(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 718 652**

(51) Int. CI.:

H04L 12/701 (2013.01)
H04L 12/717 (2013.01)
G06F 9/455 (2008.01)
H04L 12/24 (2006.01)
H04L 12/721 (2013.01)
H04L 12/741 (2013.01)
H04L 12/751 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.03.2013 PCT/JP2013/002183**

(87) Fecha y número de publicación internacional: **03.10.2013 WO13145780**

(96) Fecha de presentación y número de la solicitud europea: **29.03.2013 E 13769685 (2)**

(97) Fecha y número de publicación de la concesión europea: **02.01.2019 EP 2832058**

(54) Título: **Sistema de comunicación, aparato de control, aparato de comunicación, método de control de comunicación, y programa**

(30) Prioridad:

30.03.2012 JP 2012080279

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.07.2019

(73) Titular/es:

NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:

SONODA, KENTARO;
SHIMONISHI, HIDEYUKI;
KOIDE, TOSHIO;
HATANO, YOICHI;
NAKAE, MASAYUKI;
YAMAGATA, MASAYA;
MORITA, YOICHIRO;
SASAKI, TAKAYUKI;
ASHINO, YUKI y
OHNO, TAKEO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de comunicación, aparato de control, aparato de comunicación, método de control de comunicación, y programa

La presente invención se basa y reivindica el beneficio de la prioridad de la solicitud de patente japonesa No. 2012-080279, archivada el 30 de marzo de 2012.

La presente invención se relaciona con un sistema de comunicación, un aparato de control, un aparato de comunicación, un método de control de comunicación, y un programa. En particular, se relaciona con un sistema de comunicación, un aparato de control, un aparato de comunicación, un método de control de comunicación, y un programa para establecer un camino de reenvío de paquetes en una red.

El documento PTL (Literatura de Patente) 1, y el documento NPL (Literatura de No Patente) 1, y NPL 2 describen métodos de control de caminos de tipo gestión central que usan una técnica de OpenFlow. La técnica de OpenFlow descrita en el documento PTL 1 reconoce comunicaciones como flujos extremo a extremo, realiza control de camino en una base por flujo, y ejecuta balanceo de carga y optimización del camino.

En los documentos PTL 1, NPL 1, y NPL 2, un conmutador que sirve como un nodo de reenvío incluye un canal seguro que se comunica con un controlador (aparato de control) que calcula caminos de paquetes. El conmutador opera según una tabla de flujo establecida por el controlador. En la tabla de flujo, una combinación de una regla de correspondencia que se hace corresponder contra la información de la cabecera del paquete y una acción que describe un contenido de procesamiento aplicado a los paquetes que se corresponden con la regla de correspondencia es definida. Por ejemplo, la acción es un proceso de reenvío de un paquete a una cierta interfaz.

Cuando un conmutador descrito en los documentos PTL1, NPL1, y NPL 2 recibe un paquete, el conmutador busca en la tabla de flujo una entrada que tenga una regla de correspondencia que se corresponda con la información de la cabecera del paquete recibido. Como resultado de la búsqueda, si el conmutador encuentra una entrada que se corresponda con el paquete recibido, el conmutador ejecuta un contenido de procesamiento descrito en el campo de acción de la entrada (por ejemplo, el conmutador reenvía el paquete recibido a una cierta interfaz).

Si el conmutador no encuentra una entrada que se corresponda con el paquete como resultado de la búsqueda, el conmutador solicita al controlador establecer una entrada para el paquete recibido. En respuesta a la solicitud, el controlador calcula un camino para el paquete recibido y notifica a los conmutadores relacionados con el camino de una entrada que realiza el reenvío que usa el camino. Notificada la entrada, los conmutadores actualizan sus tablas de flujo y ejecutan los contenidos de procesamiento descritos en las entradas en las tablas de flujo actualizadas. A saber, los conmutadores reenvían los paquetes recibidos respectivos.

El documento WO-A-2011/037148 se relaciona con un sistema informático y un método de migración de una máquina virtual, y en particular con un sistema informático capaz de migrar una máquina virtual a la vez que centraliza la gestión de un entorno de red y un entorno de IT. El documento WO-A-2012/039176 describe un aparato para controlar la red de un sistema de comunicación; el aparato tiene una unidad de control de caminos que establece una ruta a un aparato de comunicación seleccionado en base a una relación de conexión entre el aparato de comunicación y un grupo de aparatos de comunicación. El documento US-A-2011/261723 describe un sistema de red que tiene un controlador que calcula una nueva ruta que no pasa a través de un nodo al cual el reenrutamiento se le instruye y genera un movimiento de prescripción de información de flujo con respecto al flujo del nodo que forma la nueva ruta.

PTL 1: Publicación Internacional No. 2008/095010
NPL 1: Nick McKeown, y otros siete, "Open-Flow: Enabling Innovation in Campus Networks," [online], [Buscado el 31 de octubre del 2011], Internet <URL:http://www.openflowswitch.org/documents/openflow-wp-latest.pdf>
NPL 2: "OpenFlow Switch Specification, Version 1.1.0 Implemented (Wire Protocol 0x02)," [Buscado el 31 de octubre del 2011], Internet <URL:http://www.openflowswitch.org/documents/openflowspec-v1.1.0.pdf>

Los siguientes análisis son dados por la presente invención. En los sistemas descritos en los documentos PTL1, NPL1, y NPL 2, si la relación de conexión entre un aparato de comunicación al cual un paquete está dirigido y un nodo de reenvío es cambiada, un conmutador necesita reenviar paquetes dirigidos al aparato de comunicación a través de un camino de reenvío en base a la relación de conexión cambiada. Sin embargo, el conmutador no tiene una regla de procesamiento para realizar tal camino de reenvío en base a la relación de conexión cambiada. Así, cuando el conmutador recibe un paquete dirigido al aparato de comunicación, el

conmutador solicita al aparato de control que establezca una regla de procesamiento para procesar el paquete recibido. En respuesta a la solicitud, el aparato de control calcula un camino de reenvío para el paquete recibido, en base a la relación de conexión cambiada.

Como se describió anteriormente, cada vez que la relación de conexión entre un aparato de comunicación al cual un paquete es dirigido y un nodo de reenvío es cambiada, el aparato de control necesita recibir una solicitud para una regla de procesamiento desde un conmutador. Esto es una causa de aumento de carga en el aparato de control.

Por lo tanto existe la necesidad en la técnica de suprimir un aumento de la carga del aparto de control mediante la reducción del número de solicitudes para reglas de procesamiento desde los conmutadores. Es un objeto de la presente invención proporcionar un sistema de comunicación, un aparato de control, un método de control de comunicación, y un programa que contribuyan a satisfacer la necesidad.

Según un primer aspecto de la presente invención, se proporciona un sistema de comunicación, como en la reivindicación 1.

Según un segundo aspecto de la presente invención, se proporciona un aparato de control, como en la reivindicación 3.

Según un tercer aspecto de la presente invención, se proporciona un método de comunicación, como en la reivindicación 5.

Según un cuarto aspecto de la presente invención, se proporciona un programa, como en la reivindicación 6.

Según la presente invención, la carga en un aparato de control que determina reglas de procesamiento para procesar paquetes dirigidos a aparatos de comunicación puede ser reducida.

Breve descripción de los dibujos

La Figura 1 ilustra una configuración de un sistema de comunicación según una realización ejemplar.
La Figura 2 ilustra una configuración de un nodo de comunicación según una realización ejemplar.
La Figura 3 ilustra una configuración de una regla de procesamiento según una realización ejemplar.
La Figura 4 ilustra una configuración de un aparato de control según una realización ejemplar.
La Figura 5 ilustra una configuración de un sistema de comunicación según una primera realización ejemplar.
La Figura 6 ilustra una configuración de un aparato de gestión de máquinas virtuales según la primera realización ejemplar.
La Figura 7 ilustra información de especificación de la máquina virtual e información de red lógica creada por el aparato de gestión de máquinas virtuales según la primera realización ejemplar.
La Figura 8 ilustra una configuración de un aparato de control según la primera realización ejemplar.
La Figura 9 ilustra una configuración de un nodo de reenvío y un nodo de reenvío virtual según la primera realización ejemplar.
La Figura 10 ilustra reglas de procesamiento establecidas en el nodo de reenvío según la primera regla ejemplar.
La Figura 11 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la primera realización ejemplar.
La Figura 12 ilustra una configuración de un sistema de comunicación según una segunda realización ejemplar.
La Figura 13 ilustra información de autenticación según la segunda realización ejemplar.
La Figura 14 ilustra una configuración de un aparto de gestión de políticas de comunicación según la segunda realización ejemplar.
La Figura 15 ilustra una política de comunicación según la segunda realización ejemplar.
La Figura 16 ilustra información de recursos según la segunda realización ejemplar.
La Figura 17 ilustra reglas de acceso según la segunda realización ejemplar.
La Figura 18 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la segunda realización ejemplar.
La Figura 19 ilustra una configuración de un sistema de comunicación según una tercera realización ejemplar.
La Figura 20 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la tercera realización ejemplar.
La Figura 21 ilustra una configuración de un sistema de comunicación según una cuarta realización ejemplar.
La Figura 22 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la cuarta realización ejemplar.
La Figura 23 es un diagrama de secuencias que ilustra otra operación del sistema de comunicación según la cuarta realización ejemplar.

Descripción de realizaciones

Primero, se describirá un esquema de una realización ejemplar con referencia a los dibujos. Como se ilustra en la Figura 1, un sistema de comunicación según una realización ejemplar incluye nodos 20-1 y 20-2 de reenvío que reenvían paquetes. Además, el sistema de comunicación incluye un aparato 10 de control que controla los caminos de reenvío de paquetes en respuesta a una solicitud desde al menos uno de los nodos 20-1 y 20-2 de reenvío. Además, el sistema de comunicación incluye un aparato 30 de comunicación como un destino de paquetes. Además, el sistema de comunicación incluye un aparato 40 de gestión de aparatos de comunicación que gestiona la relación de conexión entre los nodos 20-1 y 20-2 de reenvío y el aparato 30 de comunicación.

El aparato 10 de control controla los caminos de reenvío de paquetes en respuesta a una solicitud desde al menos una pluralidad de nodos 20-1 y 20-2 de reenvío.

Como se describió anteriormente, la técnica de OpenFlow es un ejemplo de la técnica de tipo de gestión central. La técnica de OpenFlow puede ser usada para realizar la presente invención. En adelante, una realización ejemplar en la que la técnica de OpenFlow es aplicada a la presente invención será descrita. Sin embargo, una técnica arbitraria puede ser usada para realizar la presente invención, siempre que un aparato de control (aparato de control de caminos) controle los caminos de reenvío de paquetes involucrando a una pluralidad de nodos de una forma centralizada. A saber, la presente invención no está limitada a la técnica OpenFlow.

El aparato 30 de comunicación es un aparato que puede servir como un destino de paquetes. Por ejemplo, el aparato 30 de comunicación es un servidor, un terminal móvil, o un servidor virtual.

El aparato 40 de gestión de aparatos de comunicación es un aparato que gestiona la relación de conexión entre los nodos 20 de reenvío y el aparato 30 de comunicación. Por ejemplo, el aparato 40 de gestión de aparatos de comunicación es un aparato que gestiona la relación de conexión entre los nodos 20 de reenvío y un servidor. Por ejemplo, el aparato 40 de gestión de aparatos de comunicación es un aparato que gestiona la relación de conexión entre los nodos 20 de reenvío y un terminal móvil. Por ejemplo, el aparato 40 de gestión de aparatos de comunicación es un aparato de gestión de máquinas virtuales que crea un nodo de reenvío virtual y una máquina virtual en un recurso virtual y gestiona la relación de conexión entre el nodo de reenvío virtual creado y los nodos 20 de reenvío.

Para comunicarse con el aparato 10 de control, cada uno de los nodos 20-1 y 20-2 de reenvío establece un canal de comunicación que asegura seguridad con el aparato 10 de control (líneas punteadas en la Figura 1). Cada uno de los nodos 20-1 y 20-2 de reenvío procesa un paquete entrante según una regla de procesamiento (que en adelante será referenciada como “una entrada de flujo”) adecuadamente añadida o reescrita por el aparato 10 de control.

Una configuración de cada uno de los nodos 20-1 y 20-2 de reenvío es ilustrada en la Figura 2.

La Figura 2 ilustra una configuración de cada uno de los nodos 20 de reenvío según la presente invención. Cada nodo 20 de reenvío incluye una unidad 21 de procesamiento de reenvíos que procesa un paquete entrante según una regla de procesamiento que se corresponde con el paquete entrante. Cuando recibe un paquete, la unidad 21 de procesamiento de reenvíos busca en una base de datos 22 de tabla (DB de tabla) una regla 100 de procesamiento que se corresponda con el paquete entrante. Si la unidad 21 de procesamiento de reenvíos encuentra una regla 100 de procesamiento que se corresponde con el paquete entrante, la unidad 21 de procesamiento de reenvíos procesa el paquete entrante según las instrucciones en la regla 100 de procesamiento. En constraste, si la unidad 21 de procesamiento de reenvíos no encuentra una regla de procesamiento que se corresponda con el paquete entrante, la unidad 21 de procesamiento de reenvíos solicita al aparato 10 de control establecer una regla de procesamiento para procesar el paquete entrante. En la regla 100 de procesamiento que se corresponde con el paquete entrante, si un contenido de procesamiento que indica una consulta al aparato 10 de control es definida, la unidad 21 de procesamiento de reenvíos puede consultar al aparato 10 de control según la regla de procesamiento.

Por ejemplo, la unidad 21 de procesamiento de reenvíos puede ser realizada mediante el uso de un mecanismo equivalente al conmutador de OpenFlow en el documento NPL 2.

La Figura 3 ilustra una configuración de una regla 100 de procesamiento almacenada en el nodo 20 de reenvío en la Figura 2. Dado que la Figura 3 es un ejemplo, la configuración de la regla 100 de procesamiento no está limitada a la configuración ilustrada en la Figura 3. Como se ilustra en la Figura 3, la regla 100 de procesamiento incluye campos de correspondencia. Cuando un nodo 20 de reenvío recibe un paquete, el nodo 20 de reenvío se refiere a los campos de correspondencia para buscar una regla 100 de procesamiento que se corresponda con el paquete entrante. Si el nodo 20 de reenvío encuentra una regla 100 de procesamiento que se corresponda con el paquete entrante, el nodo 20 de reenvío procesa el paquete según las instrucciones en

la regla 100 de procesamiento. Además, en base al procesamiento ejecutado en el paquete entrante, el nodo 20 de reenvío actualiza la información estadística (Contadores) en la regla 100 de procesamiento.

En contraste, si el nodo 20 de reenvío no encuentra tal regla 100 de procesamiento que se corresponda con el paquete entrante, el nodo 20 de reenvío solicita al aparato 10 de control establecer una regla de procesamiento. En base a una regla de procesamiento en la cual un contenido de procesamiento que solicita que el aparato 10 de control establezca una regla de procesamiento es definida, el nodo 20 de reenvío puede solicitar al aparato 10 de control establecer una regla de procesamiento.

Cada nodo 20 de reenvío incluye la BD 22 de tabla que almacena reglas de procesamiento. Por ejemplo la DB 22 de tabla es configurada por una base de datos capaz de almacenar al menos una tabla a la cual la unidad 21 de procesamiento de reenvíos se refiere cuando procesa un paquete entrante.

Cada nodo 20 de reenvío incluye una unidad 23 de gestión de reglas de procesamiento que gestiona reglas de procesamiento.

Una unidad 24 de comunicación es un medio de realizar comunicación con el aparato 10 de control que establece una regla de procesamiento en el nodo 20 de reenvío.

La Figura 4 ilustra una configuración del aparato 10 de control en la Figura 1. El aparato 10 de control incluye una unidad 11 de gestión de topologías, una unidad 12 de procesamiento de mensajes de control, una unidad 13 de cálculo de camino y acción, una unidad 14 de gestión de nodos de reenvío, una unidad 15 de gestión de las reglas de procesamiento, una base de datos 16 de reglas de procesamiento, y una unidad 17 de comunicación del nodo.

La unidad 11 de gestión de topologías establece información de topología de la red, en base a la relación de conexión entre los nodos 20-1 y 20-2 de reenvío recogida a través de la unidad 17 de comunicación del nodo. Si la información de topología cambia, la unidad 11 de gestión de topologías notifica a la unidad 13 de cálculo del camino y acción del cambio de la información de la topología, para causar que la unidad 13 de cálculo del camino y acción reestablezca las reglas de procesamiento existentes, por ejemplo.

La unidad 12 de procesamiento de mensajes de control analiza un mensaje de control recibido desde al menos uno de los nodos 20 de reenvío y transmite información sobre el mensaje de control a medios de procesamiento relevantes en el aparato 10 de control.

La unidad 13 de cálculo del camino y acción incluye medios para calcular un camino de reenvío de paquetes en base a la información de la topología gestionada por la unidad 11 de gestión de topologías. Además, la unidad 12 de cálculo del camino y acción sirve como medio para referirse a información sobre cada nodo 20 de reenvío gestionado por la unidad 14 de gestión de nodos de reenvío (por ejemplo, información de capacidad sobre cada nodo 20 de reenvío) y determinar un contenido de procesamiento (acción) para ser ejecutado por cada nodo 20 de reenvío. Ejemplos de la información de capacidad sobre cada nodo 20 de reenvío incluye el número de puertos de cada nodo de reenvío, los tipos de los puertos, y los tipos de las acciones soportadas. La información de capacidad no está limitada a la información anterior. A saber, información arbitraria puede ser usada como la información de capacidad.

Según una realización ejemplar, el aparato 40 de gestión de aparatos de comunicación notifica a la unidad 13 de cálculo del camino y acción del cambio de la relación de conexión entre el aparato 30 de comunicación y los nodos 20-1 y 20-2 de reenvío. En base a la notificación desde el aparato 40 de gestión de aparatos de comunicación, la unidad 13 de calculo del camino y acción determina un camino de reenvío para un paquete dirigido al aparato 30 de comunicación. La unidad 13 de cálculo del camino y acción previamente notifica al menso uno de los nodos 20-1 y 20-2 de reenvío de una regla de procesamiento para realizar el camino de reenvío determinado.

La unidad 14 de gestión de nodos de reenvío gestiona capacidades de cada nodo 20 de reenvío gestionado de este modo (por ejemplo, el número de puertos, los tipos de los puertos, y los tipos de las acciones soportadas).

La unidad 15 de gestión de las reglas de procesamiento gestiona las reglas de procesamiento establecidas en los nodos 20 de reenvío. La unidad 15 de gestión de las reglas de procesamiento almacena resultados calculados por la unidad 13 de cálculo del camino y acción en la base de datos 16 de reglas de procesamiento como reglas de procesamiento. Además, por ejemplo, si un nodo 20 de reenvío notifica al aparato 10 de control de la eliminación de una regla de procesamiento, esto es, cambio de las reglas de procesamiento establecidas en el nodo 20 de reenvío, la unidad 15 de gestión de las reglas de procesamiento actualiza el contenido de la base de datos 16 de reglas de procesamiento.

La base de datos 16 de reglas de procesamiento almacena al menos una regla de procesamiento.

La unidad 17 de comunicación del nodo se comunica con cada nodo 20 de reenvío. En la presente realización ejemplar, la unidad 17 de comunicación del nodo usa el protocolo de OpenFlow en el documento NPL 2 para comunicarse con cada nodo 20 de reenvío. Sin embargo, el protocolo de comunicación usado entre la unidad 17 de comunicación del nodo y cada nodo 20 de reenvío no está limitado al protocolo de OpenFlow.

Con la configuración anterior, si la relación de conexión entre el aparato de comunicación que sirve como un destino de paquetes y los nodos de reenvío cambia, el aparato de control previamente notifica a un nodo de reenvío (conmutador) de una regla de procesamiento para el procesamiento de paquetes dirigidos al aparato de comunicación. Cuando el nodo de reenvío (conmutador) recibe un paquete dirigido al aparato de comunicación, dado que una regla de procesamiento ya ha sido establecida, el nodo de reenvío (conmutador) no solicita al aparato de control establecer una regla de procesamiento. Así, según una realización ejemplar, dado que el número de solicitudes de reglas de procesamiento desde los conmutadores es reducida, la carga en el aparato de control puede reducirse.

<Primera realización ejemplar>

Una primera realización ejemplar será descrita con referencia a los dibujos. La Figura 5 ilustra una configuración de un sistema según una primera realización ejemplar. Como se ilustra en la Figura 5, el sistema según la primera realización ejemplar incluye un aparato 10 de control, un nodo 20 de reenvío, un recurso 300 virtual, un aparato 400 de gestión de máquinas virtuales, y un terminal 50 de usuario. El sistema puede incluir una pluralidad de nodos 20 de reenvío. El aparato 10 de control y el aparato 400 de gestión de máquinas virtuales pueden operar como aparatos separados como se ilustra en la Figura 5 o pueden operar como un único aparato.

