(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 600 678**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)
G06F 15/16 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.03.2011 PCT/US2011/026931**

(87) Fecha y número de publicación internacional: **09.09.2011 WO11109565**

(96) Fecha de presentación y número de la solicitud europea: **02.03.2011 E 11751325 (9)**

(97) Fecha y número de publicación de la concesión europea: **03.08.2016 EP 2543162**

(54) Título: **Inhabilitación selectiva de mecanismos de fiabilidad en conexión de red**

(30) Prioridad:

04.03.2010 US 717784

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.02.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

BANSAL, DEEPAK y
ALKHATIB, HASAN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Inhabilitación selectiva de mecanismos de fiabilidad en conexión de red

Antecedentes

Los sistemas de conexión en red a gran escala son plataformas comunes empleadas en una variedad de escenarios para la ejecución de aplicaciones y mantenimiento de datos para funciones comerciales y operacionales. Por ejemplo, un centro de datos (por ejemplo una infraestructura física informática en la nube) puede proporcionar una variedad de servicios (por ejemplo, aplicaciones web, servicios de correo electrónico, servicios de motores de búsqueda, etc.) simultáneamente para una pluralidad de clientes. Estos sistemas de conexión en red a gran escala incluyen un gran número de recursos distribuidos a lo largo del centro de datos, en el que cada recurso se asemeja a una máquina física o una máquina virtual en ejecución en un alojamiento físico. Cuando el centro de datos aloja múltiples inquilinos (por ejemplo, programas cliente), estos recursos se asignan óptimamente desde el mismo centro de datos a los diferentes inquilinos.

Los clientes del centro de datos requieren frecuentemente que se ejecuten aplicaciones comerciales en una red de empresa privada (por ejemplo, un servidor gestionado por el cliente que se sitúa geográficamente remoto respecto al centro de datos) para interactuar con el software que está siendo ejecutado sobre los recursos en el centro de datos. En este caso, se establece una conexión de red entre componentes de la aplicación comercial y los componentes del software en ejecución en el centro de datos. Esta conexión de red utiliza típicamente protocolos de transporte de la red, tales como el protocolo de control de transmisión (TCP) para facilitar una entrega fiable de paquetes a través de la conexión de red.

Esta conexión de red basada en TCP, o conexión TCP, es la responsable de la gestión de las transferencias de mensajes de extremo a extremo a través de la red de la empresa privada operando independientemente y el centro de datos. Por ejemplo, estas herramientas pueden gestionar el control de errores, la segmentación, el control de flujo, el control de la congestión, y el direccionamiento de la aplicación (por ejemplo, números de puertos). Durante la operación, un comportamiento problemático de la red, tal como la congestión de la red, y pérdidas de paquetes pueden detectarse y mejorarse por estas herramientas mediante la solicitud de retransmisiones de los paquetes perdidos, y cambio de la velocidad a la que se envían los paquetes para reducir la congestión.

Cuando una conexión basada en TCP se está ejecutando por encima de otra conexión TCP, la interacción entre estos mecanismos empleados por la conexión TCP interior y por la conexión TCP exterior pueden dar como resultado retransmisiones exageradas y estrangulamiento del flujo lo que a su vez provoca una caída significativa en el rendimiento global de la conexión. De ese modo, el empleo de las tecnologías emergentes para inhabilitar una o más de las herramientas asociadas con las capas de la comunicación basada en TCP mejoraría el resultado y el rendimiento de una conexión de red establecida mientras que aún asegura una entrega fiable de paquetes y el control de la congestión.

El documento de Osamu Honda et ál.: "Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency" (Proceedings of SPIE, vol. 6011, 23 de octubre de 2005) describe el establecimiento en la red de una tunelación de la conexión TCP sobre otro canal TCP. El documento describe un estudio de parámetros para descubrir el impacto en el rendimiento del retardo de la propagación, acuse de recibo selectivo, y tamaño de la memoria intermedia del conector para los túneles TCP sobre TCP. El documento y la técnica anterior citada en el presente documento desvelan adicionalmente el problema del "decaimiento TCP" debido a la interacción entre mecanismos de fiabilidad de las conexiones en túnel y TCP tunelada, pero el documento no describe cómo adaptar la conexión subyacente para mitigar dicho efecto de "decaimiento".

El documento de Joel Reardon et ál: "Improving Tor using a TCP over-DTLS Tunnel", 25 de mayo de 2009, se refiere a la mejora de Tor con el uso de un túnel TCP sobre DTLS. Todo el tráfico entre cualquier par de enrutadores, incluso si representan circuitos para diferentes clientes, se multiplexa a través de una conexión TCP única. Los mecanismos de control de la congestión se han aplicado injustamente a todos los circuitos cuando se pretende que estrangulen solamente los remitentes de ruido. La caída de paquetes en un circuito provoca interferencia en otros circuitos. El tunelado TCP sobre DTLS transporta paquetes TCP entre iguales usando DTLS, un transporte seguro de datagramas (basado en UDP). Una pila TCP de nivel de usuario en ejecución dentro del Tor genera y analiza paquetes TCP que se envían sobre DTLS entre enrutadores en línea (OR). Usa una conexión TCP de nivel de usuario separada para cada circuito. Esto elimina la correlación de los circuitos a los flujos TCP. Se emplea una pila TCP de nivel de usuario para generar paquetes TCP, que se encapsulan dentro de un paquete DTLS que se envía a continuación por un sistema en un datagrama UDP IP. El sistema receptor eliminada la cabecera UPD/IP cuando recibe los datos desde el conector, descifrando la carga útil DTLS para obtener el paquete TCP, y lo traduce en un paquete TCP/IP que se envía a continuación a la pila TCP de nivel de usuario que procesa el paquete.

El documento US 2009/222906 A1 se refiere a un sistema de comunicación informático para la comunicación a través de redes públicas. El PPTP, el "Protocolo de Tunelación Punto a Punto" encapsula datos VPN dentro de paquetes PPP. El PPTP usa una conexión TCP. Los clientes VPN construidos dentro del sistema operativo pueden usar alternativamente el L2TP, el "Protocolo de Tunelado Capa 2". Los paquetes L2TP se envían a través de un

puerto UDP 1701. El SSL-VPN usa el puerto TCP 443, que se usa normalmente para conexiones HTTPS cifradas a la Internet pública, y por lo tanto el tráfico destinado al puerto TCP 443 no es bloqueado en los cortafuegos. PPP, PPTP, o L2TP se tunelan usando SSL sin la necesidad de instalar manualmente y configurar software cliente VPN.

El documento "Space Communications Protocol Specification (SCPS) - Transport Protocol (SCPS-TP)", de 1 de octubre de 2006, se refiere a la especificación del protocolo de comunicación espacial (SCPS) - protocolo de transporte (SCPS-TP). Se realizan modificaciones y extensiones al TCP y al UDP para su uso en los entornos de comunicaciones aeroespaciales, caracterizadas potencialmente por largos retardos, tasas de datos del enlace directo e inverso desequilibradas, y tasas de error potencialmente altas. La total fiabilidad del servicio es proporcionada por el TCP. El servicio del mejor esfuerzo es proporcionado por TCP con modificaciones menores. El servicio de fiabilidad mínima es proporcionado por UDP. El TCP que inicia la conexión debe invocar las capacidades SCPS mediante la inclusión de la opción de capacidades SCPS en la cabecera del segmento SYN. La escucha TCP deberá indicar su disposición a usar las capacidades especificadas incluyendo la opción de capacidades SCPS en la cabecera del segmento SYN ACK. Cuando se elige la implementación no para proporcionar control de congestión, los siguientes algoritmos no están disponibles: el algoritmo de arranque lento de Van Jacobson; el algoritmo de evitación de la congestión de Van Jacobson; el retroceso exponencial del temporizador de retransmisión para retransmisiones sucesivas. Para retransmisiones de datos en las que no hay indicación de que se esté experimentando corrupción, el algoritmo de retroceso exponencial debería usarse para calcular valores de tiempos de retransmisión sucesivos para el mismo segmento. Una implementación conforme debería proporcionar al protocolo de la capa de aplicación (ALP) un mecanismo para especificar los siguientes parámetros en relación al BETS: habilitación BETS - la operación BETS debe habilitarse mediante una aplicación antes o en cualquier momento del establecimiento de la conexión si ha de usarse en cualquier momento en la conexión; límite de retransmisión BETS (R2) - número máximo de retransmisiones antes de que comience la operación de envío en el lado BETS.

Sumario

Es el objeto de la presente invención simplificar la comunicación entre un punto final de origen y punto final de destino a través de un túnel basado en TCP sin degradación del rendimiento.

Este objeto se resuelve mediante la materia sujeto de las reivindicaciones independientes.

Las reivindicaciones preferidas se definen por las reivindicaciones dependientes.

El presente sumario se proporciona para introducir conceptos en una forma simplificada que se describen adicionalmente a continuación en la Descripción detallada. Este sumario no se pretende que identifique características claves o características esenciales de la materia sujeto reivindicada, ni se pretende que se use como una ayuda en la determinación del alcance de la materia sujeto reivindicada.

Realizaciones de la presente invención proporcionan sistemas, procedimientos, y medios legibles por ordenador que configuran herramientas (por ejemplo mecanismos de fiabilidad) que se ejecutan integralmente con túneles basados en el protocolo de control de transmisión (TCP) y que sirven para combatir una degradación del rendimiento no garantizada provocada por esfuerzos duplicados de esas herramientas. Típicamente, los túneles basados en TCP funcionan como conexiones de red entre puntos finales dispersamente localizados. Por ejemplo, los puntos finales pueden incluir un punto final de origen alojado en una plataforma informática en la nube y un punto final de destino alojado en un recurso dentro una red de empresa privada.

Las realizaciones ejemplares de estas herramientas de configuración pertenecen a la habilitación e inhabilitación de modo selectivo de mecanismos de fiabilidad (por ejemplo, mecanismos de control de la congestión y mecanismos de recuperación de pérdidas) individualmente sobre conexiones respectivas que comprenden el túnel basado en TCP. En un caso, estos canales incluyen una conexión basada en TCP de nivel inferior y una conexión basada en TCP de nivel superior. Durante la operación, los paquetes de datos de la aplicación se transmiten a través de la conexión basada en TCP de nivel superior en ejecución por encima de la conexión basada en TCP de nivel inferior.

En realizaciones, puede emplearse un controlador matricial para permitir la habilitación (activación) del mecanismo de control de la congestión y/o del mecanismo de recuperación de pérdidas, construidos dentro de la conexión basada en TCP de nivel inferior. La inhabilitación selectiva de uno o más mecanismos de fiabilidad integrados dentro del canal basado en TCP de nivel inferior puede invocarse mediante criterios predefinidos (por ejemplo instrucciones desde el modelo de servicio informático en la nube, identidad de un punto final de origen, identidad y punto final de destino, y similares), que pueden invocarse basándose en cada conexión de red. En esta forma, las herramientas del canal basado en TCP de nivel superior imponen activamente un conjunto de reglas de fiabilidad que aseguran la entrega completa y eficiente de los paquetes de datos sobre el túnel basado en TCP, mientras que se desactivan una o más de las herramientas del canal basado en TCP de nivel inferior para reducir la degradación potencial del rendimiento resultante de los esfuerzos redundantes de los mismos.

