(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 395 860**

(51) Int. CI.:

H04L 12/56 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.09.2007 E 07802090 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.11.2012 EP 2062400**

(54) Título: **Procedimiento y sistema para direccionamiento y encaminamiento en enlaces de comunicaciones codificados**

(30) Prioridad:

14.09.2006 DE 102006043156
12.01.2007 DE 102007001831

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.02.2013

(73) Titular/es:

ROHDE & SCHWARZ GMBH & CO. KG (100.0%)
MÜHLDORFSTRASSE 15
81671 MÜNCHEN, DE

(72) Inventor/es:

GRUBER, INGO;
LANGGUTH, TORSTEN y
SCHOBER, HENRIK

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimiento y sistema para direccionamiento y encaminamiento en enlaces de comunicaciones codificados

[0001] Los equipos de radio del futuro tendrán unas posibilidades de utilización claramente más flexibles que los equipos de radio actuales. Esto se consigue por el concepto de “Radios Definidas por Software” (SDR). Los equipos SDR ofrecen la posibilidad de cargar procedimientos de radio (formas de ondas) en forma de software y de modificar la configuración de las formas de ondas y del equipo de radio de modo flexible a través de un control de software. Los procedimientos modernos de transmisión por radio pueden apoyar aquí también la transmisión de paquetes de datos según el estándar de Protocolo de Internet (IP). Esto permite la utilización de aplicaciones estándar de IP y de conceptos conocidos que también se utilizan para Internet.

[0002] Según los requisitos de seguridad ha de ser posible transmitir informaciones sensibles codificadas (seguridad de comunicación, COMSEC). Esto se puede conseguir mediante la aplicación de la norma IPsec, descrita en S. Kent, K. Seo, “Security Architecture for the Internet Protocol”, IETP RFC 4301, diciembre del 2005.

[0003] Esta norma permite dos procedimientos de transmisión diferentes para informaciones codificadas: El modo de transporte y el modo de túnel, como se ha representado en la figura 1. En el modo de transporte se codifican únicamente los datos útiles del paquete IP, mientras que el encabezado del IP (entre otros con las direcciones de IP del emisor y del receptor) no se modifica. En el modo túnel se codifica todo el paquete IP original y se añade un nuevo encabezado. El nuevo encabezado contiene como dirección de origen la dirección del equipo de codificación y no la del nodo fuente original. De la misma forma, la dirección de destino en el nuevo encabezado es la del equipo decodificador y no la del equipo receptor real. Así se puede impedir de modo efectivo que un potencial transgresor de la dirección de origen y de destino pueda detectar una comunicación que tiene lugar entre las partes comunicantes. El transgresor potencial puede ver únicamente que se intercambian datos entre los dos equipos de codificación. Los usuarios finales propiamente dichos del intercambio de datos permanecen ocultos.

[0004] Para la comunicación relevante en cuanto a seguridad y confidencial se utiliza el modo túnel. Por el modo túnel se producen dos niveles de red completamente separadas entre si. El nivel rojo es el nivel confidencial. A una red roja solamente tienen acceso personas autorizadas. Por el contrario, la red negra representa una red pública, por lo que ha de clasificarse como insegura. Las informaciones confidenciales de una red roja solamente pueden transmitirse a través de una red de modo codificado. Debido a la utilización estricta del modo túnel, estas redes no disponen de momento de informaciones mutuas. Desde el punto de vista del nivel rojo de red, el modo túnel representa un túnel transparente para otra red roja y oculta el nivel negro de red existente detrás. La figura 1 aclara esta circunstancia. Los usuarios A y D no tienen ningún conocimiento sobre cualquier usuario de red X e Y adicional que posiblemente pueda existir y que participa en la transmisión de los datos entre B y C.

[0005] El documento US 2005/091482 A1, revela un procedimiento de encaminamiento de modo que el usuario de red puede configurar una red como red física o virtual. En el primer caso, el encaminamiento se realiza a través del protocolo IP; en el segundo caso, el encaminamiento se basa en la norma IPSec y se ejecuta con direcciones codificadas en el modo túnel. Existe la posibilidad de acoplar a través de una pasarela la red definida en US 2005/091482 A1 con otra red que implemente otro protocolo de encaminamiento.

[0006] Una separación completa, sin embargo, también afecta negativamente a toda la arquitectura de la red. En los equipos de codificación han de estar disponibles informaciones de cuales redes rojas están conectadas con un equipo de descodificación negro. Esto es necesario para poder registrar en el modo túnel, en los nuevos encabezados IP generados, la dirección de destino negra correspondiente.

[0007] En una red de comunicación se han agrupado varios usuarios de red. Como se muestra en la figura 2, varios equipos terminales pueden utilizar el mismo equipo de codificación. Cada equipo de codificación tiene una dirección confidencial roja, así como también una dirección pública negra. Los equipos terminales de una subred confidencial envían datos sin codificar al equipo de codificación. Éste codifica los datos en el modo túnel y los transmite a través de una conexión insegura de comunicación al equipo receptor de codificación, donde se descodifican y transmiten al receptor.

[0008] Las direcciones negras del equipo de codificación de una red se determinan automáticamente por un protocolo con autoconfiguración de direcciones. Para el encaminamiento en la jerarquía negra se utiliza un protocolo de encaminamiento tradicional. El intercambio de informaciones de señalización se encarga de la consistencia de la topología dentro de la red negra. Sin embargo, para una conexión de equipos terminales ha de ser posible intercambiar también datos entre la red roja y la red negra. Esto a su vez, presupone el conocimiento de la correlación de direcciones entre direcciones negras y rojas del equipo de codificación. Sin embargo, el modo túnel de IPsec impide una reproducción directa de las direcciones negras conocidas sobre las direcciones rojas.

[0009] Debido a ello, ya no es posible un encaminamiento común y simultáneo en ambas redes. Para intercambiar automáticamente las informaciones de encaminamiento de la red roja entre dos equipos de codificación se puede utilizar, por ejemplo, el protocolo de descubrimiento de la norma IPsec.

[0010] Para poder reproducir la solución propuesta por la invención y los problemas derivados de la solución propuesta por la técnica actual se ofrece a continuación una corta introducción acerca del direccionamiento de redes IP.

[0011] Para poder enviar datos entre dos usuarios en la red Internet global es necesaria una identificación unívoca del usuario final. Los nodos de transmisión pueden determinar entonces, con ayuda de la dirección de destino, el recorrido óptimo entre el emisor y receptor sin que el emisor haya de conocer el recorrido exacto. Una dirección se compone, para poder identificar de modo claro un usuario, de una identificación de red y una identificación de equipo. La identificación de red identifica la red en la que se encuentra el usuario, mientras que la identificación de equipo determina el usuario individual en una red. La dirección completa se genera aquí mediante la unión de las dos partes de direcciones, lo que se ha representado en la figura 3.

[0012] Todos los equipos que se encuentran dentro de una red utilizan la misma identificación de red, mientras que la identificación de equipo es respectivamente diferente. Por esta razón es necesario que un usuario final modifique su identificación de red en cuando cambia la red. Esto es necesario para que no sea necesario señalar a cada nodo de transmisión en Internet la nueva conexión del equipo final, si no se puede conocer directamente la red con ayuda de la identificación de red. La identificación de red de un equipo terminal es requerida para efectuar el encaminamiento dentro de la red global.

[0013] La identificación de equipo debería ser individual y unívoca para todos los equipos que participan en la red global. Se basa, por ejemplo, en la dirección de control de acceso al medio (MAC) de la tarjeta de red, aunque sin embargo, también puede generarse a partir de otro parámetro. Con ello se puede identificar unívocamente un equipo con ayuda de la identificación de equipo. Es constante y no se modifica con el tiempo.