El aparato 400 de gestión de máquinas virtuales recibe una solicitud desde el terminal 50 de usuario tal como para la creación o cambio de una configuración de una máquina virtual. En base a la solicitud, el aparato 400 de gestión de máquinas virtuales crea una máquina virtual en un recurso arbitrario.

La Figura 6 ilustra una configuración del aparato 400 de gestión de máquinas virtuales ilustrada en la Figura 5.

Como se ilustra en la Figura 6, el aparato 400 de gestión de máquinas virtuales incluye una unidad 410 de almacenamiento de información de gestión, una unidad 420 de almacenamiento de imágenes, y una unidad 430 de creación de máquinas virtuales.

La unidad 410 de almacenamiento de información de gestión incluye medios para recibir una solicitud para crear una máquina virtual desde el terminal 50 de usuario y almacenar la solicitud. En base a la solicitud recibida desde el terminal 50 de usuario, la unidad 410 de almacenamiento de información de gestión crea información sobre una red lógica configurada de manera lógica. En base a la solicitud recibida desde el terminal 50 de usuario, la unidad 410 de almacenamiento de información de gestión transmite la información de red lógica creada a la unidad 430 de creación de máquinas virtuales.

Las Figura 7(a) y 7(b) ilustran las configuraciones de información de gestión almacenadas en la unidad 410 de almacenamiento de información de gestión. Como se ilustra en las Figura 7(a) y 7(b), la unidad 410 de almacenamiento de información de gestión almacena la información de gestión como tablas.

La Figura 7(a) ilustra solicitudes recibidas desde el terminal 50 de usuario. Por ejemplo, las solicitudes recibidas desde el terminal 50 de usuario son almacenadas como información de especificación de máquina virtual. Como se ilustra en la Figura 7(a), la información de especificación de información de máquina virtual representa especificaciones de máquinas virtuales solicitadas por el terminal 50 de usuario. Por ejemplo, en la información de especificación de máquina virtual, el número de núcleos de CPU (Unidad de Procesamiento Central) y una cantidad de memoria solicitada por un usuario están asociados con una ID (Identificación) de máquina virtual y una ID de usuario. Por ejemplo, la información descrita en la segunda fila en la tabla en la Figura 7(a) significa que “un usuario que tiene una ID de usuario 0001 solicita la creación de una máquina virtual cuya ID de máquina virtual es a, número de núcleo de CPU es 2, y cantidad de memoria es 2GB”. Varios tipos de información de especificación diferente a número de núcleos de CPU y cantidad de memoria, tal como cantidad de almacenamiento y un OS (Sistema Operativo), pueden ser usados en la información de especificación de la máquina virtual.

La Figura 7(b) ilustra información sobre redes lógicas creadas en base a solicitudes recibidas desde el terminal 50 de usuario, Por ejemplo, la unidad 410 de almacenamiento de información de gestión almacena información de redes lógicas creadas en base a la información de especificación de máquina virtual. Cuando se determina un recurso en el cual una máquina virtual va a ser creada, el aparato 400 de gestión de máquinas virtuales selecciona un recurso que tiene un número mínimo de máquinas virtuales operativas o selecciona un recurso que tiene una tasa de utilización de CPU mínima, por ejemplo. El método para determinar un recurso en el cual una máquina virtual ha de ser creada no está limitado a estos métodos. Un método arbitrario puede ser usado para determinar tal recurso.

Como se ilustra en la Figura 7(b), en la información de red lógica, la ID de una máquina virtual está asociada con la ID de una red asignada a la cual la máquina virtual pertenece. La ID de red asignada es información usada para distinguir una pluralidad de redes lógicas entre ellas. La misma ID de red es asignada a la máquina virtual perteneciente a la misma red lógica. Las máquinas virtuales que tienen la misma ID de red asignada pueden comunicarse entre ellas. En contraste, dado que las máquinas virtuales que tienen diferentes ID de red asignadas pertenecen a diferentes redes lógicas, esas máquinas virtuales no pueden comunicarse entre ellas.

En la información de red lógica, la ID de una máquina virtual está asociada con la ID y el número de puerto de un nodo de reenvío virtual conectado a la máquina virtual. La información descrita en la segunda fila en la tabla en la Figura 7(b) significa que “la máquina virtual que tiene una ID de máquina virtual a pertenece a una ID de red 100, está conectada a un nodo de reenvío cuya ID es 210 y cuyo número de puerto es 1”.

La unidad 420 de almacenamiento de imágenes almacena por adelantado archivos de imágenes que son usados cuando la unidad 430 de creación de máquinas virtuales crea máquinas virtuales. Esos archivos de imágenes son datos duplicados que tienen una estructura de archivo o directorio. El terminal 50 de usuario puede almacenar archivos de imágenes usados de este modo. La unidad 420 de almacenamiento de imágenes notifica a la unidad 430 de creación de máquinas virtuales de esos archivos de imágenes.

La unidad 430 de creación de máquinas virtuales recibe la información de especificación de la máquina virtual y la información de red lógica de la unidad 410 de almacenamiento de información de gestión y los archivos de imágenes de la unidad 420 de almacenamiento de imágenes y crea máquinas virtuales. La creación de una máquina virtual puede ser realizada por un tipo arbitrario de software de creación de máquinas virtuales tal como KVM (Máquina Virtual Basada en Núcleo). Una máquina virtual es creada en base a la información de especificación de máquina virtual y es dispuesta en un recurso que tiene una ID de nodo de reenvío y un número de puerto en la información de red lógica. Tras crear una máquina virtual, la unidad 430 de creación de máquinas virtuales notifica al aparato 10 de control la información de red lógica.

Un nodo 310 de reenvío virtual y una máquina 320 virtual creada por la unidad 400 de gestión de máquinas virtuales son dispuestos en el recurso 300 virtual. Una pluralidad de nodos 310 de reenvío virtuales y máquinas 320 virtuales pueden ser dispuestos en el recurso 300 virtual. El nodo 310 de reenvío virtual es un nodo de reenvío, tal como un OpenvSwitch, realizado mediante software. Mientras que una red es realizada por una combinación de un nodo de reenvío y un nodo de reenvío virtual, en la primera realización ejemplar, una red puede ser realizada mediante solo nodos de reenvío o solo nodos de reenvío virtuales.

La Figura 8 ilustra una configuración del aparato 10 de control en la Figura 5. El aparato 10 de control recibe la información de red lógica del aparato 400 de gestión de máquinas virtuales, genera una regla de procesamiento para controlar la comunicación de paquetes, y establece la regla de procesamiento en el nodo 20 de reenvío y el nodo 310 de reenvío virtual. Cuando recibe una solicitud de establecimiento de regla de procesamiento, el aparato 10 de control crea un camino de reenvío de paquetes y una regla de procesamiento para realizar el camino de reenvío, en base a la información del paquete incluida en la solicitud de establecimiento de regla de procesamiento. El aparato 10 de control establece la regla de procesamiento creada en el nodo 20 de reenvío y el nodo 310 de reenvío virtual en el camino de reenvío.

El aparato 10 de control incluye una unidad 11 de gestión de topologías, una unidad 12 de procesamiento de mensajes de control, una unidad 13 de cálculo de camino y acción, una unidad 14 de gestión de nodos de reenvío, una unidad 15 de gestión de reglas de procesamiento, una base de datos 16 de reglas de procesamiento, una unidad 17 de comunicación del nodo, y una unidad 18 de gestión de recursos virtuales.

La unidad 11 de gestión de topologías establece información de topología de la red, en base a la información sobre el nodo 20 de reenvío recogida a través de la unidad 17 de comunicación del nodo. Si la información de la topología cambia, la unidad 11 de gestión de topologías notifica a la unidad 13 de cálculo del camino y acción del cambio de la información de la topología, para causar que la unidad 13 de cálculo del camino y acción reestablezca una regla existente, por ejemplo. La unidad 11 de gestión de topologías puede establecer información de la topología de la red, no solo en base a la información sobre el nodo 20 de reenvío sino también en base a la información sobre el nodo 310 de reenvío virtual. En este caso, el aparato 400 de gestión de máquinas virtuales notifica a la unidad 11 de gestión de topologías de la información sobre el nodo 310 de reenvío virtual. De manera alternativa, la unidad 11 de gestión topologías puede recoger la información a través de la unidad 17 de comunicación del nodo.

La unidad 12 de procesamiento de mensajes de control analiza un mensaje de control recibido desde al menos un nodo 20 de reenvío y transmite información sobre el mensaje de control a los medios de procesamiento relevantes en el aparato 10 de control.

La unidad 13 de cálculo del camino y acción incluye medios para calcular un camino de reenvío de paquetes basado en la información de la topología gestionada por la unidad 11 de gestión de topologías y la información de red lógica suministrada desde el aparato 400 de gestión de máquinas virtuales. Además, la unidad 13 de

cálculo del camino y acción sirve como medio para referir la información sobre el nodo 20 de reenvío gestionada por la unidad 14 de gestión de nodos de reenvío (por ejemplo, información de capacidad sobre cada nodo 20 de reenvío) e información sobre el nodo 310 de reenvío virtual incluida en la información de red lógica y determinar un contenido (acción) de procesamiento a ser ejecutado por el nodo 20 de reenvío y el nodo 310 de reenvío virtual.

En la realización ejemplar, el aparato 400 de gestión de máquinas virtuales notifica a la unidad de cálculo del camino y acción de la información de red lógica. Cuando es notificado de la información de red lógica, la unidad 13 de cálculo del camino y acción determina un camino de reenvío para paquetes dirigidos a la máquina 320 virtual, en base a la información sobre el nodo 20 de reenvío almacenada en la unidad 11 de gestión de topologías y la información sobre el nodo 310 de reenvío virtual incluida en la información de red lógica suministrada. La unidad 13 de cálculo del camino y acción comprende que el nodo 20 de reenvío está conectado al nodo 310 de reenvío virtual, en base a la información de capacidad sobre el nodo 20 de reenvío almacenada en la unidad 11 de gestión de topologías (por ejemplo, el número de puertos, los tipos de puertos, los tipos de acciones soportadas, etc.). Además, la unidad 13 de cálculo del camino y acción comprende que el nodo 310 de reenvío virtual está conectado con la máquina 320 virtual como un destino de paquetes, en base a las capacidades del nodo 310 de reenvío virtual incluidas en la información de red lógica (por ejemplo, el número de puertos, los tipos de los puertos, los tipos de las acciones soportadas, etc.).

En base a la información comprendida, la unidad 13 de cálculo del camino y acción calcula un camino de reenvío de paquetes desde el terminal 50 de usuario a la máquina 320 virtual y anteriormente notifica al nodo 20 de reenvío y el nodo 310 de reenvío virtual de una regla de procesamiento para realizar el camino de reenvío calculado.

La unidad 14 de gestión de nodos de reenvío gestiona capacidades del nodo 20 de reenvío gestionado de este modo (por ejemplo, el número de puertos, los tipos de los puertos, los tipos de las acciones soportadas, etc.).

La unidad 18 de gestión de recursos virtuales almacena la información de red lógica suministrada desde el aparato 400 de gestión de máquinas virtuales y gestiona las capacidades del nodo 310 de reenvío virtual gestionado de este modo (por ejemplo, el número de puertos, los tipos de los puertos, los tipos de las acciones soportadas, etc.).

La unidad 15 de gestión de reglas de procesamiento gestiona las reglas de procesamiento establecidas en el nodo 20 de reenvío. La unidad 15 de gestión de reglas de procesamiento almacena resultados calculados por la unidad 13 de cálculo del camino y acción en la base de datos 16 de reglas de procesamiento como reglas de procesamiento. Además, si el nodo 20 de reenvío notifica al aparato 10 de control de la eliminación de una regla de procesamiento y cambio de las reglas de procesamiento establecidas en el nodo 20 de reenvío, la unidad 15 de gestión de las reglas de procesamiento actualiza el contenido de la base de datos 16 de reglas de procesamiento.

La base de datos 16 de reglas de procesamiento almacena al menos una regla de procesamiento.

La unidad 17 de comunicación del nodo se comunica con el nodo 20 de reenvío y el nodo 310 de reenvío virtual. En la presente realización ejemplar, la unidad 17 de comunicación del nodo usa el protocolo de OpenFlow en el documento PTL 1 para comunicarse con el nodo 20 de reenvío y el nodo 310 de reenvío virtual. Sin embargo, el protocolo de comunicación usado entre la unidad 17 de comunicación del nodo, el nodo 20 de reenvío, y el nodo 310 de reenvío virtual no está limitado al protocolo de OpenFlow.

Las unidades anteriores (medios de procesamiento) del aparato 10 de control pueden ser realizadas mediante el uso del hardware de un ordenador que constituye el aparato 10 de control, almacenar la información anterior, y causar que un programa informático ejecute el procesamiento anterior.

La Figura 9 ilustra una configuración del nodo 20 de reenvío y del nodo 310 de reenvío virtual en la Figura 5. El nodo 310 de reenvío virtual y el nodo 20 de reenvío tienen la misma configuración. El conmutador de OpenFlow en el documento NPL 2 que opera con la entrada de flujo ilustrada en la Figura 3 como una regla de procesamiento puede ser usado como cada uno del nodo 20 de reenvío y el nodo 310 de reenvío virtual.

El nodo 20 de reenvío y el nodo 310 de reenvío virtual incluyen una unidad 21 de procesamiento de reenvíos, una base de datos 22 de tabla (DB de tabla), una unidad 23 de gestión de reglas de procesamiento, y una unidad 24 de comunicación.

La unidad 21 de procesamiento de reenvíos incluye una unidad 210 de búsqueda de tablas y una unidad 211 de ejecución de acciones, como se ilustra en la Figura 9. La unidad 210 de búsqueda de tablas busca una tabla almacenada en la BD 22 de tabla para una regla de procesamiento que tiene un campo de correspondencia que se corresponde con un paquete entrante. La unidad 211 de ejecución de acciones ejecuta procesamiento

de paquetes, según un contenido de procesamiento indicado en el campo de instrucción de la regla de procesamiento encontrada por la unidad 210 de búsqueda de tablas.

Si la unidad 210 de búsqueda de tablas no encuentra una regla de procesamiento que tiene un campo de correspondencia que se corresponda con el paquete entrante, la unidad 21 de procesamiento de reenvíos notifica a tal efecto a la unidad 23 de gestión de reglas de procesamiento. Si una consulta al aparato 10 de control es definida como un método de procesamiento de paquetes en una regla de procesamiento que tiene un campo de correspondencia que se corresponde con el paquete entrante, la unidad 21 de procesamiento de reenvíos puede notificar a tal efecto a la unidad 23 de gestión de reglas de procesamiento. Cuando es notificada por la unidad 21 de procesamiento de reenvíos, la unidad 23 de gestión de reglas de procesamiento transmite una consulta al aparato 10 de control a través de la unidad 24 de comunicación.

Dependiendo del procesamiento de paquetes, la unidad 21 de procesamiento de reenvíos actualiza la información estadística (Contadores) en la regla de procesamiento registrada en la DB 22 de tabla. La unidad 21 de gestión de reenvíos puede determinar un valor estadístico a partir de información estadística (Contadores) correspondiente a cada uno de una pluralidad de reglas de procesamiento. Por ejemplo, la unidad 21 de procesamiento de reenvíos añade información estadística correspondiente a cada uno de la pluralidad de reglas de procesamiento para calcular un valor estadístico. La unidad 23 de gestión de reglas de procesamiento compara este valor estadístico con cada condición de caducidad de las reglas de procesamiento para determinar si cada regla de procesamiento es válida. De manera alternativa, por ejemplo, la unidad 21 de procesamiento de reenvíos calcula un valor estadístico a partir de la información estadística correspondiente a una regla de procesamiento correspondiente a una condición predeterminada, entre las reglas de procesamiento almacenadas en la DB 22 de tabla. De manera alternativa, por ejemplo, la unidad 21 de procesamiento de reenvíos calcula un valor estadístico a partir de la información estadística correspondiente a una regla de procesamiento para procesar paquetes introducidos a través de un puerto predeterminado o una regla de procesamiento para sacar paquetes a un puerto predeterminado.

Por ejemplo, la DB 22 de tabla es configurada por una base de datos capaz de almacenar al menos una tabla a la cual la unidad 21 de procesamiento de reenvíos se refiere cuando procesa un paquete entrante.

La Figura 10 ilustra una tabla configurada en la DB 22 de tabla del nodo 20 de reenvío. En la Figura 10, las reglas de procesamiento para realizar la comunicación entre el terminal 50 de usuario y la máquina 320 virtual en la Figura 5 son establecidas. Por ejemplo, la dirección IP del terminal 50 de usuario es establecida como la dirección IP origen y la dirección IP de la máquina 320 virtual es establecida como la dirección IP destino en un campo de cabecera de un paquete dirigido desde el terminal 50 de usuario a la máquina 320 virtual. Así, cuando el nodo 20 de reenvío recibe un paquete dirigido a la máquina 320 virtual desde el terminal 50 de usuario, la unidad 210 de búsqueda de tablas del nodo 20 de reenvío encuentra la regla de procesamiento superior en la tabla en la Figura 10 como una regla de procesamiento que se corresponde con el paquete entrante. A continuación, según los contenidos de los campos de instrucción, las unidades 211 de ejecución de acciones del nodo 20 de reenvío y el nodo 310 de reenvío virtual reenvían el paquete entrante a través del puerto (#1) conectado al nodo 20 de reenvío y el nodo 310 de reenvío virtual. Por ejemplo, si no existe ninguna regla de procesamiento que se corresponda con el paquete entrante o si las “Instrucciones” definidas en la regla de procesamiento indican una consulta al aparato 10 de control, el nodo 20 de reenvío y el nodo 310 de reenvío virtual solicitan al aparato 10 de control establecer una regla de procesamiento.

Igualmente, por ejemplo, en un campo de cabecera de un paquete dirigido desde la máquina 320 virtual al terminal 50 de usuario, la dirección IP de la máquina 320 virtual es establecida como la dirección IP origen y la dirección IP del terminal 50 de usuario es establecida como la dirección IP destino. Así, cuando el nodo 20 de reenvío recibe un paquete dirigido desde la máquina 320 virtual al terminal 50 de usuario, la unidad 210 de búsqueda de tablas del nodo 20 de reenvío encuentra la segunda regla de procesamiento superior en la tabla en la Figura 10 como una regla de procesamiento que se corresponda con el paquete entrante. A continuación, según los contenidos de los campos de instrucción, las unidades 211 de ejecución de acciones del nodo 20 de reenvío y el nodo 310 de reenvío virtual reenvían el paquete entrante a través del puerto (#2) conectado al terminal 50 de usuario. Por ejemplo, si no existe ninguna regla de procesamiento que se corresponda con el paquete entrante o si las “Instrucciones” definidas en la regla de procesamiento indican una consulta al aparato 10 de control, el nodo 20 de reenvío y el nodo 310 de reenvío virtual solicitan al aparato 10 de control establecer una regla de procesamiento.

La unidad 23 de gestión de reglas de procesamiento es un medio de gestionar la tabla en la DB 22 de tabla. Más específicamente, la unidad 23 de gestión de reglas de procesamiento registra reglas de procesamiento especificadas por el aparato 10 de control en la DB 22 de tabla. Además, cuando es notificada por la unidad 21 de procesamiento de reenvíos de la recepción de un nuevo paquete, la unidad 23 de gestión de reglas de procesamiento solicita al aparato 10 de control establecer una regla de procesamiento para procesar el paquete entrante.

La unidad 24 de comunicación es un medio para realizar comunicaciones con el aparato 10 de control que establece una regla de procesamiento en el nodo 20 de reenvío y el nodo 310 de reenvío virtual. En la primera realización ejemplar, la unidad 24 de comunicación usa el protocolo OpenFlow en el documento NPL 2 para comunicarse con el aparato 10 de control. Sin embargo, el protocolo de comunicación usado entre la unidad 24 de comunicación y el aparato 10 de control no está limitado al protocolo OpenFlow.

La Figura 11 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la primera realización ejemplar.

El terminal 50 de usuario autentica un usuario (paso S001 en la Figura 11). La autenticación del usuario es ejecutada para identificar de manera única a un usuario. El terminal 50 de usuario puede ser una ID de usuario y una contraseña para autenticar a un usuario. De manera alternativa, el terminal 50 de usuario puede usar la dirección MAC (Control de Acceso al Medio) de un terminal de usuario usada por un usuario. A saber, un método arbitrario puede ser usado para autenticar a un usuario. Para la autenticación del usuario, un aparato de autenticación dedicado (no ilustrado) que ejecuta procesamiento de autenticación puede ser usado. De manera alternativa, el aparato 400 de gestión de máquinas virtuales puede ejecutar procesamiento de autenticación.

A continuación, el terminal 50 de usuario solicita al aparato 400 de gestión de máquinas virtuales crear una máquina virtual (paso S002 en la Figura 11).

Según la solicitud desde el terminal 50 de usuario, el aparato 400 de gestión de máquinas virtuales crea una máquina 320 virtual (paso S003 en la Figura 11) y dispone la máquina 320 virtual en un recurso 300 virtual especificado (paso S004 en la Figura 11). La máquina 320 virtual es dispuesta en el recurso 300 virtual (paso S005 en la Figura 11). El aparato 400 de gestión de máquinas virtuales forma una red a la que pertenece la máquina 320 virtual creada (paso S006 en la Figura 11).