Breve descripción de los dibujos

Se describen en detalle a continuación realizaciones de la presente invención con referencia a las figuras de los

dibujos adjuntos, en las que:

la FIG. 1 es un diagrama de bloques de un entorno informático ejemplar adecuado para su uso en la implementación de las realizaciones de la presente invención;
la FIG. 2 es un diagrama de bloques que ilustra una plataforma informática ejemplar en la nube, adecuada para el uso en la implementación de las realizaciones de la presente invención, que se provee para configurar mecanismos de fiabilidad construidos dentro de un túnel basado en el protocolo de control de transporte (TCP);
la FIG. 3 es un diagrama de bloques de un entorno informático distribuido ejemplar con un túnel basado en TCP establecido en él, de acuerdo con una realización de la presente invención;
la FIG. 4 es una representación esquemática de una disposición en capas de canales basados en TCP que comprenden el túnel basado en TCP, de acuerdo con una realización de la presente invención;
la FIG. 5 es un diagrama de bloques de un centro de datos ejemplar que emplea un controlador matricial para habilitar/inhabilitar selectivamente mecanismos de fiabilidad construidos dentro de los túneles basados en TCP, de acuerdo con realizaciones de la presente invención; y
las FIGS. 6 y 7 son diagramas de flujo que muestran procedimientos para facilitar la comunicación a través de una conexión de red establecida entre una pluralidad de puntos finales que residen en localizaciones dispares, de acuerdo con una realización de la presente invención.

Descripción detallada

La materia sujeto de las realizaciones de la presente invención se describe con especificidad en el presente documento para cumplir requisitos reglamentarios. Sin embargo, la descripción en sí no se pretende que limite el alcance de la presente patente. Por el contrario, los presentes inventores han contemplado que la materia sujeto reivindicada podría realizarse también en otras formas, para incluir diferentes etapas o combinaciones de etapas similares a las descritas en el presente documento, en conjunto con otras tecnologías presentes o futuras. Más aún, aunque los términos "etapa" y/o "bloque" pueden usarse en el presente documento para connotar diferentes elementos o procedimientos empleados, los términos no deberían interpretarse como la implicación de cualquier orden particular en medio de o entre varias etapas desveladas en el presente documento a menos y con la excepción de cuando el orden de las etapas individuales se describe explícitamente.

Las realizaciones de la presente invención se refieren a procedimientos, sistemas informáticos, y medios legibles por ordenador para el establecimiento y configuración de túneles que abarcan redes localizadas remotamente o puntos finales dentro de una red conectada. Como se usa en el presente documento, el término "túnel" se quiere indicar que es limitativo, pero puede englobar cualquier conexión de red que enlace comunicativamente un punto final de origen y un punto final de destino, con la intención de puentear la comunicación sobre redes dispares. En un caso, un túnel puede establecerse como conexión de red que transmite paquetes de datos entre puntos finales alojados en redes locales separadas, en donde los puntos finales se descubren e identifican por medio de direcciones del protocolo de Internet (IP) asignadas a ellos. Adicionalmente, la transmisión de paquetes de datos, y otro tráfico, puede atravesar múltiples enlaces, cortafuegos, y otras medidas de seguridad cuando se trasladan a través de un túnel. Esta conexión ostensiblemente directa entre los puntos finales permite que ambos puntos finales hablen en una forma similar a como si estuvieran situados adyacentes en una red común que comunica a través de la capa IP.

En algunas realizaciones, el túnel se establece usando el protocolo de control de transporte (TCP) o el protocolo de transferencia de hipertexto (HTTP), o el HTTP seguro (HTTPS), respectivamente, en los que los puntos finales pueden o no participar. El túnel conecta ventajosamente los puntos finales y habilita la comunicación a través de una red o redes dispares. Por ejemplo, un túnel HTTP o HTTPS ofrece a los puntos finales la capacidad de establecer una conexión de nivel IP virtual directa incluso cuando los puntos finales estén en dos redes dispares. En otras palabras, el túnel permite que ambos puntos finales hablen de la misma manera a como si estuvieran situados adyacentes en una red común comunicando a través de la capa IP. A modo de ejemplo, una aplicación actualmente en ejecución sobre los dos puntos finales puede no ser consciente de que los puntos finales de la misma están residiendo en dos redes dispares; por ello, la aplicación no es consciente de que se está ejecutando por encima de un túnel. Esta característica de un túnel HTTP o HTTPS es un producto de la capacidad de las conexiones de red basadas en HTTP y HTTPS para contornear cortafuegos y otros dispositivos de los bordes de la red tales como servidores de proximidad.

Adicionalmente, los túneles HTTP o HTTPS están soportados por conexiones basadas en TCP que tienen mecanismos de fiabilidad de extremo a extremo construidos en ellas, dado que las conexiones basadas en TCP se utilizan en un amplio intervalo de varias redes. Estos mecanismos de fiabilidad realizan funciones, tales como la recuperación de pérdidas y control de la congestión para gestionar las pérdidas y congestión sobre estos enlaces que conectan estas diversas redes. En otras palabras, TCP está provisto con mecanismos de fiabilidad integrados para la detección de pérdida de paquetes y la detección de congestión, y para responder a cada uno. En un caso, tras la detección de la congestión en una conexión basada en TCP, la respuesta del mecanismo de fiabilidad puede ser reducir la tasa a la que se distribuye el tráfico de paquetes de datos a través de la conexión de red. En otro caso, tras la detección de paquetes perdidos en una conexión basada en TCP, la respuesta del mecanismo de fiabilidad puede ser retransmitir los paquetes de datos perdidos.

Potencialmente, puede haber dos o más conexiones basadas en TCP en ejecución, una encima de la otra, durante la conexión TCP de extremo a extremo. En esta situación, si tiene lugar una pérdida de paquetes o congestión de la red, entonces los mecanismos de fiabilidad integrados en cada una de las conexiones en capas responden independientemente a la pérdida de paquetes y a la congestión de la red sin comunicación entre ellos. Por ejemplo, el mecanismo de recuperación de pérdidas de una conexión basada en TCP del nivel superior puede intentar realizar su propia respuesta además de la respuesta desde el mecanismo de recuperación de pérdidas de la conexión de nivel inferior. Esto es, ambos mecanismos de recuperación de pérdidas reenvían los datos, provocando una degradación incrementada e innecesaria del rendimiento de la conexión de red.

También, ambos canales pueden tener mecanismos de control de la congestión que pueden reaccionar a la pérdida de paquetes como un problema de la congestión y, tras la operación en conjunto, duplicar sus esfuerzos cuando estrangulan la tasa de transmisión. Por ejemplo, si ambos mecanismos de control de la congestión reducen la tasa de la transmisión de paquetes de datos a la mitad, el efecto agregado es una reducción en la tasa a un cuarto, que es bastante más allá de lo necesario para resolver el problema de pérdida de paquetes. Por ello, estas correcciones duplicadas, en efecto, compensan en exceso la causa y se convierten en inefectivas. Esta sobrecompensación crea frecuentemente un impacto adverso sobre la comunicación entre los puntos finales que incrementa la latencia más allá de lo que es deseable para acometer adecuadamente los problemas de pérdida de paquetes pendientes o congestión de la red.

En un aspecto, realizaciones de la presente invención se refieren a uno o más medios legibles por ordenador que tienen instrucciones ejecutables por ordenador realizadas en los mismos que, cuando se ejecutan, realizan un procedimiento para la comunicación a través de una conexión de red establecida entre una pluralidad de puntos finales que residen en redes dispares. Inicialmente, el procedimiento incluye una etapa para proporcionar la conexión de red que se extiende entre un punto final de origen y un punto final de destino. Como se ha explicado anteriormente, la conexión de red funciona como un túnel basado en TCP que puentea las redes dispares en las que residen el punto final de origen y el punto final de destino, respectivamente. El procedimiento implica adicionalmente las etapas de inhabilitar selectivamente uno o más mecanismos de fiabilidad del nivel inferior, que se ejecutan integralmente sobre el túnel basado en TCP, y mensajes de comunicación entre el primer punto final y el segundo punto final sin que los mecanismos de fiabilidad del nivel inferior interfieran con unos tiempos en los que los mensajes se envían. En realizaciones, los mensajes de comunicación entre el primer punto final y el segundo punto final pueden incluir específicamente la transmisión de paquetes IP desde el primer punto final al segundo punto final a través del túnel basado en TCP.

En una realización ejemplar, los mecanismos de fiabilidad del nivel inferior comprenden un mecanismo de control de la congestión y un mecanismo de pérdida de paquetes. El mecanismo de control de la congestión puede configurarse para manejar una cantidad de datos que se transporta dentro de los paquetes IP. El mecanismo de pérdida de paquetes puede configurarse para manejar la pérdida de paquetes a través de la conexión de red mediante la retransmisión automáticamente de los paquetes IP no entregados o retrasados.

En otro aspecto, realizaciones de la presente invención se refieren a un sistema informático para la gestión de un flujo de datos entre puntos finales que residen en redes locales individuales. Inicialmente, el sistema informático incluye los siguientes elementos: un centro de datos dentro de una plataforma informática en la nube, un recurso dentro de una red de empresa privada, un controlador matricial y una máquina virtual. En realizaciones, el centro de datos puede alojar un punto final de origen que se asigna a una aplicación en ejecución tanto en la plataforma informática en la nube como en una red de empresa privada. El recurso puede alojar un punto final de destino que se asigna también a la aplicación. Tras el inicio de una comunicación entre ellos, el punto final de origen y el punto final de destino se conectan mediante un túnel que transporta el flujo de datos directamente entre ellos, en donde el túnel puede incluir una conexión de nivel superior en ejecución por encima de una conexión de nivel inferior. Como se ha explicado anteriormente, están construidos dentro de cada una de la conexión de nivel superior y la conexión de nivel inferior, un mecanismo de control de la congestión y un mecanismo de pérdida de paquetes, respectivamente.

El controlador matricial se ejecuta dentro del centro de datos y es capaz de establecer el túnel y de configurarlo. En un caso, la configuración del túnel incluye la inhabilitación selectiva del mecanismo de control de la congestión y del mecanismo de pérdida de paquetes construidos dentro de la conexión de nivel inferior. En otro caso, la configuración de las conexiones puede incluir la habilitación selectivamente del mecanismo de control de la congestión y del mecanismo de pérdida de paquetes construidos dentro de la conexión de nivel superior.

La máquina virtual dentro del centro de datos genera los primeros paquetes IP que se transportan al punto final de origen sobre la conexión de nivel superior. Tras la recepción, el punto final de origen (o el punto final de terminación del túnel de origen) encapsula los primeros paquetes IP en segundos paquetes IP y transmite los segundos paquetes IP sobre la conexión de nivel inferior. Como tal, ambas conexiones están acopladas cuando transmiten paquetes de datos entre los puntos finales de un túnel basado en TCP.

En otro aspecto más, realizaciones de la presente invención se refieren a un procedimiento informatizado para facilitar la comunicación entre un punto final de origen y un punto final de destino a través de un túnel basado en TCP. En una realización ejemplar, el procedimiento incluye el empleo de un controlador matricial para establecer el

túnel basado en TCP que enlaza comunicativamente el punto final de origen y el punto final de destino a través de una red o a través de redes dispares. Como se ha mencionado anteriormente, la operación del punto final de origen está soportada por un centro de datos y la operación del punto final de destino está soportada por un recurso, localizado remotamente, que reside en una red de empresa privada gestionada por un cliente del centro de datos. El procedimiento incluye adicionalmente una etapa de recepción de primeros paquetes IP en el punto final de origen, que se pasan desde una máquina virtual instanciada dentro de un centro de datos. Estos primeros paquetes IP son transportados a través de una conexión de nivel superior con un primer conjunto de mecanismos de fiabilidad provistos en ella. Los primeros paquetes IP se encapsulan dentro de segundos paquetes IP en el punto final de origen (o en un punto final de terminación del túnel de origen en la misma red que el punto final de origen) y se transmiten sobre un túnel basado en TCP a través de una conexión de nivel inferior a un punto final de terminación del túnel en la red de destino, a continuación se envían al punto de destino final en la red remota. Típicamente, la conexión de nivel superior está provista con un segundo conjunto de mecanismos de fiabilidad. Este primer y segundo conjuntos de mecanismos de fiabilidad, en realizaciones, incluyen cada uno un mecanismo de control de la congestión y un mecanismo de recuperación de pérdidas, respectivamente.

