(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 939**

(51) Int. CI.:

H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.10.2010 PCT/US2010/054571**

(87) Fecha y número de publicación internacional: **19.05.2011 WO11059773**

(96) Fecha de presentación y número de la solicitud europea: **28.10.2010 E 10830473 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.02.2017 EP 2499784**

(54) Título: **Interconexión virtual de redes basada en modelo**

(30) Prioridad:

12.11.2009 US 616800

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.07.2017

(73) Titular/es:

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

(72) Inventor/es:

PANASYUK, ANATOLIY;
RANGEGOWDA, DHARSHAN;
VISWANATHAN, RAM;
CHAVEZ, ANTHONY S.;
CHEN, JIAZHEN;
BROWN, MORGAN;
ALKHATIB, HASAN S. y
OUTHRED, GEOFFREY H.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Interconexión virtual de redes basada en modelo

Antecedentes

La administración de redes ha dejado de ser una tarea sencilla. Por lo general, las empresas grandes tienen una gran presencia en una única ubicación o están dispersas por varias ubicaciones geográficas que están interconectadas por medio de una empresa corporativa. Con tales implementaciones grandes y complejas, la dinámica frecuentemente cambiante que está asociada con las redes implica añadir / suprimir empleados, añadir / suprimir dispositivos de empleados (por ejemplo, ordenadores, impresoras), etc., y es particularmente evidente cuando se trata con redes complejas que abarcan múltiples ubicaciones, o incluyen múltiples subredes, VPN (*virtual private network*, red virtual privada), múltiples encaminadores u otros dispositivos de red, tales como servidores, encaminadores, pasarelas, conmutadores, y así sucesivamente. Además, la gestión de redes de hoy en día con frecuencia incluye un conocimiento específico del proveedor y unos datos que complican adicionalmente la gestión y administración de redes.

El documento US 7 277 931 B1 se refiere a una interfaz de usuario y una representación de conectividad. En un ejemplo, se forman catálogos. Se crea y se visualiza una matriz. Se forma una representación de conexión entre pares de elementos en el catálogo. A partir de esta información de conexión, se pueden emprender acciones dentro de la red para dar lugar a que la red cree una instancia de las conexiones que se definen. Un administrador de redes usa la matriz creada como una base para la supervisión, la determinación de problemas, el ajuste y/o el modelado. En un ejemplo, se selecciona una conexión lógica al seleccionar o hacer clic sobre un punto de intersección. Esto hace aparecer un recuadro de selección que contiene campos para la información pertinente. Para cada campo, se selecciona un valor de entre un catálogo de valores posibles. Después de seleccionar valores para todos los campos, el usuario ha completado la configuración para la conexión entre los dos puntos de extremo y la configuración se almacena para su recuperación y/o visualización según se desee.

El documento US 2008/0259790 A1 se refiere a técnicas para una conectividad de extremo a extremo resistente y fiable en una red heterogénea. En un ejemplo, la técnica incluye crear un caso de un modelo de recurso de red (NRM, *network resource model*) abstraído para un entorno de red heterogéneo de diferentes nodos de recurso de red. La técnica puede incluir adicionalmente enlazar un punto de extremo de aplicación en el caso del NRM abstraído con un punto de extremo de conectividad para un primer nodo de los diferentes nodos de recurso de red. La técnica puede incluir, aún más adicionalmente, detectar una interrupción en el primer nodo de los diferentes nodos de recurso de red. Por último, la técnica puede incluir enlazar de nuevo el punto de extremo de aplicación con un segundo nodo de los diferentes nodos de recurso de red en respuesta a la detección de la interrupción.

Sumario

El objeto de la presente invención es la simplificación de la tarea de administrar una arquitectura de red. El presente objeto se soluciona por medio de la materia objeto de las reivindicaciones independientes. Algunas realizaciones preferidas se definen por medio de las reivindicaciones dependientes.

Lo sucesivo presenta un sumario simplificado con el fin de proporcionar una comprensión básica de algunas realizaciones novedosas que se describen en el presente documento. Este sumario no es una visión de conjunto exhaustiva, y el mismo no tiene por objeto identificar elementos clave / críticos o delimitar el ámbito de los mismos. Su único fin es presentar algunos conceptos en una forma simplificada como una introducción a la descripción más detallada que se presenta más adelante.

La arquitectura desvelada facilita la especificación virtual de una conexión entre puntos de extremo. Una red se puede definir como un modelo de conectividad abstracto que se expresa en términos de la intención de conectividad, en lugar de tecnología específica alguna. La arquitectura compila (traduce) el modelo de conectividad para dar unos ajustes de configuración, directivas, reglas de cortafuegos, etc., para implementar la intención de conectividad sobre la base de las capacidades de los dispositivos y las redes físicas disponibles.

El modelo de conectividad se usa para definir la semántica de conectividad de una red. El modelo se puede traducir a un conjunto de directivas y configuración de red que controlan la comunicación entre los nodos físicos en la red física. La red virtual resultante puede ser una superposición virtual que es independiente de la capa física. Como alternativa, la superposición virtual también puede incluir elementos y abstracciones de la red o redes físicas. Además, se pueden obtener reglas de seguridad de red automáticas (por ejemplo, *Internet Protocol security*, seguridad de Protocolo de Internet - IPSec) a partir del modelo de conectividad de la red.

Para la consecución de los fines anteriores y de otros fines relacionados, determinados aspectos ilustrativos se describen en el presente documento en conexión con la siguiente descripción y los dibujos adjuntos. Estos aspectos son indicativos de las diversas formas en las que se pueden poner en práctica los principios que se desvelan en el presente documento y se tiene por objeto que todos los aspectos y equivalentes de los mismos se encuentren dentro del ámbito de la materia objeto que se reivindica. Otras ventajas y características novedosas serán evidentes a partir de la siguiente descripción detallada cuando se considere junto con los dibujos.

Breve descripción de los dibujos

La figura 1 ilustra un sistema de gestión de redes implementado por ordenador de acuerdo con la arquitectura desvelada.

La figura 2 ilustra una realización alternativa de un sistema de gestión de redes que incluye una capa de traducción.

La figura 3 ilustra una representación más detallada de un sistema de gestión de redes de acuerdo con la arquitectura desvelada.

La figura 4 ilustra unos detalles a modo de ejemplo de unos modelos de conectividad.

La figura 5 ilustra un procedimiento de gestión de redes implementado por ordenador.

La figura 6 ilustra aspectos adicionales del procedimiento de la figura 5.

La figura 7 ilustra un diagrama de bloques de un sistema informático operable para desarrollar, traducir e implementar un modelo de conectividad de acuerdo con la arquitectura desvelada.

La figura 8 ilustra un diagrama de bloques esquemático de un entorno informático que es para el desarrollo, la traducción y la implementación de un modelo de conectividad.

Descripción detallada

La arquitectura desvelada facilita el desarrollo y la implementación de un modelo de conectividad que define una red virtual para configurar y gestionar una red física. Dicho de otra forma, una red física se define como un modelo abstracto, que se expresa en términos de la intención de conectividad, en lugar de tecnología específica alguna. Por ejemplo, el modelo de conectividad puede especificar de forma virtual que los ordenadores X, Y y Z se deberían comunicar libremente entre sí y también deberían tener una comunicación controlada en puertos particulares con el ordenador D. La traducción (compilación) del modelo aplica la red virtual a la red física de tal modo que los ajustes de configuración, directivas, reglas de cortafuegos, etc., implementan la intención de conectividad dadas las capacidades de los dispositivos físicos y las redes físicas disponibles.

Por ejemplo, se pueden asignar direcciones de IP en un intervalo específico a las máquinas físicas A y B. En lugar de solicitar de forma específica el encaminamiento entre subredes apropiadas, tal como se representa en las técnicas existentes para configurar la red física, la semántica de conectividad de un modelo de conectividad simplemente define que las máquinas A y B deberían ser capaces de comunicarse entre sí.

El modelo de conectividad opera en términos de identidades (por ejemplo, máquinas y usuarios), grupos (por ejemplo, máquinas y usuarios) y otras abstracciones (modelo lógico sin los detalles de conectividad), en lugar de direcciones de red física.

La implementación de la conectividad deseada se puede lograr mediante la creación de una o más superposiciones de red que son independientes de la red o redes físicas, y/o mediante el control de redes físicas por medio de una API (*application programming interface*, interfaz de programación de aplicaciones) / ajustes apropiados. En configuraciones que usan superposiciones de red, el modelo de conectividad también se puede usar para controlar la asignación de direcciones de IP a las máquinas y/o usuarios en la superposición de red. Por ejemplo, es posible atribuir una dirección de IP específica a una máquina y, entonces, esa dirección será válida con independencia de la dirección de red física o de IP de la máquina, debido a que la dirección de IP asignada se encuentra en el espacio de superposición de red. Esta capacidad facilita dar soporte a aplicaciones heredadas.

