UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T G.965

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/95)

SECCIONES DIGITALES Y SISTEMAS DE LÍNEA DIGITALES

INTERFACES V EN LA CENTRAL LOCAL DIGITAL – INTERFAZ V5.2 (BASADA EN 2048 kbit/s) PARA SOPORTAR LA RED DE ACCESO

Recomendación UIT-T G.965

(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.° 1 de la CMNT (Helsinki, 1 al 12 de marzo de 1993).

La Recomendación UIT-T G.965 ha sido preparada por la Comisión de Estudio 13 (1993-1996) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 19 de marzo 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 1995

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

ÍNDICE

Página

Página

Página

Página

Página

RESUMEN

La presente Recomendación define una interfaz V (V5.2) para la conexión de una red de acceso (AN, *access network*) y la central local (LE, *local exchange*) con el fin de soportar los siguientes tipos de acceso:

- acceso telefónico analógico;
- acceso básico RDSI con una terminación de red (NT1) separada de la red de acceso, o integrada en dicha red, basado en las Recomendaciones G.960 e I.430;
- acceso a velocidad primaria RDSI con una NT1 separada de la AN, o integrada en la AN, basado en las Recomendaciones G.962 e I.431;
- otros accesos analógicos o digitales para conexiones semipermanentes sin información de señalización fuera de banda asociada,

con asignación flexible de canal de información (canal portador) mediante la utilización de un protocolo de conexión de canal portador que proporciona la capacidad de concentración en la AN.

Esta Recomendación se basa en la Recomendación G.964 y se refiere a ella para las partes comunes a ambas Recomendaciones.

En la especificación de interfaz eléctrica y funcional para los enlaces de interfaz se utilizan las partes a 2048 kbit/s de las Recomendaciones G.703, G.704 y G.706. Puede haber hasta 16 enlaces de interfaz en paralelo, que constituyen la interfaz V5.2.

La señalización desde el puerto de usuario de la red telefónica pública conmutada se convierte en un protocolo de estímulo con una parte funcional para el trayecto de señalización que utiliza la multiplexación de capa 3 para la información procedente de los diferentes puertos de usuario.

La información de los canales D de la RDSI se retransmite en tramas en la red de acceso utilizando los mecanismos definidos en la Recomendación Q.933.

Se utiliza un protocolo de control definido en esta Recomendación para el intercambio del estado de los puertos individuales y las funciones de control que se requieren para la coordinación con los procedimientos de control en la central local.

Un protocolo de conexión de canal portador establece y desestablece las conexiones portadoras necesarias a petición, identificadas por la información de señalización, bajo el control de la central local.

Se define un protocolo de control de enlace para la gestión multienlace a fin de controlar las condiciones de identificación de enlace, bloqueo de enlace y fallo de enlace.

Con el fin de coordinar las demandas de tráfico en los distintos protocolos, se pueden proveer hasta 3 canales de comunicación por enlace de interfaz para transportar los distintos protocolos y la información retransmitida en tramas. La capa de enlace de datos para los protocolos se define de acuerdo con las Recomendaciones Q.920 y Q.921.

Para gestionar la conmutación de protección de los canales de comunicación en caso de averías de los enlaces, se define un protocolo de protección, que funciona en dos enlaces de datos separados por motivos de seguridad.

INTRODUCCIÓN

Diferencias principales entre la interfaz V5.1 y la interfaz V5.2

Recomendación sobre V5.1 (Recomendación G.964) es una Recomendación completa por sí misma, mientras que la presente Recomendación sobre V5.2 hace referencia a partes de la Recomendación G.964.

La V5.1 utiliza únicamente un enlace a 2048 kbit/s, mientras que la V5.2 puede utilizar hasta dieciséis (16) enlaces a 2048 kbit/s en una interfaz.

La V5.1 no admite la concentración, mientras que la V5.2 está intrínsecamente concebida para ello, utilizando un protocolo especializado conocido como protocolo de conexión de canal portador (BCC, *bearer channel connection*).

La V5.1 no admite puertos de usuario de acceso a velocidad primaria de la RDSI, mientras que la V5.2 sí los admite.

La V5.1 no incluye el concepto de protección del canal de comunicación, función que sí está disponible en el caso de la interfaz V5.2 cuando utiliza más de un enlace a 2048 kbit/s. Se proporciona un protocolo específico para esta función, conocido como protocolo de protección.

El protocolo de control para V5.2 tiene ligeras modificaciones con relación al que se utiliza para V5.1.

Se especifica un protocolo de control de enlace para V5.2, dado que deben gestionarse múltiples enlaces.

Recomendación G.965

INTERFACES V EN LA CENTRAL LOCAL DIGITAL – INTERFAZ V5.2 (BASADA EN 2048 kbit/s) PARA SOPORTAR LA RED DE ACCESO

(Ginebra, 1994)

1 Alcance

La presente Recomendación especifica los requisitos eléctricos, físicos, de procedimiento y de protocolo para la interfaz V5.2 entre una red de acceso (AN, *access network*) y la central local (LE, *local exchange*) para sustentar los siguientes tipos de acceso:

- acceso telefónico analógico;
- acceso básico RDSI con un sistema de transmisión de línea conforme a la Recomendación G.960 [4] cuando se utiliza una NT1 separada de la AN;
- acceso básico RDSI con una interfaz usuario-red conforme a la Recomendación I.430 [3] en el lado usuario de la AN (es decir, la interfaz en el punto de referencia T);
- acceso a velocidad primaria RDSI con un sistema de transmisión de línea conforme a la Recomendación G.962 [10] cuando se utiliza una NT1 separada de la AN;
- acceso a velocidad primaria RDSI con una interfaz usuario-red conforme a la Recomendación I.431 [9] en el lado usuario de la AN (es decir, la interfaz en el punto de referencia T);
- otros accesos analógicos o digitales para conexiones semipermanentes sin información de señalización fuera de banda asociada,

con asignación flexible de canal de información (canal portador) llamada por llamada que proporciona la capacidad de concentración en la AN y a través de la interfaz V5.2. Esta Recomendación no especifica la implementación de los requisitos en la AN y no impone ninguna alternativa de implementación mientras se cumpla la funcionalidad en la interfaz V5.2 especificada en esta Recomendación.

Esta Recomendación debe utilizarse junto con la Recomendación G.964 [8]. Las dos Recomendaciones tienen un formato común y, en la presente Recomendación, se hace referencia a cláusulas de la Recomendación G.964 [8].

Se proporciona una capacidad de control de enlace con el fin de gestionar las posibles disposiciones multienlace en una interfaz V5.2. Véase la cláusula 16.

Se contempla una capacidad de protección, a fin de que la interfaz pueda seguir funcionando en caso de fallo del enlace a 2048 kbit/s.

El Anexo A contiene una sinopsis de los casos de servicio y la arquitectura considerados como base conceptual para la especificación de la interfaz V5.2.

El Anexo B define la utilización de los elementos de información de protocolo para definir los protocolos nacionales de las redes telefónicas públicas conmutadas (RTPC) y los diagramas de flujo de información para la especificación de protocolos RTPC. El anexo H contiene la definición de la detección de errores del protocolo RTPC de capa 3.

El Anexo C especifica las hipótesis básicas de la función de gestión en la LE y en la AN para sustentar el funcionamiento y control correctos de la configuración.

El Anexo D describe la arquitectura de protocolo para la transferencia de información de control de estado de los puertos de usuario de la RDSI y de la RTPC.

El Anexo E proporciona una sinopsis de los formatos de trama utilizados en la interfaz V5.2, así como los tipos de mensajes asignados a la interfaz V5.2.

2 Referencias normativas

Las siguientes Recomendaciones contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones son objeto de revisiones, por lo que se preconiza que todos los usuarios de la presente Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones citadas a continuación. Se publica regularmente una lista de las Recomendaciones UIT-T actualmente válidas.

[1] Recomendación G.703 del CCITT, *Características físicas y eléctricas de las interfaces digitales jerárquicas*.

[2] Recomendaciones G.704 del CCITT, *Estructuras de trama síncrona utilizadas en los niveles jerárquicos primario y secundario*.

[3] Recomendación UIT-T I.430, *Especificación de la capa 1 de la interfaz usuario-red básica*.

[4] Recomendación UIT-T G.960, *Sección digital para el acceso a velocidad básica a la RDSI*.

[5] Recomendaciones UIT-T Q.920 y Q.921, *Especificación de la capa de enlace de datos de la interfaz usuario-red de la RDSI*.

[6] Recomendación UIT-T Q.931, *Especificación de la capa 3 de la interfaz usuario-red de la RDSI para el control de llamada básica*.

[7] Recomendación UIT-T G.823, *Control de la fluctuación de fase y de la fluctuación lenta de fase en las redes digitales basadas en la jerarquía de 2048 kbit/s*.

[8] Recomendación UIT-T G.964, *Interfaces V en la central local digital; interfaz V5.1 (basada en 2048 kbit/s) para sustentar la red de acceso*.

[9] Recomendación UIT-T I.431, *Especificación de la capa 1 de la interfaz usuario-red a velocidad primaria*.

[10] Recomendación UIT-T G.962, *Sección digital de acceso a la velocidad primaria de 2048 kbit/s a la RDSI*.

[11] Recomendación G.706 del CCITT, *Procedimientos de alineación de trama y de verificación por redundancia cíclica relativos a las estructuras de trama básica definidas en la Recomendación G.704*.

3 Definiciones, símbolos y abreviaturas

3.1 Definiciones

A los efectos de esta Recomendación, se aplican las siguientes definiciones, además de las que figuran en la Recomendación G.964 [8] y en las referencias normativas:

3.1.1 canal C activo: Canal C físico que transporta actualmente un canal C lógico. Un canal C activo se convierte en un canal C de reserva cuando no está transportando un canal C lógico.

3.1.2 canales portadores: Los canales portadores se utilizan con el fin de proporcionar la capacidad de transmisión bidireccional para los canales B asignados desde los puertos de usuario de acceso básico, los puertos de usuario de acceso a velocidad primaria, o para los canales a 64 kbit/s con codificación MIC de ley A desde los puertos de usuario RTPC. Pueden ser utilizados en múltiplos de canales a 64 kbit/s con el fin de facilitar algunos servicios de la RDSI.

3.1.3 protocolo de conexión de canal portador (BCC, *bearer channel connection***)**: Protocolo gracias al cual la LE puede indicarle a la AN que asigne canales portadores, ya sea individualmente o en múltiplos, a petición.

3.1.4 canal de comunicación (canal C): Intervalo de tiempo a 64 kbit/s en una interfaz V5.2 previsto para trayectos de comunicación.

3.1.5 trayecto de comunicación (trayecto C): Cualquiera de los siguientes tipos de información (véase también 8.4.1):

- el enlace de datos de capa 2 que transporta el protocolo de control;
- el enlace de datos de capa 2 que transporta el protocolo de control de enlace;
- el enlace de datos de capa 2 que transporta la señalización de la RTPC;
- cada uno de los enlaces de datos de capa 2 que transportan el protocolo de protección;
- el enlace de datos de capa 2 que transporta el protocolo BCC;

– todos los datos de tipo Ds de la RDSI desde uno o más puertos de usuario;

– todos los datos de tipo p de la RDSI desde uno o más puertos de usuario;

– todos los datos de tipo f de la RDSI desde uno o más puertos de usuario.

Deber observarse que esta definición incluye la posibilidad de que haya varios trayectos C del mismo tipo de información, asignados cada uno a un canal C lógico diferente.

3.1.6 información de canal D de la RDSI: La información de canal D de la RDSI se define como la información del canal D procedente de puertos de usuario con acceso básico o a velocidad primaria (incluidos los datos de los tipos Ds, p y f).

3.1.7 canal de comunicación lógico (canal C lógico): Grupo de uno o más trayectos C, todos de tipos diferentes, pero excluido el trayecto C para el protocolo de protección.

3.1.8 multienlace: Colección de varios enlaces a 2048 kbit/s que constituyen juntos una interfaz V5.2 (pese a que una interfaz V5.2 no necesita tener más de un enlace a 2048 kbit/s).

3.1.9 multiintervalo: Grupo de más de un canal a 64 kbit/s que proporciona 8 kHz e integridad de secuencia de intervalos de tiempo, generalmente utilizado junto con un puerto de usuario con acceso a velocidad primaria a la RDSI, a fin de proporcionar un servicio a velocidad binaria más alta.

3.1.10 canal de comunicación físico (canal C físico): Intervalo de tiempo a 64 kbit/s en una interfaz V5.2 que ha sido asignado para transportar canales C lógicos. Un canal C físico no puede ser utilizado para canales portadores.

Los intervalos de tiempo 16 en el enlace primario y el enlace secundario (únicamente en una interfaz V5.2 con más de un enlace a 2048 kbit/s) son siempre canales C físicos.

3.1.11 canales portadores preconectados: Cualquier canal portador o múltiplos del mismo establecidos utilizando el protocolo BCC a fin de proporcionar servicios conmutados en la AN en anchura de banda reservada en la interfaz V5.2 reservada para ello.

3.1.12 enlace primario: El enlace a 2048 kbit/s en una interfaz V5.2 multienlace cuyo canal C físico transporta en el intervalo de tiempo 16 un trayecto C para el protocolo de protección y, al inicializar V5.2, también el trayecto C para el protocolo de control, el protocolo de control de enlace y el protocolo BCC. Pueden transportarse también otros trayectos C en el intervalo de tiempo 16.

3.1.13 grupo protegido: Grupo de N canales C lógicos.

3.1.14 grupo de protección: Grupo de (N + K) canales C físicos, donde K es el número de canales C físicos que actúan como canales C de reserva para los N canales C lógicos.

3.1.15 enlace secundario: El enlace a 2048 kbit/s en una interfaz V5.2 multienlace cuyo intervalo de tiempo 16 transporta un trayecto C para el protocolo de protección y, en la inicialización de V5.2, actúa como canal C de reserva para el protocolo de control, el protocolo de control de enlace y el protocolo BCC y cualesquiera otros trayectos C transportados inicialmente en el intervalo de tiempo 16 del enlace primario.

3.1.16 canal C de reserva: Canal C físico que no transporta un canal C lógico, pero que es utilizado para la protección de canales C lógicos. Al ser utilizado para transportar un canal C lógico, un canal C de reserva se transforma en un canal C activo.

3.1.17 punto de referencia T: El término punto de referencia T se utiliza en un sentido general. Si un terminal RDSI o un adaptador de terminal es conectado a la interfaz en el punto de referencia T, entonces, de acuerdo con la configuración de referencia RDSI, los puntos de referencia S y T coinciden o, si una terminación de red de tipo 2 está conectada a la interfaz en el punto de referencia T, éste es el punto de referencia T explícito.

3.2 Símbolos y abreviaturas

A los efectos de esta Recomendación se aplican las abreviaturas siguientes, además de las que figuran en la Recomendación G.964 [8]:

BCC	Conexión de canal portador (*bearer channel connection*)
dB	decibel
AVP-RDSI	Acceso a velocidad primaria RDSI
H0	Canal con 384 kbit/s acompañado por temporización
H12	Canal con 1920 kbit/s acompañado por temporización

LFA	Pérdida de alineación de trama (*loss of frame alignment*)
O	Elemento de protocolo obligatorio
NOF	Tramas operacionales normales (*normal operational frames*)
F	Elemento de protocolo facultativo
REQ	Petición (*request*)
SN	Número de secuencia (*sequence number*)
TSSI	Integridad de secuencia de intervalo de tiempo (*time slot sequence integrity*)
VP(S)	Variable de estado emisión para el protocolo de protección
VP(R)	Variable de estado recepción para el protocolo de protección

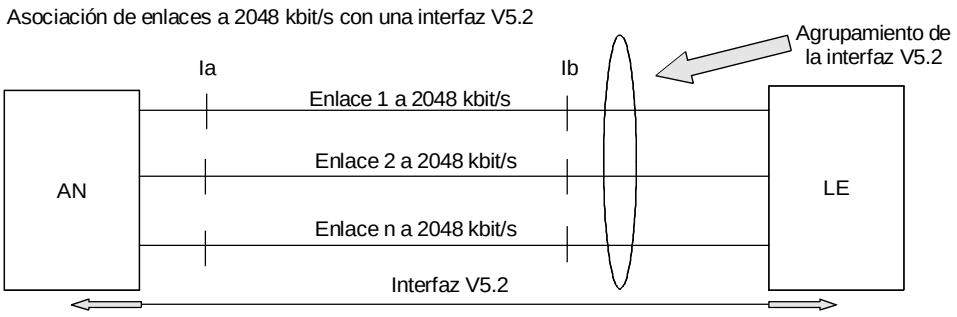
4 Requisitos eléctricos y físicos de la interfaz

La interfaz V5.2 puede tener entre uno y 16 enlaces a 2048 kbit/s, según proceda.

Las características eléctricas y físicas de cada una de las interfaces a 2048 kbit/s se conformarán a la Recomendación G.703 [1], caso 2048 kbit/s.

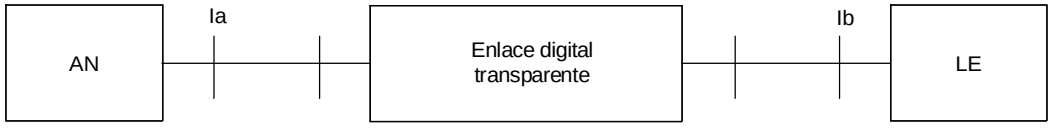
En la Recomendación G.703 [1] se definen dos alternativas de presentación de interfaz, a saber, el tipo par de interfaces equilibrado y el tipo coaxial. De acuerdo con las dos alternativas de aplicaciones de interfaz mostradas en la Figura 1, corresponde al operador de la red solicitar la presentación de interfaz requerida.

Los requisitos de fluctuación de fase para cada uno de los enlaces a 2048 kbit/s serán los mismos que en la Recomendación G.964 [8].



NOTA – Se muestran n enlaces a 2048 kbit/s (n = 1 a 16).

Todos los enlaces a 2048 kbit/s (o cualquiera de ellos) pueden utilizar un enlace digital transparente como se indica a continuación:



Ia Punto de interfaz en el lado AN
Ib Punto de interfaz en el lado LE

FIGURA 1/G.965

Aplicación de V5.2 con y sin enlace digital transparente

5 Requisitos de procedimiento de la interfaz

Los requisitos funcionales y de procedimiento de cada uno de los enlaces a 2048 kbit/s serán los mismos que en la Recomendación G.964 [8].

5.1 Requisitos y procedimientos de control de enlace

Como la interfaz V5.2 puede constar de múltiples enlaces a 2048 kbit/s, es necesario poder verificar la identidad de los enlaces y bloquear un enlace específico. Se han definido dos procedimientos para estas funciones en 16.2; estas funciones son realizadas a través del protocolo de control de enlace.

5.1.1 Verificación de la identidad del enlace

La verificación de la identidad del enlace es un procedimiento simétrico que será aplicado desde ambos extremos de los enlaces de la interfaz V5.2 cuando la máquina de estados finitos de la capa 1 (L1-FSM, *layer 1 finite state machine*) de la interfaz entre en el estado normal. Si el procedimiento falla, la máquina de estados finitos FSM, (*finite state machine*) retornará al estado no operacional.

Este procedimiento se aplicará a todos los enlaces, incluidos los enlaces primario y secundario. También puede llevarse a cabo cuando se está de manera permanente en el estado normal, por ejemplo, con base en una temporización, o a petición de la interfaz Q (AN/LE).

Este procedimiento se aplicará incluso en el caso de la interfaz V5.2 con un solo enlace a 2048 kbit/s.

5.1.2 Bloqueo de enlace

A los efectos de mantenimiento de los enlaces, es necesario poder bloquear un solo enlace a 2048 kbit/s de una interfaz V5.2. El bloqueo de enlace es un procedimiento asimétrico, en el que la AN puede solicitar el bloqueo de un enlace, pero la LE decide, en calidad de dueño del servicio. La LE libera cualquier conexión conmutada en el enlace solicitado según proceda para el servicio y, a su debido tiempo, restablece conexiones semipermanentes y preconectadas en otros enlaces dentro de la misma interfaz V5.2. La LE utilizará el protocolo de protección para desplazar los canales C lógicos afectados, si es posible.

Este procedimiento puede aplicarse incluso en el caso de la interfaz V5.2 con un solo enlace a 2048 kbit/s.

NOTA – En este caso, el bloqueo pone toda la interfaz fuera de servicio.

6 Servicios y aspectos y requisitos de la arquitectura

Los servicios que ha de soportar la interfaz V5.2 incluirán todos los soportados por V5.1 (definida en la Recomendación G.964 [8]), además de AVP-RDSI. Sin embargo, esta Recomendación no tiene por objeto restringir ninguna implementación de las AN o LE para soportar el conjunto completo o un subconjunto de los servicios enumerados en esta Recomendación.

En la Figura 2 se muestra la arquitectura de V5.2 desde el punto de vista del servicio.

6.1 Servicios a petición

Los servicios a petición pasan a través de la interfaz V5.2. Se admiten los tres tipos de acceso siguientes.

6.1.1 RTPC

El contenido de esta subcláusula es idéntico al de 6.1.1/G.964 [8].

6.1.2 Acceso básico RDSI (AB-RDSI)

El contenido de esta subcláusula es idéntico al de 6.1.2/G.964 [8].

Además, el servicio portador multiintervalo de 2×64 kbit/s puede ser soportado mediante la capacidad de canal portador definida en esta Recomendación.

6.1.3 Acceso a velocidad primaria RDSI (AVP-RDSI)

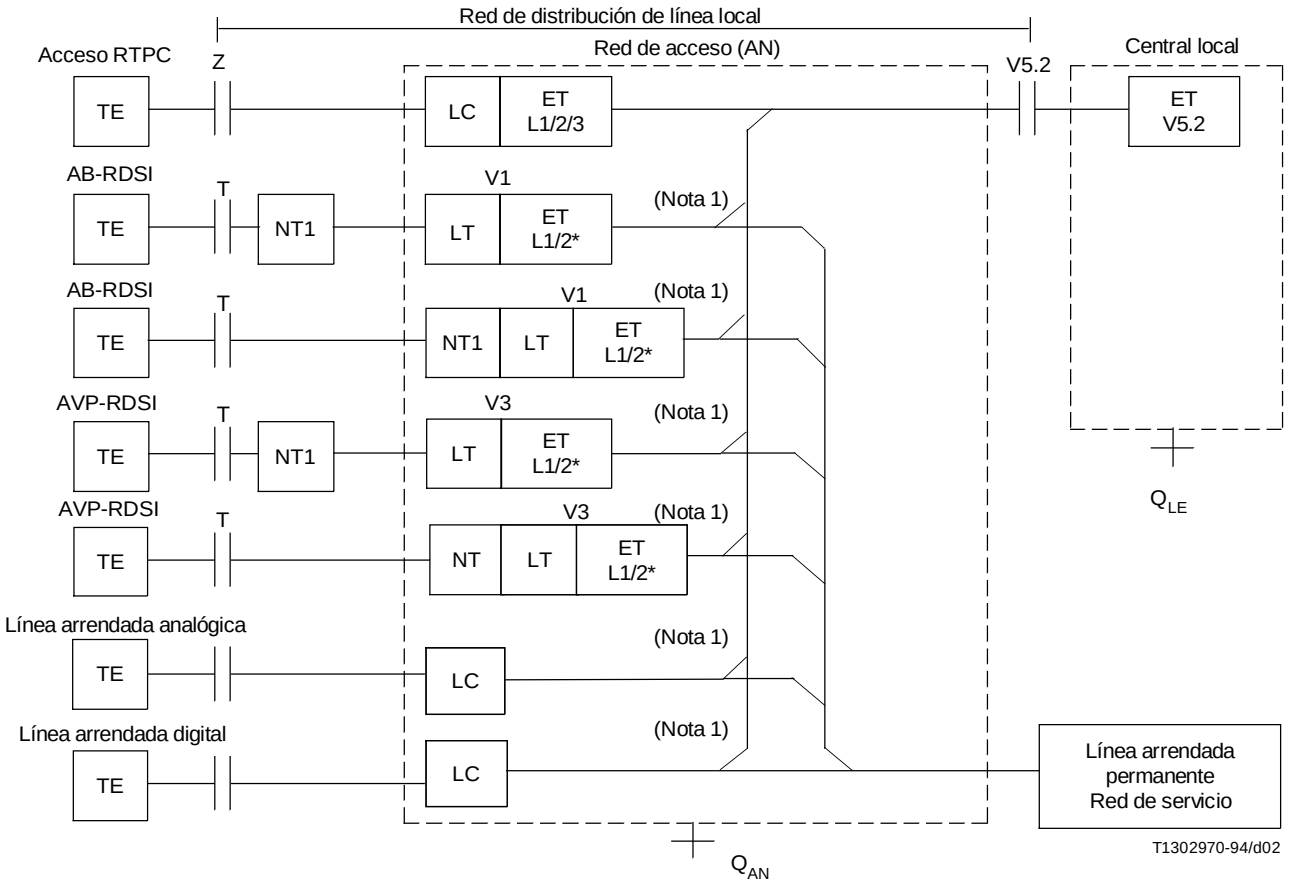
El acceso a velocidad primaria RDSI es admitido con una NT1 como parte integral de la AN o como equipo separado que soporta sistemas de transmisión conformes a la Recomendación G.962 [10] para el soporte de NT2 (por ejemplo PABX RDSI), conectada al punto de referencia T.

Las velocidades binarias inferiores a 64 kbit/s no son admitidas directamente. Se ven como aplicaciones de usuario dentro de un canal B a 64 kbit/s en el AVP.

Uno o más canales B en el AVP pueden ser utilizados para la capacidad de línea permanente facultativa o el servicio de línea arrendada semipermanente.

Los servicios portadores multivelocidad, que pueden utilizar H0, H12 u otros canales multiintervalo entre el puerto de usuario y la LE, también son soportados por una interfaz V5.2 que admita los AVP-RDSI que utilizan los sistemas de señalización RDSI apropiados.

NOTA – Si estos servicios no disponen del soporte de la LE o la AN, no podrán estar a disposición de los usuarios.



NOTAS

1 La selección de canales y la asignación de servicio forman parte del aprovisionamiento.
2 El asterisco indica que la capa 2 es sólo parcialmente terminada en la AN.

FIGURA 2/G.965

Arquitectura de la interfaz V5.2 desde el punto de vista del servicio

6.2 Capacidad de línea permanente (PL, permanent line)

El contenido de esta subcláusula es idéntico al de 6.2/G.964 [8]. Sin embargo, la capacidad PL se proporcionará para el servicio AVP-RDSI como se especifica en 15.3.

6.3 Línea arrendada semipermanente

El contenido de esta subcláusula es idéntico al de 6.3/G.964 [8]. Sin embargo, el requisito de línea arrendada semipermanente será aplicable también para el AVP-RDSI.

6.4 Servicio de línea arrendada permanente

El contenido de esta subcláusula es idéntico al de 6.4/G.964 [8].

7 Control y aprovisionamiento

7.1 Principios de control

7.1.1 Requisitos generales e hipótesis

Con base en la Figura 3, se han definido los siguientes requisitos generales para el puerto de acceso básico RDSI y el puerto de acceso a velocidad primaria RDSI. Se aplicaría también a los puertos RTPC si no se indica lo contrario.

1) La responsabilidad del control de la llamada corresponde a la LE (es decir, la AN puede no tener conocimiento del estado de la llamada durante el funcionamiento normal de la interfaz V5.2).

2) La gestión de acceso en la AN y la gestión de servicio en la LE mantienen cada una sus máquinas de estados finitos (FSM, *finite state machine*) y entidades de protocolo, y comunican por la interfaz V5.2.

   Se requieren FSM para cada puerto de usuario y para las interfaces a 2048 kbit/s, así como entidades de protocolo para los enlaces de capa 2, en la AN y en la LE (véanse la Figura 4 para aclaración y la cláusula 15 para la definición de las FSM, entidades de protocolo y el protocolo de capa 3). La información proporcionada por la FSM o entidad de protocolo a la gestión se utilizará para decidir la acción apropiada hacia otras FSM y entidades de protocolo, la función de control de llamada y el sistema operativo. En el Anexo C se proporciona información adicional sobre algunas hipótesis básicas.

3) La petición de bloqueo de puerto, para mantenimiento de puerto no urgente a través de la interfaz Q de la AN, sólo puede ser concedida por la LE (es decir, la petición de bloqueo no debe interferir con llamadas en curso, llamadas que se estén estableciendo o liberando o conexiones semipermanentes).

4) El mantenimiento de puerto urgente solicitado por la interfaz Q de la AN se indicará a la LE con independencia del estado de la LE (es decir, el «bloqueo inmediato» es efectivo inmediatamente, pero el nuevo estado ha de sincronizarse con la LE).

5) Los fallos de capa 1 detectados que se relacionan con canales portadores dentro de los enlaces a 2048 kbit/s con fallo darán como resultado la liberación de las llamadas. Los fallos de capa 1 detectados que se relacionan con los canales C físicos dentro de un enlace a 2048 kbit/s con fallo darán como resultado la reasignación de estos canales C mediante el protocolo de protección si hay recursos suficientes para hacerlo. No se permite la apropiación de canales C físicos de manera autónoma por el protocolo de protección. Los fallos de capa 1 detectados que se relacionan con líneas arrendadas semipermanentes dentro de un enlace a 2048 kbit/s con fallo darán como resultado que el gestor de recursos de la LE intente establecer otra conexión portadora en la que el servicio ha de proveerse. Puede haber anomalías y defectos que pueden degradar el servicio pero que no resultan en una pérdida total del servicio y, por tanto, no ocasionan la generación de las reconfiguraciones anteriores. Estas anomalías o defectos que afectan al servicio de la RTPC pueden repercutir en el protocolo de la RTPC, por ejemplo, mediante el acuse de recibo negativo de un mensaje de petición, pero no afectarán a la FSM del puerto.

6) Se requiere que las anomalías detectadas y otros eventos se informen a la gestión asociada en la AN o LE y se registren.

7) Cuando un puerto está bloqueado, no es posible efectuar llamadas de origen, y las llamadas de terminación serán tratadas por la LE como si el puerto estuviera fuera de servicio de acuerdo con el protocolo nacional.

8) La LE debe conocer el nivel de calidad de transmisión relativo a los puertos de usuario por medio de mensajes de «grado de servicio» procedentes de la AN a la LE que no afectan a las FSM de estado de puerto. Estos mensajes contienen información de grado de servicio que ha de ser registrada en la LE. La LE puede utilizar esta información para decidir si debe prestar o no un servicio solicitado.

   Este requisito es sólo pertinente para un puerto RDSI con una NT1 que está fuera de la AN. La calidad de funcionamiento entre el puerto de usuario y la interfaz V5.2 no será afectada indebidamente por una calidad de funcionamiento degradada debido a errores en los bits ocurridos en enlaces internos de la AN. Esto se excluirá mediante la supervisión en servicio y el bloqueo por el servicio de los enlaces internos de la AN en caso de degradación de la característica de error.

9) Se aplicarán bucles únicamente cuando el puerto esté en el estado bloqueado. Esta función está bajo el control de la AN.

   La ejecución de la localización de fallos dentro de la AN y el puerto de usuario es responsabilidad de la AN. La prueba activa que interfiere con el servicio bajo la responsabilidad de la LE no se realizará hasta que el puerto esté bloqueado (la FSM en condición bloqueado) por la LE.

10) Habrá un mecanismo para identificar individualmente a las interfaces V5 y las etiquetas de sus variantes de aprovisionamiento vigentes y nuevas. La variante de aprovisionamiento es una etiqueta única de un conjunto completo de datos de aprovisionamiento aplicada a través de las interfaces Q (véase 15.7).

11) Será posible identificar cada enlace individual a 2048 kbit/s en una interfaz V5.2. Se aplicará un procedimiento (simétrico) para comprobar la identidad de los enlaces a 2048 kbit/s en cualquier restablecimiento de alineación de trama y después de un reaprovisionamiento (que puede afectar o no a los enlaces V5.2).

12) Será posible bloquear un enlace a 2048 kbit/s individual para una interfaz V5.2. La AN puede emitir una petición, pero la LE decide: para las conexiones conmutadas, esperará hasta que las llamadas terminen, las conexiones semipermanentes y reservadas por la AN se restablecerán en otros enlaces. La gestión del sistema de la LE utilizará el protocolo de protección para desplazar los canales C lógicos afectados antes de que un enlace a 2048 kbit/s sea bloqueado. Utilizando un mecanismo ligeramente diferente, la AN puede realizar un bloqueo inmediato de un enlace a 2048 kbit/s designado.

13) Los enlaces a 2048 kbit/s pueden retirarse del servicio dentro de una interfaz V5.2 a efectos de mantenimiento a través de Q_{LE} y Q_{AN} con el soporte del protocolo de control de enlace de interfaz V5.2. Se pondrán de nuevo en servicio utilizando también el protocolo de control de enlace V5.2.

14) A través de Q_{LE} podrá prohibirse el uso de canales portadores individuales dentro de una interfaz V5.2.

7.1.2 Control de puerto de usuario AB-RDSI para la capacidad PL

El control de los puertos de usuario AB-RDSI cuando se suministra la capacidad PL será el mismo que el contemplado en 7.1.2/G.964 [8].

7.1.3 Control de los puertos de usuario AVP-RDSI cuando se suministra la capacidad PL

El suministro de la capacidad PL no afectará la operación de un puerto de usuario AVP-RDSI.

7.1.3.1 Enunciados e hipótesis

1) La capacidad PL soportada por la AN en la configuración V5.2 es una característica adicional en una interfaz usuario-red RDSI, que no puede ser soportada por un acceso conectado directamente a una LE.

2) La capacidad PL puede, facultativamente, utilizar uno o varios (o posiblemente todos) canales B en un puerto de usuario no previstos en la AN o LE para transportar servicios a petición. Como se muestra en la Figura 3, únicamente tramas operacionales normales (NOF, *normal operational frames*) pueden ser enviadas al punto de referencia V.

3) La LE es la responsable de los servicios a petición.

4) Cuando la LE bloquea el puerto de usuario, lo que pone al puerto de usuario en un estado no operacional para todos los tipos de servicios, la AN puede recuperar el control para permitir que los puertos que disponen de la capacidad PL puedan seguir funcionando.

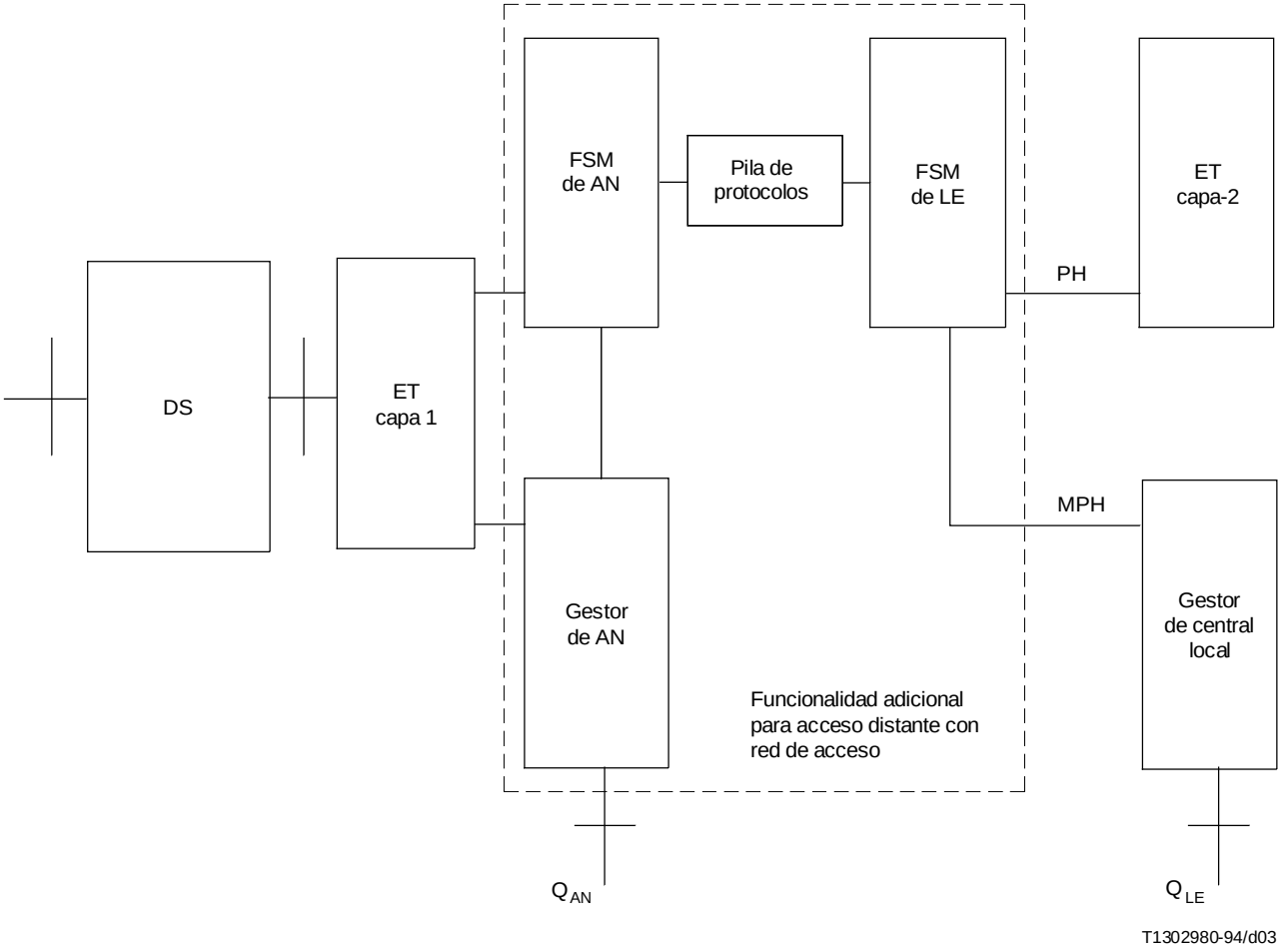
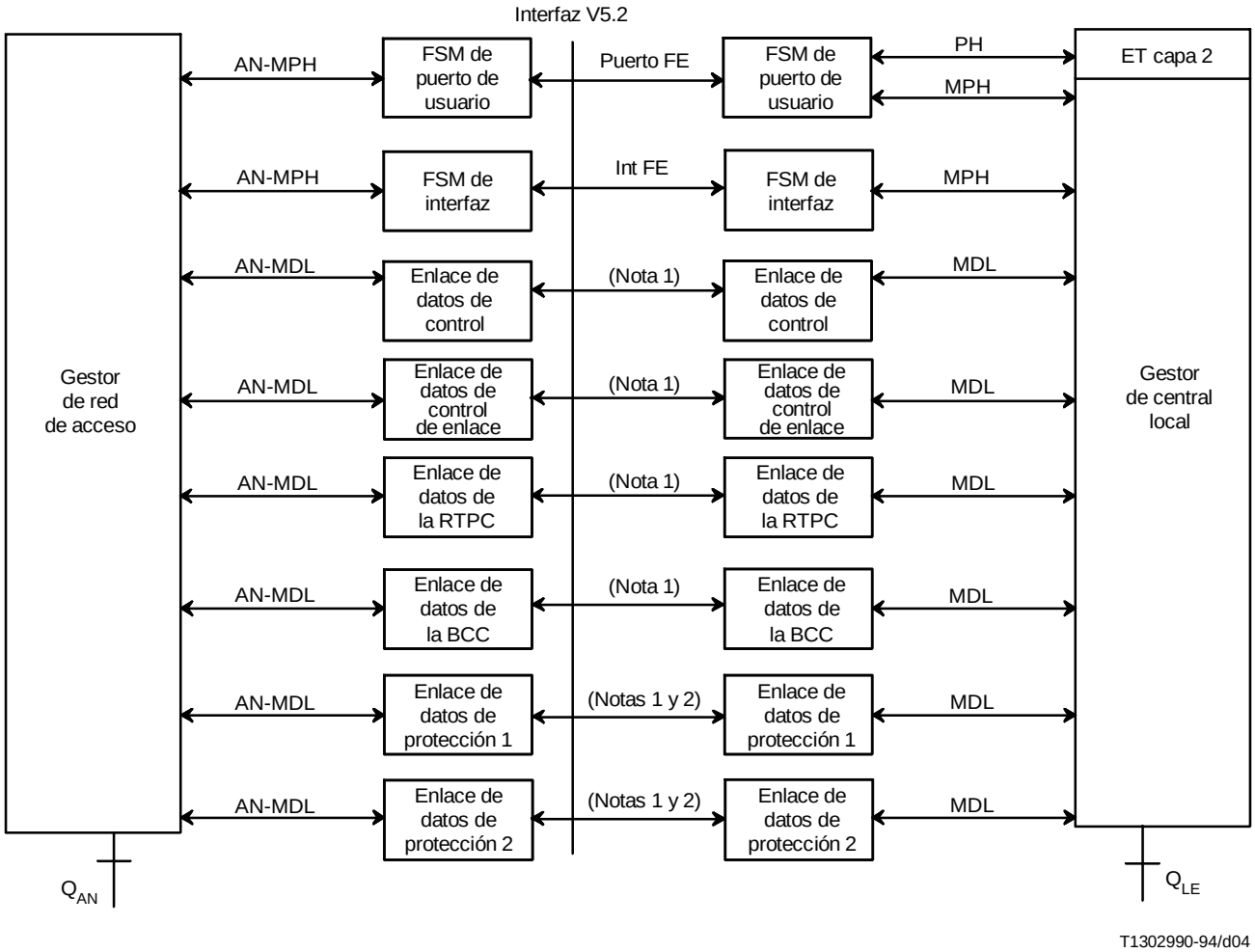


FIGURA 3/G.965

Modelo funcional de puerto de usuario RDSI



NOTAS

1 Véase 10.4.

2 Las entidades de protocolo de enlace de protección se utilizarán únicamente en el caso de una interfaz V5.2 con más de un enlace a 2048 kbit/s.

FIGURA 4/G.965

Modelo funcional de FSM de capa 1 y de capa 2

7.1.3.2 RDSI y capacidad PL

El servicio PL no utilizará el canal D para mensajes destinados a la LE. El servicio AVP-RDSI definido actualmente, Recomendación G.962 [10], entregado a un puerto de usuario RDSI en una AN será el mismo que para las conexiones de acceso directo a la LE.

Para una AN, no se puede aceptar que un servicio (por ejemplo PL) que utiliza uno o más canales B a efectos distintos del servicio a petición tenga repercusiones en un servicio a petición RDSI.

7.2 Estrategia y requisitos de aprovisionamiento

7.2.1 Generalidades

El aprovisionamiento es uno de los muchos aspectos para controlar las funciones. Se ha separado de otros requisitos de control porque el aprovisionamiento se efectuará a través de las interfaces Q de la AN y la LE y, por tanto, no es directamente pertinente a la especificación de la interfaz V5.2. Sólo se definen a continuación aquellos aspectos del aprovisionamiento que tienen por lo menos una repercusión conceptual o indirecta sobre la definición de la interfaz.

7.2.2 Requisitos de aprovisionamiento

Véase en 7.2.2/G.964 [8] una lista de los elementos que han de proveerse, además de los que figuran a continuación. Sin embargo, el primer elemento de la lista mencionada no es válido para la interfaz V5.2, ya que la asociación de canales portadores está bajo el control del protocolo de la BCC y no está asociada estáticamente a través del aprovisionamiento.

Requisitos de aprovisionamiento

1) El número de enlaces a 2048 kbit/s utilizados en una interfaz V5.2, así como su identificación, se asigna mediante el aprovisionamiento.

2) Los canales C físicos son asignados a intervalos de tiempo/enlaces mediante el aprovisionamiento.

3) Los canales C físicos de los intervalos de tiempo 16 de los enlaces primario y secundario forman el grupo de protección 1, incluyendo el protocolo de protección. (Se supone que hay más de un enlace a 2048 kbit/s en esa interfaz V5.2.) De no ser así, este aprovisionamiento no es válido.

4) Uno de los canales C físicos del grupo de protección 1 actúa como canal C activo. El otro canal C físico del grupo de protección 1 actúa como canal C de reserva de este grupo.

5) El aprovisionamiento asigna por defecto canales C lógicos a canales C físicos.

6) Un canal C físico sin canal C lógico asignado actúa como canal C de reserva. (La asignación de trayectos C a canales C lógicos se hará a través del aprovisionamiento).

7) La asignación de trayectos C para datos de tipo Ds (así como para datos de tipo p y f) o la señalización RTPC es una opción aprovisionada.

8) El canal C físico activo del grupo de protección 1 transportará por lo menos los trayectos C del protocolo de protección, el protocolo BCC, el protocolo de control y el protocolo de control de enlace.

9) Q_{LE} puede utilizarse para retirar la asignación de un canal C lógico a un canal C físico.

10) Q_{LE} puede utilizarse para asignar un canal C lógico determinado a un canal C físico. La protección puede cambiarlo ulteriormente.

11) Al aprovisionar canales C físicos para una instalación, debe prestarse atención si la LE y/o la AN consiste en módulos que comparten las funciones de terminación de soporte lógico para la interfaz V5.2. Debe tenerse en cuenta el efecto de qué canal C físico es servido por qué módulo. Debe tenerse cuidado al provisionar canales C físicos para uso de reserva, a fin de que la futura conmutación de protección a esos canales C físicos no cause irregularidades indebidas en la carga de estos módulos.

De manera similar, si una LE y/o AN está modularizada a efectos de salvaguardar la calidad de funcionamiento en presencia de fallos, debe velarse por que se aprovisionen los canales C físicos (tanto los utilizados como los de reserva) de manera que dicha calidad de funcionamiento pueda salvaguardarse mediante la conmutación de protección, no sólo en presencia de fallos de los enlaces a 2048 kbit/s, sino también en presencia de fallos de módulos en la LE y la AN.

7.3 Conexión de canal portador (BCC, bearer channel connection)

El protocolo BCC se utiliza para asignar canales portadores en un enlace a 2048 kbit/s específico a los puertos de usuario, por lo general de manera individual para cada llamada. Se supone que los sistemas de gestión de recursos de canal portador se proporcionan dentro de la LE y la AN, pero esta Recomendación define únicamente las funciones que tienen repercusiones directas sobre la interfaz V5.2.

A continuación se indican los canales portadores asignados mediante el protocolo BCC, pero no individualmente para cada llamada:

– *La conexión de línea arrendada semipermanente* – Estas utilizan uno o más canales portadores que son asignados a puertos de usuario utilizando Q_{LE} y son establecidos utilizando el protocolo BCC.

– *Los canales portadores preconectados* – Estos utilizan uno o más canales portadores que son asignados a puertos de usuario utilizando Q_{LE} y son establecidos utilizando el protocolo BCC.

Se proporciona una función de auditoría a través del protocolo BCC con el fin de que puedan comprobarse la asignación de canales portadores en la V5.2 y las conexiones en la AN.

Se proporciona también una función de fallo interno de la AN en el protocolo BCC con el fin de que la AN pueda notificar a la LE los fallos internos que afectan las conexiones de canales portadores.

7.4 Protección

El protocolo de protección se utiliza en el caso de interfaces con más de un enlace a 2048 kbit/s. Es necesario que el control de enlace, el control y los protocolos BCC tengan un trayecto de comunicación a través de la interfaz V5.2, incluso en caso de fallo de un enlace a 2048 kbit/s (es decir, un enlace primario o secundario).

El protocolo de protección tiene la responsabilidad de garantizar que haya un método gracias al cual las entidades de la LE y la AN puedan comunicar para proteger los canales C lógicos en caso de fallo de un solo enlace, si existen canales C físicos de reserva.

Si se necesita conmutación de protección para los canales C lógicos, incumbe a la función de gestión de protección iniciar la transferencia de manera controlada, utilizando el protocolo de protección.

8 Arquitectura de protocolo y estructura de multiplexación

8.1 Descripción funcional

En la Figura 5 se ilustra la descripción funcional. Las subcláusulas de la Recomendación G.964 [8] relacionadas con el acceso básico RDSI se aplicarán también al acceso a velocidad primaria RDSI. Además de los requisitos funcionales que figuran en la Recomendación G.964 [8] se definen los siguientes:

- se utiliza un protocolo BCC para asignar canales portadores bajo el control de la LE;
- el servicio que requiera conexiones multiintervalo se proporcionará a través de un enlace a 2048 kbit/s dentro de una interfaz V5.2. En este caso, se dispondrá siempre de 8 kHz y de integridad de la secuencia de intervalos de tiempo;
- se define un protocolo de control de enlace que soportará las funciones de gestión de los enlaces a 2048 kbit/s de la interfaz V5.2;
- se define un protocolo de protección que soportará la conmutación de los canales C lógicos entre los canales C físicos según proceda.

8.2 Requisitos de protocolo de la RTPC y la RDSI

En la Figura 6 se ilustra la arquitectura de protocolo de manera simplificada. Las funciones especificadas en esta Recomendación aparecen sombreadas.

Las funciones se definen en las cláusulas siguientes:

- subcapa de función de envolvente de LAPV5 (LAPV5-EF) Cláusula 9;
- subcapa de enlace de datos de LAPV5 (LAPV5-DL) Cláusula 10;
- subcapa de retransmisión de tramas de la AN (AN-FR) Cláusula 11;
- comunicación entre subcapas y función de correspondencia Cláusula 12;
- estructuras generales de protocolo de capa 3 Cláusula 13;
- especificación de protocolo de señalización RTPC Cláusula 14;
- protocolo de control Cláusula 15;
- protocolo de control de enlace Cláusula 16;
- protocolo BCC Cláusula 17;
- protocolo de protección Cláusula 18.

La información del canal D de la RDSI procedente de los puertos AB-RDSI y AVP-RDSI será multiplexada en la capa 2 y retransmitida por tramas a través de la interfaz V5.2. La capacidad de separar los datos de tipo p y f de los datos de señalización de tipo Ds en diferentes canales de comunicación será soportada por la AN y la LE, pero, como opción de aprovisionamiento, será posible transportarlos por un solo canal de comunicación (véase también 8.4).

En el Anexo E se presenta una sinopsis de los puntos de código de mensaje y de los formatos de trama utilizados en la interfaz V5.2.

La especificación del protocolo para los puertos RTPC se da en la Recomendación G.964 [8].

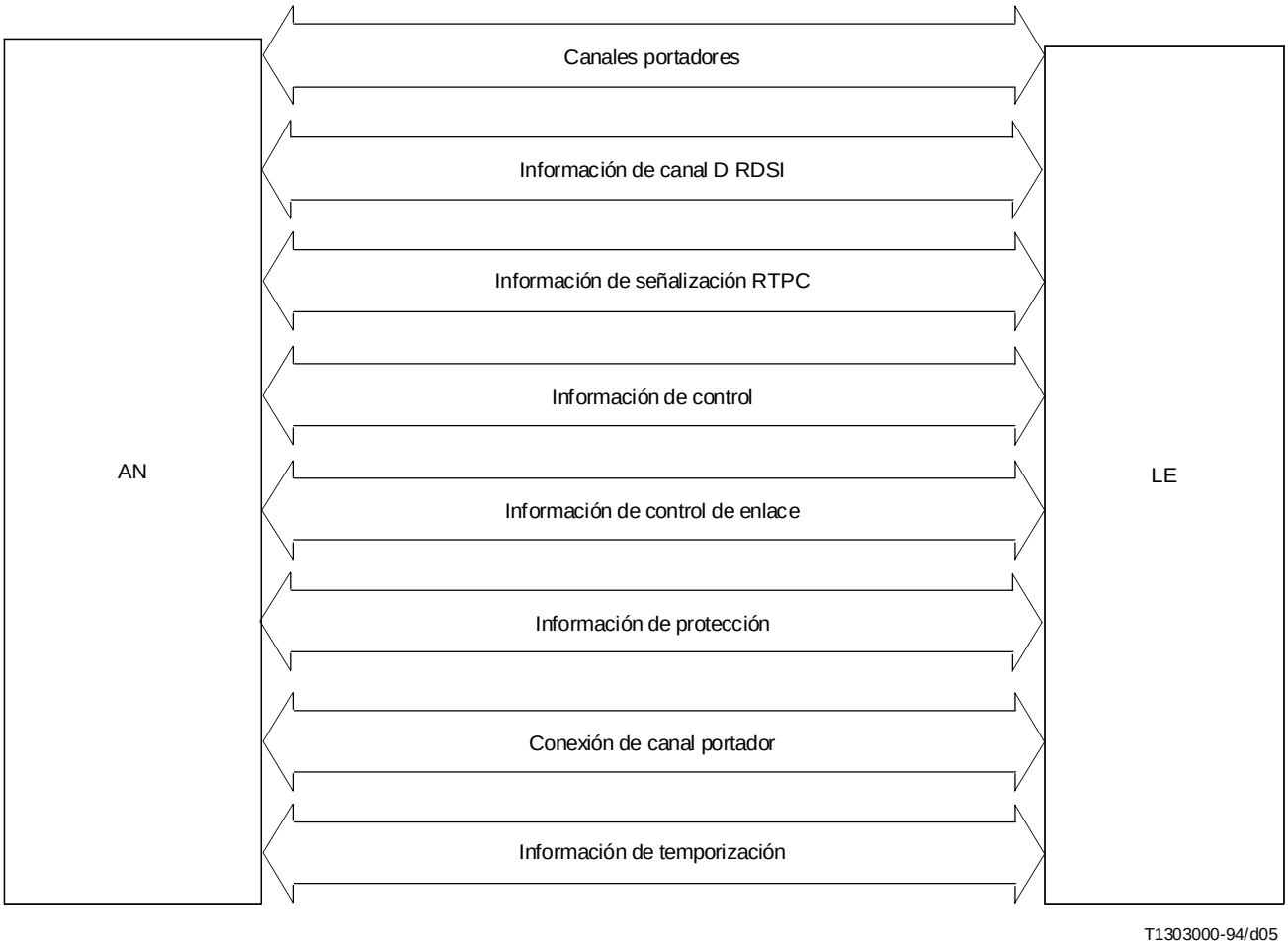


FIGURA 5/G.965

Descripción funcional de la interfaz V5.2

8.3 Intervalos de tiempo

Habrá como mínimo uno y como máximo 16 enlaces a 2048 kbit/s en una interfaz V5.2. Cada uno de éstos tendrá una capa 1 estructurada de conformidad con las cláusulas 4 y 5.

Los intervalos de tiempo 16, 15 y 31 de cada enlace a 2048 kbit/s pueden utilizarse como canales de comunicación físicos y se asignarán según proceda en el aprovisionamiento.

Los intervalos de tiempo no aprovisionados como canales de comunicaciones físicos pueden utilizarse como canales portadores bajo el control del protocolo BCC.

8.4 Asignación de intervalos de tiempo para canales de comunicación físicos

En el caso de un solo enlace a 2048 kbit/s, la asignación de intervalos de tiempo para los canales C físicos será la misma que para los canales C físicos en la Recomendación G.964 [8], con el fin de garantizar la compatibilidad total con V5.1.

En el caso en que la interfaz V5.2 esté constituida por más de un enlace a 2048 kbit/s, se utilizará el protocolo de protección. En este caso, el intervalo de tiempo 16 del enlace primario contendrá el protocolo de protección y cualquier trayecto C que haya sido aprovisionado en el mismo canal C. El intervalo de tiempo 16 del enlace secundario contendrá también el protocolo de protección.

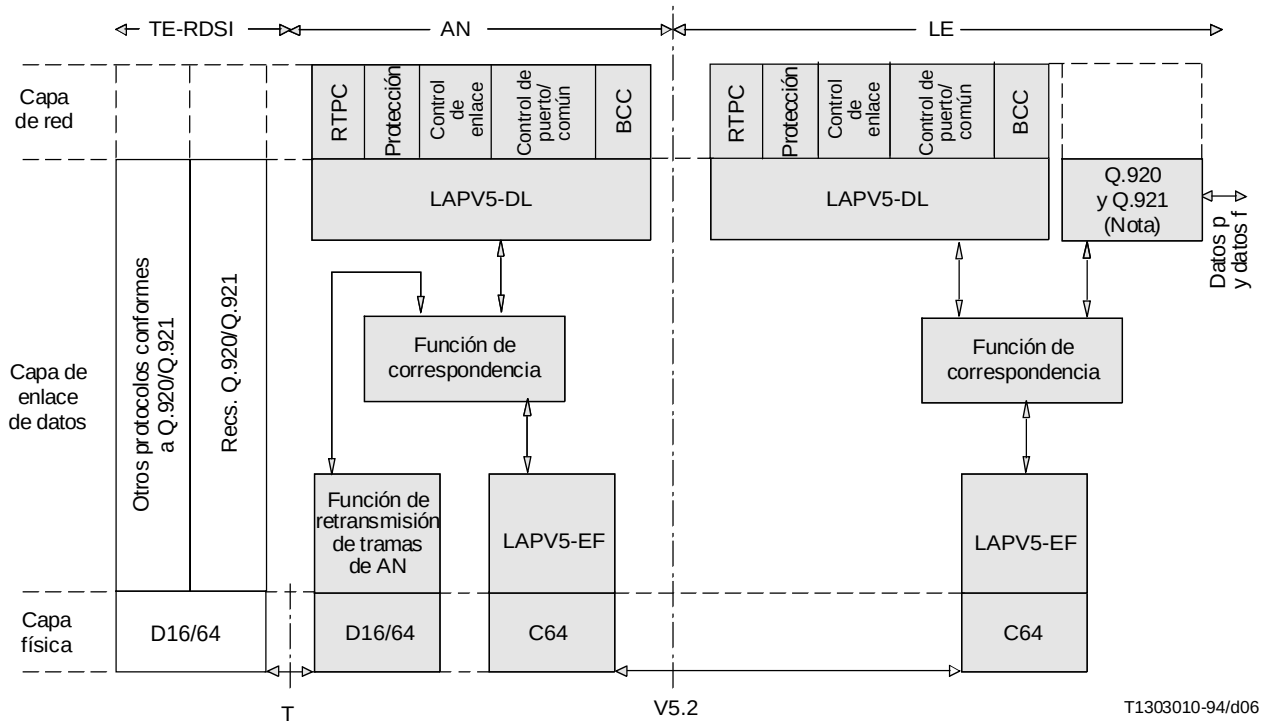
Los demás canales C físicos se asignarán de preferencia conforme a la secuencia siguiente:

- los intervalos de tiempo 16 de los enlaces a 2048 kbit/s restantes según proceda. Si se requieren más, entonces:
- el intervalo de tiempo 15 de un enlace a 2048 kbit/s. Si se requieren aún más, entonces:

– se asignará el intervalo de tiempo 31 del mismo enlace a 2048 kbit/s. Si se requieren aún más, entonces:

– se proseguirá asignando el intervalo de tiempo 15 y luego el intervalo de tiempo 31 del siguiente enlace a 2048 kbit/s tal como se indica en la subcláusula anterior. Este proceso puede repetirse hasta que todos los intervalos de tiempo 15 y 31 de todos los enlaces a 2048 kbit/s hayan sido asignados.

Las directrices anteriores han sido creadas para obtener la máxima flexibilidad al asignar intervalos de tiempo como canales C físicos, sin imponer condiciones sobre las futuras adiciones de servicios, tales como canales H de la RDSI. No es necesario seguir el procedimiento de asignación indicado, especialmente al pasar de V5.1 a V5.2 o al aumentar la capacidad de una interfaz V5.2, dado que el ceñirse explícitamente estas directrices puede llevar a la necesidad de cambiar totalmente la disposición de los canales C físicos en una interfaz V5.2.



NOTA – Salvo las funciones terminadas en la función de retransmisión de tramas de AN en la AN.

FIGURA 6/G.965

Arquitectura de protocolo

8.4.1 Tipos de datos para trayectos C V5.2

Se han definido los siguientes tipos de datos que son transportados a través de la interfaz V5.2 como trayectos de comunicación:

a) Datos de tipo p – Estos son los datos del canal D de la RDSI con SAPI = 16;

b) Datos de tipo f – Estos son los datos del canal D de la RDSI con SAPI = 32 a 62;

c) Tipo Ds – Estos son los datos de tipo señalización por canal D de la RDSI con SAPI distinto de los anteriores.

NOTA – Se ha determinado que en el futuro podrán proporcionarse servicios que utilicen SAPI previamente reservados. El dar una asignación por defecto permite por lo menos que las primeras implementaciones de V5.2 transporten estos tipos de señalización por canal D a través de la AN, pese a que su futura asignación de tipos de datos puede cambiar.

d) RTPC – Esta es la información de señalización de la RTPC;

e) Control – Estos son los datos de información de control;

f) Control de enlace – Estos son los datos de información de control de enlace;

g) BCC – Este es un protocolo que asigna canales portadores a petición;

h) Protección – Este es un protocolo que asigna canales C lógicos a diferentes canales C físicos cuando hay fallos de enlace en una interfaz V5.2.

Los trayectos de comunicación de control, BCC, control de enlace y protección se asignarán siempre al intervalo de tiempo 16 del enlace primario en la inicialización. Los otros trayectos de comunicación se asignarán a cualquier canal C lógico, excluyendo el intervalo de tiempo 16 del enlace secundario o los que están previstos a efectos de protección.

8.4.2 Trayectos de comunicación cuando se proporciona la RTPC en una interfaz V5.2

Sólo un canal C lógico contendrá el protocolo RTPC.

8.4.3 Trayectos de comunicación cuando se proporciona la RDSI en una interfaz V5.2

Los datos de tipo p de puertos de usuario RDSI pueden colocarse en uno o más canales C lógicos.

Los datos de tipo f de puertos de usuario RDSI pueden colocarse en uno o más canales C lógicos.

Los datos de tipo Ds de puertos de usuario RDSI pueden colocarse en uno o más canales C lógicos.

Los trayectos de comunicación que transportan datos de tipo p, tipo f o tipo Ds de un puerto de usuario RDSI pueden colocarse en el mismo canal C lógico o pueden dividirse en diferentes canales C lógicos.

Los datos de tipo p de un solo puerto de usuario no se dividirán en diferentes canales C lógicos.

Los datos de tipo f de un solo puerto de usuario no se dividirán en diferentes canales C lógicos.

Los datos de tipo Ds de un solo puerto de usuario no se dividirán en diferentes canales C lógicos.

NOTA – Los datos de tipo p o de tipo f pueden también ser encaminados por una AN a través de la red de servicios de líneas arrendadas mediante el aprovisionamiento. No hay repercusiones en esta Recomendación.

8.5 Subestratificación y multiplexación de la capa 2 en canales de comunicación

La especificación de protocolo y los procedimientos para V5.2 se derivan directamente de los que figuran en 8.5/G.964 [8].

8.6 Multiplexación de la capa 3

Por lo general, la multiplexación de la capa 3 es la misma que en 8.6/G.964 [8], con las siguientes adiciones relativas a V5.2:

El protocolo de control de enlace multiplexa información en la capa 3 que es transportada a través del enlace de datos de la capa 2 de control de enlace por la interfaz V5.2. El protocolo de control de enlace se define en la cláusula 16.

El protocolo BCC multiplexa información en la capa 3 que es transportada a través del enlace de datos de la capa 2 BCC por la interfaz V5.2. El protocolo BCC se define en la cláusula 17.

El protocolo de protección multiplexa información en la capa 3 que es transportada a través de dos enlaces de datos de la capa 2 de protección, uno por el enlace primario y otro por el enlace secundario a 2048 kbit/s. El protocolo de protección se define en la cláusula 18.

8.7 Control de congestión

El contenido de esta subcláusula es idéntico al de 8.7/G.964 [8].

8.7.1 Control de flujo de extremo a extremo

El contenido de esta subcláusula es idéntico al de 8.7.1/G.964 [8].

8.7.2 Control de congestión en la interfaz V5.2

El contenido de esta subcláusula es idéntico al de 8.7.2/G.964 [8].

8.7.3 Bloqueo de puertos de usuario RDSI en la capa 2

El contenido de esta subcláusula es idéntico al de 8.7.3/G.964 [8] y abarcará asimismo los puertos AVP-RDSI.

9 Subcapa de función de envolvente de LAPV5 (LAPV5-EF)

El contenido de esta cláusula es idéntico al de la cláusula 9/G.964 [8].

10 Subcapa de enlace de datos de LAPV5 (LAPV5-DL)

10.1 Estructura de trama para la comunicación entre pares

El contenido de esta subcláusula es idéntico al de 10.1/G.964 [8].

10.2 Tramas inválidas

El contenido de esta subcláusula es idéntico al de 10.2/G.964 [8].