El procedimiento continúa mediante la realización de una etapa de empleo del controlador matricial para inhabilitar selectivamente el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos en la conexión de nivel inferior. El controlador matricial se emplea también para permitir pasivamente que el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos en la conexión de nivel superior permanezcan habilitados. La condición inhabilitada de la conexión de nivel inferior y la condición habilitada de la conexión de nivel superior se almacenan, al menos temporalmente. A modo de clarificación, la condición inhabilitada representa la inhabilitación del mecanismo de control de la congestión y/o del mecanismo de recuperación de pérdidas provistos en la conexión de nivel inferior. Por el contrario, la condición habilitada representa la habilitación del mecanismo de control de la congestión y del mecanismo de recuperación de pérdidas provistos sobre la conexión de nivel superior.

Habiendo descrito brevemente una visión global de las realizaciones de la presente invención, se describe a continuación un entorno de operación ejemplar adecuado para la implementación de realizaciones de la presente invención.

En referencia a los dibujos en general, e inicialmente a la FIG. 1 en particular, se muestra un entorno operativo ejemplar para la implementación de realizaciones de la presente invención y se designa en general como dispositivo 100 informático. El dispositivo 100 informático no es más que un ejemplo de un entorno informático adecuado y no se pretende que sugiera ninguna limitación sobre el alcance de uso o funcionalidad de las realizaciones de la presente invención. Ni deberían interpretarse el entorno 100 informático como que tiene cualquier dependencia o requisito en relación a uno cualquiera o combinación de los componentes ilustrados.

Las realizaciones de la presente invención pueden describirse en el contexto general de un código informático o instrucciones utilizables por máquina, que incluyen instrucciones ejecutables por ordenador tales como componentes de programa, que se ejecutan por un ordenador u otra máquina, tal como un asistente de datos personal u otro dispositivo portátil. Generalmente, los componentes del programa incluyen rutinas, programas, objetos, componentes, estructuras de datos y similares que se refieren a códigos que realizan tareas particulares, o implementan tipos de datos abstractos particulares. Las realizaciones de la presente invención pueden ponerse en práctica en una variedad de configuraciones de sistemas, incluyendo dispositivos portátiles, electrónica de consumo, ordenadores de finalidad general, especialmente dispositivos informáticos, etc. Las realizaciones de la invención pueden ponerse en práctica también en entornos informáticos distribuido en donde las tareas se realizan mediante dispositivos de procesamiento remoto que están enlazados a través de una red de comunicaciones.

Continuando con la referencia a la FIG. 1, el dispositivo 100 informático incluye un bus 110 que conecta directa o indirectamente los siguientes dispositivos: memoria 112, uno o más procesadores 114, uno o más componentes 116 de presentación, puertos 118 de entrada/salida (E/S), componentes 120 de E/S, y una fuente de alimentación 122 ilustrativa. El bus 110 representa lo que puede ser uno o más buses (tal como un bus de direcciones, bus de datos, o combinaciones de los mismos). Aunque los diversos bloques de la FIG. 1 se muestran con líneas por razones de claridad, en realidad, la delimitación de los diversos componentes no está clara y, metafóricamente, las líneas serían más precisas siendo grises y borrosas. Por ejemplo, se puede considerar que un componente de presentación tal como un dispositivo de pantalla es un componente de E/S. También, los procesadores tienen memoria. Los presentes inventores reconocen que tal es la naturaleza de la técnica y reiteran que el diagrama de la FIG. 1 es meramente ilustrativo de un dispositivo informático ejemplar que puede usarse en conexión con una o más realizaciones de la presente invención. No se hace distinción entre categorías tales como "estación de trabajo", "servidor", "ordenador portátil", "dispositivo portátil" etc., dado que todos están contemplados dentro del alcance de la FIG. 1 y referidos como un "ordenador" o "dispositivo informático".

El dispositivo 100 informático incluye típicamente una variedad de medios legibles por ordenador. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender una memoria de acceso aleatorio (RAM); memoria solo de lectura (ROM); memoria solo de lectura programable y borrable electrónicamente (EEPROM); memoria flash u otras tecnologías de memoria; CD ROM, discos versátiles digitales (DVD) u otros medios ópticos u holográficos; casetes magnéticas, cintas magnéticas, almacenamiento en discos magnéticos u

otros dispositivos de almacenamiento magnético o cualquier otro medio que pueda usarse para codificar la información deseada y al que se pueda acceder por parte del dispositivo 100 informático.

La memoria 112 incluye medios de almacenamiento de ordenador en la forma de memoria volátil y/o no volátil. La memoria puede ser extraíble, no extraíble o una combinación de las mismas. Los dispositivos de hardware ejemplares incluyen memorias de estado sólido, discos duros, unidades de disco óptico, etc. El dispositivo 100 informático incluye uno o más procesadores que leen datos desde varias entidades tales como la memoria 112 o componentes 120 de E/S. El (los) componente(s) 116 de presentación presentan indicaciones de datos a un usuario u otro dispositivo. Los componentes de presentación ejemplares incluyen un dispositivo de pantalla, altavoz, componente de impresión, componente de vibración, etc. Los puertos 118 de E/S permiten al dispositivo 100 informático estar lógicamente conectado a otros dispositivos incluyendo los componentes 120 de E/S, algunos de los cuales pueden estar integrados. Los componentes ilustrativos incluyen un micrófono, palanca de juegos, alfombrilla táctil, antena de satélite, escáner, impresora, dispositivo inalámbrico, etc.

Con referencia a las FIGS. 1 y 2, un primer dispositivo 255 informático y/o un segundo dispositivo 265 informático pueden implementarse mediante el dispositivo 100 informático ejemplar de la FIG. 1. Adicionalmente, el punto final 201 y/o el punto final 202 pueden incluir partes de la memoria 112 de la FIG. 1 y/o partes de los procesadores 114 de la FIG. 1.

Pasando ahora a la FIG. 2, se ilustra un diagrama de bloques, de acuerdo con una realización de la presente invención, que muestra una plataforma 200 informática en la nube ejemplar que se configura para asignar máquinas virtuales 270 y 275 dentro de un centro 225 de datos para su uso por un aplicación de servicio. Se entenderá y apreciará que la plataforma 200 informática en la nube mostrada en la FIG. 2 es meramente un ejemplo de un entorno de sistema informático adecuado y no se pretende que sugiera ninguna limitación tal como el alcance de uso o funcionalidad de las realizaciones de la presente invención. Por ejemplo, la plataforma 200 informática en la nube puede ser una nube pública, una nube privada, o una nube dedicada. Tampoco debería interpretarse la plataforma 200 informática en la nube como que tienen ninguna dependencia o requisito relacionado con cualquier componente único o combinación de componentes ilustrados en el presente documento. Adicionalmente, aunque los diversos bloques de la FIG. 2 se muestran con líneas por razones de claridad, en realidad, la delimitación de los diversos componentes no está clara, y metafóricamente, las líneas serían más precisas grises y difuminadas. Además, cualquier número de máquinas físicas, máquinas virtuales, centros de datos, puntos finales, o combinaciones de los mismos puede emplearse para conseguir la funcionalidad deseada dentro del alcance de las realizaciones de la presente invención.

La plataforma 200 informática en la nube incluye el centro 225 de datos configurado para alojar y soportar la operación de los puntos finales 201 y 202 de una aplicación de servicio particular. La expresión "aplicación de servicio", tal como se usa en el presente documento se refiere ampliamente a cualquier software, o porciones de software, que se ejecute por encima de, o acceda a localizaciones de almacenamiento dentro de, el centro 225 de datos. En una realización, uno o más de los puntos finales 201 y 202 puede representar las partes de software, programas componentes, o instancias de papeles que participen en la aplicación de servicio. En otra realización, uno o más de los puntos finales 201 y 202 pueden representar datos almacenados que son accesibles a la aplicación de servicio. Se entenderá y apreciará que los puntos finales 201 y 202 mostrados en la FIG. 2 son meramente un ejemplo de partes adecuadas para soportar la aplicación de servicio y no se pretende que sugieran ninguna limitación tal como el alcance de uso o funcionalidad de las realizaciones de la presente invención.

Generalmente, las máquinas 270 y 275 virtuales se asignan a los puntos finales 201 y 202 de la aplicación de servicio basándose en demandas (por ejemplo, cantidad de carga de procesamiento) situada sobre la aplicación de servicio. Tal como se usa en el presente documento, la expresión "máquina virtual" no se quiere indicar que sea limitativa, y puede referirse a cualquier software, aplicación, sistema operativo o programa que se ejecute por una unidad de procesamiento para sustentar la funcionalidad de los puntos finales 201 y 202. Adicionalmente, las máquinas 270 y 275 virtuales pueden incluir capacidad de procesamiento, localizaciones de almacenamiento, y otros activos dentro del centro 225 de datos para dar soporte apropiadamente a los puntos finales 201 y 202.

En el funcionamiento, las máquinas 270 y 275 virtuales se asignan dinámicamente dentro de los recursos (por ejemplo, primer dispositivo 255 informático y segundo dispositivo 265 informático) del centro 225 de datos, y los puntos finales (por ejemplo, los puntos finales 201 y 202) se sitúan dinámicamente sobre las máquinas 270 y 275 virtuales asignadas para satisfacer la carga de procesamiento actual. En una instancia, un controlador 210 matricial es responsable de la asignación automáticamente de las máquinas 270 y 275 virtuales y de la colocación de los puntos finales 201 y 202 dentro del centro 225 de datos. A modo de ejemplo, el controlador 210 matricial puede basarse en un modelo de servicio (por ejemplo diseñado por un cliente que posee la aplicación de servicio) para proporcionar guía sobre cómo y cuándo asignar las máquinas 270 y 275 virtuales y para colocar los puntos finales 201 y 202 en ellas. Adicionalmente, el controlador 210 matricial puede leer instrucciones desde el modelo de servicio informático en la nube cuando determina si habilitar (activar) o inhabilitar (desactivar) los mecanismos de fiabilidad integrados con una conexión de red de tipo túnel entre los puntos finales 201 y 202 y puntos finales localizados remotamente. Esto se explica más completamente a continuación con referencia a la FIG. 3.

Como se ha explicado anteriormente, las máquinas 270 y 275 virtuales pueden asignarse dinámicamente dentro del

primer dispositivo 255 informático y el segundo dispositivo 265 informático. Para realizaciones de la presente invención, los dispositivos 255 y 265 informáticos representan cualquier forma de dispositivos informáticos, tales como, por ejemplo, un servidor, un ordenador personal, un ordenador de sobremesa, un ordenador portátil, un dispositivo móvil, un dispositivo electrónico de consumo, servidores, el dispositivo 100 informático de la FIG. 1, y similares. En un caso, los dispositivos 255 y 265 informáticos alojan y soportan las operaciones de las máquinas 270 y 275 virtuales, estas alojan simultáneamente otras máquinas virtuales forjadas para el soporte de otros inquilinos del centro 225 de datos, en donde los inquilinos incluyen puntos finales de otras aplicaciones de servicio propiedad de diferentes clientes.

