(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 614 853**

(51) Int. CI.:

H04L 12/701 (2013.01)
H04L 12/751 (2013.01)
H04L 12/715 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.05.2009 PCT/CN2009/071660**

(87) Fecha y número de publicación internacional: **03.12.2009 WO2009143739**

(96) Fecha de presentación y número de la solicitud europea: **06.05.2009 E 09753457 (2)**

(97) Fecha y número de publicación de la concesión europea: **23.11.2016 EP 2276206**

(54) Título: **Un método, un dispositivo y un sistema de comunicación para gestionar y solicitar información de mapeado**

(30) Prioridad:

29.05.2008 CN 200810028535

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District , Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LIU, YA y
XU, XIAOHU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Un método, un dispositivo y un sistema de comunicación para gestionar y solicitar información de mapeado

Campo de la invención

La presente invención está relacionada con una tecnología de transmisión de datos en una red de comunicaciones y, en particular, con un método, un dispositivo y un sistema de comunicaciones para gestionar y consultar información de mapeado.

Antecedentes de la invención

Con el amplio despliegue de sistemas de multi-homing (conexión simultánea a múltiples redes) de ingeniería de tráfico (TE), las rutas de Internet están aumentando rápidamente. Esto, por un lado, requiere chips de mayor capacidad para almacenar tablas de encaminamiento de gran tamaño, aumentando de este modo los costes de los routers y, por otro lado, provoca una convergencia de rutas más lenta.

Con el fin de resolver el problema de tablas de encaminamiento de gran tamaño provocado por el aumento brusco de las rutas, tal como se muestra en la FIG. 1, Internet se divide en dos partes: una red de tránsito que se encuentra en una posición central de la red y una red perimetral que conecta con la red de tránsito a través de un router frontera (BR). El BR conoce la información de encaminamiento de la red perimetral y la información de encaminamiento de la red de tránsito con las que se conecta, pero la información de encaminamiento no penetra en cada una.

Los prefijos de encaminamiento dentro de la red perimetral no se difunden a la red de tránsito. En su lugar, el BR de la red perimetral registra los prefijos de la red perimetral con un agente de registro (RA) de la red de tránsito. El mapeado entre un prefijo y el BR que registra el prefijo se describe como información de mapeado. Cada RA mantiene una base de datos que almacena información de mapeado, esto es una base de datos de información de mapeado. Múltiples RA en la red de tránsito sincronizan la información de sus bases de datos de información de mapeado a través de un protocolo de comunicaciones como, por ejemplo, una extensión del Border Gateway Protocol (Protocolo de Pasarela Frontera) (BGP), de modo que se sincronizan las bases de datos y mantienen los mismos registros de información de mapeado. Después de la sincronización, cualquier RA en la red de tránsito conoce qué BR atraviesa una ruta desde el RA a un prefijo. En la FIG. 1, por ejemplo, el tráfico desde la red perimetral A hacia la red perimetral B se encaminará en primer lugar a BR-A que conecta con la red perimetral A. A continuación, BR-A consulta al RA la información de mapeado del prefijo más largo que coincide con la dirección del Protocolo de Internet (IP) de destino con el fin de obtener la información del BR que registra la información de mapeado, esto es, BR-B. A continuación, BR-A le reenvía los paquetes a BR-B a través de un túnel dirigido a BR-B como, por ejemplo, un túnel de Multi-Protocol Label Switching (Conmutación mediante Etiquetas Multiprotocolo) (MPLS), un túnel IP en IP, o un túnel de Generic Route Encapsulation (Encapsulación Genérica de Rutas) (GRE). BR-B conoce la información de rutas dentro de la red perimetral con la que se encuentra conectado y reenvía los paquetes en función de su tabla de encaminamiento en la red perimetral B hasta que los paquetes finalmente alcanzan el destino. Esta solución de reenvío es una solución de separación de reenvío y consulta. Esto es, el RA únicamente responde a la consulta de información de mapeado y el RA no reenvía el tráfico entre redes perimetrales.

Sin embargo, en la solución de separación descrita anteriormente se hacen evidentes algunos problemas potenciales de seguridad:

Seguridad del registro de la información de mapeado: un atacante puede registrar información de mapeado falsa en el RA utilizando una identidad falsa, por ejemplo, registrando un prefijo que pertenece a alguien más.

Seguridad de la consulta de información de mapeado: el atacante puede simular un RA para proporcionar información de mapeado falsa a una entidad que realice una consulta o, con algún propósito, alterar la información en algunas parejas de información de mapeado como, por ejemplo, la longitud del prefijo y la dirección de entrada, cambiando la entrada de la red perimetral B desde BR-B a BR-B' en el escenario que se muestra en la FIG. 1.

Seguridad de la sincronización de la base de datos de información de mapeado: cuando se sincronizan las bases de datos de información de mapeado de múltiples RA, algunos RA pueden publicar información de mapeado falsa, por ejemplo, publicando un registro de mapeado con una longitud de prefijo alterada o fabricar una pareja de información de mapeado no existente.

El documento 'Zhao M y otros, "The performance impact of BGP security (El impacto del rendimiento de la seguridad del BGP)", IEEE NETWORK, IEEE SERVICE CENTER, NUEVA YORK, NY, EE.UU. vol. 19, núm. 6, páginas 42-48 (1 de noviembre de 2005), XP001512559' describe que el Protocolo de la Pasarela Frontera posee vulnerabilidades de seguridad debido a que los interlocutores pueden proporcionar información falsa. Los

protocolos de seguridad propuestos pueden cubrir dichas vulnerabilidades, pero aumentan de forma significativa los costos de rendimiento, lo cual evita su despliegue en el mundo real. La criptografía de clave pública puede cubrir estas vulnerabilidades. El documento informa de la investigación de los inventores analizando los protocolos de seguridad propuestos recientemente y construyendo entornos de simulación para evaluar sus costes, y diseñando y validando técnicas para reducirlos.

El documento 'CHARLES LYNN JOANNE MIKKELSON KAREN SEO BBN TECHNOLOGIES, "Secure BGP (BGP Seguro) (S-BGP) draft-clynn-s-bgp-protocol-01.txt; draft-clynn-s-bgp-protocol-01.txt", BORRADOR DE TRABAJO DEL ESTÁNDAR DE IETF, IETF TASK FORCE, IETF, Suiza, núm. 1, (1 de junio de 2003), XP015000564' describe que el Protocolo de la Pasarela Frontera (BGP), el cual se utiliza para distribuir información de encaminamiento entre sistemas autónomos (AS), es un componente crítico de la infraestructura de encaminamiento de Internet. Es altamente vulnerable a una variedad de ataques maliciosos tanto en teoría como en la práctica, debido a la ausencia de medios escalables para verificar la autenticidad y legitimidad del tráfico de control BGP. Este documento es una especificación del protocolo para BGP Seguro (S-BGP), una extensión a BGP-4. S-BGP sigue el principio del menor privilegio y utiliza contramedidas que crea un sistema de autenticación y autorización que cubre la mayor parte de los problemas de seguridad asociados a BGP. Con el fin de facilitar su adopción y despliegue, S-BGP se ha diseñado para minimizar la sobrecarga (de procesamiento, ancho de banda y almacenamiento) añadida por sus contramedidas y para poder interoperar con el BGP actual con el fin de poderse desplegar de forma incremental.

Resumen de la invención

El objeto de la presente invención es proporcionar un método para gestionar información de mapeado en el encaminamiento de red, un método para consultar información de mapeado, y un dispositivo de red perimetral, con el fin de garantizar la seguridad de la información de mapeado en las operaciones de registro, consulta y sincronización.

De acuerdo con el primer aspecto de la presente invención, un método para gestionar información de mapeado en encaminamiento de red incluye:

firmar, por parte de un dispositivo de una red perimetral, un par de información de mapeado utilizando una clave privada de un certificado correspondiente a un prefijo de la red perimetral en el par de información de mapeado con el fin de generar un par de mapeado firmado;

enviarle, por parte del dispositivo de la red perimetral, el par de mapeado firmado a un RA en una red de tránsito; y

compartir, por parte del RA, el par de mapeado firmado con otros RA mediante sincronización de datos; en donde el par de información de mapeado comprende al menos la siguiente información: el prefijo, una dirección del Protocolo de Internet (IP) del dispositivo, en donde la dirección IP se encuentra en la red de tránsito, y una información de control de mapeado; y

el par de mapeado firmado comprende al menos la siguiente información: el prefijo, la dirección IP, la información de control de mapeado, información de control de firma, y una firma, en donde:

la información de control de firma comprende: información del certificado utilizado para la firma, punto de revocación del par de mapeado firmado, fecha de expiración e información del algoritmo de firma.

De acuerdo con el segundo aspecto de la presente invención un método para consultar información de mapeado incluye:

consultarle, por parte de una organización de una primera red perimetral, a un RA en función de un prefijo de una segunda red perimetral y obtener un par de mapeado firmado de una organización de la segunda red perimetral devuelto por el RA;

comprobar, por parte de la organización de una primera red perimetral, si el par de mapeado firmado es válido en función de la información de control de firma en el par de mapeado firmado; y

después de haber determinado mediante la comprobación que el par de mapeado firmado es válido, extraer, por parte de la primera organización de la red perimetral, información de mapeado en el par de mapeado firmado;

en donde la información de mapeado comprende un mapeado entre el prefijo de la segunda red perimetral y una dirección del Protocolo de Internet, IP, de un dispositivo de la segunda red perimetral que registra el prefijo, en donde la dirección IP se encuentra en una red de tránsito; y

en donde el par de mapeado firmado comprende al menos la siguiente información: el prefijo, la dirección IP, la información de control de mapeado, información de control de firma, y una firma, en donde:

la información de control de firma comprende: información del certificado utilizado para la firma, punto de revocación del par de mapeado firmado, fecha de expiración e información del algoritmo de firma.