La arquitectura incluye un mecanismo para definir el modelo de conectividad de una red o redes como un conjunto de reglas que expresan una intención de conectividad. El mecanismo puede ser un editor de GUI (*graphical user interface*, interfaz gráfica de usuario), por ejemplo, para editar de forma gráfica el modelo de conectividad. También se incluye un mecanismo para compilar el modelo de conectividad para dar unos ajustes de configuración, directivas, reglas de cortafuegos, etc., para implementar el modelo de conectividad deseado.

El traductor (compilador) de modelo de conectividad puede ser específico de un conjunto de tecnologías de interconexión de redes que son utilizadas por una implementación particular. Por ejemplo, una posible implementación puede ser por medio de Direct Access ™ (DA) de Windows™ de Microsoft Corporation, en el que el modelo de conectividad se puede compilar para dar una serie de ajustes de IPSec, de Teredo (un protocolo de transmisión para enviar datagramas de IPv6 a través de dispositivos de NAT (*network address translation*, traducción de direcciones de red)), de SSTP (*secure socket tunneling protocol*, protocolo de túnel de sockets seguros), de cortafuegos y de otro tipo que se usan en una implementación.

Es posible crear traductores para otros conjuntos de tecnologías de redes de superposición, tales como IPv4 e IPv6, por ejemplo. Los traductores (compiladores) también se pueden crear para aplicar el modelo de conectividad a las redes físicas mediante el control de conmutadores programables y VLAN (*virtual local area network*, red de área local virtual), por ejemplo.

La arquitectura desvelada también hace posible la implementación de sistemas híbridos, en los que partes del modelo de conectividad son soportadas por la superposición o superposiciones de red mientras que otras partes del modelo son soportadas por las redes físicas. Un ejemplo de tal disposición es una combinación de máquinas que están conectadas con una LAN que se pueden controlar por medio de programación (por ejemplo, por medio de

VLAN, IPSec, etc.), y máquinas que están conectadas de forma remota (por ejemplo, por medio de Teredo o SSTP), la totalidad de las cuales son controladas por el único modelo de conectividad.

La arquitectura también proporciona el mecanismo para ejecutar elementos necesarios del modelo de conectividad. Esta administración necesaria depende de la implementación física (por ejemplo, una red de superposición frente a una red física, Teredo frente a SSTP frente a L2TP (*Layer 2 tunneling protocol*, protocolo de túnel de Capa 2) frente a otros protocolos).

La arquitectura simplifica de forma significativa la creación, la gestión y el uso de redes al centrarse en la conectividad (intención de conectividad) deseada en lugar de en los detalles de implementación (por ejemplo, intervalos de IP, IPSec, directivas, etc.). Además, deja de ser necesario que el personal de TI tenga un conocimiento profundo de la interconexión de redes para crear o gestionar la red. En casos simples, tales como pequeña o mediana empresa, y aplicaciones de consumo, la complejidad se puede eliminar por completo, lo que permite que administradores sin conocimiento alguno de la interconexión de redes configuren y gestionen con éxito la red.

Adicionalmente, se proporciona una simplificación al hacer la red consistente y coherente y mediante la obtención de todos los ajustes, directivas, etc., relevantes, a partir del único modelo de conectividad. Está garantizado que todos los ajustes / directivas que se requieren estén bien alineados y que no entren en conflicto. Esto es diferente de las situaciones existentes en las que cada tipo de ajuste / directiva / regla se define de forma independiente, dejando espacio para errores e inconsistencias.

La simplificación también proporciona una alta fiabilidad al asegurar la consistencia y la coherencia, y al incluir unos mecanismos de autocomprobación integrados que verifican que los ajustes reales y la conectividad están alineados con el modelo de conectividad previsto.

Las capacidades de autoajuste de la arquitectura permiten que la red conmute de forma automática a tecnologías y sistemas de conectividad alternativos (por ejemplo, SSTP frente a IPv6 directo o Teredo) para conservar el modelo de conectividad deseado mientras que los sistemas de red subyacentes están cambiando (por ejemplo, un ordenador portátil que se está moviendo entre diferentes redes).

Adicionalmente, se puede lograr una alta seguridad mediante la obtención, de forma automática, de reglas de seguridad de red (por ejemplo, IPSec) a partir del modelo de conectividad. Esto permite una conectividad segura sin emplear tiempo alguno para configurar o gestionar la seguridad de red.

El modelo de conectividad desvelado también prevé la creación de redes y sistemas más complejos que usan una combinación de tecnologías con sistemas alojados.

Se hace referencia a continuación a los dibujos, en los que números de referencia semejantes se usan para hacer referencia a elementos semejantes por la totalidad del presente documento. En la siguiente descripción, por razones de explicación, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión exhaustiva de la misma. Puede ser evidente, no obstante, que las realizaciones novedosas se pueden poner en práctica sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques con el fin de facilitar una descripción de los mismos. La intención es cubrir todas las modificaciones, equivalentes y alternativas que caigan dentro del ámbito de la materia objeto que se reivindica.

La figura 1 ilustra un sistema de gestión de redes implementado por ordenador 100 de acuerdo con la arquitectura desvelada. El sistema 100 incluye una disposición de nodos 102 de una red física 104 y un modelo de conectividad 106 que define una conectividad virtual entre los nodos 102 usando la semántica de conectividad 108. El modo de conectividad se crea para gestionar las comunicaciones entre los nodos 102 de la red física 104.

El modelo de conectividad 106 describe una red virtual que se superpone a una capa física y es independiente de la capa física. El modelo de conectividad 106 describe una red virtual que se superpone a una capa física e incluye elementos y abstracciones de la red física 104. El modelo de conectividad 106 también puede definir seguridad de red como parte de la semántica de conectividad 108. La semántica de conectividad 108 puede incluir identidades de máquina e identidades de usuario de los nodos, grupos de nodos y grupos de usuarios y/o identidades de nodo. La semántica de conectividad 108 gestiona puertos y pasarelas de la red física 108.

Por lo tanto, la administración de redes que está ligada a un ordenador portátil que se está moviendo de una red a otra red (por ejemplo, a través de ubicaciones geográficas corporativas) se maneja sin problemas debido a que el modelo de conectividad indica los grupos a los que debería estar conectado el usuario incluso cuando es móvil.

La figura 2 ilustra una realización alternativa de un sistema de gestión de redes 200 que incluye una capa de traducción 202. El sistema 200 incluye la disposición de nodos 102 de la red física 104 (capa física), y el modelo de conectividad 106 que define una conectividad virtual entre los nodos 102 usando la semántica de conectividad 108. El modo de conectividad se crea para gestionar las comunicaciones entre los nodos 102 de la red física 104. La capa de traducción 202 traduce la semántica de conectividad 108 a unas directivas e información de configuración que gestionan las comunicaciones entre los nodos 102 de la red física 104.

Dicho de otra forma, el sistema 200 incluye la disposición de nodos 102 de la red física 104, el modelo de conectividad 106 que define una conectividad virtual entre los nodos 102 usando la semántica de conectividad 108, y la capa de traducción 202 que traduce la semántica de conectividad 108 a unas directivas e información de configuración que gestionan las comunicaciones entre los nodos 102 de la red física 104.

La conectividad virtual describe una red virtual 204 que se superpone a una capa física y es independiente de la capa física. La conectividad virtual describe una red virtual 204 que se superpone a una capa física e incluye elementos y abstracciones de la red física 104. El modelo de conectividad 106 define seguridad de red como parte de la semántica de conectividad 108. La semántica de conectividad 108 incluye identidades de máquina e identidades de usuario de los nodos, grupos de nodos y grupos de usuarios y/o identidades de nodo.

La figura 3 ilustra una representación más detallada de un sistema de gestión de redes 300 de acuerdo con la arquitectura desvelada. El sistema 300 incluye el modelo de conectividad 106 (y la semántica de conectividad de la red virtual), el cual se puede aplicar a una capa física 302 por medio de la capa de traducción 202. La capa de traducción puede incluir uno o múltiples traductores para traducir la semántica a unas directivas y reglas, etc., para su aplicación directa a la capa física 302.

El sistema 300 también incluye una interfaz de usuario 304 (por ejemplo, UI gráfica) para desarrollar y configurar el modelo de conectividad 106 usando unas definiciones de modelo 306. Las definiciones 306 pueden incluir una amplia diversidad de definiciones para una implementación selectiva en diferentes modelos de conectividad. El sistema 300 también puede incluir un componente de almacenamiento 308 para el almacenamiento de los modelos existentes para su recuperación y utilización automática o dinámica según se desee. Los modelos de conectividad se pueden desarrollar con conexión o sin conexión, y almacenarse para su posterior recuperación y uso, a petición.