[0014] Los equipos de codificación solamente tienen conocimiento de las direcciones negras de todos los usuarios que participan en la red a través del protocolo de encaminamiento. Para poder generar una conexión segura entre usuarios finales que se encuentran cada uno en una red roja, ha de realizarse en primer lugar una correspondencia clara y confidencial entre la dirección negra del equipo de decodificación y la red roja conectada al mismo. Esta correspondencia de direcciones rojas y negras, puede averiguarse con ayuda del protocolo de descubrimiento IPsec. En la figura 4 se ha representado el diagrama de flujo del protocolo, el cual describe la autenticación con ayuda de certificados. Sin embargo, dicha autenticación también es posible con ayuda de claves previamente intercambiadas (pre-shared keys (claves previamente compartidas), o PSK) si bien no se describe aquí más en detalle.

[0015] Para obtener una correlación confidencial entre una dirección negra y una roja de un equipo de codificación, el equipo de codificación A envía un mensaje “prueba *Hello*” a una dirección de multidifusión especialmente prevista para este fin. Así todos los usuarios participantes de la red reciben este mensaje. El mensaje contiene el certificado de seguridad del equipo de codificación A con una firma válida de la entidad de certificación. El certificado contiene, además, la clave del equipo de codificación A. Una vez recibido el mensaje, el equipo de codificación B comprueba la autenticidad del certificado con ayuda del certificado raíz de la entidad certificadora y autentifica el mismo mediante la firma o la clave del equipo de codificación A. Una vez obtenida con éxito la autenticación, el equipo de codificación B devuelve un mensaje de “respuesta *Hello*” al equipo de codificación. Este mensaje contiene las mismas informaciones del equipo de codificación B. Después de que el equipo de codificación A haya comprobado estas informaciones se inicia la negociación de la Security Association (Asociación de Seguridad) (SA) en la que se encuentran determinados, entre otros, el algoritmo de encriptación y las duraciones de validez para la autenticación y la clave. Puesto que hasta ahora los participantes de comunicación no conocen las direcciones rojas mutuas, no es posible realizar la negociación SA en el modo túnel del protocolo IPsec, sino que ésta ha de tener lugar en el modo transporte del IPsec. El encabezado del IP de los paquetes de datos se transmite aquí sin codificar entre los equipos de codificación y solamente se codifica el contenido propiamente dicho del paquete de datos. Los equipos de codificación pueden transmitir sus direcciones rojas codificadas en el modo de transporte IPsec después de que la SA haya realizado con éxito la negociación. Solamente entonces es posible la generación de una conexión de túnel entre los equipos de codificación.

[0016] Para poder comunicar con un usuario en particular de otra red roja es necesario, en primer lugar, generar un túnel a prueba de escuchas entre estas dos redes rojas. Esto requiere el conocimiento del equipo de codificación responsable para el equipo terminal correspondiente y las redes rojas conectadas con el mismo. Puesto que el protocolo de descubrimiento IPsec solamente apoya un intercambio secuencial de las informaciones de correlación con cada equipo de codificación por separado, es necesario generar túneles por pares entre todos los equipos de codificación para obtener un conocimiento completo de las asignaciones de direcciones de todos los equipos de codificación que se encuentran en la red. Por lo tanto ha de utilizarse para establecer un enlace con un usuario rojo, hasta ahora desconocido, en el peor de los casos el protocolo de descubrimiento del IPsec con todos los equipos posibles de codificación. El coste del equipo de codificación original aumenta, por lo tanto, de modo lineal con la cantidad de equipos de codificación N: Coste ~O (N). Para la integración de nuevos equipos de codificación y sus redes conectadas en la red en su totalidad es necesario, por lo tanto, realizar con cada uno de los otros equipos de codificación el protocolo de descubrimiento del IPsec. Debido a ello se aumenta el coste potencial de señalización de toda la red con O (N^2).

[0017] Además del coste, para identificar los equipos terminales rojos en su propia red, es necesario ejecutar también el protocolo de descubrimiento del IPsec cuando se produce un cambio en la red. Según se ha descrito, al producirse un cambio en la red es necesario modificar la identificación de red, por lo que también se modifica la dirección completa del equipo de codificación. Con ello en la nueva red ya no se pueden identificar los equipos terminales conectados con el equipo de codificación, por lo que se ha de ejecutar de nuevo con cada equipo de codificación adicional de la nueva red el protocolo de descubrimiento del IPsec para que todos conozcan mutuamente las asignaciones confidenciales correspondientes y con ello también las redes rojas a las que se han conectado los equipos terminales.

[0018] Esta acción resulta especialmente crítica en las redes radioeléctricas. En un entorno con recursos radioeléctricos limitados es especialmente importante el mayor coste de señalización que conlleva el protocolo de descubrimiento del IPsec, particularmente en un entorno altamente dinámico en el que se modifica con frecuencia la topología. Además, especialmente en entornos radioeléctricos se puede producir un cambio frecuente de red de equipos individuales, es decir de equipos de codificación junto con equipos terminales. La cantidad de pasadas del protocolo de descubrimiento del IPsec necesarias para ello puede representar otra carga para los recursos radioeléctricos, por lo que ya puede no ser posible una comunicación oportuna de aplicaciones en el modo de codificación de túnel en entornos radioeléctricos puesto que el tráfico de datos de señalización ha aumentado enormemente.

[0019] El objetivo de la invención consiste, por lo tanto, en proporcionar un procedimiento y un sistema para la comunicación segura que permita una alta seguridad de los datos y disponibilidad del sistema con un coste de señalización reducido.

[0020] En lo que respecta al procedimiento, dicho objetivo se alcanza gracias a las características de la reivindicación 1, y en lo tocante al sistema, gracias a las características de la reivindicación 15. Las reivindicaciones dependientes se refieren a perfeccionamientos ventajosos del procedimiento conforme con la invención o del sistema conforme con la invención.

[0021] La invención propone un procedimiento eficiente para la obtención de informaciones actuales de encaminamiento, a partir de asignaciones unívocas entre direcciones rojas de red e identificaciones negras de equipos. Estas asignaciones pueden describirse, por ejemplo, con funciones claras o mediante una tabla de consulta. Este procedimiento evita largos intercambios a cargo de los recursos de mensajes de señalización y sobre el encaminamiento para la obtención de la topología roja actual de red y las correspondientes informaciones de encaminamiento. Estas informaciones pueden deducirse directamente de la topología de red negra conocida con ayuda de una asignación clara de identificaciones negras de equipos con direcciones rojas de red. Si se conoce un equipo con su identificación negra de equipo en la red negra, se puede deducir de inmediato la red roja conectada con este usuario a través de la asignación.

[0022] El concepto de tablas de consulta utiliza una tabla configurada de momento en el campo preliminar y archivada en el equipo de codificación para la asignación entre identificaciones negras de equipos y redes rojas. Mediante la aplicación del procedimiento conforme con la invención, es posible renunciar a la utilización del protocolo de descubrimiento del IPsec y se puede evitar el tráfico de señalización necesario para el intercambio de informaciones de ruta entre las redes rojas de los usuarios. Particularmente en entornos con recursos radioeléctricos limitados, es posible aumentar claramente la posibilidad de utilización de la red radioeléctrica.

[0023] A continuación se describe un ejemplo de realización de la invención, haciendo referencia a las figuras. Las figuras muestran:

La figura 1 el modo de transporte y de túnel con IPsec;

La figura 2 la topología de una red utilizando el modo túnel de IPsec:

La figura 3 el esquema de direccionamiento en redes IP;

La figura 4 el diagrama de flujo del protocolo de descubrimiento de IPsec;

La figura 5 la tabla de consulta situada en el equipo de codificación para la correlación entre direcciones negras y rojas.

La figura 6 la estructura interna del equipo de codificación con la tabla de consulta.

La figura 7 el modo túnel, dentro de una red confidencial y

La figura 8 un ejemplo de realización del sistema conforme con la invención para el direccionamiento y encaminamiento en relaciones de comunicación codificadas.

