(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 013 309**

(51) Int. CI.:

G06F 9/30 (2008.01)
G06F 9/38 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.11.2021 PCT/EP2021/082175**

(87) Fecha y número de publicación internacional: **23.06.2022 WO22128320**

(96) Fecha de presentación y número de la solicitud europea: **18.11.2021 E 21816013 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2025 EP 4264419**

(54) Título: **Filtrado del tipo de comando basado en el indicador de filtrado por cada comando**

(30) Prioridad:

15.12.2020 US 202017122346

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2025

(73) Titular/es:

INTERNATIONAL BUSINESS MACHINES CORPORATION (100.00%)
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es:

GOMES, LOUIS y
KISLEY, RICHARD

(74) Agente/Representante:

ELZABURU, S.L.P

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

Filtrado del tipo de comando basado en el indicador de filtrado por cada comando

Antecedentes

Uno o más aspectos se refieren, en general, a facilitar el procesamiento dentro de un entorno informático y, en particular, a facilitar el procesamiento asociado con el procesamiento de comando dentro del entorno informático.

Los entornos informáticos suelen incluir diferentes tipos de procesadores para mejorar el procesamiento. Como ejemplo, un entorno informático puede incluir una o más unidades centrales de procesamiento, que se consideran los procesadores principales, y uno o más procesadores adjuntos que se consideran subordinados a las unidades centrales de procesamiento. Un procesador adjunto habitualmente realiza tipos específicos de tareas. Por ejemplo, un ejemplo particular de un procesador adjunto es una tarjeta criptográfica (crypto) que se utiliza para realizar operaciones criptográficas.

Un ejemplo de tarjeta criptográfica comercializada por la firma International Business Machines Corporation, de Armonk, Nueva York, es una tarjeta Crypto Express conectada a un canal. Una tarjeta Crypto Express está definida para admitir varios tipos de comandos, tales como comandos que utilizan claves cifradas (denominados comandos de clave segura), comandos que utilizan claves no cifradas (denominados comandos de clave no cifrada), comandos hash, comandos de consulta, comandos de generación de números aleatorios, etc. Además, una tarjeta Crypto Express está diseñada para admitir múltiples modos, incluyendo, por ejemplo: un modo de arquitectura criptográfica común (Common Cryptographic Architecture, CCA), un modo de acelerador y un modo de estándares criptográficos de clave pública de empresa (Enterprise Public Key Cryptographic Standards, PKCS) (también conocido como modo XCP/EP11 - PKSC #11 de empresa). Cada modo está configurado para procesar tipos específicos de comandos.

Se puede configurar una tarjeta Crypto Express para que funcione en uno de los diferentes modos múltiples mientras dura la configuración de la máquina activada. Por lo tanto, si un cliente desea utilizar los diferentes modos, el entorno informático incluiría al menos el número de tarjetas para los diferentes múltiples modos, cada una configurada en un modo diferente y capaz de procesar tipos específicos de comandos según lo definido para ese modo.

La solicitud de Patente internacional número WO 2003/042819 A1, Moyer, W.C. («Method and apparatus for interfacing a processor to a coprocessor», 22 de mayo de 2003) da a conocer un procesador que tiene un conjunto de especificadores de difusión que utiliza para difundir selectivamente un operando que se está escribiendo en un registro dentro del procesador, a un bus de comunicación del coprocesador. Por lo tanto, cada especificador de difusión puede incluir un indicador de difusión correspondiente a cada registro de propósito general del procesador. Una realización alternativa también puede utilizar el concepto de regiones de difusión, donde cada región de difusión puede tener un especificador de difusión correspondiente, donde un especificador de difusión puede corresponder a múltiples regiones de difusión. Alternativamente, el procesador puede utilizar regiones de difusión independientes de los especificadores de difusión, donde el coprocesador puede alterar su funcionalidad en respuesta a la región de difusión actual. El procesador puede proporcionar un especificador de región (REGIÓN H) a través del bus de comunicación del coprocesador (30) para indicar la región de difusión actual. La solicitud de patente internacional número WO 99/61982 A1, Gorishek, F. J. et al. («Coprocessor support allowing non-native code to run in a system», 2 de diciembre de 1999) da a conocer un procesador del ordenador central que incluye hardware configurado para ejecutar instrucciones definidas por una arquitectura de conjunto de instrucciones del ordenador central, mientras que un coprocesador de emulación incluye hardware configurado para ejecutar instrucciones definidas por una arquitectura de conjunto de instrucciones diferente de la arquitectura del conjunto de instrucciones del ordenador central. La solicitud de Patente estadounidense número US 2010/100656 A1, Gainey, Charles W. Jr, et al. («Interruption facility for adjunct processor queues», 22 de abril de 2010) da a conocer el servicio de interrupción para las colas de procesadores adjuntos. En respuesta a que una cola pasa de un estado sin respuesta pendiente a un estado de respuesta pendiente, se inicia una interrupción. Esta interrupción indica a un procesador que la respuesta a una solicitud está esperando en la cola. Para que la cola aproveche la capacidad de interrupción, está habilitada para interrupciones.

Compendio

Según la presente invención, se dan a conocer un método, un sistema y un producto de programa informático según las reivindicaciones independientes. Se superan los inconvenientes de la técnica anterior y se proporcionan ventajas adicionales proporcionando un producto de programa informático para facilitar el procesamiento en un entorno informático. El producto de programa informático incluye uno o más medios de almacenamiento legibles por ordenador e instrucciones de programa almacenadas conjuntamente en el uno o más medios de almacenamiento legibles por ordenador, para realizar un método. El método incluye determinar dinámicamente, por un procesador adjunto, si las órdenes obtenidas por el procesador adjunto deben ser procesadas por el procesador adjunto. La determinación dinámica se realiza por cada comando e incluye la obtención, por el procesador adjunto, de una solicitud de comando de un solicitante. La solicitud de comando incluye al menos un indicador de filtrado que indica al menos un tipo de comando válido para su procesamiento por el procesador adjunto, para el solicitante. El procesador adjunto determina, utilizando el al menos un indicador de filtrado, si un comando de la solicitud de comando es válido para ser procesado por el procesador adjunto, para el solicitante. El procesador adjunto procesa el comando basándose en la

determinación de que el comando es válido para el procesamiento por el procesador adjunto, para el solicitante.

Determinando dinámicamente por cada comando si un procesador adjunto debe procesar un comando en particular, se proporciona flexibilidad en el procesamiento de comandos. Un comando es válido o no válido en el momento del procesamiento del comando y, por lo tanto, el programa no tiene que cambiar entre diversos procesadores adjuntos para ejecutar diferentes tipos de comandos. Esto reduce la complejidad del programa, proporcionando un código más eficiente y mejorando el tiempo de ejecución y el rendimiento del código.

En una realización, el procesador adjunto está configurado en un modo y la determinación dinámica le permite funcionar de manera diferente al modo en el que está configurado. Por ejemplo, en un ejemplo, el procesador adjunto configurado en el modo único puede procesar un conjunto de comandos; sin embargo, el procesador adjunto funciona de manera diferente en que procesa un conjunto reducido del conjunto de comandos. El procesador adjunto puede cambiar los modos de filtrado de manera dinámica para cada comando, puesto que el filtrado por tipo de comando se proporciona por cada comando. Esto permite utilizar un procesador adjunto particular en diferentes modos. Por ejemplo, el procesador adjunto puede ser configurado en un modo, pero puede funcionar en un modo diferente sin reconfigurar el procesador adjunto. Además, permitiendo que un procesador adjunto funcione en diferentes modos, se ahorra el gasto de procesadores adjuntos adicionales y se proporciona flexibilidad en el sistema.

En una realización, el al menos un indicador de filtrado se configura por cada comando. Proporcionando un indicador de filtrado por cada comando, se proporciona flexibilidad en el procesamiento de comandos, así como una menor complejidad del código, un mayor rendimiento y una reducción de los gastos, puesto que es posible que se necesiten menos procesadores adjuntos.

En una realización, el al menos un indicador de filtrado se configura basándose en una política informática correspondiente al solicitante de la solicitud de comando. Esto permite tener en cuenta los atributos particulares de la licencia, los permisos y/o los requisitos del cliente en el procesamiento de los comandos.

En una realización, el al menos un indicador de filtrado incluye un indicador del tipo de comando sin estado, en el que, basándose en que el indicador del tipo de comando sin estado se configura en un valor, los comandos que se determina que son comandos del tipo de comando sin estado son válidos para su procesamiento por el procesador adjunto, para el solicitante, y otros comandos del tipo de comando no son válidos para su procesamiento por parte del procesador adjunto, para el solicitante. Además, en una realización, basándose en que el indicador del tipo de comando sin estado se configura en otro valor, los otros comandos del tipo de comando también se consideran válidos para su procesamiento por el procesador adjunto, para el solicitante. Esto permite que un procesador adjunto configurado en un modo que proporciona un conjunto completo de comandos se utilice para proporcionar comandos selectivos, en lugar del conjunto completo de comandos para uno o más solicitantes y el conjunto completo de comandos para otros solicitantes. Esto proporciona flexibilidad, reduce la complejidad del código, aumenta el rendimiento y reduce los gastos, puesto que es posible que se necesiten menos procesadores adjuntos.

En una realización, el procesamiento incluye la preparación de una respuesta que incluye un resultado del procesamiento del comando, la respuesta que se enviará al solicitante. Además, en una realización, se prepara una respuesta a error que indica un error basándose en la determinación de que el comando no es válido para su procesamiento por el procesador adjunto, para el solicitante, y la respuesta a error se enviará al solicitante. La respuesta a error informa al solicitante de que el comando es un tipo de comando no válido.

Como ejemplo, el procesador adjunto es una tarjeta criptográfica.

También se describen y se reivindican en la presente memoria métodos y sistemas relacionados con uno o más aspectos. Además, también se describen y pueden estar reivindicados en la presente memoria servicios relacionados con uno o más aspectos.

Se obtienen características y ventajas adicionales a través de las técnicas descritas en la presente memoria. Otras realizaciones y aspectos se describen en detalle en la presente memoria y se consideran parte de los aspectos reivindicados.

Breve descripción de los dibujos

A continuación se describirán realizaciones preferidas de la presente invención, sólo a modo de ejemplo, y haciendo referencia a los siguientes dibujos:

la figura 1A representa un ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención;

la figura 1B representa otro ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención;

las figuras 2A-2D representan un ejemplo de una instrucción de Procesar cola de procesadores adjuntos, según uno o más aspectos de la presente invención;

la figura 3A representa un ejemplo de un mensaje de solicitud de comando de procesador adjunto, según uno o más aspectos de la presente invención;

la figura 3B representa un ejemplo de una solicitud de Bloque de solicitud de programación de conectividad (Connectivity Programming Request Block, CPRB), según uno o más aspectos de la presente invención;

la figura 3C representa un ejemplo de un mensaje de solicitud de comando de procesador adjunto, según uno o más aspectos de la presente invención;

la figura 3D representa un ejemplo de una respuesta de Bloque de solicitud de programación de conectividad (CPRB), según uno o más aspectos de la presente invención;

la figura 4 representa un ejemplo de un flujo para proporcionar filtrado por cada comando, según uno o más aspectos de la presente invención;

las figuras 5A-5B representan una realización de aspectos relacionados con la facilitación del procesamiento dentro de un entorno informático, según uno o más aspectos de la presente invención;

la figura 6A representa un ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención;

la figura 6B representa otro ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención;

la figura 6C representa un ejemplo de detalles adicionales de una memoria de la figura 6B, según uno o más aspectos de la presente invención;

la figura 6D representa otro ejemplo de detalles adicionales de una memoria de la figura 6B, según uno o más aspectos de la presente invención;

la figura 7A representa otro ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención;

la figura 7B representa detalles adicionales de la memoria de la figura 7A, según uno o más aspectos de la presente invención;

la figura 8 representa una realización de un entorno informático en la nube, según uno más aspectos de la presente invención; y

la figura 9 representa un ejemplo de capas de modelo de abstracción, según uno o más aspectos de la presente invención.

Descripción detallada

Según uno o más aspectos de la presente invención, se proporciona una capacidad de filtrado que permite a un procesador adjunto, tal como una tarjeta criptográfica (crypto), determinar dinámicamente, por cada comando, si un comando obtenido por el procesador adjunto va a ser ejecutado por el procesador adjunto. Por ejemplo, se utilizan uno o más indicadores de filtrado por cada comando (por ejemplo, indicadores de filtrado del tipo de comando seleccionados) para determinar si un comando recibido es un tipo de comando válido según lo especificado por los indicadores de filtrado por cada comando y, por lo tanto, debe ser ejecutado por el procesador adjunto. En una realización, los uno o más indicadores de filtrado por cada comando se configuran por cada comando basándose en una política informática asociada con el solicitante del comando. Por lo tanto, un comando emitido por un solicitante puede ser un tipo de comando válido para su ejecución, pero emitido por otro solicitante puede no ser válido, según lo especificado por los indicadores de filtrado por cada comando configurados basándose en las políticas informáticas de los solicitantes.

En uno o más aspectos, el procesador adjunto está configurado en un modo de procesamiento particular (por ejemplo, el modo de arquitectura criptográfica común (CCA); también conocido como modo de coprocesador) pero se le puede aplicar el filtrado de tal manera que funciona de manera diferente al modo configurado sin tener que ser reconfigurado. Por ejemplo, basándose en el filtrado, tal como el filtrado del tipo de comando seleccionado, el procesador adjunto ejecuta los comandos de uno o más tipos de comandos seleccionados (por ejemplo, comandos del tipo de comando sin estado), en el que los tipos de comando seleccionados son menos que todos los tipos de comando admitidos por el modo configurado. Es decir, un comando que puede estar admitido en el modo de procesamiento configurado (por ejemplo, un comando del tipo de comando sin estado) puede no ser ejecutado por el procesador adjunto, en un caso particular, cuando se aplica el filtrado del tipo de comando seleccionado, si no es de un tipo de comando seleccionado (por ejemplo, un comando del tipo de comando sin estado).

En un ejemplo, la técnica de filtrado que se aplica es una técnica de filtrado del tipo de comando sin estado, en la que el procesador adjunto configurado en un modo (por ejemplo, un modo de coprocesador) se puede utilizar para ejecutar un conjunto completo de tipos de comando admitidos en este modo, o un conjunto reducido de tipos de comando (por ejemplo, solo comandos del tipo de comando sin estado). Sin embargo, aunque la técnica de filtrado del tipo comando sin estado se describe en el presente documento como un ejemplo, se pueden aplicar otras técnicas de filtrado del tipo de comando y/u otras técnicas de filtrado. Por ejemplo, se puede utilizar una técnica de filtrado de claves principales en la que los tipos de comando seleccionados son comandos de clave de gestión de claves principales. Como ejemplo adicional, el filtrado puede ser implementado con límites de casos de uso impuestos por política. Por ejemplo, si el acceso a un comando seleccionado tiene un precio diferente al de los accesos a comandos de criptografía generales, se puede imponer un filtro para el caso de utilización adquirido. Un nivel adicional de filtrado puede estar basado en un acuerdo de servicio de rendimiento, en el que los comandos se designan con prioridades de rendimiento de respuesta de servicio altas o bajas en función del rendimiento adquirido. También se pueden utilizar otras técnicas de filtrado. Se permite la aplicación de cada una de las técnicas de filtrado sin reconfigurar el procesador adjunto para otro modo. Las técnicas de filtrado se pueden utilizar en conjunto o por separado unas de otras. Son posibles muchos ejemplos.

Una realización de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención se describe haciendo referencia a la figura 1A. En un ejemplo, un entorno informático 100 incluye al menos una unidad central de procesamiento 102 y al menos un procesador adjunto (Adjunct Processor, AP) 104, cada uno de los cuales está acoplado a al menos una parte de la memoria, denominada memoria del sistema 106. Como ejemplo, la memoria del sistema 106 incluye un área del sistema de hardware, que es accesible indirectamente y no es visible para los programas que se ejecutan en la una o varias unidades centrales de procesamiento. (Accesible indirectamente se utiliza en el presente documento con el significado de que el área del sistema de hardware o la una o varias colas de procesadores adjuntos almacenadas en ella (que se describen a continuación) solo son accesibles mediante instrucciones limitadas específicas, y no se puede acceder a ellas de otro modo (por ejemplo, no pueden ser cargados en ella, los programas desconocen las direcciones, etc.)). Dentro de la memoria del sistema se encuentran una o más colas de procesadores adjuntos 108. Estas colas no son visibles directamente desde los programas de usuario y, por el contrario, se consideran parte de la máquina (es decir, la máquina que incluye la una o varias unidades centrales de procesamiento, la memoria del sistema y el uno o varios procesadores adjuntos). Una unidad central de procesamiento tiene acceso a las colas de la memoria del sistema, por ejemplo, emitiendo instrucciones para colocar solicitudes en la cola y/o para eliminar las respuestas de la cola. Sin embargo, el procesador adjunto tiene acceso directo a las colas a través de, por ejemplo, una capa de transporte 110 (por ejemplo, i390CO), y es responsable de eliminar las solicitudes de la cola, de procesar las solicitudes y de colocar las respuestas a las solicitudes en la cola.

Otra realización de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención se describe haciendo referencia a la figura 1B. En esta realización, la máquina incluye soporte virtual y hay al menos una unidad central de procesamiento 150 del ordenador central que incluye una pluralidad de huéspedes 152 (por ejemplo, sistemas operativos huésped y/o programas huésped). La unidad central de procesamiento del ordenador central está acoplada a al menos una parte de la memoria, denominada memoria del sistema 154. Además, hay al menos un procesador adjunto 156, que también está acoplado a la memoria del sistema 154, a través de, por ejemplo, una capa de transporte 160. Como ejemplo, la memoria del sistema 154 incluye un área del sistema de hardware y, dentro de la memoria del sistema, se encuentran una o más colas de procesadores adjuntos 158.

Como se ha indicado, existen diferentes tipos de procesadores adjuntos, incluidos, entre otros, tarjetas criptográficas o adaptadores. Un ejemplo específico de una tarjeta criptográfica es una tarjeta Crypto Express comercializada por la firma International Business Machines Corporation, de Armonk, Nueva York. Aunque se proporciona un ejemplo de tarjeta criptográfica, otras tarjetas criptográficas comercializadas por la firma International Business Machines Corporation y/u otras firmas pueden incorporar y/o utilizar uno o más aspectos de la presente invención. Además, otros tipos de procesadores adjuntos pueden incorporar y/o utilizar uno o más aspectos de la presente invención.

En una realización, un procesador adjunto, tal como una tarjeta criptográfica (por ejemplo, una tarjeta Crypto Express), admite una pluralidad de modos, incluidos, entre otros, un modo de coprocesador, un modo de acelerador y un modo de estándares criptográficos de clave pública de empresa (PKCS) (por ejemplo, XCP/EP11 - Enterprise PKCS#11), como ejemplos. En otros ejemplos, se pueden admitir menor y/u otros modos adicionales. Cada uno de los modos puede tener sus propias estructuras y formatos de mensajes de AP.