De acuerdo con el tercer aspecto de la presente invención un dispositivo de una red perimetral incluye:

una unidad de generación del par de mapeado firmado, configurada para firmar un par de información de mapeado utilizando una clave privada de un certificado correspondiente a un prefijo de la red perimetral en el par de información de mapeado con el fin de generar un par de mapeado firmado; y

una unidad de envío, configurada para enviarle el par de mapeado firmado a un RA en una red de tránsito; en donde el par de información de mapeado comprende al menos la siguiente información: el prefijo, una dirección del Protocolo de Internet (IP) del dispositivo, en donde la dirección IP se encuentra en la red de tránsito, y una información de control de mapeado; y

el par de mapeado firmado comprende al menos la siguiente información: el prefijo, la dirección IP, la información de control de mapeado, información de control de firma, y una firma, en donde:

la información de control de firma comprende: información del certificado utilizado para la firma, punto de revocación del par de mapeado firmado, fecha de expiración e información del algoritmo de firma.

Con el método de gestión de mapeado de información, el método de consulta de información de mapeado, los dispositivos y el sistema de comunicaciones proporcionados por la presente invención, con la clave privada de un certificado se firma un par de información de mapeado, lo cual asegura la fiabilidad de la información de mapeado en las operaciones de registro, consulta y sincronización y elimina los problemas de seguridad potenciales de la técnica anterior. En consecuencia, se mejora la fiabilidad de la red o el sistema de comunicaciones.

Breve descripción de los dibujos

La FIG. 1 ilustra una arquitectura de Internet en la técnica anterior;

la FIG. 2 es un diagrama de flujo principal de un método para gestionar información de mapeado de acuerdo con un modo de realización de la presente invención;

la FIG. 3 ilustra un prefijo y una asignación de certificado de acuerdo con un modo de realización de la presente invención;

la FIG. 4 ilustra un escenario de aplicación de un modo de realización de la presente invención;

la FIG. 5 ilustra un método para gestionar información de mapeado de acuerdo con un primer modo de realización de la presente invención;

la FIG. 6 ilustra un método para gestionar información de mapeado de acuerdo con un segundo modo de realización de la presente invención;

la FIG. 7 es un diagrama de flujo de un método para consultar información de mapeado de acuerdo con un modo de realización de la presente invención;

la FIG. 8 ilustra un método para gestionar información de mapeado de acuerdo con un tercer modo de realización de la presente invención;

la FIG. 9 ilustra un certificado de una Organización A de acuerdo con un modo de realización de la presente invención;

la FIG. 10 ilustra un certificado de una organización de una red de tránsito de acuerdo con un modo de realización de la presente invención;

la FIG. 11 ilustra la estructura de un sistema de comunicaciones de acuerdo con un modo de realización de la presente invención;

la FIG. 12 ilustra un dispositivo de red perimetral de acuerdo con un primer modo de realización de la presente invención;

la FIG. 13 ilustra un dispositivo de red perimetral de acuerdo con un segundo modo de realización de la presente invención;

la FIG. 14 ilustra un dispositivo de red perimetral de acuerdo con un tercer modo de realización de la presente invención;

la FIG. 15 ilustra un dispositivo de red perimetral de acuerdo con un cuarto modo de realización de la presente invención;

la FIG. 16 ilustra un dispositivo RA de acuerdo con un primer modo de realización de la presente invención;

la FIG. 17 ilustra un dispositivo RA de acuerdo con un segundo modo de realización de la presente invención;

la FIG. 18 ilustra un dispositivo RA de acuerdo con un tercer modo de realización de la presente invención; y

la FIG. 19 ilustra un dispositivo RA de acuerdo con un cuarto modo de realización de la presente invención.

Descripción detallada de los modos de realización

Con el fin de explicar mejor la solución técnica de los modos de realización de la presente invención, de aquí en adelante se describe detalladamente, haciendo referencia a los dibujos adjuntos, un método para gestionar información de mapeado en un encaminamiento de red, un método para consultar información de mapeado, un dispositivo de red perimetral, un dispositivo RA y un sistema de comunicaciones proporcionados por los modos de realización de la presente invención.

Antes de explicar la solución técnica, se debe observar que, en la descripción de los modos de realización de la presente invención, una organización de red perimetral y un dispositivo de red perimetral se refieren al mismo objeto; un RA y un dispositivo RA se refieren al mismo objeto; la organización de la primera red perimetral y la Organización A se refieren al mismo objeto y la organización de la segunda red perimetral y la Organización B se refieren al mismo objeto.

La FIG. 2 ilustra un diagrama de flujo de un método para gestionar información de mapeado en encaminamiento de red de acuerdo con un modo de realización de la presente invención. El método incluye los siguientes pasos:

S101. Un dispositivo de red perimetral firma un par de información de mapeado utilizando la clave privada de un certificado correspondiente al prefijo en el par de información de mapeado con el fin de generar un par de mapeado firmado.

El par de información de mapeado incluye al menos la siguiente información: prefijo, dirección IP de la red de tránsito e información de control de mapeado.

El par de mapeado firmado incluye al menos la siguiente información: prefijo, dirección IP de la red de tránsito, información de control de mapeado, información de control de firma y firma. La información de control de firma incluye: información de certificado utilizado para la firma, punto de revocación del par de mapeado firmado, fecha de expiración y algoritmo de firma.

S102. El dispositivo de red perimetral le envía el par de mapeado firmado a un RA en la red de tránsito.

S103. El RA comparte el par de mapeado firmado con otros RA mediante sincronización de datos. En particular, el RA puede crear una base de datos de pares de mapeado firmados independiente con el fin de almacenar el par firmado.

Los RA sincronizan sus bases de datos de pares de mapeado firmados tomando un par de mapeado firmado como la unidad básica de registro y responden a las consultas proporcionando el par de mapeado firmado solicitado. En cada par de mapeado firmado se incluye un tiempo de vida. Se descartarán los pares de mapeado firmados cuyo tiempo de vida haya expirado. El RA no acepta ni distribuye un par de mapeado firmado cuyo tiempo de vida haya expirado. Cuando un solicitante recibe el par de mapeado firmado, el solicitante comprueba la firma sobre el par de mapeado de acuerdo con la información de certificado y la información del algoritmo de firma. El solicitante no llevará a cabo un procesamiento posterior hasta que la comprobación de firma sea satisfactoria.

Los pasos S101 y S102 se pueden implementar del siguiente modo:

a. El dispositivo de red perimetral firma el prefijo y el número de sistema autónomo (AS) de la red de tránsito utilizando la clave privada del certificado correspondiente al prefijo con el fin de generar un primer par de mapeado firmado y envía el primer par de mapeado firmado a la organización de la red de tránsito.

b. La organización de la red de tránsito firma el primer par de mapeado firmado de acuerdo con el certificado que contiene el número de AS con el fin de generar un segundo par de mapeado firmado y le envía el segundo par de mapeado firmado al RA en la red.

El método para gestionar información de mapeado en el enrutamiento de red de acuerdo con el modo de realización de la presente invención se ha descrito más arriba en un sentido general. Aquellos experimentados en

la técnica pueden entender que, firmando un par de información de mapeado utilizando la clave privada de un certificado de acuerdo con el modo de realización de la presente invención, se garantiza la fiabilidad de la información de mapeado en las operaciones de registro, consulta y sincronización y se elimina el problema potencial de la técnica anterior.

A continuación se explica la solución técnica de los modos de realización de la presente invención tomando como ejemplo el certificado de infraestructura de clave pública (PKI). Tal como se muestra en la FIG. 3, la organización superior de gestión de prefijos y AS en el mundo es la Internet Assigned Numbers Authority (Autoridad de Asignación de Números de Internet) (IANA), bajo la cual se configuran cinco agentes regionales de nivel 1. El agente en la región Asia-Pacífico es Asia-Pacific Network Information Center (Centro de Información de Red Asia-Pacífico) (APNIC). Por lo tanto, los operadores en la región Asia-Pacífico como, por ejemplo, China Mobile, China Telecom y China Netcom, y otras organizaciones que requieren prefijos de red y números de AS como, por ejemplo, la red de educación China, pueden enviar solicitudes de direcciones IP y números de AS al APNIC. Un operador también puede funcionar como un agente en el área de cobertura de su red. Por ejemplo, China Netcom puede recibir solicitudes de prefijo de organizaciones en el área de Beijing. La FIG. 3 demuestra la asignación de prefijos de la IANA a una organización final así como la correspondiente ruta de verificación de certificados de recursos con respecto al segmento de red de ejemplo 10.0.0.0/8.

