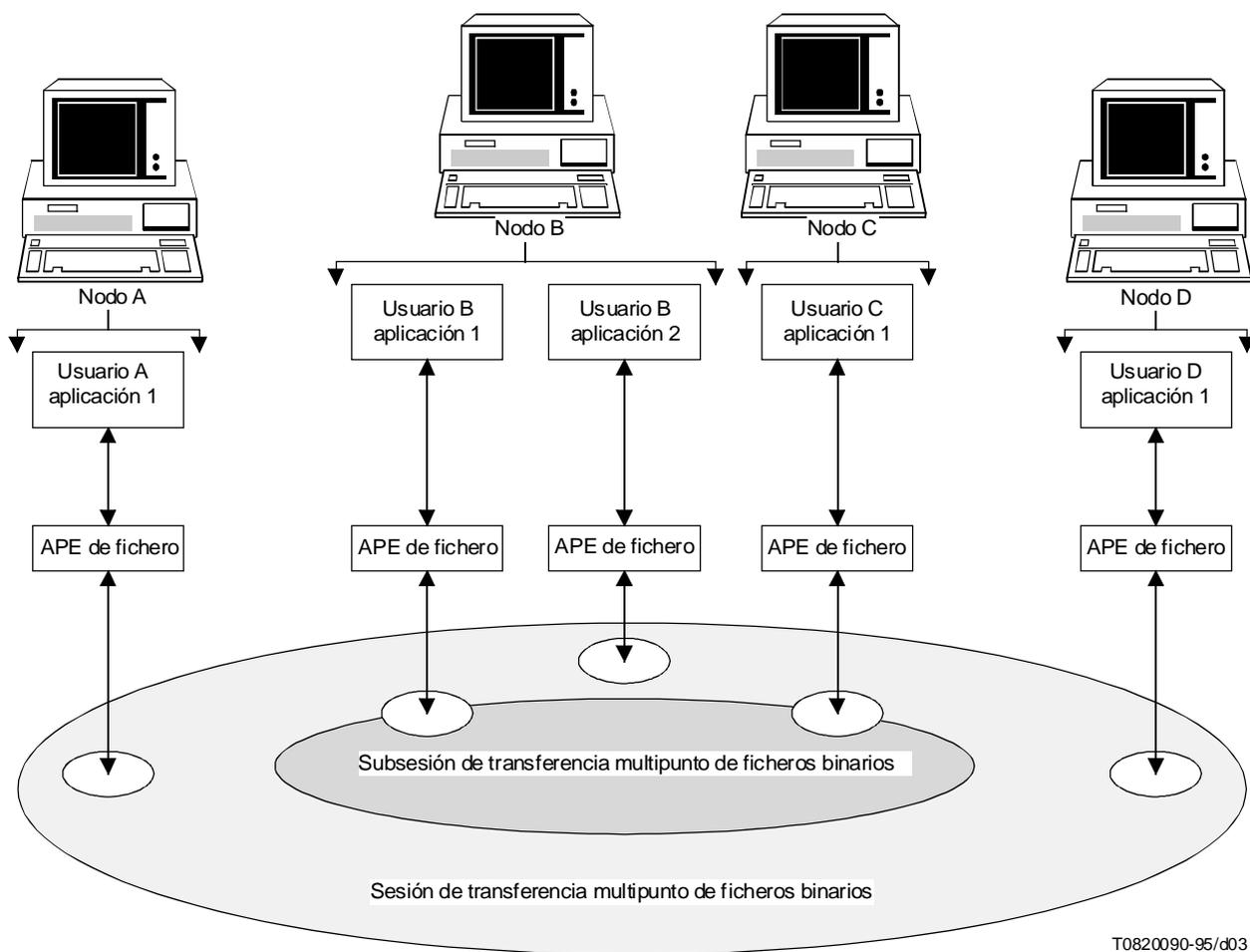
- 1 Todos los nodos están anexionados al canal de control y al canal de datos de difusión.
- 2 Los nodos deben recibir ficheros de datos por el canal de difusión, los necesiten o no.
- 3 Los nodos solamente se incorporan a un canal de datos con acuse de recibo cuando desean recibir el fichero que en ese momento se les ofrece por él.

FIGURA 2/T.127
Modelo de conferencia T.127

La distribución selectiva de ficheros a un subconjunto de nodos dentro de una conferencia puede lograrse mediante la creación de una sesión de transferencia de fichero privada, o el establecimiento de una *subsesión* de transferencia de fichero privada dentro de la sesión existente.

Una subsesión sigue el mismo modelo que la sesión, disponiendo de un canal de control único y de uno o más canales de datos. Véase la Figura 3. No obstante, difiere de la sesión en que no necesita tener un canal de datos de difusión. La subsesión tiene el mismo conjunto de capacidades que su sesión principal, y sus participantes se seleccionan entre los participantes de la sección principal. Las subsesiones no tienen status reconocido dentro del GCC y no aparecen en el registro de aplicaciones GCC. La subsesión no posee un identificador de sesión distinto, sino que trabaja con el identificador de la sesión principal de MBFT. Al evitar el retardo que entraña el proceso de inscripción, las subsesiones permiten iniciar de manera expeditiva los intercambios privados de ficheros interactivos, conservando al mismo tiempo los recursos GCC y MCS.

Se ha previsto que las posiciones soliciten ficheros de otros nodos con el fin de que pueda extraerse información de bases de datos, tableros de anuncios, etcétera. En la petición debe aportarse información suficiente para que la posición de origen identifique inequívocamente el fichero requerido.



T0820090-95/d03

FIGURA 3/T.127
Relación entre subsesión y sesión

6.1 Modelo de sistema T.127

Una sesión MBFT se caracteriza por los siguientes atributos indicados en la Figura 4.

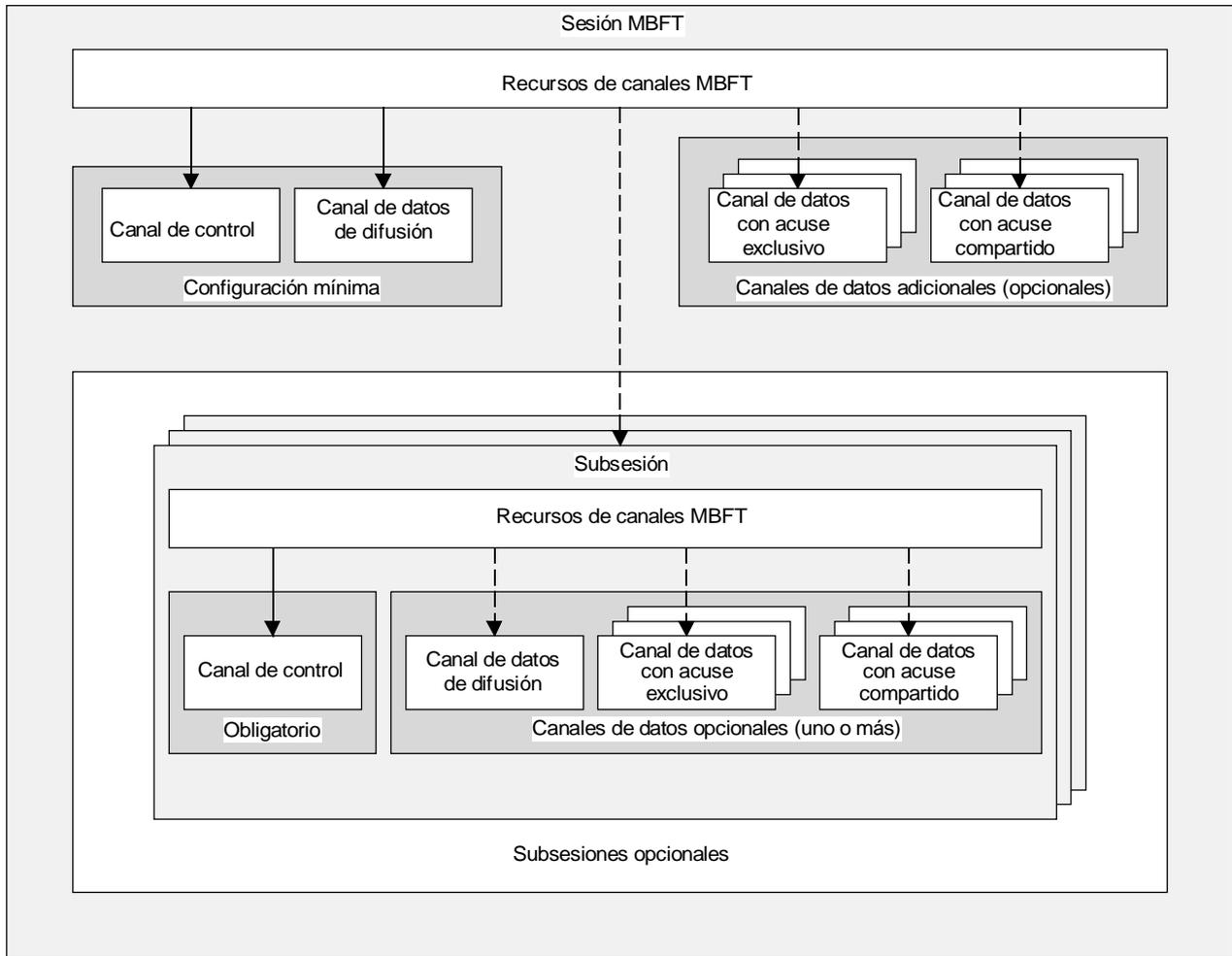
- un canal de control único;
- un canal de datos de difusión único;
- cero o más canales de datos con acuse de recibo;
- cero o más subsesiones privadas (para permitir el intercambio de ficheros entre un subconjunto escogido de participantes en conferencia);
- un identificador de sesión.

Cada subsesión posee los atributos siguientes:

- un canal de control privado único;
- cero o uno canales de datos de difusión privados;
- cero o más canales de datos con acuse de recibo privados;
- ningún identificador de sesión individual (trabaja con el identificador de la sesión MBFT principal).

A cada canal de control se asocia un testigo PETICIÓN-FICHERO (a menos que el creador del canal requiera el derecho exclusivo a solicitar ficheros de otras posiciones).

A cada canal de datos se asocia un testigo TRANSMISIÓN-FICHERO (a menos que el creador del canal requiera el derecho exclusivo a transmitir ficheros por ese canal).



T0820100-95/d04

FIGURA 4/T.127
Modelo de canal T.127

6.2 Compresión

Puede aplicarse compresión a los ficheros, como resultado de una fructuosa negociación; por defecto, los ficheros están sin comprimir. Es posible identificar técnicas de propiedad reservada utilizando los formatos especificados en la Recomendación T.124; por ejemplo, el código de país T.35, el código de asignación nacional, el código de fabricante, el código de capacidad no normalizada. En cambio pueden adquirirse identificadores de objetos. De hecho, a través de este mecanismo pueden identificarse también formatos de compresión no normalizados. Adviértase que la compresión se aplica únicamente al contenido útil de datos del fichero, y no a su encabezamiento.

6.3 Prioridad

La Recomendación T.127 puede utilizarse como una tarea básica que realiza la transferencia de gran volumen de datos, y también como tarea de primer término para la inmediata distribución de ficheros. La posición transmisora selecciona el modo que ha de utilizarse; a la transferencia rápida de datos ha de asignarse una prioridad media, y una prioridad baja a la transferencia de datos en bloque. A lo largo de la transmisión de un fichero debe mantenerse la misma prioridad, pero ésta puede variar entre transmisiones sucesivas.

La gestión de las transacciones de ficheros por el canal de control utilizará una prioridad alta.

6.4 Entrega previa de ficheros

Con miras a reducir al mínimo el tráfico de transferencia de ficheros durante una conferencia interactiva, pueden entregarse ficheros en una reunión convocada con el fin expreso de distribuir material de la conferencia anticipadamente. Este proceso puede ser automatizado, y si las posiciones receptoras son capaces de identificar los ficheros que desean recibir, el tráfico de ficheros podrá mantenerse en el nivel mínimo.

7 Aplicación MBFT básica

Las aplicaciones que desean sustentar el protocolo de transferencia de ficheros deben ser capaces de incorporarse al canal de control y de enviar o recibir por el canal de datos de difusión. El Cuadro 1 identifica las PDU que han de admitirse.

CUADRO 1/T.127

PDU de MBFT admitidas

MBFTPDU	APE para sólo recibir ficheros		APE para sólo transmitir fichero		APE para transmitir y recibir ficheros	
	PDU de envío	PDU de recepción	PDU de envío	PDU de recepción	PDU de envío	PDU de recepción
Oferta-fichero	–	M	M	M	M	M
Aceptación-fichero	M	–	–	M	M	M
Rechazo-fichero	M	–	M	M	M	M
Petición-fichero	O	M	–	M	O	M
Denegación-fichero	M	O	M	–	M	O
Error-fichero	O	–	–	O	O	O
Aborto-fichero	O	–	O	M	O	M
Inicio-fichero	–	M	M	–	M	M
Datos-fichero	–	M	M	–	M	M
Petición-directorio	O	M	O	M	O	M
Respuesta-directorio	M	O	M	O	M	O
MBFT-no normalizada	O	O	O	O	O	O
MBFT-petición-privilegio	O	O	M	O	M	O
MBFT-asignación-privilegio	O	M	O	M	O	M
Invitación-incorporación-canal-privado	O	M	O	M	O	M
Respuesta-incorporación-canal-privado	M	O	M	O	M	O
M Obligatorio O Opcional – No requerido						

8 Descripción de funcionamiento

Una aplicación de usuario de transferencia de ficheros se apoya en los servicios de una entidad de protocolo de aplicación transferencia de ficheros (APE de fichero) para comunicarse con aplicaciones pares en otros nodos. La APE mencionada tiene dos componentes, ilustrados en la Figura 5: un gestor de recursos de aplicación transferencia de ficheros (ARM de fichero) y un elemento de servicio de aplicación transferencia de ficheros (ASE de fichero). El ARM proporciona la funcionalidad genérica, común a todos los protocolos de aplicación normalizados, mientras que el ASE proporciona la funcionalidad específica de ese protocolo de aplicación para permitir el interfuncionamiento de las aplicaciones de transferencia de ficheros. Adviértase que este modelo es conceptual y no impone restricción alguna sobre la estructura de las implementaciones reales.

Cada componente se describe a continuación con más detalle.

8.1 Aplicación de usuario transferencia de ficheros

Es la parte de la aplicación transferencia de ficheros que aborda los aspectos que no tienen un influjo directo sobre el interfuncionamiento (por ejemplo, la interfaz de usuario) y que por ello pueden ser específicos del producto y de la estructura. La influencia de la aplicación de usuario es por tanto local respecto a la posición en la que reside, y en cuanto tal cae fuera del alcance de esta Recomendación. Una aplicación de usuario se apoya en los servicios de una entidad de protocolo de aplicación (APE) transferencia de ficheros para comunicarse con aplicaciones pares. No se comunica con el MCS ni con el GCC; es la APE quien lo hace. La aplicación de usuario inicia una sesión de transferencia de ficheros a través de su APE, especificando las capacidades de la aplicación y el modo de la sesión. Una vez establecida la sesión, todas las transacciones características de la MBFT son realizadas por la APE en nombre de la aplicación de usuario.

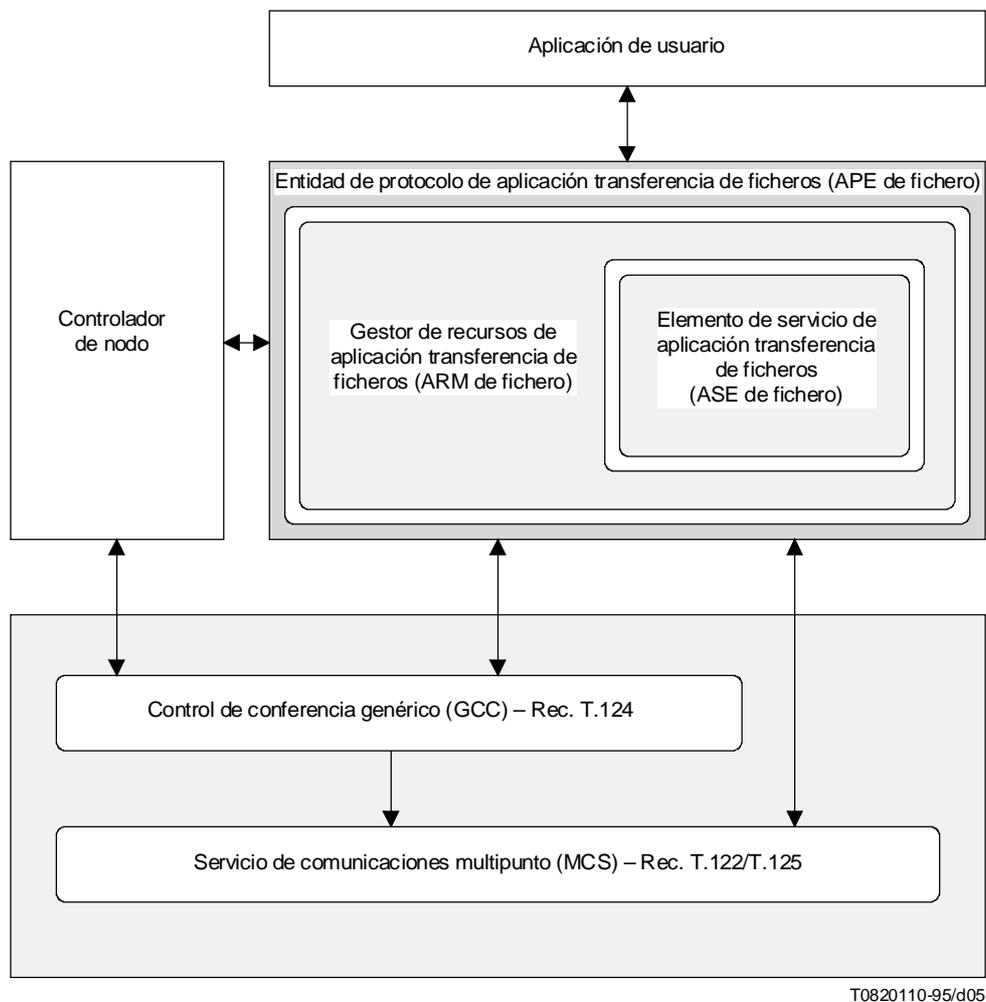
8.2 Gestor de recursos de aplicación transferencia de ficheros

El gestor de recursos de aplicación transferencia de ficheros (ARM de fichero) es responsable de gestionar los recursos GCC y MCS en nombre del ASE de fichero. Proporciona los servicios siguientes:

- Respuesta a las indicaciones de GCC (por ejemplo, permiso de inscripción, invocación).
- Inscripción de la APE de fichero con el GCC.
- Anexión a un dominio MCS con miras a obtener un identificador de usuario MCS para la APE.
- Incorporación de canales estáticos.
- Identificación e incorporación de canales multidifusión que utilizan el registro GCC y el MCS.
- Formación de canales privados y admisión en estos canales de APE pares.
- Incorporación de todo canal privado en el que se haya admitido la APE.
- Identificación y obtención de testigos del registro GCC.
- Supresión de las entradas del registro asociadas con cualquier canal que pueda haber creado.
- Invocación de APE pares en otros nodos.
- Procesamiento de informes del registro de aplicaciones para determinar la lista de capacidades de aplicación negociadas y la identidad de las APE pares.

8.3 Elemento de servicio de aplicación transferencia de ficheros

El elemento de servicio de aplicación transferencia de ficheros (ASE de fichero) proporciona la funcionalidad de transferencia de fichero a la aplicación de usuario con los recursos obtenidos por el ARM de fichero. Su funcionamiento es independiente del tipo (es decir, estático o dinámico) y de la identidad de los testigos que se le han pasado. La aplicación de usuario especifica si se necesita un canal de datos de difusión o con acuse de recibo. Para las transferencias privadas a un subconjunto de la conferencia, se necesita además una lista de los identificadores de usuario MBFT.



T0820110-95/d05

FIGURA 5/T.127
Modelo de aplicación T.127

El ASE proporciona los servicios siguientes:

- Envío y recepción de las PDU MBFT.
- Toma y liberación de testigos y determinación de status de testigos mediante el MCS.
- Respuesta a las indicaciones GCC-asignar-conductor y liberación.
- Emisión de peticiones GCC-petición-permiso-conductor a través del controlador de nodo.
- Respuesta a las indicaciones GCC-concesión-permiso-conductor.

8.4 Recursos MBFT

Una sesión de transferencia de ficheros binarios utiliza *canales de control* para la gestión de las transferencias y *canales de datos* para la distribución de ficheros. A cada canal de control se asocian uno o más canales de datos, y cada canal de datos sustenta una transferencia de ficheros a la vez.

Cada sesión MBFT dispone de un canal de control de sesión (con el nemotécnico CONTROL-MBFT asociado) y un canal de datos de difusión (al cual se asigna el nemotécnico DATOS-MBFT), a los que se han de incorporar todas las aplicaciones que participen en esa sesión. El canal de control se utiliza para gestionar todas las transferencias de ficheros por el canal de datos de difusión. Todos los nodos se ven obligados a recibir los ficheros transmitidos por dicho canal de

difusión, y a descartarlos en el caso de que no necesiten esos datos. De ahí puede derivarse una degradación innecesaria en la calidad de funcionamiento de la conferencia si los nodos que no requieren los datos están situados sobre enlaces de escasa anchura de banda.