La figura 4 ilustra unos detalles a modo de ejemplo de unos modelos de conectividad 400. En el presente caso, el modelo de conectividad 106 incluye la semántica de conectividad 108 que puede definir unas ID de máquina y/o de usuario 402, unos grupos 404 (de máquinas y/o usuarios), y otras abstracciones 406. La semántica 108 se pasa a través de un traductor 408 específico del modelo de conectividad 108 (o porciones semánticas del mismo) para traducir la semántica 108 a unos ajustes, directivas y reglas 410 que facilitan la gestión de las comunicaciones de una red física 412.

De forma similar, un segundo modelo de conectividad 414 incluye la semántica de conectividad 416 que puede definir unas ID de máquina y/o de usuario 418, unos grupos 420 (de máquinas y/o usuarios), y otras abstracciones 422. La semántica 416 se pasa a través de un traductor 424 específico del segundo modelo de conectividad 414 (o porciones semánticas del mismo) para traducir la semántica 416 a unos ajustes, directivas y reglas 426 que facilitan la gestión de las comunicaciones de una red física 428.

Dicho de otra forma, se pueden emplear múltiples modelos de conectividad para la configuración y para la gestión de las correspondientes redes físicas, subredes de una red, dispositivos físicos (por ejemplo, pasarelas, encaminadores, etc.) y puertos, por ejemplo, de dispositivos y nodos físicos, restringidos solo por la semántica que se emplea y que se puede traducir a la semántica de conectividad. Con respecto a los múltiples traductores, un traductor se puede dedicar al manejo de directivas de IPsec, un segundo traductor se puede dedicar al manejo de directivas de cortafuegos, un tercer traductor está dedicado a manejar conexiones de SSL (*secure socket layer*, capa de sockets seguros), un cuarto traductor se puede dedicar al manejo de pasarelas, y así sucesivamente.

El modelo de conectividad que se desvela en el presente documento proporciona un mecanismo conveniente y potente para que los administradores de redes definan directivas para los requisitos de salud del sistema, tal como la asignación de directivas a grupos de máquinas / usuarios tal como es facilitado por NAP (*network access protection*, protección de acceso a redes), una tecnología desarrollada por Microsoft Corporation. Los requisitos de salud pueden estar relacionados con nodos que tienen la versión deseada de soporte lógico de detección y de prevención de soporte lógico malicioso y un cortafuegos activo, por ejemplo.

En el presente documento se incluye un conjunto de diagramas de flujo representativos de metodologías a modo de ejemplo para realizar aspectos novedosos de la arquitectura desvelada. Mientras que, por razones de simplicidad de explicación, las una o más metodologías que se muestran en el presente documento, por ejemplo, en forma de diagrama de flujo o gráfico de flujo, se muestran y se describen como una serie de actos, se ha de entender y apreciar que las metodologías no están limitadas por el orden de los actos, debido a que algunos actos pueden, de acuerdo con las mismas, tener lugar en un orden diferente y/o de forma concurrente con actos que no sean aquellos que se muestran y se describen en el presente documento. Por ejemplo, los expertos en la materia entenderán y apreciarán que, como alternativa, una metodología se podría representar como una serie de estados o eventos interrelacionados, tal como en un diagrama de estados. Además, puede que no todos los actos que se ilustran en una metodología se requieran para una implementación novedosa.

La figura 5 ilustra un procedimiento de gestión de redes implementado por ordenador. En 500, se define un modelo de conectividad que describe una red virtual de conectividad entre nodos de una capa física sobre la base de una semántica de conectividad. En 502, se gestionan las comunicaciones entre los nodos de la capa física sobre la base del modelo de conectividad.

La figura 6 ilustra aspectos adicionales del procedimiento de la figura 5. En 600, la semántica de conectividad se traduce a unas directivas y reglas que gestionan las comunicaciones entre los nodos de la capa física. En 602, la red virtual se aplica como una superposición de la capa física e independiente de la capa física. En 604, la red virtual se aplica como una superposición de la capa física que incluye elementos y abstracciones de la capa física. En 606, se aplica seguridad de red a la capa física como parte del modelo de conectividad. En 608, se crea una semántica de conectividad que incluye identidades de máquina e identidades de usuario de los nodos, grupos de nodos y grupos de usuarios e identidades de nodo.

Tal como se usa en la presente solicitud, se tiene por objeto que las expresiones “componente” y “sistema” hagan referencia a una entidad relacionada con un ordenador, o bien soporte físico, o bien una combinación de soporte físico y soporte lógico, o bien soporte lógico o bien soporte lógico en ejecución. Por ejemplo, un componente puede ser, pero no se limita a ser, un procedimiento que se está ejecutando en un procesador, un procesador, una unidad de disco duro, múltiples unidades de almacenamiento (de medio de almacenamiento óptico, de estado sólido y/o magnético), un objeto, un ejecutable, un subprocedimiento de ejecución, un programa y/o un ordenador. A modo de ilustración, tanto una aplicación que se está ejecutando en un servidor como el servidor pueden ser un componente. Uno o más componentes pueden residir dentro de un procedimiento y/o un subprocedimiento de ejecución, y un componente puede estar localizado en un ordenador y/o distribuido entre dos o más ordenadores. La expresión “a modo de ejemplo” se puede usar en el presente documento para querer decir servir como un ejemplo, caso o ilustración. Cualquier aspecto o diseño que se describa en el presente documento como “a modo de ejemplo” no se ha de interpretar necesariamente como preferido o ventajoso frente a otros aspectos o diseños.

Haciendo referencia a continuación a la figura 7, se ilustra un diagrama de bloques de un sistema informático 700 operable para desarrollar, traducir e implementar un modelo de conectividad de acuerdo con la arquitectura desvelada. Con el fin de proporcionar un contexto adicional para diversos aspectos del mismo, se tiene por objeto que la figura 7 y la siguiente descripción proporcionen una descripción breve y general del sistema informático 700 adecuado en el que se puedan implementar los diversos aspectos. A pesar de que la descripción en lo que antecede se encuentra en el contexto general de las instrucciones ejecutables por ordenador que se pueden ejecutar en uno o más ordenadores, los expertos en la materia reconocerán que una realización novedosa también se puede implementar en combinación con otros módulos de programa y/o como una combinación de soporte físico y soporte lógico.

El sistema informático 700 para implementar diversos aspectos incluye el ordenador 702 que tiene una unidad o unidades de procesamiento 704, un almacenamiento legible por ordenador tal como una memoria de sistema 706, y un bus de sistema 708. La unidad o unidades de procesamiento 704 pueden ser cualquiera de diversos procesadores disponibles en el mercado, tal como procesador único, procesador múltiple, unidades de núcleo único y unidades de núcleo múltiple. Además, los expertos en la materia apreciarán que los procedimientos novedosos se pueden poner en práctica con otras configuraciones del sistema informático, incluyendo miniordenadores, ordenadores centrales, así como ordenadores personales (por ejemplo, de escritorio, portátiles, etc.), dispositivos informáticos de mano, electrónica de consumo programable o basada en microprocesador, y similares, cada uno de los cuales se puede acoplar de forma operativa con uno o más dispositivos asociados.

La memoria de sistema 706 puede incluir un almacenamiento legible por ordenador tal como una memoria volátil (VOL) 710 (por ejemplo, una memoria de acceso aleatorio (RAM, *random access memory*)) y una memoria no volátil (NO VOL) 712 (por ejemplo, ROM, EPROM, EEPROM, etc.). Un sistema básico de entrada / salida (BIOS, *basic input / output system*) se puede almacenar en la memoria no volátil 712, e incluye las rutinas básicas que facilitan la comunicación de datos y señales entre componentes dentro del ordenador 702, tal como durante el arranque. La memoria volátil 710 también puede incluir una RAM de alta velocidad tal como una RAM estática para almacenar temporalmente los datos.

El bus de sistema 708 proporciona una interfaz para componentes de sistema incluyendo, pero sin limitarse a, el subsistema de memoria 706 con la unidad o unidades de procesamiento 704. El bus de sistema 708 puede ser cualquiera de varios tipos de estructura de bus que se pueden interconectar adicionalmente con un bus de memoria (con o sin un controlador de memoria) y un bus de periféricos (por ejemplo, PCI, PCIe, AGP, LPC, etc.), usando cualquiera de una diversidad de arquitecturas de bus disponibles en el mercado.

