(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 630 014**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)
H04L 12/801 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.08.2011 PCT/JP2011/004817**

(87) Fecha y número de publicación internacional: **26.07.2012 WO12098596**

(96) Fecha de presentación y número de la solicitud europea: **30.08.2011 E 11856261 (0)**

(97) Fecha y número de publicación de la concesión europea: **19.04.2017 EP 2666264**

(54) Título: **Sistema de comunicación, dispositivo de control, dispositivo de gestión de políticas, método de comunicación, y programa**

(30) Prioridad:

20.01.2011 JP 2011009817

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.08.2017

(73) Titular/es:

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

(72) Inventor/es:

SHIMONISHI, HIDEYUKI;
SONODA, KENTARO;
NAKAE, MASAYUKI;
YAMAGATA, MASAYA y
MORITA, YOICHIRO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de comunicación, dispositivo de control, dispositivo de gestión de políticas, método de comunicación, y programa

CAMPO TÉCNICO

La presente invención se refiere a un sistema de comunicación, un dispositivo de control, un método de comunicación, y un programa, y en particular, se refiere a un sistema de comunicación, un dispositivo de control, un dispositivo de gestión de políticas, un método de comunicación, y un programa, que realiza la comunicación reenviando un paquete a través de los nodos de reenvío dispuestos en una red.

ANTECEDENTES DE LA TÉCNICA

En los últimos años, se ha propuesto la tecnología conocida como FlujoAbierto (referirse a la Publicación Internacional Número WO2008/09501A1, y el artículo de Nick McKeown, y otros 7, "FlujoAbierto: Habilitar la Innovación en las Redes de Campus", [en línea], [búsqueda realizada el 22 de Diciembre de 2010] Internet <URL: http://www.openflowswitch.org//documents/openflow-wp-latest.pdf> y el "FlujoAbierto: Especificación del Conmutador" Versión 1.0.0. (Protocolo de Cableado 0x01), [búsqueda realizada el 22 de Diciembre de 2010] Internet <URL: http://www.openflowswitch.org/documents/openflow-spec-v.1.0.0.pdf>).

En FlujoAbierto, la comunicación se toma como el flujo de extremo a extremo, y el control del trayecto, la recuperación del fallo, el balanceo de la carga y la optimización se realizan en unidades de flujo. Un conmutador de FlujoAbierto como se especifica en "FlujoAbierto: Especificación del Conmutador" está provisto con un canal seguro para la comunicación con un controlador de FlujoAbierto que se considera como un dispositivo de control, y funciona según una tabla de flujo en la que la adición o reescritura apropiada es instruida por el controlador de FlujoAbierto. En la tabla de flujo son definiciones de conjuntos de reglas de coincidencia (campos de la cabecera) que se refieren a las cabeceras de los paquetes, la información estadística de flujo (Contadores), y las acciones (Acciones) que definen el contenido de procesamiento, para cada flujo (referirse a la Figura 24).

Por ejemplo, cuando un conmutador de FlujoAbierto recibe un paquete, se busca una entrada que tenga una regla de coincidencia (referirse a los campos de la cabecera de la Figura 24) que coincida con la información de cabecera del paquete recibido, de la tabla de flujo. Como resultado de la búsqueda, en un caso donde se encuentra una entrada que coincida con el paquete recibido, el conmutador de FlujoAbierto actualiza la información estadística de flujo (Contadores), y también implementa el contenido de procesamiento (transmisión de paquetes desde un puerto especificado, inundación, eliminación y similares) descrito en un campo de Acciones de la entrada, para el paquete recibido. Por otra parte, como resultado de la búsqueda, en una caso donde no se encuentra una entrada que coincida con el paquete recibido, el conmutador de FlujoAbierto reenvía el paquete recibido al controlador de FlujoAbierto a través de un canal seguro, solicita la determinación de un trayecto del paquete basándose en el origen y el destino del paquete recibido, recibe una entrada de flujo para realizar esto, y actualiza la tabla de flujo. De este modo, el conmutador de FlujoAbierto utiliza la entrada contenida en la tabla de flujo como una regla de procesamiento para realizar el reenvío del paquete.

Además, la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1 tiene una descripción en la que un dispositivo de control correspondiente al controlador de FlujoAbierto mencionado anteriormente busca un host autenticado o política de grupo, referido a la política, y únicamente en un caso donde se permite un flujo perteneciente al paquete recibido, realiza la determinación y el establecimiento de un trayecto según la política (referirse a la Figura 6 y a la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1).

Un controlador de FlujoAbierto de la Publicación Internacional Número WO2008/095010A1 se refiere a un archivo de política cuando se genera un nuevo flujo, realiza una comprobación de permiso, y a continuación, lleva a cabo el control de acceso calculando un trayecto (referirse a la Publicación Internacional Número WO2008/095010A1, y a la Figura 6, y a la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1).

De una manera aproximadamente similar, después de confirmar si un host de origen es o no un host autenticado según un puerto de entrada, una dirección de MAC (Control de Acceso al Medio), o una dirección IP, cada vez que se recibe un paquete desde un conmutador subordinado, un NOX (Controlador) de la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1 busca una política basada en un grupo o nombre dado a un usuario o host, y según un resultado de la misma, realiza el reenvío del paquete a un sistema autenticado, la determinación y el establecimiento de un trayecto según la política, y la eliminación de paquetes.

Por lo tanto, hay un problema en eso, con una configuración de bien la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1 o bien de la Publicación de Solicitud de Patente Estadounidense Número US2009/0138577A1, la carga de un dispositivo de control que responde a una solicitud de establecimiento de trayecto de un conmutador subordinado incrementa. Además, debe tenerse en cuenta también una posibilidad de un ataque de DoS (Denegación de Servicio) en un dispositivo de control que utiliza este tipo de disposición.

El artículo titulado “Redes escalares basadas en flujo con DIFANE”, de Minlan Yu et al, publicado en la Revisión de Comunicación Informática, ACM, Nueva York, NY, EE.UU., volumen 41, número 4, 30 de Agosto del 2010, páginas 351-362 discute un sistema en el que las reglas para dirigir paquetes se dividen sobre los conmutadores en la red.

La presente invención se ha hecho a la luz de la situaciones mencionadas anteriormente, y hemos apreciado que sería deseable proporcionar un sistema de comunicación, un dispositivo de control, un método de comunicación, y un programa, con lo cual es posible reducir la carga en un dispositivo de control que realiza una comprobación de política y un control de trayecto en un nodo de reenvío, de acuerdo con una solicitud de un nodo de reenvío como se ha descrito anteriormente.

SUAMRIO DE LA INVENCIÓN

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

Según un segundo, tercer y cuarto aspecto de la presente invención, se proporciona un dispositivo de control correspondiente, un método de comunicación correspondiente realizado por un dispositivo de control y un programa correspondiente para controlar un dispositivo de control.

Debe tenerse en cuenta que el programa puede grabarse en medios informáticos de almacenamiento legibles. Es decir, la presente invención se puede materializar como un producto de programa informático.

Según la presente invención, se puede reducir la carga en un dispositivo de control que realiza una comprobación de política y un control de trayecto de un nodo de reenvío, de acuerdo con una solicitud del nodo de reenvío. Las realizaciones preferidas están cubiertas por las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama para describir un esquema de la presente invención.

La Figura 2 es un diagrama que representa una configuración de un sistema de comunicación de una primera realización de ejemplo de la presente invención.

La Figura 3 es un ejemplo de la información de autenticación almacenada en un dispositivo de autenticación de la primera realización de ejemplo de la presente invención.

La Figura 4 es un ejemplo de la información de la política de comunicación almacenada en una unidad de almacenamiento de políticas de comunicación de la primera realización de ejemplo de la presente invención.

La Figura 5 es un ejemplo de la información de recursos almacenada en una unidad de almacenamiento de información de recursos de la primera realización de ejemplo de la presente invención.

La Figura 6 es un ejemplo de una política de comunicación notificada a un dispositivo de control de un dispositivo de gestión de políticas de la primera realización de ejemplo de la presente invención.

La Figura 7 es un diagrama de bloques que representa una configuración de un dispositivo de control de la primera realización de ejemplo de la presente invención.

La Figura 8 es un diagrama de secuencia que representa una secuencia de las operaciones de la primera realización de ejemplo de la presente invención.

La Figura 9 es un diagrama que representa una tabla de almacenamiento de reglas de procesamiento almacenada en un nodo de reenvío de la primera realización de ejemplo de la presente invención.

La Figura 10 es un diagrama para describir las operaciones hasta que un usuario, que está utilizando un sistema de comunicación de la primera realización de ejemplo de la presente invención, recibe la autenticación del usuario de un dispositivo de autenticación.

La Figura 11 es un diagrama de continuación de la Figura 10.

La Figura 12 es un diagrama que muestra un estado donde se añade una primera regla de procesamiento a la tabla de almacenamiento de reglas de procesamiento de la Figura 9.

La Figura 13 es un diagrama de continuación de la Figura 11.

La Figura 14 es un diagrama de continuación de la Figura 13.

La Figura 15 es un diagrama que muestra un estado donde se añade una segunda regla de procesamiento a la tabla de almacenamiento de reglas de procesamiento de la Figura 12.

La Figura 16 es un diagrama de continuación de la Figura 14.

La Figura 17 es un diagrama de secuencia que representa las operaciones cuando el sistema de comunicación de la primera realización de ejemplo de la presente invención recibe un paquete de datos de un usuario no autenticado.

La Figura 18 es un diagrama de secuencia que representa las operaciones cuando el sistema de comunicación de la primera realización de ejemplo de la presente invención recibe un paquete de datos del usuario que excede los derechos de acceso del usuario.

La Figura 19 es un diagrama de secuencia que representa las operaciones de una segunda realización de ejemplo de la presente invención.

La Figura 20 es un diagrama para describir una configuración de un sistema de comunicación de una tercera realización de ejemplo de la presente invención.

La Figura 21 es un diagrama de secuencia que representa las operaciones de la tercera realización de ejemplo de la presente invención.

La Figura 22 es un ejemplo de la información de la política de comunicación almacenada en una unidad de almacenamiento de políticas de comunicación de una cuarta realización de ejemplo de la presente invención.
La Figura 23 es un diagrama para describir las operaciones de la cuarta realización de ejemplo de la presente invención.
La Figura 24 es un diagrama que representa una configuración de una entrada de flujo descrita en "FlujoAbierto: Especificación del Conmutador".

DESCRIPCIÓN DE LAS REALIZACIONES

Primero, se da una descripción acerca de un esquema de la presente invención, haciendo referencia a los dibujos. Como se muestra en la Figura 1, la presente invención se realiza mediante los nodos 200A y 200B de reenvío, que reenvían un paquete transmitido desde un terminal de usuario de acuerdo con una regla de procesamiento establecida por un dispositivo 300 de control, un dispositivo 320 de gestión de políticas que gestiona una política de comunicación y notifica al dispositivo 300 de control de una política de comunicación, que se ha concedido a un usuario para quien la autenticación ha tenido éxito, y el dispositivo 300 de control que establece una regla de procesamiento en los nodos 200A y 200B de reenvío. Hay que señalar que los símbolos de referencia en los dibujos anexados a este resumen se adjuntan a los elementos respectivos por conveniencia como un ejemplo con el fin de ayudar a la comprensión, y no pretenden limitar la presente invención a los modos mostrados en los dibujos.

Más específicamente, el dispositivo 300 de control comprende una unidad 301 de autorización de transmisión de la solicitud de establecimiento y una unidad 302 de control del trayecto. La unidad 301 de autorización de transmisión de la solicitud de establecimiento establece una primera regla de procesamiento que causa que un nodo de reenvío (por ejemplo, el nodo 200A de reenvío de la Figura 1), que recibe un paquete del terminal 100 de usuario, haga una solicitud de establecimiento de una regla de procesamiento con respecto a un paquete transmitido desde el terminal 100 de usuario, basándose en una notificación (Figura 1, (2) política de comunicación) del dispositivo 320 de gestión de políticas, enviado en un disparador prescrito (por ejemplo, Figura 1, (1) protocolo de autenticación de usuario) (Figura 1, (3) establecimiento de la primera regla de procesamiento).

Después, al recibir un paquete de datos del terminal 100 de usuario (Figura 1, (4) paquete de datos), un nodo de reenvío (por ejemplo, el nodo 200A de reenvío de la Figura 1) hace una solicitud al dispositivo 300 de control para establecer una regla de procesamiento con respecto a un paquete transmitido desde el terminal 100 de usuario de acuerdo con la primera regla de procesamiento.

En un caso de recibir una solicitud para el establecimiento de una regla de procesamiento desde un nodo de reenvío como se ha descrito anteriormente (Figura 1, (5) solicitud de establecimiento para la segunda regla de procesamiento), la unidad 302 de control del trayecto del dispositivo 300 de control genera un trayecto desde el terminal 100 de usuario a un destino de acceso (por ejemplo, un recurso 600 de red) de acuerdo con la política de comunicación, y establece la segunda regla de procesamiento que realiza el trayecto (Figura 1, (6) establecimiento de la segunda regla de procesamiento).

Además, en un caso de recibir un paquete para el que ni la primera ni la segunda regla de procesamiento son relevantes, los nodos 200A y 200B de reenvío realizan el procesamiento para eliminar (descartar) el paquete.

Como se ha descrito anteriormente, ya que debe satisfacerse una condición en la que se establece la primera regla de procesamiento para solicitar al dispositivo 300 de control que establezca la segunda regla de procesamiento que procesa un flujo real, es posible tener una disposición tal que las solicitudes para establecer las reglas de procesamiento no se concentren en el dispositivo de control, y también que se pueda mejorar la resistencia a un ataque de DoS.

Hay que señalar que el ejemplo de la Figura 1 muestra una configuración en la que el dispositivo 300 de control comprende la unidad 301 de autorización de transmisión de la solicitud de establecimiento y el dispositivo 302 para el control del trayecto, cada una de los cuales es independiente, pero dado que ambos tienen un punto en común en que generan y establecen una regla de procesamiento, la realización es posible por dos medios de procesamiento con funciones separadas, siendo un medio para generar una regla de procesamiento (unidad de cálculo de trayecto y acción de una primera realización de ejemplo como se describe más adelante) y un medio para establecer una regla de procesamiento (una unidad de gestión de reglas de procesamiento de la primera realización de ejemplo como se describe más adelante), tal como se adoptó en una realización de ejemplo que se describirá más adelante.

(Primera realización de ejemplo)

A continuación, se da una descripción detallada acerca de una primera realización de ejemplo de la presente invención, haciendo referencia a los dibujos. La Figura 2 es un diagrama que representa una configuración de un sistema de comunicación de la primera realización de ejemplo de la presente invención. Referente a la Figura 2, se muestra una configuración que incluye una pluralidad de nodos 201 a 204 de reenvío, un dispositivo 300 de control que establece una regla de procesamiento en estos nodos de reenvío, un dispositivo 320 de gestión de políticas que notifica al dispositivo 300 de control de una política de comunicación, y un dispositivo 310 de autenticación que proporciona la información de autenticación mostrando un resultado de la autenticación al dispositivo 320 de gestión de políticas.

Los nodos 201 a 204 de reenvío son dispositivos de conmutación que procesan un paquete recibido de acuerdo con una regla de procesamiento que asocia una regla de coincidencia que se refiere a un paquete recibido y que procesa el contenido aplicado a un paquete que coincide con la regla de coincidencia. Con respecto a estos nodos 201 a 204 de reenvío, es posible utilizar un conmutador de FlujoAbierto como en “FlujoAbierto: Especificación del Conmutador” mediante el cual una entrada de flujo mostrada en la Figura 24 se opera como una regla de procesamiento.

Además, los recursos 600A y 600B de red están conectados al nodo 204 de reenvío, y un terminal 100 de usuario puede comunicarse con los recursos 600A y 600B de red, a través de los nodos 201 a 204 de reenvío. En la siguiente realización de ejemplo, el recurso 600A de red y el recurso 600B de red pertenecen respectivamente a diferentes grupos de recursos, y el grupo_0001_de recursos y el grupo_0002_de recursos se adjuntan a ellos como IDs respectivos de grupos de recursos.