En un aspecto, los puntos finales 201 y 202 operan dentro del contexto de la plataforma 200 informática en la nube y, en consecuencia, comunican internamente a través de conexiones realizadas dinámicamente entre las máquinas 270 y 275 virtuales, y externamente a través de una topología de red física con los recursos de una red remota (por ejemplo, el recurso 375 de la red 325 privada de empresa de la FIG. 3). Las conexiones internas pueden implicar la interconexión de las máquinas 270 y 275 virtuales, distribuidas a través de los recursos físicos del centro 225 de datos, a través de una nube de la red (no mostrada). La nube de la red interconecta estos recursos de modo que el punto final 201 puede reconocer una localización del punto final 202, y de otros puntos finales, para establecer una comunicación entre ellos. Además, la nube de la red puede establecer esta comunicación a través de un túnel entre el punto final del primer dispositivo 255 informático y el segundo dispositivo 265 informático enlazando lógicamente los puntos finales 201 y 202. A modo de ejemplo, los canales se basan en, sin limitación, una o más redes de área local (LAN) y/o redes de área grande (WAN). Dichos entornos de conexión en red son comunes en oficinas, redes de ordenador del ámbito de empresa, intranets, y la Internet. En consecuencia, la red no se describirá adicionalmente en el presente documento.

Pasando ahora a la FIG. 3, se muestra un diagrama de bloques que ilustra un entorno 300 informático distribuido ejemplar, con un túnel 330 basado en TCP establecido en él, de acuerdo con una realización de la presente invención. Inicialmente, el entorno 300 informático distribuido incluye una red 325 privada de empresa y la plataforma 200 informática en la nube, tal como se ha explicado con referencia a la FIG. 2. La red 325 privada de empresa y la plataforma 200 informática en la nube pueden conectarse a través de una red 315 que está soportada por una red física. Tal como se usa en el presente documento, la expresión "red física" no se quiere indicar que sea limitativa, sino que puede englobar mecanismos de equipos tangibles (por ejemplo líneas de fibra, cajas de circuitos, interruptores, antenas, enrutadores IP y similares), así como comunicaciones y ondas portadoras intangibles, que facilitan la comunicación entre puntos finales y localizaciones geográficamente remotas. A modo de ejemplo, la red física (no mostrada en la Figura 3) puede incluir cualquier tecnología cableada o inalámbrica utilizada dentro de la Internet, o disponible para promover la comunicación entre redes dispares.

Generalmente, la red 325 privada de empresa incluye recursos, tal como el recurso 375 que son gestionados por un cliente de la plataforma 200 informática en la nube. Frecuentemente, estos recursos alojan y soportan operaciones de componentes de la aplicación de servicio propiedad del cliente. El punto final B 385 representa uno o más de los componentes de la aplicación de servicio. En ciertas realizaciones, los recursos, tales como la máquina 270 virtual de la FIG. 2, están asignados dentro del centro 225 de datos de la FIG. 2 para alojar y soportar operaciones de componentes de la aplicación de servicio distribuidos remotamente. El punto final A 395 representa uno o más de estos componentes remotamente distribuidos de la aplicación de servicio dentro de la plataforma 200 informática en la nube. Durante la operación, los puntos finales A 395 y B 385 trabajan en sintonía entre sí para asegurar que la aplicación de servicio se ejecuta apropiadamente. En un caso, el trabajo en sintonía implica la transmisión entre los puntos finales A 395 y B 385 de paquete(s) 316 de datos, o paquetes de datos IP, a través de una red 315 soportada por la red física.

En ciertas realizaciones, el (los) paquete(s) 316 pueden actuar para intercambiar piezas de información entre los puntos finales A 395 y B 385. Generalmente el (los) paquete(s) 316 están compuestos de una secuencia de bytes, y adicionalmente incluyen una cabecera seguida por un cuerpo. La cabecera describe el destino del paquete 316 y, opcionalmente, los enrutadores en la red física a usar para el envío hasta que el paquete 316 llegue a su destino final, tal como el recurso 375. El cuerpo contiene los datos, o carga útil, generados en el originador del paquete 316, tal como la máquina 270 virtual.

Típicamente, el recurso 375 y el centro 225 de datos incluyen, o están enlazados a, alguna forma de una unidad informática (por ejemplo, la unidad de procesamiento central, microprocesador, etc.) para dar soporte a operaciones de los puntos finales y/o componentes que se ejecutan en él. Tal como se usa en el presente documento, la expresión "unidad informática" se refiere en general a un dispositivo de cálculo dedicado con potencia de procesamiento y memoria de almacenamiento, que soporta uno o más sistemas operativos u otro software subyacente. En un caso, la unidad informática se configura con elementos de hardware tangibles, o máquinas, que son parte integral, o conectados operativamente, al recurso 375 y al centro 225 de datos para habilitar que cada dispositivo realice una variedad de procedimientos y operaciones. En otro caso, la unidad de cálculo pueden englobar un procesador (no mostrado) conectado al medio legible por ordenador incluido en cada uno de los recurso 375, y centro 225 de datos. Generalmente, el medio legible por ordenador almacena, al menos temporalmente, una pluralidad de componentes de software informático (por ejemplo, los puntos finales A 395 y B 385) que son ejecutables por el procesador. Tal como se utiliza en el presente documento, el término "procesador "no se quiere indicar que sea limitativo y puede englobar cualquier elemento de la unidad informático que actúe con una capacidad

de cálculo. En dicha capacidad, el procesador puede configurarse como un artículo tangible que procesa instrucciones. En una realización ejemplar, el procesamiento puede implicar la recolección, decodificación/interpretación, ejecución, y escritura de instrucciones.

El túnel 330 basado en TCP ("túnel 330") puede establecerse para comunicar entre puntos finales asignados a una única aplicación de servicio, tal como la aplicación de servicio que incluye los puntos finales A 395 y B 385, o múltiples pares que sirven a aplicaciones de servicio independientes para puentear la comunicación entre los puntos finales asignados a través de redes dispares. El túnel 330 usa TCP, que proporciona un servicio de comunicación en una capa de transporte entre la capa de aplicación y la capa de red/IP y puede incluir la capa de aplicación en 430 y 440, cuando emplea HTTP o HTTPS. Esto se muestra en las pilas 430 y 440 TCP/IP de la FIG. 4, en la que el túnel 330 sirve como un enlace lógico entre un canal 425 de nivel inferior de la capa de transporte en la máquina 270 virtual.

Durante la operación, cuando el programa de aplicación desea enviar un gran cantidad de datos a través de la red (por ejemplo Internet) usando IP, en lugar de romper los datos en piezas de tamaño IP y enviar una serie de solicitudes IP, el programa de aplicación puede enviar una única solicitud a través de la capa de transporte, que emplea TCP, para manejar los detalles IP. De ese modo, la capa de transporte puede pensarse como un mecanismo de transporte que asegura una entrega completa, por ejemplo, un vehículo con la responsabilidad de asegurar que su contenido o carga útil alcanza su destino con seguridad y sólidamente. En ciertos casos, asegurar la entrega implica mecanismos de fiabilidad construidos dentro del túnel 330 que acometen numerosos problemas de fiabilidad y proporcionan una transmisión fiable de los paquetes 316 de datos. Estos mecanismos de fiabilidad operan a un alto nivel, y están afectados por los dos sistemas extremos (por ejemplo, un navegador web y un servidor web).

En particular, TCP proporciona una entrega fiable, ordenada de un flujo de paquetes 316 desde el punto final 395 en un ordenador al punto final 385 en otro ordenador mediante la imposición de una serie de reglas. El conjunto de reglas puede dictar que los paquetes 316 de datos llegan en orden, que los paquetes 316 de datos no tienen errores (es decir corrección), que los paquetes 316 de datos duplicados se descartan y que los paquetes 316 perdidos/retrasados se reenvían. Este conjunto de reglas de ejemplo precedente puede imponerse mediante un mecanismo 505 de recuperación de pérdida de la FIG. 5, que inspecciona el flujo de datos para identificar cualquier paquete 316 perdido. Los mecanismos de fiabilidad pueden incluir también un mecanismo 515 de control de la congestión de la FIG. 5 configurado para gestionar una cantidad de datos que se transmiten dentro de los paquetes IP, y para gestionar en general la congestión de tráfico a través del túnel 330.

Generalmente, el túnel 330 representa un enlace lógico que conecta puntos finales a través de la capa de transporte a lo largo de parte de la trayectoria entre los dos puntos finales o en la trayectoria en conjunto. En ciertas realizaciones, el túnel 330 utiliza IP-HTTPS, SSL, SSTP u otra tecnología de tunelación basada en TCP que se diseña para crear un enlace de puente que atraviesa los límites de la red IP a través de la red 315. De ese modo, el túnel 330 habilita ostensiblemente el establecimiento de un enlace lógico entre puntos finales 385 y 395 que es dependiente de la red física subyacente, permitiendo de ese modo que interactúe como si estuviera posicionado de forma adyacente dentro del centro 225 de datos.

En una realización ejemplar, el túnel 330 puede incluir una o más conexiones basadas en TCP dispuestas en capas, una encima de la otra. Pasando a la FIG. 4, se muestra una representación esquemática de la disposición en capas de las conexiones basadas en TCP que comprenden el túnel 330, de acuerdo con una realización de la presente invención. Tal como se ilustra en la FIG. 4, hay dos conexiones basadas en TCP ejecutándose una encima de la otra en las que están ambas imponiendo el conjunto de reglas (explicadas anteriormente) sobre cada flujo respectivo de paquetes 316 de datos para asegurar una entrega completa y eficiente. Estas dos conexiones basadas en TCP incluyen un canal 415 de nivel superior y un canal 425 de nivel inferior. El canal 415 de nivel superior transmite datos sin encapsular desde la máquina 270 virtual al punto final A 395 dentro del centro 225 de datos. Los datos sin encapsular pueden encapsularse en el punto final A 395 y colocarse en el canal 425 de nivel inferior que transporta los datos encapsulados en paquetes 316 de datos al punto final B 385. Tras la llegada al punto final B 385, los paquetes de datos 316 son recibidos en el canal 425 de nivel inferior, desencapsulados y enviados al recurso 375 a través del canal 415 de nivel superior.

Aunque se han descrito dos canales diferentes que influyen el túnel 330, debería entenderse y apreciarse que pueden usarse otros tipos de conexiones adecuadas que proporcionen la transmisión de paquetes de datos IP, y que las realizaciones de la presente invención no están limitadas a estos canales 415 y 425 descritos en el presente documento.

El mecanismo 505 de recuperación de pérdidas y el mecanismo 515 de control de la congestión (véase la FIG. 5) pueden construirse ambos dentro, y ejecutarse integralmente sobre, cada uno de entre el canal 415 de nivel superior y el canal 425 de nivel inferior. La operación activa simultánea de estos mecanismos 515 y 525 da como resultado frecuentemente una degradación del rendimiento por los esfuerzos duplicados y redundantes. Por ejemplo, si se pierde el paquete de 316 de datos, ambos mecanismos 515 y 525 dentro de ambos canales 415 y 425 realizarán la recuperación de pérdida y control de la congestión, respectivamente. En consecuencia, el controlador 210 matricial las FIGS. 2 y 5 puede emplearse para fijar selectivamente (activar o desactivar) cualquiera de los mecanismos 515 y 525 en cualquiera de los dos canales 415 y 425, independientemente.

