



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 298 835**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(86) Número de solicitud europea: **04794633 .0**

(86) Fecha de presentación : **08.10.2004**

(87) Número de publicación de la solicitud: **1678918**

(87) Fecha de publicación de la solicitud: **12.07.2006**

(54) Título: **Una sesión persistente y fiable que recorre de manera segura componentes de red utilizando un protocolo de encapsulación.**

(30) Prioridad: **10.10.2003 US 683881**
30.09.2004 US 711719

(45) Fecha de publicación de la mención BOPI:
16.05.2008

(45) Fecha de la publicación del folleto de la patente:
16.05.2008

(73) Titular/es: **Citrix Systems, Inc.**
851 W. Cypress Creek Road
Fort Lauderdale, Florida 33309, US

(72) Inventor/es: **Panasyuk, Anatoliy;**
Kramer, Andre;
Pedersen, Bradley Jay;
Stone, David Sean y
Treder, Terry

(74) Agente: **Elzaburu Márquez, Alberto**

ES 2 298 835 T3

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

Una sesión persistente y fiable que recorre de manera segura componentes de red utilizando un protocolo de encapsulación.

Campo de la técnica

El invento se refiere, en general, comunicaciones por red. Más particularmente, el invento se refiere a sistemas y métodos para restablecer comunicaciones de clientes recorriendo de manera segura componentes de red merced al uso de un protocolo de comunicaciones de encapsulamiento para proporcionar persistencia y fiabilidad de la sesión.

Información sobre antecedentes

Las comunicaciones por una red entre dos ordenadores, por ejemplo, un cliente y un servidor, pueden llevarse a la práctica utilizando una variedad de protocolos de comunicaciones conocidos. Típicamente, el cliente comunica con el servidor para descargar un contenido del servidor por la red. Por ejemplo, el servidor puede hospedar una o más aplicaciones accesibles para el cliente. Además, el cliente puede comunicar con el servidor a través de un equipo representante (proxy) que, típicamente, es una pasarela de seguridad, tal como un encaminador o un cortafuegos, a través del cual pasa el contenido del servidor. Además, el servidor puede incluir un cortafuegos para prohibir las comunicaciones no autorizadas hacia y desde el servidor. El cliente accede al servidor y a su contenido a través de la seguridad que ofrecen el representante y el cortafuegos del servidor. Sin embargo, con frecuencia la conexión de red que va al servidor a través de un representante, es susceptible de ser desbaratada. Por ejemplo, con frecuencia una conexión inalámbrica entre un cliente y un representante no es fiable. En otros casos, la conexión de red es intermitente. Como tal, puede perderse una conexión cuando se entra en un ascensor o en un túnel y sólo se la puede recuperar después de salir del ascensor o del túnel.

Si una sesión de comunicación establecida entre el cliente y el ordenador servidor termina de manera anormal, el cliente ha de restablecer, generalmente, la conexión iniciando una nueva sesión de comunicación. Para dar comienzo a la nueva sesión de comunicación, el usuario tiene retransmitir, típicamente, las credenciales de autenticación tales como el registro de entrada y la palabra de paso, al representante y al ordenador servidor, de forma que se le pueda autorizar al usuario la nueva sesión de comunicación. Esta retransmisión de las credenciales de autenticación de un usuario a través de múltiples sesiones de comunicaciones expone en forma repetida a las credenciales de autenticación de ese usuario, a la actuación de potenciales atacantes, disminuyendo por tanto el nivel de seguridad de las credenciales de autenticación. Además, si un atacante soslaya la seguridad del representante o del cortafuegos del servidor, puede acceder al contenido de éste sin tropezar con una seguridad adicional. Además, hacer que el usuario vuelva a introducir sus credenciales de autenticación es, con frecuencia, un proceso lento que puede tener como consecuencia la frustración y la sensación de incompetencia del usuario.

Cuando se lleva a cabo una comunicación mediante una conexión de red utilizando muchos protocolos corrientes, se pierden paquetes de datos cuando se interrumpe la conexión de red. Por ejemplo, cuando se comunica a través de una conexión de red TCP estándar, las memorias intermedias de datos son limpiadas, típicamente, al interrumpirse la conexión. Como tal, cuando se restablece la conexión de red, una aplicación ejecutada en la red, tal como una sesión de un usuario sobre un servidor, no es capaz de reanudarse en el punto en que se encontraba antes de la interrupción. Típicamente, se presenta un mensaje de error, aumentando la frustración del usuario hasta molestarle. Además, una comunicación por una red con muchos protocolos requiere el frecuente restablecimiento de la conexión de transporte. Por ejemplo, al utilizar HTTP, bien por sí solo o en conjunto con un protocolo representante, navegar por un sitio de la red a través de una conexión TCP estándar requiere, además de una nueva conexión HTTP para cada recurso, el cierre de una conexión previa con protocolo TCP/representante y la apertura de una nueva conexión con protocolo TCP/representante para cada recurso.

Así, es deseable proporcionar una técnica para restablecer una sesión de comunicación entre un ordenador cliente y un ordenador servidor sin requerir la transmisión repetida de las credenciales de autenticación del cliente y aumentando, sin embargo, la protección del servidor frente a un usuario no autorizado. Se necesitan sistemas y métodos mejorados para restablecer una sesión de comunicación entre un ordenador cliente y un ordenador servidor sin tener que transmitir repetidamente las credenciales de autenticación para pasar, de forma segura, por múltiples componentes de red.

La publicación US 2003/0163569 se refiere, en general, a un mecanismo de billete (grupo temporal de credenciales electrónicas que verifica la identidad de un cliente para un servicio particular) por salto para autenticar cada una de las conexiones múltiples entre un cliente y un servidor. La publicación WO/0223362 se refiere, en general, a un mecanismo que funciona en la interfaz de transporte de la pila de red que intercepta comunicaciones desde una aplicación y las transmite utilizando un protocolo de llamada a procedimientos remotos sobre un protocolo de movilidad de Internet, para establecer comunicaciones entre un servidor representante y cada sistema de extremo de móvil.

Sumario del invento

El presente invento se refiere a sistemas y métodos para volver a conectar un cliente, mediante una conexión persistente y fiable, con un servicio anfitrión, en los que la conexión pasa, de forma segura, a través de componentes

de red. La nueva conexión del cliente incluye restablecer la conexión del cliente con el servicio anfitrión y autenticar de nuevo al usuario del cliente ante el servicio anfitrión, incluyendo autenticar de nuevo una o más de las conexiones entre el cliente y el servicio anfitrión. Una conexión fiable y persistente con un servicio anfitrión es mantenida por uno o más primeros servicios de protocolo en nombre de un cliente. Los primeros servicios de protocolo garantizan que los datos comunicados entre el cliente y el servicio anfitrión, son almacenados en memorias intermedias y conservados durante cualquier interrupción de la conexión de red entre el cliente y el servicio anfitrión. Por ejemplo, una interrupción temporal en una conexión de red puede producirse cuando un cliente, tal como un cliente móvil, se desplaza entre diferentes puntos de acceso de la misma red, o cuando un cliente cambia entre redes (por ejemplo, de una red cableada a una red inalámbrica).

Además de mantener los datos en almacenamientos intermedios durante una interrupción de la red, el servicio de primer protocolo autentica de nuevo al cliente frente al servicio anfitrión cuando se restablece la conexión del cliente con el servicio de primer protocolo. Esto evita que el usuario del cliente tenga que introducir de nuevo sus credenciales de autenticación para restablecer la conexión con el servicio anfitrión. Además, cada una de las múltiples conexiones entre el cliente y el servicio anfitrión, por ejemplo, a través de un servicio de primer protocolo que actúa como representante, es autenticada de nuevo para proporcionar protección adicional de seguridad al acceder al servicio anfitrión. Tras autenticarse de nuevo, el servicio de primer protocolo restaura la conexión del cliente con el servicio anfitrión. En resumen, el presente invento permite restablecer una conexión de red entre un cliente y un servicio anfitrión para recorrer en forma segura componentes de red hasta llegar al servidor y sin que el usuario tenga que introducir de nuevo sus credenciales de autenticación.

En un aspecto, el presente invento se refiere a un método para reconectar a un cliente con un servicio anfitrión. El método comprende el paso de proporcionar una sesión de comunicación entre un cliente y un servicio anfitrión a través de una primera conexión entre el cliente y un servicio de primer protocolo, y una segunda conexión entre el servicio de primer protocolo y el servicio anfitrión. El método incluye, además, detectar una interrupción en una de las conexiones primera y segunda, y mantener la otra de las conexiones, primera y segunda. En otro paso del método, el servicio de primer protocolo obtiene un primer billete y un segundo billete y valida el primero para restablecer la conexión interrumpida. El servicio de primer protocolo valida el segundo billete para continuar el uso de la conexión mantenida, y enlaza la conexión restablecida con la conexión mantenida.

En una realización, el método comprende mantener la sesión de comunicación durante la rotura de la conexión interrumpida. En otra realización, el método comprende además generar uno de entre el primer billete y el segundo billete mediante, al menos, uno de entre el servicio de primer protocolo y la autoridad que emite el billete. El método puede incluir la validación, por parte de la autoridad que emite el billete, de al menos uno de entre el primer billete y el segundo billete.

En otra realización, el método comprende, además, autenticar al cliente frente a un servidor web y transmitir el primer billete al cliente mediante el servidor web. El método puede comprender, además, autenticar, mediante el servicio anfitrión al cliente al establecerse la sesión de comunicación. En una realización, el método incluye que el cliente transmita el primer billete al servicio de primer protocolo.

En otra realización, el servicio de primer protocolo comprende un servidor representante. En otra realización, el servicio de primer protocolo comprende una pasarela de seguridad. El método puede incluir, además, que el cliente y el servicio de primer protocolo se comuniquen empleando un primer protocolo que encapsule a un segundo protocolo, y que el servicio de primer protocolo y el servicio anfitrión se comuniquen utilizando el segundo protocolo.

En otra realización, el primer billete es válido para la primera conexión, y el segundo billete es válido para la segunda conexión. Opcionalmente, el segundo billete puede estar inhabilitado hasta que se valide el primer billete. En una realización, la conexión restablecida se enlaza con la conexión mantenida después de haberse validado el primer billete y el segundo billete.

En otra realización, la primera y/o la segunda conexión pueden comprender una pluralidad de conexiones realizadas a través de un nodo intermediario y uno o más primeros servicios de protocolo. El método puede incluir, también, generar un tercer billete para, al menos, una de la pluralidad de conexiones. El tercer billete puede ser válido para dicha al menos una de la pluralidad de conexiones.

En otro aspecto, el presente invento se refiere a un sistema para reconectar un cliente con un servicio anfitrión. El sistema comprende un cliente y un servicio de primer protocolo. El cliente establece una sesión de comunicación con un servicio anfitrión a través de una primera conexión. El servicio de primer protocolo establece la primera conexión con el cliente y una segunda conexión con el servicio anfitrión. El servicio de primer protocolo mantiene una conexión que comprende al menos una de entre la primera conexión y la segunda conexión. Además, el servicio de primer protocolo valida un primer billete para restablecer una conexión interrumpida de una de entre la primera conexión y la segunda conexión, y valida un segundo billete para utilizar la otra de entre la primera conexión y la segunda conexión. El sistema incluye, además, que el servicio de primer protocolo enlace la conexión restablecida con la conexión mantenida.

En una realización, el sistema comprende, además, una autoridad a cargo de los billetes que genera al menos uno de entre el primer billete y el segundo billete. En otra realización, el servicio de primer protocolo mantiene la sesión

de comunicación durante la rotura de la conexión interrumpida. En otra realización, el servicio de primer protocolo genera al menos uno de entre el primer billete y el segundo billete. El sistema puede incluir que la autoridad a cargo de los billetes valide, al menos, uno de entre el primer billete y el segundo billete.

- 5 En otra realización, el sistema comprende, además, un servidor web. El servidor web autentica al cliente y, en una realización, transmite el primer billete al cliente. En otra realización, el cliente transmite el primer billete al servicio de primer protocolo. En todavía otra realización, el servicio anfitrión autentica al cliente al establecerse la sesión de comunicación.
- 10 En una realización, el servicio de primer protocolo comprende un servidor representante y, en otra realización, el servicio de primer protocolo puede comprender una pasarela de seguridad. El sistema puede incluir que el cliente y el servicio de primer protocolo se comuniquen utilizando un primer protocolo que encapsule a un segundo protocolo, y que el servicio de primer protocolo y el servicio anfitrión se comuniquen utilizando el segundo protocolo.
- 15 En otra realización, el primer billete es válido para la primera conexión y el segundo billete es válido para la segunda conexión. Además, el segundo billete puede estar inhabilitado hasta validarse el primer billete. En una realización, el servicio de primer protocolo enlaza la conexión restablecida con la conexión mantenida, después de haberse validado el primer billete y el segundo billete.
- 20 En todavía otra realización, una de entre la primera conexión y la segunda conexión, comprende una pluralidad de conexiones realizadas a través de un nodo intermediario y uno o más primeros servicios de protocolo. El sistema incluye, además, generar un tercer billete para, al menos, una de la pluralidad de conexiones y, en una realización, el tercer billete es válido para, al menos, una de la pluralidad de conexiones.
- 25 Los detalles de diversas realizaciones del invento se establecen en los dibujos adjuntos y en la descripción siguiente.

Breve descripción de los dibujos

30 Los anteriores y otros objetos, aspectos, características y ventajas del invento resultarán más evidentes y pueden comprenderse mejor haciendo referencia a la siguiente descripción tomada en conjunto con los dibujos anejos, en los que:

35 la Fig. 1A es un diagrama de bloques de un sistema para ofrecer a un cliente una conexión fiable con un servicio anfitrión, de acuerdo con una realización ilustrativa del invento;

la Fig. 1B es un diagrama de bloques de un sistema para ofrecer a un cliente una conexión fiable con un servicio anfitrión, de acuerdo con otra realización ilustrativa del invento;

40 la Fig. 2A representa comunicaciones que tienen lugar por una red de acuerdo con una realización ilustrativa del invento;

la Fig. 2B representa comunicaciones que tienen lugar por una red de acuerdo con otra realización ilustrativa del invento;

45 la Fig. 3 ilustra un proceso para encapsular una pluralidad de protocolos secundarios dentro de un primer protocolo para comunicaciones sobre una red de acuerdo con una realización ilustrativa del invento;

la Fig. 4 es un diagrama de flujo que ilustra una realización del funcionamiento del sistema de comunicaciones de las Figs. 1A-1B de acuerdo con el invento;

50 la Fig. 5A es un diagrama de bloques de otra realización de un sistema de comunicaciones construido de acuerdo con el invento;

55 la Fig. 5B es un diagrama de flujo que ilustra una realización del funcionamiento del sistema de comunicaciones de la Fig. 5A, de acuerdo con el invento;

la Fig. 6A es un diagrama de bloques del sistema ilustrativo de la Fig. 1A, que incluye además componentes para volver a conectar al cliente con un servicio anfitrión, de acuerdo con una realización ilustrativa del invento;

60 la Fig. 6B es un diagrama de bloques del sistema ilustrativo de la Fig. 6A, que incluye además componentes para conectar inicialmente al cliente con un servicio anfitrión, de acuerdo con otra realización ilustrativa del invento;

la Fig. 6C es un diagrama de bloques del sistema ilustrativo de la Fig. 6B, que incluye además un componente para conectar inicialmente al cliente con el servicio anfitrión y para volver a conectar al cliente con el servicio anfitrión, de acuerdo con otra realización ilustrativa del invento;

65 la Fig. 6D es un diagrama de bloques de una realización alternativa del sistema de la Fig. 6C;

la Fig. 7 es un diagrama de flujo de un método para comunicaciones de red, de acuerdo con una realización ilustrativa del invento;

las Figs. 8A-8C son diagramas de flujo de un método para conectar a un cliente con una pluralidad de servicios anfitriones, de acuerdo con una realización ilustrativa del invento;

la Fig. 9 es un diagrama de flujo de un método para ofrecer a un cliente una conexión fiable con servicios anfitriones y para volver a conectar al cliente con los servicios anfitriones, de acuerdo con una realización ilustrativa del invento;

las Figs. 10A-10B son diagramas de flujo de un método para volver a conectar a un cliente con servicios anfitriones, de acuerdo con una realización ilustrativa del invento.

Descripción

En lo que sigue, se describen determinadas realizaciones del presente invento. Sin embargo, ha de hacerse notar, de forma expresa, que el presente invento no está limitado a estas realizaciones, sino que la intención es que las adiciones y modificaciones a lo que expresamente se describe en esta memoria, queden incluidas, también, dentro del alcance del invento. Además, ha de comprenderse que las características de las diversas realizaciones descritas en este documento, no son mutuamente exclusivas y pueden existir en varias combinaciones y permutaciones, aún cuando tales combinaciones y permutaciones no se incluyan aquí expresamente, sin apartarse por ellos del espíritu ni del alcance del invento.

La realización ilustrativa del presente invento proporciona sistemas y métodos para establecer una conexión fiable y persistente entre un cliente y un servicio anfitrión, y para volver a establecer la conexión cuando se produce una interrupción de la misma. Un cliente establece una sesión de comunicación con un servicio anfitrión a través de una primera conexión entre un cliente y un servicio de primer protocolo y una segunda conexión entre el servicio de primer protocolo y el servicio anfitrión. El cliente comunica con el servicio de primer protocolo empleando un primer protocolo y el servicio de primer protocolo comunica con el servicio anfitrión utilizando un segundo protocolo. El segundo protocolo se emplea para comunicación del cliente con el servicio de primer protocolo, encapsulado dentro de las comunicaciones del primer protocolo. Cuando se detecta una interrupción en la primera conexión o en la segunda conexión, el servicio de primer protocolo restablece la conexión interrumpida al tiempo que conserva la conexión que no se ha interrumpido. La conexión interrumpida se enlaza con la conexión mantenida con el fin de volver a conectar al cliente con el servicio anfitrión.

Además, la realización ilustrativa del presente invento proporciona sistemas y métodos para recorrer en forma segura componentes de red al establecer una conexión de un cliente con un servicio anfitrión y al volver a establecer nuevamente dicha conexión. El servicio de primer protocolo puede actuar como representante entre el cliente y el servicio anfitrión y, como tal, puede comprender una pasarela de seguridad. El servicio de primer protocolo obtiene un primer billete y un segundo billete a partir de una autoridad a cargo de los billetes. El primer billete se utiliza para validar la conexión entre el cliente y el servicio de primer protocolo, y el segundo billete se utiliza para validar la conexión entre el servicio de primer protocolo y el servicio anfitrión. El segundo billete puede estar inhabilitado hasta la validación del primer billete. El servicio de primer protocolo valida el primer billete restableciendo o manteniendo el uso de la primera conexión, y el segundo billete restableciendo o manteniendo el uso de la segunda conexión. Cuando se validan el primero y el segundo billetes y se restablecen las conexiones, el servicio de primer protocolo enlaza la primera conexión con la segunda conexión para mantener la sesión de comunicación del cliente con el servicio anfitrión. Pueden generarse y validarse billetes adicionales para restablecer o mantener conexiones adicionales del usuario, o “saltos”, entre el cliente y el servicio anfitrión. De esta forma, se valida cada conexión, o “salto”, entre el cliente y el servicio anfitrión.

Haciendo referencia a la Fig. 1A, en general, el invento se refiere a comunicaciones de redes y puede tener una utilidad particular a la hora de ofrecer a un cliente una conexión fiable con un servicio anfitrión. En una visión global, un sistema 100 para comunicaciones de red incluye un cliente 108 (por ejemplo, un primer dispositivo de ordenador) en comunicación con un servicio 112 de primer protocolo (por ejemplo, un segundo dispositivo de ordenador), por una red 104. También se incluyen en el sistema 100 una pluralidad de servicios anfitriones 116a-116n residentes en un nodo anfitrión 188 (por ejemplo, un tercer dispositivo de ordenador) que están en comunicación con el servicio 112 de primer protocolo y, a través del servicio 112 de primer protocolo y por la red 104, con el cliente 108. Alternativamente, en otra realización ilustrativa del invento, y con referencia ahora a la Fig. 1B, el servicio 112 de primer protocolo y los servicios anfitriones 116a-116n no están incorporados en dispositivos de ordenador separados, como se muestra en la Fig. 1A, sino que están incorporados en el mismo dispositivo de ordenador tal como, por ejemplo, el nodo anfitrión 118a. En la Fig. 1B, los servicios anfitriones 116a-116n comunican con el servicio 112 de primer protocolo por la red 104'. El sistema 100 puede incluir uno, dos o cualquier número de nodos anfitriones 118a-118n.

En una realización, las redes 104 y 104' son redes separadas, como en la Fig. 1B. Las redes 104 y 104' pueden ser la misma red 104, como se muestra en la Fig. 1A. En una realización, la red 104 y/o la red 104' están constituidas, por ejemplo, como redes de área local (LAN), tales como una Intranet corporativa o una red de área amplia (WAN), tal como Internet o la World Wide Web. El cliente 108, el servicio 112 de primer protocolo, los servicios anfitriones 116a-116n, y/o los nodos anfitriones 118a-118n, pueden conectarse a las redes 104 y/o 104' a través de una variedad

ES 2 298 835 T3

de conexiones que incluyen, aunque sin limitarse a ellas, líneas estándar de telefonía, enlaces LAN o WAN (por ejemplo, 802, 11, T1, T3, 56kb, X.25), conexiones de banda ancha (por ejemplo, ISDN, retransmisión de tramas, ATM) conexiones inalámbricas o combinaciones de cualesquiera o de todas las anteriores.

5 El cliente 108 está en comunicación con el servicio 112 de primer protocolo por el canal 135 de comunicaciones entre cliente y servicio de primer protocolo y, también, está en comunicación con el servidor 120 de red mediante el canal 140 de comunicaciones entre cliente y servidor web. El servicio 112 de primer protocolo se encuentra en comunicación con la autoridad 136 a cargo de los billetes a través de un canal 145 de comunicaciones entre el servicio de primer protocolo y dicha autoridad, y el servidor web 120 está en comunicación con la autoridad 136 a cargo de los billetes a través de un canal 150 de comunicaciones entre el servidor de red y la citada autoridad. El servicio 112 de primer protocolo está, también, en comunicación con el nodo anfitrión 118 por los canales 124a-124n de comunicaciones entre el servicio de primer protocolo y el servidor. En otra realización, el servidor web 120 puede comunicarse con el nodo anfitrión 118 a través de un canal 155 de comunicaciones agente-servidor. Similarmente, el nodo anfitrión 118 puede comunicarse con la autoridad 136 a cargo de los billetes a través de un canal 157 de comunicaciones billetes-servidor. En una realización, los respectivos canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157 se establecen sobre la red 104.

Realizaciones ilustrativas de los canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157, incluyen líneas estándar de telefonía, enlaces LAN o WAN (por ejemplo, T1, T3, 56kb, X.25), conexiones de banda ancha (por ejemplo, ISDN, retransmisión de tramas, ATM) y conexiones inalámbricas. Las conexiones por los canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157 pueden establecerse utilizando una variedad de protocolos de comunicaciones (por ejemplo, HTTP, HTTPS, TCP/IP, IPX, SPX, NetBIOS, Ethernet, RS232, protocolo MAPI (interfaz de programación para aplicaciones de mensajería), RTSP (protocolo de reproducción directa en tiempo real), RTSPU (protocolo de reproducción directa en tiempo real utilizado para esquema de protocolo de datagramas de usuario), el protocolo PNM (Progressive Networks Multimedia) desarrollado por RealNetworks, Inc., de Seattle, WA, EE.UU., protocolo MMS (especificación para la fabricación de mensajes, y conexiones asíncronas directas.

En otro aspecto, la Fig. 1A muestra un diagrama de bloques de una realización de un sistema 100 de comunicaciones para garantizar la entrega de contenido. En una realización, el servicio 112 de primer protocolo comprende un representante 115 y el sistema 100 incluye un servidor web 120, y una autoridad 136 a cargo de los billetes. El sistema 100 incluye, también, dos cortafuegos 160, 161 que prohíben las comunicaciones no autorizadas hacia/desde el nodo anfitrión 118. La red entre los cortafuegos 160, 161 se denomina, con frecuencia, DMZ ("zona desmilitarizada") 130. En una realización, la DMZ 130 incluye el servicio 112 de protocolo de billetes, que comprende un representante 115 y el servidor web 120.

La DMZ 130 separa los servicios anfitriones 116a-116n de los componentes (por ejemplo, el servicio 112 de primer protocolo) del sistema 100 a los que pueden acceder individuos no autorizados. Como se ha descrito anteriormente, la DMZ 130 está definida por dos cortafuegos 160, 161 que prohíben las comunicaciones no autorizadas. El primer cortafuegos 160 y el segundo cortafuegos 161 aplican, cada uno, un conjunto de normas para determinar qué mensajes pueden atravesar la DMZ 130. En una realización, el primer cortafuegos 160 y el segundo cortafuegos 161 aplican el mismo conjunto de normas. Alternativamente, el primer cortafuegos 160 y el segundo cortafuegos 161 pueden aplicar diferentes conjuntos de normas. Cada cortafuegos 160, 161, puede ser un encaminador, un ordenador o cualquier otro dispositivo de control de acceso a la red. En otra realización, el sistema 100 incluye uno de los cortafuegos 160, 161 o carece de ellos. En otra realización, uno de los cortafuegos 160, 161 está desplegado en el nodo anfitrión 118. En otra realización (no mostrada), uno o más de los cortafuegos 160, 161, están desplegados en un nodo intermediario.

En una realización, el servicio 112 de primer protocolo incluye un representante 115 que comprende una pasarela de seguridad a través de la cual deben pasar los mensajes por el canal 135 de comunicaciones entre cliente y servicio de primer protocolo. En una realización, el cortafuegos 160 de la red rechaza cualquier mensaje entrante desde el canal 135 de comunicaciones entre cliente y servicio de primer protocolo que no tengan el servicio 112 de primer protocolo como su destino. De igual manera, el cortafuegos 160 de la red rechaza cualquier mensaje saliente para el canal 135 de comunicaciones entre cliente y servicio de primer protocolo, a no ser que su fuente sea el servicio 112 de primer protocolo. Si bien se ilustra como un representante 115 del servicio 112 de primer protocolo, la pasarela de seguridad puede ser, alternativamente, un encaminador, un cortafuegos, un repetidor o cualquier componente de red que pueda ofrecer la seguridad necesaria. En otra realización, el representante 115 es un componente de red separado del servicio 112 de primer protocolo que puede ejecutarse en el mismo dispositivo de ordenador que el servicio 112 de primer protocolo o en un dispositivo de ordenador diferente. Por ejemplo, en la Fig. 1B el representante 115 está separado del servicio 112 de primer protocolo. El representante 115 está en la DMZ 130 con el servidor web 120. En cada uno de los nodos anfitriones 118a-118n se ejecutan múltiples instancias del servicio 112 de primer protocolo. Cada servicio 112 de primer protocolo comunica con el representante 115 por el canal 135 de comunicaciones, que es el canal 135 de comunicaciones entre cliente y servicio de primer protocolo. En este caso, el componente representante 115 es un intermediario para permitir el paso seguro de comunicaciones entre el cliente 108 y el servicio 112 de primer protocolo.