[0024] Debido a la separación del nivel rojo de la red confidencial (que se denominará en adelante, y de forma abreviada, nivel rojo de red) del nivel negro de la red pública (que se denominará en adelante, y de forma abreviada, nivel negro de red) por el equipo de codificación 4 es necesario reproducir en primer lugar la topología de red en las

tablas de encaminamiento 17 de los dispositivos de encaminamiento (routers) correspondientes en los dos niveles de red mutuamente independientes. Puesto que la tabla negra de encaminamiento 17 contiene en principio toda la información sobre los usuarios de la red pública negra 2, es posible reducir también los mensajes de señalización en el lado rojo confidencial mediante la utilización de estas informaciones. Esto se puede conseguir a través de la introducción de una asignación unívoca que describe una relación entre la identificación negra y pública del equipo y las direcciones de redes rojas (8) y confidenciales. Esta reproducción describe las redes rojas que están conectadas con el lado negro a través de un equipo de codificación con una determinada identificación negra de equipo. El conocimiento de la accesibilidad de equipos con una identificación negra individual de equipos permite, por lo tanto, obtener informaciones sobre las redes rojas conectadas.

[0025] Este concepto se puede realizar, por ejemplo, a través de tablas configuradas previamente en todos los equipos de codificación 4 presentes, o mediante una reproducción clara, por ejemplo una función matemática. Como base para la instrucción de correspondencia se utiliza una identificación negra unívoca de un equipo. Entre los ejemplos de tales identificaciones de equipo se encuentran las direcciones de control de acceso al medio (MAC) o identificadores de anfitrión (Host-IDs) de acuerdo con el protocolo IPv6.

[0026] En las direcciones públicas negras resulta una imagen diferente. Todos los usuarios han de utilizar la misma identificación de red dentro de una red 2 negra pública. Con un cambio de la red se modifica esta identificación de red. Por lo tanto, la identificación negra de la red pública no resulta adecuada para la identificación de un equipo de codificación 4. Sin embargo, una identificación unívoca de equipo, por ejemplo la ID de interfaz del IPv6 basada en la dirección MAC de 48 bits, permite una identificación del equipo de codificación 4 en un entorno cualquiera de red.

[0027] De este modo se puede identificar la red conectada en el lado rojo 3 con ayuda de la identificación negra de equipo. La figura 5 representa la relación entre las partes negras – no confidenciales – y rojas – confidenciales - de las direcciones 8 con ayuda de un ejemplo. Debido a los requisitos de seguridad para el equipo de codificación 4, las informaciones de la tabla de consulta 6 o de la tabla de encaminamiento 17 nunca pueden difundirse en la red pública negra, sino que solamente pueden analizarse dentro del equipo de codificación 4.

[0028] Debido a ello es necesario configurar previamente las informaciones necesarias para la estructuración de la tabla en cada equipo de codificación 4 antes de la puesta en servicio. Debido a la movilidad de los equipos de codificación 4 junto con sus redes correspondientes, por ejemplo en una red radioeléctrica, y la incorporación a diferentes redes regionales, puede aumentar el número de datos registrados en la tabla. De este modo es necesario prever la suficiente memoria en el equipo de codificación para poder incorporar las tablas.

[0029] Con una entrada adicional en la tabla de consulta 6 pueden identificarse y darse a conocer otras redes rojas confidenciales 3 conectadas con un equipo de codificación 4. Esto es en la figura 5, por ejemplo, la red w conectada al dispositivo de encaminamiento (router) R6.

[0030] Normalmente, se tiene acceso a otras redes a través de transiciones de red NÜ dentro de la propia red. Las direcciones de las transiciones de red se dan a conocer aquí dentro de la red con ayuda de un protocolo. Así, cada usuario puede reconocer directamente las transiciones de red con ayuda de las correspondientes direcciones negras, no confidenciales. Sin embargo, si una transición de red queda posicionada dentro de la red roja 3 confidencial de un equipo de codificación, no es posible realizar una señalización simple de la dirección. Este problema se evita mediante una información adicional recogida dentro de la tabla de consulta 6 referente al equipo de codificación 4 responsable de la transición de red. Con ello sobra una señalización adicional para la detección de la transición de red. Por lo tanto es posible, sin que ello represente problema alguno, llevar a cabo la estructuración de un túnel hacia estos usuarios importantes de la red.

[0031] El concepto de utilización de tablas de consulta 6 permite también, además de evitar un gran tráfico de señalizaciones dentro de la red, mantener una consistencia actualizada de las redes 2, 3 negras, públicas, y rojas, confidenciales. En cuando el protocolo de encaminamiento negro reconoce que no tiene acceso a un usuario en la red negra 2, es posible señalar esta circunstancia al equipo de codificación. Esto, a su vez, permite deducir con ayuda de la tabla que la dirección 8 del usuario sin acceso es roja y confidencial. Con ello se puede actualizar directamente la tabla de encaminamiento 17 del equipo terminal rojo. Por lo tanto, se pueden rechazar directamente los paquetes de datos en el dispositivo de encaminamiento (router) rojo. Por lo tanto, se puede renunciar por completo a un intercambio de informaciones de encaminamiento entre las redes rojas conectadas con los diferentes equipos de codificación. La red roja 3 confidencial reconoce automáticamente después de un corto período de tiempo la topología básica de la red negra pública 2.

[0032] Después de describir la estructura de principio de la tabla de consulta 6 se pretende describir a continuación, a grosso modo, el desarrollo del procesamiento de datos y obtención de informaciones con ayuda de la tabla de consulta 6.

[0033] La figura 6 muestra la estructura esquemática del equipo de codificación 4. El lado público negro 2 del equipo de codificación 4 recibe continuamente informaciones de encaminamiento, es decir informaciones de red 18 desde el nivel negro público 2 de la red. El proceso de gestión 19, alojado en la tabla de consulta, puede identificar las correspondientes redes rojas confidenciales conectadas con ayuda de las identificaciones intercambiadas de

equipos públicos negros de los otros equipos de codificación 4. Estas informaciones de red 18 son transmitidas por el proceso de gestión 19 al nivel rojo confidencial 3. El equipo de codificación 4 recibe con ello informaciones sobre la accesibilidad de otras redes rojas 3 conectadas.

[0034] Los dispositivos de encaminamiento (routers) rojos confidenciales 17 pueden así reconocer de inmediato todas las redes rojas 3 potencialmente accesibles. La topología del nivel público negro 2 es reproducida de forma actualizada en la topología de la red roja 3. Así, por un lado, se puede ahorrar un gran coste de señalización y, por el otro lado, se puede reconocer inmediatamente una inaccesibilidad de un equipo de codificación en especial y, en su caso, reaccionar de modo adecuado. Un proceso de codificación 20, alojado en el equipo de codificación, se encarga de decodificar los paquetes de datos en la dirección del nivel rojo confidencial 3 y de codificarlos en la dirección del nivel negro 2.

[0035] La segunda ventaja de este procedimiento se deriva de la codificación de datos rojos confidenciales del nivel rojo confidencial. El proceso de codificación 20 puede deducir con ayuda de la tabla de consulta 6, de forma inmediata, el equipo de decodificación correspondiente del equipo destinatario final. Se puede omitir la costosa pasada del protocolo de descubrimiento del IPsec. En la medida en la que el equipo de codificación está registrado en la tabla de consulta 6 y conectado con la red, se puede codificar y transmitir el flujo de datos prácticamente sin retardo.

[0036] Con el fin de minimizar el tamaño de las tablas de consulta 6, las redes rojas confidenciales 3 conectadas con el equipo de codificación 4 pueden utilizar un direccionamiento jerárquico. Esto significa que las direcciones de todos los equipos terminales provienen de la misma área de direcciones, aún cuando haya dispositivos de encaminamiento (routers) adicionales que separan las diferentes redes. Así se puede evitar la necesidad de varias entradas de tabla para un equipo de codificación, como se muestra en la figura 5. Con el direccionamiento jerárquico se pueden agrupar todos los equipos terminales conectados de un equipo de codificación 4 bajo una sola entrada de dirección 8 y registrarla en la tabla de consulta 6.

