UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.323

Anexo R

(07/2001)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Sistemas y equipos terminales para los servicios audiovisuales

---

Sistemas de comunicación multimedios basados en paquetes

Anexo R: Métodos de robustez para entidades H.323

Recomendación UIT-T H.323 – Anexo R

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
SISTEMAS Y EQUIPOS TERMINALES PARA LOS SERVICIOS AUDIOVISUALES	**H.300–H.399**
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	H.450–H.499

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

Recomendación UIT-T H.323

Sistemas de comunicación multimedios basados en paquetes

ANEXO R

Métodos de robustez para entidades H.323

Resumen

Este anexo especifica los métodos que pueden ser utilizados por entidades H.323 para implementar robustez o tolerancia a un conjunto específico de fallos, y especifica métodos de recuperación de canales de señalización de llamada (UIT-T H.225.0) y de señalización de control de llamada (UIT-T H.245). El RAS (UIT-T H.225.0), que no requiere conexión ni recuperación, mas sí registro en un controlador de acceso alternativo, se trata en otro lugar, por lo que no se describe en este anexo. La recuperación de las relaciones de servicio del anexo G queda en estudio.

Orígenes

El anexo R a la Recomendación UIT-T H.323, preparado por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobado por el procedimiento de la Resolución 1 de la AMNT el 29 de julio de 2001.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

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

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2002

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
Anexo R – Métodos de robustez para entidades H.323		1
R.1	Introducción y alcance	1
R.2	Referencias normativas	1
R.3	Definiciones	2
R.4	Abreviaturas	2
R.5	Sinopsis de los dos métodos	3
	R.5.1 Método A: Recuperación de estado a través de los vecinos	3
	R.5.2 Método B: Recuperación de estado a través de un depositario compartido	3
	R.5.3 Comparación	4
R.6	Mecanismos comunes	4
	R.6.1 Detección de conexión basada en TCP perdida	4
	R.6.2 Tratamiento de fallo de protocolo	5
	R.6.3 Detección de fallos – Mantener vivo (*keepAlive*)	5
	R.6.4 Dirección de transporte y conexiones restablecidas	5
	R.6.5 Soporte de la situación extendida	6
R.7	Método A: Recuperación de estado a través de los vecinos	6
	R.7.1 Introducción	6
	R.7.2 Alcance	7
	R.7.3 El procedimiento de robustez	7
	R.7.4 Diagrama SDL para la máquina de estados del método A	9
R.8	Método B: Recuperación de estado a través de un depositario compartido	11
	R.8.1 Plataforma tolerante a los fallos	11
	R.8.2 Conglomerado tolerante a los fallos	11
	R.8.3 Restablecimiento de conexión de señalización de llamada	11
	R.8.4 Restablecimiento de conexión H.245	12
	R.8.5 Datos compartidos a través de un depositario compartido	12
	R.8.6 Puntos de verificación	13
R.9	Interfuncionamiento entre métodos de robustez	13
R.10	Procedimientos para la recuperación	13
R.11	Utilización de datos genéricos (GenericData)	14
	R.11.1 Utilización de GenericData en los mensajes H.225.0	14
R.12	Nota Informativa 1: Antecedentes de los métodos de robustez	15
	R.12.1 Tipos de métodos de robustez	15
	R.12.2 Entidades robustas	15
	R.12.3 Ámbito de un sistema robusto	16
	R.12.4 Terminación y fallos de sistema	16

Página

R.13 Nota Informativa 2: Compartición de estado de llamada entre una entidad y su par de seguridad 18

R.13.1 Memoria compartida 18

R.13.2 Disco compartido 18

R.13.3 Paso de mensaje 18

Recomendación UIT-T H.323

Sistemas de comunicación multimedios basados en paquetes

ANEXO R

Métodos de robustez para entidades H.323

R.1 Introducción y alcance

Este anexo especifica los métodos que pueden ser utilizados por entidades H.323 para implementar robustez o tolerancia a un conjunto específico de fallos, y especifica métodos de recuperación de canales de señalización de llamada (UIT-T H.225.0) y de señalización de control de llamada (UIT-T H.245). El RAS (UIT-T H.225.0), que no requiere conexión ni recuperación, mas sí registro en un controlador de acceso alternativo, se trata en otro lugar, por lo que no se describe en este anexo. La recuperación de las relaciones de servicio del anexo G queda en estudio.

Las llamadas H.323 requieren la cooperación de dos o más entidades H.323. La información de estado de llamada es distribuida entre las diversas entidades que intervienen en la llamada. La señalización de llamada puede depender de que haya conexiones persistentes entre algunas de las entidades que intervienen. Si una entidad falla y no posee un par de seguridad, podría resultar imposible establecer nuevas llamadas. Si una entidad que interviene en una llamada activa falla y no posee un par de seguridad, o ese par no tiene un método de recuperar suficiente información de estado de llamada, podría resultar imposible continuar la llamada. La Recomendación H.323 proporciona cierto soporte para la construcción de sistemas robustos, pero los mecanismos se hallan repartidos en todo este anexo y se indican pocos procedimientos, o ninguno, para utilizarlos.

Este anexo describe dos métodos alternativos compuestos de mecanismos, así como procedimientos para utilizarlos en la construcción de sistemas que puedan recuperarse de un conjunto importante de fallos específicos. Un método es más apropiado para sistemas de pequeña escala, utiliza entidades más simples y no recupera tanta información de estado de llamada. El otro método es adecuado para sistemas de gran escala, y puede recuperar tanta información como se desee, pero requiere entidades más complejas. Ambos métodos comparten varios mecanismos y pueden utilizarse simultáneamente en diferentes partes de un sistema.

R.2 Referencias normativas

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

[1] UIT-T H.225.0 (2000), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

[2] UIT-T H.323 (2000), *Sistemas de comunicación multimedios basados en paquetes*.

[3] UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

[4] UIT-T X.680 (1997), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

R.3 Definiciones

Además de los términos definidos en UIT-T H.323, se definen los términos siguientes.

R.3.1 entidad de seguridad o par de seguridad: Par de una entidad que puede asumir las funciones de la entidad si ésta falla.

R.3.2 entidades pares: Dos entidades del mismo tipo en un sistema H.323, por ejemplo, dos controladores de acceso. Las dos entidades pueden cooperar en una llamada (por ejemplo, los controladores de acceso de origen y de terminación en una señalización de llamada encaminada por controlador de acceso) o una de las dos puede proporcionar seguridad a la otra.

R.3.3 métodos de robustez: Procedimientos y mecanismos que permiten la recuperación después del fallo de una o más entidades H.323. La amplitud de la recuperación varía de un método a otro y puede incluir mantenimiento de llamadas activas en estado estable o solamente la posibilidad de efectuar nuevas llamadas. Los métodos descritos en el presente anexo suelen poder mantener las llamadas activas.

R.3.4 vecino de señalización: Otras entidades con las que una entidad determinada tiene conexiones directas de señalización de llamada o de control de llamada en una llamada determinada. Por ejemplo, un controlador de acceso que utiliza el modelo de encaminamiento por controlador de acceso puede tener una conexión directa de señalización de llamada en una llamada determinada a una pasarela y otro controlador de acceso. Estas otras dos entidades serían vecinos de señalización del controlador de acceso en esa llamada.

R.3.5 llamadas estables: Una llamada se considera estable o en un estado estable después de que se ha enviado o recibido Conexión y se han establecido canales de medios en ambos sentidos (mediante procedimientos H.245 o de conexión rápida). Una llamada es inestable cuando se ha enviado o recibido Liberación completa. Ciertas instrucciones de Facilidad utilizadas para cambiar conexiones de señalización de llamada pueden también hacer que una llamada se considere inestable. Esta versión de esta Recomendación ofrece métodos para mantener únicamente llamadas estables durante la recuperación.

R.3.6 entidades en tándem: Dos o más entidades pares, todas las cuales menos una actúan como entidades de seguridad para una entidad activa.

R.3.7 entidad virtual: Dos o más entidades par estrechamente acopladas que aparecen colectivamente como una sola entidad al resto de un sistema H.323 mientras se produce la recuperación tras un fallo.

R.4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

CRV Valor de referencia de llamada (*call reference value*)

GK Controlador de acceso (*gatekeeper*)

GW Pasarela (*gateway*)

RAS Registro, admisión y situación (*registration, admission and status*)

SCTP Protocolo de transmisión de control de trenes (*stream control transmission protocol*) (IETF RFC 2960) (para información solamente)

SDL Lenguaje de especificación y descripción (*specification and description language*)

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

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

R.5 Sinopsis de los dos métodos

En esta versión del anexo se ofrecen dos métodos de robustez.

El problema que se pretende resolver es la recuperación de un fallo de entidad H.323 que falla. El objetivo es mantener tantas llamadas activas como sea posible. Como mínimo se desea mantener todas las llamadas en un estado "estable". Las llamadas aún no completamente conectadas o que se encuentran en proceso de desconexión pueden perderse. También se persigue el objetivo de conservar la información de facturación más pertinente, como la hora de comienzo y de fin de la llamada, etc., incluso si esta información es mantenida en la entidad que falla (por ejemplo, el controlador de acceso de encaminamiento).