El dispositivo 310 de autenticación es un servidor de autenticación o similar, que utiliza una contraseña o información biométrica de autenticación para realizar un protocolo de autenticación del usuario con un terminal 100 de usuario. El dispositivo 310 de autenticación transmite la información de autenticación que indica un resultado del protocolo de autenticación del usuario con el terminal 100 de usuario al dispositivo 320 de gestión de políticas.

La Figura 3 es un ejemplo de la información de autenticación almacenada en el dispositivo 310 de autenticación de la presente realización de ejemplo. Por ejemplo, en un caso donde la autenticación de un usuario cuyo ID de usuario es usuario1 tenga éxito, el dispositivo 310 de autenticación transmite los atributos del usuario1, la dirección IP: 192.168.100.1, y la dirección MAC: 00-00-00-44-55-66, y una entrada de usuario1 de ID de rol: rol_0001 y rol_0002 como la información de autenticación al dispositivo 320 de gestión de políticas. De manera similar, en un caso donde la autenticación de un usuario cuyo ID de usuario es usuario2 tenga éxito, los atributos del usuario2, la dirección IP: 192.168.100.2, y la dirección MAC: 00-00-00-77-88-99, y una entrada de usuario2 de ID de rol: rol_0002 se transmiten como información de autenticación al dispositivo 320 de gestión de políticas.

Hay que señalar que la información de autenticación puede ser información mediante la cual el dispositivo 320 de gestión de políticas puede determinar una política de comunicación dada a un usuario, y no se limita a un ejemplo de la Figura 3. Por ejemplo, es posible utilizar el ID de usuario de un usuario para quien la autenticación ha tenido éxito, un ID de rol derivado del ID de usuario, un ID de acceso tal como una dirección MAC o similar, la información de la localización para el terminal 100 de usuario, o una combinación de los mismos, como información de autenticación. Evidentemente, la información acerca de un usuario para el que ha fallado la autenticación puede transmitirse al dispositivo 320 de gestión de políticas, como información de autenticación, y una política de comunicación mediante la cual el dispositivo 320 de gestión de políticas limita el acceso del usuario puede transmitirse al dispositivo 300 de control.

El dispositivo 320 de gestión de políticas es un dispositivo que está conectado a una unidad 321 de almacenamiento de políticas de comunicación y a una unidad 322 de almacenamiento de información de recursos; determina una política de comunicación en respuesta a la información de autenticación recibida del dispositivo 310 de autenticación; y transmite al dispositivo 300 de control.

La Figura 4 es un ejemplo de la información de la política de comunicación almacenada en la unidad 321 de almacenamiento de políticas de comunicación. En el ejemplo de la Figura 4, para cada rol identificado por un ID de rol, se muestra la información de la política de comunicación que establece un ID de grupo de recursos dado a un grupo de recursos, y derechos de acceso. Por ejemplo, un usuario que tiene un ID de rol: rol_0001 tiene acceso a ambos IDs de grupos de recursos: grupo_0001_de recursos y grupo_0002_de recursos. Por otro lado, un usuario que tiene un ID de rol_ rol_0002 no tiene acceso al ID de grupo de recursos: grupo_0001_de recursos, pero tiene acceso al grupo_0002_de recursos.

La Figura 5 es un ejemplo de la información de recursos almacenada en la unidad 322 de almacenamiento de información de recursos. El ejemplo de la Figura 5 tiene contenido que asocia los IDs de recursos de los recursos pertenecientes a los IDs de grupos de recursos antes mencionados y a los atributos detallados de los mismos. Por ejemplo, se incluyen el recurso_0001, el recurso_0002, y el recurso_0003 de los recursos en un grupo identificado por el ID de grupo de recursos: grupo_0001_de recursos, y es posible identificar la dirección IP, la dirección MAC, y los números de puerto utilizados en los servicios, para cada uno de ellos.

Referente a la información de la política de comunicación y a la información de recursos descritas anteriormente, el dispositivo 320 de gestión de políticas determina una política de comunicación para un usuario que ha recibido la autenticación en el dispositivo 310 de autenticación, y entrega una notificación al dispositivo 300 de control. Por ejemplo, con un ID de rol incluido en la información de autenticación recibida del dispositivo 310 de autenticación, es posible identificar el contenido de un ID de grupo de recursos adjunto al ID de rol correspondiente y a los derechos de acceso del mismo, de la información de la política de la Figura 4. La información de un recurso perteneciente al ID de grupo de recursos de la información de recursos de la Figura 5 se utiliza para generar una política de comunicación.

La Figura 6 ilustra una política de comunicación de un usuario que tiene un ID de usuario: usuario_1 generado de la información mostrada en la Figura 3, Figura 4, y Figura 5. Se establece un valor de la información de los atributos del ID de usuario: usuario_1 de la información de autenticación de la Figura 3 en un campo de origen de la Figura 6. Además, se establece un atributo del recurso extraído de la información de recursos de la Figura 5, basándose en el contenido del ID de rol: rol_0001 de la información de la política de la Figura 4, en un campo de destino. Asimismo, se establece un valor igual al de los derechos de acceso del ID de rol: rol_0001 de la información de la política de la Figura 4 en un campo de derechos de acceso. Además, un servicio que se establece en un campo de atributos del recurso de la información de recursos de la Figura 5 y un número de puerto se establecen en un campo de condiciones (opciones).

Al recibir la política de comunicación como se ha descrito anteriormente, el dispositivo 300 de control primero genera una primera regla de procesamiento mediante la cual se transmite una solicitud para el establecimiento de un procesamiento con respecto a un paquete desde un usuario que es un objetivo de la aplicación de la política de comunicación, y para establecerse en un nodo de reenvío seleccionado de los nodos 201 a 204 de reenvío. Además, en un caso de recibir una solicitud para el establecimiento de una regla de procesamiento, según la primera regla de procesamiento, el dispositivo 300 de control genera un trayecto de reenvío para un paquete y una regla de procesamiento que realiza el trayecto de reenvío, basándose en la información del paquete incluida en la solicitud para el establecimiento de la regla de procesamiento, para establecerse en un nodo de reenvío a lo largo del trayecto de reenvío del paquete.

La Figura 7 es un diagrama de bloques que representa una configuración detallada del dispositivo 300 de control de la presente realización de ejemplo. Referente a la Figura 7, el dispositivo 300 de control comprende: una unidad 11 de comunicación del nodo que realiza la comunicación con los nodos 201 a 204 de reenvío, una unidad 12 de procesamiento de mensajes de control, una unidad 13 de gestión de reglas de procesamiento, una unidad 14 de almacenamiento de reglas de procesamiento, una unidad 15 de gestión del nodo de reenvío, una unidad 16 de cálculo de trayecto y acción, una unidad 17 de gestión de topologías, una unidad 18 de gestión de la localización del terminal, una unidad 19 de gestión de políticas de comunicación, y una unidad 20 de almacenamiento de políticas de comunicación. Estas operan respectivamente como sigue.

La unidad 12 de procesamiento de mensajes de control analiza un mensaje de control recibido de un nodo de reenvío, y entrega la información del mensaje de control a un medio de procesamiento relevante en el dispositivo 300 de control.

La unidad 13 de gestión de reglas de procesamiento gestiona como se establece una regla de procesamiento y en que nodo de reenvío. Específicamente, una regla de procesamiento generada en la unidad 16 de cálculo de trayecto y acción se registra en la unidad 14 de almacenamiento de reglas de procesamiento y se establece en un nodo de reenvío, y en respuesta a un caso donde ocurre un cambio en una regla de procesamiento que ha sido establecida en un nodo de reenvío, según una notificación de eliminación de la regla de procesamiento o similar de un nodo de reenvío, la información registrada en la unidad 14 de almacenamiento de reglas de procesamiento se actualiza.

La unidad 15 de gestión del nodo de reenvío gestiona la capacidad (por ejemplo, el número y tipo de los puertos, el tipo de acciones soportadas, y similares) de un nodo de reenvío controlado por el dispositivo 300 de control.

Al recibir una política de comunicación de la unidad 19 de gestión de políticas de comunicación, la unidad 16 de cálculo de trayecto y acción se refiere primero a la topología de red almacenada en la unidad 17 de gestión de topologías, de acuerdo con la política de comunicación, y genera una regla de procesamiento (primera regla de procesamiento) que ejecuta una solicitud para el establecimiento de un procesamiento con respecto a un paquete de un usuario. Hay que señalar que el nodo de reenvío, que tiene un destino de conjunto de la regla de procesamiento (primera regla de procesamiento), puede ser todos los nodos de reenvío a los que existe una posibilidad de que el terminal 100 de usuario se conecte a, o bien, se puede seleccionar un nodo de reenvío (por ejemplo, el nodo 201 de reenvío de la Figura 1) de la unidad 18 de gestión de la localización del terminal basándose en la información de origen incluida en la política de comunicación.

Además, al recibir una solicitud para el establecimiento de una regla de procesamiento, basándose en la regla de procesamiento antes mencionada (primera regla de procesamiento), la unidad 16 de cálculo de trayecto y acción genera, basándose en la información del paquete incluida en la solicitud para el establecimiento de la regla de procesamiento, un nodo de reenvío para el paquete y una regla de procesamiento que realiza el trayecto de reenvío.

Específicamente, la unidad 16 de cálculo de trayecto y acción calcula el trayecto de reenvío del paquete basándose en la información de localización de un terminal de comunicación gestionado por la unidad 18 de gestión de la localización del terminal y en la información de la topología de red configurada en la unidad 17 de gestión de topologías. A continuación, la unidad 16 de cálculo de trayecto y acción adquiere la información del puerto y similares de un nodo de reenvío en el trayecto de reenvío, de la unidad 15 de gestión del nodo de reenvío, y obtiene una acción ejecutada en un nodo de reenvío en el trayecto con el fin de realizar el trayecto de reenvío calculado y una regla de coincidencia que identifica el flujo al que se aplica la acción. Hay que señalar que la regla de

coincidencia se puede generar utilizando una dirección IP de origen, una dirección IP de destino, las condiciones (opciones), o similar, de la política de comunicación de la Figura 6. Por lo tanto, en un caso de una primera entrada de la política de comunicación de la Figura 6, con respecto a un paquete desde una IP 192.168.100.1 de origen a una IP 192.168.0.1 de destino, se generan las reglas de procesamiento respectivas que deciden un nodo de reenvío que es el salto siguiente, o una acción para reenviar desde un puerto al que están conectados los recursos 600A y 600B de red. Hay que señalar que, con ocasión del establecimiento de la regla de procesamiento antes mencionada, se puede generar una regla de procesamiento no sólo para un paquete para el que se ha recibido una solicitud para el establecimiento de una regla de procesamiento, sino también para realizar el reenvío del paquete a un recurso para el que un terminal de usuario tiene derechos de acceso.

La unidad 17 de gestión de topologías configura la información de la topología de red basándose en las relaciones de conexión de los nodos 201 a 204 de reenvío recogidas a través de la unidad 11 de comunicación del nodo.

La unidad 18 de gestión de la localización del terminal gestiona la información que identifica la localización de un terminal de usuario conectado al sistema de comunicación. En la presente realización de ejemplo, se da una descripción en la que, con una dirección IP como la información para identificar un terminal de usuario, se utiliza la información de un identificador del nodo de reenvío de un nodo de reenvío al que está conectado el terminal de usuario, y de un puerto del mismo, como información para identificar la localización del terminal de usuario. Claramente, en lugar de estos elementos de información, la información proporcionada por el dispositivo 310 de autenticación, por ejemplo, o similar se puede utilizar para identificar el terminal y su localización.

Al recibir la información de la política de comunicación del dispositivo 320 de gestión de políticas, la unidad 19 de gestión de políticas de comunicación almacena la información en la unidad 20 de almacenamiento de políticas de comunicación, y también transmite la información a la unidad 16 de cálculo de trayecto y acción.

El tipo anterior de dispositivo 300 de control se puede realizar añadiendo una función para generar la primera regla de procesamiento (entrada de flujo) con la recepción de la política de comunicación antes mencionada como un disparador, basándose en un controlador de FlujoAbierto de Nick McKeown, y otros 7, “FlujoAbierto: Habilitar la Innovación en las Redes de Campus”, y “FlujoAbierto: Especificación del Conmutador”.

Además, las unidades respectivas (medios de procesamiento) del dispositivo 300 de control mostrado en la Figura 7 pueden realizarse mediante un programa informático que almacena los elementos de información respectivos descritos anteriormente, y que ejecuta cada uno de los procesos descritos anteriormente, en un ordenador que forma el dispositivo 300 de control, utilizando su hardware.

A continuación, se da una descripción detallada acerca de una operación de la presente realización de ejemplo haciendo referencia a los dibujos. En lo que sigue, se da una descripción en la que se establece una regla de procesamiento, como se muestra en la Figura 8, en el nodo 201 de reenvío conectado al terminal de usuario. La entrada superior es una regla de procesamiento que reenvía un paquete perteneciente al flujo #A al nodo 203 de reenvío. La tercera entrada desde arriba es una regla de procesamiento que reenvía un paquete autenticado al dispositivo 310 de autenticación. Además, la entrada inferior es una regla de procesamiento que elimina los otros paquetes que no se relacionan con la regla de procesamiento de prioridad más alta como se ha descrito anteriormente. Además, con el fin de buscar una regla de procesamiento que tenga una regla de coincidencia que coincida con un paquete recibido, en secuencia desde arriba, se le da una prioridad a un nodo de reenvío en la cual, cuanto mayor es la posición, mayor es la prioridad.

La Figura 9 es un diagrama de secuencia que representa una secuencia de las operaciones de la presente realización de ejemplo. Referente a la Figura 9, primero, cuando un terminal de usuario hace una solicitud de inicio de sesión al dispositivo 310 de autenticación, como se muestra en la Figura 10, el nodo 201 de reenvío realiza el reenvío del paquete al dispositivo 310 de autenticación, de acuerdo con una regla de procesamiento para un paquete autenticado mostrado en la Figura 8 (S001 en la Figura 9).

Cuando el dispositivo 310 de autenticación realiza la autenticación del usuario (S002 en la Figura 9), y transmite la información de autenticación al dispositivo 320 de gestión de políticas (S003 en la Figura 9), el dispositivo 320 de gestión de políticas se refiere a la unidad 321 de almacenamiento de políticas de comunicación y a la unidad 322 de almacenamiento de información de recursos basándose en la información de autenticación recibida, determina una política de comunicación (S004 en la Figura 9), y transmite al dispositivo 300 de control (referirse a S005 en la Figura 9, y a la Figura 11).

Al recibir la política de comunicación, el dispositivo 300 de control establece una primera regla de procesamiento para hacer una solicitud de establecimiento de un procesamiento con respecto a un paquete del terminal de usuario, en el nodo 201 de reenvío (referirse a S006 en la Figura 9, y a la Figura 11).

La Figura 12 es un diagrama que muestra una regla de procesamiento establecida en el nodo 201 de reenvío, después de establecer la primera regla de procesamiento. En el ejemplo de la Figura 12, se establece una regla de procesamiento (primera regla de procesamiento), que causa que un paquete recibido sea reenviado al dispositivo

300 de control de un terminal autenticado, en una localización con una prioridad más baja que la de un paquete autenticado.

Después, cuando el terminal de usuario transmite un paquete con un destino de un recurso de red (S007 en la Figura 9), como se muestra en la Figura 13, el nodo 201 de reenvío en el que se ha establecido la primera regla de procesamiento transmite una solicitud para el establecimiento de una regla de procesamiento, al dispositivo 300 de control (S008 en la Figura 9).