10.3 Elementos de procedimientos y formatos de campos para la comunicación entre pares de la subcapa de enlace de datos

10.3.1 Formato del campo de dirección de enlace

El contenido de esta subcláusula es idéntico al de 10.3.1/G.964 [8].

10.3.2 Variables del campo de dirección de enlace

10.3.2.1 Bit de extensión del campo de dirección (EA)

El contenido de esta subcláusula es idéntico al de 10.3.2.1/G.964 [8].

10.3.2.2 Bit del campo de instrucción/respuesta

El contenido de esta subcláusula es idéntico al de 10.3.2.2/G.964 [8].

10.3.2.3 V5DLaddr

La V5DLaddr será un número de 13 bits. No se utilizarán valores en la gama de 0 a 8175 para identificar una entidad de protocolo de capa 3, porque esa gama se utiliza para identificar puertos de usuario RDSI.

En el Cuadro 1 se indican los valores definidos de la V5DLaddr.

10.4 Definición de los procedimientos entre pares de la subcapa de enlace de datos

El contenido de esta subcláusula es idéntico al de 10.4/G.964 [8].

11 Subcapa de retransmisión de tramas de la AN

El contenido de esta cláusula es idéntico al de la cláusula 11/G.964 [8].

12 Comunicación entre subcapas y función de correspondencia

El contenido de esta cláusula es idéntico al de la cláusula 12/G.964 [8].

CUADRO 1/G.965

Codificación de valores de dirección V5DL

Bits								V5DLaddr	
8	7	6	5	4	3	2	1		
1	1	1	1	1	1	C/R	EA	Octeto 1	
								Octeto 2	
1	1	1	0	0	0	0	EA	Señalización RTPC	(8176 decimal)
1	1	1	0	0	0	1	EA	Protocolo de control	(8177 decimal)
1	1	1	0	0	1	0	EA	Protocolo BCC	(8178 decimal)
1	1	1	0	0	1	1	EA	Protocolo de protección	(8179 decimal)
1	1	1	0	1	0	0	EA	Protocolo de control de enlace	(8180 decimal)

13 Estructuras generales del protocolo de la capa 3

13.1 Generalidades

En las interfaces V5.2 se sustentan diferentes protocolos de capa 3, que utilizan todos el mismo «discriminador de protocolo». Por consiguiente, la totalidad del conjunto de protocolos puede verse como un protocolo «V5.2» único compuesto por diferentes subprotocolos:

- protocolo RTPC;
- protocolo de control (control común y control de puerto de usuario);
- protocolo de control de enlace;
- protocolo BCC; y
- protocolo de protección.

Todos estos protocolos de capa 3 se definen como protocolos orientados a mensajes. Cada mensaje constará de las partes siguientes (elementos de información). Para cada una de ellas se indica el número de octetos (entre paréntesis):

a) discriminador de protocolo (1 octeto);

b) dirección de capa 3 (2 octetos);

c) tipo de mensaje (1 octeto); y

d) otros elementos de información, según proceda (el número de octetos depende del elemento de información).

Los elementos de información a), b) y c) estarán presentes en todos los mensajes, actuando como «encabezamiento» para cada uno de los mensajes, mientras que los elementos de información d) son específicos de cada tipo de mensaje.

Esta organización se ilustra en el ejemplo de la Figura 7.

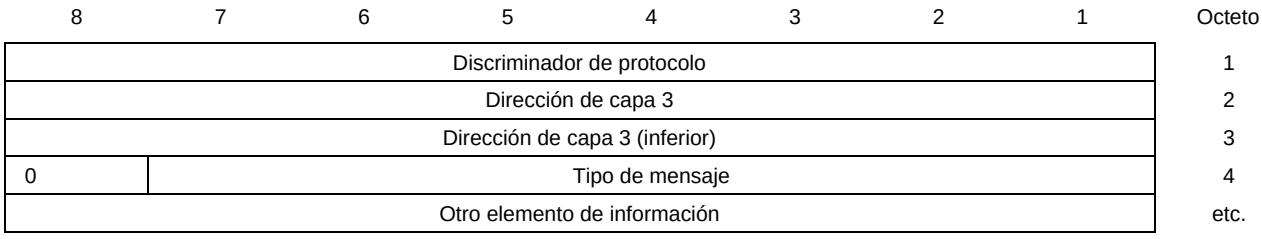


FIGURA 7/G.965

Ejemplo de organización general de los mensajes

Para todos los protocolos V5.2, cada elemento de información dado puede estar presente una sola vez en un mensaje dado.

Para cada uno de los octetos que componen cada uno de los elementos de información, el bit designado «bit 1» es transmitido primero, seguido por los bits 2, 3, 4, etc. De manera similar, para cada uno de los elementos de información, el octeto designado «octeto 1» es transmitido primero, seguido por los octetos 2, 3, 4, etc.

Cuando un campo abarca más de un octeto, el orden de los valores de los bits decrece progresivamente a medida que aumenta el número de octetos. El bit menos significativo del campo es representado por el bit de más baja numeración del octeto de más alta numeración del campo.

Los bits posibles no utilizados en la estructura de octetos de un elemento de información dado se consideran «reservados» y se codificarán como «todo 0» binario. Sin embargo, la recepción de un campo reservado no codificado de «todo 0» no causará un error de protocolo.

13.2 Elementos de información que aparecen en cada mensaje (encabezamiento)

En esta subcláusula se describen los elementos de información que aparecen en cada mensaje (actuando como encabezamiento de mensaje).

Estos elementos de información no incluyen un campo explícito de identificador de elemento de información. Por consiguiente, cada uno de ellos será identificado a partir de la posición de los octetos en cada mensaje.

13.2.1 Elemento de información discriminador de protocolo

El objetivo del elemento de información discriminador de protocolo consiste en distinguir los mensajes correspondientes a uno de los protocolos V5 (protocolo RTPC, protocolo de control, protocolo de control de enlace, protocolo BCC o protocolo de protección) definidos en la Recomendación G.964 [8] y en esta Recomendación, de otros mensajes correspondientes a otros protocolos (no definidos en estas Recomendaciones) que utilizan las mismas conexiones de enlaces de datos V5 (en este caso V5.2).

NOTA – El elemento de información discriminador de protocolo ha sido incluido en los protocolos V5 a efectos de compatibilidad de estructura con otros protocolos (por ejemplo, con la Recomendación Q.931 [6]). Proporciona un mecanismo para la compatibilidad en el futuro, permitiendo el uso de la misma conexión de enlace de datos V5 para otros protocolos de capa 3 no identificados todavía.

El elemento de información discriminador de protocolo es la primera parte de cada mensaje.

La longitud del elemento de información discriminador de protocolo será de 1 octeto.

La estructura y codificación del elemento de información discriminador de protocolo serán las que se indican en la Figura 8.

8	7	6	5	4	3	2	1	
0	1	0	0	1	0	0	0	Octeto 1

NOTA – Todos los valores están reservados.

FIGURA 8/G.965

Elemento de información discriminador de protocolo

13.2.2 Elemento de información dirección de capa 3

El elemento de información dirección de capa 3 tiene por objeto identificar la entidad de capa 3, dentro de la interfaz V5.2, a la que se aplica el mensaje transmitido o recibido.

El elemento de información dirección de capa 3 será la segunda parte de cada mensaje (situado después del elemento de información discriminador de protocolo).

La longitud del elemento de información dirección de capa 3 será de dos octetos.

La estructura del elemento de información dirección de capa 3 depende del protocolo; para el protocolo RTPC, véase 13.4.3/G.964 [8], para el protocolo de control véase 14.4.2.3/G.964 [8]. Para el protocolo de control de enlace, este elemento de información conserva el nombre dirección de capa 3, si bien se utiliza para referirse a enlaces a 2048 kbit/s (se define en 16.3.2.1). Para el protocolo BCC, este elemento de información ha sido denominado elemento de información «número de referencia BCC» y se define en 17.4.1. Para el protocolo de protección, este elemento de información ha sido denominado elemento de información «identificación de canal C lógico» y se define en 18.5.1.

13.2.3 Elemento de información tipo de mensaje

El elemento de información tipo de mensaje tiene por objeto identificar la función del mensaje que se envía o recibe.

El elemento de información tipo de mensaje será la tercera parte de cada mensaje (situado después del elemento de información dirección de capa 3).

La longitud del elemento de información tipo de mensaje será de 1 octeto.

La estructura del elemento de información tipo de mensaje será la que se indica en la Figura 9.

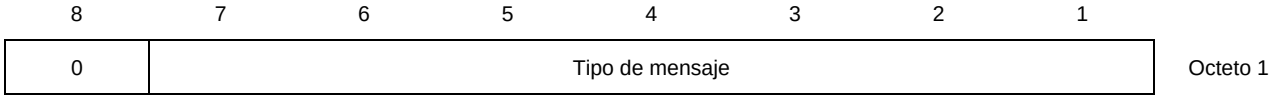


FIGURA 9/G.965

Elemento de información tipo de mensaje

La codificación del elemento de información tipo de mensaje será la que se especifica en esta Recomendación. En el Anexo E figura una lista completa de los puntos de código de mensaje.

La disposición general de la codificación del campo tipo de mensaje será la que se indica en el Cuadro 2.

CUADRO 2/G.965

Estructuras de codificación del tipo de mensaje para los protocolos V5.2

Bits							Tipo de mensaje
7	6	5	4	3	2	1	
0	0	0	–	–	–	–	Tipos de mensaje del protocolo RTPC
0	0	1	0	–	–	–	Tipos de mensaje del protocolo de control
0	0	1	1	–	–	–	Tipos de mensaje del protocolo de protección
0	1	0	–	–	–	–	Tipos de mensaje del protocolo BCC
0	1	1	0	–	–	–	Tipos de mensaje del protocolo de control de enlace
NOTA – Todos los demás valores están reservados.							

13.3 Otros elementos de información

Estos elementos de información pueden aparecer en los diferentes mensajes, y pueden ser facultativos u obligatorios, según la semántica del mensaje y/o la aplicación del protocolo del mensaje.

Estos elementos de información son específicos de cada protocolo. Para los elementos de información específicos del protocolo de la RTPC, véase 13.4/G.964 [8], para los elementos de información específicos del protocolo de control véase 14.4.4.2/G.964 [8], para los elementos de información específicos del protocolo de control de enlace véase 16.3.2, para los elementos de información específicos del protocolo BCC véase 17.4 y para los elementos de información específicos del protocolo de protección véase 18.5.

Véase el Anexo E para una lista completa de los elementos de información de V5.2.

13.4 Definición funcional y contenido de información de mensaje de protocolo

En las definiciones de protocolo de esta Recomendación, los diferentes mensajes se especifican resaltando la definición funcional y el contenido de información (es decir, la semántica) de cada mensaje. Cada definición incluye:

a) Una breve descripción del mensaje, el sentido y el uso.

b) Un cuadro que da los elementos de información por orden de aparición en el mensaje (mismo orden relativo para todos los tipos de mensajes). Para cada elemento de información, el cuadro indica:

   1) la subcláusula de esta Recomendación que describe el elemento de información;

   2) el sentido en el que puede ser enviado: es decir, AN hacia LE, LE hacia AN, o ambos;

   3) si la inclusión es obligatoria («M») o facultativa («O»);

   4) la longitud del elemento de información, en octetos.

13.5 Juegos de códigos

Para la codificación de los elementos de información se aplican las mismas reglas definidas en 4.5.1/G.964 [8], sin la funcionalidad del elemento de información cambio, es decir, que habrá únicamente un juego de códigos.

14 Especificación del protocolo de señalización RTPC y multiplexación de capa 3

El contenido de esta cláusula es idéntico al de la cláusula 13/G.964 [8].

15 Requisitos y protocolo de control

En esta cláusula se definen los requisitos, protocolos y procedimientos de control común y de puerto en forma de especificaciones de FSM normativas que apoyan la descripción textual de los procedimientos.

15.1 Indicación y control de estado de puerto de usuario AB-RDSI

El contenido de esta subcláusula es idéntico a 14.1/G.964 [8].

15.2 Indicación y control de estado de puerto de usuario RTPC

El contenido de esta subcláusula es idéntico a 14.2/G.964 [8].

15.3 Indicación y control de estado de puerto de usuario a velocidad primaria RDSI

15.3.1 Aspectos generales

La indicación del estado del puerto de usuario RDSI se basa en la separación de responsabilidades definida entre la AN y la LE. Sólo la información del estado del puerto de usuario que es relevante para el control de la llamada influirá en la máquina de estados de la LE a través de la interfaz V5.2.

Las pruebas de puertos, por ejemplo, el funcionamiento en bucle, serán responsabilidad de la AN. Sin embargo, las pruebas que interfieren con el servicio sólo serán realizadas cuando el puerto esté «bloqueado», ya sea debido a fallo o a petición a la LE y con permiso de la misma. Esto requiere dos grupos de estados, pertinentes al protocolo de interfaz V5.2, en ambos lados:

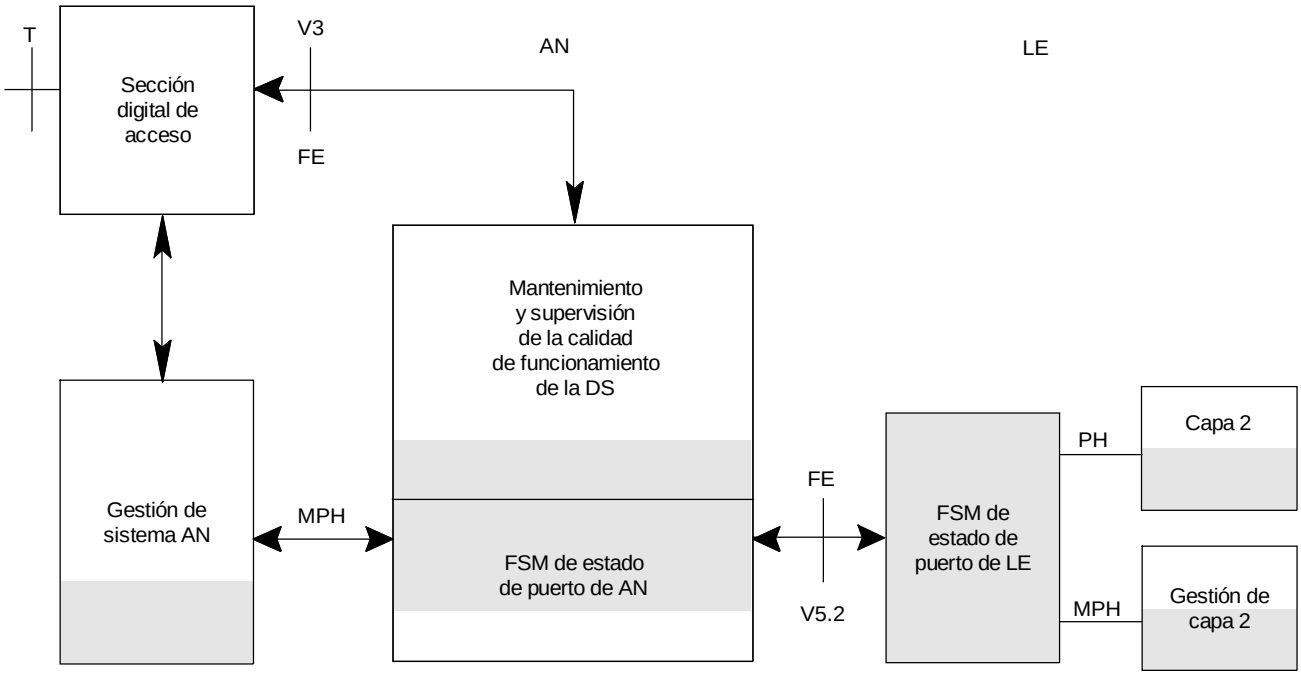
– estado operacional; y

– estado no operacional.

Se requieren estados adicionales en la AN para el mantenimiento de la DS y el puerto de usuario. El acceso a velocidad primaria RDSI está activo permanentemente en la capa 1. Si la DS detecta una pérdida de capacidad de la capa 1 en su lado usuario, el acceso será considerado como no operacional desde el punto de vista de la LE, mientras que, desde el punto de vista de la AN, la DS seguirá en condición normal. Esta distinción es hecha por la gestión de la AN y es informada a la LE utilizando elementos funcionales (FE, *function elements*) y primitivas de gestión adicionales.

En la Figura 10 se muestra el modelo funcional para el control del puerto de usuario a velocidad primaria RDSI. El sombreado indica la zona definida en esta Recomendación. La definición de las otras funciones y capacidades está fuera del ámbito de esta Recomendación. Se hace referencia al Anexo C para mayor información acerca de las hipótesis relativas a las funciones de gestión en la AN y la LE.

En lo que sigue se especifican únicamente las funciones y los procedimientos pertinentes a la interfaz V5.2.



NOTA – Los FE y las primitivas correspondientes a esta Figura se definen a continuación, en 15.3.2.

FIGURA 10/G.965

Modelo funcional de control de puerto a velocidad primaria

15.3.2 Eventos y elementos de función pertinentes al control de las máquinas de estados

En los Cuadros 3, 4, 5 y 6 se da el conjunto de FE pertinentes a la interfaz V5.2, los FE definidos en la Recomendación G.962 [10] y las primitivas (PH y MPH) hacia la capa 2 y la función de gestión en la AN o la LE (véanse también las Figuras 3/G.964 [8] y 4/G.964 [8]). En la Figura 10 se dan las definiciones y los procedimientos relativos a los FE y los eventos utilizados en los Cuadros 3 a 6.

CUADRO 3/G.965

Conjunto de elementos de función de la Recomendación G.962 [10] pertinentes a la interfaz V5.2

FE	Nombre	DS ET	Significado en ET en LE
FE-A	Funcionamiento normal de DS	→	No pertinente directamente
FE-B	Funcionamiento normal de ET	←	No pertinente directamente
FE-C	Bucle no intencional	Mantenimiento de la AN	No pertinente directamente
FE-D	LOS/LFA en TE (FC2)	Mantenimiento de la AN	No pertinente directamente
FE-E	LOS en el lado línea de NT1 (FC3)	Mantenimiento de la AN	No pertinente directamente
FE-F	LOS/LFA en el punto de referencia V3 de ET (FCL)	Mantenimiento de la AN	No pertinente directamente
FE-G	LOS/LFA en el punto de referencia T de NT1 (FC4)	Mantenimiento de la AN	No pertinente directamente
FE-H	FC3 y FC4 simultáneamente	Mantenimiento de la AN	No pertinente directamente
FE-I	Pérdida de potencia en NT1	Mantenimiento de la AN	No pertinente directamente
FE-K	FE-I y FE-D simultáneamente	Mantenimiento de la AN	No pertinente directamente
FE-L	LOS en el lado línea de LT (FC1)	Mantenimiento de la AN	No pertinente directamente

NOTA – Los FE-M a FE-P de la Recomendación G.962 [10] se refieren a fallos en un enlace digital separado y no son pertinentes. Los FE-Q a FE-T se refieren al funcionamiento en bucle y están fuera del alcance de la interfaz V5.2. Los FE-U a FE-Y están relacionados con la detección de errores CRC-4 y son pertinentes únicamente a la supervisión de la calidad de funcionamiento (véase 15.3.4).

CUADRO 4/G.965

Conjunto de elementos de función de la interfaz V5.2

FE	Nombre	AN LE	Descripción
FE201	Desbloqueo	←	Petición o acuse de recibo
FE202	Desbloqueo	→	Petición o acuse de recibo
FE203	Bloqueo	←	Instrucción
FE204	Bloqueo	→	Instrucción
FE205	Petición de bloqueo	→	Petición
FE206	Grado de servicio	→	Información de calidad de funcionamiento (Nota 1)
FE207	Bloqueo canal D	←	Instrucción (Nota 2)
FE208	Desbloqueo canal D	←	Instrucción (Nota 2)
FE209	TE fuera de servicio	→	Indicación de fallo de usuario
FE210	Fallo dentro de la red	→	Indicación de fallo de red

NOTAS

1 La información del grado de servicio puede ser enviada por la gestión AN cuando está en el estado AN/LE2.0; véase también 15.3.4.

2 Las instrucciones «bloqueo canal D» y «desbloqueo canal D» se utilizarán para interrumpir o reanudar el funcionamiento del canal D hacia el origen de un puerto de usuario RDSI de acuerdo con el requisito indicado en 8.7.3/G.964 [8]. Estas instrucciones pueden aparecer cuando se está en el estado AN/LE2.0 sin cambio de estado.

Los elementos de función son comunicados por la DS inmediatamente después de la detección de un evento. El efecto en el control del puerto, que es relevante para los procedimientos de control de llamada, será diferido mediante un procedimiento de comprobación de persistencia apropiado. Esto está fuera del ámbito de la presente Recomendación y no se refleja en la FSM de la AN (puerto primario RDSI). Se hace referencia a la Recomendación I.431 [9] que da un ejemplo de procedimiento de comprobación de persistencia adecuado.

CUADRO 5/G.965

Conjunto de primitivas en la LE

Primitiva	FSM L2/Gestión	Descripción
MPH-UBR	←	Petición de desbloqueo
MPH-UBR	→	Petición de desbloqueo
MPH-UBI	→	Indicación de desbloqueo
MPH-BI	←	Instrucción de bloqueo
MPH-BI	→	Instrucción de bloqueo
MPH-BR	→	Petición de bloqueo entrante
PH/MPH-AI	→	Acceso activado (operacional)
PH/MPH-DI	→	Acceso desactivado (no operacional)
MPH-UF	→	Indicación de fallo de usuario
MPH-NF	→	Indicación de fallo de red
MPH-GI	→	Información de grado de servicio con parámetro (Nota 1)
MPH-DB	←	Bloqueo canal D desde puerto de usuario (Nota 2)
MPH-DU	←	Desbloqueo canal D desde puerto de usuario (Nota 2)

NOTAS

1 La información de grado de servicio puede ser enviada por la gestión AN cuando está en el estado LE2.0; véase también 15.3.4.

2 Las instrucciones «MPH-DB» y «MPH-DU» se utilizarán para interrumpir o reanudar el funcionamiento del canal D hacia el origen de un puerto de usuario RDSI de acuerdo con el requisito indicado en 8.7.3/G.964 [8]. Estas instrucciones pueden aparecer cuando se está en el estado LE2.0 sin cambio de estado.

15.3.3 FSM de puerto de usuario AVP-RDSI, AN (puerto RDSI) y LE (puerto RDSI)

Las primitivas, elementos de funciones y tablas de estado se proporcionan para la definición del comportamiento funcional y la cooperación entre los distintos bloques funcionales. No hay restricciones para la realización de estas funciones, siempre que dicha realización se ajuste a la funcionalidad definida en la presente Recomendación en la interfaz V5.2 y a la sección digital de acceso a velocidad primaria.

CUADRO 6/G.965

Conjunto de primitivas de gestión en la AN pertinentes a la interfaz V5.2

Primitiva	FSM de gestión	Descripción
MPH-UBR	→	Petición de desbloqueo
MPH-UBR	←	Petición de desbloqueo
MPH-UBI	←	Indicación de desbloqueo
MPH-BI	→	Instrucción de bloqueo
MPH-BI	←	Instrucción de bloqueo
MPH-BR	→	Petición de bloqueo
MPH-NOF	←	Usuario y DS normal
MPH-EIc	←	Mantenimiento de la AN
MPH-EId	←	Mantenimiento de la AN
MPH-EIe	←	Mantenimiento de la AN
MPH-EIg	←	Mantenimiento de la AN
MPH-EIh	←	Mantenimiento de la AN
MPH-EIi	←	Mantenimiento de la AN
MPH-EIk	←	Mantenimiento de la AN
MPH-EIl	←	Mantenimiento de la AN
MPH-EIlos	←	Mantenimiento de la AN
MPH-UF	→	Indicación de fallo de usuario
MPH-NF	→	Indicación de fallo de red
MPH-GI	→	Información de grado de servicio con parámetro (Nota 1)
MPH-DB	←	Bloqueo canal D desde puerto de usuario (Nota 2)
MPH-DU	←	Desbloqueo canal D desde puerto de usuario (Nota 2)
MPH-PAR	→	Petición de funcionamiento de puerto para capacidad PL
MPH-PAI	←	Indicación de funcionamiento de puerto para capacidad PL
MPH-PDR	→	Petición de no funcionamiento de puerto para capacidad PL
MPH-PDI	←	Indicación de no funcionamiento de puerto para capacidad PL
MPH-LxAR	→	Activar bucle
MPH-AI	←	Indicación de activación de bucle
MPH-DR	→	Petición de liberación de bucle

NOTAS

1 La información de grado de servicio puede ser enviada por la gestión AN cuando está en el estado AN2.0; véase también 15.3.4.

2 Las instrucciones «MPH-DB» y «MPH-DU» se utilizan para interrumpir o reanudar el funcionamiento del canal D hacia el origen de un puerto de usuario RDSI de acuerdo con el requisito indicado en 8.7.3/G.964 [8]. Estas instrucciones pueden aparecer cuando se está en el estado AN2.0 sin cambio de estado.

3 Las últimas siete primitivas no están relacionadas directamente con la interfaz V5.2, pero se indican para información y descripción completa de la reacción en la FSM al recibir estos eventos, incluso en estados pertinentes a la interfaz V5.2.

15.3.3.1 Descripción de los estados

El procedimiento aplicable al bloqueo y desbloqueo del puerto de usuario, tal como se especifica en las FSM del puerto, tiene en cuenta los principios dados en 7.1/G.964 [8].

La gestión de la AN emitirá una petición de bloqueo únicamente cuando esté en el estado operacional. Esta petición no tiene ningún efecto sobre el estado, a menos que la LE responda con FE203.

La indicación de bloqueo inmediato tiene un efecto inmediato en cualquier estado pertinente en ambas FMS. No se requiere confirmación específica de esta indicación.

El desbloqueo tiene que ser coordinado en ambos lados. Por consiguiente, una petición de desbloqueo requiere confirmación del otro lado. La coordinación es garantizada mediante los dos estados de desbloqueo. Si se recibe una indicación de bloqueo del otro lado cuando se está en el estado de desbloqueo, esto se interpretará únicamente como una ausencia de confirmación y puede ser relevante únicamente para el sistema de gestión.

La petición de desbloqueo puede ser utilizada también por el sistema de gestión para confirmar el estado de las máquinas de estado de la capa 1.

La FSM de AN definida para el puerto a velocidad primaria RDSI soporta la capacidad PL facultativa que requiere que la sección digital de acceso y el terminal de usuario puedan ser operacionales bajo el control de la AN cuando la LE no es operacional. El procedimiento utiliza los estados AN1.1 y AN3.0.

El mantenimiento de la DS y las pruebas de bucle (véase FE-Q a FE-T de la Recomendación G.962 [10]) pueden utilizar los estados adicionales AN4 que están fuera del ámbito de la presente Recomendación. A estos estados sólo se pasará desde los estados AN1.0 o AN1.2.

Al estado AN4 puede entrarse únicamente desde los estados AN1 y se retornará únicamente a AN1.0. Para armonizar las FSM de AN y LE, se enviará FE204 a la LE y entonces se podrá aplicar el procedimiento de desbloqueo.

15.3.3.2 Definición de los estados de control de puerto

Las FSM de puerto de usuario reflejan la visión de la AN y de la LE del estado de la capa 1 del puerto RDSI solamente. El control de llamada es responsabilidad del protocolo RDSI.

15.3.3.2.1 FSM del puerto de usuario AVP-RDSI – AN (puerto RDSI)

No operacional (AN1 y AN3): se ha aplicado bloqueo del canal D al puerto. Por lo tanto, ninguna información de capa 2 será retransmitida en tramas a la LE, y no se puede utilizar el puerto para originar o terminar llamadas.

Bloqueado (AN1.0): el puerto está en el estado no operacional y ninguno de los dos lados ha iniciado el desbloqueo. Se requieren dos subestados para satisfacer la especificación de interfaz usuario-red y la DS.

Desbloqueo local (AN1.1): la AN ha iniciado el desbloqueo (enviando FE202) y espera confirmación de la LE. Si bien la DS está en condición normal, la FSM de AN debe señalar al TE que el acceso no es operacional enviando RAI.

Desbloqueo a distancia (AN1.2): la LE ha iniciado el desbloqueo (enviando FE201) y espera confirmación de la AN. Se requieren dos subestados para satisfacer la especificación de interfaz usuario-red y la DS. Ello corresponde a los dos subestados de AN1.0.

NOTA – Los estados AN1.1 y AN1.2 proporcionan un mecanismo para el desbloqueo sincronizado de los puertos. La AN puede permanecer en estos estados durante un periodo de tiempo indeterminado.

PL operacional (AN3): la gestión de la AN ha iniciado el funcionamiento del puerto para la capacidad PL cuando la LE no soporta el desbloqueo del puerto (AN1.1). En caso de informe de fallo procedente de la DS o a petición de la gestión de la AN, la FSM del puerto AN regresa al estado AN1.02.

Operacional (AN2.0): el puerto es operacional desde el punto de vista de la AN y la LE, pueden establecerse enlaces de capa 2 (y de capa 3) y el puerto puede utilizarse para originar o terminar llamadas.

15.3.3.2.2 FSM de puerto de usuario AVP-RDSI – LE (puerto RDSI)

No operacional (LE1): no se espera información de capa 2 en la LE, y el puerto no puede ser utilizado para originar o terminar llamadas.

Bloqueado (LE1.0): el puerto está en el estado no operacional y ninguno de los lados ha iniciado el desbloqueo.

Desbloqueo local (LE1.1): la LE ha iniciado el desbloqueo (enviando FE201) y espera confirmación de la AN.

Desbloqueo a distancia (LE1.2): la AN ha iniciado el desbloqueo (enviando FE202) y espera confirmación de la LE.

NOTA – Los estados LE1.1 y LE1.2 proporcionan un mecanismo para el desbloqueo sincronizado de los puertos. La LE puede permanecer en estos estados durante un periodo de tiempo indeterminado.

Operacional (LE2.0): la capa 1 del acceso a velocidad primaria es operacional. Pueden establecerse enlaces de capa 2 (y de capa 3). El puerto puede utilizarse para originar o terminar llamadas.

15.3.3.3 Principios y procedimientos

15.3.3.3.1 Generalidades

En las subcláusulas siguientes se describe el mecanismo aplicado en las FSM de la AN y la LE para los puertos (acceso a velocidad primaria) RDSI, que se presentan en las tablas de transición de estados pertinentes.

Se describen los mecanismos siguientes:

- bloqueo;
- petición de bloqueo;
- desbloqueo coordinado;
- indicación de fallo usuario/fallo de red;
- soporte de la capacidad de línea permanente.

15.3.3.3.2 Bloqueo

Un puerto de usuario que está en el estado operacional (AN2/LE2) puede ser bloqueado desde ambos lados. Sin embargo, la gestión de la AN no tiene conocimiento del estado de la llamada del puerto, por lo que sólo aplicará este procedimiento en condiciones de fallo u otras condiciones (cuando se haya efectuado el procedimiento de verificación de persistencia) que puedan afectar al servicio.

Cuando la gestión de la AN emite MPH-BI, la FSM envía FE204 (instrucción de bloqueo) a la LE y pasa al estado bloqueado AN1.0, subestado AN1.02, para señalar la condición no operacional al TE.

La FSM de AN puede también bloquear autónomamente el puerto cuando la DS indica una condición de fallo. El subestado apropiado soporta el control del puerto a través de la DS, tal como se especifica en las Recomendaciones pertinentes.

Cuando la gestión de la LE emite MPH-BI, la FSM envía FE203 (instrucción de bloqueo) a la AN y pasa al estado bloqueado LE1.0.

15.3.3.3.3 Petición de bloqueo

El mecanismo de petición de bloqueo permite el bloqueo no urgente del puerto (por ejemplo, mantenimiento diferible). En este caso la gestión de la AN emite una petición de bloqueo (MPH-BR) que resulta en FE205 a la LE. La FSM de la LE (LE-FSM) pasará esta petición a la gestión de la LE mediante MPH-BR.

La gestión de la LE, que conoce el estado de la llamada, puede conceder la petición emitiendo MPH-BI, que resulta en FE203 (instrucción de bloqueo) a la AN y pasa luego al estado bloqueado.

En el caso de una conexión semipermanente, la gestión de la LE no aceptará esta petición sino que enviará MPH-UB como confirmación negativa.

La gestión de la AN puede cancelar la petición de bloqueo emitiendo MPH-UBR. La gestión de la LE puede entonces recibir MPH-UBI y cancelar la petición de bloqueo (es decir, pasar por alto la petición recibida anteriormente) si el puerto no ha sido bloqueado aún. En este último caso, la LE puede iniciar el procedimiento de desbloqueo emitiendo MPH-UBR.

15.3.3.3.4 Desbloqueo coordinado

El desbloqueo de un puerto tiene que ser coordinado en ambos lados. Una petición de desbloqueo requiere confirmación del otro lado. Para garantizar esta coordinación hay dos estados de desbloqueo separados (desbloqueo local y desbloqueo distante) en ambas FSM. Este procedimiento es totalmente simétrico entre la AN y la LE. Si la LE desea desbloquear, emite MPH-UBR, envía FE201 (petición de desbloqueo) y pasa al estado «desbloqueo local» (LE1.1). La AN pasa al estado «desbloqueo distante» (AN1.2), al subestado correspondiente, como en el estado AN1.0, y envía MPH-UBR a su gestión, que puede estar de acuerdo, y responde con MPH-UBR (acuse de desbloqueo), envía FE202 y pasa al estado «operacional» (AN2.0).

Cuando la LE está en «desbloqueo local» y recibe este acuse, la FSM pasa al estado «operacional» (LE2.0) y emite MPH-UBI a su gestión. La gestión de la AN puede tomar también esta iniciativa, para lo cual se aplica el mismo procedimiento.

Cuando la AN y la LE están en el estado «desbloqueo distante» y reciben FE204 o FE203 respectivamente, el estado se reiniciará a bloqueado y se enviará MPH-BI a la gestión. Esto anula una anterior petición de desbloqueo del otro lado.

La gestión de la AN puede cancelar la petición de bloqueo emitiendo MPH-UBR. La gestión de la LE puede entonces recibir MPH-UBI y cancelar la petición de bloqueo (es decir, ignorar la petición recibida anteriormente) si el puerto no ha sido bloqueado todavía. En este último caso, la LE puede iniciar el procedimiento de desbloqueo emitiendo MPH-UBR.

15.3.3.3.5 Indicación de fallo de usuario/fallo de red

Para sustentar totalmente el servicio RDSI, la LE tiene que conocer el motivo del bloqueo del puerto, es decir si el puerto ha sido bloqueado debido a un fallo que es responsabilidad del usuario o de la red. Esta información sólo puede proporcionarse si la gestión de la AN conoce la localización del fallo a partir de la información suministrada por la sección digital de acceso y las capacidades de detección de fallo internas. Las condiciones de fallo (FC, *failure conditions*) 2 y 4 (FE-G únicamente, FE-G y FE-K juntas, bajo ciertas condiciones) se entienden como fallos de usuario, pero la AN puede confirmarlo aplicando la localización de fallo antes de la indicación a la LE. La identificación de «pérdida de potencia en NT1» (FE-I) como fallo de usuario o fallo de red depende de la disposición adoptada para la alimentación de NT1.

La gestión de la AN informará a la gestión de la LE enviando la información apropiada (MPH-UF o MPH-NF) a la FSM de la AN (puerto primario RDSI) que enviará FE209 o FE210 a la FSM de la LE (puerto primario RDSI) respectivamente. La FSM de la LE informará entonces en consecuencia a la gestión de la LE.

15.3.3.3.6 Soporte de la capacidad de línea permanente

Dado que el puerto de usuario a velocidad primaria está activo permanentemente, no existe ningún requisito especial para el control del puerto a velocidad primaria V5.2, además de los procedimientos ya definidos. Si la LE bloquea el puerto de usuario o, si después de restablecimiento a partir de un fallo en la DS o el TE, el procedimiento de desbloqueo no es admitido por la LE, la gestión de la AN puede llevar el puerto de usuario a PL operacional emitiendo MPH-PAR. La FSM de la AN pasará al estado AN3.0 y confirmará mediante MTH-PAI. Con MPH-PDR, la gestión de la AN puede inhabilitar la capacidad PL, a lo que la FSM responderá mediante un cambio al estado AN1.02 y MPH-PDI. Este procedimiento no es relevante para la LE.

15.3.3.4 FSM del puerto RDSI en la AN

La FSM del puerto de usuario AVP-RDSI se define en el Cuadro 7 de conformidad con la Figura 10.

CUADRO 7/G.965

FSM de la AN (puerto primario RDSI) para puertos de usuario AVP-RDSI

Estado	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
Nombre del estado Evento	Bloqueado 1	Bloqueado 2	Desbloqueo local	Desbloqueo distante 1	Desbloqueo distante 2	Acceso operacional	PL operacional
Señal a V3	NOF	RAI	RAI	NOF	RAI	NOF	NOF
FE201	MPH-UBR 1.21	MPH-UBR 1.22	MPH-UBI 2.0	MPH-UBR –	MPH-UBR –	FE202; MPH-UBI –	MPH-UBI 2.0
FE203	–	–	MPH-BI 1.02	MPH-BI 1.01	MPH-BI 1.02	MPH-BI 1.02	MPH-BI –
MPH-UBR	MPH-BI –	FE202 1.1	FE202 –	FE204; MPH-BI 1.01	FE202; MPH-UBI 2.0	FE202; MPH-UBI –	MPH-PAI –
MPH-BI	FE204 –	FE204 –	FE204 1.02	FE204 1.01	FE204 1.02	FE204 1.02	FE204 1.02
MPH-BR	–	–	/	/	/	FE205 –	/
NOF	MPH-NOF 1.02	MPH-NOF –	–	MPH-NOF 1.22	MPH-NOF –	–	–
LOS/LFA	MPH-EIlos 1.02	MPH-Eilos –	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02
FE-C	MPH-EIc 1.02	MPH-Eic –	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-EIc 1.02
FE-D	MPH-EId –	MPH-EId 1.01	FE204; MPH–Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-EId 1.01	FE204; MPH-EId 1.01
FE-E	MPH-EIe –	MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01
FE-G	MPH-EIg 1.02	MPH-EIg –	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02
FE-H	MPH-EIh 1.02	MPH-EIh –	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02
FE-I	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –

CUADRO 7/G.965 *(fin)*

FSM de la AN (puerto primario RDSI) para puertos de usuario AVP-RDSI

Estado	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
Nombre del estado Evento	Bloqueado 1	Bloqueado 2	Desbloqueo local	Desbloqueo distante 1	Desbloqueo distante 2	Acceso operacional	PL operacional
Señal a V3	NOF	RAI	RAI	NOF	RAI	NOF	NOF
FE-K	MPH-EIk –	MPH-EIk 1.01	FE204; MPH–EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01
FE-L	MPH-EIl 1.02	MPH-EIl –	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02
MPH-LxAR	FE-Q/R 4.x	FE-Q/R 4.x	/	FE-Q/R 4.x	FE-Q/R 4.x	/	/
MPH-UF	FE209 –	FE209 –	/	FE209 –	FE209 –	/	/
MPH-PAR	/	/	MPH-PAI 3.0	/	/	/	–
MPH-PDR	/	/	/	/	/	/	MPH-PDI 1.02
MPH-NF	FE210 –	FE210 –	/	FE210 –	FE210 –	/	/
MPH-GI	/	/	/	/	/	FE206 –	/
FE207	/	/	/	/	/	MPH-DB –	/
FE208	/	/	/	/	/	MPH-DU –	/

– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado; NOF: Tramas operacionales normales (*normal operational frames*); LOS/LFA: Pérdida de señal/pérdida de alineación de trama (*loss of signal/loss of frame alignment*).

NOTAS

1 Los estados AN4 no son pertinentes a la interfaz V5.2 y no se definen en esta Recomendación.

2 Si se ha aplicado el bloqueo de canal D al puerto de usuario después de recibir FE207, cuando se está en el estado AN2.0 y si la FSM del puerto sale del estado AN2.0, se suprimirá el bloqueo de canal D.

La FSM de la AN abarca eventos de un solo fallo procedentes de la DS, salvo cuando múltiples fallos son informados por la DS, es decir FE-H y FE-K. La detección de un nuevo evento significa que un fallo informado anteriormente ha desaparecido.

La FSM de la AN proporciona un mecanismo que permite al gestor local de la AN verificar que la FSM está en el estado operacional, sin tener que pasar por la secuencia de bloqueo y desbloqueo. Este mecanismo es interno de la AN. Para ello, la gestión de la AN emite MPH-UBR y recibe la información sobre si la FSM está en un estado no operacional.

15.3.3.5 FSM de puerto RDSI en la LE

El Cuadro 8 da la FSM de la LE.

CUADRO 8/G.965

FSM de la LE (puerto primario RDSI) para puertos de usuario de acceso a velocidad primaria RDSI

Estado	LE1.0	LE1.1	LE1.2	LE2.0
Nombre del estado Evento	Bloqueado	Desbloqueo local	Desbloqueo distante	Acceso operacional
MPH-UBR	FE201 1.1	FE201 –	PH/MPH-AI; FE201 2.0	FE201 –
MPH-BI	FE203 –	FE203 1.0	FE203 1.0	FE203 1.0
FE202	MPH-UBR 1.2	PH/MPH-AI 2.0	MPH-UBR –	MPH-UBI
FE204	–	MPH-BI 1.0	MPH-BI 1.0	MPH-BI; PH/MPH-DI 1.0
FE205	–	–	–	MPH-BR –
FE206	/	/	/	MPH-GI –
FE209	MPH-UF –	MPH-UF –	/	/
FE210	MPH-NF –	MPH-NF –	/	/
MPH-DB	/	/	/	FE207 –
MPH-DU	/	/	/	FE208 –

– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado.

NOTA – Si se ha aplicado el bloqueo de canal D a un puerto de usuario cuando está en el estado LE2.0 emitiendo la primitiva MPH-DB, la gestión del sistema debe saber que el bloqueo del canal D en la AN se suprimirá cuando la FSM del puerto en la AN salga del estado AN2.0.

La FSM de la LE proporciona un mecanismo que permite al gestor local de la LE verificar que la FSM está en el estado operacional emitiendo MPH-UBR, sin tener que pasar por la secuencia de bloqueo y desbloqueo.

A diferencia de la situación correspondiente para la AN, este mecanismo no es interno de la LE por lo que requiere la cooperación de la FSM de la AN, y confirma la armonización de ambas FSM y el enlace entre ellas.

En este caso la asimetría refleja la responsabilidad de la LE para sustentar el servicio.

15.3.4 Aspectos relativos a la supervisión de la calidad de funcionamiento

La calidad de funcionamiento de la sección digital de acceso a velocidad primaria, si la NT1 está realizada separadamente de la AN, será supervisada por la AN (FE-U para el sentido hacia adelante o bloque CRC-4 con error detectado en AN para el sentido hacia atrás). La aplicación de este mecanismo ha de proveerse en la AN y en la LE puerto por puerto.

Como se refleja en la Recomendación G.964 [8] (subcláusula 7.1.1, apartado 7), el concepto de trabajo es que en la interfaz V5 no debe haber repercusión de ninguna realización del puerto de usuario. Se supone que la AN supervisa la calidad de funcionamiento de la sección digital de acceso. Los parámetros para los algoritmos de validación y umbrales específicos estarán predefinidos en la AN. Sólo se informará el rebasamiento de umbral («grado de servicio» con

parámetro que indica qué grado es ahora pertinente) como máximo una vez por minuto. La LE puede utilizar estos informes para decidir si se prestará o no un servicio solicitado. Este concepto hace que la supervisión de la calidad de funcionamiento en la interfaz V5 sea independiente de la realización del acceso y no tenga efecto sobre la FSM de estados del puerto.

El rebasamiento persistente de una tasa de errores en los bits de 10^{-3} se considerará como un fallo que requiere mantenimiento (de acuerdo con las Recomendaciones de la serie M y la Recomendación G.921) y, por tanto, el bloqueo inmediato del puerto de usuario.

El uso de FE-W, FE-X y FE-Y para el mantenimiento de usuario distante bajo el control de la AN es facultativo y corresponde al operador. Esto no tiene ninguna repercusión sobre la interfaz V5.2.

15.4 Protocolo de control

El contenido de esta subcláusula es idéntico a 14.4/G.964 [8], con la excepción del Cuadro 56 de esa Recomendación, que se modifica debido a dos elementos de función de control adicionales que se requieren para el puerto a velocidad primaria RDSI. En el Cuadro 9 se muestra el Cuadro 56 modificado de la Recomendación G.964 [8].

CUADRO 9/G.965

Codificación de los elementos de función de control

Bits (octeto 3)							Elemento de función de control
7	6	5	4	3	2	1	
0	0	0	0	0	0	1	FE101 (activar acceso)
0	0	0	0	0	1	0	FE102 (activación iniciada por el usuario)
0	0	0	0	0	1	1	FE103 (DS activada)
0	0	0	0	1	0	0	FE104 ((acceso activado)
0	0	0	0	1	0	1	FE105 (desactivar acceso)
0	0	0	0	1	1	0	FE106 (acceso desactivado)
0	0	1	0	0	0	1	FE201/202 (desbloqueo)
0	0	1	0	0	1	1	FE203/204 (bloqueo)
0	0	1	0	1	0	1	FE205 (petición de bloqueo)
0	0	1	0	1	1	0	FE206 (grado de calidad de servicio)
0	0	1	0	1	1	1	FE207 (bloqueo de canal D)
0	0	1	1	0	0	0	FE208 (desbloqueo de canal D)
0	0	1	1	0	0	1	FE209 (TE fuera de servicio)
0	0	1	1	0	1	0	FE210 (fallo dentro de la red)
NOTA – Todos los demás valores están reservados.							

15.5 Procedimientos de reaprovisionamiento V5.2

El contenido de esta subcláusula es idéntico a 14.5/G.964 [8].

16 Requisitos y protocolo de control de enlace

Esta cláusula define los requisitos, protocolos y procedimientos de control de enlace en forma de especificaciones de FSM normativas con el apoyo de la descripción textual de los procedimientos.

En la interfaz V5.2, para cada enlace a 2048 kbit/s es necesario cumplir los siguientes requisitos y disponer de las siguientes funciones:

a) el estado del enlace y la identificación del enlace de capa 1 a 2048 kbit/s, según proceda (véase 16.1);

b) el bloqueo y desbloqueo coordinado de un enlace de capa 1 por la gestión (véase 16.2);

c) la verificación de la continuidad del enlace mediante la identificación del enlace (véase 16.2);

d) la coordinación de estas funciones de control de enlace (véase 16.2); y

e) el protocolo de control de enlace para la comunicación entre la AN y la LE sobre la coordinación de estas funciones en ambos lados (véase 16.3).

Todos estos requisitos se definen en esta cláusula.

En la Figura 11 se muestra el modelo funcional para el control de un solo enlace de una interfaz V5.2. Se hace referencia al Anexo C para mayor información acerca de las hipótesis relativas a las funciones de gestión en la AN y la LE.

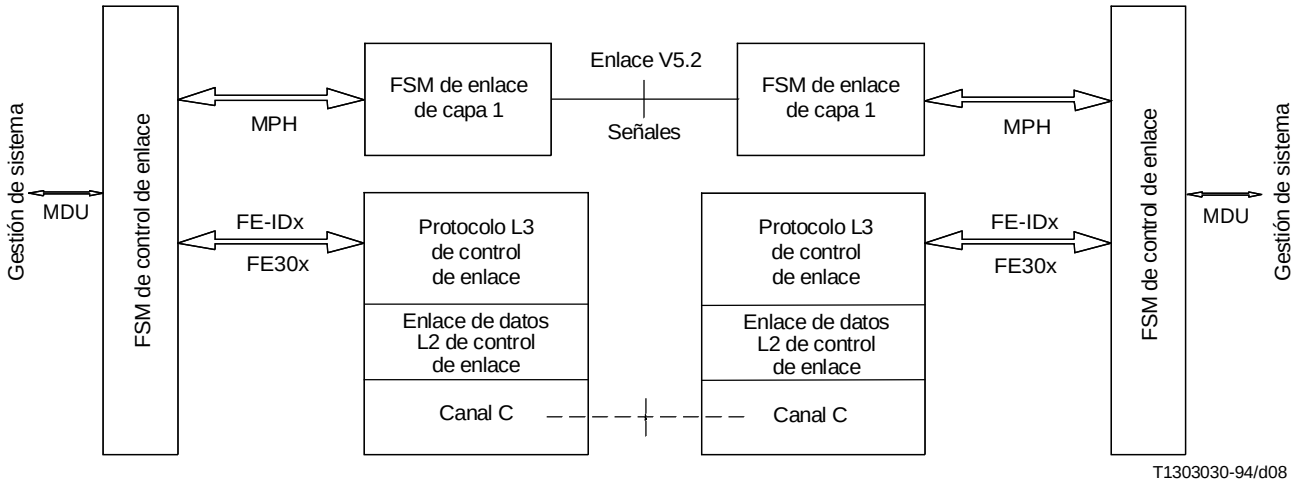


FIGURA 11/G.965

Modelo funcional de control de enlace

El modelo funcional muestra que la FSM del enlace de capa 1, que está relacionada directamente con las señales de la interfaz, reacciona de manera autónoma con relación a las funciones y los procedimientos de control de enlace. Pertenece al control del enlace coordinar los procedimientos de enlace de capa 1 y los procedimientos de control de enlace de manera que la gestión del sistema esté siempre al corriente del estado de ese enlace.

La comunicación de cada FSM de control de enlace con su FSM de enlace de capa 1 es proporcionada a través de primitivas de gestión (MPH, *management primitive*), mientras que la comunicación con la gestión del sistema utiliza unidades de datos de gestión (MDU, *management data unit*). Para la comunicación con la FSM de control de enlace distante, los FE son transferidos mediante un protocolo de capa 3 especificado en 16.3. Asimismo se envían MDU desde la entidad de protocolo de control de enlace hacia la gestión del sistema para el soporte de los procedimientos de tratamiento de errores de protocolo.

La FSM de enlace de capa 1 actúa de manera autónoma sobre las señales de capa 1 e identifica el estado del enlace de capa 1 a la FSM de control de enlace mediante MPH-DI y MPH-AI. La condición de la capa 1 será detectada en ambos lados de la interfaz de enlace de capa 1. Habida cuenta de que los temporizadores de comprobación de persistencia predefinidos pueden tener diferentes valores en la LE y la AN, la indicación a la FSM de control de enlace puede tener lugar en diferentes puntos del tiempo. En la definición de la FSM de control de enlace se han tenido en cuenta los posibles problemas resultantes.

Pertenece a la gestión del sistema de la LE decidir si el funcionamiento del enlace debe iniciarse después de la recuperación de la capa 1 de una condición de fallo (la FSM de control de enlace emite MDU-LAI) sin aplicar el procedimiento de identificación de enlace o únicamente después de la identificación fructuosa del enlace.

16.1 Requisitos de mantenimiento del enlace de capa 1 a 2048 kbit/s

16.1.1 Eventos e informes de fallo

Los requisitos y especificaciones de esta subcláusula son pertinentes a la AN y a la LE debido a la simetría de las funciones de la interfaz.

La especificación del enlace de capa 1 a 2048 kbit/s se basa en los requisitos y procedimientos de la interfaz de capa 1 V5.1. Para facilitar la comprensión del paso de V5.1 a V5.2, se muestran primero las partes comunes a V5.1 y V5.2, y luego se muestran las partes adicionales para V5.2. En el Cuadro 10 figura primero el conjunto de eventos comunes y, debajo de la línea figuran los eventos específicos de V5.2. En el Cuadro 12, los estados específicos de V5.2 que se indican como AN/LE5.1 y AN/LE5.2 aparecen señalados por líneas dobles.

En el Cuadro 10 se muestran los eventos identificados para cada enlace de capa 1 a 2048 kbit/s de una interfaz V5.2.

CUADRO 10/G.965

Eventos y primitivas para la FSM del enlace de capa 1 de la interfaz

Evento (señal)	Gestión de AN/LE	Primitiva
Señal operacional (tramas normales, no RAI)	→	MPH-AI
Condición no operacional	→	MPH-DI
Pérdida de señal	→	MPH-EIa
Pérdida de alineación de trama	→	MPH-Eia
Recepción de indicación de alarma distante (RAI)	→	MPH-EIb
Recepción de AIS (Nota 1)	→	MPH-EIc
Fallo interno	→	MPH-EId
Bloque CRC recibido con error	→	MPH-EIe
Información de error CRC (es decir bit E puesto a CERO) (Nota 2)	→	MPH-EIf
Petición de parar con informe de error (Nota 2)	←	MPH-stop
Petición de proseguir con informe de error (Nota 2)	←	MPH-proceed
Indicación de identificación de enlace	→	MPH-IDI
Envío de señal de identificación de enlace	←	MPH-ID
Retiro de señal de identificación de enlace	←	MPH-NOR
Petición de identificación de enlace	←	MPH-IDR
Fallo de identificación de enlace	→	MPH-EIg

NOTAS

1 AIS puede ser generada por el enlace de la interfaz V5.2 si ha detectado un fallo interno que le impide generar la señal de salida normal. No obstante, el lado de recepción de la interfaz detectará este evento, ya que en la alternativa de aplicación con un enlace digital transparente entre la LE y la AN, AIS puede ser generada por este enlace de conformidad con las Recomendaciones UIT-T (véase también la cláusula 4).

2 Estos eventos son relevantes para la interfaz y la relación con el sistema de gestión, pero no tienen repercusiones sobre la FSM.

Puede considerarse que las FSM de AN (interfaz) y LE (interfaz) son construidas a partir de dos estados fundamentales: operacional y no operacional. La transición a estas condiciones será notificada mediante MPH-AI o MPH-DI en la AN, y MPH-AI o MPH-DI en la LE respectivamente.

El mecanismo de informe disponible para el lado distante de la interfaz es la función RAI y la función de informe de error CRC (bit E).

16.1.2 Algoritmo de detección para eventos y señales

El algoritmo de detección para eventos y señales se define en el Cuadro 11.

CUADRO 11/G.965

Algoritmo de detección para las señales de capa 1

Tramas normales	Los algoritmos serán conformes a los que se dan en 4.1.2/G.706 [11] y 4.2/G.706 [11].
Pérdida de alineación de trama	El algoritmo será conforme al que se da en 4.1.1/G.706 [11].
RAI	RAI es detectada cuando ocurren las dos condiciones: – condición de alineación de trama; y – recepción de un bit A con contenido binario UNO.
Pérdida de señal	El equipo incluirá una o las dos alternativas siguientes para detectar la «pérdida de señal». La detección de este evento no inhibirá el funcionamiento del procedimiento de alineación de trama. a) La amplitud de la señal entrante es, durante un tiempo de al menos 1 ms más que 20 dB por debajo de la amplitud de salida nominal definida en la Recomendación G.703 [1]. b) La entrada detecta más de 10 CEROS HDB3 consecutivos.
AIS	AIS es detectada cuando ocurren las dos condiciones siguientes: – pérdida de alineación de trama; y – recepción de 512 periodos de bits que contienen menos de 3 CEROS binarios (esto se basa en 3.3.2/O.162).
Información de error CRC	Recepción de un bit E puesto a CERO.
Señal de identificación de enlace	Tramas normales recibidas con 2 de 3 bits Sa7 puestos a CERO.

16.1.3 FSM del enlace de capa 1 de la interfaz V5.2

Se han identificado tres alternativas de realización en lo concerniente al informe de detección de eventos de la FSM a la gestión y en lo concerniente a la decisión sobre la acción subsiguiente en relación con la prestación del servicio:

a) informe inmediato del evento detectado a la gestión para registro (MPH-Eie) y procesamiento a fin de evaluar el estado de la interfaz con relación a las acciones subsiguientes sobre el servicio y las demás FSM. En este caso, la gestión llevará a cabo la comprobación de persistencia necesaria de los eventos informados con el fin de identificar el estado operacional o no operacional de la interfaz; o

b) informe inmediato del evento detectado a la gestión para registro (MPH-EIe). La capa 1 realiza la comprobación de persistencia para evaluar el estado de la interfaz que da lugar a un informe de estado a la gestión (es decir, MPH-AI, MPH-DI en la AN y la LE); o

c) una combinación de las alternativas a) y b).

En el Cuadro 12 se presenta la FSM de la interfaz en la LE y la AN, enfoque simétrico. Debe observarse que esta FSM permite los tres enfoques en relación con la realización del procedimiento de comprobación de persistencia.

El o los temporizadores de comprobación de persistencia en la AN y la LE estarán predefinidos de 100 ms a 25 s, por pasos de 100 ms. El o los temporizadores de comprobación de persistencia tendrán una tolerancia de ± 50 ms para valores nominales de 100 ms a 1 s, y de $\pm$ 10 % por encima de 1 s.

La FSM de enlace capa 1 no realiza ninguna acción hacia la FSM de control de enlace en relación con el procedimiento de identificación de enlace. El motivo de esto es que debe evitarse cualquier información errónea posible si ocurren errores en los bits o problemas de coordinación. Cualquier acción hacia la FSM de control de enlace requerida es controlada por una función de control apropiada desde la FSM de control de enlace. Si la FSM de enlace de capa 1, estando en el estado 1, detecta el bit Sa7 puesto a CERO (después de realizar fructuosamente el procedimiento de comprobación de persistencia especificado), la FSM pasa al estado 5.2, a fin de mantener a disposición la información mientras permanece sin cambios el resultado del procedimiento de comprobación de persistencia. Si la FSM de control de enlace solicita mediante MPH-IDR la información de identificación de enlace, la FSM de enlace de capa 1 responderá en este caso con MPH-IDI, de no ser así con MPH-EIg, lo que indica fallo de identificación de enlace. Si la FSM de enlace de capa 1 está en uno de los estados no operacionales 2 a 4, no es posible la identificación de enlace y, por consiguiente, responderá con MPH-DI para informar y alinear la FSM de control de enlace con relación a esta situación.

CUADRO 12/G.965

FSM de enlace de capa 1 de interfaz V5.2 – AN (interfaz) y LE (interfaz)

Número del estado	AN/LE1	AN/LE2	AN/LE3	AN/LE4	AN/LE5.1	AN/LE5.2
Condición	Normal	Fallo detectado localmente	Fallo detectado a distancia	Fallo interno	Envío de ID de enlace	ID de enlace recibido
Señal enviada al lado distante	Tramas normales; Sa7 = UNO	RAI Sa7 = UNO	Tramas normales; Sa7 = UNO	AIS	Tramas normales; Sa7 = CERO	Tramas normales; Sa7 = UNO
Tramas normales, Sa7 = UNO	–	Arrancar temporizador; 1	Arrancar temporizador; 1	–	–	1
Pérdida de señal o pérdida de alineación de trama	Arrancar temporizador; MPH-EIa; 2	MPH-EIa; –	MPH-EIa; MPH-EIbr; 2	MPH-EIa; –	Arrancar temporizador; MPH-EIa; 2	Arrancar temporizador; MPH-EIa; 2
RAI	Arrancar temporizador; MPH-EIb; 3	MPH-EIdr; MPH-EIb; 3	–	–	Arrancar temporizador; MPH-EIb; 3	Arrancar temporizador; MPH-EIb; 3
AIS	Arrancar temporizador; MPH-EIc; 2	MPH-EIc; –	MPH-EIc; MPH-EIbr; 2	MPH-EIc; –	Arrancar temporizador; MPH-EIc; 2	Arrancar temporizador; MPH-EIc; 2
Fallo interno	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	–	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4
Desaparición del fallo interno	/	/	/	MPH-EIdr; 3	/	/
Expiración del temporizador de comprobación de persistencia	MPH-AI; –	MPH-DI; –	MPH-DI; –	–	/	MPH-AI; –
MPH-ID	5.1	MPH-DI; –	MPH-DI; –	MPH-DI; –	–	5.1
MPH-NOR	–	MPH-DI; –	MPH-DI; –	MPH-DI; –	1	/
Tramas normales, Sa7 = CERO	5.2	Arrancar temporizador; 5.2	Arrancar temporizador; 5.2	–	–	–
MPH-IDR	MPH-EIg; –	MPH-DI; –	MPH-DI; –	MPH-DI; –	/	MPH-IDI

– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado; MPH-EI indicación de error (el parámetro «r» significa recuperación de una condición de error informada anteriormente).

NOTAS

1 La generación de AIS puede no ser posible en todas las condiciones de fallo interno.

2 El temporizador de comprobación de persistencia arrancará al recibir el evento apropiado indicado por «arrancar temporizador». Si, debido a la recepción de otro evento, arranca otro temporizador, un temporizador que esté vigente debe ser parado y reiniciado.

Los valores de los temporizadores, que pueden ser específicos de cada evento, estarán predefinidos. Los valores de temporizador para la AN serán:

- mayores para pasar a la condición no operacional que para la LE; y
- menores para pasar a la condición operacional que para la LE.

Cuando la FSM de enlace de capa 1 recibe MPH-ID estando en el estado 1 ó 5.2, pasa al estado 5.1 y pone a CERO el bit Sa7 en el tren de bit enviado. Cuando está en el estado 5.1, al recibir MPH-NOR, la FSM regresará al estado 1 (es decir, el bit Sa7 puesto a uno). Regresa al estado apropiado al detectar una condición de fallo y enviará la señal pertinente de conformidad con la condición actual de la interfaz de enlace de capa 1.

16.1.4 Requisitos y procedimientos para las funciones adicionales

Se establecerá la alineación multitramas CRC-4 en los estados AN/LE1, AN/LE3 y AN/LE5.x y los bloques CRC detectados con error se informarán al extremo distante poniendo a CERO el bit E y a la gestión del sistema mediante MPH-EIe. La gestión del sistema puede procesar la información de error CRC de acuerdo con los umbrales predefinidos y puede reaccionar hacia el sistema operativo. Esto está fuera del ámbito de la FSM de interfaz. Una tasa de errores persistente o peor que 1 en 10^{-3} se considerará no operacional.

Puede recibirse información de error CRC-4 en los estados AN/LE1, AN/LE3, AN/LE4 y AN/LE5.x. Los bits E puestos a CERO, que pueden ser recibidos en el estado AN/LE1, se informarán a la gestión mediante MPH-EIf. La gestión puede tratar la información de error CRC de acuerdo con umbrales predefinidos y puede reaccionar hacia el sistema operativo. Esto está fuera del ámbito de la FSM de interfaz. Una tasa de errores persistente o peor que 1 en 10^{-3} se considerará no operacional.

Si la FSM de interfaz recibe la primitiva MPH-Stop (parada) de la gestión, la FSM sigue operando pero no enviará ninguna MPH-EI a la gestión. Al recibir la primitiva MPH-Proceed (proseguir), enviará el estado actual (última MPH-EI generada a la gestión y cualquier otra ulterior).

16.2 Requisitos y procedimientos de control de enlace

16.2.1 Bloqueo y desbloqueo del enlace

Existen dos tipos diferentes de peticiones de bloqueo de la AN a la LE: diferido y no diferido.

La AN puede solicitar el bloqueo no diferido de un enlace, pero la LE, en su calidad de «patrón» del servicio, decide. Si el enlace transporta uno o más canales C activos, la gestión de la LE utilizará el protocolo de protección para conmutar el o los canales C lógicos a canales C físicos de reserva. A continuación, la LE liberará todas las conexiones conmutadas en ese enlace, según proceda para el servicio, pero restablecerá las conexiones semipermanentes y reservadas de la AN en otros enlaces dentro de la misma interfaz V5.2 y enviará entonces «indicación de bloqueo» a la AN. No obstante, si no es posible proteger los canales C lógicos, la LE rechazará la petición enviando «indicación de desbloqueo» a la AN.

La AN puede también solicitar el bloqueo diferido de un enlace. En este caso, la LE inhabilitará la asignación futura de todos los canales portadores no asignados en este enlace y esperará hasta el momento en que todos los canales portadores (asignados para servicios a petición) estén no asignados. Después de ello, la LE proseguirá con la protección de los canales C lógicos y las conexiones semipermanentes y reservadas de la AN, si procede, y enviará «indicación de bloqueo» a la AN.

Sólo si la petición de bloqueo no diferido ha sido rechazada por la LE pero el bloqueo del enlace es urgentemente necesario desde el punto de vista de la AN, ésta puede bloquear un solo enlace de la interfaz V5.2 inmediatamente. Debe observarse que este bloqueo forzado de un solo enlace por la AN puede llevar toda la interfaz V5.2 a un estado no operacional, si afecta al enlace primario o secundario.

La indicación de estado de enlace de un solo enlace de una interfaz V5.2 se basa en la división de responsabilidades definidas entre la AN y LE.