Se supone que la entidad que falla tiene una o varias entidades de seguridad designadas, aunque la solución a pequeña escala puede permitir la recuperación cuando la entidad que falla vuelve rápidamente al servicio. Deben resolverse dos problemas básicos para recuperar señalización de llamadas activas:

1) Redireccionamiento y restablecimiento de señalización a la entidad de seguridad.
2) La entidad de seguridad debe recuperar suficiente información de estado de llamada de la que residía en la entidad que falla.

Los dos métodos se distinguen sobre todo por el método de recuperar información de estado acerca de las llamadas activas y por la cantidad de información recuperada.

R.5.1 Método A: Recuperación de estado a través de los vecinos

En el método A, cada entidad conoce las direcciones de transporte de señalización de las entidades de seguridad de cada vecino de señalización ascendente y descendente. Cuando las entidades se enteran del fallo de su vecino de señalización ascendente o descendente, intentan conectarse a una de las entidades de seguridad. La entidad de seguridad recupera el estado mínimo de llamada por su vecino de señalización utilizando los mensajes Estado e Indagación de estado (ampliados con campos adicionales). Adviértase que en algunos casos puede ser necesario que el vecino pregunte a su vecino el estado de llamada si no ha mantenido localmente toda la información necesaria (por ejemplo, un controlador de acceso de encaminamiento puede tener información de canal lógico abierto *caché*).

El estado de llamada recuperado es suficiente para continuar la llamada (envío de señalización de llamada y de señalización de control de llamada y conocimiento de canales lógicos abierto) pero no para permitir a la entidad recuperada participar en la facturación y en algunos otros servicios.

R.5.2 Método B: Recuperación de estado a través de un depositario compartido

La segunda arquitectura se basa en una seudoentidad tolerante a los fallos. Puede implementarse:

1) Utilizando una plataforma o sistema operativo tolerantes a los fallos.
2) Un fondo común de entidades no tolerantes a los fallos y que compartan información de estado de llamada mediante memoria compartida, discos compartidos, o a través de mensajes. El mecanismo de compartición no se especifica en esta Recomendación.

Las entidades reales en esta seudoentidad tolerante a los fallos deben compartir suficiente información de estado con sus entidades pares para permitir la recuperación del estado de llamada deseado sin ayuda alguna de sus vecinos de señalización. Esta Recomendación definirá las entidades de información mínimas que deben ser compartidas. Toda información adicional que se desea que sea recuperable puede ser compartida. Hay que señalar que este método exigirá que todas las entidades del fondo común que constituyen la seudoentidad provengan del mismo vendedor, ya que el mecanismo de compartición no está normalizado. La comisión sugeriría una o dos posibles soluciones y consideraría recomendar un mecanismo de compartición normalizado en las versiones de la H.323 superiores a 4.

Más adelante se darán más detalles de esta arquitectura.

R.5.3 Comparación

Cada una de estas dos arquitecturas presenta ventajas, lo cual hace que la elección diste de ser evidente. Algunos de los aspectos a tener en cuenta son:

El método de recuperación a través de los vecinos:

1) Permite entidades más simples.
2) Añade menos tara antes de un fallo (aunque necesita mensajes Mantener vivo en algunos casos).

Pero:

1) Requiere más cambios en los mensajes H.323.
2) Hace la recuperación algo más lenta (debido a los mensajes Estado e Indagación de estado).
3) No es escalable; sólo es adecuado para sistemas de pequeña escala.

El método del depositario compartido:

1) Oculta la mayor parte del proceso de recuperación de la entidad H.323, por lo cual requiere menos cambios en los mensajes existentes.
2) Hace la recuperación más rápida.
3) Permite el uso futuro de protocolos de mantenimiento de estado que pueden implementarse por debajo de la capa de aplicación H.323 (véase la Nota Informativa 2 en R.13).
4) Puede soportar recuperación de información de facturación y otra información de estado deseada.

Pero:

1) Añade considerable tara a toda la señalización (antes del fallo).
2) Requiere entidades o seudoentidades más complejas.

R.6 Mecanismos comunes

Los dos métodos comparten varios mecanismos comunes.

R.6.1 Detección de conexión basada en TCP perdida

En caso de fallo de red, el primer intento "automático" se haría a nivel de protocolos de encaminamiento IP. Si no tiene éxito, se informará del fallo TCP a ambos extremos (la entidad y su vecino de señalización, por ejemplo, controlador de acceso y punto extremo). Tanto un fallo de red como un fallo del vecino de señalización aparecerá como un fallo TCP.

Cuando se estableció la comunicación, se determinó si el vecino de la entidad soportaba procedimientos de robustez.

En caso de que uno de los extremos no soporte el procedimiento de robustez definido, se sugiere liberar la llamada debido a estado de fallo de conexión TCP.

En el lado punto extremo, en caso de que ambos lados soporten el procedimiento de robustez, se sugiere mantener un tiempo muerto para que el procedimiento de robustez pueda ser iniciado por el otro lado. Este tiempo es necesario para tratar un posible problema de conectividad de red. Una vez expirado este plazo, deben liberarse los recursos internos (consumidos por la llamada).

R.6.2 Tratamiento de fallo de protocolo

Para las entidades que utilizan este anexo, si se produce un fallo de protocolo en un canal de control y ambos vecinos de señalización soportan la robustez, el canal y todos los canales lógicos asociados **no** se cierran (al contrario de la cláusula 8.6 de H.323). En su lugar, se intentan los procedimientos de recuperación de este anexo.

R.6.3 Detección de fallos – Mantener vivo (*keepAlive*)

Sin un mecanismo keepAlive, un fallo de entidad o de conexión de señalización se conocerá solamente cuando se utilice la conexión. El anexo E proporciona un mecanismo keepAlive para detectar el fallo aun con poco tráfico. El mecanismo keepAlive del TCP tiene un tiempo muerto demasiado largo para ser de utilidad y, por tanto, con un fallo TCP podría no ser detectado durante largo tiempo en condiciones de bajo tráfico enviado a la entidad que falla. Nuestra solución de pequeña escala depende de que el fallo sea detectado por ambos vecinos de señalización (las conexiones se establecen siempre desde el vecino hacia la entidad recuperada), por lo que necesitamos mensajes keepAlive a nivel H.323 que puedan utilizarse con conexiones TCP. Hay mensajes keepAlive que pueden opcionalmente utilizarse en H.245. Especificaríamos que se utilicen periódicamente mensajes Estado/Indagación de estado en las conexiones TCP para proporcionar este mecanismo keepAlive. Aunque éste es un aspecto común, veremos que es solamente un problema importante en el método A, de recuperación de estado a través de los vecinos.

La entidad más próxima a la parte llamada (lado destino de la conexión o lado que utiliza la bandera de referencia de llamada = 1 en el CRV utilizado en la conexión – véase en UIT-T Q.931 la definición de la bandera de referencia de llamada) enviará periódicamente Indagación de estado (éste es el sentido de menor tráfico durante las llamadas establecidas). El periodo debe variar aleatoriamente desde un valor máximo configurable hasta la mitad de ese valor a fin de evitar la congestión. Dos segundos es el máximo por defecto recomendado a fin de permitir la detección del fallo antes del vencimiento del plazo de otros mensajes. El valor máximo se incluirá en la Indagación de estado como el tiempo hasta en directo (timeToLive), para que el recibiente pueda también supervisar el fallo sin necesidad de un intercambio adicional de Indagación de estado/Estado en sentido opuesto. El sistema recibiente necesitará solamente mantener un temporizador que utilice el valor máximo indicado como tiempo muerto.

Cuando se utilizan canales multiplexados, no es necesario enviar Indagación de estado/Estado para cada llamada señalizada en el canal. Se aplica a todas las llamadas que utilizan el canal un mensaje de Indagación de estado o Estado con un CRV IE igual a 0 (cero) y con el campo de identificador de la llamada igual a 0 (cero).

Los mensajes keepAlive, especialmente al nivel H.323, pueden añadir considerable tara de señalización. Pero adviértase que sólo el método A utiliza estos mensajes con conexiones TCP y que el método A es para el caso de pequeña escala en el que el número de conexiones por entidad es bajo. Para minimizar la tara debe evitarse la utilización del TCP. StatusInquiry/Status keepAlives **no** se necesitan en nuestra solución de gran escala.

R.6.4 Dirección de transporte y conexiones restablecidas

Estas dos soluciones (con la posible excepción de alguna de plataforma tolerante a los fallos) deben ocuparse de la recuperación del canal de señalización utilizando una dirección de transporte de seguridad. Éstas deben ser intercambiadas cuando se establece la señalización de llamada, utilizando los campos backupCallSignalAddresses en los mensajes Establecimiento y Conexión. Una entidad envía la dirección de señalización de llamada de su par de seguridad en Establecimiento y en Conexión. Una entidad recibe la dirección de señalización de llamada de la entidad de seguridad de su vecino del lado origen cuando recibe Establecimiento, y de su vecino del lado terminación cuando recibe Conexión.

