



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 302 993**

(51) Int. Cl.:
H04Q 3/00 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(86) Número de solicitud europea: **04008261 .2**

(86) Fecha de presentación : **05.04.2004**

(87) Número de publicación de la solicitud: **1585349**

(87) Fecha de publicación de la solicitud: **12.10.2005**

(54) Título: **Procedimiento para manejo transparente de una base de datos inaccesible temporalmente en un servidor de portabilidad de números.**

(45) Fecha de publicación de la mención BOPI:
01.08.2008

(45) Fecha de la publicación del folleto de la patente:
01.08.2008

(73) Titular/es:
**Nokia Siemens Networks GmbH & Co. KG.
St. Martin Strasse 76
81541 München, DE**

(72) Inventor/es: **Schwarzbauer, Hanns Jürgen;
Serroyen, Gert y
Verwimp, Gery**

(74) Agente: **Zuazo Araluze, Alexander**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento para manejo transparente de una base de datos inaccesible temporalmente en un servidor de portabilidad de números.

5

Antecedentes**Campo de la invención**

La presente invención se refiere a la gestión de una base de datos de portabilidad de números y, más en particular, al manejo transparente de una base de datos inaccesible temporalmente en un servidor de portabilidad de números.

Información relacionada

La portabilidad de números de teléfono es un servicio que proporciona a los clientes de teléfono residenciales y de negocios la capacidad de conservar, en la misma ubicación, sus números de teléfono locales existentes cuando se cambian de un proveedor de servicios telefónicos local a otro. Además de ser cómodo para el cliente, la legislación ha introducido la portabilidad de números para fomentar la competencia y reducir la regulación en todos los mercados de telecomunicaciones. Antes de esto, una barrera principal para la competencia era la incapacidad de los clientes para cambiar de una compañía telefónica a otra conservando el mismo número de teléfono.

Por lo tanto, debido a requisitos de regulación un número de teléfono E.164 ya no podría considerarse más la “propiedad” de una cierta compañía telefónica. Un cliente que migra de la compañía telefónica a la que se suscribió originalmente a otra compañía dentro de la misma zona local, tiene derecho a mantener su número E.164 asignado originalmente. E.164 es una recomendación de ITU-T que define el plan de numeración de telecomunicaciones público internacional utilizado en la PSTN y algunas otras redes de datos. Por lo tanto, el número de teléfono solo no podría servir ya más como número de “encaminamiento” en todas las circunstancias.

Antes de establecer una llamada a la parte llamada, tiene que garantizarse si la parte llamada se ha migrado a un operador diferente. Esta pregunta se envía a y se responde mediante por ejemplo un servidor de portabilidad de números (NBDB, *Number Portability Server*). El mensaje se envía normalmente a través de una red SS7 utilizando el protocolo SCCP. La norma SS7 y el protocolo SCCP (SCCP *Signalling Connection Control Part*, parte de control de conexión de señalización) no se comentarán en detalle en el presente documento puesto que son amplia y fácilmente conocidos en la técnica. En lo que respecta a este comentario, se comentará brevemente en el presente documento el modelo de referencia de comunicación de interconexión de sistemas abiertos OSI (*Open Systems Interconnect*) según lo define ISO. Las funciones de hardware y software del protocolo SS7 se dividen en abstracciones funcionales denominadas “niveles”. Estos niveles se corresponden de manera general con el modelo de 7 capas de la interconexión de sistemas abiertos (OSI) definido por la organización internacional de normalización (ISO, *International Standards Organization*).

En general, OSI está dividida en dos componentes de comunicación. La primera componente de comunicación, “Pila OSI”, representa la capa de aplicación a través de la capa de transporte según lo define el modelo de referencia de comunicación OSI. El conjunto de herramientas CMIP envía y recibe datos a la pila OSI. Tras recibir una solicitud del conjunto de herramientas CMIP la solicitud de filtrar descendientemente la pila de protocolos con cada capa respectiva de la pila de protocolos añade esta información al mensaje. Puesto que el IIS implementa RFC 1006, la pila OSI envía/recibe datos a/desde la red utilizando TCP. Una vez que el mensaje desciende a la capa de transporte se entrega utilizando TCP. Cuando la pila OSI recibe una solicitud desde el controlador TCP, se pasa a la pila y se reenvía al conjunto de herramientas CMIP.