Como ejemplo, un mensaje de procesador adjunto se compone de múltiples segmentos de datos y los segmentos de datos pueden no ser adyacentes entre sí; por el contrario, uno o más pueden estar intercalados. Estos segmentos de datos se denominan segmentos de datos de recopilación dispersa. En un ejemplo, una tarjeta criptográfica no tiene acceso directo al mensaje de AP puesto en cola, y una parte del mensaje (por ejemplo, la parte inferior del mensaje de AP) contiene los datos que utilizará, por ejemplo, la tarjeta criptográfica para ejecutar el comando de AP. Por lo tanto, la capa de transporte de comandos de AP (por ejemplo, la capa de transporte 110, 160) copia los datos relevantes del mensaje de solicitud de comando de AP, los empaqueta en un formato que la tarjeta criptográfica entiende (por ejemplo, el mensaje de solicitud de comando de la tarjeta cripto) y los envía a la tarjeta criptográfica. De manera similar, después de que la tarjeta criptográfica ejecute el comando de AP, la capa de transporte del comando de AP genera un mensaje de respuesta del comando de AP utilizando diversas partes del mensaje de solicitud del comando de AP y el mensaje de respuesta del comando de la tarjeta criptográfica, y lo envía a la cola de AP para que

el programa lo elimine de la cola más adelante. Otros detalles de un mensaje de solicitud de comando de AP y un mensaje de respuesta de comando de AP, se describen a continuación, incluidos aspectos de los mensajes utilizados según el filtrado del tipo de comando de uno o más aspectos de la presente invención.

Según un aspecto de la presente invención, se diseña un procesador adjunto (por ejemplo, una tarjeta criptográfica) que permite al hipervisor de la máquina solicitar un filtrado del tipo de comando según las políticas informáticas (por ejemplo, los términos de la licencia, los permisos y/o los requisitos de recursos, tales como los requisitos de alta disponibilidad, de los clientes, etc.). Puesto que los clientes tienen diferentes políticas informáticas asociadas (por ejemplo, condiciones de licencia, permisos y/o requisitos de recursos, tales como requisitos de alta disponibilidad), es posible que no todos los tipos de comandos estén disponibles para un cliente en particular. Por lo tanto, según un aspecto de la presente invención, se da a conocer un filtrado del tipo de comando, de tal manera que un procesador adjunto seleccionado (por ejemplo, una tarjeta criptográfica configurada para un modo particular (por ejemplo, el modo de coprocesador)) puede ser utilizado para clientes con diferentes políticas informáticas y, por lo tanto, diferentes permisos, sin necesidad de que el procesador adjunto sea reconfigurado en un modo compatible diferente.

Como ejemplo, se da a conocer una función de filtrado del tipo de comando de AP (APFT) que permite filtrar los comandos de AP basándose en una o más funciones de filtrado del tipo de comando de AP seleccionadas por cada comando, según uno o más aspectos de la presente invención. En un ejemplo, la una o más funciones de filtrado del tipo de comando de AP seleccionada incluye una función de filtrado de comando de AP sin estado (stateless AP Command Filtering, SAPCF). Aspectos de la función de filtrado del tipo de comando de AP y de la función de filtrado de comando de AP sin estado se describen en el presente documento con respecto a una arquitectura particular, tal como la arquitectura de hardware z/Architecture®, comercializada por la firma International Business Machines Corporation, Armonk, Nueva York. Una realización de la arquitectura de hardware z/Architecture se describe en una publicación de IBM titulada "z/Architecture Principles of Operation" No. SA22-7832-12, decimotercera edición, septiembre de 2019.

IBM y Z/ARCHITECTURE son marcas comerciales registradas de International Business

Machines Corporation en al menos una jurisdicción. Sin embargo, la arquitectura de hardware z/Architecture es solo un ejemplo de arquitectura. Aspectos de la invención también pueden estar basados en otras arquitecturas. que incluyen, entre otros, las arquitecturas Intel® x86, otras arquitecturas comercializadas por la firma International Business Machines Corporation y/o arquitecturas comercializadas por otras firmas.

En un ejemplo, cuando se instala la función de filtrado de comando de AP sin estado, se instala la función de filtrado del tipo de comando de AP. Para determinar si la función de filtrado de comando de AP sin estado está instalada, se utiliza una instrucción de Procesar cola de procesadores adjuntos, según un aspecto de la presente invención.

Un ejemplo de una instrucción de Procesar cola de procesadores adjuntos (Process Adjunct Processor Queue, PQAP) se describe haciendo referencia a la figura 2A. Como se muestra, en un ejemplo, una instrucción 200 de procesar una cola de procesadores adjuntos incluye un código de operación (opcode) 202 (por ejemplo, los bits 0 a 15 de una instrucción de 32 bits) que indica una operación de proceso de una cola de procesadores adjuntos. En una realización, la instrucción Procesar cola de procesadores adjuntos emplea una pluralidad de registros generales, incluidos los registros generales 0, 1 y 2. La cola de AP designada por el número de cola de AP (AP Queue Number, APQN) en el registro general 0 se procesa según el código de función especificado en el registro general 0. Ejemplos de los registros generales 0, 1 y 2 se describen con más detalle a continuación.

Haciendo referencia a la figura 2B, en una realización, el registro general 0 (GR0) 210 es, por ejemplo, un registro de 64 bits que incluye, por ejemplo, un código de función (function code, FC) 212 (por ejemplo, los bits 32 a 39) para indicar una función seleccionada que se va a realizar; un indicador de funciones de prueba (Test, T) 214 (por ejemplo, el bit 40) utilizado para indicar si se proporciona una máscara de funciones instaladas en el registro general 2; y un número de cola de procesadores adjuntos (APQN) 216 (por ejemplo, los bits 48 a 63) que identifican una cola de procesadores adjuntos (por ejemplo, la cola de AP 108 (figura 1A); la cola de AP 158 (figura 1B)) procesada según el código de función.

Basándose en la emisión de la instrucción de Procesar cola de procesadores adjuntos, el código de función 212 debe incluir uno de una pluralidad de códigos aceptables, un ejemplo de los cuales es el código 00 de cola de AP de prueba (Test AP Queue, TAPQ).

Según uno o más aspectos de la presente invención, cuando el entorno informático está, por ejemplo, en modo arquitectónico de z/Architecture y la función APFT está instalada, si se especifica el código de función de TAPQ (por ejemplo, FC=00 en GR0), el bit 40 del registro general 0 se define como el bit de las funciones de prueba (T) para la función de TAPQ. Cuando T es uno, los bits 0-31 del registro general 2 se sustituyen por una máscara de las funciones de AP instaladas y otra información asociada, un ejemplo de lo cual se describe a continuación. Cuando T es cero, lo que indica, por ejemplo, que la función de APFT no está instalada, los resultados del registro general 2 se limitan, por ejemplo, a las posiciones de bits 32-63, y las posiciones de bits 0-31 se ignoran y no cambian. En este caso, los campos AT y QD (descritos a continuación) son válidos y las demás posiciones de bits se almacenan como ceros.

Como se ha indicado, además del registro general 0, la instrucción Procesar cola de procesadores adjuntos utiliza los registros generales 1 y 2, cada uno de los cuales se describe con más detalle en el presente documento.

Haciendo referencia a la figura 2C, en una realización, el registro general 1 (GR1) 220 es, por ejemplo, un registro de 64 bits que incluye, por ejemplo, una palabra de estado de cola de procesadores adjuntos (Adjunct Processor Queue Status Word, APQSW) 222 (por ejemplo, los bits 32 a 63). Al finalizar la instrucción de Procesar cola de procesadores adjuntos, el campo de APQSW contiene una palabra de estado de la cola del AP, a menos que se indique lo contrario para una función en particular. La palabra de estado de la cola del AP indica, por ejemplo, el estado de la cola del AP al finalizar la instrucción.

Además, haciendo referencia a la figura 2D, en una realización, el registro general 2 (GR2) 230 es, por ejemplo, un registro de 64 bits que incluye una pluralidad de campos. Como se describe en el presente documento, en una realización, las posiciones de bits 0-31, cuando están configuradas, incluyen una máscara de las funciones de AP instaladas y otra información asociada. Los campos de ejemplo de GR2, según uno o más aspectos de la presente invención, incluyen, por ejemplo:

Modo 232: Cuando está configurado, este campo (por ejemplo, los bits 3-5) indica una pluralidad de posibles funciones de modo de AP. Por ejemplo, cuando D (por ejemplo, el bit 3) es uno, el AP especificado proporciona la función de modo de coprocesador; cuando A (por ejemplo, el bit 4) es uno, el AP especificado proporciona la función de modo de acelerador; y cuando X (por ejemplo, el bit 5) es uno, el AP especificado proporciona la función de modo de XCP;

SL 234: Cuando este campo (por ejemplo, el bit 7) es uno, se instala la función de filtrado de comando de AP sin estado (SAPCF) de uno o más aspectos de la presente invención. La función SAPCF es, por ejemplo, una función de dispositivo cripto PCI-X (Peripheral Component Interconnect Extended) y se instala, por ejemplo, en el modo arquitectónico z/Architecture, en una realización;

Otras funciones y/o información relacionada con una o más funciones que pueden ser compatibles con el entorno informático pueden indicarse con uno o más bits de la máscara en, por ejemplo, los bits 0-31.

Tipo de procesador adjunto (Adjunct processor Type, AT) 236: Este campo (por ejemplo, las posiciones de bits 32-39) incluye ejemplos de valores de tipo de AP válidos en el intervalo de, por ejemplo, 0-255 que indican diversos tipos de AP;

Número de entradas de cola de AP (QD) 240: El número de entradas de cola en cada cola de AP en la configuración. QD es un valor en el rango, por ejemplo, 0-31, que representa un número de entradas de cola en el rango, por ejemplo, 1-32 decimales.

En un ejemplo, la información de la función instalada devuelta en el registro general 2 se aplica a todos los AP del mismo tipo de AP y, para los AP consolidados (por ejemplo, AP de tipo 10 o superior), en el mismo modo de configuración. La información de la función instalada es, en una realización, persistente al menos hasta el siguiente reinicio del subsistema. Se puede agregar una función simultáneamente. Una función puede o no ser eliminada simultáneamente cuando se desconfigura el último AP de un tipo de AP.

El registro general 2 se modifica tal como se define cuando la función TAPQ finaliza con, por ejemplo, el código de condición 0 (finalización satisfactoria); o el código de condición 3, los códigos de respuesta, por ejemplo, 02-05 (condiciones inesperadas; por ejemplo, restablecimiento de la cola de AP en curso, AP desconfigurado, parada de verificación de AP, AP ocupado). De lo contrario, el registro general 2 no se modifica.

Aunque en una realización del presente documento se describen campos, ubicaciones de campos, tamaños de campos, bits y valores de campos o bits específicos para la instrucción Procesar cola de procesadores adjuntos y sus registros asociados, se pueden utilizar otros campos, ubicaciones de campos, tamaños de campos, bits y/o valores de campos o bits sin apartarse del alcance de uno o más aspectos de la invención. Los campos y/o bits de cada uno de los registros generales no descritos en el presente documento pueden estar en blanco, tener un valor predefinido (por ejemplo, cero) y/o incluir valores que deben ser ignorados en una realización. Existen muchas posibilidades.

Según uno o más aspectos, el procesador adjunto (por ejemplo, una tarjeta cripto) tiene una lógica que reconoce los atributos de diferentes tipos de comandos. Los diferentes tipos de comandos son proporcionados, en una realización, por un hipervisor. El hipervisor determina, por ejemplo, un conjunto de etiquetas del tipo de comando basándose, por ejemplo, en un conjunto de clientes desde los que se pueden recibir solicitudes de comando. Por ejemplo, los tipos de comando que se van a representar mediante el conjunto de etiquetas del tipo de comando se basan, por ejemplo, en las políticas informáticas (por ejemplo, condiciones de la licencia, permisos, requisitos de recursos, tales como, por ejemplo, requisitos de alta disponibilidad, etc.) de los clientes desde los que se van a recibir las solicitudes de comando.

En un ejemplo, un comando tiene un conjunto de etiquetas (por ejemplo, etiquetas de política o de filtrado) asociadas al mismo que representan los atributos del comando. Un comando puede tener múltiples etiquetas asociadas para múltiples tipos de comando y, por lo tanto, el conjunto de etiquetas incluye una o más etiquetas dependiendo de los tipos de comando para los que esté asociado el comando. Por ejemplo, un comando puede tener una etiqueta del tipo de comando sin estado para indicar que el comando es un comando del tipo de comando sin estado válido, una

etiqueta del tipo de comando de clave principal, para indicar que el comando es un comando del tipo de comando de clave principal válido, etc. El procesador adjunto obtiene una indicación del conjunto de etiquetas del tipo de comando (por ejemplo, proporcionadas, recibidas, recuperadas, etc.). En un ejemplo, el procesador adjunto recibe un conjunto de etiquetas del tipo de comando que incluye una etiqueta para comandos del tipo de comando de clave segura (por ejemplo, utilizada para deshabilitar comandos de clave segura cuando lo solicita la persona que llama); y una etiqueta para comandos del tipo de comando sin estado. En otras realizaciones, el hipervisor proporciona otras etiquetas para otras técnicas de filtrado, tales como otras técnicas de filtrado del tipo de comando. Existen muchas posibilidades.

Además, en una realización, una solicitud de comando está configurada para incluir uno o más indicadores de filtrado, tales como uno o más indicadores de filtrado del tipo de comando, utilizados para proporcionar un filtrado por cada comando, según uno o más aspectos de la presente invención. Detalles adicionales con respecto a los indicadores de filtrado del tipo de comando seleccionados incluidos en una solicitud de comando se describen haciendo referencia a las figuras 3A-3B.

Haciendo referencia a la figura 3A, en un ejemplo, un mensaje de solicitud de comando de AP 300 incluye una cabecera 302, una subcabecera 304 y una pluralidad de paquetes 306-312. En un ejemplo, uno o más de los paquetes (por ejemplo, uno o más del paquete-1 308-310) están configurados para proporcionar un comando y uno o más de los paquetes (por ejemplo, el paquete-2 312) están configurados para proporcionar datos de entrada. Uno de los paquetes incluye un bloque 308 de solicitud de programación de conectividad (CPRB) que incluye uno o más indicadores de filtrado relacionados con el filtrado del tipo de comando, según un aspecto de la presente invención.

Por ejemplo, como se muestra en la figura 3B, la solicitud de CPRB 308 incluye una máscara de filtro de comando de AP 320 que incluye uno o más indicadores de filtrado del tipo de comando. Un ejemplo de un indicador de filtrado del tipo de comando es un indicador 322 del tipo de comando sin estado. Este indicador indica si el conjunto de comando permitido es para comandos de tipo de comando sin estado (por ejemplo, el indicador 322, tal como un bit seleccionado, configurado en uno) o para el conjunto completo de comando (por ejemplo, el indicador 322 configurado en cero). Se pueden incluir otros indicadores, marcadores, bits, etc., en la solicitud de CPRB 308 para indicar otros tipos de comando que pueden ser filtrados. Por ejemplo, otro indicador puede indicar un filtrado basado en claves principales. Son posibles muchos otros ejemplos.

En respuesta a un mensaje, se proporciona una respuesta y, en una realización, tiene la forma de un mensaje de respuesta de un comando de AP, un ejemplo del cual se representa en la figura 3C. Como se muestra, un mensaje 330 de respuesta a un comando de AP incluye, por ejemplo, una cabecera 332, una subcabecera 334 y una pluralidad de paquetes 336-340. Uno de los paquetes incluye una respuesta de CPRB 336 que incluye una respuesta a la solicitud y puede indicar un error, según un aspecto de la presente invención.

Por ejemplo, como se muestra en la figura 3D, la respuesta CPRB 336 incluye una indicación de error. La indicación de error puede incluir un código de error 350 (por ejemplo, CPRB código-de-devolución/código-de-motivo) para informar de que un comando solicitado por el cliente no está permitido por un conjunto definido de etiquetas del tipo de comando (por ejemplo, impuesto por un hipervisor o por otra entidad).

Como se describe en el presente documento, los mensajes de solicitud de comando/respuesta se utilizan según un aspecto de la presente invención para proporcionar un filtrado del tipo de comando por cada comando. Detalles adicionales con respecto al filtrado del tipo de comando por cada comando se describen haciendo referencia a la figura 4. En el ejemplo de la figura 4, el entorno informático es un entorno en la nube; sin embargo, en otras realizaciones, el entorno informático es un entorno no en la nube.

Los aspectos de la invención no están limitados a un entorno informático particular.

Además, en el ejemplo de la figura 4, el procesador adjunto es una tarjeta criptográfica. Sin embargo, otros procesadores adjuntos pueden utilizar el filtrado; la tarjeta criptográfica es solo un ejemplo.

Haciendo referencia a la figura 4, en una realización, una solicitud criptográfica es creada por un solicitante, tal como un huésped 400 (por ejemplo, una aplicación huésped o un sistema operativo huésped en, por ejemplo, un entorno de nube), ETAPA 420. En un ejemplo, se codifica un mensaje de solicitud de comando de AP 300, y se proporciona a un hipervisor 402.

La solicitud criptográfica es obtenida (por ejemplo, recibida, recuperada, proporcionada, etc.) por el hipervisor 402 del huésped 400 y procesada, ETAPA 422. Según un aspecto de la presente invención, el hipervisor agrega (o configura) uno o más indicadores de filtrado, tales como indicadores de filtrado del tipo de comando, a la solicitud basándose en una política de solicitud 414 (por ejemplo, una política de solicitud en la nube). La política de solicitud 414 incluye, por ejemplo, una indicación para cada solicitante (por ejemplo, huésped, llamante, cliente) de los tipos de comandos permitidos que se procesarán para el solicitante basándose en la política informática del solicitante (por ejemplo, los términos de la licencia; los requisitos de recursos, tales como los requisitos de alta disponibilidad; y/o los permisos; etc.) proporcionada por la configuración de la cuenta 416 (por ejemplo, una configuración de cuenta en la nube).

Como ejemplo, el hipervisor 402 determina, basándose en la política de solicitud (que se basa en la política informática del huésped), si el indicador 322 de tipo de comando sin estado (u otro indicador de filtrado) se debe configurar en un valor de selección, por ejemplo, uno (por ejemplo, se permite un conjunto de comandos reducido, tal como que solo se permiten los comandos de tipo comando sin estado), o en otro valor de selección, por ejemplo, cero (por ejemplo, se permite un conjunto de comandos completo). El hipervisor configura el indicador 322 del tipo de comando sin estado (y/u otros indicadores de filtrado en otros ejemplos) basándose en la determinación.

El hipervisor 402 proporciona el mensaje de solicitud modificado (es decir, el mensaje de solicitud con los indicadores de filtrado configurados) a un procesador adjunto (por ejemplo, la tarjeta criptográfica 406). Por ejemplo, el hipervisor 402 envía o reenvía el mensaje de solicitud al procesador adjunto a través de, por ejemplo, un bus del sistema 404; o el procesador adjunto obtiene (por ejemplo, recupera) el mensaje de solicitud a través del bus del sistema 404.