El empleo de *canales de datos con acuse de recibo* [con el nemotécnico DATOS-MBFT(n), siendo n el identificador de canal MCS del canal de datos] permite la distribución simultánea de varios ficheros. La gestión de las transferencias de ficheros por estos canales se realiza a través del canal de control de sesión, pero en este caso los nodos tienen la facultad de rechazar los ficheros que se les ofrecen. Se garantiza así que los ficheros se distribuyen solamente a aquellos nodos que los necesitan, aunque a expensas de introducir cierto periodo de latencia en cada transferencia de fichero.

La distribución selectiva de ficheros a un subgrupo de participantes dentro de una sesión existente puede conseguirse mediante la apertura de *subsesión*. Para ello se dispone de un *canal de control* de subsesión privado [al que se le asigna el nemotécnico CONTROL-MBFT(p), siendo p el identificador de canal MCS del canal de control]. Se utiliza éste para gestionar las transferencias de ficheros por cero o uno *canales de datos de difusión privados* [que llevan asignado el nemotécnico DATOS-MBFT(p), siendo p el identificador de canal MCS del canal de datos], y por cero o más *canales de datos con acuse de recibo privados* [con el nemotécnico DATOS-MBFT(n) asignado, siendo n el identificador de canal MCS del canal de datos]. Para cada subsesión privada se requiere un canal de control privado individual.

Cada canal de control puede poseer un testigo PETICIÓN-FICHERO, cuyo propósito es asegurar que en ese canal no haya más de una petición de fichero pendiente en ningún caso. Un ASE que necesite un fichero debe tomar ese testigo antes de emitir la petición y retenerlo hasta que determine si otro nodo puede suministrar ese fichero. Se permiten canales de control dinámico sin testigo PETICIÓN-FICHERO, pero sólo el creador de un canal de ese tipo puede emitir peticiones de ficheros a través de él. Al testigo para el canal de control de sesión CONTROL-MBFT se le asigna el nemotécnico PETICIÓN-FICHERO; para un canal de control de subsesión CONTROL-MBFT(p) el testigo es PETICIÓN-FICHERO(p).

Cada canal de datos puede contar con un testigo TRANSMISIÓN-FICHERO, cuyo propósito es asegurar que sólo haya una transferencia de ficheros en curso por dicho canal de datos en cualquier caso. Un ASE transmisor tomará ese testigo antes de ofrecer un fichero a transmisión, y lo retendrá mientras dure la transferencia del mismo, liberando el testigo una vez despachado el último bloque de datos del fichero. Se permiten canales de control dinámico sin testigo TRANSMISIÓN-FICHERO, pero sólo el creador de un canal de ese tipo podrá enviar ficheros por él. Al testigo para el canal de datos de difusión de la sesión DATOS-MBFT se le asigna el nemotécnico TRANSMISIÓN-FICHERO, al testigo del canal de datos de difusión de subsesión DATOS-MBFT(p) se le asigna TRANSMISIÓN-FICHERO(p), y TRANSMISIÓN-FICHERO(n) al testigo del canal de datos con acuse de recibo DATOS-MBFT(n).

Todos estos canales y testigos reunidos constituyen los *recursos* disponibles para una sesión MBFT; pueden ser de tipo estático o dinámico. El gestor de recursos de aplicación transferencia de ficheros (ARM de fichero) es responsable de determinar la identidad de dichos recursos. Para cualquier transacción de fichero determinada, la aplicación de usuario debe especificar los recursos que ha de utilizar el ASE. Los recursos estáticos y dinámicos son tratados de modo idéntico por el ASE de fichero.

8.4.1 Inicialización de MBFT

Una sesión MBFT puede ser iniciada localmente por una aplicación de usuario o a distancia por medio del mecanismo GCC-invocación-aplicación. En ambos casos, los parámetros indicados en el Cuadro 2 se pasan al ARM de fichero. La acción que debe ejercer dicho ARM para identificar el conjunto inicial de recursos utilizable por la sesión, viene determinada por el modo de sesión, como seguidamente se describe:

Se utiliza el *modo estático* para la difusión sin restricciones de los datos a la conferencia. Es el modo de operación más sencillo, puesto que utiliza canales y testigos estáticos previamente definidos. Las aplicaciones pueden incorporarse a una sesión en modo estático y abandonarla, a su albedrío. Aunque el ASE de fichero puede ser empleado simultáneamente por otros protocolos de aplicación que utilizan diferentes subconjuntos de canales y testigos estáticos, esta Recomendación solamente predefine un modo estático del ARM de fichero.

Puede utilizarse el *modo de multidifusión* para la difusión de datos cuando la sesión estática está ya en uso. Es idéntico en su función al modo estático, pero utiliza recursos dinámicos y por ello las identidades de canales y testigos deben ser asignadas a través del registro GCC y los servicios MCS por el creador de la sesión de multidifusión (denominado *creador de multidifusión*). Todos los demás participantes (*miembros de multidifusión*) pueden determinar las identidades de canales y testigos a través del registro GCC. Las aplicaciones pueden incorporarse a una sesión multidifusión y abandonarla, a su albedrío. No existen restricciones en cuanto al número de sesiones en modo multidifusión dentro de una conferencia.

Parámetros de APE de fichero

Parámetro	Descripción
SessionMode (modo de sesión)	<p>Este parámetro puede recibir uno de los tres valores siguientes:</p> <p><i>estático</i>: Este valor indica que la APE de fichero debe inscribirse mediante una clave de sesión compuesta del identificador de objeto MBFT y el parámetro sessionID (identificador de sesión). Utilizará los canales estáticos CONTROL-MBFT y DATOS-MBFT previamente definidos, y los testigos estáticos TRANSMISIÓN-FICHERO y PETICIÓN-FICHERO.</p> <p><i>dinámico multidifusión</i>: Este valor indica que la APE de fichero debe inscribirse mediante una clave de sesión compuesta del identificador de objeto MBFT y el parámetro sessionID. Todos los recursos de canales y testigos son dinámicos y son atribuidos por el creador de la sesión de multidifusión utilizando el mecanismo MCS-INCORPORACIÓN-CANAL y el mecanismo registro-GCC, respectivamente. Los miembros de una sesión multidifusión determinan los identificadores de testigo y de canal a través del registro GCC.</p> <p><i>dinámico privado</i>: Este valor indica que la APE de fichero debe inscribirse mediante una clave de sesión compuesta del identificador de objeto MBFT y el parámetro sessionID.</p> <p>Todos los recursos de testigos y canales son dinámicos y son atribuidos por el ARM de fichero del formador privado utilizando el mecanismo registro-GCC y el mecanismo MCS-FORMACIÓN-CANAL, respectivamente. El ARM de fichero que crea la sesión puede entonces admitir a los canales CONTROL-MBFT y DATOS-MBFT todas las APE pares cuyos identificadores de usuario MCS (MCS User IDs) están presentes en el parámetro de protocolo admitList (lista de admisión).</p> <p>Un ARM de fichero de miembro privado debe esperar que su APE de fichero sea admitida por el formador de los canales MCS privados antes de intentar incorporarse a ellos. Las identidades de testigos son transportadas dentro de la banda por el formador de canal en la primera transacción.</p>
sessionID (identificador de sesión)	<p>Se utiliza este parámetro para diferenciar los recursos utilizados por múltiples sesiones del protocolo que pueden existir simultáneamente dentro del mismo dominio MCS. El identificador de canal MCS asignado al canal CONTROL-MBFT es utilizado como SessionID, puesto que tiene la garantía de ser único dentro del dominio de la conferencia.</p> <p>Debe especificarse el SessionID si la aplicación desea participar en una sesión estática o en una sesión multidifusión o privada existente. Se omite si la aplicación desea crear una nueva sesión multidifusión o privada.</p>
admitList (lista de admisión)	<p>SessionMode = private y SessionID omitida</p> <p>Lista de identificadores de usuario GCC correspondientes a los nodos en que las APE de fichero han de ser admitidas a los canales formados privadamente.</p> <p>else (en los demás casos).</p> <p>Omitida.</p>

El *modo privado* se utiliza para la distribución selectiva de ficheros a un subconjunto de participantes. El ARM (denominado *formador privado*) es el responsable de iniciar la sesión privada para obtener testigos y canales que utilicen el GCC y el MCS respectivamente, y para admitir APE de fichero pares (*miembros privados*) a los canales. La identidad de los testigos se transporta dentro de la banda, pero puede también determinarse a través del registro GCC. No existe restricción en cuanto al número de sesiones en modo privado dentro de una conferencia. Un ARM miembro privado debe esperar a que su APE sea admitida a los canales privados y a que el formador asigne los testigos que han de utilizarse en la sesión. En cuanto el formador abandona la sesión privada, todos los demás participantes son excluidos. Solamente pueden incorporarse aplicaciones a una sesión privada a invitación del formador de sesión.

En todos los casos, el conjunto inicial de recursos permite la transferencia de un fichero a la vez. La transferencia concurrente de múltiples ficheros se describe en 8.6.

Un APE de fichero creado en un nodo cualquiera debe establecer primeramente un GCCSAP que le permita comunicarse con el proveedor GCC en ese nodo. Cuando el nodo se incorpore a una conferencia, el proveedor GCC emitirá un GCC-aplicación-permiso-para-inscribir con la bandera *concesión/revocación* fijada en *concesión*. El ARM de fichero deberá entonces emitir una petición GCC-inscribir-aplicación sin considerar si la aplicación de usuario desea o no inscribirse en ese momento. Si la aplicación de usuario no deseara inscribirse, el ARM de fichero tendrá que fijar en *desinscripción* la bandera *inscripción/desinscripción* de la petición GCC-inscribir-aplicación y especificar el identificador de la conferencia. No se requiere ningún otro parámetro. La aplicación puede inscribirse en cualquier momento posterior, a

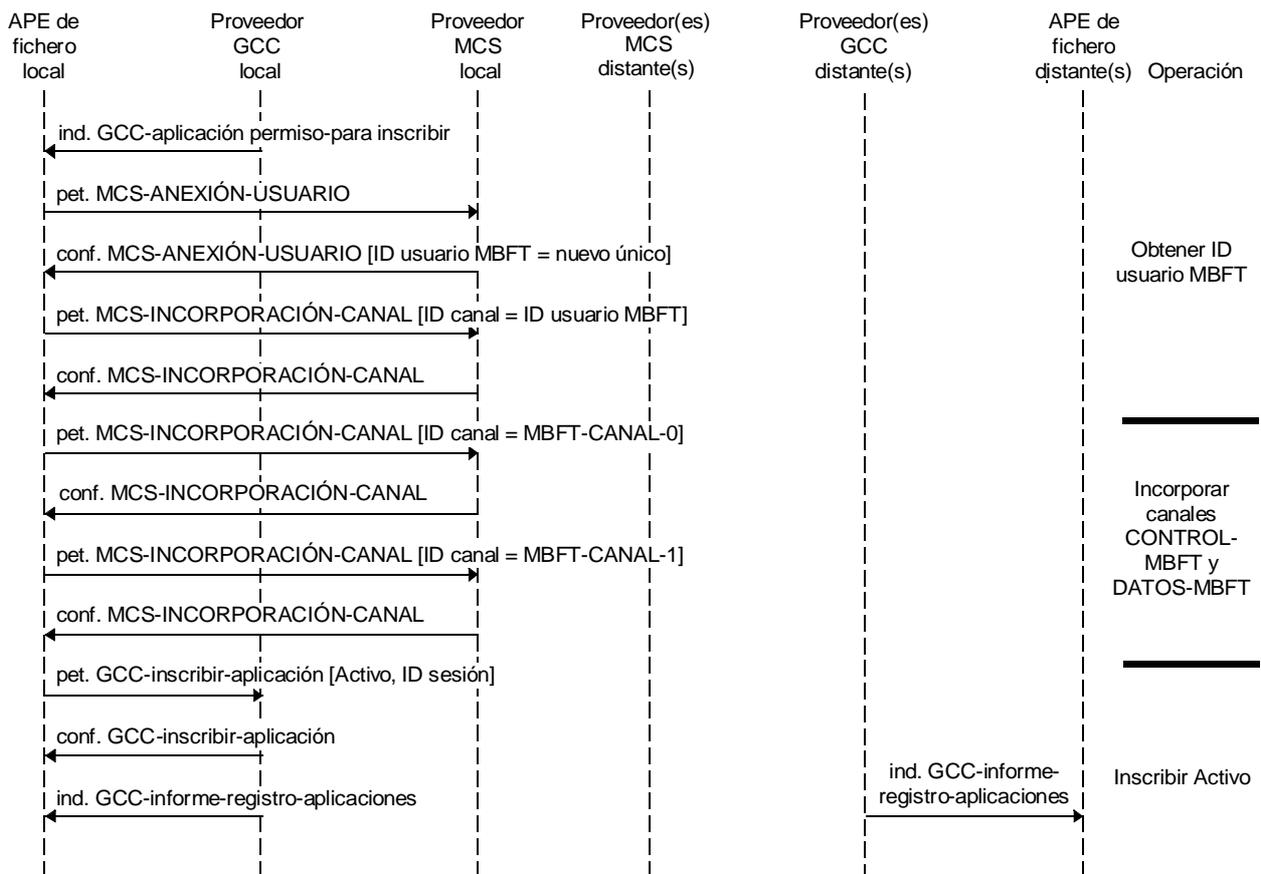
menos que el permiso sea revocado por recibirse una indicación GCC-aplicación-permiso-para-inscribir con la bandera *concesión/revocación* fijada en *revocación*.

Si la aplicación de usuario desea recibir del registro de aplicaciones GCC informes sobre todas las sesiones MBFT en curso antes de decidir en cuál sesión va a participar, el ARM de fichero deberá inscribirse *inactivo*, especificando la clave de sesión sin identificador de sesión. En el caso de que la aplicación de usuario desee declarar que sustenta el protocolo MBFT sin consumir recursos MCS, el ARM de fichero deberá inscribirse *inactivo* sin identificador de usuario MCS.

Cuando la aplicación de usuario decida inscribirse como activa, el ARM de fichero emitirá una petición MCS-anexión-usuario hacia el proveedor MCS, utilizando el identificador de conferencia contenido en la indicación GCC-aplicación-permiso-para-inscribir como selector de dominio. Cuando se reciba una confirmación MCS-anexión-usuario exitosa en respuesta, el ARM deberá incorporar el canal del identificador de usuario indicado emitiendo una petición MCS-incorporación-canal.

8.4.2 Modo estático

Obtenido un identificador de usuario MCS, el ARM de fichero incorporará los canales MBFT de control y de datos estáticos mediante la emisión de dos peticiones MCS-incorporación-canal, en las que se especifique MBFT-CANAL-0 y MBFT-CANAL-1 como los respectivos canales a incorporar. Una vez recibida la confirmación positiva de la incorporación de estos canales, el ARM de fichero debe inscribirse *activo* emitiendo una petición GCC-inscribir-aplicación hacia el proveedor GCC, con los parámetros señalados en el Cuadro 3. La bandera *activo/inactivo* deberá fijarse en *activo*, el Session ID será especificado como parte de la clave de sesión, el canal de iniciación se especificará como estático y deberá proporcionarse la lista completa de capacidades de aplicación. Véase la Figura 6.



T0820120-95/d06

FIGURA 6/T.127
Secuencia de iniciación de protocolo de sesión estática

Parámetros de la petición GCC-inscribir-aplicación

Parámetro	Contenido
ID de conferencia	Proporcionado por indicación GCC-aplicación-permiso-para-inscribir.
Clave de sesión	{recomendación uit-t 127 versión(0) 1} y MBFT-ID-SESIÓN si se especificara este parámetro de APE de fichero.
ID usuario de aplicación	Proporcionado por confirmación MCS-anexión-usuario.
Activo/inactivo	Activo cuando indica que el ARM de fichero ha incorporado los canales CONTROL-MBFT y DATOS-MBFT y determinado los ID de testigo MBFT que se necesiten. Inactivo en el caso de modos multidifusión o privados cuando la inscripción es anterior a la incorporación de los canales CONTROL-MBFT y DATOS-MBFT.
Bandera de operación conductora	Fijada, si el APE de fichero es capaz de convertirse en conductor MBFT de la sesión en modo conducido, es decir, si puede responder a las PDU MBFT-petición-privilegio. Esta bandera no debe estar fijada si la bandera activo/inactivo se fija en inactivo.
Canal de iniciación	Este parámetro depende de los parámetros de APE de fichero especificados en el Cuadro 2: Static (estático), si SessionMode = Static Dynamic Multicast (multidifusión dinámico), si SessionMode = Dynamic Multicast y se omite sessionID Dynamic Private (privado dinámico), si SessionMode = Dynamic Private y se omite sessionID Omitido en los demás casos.
Lista de capacidades no colapsables	Este protocolo no especifica ninguna capacidad no colapsable. En este campo pueden incluirse capacidades no normalizadas y no colapsables especificadas por la aplicación de usuario.
Lista de capacidades de aplicación	Véase Cuadro 7; omitida si la bandera activo/inactivo está fijada en inactivo.
Inscripción/desinscripción	INSCRIPCIÓN.

8.4.3 Modo multidifusión

Obtenido un identificador de usuario MCS, el ARM de fichero deberá examinar el parámetro sessionID de la APE de fichero para determinar si indica que ha de participar en una sesión multidifusión existente (como miembro de multidifusión) o crear una nueva (como creador de multidifusión).

Si el parámetro sessionID está presente, el ARM de fichero intentará incorporar la sesión indicada emitiendo una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en inactivo y especificando la clave de sesión con el indispensable identificador de sesión. A continuación emitirá una petición MCS-incorporación-canal, especificando el sessionID de la sesión elegida como parámetro identificador de canal. Este canal se utiliza como canal CONTROL-MBFT. El ARM de fichero deberá seguidamente identificar e incorporar el canal DATOS-MBFT emitiendo una petición GCC-extracción-entrada-registro, que utilizará los parámetros señalados en el Cuadro 4. A la recepción de la confirmación GCC-extracción-entrada-registro, el ARM de fichero examinará el parámetro elemento-registro. El identificador de canal contenido en ese parámetro será utilizado como canal DATOS-MBFT, y el ARM de fichero lo incorporará emitiendo una petición MCS-incorporación-canal.

Si desea iniciar una transacción de ficheros, el ARM de fichero podrá entonces identificar el testigo TRANSMISIÓN-FICHERO que ha de utilizar el canal de datos de difusión emitiendo una petición GCC-extracción-entrada-registro, que utilizará los parámetros señalados en el Cuadro 4. Si el parámetro de resultado contenido en la confirmación GCC-extracción-entrada-registro fuera 'entrada no encontrada', solamente al creador de la sesión le sería permitido solicitar ficheros por el canal de control. El ARM de fichero podrá también identificar el testigo PETICIÓN-FICHERO que ha de

utilizar el canal de control emitiendo una petición GCE-extracción-entrada-registro. Si el parámetro de resultado contenido en la confirmación GCE-extracción-entrada-registro fuera 'entrada no encontrada', solamente al creador de la sesión le sería permitido solicitar ficheros por el canal de control.

En caso de que el ARM de fichero no desee iniciar una transacción de ficheros, ya no necesitará identificar el testigo TRANSMISIÓN-FICHERO ni el testigo PETICIÓN-FICHERO durante el proceso de inscripción. En lugar de ello, puede determinar los identificadores de estos testigos posteriormente, a partir de las PDU oferta-fichero o petición-fichero que emitan ARM de fichero pares por el canal CONTROL-MBFT.

Una vez determinados todos los recursos requeridos para la sesión e incorporados los canales, el ARM de fichero emitirá una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en activo, especificando el identificador de sesión como parte de la clave de sesión y proporcionando la lista completa de capacidades de protocolo de aplicación. Véanse las Figuras 7 y 8.

CUADRO 4/T.127

Parámetros de la petición GCC-extracción-entrada-registro

Parámetro	Contenido
ID conferencia	Proporcionado por indicación GCC-aplicación-permiso-para-inscribir
Clave de registro	Clave de registro formada según lo descrito en 8.4.5

Si se omite el parámetro sessionID de la APE, el ARM intentará crear una nueva sesión. Primero emitirá una primitiva de petición MCS-incorporación-canal con ID canal = 0. La confirmación MCS-incorporación-canal devuelta contiene, si se ha logrado éxito, el ID asignado al canal que ha de utilizarse como canal CONTROL-MBFT. El proceso se repite luego para asignar e incorporar el canal DATOS-MBFT. El ARM inscribirá a continuación inactivo en esta sesión emitiendo una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en inactivo, especificando la clave de sesión con el ID de sesión, pero omitiendo la lista de capacidades de aplicación. Una vez que el ARM haya recibido una GCC-informe-registro-aplicaciones que contenga una entrada correspondiente a la nueva sesión, registrará el canal DATOS-MBFT emitiendo una petición GCC-registrar-canal-registro con los parámetros señalados en el Cuadro 5.

El ARM de fichero puede seguidamente asignar los testigos TRANSMISIÓN-FICHERO y PETICIÓN-FICHERO emitiendo dos peticiones GCC-asignar testigo-registro que utilizan los parámetros indicados en el Cuadro 6. Si el ARM de fichero requiere acceso exclusivo al canal de datos de difusión, no necesitará asignar el testigo TRANSMISIÓN-FICHERO. Y si el ARM de fichero requiere el derecho exclusivo a la petición de ficheros, no tendrá que asignar el testigo PETICIÓN-FICHERO.