[0037] Adicionalmente es posible un intercambio periódico de las tablas de consulta 6 entre equipos de codificación. Para este fin, un equipo de codificación 4 ha de generar un túnel a prueba de escuchas con otro equipo de codificación 4. A través del mismo se puede ajustar entonces la tabla 6. La ventaja consiste en que pueden introducirse aún modificaciones en la configuración de la tabla 6 durante el tiempo de funcionamiento del equipo de codificación 4. De este modo, el equipo de codificación 4 puede, por ejemplo, distribuir direcciones de red rojas confidenciales adicionales en la pasarela 21. Además, se puede minimizar el coste de configuración necesario antes de la puesta en servicio puesto que las informaciones de la tabla de consulta 6 se pueden hacer accesibles aún incluso durante el funcionamiento.

[0038] La señalización necesaria durante la pasada del protocolo de descubrimiento de IPsec, es significativa. Especialmente, en los entornos de radio con una velocidad de datos limitada se reduce aún más la capacidad de transmisión disponible. Mediante la utilización de la tabla de consulta 6 previamente configurada en los equipos de codificación 4 se puede omitir por completo la utilización del protocolo de descubrimiento IPsec. Las redes rojas confidenciales conectadas 3 pueden deducirse después de un corto intervalo a partir de la topología de las redes negras 2 no confidenciales, con ayuda de la tabla de consulta 6. Así se reduce aún más el derroche de recursos de red, ya que el equipo emisor o el equipo de codificación 4 reconocen la no accesibilidad de equipos de codificación y de las redes rojas conectadas a los mismos.

[0039] Si, además se utiliza un direccionamiento jerárquico de las redes rojas confidenciales 10, se pueden reducir aun más el tamaño de las tablas de consulta 6 necesarias. Con el intercambio de las tablas 6 entre diferentes equipos de codificación 4 es posible, además, llevar a cabo otro ajuste durante su funcionamiento. De este modo se puede reducir claramente el coste de configuración antes de la puesta en marcha, puesto que no es necesario configurar previamente todas las entradas.

[0040] La figura 7 muestra el modo de túnel entre dos redes rojas confidenciales 3 aplicándose el procedimiento conforme con la invención para el direccionamiento y encaminamiento de relaciones de comunicación codificadas 1. Las relaciones de comunicación o las comunicaciones entre dos usuarios finales se extienden a dos niveles de red 2, 3 diferentes y mutuamente separados, donde también se distinguen los niveles de encaminamiento correspondientes a los niveles de red 2, 3. La delimitación de estos dos niveles de red 2, 3 con sus niveles de encaminamiento se realiza a través de un equipo de codificación 4, el cual está conectado tanto con el primer nivel de red 2, que es una red negra, públicamente accesible e insegura, como con el segundo nivel de red rojo, el cual no es públicamente accesible.

[0041] En los dos niveles de encaminamiento se averigua respectivamente una topología actual de red, donde dicha averiguación de la topología de red de un nivel de red 2, 3 se realiza independientemente de la averiguación de la topología de red del segundo nivel de red 3, 2, que se utiliza para la comunicación confidencial protegida hacia el exterior y se almacena en las correspondientes tablas de encaminamiento 17. Está previsto, dentro de los equipos de codificación 4 existentes en la totalidad de la red, una interfaz 7 con una asignación clara de direcciones 8 del segundo nivel de encaminamiento a las direcciones 8 del primer nivel de encaminamiento, de modo que sea posible

encontrar el recorrido incluso sobrepasando los límites de los dos niveles de red 2, 3. Esto también puede verse en la figura 2.

[0042] El primer nivel de red 2 es un área pública, como por ejemplo, la red fija, o una parte de una red radiotelefonía móvil que funciona a nivel mundial, por ejemplo la red UMTS o GSM, y el segundo nivel de red 3 es un área confidencial, como por ejemplo redes de empresa protegidas hacia el exterior o similares, donde también se subdividen las correspondientes direcciones 8 de los niveles de encaminamiento en direcciones públicas 8 y en direcciones confidenciales 8.

[0043] En el propio equipo de codificación 4 se ha previsto una tabla de consulta 6 que se puede actualizar durante el funcionamiento de la red, la cual se configura previamente. La interfaz 7 funciona como transición controlada entre el nivel público y el nivel confidencial de la red 2, 3 y, por lo tanto, también funciona como límite entre el nivel de encaminamiento público y confidencial.

[0044] La figura 8 muestra un ejemplo de realización del sistema 11 conforme con la invención para direccionamiento y encaminamiento en relaciones de comunicación 1 codificadas en su totalidad dentro de una red, al menos con dos diferentes niveles de red independientes 1, 3. El nivel de red negro 2 queda aquí delimitado frente a un segundo nivel de red 3, al menos a través de un equipo de codificación. La topología de red de ambos niveles de red se almacena en las áreas separadas 1, 13 del sistema 11 conforme con la invención, en las tablas de encaminamiento del dispositivo de encaminamiento (router) 17.

[0045] Entre estas áreas 12, 13 se ha previsto una entidad de protocolo 14 como área intermedia 15, donde la entidad de protocolo 14 tiene respectivamente un itinerario de comunicación 16 bidireccional hasta una de las dos áreas 12, 13 y se ha ejecutado, por ejemplo, según la norma del protocolo IPsec. El primer nivel de red 2 se ha definido como un área pública 2 dentro de una red completa y corresponde a una red 2 de acceso público, como por ejemplo, una red fija o una red de radiotelefonía móvil. El segundo nivel de red 3, situado dentro de una red completa se ha previsto como un área confidencial y corresponde, por ejemplo, a una red 3 protegida no pública, como por ejemplo una red de empresa o una red logística. Puede establecerse una diferenciación entre las direcciones de los correspondientes niveles de red 2, 3 ó los correspondientes niveles de encaminamiento, como direcciones públicas y direcciones confidenciales 8.

[0046] La entidad de protocolo 14 tiene conectado un dispositivo de encaminamiento (router) 17 tanto en el lado no codificado 12 como también en el lado codificado 13, en el ejemplo de realización conforme a la norma del protocolo IPv6, donde el dispositivo de encaminamiento (router) 17 comprende también una tabla de encaminamiento.

[0047] El dispositivo de encaminamiento (router) 17 del lado codificado 12 del sistema conforme a la invención 11 está conectado a una red pública 2 a través de un procedimiento definido de transmisión de modo que se puede establecer con la misma una conexión de comunicación, puesto que el procedimiento de transmisión ejecutado es compatible con el procedimiento de transmisión de la red pública 2.

[0048] Además en el ejemplo de realización se ha implementado un protocolo MANET en el lado codificado 13 y un protocolo IGP en el lado no codificado 12 para la actualización de las correspondientes tablas de encaminamiento 6, habiéndose previsto como IGP un algoritmo OSPF. Se ha previsto una transmisión no codificada de datos de información de IP, como por ejemplo, lenguaje o imágenes digitalizadas, a una red confidencial 3 sin acceso público, a través del dispositivo de encaminamiento (router) 17 Ipv6 situado en el lado no codificado del sistema conforme a la invención 11.

[0049] La invención no se limita al ejemplo de realización que se ha descrito. Todas las características descritas o representadas en los dibujos pueden combinarse opcionalmente dentro del marco de la invención.

REIVINDICACIONES

1. Procedimiento para direccionamiento y encaminamiento en relaciones de comunicación codificadas (1) en una red que dispone de, al menos, dos niveles de red (2, 3) diferentes mutuamente separados con diferentes niveles de encaminamiento,

delimitándose respectivamente un primer nivel de red (2) con el correspondiente primer nivel de encaminamiento a través de, al menos, un equipo de codificación (4) frente a un segundo nivel de red (3) con un segundo nivel de encaminamiento,

donde se averigua, al menos en los dos niveles de encaminamiento mutuamente independientes, una topología de red de ambos niveles de red (2, 3) que se almacena en las correspondientes tablas de encaminamiento (17), y

donde una interfaz (7) ubicada, al menos, en el equipo de codificación (4) está provista de una asignación de direcciones (8) unívoca del segundo nivel de encaminamiento a direcciones (8) del primer nivel de encaminamiento.

2. Procedimiento según la reivindicación 1, caracterizado porque el primer nivel de red (2) es una red (9) de acceso público e insegura.