El aparato 400 de gestión de máquinas virtuales comprueba la ID del usuario usada para la autenticación del usuario con las ID de usuarios en la información de especificación de la máquina virtual almacenada en la unidad 410 de almacenamiento de información de gestión. Si la información de especificación de la máquina virtual incluye la ID del usuario, el aparato 400 de gestión de máquinas virtuales notifica al aparato 10 de control la información de red lógica (paso S007 en la Figura 11).

Si la información de especificación de la máquina virtual no incluye la ID del usuario, el aparato 400 de gestión de máquinas virtuales registra una nueva ID de red asignada para la ID del usuario en la información de red lógica y notifica al aparato 10 de control de la información de red lógica en la cual la ID de red asignada ha sido registrada (paso S007 en la Figura 11).

El aparato 10 de control recibe información sobre la red asignada de la máquina virtual desde el aparato 400 de gestión de máquinas virtuales y crea una regla de procesamiento según la información de red asignada (paso S008 en la Figura 11).

El aparato 10 de control notifica al nodo 20 de reenvío y el nodo 310 de reenvío virtual de la regla de procesamiento creada (ModoFlujo en el paso S009 en la Figura 11).

El nodo 20 de reenvío y el nodo 310 de reenvío virtual reciben la regla de procesamiento desde el aparato 10 de control y establecen la regla de procesamiento (paso S010 en la Figura 11).

El aparato 400 de gestión de máquinas virtuales puede crear una máquina virtual primero o notificar al aparato 10 de control de la información de red lógica primero. De manera alternativa, esos pasos pueden ser ejecutados de manera simultánea.

El terminal 50 de usuario transmite un paquete dirigido a la máquina 320 virtual (paso S011 en la Figura 11).

El paquete transmitido desde el terminal 50 de usuario es reenviado de manera secuencial al nodo 20 de reenvío y el nodo 310 de reenvío virtual. El nodo 20 de reenvío y el nodo 310 de reenvío virtual determinan el reenvío del paquete según la regla de procesamiento establecida por el aparato 10 de control y reenvían el paquete (paso S012 en la Figura 11).

En la primera realización ejemplar, si el aparato 400 de gestión de máquinas virtuales notifica al aparato 10 de control información sobre la relación de conexión entre la máquina 320 virtual y el nodo 310 de reenvío virtual, el aparato 10 de control notifica previamente al nodo 20 de reenvío y el nodo 310 de reenvío virtual de una regla de procesamiento para procesar paquetes dirigidos a la máquina 320 virtual. Si el nodo 20 de reenvío o el nodo 310 de reenvío virtual reciben un paquete dirigido a la máquina 320 virtual, dado que la regla de procesamiento ya ha sido establecida, el nodo 20 de reenvío o el nodo 310 de reenvío virtual no solicitan al aparato 10 de control una regla de procesamiento. Así, según la primera realización ejemplar, dado que el

número de solicitudes de reglas de procesamiento desde el nodo 20 de reenvío o el nodo 310 de reenvío virtual es reducido, la carga en el aparato de control puede ser reducida.

<Segunda realización ejemplar>

Una segunda realización ejemplar será descrita con referencia a los dibujos. Un aparato 60 de autenticación y un aparato 70 de gestión de políticas de comunicación son incluidos en un sistema de comunicación según la segunda realización ejemplar.

En la segunda realización ejemplar, el aparato 60 de autenticación autentica al terminal 50 de usuario. El aparato 70 de gestión de políticas de comunicación determina una regla de acceso que indica autorización de acceso de la máquina 320 virtual creada por el terminal 50 de usuario con respecto a otras máquinas virtuales.

En la segunda realización ejemplar, el terminal 50 de usuario transmite una instrucción para cambiar una regla de acceso al aparato 70 de gestión de políticas. En base a la instrucción de cambio de una regla de acceso, el aparato 70 de gestión de políticas de comunicación determina una nueva regla de acceso. En base a la nueva regla de acceso, el aparato 10 de control reestablece el camino de reenvío desde el terminal 50 de usuario a la máquina 320 virtual. El aparato 10 de control establece previamente una regla de procesamiento para realizar el restablecimiento del camino de reenvío en el nodo 20 de reenvío y el nodo 310 de reenvío virtual.

Así, en la segunda realización ejemplar, dado que el aparato 70 de gestión de las políticas de comunicación es dispuesto, el aparato 70 de gestión de las políticas de comunicación puede recibir una instrucción para cambiar una regla de acceso desde el terminal 50 de usuario y previamente establecer una regla de procesamiento basada en la instrucción de cambio en el nodo 20 de reenvío y el nodo 310 de reenvío virtual.

La Figura 12 ilustra una configuración del sistema de comunicación según la segunda realización ejemplar. Como se ilustra en la Figura 12, la segunda realización ejemplar es diferente de la primera realización ejemplar en que el sistema de comunicación según la segunda realización ejemplar incluye el aparato 60 de autenticación y el aparato 70 de gestión de políticas de comunicación. Dado que otros elementos son los mismos entre la primera y la segunda realización, la segunda realización ejemplar será descrita con foco en la diferencia.

El aparato 60 de autenticación es un aparato para autenticar al terminal 50 de usuario. Por ejemplo, en respuesta a una solicitud desde el terminal 50 de usuario, el aparato 60 de autenticación autentica al terminal 50 de usuario. El terminal 50 de usuario transmite una instrucción para cambiar una regla de acceso solicitándolo al aparato 60 de autenticación.

Mientras que el terminal 50 de usuario transmite una instrucción para cambiar una regla de acceso a través del aparato 60 de autenticación en la segunda realización ejemplar, el terminal 50 de usuario puede directamente dar una instrucción para cambiar una regla de acceso al aparato 70 de gestión de políticas de comunicación.

La Figura 13 ilustra información de autenticación transmitida al aparato 70 de gestión de políticas de comunicación cuando el aparato 60 de autenticación tiene éxito en la autenticación del terminal 50 de usuario. Por ejemplo, cuando tiene éxito al autenticar al terminal 50 de usuario, el aparato 60 de autenticación notifica al aparato 70 de gestión de políticas de comunicación de información de autenticación en la cual una ID de usuario, una ID de rol, e información de atributo están asociadas entre ellas.

La ID de usuario es un identificador para identificar al terminal 50 de usuario.

La ID de rol es un identificador para identificar información sobre el control de acceso. Si la ID de rol es rol_0001, por ejemplo, el acceso a grupos de recursos que tienen ID de grupos de recursos grupo_recurso_0001 y grupo_recurso_0002 es permitido. La relación de correspondencia entre la ID de rol y la información sobre el control de acceso es almacenada en la unidad 71 de almacenamiento de políticas de comunicación del aparato 70 de gestión de políticas de comunicación (Figura 14). Un grupo de recursos es un grupo de una pluralidad de recursos virtuales. Una ID de grupo de recursos es un identificador para distinguir grupos de recursos entre ellos.

La información de atributo es información sobre una máquina virtual creada por el terminal 50 de usuario (por ejemplo, una dirección IP o una dirección MAC).

Por ejemplo, como se ilustra en la Figura 13, cuando el aparato 60 de autenticación tiene éxito en la autenticación del terminal de usuario que tiene ID 0001, el aparato 60 de autenticación notifica al aparato 70 de gestión de políticas de comunicación de 0001 como la ID de usuario, rol_0001 como la ID del rol, la dirección IP 192.168.100.1 y la dirección MAC 00-00-00-44-55-66 como la información de atributo.

En respuesta a la solicitud desde el terminal 50 de usuario, el aparato 60 de autenticación notifica al aparato 70 de gestión de políticas de comunicación de nueva información de autenticación. Por ejemplo, en respuesta a la

solicitud desde el terminal 50 de usuario, el aparato 60 de autenticación notifica al aparato 70 de gestión de políticas de comunicación de información de autenticación que incluye una ID de rol cambiada a rol_0002. A saber, por ejemplo, en respuesta a la solicitud desde el terminal 50 de usuario, el aparato 60 de autenticación notifica al aparato 70 de gestión de políticas de comunicación de 0001 como la ID de usuario, rol_0002 como la ID de rol, y dirección IP 102.168.100.1 y dirección MAC 00-00-00-44-55-66 como la información de atributo.

La información de autenticación no está limitada al ejemplo en la Figura 13. Información arbitraria puede ser usada siempre que el aparato 70 de gestión de políticas de comunicación pueda determinar una regla de acceso para el terminal 50 de usuario en base a la información. Por ejemplo, la información de autenticación puede incluir información posicional del terminal 50 de usuario. Además, la información transmitida desde el aparato 60 de autenticación al aparato 70 de gestión de políticas de comunicación no está limitada a la información de autenticación. La ID de usuario, la ID de rol, y la información posicional del terminal 50 de usuario pueden ser usadas.

Como se ilustra en la Figura 12, en la segunda realización ejemplar, el sistema de comunicación incluye el aparato 70 de gestión de políticas de comunicación. Este aparato 70 de gestión de políticas de comunicación determina una regla de acceso que indica autorización de acceso de la máquina 320 virtual creada por el terminal 50 de usuario con respecto a la otra máquina virtual.

La Figura 14 ilustra una configuración del aparato 70 de gestión de políticas de comunicación en la Figura 12.

Como se ilustra en la Figura 14, el aparato 70 de gestión de políticas comunicación incluye la unidad 71 de almacenamiento de políticas de comunicación y una unidad 72 de control de políticas.

La unidad 71 de almacenamiento de políticas de comunicación almacena políticas de comunicación e información de recursos.

La Figura 15 ilustra políticas de comunicación almacenadas en la unidad 71 de almacenamiento de políticas de comunicación. Como se ilustra en la Figura 15, la unidad 71 de almacenamiento de políticas de comunicación almacena una ID de grupo de recursos e información de control de acceso correspondiente al grupo de recursos por ID de rol. Por ejemplo, cuando la información de control de acceso representa permitido, el acceso está permitido, y cuando la información de control de acceso represente denegado, el acceso es rechazado. Por ejemplo, la política de comunicación en la segunda fila en la Figura 15 indica que una máquina virtual que tiene ID de rol rol_0001 se le permite (permitido) el acceso al grupo de recursos que tiene la ID de grupo de recursos grupo_recursos_0002. Igualmente, por ejemplo, la política de comunicación en la tercera fila en la Figura 15 indica que una máquina virtual que tiene una ID de rol rol_0002 no le está prohibido el acceso al grupo de recursos que tiene la ID de grupo de recursos grupo_recursos_0001.

La Figura 16 ilustra información de recursos almacenada en la unidad 71 de almacenamiento de políticas de comunicación. Como se ilustra en la Figura 16, la unidad 71 de almacenamiento de políticas de comunicación almacena, por ID de grupo de recursos, recursos virtuales incluidos en un grupo de recursos e información sobre los recursos virtuales que están asociados entre ellos. En la Figura 16, por ejemplo, la unidad 71 de almacenamiento de políticas de comunicación almacena un grupo de recursos identificado mediante la ID de grupo de recursos grupo_recurso_0001 y el grupo de recursos está asociado con recurso_0001, recurso_0002, y recurso_0003 como recursos indicados en el grupo. Además, la unidad 71 de almacenamiento de políticas de comunicación almacena información sobre cada uno de los recursos (por ejemplo, direcciones IP, direcciones MAC, y números de puertos usados para servicios).

En base a tal política de comunicación e información de recursos almacenada en la unidad 71 de almacenamiento de políticas de comunicación e información de autenticación suministrada desde el aparato 400 de gestión de máquinas virtuales, la unidad 72 de control de políticas crea una regla de acceso sobre la autorización de acceso de la máquina 320 virtual creada por el terminal 50 de usuario. La unidad 72 de control de políticas notifica al aparato 10 de control de la regla de acceso creada.

La Figura 17 ilustra reglas de acceso que indican autorización de acceso de la máquina 320 virtual creada por la unidad 72 de control de políticas con respecto a otras máquinas virtuales. En un campo origen en la Figura 17, información sobre la máquina 320 virtual, creación de la cual es solicitada por el terminal 50 de usuario, es almacenada (por ejemplo, una dirección IP o una dirección MAC). La información almacenada en el campo origen es creada a partir del campo atributo en la información de autenticación transmitida desde el aparato 60 de autenticación al aparato 70 de gestión de políticas.

En un campo destino en la Figura 17, información sobre un recurso virtual es almacenada (por ejemplo, la dirección IP del recurso, la dirección MAC del recurso, o información de recursos sobre un número de puerto usado para un servicio). La información almacenada en el campo destino es creada a partir del campo de atributo de recurso en la información de recurso almacenada en la unidad 71 de almacenamiento de políticas de comunicación.

En un campo de autoridad de acceso en la Figura 17, información sobre el control de acceso es almacenada. La información almacenada en el campo de autoridad de acceso es creada a partir del campo de autoridad de acceso en las políticas de comunicación almacenadas en la unidad 71 de almacenamiento de políticas de comunicación.

En un campo condición (opción) en la Figura 17, por ejemplo, un número de puerto usado para un servicio establecido en el campo atributo de recurso en la información de recurso almacenada en la unidad 71 de almacenamiento de políticas de comunicación es establecido.

Por ejemplo, como se ilustra en la cuarta fila en la tabla en la Figura 17, la unidad 72 de control de políticas crea una regla de acceso que indica que una máquina virtual que tiene dirección origen 192.168.100.1 está prohibida (denegada) para comunicarse con una máquina virtual que tiene una dirección destino 102.168.0.3 y notifica al aparato 10 de control de la regla de acceso.

Si el cambio de una máquina virtual dispuesta en un recurso 300 virtual es causado, la unidad 72 de control de políticas actualiza una política de comunicación correspondiente e información de recursos almacenada en la unidad 71 de almacenamiento de políticas. Por ejemplo, cuando la unidad 72 de políticas de control es notificada de información de red lógica mediante el aparato 400 de gestión de máquinas virtuales y reconoce un cambio de un recurso en un grupo de recursos, la unidad 72 de control de políticas actualiza la relación correspondiente entre la ID del grupo de recursos y la ID de recurso incluida en la información de recurso.

Por ejemplo, el aparato 70 de gestión de políticas de comunicación según la segunda realización ejemplar crea, modifica, y elimina políticas, en respuesta a una solicitud desde el terminal 50 de usuario. Tal mecanismo de gestión de políticas de comunicación (sistema de gestión de políticas) puede ser proporcionado como un sistema basado en Web o una aplicación que opera en un PC (Ordenador Personal) separado. Además, el mecanismo de gestión de políticas del aparato 70 de gestión de políticas de comunicación puede ser proporcionado a través de una aplicación que usa GUI (Interfaz de Usuario Gráfica). De manera alternativa, una CLI (Interfaz de Línea de Comandos) o un modo arbitrario pueden ser usados.

Cuando es notificado de una regla de acceso por el aparato 70 de gestión de políticas de comunicación, el aparato 10 de control calcula un camino de reenvío del paquete basado en la regla de acceso y determina una regla de procesamiento para realizar el camino de reenvío calculado. El aparato 10 de control notifica al nodo 20 de reenvío y el nodo 310 de reenvío virtual de la regla de procesamiento determinada. El aparato 10 de control puede establecer un periodo válido en la regla de procesamiento determinada. En tal caso, el aparato 10 de control establece el periodo válido tal que, cuando el periodo válido pasa después de la regla de procesamiento es establecida en el nodo 210 de reenvío y el nodo 310 de reenvío virtual o después de que un paquete que se corresponde con la regla de correspondencia es recibido el último, la regla de procesamiento es inválida o eliminada.

Una operación del sistema de comunicación según la segunda realización ejemplar será descrita con referencia a los dibujos. La Figura 18 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la segunda realización ejemplar. En la operación en la Figura 18, el terminal 50 de usuario transmite una instrucción para cambiar una regla de acceso mediante la solicitud al aparato 60 de autenticación.

En la Figura 18, el terminal 50 de usuario solicita al aparto 60 de autenticación que ejecute la autenticación (paso S101 en la Figura 18). El aparato 60 de autenticación autentica al usuario del terminal 50 de usuario (paso S102 en la Figura 18). Si el aparato 60 de autenticación tiene éxito en la autenticación del terminal 50 de usuario, el aparato 60 de autenticación transmite información de autenticación al aparato 70 de gestión de políticas de comunicación (paso S103 en la Figura 18).

En base a la información de autenticación suministrada y la política de comunicación e información de recursos almacenada en la unidad 71 de almacenamiento de políticas de comunicación, el aparato 70 de gestión de políticas de comunicación crea una regla de acceso sobre acceso de la máquina 320 virtual creada en respuesta a una solicitud del terminal 50 de usuario (paso S104 en la Figura 18). El aparato 70 de gestión de políticas de comunicación transmite la regla de acceso creada al aparato 10 de control (paso S105 en la Figura 18).

Cuando es notificado de la regla de acceso por el aparato 70 de gestión de políticas de comunicación, el aparato 10 de control calcula un camino de reenvío de paquetes basado en la regla de acceso y determina una regla de procesamiento para realizar el camino de reenvío calculado (paso S106 en al Figura 18). El aparato 10 de control notifica al nodo 20 de reenvío y al nodo 310 de reenvío virtual de la regla de procesamiento determinada (ModoFlujo en paso S107 en la Figura 18).

El nodo 20 de reenvío y el nodo 310 de reenvío virtual reciben la regla de procesamiento desde el aparato 10 de control y establecen la regla de procesamiento (paso S108 en la Figura 18).

El terminal 50 de usuario transmite un paquete dirigido a la máquina 320 virtual (paso S109 en la Figura 18).

El paquete transmitido desde el terminal 50 de usuario es reenviado de manera secuencial al nodo 20 de reenvío y al nodo 310 de reenvío virtual. El nodo 20 de reenvío y el nodo 310 de reenvío virtual reenvían el paquete según la regla de procesamiento establecida por el aparato 10 de control (paso S110 en la Figura 18).

Como se describió anteriormente, el sistema de comunicación según la segunda realización ejemplar incluye el aparato 70 de gestión de políticas de comunicación. Si el aparato 70 de gestión de políticas de comunicación recibe una instrucción para cambiar una regla de acceso desde el terminal 50 de usuario, una regla de procesamiento basada en la instrucción de cambio puede ser establecida previamente en el nodo 20 de reenvío y el nodo 310 de reenvío virtual. Así, según la segunda realización ejemplar, dado que el número de solicitudes para reglas de procesamiento desde el nodo 20 de reenvío o el nodo 310 de reenvío virtual es reducido, la carga en el aparato de control puede ser reducida.

<Tercera realización ejemplar>

Una tercera realización ejemplar es realizada mediante la adición de un aparato 80 de movimiento de máquinas virtuales al sistema de comunicación según la segunda realización ejemplar. En la tercera realización ejemplar, dado que el aparato 80 de movimiento de máquinas virtuales es dispuesto, un sistema capaz de mover una máquina virtual entre recursos virtuales puede ser provisto.

La tercera realización ejemplar será descrita con referencia a los dibujos.

La Figura 19 ilustra una configuración de un sistema de comunicación según la tercera realización ejemplar. Como se ilustra en la Figura 19, la segunda y tercera realizaciones ejemplares son diferentes en que el aparato 80 de movimiento de máquinas virtuales es añadido al sistema de comunicación según la tercera realización ejemplar. Dado que otros elementos son los mismos entre la segunda y la tercera realizaciones ejemplares, la tercera realización ejemplar será en adelante descrita con un foco en la diferencia.

Por ejemplo, en respuesta a una solicitud desde un terminal 50 de usuario o en base a un estado operacional del recurso 300 virtual, el aparato 80 de movimiento de máquinas virtuales mueve la máquina 320 virtual incluida en el recurso 300 virtual a otro recurso 900 virtual.

En respuesta a una solicitud de movimiento de la máquina 320 virtual, el aparato 80 de movimiento de máquinas virtuales notifica al aparato 400 de gestión de máquinas virtuales de información sobre el destino de la máquina 320 virtual. La información sobre el destino de la máquina 320 virtual es la ID de máquina virtual de una máquina virtual que se solicita sea movida por el terminal 50 de usuario. La información sobre el destino no está limitada a la ID de la máquina virtual. Información arbitraria puede ser usada, siempre que la información pueda identificar la máquina virtual que se solicita se mueva por el terminal 50 de usuario.

Cuando la unidad 430 de creación de máquinas virtuales del aparato 400 de gestión de máquinas virtuales recibe la información sobre el destino de la máquina 320 virtual desde el aparato 80 de movimiento de máquinas virtuales, la unidad 430 de creación de máquinas virtuales se refiere al destino de la máquina 320 virtual.

Tras determinar el destino de la máquina 320 virtual, el aparato 400 de gestión de maquinas virtuales mueve la máquina 320 virtual al recurso 900 virtual destino. Tras mover la máquina 320 virtual, el aparato 400 de gestión de máquinas virtuales actualiza la información de red lógica. El aparato de gestión de máquinas virtuales notifica al aparato 10 de control de la información de red lógica actualizada.