Las pruebas que interfieren con cualquier servicio a través de este enlace se realizarán únicamente cuando el enlace esté en uno de los estados no operacionales, ya sea debido a un fallo o habiéndolo solicitado a la LE y obtenido su permiso. Esto requiere dos estados principales, pertinentes al protocolo de interfaz V5.2, en ambos lados:

- operacional; y
- no operacional.

16.2.2 Identificación del enlace

Este procedimiento se utiliza para comprobar la identificación de enlace de un enlace específico. Si el otro extremo puede aceptar esta petición (en particular, si no está realizando en ese momento un procedimiento similar), envía una señal física específica (bit Sa7 en el intervalo de tiempo 0 puesto a cero, mientras que de no ser así estará puesto a uno) en el enlace con la dirección indicada en el mensaje. Gracias a esto, el extremo solicitante puede comprobar que no hay discordancia entre los extremos de este enlace.

El procedimiento es simétrico y puede aplicarse desde cualquiera de los extremos del enlace a 2048 kbit/s. La identificación de enlace iniciada desde la LE tiene prioridad sobre un procedimiento iniciado por la AN en caso de colisión de peticiones de la AN y la LE.

Cuando la FSM de interfaz L1 indica a la FSM de control de enlace mediante MPH-AI que ha entrado en el estado normal, la gestión del sistema puede solicitar que se realice el procedimiento de identificación de enlace. Este procedimiento es aplicable a todos los enlaces, incluidos el primario y el secundario.

NOTA – El procedimiento de identificación de enlace puede ser realizado también por la gestión del sistema de manera programada en el tiempo. La identificación de enlace puede ser aplicada después del reaprovisionamiento. Al arrancar el sistema, la gestión del sistema o el sistema operativo pueden decidir no aplicar el procedimiento de identificación de enlace.

En la Figura 12 se ilustra el principio del procedimiento de identificación de enlace.

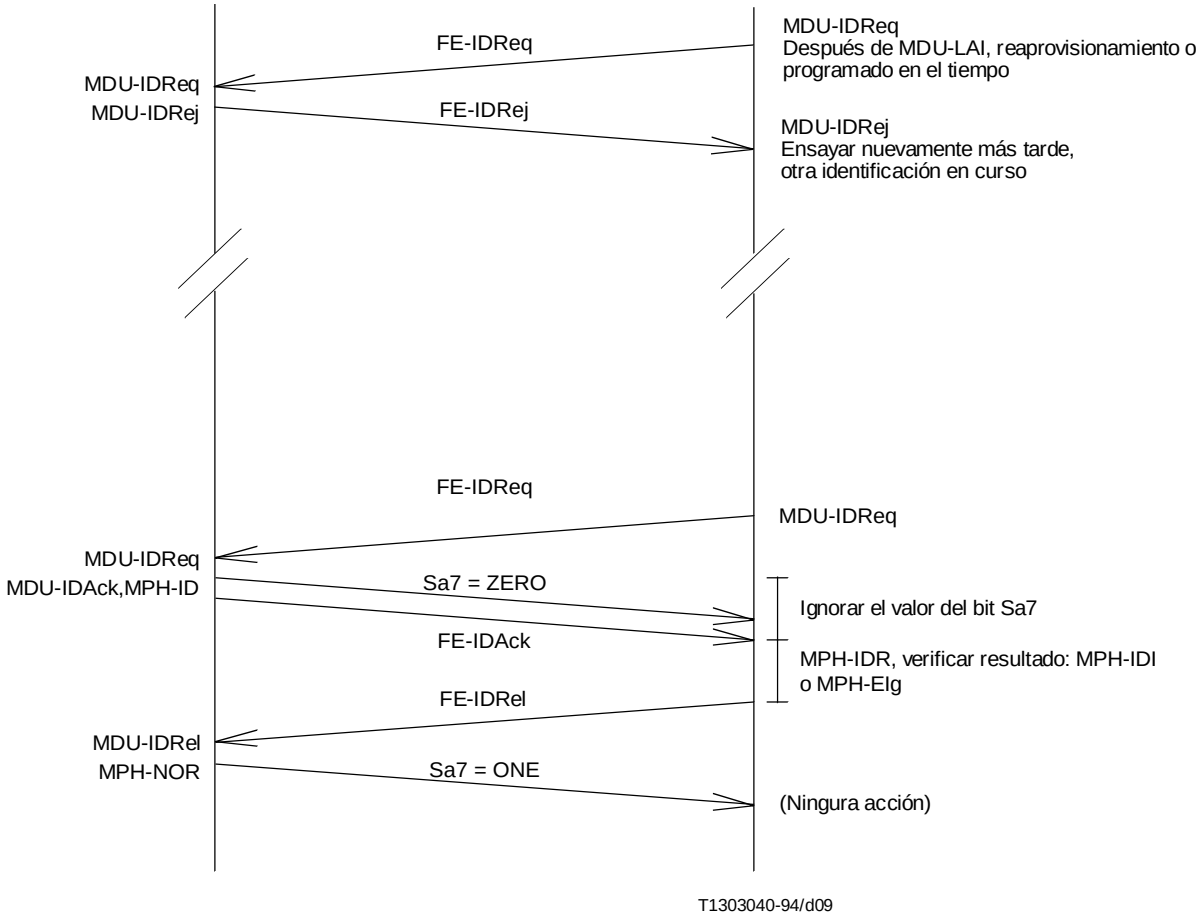


FIGURA 12/G.965

Diagrama de flechas del procedimiento funcional de identificación de enlace

16.2.3 Eventos y elementos de función pertinentes al control de las máquinas de estado del enlace

En los Cuadros 13, 14 y 15 figura el conjunto de los FE y las primitivas de gestión pertinentes a los procedimientos de control de enlace de la interfaz V5.2 y la gestión, así como las primitivas de unidades de datos de gestión hacia la FSM del enlace de capa 1 y la función de gestión del sistema en la AN o la LE.

CUADRO 13/G.965

Conjunto de elementos de función de control de enlace

FE	Nombre	AN LE	Descripción
FE-IDReq	Identificación de enlace	↔	Petición
FE-IDAck	Identificación de enlace	↔	Acuse de recibo
FE-IDRel	Identificación de enlace	↔	Petición de liberación
FE-IDRej	Identificación de enlace	↔	Indicación de rechazo
FE301	Desbloqueo de enlace	←	Petición o indicación
FE302	Desbloqueo de enlace	→	Petición o indicación
FE303	Bloqueo de enlace	←	Indicación
FE304	Bloqueo de enlace	→	Indicación
FE305	Bloqueo de enlace	→	Petición, diferido
FE306	Bloqueo de enlace	→	Petición, no diferido

CUADRO 14/G.965

Conjunto de primitivas y unidades de datos para el control de enlace en la LE

Primitiva	FSM L1 Control de enlace	Control de enlace Gestión de sistema	Descripción
MPH-AI	→		Enlace de capa 1 operacional
MDU-AI		→	Enlace operacional
MPH-DI	→		Enlace de capa 1 no operacional
MDU-DI		→	Enlace no operacional
MDU-LAI		→	Identificación de enlace requerida
MDU-IDReq		↔	Petición de identificación de enlace
MDU-IDAck		←	Envío de acuse de recibo de identificación de enlace
MPH-ID	←		Envío de identificación de enlace
MPH-IDR	←		Envío de información de identificación de enlace
MPH-IDI	→		Indicación de identificación de enlace
MPH-NOR	←		Retiro de identificación de enlace
MDU-IDRel		→	Indicación de liberación de identificación de enlace
MDU-IDRej		↔	Petición de identificación de enlace rechazada
MPH-EIg	→		Fallo de identificación de enlace
MDU-EIg		→	Indicación de fallo de identificación de enlace
MPH-EIa-f	→		Indicaciones de error de la capa 1
MDU-LUBR		↔	Petición de desbloqueo de enlace
MDU-LUBI			Indicación de desbloqueo de enlace
MDU-LBI		→	Indicación de bloqueo de enlace
MDU-LBR		↔	Petición de bloqueo de enlace, diferido
MDU-LBRN		→	Petición de bloqueo de enlace, no diferido

16.2.4 FSM de control de enlace, AN (enlace) y LE (enlace)

Se dan las primitivas, las unidades de datos, los FE y los cuadros de estado para la definición del comportamiento funcional y la cooperación entre los distintos bloques funcionales. No habrá restricciones para la realización de estas funciones siempre que la realización sea conforme a la funcionalidad definida en esta Recomendación en la interfaz V5.2, la FSM de enlace de capa 1 y la gestión de sistema.

16.2.4.1 Descripción de los estados

Las FSM de control de enlace en la AN y en la LE pueden considerarse construidas a partir de dos estados fundamentales: operacional y no operacional.

El estado no operacional se divide en 5 subestados:

- fallo de enlace de capa 1 (0.1);
- fallo de enlace de capa 1 y enlace bloqueado (0.2);
- enlace bloqueado (1.0);
- enlace local desbloqueado (1.1); y
- enlace distante desbloqueado (1.2).

CUADRO 15/G.965

Conjunto de primitivas y unidades de datos para el control de enlace en la AN

Primitiva	FSM L1 Control de enlace	Control de enlace Gestión de sistema	Descripción
MPH-AI	→		Enlace de capa 1 operacional
MDU-AI		→	Enlace operacional
MPH-DI	→		Enlace de capa 1 no operacional
MDU-DI		→	Enlace no operacional
MDU-LAI		→	Identificación de enlace requerida
MDU-IDReq		↔	Identificación de enlace solicitada
MDU-IDAck		←	Envío de acuse de recibo de identificación de enlace
MPH-ID	←		Envío de identificación de enlace
MPH-IDR	←		Envío de información de identificación de enlace
MPH-IDI	→		Indicación de identificación de enlace
MPH-NOR	←		Retiro de identificación de enlace
MDU-IDRel		→	Indicación de liberación de identificación de enlace
MDU-IDRej		↔	Petición de identificación de enlace rechazada
MPH-EIg	→		Fallo de identificación de enlace
MDU-EIg		→	Indicación de fallo de identificación de enlace
MPH-EIa-f	→		Indicaciones de error de la capa 1
MDU-LUBR		↔	Petición de desbloqueo de enlace
MDU-LUBI		→	Indicación de desbloqueo
MDU-LBI		↔	Indicación de bloqueo de enlace
MDU-LBR		←	Petición de bloqueo de enlace, diferido
MDU-LBRN		←	Petición de bloqueo de enlace, no diferido

Esta subdivisión simplifica la coordinación de ambas FSM de control de enlace en la secuencia de desbloqueo y garantiza que ambos lados acusen recibo del desbloqueo antes de pasar al estado operacional.

Las unidades de datos MDU-LUBI y MDU-LBI se utilizarán por ambas FSM de control de enlace para notificar a sus gestores una transición al y del estado operacional respectivamente.

Se acusa recibo del mecanismo para el desbloqueo de enlace, tal como se hace para la petición de bloqueo de enlace en el lado AN. No se acusa recibo del mecanismo para el bloqueo inmediato.

El estado operacional se divide en tres subestados:

- enlace operacional (2.0);
- identificación de enlace distante (2.1); e
- identificación de enlace local (2.2).

Desde el punto de vista del control de enlace, los tres subestados se consideran operacionales. Corresponde a la gestión de sistema pertinente iniciar cualquier acción subsiguiente que se requiera conforme al estado del enlace de gestión de sistema, por ejemplo, la gestión de protocolo de protección y la gestión de recursos de canal portador.

16.2.4.2 Definición de los estados de control de enlace y requisitos generales de coordinación

Las FSM de control de enlace reflejan la visión que tienen la AN y la LE del estado funcional de un solo enlace de la interfaz V5.2.

Con el fin de coordinar la condición de fallo de enlace de capa 1 y la condición de enlace bloqueado, se ha introducido el subestado 0.2 para la condición combinada de estado de enlace. Si, durante un fallo de enlace de capa 1, la gestión de sistema solicita un bloqueo, esto se indicará a la entidad distante y se entrará en el subestado 0.2. Al recuperarse el enlace de capa 1, la FSM de control de enlace pasará al estado bloqueado enviando MDU-LBI para hacer que la gestión del sistema coordine el desbloqueo, si se desea. Este procedimiento permite asimismo el recuperamiento coordinado a partir de la desalineación de la gestión de sistema, por ejemplo, la pérdida del enlace de datos de control debida al fallo del enlace de capa 1 o la pérdida de los datos de estado de gestión de sistema después del rearranque.

Una petición de desbloqueo de enlace procedente de cualquiera de los lados, estando en condición de fallo de enlace de capa 1, se considerará como una desalineación de la gestión de sistema y la FSM de control de enlace pasará al subestado 0.2 para desencadenar el desbloqueo coordinado después de la recuperación del enlace de capa 1. Se recomienda la misma acción en caso de que se reciba Pet. FE-ID (FE-IDReq) cuando la FSM está en la condición de fallo de enlace de capa 1.

16.2.4.2.1 FSM de control de enlace – AN (AN_enlace)

No operacional (AN_enlace0 y AN_enlace1): el enlace es forzado al estado fallo de enlace de capa 1 o enlace bloqueado. Por consiguiente, los canales C físicos de este enlace no se utilizarán como canales C lógicos ni como reserva. Ninguno de los intervalos de tiempo de este enlace estará disponible para control de llamada como canal portador. Se rechazará una petición de identificación de enlace.

Fallo de enlace (AN_enlace0.1): la FSM de enlace de capa 1 ha indicado pérdida persistente de la capacidad de capa 1 mediante MPH-DI.

Fallo de enlace y bloqueo (AN_enlace0.2): la FSM de enlace de capa 1 ha indicado pérdida persistente de capacidad de capa 1 mediante MPH-DI mientras el enlace estaba bloqueado o debido a acciones solicitadas por la gestión del sistema o el lado LE que pueden considerarse como desalineación de las FSM de control de enlace que requiere coordinación.

Enlace bloqueado (AN_enlace1.0): el enlace está en el estado no operacional y ninguno de los lados ha iniciado el desbloqueo.

Desbloqueo de enlace local (AN_enlace1.1): la AN ha iniciado el desbloqueo (enviando FE302) y espera confirmación de la LE.

Desbloqueo de enlace distante (AN_enlace1.2): la LE ha iniciado el desbloqueo (enviando FE301) y espera confirmación de la AN.

NOTA – Los estados AN_enlace1.1 y AN_enlace1.2 proporcionan un mecanismo para el desbloqueo sincronizado de enlaces. La AN puede permanecer en estos estados durante un periodo de tiempo indeterminado.

Enlace operacional (AN_enlace2.0): el enlace se considerará listo desde el punto de vista del control de enlace y de la capa 1 para soportar las capacidades aprovisionadas. Puede ser necesario realizar el procedimiento de identificación de enlace para verificar la continuidad del enlace.

Identificación de enlace distante (AN_enlace2.1): la LE ha iniciado la identificación del enlace y, al confirmarlo la gestión del sistema, se ha solicitado a la FSM de enlace de capa 1 que ponga el bit de identificación de enlace Sa7 a CERO. El control de enlace de la AN espera el elemento de función liberación de identificación de enlace.

Identificación de enlace local (AN_enlace2.2): la gestión del sistema de la AN ha iniciado la identificación del enlace y espera, ya sea acuse de recibo de FE-ID (FE-IDAck) de la LE o, si ya lo ha recibido, espera la indicación de identificación de enlace o el fallo de identificación de enlace, en respuesta a MPH-IDR, lo que generará entonces la información apropiada a la gestión del sistema y liberará la identificación de enlace.

16.2.4.2.2 FSM de control de enlace – LE (LE_enlace)

No operacional (LE_enlace0 y LE_enlace1): el enlace es forzado al estado fallo de enlace de capa 1 o enlace bloqueado. Por consiguiente, los canales C físicos de este enlace no se utilizarán como canales C lógicos ni como reserva. Ninguno de los intervalos de tiempo de este enlace estará disponible para control de llamada como canal portador. Se rechazará una petición de identificación de enlace.

Fallo de enlace (LE_enlace0.1): la FSM de enlace de capa 1 ha indicado pérdida persistente de la capacidad de capa 1 mediante MPH-DI.

Fallo de enlace y bloqueo (LE_enlace0.2): la FSM de enlace de capa 1 ha indicado pérdida persistente de capacidad de capa 1 mediante MPH-DI mientras el enlace estaba bloqueado o debido a acciones solicitadas por la gestión del sistema o el lado AN que pueden considerarse como desalineación de las FSM de control de enlace que requiere coordinación.

Enlace bloqueado (LE_enlace1.0): el enlace está en el estado no operacional y ninguno de los lados ha iniciado el desbloqueo.

Desbloqueo de enlace local (LE_enlace1.1): la LE ha iniciado el desbloqueo (enviando FE301) y espera confirmación de la LE.

Desbloqueo de enlace distante (LE_enlace1.2): la LE ha iniciado el desbloqueo (enviando FE302) y espera confirmación de la LE.

NOTA – Los estados LE_enlace1.1 y LE_enlace1.2 proporcionan un mecanismo para el desbloqueo sincronizado de enlaces. La LE puede permanecer en estos estados durante un periodo de tiempo indeterminado.

Enlace operacional (LE_enlace2.0): el enlace se considerará listo desde el punto de vista del control de enlace y de la capa 1 para soportar las capacidades aprovisionadas. Puede ser necesario realizar el procedimiento de identificación de enlace para verificar la continuidad del enlace. Esto incumbe a la gestión del sistema.

Identificación de enlace distante (LE_enlace2.1): la AN ha iniciado la identificación del enlace y, al confirmarlo la gestión del sistema, se ha solicitado a la FSM de enlace de capa 1 que ponga el bit de identificación de enlace Sa7 a CERO. El control de enlace de la LE espera el elemento de función liberación de identificación de enlace.

Identificación de enlace local (LE_enlace2.2): la gestión del sistema de la LE ha iniciado la identificación del enlace y espera, ya sea FE-IDAck de la AN o, si ya lo ha recibido, espera la indicación de identificación de enlace o el fallo de identificación de enlace, en respuesta a MPH-IDR, lo que generará entonces la información apropiada a la gestión del sistema y liberará la identificación de enlace.

16.2.4.3 Principios y procedimientos

16.2.4.3.1 Generalidades

La AN puede solicitar el bloqueo de un enlace específico: petición de bloqueo (diferida o no diferida, ambas con elementos de información de identificación de enlace). La LE satisfará esta petición (una vez que pueda hacerlo) y enviará una indicación de bloqueo (con el elemento de información ID de enlace). La AN puede también solicitar el desbloqueo de un enlace (bloqueado) específico: petición de desbloqueo (con el elemento de información identificación de enlace). La LE envía una indicación de desbloqueo (con el elemento de información identificación de enlace) o una indicación de bloqueo (con el elemento de información identificación de enlace). El procedimiento es simétrico y, por consiguiente, es válido también para la LE.

Únicamente si la petición de bloqueo no diferida no es fructuosa pero el bloqueo del enlace es necesario urgentemente, la AN podrá bloquear un solo enlace de la interfaz V5.2 inmediatamente. El bloqueo inmediato de un solo enlace forzado por la AN puede poner el conjunto de la interfaz V5.2 en un estado no operacional.

Todos los mensajes que llevan un elemento de función de control de enlace de un enlace específico contendrán el elemento de información identificación de enlace.

Las siguientes subcláusulas describen los mecanismos realizados en las FSM en la AN y la LE para enlaces individuales de una interfaz V5.2, que se presentan en los cuadros de transición de estados pertinentes.

Se describen los mecanismos siguientes:

- bloqueo de enlace;
- petición de bloqueo de enlace procedente de la AN (diferida o no diferida);
- desbloqueo coordinado;
- procedimiento de identificación de enlace.

16.2.4.3.2 Bloqueo de enlace

Un enlace individual de una interfaz V5.2 puede ser bloqueado desde los dos lados. La LE libera cualquier conexión conmutada en este enlace según lo apropiado para el servicio, pero restablece las conexiones semipermanentes y reservadas por la AN en otros enlaces dentro de la misma interfaz V5.2. La gestión de la LE utilizará el protocolo de protección para desplazar los canales C lógicos, si es posible y necesario.

Cuando la gestión de la LE emite MDU-LBI, la FSM envía FE303 (indicación de bloqueo de enlace) a la AN y pasa al estado enlace bloqueado LE_enlace1.0.

16.2.4.3.3 Petición de bloqueo de enlace

La AN puede solicitar el bloqueo de un enlace específico: petición de bloqueo de enlace diferida o no diferida. La LE admitirá esta petición (una vez que pueda hacerlo y después de la compleción de las acciones consecuentes) y enviará una indicación de bloqueo de enlace.

Cuando la gestión de la AN emite MDU-LBR o MDU-LBRN y el enlace está en el estado operacional, la FSM de enlace de AN enviará FE305 o FE306, según proceda. La FSM de control de enlace de LE transmitirá esta petición a la gestión del sistema de la LE mediante MDU-LBR o MDU-LBRN.

16.2.4.3.4 Desbloqueo de enlace coordinado

El desbloqueo de un solo enlace de una interfaz V5.2 tiene que ser coordinado en ambos lados. Una petición de desbloqueo de enlace requiere confirmación del otro lado antes de que el enlace sea puesto en funcionamiento. Para garantizar esta coordinación hay dos estados de desbloqueo de enlace separados (desbloqueo de enlace local y distante) en ambas FSM de control de enlace. Este procedimiento es totalmente simétrico entre la AN y la LE.

Si la gestión del sistema de la LE desea desbloquear el enlace, emite MDU-LUBR, la FSM de control de enlace emite FE301 (petición de desbloqueo) y pasa al estado «desbloqueo de enlace local» (LE_enlace1.1). Al recibir FE301, la AN pasa a «desbloqueo de enlace distante» (AN_enlace1.2) y envía MDU-LUBR a su gestión de sistema. Si la gestión del sistema de la AN acepta, responde mediante MDU-LUBI (indicación de desbloqueo de enlace), la FSM de control de enlace de AN enviará FE302 y pasará al estado «enlace operacional» (AN_L2.0). Para la FSM de control de enlace de la LE que está en «desbloqueo de enlace local» y recibe esta FE302, la FSM de control de enlace pasa a «enlace operacional» (LE_L2.0) y emite MDU-LUBI a su gestión.

La gestión del sistema de la AN puede también tomar la iniciativa, para lo cual se aplica el mismo procedimiento.

Para la FSM de control de enlace de AN y LE, al estar en el estado «desbloqueo de enlace distante» y recibir FE304 o FE303 respectivamente, el estado será repuesto a «enlace bloqueado», y se enviará una MDU-LBI a la gestión. Esto deshace una petición de bloqueo de enlace anterior procedente del otro lado.

En caso de colisión de FE301/2 y FE303/4, esto puede dar lugar a un desbloqueo descoordinado ulteriormente. Esto puede ser detectado por la gestión del sistema mediante la identificación de la secuencia de primitivas. Se recomienda que en este caso la gestión del sistema aplique el procedimiento de verificación después del desbloqueo con el fin de garantizar la coordinación de los dos lados. El desbloqueo descoordinado puede dar lugar a rechazos en el procedimiento de asignación de BCC o en el procedimiento de conmutación de protección o al uso ineficaz de recursos en la interfaz.

16.2.4.3.5 Identificación del enlace

La identificación del enlace puede ser necesaria después de una recuperación de fallo de capa 1 de enlace indicada mediante MPH-AI desde la FSM de enlace de capa 1 e indicada a la gestión de sistema mediante MDU-LAI. Corresponde a la gestión de sistema el invocar o no el procedimiento de identificación de enlace. Puede haber otros elementos dentro de la gestión del sistema que soliciten este procedimiento. Habrá únicamente una petición a la vez del procedimiento de identificación de enlace procedente de la gestión del sistema para todas las interfaces V5 de la AN o la LE.

Si el enlace primario o el secundario han sido afectados por un fallo de capa 1, la gestión del sistema no puede invocar este procedimiento si el enlace de datos de control de enlace no está (todavía) en el estado operacional indicado por indicación MDL-ESTABLECIMIENTO o confirmación MDL-ESTABLECIMIENTO. El establecimiento del enlace de control de enlace tiene prioridad en todas las circunstancias, ya que el procedimiento de identificación de enlace se basa en el funcionamiento adecuado del enlace de datos de control de enlace.

Con el fin de evitar situaciones de bloqueo interno, la colisión de la identificación del enlace invocada desde ambos lados en el mismo punto del tiempo se resuelve mediante la prioridad de la petición procedente de la LE, que contraordena la petición de la AN si la LE aún no ha acusado recibo de ella. La siguiente descripción del procedimiento es, salvo para la resolución de la colisión, simétrica y, por lo tanto, se describe como si se realizara únicamente desde un solo lado.

La identificación de enlace puede iniciarse fructuosamente únicamente cuando la FSM de control de enlace está en el estado 2.0 mediante petición MDU_ID (MDU-IDReq). En todos los demás casos, la respuesta a la gestión del sistema da un rechazo directo e indirecto con la información acerca del estado del control de enlace. Al recibir MDU-IDReq, la FSM envía petición FE-ID (FE-IDReq) al lado distante, pasa al estado 2.2 y espera el acuse de recibo de la petición, que es indicado mediante acuse de recibo FE-ID (FE-IDAck). Al recibir FE-IDAck, está implícito que la FSM de control de enlace distante ha solicitado a la FSM de enlace de capa 1 pertinente que ponga el bit Sa7 a CERO (mediante MPH-ID), lo cual es detectado entonces por la FSM de enlace de capa 1 local. Esta información no se transmite directamente a la FSM de control de enlace para evitar peticiones superpuestas de identificación del enlace.

Al estar en el estado 2.0, el lado distante que recibe FE-IDReq informa a la gestión del sistema mediante petición MDU-ID (MDU-IDReq). Si la gestión del sistema puede satisfacer esta petición, responde mediante acuse de recibo MDU-ID (MDU-IDAck) y la FSM de control de enlace envía acuse de recibo FE-ID (FE-IDAck) y pasa al estado 2.1.

Al recibir FE-IDAck, la FSM de control de enlace solicita la información de identificación de enlace emitiendo MPH-IDR a la FSM de enlace de capa 1, que devuelve entonces la información pertinente, ya sea MPH-IDI o MPH-EIg, que está presente en ese punto del tiempo en la FSM de enlace de capa 1. La FSM de control de enlace informa a la gestión del sistema mediante la MDU apropiada, ya sea MDU-AI, que es la indicación de identificación de enlace fructuosa, o mediante MDU-EIg o MDU-DI, si la FSM de enlace de capa 1 está en condición de fallo en este punto del tiempo, que son las indicaciones de identificación de enlace infructuosas. Independientemente de la información enviada a la gestión del sistema, la FSM de control de enlace solicitará la liberación de la identificación de enlace en el lado distante y pasará al estado 2.0. Esto es hecho mediante liberación FE-ID (FE-IDRel), que hace que el bit Sa7 sea repuesto a UNO (mediante MPH-NOR desde la FSM del control de enlace distante hacia la FSM de enlace de capa 1).

Si la gestión del sistema distante no puede satisfacer la petición de identificación de enlace, emite rechazo MDU-ID (MDU-IDRej) hacia la FSM de control del enlace, que rechazará la petición mediante rechazo FE-ID (FE-IDRej). Esto provoca información subsiguiente desde la FSM de control de enlace local hacia la gestión del sistema mediante rechazo MDU-ID (MDU-IDRej).

Corresponde a la gestión del sistema realizar las acciones apropiadas al recibir cualquier información procedente de la FSM de control de enlace, por ejemplo, MDU-IDRej, MDU-IDRel, MDU-AI, MDU-Elg, MDU-DI, como resultado de un procedimiento de identificación de enlace que la gestión del sistema ha solicitado a la FSM de control del enlace.

16.2.4.4 FSM de control de enlace en la AN

En el Cuadro 16 figura la FSM de control de enlace de la AN.

La FSM de control de enlace en la AN proporciona un mecanismo gracias al cual el gestor del sistema de la AN puede verificar que la FSM de control de enlace está en el estado operacional, sin tener que pasar por la secuencia de bloqueo y desbloqueo. Este es un mecanismo interno de la AN. Para hacerlo, la gestión del sistema de la AN emite MDU-LUBR y recibe la información sobre si la FSM de control de enlace está en un estado no operacional.

16.2.4.5 FSM de control de enlace en la LE

En el Cuadro 17 figura la FSM de control de enlace de la LE.

La FSM de control de enlace de la LE proporciona un mecanismo gracias al cual el gestor del sistema de la LE puede verificar que la FSM de control de enlace está en el estado operacional, emitiendo MDU-LUBR, sin tener que pasar por la secuencia de bloqueo y desbloqueo.

A diferencia de la situación correspondiente para la AN, este mecanismo no es interno de la LE, y requiere la cooperación de la FSM de control de enlace de la AN, y confirma la alineación de ambas FSM de control de enlace cuando se recibe MDU-LUBI.

Esta asimetría refleja la responsabilidad de la LE para el soporte del servicio.

16.3 Protocolo de control de enlace

16.3.1 Definición y contenido de los mensajes del protocolo de control de enlace

El formato de los mensajes de protocolo de control de enlace corresponderá a la estructura genérica de los mensajes definida en la cláusula 13.

El conjunto completo de mensajes para el protocolo de control de enlace figura en el Cuadro 18. Las siguientes subcláusulas dan la estructura detallada de cada uno de los mensajes.

16.3.1.1 Mensaje CONTROL DE ENLACE

Este mensaje es enviado por la AN o la LE para transportar información necesaria para las funciones de control para cada uno de los enlaces individuales a 2048 kbit/s (véase el Cuadro 19).

CUADRO 16/G.965

FSM de control de enlace en la AN

Estado	AN0.1	AN0.2	AN1.0	AN1.1	AN1.2	AN2.0	AN2.1	AN2.2
Nombre de estado Evento	Fallo de enlace	Fallo y bloqueo de enlace	Enlace bloqueado	Desbloqueo de enlace local	Desbloqueo de enlace distante	Enlace operacional	Identificación de enlace distante	Identificación de enlace local
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	–	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU-LBI; 1.0	MDU-LUBR; MDU-IDRej: –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-EIg	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE304; 0.2	FE304; –	FE304; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	–	MDU-IDRej; MDU-IDReq; 2.0
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	/	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	/	–	/	/	MDU-IDRej; –	MDU-IDRej; 2.0
FE301	FE304; 0.2	FE304; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	FE302; MDU-LUBI; –	FE302; MDU-LUBI; MDU-IDRel; MPU-NOR; 2.0	FE302; MDU-IDRej; 2.0
FE303	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0
MDU-LUBR	FE304; MDU-DI; 0.2	FE304; MDU-DI; –	FE302; 1.1	FE302; –	FE302; MDU-LUBI; 2.0	FE302; MDU-LUBI; –	FE-IDRej; MDU-LUBI; MPH-NOR; 2.0	FE-IDRel; MDU-LUBI; 2.0
MDU-LBI	FE304; 0.2	FE304; –	FE304; –	FE304; 1.0	FE304; 1.0	FE304; 1.0	FE304; MPH-NOR; 1.0	FE304; 1.0
MDU-LBR	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE305; –	FE305; –	FE305; –
MDU-LBRN	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE306; –	FE306; –	FE306; –

– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado.

NOTAS

1 Se registrarán los MPH-EIa-f, pero el informe de estos eventos desde la FSM de capa 1 de interfaz puede ser suprimido mediante la utilización de MPH-EIstop (parada MPH-EI) y puede proseguir mediante MPH-EIproceed (proseguir MPH-EI).

2 El primer conjunto de eventos (MPH-AI/DI) refleja la disponibilidad de la capa 1 del enlace.

3 El segundo conjunto (MDU-IREQ ... LE-IDrej) es utilizado para el procedimiento de identificación de enlace.

4 El tercer conjunto es utilizado para el procedimiento de bloqueo de enlace.

CUADRO 17/G.965

FSM de control de enlace de la LE

Estado	LE0.1	LE0.2	LE1.0	LE1.1	LE1.2	LE2.0	LE2.1	LE2.2
Nombre de estado Evento	Fallo de enlace	Fallo y bloqueo de enlace	Enlace bloqueado	Desbloqueo de enlace local	Desbloqueo de enlace distante	Enlace operacional	Identificación de enlace distante	Identificación de enlace local
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	_	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU.LBI; 1.0	MDU-LUBR; MDU-IDRej; –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-EIg	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE303; 0.2	FE303; –	FE303; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	–	FE-IDRej; –
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	–	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	–	–	/	/	/	MDU-IDRej; 2.0
MDU-LUBR	MDU-DI; FE303; 0.2	MDU-DI; FE303; –	FE301; 1.1	FE301; –	FE301; MDU-LUBI; 2.0	FE301; –	FE301; MPH-NOR; 2.0	FE301; 2.0
MDU-LBI	FE303; 0.2	FE303; –	FE303; –	FE303; 1.0	FE303; 1.0	FE303; 1.0	FE303; MPH-NOR; 1.0	FE303; 1.0
FE302	FE303; 0.2	FE303; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	MDU-LUBI; –	MDU-IDRel; MDU-LUBI; MPH-NOR; 2.0	MDU-IDRej; MDU-LUBI; 2.0
FE304	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0
FE305	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBR; –	MDU-LBR; –	MDU-LBR; –
FE306	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBRN; –	MDU-LBRN; –	MDU-LBRN; –

– Ningún cambio de estado; / evento inesperado, ningún cambio de estado.

NOTAS

1 Se registrarán los MPH-EIa-f, pero el informe de estos eventos desde la FSM de capa 1 de interfaz puede ser suprimido mediante la utilización de MPH-EIstop (parada MPH-EI) y puede proseguir mediante MPH-EIproceed (proseguir MPH-EI).

2 El primer conjunto de eventos (MPH-AI) refleja la disponibilidad de la capa 1 del enlace.

3 El segundo conjunto (MDU-IDreq – FE-IDrej) es utilizado para el procedimiento de identificación de enlace.

4 El tercer conjunto es utilizado para el procedimiento de bloqueo de enlace.

CUADRO 18/G.965

Mensajes para el protocolo de control de enlace V5.2

Codificación dentro del elemento de información tipo de mensaje							Tipos de mensajes	Referencia (subcláusula)
7	6	5	4	3	2	1		
0	1	1	0	0	0	0	CONTROL DE ENLACE	16.3.1.1
0	1	1	0	0	0	1	ACUSE DE RECIBO DE CONTROL DE ENLACE	16.3.1.2

CUADRO 19/G.965

Contenido del mensaje CONTROL DE ENLACE

Tipo de mensaje: CONTROL DE ENLACE

Sentido: Ambos

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	Ambos	M	1
Dirección de capa 3	16.3.2.1	Ambos	M	2
Tipo de mensaje	13.2.3	Ambos	M	1
Función de control de enlace	16.3.2.2	Ambos	M	3

16.3.1.2 Mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE

Este mensaje es enviado por la AN o la LE como acuse de recibo inmediato de la recepción de un mensaje CONTROL DE ENLACE (véase el Cuadro 20).

CUADRO 20/G.965

Contenido del mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE

Tipo de mensaje: ACUSE DE RECIBO DE CONTROL DE ENLACE

Sentido: Ambos

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	Ambos	M	1
Dirección de capa 3	16.3.2.1	Ambos	M	2
Tipo de mensaje	13.2.3	Ambos	M	1
Función de control de enlace	16.3.2.2	Ambos	M	3

16.3.2 Definición, estructura y codificación de los elementos de información del protocolo de control de enlace

Los elementos de información del protocolo de control de enlace se definen en las siguientes subcláusulas y se resumen en el Cuadro 21, que da también la codificación de los bits de identificador de elemento de información. Para cada uno de los elementos de información, se suministra la codificación de los diferentes campos.

CUADRO 21/G.965

Codificación de identificador de elemento de información

Bits								Elemento de información	Referencia
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	LONGITUD VARIABLE	
0	0	1	0	0	0	0	1	Función de control de enlace	16.3.2.2

16.3.2.1 Elemento de información dirección de capa 3

El elemento de información dirección de capa 3 tiene por objeto identificar el enlace a 2048 kbit/s al que se refiere el mensaje de control de enlace.

El elemento de información dirección de capa 3 es la segunda parte de cada mensaje y se codifica como se muestra en la Figura 13.

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Octeto 1
Campo dirección de capa 3 (bajo)								Octeto 2

FIGURA 13/G.965

Elemento de información dirección de capa 3 para la identificación de enlace a 2048 kbit/s

El elemento de información dirección de capa 3 se codifica en binario.

Para un enlace individual V5 a 2048 kbit/s, el campo dirección de capa 3 (bajo) del elemento de información dirección de capa 3 tendrá el mismo valor que el campo de identificador de enlace V5 a 2048 kbit/s del elemento de información identificación de intervalo de tiempo V5 que se utiliza para el protocolo BCC.

16.3.2.2 Elemento de información función de control de enlace

Este elemento de información identifica la función de control de enlace que ha de ser transportada por el mensaje.

La estructura del elemento de información función de control de enlace será como se indica en la Figura 14.

8	7	6	5	4	3	2	1	
0	0	1	0	0	0	0	1	Octeto 1
Longitud del contenido de la función de control de enlace								Octeto 2
1 ext.	Función de control de enlace							Octeto 3

FIGURA 14/G.965

Elemento de información función de control de enlace

La codificación del contenido de este elemento de información será tal como se especifica en el Cuadro 22.

CUADRO 22/G.965

Codificación de la función de control de enlace

Bits (octeto 3)							Función de control de enlace
7	6	5	4	3	2	1	
0	0	0	0	0	0	0	FE-IDReq (petición FE-ID)
0	0	0	0	0	0	1	FE-IDAck (acuse de recibo FE-ID)
0	0	0	0	0	1	0	FE-IDRel (liberación FE-ID)
0	0	0	0	0	1	1	FE-IDRej (rechazo FE-ID)
0	0	0	0	1	0	0	FE301/302 (desbloqueo de enlace)
0	0	0	0	1	0	1	FE303/304 (bloqueo de enlace)
0	0	0	0	1	1	0	FE305 (petición de bloqueo de enlace diferido)
0	0	0	0	1	1	1	FE306 (petición de bloqueo de enlace no diferido)
NOTA – Todos los demás valores están reservados.							

16.3.3 Definiciones de los estados del protocolo de control de enlace

FUERA DE SERVICIO

Se entrará en este estado cuando el sistema arranque o cuando se reciba la MDU-parar_tráfico de la gestión del sistema.

EN SERVICIO

Se entrará en este estado cuando la entidad de control de protocolo esté en el estado FUERA DE SERVICIO y reciba una MDU-iniciar_tráfico de la gestión del sistema.

ESPERA DE ACUSE DE RECIBO DE CONTROL DE ENLACE

Se entrará en este estado cuando haya sido enviado un mensaje CONTROL DE ENLACE al enlace de datos de control de enlace.

16.3.4 Procedimientos del protocolo de control de enlace

16.3.4.1 Generalidades

Esta subcláusula especifica los procedimientos para el protocolo de control de enlace. El protocolo de control de enlace es simétrico, es decir que los procedimientos se aplican tanto al lado AN como al lado LE de la interfaz V5.2.

Existe una entidad de protocolo de control de enlace relacionada con el enlace para cada uno de los enlaces de capa 1 a 2048 kbit/s.

Además de los procedimientos anteriores, cada mensaje recibido por una entidad de control de protocolo de enlace pasará por los procedimientos de tratamiento de errores especificados en 16.3.5 antes de ser tratado ulteriormente.

La descripción del procedimiento se hace para el tratamiento de un solo evento (FE o MDU-CONTROL) en el mismo punto del tiempo. Habrá una memoria por entidad de protocolo de enlace en la AN y la LE para almacenar los eventos ulteriores que han de transmitirse en el orden recibido de la FSM. El evento siguiente será transmitido cuando la FSM de protocolo de control de enlace pertinente haya entrado en el estado 1.

Cada mensaje de protocolo de control de enlace contiene una dirección de capa 3 para identificar la entidad de protocolo de control de enlace de capa 1 particular.

Los mensajes de protocolo de control de enlace serán enviados al enlace de datos mediante una primitiva petición DL-DATOS; el servicio de enlace de datos se especifica en la cláusula 10.

16.3.4.2 Indicación iniciar tráfico

16.3.4.2.1 Funcionamiento normal

Si una entidad de protocolo de capa 3 de control de enlace recibe, en el estado FUERA DE SERVICIO, una MDU-iniciar_tráfico desde la entidad de gestión de sistema, se entrará en el estado EN SERVICIO.

16.3.4.2.2 Procedimientos excepcionales

Si una entidad de protocolo de capa 3 de control de enlace recibe, en el estado FUERA DE SERVICIO, cualquier CONTROL DE ENLACE o cualquier FE, se generará una indicación MDU-error. No hay cambio de estado.

16.3.4.3 Indicación parar tráfico

16.3.4.3.1 Funcionamiento normal

Si una entidad de protocolo de capa 3 de control de enlace recibe, en el estado EN SERVICIO o en el estado ESPERA DE ACUSE DE RECIBO DE CONTROL DE ENLACE, una MDU-parar_tráfico de la entidad de gestión del sistema, se entrará en el estado FUERA DE SERVICIO.

16.3.4.3.2 Procedimientos excepcionales

Ninguno.

16.3.4.4 Procedimiento de entidad de protocolo de capa 3 de control de enlace

Cuando la entidad de protocolo de capa 3 de control de enlace está en el estado «en servicio» y recibe un mensaje CONTROL DE ENLACE, se enviará un mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE y se enviará una primitiva FE que contiene la función de control de enlace y la dirección de capa 3 a la entidad de gestión del sistema.

Cuando la entidad de protocolo de capa 3 de control de enlace está en el estado «en servicio» y recibe de la entidad de gestión de control de enlace una primitiva FE, se enviará un mensaje CONTROL DE ENLACE que contiene la función de control de enlace y la dirección de capa 3, arrancará el temporizador LCT01 y se entrará en el estado «espera de acuse de recibo de control de enlace».

Si se recibe un mensaje CONTROL DE ENLACE en el estado «espera de acuse de recibo de control de enlace», se enviará un mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE y se enviará una primitiva FE que contiene la función de control de enlace y la dirección de capa 3 a la entidad de gestión de control de enlace.

Al recibir un mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE en el estado «espera de acuse de recibo de control de enlace», se parará el temporizador LCT01 y se entrará en el estado «en servicio».

Si se recibe una primitiva FE de la entidad de gestión de control de enlace en el estado «espera de acuse de recibo de control de enlace», se conservará la primitiva FE.

Si el temporizador LCT01 expira por primera vez en el estado «espera de acuse de recibo de control de enlace», se retransmitirá el mensaje CONTROL DE ENLACE y rearrancará el temporizador LCT01. Si el temporizador LCT01 expira por segunda vez en el estado «espera de acuse de recibo de control de enlace», se enviará una primitiva indicación MDU-error de control de enlace a la entidad de gestión del sistema y se entrará en el estado «en servicio».

16.3.5 Tratamiento de las condiciones de error

Antes de actuar sobre un mensaje, la entidad de recepción, ya sea la entidad de protocolo de control de enlace V5 de AN o la entidad de protocolo de control de enlace V5 de LE, realizará los procedimientos especificados en esta subcláusula.

Como regla general, todos los mensajes contendrán por lo menos los elementos de información discriminador de protocolo, dirección de capa 3 y tipo de mensaje. Estos elementos de información, que son el encabezamiento de todos los mensajes del protocolo de protección de enlace, se especifican en 13.2. Al recibir un mensaje con menos de cuatro octetos, la entidad de protocolo de control de enlace de recepción en la AN o la LE emitirá una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

Cada recepción de un mensaje del protocolo de control de enlace activará las comprobaciones descritas en 16.3.5.1 a 16.3.5.7 por orden de precedencia. No ocurre ningún cambio de estado durante estas comprobaciones.

Los procedimientos de tratamiento de errores en la AN y en la LE son simétricos.

Después de que el mensaje ha sido comprobado utilizando los procedimientos de tratamiento de errores y si el mensaje no ha de ignorarse, seguirán los procedimientos del protocolo de control de enlace (véase 16.3.4).

NOTA – En esta subcláusula, el término «ignorar el mensaje» significa no cambiar el contenido del mensaje.

16.3.5.1 Error de discriminador de protocolo

Cuando una entidad de protocolo de control de enlace V5 reciba un mensaje con un discriminador de protocolo codificado de manera diferente a lo especificado para el discriminador de protocolo en 13.2.1, la entidad de protocolo de enlace V5 enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

16.3.5.2 Error de dirección de capa 3

Si la dirección de capa 3 es tal que:

a) no está codificada como se especifica en 16.3.2.1; o

b) el valor no se reconoce o no corresponde a un enlace existente V5 a 2048 kbit/s, entonces:

- la entidad de protocolo de control de enlace V5 enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

16.3.5.3 Error de tipo de mensaje

Al recibir un mensaje no reconocido, la entidad de protocolo de control de enlace V5 enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

16.3.5.4 Elementos de información repetidos

Si un elemento de información obligatorio está repetido en un mensaje, la entidad de protocolo de control de enlace V5 de recepción enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

16.3.5.5 Elemento de información obligatorio faltante

Al recibir un mensaje en el que falta un elemento de información obligatorio, la entidad de protocolo de control de enlace V5 enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

16.3.5.6 Elemento de información no reconocido

Cuando se recibe un mensaje con uno o más elementos de información no reconocidos, la entidad de protocolo de control de enlace V5 retirará todos los elementos de información no reconocidos y continuará el tratamiento del mensaje; enviará también una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema.

A los efectos de los procedimientos de tratamiento de errores, los elementos de información no reconocidos serán los que no se definen en esta Recomendación.

16.3.5.7 Error de contenido de elementos de información obligatorios

Cuando se recibe un mensaje en el que un elemento de información obligatorio tiene un error de contenido, a saber:

a) la longitud no es conforme a la longitud especificada en 16.3.1; o

b) el contenido no es conocido, entonces:

– la entidad de protocolo de control de enlace V5 enviará una primitiva indicación MDU-error de protocolo de control de enlace a la gestión del sistema e ignorará el mensaje.

NOTA – A los efectos de los procedimientos de tratamiento de errores, los errores de contenido de los elementos de información son puntos de código incluidos en un elemento de información particular que no están definidos en esta Recomendación.

16.3.6 Temporizadores para el protocolo de control de enlace

En el Cuadro 23 se especifican los temporizadores para el protocolo de control de enlace en la AN y la LE. Las tolerancias de los temporizadores serán de ±10%.

CUADRO 23/G.965

Temporizadores para el protocolo de control de enlace

Número del temporizador	Valor de expiración	Estado	Causa para arrancar	Parada normal
LCT01	1 s	AN1(enlace CTRL) LE1(enlace CTRL)	Enviado mensaje CONTROL DE ENLACE	Recibido mensaje ACUSE DE RECIBO DE CONTROL DE ENLACE

16.3.7 Cuadros de estados de entidad de protocolo de capa 3 del lado AN y LE

El Cuadro 24 define las transiciones de estado de la entidad de protocolo de capa 3 de control de enlace para el lado AN de la interfaz V5.2.

El Cuadro 25 define las transiciones de estado de la entidad de protocolo de capa 3 de control de enlace para el lado LE de la interfaz V5.2.

17 Procedimientos y elementos del protocolo BCC

17.1 Generalidades

El protocolo BCC V5.2 proporciona los medios para que la LE solicite a la AN que establezca y libere conexiones entre puertos de usuarios AN especificados e intervalos de tiempo de interfaz V5.2 especificados. Permite que los canales portadores de la interfaz V5.2 sean asignados o desasignados mediante procesos independientes (llamada por llamada, canales preconectados o semipermanentes). Para un puerto de usuario dado puede haber más de un proceso activo en cualquier momento.

CUADRO 24/G.965

Cuadro de transiciones de estado de la entidad de protocolo de capa 3 de control de enlace para la AN

Estado / Evento	AN0 FUERA DE SERVICIO	AN1 EN SERVICIO	AN2 ESPERA DE ACUSE DE RECIBO DE CONTROL DE ENLACE
MDU-iniciar_tráfico	AN1	–	–
MDU-parar_tráfico	–	Parar LCT01; AN0	Parar LCT01; AN0
FE o FE conservado	Enviar indicación MDU-error de control de enlace; –	Enviar CONTROL DE ENLACE; arrancar LCT01; AN2;	Conservar el nuevo FE recibido; –
CONTROL DE ENLACE	Enviar indicación MDU-error de control de enlace; –	Enviar FE; enviar ACUSE DE RECIBO DE CONTROL DE ENLACE; –	Enviar FE; enviar ACUSE DE RECIBO DE CONTROL DE ENLACE; –
ACUSE DE RECIBO DE CONTROL DE ENLACE	Enviar indicación MDU-error de control de enlace; –	/	Parar LCT01; AN1
Primera expiración de LCT01	/	/	Repetir CONTROL DE ENLACE; arrancar LCT01; –
Segunda expiración de LCT01	/	/	Enviar indicación MDU-error de control de enlace; AN1
MAYÚSCULAS = mensaje o evento externo; minúsculas = mensaje o evento interno; – Ningún cambio de estado; / Mensaje inesperado, ningún cambio de estado.			

CUADRO 25/G.965

Cuadro de transiciones de estado de la entidad de protocolo de capa 3 de control de enlace para la LE

Estado / Evento	LE0 FUERA DE SERVICIO	LE1 EN SERVICIO	LE2 ESPERA DE ACUSE DE RECIBO DE CONTROL DE ENLACE
MDU-iniciar_tráfico	LE1	–	–
MDU-parar_tráfico	–	Parar LCT01; LE0	Parar LCT01; LE0
FE o FE conservado	Enviar indicación MDU-error de control de enlace; –	Enviar CONTROL DE ENLACE; arrancar LCT01; LE2	Conservar el nuevo FE recibido; –
CONTROL DE ENLACE	Enviar indicación MDU-error de control de enlace; –	Enviar FE; enviar ACUSE DE RECIBO DE CONTROL DE ENLACE; –	Enviar FE; enviar ACUSE DE RECIBO DE CONTROL DE ENLACE; –
ACUSE DE RECIBO DE CONTROL DE ENLACE	Enviar indicación MDU-error de control de enlace; –	/	Parar LCT01; LE1
Primera expiración de LCT01	/	/	Repetir CONTROL DE ENLACE; arrancar LCT01; –
Segunda expiración de LCT01	/	/	Enviar indicación MDU-error de control de enlace; LE1
MAYÚSCULAS = mensaje o evento externo; minúsculas = Mensaje o evento interno; – Ningún cambio de estado; / Mensaje inesperado, ningún cambio de estado.			

Se han definido los siguientes procesos soportados por el protocolo BCC:

Proceso de asignación

Este es el procedimiento utilizado por el protocolo BCC que define las interacciones entre la AN y la LE a fin de asignar un número definido de canales portadores en la interfaz V5.2 a un puerto de usuario determinado. El proceso tiene una vida finita y se terminará cuando:

a) el protocolo BCC informe de vuelta al gestor de recursos de la LE que el gestor de recursos de la AN le ha confirmado que los canales propuestos han sido asignados; o

b) la asignación no haya sido fructuosa.

En el segundo caso, toda la información pertinente es devuelta al gestor de recursos de la LE.

Proceso de desasignación

Este es el procedimiento utilizado por el protocolo BCC que define las interacciones entre la AN y la LE a fin de desasignar un número definido de canales portadores en una interfaz V5.2 de un puerto de usuario determinado. El proceso tiene una vida finita y se terminará cuando:

a) el protocolo BCC informe de vuelta al gestor de recursos de la LE que el gestor de recursos de la AN le ha confirmado que los canales propuestos han sido desasignados; o

b) la desasignación no haya sido fructuosa.

En el segundo caso toda la información pertinente es devuelta al gestor de recursos de la LE.

Proceso de verificación

Este es el procedimiento utilizado por el protocolo BCC que define las interacciones entre la AN y la LE a fin de comprobar el encaminamiento de un canal portador en la interfaz V5.2 y su conexión subsiguiente en un puerto de usuario. Los encaminamientos que tengan lugar entretanto no pueden suponerse totalmente comprobados (por lo general). El proceso se considerará terminado cuando la respuesta a la verificación sea enviada al gestor de recursos.

Para identificar un proceso, se asignará un número de referencia BCC a dicho proceso.

Las interfaces V5.2 tendrán la capacidad de admitir los tres tipos siguientes de conexión de portador:

a) conexiones conmutadas llamada por llamada en la LE y en la interfaz V5.2, con el fin de admitir los servicios conmutados de la RTPC y la RDSI, con concentración de tráfico en la AN;

b) conexiones conmutadas llamada por llamada en la LE, pero preconectadas en la interfaz V5.2 y la AN, con el fin de admitir los servicios conmutados de la RTPC y la RDSI (sin concentración de tráfico en la AN), para líneas de alta densidad de tráfico (por ejemplo, líneas PBX) y situaciones en las que el bloqueo de llamada en la AN o en la interfaz V5 es inaceptable (por ejemplo, líneas de servicio de emergencia);

c) conexiones establecidas semipermanentemente en la LE y la AN, con el fin de admitir servicios de líneas arrendadas semipermanentes (sin señalización por canal C físico o lógico asociado).

Para el tipo de conexión a) se aplicará el procedimiento BCC al comienzo y al final de cada llamada, bajo el control de llamada RTPC o RDSI de la LE.

Para los tipos de conexión b) y c) se aplicará el procedimiento BCC bajo el control de la gestión de la LE (por ejemplo, desde la interfaz Q_{LE}), según proceda para el aprovisionamiento o para cesar el servicio de línea arrendada o conmutada. La gestión de la LE no especificará un intervalo de tiempo ni un enlace a 2 Mbit/s particular de la interfaz V5, pero será informada del intervalo de tiempo y del enlace seleccionados.

Para los tipos de conexión b) y c), la gestión de la LE especificará el puerto de usuario y el intervalo de tiempo de puerto de usuario.

Las interfaces V5.2 tendrán la capacidad de establecer y liberar conexiones multiintervalos, $n \times 64$ kbit/s, donde $n = 1$ a 30, con el fin de admitir H0, H12 y los futuros servicios multivelocidad. Estas conexiones pueden ser de tipo a), tipo b) o tipo c).

Los tipos de canal DSS1 no serán visibles para la interfaz V5 pero serán tratados transparentemente como conexiones $n \times 64$ kbit/s. Las llamadas multimedios no serán visibles para la interfaz V5 pero serán tratadas transparentemente como varias conexiones independientes.

El protocolo BCC admite únicamente las conexiones entre los puertos de usuario AN y la interfaz V5.2. El protocolo no ha de admitir la conmutación interna (es decir, la conexión de puerto de usuario a puerto de usuario). Esto no excluye la conmutación interna que está totalmente bajo el control de la AN, por ejemplo, cuando una AN está aislada de su LE progenitora debido a un fallo de la interfaz V5.

NOTA – En el Anexo K se da información adicional sobre cómo es utilizado el protocolo BCC por la LE y la AN.

En la Figura 15 se muestra el modelo funcional para el protocolo BCC.

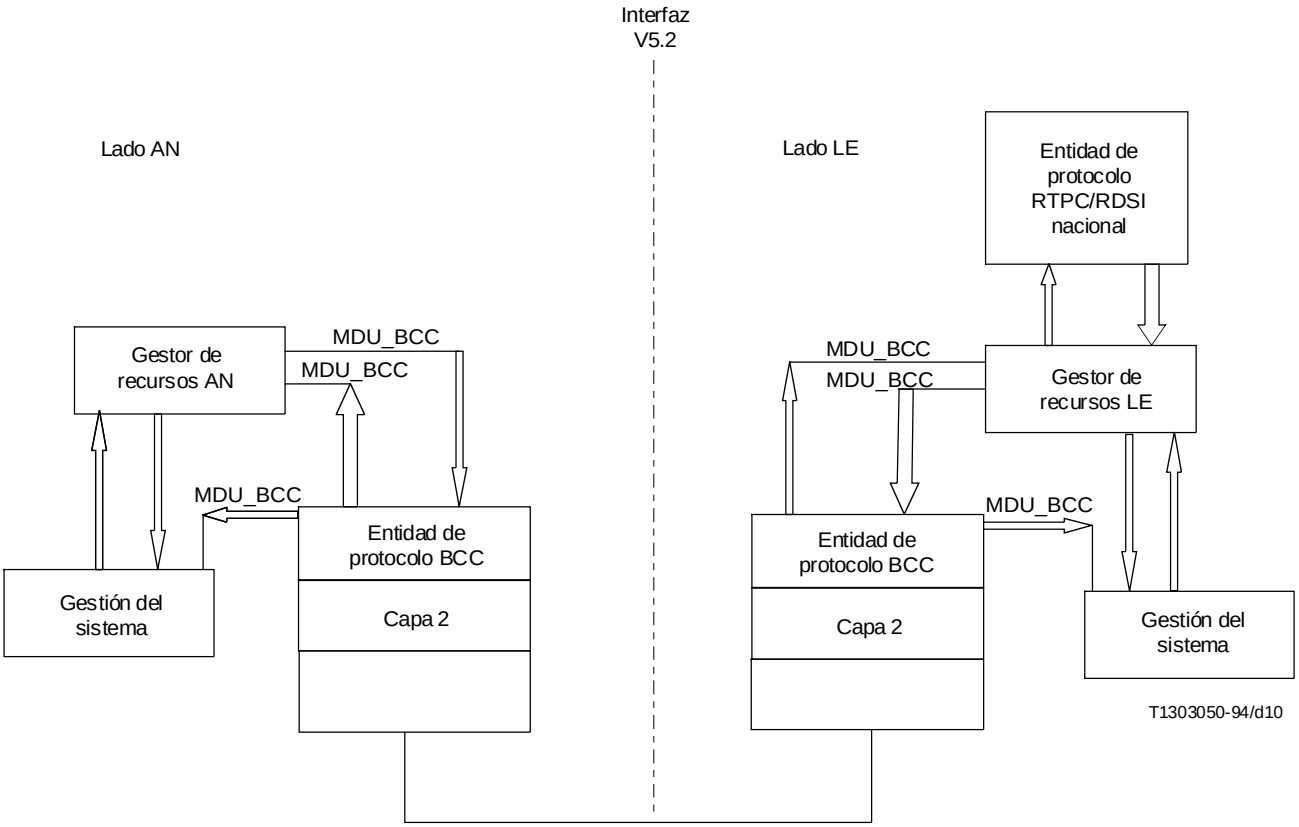


FIGURA 15/G.965

Modelo funcional para el protocolo BCC

17.2 Definición de la entidad de protocolo BCC

17.2.1 Definición de los estados del protocolo BCC

17.2.1.1 Estados BCC en la AN

Estado BCC OPERACIONAL (ANBcc0)

La entidad de protocolo BCC de la AN es esclava de la LE a los efectos de los procesos del protocolo BCC iniciados por la LE (procesos de asignación, desasignación y verificación). Para todos estos procesos, sólo se define un estado operacional («estado Bcc operacional») en la entidad de protocolo BCC de la AN.

Estado BCC INFORME DE AVERÍA DE AN (ANBcc1)

La entidad de protocolo BCC en la AN considera que un proceso está en este estado cuando ha sido enviado un mensaje AVERÍA DE AN. La AN espera la recepción de un mensaje ACUSE DE RECIBO DE AVERÍA DE AN antes de la expiración del temporizador Tbcc5.

17.2.1.2 Estados BCC en la LE

Estado BCC NULO (LEBcc0)

La entidad de protocolo BCC en la LE considera que un proceso está en este estado cuando no está todavía relacionado con ningún procedimiento de asignación o desasignación.

Estado BCC ESPERA DE ASIGNACIÓN (LEBcc1)

La entidad de protocolo BCC en la LE considera que un proceso está en este estado cuando ha sido enviado un mensaje ASIGNACIÓN. La LE espera la recepción de un mensaje ASIGNACIÓN COMPLETA o de un mensaje RECHAZO DE ASIGNACIÓN antes de la expiración del temporizador Tbcc1.

Estando en este estado puede también ocurrir una petición interna de iniciación de una desasignación (aborto de asignación).

Estado BCC ABORTO DE ASIGNACIÓN (LEBcc2)

La entidad de protocolo BCC en la LE considera que un proceso está en este estado cuando ha sido enviado un mensaje DESASIGNACIÓN estando en el estado BCC espera de asignación. La LE espera ahora la recepción de un mensaje DESASIGNACIÓN COMPLETA o de un mensaje RECHAZO DE DESASIGNACIÓN antes de la expiración del temporizador Tbcc2.

Estado BCC ESPERA DE DESASIGNACIÓN (LEBcc3)

La entidad de protocolo BCC en la LE considera que un proceso está en este estado cuando ha sido enviado un mensaje DESASIGNACIÓN. La LE espera la recepción de un mensaje DESASIGNACIÓN COMPLETA o de un mensaje RECHAZO DE DESASIGNACIÓN antes de la expiración del temporizador Tbcc3.

Estado BCC ESPERA DE VERIFICACIÓN (LEBcc4)

La entidad de protocolo BCC en la LE considera que un proceso está en este estado cuando ha sido enviado un mensaje VERIFICACIÓN. La LE espera la recepción de un mensaje VERIFICACIÓN COMPLETA antes de la expiración del temporizador Tbcc4.

17.2.2 Definición de las primitivas, los mensajes y los temporizadores del protocolo BCC

En el Cuadro 26 se definen las primitivas, los mensajes y los temporizadores del protocolo BCC en el lado LE de la interfaz V5.2. Estos eventos de protocolo se utilizan en el cuadro de transiciones de estado de la LE (Cuadro 46 de la subcláusula 17.7).

En el Cuadro 27 se definen las primitivas, los mensajes y los temporizadores del protocolo BCC en el lado AN de la interfaz V5.2. Estos eventos de protocolo se utilizan en el cuadro de transiciones de estado de la AN (Cuadro 47 de la subcláusula 17.7).

17.3 Definición y contenido de los mensajes del protocolo BCC

El formato de los mensajes del protocolo BCC corresponderá a la estructura de mensaje genérica definida en la Cláusula 13.

El conjunto completo de mensajes para el protocolo BCC se da en el Cuadro 28. Las subcláusulas siguientes dan la estructura detallada de los mensajes para cada uno de estos mensajes.

17.3.1 Mensaje ASIGNACIÓN

Este mensaje es utilizado por la central local para solicitar de la red de acceso la asignación de uno o varios canales portadores a un determinado puerto de usuario mediante la identificación y el uso de un intervalo de tiempo V5 particular dentro de la interfaz V5.2 (véase el Cuadro 29).