En la FIG. 3, las autoridades certificadoras (CA) incluyen IANA, APNIC, China Netcom y China Telecom, y organizaciones que tienen concedidos certificados de recursos son la red de educación China, una organización de una primera red perimetral (Organización A) y una organización de una segunda red perimetral (Organización B). China Netcom y China Telecom son propietarias de redes de tránsito que operan en la práctica. Requieren prefijos IP y números de AS. Los prefijos y los números de AS de diferentes certificados de recursos son mutuamente excluyentes. Esto es, en la FIG. 3, donde China Netcom ha asignado el prefijo 10.2.1.0/24 a la Organización A, no podrá asignar el prefijo a la Organización B o a propia red de tránsito de China Netcom. Una red de usuario también puede solicitar directamente a la IANA secciones de direcciones IP independientes. Cuando el usuario cambia de red de acceso, la renumeración de direcciones de red internas es innecesaria.

A continuación se explica la solución técnica de los modos de realización de la presente invención bajo la arquitectura de red que se muestra en la FIG. 4 con referencia a los pasos de los métodos que se muestran en la FIG. 5, la FIG. 6, la FIG. 7 y la FIG. 8.

Se supone que se adopta el formato de certificado X.509 v3 de PKI. Tal como se muestra en la FIG. 9, la Organización A obtiene un certificado mediante el modo de distribución de certificados que se muestra en la FIG. 3. Se supone que la Organización A y la Organización B se conectan, respectivamente, a las redes de tránsito de China Netcom y China Telecom. Los prefijos de la Organización A y la Organización B no se distribuirán a las redes de tránsito. El prefijo 10.2.1.0/24 de la Organización A se asociará a la dirección 192.168.1.2 en la red de tránsito y el prefijo 10.3.1.0/24 de la Organización B se asociará a la dirección 192.168.2.2 en la red de tránsito. Tal como se muestra en la FIG. 5, el procedimiento en el que la Organización A y la Organización B registran y sincronizan la información de mapeado incluye:

S200. Ambas organizaciones generan pares de información de mapeado en función de los prefijos y los ID de salida que se corresponden con los prefijos.

El par de información de mapeado de la Organización A es {prefijo=10.2.1.0/24, IP de tránsito=192.168.1.2, información de control de mapeado}; el par de información de mapeado de la Organización B es {prefijo=10.3.1.0/24, IP de tránsito=192.168.2.2, información de control de mapeado}.

S201. La Organización A firma su par de información de mapeado utilizando la clave privada de su certificado de recursos y genera el par de mapeado firmado {prefijo=10.2.1.0/24, IP de tránsito=192.168.1.2, información de control de mapeado, información de control de firma, Firma A}.

De la misma forma, la Organización B genera del mismo modo un par de mapeado firmado {prefijo=10.3.1.0/24, IP de tránsito=192.168.2.2, información de control de mapeado, información de control de firma, Firma B}.

S202. Ambas organizaciones envían los pares de mapeado firmados a los RA apropiados en la red de tránsito.

Preferiblemente, el par de mapeado firmado se envía al RA adyacente. Esto es, el par de mapeado firmado de la Organización A se envía al RA1 adyacente y el par de mapeado firmado de la Organización B se envía al RA2 adyacente.

S203. El RA comparte el par de mapeado firmado con otros RA mediante sincronización de datos. Específicamente, RA1 y RA2 sincronizan sus bases de datos de modo que la base de datos de mapeados firmados de RA1 tiene el par de mapeado firmado de la Organización B y la base de datos de RA2 tiene el par de mapeado firmado de la Organización A.

En la práctica, los pasos S201 a S203 se pueden implementar del siguiente modo. Se toma como ejemplo de ilustración la Organización A. En el caso de la Organización B la implementación es igual. Tal como se muestra en la FIG. 6, la implementación incluye:

S301. La Organización A firma el par de información de mapeado {10.2.1.0/24,100} utilizando la clave privada del certificado correspondiente al prefijo 10.2.1.0/24 en el par de información de mapeado con el fin de generar el par 1 de mapeado firmado {prefijo=10.2.1.0/24, AS#=100, información 1 de control de firma, firma 1}, y envía el par 1 de mapeado firmado a la organización de la red de tránsito (la red de tránsito de China Netcom que se muestra en la FIG. 4).

S302. La red de tránsito de China Network firma el par 1 de mapeado firmado enviado por la Organización A con el certificado de recursos (el formato del cual se muestra en la FIG. 10) que contiene su AS# (100) con el fin de generar un par 2 de mapeado firmado {{prefijo=10.2.1.0/24, AS#=100, información 1 de control de firma, firma 1}, IP de tránsito=192.168.1.2, información de control de mapeado, información 2 de control de firma, firma 2}, y le envía el par 2 de mapeado firmado al RA1.

S303. El RA1 comparte el par 2 de mapeado firmado con otros RA (RA2) mediante sincronización de datos.

La solución técnica que se muestra en la FIG. 6 reduce el acoplamiento de la gestión y mejora la flexibilidad de reasignación de direcciones de encaminamiento de un router frontera en la red de tránsito. Una organización únicamente necesita conocer el AS# de la red de tránsito autorizada. Este AS# no cambia frecuentemente. La dirección de encaminamiento de un router frontera específico en la red de tránsito es completamente decidida por la red de tránsito y se puede reasignar dinámicamente muchas veces. Mientras que el AS# no cambie, no es necesaria una nueva firma de la organización del prefijo.

Consecuentemente, en un modo de realización de la presente invención se proporciona un método para consultar información de mapeado. A continuación se explica el método haciendo referencia a la FIG. 7.

Cuando la Organización A intenta enviar datos a la Organización B, en primer lugar la Organización A comprueba si BR-A tiene la información de mapeado correspondiente al prefijo de la Organización B. Si BR-A tiene la información de mapeado correspondiente al prefijo de la Organización B, la Organización A le envía directamente los datos a la Organización B de acuerdo con la información de mapeado. En caso contrario se ejecutan los pasos que se muestran en la FIG. 7.

S401. La Organización A consulta a RA1 de acuerdo con el prefijo 10.3.1.0/24 de la Organización B y obtiene el par de mapeado firmado {prefijo=10.3.1.0/24, IP de tránsito=192.168.2.2, información de control de mapeado, información de control de firma, Firma B} devuelto por RA1. De hecho, la Organización A puede obtener el par de mapeado firmado de la Organización B consultando a RA1 o a RA2 de acuerdo con el prefijo 10.3.1.0/24 de la Organización B.

S402. La Organización A comprueba si el par de mapeado firmado es válido en función de la información de control de firma en el par de mapeado firmado, lo cual incluye:

comprobar si el formato del certificado es válido;

comprobar si se ha recibido la fecha de expiración del par de mapeado firmado;

comprobar si el certificado de la Organización B es creíble y si el certificado ha expirado; y

verificar si el campo de firma en el par de mapeado firmado es válido con la clave privada en el certificado de la Organización B.

El BR-A toma el par de mapeado firmado como válido únicamente si la comprobación es satisfactoria.

S403. Después de haber determinado mediante la comprobación que el par de mapeado firmado es válido, la Organización A le envía datos a la Organización B de acuerdo con la información de mapeado en el par de mapeado firmado.

Tal como se puede ver a partir de la descripción anterior, con el método de consulta de información de mapeado proporcionado en el modo de realización de la presente invención, se firma un par de información de mapeado utilizando la clave privada de un certificado X.509v3. Cuando se consulta la información de mapeado, se verifica la firma del par de mapeado firmado y el par de mapeado firmado es válido únicamente cuando la verificación es satisfactoria. De este modo, el método evita que un atacante proporcione información falsa al solicitante haciéndose pasar por un RA. El método también evita que un RA altere la información de mapeado y de este modo mejora la fiabilidad de la consulta de información de mapeado y elimina los potenciales problemas de seguridad de la técnica anterior. En consecuencia, se mejora la fiabilidad de la red o el sistema de comunicaciones.

En un método de gestión de encaminamiento de red de acuerdo con un modo de realización de la presente invención, la organización de red perimetral puede revocar un par de mapeado firmado que ella ha registrado con el RA. Específicamente, tomando como ejemplo la Organización A, tal como se muestra en la FIG. 8, el proceso de revocación incluye:

S501. La Organización A genera un registro de revocación del par de mapeado firmado en la forma primaria {{prefijo=10.2.1.0/24, IP de tránsito=192.168.1.2, información de control de mapeado}, información de control de firma de revocación, Firma A de Revocación}.

S502. La Organización A envía el registro de revocación del par de mapeado firmado generado a la base de datos de registros de revocación de pares de mapeado firmados del RA1 adyacente. De hecho, la Organización A le puede enviar el registro de revocación del par de mapeado firmado generado a la base de datos de registro de revocación de pares de mapeado firmados de RA1 o de RA2.

S503. El RA1 elimina de la base de datos de pares de mapeado firmados el par de mapeado firmado que se corresponde con el registro de revocación del par de mapeado firmado y sincroniza el registro de revocación del par de mapeado firmado con las bases de datos de registro de revocación de pares de mapeado firmados de otros RA (por ejemplo, el RA2). El resto de RA (por ejemplo, el RA2) eliminan de sus bases de datos de pares de mapeado firmados el par de mapeado firmado que se corresponde con el registro de revocación del par de mapeado firmado.

En el caso de que la Organización B desee revocar su par de mapeado firmado, se ejecutan unos pasos similares a los descritos más arriba y no se volverán a describir aquí.

Con el método de gestión de información de mapeado proporcionado en el modo de realización de la presente invención, se firma un par de información de mapeado utilizando la clave privada de un certificado X.509v3, lo cual asegura la fiabilidad de la información de mapeado en las operaciones de registro, consulta y sincronización y elimina los potenciales problemas de seguridad de la técnica anterior. En consecuencia, se mejora la fiabilidad de la red o el sistema de comunicaciones.