Una operación del sistema de comunicación según la tercera realización ejemplar será descrita con referencia a los dibujos. La Figura 20 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la tercera realización ejemplar.

El terminal 50 de usuario usa el aparato 60 de autenticación para autenticación de usuarios (paso S201 en la Figura 20).

A continuación, el terminal 50 de usuario transmite una solicitud al aparato 80 de movimiento de máquinas virtuales para mover una máquina virtual (paso S202 en la Figura 20).

En respuesta a una solicitud para mover la máquina 320 virtual, el aparato 80 de movimiento de máquinas virtuales notifica al aparato 400 de gestión de máquinas virtuales de información sobre el destino de la máquina 320 virtual (paso S203 en la Figura 20).

Cuando la unidad 430 de creación de máquinas virtuales del aparato 400 de gestión de máquinas virtuales recibe la información sobre el destino de la máquina 320 virtual desde el aparato 80 de movimiento de máquinas virtuales, la unidad 430 de creación de máquinas virtuales se refiere a la información de red lógica almacenada en la unidad 410 de almacenamiento de información de gestión y determina el destino de la máquina 320 virtual (paso S204 en la Figura 20).

El aparato 400 de gestión de máquinas virtuales solicita al recurso 300 virtual crear un duplicado de la máquina 320 virtual (paso 205 en la Figura 20).

En respuesta a la solicitud de un duplicado desde el aparato 400 de gestión de máquinas virtuales, el recurso 300 virtual duplica la máquina 320 virtual (paso S206 en la Figura 20) y notifica al aparato 400 de gestión de máquinas virtuales de la máquina 320 virtual duplicada (paso S207 en la Figura 20). El aparato 400 de gestión de máquinas virtuales recibe y almacena temporalmente la máquina 320 virtual en la unidad 420 de almacenamiento de imágenes (paso S208 en la Figura 20). El aparato 400 de gestión de máquinas virtuales solicita al recurso 300 virtual eliminar la máquina 320 virtual (paso S209 en la Figura 20). En respuesta a la solicitud de eliminación del aparato 400 de gestión de máquinas virtuales, el recurso 300 elimina la máquina 320 virtual (paso S210 en la Figura 20) y notifica al aparato 400 de gestión de máquinas virtuales de la terminación de la eliminación (paso S211 en la Figura 20).

Cuando es notificado de la terminación de la eliminación de la máquina 320 virtual por el recurso 300 virtual, el aparato 400 de gestión de máquinas virtuales notifica al recurso 900 virtual de la máquina 320 virtual duplicada almacenada temporalmente en la unidad 320 de almacenamiento de imágenes (paso S212 en la Figura 20). El recurso 900 virtual recibe la máquina 320 virtual duplicada del aparato 400 de gestión de máquinas virtuales y dispone la máquina 320 virtual en el recurso 900 virtual (paso S213 en la Figura 20).

El aparato 400 de gestión de máquinas virtuales notifica al aparato 10 de control de la información de red lógica tras el movimiento de la máquina 320 virtual (paso S214 en la Figura 20).

El aparato 10 de control recibe información sobre una red asignada a la cual la máquina virtual pertenece desde el aparato 400 de gestión de máquinas virtuales y crea una regla de procesamiento según la información de red asignada (paso S215 en la Figura 20).

El aparato 10 de control notifica al nodo 20 de reenvío y al nodo 910 de reenvío virtual en el recurso 900 de la regla de procesamiento creada (ModoFlujo en paso S216 en la Figura 20).

El nodo 20 de reenvío y el nodo 910 de reenvío virtual reciben la regla de procesamiento desde el aparato 10 de control y establecen la regla de procesamiento (paso S217 en la Figura 20).

El terminal 50 de usuario transmite un paquete dirigido a la máquina 320 virtual (paso S218 en la Figura 20).

El paquete transmitido desde el terminal 50 de usuario es reenviado de manera secuencial al nodo 20 de reenvío y el nodo 910 de reenvío virtual. El nodo 20 de reenvío y el nodo 910 de reenvío virtual determinan el reenvío del paquete y reenvían el paquete, según la regla de procesamiento establecida por el aparato 10 de control (paso S219 en la Figura 20).

Como se describió anteriormente, el sistema de comunicación según la tercera realización ejemplar incluye el aparato 80 de movimiento de máquinas virtuales. De este modo, una máquina virtual puede ser movida entre recursos virtuales, y una regla de procesamiento que refleja el movimiento del recurso virtual puede ser establecida previamente en el nodo 20 de reenvío y el nodo 910 de reenvío virtual. Así, según la tercera realización ejemplar, dado que el número de solicitudes para reglas de procesamiento desde el nodo 20 de reenvío o el nodo 910 de reenvío virtual es reducido, la carga en el aparato de control puede ser reducida.

<Cuarta realización ejemplar>

Una cuarta realización ejemplar según la presente invención es realizada mediante la formación redundante de sistemas de comunicación según la tercera realización ejemplar. Mediante la formación redundante de sistemas de comunicación, incluso si alguno de los sistemas de comunicación se para, los servicios que han sido proporcionados por el sistema de comunicación parado pueden ser proporcionados de manera continua.

La cuarta realización ejemplar será descrita con referencia a los dibujos.

La Figura 21 ilustra una configuración de un sistema de comunicación según la cuarta realización ejemplar. Como se ilustra en la Figura 21, la diferencia entre la tercera y la cuarta realizaciones ejemplares es que el sistema de comunicación es formado de manera redundante. Dado que otros elementos son los mismos entre la tercera y la cuarta realizaciones ejemplares, la cuarta realización ejemplar será en adelante descrita con un foco en la diferencia.

Como se ilustra en la Figura 21, el sistema de comunicación según la cuarta realización ejemplar incluye un primer sistema de comunicación y un segundo sistema de comunicación. De manera alternativa, el sistema de comunicación según la cuarta realización ejemplar puede incluir varios sistemas de comunicación, además del primero y segundo sistemas de comunicación. El primero y segundo sistemas de comunicación proporcionan los mismos servicios. Por ejemplo, el primer sistema de comunicación es establecido en un centro de datos. Por ejemplo, en contraste al primer sistema de comunicación, el segundo sistema de comunicación es establecido en una compañía a través de una red externa tal como a través de Internet o una red de área ancha.

Como se ilustra en la Figura 21, el segundo sistema de comunicación según la cuarta realización incluye un aparato 10A de control local, un nodo 20A de reenvío local, un recurso 300A virtual local, un aparato 400A de gestión de máquinas virtuales local, un aparato 60A de autenticación local, un aparato 70A de gestión de políticas de comunicación local, y un aparato 80A de movimiento de máquinas virtuales local.

El aparato 10A de control local ejecuta el mismo procesamiento que el del aparato 10 de control en el primer sistema de comunicación. El nodo 20A de reenvío local ejecuta el mismo procesamiento que el del nodo 20 de reenvío en el primer sistema de comunicación. El recurso 300A virtual local ejecuta el mismo procesamiento que el del recurso 300 virtual en el primer sistema de comunicación. El aparato 400A de gestión de máquinas virtuales local ejecuta el mismo procesamiento que el del aparato 400 de gestión de máquinas virtuales. El aparato 60A de autenticación local ejecuta el mismo procesamiento que el aparato 60 de autenticación en el primer sistema de comunicación. El aparato 70A de gestión de políticas de comunicación local ejecuta el mismo procesamiento que el aparato 70 de gestión de políticas de comunicación en el primer sistema de comunicación. El aparato 80A de movimiento de máquinas virtuales local ejecuta el mismo procesamiento que el aparato 80 de movimiento de máquinas virtuales en el primer sistema de comunicación.

La cuarta realización ejemplar será descrita, asumiendo que las unidades incluidas en el primer sistema de comunicación y las unidades incluidas en el segundo sistema de comunicación operan en sincronización entre ellas. Las unidades incluidas en el primer sistema de comunicación y las unidades incluidas en el segundo sistema de comunicación pueden operar de manera independiente, en vez de en sincronización entre ellas.

En la cuarta realización ejemplar, el aparto 400 de gestión de máquinas virtuales recibe una solicitud para crear o establecer un cambio de una máquina virtual desde el terminal 50 de usuario y crea una máquina virtual en un recurso arbitrario en base a la solicitud. En respuesta a la solicitud del terminal 50 de usuario, la unidad 410 de almacenamiento de información de gestión del aparato 400 de gestión de máquinas virtuales crea información de red lógica.

En la cuarta realización ejemplar, el aparto 400 de gestión de máquinas virtuales notifica al aparato 400A de gestión de máquinas virtuales local incluido en el segundo sistema de comunicación de la información de red lógica creada. En base a la información de red lógica suministrada, el aparato 400A de gestión de máquinas virtuales local crea una máquina 320A virtual local en el recurso 300A virtual local. Si el terminal 50 de usuario transmite una solicitud al aparto 300A de gestión de máquinas virtuales para crear o establecer un cambio en una máquina virtual, el aparato 400A de gestión de máquinas virtuales puede notificar al aparato 400 de gestión de máquinas virtuales de la información de red lógica.

Igualmente, en la cuarta realización ejemplar, si el terminal 50 de usuario solicita un cambio de una regla de acceso, el aparato 70 de gestión de políticas notifica al aparato 10 de control y el aparato 10A de control local de una regla de acceso determinada. En base a la regla de acceso suministrada, el aparato 10A de control local calcula un camino de reenvío de paquetes y determina una regla de procesamiento para realizar el camino de reenvío calculado. El aparato 10A de control local previamente establece la regla de procesamiento determinada en el nodo 20A de reenvío local y el nodo 310A de reenvío virtual local.

Igualmente, en la cuarta realización ejemplar, si el terminal 50 de usuario solicita un movimiento de una máquina virtual, el aparato 400 de gestión de maquinas virtuales notifica al aparto 400A de gestión de máquinas virtuales local de la información de red lógica actualizada después de que la máquina virtual sea movida. En base a la información de red lógica suministrada, el aparato 400A de gestión de máquinas virtuales mueve la máquina 320A virtual local.

Una operación del sistema de comunicación según la cuarta realización ejemplar será descrita con referencia a las figuras.

La Figura 22 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la cuarta realización ejemplar. En la operación en la Figura 22, el terminal 50 de usuario transmite una solicitud al aparato 400 de gestión de máquinas virtuales para crear o establecer un cambio de una máquina virtual.

El terminal 50 de usuario ejecuta autenticación de usuario (paso S201 en la Figura 22).

A continuación, el terminal 50 de usuario solicita al aparato 400 de gestión de máquinas virtuales crear una máquina virtual (paso S202 en la Figura 22).

El aparato 400 de gestión de máquinas virtuales crea una máquina 320 virtual en respuesta a la solicitud desde el terminal 50 de usuario (paso S203 en la Figura 22) y ejecuta un proceso para disponer la máquina 320 virtual en un recurso 300 virtual específico (paso S204 en la Figura 22). La máquina 320 virtual es dispuesta en el recurso 300 virtual (paso S205 en la Figura 22). El aparato 400 de gestión de máquinas virtuales crea una red a la cual la máquina 320 virtual creada pertenece (paso S206 en la Figura 22).

El aparato 400 de gestión de máquinas virtuales comprueba la ID de usuario usada para la autenticación del usuario con las ID de usuario en la información de especificación de la máquina virtual almacenada en la unidad 410 de almacenamiento de información de gestión. Si la información de especificación de la máquina virtual incluye la ID del usuario, el aparato 400 de gestión de máquinas virtuales notifica al aparato 10 de control de la información de red lógica (paso S207 en la Figura 22).

Si la información de especificación de la máquina virtual no incluye la ID de usuario, el aparato 400 de gestión de máquinas virtuales registra una nueva ID de red asignada para la ID del usuario en la información de red lógica y notifica al aparato 10 de control de la información de red lógica en la cual la ID de red asignada ha sido registrada (paso S207 en la Figura 22).

En la cuarta realización ejemplar, la unidad 400 de gestión de máquinas virtuales incluida en el primer sistema de comunicación también notifica al aparato 400A de gestión de máquinas virtuales local incluido en el segundo sistema de comunicación de la información de red lógica (paso S207 en la Figura 22).

El aparato 10 de control recibe la información sobre la red a la cual la máquina virtual pertenece desde el aparato 400 de gestión de máquinas virtuales y crea una regla de procesamiento según la información de red asignada (paso S208 en la Figura 22).

El aparato 10 de control notifica al nodo 20 de reenvío y al nodo 310 de reenvío virtual de la regla de procesamiento creada (ModoFlujo en el paso S209 en la Figura 22).

El nodo 20 de reenvío y el nodo 310 de reenvío virtual reciben la regla de procesamiento desde el aparato 10 de control y establecen la regla de procesamiento (paso S210 en la Figura 22).

En la cuarta realización ejemplar, después de ser notificado de la información de red lógica por el aparato 400 de gestión de máquinas virtuales en el primer sistema de comunicación, en base a la información de red lógica, el aparato 400A de gestión de máquinas virtuales local crea la máquina 320A virtual local (paso S211 en la Figura 22) y dispone la máquina 320A virtual local en un recurso 300A virtual local especificado (paso S212 en la Figura 22). Una máquina 320A virtual local es dispuesta en el recurso 300A virtual local (paso S213 en la Figura 22).

El aparato 400A de gestión de máquinas virtuales notifica al aparato 10A de control local de la información de red lógica (paso S214 en la Figura 22).

El aparato 10A de control local recibe la información de red lógica desde el aparato 400A de gestión de máquinas virtuales local y crea una regla de procesamiento según la información de red lógica (paso S215 en la Figura 22).

El aparato 10A de control local notifica al nodo 20A de reenvío local y al nodo 310A de reenvío virtual local de la regla de procesamiento creada (ModoFlujo en el paso S216 en la Figura 22).

El nodo 20A de reenvío local y el nodo 310A de reenvío virtual local reciben la regla de procesamiento desde el aparato 10A de control local y establecen la regla de procesamiento (paso S217 en la Figura 22).

El terminal 50 de usuario trasmite un paquete dirigido a la máquina 320 virtual (paso S218 en la Figura 22).

El paquete transmitido desde el terminal 50 de usuario es reenviado de manera secuencial al nodo 20 de reenvío y el nodo 310 de reenvío virtual. El nodo 20 de reenvío y el nodo 310 de reenvío virtual reenvían el paquete según la regla de procesamiento establecida por el aparato 10 de control (paso S219 en la Figura 22).

La Figura 23 es un diagrama de secuencias que ilustra una operación del sistema de comunicación según la cuarta realización ejemplar. En la operación en la Figura 23, el terminal 50 de usuario transmite una instrucción para cambiar una regla de acceso solicitándolo al aparato 60 de autenticación.

En la Figura 23, el terminal 50 de usuario solicita al aparato 60 de autenticación ejecutar la autenticación (paso S301 en la Figura 23). El aparato 60 de autenticación autentica el usuario del terminal 50 de usuario (paso

S302 en la Figura 23). Si el aparato 60 de autenticación tiene éxito en la autenticación del terminal 50 de usuario, el aparato 60 de autenticación transmite la información de autenticación al aparato 70 de gestión de políticas (paso S303 en al Figura 23).

En base a la información de autenticación suministrada y las políticas de comunicación y la información de recursos almacenada en la unidad 71 de almacenamiento de políticas de comunicación, el aparato 70 de gestión de políticas de comunicación crea una regla de acceso sobre el acceso de la máquina 320 virtual creada en respuesta a una solicitud desde el terminal 50 de usuario (paso S304 en la Figura 23). El aparato 70 de gestión de políticas de comunicación transmite la regla de acceso creada al aparato 10 de control (paso S305 en la Figura 23).

En la cuarta realización ejemplar, el aparato 70 de gestión de políticas de comunicación en el primer sistema de comunicación también notifica al aparato 10A de control local en el segundo sistema de comunicación de la regla de acceso creada (paso s305 en la Figura 23).

Cuando es notificado de la regla de acceso por el aparato 70 de gestión de políticas de comunicación, el aparato 10 de control calcula un camino de reenvío de paquetes en base a la regla de acceso y determina una regla de procesamiento para realizar el camino de reenvío calculado (paso s306 en al Figura 23). El aparato 10 de control notifica al nodo 20 de reenvío y al nodo 310 de reenvío virtual de la regla de procesamiento determinada (ModoFlujo en el paso S307 en la Figura 23).

El nodo 20 de reenvío y el nodo 310 de reenvío virtual reciben la regla de procesamiento desde el aparato 10 de control y establece la regla de procesamiento (paso S308 en la Figura 23).

En la cuarta realización ejemplar, después de recibir una regla de acceso desde el aparato 70 de gestión de políticas en el primer sistema de comunicación, el aparato 10A de control local en el segundo sistema de comunicación calcula un camino de reenvío de paquetes en base a la regla de acceso y determina una regla de procesamiento para realizar el camino de reenvío calculado (paso S309 en la Figura 23). El aparato 10A de control local notifica al nodo 20A de reenvío local y al nodo 310A de reenvío virtual local de la regla de procesamiento determinada (ModoFlujo en el paso S310 en la Figura 23).

El nodo 20A de reenvío local y el nodo 310A de reenvío virtual local reciben la regla de procesamiento desde el aparato 10A de control loca y establecen la regla de procesamiento (paso S311 en la Figura 23).

El terminal 50 de usuario transmite un paquete dirigido a la máquina 320 virtual (paso S312 en la Figura 23).

El paquete transmitido desde el terminal 50 de usuario es reenviado de manera secuencia al nodo 20 de reenvío y al nodo 310 de reenvío virtual. El nodo 20 de reenvío y el nodo 310 de reenvío virtual reenvían el paquete según la regla de procesamiento establecida por el aparato 10 de control (paso S313 en la Figura 23).

Como se describió anteriormente, el sistema de comunicación según la cuarta realización ejemplar es formado de manera redundante. Así, por ejemplo, cuando un aparato tal como el aparato 10 de control mal funciona o cuando un fallo es causado en la red entre el nodo 20 de reenvío y el nodo 310 de reenvío virtual, si uno de los sistemas de comunicación se para, el servicio que ha sido proporcionado por el sistema de comunicación parado puede ser proporcionado de manera continuada por el otro sistema de comunicación.

Modificaciones y ajustes de la realización ejemplar son posibles dentro del alcance de la descripción general (incluyendo las reivindicaciones) de la presente invención y en base al concepto técnico básico de la presente invención. Varias combinaciones y selecciones de varios elementos descritos (incluyendo cada elemento de cada reivindicación, cada elemento de cada realización ejemplar, cada elemento de cada dibujo, etc.) son posibles dentro del alcance de las reivindicaciones de la presente invención. Esto es, la presente invención por supuesto incluye varias variaciones y modificaciones que podrían hacerse por los expertos en la técnica según la descripción general que incluye las reivindicaciones y el concepto técnico. En particular, cualquier intervalo numérico descrito en este documento debe interpretarse que cualquier valor intermedio o subintervalo que entre dentro del intervalo descrito son también descritos de manera concreta aun sin una descripción específica del mismo.

Lista de señales de referencia
10 aparato de control
10A aparato de control local
11 unidad de gestión de topologías
12 unidad de procesamiento de mensajes de control
13 unidad de cálculo del camino y acción
14 unidad de gestión de nodos de reenvío
15 unidad de gestión de reglas de procesamiento
16 base de datos de reglas de procesamiento

17 unidad de comunicación del nodo
18 unidad de gestión de recursos virtuales
20, 20-1, 20-2 nodo de reenvío
20A nodo de reenvío local
21 unidad de procesamiento de reenvíos
22 base de datos de tabla (DB tabla) 22
23 unidad de gestión de reglas de procesamiento
24 unidad de comunicación
30 aparato de comunicación
40 aparato de gestión de aparatos de comunicación
50 terminal de usuario
60 aparato de autenticación
60A aparato de autenticación local
70 aparato de gestión de políticas de comunicación
70A aparato de gestión de políticas de comunicación local
71 unidad de almacenamiento de políticas de comunicación
72 unidad de control de políticas
80 aparato de movimiento de máquinas virtuales
80A aparato de movimiento de máquinas virtuales local
300 recurso virtual
300A recurso virtual local
310 nodo de reenvío virtual
310A nodo de reenvío virtual local
320 máquina virtual
320A máquina virtual local
400 aparato de gestión de máquinas virtuales
400A aparato de gestión de máquinas virtuales local
410 unidad de almacenamiento de información de gestión
420 unidad de almacenamiento de imágenes
430 unidad de creación de máquinas virtuales
900 recurso virtual
910 nodo de reenvío virtual
920 máquina virtual

REIVINDICACIONES

1. Un sistema de comunicación, que comprende:

uno o unos nodos (20, 310) que solicitan una regla de procesamiento para procesar un paquete;
un aparato (10) de control que notifica al o a los nodos de la regla de procesamiento en respuesta a la solicitud; y
un aparato (400) de gestión de aparatos de comunicación para gestionar una relación de conexión entre un aparato (30) de comunicación que es un destino de paquetes y el o los nodos, donde

el aparato (10) de control, tras ser notificado del cambio de la relación de conexión entre el aparato (30) de comunicación y el o los nodos, es adaptado, antes de que el o los nodos reciban un paquete dirigido al aparato (30) de comunicación, para determinar un camino de reenvío para el paquete dirigido al aparato (30) de comunicación y notifica al o a los nodos de una regla de procesamiento para realizar el camino de reenvío,
el aparato (30) de comunicación comprende una o unas máquinas (320) virtuales dispuestas en uno o unos recursos (300) virtuales por el aparato (400) de gestión de aparatos de comunicación,
el aparato (400) de gestión de aparatos de comunicación, tras disponer la o las máquinas (320) virtuales en el o los recursos (300) virtuales, notifica al aparato (10) de control del cambio de una relación de conexión entre la o las máquinas (320) virtuales y el o los nodos,
el sistema de comunicación además comprende:

un terminal (50) de usuario que solicita la creación de la o las máquinas (320) virtuales; y
un aparato (70) de gestión de políticas de comunicación que gestiona una regla de acceso que indica la conectividad entre una o unas máquinas virtuales, creación de la cual es solicitada por el terminal (50) de usuario, y otra u otras máquinas virtuales, donde

en base a la regla de acceso suministrada desde el aparato (70) de gestión de políticas de comunicación, el aparato (10) de control es adaptado, antes de que el o los nodos reciban un paquete dirigido a la o las máquinas virtuales, para determinar un camino de reenvío para el paquete dirigido a la o las máquinas virtuales y notifica al nodo o nodos de una regla de procesamiento para realizar el camino de reenvío.