La red 104 puede ser una red de área local (LAN), una red de área amplia (WAN) o una red de redes tal como Internet o la World Wide Web (es decir, la web). Cada uno de los respectivos canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157 puede ser parte de diferentes redes. Por ejemplo, el canal 135 de comunicaciones entre cliente y servicio de primer protocolo puede pertenecer a una primera red (por ejemplo, la World Wide Web) y el

ES 2 298 835 T3

canal 140 de comunicaciones entre cliente y servidor web puede pertenecer a una segunda red (por ejemplo, una extranet segura o una red privada virtual (VPN)). En otras realizaciones, la red 104 abarca tanto la DMZ 230 como la agrupación centralizada 169 de servidores y en todos ellos se utiliza el mismo protocolo de comunicaciones. En algunas realizaciones, ningún cortafuegos 160 separa el servicio 112 de primer protocolo y el servidor web 120 del nodo anfitrión 118 y la autoridad 136 a cargo de los billetes.

Realizaciones ilustrativas de los canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157 incluyen líneas estándar de telefonía, enlaces LAN o WAN (por ejemplo, T1, T3, 56kb, X.25), conexiones de banda ancha (por ejemplo, ISDN, retransmisión de tramas, ATM) y conexiones inalámbricas. Las conexiones por los canales de comunicaciones 124a-124n, 135, 140, 145, 150, 155, 157 pueden establecerse utilizando una variedad de protocolos de comunicaciones (por ejemplo, HTTP, HTTPS, TCP/IP, IPX, SPX, NetBIOS, Ethernet, RS232, protocolo MAPI (interfaz de programación para aplicaciones de mensajería), RTSP (protocolo de reproducción directa en tiempo real), RTSPU (protocolo de reproducción directa en tiempo real utilizado para esquema de protocolo de datagramas de usuario), el protocolo PNM (Progressive Networks Multimedia) desarrollado por RealNetworks, Inc., de Seattle, WA, EE.UU., protocolo MMS (especificación para la fabricación de mensajes, y conexiones asíncronas directas.

El cliente 108 puede ser cualquier puesto de trabajo, ordenador de sobremesa, ordenador portátil, ordenador de mano, teléfono móvil, terminal inteligente o no inteligente, ordenador de red, dispositivo inalámbrico, aparato para acceso a información, miniordenador, ordenadores centrales u otras formas de dispositivo de computación o de comunicaciones que sea capaz de comunicarse y dotado de suficiente potencia de tratamiento y de suficiente capacidad de memoria para llevar a cabo las operaciones descritas en este documento. Además, el cliente 108 puede ser un ordenador cliente de sobremesa, local, conectado en una red local 104 o puede ser un dispositivo de presentación cliente remoto de una red 104' separada. El cliente 108 puede incluir, por ejemplo, un dispositivo de presentación visual (por ejemplo, un monitor de ordenador), un dispositivo de entrada de datos (por ejemplo, un teclado), un almacenamiento persistente y/o volátil (por ejemplo, una memoria de ordenador), un procesador y un ratón. Los sistemas operativos soportados por el cliente 108 pueden incluir cualquier miembro de la familia de sistemas operativos WINDOWS, de Microsoft Corporation, de Redmond, Washington, EE.UU., el sistema operativo Macintosh, el sistema operativo Java y diversas variedades de Unix (por ejemplo, Solaris, SunOS, Linux, HP-UX, A/IX y distribuciones basadas en BSD) o cualquier otro sistema operativo capaz de soportar al cliente 108 cuando ejecuta las operaciones descritas en esta memoria.

En una realización, el cliente 108 incluye un navegador web 162, tal como INTERNET EXPLORER, desarrollado por Microsoft Corporation, de Redmond, Washington, EE.UU., para conexión con la web. En otra realización, el navegador 162 utiliza el existente soporte de SSL (capa de conexión segura) para establecer el canal 140 de comunicaciones seguro entre cliente y servidor web, con el servidor web 120. SSL es un protocolo seguro desarrollado por Netscape Communication Corporation, de Mountain View, California, EE.UU., y en la actualidad constituye un estándar promulgado por la Internet Engineering Task Force (IETF).

En algunas realizaciones, como se muestra en las Figs. 1A y 1B, un agente cliente 128 está incluido dentro del cliente 108. El agente cliente 128 puede ser utilizado para establecer e intercambiar comunicaciones con el servicio anfitrión 116a-116n por el canal de comunicaciones 135 entre cliente y servicio de primer protocolo. El agente cliente 128 puede incorporarse, por ejemplo, como un programa de software y/o como un dispositivo de hardware tal como, por ejemplo, un ASIC (circuito integrado específico para aplicaciones) o una FPGA (agrupación de puertas lógicas programables en el campo). El agente cliente 128 puede utilizar cualquier tipo de protocolo y puede ser, por ejemplo, un agente cliente FFTP, un agente cliente FTP, un agente cliente Oscar o un agente cliente Telnet. En una realización, el agente cliente 128 es un cliente ICA, desarrollado por Citrix Systems, Inc., de Fort Lauderdale, Florida, EE.UU. y denominado en lo que sigue cliente ICA 128. Otras realizaciones del agente cliente 128 incluyen un cliente RDP, desarrollado por Microsoft Corporation, de Redmond, Washington, EE.UU., un cliente de entrada de datos en una aplicación cliente/servidor tradicional, un control ActiveX, o un pequeño programa Java. En algunas realizaciones, el agente cliente 128 está configurado, en sí mismo, para comunicarse utilizando el primer protocolo. En algunas realizaciones (no mostradas), el cliente 108 incluye una pluralidad de agentes cliente 128a-128n, cada uno de los cuales comunica con un servicio anfitrión 116a-116n, respectivamente. Además, la salida de una aplicación en ejecución en el servicio anfitrión 116a-116n puede presentarse en el cliente 108 a través, por ejemplo, del agente cliente 128 o del navegador web 162.

En otra realización, se configura un agente cliente autónomo para permitir que el cliente 108 se comunique utilizando el primer protocolo. El agente cliente autónomo puede estar incorporado dentro del cliente 108 o, alternativamente, el agente cliente autónomo puede estar separado del cliente 108. El agente cliente autónomo es, por ejemplo, un representante anfitrión local. En general, el agente cliente autónomo puede llevar a la práctica cualquiera de las funciones descritas en este documento en relación con el agente cliente 128.

Similarmemente, con referencia a la Fig. 1A, cada uno de entre el servicio 112 de primer protocolo y los servicios anfitriones 116a-116n puede estar previsto en cualquier dispositivo de computación que sea capaz de comunicarse y que tenga una capacidad de memoria y una potencia de tratamiento suficientes para llevar a cabo las operaciones descritas en este documento. Alternativamente, cuando la funcionalidad del servicio 112 de primer protocolo y de los servicios 116a-116n están incorporadas en el mismo dispositivo de computación, tal como, por ejemplo, uno de los nodos anfitrión 118a-118n, como en la Fig. 1B, el servicio 112 de primer protocolo y/o los servicios anfitriones 116a-116n pueden incorporarse en la práctica como un programa de software que se ejecuta en un ordenador para

finés generales y/o como un dispositivo de hardware para fines especiales tal como, por ejemplo, un ASIC o una FPGA.

De manera similar al cliente 108, cada uno de los nodos anfitriones 118a-118n puede estar constituido por cualquier dispositivo de computación descrito en lo que antecede (por ejemplo, un ordenador personal) que sea capaz de comunicarse y que tenga capacidad de memoria y potencia de tratamiento suficientes para llevar a cabo las operaciones descritas en este documento. Cada uno de los nodos anfitriones 118a-118n puede establecer comunicación por los canales de comunicaciones 124a-124n utilizando una variedad de protocolos de comunicaciones (por ejemplo, ICA, HTTP, TCP/IP e IPX, SPX, NetBIOS, Ethernet, RS232 y conexiones asíncronas directas).

En una realización, cada uno de los servicios anfitriones 116a-116n aloja uno o más programas de aplicaciones que están disponibles remotamente para el cliente 108. Las aplicaciones puestas a disposición del cliente 108 para que éste las utilice, pueden denominarse aplicaciones publicadas. El mismo programa de aplicación puede estar alojado en uno o en cualquier número de servicios anfitriones 116a-116n. Ejemplos de tales aplicaciones incluyen programas de tratamiento de textos, tales como MICROSOFT WORD y programas de hojas de cálculo, tales como MICROSOFT EXCEL, disponibles ambos de Microsoft Corporation, de Redmond, Washington, EE.UU. Otros ejemplos de programas de aplicaciones que pueden alojarse en cualquiera o en todos los servicios anfitriones 116a-116n, incluyen programas de información financiera, programas de registro de clientes, programas que proporcionen información de soporte técnico, aplicaciones de bases de datos de clientes, y gestores de conjuntos de aplicaciones. Además, en una realización, uno o más de los servicios anfitriones 116a-116n está constituido por un servidor de reproducción directa de audio/vídeo que proporciona audio y/o vídeo en reproducción directa al cliente 108. En otra realización, los servicios anfitriones 116a-116n incluyen servidores de ficheros que le proporcionan al cliente 108 todo tipo de ficheros. En una realización, los servicios anfitriones 116a-116n pueden comunicarse con el cliente 108 utilizando un protocolo de presentación tal como ICA, de Citrix Systems, inc., de Fort Lauderdale, Florida, EE.UU., o RDP, de Microsoft Corporation, de Redmond, Washington, EE.UU.

En otra realización, el nodo anfitrión 118 es miembro de una agrupación centralizada 169 de servidores, o red de servidores, que es un grupo lógico constituido por uno o más servidores administrados como una sola entidad. En una realización, una agrupación centralizada 169 de servidores incluye múltiples nodos anfitriones 118a-118n (en general, 118). Aunque la realización mostrada en la Fig. 1B tiene tres nodos anfitriones 118a-118n, la agrupación centralizada 169 de servidores puede tener cualquier número de nodos anfitriones 118, o servidores. En otras realizaciones, la agrupación centralizada 169 de servidores es una red protegida inaccesible para individuos no autorizados, tal como una Intranet corporativa, una VPN (red privada virtual) o una extranet segura. Además, los servidores que constituyen la agrupación centralizada 169 de servidores pueden comunicarse por cualquiera de las redes descritas en lo que antecede (por ejemplo, WAN, LAN) empleando cualquier a de los protocolos descritos.

La autoridad 136 a cargo de los billetes que, en la realización mostrada en la Fig. 1A es parte de la agrupación centralizada 169 de servidores, emite uno o más billetes para autenticar al cliente 108. En particular, la autoridad 136 a cargo de los billetes permite la autenticación del cliente 108 por un canal de comunicaciones (es decir, el canal de comunicaciones 140 cliente-servidor web), basándose en las credenciales de autenticación. La autoridad 136 a cargo de los billetes permite, además, que el cliente 108 sea autenticado para otro canal de comunicaciones (es decir, el canal de comunicaciones 135 cliente-servicio de primer protocolo) sin que el cliente 135 haya de proporcionar repetidamente sus credenciales de autenticación en el otro canal de comunicaciones.

En una realización, la autoridad 136 a cargo de los billetes es un componente de red autónomo. En otras realizaciones, una autoridad 136 a cargo de los billetes, modular, está constituida por un módulo de software que reside en uno o más de los nodos anfitriones 118. Por ejemplo, puede existir una autoridad 136 a cargo de los billetes para cada nodo anfitrión 116a-116n, como se muestra en la Fig. 1B. En esta realización, el servidor web 120 puede comunicarse con la autoridad 136 a cargo de los billetes y/o con el nodo anfitrión 118 por el canal 155 de comunicaciones agente-servidor. En otra realización, la autoridad 136 a cargo de los billetes puede residir en un nodo intermediario, separado de cualquiera de los nodos anfitriones 118a-118n.

En una realización, la autoridad 136 a cargo de los billetes genera un primer billete y un segundo billete. En algunas realizaciones, los billetes son, ambos, para la ocasión. En otras realizaciones, los billetes son generados utilizando un generador de números aleatorios para cifrado en el que se ha sembrado una adecuada aleatoriedad. El primer billete es transmitido al cliente 108 y se utiliza para establecer una primera sesión de comunicaciones entre el cliente 108 y el servicio 112 de primer protocolo. El segundo billete es transmitido al servicio 112 de primer protocolo y es utilizado para establecer una segunda sesión de comunicaciones entre el servicio 112 de primer protocolo y el nodo anfitrión 118.

En una realización, el servidor web 120 entrega páginas web al cliente 108. El servidor web 120 puede ser cualquier ordenador personal (por ejemplo, un ordenador Macintosh, un ordenador personal con microprocesador Intel, desarrollado por Intel Corporation, de Santa Clara, California, EE.UU., un ordenador personal con un microprocesador AMD, desarrollado por Advanced Micro Devices, inc., de Sunnyvale, California, EE.UU., etc.), un terminal basado en Windows, un ordenador de red, un dispositivo inalámbrico (por ejemplo, un teléfono celular), un aparato para acceso a la información, Power PC RISC, dispositivo X, puesto de trabajo, miniordenador, ordenador central, asistente digital personal u otro dispositivo de comunicaciones que sea capaz de establecer con el cliente 108 el canal 140 de comunicaciones, seguro, entre cliente y servidor web.

ES 2 298 835 T3

En otra realización, el servidor web 120 proporciona un portal corporativo, denominado también portal de información empresarial, para el cliente 108. Los portales empresariales son sitios web de una compañía que agregan, personalizan y sirven aplicaciones, datos y contenidos a los usuarios, al tiempo que ofrecen herramientas de gestión para organizar y utilizar la información de manera más eficaz. En otras realizaciones, el servidor web 120 proporciona un portal web, o portal de Internet, para el cliente 108. Un portal web es similar a un portal corporativo pero, típicamente, no incluye información específica sobre el negocio.

En una realización, un usuario del cliente 108 emplea el navegador web 162 para autenticar al usuario frente al servidor web 120. En una realización, el cliente 108 transmite las credenciales del usuario, tales como información sobre registro y clave de paso, al servidor web 120. El servidor web 120 verifica que el usuario tiene acceso a la red 169 de servidores.

En otra realización, el navegador web 162 utiliza SSL para establecer el canal 140 de comunicaciones cliente-servidor web seguro. El navegador web 162 puede conectarse, alternativamente, con el servidor web 120 por el canal 140 de comunicaciones cliente-servidor web, utilizando otros protocolos de seguridad tales como, el protocolo seguro de transferencia de hipertexto (SHTTP) desarrollado por Terisa Systems, de Los Altos, CA., EE.UU.; HTTP sobre SSL (HTTPS), la tecnología de comunicaciones privadas (PCT) desarrollada por Microsoft Corporation, de Redmond, Washington, EE.UU., y la norma de seguridad del nivel de transporte (TLS) promulgada por la Internet Engineering Task Force (IETF). En una realización, el servidor web 120 transmite un portal web o portal empresarial, como se ha descrito anteriormente, al cliente 108 al producirse la validación del usuario para permitir que el cliente 108 solicite que una aplicación o un servidor de sobremesa, por ejemplo, sea presentado remotamente en el cliente 108.

El canal 140 de comunicaciones cliente-servidor web es cualquier canal seguro de comunicaciones. En algunas realizaciones, las comunicaciones por el canal 140 son cifradas. En determinadas, de estas realizaciones, el cliente 108 y el servidor web 120 pueden comunicarse utilizando la capa de conexión segura (SSL) del protocolo de transferencia de hipertexto (HTTPS). Alternativamente, el cliente 108 y el servidor web 120 pueden utilizar otras técnicas de cifrado, tales como técnicas de cifrado simétrico, para proteger las comunicaciones.

Además, en una realización, el canal 135 de comunicaciones entre cliente y servicio de primer protocolo puede establecerse utilizando, por ejemplo, un protocolo de servicios de presentación tal como el protocolo ICA (de arquitectura de cálculo independiente), fabricado por Citrix Systems, Inc., de Fort Lauderdale, Florida, EE.UU. El ICA es un protocolo para servicios de presentación con fines generales, diseñado para ejecutarse sobre protocolos de red estándar industriales tales como TCP/IP, IPX/SPX, NetBEUI, usando protocolos de transporte estándar en la industria tales como ISDN, repetición de tramas y ATM (modo de transferencia asíncrono). El protocolo ICA permite canales virtuales, que son conexiones de transmisión orientadas a sesiones que pueden ser utilizadas por un código de capa de aplicaciones para emitir órdenes para intercambiar datos. En otras realizaciones, el canal 135 de comunicaciones entre cliente y servicio de primer protocolo, puede establecerse empleando el protocolo Thin X o el protocolo de presentación remota (RDP) creado por Microsoft Corporation, de Redmond, Washington, EE.UU.

Si bien se ha descrito estableciendo una primera sesión de comunicaciones entre el cliente 108 y el servicio 112 de primer protocolo y una segunda sesión de comunicaciones entre el servicio 112 de primer protocolo y el nodo anfitrión 118, la sesión de comunicaciones puede verse como una única sesión de comunicaciones lógica entre el cliente 108 y el servicio anfitrión 116.

Refiriéndonos todavía a las realizaciones ilustrativas de las Figs. 1A y 1B, el cliente 108 está configurado para establecer una conexión 135 entre el cliente 108 y un servicio 112 de primer protocolo por la red 104 utilizando un primer protocolo. Por su parte, el servicio 112 de primer protocolo está configurado para aceptar la conexión 135. El cliente 108 y el servicio 112 de primer protocolo pueden, por tanto, comunicarse uno con otro utilizando el primer protocolo como se describe en lo que sigue con referencia a las Figs. 2A-2B y a la Fig. 3.

Como se describe también, con mayor detalle, más adelante, el servicio 112 de primer protocolo está configurado, en una realización, para comunicarse utilizando el primer protocolo. El servicio 112 de primer protocolo está configurado para establecer una conexión 124a-124n entre el servicio 112 de primer protocolo y el servicio anfitrión 116a-116n, respectivamente. Por ejemplo, el servicio 112 de primer protocolo puede establecer una conexión 124a entre el servicio 112 de primer protocolo y un servicio anfitrión 116a y una conexión 124b entre el servicio 112 de primer protocolo y otro servicio anfitrión 116b. En una realización, el servicio 108 de primer protocolo establece por separado tales conexiones 124a-124n (es decir, el servicio 112 de primer protocolo establece una conexión cada vez). En otra realización, el servicio 112 de primer protocolo establece simultáneamente dos o más de tales conexiones 124a-124n.

En todavía otra realización, el servicio 112 de primer protocolo puede establecer y mantener concurrentemente múltiples conexiones 124a-124n. El servicio 112 de primer protocolo está configurado para proporcionar dos o más conexiones 124a-124n sin interrumpir la conexión 135 con el cliente 108. Por ejemplo, el servicio 112 de primer protocolo puede configurarse para establecer la conexión 124a entre el servicio 112 de primer protocolo y el servicio anfitrión 116a cuando un usuario del cliente 108 solicita la ejecución de un primer programa de aplicación residente en el servicio anfitrión 116a. Cuando el usuario da por terminada la ejecución del primer programa de aplicación e inicia la ejecución de un segundo programa de aplicación residente, por ejemplo, en el servicio anfitrión 116b, el servicio 112 de primer protocolo está configurado, en una realización, para interrumpir la conexión 124a y establecer

la conexión 124b entre el servicio 112 de primer protocolo y el servicio anfitrión 116b sin interrumpir la conexión 135 entre el servicio 112 de primer protocolo y el cliente 108.

El servicio 112 de primer protocolo y los servicios anfitriones 116a, 116n, pueden comunicarse por las conexiones 124a, 124n, respectivamente, empleando cualquiera de una variedad de protocolos secundarios, incluyendo, aunque sin limitarse a ellos, HTTP, FTP, Oscar, Telnet, el protocolo de presentación remota ICA de Citrix Systems, Inc., de Fort Lauderdale, Florida, EE.UU., y/o el protocolo RDP de presentación remota de Microsoft Corporation, de Redmond, Washington, EE.UU. Por ejemplo, el servicio 112 de primer protocolo y el servicio anfitrión 116a pueden comunicarse por la conexión 124a utilizando el protocolo de presentación remota ICA, mientras que el servicio 112 de primer protocolo y el servicio anfitrión 116b pueden comunicarse mediante la conexión 124b utilizando el protocolo de presentación remota RDP.

En una realización, el protocolo secundario utilizado para comunicar entre el servicio 112 de primer protocolo y un servicio anfitrión 116 tal como, por ejemplo, el protocolo de presentación remota ICA, incluye una pluralidad de canales virtuales. Un canal virtual es una conexión de transmisión orientada a una sesión, que es utilizada por el código de capa de aplicaciones para emitir órdenes para el intercambio de datos. Por ejemplo, cada uno de la pluralidad de canales virtuales puede incluir una pluralidad de paquetes de protocolo que habilitan la funcionalidad en el cliente remoto 108. En una realización, uno de la pluralidad de canales virtuales incluye paquetes de protocolo para transmitir órdenes de pantalla gráfica desde un servicio anfitrión 116, a través del servicio 112 de primer protocolo, al cliente 108, para hacer que el cliente 108 visualice una interfaz gráfica de usuario. En otra realización, uno de la pluralidad de canales virtuales incluye paquetes de protocolo para transmitir órdenes a la impresora desde un servicio anfitrión 116, a través del servicio 112 de primer protocolo, al cliente 108, para hacer que en el cliente 108 se imprima un documento.

En otra realización, el primer protocolo es un protocolo de tunelización. El servicio 112 de primer protocolo encapsula una pluralidad de protocolos secundarios, cada uno de ellos utilizado para comunicación entre uno de los servicios anfitriones 116a-116n y el servicio 112 de primer protocolo, dentro del primer protocolo. Como tales, los servicios anfitriones 116a-116n y el servicio 112 de primer protocolo se comunican con el cliente 108 a través de la pluralidad de protocolos secundarios. En una realización, el primer protocolo es, por ejemplo, un protocolo de transporte de nivel de aplicaciones capaz de tunelizar los múltiples protocolos secundarios por una conexión TCP/IP.

Refiriéndonos a la Fig. 2A, las comunicaciones entre el cliente 108 y el servicio 112 de primer protocolo a través de la conexión 135, adoptan la forma de una pluralidad de protocolos secundarios 200a-200n (por ejemplo, HTTP, FTP, Oscar, Telnet, ICA y/o RDP) encapsulados dentro de un primer protocolo 204. Esto se indica mediante la situación de los protocolos secundarios 200a-200n dentro del primer protocolo 204. Cuando no se ha solicitado una comunicación segura, el primer protocolo 204 puede comunicarse, como se ilustra en la Fig. 2A, por una conexión 208 TCP/IP no segura.

Refiriéndonos ahora a la Fig. 2B, se utiliza una comunicación segura, el primer protocolo 204 se comunica por una conexión cifrada tal como, por ejemplo, una conexión TCP/IP 212 asegurada mediante el uso de un protocolo seguro 216 tal como el SSL (capa de conexión segura). El SSL es un protocolo seguro desarrollado primero por Netscape Communication Corporation, de Mountain View, California, EE.UU. y, ahora, constituye un estándar promulgado por la Internet Engineering Task Force (IETF) como protocolo TLS (de seguridad de capa de transporte) y descrito en la RFC-2246 del IETF.

Así, la pluralidad de protocolos secundarios 200a-200n se comunican dentro del primer protocolo 204 con (Fig. 2B) o sin (Fig. 2A) un protocolo seguro 216 por la conexión 135. Los protocolos secundarios que pueden utilizarse para comunicación por las conexiones 124a-124n incluyen, aunque sin limitarse a ellos, HTTP, FTP, Oscar, Telnet, ICA y RDP. Además, en una realización, al menos uno de los protocolos secundarios, como se ha descrito en lo que antecede, incluye una pluralidad de canales virtuales, cada uno de los cuales puede incluir una pluralidad de paquetes de protocolo que permitan la funcionalidad en el cliente remoto 108. Por ejemplo, en una realización, un servicio anfitrión 116a es un servidor web, que comunica con el servicio 112 de primer protocolo por la conexión 124a utilizando el protocolo HTTP y otro servicio anfitrión 116b es un servidor de aplicaciones, que comunica con el servicio 112 de primer protocolo por la conexión 124b utilizando el protocolo ICA. El servicio anfitrión 116b genera paquetes de protocolo para transmitir órdenes de pantalla gráfica al cliente 108, para hacer que el cliente 108 visualice una interfaz gráfica de usuario, y paquetes de protocolo para transmitir órdenes de impresión al cliente 108, para hacer que se imprima un documento en el cliente 108.

Otro aspecto del presente invento reside en que el método y en los sistemas descritos en esta memoria reducen el número de veces que se abren y se cierran la conexiones de red. En una realización, el primer protocolo 204 permite que las conexiones 200a-200n de protocolo secundario tunelizadas en él tales como, por ejemplo, una conexión HTTP 200n, sean abiertas y/o cerradas repetidamente, sin requerir también que la conexión de transporte por la que se comunica el primer protocolo 204 (por ejemplo, la conexión TCP 208 y/o 212), la conexión 216 de protocolo seguro, o la propia conexión 204 de primer protocolo, sean abiertas y/o cerradas repetidamente. Sin la encapsulación del primer protocolo 204, el protocolo secundario 200a-200n puede abrir y cerrar con frecuencia conexiones de red, tales como conexiones TCP. Esto añadiría retardos significativos y sobrecarga al sistema. Estos retardos y esta sobrecarga se verían incrementados, además, por el uso de un protocolo 214 de encapsulación seguro, tal como SSL, que aporta una sobrecarga significativa al establecer conexiones de red. Encapsulando el protocolo secundario 200a-200n dentro

del primer protocolo 204 y manteniendo la conexión de transporte (208, 212), los protocolos secundarios 200a-200n, como parte de la carga útil del primer protocolo 204, no necesitan realizar frecuentes y costosas aperturas y cierres de la conexión 135 de red. Además, como los protocolos secundarios 200a-200n pueden comunicarse dentro del primer protocolo 204 con un protocolo seguro 216, los protocolos secundarios 200a-200n no necesitan abrir y cerrar conexiones seguras, tal como con SSL. La conexión de transporte (208, 212) establece y mantiene la conexión 135 de red de modo que los segundos protocolos encapsulados 200a-200n pueden comunicarse sin abrir y cerrar repetidamente la conexión 135 de red, segura o no. Esto incrementa significativamente la velocidad de comunicación de los protocolos secundarios 200a-200n.

Como se ha descrito anteriormente, los protocolos secundarios 200a-200n llevan paquetes de protocolo relacionados con aplicaciones que utilizan protocolos tales como HTTP, FTP, Oscar, Telnet, RDA o ICA. Los paquetes de protocolo secundario 304a-304n transportan datos relacionados con la funcionalidad de aplicaciones sometidas a transacciones entre el cliente 108 y el servicio anfitrión 116a-116n. Por ejemplo, un usuario en el cliente 108 puede interactuar con una página web proporcionada por un servicio anfitrión 116a-116n. En las transacciones entre el cliente 108 y el servicio anfitrión 116a-116n, el protocolo secundario 200a-200n encapsulado en el primer protocolo 204, puede tener paquetes de protocolo http relacionados para visualizar la página web y recibir cualquier interacción del usuario para comunicar con el servicio anfitrión 116a-116n. Como la conexión de transporte (208, 212) no es mantenida por los protocolos secundarios 200a-200n, los protocolos secundarios 200a-200n no tienen que gestionar ninguna interrupción de conexión a nivel de red. Como tales, los protocolos secundarios 200a-200n pueden no proporcionar, en sus cargas útiles, información alguna sobre interrupciones de conexión a nivel de red. En el ejemplo anterior, los paquetes 304a-304n de protocolo secundario http relacionados de los protocolos secundarios 200a-200n transmitidos al cliente 108, no proporcionarían notificación alguna acerca de que se haya producido una interrupción de red, por ejemplo, un mensaje de error en una página web. Por tanto, al usuario en el cliente 108 no se le notificará de interrupción alguna de la conexión a nivel de red a través del protocolo secundario 200a-200n. Esto, efectivamente, le oculta las interrupciones de conexión de red al usuario durante la utilización de las aplicaciones relacionadas con los protocolos secundarios 200a-200n.