R.6.4.1 Establecimiento de una nueva conexión TCP

Una entidad que detecte pérdida de un canal de señalización de llamada con un vecino de señalización, tratará de restablecer este canal utilizando la dirección de transporte de seguridad. Alternativamente, la entidad que detecta fallo puede intentar sondear a su vecino de señalización original utilizando otros métodos que están fuera del alcance de esta Recomendación (por ejemplo, ping) y, si cree que el vecino de señalización original puede ser utilizable, puede tratar de restablecer el canal hacia aquél antes de ensayar con la dirección de transporte de seguridad. Los implementadores que escojan esta opción deben saber que intentar establecer una conexión TCP con una entidad que no responde puede causar retardos importantes.

El canal de señalización de llamada restablecido asumirá el estado del anterior –no se comporta como un nuevo canal (**no** comenzará con Establecimiento). Véanse más adelante detalles a continuación para asegurar la sincronización de estado entre vecinos de señalización.

PARA INFORMACIÓN – Una alternativa es utilizar el SCTP para el transporte en lugar del TCP. Los canales SCTP se asocian con una lista de direcciones de transporte alternativas que pueden ser utilizadas si es necesario para mantener el canal sin intervención de la capa de aplicación. La Nota Informativa 2 de R.13 contiene más información acerca de la utilización del SCTP.

R.6.4.2 Asociación entre la llamada y la nueva conexión TCP

La asociación entre la llamada y la nueva conexión TCP (en el lado punto extremo) se hará mediante la recuperación del valor del identificador de llamada (callIdentifier) a partir del mensaje recibido en la nueva conexión TCP.

R.6.4.3 Cierre de una antigua conexión TCP

Una vez abierta la nueva conexión, podría haber dos conexiones TCP abiertas pertenecientes a la misma llamada en el lado que no falló. Hay dos opciones en este caso:

1) La conexión TCP se perdió después de enviarse (y recibirse) el mensaje ESTABLECIMIENTO. En este caso el lado que no falló identificará la situación y cerrará la conexión. Esto debe realizarse detectando un identificador de llamada idéntico para ambas conexiones.

2) La conexión TCP se perdió antes de transferirse el primer mensaje.

En ese caso, el lado que no falló no tiene ningún modo de distinguir entre la primera conexión TCP (antigua) y la segunda (nueva). Esto puede resolverse por un procedimiento que permita al lado receptor cerrar una conexión si ha estado abierta durante un tiempo sin que se haya recibido por ella ningún mensaje en un plazo previamente definido. (Este procedimiento no se describe en este anexo.)

R.6.5 Soporte de la situación extendida

Para mejorar la interoperabilidad entre los dos métodos, todas las entidades que soportan la robustez soportarán el mensaje Estado ampliado que incluye el campo comienzo rápido (fastStart). Esto permitirá a una entidad con un depositario compartido cooperar con un vecino que requiera Estado para la recuperación de estado.

R.7 Método A: Recuperación de estado a través de los vecinos

R.7.1 Introducción

Actualmente UIT-T H.323 y UIT-T H.225.0 no definen explícitamente los procedimientos para la detección y la consiguiente recuperación de un fallo de conexión. El objetivo de este método es introducir un procedimiento para:

- la detección de fallo de conexión basada en TCP;

- la sincronización entre los dos lados de la conexión en términos de estado de llamada;
- la definición del comportamiento recomendado en cada lado a fin de renovar la conexión de señalización de llamada y proceder con la llamada como sea normal en cada estado de la llamada.

La principal motivación para mantener una llamada (cuando se ha perdido una conexión) se presenta en situaciones en donde un controlador de acceso, que trata un número considerable de llamadas, falla debido a un problema de hardware o de software. En este caso, puede transferirse un control a un controlador de acceso de reserva (que puede conservar toda la información acerca de las llamadas mediante alguna base de datos común). El procedimiento definido y presentado en este anexo se refiere al caso de fallo del controlador de acceso y hace posible que las llamadas gestionadas continúen sin interrupción alguna.

Este procedimiento no trata todos los aspectos de fallo y recuperación de conexión basada en TCP en otros casos y topologías posibles. No obstante, en el futuro podrán tratarse casos adicionales de manera similar.

R.7.2 Alcance

Esta propuesta trata solamente las conexiones basadas en TCP (canales de señalización de llamada Q.931 y de control de llamada H.245). Los canales UDP (RAS) no se tratarán puesto que sus situaciones de fallo ya se han tratado en el mecanismo de reintentos definido para canales UDP.

R.7.3 El procedimiento de robustez

Después de un fallo, la entidad H.323 restablecerá la conexión de señalización de llamada y enviará los mensajes INDAGACIÓN DE ESTADO y ESTADO a la otra entidad H.323. La otra entidad H.323 responderá con mensajes ESTADO, alcanzándose así un estado en el que ambos lados conocen el estado de llamada del otro. La conexión de señalización de llamada debe establecerse a una de las entradas de **backupCallSignalAddresses** en un orden de preferencia definido por el orden de los elementos en la estructura **backupCallSignalAddresses**.

En el caso de que ambas entidades inicien simultáneamente la conexión de señalización de llamada, la entidad con el menor valor numérico del TransportAddress utilizado a partir de **backupCallSignalAddresses** cerrará la conexión TPC que abrió y utilizará la conexión abierta por el otro punto extremo. Para comparar los valores numéricos de TransportAddress de **backupCallSignalAddresses**, cada octeto de la dirección se comparará individualmente empezando por el primer octeto de la CADENA DE OCTETOS y continuando de izquierda a derecha en la CADENA DE OCTETOS hasta que se encuentren valores diferentes. La comparación se efectuará con el elemento de dirección de capa de red del TransportAddress de **backupCallSignalAddresses**, y si se ve que es igual, con el elemento de dirección (puerto) de transporte. Véase la figura R.1.

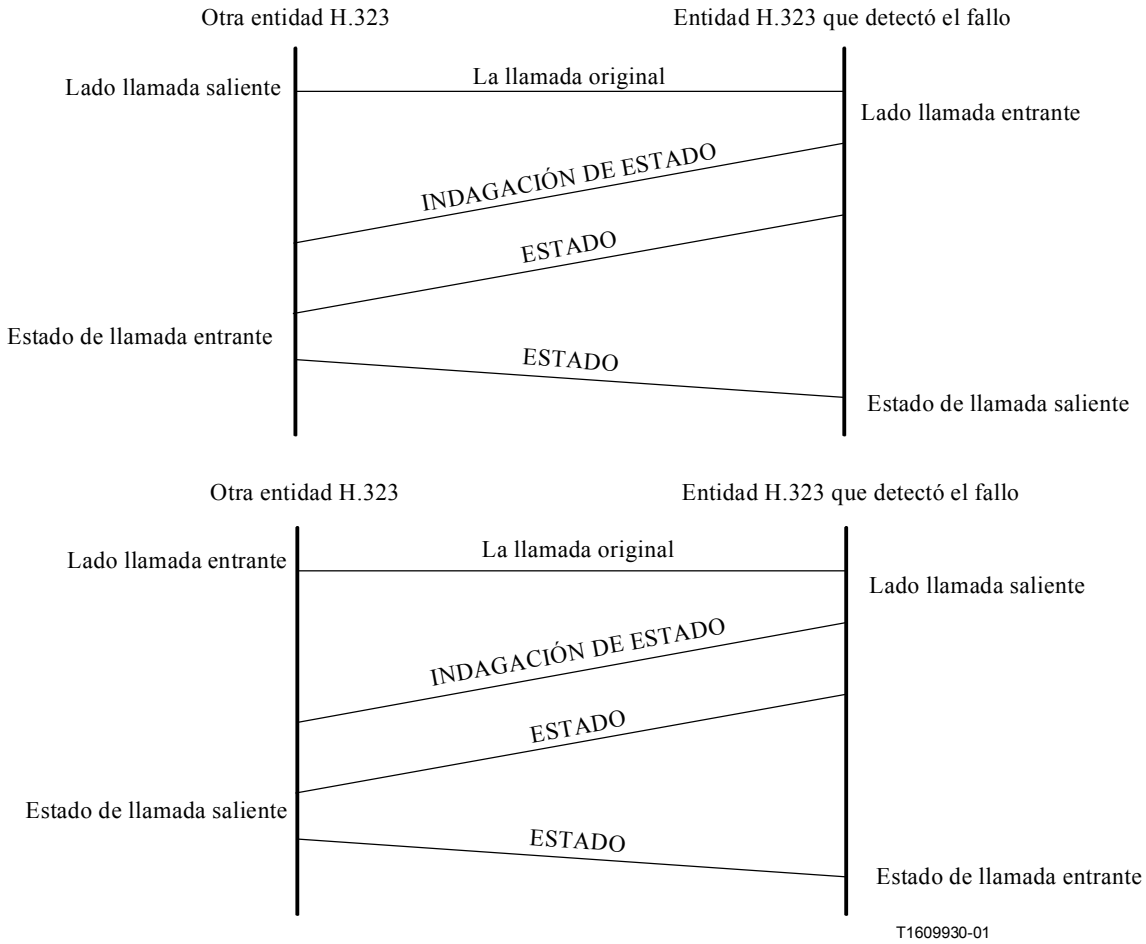


Figura R.1/H.323 – Procedimiento de robustez

Se cerrarán todas las conexiones anteriores que pudieran aún estar abiertas para la llamada, lo cual se aplica a la conexión de señalización de llamada y a la conexión de control de llamada.