Una vez determinados con éxito todos los recursos, el ARM de fichero debe inscribirse activamente emitiendo para ello una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en activo, el canal de iniciación especificado como multidifusión dinámico, y proporcionando la lista completa de capacidades de protocolos de aplicación. Se utiliza el identificador de canal CONTROL-MBFT como SessionID en la clave de sesión.

CUADRO 5/T.127

Parámetros de la petición GCC-registrar-canal-registro

Parámetro	Contenido
ID conferencia	Proporcionado por indicación GCC-aplicación-permiso-para-inscribir
Clave de registro	Clave de registro formada según lo descrito en 8.4.5
ID canal	ID canal devuelto en confirmación MCS-incorporación-canal

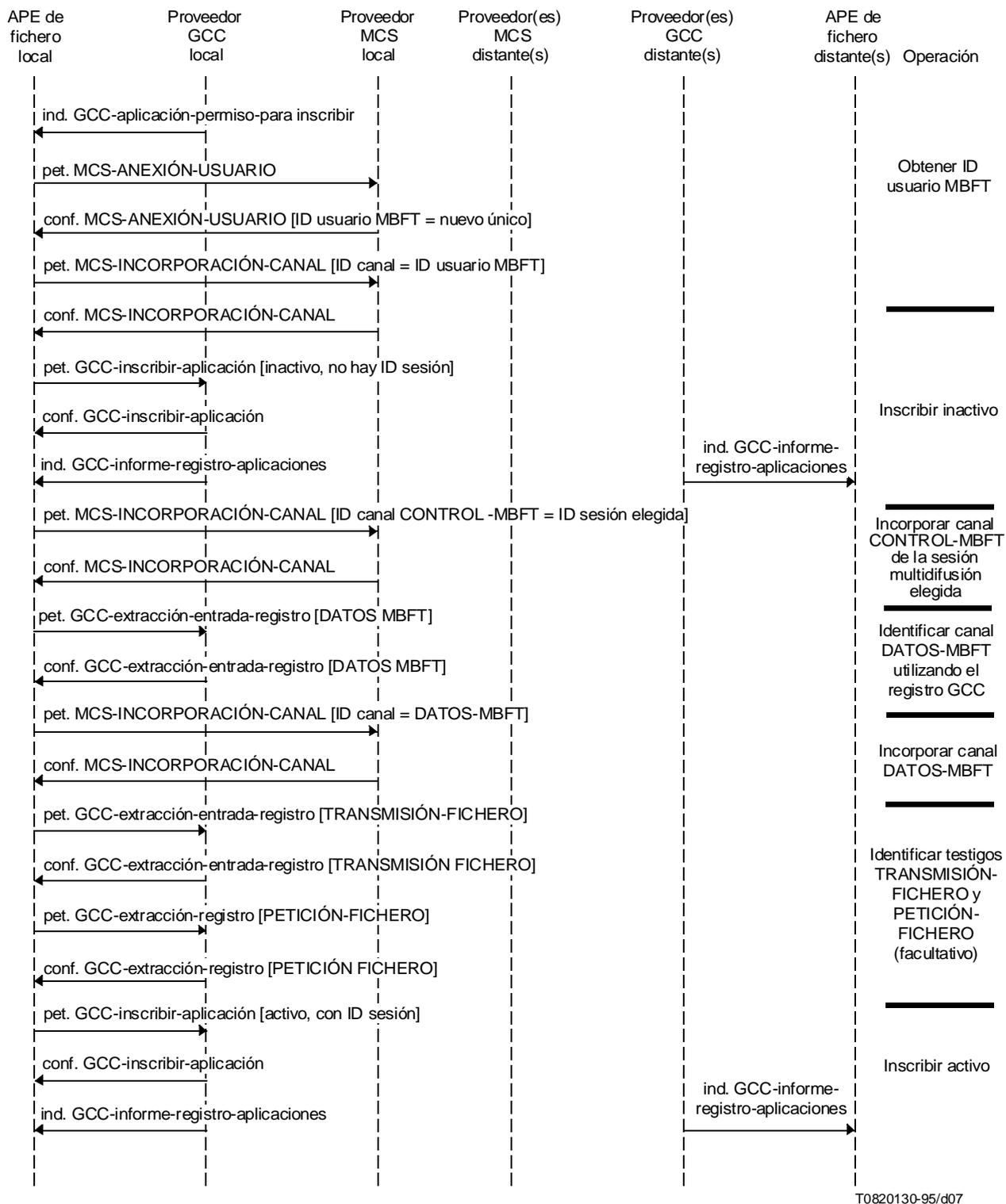


FIGURA 7/T.127
Secuencia de iniciación de protocolo de sesión multidifusión (miembro)

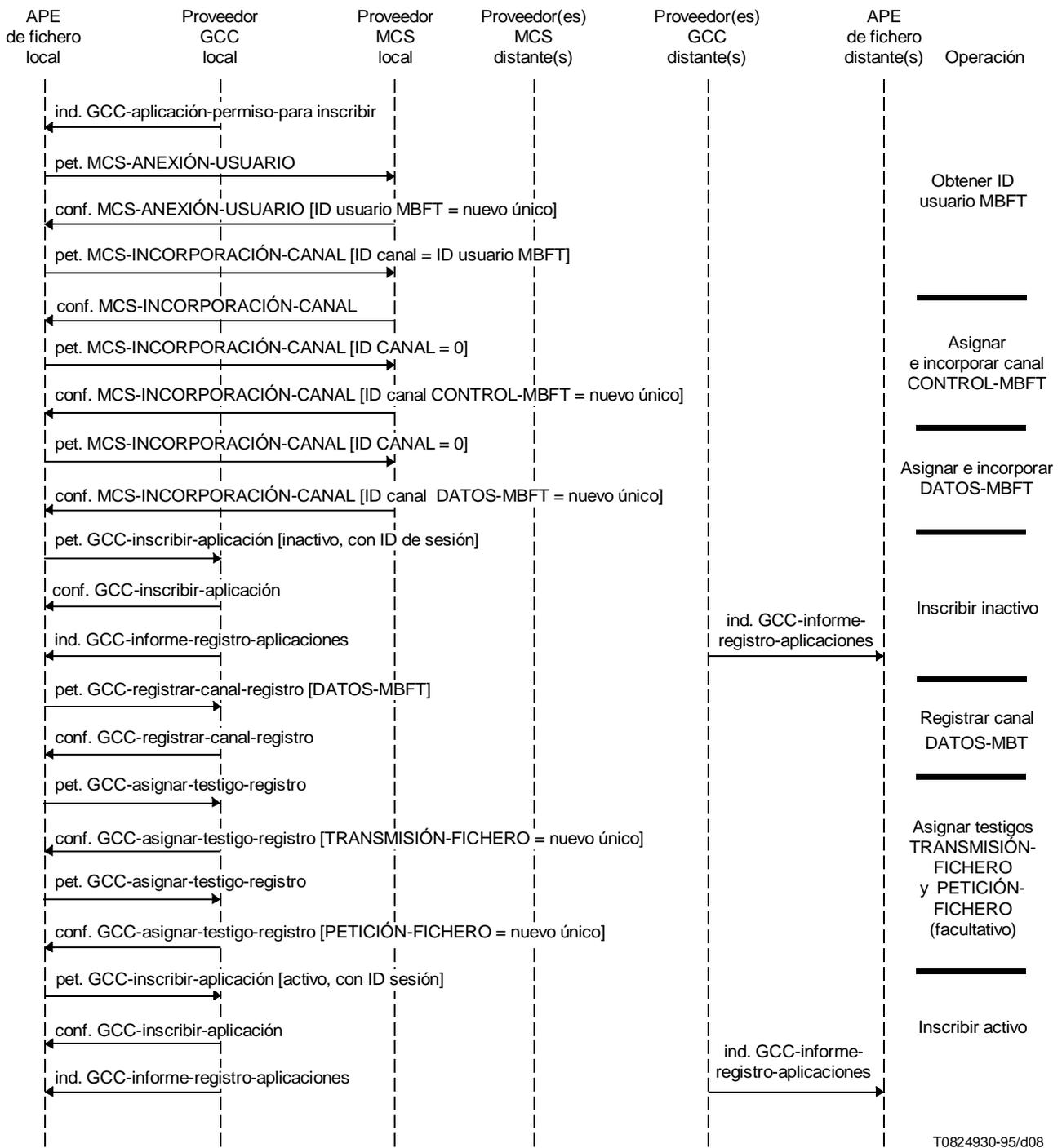


FIGURA 8/T.127

Secuencia de iniciación de protocolo de sesión multidifusión (creador)

Parámetros de la petición GCC-asignar-testigo-registro

Parámetro	Contenido
ID conferencia	Proporcionado por indicación GCC-aplicación-permiso-para-inscribir
Clave de registro	Clave de registro formada según lo descrito en 8.4.5

8.4.4 Modo privado

Obtenido un identificador de usuario MCS, el ARM de fichero examina el parámetro sessionID de la APE de fichero para determinar si indica que ha de participar en una sesión privada existente (como miembro privado) o crear una nueva (como formador privado).

Si se omite el parámetro sessionID, el ARM intentará crear una nueva sesión privada. Primero emitirá una petición MCS-formación-canal con el fin de obtener un canal CONTROL-MBFT privado. Si se logra éxito, la confirmación MCS-formación-canal devuelta contendrá el ID del canal atribuido. El ARM deberá entonces incorporar ese canal emitiendo una petición MCS-incorporación-canal, en la que se especifique el ID de canal devuelto en la confirmación MCS-formación-canal. Este proceso se repetirá para asignar e incorporar un canal DATOS-MBFT independiente del anterior. El ARM inscribirá a continuación inactivo en la nueva sesión emitiendo una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en inactivo, especificando la clave de sesión con el ID del canal CONTROL-MBFT como ID de sesión y omitiendo la lista de capacidades de aplicación.

El ARM de fichero puede entonces asignar testigos TRANSMISIÓN-FICHERO y PETICIÓN-FICHERO mediante la emisión de dos peticiones GCC-asignar-testigo-registro que utilicen los parámetros señalados en el Cuadro 6. Si el ARM de fichero requiere un acceso exclusivo al canal de datos de difusión, no necesitará asignar el testigo TRANSMISIÓN-FICHERO. Y si requiere el derecho exclusivo a la petición de ficheros, no tendrá que asignar el testigo PETICIÓN-FICHERO.

A continuación, el ARM de fichero deberá inscribirse activamente emitiendo para ello una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en activo, el canal de iniciación especificado como privado dinámico, y proporcionando la lista completa de capacidades de protocolos de aplicación. Se utiliza el identificador de canal CONTROL-MBFT como SessionID en la clave de sesión.

Si no hay ninguna APE de fichero activa par en uno o varios de los nodos que han de invitarse a la sesión privada, el ARM de fichero emitirá una petición GCC-invocar-aplicación, especificando una lista de los ID de usuario GCC a invitar o bien NULL (indicando que están invitados todos los nodos de la conferencia) como parámetro de los nodos de destino. Además especificará 'privado dinámico' como canal de iniciación en la correspondiente entrada del protocolo de aplicación.

El ARM de fichero formador de la sesión esperará entonces hasta recibir una indicación GCC-aplicación-informe-registro que contenga los ID de usuario MCS de las APE de fichero que han de invitarse a la sesión privada (se recomienda establecer una temporización en el caso de que no se haya iniciado ninguna aplicación MBFT en uno o más de los nodos invitados). El ARM de fichero emitirá a continuación una petición MCS-admisión-canal para los canales de control y de datos, especificando los ID de usuario MCS de las APE de fichero invitadas como lista de ID de usuario MCS.

Si está presente el parámetro sessionID de la APE de fichero, el ARM de fichero intentará incorporar la sesión indicada mediante la emisión de una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en inactivo y especificando la clave de sesión con la ID de sesión indispensable. Seguidamente esperará hasta recibir una indicación MCS-admisión-canal del ARM de fichero correspondiente al nodo que entra a formar la sesión MBFT privada. A continuación intentará incorporar el canal indicado en esa primitiva emitiendo una petición MCS-incorporación-canal. Desde el formador de la sesión privada se recibirá una nueva indicación MCS-admisión-canal, y el ARM de fichero miembro privado deberá asimismo incorporar el canal indicado en esta primitiva mediante la emisión de una petición MCS-incorporación-canal. Para determinar cuál de los dos canales va a utilizarse como canal CONTROL-MBFT, el ARM de fichero compara ambos ID de canal con los SessionID. El ID de canal que sea igual a un ID de sesión, señalará el canal CONTROL-MBFT. El ID de canal que no coincida con un ID de sesión pero que tenga igual ID de usuario

gestor de canal, indicará el canal DATOS-MBFT correspondiente. Cuando se haya invocado a distancia un ARM de fichero miembro privado, el ID de sesión (y por tanto el ID del canal CONTROL-MBFT) se obtendrá de la indicación GCC-invocar-aplicación.

Tras la recepción de una indicación GCC-informe-registro-aplicaciones que contenga el ID de usuario de su APE de fichero, el ARM de fichero volverá a inscribirse con la bandera activo/inactivo fijada en activo, incluyendo el ID de sesión como parte de la clave de sesión y proporcionando la lista completa de capacidades de protocolos de aplicación.

Las identidades de los testigos que han de utilizarse para la sesión privada son transportadas por el ASE de fichero que accede a la sesión cuando éste inicia la primera transacción por el canal de control (es decir, en la PDU de oferta-fichero o la PDU de petición-fichero). Los miembros privados tienen individualmente acceso al Registro GCC para determinar las identidades de los testigos, si bien cabe resaltar que tal procedimiento es mucho menos eficaz. Para identificar el testigo TRANSMISIÓN-FICHERO utilizado con el canal de datos de difusión, el ARM de fichero emitirá una petición GCC-extracción-entrada-registro con los parámetros señalados en el Cuadro 4. Si el parámetro de resultado en la confirmación GCC-extracción-entrada-registro es 'entrada no hallada', solamente al formador de la sesión le será permitido ofrecer ficheros por el canal de datos de difusión. El ARM de fichero puede asimismo identificar el testigo PETICIÓN-FICHERO utilizado para el canal de control mediante la emisión de una petición GCC-extracción-entrada-registro. Si el parámetro de resultado en la confirmación GCC-extracción-entrada-registro es 'entrada no hallada', solamente al formador de la sesión le será permitido solicitar ficheros por el canal de control. Véase la Figura 9.

8.4.5 Formación de las claves de registro

Para determinar la identidad de un testigo o canal dinámico a través del registro GCC, el ARM de fichero debe formar una clave de registro que consta de la clave de sesión para la sesión MBFT vigente y de un identificador de recurso MBFT. Los identificadores de recurso se definen en los Cuadros 29 y 30 para canales y testigos, respectivamente.

8.5 Capacidades MBFT

La negociación de las capacidades asociadas con las aplicaciones de transferencia de ficheros se efectúa a través del mecanismo de inscripción de aplicaciones. Cuando un ARM de fichero emite una petición GCC-inscribir-aplicación con la bandera activo/inactivo fijada en activo, indicará las capacidades de su aplicación de usuario en el parámetro lista de capacidades de aplicación de dicha petición.

Se notifican a una APE de fichero las capacidades disponibles dentro de su sesión mediante la recepción de una indicación GCC-informe-registro-aplicaciones que contiene el registro de aplicaciones correspondiente a esa sesión. Dicho registro incluye una lista de nodos para los cuales se ha inscrito una APE de fichero par. Para cada uno de los nodos, la lista contiene su ID de usuario GCC y el/los ID de usuario MCS de la(s) APE de fichero pares en dicho nodo. El registro de aplicación posee un número de instancia y contiene banderas que indican si hay APE de fichero que se hayan incorporado a la sesión o la hayan abandonado desde que se emitió el informe-registro-aplicaciones anterior. Contiene además una bandera que indica si se ha actualizado la lista de capacidades de aplicación desde el último registro y, en caso afirmativo, la nueva lista de capacidades. Si se ha inscrito recientemente una APE de fichero, la lista de capacidades de aplicación está actualizada, ya que esta APE de fichero no tiene acceso a las instancias anteriores de la lista.

La lista de capacidades de aplicación recibida en la indicación GCC-informe-registro-aplicaciones corresponde a las listas de capacidades de aplicación colapsadas de todas las APE de fichero pares inscritas, es decir, contiene una entrada por cada capacidad de aplicación que haya sido declarada por una APE de fichero par cualquiera. Para cada entrada comprende el ID de capacidad, el número de APE de fichero pares (incluida la local) que hayan anunciado esa capacidad y, en capacidades de la clase 'mínimo no señalado', el valor mínimo del parámetro entre todas las APE de fichero pares que declararon dicha capacidad. El Cuadro 7 define los elementos de la lista de capacidades para MBFT y las reglas para colapsar cada elemento. Adviértase que ciertas capacidades se especifican como dependientes de otras capacidades. Esto significa que no debe incluirse una capacidad en la lista de capacidades del protocolo de aplicación a menos que se incluya también la capacidad de la cual depende.

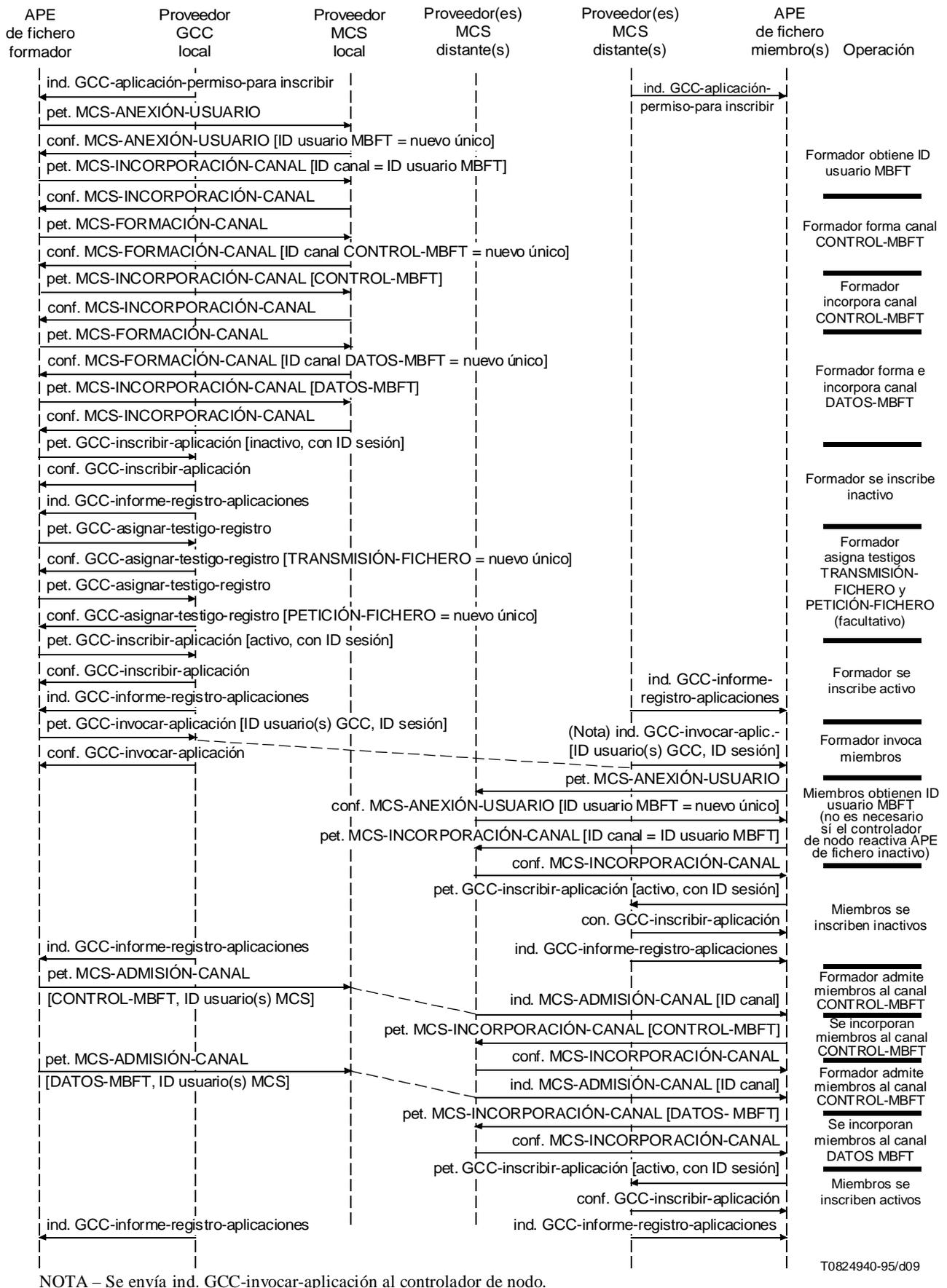


FIGURA 9/T.127

Secuencia de iniciación de protocolo de sesión privada

Mientras una APE de fichero está inscrita en una conferencia, puede en cualquier momento recibir una indicación GCC-informe-registro-aplicación suplementaria en la que se le notifique un cambio en el contenido del registro. El motivo puede ser la inscripción de nuevas APE de fichero pares en la conferencia, el abandono de dicha conferencia por algunas APE de fichero pares, o el que ciertas APE de fichero pares hayan modificado su información de inscripción.

Una APE de fichero puede en cualquier momento cambiar su lista de capacidades de aplicación inscribiéndose de nuevo. Para llevarlo a cabo, el ARM de fichero emite una petición GCC-inscribir-aplicación con la bandera inscribir/-desinscribir fijada en inscribir, incluyendo la lista de capacidades de aplicación revisada y proporcionando todos los demás parámetros tal como figuran en la inscripción en activo inicial. Esto puede dar lugar a un cambio en el conjunto de capacidades colapsado, en cuyo caso todas las APE de fichero de la sesión recibirán una indicación GCC-informe-registro-aplicación.