El dispositivo 300 de control que ha recibido la solicitud para el establecimiento de una regla de procesamiento realiza el cálculo de un trayecto de reenvío de un paquete para el que se ha recibido la solicitud para el establecimiento de la regla de procesamiento, de acuerdo con la política de comunicación, y como se muestra en la Figura 14, genera y establece una regla de procesamiento que prescribe el contenido de procesamiento del paquete en los respectivos nodos de reenvío (S009 en la Figura 9).

La Figura 15 es un diagrama que muestra una regla de procesamiento establecida en el nodo 201 de reenvío, después de establecer la segunda regla de procesamiento. En el ejemplo de la Figura 15, una regla de procesamiento (segunda regla de procesamiento) que causa que un terminal de usuario reenvíe un paquete (flujo #B) con un destino de un recurso de red al nodo 202 de reenvío.

Como se ha descrito anteriormente, cuando el dispositivo 300 de control establece una regla de procesamiento en un nodo de reenvío en un trayecto de reenvío, como se muestra en la Figura 16, la comunicación se hace posible entre el terminal de usuario y el recurso de red (“iniciar la comunicación” en la Figura 9).

La Figura 17 es un diagrama de secuencia que representa las operaciones en un caso donde un paquete con un destino de un recurso de red es trasmitido por el terminal de usuario, sin pasar la autenticación de usuario. Como se muestra en la Figura 8, puesto que se ha establecido, en el nodo 201 de reenvío, una regla de procesamiento que elimina (descarta) los paquetes (otros paquetes en la Figura 8) que no coinciden con una regla de procesamiento que ya se ha establecido, el nodo 201 de reenvío elimina el paquete recibido (S009 en la Figura 17).

La Figura 18 es un diagrama de secuencia que representa las operaciones en un caso donde se ha pasado la autenticación de usuario pero un paquete (por ejemplo, el flujo #C), que tiene un destino de un recurso de red sin derechos de acceso, es transmitido por el terminal de usuario. En este caso también, como se muestra en la Figura 15, puesto que en el nodo 201 de reenvío se establece una regla de procesamiento que elimina los paquetes (otros paquetes en la Figura 15) que no coinciden con una regla de procesamiento que ya se ha establecido, el nodo 201 de reenvío elimina un paquete recibido (S009 en la Figura 18). Además, especificando un destino o puerto como una regla de coincidencia de la primera regla de procesamiento, es posible reducir el número de paquetes para los que se solicita al dispositivo 300 de control establecer una regla de procesamiento, y eliminar los otros paquetes.

Como se ha descrito anteriormente, mediante una disposición en la que, cuando se recibe un paquete desconocido, se hace que el nodo de reenvío elimine el paquete, y con la recepción de una política de comunicación como un disparador, el dispositivo 300 de control primero establece una primera regla de procesamiento que permite la propia solicitud para el establecimiento de una regla de procesamiento, es posible reducir el número de solicitudes para establecer una regla de procesamiento emitidas por los nodos de reenvío. Como resultado, es posible reducir la carga en el dispositivo de control que acompaña las solicitudes para establecer una regla de procesamiento.

(Segunda realización de ejemplo)

A continuación, se da una descripción acerca de una segunda realización de ejemplo de la presente invención, en la que se añade una modificación a las operaciones de un dispositivo de autenticación y de un dispositivo de gestión de políticas de la primera realización de ejemplo como se ha descrito anteriormente. Puesto que la presente realización de ejemplo puede realizarse con una configuración que es equivalente a la primera realización de ejemplo descrita anteriormente, se da a continuación una descripción centrándose en los puntos de diferencia en sus operaciones.

La Figura 19 es un diagrama de secuencia que representa una secuencia de las operaciones de la presente realización de ejemplo. Las operaciones hasta donde un terminal de usuario hace una solicitud de inicio de sesión a un dispositivo 310 de autenticación (S101 en la Figura 19), y la autenticación del usuario se realiza en el dispositivo 310 de autenticación, son similares a la primera realización de ejemplo. En la presente realización de ejemplo, si la autenticación del usuario falla (S102 en la Figura 19), el dispositivo 310 de autenticación transmite la información (NG) de autenticación a un dispositivo 320 de gestión de políticas (S103-1 en la Figura 19).

El dispositivo 320 de gestión de políticas que recibe la información NG de autenticación transmite la información NG de autenticación recibida a un dispositivo 300 de control (S103-2 en la Figura 19). Aquí, la información que especifica un terminal de usuario para el que la autenticación ha fallado (dirección MAC o información sobre los nodos de reenvío conectados) se incluye en la información NG de autenticación recibida.

El dispositivo 300 de control que recibe la información NG de autenticación establece una regla de procesamiento para eliminar un paquete del terminal de usuario en un nodo 201 de reenvío, y también en un nodo de reenvío para el que hay una posibilidad de estar conectado al terminal de usuario. Hay que señalar que es deseable dar una mayor prioridad a esta regla de procesamiento que a otras reglas de procesamiento.

Después, cuando el terminal de usuario transmite un paquete para intentar iniciar sesión nuevamente (S101A en la Figura 19), el nodo 201 de reenvío realiza el procesamiento para eliminar el paquete transmitido desde el terminal de usuario (S109 en la Figura 19).

Como se ha descrito anteriormente, según la presente realización de ejemplo, además de un efecto de la primera realización de ejemplo descrita anteriormente, es posible restringir el reenvío al dispositivo 310 de autenticación de un paquete desde un usuario para el que la autenticación ha fallado una vez, y proteger del acceso no autorizado de un usuario malintencionado. Además, en la realización de ejemplo descrita anteriormente se ha dado una descripción en la que se elimina el paquete del terminal de usuario, pero se puede establecer una regla de procesamiento, lo que causa el acceso a un servidor específico que muestra un mensaje que no es posible el acceso para el terminal de usuario. Hay que señalar que en la descripción antes mencionada, se transmite la información de un usuario (terminal) para el que la autenticación ha fallado, pero se puede hacer que una política de comunicación de la primera realización de ejemplo descrita anteriormente mantenga una bandera o similar prohibiendo el establecimiento de una primera regla de procesamiento, y se puede dar una instrucción para eliminar un paquete del terminal de usuario.

(Tercera realización de ejemplo)
A continuación, se da una descripción acerca de una tercera realización de ejemplo de la presente invención, en la que se refuerza una función de seguridad de la primera realización de ejemplo descrita anteriormente. Puesto que la presente realización de ejemplo puede realizarse con una configuración que está aproximadamente en común con la primera realización de ejemplo descrita anteriormente, se da a continuación una descripción centrándose en los puntos de diferencia.

La Figura 20 es un diagrama para describir una configuración de un sistema de comunicación de la tercera realización de ejemplo de la presente invención. Un punto de diferencia en la configuración con respecto a la primera realización de ejemplo representada en la Figura 2 es que se añade un segundo dispositivo 311 de autenticación en paralelo a un (primer) dispositivo 310 de autenticación. El segundo dispositivo 311 de autenticación, similar al dispositivo 310 de autenticación, puede transmitir un resultado de la autenticación del usuario con respecto a un terminal 100 de usuario a través de un nodo 201 de reenvío a un dispositivo 320 de gestión de políticas.

La Figura 21 es un diagrama de secuencia que representa una operación de la tercera realización de ejemplo de la presente invención. El terminal de usuario hace una solicitud de inicio de sesión al dispositivo 310 de autenticación (S201 en la Figura 21), y se realiza un protocolo de autenticación del usuario en el dispositivo 310 de autenticación (S202 en la Figura 21). El dispositivo 310 de autenticación transmite un resultado del mismo a un dispositivo 320 de gestión de políticas y al segundo dispositivo 311 de autenticación (S203 en la Figura 21).

Al confirmar que un origen de la información de autenticación es el dispositivo 310 de autenticación, el dispositivo 320 de gestión de políticas genera una política de comunicación que indica que no se ha completado por el terminal de usuario un protocolo de autenticación del usuario con el dispositivo 311 de autenticación, y transmite a un dispositivo 300 de control (S204 y 205 en la Figura 21).

El dispositivo 300 de control que recibe la política de comunicación establece al nodo 201 de reenvío una regla de procesamiento que redirige un paquete enviado después desde un terminal de usuario al segundo dispositivo 311 de autenticación (S206 en la Figura 21).

Después, al recibir el paquete del terminal de usuario, el nodo 201 de reenvío redirige al segundo dispositivo 311 de autenticación, de acuerdo con la regla de procesamiento (S207-1 y S207-2 en la Figura 21). El segundo dispositivo 311 de autenticación hace una solicitud para un protocolo de autenticación del usuario al terminal de usuario (S208 de la Figura 21).

Después, se realiza el protocolo de autenticación del usuario entre el terminal de usuario y el dispositivo 311 de autenticación (S209 y S210 en la Figura 21), y se transmite un resultado de la misma a un dispositivo 320 de gestión de políticas (S211 de la Figura 21).

Al confirmar que un origen de la información de autenticación es el dispositivo 311 de autenticación, similar a la primera realización de ejemplo, el dispositivo 320 de gestión de políticas se refiere a una unidad 321 de almacenamiento de políticas de comunicación y a una unidad 322 de almacenamiento de información de recursos basándose en la información de autenticación recibida, determina una política de comunicación (S212 de la Figura 21), y transmite la política al dispositivo 300 de control (S213 de la Figura 21).

Las siguientes operaciones son similares a la primera realización de ejemplo: al recibir la política de comunicación, el dispositivo 300 de control establece una primera regla de procesamiento para hacer una solicitud para el establecimiento de un procesamiento con respecto a un paquete de un terminal de usuario en un nodo 201 de reenvío (S214 en la Figura 21).

De este modo, es posible solicitar el establecimiento de la regla de procesamiento para el paquete recibido del terminal de usuario, y después, basándose en el paquete recibido del terminal de usuario se hace una solicitud al dispositivo 300 de control para establecer una regla de procesamiento (S215 y S216 de la Figura 21), y el cálculo del trayecto y el establecimiento de una regla de procesamiento se realizan en el dispositivo 300 de control (S217 en la Figura 21).

Como se ha descrito anteriormente, según la presente realización de ejemplo, se puede reducir aún más la posibilidad de que una primera y una segunda regla de procesamiento sean establecidas por un usuario malintencionado.

Hay que señalar que en la tercera realización de ejemplo descrita anteriormente, se ha dado una descripción en la que se utilizan dos dispositivos de autenticación, los dispositivos 310 y 311 de autenticación, pero también se puede emplear una configuración en la que se utilizan 3 o más dispositivos de autenticación. Además, también se puede emplear una realización de ejemplo modificada en la que, según un resultado inicial de la autenticación, se asigna un destino de redirección al segundo dispositivo 311 de autenticación u otros dispositivos de autenticación.

Además, en la tercera realización de ejemplo descrita anteriormente, se ha dado una descripción en la que el dispositivo 320 de gestión de políticas determina si se ha completado o no un protocolo de autenticación del usuario con una pluralidad predeterminada de dispositivos de autenticación por el terminal de usuario. Sin embargo, también es posible una configuración en la que se proporciona una tabla o similar que gestiona un estado de autenticación de los respectivos usuarios, en el lado del dispositivo 320 de gestión de políticas. De este modo, es posible utilizar un método en el que, después de realizar primero el protocolo de autenticación del usuario con el dispositivo 311 de autenticación, se realiza el protocolo de autenticación del usuario con el dispositivo 310 de autenticación. Además, es posible una disposición en la que es suficiente si la gestión se realiza proporcionando un período de validez apropiado para los resultados de la autenticación obtenidos de los respectivos dispositivos de autenticación, y se realiza un protocolo de autenticación del usuario con los dispositivos de autenticación para los que ha expirado el período de validez.

(Cuarta realización de ejemplo)

Además, en la realización de ejemplo descrita anteriormente se ha dado una descripción en la que un dispositivo 300 de control establece una primera regla de procesamiento en un nodo 201 de reenvío. Sin embargo, es posible una disposición donde se establece la primera regla de procesamiento en una pluralidad de nodos de reenvío. Se da a continuación una descripción acerca de una cuarta realización de ejemplo en la que el dispositivo 300 de control establece una primera regla de procesamiento en una pluralidad de nodos de reenvío. Puesto que la presente realización de ejemplo puede realizarse con una configuración que es equivalente a la primera realización de ejemplo descrita anteriormente, se da a continuación una descripción centrada en los puntos de diferencia.

La Figura 22 es un ejemplo de la información de la política de comunicación almacenada en una unidad de almacenamiento de políticas de comunicación de la cuarta realización de ejemplo de la presente invención. Un punto de diferencia de la información de la política de comunicación almacenada en la unidad de almacenamiento de políticas de comunicación de la primera realización de ejemplo es que se añade un campo de limitación del rango de movimiento que indica un rango de movimiento posible de un terminal de usuario.

Las operaciones generales son similares a la primera realización de ejemplo descrita anteriormente. Sin embargo, un dispositivo 320 de gestión de políticas, basándose en la información de la política de comunicación como se ha descrito anteriormente, da una instrucción a un dispositivo 300 de control para establecer una primera regla de procesamiento en un nodo de reenvío determinado en el campo de limitación del rango de movimiento, como se muestra en la Figura 23.

De este modo, además del nodo 201 de reenvío, es posible establecer también una primera regla de procesamiento en un nodo de reenvío al cual es posible una conexión por el movimiento del terminal de usuario (por ejemplo, el nodo 203 de reenvío en la Figura 23), y se permite el movimiento del usuario con limitaciones. Además, en un caso donde el usuario se mueve realmente a estos nodos de reenvío, es posible omitir un proceso de un protocolo de autenticación del usuario (S001 “iniciar sesión” en la Figura 9) hasta el establecimiento (S006 en la Figura 9) de la primera regla de procesamiento por el dispositivo 300 de control.

Hay que señalar que, como se muestra en la Figura 22, el número de nodos de reenvío establecidos en el campo de limitación del rango de movimiento puede establecerse de manera apropiada de acuerdo con los roles o grupos de recursos de los respectivos usuarios. Además, como en la Figura 22, en lugar de describir un nodo de reenvío para el que se establece la primera regla de procesamiento, se puede especificar una distancia (número de saltos) desde un nodo de reenvío al que está conectado actualmente el terminal de usuario en el campo de limitación del rango de

movimiento, y la primera regla de procesamiento se puede establecer en un nodo de reenvío que está en un rango de distancia fijo, en una topología de red.

Se ha dado anteriormente una descripción de las realizaciones de ejemplo preferidas de la presente invención, pero la invención no se limita a las realizaciones de ejemplo antes mencionados, y se pueden añadir modificaciones, sustituciones y ajustes adicionales dentro de un alcance que no se aparta de un concepto tecnológico fundamental de la presente invención. Por ejemplo, en las respectivas realizaciones de ejemplo descritas anteriormente, se ha dado una descripción en la que se proporcionan el dispositivo 300 de control, el dispositivo 310 de autenticación, el dispositivo 320 de gestión de políticas, la unidad 321 de almacenamiento de políticas de comunicación, y la unidad 322 de almacenamiento de información de recursos, cada uno de manera independiente, pero también es posible utilizar una configuración en la que estos se consolidan según sea apropiado.

Además, en las realizaciones de ejemplo descritas anteriormente, se ha dado una descripción en la que se utiliza una política de comunicación con información sobre si es posible o no el acceso como un componente principal, como en la Figura 6. Sin embargo, también es posible incluir información tal como los atributos de la comunicación, tal como la QoS o similar, los nodos de reenvío que pueden utilizarse en un trayecto, un período de tiempo en el que es posible el acceso, y similares, en la política de comunicación. Utilizando este tipo de política de comunicación para generar la primera regla de procesamiento, es posible ajustar finamente un rango y tiempo en los que se puede hacer una solicitud al dispositivo de control para establecer una regla de procesamiento. Además del tiempo en el que el dispositivo 320 de gestión de políticas da una notificación de la política de comunicación al dispositivo 300 de control, que es directamente después de la autenticación del usuario, el dispositivo 320 de gestión de políticas puede actualizar la política de comunicación según el tiempo, la localización del usuario, o similar, y re-notificar al dispositivo 300 de control. Además, es también posible un modo en el que el contenido de control detallado tal como el tiempo, la localización del usuario, y similares, se incluye en la propia política de comunicación, y el establecimiento, modificación y supresión detallados de la primera y segunda reglas de procesamiento se realizan en el lado del dispositivo 300 de control.