Para facilitar la sincronización del estado de canales lógicos, pueden utilizarse los nuevos campos **IncludeFastStart** en los mensajes INDAGACIÓN DE ESTADO y **RobustnessFastStart** en ESTADO. El emisor del mensaje ESTADO debe incluir el campo **RobustnessFastStart** que contiene los canales entonces activos de recepción y transmisión con las direcciones de recepción para trenes de medios y de control de medios. El emisor de un mensaje INDAGACIÓN DE ESTADO puede solicitar la inclusión del campo **RobustnessFastStart** en el mensaje de ESTADO fijando el valor **IncludeFastStart** a TRUE.

Si una entidad intermedia necesita sincronizar el estado de canal lógico, debe enviar el mensaje INDAGACIÓN DE ESTADO a uno de los tramos de llamada, debe esperar el mensaje ESTADO con un campo comienzo rápido, debe emitir los mensajes ESTADO e INDAGACIÓN DE ESTADO al otro tramo de la llamada, debe esperar el mensaje ESTADO que contenga la información de canal lógico del segundo tramo y debe enviar el mensaje ESTADO al primer tramo de la llamada.

Este procedimiento se utiliza para sincronizar los estados de los canales lógicos abiertos que se abrieron mediante el procedimiento de comienzo rápido y de establecimiento de canal lógico H.245.

En las situaciones en que la llamada no haya alcanzado el estado activo antes del fallo, la llamada debe abandonarse.

R.7.4 Diagrama SDL para la máquina de estados del método A

Véase la figura R.2.

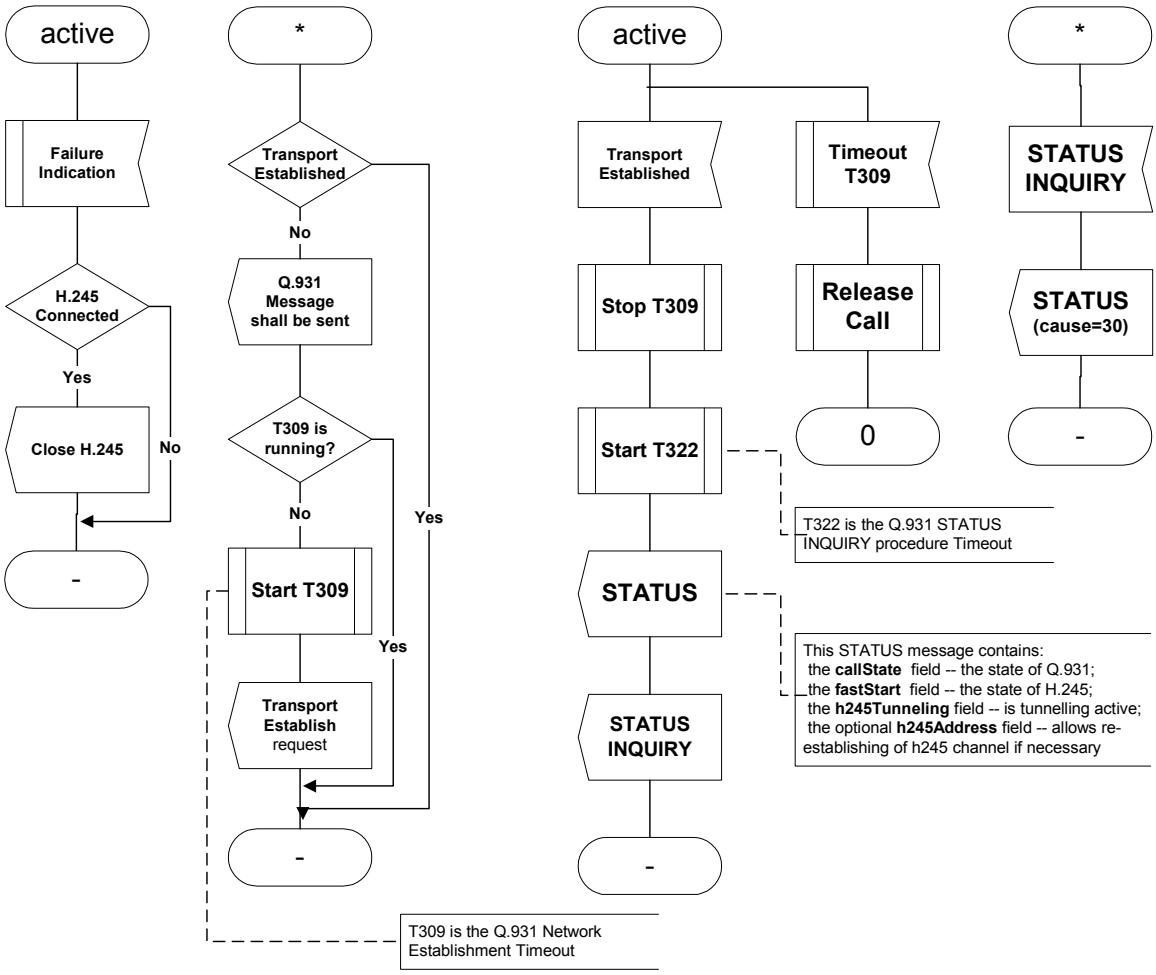


Figura R.2/H.323 – Máquina de estados del método A (*hoja 1 de 2*)

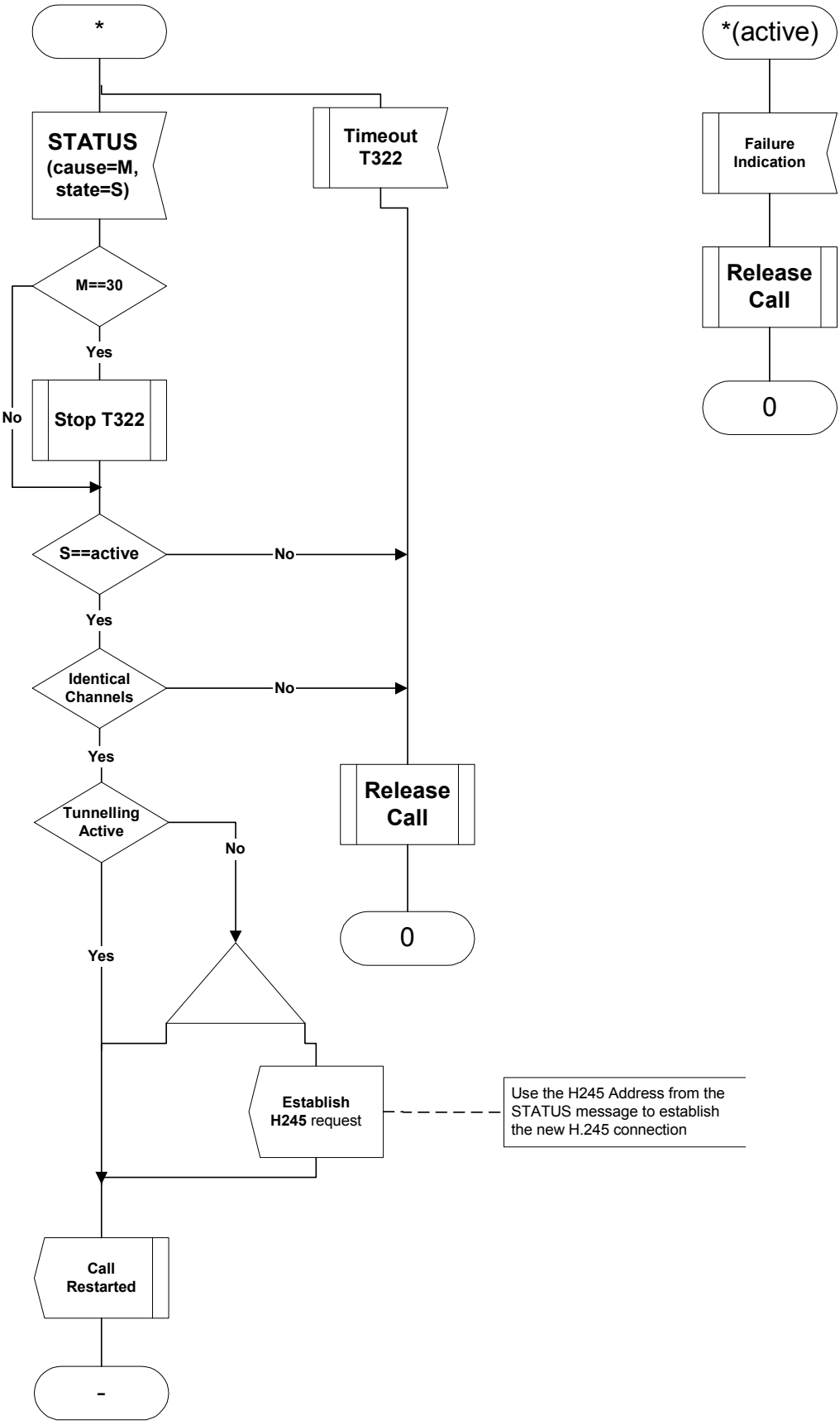


Figura R.2/H.323 – Máquina de estados del método A (*hoja 2 de 2*)

R.8 Método B: Recuperación de estado a través de un depositario compartido

Este método depende de una entidad o seudoentidad tolerante a los fallos y (si la entidad de seguridad requiere una dirección de señalización diferente) de un mecanismo para restablecer la señalización de llamada en la entidad de seguridad. Hay varias maneras de hacerlo. El mecanismo tolerante a los fallos no se normalizará en esta versión de esta Recomendación, pero sugeriremos algunas soluciones. Podemos recomendar la normalización de la solución en una versión futura de esta Recomendación. Existen algunos protocolos IETF emergentes que pueden ayudar a resolver este problema, pero aún no se encuentran en un estado tal que puedan ser referenciados por H.323v4 (noviembre de 2000).