3. Procedimiento según la reivindicación 1 ó 2, caracterizado porque el segundo nivel de red (3) es una red sin acceso público destinada a comunicaciones confidenciales protegidas hacia el exterior.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque el primer nivel de red (2) es un área pública y el segundo nivel de red (3) es un área confidencial y porque las direcciones (8) del primer nivel de encaminamiento se identifican como direcciones públicas y las direcciones (8) del segundo nivel de encaminamiento se identifican como direcciones confidenciales.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque la interfaz (7) entre un nivel de red público y un nivel de red confidencial (2, 3) o respectivamente entre un nivel de encaminamiento público y un nivel de encaminamiento confidencial, se almacena en tablas de consulta (6) del equipo de codificación (4) antes de la puesta en funcionamiento.

6. Procedimiento según la reivindicación 5 caracterizado porque las tablas de consulta (6) del equipo de codificación (4) se modifican durante el funcionamiento de una red.

7. Procedimiento según la reivindicación 5 ó 6, caracterizado porque se realiza una actualización de una tabla confidencial de encaminamiento con ayuda de las tablas de consulta (6) del equipo de codificación (4) a partir de informaciones, localmente disponibles, temporalmente variables del nivel de red público (2).

8. Procedimiento según la reivindicación 7, caracterizado porque la instrucción de correspondencia para asignación de direcciones (8) confidenciales a direcciones (8) públicas, se genera de modo independiente de la integración del equipo de codificación (4) dentro una red global.

9. Procedimiento según una de las reivindicaciones 5 a 7, caracterizado porque las tablas de consulta (6) se configuran previamente en todos los equipos de codificación (4) a utilizar, como realización de una función que describe una relación entre las direcciones (8) públicas y confidenciales.

10. Procedimiento según una de las reivindicaciones 5 a 7, caracterizado porque las tablas de consulta (6) se actualizan dinámicamente durante el funcionamiento de la red en todos los equipos de codificación (4) a utilizar, como realización de una función que describe una relación entre las direcciones (8) públicas y confidenciales.

11. Procedimiento según una de las reivindicaciones 5 a 7, caracterizado porque el contenido de las tablas de consulta (6) se distribuye exclusivamente dentro del área confidencial (3), como realización de una función que describe la relación entre las direcciones (8) públicas y confidenciales.

12. Procedimiento según una de las reivindicaciones 5 a 7 ó 9 a 11 caracterizado porque opcionalmente en las tablas de consulta (6) se ejecuta una entrada adicional que da a conocer otras redes confidenciales conectadas a un equipo de codificación (4).

13. Procedimiento según la reivindicación 7 ó 8, caracterizado porque una base para la instrucción de correspondencia la constituye una identificación de equipo unívoca correspondiente con un equipo conectado a la red.

14. Procedimiento según la reivindicación 13, caracterizado porque la identificación del equipo se diseña como una dirección de control de acceso al medio (MAC) o un identificador de anfitrión (Host-Id) conforme al protocolo Ipv6.

15. Sistema (11) para direccionamiento y encaminamiento en relaciones de comunicación codificadas (1) dentro de una red con menos, al menos, dos niveles (2, 3) de red diferentes, mutuamente separados, y los correspondientes niveles de encaminamiento,

donde se delimita respectivamente un primer nivel de red (2) con el correspondiente primer nivel de encaminamiento a través de, al menos, un equipo de codificación (4) frente a un segundo nivel de red (3) con un segundo nivel de encaminamiento,

donde la topología de red de ambos niveles de red (2, 3) se archiva en áreas separadas (12, 13) del sistema y

donde se ha previsto un área intermedia (15) dispuesta entre las áreas (12, 13) independientes como entidad de protocolo (14) con dos itinerarios de comunicación (16) bidireccionales.

16. Sistema según la reivindicación 15, caracterizado porque como primer nivel de red (2) que se define como área pública, está prevista una red parcial de acceso público.

17. Sistema según la reivindicación 15 ó 16, caracterizado porque como segundo nivel de red (3) que se define como área confidencial, está prevista una red parcial no pública protegida.

18. Sistema según una de las reivindicaciones 15 a 17, caracterizado porque las direcciones (8) del primer nivel de encaminamiento como direcciones públicas y las direcciones (8) del segundo nivel de encaminamiento como direcciones confidenciales, pueden diferenciarse mutuamente de manera respectiva.

19. Sistema según una de las reivindicaciones 15 a 18, caracterizado porque la entidad de protocolo (14) se implementa en el área intermedia de acuerdo con la norma IPsec u otro procedimiento de codificación.

20. Sistema según una de las reivindicaciones 15 a 19, caracterizado porque la entidad de protocolo (14) tiene conectado respectivamente un dispositivo de encaminamiento (router) (17) que incluye una tabla de encaminamiento (17) tanto en un lado sin codificar en una primera área (12) como en un lado codificado en una segunda área (13).

21. Sistema según una de las reivindicaciones 15 a 20, caracterizado porque el dispositivo de encaminamiento (router) (17) establece un enlace de comunicación con una red pública (2) en el lado codificado (13) mediante un procedimiento definido de transmisión.

22. Sistema según la reivindicación 21, caracterizado porque el procedimiento de transmisión es compatible con una red pública (2).

23. Sistema según una de las reivindicaciones 15 a 22, caracterizado porque se ha instalado un protocolo MANET en el lado codificado (13) para actualización de las correspondientes tablas de encaminamiento (17).

24. Sistema según una de las reivindicaciones 15 a 23, caracterizado porque se ha instalado un protocolo IGP (Protocolo de Pasarela Interior) en el lado no codificado (12).

25. Sistema según la reivindicación 24, caracterizado porque para actualización de las correspondientes tablas de encaminamiento (6), se ha instalado un algoritmo de OSPF (primer trayecto más corto abierto) del protocolo IGP.

26. Sistema según la reivindicación 20, caracterizado porque se ha previsto una transmisión no codificada de datos útiles a través del dispositivo de encaminamiento (router) (17) del lado no codificado (12) hacia una red (3) confidencial sin acceso público.