El procesador adjunto, tal como la tarjeta criptográfica 406, en este ejemplo, procesa la solicitud, ETAPA 424. El procesamiento incluye determinar si la solicitud está permitida utilizando, por ejemplo, los indicadores de filtrado del tipo de comando incluidos en la solicitud, CONSULTA 426. Por ejemplo, si el indicador 322 del tipo de comando sin estado en el mensaje de solicitud recibido se configura en un valor, por ejemplo, uno, que indica que este solicitante (por ejemplo, huésped) está autorizado, por ejemplo, para comandos del tipo de comando sin estado, y el comando es un comando del tipo de comando sin estado, como indican una o más etiquetas (por ejemplo, etiquetas de política o de filtrado) asociadas con el comando, entonces la solicitud es válida. Sin embargo, si el comando es un comando del tipo de comando sin estado y el indicador 322 se configura en un valor (por ejemplo, uno), el comando es un comando no válido para este solicitante. De manera similar, si el indicador 322 está configurado en otro valor (por ejemplo, cero), entonces si el comando está incluido en el conjunto completo de comandos, como indican las etiquetas de política de tipo de comando, se considera válido.

Si la solicitud está permitida, se procesa (por ejemplo, se realizan operaciones de comando), ETAPA 428; de lo contrario, se produce un error, ETAPA 430. El procesador adjunto (por ejemplo, la tarjeta criptográfica) procesa una respuesta, ETAPA 432, que incluye colocar la respuesta en un mensaje de respuesta a un comando de AP, y se envía al huésped 400 a través de, por ejemplo, una capa de transporte (por ejemplo, la capa de transporte 110, 160). La respuesta puede incluir los resultados del procesamiento, un código de condición, un código de devolución, un código de motivo y/o una indicación de error (por ejemplo, el código de error en el CPRB de respuesta 336), como ejemplos. El huésped 400 recibe la respuesta, ETAPA 434.

Como se describe en el presente documento, en una realización, un procesador adjunto (por ejemplo, una tarjeta criptográfica) recibe un mensaje de solicitud de comando de un solicitante (por ejemplo, un huésped) y determina si se permite la ejecución del comando basándose en un conjunto de indicadores del tipo de comando impuesto por el hipervisor (por ejemplo, indicadores de filtrado del tipo de comando) en el bloque de solicitud de CPRB. El conjunto de indicadores de filtrado del tipo de comando impuesto por el hipervisor se utiliza en el filtrado por cada comando. Por ejemplo, el procesador adjunto ejecuta el comando si se determina que es válido basándose, por ejemplo, en los indicadores de filtrado del tipo de comando, y los resultados se colocan en un mensaje de respuesta al comando, que se envía a la persona que llama. Si se determina que el comando no es válido, se coloca un código de error en el CPRB del mensaje de respuesta al comando y se devuelve a la persona que llama.

Uno o más aspectos de la presente invención están inextricablemente ligados a la tecnología informática y facilitan el procesamiento, incluido el procesamiento de comandos, dentro de un entorno informático, mejorando el rendimiento del mismo. Detalles adicionales de una realización de aspectos relacionados con la facilitación del procesamiento dentro de un entorno informático se describen haciendo referencia a las figuras 5A-5B.

Haciendo referencia a la figura 5A, en una realización, un procesador adjunto determina dinámicamente si las órdenes obtenidas por el procesador adjunto deben ser procesadas por el procesador adjunto (500). La determinación dinámica se realiza por cada comando (502), e incluye, por ejemplo, la obtención por el procesador adjunto de una solicitud de comando de un solicitante (504). La solicitud de comando incluye al menos un indicador de filtrado que indica al menos un tipo de comando válido para su procesamiento por el procesador adjunto, para el solicitante (506). El procesador adjunto determina, utilizando el al menos un indicador de filtrado, si un comando de la solicitud de comando es válido para ser procesado por el procesador adjunto, para el solicitante (508). El procesador adjunto procesa el comando basándose en la determinación de que el comando es válido para ser procesado por el procesador adjunto, para el solicitante (510).

Determinando dinámicamente por cada comando si un procesador adjunto puede procesar un comando en particular, se proporciona flexibilidad en el procesamiento de comandos. Un comando es válido o no válido en el momento del procesamiento del comando y, por lo tanto, el programa no tiene que cambiar entre diversos procesadores adjuntos para ejecutar diferentes tipos de comandos. Esto reduce la complejidad del programa, proporcionando un código más eficiente y mejorando el tiempo de ejecución y el rendimiento del código.

En una realización, el procesador adjunto está configurado en un modo y la determinación dinámica le permite funcionar de manera diferente al modo en el que está configurado (512). Como ejemplo, el procesador adjunto configurado en el un modo puede procesar un conjunto de comandos (514), y el procesador adjunto funciona de manera diferente en que procesa un conjunto reducido del conjunto de comandos (516). El procesador adjunto puede

cambiar los modos de filtrado de manera dinámica para cada comando, puesto que el filtrado por tipo de comando se proporciona por cada comando. Esto permite utilizar un procesador adjunto en particular en diferentes modos. Por ejemplo, el procesador adjunto puede ser configurado en un modo, pero puede funcionar en un modo diferente sin reconfigurar el procesador adjunto. Además, al permitir que un procesador adjunto funcione en diferentes modos, se ahorra el gasto de procesadores adjuntos adicionales y se proporciona flexibilidad dentro del sistema.

Además, haciendo referencia a la figura 5B, en una realización, el al menos un indicador de filtrado se configura por cada comando (520). Proporcionando un indicador de filtrado por cada comando, se proporciona flexibilidad en el procesamiento de comandos, así como una menor complejidad del código, un mayor rendimiento y una reducción de los gastos, puesto que es posible que se necesiten menos procesadores adjuntos.

En una realización, el al menos un indicador de filtrado se configura basándose en una política informática correspondiente al solicitante de la solicitud de comando (522). Esto permite tener en cuenta los atributos particulares de la licencia, los permisos y/o los requisitos del cliente en el procesamiento de los comandos.

Como ejemplo, el al menos un indicador de filtrado incluye un indicador de tipo de comando sin estado (524). Basándose en que el indicador de tipo de comando sin estado está configurado en un valor, los comandos que se determine que son comandos del tipo de comando sin estado son válidos para su procesamiento por el procesador adjunto, para el solicitante, y otros comandos del tipo de comando son no válidos para su procesamiento por el procesador adjunto, para el solicitante (526). Basándose en que el indicador del tipo de comando sin estado está configurado en otro valor, los otros comandos del tipo de comando también se consideran válidos para su procesamiento por el procesador adjunto, para el solicitante (528). Esto permite que un procesador adjunto configurado en un modo que proporciona un conjunto completo de comandos se utilice para proporcionar comandos selectivos en lugar del conjunto completo de comandos para uno o más solicitantes, y el conjunto completo de comandos para otros solicitantes. Esto proporciona flexibilidad, reduce la complejidad del código, aumenta el rendimiento y reduce los gastos, puesto que es posible que se necesiten menos procesadores adjuntos.

En una realización, el procesamiento incluye la preparación de una respuesta que incluye un resultado del procesamiento del comando, respuesta que se enviará al solicitante (530). Además, en un ejemplo, se prepara una respuesta a error que indica un error basándose en la determinación de que el comando es no válido para su procesamiento por parte del procesador adjunto, para el solicitante, respuesta al error que se enviará al solicitante (532). La respuesta al error informa al solicitante de que el comando es un tipo de comando no válido.

Además, como ejemplo, el procesador adjunto es una tarjeta criptográfica (534).

Son posibles otras variaciones y realizaciones.

El filtrado del tipo de comando de uno o más aspectos de la presente invención puede ser incorporado y utilizado en muchos entornos informáticos. Un entorno informático de ejemplo se describe haciendo referencia a la figura 6A. Como ejemplo, el entorno informático se basa en la arquitectura de hardware z/Architecture®, comercializada por la firma International Business Machines Corporation, Armonk, Nueva York. Sin embargo, la arquitectura de hardware z/Architecture es solo un ejemplo de arquitectura. El entorno informático también puede estar basado en otras arquitecturas, que incluyen, entre otras, las arquitecturas Intel® x86, otras arquitecturas comercializadas por la firma International Business Machines Corporation y/o arquitecturas comercializadas por otras firmas.

Tal como se muestra en la figura 6A, un entorno informático 600 incluye, por ejemplo, un sistema informático 602 mostrado, por ejemplo, en forma de un dispositivo informático de propósito general. El sistema informático 602 puede incluir, entre otros, uno o más procesadores o unidades de procesamiento (por ejemplo, unidades centrales de procesamiento (Central Processing Units, CPU)) 604, una memoria 606 (también conocida como memoria del sistema, memoria principal, almacenamiento principal, almacenamiento o almacenamiento central, como ejemplos) y una o más interfaces de entrada/salida (E/S) 608, acopladas entre sí a través de uno o más buses y/o de otras conexiones 610.

El bus 610 representa uno o más de cualquiera de varios tipos de estructuras de bus, incluyendo un bus de memoria o controlador de memoria, un puerto de gráficos acelerado, y un procesador o bus local que usa cualquiera de una variedad de arquitecturas de bus. A modo de ejemplo, y no de limitación, tales arquitecturas incluyen la Arquitectura estándar de la industria (Industry Standard Architecture, ISA), la Arquitectura de microcanales (Micro Channel Architecture, MCA), la ISA mejorada (Enhanced ISA, EISA), el bus local de la Asociación de estándares de electrónicos de vídeo (Video Electronics Standards Association, VESA) y la Interconexión de componentes periféricos (Peripheral Component Interconnect, PCI).

La memoria 606 puede incluir, por ejemplo, una caché 612, tal como una caché compartida, que puede estar acoplada a las cachés locales 614 de los procesadores 604. Además, la memoria 606 puede incluir uno o más programas o aplicaciones 616, al menos un sistema operativo 618 y una o más instrucciones de programa legibles por ordenador 620. Las instrucciones de programa legibles por ordenador 620 pueden ser configuradas para llevar a cabo funciones de realizaciones de aspectos de la invención.

En una realización, la memoria 606 (por ejemplo, al menos un área del sistema de hardware de la memoria 606) se acopla a uno o más procesadores adjuntos 621 a través de uno o más buses de procesador adjunto 623, y en una o más realizaciones a través de una capa de transporte de AP.

El sistema informático 602 puede comunicarse a través de, por ejemplo, interfaces de E/S 608 con uno o más dispositivos externos 630, tales como un terminal de usuario, una unidad de cinta, un dispositivo señalador, una pantalla y uno o más dispositivos de almacenamiento de datos 634, etc. Un dispositivo de almacenamiento de datos 634 puede almacenar uno o más programas 636, una o más instrucciones de programa legibles por ordenador 638 y/o datos, etc. Las instrucciones de programa legibles por ordenador pueden ser configuradas para llevar a cabo funciones de realizaciones de aspectos de la invención.

El sistema informático 602 también puede comunicarse a través de, por ejemplo, interfaces de E/S 608 con la interfaz de red 632, lo que permite que el sistema informático 602 se comunique con una o más redes, tales como una red de área local (Local Area Network, LAN), una red de área amplia general (Wide Area Network, WAN) y/o una red pública (por ejemplo, Internet), proporcionando comunicación con otros dispositivos o sistemas informáticos.

El sistema informático 602 puede incluir y/o estar acoplado a medios de almacenamiento del sistema informático, volátiles/no volátiles, extraíbles/no extraíbles. Por ejemplo, puede incluir y/o estar acoplado a un medio magnético no extraíble y no volátil (habitualmente denominado "disco duro"), una unidad de disco magnético para leer y escribir en un disco magnético extraíble y no volátil (por ejemplo, un "disquete") y/o una unidad de disco óptico para leer o escribir en un disco óptico extraíble y no volátil, tal como un CD-ROM, un DVD-ROM u otros medios ópticos. Se debe comprender que otros componentes de hardware y/o software podrían ser utilizados junto con el sistema informático 602. Ejemplos incluyen, entre otros: microcódigo, controladores de dispositivo, unidades de procesamiento redundantes, matrices de unidades de disco externo, sistemas RAID, unidades de cinta y sistemas de almacenamiento de archivado de datos, etc.

El sistema informático 602 puede funcionar con otros numerosos entornos o configuraciones de sistemas informáticos de propósito general o de propósito especial. Ejemplos de sistemas informáticos, entornos y/o configuraciones conocidos que pueden ser adecuados para ser utilizados con el sistema informático 602 incluyen, entre otros, sistemas de ordenadores personales (Personal Computers, PC), sistemas informáticos de servidor, clientes ligeros, clientes pesados, dispositivos portátiles o de mano, sistemas basados en multiprocesador, sistemas basados en microprocesador, decodificadores de TV, productos electrónicos programables para el consumidor, ordenadores de red, sistemas de miniordenador, sistemas informáticos de ordenador central y entornos informáticos distribuidos en la nube que incluyen cualquiera de los sistemas o dispositivos anteriores, y similares.

Otro ejemplo de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención se describe haciendo referencia a la figura 6B. Como ejemplo, el entorno informático de la figura 6B puede estar basado en arquitectura de hardware z/Architecture®, comercializada por la firma International Business Machines Corporation. Sin embargo, la arquitectura de hardware z/Architecture es solo un ejemplo de arquitectura. De nuevo, el entorno informático puede estar basado también en otras arquitecturas, que incluyen, entre otros, las arquitecturas Intel® x86, otras arquitecturas comercializadas por la firma International Business Machines Corporation y/o arquitecturas comercializadas por otras firmas.

En un ejemplo, un entorno informático 650 incluye un complejo electrónico central (Central Electronics Complex, CEC) 652. CEC 652 incluye una pluralidad de componentes, tales como, por ejemplo, una memoria 654 (también conocida como memoria del sistema, memoria principal, almacenamiento principal, almacenamiento central, almacenamiento) acoplada a uno o más procesadores (también conocidos como unidades centrales de procesamiento (CPU)) 656 y a un subsistema de entrada/salida (E/S) 658. En una realización, la memoria 654 (por ejemplo, al menos un área de sistema de hardware de la memoria 654) se acopla a uno o más procesadores adjuntos 657 a través de uno o más buses de procesador adjunto, y en una o más realizaciones a través de una capa de transporte de AP.

El subsistema de E/S 658 puede formar parte del complejo electrónico central o estar separado del mismo. Dirige el flujo de información entre el almacenamiento principal 654 y las unidades de control de entrada/salida 660 y los dispositivos de entrada/salida (E/S) 662 acoplados al complejo electrónico central.

Se pueden utilizar muchos tipos de dispositivos de E/S. Un tipo particular es un dispositivo de almacenamiento de datos 664. El dispositivo de almacenamiento de datos 664 puede almacenar uno o más programas 666, una o más instrucciones de programa legibles por ordenador 668 y/o datos, etc. Las instrucciones de programa legibles por ordenador pueden ser configuradas para llevar a cabo funciones de realizaciones de aspectos de la invención.

El complejo electrónico central 652 puede incluir y/o estar acoplado a medios de almacenamiento del sistema informático, volátiles/no volátiles, extraíbles/no extraíbles. Por ejemplo, puede incluir y/o estar acoplado a un medio magnético no extraíble y no volátil (habitualmente denominado "disco duro"), una unidad de disco magnético para leer y escribir en un disco magnético extraíble y no volátil (por ejemplo, un "disquete") y/o una unidad de disco óptico para leer o escribir en un disco óptico extraíble y no volátil, tal como un CD-ROM, un DVD-ROM u otros medios ópticos. Se debe comprender que se podrían utilizar otros componentes de hardware y/o software junto con el complejo electrónico central 652. Ejemplos incluyen, entre otros: microcódigo, controladores de dispositivo, unidades de procesamiento

redundantes, matrices de unidades de disco externo, sistemas RAID, unidades de cinta y sistemas de almacenamiento de archivado de datos, etc.

Además, el complejo electrónico central 652 puede funcionar con muchos otros entornos o configuraciones de sistema informático de propósito general o de propósito especial. Ejemplos de sistemas informáticos, entornos y/o configuraciones bien conocidos que pueden ser adecuados para su uso con el complejo electrónico central 652 incluyen, entre otros, sistemas de ordenadores personales (PC), sistemas informáticos de servidores, clientes ligeros, clientes pesados, dispositivos de mano o portátiles, sistemas de multiprocesadores, sistemas basados en microprocesadores, decodificadores, productos electrónicos de consumo programables, PC en red, sistemas de miniordenadores, sistemas informáticos centralizados y entornos informáticos distribuidos en la nube que incluyen cualquiera de los sistemas o dispositivos anteriores, y similares.

El complejo electrónico central 652 proporciona, en una o más realizaciones, particionamiento lógico y/o soporte de virtualización. En una realización, como se muestra en la figura 6C, la memoria 654 incluye, por ejemplo, una o más particiones lógicas 670, un hipervisor 672 que gestiona las particiones lógicas, y el firmware 674 del procesador. Un ejemplo de hipervisor 672 es el Processor Resource/System Manager (PR/SM™), comercializado por la firma International Business Machines Corporation, Armonk, Nueva York. Tal como se utiliza en la presente memoria descriptiva, el firmware incluye, por ejemplo, el microcódigo del procesador. Incluye, por ejemplo, las instrucciones a nivel de hardware y/o las estructuras de datos usadas en la implementación del código máquina de nivel superior. En una realización, incluye, por ejemplo, código patentado que habitualmente se suministra como microcódigo que incluye software fiable, o microcódigo específico para el hardware subyacente, y controla el acceso del sistema operativo al hardware del sistema.

Cada partición lógica 670 es capaz de funcionar como un sistema independiente. Es decir, cada partición lógica se puede reiniciar de manera independiente, ejecutar un sistema operativo huésped 676, tal como el sistema operativo z/OS®, comercializado por la firma International Business Machines Corporation, Armonk, Nueva York, u otro código de control 678, tal como el código de control de funcionalidad de acoplamiento (Coupling Facility Control Code, CFCC), y funcionar con diferentes programas 680. Un sistema operativo o un programa de aplicación que se ejecuta en una partición lógica parece tener acceso a un sistema entero y completo, pero en realidad solo una parte del mismo está disponible. Aunque z/OS se ofrece como ejemplo, se pueden utilizar otros sistemas operativos según uno o más aspectos de la presente invención.

La memoria 654 está acoplada a las CPU 656 (figura 6B), que son recursos de procesador físico que pueden asignarse a las particiones lógicas. Por ejemplo, una partición lógica 670 incluye uno o más procesadores lógicos, cada uno de los cuales representa la totalidad o una parte de un recurso físico del procesador 656 que puede ser asignado dinámicamente a la partición lógica.

En otra realización más, el complejo electrónico central proporciona soporte para máquinas virtuales (con o sin soporte de particionamiento lógico). Como se muestra en la figura 6D, la memoria 654 del complejo electrónico central 652 incluye, por ejemplo, una o más máquinas virtuales 690, un gestor de máquinas virtuales, tal como un hipervisor 692, que administra las máquinas virtuales, y el firmware del procesador 694. Un ejemplo de hipervisor 692 es el hipervisor z/VM®, comercializado por la firma International Business Machines Corporation, Armonk, Nueva York. El hipervisor algunas veces se denomina ordenador central. z/OS y z/VM, son marcas comerciales o marcas comerciales registradas de la firma International Business Machines Corporation en al menos una jurisdicción.