Haciendo referencia a la Fig. 3, un proceso ilustrativo 200 utilizado por el servicio 112 de primer protocolo y el agente cliente 129 del cliente 108 encapsula la pluralidad de protocolos secundarios 200 (por ejemplo, HTTP, FTP, Oscar, Telnet, ICA y/o RDP) dentro del primer protocolo 204 para comunicación vía la conexión 135. Opcionalmente, como se describe en lo que sigue, el proceso ilustrativo 200 utilizado por el servicio 112 de primer protocolo y el agente cliente 128 del cliente 108 también comprime y/o cifra las comunicaciones al nivel del primer protocolo antes de comunicarse por la conexión 135. Desde el punto de vista del servicio 112 de primer protocolo, se reciben paquetes de protocolo secundario, 304a-304n, a través de las conexiones 124a-124n en el servicio 112 de primer protocolo. Por ejemplo, dos paquetes, 304a y 304b, de protocolo secundario son recibidos por el servicio 112 de primer protocolo. Pueden recibirse uno, dos o cualquier número de paquetes 304a-304n de protocolo secundario. En una realización, los paquetes 304a-304n de protocolo secundario son transmitidos por los servicios anfitriones 116 al servicio 112 de primer protocolo por la conexión 124. Los paquetes 304a-304n de protocolo secundario incluyen una cabecera 308 y un paquete de datos 312, denominado también carga útil de datos.

Después de recibirse los paquetes 304a-304n de protocolo secundario, el servicio 112 de primer protocolo encapsula uno o más de los paquetes 304 de protocolo secundario dentro de un paquete 316 de primer protocolo. En una realización, el servicio 112 de primer protocolo genera una cabecera 320 de paquete de primer protocolo y encapsula, dentro de la carga útil 324 de datos del paquete 316 de primer protocolo, uno o más paquetes 304a-304n de protocolo secundario tal como, por ejemplo, dos paquetes 304a y 304b de protocolo secundario. En otra realización, solamente un paquete 304a de protocolo secundario es encapsulado en cada paquete 316 de primer protocolo.

En una realización, los paquetes 316 de primer protocolo son entonces transmitidos por la conexión 135, por ejemplo por la conexión 208 descrita con referencia a la Fig. 2A, al agente cliente 128 del cliente 108. Alternativamente, en otra realización, el servicio 112 de primer protocolo está configurado, además, para cifrar, antes de la transmisión de cualesquiera paquetes 316 de primer protocolo, las comunicaciones al nivel del primer protocolo 204. En tal realización, los paquetes 316 de primer protocolo se cifran utilizando, por ejemplo, el protocolo SSL descrito con referencia a la Fig. 2B. Como resultado, se generan un paquete seguro 328, que incluye una cabecera 332, y un paquete 316' de primer protocolo, cifrado, como cara útil 336 de datos. El paquete seguro 328 puede ser transmitido entonces por la conexión 135, por ejemplo por la conexión segura TCP/IP 212 ilustrada en la Fig. 2B, al agente cliente 128 del cliente 108.

En otra realización, el servicio 112 de primer protocolo está configurado, además, para comprimir, antes de la transmisión de cualesquiera paquetes 316 de primer protocolo, las comunicaciones al nivel del primer protocolo 204. En una realización, antes de cifrar el paquete 316 de primer protocolo, el servicio 112 de primer protocolo comprime, utilizando una técnica de compresión estándar, el paquete 316 de primer protocolo. Como tal, resulta mejorada la eficacia del sistema 100.

Refiriéndonos de nuevo a las Figs. 1A-1B, el sistema 100 del presente invento, en una realización, le ofrece al cliente remoto 108 una conexión persistente con un servicio anfitrión 116 tal como, por ejemplo, el servicio anfitrión 116a. Por ejemplo, si el cliente 108 establece una conexión 135 entre el cliente 108 y el servicio 112 de primer protocolo y el servicio 112 de primer protocolo establece una conexión 124a entre el servicio 112 de primer protocolo y el servicio anfitrión 116a, entonces el agente cliente 128, el servicio 112 de primer protocolo, o ambos, están configura-

ES 2 298 835 T3

dos para mantener una cola de los paquetes de datos de primer protocolo más recientemente transmitidos a través de la conexión 135. Por ejemplo, los paquetes de datos puestos en cola pueden ser mantenidos por el agente cliente 128 y/o el servicio 112 de primer protocolo tanto antes como después de un fallo de la conexión 135. Además, al fallar la conexión 135, el servicio 112 de primer protocolo y, del mismo modo, el servicio anfitrión 116a, están configurados para mantener la conexión 124a.

Después de un fallo de la conexión 135, el cliente 108 establece una nueva conexión 135 con el servicio 112 de primer protocolo, sin perder dato alguno. Más específicamente, como la conexión 124a es mantenida al fallar la conexión 135, una conexión 135 recién establecida puede enlazarse con la conexión 124a mantenida. Además, como los paquetes de datos de primer protocolo más recientemente transmitidos están en cola, pueden ser transmitidos de nuevo por el cliente 108 al servicio 112 de primer protocolo y/o por el servicio 112 de primer protocolo al cliente 108 por la conexión 135 recién establecida. Como tal, la sesión de comunicaciones entre el servicio anfitrión 116a y el cliente 108 a través del servicio 112 de primer protocolo, es persistente y se mantiene sin pérdida alguna de datos.

En una realización, el agente cliente 128 del cliente 108 y/o el servicio 112 de primer protocolo numera los paquetes de datos que transmiten por la conexión 135. Por ejemplo, cada uno de entre el agente cliente 128 y el servicio 112 de primer protocolo numera por separado sus propios paquetes de datos transmitidos, sin tener en cuenta como numera el otro sus paquetes de datos. Además, la numeración de los paquetes de datos puede ser absoluta, sin renumeración alguna de los paquetes de datos, es decir, el primer paquete de datos transmitido por el agente cliente 128 y/o el servicio 112 de primer protocolo, puede numerarse como 1, numerándose tras él, consecutivamente, cada paquete de datos transmitido por la conexión 135 por el agente 128 y/o el servicio 112 de primer protocolo, respectivamente.

En una realización de esta clase, después de interrumpirse y restablecerse una conexión 135, el agente cliente 128 y/o el servicio 112 de primer protocolo informa al otro del siguiente paquete de datos que necesita. Por ejemplo, cuando el agente cliente 128 ha recibido los paquetes de datos números 1-10 antes de la interrupción de la conexión 135, el agente cliente 128, al restablecerse la conexión 135, informa al servicio 112 de primer protocolo de que, ahora, necesita el paquete de datos número 11. Similarmemente, el servicio 112 de primer protocolo también puede funcionar como tal. Alternativamente, en otra de tales realizaciones, el agente cliente 128 y/o el servicio 112 de primer protocolo informa al otro del último paquete de datos recibido. Por ejemplo, cuando el agente cliente 128 ha recibido los paquetes de datos números 1-10 antes de interrumpirse la conexión 135, el agente cliente 128, al restablecerse la conexión 135, informa al servicio 112 de primer protocolo de que el último paquete de datos que recibió fue el número 10. De nuevo, el servicio 112 de primer protocolo puede funcionar, también, como tal. En todavía otra realización, el agente cliente 128 y/o el servicio 112 de primer protocolo informa al otro, al restablecerse la conexión 135, tanto del último paquete de datos que recibió como del siguiente paquete de datos que necesita.

En tales realizaciones, al restablecerse la conexión 135 el agente cliente 128 y/o el servicio 112 de primer protocolo pueden retransmitir los paquetes de datos almacenados temporalmente no recibidos por el otro, permitiendo que la sesión de comunicaciones entre el servicio anfitrión 116 y el cliente 108, a través del servicio 112 de primer protocolo, continúe sin perderse datos. Además, al restablecerse la conexión 135, el agente cliente 128 y/o el servicio 112 de primer protocolo, pueden limpiar de cada una de sus memorias intermedias respectivas los paquetes de datos almacenados temporalmente que ahora se sabe que han sido recibidos por el otro.

Aunque el almacenamiento temporal de datos para una conexión persistente se describe, en general, en términos de un único servicio 112 de primer protocolo, las técnicas de almacenamiento intermedio y de reconexión descritas en lo que antecede, también son aplicables, en forma similar, a una sesión de comunicaciones de un cliente con un servicio anfitrión 116 que recorra múltiples servicios 112 de primer protocolo. Uno o más de los servicios 112 de primer protocolo adicionales pueden almacenar temporalmente parte del tráfico de datos entre el cliente 108 y el servicio anfitrión 116, o la totalidad de dicho tráfico. En otra realización, un servicio 112 de primer protocolo que gestione uno de los “saltos” entre un cliente y el servicio anfitrión 116, puede almacenar temporalmente los datos enviados a ese “salto” y los recibidos desde él. Como tal, uno o más de los servicios 112 de primer protocolo puede utilizarse para retransmitir paquetes de datos al restablecerse una conexión interrumpida entre el cliente 108 y el servicio anfitrión 116.

Ofreciendo al cliente 108 una conexión fiable y persistente con un servicio anfitrión 116a-116n, el presente invento evita el proceso de abrir una nueva sesión de usuario con el servicio anfitrión 116a-116n al mantener la sesión de usuario a través de las interrupciones de la conexión de red. Para cada sesión de usuario con un servicio anfitrión 116a-116n, el cliente 108 y el servicio anfitrión 116a-116n puede mantener un contexto y contenidos en memoria caché específicos de la sesión y otros mecanismos específicos de las aplicaciones relacionados con esa instancia de la sesión de usuario. Para cada nueva sesión de usuario establecida, tanto los contenidos de memoria caché como el contexto específicos de la sesión han de dotarse de contenido de nuevo o restablecerse para reflejarla nueva sesión de usuario. Por ejemplo, un usuario del cliente 108 puede tener una sesión http con un servicio anfitrión 116a-116n. El servicio anfitrión 116a-116n puede mantener el contexto específico para proporcionar esta instancia de la sesión http con el cliente 108. El contexto puede almacenarse en la memoria del servidor, en ficheros del servidor, una base de datos u otro componente relacionado para proporcionar la funcionalidad del servicio anfitrión 116a-116n. Asimismo, el cliente 108 puede tener un contexto local específico para la instancia de la sesión http, tal como un mecanismo para seguir la pista de una petición pendiente al servicio anfitrión 116a-116n. Este contexto puede almacenarse en la memoria del cliente 108, en ficheros del cliente 108 o en otro componente de software interconectado con el cliente 108. Si la conexión entre el cliente 108 y el servicio anfitrión 116a-116n no es persistente, entonces es necesario

establecer una nueva sesión de usuario con un nuevo contexto específico de la sesión en el servicio anfitrión 116a-116n y el cliente 108. El presente invento mantiene la sesión de forma que, por tanto, no es necesario restablecer un nuevo contexto de sesión específico.

5 El presente invento mantiene la sesión de usuario a través de interrupciones de conexión a nivel de red y sin notificar al usuario del cliente de que la sesión se interrumpió. En la puesta en práctica de este aspecto del invento, el servicio 112 de primer protocolo establece y mantiene una primera conexión con un cliente 108 y una segunda conexión con un servicio anfitrión 116a-116n. A través de la primera conexión y de la segunda conexión, se establece una sesión entre el cliente 108 y el servicio anfitrión 116a-116n. El servicio 112 de primer protocolo puede almacenar y mantener cualquier información relacionada con la sesión, tal como credenciales de autenticación, y el contexto del cliente 108 y el servicio anfitrión 116a-116n para la sesión establecida. Un usuario del cliente 108 ejercerá la funcionalidad ofrecida por el servicio anfitrión 116a-116n a través de la sesión establecida. Como tal, los paquetes 304a-304n de protocolo secundario relacionados contendrán datos relacionados con la transacción de dicha funcionalidad. Estos paquetes 304a-304n de protocolo secundario, como parte del protocolo secundario 200a-200n son encapsulados y comunicados en un primer protocolo 204. Al detectarse una interrupción de la primera conexión o de la segunda conexión, el servicio 112 de primer protocolo puede restablecer la conexión interrumpida al tiempo que mantiene la otra conexión que puede no haber sido interrumpida. La interrupción de la conexión de red puede causar la interrupción de la sesión entre el cliente 108 y el servicio anfitrión 116a-116n. Sin embargo, como el mecanismo de transporte no es mantenido por los protocolos secundarios 200a-200n, la sesión puede restablecerse una vez restablecida la conexión de red, sin que al usuario del cliente 108 se le haya notificado que la sesión fue interrumpida. El protocolo secundario 200a-200n no tiene que contener ninguna información relacionada con la interrupción para su transmisión al cliente 108. Así, la interrupción de la sesión provocada por la interrupción de la conexión de red se le oculta efectivamente al usuario debido al encapsulamiento del primer protocolo 204.

25 El servicio 112 de primer protocolo que mantiene información relacionada con la sesión, puede restablecer la sesión entre el cliente 108 y el servicio anfitrión 116a-116n. Por ejemplo, si se interrumpe la primera conexión entre el cliente 108 y el servicio 112 de primer protocolo, el servicio 112 de primer protocolo puede mantener activa o abierta la sesión del cliente 108 entre el servicio 112 de primer protocolo y el servicio anfitrión 116a-116n. Una vez restablecida la primera conexión, el servicio 112 de primer protocolo puede enlazar la sesión del cliente 108 con la sesión mantenida entre el servicio 112 de primer protocolo y el servicio anfitrión 116. El servicio 112 de primer protocolo puede enviar al cliente 108 cualquier dato que estuviese en cola antes de la interrupción de la primera conexión. Como tal, el cliente 108 estará utilizando la misma sesión de antes de la interrupción, y el servicio anfitrión 116a-116n y el cliente 108 pueden continuar utilizando cualquier contexto específico de la sesión que pueda existir en la memoria o estar almacenado en otro sitio. Además, por intermedio del servicio 112 de primer protocolo, el servicio anfitrión 116a-116n puede no enterarse de la interrupción de la red entre el servicio 112 de primer protocolo y el cliente 108.

En otro ejemplo, si se interrumpe la segunda conexión entre el servicio 112 de primer protocolo y el servicio anfitrión 116a-116n, el servicio de primer protocolo puede mantener la primera conexión con el cliente 108 mientras restablece la segunda conexión con el servicio anfitrión 116a-116n. Después de restablecida la segunda conexión, el servicio 112 de primer protocolo puede restablecer la sesión del cliente, en nombre del cliente, con el servicio anfitrión 116a-116n. Como el servicio 112 de primer protocolo mantenía información relacionada con la sesión, el servicio de primer protocolo puede restablecer la misma sesión o una sesión similar de modo que el cliente 108 no aprecie la interrupción de la segunda conexión de red ni la interrupción resultante de la sesión entre el servicio 112 de primer protocolo y el servicio anfitrión 116a-116n. Durante el restablecimiento de la segunda conexión de red y de la sesión, el servicio 112 de primer protocolo puede poner en cola cualesquiera transacciones de sesión enviadas por el cliente 108 durante la interrupción. Luego, una vez restablecidas la sesión con el servicio anfitrión 116a-116n, el servicio 112 de primer protocolo puede transmitir las transacciones puestas en cola al servicio anfitrión 116a-116n y la sesión puede continuar normalmente. De esta forma, el cliente 108 continúa funcionando como si no se hubiese producido interrupción de la sesión.

Además, al proporcionar una conexión fiable y persistente, el presente invento también evita interrupciones de las transacciones, órdenes u operaciones como parte de la funcionalidad ejercida entre el cliente 108 y un nodo anfitrión 118, o un servicio anfitrión 116a-116n. Por ejemplo, una operación de copia de ficheros utilizando Windows Explorer no ha sido diseñada para continuar trabajando después de producirse una interrupción en una conexión de red. Un usuario del cliente 108 puede utilizar la característica de copia de ficheros de Windows Explorer para copiar un fichero del cliente 108 a un nodo anfitrión 118. Debido al tamaño del o de los ficheros, esta operación puede tardar en completarse un período relativamente largo. Si, durante la parte media de la operación de copia del fichero al nodo anfitrión 118, se produce una interrupción en la conexión de red entre el cliente 108 y el nodo anfitrión 118, la copia del fichero fallará. Una vez restablecida la conexión de red, el usuario tendrá que poner en marcha otra operación de copia de ficheros desde el Windows Explorer para copiar el fichero desde el cliente 108 al nodo anfitrión 118. Merced al presente invento, el usuario no tendría que iniciar otra operación de copia de ficheros. La conexión de red se restablecería como parte de la conexión del primer protocolo 204. Las operaciones de copia de ficheros se encapsularían en la carga útil de los protocolos secundarios 200a-200n. Como tal, la copia de ficheros de Windows Explorer no sería notificado de la interrupción de la conexión de red y, por tanto, no fallaría. El servicio 112 de primer protocolo restablecería cualquier conexión y transmitiría cualquier dato puesto en cola de modo que la operación puede proseguir sin fallo. El servicio 112 de primer protocolo mantendría una cola con los datos relacionados con las operaciones de copia de ficheros que no han sido transferidas al nodo anfitrión 118 debido a la interrupción de la

conexión de red. Una vez restablecida la conexión de red, el servicio 112 de primer protocolo puede transmitir los datos puestos en cola y, luego, continúa transmitiendo los datos relacionados con la operación de copia de ficheros en la forma debida.

Si bien este aspecto del invento se describe en términos de un ejemplo de operación de copia de ficheros, un experto normal en la técnica reconocerá que cualquier operación, transacción, orden, llamada de función, etc., objeto de transacción entre el cliente 108 y el nodo anfitrión 118, o el servicio anfitrión 116a-116n, puede mantenerse y continuarse sin fallos debidos a la interrupción de la conexión de la red y, además, sin que el cliente 108 reconozca que existió una interrupción o sin haber tenido conocimiento de ella.

Además, al proporcionar una conexión fiable y persistente, el presente invento también permite que un cliente 108 pase por diferentes topologías de red sin tener que reiniciar una sesión o una aplicación en el cliente 108. Por ejemplo, el cliente 108 puede ser un ordenador portátil con una conexión de red inalámbrica. Cuando el cliente 108 se mueve de una primera red inalámbrica a una segunda red inalámbrica, la conexión 135 de red del cliente puede interrumpirse temporalmente en la primera red inalámbrica, cuando se establece una conexión de red con la segunda red inalámbrica. La segunda red inalámbrica puede asignar un nuevo identificador de red, tal como un nombre de anfitrión o una dirección de protocolo de Internet, al cliente 108. Este nuevo identificador de red puede ser diferente del identificador de red asignado al cliente 108 por la primera red inalámbrica. En otro ejemplo, el cliente 108 puede estar conectado físicamente a través de un cable Ethernet con una puerta de la red. La conexión física puede desenchufarse y el cliente 108 puede moverse a otra posición, para enchufarse en una puerta diferente de la red. Esto provocaría una interrupción de la conexión 135 de red y, posiblemente, un cambio del identificador de red asignado. Sin el presente invento, habría que reiniciar cualesquiera sesiones con un servicio anfitrión 116a-116n en el cliente 108 o aplicación en el cliente 108, que accediesen a la red debido al cambio de topología de la red, la interrupción de la conexión 135 de red y/o el cambio del identificador de red asignado. Merced al método y a los sistemas descritos en este documento, el presente invento mantiene la conexión de red para el cliente y restablece automáticamente la conexión de red del cliente 108, incluyendo la gestión de los cambios de topología de red y del identificador de la red. El cliente 108 y cualesquiera aplicaciones o sesiones en el cliente 108, puede continuar funcionando como si no se hubiese producido una interrupción de la conexión de red o un cambio del identificador de red. Además, el usuario en el cliente 108 puede no reconocer si ha habido interrupciones o cambios y el cliente 108 puede no recibir ninguna noticia sobre dichas interrupciones.

En otro aspecto, el presente invento se refiere al establecimiento seguro de una sesión de comunicaciones entre el cliente 108 y el servicio anfitrión 116 a través de múltiples conexiones o “saltos” que recorren múltiples componentes de red, tales como un representante, una pasarela de seguridad, un cortafuegos o un encaminador. El establecimiento de la sesión de comunicaciones segura con saltos múltiples puede iniciarse, además, a través de un canal seguro de comunicaciones entre cliente y servidor web, por ejemplo, entre el navegador web 162 y el servidor web 120 utilizando SSL. La autoridad 136 a cargo de los billetes puede proporcionar billetes para cada uno de los saltos tales como la conexión 135 entre cliente y servicio de primer protocolo y las conexiones 124a-124n entre el servicio de primer protocolo y el servicio anfitrión. De esta forma, el cliente 108 es autenticado a través de todas las conexiones entre el cliente 108 y el servicio anfitrión 116a-116n.

En funcionamiento, y también haciendo referencia a la Fig. 4, el usuario cliente solicita (paso 400) que el contenido (por ejemplo, una aplicación, un portátil de sobremesa) sea visualizada remotamente en el cliente 108 (es decir, el cliente 108 ICA). En otra realización, el cliente 108 utiliza el navegador de red 162 para solicitar una aplicación y el servidor web 120 autentica entonces al usuario. Tras recibir la petición, el servidor web 120 valida (paso 405) la petición con la autoridad 136 a cargo de los billetes. La autoridad 136 a cargo de los billetes genera entonces (paso 4010) un billete, que incluye un primer billete, o billete de cliente, y un segundo billete o billete de servicio de primer protocolo. Los billetes primer y segundo con billetes “de un solo uso” que carecen de valor tras usarlos por primera vez. En otra realización, el primer y el segundo billetes deben ser utilizados dentro de un período de tiempo predeterminado.

En una realización, la autoridad 136 a cargo de los billetes guarda en la memoria los billetes primero y segundo (por ejemplo, en la RAM), hasta que se utilice el billete. Alternativamente, la autoridad 136 a cargo de los billetes almacena el primero y el segundo billetes en un dispositivo de almacenamiento (no mostrado) hasta que se utilice el billete. El dispositivo de almacenamiento puede incluir, por ejemplo, una base de datos o una memoria persistente (por ejemplo, un disquete, una unidad de disco duro). La autoridad 136 a cargo de los billetes transmite subsiguientemente (paso 415) el billete del cliente al servidor web 120 y, luego, el servidor web 120 envía el billete de cliente (paso 420) al cliente 108.

El cliente 108 inicia entonces (paso 425) una sesión de comunicaciones con el servicio 112 de primer protocolo transmitiendo una petición de conexión de representante por el canal de comunicaciones 135 entre cliente y servicio de primer protocolo. La petición de conexión de representante incluye el billete de cliente. En una realización, la petición de conexión de representante también incluye una palabra de paso falsa que puede ser sustituida por el servicio 112 de primer protocolo cuando se establezca una sesión de comunicaciones con el nodo anfitrión 118. En otra realización, el servidor web 120 transmite la palabra de paso falsa al cliente 108 para la futura generación de una petición de conexión de representante que tenga un formato aceptable para el servicio 112 de primer protocolo. El servicio 112 de primer protocolo extrae (paso 430) el billete de cliente de la petición de conexión de representante y envía el billete de cliente a la autoridad 136 a cargo de los billetes para su validación. La autoridad 136 a cargo de los billetes valida

ES 2 298 835 T3

entonces (paso 435 el primer billete. En una realización, la autoridad 136 a cargo de los billetes verifica que primer billete buscando en su dispositivo de almacenamiento (por ejemplo, una base de datos) el primer billete esperado.

Si la autoridad 136 a cargo de los billetes no encuentra el primer billete en el dispositivo de almacenamiento (por ejemplo, si el primer billete ya ha sido utilizado), la autoridad 136 a cargo de los billetes da por finalizada la sesión de comunicaciones. Si el billete recibido coincide con el billete de cliente que la autoridad 136 a cargo de los billetes espera, el billete de cliente es validado. La autoridad 136 a cargo de los billetes transmite entonces (paso 440) el billete de servicio de segundo o de primer protocolo al servicio 112 de primer protocolo. Además, la autoridad 136 a cargo de los billetes borra el billete del cliente del dispositivo de almacenamiento cuando el billete del cliente ya ha sido utilizado una vez. En otra realización, la autoridad 136 a cargo de los billetes también transmite la dirección de protocolo de Internet (IP) del nodo anfitrión 118 al servicio 112 de primer protocolo. En todavía otra realización, la autoridad 136 a cargo de los billetes transmite el nombre de dominio del nodo anfitrión 118 al servicio 112 de primer protocolo para futura conversión en la dirección IP.

El servicio 112 de primer protocolo recibe el segundo billete, o el billete de servicio de primer protocolo y, subsecuentemente, abre las comunicaciones a través del canal 145 de comunicaciones del servidor representante, transmitiendo (paso 445) el segundo billete al nodo anfitrión 118. El nodo anfitrión 118 recibe el billete de servicio de primer protocolo y, luego, transmite el billete por el canal 157 de comunicaciones billete-servidor hasta la autoridad 136 a cargo de los billetes par validación (paso 447). En una realización, si la autoridad 136 a cargo de los billetes determina que el billete de servicio de primer protocolo recibido del nodo anfitrión 118 ha sido utilizado previamente o no tiene el valor correcto (es decir, el mismo valor que el almacenado en el dispositivo de almacenamiento asociado), la autoridad 136 a cargo de los billetes transmite un mensaje de error al servicio 112 de primer protocolo (o servidor web 120) para dar por terminada la sesión de comunicaciones establecida con el cliente 108. Si la autoridad 136 a cargo de los billetes valida el billete de servicio de primer protocolo (paso 448), el nodo anfitrión 118 lanza entonces (paso 450) la aplicación publicada en ICA. El nodo anfitrión transmite entonces información sobre la aplicación al servicio 112 de primer protocolo (paso 452) para presentación remota de la aplicación en el cliente 108 (paso 455) utilizando el cliente ICA 128.

En otra realización, el cliente 108 lanza el cliente ICA 128 cuando inicia las comunicaciones con el servicio 112 de primer protocolo en el paso 425. En otras realizaciones, el cliente 108 lanza el cliente ICA 128 cuando el cliente 108 recibe la información sobre la aplicación procedente del servicio 112 de primer protocolo en el paso 453.

Así, el cliente 108 no está al tanto del billete de servicio de primer protocolo sino, solamente, del billete del cliente. Además, el cliente ICA 128 no puede acceder al nodo anfitrión 118 sin comunicarse con el servicio 112 de primer protocolo y presentar el billete del cliente.