El conjunto de herramientas CMIP es una componente de comunicación que implementa el protocolo CMIP. Proporciona una interfaz que utilizan aplicaciones LNP para enviar/recibir datos. Tras recibir un mensaje para su entrega, el conjunto de herramientas CMIP realizará el empaquetado que deba realizar y enviará la solicitud a la pila OSI. Cuando el conjunto de herramientas CMIP recibe un mensaje desde la pila OSI, el conjunto de herramientas CMIP o bien envía una notificación a las aplicaciones LNP indicando que hay datos disponibles para la recepción o bien las aplicaciones LNP interrogan al conjunto de herramientas CMIP. La parte de aplicaciones de capacidades de transacción (TCAP, *Transaction Capabilities Applications Part*) soporta el intercambio de datos no relacionados con circuitos entre aplicaciones a través de la red SS7 utilizando el servicio sin conexiones SCCP. Las preguntas y respuestas enviadas entre SSP y SCP se llevan en mensajes TCAP.

Es crítico que los tiempos de respuesta desde el servidor NP sean cortos con el fin de no retardar el establecimiento de llamada. De manera problemática, el número de números de teléfonos portados ha aumentado espectacularmente y se espera que aumente. Como resultado, la probabilidad de que la base de datos direccionada sea inaccesible debido a la congestión está asimismo aumentando. La inaccesibilidad puede agravarse por acciones de gestión, tales como sincronización con una base de datos maestra u operaciones de recuperación. En cualquier caso, incluso una situación de sobrecarga temporal puede intensificarse rápidamente.

Sin embargo, aún no existe ninguna solución adecuada para la congestión y la sobrecarga. En primer lugar, esto se debe al hecho de que el control de la congestión está prohibido por las normas ISO que gobiernan el protocolo SCCP, que dejan poco espacio para gestionar una situación de sobrecarga en el lado SCCP. Más en particular, la

ES 2 302 993 T3

recomendación para el control de la congestión sigue el mecanismo de “control de flujo” descrito en el modelo de referencia de comunicación OSI (ISO/IEC 7498). Se definen dos tipos de control de flujo como (1) control de flujo de semejantes y (2) control de flujo entre capas.

- 5 El control de flujo de semejantes puede utilizarse cuando dos capas semejantes de la pila OSI hablan entre sí. La forma más común de control de flujo de semejantes es el protocolo de ventana deslizante. Este protocolo se implementa mediante TCP. El protocolo de ventana deslizante impide que el emisor invada el destino poniendo un límite en el número de mensajes sin confirmación de recepción que pueden estar pendientes en un momento. El control de flujo entre capas opera sobre los mensajes que se transmiten entre cada capa de la pila de protocolos. Las capas inferiores del modelo OSI devolverán un error al que llama cuando se ha superado una limitación de recursos.

- Desde el punto de vista de NPAC, estos dos mecanismos funcionan como a continuación. Cuando el TCP se encuentra con una situación en la que su ventana deslizante está impidiendo la entrada de cualquier mensaje nuevo, el TCP DETENDRÁ la aceptación de cualquier mensaje nuevo. Si un emisor (en este caso es la capa de sesión) intenta enviar un mensaje, TCP devolverá un error de limitación de recursos. Finalmente, el emisor (de nuevo en este caso la capa de sesión) alcanzará una limitación de recursos porque su cola de mensajes es demasiado grande y tendrá que devolver una limitación de recursos a su emisor. Este proceso continúa hacia arriba de la pila hasta que el conjunto de herramientas CMIP se considera el emisor.

- 20 Cuando el conjunto de herramientas CMIP recibe un error de limitación de recursos, debe o bien poner en cola el mensaje o devolver el error a la aplicación LNP. Si el mensaje se pone en cola, entonces debe existir un umbral en el que se notificará a la aplicación LNP finalmente la situación. Una vez que la aplicación LNP recibe este mensaje de error suspenderá temporalmente la entrega del mensaje y lo intentará de nuevo en un momento posterior. Cómo se implemente el algoritmo “inténtelo de nuevo más tarde” se deja a la elección de cada proveedor. El punto clave es que el mensaje NO se descende y la entrega se suspende. Lo que esto significa es que la aplicación LNP será un depósito de contención final.