Ningún cambio en el conjunto de capacidades colapsado de una sesión MBFT afectará a las transacciones ya en curso. Los cambios se llevarán a efecto cuando se inicie la transacción siguiente.

8.6 Soporte de transferencias de ficheros adicionales concurrentes

Se dispone de dos mecanismos para sustentar la transmisión simultánea de varios ficheros en una conferencia:

- 1) Crear una sesión MBFT adicional por los procedimientos anteriormente definidos
- 2) Crear canales de datos con acuse de recibo dentro de la sesión MBFT existente.

Para los modos estático y multidifusión pueden utilizarse canales multidifusión o privados; para el modo privado sólo deberán emplearse canales privados. Hay que poner un especial cuidado en el uso de canales multidifusión, ya que estos canales cesan de existir cuando los abandonan todos los usuarios incorporados. Se recomienda por tanto que las APE solamente intenten utilizar un canal multidifusión si no han abandonado el canal desde su creación o desde la última transacción que tuvo lugar por él.

Cada canal de datos con acuse de recibo DATOS-MBFT(n) requiere su propio testigo TRANSMISIÓN-FICHERO(n) para gestionar las transacciones de ficheros por ese canal, a menos que el uso del mismo esté restringido a su creador.

8.6.1 Canales multidifusión

Un ARM de fichero que desee utilizar un canal de datos multidifusión con acuse de recibo debe en primer lugar emitir una petición MCS-incorporación-canal con ID canal = 0. La confirmación MCS-incorporación-canal devuelta contiene, en caso de éxito, el ID canal asignado. Si el canal de datos ha de ser un canal de datos con acuse de recibo compartido, el ARM de fichero deberá entonces emitir una petición GCC-asignar-testigo-registro con el fin de obtener un testigo TRANSMISIÓN-FICHERO(n). La clave de registro se forma siguiendo el proceso descrito en 8.4.5. Los ID de canal y testigo son transportados hacia APE de fichero pares por el canal CONTROL-MBFT cuando el creador emite una PDU oferta-fichero (para transmitir fichero) o una PDU petición-fichero (para recibir fichero) al objeto de efectuar una transacción de ficheros por el nuevo canal de datos.

8.6.2 Canales privados

Un ARM de fichero que desee utilizar un canal de datos con acuse de recibo privado compartido debe en primer lugar emitir una petición MCS-formación-canal. Si logra éxito, incorporará el canal asignado en la confirmación MCS-formación-canal emitiendo una petición MCS-incorporación-canal. El ARM de fichero debe entonces emitir una petición GCC-asignar-testigo-registro con miras a obtener un testigo TRANSMISIÓN-FICHERO(n). La clave de registro se forma utilizando el proceso descrito en 8.4.5.

Si el ARM de fichero desea utilizar un canal de datos privado exclusivo debe emitir primeramente una petición MCS-formación-canal. No necesita incorporar ese canal (puesto que nunca recibirá datos por él), ni tampoco necesita asignar un testigo.

Una vez asignados con éxito los recursos, el ARM de fichero emitirá una petición MCS-admisión-canal, en la que se especifiquen los ID de usuario MCS o las APE de fichero que han de admitirse a ese canal como ID de usuario MCS.

Las APE de fichero que sean admitidas al canal de datos privado recibirán una indicación MCS-admisión-canal, y entonces deberán intentar incorporarse al canal indicado emitiendo una petición MCS-incorporación-canal.

CUADRO 7/T.127

Elementos de la lista de capacidades de aplicación

Nombre de capacidad (valor por defecto): Descripción	ID	Clase	Regla cómputo APE	Gama del valor de capacidad	Dependencia
Volumen máximo del fichero (valor por defecto: ilimitado) Cada APE debe especificar el contenido útil máximo de datos en octetos que sea capaz de recibir.	1	Mínimo no señalado	> 0	(65536..MAX)	–
Contenido de datos máximo (valor por defecto: 8 192) Es el máximo número de octetos admitidos en el campo de datos de las PDU inicio-fichero y datos-fichero.	2	Mínimo no señalado	= ALL	(8193..65536)	–
V.42 bis-Compresión (por defecto sin compresión) Se emplea para negociar el uso de compresión V.42 bis para los datos del fichero. Las APE deben afirmar esta capacidad si son capaces de recibir datos comprimidos según V.42 bis.	3	Logical	= ALL	–	–
V.42 bis-Número-de-palabras-código (valor por defecto: 512) Especifica el número total de palabras de código a utilizar por el algoritmo de compresión V.42 bis. Es un límite superior del parámetro P1 de V.42 bis. La V.42 bis no impone límite superior a su valor.	4	Mínimo no señalado	= D	(513..65535)	V.42 bis- Compresión
V.42 bis-longitud-máx-secuencia (valor por defecto: 6) Especifica la longitud máxima de la secuencia de entrada al codificador V.42 bis. Es un límite superior del parámetro P2 de 42 bis.	5	Mínimo no señalado	= D	(7..250)	V.42 bis- Compresión
Capacidad no normalizada (por defecto: no especificada) Se utiliza para negociar funciones no normalizadas, incluyendo técnicas de compresión sin normalizar. Puede aparecer cualquier número de ellas en la lista de capacidades de aplicación, siempre que cada una tenga un identificador no normalizado exclusivo. La interpretación de estas capacidades no se define en esta Recomendación.	Identif. no normalizado	–	–	–	–
<p>Regla de cómputo APE:</p> <p>> 0 – Si el parámetro numberOfEntities (número de entidades) devuelto por la indicación GCC-informe-registro-aplicaciones para esta capacidad es mayor que cero, se establece el resultado de la operación de mínimo no señalado; en los demás casos se establece el valor por defecto de la capacidad.</p> <p>= ALL (TODOS) – El parámetro numberOfEntities devuelto por la indicación GCC-informe-registro-aplicaciones para esta capacidad debe ser igual al número de APE en activo inscritas en la sesión vigente; en los demás casos se establece el valor por defecto de la capacidad.</p> <p>= D – Si el parámetro numberOfEntities devuelto por la indicación GCC-informe-registro-aplicación para esta capacidad es igual al parámetro numberOfEntities relativo a la capacidad de la cual depende, se establece el resultado de la operación de mínimo no señalado; en los demás casos se establece el valor por defecto de la capacidad.</p>					

El ID de testigo TRANSMISIÓN-FICHERO(n) es transportado, en caso de ser aplicable, hacia APE de fichero pares por el canal CONTROL-MBFT cuando el creador emite una PDU oferta-fichero (para transmitir fichero) o una PDU petición-fichero (para recibir fichero) al objeto de efectuar una transacción de ficheros por el nuevo canal de datos.

8.7 Transferencia de ficheros selectiva

Se dispone de dos mecanismos para permitir la distribución de ficheros a un subgrupo de participantes:

- 1) Formar una nueva sesión privada
- 2) Establecer una subsesión privada dentro de la sesión MBFT existente.

El último método se describe seguidamente. Una vez establecido el trayecto de comunicación, el intercambio de ficheros sigue un proceso idéntico al del trayecto de comunicación inicial.

Un ARM de fichero que desee iniciar una transferencia de fichero privada dentro de una sesión MBFT existente debe asignar un canal de control privado y un canal de datos privado utilizando los servicios MCS. Primeramente, el ARM de fichero emite una petición MCS-formación-canal relativa al canal de control. Si logra éxito, emitirá una petición MCS-incorporación-canal, especificando el ID de canal devuelto en la confirmación MCS-formación-canal. Este proceso se repite luego para el canal de datos privado. Seguidamente el ARM de fichero formador deberá emitir una PDU invitación-incorporar-canal-privado dirigida al ID de usuario MCS de cada APE de fichero que se invite a los canales privados, en la que se especifique la identidad de los canales de control y de datos como muestra el Cuadro 8. Esta PDU indica asimismo si el modo del canal de datos es de difusión o con acuse de recibo.

El ARM de fichero invita luego a otras APE de fichero a incorporarse al canal de control emitiendo una petición MCS-admisión-canal en la que se especifica como ID de canal el canal devuelto en la indicación MCS-formación-canal y se incluye la lista de los ID de usuario MCS de las APE de fichero que serán invitadas al canal privado. El proceso se repite luego para el canal de datos privado.

CUADRO 8/T.127

PDU invitación-incorporar-canal-privado

Parámetro	Descripción
ID canal control	Identifica el canal de control privado a incorporar
ID canal datos	Identifica el canal de datos privado a incorporar
Modo	La bandera se fija en TRUE (VERDADERO) para modo difusión, FALSE (FALSO) para modo de acuse de recibo

Un ARM de fichero que recibe una PDU invitación-incorporar-canal-privado con la bandera de modo fijada en TRUE deberá intentar incorporar tanto el canal de control como el de datos indicados en la PDU en cuanto reciba las correspondientes indicaciones MCS-admisión-canal del formador de la subsesión. Seguidamente indicará si se han incorporado con éxito ambos canales mediante el envío de una PDU respuesta-incorporar-canal-privado al formador de canal, con el parámetro resultado fijado en consecuencia.

Si un ARM de fichero recibe una PDU invitación-incorporar-canal-privado con la bandera de modo fijada en FALSE, deberá intentar incorporar el canal de control indicado en la PDU en cuanto reciba la correspondiente indicación MCS-admisión-canal del formador de la subsesión. Facultativamente puede incorporar en ese momento el canal de datos con

acuse de recibo. El ARM de fichero indicará luego si se ha incorporado con éxito el canal de control enviando una PDU respuesta-incorporar-canal-privado al formador de canal, con el parámetro resultado fijado en consecuencia.

Una vez que el formador de subsesión ha recibido una PDU respuesta-incorporar-canal-privado de cada una de las APE de fichero invitadas a la subsesión, puede ya comenzar sus transacciones de ficheros. Se recomienda una temporización en el caso de que una o varias APE de fichero dejen de responder. Véase el Cuadro 9.

CUADRO 9/T.127

PDU respuesta-incorporar-canal-privado

Parámetro	Descripción
ID canal	Identifica el canal de control privado que ha sido invitada a incorporar la APE de fichero.
Resultado	Si la bandera de modo en la PDU invitación-incorporar-canal-privado correspondiente estaba fijada en TRUE, este parámetro indica si ha tenido éxito o no el intento de incorporar el canal de control privado y el canal de datos de difusión. Si la bandera de modo en la PDU invitación-incorporar-canal-privado correspondiente estaba fijada en FALSE, este parámetro indica si tuvo éxito o no el intento de incorporar el canal de control privado.

Una vez que el ARM de fichero formador ha recibido la respuesta-incorporar-canal-privado de todas las APE de fichero invitadas, puede permitir que su ASE de fichero utilice el canal. El ARM de fichero tiene que vigilar el registro de aplicaciones en caso de que alguna de las APE de fichero invitadas abandone la sesión prematuramente, y debe contar con una temporización para cuando alguna de las APE de fichero deje de emitir la PDU respuesta-incorporar-canal-privado.

El ARM de fichero formador puede obtener un testigo TRANSMISIÓN-FICHERO(n) y un testigo PETICIÓN-FICHERO(n) en cualquier momento antes de que el ASE de fichero necesite utilizar los canales privados. Esto se lleva a cabo mediante la emisión de dos peticiones GCC-asignar-testigo-registro sucesivas, que forman la clave de registro como se describe en 8.4.5.

Adviértase que la primera transacción debe ser iniciada por el gestor de canal, puesto que la identidad de los testigos a utilizar va transportada dentro de banda en la primera PDU oferta-fichero o petición-fichero.

NOTA – El ARM formador deberá actuar con precaución cuando excluya miembros de un canal de datos privado, o lo disuelva, ya que MCS puede excluir a las APE receptoras del canal antes de que se hayan entregado todas las PDU datos-fichero.

8.8 Abandono de una sesión MBFT

Cuando una aplicación desee abandonar una sesión MBFT, el ARM de fichero emitirá una petición GCC-inscribir-aplicación con la bandera inscribir/desinscribir fijada en desinscribir. No se requiere ningún otro parámetro.

Si, en algún momento, el ARM de fichero recibe una indicación GCC-informe-registro-aplicaciones que ya no esté incluida (es decir, que su ID usuario MBFT esté ausente), dicho ARM de fichero emitirá inmediatamente una petición MCS-desanexión-usuario para separarla de la conferencia especificada. En ese instante la aplicación ya no se considera inscrita en la conferencia pero puede intentar inscribirse de nuevo mediante la emisión de una petición GCC-inscribir-aplicación.

Si, en un momento cualquiera, el ARM de fichero recibe una indicación GCC-permiso-para-inscribir con la bandera concesión/revocación fijada en revocación, emitirá inmediatamente una petición MCS-desanexión-usuario para separarla de la conferencia especificada. En ese momento la aplicación ya no se considera inscrita en la conferencia y no debe intentar volver a inscribirse.

8.9 Intercambio de ficheros

Esta subcláusula considera las transacciones MBFT iniciadas por una posición emisora o una posición receptora. Las transacciones de fichero son realizadas por el elemento de servicio de aplicación transferencia de ficheros (ASE de fichero).

8.9.1 Operación invocada por el transmisor

Un ASE de fichero que desee transmitir un fichero debe primeramente tomar el testigo TRANSMISIÓN-FICHERO asociado con el canal de datos para evitar que otros ASE de fichero intenten enviar datos al canal al mismo tiempo. Si no hay ningún testigo asociado con el canal de datos, solamente el creador del canal podrá intentar enviar ficheros por él. Si el testigo estuviera en poder de otro ASE de fichero (indicando que está en curso una transferencia de fichero), el ASE de fichero que desee transmitir puede optar por esperar a que se libere el testigo o por tratar de utilizar otro canal de datos. Como alternativa, el ASE de fichero puede pedir el testigo al transmisor vigente mediante la emisión de una primitiva de petición MCS-solicitud-testigo en la que se especifique como ID testigo el ID del testigo TRANSMISIÓN-FICHERO. Un ASE de fichero que reciba una primitiva de indicación MCS-solicitud-testigo mientras está transmitiendo un fichero puede optar por hacer caso omiso de ella, o por ofrecer el testigo TRANSMISIÓN-FICHERO al ASE de fichero solicitante al final de la transferencia de fichero mediante la emisión de una petición MCS-cesión-testigo en la que se especifique el ID de usuario MCS del ASE de fichero solicitante como ID de usuario que va a recibir el testigo, y como ID testigo el ID del testigo TRANSMISIÓN-FICHERO. Al recibir una indicación MCS-cesión-testigo, el ASE de fichero solicitante emitirá una primitiva de respuesta MCS-cesión-testigo con el parámetro resultado 'rt-successful' (conseguido éxito) o 'rt-user-rejected' (rechazo por usuario), dependiendo de que el ASE de fichero todavía requiera el testigo o no. Si el resultado es 'rt-successful', el ASE de fichero puede contar con que está en posesión del testigo.

Con el testigo TRANSMISIÓN-FICHERO en su poder (o bien por ser el creador de un canal de datos con acuse de recibo exclusivo), el ASE de fichero ofrecerá el fichero a todos los receptores previstos por el canal de control emitiendo una PDU oferta-fichero. El contenido de esta PDU oferta-fichero se define en el Cuadro 10. En el caso de transferencias de ficheros por el canal de datos de difusión, la bandera 'ack' (acuse) debe fijarse en FALSE para indicar que no se requiere ningún acuse de recibo. Si las transferencias se realizan por canales de datos con acuse de recibo, la bandera ack estará fijada en TRUE, indicando que los ASE de fichero receptores deben señalar si desean o no aceptar los datos. En el parámetro 'File Header' (encabezamiento de fichero) debe transportarse información suficiente para identificar de manera inequívoca el fichero y permitir que los receptores determinen si lo necesitan. El ASE de fichero transmisor tiene la facultad de decidir si transmite todos los parámetros T.434 disponibles para ese fichero, o sólo un subconjunto de los mismos. Se recomienda incluir en la PDU oferta-fichero todos los parámetros que el transmisor considere importantes para la aplicación. Si el transmisor desea comprobar si los receptores son capaces de admitir tales parámetros, deberá utilizar un canal de datos con acuse de recibo para la transacción. El método para determinar si se necesita un fichero, es asunto a resolver localmente; la aplicación puede determinar automáticamente si un fichero está ya presente, o tal vez necesita interacción con un operador.

Los ASE de fichero que reciban una oferta-fichero con la bandera ack fijada en TRUE y que deseen recibir el fichero ofrecido, tienen que incorporarse al canal de datos indicado antes de devolver una confirmación (aceptación-fichero, Cuadro 11) al transmisor. Los ASE de fichero que no deseen recibir el fichero responden con un acuse negativo (rechazo-fichero, Cuadro 12) y no se incorporan al canal de datos. De modo similar, los ASE de fichero que no sean capaces de admitir uno o más de los parámetros incluidos en el encabezamiento del fichero deberán rechazar la oferta. Si un ASE de fichero que no necesita un cierto fichero está incorporado al canal de datos cuando recibe la oferta-fichero correspondiente, deberá abandonar el canal emitiendo una petición MCS-abandono-canal. Cuando un ASE de fichero no pueda admitir más transferencias de ficheros concurrentes, deberá demorar su respuesta hasta que la transferencia del fichero esté completa o bien emitir un rechazo-oferta. Únicamente pueden responder los ASE de fichero incluidos en la instancia de registro de aplicaciones que especifique la PDU oferta-fichero, con el fin de que el ASE de fichero transmisor sepa cuántos acuses de recibo ha de aceptar. Los ASE de fichero no incluidos en la instancia del registro de aplicaciones deben hacer caso omiso de la oferta-fichero.

Los ASE de fichero que reciban una oferta-fichero con la bandera ack fijada en FALSE deben estar preparados para recibir inmediatamente datos por el canal de datos de difusión. Si no se necesita ese fichero, el ASE de fichero puede descartar los datos que le llegan o abandonar la sesión.

CUADRO 10/T.127

PDU oferta-fichero

Parámetro	Descripción
File Header (encabezamiento de fichero)	Utiliza la estructura de encabezamiento de fichero T.434 y debe incluir información suficiente para que los receptores propuestos puedan determinar si necesitan el fichero. Se sugiere como conjunto mínimo el nombre y el tamaño del fichero.
Data Channel ID (ID canal de datos)	Identifica el canal por el que va a transmitirse el fichero
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero a lo largo de toda la operación de transferencia de fichero. Sólo tiene que ser localmente exclusivo en la APE de fichero transmisor.
Roster Instance (instancia de registro)	Número de instancia de registro de aplicaciones, tal como es devuelto en la indicación GCC-informe-registro-aplicaciones recibida más recientemente. Únicamente pueden responder a esta PDU las APE de fichero inscritas activas en el registro identificado. Se incluye este campo sólo si se fija en TRUE la bandera ack. Quizá tengan que esperar las APE de fichero a recibir la indicación de informe de registro correspondiente para poder generar una respuesta.
FILE-TRANSMIT TOKEN ID (ID testigo TRANSMISIÓN-FICHERO)	Identifica el testigo utilizado para regular la transmisión de fichero por el canal especificado en el parámetro Data Channel ID. Si se omite el testigo, entonces sólo al creador del canal de datos se le permite enviar ficheros por ese canal. Si se ha asignado un testigo TRANSMISIÓN-FICHERO al canal de datos, éste debe ser incluido.
FILE-REQUEST Token ID (ID testigo PETICIÓN-FICHERO)	Identifica el testigo utilizado para regular peticiones de ficheros. Si se omite el testigo, entonces sólo al creador del canal de control se le permite emitir las PDU petición-fichero. Si se ha asignado un testigo PETICIÓN-FICHERO al canal de control, éste debe ser incluido.
Compression Specifier (especificador de compresión)	Este campo facultativo especifica la compresión (en caso de que exista) aplicada al contenido útil de datos de las PDU inicio-fichero y datos-fichero.
Tamaño de fichero comprimido	Este parámetro facultativo expresa el número de octetos del contenido útil de datos después de aplicar la compresión.
Ack Flag (bandera ack, de acuse)	Esta bandera se fija en TRUE si el fichero va a enviarse por un canal de datos con acuse de recibo, exigiendo que todas las APE de fichero receptoras acusen recibo de la PDU oferta-fichero. Si la bandera se fija en FALSE, el fichero será transmitido por el canal de datos de difusión y no se requiere acuse de recibo.

CUADRO 11/T.127

PDU aceptación fichero

Parámetro	Descripción
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero a lo largo de toda la operación de transferencia. Su valor se obtiene de la PDU oferta-fichero.

PDU rechazo fichero

Parámetro	Descripción
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero a lo largo de toda la operación de transferencia. Su valor se obtiene de la PDU oferta-fichero.
Motivo	Se utiliza este parámetro para informar al transmisor del motivo por el cual el receptor propuesto no puede o no quiere recibir el fichero ofrecido.

Si el fichero ha de distribuirse por el canal de datos de difusión, el ASE de fichero transmisor puede comenzar a enviar el fichero por ese canal inmediatamente después de expedir la PDU oferta-fichero; si no es así, deberá esperar hasta recibir el acuse de recibo de todos los ASE de fichero incorporados al canal de control. En este último caso, el transmisor debe vigilar el registro de aplicaciones para determinar qué posiciones están actualmente conectadas, ya que algunas APE de fichero pueden haber abandonado el canal de control después de haberse emitido la PDU oferta-fichero. Se recomienda establecer una temporización para evitar el bloqueo de la aplicación por las ASE de fichero que dejen de responder. No se señalan valores de temporización en esta especificación de protocolo; deben tener la amplitud suficiente para admitir los periodos de latencia de la red y los tiempos de respuesta de los usuarios.