La autoridad 136 a cargo de los billetes podría, también, transmitir el billete de servicio de primer protocolo al servicio 112 de primer protocolo en el paso 440 como palabra de paso de usuario para el usuario del cliente 108. Esto le permite al servicio 112 de primer protocolo utilizar el billete de servicio de primer protocolo como palabra de paso de registro a fin de poder acceder al nodo anfitrión 118 sin exponer la palabra de paso de registro del usuario en la parte no segura de la web (es decir, el canal 135 de comunicaciones entre cliente y servicio de primer protocolo, durante el paso 425). Así, en una realización, el sistema 100 de comunicaciones podría incluir una base de datos de cartografiado de palabras de paso centralizada gestionada por la autoridad 136 a cargo de los billetes y situada conjuntamente con el nodo anfitrión 118, a fin de correlacionar el billete de servicio de primer protocolo con una palabra de paso de usuario.

Por tanto, la palabra de paso puede acompañar a ambos billetes (es decir al billete de servicio de primer protocolo y al billete de cliente) o la palabra de paso puede acompañar a uno de los dos billetes. Como se ha descrito en lo que antecede, si la palabra de paso acompaña a uno de los dos billetes, por ejemplo al billete del cliente, entonces el billete de servicio de primer protocolo es la palabra de paso. En una realización, la palabra de paso puede ser una palabra de paso del sistema que no cambie de valor o puede ser una palabra de paso de un solo uso, tal como las generadas por los testigos SecureID desarrollados por RSA Security Inc., de Bedford, Massachusetts, EE.UU.

Además, el invento puede extenderse a un sistema de comunicaciones que disponga de cualquier número de servicios 112 de primer protocolo, o "saltos", con el que hay de comunicarse el cliente 108 antes de establecer una sesión de comunicaciones con el nodo anfitrión 118. Si bien se ha descrito con relación a un servicio 112 de primer protocolo, un salto puede comprender cualquier componente de red, tale como un representante 115, un cortafuegos, un encaminador, y un repetidor.

Por ejemplo, y haciendo referencia a la Fig. 5A, un ejemplo de cuatro saltos lo constituye un sistema de comunicaciones 505 que tiene un servicio 112' de primer protocolo con un representante 115', un segundo servicio 112'' de primer protocolo con un representante 115'', y un tercer servicio 112''' de primer protocolo con un representante 115''' (generalmente 115). Los servicios 112 de primer protocolo con representantes 115 se comunican por un canal de comunicaciones de representante a representante, tal como un canal 510' de comunicaciones representante-representante y un segundo canal 510'' de comunicaciones representante-representante (de manera general, canal 510 de comunicaciones representante-representante). El cliente 108 se comunica con el servicio 112' de primer protocolo, que comunica con el segundo servicio 112'' de primer protocolo. A su vez, el segundo servicio 112'' de primer protocolo comunica con el tercer servicio 112''' de primer protocolo y, luego, el tercer servicio 112''' de primer protocolo se comunica con el nodo anfitrión 118 por el canal 145 de comunicaciones representante-servidor para establecer la

sesión de comunicaciones con el nodo anfitrión 118. Además, aunque la realización anteriormente descrita incluye un billete que tiene un billete de cliente y un billete de servicio de primer protocolo, otra realización incluye el billete que comprende numerosos billetes.

De manera más explícita y haciendo referencia, también, a la Fig. 5B, el servidor web 120 recibe una petición de una aplicación desde el cliente 108 y el servidor web 120 valida la petición con la autoridad 136 a cargo de los billetes (paso 405). La autoridad 136 a cargo de los billetes genera, entonces, un billete de N partes (por ejemplo, T_1 a T_N) en el paso 410. En una realización, la autoridad 136 a cargo de los billetes transmite entonces una parte T_i del billete de N partes (por ejemplo, la primera parte del billete o primer billete T_1) al servidor web 120 (paso 415). El servidor web 120 transmite entonces el billete T_1 al cliente 108 (paso 420). En una realización, la autoridad 136 a cargo de los billetes transmite, también, la dirección del siguiente “salto” (por ejemplo, el servicio 112’ de primer protocolo) al servidor web 120 que, entonces, transmite la dirección al cliente 108. Esta dirección es la dirección del siguiente salto (por ejemplo el servicio 112 de primer protocolo) que este salto (por ejemplo, el cliente 108) tiene que comunicar con el cliente 108 para, eventualmente, ser autenticado con el nodo anfitrión 118.

El cliente 108 utiliza la dirección para entra en contacto, entonces, con el siguiente “salto” (por ejemplo, el servicio 112’ de primer protocolo) e inicia una sesión de comunicaciones con el servicio 112’ de primer protocolo transmitiendo una petición de conexión con un representante por el canal 135 de comunicaciones entre cliente y servicio de primer protocolo. El servicio 112’ de primer protocolo extrae entonces (paso 530) el primer billete T_1 de la petición de conexión con el representante y envía este billete a la autoridad 136 a cargo de los billetes para su validación. La autoridad 136 a cargo de los billetes valida entonces (paso 535) el primer billete T_1 .

Al producirse una verificación apropiada del primer billete T_1 , la autoridad 136 a cargo de los billetes transmite el siguiente billete T_i del billete de N partes (por ejemplo, T_2) al siguiente servicio 112 de primer protocolo (por ejemplo, el servicio 112’ de primer protocolo) (paso 540). En algunas realizaciones, la autoridad 136 a cargo de los billetes transmite también la dirección del siguiente salto (por ejemplo, el segundo servicio 112’ de primer protocolo) a este salto (por ejemplo, el servicio 112’ de primer protocolo). El servicio 112’ de primer protocolo transmite este billete al siguiente salto (por ejemplo, el segundo servicio 112’ de primer protocolo) (paso 545). En una realización, el segundo servicio 112’ de primer protocolo verifica T_2 transmitiendo el billete a la autoridad 136 a cargo de los billetes (paso 550). La autoridad 136 a cargo de los billetes valida el segundo billete T_2 (paso 555) y el proceso continúa, como se muestra en los pasos 560 a 575. Una vez que se ha validado la última parte del billete de N partes, ocurren los pasos 450 a 455, como se muestra en la Fig. 4, para lanzar la aplicación en el cliente 108.

En una realización, cada servicio 112 de primer protocolo (es decir, cada salto) valida T_i (por ejemplo, T_2) con una autoridad 136 a cargo de los billetes asociada con el servicio 112 de primer protocolo (es decir, el salto). En esta realización, después de que cada servicio 112 de primer protocolo valida el billete T_i (por ejemplo, T_2) con una autoridad 136 a cargo de los billetes, la autoridad 136 a cargo de los billetes en la que tiene lugar la validación transmite el siguiente billete T_{i+1} (por ejemplo, T_3) y la dirección del siguiente servicio 112 de primer protocolo (es decir, el siguiente “salto” de destino) al servicio 112 de primer protocolo que ha validado el billete T_i . Así, cada servicio 112 de primer protocolo está asociado con una autoridad 136 a cargo de los billetes que ha sido configurada con los billetes de salto corriente y siguiente (es decir, validando T_i y transmitiendo T_{i+1} para el siguiente salto). Consiguientemente, el siguiente servicio 112 de primer protocolo actúa como cliente para ese salto. Este proceso se repite hasta alcanzar el nodo anfitrión 118 del sistema de comunicaciones 505. Así, cada salto ha sido validado individualmente sin tener que revelar todo el billete a ningún salto.

En otras realizaciones, la autoridad 136 a cargo de los billetes puede emitir más de un billete en lugar de emitir un billete con muchas partes. Por ejemplo, la autoridad 136 a cargo de los billetes genera un billete de primer salto y un billete de segundo salto en el paso 510, no estando asociado el billete de primer salto con el billete de segundo salto. La autoridad 136 a cargo de los billetes transmite, subsiguientemente el billete de primer salto al servidor web 120 y el servidor web 120 transmite el billete de primer salto al cliente 108. El cliente 108 transmite este billete de primer salto al servicio 112 de primer protocolo (por ejemplo, al servicio 112’ de primer protocolo) para validación por la autoridad 136 a cargo de los billetes. Al producirse la validación en el paso 535, la autoridad 136 a cargo de los billetes transmite, en el paso 540, el billete de segundo salto al siguiente servicio 112 de primer protocolo (por ejemplo el segundo servicio 112’ de primer protocolo) mientras que el billete de primer salto es independiente del billete de segundo salto.

En otra realización, una o más de las autoridades 136 a cargo de los billetes proporcionan a los representantes 115, como parte del servicio 112 de primer protocolo o por separado del servicio 112 de primer protocolo, cualquier información necesaria para conectar con el siguiente salto, tal como, pero sin limitarse a ello, claves de cifrado, información sobre la configuración del método SSL, e información de autenticación para conectar con un servidor SOCKS (por ejemplo, un servidor SOCKS5, desarrollado por NEC Corporation, de Tokyo, Japón).

En todavía otra realización, una autoridad 136 a cargo de los billetes solamente genera un único billete. La autoridad 136 a cargo de los billetes transmite el único billete al servidor web 120. EL servidor web 120 envía el único billete al cliente 108. El servicio 112 de primer protocolo recibe, subsiguientemente, el billete del cliente 108 y “consume” el billete único al realizar la validación. Como resultado, el sistema 100 de comunicaciones puede utilizar un único billete para proporcionar la posibilidad de utilizar protocolos de comunicaciones arbitrarios por el canal 135 de comunicaciones cliente-representante y el canal 140 de comunicaciones cliente-servidor web. Además, como el

nodo anfitrión 118 no recibe ni verifica el billete único, el billete es transparente para el nodo anfitrión 118 y, en consecuencia, el nodo anfitrión 118 no se “entera” del uso del billete.

5 Explotando la seguridad de las comunicaciones seguras entre el cliente 108 y el servidor web 120 por el canal 140 de comunicaciones seguras cliente-servidor web, el sistema de comunicaciones 505 establece un enlace seguro de comunicaciones por el canal 135 de comunicaciones no seguras cliente-representante para presentar a distancia aplicaciones de sobremesa en forma segura en el cliente 108.

10 En todavía otra realización, y haciendo referencia de nuevo a la Fig. 4, la autoridad 136 a cargo de los billetes transmite, en el paso 415, una versión inhabilitada del billete de servicio de primer protocolo con el billete de cliente al servidor web 120, para transmisión al cliente 108. El cliente 108 transmite subsiguientemente (paso 425) el billete de servicio de primer protocolo junto con el billete de cliente al servicio 112 de primer protocolo, como parte de la petición de conexión al representante. El servicio 112 de primer protocolo envía entonces ambos billetes a la autoridad 136 a cargo de los billetes. Al recibirse un billete de servicio de primer protocolo inhabilitado, la autoridad 136 a cargo de los billetes habilita el billete de servicio de primer protocolo después de validar el billete de cliente. La autoridad 15 136 a cargo de los billetes transmite entonces el billete de servicio de primer protocolo habilitado al servicio 112 de primer protocolo, para autenticación al nodo anfitrión 118.

20 Alternativamente, en otra realización, el servidor web 120 recibe un billete de servicio de primer protocolo inhabilitado y un billete de cliente habilitado de la autoridad 136 a cargo de los billetes y solamente transmite el billete de cliente al cliente 108. El cliente 108 transmite (paso 425) el billete de cliente al servicio 112 de primer protocolo como parte de la petición de conexión del representante. El servicio 112 de primer protocolo envía entonces el billete de cliente a la autoridad 136 a cargo de los billetes. La autoridad 136 a cargo de los billetes valida el billete del cliente y, al validarlo, habilita el billete de servicio de primer protocolo previamente transmitido al servidor web 120. En todavía otra realización, la autoridad 136 a cargo de los billetes transmite un billete de servicio de primer protocolo habilitado al servidor web 120 al validar el billete de cliente para autenticación al nodo anfitrión 118.

30 Así, en un momento dado, la autoridad 136 a cargo de los billetes solamente proporciona un billete habilitado al cliente 108 o al servicio 112 de primer protocolo, que la autoridad 136 a cargo de los billetes pueda validar. La autoridad 136 a cargo de los billetes puede proporcionar otro billete que puede ser validado (es decir, un billete inhabilitado) hasta que se valide el billete habilitado. Alternativamente, la autoridad 136 a cargo de los billetes puede no transmitir el billete de servicio de primer protocolo al servicio 112 de primer protocolo hasta que la autoridad 136 a cargo de los billetes valide el billete habilitado. Como se expone con mayor detalle en lo que sigue, esto obliga al encaminamiento de comunicaciones en la red utilizando el sistema de comunicaciones 505 porque el cliente 108 no 35 puede pasar por el servidor web 120 ni el servicio 112 de primer protocolo sin que la autoridad 136 a cargo de los billetes haya validado el billete habilitado y transmita el billete necesario para comunicarse con el nodo anfitrión 118.

40 En otra realización, en vez de transmitir el billete de servicio de primer protocolo al servicio 112 de primer protocolo, como en el paso 440, la autoridad 136 a cargo de los billetes transmite el billete de servicio de primer protocolo al servidor web 120 directamente por el canal 250 de comunicaciones entre servidor web y autoridad a cargo de los billetes. El servidor web 120 transmite entonces automáticamente el billete de servicio de primer protocolo al nodo anfitrión 118. Dicho de otro modo, el servidor web 120 “empuja” al billete de servicio de primer protocolo hacia el nodo anfitrión 118. La autoridad 136 a cargo de los billetes puede, también, empujar al billete de servicio de primer protocolo hacia el nodo anfitrión 118, sin transmisión del billete de servicio de primer protocolo al servicio 112 de 45 primer protocolo ni al servidor web 120.

50 En todavía otra realización, el nodo anfitrión 118 recupera el billete de servicio de primer protocolo de la autoridad 136 a cargo de los billetes por el canal 157 de comunicaciones billete-servidor de contenidos. Dicho de otro modo, el nodo anfitrión 118 “tira” del billete de servicio de primer protocolo desde la autoridad 136 a cargo de los billetes. Los anteriores ejemplos son ilustraciones de técnicas utilizadas para eliminar el paso 345 (modificando, al tiempo, el destino de la transmisión en el paso 440).

55 Además, el invento favorece el encaminamiento del cliente 108 a través de servicio 112 de primer protocolo. Como se ha establecido en lo que antecede, el cliente 108 ha de estar en posesión del billete de servicio de primer protocolo para establecer una sesión de comunicaciones con el nodo anfitrión 118. Más específicamente, para establecer una conexión con el nodo anfitrión 118, el servidor web 120 ha de validar primero la petición del cliente 108 con la autoridad 136 a cargo de los billetes. Una vez validada, el cliente 108 obtiene el primer billete y transmite este primer billete a la autoridad 136 a cargo de los billetes para su validación. Sin embargo, al realizar la validación, la autoridad 136 a cargo de los billetes transmite el billete de servicio de primer protocolo de vuelta al servicio 112 de primer 60 protocolo en vez de al cliente 108. La sesión de comunicaciones entre el cliente 108 y el servicio anfitrión 116 se establece cuando el servicio anfitrión 116 recibe el billete de servicio de primer protocolo. Así, el cliente 108 ha de comunicar con el servicio 112 de primer protocolo con el fin de que el billete de servicio de primer protocolo sea transmitido al servicio anfitrión 116, favoreciendo así el encaminamiento del cliente 108 a través del servicio 112 de primer protocolo. Así, el invento puede garantizar el recorrido apropiado de un dispositivo de seguridad (por ejemplo, 65 el servicio 112 de primer protocolo) antes de conceder acceso al nodo anfitrión 119.

Por ejemplo, un nodo anfitrión 118 ejecuta varias aplicaciones, tales como MICROSOFT WORD o MICROSOFT EXCEL, desarrolladas, ambas, por Microsoft Corporation, de Redmond, Washington, EE.UU. En una realización, el

cliente 108 utiliza NFUSE, desarrollado por Citrix Systems, Inc., de Fort Lauderdale, Florida, EE.UU. para obtener información de la agrupación centralizada 169 de servidores en la que el cliente 108 puede acceder a aplicaciones. Si un usuario cliente quiere acceder a MICROSOFT WORD y utilizarlo, el cliente 108 solicita la aplicación del servidor web 120. Sin embargo, solamente los usuarios que abonen una tasa por aplicación a MICROSOFT WORD pueden ser autorizados para acceder a la aplicación.

Para garantizar el pago de la tasa por aplicación, el sistema de comunicaciones 505 incluye el servicio 112 de primer protocolo y la autoridad 136 a cargo de los billetes para forzar el encaminamiento del cliente 108 a través del servicio 112 de primer protocolo. El encaminamiento del cliente 108 a través del servicio 112 de primer protocolo resulta valioso para el proveedor de la aplicación si se utiliza el servicio 112 de primer protocolo para recoger la tasa de la aplicación y autorizar al usuario a que acceda a la aplicación.

La autoridad 136 a cargo de los billetes genera, subsiguientemente, un billete asociado con la petición de la aplicación. Un primer billete habilitado es transmitido entonces al cliente 108. Como el cliente 108 no tiene la dirección del nodo anfitrión 118, el cliente 108 no puede acceder a la aplicación. Además, el cliente 108 no ha sido autorizado aún por el servicio 112 de primer protocolo (es decir, todavía no ha realizado el pago). Así, el cliente 108 tiene que comunicar con el servicio 112 de primer protocolo para que se le autorice. El servicio 112 de primer protocolo puede transmitir, entonces, el primer billete habilitado a la autoridad 136 a cargo de los billetes al pagarse la tasa de la aplicación.

La autoridad a cargo de los billetes valida entonces el billete del cliente y, subsiguientemente, transmite (o habilita) un billete de servicio de primer protocolo al representante 115. El servicio 112 de primer protocolo transmite entonces el billete de servicio de primer protocolo al nodo anfitrión 118 (por ejemplo, suponiendo que el usuario cliente ha pagado la tasa de la aplicación), que habilita al nodo anfitrión 118 para transmitir la aplicación al cliente 108. El sistema de comunicaciones 505 también puede utilizar tecnología ALE (lanzamiento e integración de aplicaciones), desarrollada por Citrix Systems, Inc., para permitir el lanzamiento de la aplicación desde una página HTML o la integración de la aplicación en una página HTML, para su entrega al cliente 108.

En otro aspecto, el presente invento se refiere a la reconexión de un cliente 108 con un servicio anfitrión 116 y a la nueva autenticación de las conexiones o “saltos” entre el cliente 108 y el servicio anfitrión 116. La Fig. 6A representa otra realización ilustrativa de un sistema 600 que es capaz de volver a conectar al cliente 108 con un servicio anfitrión 116. Además de las redes 104 y 104', el cliente 108, el servicio 112 de primer protocolo y los servicios anfitriones 116, todos los cuales se han descrito en lo que antecede, el sistema 600 incluye, además, un nodo intermediario 632 y una autoridad 1326 a cargo de los billetes. En una realización, el nodo intermediario 632 es una pasarela de seguridad tal como, por ejemplo, un cortafuegos y/o un encaminador, a través de la cual deben pasar los mensajes entre el cliente 108 y el servicio 112 de primer protocolo debido a la configuración de la red 104. Además, el nodo intermediario 632 puede comprender el representante 115 del servicio 112 de primer protocolo, con o sin el servicio 112 de primer protocolo. La autoridad 136 a cargo de los billetes puede ser, como se ha ilustrado, un componente autónomo de red que sea capaz de establecer comunicaciones y que tenga suficiente capacidad de memoria y potencia de procesador para llevar a cabo las operaciones descritas en este documento.

Como se muestra en la realización ilustrativa de la Fig. 6A, el nodo intermediario 632 está configurado para aceptar una conexión 135a iniciada por el cliente 108 y establecer una segunda conexión 135b con el servicio 112 de primer protocolo. Juntas, la conexión 135a y la segunda conexión 135b, constituyen la conexión 135, descrita anteriormente, por la que el cliente 108 y el servicio 112 de primer protocolo se comunican utilizando el primer protocolo.

El nodo intermediario 632, como se muestra, también está configurado para comunicar con la autoridad 136 a cargo de los billetes. En una realización, la autoridad 136 a cargo de los billetes está configurada para recibir una petición para un primer billete de reconexión procedente del nodo intermediario 632 y para generar, después, el primer billete de reconexión. El primer billete de reconexión puede incluir, por ejemplo, un número aleatorio grande. En otra realización, la autoridad 136 a cargo de los billetes está configurada para recibir una petición de un primer billete de reconexión para cada uno de los “saltos” entre el cliente y el servicio anfitrión 116. Por ejemplo, el nodo intermediario 632 puede requerir billetes de reconexión para la conexión entre el cliente 108 y el nodo intermediario 632, entre el nodo intermediario 632 y el servicio 112 de primer protocolo y entre el servicio 112 de primer protocolo y el servicio anfitrión 116. Estos billetes de reconexión solamente pueden ser válidos para cada uno de los “saltos”. Por ejemplo, un primer billete de reconexión para la conexión entre el servicio 112 de primer protocolo y el servicio anfitrión 116, solamente es válido para autenticar el servicio 112 de primer protocolo ante el servicio anfitrión 116 en nombre del cliente 108.

En otra realización, la autoridad 136 a cargo de los billetes está configurada para generar un identificador. El identificador puede ser, por ejemplo, un número aleatorio que esté asociado (por ejemplo, correlacionado) con el primer billete de reconexión. En una realización, el identificador es un número aleatorio menor que el número aleatorio que forma el primer billete de reconexión. Por ejemplo, el identificador puede ser un número aleatorio de 42 bits. En otra realización, el identificador asociado con un billete o un billete de reconexión es una dirección o un puntero que señala al siguiente “salto” de la conexión de múltiples saltos entre el cliente 108 y el servicio anfitrión 116. En este caso, un billete o un billete de reconexión es validado para un solo “salto” con un puntero que señala al siguiente “salto”. El siguiente “salto” tendrá que obtener y validar un billete o un billete de reconexión diferente y así sucesivamente hasta validarse el último “salto” y conectarse al servicio anfitrión 116 en nombre del cliente 108.

La autoridad 136 a cargo de los billetes transmite el primer billete de reconexión y el identificador al nodo intermediario 632, al tiempo que mantiene una copia del primer billete de reconexión y una copia del identificador. La copia del primer billete de reconexión puede ser utilizada posteriormente por la autoridad 136 a cargo de los billetes para validar el primer billete de reconexión originalmente transmitido al cliente 108 cuando sea presentado posteriormente a la autoridad 136 a cargo de los billetes durante el proceso de reconexión del cliente 108. En una realización, la autoridad 136 a cargo de los billetes mantiene, también, una dirección para el servicio 112 de primer protocolo que, como se explica más adelante, está asociada con el primer billete de reconexión y, al validarse el primer billete de reconexión, es transmitida al nodo intermediario 632.

En una realización, el nodo intermediario 632 está configurado, además, para usar el identificador a él transmitido por la autoridad 136 a cargo de los billetes a fin de suprimir la copia del primer billete de reconexión conservado en la autoridad 136 a cargo de los billetes. En otra realización, como se describe en lo que sigue, la autoridad 136 a cargo de los billetes está configurada, además, para borrar, durante el proceso de reconexión del cliente 108 con un servicio anfitrión 116, el primer billete de reconexión y, después, generar un primer billete de reconexión que lo reemplace. Además, en otra realización, el primer billete de reconexión está configurado para borrado automático tras un período de tiempo predeterminado. En la realización de billetes de reconexión para cada uno de los “saltos” entre el cliente y el servicio anfitrión 116, uno, algunos o todos los billetes de reconexión pueden configurarse para borrado automático después de transcurrido un período de tiempo predeterminado. En otras realizaciones, la autoridad 136 a cargo de los billetes o el nodo intermediario 632, está configurada para borrar cada uno de los billetes de múltiples saltos y generar billetes que los reemplacen.

En otra realización, el servicio 112 de primer protocolo está configurado para generar un segundo billete de reconexión que, como en el caso del primer billete de reconexión, puede incluir, por ejemplo, un número aleatorio grande. En una realización, el servicio 112 de primer protocolo genera segundo billetes de reconexión para cada uno de los “saltos” entre el cliente 108 y el servicio 112 de primer protocolo. El servicio 112 de primer protocolo puede estar configurado, también, para retransmitir el segundo billete de reconexión al cliente 108, al tiempo que conserva una copia del segundo billete de reconexión y un número de sesión. La copia del segundo billete de reconexión puede ser utilizada posteriormente por el servicio 112 de primer protocolo para validar el segundo billete de reconexión originalmente transmitido al cliente 108 cuando le es presentando posteriormente al servicio 112 de primer protocolo durante el proceso de reconexión del cliente 108. En una realización, el servicio 112 de primer protocolo transmite el segundo billete de reconexión al cliente 108 a través del nodo intermediario 632. En otra realización, el servicio 112 de primer protocolo transmite el segundo billete de reconexión al cliente 108 directamente. En otra realización, el servicio 112 de primer protocolo puede transmitir segundos billetes de reconexión a los otros servicios 112 de primer protocolo o nodos intermediarios 632 que pueden comprender la conexión de múltiples saltos entre el cliente 108 y el servicio anfitrión 116.

Además, como se describe con mayor detalle en lo que sigue, el servicio 112 de primer protocolo puede configurarse, además, para borrar, durante el proceso de reconectar el cliente 108 a un servicio anfitrión 116, el segundo billete de reconexión y, después, generar un segundo billete de reconexión de repuesto. Además, en otra realización, el segundo billete de reconexión está configurado para borrado automático tras un período de tiempo predeterminado. En otras realizaciones, un servicio 112 de primer protocolo de uno o más servicios 112 de primer protocolo en una conexión de múltiples saltos, está configurado para borrar los segundos billetes de reconexión para cada uno de los “saltos” y, después, generar segundo billetes de reconexión de repuesto para uno, algunos o todos los “saltos”.

En una realización, el nodo intermediario 632 sirve como intermediario para el primero y el segundo billetes de reconexión. El nodo intermediario 632 recibe, por ejemplo, el primer billete de reconexión generado por la autoridad 136 a cargo de los billetes y el segundo billete de reconexión generado por el servicio 112 de primer protocolo. El nodo intermediario 632 puede transmitir entonces el primer billete de reconexión y el segundo billete de reconexión al cliente 108. Además, durante el proceso de reconexión del cliente 108 al servicio anfitrión 116, el nodo intermediario 632 puede aceptar el primer billete de reconexión y el segundo billete de reconexión del cliente 108 y, después, transmitir el primer billete de reconexión a la autoridad 136 a cargo de los billetes y, si resulta apropiado, el segundo billete de reconexión al servicio 112 de primer protocolo.

En otra realización, el nodo intermediario 632 sirve como intermediario para los billetes de reconexión para los múltiples saltos entre el cliente 108 y el servicio anfitrión 116. El nodo intermediario 632 recibe, por ejemplo, el primer billete de reconexión para el cliente 108 para conexión con el servicio 112 de primer protocolo y el primer billete de reconexión para el servicio 112 de primer protocolo al servicio anfitrión 116. En otra realización, el nodo intermediario 632 recibe un primer billete de reconexión para la conexión entre el nodo intermediario 632 y el servicio 112 de primer protocolo. El nodo intermediario 632 puede transmitir entonces el primer billete de reconexión para el cliente 108 al cliente 108 y el primer billete de reconexión para el servicio 112 de primer protocolo al servicio 112 de primer protocolo. Además, durante el proceso de reconexión del cliente 108 con el servicio anfitrión 116, el nodo intermediario 632 puede aceptar el primer billete de reconexión del cliente 108 para validar el billete a fin de restablecer la conexión del cliente con el nodo intermediario 632 o el servicio 112 de primer protocolo.