Basándose en el método para gestionar y consultar información de mapeado de acuerdo con los modos de realización de la presente invención descritos más arriba, un modo de realización de la presente invención proporciona un sistema de comunicaciones. Tal como se muestra en la FIG. 11, el sistema incluye:

un dispositivo de red perimetral, configurado para firmar un par de información de mapeado utilizando la clave privada de un certificado correspondiente al prefijo en el par de información de mapeado con el fin de generar un par de mapeado firmado y enviarle el par de mapeado firmado a un dispositivo RA; y

el dispositivo RA, configurado para recibir el par de mapeado firmado enviado por el dispositivo de red perimetral y compartir el par de mapeado firmado con otros RA mediante sincronización de datos.

La FIG. 12 ilustra un dispositivo de red perimetral de acuerdo con un primer modo de realización de la presente invención. El dispositivo de red perimetral incluye:

una unidad 1100 de generación de pares de mapeado firmados, configurada para firmar el par de información de mapeado utilizando la clave privada del certificado correspondiente al prefijo en el par de información de mapeado con el fin de generar el par de mapeado firmado; y

una unidad 1200 de envío, configurada para enviarle el par de mapeado firmado al RA en la red de tránsito.

La FIG. 13 ilustra un dispositivo de red perimetral de acuerdo con un segundo modo de realización de la presente invención. Además de la unidad 1100 de generación de pares de mapeado firmados y la unidad 1200 de envío, el dispositivo de red perimetral incluye, además:

una unidad 1300 de consulta, configurada para consultar al RA de acuerdo con el prefijo de la organización de la segunda red perimetral y obtener el par de mapeado firmado de la organización de la segunda red perimetral devuelto por el RA;

una unidad 1400 de comprobación, acoplada a la unidad 1300 de consulta y configurada para comprobar si es válido el par de mapeado firmado de la organización de la segunda red perimetral; y

una unidad 1500 de envío de datos, configurada para enviarle datos a la organización de la segunda red perimetral de acuerdo con la información de mapeado en el par de mapeado firmado después de que la unidad 1400 de comprobación haya determinado que el par de mapeado firmado es válido.

La FIG. 14 ilustra un dispositivo de red perimetral de acuerdo con un tercer modo de realización de la presente invención. En el tercer modo de realización, el dispositivo de red perimetral tiene la misma estructura que el del segundo modo de realización e incluye, además:

una unidad 1600 de generación de registros de revocación, configurada para generar un registro de revocación del par de mapeado firmado; y

una unidad 1700 de envío de registros de revocación, configurada para enviarle al RA el registro de revocación del par de mapeado firmado con el fin de revocar el par de mapeado firmado que se corresponde con el registro de revocación del par de mapeado firmado.

La FIG. 15 ilustra un dispositivo de red perimetral de acuerdo con un cuarto modo de realización de la presente invención. En el cuarto modo de realización, el dispositivo de red perimetral tiene la misma estructura que el del primer modo de realización e incluye, además, la unidad 1600 de generación de registros de revocación y la unidad 1700 de envío de registros de revocación.

La FIG. 16 ilustra un dispositivo RA de acuerdo con un primer modo de realización de la presente invención. El dispositivo RA incluye:

una unidad 2100 de recepción, configurada para recibir un par de mapeado firmado enviado por una organización de la red perimetral;

una unidad 2200 de base de datos de pares de mapeado firmados, configurada para almacenar el par de mapeado firmado recibido por la unidad 2100 de recepción; y

una unidad 2300 de sincronización, configurada para sincronizar con otros RA el par de mapeado firmado almacenado por la unidad 2200 de base de datos de pares de mapeado firmados.

La FIG. 17 ilustra un dispositivo RA de acuerdo con un segundo modo de realización de la presente invención. Además de la unidad 2100 de recepción, la unidad 2200 de base de datos de pares de mapeado firmados y la unidad 2300 de sincronización, el dispositivo RA en el segundo modo de realización incluye, además:

una unidad 2400 de respuesta a consultas, configurada para consultar un par de mapeado firmado correspondiente a un prefijo en función del prefijo proporcionado por una organización de la red perimetral y devolver el par de mapeado firmado a la organización de la red perimetral.

La FIG. 18 ilustra un dispositivo RA de acuerdo con un tercer modo de realización de la presente invención. En el tercer modo de realización, el dispositivo RA tiene la misma estructura que el segundo modo de realización e incluye, además:

una unidad 2500 de respuesta a la revocación, configurada para eliminar el par de mapeado firmado que se corresponde con un registro de revocación del par de mapeado firmado proporcionado por la organización de la red perimetral desde la unidad de base de datos de pares de mapeado firmados y para sincronizar el registro de revocación del par de mapeado firmado con otros RA; y

una unidad 2600 de base de datos de registros de revocación, configurada para almacenar el par de mapeado firmado eliminado por la unidad 2500 de respuesta a la revocación.

La FIG. 19 ilustra un dispositivo RA de acuerdo con un cuarto modo de realización de la presente invención. En el cuarto modo de realización, el dispositivo RA tiene la misma estructura que el del primer modo de realización e incluye, además, la unidad 2500 de respuesta a la revocación y la unidad 2600 de base de datos de registros de revocación.

Para resumir, con el método de gestión de información de mapeado, el método de consulta de información de mapeado, los dispositivos y el sistema de comunicaciones proporcionados en los modos de realización de la presente invención, un par de información de mapeado es firmado utilizando la clave privada de un certificado, lo cual asegura la fiabilidad de la información de mapeado en las operaciones de registro, consulta y sincronización, y elimina los potenciales problemas de seguridad de la técnica anterior. En consecuencia, se mejora la fiabilidad de la red o el sistema de comunicaciones.

Mediante las descripciones de los modos de realización anteriores, aquellos experimentados en la técnica pueden entender que la presente invención se puede implementar utilizando únicamente hardware o utilizando software y una plataforma hardware universal necesaria. Basándose en dichos conocimientos, toda o parte de la solución técnica bajo la presente invención que hace contribuciones a la técnica anterior se puede materializar esencialmente en forma de un producto software. El producto software se puede almacenar en un medio de almacenamiento, el cual puede ser un disco magnético, un disco compacto de memoria de sólo lectura (CD-ROM), una memoria de sólo lectura (ROM) o una memoria de acceso aleatorio (RAM). El producto de software

incluye una serie de instrucciones que permiten que un dispositivo informático (ordenador personal, servidor o dispositivo de red) ejecute los métodos proporcionados en los modos de realización de la presente invención.

Las descripciones anteriores son únicamente algunos ejemplos de modos de realización de la presente invención, pero no pretenden limitar la presente invención.

REIVINDICACIONES

1. Un método para gestionar información de mapeado en encaminamiento de red, que comprende:

firmar (S101), por parte de un dispositivo de una red perimetral, un par de información de mapeado utilizando una clave privada de un certificado correspondiente a un prefijo de la red perimetral en el par de información de mapeado con el fin de generar un par de mapeado firmado;

enviar (S102), por parte del dispositivo de la red perimetral, el par de mapeado firmado a un agente de registro, RA, en una red de tránsito; y

compartir (S103), por parte del RA, el par de mapeado firmado con otros RA mediante sincronización de datos;

en donde el par de información de mapeado comprende al menos la siguiente información: el prefijo, una dirección del Protocolo de Internet, IP, del dispositivo, en donde la dirección IP se encuentra en la red de tránsito, e información de control de mapeado; y

el par de mapeado firmado comprende al menos la siguiente información: el prefijo, la dirección IP, la información de control de mapeado, una información de control de firma y una firma, en donde:

la información de control de firma comprende: una información de certificado utilizada para la firma, un punto de revocación del par de mapeado firmado, una fecha de expiración y una información del algoritmo de firma.

2. El método de la reivindicación 1, que comprende, además:

generar, por parte del dispositivo de red perimetral, un registro de revocación del par de mapeado firmado que comprende: el prefijo, la dirección IP, la información de control de mapeado, una información de control de firma de revocación y una firma de revocación;

enviar, por parte del dispositivo de red perimetral, al RA en la red de tránsito el registro de revocación del par de mapeado firmado generado; y

eliminar, por parte del RA, un par de mapeado firmado que se corresponde con el registro de revocación del par de mapeado firmado y sincronizar el registro de revocación del par de mapeado firmado con otros RA.

3. Un método para consultar información de mapeado, que comprende:

consultar, por parte de una organización de la primera red perimetral, un agente de registro, RA, de acuerdo con un prefijo de una segunda red perimetral y obtener un par de mapeado firmado de una organización de la segunda red perimetral devuelto por el RA;

comprobar, por parte de la organización de la primera red perimetral, si el par de mapeado firmado es válido de acuerdo con la información de control de firma en el par de mapeado firmado; y

después de haber determinado mediante la comprobación que el par de mapeado firmado es válido, extraer, por parte de la organización de la primera red perimetral, la información de mapeado en el par de mapeado firmado;

en donde la información de mapeado comprende un mapeado entre el prefijo de la segunda red perimetral y una dirección del Protocolo de Internet, IP, de un dispositivo de la segunda red perimetral que registra el prefijo, en donde la dirección IP se encuentra en la red de tránsito; y

en donde el par de mapeado firmado comprende al menos la siguiente información: el prefijo, la dirección IP, una información de control de mapeado, una información de control de firma y una firma, en donde:

la información de control de firma comprende: información de certificado utilizado por la firma, un punto de revocación del par de mapeado firmado, una fecha de expiración y una información del algoritmo de firma.