- Por tanto, la norma proporciona que el SCCP de origen maneje el problema tal como ya se comentó. Desde el punto de vista del receptor, no se proporciona ningún procesamiento especial para manejar la congestión. Si la aplicación LNP de recepción no puede procesar la solicitud tan rápido como pueden entrar entonces el conjunto de herramientas CMIP en el receptor los devolverá y detendrá finalmente la aceptación de nuevos mensajes desde la pila OSI. Asimismo, la pila OSI volverá hacia arriba. Finalmente, TCP no podrá confirmar la recepción de la nueva solicitud. Esto provocará que los emisores TCP resulten controlados en flujo. Si la condición continúa, la aplicación LNP se suspenderá en última instancia. Cuando el problema está relacionado con la red, la congestión se reconoce puesto que TCP utiliza el protocolo de ventana deslizante. Si la red está congestionada entonces el emisor no recibirá ninguna señal de confirmación de recepción de nivel TCP desde el destino. Si el enlace resulta congestionado durante la recuperación, el NPAC se adhiere el mismo paradigma que tiene lugar para la congestión ya comentada.

- La situación se muestra en la figura 1, en la que un centro 100 de llamadas, que puede ser un dispositivo de conmutación mundial electrónica (EWS, *Electronic World Wide Switching Device*), inicia una petición, en este caso un número de peticiones que se distribuyen uniformemente a las bases de datos 102a y 102b NP en un entorno de protocolo SCCP encaminado a través de un conmutador de paquetes respectivo denominado dispositivos 104a, 104b STP/SRP de puntos de transferencia de señal, que sirven como los servidores NP respectivos. Un STP encamina cada mensaje entrante a un enlace de señalización saliente, en este caso a las bases de datos NP respectivas, basándose en información de encaminamiento contenida en el mensaje SS7. Según el protocolo SCCP descrito anteriormente, en el caso de que los servidores NP estén sobrecargados, se genera un mensaje de error SCCP apropiado y se envía de vuelta al nodo de origen, concretamente el centro 100 de llamadas.

- Debido a esto, el centro 100 de llamadas debe analizar y redistribuir la petición a otras bases de datos NP, lo que quita un tiempo crítico a la conexión de la llamada. Por no mencionar que el mensaje de error de vuelta puede retrasarse por razones de red. Todo esto retarda el tiempo de establecimiento de llamada para todas las llamadas, hasta que el nodo de origen es consciente de la situación y redistribuye apropiadamente el tráfico. Como resultado, el aumento en el tiempo de establecimiento de llamada es perceptible. Para agravar el problema, el nodo de origen también podría sufrir el hecho de que su capacidad de comunicación total hacia los servidores NP se viese disminuida bruscamente, provocando potencialmente la congestión sobre los enlaces SS7 restantes, perturbando posiblemente de ese modo otros tiempos de establecimiento de llamada. Por tanto, el presente procedimiento prohibido por la norma es inadecuado.

- Lo que se necesita es un procedimiento que maneje la congestión de una manera mejor que la ya proporcionada por la norma SCCP. Sin embargo, la norma también debe cumplirse. Por lo tanto, lo que se necesita es una solución que mejore sobre la norma SCCP el manejo de congestión, y que al mismo tiempo no interfiera con la norma. Hasta ahora no ha habido tal solución.

- La patente estadounidense 6.137.806 describe una red inteligente que comprende una pluralidad de puntos de señalización de servicio (SSP, *Service Signalling Points*) y un punto de control de servicio (SCP, *Service Control Point*) se proporciona manejo mejorado de situaciones de sobrecarga en el punto de control de servicio por medio de un punto de señalización de red interpuesto entre los SSP y el SCP. Sin embargo, esta patente no describe cómo manejar sobrecargas de peticiones NP.

Objetos y resumen de la invención

Un objeto de la invención es proporcionar manejo transparente de una base de datos NP inaccesible.

5 Otro objeto de la invención es mantener el protocolo SCCP actual.

Como característica adicional, la presente invención proporciona un mensaje que incluye parámetros de control que provocan que los servidores NP conmuten bases de datos NP.