En referencia ahora a la FIG. 5, se muestra un diagrama de bloques que ilustra un centro 225 de datos ejemplar que emplea un controlador 210 matricial para habilitar/inhabilitar selectivamente los mecanismos de fiabilidad 505 y 515 construidos dentro de los túneles 330 basados en TCP, de acuerdo con realizaciones de la presente invención. Tal como se ha representado, los datos se transmiten desde la máquina 270 virtual sobre el canal 415 de nivel superior hasta el punto final A 395. El punto final A 395 encapsula los datos transmitidos y los envía a través de la red 315 por medio del canal 415 de nivel inferior. El controlador 210 matricial puede transmitir instrucciones 510 al punto final A 395 que inhabilitan selectivamente el mecanismo 505 de recuperación de pérdida y/o el mecanismo 515 de control de la congestión construidos dentro del canal 425 del nivel inferior. Estas instrucciones 510 pueden generarse mediante criterios, y se entregan típicamente por cada conexión de los canales 415 y 425 basados en TCP usados para el túnel 330. Por conexión, o por opción de conector, las instrucciones 510 para activar o desactivar el mecanismo 505 de control de la congestión y/o del mecanismo 515 de recuperación de pérdida, independientemente, pueden invocarse mediante criterios, tales como las políticas que deben proporcionarse por el cliente (por ejemplo, modelo de servicio informático en la nube, acuerdo a nivel de servicio negociado, y similares). En otra realización, la inhabilitación selectiva de los mecanismos 505 y 515 puede invocarse por criterios que pertenecen a una identidad del punto final de origen (punto final A 395), y la identidad del punto final de destino (punto final B 385), un tipo de datos que está siendo transmitido, un tipo de túnel que está siendo establecido, un tipo de aplicación/operación que está siendo ejecutada, o información basada en la política.

En una realización ejemplar, el controlador 210 matricial envía las instrucciones 510 para inhabilitar los mecanismos 505 y 515 en ejecución sobre el canal 425 de nivel inferior, mientras deja habilitados los mecanismos (no mostrados) en ejecución en el canal 415 de nivel superior, proporcionando de ese modo una fiabilidad de extremo a extremo del flujo de datos y reduciendo la redundancia de mecanismos dobles que provoca latencia. En un caso, esta configuración de inhabilitar los mecanismos 505 y 515 del canal 425 del nivel inferior se provee dentro del controlador 210 matricial como el ajuste por defecto. En esta realización, el controlador 210 matricial inhabilita automáticamente los mecanismos 505 y 515 a menos que haya una entrada para lo contrario.

En ciertas realizaciones, cuando se inhabilita el mecanismo 515 de control de la congestión, el controlador 210 matricial puede actuar sobre (un) componente(s) en el extremo de transmisión (por ejemplo el punto final de origen, punto final A 395 de las FIGS. 3-5, o máquina 270 virtual de las FIGS. 2-5) del túnel 330 sin realizar cambios sobre el extremo receptor (por ejemplo, el punto final de destino, punto final B 385 de las FIGS. 3-5, o recurso 375 de las FIGS. 3 y 4) del túnel 330. De ese modo, el mecanismo 515 de control de la congestión puede desactivarse sin ninguna negociación con el extremo receptor y, por ello, es compatible hacia atrás. Durante el funcionamiento, con referencia a la FIG. 5, tras actuar sobre el punto final A 395, este punto final de origen envía una cantidad de datos, o tasa de paquetes 316 de datos, diseñados por un mecanismo de control de la congestión (no mostrado) del canal 415 de nivel superior. De ese modo, solo el mecanismo de control de la congestión del canal 415 de nivel superior controla la cantidad de datos de modo que la red 315 no esté sobrecargada con demasiados datos provocando alta pérdida de datos.

En ciertas realizaciones, cuando se inhabilita el mecanismo 505 de recuperación de pérdidas, el controlador 210 matricial puede actuar sobre (un) componente(s) en el extremo de transmisión (por ejemplo el punto final de origen, punto final A 395 de las FIGS. 3-5, o máquina 270 virtual de las FIGS. 2-5) del túnel 330 y sobre el extremo receptor (por ejemplo, el punto final de destino, punto final B 385 de las FIGS. 3-5, o recurso 375 de las FIGS. 3 y 4) del túnel 330. De ese modo, el mecanismo 515 de recuperación de pérdidas puede desactivarse a través de la cooperación por medio de negociación entre el extremo de transmisión y el extremo de recepción del túnel 330. Esto es, el extremo de recepción es consciente a través de la negociación que las pérdidas de los paquetes 316 de datos no serán recuperadas por el extremo de transmisión. En consecuencia, durante la operación, el extremo de recepción pasará los paquetes 316 de datos entregados incluso aunque pueden perderse datos intermedios hasta el recurso 375, u otro punto final de destino de la aplicación de servicio que esté aguas abajo del punto final B 385. Sin embargo, si el extremo de recepción del túnel 330 no soporta la desactivación del mecanismo 515 de recuperación de pérdidas, entonces el mecanismo 515 de recuperación de pérdidas permanecerá típicamente activo y habilitado.

En un caso de negociación, el punto final A 395 puede enviar un paquete de sincronización (SYN) inicial (que transporta información de negociación) al punto final de 385, que puede acusar recibo del paquete SYN. Adicionalmente, el punto final de 385 puede devolver un saludo inicial con el punto final A 395 mediante el envío de un paquete de acuse de recibo (SYN-ACK) al mismo. En este punto, cuando tiene lugar la devolución, el mecanismo 515 de recuperación de pérdidas del canal 425 del nivel inferior se inhabilita, mientras que el mecanismo de recuperación de pérdidas (no mostrado) del canal 415 de nivel superior permanece activo y habilitado, ayudando de ese modo a recuperarse de cualesquiera pérdidas o retardos durante la entrega de los paquetes 316 de datos mediante la retransmisión de cualquier dato partido o retrasado en la red 315.

En referencia ahora a la FIG. 6, se muestra un diagrama de flujo que ilustra un procedimiento 600 para facilitar la comunicación a través de una conexión de red establecida entre una pluralidad de puntos finales que residen en redes dispares, de acuerdo con una realización de la presente invención. Como se indica en el bloque 602, se proporciona la conexión de red. En un caso, la conexión de red se extiende entre un punto final de origen (por ejemplo, el punto final a 395 de la FIG. 4) y un punto final de destino (por ejemplo, punto final B 385 de la FIG. 4). Como se ha descrito anteriormente, la conexión de red funciona como un túnel basado en TCP que puentea las redes dispares (por ejemplo, la plataforma 200 informática en la nube y una red 325 privada de empresa de la FIG.

3) en las que residen el punto final de origen y el punto final de destino, respectivamente. El procedimiento 600, en los bloques 604 y 606, implica adicionalmente las etapas de inhabilitar selectivamente uno o más de los mecanismos de fiabilidad del nivel inferior, que se ejecutan integralmente en el túnel basado en TCP, y comunicar mensajes entre el primer punto final y el segundo pinto final sin que interfieran los mecanismos de fiabilidad del nivel inferior con unos tiempos en los que se envían los mensajes. En ciertas realizaciones, los mensajes de comunicación entre el primer punto final y el segundo punto final pueden incluir específicamente la transmisión de paquetes IP desde el primer punto final al segundo punto final a través del túnel basado en TCP.

En una realización ejemplar, el acto de inhabilitar selectivamente puede iniciarse tras evento(s) que sucede(n) correspondiente(s) con criterios predefinidos. Los criterios predefinidos pueden ser conocidos para el controlador matricial, que puede inhabilitar selectivamente uno o más de los mecanismos de fiabilidad (por ejemplo, el mecanismo 505 de control de pérdidas y el mecanismo 515 de control de la congestión de la FIG. 5) tras la detección de los siguientes eventos correspondientes: un puerto predefinido está intentando enviar paquetes de datos a través de un túnel; se está estableciendo una nueva conexión de red en un centro de datos, máquina virtual, o punto final de origen predefinidos; o se está estableciendo una nueva conexión de red en un recurso o punto final de destino predefinidos.

En otra realización, el usuario o cliente del centro de datos puede tener concedidos derechos para ejercer un control manual para activar/desactivar un grupo de mecanismos de fiabilidad instanciados en la plataforma informática en la nube. En esta forma, el usuario o cliente puede decidir si inhabilitar o habilitar uno o más mecanismos de fiabilidad dinámicamente mediante la especificación de un punto final de un túnel en una interfaz de usuario. En consecuencia, el usuario o cliente es capaz de determinar si evitar penalidades de rendimiento asociadas con la ejecución de capas duplicadas de protocolos de fiabilidad, tal como TCP, sobre los túneles que realizarían normalmente un control de la congestión y recuperación de pérdidas en una forma redundante e ineficiente.

Pasando a la FIG. 7, se muestra un diagrama de flujo que ilustra un procedimiento 700 para facilitar la comunicación entre un punto final de origen y un punto final de destino a través de un túnel basado en TCP, de acuerdo con una realización de la presente invención. Como se indica en el bloque 702, el procedimiento 700 incluye el empleo de un controlador matricial para establecer el túnel basado en TCP que enlaza comunicativamente el punto final de origen y el punto final de destino sobre una red o a través de redes dispares. En ciertas realizaciones, la operación del punto final de origen está soportada por un centro de datos (por ejemplo, utilizando el centro 225 de datos de la FIG. 3), mientras que la operación del punto final de destino está soportada por un recurso, localizado remotamente, por ejemplo, utilizando el recurso 375 de la FIG. 3) que reside en una red de empresa privada, en donde el recurso puede gestionarse/poseerse por un cliente del centro de datos. El procedimiento 700 incluye adicionalmente una etapa de recepción de un primer flujo de paquetes IP en el punto final de origen, que se pasan desde una máquina virtual instanciada dentro de un centro de datos. Esta etapa es indicada en el bloque 704. En algunas realizaciones, el primer flujo de paquetes IP es transportada a través de un canal de nivel superior con un primer conjunto de mecanismos de fiabilidad provistos sobre él. Tras la llegada en el punto final de origen del túnel, el primer flujo de paquetes IP se encapsula en un segundo flujo de paquetes IP que se transmite a través del túnel basado en TCP por medio de una conexión de nivel inferior, como se indica en los bloques 706 y 708. En una configuración del túnel basado en TCP, la conexión de nivel inferior se dispone en capas por debajo del canal de nivel superior, operando de ese modo en tándem para transmitir los paquetes IP y para asegurar la fiabilidad de su transmisión. De esta forma, el canal de nivel inferior está frecuentemente provisto con un segundo conjunto de mecanismos de fiabilidad. En una realización ejemplar, el primer y segundo conjuntos de mecanismos de fiabilidad incluyen cada uno al menos un mecanismo de control de la congestión y un mecanismo de recuperación de pérdidas, respectivamente.

El procedimiento 700 continúa mediante la realización de una etapa de empleo del controlador matricial para inhabilitar selectivamente el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos en el canal de nivel inferior, tal como se indica en el bloque 710. El controlador matricial se emplea también para permitir pasivamente que el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos en el canal de nivel superior permanezcan habilitados, tal como se indica en el bloque 712. La condición de inhabilitado del canal de nivel inferior y la condición de habilitado del canal de nivel superior se almacenan, tal como se indica en el bloque 714. A modo de clarificación, la condición inhabilitada representa la inhabilitación del mecanismo de control de la congestión y del mecanismo de recuperación de datos provistos en el canal de nivel inferior. Por el contrario, la condición de habilitado representa la habilitación del mecanismo de control de la congestión y del mecanismo de recuperación de pérdidas provistos en el canal de nivel superior. Las condiciones de los canales pueden almacenarse en el centro de datos, recurso, puntos finales o cualquier otra localización que esté accesible al controlador matricial.

Se han descrito realizaciones de la presente invención en relación a realizaciones particulares, que se pretende en todos los aspectos que sean ilustrativas en lugar de restrictivas. Serán evidentes para los expertos en la materia realizaciones alternativas a las que pertenecen las realizaciones de la presente invención sin apartarse de su alcance.

A partir de lo anterior, se verá que la presente invención está bien adaptada para alcanzar todos los extremos y objetivos expuestos anteriormente, junto con otras ventajas que son obvias e inherentes al sistema y procedimiento.