CUADRO 26/G.965

Primitivas, mensajes y temporizadores del protocolo BCC en el lado LE

	Sentido	Descripción
Petición MDU-BCC – ASIGNACIÓN	RM → BCC_PE	Iniciación del proceso de asignación de canal portador
Confirmación MDU-BCC – ASIGNACIÓN	RM ← BCC_PE	Compleción del proceso de asignación de canal portador
Indicación MDU-BCC – RECHAZO DE ASIGNACIÓN	RM ← BCC_PE	La compleción del proceso de asignación de canal portador no es posible
Indicación MDU-BCC – ERROR DE ASIGNACIÓN	RM ← BCC_PE	Después de retransmitido el mensaje ASIGNACIÓN no se recibe respuesta del lado AN
Indicación MDU-BCC DESASIGNACIÓN	RM → BCC_PE	Iniciación del proceso de desasignación de canal portador
Confirmación MDU-BCC – DESASIGNACIÓN	RM ← BCC_PE	Compleción del proceso de desasignación de canal portador
Indicación MDU-BCC – RECHAZO DE DESASIGNACIÓN	RM ← BCC_PE	La compleción del proceso de desasignación de canal portador no es posible
Indicación MDU-BCC – ERROR DE DESASIGNACIÓN	RM ← BCC_PE	Después de retransmitido el mensaje DESASIGNACIÓN, no se recibe respuesta del lado AN
Petición MDU-BCC – VERIFICACIÓN	RM → BCC_PE	Iniciación de proceso del procedimiento de verificación
Confirmación MDU-BCC – VERIFICACIÓN	RM ← BCC_PE	Compleción de proceso del procedimiento de verificación
Indicación MDU-BCC – ERROR DE VERIFICACIÓN	RM ← BCC_PE	Después de retransmitido el mensaje VERIFICACIÓN, no se recibe respuesta del lado AN
Indicación MDU-BCC – AVERÍA AN	RM ← BCC_PE	Iniciación de proceso del procedimiento de fallo interno de AN
Indicación MDU-BCC – ERROR DE PROTOCOLO	SYS ← BCC_PE	Error de protocolo detectado por la comprobación del tratamiento de errores
ASIGNACIÓN	LE → AN	Mensaje inicial en un proceso de asignación de canal portador
ASIGNACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso de asignación de canal portador completado fructuosamente
RECHAZO DE ASIGNACIÓN	LE ← AN	Mensaje final en un proceso de asignación de canal portador completado infructuosamente
DESASIGNACIÓN	LE → AN	Mensaje inicial en un proceso de desasignación de canal portador
DESASIGNACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso de desasignación de canal portador completado fructuosamente
RECHAZO DE DESASIGNACIÓN	LE ← AN	Mensaje final en un proceso de desasignación de canal portador completado infructuosamente
VERIFICACIÓN	LE → AN	Mensaje inicial en un proceso del procedimiento de verificación
VERIFICACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso del procedimiento de verificación completado fructuosamente

CUADRO 26/G.965 (*fin*)

Primitivas, mensajes y temporizadores del protocolo BCC en el lado LE

	Sentido	Descripción
AVERÍA DE AN	LE ← AN	Mensaje inicial en un proceso de notificación de fallo interno de AN
ACUSE DE RECIBO DE AVERÍA DE AN	LE → AN	Mensaje final en un proceso de notificación de fallo interno de AN completado fructuosamente
ERROR DE PROTOCOLO	LE ← AN	Notificación de un error de protocolo BCC
Expiración Tbcc1	LE_BCC interno	Estando en el estado Bcc espera de asignación, no se recibe un mensaje adecuado
Expiración Tbcc2	LE_BCC interno	Estando en el estado Bcc aborto de asignación, no se recibe un mensaje adecuado
Expiración Tbcc3	LE_BCC interno	Estando en el estado Bcc espera de desasignación, no se recibe un mensaje adecuado
Expiración Tbcc4	LE_BCC interno	Estando en el estado Bcc espera de verificación, no se recibe un mensaje adecuado

RM	Entidad de gestión de recursos de LE
BCC_PE	Entidad de protocolo BCC de LE
LE_BCC interno	Interno de la entidad de protocolo BCC de la LE
SYS	Gestión del sistema de la LE

CUADRO 27/G.965

Primitivas, mensajes y temporizadores del protocolo BCC en el lado AN

	Dirección	Descripción
Indicación MDU-BCC – ASIGNACIÓN	RM ← BCC_PE	Iniciación del proceso de asignación de canal portador
Respuesta MDU-BCC – ASIGNACIÓN COMPLETA	RM → BCC_PE	Compleción del proceso de asignación de canal portador
Respuesta MDU-BCC – RECHAZO ASIGNACIÓN	RM → BCC_PE	La compleción del proceso de asignación de canal portador no es posible
Indicación MDU-BCC – DESASIGNACIÓN	RM ← BCC_PE	Iniciación del proceso de desasignación de canal portador
Respuesta MDU-BCC – DESASIGNACIÓN COMPLETA	RM → BCC_PE	Compleción del proceso de desasignación de canal portador
Respuesta MDU-BCC – RECHAZO DESASIGNACIÓN	RM → BCC_PE	La compleción del proceso de desasignación de canal portador no es posible
Indicación MDU-BCC – VERIFICACIÓN	RM ← BCC_PE	Iniciación de proceso del procedimiento de verificación
Respuesta MDU-BCC – VERIFICACIÓN	RM → BCC_PE	Compleción de proceso del procedimiento de verificación
Petición MDU-BCC – AVERÍA AN	RM → BCC_PE	Iniciación de proceso de notificación de fallo interno de AN
Confirmación MDU-BCC – AVERÍA AN	RM ← BCC_PE	Compleción de proceso de notificación de fallo interno de AN
Indicación MDU-BCC – ERROR – AVERÍA AN	RM ← BCC_PE	Después de retransmisiones del mensaje AVERÍA DE AN, no se recibe ninguna respuesta del lado LE
Indicación MDU-BCC – ERROR – PROTOCOLO	SYS ← BCC_PE	Error de protocolo detectado mediante la comprobación del tratamiento de errores
ASIGNACIÓN	LE → AN	Mensaje inicial en un proceso de asignación de canal portador
ASIGNACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso de asignación de canal portador completado fructuosamente
RECHAZO DE ASIGNACIÓN	LE ← AN	Mensaje final en un proceso de asignación de canal portador completado infructuosamente
DESASIGNACIÓN	LE → AN	Mensaje inicial en un proceso de desasignación de canal portador
DESASIGNACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso de desasignación de canal portador completado fructuosamente
RECHAZO DE DESASIGNACIÓN	LE ← AN	Mensaje final en un proceso de desasignación de canal portador completado infructuosamente
VERIFICACIÓN	LE → AN	Mensaje inicial en un proceso del procedimiento de verificación
VERIFICACIÓN COMPLETA	LE ← AN	Mensaje final en un proceso del procedimiento de verificación completado fructuosamente
AVERÍA DE AN	LE ← AN	Mensaje inicial en un proceso de notificación de fallo interno de AN
ACUSE DE RECIBO DE AVERÍA DE AN	LE → AN	Mensaje final en un proceso de notificación de fallo interno de AN completado fructuosamente
ERROR DE PROTOCOLO	LE ← AN	Notificación de un error de protocolo BCC
Expiración Tbcc5	AN_BCC interno	Estando en el estado informe de avería Bcc, no se recibe ningún mensaje adecuado

RM	Entidad de gestión de recursos de la AN
BCC_PE	Entidad de protocolo BCC de la AN
AN_BCC interno	Interno de la entidad de protocolo BCC de la AN
SYS	Gestión del sistema

CUADRO 28/G.965

Conjunto de los mensajes del protocolo BCC

Codificación en el elemento de información tipo de mensaje							Mensajes del protocolo BCC	Referencia (subcláusula)
7	6	5	4	3	2	1		
0	1	0	0	0	0	0	ASIGNACIÓN	17.3.1
0	1	0	0	0	0	1	ASIGNACIÓN COMPLETA	17.3.2
0	1	0	0	0	1	0	RECHAZO DE ASIGNACIÓN	17.3.3
0	1	0	0	0	1	1	DESASIGNACIÓN	17.3.4
0	1	0	0	1	0	0	DESASIGNACIÓN COMPLETA	17.3.5
0	1	0	0	1	0	1	RECHAZO DE DESASIGNACIÓN	17.3.6
0	1	0	0	1	1	0	VERIFICACIÓN	17.3.7
0	1	0	0	1	1	1	VERIFICACIÓN COMPLETA	17.3.8
0	1	0	1	0	0	0	AVERÍA DE AN	17.3.9
0	1	0	1	0	0	1	ACUSE DE RECIBO DE AVERÍA DE AN	17.3.10
0	1	0	1	0	1	0	ERROR DE PROTOCOLO	17.3.11

CUADRO 29/G.965

Contenido del mensaje ASIGNACIÓN

Tipo de mensaje: ASIGNACIÓN

Sentido: LE hacia AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE hacia AN	M	1
Número de referencia BCC	17.4.1	LE hacia AN	M	2
Tipo de mensaje	17.3	LE hacia AN	M	1
Identificación de puerto de usuario	17.4.2.1	LE hacia AN	M	4
Identificación de canal de puerto RDSI	17.4.2.2	LE hacia AN	O (Nota 1)	3
Identificación de intervalo de tiempo V5	17.4.2.3	LE hacia AN	O (Nota 2)	4
Correspondencia de multiintervalos	17.4.2.4	LE hacia AN	O (Nota 3)	11

NOTAS

1 El elemento de información identificación de canal de puerto RDSI ha de incluirse al asignar un solo intervalo de tiempo con el fin de soportar un canal portador relacionado con un puerto RDSI. Este elemento de información especificará el intervalo de tiempo de puerto de usuario dentro de la interfaz (básica o primaria) usuario/red RDSI a la que ha de transconectarse el canal portador.

2 El elemento de información identificación de intervalo de tiempo ha de incluirse al asignar un solo intervalo de tiempo con el fin de identificar el intervalo de tiempo pertinente de la interfaz V5.2.

3 El elemento de información correspondencia de multiintervalos ha de incluirse al asignar múltiples intervalos de tiempo con el fin de soportar servicios portadores RDSI multivelocidades ($n \times 64$ kbit/s). Este elemento de información especificará también los intervalos de tiempo de puerto de usuario dentro de la interfaz (básica o primaria) usuario/red RDSI a la que el canal portador ha de transconectarse.

En el caso de asignaciones de canal portador a un puerto RDSI a los efectos de transconexión, la central local indicará también el intervalo de tiempo de puerto de usuario que ha de utilizarse en la interfaz RDSI.

Este mensaje permite también la asignación en bloque de canales portadores multivelocidades (múltiples intervalos de tiempo V5) para soportar servicios multivelocidades (n × 64 kbit/s).

17.3.2 Mensaje ASIGNACIÓN COMPLETA

Este mensaje es utilizado por la red de acceso para indicar a la central local que la asignación del o de los canales portadores solicitados a determinado puerto de usuario ha sido completada fructuosamente (véase el Cuadro 30).

CUADRO 30/G.965

Contenido del mensaje ASIGNACIÓN COMPLETA

Tipo de mensaje: ASIGNACIÓN COMPLETA

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1

17.3.3 Mensaje RECHAZO DE ASIGNACIÓN

Este mensaje es utilizado por la red de acceso para indicar a la central local que la asignación del o de los canales portadores solicitados a un puerto de usuario determinado no ha sido completada (véase el Cuadro 31).

CUADRO 31/G.965

Contenido del mensaje RECHAZO DE ASIGNACIÓN

Tipo de mensaje: RECHAZO DE ASIGNACIÓN

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1
Causa de rechazo	17.4.2.5	AN hacia LE	M	3 a 14

17.3.4 Mensaje DESASIGNACIÓN

Este mensaje es utilizado por la central local para solicitar de la red de acceso la desasignación de uno o múltiples canales portadores de determinado puerto de usuario. El intervalo de tiempo V5 particular dentro de la interfaz V5.2 es identificado explícitamente (véase el Cuadro 32).

Este mensaje permite también la desasignación en bloque de canales portadores multivelocidades (múltiples intervalos de tiempo V5) que soportan servicios multivelocidades (n × 64 kbit/s).

CUADRO 32/G.965

Contenido del mensaje DESASIGNACIÓN

Tipo de mensaje: DESASIGNACIÓN

Sentido: LE hacia AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE hacia AN	M	1
Número de referencia BCC	17.4.1	LE hacia AN	M	2
Tipo de mensaje	17.3	LE hacia AN	M	1
Identificación de puerto de usuario	17.4.2.1	LE hacia AN	M	4
Identificación de canal de puerto RDSI	17.4.2.2	LE hacia AN	O (Nota 1)	3
Identificación de intervalo de tiempo V5	17.4.2.3	LE hacia AN	O (Nota 2)	4
Correspondencia de multiintervalos	17.4.2.4	LE hacia AN	O (Nota 3)	11

NOTAS

1 El elemento de información identificación de canal de puerto RDSI ha de incluirse al desasignar un solo intervalo de tiempo con el fin de soportar un canal portador relacionado con un puerto RDSI. Este elemento de información especificará el intervalo de tiempo de puerto de usuario dentro de la interfaz (básica o primaria) usuario/red RDSI de la que ha de desconectarse el canal portador.

2 El elemento de información identificación de intervalo de tiempo ha de incluirse al desasignar un solo intervalo de tiempo con el fin de identificar el intervalo de tiempo pertinente de la interfaz V5.2.

3 El elemento de información correspondencia de multiintervalos ha de incluirse al desasignar múltiples intervalos de tiempo con el fin de soportar servicios portadores RDSI multivelocidades ($n \times 64$ kbit/s). Este elemento de información especificará también el intervalo de tiempo de puerto de usuario dentro de la interfaz (básica o primaria) usuario/red RDSI de la que ha de desconectarse el canal portador.

17.3.5 Mensaje DESASIGNACIÓN completa

Este mensaje es utilizado por la red de acceso para indicar a la central local que la desasignación del o de los canales portadores solicitados de un puerto de usuario determinado ha sido completada fructuosamente (véase el Cuadro 33).

CUADRO 33/G.965

Contenido del mensaje DESASIGNACIÓN COMPLETA

Tipo de mensaje: DESASIGNACIÓN COMPLETA

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1

17.3.6 Mensaje RECHAZO DE DESASIGNACIÓN

Este mensaje es utilizado por la red de acceso para indicar a la central local que la desasignación del o de los canales portadores solicitados de un puerto de usuario determinado no ha sido completada (véase el Cuadro 34).

CUADRO 34/G.965

Contenido del mensaje RECHAZO DE DESASIGNACIÓN

Tipo de mensaje: RECHADO DE DESASIGNACIÓN

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1
Causa del rechazo	17.4.2.5	AN hacia LE	M	3 a 14

17.3.7 Mensaje VERIFICACIÓN

Este mensaje es utilizado por la central local para solicitar de la red de acceso el suministro de la información completa que identifica una conexión de canal portador a 64 kbit/s (véase el Cuadro 35).

Gracias a este mensaje, la central local puede solicitar información relativa a la conexión del canal portador sobre la base de la información parcial disponible en algunas circunstancias tales como la identificación del puerto de usuario, junto con la identificación del canal del puerto RDSI cuando procede o la identificación del intervalo de tiempo V5.

CUADRO 35/G.965

Contenido del mensaje VERIFICACIÓN

Tipo de mensaje: VERIFICACIÓN

Sentido: LE hacia AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE hacia AN	M	1
Número de referencia BCC	17.4.1	LE hacia AN	M	2
Tipo de mensaje	17.3	LE hacia AN	M	1
Identificación de puerto de usuario	17.4.2.1	LE hacia AN	O (Nota 1)	4
Identificación de canal de puerto RDSI	17.4.2.2	LE hacia AN	O (Nota 2)	3
Identificación de intervalo de tiempo V5	17.4.2.3	LE hacia AN	O (Nota 3)	4

NOTAS

1 Al efectuar una verificación sobre la base del puerto de usuario, este elemento de información identifica el puerto de usuario que termina la conexión de canal portador sobre la cual ha de realizarse la verificación.

2 Al efectuar una verificación sobre la base del puerto de usuario, y si el puerto es un puerto de usuario RDSI, este elemento de información identifica el intervalo de tiempo de puerto de usuario que termina la conexión de canal portador en la cual ha de realizarse la verificación. Este elemento de información aparecerá junto con el elemento de información identificación de puerto de usuario.

3 Al efectuar una verificación sobre la base del intervalo de tiempo V5, este elemento de información identifica el intervalo de tiempo V5 dentro de la interfaz V5.2 que soporta la conexión de canal portador sobre la que ha de realizarse la verificación.

17.3.8 Mensaje VERIFICACIÓN COMPLETA

Este mensaje es utilizado por la red de acceso para indicar a la central local el resultado de la verificación solicitada proporcionando la información que identifica la conexión de canal portador o indicando que no hay conexión disponible en la referencia suministrada (véase el Cuadro 36).

CUADRO 36/G.965

Contenido de mensaje VERIFICACIÓN COMPLETA

Tipo de mensaje: VERIFICACIÓN COMPLETA

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1
Identificación de puerto de usuario	17.4.2.1	AN hacia LE	O (Nota 1)	4
Identificación de canal de puerto RDSI	17.4.2.2	AN hacia LE	O (Nota 1)	3
Identificación de intervalo de tiempo V5	17.4.2.3	AN hacia LE	O (Nota 1)	4
Conexión incompleta	17.4.2.7	AN hacia LE	O (Nota 2)	3

NOTAS

1 El elemento de información identificación de puerto de usuario se incluirá, junto con el elemento de información identificación de canal de puerto RDSI, cuando proceda, y el elemento de información identificación de intervalo de tiempo V5, si el resultado de la verificación refleja una conexión completa existente.

2 Este elemento de información se incluirá cuando el resultado de un proceso de verificación no sea fructuoso debido a que no hay conexión asociada con la información de referencia suministrada del proceso de verificación.

17.3.9 Mensaje AVERÍA DE AN

Este mensaje es utilizado por la red de acceso para notificar a la central local la ruptura de una conexión de canal portador a 64 kbit/s en la red de acceso debido a un fallo interno (véase el Cuadro 37).

Al notificar un fallo interno, la AN debe suministrar la información necesaria para que la LE pueda identificar todos los datos relacionados con esa conexión.

CUADRO 37/G.965

Contenido del mensaje AVERÍA DE AN

Tipo de mensaje: AVERÍA DE AN

Sentido: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1
Identificación de puerto de usuario	17.4.2.1	AN hacia LE	O (Nota 1)	4
Identificación de canal de puerto RDSI	17.4.2.2	AN hacia LE	O (Nota 2)	3
Identificación de intervalo de tiempo V5	17.4.2.3	AN hacia LE	O (Nota 3)	4

NOTAS

1 Cuando falla una conexión interna de la AN, este elemento de información se incluirá, si está disponible, junto con el elemento de información identificación de canal de puerto RDSI, cuando proceda, a fin de notificar a la LE el puerto de usuario afectado por el fallo de la AN.

2 Cuando falla una conexión interna de la AN, este elemento de información se utilizará cuando la notificación de fallo se refiere a un puerto RDSI identificado por el elemento de información identificación de puerto de usuario.

3 Cuando falla una conexión interna de la AN, este elemento de información se incluirá, si está disponible, a fin de notificar a la LE el intervalo de tiempo V5 de la interfaz V5.2 afectado por el fallo de la AN.

17.3.10 Mensaje ACUSE DE RECIBO DE AVERÍA DE AN

Este mensaje es utilizado por la central local para acusar recibo a la red de acceso de un mensaje AVERÍA DE AN (véase el Cuadro 38).

NOTA – El envío de este mensaje es un acuse de recibo del mensaje AVERÍA DE AN, y no una notificación de que las acciones apropiadas han sido emprendidas.

CUADRO 38/G.965

Contenido del mensaje ACUSE DE RECIBO DE AVERÍA DE AN

Tipo de mensaje: ACUSE DE RECIBO DE AVERÍA DE AN

Sentido: LE hacia AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE hacia AN	M	1
Número de referencia BCC	17.4.1	LE hacia AN	M	2
Tipo de mensaje	17.3	LE hacia AN	M	1

17.3.11 Mensaje ERROR DE PROTOCOLO

Este mensaje es utilizado por la red de acceso para indicar a la central local que ha sido identificado un error de protocolo en un mensaje recibido (véase el Cuadro 39).

CUADRO 39/G.965

Contenido del mensaje ERROR DE PROTOCOLO

Tipo de mensaje: ERROR DE PROTOCOLO

Sens: AN hacia LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN hacia LE	M	1
Número de referencia BCC	17.4.1	AN hacia LE	M	2
Tipo de mensaje	17.3	AN hacia LE	M	1
Causa del error de protocolo	17.4.2.6	AN hacia LE	M	3 a 5

17.4 Definición, estructura y codificación de los elementos de información BCC

Esta subcláusula define la codificación de los elementos de información específicos del protocolo BCC, utilizados dentro de los mensajes específicos del protocolo BCC. Para cada uno de los elementos de información se suministra la codificación de sus diferentes campos.

Los elementos de información específicos del protocolo BCC se enumeran en el Cuadro 40, que da también la codificación del identificador de elemento de información.

CUADRO 40/G.965

Elementos de información específicos del protocolo BCC

Bits								Elemento de información	Referencia
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	ELEMENTOS DE INFORMACIÓN DE LONGITUD VARIABLE	
0	1	0	0	0	0	0	0	Identificación de puerto de usuario	17.4.2.1
0	1	0	0	0	0	0	1	Identificación de canal de puerto RDSI	17.4.2.2
0	1	0	0	0	0	1	0	Identificación de intervalo de tiempo V5	17.4.2.3
0	1	0	0	0	0	1	1	Correspondencia de multiintervalos	17.4.2.4
0	1	0	0	0	1	0	0	Causa del rechazo	17.4.2.5
0	1	0	0	0	1	0	1	Causa del error de protocolo	17.4.2.6
0	1	0	0	0	1	1	0	Conexión incompleta	17.4.2.7
NOTA – Todos los demás valores están reservados.									

17.4.1 Elemento de información número de referencia BCC

Este elemento de información es específico del protocolo BCC y utiliza la localización del elemento de información dirección de capa 3 dentro de la estructura general del mensaje definida en la cláusula 13.

El elemento de información número de referencia BCC tiene por objeto identificar el proceso del protocolo BCC, dentro de la interfaz V5.2, al que se aplica el mensaje transmitido o recibido.

El valor de número de referencia BCC será un número aleatorio generado por la entidad (AN o LE) que crea el nuevo proceso del protocolo BCC (este valor aleatorio puede implementarse como una generación secuencial de valores). Es esencial que los valores no se repitan en los mensajes para los cuales se requiere un proceso BCC diferente (en el mismo sentido), hasta cuando el antiguo proceso BCC haya concluido y el número haya sido suprimido. El elemento de información número de referencia BCC, al formar parte del encabezamiento del mensaje, será la segunda parte de cada mensaje (situado después del elemento de información discriminador de protocolo). En caso de que un proceso genere indicaciones de error, el número de referencia BCC no deberá reutilizarse hasta cuando haya transcurrido el tiempo suficiente para la llegada diferida de mensajes que contengan el mismo número de referencia BCC.

La longitud del elemento de información número de referencia BCC será de 2 octetos.

La estructura del elemento de información número de referencia BCC será la indicada por la Figura 16.

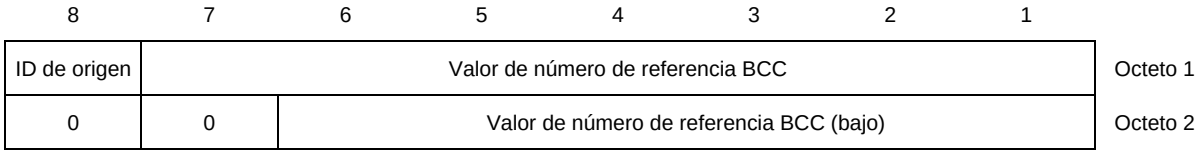


FIGURA 16/G.965

Elemento de información número de referencia BCC

La identificación de origen es un campo de 1 bit que especifica la entidad (LE o AN) que ha creado el número de referencia BCC (es decir, la entidad que ha creado el proceso del protocolo BCC). La codificación de este campo será CERO para un proceso creado por la LE y UNO para un proceso creado por la AN.

El campo valor de número de referencia BCC consta de 13 bits y se utiliza para suministrar la codificación binaria que identifica el proceso BCC.

17.4.2 Otros elementos de información

En esta subcláusula se describen los elementos de información que pueden aparecer en los diferentes mensajes.

Estos elementos de información pueden aparecer en los diferentes mensajes, y son facultativos u obligatorios, según la semántica del mensaje y/o la aplicación de proceso del mensaje.

17.4.2.1 Elemento de información identificación de puerto de usuario

El elemento de información identificación de puerto de usuario tiene por objeto identificar, a través de la interfaz V5.2, el puerto RTPC o RDSI al que se aplica el mensaje relativo al proceso del protocolo BCC.

La longitud del elemento de información identificación de puerto de usuario será de 4 octetos.

La estructura del elemento de información identificación de puerto de usuario será la indicada por las Figuras 17 y 18.

La codificación del elemento de información identificación de puerto de usuario se hará en binario. Para la codificación del elemento de información identificación de puerto de usuario se han definido dos estructuras, una para puertos RTPC (véase la Figura 17) y la otra para puertos RDSI (véase la Figura 18).

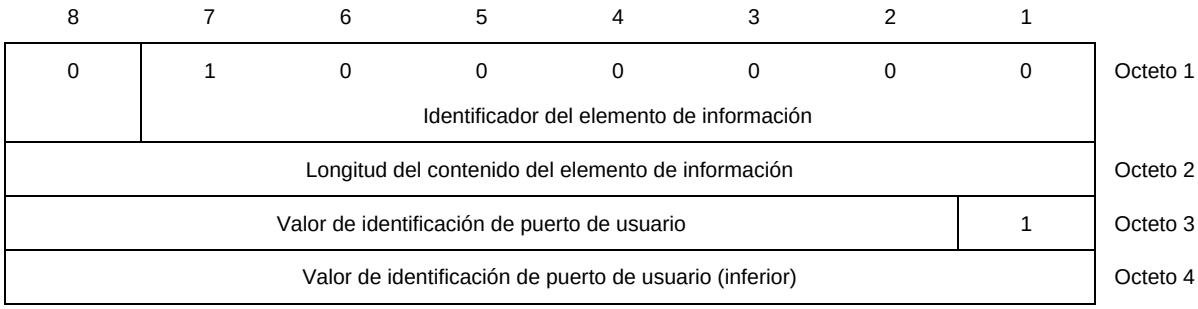


FIGURA 17/G.965

Elemento de información identificación de puerto de usuario (puerto RTPC)

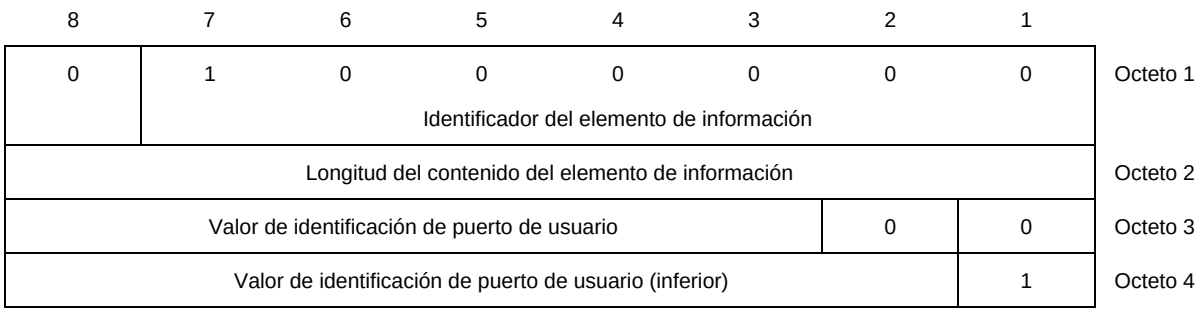


FIGURA 18/G.965

Elemento de información identificación de puerto de usuario (puerto RDSI)

Para el caso de los puertos RTPC, el valor de identificación de puerto de usuario (15 bits) tendrá el mismo valor que el elemento de información dirección de capa 3 contenido en los mensajes del protocolo RTPC relativos al puerto de usuario RTPC al que se aplica el mensaje relativo al proceso.

Para el caso de los puertos RDSI, el valor de identificación de puerto de usuario (13 bits) tendrá el mismo valor que la dirección de envolvente contenida en las tramas de función de envolvente utilizadas para retransmitir los mensajes DSS1 relacionados con el puerto de usuario RDSI al que se aplica el mensaje relativo al proceso.

17.4.2.2 Elemento de información identificación de intervalo de tiempo de puerto RDSI

El elemento de información identificación de intervalo de tiempo de puerto RDSI tiene por objeto indicar, únicamente en el caso de un protocolo BCC de intervalo de tiempo V5 relacionado con un puerto de usuario RDSI, el intervalo de tiempo de puerto de usuario dentro de la interfaz (de acceso básico o a velocidad primaria) usuario/red RDSI al que ha de transconectarse el intervalo de tiempo V5 dentro del enlace a 2048 kbit/s de la interfaz V5.2, o del que el intervalo de tiempo V5 identificado ha de desconectarse.

La longitud del elemento de información identificación de intervalo de tiempo de puerto RDSI será de 3 octetos.

La estructura del elemento de información identificación de intervalo de tiempo de puerto RDSI será la indicada por la Figura 19.

El número de intervalo de tiempo de puerto de usuario RDSI es un campo de 5 bits utilizado para proporcionar la codificación binaria que identifica al intervalo de tiempo de puerto de usuario dentro del puerto de usuario RDSI. Para el caso de los puertos de usuario AVP-RDSI, los canales B1 a B31 se denominarán intervalos de tiempo de puerto de usuario RDSI números 1 (00001) a 31 (11111). Para el caso del puerto de usuario de acceso básico RDSI, el canal B1 se denominará intervalo de tiempo de puerto de usuario RDSI número 1 (00001) y el canal B2 se denominará intervalo de tiempo de puerto de usuario RDSI número 2 (00010).

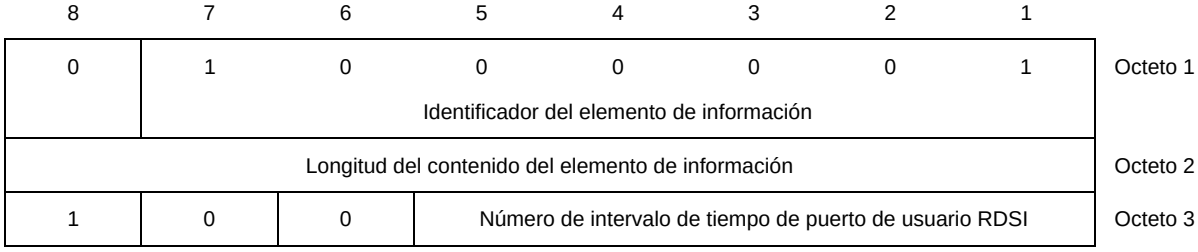


FIGURA 19/G.965

Elemento de información identificación de intervalo de tiempo de puerto RDSI

17.4.2.3 Elemento de información identificación de intervalo de tiempo V5

El elemento de información identificación de intervalo de tiempo V5 tiene por objeto identificar, en el caso de un proceso del protocolo BCC de un solo intervalo de tiempo V5, al intervalo de tiempo V5 dentro de un enlace determinado a 2048 kbit/s al que se aplica el proceso.

La longitud del elemento de información identificación de intervalo de tiempo V5 será de 4 octetos.

La estructura del elemento de información número de referencia BCC será la indicada por la Figura 20.

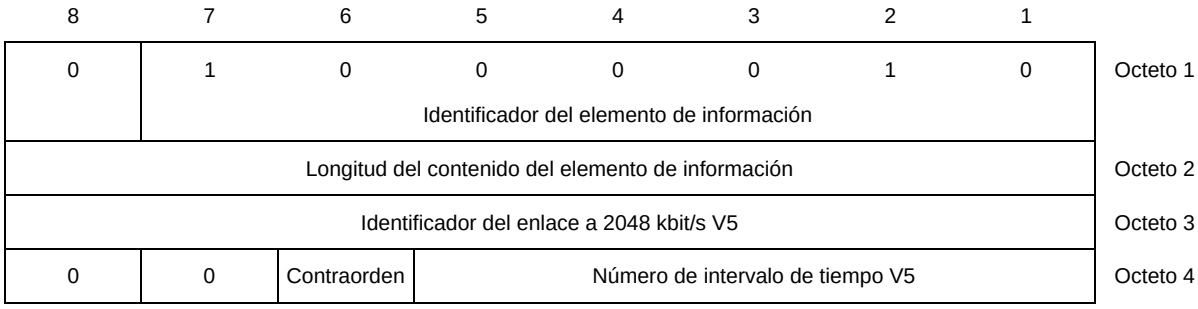


FIGURA 20/G.965

Elemento de información identificación de intervalo de tiempo V5

El identificador de enlace a 2048 kbit/s V5 es un campo de 8 bits utilizado para suministrar la codificación binaria que identifica un enlace determinado a 2048 kbit/s entre los que comprende la interfaz V5.2 en la que está situado el intervalo de tiempo V5 seleccionado que ha de utilizarse como canal portador. Pueden identificarse explícitamente un máximo de 256 enlaces a 2048 kbit/s.

El número de intervalo de tiempo V5 es un campo de 5 bits utilizado para suministrar la codificación binaria que identifica el intervalo de tiempo V5, o el primer intervalo de tiempo V5 de un bloque de intervalos de tiempo V5 (dentro del enlace a 2048 kbit/s identificado en el octeto anterior) que ha de utilizarse, o que está utilizándose, como canal portador.

El bit de contraorden especifica la petición de la LE de contraordenar la conexión de canal portador existente en el intervalo de tiempo V5 identificado al establecer la conexión de canal portador solicitada. La codificación de este campo será CERO para «contraorden no solicitada» y UNO para «contraorden solicitada».

17.4.2.4 Elemento de información correspondencia de multiintervalos

El elemento de información correspondencia de multiintervalos tiene por objeto identificar, en el caso de asignación o desasignación *en bloque* de múltiples intervalos de tiempo V5, todos los intervalos de tiempo V5 dentro de un enlace a 2048 kbit/s V5 dado al que se aplica el proceso de asignación o desasignación.

El elemento de información correspondencia de multiintervalos identificará también los intervalos de tiempo de puerto de usuario dentro de la interfaz usuario/red RDSI a la que han de transconectarse los intervalos de tiempo V5 identificados, o de la que deben desconectarse los intervalos de tiempo V5 identificados.

La relación entre los intervalos de tiempo V5 identificados y los intervalos de tiempo de puerto de usuario será de uno a uno en el mismo orden de aparición dentro de los respectivos mapas de codificación.

NOTA – Cuando varios intervalos de tiempo V5 han sido asignados como un solo bloque, éstos pueden ser o no ser desasignados *en bloque*.

El número de intervalos de tiempo V5 afectados por un proceso de desasignación estará determinado por el sistema de gestión de recursos sobre la base del servicio RDSI suministrado.

En algunas circunstancias (por ejemplo, rearranque de la interfaz RDSI) un proceso de desasignación que afecta a varios intervalos de tiempo V5 puede ser solicitado por el sistema de gestión de recursos, incluso si los intervalos de tiempo V5 han sido asignados individualmente.

La longitud del elemento de información correspondencia de multiintervalos será de 11 octetos.

La estructura del elemento de información correspondencia de multiintervalos será la indicada en la Figura 21.

8	7	6	5	4	3	2	1	
0	1	0	0	0	0	1	1	Octeto 1
	Identificador del elemento de información							
Longitud del contenido del elemento de información								Octeto 2
Identificador del enlace a 2048 kbit/s V5								Octeto 3
V5TS31	V5TS30	V5TS29	V5TS28	V5TS27	V5TS26	V5TS25	V5TS24	Octeto 4
V5TS23	V5TS22	V5TS21	V5TS20	V5TS19	V5TS18	V5TS17	V5TS16	Octeto 5
V5TS15	V5TS14	V5TS13	V5TS12	V5TS11	V5TS10	V5TS9	V5TS8	Octeto 6
V5TS7	V5TS6	V5TS5	V5TS4	V5TS3	V5TS2	V5TS1	0	Octeto 7
UPTS31	UPTS30	UPTS29	UPTS28	UPTS27	UPTS26	UPTS25	UPTS24	Octeto 8
UPTS23	UPTS22	UPTS21	UPTS20	UPTS19	UPTS18	UPTS17	UPTS16	Octeto 9
UPTS15	UPTS14	UPTS13	UPTS12	UPTS11	UPTS10	UPTS9	UPTS8	Octeto 10
UPTS7	UPTS6	UPTS5	UPTS4	UPTS3	UPTS2	UPTS1	0	Octeto 11

FIGURA 21/G.965

Elemento de información identificación de multiintervalos

El identificador del enlace a 2048 kbit/s V5 es un campo de 8 bits utilizado para suministrar la codificación binaria que identifica el enlace a 2048 kbit/s (entre los que pueden componer la interfaz V5.2) en el que están situados los intervalos de tiempo V5 que han de utilizarse como canales portadores. Pueden identificarse explícitamente un máximo de 256 enlaces a 2048 kbit/s.

Los octetos 4 a 7 identifican los intervalos de tiempo V5 dentro de la interfaz V5.2 que están siendo asignados o desasignados *en bloque*. Los bits correspondientes a los intervalos de tiempo V5 afectados por el proceso se codificarán como «1» binario, los bits correspondientes a los intervalos de tiempo V5 no afectados por el proceso serán codificados como »0» binario.

Los octetos 8 a 11 identifican múltiples intervalos de tiempo de puerto de usuario dentro del puerto de usuario RDSI (básico o primario) al que o del que han de conectarse o desconectarse los intervalos de tiempo V5 especificados en los octetos 4 a 7. La relación entre los intervalos de tiempo V5 y los intervalos de tiempo de puerto de usuario será de uno a uno en el orden de numeración especificado. Los bits correspondientes a los intervalos de tiempo de puerto de usuario afectados por el proceso serán codificados como «1» binario, los bits correspondientes a los intervalos de tiempo de puerto de usuario no afectados por el proceso serán codificados como »0» binario.

Para el caso del puerto de usuario de acceso básico RDSI, los dos canales B se denominarán intervalos de tiempo de puerto de usuario uno (UPTS1, *user port time slot 1*) e intervalo de tiempo de puerto de usuario dos UPTS2 en el mapa; en este caso, no se activarán nunca UPTS3 a UPTS1.

17.4.2.5 Elemento de información causa de rechazo

El elemento de información causa de rechazo tiene por objeto indicar de la red de acceso a la central local el motivo por el cual no ha sido completada la asignación o desasignación del o de los canales portadores solicitados.

El elemento de información causa de rechazo incluirá, para algunos tipos de causa de rechazo, un campo de diagnóstico con el fin de suministrar información adicional relativa a estos valores de causa de rechazo. El campo de diagnóstico, cuando esté presente, será siempre una copia del elemento de información recibido que contiene la información que ha provocado el envío del mensaje de rechazo.

La longitud del elemento de información causa de rechazo estará comprendida entre 3 y 14 octetos. Para los tipos de causa de rechazo que no incluyen información de diagnóstico, la longitud del elemento de información será de 3 octetos. Para los tipos de causa de rechazo que incluyen información de diagnóstico, la longitud del elemento de información estará comprendida entre 6 y 14 octetos (6, 7 y 14 octetos son valores válidos).

La estructura del elemento de información causa de rechazo será la indicada por la Figura 22.

8	7	6	5	4	3	2	1	
0	1	0	0	0	1	0	0	Octeto 1
Identificador del elemento de información								
Longitud del contenido del elemento de información								Octeto 2
1	Tipo de causa de rechazo							Octeto 3
Diagnóstico								Octeto 4 Octeto n

FIGURA 22/G.965

Elemento de información causa de rechazo

La codificación del campo tipo de causa de rechazo será tal como se especifica en el Cuadro 41.

CUADRO 41/G.965

Codificación del tipo de causa de rechazo

7	6	5	4	3	2	1	Causa de rechazo
0	0	0	0	0	0	0	No especificada
0	0	0	0	0	0	1	Avería de red de acceso
0	0	0	0	0	1	0	Red de acceso bloqueada (internamente)
0	0	0	0	0	1	1	Conexión ya presente en el puerto de usuario RTPC con un intervalo de tiempo V5 diferente
0	0	0	0	1	0	0	Conexión ya presente en el o los intervalos de tiempo V5 con un puerto o intervalo tiempo de puerto de usuario RDSI diferentes
0	0	0	0	1	0	1	Conexión ya presente en el o los intervalos de tiempo de puerto de usuario RDSI con uno o varios intervalos de tiempo V5 diferentes
0	0	0	0	1	1	0	Puerto de usuario no disponible (bloqueado)
0	0	0	0	1	1	1	La desasignación no puede completarse debido a contenido de datos incompatible
0	0	0	1	0	0	0	La desasignación no puede completarse debido a incompatibilidad de datos del o de los intervalos de tiempo V5
0	0	0	1	0	0	1	La desasignación no puede completarse debido a incompatibilidad de datos de puerto
0	0	0	1	0	1	0	La desasignación no puede completarse debido a incompatibilidad de datos del o de los intervalos de tiempo de puerto de usuario
0	0	0	1	0	1	1	Puerto de usuario no aprovisionado
0	0	0	1	1	0	0	Identificación(es) inválida(s) de intervalo(s) de tiempo V5
0	0	0	1	1	0	1	Identificación inválida de enlace a 2048 kbit/s V5
0	0	0	1	1	1	0	Identificación(es) inválida(s) de intervalo(s) de tiempo de puerto de usuario
0	0	0	1	1	1	1	Intervalo(s) de tiempo V5 utilizado(s) como canal(es) C físico(s)
0	0	1	0	0	0	0	Enlace V5 indisponible (bloqueado)
NOTA – Todos los demás valores están reservados.							

En el Cuadro K.1 se suministra información adicional sobre cuándo han de utilizarse los diferentes tipos de causa de rechazo en los procedimientos del protocolo BCC.

El campo de diagnóstico es un campo de múltiples octetos (el número de octetos depende del valor de la causa) que proporciona el diagnóstico pertinente para cada uno de los tipos de causa de rechazo conforme al Cuadro 42.

CUADRO 42/G.965

Diagnóstico para los tipos de causa de rechazo

Causa	Diagnóstico	Longitud
No especificada	No presente	0
Avería de red de acceso	No presente	0
Acceso de red bloqueado (internamente)	No presente	0
Conexión ya presente en el puerto de usuario RTPC con un intervalo de tiempo V5 diferente	Elemento de información identificación de puerto de usuario	4
Conexión ya presente en el o los intervalos de tiempo V5 de la interfaz V5.2 con un puerto o con intervalo(s) de tiempo de puerto de usuario RDSI diferente(s)	Elemento de información identificación de intervalo de tiempo V5 o correspondencia de multiintervalos	4 u 11
Conexión ya presente en el(los) intervalo(s) de tiempo de puerto de usuario RDSI con uno o varios intervalos de tiempo V5 diferentes	Elemento de información identificación de canal de puerto RDSI o elemento de información correspondencia de multiintervalos	3 u 11
Puerto de usuario indisponible (bloqueado)	Elemento de información identificación de puerto de usuario	4
La desasignación no puede completarse debido a contenido de datos incompatible	No presente	0
La desasignación no puede completarse debido a incompatibilidad de datos de intervalo(s) de tiempo V5	Elemento de información identificación de intervalo de tiempo V5 o elemento de información correspondencia de multiintervalos	4 u 11
La desasignación no puede completarse debido a incompatibilidad de datos de puerto	Elemento de información identificación de puerto de usuario	4
La desasignación no puede completarse debido a incompatibilidad de datos de intervalo(s) de tiempo de puerto de usuario	Elemento de información identificación de canal de puerto RDSI o elemento de información correspondencia de multiintervalos	3 u 11
Puerto de usuario no aprovisionado	Elemento de información identificación de puerto de usuario	4
Identificación(es) de intervalo(s) de tiempo V5 no válidas	Elemento de información identificación de intervalo de tiempo V5 o elemento de información correspondencia de multiintervalos	4 u 11
Identificación de enlace a 2048 kbit/s V5 inválida	Elemento de información identificación de intervalo de tiempo V5 o elemento de información correspondencia de multiintervalos	4 u 11
Identificación(es) de intervalo(s) de tiempo de puerto de usuario inválida(s)	Elemento de información identificación de canal de puerto RDSI o elemento de información correspondencia de multiintervalos	3 u 11
Intervalo(s) de tiempo V5 utilizado(s) como canal(es) C físico(s)	Elemento de información identificación de puerto de usuario	4 u 11

17.4.2.6 Elemento de información causa de error de protocolo

El elemento de información causa de error de protocolo tiene por objeto indicar desde la red de acceso a la central local el tipo de error de protocolo detectado en un proceso de protocolo BCC dado.

El elemento de información causa de error de protocolo incluirá, para algunos tipos de causa de error de protocolo, un campo de diagnóstico con el fin de proporcionar información adicional relacionada con estos tipos de causa de error de protocolo. Este campo de diagnóstico de uno o de dos octetos, cuando esté presente, será una copia del identificador de tipo de mensaje recibido que ha ocasionado el envío del mensaje que contiene el elemento de información causa de error de protocolo y, cuando se necesite, del identificador del elemento de información pertinente dentro de ese mensaje.

La longitud del elemento de información causa de error de protocolo estará comprendida entre 3 y 5 octetos. Para los tipos de causa de error de protocolo que no incluyen información de diagnóstico, la longitud del elemento de información será de 3 octetos, para los tipos de causa de error de protocolo que incluyen información de diagnóstico, la longitud del elemento de información será de 4 ó 5 octetos.

La estructura del elemento de información causa de error de protocolo será tal como se indica en la Figura 23.

8	7	6	5	4	3	2	1	
0	1	0	0	0	1	0	1	Octeto 1
Identificador del elemento de información								
Longitud del contenido del elemento de información								Octeto 2
1	Tipo de causa de error de protocolo							Octeto 3
0	Diagnóstico (identificador de tipo de mensaje)							Octeto 4
Diagnóstico (identificador del elemento de información)								Octeto 5

FIGURA 23/G.965

Elemento de información causa de error de protocolo

La codificación del campo tipo de causa de error de protocolo será la especificada en el Cuadro 43.

CUADRO 43/G.965

Tipo de causa de error de protocolo

•	6	5	4	3	2	1	Causa de error de protocolo
0	0	0	0	0	0	1	Error de discriminador de protocolo
0	0	0	0	1	0	0	Tipo de mensaje no reconocido
0	0	0	0	1	0	1	Elemento de información fuera de secuencia
0	0	0	0	1	1	0	Elemento de información facultativo repetido
0	0	0	0	1	1	1	Elemento de información obligatorio faltante
0	0	0	1	0	0	0	Elemento de información no reconocido
0	0	0	1	0	0	1	Error de contenido de elemento de información obligatorio
0	0	0	1	0	1	0	Error de contenido de elemento de información facultativo
0	0	0	1	0	1	1	Mensaje no compatible con el estado del protocolo BCC
0	0	0	1	1	0	0	Elemento de información obligatorio repetido
0	0	0	1	1	0	1	Demasiados elementos de información
NOTA – Todos los demás valores están reservados.							

La subcláusula 16.5.8 especifica cuándo han de utilizarse los diferentes valores de tipo de causa de error de protocolo.

El campo de diagnóstico es un campo de múltiples octetos (el número de octetos depende del valor de la causa) que proporciona el diagnóstico pertinente para cada valor de causa de error de protocolo de conformidad con el Cuadro 44.

CUADRO 44/G.965

Diagnóstico para los tipos de error de protocolo

Causa	Diagnóstico	Longitud
Error de discriminador de protocolo	No presente	0
Tipo de mensaje no reconocido	Identificador de tipo de mensaje	1
Elemento de información fuera de secuencia	Identificador de tipo de mensaje Identificador de elemento de información	2
Elemento de información facultativo repetido	Identificador de tipo de mensaje Identificador de elemento de información	2
Elemento de información obligatorio faltante	Identificador de tipo de mensaje Identificador de elemento de información	2
Elemento de información no reconocido	Identificador de tipo de mensaje Identificador de elemento de información	2
Error de contenido de elemento de información obligatorio	Identificador de tipo de mensaje Identificador de elemento de información	2
Error de contenido de elemento de información facultativo	Identificador de tipo de mensaje Identificador de elemento de información	2
Mensaje no compatible con el estado del protocolo BCC	Identificador de tipo de mensaje	1
Elemento de información obligatorio repetido	Identificador de tipo de mensaje Identificador de elemento de información	2
Demasiados elementos de información	Identificador de tipo de mensaje	1

17.4.2.7 Elemento de información conexión incompleta

El elemento de información conexión incompleta tiene por objeto indicar desde la red de acceso a la central local que el resultado de un proceso de verificación no es fructuoso debido a que no existe conexión AN.

Dentro del campo de motivo, este elemento de información da información acerca del motivo por el cual esa conexión está incompleta.

La longitud del elemento de información conexión incompleta será de 3 octetos.

La estructura del elemento de información conexión incompleta será tal como se indica en la Figura 24.

8	7	6	5	4	3	2	1	
1	1	0	0	0	0	0	1	Octeto 1
	Identificador del elemento de información							
Longitud del contenido del elemento de información								Octeto 2
1 ext	Motivo							Octeto 3

FIGURA 24/G.965

Elemento de información conexión incompleta

La codificación del campo motivo del elemento de información conexión incompleta será tal como se especifica en el Cuadro 45.

CUADRO 45/G.965

Codificación del campo de motivo

7	6	5	4	3	2	1	Motivo
0	0	0	0	0	0	0	Incompleto normal
0	0	0	0	0	0	1	Avería de red de acceso
0	0	0	0	0	1	0	Puerto de usuario no aprovisionado
0	0	0	0	0	1	1	Identificación de intervalo de tiempo V5 inválida
0	0	0	0	1	0	0	Identificación de enlace a 2048 kbit/s V5 inválida
0	0	0	0	1	0	1	Intervalo de tiempo utilizado como canal C físico
NOTA – Todos los demás valores están reservados.							

17.5 Descripción del protocolo BCC y de los procedimientos BCC

En el Anexo K se proporciona información adicional sobre la interacción de las llamadas conmutadas con el protocolo BCC.

17.5.1 Generalidades

Debido a la transparencia de la AN y la interfaz V5.2 con relación a los protocolos de control de llamada RDSI y RTPC, el procedimiento pertinente a este protocolo BCC ha de ser ocasionado por la entidad de gestión de recursos de la LE como consecuencia del análisis de los procedimientos de control de llamada RDSI/RTPC.

Desde el punto de vista del BCC, cada asignación o desasignación de intervalo de tiempo V5 se considera como un proceso independiente que ha de concluir con la compleción fructuosa o el aborto de la asignación o desasignación del intervalo de tiempo V5.

Cada uno de los procesos estará identificado por un número de referencia BCC diferente. La entidad de protocolo BCC y la entidad de gestión de recursos permitirán que se lleven a cabo múltiples procesos BCC en paralelo.

NOTA – A los efectos del protocolo BCC (procedimientos de control de canal portador) se supone que ha de implementarse una FSM individual para cada una de las peticiones de asignación o desasignación relacionadas con uno o más intervalos de tiempo V5.2 disponibles para ser utilizados como canales portadores.

Los procedimientos que forman el protocolo BCC, y que se describen en las subcláusulas siguientes, son los siguientes:

- asignación de canal portador: procedimiento normal;
- asignación de canal portador: procedimientos excepcionales;
- desasignación de canal portador: procedimiento normal;
- desasignación de canal portador: procedimientos excepcionales;
- procedimiento de verificación;
- procedimiento de notificación de fallo interno de la AN;
- tratamiento de las condiciones de error.

17.5.2 Asignación de canal portador – Procedimiento normal

La entidad de protocolo BCC en la LE, al estar en el estado «Bcc nulo», y recibir la primitiva petición MDU-BCC-ASIGNACIÓN iniciará la asignación del canal portador enviando a la AN un mensaje ASIGNACIÓN que indica el o los intervalos de tiempo V5 en la interfaz V5.2 que han de utilizarse. En el caso de asignaciones relacionadas con puertos RDSI, la LE indicará también el o los intervalos de tiempo de puerto de usuario RDSI en la interfaz usuario-red RDSI que han de transconectarse con el intervalo de tiempo V5 seleccionado.

Con el envío del mensaje ASIGNACIÓN, la LE arrancará el temporizador Tbcc1 y entrará en el estado «Bcc espera de asignación».

Al recibir el mensaje DESASIGNACIÓN, la entidad de protocolo BCC en la AN notificará el evento a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC ASIGNACIÓN. Cuando sea posible la AN asignará el o los intervalos de tiempo V5 especificados al puerto especificado. Después de la recepción de la primitiva respuesta MDU-BCC-ASIGNACIÓN (COMPLETA), la entidad de protocolo BCC en la AN enviará a la LE el mensaje ASIGNACIÓN COMPLETA.

Con la recepción de un mensaje ASIGNACIÓN COMPLETA que, mediante el análisis del elemento de información número de referencia BCC, la LE considera como respuesta a un mensaje ASIGNACIÓN enviado previamente, la LE parará el temporizador Tbcc1, notificará a la entidad de gestión de recursos mediante la primitiva confirmación MDU-BCC-ASIGNACIÓN, y entrará en el estado «Bcc nulo».

Si el temporizador Tbcc1 expira por primera vez antes de la recepción del mensaje ASIGNACIÓN COMPLETA o RECHAZO DE ASIGNACIÓN, la LE retransmitirá el mensaje ASIGNACIÓN, rearrancará el temporizador Tbcc1 y permanecerá en el estado «Bcc espera de asignación».

Si el temporizador Tbcc1 expira por segunda vez antes de la recepción del mensaje ASIGNACIÓN COMPLETA o RECHAZO DE ASIGNACIÓN, el proceso será concluido entrándose en el estado «Bcc nulo». El evento será notificado también a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-ERROR-ASIGNACIÓN, para que se realice la acción de mantenimiento adecuada.

17.5.3 Asignación de canal portador – Procedimientos excepcionales

17.5.3.1 Asignación de canal portador

La entidad de protocolo BCC en la LE, al estar en el estado NULO y recibir un mensaje ASIGNACIÓN COMPLETA, informará a la gestión de recursos emitiendo la primitiva confirmación MDU-BCC-ASIGNACIÓN y permanecerá en el estado NULO. Esta situación puede ocurrir debido a pérdida de mensajes y expiración de temporizadores de la capa 3 pero habiendo retransmisión del mensaje por la capa 2. Pertenece al gestor de recursos realizar la acción necesaria.

17.5.3.2 Rechazo de asignación de canal portador

Si la entidad de control en la AN recibe el mensaje ASIGNACIÓN y el gestor de recursos de la AN detecta que el o los intervalos de tiempo V5 solicitados no pueden ser asignados al puerto identificado (y al intervalo de tiempo de puerto de usuario, si procede) en las condiciones solicitadas, la entidad de gestión de recursos generará una primitiva respuesta MDU-BCC-RECHAZO-ASIGNACIÓN, y la AN notificará el evento enviando a la LE el mensaje RECHAZO DE ASIGNACIÓN, especificando en el elemento de información causa de rechazo el motivo de este rechazo.

Con la recepción de un mensaje RECHAZO DE ASIGNACIÓN que, mediante el análisis del elemento de información número de referencia BCC, la LE considera como la respuesta a un mensaje ASIGNACIÓN enviado previamente, la LE concluirá el proceso de asignación de canal portador, parará el temporizador Tbcc1, notificará a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-RECHAZO-ASIGNACIÓN, y entrará en el estado «Bcc nulo».

La entidad de protocolo BCC en la LE, al estar en el estado NULO y recibir un mensaje RECHAZO DE ASIGNACIÓN, informará a la entidad de recursos emitiendo la indicación MDU-BCC-RECHAZO-ASIGNACIÓN y permanecerá en el estado NULO. Esta situación puede ocurrir debido a la pérdida de mensajes y a la expiración de temporizadores de la capa 3, pero habiendo retransmisión del mensaje por la capa 2. Corresponde al gestor de recursos realizar cualquier acción que sea necesaria.

17.5.3.3 Aborto de asignación de canal portador

Estando en espera de la recepción de un mensaje ASIGNACIÓN COMPLETA o RECHAZO DE ASIGNACIÓN, si la entidad de protocolo BCC recibe una primitiva petición MDU-BCC-DESASIGNACIÓN en la que se solicita la liberación del canal portador que está estableciéndose (por ejemplo, como consecuencia de una liberación de llamada prematura), la LE procederá a desasignar el canal portador y parará el temporizador Tbcc1, enviará el mensaje DESASIGNACIÓN y arrancará el temporizador Tbcc2 y entrará en el estado «Bcc aborto de asignación».

Cuando esté en el estado «Bcc aborto de asignación», la LE descartará cualquier mensaje recibido ASIGNACIÓN COMPLETA o RECHAZO DE ASIGNACIÓN.

Cuando la entidad de protocolo BCC en la AN recibe el mensaje DESASIGNACIÓN, el evento es notificado a la entidad de gestión de recursos mediante una primitiva indicación MDU-BCC-DESASIGNACIÓN, después de lo cual la AN desasignará el o los intervalos de tiempo V5 especificados del puerto pertinente y enviará a la LE el mensaje DESASIGNACIÓN COMPLETA.

Con la recepción de un mensaje DESASIGNACIÓN COMPLETA que, por el análisis del elemento de información número de referencia BCC, la entidad de control BCC en la LE considera como respuesta a un mensaje DESASIGNACIÓN enviado previamente, el evento será notificado a la entidad de gestión de recursos en la LE mediante una primitiva confirmación MDU-BCC-DESASIGNACIÓN, a continuación de lo cual el temporizador Tbcc2 será parado y se entrará en el estado «Bcc nulo».

Si el temporizador Tbcc2 expira por primera vez antes de la recepción del mensaje DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN, la LE retransmitirá el mensaje DESASIGNACIÓN, rearrancará el temporizador Tbcc2 y permanecerá en el estado «Bcc aborto de asignación».

Si el temporizador Tbcc2 expira por segunda vez antes de la recepción del mensaje DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN, el procedimiento concluirá, entrándose en el estado «Bcc nulo». El evento será notificado también a la entidad de gestión de recursos mediante una primitiva indicación MDU-BCC-ERROR-DESASIGNACIÓN, a fin de que se realice la acción de mantenimiento adecuada.

17.5.3.4 Petición de asignación de canal portador recibida para una conexión existente

Cuando la entidad de gestión de recursos en la AN recibe un mensaje ASIGNACIÓN en el que se solicita la asignación de un canal portador ya establecido, la AN transmitirá un mensaje ASIGNACIÓN COMPLETA.

17.5.3.5 Asignación de canal portador, contraorden de conexión solicitada

En algunas condiciones de servicio (por ejemplo, como consecuencia de la negociación del intervalo de tiempo de puerto de usuario DSS1 en la interfaz usuario-red RDSI llamada), la LE arrancará un proceso de asignación de canal portador BCC en un intervalo de tiempo V5 de interfaz V5.2 ya involucrado en una conexión con el mismo puerto de usuario. La LE notificará la petición mediante el campo indicador «contraorden» contenido en el elemento de información identificación de intervalo de tiempo V5 del mensaje ASIGNACIÓN transmitido.

Al recibir un mensaje ASIGNACIÓN que contiene una petición de contraorden, la AN procederá a completar la asignación de canal portador contraordenando la conexión anterior mediante el envío de mensaje ASIGNACIÓN COMPLETA de conformidad con el procedimiento normal para la asignación de canal portador descrita en 17.5.2. En caso de que la LE solicite la contraorden de una conexión no completada en el puerto de usuario especificado en el mensaje ASIGNACIÓN, la AN rechazará el procedimiento de asignación enviando un mensaje RECHAZO DE ASIGNACIÓN de conformidad con el procedimiento de rechazo de asignación de canal portador descrito en 17.5.3.2.

17.5.4 Desasignación de canal portador – Procedimiento normal

La entidad de gestión de recursos en la LE notificará la necesidad de desasignar un canal portador mediante una primitiva petición MDU-BCC-DESASIGNACIÓN. A continuación, la entidad de protocolo BCC en la LE, estando en el estado «Bcc nulo», iniciará la desasignación del canal portador enviando a la AN un mensaje DESASIGNACIÓN en el que se indica el o los intervalos de tiempo V5 en la interfaz V5.2 que han de liberarse.

Con el envío del mensaje DESASIGNACIÓN, la LE arrancará el temporizador Tbcc3 y entrará en el estado «Bcc espera de desasignación».

Cuando la entidad de protocolo BCC en la AN recibe el mensaje DESASIGNACIÓN, el evento es notificado a la entidad de gestión de recursos mediante una primitiva indicación MDU-BCC-DESASIGNACIÓN. A continuación la AN desasignará el o los intervalos de tiempo V5 especificados del puerto pertinente y enviará a la LE el mensaje DESASIGNACIÓN COMPLETA.

Con la recepción de un mensaje DESASIGNACIÓN COMPLETA que, por el análisis del elemento de información número de referencia BCC, la entidad de protocolo BCC en la LE considera como la respuesta a un mensaje DESASIGNACIÓN enviado previamente, el evento será notificado mediante una primitiva confirmación MDU-BCC-DESASIGNACIÓN, después de lo cual la LE parará el temporizador Tbcc3 y entrará en el estado «Bcc nulo».

Si el temporizador Tbcc3 expira por primera vez antes de la recepción del mensaje DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN, la LE transmitirá el mensaje DESASIGNACIÓN, rearrancará el temporizador Tbcc3 y permanecerá en estado «Bcc espera de desasignación».

Si el temporizador Tbcc3 expira por segunda vez antes de la recepción del mensaje DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN, el procedimiento abortará, entrándose en el estado «Bcc nulo». El evento será notificado también a la entidad de gestión de recursos mediante la primitiva MDU-BCC (error de desasignación), a fin de que realice la acción de mantenimiento adecuada.

17.5.5 Desasignación de canal portador – Procedimientos excepcionales

17.5.5.1 Desasignación de canal portador

La entidad de protocolo BCC en la LE, al estar en el estado NULO y recibir un mensaje DESASIGNACIÓN COMPLETA, informará a la gestión de recursos emitiendo una confirmación MDU-BCC-DESASIGNACIÓN y permanecerá en el estado NULO. Esta situación puede producirse debido a la pérdida de mensajes y a la expiración de temporizadores de la capa 3, pero habiendo retransmisión del mensaje por la capa 2. Corresponde al gestor de recursos realizar la acción necesaria.

17.5.5.2 Rechazo de desasignación de canal portador

Después de recibirse un mensaje DESASIGNACIÓN, cuando la entidad de gestión de recursos en la AN detecta que el o los intervalos de tiempo V5 solicitados no pueden ser desasignados del puerto identificado (y del intervalo de tiempo de puerto de usuario, si procede), o no pueden ser desasignados en las condiciones solicitadas por la LE, se generará una primitiva respuesta MDU-BCC-RECHAZO-DESASIGNACIÓN, y la AN notificará el evento enviando a la LE el mensaje RECHAZO DE DESASIGNACIÓN, especificando en el elemento causa de rechazo el motivo de este rechazo.

Con la recepción de un mensaje RECHAZO DE DESASIGNACIÓN que, por el análisis del elemento de información número de referencia BCC, la entidad de protocolo BCC en la LE considera como la respuesta a un mensaje DESASIGNACIÓN enviado previamente, la LE concluirá el procedimiento de desasignación de canal portador, parará el temporizador Tbcc3, notificará a la entidad de gestión de recursos mediante una primitiva indicación MDU-BCC-RECHAZO-DESASIGNACIÓN, y entrará en el estado «Bcc nulo».

La entidad de protocolo BCC en la LE, al estar en el estado NULO y recibir un mensaje RECHAZO DE DESASIGNACIÓN, informará a la gestión de recursos emitiendo una indicación MDU-BCC-RECHAZO-DESASIGNACIÓN y permanecerá en el estado NULO. Esta situación puede producirse debido a la pérdida de mensajes y a la expiración de los temporizadores de la capa 3, pero habiendo retransmisión del mensaje por la capa 2. Corresponde al gestor de recursos realizar la acción necesaria.

17.5.5.3 Falta mensaje de proceso de desasignación de canal portador

Cuando la entidad de gestión de recursos en la AN reciba un mensaje DESASIGNACIÓN que se refiere al intervalo de tiempo V5 y al puerto (y al intervalo de tiempo de puerto de usuario, cuando proceda) considerados libres, la AN transmitirá un mensaje DESASIGNACIÓN COMPLETA.

17.5.6 Procedimiento de verificación

La entidad de protocolo BCC en la LE, al estar en el estado «Bcc nulo» y recibir la primitiva petición MDU-BCC-VERIFICACIÓN, iniciará el procedimiento de verificación enviando a la AN un mensaje VERIFICACIÓN que indica el intervalo de tiempo V5 a 64 kbit/s o el puerto de usuario y el intervalo de tiempo de puerto de usuario, si procede, en los que hay que realizar la verificación.

Con el envío del mensaje VERIFICACIÓN, la LE arrancará el temporizador Tbcc4 y entrará en el estado «BCC espera de verificación».

Cuando la entidad de protocolo BCC en la AN reciba el mensaje VERIFICACIÓN, notificará el evento a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-VERIFICACIÓN. A continuación, el gestor de recursos de la AN ha de verificar la información recibida con su información interna en relación con las conexiones de canal portador establecidas en la AN. Después de esta comprobación, la AN notificará a la LE la conexión portadora relacionada con la información suministrada por la LE o la ausencia de conexión que corresponda a la información proporcionada por la LE. Después de la recepción de la primitiva respuesta MDU-BCC-VERIFICACIÓN, la entidad de protocolo BCC en la AN enviará a la LE el mensaje VERIFICACIÓN COMPLETA.

Con la recepción de un mensaje VERIFICACIÓN COMPLETA que, por el análisis del elemento de información número de referencia BCC, la LE considera como la respuesta a un mensaje VERIFICACIÓN enviado previamente, la LE parará el temporizador Tbcc4, notificará a la entidad de gestión de recursos mediante la primitiva confirmación MDU-BCC-VERIFICACIÓN, y entrará en el estado «Bcc nulo».

Si el temporizador Tbcc4 expira por primera vez antes de la recepción del mensaje VERIFICACIÓN COMPLETA, la LE retransmitirá el mensaje VERIFICACIÓN, rearrancará el temporizador Tbcc4 y permanecerá en el estado «BCC espera de verificación».