El ordenador 702 incluye adicionalmente un subsistema o subsistemas de almacenamiento legibles por máquina 714 y una interfaz o interfaces de almacenamiento 716 para interconectar el subsistema o subsistemas de almacenamiento 714 con el bus de sistema 708 y otros componentes informáticos deseados. El subsistema o subsistemas de almacenamiento 714 pueden incluir una o más de una unidad de disco duro (HDD, *hard disk drive*), una unidad de disco flexible (FDD, *floppy disk drive*) magnético y/o una unidad de almacenamiento en disco óptico (por ejemplo, una unidad de CD-ROM, una unidad de DVD), por ejemplo. La interfaz o interfaces de almacenamiento 716 pueden incluir tecnologías de interfaz tales como EIDE, ATA, SATA e IEEE 1394, por ejemplo.

Uno o más programas y datos se pueden almacenar en el subsistema de memoria 706, un subsistema de memoria legible por máquina y extraíble 718 (por ejemplo, una tecnología de formato de unidad flash), y/o el subsistema o subsistemas de almacenamiento 714 (por ejemplo, óptico, magnético, de estado sólido), incluyendo un sistema operativo 720, uno o más programas de aplicación 722, otros módulos de programa 724 y unos datos de programa

726.

Los uno o más programas de aplicación 722, los otros módulos de programa 724 y los datos de programa 726 pueden incluir el modelo de conectividad y la semántica de conectividad que se describen en el presente documento, la capa de traducción y los traductores, el sistema 300 de la figura 3, los modelos 400 y las entidades asociadas de la figura 4, y los procedimientos que son representados por los diagramas de flujo de las figuras 5 - 6, por ejemplo.

En general, los programas incluyen rutinas, procedimientos, estructuras de datos, otros componentes de soporte lógico, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. La totalidad o unas porciones del sistema operativo 720, las aplicaciones 722, los módulos 724 y/o los datos 726 también se pueden almacenar temporalmente en una memoria tal como la memoria volátil 710, por ejemplo. Se ha de apreciar que la arquitectura desvelada se puede implementar con diversos sistemas operativos o combinaciones de sistemas operativos (por ejemplo, como máquinas virtuales) disponibles en el mercado.

El subsistema o subsistemas de almacenamiento 714 y las subsistemas de memoria (706 y 718) sirven como medios legibles por ordenador para un almacenamiento volátil y no volátil de datos, estructuras de datos, instrucciones ejecutables por ordenador, y así sucesivamente. Los medios legibles por ordenador pueden ser cualesquiera medios disponibles a los que se pueda acceder por medio del ordenador 702 e incluyen medios internos y/o externos volátiles y no volátiles que son extraíbles o no extraíbles. Para el ordenador 702, los medios dan cabida al almacenamiento de datos en cualquier formato digital adecuado. Debería ser apreciado por los expertos en la materia que se pueden emplear otros tipos de medios legibles por ordenador, tales como unidades zip, cinta magnética, tarjetas de memoria flash, unidades flash, cartuchos, y similares, para almacenar instrucciones ejecutables por ordenador para realizar los procedimientos novedosos de la arquitectura desvelada.

Un usuario puede interactuar con el ordenador 702, los programas y los datos usando unos dispositivos de entrada de usuario externos 728 tal como un teclado y un ratón. Otros dispositivos de entrada de usuario externos 728 pueden incluir un micrófono, un control remoto de IR (infrarrojos), una palanca de mando, un controlador para juegos, sistemas de reconocimiento por cámara, un lápiz electrónico, una pantalla táctil, sistemas de gestos (por ejemplo, el movimiento del ojo, el movimiento de la cabeza, etc.), y/o similares. El usuario puede interactuar con el ordenador 702, programas y datos usando unos dispositivos de entrada de usuario integrados 730 tales como una alfombrilla táctil, un micrófono, un teclado, etc., en los que el ordenador 702 es un ordenador portátil, por ejemplo. Estos y otros dispositivos de entrada se conectan con la unidad o unidades de procesamiento 704 a través de una interfaz o interfaces de dispositivos de entrada / salida (E / S) 732 por medio del bus de sistema 708, pero se pueden conectar mediante otras interfaces tales como un puerto paralelo, un puerto serie de IEEE 1394, un puerto de juegos, un puerto de USB, una interfaz de IR, etc. La interfaz o interfaces de dispositivos de E / S 732 también facilitan el uso de unos periféricos de salida 734 tales como impresoras, dispositivos de audio, dispositivos de cámara, y así sucesivamente, tal como una tarjeta de sonido y/o una capacidad de procesamiento de audio integrada.

Una o más interfaz o interfaces de gráficos 736 (a las que también se hace referencia por lo general como unidad de procesamiento de gráficos (GPU, *graphics processing unit*)) proporcionan señales de gráficos y de vídeo entre el ordenador 702 y pantalla o pantallas externas 738 (por ejemplo, LCD, plasma) y/o pantallas integradas 740 (por ejemplo, para ordenador portátil). La interfaz o interfaces de gráficos 736 también se puede fabricar como parte de la placa del sistema informático.

El ordenador 702 puede operar en un entorno en red (por ejemplo, basado en IP) usando conexiones lógicas por medio de un subsistema de comunicaciones cableado / inalámbrico 742 con una o más redes y/u otros ordenadores. Los otros ordenadores pueden incluir estaciones de trabajo, servidores, encaminadores, ordenadores personales, aparatos de entretenimiento basados en microprocesador, dispositivos del mismo nivel u otros nodos de red comunes y, por lo general, incluyen muchos o la totalidad de los elementos que se describen en relación con el ordenador 702. Las conexiones lógicas pueden incluir una conectividad cableada / inalámbrica con una red de área local (LAN, *local area network*), una red de área extensa (WAN, *wide area network*), una zona con cobertura inalámbrica, y así sucesivamente. Los entornos de interconexión de redes de LAN y de WAN son habituales en oficinas y empresas y facilitan redes informáticas a nivel de empresa, tales como intranets, la totalidad de las cuales pueden conectar con una red de comunicaciones global tal como Internet.

Cuando se usa en un entorno de interconexión de redes, el ordenador 702 conecta con la red por medio de un subsistema de comunicación cableado / inalámbrico 742 (por ejemplo, un adaptador de interfaz de red, un subsistema de transcepción integrado, etc.) para comunicar con redes cableadas / inalámbricas, impresoras cableadas / inalámbricas, dispositivos de entrada cableados / inalámbricos 744, y así sucesivamente. El ordenador 702 puede incluir un módem u otros medios para establecer comunicaciones a través de la red. En un entorno en red, los programas y datos en relación con el ordenador 702 se pueden almacenar en la memoria / dispositivo de almacenamiento remoto, debido a que está asociado con un sistema distribuido. Se apreciará que las conexiones de red que se muestran son a modo de ejemplo y que se pueden usar otros medios de establecimiento de un enlace de comunicaciones entre los ordenadores.

El ordenador 702 es operable para comunicar con dispositivos o entidades cableados / inalámbricos usando las tecnologías de radio tales como la familia de normas IEEE 802.xx, tales como dispositivos inalámbricos que están dispuestos de forma operativa en comunicación inalámbrica (por ejemplo, técnicas de modulación en el transcurso de la comunicación de IEEE 802.11) con, por ejemplo, una impresora, un escáner, un ordenador de escritorio y/o portátil, un asistente digital personal (PDA, *personal digital assistant*), un satélite de comunicaciones, cualquier pieza de equipo o ubicación que esté asociada con una etiqueta detectable por medios inalámbricos (por ejemplo, un kiosco, un puesto de periódicos, un baño público) y teléfono. Esto incluye al menos las tecnologías inalámbricas de Wi-Fi (o *Wireless Fidelity*, Fidelidad Inalámbrica) para zonas con cobertura inalámbrica, de WiMax y de Bluetooth™. Por lo tanto, las comunicaciones pueden ser una estructura previamente definida al igual que con una red convencional o simplemente una comunicación *ad hoc* entre al menos dos dispositivos. Las redes de Wi-Fi usan unas tecnologías de radio que se denominan IEEE 802.11x (a, b, g, etc.) para proporcionar una conectividad inalámbrica segura, fiable y rápida. Una red de Wi-Fi se puede usar para conectar ordenadores entre sí, con Internet y con redes por cable (que usan medios y funciones relacionados con IEEE 802.3).

Los aspectos ilustrados también se pueden poner en práctica en entornos informáticos distribuidos en los que determinadas tareas se realizan por medio de unos dispositivos de procesamiento remotos que están enlazados a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programa se pueden encontrar en un sistema de memoria y/o almacenamiento local y/o remoto.