4. El método de la reivindicación 3, en donde el paso de comprobación de si el par de mapeado firmado es válido de acuerdo con la información de control de firma en el par de mapeado firmado comprende:

comprobar si está cualificado un formato de certificado;

comprobar si ha llegado la fecha de expiración del par de mapeado firmado;

comprobar si es creíble un certificado de una organización de la segunda red perimetral y si ha expirado el certificado; y

verificar si es válido un campo de firma en el par de mapeado firmado utilizando una clave pública en el certificado de la organización de la segunda red perimetral.

5. Un dispositivo de una red perimetral, que comprende:

una unidad (1100) de generación de pares de mapeado firmados, configurada para firmar un par de información de mapeado utilizando una clave privada de un certificado correspondiente a un prefijo de la red perimetral en el par de información de mapeado con el fin de generar un par de mapeado firmado; y

una unidad (1200) de envío, configurada para enviar el par de mapeado firmado a un agente de registro, RA, en una red de tránsito;

en donde el par de información de mapeado comprende al menos la siguiente información: el prefijo, una dirección del Protocolo de Internet, IP, del dispositivo, en donde la dirección IP se encuentra en la red de tránsito, y una información de control de mapeado; y

el par de mapeado firmado comprende al menos la siguiente información: el prefijo, dirección IP k, una información de control de mapeado, una información de control de firma y una firma, en donde:

la información de control de firma comprende: una información de certificado utilizado para la firma, un punto de revocación del par de mapeado firmado, una fecha de expiración y una información del algoritmo de firma.

6. El dispositivo de la red perimetral de la reivindicación 5, que comprende, además:

una unidad (1300) de consulta, configurada para consultar un RA de acuerdo con un prefijo de una segunda red perimetral y obtener un par de mapeado firmado de una organización de la segunda red perimetral devuelto por el RA;

una unidad (1400) de comprobación, acoplada a la unidad (1300) de consulta y configurada para comprobar si es válido el par de mapeado firmado de la organización de la segunda red perimetral;

una unidad (1500) de envío de datos, configurada para enviar datos a la organización de la segunda red perimetral de acuerdo con la información de mapeado en el par de mapeado firmado después de que la unidad de comprobación haya determinado que el par de mapeado firmado es válido.

7. El dispositivo de la red perimetral de la reivindicación 5 ó 6, que comprende, además:

una unidad (1600) de generación de registros de revocación, configurada para generar un registro de revocación de un par de mapeado firmado; y

una unidad (1700) de envío de registros de revocación, configurada para enviar el registro de revocación del par de mapeado firmado a un RA con el fin de revocar un par de mapeado firmado que se corresponde con el registro de revocación del par de mapeado firmado.

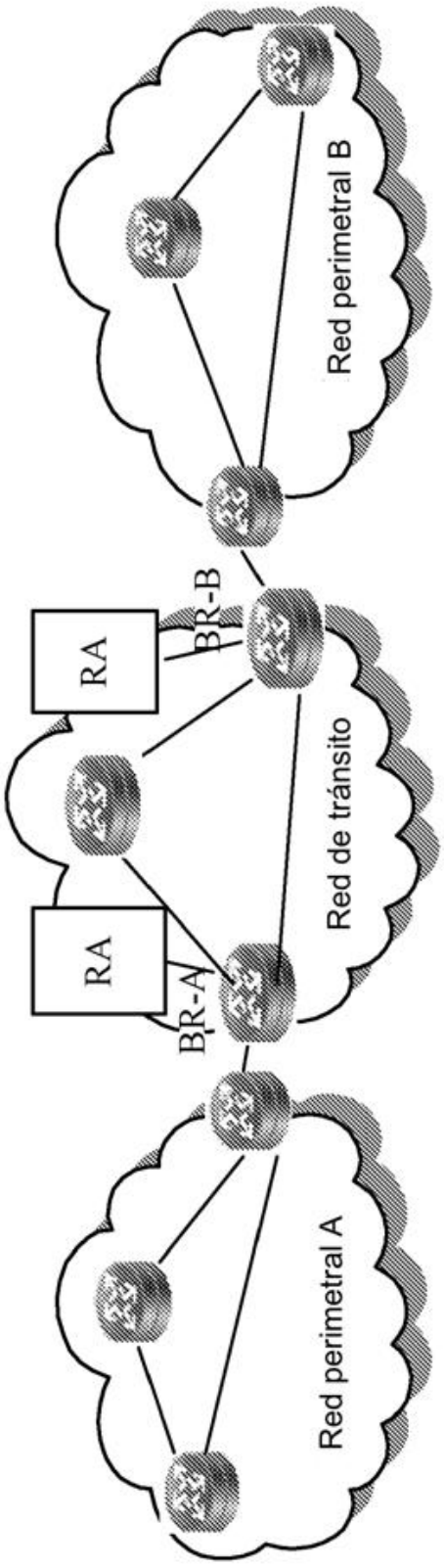
Red perimetral B
BR-B
RA
Red de tránsito
RA
BR-A
Red perimetral A

FIG. 1

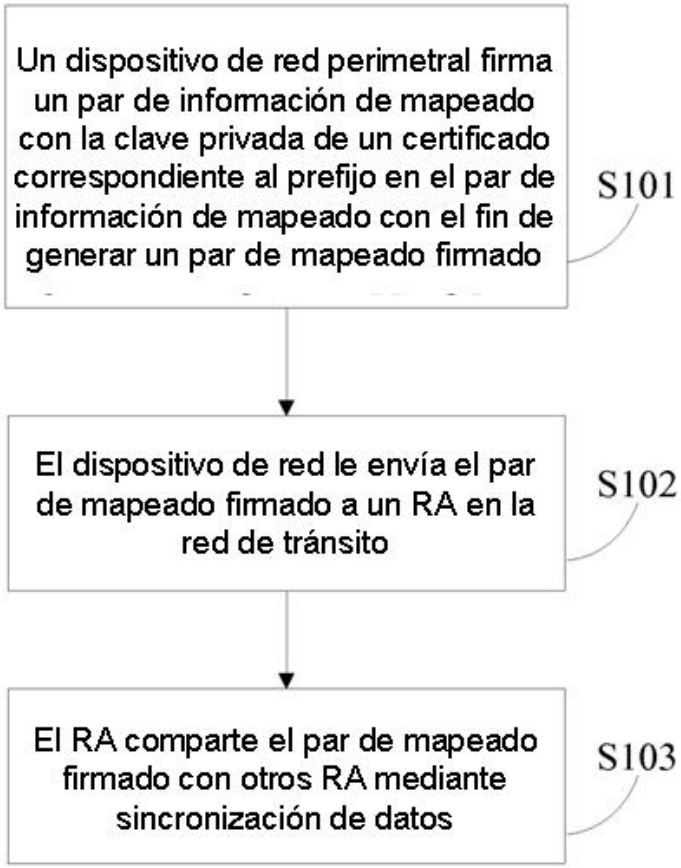
Un dispositivo de red perimetral firma un par de información de mapeado con la clave privada de un certificado correspondiente al prefijo en el par de información de mapeado con el fin de generar un par de mapeado firmado
S101
El dispositivo de red le envía el par de mapeado firmado a un RA en la red de tránsito
S102
El RA comparte el par de mapeado firmado con otros RA mediante sincronización de datos
S103