Si el temporizador Tbcc4 expira por segunda vez antes de la recepción del mensaje VERIFICACIÓN COMPLETA, el proceso concluirá, entrándose en el estado «Bcc nulo». El evento será notificado también a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-ERROR-VERIFICACIÓN, para que se lleve a cabo la acción de mantenimiento apropiada.

17.5.7 Procedimiento de notificación de fallo interno de la AN

La entidad de protocolo BCC en la AN, al estar en el estado «Bcc operacional» y recibir la primitiva petición MDU-BC-AVERÍA-AN iniciará el procedimiento de notificación de fallo interno de la AN enviando a la LE un mensaje AVERÍA DE AN que indica la conexión portadora a 64 kbit/s afectada por el fallo interno de la AN, especifica el intervalo de tiempo V5 o el puerto de usuario y el intervalo de tiempo de puerto de usuario, cuando proceda, o ambos.

Con el envío de un mensaje AVERÍA DE AN, la AN arrancará el temporizador Tbcc5 y entrará en el estado «BCC informe de avería de AN».

Cuando la entidad de protocolo BCC en la LE recibe el mensaje AVERÍA DE AN, notificará el evento a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-AVERÍA-AN y enviará a la AN el mensaje ACUSE DE AVERÍA DE AN.

Con la recepción de un mensaje ACUSE DE AVERÍA DE AN que, por el análisis del elemento de información número de referencia BCC, la AN considera como la respuesta a un mensaje AVERÍA DE AN enviado previamente, la AN parará el temporizador Tbcc5, notificará a la entidad de gestión de recursos mediante la primitiva confirmación MDU-BCC-AVERÍA-AN y entrará en el estado «Bcc operacional».

Si el temporizador Tbcc5 expira por primera vez antes de la recepción del mensaje ACUSE DE AVERÍA DE AN, la AN retransmitirá el mensaje AVERÍA DE AN, rearrancará el temporizador Tbcc5 y permanecerá en el estado «Bcc informe de avería de AN».

Si el temporizador Tbcc5 expira por segunda vez antes de la recepción del mensaje ACUSE DE AVERÍA DE AN, el proceso concluirá, entrándose en el estado «Bcc operacional». El evento se notificará también a la entidad de gestión de recursos mediante la primitiva indicación MDU-BCC-ERROR-AVERÍA-AN, para que se realice la acción de mantenimiento apropiada.

17.5.8 Tratamiento de las condiciones de error

Antes de actuar sobre un mensaje, la entidad receptora, ya sea la entidad de protocolo BCC V5.2 de la AN o la entidad de protocolo BCC V5.2 de la LE, realizará los procedimientos especificados en esta subcláusula.

Por regla general, todos los mensajes incluirán por lo menos los elementos de información discriminador de protocolo, número de referencia BCC y tipo de mensaje. Estos elementos de información, actuando como encabezamiento de todos los mensajes BCC, se especifican en 13.2. Al recibir un mensaje con menos de 4 octetos, la entidad de protocolo BCC receptora en la AN o la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia la gestión del sistema e ignorará el mensaje.

Si se detectan más de dos elementos de información facultativos en un mensaje, dicho mensaje será considerado demasiado largo y será truncado después del segundo elemento de información facultativo. Se supone que toda la información truncada son elementos de información facultativos repetidos. Al efectuar el truncamiento, la entidad reaccionará de conformidad con 17.5.8.4 para los elementos de información repetidos.

Cada recepción de un mensaje del conjunto de mensajes del protocolo BCC activará las comprobaciones descritas en 17.5.8.1 a 17.5.8.10 por orden de precedencia. No ocurre ningún cambio de estado durante estas comprobaciones.

Después de que el mensaje haya sido comprobado mediante los procedimientos de tratamiento de error que siguen, si el mensaje no ha de ser ignorado, entonces seguirán:

- los procedimientos de asignación de canal portador (véanse 17.5.2 y 17.5.3); o
- los procedimientos de desasignación de canal portador (véanse 17.5.4 y 17.5.5); o
- el procedimiento de verificación (véase 17.5.6); o
- el procedimiento de notificación de fallo interno de la AN (véase 17.5.7).

NOTA – En esta subcláusula, el término «ignorar el mensaje» significa dejar sin modificaciones el contenido del mensaje.

17.5.8.1 Error de discriminador de protocolo

Cuando una entidad de protocolo BCC de capa 3 recibe un mensaje con un discriminador de protocolo codificado de manera distinta a lo especificado en 13.2.1 para los protocolos V5:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «error de discriminador de protocolo»;
- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

17.5.8.2 Error de tipo de mensaje

Cuando se reciba un mensaje no reconocido:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «tipo de mensaje no reconocido» e incluya el diagnóstico correspondiente tal como se especifica en 17.4.2.6;
- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

17.5.8.3 Elemento de información fuera de secuencia

Un elemento de información que tiene un valor de código de identificador de elemento de información inferior al valor de código del elemento de información precedente será considerado como un elemento de información fuera de secuencia.

Cuando se reciba un elemento de información fuera de secuencia:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento de información que esté fuera de secuencia y proseguirá el procesamiento del mensaje; asimismo, enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «elemento de información fuera de secuencia», incluido el diagnóstico correspondiente tal como se especifica en 17.4.2.6;

– la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento de información que esté fuera de secuencia y continuará el tratamiento del mensaje.

Si el elemento de información retirado es obligatorio, esto dará lugar a una situación de error correspondiente a la falta de un elemento de información obligatorio, que será tratada de conformidad con 17.5.8.5.

17.5.8.4 Elementos de información repetidos

Cuando un elemento de información obligatorio esté repetido en un mensaje, la reacción de la entidad receptora será la siguiente:

– la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «elemento de información obligatorio repetido», incluido el diagnóstico correspondiente tal como se especifica en 17.4.2.6;

– la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

Cuando un elemento de información facultativo esté repetido en un mensaje, la reacción de la entidad receptora será la siguiente:

– la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento de información facultativo repetido y continuará el tratamiento del mensaje; asimismo, enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «elemento de información facultativo repetido», incluido el diagnóstico correspondiente tal como se especifica en 17.4.2.6;

– la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento de información facultativo repetido y continuará el tratamiento del mensaje.

17.5.8.5 Elemento de información obligatorio faltante

Cuando se reciba un mensaje en el que falte un elemento de información obligatorio, la reacción de la entidad receptora será la siguiente:

– la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «elemento de información obligatorio faltante», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

– la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

En caso de que falte más de un elemento de información obligatorio, la reacción de la entidad receptora estará basada en el primer elemento de información obligatorio identificado como faltante.

17.5.8.6 Elemento de información no reconocido

Cuando se reciba un mensaje con uno o más elementos de información no reconocidos, la reacción de la entidad receptora será la siguiente:

– la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO al sistema de gestión, retirará todos los elementos de información no reconocidos y continuará el tratamiento del mensaje; asimismo, enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «elemento de información no reconocido», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

– la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO al sistema de gestión, retirará todos los elementos de información no reconocidos y continuará el tratamiento del mensaje.

En caso de que haya más de un elemento de información no reconocido, la reacción de la entidad receptora se basará en el primer elemento de información no reconocido identificado.

A efectos de los procedimientos de tratamiento de errores de protocolo BCC, los elementos de información no reconocidos son los que no están definidos en 13.2 y 17.4.

17.5.8.7 Error de contenido de elemento de información obligatorio

Cuando se recibe un mensaje con un elemento de información obligatorio que tiene un error de contenido tal que:

a) la longitud no es conforme a la longitud especificada en 13.2 y 17.4; o

b) el contenido no es conocido, entonces:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «error de contenido de elemento de información obligatorio», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

17.5.8.8 Error de contenido de elemento de información facultativo

Cuando se recibe un mensaje con un elemento de información facultativo que tiene un error de contenido tal que:

a) la longitud no es conforme a la longitud especificada en 17.4; o

b) el contenido no es conocido o no puede ser interpretado, entonces:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento que tiene el error de contenido y continuará el tratamiento del mensaje; asimismo, enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «error de contenido de elemento de información facultativo», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, retirará el elemento de información que tiene un error de contenido y continuará el tratamiento del mensaje.

17.5.8.9 Mensaje inesperado

Se produce un error de flujo de mensajes cuando se recibe un mensaje inesperado. Los cuadros de transición de estados indican la acción apropiada que debe realizarse al recibir cualquier evento.

Cuando se recibe un mensaje inesperado, no se produce ningún cambio de estado y:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa de error de protocolo «mensaje no compatible con el estado del protocolo BCC», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

17.5.8.10 Elemento de información facultativo no admitido

Cuando se recibe un mensaje que contiene más elementos de información facultativos que los que se necesitan, entonces:

- la entidad de protocolo BCC de la AN generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO que indique la causa del error de protocolo «demasiados elementos de información», incluido el diagnóstico correspondiente, tal como se especifica en 17.4.2.6;

- la entidad de protocolo BCC de la LE generará una primitiva indicación MDU-BCC-ERROR-PROTOCOLO hacia el sistema de gestión e ignorará el mensaje.

17.6 Lista de los parámetros (temporizadores) del sistema

En el Cuadro 46 se da la definición de los temporizadores utilizados en el protocolo BCC. Los temporizadores mencionados se mantienen en la entidad de protocolo BCC de la LE o la AN. Las tolerancias de los temporizadores serán de ±10%.

CUADRO 46/G.965

Temporizadores del protocolo BCC

Número de temporizador	Valor de expiración	Estado	Causa de arranque	Parada normal	Al expirar por primera vez	Al expirar por segunda vez	Referencia
Tbcc1	500 a 1500 ms (Nota)	LE Bcc0 LE Bcc1	envío de ASIGNACIÓN	Después de recepción de ASIGNACIÓN COMPLETA, RECHAZO DE ASIGNACIÓN, o una petición de aborto de asignación	Repetir ASIGNACIÓN y rearrancar Tbcc1	Proceso de asignación concluido y notificación a la gestión de recursos	17.5.2
Tbcc2	2 s	LE Bcc1 LE Bcc2	envío de DESASIGNACIÓN	Después de recepción de DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN	Repetir DESASIGNACIÓN y rearrancar Tbcc2	Proceso de desasignación concluido y notificación a la gestión de recursos	17.5.3
Tbcc3	2 s	LE Bcc2 LE Bcc3	envío de DESASIGNACIÓN	Después de recepción de DESASIGNACIÓN COMPLETA o RECHAZO DE DESASIGNACIÓN	Repetir DESASIGNACIÓN y rearrancar Tbcc3	Proceso de desasignación concluido y notificación a la gestión de recursos	17.5.4
Tbcc4	500 a 1500 ms (Nota)	LE Bcc3 LE Bcc4	envío de VERIFICACIÓN	Después de recepción de VERIFICACIÓN COMPLETA	Repetir VERIFICACIÓN y rearrancar Tbcc4	Proceso de verificación concluido y notificación a la gestión de recursos	17.5.6
Tbcc5	500 a 1500 ms (Nota)	AN Bcc0 AN Bcc1	envío de AVERÍA DE AN	Después de recepción de ACUSE DE RECIBO DE AVERÍA DE AN	Repetir AVERÍA DE AN y rearrancar Tbcc5	Proceso de avería de AN concluido y notificación a la gestión de recursos	17.5.7
NOTA – Estos temporizadores podrán predefinirse por pasos de 100 ms y tendrán todos el mismo valor de expiración.							

17.7 Cuadros de transición de estados en el lado LE y en el lado AN

El Cuadro 47 define el cuadro de transiciones de estado para un proceso en el lado LE de la entidad de protocolo BCC V5.2.

CUADRO 47/G.965

Cuadro de transiciones de estado en la LE

Estado / Evento	Bcc nulo (LEBcc0)	Bcc espera de asignación (LEBcc1)	Bcc aborto de asignación (LEBcc2)	Bcc espera de desasignación (LEBcc3)	Bcc espera de verificación (LEBcc4)
Petición MDU-BCC-ASIGNACIÓN	ASIGNACIÓN; arrancar Tbcc1; LEBcc1; –	/	/	/	/
ASIGNACIÓN COMPLETA	Confirmación MDU-BCC-ASIGNACIÓN; –	Confirmación MDU-BCC-ASIGNACIÓN; parar Tbcc1; LEBcc0	–	/	/
RECHAZO DE ASIGNACIÓN	Indicación MDU-BCC-RECHAZO-ASIGNACIÓN; –	Indicación MDU-BCC-RECHAZO-ASIGNACIÓN; parar Tbcc1; LEBcc0	–	/	/
Petición MDU-BCC-DESASIGNACIÓN	DESASIGNACIÓN; arrancar Tbcc3; LEBcc3	DESASIGNACIÓN; parar Tbcc1; parar Tbcc2; LEBcc2	/	/	/
DESASIGNACIÓN COMPLETA	Confirmación MDU-BCC-DESASIGNACIÓN; –	/	Confirmación MDU-BCC-DESASIGNACIÓN; parar Tbcc2; LEBcc0	Confirmación MDU-BCC-DESASIGNACIÓN; parar Tbcc3; LEBcc0	/
RECHAZO DE DESASIGNACIÓN	Indicación MDU-BCC-RECHAZO-DESASIGNACIÓN; –	/	Indicación MDU-BCC-RECHAZO-DESASIGNACIÓN; parar Tbcc2; LEBcc0	Indicación MDU-BCC-RECHAZO-DESASIGNACIÓN; parar Tbcc3; LEBcc0	/
Petición MDU-BCC-VERIFICACIÓN	VERIFICACIÓN; arrancar Tbcc4; LEBcc4	/	/	/	/
VERIFICACIÓN COMPLETA	/	/	/	/	Confirmación MDU-BCC-VERIFICACIÓN; parar Tbcc4; LEBcc0
Expiración Tbcc1 (primera)	/	ASIGNACIÓN; rearrancar Tbcc1; –	/	/	/
Expiración Tbcc1 (segunda)	/	Indicación MDU-BCC-ERROR-ASIGNACIÓN; LEBcc0	/	/	/
Expiración Tbcc2 (primera)	/	/	DESASIGNACIÓN; rearrancar Tbcc2; –	/	/
Expiración Tbcc2 (segunda)	/	/	Indicación MDU-BCC-ERROR-DESASIGNACIÓN; LEBcc0	/	/
Expiración Tbcc3 (primera)	/	/	/	DESASIGNACIÓN; rearrancar Tbcc3; –	/
Expiración Tbcc3 (segunda)	/	/	/	Indicación MDU-BCC-ERROR-DESASIGNACIÓN; LEBcc0	/
Expiración Tbcc4 (primera)	/	/	/	/	VERIFICACIÓN; rearrancar Tbcc4; –
Expiración Tbcc4 (segunda)	/	/	/	/	Indicación MDU-BCC-ERROR-VERIFICACIÓN; LEBcc0
AVERÍA DE AN	ACUSE AVERÍA AN; Indicación MDU-BCC-AVERÍA-AN; –	/	/	/	/
ERROR DE PROTOCOLO	/	Indicación MDU-BCC-ERROR-PROTOCOLO; parar Tbcc1; LEBcc0	Indicación MDU-BCC-ERROR-PROTOCOLO; parar Tbcc2; LEBcc0	Indicación MDU-BCC-ERROR-PROTOCOLO; parar Tbcc3; LEBcc0	Indicación MDU-BCC-ERROR-PROTOCOLO; parar Tbcc4; LEBcc0
– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado.					

El Cuadro 48 define el cuadro de transiciones de estado para un proceso en el lado AN de la entidad de protocolo BCC V5.2.

CUADRO 48/G.965

Cuadro de transiciones de estado en la AN

Estado / Evento	Bcc operacional (ANBcc0)	Bcc informe de avería de AN (ANBcc1)
ASIGNACIÓN	Indicación MDU-BCC-ASIGNACIÓN; ANBcc0	/
Respuesta MDU-BCC-ASIGNACIÓN COMPLETA	ASIGNACIÓN COMPLETA; ANBcc0	/
Respuesta MDU-BCC-RECHAZO-ASIGNACIÓN	RECHAZO DE ASIGNACIÓN; ANBcc0	/
DESASIGNACIÓN	Indicación MDU-BCC-DESASIGNACIÓN; ANBcc0	/
Respuesta MDU-BCC-DESASIGNACIÓN COMPLETA	DESASIGNACIÓN COMPLETA; ANBcc0	/
Respuesta MDU-BCC-RECHAZO-DESASIGNACIÓN	RECHAZO DE DESASIGNACIÓN ANBcc0	/
VERIFICACIÓN	Indicación MDU-BCC-VERIFICACIÓN; ANBcc0	/
Respuesta MDU-BCC-VERIFICACIÓN	VERIFICACIÓN COMPLETA; ANBcc0	/
Petición MDU-BCC-AVERÍA-AN	AVERÍA DE AN, arrancar Tbcc5; ANBcc1	/
ACUSE DE AVERÍA DE AN	/	Confirmación MDU-BCC-AVERÍA-AN, parar Tbcc5; ANBcc0
Expiración de Tbcc5 (primera)	/	AVERÍA DE AN, rearrancar Tbcc5; ANBcc1
Expiración de Tbcc5 (segunda)	/	Indicación MDU-BCC-ERROR-AVERÍA-AN; ANBcc0
– Ningún cambio de estado; / Evento inesperado, ningún cambio de estado.		

18 Especificación del protocolo de protección

18.1 Consideraciones generales

18.1.1 Introducción

Una sola interfaz V5.2 puede contener hasta dieciséis (16) enlaces de 2048 kbit/s. De acuerdo con la arquitectura de protocolo y la estructura de multiplexión (ver cláusula 8), un trayecto de comunicación puede cursar información asociada a varios enlaces de 2048 kbit/s (transferencia de información no asociada). Por consiguiente, el fallo de un trayecto de comunicación puede afectar al servicio de un elevado número de abonados de manera inaceptable. Ello es especialmente cierto en el caso del protocolo BCC, del protocolo de control y del protocolo de control del enlace, donde todos los puertos de usuario resultan afectados si se produce un fallo en el trayecto de comunicación pertinente.

Para mejorar la fiabilidad de la interfaz V5.2, se proporcionan procedimientos de protección para la conmutación de los trayectos de comunicación que han fallado.

Los mecanismos de protección se utilizarán para proteger todos los canales C activos. Dichos mecanismos protegerán igualmente el propio trayecto C del protocolo de protección que se emplea para controlar los procedimientos de conmutación de protección.

El protocolo de protección no protege los canales portadores ni permite la reconfiguración de dichos canales si se produce un fallo en su enlace de 2048 kbit/s asociado. Si aparece dicho fallo, las conexiones de los abonados en estos canales portadores fallarán. Esto se considera aceptable teniendo en cuenta la probabilidad muy reducida de que se produzcan tales fallos.

El suceso primario para el que se requiere protección es el fallo de los enlaces de 2048 kbit/s. El protocolo de protección deberá ofrecer protección igualmente frente a fallos persistentes de los enlaces de datos V5 (es decir, fallo persistente de uno de los enlaces de datos para el protocolo de control, de control del enlace, de BCC, de la RTPC o de protección). Además, se deberán supervisar de forma continua las banderas de todos los canales C físicos (canales C activos y de reserva) a fin de protegerlos contra fallos no detectados aún por los mecanismos de detección de capa 1. Si se detecta un fallo en un canal C de reserva, deberá notificarse de dicha circunstancia a la gestión del sistema y, como resultado, no se conmutará un canal C lógico a dicho canal C de reserva no operativo. Otros fallos de los equipos (en otras capas, o dentro de la AN o de la LE) se tratarán de forma separada, en una realización particular, y caen fuera del ámbito de la especificación V5.

No se dispondrá de protección alguna para los canales C lógicos en el caso de un solo enlace de 2048 kbit/s. Ello supone que no habrá protocolo de protección en el intervalo de tiempo 16 ni en ningún otro canal C físico y durante el arranque del sistema no se establecerá el enlace de datos para protección.

Tras la conmutación se restablecerán todos los enlaces de datos LAPV5 afectados, salvo los enlaces de datos del protocolo de protección (intervalos de tiempo 16 en los enlaces primario y secundario). Si falla el intervalo de tiempo 16 del enlace primario o secundario tras la recuperación del fallo, el enlace de datos para protección que ha fallado se restablecerá de manera automática. Como resultado de un procedimiento de conmutación de protección, que puede incluir también el restablecimiento de los enlaces de datos LAPV5, pueden perderse los mensajes de capa 2 y/o los mensajes de capa 3. Corresponde a las entidades de protocolo de capa 3 pertinentes la cobertura de estas situaciones.

En esta subcláusula se indican los principios y la especificación del protocolo de control.

18.1.2 Aprovisionamiento de los canales C físicos y lógicos

Debe establecerse la correspondencia entre el trayecto C y los canales C lógicos, tanto en la LE como en la AN.

Debe aprovisionarse la correspondencia inicial entre los canales C lógicos y los canales C físicos, tanto en la LE como en la AN.

Los dos trayectos C para el protocolo de protección se aprovisionarán siempre en los intervalos de tiempo 16 de los enlaces primario y secundario y no deberán conmutarse por el mecanismo de protección.

Los trayectos C del protocolo de control, del enlace de control y de BCC arrancarán en el intervalo de tiempo 16 del enlace primario. El intervalo de tiempo 16 del enlace secundario se utilizará para la protección de los trayectos C del protocolo de control, de control del enlace y de BCC.

En la transmisión de trama se concederá prioridad a los mensajes del protocolo de protección sobre otros mensajes en el mismo canal C físico. La controversia se resuelve basándose en la dirección de envolvente, que es única para los mensajes del protocolo de protección, dando prioridad a la EFaddr = 8179.

Cada interfaz V5.2 que conste de más de un enlace de 2048 kbit/s tendrá un grupo 1 de protección y, si se aprovisiona, un grupo 2 de protección.

El grupo 1 de protección se incluirá siempre en el intervalo de tiempo 16 del enlace primario y el intervalo de tiempo 16 del enlace secundario. Por consiguiente, para el grupo 1 de protección se utilizan los siguientes valores fijos (véanse las definiciones):

N1 = 1; y

K1 = 1.

Si se aprovisiona el grupo 2 de protección, se dispondrá de N2 canales C lógicos (y los trayectos C contenidos) y se incorporará un grupo de K2 canales C de reserva, siendo:

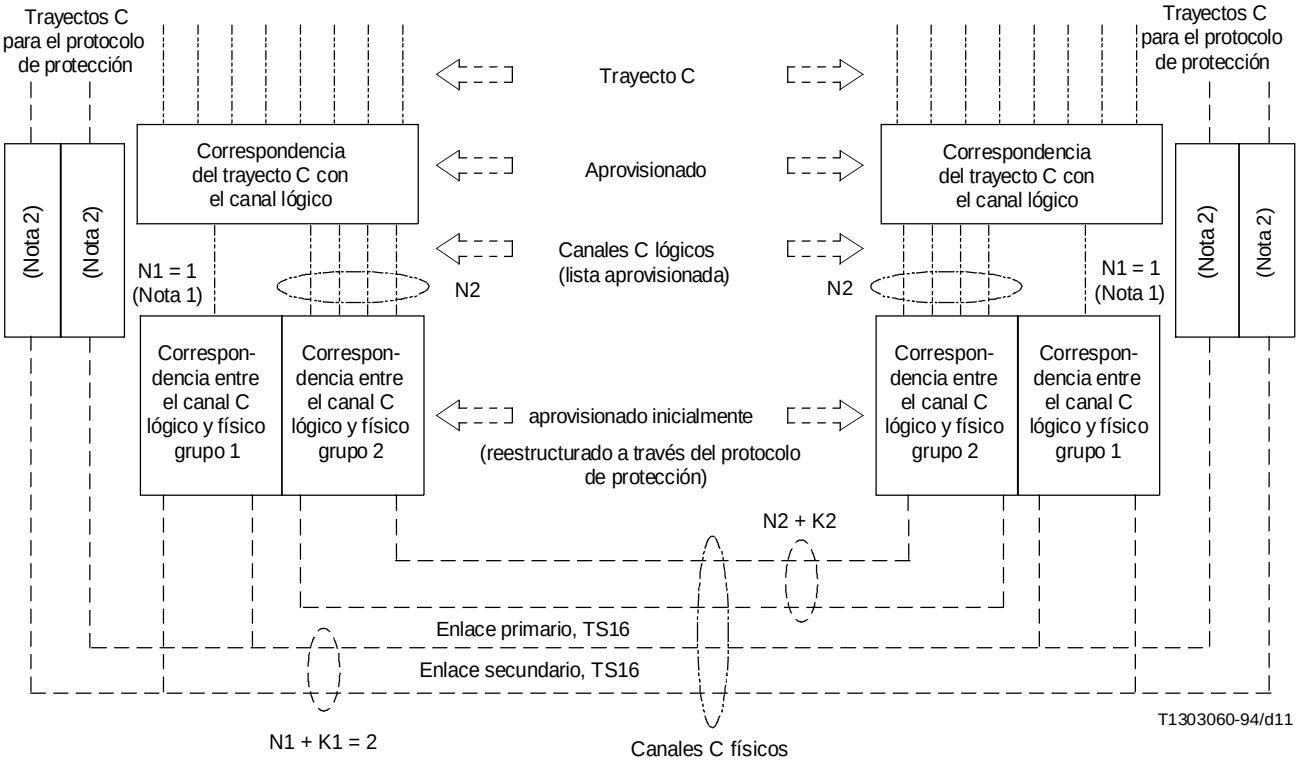
$1 \leq K2 \leq 3$; y

$1 \leq N2 \leq (3 \times L - 2 - K2)$,

donde L es el número de enlaces de 2048 kbit/s en la interfaz V5.2. K2 se elegirá de tal forma que sea igual o mayor al máximo número de canales C físicos en cualquier enlace sencillo de 2048 kbit/s de dicha interfaz V5.2. Para esta regla no se consideran los intervalos de tiempo 16 de los enlaces primario y secundario. Esta regla asegura la protección de todos los canales C activos en caso de que se produzca un fallo en uno de los enlaces de 2048 kbit/s.

NOTA – Puede que el operador de red no establezca ningún canal C de reserva para el grupo 2 de protección 2 (K2 = 0), si no se requiere protección para los canales C lógicos del grupo 2 de protección. Sin embargo, en ese caso algunos fallos de los enlaces de 2048 kbit/s pueden repercutir en los servicios relacionados con los canales C lógicos averiados.

En la Figura 25 aparece la correspondencia de los trayectos C con el canal C lógico y, por lo tanto, con los canales C físicos.



NOTAS

1 Trayectos C del protocolo de control, del protocolo de control del enlace y del protocolo BCC más, de manera opcional, otros trayectos C.

2 Asignación del trayecto C al canal C físico.

FIGURA 25/G.965

Correspondencia entre los trayectos C con los canales C lógicos y, por consiguiente, con los canales C físicos

18.1.3 Separación de responsabilidades

Una conmutación de protección puede ser activada de manera autónoma por la gestión del sistema en la LE o la AN como resultado de una detección de avería o de un procedimiento de bloqueo del enlace, o por el operador u operadores a través de las interfaces Q_{LE} y Q_{AN}. Para el grupo 1 de protección, la gestión del sistema no permitirá la conmutación iniciada por el operador u operadores a través de las interfaces Q_{AN} o Q_{LE}.

La LE tendrá el control a efectos de conmutación de protección en el sentido de que dicha LE asignará otro canal C físico a ese canal C lógico.

La AN puede solicitar una conmutación de cualquiera de los canales C lógicos en cualquier instante. Si la conmutación ha sido iniciada por el operador de la AN a través de la Q_{AN}, éste puede solicitar la conmutación a un canal C físico preferido. En ese caso, la LE satisfará esa petición, en la medida de lo posible. Si no hay ninguna preferencia del lado AN (como sucede siempre si el fallo se detecta en la AN y la conmutación autónoma es iniciada por la gestión del sistema AN), la gestión del sistema LE elegirá un canal C de reserva disponible.

La AN puede rechazar una instrucción de conmutación de protección de la LE si por cualquier razón no puede satisfacerla. Si la LE o la AN no pueden cumplir la petición, dicha circunstancia deberá ser notificada a través de la interfaz Q_{LE} y Q_{AN} indicando la causa.

18.1.4 Gestión de los recursos de canal C tras el fallo

La gestión del sistema LE decidirá qué canal C físico se utilizará para proteger un canal C lógico. Con respecto a la gestión y control de los recursos disponibles deberán seguirse las reglas siguientes.

Si la conmutación de protección se activa de manera autónoma por la gestión del sistema en la LE o la AN como resultado de la detección de un fallo, no se reservarán los canales C activos para proteger otro canal C lógico. Este principio se aplicará igualmente a una conmutación iniciada a través de la interfaz Q_{AN}.

Unicamente el operador de la LE (a través de Q_{LE}) puede solicitar la asignación de un canal C lógico averiado a un canal C activo (canal C físico que ya cursa un canal C lógico). En este caso se enviará una instrucción especializada a la AN y ésta no rechazará la conmutación debido al hecho de que ya se ha asignado un canal C lógico a este canal C físico. La AN desasignará los canales C lógicos previamente asignados y asignará los nuevos canales C lógicos, que deberán protegerse. El canal C lógico desasignado se protegerá mediante el mecanismo de protección normal, siempre que haya recursos disponibles. Este mecanismo permite al operador de la LE proteger manualmente los protocolos con mayor prioridad (por ejemplo, el protocolo RTPC) en caso de que se produzcan fallos en varios enlaces de 2048 kbit/s, aun en situaciones en que no haya tenido éxito el procedimiento de protección autónomo debido a la falta de recursos (canales C de reserva operativos).

Cuando se necesite protección, se seleccionará y utilizará un canal C de reserva disponible del mismo grupo de protección. Si se dispone de más de un canal C de reserva, el gestor de recursos seguirá la siguiente secuencia de asignación. En primer lugar se utilizarán todos los canales C de reserva disponibles en los intervalos de tiempo 16, a continuación se utilizarán los intervalos de tiempo 15 y por último los intervalos de tiempo 31. Una vez restaurado el enlace, todos los canales C físicos aprovisionados en dicho enlace pasarán a ser canales C de reserva (la conmutación de protección no es reversible).

Además, el reaprovisionamiento permitiría imponer manualmente la prioridad si fuese necesario debido a condiciones de avería grave (por ejemplo, fallo de los enlaces primario y secundario). Los servicios soportados por la interfaz V5 no están disponibles durante el reaprovisionamiento de la interfaz V5 y el arranque del sistema. La prioridad, impuesta de forma manual durante el aprovisionamiento inicial, puede cambiar tras una conmutación de protección; por ejemplo, como resultado de un fallo en un enlace de 2048 kbit/s.

En caso de que se produzca dicho fallo, el gestor de recursos para el protocolo de protección conmutará en primer lugar el canal C lógico en el TS16, a continuación el que se encuentra en el TS15 y por último el del TS31, mientras se disponga de recursos. Si no pueden conmutarse todos los canales C lógicos a canales C físicos, debe notificarse esta circunstancia al operador de la red a través de Q_{LE} y Q_{AN}.

La pérdida de los trayectos C de protección, de BCC, de control y de control del enlace, debido a fallos en ambos enlaces de 2048 kbit/s, primario y secundario, puede subsanarse únicamente mediante reaprovisionamiento en otro enlace de 2048 kbit/s.

Las acciones de conmutación deberán ser secuenciales, es decir, sólo se efectuará una segunda conmutación una vez completada la primera.

Deberá invocarse solamente una acción por mensaje de protocolo de protección (por ejemplo, conmutar el canal C lógico X al canal C de reserva Y).

Una petición de conmutación de la AN o una instrucción de conmutación de la LE pueden ser reconocidas o rechazadas únicamente por la entidad par. El mensaje de rechazo no deberá incluir ninguna propuesta de conmutación alternativa. Cada extremo puede iniciar una nueva acción de conmutación como resultado del rechazo de una conmutación.

18.1.5 Funciones de supervisión y detección de fallos

El suceso primario para el que se requiere protección es el fallo de los enlaces de 2048 kbit/s.

Además de la supervisión de capa 1, deberán realizarse otras dos funciones de supervisión para detectar los fallos de canal C y desencadenar la conmutación de protección autónoma. Estos métodos son la supervisión de bandera y la supervisión del enlace de datos.

18.1.5.1 Fallo de un enlace de 2048 kbit/s

Al recibir una primitiva MDU-DI de la FSM de control del enlace en la AN o la LE (véase 16.1), la gestión del sistema en la AN o la LE activará una conmutación autónoma de todos los canales C activos en dicho enlace de 2048 kbit/s.

18.1.5.2 Supervisión de bandera

Las banderas deberán supervisarse de manera continua tanto en los canales C activos como de reserva.

Si no se recibe ninguna bandera en un canal C físico durante un periodo de tiempo de 1 segundo, dicho canal C físico se considerará como no operativo y se emitirá una indicación de error a la gestión del sistema. Esta indicación deberá tener el mismo significado que la recepción de una primitiva indicación MDL-LIBERACIÓN de la FSM del enlace de datos V5. Mientras persista la situación, esta condición deberá notificarse a la gestión del sistema de manera continua, a la velocidad de una vez por segundo.

Si se recibe al menos una bandera en un canal C físico durante un periodo de tiempo de 1 segundo, se considerará dicho canal como operativo.

18.1.5.3 Supervisión del enlace de datos

En la AN y en la LE se utilizará supervisión del enlace de datos (capa 2) en los canales que cursen trayectos C cuando existe un enlace de datos V5 completo terminado en la AN (es decir, protocolos de protección, de control, de control del enlace, BCC y RTPC).

Si la gestión del sistema de la AN o la LE recibe una primitiva indicación MDL-LIBERACIÓN de uno de los LAPV5-DL, el canal C físico que curse el trayecto C se considerará como no operativo. La gestión del sistema activará una conmutación de protección de dicho canal C lógico.

Una vez realizada la conmutación, el lado LE intentará restablecer los enlaces de datos LAPV5 afectados. Si la gestión del sistema recibe otra primitiva indicación MDL-LIBERACIÓN como resultado de un fallo en el trayecto C que ha provocado la conmutación, la gestión del sistema correspondiente no iniciará una nueva conmutación a menos que se reciba mientras tanto una primitiva indicación MDL-ESTABLECIMIENTO o confirmación MDL-ESTABLECIMIENTO. Ello significa que la FSM del enlace de datos del trayecto C que ha fallado tomará en primer lugar el estado múltiple trama establecida (al menos una vez) antes de activar una segunda conmutación al recibir una primitiva indicación MDL-LIBERACIÓN. De no ser así, se supone que se ha producido un fallo interno del que no es posible recuperarse con el mecanismo de protección V5. En este caso la gestión del sistema iniciará las acciones adecuadas.

18.1.6 Modelo funcional del protocolo de protección

Se establecerá de manera permanente un enlace de datos independiente en cada TS16 del enlace primario y secundario. Los procedimientos para la capa del enlace de datos se especifican en 10.4.

La EFaddr y la correspondiente V5DLaddr para el protocolo de protección en el TS16 del enlace primario y el TS16 del enlace secundario deberán tener el mismo valor y deberán estar codificadas de acuerdo con lo indicado en 9.2 y 10.3.2.3.

Los dos enlaces de datos se utilizan para cursar información entre las entidades de protocolo de protección en la AN y la LE. Cada mensaje L3 se difundirá por ambos enlaces de datos. La entidad par de capa 3 que reciba los mensajes de ambos enlaces de datos procesará el mensaje en su primera aparición y a continuación ignorará los mensajes de datos idénticos recibidos por el otro enlace de datos. Se utilizarán números de secuencia para distinguir entre un mensaje recibido la primera vez y un mensaje que ya ha sido recibido por el otro enlace de datos.

Al detectar un fallo que haga necesaria la conmutación de protección, la gestión del sistema de LE o AN invocará una conmutación utilizando las unidades de datos de gestión (MDU, *management data units*).

Si se realiza una conmutación de protección, se notificará tal circunstancia a las interfaces Q_{AN} y Q_{LE}, indicando el estado actual de los canales C lógicos y físicos afectados.

Los sistemas operativos de la LE y la AN pueden recuperar la correspondencia actual entre los canales C lógicos y los canales C físicos, si así se solicita, a través de Q_{AN} y Q_{LE}.

La Figura 26 muestra el modelo funcional del protocolo de protección.

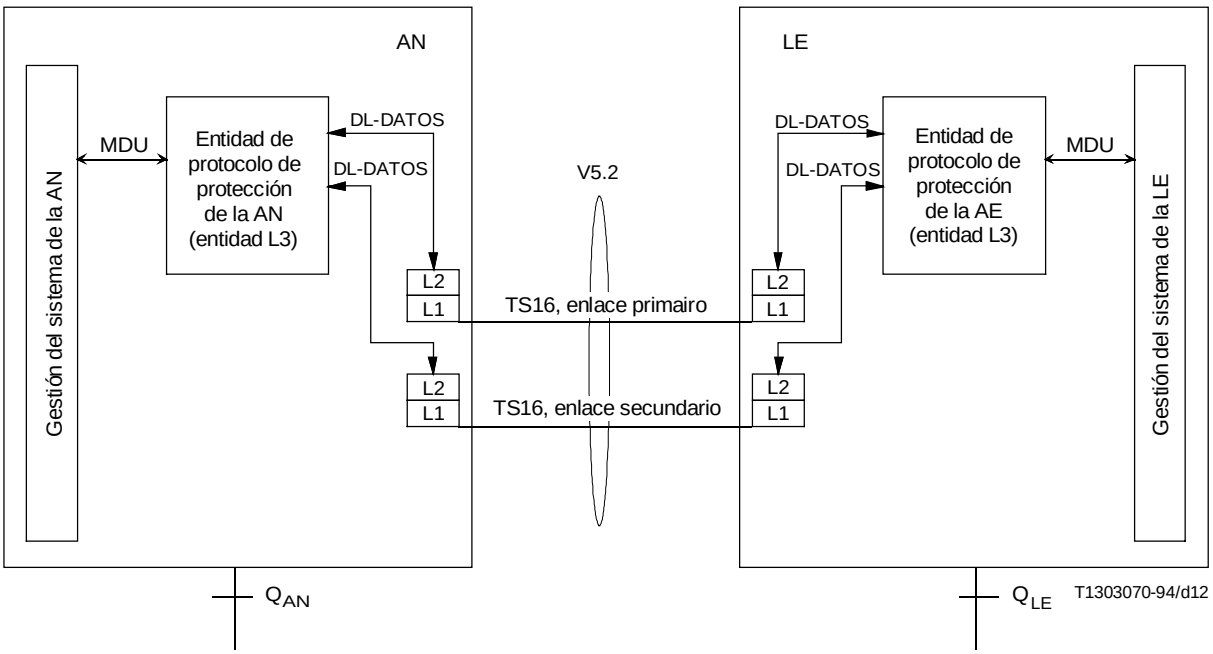


FIGURA 26/G.965

Modelo funcional del protocolo de protección

18.2 Otros principios

La conmutación de protección se realizará de manera efectiva basándose en un canal C lógico; es decir, sin cambiar la asignación del trayecto C al canal C lógico debido a la conmutación de protección.

Cuando se protege un canal C lógico, todos los trayectos C de dicho canal dejan el canal C activo y se conmutan a un solo canal C de reserva.

El hecho de que la realización conmute los canales C lógicos o los trayectos C individuales de un canal C lógico es un tema que cae fuera del ámbito de la presente Recomendación.

Tras la conmutación de un canal C lógico deberán restablecerse los siguientes enlaces de datos LAPV5, si son cursados en dicho canal C lógico: protocolo de BCC, de control del enlace, de control y de RTPC. Los enlaces de datos del protocolo de protección no se restablecerán de manera automática tras la conmutación. El restablecimiento de un enlace de datos del protocolo de protección se intentará únicamente en caso de fallo de dicho enlace de datos.

18.3 Definición de entidad de protocolo de protección

18.3.1 Definición de los estados del protocolo de protección

18.3.1.1 Estados en la AN

Estado NULO (SOAN0)

No se ha iniciado la conmutación ni por el lado AN ni por el lado LE.

Estado CONMUTACIÓN SOLICITADA POR AN (SOAN1)

La gestión del sistema AN ha solicitado la conmutación a través de una unidad de datos de gestión (MDU) especializada.

Estado CONMUTACIÓN INICIADA POR LE (SOAN2)

Se ha recibido del extremo LE un mensaje INSTRUCCIÓN DE CONMUTACIÓN o INSTRUCCIÓN OS-COMUTACIÓN. La gestión de sistema AN debe entonces decidir si es posible o no realizar la conmutación.

18.3.1.2 Estados en la LE

Estado NULO (SOLE0)

No se ha iniciado la conmutación ni por el lado AN ni por el lado LE.

Estado CONMUTACIÓN INICIADA POR LE (SOLE1)

La gestión de sistema LE ha solicitado la conmutación mediante una MDU especializada.

Estado CONMUTACIÓN INICIADA POR AN (SOLE2)

Se ha recibido del lado AN un mensaje PETICIÓN DE CONMUTACIÓN. La gestión de sistema LE ha de decidir entonces si es posible o no realizar la conmutación.

18.3.2 Definición de los eventos del protocolo de protección

En los Cuadros 49 y 50 se definen las MDU, los mensajes y los temporizadores utilizados en las FSM de protección de AN y LE.

CUADRO 49/G.965

MDU, mensajes y temporizadores utilizados en la FSM de protección de AN

	Sentido	Descripción
MDU-protección (petición de conmutación)	PROTECCIÓN_AN ← SYS	La gestión del sistema ha detectado un fallo y solicita una conmutación, el OS-AN ha iniciado una conmutación a través de Q_{AN}
MDU-protección (acuse de conmutación)	PROTECCIÓN_AN ← SYS	La gestión de sistema acusa recibo de una conmutación en la AN
MDU-protección (rechazo de conmutación; causa)	PROTECCIÓN_AN ← SYS	La gestión de sistema rechaza una conmutación e indica la causa
MDU-protección (instrucción de conmutación)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección ha recibido una instrucción de conmutación de la LE
MDU-protección (instrucción OS-conmutación)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección ha recibido una instrucción de conmutación de OS-LE
MDU-protección (indicación de rechazo de conmutación; causa)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica la recepción de un mensaje de rechazo de conmutación a la gestión del sistema e indica la causa
MDU-protección (indicación de error de conmutación)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección señala la expiración del temporizador TSO2 a la gestión del sistema
MDU-protección (instrucción de reposición de SN)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica a la gestión del sistema que se ha iniciado la reposición de SN
MDU-protección (indicación de reposición de SN)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica la recepción de un mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN a la gestión del sistema
MDU-protección (acuse de reposición de SN)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica a la gestión del sistema que la entidad par ha acusado recibo de la reposición de SN
MDU-protección (indicación de error en reposición de SN)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica a la gestión del sistema que se ha producido un error en el procedimiento de reposición de SN
MDU-protección (petición de reposición de SN)	PROTECCIÓN_AN → SYS	La entidad de protocolo de protección indica a la gestión del sistema que la entidad par ha solicitado la reposición de SN
INSTRUCCIÓN DE CONMUTACIÓN	PROTECCIÓN_AN←PROTECCIÓN_LE	Iniciación por la LE de la conmutación
INSTRUCCIÓN DE OS-CONMUTACIÓN	PROTECCIÓN_AN←PROTECCIÓN_LE	Iniciación por OS-LE de la conmutación
PETICIÓN DE CONMUTACIÓN	PROTECCIÓN_AN→PROTECCIÓN_LE	Petición de conmutación por la AN
ACUSE DE CONMUTACIÓN	PROTECCIÓN_AN→PROTECCIÓN_LE	Respuesta positiva a una instrucción de conmutación
RECHAZO DE CONMUTACIÓN (causa)	PROTECCIÓN_AN↔PROTECCIÓN_LE	Rechazo de una instrucción de conmutación indicando la causa
INSTRUCCIÓN DE REPOSICIÓN DE SN	PROTECCIÓN_AN↔PROTECCIÓN_LE	Instrucción del número de secuencia de reposición
ACUSE DE REPOSICIÓN DE SN	PROTECCIÓN_AN↔PROTECCIÓN_LE	Acuse de recibo de que se han repuesto las variables de estado
MDU-protección (indicación de error de protocolo)	PROTECCIÓN_AN → SYS	El procedimiento de tratamiento de errores ha detectado un error de protocolo
Expiración de TSO3	Interno AN	El temporizador TSO3 ha expirado
Expiración de TSO4	Interno AN	El temporizador TSO4 ha expirado
Expiración de TSO5	Interno AN	El temporizador TSO5 ha expirado
PROTECCIÓN_AN Entidad de protocolo de protección en la AN PROTECCIÓN_LE Entidad de protocolo de protección en la LE SYS Gestión del sistema		

CUADRO 50/G.965

MDU, mensajes y temporizadores utilizados en la FSM de protección de LE

	Sentido	Descripción
MDU-protección (instrucción de conmutación)	PROTECCIÓN_LE ← SYS	La gestión del sistema ha detectado un fallo e inicia la conmutación, o se ha iniciado la conmutación por el OS-LE a través de Q_{LE} o por la AN a través de V5.2
MDU-protección (instrucción OS-conmutación)	PROTECCIÓN_LE ← SYS	El OS-LE ha iniciado una conmutación; esta instrucción puede provocar la reserva de un canal C físico que cursa actualmente un canal C lógico
MDU-protección (acuse de conmutación)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica la recepción de una respuesta de conmutación positiva de la AN a la gestión del sistema
MDU-protección (rechazo de conmutación; causa)	PROTECCIÓN_LE ← SYS	La gestión del sistema rechaza una conmutación e indica la causa
MDU-protección (petición de conmutación)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica la recepción de una petición de conmutación de la AN a la gestión del sistema
MDU-protección (indicación de rechazo de conmutación)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica la recepción de un mensaje de rechazo de conmutación a la gestión del sistema
MDU-protección (indicación de error de conmutación)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica la expiración del temporizador TSO1 a la gestión del sistema
MDU-protección (indicación de reposición de SN)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica la recepción de un mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN
MDU-protección (instrucción de reposición de SN)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica a la gestión del sistema que se ha iniciado la reposición de SN
MDU-protección (petición de reposición de SN)	PROTECCIÓN_LE ← SYS	La gestión del sistema inicia la reposición de SN durante el procedimiento de arranque del sistema
MDU-protección (acuse de reposición de SN)	PROTECCIÓN_LE → SYS	La entidad de protocolo de protección indica a la gestión del sistema que la entidad par ha acusado recibo de la reposición de SN
MDU-protección (indicación de error en la reposición de SN)	PROTECCIÓN_LE → SYS	Se indica a la gestión del sistema un error en el procedimiento de reposición
MDU-protección (indicación de error de protocolo)	PROTECCIÓN_LE → SYS	El procedimiento de tratamiento de errores ha detectado un error de protocolo
INSTRUCCIÓN DE CONMUTACIÓN	PROTECCIÓN_LE→PROTECCIÓN_AN	Iniciación de la conmutación por la LE
INSTRUCCIÓN DE OS-CONMUTACIÓN	PROTECCIÓN_LE→PROTECCIÓN_AN	Iniciación de la conmutación por OS-LE, puede ser necesaria la apropiación de un canal C activo
PETICIÓN DE CONMUTACIÓN	PROTECCIÓN_LE←PROTECCIÓN_AN	Petición de conmutación por la AN
ACUSE DE CONMUTACIÓN	PROTECCIÓN_LE←PROTECCIÓN_AN	Respuesta positiva a una instrucción de conmutación

CUADRO 50/G.965 *(fin)*

MDU, mensajes y temporizadores utilizados en la FSM de protección de LE

	Sentido	Descripción
RECHAZO DE CONMUTACIÓN (causa)	PROTECCIÓN_LE↔PROTECCIÓN_AN	Rechazo de una instrucción de conmutación indicando la causa
ERROR DE PROTOCOLO	PROTECCIÓN_LE←PROTECCIÓN_AN	El procedimiento del tratamiento de error en la AN ha detectado un error de protocolo, esta circunstancia se indica al lado LE
INSTRUCCIÓN DE REPOSICIÓN DE SN	PROTECCIÓN_LE↔PROTECCIÓN_AN	Instrucción de número de secuencia de reposición
ACUSE DE REPOSICIÓN DE SN	PROTECCIÓN_LE↔PROTECCIÓN_AN	Acuse de recibo de que se han repuesto las variables de estado
Expiración de TSO1	Interno LE	El temporizador TSO1 ha expirado
Expiración de TSO2	Interno LE	El temporizador TSO2 ha expirado
Expiración de TSO4	Interno LE	El temporizador TSO4 ha expirado
Expiración de TSO5	Interno LE	El temporizador TSO5 ha expirado
PROTECCIÓN_AN Entidad de protocolo de protección en la AN PROTECCIÓN_LE Entidad de protocolo de protección en la LE SYS Gestión del sistema		

18.4 Definición y contenido de los mensajes del protocolo de protección

En el Cuadro 51 aparece el conjunto completo de mensajes del protocolo de protección. En este punto se describe la estructura detallada de cada uno de estos mensajes.

CUADRO 51/G.965

Conjunto de mensajes del protocolo de protección

Codificación en el elemento de información de tipo de mensaje							Mensajes del protocolo de protección	Referencia
7	6	5	4	3	2	1		
0	0	1	1	0	0	0	PETICIÓN DE CONMUTACIÓN	18.4.1
0	0	1	1	0	0	1	INSTRUCCIÓN DE CONMUTACIÓN	18.4.2
0	0	1	1	0	1	0	INSTRUCCIÓN DE OS-CONMUTACIÓN	18.4.3
0	0	1	1	0	1	1	ACUSE DE CONMUTACIÓN	18.4.4
0	0	1	1	1	0	0	RECHAZO DE CONMUTACIÓN	18.4.5
0	0	1	1	1	0	1	ERROR DE PROTOCOLO	18.4.6
0	0	1	1	1	1	0	INSTRUCCIÓN DE REPOSICIÓN SN	18.4.7
0	0	1	1	1	1	1	ACUSE DE REPOSICIÓN SN	18.4.8

18.4.1 Mensaje PETICIÓN DE CONMUTACIÓN

Este menaje es utilizado por la AN para solicitar una conmutación de un canal C lógico a un canal C físico particular. El mensaje incluye una propuesta para la asignación del canal C lógico que ha fallado a un nuevo canal C físico.

En el Cuadro 52 se define el contenido del mensaje PETICIÓN DE CONMUTACIÓN.

CUADRO 52/G.965

Contenido del mensaje PETICIÓN DE CONMUTACIÓN

Tipo de mensaje: PETICIÓN DE CONMUTACIÓN
Sentido: AN a LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN a LE	M	1
Identificación de canal C lógico	18.5.1	AN a LE	M	2
Tipo de mensaje	13.2.3	AN a LE	M	1
Número de secuencia	18.5.2	AN a LE	M	3
Identificación de canal C físico	18.5.3	AN a LE	M	4

18.4.2 Mensaje INSTRUCCIÓN DE CONMUTACIÓN

Este mensaje es utilizado por la LE para iniciar una conmutación de un canal C lógico a un canal C físico en particular. El mensaje incluye la nueva asignación del canal C lógico al canal C de reserva concreto que cursará el canal C lógico tras efectuarse con éxito la conmutación.

En el Cuadro 53 se define el contenido del mensaje INSTRUCCIÓN DE CONMUTACIÓN.

CUADRO 53/G.965

Contenido del mensaje INSTRUCCIÓN DE CONMUTACIÓN

Tipo de mensaje: INSTRUCCIÓN DE CONMUTACIÓN
Sentido: LE a AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE a AN	M	1
Identificación de canal C lógico	18.5.1	LE a AN	M	2
Tipo de mensaje	13.2.3	LE a AN	M	1
Número de secuencia	18.5.2	LE a AN	M	3
Identificación de canal C físico	18.5.3	LE a AN	M	4

18.4.3 Mensaje INSTRUCCIÓN DE OS-CONMUTACIÓN

Este mensaje es utilizado por la LE para iniciar una conmutación de un canal C lógico a un canal C físico dado a petición del operador a través de Q_{LE}. El mensaje incluye la nueva asignación del canal C lógico a un canal C físico dado que cursará el canal C lógico tras realizarse con éxito la conmutación.

En el Cuadro 54 se define el contenido del mensaje INSTRUCCIÓN DE OS-CONMUTACIÓN.

CUADRO 54/G.965

INSTRUCCIÓN DE OS-CONMUTACIÓN

Tipo de mensaje: INSTRUCCIÓN DE OS-CONMUTACIÓN
Sentido: LE a AN

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	LE a AN	M	1
Identificación de canal C lógico	18.5.1	LE a AN	M	2
Tipo de mensaje	13.2.3	LE a AN	M	1
Número de secuencia	18.5.2	LE a AN	M	3
Identificación de canal C físico	18.5.3	LE a AN	M	4

18.4.4 Mensaje ACUSE DE CONMUTACIÓN

Este mensaje es utilizado por la AN para acusar recibo de la conmutación de un canal C lógico a un canal C físico dado como resultado de la instrucción de conmutación recibida de la LE.

En el Cuadro 55 se define el contenido del mensaje ACUSE DE CONMUTACIÓN.

CUADRO 55/G.965

ACUSE DE CONMUTACIÓN

Tipo de mensaje: ACUSE DE CONMUTACIÓN
Sentido: AN a LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN a LE	M	1
Identificación de canal C lógico	18.5.1	AN a LE	M	2
Tipo de mensaje	13.2.3	AN a LE	M	1
Número de secuencia	18.5.2	AN a LE	M	3
Identificación de canal C físico	18.5.3	AN a LE	M	4

18.4.5 Mensaje RECHAZO DE CONMUTACIÓN

Este mensaje es utilizado por la AN o la LE para indicar a la entidad par que no puede llevarse a cabo la conmutación.

En el Cuadro 56 se define el contenido del mensaje RECHAZO DE CONMUTACIÓN.

CUADRO 56/G.965

RECHAZO DE CONMUTACIÓN

Tipo de mensaje: RECHAZO DE CONMUTACIÓN
Sentido: Ambos

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	Ambos	M	1
Identificación de canal C lógico	18.5.1	Ambos	M	2
Tipo de mensaje	13.2.3	Ambos	M	1
Número de secuencia	18.5.2	Ambos	M	3
Identificación de canal C físico	18.5.3	Ambos	M	4
Causa del rechazo	18.5.5	Ambos	M	3

18.4.6 Mensaje ERROR DE PROTOCOLO

Este mensaje es utilizado por la AN para indicar al lado LE que se ha identificado un error de protocolo en un mensaje recibido. Se da la causa del error de protocolo.

En el Cuadro 57 se define el contenido del mensaje ERROR DE PROTOCOLO.

CUADRO 57/G.965

ERROR DE PROTOCOLO

Tipo de mensaje: ERROR DE PROTOCOLO
Sentido: AN a LE

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	AN a LE	M	1
Identificación de canal C lógico	17.5.1	AN a LE	M	2
Tipo de mensaje	13.2.3	AN a LE	M	1
Número de secuencia	17.5.2	AN a LE	M	3
Causa del error de protocolo	17.5.5	AN a LE	M	3 a 5

18.4.7 Mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN

Este mensaje es utilizado por la LE o la AN para indicar a la entidad par que ha aparecido un desajuste de las variables de estado de envío y recepción en el lado de envío y recepción y que todas las variables deben ponerse a cero.

En el Cuadro 58 se define el contenido del mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN.

CUADRO 58/G.965

INSTRUCCIÓN DE REPOSICIÓN DE SN

Tipo de mensaje: INSTRUCCIÓN DE REPOSICIÓN DE SN
Sentido: Ambos

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	Ambos	M	1
Identificación de canal C lógico	18.5.1	Ambos	M	2
Tipo de mensaje	13.2.3	Ambos	M	1

18.4.8 Mensaje ACUSE DE REPOSICIÓN DE SN

Este mensaje es utilizado por la LE o la AN para indicar a la entidad par que las variables de estado de envío y recepción se han puesto a cero.

En el Cuadro 59 se define el contenido del mensaje ACUSE DE REPOSICIÓN DE SN.

CUADRO 59/G.965

ACUSE DE REPOSICIÓN DE SN

Tipo de mensaje: ACUSE DE REPOSICIÓN DE SN
Sentido: Ambos

Elemento de información	Referencia	Sentido	Tipo	Longitud
Discriminador de protocolo	13.2.1	Ambos	M	1
Identificación de canal C lógico	18.5.1	Ambos	M	2
Tipo de mensaje	13.2.3	Ambos	M	1

18.5 Definición, estructura y codificación de los elementos de información del protocolo de protección

En este punto se define la codificación de los elementos de información específicos de los mensajes del protocolo de protección. Para cada uno de los elementos de información se indica la codificación de sus distintos campos.

Todos los elementos de información específicos del protocolo de protección, salvo el elemento de información de identificación del canal C lógico, se indican en el Cuadro 60, donde también aparece la codificación del identificador de elemento de información.

CUADRO 60/G.965

Elementos de información específicos del protocolo de protección

Codificación del elemento de información								Mensajes del protocolo de protección	Referencia
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	LONGITUD VARIABLE	
0	1	0	1	0	0	0	0	Número de secuencia	18.5.2
0	1	0	1	0	0	0	1	Identificación de canal C físico	18.5.3
0	1	0	1	0	0	1	0	Causa del rechazo	18.5.4
0	1	0	1	0	0	1	1	Causa del error de protocolo	18.5.5
NOTA – Todos los demás valores se reservan.									

18.5.1 Elemento de información identificación de canal C lógico

Tanto el lado AN como el lado LE mantendrán una lista aprovisionada de canales C lógicos. Cada canal C lógico viene identificado unívocamente mediante el número de identificación de canal C lógico correspondiente.

El número de identificación de canal C lógico tendrá una longitud de 16 bits y se codificará en sistema binario. Todos los números desde 0 hasta 65535 serán válidos. Pueden aprovisionarse hasta 44 distintos números de identificación de canal C lógico para una sola interfaz V5.2.

NOTA – El valor 44 corresponde al número máximo de canales C lógicos en una interfaz V5.2. Es igual al número máximo de canales C físicos (= 3 × 16 = 48) menos 1 canal C de reserva para el grupo 1 de protección y menos 3 canales C de reserva para el grupo 2 de protección (48 – 1 – 3 = 44).

La longitud del elemento de información identificación del canal C lógico será de 2 octetos.

En los mensajes INSTRUCCIÓN DE REPOSICIÓN DE SN y ACUSE DE REPOSICIÓN DE SN el valor de la identificación de canal C lógico será 0 (es decir, todos los bits se pondrán a cero).

La codificación del elemento de información identificación del canal C lógico se realizará de acuerdo con la Figura 27.

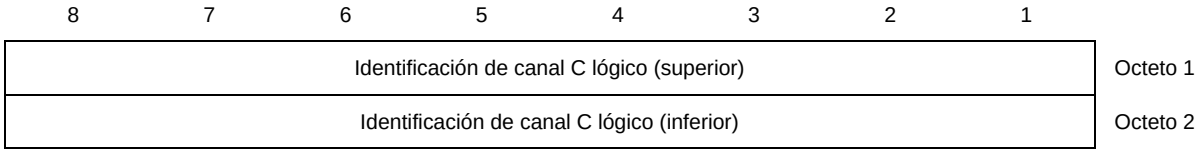


FIGURA 27/G.965

Elemento de información identificación de canal C lógico

18.5.2 Elemento de información número de secuencia

El elemento de información número de secuencia se utiliza en el lado de recepción para distinguir entre un mensaje recibido por primera vez y un mensaje que ya se ha recibido a través de otro enlace de datos para el protocolo de protección.

La longitud de este elemento de información será de 3 octetos.

El elemento de información número de secuencia contiene un campo de número de secuencia de 7 bits. El número de secuencia está codificado en sistema binario y puede tomar valores entre 0 y 127.

La codificación de este elemento de información será conforme a la Figura 28.

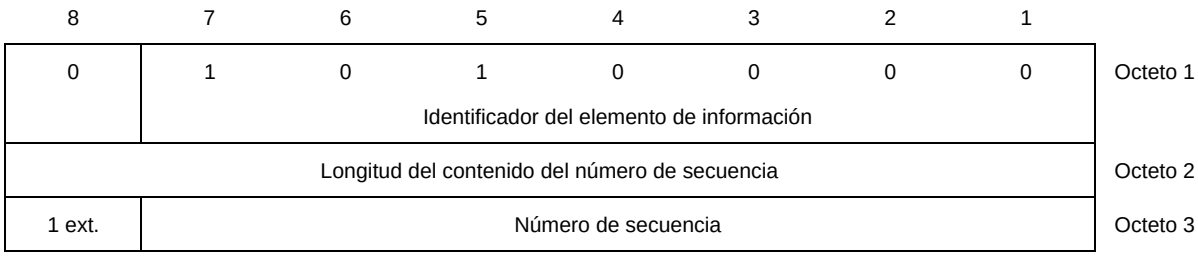


FIGURA 28/G.965

Elemento de información número de secuencia

18.5.3 Elemento de información identificación de canal C físico

Este elemento de información identifica el intervalo de tiempo en una interfaz V5.2 asignado a un canal C físico en particular. La gestión del sistema en la LE asegurará que en este elemento de información sólo se haga referencia a los intervalos de tiempo aprovisionados como canales C físicos.

La longitud del elemento de información identificación del canal C físico será de 4 octetos.

En la Figura 29 aparece la estructura del elemento de información identificación de canal C físico.

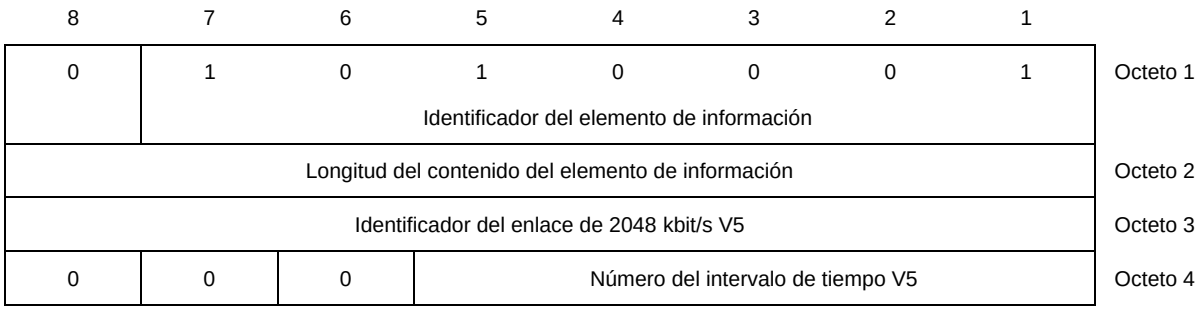


FIGURA 29/G.965

Elemento de información identificación de canal C físico

El identificador del enlace de 2048 kbit/s V5 es un campo de 8 bits utilizado para proporcionar la codificación binaria que identifica un enlace de 2048 kbit/s concreto entre los que constituyen la interfaz V5.2, donde se encuentra situado el intervalo de tiempo V5 seleccionado que va a utilizarse como canal C físico. Pueden identificarse de forma explícita un máximo de 256 (enlaces de 2048 kbit/s).

El número del intervalo de tiempo V5 es un campo de 5 bits utilizado para proporcionar la codificación binaria que identifica el intervalo de tiempo V5 (en el enlace de 2048 kbit/s identificado en el octeto anterior) que va a utilizarse como canal C físico.

18.5.4 Elemento de información causa de rechazo

El objetivo del elemento de información causa de rechazo es indicar a la entidad par las razones por las que se ha rechazado la conmutación de un canal C lógico en particular a otro canal C físico.

La longitud del elemento de información causa de rechazo será de 3 octetos.

La codificación del elemento de información causa de rechazo se realizará de acuerdo con la Figura 30.

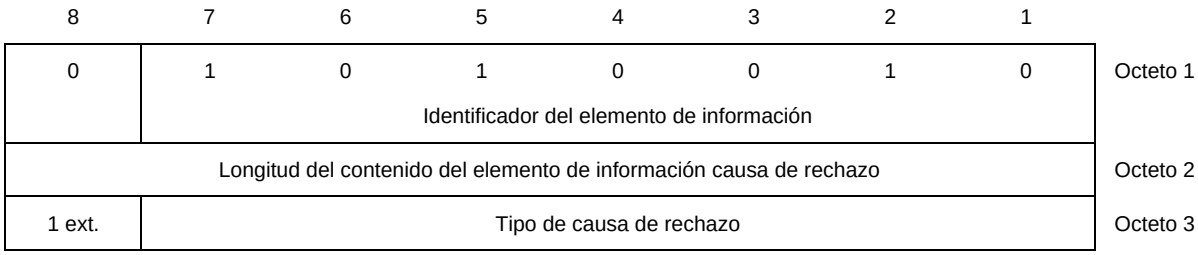


FIGURA 30/G.965

Elemento de información causa de rechazo

En el Cuadro 61 aparece la lista completa de los tipos de causa de rechazo y las codificaciones correspondientes. El cuadro indica igualmente en qué sentidos pueden utilizarse los tipos de causa de rechazo.