R.8.1 Plataforma tolerante a los fallos

Una solución es implementar la entidad robusta en una plataforma tolerante a los fallos que utilice hardware y soporte OS. Esta solución haría la recuperación de estado completamente transparente a la H.323. Si la plataforma también mantiene una dirección de transporte constante, es entonces una entidad virtual tolerante a los fallos, el canal de señalización no fallará y no se necesitan procedimientos a nivel de aplicación. Si cambia la dirección de transporte, se necesitará el mecanismo de esta cláusula.

R.8.2 Conglomerado tolerante a los fallos

Otra solución es establecer un conglomerado (dos o más) de entidades tándem no tolerantes a los fallos, que se comporten colectivamente como una seudoentidad tolerante a los fallos. Las entidades del conglomerado se arreglarían para compartir suficiente información de estado de llamada especificada para permitir a un par asumir el mando en caso de fallo de la entidad activa. Posibles soluciones podrían ser:

1) activo/reserva ("1+1");
2) reserva única compartida por varias entidades activas (la entidad de reserva comparte información de estado de compartición de reserva con cada entidad activa a la que pudiera sustituir) ("N+1");
3) y otras configuraciones.

Aunque la información de estado es compartida, lo que permite al conglomerado aparecer como una entidad virtual tolerante a los fallos, no será posible mantener una dirección de transporte de señalización de llamada constante, por lo cual, debe utilizarse uno de los mecanismos de R.8.3 para restablecer el canal de señalización de llamada.

Un problema clave del modelo de conglomerado es cómo compartir el estado. La información de estado debe ser sincronizada en momentos clave de la llamada, de modo que el sistema pueda con seguridad recurrir a ellos. Estos momentos se denominarán *puntos de verificación* (*checkpoints*). Esta Recomendación especifica los puntos de verificación y los datos mínimos que deben ser compartidos. En esta versión de esta Recomendación no sugerimos una solución normalizada de la compartición, pero en la Nota Informativa 2 de R.13 consideraremos varias soluciones para ilustrar las ventajas prácticas de este modelo.

R.8.3 Restablecimiento de conexión de señalización de llamada

La compartición de direcciones de señalización de seguridad es la misma que en el método A. El restablecimiento de conexiones de señalización de llamada es similar pero presenta diferencias, pues la entidad de seguridad tiene suficiente información para restablecer la conexión en el segundo lado en lugar de esperar a que el otro vecino también detecte el fallo.

Cuando una entidad de seguridad toma el lugar de un par que ha fallado y recibe un mensaje en una nueva conexión, recuperará el estado de llamada [utilizando como clave el identificador de llamada (callIdentifier)], lo cual permitirá continuar soportando la llamada, incluida la señalización de encaminamiento, mantener la información de facturación, etc. Una entidad que detecte un fallo no

restablecerá la conexión hasta que tenga un mensaje que enviar por la conexión. La entidad de seguridad tendrá canales nuevos para cada llamada utilizada por el par que falla, a menos que se hayan utilizado canales multiplexados. La política de restablecer solamente cuando sea necesario repartirá los restablecimientos en el tiempo.

La posibilidad de retrasar el restablecimiento hasta que se necesite el canal para un mensaje, y el hecho de que la entidad de seguridad posea suficiente información para establecer el nuevo canal en el otro lado, significa que no es necesario un mecanismo keepAlive en el método B.

Como tanto la entidad recuperada como su vecino de señalización pueden restablecer la conexión, existe una condición potencial de competición en velocidad, pero evitamos la necesidad de mensajes de mantenimiento en activo con las conexiones TCP. Como el tráfico es mayor en un sentido que en el otro y el restablecimiento se produce solamente cuando existe tráfico de mensaje, la condición de competición en velocidad será rara. Podemos resolver la condición de competición por los mismos métodos utilizados en el establecimiento de canal H.245. La entidad que tenga el menor valor numérico de la dirección h245 cerrará la conexión TCP que abrió y utilizará la conexión abierta por el otro punto extremo.

Para los canales de señalización multiplexados, la detección de un fallo en cualquier llamada implicará fallo del canal. Cuando se establece un nuevo canal, se utilizará para el mismo conjunto de llamadas que el canal que falla. Adviértase que esto implica que la lista de llamadas que comparten un canal debe formar parte de los datos compartidos entre una entidad y su entidad o entidades de seguridad, o entre entidades a través del depositario compartido. Después de un fallo, se restablece el canal multiplexado cuando hay un mensaje que enviar para cualesquiera de las llamadas que comparten el canal. Existe una condición de competición de velocidad similar a esa en los canales no multiplexados. Si se ve que dos canales de señalización tratan el mismo conjunto de llamadas o llamadas del mismo conjunto, se abandonará una conexión.

Si una entidad recibe una nueva conexión de señalización que incluye un identificador de llamada que concuerda con el de una conexión existente, verificará si la conexión proviene de la misma entidad que la conexión anterior o tiene la misma dirección de señalización de llamada de seguridad de esa misma entidad. Si se cumple una de esas condiciones, la entidad que recibe la nueva conexión considerará que la conexión anterior ha fallado y la cerrará.

R.8.4 Restablecimiento de conexión H.245

Una vez que se ha restablecido el canal de señalización de llamada y que el procedimiento de robustez ha alcanzado un estado estable, si se utilizaba tunelización H.245, las entidades pueden continuar tunelizando mensajes utilizando el nuevo canal de señalización de llamada.

Si se estaba utilizando una conexión H.245 separada, puede que haya fallado sola o junto con el canal de señalización de llamada. Si la entidad ha detectado fallo en un canal H.245, abandonará su conexión sin cerrarla (sin enviar la instrucción EndSessionCommand, que indicaría al otro extremo la finalización de la llamada). Intentará entonces establecer una nueva conexión enviando su dirección h245 en un mensaje Facilidad a su vecino de señalización. Una entidad que recibe Facilidad con una dirección h245 en una llamada para la que ya posee un canal H.245 (que posiblemente, haya fallado sin haber sido detectado) cerrará el canal existente y abrirá uno nuevo. Ninguna de las dos entidades aplicará procedimientos de inicialización H.245 (determinación de principal-subordinado e intercambio de capacidad de terminal) para el nuevo canal.

R.8.5 Datos compartidos a través de un depositario compartido

Como mínimo, deben compartirse los datos siguientes a través de un depositario compartido:

1) backupCallSignallingAddresses;

2) hasSharedRepository;

3) identificador de llamada (callIdentifier);

4) estructuras OpenLogicalChannel, de H.245 o Comienzo rápido (fastStart).

Pueden compartirse datos adicionales para soportar la recuperación de llamadas inestables o permitir la recuperación de datos adicionales que cambian durante llamadas estables (por ejemplo, registros de detalles de llamada, datos de temporización de llamada, datos de facturación, testigos de autorización).

R.8.6 Puntos de verificación

En esta versión de esta Recomendación mantenemos solamente las llamadas que están en el estado estable. Por tanto, sólo se necesita un punto de verificación cuando se entra en el estado estable. Así ocurre cuando se ha enviado o recibido Conexión y se han establecido canales de medios en ambos sentidos (mediante procedimientos H.245 o de conexión rápida).

Las entidades pueden utilizar puntos de verificación adicionales para soportar la recuperación de llamadas inestables o permitir la recuperación de datos adicionales que puedan cambiar durante llamadas estables.

R.9 Interfuncionamiento entre métodos de robustez

Los vecinos de señalización deben acordar un método de robustez que será utilizado entre ellos. **No** es necesario que se utilice el mismo método de extremo a extremo.

El soporte de robustez (cualquier método) es indicado por la entidad del lado origen incluyendo el campo RobustnessGenericData en Establecimiento. Además, es indicado por el soporte del método B (depositario compartido) el campo hasSharedRepository de Establecimiento. La entidad de lado terminación indica su soporte de robustez y del método B mediante los mismos campos de Conexión. La selección del método A o del método B se indica en la cláusula **R.10, Procedimientos para la recuperación**.

Si una entidad que encamina señalización de llamada soporta el método B (tiene un depositario compartido), puede ser necesario utilizar el método B en una conexión y el método A en la otra para la misma llamada. En este caso, sigue las reglas indicadas en la cláusula de **Procedimientos para recuperación** independientemente en las dos conexiones. Si una entidad de seguridad con un depositario compartido recibe una Indagación de estado, puede responder con Estado utilizando la información del depositario compartido.