Haciendo referencia a continuación a la figura 8, se ilustra un diagrama de bloques esquemático de un entorno informático 800 que es para el desarrollo, la traducción y la implementación de un modelo de conectividad. El entorno 800 incluye uno o más cliente o clientes 802. El cliente o clientes 802 pueden ser soporte físico y/o soporte lógico (por ejemplo, subprocedimientos, procedimientos, dispositivos informáticos). El cliente o clientes 802 pueden albergar una *cookie* o *cookies* y/o una información de contexto asociada, por ejemplo.

El entorno 800 también incluye uno o más servidor o servidores 804. El servidor o servidores 804 también pueden ser soporte físico y/o soporte lógico (por ejemplo, subprocedimientos, procedimientos, dispositivos informáticos). Los servidores 804 pueden albergar subprocedimientos para realizar transformaciones mediante el empleo de la arquitectura, por ejemplo. Una posible comunicación entre un cliente 802 y un servidor 804 se puede encontrar en forma de paquete de datos adaptado para transmitirse entre dos o más procedimientos informáticos. El paquete de datos puede incluir una *cookie* y/o una información de contexto asociada, por ejemplo. El entorno 800 incluye un marco de comunicación 806 (por ejemplo, una red de comunicaciones global tal como Internet) que se puede emplear para facilitar las comunicaciones entre el cliente o clientes 802 y el servidor o servidores 804.

Las comunicaciones se pueden facilitar por medio de una tecnología por cable (incluyendo fibra óptica) y/o inalámbrica. El cliente o clientes 802 están conectados de forma operativa con uno o más almacén o almacenes de datos de cliente 808 que se pueden emplear para almacenar información local con respecto al cliente o clientes 802 (por ejemplo, una *cookie* o *cookies* y/o una información de contexto asociada). De forma similar, el servidor o servidores 804 están conectados de forma operativa con uno o más almacén o almacenes de datos de servidor 810 que se pueden emplear para almacenar información local con respecto a los servidores 804.

Lo que se ha descrito en lo que antecede incluye ejemplos de la arquitectura desvelada. No es, por supuesto, posible describir cada combinación concebible de componentes y/o metodologías, pero un experto en la materia puede reconocer que son posibles muchas combinaciones y permutaciones adicionales. Por consiguiente, se tiene por objeto que la arquitectura novedosa abarque todas aquellas alteraciones, modificaciones y variaciones que caigan dentro del ámbito de las reivindicaciones adjuntas. Además, en la medida en la que se use la expresión “incluye” o bien en la descripción detallada o bien en las reivindicaciones, se tiene por objeto que tal expresión sea inclusiva de una forma similar a la expresión “comprendiendo / que comprende” tal como se interpreta “comprendiendo / que comprende” cuando se emplea como una expresión de transición en una reivindicación.

REIVINDICACIONES

1. Un sistema de gestión de redes implementado por ordenador, que comprende:

una disposición de nodos (102) de una red física;
un modelo de conectividad (106) que define una conectividad virtual entre los nodos usando la semántica de conectividad (108) y que se crea para gestionar las comunicaciones entre los nodos de la red física; y
un traductor (202) que traduce la semántica de conectividad a unas directivas e información de configuración que gestionan las comunicaciones entre los nodos de la red física.

2. El sistema de la reivindicación 1, en el que el modelo de conectividad describe una red virtual que se superpone a una capa física y es independiente de la capa física.

3. El sistema de la reivindicación 1, en el que el modelo de conectividad describe una red virtual que se superpone a una capa física e incluye elementos y abstracciones de la red física.

4. El sistema de la reivindicación 1, en el que el modelo de conectividad define seguridad de red como parte de la semántica de conectividad.

5. El sistema de la reivindicación 1, en el que la semántica de conectividad incluye identidades de máquina e identidades de usuario de los nodos.

6. El sistema de la reivindicación 1, en el que la semántica de conectividad incluye grupos de nodos y grupos de usuarios.

7. El sistema de la reivindicación 1, en el que la semántica de conectividad incluye identidades de nodo.

8. El sistema de la reivindicación 1, en el que la semántica de conectividad gestiona puertos y pasarelas de la red física.

9. Un procedimiento de gestión de redes implementado por ordenador, que comprende:

definir (500) un modelo de conectividad que describe una red virtual de conectividad entre nodos de una capa física en base a una semántica de conectividad;
gestionar (502) las comunicaciones entre los nodos de la capa física sobre en base al modelo de conectividad; y
traducir (600) la semántica de conectividad a unas directivas y reglas que gestionan las comunicaciones entre los nodos de la capa física.

10. El procedimiento de la reivindicación 9, que comprende adicionalmente aplicar la red virtual como una superposición de la capa física e independiente de la capa física.

11. El procedimiento de la reivindicación 9, que comprende adicionalmente aplicar la red virtual como una superposición de la capa física que incluye elementos y abstracciones de la capa física.

12. El procedimiento de la reivindicación 9, que comprende adicionalmente aplicar seguridad de red a la capa física como parte del modelo de conectividad.

13. El procedimiento de la reivindicación 9, que comprende adicionalmente crear una semántica de conectividad que incluye identidades de máquina e identidades de usuario de los nodos, grupos de nodos y grupos de usuarios e identidades de nodo.

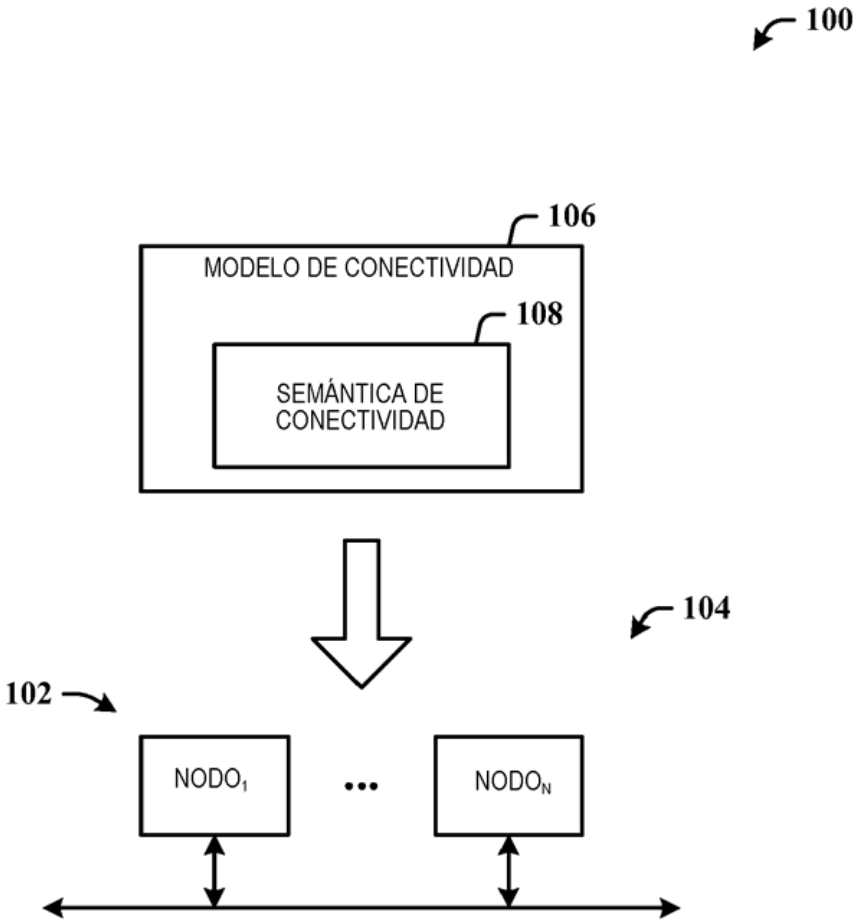
100
106
MODELO DE CONECTIVIDAD
108
SEMÁNTICA DE CONECTIVIDAD
104
102
NODO1
...
NODON