Además, en la realización de ejemplo descrita anteriormente, se ha dado una descripción en la que se da un ID de rol a un usuario, como se muestra en la Figura 3 hasta la Figura 6, para realizar el control de acceso. Sin embargo, también es posible realizar el control de acceso utilizando un ID de usuario dado a cada usuario, un ID de acceso tal como una dirección de MAC, la información de localización del terminal 100 de usuario y similares.

Además, en las realizaciones de ejemplo descritas anteriormente, se ha dado una descripción en la que el dispositivo 300 de control genera y establece la segunda regla de procesamiento con respecto a un paquete para el que se recibe una solicitud para establecer una regla de procesamiento, basándose en la primera regla de procesamiento. Sin embargo, también es posible para el dispositivo 300 de control, con la recepción de una solicitud de establecimiento de una regla de procesamiento como un disparador, referirse a la política de comunicación y calcular un trayecto a todos los destinos de acceso permitidos para un usuario, y establecer las reglas de procesamiento que realizan estos trayectos por adelantado. Al hacerlo, es posible restringir aún más la frecuencia de aparición de solicitudes para establecer una regla de procesamiento.

Además, en la realización de ejemplo descrita anteriormente, se ha dado una descripción en la que el terminal 100 de usuario lleva a cabo un protocolo de autenticación con el dispositivo 310 de autenticación a través del nodo 201 de reenvío. Sin embargo, también es posible utilizar una configuración en la que el terminal 100 de usuario se comunica directamente con el dispositivo 310 de autenticación, e implementa el protocolo de autenticación.

El alcance de la invención está definido por las reivindicaciones adjuntas.

[Listado de signos de referencia]

11	unidad de comunicación del nodo
12	unidad de procesamiento de mensajes de control
13	unidad de gestión de reglas de procesamiento
14	unidad de almacenamiento de reglas de procesamiento
15	unidad de gestión del nodo de reenvío
16	unidad de cálculo de trayecto y acción
17	unidad de gestión de topologías
18	unidad de gestión de la localización del terminal
19	unidad de gestión de políticas de comunicación
20	unidad de almacenamiento de políticas de comunicación
100	terminal de usuario
200A, 200B, 201 a 204	nodos de reenvío (nodos de red)
300	dispositivo de control
301	unidad de autorización de transmisión de la solicitud de establecimiento
302	unidad de control del trayecto
310, 311	dispositivos de autenticación
320	dispositivo de gestión de políticas

321	unidad de almacenamiento de políticas de comunicación
322	unidad de almacenamiento de información de recursos
600, 600A, 600B	recursos de red

REIVINDICACIONES

1. Un sistema de comunicación, que comprende:

un dispositivo (300) de control;
un dispositivo (320) de gestión de políticas que está configurado para gestionar la información de la política de comunicación y para notificar, basándose en la información de la política de comunicación, al dispositivo (300) de control de una política de comunicación que corresponde a un usuario para el que la autenticación ha tenido éxito; y
un nodo (200) de reenvío que está configurado para procesar, de acuerdo con las reglas de procesamiento de paquetes establecidas por el dispositivo (300) de control, los paquetes transmitidos desde un terminal (100) de usuario,
en donde el nodo (200) de reenvío se configura para recibir un paquete transmitido desde un terminal (100) de usuario en donde la autenticación para el usuario ha tenido éxito, y en donde el dispositivo (300) de control comprende además:

una unidad (301) de autorización de transmisión de la solicitud de establecimiento que, basándose en una notificación del dispositivo (320) de gestión de políticas de una política de comunicación correspondiente al usuario para el que la autenticación ha tenido éxito, se configura para establecer en el nodo (200) de reenvío que recibió el paquete del terminal (100) de usuario, una primera regla de procesamiento que causa que el nodo (200) de reenvío haga una solicitud de establecimiento de una regla de procesamiento de paquetes con respecto al paquete transmitido desde el terminal (100) de usuario; y
una unidad (302) de control del trayecto que, en un caso de recibir la solicitud de establecimiento desde el nodo (200) de reenvío para el que se establece la primera regla de procesamiento, se configura para determinar un trayecto desde el terminal (100) de usuario a un destino de acceso de acuerdo con dicha política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito, y para establecer en el nodo (200) de reenvío una segunda regla de procesamiento que corresponde al trayecto, estando situado el nodo de reenvío a lo largo del trayecto determinado.

2. El sistema de comunicación según la reivindicación 1, en donde:

la política de comunicación incluye una política de generar, para la primera regla de procesamiento, una regla de coincidencia que identifica un paquete para el que se permite una solicitud de establecimiento de una regla de procesamiento de paquetes; y
la unidad (301) de autorización de transmisión de la solicitud de establecimiento se refiere a la política de comunicación, y, en un caso de recibir un paquete que coincida con la regla de coincidencia del terminal (100) de usuario, establece una primera regla de procesamiento que origina una solicitud de establecimiento de una regla de procesamiento de paquetes al dispositivo (300) de control.

3. El sistema de comunicación según la reivindicación 1 ó 2, en donde:

la política de comunicación incluye la información de un recurso que es accesible por el usuario, o de un recurso que es inaccesible por el usuario; y
la unidad (302) de control del trayecto establece la segunda regla de procesamiento, en un caso donde un destino de un paquete relacionado con una solicitud de establecimiento de una regla de procesamiento de paquetes recibida del nodo de reenvío es un destino que es accesible por el usuario.

4. El sistema de comunicación según una cualquiera de las reivindicaciones 1 a 3, en donde:

el dispositivo (320) de gestión de políticas notifica además al dispositivo (300) de control que se detecta un usuario, para el que la autenticación ha fallado; y
el dispositivo (300) de control, basándose en la notificación, establece a un nodo de reenvío predeterminado una regla de procesamiento de paquetes que previene el reenvío de un paquete desde el usuario a un dispositivo de autenticación predeterminado.

5. El sistema de comunicación según una cualquiera de las reivindicaciones 1 a 4, en donde
se da un notificación al dispositivo (300) de control sobre si está completo o no un procedimiento de autenticación del usuario contra todos los dispositivos de autenticación predeterminados, y
el dispositivo (300) de control, en un caso donde una política de comunicación recibida del dispositivo (320) de gestión de políticas indica que no está completo un procedimiento de autenticación del usuario contra todos los dispositivos de autenticación predeterminados, establece a un nodo de reenvío predeterminado una regla de procesamiento de paquetes que causa que el nodo de reenvío predeterminado inicie un procedimiento de autenticación del usuario entre el usuario y un dispositivo de autenticación predeterminado.

6. El sistema de comunicación según una cualquiera de las reivindicaciones 1 a 5, en donde:

la política de comunicación incluye la información para determinar un nodo de reenvío, al que se ha de establecer la primera regla de procesamiento; y
la unidad (301) de autorización de transmisión de la solicitud de establecimiento se refiere a la política de comunicación para establecer la primera regla de procesamiento a una pluralidad de nodos de reenvío.

7. Un dispositivo (300) de control, que está conectado a:

un nodo (200) de reenvío que está configurado para procesar, de acuerdo con las reglas de procesamiento de paquetes establecidas por el dispositivo (300) de control, los paquetes transmitidos desde un terminal (100) de usuario; y
un dispositivo (320) de gestión de políticas que está configurado para gestionar la información de la política de comunicación y para notificar, basándose en la información de la política de comunicación, al dispositivo (300) de control de una política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito;
en donde el nodo (200) de reenvío se configura para recibir un paquete transmitido desde un terminal (100) de usuario en donde la autenticación para el usuario ha tenido éxito; en donde el dispositivo (300) de control comprende:

una unidad (19) de gestión de políticas de comunicación configurada para almacenar, en una unidad (20) de almacenamiento de políticas de comunicación, la información de la política de comunicación recibida del dispositivo (320) de gestión de políticas;
una unidad (301) de autorización de transmisión de la solicitud de establecimiento que, basándose en una notificación del dispositivo (320) de gestión de políticas de una política de comunicación correspondiente al usuario para el que la autenticación ha tenido éxito, se configura para establecer en el nodo (200) de reenvío que recibió el paquete del terminal (100) de usuario, una primera regla de procesamiento que causa que el nodo (200) de reenvío haga una solicitud de establecimiento de una regla de procesamiento de paquetes con respecto al paquete transmitido desde el terminal (100) de usuario; y

una unidad (302) de control del trayecto que, en un caso de recibir la solicitud de establecimiento desde el nodo (200) de reenvío para el que se establece la primera regla de procesamiento, se configura para determinar un trayecto desde el terminal (100) de usuario a un destino de acceso de acuerdo con dicha política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito, y para establecer en el nodo (200) de reenvío una segunda regla de procesamiento que corresponde al trayecto, estando situado el nodo de reenvío a lo largo del trayecto determinado.

8. El dispositivo (300) de control según la reivindicación 7, en donde:

la política de comunicación incluye una política de generar una regla de coincidencia que identifica un paquete, al que se aplica el contenido del procesamiento prescrito en la primera regla de procesamiento; y
la unidad (301) de autorización de transmisión de la solicitud de establecimiento se refiere a la política de comunicación, y, en un caso de recibir un paquete que coincida con la regla de coincidencia del terminal (100) de usuario, establece una primera regla de procesamiento que origina una solicitud de establecimiento de una regla de procesamiento de paquetes al dispositivo (300) de control.

9. El dispositivo (300) de control según la reivindicación 7 u 8, en donde:

la política de comunicación incluye la información de un recurso que es accesible por el usuario, o de un recurso que es inaccesible por el usuario; y
la unidad (302) de control del trayecto establece la segunda regla de procesamiento, en un caso donde un destino de un paquete relacionado con una solicitud de establecimiento de una regla de procesamiento de paquetes recibida del nodo de reenvío es un destino que es accesible por el usuario.

10. El dispositivo (300) de control según una cualquiera de las reivindicaciones 7 a 9, en donde
en un caso donde el dispositivo (300) de control recibe del dispositivo (320) de gestión de políticas una notificación de que se detecta un usuario, para el que la autenticación ha fallado, el dispositivo (300) de control establece a un nodo de reenvío predeterminado una regla de procesamiento de paquetes que previene el reenvío de un paquete desde el usuario a un dispositivo de autenticación predeterminado.

11. El dispositivo (300) de control según una cualquiera de las reivindicaciones 7 a 10, en donde
en un caso donde una política de comunicación recibida del dispositivo (320) de gestión de políticas indica que no está completo un procedimiento de autenticación del usuario contra todos los dispositivos de autenticación predeterminados, el dispositivo (300) de control establece a un nodo de reenvío predeterminado una regla de procesamiento de paquetes que causa que el nodo de reenvío predeterminado inicie un procedimiento de autenticación del usuario entre el usuario y un dispositivo de autenticación predeterminado.

12. El dispositivo (300) de control según una cualquiera de las reivindicaciones 7 a 11, en donde:

la política de comunicación incluye la información para determinar un nodo de reenvío, al que se ha de establecer la primera regla de procesamiento; y
la unidad (301) de autorización de transmisión de la solicitud de establecimiento se refiere a la política de comunicación para establecer la primera regla de procesamiento a una pluralidad de nodos de reenvío.

13. Un método de comunicación realizado por un dispositivo (300) de control conectado a:

un nodo (200) de reenvío que está configurado para procesar, de acuerdo con las reglas de procesamiento de paquetes establecidas por el dispositivo (300) de control, los paquetes transmitidos desde un terminal (100) de usuario; y
un dispositivo (320) de gestión de políticas que está configurado para gestionar la información de la política de comunicación y para notificar, basándose en la información de la política de comunicación, al dispositivo (300) de control de una política de comunicación correspondiente al usuario para el que la autenticación ha tenido éxito; y
en donde el nodo (200) de reenvío se configura para recibir un paquete transmitido desde un terminal (100) de usuario en donde la autenticación para el usuario ha tenido éxito;
en donde el método de comunicación comprende:

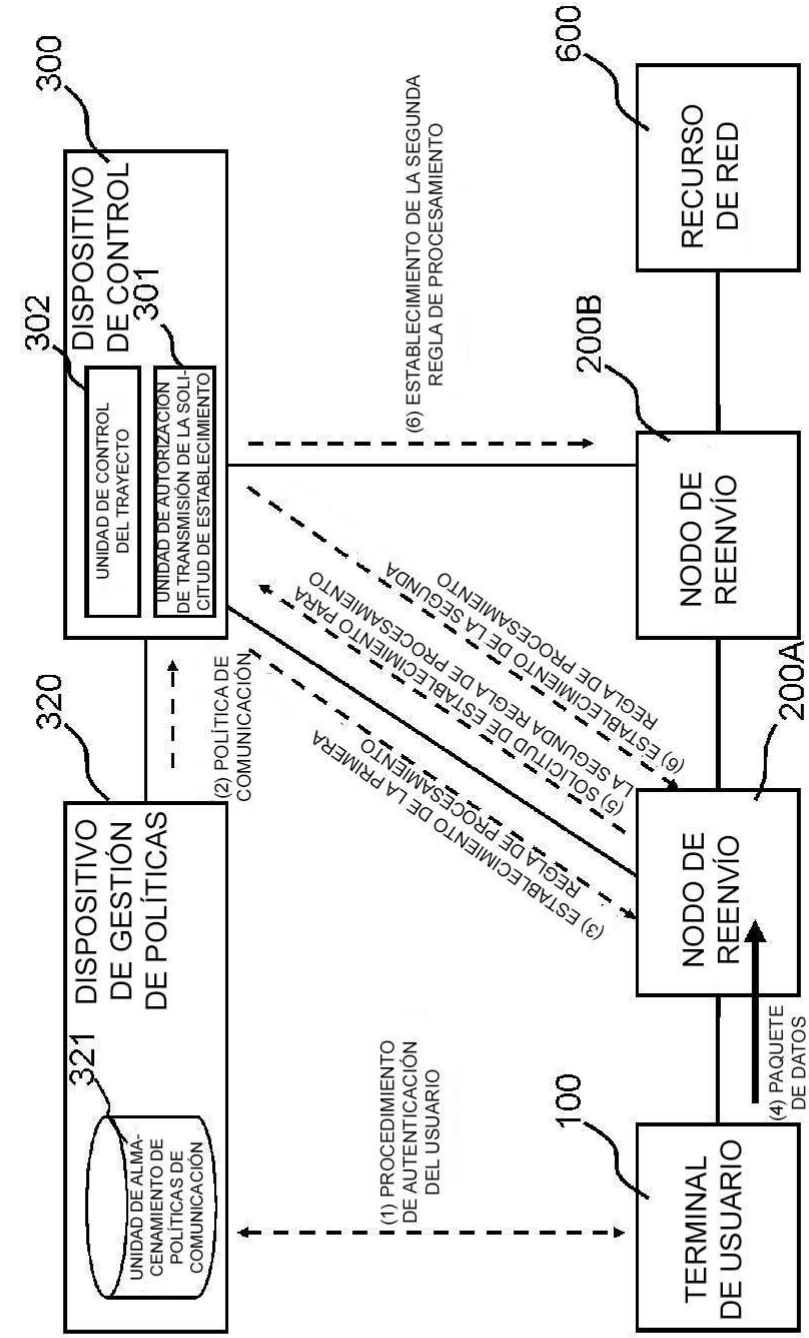
basándose en una notificación del dispositivo (320) de gestión de políticas de una política de comunicación correspondiente al usuario para el que la autenticación ha tenido éxito, establecer en el nodo (200) de reenvío que recibió el paquete del terminal (100) de usuario una primera regla de procesamiento que causa que el nodo (200) de reenvío haga una solicitud de establecimiento de una regla de procesamiento de paquetes con respecto al paquete transmitido desde el terminal (100) de usuario; y
en un caso de recibir una solicitud de establecimiento desde el nodo (200) de reenvío para el que se establece la primera regla de procesamiento, determinar un trayecto desde el terminal (100) de usuario a un destino de acceso de acuerdo con dicha política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito; y
establecer en el nodo (200) de reenvío una segunda regla de procesamiento que corresponde al trayecto, estando situado el nodo de reenvío a lo largo del trayecto determinado.