El soporte de máquina virtual del CPC proporciona la capacidad de operar un gran número de máquinas virtuales 690, cada una capaz de funcionar con diferentes programas 696 y ejecutar un sistema operativo huésped 698, tal como el sistema operativo Linux®. Cada máquina virtual 690 es capaz de funcionar como un sistema separado. Es decir, cada máquina virtual se puede reiniciar de manera independiente, ejecutar un sistema operativo huésped y operar con diferentes programas. Un sistema operativo o un programa de aplicación que se ejecuta en una máquina virtual parece tener acceso a un sistema total y completo, pero en realidad solo una parte de él está disponible. Aunque z/VM y Linux se ofrecen como ejemplos, se pueden usar otros gestores de máquinas virtuales y/o sistemas operativos según uno o más aspectos de la presente invención. La marca registrada Linux® se usa de conformidad con una sublicencia de la Fundación Linux, la licenciataria exclusiva de Linus Torvalds, propietario de la marca en todo el mundo.

Otra realización de un entorno informático para incorporar y utilizar uno o más aspectos de la presente invención se describe haciendo referencia a la figura 7A. En este ejemplo, un entorno informático 10 incluye, por ejemplo, una unidad central de procesamiento (CPU) nativa 12, una memoria 14 y uno o más dispositivos y/o interfaces de entrada/salida 16 acoplados entre sí mediante, por ejemplo, uno o más buses 18 y/u otras conexiones. Como ejemplos, el entorno informático 10 puede incluir un procesador PowerPC® comercializado por la firma International Business Machines Corporation, Armonk, Nueva York; un HP Superdome con procesadores Intel Itanium II comercializados por la firma Hewlett Packard Co., Palo Alto, California; y/u otras máquinas basadas en arquitecturas comercializadas por la firma International Business Machines Corporation, Hewlett Packard, Intel Corporation, Oracle u otros. PowerPC es una marca comercial o marca comercial registrada comercializada por la firma International Business Machines Corporation en al menos una jurisdicción. Intel e Itanium son marcas comerciales o marcas comerciales registradas de Intel Corporation o sus subsidiarias en los Estados Unidos y en otros países.

La unidad central de procesamiento nativa 12 incluye uno o más registros nativos 20, tales como uno o más registros de propósito general y/o uno o más registros de propósito especial utilizados durante el procesamiento dentro del entorno. Estos registros incluyen información que representa el estado del entorno en cualquier punto particular del tiempo.

Además, la unidad central de procesamiento nativa 12 ejecuta instrucciones y código que están almacenados en la memoria 14. En un ejemplo particular, la unidad central de procesamiento ejecuta el código de emulador 22 almacenado en la memoria 14. Este código permite al entorno informático configurado en una arquitectura emular otra arquitectura. Por ejemplo, el código de emulador 22 permite a máquinas basadas en arquitecturas diferentes de la arquitectura de hardware z/Architecture, tales como los procesadores PowerPC, los servidores Superdome HP u otros, emular la arquitectura de hardware z/Architecture y ejecutar el software y las instrucciones desarrolladas basadas en la arquitectura de hardware z/Architecture.

Haciendo referencia a la figura 7B se describen detalles adicionales relacionados con el código de emulador 22. Las instrucciones de huésped 30 almacenadas en la memoria 14 comprenden instrucciones de software (por ejemplo, que se correlacionan con instrucciones de máquina) que fueron desarrolladas para ser ejecutadas en una arquitectura distinta a la de la CPU nativa 12. Por ejemplo, las instrucciones de huésped 30 pueden haber sido diseñadas para ejecutarse en un procesador basado en la arquitectura de hardware z/Architecture, pero en cambio, están siendo emuladas en la CPU nativa 12, que puede ser, por ejemplo, un procesador Intel Itanium II. En un ejemplo, el código de emulador 22 incluye una rutina de búsqueda de instrucciones 32 para obtener una o más instrucciones de huésped 30 de la memoria 14 y, opcionalmente, proporcionar almacenamiento en memoria intermedia local para las instrucciones obtenidas. También incluye una rutina de traducción de instrucciones 34 para determinar el tipo de instrucción de huésped que se ha obtenido y para traducir la instrucción de huésped en una o más instrucciones nativas 36 correspondientes. Esta traducción incluye, por ejemplo, identificar la función que realizará la instrucción de huésped y elegir la instrucción o instrucciones nativas para realizar esa función.

Además, el código de emulador 22 incluye una rutina de control de emulación 40 para hacer que se ejecuten las instrucciones nativas. La rutina de control de emulación 40 puede hacer que la CPU nativa 12 ejecute una rutina de instrucciones nativas que emulen una o más instrucciones de huésped obtenidas previamente y, al concluir dicha ejecución, devuelva el control a la rutina de búsqueda de instrucciones para emular la obtención de la siguiente instrucción de huésped o de un grupo de instrucciones de huésped. La ejecución de las instrucciones nativas 36 puede incluir cargar datos en un registro desde la memoria 14; almacenar datos de vuelta a la memoria desde un registro; o realizar algún tipo de operación aritmética o lógica, según lo determinado por la rutina de traducción.

Cada rutina se implementa, por ejemplo, en un software, que se almacena en la memoria y se ejecuta mediante la unidad central de procesamiento nativa 12. En otros ejemplos, una o más de las rutinas u operaciones se implementan en firmware, hardware, software o alguna combinación de los mismos. Los registros del procesador emulado pueden ser emulados utilizando los registros 20 de la CPU nativa o utilizando ubicaciones en la memoria 14. En realizaciones, las instrucciones de huésped 30, las instrucciones nativas 36 y el código de emulador 22 pueden residir en la misma memoria o pueden estar distribuidas entre diferentes dispositivos de memoria.

Además, en una realización, el entorno informático 10 incluye uno o más procesadores adjuntos 15 acoplados a la memoria 14. El uno o más procesadores adjuntos están definidos en una arquitectura y se configuran para emular otra arquitectura. Por ejemplo, un procesador adjunto obtiene los comandos de huésped de la arquitectura que se está emulando, traduce los comandos de huésped en comandos nativos de la arquitectura y ejecuta los comandos nativos.

Los entornos informáticos descritos anteriormente son solo ejemplos de entornos informáticos que se pueden utilizar. Se pueden utilizar otros entornos, que incluyen, entre otros, entornos no particionados, entornos particionados, entornos informáticos y/o entornos emulados; las realizaciones no están limitadas a ningún entorno. Aunque en la presente memoria se describen diversos ejemplos de entornos informáticos, uno o más aspectos de la presente invención se pueden utilizar con muchos tipos de entornos. Los entornos informáticos proporcionados en la presente memoria son solo ejemplos.

Cada entorno informático puede ser configurado para incluir uno o más aspectos de la presente invención. Por ejemplo, cada uno puede ser configurado para realizar filtrado por cada comando, según uno o más aspectos de la presente invención.

Como se describe en el presente documento, en uno o más aspectos, se proporciona un filtrado del tipo de comando por cada comando. Se pueden utilizar muchas técnicas de filtrado, incluidas muchas técnicas de filtrado del tipo de comando. En una realización particular, se da a conocer un filtrado del tipo de comando sin estado. Con este filtrado, en un ejemplo, si la función de filtrado de comandos sin estado se configura, por ejemplo, en cero, entonces la función de filtrado de comandos sin estado no se instala y el procesador adjunto (por ejemplo, la tarjeta cripto) permite que se ejecuten los comandos que son compatibles con el procesador adjunto; de lo contrario, la función de filtrado de comandos sin estado se instala y, el que un comando sea ejecutado por el procesador adjunto depende, al menos, del valor del conjunto de indicadores de filtrado del tipo de comando impuestos por el hipervisor en una solicitud de comando. A continuación se describe un ejemplo de realización que incluye un indicador del tipo de comando sin estado en el mensaje de solicitud de comando:

Si el indicador del tipo de comando sin estado (por ejemplo, el indicador 322) está puesto a cero en el mensaje de solicitud de comando (por ejemplo, el mensaje 300), la tarjeta cripto permite ejecutar todos los comandos admitidos por la tarjeta criptográfica Si el indicador del tipo de comando sin estado (por ejemplo, el indicador 322) está puesto a cero en el mensaje de solicitud de comando (por ejemplo, el mensaje 300), la tarjeta cripto permite ejecutar todos los comandos admitidos por la tarjeta criptográfica Si el comando del mensaje de solicitud de comando es un comando del tipo de comando sin estado, se ejecuta el comando. Si el comando del mensaje de solicitud de comando no es un comando de tipo comando sin estado, entonces el comando se rechaza con un código de error en el CPRB (por ejemplo, la respuesta CPRB 336) del mensaje de respuesta del comando (por ejemplo, el mensaje 330).

En uno o más aspectos, el modo configurado de la tarjeta cripto (por ejemplo, el modo de coprocesador) se puede utilizar para proporcionar el filtrado de comandos sin estado (también denominado modo de filtrado de claves no seguras; por ejemplo, solo se procesan los comandos del tipo de comando sin estado) u otro modo de filtrado con un conjunto reducido de comandos sin configurar la tarjeta cripto en un nuevo modo de tarjeta cripto, como, por ejemplo, el modo de acelerador. La técnica de filtrado se puede utilizar para filtrar un conjunto de comandos de tipo comando, tales como comandos del tipo de comando sin estado u otros comandos del tipo de comando en otros ejemplos, tales como comandos de gestión de claves principales, etc. Esto reduce la cantidad de procesadores adjuntos que se deben comprar y gestionar.

Además, uno o más aspectos de la invención proporcionan la capacidad de cambiar el modo de filtrado dinámicamente para cada comando; el filtrado del tipo de comando se realiza por cada comando. Por lo tanto, cada comando puede ser válido o no válido en el momento del procesamiento de los comandos en función de los valores de los indicadores del tipo de comando (por ejemplo, indicadores de filtrado de tipo de comando). El programa no tiene que cambiar entre diversos modos de tarjeta cripto para ejecutar diferentes conjuntos de comandos de filtrado. Por lo tanto, la complejidad de gestionar y utilizar la cantidad de tarjetas cripto sigue siendo la misma independientemente de la cantidad de modos de filtrado compatibles. La reducción de la complejidad del programa también contribuye a un código más eficiente y mejora el tiempo de ejecución y el rendimiento del código.

En otra realización, para proporcionar la funcionalidad de filtrado, se utiliza una lista de códigos de comando o mnemónicos reales, junto con sus códigos de función o mnemónicos para comunicar los códigos de comando compatibles y/o sus códigos de función.

Aunque en el presente documento se describen diversas realizaciones, son posibles muchas variaciones y otras realizaciones sin apartarse del alcance de la presente invención. Cabe señalar que, salvo incoherencia, cada aspecto o característica descrita en la presente memoria, y variantes de los mismos, pueden ser combinados con cualquier otro aspecto o característica.

Uno o más aspectos pueden estar relacionados con la informática en la nube.

Se debe comprender que, aunque esta descripción incluye una descripción detallada de la informática en la nube, la implementación de las explicaciones mencionadas en la presente memoria no está limitada a un entorno informático en la nube. Más bien, las realizaciones de la presente invención son capaces de ser implementadas junto con cualquier otro tipo de entorno informático conocido actualmente o desarrollado posteriormente.

La informática en la nube es un modelo de prestación de servicios para permitir un acceso de red cómodo y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, ancho de banda de red, servidores, procesamiento, memoria, almacenamiento, aplicaciones, máquinas virtuales y servicios) que se pueden aprovisionar y lanzar rápidamente con un mínimo esfuerzo de gestión o interacción con un proveedor del servicio. Este modelo en la nube puede incluir al menos cinco características, al menos tres modelos de servicio y al menos cuatro modelos de implementación.

Las características son como sigue:

Autoservicio bajo demanda: Un consumidor en la nube puede aprovisionar capacidades informáticas de unilateralmente, tales como tiempo de servidor y almacenamiento en red, según sea necesario automáticamente, sin requerir interacción humana con el proveedor del servicio.

Acceso a red ancha: las capacidades están disponibles sobre una red y se accede a ellas a través de mecanismos estándar que favorecen la utilización por parte de plataformas heterogéneas de clientes ligeros o pesados (por ejemplo, teléfonos móviles, ordenadores portátiles y PDA).

Agrupación de recursos: los recursos informáticos del proveedor se agrupan para servir a múltiples consumidores utilizando un modelo de múltiples inquilinos, con diferentes recursos físicos y virtuales asignados dinámicamente y reasignados según la demanda. Hay un sentido de independencia de ubicación en el sentido de que el consumidor generalmente no tiene control ni conocimiento sobre la ubicación exacta de los recursos proporcionados, pero puede ser capaz de especificar la ubicación en un nivel de abstracción superior (por ejemplo, país, estado o centro de datos).

Elasticidad rápida: las capacidades se pueden aprovisionar rápida y elásticamente, en algunos casos de manera automática, para ampliar y liberar rápidamente para reducir rápidamente. Para el consumidor, las capacidades disponibles para el aprovisionamiento a menudo parecen ilimitadas y pueden ser adquiridas en cualquier cantidad en cualquier momento.

Servicio medido: los sistemas en la nube controlan y optimizan automáticamente el uso de los recursos al aprovechar una capacidad de medición en algún nivel de abstracción apropiado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de recursos se puede monitorizar, controlar e informar, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Los modelos de servicio son como sigue:

Software como servicio (Software as a Service, SaaS): La capacidad proporcionada al consumidor es para utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Las aplicaciones son accesibles desde diversos dispositivos cliente a través de una interfaz de cliente ligero, tal como un navegador web (por ejemplo, correo electrónico basado en web). El consumidor no gestiona ni controla la infraestructura en la nube subyacente, incluidas la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de aplicaciones individuales, con la posible excepción de ajustes limitados de configuración de aplicaciones específicas del usuario.

Plataforma como servicio (Platform as a Service, PaaS): la capacidad proporcionada al consumidor es para desplegar en la infraestructura en la nube aplicaciones creadas o adquiridas por el consumidor, creadas usando lenguajes de programación y herramientas soportadas por el proveedor. El consumidor no gestiona ni controla la infraestructura en la nube subyacente incluidas las redes, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones desplegadas y, posiblemente, las configuraciones del entorno del alojamiento de aplicaciones.

Infraestructura como servicio (Infrastructure as a Service, Infrastructure as a Service, IaaS): la capacidad proporcionada al consumidor es para aprovisionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor es capaz de implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura en la nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento, las aplicaciones implementadas y, posiblemente, un control limitado de los componentes de interconexión de redes seleccionados (por ejemplo, los cortafuegos del ordenador central).

Los modelos de despliegue son como sigue:

Nube privada: la infraestructura en la nube opera solamente para una organización. La pueden gestionar la organización o un tercero y puede existir en las instalaciones o fuera de las instalaciones.

Nube comunitaria: la infraestructura en la nube es compartida por varias organizaciones y soporta una comunidad específica que tiene intereses compartidos (por ejemplo, misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser gestionada por parte de las organizaciones o por un tercero, y puede existir en las instalaciones o fuera de las instalaciones.

Nube pública: La infraestructura en la nube es puesta a disposición del público en general o de un gran grupo industrial y es propiedad de una organización que vende servicios en la nube.

Nube híbrida: la infraestructura en la nube es una composición de dos o más nubes (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas entre sí por una tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones (por ejemplo, la ráfaga en la nube para equilibrar la carga entre nubes).

Un entorno informático en la nube está orientado a servicio con un enfoque en ausencia de estado, bajo acoplamiento, modularidad e interoperabilidad semántica. En el corazón de la informática en la nube hay una infraestructura que incluye una red de nodos interconectados.

Haciendo referencia a continuación a la figura 8, se representa un entorno informático en la nube 50 ilustrativo. Como se muestra, el entorno informático 50 en la nube incluye uno o más nodos informáticos 52 en la nube con los que se pueden comunicar los dispositivos informáticos locales utilizados por los consumidores de la nube, tales como, por ejemplo, un asistente digital personal (Personal Digital Assistant, PDA) o un teléfono celular 54A, un ordenador de sobremesa 54B, un ordenador portátil 54C y/o el sistema informático de automóvil 54N. Los nodos 52 pueden comunicarse entre sí. Se pueden agrupar (no mostrado) física o virtualmente, en una o más redes, tales como nubes privadas, comunitarias, públicas o híbridas, como se ha descrito anteriormente, o en una combinación de las mismas. Esto permite que el entorno informático en la nube 50 ofrezca infraestructura, plataformas y/o software como servicios para los que un consumidor en la nube no necesita mantener recursos en un dispositivo informático local. Se entiende que los tipos de dispositivos informáticos 54A-N que se muestran en la figura 8 pretenden ser solo ilustrativos y que los nodos informáticos 52 y el entorno informático en la nube 50 pueden comunicarse con cualquier tipo de dispositivo informático a través de cualquier tipo de red y/o conexión direccionable por red (por ejemplo, utilizando un navegador web).

Haciendo referencia a continuación a la figura 9, se muestran un conjunto de capas de abstracción funcionales proporcionadas por el entorno informático en la nube 50 (figura 8). Se debe comprender de antemano que los componentes, capas y funciones mostrados en la figura 9 son solamente ilustrativos y las realizaciones de la invención no están limitadas a los mismos. Como se representa, están dispuestas las siguientes capas y funciones correspondientes:

La capa de hardware y software 60 incluye componentes de hardware y software. Ejemplos de componentes de hardware incluyen: ordenadores centrales 61; servidores basados en arquitectura RISC (Reduced Instruction Set Computer) 62; servidores 63; servidores blade 64; dispositivos de almacenamiento 65; y redes y componentes de red 66. En algunas realizaciones, los componentes de software incluyen software de servidor de aplicaciones de red 67 y el software de base de datos 68.

La capa de virtualización 70 proporciona una capa de abstracción a partir de la que se pueden proporcionar los siguientes ejemplos de entidades virtuales: servidores virtuales 71; almacenamiento virtual 72; redes virtuales 73, que incluyen redes privadas virtuales; aplicaciones virtuales y sistemas operativos 74; y clientes virtuales 75.

En un ejemplo, la capa de gestión 80 puede proporcionar las funciones descritas a continuación. El aprovisionamiento de recursos 81 proporciona una obtención dinámica de recursos informáticos y de otros recursos que se utilizan para realizar tareas dentro del entorno informático en la nube. La Medición y Fijación de Precios 82 proporcionan un seguimiento de los costes a medida que se utilizan los recursos dentro del entorno informático en la nube, y el cobro o facturación por el consumo de estos recursos. En un ejemplo, estos recursos pueden incluir licencias de software de aplicaciones. La seguridad proporciona comprobación de identidad para los consumidores y las tareas en la nube, así como protección para los datos y otros recursos. El portal de usuario 83 proporciona acceso al entorno informático en la nube para consumidores y administradores de sistemas. La gestión de nivel de servicio 84 proporciona la asignación y gestión de recursos informáticos en la nube de tal manera que se cumplen los niveles de servicio requeridos. La planificación y cumplimiento de Acuerdos de Nivel de Servicio (Service Level Agreement, SLA) 85 proporciona el preacuerdo para, y la contratación de, los recursos de informáticos en nube para los que se anticipa un requisito futuro según un SLA.