R.10 Procedimientos para la recuperación

1) Si el vecino no soporta el método B (depositario compartido) y se utiliza señalización TCP, se utilizarán entonces los StatusInquiry keepAlives. Si la entidad tiene un depositario compartido (incluso si el vecino no lo tiene) enviará periódicamente Indagación de estado (StatusInquiry). Si la entidad no tiene un depositario compartido, sólo la entidad más próxima a la parte llamada enviará periódicamente StatusInquiry.

2) Si una entidad tiene un mensaje que enviar por un canal de señalización de llamada (incluido un keepAlive StatusInquiry) y detecta fallo, intentará establecer un canal con la primera dirección en backupCallSignalAddresses (entidad de seguridad).

3) Después de que un canal de señalización de llamada está restablecido, si el vecino no tiene depositario compartido, se utilizará el método A y la entidad que establece enviará Estado (con el campo fastStart) antes del mensaje en espera de envío.

4) La entidad que establece la conexión puede también enviar un mensaje Indagación de estado antes del mensaje, si desea auditar la consistencia del estado.

5) Si una entidad con depositario compartido recibe StatusInquiry, enviará una StatusInquiry a su vecino del otro lado para recuperar la información de estado necesaria (incluidos datos fastStart), a menos que mantenga todos esos datos en su depositario.

6) Si una entidad que no tiene depositario compartido recibe una StatusInquiry, esperará hasta que recibe un Status de su vecino del otro lado (enviando StatusInquiry, si es necesario, al otro vecino, si el canal de señalización del otro lado está disponible).

R.11 Utilización de datos genéricos (GenericData)

Los campos de datos necesarios para implementar las características de este anexo son transportados en los campos de datos genéricos de los diferentes mensajes, como se define a continuación. Los datos de robustez (`RobustnessData`) serán codificados y los datos binarios resultantes serán transportados como un ejemplar sin procesar de datos genéricos en los mensajes especificados.

```
RobustnessData ::= SEQUENCE
{
    backupCallSignalAddresses   SEQUENCE OF TransportAddress,
                                -- empty when not required
    h245Address                 TransportAddress OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
    timeToLive                  TimeToLive OPTIONAL
    hasSharedRepository         NULL OPTIONAL,
    includeFastStart            NULL OPTIONAL,
    ...
}
```

El GenericIdentifier será 1:

```
robustnessId GenericIdentifier ::= standard:1
```

Además, se incluirá un featureDescriptor que transporta el robustnessId en las desiredFeatures de los mensajes especificados a continuación.

R.11.1 Utilización de GenericData en los mensajes H.225.0

Las entidades que soportan robustez utilizarán campos relacionados con GenericData de la siguiente manera (véase el cuadro R.1):

Cuadro R.1/H.323 – Utilización de los campos GenericData por datos de robustez

Mensaje	incluye datos de robustez en GenericData	Campos necesarios						FeatureDescr de robustez en indesiredFeatures de featureSet
		tiene depositario compartido	direcciones backupCallSig	FastStart de robustez	incluye FastStart	TimeToLive de robustez	H245Addr de robustez	
RRQ	M	M						M
RCF	M	M						M
ARQ								M
ACF								M
Setup	M	M	M					M#
Connect	M	M	M					M
Status+	M			M			M	
StatusInquiry+	M				M	M	M	
M obligatorio – prohibidos todos los demás. + cuando se utiliza en procedimientos de robustez. # desiredFeatures no está dentro de featureSet en Setup.								

Todas las entidades que soportan procedimientos de robustez soportarán Status con el campo RobustnessData añadido, a fin de aumentar la interoperabilidad entre los métodos A y B.

R.12 Nota Informativa 1: Antecedentes de los métodos de robustez

Esta cláusula describe los tipos de fallo de sistema y tipos de robustez desde un punto de vista general. No todos los fallos de sistema que aquí se describen son tratados mediante métodos de robustez en la actual versión de este anexo. Se ofrece esta visión más general para dar contexto a los métodos actualmente definidos y ayudar al lector a entender qué tipos de fallo de sistema son tratados aquí. También sirve como lista de fallos que podrían tratarse en versiones futuras del anexo.

R.12.1 Tipos de métodos de robustez

Puede proporcionarse robustez de sistema de varias maneras:

1) métodos de redundancia de hardware/sistema operativo (posiblemente incluyendo varias tarjetas NIC);
2) entidades en tándem;
3) entidades virtuales.

R.12.2 Entidades robustas

Las entidades a considerar para la robustez incluyen esencialmente todas las entidades H.323:

1) controladores de acceso;
2) elementos de frontera;
3) controladores multipunto;
4) posibles procesadores multipunto (para el fallo de trenes de medios);

5) pasarelas (incluidas pasarelas IP a IP);

6) mandatarios cortafuegos; y

7) ciertos tipos de puntos extremos.

No todos los modelos de robustez son adecuados para todos los componentes de sistema.

R.12.3 Ámbito de un sistema robusto

El ámbito de robustez o la parte de un sistema que implementa robustez puede incluir uno o varios de los siguientes aspectos:

1) zonas H.323 (intrazona, con uno o varios controladores de acceso);

2) intradominio H.323 (intradominio, interzona con varios controladores de acceso);

3) interdominio H.323 (interdominio, con varios controladores de acceso y elementos de frontera).

R.12.4 Terminación y fallos de sistema

Debe proveerse una terminación de sistema ordenada (tal como un MC que abandona una conferencia) así como un fallo de sistema. La terminación ordenada permite, en principio, al punto extremo de terminación notificar a sus pares, simplificando así la detección, pero también requiere mecanismos adicionales o ligeramente diferentes. Nótese que la notificación puede fallar debido a pérdida de paquetes repetida, de manera que la frontera con los fallos de sistema es casi imperceptible.

En las subcláusulas siguientes se trata el tema de los aspectos de fallo de sistema.

R.12.4.1 Tipos de fallos

Los métodos descritos en este anexo tratan solamente con fallos que puedan ser detectados desde el punto de vista de un protocolo "en línea". El fallo de un procesador en un sistema de multiprocesador con memoria compartida no es visible desde el exterior, por lo que no se trata en estos métodos. En cambio, el fallo de una tarjeta NIC requiere la utilización de una dirección de transporte diferente, por lo cual es visible y debe tratarse. Los siguientes tipos de fallos serán visibles a los vecinos de señalización y son objetivos de este trabajo:

1) fallo total de un componente del sistema (fallo de alimentación eléctrica, fallo total del software);

2) fallo parcial de un componente del sistema (fallo de una de las varias interfaces de comunicación);

3) fallo total del enlace de red (un componente del sistema ha dejado de ser accesible); y

4) fallo parcial del enlace de red (no todos los componentes del sistema son accesibles entre sí, pero algunos pueden aún comunicarse, incluido, en particular, la conectividad parcial y el fallo de media conexión).

Debe señalarse que algunos de estos fallos pueden no sólo ser difíciles de detectar (simétricamente) sino también no distinguirse entre sí (véase más adelante).

5) Ataques malintencionados al sistema deben considerarse en el contexto de los trabajos de seguridad H.323.

R.12.4.2 Detección de fallo

1) Tiempo para detectar un fallo.

2) Formas de detectar un fallo (vigilancia permanente explícita o detección al invocarse una función).

3) Entidades responsables de/o que intervienen en la detección de un fallo.

4) Aparición de un fallo a un componente de sistema o a un conjunto de componentes de sistema.

5) Posibilidad de determinar el tipo de fallo.

6) Coherencia/temporización de la detección de fallos entre los diferentes componentes de un sistema.

7) La detección de fallo puede no ser transitiva, es decir, de "A puede/no puede hablar con B" y "B puede/no puede hablar con C" no puede deducirse necesariamente que "A puede/no puede hablar con C".

8) ¿Cuánta tara es aceptable?

R.12.4.3 Tratamiento de un fallo

1) Tiempo hasta la reparación.

2) Entidad que inicia el proceso de reparación.

3) Posibilidad de reparar el fallo.

4) Consecuencias si no puede repararse el fallo.

5) Cómo asegurar el tratamiento coherente de un fallo por todas las entidades que intervienen.

6) ¿Cómo tratar las opiniones/detecciones de fallos divergentes por diversos componentes (fallan o no)?

7) ¿Cómo tratar la diferente temporización de la detección de fallos?

8) ¿Cómo tratar con estado incoherente cuando se trata un fallo?

9) ¿Cómo tratar los vacíos de información de estado cuando se trata un fallo?

10) Consecuencias sobre la operación total del sistema (por ejemplo, una llamada saliente).

11) ¿Cuánta tara es aceptable?

12) ¿Cómo tratar con múltiples fallos simultáneos?

R.12.4.4 Escenarios de fallo

Esta subcláusula enumera muchos escenarios de fallo identificados para los sistemas H.323. Los métodos de robustez del presente anexo no permiten la recuperación tras todos estos fallos, pero se enumeran para tener una visión completa y para dar contexto a los fallos cubiertos por los métodos de robustez.

1) (Controlador de acceso – punto extremo): sin relación aún, o sin más relación.