CUADRO 61/G.965

Codificación del campo tipo de causa de rechazo

7	6	5	4	3	2	1	Significado	Sentido
0	0	0	0	0	0	0	No hay disponible ningún canal C de reserva	LE a AN
0	0	0	0	0	0	1	Canal C físico objetivo no operativo	Ambos
0	0	0	0	0	1	0	Canal C físico objetivo no provisionado	Ambos
0	0	0	0	0	1	1	Conmutación de protección imposible (fallo AN/LE)	Ambos
0	0	0	0	1	0	0	Desajuste de grupo de protección	Ambos
0	0	0	0	1	0	1	La asignación solicitada ya existe	Ambos
0	0	0	0	1	1	0	El canal C físico objetivo ya tiene un canal C lógico	Ambos
NOTA – Todos los demás valores se reservan.								

18.5.5 Elemento de información causa de error de protocolo

El objetivo del elemento de información causa de error de protocolo es que la AN indique a la LE el tipo de error de protocolo detectado en un proceso determinado.

En algunos tipos de causa de error de protocolo, el elemento de información causa de error de protocolo incluirá un campo de diagnóstico a fin de ofrecer información adicional relativa a estos tipos de causa de error de protocolo. Cuando esté presente, este campo de diagnóstico de uno o dos octetos será una copia del identificador de tipo de mensaje recibido que haya activado el envío del mensaje que contiene el elemento de información causa de error de protocolo y, cuando sea necesario, del identificador del elemento de información pertinente dentro del mensaje.

La longitud del elemento de información causa de error de protocolo puede ser de 3 a 5 octetos. Para los tipos de causa de error de protocolo que no incluyan información de diagnóstico, la longitud del elemento de información será de 3 octetos. En los tipos de error de protocolo que incluyan información de diagnóstico, la longitud del elemento de información será de 4 ó 5 octetos.

La estructura del elemento de información causa de error de protocolo será la indicada en la Figura 31.

8	7	6	5	4	3	2	1	
0	1	0	1	0	0	1	1	Octeto 1
	Identificador del elemento de información							
Longitud del contenido del elemento de información								Octeto 2
1	Tipo de causa de error de protocolo							Octeto 3
0	Diagnóstico (identificador de tipo de mensaje)							Octeto 4
Diagnóstico (identificador del elemento de información)								Octeto 5

FIGURA 31/G.965

Elemento de información causa de error de protocolo

Se utiliza un campo de 7 bits para especificar el tipo de causa de error de protocolo, como se indica en el Cuadro 62.

CUADRO 62/G.965

Codificación del tipo de causa de error de protocolo

7	6	5	4	3	2	1	Tipo de causa de error de protocolo
0	0	0	0	0	0	1	Error de discriminador de protocolo
0	0	0	0	1	0	0	Tipo de mensaje no reconocido
0	0	0	0	1	1	1	Elemento de información obligatorio faltante
0	0	0	1	0	0	0	Elemento de información no reconocido
0	0	0	1	0	0	1	Error de contenido de elemento de información obligatorio
0	0	0	1	0	1	1	Mensaje no compatible con el estado del protocolo de protección
0	0	0	1	1	0	0	Elemento de información obligatorio repetido
0	0	0	1	1	0	1	Demasiados elementos de información
NOTA – Todos los demás valores se reservan.							

En 18.6.6 se indica cuándo deben utilizarse los distintos valores de tipo de causa de error de protocolo.

El campo de diagnóstico tiene varios octetos (el número de octetos depende del valor de la causa) y proporciona el diagnóstico pertinente para cada valor de causa de error de protocolo de acuerdo con el Cuadro 63.

CUADRO 63/G.965

Campo de diagnóstico para los tipos de error de protocolo

Causa	Diagnóstico	Longitud
Error de discriminador de protocolo	No está presente	0
Tipo de mensaje no reconocido	Identificador de tipo de mensaje	1
Elemento de información obligatorio faltante	Identificador de tipo de mensaje Identificador de elemento de información	2
Elemento de información no reconocido	Identificador de tipo de mensaje Identificador de elemento de información	2
Error de contenido de elemento de información obligatorio	Identificador de tipo de mensaje Identificador de elemento de información	2
Mensaje no compatible con el estado del protocolo de protección	Identificador de tipo de mensaje	1
Elemento de información obligatorio repetido	Identificador de tipo de mensaje Identificador de elemento de información	2
Demasiados elementos de información	Identificador de tipo de mensaje	1

18.6 Procedimientos del protocolo de protección

18.6.1 Consideraciones generales

El protocolo de protección es un protocolo funcional. Las entidades pares acusan recibo explícitamente tanto de la petición de conmutación desde el lado AN como de la instrucción de conmutación desde el lado LE mediante los mensajes INSTRUCCIÓN DE CONMUTACIÓN o ACUSE DE CONMUTACIÓN, respectivamente. La recepción de un acuse será supervisada por los temporizadores. Al expirar por primera vez un temporizador sin recibir acuse de la entidad par, el mensaje se retransmitirá. Al expirar por segunda vez, se enviará una indicación de error a la gestión del sistema y la entidad de protocolo de protección pasará al estado NULO sin retransmitir el mensaje nuevamente. La gestión del sistema tendrá entonces la responsabilidad de efectuar las acciones de mantenimiento necesarias.

Es responsabilidad de la gestión del sistema LE controlar a qué canal C físico se asignará un canal C lógico mediante el protocolo de protección. La gestión del sistema LE obtiene esta información de manera autónoma a partir del gestor de recursos de protección en la gestión del sistema LE en caso de un fallo detectado por la LE o esta información es suministrada por el operador de la LE a través de Q_{LE}.

Si la conmutación es iniciada por el operador a través de Q_{LE} y si éste ha decidido que es necesario reservar un canal C activo, la gestión del sistema LE indicará esta circunstancia a la entidad de protocolo de protección con una primitiva especializada [MDU-protección (instrucción OS-conmutación)]. No se utilizará la apropiación para el grupo 1 de protección.

La gestión del sistema AN puede iniciar una conmutación debido a la detección de un fallo interno o activada por el operador del OS a través de Q_{AN}. El operador puede indicar una preferencia por el canal C de reserva que va a utilizarse.

Al recibir una primitiva MDU-protección (instrucción de conmutación) o MDU-protección (instrucción OS-conmutación) la gestión del sistema AN verificará únicamente si los recursos necesarios para la conmutación están o no disponibles. Se comunicará a la LE el resultado de dicha verificación mediante un mensaje ACUSE DE CONMUTACIÓN o RECHAZO DE CONMUTACIÓN. Ello significa que no se acusará recibo de la propia conmutación realizada con éxito. Si posteriormente algún lado identifica problemas con la conmutación, debe iniciarse una nueva acción de conmutación.

18.6.2 Difusión de mensajes de protocolo de protección en los dos enlaces de datos del enlace primario y secundario

18.6.2.1 Transmisión de mensajes del protocolo de protección

Las entidades del protocolo de protección en la AN y la LE cursarán todo mensaje del protocolo de protección a través de las primitivas DL-DATOS a las correspondientes capas del enlace de datos en los intervalos de tiempo 16 del enlace primario y secundario. Cada entidad de protocolo de protección tendrá una variable de estado de emisión VP(S). Tras el arranque del sistema, dicha variable de estado de emisión VP(S) se pondrá a cero. Siempre que deba enviarse un mensaje de protocolo de protección que contenga un elemento de información número de secuencia, el número de secuencia (SN, *sequence number*) dentro de dicho elemento se pondrá al mismo valor que la variable de estado de emisión en el lado emisor. A continuación se emite el mensaje a las dos entidades de enlace de datos mediante las primitivas DL-DATOS y la variable de estado de emisión en el lado de emisión se incrementará en uno módulo 128.

NOTA – SN y VP(S) pueden tomar valores entre 0 y 127 y el módulo es 128.

18.6.2.2 Recepción de mensajes del protocolo de protección

Cada entidad de protocolo de protección contará con una variable de estado de recepción VP(R) que indica el número de secuencia del siguiente mensaje en secuencia que se espera recibir. Tras el arranque del sistema, la variable de estado de recepción VP(R) se pondrá a cero.

Un mensaje recibido por una entidad de protocolo de protección de capa 3 se verificará en primer lugar mediante el procedimiento de tratamiento de error especificado en 18.6.6.

Si el mensaje del protocolo de protección contiene un elemento de información número de secuencia, la entidad de protocolo de protección del lado receptor decidirá, basándose en SN junto con la variable de estado de recepción VP(R), si este mensaje ya se ha recibido a través de otro enlace de datos, si es un nuevo mensaje válido recibido por primera vez o si hay un desajuste entre las variables de estado de emisión y recepción en el lado de emisión y recepción, respectivamente.

NOTA 1 – VP(R) puede tomar valores entre 0 y 127 y el módulo es 128.

El lado receptor deberá:

- Ignorar el mensaje, si SN está en la gama $VP(R) - 5 \leq SN \leq VP(R) - 1$, sin notificación a la gestión del sistema.
- Considerar el mensaje como un nuevo mensaje válido, si SN se encuentra en la gama $VP(R) \leq SN \leq VP(R) + 4$. En este caso, en primer lugar se pondrá VP(R) al mismo valor que SN y a continuación se incrementará en uno módulo 128.
- De no ser así, el lado receptor supondrá que hay un desajuste entre las variables de estado en los lados emisor y receptor. La entidad de protocolo iniciará el procedimiento de reposición del número de secuencia, descrito en 18.6.2.3.

  NOTA 2 – Las desigualdades anteriores tiene en cuenta el módulo 128.

18.6.2.3 Procedimiento de reposición del numero de secuencia

18.6.2.3.1 Procedimiento normal

El procedimiento de reposición del número de secuencia es un procedimiento simétrico que iniciará la entidad que detecte un desajuste en las variables de estado. El procedimiento se iniciará igualmente durante el arranque del sistema una vez establecido al menos uno de los dos enlaces de datos para protección. En este caso, el procedimiento será iniciado por la gestión del sistema LE, que emitirá una primitiva MDU-protección (petición de reposición de SN) a la entidad de protocolo de protección LE. Este procedimiento hace uso de los mensajes INSTRUCCIÓN DE REPOSICIÓN DE SN y ACUSE DE REPOSICIÓN DE SN que no contienen un elemento de información número de secuencia.

La entidad que inicia el procedimiento de reposición enviará una INSTRUCCIÓN DE REPOSICIÓN DE SN a la entidad par, pondrá a cero la variable de estado de emisión VP(S) y la variable de estado de recepción VP(R), arrancará el temporizador TSO4 y enviará una primitiva MDU-protección (instrucción de reposición de SN) a la gestión del sistema. Si la LE ha activado la reposición de SN y la entidad de protocolo de protección LE no se encuentra en estado NULO (SOLE0) se detendrán, si están activos, los temporizadores TSO1 y TSO2 y la entidad de protocolo de protección LE volverá al estado NULO. Si la AN ha activado la reposición de SN y la entidad de protocolo de protección AN no se encuentra en estado NULO (SOAN0) se detendrá, si está activo, el temporizador TSO3 y la entidad de protocolo de protección AN volverá al estado NULO.

El lado que reciba el mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN responderá, siempre que el temporizador TSO5 no esté activo, con un mensaje ACUSE DE REPOSICIÓN DE SN, repondrá a cero la variable de estado de emisión VP(S) y la variable de estado de recepción VP(R), arrancará el temporizador TSO5 y enviará una primitiva MDU-protección (indicación de reposición de SN) a la gestión del sistema. Si la LE ha recibido el mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN y la entidad de protocolo de protección LE no se encuentra en estado NULO (SOLE0) se detendrán, si están activos, los temporizadores TSO1 y TSO2 y la entidad de protocolo de protección LE volverá al estado NULO. Si la AN ha recibido el mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN y la entidad de protocolo de protección AN no se encuentra en estado NULO (SOAN0) se detendrá, si está activo, el temporizador TSO3 y la entidad de protocolo de protección AN volverá al estado NULO.

Si se recibe INSTRUCCIÓN DE REPOSICIÓN DE SN mientras está activo el temporizador TSO5, no se producirá ninguna acción y no habrá ningún cambio de estado.

Al recibirse un mensaje ACUSE DE REPOSICIÓN DE SN, estando el temporizador TSO4 activo, se detendrá dicho temporizador y se enviará a la gestión del sistema una primitiva MDU-protección (acuse de reposición de SN). Al recibir un mensaje ACUSE DE REPOSICIÓN DE SN, si el temporizador TSO4 no está activo, no se producirá ninguna acción y no habrá ningún cambio de estado.

Mientras el temporizador TSO4 esté activo, todos los mensajes recibidos que contengan un elemento de información número de secuencia se descartarán sin notificación a la gestión del sistema. En ese caso, no se llevan a cabo los procedimientos de verificación de SN descritos en 17.6.2.2. No se producirá ningún cambio de estado.

Mientras el temporizador TSO4 esté activo en la AN, al recibirse una primitiva MDU-protección (petición de conmutación) en la AN, se enviará a la gestión de sistema una primitiva MDU-protección (ind. reposición SN error). No se producirá ningún cambio de estado.

Mientras el temporizador TSO4 en la LE esté activo, al recibirse una primitiva MDU-protección (instrucción de conmutación) o una primitiva MDU-protección (instrucción de OS-conmutación) en la LE, se enviará a la gestión del sistema una primitiva MDU-protección (indicación de error en reposición de SN). No se producirá ningún cambio de estado.

Al expirar el temporizador TSO5 no se producirá ninguna acción y no habrá ningún cambio de estado.

18.6.2.3.2 Procedimientos excepcionales

Al expirar por primera vez el temporizador TSO4, se enviará un mensaje INSTRUCCIÓN DE REPOSICIÓN DE SN a la entidad par, la variable de estado de emisión VP(S) y la variable de estado de recepción VP(R) se repondrán a cero, se enviará a la gestión del sistema una primitiva MDU-protección (instrucción de reposición de SN) y se reactivará el temporizador TSO4.

Al expirar por segunda vez el temporizador TSO4, se enviará a la gestión del sistema una primitiva MDU-protección (indicación de error en reposición de SN). Entonces corresponderá a la gestión del sistema la responsabilidad de efectuar las acciones adecuadas.

En caso de que expire de manera inesperada el temporizador TSO4 (es decir, cuando no se está en estado NULO) no se producirá ninguna acción y no habrá ningún cambio de estado.

18.6.3 Procedimiento de conmutación de protección normalizado iniciado por el lado LE

18.6.3.1 Procedimiento normal

Se utilizará este procedimiento si el lado LE detecta un fallo o si se inicia una conmutación a través de Q_{LE}. Utiliza la instrucción CONMUTACIÓN que no permite apropiar canales C asignados.

El protocolo de protección en la LE, estando en estado NULO (SOLE0) o en estado CONMUTACIÓN SOLICITADA POR AN (SOLE2), al recibir una primitiva MDU-protección (instrucción de conmutación) enviará un mensaje INSTRUCCIÓN DE CONMUTACION, arrancará el temporizador TSO1 y pasará al estado CONMUTACIÓN INICIADA POR LE (SOLE1). El mensaje INSTRUCCIÓN DE CONMUTACIÓN indicará el canal C lógico que debe conmutarse y el canal C de reserva objetivo.

Al recibir la entidad de protocolo de protección AN el mensaje INSTRUCCIÓN DE CONMUTACIÓN, estando en estado NULO (SOAN0), la AN entrará en el estado CONMUTACIÓN INICIADA POR LE (SOAN2) y enviará una primitiva MDU-protección (instrucción de conmutación) a la gestión del sistema de la AN.

Si puede satisfacer la instrucción de conmutación, la gestión del sistema AN iniciará la acción de conmutación en la AN y enviará una primitiva MDU-protección (acuse de conmutación) a la entidad de protocolo de protección AN, que a su vez enviará un mensaje ACUSE DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0).

Al recibir el mensaje ACUSE DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (acuse de conmutación) a la gestión del sistema LE, detendrá el temporizador TSO1 y pasará al estado NULO (SOLE0).

Al recibirse un mensaje PETICIÓN DE CONMUTACIÓN de la AN, estando en estado CONMUTACIÓN INICIADA POR LE (SOLE1), no se producirá ninguna acción y no habrá ningún cambio de estado.

La LE continuará llevando a cabo la conmutación iniciada.

18.6.3.2 Procedimientos excepcionales

Si la gestión del sistema AN no puede satisfacer la instrucción de conmutación, enviará una primitiva MDU-protección (rechazo de conmutación) a la entidad de protocolo de protección AN que, a su vez, enviará un mensaje RECHAZO DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0). El mensaje indicará a la LE la causa por la que no ha sido posible la conmutación.

Al recibir el mensaje RECHAZO DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (indicación de rechazo de conmutación) a la gestión del sistema LE, detendrá el temporizador TSO1 y pasará al estado NULO (SOLE0).

Si la entidad de protocolo de protección AN o LE, recibe una primitiva MDU-protección inesperada no se llevará a cabo ninguna acción y no se producirá ningún cambio de estado.

18.6.3.3 Procedimiento al expirar el temporizador TSO1

Si el temporizador TSO1 expira por primera vez estando la entidad de protocolo de protección LE en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), dicha entidad enviará un mensaje INSTRUCCIÓN DE CONMUTACIÓN a la AN y rearrancará el temporizador TSO1.

Al recibirse un mensaje ACUSE DE CONMUTACIÓN de la AN en estado SOLE0, se enviará a la gestión del sistema una primitiva MDU-protección (acuse de conmutación). Corresponde a la gestión del sistema la responsabilidad de llevar a cabo las acciones adecuadas de acuerdo con la secuencia de los mensajes previamente recibidos (es decir, la gestión del sistema puede activar la conmutación en la LE o puede iniciar un nuevo proceso de conmutación).

Al recibir un mensaje RECHAZO DE CONMUTACIÓN de una AN en estado SOLE0, la entidad de protocolo de protección LE enviará a la gestión del sistema una primitiva MDU-protección (indicación de rechazo de conmutación). Corresponde a la gestión del sistema la responsabilidad de llevar a cabo las acciones adecuadas de acuerdo con la secuencia de los mensajes previamente recibidos y el contenido del elemento de información causa de rechazo (es decir, la gestión del sistema puede iniciar un nuevo proceso de conmutación).

Si el temporizador TSO1 expira por segunda vez estando la entidad de protocolo de protección LE en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), dicha entidad enviará una primitiva MDU-protección (indicación de error de conmutación) a la gestión del sistema y pasará al estado NULO (SOLE0).

En caso de que expire inesperadamente el temporizador TSO1 (es decir, que expire cuando no se encuentre en el estado CONMUTACIÓN INICIADA POR LE), no se llevará a cabo ninguna acción y no se producirá ningún cambio de estado.

18.6.4 Procedimiento de conmutación de protección especial iniciado por OS LE

18.6.4.1 Procedimiento normal

Este procedimiento se utilizará únicamente si la conmutación es iniciada por el operador de la LE a través de Q_{LE}. Si el canal C físico objetivo es un canal C activo, se apropiará. El procedimiento se utiliza fundamentalmente para modificar la asignación de canales C lógicos en caso de múltiples fallos en el enlace de 2048 kbit/s. Ese procedimiento deberá utilizarse únicamente para el grupo 2 de protección.

El protocolo de protección en la LE, estando en estado NULO (SOLE0) o en estado CONMUTACIÓN SOLICITADA POR AN (SOLE2), al recibir una primitiva MDU-protección (instrucción OS-conmutación) emitirá un mensaje INSTRUCCIÓN OS-CONMUTACIÓN, arrancará el temporizador TSO2 y pasará al estado CONMUTACIÓN INICIADA POR LE (SOLE1). El mensaje INSTRUCCIÓN OS-CONMUTACIÓN indicará el canal C lógico que debe conmutarse y el canal C físico objetivo.

Al recibir la entidad del protocolo de protección AN el mensaje INSTRUCCIÓN OS-CONMUTACIÓN estando en estado NULO (SOAN0), la AN pasará al estado CONMUTACIÓN INICIADA POR LE (SOAN2) y enviará una primitiva MDU-protección (instrucción OS-conmutación) a la gestión del sistema de la AN.

Si puede llevar a cabo la instrucción de conmutación, la gestión del sistema AN iniciará la acción de conmutación en la AN y enviará una primitiva MDU-protección (acuse de conmutación) a la entidad de protocolo de protección AN, que a su vez enviará un mensaje ACUSE DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0).

Al recibir el mensaje ACUSE DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (acuse de conmutación) a la gestión del sistema LE, detendrá el temporizador TSO2 y pasará al estado NULO (SOLE0).

Al recibir un mensaje PETICIÓN DE CONMUTACIÓN de la AN, estando en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), no se producirá ninguna acción y no habrá ningún cambio de estado.

La LE continuará llevando a cabo la conmutación iniciada.

18.6.4.2 Procedimientos excepcionales

Si no puede satisfacer la instrucción de conmutación, la gestión del sistema AN enviará una primitiva MDU-protección (rechazo de conmutación) a la entidad de protocolo de protección AN, que a su vez enviará un mensaje RECHAZO DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0). El mensaje indicará a la LE la causa por la que no ha sido posible realizar la conmutación. La instrucción de conmutación no se rechazará debido al hecho de que el canal C físico objetivo ya cursa un canal C lógico; por consiguiente, no se permite como respuesta a un mensaje INSTRUCCIÓN DE OS-CONMUTACIÓN la causa de rechazo «canal C físico objetivo ya tiene un canal C lógico».

Al recibir el mensaje RECHAZO DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (indicación de rechazo de conmutación) a la gestión del sistema, detendrá el temporizador TSO2 y pasará al estado NULO (SOLE0).

Si la entidad de protocolo de protección AN o LE recibe una primitiva MDU-protección inesperada, no se llevará a cabo ninguna acción y no se producirá ningún cambio de estado.

18.6.4.3 Procedimiento al expirar el temporizador TSO2

Si el temporizador TSO2 expira por primera vez estando la entidad de protocolo de protección LE en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), la entidad de protocolo de protección LE enviará un mensaje INSTRUCCIÓN OS-CONMUTACIÓN a la AN y rearrancará el temporizador TSO2.

Si el temporizador TSO2 expira por segunda vez estando la entidad de protocolo de protección LE en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), la entidad de protocolo de protección enviará una primitiva MDU-protección (indicación de error de conmutación) a la gestión del sistema y pasará al estado NULO (SOLE0).

Al recibirse un mensaje ACUSE DE CONMUTACIÓN de la AN en estado SOLE0, se enviará a la gestión del sistema una primitiva MDU-protección (acuse de conmutación). La gestión del sistema tiene la responsabilidad de llevar a cabo las acciones adecuadas de acuerdo con la secuencia de los mensajes previamente recibidos (es decir, la gestión de sistema puede activar la conmutación en la LE o puede iniciar un nuevo proceso de conmutación).

Al recibirse un mensaje RECHAZO DE CONMUTACIÓN de la AN en estado SOLE0, se emitirá una primitiva MDU-protección (indicación de rechazo de conmutación) de la entidad de protocolo de protección LE a la gestión del sistema. Es responsabilidad de la gestión del sistema llevar a cabo las acciones adecuadas de acuerdo con la secuencia de los mensajes previamente recibidos y según el contenido del elemento de información causa de rechazo (es decir, la gestión de sistema puede iniciar un nuevo proceso de conmutación).

En caso de que el temporizador TSO2 expire de forma inesperada (es decir, que expire cuando no se encuentra en el estado CONMUTACIÓN INICIADA POR LE), no se llevará a cabo ninguna acción ni tendrá lugar ningún cambio de estado.

18.6.5 Procedimiento de conmutación de protección solicitado por el lado AN

18.6.5.1 Procedimiento normal

Se utilizará este procedimiento si el lado AN detecta un fallo o si se inicia una conmutación a través de Q_{AN}. La LE puede responder únicamente mediante un mensaje INSTRUCCIÓN DE CONMUTACIÓN (no se permiten apropiaciones) o un mensaje RECHAZO DE CONMUTACIÓN.

El protocolo de protección en la AN, estando en estado NULO (SOAN0), al recibir una primitiva MDU-protección (petición de conmutación) enviará un mensaje PETICIÓN DE CONMUTACIÓN, arrancará el temporizador TSO3 y pasará al estado CONMUTACIÓN SOLICITADA POR AN (SOAN1). Si la conmutación ha sido iniciada por el operador de OS a través de Q_{AN}, el mensaje PETICIÓN DE CONMUTACIÓN indicará el canal C lógico que debe conmutarse y, de forma opcional, el canal C físico objetivo preferido (canal C de reserva). Si la conmutación ha sido activada de manera autónoma por la gestión de sistema AN debido a la detección de un fallo, el mensaje PETICIÓN DE CONMUTACIÓN indicará únicamente el canal C lógico que debe conmutarse y no se otorgará ninguna preferencia a un canal C de reserva en particular.

En los casos en que no hay preferencia, todos los bits del identificador del enlace de 2048 kbit/s y del número del intervalo de tiempo en el elemento de información de canal C físico se codificarán a cero.

Cuando la entidad de protocolo de protección LE reciba el mensaje PETICIÓN DE CONMUTACIÓN, estando en estado NULO (SOLE0), la LE entrará en el estado CONMUTACIÓN SOLICITADA POR AN (SOLE2) y enviará una primitiva MDU-protección (petición de conmutación) a la gestión del sistema de la LE.

Cuando la entidad de protocolo de protección LE reciba el mensaje PETICIÓN DE CONMUTACIÓN, estando en el estado CONMUTACIÓN INICIADA POR LE (SOLE1), la LE ignorará el mensaje y no modificará el estado.

Si puede satisfacer la solicitud de conmutación, la gestión del sistema LE iniciará la acción de conmutación enviando una primitiva MDU-protección (instrucción de conmutación) a la entidad de protocolo de protección LE que, a su vez, enviará un mensaje INSTRUCCIÓN DE CONMUTACIÓN a la AN, entrará en el estado CONMUTACIÓN INICIADA POR LE (SOLE1) y arrancará el temporizador TSO1.

Cuando la entidad de protocolo de protección AN reciba el mensaje INSTRUCCIÓN DE CONMUTACIÓN, estando en el estado CONMUTACIÓN SOLICITADA POR AN (SOAN1), la AN entrará en el estado CONMUTACIÓN INICIADA POR LE (SOAN2), enviará una primitiva MDU-protección (instrucción de conmutación) a la gestión de sistema de la AN y parará el temporizador TSO3.

Cuando la entidad de protocolo de protección AN reciba el mensaje INSTRUCCIÓN OS-CONMUTACIÓN, estando en el estado CONMUTACIÓN SOLICITADA POR AN (SOAN1), la AN pasará al estado CONMUTACIÓN INICIADA POR LE (SOAN2), enviará una primitiva MDU-protección (instrucción OS-conmutación) a la gestión del sistema de la AN y parará el temporizador TSO3.

Si puede satisfacer la instrucción de conmutación, la gestión del sistema AN iniciará la acción de conmutación en la AN y enviará una primitiva MDU-protección (acuse de conmutación) a la entidad de protocolo de protección AN que, a continuación, enviará un mensaje ACUSE DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0).

Al recibir el mensaje ACUSE DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (acuse de conmutación) a la gestión del sistema LE, parará el temporizador TSO1 y pasará al estado NULO (SOLE0).

A continuación, la LE realizará la conmutación. Si por cualquier razón la LE no puede llevar a cabo la conmutación, la gestión del sistema LE tiene la responsabilidad de iniciar una nueva acción de conmutación.

18.6.5.2 Procedimiento excepcional, la AN no puede llevar a cabo la instrucción de conmutación de la LE

Si no puede satisfacer la instrucción de conmutación, la gestión del sistema AN enviará una primitiva MDU-protección (rechazo de conmutación) a la entidad de protocolo de protección AN que, a continuación, enviará un mensaje RECHAZO DE CONMUTACIÓN a la LE y pasará al estado NULO (SOAN0). El mensaje indicará a la LE la razón por la que no ha sido posible la conmutación.

Al recibir el mensaje RECHAZO DE CONMUTACIÓN de la AN, la entidad de protocolo de protección LE enviará una primitiva MDU-protección (indicación de rechazo de conmutación) a la gestión del sistema LE, detendrá el temporizador TSO1 y pasará al estado NULO (SOLE0).

Si la entidad de protocolo de protección AN o LE recibe una primitiva MDU-protección inesperada, no se llevará a cabo ninguna acción ni se producirá ningún cambio de estado.

18.6.5.3 Procedimiento excepcional, la LE no puede satisfacer la solicitud de conmutación de la AN

La gestión del sistema LE, estando en el estado CONMUTACIÓN SOLICITADA POR AN (SOLE2), si no puede realizar la instrucción de conmutación, enviará una primitiva MDU-protección (rechazo de conmutación) a la entidad de protocolo de protección LE, que a su vez enviará un mensaje RECHAZO DE CONMUTACIÓN a la AN y pasará al estado NULO (SOLE0). El mensaje indicará a la AN la causa por la que no ha sido posible la conmutación.

Al recibir el mensaje RECHAZO DE CONMUTACIÓN de la LE, estando en estado CONMUTACIÓN SOLICITADA POR AN, la entidad de protocolo de protección AN enviará una primitiva MDU-protección (indicación de rechazo de conmutación) a la gestión del sistema AN, parará el temporizador TSO3 y pasará al estado NULO (SOAN0).

Si la entidad de protocolo de protección AN o LE reciben una primitiva MDU-protección inesperada, no se llevará a cabo ninguna acción y no se producirá ningún cambio de estado.

18.6.5.4 Procedimiento al expirar el temporizador TSO3

Si el temporizador TSO3 expira por primera vez estando la entidad de protocolo de protección AN en el estado CONMUTACIÓN SOLICITADA POR AN (SOAN1), la entidad de protocolo de protección AN enviará un mensaje PETICIÓN DE CONMUTACIÓN a la LE y rearrancará el temporizador TSO3.

Si el temporizador TSO3 expira por segunda vez estando la entidad de protocolo de protección AN en el estado CONMUTACIÓN SOLICITADA POR AN (SOAN1), la entidad de protocolo de protección AN enviará una primitiva MDU-protección (indicación de error de conmutación) a la gestión del sistema y pasará al estado NULO (SOAN0).

Si el temporizador TSO3 expira de forma inesperada (es decir, expira cuando no se encuentra en el estado CONMUTACIÓN SOLICITADA POR AN), no se llevará a cabo ninguna acción ni se producirá ningún cambio de estado.

18.6.6 Tratamiento de las condiciones de error

Antes de actuar ante un mensaje, la entidad receptora, ya sea la entidad de protocolo de protección AN V5.2 o la entidad de protocolo de protección LE V.5, llevará a cabo los procedimientos especificados en este punto.

Por regla general, todos los mensajes, salvo los mensajes INSTRUCCIÓN DE REPOSICIÓN DE SN y ACUSE DE REPOSICIÓN DE SN, contendrán al menos los elementos de información discriminador de protocolo, identificación de canal C lógico y tipo de mensaje. Al recibir un mensaje con menos de 4 octetos, la entidad de protocolo de protección de recepción en la AN o en la LE generará una primitiva MDU-protección (indicación de error de protocolo) a la gestión del sistema e ignorará el mensaje.

Un mensaje recibido se verificará como se indica en 18.6.6.1 a 18.6.6.7 en orden de precedencia. Durante estas verificaciones no tendrá lugar ningún cambio de estado.

Si en un mensaje se detectan más de dos elementos de información opcionales, el mensaje se considerará demasiado largo y se truncará tras el segundo elemento de información opcional. Toda información truncada se considera elementos de información opcionales repetidos. Al efectuar el truncamiento, la entidad actuará de acuerdo con 18.6.6.3 para los elementos de información opcional repetidos.

Si se detecta un error de protocolo en la AN mientras se encuentra activo el temporizador TSO4, no se enviará al lado LE ningún mensaje ERROR DE PROTOCOLO.

Tras verificar el mensaje utilizando los siguientes procedimientos de tratamiento de error, si el mensaje no ha de ignorarse, deberán aplicarse los procedimientos del protocolo de protección especificados en 18.6.2 a 18.6.5.

NOTA – En esta subcláusula, «ignorar el mensaje» significa que no se modifica el contenido del mensaje.

18.6.6.1 Error de discriminador de protocolo

Cuando una entidad de protocolo de protección de capa 3 reciba un mensaje con un discriminador de protocolo codificado de forma distinta a lo especificado en 13.2.1 para su utilización en los protocolos V.5:

- la entidad de protocolo de protección AN generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «error de discriminador de protocolo»;

- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión e ignorará el mensaje.

18.6.6.2 Error de tipo de mensaje

Cuando se reciba un tipo de mensaje no reconocido:

- la entidad de protocolo de protección AN generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «tipo de mensaje no reconocido», incluyendo el correspondiente diagnóstico como se indica en 18.5.5;

- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión e ignorará el mensaje.

18.6.6.3 Elementos de información repetidos

Cuando en un mensaje se repita un elemento de información obligatorio, la reacción de la entidad receptora será la siguiente:

- la entidad de protocolo de protección AN generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «elemento de información obligatorio repetido», incluyendo el correspondiente diagnóstico tal como se especifica en 18.5.5;
- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión e ignorará el mensaje.

18.6.6.4 Elemento de información obligatorio faltante

Al recibir un mensaje con un elemento de información obligatorio faltante, la reacción de la entidad receptora será la siguiente:

- la entidad de protocolo de protección AN generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «elemento de información obligatorio faltante», incluyendo el correspondiente diagnóstico tal como se especifica en 18.5.5;
- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión e ignorará el mensaje.

Si falta más de un elemento de información obligatorio, la reacción de la entidad receptora deberá basarse en el primer elemento de información obligatorio que se identifique como faltante.

18.6.6.5 Elemento de información no reconocido

Cuando se reciba un mensaje con uno o más elementos de información no reconocidos, la reacción de la entidad receptora será la siguiente:

- la entidad de protocolo de protección AN generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, suprimirá todos los elementos de información no reconocidos y continuará el tratamiento del mensaje; enviará igualmente un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «elemento de información no reconocido», incluyendo el correspondiente diagnóstico tal como se especifica en 18.5.5;
- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, suprimirá todos los elementos de información no reconocidos y continuará el procesamiento del mensaje.

Si aparece más de un elemento de información no reconocido, la reacción de la entidad receptora deberá basarse en el primer elemento de información no reconocido que se identifique.

A efectos de los procedimientos de tratamiento de error de protocolo de protección, los elementos de información no reconocidos son aquéllos no definidos en 13.2 y 18.5.

18.6.6.6 Error de contenido de elemento de información obligatorio

Cuando se reciba un mensaje con un elemento de información obligatorio que tiene un error de contenido tal que:

a) la longitud no es conforme a lo especificado en 13.2 y 18.5; o

b) el contenido no es conocido, entonces:

- la entidad de protocolo de protección AN generará un primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión, ignorará el mensaje y enviará un mensaje ERROR DE PROTOCOLO indicando como causa de error de protocolo «error de contenido de elemento de información obligatorio», incluyendo el correspondiente diagnóstico tal como se especifica en 18.5.5;
- la entidad de protocolo de protección LE generará una primitiva MDU-protección (indicación de error de protocolo) al sistema de gestión e ignorará el mensaje.

A efectos de los procedimientos de tratamiento de error, los errores de contenido de elemento de información son puntos de código incluidos en un elemento de información particular no definidos en 13.2 y 18.5.

18.6.6.7 Mensaje no esperado

Cuando se recibe un mensaje inesperado se produce un error de flujo de mensajes. Los mensajes inesperados son aquéllos explícitamente calificados como mensajes inesperados (/) en los cuadros transición de estado de las entidades de protocolo de protección V.5.2 del lado LE y AN (véanse Cuadro 65 y Cuadro 66). Los cuadros de transición de estado indican las acciones apropiadas al recibir cualquier suceso.

Cuando se recibe un mensaje inesperado no se produce ningún cambio de estado. Además:

- la entidad de protocolo de protección enviará una primitiva MDU-protección (indicación de error de protocolo) a la gestión del sistema, ignorará el mensaje y enviará un mensaje de ERROR DE PROTOCOLO indicando como causa de error de protocolo «mensaje no compatible con el estado del protocolo de protección», incluyendo el correspondiente diagnóstico tal como se especifica en 18.5.5;
- la entidad de protocolo de protección LE enviará una primitiva MDU-protección (indicación de error de protocolo) a la gestión del sistema e ignorará el mensaje.

18.7 Lista de parámetros del sistema

En el Cuadro 64 figura la definición de los temporizadores utilizados en el protocolo de protección. Los temporizadores mencionados se mantienen en las entidades de protocolo de protección LE o AN. La tolerancia de los temporizadores será de ± 10%.

CUADRO 64/G.965

Temporizadores del protocolo de protección

Nombre del temporizador	Valor de temporización	Causa de arranque	Parada normal	A la primera expiración	A la segunda expiración	Referencia
TSO1	1500 ms	INSTRUCCIÓN DE CONMUTA-CIÓN enviada, se pasa al estado SOLE1	Recepción de ACUSE DE CONMUTACIÓN	Retransmisiones de INSTRUCCIÓN DE CONMUTACIÓN	Indicación de error a la gestión del sistema	18.6
TSO2	1500 ms	INSTRUCCIÓN DE OS-CONMU-TACIÓN enviada, se pasa al estado SOLE1	Recepción de ACUSE DE CONMUTACIÓN	Rretransmisiones de INSTRUCCIÓN DE OS-CONMUTACIÓN	Indicación de error a la gestión del sistema	18.6
TSO3	1500 ms	PETICIÓN DE CONMUTACIÓN enviada, se pasa al estado SOAN1	Recepción de INSTRUCCIÓN DE CONMUTACIÓN	Retransmisiones de PETICIÓN DE CONMUTACIÓN	Indicación de error a la gestión del sistema	18.6
TSO4	20 s	INSTRUCCIÓN DE REPOSICIÓN DE SN enviada, se pasa al estado NULO	Recepción de ACUSE DE REPOSICIÓN DE SN	Retransmisión de INSTRUCCIÓN DE REPOSICIÓN DE SN	Indicación de error a la gestión del sistema	18.6
TSO5	10 s	Recepción de INSTRUCCIÓN DE REPOSICIÓN DE SN, se pasa al estado NULO	TSO5 expirará siempre	No hay acción, no hay cambio de estado	No es aplicable	18.6

18.8 Cuadros de estado de lado AN y LE

18.8.1 FSM del protocolo de protección en la AN

En el Cuadro 65 aparecen las transiciones de estado para la FSM del protocolo de protección en la AN.

CUADRO 65/G.965

FSM del protocolo de protección AN

Estado	SOAN0	SOAN1	SOAN2
Nombre del estado Evento	NULO	CONMUTACIÓN SOLICITADA POR AN	CONMUTACIÓN SOLICITADA POR LE
MDU-protección (acuse de conmutación)	/	/	ACUSE DE CONMUTACIÓN; SOAN0
MDU-protección (petición de conmutación) (Nota 1)	PETICIÓN DE CONMUTACIÓN; arrancar TSO3; SOAN1	/	/
	MDU-protección (indicación de error en reposición de SN); –		
MDU-protección (rechazo de conmutación)	/	/	RECHAZO DE CONMUTACIÓN; SOAN0
INSTRUCCIÓN DE CONMUTACIÓN (Nota 1)	MDU-protección (instrucción de conmutación); SOAN2	MDU-protección (instrucción de conmutación); parar TSO3; SOAN2	/
	–		
INSTRUCCIÓN DE OS-CONMUTACIÓN (Nota 1)	MDU-protección (instrucción de OS conmutación); SOAN2	MDU-protección (instrucción de OS conmutación); parar TS03; SOAN2	/
	–		
RECHAZO DE CONMUTACIÓN (Nota 1)	/	MDU-protección (indicación de rechazo de conmutación); parar TS03; SOAN0	/
	–		
Expiración del temporizador TSO3 (primera)	/	PETICIÓN DE CONMUTACIÓN; arrancar TSO3; –	/
Expiración del temporizador TSO3 (segunda)	/	MDU-protección (indicación de error de conmutación); SOAN0	/
VP(S), VP(R) desajuste detectado	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; –	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; parar TSO3; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; SOAN0	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; SOAN0
INSTRUCCIÓN DE REPOSICIÓN DE SN (Nota 2)	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; MDU-protección (indicación de reposición de SN); –	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; parar TSO3; MDU-protección (indicación de reposición de SN); SOAN0	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; MDU-protección (indicación de reposición de SN); SOAN0
	–	–	–
ACUSE DE REPOSICIÓN DE SN (Nota 1)	–	–	–
	Parar TSO4; MDU-protección (acuse de reposición de SN); –		
Expiración del temporizador TSO4 (primera)	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; –	/	/

CUADRO 65/G.965 *(fin)*

FSM del protocolo de protección AN

Estado	SOAN0	SOAN1	SOAN2
Nombre del estado Evento	NULO	CONMUTACIÓN SOLICITADA POR AN	CONMUTACIÓN SOLICITADA POR LE
Expiración del temporizador TSO4 (segunda)	MDU-protección (indicación de error de reposición de SN); –	/	/
Expiración del temporizador TSO5	–	–	–
Detección de error de protocolo (Nota 1)	MDU-protección (indicación de error de protocolo); ERROR DE PROTOCOLO; –	MDU-protección (indicación de error de protocolo); ERROR DE PROTOCOLO; –	MDU-protección (indicación de error de protocolo); ERROR DE PROTOCOLO; –
	MDU-protección (indicación de error de protocolo); –		
– No hay cambio de estado, no hay acción; / Evento inesperado, no hay cambio de estado, no hay acción. NOTAS 1 Deberá elegirse la opción de abajo si el temporizador TSO4 está activo. 2 Deberá elegirse la opción de abajo si el temporizador TSO5 está activo.			

18.8.2 FSM del protocolo de protección en la LE

En el Cuadro 66 aparecen las transiciones de estado para la FSM del protocolo de protección en la LE.

CUADRO 66/G.965

FSM del protocolo de protección LE

Estado	SOLE0	SOLE1	SOLE2
Nombre del estado Evento	NULO	CONMUTACIÓN INICIADA POR LE	CONMUTACIÓN SOLICITADA POR AN
MDU-protección (instrucción de conmutación) (Nota 1)	INSTRUCCIÓN DE CONMUTACIÓN; arrancar TSO1; SOLE1	/	INSTRUCCIÓN DE CONMUTACIÓN; arrancar TSO1; SOLE1
	MDU-protección (indicación de error en reposición de SN); –		
MDU-protección (instrucción de OS conmutación) (Nota 1)	PETICIÓN DE OS-CONMUTACIÓN; arrancar TSO2; SOLE1	/	PETICIÓN DE OS-CONMUTACIÓN; arrancar TSO2; SOLE1
	–		
MDU-protección (rechazo de conmutación)	/	/	RECHAZO DE CONMUTACIÓN; SOLE0
ACUSE DE CONMUTACIÓN (Nota 1)	MDU-protección (acuse de conmutación); –	MDU-protección (acuse de conmutación); parar TSO1; parar TSO2; SOLE0	/
	–		
PETICIÓN DE CONMUTACIÓN (Nota 1)	MDU-protección (petición de conmutación); SOLE2	–	/
	–		

CUADRO 66/G.965 *(fin)*

FSM del protocolo de protección LE

Estado	SOLE0	SOLE1	SOLE2
Nombre del estado Evento	NULO	CONMUTACIÓN INICIADA POR LE	CONMUTACIÓN SOLICITADA POR AN
RECHAZO DE CONMUTACIÓN (Nota 1)	MDU-protección (indicación de rechazo de conmutación); –	MDU-protección (indicación de rechazo de conmutación); parar TSO1; parar TSO2; SOLE0	/
	–		
Expiración del temporizador TSO1 (primera)	/	INSTRUCCIÓN DE CONMUTACIÓN; arrancar TSO1; –	/
Expiración del temporizador TSO1 (segunda)	/	MDU-protección (indicación de error de conmutación); SOLE0	/
Expiración del temporizador TSO2 (primera)	/	INSTRUCCIÓN DE OS-CONMUTACIÓN; arrancar TSO2; –	/
Expiración del temporizador TSO2 (segunda)	/	MDU-protección (indicación de error de conmutación); SOLE0	/
3VP(S), VP(R) detectado desajuste o MDU-protección (petición de reposición de SN)	INSTRUCCIÓN DE REPOSICIÓN DE SN; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; –	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; parar TSO1; parar TSO2; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; SOLE0	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; MDU-protección (instrucción de reposición de SN); poner VP(S)=VP(R)=0; SOLE0
INSTRUCCIÓN DE REPOSICIÓN DE SN (Nota 2)	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; MDU-protección (indicación de reposición de SN); –	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; parar TSO1; parar TSO2; MDU-protección (indicación de reposición de SN); SOLE0	ACUSE DE REPOSICIÓN DE SN; poner VP(S) = VP(R) = 0; arrancar TSO5; MDU-protección (indicación de reposición de SN); SOLE0
	–	–	–
ACUSE DE REPOSICIÓN DE SN (Nota 1)	–	–	–
	Parar TSO4; MDU-protección (acuse de reposición de SN); –		
Expiración del temporizador TSO4 (primera)	INSTRUCCIÓN DE REPOSICIÓN DE SN; arrancar TSO4; MDU-protección (instrucción de reposición de SN); poner VP(S) = VP(R) = 0; –	/	/
Expiración del temporizador TSO4 (segunda)	MDU-protección (indicación de error en reposición de SN); –	/	/
Expiración del temporizador TSO5	–	–	–
ERROR DE PROTOCOLO (Causa) (Nota 1)	MDU-protección (indicación de error de protocolo); –	MDU-protección (indicación de error de protocolo); –	MDU-protección (indicación de error de protocolo); –
	–		

– No hay cambio de estado, no hay acción; / Evento inesperado, no hay cambio de estado, no hay acción.

NOTAS

1 Deberá elegirse la opción de abajo si el temporizador TSO4 está activo.

2 Deberá elegirse la opción de abajo si el temporizador TSO5 está activo.

Anexo A

Casos de servicio, arquitectura y definición funcional de las configuraciones de acceso con una red de acceso en la central local

(Este anexo es parte integrante de esta Recomendación)

A.1 Conclusiones sobre las aplicaciones de múltiples interfaces V5

El contenido de esta subcláusula es idéntico al de A.1/G.964 [8].

A.2 Conclusiones sobre aspectos arquitectónicos

Toda interfaz V5.2 puede tener un mínimo de 1 enlace de 2048 kbit/s físico y un máximo de 16.

El número y combinación de interfaces V5.1 y V5.2 entre cualquier AN y LE es ilimitado.

Las funciones de capa 1 de ET para el servicio acceso básico RDSI, definidas en la Recomendación G.960 [4], se reparten entre la AN y la LE (véase la Figura 3 de la presente Recomendación).

Las funciones de capa 1 de ET para el servicio de acceso a velocidad primaria RDSI, definidas en la Recomendación G.962 [10], son controladas por la AN.

La conmutación de canales adicionales entre la AN y la LE, por ejemplo mediante una transconexión separada, está autorizada pero sin que repercuta en la funcionalidad de la interfaz V5.2 especificada en esta Recomendación. La conexión en cascada de las AN (es decir, conectándolas con una interfaz de «tipo V5») no tiene repercusión en las funciones de la interfaz V5.2.

El objeto de la interfaz V5 no se limita exclusivamente a las AN y debe ser independiente de su arquitectura. La transconexión o transconexiones entre una AN y la LE se observa desde la interfaz V5 como parte integrante de la AN.

Es posible la coexistencia de interfaces V5.1, V5.2 y V3.

A.3 Implementación de la Q_{AN}

El contenido de esta subcláusula es idéntico al de A.3/G.964 [8].

A.4 Requisitos para el soporte de la capacidad PL a través de un acceso básico a la RDSI

El contenido de esta subcláusula es idéntico al de A.4/G.964 [8].

A.5 Requisitos para el soporte de la capacidad PL a través de un acceso de velocidad primaria a la RDSI

Las líneas permanentes rodean la LE y caen fuera del ámbito de la especificación de la interfaz V5.2. Como el puerto del acceso a velocidad primaria RDSI está permanentemente activo, no es necesaria una FSM en la LE para soportar la función.

Para que el protocolo BCC funcione correctamente, deberá controlarse a través de dos gestores de recursos; uno en la LE y otro en la AN. La presente Recomendación supone que estos gestores de recursos existen, pero no pretende limitar su funcionalidad.

Para que los gestores de recursos funcionen correctamente, el gestor de recursos en la LE deberá ser informado de las peticiones efectuadas en los intervalos de tiempo del puerto de usuario que controla. Esta información deberá introducirse en el sistema a través de Q_{LE}.

A.6 Hipótesis y requisitos para el soporte de líneas arrendadas semipermanentes

A.6.1 Consideraciones generales

Las líneas arrendadas semipermanentes pasan a través de la interfaz V5.2.

Para la interfaz V5.2, donde la conexión para todos los canales portadores es establecida entre el puerto de usuario de la AN y la LE por la BCC, no se necesita un procedimiento adicional entre la LE y la AN para el soporte de las líneas arrendadas semipermanentes. Dichas líneas se aprovisionan mediante Q_{LE}.

El aprovisionamiento del puerto de usuario de acuerdo con los requisitos del usuario es responsabilidad de la AN y, por consiguiente, cae fuera del ámbito de la especificación de la interfaz V5.2.

A.6.2 Señalización asociada a líneas arrendadas semipermanentes

El contenido de esta subcláusula es idéntico al de A.5.2/G.964 [8].

A.6.3 Puertos de usuario

El contenido de esta subcláusula es idéntico al de A.5.3/G.964 [8].

A.6.4 Requisitos de los puertos de usuario en redes distintas de la RDSI para líneas arrendadas semipermanentes

El contenido de esta subcláusula es idéntico al de A.5.4/G.964 [8].

Anexo B

Utilización de los elementos de información de protocolo para protocolos RTPC nacionales

(Este anexo es parte integrante de esta Recomendación)

El contenido de este anexo es idéntico al del Anexo B/G.964 [8].

Anexo C

Requisitos básicos de las funciones de gestión del sistema de la AN y la LE

(Este anexo es parte integrante de esta Recomendación)

C.1 Procedimiento para la prueba de continuidad de acceso básico a la RDSI

La Recomendación G.960 [4] define un procedimiento de prueba de continuidad para la verificación del estado del acceso básico a la RDSI, por ejemplo, un cierto tiempo sin actividad. El procedimiento se basa en los requisitos definidos en la Recomendación I.603. La prueba utiliza los elementos del procedimiento de activación y ha de ser iniciada por la LE con el conocimiento de la actividad del servicio y de la prestación del servicio. Si la prueba fracasa, el mecanismo para verificar la situación es la localización de fallos bajo la responsabilidad de la AN.

A fin de soportar la división de funciones de control entre la LE y la AN para el acceso básico a la RDSI, la AN activará la función temporizador T1 especificada en 14.1/G.964 [8]. El temporizador T1 no es necesario en la LE. La información sobre una activación infructuosa, que es de interés para la identificación de la causa apropiada a enviar para rechazar una llamada entrante, puede tomarse del recibo de FE106 cuando se está en el estado LE2.1.

El temporizador T1 se define en la Recomendación UIT-T I.430 [3].

MPH-T1 puede utilizarse en la AN para iniciar las pruebas de verificación necesarias que requiere el bloqueo del puerto de usuario. La AN no sabe si el intento de activación desde la LE fue iniciado para la entrega de una llamada entrante o para la prueba de continuidad. La LE considera el puerto operacional aun después de una activación infructuosa, y corresponderá a la AN clarificar el estado del puerto.

C.2 La gestión AN no enviará MPH-BR cuando el puerto está en uno de los estados no operacionales.

La gestión LE puede responder con MPH-BI en un plazo de tiempo apropiado según las condiciones de servicio de este puerto de usuario. Véase también 7.1.1, apartado 3). En el caso de conexiones semipermanentes, la gestión LE emitirá MPH-UBI.

Si la gestión por la AN ha enviado erróneamente una petición de bloqueo a la LE, la gestión AN puede cancelar la petición de bloqueo emitiendo MPH-UBR. La gestión LE puede entonces recibir PMH-UBI y cancelar la petición de bloqueo (es decir, ignorar la petición anteriormente recibida) si el puerto aún no ha sido bloqueado. En este último caso, la LE puede iniciar el procedimiento de desbloqueo emitiendo MPH-UBR.

C.3 La colisión entre primitivas enviadas desde la FSM a la gestión y viceversa al mismo tiempo se resuelven en la correspondiente FSM.

C.4 MPH-BI sólo se emitirá por la gestión AN en caso de fallo grave o característica de error inaceptable en enlaces internos de la AN utilizados y que afecten significativamente a la prestación del servicio en el puerto de usuario. No se acusará recibo de MPH-BI, lo que conduce directamente a la terminación de las llamadas en curso o en fase de establecimiento. Se necesita que la AN compruebe si la situación persiste durante más tiempo que los efectos intermitentes típicos.

C.5 El desbloqueo de un puerto requiere acuse de recibo por el otro lado para establecer transición coordinada al estado operacional. Si la reacción desde el lado distante en MPH-UBR es MPH-BI, debe interpretarse solamente como una indicación de que el otro lado no está de acuerdo en ese momento en pasar al estado operacional y la FSM ha vuelto al estado totalmente bloqueado. La falta de respuesta a MPH-UBR se interpretará como que el otro lado no está de acuerdo en pasar al estado operacional ese instante, pero puede reaccionar posteriormente. La FSM permanece en el estado desbloqueo local.

C.6 Se hace referencia a 7.1.1, apartados 2), 4), 6), 8) y 9).

C.7 Se hace referencia a 15.3.3.4 y a la Recomendación G.964 [8] (14.1.3.4 y 14.2.3.4) para el mecanismo de verificación AN y a 15.3.3.5 y a la Recomendación G.964 [8] (14.1.3.5 y 14.2.3.5) para el mecanismo de verificación LE utilizando MPH-UBR.

C.8 Se hace referencia a 15.3.3.3.6 y a la Nota 1 al Cuadro 38/G.964 [8] relativa a la activación permanente del acceso a la RDSI.

C.9 La comunicación de una FSM o una entidad de protocolo de capa 2 se produce solamente hacia la gestión del sistema. Como no existe comunicación directa entre las diferentes FSM o la entidad de protocolo de capa 2 de la AN o la LE, la gestión del sistema coordinará las FSM o la entidad de protocolo de capa 2 mediante el uso de las primitivas apropiadas teniendo en cuenta tanto la información recibida de diversos bloques funcionales en la AN o en la LE sobre el estado y los fallos.

C.10 La característica de error en la sección digital de acceso por debajo de cierto nivel mínimo en un periodo de tiempo se considerará inaceptable desde cualquier punto de vista de servicio. La gestión AN bloqueará el puerto de usuario correspondiente si se ha detectado esta condición.

C.11 Verificación del provisionamiento

El procedimiento para la verificación del provisionamiento utiliza los mensajes definidos en 14.5/G.964 [8] y los elementos del protocolo, codificación y procedimientos definidos en 14.3/G.964 [8] y 14.4/G.964 [8].

Antes del reprovisionamiento, se sugiere que el mecanismo de verificación se utilice para verificar que está disponible la nueva variante de provisionamiento en la AN y en la LE. Para hacerlo, el lado que desee efectuar el reprovisionamiento emite el mensaje «VERIFICAR REPROVISIONAMIENTO» y recibe:

- PREPARADO PARA REPROVISIONAMIENTO, o bien
- NO PREPARADO PARA REPROVISIONAMIENTO.

En este último caso, corresponderá a la gestión efectuar cualquier función necesaria.

C.12 Sincronización del reprovisionamiento

El procedimiento para la sincronización del provisionamiento se aplicará solamente en el momento de reprovisionamiento acordado. El procedimiento utiliza los mensajes definidos en 14.3/G.964 [8] y 14.5/G.964 [8].

Reprovisionamiento iniciado desde la gestión LE

El procedimiento se muestra en la Figura C.1.

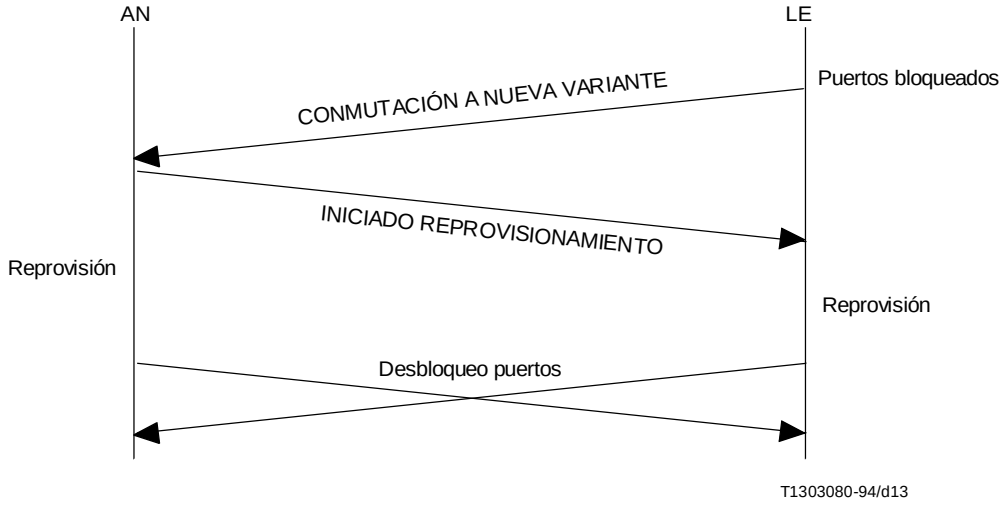


FIGURA C.1/G.965
Procedimiento de reprovisionamiento iniciado desde la LE

La LE bloquea todos los puertos pertinentes. La LE emite el mensaje «CONMUTAR A NUEVA VARIANTE» y recibe:

- INICIADO REPROVISIONAMIENTO, o bien
- NO PUEDE REPROVISIONAR indicando la causa.

En el primer caso, la AN comienza el reprovisionamiento cuando se envía el valor «INICIADO REPROVISIONAMIENTO» dentro del elemento de información ID función de control, y la LE comienza el reprovisionamiento al recibir el valor «INICIADO REPROVISIONAMIENTO» con el elemento de información ID función de control, y ambos extremos inician el desbloqueo de los puertos cuando están preparados utilizando el mecanismo de desbloqueo definido. En el último caso, la LE informa solamente a su gestión y puede desbloquear los puertos.

La AN y la LE pueden demorar el comienzo del reprovisionamiento para asegurar la entrega a la AN del mensaje INICIADO REPROVISIONAMIENTO. En el último caso, corresponderá a la gestión efectuar cualquier acción necesaria.

Reprovisionamiento iniciado por la gestión AN

El procedimiento se muestra en la Figura C.2.

La AN envía el mensaje CONMUTAR A NUEVA VARIANTE. Si la LE puede soportar reprovisionamiento, comienza el bloqueo de los puertos pertinentes y responde con INICIADO BLOQUEO. El procedimiento es entonces el mismo que para el reprovisionamiento iniciado por la LE. Si no hay puertos que bloquear o ya están bloqueados, la LE puede proceder inmediatamente con CONMUTAR A NUEVA VARIANTE.

Si la LE no puede reprovisionar, responde al mensaje CONMUTAR A NUEVA VARIANTE con el mensaje NO PUEDE REPROVISIONAR. En este caso no se efectuará ninguna otra acción en la LE.

Verificación del reprovisionamiento

Puede ser necesario solicitar el ID de variante e interfaz antes de comenzar a desbloquear los puertos. Este procedimiento evita que haya puertos en funcionamiento, pero con una desadaptación de variante o interfaz después del reprovisionamiento.

Procedimiento de repliegue

Puede resultar posible «deshacer» el reprovisionamiento utilizando el mecanismo de sincronización de reprovisionamiento si el enlace de protocolo de control está aún activo. En este caso, la variante utilizada calificaría un conjunto de datos correspondiente al antiguo conjunto de datos.

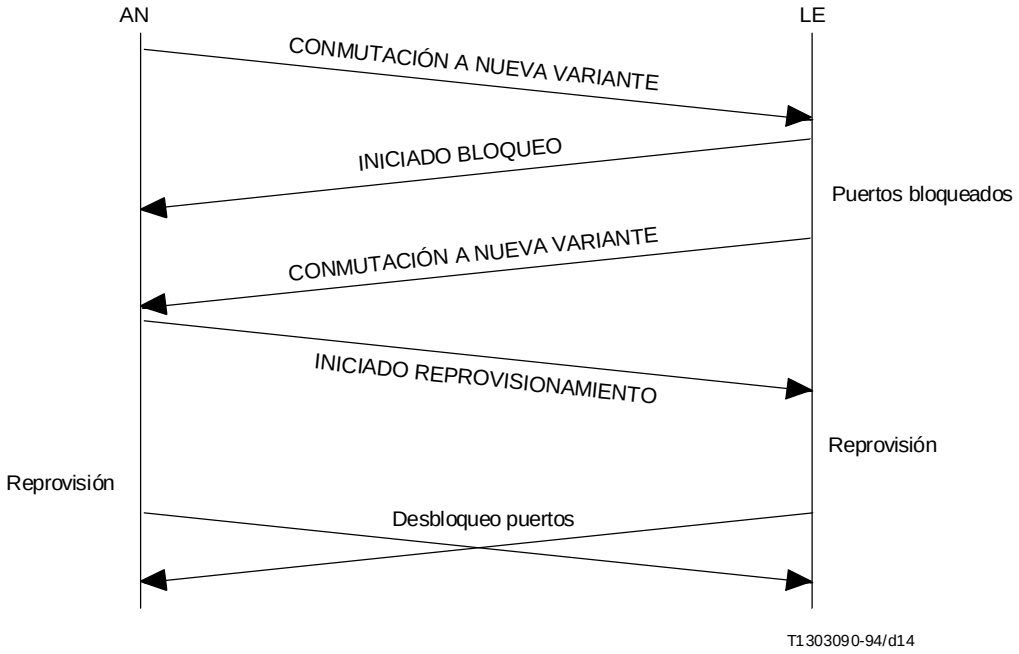


FIGURA C.2/G.965

Procedimiento para reprovisionamiento iniciado desde la AN

C.13 Arranque del sistema

Dentro del procedimiento de arranque del sistema, se comprobará la variante&id después de establecer el enlace de datos para los diversos protocolos: enlace de protección en el enlace primario y secundario (si existen), protocolo de control, protocolo de control del enlace, protocolo BCC y protocolo RTPC (si existe). Si la variante&id corresponde a la propia variante&id, el procedimiento de identificación de enlace puede iniciarse para el enlace primario y secundario y el enlace que transporta el protocolo RTPC (si se proporciona). Tras completar con éxito el procedimiento de identificación del enlace para los enlaces que cursan los protocolos BCC, de control y de RTPC, se invocará el procedimiento de rearranque de RTPC. A continuación puede completarse la identificación del enlace de cualquier otro enlace. Si el trayecto C que transporta la señalización RTPC no está provisionado, no se establecerá el enlace de datos RTPC. En el arranque del sistema, la gestión de sistema o el OS puede decidir no aplicar el procedimiento de identificación del enlace.

C.14 Procedimiento de rearranque

El procedimiento de rearranque será invocado por la gestión de sistema o el OS. El rearranque será invocado después del fallo RTPC-V5DL descrito en C.17 o por arranque del sistema descrito en C.13 del presente anexo. Sólo se define un procedimiento de rearranque específico para el protocolo RTPC. Para el protocolo de control, la gestión del sistema utilizará el procedimiento de bloqueo de puerto, si es necesario. Para el protocolo de control del enlace, la gestión del sistema utilizará un procedimiento de bloqueo del enlace, si es necesario:

a) dentro del procedimiento de arranque del sistema, o si se genera de forma interna una petición de rearranque, se enviará una MDU-CTRL (petición de rearranque) a la entidad de protocolo de control y a todas las máquinas de estado del protocolo RTPC y se arrancarán los temporizadores TR1 y TR2.