10 La clave de la mejora propuesta del procedimiento descrito anteriormente es el hecho de que sólo la base de datos NP del servidor NP está inaccesible, mientras que toda la comunicación externa basada en SCCP está todavía funcionando. Se proporciona la gestión de congestión de una de una pluralidad de bases de datos NP de un sistema SCCP. Se envía un mensaje desde un nodo en un lado SCCP a un servidor en un lado NP que inicia una petición para obtener información NP. Una base de datos NP actual se detecta como sobrecargada con peticiones de obtener información NP. El mensaje SCCP se encamina desde el servidor NP a un servidor NP alternativo.

La ventaja de la solución propuesta es el hecho de que ya no necesita señalizarse más la inaccesibilidad de la base de datos NP a todos los nodos de origen potenciales. No necesita retransmitirse ningún mensaje por el origen. Por lo tanto se espera que el retardo sea perceptible. Especialmente los nodos de origen no se enfrentan a congestión de enlace SS7, especialmente cuando la respuesta se envía a través de la trayectoria original.

Breve descripción de los dibujos

Las siguientes figuras ilustran al menos un ejemplo de la presente invención:

25 la figura 1 ilustra la técnica anterior;

la figura 2 ilustra la presente invención; y

30 la figura 3 ilustra el mensaje de la presente invención.

Descripción detallada de las realizaciones preferidas

Ahora con referencia a la figura 2, se describirá a continuación la presente invención, en la que un conmutador 200 señala bases de datos 202a NP, b a través de servidores 204a NP, b respectivamente. La invención hace que las bases de datos NP se conmuten en el lado de servidor NP por medio de un único mensaje, que va a comentarse con referencia a la figura 3. Por tanto, la conmutación es transparente para el lado SCP, no afectando de ese modo la norma SCCP para el control de la congestión.

40 Ahora en funcionamiento, el conmutador 200, en respuesta a una solicitud de establecimiento de llamada de un abonado, inicia una petición para buscar la base de datos 202a NP para el servidor 204a NP correspondiente. En el caso de que el acceso a la base de datos 202a NP esté sobrecargado, debido a otras peticiones, el servidor 204a NP envía la respuesta de sobrecarga a otro servidor NP, en este caso 204b, es decir, en lugar de, de nuevo al conmutador 200 tal como en el procedimiento antiguo. En caso de que la base de datos 202b NP alternativa esté sobrecargada, el servidor 204a NP correspondiente envía la respuesta a un tercer servidor NP, y así sucesivamente, hasta que se encuentre una base de datos NP que esté libre. De esta manera, el manejo de la congestión de una base de datos NP es completamente transparente para el lado SCCP.

50 Ahora con respecto a la figura 3, se explicará el mensaje SCCP de la presente invención. Tal como se explicó anteriormente, la invención crea un único mensaje SCCP para el manejo de congestión de una base de datos NP de manera transparente.

Aquí se muestran dos mensajes 300a, 300b SCCP correspondientes a las bases de datos (202a, 202b) NP ilustradas en la figura 2. Estos mensajes SCCP siguen el formato de mensaje SCCP de norma prohibido. Los mensajes 300a, 300b comprenden una parte 302a, b de capa TC de datos que proporciona datos para la capa TC (*Transaction Capabilities Layer*, capa de capacidades de transacción). Es un medio basado en el modelo de referencia OSI para soportar aplicaciones en redes de telecomunicaciones. Los procedimientos y funciones del protocolo que controlan la información no relacionada con circuitos se intercambian entre puntos de señalización en redes SS7. Proporciona un enfoque de propósito general para la introducción de nuevos servicios dentro de una red así como un marco de trabajo para arquitectura de servicios para proporcionar servicios de trabajo de Internet. Las capacidades de transacción incluyen el protocolo de capa de aplicación denominado parte de aplicación de capacidades de transacción (TCAP, *Transaction Capabilities Application Part*) así como las capas de presentación, sesión y transporte de soporte denominadas la parte de servicio de aplicación (ASP, *Application Service Part*).

65 La dirección 304a, b ClgPty (*Calling Party*) de la parte que llama es la dirección de la parte que llama y la dirección clldpty (*Called Party*) es la dirección 306b de la parte llamada. La dirección de la parte llamada puede incluir puede incluir los dígitos marcados GT (*Global Title*, título global) o NP (*Number Portability*, portabilidad de números) lógica GT. El título global es una dirección "lógica" o "virtual" utilizada para encaminar mensajes del sistema de señalización

ES 2 302 993 T3

número 7 (SS7) utilizando capacidades de la parte de control de conexión de señalización (SCCP). Para completar el encaminamiento de mensajes, un GT debe traducirse a número de subsistema y código de punto SS7.