14. Un programa que cuando se ejecuta en un ordenador incluido en un dispositivo de control causa que el ordenador realice un método; en donde el dispositivo (300) de control está conectado a:

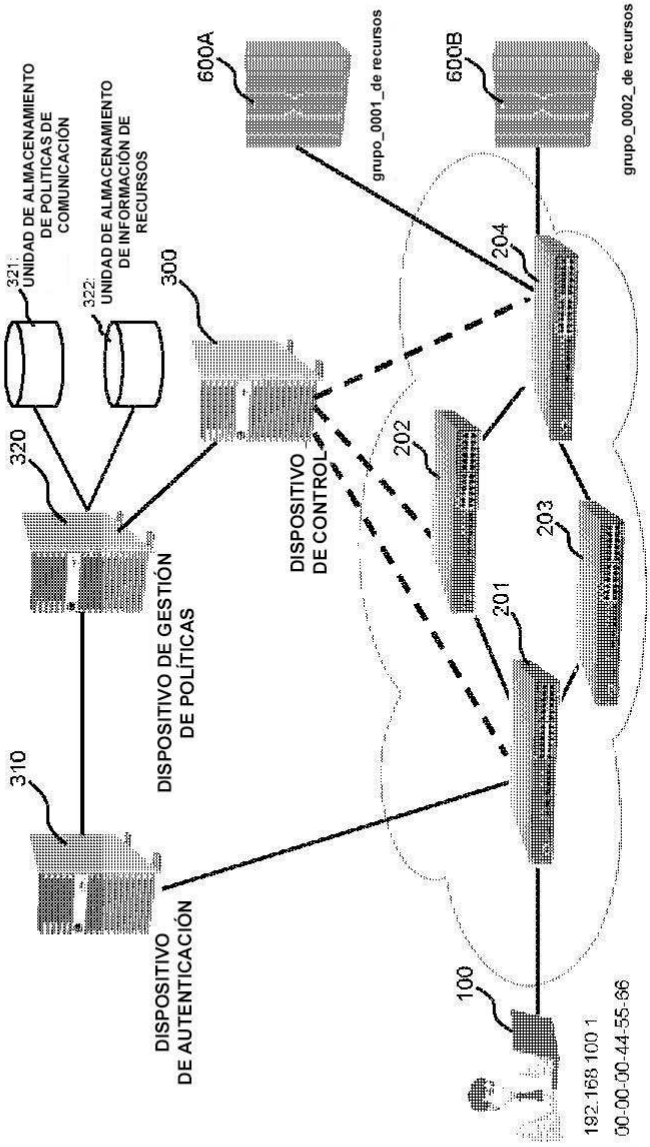
un nodo (200) de reenvío que está configurado para procesar, de acuerdo con las reglas de procesamiento de paquetes establecidas por el dispositivo (300) de control, los paquetes transmitidos desde un terminal (100) de usuario; y
un dispositivo (320) de gestión de políticas que está configurado para gestionar la información de la política de comunicación y para notificar, basándose en la información de la política de comunicación, al dispositivo (300) de control de una política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito; y
en donde el nodo (200) de reenvío se configura para recibir un paquete transmitido desde un terminal (100) de usuario en donde la autenticación para el usuario ha tenido éxito;
en donde el método realizado por el ordenador mediante la ejecución del programa comprende los siguientes pasos:

basándose en una notificación del dispositivo (320) de gestión de políticas de una política de comunicación correspondiente al usuario para el que la autenticación ha tenido éxito, establecer en el nodo (200) de reenvío que recibió el paquete del terminal (100) de usuario una primera regla de procesamiento que causa que el nodo (200) de reenvío haga una solicitud de establecimiento de una regla de procesamiento de paquetes con respecto al paquete transmitido desde el terminal (100) de usuario; y
en un caso de recibir una solicitud de establecimiento desde el nodo (200) de reenvío para el que se establece la primera regla de procesamiento, determinar un trayecto desde el terminal (100) de usuario a un destino de acceso de acuerdo con dicha política de comunicación que corresponde al usuario para el que la autenticación ha tenido éxito; y
establecer en el nodo (200) de reenvío una segunda regla de procesamiento que corresponde al trayecto, estando situado el nodo de reenvío a lo largo del trayecto determinado.

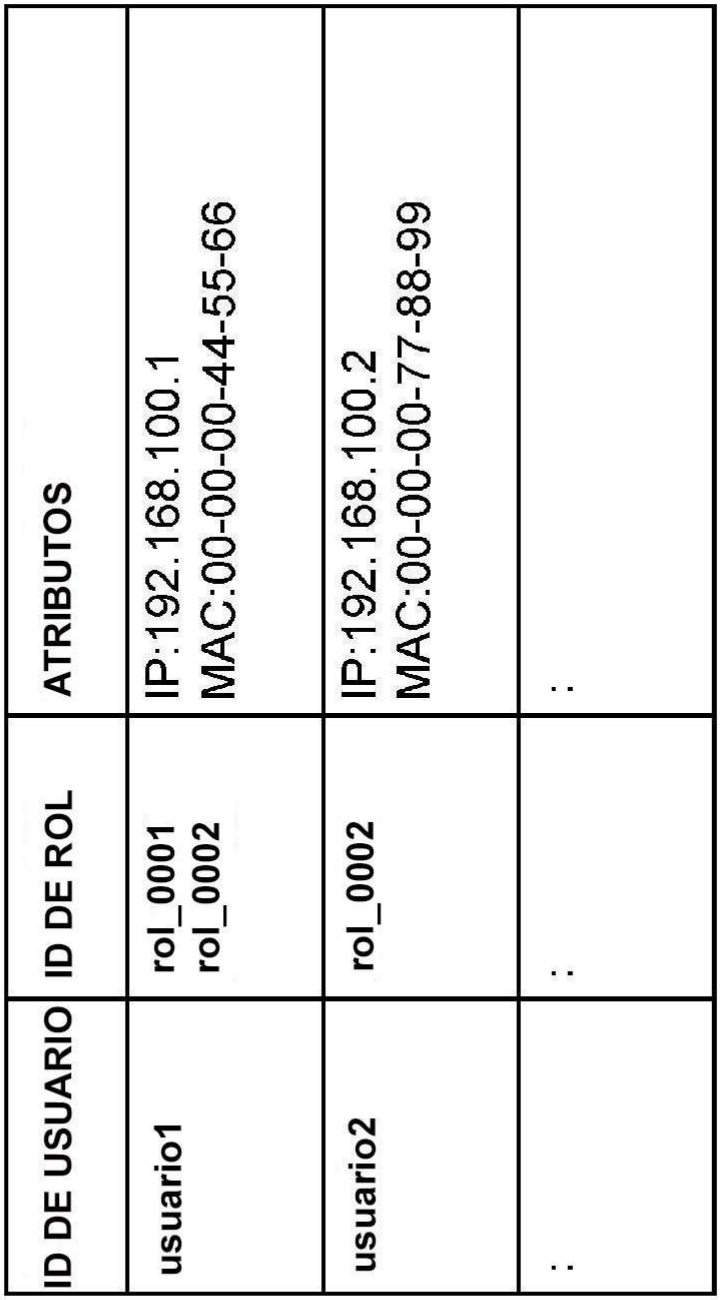
[Fig. 1]


300
DISPOSITIVO DE CONTROL
301
302
UNIDAD DE CONTROL DEL TRAYECTO
UNIDAD DE AUTORIZACIÓN DE TRANSMISIÓN DE LA SOLICITUD DE ESTABLECIMIENTO
600
RECURSO DE RED
200B
NODO DE REENVÍO
200A
NODO DE REENVÍO
320
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
321
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN
100
TERMINAL DE USUARIO
(1) PROCEDIMIENTO DE AUTENTICACIÓN DEL USUARIO
(2) POLÍTICA DE COMUNICACIÓN
(3) ESTABLECIMIENTO DE LA PRIMERA REGLA DE PROCESAMIENTO
(4) PAQUETE DE DATOS
(5) SOLICITUD DE ESTABLECIMIENTO PARA LA SEGUNDA REGLA DE PROCESAMIENTO
(6) ESTABLECIMIENTO DE LA SEGUNDA REGLA DE PROCESAMIENTO

[Fig. 2]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENAMIENTO
DE POLITICAS DE
COMUNICACIÓN
322:
UNIDAD DE ALMACENAMIENTO
DE INFORMACIÓN DE
RECURSOS
300
204
320
DISPOSITIVO
DE CONTROL
202
203
201
DISPOSITIVO DE GESTIÓN
DE POLÍTICAS
310
DISPOSITIVO
DE AUTENTICACIÓN
100
192.168.100.1
00-00-00-44-55-66

[Fig. 3]

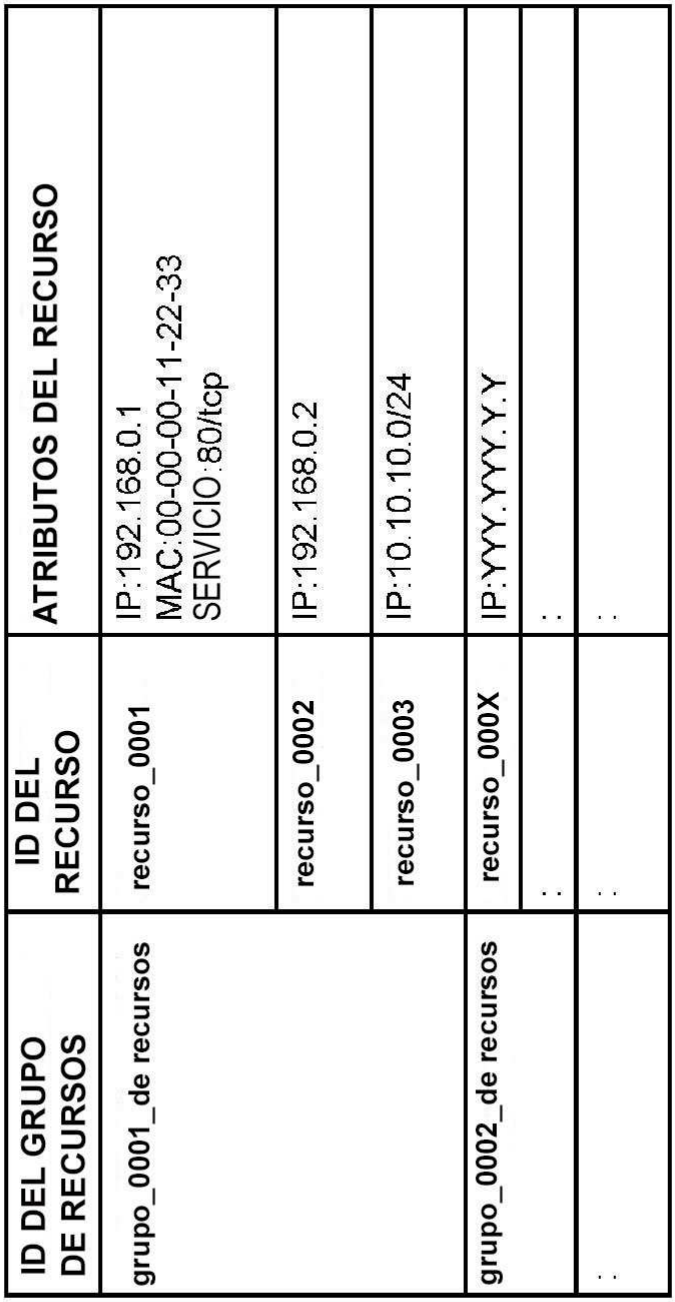


ID DE USUARIO	ID DE ROL	ATRIBUTOS
usuario1	rol_0001 rol_0002	IP:192.168.100.1 MAC:00-00-00-44-55-66
usuario2	rol_0002	IP:192.168.100.2 MAC:00-00-00-77-88-99
..	..	..

[Fig. 4]

ID DE ROL	ID DE GRUPO DE RECURSOS	DERECHOS DE ACCESO
rol_0001	grupo_0001_de recursos	permitido
rol_0001	grupo_0002_de recursos	permitido
rol_0002	grupo_0001_de recursos	denegado
rol_0002	grupo_0002_de recursos	permitido
. .	. .	. .

[Fig. 5]

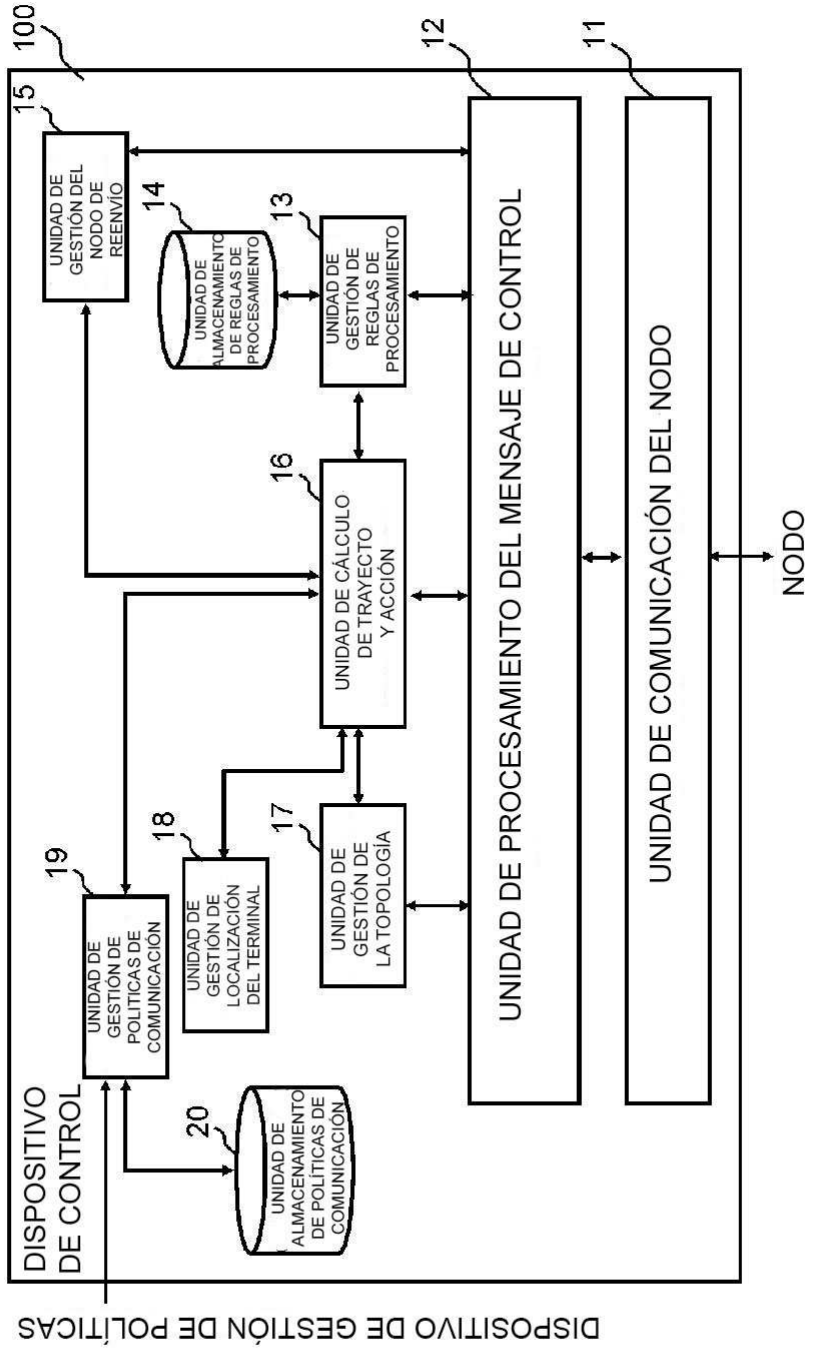


ID DEL GRUPO DE RECURSOS	ID DEL RECURSO	ATRIBUTOS DEL RECURSO
grupo_0001_de recursos	recurso_0001	IP:192.168.0.1 MAC:00-00-00-11-22-33 SERVICIO:80/tcp
	recurso_0002	IP:192.168.0.2
	recurso_0003	IP:10.10.10.0/24
grupo_0002_de recursos	recurso_000X	IP:YYY.YYY.Y.Y
	. .	. .
. .	. .	. .