Los ficheros van transportados en una PDU inicio-fichero seguida de cero o más PDU datos-fichero (véanse los Cuadros 13 y 14). Adviértase que la PDU inicio-fichero contiene un encabezamiento T.434. Se incluye éste para asegurar que la estructura de fichero completa (encabezamiento más datos) es transportada como una entidad aislada, y también porque la información suministrada en la PDU oferta-fichero sólo puede ser un subconjunto del encabezamiento. La bandera EOF sirve para indicar el final del fichero.

Aunque las Recomendaciones de la serie T.120 permiten la transferencia fiable de datos, algunas aplicaciones de usuario pueden imponer requisitos adicionales para la validación de los datos mediante verificación por redundancia cíclica (CRC). La Recomendación T.127 admite la posibilidad de que los transmisores puedan facultativamente incluir la CRC con los datos del fichero. Podría ser una CRC individual incluida en la última PDU datos-fichero (o en la PDU inicio-fichero si fuera posible transportar los datos en una sola PDU), o bien una CRC acumulativa incluida en la PDU inicio-fichero y en todas las PDU datos-fichero siguientes. La presencia de una CRC se indica fijando la bandera CRC en la PDU inicio-fichero. Los receptores pueden ignorar la CRC si no lo requiere la aplicación de usuario. El método de calcular la CRC se ilustra en la Figura 10. Los octetos de datos se introducen al cálculo de CRC ordenadamente, comenzando por el bit de orden inferior.

La CRC se reinicia al comienzo de cada transferencia de fichero y se calcula a partir del contenido útil de datos de las PDU inicio-fichero y datos-fichero, utilizando la secuencia de verificación de trama de 32 bit definida en ISO/CEI 3309. Si el fichero de datos está comprimido, la CRC se aplica a los datos comprimidos y no a los datos fuente.

Si se aplica la compresión V.42 *bis* al contenido útil de datos del fichero, el codificador se inicializa al principio del fichero y efectúa el tratamiento de los octetos de la cabida útil de datos continuamente hasta el final del fichero. El codificador no se reinicia al final de cada PDU.

Al concluir la transferencia de cada fichero, los ASE de fichero deben permanecer incorporados a los canales de control y de datos con el fin de no tener que abandonar y volver a incorporarse para operaciones subsiguientes. No obstante, si un ASE de fichero está incorporado a un canal de datos con acuse de recibo y a continuación se le ofrece un fichero que no necesita, deberá abandonar el canal de datos antes de devolver un rechazo-fichero.

Cuando el nodo transmisor haya expedido la última PDU datos-fichero, deberá liberar el testigo TRANSMISIÓN-FICHERO (si estuviera presente) emitiendo una petición MCS-liberación-testigo al objeto de permitir que otras posiciones inicien transmisiones de ficheros por el canal de datos. Si el transmisor hubiera recibido previamente una MCS-solicitud-testigo durante la transferencia, podrá entonces ofrecer el testigo al ASE de fichero solicitante mediante la emisión de una petición MCS-cesión-testigo. Si se hubieran recibido indicaciones MCS-solicitud-testigo de más de un ASE de fichero, es asunto local decidir a cuál de ellas se ha de responder.

CUADRO 13/T.127

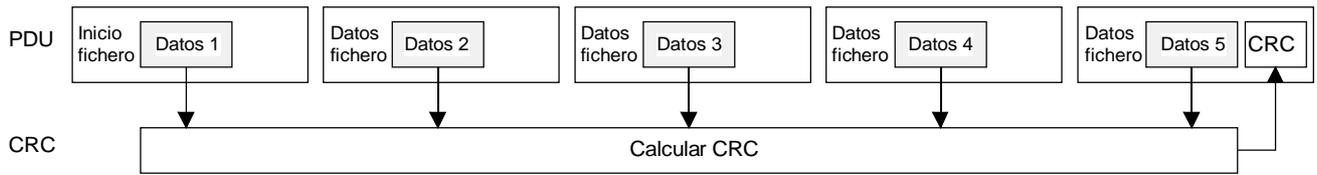
PDU inicio-fichero

Parámetro	Descripción
File Header (encabezamiento de fichero)	Este parámetro adopta la estructura del encabezamiento de fichero T.434 y debe incluir todos los campos definidos en el fichero fuente, estuvieran o no incluidos en la PDU oferta-fichero precedente.
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero a lo largo de toda la operación de transferencia. Deberá fijarse en el mismo valor que el asa de la PDU oferta-fichero correspondiente a esta transferencia.
EOF Flag (bandera EOF)	Esta bandera se fija en TRUE para indicar fin del fichero.
CRC Flag (bandera CRC)	Indica si la última PDU datos-fichero (o la PDU inicio-fichero si la bandera EOF está en TRUE) contiene una verificación de redundancia cíclica (CRC).
Compression Specifier (especificador de compresión)	Este campo facultativo especifica la compresión (en caso de que exista) aplicada al contenido útil de datos de las PDU inicio-fichero y datos-fichero.
Compressed Filesize (tamaño de fichero comprimido)	Número de octetos del fichero comprimido, excluido el encabezamiento.
Data Offset (desplazamiento de los datos)	Especifica el desplazamiento inicial en octetos desde el comienzo de los datos del fichero (cero indica el origen).
Data (datos)	El máximo número de octetos de datos del fichero binario que puede incluirse en este campo se negocia por medio del mecanismo de intercambio de capacidad.
CRC Check (Verificación CRC)	Se incluye una verificación de redundancia cíclica en la PDU inicio-fichero si la bandera CRC está fijada en TRUE y además, o se utiliza una CRC acumulativa o la bandera EOF está fijada en TRUE.

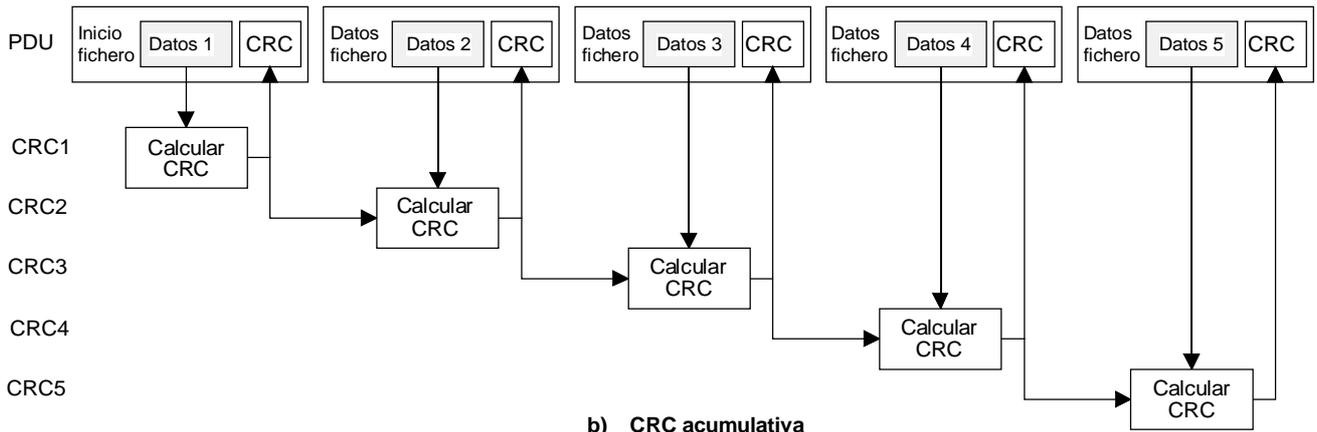
CUADRO 14/T.127

PDU datos-fichero

Parámetro	Descripción
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero a lo largo de toda la operación de transferencia. Deberá fijarse en el mismo valor que el asa de la PDU oferta-fichero correspondiente a esta transferencia.
EOF Flag (bandera EOF)	Esta bandera se fija en TRUE en la última PDU datos-fichero para indicar el fin del fichero.
Abort Flag (bandera aborto)	La bandera aborto está fijada en TRUE si la transferencia de fichero se termina anormalmente, bien como resultado de la intervención del conductor o por deseo del transmisor. En la transmisión en curso no se enviarán más PDU datos-fichero después de una PDU datos-fichero cuya bandera aborto esté fijada en TRUE.
Data (datos)	El máximo número de octetos de datos del fichero binario que puede incluirse en este campo se negocia por medio del mecanismo de intercambio de capacidad.
CRC Check (verificación CRC)	Se incluye una verificación de redundancia cíclica en la PDU datos-fichero si la bandera CRC está fijada en TRUE en el inicio-fichero correspondiente y además, o se utiliza una CRC acumulativa o la bandera EOF está fijada en TRUE.



a) CRC única enviada al final de la transferencia de fichero



b) CRC acumulativa

T0820170-95/d10

FIGURA 10/T.127
Cálculo de CRC

8.9.2 Operación invocada por el receptor

Una prestación facultativa de la MBFT es la capacidad de solicitar la transmisión de un fichero determinado (para aplicaciones de extracción de ficheros) o la retransmisión parcial de un fichero (para poder recuperarlo cuando se ha desconectado una posición durante la transferencia del fichero). La retransmisión parcial es particularmente útil cuando se interrumpe una transferencia en bloque de ficheros. Como el protocolo no exige el acuse de recibo de cada PDU datos-fichero, el ASE de fichero que emite la petición es responsable de indicar qué parte del fichero se ha recibido satisfactoriamente.

Para iniciar una petición de fichero, un ASE de fichero primeramente debe tomar el testigo PETICIÓN-FICHERO antes de emitir la PDU petición-fichero. Se asegura así que no haya más de una petición pendiente en el canal de control. Si no hubiese testigo PETICIÓN-FICHERO, solamente el creador del canal podría emitir una petición-fichero. Si el testigo está en poder de otro ASE de fichero, entonces el ASE de fichero que desee iniciar la petición-fichero podrá solicitarlo emitiendo una petición MCS-solicitud-testigo, en la que se especifique como ID testigo el ID del testigo PETICIÓN-FICHERO. El poseedor del testigo puede optar por ceder el testigo PETICIÓN-FICHERO al ASE de fichero solicitante una vez que ha determinado si puede satisfacerse su propia petición de fichero. Para llevar esto a efecto, emitirá una petición MCS-cesión-testigo en la que se especifique el ID de usuario MCS del ASE de fichero solicitante como ID de usuario que va a recibir el testigo, y como ID testigo el ID del testigo TRANSMISIÓN-FICHERO. Al recibir una indicación MCS-cesión-testigo, el ASE de fichero solicitante emitirá una primitiva de respuesta MCS-cesión-testigo con el parámetro resultado 'rt-successful' (conseguido éxito) o 'rt-user-rejected' (rechazo por usuario), dependiendo de que el ASE de fichero todavía requiera el testigo o no. Si el resultado es 'rt-successful', el ASE de fichero puede contar con que está en posesión del testigo.

El contenido de la PDU petición-fichero se define en el Cuadro 15. En la petición debe incluirse información suficiente para que los receptores de la PDU puedan determinar si son capaces de suministrar el fichero. Para la retransmisión parcial de un fichero, el ASE de fichero deberá especificar el número de octetos recibidos satisfactoriamente antes de interrumpirse la transferencia del fichero. En la PDU se incluye un «asa» (distintivo) con el fin de poder correlacionar las respuestas con la petición. La PDU debe también contener un testigo TRANSMISIÓN-FICHERO para garantizar que solamente un ASE de fichero intente atender la petición.

La PDU petición-fichero incluye la identidad del canal de datos a utilizar de manera que el ASE de fichero solicitante pueda especificar una de las opciones siguientes:

- el fichero se ha de enviar exclusivamente al solicitante por su canal de usuario MCS de APE de fichero;
- el fichero se ha de difundir a todos los ASE de fichero de la sesión por el canal de datos de difusión. En este caso, todos los ASE de fichero están obligados a recibir los datos y a desecharlos si no los necesitan;
- el fichero se ha de ofrecer a todos los ASE de fichero de la sesión por un canal de datos con acuse de recibo. En este caso, los ASE de fichero pueden elegir si desean o no recibir los datos.

Con miras a que el ASE de fichero que emitió la petición-fichero sepa cuántos acuses de recibo ha de aceptar, todos los ASE de fichero incluidos en la instancia del registro de aplicaciones especificada en la PDU petición-fichero deben responder, utilizando la PDU denegación-fichero (véase el Cuadro 16) si no pueden suministrar el fichero pedido. Los ASE de fichero que no figuren en la instancia del registro de aplicaciones especificada deben hacer caso omiso de la petición-fichero.

Un ASE de fichero que sea capaz de suministrar el fichero deberá en primer lugar tomar el testigo TRANSMISIÓN-FICHERO identificado en la PDU petición-testigo, antes de ofrecer ese fichero para su transmisión por el canal de datos indicado en la petición, utilizando la oferta-fichero como si él hubiera iniciado la transacción. Si el testigo TRANSMISIÓN-FICHERO no está libre, el ASE de fichero responderá con una denegación-fichero, señalando como motivo 'noChannel' (falta canal). El ASE de fichero solicitante puede entonces renovar su tentativa, especificando un canal de datos diferente.

Si todos los ASE de fichero responden con denegación-fichero, entonces el ASE de fichero solicitante debe abandonar el testigo PETICIÓN-FICHERO, de lo contrario el testigo se entregaría al recibir la PDU oferta-fichero correspondiente al fichero requerido. En cuanto un ASE de fichero haya satisfecho la petición enviando una oferta-fichero, todas las posiciones que todavía no hayan respondido enviarán denegación-fichero, aun cuando fueran capaces de expedir ese fichero. Cualquier ASE de fichero puede emitir peticiones ulteriores por el canal de control una vez liberado el testigo PETICIÓN-FICHERO.

El ASE de fichero solicitante debe vigilar el registro de aplicaciones para determinar de cuáles ASE de fichero debe esperar respuesta. Se recomienda utilizar una temporización para impedir que la aplicación se vea bloqueada por la falta de respuesta de algunas posiciones. Todas las respuestas que se reciban tras haber expirado la temporización pueden ser identificadas por el asa de la petición.

8.10 Listado de directorio distante

Es una prestación facultativa mediante la cual un ASE de fichero puede obtener un listado del directorio de una posición distante. Puede utilizarse conjuntamente con el mecanismo de petición-fichero para prestar un servicio de extracción de ficheros. Un ASE de fichero que necesite un listado de directorio emite una PDU petición-directorio hacia el canal usuario MBFT de la posición distante elegida, utilizando los parámetros especificados en el Cuadro 17.

Un ASE de fichero que reciba una PDU de petición de directorio responderá enviando una PDU de respuesta de directorio al canal de usuario MBFT del originador, para lo cual utilizará los parámetros definidos en el Cuadro 18. Si el ASE de fichero está apto para satisfacer la petición, incluirá una lista de los ficheros y subdirectorios contenidos en el directorio identificado en la PDU de petición de directorio. Si no está apto para proporcionar la lista, o no desea hacerlo, el ASE de fichero rechazará la petición indicando el motivo del rechazo. Obsérvese que no se requiere que la estructura de directorio presentada a posiciones distantes sea igual a la presentada localmente.

CUADRO 15/T.127

PDU petición-fichero

Parámetro	Descripción
File Header (encabezamiento de fichero)	Este parámetro adopta la estructura del encabezamiento de fichero T.434 y debe incluir información suficiente para que los transmisores puedan determinar si son capaces de cumplimentar la petición de fichero. Como subconjunto mínimo se sugiere el nombre y el tamaño del fichero.
Data Channel ID (identificador de canal de datos)	Identifica el canal por el que debe transmitirse el fichero. Puede ser el canal de datos de difusión, un canal de datos con acuse de recibo o el ID de usuario MBFT de la APE de fichero solicitante.
Request Handle (asa de la petición)	Es un distintivo exclusivo que sirve para referenciar la petición de fichero. Sólo necesita ser localmente exclusivo en la APE de fichero solicitante.
Roster Instance (instancia de registro)	Número de instancia de registro de aplicaciones, tal como es devuelto en la indicación GCC-informe-registro-aplicaciones recibida más recientemente. Únicamente necesitan responder a esta PDU las APE de fichero inscritas activas en el registro identificado. Las APE de fichero tal vez tengan que esperar a recibir esta indicación de informe del registro antes de generar una respuesta.
FILE-TRANSMIT Token ID (ID testigo TRANSMISIÓN-FICHERO)	Identifica el testigo utilizado para asegurar que no haya más de una APE de fichero que intente atender la petición de fichero. Su inclusión es obligatoria.
FILE-REQUEST Token ID (ID testigo PETICIÓN-FICHERO)	Identifica el testigo utilizado para regular la emisión de peticiones de fichero, evitando así que otros ASE de fichero necesiten consultar el registro. Si se ha omitido el testigo, solamente al creador del canal de control se le permite emitir las PDU petición-fichero. Si se hubiera asignado un testigo PETICIÓN-FICHERO al canal de control, éste deberá ser incluido.
Data Offset (desplazamiento de los datos)	Especifica el desplazamiento inicial en octetos desde el comienzo de los datos del fichero (cero indica el origen).

CUADRO 16/T.127

PDU denegación-fichero

Parámetro	Descripción
Request Handle (asa de la petición)	Es un distintivo exclusivo que sirve para referenciar la petición de fichero. Deberá fijarse en el mismo valor que tenga el asa en la PDU petición-fichero correspondiente.
Reason (motivo)	Este parámetro indica a la APE de fichero solicitante el motivo de no poder suministrar el fichero.

CUADRO 17/T.127

PDU petición-directorio

Parámetro	Descripción
Pathname (nombre de ruta de acceso)	Es el nombre completo de la ruta de acceso del directorio cuyo listado se necesita. En su ausencia, se supone que se requiere un listado del directorio designado por defecto.

PDU respuesta-directorio

Parámetro	Descripción
Result (resultado)	Indica si el ASE de fichero es capaz de atender la petición y, si así no fuera, da el motivo de la negativa.
Pathname (nombre de ruta de acceso)	Es el nombre de la ruta de acceso del directorio que se está listando. Si se omite, la lista se refiere al directorio por defecto.
Directory List (listado de directorio)	Este parámetro contiene una lista de ficheros y subdirectorios.

8.11 Comportamiento en modo conducido

El MBFT es un protocolo de aplicación consciente de la conducción, es decir, tiene dos modos de operación, uno conducido y otro no conducido, como aquí se describe. El efecto de la operación en modo conducido sobre las transacciones de fichero viene determinado por el ASE de fichero par (esto es, un ASE de fichero que participe en la misma sesión MBFT) del nodo que posee el GCC-testigo-conductor en caso de que este ASE de fichero sea capaz de asumir el papel de conductor. Cada sesión tiene su propio conductor, que es el ASE de fichero del nodo conductor que participa en dicha sesión. Si hubiera más de una APE de fichero en el nodo conductor participando en una sesión MBFT determinada, será asunto local del GCC del nodo conductor decidir cuál ASE de fichero asumirá la función conductora. Cuando el nodo conductor no tenga una APE de fichero par que sustente la función conductora, será el controlador del nodo conductor quien, por sustitución, ejerza de conductor MBFT. Es obligatorio admitir el modo conducido MBFT. Adviértase que, si bien las aplicaciones han de ser capaces de operar en modo conducido, no tienen que sustentar la función conductora de la MBFT.

Las aplicaciones se enteran de que se les asigna un conductor de conferencia GCC mediante la recepción de una indicación GCC-asignar-conductor procedente del proveedor GCC. En ésta se incluye el ID usuario GCC del nodo conductor. Las aplicaciones determinan la identidad del ASE de fichero conductor a partir del registro de aplicaciones GCC. No se admiten nuevas transacciones de ficheros (oferta-fichero o petición-fichero) después de haber entrado en el modo conducido, mientras que el conductor MBFT no conceda el permiso. Las transacciones de ficheros que se encontraran en curso al introducirse el modo conducido podrán continuar hasta su compleción, a menos que sean específicamente abortadas por medio de una PDU aborto-fichero (véase 8.12).

Los ASE de fichero del nodo conductor pueden iniciar transacciones sin ejercer ninguna nueva acción. Los ASE de fichero pares de otras posiciones deben solicitar permiso para actuar al conductor MBFT como se detalla más adelante. Adviértase que los ASE de fichero que no deseen iniciar transacciones de ficheros (esto es, los que sólo quieren recibir los ficheros que se les ofrezcan) no necesitan pedir permiso al conductor MBFT.

8.11.1 APE de fichero par presente en el nodo conductor

Los ASE de fichero pares de nodos no conductores deben solicitar permiso para iniciar transacciones de ficheros enviando una PDU petición-privilegio-MBFT (Cuadro 19) al nodo conductor, en la que se especifiquen los privilegios requeridos. Están disponibles los privilegios siguientes:

- Privilegio para originar transferencias de ficheros.
- Privilegio para pedir transferencias de ficheros.
- Privilegio para crear canales privados.
- Privilegio para utilizar prioridad media en transferencias de ficheros.
- Privilegio para emitir PDU aborto-fichero.
- Privilegio para utilizar extensiones no normalizadas.