REIVINDICACIONES

1. Uno o más medios legibles por ordenador que tienen instrucciones ejecutables por ordenador integradas en los mismos que, cuando se ejecutan, realizan un procedimiento de comunicación a través de una conexión de red establecida entre un primer punto final y un segundo punto final que residen en redes dispares, comprendiendo el procedimiento:

proporcionar (602) la conexión de red que se extiende entre el primer punto final y el segundo punto final, en el que la conexión de red opera como un túnel que puentea las redes dispares en las que residen el primer punto final y el segundo punto final, respectivamente, en el que los mensajes de comunicación entre el primer punto final y el segundo punto final comprenden la transmisión de paquetes del protocolo de Internet, IP, desde el primer punto final al segundo punto final a través del túnel, en el que la conexión de red incluye una conexión de nivel superior que se ejecuta por encima de la conexión de nivel inferior, en el que se ejecutan integralmente uno o más mecanismos de fiabilidad del nivel superior en la conexión de nivel superior y el que se ejecutan integralmente uno o más mecanismos de fiabilidad del nivel inferior en la conexión de nivel inferior, en el que el uno o más mecanismos de fiabilidad del nivel inferior comprenden un mecanismo de control de la congestión configurado para gestionar la tasa de transmisión de paquetes IP;
inhabilitar (604) selectivamente el uno o más mecanismos de fiabilidad del nivel inferior, siendo realizada automáticamente la inhabilitación a menos que se proporcione una entrada en sentido contrario, en el que el mecanismo de control de la congestión construido dentro de la conexión de nivel inferior se inhabilita por el primer punto final sin ninguna negociación con el segundo punto final cuando el primer punto final actúa como el extremo de transmisión; y
comunicar (606) mensajes entre el primer punto final y el segundo punto final a través del túnel.

2. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el uno o más mecanismos de fiabilidad del nivel inferior comprenden un mecanismo de pérdida de paquetes configurado para gestionar la pérdida de paquetes a través de la conexión de red mediante la retransmisión automáticamente de los paquetes IP no entregados o retrasados.

3. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el uno o más mecanismos de fiabilidad del nivel superior permanecen habilitados tras la inhabilitación selectiva del uno o más mecanismos de fiabilidad del nivel inferior.

4. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el uno o más mecanismos de fiabilidad del nivel superior comprenden un mecanismo de control de la congestión configurado para gestionar la tasa de transmisión de paquetes IP y un mecanismo de pérdida de paquetes configurado para gestionar la pérdida de paquetes en la conexión de red mediante la retransmisión automáticamente de los paquetes IP no entregados o retrasados.

5. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el uno o más mecanismos de fiabilidad del nivel superior, cuando están habilitados, imponen un conjunto de reglas que gestionan el flujo de datos en la conexión del nivel superior, y en el que el uno o más mecanismos de fiabilidad del nivel inferior, cuando están habilitados, imponen el mismo conjunto de reglas que gestionan el flujo de datos en la conexión de nivel inferior.

6. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el uno o más mecanismos de fiabilidad del nivel inferior se inhabilitan selectivamente en función de un modelo de servicio informático en la nube diseñado, en parte, por un cliente de una plataforma informática en la nube, y en el que la plataforma informática en la nube incluye un centro de datos que aloja el punto final de origen.

7. El uno o más medios legibles por ordenador de la reivindicación 1, en el que el punto final de destino está alojado por un recurso localizado dentro de una red de empresa privada gestionada por un cliente.

8. Un sistema informático para la gestión de un flujo de datos entre puntos finales que residen en redes individuales, comprendiendo el sistema informático:

un centro (225) de datos dentro de una plataforma (200) informática en la nube que aloja un punto final (395) de origen, en el que el punto final de origen está asignado a una aplicación que se ejecuta tanto en la plataforma informática en la nube como en una red (325) de empresa privada;
un recurso (375) dentro de la red de empresa privada que aloja un punto final (385) de destino que está asignado a la aplicación, en el que el punto final de origen y el punto final de destino están conectados por un túnel que transporta el flujo de datos directamente entre ellos, en el que el túnel habilita una conexión de nivel superior que se ejecuta por encima de una conexión de nivel inferior, y en el que se construyen un mecanismo (515) de control de la congestión y un mecanismo (505) de pérdida de paquetes en cada una de las conexiones de nivel superior y la conexión de nivel inferior, respectivamente; y
un controlador (210) matricial que se ejecuta dentro del centro de datos que establece el túnel y que configura las conexiones dentro del túnel, en el que la configuración de las conexiones incluye la inhabilitación selectiva del mecanismo de control de la congestión y del mecanismo de pérdida de datos construidos dentro de la conexión de nivel inferior, siendo realizada automáticamente la inhabilitación a menos que se proporcione una entrada en

sentido contrario, en el que el mecanismo de control de la congestión construido dentro de la conexión de nivel inferior se inhabilita por el controlador matricial actuando sobre componentes del punto final de origen sin ninguna negociación con el punto final de destino.

9. El sistema informático de la reivindicación 8, que comprende además una máquina virtual dentro del centro de datos, genera primeros paquetes en el protocolo de Internet, IP, que son transportados al punto final de origen sobre la conexión de nivel superior, y en el que el punto final de origen encapsula los primeros paquetes IP en segundos paquetes IP y transmite los segundos paquetes IP sobre la conexión de nivel inferior.

10. El sistema informático de la reivindicación 9, en el que el controlador matricial comunica con el punto final de origen cuando inhabilita selectivamente el mecanismo de control de la congestión construido dentro de la conexión de nivel inferior, y el punto final de origen negocia con el punto final de destino, cuando inhabilita selectivamente el mecanismo de pérdida de paquetes construido dentro de la conexión de nivel inferior.

11. El sistema informático de la reivindicación 8, en el que se permite que el mecanismo de control de la congestión y el mecanismo de pérdida de paquetes construidos dentro de la conexión de nivel superior permanezcan habilitados.

12. Un procedimiento informatizado para facilitar la comunicación entre un punto final de origen y un punto final de destino a través de un túnel, comprendiendo el procedimiento:

emplear un controlador matricial para establecer (702) el túnel que enlaza comunicativamente el punto final de origen y el punto final de destino a través de redes dispares, en el que la operación del punto final de origen está soportada por un centro de datos y la operación del punto final de destino está soportada por un recurso, localizado remotamente, que reside en una red de empresa privada gestionada por un cliente del centro de datos;
recibir (704) primeros paquetes en el protocolo de Internet, IP, en el punto final de origen que se pasa desde una máquina virtual instanciada dentro de un centro de datos, en el que los primeros paquetes IP se transportan a través de una conexión de nivel superior con un primer conjunto de mecanismos de fiabilidad provistos en la misma;
encapsular (706) los primeros paquetes IP en segundos paquetes IP en el punto final de origen;
transmitir (708) los segundos paquetes IP sobre el túnel a través de una conexión del nivel inferior que se dispone en capas por debajo de la conexión de nivel superior, en el que la conexión de nivel inferior está provista con un segundo conjunto de mecanismos de fiabilidad, y en el que el primer y segundo conjuntos de mecanismos de fiabilidad incluyen cada uno un mecanismo (515) de control de la congestión y un mecanismo (505) de recuperación de pérdidas, respectivamente; y
emplear el controlador matricial para inhabilitar (710) selectivamente el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos sobre la conexión de nivel inferior, siendo realizada automáticamente la inhabilitación a menos que se proporcione una entrada para lo contrario, en el que el mecanismo de control de la congestión provisto sobre la conexión de nivel inferior se inhabilita por el punto final de origen sin ninguna negociación con el punto final de destino.

13. El procedimiento de la reivindicación 12 que comprende además:

emplear el controlador matricial para permitir que el mecanismo de control de la congestión y el mecanismo de recuperación de pérdidas provistos sobre la conexión de nivel superior permanezcan habilitados; y
almacenar una condición de inhabilitada de la conexión de nivel inferior y una condición de habilitada de la conexión de nivel superior, en el que la condición de inhabilitada representa la inhabilitación del mecanismo de control de la congestión y del mecanismo de recuperación de pérdidas provistos sobre la conexión de nivel inferior, y en el que la condición habilitada representa la habilitación del mecanismo de control de la congestión y del mecanismo de recuperación de pérdidas provistos sobre la conexión de nivel superior.

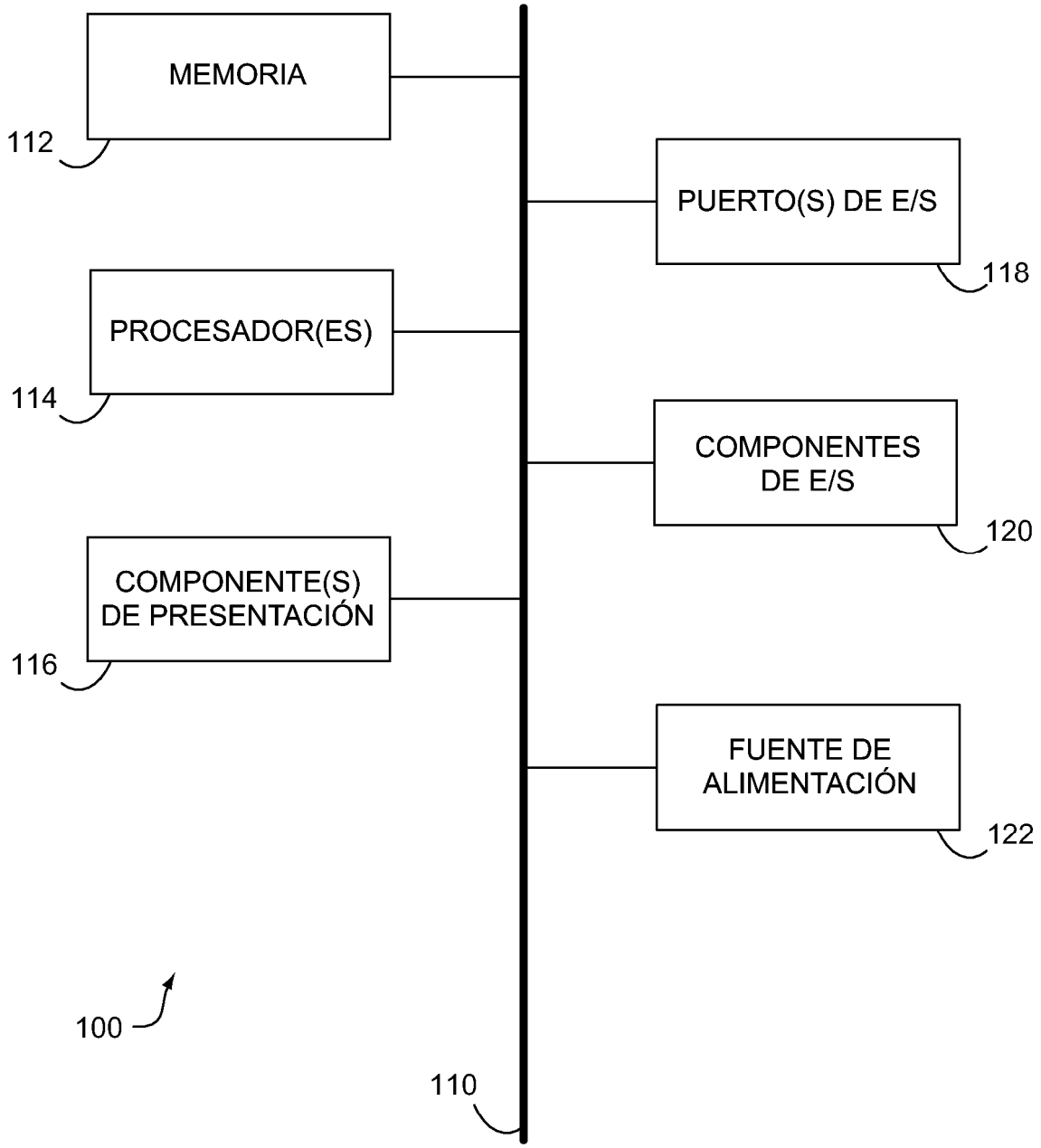
MEMORIA
112
PUERTO(S) DE E/S
118
PROCESADOR(ES)
114
COMPONENTES DE E/S
120
COMPONENTE(S) DE PRESENTACIÓN
116
FUENTE DE ALIMENTACIÓN
122
100
110

FIG. 1.