La capa de cargas de trabajo 90 proporciona ejemplos de funcionalidad para lo cual se puede utilizar el entorno informático en la nube. Ejemplos de cargas de trabajo y funciones que se pueden proporcionar desde esta capa incluyen: mapeo y navegación 91; desarrollo de software y gestión del ciclo de vida 92; distribución de educación en el aula virtual 93; procesamiento de analíticas de datos 94; procesamiento de transacciones 95; y procesamiento de filtrado del tipo de comando 96.

Aspectos de la presente invención puede ser un sistema, un método y/o un producto de programa informático en cualquier posible nivel de detalle técnico de integración. El producto de programa informático puede incluir un medio (o medios) de almacenamiento legible por ordenador que tiene instrucciones de programa legibles por ordenador en el mismo para hacer que un procesador lleve a cabo aspectos de la presente invención.

El medio de almacenamiento legible por ordenador puede ser un dispositivo tangible que puede retener y almacenar instrucciones para su uso por un dispositivo de ejecución de instrucciones. El medio de almacenamiento legible por ordenador puede ser, por ejemplo, entre otros, un dispositivo de almacenamiento electrónico, un dispositivo de almacenamiento magnético, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento electromagnético, un dispositivo de almacenamiento semiconductor o cualquier combinación adecuada de los anteriores. Una lista no exhaustiva de ejemplos más específicos del medio de almacenamiento legible por ordenador incluye lo siguiente: un disquete de ordenador portátil, un disco duro, una memoria de acceso aleatorio (Random Access Memory, RAM), una memoria de solo lectura (Read Only Memory, ROM), una memoria de solo lectura programable y borrable (Erasable Programmable Read-Only Memory, EPROM o memoria Flash), una memoria de acceso aleatorio estática (Static RAM, SRAM), una memoria de solo lectura de disco compacto portátil (Compact Disc-ROM, CD-ROM), un disco versátil digital (Digital Versatile Disk, DVD), una memoria USB, un disquete, un dispositivo codificado mecánicamente tal como tarjetas perforadas o estructuras elevadas en una ranura que tienen instrucciones grabadas en ellas, y cualquier combinación adecuada de los anteriores. Un medio de almacenamiento legible por ordenador, tal como se utiliza en la presente memoria, no debe ser interpretado como señales transitorias en sí, tales como ondas de radio u otras ondas electromagnéticas que se propagan libremente, ondas electromagnéticas que se propagan a través de una guía de ondas u otro medio de transmisión (por ejemplo, pulsos de luz que pasan a través de un cable de fibra óptica) o señales eléctricas transmitidas a través de un cable.

Las instrucciones de programa legibles por ordenador descritas en la presente memoria pueden descargarse en los respectivos dispositivos informáticos/de procesamiento desde un medio de almacenamiento legible por ordenador o a un ordenador externo o dispositivo de almacenamiento externo a través de una red, por ejemplo, Internet, una red de área local, una red de área amplia y/o una red inalámbrica. La red puede comprender cables de transmisión de cobre, fibras de transmisión óptica, transmisión inalámbrica, enrutadores, cortafuegos, conmutadores, ordenadores de puerta de enlace y/o servidores periféricos. Una tarjeta de adaptador de red o interfaz de red en cada dispositivo informático/de procesamiento recibe instrucciones de programa legibles por ordenador desde la red y reenvía las instrucciones de programa legibles por ordenador para su almacenamiento en un medio de almacenamiento legible por ordenador dentro del dispositivo informático/de procesamiento respectivo.

Las instrucciones de programa legibles por ordenador para llevar a cabo las operaciones de la presente invención pueden ser instrucciones de ensamblador, instrucciones de arquitectura de conjunto de instrucciones (ISA), instrucciones de máquina, instrucciones dependientes de máquina, microcódigo, instrucciones de firmware, datos de ajuste de estado, datos de configuración para circuito integrado o código fuente o código objeto escritos en cualquier combinación de uno o más lenguajes de programación, incluido un lenguaje de programación orientado a objetos tal como Smalltalk, C++ o similares, y lenguajes de programación procedimentales, como el lenguaje de programación "C" o lenguajes de programación similares. Las instrucciones de programa legibles por ordenador pueden ejecutarse completamente en el ordenador del usuario, parcialmente en el ordenador del usuario, como un paquete de software independiente, parcialmente en el ordenador del usuario y parcialmente en un ordenador remoto o completamente en el ordenador remoto o servidor. En este último escenario, el ordenador remoto puede conectarse al ordenador del usuario a través de cualquier tipo de red, que incluye una red de área local (LAN) o una red de área amplia (WAN), o la conexión puede realizarse a un ordenador externo (por ejemplo, a través de Internet usando un Proveedor de Servicios de Internet). En algunas realizaciones, los circuitos electrónicos incluyen, por ejemplo, circuitos lógicos programables, matrices de puertas programables en campo (Field-Programmable Gate Arrays, FPGA) o matrices lógicas programables (Programmable Logic Arrays, PLA) que pueden ejecutar instrucciones de programa legibles por ordenador utilizando información de estado de las instrucciones de programa legibles por ordenador para personalizar los circuitos electrónicos, con el fin de realizar aspectos de la presente invención.

Aspectos de la presente invención se describen en el presente documento haciendo referencia a ilustraciones de diagramas de flujo y/o diagramas de bloques de métodos, aparatos (sistemas) y productos de programas informáticos, según las realizaciones de la invención. Se comprenderá que cada bloque de las ilustraciones de diagrama de flujo y/o diagramas de bloques, y las combinaciones de bloques en las ilustraciones de diagrama de flujo y/o diagramas de bloques, pueden ser implementados mediante instrucciones de programa legibles por ordenador.

Estas instrucciones de programa legibles por ordenador pueden ser proporcionadas a un procesador de un ordenador, u otro aparato de procesamiento de datos programable para producir una máquina, de tal manera que las instrucciones, que se ejecutan a través del procesador del ordenador u otro aparato programable de procesamiento de datos, crean medios para implementar las funciones/acciones especificadas en el bloque o bloques del diagrama de flujo y/o diagrama de bloques. Estas instrucciones de programa legibles por ordenador también pueden almacenarse en un medio de almacenamiento legible por ordenador que puede dirigir un ordenador, un aparato de procesamiento de datos programable y/u otros dispositivos para que funcionen de una manera particular, de tal manera que el medio de almacenamiento legible por ordenador que tiene instrucciones almacenadas en el mismo comprende un artículo de fabricación, que incluye instrucciones que implementan aspectos de la función/acciones especificadas en el bloque o bloques en el diagrama de flujo y/o diagrama de bloques.

Las instrucciones de programa legibles por ordenador también pueden ser cargadas en un ordenador, otro aparato de procesamiento de datos programable u otro dispositivo para hacer que se realicen una serie de etapas operativas en el ordenador, en otro aparato programable o en otro dispositivo para producir un proceso implementado por ordenador, de tal manera que las instrucciones que se ejecutan en el ordenador, en otro aparato programable o en otro dispositivo implementan las funciones/acciones especificadas en el diagrama de flujo y/o diagrama de bloques, bloque o bloques.

El diagrama de flujo y los diagramas de bloques de las Figuras ilustran la arquitectura, la funcionalidad y la operación de posibles implementaciones de sistemas, métodos y productos de programas informáticos según varias realizaciones de la presente invención. A este respecto, cada bloque en el diagrama de flujo o los diagramas de bloques puede representar un módulo, un segmento o una parte de instrucciones, que comprende una o más instrucciones ejecutables para implementar la función o funciones lógicas especificadas. En algunas implementaciones alternativas, las funciones indicadas en los bloques pueden ocurrir fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ser realizados como una sola etapa, ejecutados concurrentemente, sustancialmente concurrentes, de manera parcial o totalmente superpuesta temporalmente, o los bloques pueden a veces ser ejecutados en el orden inverso, dependiendo de la funcionalidad implicada. También cabe señalar que cada bloque de los diagramas de bloques y/o la ilustración del diagrama de flujo, y las combinaciones de bloques en los diagramas de bloques y/o la ilustración del diagrama de flujo, pueden implementarse mediante sistemas basados en hardware de propósito especial que realizan las funciones o actos especificados o llevan a cabo combinaciones de hardware de propósito especial e instrucciones informáticas.

Además de lo anterior, un proveedor de servicios que ofrezca la gestión de entornos de cliente puede proporcionar, ofrecer, desplegar, gestionar, atender, etc., uno o más aspectos. Por ejemplo, el proveedor de servicios puede crear, mantener, soportar, etc. un código informático y/o una infraestructura informática que realice uno o más aspectos para uno o más clientes. A cambio, el proveedor de servicios puede recibir el pago del cliente bajo una suscripción y/o un acuerdo de tarifa, como ejemplos. Adicional o alternativamente, el proveedor de servicios puede recibir el pago de la venta de contenido publicitario a uno o más terceros.

En un aspecto, se puede desplegar una aplicación para realizar una o más realizaciones. Como ejemplo, la implementación de una aplicación comprende proporcionar una infraestructura informática operable para realizar una o más realizaciones.

Como aspecto adicional, se puede desplegar una infraestructura informática que comprende integrar un código legible por ordenador en un sistema informático, en el que el código en combinación con el sistema informático es capaz de realizar una o más realizaciones.

Como un aspecto adicional más, se puede proporcionar un proceso para integrar una infraestructura informática que comprende integrar un código legible por ordenador en un sistema informático. El sistema informático comprende un medio legible por ordenador, donde el medio informático comprende una o más realizaciones. El código, en combinación con el sistema informático, es capaz de realizar una o más realizaciones.

Aunque anteriormente se han descrito diversas realizaciones, estas son solamente ejemplos. Por ejemplo, se pueden utilizar entornos informáticos de otras arquitecturas para incorporar y utilizar una o más realizaciones. Además, se pueden utilizar diferentes instrucciones u operaciones. Adicionalmente, se pueden especificar diferentes tipos de indicadores o marcadores. Son posibles muchas variaciones.

En la presente memoria se describen diversos aspectos. Además, son posibles muchas variaciones sin apartarse del alcance de la presente invención. Cabe señalar que, salvo incoherencia, cada aspecto o característica descrita en la presente memoria, y variantes de los mismos, pueden combinarse con cualquier otro aspecto o característica.

Además, otros tipos de entornos informáticos pueden beneficiarse y usarse. Como ejemplo, se puede utilizar un sistema de procesamiento de datos adecuado para almacenar y/o ejecutar código de programa que incluye al menos dos procesadores acoplados directa o indirectamente a elementos de memoria a través de un bus de sistema. Los elementos de memoria incluyen, por ejemplo, la memoria local empleada durante la ejecución real del código del programa, un almacenamiento masivo y una memoria caché que proporciona almacenamiento temporal de al menos parte del código del programa con el fin de reducir el número de veces que el código debe ser recuperado del almacenamiento masivo durante la ejecución.

Los dispositivos de entrada/salida (E/S)que incluyen, entre otros, teclados, pantallas, dispositivos señaladores, DASD, cintas, CD, DVD, memorias USB y otros medios de memoria, etc.) se pueden acoplar al sistema o bien directamente o a través de controladores de E/S intermedios. Los adaptadores de red también se pueden acoplar al sistema para permitir que el sistema de procesamiento de datos llegue a acoplarse a otros sistemas de procesamiento de datos o impresoras remotas o dispositivos de almacenamiento a través de redes privadas o públicas intermedias. Los módems, módems de cable y tarjetas Ethernet son tan solo algunos de los tipos de adaptadores de red disponibles.

La terminología usada en la presente memoria tiene el propósito de describir las realizaciones particulares solamente y no se pretende que sea limitante. Como se usa en la presente memoria, las formas singulares “un/una” y “el/la” pretenden incluir también las formas plurales, a menos que el contexto indique claramente lo contrario. Se comprenderá además que los términos "comprende" y/o "que comprende", cuando se usan en esta memoria descriptiva, especifican la presencia de características, enteros, etapas, operaciones, elementos y/o componentes indicados, pero no excluyen la presencia o adición de una o más características, enteros, etapas, operaciones, elementos, componentes y/o grupos de los mismos.

Las correspondientes estructuras, materiales, acciones y equivalentes de todos los medios o etapas más los elementos de función en las reivindicaciones siguientes, si los hay, se pretende que incluyan cualquier estructura, material o acción para realizar la función junto con otros elementos reivindicados, como se reivindica específicamente. La descripción de una o más realizaciones se ha presentado con propósitos de ilustración y descripción, pero no se pretende que sea exhaustiva o limitada a la forma dada a conocer. Muchas modificaciones y variaciones resultarán evidentes para los expertos en la materia. La realización se eligió y describió con el fin de explicar mejor diversos aspectos y la aplicación práctica, y para permitir que otros expertos en la materia comprendan diversas realizaciones con diversas modificaciones que sean adecuadas para el uso particular contemplado.

REIVINDICACIONES

1. Un producto de programa informático para facilitar el procesamiento dentro de un entorno informático, comprendiendo el producto de programa informático:

determinar dinámicamente (500), por un procesador adjunto (104, 156), si los comandos obtenidos por el procesador adjunto deben ser procesados por el procesador adjunto, realizándose la determinación dinámica por cada comando, y comprendiendo:

obtener (504), por el procesador adjunto, una solicitud de comando (300) de un solicitante, incluyendo la solicitud de comando al menos un indicador de filtrado (320) que indica al menos un tipo de comando válido para su procesamiento por parte del procesador adjunto, para el solicitante, indicando el al menos un tipo de comando válido como válido para el solicitante, basándose en uno o más tipos de comando permitidos para el solicitante;

determinar (508), por el procesador adjunto utilizando el al menos un indicador de filtrado, si un comando de la solicitud de comando es válido para su procesamiento por parte del procesador adjunto para el solicitante, incluyendo el al menos un indicador de filtrado un indicador del tipo de comando sin estado (322), en el que, basándose en que el indicador del tipo de comando sin estado está configurado en un valor, los comandos determinados como comandos del tipo de comando sin estado son válidos para su procesamiento por parte del procesador adjunto, para el solicitante, y otros comandos del tipo de comando no son válidos para su procesamiento por parte del procesador adjunto, para el solicitante; y

procesar el comando (510), por el procesador adjunto, basándose en la determinación de que el comando es válido para ser procesado por el procesador adjunto, para el solicitante.

2. El método implementado por ordenador de la reivindicación 1, en el que el procesador adjunto (104, 156) está configurado (512) en un modo y la determinación dinámica le permite funcionar de manera diferente que el modo en el que está configurado.

3. El método implementado por ordenador de la reivindicación 2, en el que el procesador adjunto (104, 156) configurado (514) en el modo único es capaz de procesar un conjunto de comandos, y en el que el procesador adjunto funciona de manera diferente (516) en que procesa un conjunto reducido del conjunto de comandos.

4. El método implementado por ordenador de la reivindicación 1, en el que el al menos un indicador de filtrado es configurado por cada comando (520).

5. El método implementado por ordenador de la reivindicación 4, en el que el al menos un indicador de filtrado es configurado basándose en una política informática correspondiente al solicitante de la solicitud de comando (522).

6. El método implementado por ordenador de cualquiera de las reivindicaciones anteriores, en el que, basándose en que el indicador del tipo de comando sin estado está configurado en otro valor (528), los otros comandos del tipo comando también se consideran válidos para su procesamiento por parte del procesador adjunto (104, 156), para el solicitante.

7. El método implementado por ordenador de la reivindicación 1, en el que el procesamiento incluye la preparación (530) de una respuesta que incluye un resultado del procesamiento del comando, debiendo ser enviada la respuesta al solicitante.

8. El método implementado por ordenador de la reivindicación 1, en el que el método comprende además preparar una respuesta al error (530) que indica un error basándose en la determinación de que el comando es no válido para su procesamiento por parte del procesador adjunto (104, 156), para el solicitante, y la respuesta al error se enviará al solicitante.

9. El método implementado por ordenador de la reivindicación 1, en el que el procesador adjunto (104, 156) comprende una tarjeta criptográfica.

10. Un sistema informático para facilitar el procesamiento seguro dentro de un entorno informático, comprendiendo el sistema informático:

una memoria (606); y

al menos un procesador (604) en comunicación con la memoria, en donde el sistema informático está configurado para realizar un método, comprendiendo dicho método:

determinar dinámicamente (500), por un procesador adjunto (104, 156), si los comandos obtenidos por el procesador adjunto deben ser procesados por el procesador adjunto, realizándose la determinación dinámica por cada comando y comprendiendo:

obtener (504), por el procesador adjunto, una solicitud de comando de un solicitante, incluyendo la solicitud de comando al menos un indicador de filtrado (320), que indica al menos un tipo de comando válido para su procesamiento por parte del procesador adjunto, para el solicitante, indicando el al menos un tipo de comando válido como válido para el solicitante basándose en uno o más tipos de comando permitidos para el solicitante;

determinar (508), por el procesador adjunto utilizando al menos un indicador de filtrado, si un comando de la solicitud de comando es válido para su procesamiento por parte del procesador adjunto, para el solicitante, incluyendo el al menos un indicador de filtrado un indicador del tipo de comando sin estado (322),

en el que, basándose en que el indicador del tipo de comando sin estado está configurado en un valor, los comandos determinados como comandos del tipo de comando sin estado son válidos para su procesamiento por parte del procesador adjunto, para el solicitante, y otros comandos del tipo de comando son no válidos para su procesamiento por parte del procesador adjunto, para el solicitante; y

procesar el comando (510), por el procesador adjunto, basándose en la determinación de que el comando es válido para ser procesado por el procesador adjunto, para el solicitante.

11. El sistema informático según la reivindicación 10, en el que el procesador adjunto (104, 156) está configurado en un modo y la determinación dinámica le permite funcionar de manera diferente que el modo en el que está configurado.

12. El sistema informático de la reivindicación 10, en el que el al menos un indicador de filtrado (320) está configurado por cada comando.

13. El sistema informático de cualquiera de las reivindicaciones 10 a 12, en el que el método comprende, además, preparar una respuesta a error (530) que indica un error basándose en la determinación de que el comando es no válido para su procesamiento por parte del procesador adjunto (104, 156), para el solicitante, y la respuesta a error se enviará al solicitante.

14. Un producto de programa informático para facilitar el procesamiento dentro de un entorno informático, comprendiendo el producto de programa informático: un medio de almacenamiento legible por ordenador, legible por un circuito de procesamiento, y que almacena instrucciones para su ejecución por el circuito de procesamiento para realizar un método según cualquiera de las reivindicaciones 1 a 9.