2. El sistema de comunicación según la reivindicación 1, donde
el aparato (400) de gestión de aparatos de comunicación, tras mover la o las máquinas (320) virtuales desde el o los recursos (300) virtuales, notifica al aparato (10) de control del cambio en la relación de conexión entre la o las máquinas (320) virtuales y el o los nodos.

3. Un aparato de control, que comprende:

primeros medios que generan una regla de procesamiento para procesar un paquete y transmitir la regla de procesamiento a uno o unos nodos (20, 210); y
segundos medios que, tras ser notificados de un cambio de una relación de conexión entre un aparato (30) de comunicación que es un destino de paquetes y el o los nodos, son adaptados, antes de que el o los nodos reciban un paquete dirigido al aparato (30) de comunicación, para determinar un camino de reenvío para el paquete dirigido al aparato (30) de comunicación y notificar al o a los nodos de una regla de procesamiento para realizar el camino de reenvío,

donde los segundos medios son notificados del cambio de una relación de conexión entre el aparato (30) de comunicación y el o los nodos desde un aparato (400) de gestión de aparatos de comunicación para cambiar la relación de conexión,
el aparato (30) de comunicación comprende una o unas máquinas (320) virtuales dispuestas en uno o unos recursos (300) virtuales por el aparato (400) de gestión de aparatos de comunicación, y
el aparato (400) de gestión de aparatos de comunicación que ha dispuesto la o las máquinas (320) virtuales en el o los recursos (300) virtuales es adaptado para notificar a los segundos medios del cambio de la relación de conexión entre la o las máquinas (320) virtuales y el o los nodos, y
en base a una regla de acceso que indica la conectividad entre una o unas maquinas virtuales, la creación de las cuales es solicitada por un terminal (50) de usuario, y otra u otras máquinas virtuales, los segundos medios son adaptados, antes de que el o los nodos reciban un paquete dirigido a la o las máquinas virtuales, para determinar un camino de renvío para el paquete dirigido a la o las máquinas virtuales y notificar al o a los nodos de una regla de procesamiento para realizar el camino de reenvío.

4. El aparato de control según la reivindicación 3, donde el aparato (400) de gestión de aparatos de comunicación que ha movido la o las máquinas (320) virtuales desde el o los recursos (300) virtuales notifica a los segundos medios del cambio en la relación de conexión entre la o las máquinas (320) virtuales y el o los nodos.

5. Un método de control de comunicación por un aparato (10) de control, que comprende:

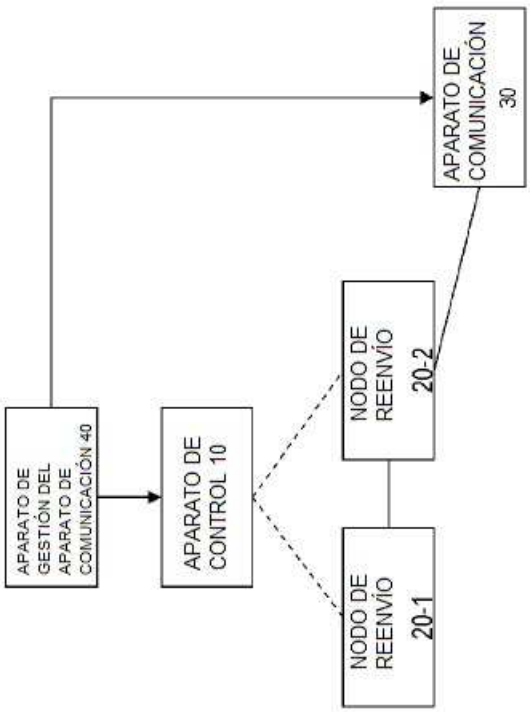
generar una regla de procesamiento para procesar un paquete;
notificar al o a los nodos (20, 310) de la regla de procesamiento generada;
tras ser notificado, desde un aparato (400) de gestión de aparatos de comunicación, de un cambio de una relación de conexión entre un aparato (30) de comunicación que es un destino de paquetes y el o los nodos, determinar un camino de reenvío para el paquete dirigido al aparato (30) de comunicación; y
antes de que el o los nodos reciban un paquete dirigido al aparato (30) de comunicación, notificar al o a los nodos de una regla de procesamiento para realizar el camino de reenvío,

donde el aparato (30) de comunicación comprende una o unas máquinas (320) virtuales dispuestas en uno o unos recursos (300) virtuales por el aparato (400) de gestión de aparatos de comunicación, y
el aparato (400) de gestión de aparatos de comunicación que ha dispuesto la o las máquinas (320) virtuales en el o los recursos (300) virtuales notifica al aparato (10) de control del cambio de la relación de conexión entre la o las máquinas (320) virtuales y el o los nodos, y
el método además comprende:

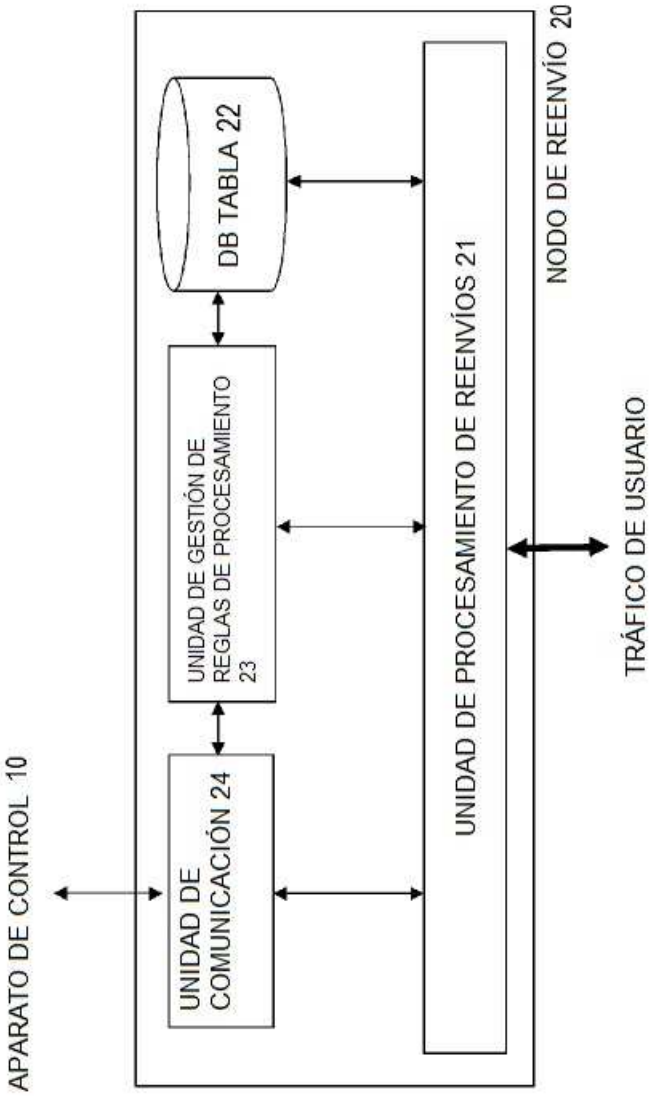
en base a una regla de acceso que indica la conectividad entre una o unas máquinas virtuales, la creación de las cuales es solicitada por un terminal (50) de usuario, y otra u otras máquinas virtuales, antes de que el o los nodos reciban un paquete dirigido a la o las máquinas virtuales, determinar un camino de reenvío para el paquete dirigido a la o las máquinas virtuales y notificar al o a los nodos de una regla de procesamiento para realizar el camino de reenvío.

6. Un programa, que causa que un aparato de control que controla un aparato de comunicación que procese un paquete, para ejecutar el método de control de comunicación según la reivindicación 5.

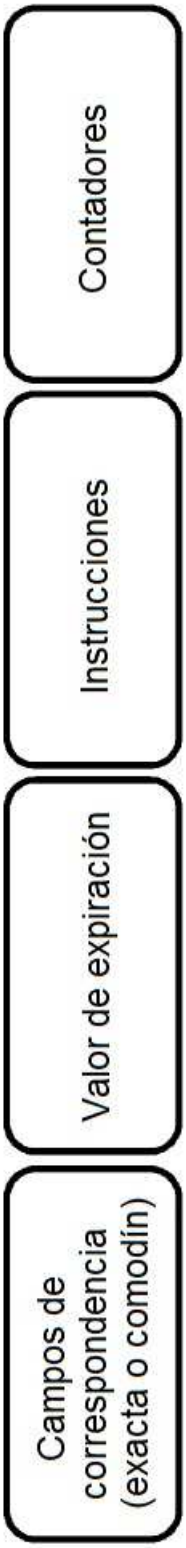
[Fig. 1]


APARATO DE COMUNICACIÓN 30
NODO DE REENVÍO 20-2
NODO DE REENVÍO 20-1
APARATO DE CONTROL 10
APARATO DE GESTIÓN DEL APARATO DE COMUNICACIÓN 40

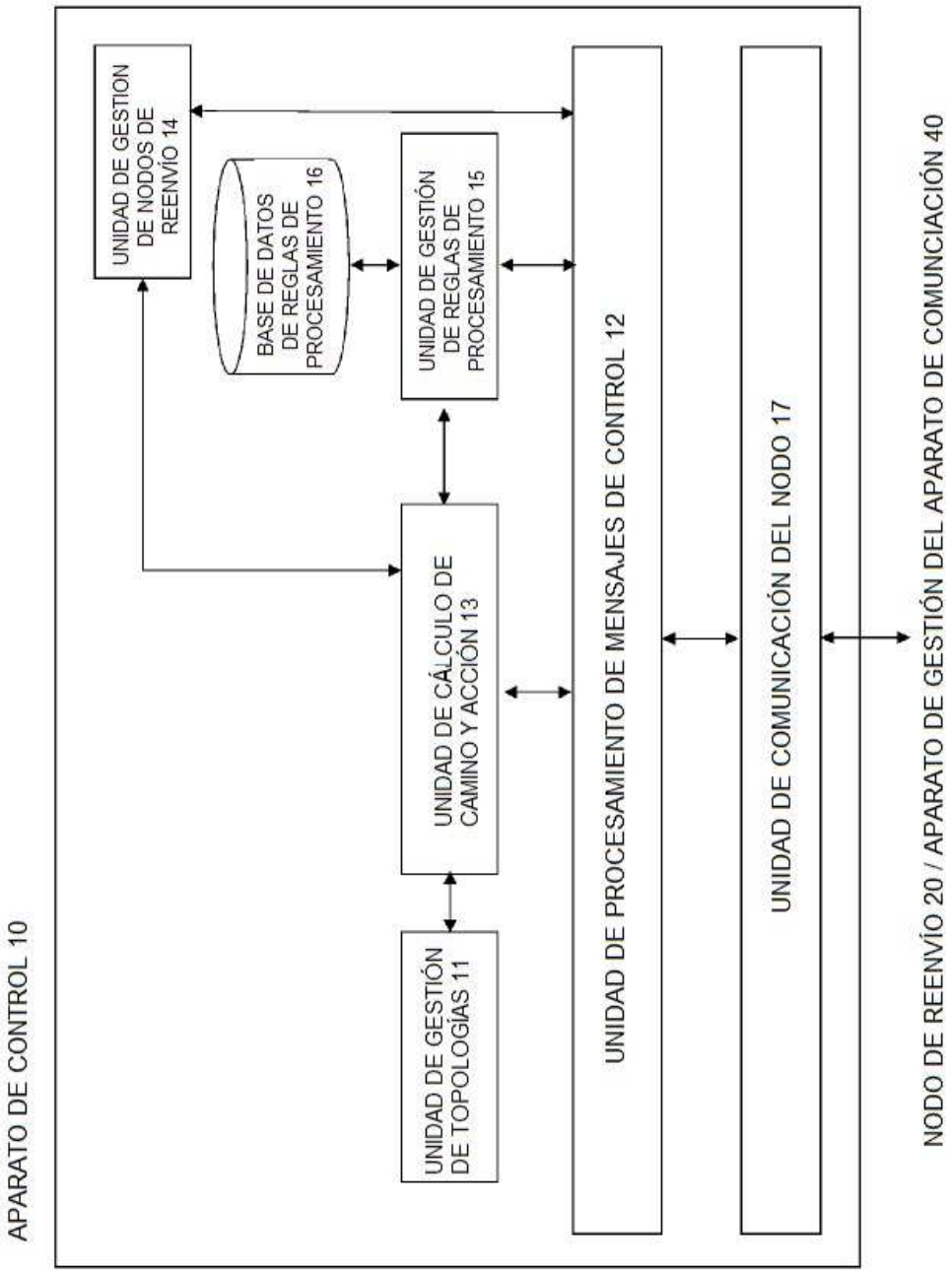
[Fig. 2]


APARATO DE CONTROL 10
UNIDAD DE COMUNICACIÓN 24
UNIDAD DE GESTIÓN DE REGLAS DE PROCESAMIENTO 23
DB TABLA 22
UNIDAD DE PROCESAMIENTO DE REENVÍOS 21
NODO DE REENVÍO 20
TRÁFICO DE USUARIO

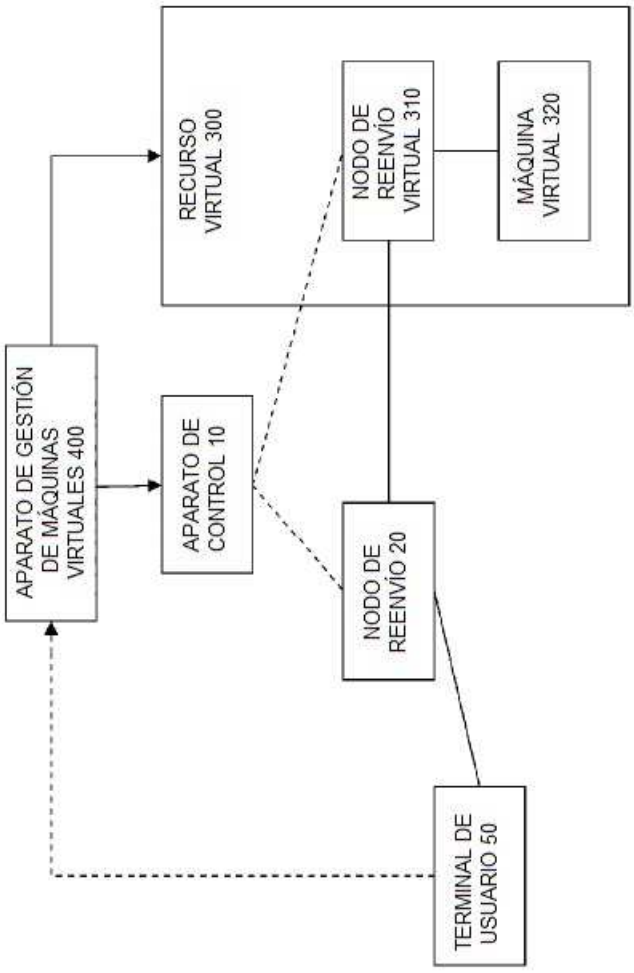
[Fig. 3]


Contadores
Instrucciones
Valor de expiración
Campos de correspondencia (exacta o comodín)

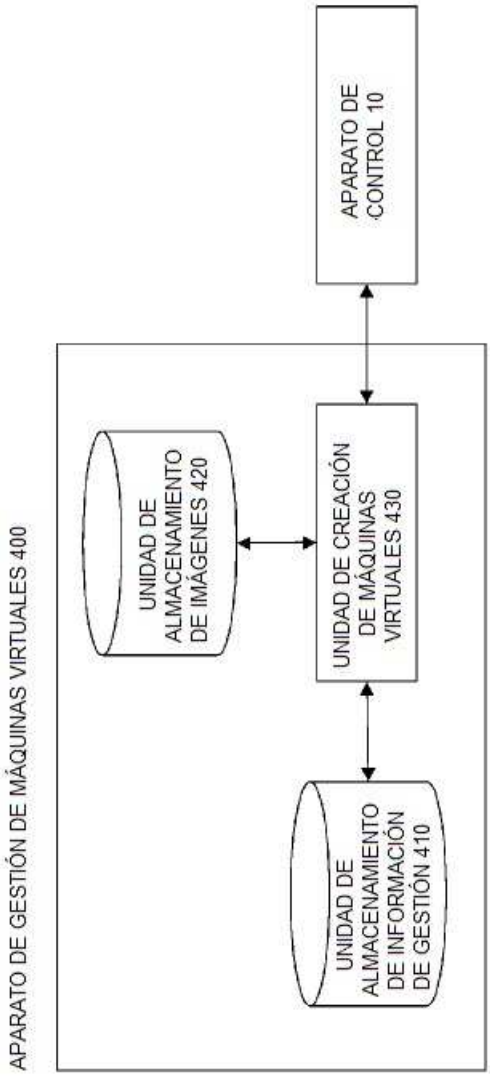
[Fig. 4]


APARATO DE CONTROL 10
UNIDAD DE GESTION DE NODOS DE REENVÍO 14
BASE DE DATOS DE REGLAS DE PROCESAMIENTO 16
UNIDAD DE GESTIÓN DE REGLAS DE PROCESAMIENTO 15
UNIDAD DE CÁLCULO DE CAMINO Y ACCIÓN 13
UNIDAD DE GESTIÓN DE TOPOLOGÍAS 11
UNIDAD DE PROCESAMIENTO DE MENSAJES DE CONTROL 12
UNIDAD DE COMUNICACIÓN DEL NODO 17
NODO DE REENVÍO 20 / APARATO DE GESTIÓN DEL APARATO DE COMUNCIACIÓN 40

[Fig. 5]


RECURSO VIRTUAL 300
NODO DE REENVÍO VIRTUAL 310
MÁQUINA VIRTUAL 320
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
TERMINAL DE USUARIO 50

[Fig. 6]


APARATO DE CONTROL 10
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
UNIDAD DE ALMACENAMIENTO DE IMÁGENES 420
UNIDAD DE CREACIÓN DE MÁQUINAS VIRTUALES 430
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE GESTIÓN 410

[Fig. 7]