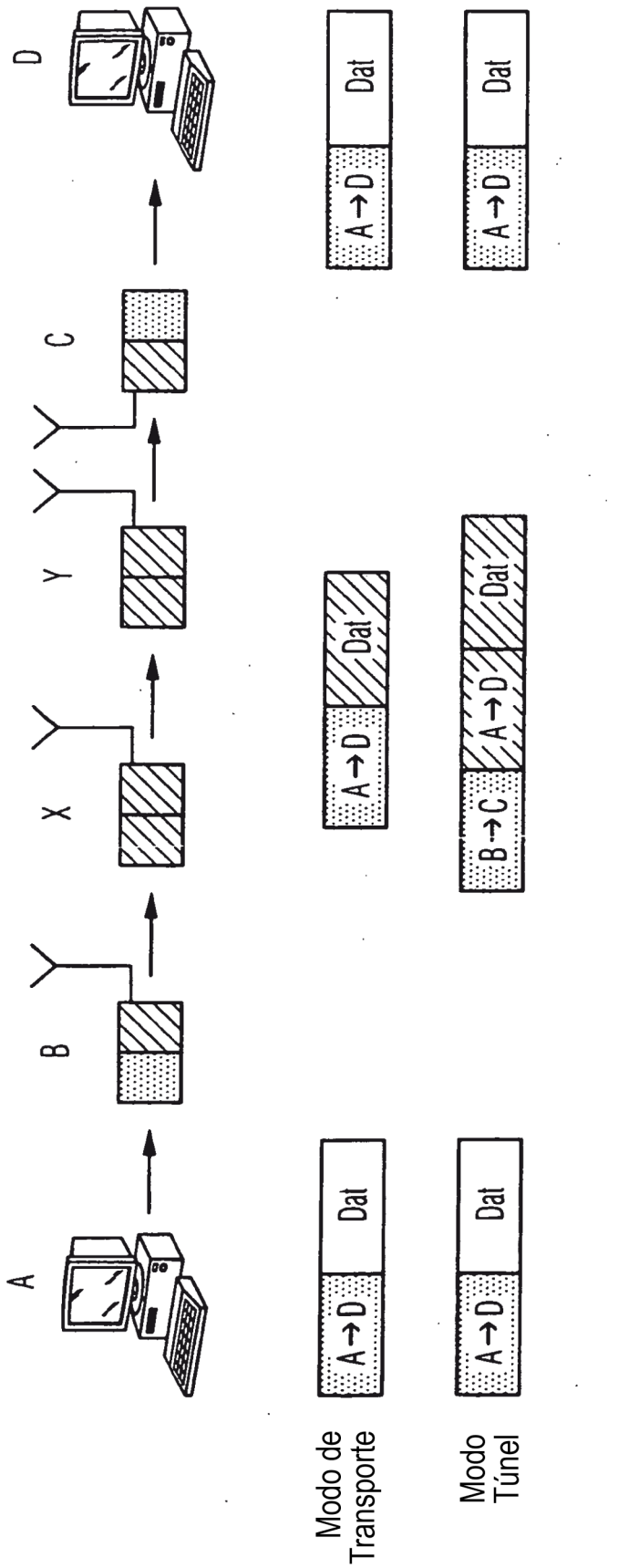

Fig. 1

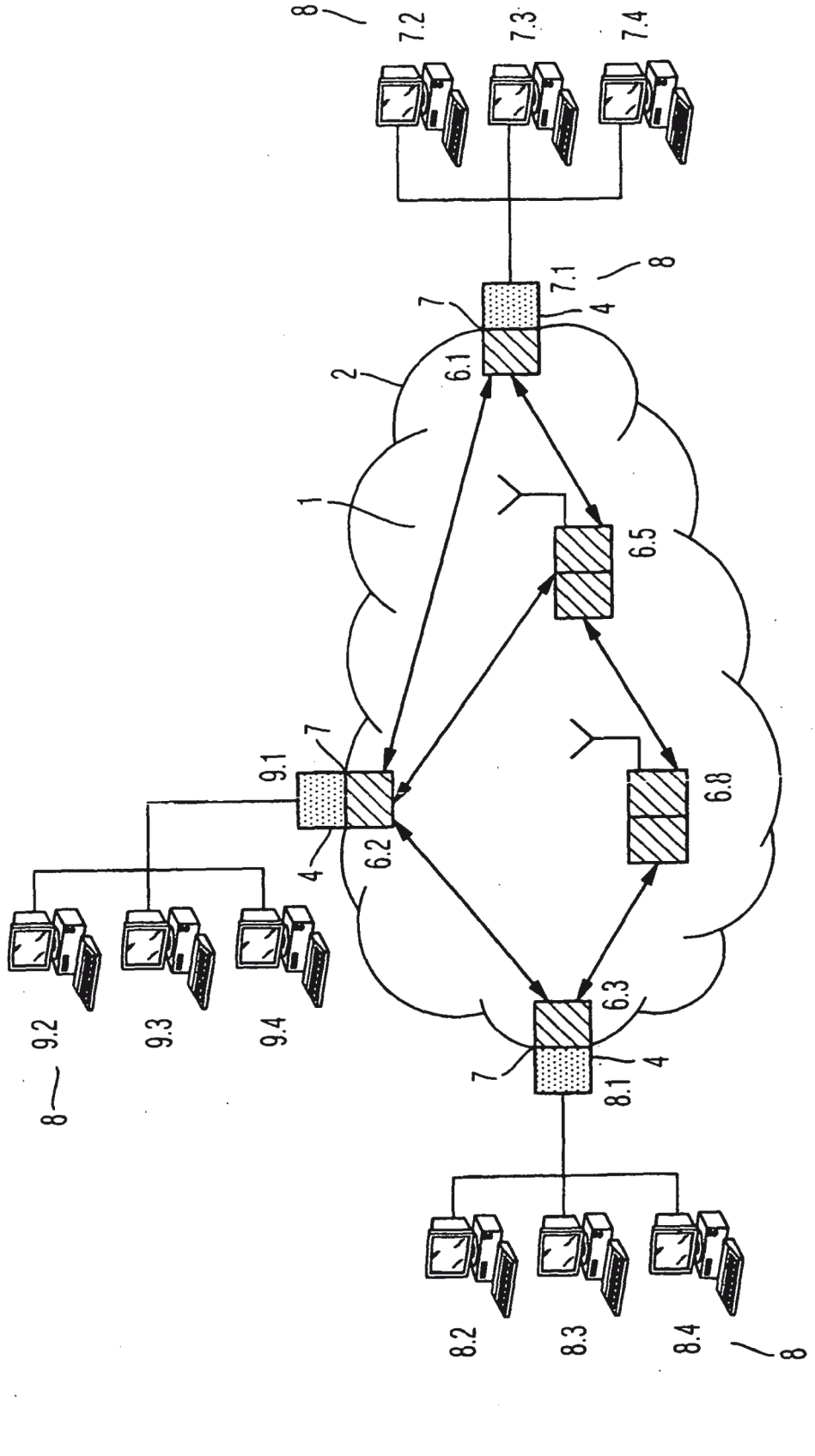
8
7.2
7.3
7.4
8
7.1
7
4
6.1
2
1
6.5
9.1
7
6.8
4
6.2
6.3
9.2
9.3
9.4
8
7
8.1
4
8.2
8.3
8.4
8

Fig. 2

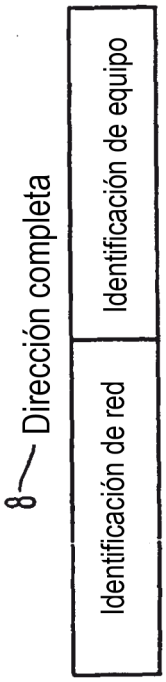
8
Dirección completa
Identificación de red
Identificación de equipo

Fig. 3

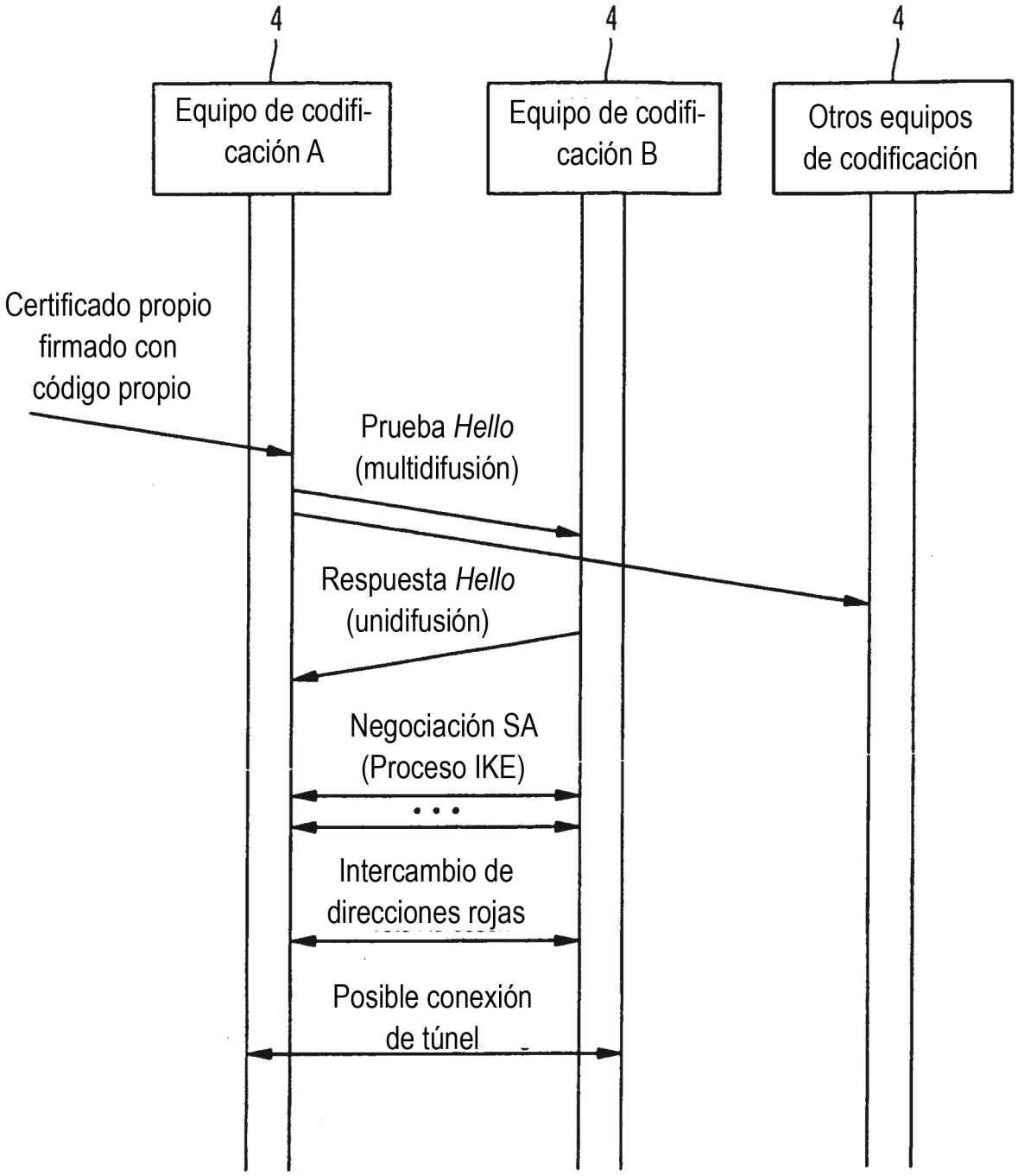
4
4
4
Equipo de codifi-
cación A
Equipo de codifi-
cación B
Otros equipos
de codificación
Certificado propio
firmado con
código propio
Prueba *Hello*
(multidifusión)
Respuesta *Hello*
(unidifusión)
Negociación SA
(Proceso IKE)
• • •
Intercambio de
direcciones rojas
Posible conexión
de túnel