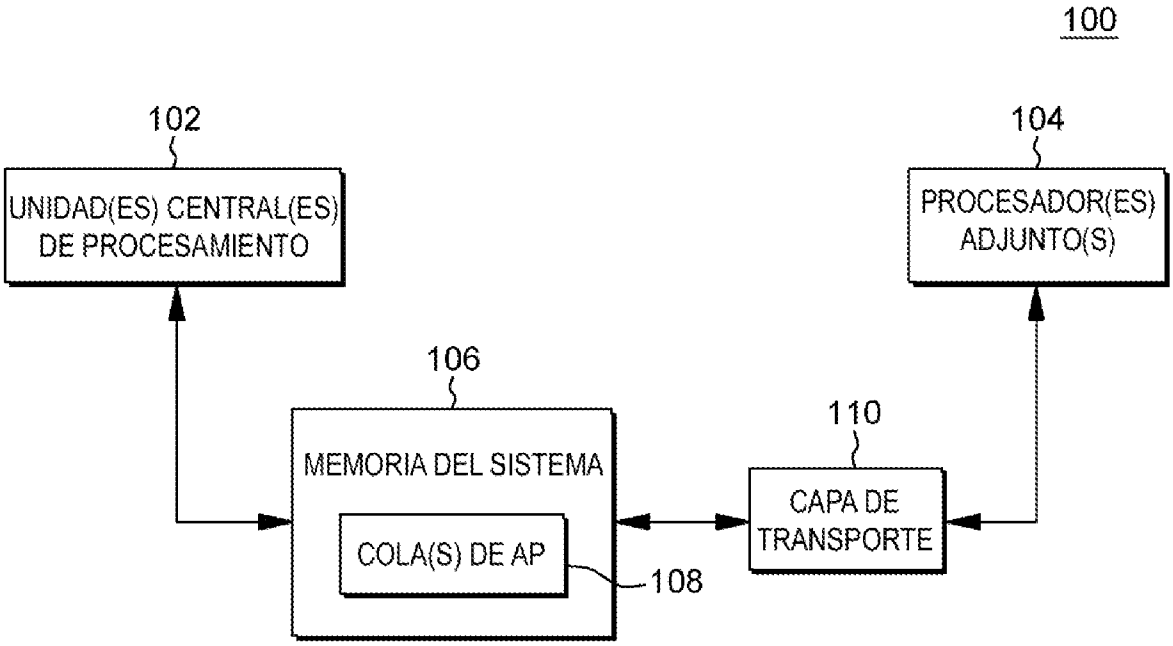

100
102
UNIDAD(ES) CENTRAL(ES) DE PROCESAMIENTO
104
PROCESADOR(ES) ADJUNTO(S)
106
MEMORIA DEL SISTEMA
COLA(S) DE AP
108
110
CAPA DE TRANSPORTE

FIG. 1A

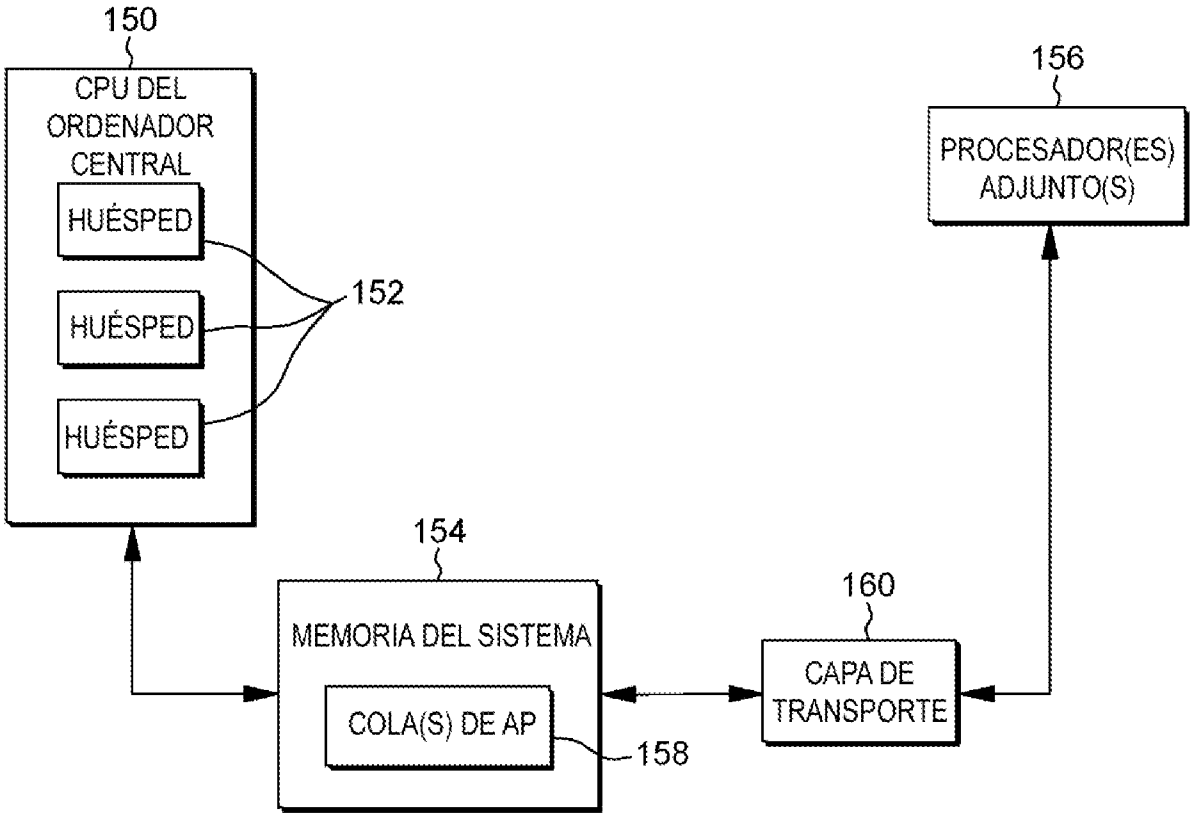

150
CPU DEL ORDENADOR CENTRAL
HUÉSPED
HUÉSPED
HUÉSPED
152
156
PROCESADOR(ES) ADJUNTO(S)
154
MEMORIA DEL SISTEMA
COLA(S) DE AP
158
160
CAPA DE TRANSPORTE

FIG. 1B

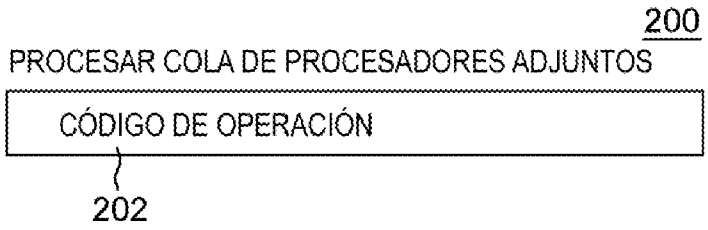


FIG. 2A

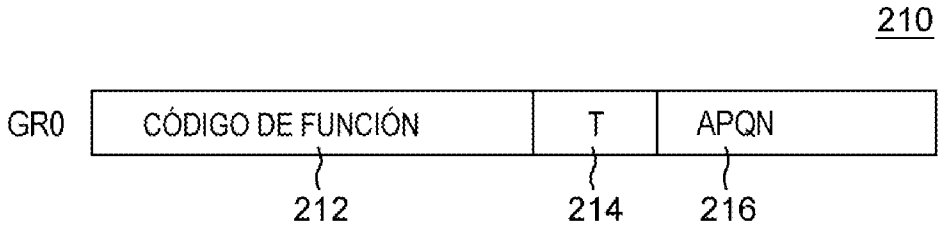


FIG. 2B

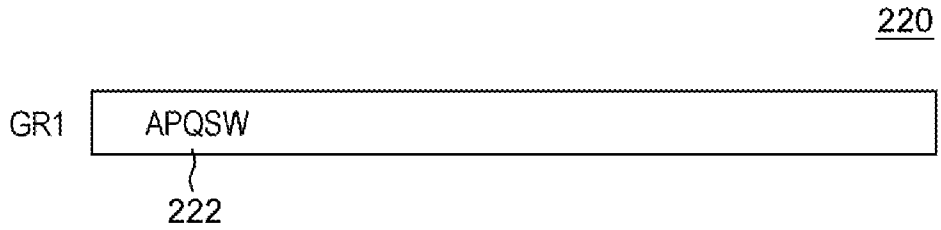


FIG. 2C

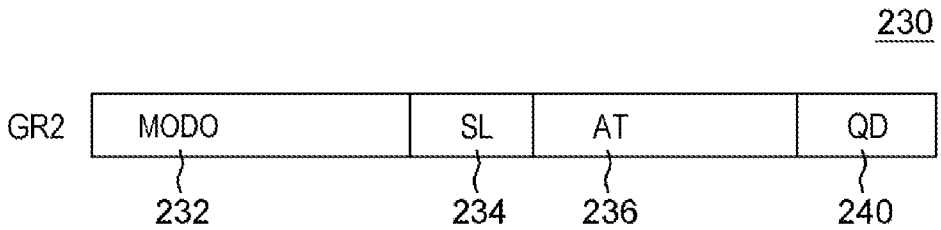


FIG. 2D

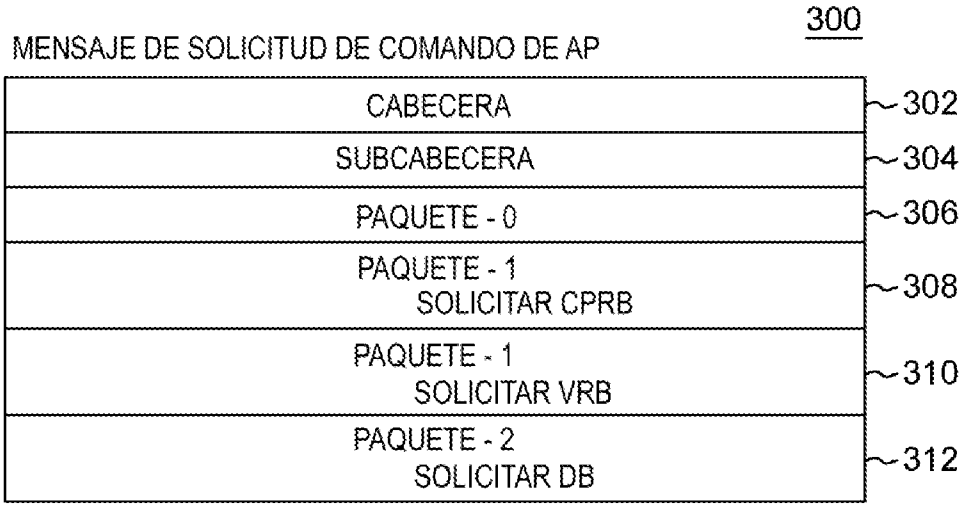


FIG. 3A

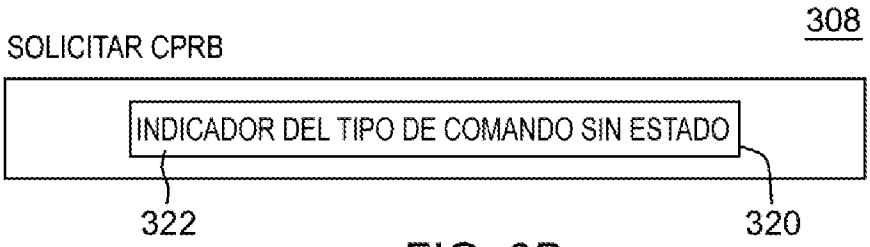


FIG. 3B

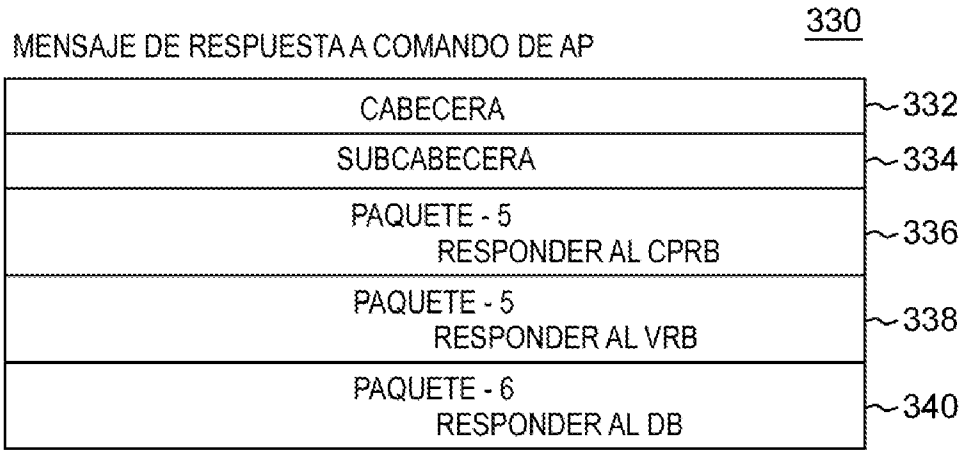


FIG. 3C

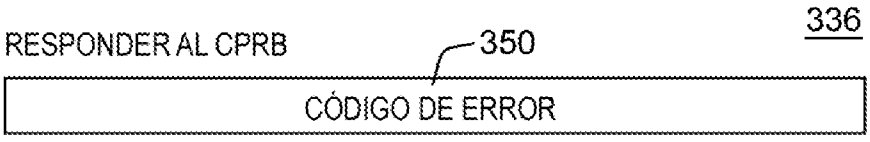


FIG. 3D

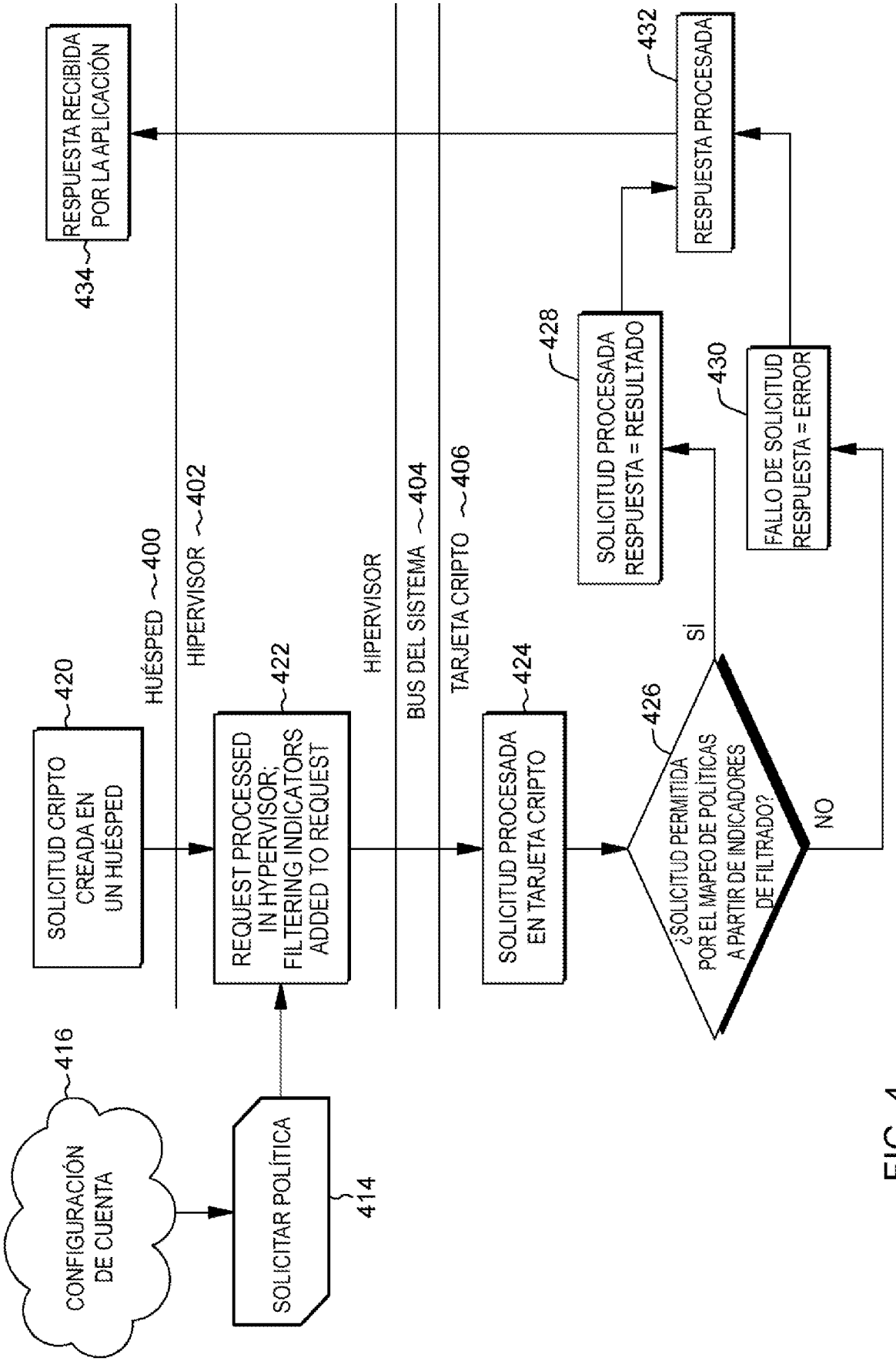

CONFIGURACIÓN DE CUENTA
416
SOLICITAR POLÍTICA
414
HUÉSPED
400
HIPERVISOR
402
HIPERVISOR
BUS DEL SISTEMA
404
TARJETA CRIPTO
406
SOLICITUD CRIPTO CREADA EN UN HUÉSPED
420
REQUEST PROCESSED IN HYPERVISOR; FILTERING INDICATORS ADDED TO REQUEST
422
SOLICITUD PROCESADA EN TARJETA CRIPTO
424
¿SOLICITUD PERMITIDA POR EL MAPEO DE POLÍTICAS A PARTIR DE INDICADORES DE FILTRADO?
426
SÍ
NO
SOLICITUD PROCESADA RESPUESTA = RESULTADO
428
FALLO DE SOLICITUD RESPUESTA = ERROR
430
RESPUESTA PROCESADA
432
RESPUESTA RECIBIDA POR LA APLICACIÓN
434