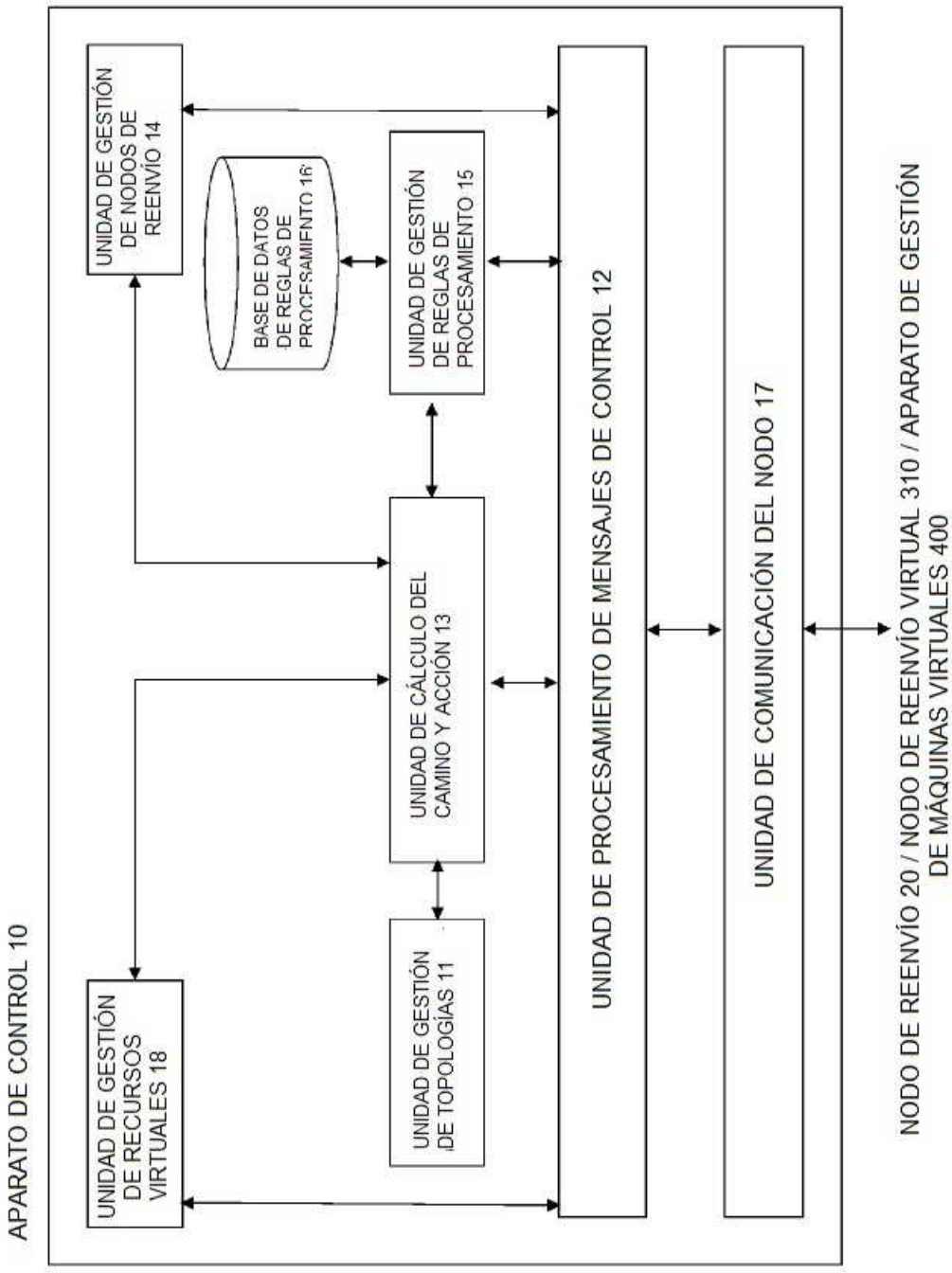
(a) INFORMACIÓN DE ESPECIFICACIÓN DE MÁQUINA VIRTUAL

ID DE MÁQUINA VIRTUAL	ID DE USUARIO	NÚMERO DE NÚCLEO DE CPU	CANTIDAD DE MEMORIA
a	0001	2	2GB
b	0001	4	8GB
c	0001	1	1GB
d	0002	2	4GB

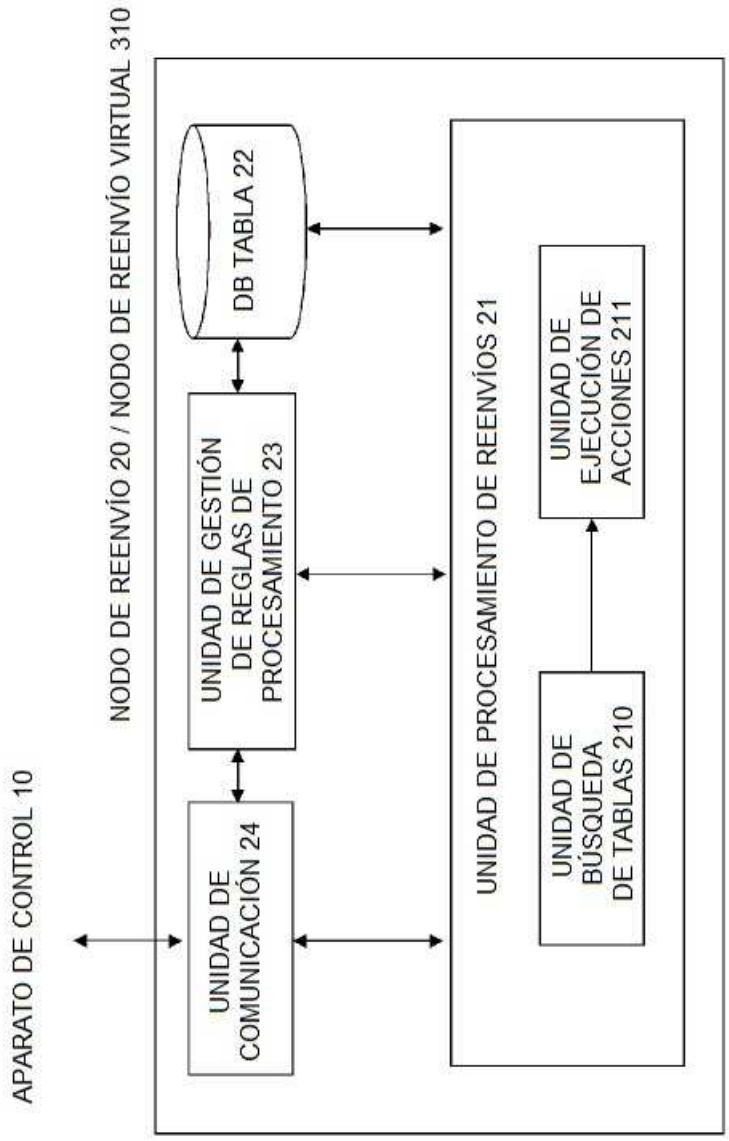
(b) INFORMACIÓN DE RED LÓGICA

ID DE MÁQUINA VIRTUAL	ID DE RED ASIGNADA	ID DE NODO DE REENVÍO	NÚMERO DE PUERTO
a	100	210	1
b	100	210	2
c	100	240	1
d	200	240	2

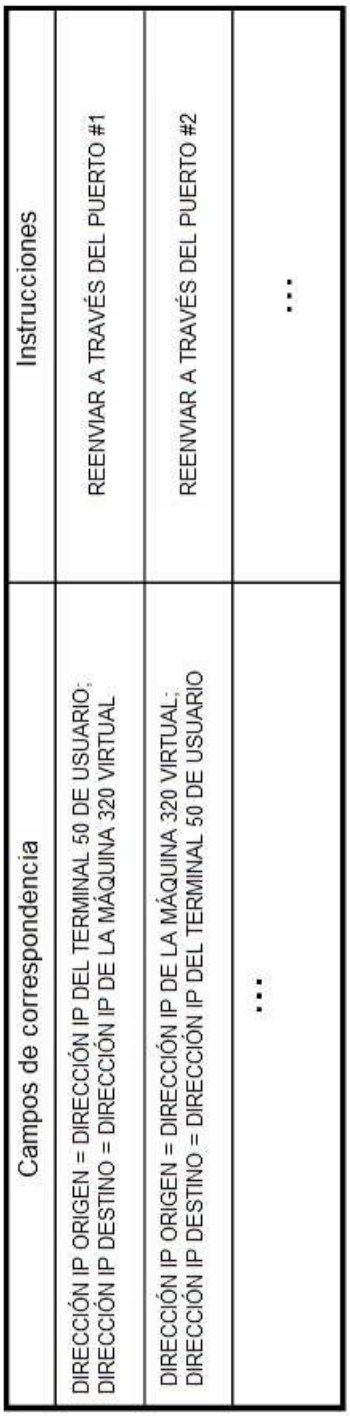
[Fig. 8]


APARATO DE CONTROL 10
UNIDAD DE GESTIÓN DE RECURSOS VIRTUALES 18
UNIDAD DE GESTIÓN DE TOPOLOGÍAS 11
UNIDAD DE CÁLCULO DEL CAMINO Y ACCIÓN 13
BASE DE DATOS DE REGLAS DE PROCESAMIENTO 16
UNIDAD DE GESTIÓN DE REGLAS DE PROCESAMIENTO 15
UNIDAD DE GESTIÓN DE NODOS DE REENVÍO 14
UNIDAD DE PROCESAMIENTO DE MENSAJES DE CONTROL 12
UNIDAD DE COMUNICACIÓN DEL NODO 17
NODO DE REENVÍO 20 / NODO DE REENVÍO VIRTUAL 310 / APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400

[Fig. 9]

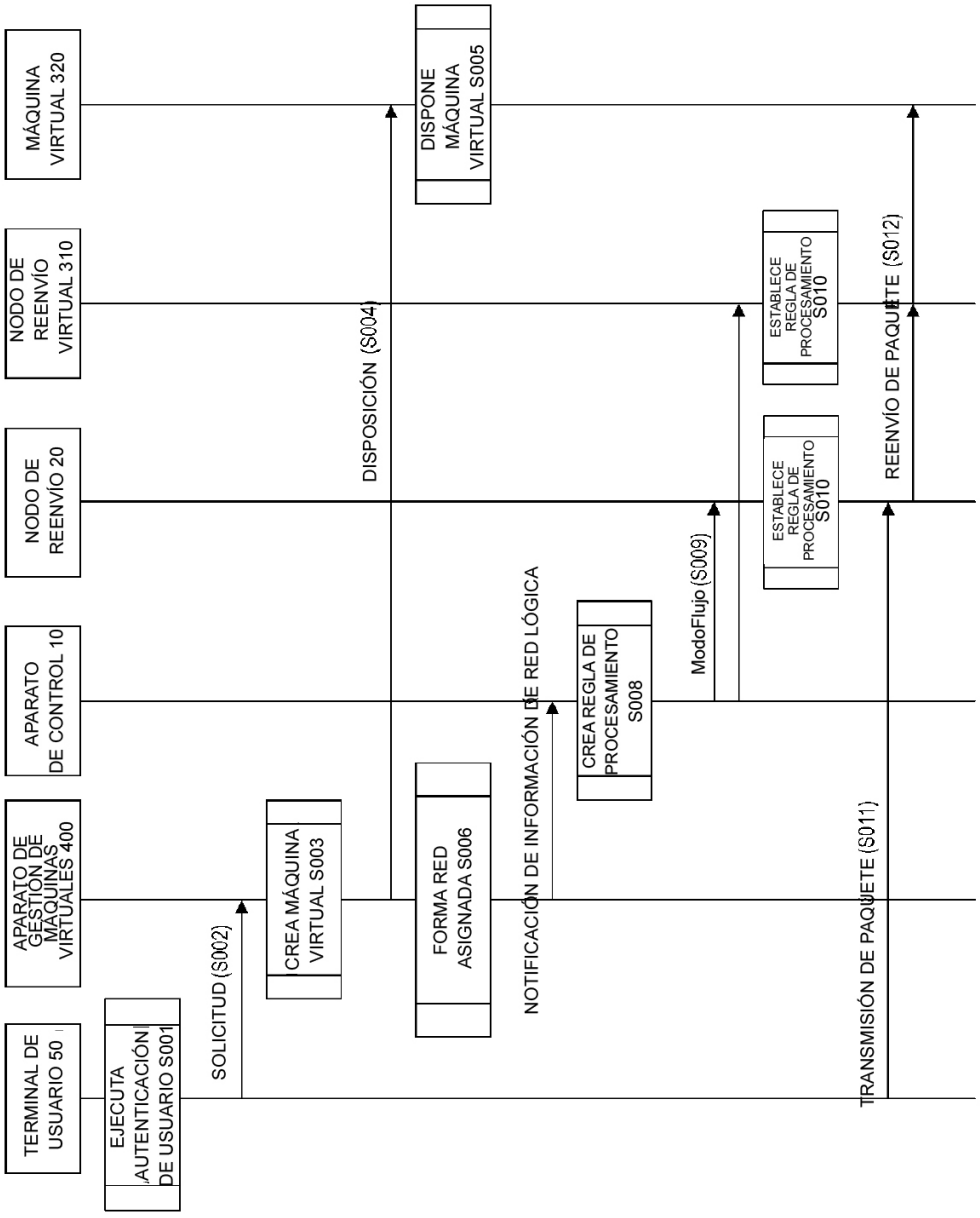

APARATO DE CONTROL 10
NODO DE REENVÍO 20 / NODO DE REENVÍO VIRTUAL 310
UNIDAD DE COMUNICACIÓN 24
UNIDAD DE GESTIÓN DE REGLAS DE PROCESAMIENTO 23
DB TABLA 22
UNIDAD DE PROCESAMIENTO DE REENVÍOS 21
UNIDAD DE BÚSQUEDA DE TABLAS 210
UNIDAD DE EJECUCIÓN DE ACCIONES 211

[Fig. 10]

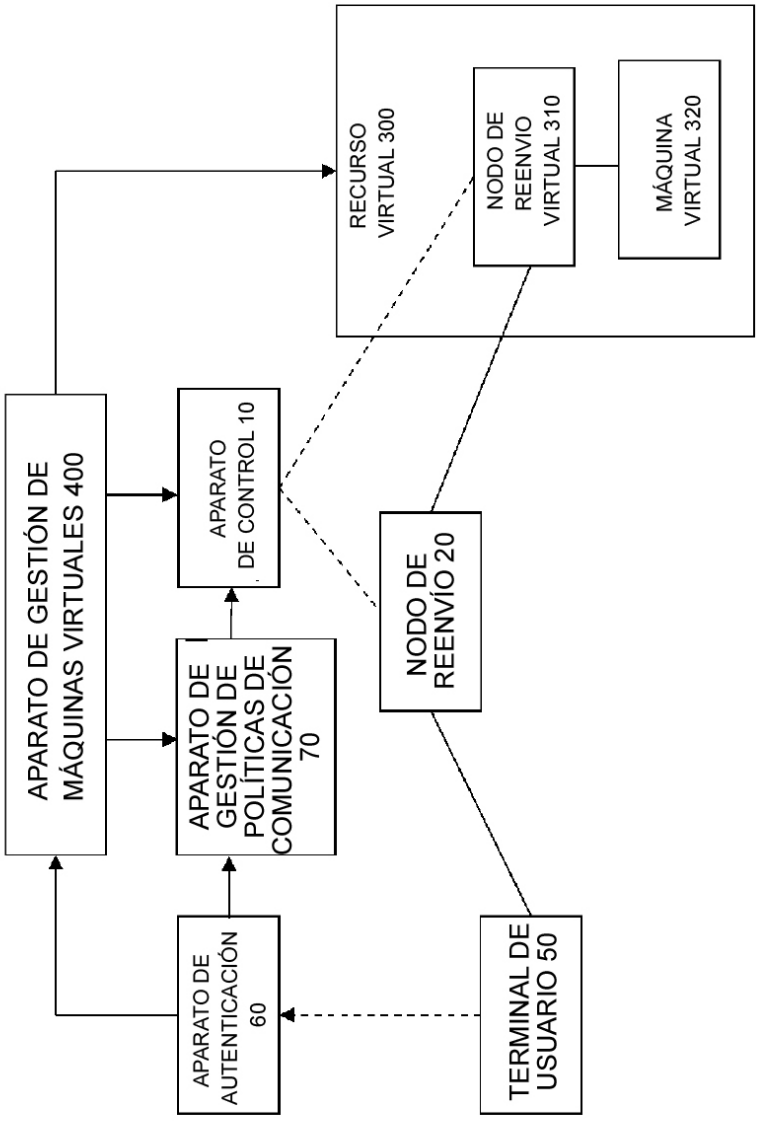


Campos de correspondencia	Instrucciones
DIRECCIÓN IP ORIGEN = DIRECCIÓN IP DEL TERMINAL 50 DE USUARIO; DIRECCIÓN IP DESTINO = DIRECCIÓN IP DE LA MÁQUINA 320 VIRTUAL	REENVIAR A TRAVÉS DEL PUERTO #1
DIRECCIÓN IP ORIGEN = DIRECCIÓN IP DE LA MÁQUINA 320 VIRTUAL; DIRECCIÓN IP DESTINO = DIRECCIÓN IP DEL TERMINAL 50 DE USUARIO	REENVIAR A TRAVÉS DEL PUERTO #2
...	...

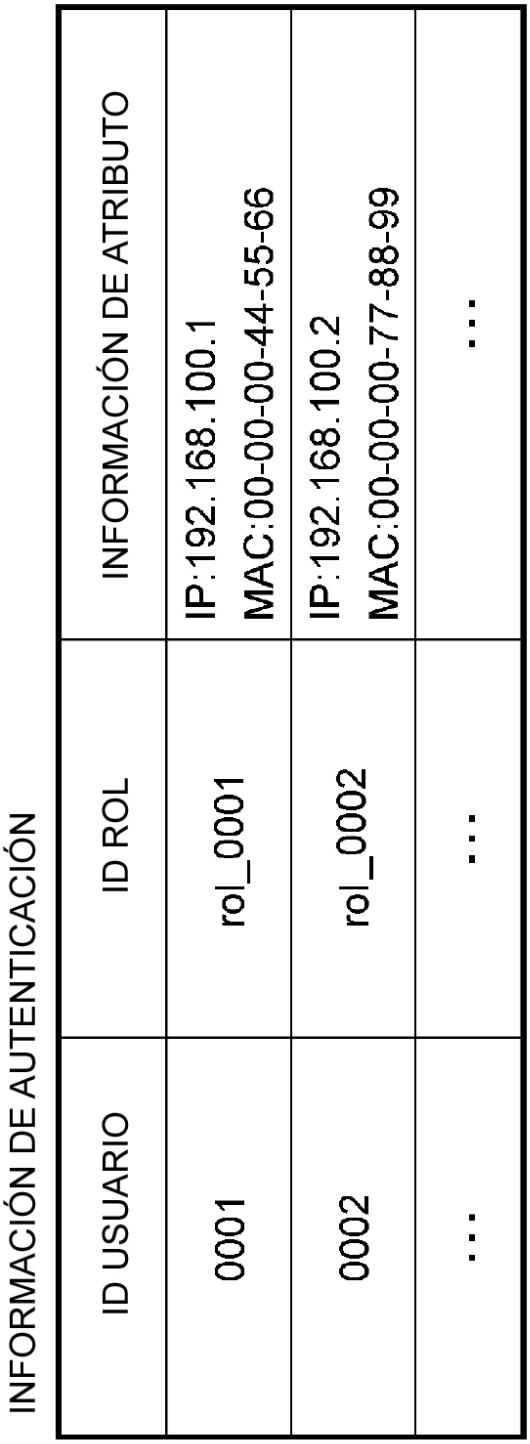
[Fig. 11]


TERMINAL DE USUARIO 50
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
NODO DE REENVÍO VIRTUAL 310
MÁQUINA VIRTUAL 320
EJECUTA AUTENTICACIÓN DE USUARIO S001
SOLICITUD (S002)
CREA MÁQUINA VIRTUAL S003
DISPONE MÁQUINA VIRTUAL S005
DISPOSICIÓN (S004)
FORMA RED ASIGNADA S006
NOTIFICACIÓN DE INFORMACIÓN DE RED LÓGICA
CREA REGLA DE PROCESAMIENTO S008
ModoFlujo (S009)
ESTABLECE REGLA DE PROCESAMIENTO S010
ESTABLECE REGLA DE PROCESAMIENTO S010
REENVÍO DE PAQUETE (S012)
TRANSMISIÓN DE PAQUETE (S011)

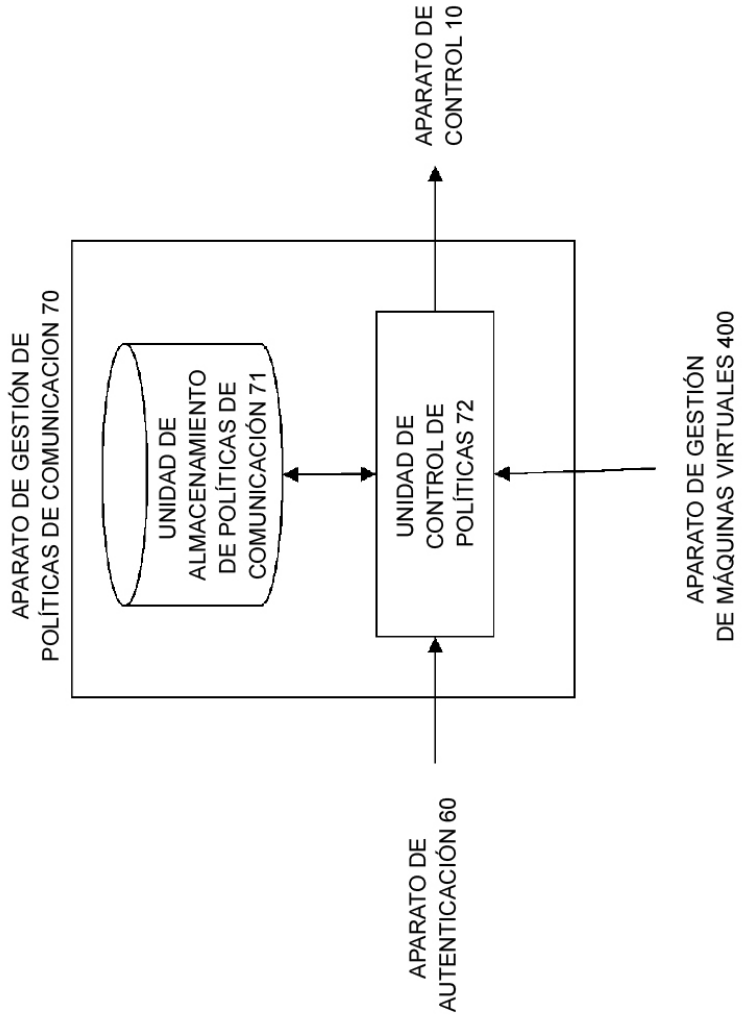
[Fig. 12]