PDU petición-privilegio- MBFT

Parámetro	Descripción
File Transfer Privilege (privilegio de transferencia de fichero)	Esta bandera indica si el ASE de fichero solicitante desea permiso para originar transferencias de ficheros.
File Request Privilege (privilegio de petición de fichero)	Esta bandera indica si el ASE de fichero solicitante desea permiso para pedir ficheros o retransmisiones.
Private Channel Privilege (privilegio de canal privado)	Esta bandera indica si el ASE de fichero solicitante desea permiso para crear canales privados.
Priority Privilege (privilegio de prioridad)	Esta bandera indica si el ASE de fichero solicitante desea permiso para enviar PDU datos-fichero de prioridad media.
Abort Privilege (privilegio de aborto)	Esta bandera indica si el ASE de fichero solicitante desea permiso para emitir PDU aborto-fichero.
Non-Standard Privilege (privilegio no normalizado)	Esta bandera indica si el ASE de fichero solicitante desea permiso para utilizar ampliaciones no normalizadas del protocolo MBFT que se hayan negociado.

Al recibir una PDU petición-privilegio-MBFT, el conductor MBFT puede responder difundiendo una PDU asignar-privilegio-MBFT por el canal de control. La PDU contiene una lista de privilegios concedidos y el ID usuario del ASE de fichero solicitante, y permite a los ASE de fichero determinar qué privilegios han sido asignados a sus ASE de fichero pares. El conductor MBFT no necesita enviar una PDU asignar-privilegio-MBFT si no desea modificar los privilegios de la aplicación solicitante. Adviértase que el conductor MBFT puede en cualquier momento revocar alguno de los privilegios concedidos, o la totalidad de ellos, mediante la emisión de una PDU asignar-privilegio-MBFT con una lista de privilegios revisada para el nodo (o nodos) que se designe. Cualquier transacción en curso podrá completarse a menos que se aborte específicamente.

Si el conductor MBFT recibe un GCC-informe-registro-aplicaciones indicando que se han añadido nuevos nodos a la lista de ASE de fichero activos, difundirá por el canal de control una PDU asignar-privilegio-MBFT en la que se especifique una lista de ASE de fichero y sus privilegios asociados (véase Cuadro 20). En esta lista sólo necesitan anotarse los nodos con uno o más privilegios asignados.

Si se produce un cambio de conductor sin abandonar el modo conducido, todos los privilegios se revocarán automáticamente y los ASE de fichero deberán solicitar su readquisición al nuevo conductor MBFT. Los ASE de fichero consultarán el registro de aplicaciones para determinar si hay un conductor MBFT nuevo para la sesión. Si no hubiera ninguno presente en el nuevo nodo conductor, los ASE de fichero deberán cesar inmediatamente todas las transacciones. En caso de haber un conductor MBFT, toda transacción que esté en curso en el momento del cambio podrá continuar salvo que sea específicamente abortada por el nuevo conductor.

A un ASE de fichero que reciba una indicación GCC-concesión-permiso-conductor con la bandera permiso fijada en TRUE se le concederán todos los privilegios MBFT. Si a continuación este ASE de fichero recibe una indicación GCC-concesión-permiso-conductor con la bandera permiso fijada en FALSE, volverá a los privilegios que le asignara el conductor MBFT.

Si el ASE de fichero recibe una indicación GCC-informe-registro-aplicación en la cual ya no está presente el conductor MBFT, todos los privilegios se revocan y los ASE de ficheros deberán cesar las transacciones inmediatamente.

PDU asignar-privilegio-MBFT

Parámetro	Descripción
Privilege List (lista de privilegios)	Contiene una lista de uno o más ID usuario MBFT y los privilegios que tienen asignados. Los privilegios se identifican a continuación.
File Transfer Privilege (privilegio de transferencia de fichero)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para originar transferencias de ficheros.
File Request Privilege (privilegio de petición de fichero)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para pedir ficheros o retransmisiones.
Private Channel Privilege (privilegio de canal privado)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para crear canales privados.
Priority Privilege (privilegio de prioridad)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para enviar PDU datos fichero de prioridad media. Si la bandera está en FALSE, solamente podrá utilizarse prioridad baja para las transferencias de ficheros.
Abort Privilege (privilegio de aborto)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para enviar PDU aborto-fichero
Non-Standard Privilege (privilegio no normalizado)	Esta bandera indica si al ASE de fichero solicitante se le ha concedido permiso para utilizar ampliaciones no normalizadas del protocolo MBFT que se hayan negociado.

8.11.2 Ausencia de APE de fichero pares en el nodo conductor

Si no existe ninguna APE de fichero par en el nodo conductor que sea capaz de asumir la función conductora, un ASE de fichero debe dirigir, a través de su controlador de nodo local, peticiones de acción al controlador del nodo conductor mediante la emisión de una primitiva de petición GCC-petición-permiso-conductor. Si el permiso se concede, entonces el ASE de fichero recibirá una indicación GCC-concesión-permiso-conductor con la bandera permiso fijada en TRUE. Esto faculta al ASE de fichero para actuar de un modo no restringido (como en el modo no conducido) hasta nueva noticia.

El permiso para actuar puede ser revocado por el nodo conductor en cualquier momento. Si el ASE de fichero recibe una indicación GCC-concesión-permiso-conductor con la bandera permiso fijada en FALSE, deberá entonces cesar todas las transacciones con efectos inmediatos. Si el ASE de fichero estuviera transmitiendo un fichero, emitirá una PDU datos-fichero final que no contenga dato alguno y con la bandera aborto fijada en TRUE, y abandonará el testigo TRANSMISIÓN-FICHERO.

Adviértase que un ASE de fichero puede recibir sin haberla solicitado una indicación GCC-concesión-permiso-conductor realizada con éxito como respuesta a una petición GCC-concesión-permiso-conductor de su propio controlador de nodo u otra entidad de protocolo de aplicación de ese nodo, o bien porque el conductor decida conceder permiso sin haber recibido una petición al respecto.

8.12 Aborto de una transferencia de fichero

Si un ASE de fichero individual no puede recibir un fichero o determina que los datos no son ya necesarios, deberá desconectarse del canal de datos o bien continuar recibiendo los datos que le llegan y desecharlos.

En el modo conducido, el conductor MBFT puede conceder permiso a los ASE de fichero para emitir PDU aborto-fichero utilizables para ordenar a un ASE de fichero transmisor que termine una transferencia de fichero. Tras recibir una PDU aborto-fichero, el transmisor está obligado a fijar en TRUE la bandera aborto de la PDU datos-fichero vigente, y seguidamente a cesar la transmisión y abandonar el testigo TRANSMISIÓN-FICHERO.

Puede valerse de este mecanismo el conductor MBFT para terminar cualquier transferencia que esté en curso al introducirse el modo conducido.

El transmisor puede dejar de transmitir por voluntad propia, sin más que fijar la bandera aborto en una PDU datos-fichero.

La PDU aborto-fichero incluye un código de motivo para informar al transmisor la causa de haber generado la petición de aborto. Puede seleccionarse la transmisión que ha de terminar por el ID canal, el ID usuario MBFT, o por el asa del fichero junto con el ID usuario MBFT. En caso de que no apareciera parámetro alguno, deberían cesar las transmisiones por todos los canales (ya sean estáticos, de multidifusión o privados). Si solamente está presente la entrada ID usuario MBFT, entonces el ASE de fichero identificado deberá cesar la transmisión por todos los canales. Si están presentes el ID usuario MBFT y el asa del fichero, deberá terminar la transacción de fichero especificada. Véase el Cuadro 21.

CUADRO 21/T.127

PDU aborto-fichero

Parámetro	Descripción
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero durante toda la operación de transferencia. Su valor se obtiene de la PDU oferta-fichero.
Data Channel ID (ID canal datos)	Identifica el canal por el cual deben cesar las transferencias de ficheros.
Transmitter User Channel ID (ID canal usuario transmisor)	Identifica el ASE de fichero al que se solicita cesar la transmisión de ficheros.
Reason (motivo)	Se utiliza para comunicar al transmisor el motivo de tener que terminar su presente operación.

8.13 Diagnóstico

Se presta soporte para el intercambio de mensajes de diagnóstico entre posiciones transmisoras y receptoras por medio de la PDU error-fichero. Esta PDU contiene tres parámetros de error: un tipo de error (que indica error permanente, error transitorio o mensaje informativo), un identificador de error y un mensaje textual facultativo. Este protocolo no define la acción a ejercer cuando se recibe una PDU error-fichero. Véase el Cuadro 22.

CUADRO 22/T.127

PDU error-fichero

Parámetro	Descripción
File Handle (asa de fichero)	Es un distintivo exclusivo que sirve para referenciar el fichero durante toda la operación de transferencia e identifica el fichero afectado. Su valor se obtiene de la PDU oferta-fichero.
Error type (tipo de error)	Este campo proporciona indicación de la gravedad del fallo. Los fallos pueden ser permanentes (haciendo fracasar todas las transacciones), transitorios (provocando el fallo de la transmisión en curso) o informativos (cuando la transacción en curso se ha completado con éxito).
Error ID (ID error)	Este parámetro es un código de fallo para identificar la naturaleza del problema.
Error Text (texto error)	Este campo opcional permite que los ASE de fichero transporten una descripción textual de la situación de fallo al ASE de fichero transmisor.

8.14 Operaciones no normalizadas

Esta PDU permite transmitir cualquier información que no esté normalizada, con lo cual las aplicaciones pueden emprender operaciones sin normalizar. El empleo de operaciones no normalizadas puede estar sujeto a la negociación de las capacidades, tampoco normalizadas, que a ellas se asocian. En cualquier momento pueden enviarse PDU no-normalizadas-MBFT, pero en el modo conducido solamente podrán enviarlas las APE de fichero a las que se les haya concedido el Non-Standard Privilege. Véase el Cuadro 23.

CUADRO 23/T.127

PDU no-normalizada-MBFT

Parámetro	Descripción
Data (datos)	Parámetro no normalizado. El uso de esta PDU no está definido en esta Recomendación.

9 Definiciones de PDU MBFT

La estructura de las PDU MBFT se especifica del modo descrito seguidamente mediante la notación ASN.1 de la Recomendación X.680. Todas las PDU MBFT se codificarán para la transmisión aplicando las reglas de codificación compactada (PER, Packed Encoding Rules) de la Recomendación X.691 en su variante BASIC ALIGNED (básica alineada). Las PDU MBFT se codifican y se colocan en el campo de datos de las primitivas MCS-envío-datos o MCS-envío-datos-uniforme. La sucesión de bits generada por la codificación ASN.1 se coloca en la OCTET STRING (cadena de octetos) utilizada por el MCS en un orden tal que, dentro de cada octeto, el bit anterior se coloca en la posición del bit más significativo y el bit posterior en la posición del bit menos significativo.

MBFT-PROTOCOL DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

```

IMPORTS          ChannelID,
                  StaticChannelID,
                  DynamicChannelID,
                  UserID,
                  TokenID,
                  StaticTokenID,
                  DynamicTokenID,
                  Key,
                  H221NonStandardIdentifier,
                  NonStandardParameter,
                  TextString

```

FROM GCC-PROTOCOL;

-- Export all symbols

-- Part 1: Message Components

Handle ::= INTEGER (0..65535) -- 16-bit value

Contents-Type-Attribute ::= CHOICE

```

{
-- See Annex B/ISO 8571-2 for more information
  document-type [0] SEQUENCE
  {
    document-type-name [1] Document-Type-Name,
    parameter [0] ISO-8571-2-Parameters OPTIONAL
    -- The actual types to be used for values of the parameter
    -- field are defined in the document-type-name.
    -- Currently, only UNSTRUCTURED TEXT and UNSTRUCTURED BINARY
    -- are supported.
  }
}

```

Document-Type-Name ::= OBJECT IDENTIFIER

ISO-8571-2-Parameters ::= SEQUENCE

```
{
    universal-class-number          [0] INTEGER OPTIONAL,
    maximum-string-length          [1] INTEGER OPTIONAL,
    string-significance             [2] INTEGER
    {variable (0), fixed (1), not-significant (2)} OPTIONAL
}
```

Entity-Reference ::= INTEGER

```
{
    no-categorisation-possible      (0),
    initiating-file-service-user     (1),
    initiating-file-protocol-machine (2),
    service-supporting-the-file-protocol-machine (3),
    responding-file-protocol-machine (4),
    responding-file-service-user     (5)
}
```

Filename-Attribute ::= SEQUENCE OF GraphicString

Access-Control-Attribute ::= CHOICE

```
{
    simple-password                [0] OCTET STRING,
    -- A simplified form of the access control syntax. Specifies
    -- one password for all types of access to the files and its attributes
    actual-values                  [1] SET OF Access-Control-Element
    -- The semantics of this attribute are described in ISO 8571-2
}
```

Access-Control-Element ::= SEQUENCE

```
{
    action-list                   [0] Access-Request,
    concurrency-access            [1] Concurrency-Access OPTIONAL,
    identity                      [2] User-Identity OPTIONAL,
    passwords                     [3] Access-Passwords OPTIONAL,
    ...
}
```

Access-Request ::= BIT STRING

```
{
    read                          (0),
    insert                        (1),
    replace                       (2),
    extend                       (3),
    erase                        (4),
    read-attribute                (5),
    change-attribute              (6),
    delete-file                   (7)
}
```

Concurrency-Access ::= SEQUENCE

```
{
    read                          [0] Concurrency-Key,
    insert                        [1] Concurrency-Key,
    replace                       [2] Concurrency-Key,
    extend                       [3] Concurrency-Key,
    erase                        [4] Concurrency-Key,
    read-attribute                [5] Concurrency-Key,
    change-attribute              [6] Concurrency-Key,
    delete-file                   [7] Concurrency-Key
}
```

Access-Passwords ::= SEQUENCE

```
{
    read-password                [0] Password,
    insert-password              [1] Password,
    replace-password             [2] Password,
    extend-password              [3] Password,
}
```

```

    erase-password                [4] Password,
    read-attribute-password       [5] Password,
    change-attribute-password     [6] Password,
    delete-password              [7] Password
}

Password ::= CHOICE
{
    graphic-string                GraphicString,
    octet-string                  OCTET STRING
}

Concurrency-Key ::= BIT STRING
{
    not-required                  (0),
    shared                        (1),
    exclusive                      (2),
    no-access                      (3)
}

Permitted-Actions-Attribute ::= BIT STRING
{
    -- Actions available
    read                          (0),
    insert                        (1),
    replace                        (2),
    extend                         (3),
    erase                          (4)
}

Private-Use-Attribute ::= SEQUENCE
{
    manufacturer-values           [0] EXTERNAL OPTIONAL
}

Protocol-Version ::= BIT STRING {version-1 (0)}

User-Identity ::= GraphicString

FileHeader ::= SEQUENCE
{
    protocol-version              [28] Protocol-Version DEFAULT {version-1}, -- T.434 Version
    filename                      [0] Filename-Attribute OPTIONAL,
    permitted-actions              [1] Permitted-Actions-Attribute OPTIONAL,
    contents-type                  [2] Contents-Type-Attribute OPTIONAL,
    -- DEFAULT {UNSTRUCTURED BINARY}
    -- not specifying this attribute implies that the data content of the file is unstructured binary
    storage-account                [3] GraphicString OPTIONAL,
    date-and-time-of-creation      [4] GeneralizedTime OPTIONAL,
    date-and-time-of-last-modification [5] GeneralizedTime OPTIONAL,
    date-and-time-of-last-read-access [6] GeneralizedTime OPTIONAL,
    -- 7 is reserved for date-and-time-of-last-attribute-modification
    identity-of-creator            [8] GraphicString OPTIONAL,
    identity-of-last-modifier      [9] GraphicString OPTIONAL,
    identity-of-last-reader       [10] GraphicString OPTIONAL,
    -- 11 is reserved for identity-of-last-attribute-modifier
    -- 12 is reserved for file-availability
    filesize                       [13] INTEGER OPTIONAL,
    future-filesize                [14] INTEGER OPTIONAL,
    access-control                  [15] Access-Control-Attribute OPTIONAL,
    -- the use of this attribute is for further study
    legal-qualifications           [16] GraphicString OPTIONAL,
    private-use                     [17] Private-Use-Attribute OPTIONAL,
    structure                       [18] OBJECT IDENTIFIER OPTIONAL,
    application-reference           [19] SEQUENCE OF GraphicString OPTIONAL,
    machine                         [20] SEQUENCE OF GraphicString OPTIONAL,
    operating-system                [21] OBJECT IDENTIFIER OPTIONAL,

```

```

recipient          [22] SEQUENCE OF GraphicString OPTIONAL,
character-set      [23] OBJECT IDENTIFIER OPTIONAL,
compression        [24] SEQUENCE OF GraphicString OPTIONAL,
-- indicates an optional compression applied to the content
-- octets of the file
environment        [25] SEQUENCE OF GraphicString OPTIONAL,
pathname           [26] SEQUENCE OF GraphicString OPTIONAL,
user-visible-string [29] SEQUENCE OF GraphicString OPTIONAL,
...
}

```

CompressionSpecifier ::= CHOICE

```

{
    v42bis-parameters          V42bis-Parameter-List,
    nonstandard-compression-parameters SET OF NonStandardParameter,
    ...
}

```

V42bis-Parameter-List ::= SEQUENCE

```

{
    p1      INTEGER (512..65535),
    p2      INTEGER (6..250),
    ...
}

```

MBFTPrivilege ::= ENUMERATED

```

{
    file-transmit-privilege      (0), -- Privilege to transmit files
    file-request-privilege      (1), -- Privilege to request files
    create-private-privilege     (2), -- Privilege to create private channels
    medium-priority-privilege    (3), -- Privilege to use medium priority for
    -- file transfers
    abort-privilege             (4), -- Privilege to issue File-AbortPDUs
    nonstandard-privilege       (5), -- Privilege to use non-standard options
    -- subject to negotiation
    ...
}

```

DirectoryEntry ::= SEQUENCE

```

{
    subdirectory-flag          BOOLEAN, -- TRUE for sub-directory entries
    -- FALSE for file entries
    attributes                  FileHeader,
    ...
}

```

ErrorType ::= ENUMERATED

```

{
    informative      (0), -- No recovery required
    transient-error  (1), -- Current transfer failed, future transfers may be OK
    permanent-error (2), -- Error occurs each time file transfer is performed
    ...
}

```

ErrorID ::= INTEGER

```

{
    no-reason              (0),
    responder-error        (1),
    system-shutdown        (2),
    bft-management-problem (3),
    bft-management-bad-account (4),
    bft-management-security-not-passed (5),
    delay-may-be-encountered (6),
    initiator-error        (7),
    subsequent-error       (8),
    temporal-insufficiency-of-resources (9),
}

```

access-request-violates-VFS-security	(10),
access-request-violates-local-security	(11),
conflicting-parameter-values	(1000),
unsupported-parameter-values	(1001),
mandatory-parameter-not-set	(1002),
unsupported-parameter	(1003),
duplicated-parameter	(1004),
illegal-parameter-type	(1005),
unsupported-parameter-types	(1006),
bft-protocol-error	(1007),
bft-protocol-error-procedure-error	(1008),
bft-protocol-error-functional-unit-error	(1009),
bft-protocol-error-corruption-error	(1010),
lower-layer-failure	(1011),
timeout	(1013),
invalid-filestore-password	(2020),
filename-not-found	(3000),
initial-attributes-not-possible	(3002),
non-existent-file	(3004),
file-already-exists	(3005),
file-cannot-be-created	(3006),
file-busy	(3012),
file-not-available	(3013),
filename-truncated	(3017),
initial-attributes-altered	(3018),
bad-account	(3019),
ambiguous-file-specification	(3024),
attribute-non-existent	(4000),
attribute-not-supported	(4003),
bad-attribute-name	(4004),
bad-attribute-value	(4005),
attribute-partially-supported	(4006),
bad-data-element-type	(5014),
operation-not-available	(5015),
operation-not-supported	(5016),
operation-inconsistent	(5017),
bad-write	(5026),
bad-read	(5027),
local-failure	(5028),
local-failure-filespace-exhausted	(5029),
local-failure-data-corrupted	(5030),
local-failure-device-failure	(5031),
future-filesize-exceeded	(5032),
future-filesize-increased	(5034)

}

-- Part 2: PDU Messages

File-OfferPDU ::= SEQUENCE

```

{
    file-header           FileHeader,
    data-channel-id      ChannelID,
    file-handle          Handle,
    roster-instance      INTEGER (0..65535) OPTIONAL,
    file-transmit-token  TokenID OPTIONAL,
    file-request-token   TokenID OPTIONAL,
    compression-specifier CompressionSpecifier OPTIONAL,
    compressed-filesize  INTEGER OPTIONAL,
    ack-flag             BOOLEAN,           -- True if acknowledgements required
    ...
}

```

File-AcceptPDU ::= SEQUENCE

```

{
    file-handle          Handle,
    ...
}

```

File-RejectPDU ::= SEQUENCE

```
{
    file-handle          Handle,
    reason               ENUMERATED
    {
        unspecified     (0),
        file-exists     (1),
        file-not-required (2),
        insufficient-resources (3),
        transfer-limit  (4),    -- maximum no. of concurrent file transfers exceeded
        compression-unsupported (5), -- algorithm identified in FileOffer not supported
        unable-to-join-channel (6),
        parameter-not-supported (7), -- at least one File Header parameter is not supported
        ...
    },
    ...
}
```

File-RequestPDU ::= SEQUENCE

```
{
    file-header          FileHeader,
    data-channel-id      ChannelID,
    request-handle       Handle,
    roster-instance     INTEGER (0..65535),
    file-transmit-token  TokenID,
    file-request-token   TokenID OPTIONAL,
    data-offset          INTEGER,
    ...
}
```