Haciendo referencia a la Fig. 6B, otra realización de un sistema 602 para comunicaciones de redes, incluye las redes 104 y 104', el cliente 108, el servicio 112 de primer protocolo, los servicios anfitriones 116a-116n, el nodo intermediario 632 y la autoridad 136 a cargo de los billetes, como se ha descrito en lo que antecede y, además, ilustra un primer nodo 640 de computación y un segundo nodo 644 de computación, siendo utilizados ambos, en

ES 2 298 835 T3

una realización, para conectar inicialmente el cliente 108 con un servicio anfitrión 116. Además, en la realización ilustrativa de la Fig. 6A, el cliente 108 incluye, además, un navegador de web 162 tal como, por ejemplo, el programa INTERNET EXPLORER, de Microsoft Corporation, de Redmond, WA., EE.UU., para conectar con la World Wide Web.

En una realización (no mostrada), el sistema 602 incluye dos o más nodos intermediarios 632 y/o dos o más servicios 11 de primer protocolo. El nodo intermediario 632, a través del cual deben pasar los mensajes entre el cliente 108 y el servicio 112 de primer protocolo, y/o el servicio 112 de primer protocolo pueden elegirse, como se explica en lo que sigue, cada uno, basándose en, por ejemplo, una ecuación de equilibrio de carga.

Cada uno de entre el primer nodo 640 de computación y el segundo nodo 644 de computación puede estar constituido por cualquier dispositivo de computación que sea capaz de comunicarse y que tenga capacidad de memoria y potencia de procesador suficientes para llevar a cabo las operaciones descritas en este documento. Por ejemplo, en una realización, el primer dispositivo 640 de computación comprende un servidor web 120, que proporcione uno o más sitios web. En otra realización, el segundo nodo 644 de computación proporciona un servicio XML.

En una realización, el cliente 108 y la red 104 forman una red externa 652, separada del resto del sistema 602 por un primer cortafuegos 160, representado en línea interrumpida. El nodo intermediario 632 y el primer nodo 640 de computación pueden estar situados en una DMZ 130 separada del resto del sistema 602 por el primer cortafuegos 160 y un segundo cortafuegos 161, representado también con línea interrumpida. Luego, como se muestra, la red 104', el servicio 112 de primer protocolo, los servicios anfitriones 116a-116n, la autoridad 136 a cargo de los billetes, y el segundo nodo 644 de computación, forman una red interna 668, separada del resto del sistema 602 por el segundo cortafuegos 161.

Alternativamente, en otra realización y con referencia a la Fig. 6C, el sistema 604 incluye, además, un tercer nodo 646 de computación posicionado en la DMZ 130, entre la red 104 y el nodo intermediario 632. El tercer nodo 646 de computación puede ser cualquier dispositivo de computación que sea capaz de comunicarse por red y que tenga capacidad de memoria y potencia de procesador suficientes para llevar a cabo las operaciones descritas en este documento. Como se describe en lo que sigue, el tercer nodo 646 de computación se utiliza, en algunas realizaciones, durante el proceso de conectar inicialmente el cliente 108 a un servicio anfitrión 116 y/o durante el proceso de reconectar el cliente 108 a un servicio anfitrión 116. Más específicamente, como se describe más adelante, cuando el sistema 604 incluye dos o más nodos intermediarios 632, el tercer nodo 646 de computación puede, basándose en una ecuación de equilibrio de carga, por ejemplo, elegir el nodo intermediario 632 a través del cual deben pasar las comunicaciones entre el agente cliente 128 del cliente 108 y el servicio 112 de primer protocolo.

Además, con referencia a la Fig. 6D, el nodo intermediario 632 de la Fig. 6C puede, en una realización alternativa, ser sustituido por dos o más niveles "a"- "n" de nodos intermediarios 632. Como se ilustra, cada nivel "a"- "n" puede incluir dos o más nodos intermediarios 632a-632n. Como se describe en lo que sigue, el agente cliente 128 del cliente 108 puede ser encaminado a través de cualquier combinación de nodos intermediarios 632 basada en, por ejemplo, ecuaciones de equilibrio de carga. Por ejemplo, como se ilustra, el agente cliente 128 puede ser encaminado a través de los nodos intermediarios 632 mediante la conexión 622. Para mayor seguridad, cada uno de los "saltos" a través de la conexión 622 puede requerir un billete o billete de reconexión para validar y autenticar la conexión de múltiples saltos entre el cliente 108 y el servicio anfitrión 116. También son posibles otras configuraciones de los sistemas 600, 602 y 604, como le resultará fácilmente evidente a un experto en la técnica.

Refiriéndonos de nuevo a la Fig. 6B, en una realización, el navegador web 162 comunica por la red 104 con el primer nodo de computación 640 que, a su vez, se interconecta con el segundo nodo de computación 644 y la autoridad 136 a cargo de los billetes. Más específicamente, el primer nodo de computación 640 está configurado con la dirección del segundo nodo de computación 644 y la autoridad 136 a cargo de los billetes. En una realización, como se explica más adelante con mayor detalle, el primer nodo de computación 640 está configurado para retransmitir información y, por tanto, impedir la comunicación directa, entre el navegador web 162 del cliente 108, el segundo nodo de computación 644 y la autoridad 136 a cargo de los billetes. Impidiendo dicha comunicación directa, el primer nodo de computación 640 añade un nivel de seguridad adicional al sistema 602. El primer nodo de computación 640 puede estar configurado, también, con la dirección del nodo intermediario 632 o, alternativamente, con la dirección de dos o más nodos intermediarios 632.

Por su parte, el segundo nodo de computación 644 está configurado para determinar cuáles de los programas de aplicación que se ejecutan en los servicios anfitriones 116 están disponibles para un usuario del cliente 108. Dicho de otro modo, el segundo nodo de computación 644 está configurado para determinar a cuáles de los programas de aplicación está autorizado para acceder el usuario. En una realización, después de que el usuario selecciona su programa de aplicación deseado, como se describe con mayor detalle en lo que sigue, el segundo nodo de computación 644 está configurado además para determinar cuál de los servicios anfitriones 116 será utilizado para ejecutar la aplicación deseada del usuario con fines de equilibrado de carga. El segundo nodo de computación 644 devuelve la dirección de ese servicio anfitrión 116 al primer nodo de computación 640. El segundo nodo de computación 644 también devuelve la dirección del servicio 112 de primer protocolo, que también puede seleccionarse de entre una pluralidad de servicios 112 de primer protocolo utilizando una ecuación de equilibrio de carga, al primer nodo de computación 640. A su vez, el primer nodo de computación 640 transmite la dirección del servicio 112 de primer protocolo seleccionado y del servicio anfitrión 116 elegido, a la autoridad 136 a cargo de los billetes.

Por su parte, la autoridad 136 a cargo de los billetes genera billetes de conexión. En una realización, la autoridad 136 a cargo de los billetes transmite un billete de conexión inicial al primer nodo de computación 640 para transmisión al cliente 108. EN otra realización, la autoridad 136 a cargo de los billetes transmite billetes de conexión inicial al primer nodo de computación 640 para uno o más de los “saltos” entre el cliente 108 y el servicio anfitrión 116.

Refiriéndonos ahora a la Fig. 7, en ella se ilustra una realización de un método 600 para comunicaciones de red, que utiliza la realización ilustrativa de las Figs. 6A-6D. En el paso 604, el cliente 108 se conecta inicialmente a una pluralidad de servicios anfitriones 116 empleando, por ejemplo, el método 700 descrito en lo que sigue. Después de que el cliente 108 se conecta a la pluralidad de servicios anfitriones 116, el cliente 108 y los servicios anfitriones 116 se comunican, a través del servicio 112 de primer protocolo, y en el paso 608, mediante una pluralidad de protocolos secundarios encapsulados dentro del primer protocolo. En una realización, el servicio 112 de primer protocolo cifra, antes de la transmisión de ningún paquete de primer protocolo, las comunicaciones al nivel del primer protocolo 204, asegurando así las comunicaciones. En otra realización, el servicio 112 de primer protocolo comprime, antes de la transmisión de ningún paquete de primer protocolo, las comunicaciones al nivel del primer protocolo, mejorando por tanto la eficacia de las comunicaciones.

En el paso 612, el agente cliente 128 determina si ha fallado la conexión 135 entre el agente cliente 128 y el servicio 112 de primer protocolo. Por ejemplo, la conexión 135a entre el agente cliente 128 y el nodo intermediario 632 puede haber fallado, la conexión 135b entre el nodo intermediario 632 y el servicio 112 de primer protocolo puede haber fallado o ambas conexiones, 135a y 135b, pueden haber fallado. En otra realización, puede haber fallado la conexión entre el servicio 112 de primer protocolo y el servicio anfitrión. Si el agente cliente 128 determina que la conexión 135 no ha fallado, el método 600 continúa hasta el paso 620. Si, por otro lado, el agente cliente 128 determina que la conexión 135 ha fallado, al cliente 108 se le proporciona, en el paso 616, una conexión fiable con los servicios anfitriones 116 y se le vuelve a conectar con los servicios anfitriones 116.

En el paso 620 se determina si el cliente 108 desea terminar limpiamente su conexión 135 con el servicio 112 de primer protocolo y, en consecuencia, sus conexiones 124a-124n con los servicios anfitriones 116. Si no es así, la comunicación entre el cliente 108 y el servicio 112 de primer protocolo, a través de la pluralidad de protocolos secundarios encapsulados dentro del primer protocolo, continúa en el paso 608. Si la respuesta es afirmativa, en el paso 624 se rompen todas las conexiones 135a, 135b, y 124a-124n y se borran todos los billetes de reconexión. En una realización, el nodo intermediario 632 utiliza un identificador que recibe de la autoridad 136 a cargo de los billetes para borrar una copia de un primer billete de reconexión conservada en la autoridad 136 a cargo de los billetes. En otra realización, el servicio 112 de primer protocolo borra una copia de un segundo billete de reconexión conservada en el servicio 112 de primer protocolo. En otra realización, si por cualquier razón falla una conexión 124 de protocolo secundario, el servicio 112 de primer protocolo borra una copia del segundo billete de reconexión asociado con ella y conservada en el servicio 112 de primer protocolo. En todavía otra realización, un primer billete de reconexión y/o un segundo billete de reconexión son borrados automáticamente después de transcurrido un período de tiempo predeterminado a contar de un fallo de la conexión 135, como en el paso 612, y/o a contar de una terminación limpia de la conexión 135, como en el paso 620. En otras realizaciones, el servicio 112 de primer protocolo o la autoridad 136 a cargo de los billetes, suprime uno o más de los billetes de reconexión para uno o más de los “saltos” entre el cliente 108 y el servicio anfitrión 116.

Con referencia a las Figs. 8A-8C, en ellas se ilustra una realización de un método 700 para conectar inicialmente el cliente 108 a los servicios anfitriones 116 (por ejemplo, en el paso 604 de la Fig. 7), utilizando la realización ilustrativa de las Figs. 6A-6D. En el paso 704, el cliente 108, empleando el navegador 162, envía una petición, tal como por ejemplo una petición HTTP, al primer nodo de computación 640. El primer nodo de computación 640 devuelve una página web tal como, por ejemplo, un formulario HTML solicitando información de autenticación (por ejemplo, un nombre de usuario y una palabra de paso). Un usuario del cliente 108 introduce sus credenciales y transmite el formulario completado al primer nodo de computación 640.

El primer nodo de computación 640, en el paso 706, informa entonces al usuario del cliente 108 de las aplicaciones disponibles para su ejecución. En una realización, el primer nodo de computación 640 extrae las credenciales de usuario a partir de la página de registro y las transmite al segundo nodo de computación 644 junto con una petición al segundo nodo de computación 644 para que enumere las aplicaciones disponibles para el usuario. Basándose en las credenciales del usuario, el segundo nodo de computación 644 devuelve una lista de aplicaciones específicas disponibles para el usuario, al primer nodo de computación 640 que, entonces, envía la lista, en forma de página web, por ejemplo, al usuario del cliente 108.

En el paso 712, el usuario selecciona la aplicación deseada y una petición de esa aplicación es enviada al primer nodo de computación 640. Por ejemplo, en una realización, el usuario selecciona mediante el ratón una aplicación deseada de las enumeradas en la página web que le presenta el primer nodo de computación 640 y una petición HTTP para que esa aplicación sea enviada al primer nodo de computación 640. La petición es tratada por el primer nodo de computación 640 y enviada al segundo nodo de computación 644.

En el paso 716, el segundo nodo de computación 644 determina el servicio anfitrión 116 en el que se ejecutará la aplicación deseada. El segundo nodo de computación 644 puede realizar la determinación basándose, por ejemplo, en una ecuación de equilibrio de carga. En una realización, el segundo nodo de computación 644 determina, también, un servicio 112 de primer protocolo de entre una pluralidad de servicios 112 de primer protocolo, que se utilizará para

comunicar con el servicio anfitrión 116 a través de la conexión 124. Nuevamente, el segundo nodo de computación 644 puede realizar la determinación basándose, por ejemplo, en una ecuación de equilibrio de carga. El segundo nodo de computación 644 devuelve la dirección del servicio anfitrión 116 seleccionado y del servicio 112 de primer protocolo elegido, al primer nodo de computación 640.

5 El cliente 108, en el paso 720, es dotado entonces de un billete de conexión inicial y de una dirección para el nodo intermediario 632 (que es su dirección real o su dirección virtual, como se describe en lo que sigue). En una realización, el primer nodo de computación 640 proporciona la dirección para el servicio anfitrión 116 elegido y el servicio 112 de primer protocolo seleccionado, a la autoridad 136 a cargo de los billetes, junto con una petición para el billete de conexión inicial. La autoridad 136 a cargo de los billetes mantiene la dirección del servicio anfitrión 116 seleccionado y del servicio 112 de primer protocolo elegido, genera el billete de conexión inicial y transmite el billete de conexión inicial al primer nodo de computación 640, al tiempo que conserva una copia para ella. En una realización, la autoridad 136 a cargo de los billetes, en respuesta a la petición del billete de conexión inicial por parte del primer nodo de computación 640, genera billetes de conexión para cada uno de los “saltos” entre el cliente 108 y el servicio anfitrión 116. En otra realización, el primer nodo de computación 640 solicita billetes de conexión inicial para cada uno de los “saltos”, bien en una sola petición o en múltiples peticiones. Por ejemplo, la autoridad 136 a cargo de los billetes puede generar un billete con múltiples partes, como se ha descrito en lo que antecede en relación con la Fig. 5B.

20 El primer nodo de computación 640, configurado en una realización con la dirección real del nodo intermediario 632, transmite entonces la dirección real del nodo intermediario 632 y el billete de conexión inicial al navegador 162 del cliente 108. El primer nodo de computación 640 puede crear primero, por ejemplo, un fichero que contenga tanto la dirección real del nodo intermediario 632 como el billete de conexión inicial y, luego, transmitir el fichero al navegador 162 del cliente 108. Opcionalmente, en otra realización, el primer nodo de computación 640 está configurado con la dirección real de dos o más nodos intermediarios 632. En tal realización, el primer nodo de computación 632 determina primero el nodo intermediario 632 a través del cual tendrán que pasar los mensajes entre el cliente 108 y el servicio 112 de primer protocolo. El primer nodo de computación 640 transmite entonces la dirección real de ese nodo intermediario 132 elegido y el billete de conexión inicial al navegador 162 del cliente 108 utilizando, por ejemplo, el fichero anteriormente descrito. En una realización, el primer nodo de computación 640 elige el nodo intermediario 632 utilizando una ecuación de equilibrio de carga. El agente cliente 128 del cliente 108 es lanzado entonces y utiliza la dirección del nodo intermediario 632 para establecer, en el paso 724, una conexión 135a de primer protocolo entre el agente cliente 128 del cliente 108 y el nodo intermediario 632. En una realización, el primer nodo de computación 640 puede proporcionar billetes de conexión inicial obtenidos de la autoridad 136 a cargo de los billetes para uno o más de entre el servicio 112 de primer protocolo y/o nodos intermediarios 632, para validar sus respectivas conexiones.

35 Alternativamente, en otra realización, el primer nodo de computación 640 está configurado con una dirección real del tercer nodo de computación 646, que sirve como dirección virtual de un nodo intermediario 132. En tal realización, el primer nodo de computación 640 transmite, en el paso 720, la dirección real del tercer nodo de computación 646 y el billete de conexión inicial al navegador 162 del cliente 108 utilizando, por ejemplo, el fichero anteriormente descrito. El agente cliente 128 del cliente 108 es lanzado entonces y utiliza la dirección real del tercer nodo de computación 646 para establecer, en el paso 724, una conexión de primer protocolo entre el agente cliente 128 del cliente 108 y el tercer nodo de computación 646. El tercer nodo de computación 646 determina entonces el nodo intermediario 632 a través del cual tendrán que pasar los mensajes entre el cliente 108 y el servicio 112 de primer protocolo. En una realización, el tercer nodo de computación 646 selecciona el nodo intermediario 632 utilizando una ecuación de equilibrio de carga. Habiendo elegido el nodo intermediario 632, el tercer nodo de computación 646 establece una conexión de primer protocolo con el nodo intermediario 632. Existe, por tanto, una conexión 135a de primer protocolo a través del tercer nodo de computación 646, entre el agente cliente 128 del cliente 108 y el nodo intermediario 632. La dirección real del tercer nodo de computación 646 es correlacionada, por tanto con la dirección real del nodo intermediario 632. Para el agente cliente 128 del cliente 108, la dirección real del tercer nodo de computación 646 sirve, por tanto, como dirección virtual del nodo intermediario 632.

50 En una realización, cuando existen más de un nivel de nodos intermediarios 632, como se ha descrito en lo que antecede, el primer nodo de computación 640 o el tercer nodo de computación 646, respectivamente, solamente seleccionan el nodo intermediario 632 con el que se conectará el agente cliente 128 al nivel “a”. En tal realización, en cada uno de los niveles “a”-“n-1”, el nodo intermediario 632 a través del cual es encaminado el agente cliente 128 a ese nivel determina, después, basándose en una ecuación de equilibrio de carga, por ejemplo, el nodo intermediario 632 con el cual se conectará al siguiente nivel. Alternativamente, en otras realizaciones, el primer nodo de computación 640 o el tercer nodo de computación 646, respectivamente, determinan, para más de uno de los niveles “a”-“n”, los nodos intermediarios 632 a través de los cuales será encaminado el agente cliente 128.

60 Habiendo establecido la conexión 135a de primer protocolo entre el agente cliente 128 del cliente 108 y el nodo intermediario 632, por ejemplo el nodo intermediario 132 al nivel “n” (denominado en lo que sigue, en el método 700, el nodo intermediario 632), el agente cliente 128 transmite entonces el billete de conexión inicial al nodo intermediario 632.

65 En el paso 728 se determina, entonces, si es válido el billete de conexión inicial. En una realización, el nodo intermediario 632 transmite el billete de conexión inicial a la autoridad 136 a cargo de los billetes, para su validación. En una realización, la autoridad 136 a cargo de los billetes determina la validez del billete de conexión inicial compa-

ES 2 298 835 T3

rándolo, en el paso 720, con la copia del billete de conexión inicial que conserva. Si la autoridad 136 a cargo de los billetes determina que el billete de conexión inicial es válido, la autoridad 136 a cargo de los billetes transmite, en el paso 732, la dirección del servicio 112 de primer protocolo y la dirección del servicio anfitrión 116 elegido al nodo intermediario 632. La autoridad 136 a cargo de los billetes puede transmitir, también, billetes de conexión adicional para el servicio 112 de primer protocolo y para el nodo intermediario 632 a través del cual se conectará el cliente 108 con el servicio anfitrión 116. El servicio 112 de primer protocolo puede borrar, también, el billete de conexión inicial y la copia del mismo. Si, por otro lado, la autoridad 136 a cargo de los billetes determina que el billete de conexión inicial no es válido, el cliente 108, en el paso 730, rechaza la conexión con el servicio 112 de primer protocolo y, en consecuencia, la conexión con el servicio anfitrión 116.

A continuación del paso 732, el nodo intermediario 632 utiliza la dirección del servicio 112 de primer protocolo elegido para establecer, en el paso 736, una conexión 135b de primer protocolo entre el nodo intermediario 632 y el servicio 112 de primer protocolo. En una realización, el nodo intermediario 632 utiliza un billete de conexión inicial para establecer la conexión 135b de primer protocolo entre el nodo intermediario 632 y el servicio 112 de primer protocolo. En un caso, el nodo intermediario 632 utiliza el mismo billete de conexión inicial recibido del cliente 108 para validar la conexión 135b. En otro caso, el nodo intermediario 632 utiliza un billete de conexión inicial generado para la conexión 135b de primer protocolo y válido para ella. Ahora existe, por tanto, una conexión 135 de primer protocolo, a través del nodo intermediario 632, entre el agente cliente 128 del cliente 108 y el servicio 112 de primer protocolo. El nodo intermediario 632 también puede dejar pasar la dirección del servicio anfitrión 116 seleccionado al servicio 112 de primer protocolo.

En una realización, en el paso 740, el servicio 112 de primer protocolo utiliza la dirección del servicio anfitrión 116 elegido para establecer una conexión 124 de protocolo secundario entre el servicio 112 de primer protocolo y el servicio anfitrión 116 seleccionado. Por ejemplo, el servicio anfitrión qq6 elegido es, de hecho, el servicio anfitrión 116a y se establece una conexión 124a de protocolo secundario entre el servicio 112 de primer protocolo y el servicio anfitrión 116a.

En una realización, a continuación del paso 740, el usuario elige, en el paso 744, una segunda aplicación a ejecutar y el segundo nodo de computación 644 determina, en el paso 748, el servicio anfitrión 116 en el que ha de ejecutarse la segunda aplicación. Por ejemplo, calculando una ecuación de equilibrio de carga, el segundo nodo de computación 644 puede elegir el servicio anfitrión 116b para ejecutar el segundo programa de aplicación. El segundo nodo de computación 644 transmite entonces la dirección del servicio anfitrión 116b seleccionado al servicio 112 de primer protocolo. En una realización, el segundo nodo de computación 644 está en comunicación directa con el servicio 112 de primer protocolo y le transmite directamente la dirección. En otra realización, la dirección del servicio anfitrión 116b seleccionado es transmitida indirectamente al servicio 112 de primer protocolo. Por ejemplo, la dirección puede ser transmitida al servicio 112 de primer protocolo a través de cualquier combinación del primer nodo de computación 640, la autoridad 136 a cargo de los billetes, el nodo intermediario 632, y el servicio 112 de primer protocolo. Habiendo recibido la dirección del servicio anfitrión 116b elegido, el servicio 112 de primer protocolo establece, en el paso 752, una conexión 124b de protocolo secundario, entre el servicio 112 de primer protocolo y el servicio anfitrión 116b seleccionado. Al establecer una conexión 124b de protocolo secundario, el servicio 112 de primer protocolo puede validar un billete de conexión inicial para autenticar la conexión al servicio 116 de primer protocolo. El billete de conexión inicial puede ser el mismo billete de conexión inicial para la conexión del cliente 108 con el nodo intermediario 632 o la conexión del nodo intermediario 632 con el servicio 112 de primer protocolo. En otra realización, la autoridad 136 a cargo de los billetes o cualquiera de los nodos intermediarios 632 genera un billete válido solamente para la conexión 124b de protocolo secundario. El servicio 112 de primer protocolo y/o el servicio anfitrión 116 utilizan este billete para validar la conexión 124b de protocolo secundario.

Los protocolos secundarios que pueden utilizarse para comunicar por las conexiones 124a y 124b incluyen HTTP, FTP, Oscar, Telnet, ICA y RDP, pero no se limitan a ellos. Además, en una realización, al menos uno de los protocolos secundarios, como se ha descrito anteriormente, incluye una pluralidad de canales virtuales, cada uno de los cuales puede incluir una pluralidad de paquetes de protocolo que habilitan funcionalmente al cliente remoto 108. Por ejemplo, en una realización, un servicio anfitrión 116a es un servidor web, que comunica con el servicio 112 de primer protocolo por la conexión 124a utilizando el protocolo HTTP y otro servicio anfitrión 116b es un servidor de aplicaciones, que comunica con el servicio 112 de primer protocolo por la conexión 124b utilizando el protocolo ICA. El servicio anfitrión 116b genera tanto paquetes de protocolo para transmitir órdenes de pantalla gráfica al cliente 108, para hacer que el cliente 108 presente una interfaz gráfica de usuario, como paquetes de protocolo para transmitir órdenes de impresora al cliente 108, para hacer que se imprima un documento en el cliente 108.

Los pasos 744, 748 y 752 pueden repetirse cualquier número de veces. Como tal, cualquier número de programas de aplicación pueden ejecutarse en cualquier número de servicios anfitriones 116a-116n, cuyas salidas pueden comunicarse al servicio 112 de primer protocolo por las conexiones 124a-124n utilizando cualquier número de protocolos secundarios.

Volviendo ahora al paso 756, el servicio 112 de primer protocolo puede, como se ha descrito anteriormente, encapsular la pluralidad de protocolos secundarios dentro del primer protocolo. Como tal, el cliente 108 está conectado a una pluralidad de servicios anfitriones 116 y, simultáneamente, se encuentra en comunicación con ellos.

ES 2 298 835 T3

En otra realización, antes de llevar a la práctica los pasos 744, 748 y 752 para ejecutar un nuevo programa de aplicación en un servicio anfitrión 116, tal como, por ejemplo, el servicio anfitrión 116b, un usuario del cliente 108 termina la ejecución de otro programa de aplicación tal como, por ejemplo, un programa de aplicación que se ejecuta en el servicio anfitrión 116a. EN tal caso, el servicio 112 de primer protocolo interrumpe la conexión 124a entre el servicio 112 de primer protocolo y el servicio anfitrión 116a. El servicio 112 de primer protocolo establece entonces, llevando a la práctica los pasos 744, 748 y 752, la conexión 124b entre el servicio 112 de primer protocolo y el servicio anfitrión 116b, sin interrumpir la conexión 135 entre el cliente 108 y el servicio 112 de primer protocolo.

En una realización, en el paso 760 se genera un primer billete de reconexión. Por ejemplo, el nodo intermediario 632 solicita un primer billete de reconexión de la autoridad 136 a cargo de los billetes o solicita un billete de reconexión para cada uno de los “saltos” entre el cliente 108 y el servicio anfitrión 116. Al recibirse la petición, la autoridad 136 a cargo de los billetes genera el o los primeros billetes de reconexión. Un billete de reconexión es, por ejemplo, un número aleatorio grande y, también puede generar un identificador que es, por ejemplo, un número aleatorio más pequeño. La autoridad 136 a cargo de los billetes puede transmitir entonces, en el paso 764, los primeros billetes de reconexión y los identificadores al nodo intermediario 632, al tiempo que conserva una copia de los primeros billetes de reconexión y una copia de los identificadores. La autoridad 136 a cargo de los billetes continúa para mantener la dirección del servicio 112 de primer protocolo que le fue transmitido por el primer nodo de computación 640 en el paso 720. El nodo intermediario 632 transmite entonces, en el paso 768, el primer billete de reconexión del cliente al cliente 108.