FIG. 4

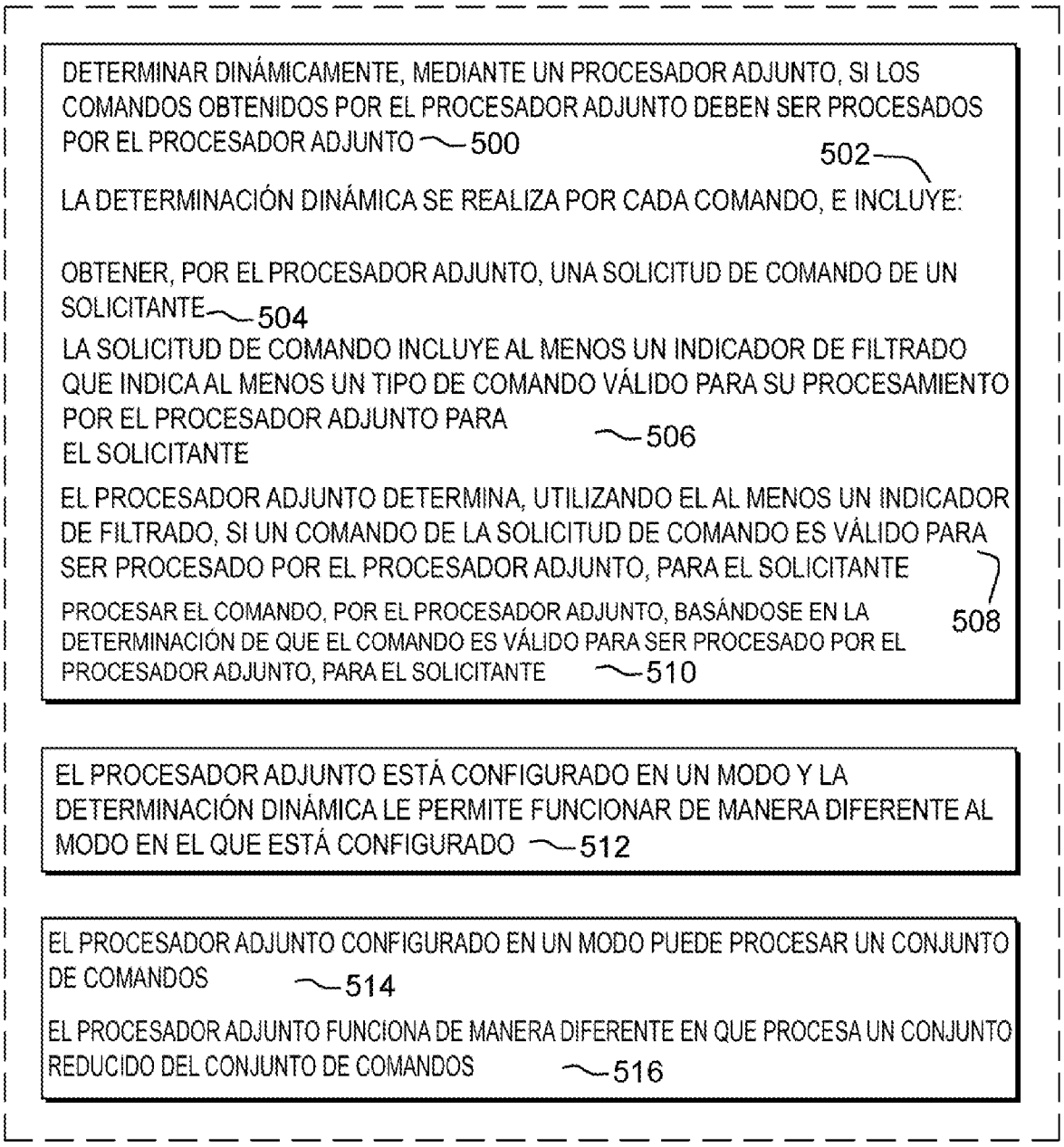

DETERMINAR DINÁMICAMENTE, MEDIANTE UN PROCESADOR ADJUNTO, SI LOS COMANDOS OBTENIDOS POR EL PROCESADOR ADJUNTO DEBEN SER PROCESADOS POR EL PROCESADOR ADJUNTO 500
502
LA DETERMINACIÓN DINÁMICA SE REALIZA POR CADA COMANDO, E INCLUYE:
OBTENER, POR EL PROCESADOR ADJUNTO, UNA SOLICITUD DE COMANDO DE UN SOLICITANTE 504
LA SOLICITUD DE COMANDO INCLUYE AL MENOS UN INDICADOR DE FILTRADO QUE INDICA AL MENOS UN TIPO DE COMANDO VÁLIDO PARA SU PROCESAMIENTO POR EL PROCESADOR ADJUNTO PARA EL SOLICITANTE 506
EL PROCESADOR ADJUNTO DETERMINA, UTILIZANDO EL AL MENOS UN INDICADOR DE FILTRADO, SI UN COMANDO DE LA SOLICITUD DE COMANDO ES VÁLIDO PARA SER PROCESADO POR EL PROCESADOR ADJUNTO, PARA EL SOLICITANTE
508
PROCESAR EL COMANDO, POR EL PROCESADOR ADJUNTO, BASÁNDOSE EN LA DETERMINACIÓN DE QUE EL COMANDO ES VÁLIDO PARA SER PROCESADO POR EL PROCESADOR ADJUNTO, PARA EL SOLICITANTE 510
EL PROCESADOR ADJUNTO ESTÁ CONFIGURADO EN UN MODO Y LA DETERMINACIÓN DINÁMICA LE PERMITE FUNCIONAR DE MANERA DIFERENTE AL MODO EN EL QUE ESTÁ CONFIGURADO 512
EL PROCESADOR ADJUNTO CONFIGURADO EN UN MODO PUEDE PROCESAR UN CONJUNTO DE COMANDOS 514
EL PROCESADOR ADJUNTO FUNCIONA DE MANERA DIFERENTE EN QUE PROCESA UN CONJUNTO REDUCIDO DEL CONJUNTO DE COMANDOS 516

FIG. 5A

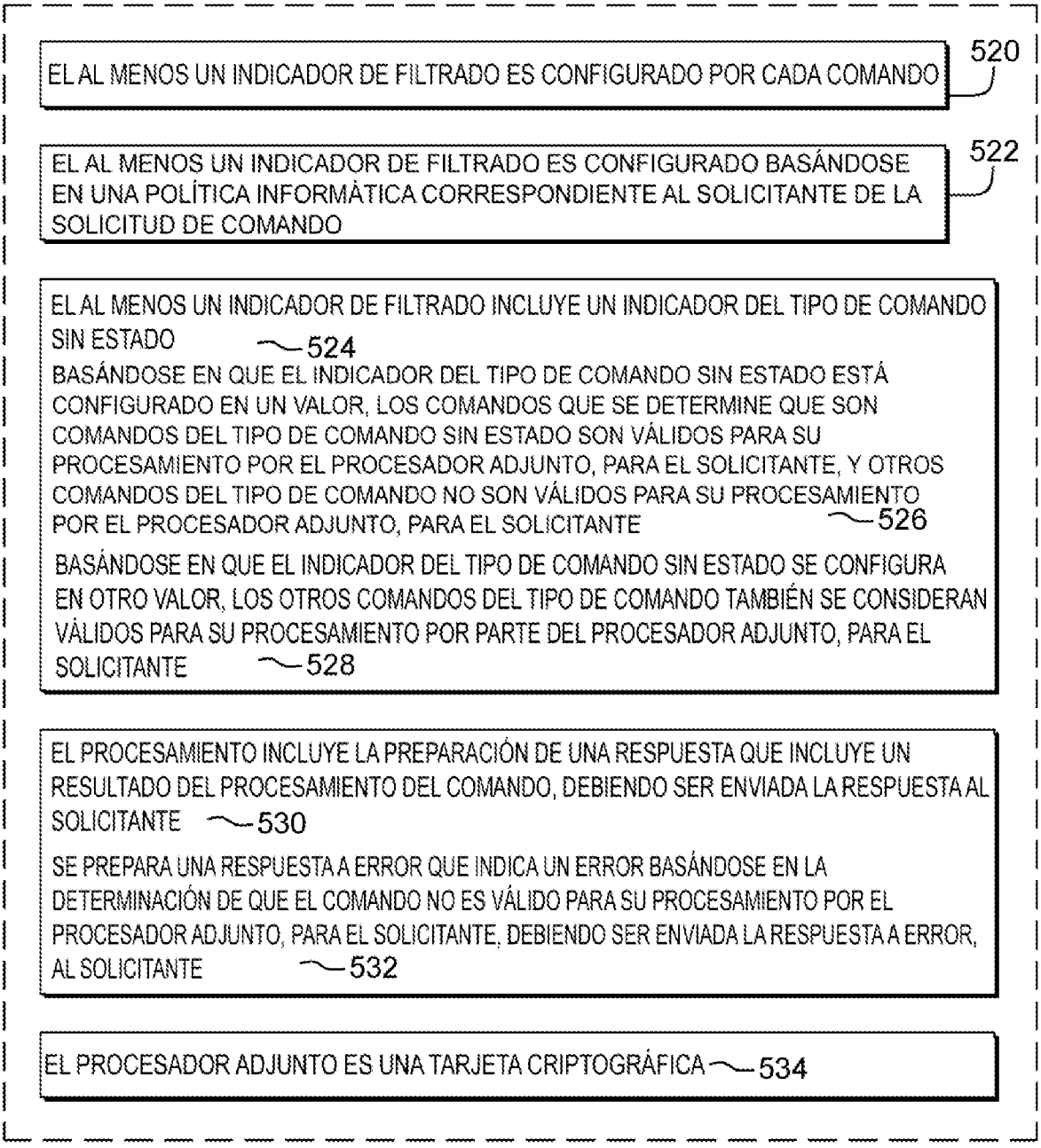

EL AL MENOS UN INDICADOR DE FILTRADO ES CONFIGURADO POR CADA COMANDO
520
EL AL MENOS UN INDICADOR DE FILTRADO ES CONFIGURADO BASÁNDOSE EN UNA POLÍTICA INFORMÀTICA CORRESPONDIENTE AL SOLICITANTE DE LA SOLICITUD DE COMANDO
522
EL AL MENOS UN INDICADOR DE FILTRADO INCLUYE UN INDICADOR DEL TIPO DE COMANDO SIN ESTADO
524
BASÁNDOSE EN QUE EL INDICADOR DEL TIPO DE COMANDO SIN ESTADO ESTÁ CONFIGURADO EN UN VALOR, LOS COMANDOS QUE SE DETERMINE QUE SON COMANDOS DEL TIPO DE COMANDO SIN ESTADO SON VÁLIDOS PARA SU PROCESAMIENTO POR EL PROCESADOR ADJUNTO, PARA EL SOLICITANTE, Y OTROS COMANDOS DEL TIPO DE COMANDO NO SON VÁLIDOS PARA SU PROCESAMIENTO POR EL PROCESADOR ADJUNTO, PARA EL SOLICITANTE
526
BASÁNDOSE EN QUE EL INDICADOR DEL TIPO DE COMANDO SIN ESTADO SE CONFIGURA EN OTRO VALOR, LOS OTROS COMANDOS DEL TIPO DE COMANDO TAMBIÉN SE CONSIDERAN VÁLIDOS PARA SU PROCESAMIENTO POR PARTE DEL PROCESADOR ADJUNTO, PARA EL SOLICITANTE
528
EL PROCESAMIENTO INCLUYE LA PREPARACIÓN DE UNA RESPUESTA QUE INCLUYE UN RESULTADO DEL PROCESAMIENTO DEL COMANDO, DEBIENDO SER ENVIADA LA RESPUESTA AL SOLICITANTE
530
SE PREPARA UNA RESPUESTA A ERROR QUE INDICA UN ERROR BASÁNDOSE EN LA DETERMINACIÓN DE QUE EL COMANDO NO ES VÁLIDO PARA SU PROCESAMIENTO POR EL PROCESADOR ADJUNTO, PARA EL SOLICITANTE, DEBIENDO SER ENVIADA LA RESPUESTA A ERROR, AL SOLICITANTE
532
EL PROCESADOR ADJUNTO ES UNA TARJETA CRIPTOGRÁFICA
534

FIG. 5B

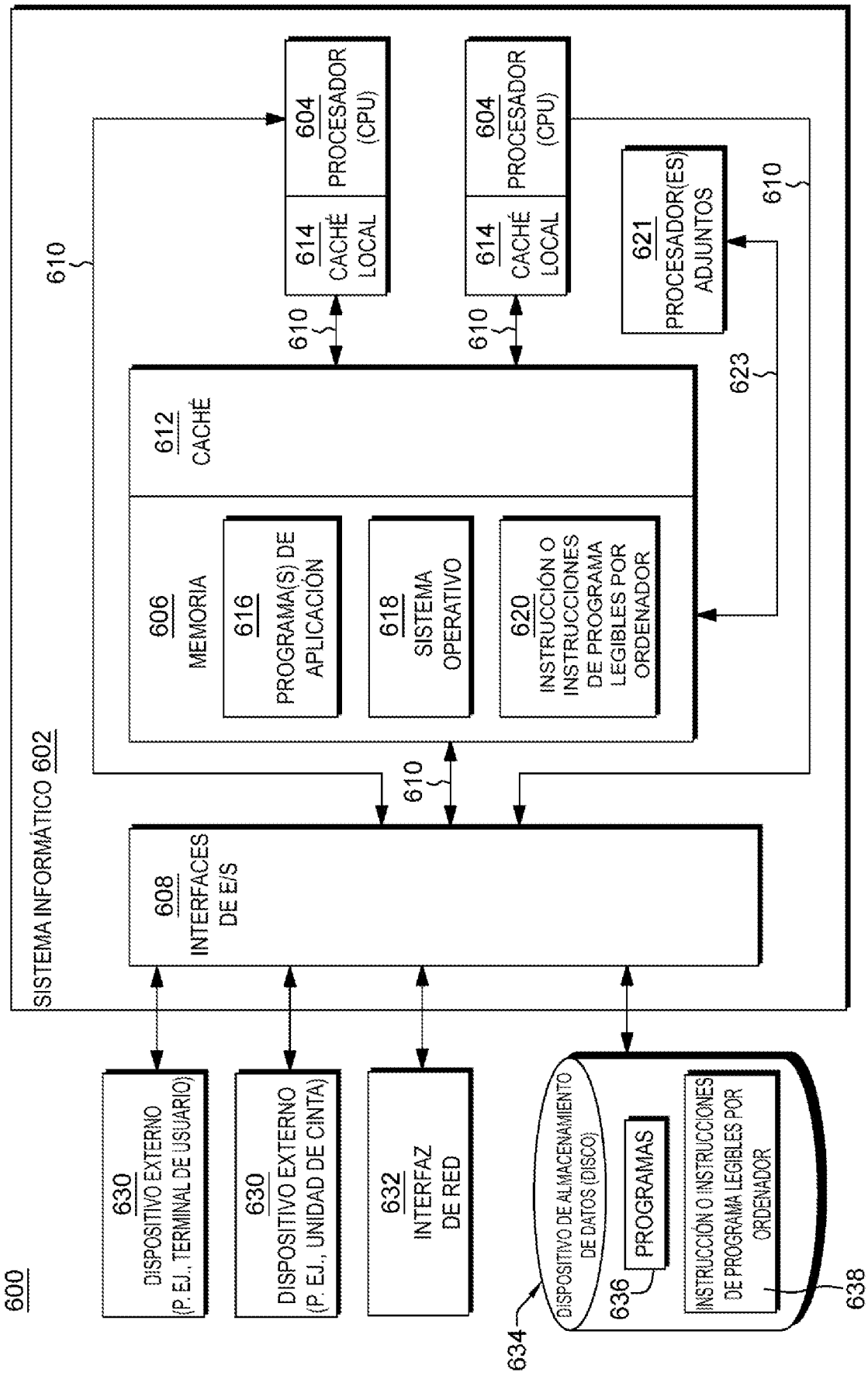

600
SISTEMA INFORMÁTICO 602
610
604 PROCESADOR (CPU)
614 CACHÉ LOCAL
604 PROCESADOR (CPU)
614 CACHÉ LOCAL
621 PROCESADOR(ES) ADJUNTOS
623
612 CACHÉ
606 MEMORIA
616 PROGRAMA(S) DE APLICACIÓN
618 SISTEMA OPERATIVO
620 INSTRUCCIÓN O INSTRUCCIONES DE PROGRAMA LEGIBLES POR ORDENADOR
608 INTERFACES DE E/S
630 DISPOSITIVO EXTERNO (P. EJ., TERMINAL DE USUARIO)
630 DISPOSITIVO EXTERNO (P. EJ., UNIDAD DE CINTA)
632 INTERFAZ DE RED
634 DISPOSITIVO DE ALMACENAMIENTO DE DATOS (DISCO)
636 PROGRAMAS
638 INSTRUCCIÓN O INSTRUCCIONES DE PROGRAMA LEGIBLES POR ORDENADOR

FIG. 6A

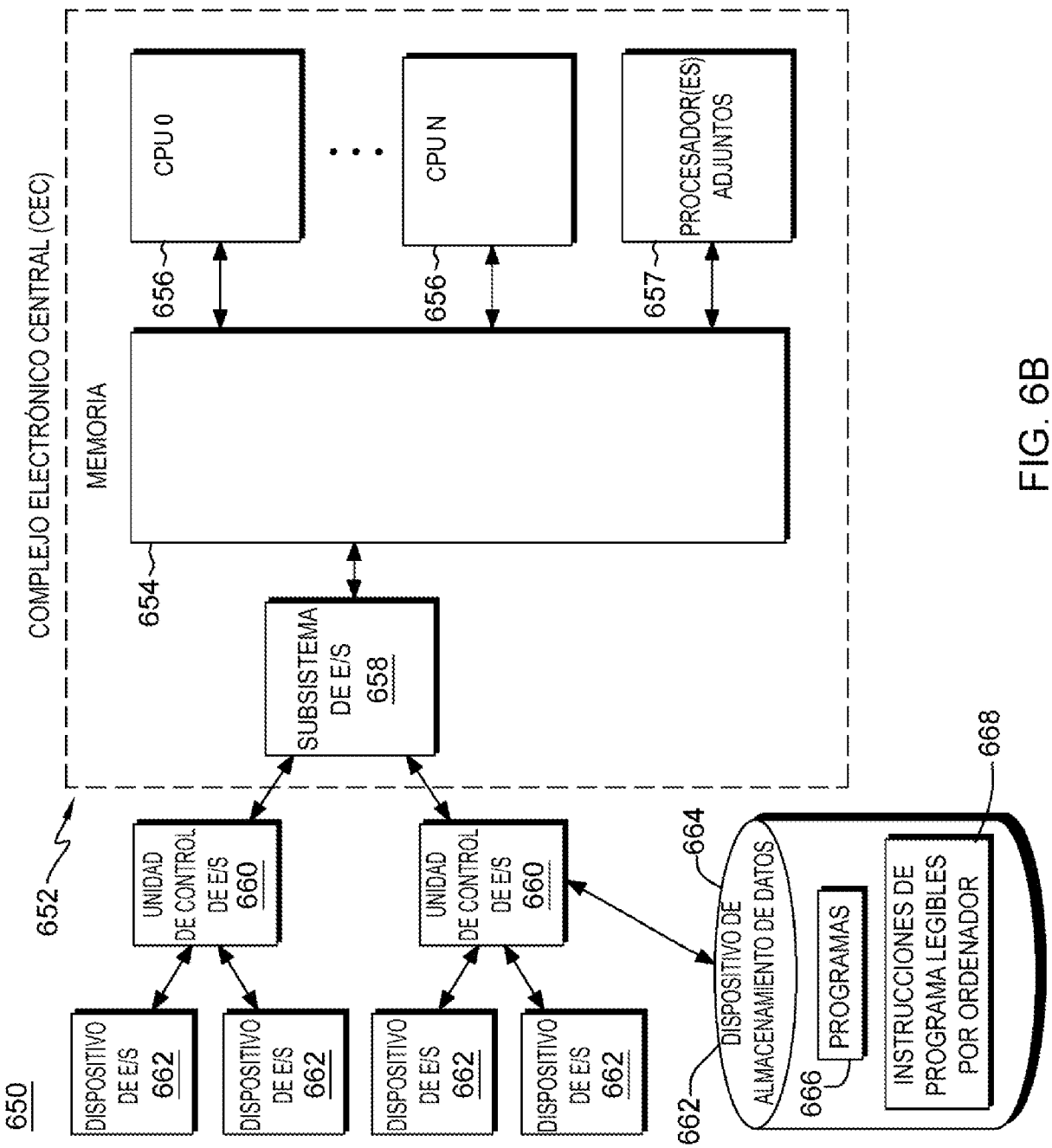

650
COMPLEJO ELECTRÓNICO CENTRAL (CEC)
MEMORIA
654
CPU 0
CPU N
PROCESADOR(ES) ADJUNTOS
656
656
657
SUBSISTEMA DE E/S 658
652
UNIDAD DE CONTROL DE E/S 660
UNIDAD DE CONTROL DE E/S 660
DISPOSITIVO DE E/S 662
DISPOSITIVO DE E/S 662
DISPOSITIVO DE E/S 662
DISPOSITIVO DE E/S 662
664
DISPOSITIVO DE ALMACENAMIENTO DE DATOS
662
666
PROGRAMAS
668
INSTRUCCIONES DE PROGRAMA LEGIBLES POR ORDENADOR