La clase 308a, b de protocolo define la clase para el protocolo.

El tipo de mensaje UDT 310a, b define un tipo de mensaje, un valor asignado utilizado para identificar la característica que genera el mensaje. La SLS 312a, b define un campo de selección de enlace de señalización, que es un campo de la etiqueta de encaminamiento que se utiliza normalmente por la función de encaminamiento de mensajes para realizar compartición de carga entre diferentes enlaces o conjuntos de enlaces de señalización.

El OPC (*Originating Point Code*, código de punto de origen) 314a, b es parte de la etiqueta de encaminamiento en un mensaje de señalización que identifica unívocamente el punto de origen de ese mensaje de señalización en una red de señalización. El DPC 316a, b define el código de punto de destino y el NI 318a, b define el indicador de red. El Si 320a, b indica el indicador de servicio.

Sin embargo, en la presente invención, el DPC 316a del mensaje 300a original se modifica mediante el servidor 204a NP para incluir el parámetro de control alternativo que hace que el mensaje se encamine al segundo servidor 204b NP. En ese caso, el DPC 316a del mensaje 300a original se carga desde DPC=STP/SRP “1”, que nombra a la primera base de datos 202a NP hasta DPC=STP/SRP “2”, que nombra a la segunda base de datos 202b NP.

Como resultado, el mensaje se encamina a la segunda base de datos 202b NP y se procesa. La invención mantiene el parámetro 314a de control de nodo de origen, concretamente OPC=Sep “o” en el segundo mensaje.

Cuando la segunda base de datos 202b NP, u otra, no está congestionada, el servidor 204a NP correspondiente devuelve el resultado de la búsqueda NP al nodo de origen, tal como se indica mediante el parámetro 314a de control OPC. De esta manera, el nodo de origen no nota el manejo de congestión y el resultado de la base de datos NP se recibe automáticamente por el nodo de origen sin redistribución desde el lado SCCP.

La clave de la mejora propuesta del procedimiento descrito anteriormente es el hecho de que sólo la base de datos NP del servidor NP está inaccesible, mientras que toda la comunicación externa basada en SCCP todavía está funcionando.

Puesto que la presente invención es transparente para el sistema SCCP, otra ventaja es que la invención puede funcionar en paralelo con la norma SCCP actual para el manejo de congestión.

REIVINDICACIONES

5 1. Procedimiento para gestionar la congestión de una de una pluralidad de bases de datos (202a) de portabilidad de números de un punto de control de conexión de señalización, abreviado como sistema SCCP, en el que se envía un mensaje SCCP desde un nodo en un lado SCCP a un servidor (204a) NP de portabilidad de números situado en un lado de servidor de portabilidad de números que inicia una petición para obtener información de portabilidad de números, que comprende las etapas de:

10 detectar que una base de datos (202a) de portabilidad de números está sobrecargada con peticiones para obtener información de portabilidad de números;

encaminar el mensaje SCCP desde el servidor (204a) de portabilidad de números situado en el lado de portabilidad de números a un servidor (204b) de portabilidad de números alternativo.

15 2. Procedimiento según la reivindicación 1, que comprende además la etapa de insertar en el lado de portabilidad de números en el mensaje SCCP un parámetro de control que indica una base de datos (202b) alternativa.

20 3. Procedimiento según la reivindicación 1, en el que la etapa de detección comprende además la etapa de recibir desde la base de datos (202a) de portabilidad de números actual una situación de sobrecarga por el servidor (204a) de portabilidad de números.

25 4. Procedimiento según la reivindicación 1, que comprende además la etapa de encaminar el mensaje desde un último servidor (204a) de portabilidad de números a otro servidor (204b) de portabilidad de números hasta que una base de datos (202a) de portabilidad de números correspondiente no esté sobrecargada.

5. Aparato para gestionar la congestión de una de una pluralidad de bases de datos (202a, b) de portabilidad de números, que comprende:

30 - un sistema SCCP, que incluye una base de datos de portabilidad de números para proporcionar información de portabilidad de números;

- un servidor de portabilidad de números que obtiene la información de portabilidad de números en respuesta a una petición de portabilidad de números correspondiente a un número marcado original relacionado;

35 en el que el servidor (204a) de portabilidad de números encamina la petición a otro servidor (204b) de portabilidad de números cuando la base de datos (202a) de portabilidad de números está sobrecargada con peticiones.