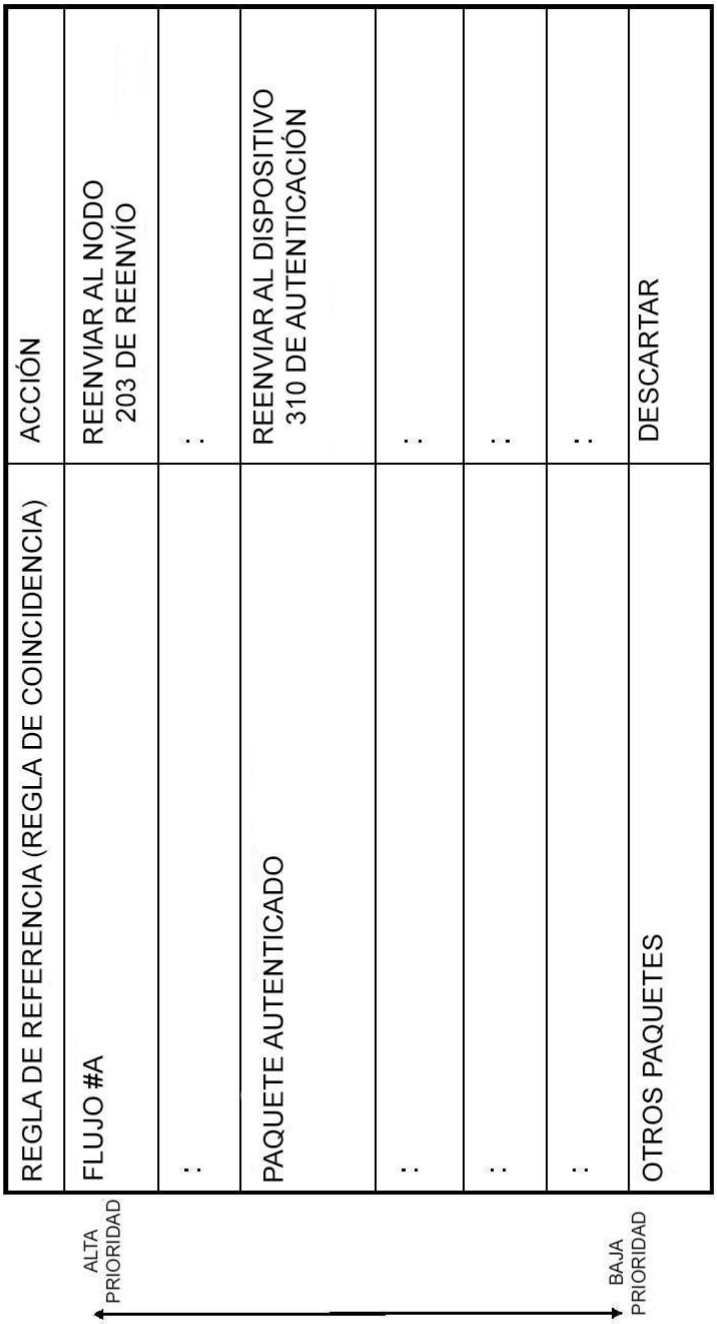
[Fig. 6]

ORIGEN	DESTINO	DERECHOS DE ACCESO	CONDICIONES (OPCIONES)
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	
:	:	:	:

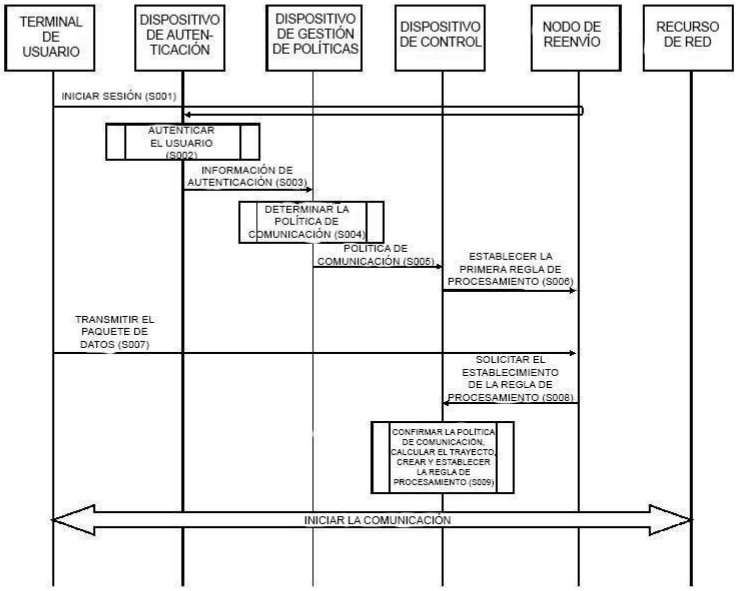
[Fig. 7]


100
12
11
15
UNIDAD DE GESTIÓN DEL NODO DE REENVÍO
14
UNIDAD DE ALMACENAMIENTO DE REGLAS DE PROCESAMIENTO
13
UNIDAD DE GESTIÓN DE REGLAS DE PROCESAMIENTO
16
UNIDAD DE CÁLCULO DE TRAYECTO Y ACCIÓN
UNIDAD DE PROCESAMIENTO DEL MENSAJE DE CONTROL
UNIDAD DE COMUNICACIÓN DEL NODO
NODO
18
17
19
UNIDAD DE GESTIÓN DE LOCALIZACIÓN DEL TERMINAL
UNIDAD DE GESTIÓN DE LA TOPOLOGÍA
UNIDAD DE GESTIÓN DE POLITICAS DE COMUNICACIÓN
DISPOSITIVO DE CONTROL
20
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS

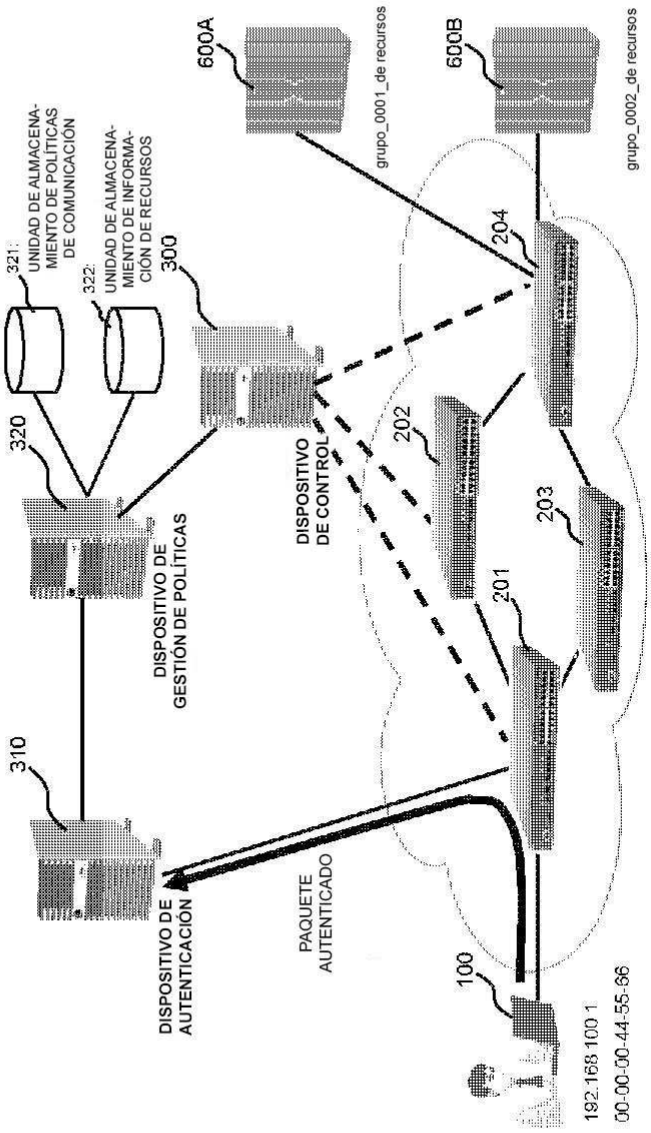
[Fig. 8]


REGLA DE REFERENCIA (REGLA DE COINCIDENCIA)
ACCIÓN
FLUJO #A
REENVIAR AL NODO 203 DE REENVÍO
PAQUETE AUTENTICADO
REENVIAR AL DISPOSITIVO 310 DE AUTENTICACIÓN
OTROS PAQUETES
DESCARTAR
ALTA PRIORIDAD
BAJA PRIORIDAD

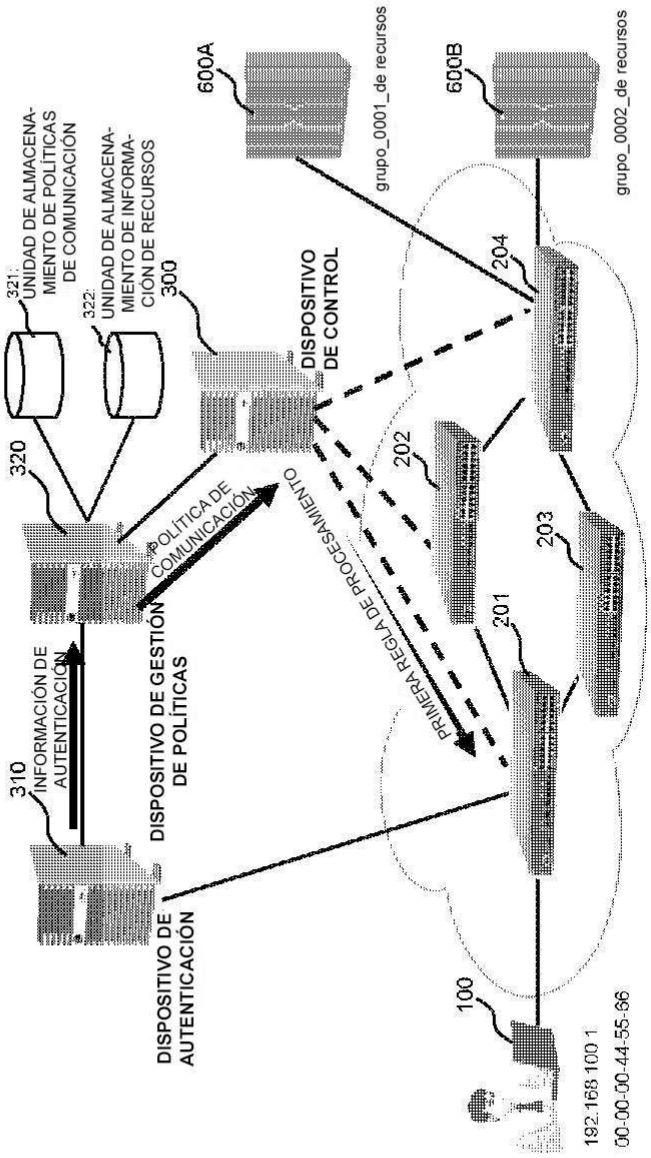
[Fig. 9]


TERMINAL DE USUARIO
DISPOSITIVO DE AUTEN-TICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
NODO DE REENVÍO
RECURSO DE RED
INICIAR SESIÓN (S001)
AUTENTICAR EL USUARIO (S002)
INFORMACIÓN DE AUTENTICACIÓN (S003)
DETERMINAR LA POLÍTICA DE COMUNICACIÓN (S004)
POLÍTICA DE COMUNICACIÓN (S005)
ESTABLECER LA PRIMERA REGLA DE PROCESAMIENTO (S006)
TRANSMITIR EL PAQUETE DE DATOS (S007)
SOLICITAR EL ESTABLECIMIENTO DE LA REGLA DE PROCESAMIENTO (S008)
CONFIRMAR LA POLÍTICA DE COMUNICACIÓN, CALCULAR EL TRAYECTO, CREAR Y ESTABLECER LA REGLA DE PROCESAMIENTO (S009)
INICIAR LA COMUNICACIÓN

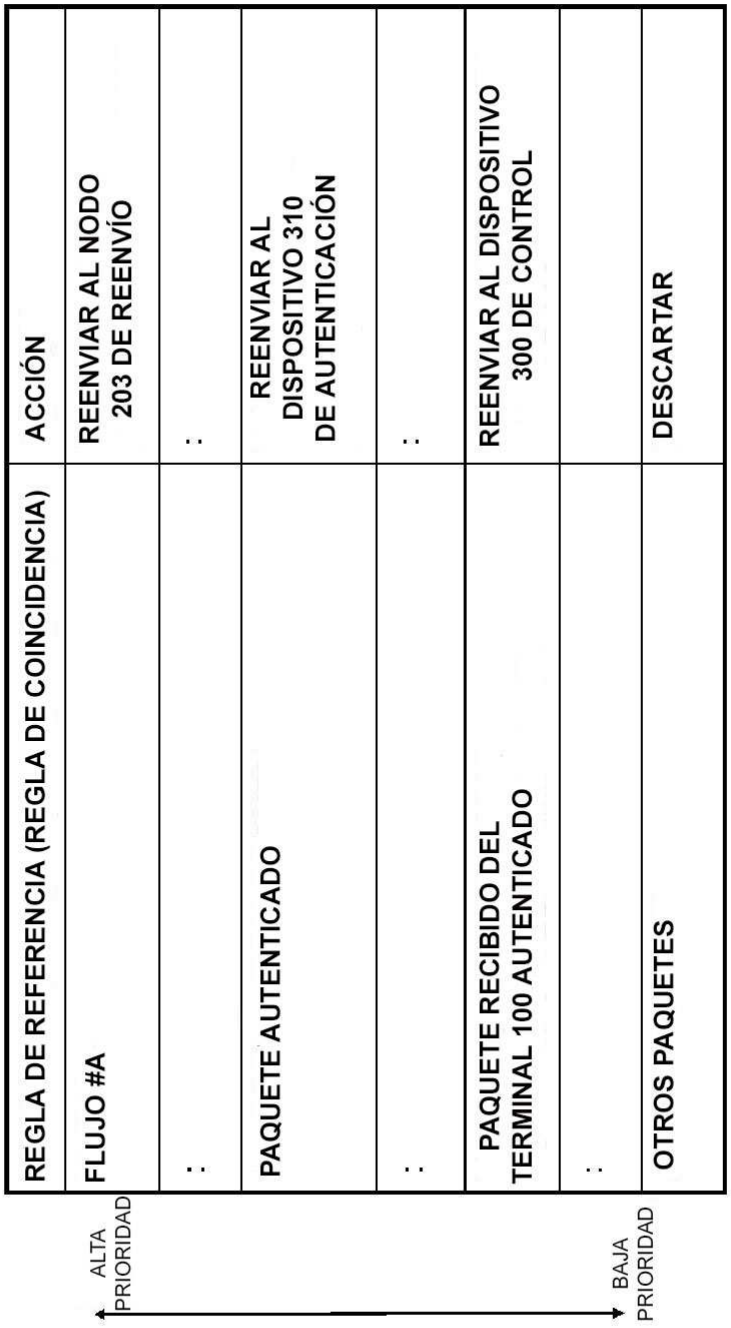
[Fig. 10]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN
322:
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE RECURSOS
300
204
320
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
202
203
201
310
DISPOSITIVO DE AUTENTICACIÓN
PAQUETE AUTENTICADO
100
192.168.100.1
00-00-00-44-55-66