RECURSO VIRTUAL 300
NODO DE REENVIO VIRTUAL 310
MÁQUINA VIRTUAL 320
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
APARATO DE GESTIÓN DE POLÍTICAS DE COMUNICACIÓN 70
NODO DE REENVÍO 20
APARATO DE AUTENTICACIÓN 60
TERMINAL DE USUARIO 50

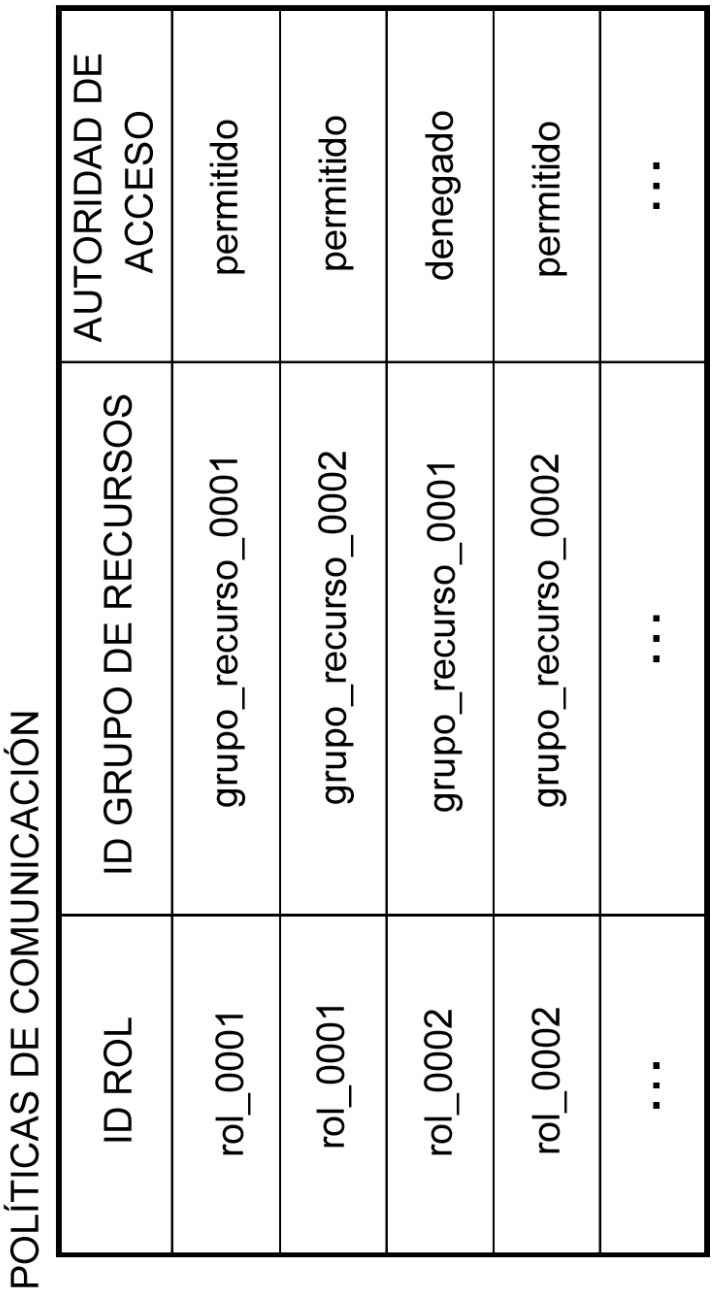
[Fig. 13]


INFORMACIÓN DE AUTENTICACIÓN
ID USUARIO
ID ROL
INFORMACIÓN DE ATRIBUTO
0001
rol_0001
IP:192.168.100.1
MAC:00-00-00-44-55-66
0002
rol_0002
IP:192.168.100.2
MAC:00-00-00-77-88-99
...
...
...

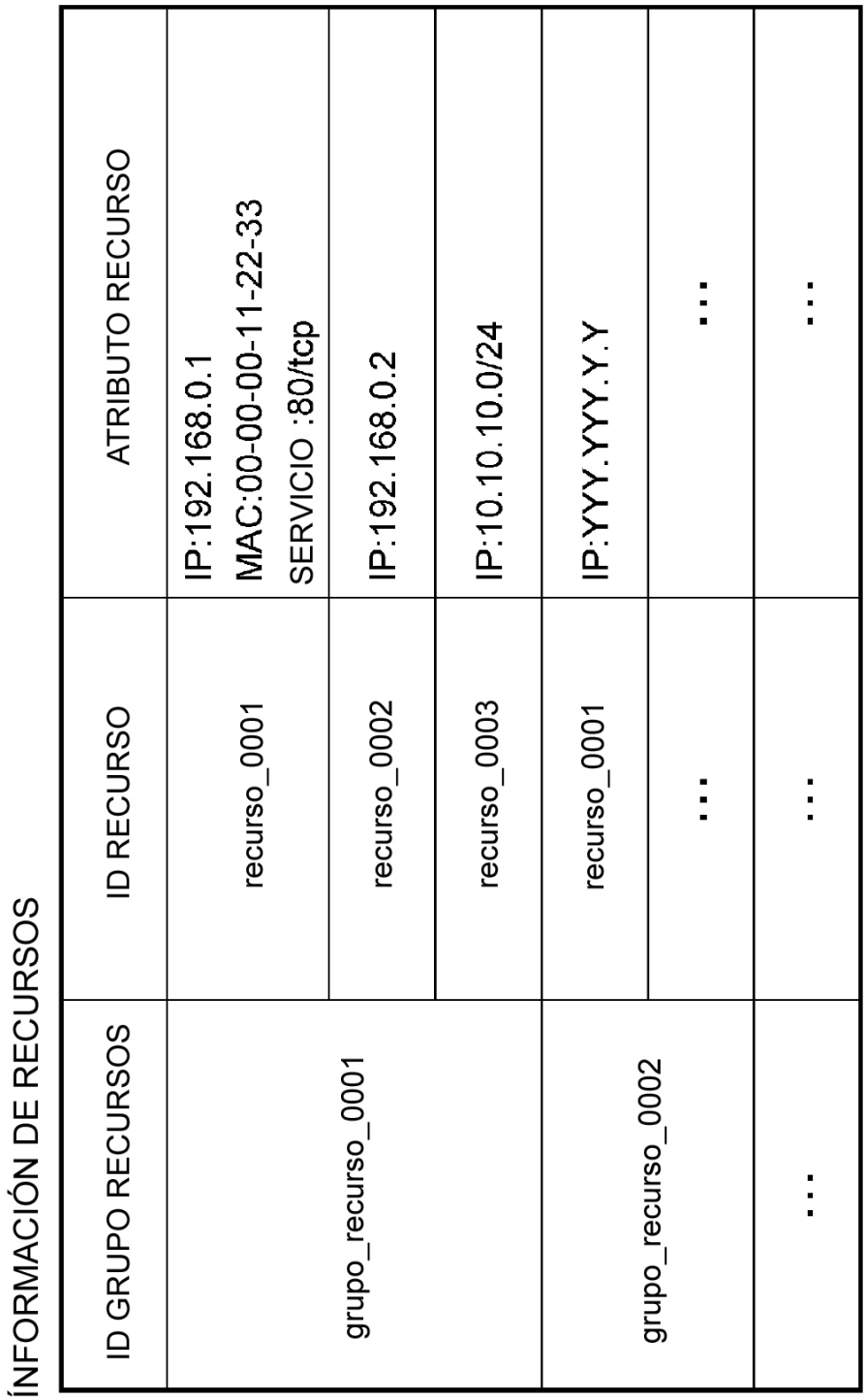
[Fig. 14]


APARATO DE CONTROL 10
APARATO DE GESTIÓN DE POLÍTICAS DE COMUNICACION 70
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN 71
UNIDAD DE CONTROL DE POLÍTICAS 72
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE AUTENTICACIÓN 60

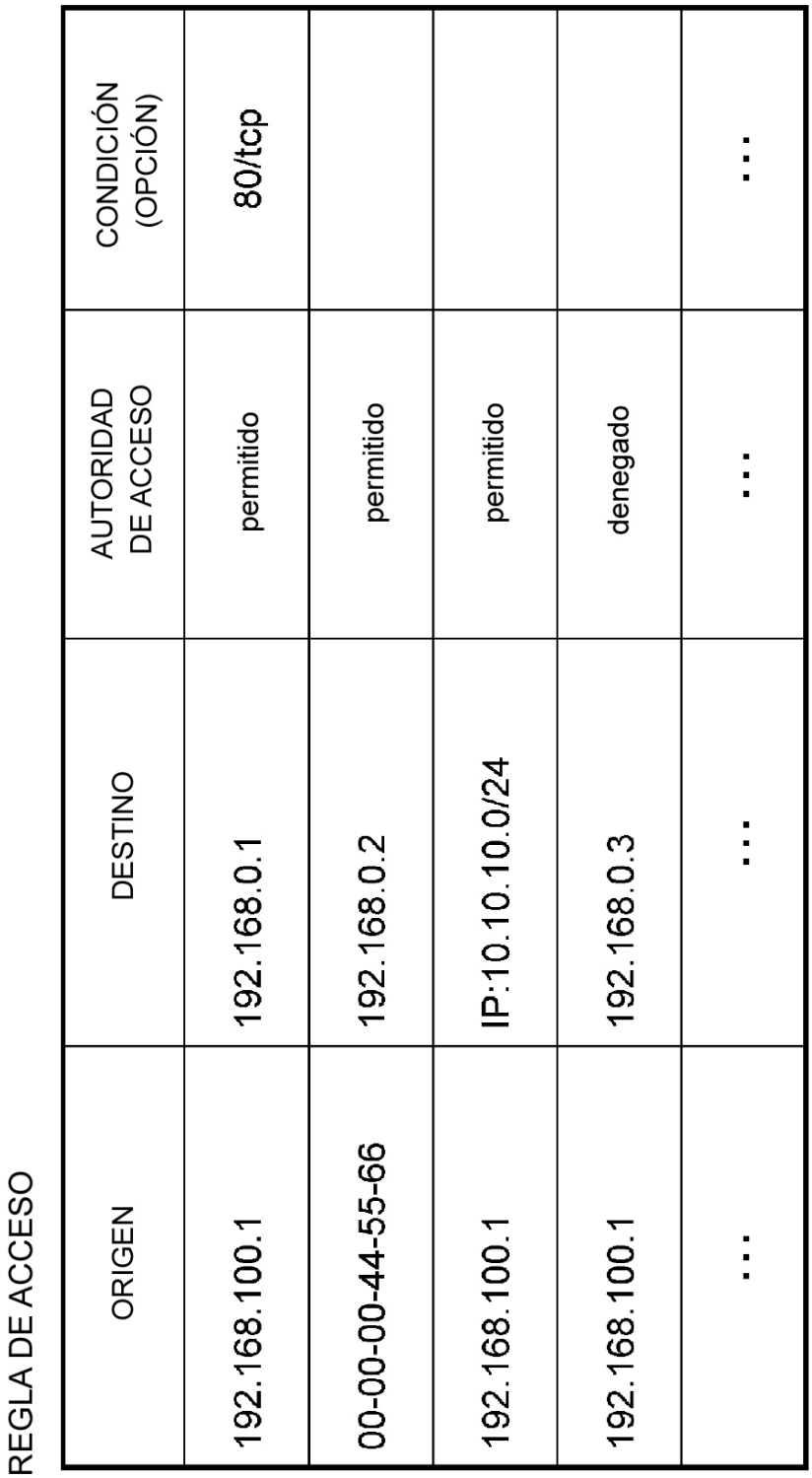
[Fig. 15]


POLÍTICAS DE COMUNICACIÓN
ID ROL
ID GRUPO DE RECURSOS
AUTORIDAD DE ACCESO
rol_0001
grupo_recurso_0001
permitido
rol_0001
grupo_recurso_0002
permitido
rol_0002
grupo_recurso_0001
denegado
rol_0002
grupo_recurso_0002
permitido
...
...
...

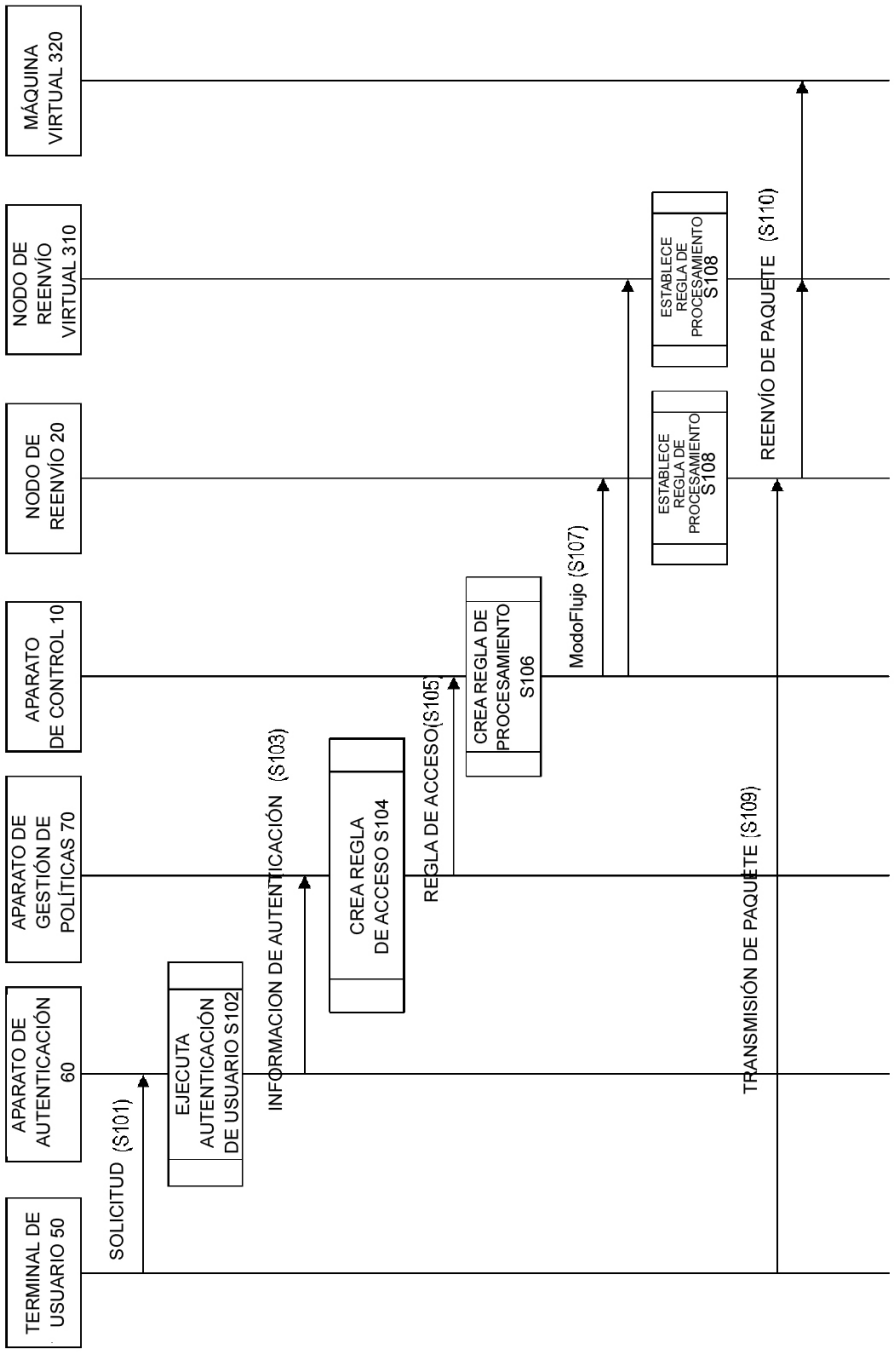
[Fig. 16]


ÍNFORMACIÓN DE RECURSOS
ID GRUPO RECURSOS
ID RECURSO
ATRIBUTO RECURSO
grupo_recurso_0001
recurso_0001
IP:192.168.0.1
MAC:00-00-00-11-22-33
SERVICIO :80/tcp
recurso_0002
IP:192.168.0.2
recurso_0003
IP:10.10.10.0/24
grupo_recurso_0002
recurso_0001
IP:YYY.YYY.Y.Y
...
...
...
...
...
...

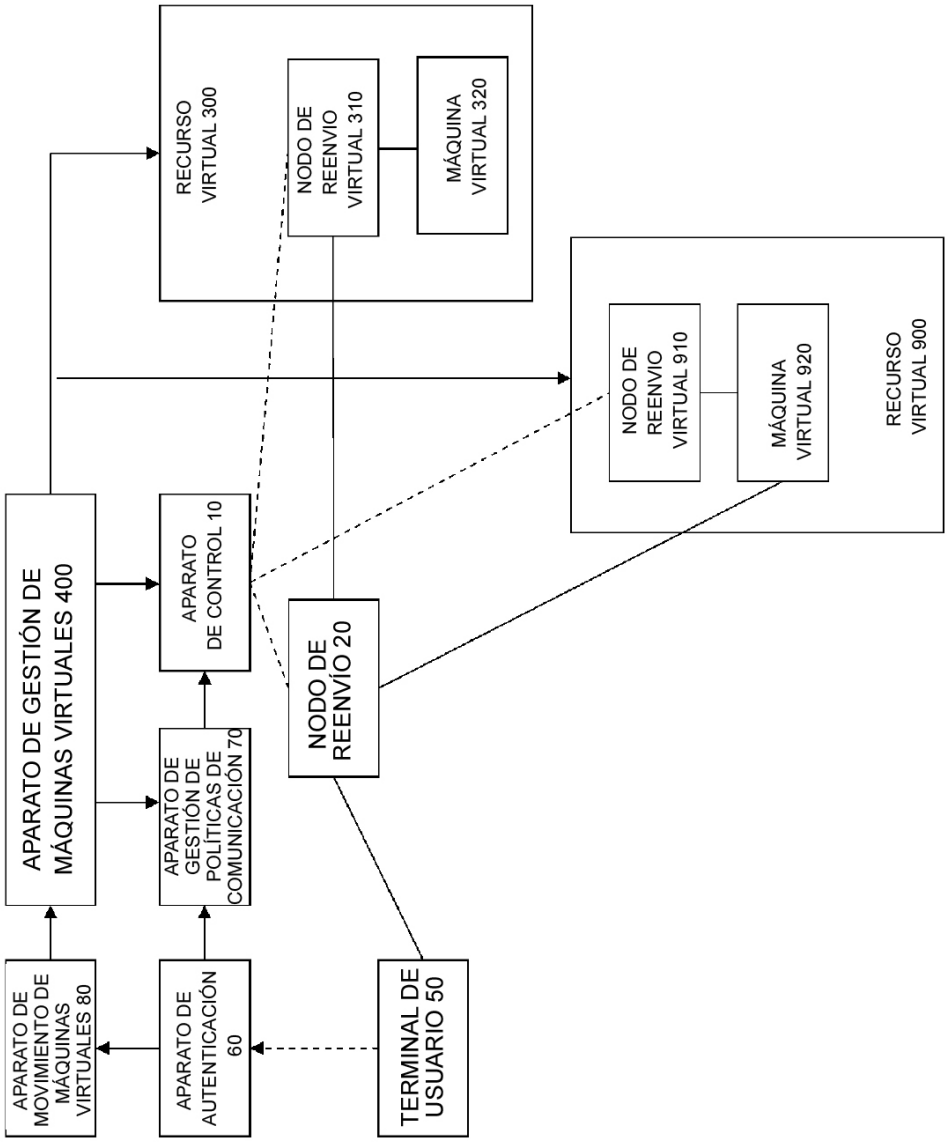
[Fig. 17]


REGLA DE ACCESO
ORIGEN
DESTINO
AUTORIDAD DE ACCESO
CONDICIÓN (OPCIÓN)
192.168.100.1
192.168.0.1
permitido
80/tcp
00-00-00-44-55-66
192.168.0.2
permitido
192.168.100.1
IP:10.10.10.0/24
permitido
192.168.100.1
192.168.0.3
denegado
...
...
...
...