FIG. 1

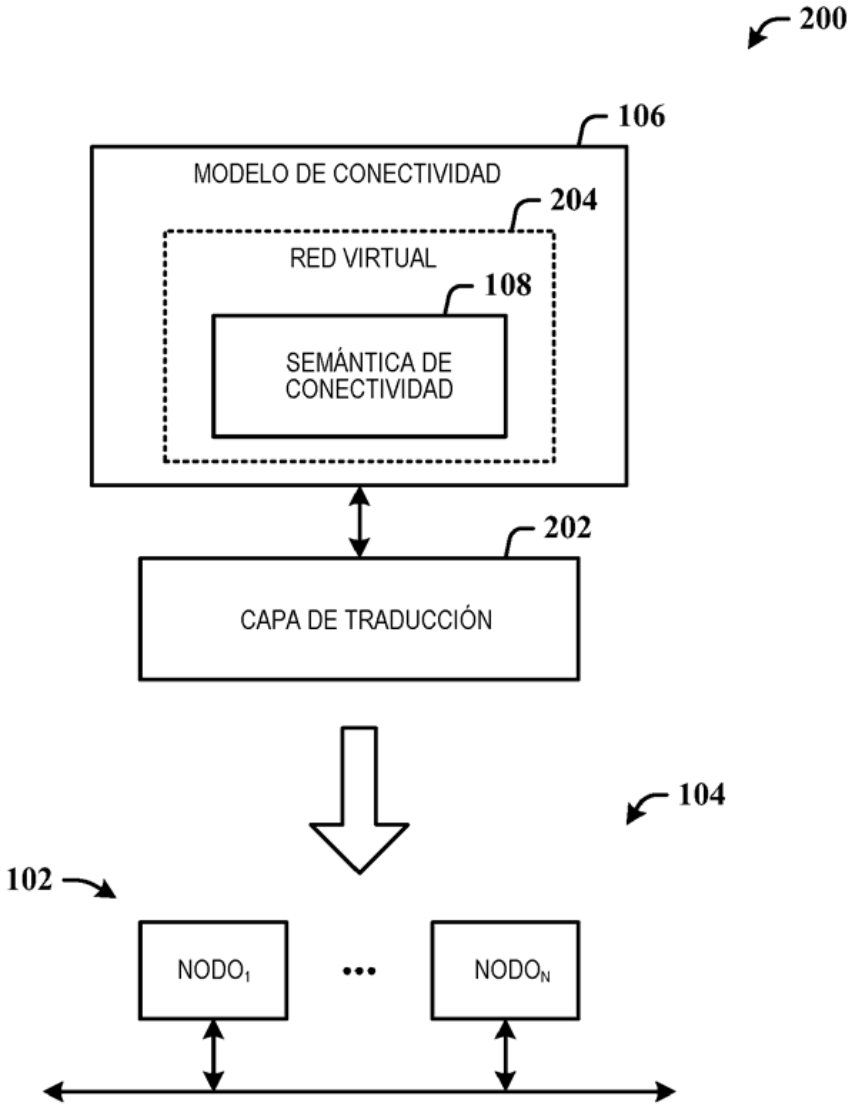
200
106
MODELO DE CONECTIVIDAD
204
RED VIRTUAL
108
SEMÁNTICA DE CONECTIVIDAD
202
CAPA DE TRADUCCIÓN
104
102
NODO1
NODON

FIG. 2

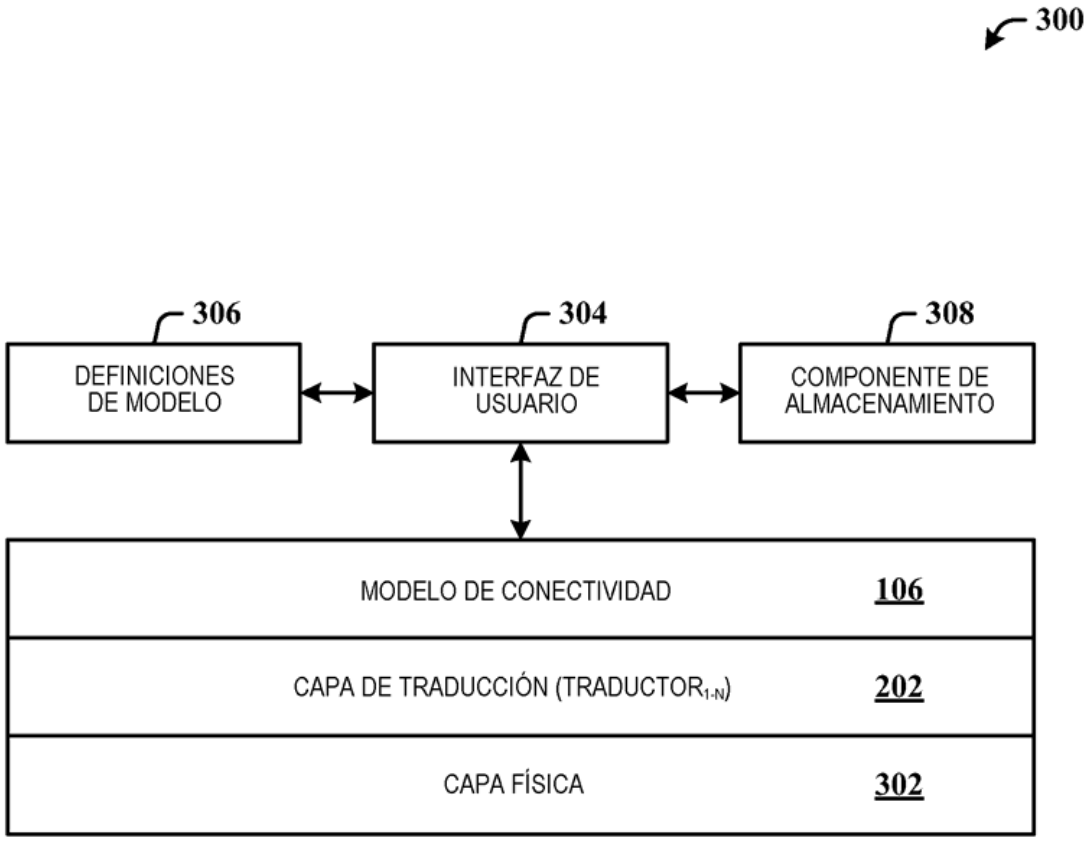
300
306
304
308
DEFINICIONES DE MODELO
INTERFAZ DE USUARIO
COMPONENTE DE ALMACENAMIENTO
MODELO DE CONECTIVIDAD
106
CAPA DE TRADUCCIÓN (TRADUCTOR1-N)
202
CAPA FÍSICA
302

FIG. 3

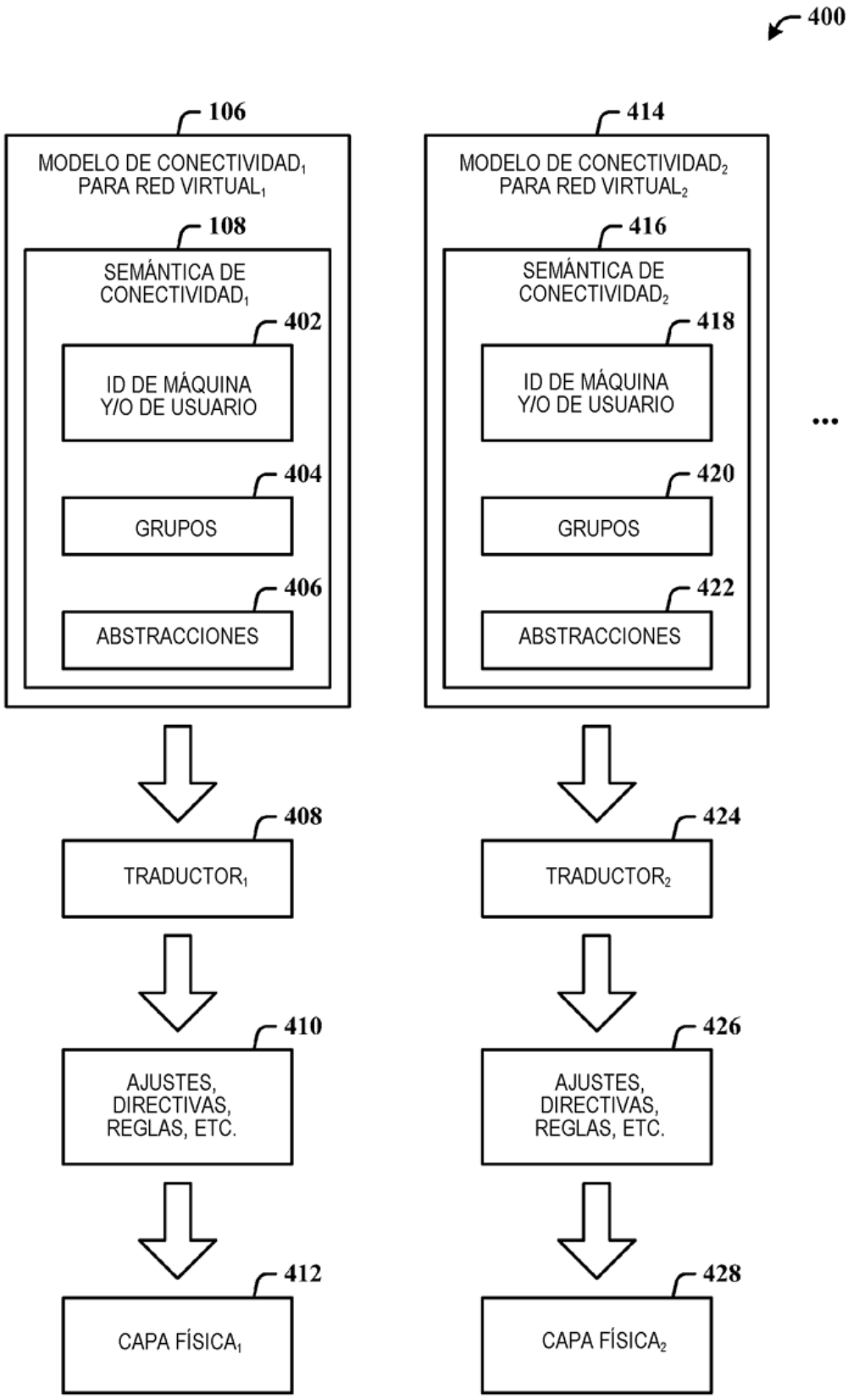
400
106
MODELO DE CONECTIVIDAD1 PARA RED VIRTUAL1
108
SEMÁNTICA DE CONECTIVIDAD1
402
ID DE MÁQUINA Y/O DE USUARIO
404
GRUPOS
406
ABSTRACCIONES
414
MODELO DE CONECTIVIDAD2 PARA RED VIRTUAL2
416
SEMÁNTICA DE CONECTIVIDAD2
418
ID DE MÁQUINA Y/O DE USUARIO
420
GRUPOS
422
ABSTRACCIONES
...
408
TRADUCTOR1
424
TRADUCTOR2
410
AJUSTES, DIRECTIVAS, REGLAS, ETC.
426
AJUSTES, DIRECTIVAS, REGLAS, ETC.
412
CAPA FÍSICA1
428
CAPA FÍSICA2