Fig. 4

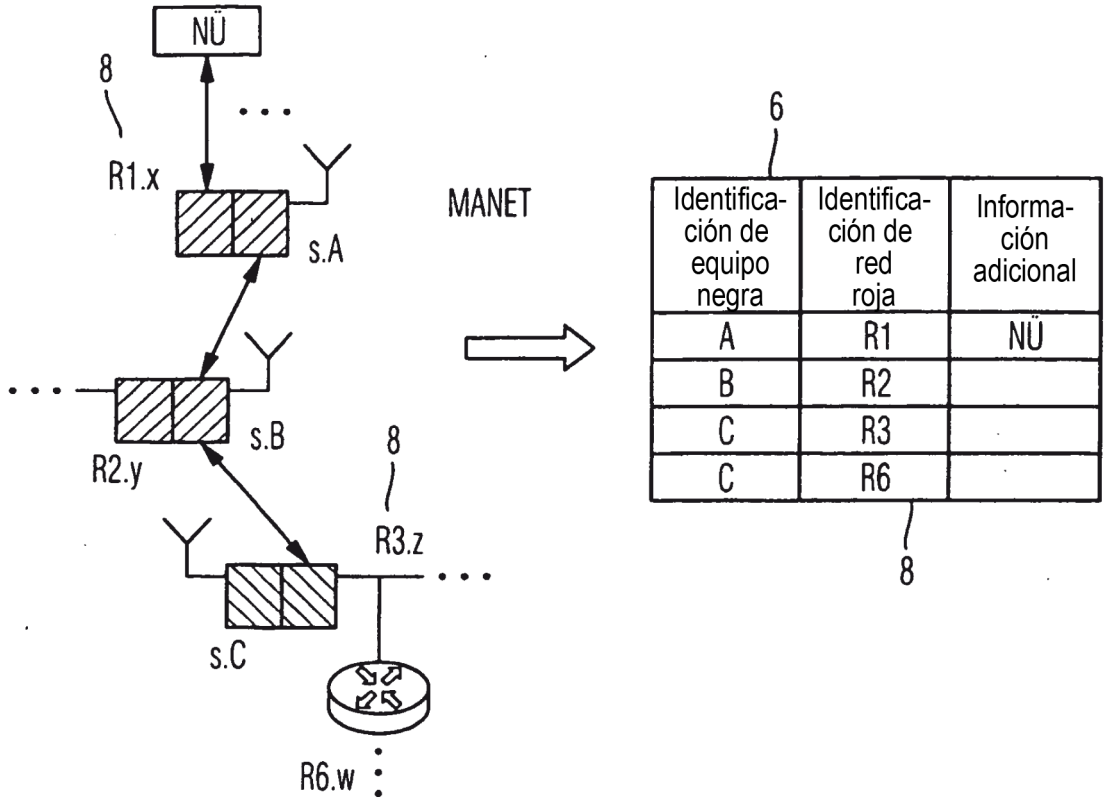
NÜ
8
R1.x
s.A
MANET
s.B
R2.y
8
R3.z
s.C
R6.w
6
Identificación de equipo negra
Identificación de red roja
Información adicional
A
R1
NÜ
B
R2
C
R3
C
R6
8

Fig. 5

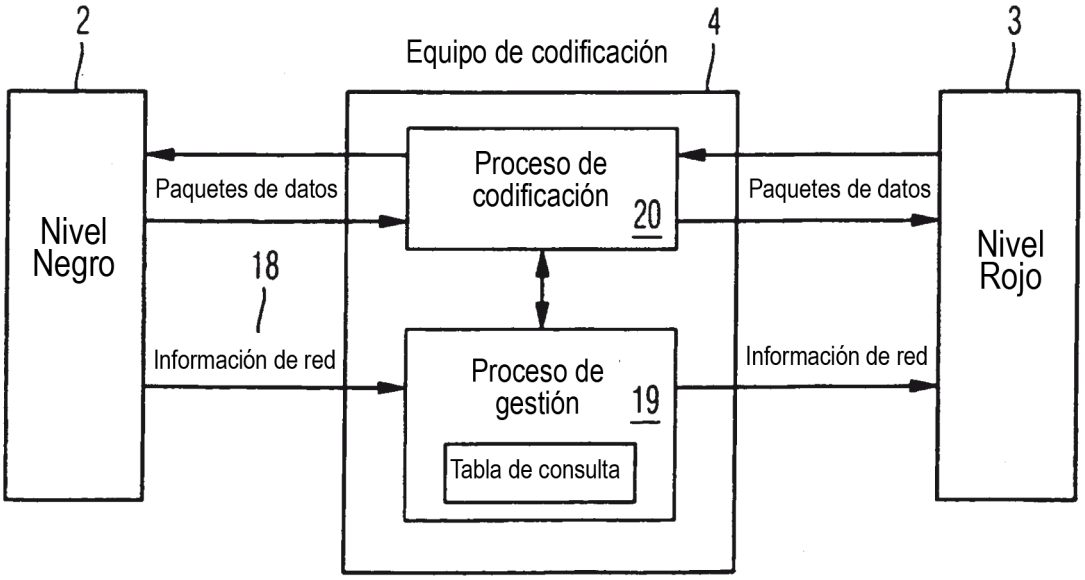
2
Nivel Negro
Equipo de codificación
4
3
Nivel Rojo
Paquetes de datos
Proceso de codificación
20
Paquetes de datos
18
Información de red
Proceso de gestión
19
Tabla de consulta
Información de red