En el paso 772, se generan entonces uno o más billetes de reconexión. En una realización, el servicio 112 de primer protocolo genera el segundo billete de reconexión para el cliente 108, el cual puede ser, por ejemplo, un número aleatorio grande. En otra realización, el servicio 112 de primer protocolo genera segundos billetes de reconexión para uno o más de los “saltos” entre el cliente 108 y el servicio anfitrión 116. El servicio 112 de primer protocolo, en el paso 776, transmite, entonces, el segundo billete de reconexión del cliente a través del nodo intermediario 632, al cliente 108. Al hacer esto, el servicio 112 de primer protocolo conserva una copia del segundo billete de reconexión y un número de sesión asociado con él para identificar la sesión que ha de reconectarse a continuación de una interrupción de la conexión 135. En una realización, por ejemplo, el servicio 112 de primer protocolo mantiene, para un número de sesión particular, una tabla que enumera las conexiones de protocolo secundario 124a-124n asociadas con ese número de sesión. En forma parecida, el servicio 112 de primer protocolo puede mantener el primero y/o el segundo billetes de reconexión para cada uno de los “saltos” que se están validando para reconectar el cliente 108 al servicio anfitrión 116.

En consecuencia, a continuación del restablecimiento de la conexión 135 de primer protocolo y la validación del segundo billete de reconexión en el servicio 112 de primer protocolo, y/o en cualesquiera servicios 112 de primer protocolo subsiguientes y/o nodos intermediarios 632, el servicio 112 de primer protocolo puede identificar las conexiones 124 de protocolo secundario que han de ser encapsuladas dentro de la conexión 135 de primer protocolo restablecida para comunicación al cliente 108. Alternativamente, en otra realización, y con referencia de nuevo a la Fig. 1A, el sistema 100 del presente invento no incluye el o los nodos intermediarios 132, la autoridad 136 a cargo de los billetes, ni el tercer nodo de computación 646. En tal realización, en lugar de generar y transmitir, en los pasos 760 a 776, el primero y el segundo billetes de reconexión, el sistema 100 y el método 700 solamente proporcionan un único billete de reconexión para el cliente 108 o para uno o más de los “saltos” entre el cliente 108 y el servicio anfitrión 116. En tal realización, el servicio 112 de primer protocolo, por ejemplo, genera el único billete de reconexión que puede ser, por ejemplo, un número aleatorio grande. El servicio 112 de primer protocolo transmite entonces el billete de reconexión del cliente directamente al cliente 108 por la conexión 135. Al hacerlo, el servicio 112 de primer protocolo conserva una copia del único billete de reconexión y un número de sesión asociado con él, para identificar la sesión a reconectar después de una interrupción de la conexión 135. En otra realización, el servicio 112 de primer protocolo conserva el billete de reconexión para su conexión al servicio anfitrión 116 y un número de sesión asociado con él para recuperar el billete de reconexión.

Refiriéndonos ahora a la Fig. 9, en ella se ilustra una realización de un método 800 para proporcionar a un cliente 108 una conexión fiable a uno o más servicios anfitriones 116 y para reconectar al cliente 108 con los servicios anfitriones 116 (por ejemplo, en el paso 616 de la Fig. 7) utilizando la realización ilustrativa de las Figs. 6A-6D. En particular, en el paso 804, se mantiene la conexión 124 de protocolo secundario entre el servicio 112 de primer protocolo y el o cada uno de los servicios anfitriones 116. Además, en el paso 808, se mantiene una cola de los paquetes de datos más recientemente transmitidos entre el agente cliente 128 del cliente 108 y el servicio 112 de primer protocolo, a través de la conexión 135 cuya interrupción se determinó, por ejemplo, en el paso 616 de la Fig. 7. En una realización, los paquetes de datos son puestos en cola y mantenidos tanto antes como durante el fallo de la conexión 135. Los paquetes de datos puestos en cola pueden ser mantenidos, por ejemplo, en una memoria intermedia, por el agente cliente 128. Alternativamente, el servicio 112 de primer protocolo puede mantener, en una memoria intermedia, los paquetes de datos puestos en cola. En todavía otra realización, tanto el agente cliente 128 como el servicio 112 de primer protocolo, mantienen los paquetes de datos puestos en cola en una memoria intermedia.

En el paso 812, se establece una nueva conexión 135 de primer protocolo entre el agente cliente 128 del cliente 108 y el servicio 112 de primer protocolo y se enlaza con la conexión 124 de protocolo secundario mantenida entre el servicio 112 de primer protocolo y el o cada uno de los servicios anfitriones 116, reconectando, por tanto, al cliente 108 con los servicios anfitriones 116. Después de que el cliente 108 ha sido reconectado, pueden transmitirse, en el paso 816, los paquetes de datos puestos en cola mantenidos en el paso 808, a través de la conexión 135 de primer

protocolo recién establecida. Como tal, la sesión de comunicaciones entre los servicios anfitriones 116 y el cliente 108, a través del servicio 112 de primer protocolo, es persistente y prosigue sin pérdida de datos.

En una realización con múltiples “saltos” que pasan por múltiples servicios 112 de primer protocolo, en el paso 808, una parte de los paquetes de datos, o todos ellos, pueden mantenerse en uno o más de los servicios 112 de primer protocolo. En el paso 812, puede restablecerse cada “salto”. Después de que el cliente 108 es reconectado y vuelto a enlazar con el primero del o de los servicios 112 de primer protocolo, como se ha descrito anteriormente, cada una de las restantes conexiones puede restablecerse y volverse a enlazar con el “salto” previamente enlazado de nuevo, hasta que se restablezca el “salto” final al servicio anfitrión 116. Después de que se haya restablecido y vuelto a enlazar el “salto” final, o cuando se restablezca y enlace de nuevo cada “salto”, pueden transmitirse, en el paso 816, los paquetes de datos mantenidos en el paso 808.

Refiriéndonos ahora a las Figs. 10A-10B, en ellas se ilustra una realización de un método 900 para reconectar el cliente 108 con el o los servicios anfitriones 116 (por ejemplo, en el paso 812 de la Fig. 9), utilizando la realización ilustrativa de las Figs. 6A-6D. En el paso 904, se rompen cualesquiera conexiones restantes entre el cliente 108 y el servicio 112 de primer protocolo. Por ejemplo, cuando ha fallado la conexión 135a, pero no lo ha hecho la conexión 135b, se rompe la conexión 135b. Alternativamente, cuando ha fallado la conexión 135b, pero no lo ha hecho la conexión 135a, se rompe la conexión 135a.

En una realización, utilizando la dirección real del nodo intermediario 632 proporcionada al cliente 108, por ejemplo en el paso 720 de la Fig. 8, el agente cliente 128 del cliente 108 restablece entonces, en el paso 908, la conexión 135a de primer protocolo entre el agente cliente 128 y el nodo intermediario 632. Alternativamente, en otra realización, utilizando la dirección real del tercer nodo de computación 646 proporcionada al cliente 108, por ejemplo en el paso 720 de la Fig. 8, el agente cliente 128 del cliente 108 restablece entonces, en el paso 908, una conexión de primer protocolo entre el agente cliente 128 y el tercer nodo de computación 646. El tercer nodo de computación 646 determina entonces el nodo intermediario 632 a través del cual tendrán que pasar los mensajes entre el cliente 108 y el servicio 112 de primer protocolo. En una realización, el tercer nodo de computación 646 selecciona el nodo intermediario 632 utilizando una ecuación de equilibrio de carga. El nodo intermediario 632 seleccionado por el tercer nodo de computación 646 al reconectar el cliente 108 al o a los servicios anfitriones 116, puede ser diferente del elegido, por ejemplo en el paso 720 de la Fig. 8, para conectar inicialmente el cliente 108 al o a los servicios anfitriones 116. En una realización, se genera un billete de conexión inicial para el nodo intermediario 632 seleccionado cuando se reconecta al cliente 108 con el servicio anfitrión 116.

Habiéndose elegido el nodo intermediario 632, el tercer nodo de computación 646 restablece una conexión 135a de primer protocolo con el nodo intermediario 632. Por tanto, se restablece una conexión 135a de primer protocolo, a través del tercer nodo de computación 646, entre el agente cliente 128 del cliente 108 y el nodo intermediario 632. En una realización, cuando se restablece la conexión 135a de primer protocolo con el nodo intermediario 632, la conexión 135a de primer protocolo es validada validando un primero o un segundo billetes de reconexión para este “salto” con la autoridad 136 a cargo de los billetes.

En una realización, cuando existe más de un nivel de nodos intermediarios 632, el nodo intermediario 632 a través del cual es encaminado después el agente cliente 128 en cada uno de los niveles “a”-“n-1”, determina, basándose por ejemplo en una ecuación de equilibrio de carga, el nodo intermediario 632 al que se conectará en el siguiente nivel. Alternativamente, en otra realización, el tercer nodo de computación 646 determina, para más de uno de los niveles “a”-“n-1”, o para todos ellos, el nodo intermediario 632 a través del cual será encaminado el agente cliente 128. En otras realizaciones, el nodo intermediario 632 o uno de los nodos de computación (por ejemplo, el tercer nodo de computación 646) genera primeros o segundos billetes de reconexión para una o más de las conexiones o “saltos” a través de los cuales es encaminado el agente cliente 128.

Habiéndose restablecido la conexión 135a de primer protocolo entre el agente cliente 128 del cliente 108 y el nodo intermediario 632, por ejemplo el nodo intermediario 132 al nivel “n” (denominado en lo que sigue, en el método 900, el nodo intermediario 632), el agente cliente 128 transmite entonces, en el paso 912, el primer billete de reconexión y el segundo billete de reconexión para el cliente 108 al nodo intermediario 632.

Se determina entonces, en el paso 916, si el primer billete de reconexión es válido. En una realización, la validez del primer billete de reconexión se determina utilizando la autoridad 136 a cargo de los billetes. Por ejemplo, el nodo intermediario 632 transmite el primer billete de reconexión a la autoridad 136 a cargo de los billetes. En una realización, la autoridad 136 a cargo de los billetes determina la validez del primer billete de reconexión comparándolo con un a copia previamente conservada del primer billete de reconexión. Si la autoridad 136 a cargo de los billetes determina que el primer billete de reconexión es válido, la autoridad 136 a cargo de los billetes transmite, en el paso 920, la dirección del servicio 112 de primer protocolo al nodo intermediario 632. De otro modo, si la autoridad 136 a cargo de los billetes determina que el primer billete de reconexión no es válido, se rechaza, en el paso 924, la reconexión del cliente 108 con el servicio 112 de primer protocolo y, en consecuencia, la reconexión con los servicios anfitriones 116.

En el paso 928, el primer billete de reconexión es borrado por, por ejemplo, la autoridad 136 a cargo de los billetes y un primer billete de reconexión de repuesto es generado por, por ejemplo, la autoridad 136 a cargo de los billetes. Además, un identificador de repuesto puede ser generado por, por ejemplo, la autoridad 136 a cargo de los billetes.

ES 2 298 835 T3

En algunas de tales realizaciones, la autoridad 136 a cargo de los billetes transmite el primer billete de reconexión de repuesto y el identificador de repuesto al nodo intermediario 632. En algunas de tales realizaciones, la autoridad 136 a cargo de los billetes conserva una copia del primer billete de reconexión de repuesto. En algunas realizaciones, la autoridad 136 a cargo de los billetes espera a que el cliente 108 comunique que ha recibido el primer billete de reconexión de repuesto, antes de proceder a borrar el primer billete de reconexión.

Después de validado el primer billete de reconexión, el nodo intermediario 632, utilizando la dirección el servicio 112 de primer protocolo, restablece, en el paso 932, la conexión 135b de primer protocolo entre el nodo intermediario 632 y el servicio 112 de primer protocolo. Habiéndose restablecido la conexión 135b de primer protocolo entre el nodo intermediario 632 y el servicio 112 de primer protocolo, se determina entonces, en el paso 936, si es válido el segundo billete de reconexión. En una realización, la validez del segundo billete de reconexión se determina utilizando el servicio 112 de primer protocolo. Por ejemplo, el nodo intermediario 632 transmite el segundo billete de reconexión al servicio 112 de primer protocolo. En una realización, el servicio 112 de primer protocolo determina la validez del segundo billete de reconexión comparándolo con una copia, previamente conservada, del segundo billete de reconexión. En otra realización del paso 936, el servicio 112 de primer protocolo valida un primer billete de reconexión para la conexión entre el servicio 112 de primer protocolo y el servicio anfitrión 116 o, en otra realización, entre el servicio 112 de primer protocolo y otro servicio 112 de primer protocolo o un nodo intermediario 632. De manera similar, cada “salto” ejecutado después entre el servicio 112 de primer protocolo y el servicio anfitrión 116, puede ser validado con uno o más billetes, ya se trate de billetes de conexión inicial o de reconexión, para validar el uso continuado del “salto” en nombre del cliente 108.

Si el servicio 112 de primer protocolo determina que el segundo billete de reconexión es válido, la conexión 135b de primer protocolo restablecida entre el primer nodo intermediario 132 y el servicio 112 de primer protocolo se enlaza, en el paso 940, con la conexión 124 de protocolo secundario mantenida entre el servicio 112 de primer protocolo y el o cada uno de los servicios anfitriones 116. De otro modo, si el servicio 112 de primer protocolo determina que el segundo billete de reconexión no es válido, la conexión 135b de primer protocolo restablecida no se enlaza con la o las conexiones 124 de protocolo secundario mantenidas y, en el paso 944, se rechaza la reconexión del cliente 108 con el o los servicios anfitriones 116. En el caso de una conexión de saltos múltiples entre el servicio 112 de primer protocolo y el servicio anfitrión 116, cada “salto” puede ser validado para reconexión y, en el paso 940, ser enlazado con el “salto” previo, hasta que se valide el “salto” final al servicio anfitrión 116, o hasta que se rechace la reconexión en uno de los “saltos”.

En el paso 948, el segundo billete de reconexión es borrado por, por ejemplo, el servicio 112 de primer protocolo y un segundo billete de reconexión de repuesto es generado por, por ejemplo, el servicio 112 de primer protocolo para transmisión al cliente 108. En una realización de esta clase, el servicio 112 de primer protocolo conserva una copia del segundo billete de reconexión de repuesto. En algunas realizaciones, el servicio 112 de primer protocolo espera a que el cliente 108 comunique que ha recibido el segundo billete de reconexión de repuesto, antes de proceder a borrar el segundo billete de reconexión. En el caso de validarse uno o más de los “saltos” para reconectar un cliente 108, en el paso 948 pueden generarse uno o más billetes de reconexión de repuesto y/o la autoridad 136 a cargo de los billetes, los nodos intermediarios 632, cualquiera de los nodos de computación o uno o más de los servicios 112 de primer protocolo, pueden salvar una copia.

En el paso 952, se le transmiten al cliente el primer billete de reconexión de repuesto y el segundo billete de reconexión de repuesto. Por ejemplo, la autoridad 136 a cargo de los billetes puede transmitir, a través del nodo intermediario 632, el primer billete de reconexión de repuesto al cliente 108. Además, en una realización, el servicio 112 de primer protocolo transmite, a través del nodo intermediario 632, el segundo billete de reconexión de repuesto al cliente 108. En otras realizaciones, los billetes de reconexión de repuesto para uno o más “saltos” pueden ser transmitidos a uno o más de los nodos intermediarios 632, cualquiera de los nodos de computación o uno o más de los servicios 112 de primer protocolo.

Alternativamente, en otras realizaciones, como se ha expuesto en lo que antecede, el sistema 100 y los métodos del invento proporcionan solamente un único billete de reconexión para el cliente 106 y/o una única reconexión para cada uno de los “saltos” entre el cliente 108 y un servicio anfitrión 116. Como tal, en lugar de utilizar ambos billetes de reconexión primero y segundo, el método ilustrativo 900 solamente emplea el billete de reconexión único antes mencionado. En una de tales realizaciones, al agente cliente 128 del cliente 108 también se le proporciona la dirección del servicio 112 de primer protocolo. Para reconectarse con los servicios anfitriones 116, el agente cliente 128 transmite el único billete de reconexión directamente al servicio 112 de primer protocolo. El servicio 112 de primer protocolo determina entonces si es válido el único billete de reconexión. En una realización, el servicio 112 de primer protocolo determina la validez del único billete de reconexión comparándolo con una copia previamente conservada del único billete de reconexión. Si el servicio 112 de primer protocolo determina que el único billete de reconexión es válido, la conexión 135 de primer protocolo restablecida entre el cliente 108 y el servicio 112 de primer protocolo es enlazada con la conexión 124 de protocolo secundario mantenida entre el servicio 112 de primer protocolo y el o cada uno de los servicios anfitriones 116. De otro modo, si el servicio 112 de primer protocolo determina que el único billete de reconexión no es válido, la conexión 135a de primer protocolo restablecida no se enlaza con la o las conexiones 124 de protocolo secundario mantenidas y se rechaza la reconexión del cliente 108 al servicio o a los servicios anfitriones 116.

ES 2 298 835 T3

Después de validado el único billete de reconexión, el único billete de reconexión es borrado por, por ejemplo, el servicio 112 de primer protocolo y un único billete de reconexión de repuesto es generado por, por ejemplo, el servicio 112 de primer protocolo para transmisión al cliente 108. Al transmitir el único billete de reconexión de repuesto al cliente 108, el servicio 112 de primer protocolo conserva una copia del único billete de reconexión de repuesto. En algunas realizaciones, el servicio 112 de primer protocolo espera a que el cliente 108 comunique que ha recibido el único billete de reconexión de repuesto, antes de proceder a borrar el único billete de reconexión.

En todavía otra realización, al igual que el primero y el segundo billetes de reconexión, el único billete de reconexión es configurado para ser borrado automáticamente una vez transcurrido un período de tiempo predeterminado a contar de un fallo de la conexión 135, como en el paso 612, y/o a contar de una terminación limpia de la conexión 135, como en el paso 620.

Los expertos normales en la técnica pueden llevar a cabo muchas alteraciones y modificaciones sin apartarse por ello del espíritu ni del alcance del invento. Por tanto, debe comprenderse, expresamente, que las realizaciones ilustradas únicamente se han mostrado con fines de ejemplo y no deben considerarse como limitativas del invento, que queda definido por las siguientes reivindicaciones. Al leer estas reivindicaciones ha de considerarse que incluyen lo literalmente establecido en ellas y, también, los elementos equivalentes que no sean esencialmente diferentes, aún cuando no resulten idénticos, en otros aspectos, a los que se muestran y describen en las anteriores ilustraciones.

REIVINDICACIONES

1. Un método para reconectar a un cliente (108) con un servicio anfitrión (116a-116n), cuyo método se **caracteriza** por:
 - proporcionar una sesión de comunicaciones entre un cliente (108) y un servicio anfitrión (116a-116n) mediante una primer conexión entre el cliente (108) y un servicio (112) de primer protocolo, y una segunda conexión entre el servicio (112) de primer protocolo y el servicio anfitrión (116a-116n);
 - detectar una interrupción en la primera conexión o en la segunda conexión, y mantener la otra de entre la primera conexión y la segunda conexión;
 - obtener, en el servicio (112) de primer protocolo, un primer billete y un segundo billete;
 - validar el primer billete para restablecer la conexión interrumpida;
 - validar el segundo billete para continuar el uso de la conexión mantenida; y
 - enlazar la conexión restablecida con la conexión mantenida.
2. El método de la reivindicación 1, que comprende mantener la sesión de comunicaciones durante la interrupción de la conexión interrumpida.
3. El método de la reivindicación 1, que comprende además generar el primer billete o el segundo billete mediante al menos uno de entre el servicio (112) de primer protocolo o una autoridad (136) a cargo de los billetes.
4. El método de la reivindicación 1, que comprende además validar, por parte de la autoridad (136) a cargo de los billetes, al menos uno de entre el primer billete o el segundo billete.
5. El método de la reivindicación 1, que comprende además autenticar el cliente (108) frente a un servidor web (120).
6. El método de la reivindicación 1, que comprende además transmitir, mediante un servidor web (120), el primer billete al cliente (108).
7. El método de la reivindicación 1, que comprende además transmitir, mediante el cliente (108), el primer billete al servicio (112) de primer protocolo.
8. El método de la reivindicación 1, que comprende además autenticar el cliente (108), mediante el servicio anfitrión (116a-116n), al establecerse la sesión de comunicaciones.
9. El método de la reivindicación 1, en el que el servicio (112) de primer protocolo comprende un servidor representante.
10. El método de la reivindicación 1, en el que el servicio (112) de primer protocolo comprende una pasarela de seguridad.
11. El método de la reivindicación 1, en el que el cliente (108) y el servicio (112) de primer protocolo se comunican utilizando un primer protocolo (204) que encapsula a un segundo protocolo (200a-200n), y el servicio (112) de primer protocolo y el servicio anfitrión (116a-116n) se comunican utilizando el segundo protocolo (200a-200n).
12. El método de la reivindicación 1, en el que el primer billete es válido para la primera conexión y el segundo billete es válido para la segunda conexión.
13. El método de la reivindicación 1, en el que el segundo billete está inhabilitado hasta que se valida el primer billete.
14. El método de la reivindicación 1, en el que la conexión restablecida se enlaza con la conexión mantenida después de que se han validado el primer billete y el segundo billete.
15. El método de la reivindicación 1, en el que una de entre la primera conexión y la segunda conexión comprende una pluralidad de conexiones establecidas a través de uno de entre un nodo intermediario o uno o más servicios (204) de primer protocolo.
16. El método de la reivindicación 15, en el que se genera un tercer billete para, al menos, una de la pluralidad de conexiones.

ES 2 298 835 T3

17. El método de la reivindicación 16, en el que el tercer billete es válido para dicha al menos una de la pluralidad de conexiones.

18. Un sistema para reconectar un cliente (108) con un servicio anfitrión (116a-116n), cuyo sistema se **caracteriza** por:

un cliente (108) con medios para establecer una sesión de comunicaciones con un servicio anfitrión (116a-116n) mediante una primera conexión;

un servicio (112) de primer protocolo con medios para establecer la primera conexión con el cliente (108) y una segunda conexión con el servicio anfitrión (116a-116n);

comprendiendo el servicio (112) de primer protocolo con medios para mantener una conexión, al menos una de entre la primera conexión o la segunda conexión;

el servicio (112) de primer protocolo tiene medios para validar un primer billete para restablecer una conexión interrumpida en una de entre la primera conexión y la segunda conexión, y tiene medios para validar un segundo billete para uso de la otra de entre la primera conexión o la segunda conexión; y

el servicio (112) de primer protocolo tiene medios para enlazar la conexión restablecida con la conexión mantenida.

19. El sistema de la reivindicación 18, que comprende además una autoridad (136) a cargo de los billetes que tiene medios para generar al menos uno de entre el primer billete o el segundo billete.

20. El sistema de la reivindicación 18, en el que el servicio (112) de primer protocolo tiene medios para mantener la sesión de comunicaciones durante una interrupción de la conexión interrumpida.

21. El sistema de la reivindicación 18, en el que el servicio (112) de primer protocolo tiene medios para generar al menos uno de entre el primer billete o el segundo billete.

22. El sistema de la reivindicación 18, en el que la autoridad (136) a cargo de los billetes tiene medios para validar al menos uno de entre el primer billete o el segundo billete.

23. El sistema de la reivindicación 18, que comprende además un servidor web (120), cuyo servidor web (120) tiene medios para autenticar al cliente (108).

24. El sistema de la reivindicación 23, en el que el servidor web (120) tiene medios para transmitir el primer billete al cliente (108).

25. El sistema de la reivindicación 18, en el que el cliente (108) tiene medios para transmitir el primer billete al servicio (112) de primer protocolo.

26. El sistema de la reivindicación 18, en el que el servicio anfitrión (116a-116n) tiene medios para autenticar al cliente (108) al establecerse la sesión de comunicaciones.

27. El sistema de la reivindicación 18, en el que el servicio (112) de primer protocolo comprende un servidor representante.

28. El sistema de la reivindicación 18, en el que el servicio (112) de primer protocolo comprende una pasarela de seguridad.

29. El sistema de la reivindicación 18, en el que el cliente (108) y el servicio (112) de primer protocolo tienen medios para comunicarse utilizando un primer protocolo (204) que encapsula a un segundo protocolo (200a-200n), y el servicio (112) de primer protocolo y el servicio anfitrión (116a-116n) tienen medios para comunicarse utilizando el segundo protocolo (200a-200n).

30. El sistema de la reivindicación 18, en el que el primer billete es válido para la primera conexión y el segundo billete es válido para la segunda conexión.

31. El sistema de la reivindicación 18, en el que el segundo billete está inhabilitado hasta que se valida el primer billete.

32. El sistema de la reivindicación 18, en el que el servicio (112) de primer protocolo enlaza la conexión restablecida con la conexión mantenida después de que se han validado el primer billete y el segundo billete.

33. El sistema de la reivindicación 18, en el que una de entre la primera conexión y la segunda conexión comprende una pluralidad de conexiones establecidas a través de uno de entre un nodo intermediario o uno o más servicios (204) de primer protocolo.

ES 2 298 835 T3

34. El sistema de la reivindicación 33, en el que se genera un tercer billete para, al menos, una de la pluralidad de conexiones.

5 35. El sistema de la reivindicación 34, en el que el tercer billete es válido para dicha al menos una de la pluralidad de conexiones.