   Al recibir la MDU-CTRL (rearranque completo) de la entidad de protocolo de control, se detendrá el temporizador TR2; al recibir la indicación MDU-CTRL (acuse de rearranque) de las entidades de

protocolo RTPC, se detendrá el temporizador TR1. Una vez recibida la indicación MDU-CTRL (rearranque completo) del protocolo de control y la indicación MDU-CTRL (acuse de rearranque) de todas las entidades de protocolo RTPC, se enviará una MDU-CTRL (rearranque completo) a todas las entidades de protocolo RTPC.

Tras expirar el temporizador TR1 o TR2, se dará a la entidad de mantenimiento una notificación de rearranque infructuoso y se detendrá el proceso. Un proceso de integridad del sistema asegurará que la gestión del sistema se ponga repetidamente en el estado ARRANQUE DEL SISTEMA (por ejemplo, cada cinco minutos).

b) Si se recibe una MDU-CTRL (petición de rearranque) de la entidad de protocolo de control, se enviará una indicación MDU-CTRL (petición de rearranque) a todas las máquinas de estado de protocolo RTPC y se arrancará el temporizador TR1.

Tras recibir las indicaciones MDU-CTRL (acuse de rearranque) de todas las máquinas de estado de protocolo RTPC, se detendrá el temporizador TR1 y se enviará una indicación MDU-CTRL (rearranque completo) a la entidad de protocolo de control y a todas las máquinas de estado de protocolo RTPC.

Al expirar el temporizador TR1 se enviará una indicación de error a la entidad de mantenimiento.

C.15 Procedimiento de activación del enlace de datos

La gestión del sistema solicitará durante el procedimiento de arranque del sistema la activación de CONTROL_DL, LINK_CONTROL_DL, BCC_DL, y, si se provisiona el trayecto C para el protocolo RTPC, RTPC_DL (y si se provisiona el enlace secundario, el PROTECTION_DLS 1 y 2) por envío de una petición MDL-ESTABLECIMIENTO a ambos enlaces de datos.

Cuando se recibe de CONTROL_DL o de LINK_CONTROL DL una confirmación MDL-ESTABLECIMIENTO o una indicación MDL-ESTABLECIMIENTO, se enviará una MDU-iniciar_tráfico a todas las entidades de protocolo pertinentes.

El arranque del sistema ha tenido éxito si los enlaces de datos para estos protocolos indican la activación mediante confirmación MDL-ESTABLECIMIENTO o indicación MDL-ESTABLECIMIENTO.

C.16 Reiniciación de enlace de datos

Si se recibe del CONTROL_DL una indicación MDL-ESTABLECIMIENTO después de la inicialización del sistema o en el estado ARRANQUE DEL SISTEMA, la gestión del sistema enviará una MDU-iniciar_tráfico a todas las entidades de protocolo de control, solicitará la variante&id y esperará las indicaciones MDU_CTRL (acuse de arranque).

Toda indicación MDL_LIBERACIÓN inesperada (es decir no forzada por la entidad de gestión debido, por ejemplo, a una conmutación de protección) de una entidad de capa 2 (PSTN_DL, CONTROL_DL, LINK_CONTROL_DL, BCC_DL, PROTECT_DL_1 o PROTECT_DL 2) puede ser utilizada por la gestión del sistema para verificar la ID de interfaz y/o la ID de enlace de los enlaces correspondientes.

C.17 Fallo del enlace de datos

Si la gestión del sistema AN o LE recibe una primitiva indicación MDL-LIBERACIÓN de LAPV5-DL para el protocolo de control, de enlace de control, de BCC o de RTPC, el canal C físico que transporte dicho trayecto C se considerará no operativo. En consecuencia, la gestión del sistema activará una conmutación de protección del citado canal C lógico y se enviará una indicación de error a la entidad de mantenimiento.

Una vez realizada la conmutación en la AN o la LE, respectivamente, la gestión del sistema enviará primitivas petición-MDL-ESTABLECIMIENTO a todas las LAPV5-DL afectadas. Tras una conmutación, la gestión del sistema intentará continuamente establecer enlaces de datos con fallo aun cuando se envíe otra primitiva indicación MDL-LIBERACIÓN del enlace de datos a la gestión del sistema. No se llevará a cabo ninguna otra conmutación como resultado de dicha primitiva indicación MDL-LIBERACIÓN, puesto que presumiblemente se ha producido un fallo interno que no es posible subsanar mediante conmutación. Ello significa que la FSM del enlace de datos del trayecto C con fallo pasará en primer lugar al estado MÚLTIPLE TRAMA ESTABLECIDA (al menos una vez) antes de llevar a cabo una segunda conmutación, activada por la recepción de la primitiva indicación MDL-LIBERACIÓN.

Una vez realizada la conmutación y tras enviar la primera primitiva petición MDL-ESTABLECIMIENTO a la LAPV5-DL para el protocolo de control, se arrancará el temporizador TC1.

Una vez realizada la conmutación y tras enviar la primera primitiva petición MDL-ESTABLECIMIENTO a la LAPV5-DL para el protocolo RTPC, se arrancará el temporizador TC3.

Una vez realizada la conmutación y tras enviar la primera primitiva petición MDL-ESTABLECIMIENTO a la LAPV5-DL para el protocolo de control del enlace, se arrancará el temporizador TC4.

Una vez realizada la conmutación y tras enviar la primera primitiva petición MDL-ESTABLECIMIENTO a la LAPV5-DL para el protocolo BCC, se arrancará el temporizador TC6.

Si no se recibe de la RTPC_DL una confirmación MDL-ESTABLECIMIENTO o una indicación MDL-ESTABLE-CIMIENTO en el plazo de 15 segundos (temporizador TC3), se invocará el bloqueo de todos los puertos RTPC enviando una MDU-CTRL (puerto bloqueado) a todas las máquinas de estado de protocolo RTPC. Se enviará una MDU-CTRL (puerto no bloqueado) a las máquinas de estado de protocolo RTPC correspondientes tras el restablecimiento de la RTPC_DL.

Si no se recibe de CONTROL_DL una confirmación MDL-ESTABLECIMIENTO o una indicación MDL-ESTABLE-CIMIENTO en el plazo de 15 segundos (temporizador TC1), se enviará una MDU-detener_tráfico a todas las entidades de protocolo de control, se invocará el bloqueo de los puertos RDSI por la gestión del sistema correspondiente y se arrancará el temporizador TC2 (1 minuto). Al expirar el temporizador TC2, se invocará el procedimiento de arranque del sistema.

Si no se recibe de LINK_CONTROL_DL una confirmación MDL-ESTABLECIMIENTO o una indicación MDL-ESTABLECIMIENTO en el plazo de 15 segundos (temporizador TC4), se enviará una MDU-parar_tráfico a las entidades de control del enlace (pero no hay bloqueo de los enlaces) y se arrancará el temporizador TC5 (1 minuto). Al expirar el temporizador TC5, se invocará el procedimiento de arranque del sistema.

Si no se recibe de BCC-DL una primitiva confirmación MDL-ESTABLECIMIENTO o indicación MDL-ESTABLE-CIMIENTO en el plazo de 15 segundos (temporizador TC6), corresponde a la gestión del sistema la responsabilidad de llevar a cabo las acciones adecuadas para subsanar esa situación de fallo.

Un fallo del enlace de datos de sólo PROTECT_DL_1 o de PROTECT_DL_2 se indicará únicamente a la entidad de gestión. Los fallos del enlace de datos de ambos PROTECT_DL_1 y PROTECT_DL_2 bloquearán el mecanismo de protección.

C.18 Error del mecanismo de protección de capa 3 del protocolo de control

Al producirse «indicación de error» procedente del mecanismo de protección de capa 3 para el protocolo de control, las FSM de puerto de usuario correspondiente en la AN y la LE pueden estar incorrectamente alineadas. Pueden necesitarse las siguientes acciones de gestión:

- despejar la cola de mensajes para este puerto;
- verificar el estado (operativo) vigente enviando «desbloquear»;
- si no se aclara, imponer realineación mediante la secuencia «bloquear/desbloquear».

C.19 Temporizadores en la entidad de gestión del sistema

En el Cuadro C.1 se especifican los temporizadores en la gestión del sistema de la AN y la LE. Todos los temporizadores definidos en dicho cuadro tendrán una tolerancia mejor de ±5%.

C.20 Puede resultar necesaria una identificación del enlace tras una recuperación de fallo de capa 1 del enlace indicada por MPH-AI de la FSM del enlace de capa 1 e indicada a la gestión del sistema mediante MDU-LAI. La gestión del sistema debe invocar el procedimiento de identificación del enlace. Puede haber otros activadores en la gestión del sistema para solicitar este procedimiento. Habrá únicamente una petición para el procedimiento de identificación del enlace de la gestión del sistema en un instante para todas las interfaces V5 de AN o LE.

C.21 Es responsabilidad de la gestión del sistema llevar a cabo las acciones adecuadas al recibir cualquier información procedente de la FSM de control del enlace; por ejemplo MDU-IDRej, MDU-AI, MDU-Elg, como resultado de un procedimiento de identificación del enlace solicitado por la gestión del sistema a la FSM de control del enlace.

C.22 No es necesario bloquear los enlaces de 2048 kbit/s antes del reaprovisionamiento. Una vez completado dicho reaprovisionamiento, estos enlaces pueden pasar al estado operativo y puede no necesitarse el desbloqueo de enlace.

CUADRO C.1/G.965

Temporizadores de la entidad de gestión del sistema

Temporizador N.°	Temporización	Causa del arranque	Parada normal
TR1	100 segundos	MDU-CTRL (petición de rearranque) a todas las máquinas de estados de protocolo RTPC	MDU-CTRL (acuse de rearranque) procedente de todas las máquinas de estados de protocolo RTPC
TR2	2 minutos	MDU-CTRL (petición de rearranque) a CONTROL-DL	MDU-CTRL (rearranque completo) procedente de CONTROL-DL
TC1	15 segundos	Pedido establecimiento CONTROL-DL	Recepción de confirmación MDL-ESTABLECIMIENTO o indicación MDL-ESTABLECIMIENTO procedente de CONTROL-DL
TC2	1 minuto	Pedido establecimiento CONTROL-DL	Recepción de confirmación MDL-ESTABLECIMIENTO o indicación MDL-ESTABLECIMIENTO procedente de CONTROL-DL
TC3	15 segundos	Pedido establecimiento RTPC-DL	Recepción de confirmación MDL-ESTABLECIMIENTO o indicación MDL-ESTABLECIMIENTO procedente de RTPC-DL
TC4	15 segundos	Pedido establecimiento LINK_CONTROL_DL	Recepción de confirmación MDL_ESTABLECIMIENTO o indicación MDL_ESTABLECIMIENTO procedente de LINK_CONTROL_DL
TC5	1 minuto	Pedido establecimiento LINK_CONTROL_DL	Recepción de indicación MDL_ESTABLECIMIENTO procedente de LINK_CONTROL_DL
TC6	15 segundos	Pedido establecimiento BCC_DL	Recepción de confirmación MDL_ESTABLECIMIENTO o indicación MDL_ESTABLECIMIENTO procedente de BCC_DL

C.23 En una interfaz V5.2 con un solo enlace, no se implantará el protocolo de protección. La gestión del sistema no invocará el establecimiento del enlace de datos de protección e ignorará una indicación MDL-LIBERACIÓN procedente de un enlace de datos de protección, caso de aparecer.

C.24 En el caso de la conmutación de protección de los trayectos C para RTPC, control de puerto y control común, control de enlace o BCC, la gestión del sistema LE solicitará el restablecimiento del enlace o enlaces de datos pertinentes emitiendo una petición MDL-ESTABLECIMIENTO.

C.25 Durante la inicialización de V5.2, es decir durante el reaprovisionamiento o después del mismo, todos los datos para el protocolo de protección, de BCC, de control del enlace y de control común se repondrán a sus valores por defecto. Ello no es necesario en la parte de control de puerto puesto que todos los puertos estarán bloqueados antes de iniciar el reaprovisionamiento y deberán desbloquearse posteriormente de forma individual. Para el protocolo RTPC se aplicará el procedimiento de restablecimiento definido en la Recomendación G.964 [8].

C.26 Tratamiento de los rechazos de asignación BCC por la gestión del sistema

La gestión del sistema registrará la información proporcionada por el gestor de recursos BCC que puede recopilarse mediante el sistema de operaciones para identificar el nivel de calidad de funcionamiento. Frecuentes rechazos de asignaciones pueden provocar igualmente una indicación autónoma al sistema de operación para llamar la atención del suministrador del servicio sobre la situación. A ese nivel elevado pueden llevarse a cabo, entonces, otras acciones.

C.27 Error de mecanismo de protección de capa 3 del protocolo de control del enlace

Al producirse «indicación de error» procedente del mecanismo de protección de capa 3 para el protocolo de control del enlace, las FSM de control del enlace correspondiente en la AN y la LE pueden estar incorrectamente alineadas. Puede que sea necesario, entonces, llevar a cabo las siguientes acciones de gestión:

- despejar la cola de mensajes para el protocolo de control del enlace;
- verificar el estado (operativo) vigente enviando «desbloquear»;
- para los enlaces en que no pueda aclararse el estado, imponer la realineación mediante las secuencias bloquear/desbloquear normales.

Anexo D

Arquitectura de protocolo para el control de puerto de usuario RTPC y RDSI (de acceso básico y de acceso a velocidad primaria)

(Este anexo es parte integrante de esta Recomendación)

D.1 Alcance

Este anexo describe la arquitectura de protocolo para la transferencia de información de control de estado de puerto de usuario AB-RDSI y AVP-RDSI y de puerto de usuario RTPC.

D.2 Control de estado de puerto de usuario AB-RDSI

El contenido de esta subcláusula es idéntico al de D.2/G.964 [8].

D.3 Control de estado de puerto de usuario AVP-RDSI

D.3.1 División funcional entre LE y AN

Para los accesos a velocidad primaria RDSI que no están directamente conectados a la LE sino a los que se accede a distancia a través de una AN, la funcionalidad de capa 1 de la ET se divide entre la LE y la AN.

En principio, la LE sólo será informada sobre la disponibilidad de capa 1 del puerto de usuario (operativo/no operativo).

Como el mantenimiento de la sección digital de acceso y las líneas de abonado es responsabilidad de la AN, el funcionamiento de los bucles u otras pruebas de la sección digital será únicamente controlado por la AN. Por consiguiente, no se transmitirá a la LE ninguna información relativa a estas funciones (FE-A-FE-Y). La identificación correcta del estado del puerto es responsabilidad de la FSM del puerto AN que indicará este estado a la LE.

D.3.2 Transferencia de información entre LE y AN

La Figura D.1 muestra el modelo de arquitectura de protocolo para las funciones de control de puerto de usuario de acceso a velocidad primaria RDSI.

Para la transferencia de información bidireccional entre las dos FSM de puerto de usuario, AN (acceso a velocidad primaria RDSI) y LE (acceso a velocidad primaria RDSI), se utilizan elementos de función (FE20x). Se transportan por un protocolo de control de capa 3. Este protocolo incluye un procedimiento de acuse de recibo para la protección contra la pérdida de tramas individuales.

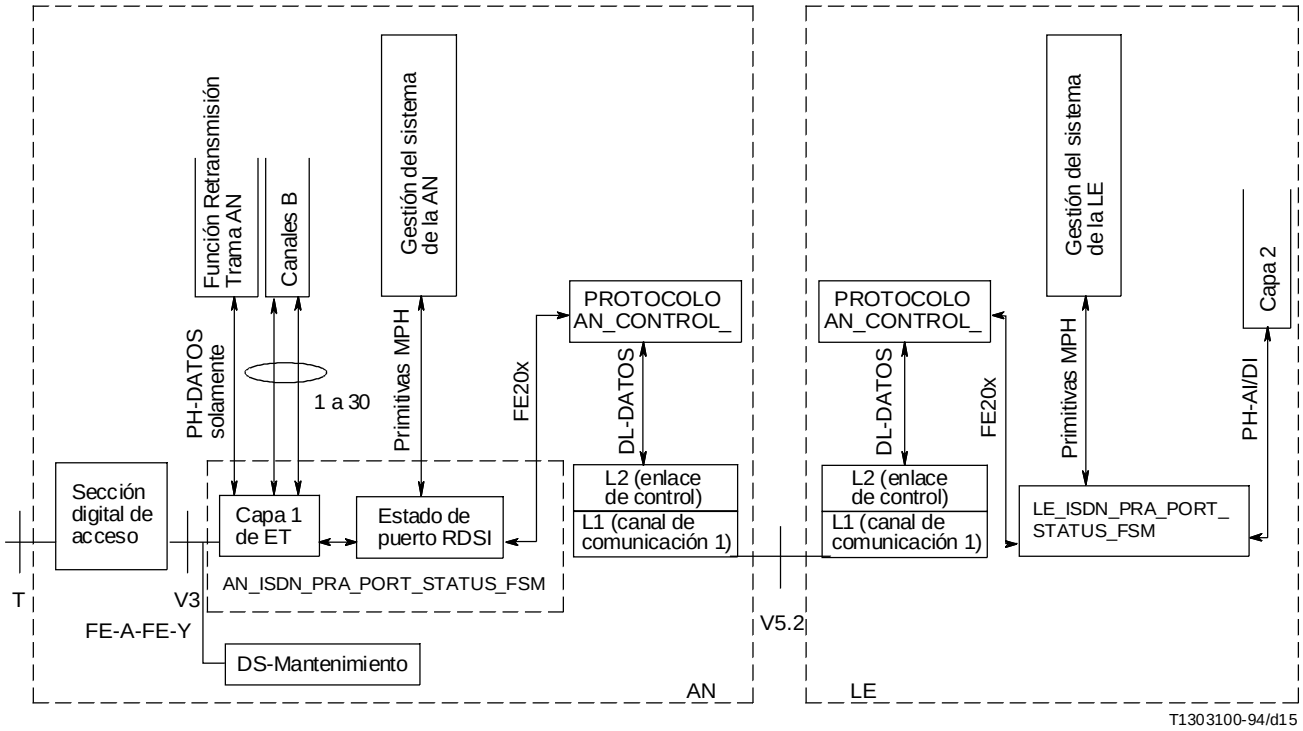


FIGURA D.1/G.965

Arquitectura de protocolo para las funciones de control de puerto de acceso a velocidad primaria RDSI

D.3.3 Activación/desactivación

Como los accesos a velocidad primaria RDSI están permanentemente activados, no existe ningún procedimiento de activación/desactivación; es decir, los elementos de función relativos a la activación/desactivación (FE10x) no se utilizan en la interfaz V5.2 para los puertos de usuario de velocidad primaria RDSI.

La capa 2 en la LE y la gestión del sistema LE son informadas únicamente sobre el estado operativo en el puerto de usuario de acceso a velocidad primaria RDSI por las primitivas PH-AI/DI y MPH-AI/DI, respectivamente.

D.4 Control de puerto de usuario RTPC

El contenido de esta subcláusula es idéntico al de D.3/G.964 [8].

Anexo E

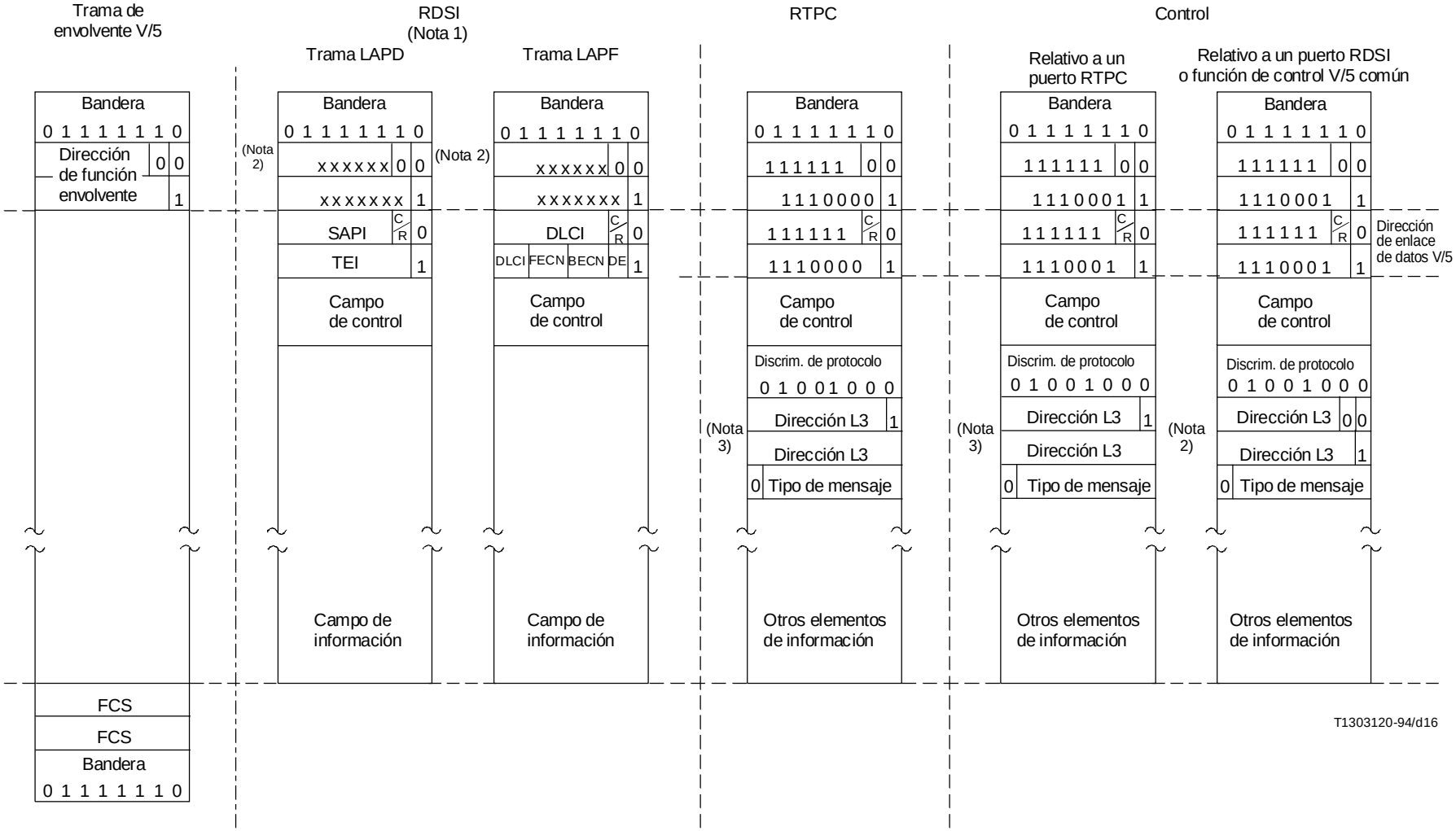
Estructuras de trama, puntos de código de mensaje y esquema de direccionamiento para V5.2

(Este anexo es parte integrante de esta Recomendación)

En las Figuras E.1 y E.2 se indican las posibles estructuras de tramas incorporadas en los diversos protocolos y canales de comunicación.

El Cuadro E.1 muestra los tipos de mensajes asignados a la interfaz V5.2.

El Cuadro E.2 muestra los elementos de información asignados a la interfaz V5.2.



NOTAS

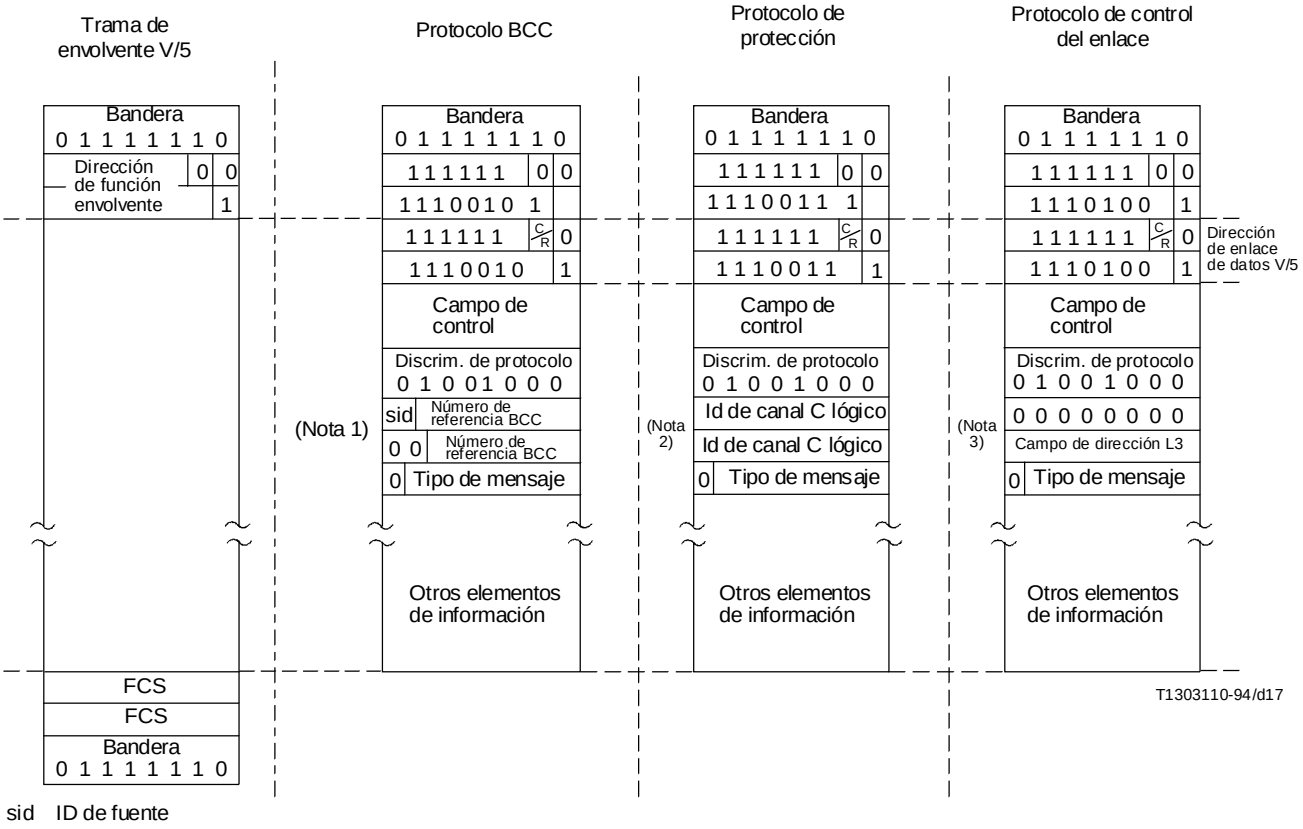
1 En el caso de la RDSI, los campos de control y de información de las tramas de capa 2 RDSI no se cambian en la interfaz V5.5.

2 Para un determinado puerto RDSI, estos campos de dirección tienen el mismo valor.

3 Para un determinado puerto RTPC, estos campos de dirección tienen el mismo valor.

FIGURA E.1/G.965

Formatos de trama utilizados en la interfaz V5.2



NOTAS

1 El número de referencia BCC identifica un proceso de protocolo BCC individual.
2 El id de canal C lógico identifica un canal de comunicaciones lógico individual.
3 El campo de dirección L3 identifica un enlace de capa 1 individual.

FIGURA E.2/G.965

Formatos de trama adicionales utilizados en la interfaz V5.2

CUADRO E.1/G.965

Puntos de código de mensaje utilizados en la interfaz V5.2

Bits							Tipos de mensaje
7	6	5	4	3	2	1	
0	0	0	–	–	–	–	Tipos de mensaje de protocolo RTPC
0	0	0	0	0	0	0	ESTABLECIMIENTO
0	0	0	0	0	0	1	ACUSE DE ESTABLECIMIENTO
0	0	0	0	0	1	0	SEÑAL
0	0	0	0	0	1	1	ACUSE DE SEÑAL
0	0	0	1	0	0	0	DESCONEXIÓN
0	0	0	1	0	0	1	DESCONEXIÓN COMPLETA
0	0	0	1	1	0	0	PETICIÓN DE ESTADO
0	0	0	1	1	0	1	ESTADO
0	0	0	1	1	1	0	PARÁMETRO DE PROTOCOLO
0	0	1	0	–	–	–	Tipos de mensaje de protocolo de control
0	0	1	0	0	0	0	CONTROL DE PUERTO
0	0	1	0	0	0	1	ACUSE DE CONTROL DE PUERTO
0	0	1	0	0	1	0	CONTROL COMÚN
0	0	1	0	0	1	1	ACUSE DE CONTROL COMÚN
0	0	1	1	–	–	–	Tipos de mensaje de protocolo de protección
0	0	1	1	0	0	0	PETICIÓN DE CONMUTACIÓN
0	0	1	1	0	0	1	INSTRUCCIÓN DE CONMUTACIÓN
0	0	1	1	0	1	0	ACUSE DE CONMUTACIÓN
0	0	1	1	0	1	1	RECHAZO DE CONMUTACIÓN
0	0	1	1	1	0	0	INSTRUCCIÓN OS CONMUTACIÓN
0	1	0	–	–	–	–	Tipos de mensaje de protocolo BCC
0	1	0	0	0	0	0	ASIGNACIÓN
0	1	0	0	0	0	1	ASIGNACIÓN COMPLETA
0	1	0	0	0	1	0	RECHAZO DE ASIGNACIÓN
0	1	0	0	0	1	1	DESASIGNACIÓN
0	1	0	0	1	0	0	DESASIGNACIÓN COMPLETA
0	1	0	0	1	0	1	RECHAZO DE DESASIGNACIÓN
0	1	0	0	1	1	0	VERIFICACIÓN
0	1	0	0	1	1	1	VERIFICACIÓN COMPLETA
0	1	0	1	0	0	0	AVERÍA EN AN
0	1	0	1	0	0	1	ACUSE DE AVERÍA EN AN
0	1	0	1	0	1	0	ERROR DE PROTOCOLO
0	1	1	0	–	–	–	Tipos de mensaje de protocolo de control del enlace
0	1	1	0	0	0	0	CONTROL DEL ENLACE
0	1	1	0	0	0	1	ACUSE DE CONTROL DEL ENLACE
NOTA – Todos los demás valores se reservan.							

CUADRO E.2/G.965

Elementos de información asignados a la inferfaz V4.2

Bits								Protocolo	Elemento de información	Referencia
8	7	6	5	4	3	2	1			
0	–	–	–	–	–	–	–		ELEMENTOS DE INFORMACIÓN DE LONGITUD VARIABLE	
0	0	0	0	0	0	0	0	RTPC	Número de secuencia	14
0	0	0	0	0	0	0	1	RTPC	Tono de llamada cadenciado	14
0	0	0	0	0	0	1	0	RTPC	Señal de impulsos	14
0	0	0	0	0	0	1	1	RTPC	Señal estable	14
0	0	0	0	0	1	0	0	RTPC	Señal de cifras	14
0	0	0	1	0	0	0	0	RTPC	Tiempo de reconocimiento	14
0	0	0	1	0	0	0	1	RTPC	Acuse de habilitación autónomo	14
0	0	0	1	0	0	1	0	RTPC	Acuse de inhabilitación autónomo	14
0	0	0	1	0	0	1	1	RTPC	Causa	14
0	0	0	1	0	1	0	0	RTPC	Recurso indisponible	14
0	0	1	0	0	0	0	0	Control	Elemento de función control	15.4
0	0	1	0	0	0	0	1	Control	Identificación de función de control	15.4
0	0	1	0	0	0	1	0	Control	Variante	15.4
0	0	1	0	0	0	1	1	Control	Identificación de interfaz	15.4
0	0	1	1	0	0	0	0	Control del enlace	Función de control del enlace	16.3.2.2
0	1	0	0	0	0	0	0	BCC	Identificación de puerto de usuario	17.4.2.1
0	1	0	0	0	0	0	1	BCC	Identificación de canal de puerto RDSI	17.4.2.2
0	1	0	0	0	0	1	0	BCC	Identificación de intervalo de tiempo V5	17.4.2.3
0	1	0	0	0	0	1	1	BCC	Mapa multiintervalos	17.4.2.4
0	1	0	0	0	1	0	0	BCC	Causa de rechazo	17.4.2.5
0	1	0	0	0	1	0	1	BCC	Causa de error de protocolo	17.4.2.6
0	1	0	0	0	1	1	0	BCC	Conexión incompleta	17.4.2.7
0	1	0	1	0	0	0	0	Protección	Número de secuencia	18.5.2
0	1	0	1	0	0	0	1	Protección	Identificación de canal C físico	18.5.3
0	1	0	1	0	0	1	0	Protección	Causa de rechazo	18.5.4
0	1	0	1	0	0	1	1	Protección	Causa de error de protocolo	18.5.5
1	–	–	–	–	–	–	–		ELEMENTOS DE INFORMACIÓN DE UN SOLO OCTETO	
1	0	0	0	X	X	X	X	RTPC	Información de línea	14
1	0	0	1	X	X	X	X	RTPC	Estado	14
1	0	1	0	X	X	X	X	RTPC	Secuencia de señalización autónoma	14
1	0	1	1	X	X	X	X	RTPC	Respuesta de secuencia	14
1	1	0	0	0	0	0	0	RTPC	Fin de impulso	14
1	1	1	0	X	X	X	X	Control	Grado de calidad de servicio	15.4
1	1	1	1	X	X	X	X	Control	Causa de rechazo	15.4

NOTA – Todos los demás valores se reservan.

Anexo F

Concepto y requisitos para elevar una interfaz V5.1 a la categoría de interfaz V5.2

(Este anexo es parte integrante de esta Recomendación)

El contenido del presente anexo es idéntico al del Anexo F de la Recomendación G.964 [8].

Anexo G

Requisitos de la AN para la marcación por impulsos

(Este anexo es parte integrante de esta Recomendación)

El contenido de este anexo es idéntico al del Anexo H de la Recomendación G.964 [8].

Anexo H

Procedimientos de detección de error de capa 3

(Este anexo es parte integrante de esta Recomendación)

El contenido de este anexo es idéntico al del Anexo K de la Recomendación G.964 [8].

Anexo J

Protocolo de protección; notas explicativas y flujo de información

(Este anexo es parte integrante de esta Recomendación)

J.1 Información adicional sobre los principios del protocolo de protección

La AN puede únicamente solicitar una conmutación, pero la instrucción de conmutación (mensaje INSTRUCCIÓN DE CONMUTACIÓN o INSTRUCCIÓN DE OS-CONMUTACIÓN) procederá siempre del lado LE. Al recibir la instrucción de conmutación, la gestión del sistema AN verificará únicamente si hay o no recursos disponibles para efectuar con éxito la conmutación. El resultado se notificará a la LE mediante un mensaje ACUSE DE CONMUTACIÓN o un mensaje RECHAZO DE CONMUTACIÓN. La AN no puede verificar si la conmutación tendrá éxito. Si por alguna razón se identifican posteriormente problemas relacionados con el procedimiento de conmutación, la AN puede indicar esta circunstancia a la LE emitiendo una nueva petición a dicha LE.

Antes del envío de una instrucción CONMUTACIÓN de la LE a la AN, la gestión del sistema/gestor de recursos LE verificará si, en principio, es posible la conmutación. Si por alguna razón se identifican posteriormente problemas relacionados con el procedimiento de conmutación, la LE puede iniciar una nueva conmutación enviando una nueva instrucción CONMUTACIÓN a la AN.

Si se pierde un mensaje ACUSE DE CONMUTACIÓN, enviado desde el lado AN, el temporizador TSO1 o el temporizador TSO2 expirarán y el lado LE retransmitirá el mensaje INSTRUCCIÓN DE CONMUTACIÓN o INSTRUCCIÓN DE OS-CONMUTACIÓN. Como ya se ha llevado a cabo la conmutación en la AN, ésta responderá con un mensaje RECHAZO DE CONMUTACIÓN indicando como causa «la asignación solicitada ya existe». La gestión del sistema LE considerará este mensaje como un acuse de recibo de la conmutación en la AN y, en consecuencia, realizará una conmutación en la LE.

Los procesos de conmutación no se llevarán a cabo de manera simultánea. Por consiguiente, si se envía una instrucción de conmutación de la LE a la AN, el lado LE debe esperar una respuesta antes de enviar una nueva instrucción CONMUTACIÓN, aun cuando durante ese intervalo el lado LE identifique problemas relativos a la instrucción CONMUTACIÓN anterior.

Si se detecta un fallo casi simultáneamente, tanto el lado LE como el lado AN pueden solicitar un procedimiento de conmutación al mismo tiempo. En este caso la controversia se resuelve en la LE puesto que dicha LE controla la conmutación de protección (véase la Figura J.7).

J.2 Flujo de información

En las Figuras J.1 a J.7 aparecen algunos ejemplos del flujo de información del protocolo de protección.

En la Figura J.1 aparece la activación de conmutación iniciada por la LE de manera autónoma al detectar un fallo o por intervención del operador.

En la Figura J.2 se muestra la activación de conmutación iniciada por la AN de manera autónoma al detectar un fallo o por intervención de operador.

En la Figura J.3 se representa el rechazo por la AN de una conmutación iniciada por la LE.

En la Figura J.4 se muestra el rechazo por la LE de una conmutación iniciada por la AN.

En la Figura J.5 aparece una conmutación iniciada por la LE con retransmisiones debidas a pérdidas de un mensaje.

En la Figura J.6 aparece una conmutación iniciada por la LE con retransmisiones debidas a pérdidas de mensaje.

En la Figura J.7 se muestra una conmutación iniciada de manera simultánea por el lado LE y por el lado AN.

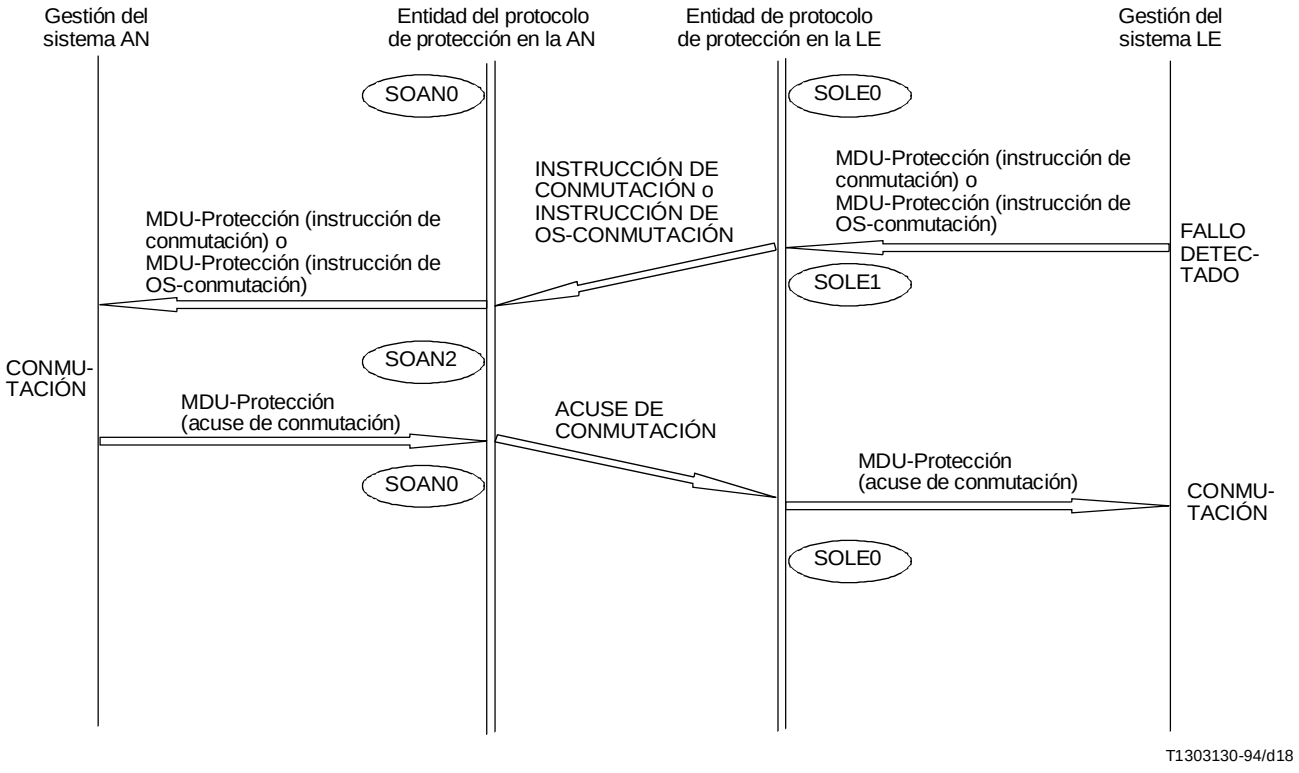


FIGURA J.1/G.965

Conmutación autónoma iniciada por la LE entre canales C físicos

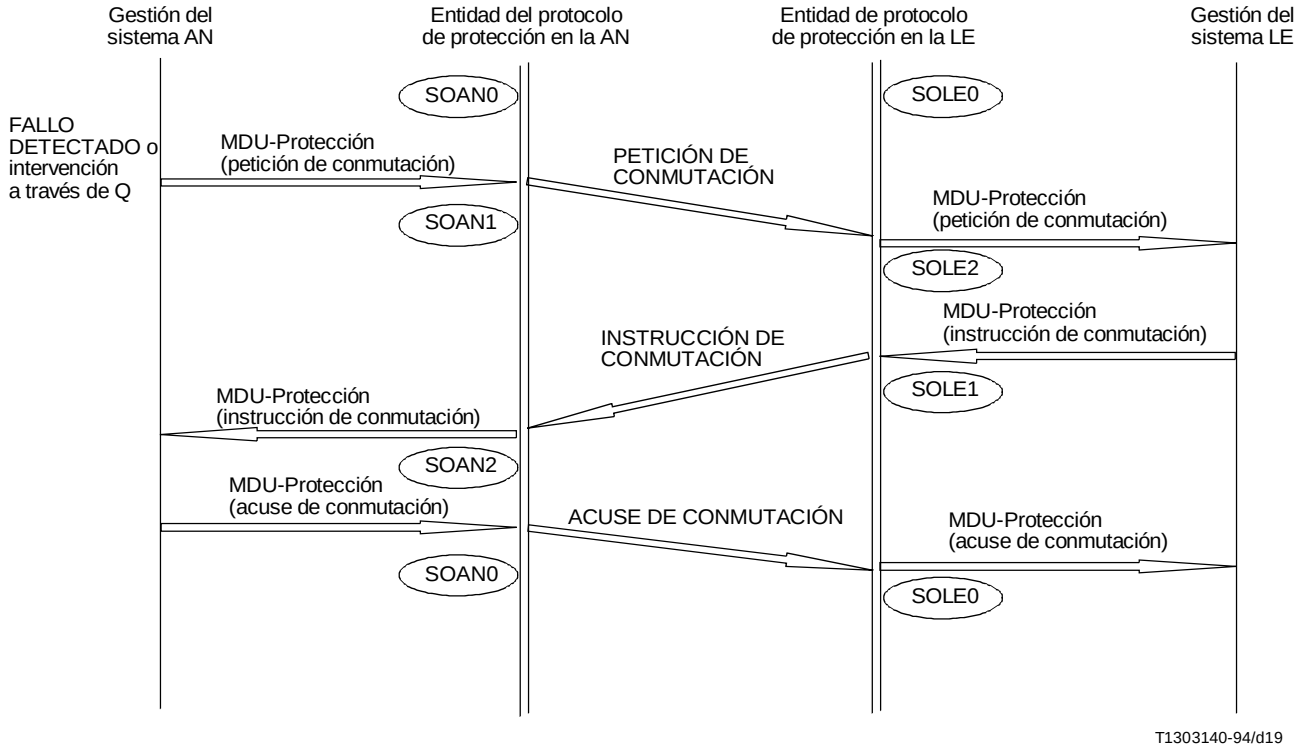


FIGURA J.2/G.965

Conmutación autónoma iniciada por la AN

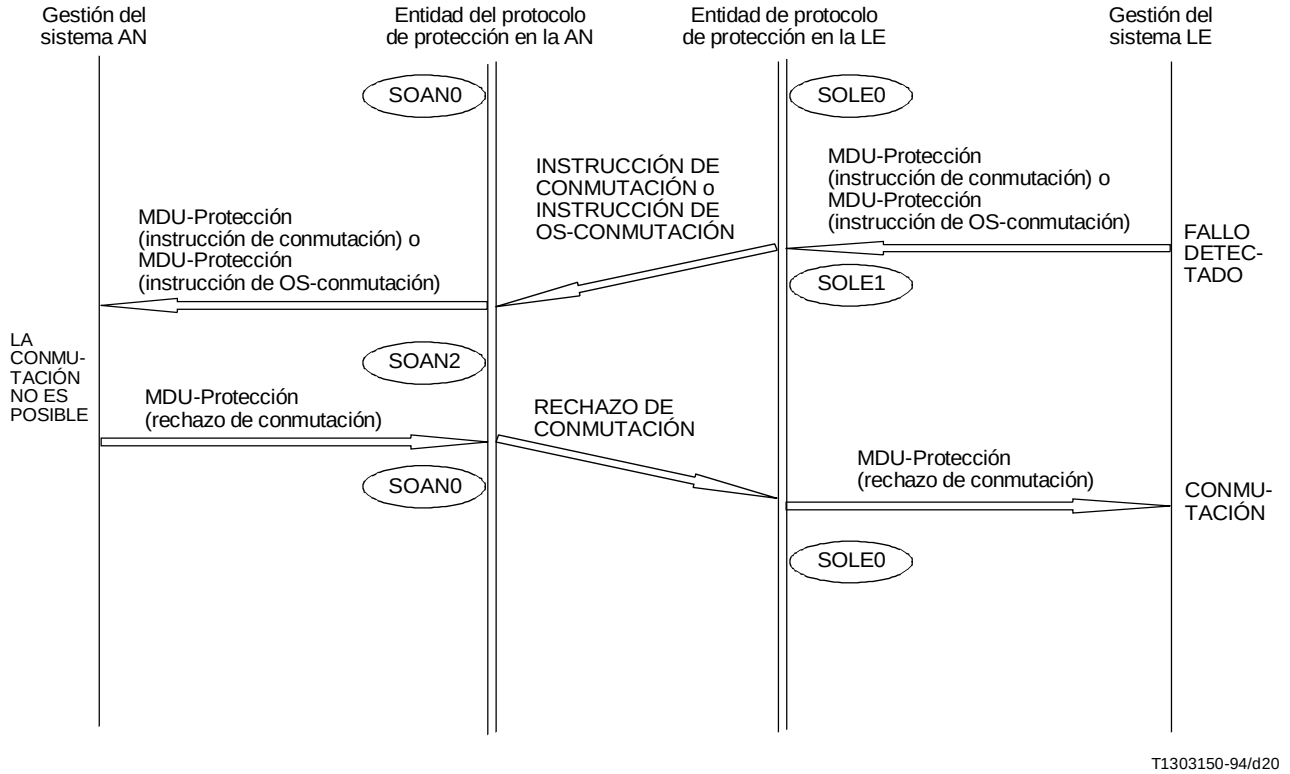


FIGURA J.3/G.965

Rechazo por la AN de una conmutación iniciada por la LE

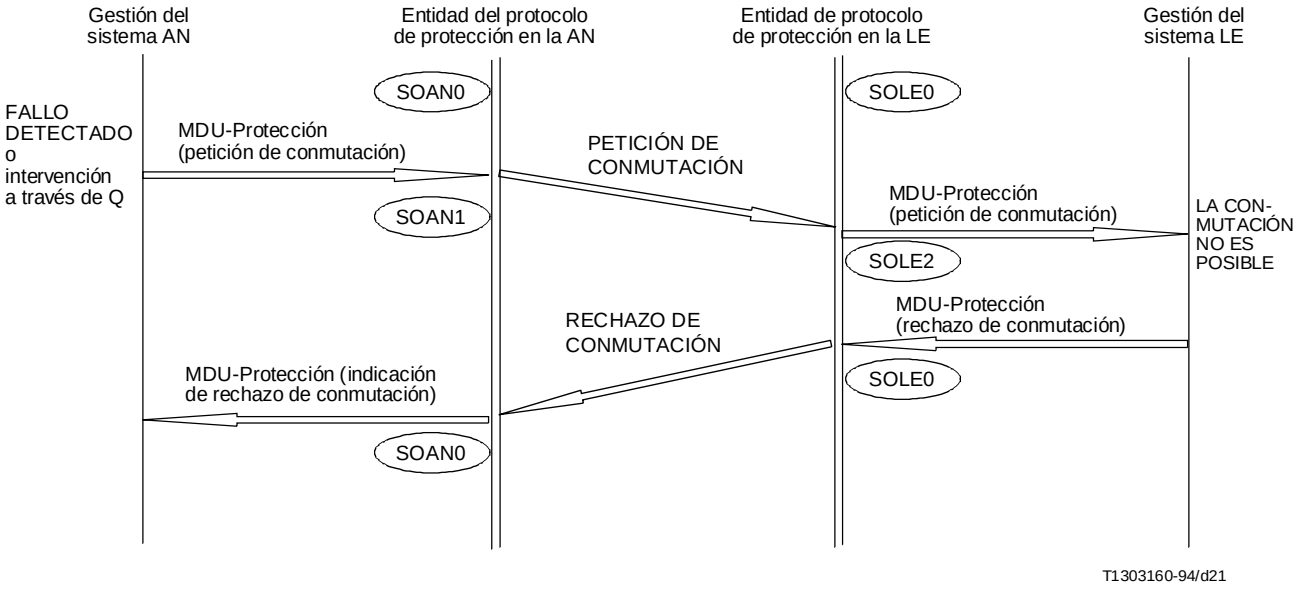
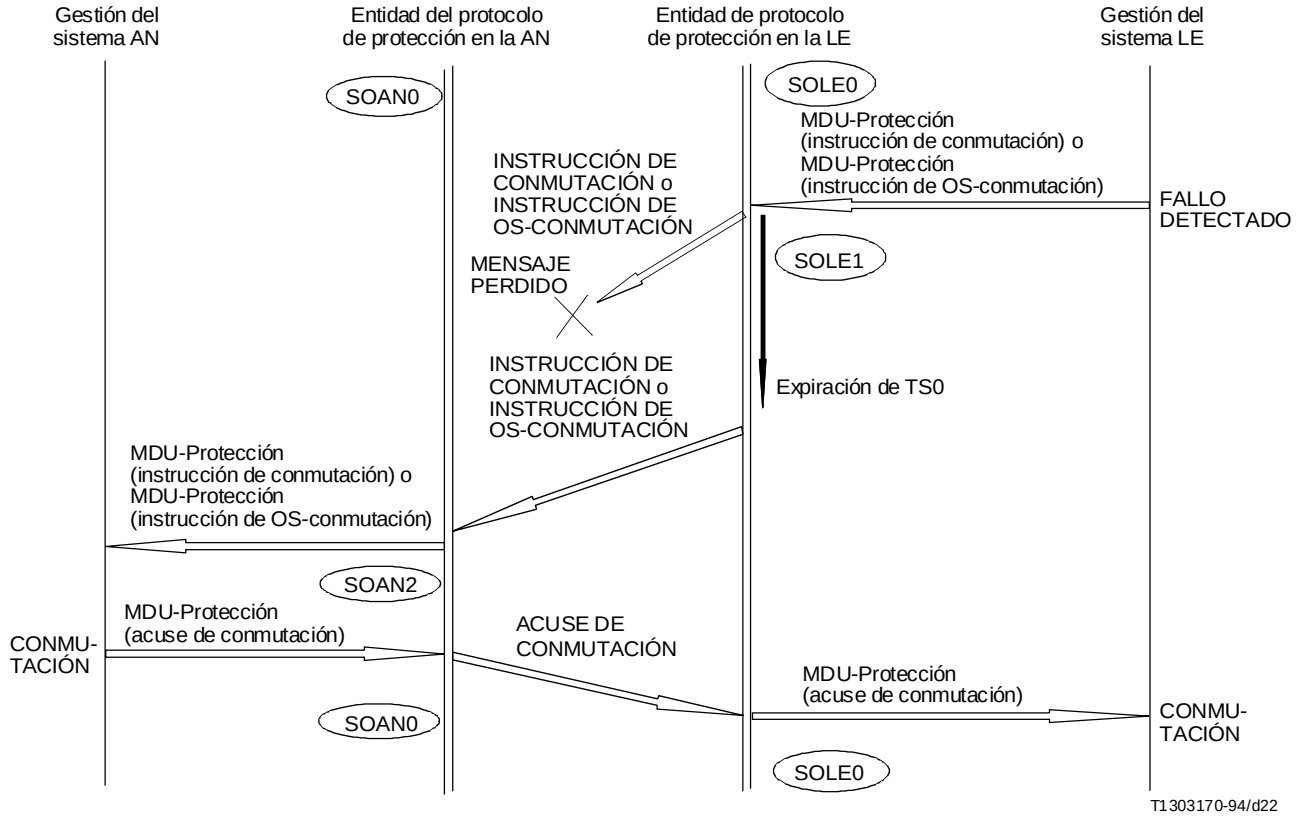


FIGURA J.4/G.965

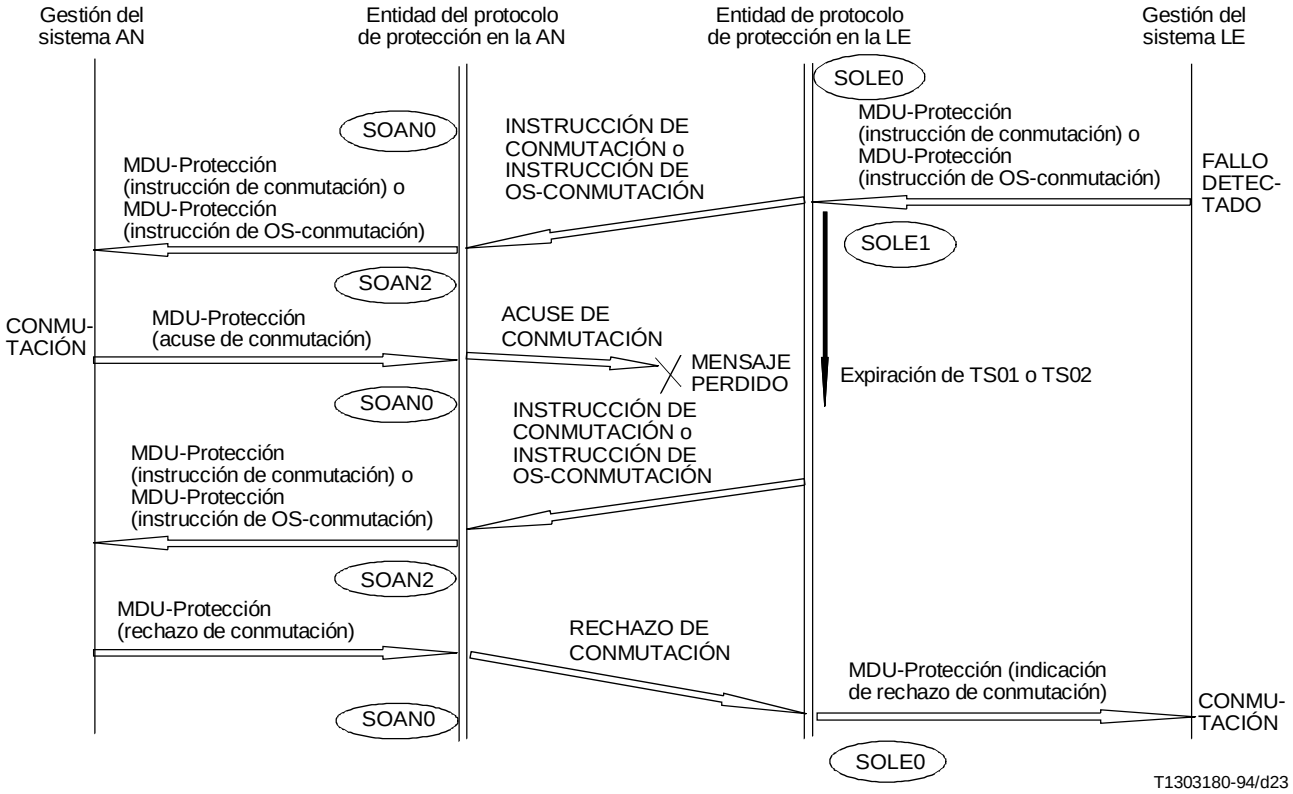
Rechazo por la LE de una conmutación iniciada por la AN



NOTA – La Figura muestra un ejemplo donde no hay retransmisión en L2 debido a la naturaleza de la condición de fallo.

FIGURA J.5/G.965

Conmutación iniciada por la LE con retransmisiones (pérdida de mensaje)



NOTA – La Figura muestra un ejemplo donde no hay retransmisión en L2 debido a la naturaleza de la condición de fallo.

FIGURA J.6/G.965

Conmutación iniciada por la LE (retransmisiones debidas a pérdida de mensaje)

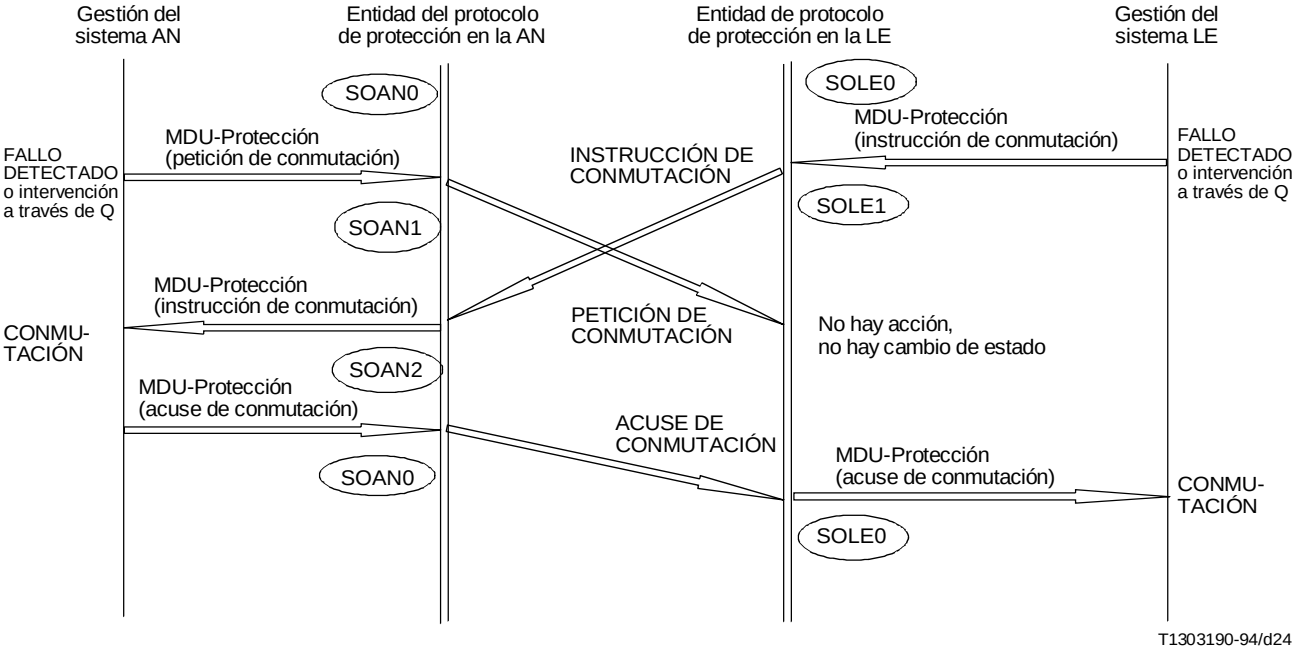


FIGURA J.7/G.965

Conmutación iniciada simultáneamente por la LE y la AN

Anexo K

Principios de aplicación del protocolo BCC

(Este anexo es parte integrante de esta Recomendación)

K.1 Introducción

El presente anexo proporciona información normativa sobre la forma de utilizar el protocolo BCC por la LE y la AN a fin de satisfacer los requisitos del servicio en la interfaz V5.2.

Las entidades de gestión de recursos gestionan los recursos implicados en el soporte de las conexiones del canal portador (intervalos de tiempo, puertos de usuario y canales de puerto de usuario RDSI) mediante el protocolo BCC. La funcionalidad es compartida entre las diversas entidades de la forma siguiente:

- las entidades de gestión de recursos de LE y de AN son responsables del mantenimiento de los recursos disponibles para soportar las conexiones de canal portador y su estado (por ejemplo, asignado o desasignado);

- el control del protocolo BCC (intercambio de mensajes entre la LE y la AN) es responsabilidad de la entidad de protocolo BCC;

- las entidades de gestión de recursos recibirán peticiones de servicio de las distintas entidades en la LE (por ejemplo, protocolo nacional RTPC, protocolo nacional DSS1, sistema de gestión); sin embargo la relación entre las entidades de gestión de recursos y las entidades que solicitan servicios BCC caen fuera del ámbito de la presente Recomendación.

El protocolo BCC proporciona los medios para soportar distintos tipos de servicios de usuario:

a) Servicio conmutado, donde la entidad de gestión de recursos asignará conexiones conmutadas para el soporte de las llamadas de usuario; estas conexiones estarán disponibles durante el tiempo de duración de la llamada. Los procesos de asignación y desasignación bajo el control de la entidad de recursos se activarán a partir de las entidades RTPC o DSS1 nacionales.

b) Servicio de líneas arrendadas semipermanentes, donde la entidad de gestión de recursos asignará conexiones conmutadas para el soporte de estas conexiones de usuario de gran duración. Los procesos de asignación y desasignación bajo el control de la entidad de recursos se activarán a partir de la entidad del sistema de gestión mediante una solicitud a través de la interfaz Q_{LE}.

   La utilización del protocolo BCC para el establecimiento de este tipo de conexiones garantiza que la entidad de gestión de recursos esté plenamente informada del estado de estas conexiones de canal portador. Si se produce una avería en el enlace de 2048 kbit/s por el que va la línea semipermanente, la entidad de gestión de recursos establecerá otro trayecto.

c) Servicio de canal portador preconectado, donde la entidad de gestión de recursos asignará conexiones conmutadas para ofrecer al usuario anchura de banda en forma de canales portadores de 64 kbit/s o múltiplos de este valor. Los procesos de asignación y desasignación bajo el control de la entidad de gestión de recursos se activarán a partir de la entidad del sistema de gestión mediante una petición a través de la interfaz Q_{LE}.

   Este servicio proporciona al usuario conexiones permanentes entre la LE y el puerto de usuario a través de la interfaz V5.2. Este servicio debe utilizarse cuando es importante que el factor de concentración ofrecido por la interfaz V5.2 no provoque un bloqueo de servicios cruciales (por ejemplo, el servicio de telefonía de un parque de bomberos).

   La utilización del protocolo BCC para el establecimiento de este tipo de conexiones garantiza que la entidad de gestión de recursos se encuentre plenamente informada del estado de estas conexiones de canal portador. Si se produce una avería en el enlace de 2048 kbit/s por el que va el canal portador preconectado, la entidad de gestión de recursos establecerá otro trayecto e informará de estas circunstancias a través de Q_{LE}.

K.2 Usabilidad de los intervalos de tiempo

Los intervalos de tiempo 1 a 14 y 17 a 30 de todos los enlaces de 2048 kbit/s de una interfaz V5.2 deberán estar disponibles para asignación como canales portadores.

Cuando no se disponga de los intervalos de tiempo 15, 16 ó 31 de cualquier enlace de 2048 kbit/s para su utilización como canal C físico, deberán estar disponibles para su empleo como canal portador.

Los canales portadores en una interfaz V5.2 deberán estar disponibles para su utilización por cualquier servicio (por ejemplo, portador RTPC, canal B de RDSI, canal H de RDSI). No habrá especialización de los canales portadores, grupos de canales portadores o enlaces de 2048 kbit/s a tipos de servicio/canal.

K.3 Reglas de asignación y desasignación de los intervalos de tiempo

K.3.1 Consideraciones generales

La LE y, cuando corresponda, la AN aplicarán las siguientes reglas para asignar los intervalos de tiempo de la interfaz V5.2 a las conexiones portadoras:

a) La LE será la única responsable de la asignación de los intervalos de tiempo.

b) La AN puede rechazar una conexión solicitada debido a una avería o a un error o a causa de un bloqueo interno de la AN.

c) La entidad de protocolo RTPC nacional de la LE o la entidad de protocolo de la RDSI nacional pueden solicitar la asignación de un nuevo intervalo de tiempo.

d) No es posible llevar a cabo un proceso de desasignación de una conexión de canal portador en el cual no estén incluidos todos los datos necesarios en el mensaje DESASIGNACIÓN.

   Cuando la LE no conozca todos los datos pertinentes que identifican una conexión de canal portador antes de iniciar el proceso de desasignación, solicitará la información restante a la AN utilizando el procedimiento de verificación.