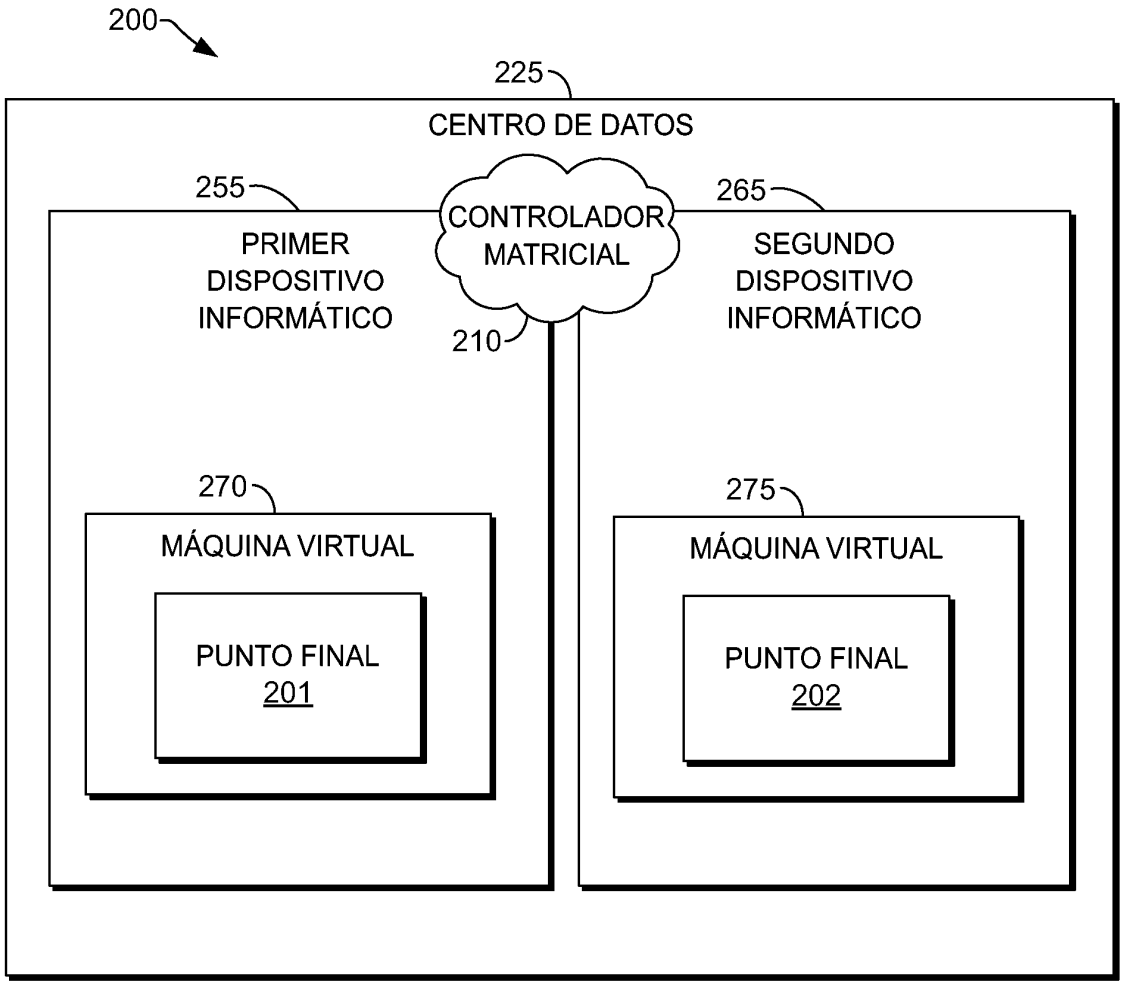
200
225
CENTRO DE DATOS
255
PRIMER DISPOSITIVO INFORMÁTICO
CONTROLADOR MATRICIAL
210
265
SEGUNDO DISPOSITIVO INFORMÁTICO
270
MÁQUINA VIRTUAL
PUNTO FINAL 201
275
MÁQUINA VIRTUAL
PUNTO FINAL 202

FIG. 2.

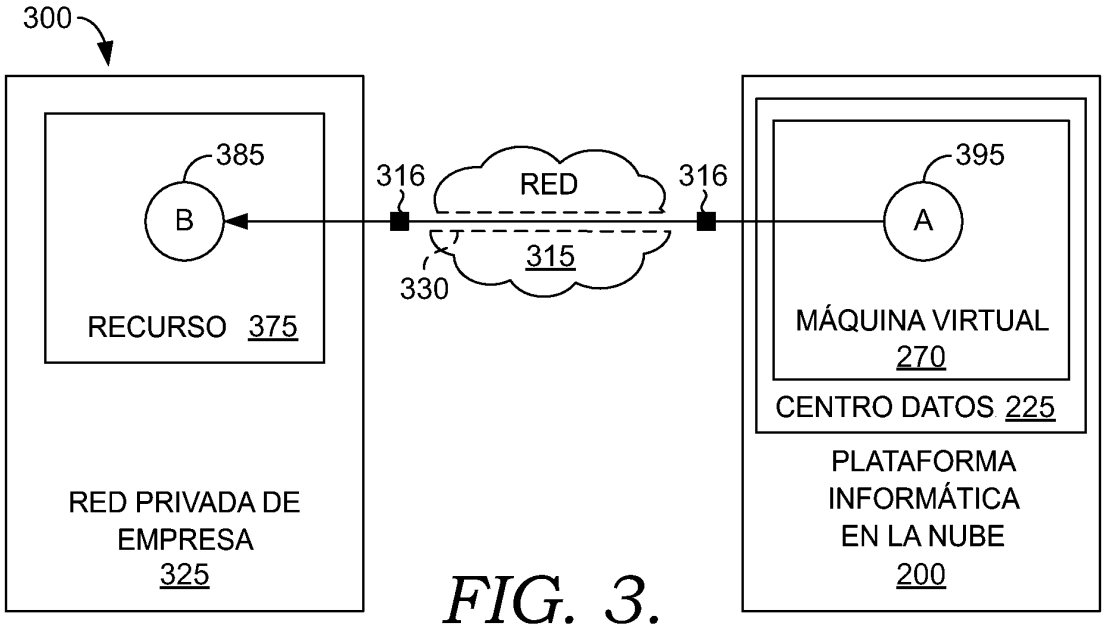
300
385
B
RECURSO 375
RED PRIVADA DE EMPRESA 325
316
RED
316
315
330
395
A
MÁQUINA VIRTUAL 270
CENTRO DATOS 225
PLATAFORMA INFORMÁTICA EN LA NUBE 200

FIG. 3.

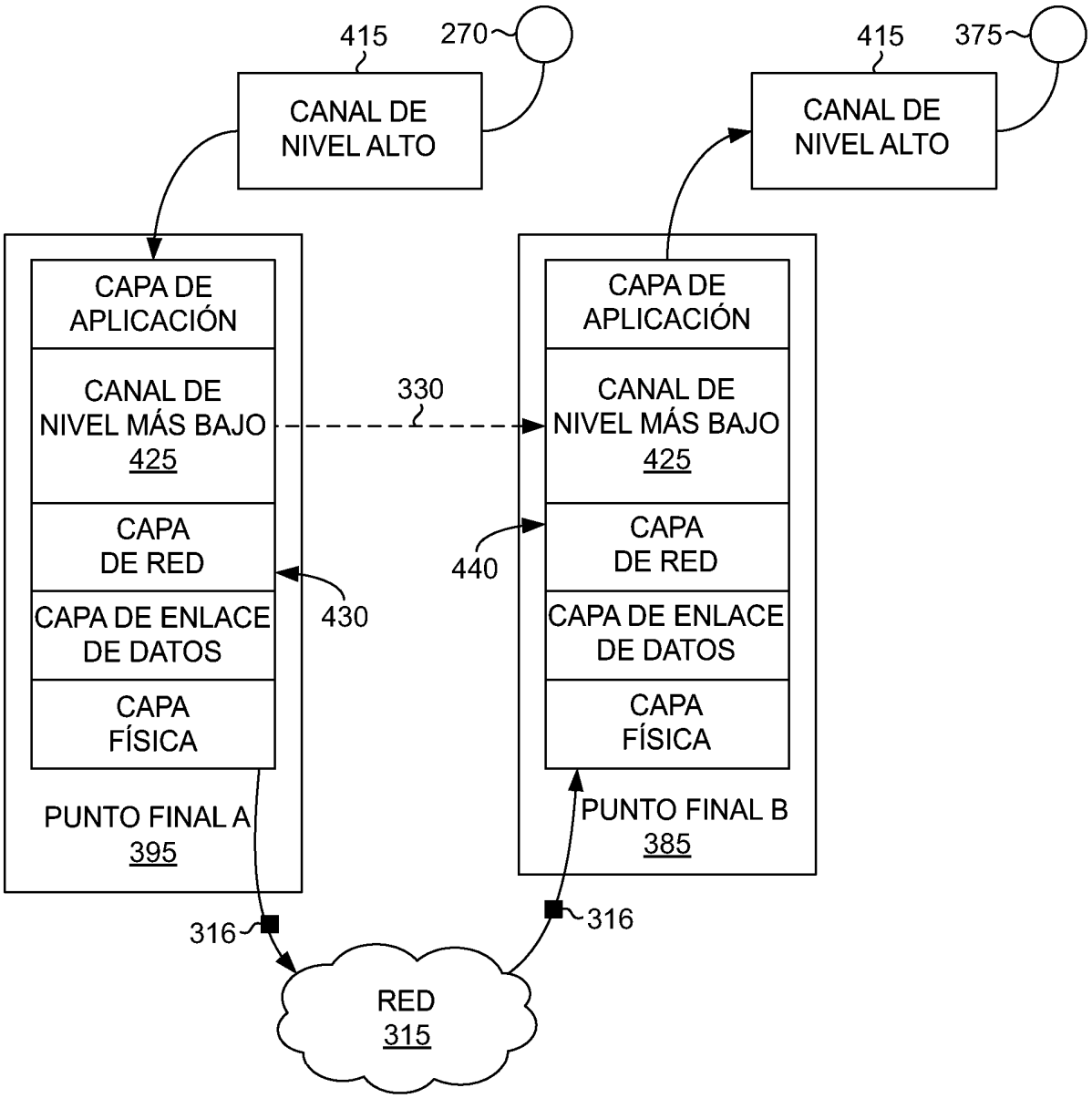
415
270
CANAL DE NIVEL ALTO
415
375
CANAL DE NIVEL ALTO
CAPA DE APLICACIÓN
CANAL DE NIVEL MÁS BAJO 425
330
CAPA DE RED
CAPA DE ENLACE DE DATOS
CAPA FÍSICA
430
440
PUNTO FINAL A 395
PUNTO FINAL B 385
316
316
RED 315

FIG. 4.