10

15

20

25

30

35

40

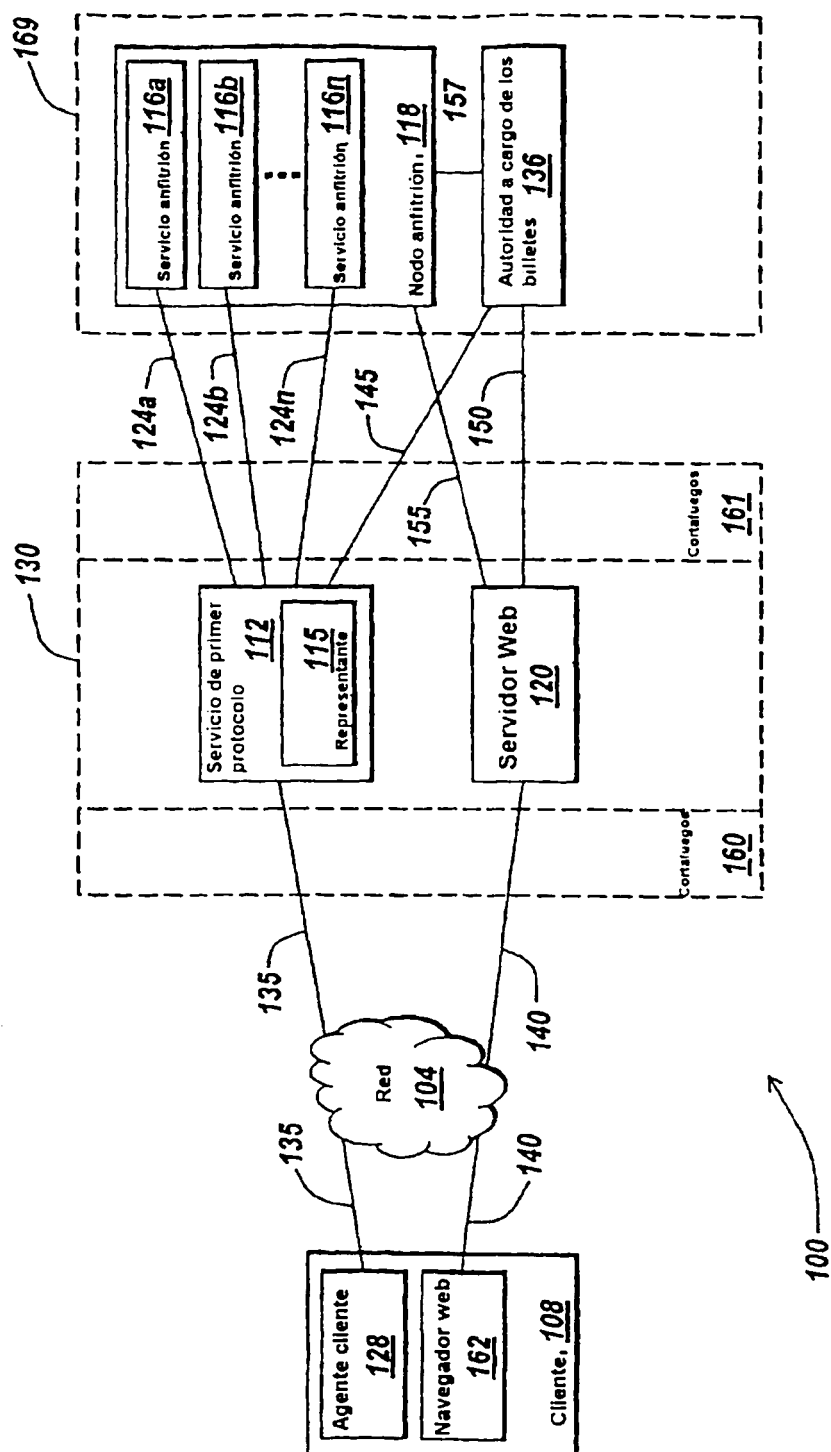
45

50

55

60

65



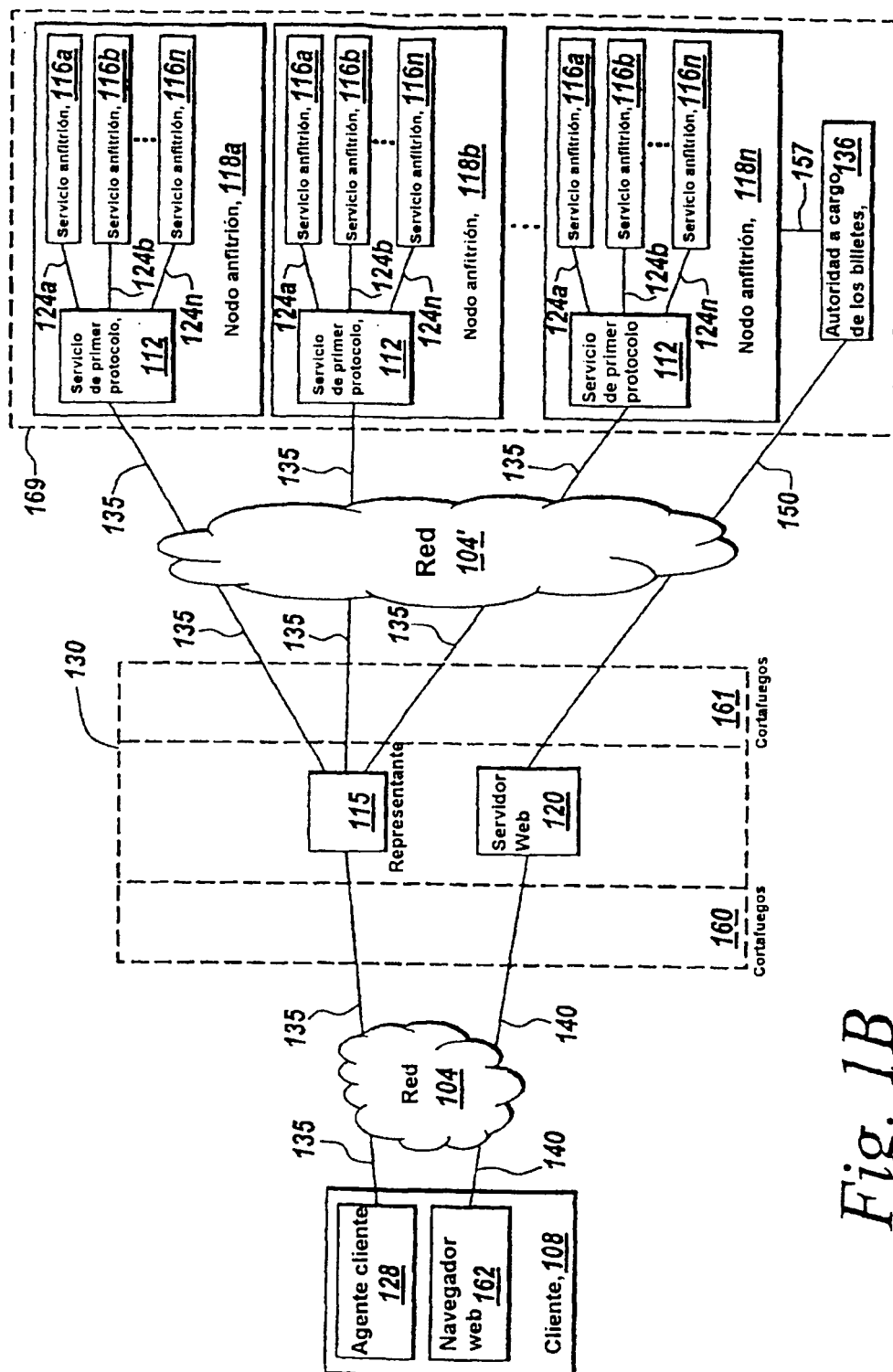


Fig. 1B

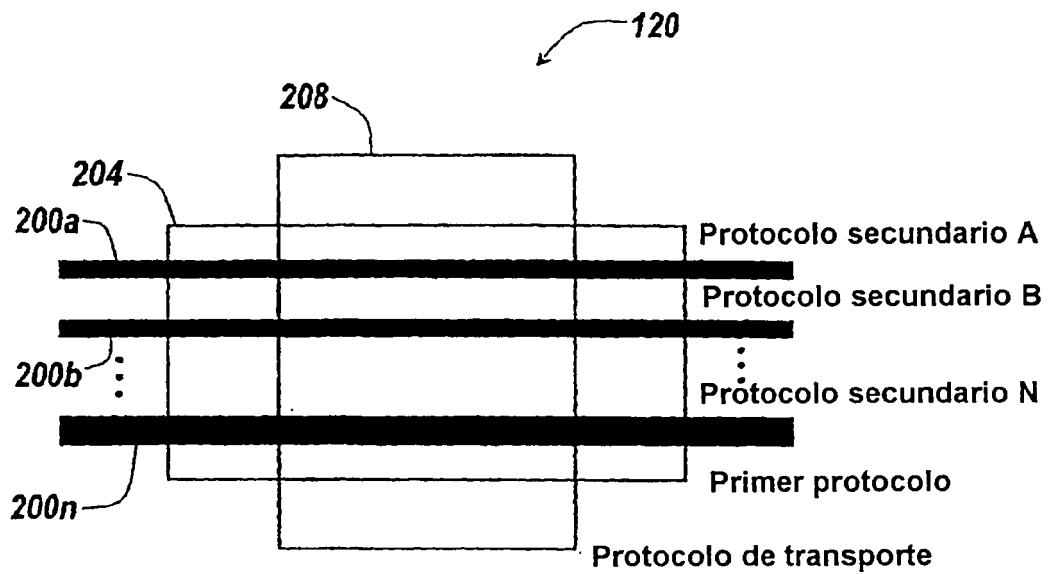


Fig. 2A

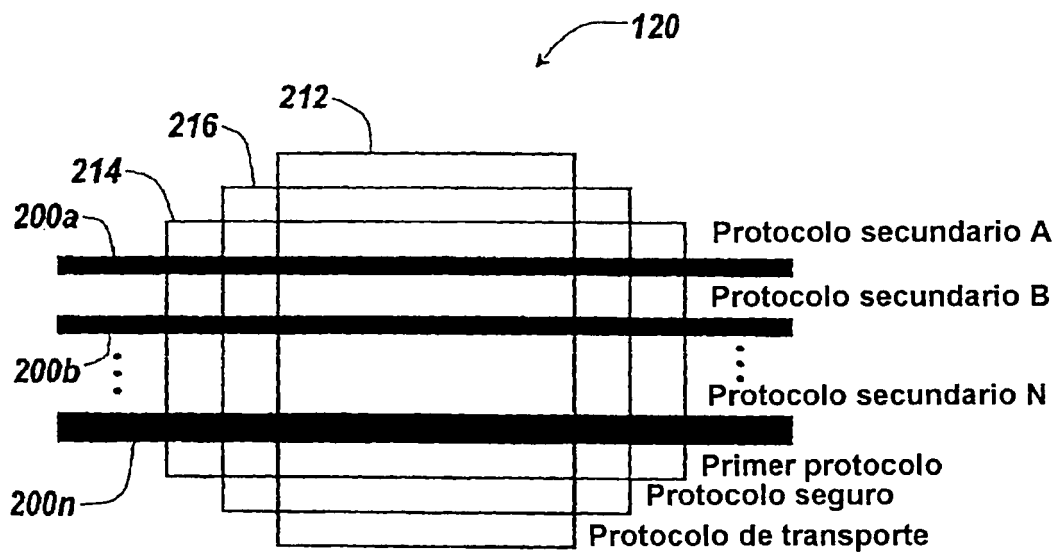


Fig. 2B

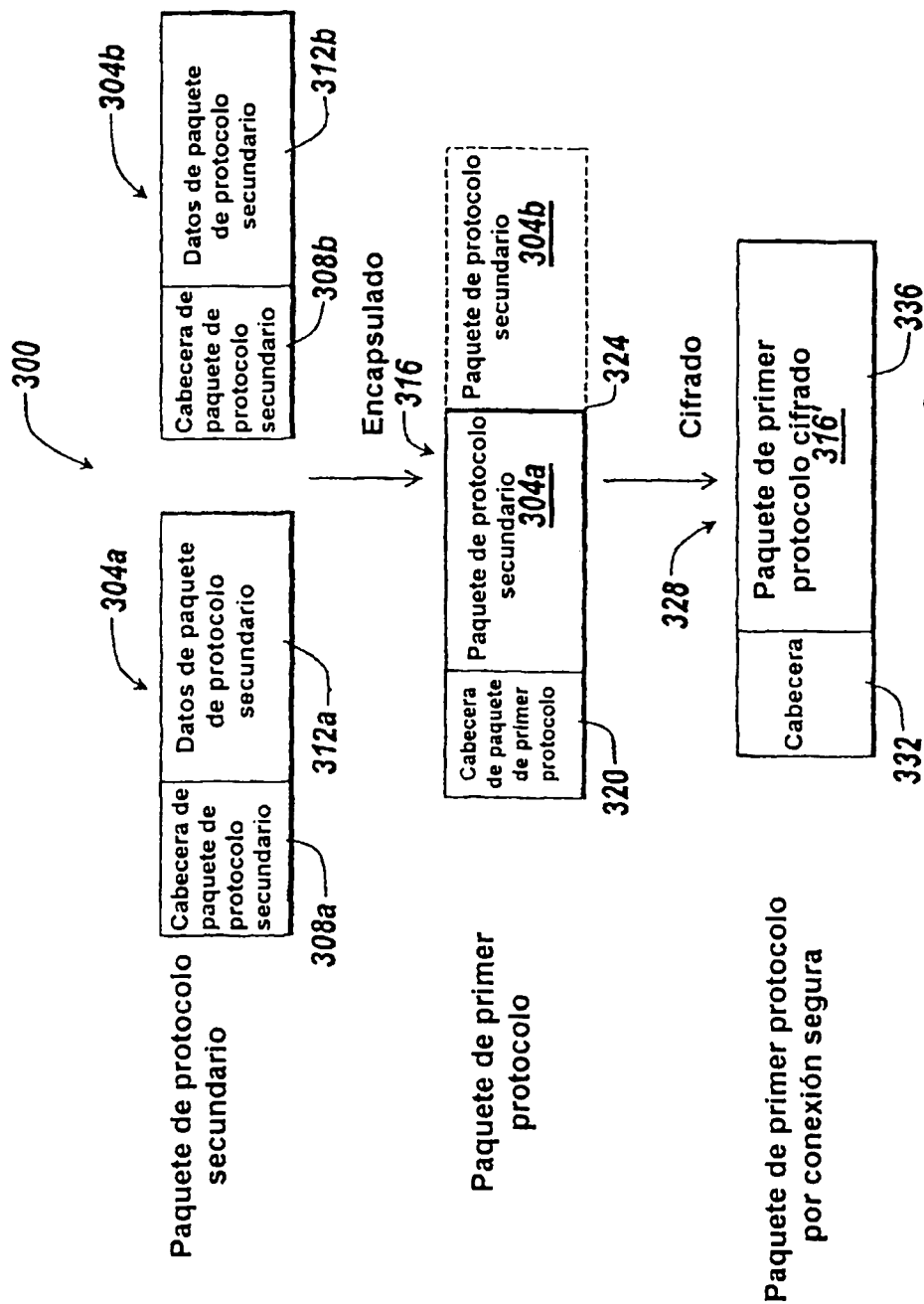


Fig. 3

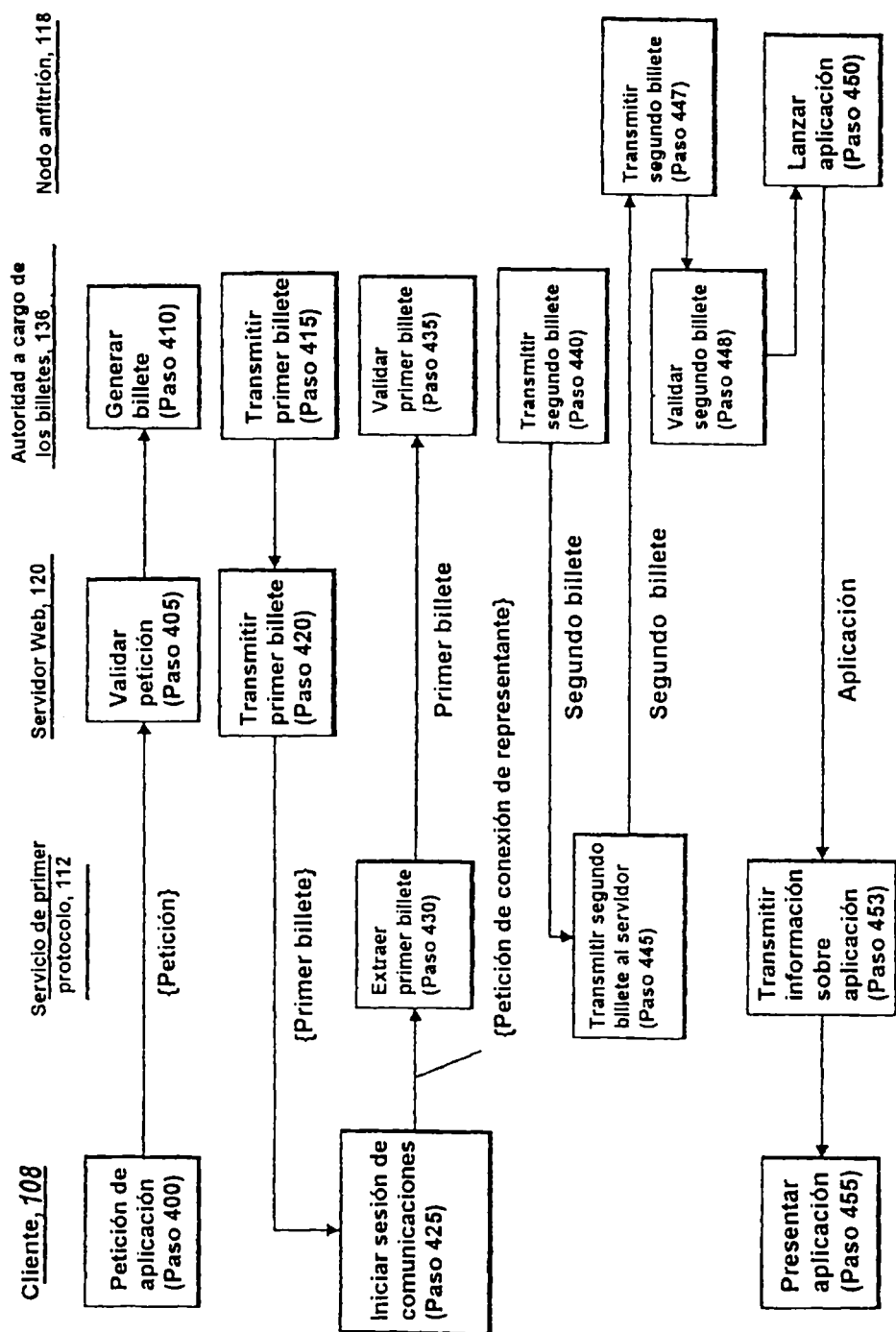


Fig. 4

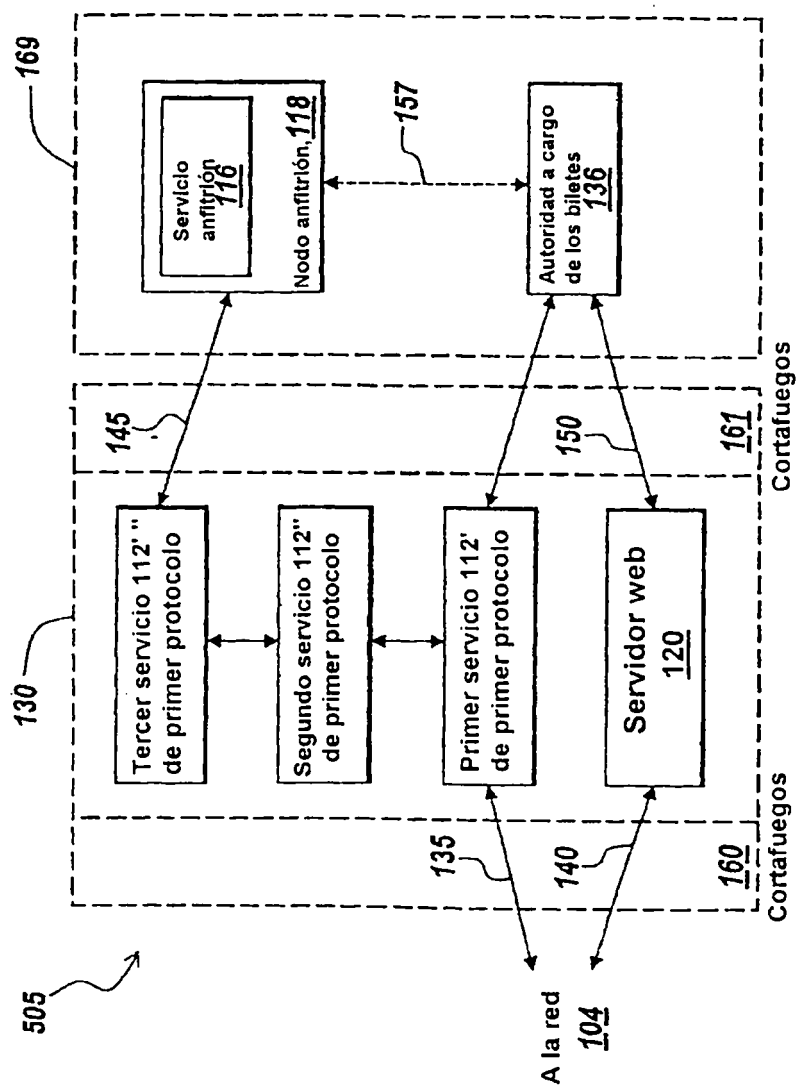


Fig. 5A

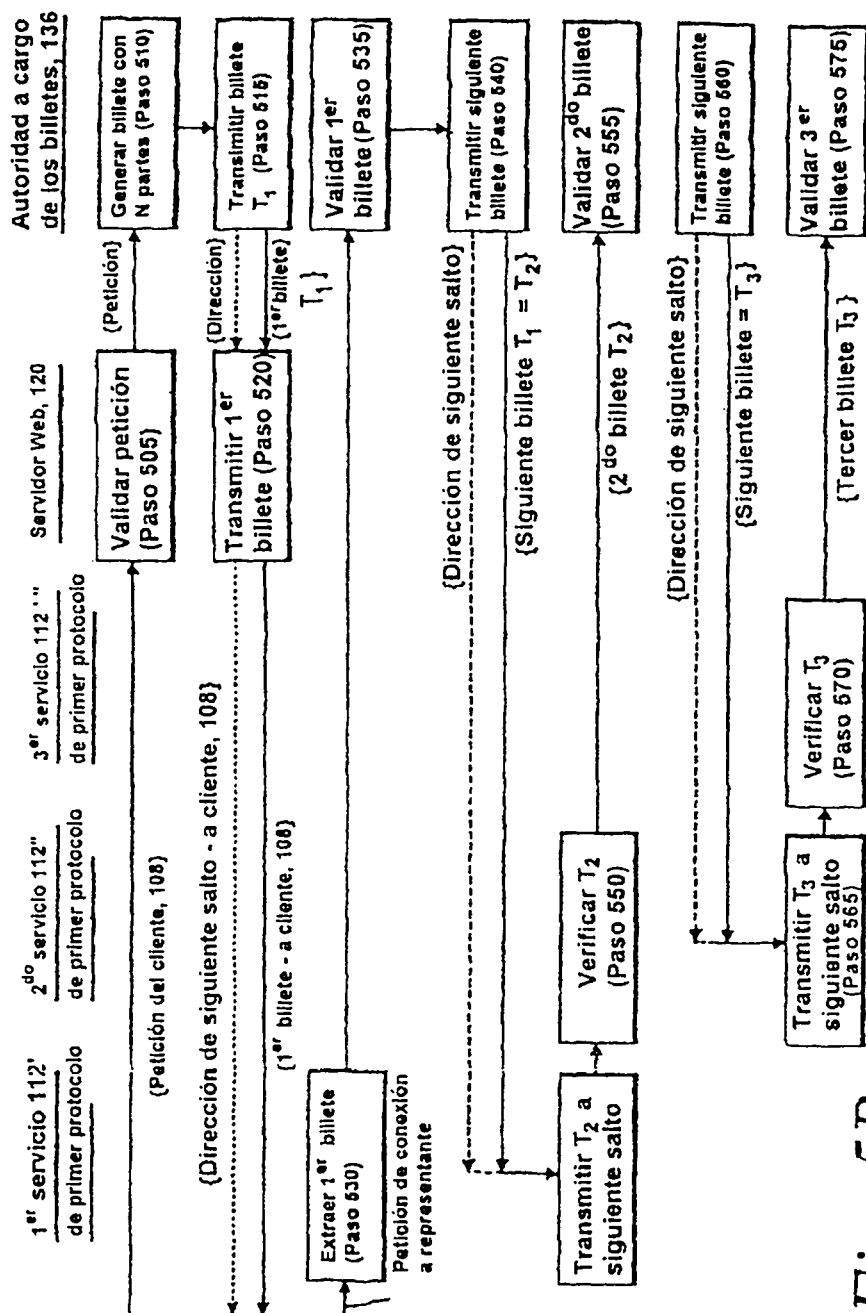


Fig. 5B

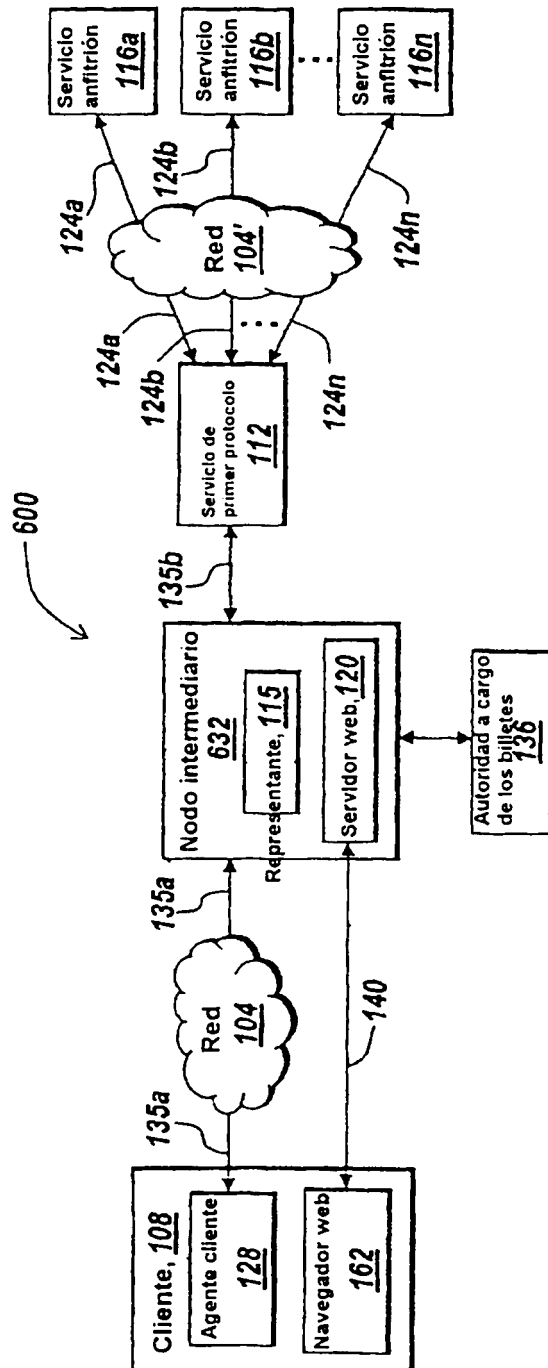


Fig. 6A