FIG. 4

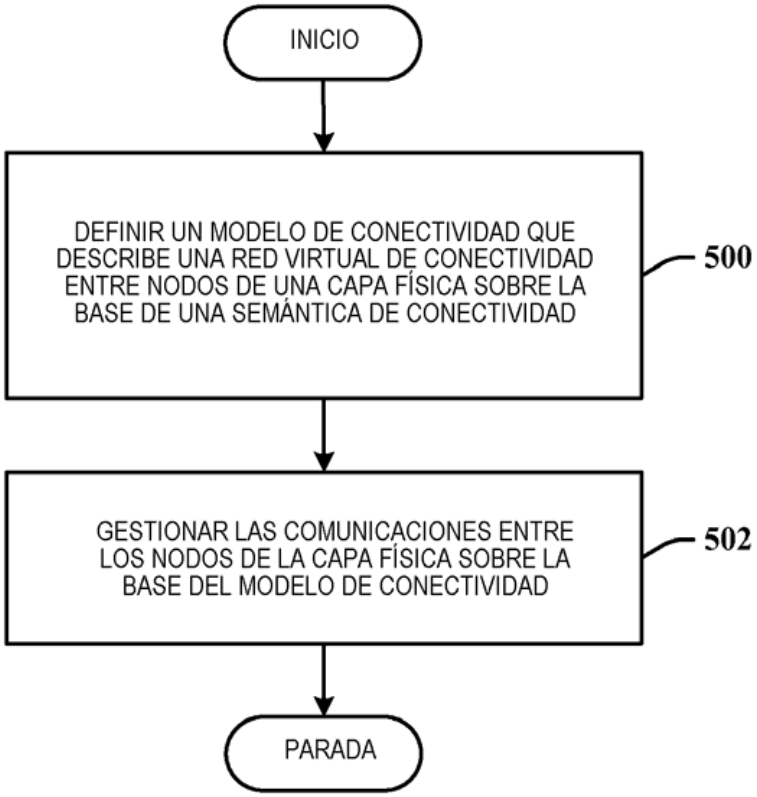
INICIO
DEFINIR UN MODELO DE CONECTIVIDAD QUE DESCRIBE UNA RED VIRTUAL DE CONECTIVIDAD ENTRE NODOS DE UNA CAPA FÍSICA SOBRE LA BASE DE UNA SEMÁNTICA DE CONECTIVIDAD
500
GESTIONAR LAS COMUNICACIONES ENTRE LOS NODOS DE LA CAPA FÍSICA SOBRE LA BASE DEL MODELO DE CONECTIVIDAD
502
PARADA

FIG. 5

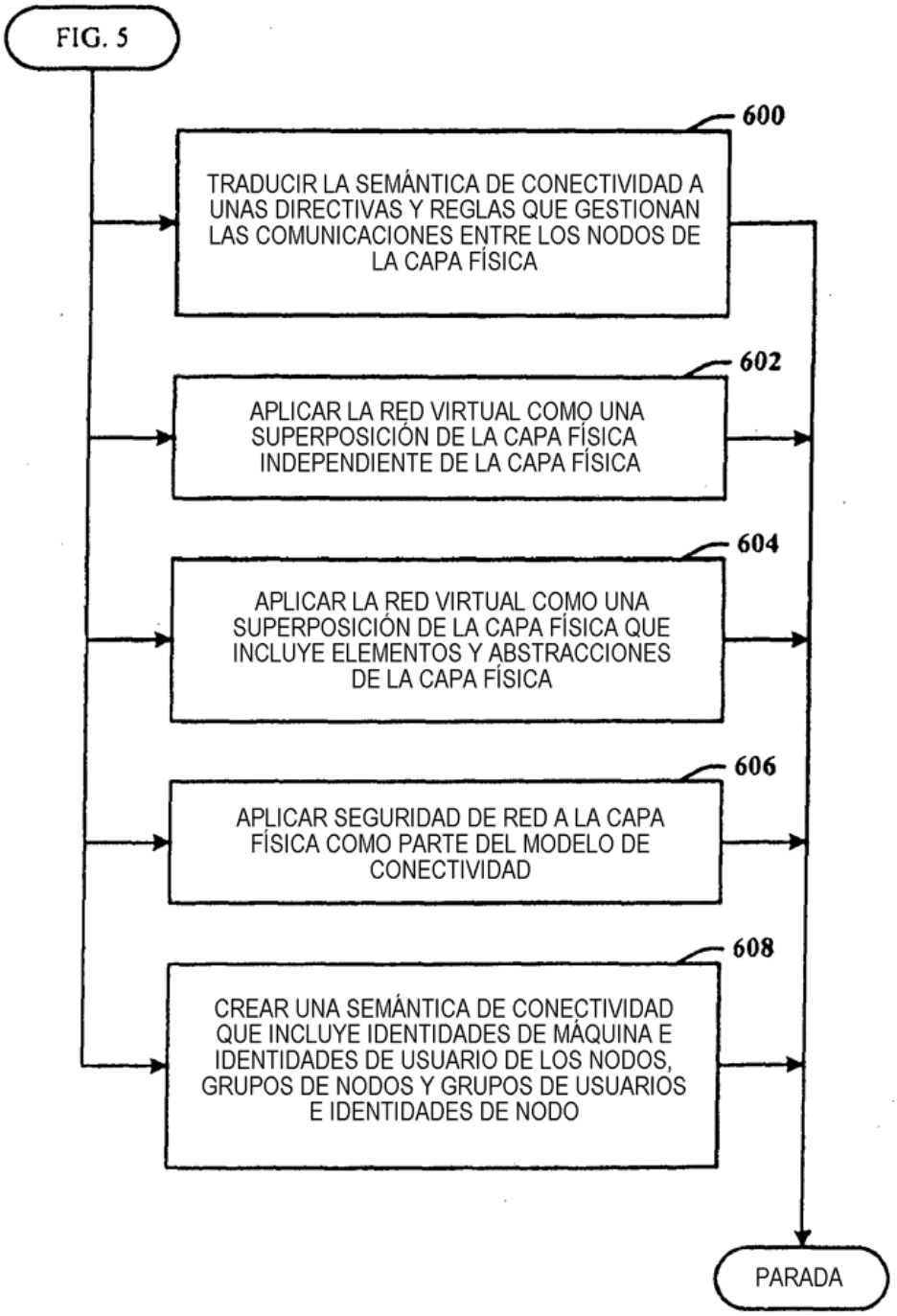
FIG. 5
600
TRADUCIR LA SEMÁNTICA DE CONECTIVIDAD A UNAS DIRECTIVAS Y REGLAS QUE GESTIONAN LAS COMUNICACIONES ENTRE LOS NODOS DE LA CAPA FÍSICA
602
APLICAR LA RED VIRTUAL COMO UNA SUPERPOSICIÓN DE LA CAPA FÍSICA INDEPENDIENTE DE LA CAPA FÍSICA
604
APLICAR LA RED VIRTUAL COMO UNA SUPERPOSICIÓN DE LA CAPA FÍSICA QUE INCLUYE ELEMENTOS Y ABSTRACCIONES DE LA CAPA FÍSICA
606
APLICAR SEGURIDAD DE RED A LA CAPA FÍSICA COMO PARTE DEL MODELO DE CONECTIVIDAD
608
CREAR UNA SEMÁNTICA DE CONECTIVIDAD QUE INCLUYE IDENTIDADES DE MÁQUINA E IDENTIDADES DE USUARIO DE LOS NODOS, GRUPOS DE NODOS Y GRUPOS DE USUARIOS E IDENTIDADES DE NODO
PARADA