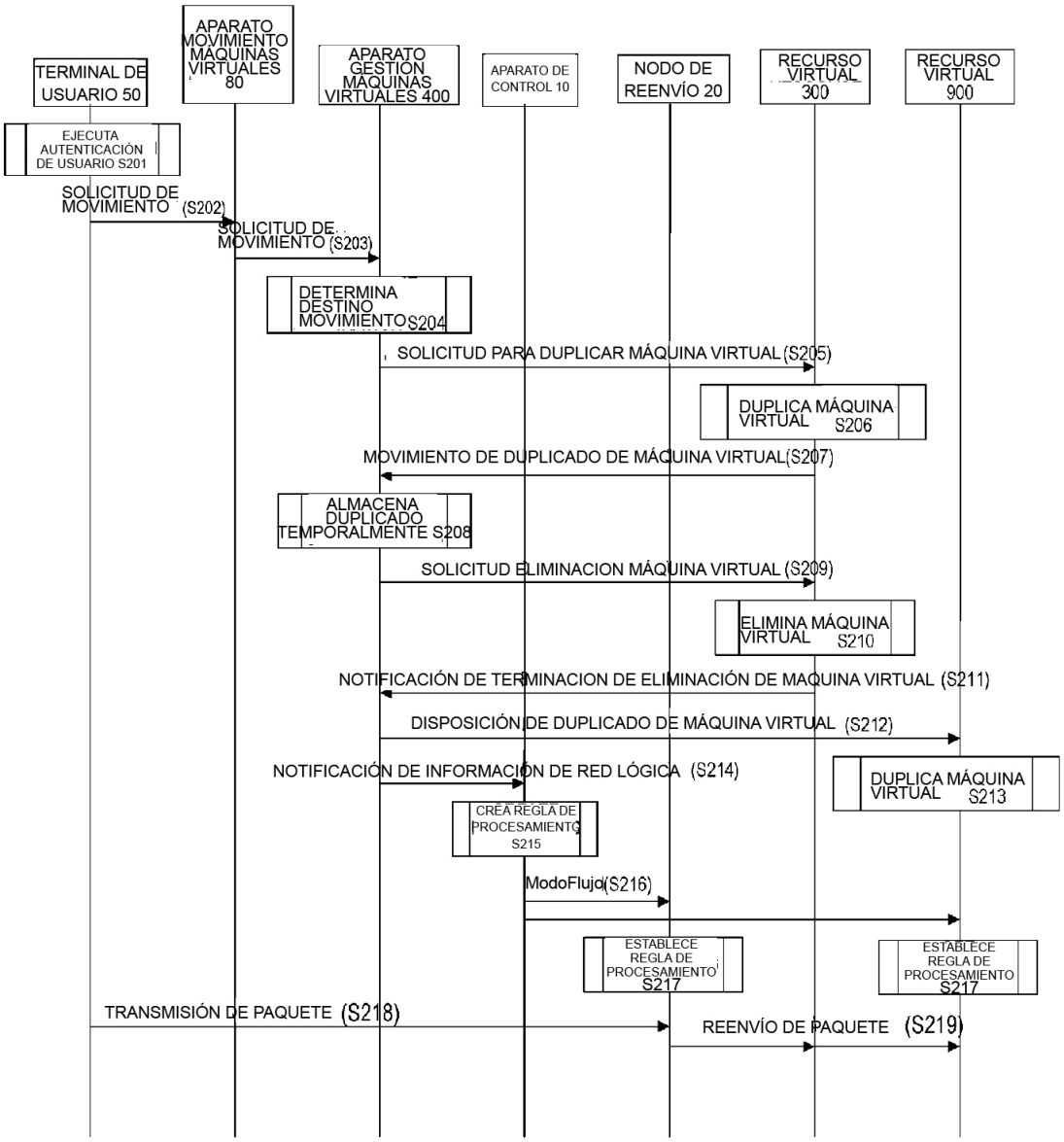
[Fig. 18]


TERMINAL DE USUARIO 50
APARATO DE AUTENTICACIÓN 60
APARATO DE GESTIÓN DE POLÍTICAS 70
APARATO DE CONTROL 10
NODO DE REENVÍO 20
NODO DE REENVÍO VIRTUAL 310
MÁQUINA VIRTUAL 320
SOLICITUD (S101)
EJECUTA AUTENTICACIÓN DE USUARIO S102
INFORMACION DE AUTENTICACIÓN (S103)
CREA REGLA DE ACCESO S104
REGLA DE ACCESO(S105)
CREA REGLA DE PROCESAMIENTO S106
ModoFlujo (S107)
ESTABLECE REGLA DE PROCESAMIENTO S108
ESTABLECE REGLA DE PROCESAMIENTO S108
REENVÍO DE PAQUETE (S110)
TRANSMISIÓN DE PAQUETE (S109)

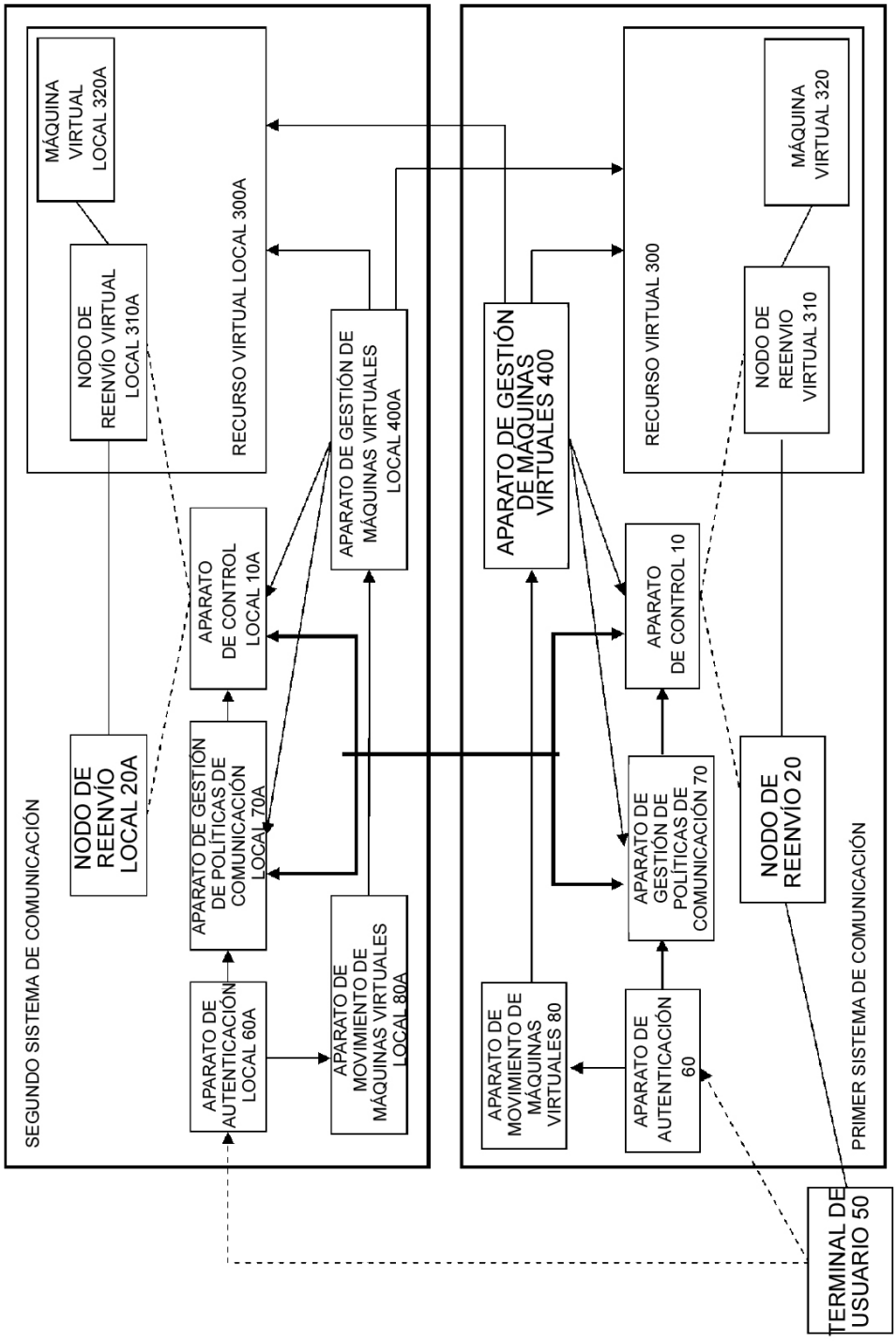
[Fig. 19]


RECURSO VIRTUAL 300
NODO DE REENVIO VIRTUAL 310
MÁQUINA VIRTUAL 320
NODO DE REENVIO VIRTUAL 910
MÁQUINA VIRTUAL 920
RECURSO VIRTUAL 900
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
APARATO DE GESTIÓN DE POLÍTICAS DE COMUNICACIÓN 70
APARATO DE MOVIMIENTO DE MÁQUINAS VIRTUALES 80
APARATO DE AUTENTICACIÓN 60
TERMINAL DE USUARIO 50

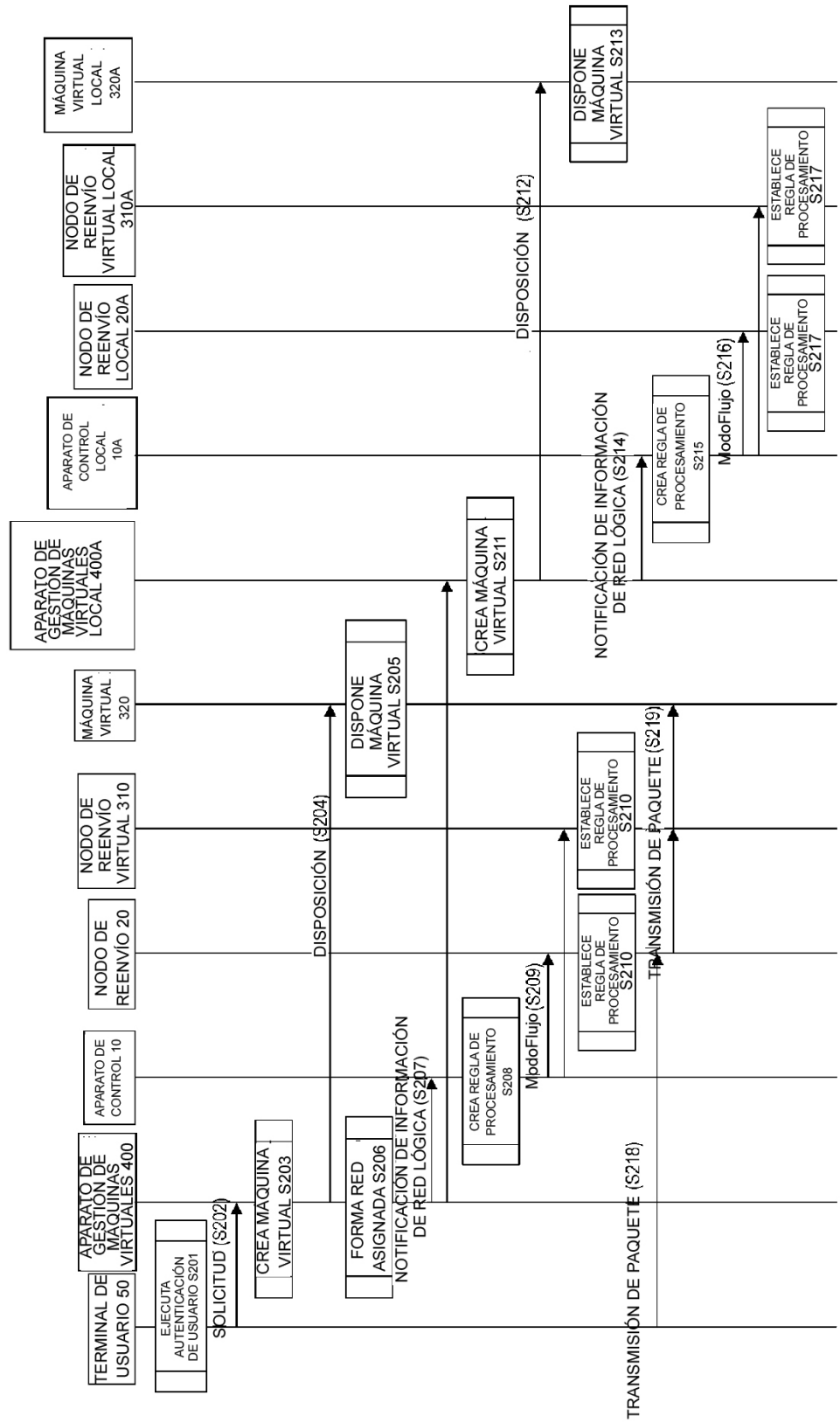
[Fig. 20]


TERMINAL DE USUARIO 50
APARATO MOVIMIENTO MÁQUINAS VIRTUALES 80
APARATO GESTIÓN MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
RECURSO VIRTUAL 300
RECURSO VIRTUAL 900
EJECUTA AUTENTICACIÓN DE USUARIO S201
SOLICITUD DE MOVIMIENTO (S202)
SOLICITUD DE MOVIMIENTO (S203)
DETERMINA DESTINO MOVIMIENTO S204
SOLICITUD PARA DUPLICAR MÁQUINA VIRTUAL (S205)
DUPLICA MÁQUINA VIRTUAL S206
MOVIMIENTO DE DUPLICADO DE MÁQUINA VIRTUAL (S207)
ALMACENA DUPLICADO TEMPORALMENTE S208
SOLICITUD ELIMINACION MÁQUINA VIRTUAL (S209)
ELIMINA MÁQUINA VIRTUAL S210
NOTIFICACIÓN DE TERMINACION DE ELIMINACIÓN DE MAQUINA VIRTUAL (S211)
DISPOSICIÓN DE DUPLICADO DE MÁQUINA VIRTUAL (S212)
DUPLICA MÁQUINA VIRTUAL S213
NOTIFICACIÓN DE INFORMACIÓN DE RED LÓGICA (S214)
CREA REGLA DE PROCESAMIENTO S215
ModoFlujo (S216)
ESTABLECE REGLA DE PROCESAMIENTO S217
ESTABLECE REGLA DE PROCESAMIENTO S217
TRANSMISIÓN DE PAQUETE (S218)
REENVÍO DE PAQUETE (S219)

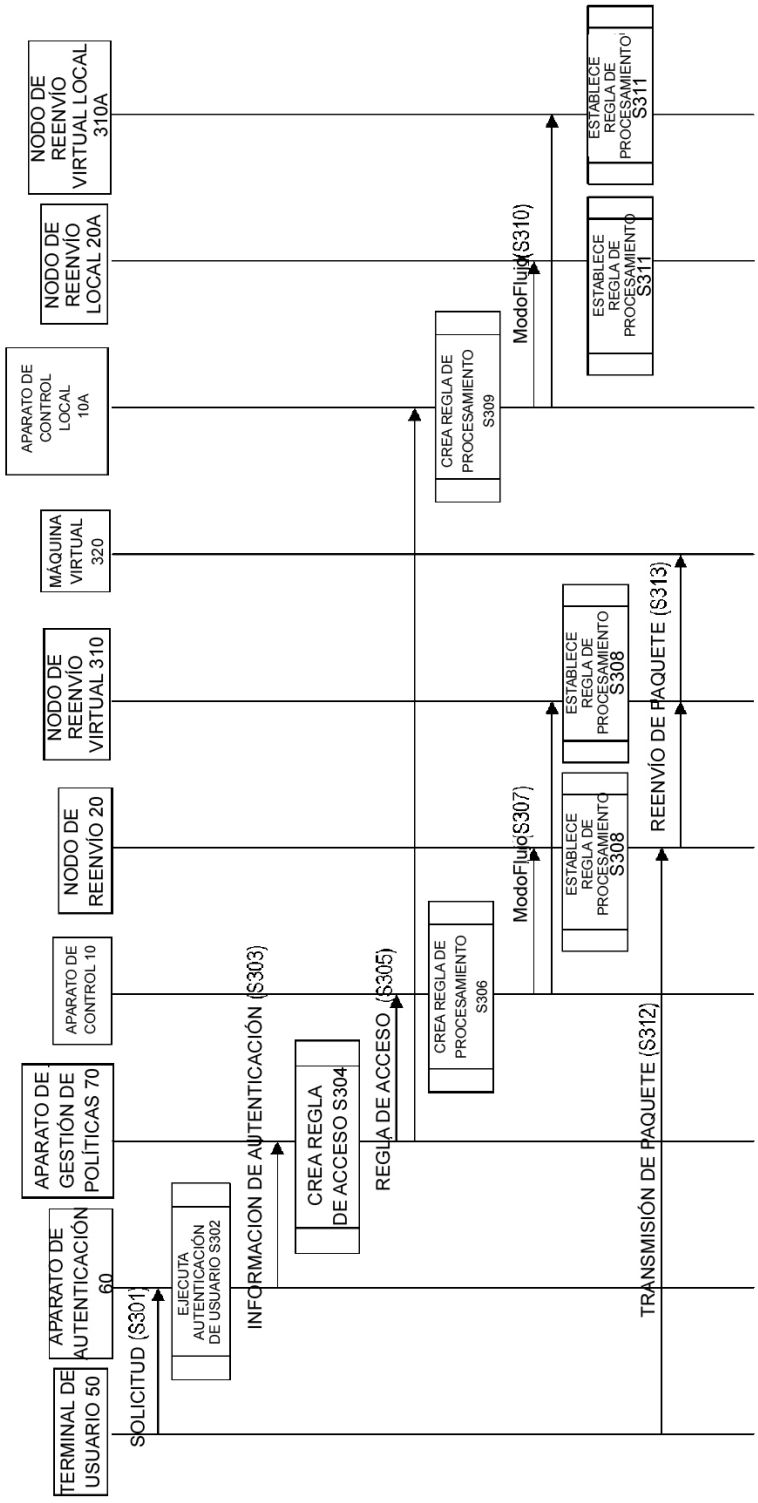
[Fig. 21]


SEGUNDO SISTEMA DE COMUNICACIÓN
PRIMER SISTEMA DE COMUNICACIÓN
MÁQUINA VIRTUAL LOCAL 320A
NODO DE REENVÍO VIRTUAL LOCAL 310A
RECURSO VIRTUAL LOCAL 300A
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES LOCAL 400A
APARATO DE CONTROL LOCAL 10A
NODO DE REENVÍO LOCAL 20A
APARATO DE GESTIÓN DE POLÍTICAS DE COMUNICACIÓN LOCAL 70A
APARATO DE AUTENTICACIÓN LOCAL 60A
APARATO DE MOVIMIENTO DE MÁQUINAS VIRTUALES LOCAL 80A
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
APARATO DE GESTIÓN DE POLÍTICAS DE COMUNICACIÓN 70
APARATO DE AUTENTICACIÓN 60
APARATO DE MOVIMIENTO DE MÁQUINAS VIRTUALES 80
RECURSO VIRTUAL 300
NODO DE REENVIO VIRTUAL 310
MÁQUINA VIRTUAL 320
TERMINAL DE USUARIO 50

[Fig. 22]


TERMINAL DE USUARIO 50
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES 400
APARATO DE CONTROL 10
NODO DE REENVÍO 20
NODO DE REENVÍO VIRTUAL 310
MÁQUINA VIRTUAL 320
APARATO DE GESTIÓN DE MÁQUINAS VIRTUALES LOCAL 400A
APARATO DE CONTROL LOCAL 10A
NODO DE REENVÍO LOCAL 20A
NODO DE REENVÍO VIRTUAL LOCAL 310A
MÁQUINA VIRTUAL LOCAL 320A
EJECUTA AUTENTICACIÓN DE USUARIO S201
SOLICITUD (S202)
CREA MÁQUINA VIRTUAL S203
DISPOSICIÓN (S204)
DISPONE MÁQUINA VIRTUAL S205
FORMA RED ASIGNADA S206
NOTIFICACIÓN DE INFORMACIÓN DE RED LÓGICA (S207)
CREA REGLA DE PROCESAMIENTO S208
ModoFlujo (S209)
ESTABLECE REGLA DE PROCESAMIENTO S210
CREA MÁQUINA VIRTUAL S211
DISPOSICIÓN (S212)
DISPONE MÁQUINA VIRTUAL S213
NOTIFICACIÓN DE INFORMACIÓN DE RED LÓGICA (S214)
CREA REGLA DE PROCESAMIENTO S215
ModoFlujo (S216)
ESTABLECE REGLA DE PROCESAMIENTO S217
TRANSMISIÓN DE PAQUETE (S218)
TRANSMISIÓN DE PAQUETE (S219)

[Fig. 23]


TERMINAL DE USUARIO 50
APARATO DE AUTENTICACIÓN 60
APARATO DE GESTIÓN DE POLÍTICAS 70
APARATO DE CONTROL 10
NODO DE REENVÍO 20
NODO DE REENVÍO VIRTUAL 310
MÁQUINA VIRTUAL 320
APARATO DE CONTROL LOCAL 10A
NODO DE REENVÍO LOCAL 20A
NODO DE REENVÍO VIRTUAL LOCAL 310A
SOLICITUD (S301)
EJECUTA AUTENTICACIÓN DE USUARIO S302
INFORMACION DE AUTENTICACIÓN (S303)
CREA REGLA DE ACCESO S304
REGLA DE ACCESO (S305)
CREA REGLA DE PROCESAMIENTO S306
ModoFlujo(S307)
ESTABLECE REGLA DE PROCESAMIENTO S308
REENVÍO DE PAQUETE (S313)
TRANSMISIÓN DE PAQUETE (S312)
CREA REGLA DE PROCESAMIENTO S309
ModoFlujo(S310)
ESTABLECE REGLA DE PROCESAMIENTO S311
ESTABLECE REGLA DE PROCESAMIENTO S311
ESTABLECE REGLA DE PROCESAMIENTO S311