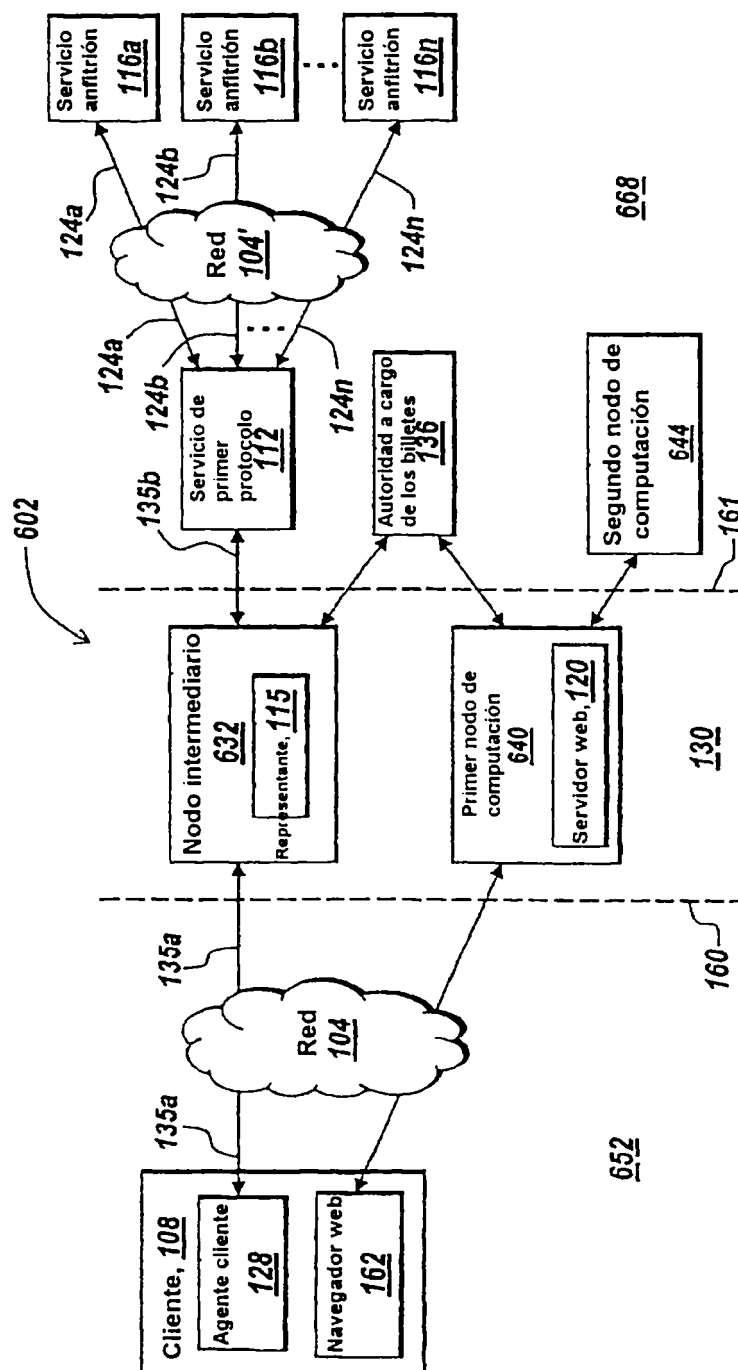


Fig. 6B

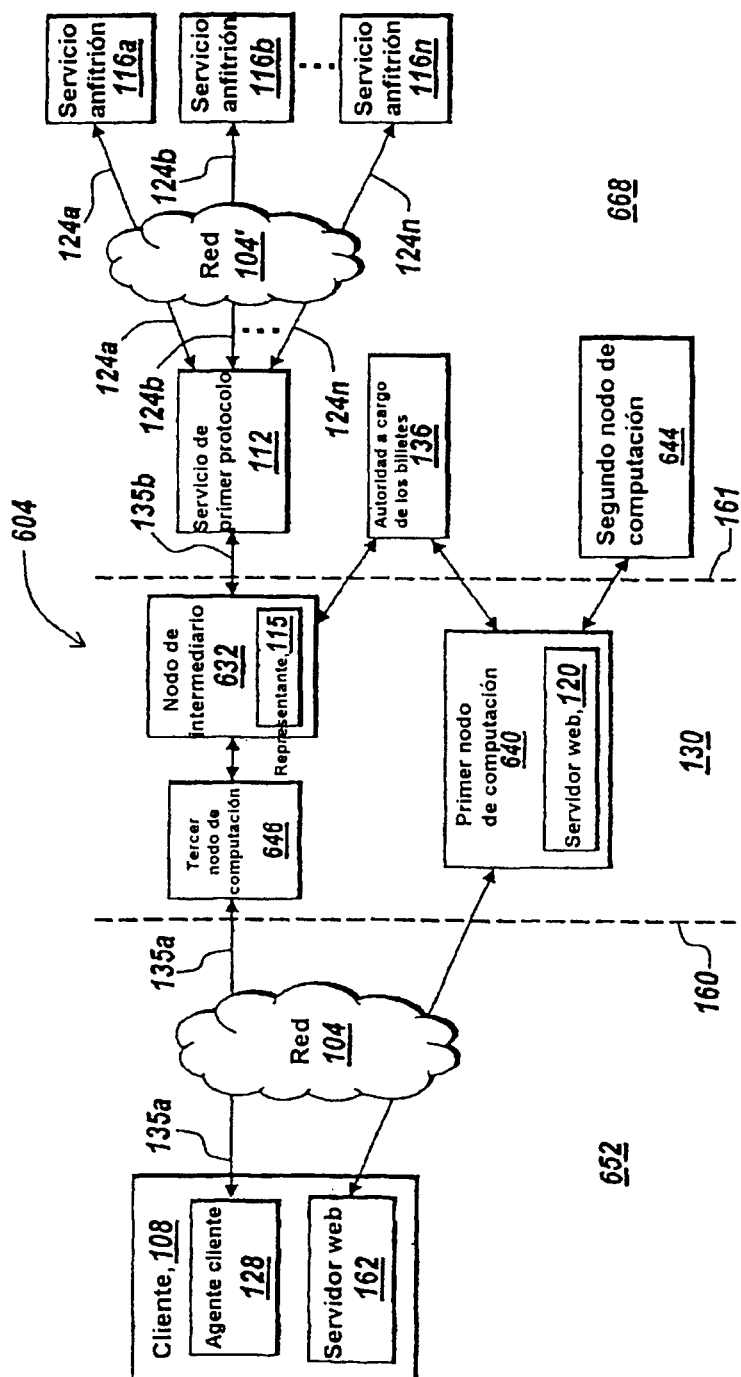


Fig. 6C

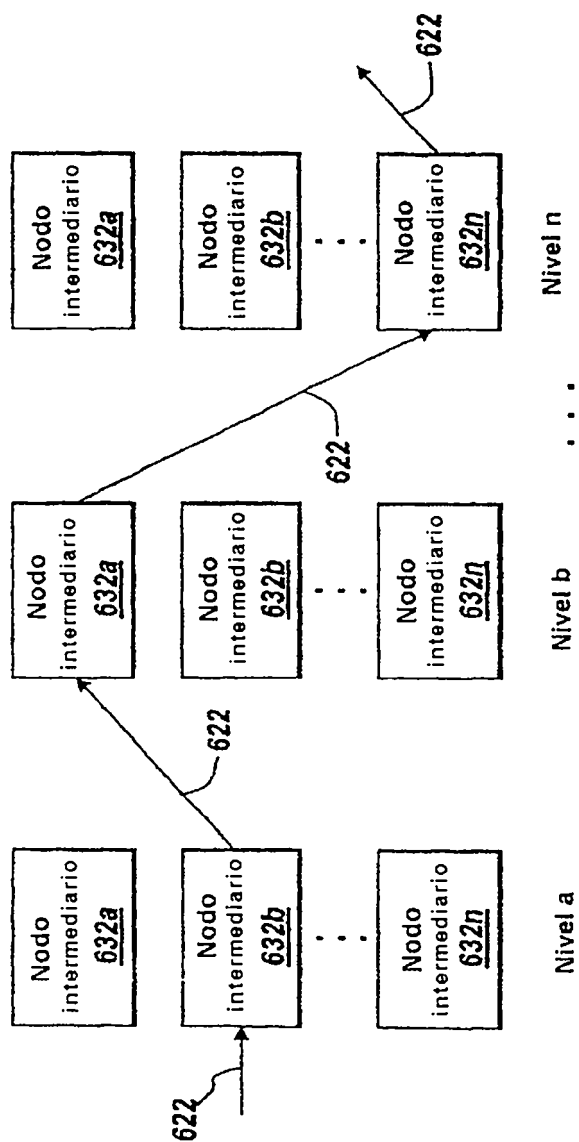


Fig. 6D

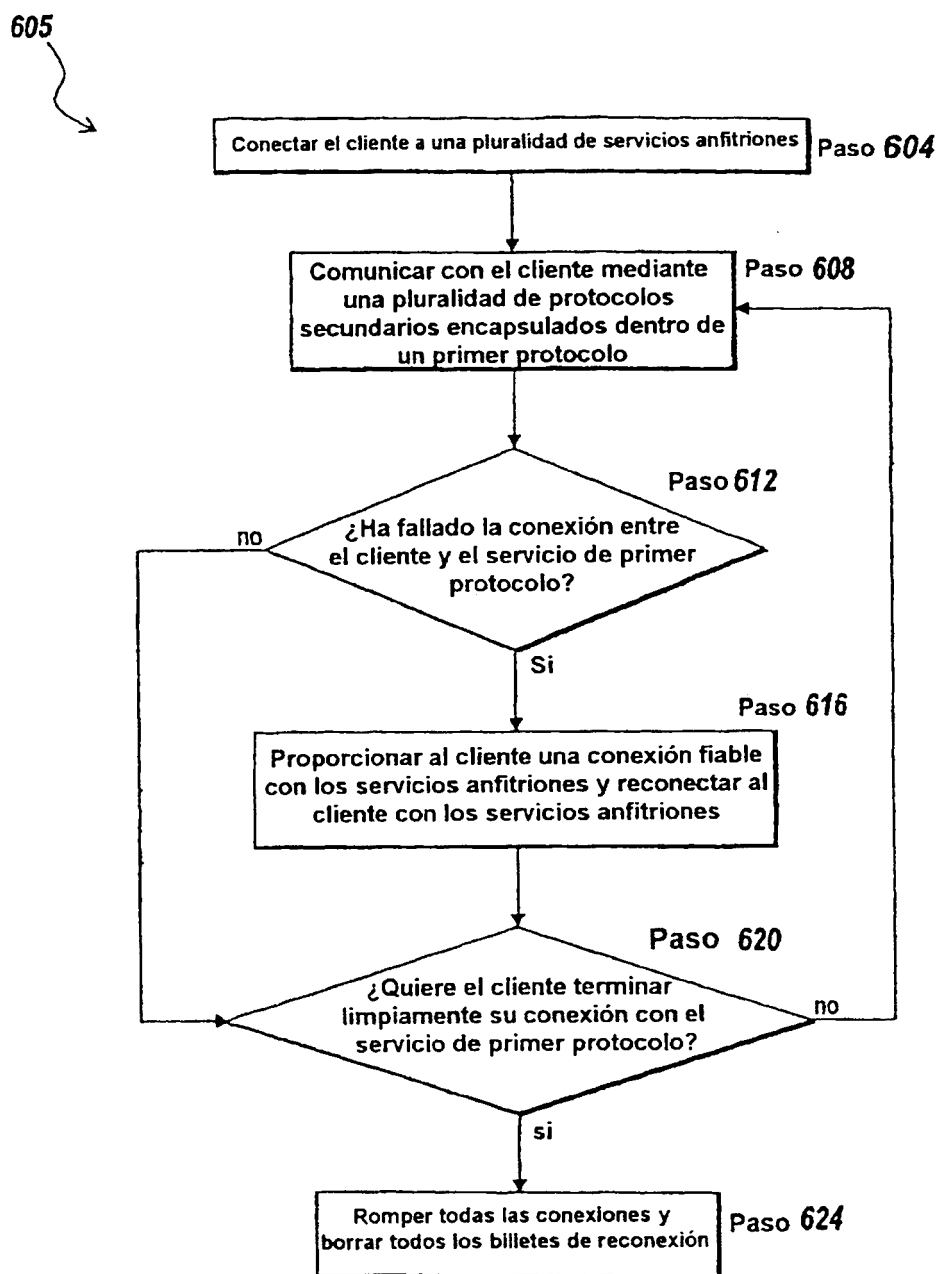
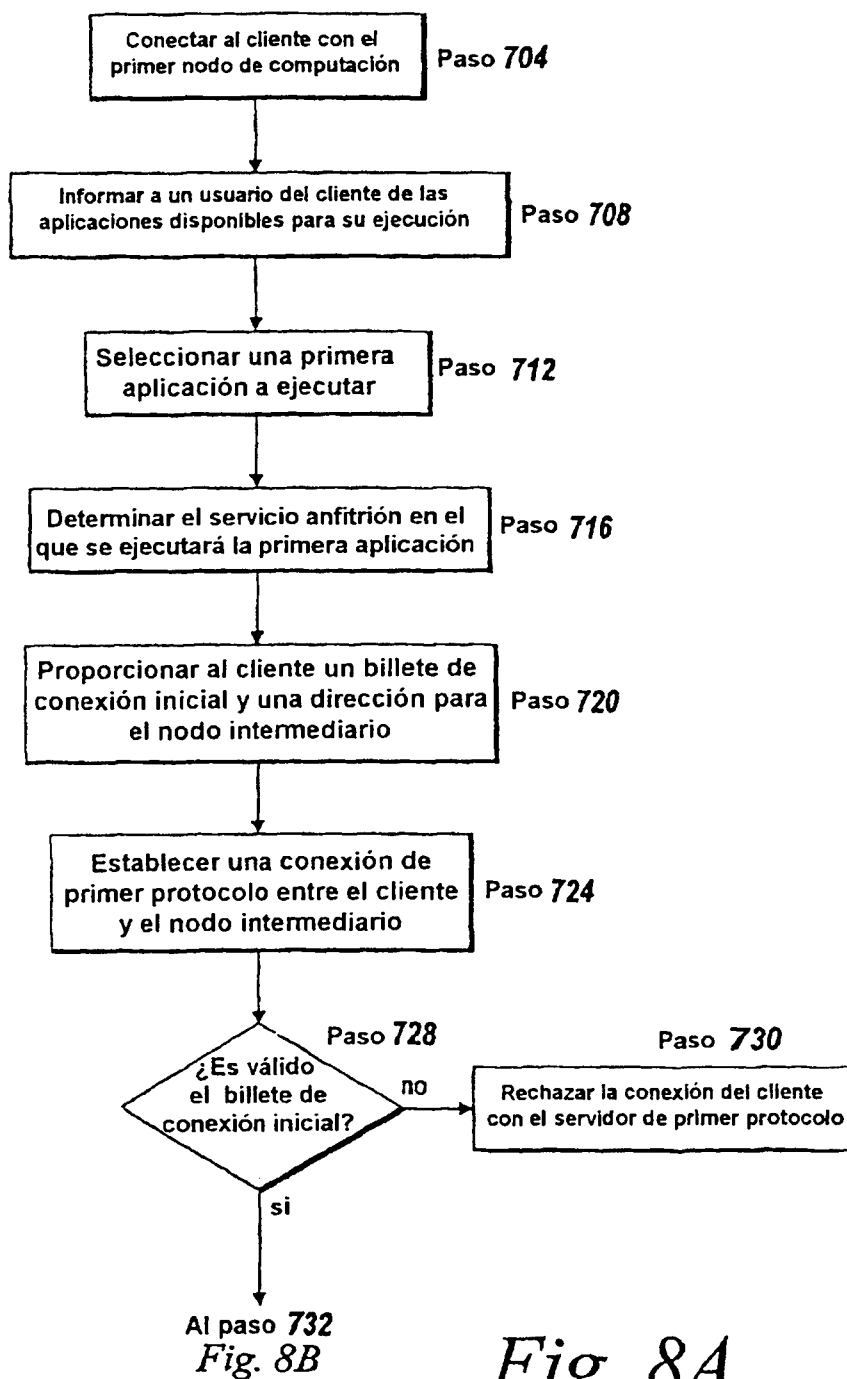
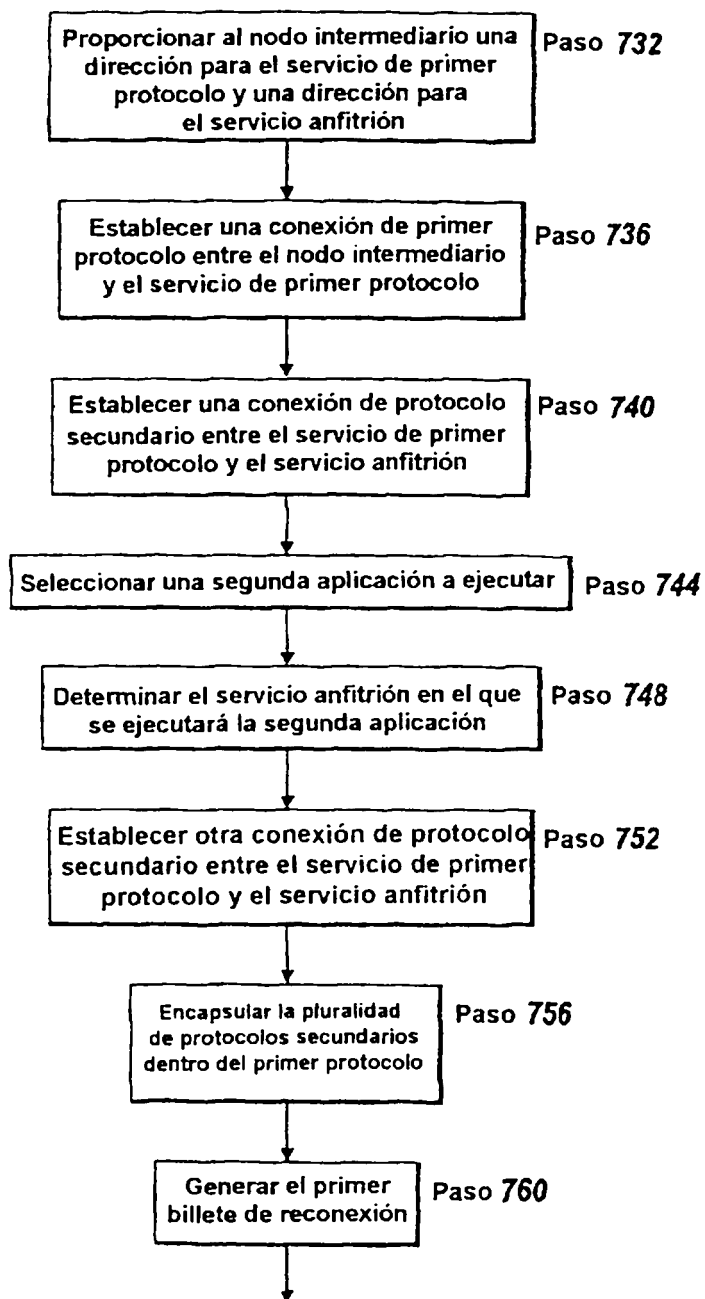


Fig. 7





Al paso 764
Fig. 8C

Fig. 8B

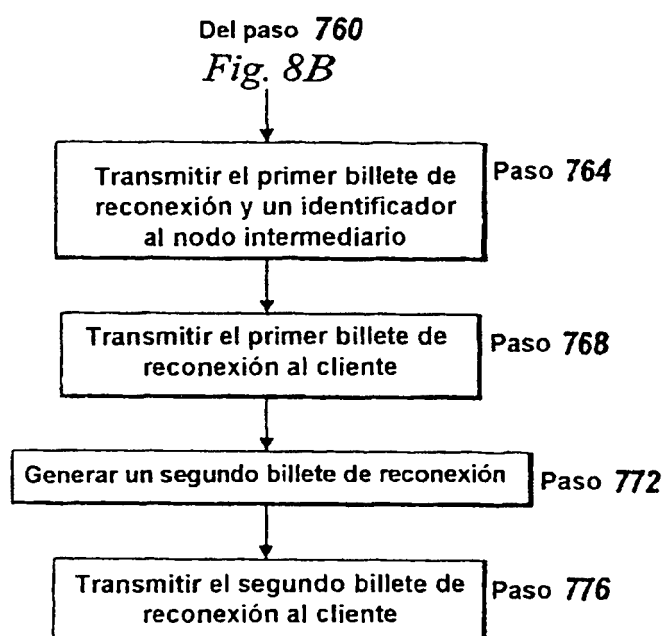


Fig. 8C

800

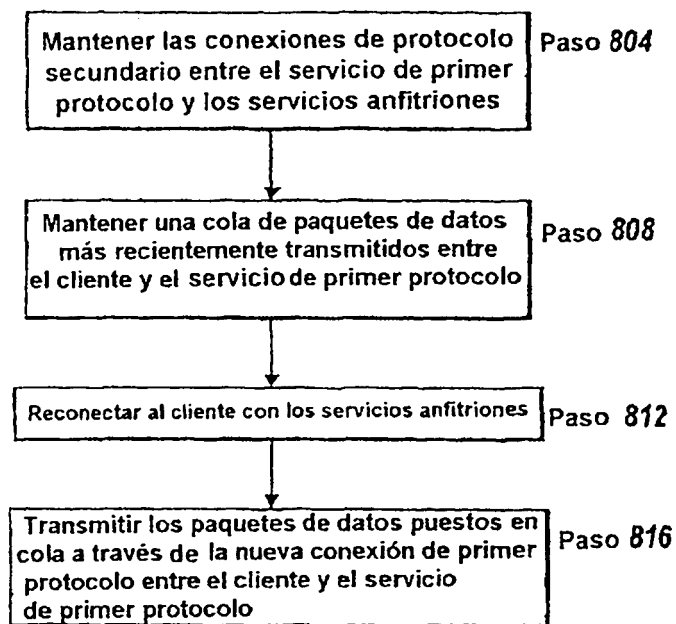


Fig. 9

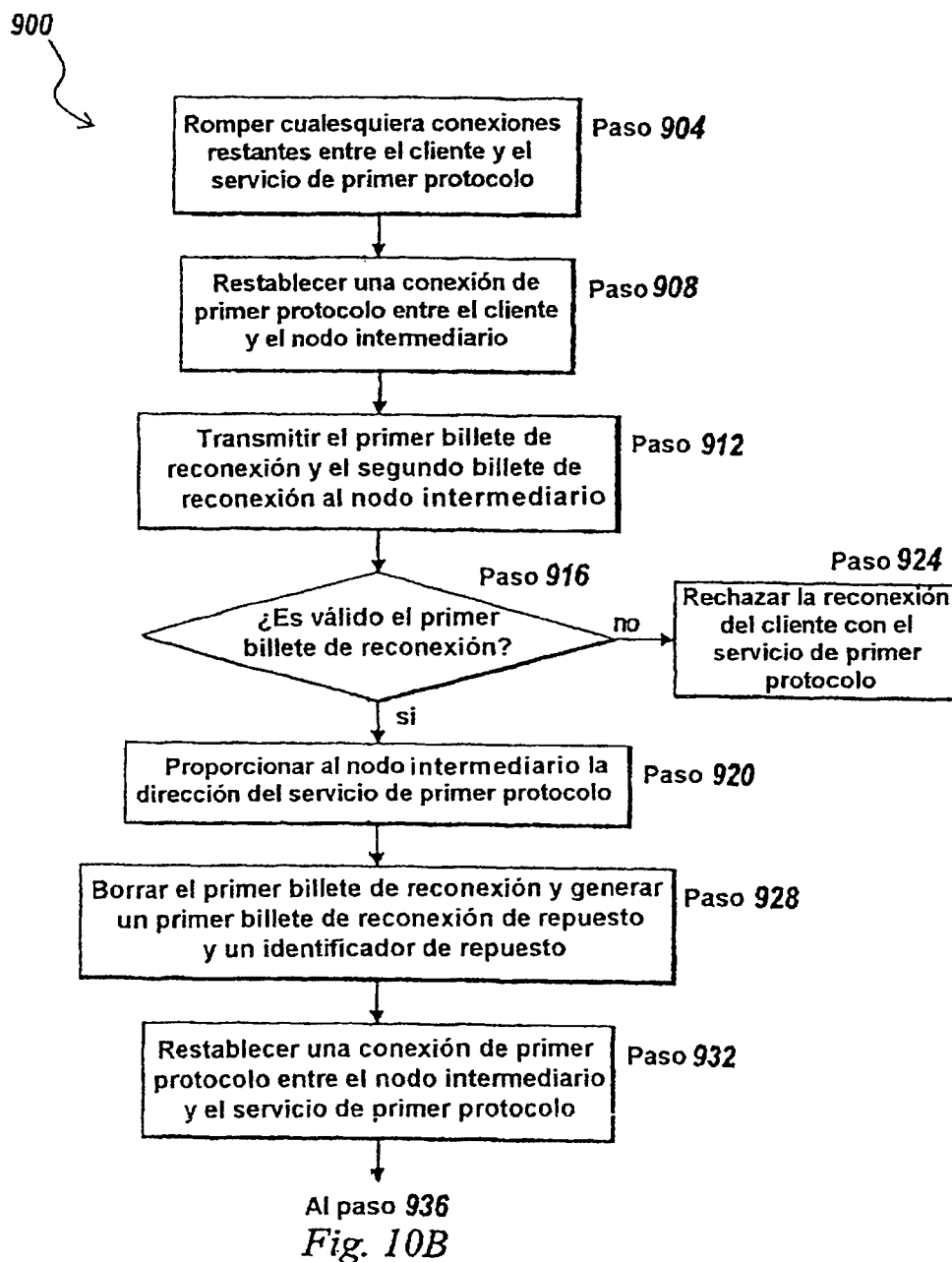


Fig. 10A

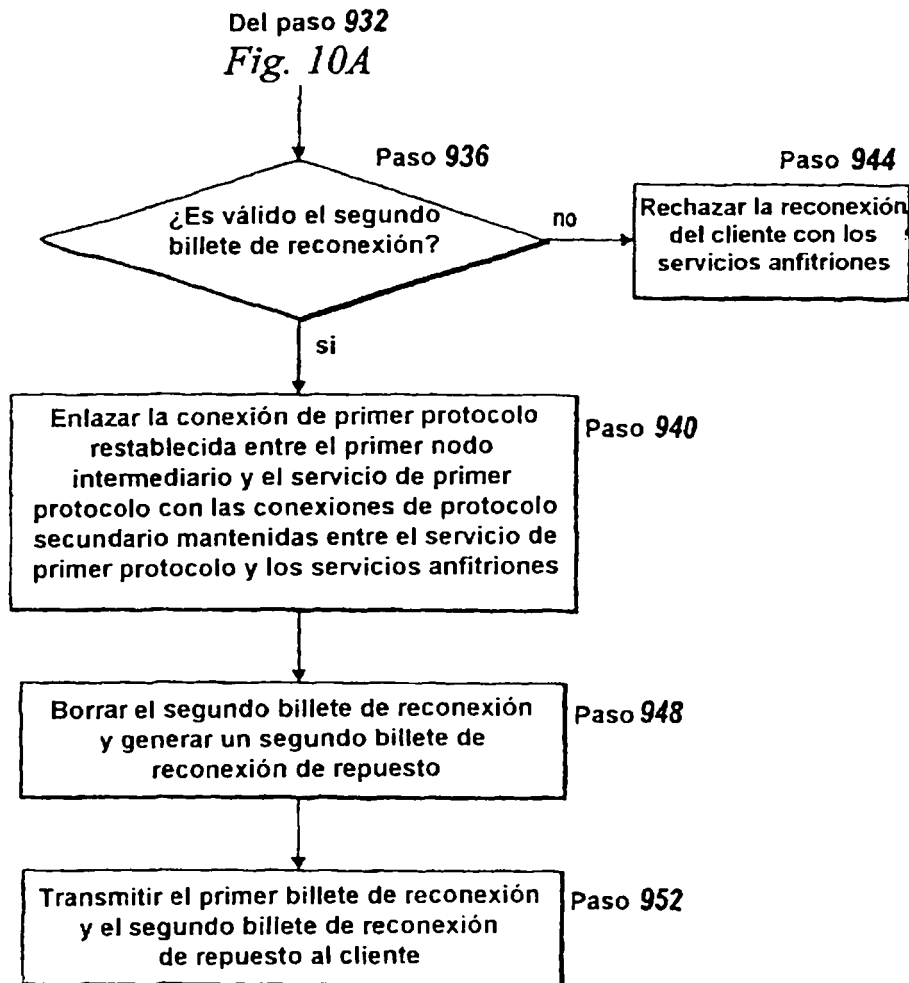


Fig. 10B