Fig. 6

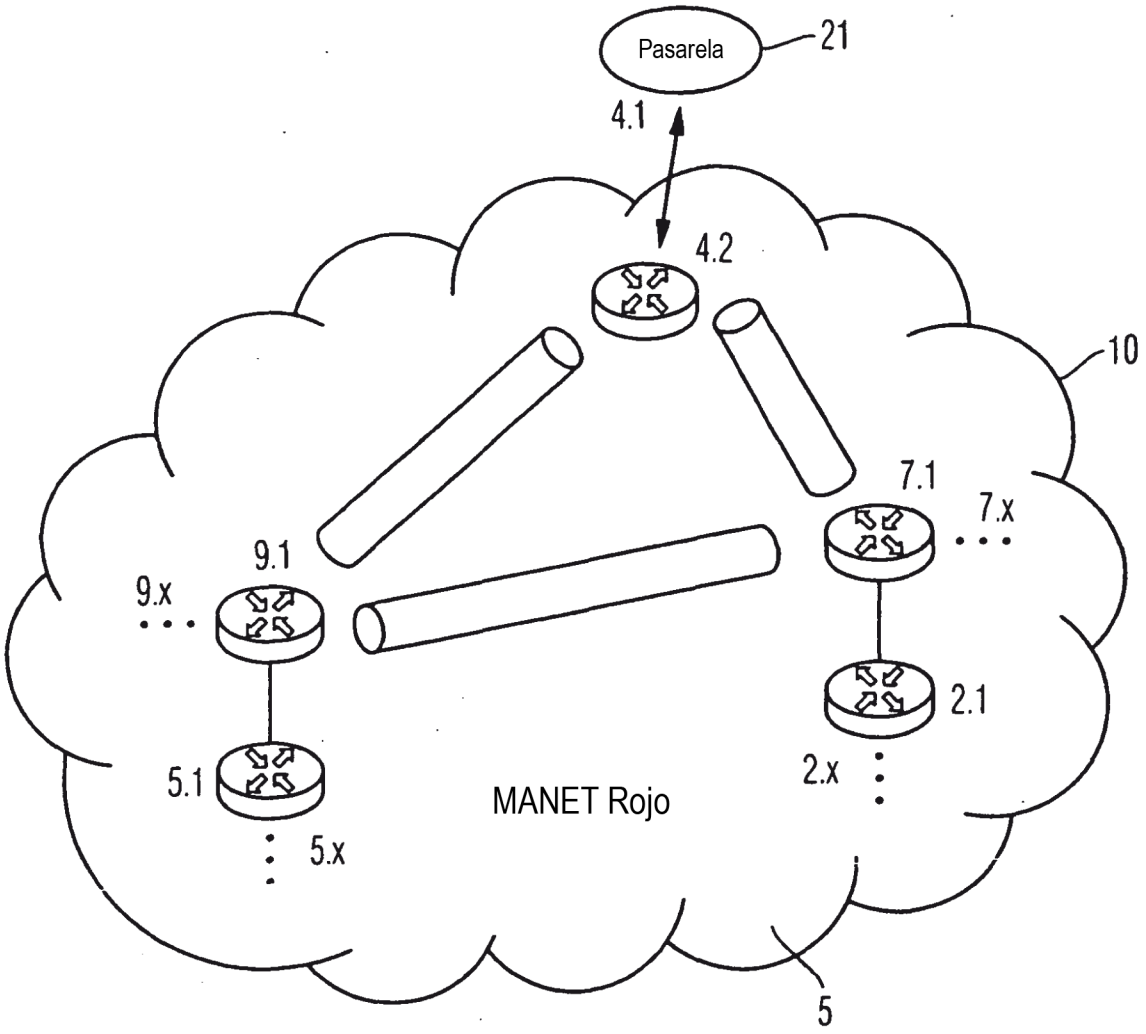

Fig. 7

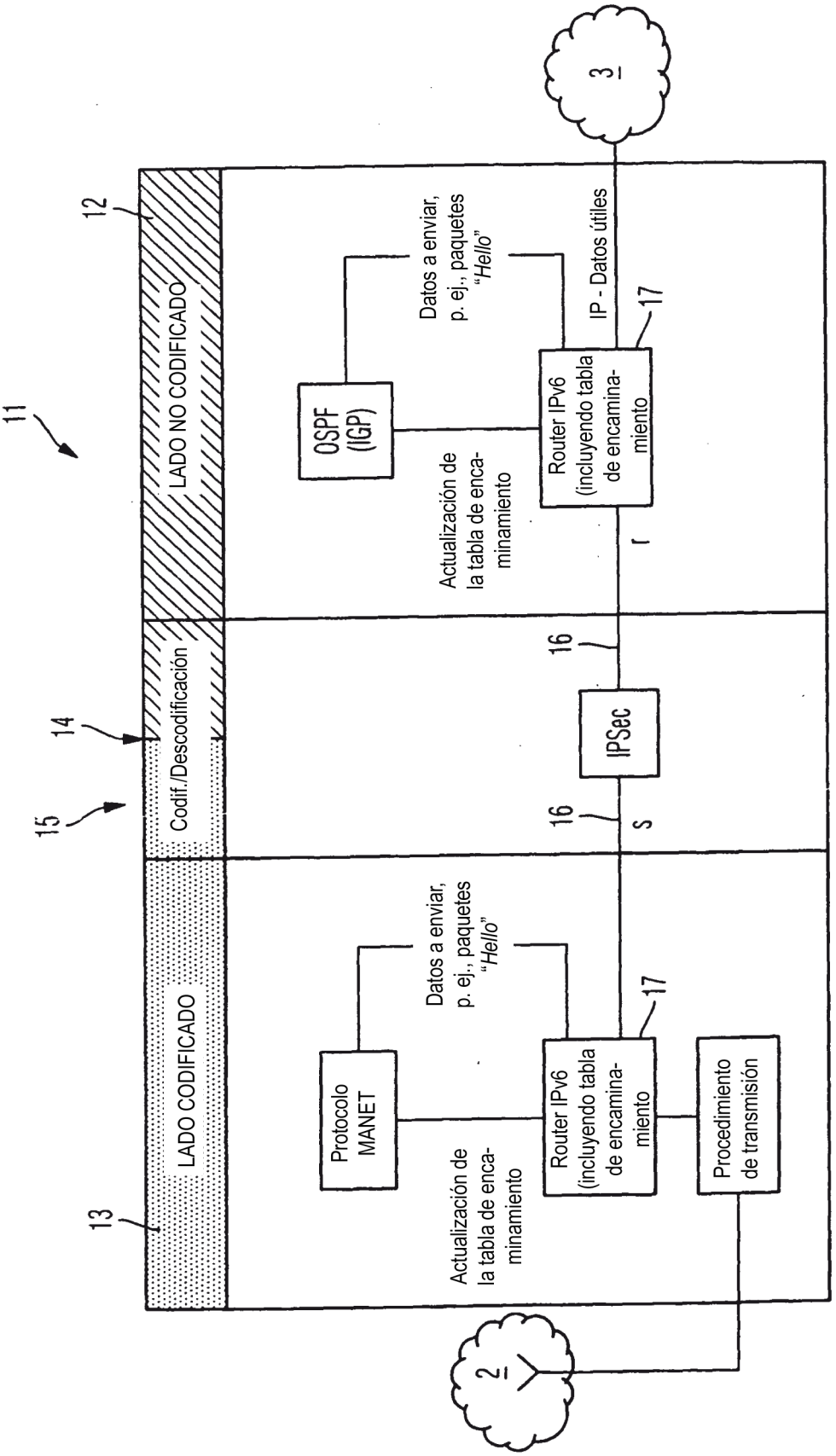
11
12
LADO NO CODIFICADO
Codif./Descodificación
LADO CODIFICADO
13
14
15
OSPF (IGP)
Datos a enviar, p. ej., paquetes "Hello"
Actualización de la tabla de encaminamiento
Router IPv6 (incluyendo tabla de encaminamiento
IP - Datos útiles
17
r
16
IPSec
16
s
Protocolo MANET
Datos a enviar, p. ej., paquetes "Hello"
Actualización de la tabla de encaminamiento
Router IPv6 (incluyendo tabla de encaminamiento
17
Procedimiento de transmisión
2
3
Datos útiles y de protocolo

Fig. 8

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citado en la descripción

• US 2005091482 A1 **[0005]**

Bibliografía de patentes citada en la descripción

• **S. KENT ; K. SEO.** Security Architecture for the Internet Protocol. *IETF RFC 4301,* Dezember 2005 **[0002]**