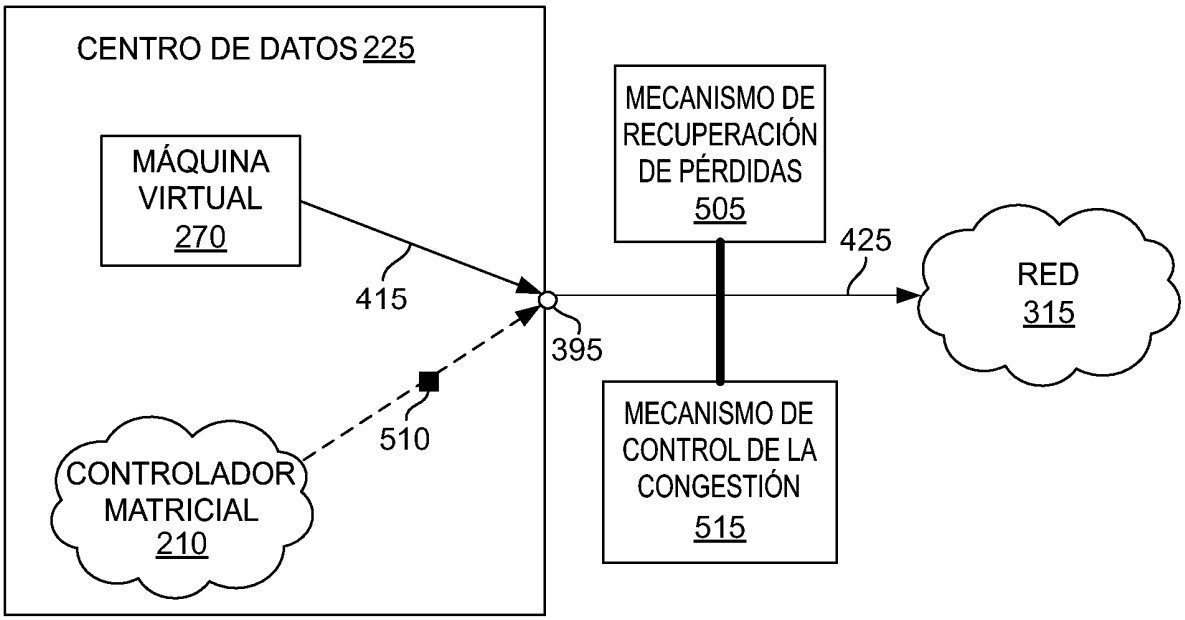
CENTRO DE DATOS 225
MÁQUINA VIRTUAL 270
415
395
510
CONTROLADOR MATRICIAL 210
MECANISMO DE RECUPERACIÓN DE PÉRDIDAS 505
425
RED 315
MECANISMO DE CONTROL DE LA CONGESTIÓN 515

FIG. 5.

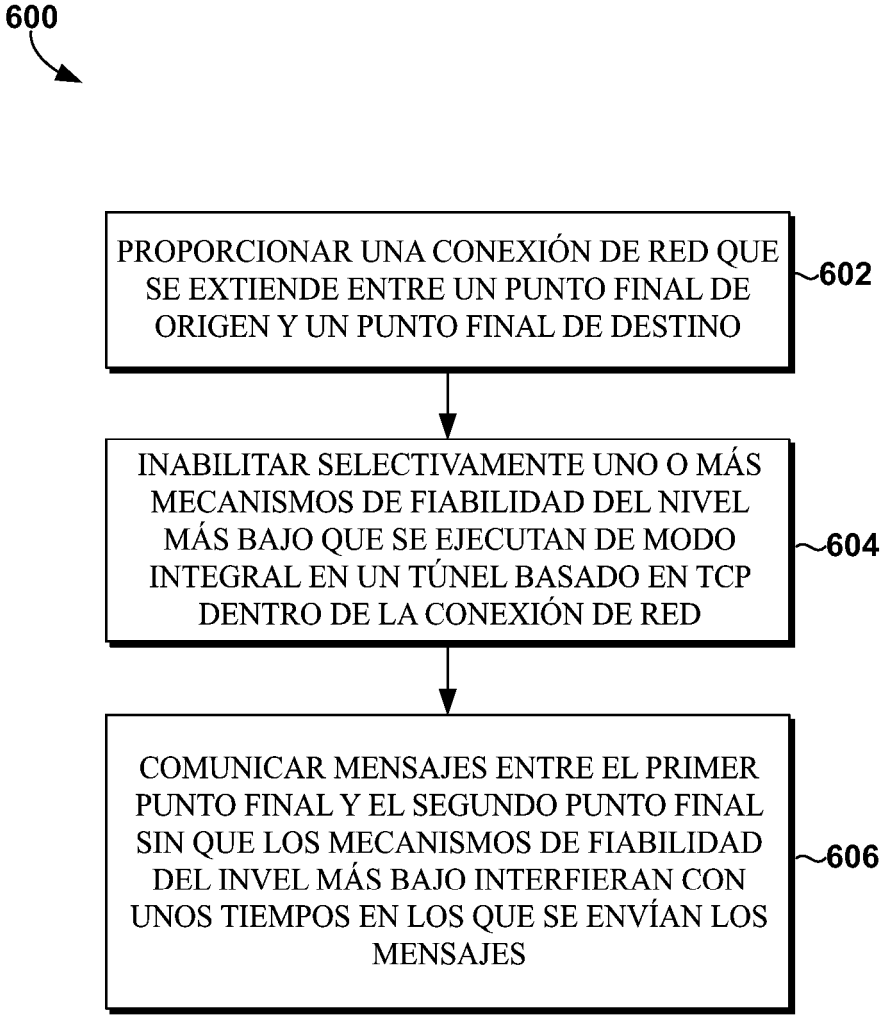
600
PROPORCIONAR UNA CONEXIÓN DE RED QUE SE EXTIENDE ENTRE UN PUNTO FINAL DE ORIGEN Y UN PUNTO FINAL DE DESTINO
602
INABILITAR SELECTIVAMENTE UNO O MÁS MECANISMOS DE FIABILIDAD DEL NIVEL MÁS BAJO QUE SE EJECUTAN DE MODO INTEGRAL EN UN TÚNEL BASADO EN TCP DENTRO DE LA CONEXIÓN DE RED
604
COMUNICAR MENSAJES ENTRE EL PRIMER PUNTO FINAL Y EL SEGUNDO PUNTO FINAL SIN QUE LOS MECANISMOS DE FIABILIDAD DEL INVEL MÁS BAJO INTERFIERAN CON UNOS TIEMPOS EN LOS QUE SE ENVÍAN LOS MENSAJES
606

FIG. 6.

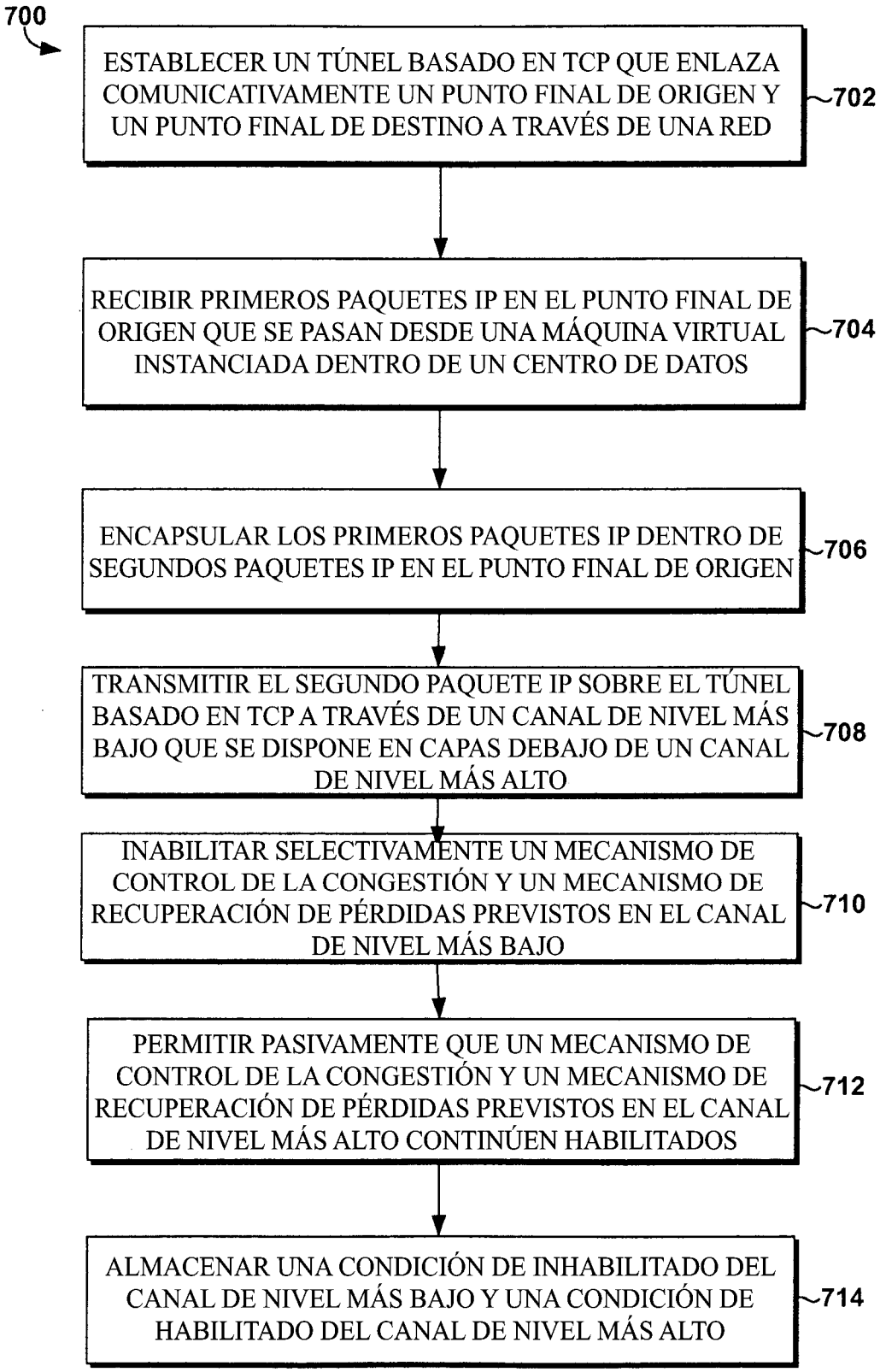
700
ESTABLECER UN TÚNEL BASADO EN TCP QUE ENLAZA COMUNICATIVAMENTE UN PUNTO FINAL DE ORIGEN Y UN PUNTO FINAL DE DESTINO A TRAVÉS DE UNA RED
702
RECIBIR PRIMEROS PAQUETES IP EN EL PUNTO FINAL DE ORIGEN QUE SE PASAN DESDE UNA MÁQUINA VIRTUAL INSTANCIADA DENTRO DE UN CENTRO DE DATOS
704
ENCAPSULAR LOS PRIMEROS PAQUETES IP DENTRO DE SEGUNDOS PAQUETES IP EN EL PUNTO FINAL DE ORIGEN
706
TRANSMITIR EL SEGUNDO PAQUETE IP SOBRE EL TÚNEL BASADO EN TCP A TRAVÉS DE UN CANAL DE NIVEL MÁS BAJO QUE SE DISPONE EN CAPAS DEBAJO DE UN CANAL DE NIVEL MÁS ALTO
708
INABILITAR SELECTIVAMENTE UN MECANISMO DE CONTROL DE LA CONGESTIÓN Y UN MECANISMO DE RECUPERACIÓN DE PÉRDIDAS PREVISTOS EN EL CANAL DE NIVEL MÁS BAJO
710
PERMITIR PASIVAMENTE QUE UN MECANISMO DE CONTROL DE LA CONGESTIÓN Y UN MECANISMO DE RECUPERACIÓN DE PÉRDIDAS PREVISTOS EN EL CANAL DE NIVEL MÁS ALTO CONTINÚEN HABILITADOS
712
ALMACENAR UNA CONDICIÓN DE INHABILITADO DEL CANAL DE NIVEL MÁS BAJO Y UNA CONDICIÓN DE HABILITADO DEL CANAL DE NIVEL MÁS ALTO
714

FIG. 7.