40 6. Aparato según la reivindicación 5, que comprende además:

- un servidor (200) SCCP para generar la petición de portabilidad de números.

45 7. Aparato según la reivindicación 5, en el que la petición de portabilidad de números es un mensaje SCCP, en el que el servidor (204a) de portabilidad de números inserta una dirección de portabilidad de números del servidor (204b) de portabilidad de números alternativo en el mensaje SCCP.

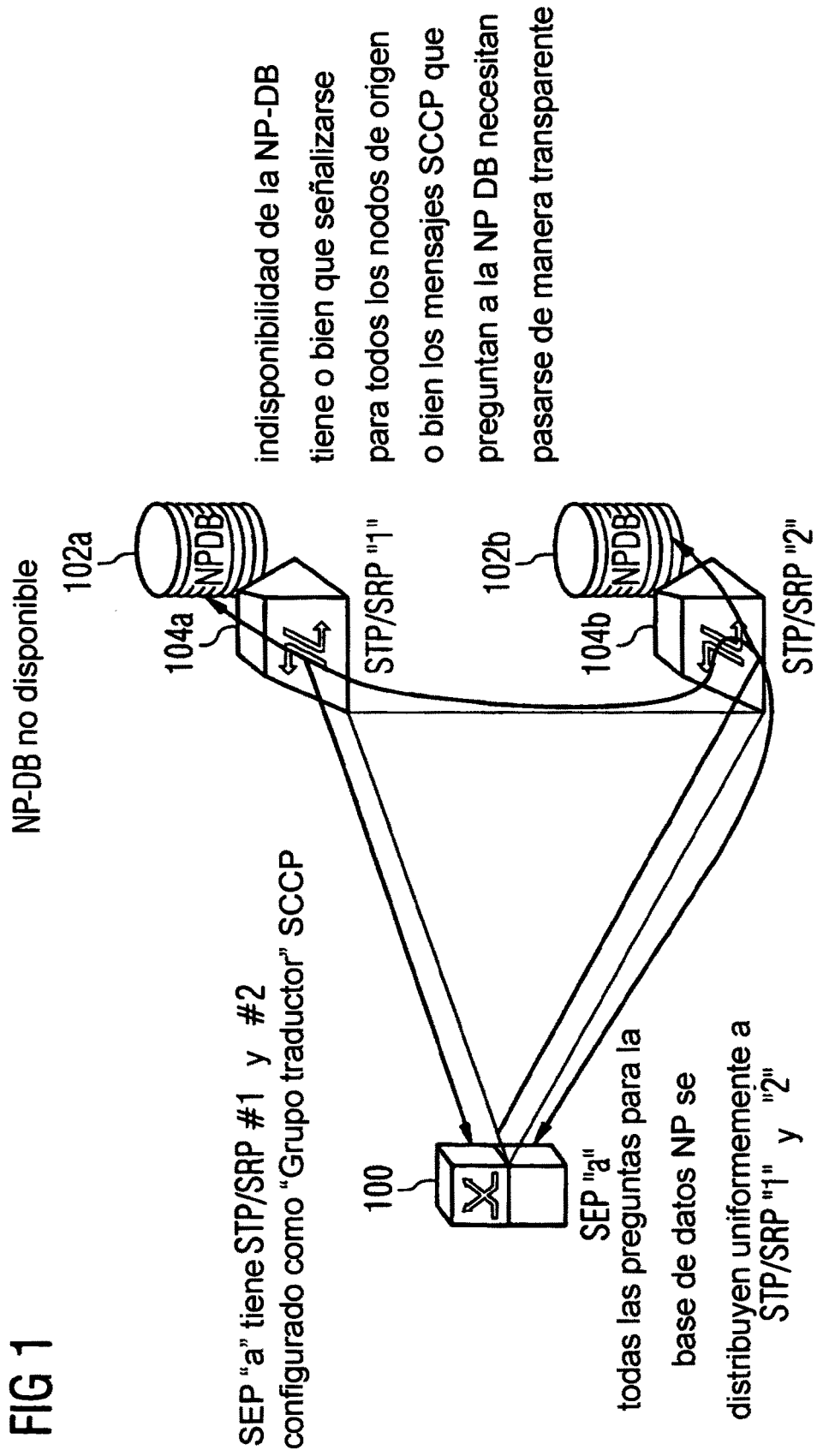
50

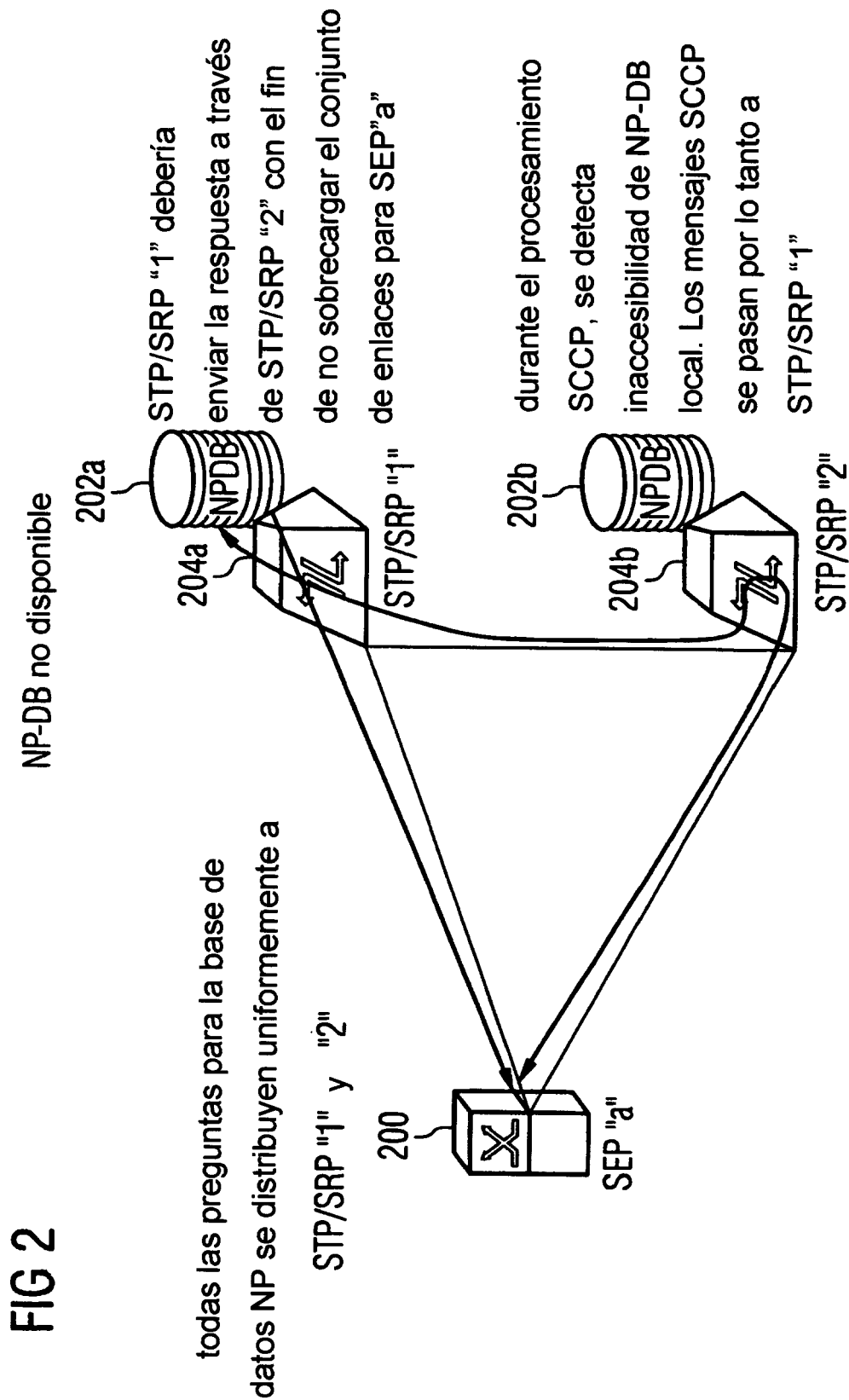
55

60

65

FIG 1





Detalles del mensaje

FIG 3