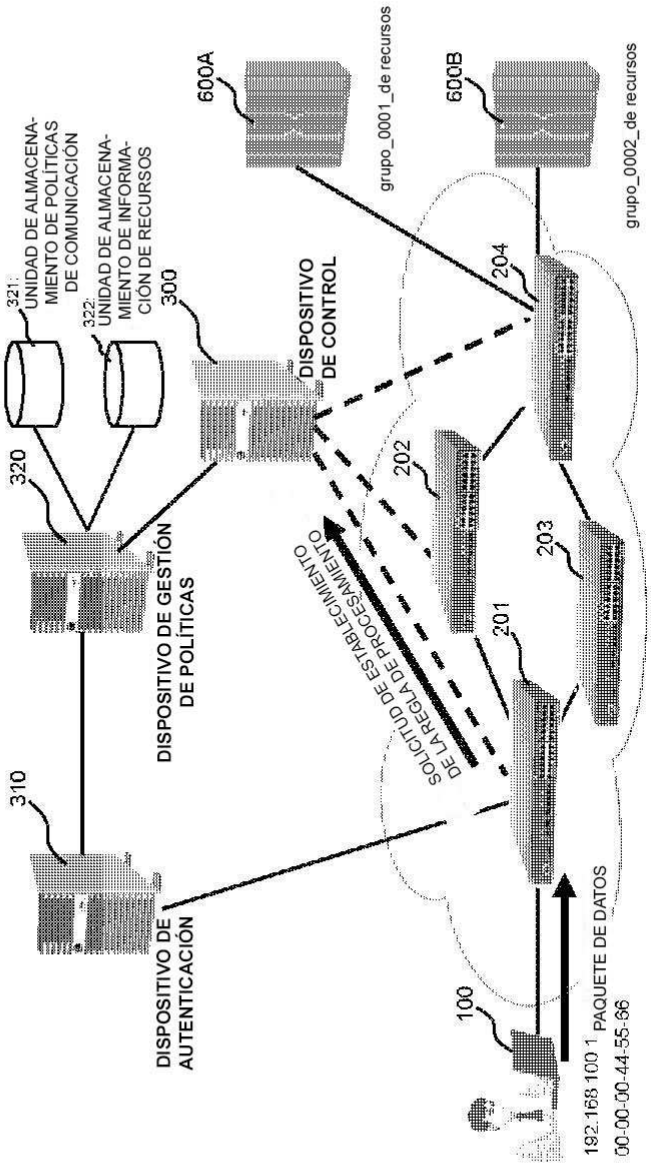
[Fig. 11]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN
322:
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE RECURSOS
300
DISPOSITIVO DE CONTROL
204
202
203
201
320
POLÍTICA DE COMUNICACIÓN
PRIMERA REGLA DE PROCESAMIENTO
310
INFORMACIÓN DE AUTENTICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE AUTENTICACIÓN
100
192.168.100.1
00-00-00-44-55-66

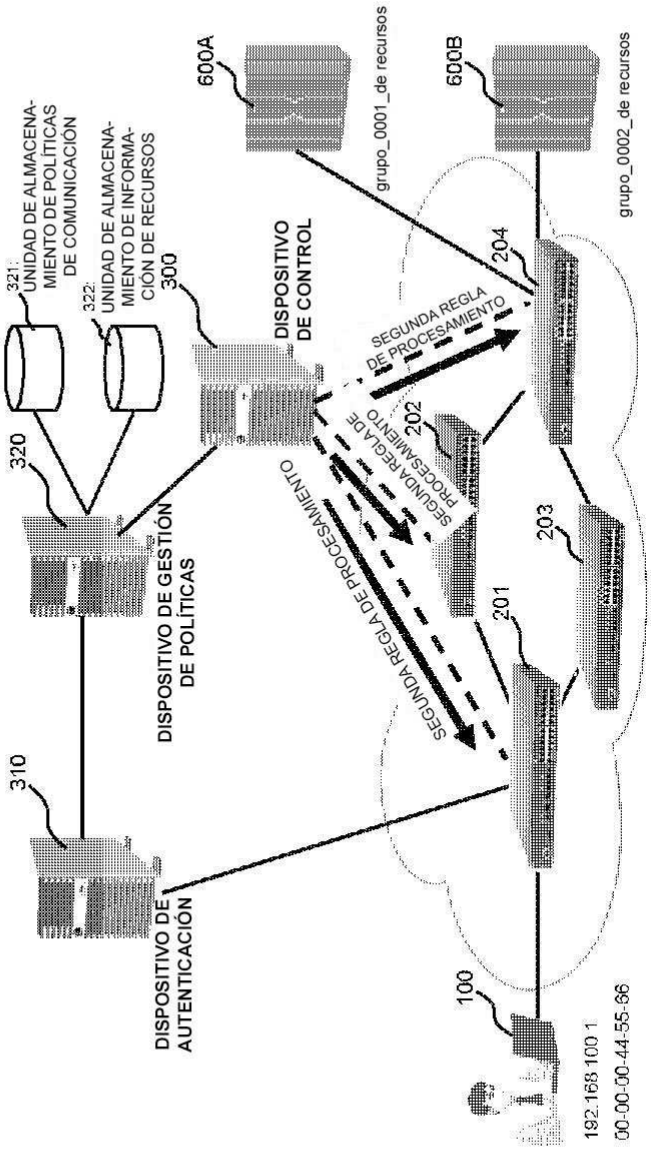
[Fig. 12]


REGLA DE REFERENCIA (REGLA DE COINCIDENCIA)
ACCIÓN
FLUJO #A
REENVIAR AL NODO 203 DE REENVÍO
PAQUETE AUTENTICADO
REENVIAR AL DISPOSITIVO 310 DE AUTENTICACIÓN
PAQUETE RECIBIDO DEL TERMINAL 100 AUTENTICADO
REENVIAR AL DISPOSITIVO 300 DE CONTROL
OTROS PAQUETES
DESCARTAR
ALTA PRIORIDAD
BAJA PRIORIDAD

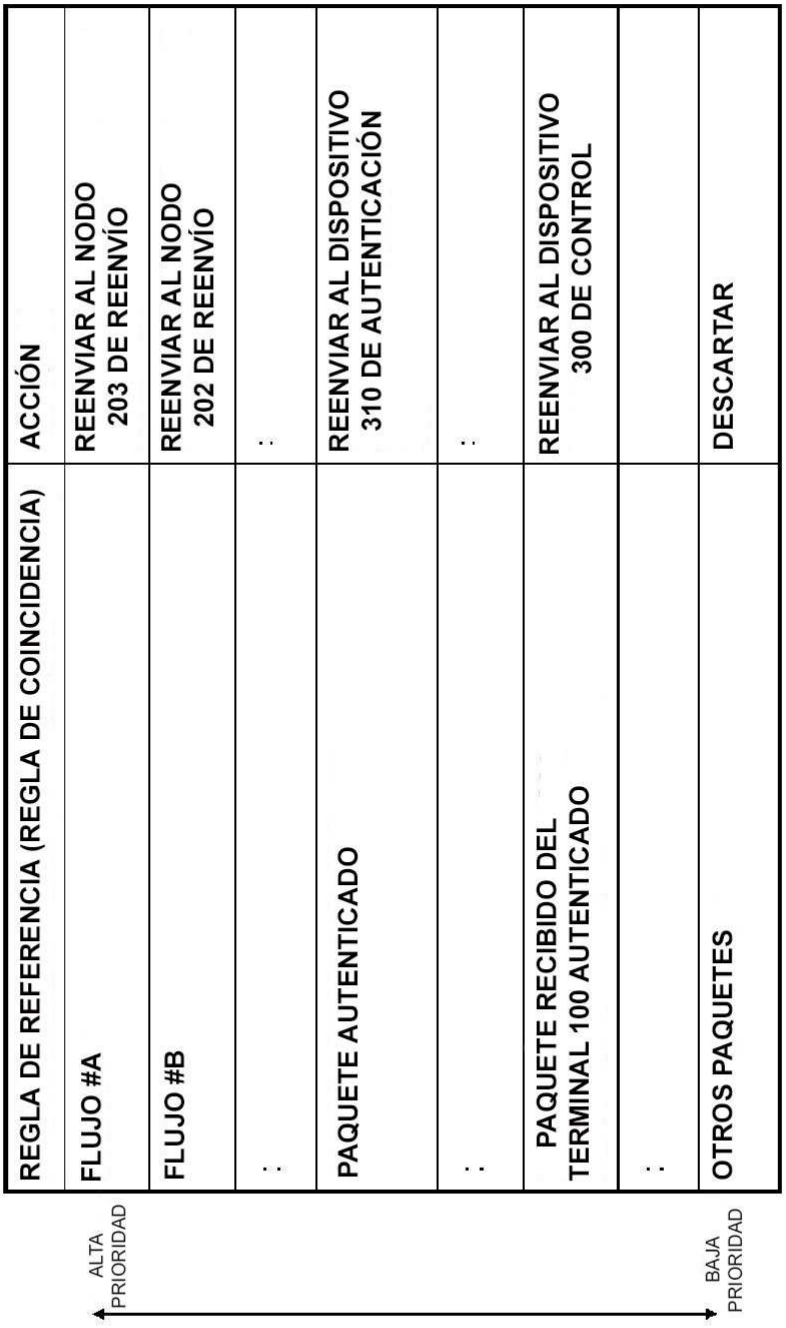
[Fig. 13]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENA-
MIENTO DE POLÍTICAS
DE COMUNICACIÓN
322:
UNIDAD DE ALMACENA-
MIENTO DE INFORMA-
CIÓN DE RECURSOS
300
DISPOSITIVO
DE CONTROL
204
320
202
203
DISPOSITIVO DE GESTIÓN
DE POLÍTICAS
SOLICITUD DE ESTABLECIMIENTO
DE LA REGLA DE PROCESAMIENTO
201
310
DISPOSITIVO DE
AUTENTICACIÓN
100
PAQUETE DE DATOS
192.168.100.1
00-00-00-44-55-66

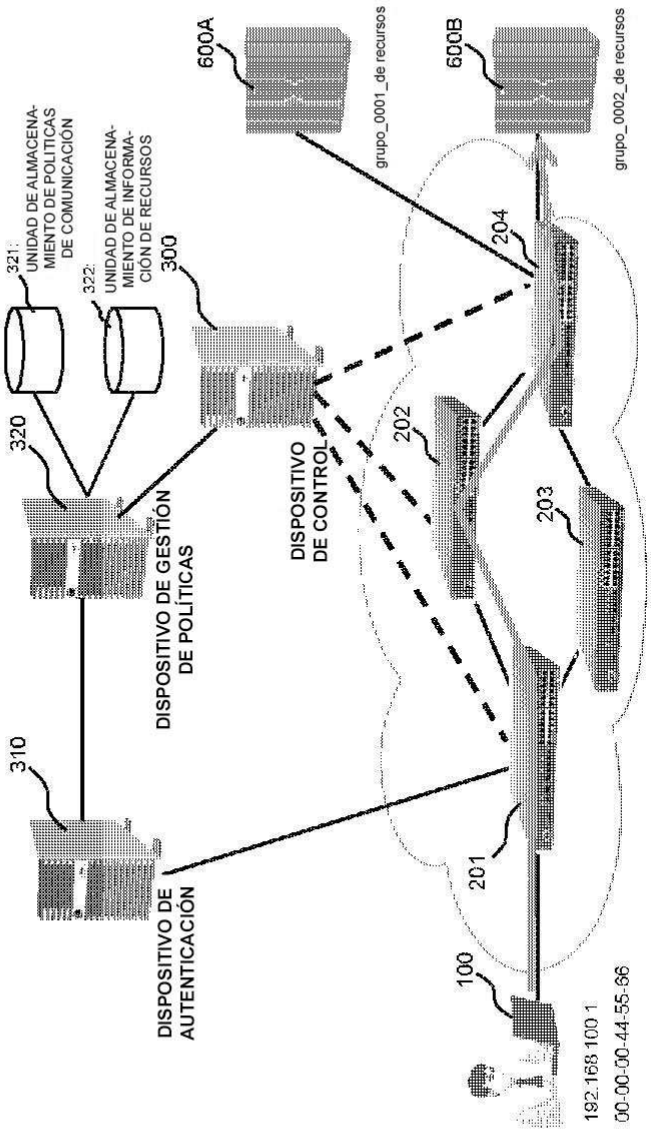
[Fig. 14]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENA-
MIENTO DE POLÍTICAS
DE COMUNICACIÓN
322:
UNIDAD DE ALMACENA-
MIENTO DE INFORMA-
CIÓN DE RECURSOS
300
DISPOSITIVO
DE CONTROL
204
SEGUNDA REGLA
DE PROCESAMIENTO
202
SEGUNDA REGLA DE
PROCESAMIENTO
320
DISPOSITIVO DE GESTIÓN
DE POLÍTICAS
203
201
SEGUNDA REGLA DE PROCESAMIENTO
310
DISPOSITIVO DE
AUTENTICACIÓN
100
192.168.100.1
00-00-00-44-55-66

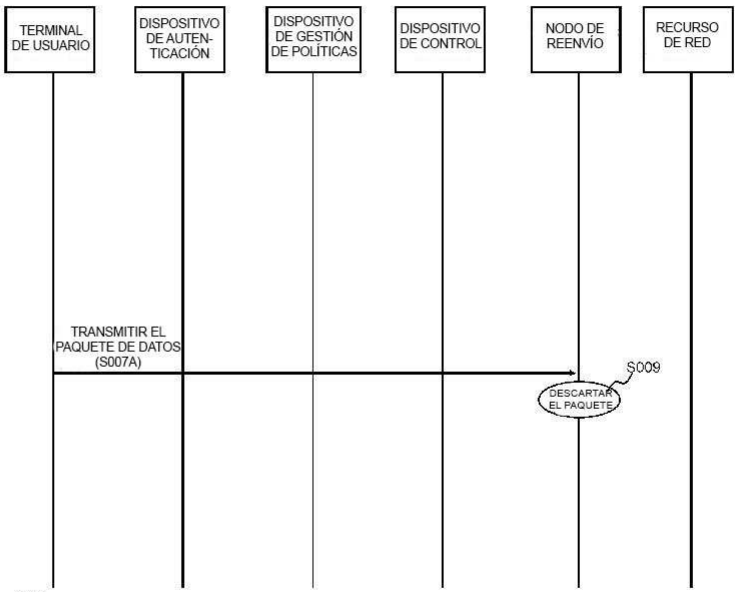
[Fig. 15]


REGLA DE REFERENCIA (REGLA DE COINCIDENCIA)
ACCIÓN
FLUJO #A
REENVIAR AL NODO 203 DE REENVÍO
FLUJO #B
REENVIAR AL NODO 202 DE REENVÍO
. .
. .
PAQUETE AUTENTICADO
REENVIAR AL DISPOSITIVO 310 DE AUTENTICACIÓN
. .
. .
PAQUETE RECIBIDO DEL TERMINAL 100 AUTENTICADO
REENVIAR AL DISPOSITIVO 300 DE CONTROL
. .
OTROS PAQUETES
DESCARTAR
ALTA PRIORIDAD
BAJA PRIORIDAD
34