FIG. 6

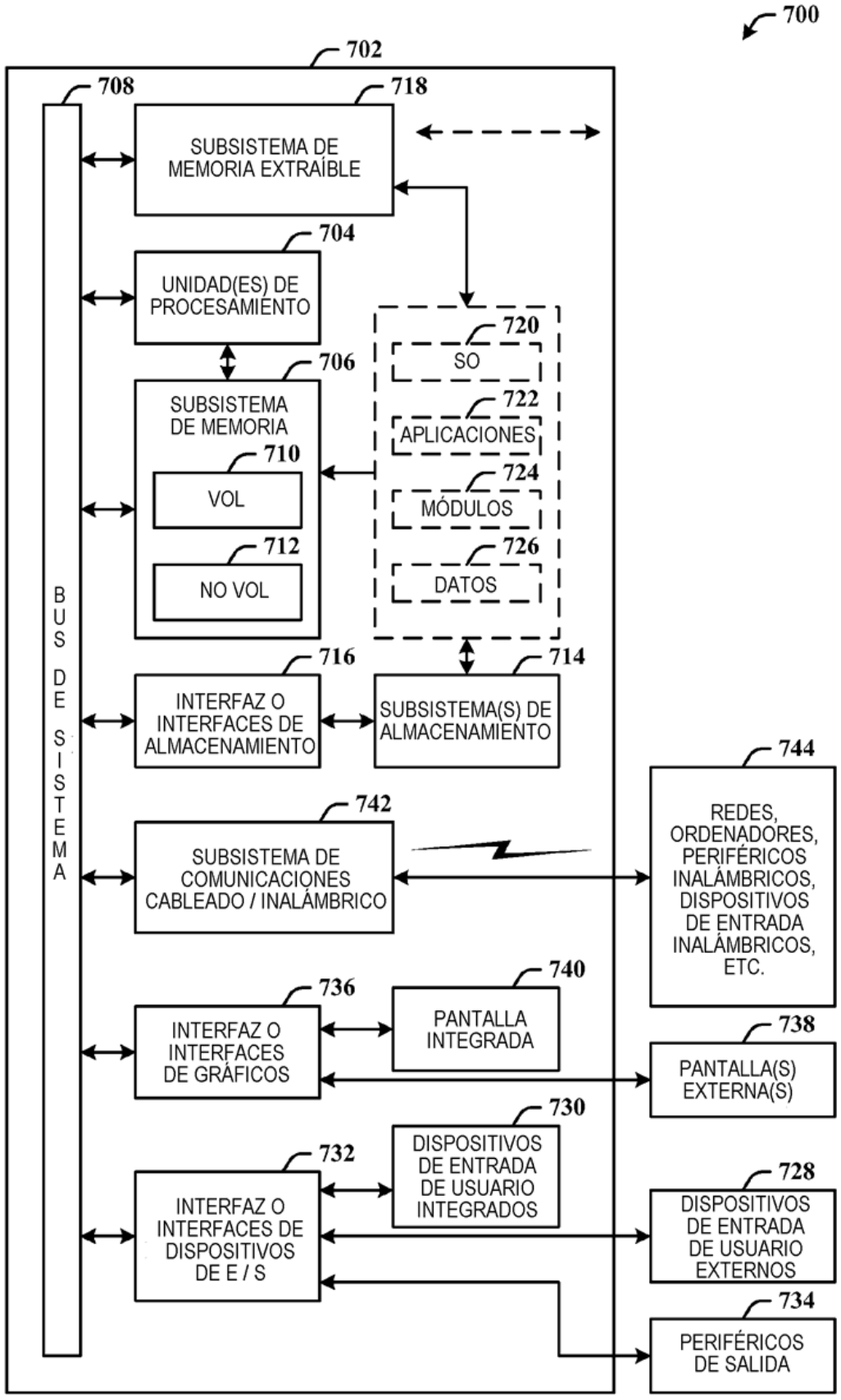
700
702
708
718
SUBSISTEMA DE MEMORIA EXTRAÍBLE
704
UNIDAD(ES) DE PROCESAMIENTO
706
SUBSISTEMA DE MEMORIA
710
VOL
712
NO VOL
720
SO
722
APLICACIONES
724
MÓDULOS
726
DATOS
716
INTERFAZ O INTERFACES DE ALMACENAMIENTO
714
SUBSISTEMA(S) DE ALMACENAMIENTO
BUS DE SISTEMA
742
SUBSISTEMA DE COMUNICACIONES CABLEADO / INALÁMBRICO
744
REDES, ORDENADORES, PERIFÉRICOS INALÁMBRICOS, DISPOSITIVOS DE ENTRADA INALÁMBRICOS, ETC.
736
INTERFAZ O INTERFACES DE GRÁFICOS
740
PANTALLA INTEGRADA
738
PANTALLA(S) EXTERNA(S)
730
DISPOSITIVOS DE ENTRADA DE USUARIO INTEGRADOS
732
INTERFAZ O INTERFACES DE DISPOSITIVOS DE E / S
728
DISPOSITIVOS DE ENTRADA DE USUARIO EXTERNOS
734
PERIFÉRICOS DE SALIDA

FIG. 7

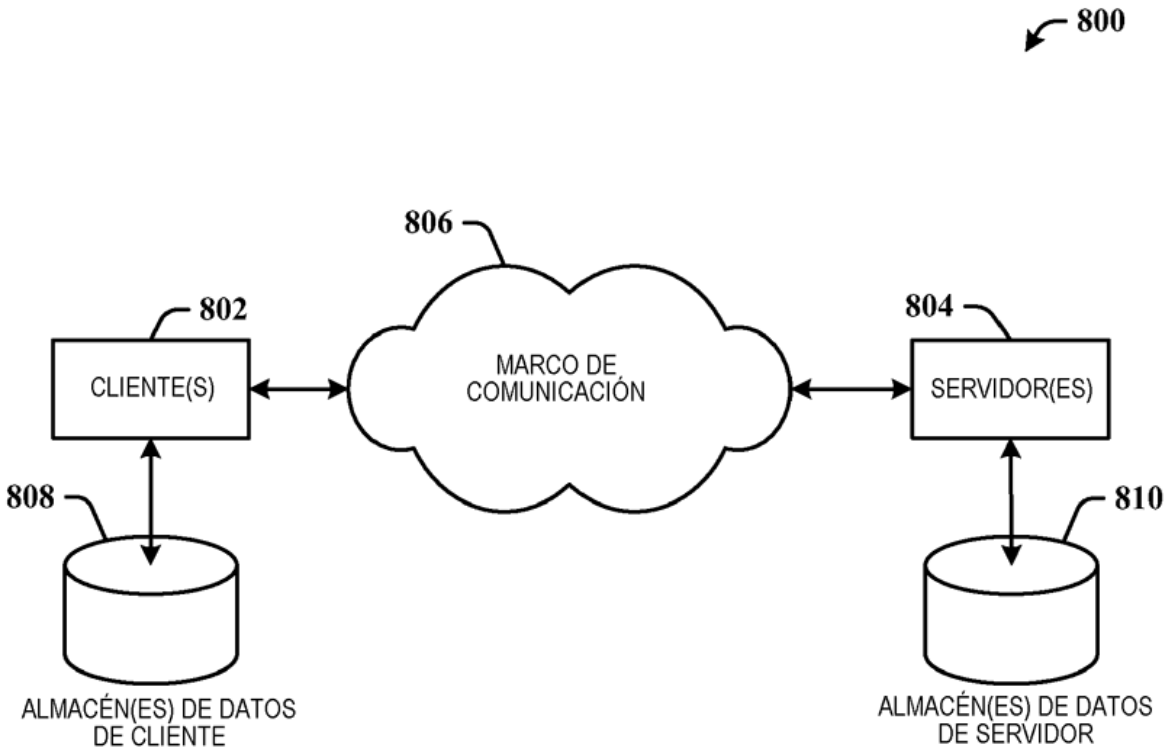
800
806
802
804
CLIENTE(S)
MARCO DE COMUNICACIÓN
SERVIDOR(ES)
808
810
ALMACÉN(ES) DE DATOS DE CLIENTE
ALMACÉN(ES) DE DATOS DE SERVIDOR

FIG. 8