FIG. 6B

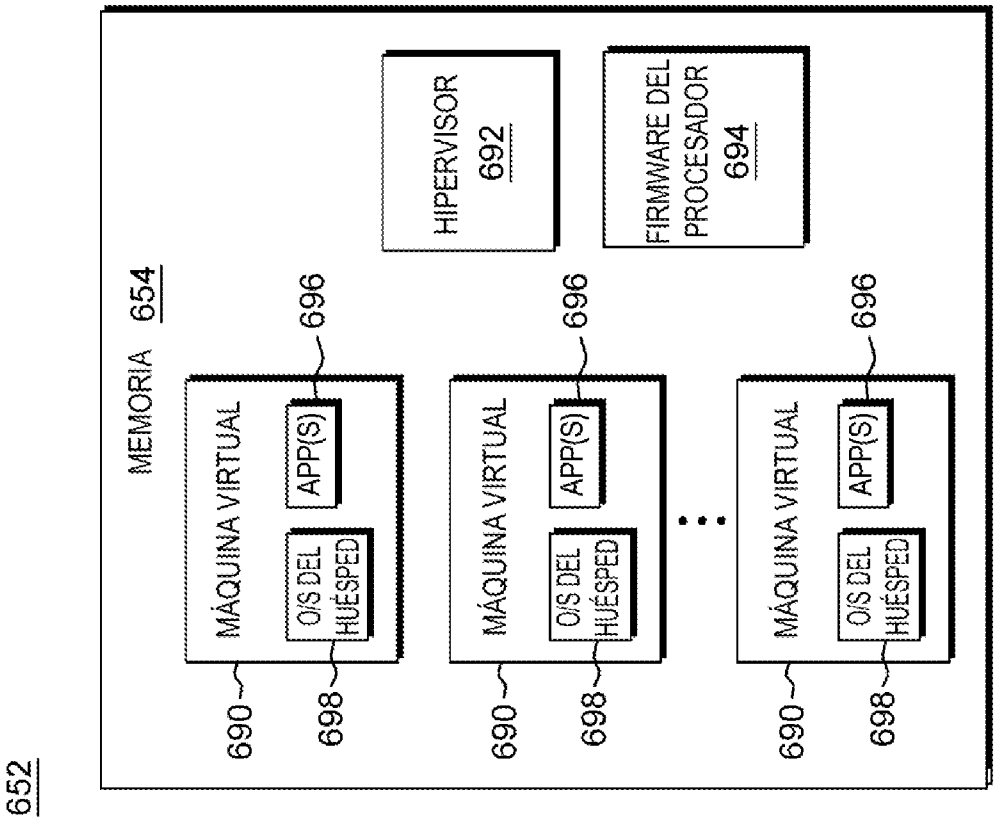

652
MEMORIA 654
MÁQUINA VIRTUAL
APP(S)
O/S DEL HUÉSPED
690
696
698
HIPERVISOR 692
FIRMWARE DEL PROCESADOR 694

FIG. 6D

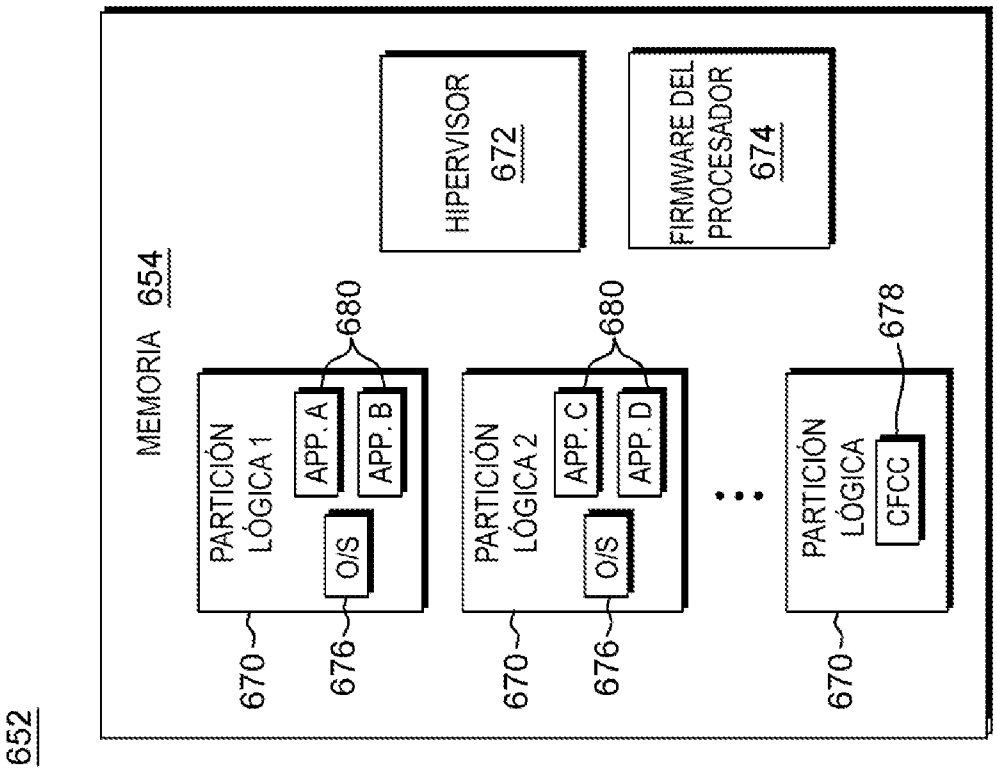

652
MEMORIA 654
PARTICIÓN LÓGICA 1
APP. A
APP. B
O/S
PARTICIÓN LÓGICA 2
APP. C
APP. D
O/S
PARTICIÓN LÓGICA
CFCC
670
676
680
678
HIPERVISOR 672
FIRMWARE DEL PROCESADOR 674

FIG. 6C

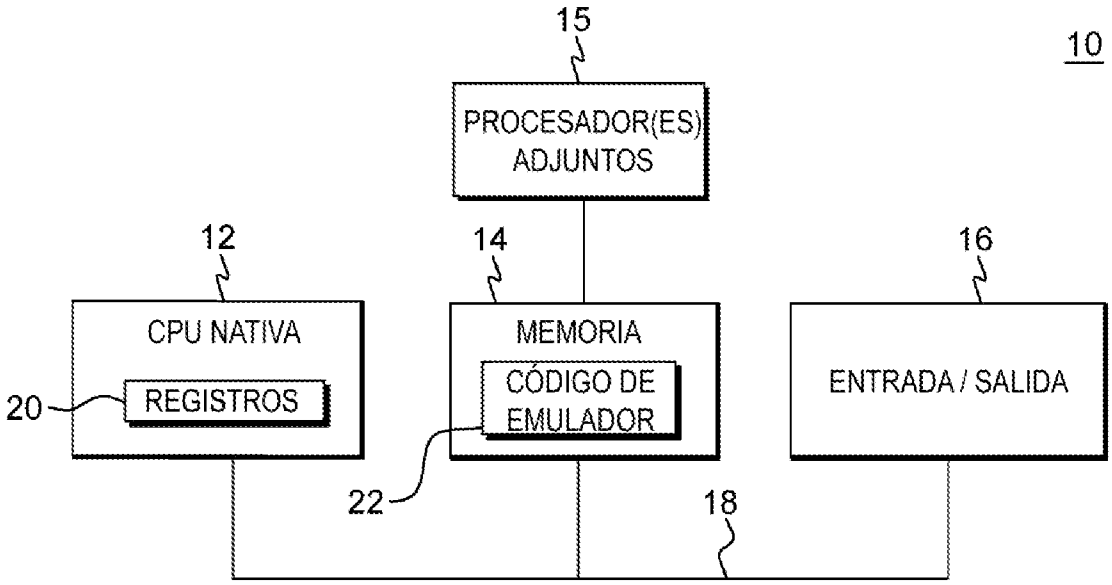

15
10
PROCESADOR(ES) ADJUNTOS
12
14
16
CPU NATIVA
MEMORIA
ENTRADA / SALIDA
20
REGISTROS
CÓDIGO DE EMULADOR
22
18

FIG. 7A

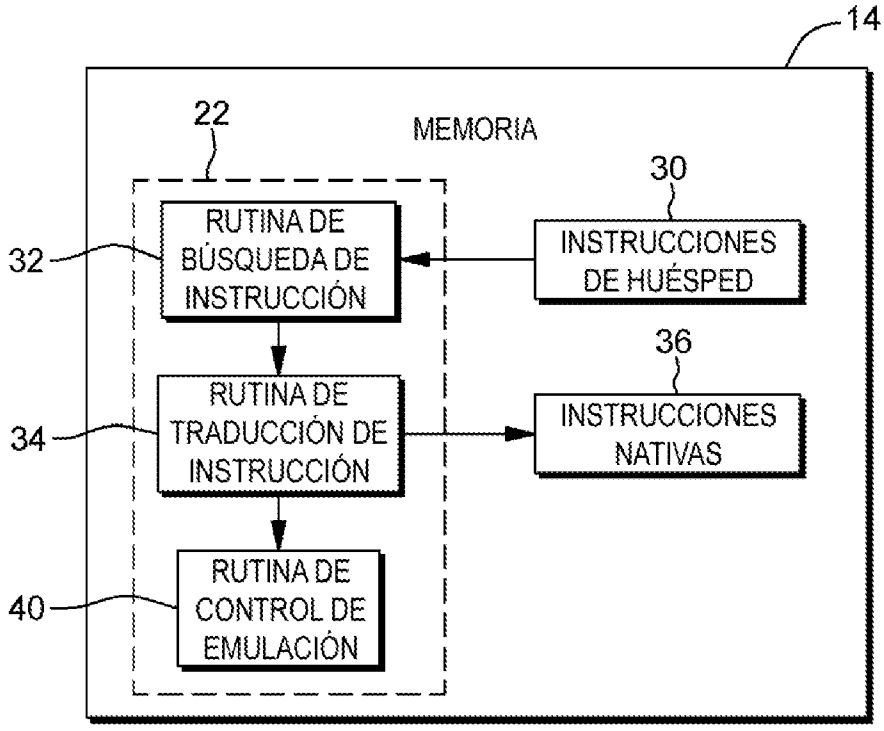

14
22
MEMORIA
30
RUTINA DE BÚSQUEDA DE INSTRUCCIÓN
32
INSTRUCCIONES DE HUÉSPED
36
RUTINA DE TRADUCCIÓN DE INSTRUCCIÓN
34
INSTRUCCIONES NATIVAS
RUTINA DE CONTROL DE EMULACIÓN
40

FIG. 7B

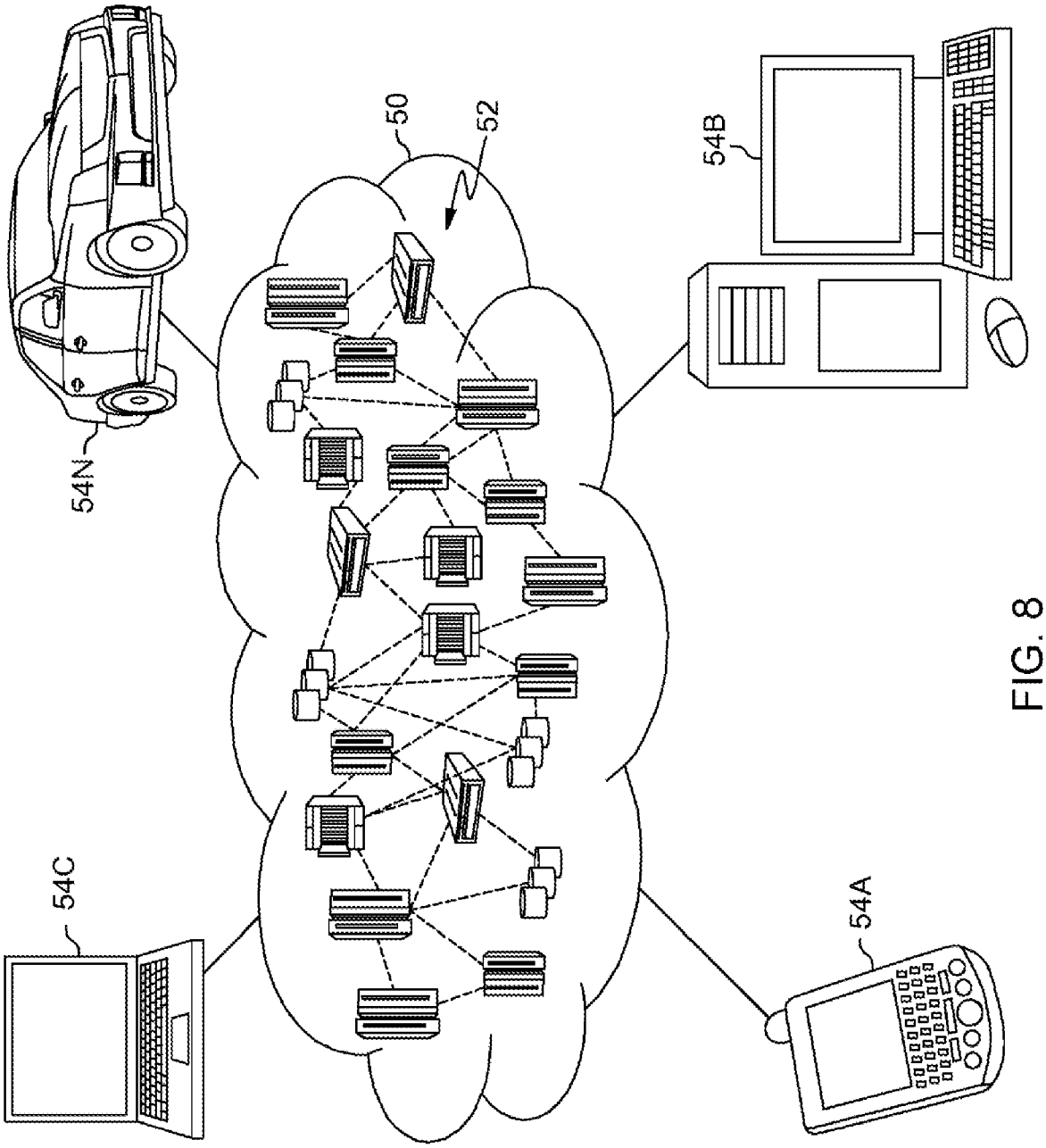


FIG. 8

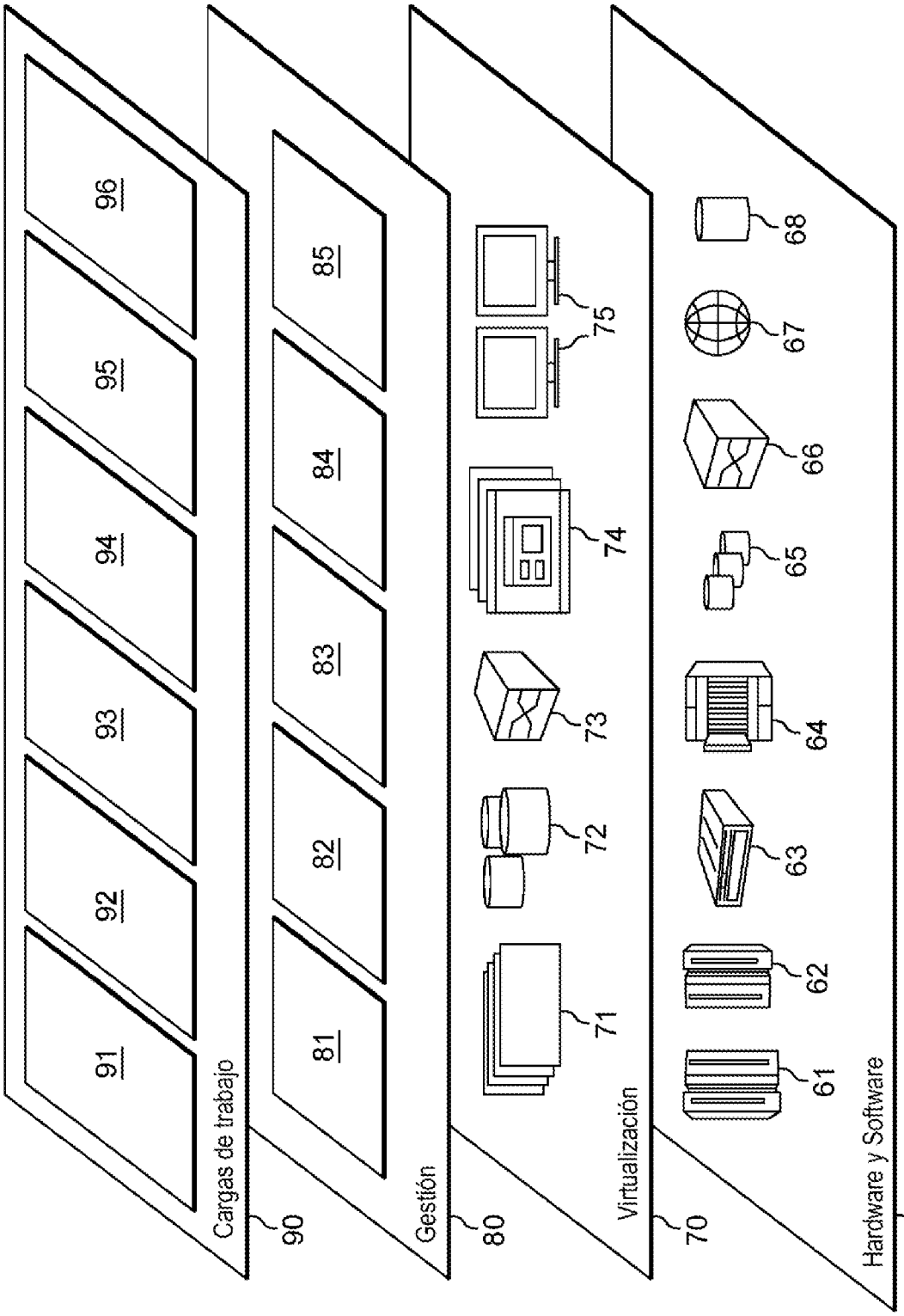

Cargas de trabajo
90
91
92
93
94
95
96
Gestión
80
81
82
83
84
85
Virtualización
70
71
72
73
74
75
Hardware y Software
60
61
62
63
64
65
66
67
68

FIG. 9