FIG. 2

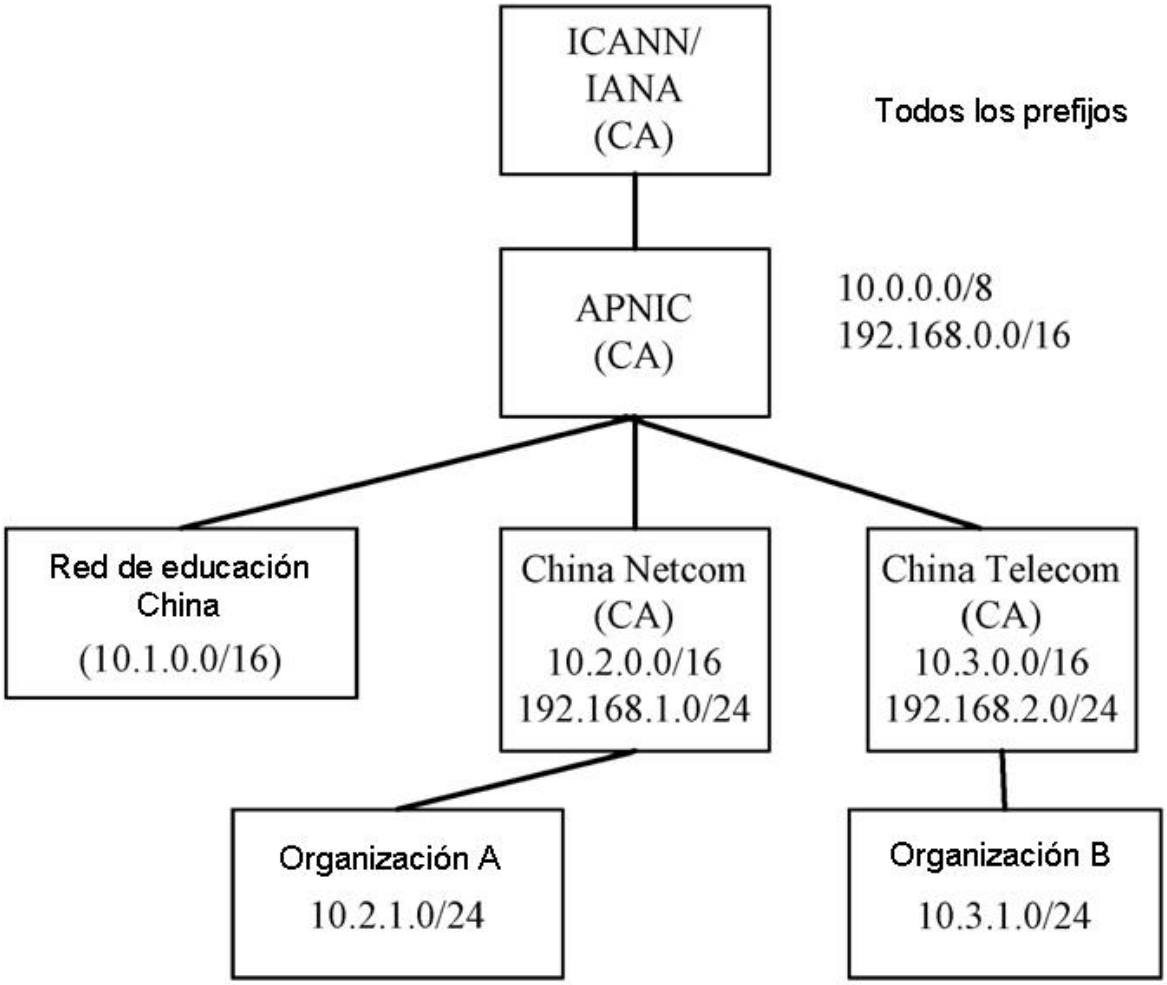
ICANN/
IANA
(CA)
Todos los prefijos
APNIC
(CA)
10.0.0.0/8
192.168.0.0/16
Red de educación
China
(10.1.0.0/16)
China Netcom
(CA)
10.2.0.0/16
192.168.1.0/24
China Telecom
(CA)
10.3.0.0/16
192.168.2.0/24
Organización A
10.2.1.0/24
Organización B
10.3.1.0/24

FIG. 3

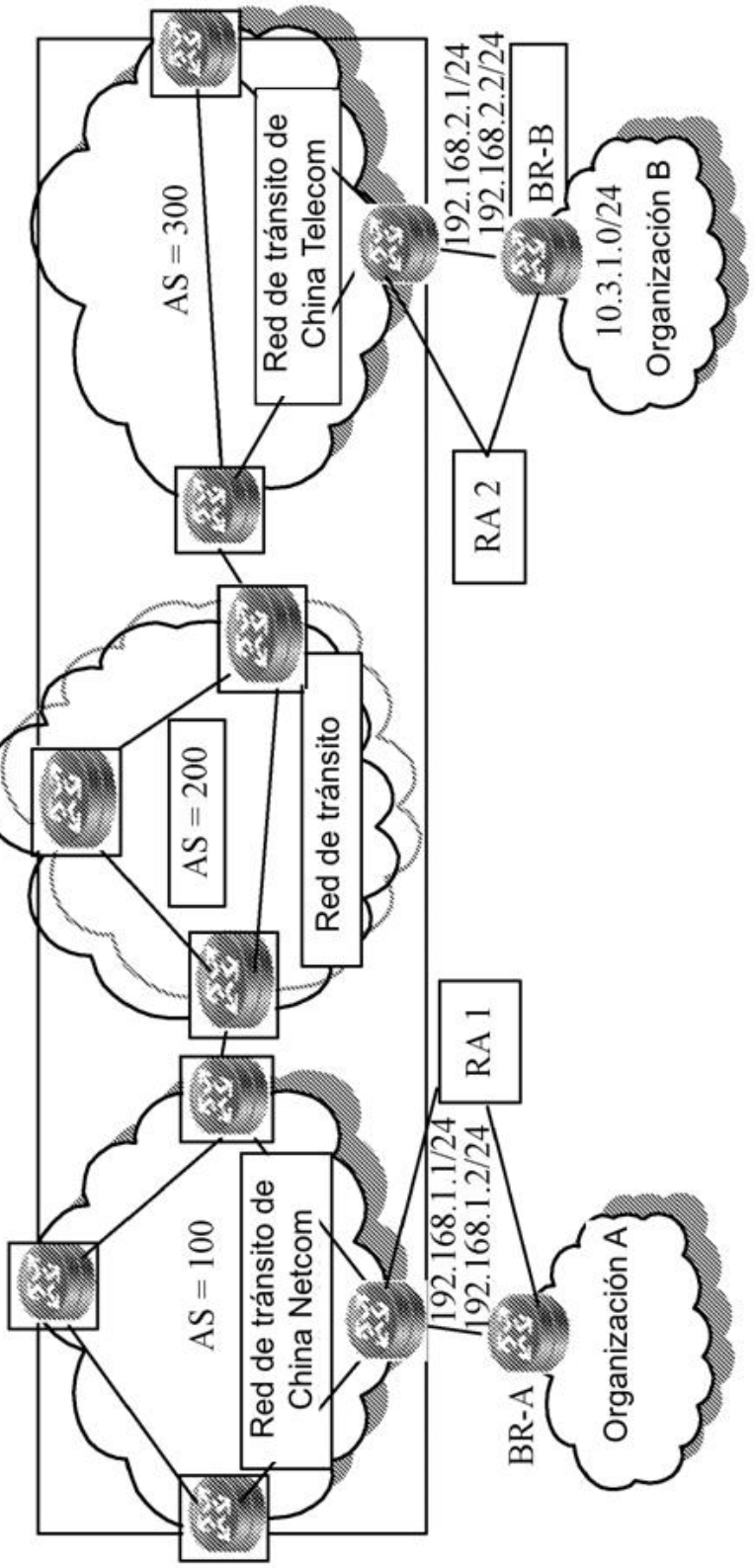
AS = 300
Red de tránsito de China Telecom
AS = 200
Red de tránsito
AS = 100
Red de tránsito de China Netcom
192.168.2.1/24
192.168.2.2/24
BR-B
10.3.1.0/24
Organización B
RA 2
RA 1
192.168.1.1/24
192.168.1.2/24
BR-A
Organización A

FIG. 4

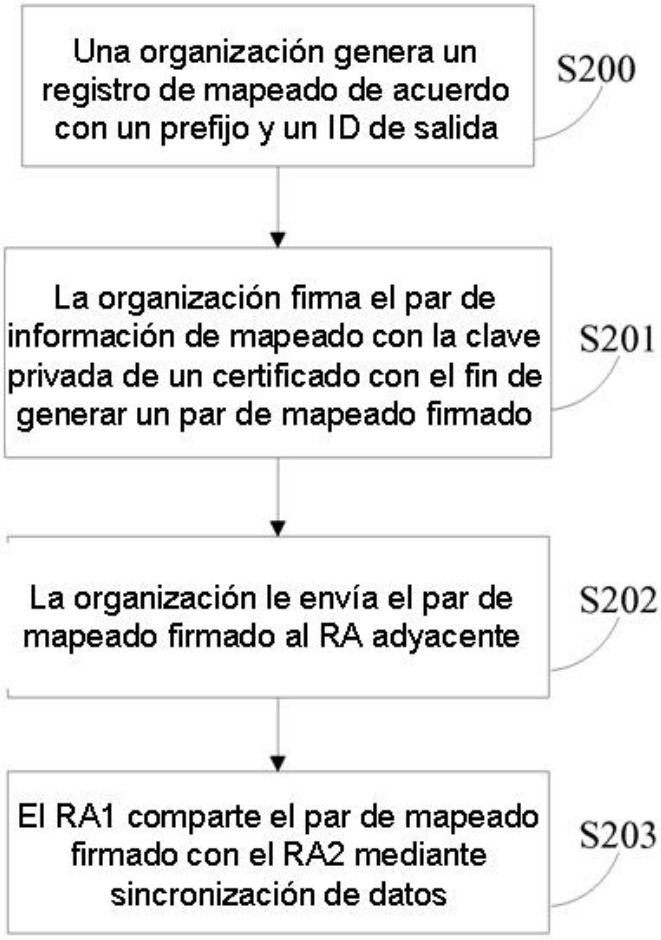
Una organización genera un registro de mapeado de acuerdo con un prefijo y un ID de salida
S200
La organización firma el par de información de mapeado con la clave privada de un certificado con el fin de generar un par de mapeado firmado
S201
La organización le envía el par de mapeado firmado al RA adyacente
S202
El RA1 comparte el par de mapeado firmado con el RA2 mediante sincronización de datos
S203