2) (Controlador de acceso – punto extremo): descubierto pero no registrado.

3) (Controlador de acceso – punto extremo): descubierto y registrado.

4) En el proceso de establecimiento de la comunicación:

   a) directo;

   b) encaminado por controlador de acceso.

5) Durante una llamada/conferencia: UIT-T D.160: "estado estable" – discutir lo que esto significa para los diversos protocolos:

   a) directo;

   b) encaminado por controlador de acceso.

6) En el proceso de liberación de llamada:

   a) directo;

   b) encaminado por controlador de acceso.

Considerar las implicaciones resultantes de los diversos nuevos protocolos que se desarrollan actualmente (familia de la serie H.450.x, anexo K, anexo L de esta Recomendación, etc.).

Considerar los trenes de medios así como las relaciones RAS/señalización de llamada/comunicación de control de conferencia.

R.13 Nota Informativa 2: Compartición de estado de llamada entre una entidad y su par de seguridad

Esta nota sugiere modos de implementar la compartición de estado de llamada entre una entidad y otra que le sirve como par de seguridad. La selección de un método no forma parte de esta Recomendación. Como el método no está normalizado, es posible que pares provenientes de diferentes vendedores puedan no ser adecuados como pares de seguridad robustos.

R.13.1 Memoria compartida

Si los miembros de un mismo conglomerado están físicamente localizados en la misma habitación, pueden utilizar un dispositivo de memoria compartido (o reflectivo). Este caso es similar al de muchas plataformas tolerantes a los fallos, pero en donde se puede simplemente escribir en una memoria compartida en cada punto de control en lugar de utilizar un sistema operativo tolerante a los fallos.

R.13.2 Disco compartido

Si los miembros del conglomerado están ubicados físicamente cerca unos de otros, pueden utilizar un disco compartido y escribir la información de estado en cada punto de verificación.

R.13.3 Paso de mensaje

La entidad activa puede enviar un mensaje actualizando el estado compartido a cada uno de los demás miembros del conglomerado en cada punto de verificación. Se implementa así una memoria compartida distribuida, conocida también como *boletín*. Los mensajes pueden enviarse utilizando diferentes mensajes UDP, mensajes multidifusión, enlaces TCP persistentes o protocolos de paso de mensajes tolerantes a los fallos tales como el ASAP (que soporta un mecanismo de multidifusión de envío al grupo que no requiere IP de multidifusión). Este aspecto se discute con más detalle en APC-1772, donde se sugieren algunos puntos de verificación.

R.13.3.1 SCTP/ASAP

Esta subcláusula ilustrará, con un ejemplo de llamada H.323, la utilización de ASAP y SCTP con fines de robustez en un sistema H.323. Incluirá en resumen:

1) una sinopsis arquitectural de un sistema H.323 que utiliza ASAP/SCTP;
2) una visión de las pilas de protocolos necesarias en los respectivos nodos H.323; y
3) escenarios de reparación de fallos en un ejemplo de llamada H.323 con dos controladores de acceso y dos puntos extremos.

R.13.3.1.1 Referencias

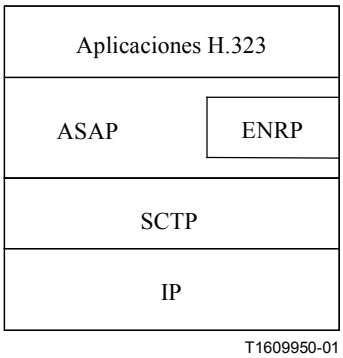
[1] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

[2] R. R. Stewart, and Q. Xie: *Aggregate Server Access Protocol (ASAP)*, <draft-xierserpool-asap-00.txt>, IETF, October 2000.

[3] Q. Xie, and R. R. Stewart: *Endpoint Name Resolution Protocol (ENRP)*, <draft-xie-rserpool-enrp-00.txt>, IETF, October 2000.

R.13.3.1.2 Pilas de protocolos

En general, una aplicación H.323 que utilice ASAP/SCTP [1] a [3] para la tolerancia de fallos tendrá la siguiente pila de protocolos:



Esto puede permitir la reparación rápida de fallos, transparente a la aplicación de capa superior, tanto a nivel de conexión como de sesión:

1) nivel de enlace (SCTP) – soporte multibuscador, supervivencia a fallos de red;

2) nivel de sesión (ASAP) – soporte de fondo común servidor (2N, N+K, etc.), supervivencia a fallos de proceso/nodo.

Además, el ASAP proporciona:

- transparencia de ubicación;
- compartición de carga;
- enchufe activo, es decir alta escalabilidad;
- evita un punto de fallo individual.

R.13.3.1.3 Visión arquitectural de un sistema H.323

La figura R.3 presenta un sistema H.323 construido sobre la base del modelo ASAP/SCTP.

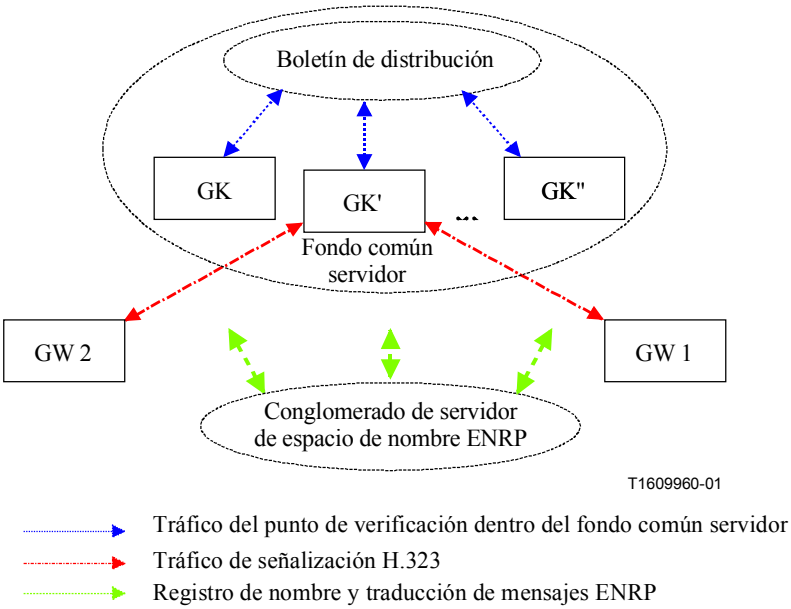


Figura R.3/H.323 – Sistema H.323 construido sobre la base del modelo ASAP/SCTP

En este sistema, todos los componentes H.323, incluidos los GW1, GW2 y los GK utilizan las pilas ASAP/SCTP que se muestran en la subcláusula anterior. En este ejemplo, suponemos que el controlador de acceso H.323 se implementa como un fondo común servidor (la figura representa las interioridades de este fondo común servidor), mientras que las pasarelas pueden o no implementarse como fondo común servidor.

Como se muestra en la figura, dentro del fondo común servidor del controlador de acceso existen múltiples ejemplares de controladores de acceso H.323 funcionalmente idénticos, GK, GK', ... GK". Los ejemplares GK comparten entre sí información de estado de llamada y otra información crítica de recuperación de llamada mediante un boletín de distribución interna. El mecanismo y la implementación de este boletín es específico del vendedor, por lo que se sale del alcance del ASAP o SCTP (este boletín puede, sin embargo, utilizar ASAP/SCTP para mejorar la tolerancia a los fallos y la escalabilidad).

Todos los nodos ASAP/SCTP, incluidos los GW y los GK, se basan en un único conglomerado servidor de espacio de nombre ENRP o en un grupo de conglomerados ENRP conectados, para el registro de nombre y los servicios de traducción de nombres [2]. Para formar el fondo común servidor de controlador de acceso, todos los ejemplares GK se registran en el espacio de nombre ENRP bajo el mismo nombre. No obstante, cada ejemplar GK puede registrarse con una capacidad de tratamiento de carga diferente.

El ASAP entregará cada mensaje de llamada H.323 a uno de los ejemplares GK en el fondo común servidor. La selección del ejemplar GK receptor se hace sobre la base de la política de compartición de carga en vigor y la situación en ese momento de cada ejemplar GK en el fondo común. Algunas veces es muy deseable que todos los mensajes de señalización H.323 relacionados con una llamada sean tratados por el mismo ejemplar GK durante el ciclo de vida completo de la llamada, y sólo dejar que otro ejemplar GK pueda relevarlo solamente en caso de desaparición total de la original. Denominamos esta relación entre la llamada y el ejemplar del servidor "vínculo holgado". El ASAP ha sido diseñado para soportar muy fácilmente este tipo de relaciones de "vínculo holgado" [2] y [3].

Además, cuando un ejemplar GK está tratando una llamada, debe publicar en el boletín distribuido (por ejemplo, en el "punto de verificación") toda la información crítica de estado de llamada, cada vez que la llamada alcanza una cierta fase de su ciclo de vida. Esta información ayudará al ejemplar GK alternativo a recuperar la llamada en caso de que el ejemplar original que le trata falle totalmente.

R.13.3.1.4 Ejemplo de llamada H.323

Para los fines de descripción de una llamada se utilizarán los flujos de señalización de la figura R.4.