   Si el resultado de dicho procedimiento es una notificación de que dicha conexión no existe, la LE suprimirá de manera interna el registro de conexión de canal portador BCC.

e) El canal o canales B de puerto de usuario de acceso básico RDSI o de acceso a velocidad primaria RDSI necesarios para realizar una llamada serán reservados de manera interna por la entidad de protocolo DSS1 antes de establecer el intervalo o intervalos de tiempo de la interfaz V5 utilizando el protocolo BCC. A continuación, utilizando los procedimientos DSS1, se asignará el canal o canales B y así se notificará al abonado RDSI en el mensaje DSS1 correspondiente. Puede resultar necesaria una redistribución de canales B bajo el control del abonado.

   Ello mantiene la capacidad del servicio DSS1 y permite solicitar a la conexión BCC que curse la identidad completa de ambos extremos de la conexión AN.

f) Para asignar los intervalos de tiempo, la LE aplicará la técnica de empaquetamiento de conexión; es decir, asignará conexiones a los enlaces de 2048 kbit/s de una interfaz V5.2 en un orden preferente. Los enlaces de 2048 kbit/s con más de un canal C físico recibirán la preferencia adecuada. Estas reglas se aplicarán a todas las conexiones a fin de minimizar la probabilidad de congestión en las conexiones multiintervalo.

   La técnica de empaquetamiento de conexión aumenta la influencia en el servicio de las averías no detectadas, especialmente en los instantes en que el nivel de tráfico es bajo. Esto puede mejorarse no estableciendo una sola preferencia fija. Por lo general, el efecto es un compromiso entre la característica de fallo y la característica de congestión de la conexión multiintervalo. La implementación de LE para el soporte de las interfaces V5.2 debe tener en cuenta este compromiso.

g) las conexiones semipermanentes de AN y los canales portadores preconectados serán reasignados por la gestión de la LE en otros enlaces de 2048 kbit/s (si hay disponibles), en caso de fallo del enlace de 2048 kbit/s que los incorpora o si el protocolo BCC informa de un fallo interno de la AN.

   Las conexiones portadoras conmutadas no se reasignarán a otros intervalos de tiempo V5.2 en caso de fallo.

h) En el caso de llamadas RDSI de terminación (llamadas ofrecidas por la LE a la AN), la LE debe indicar en el mensaje ESTABLECIMIENTO DSS1 que ha de enviarse al acceso RDSI la identificación del canal B o H que va a utilizarse para la llamada.

Por consiguiente, antes de enviar el mensaje ESTABLECIMIENTO, la LE debe asegurar la disponibilidad de los intervalos de tiempo necesarios en la interfaz que han de emplearse como canales portadores y que estos intervalos de tiempo estén adecuadamente asignados al puerto RDSI. Ello supone que es necesario contar con una sincronización de protocolo de manera que el proceso de asignación se haya completado antes de enviar el mensaje ESTABLECIMIENTO DSS1.

En caso de recepción de un mensaje RECHAZO DE ASIGNACIÓN, la entidad de protocolo BCC en la LE notificará dicha circunstancia a la entidad de gestión de recursos mediante la primitiva MDU.BCC (indicación de rechazo de asignación), que enviará igualmente la notificación adecuada a la entidad de protocolo RDSI. Al recibir dicha indicación, la entidad de protocolo RDSI puede solicitar otra asignación de canal portador antes de enviar el mensaje LIBERACIÓN COMPLETADA al abonado RDSI. El número de estos intentos, caso de haberlos, dependerá de las decisiones tomadas en la realización y de las limitaciones de temporización de DSS1 controladas por la entidad de protocolo RDSI.

i) En el caso de llamadas RDSI de origen (llamadas ofrecidas por la AN a la LE), la LE debe indicar en el mensaje de DSS1 enviado como respuesta al mensaje ESTABLECIMIENTO recibido (es decir, ALERTA, LLAMADA EN CURSO, CONEXIÓN) la identificación del canal B o H que va a utilizarse para la llamada.

Por consiguiente, antes de enviar la respuesta adecuada al mensaje ESTABLECIMIENTO recibido, la LE debe asegurarse de la disponibilidad de los intervalos de tiempo necesarios en la interfaz que han de utilizarse como canales portadores y que dichos intervalos de tiempo estén adecuadamente asignados al puerto RDSI. Ello supone la necesidad de establecer una sincronización de protocolo de forma que el proceso de asignación esté completado antes de transmitir el mensaje DSS1 como respuesta al mensaje ESTABLECIMIENTO recibido.

j) En el caso de llamadas RTPC de terminación (llamadas ofrecidas por la LE a la AN), por regla general la LE, antes de enviar la «señal de llamada inicial», debe asegurarse de la disponibilidad de un canal portador para la llamada. Sin embargo, hay algunos casos en los que se establece un trayecto de señalización RTPC y no se necesita ninguna asignación de canal portador.

k) En el caso de llamadas RTPC de origen (llamadas ofrecidas por la AN a la LE), por regla general la LE, antes de enviar el «tono de marcación», debe asegurar la disponibilidad de un canal portador para la llamada. Sin embargo, hay algunos casos en los que está establecido un trayecto de señalización RTPC y no se necesita ninguna asignación de canal portador.

l) Al liberar las llamadas RDSI o RTPC (iniciadas por el usuario o por la red), la LE iniciará las acciones adecuadas hacia la AN para liberar los recursos V5.2 asignados a esa llamada en particular.

Al iniciar un proceso de desasignación relativo al puerto RDSI, la LE puede desconectar el canal portador (intervalo de tiempo V5) de la conexión de llamada y proceder a liberar la llamada RDSI antes de finalizar el proceso de desasignación (es decir, no es necesaria la sincronización entre el protocolo DSS1 y el proceso de desasignación BCC).

m) En el cuadro K.1 aparece información sobre cuándo utilizar los distintos tipos de causa de rechazo en los procedimientos del protocolo BCC.

n) Además de la posible asignación/desasignación de los canales portadores, la prestación de servicios suplementarios DSS1 no requerirá ninguna otra función del protocolo BCC.

CUADRO K.1/G.965

Utilización de los tipos de causa de rechazo

Causa	Descripción
Sin especificar	Se ha encontrado una avería que no aparece en este cuadro
Avería en la red de acceso	El proceso de asignación o desasignación no puede completarse debido a que se ha identificado una avería interna en la AN
Red de acceso bloqueada (internamente)	No puede completarse el proceso de asignación puesto que se ha descubierto un bloqueo interno de la AN
Ya está presente la conexión en el puerto de usuario RTPC con un intervalo de tiempo V5 distinto	El proceso de asignación no puede completarse debido a que ya existe una conexión en el puerto RTPC seleccionado con un intervalo de tiempo diferente
Ya está presente la conexión en el intervalo o intervalos de tiempo con un puerto diferente o con un intervalo de tiempo de puerto de usuario RDSI diferente	El proceso de asignación no puede completarse debido a que ya existe una conexión en el intervalo o intervalos de tiempo V5.2 seleccionados con un puerto de usuario diferente o un intervalo de tiempo de puerto de usuario diferente
Ya está presente la conexión en el intervalo o intervalos de tiempo de puerto de usuario RDSI con un intervalo o intervalos de tiempo diferentes	El proceso de asignación no puede completarse debido a que ya existe una conexión en un intervalo o intervalos de tiempo de puerto de usuario seleccionados con un intervalo o intervalos de tiempo diferentes
Indisponibilidad del puerto de usuario (bloqueado)	El proceso de asignación no puede completarse porque el puerto de usuario seleccionado no está disponible para el servicio
No puede completarse la desasignación debido a contenido de datos incompatible	El proceso de desasignación no puede completarse puesto que los datos suministrados relativos al intervalo de tiempo, puerto de usuario e intervalo de tiempo de puerto de usuario no corresponden a ninguna conexión de puerto de usuario
No puede completarse la desasignación debido a incompatibilidad del intervalo o intervalos de tiempo V5	El proceso de desasignación no puede completarse debido a que los datos proporcionados relativos al intervalo o intervalos de tiempo V5 no corresponden a los datos AN
No puede completarse la desasignación debido a incompatibilidad de datos de puerto	No puede completarse el proceso de desasignación puesto que los datos proporcionados relativos al puerto de usuario no corresponden a un puerto de usuario AN
No puede completarse la desasignación debido a incompatibilidad de datos de intervalo o intervalos de tiempo de puerto de usuario	El proceso de desasignación no puede completarse puesto que los datos proporcionados relativos al intervalo o intervalos de tiempo de puerto de usuario no corresponden al (a los) puerto(s) de usuario AN
Puerto de usuario no aprovisionado	El proceso de asignación no puede completarse puesto que no se ha aprovisionado el puerto de usuario identificado
La identificación o identificaciones del intervalo o intervalos de tiempo V5 no son válidas	La identificación del intervalo o intervalos de tiempo V5 no corresponden a las disponibles para su utilización como canales portadores
La identificación del enlace 2048 kbit/s no es válida	La identificación del enlace de 2048 kbit/s en la interfaz V5.2 no corresponde a ningún enlace disponible
La identificación o identificaciones del intervalo o intervalos de tiempo de puerto de usuario no son válidas	La identificación del intervalo o intervalos de tiempo de puerto de usuario no corresponden a las disponibles en el puerto de usuario RDSI seleccionado
El intervalo o intervalos de tiempo V5 se utilizan como canal o canales C físicos	No puede completarse el proceso puesto que el intervalo de tiempo V5 identificado se está utilizando como canal C físico
NOTA – Ningún otro valor es aplicable.	

K.3.2 Conexiones multiintervalo

La LE y, cuando corresponda, la AN deberán aplicar las siguientes reglas para asignar los intervalos de tiempo de la interfaz V5.2 a las conexiones portadoras multiintervalos (es decir, n × 64 kbit/s):

a) Al principio de una llamada (o de una asignación de canal portador semipermanente o preconectado), todos los intervalos de tiempo de una conexión multiintervalo se asignarán de forma simultánea mediante un solo proceso de asignación BCC.

b) Durante una llamada (o una asignación semipermanente o preconectada), deberá ser posible liberar de manera individual los intervalos de tiempo que constituyen una conexión multiintervalo o liberar de forma simultánea una parte de los intervalos de tiempo. Esta capacidad permite reducir la asignación de anchura de banda para la parte restante de una llamada (o asignación semipermanente o preconectada).

c) Al final de una llamada (o asignación semipermanente o preconectada), todos los intervalos de tiempo que constituyen una conexión multiintervalo se liberarán de forma simultánea.

d) Los múltiples intervalos de tiempo requeridos para una conexión multiintervalo se seleccionarán entre los intervalos de tiempo libres (dentro de un enlace a 2048 kbit/s) y no tienen por qué estar en un bloque de intervalos de tiempo contiguos.

e) Se aplicará el atributo estructural de la integridad de secuencia del intervalo de tiempo al elemento de conexión entre la interfaz usuario-red y la interfaz V5. Por consiguiente:

   – en la interfaz usuario-red y la interfaz V5, los intervalos de tiempo están implícita o explícitamente señalados para cada canal de una combinación de canales;

   – las partes de información obtenidas de los intervalos de tiempo en el extremo receptor se encuentran en el mismo orden con que fueron presentadas en el extremo transmisor;

   – todos los intervalos de tiempo utilizados en el lado de usuario se encontrarán en la misma interfaz de acceso básico RDSI o de acceso a velocidad primaria RDSI;

   – todos los intervalos de tiempo utilizados en la interfaz V5 se encontrarán en el mismo enlace a 2048 kbit/s.

f) El atributo estructural de integridad de 8 kHz se aplicará al elemento de conexión entre la interfaz usuario-red y la interfaz V5. Por consiguiente:

   – en la interfaz usuario-red y la interfaz V5, los intervalos de 125 μs están implícita o explícitamente delimitados (por ejemplo mediante límites de tramas); y

   – todos los bits presentados en un solo intervalo de 125 μs delimitado se entregan dentro del intervalo de 125 μs delimitado correspondiente.

g) Si es necesario un canal portador preconectado para soportar servicios conmutados a velocidades múltiples (por ejemplo, H0 o H12), por oposición a los servicios de 64 kbit/s solamente, se establecerá como una conexión de n × 64 kbit/s, para asegurar a tales servicios integridad de secuencia del intervalo de tiempo e integridad de 8 kHz.

K.3.3 Capacidad de contraorden

Para soportar mejor algunas capacidades de servicio de usuario, al asignar las conexiones de canal portador la LE puede utilizar la capacidad de contraorden. Ello permite que el canal portador que ha sido conectado a un canal B de un puerto de usuario RDSI se conecte a otro canal B en el mismo puerto de usuario RDSI.

Esta capacidad puede utilizarse únicamente en procesos de asignación de un solo canal portador de 64 kbit/s.

K.4 Reglas del procedimiento de verificación

El protocolo BCC incluye los medios necesarios para que la LE pueda obtener información de la AN acerca de ciertas conexiones sobre las que la información es parcialmente desconocida por dicha LE. Este procedimiento deberá ajustarse a ciertas reglas tales como:

a) la LE iniciará una verificación únicamente cuando no haya ningún otro proceso pendiente de compleción (asignación o desasignación);

b) cuando se haya iniciado un proceso de verificación, la LE no arrancará ningún otro proceso de asignación o desasignación;

c) pueden realizarse simultáneamente varios procesos de verificación utilizando distintos números de referencia BCC;

d) los procesos de verificación serán iniciados por la entidad de gestión de recursos en la LE o a petición de la entidad de gestión del sistema;

e) en el Cuadro K.2 aparece información sobre cuándo utilizar los distintos valores de razón que figuran en el protocolo BCC.

CUADRO K.2/G.965

Utilización de los valores de razón

Razón	Utilización
Normal incompleto	No puede completarse el proceso de verificación debido a que la conexión no existe
No se ha aprovisionado el puerto de usuario	No puede completarse el proceso de verificación puesto que no se ha aprovisionado el puerto de usuario identificado
Identificación del intervalo de tiempo V5 no válida	La identificación del canal portador no corresponde a la disponible para el canal portador sometido a verificación
Enlace de 2048 kbit/s no válido	La identificación del enlace de 2048 kbit/s en la interfaz V5.2 no corresponde a la que soporta el canal portador sometido a verificación
Intervalo de tiempo utilizado como canal C físico	No puede completarse el proceso puesto que se está utilizando el intervalo de tiempo identificado como canal C físico

K.5 Reglas de notificación de fallo interno en la AN

El protocolo BCC incluye los medios necesarios para que la AN pueda notificar a la LE fallos internos que afectan las conexiones interiores que soportan los canales portadores. Para la utilización de este procedimiento se aplican las reglas siguientes:

a) La AN notificará todas las conexiones internas que soportan la conexión de canal portador cuando aparezca un fallo interno.

   Los fallos internos que no afecten a los canales portadores asignados no se notificarán a través del protocolo BCC.

b) La notificación de un fallo interno en la AN se realizará sobre la base de cada conexión de 64 kbit/s, iniciando un proceso individual para cada una de ellas.

c) Al notificar un fallo interno, la AN proporcionará la mayor información posible para que la LE pueda identificar la conexión portadora. Sin embargo, si la AN no puede proporcionar toda la información solicitada, la LE obtendrá la información completa a partir de sus datos internos basándose en la información parcial recibida.

K.6 Reglas de fallo interno en la AN

Cuando se notifica un fallo interno en la AN por dicha AN a la LE, la entidad de gestión de recursos en la LE iniciará el procedimiento de desasignación para la conexión de canal portador notificada. La entidad de gestión de recursos de LE notificará igualmente dicha circunstancia a la entidad de protocolo RTPC/RDSI para que se lleve a cabo la acción de servicio adecuada.

Si la entidad de gestión de recursos de LE identifica que la conexión de canal portador afectada forma parte de una disposición multiintervalo, dicha entidad de gestión de recursos no llevará a cabo ninguna acción en el resto de las conexiones de canal portador. La activación de la acción adecuada que debe tomarse (por ejemplo, desasignación del resto de conexiones de canal portador) es responsabilidad de la entidad de protocolo RDSI basándose en los requisitos del servicio.

K.7 Errores del protocolo BCC

Las entidades del protocolo BCC deberán poder detectar tres categorías distintas de errores de protocolo:

a) Errores referentes a un proceso BCC activo (por ejemplo, debido a la ausencia de respuesta a la retransmisión de un mensaje ASIGNACIÓN). Estos errores deberán notificarse a la entidad de gestión de recursos.

b) Errores relativos a un proceso BCC no existente (por ejemplo, debido a la recepción de un mensaje ASIGNACIÓN COMPLETA cuando la LE se encuentra en el estado Bcc0). Esos errores deberán notificarse a la entidad de gestión del sistema.

c) Errores referentes a los procedimientos de tratamiento de errores de protocolo (véase 17.5.8). Estos errores se notificarán a la gestión del sistema.

K.8 Diagramas de flechas: ejemplos de protocolo BCC y coordinación DSS1

K.8.1 Llamada RDSI iniciada por el abonado

K.8.1.1 Procedimiento normal

En la Figura K.1 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 para el caso de una llamada iniciada por el abonado (procedimiento normal).

En el caso de un establecimiento de llamada RDSI y una asignación de canal portador, se muestra la necesidad de realizar una sincronización de protocolo; el proceso de asignación debe completarse antes de transmitir el mensaje DSS1 en respuesta al mensaje ESTABLECIMIENTO recibido.

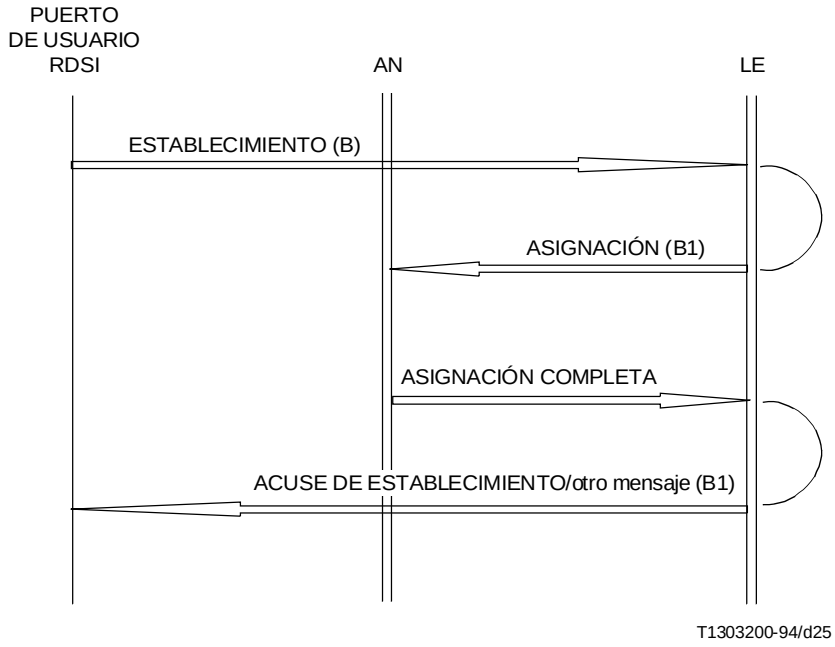


FIGURA K.1/G.965

Llamada RDSI iniciada por el abonado, procedimiento normal

K.8.1.2 Procedimiento excepcional

En la Figura K.2 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 para el caso de una llamada iniciada por el abonado (procedimiento excepcional).

K.8.1.3 Establecimiento de llamada RDSI simultánea (desde el mismo puerto RDSI)

En la Figura K.3 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 para el caso de un establecimiento de llamada RDSI simultánea desde un puerto de usuario.

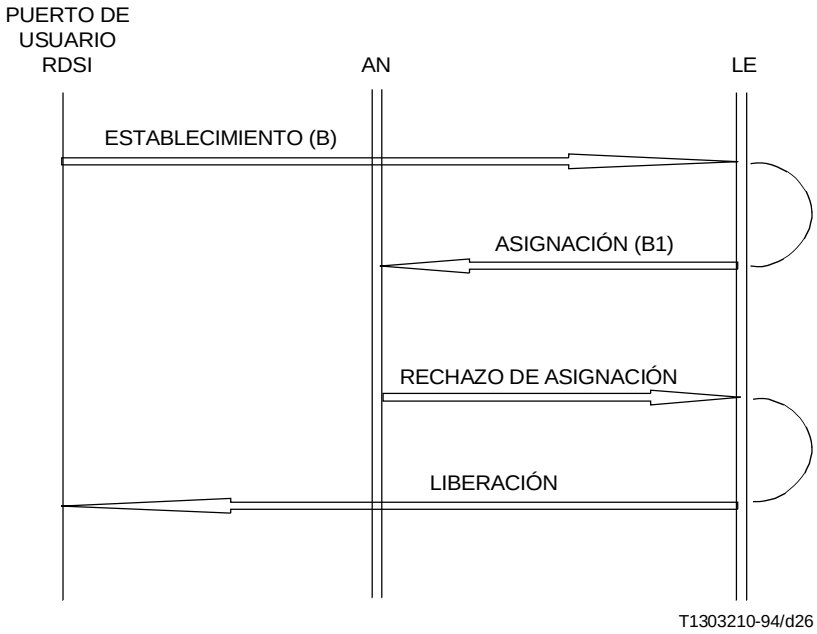


FIGURA K.2/G.965

Llamada RDSI iniciada por el abonado, procedimiento excepcional

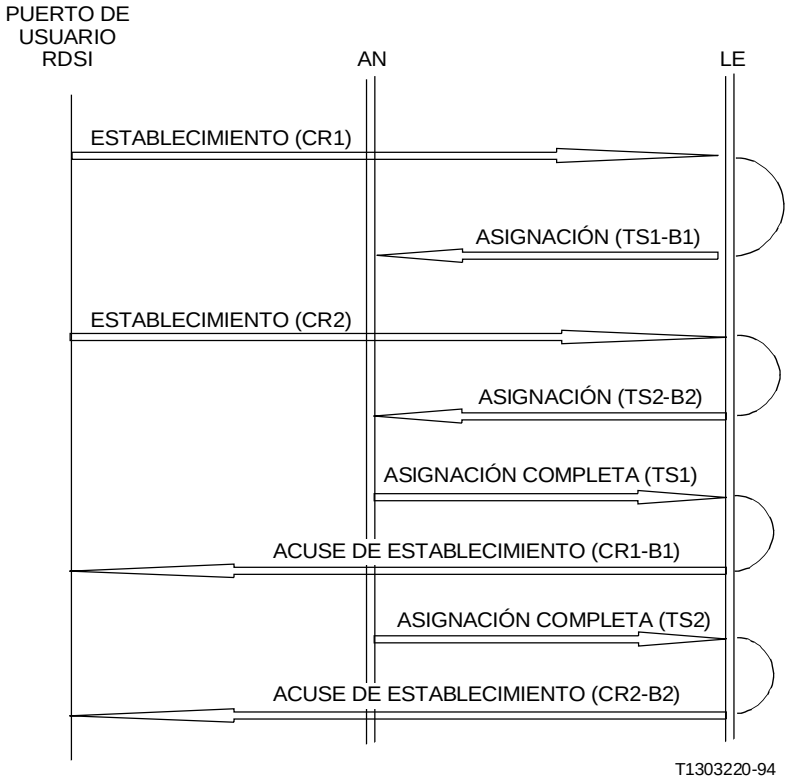


FIGURA K.3/G.965

Establecimiento de llamada RDSI simultánea desde un puerto de usuario RDSI

K.8.2 Llamada RDSI iniciada por la red

K.8.2.1 Negociación de canal B no permitida (por ejemplo, configuración de bus pasiva)

En la Figura K.4 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 para el caso de una llamada RDSI iniciada por la red (negociación de canal B no permitida).

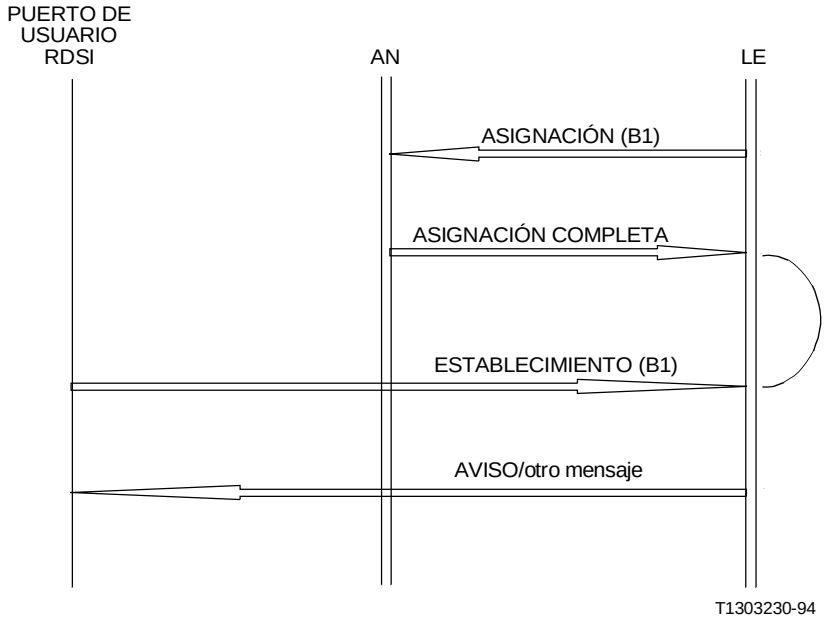


FIGURA K.4/G.965

Llamada RDSI iniciada por la red, negociación de canal B no permitida

K.8.2.2 Negociación de canal B permitida (por ejemplo, configuración punto a punto)

En la Figura K.5 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 para el caso de una llamada RDSI iniciada por la red (negociación de canal B permitida).

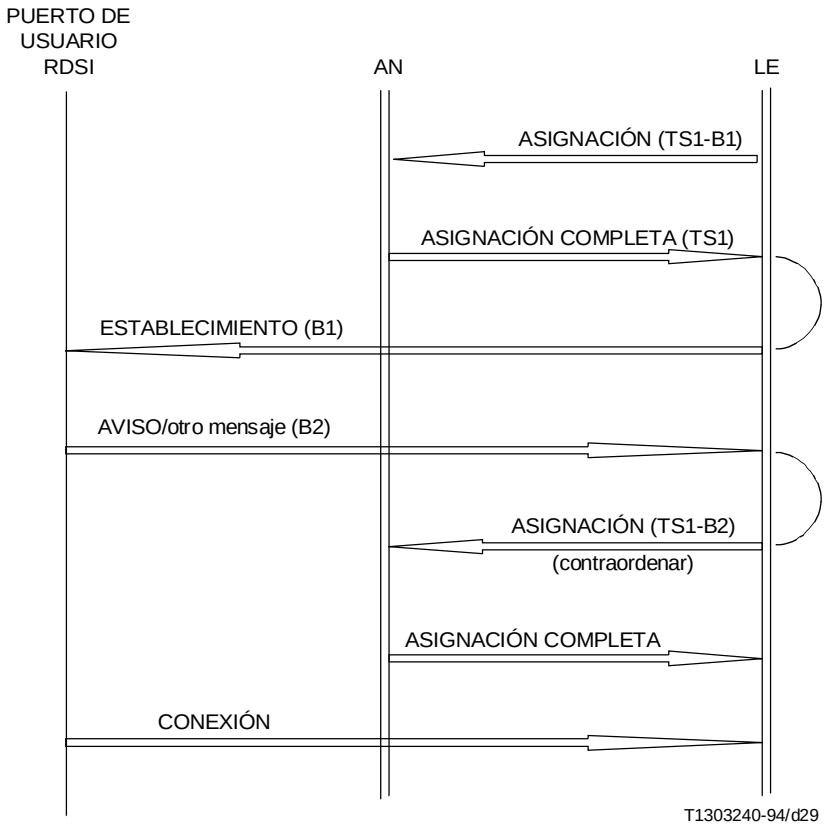


FIGURA K.5/G.965

Llamada RDSI iniciada por la red, negociación de canal B permitida

K.8.2.3 Soporte del servicio suplementario de llamada RDSI en espera

En la Figura K.6 se representa el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 cuando no se dispone de ningún canal B en la UNI.

En el punto (indicado en la Figura K.6 por X), tiene lugar una reasignación interna en la LE, los recursos utilizados por un puerto para una llamada (intervalo de tiempo y canal B) se reasignan a una nueva llamada que debe terminarse en el mismo punto final. El soporte de este servicio suplementario RDSI es una función interna de la LE correspondiente (entidad de gestión de recursos BCC), sin ninguna implicación en la entidad de protocolo BCC.

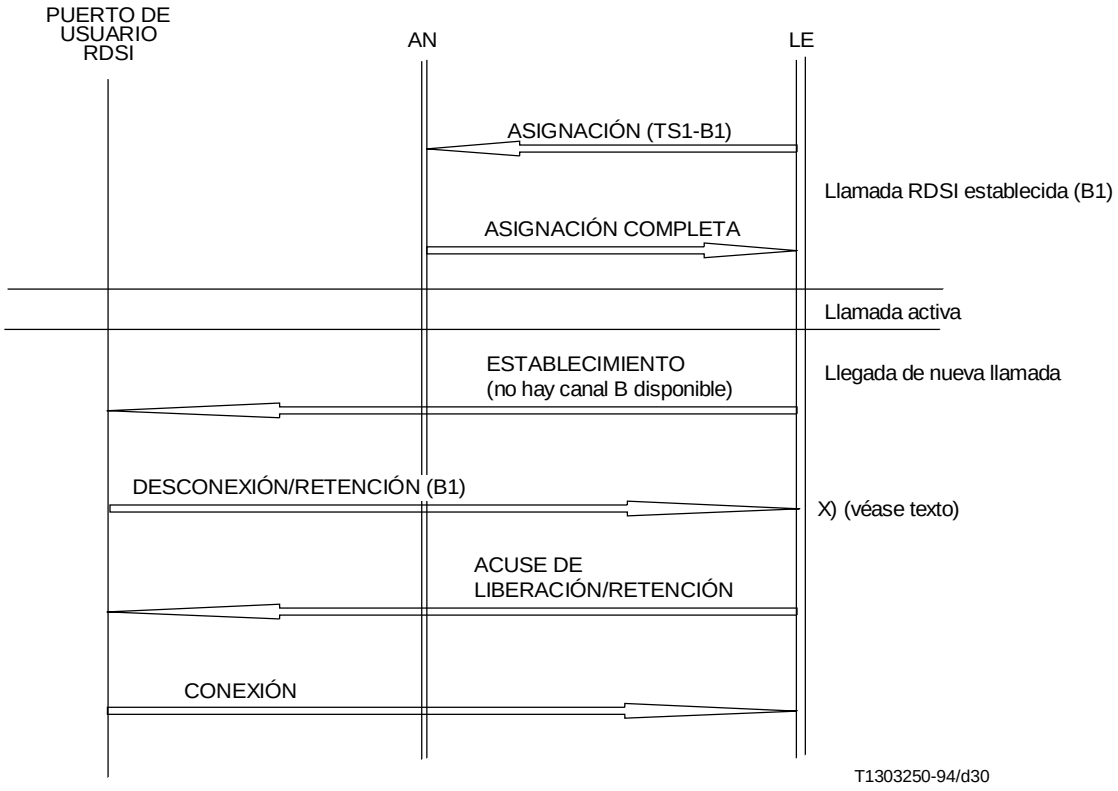


FIGURA K.6/G.965

Llamada RDSI iniciada por la red, soporte del servicio suplementario de llamada en espera

K.8.3 Liberación de llamada RDSI iniciada por el abonado

En la Figura K.7 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 en el caso de liberación de llamada iniciada por el abonado.

En el caso de liberación de llamada RDSI y desasignación de canal portador, no es necesaria la sincronización de protocolos; por consiguiente, el envío de la respuesta DSS1 al mensaje DESCONEXIÓN está desacoplado del envío del mensaje DESASIGNACIÓN.

K.8.4 Liberación de llamada RDSI iniciada por la red

En la Figura K.8 aparece el diagrama de flechas que muestra la interacción del protocolo BCC con DSS1 en el caso de liberación de llamada iniciada por la red.

En el caso de una liberación de llamada RDSI y desasignación de canal portador, no es necesaria la sincronización del protocolo; por consiguiente, el envío del mensaje DESASIGNACIÓN está desacoplado de la recepción del mensaje LIBERACIÓN DSS1.

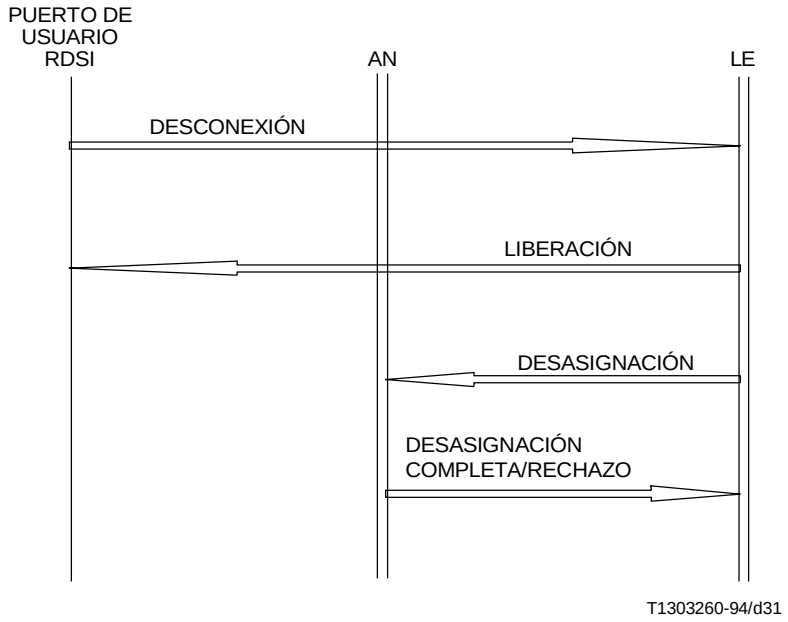


FIGURA K.7/G.965

Liberación de llamada RDSI iniciada por el abonado

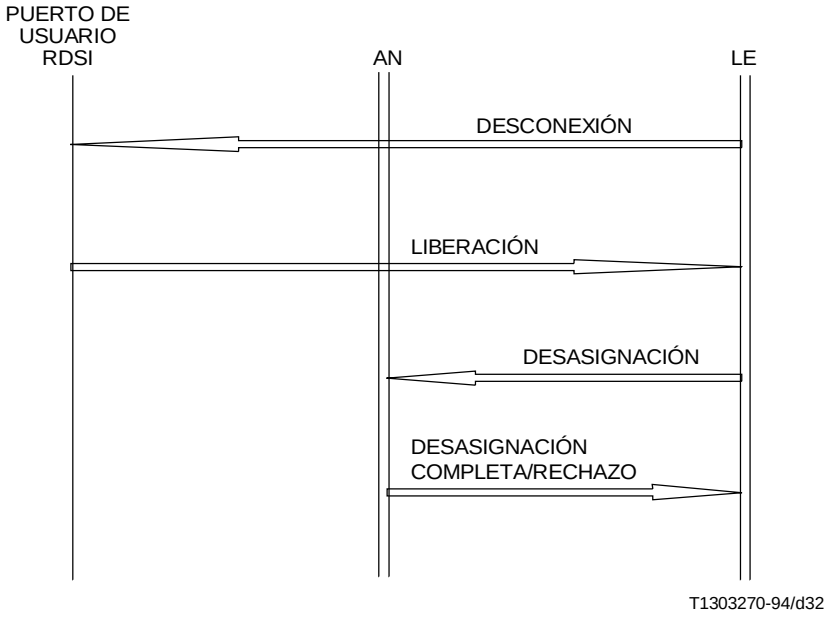


FIGURA K.8/G.965

Liberación de llamada RDSI iniciada por la red

K.8.5 Soporte del servicio suplementario de portabilidad del terminal

En la Figura K.9 aparece el diagrama de flechas que muestra la forma en que deben soportarse los mensajes DSS1 SUSPENDER y REANUDAR.

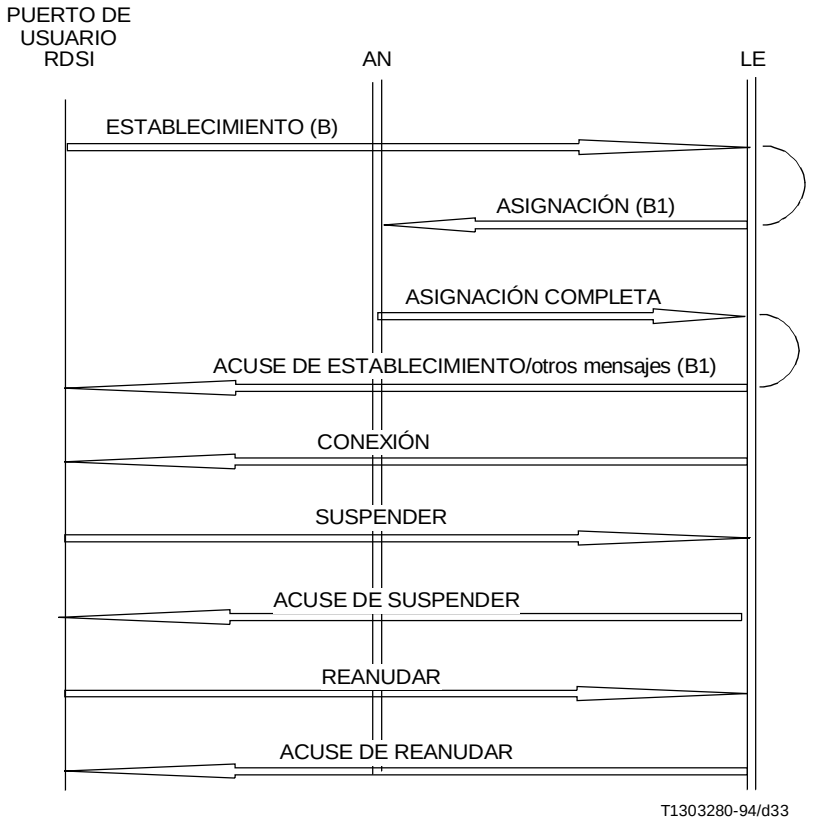


FIGURA K.9/G.965

Servicio suplementario de portabilidad del terminal

K.9 Diagramas de flechas: Ejemplos de coordinación de protocolo BCC y RTPC

En esta subcláusula se indica la coordinación esperada entre la BCC y las entidades RTPC nacionales. No aparece la lista completa de las posibilidades y tiene únicamente carácter informativo.

K.9.1 Llamada RTPC iniciada por el abonado

K.9.1.1 Procedimiento normal

En la Figura K.10 aparece el diagrama de flechas que muestra un ejemplo sobre la interacción del protocolo BCC con el protocolo RTPC para el caso de una llamada iniciada por el abonado (procedimiento normal).

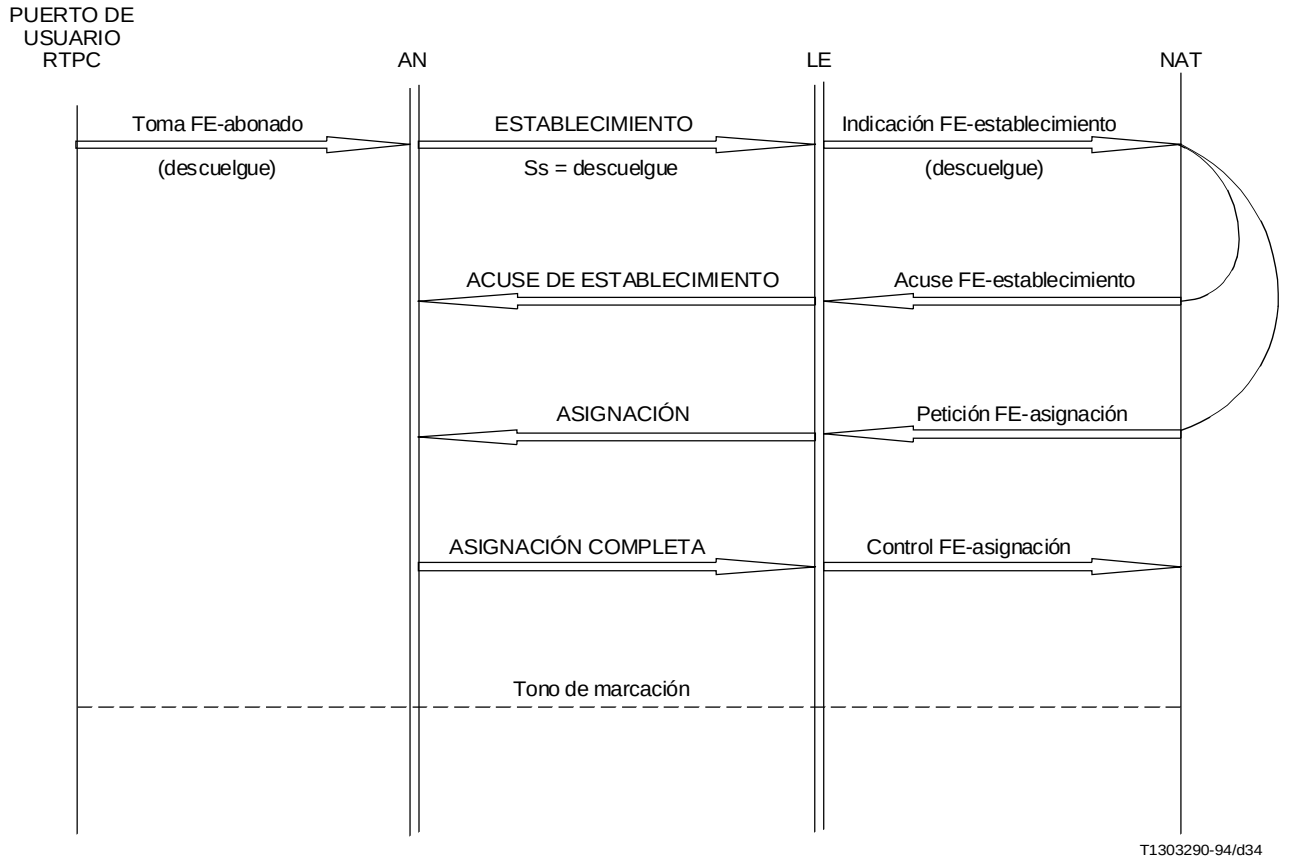


FIGURA K.10/G.965

Llamada RTPC iniciada por el abonado, procedimiento normal

K.9.1.2 Procedimiento excepcional

En la Figura K.11 aparece el diagrama de flechas que muestra un ejemplo de interacción del protocolo BCC con el protocolo RTPC para el caso de una llamada iniciada por el abonado (procedimiento excepcional). Tras el mensaje ASIGNACIÓN RECHAZADA procedente de la AN puede haber otras tentativas para asignar un canal portador (por ejemplo, controladas por un temporizador en el protocolo nacional).

K.9.2 Llamada RTPC iniciada por la red

En la Figura K.12 aparece el diagrama de flechas que muestra un ejemplo de la interacción del protocolo BCC con el protocolo RTPC para el caso de una llamada iniciada por la red.

K.9.3 Colisión de llamadas

K.9.3.1 Colisión de llamadas: La llamada de origen tiene prioridad

En la Figura K.13 aparece el diagrama de flechas que muestra un ejemplo de interacción del protocolo BCC con el protocolo RTPC en caso de colisión de llamadas (la llamada de origen tiene prioridad).

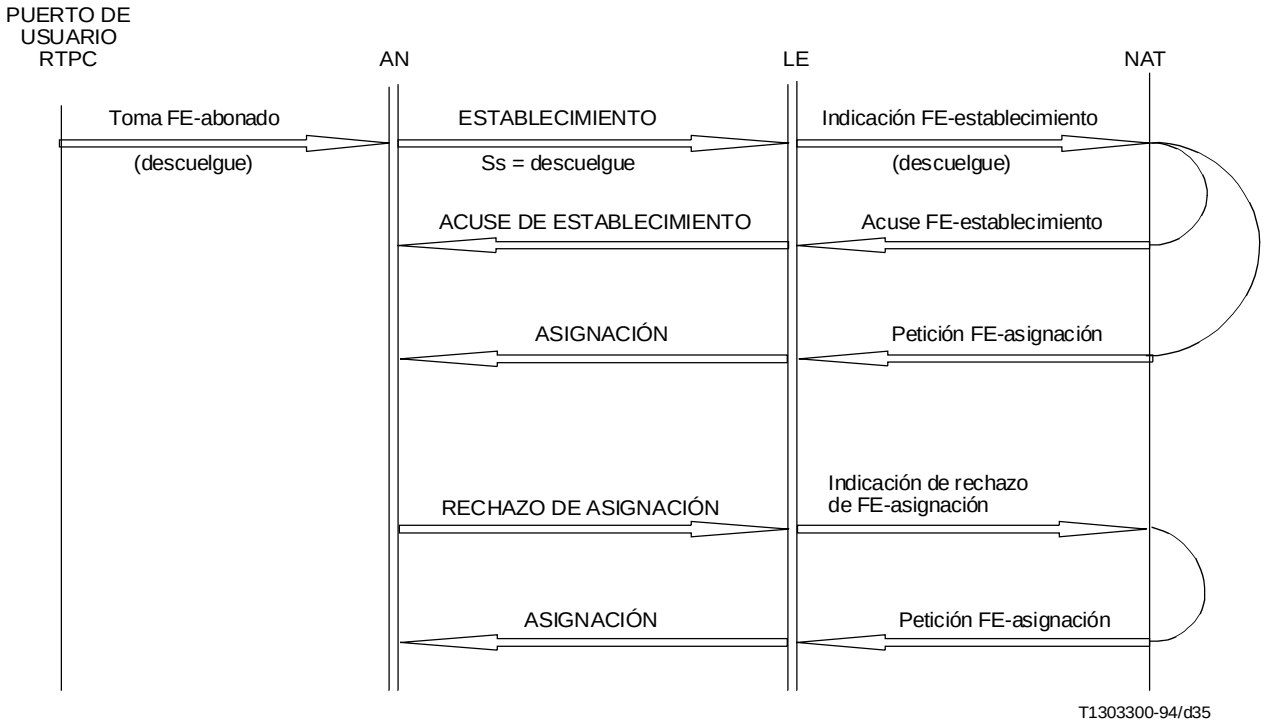


FIGURA K.11/G.965

Llamada RTPC iniciada por el abonado, procedimiento excepcional

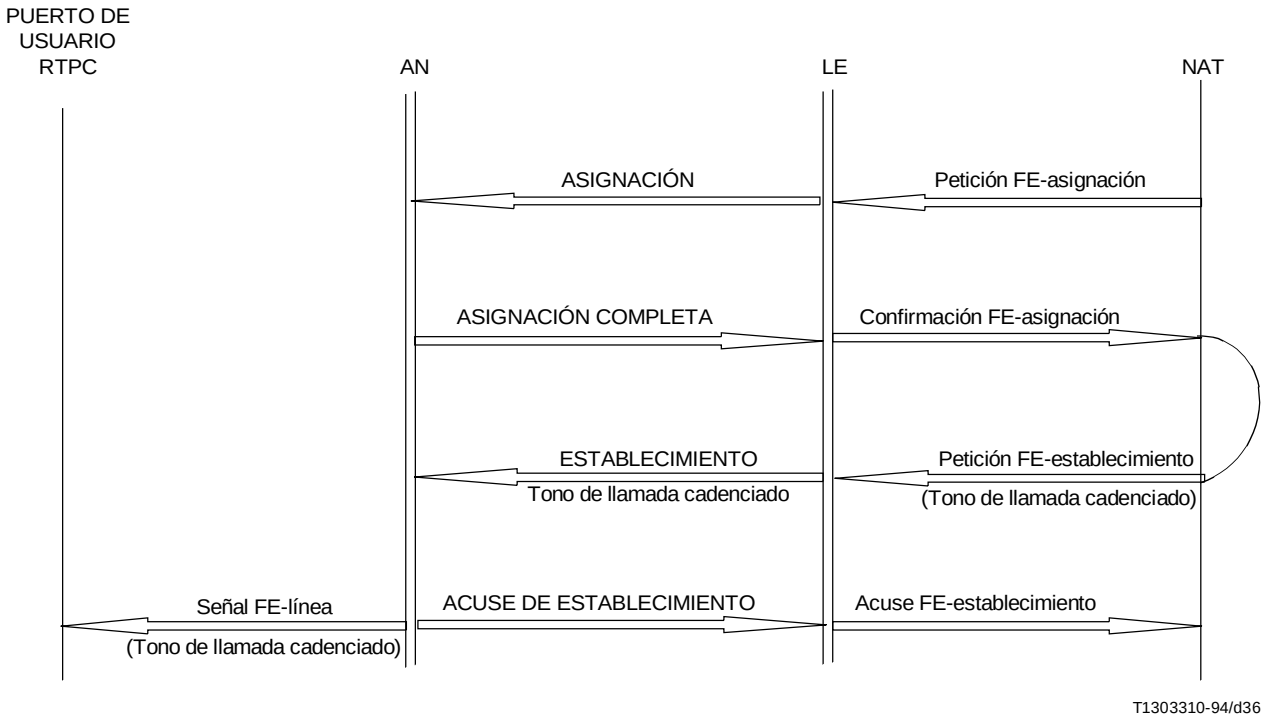


FIGURA K.12/G.965

Llamada RTPC iniciada por la red

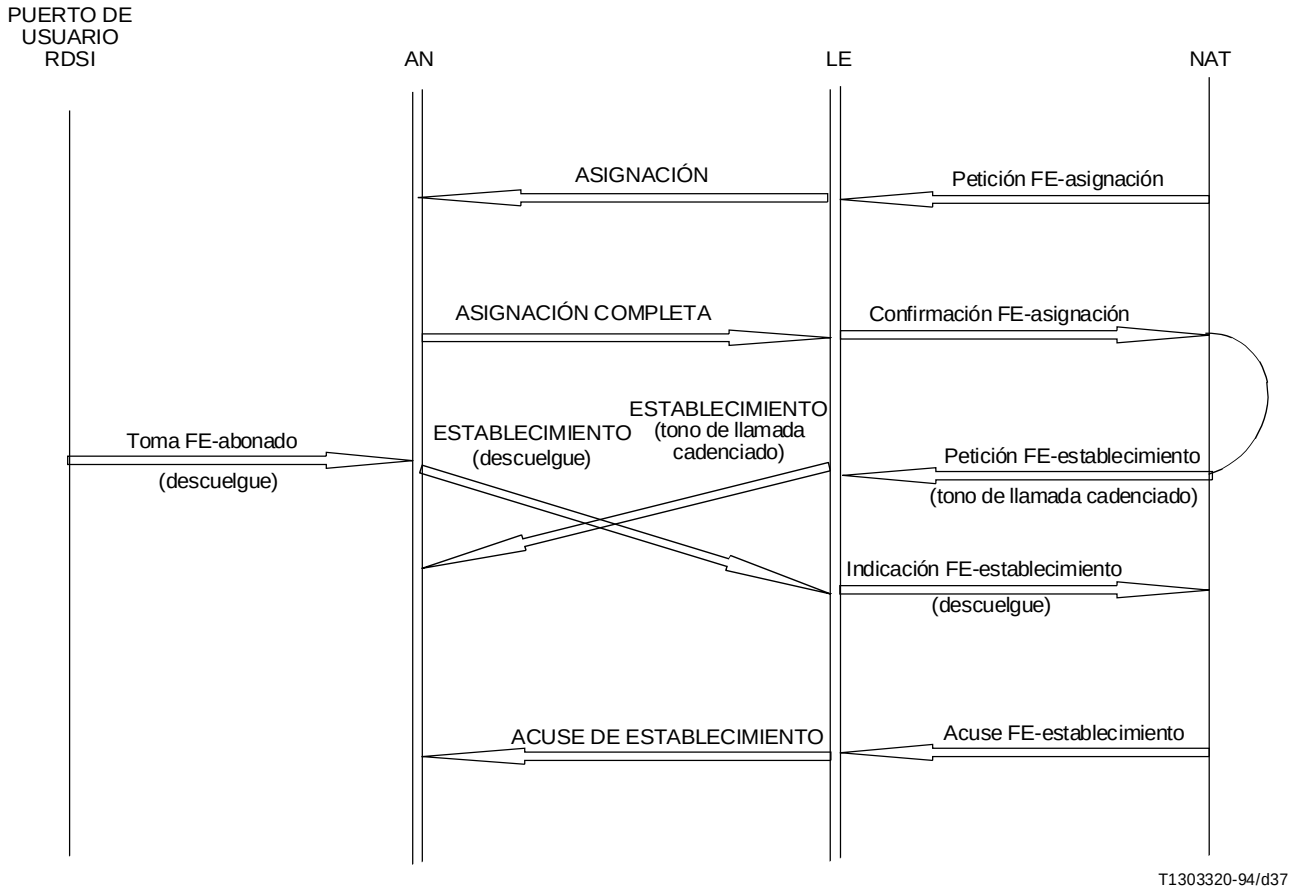


FIGURA K.13/G.965

Colisión de llamada RTPC, la llamada de origen tiene prioridad

K.9.3.2 La llamada de terminación tiene prioridad

En la Figura K.14 aparece el diagrama de flechas que muestra un ejemplo de interacción del protocolo BCC con el protocolo RTPC en el caso de colisión de llamadas (la llamada de terminación tiene prioridad).

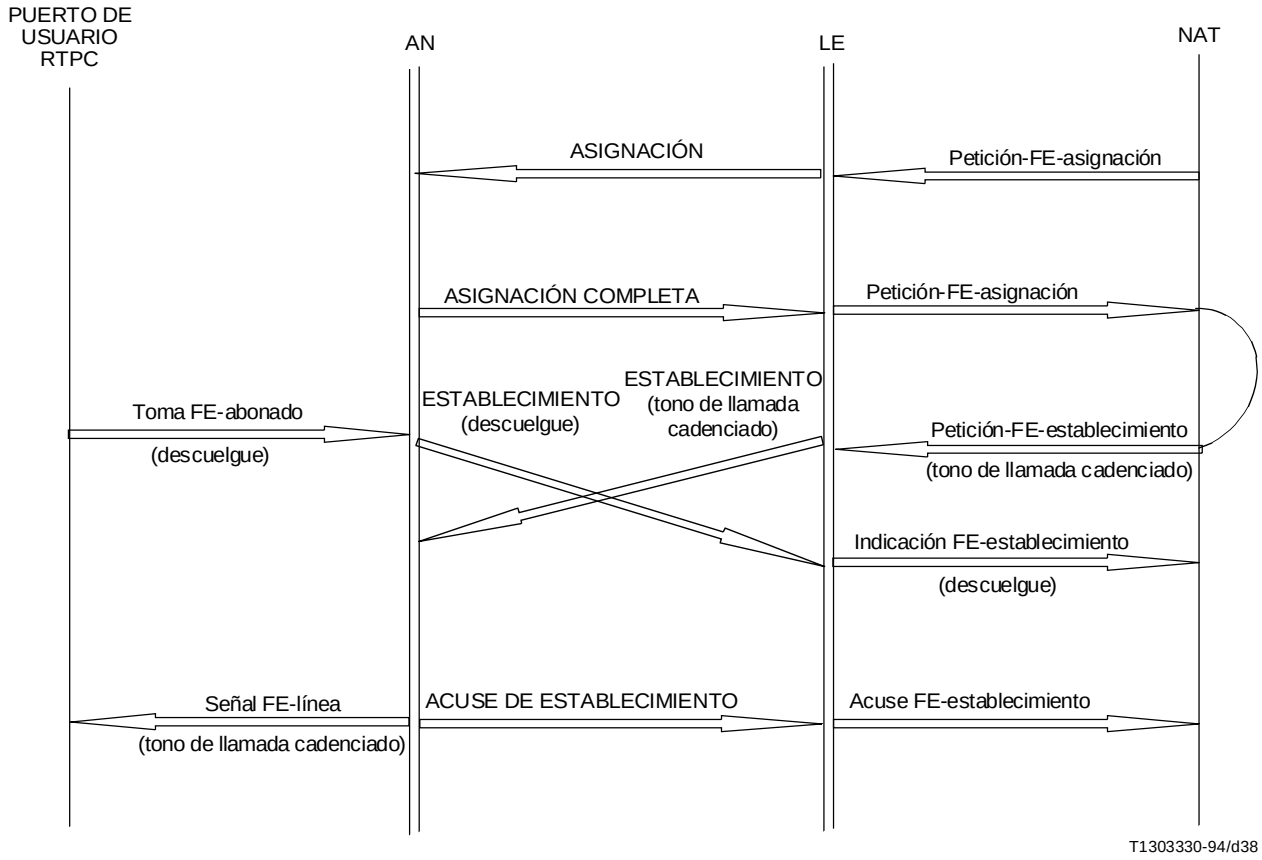


FIGURA K.14/G.965

Colisión de llamada RTPC, la llamada de terminación tiene prioridad

K.9.4 Liberación de llamada

K.9.4.1 Liberación de llamada iniciada por el abonado

En la Figura K.15 aparece el diagrama de flechas que muestra un ejemplo de la interacción del protocolo BCC con el protocolo RTPC para el caso de liberación de llamada iniciada por el abonado.

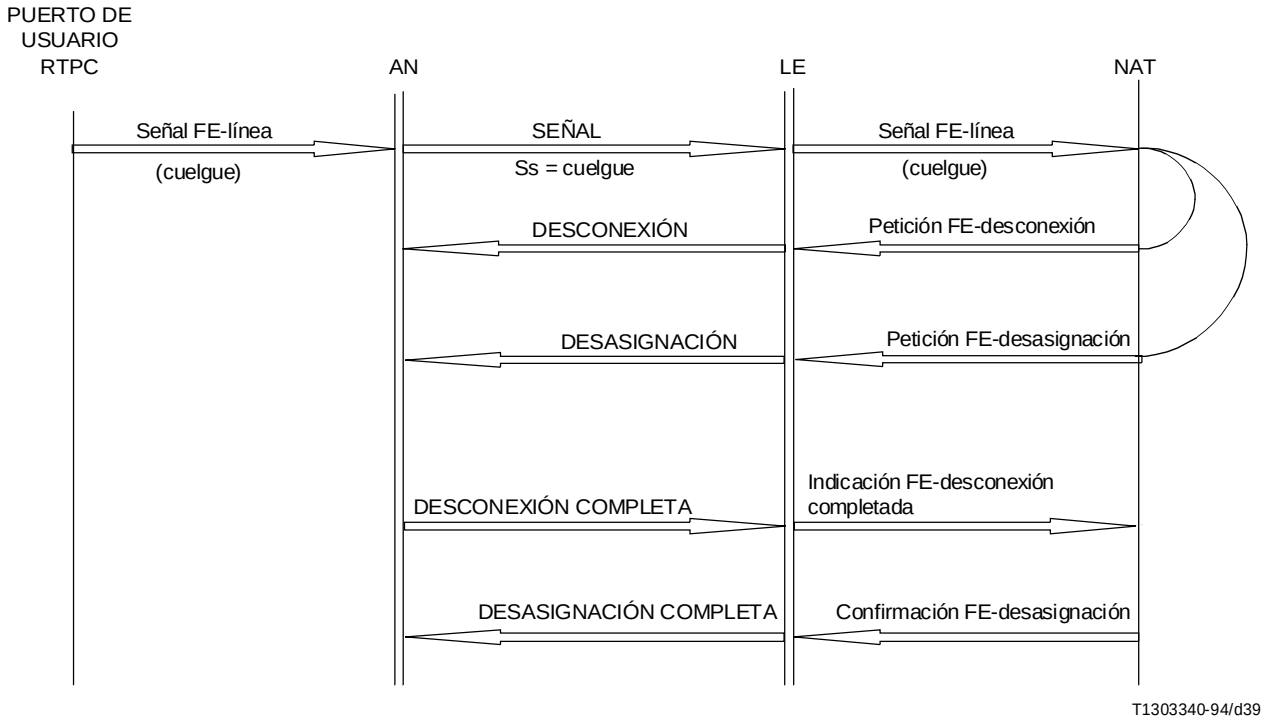


FIGURA K.15/G.965

Liberación de llamada RTPC iniciada por el abonado

K.9.4.2 Liberación de llamada iniciada por la red

En la Figura K.16 aparece el diagrama de flechas que muestra un ejemplo de interacción del protocolo BCC con el protocolo RTPC en el caso de liberación de llamada iniciada por la red.

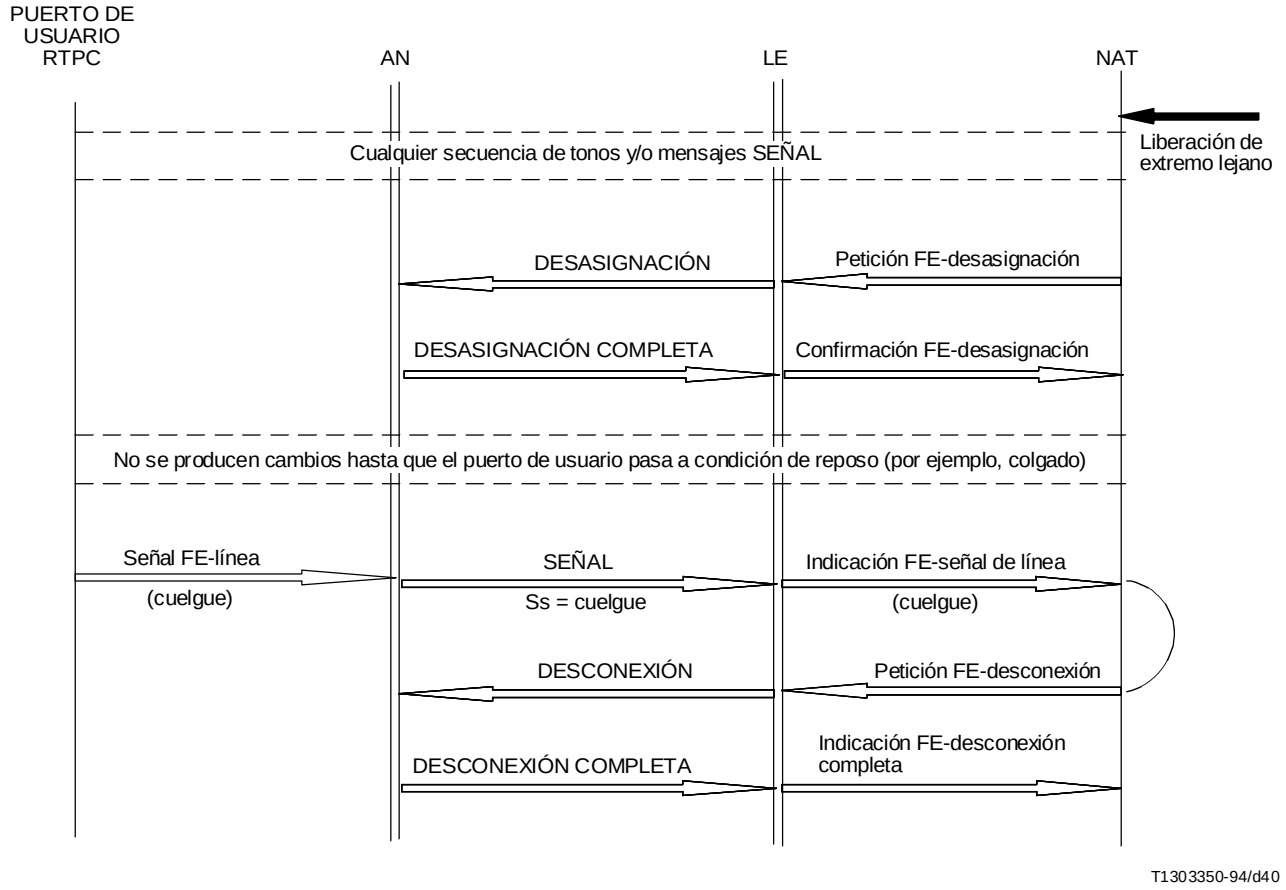


FIGURA K.16/G.965

Liberación de llamada RTPC iniciada por la red

Apéndice I

Bibliografía

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

– Recomendación G.921 del CCITT, *Secciones digitales basadas en la jerarquía de 2048 kbit/s*.

– Recomendación O.162 del CCITT, *Aparato para efectuar la supervisión en servicio de las señales de 2048, 8448, 34 368 y 139 264 kbit/s*.

– Recomendación Q.922 del CCITT, *Especificación de la capa de enlace de datos de la RDSI para servicios portadores en modo trama*.

– Recomendación UIT-T I.603, *Mantenimiento del acceso y la instalación de abonados de la RDSI*.

– Recomendación UIT-T G.961, *Acceso a velocidad primaria RDSI, sistema de transmisión digital por líneas locales metálicas*.