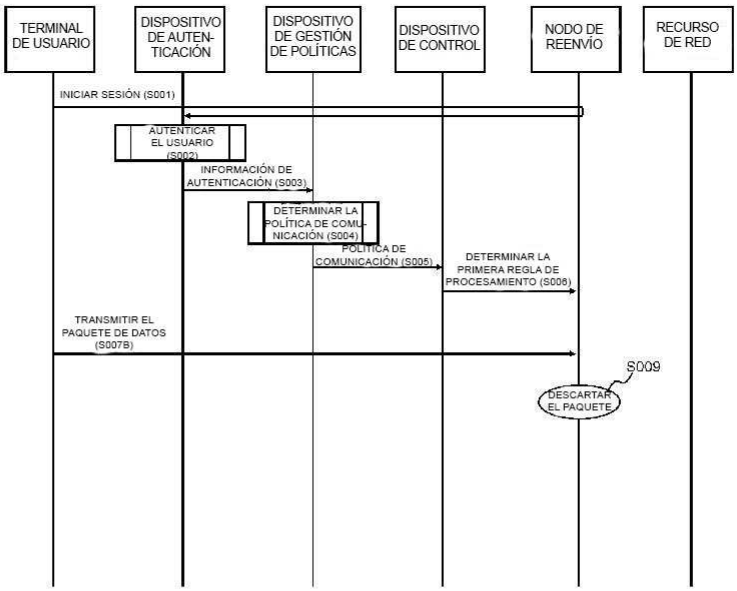
[Fig. 16]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENAMIENTO DE POLITICAS DE COMUNICACIÓN
322:
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE RECURSOS
300
320
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
202
204
203
310
DISPOSITIVO DE AUTENTICACIÓN
201
100
192.168.100.1
00-00-00-44-55-66

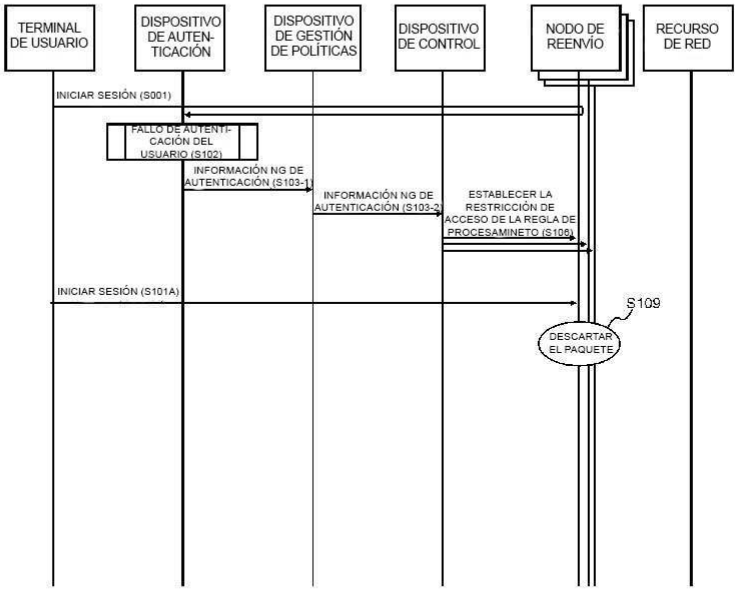
[Fig. 17]


TERMINAL DE USUARIO
DISPOSITIVO DE AUTEN-TICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
NODO DE REENVÍO
RECURSO DE RED
TRANSMITIR EL PAQUETE DE DATOS (S007A)
S009
DESCARTAR EL PAQUETE

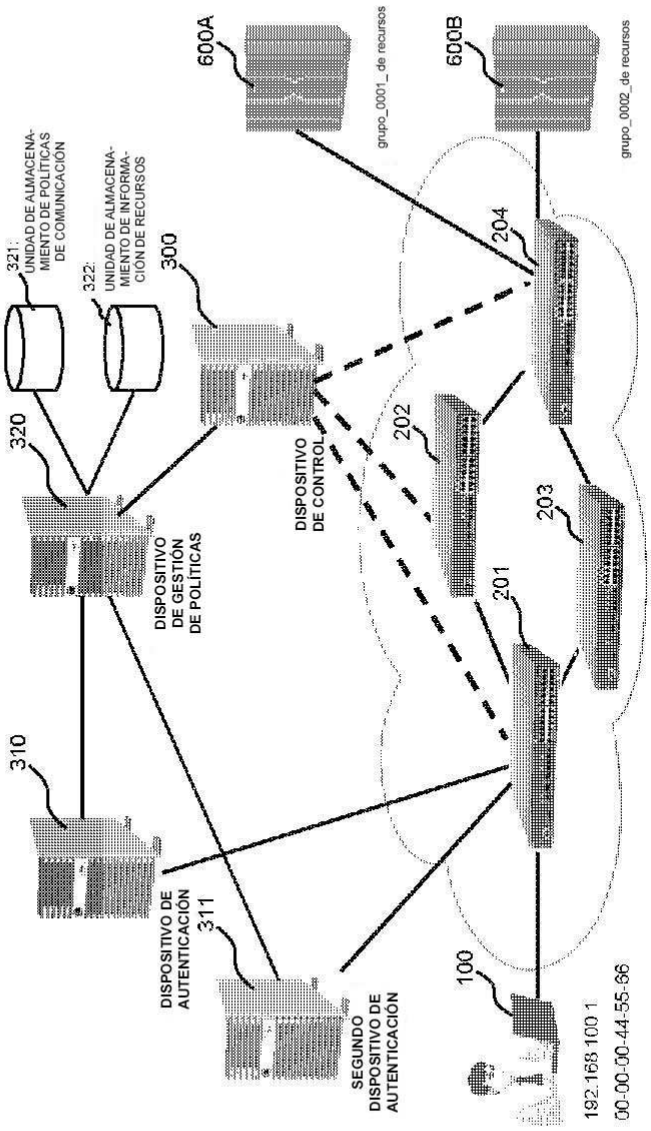
[Fig. 18]


TERMINAL DE USUARIO
DISPOSITIVO DE AUTEN-TICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
NODO DE REENVÍO
RECURSO DE RED
INICIAR SESIÓN (S001)
AUTENTICAR EL USUARIO (S002)
INFORMACIÓN DE AUTENTICACIÓN (S003)
DETERMINAR LA POLÍTICA DE COMU-NICACIÓN (S004)
POLÍTICA DE COMUNICACIÓN (S005)
DETERMINAR LA PRIMERA REGLA DE PROCESAMIENTO (S006)
TRANSMITIR EL PAQUETE DE DATOS (S007B)
S009
DESCARTAR EL PAQUETE

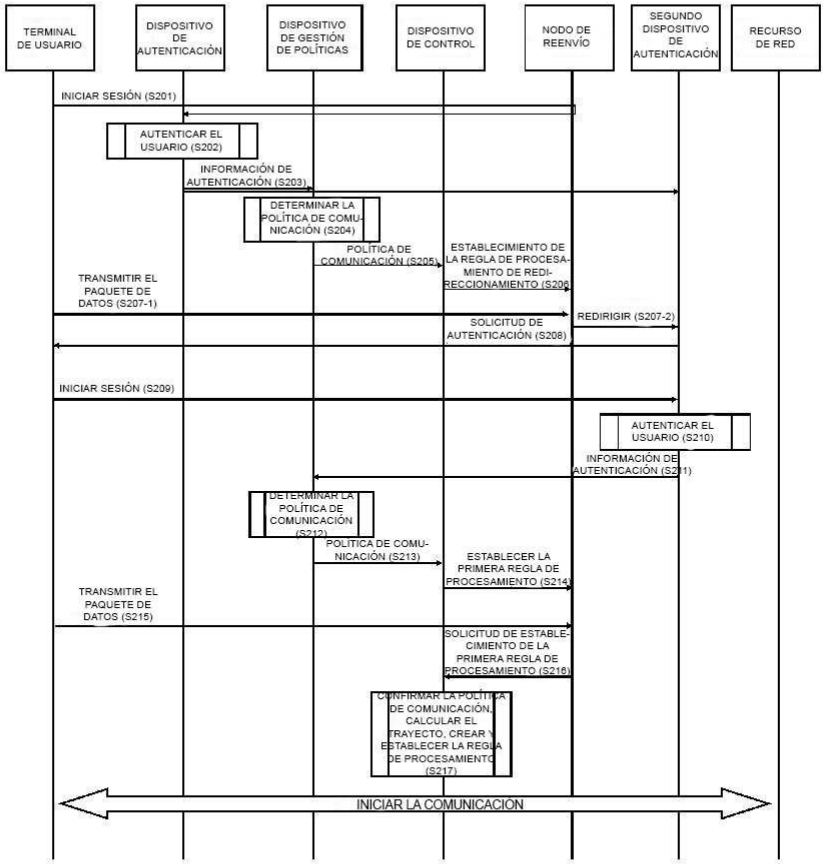
[Fig. 19]


TERMINAL DE USUARIO
DISPOSITIVO DE AUTEN-TICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
NODO DE REENVÍO
RECURSO DE RED
INICIAR SESIÓN (S001)
FALLO DE AUTENTI-CACIÓN DEL USUARIO (S102)
INFORMACIÓN NG DE AUTENTICACIÓN (S103-1)
INFORMACIÓN NG DE AUTENTICACIÓN (S103-2)
ESTABLECER LA RESTRICCIÓN DE ACCESO DE LA REGLA DE PROCESAMINETO (S106)
INICIAR SESIÓN (S101A)
S109
DESCARTAR EL PAQUETE

[Fig. 20]


600A
grupo_0001_de recursos
600B
grupo_0002_de recursos
321:
UNIDAD DE ALMACENAMIENTO DE POLÍTICAS DE COMUNICACIÓN
322:
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE RECURSOS
300
204
320
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
202
203
201
310
DISPOSITIVO DE AUTENTICACIÓN
311
SEGUNDO DISPOSITIVO DE AUTENTICACIÓN
100
192.168.100.1
00-00-00-44-55-66

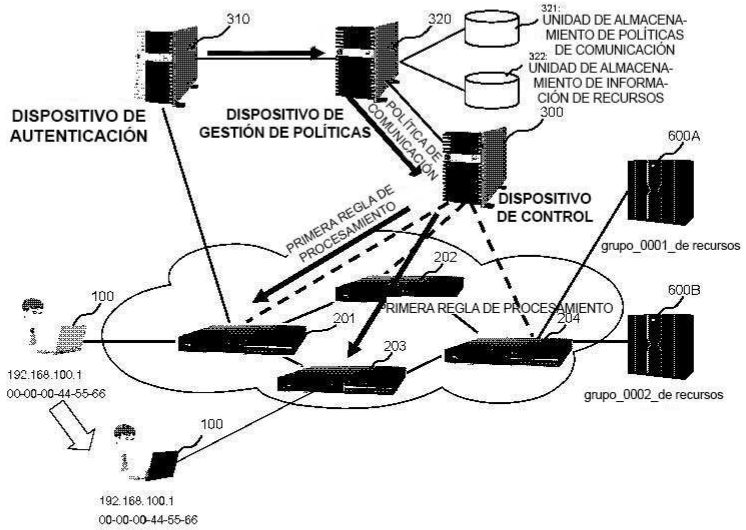
[Fig. 21]


TERMINAL DE USUARIO
DISPOSITIVO DE AUTENTICACIÓN
DISPOSITIVO DE GESTIÓN DE POLÍTICAS
DISPOSITIVO DE CONTROL
NODO DE REENVÍO
SEGUNDO DISPOSITIVO DE AUTENTICACIÓN
RECURSO DE RED
INICIAR SESIÓN (S201)
AUTENTICAR EL USUARIO (S202)
INFORMACIÓN DE AUTENTICACIÓN (S203)
DETERMINAR LA POLÍTICA DE COMUNICACIÓN (S204)
POLÍTICA DE COMUNICACIÓN (S205)
ESTABLECIMIENTO DE LA REGLA DE PROCESAMIENTO DE REDIRECCIONAMIENTO (S206)
TRANSMITIR EL PAQUETE DE DATOS (S207-1)
REDIRIGIR (S207-2)
SOLICITUD DE AUTENTICACIÓN (S208)
INICIAR SESIÓN (S209)
AUTENTICAR EL USUARIO (S210)
INFORMACIÓN DE AUTENTICACIÓN (S211)
DETERMINAR LA POLÍTICA DE COMUNICACIÓN (S212)
POLÍTICA DE COMUNICACIÓN (S213)
ESTABLECER LA PRIMERA REGLA DE PROCESAMIENTO (S214)
TRANSMITIR EL PAQUETE DE DATOS (S215)
SOLICITUD DE ESTABLECIMIENTO DE LA PRIMERA REGLA DE PROCESAMIENTO (S216)
CONFIRMAR LA POLÍTICA DE COMUNICACIÓN, CALCULAR EL TRAYECTO, CREAR Y ESTABLECER LA REGLA DE PROCESAMIENTO (S217)
INICIAR LA COMUNICACIÓN

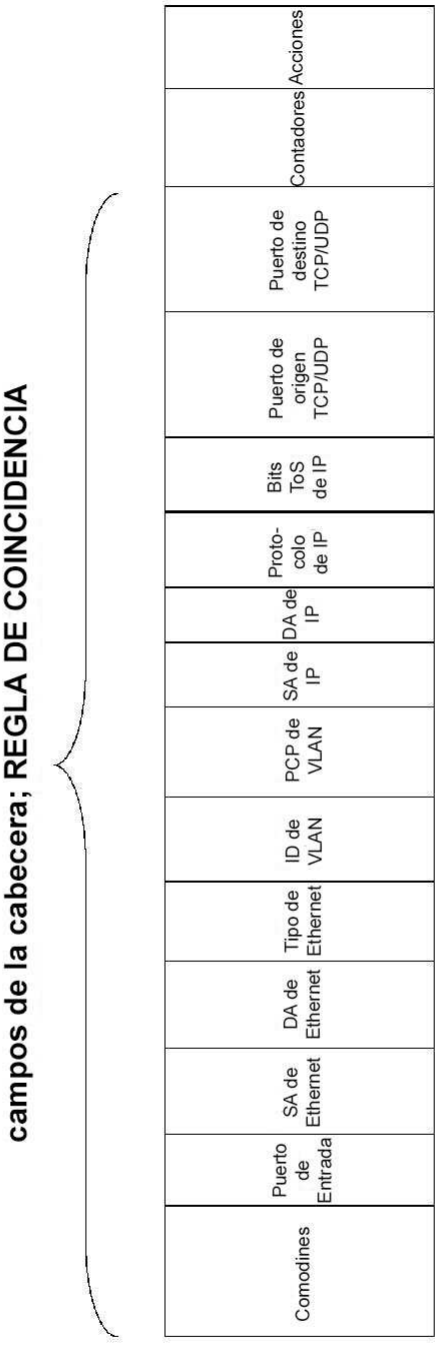
[Fig. 22]

ID DE ROL	ID DE GRUPOS DE RECURSOS	DERECHOS DE ACCESO	LIMITACIÓN DEL RANGO DE MOVIMIENTO
rol_0001	grupo_0001_de recursos	permitido	NODOS DE REENVÍO 201, 203
rol_0001	grupo_0002_de recursos	permitido	NODO DE REENVÍO 201
rol_0002	grupo_0001_ de recursos	denegado	—
rol_0002	grupo_0002_de recursos	permitido	NODO DE REENVÍO 201
:	:	:	:

[Fig. 23]


310
320
321:
UNIDAD DE ALMACENA-
MIENTO DE POLÍTICAS
DE COMUNICACIÓN
322:
UNIDAD DE ALMACENA-
MIENTO DE INFORMA-
CIÓN DE RECURSOS
DISPOSITIVO DE
AUTENTICACIÓN
DISPOSITIVO DE
GESTIÓN DE POLÍTICAS
POLÍTICA DE
COMUNICACIÓN
300
600A
DISPOSITIVO
DE CONTROL
PRIMERA REGLA DE
PROCESAMIENTO
grupo_0001_de recursos
202
100
PRIMERA REGLA DE PROCESAMIENTO
600B
201
204
203
192.168.100.1
00-00-00-44-55-66
grupo_0002_de recursos
100
192.168.100.1
00-00-00-44-55-66

[Fig. 24]


campos de la cabecera; REGLA DE COINCIDENCIA
Comodines
Puerto de Entrada
SA de Ethernet
DA de Ethernet
Tipo de Ethernet
ID de VLAN
PCP de VLAN
SA de IP
DA de IP
Proto-colo de IP
Bits ToS de IP
Puerto de origen TCP/UDP
Puerto de destino TCP/UDP
Contadores
Acciones