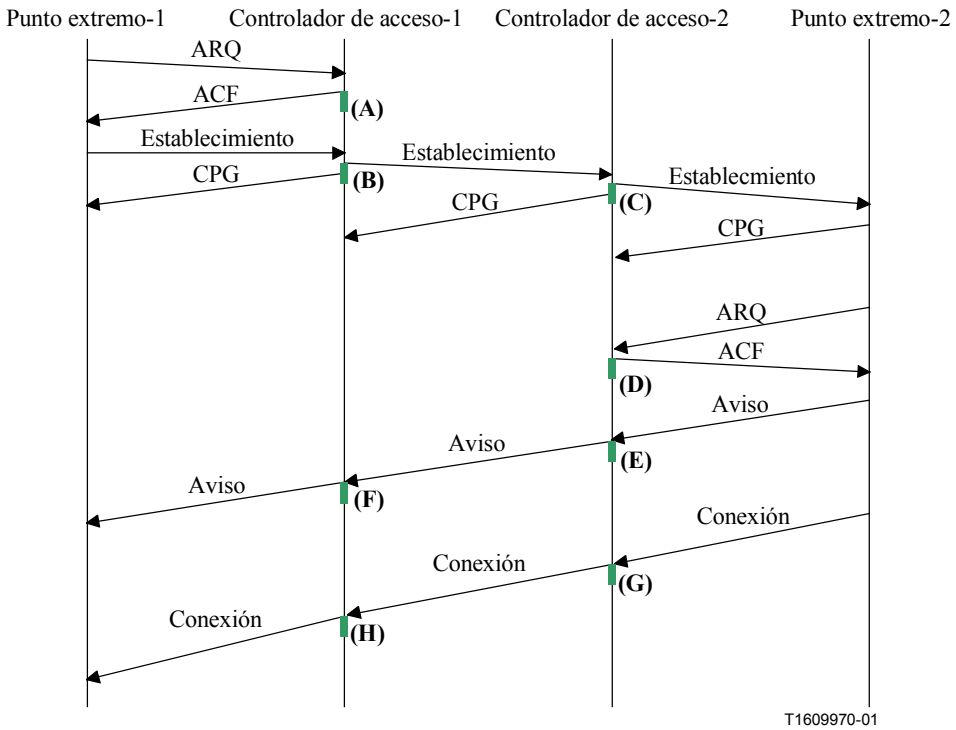


Figura R.4/H.323 – Ejemplo de llamada H.323

Adviértase que las referencias en este flujo de llamadas son bastante antiguas y que se ha extrapolado el segundo controlador de acceso. Pueden existir algunas diferencias con respecto al modo en que la actual especificación H.323 tendría un flujo de llamada, pero lo que importa aquí es resaltar cómo se utilizaría el ASAP/SCTP. Aun si algunos detalles pequeños son incorrectos en la figura anterior, esto no invalida el ejemplo.

R.13.3.1.4.1 Descripción general

La llamada se inicia con una solicitud de ancho de banda por parte del punto extremo-1, que en este caso utiliza el ASAP para solicitar a un controlador de acceso, conocido por un nombre o posiblemente por un puerto y dirección IP. En ambos casos, una demanda de traducción de nombre ENRP (que no se muestra en la figura) propagará al punto extremo el conjunto de todos los controladores de acceso (primarios y redundantes) en el fondo común servidor. Esta información será almacenada en una memoria caché local de la capa ASAP en el punto extremo-1, para su futura referencia en caso de fallo. Este mismo tipo de memoria caché aparecerá en todos los puntos extremos ASAP en la cadena transparente a la llamada. Adviértase que la memoria caché es una característica opcional. Al tratarse de una opción, los puntos extremos que no la utilicen pueden aún obtener un controlador de acceso alternativo, y se necesitaría una solicitud adicional al servidor ENRP en el momento de detección de fallo.

Llegamos ahora al punto (**A**), paso en el que el controlador de acceso atribuye ancho de banda y verifica este mensaje de información de utilización de ancho de banda en un área del "boletín", área que puede ser cualquiera de las siguientes:

- una parte de memoria distribuida compartida, mantenida por un subsistema separado;
- una parte de memoria reflectiva, específicamente construida con este fin;
- una base de datos comercial distribuida;
- alguna otra invención creativa.

Debe advertirse ahora que lo importante aquí es que, de alguna manera los controladores de acceso redundantes/pares posean un mecanismo de compartición de estado de llamada. Pueden utilizar todos los mecanismos existentes, o que existirán en el futuro, de compartición de llamada.

El controlador de acceso-1 ocupa su estado relacionado ARQ y pone esta información en el "boletín", y responde a la petición con un ACF.

El punto extremo-1 reacciona y envía el mensaje establecimiento al controlador de acceso-1, que selecciona el siguiente controlador de acceso, controlador de acceso-2, y reenvía su establecimiento, haciendo llegar la información de estado de llamada al punto **B**, posiblemente relacionada de alguna manera con la información anterior (quizás con alguna forma de referencia cruzada, es decir, la llamada X está utilizando el ancho de banda Y representado por la información ARQ). Después de depositar la información en el punto **B**, el controlador de acceso-1 envía el mensaje de llamada en curso al punto extremo-1.

El controlador de acceso-2 recibe el mensaje de establecimiento de su controlador de acceso par y selecciona el punto extremo de destino, reenviando el establecimiento y depositando la información de estado de la llamada en el punto **C**. A continuación, envía un mensaje de llamada en curso al controlador de acceso-1.

Cuando el punto extremo-2 recibe el establecimiento, envía un mensaje de llamada en curso y solicita a su controlador de acceso ancho de banda dentro de su propio mensaje ARQ.

Esto hace que el controlador de acceso-2 asigne ancho de banda, deposite información de estado en el punto **D** y envíe el mensaje ACF. El punto extremo-2, al recibir este mensaje, envía un mensaje Aviso al controlador de acceso-2.

El controlador de acceso-2 al recibir el mensaje de aviso, depositaría una pequeña actualización en su boletín (punto **E**), es decir, informa de que la llamada está en Aviso, y reenvía el mensaje Aviso al controlador de acceso-1.

El controlador de acceso-1 repetirá el procedimiento, actualizando su información de estado en el punto **F** y reenviando el mensaje de aviso.

El punto extremo-2 responde a la llamada, enviando un mensaje Conexión al controlador de acceso-2, que depositará otra pequeña actualización del estado en el punto **G**, indicando que la llamada se encuentra ahora en estado de respondida y reenvía el mensaje de conexión al controlador de acceso-1.

El controlador de acceso-1, al recibir el mensaje Conexión, repetirá la operación, registrando su estado en el punto **H** y enviando el mensaje de conexión al punto extremo-1.

R.13.3.1.4.2 Escenarios de fallo

Las anteriores descripciones suponen el máximo nivel de redundancia y de mantenimiento de estado/llamada. En este contexto, todo fallo de un controlador de acceso es transparente a ambos puntos extremos. Si se produce un fallo, el mensaje sería reencaminado por ASAP a una entidad alternativa. Esta entidad necesitaría emprender las acciones siguientes para todo mensaje que reciba, que no incluya un objeto/bloque de llamada para:

- encontrar la llamada en el "boletín";
- depositar la información de estado y construir un bloque u objeto de control de llamada a llamada;
- continuar procesando el mensaje en nombre del par desaparecido.

Los puntos extremos son entonces completamente transparentes a los escenarios de fallo. No se almacena ningún tipo de conocimiento para recuperar un fallo de controlador de acceso en el punto extremo en sí (que no sea el ASAP).

R.13.3.1.4.3 Aspectos del mantenimiento de estado

Como antes se ha dicho, este ejemplo supone un modelo de mantenimiento máximo de estado. En este modo, las actualizaciones de estado deberían reducirse a la menor cantidad de información posible. En particular, el estado debe ser limitado al menor conjunto de información necesario para reconstruir la llamada Y las actualizaciones deben ser lo más pequeñas posible. En algunos casos un operador puede no querer tener este nivel de redundancia. Para conseguir un sistema robusto con menos estado, podrían eliminarse los siguientes puntos de compartición de estado:

- En los puntos **A** y **D** – Si el controlador de acceso utiliza alguna otra metodología para calcular la utilización de ancho de banda (además del seguimiento del número de llamadas por cómputo), podrían evitarse estos pasos sin daño alguno. Puede que el operador NO se interese en el control de admisión y que sus controladores de acceso no lo efectúen, en cuyo caso este paso no es necesario.
- En los puntos **F** y **E** – Ambos puntos son opcionales, puesto que no proporcionan ninguna información digna de mantenerse, es decir, que la llamada está sonando o se está aún estableciendo.
- En los puntos **B** y **C** – Si el operador NO está interesado en mantener más que las llamadas estables, pueden eliminarse estos dos puntos. En este caso, se perderían todas las llamadas que estaban estableciéndose cuando ocurrió un fallo.

Compromisos como éstos están fuera del alcance de la utilización del ASAP/SCTP y es de la exclusiva decisión del operador/fabricante saber cuánta información de estado puede ser mantenida por una determinada implementación y qué controles/decisiones puede adoptar el operador.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	**Sistemas audiovisuales y multimedios**
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2002