File-DenyPDU ::= SEQUENCE

```
{
    request-handle      Handle,
    reason              ENUMERATED
    {
        unspecified     (0),
        file-not-present (1),
        insufficient-privilege (2),
        file-already-offered (3),    -- File already being offered by another site
        ambiguous       (4),    -- Insufficient attributes to uniquely identify file
        no-channel      (5),    -- No data channel available to fulfil the request
        ...
    },
    ...
}
```

File-AbortPDU ::= SEQUENCE

```
{
    reason               ENUMERATED
    {
        unspecified     (0),
        bandwidth-required (1),
        tokens-required  (2),
        channels-required (3),
        priority-required (4),
        ...
    },
    data-channel-id      ChannelID OPTIONAL,
    transmitter-user-id  UserID OPTIONAL,
    file-handle          Handle OPTIONAL,
    ...
}
```

```

File-StartPDU ::= SEQUENCE
{
    file-header          FileHeader,
    file-handle          Handle,
    eof-flag             BOOLEAN,      -- True if last packet of data
    crc-flag             BOOLEAN,      -- True if CRC present
    compression-specifier CompressionSpecifier OPTIONAL,
    comp-filesize        INTEGER OPTIONAL,
    data-offset          INTEGER,
    data                 OCTET STRING (SIZE (0..65535)),
    crc-check            INTEGER (0..4294967295) OPTIONAL,
    ...
}

File-DataPDU ::= SEQUENCE
{
    file-handle          Handle,
    eof-flag             BOOLEAN,      -- True if last packet of data
    abort-flag           BOOLEAN,      -- True if file transfer is being aborted
    data                 OCTET STRING (SIZE (0..65535)),
    crc-check            INTEGER (0..4294967295) OPTIONAL,
    ...
}

Directory-RequestPDU ::= SEQUENCE
{
    pathname             SEQUENCE OF GraphicString OPTIONAL,
    ...
}

Directory-ResponsePDU ::= SEQUENCE
{
    result               ENUMERATED
    {
        unspecified      (0),
        permission-denied (1),
        function-not-supported (2),
        successful        (3),
        ...
    },
    pathname             SEQUENCE OF GraphicString OPTIONAL,
    directory-list       SEQUENCE OF DirectoryEntry,
    ...
}

MBFT-Privilege-RequestPDU ::= SEQUENCE
{
    mbft-privilege       SET OF MBFTPrivilege,
    ...
}

MBFT-Privilege-AssignPDU ::= SEQUENCE
{
    privilege-list       SET OF SEQUENCE -- One for each File APE with privileges
    {
        mbftID           UserID,
        mbft-privilege   SET OF MBFTPrivilege,
        ...
    },
    ...
}

Private-Channel-Join-InvitePDU ::= SEQUENCE
{
    control-channel-id   DynamicChannelID,
    data-channel-id      DynamicChannelID,
    mode                 BOOLEAN,      -- True if broadcast
    ...
}

```

Private-Channel-Join-ResponsePDU ::= SEQUENCE

```
{
    control-channel-id      DynamicChannelID,
    result                  ENUMERATED
    {
        unspecified        (0),
        unable-to-join-channel (1),
        invitation-rejected (2),
        successful          (3),
        ...
    },
    ...
}
```

File-ErrorPDU ::= SEQUENCE

```
{
    file-handle            Handle OPTIONAL,
    error-type             ErrorType,
    error-id               ErrorID,
    error-text             TextString OPTIONAL,
    ...
}
```

MBFT-NonStandardPDU ::= SEQUENCE

```
{
    data      NonStandardParameter,
    ...
}
```

-- Part 3: Messages sent using MCS-Send-Data or MCS-Uniform-Send-Data

MBFTPDU ::= CHOICE

```
{
    file-OfferPDU           File-OfferPDU,
    file-AcceptPDU         File-AcceptPDU,
    file-RejectPDU         File-RejectPDU,
    file-RequestPDU        File-RequestPDU,
    file-DenyPDU           File-DenyPDU,
    file-ErrorPDU          File-ErrorPDU,
    file-AbortPDU          File-AbortPDU,
    file-StartPDU          File-StartPDU,
    file-DataPDU           File-DataPDU,
    directory-RequestPDU   Directory-RequestPDU,
    directory-ResponsePDU Directory-ResponsePDU,
    mbft-Privilege-RequestPDU MBFT-Privilege-RequestPDU,
    mbft-Privilege-AssignPDU MBFT-Privilege-AssignPDU,
    mbft-NonStandardPDU   MBFT-NonStandardPDU,
    private-Channel-Join-InvitePDU Private-Channel-Join-InvitePDU,
    private-Channel-Join-ResponsePDU Private-Channel-Join-ResponsePDU,
    ...
}
```

END

10 Uso del servicio de comunicación multipunto

Todas las comunicaciones MBFT se verificarán a través del MCS, según se especifica en la Recomendación T.122. En esta cláusula se detalla el uso específico de los servicios MCS, la atribución de canales, atribución de testigos y prioridades de los datos. Los testigos y canales estáticos asignados a la MBFT se establecen en la Recomendación T.120.

10.1 Uso de los servicios de transmisión de datos MCS

Puede utilizarse la primitiva envío-datos o la de envío-datos-uniforme, a discreción del transmisor. Los receptores deben ser capaces de aceptar ambos tipos de datos. En el Cuadro 25 se definen el canal y la prioridad a utilizar en cada PDU.

10.2 Atribución de canales

En cada sesión MBFT, se proporcionan dos canales para permitir la difusión de un fichero a la vez. El canal de control CONTROL-MBFT se emplea para gestionar todos los aspectos de la transferencia del fichero, la cual se realiza por el canal de datos de difusión DATOS-MBFT. Cada una de las APE de fichero se incorpora al canal ID-usuario que le ha atribuido el MCS. La transferencia simultánea de varios ficheros dentro de la misma sesión requiere utilizar canales de datos con acuse de recibo [designados por DATOS MBFT(n), siendo n el ID canal MCS del canal de datos], uno por cada transferencia de fichero concurrente. La manera de determinar los valores de ID canal para los canales CONTROL-MBFT y DATOS-MBFT depende del modo de operación de la sesión en cuestión (estático, multidifusión o privado), según se explica en 8.4.5. El método de determinación de los ID canal para DATOS-MBFT(n) depende de que se utilicen canales multidifusión o privados y se describe en 8.6.1 y 8.6.2, respectivamente.

Una subsesión dispone de un canal de control CONTROL-MBFT(p) (siendo p el ID canal MCS del canal de control). Facultativamente puede tener un único canal de datos de difusión DATOS-MBFT(p) (siendo p el ID canal MCS del canal de datos) y cero o más canales de datos con acuse de recibo DATOS-MBFT(n). Los valores de ID canal para CONTROL-MBFT(p) y DATOS-MBFT(p) se determinan siguiendo el proceso descrito en 8.7. Véase el Cuadro 24.

CUADRO 24/T.127

Descripción de canales MBFT

Nemónico	Descripción
CONTROL-MBFT	Canal de control para la comunicación de información de gestión del intercambio de ficheros entre todas las APE de fichero participantes en una sesión. Las APE de fichero deben incorporarse y mantenerse incorporadas a este canal durante toda la sesión.
DATOS-MBFT	Canal de datos de difusión para la distribución de los datos del fichero a todas las APE de fichero participantes en una sesión. Las APE de fichero deben incorporarse y mantenerse incorporadas a este canal durante toda la sesión.
CONTROL-MBFT(p) [ejemplo: CONTROL-MBFT(1001)]	Canal de control privado cuyo ID canal MCS es p. Se utiliza para la comunicación de información de gestión del intercambio de ficheros entre todas las APE de fichero participantes en una subsesión. Las APE de fichero deben incorporarse y mantenerse incorporadas a este canal durante toda la subsesión.
DATOS-MBFT(p) [ejemplo: DATOS-MBFT(1002)]	Canal de datos de difusión privado cuyo ID canal MCS es (p). Se utiliza para la distribución de datos del fichero a todas las APE de fichero participantes en una subsesión. La presencia del canal de datos de difusión dentro de una subsesión queda a discreción del formador de la subsesión. Si está presente, las APE de fichero deben incorporarse y mantenerse incorporadas a este canal durante toda la subsesión.
DATOS-MBFT(n) [ejemplo: DATOS-MBFT(1003)]	Canal de datos con acuse de recibo cuyo ID canal MCS es n. Este canal se utiliza para la distribución de los datos del fichero a las APE de fichero participantes en una sesión o subsesión. Las APE de fichero sólo tienen que incorporarse al canal para recibir los ficheros que necesiten.
Canal ID usuario MBFT	Para la comunicación desde cualquier APE de fichero de una conferencia a una APE de fichero específica de un determinado nodo. Cada APE de fichero viene identificada por su ID usuario MCS.

Utilización de canales MBFT

PDU MBFT	Canal	Prioridad
PDU oferta-fichero	CONTROL-MBFT CONTROL-MBFT(p)	Alta
PDU aceptación-fichero	ID usuario MBFT	Alta
PDU rechazo-fichero	ID usuario MBFT	Alta
PDU petición-fichero	CONTROL-MBFT CONTROL-MBFT(p)	Alta
PDU denegación-fichero	ID usuario MBFT	Alta
PDU error-fichero	ID usuario MBFT	Alta
PDU aborto-fichero	CONTROL-MBFT CONTROL-MBFT(p)	Alta
PDU datos-fichero	DATOS-MBFT DATOS-MBFT(p) DATOS-MBFT(n) ID usuario MBFT	Media, baja
PDU inicio-fichero	DATOS-MBFT DATOS-MBFT(p) DATOS-MBFT(n) ID usuario MBFT	Media, baja
PDU petición-directorio	ID usuario MBFT	Alta
PDU respuesta-directorio	ID usuario MBFT	Alta
PDU petición-privilegio-MBFT	ID usuario MBFT conductor	Alta
PDU asignar-privilegio-MBFT	CONTROL-MBFT CONTROL-MBFT(p)	Alta
PDU invitación-incorporar-canal-privado	ID usuario MBFT	Alta
PDU respuesta-incorporar-canal-privado	ID usuario gestor de canal	Alta
PDU no-normalizada-MBFT	No especificado	No especificada

10.3 Atribución de testigos

La MBFT reserva dos testigos estáticos para uso exclusivo en el modo estático: TRANSMISIÓN-FICHERO y PETICIÓN-FICHERO. Los equivalentes dinámicos de estos testigos pueden utilizarse en los modos de multidifusión y privado.

El canal de difusión de datos de la sesión puede poseer un testigo TRANSMISIÓN-FICHERO para asegurar que en ningún momento haya más de un nodo que transmite datos por el canal. Un ASE de fichero que intente transmitir un fichero deberá tomar ese testigo antes de ofrecer el fichero a los demás participantes mediante la PDU oferta-fichero. Una vez completada la transmisión del fichero (es decir, enviada una PDU inicio-fichero o PDU datos-fichero con la bandera EOF fijada en TRUE), el transmisor deberá liberar el testigo TRANSMISIÓN-FICHERO para permitir a otros nodos la transmisión por el canal de datos.

El canal de control de la sesión puede poseer un testigo PETICIÓN-FICHERO para asegurar que en ningún momento haya más de una petición de fichero pendiente de ser procesada. Un ASE de fichero que solicite un fichero deberá tomar dicho testigo antes de emitir una PDU petición-fichero. Retendrá en su poder el testigo hasta que pueda determinar si otro ASE de fichero es capaz de atender esta petición, esto es, si algún ASE de fichero responde con una oferta-fichero, o todos los ASE de fichero responden con denegación-fichero, o expira una temporización. Una vez liberado el testigo, otros ASE de fichero pueden intentar solicitar ficheros por el mismo procedimiento.

Cada canal de datos con acuse de recibo puede llevar asociado un testigo TRANSMISIÓN-FICHERO. Al testigo TRANSMISIÓN-FICHERO asociado con un canal de datos con acuse de recibo cuyo ID canal MCS es n [DATOS-MBFT(n)] se le asigna el nemónico TRANSMISIÓN-FICHERO(n) [por ejemplo, TRANSMISIÓN-FICHERO(1006)]. Funcionalmente es idéntico al testigo TRANSMISIÓN-FICHERO asociado al canal de datos de difusión.

Una subsesión posee facultativamente un testigo PETICIÓN-FICHERO(p) asociado con su canal de control CONTROL-MBFT(p). El testigo PETICIÓN-FICHERO(p) es funcionalmente idéntico al testigo PETICIÓN-FICHERO. Si la subsesión tiene un canal de datos de difusión DATOS-MBFT(p), éste puede, como opción, llevar asociado un testigo TRANSMISIÓN-FICHERO(p). Véase el Cuadro 26.

CUADRO 26/T.127

Descripción de testigos MBFT

Nemónico	Descripción
PETICIÓN-FICHERO	Testigo para asegurar que no haya más de una petición de fichero pendiente en el canal de control de la sesión CONTROL-MBFT.
TRANSMISIÓN-FICHERO	Testigo que asegura la transmisión de un fichero cada vez por el canal de datos de difusión de la sesión DATOS-MBFT.
PETICIÓN-FICHERO(p) [ejemplo: PETICIÓN-FICHERO(1001)]	Testigo para asegurar que no haya más de una petición de fichero pendiente en el canal de control de la subsesión CONTROL-MBFT(p).
TRANSMISIÓN-FICHERO(p) [ejemplo: TRANSMISIÓN-FICHERO(1002)]	Testigo que asegura la transmisión de un fichero cada vez por el canal de datos de difusión de la subsesión DATOS-MBFT(p).
TRANSMISIÓN-FICHERO(n) [ejemplo: TRANSMISIÓN-FICHERO(1003)]	Testigo que asegura la transmisión de un fichero cada vez por el canal de datos con acuse de recibo DATOS-MBFT(n).

10.4 Servicios MCS

La MBFT asume los servicios MCS enumerados en el Cuadro 27. Todas las primitivas señaladas con «M» son obligatorias, y las marcadas con «O», facultativas.

11 Uso del control de conferencia genérico

La MBFT asume los servicios enumerados en el Cuadro 28. Las primitivas señaladas con «M» son obligatorias, y las marcadas con «O», facultativas.

11.1 Identificadores de recurso

Los Cuadros 29 y 30 definen la construcción de los ID recurso MBFT necesarios para el uso del Registro GCC. No se requiere el registro para el canal CONTROL-MBFT de la sesión puesto que el ID canal MCS puede obtenerse directamente del ID sesión. Tampoco se necesita para los canales CONTROL-MBFT(p) de la subsesión privada, dado que el ID canal CONTROL-MBFT(p) es transportado a los participantes elegidos por el formador de la subsesión privada. El registro puede ser utilizado para identificar el canal de datos de difusión de la sesión mediante el ID recurso «D0». Los canales de datos de multidifusión con acuse de recibo no están incluidos en el registro, ya que la presencia de

una entrada en dicho registro no garantiza la existencia del canal (véase 8.6.2). Los canales de datos privados tampoco se incluyen en el registro, puesto que no se permite a los ASE de fichero incorporarse a estos canales hasta que no reciben una MCS-admisión-canal del formador de canales.

CUADRO 27/T.127

Servicios MCS utilizados por la MBFT

Primitivas	Uso
petición MCS-anexión-usuario	M
confirmación MCS-anexión-usuario	M
petición MCS-desanexión-usuario	M
indicación MCS-desanexión-usuario	M
petición MCS-incorporación-canal	M
confirmación MCS-incorporación-canal	M
petición MCS-abandono-canal	M
indicación MCS-abandono-canal	M
petición MCS-formación-canal	O
confirmación MCS-formación-canal	O
petición MCS-disolución-canal	O
indicación MCS-disolución-canal	M
petición MCS-admisión-canal	O
indicación MCS-admisión-canal	M
petición MCS-exclusión-canal	O
indicación MCS-exclusión-canal	M
petición MCS-envío-datos	M
indicación MCS-envío-datos	M
petición MCS-envío-datos-uniforme	M
indicación MCS-envío-datos-uniforme	M
petición MCS-toma-testigo	M
confirmación MCS-toma-testigo	M
petición MCS-cesión-testigo	O
indicación MCS-cesión-testigo	M
respuesta MCS-cesión-testigo	M
confirmación MCS-cesión-testigo	O
petición MCS-solicitud-testigo	O
indicación MCS-solicitud-testigo	M
petición MCS-liberación-testigo	O
confirmación MCS-liberación-testigo	O
indicación MCS-liberación-testigo	M
petición MCS-prueba-testigo	O
confirmación MCS-prueba-testigo	O

CUADRO 28/T.127

Primitivas GCC soportadas por la MBFT

Primitiva GCC	Uso
indicación GCC-permiso-para-inscribir	M
petición GCC-inscribir-aplicación confirmación GCC-inscribir-aplicación	M M
indicación GCC-informe-registro-aplicaciones	M
petición GCC-extracción-entrada-registro confirmación GCC-extracción-entrada-registro	O O
petición GCC-registrar-canal-registro confirmación GCC-registrar-canal-registro	O O
petición GCC-asignar-testigo-registro confirmación GCC-asignar-testigo-registro	O O
indicación GCC-asignar-conductor	M
indicación GCC-liberación-conductor	M
petición GCC-petición-permiso-conductor	O
petición GCC-concesión-permiso-conductor indicación GCC-concesión-permiso-conductor	O M

Los ID testigo TRANSMISIÓN-FICHERO(n) y TRANSMISIÓN FICHERO(p) se construyen expresando el ID canal MCS de los canales DATOS-MBFT(n) o DATOS-MBFT(p) asociados por una sucesión numérica decimal que no principie por cero y precedida de un único carácter «T», y codificando estos caracteres en octetos sucesivos de acuerdo con la Recomendación T.50. Los ID testigo PETICIÓN-FICHERO(p) se construyen expresando el ID canal MCS del canal CONTROL-MBFT asociado por una sucesión numérica decimal no iniciada en cero y precedida de un único carácter «R», y codificando estos caracteres en octetos sucesivos de acuerdo con la Recomendación T.50.

CUADRO 29/T.127

Determinación de canal

Nemónico	ID canal de canales estáticos	ID recurso de registro de aplicaciones para canales dinámicos
CONTROL-MBFT	MBFT-CANAL-0	–
DATOS-MBFT	MBFT-CANAL-1	D0
CONTROL-MBFT(p)	–	–
DATOS-MBFT(p)	–	–
DATOS-MBFT(n)	–	–

CUADRO 30/T.127

Determinación de testigo

Nemónico	ID testigo de testigos estáticos	ID recurso de registro de aplicaciones para testigos dinámicos
PETICIÓN-FICHERO	MBFT-TESTIGO-0	R0
TRANSMISIÓN-FICHERO	MBFT-TESTIGO-1	T0
PETICIÓN-FICHERO(p)	-	Rp (ejemplo: R1001)
TRANSMISIÓN-FICHERO(p)	-	Tp (ejemplo: T1002)
TRANSMISIÓN-FICHERO(n)	-	Tn (ejemplo: T1003)

Anexo A

Asignación de testigos y canales estáticos

(Este anexo es parte integrante de la presente Recomendación)

La asignación de recursos estáticos (canales y testigos) se definirá en la Recomendación T.120, pero se incluye en esta Recomendación en espera de que la Recomendación T.120 sea completada. Véanse los Cuadros A.1 y A.2.

CUADRO A.1/T.127

Asignaciones de ID canal estático

Nombre simbólico	ID canal MCS
MBFT-CANAL-0	9
MBFT-CANAL-1	10

CUADRO A.2/T.127

Asignaciones de ID testigo estático

Nombre simbólico	ID testigo MCS
MBFT-TESTIGO-0	10
MBFT-TESTIGO-1	11

Anexo B

Asignaciones de identificadores de objeto

(Este anexo es parte integrante de la presente Recomendación)

El Cuadro B.1 indica la asignación de identificadores de objeto definidos para uso en la presente Recomendación.

CUADRO B.1/T.127

Asignación de identificadores de objeto T.127

Valor de identificador de objeto	Descripción
{recomendación uit-t 127 versión(0)1}	Este identificador de objeto se utiliza para indicar la versión de esta Recomendación. En este momento existe una sola versión normalizada definida.

Apéndice I

Ejemplos de transferencia de ficheros

(Este apéndice no es parte integrante de la presente Recomendación)

I.1 Seguidamente se presentan una serie de ejemplos de transacciones de ficheros para ilustrar el empleo de esta Recomendación en diferentes situaciones.

En las Figuras se adoptan los convenios siguientes:

Cada PDU va seguida de un nombre de canal encerrado entre paréntesis, (), el cual indica el canal por el que se va a enviar la PDU. Cuando sea oportuno, se añaden parámetros PDU significativos entre paréntesis después del ID canal.

Con carácter facultativo, las primitivas van seguidas de parámetros esenciales encerrados entre corchetes, [].

Adviértase que las figuras solamente representan las transacciones entre una APE de fichero, sus APE pares y sus proveedores MCS y GCC locales. Por motivos de claridad se omiten las transacciones entre los proveedores locales MCS y GCC y los proveedores MCS y GCC superiores.