FIG. 5

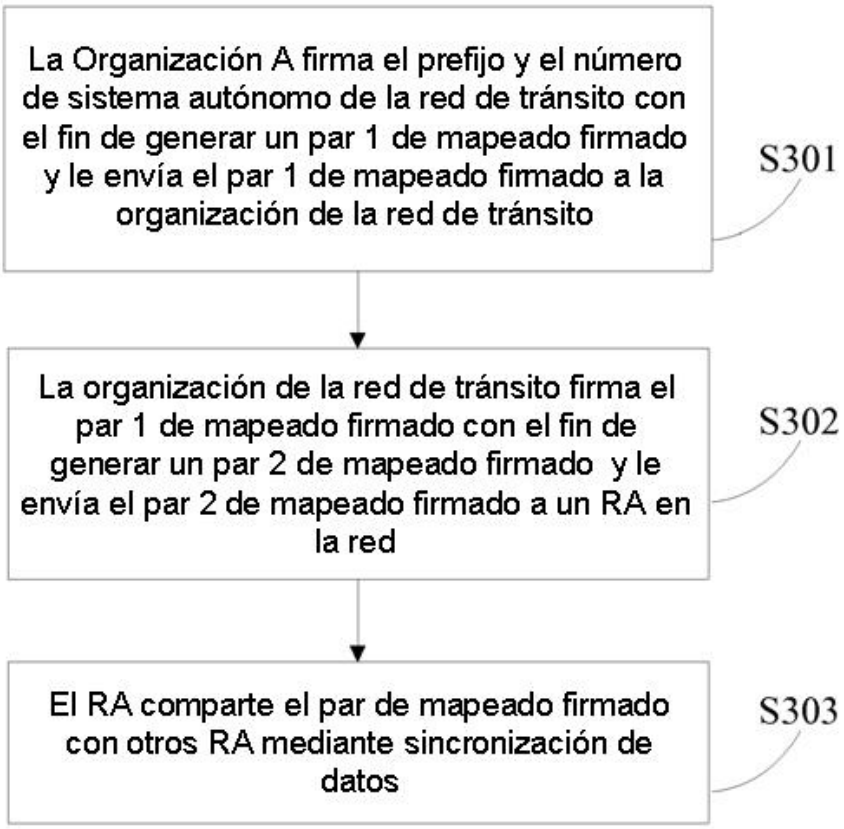
La Organización A firma el prefijo y el número de sistema autónomo de la red de tránsito con el fin de generar un par 1 de mapeado firmado y le envía el par 1 de mapeado firmado a la organización de la red de tránsito
S301
La organización de la red de tránsito firma el par 1 de mapeado firmado con el fin de generar un par 2 de mapeado firmado y le envía el par 2 de mapeado firmado a un RA en la red
S302
El RA comparte el par de mapeado firmado con otros RA mediante sincronización de datos
S303

FIG. 6

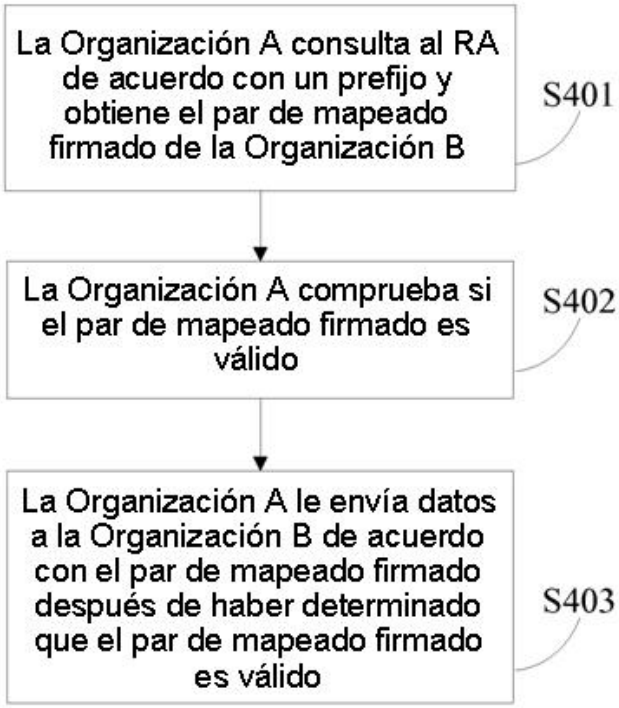
La Organización A consulta al RA de acuerdo con un prefijo y obtiene el par de mapeado firmado de la Organización B
S401
La Organización A comprueba si el par de mapeado firmado es válido
S402
La Organización A le envía datos a la Organización B de acuerdo con el par de mapeado firmado después de haber determinado que el par de mapeado firmado es válido
S403

FIG. 7

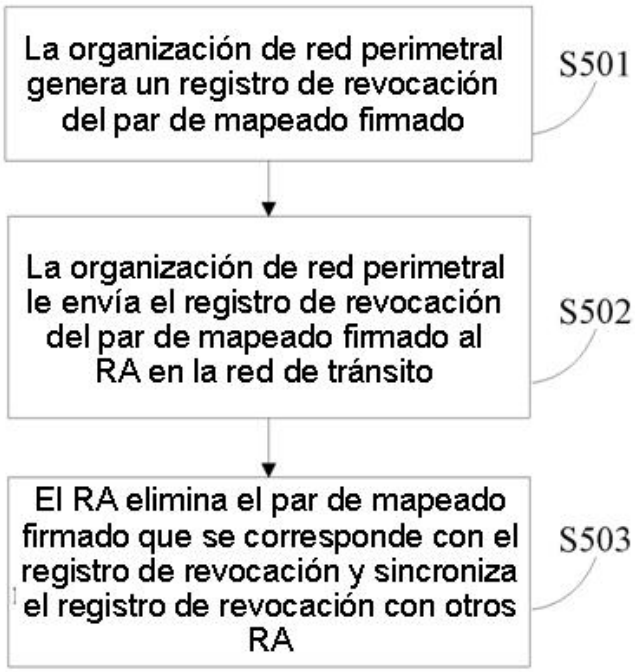
La organización de red perimetral genera un registro de revocación del par de mapeado firmado
S501
La organización de red perimetral le envía el registro de revocación del par de mapeado firmado al RA en la red de tránsito
S502
El RA elimina el par de mapeado firmado que se corresponde con el registro de revocación y sincroniza el registro de revocación con otros RA
S503

FIG. 8

X. 509 v3
Número de Serie = xx.xx.xx
Algoritmo Firmado = PKCS #1
Expedido por = China Netcom
Fecha de expiración = 01/01/2008 – 31/12/2008
Sujeto = Organización A
Información de Clave Pública del Sujeto
Prefijo = 10.2.1.0/24
...

FIG. 9

X. 509 v3
Número de Serie = xx.xx.xx
Algoritmo Firmado = PKCS #1
Expedido por = China Netcom
Fecha de expiración = 01/01/2008 – 31/12/2008
Sujeto = China Netcom
Información de Clave Pública del Sujeto
Prefijo = 192.1.1.0/24
AS = 100
...

FIG. 10

FIG. 11

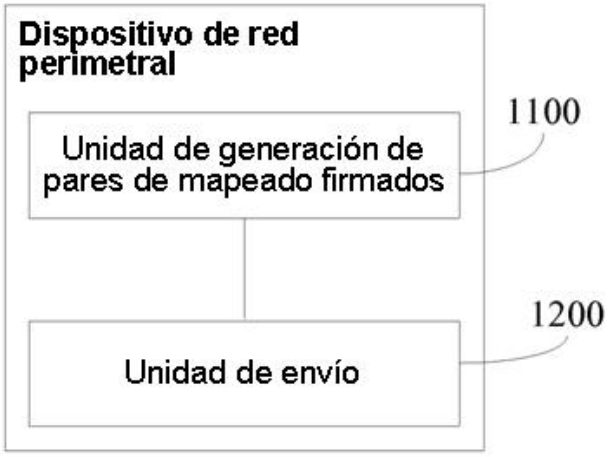
Dispositivo de red perimetral
Unidad de generación de pares de mapeado firmados
1100
Unidad de envío
1200

FIG. 12

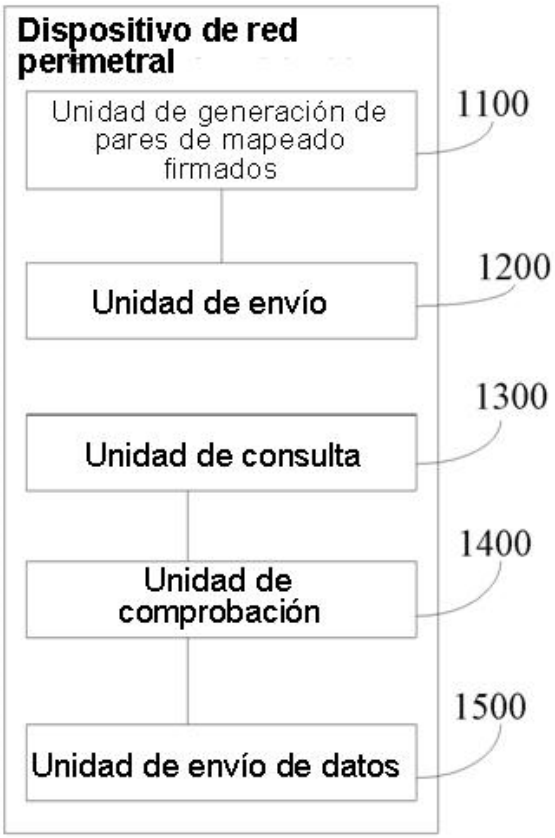
Dispositivo de red perimetral
Unidad de generación de pares de mapeado firmados
1100
Unidad de envío
1200
Unidad de consulta
1300
Unidad de comprobación
1400
Unidad de envío de datos
1500