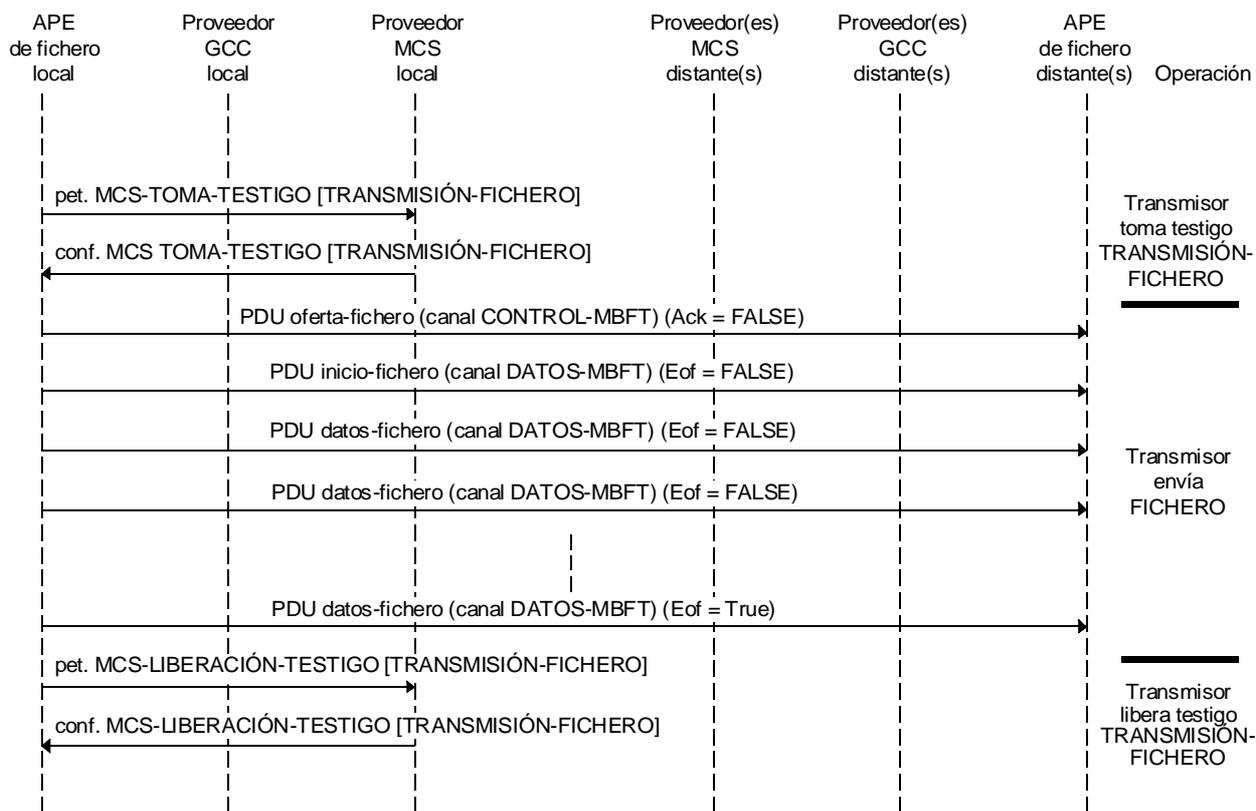
I.1.1 La Figura I.1 ilustra la distribución de un fichero por el canal de datos de difusión. Todas las APE de fichero que participan en la sesión están obligadas a recibir los datos y desecharlos si localmente no se necesitan.

I.1.2 La Figura I.2 describe la creación y el uso de un canal de datos de multidifusión con acuse de recibo cuando al menos un nodo desea recibir el fichero que se le ofrece.

I.1.3 La Figura I.3 ilustra una tentativa de distribuir un fichero por un canal con acuse de recibo, que se aborta porque todos los receptores rechazan ese fichero. Se supone que existen ya el canal de datos y el testigo TRANSMISIÓN-FICHERO(n) asociado.

I.1.4 La Figura I.4 escenifica la distribución de ficheros a un subconjunto de participantes en la sesión vigente, mediante el uso de una subsesión privada. Los participantes tienen la facultad de rechazar los ficheros que se les ofrecen, y cualquier posición puede intentar pedir u ofrecer ficheros cuando la transacción en curso haya acabado.

I.1.5 La Figura I.5 escenifica la distribución de ficheros a un subconjunto de participantes en la sesión vigente, mediante el uso de una subsesión privada. Los participantes tienen la facultad de rechazar los ficheros que se les ofrecen, pero sólo al creador se le permite transmitir ficheros. Adviértase que el creador no necesita incorporarse al canal DATOS-MBFT(n) ya que nunca va a recibir ficheros.



T0820180-95/d11

FIGURA I.1/T.127
Difusión de ficheros

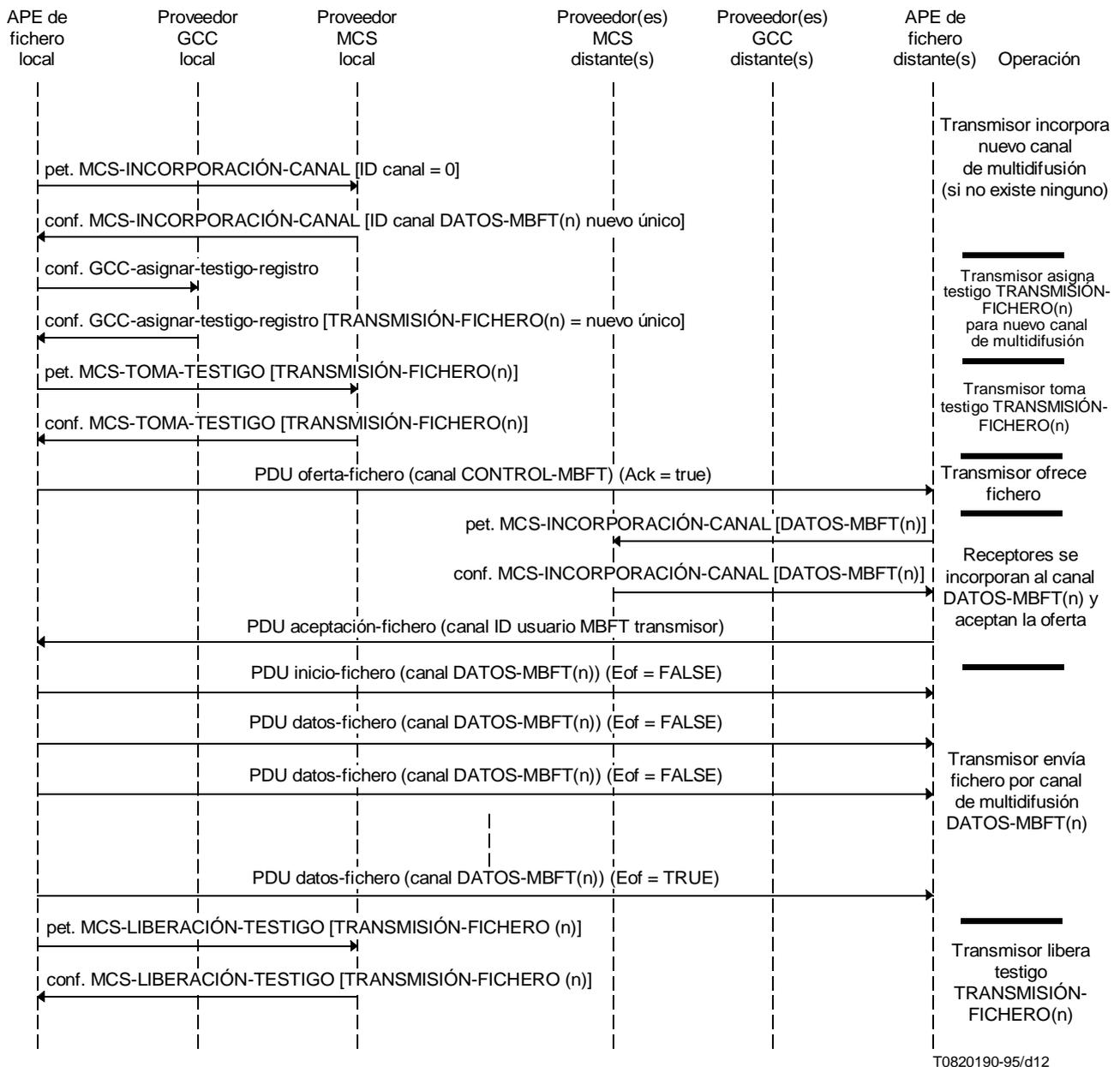
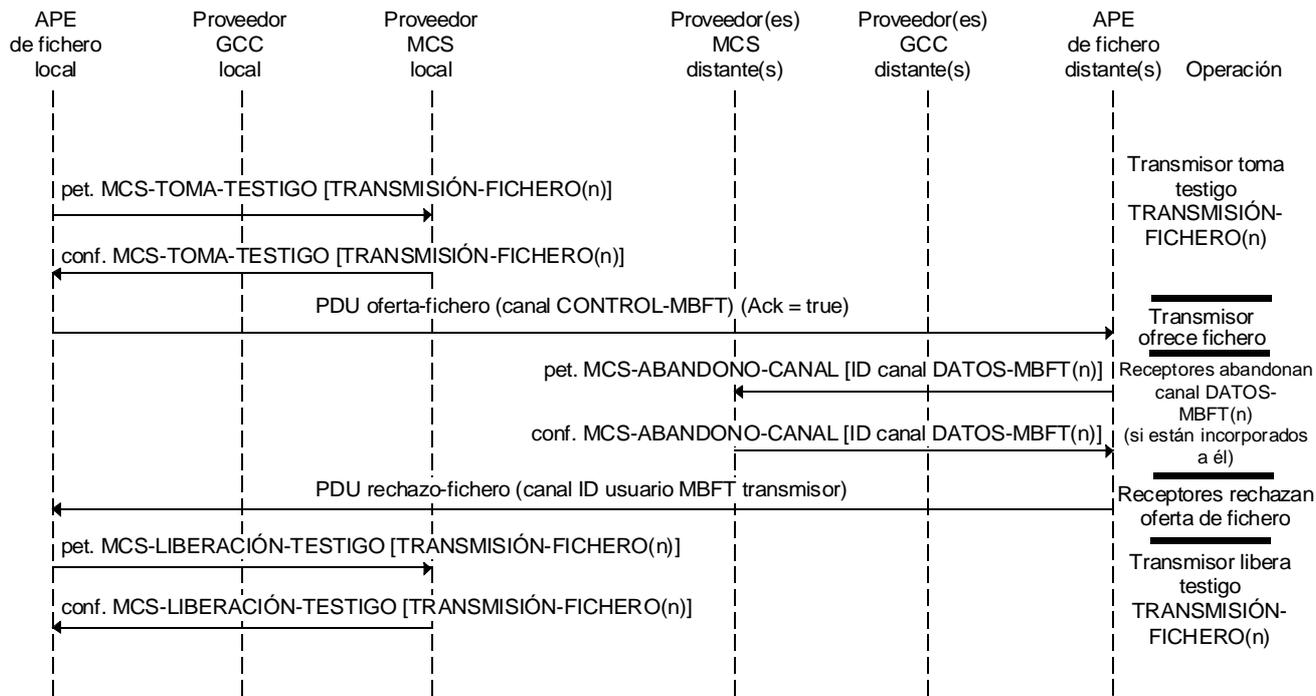


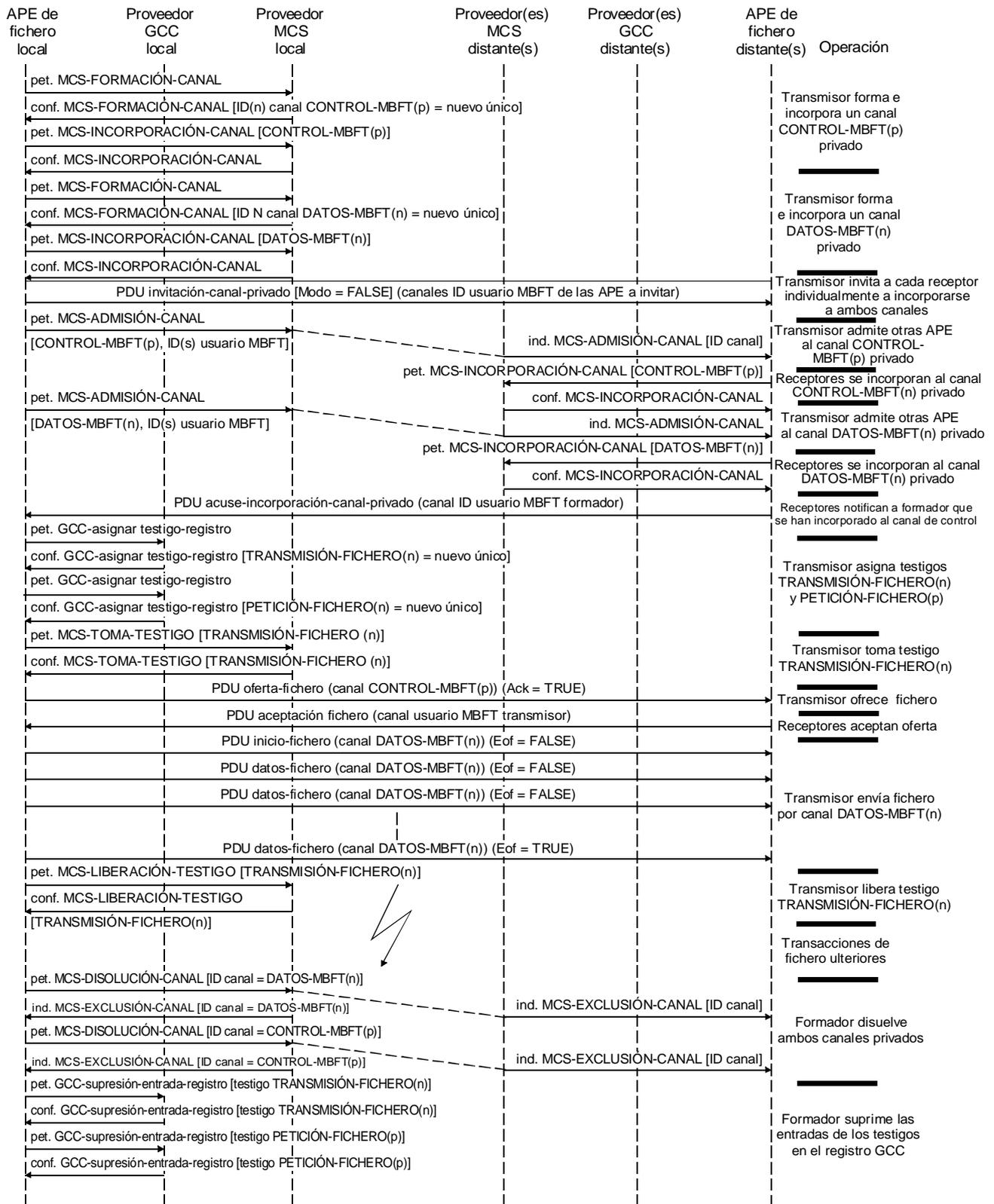
FIGURA I.2/T.127
Transferencia de fichero con acuse de recibo lograda



T0820200-95/d13

FIGURA I.3/T.127

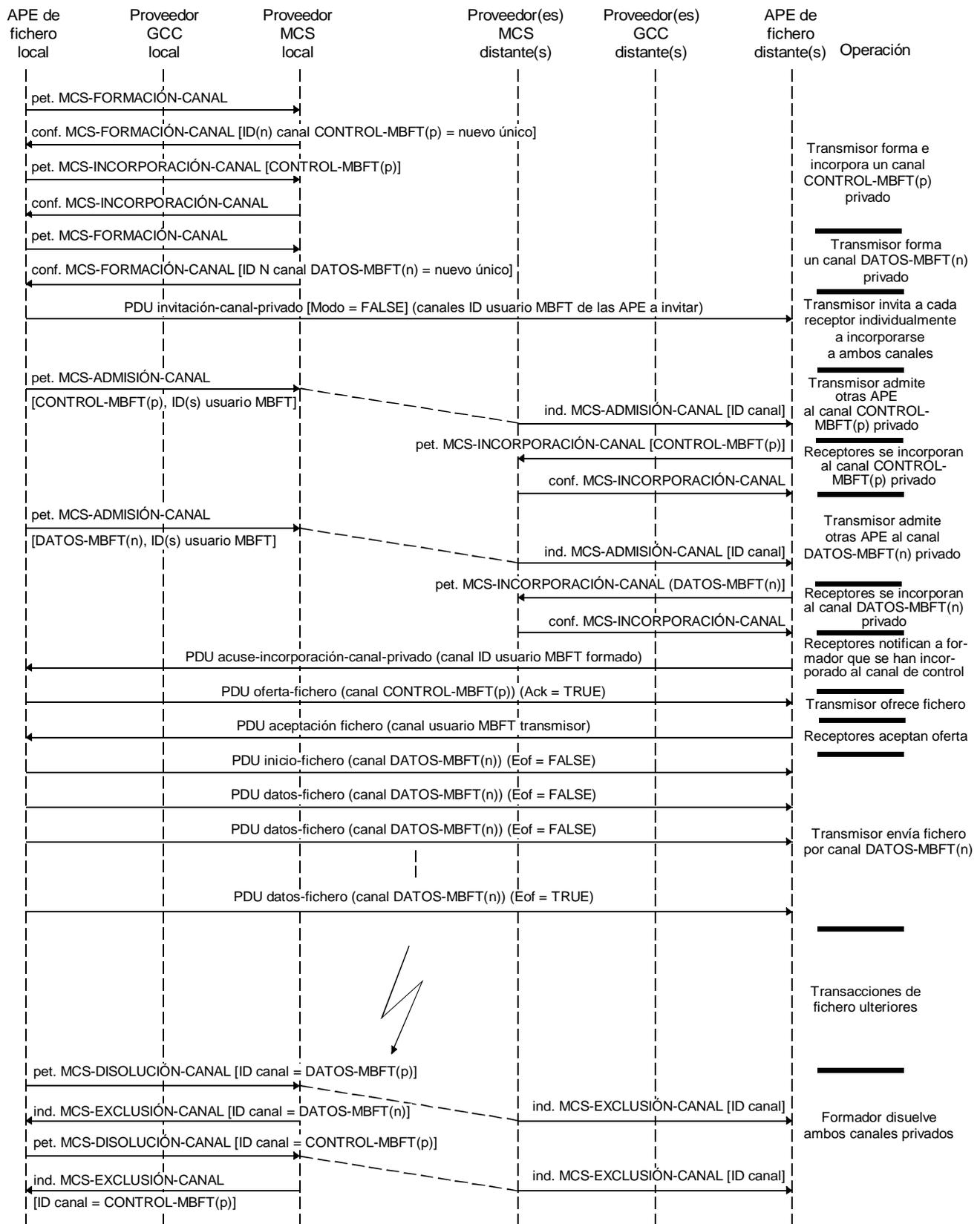
Transferencia de fichero con acuse de recibo rechazada



T0820210-95/d14

FIGURA I.4/T.127

Transferencia de fichero en subsesión privada por canal de datos con acuse de recibo



T0820220-95/d15

FIGURA I.5/T.127

Transferencia de fichero en subsesión privada por canal de datos con acuse de recibo (únicamente para uso del formador)

Apéndice II

Atributos MBFT

(Este apéndice no es parte integrante de la presente Recomendación)

Puede emplearse un gran número de parámetros para describir por completo un fichero y sus propiedades, como se detalla en Cuadro II.1. La PDU oferta-fichero debe contener información suficiente para que una posición pueda determinar si necesita un fichero y si es capaz de recibirlo; el nombre y el tamaño del fichero se sugieren pues como conjunto mínimo, pero ningún parámetro es obligatorio. Si la información suministrada fuera insuficiente (o nula) y las posiciones descubrieran en consecuencia que no deseaban, o no podían, seguir recibiendo un fichero, deberán desconectarse del canal de datos o desechar los datos que les llegan.

Las PDU inicio-fichero y datos-fichero se utilizan para transportar la estructura entera del fichero, incluida la información del encabezamiento. Adviértase que esto puede duplicar o complementar la información contenida en la PDU oferta-fichero.

Los atributos del fichero se deducen de la Recomendación T.434.

CUADRO II.1/T.127

Atributos de ficheros en MBFT

Atributo	Comentarios
Nombre fichero	Sucesión de componentes, cuyo primer elemento es el nombre del fichero y todos los siguientes están concatenados para representar el prefijo del fichero
Fecha y hora última modificación	Expresado en «tiempo generalizado»
Compresión	Sólo aplicable a datos del fichero
Tamaño fichero	Tamaño en octetos del fichero completo
Versión protocolo	Número de versión del protocolo T.434
Acciones permitidas	Leer, insertar, sustituir, ampliar, borrar
Tipo contenido	Texto sin estructurar, binario sin estructurar
Responsable almacenamiento	Identifica la autoridad responsable de los cargos por almacenamiento de ficheros
Fecha y hora creación	Expresado en «tiempo generalizado»
Fecha y hora último acceso lectura	Expresado en «tiempo generalizado»
Identidad de creador	
Identidad de último modificador	
Identificador de último lector	
Tamaño fichero futuro	Máximo tamaño del fichero en octetos
Control acceso	Para estudio ulterior
Cualificaciones legales	Refleja la situación legal del fichero
Uso privado	Permite la definición de atributos de propiedad reservada
Estructura	Indica el formato de los datos que se transfieren
Referencia aplicación	Información suplementaria que describe diversos aspectos del entorno desde el cual se origina la transferencia del fichero binario
Máquina	
Sistema operativo	
Entorno	
Nombre ruta de acceso	
Sucesión visible al usuario	
Receptor	Usuario final al que se destina la transferencia del fichero binario
Juego de caracteres	Identifica el juego de caracteres internacionales que va a utilizarse