FIG. 13

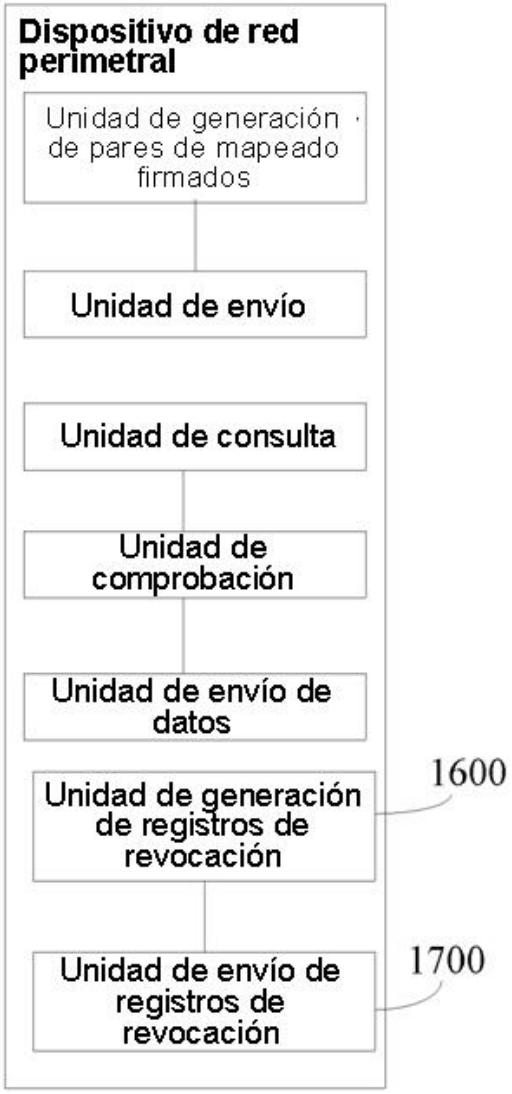
Dispositivo de red perimetral
Unidad de generación de pares de mapeado firmados
Unidad de envío
Unidad de consulta
Unidad de comprobación
Unidad de envío de datos
Unidad de generación de registros de revocación
1600
Unidad de envío de registros de revocación
1700

FIG. 14

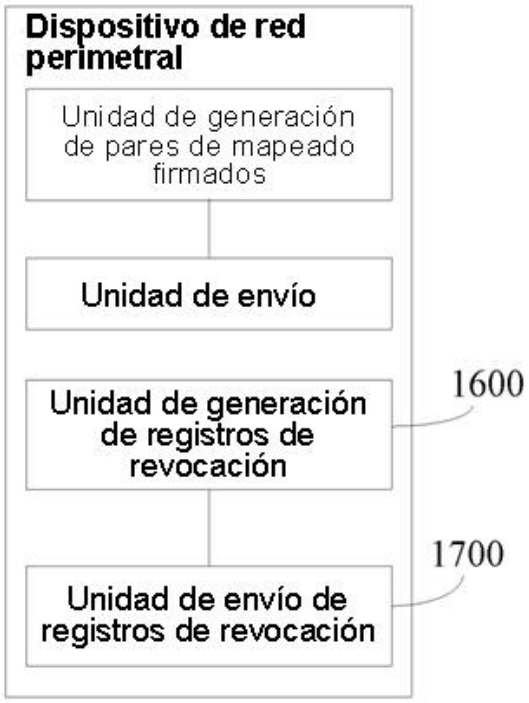
Dispositivo de red perimetral
Unidad de generación de pares de mapeado firmados
Unidad de envío
Unidad de generación de registros de revocación
1600
Unidad de envío de registros de revocación
1700

FIG. 15

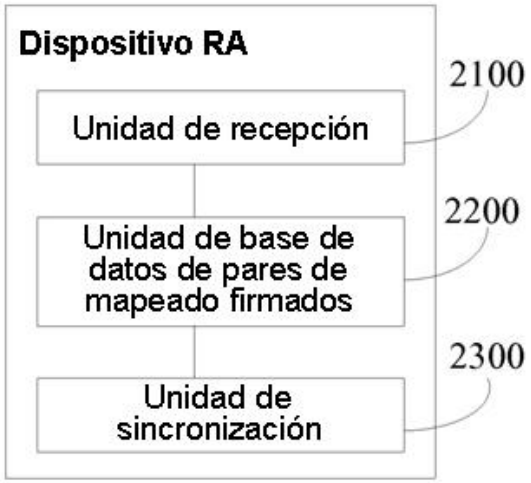
Dispositivo RA
Unidad de recepción
2100
Unidad de base de datos de pares de mapeado firmados
2200
Unidad de sincronización
2300

FIG. 16

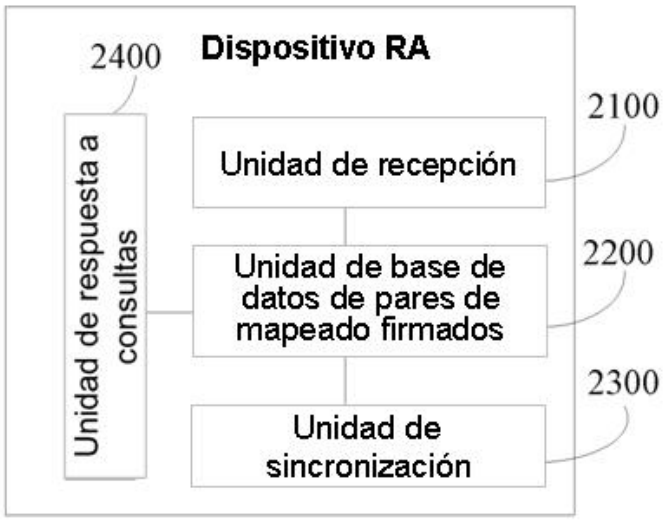
Dispositivo RA
2400
Unidad de respuesta a consultas
Unidad de recepción
2100
Unidad de base de datos de pares de mapeado firmados
2200
Unidad de sincronización
2300

FIG. 17

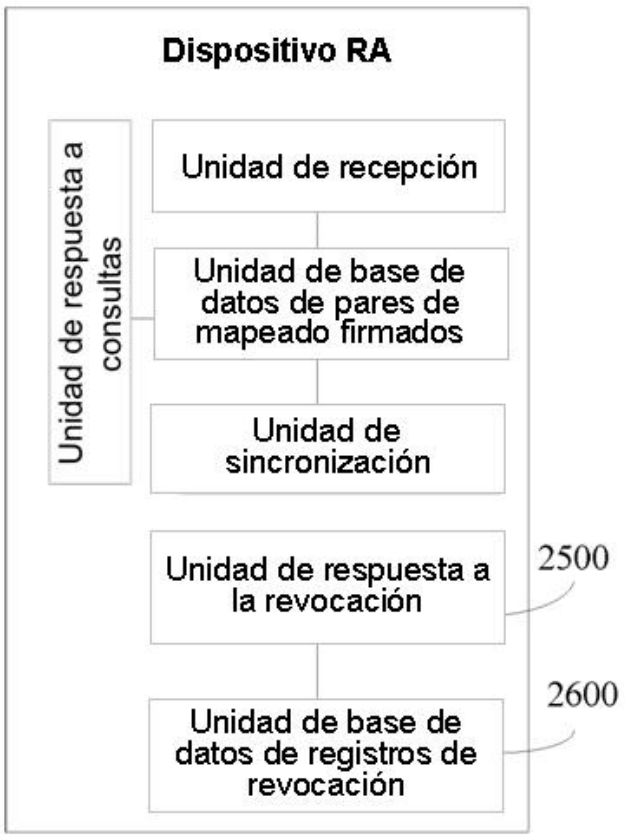
Dispositivo RA
Unidad de respuesta a consultas
Unidad de recepción
Unidad de base de datos de pares de mapeado firmados
Unidad de sincronización
Unidad de respuesta a la revocación
2500
Unidad de base de datos de registros de revocación
2600

FIG. 18

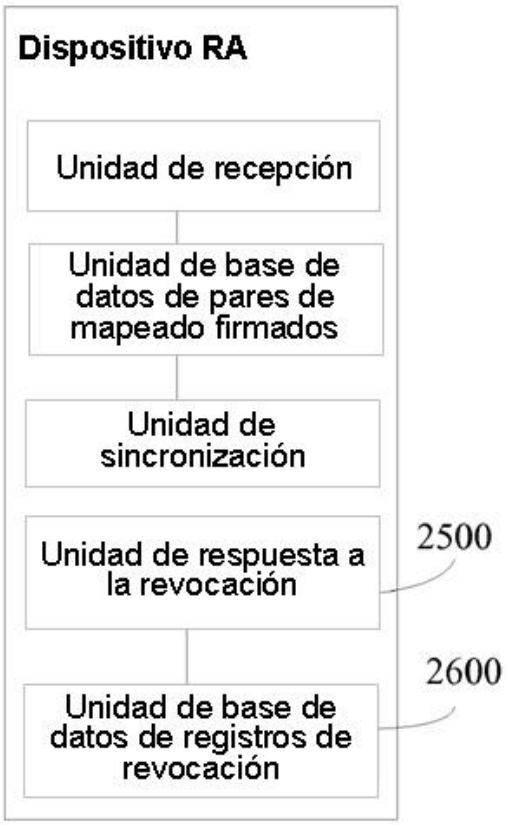
Dispositivo RA
Unidad de recepción
Unidad de base de datos de pares de mapeado firmados
Unidad de sincronización
Unidad de respuesta a la revocación
2500
Unidad de base de datos de registros de revocación
2600

FIG. 19