(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 552 675**

(21) Número de solicitud: 201430822

(51) Int. CI.:

H04W 12/06 (2009.01)
G06F 21/00 (2013.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

29.05.2014

(43) Fecha de publicación de la solicitud:

01.12.2015

(71) Solicitantes:

TECTECO SECURITY SYSTEMS, S.L. (100.0%)
Avda. Leguario, 49, planta 2, oficina 3
28981 Parla (Madrid) ES

(72) Inventor/es:

ENRIQUE SALPICO, José Antonio

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Método de enrutamiento con seguridad y autentificación a nivel de tramas**

(57) Resumen:

Método de enrutamiento con seguridad y autentificación a nivel de tramas.

Se da a conocer un método de enrutamiento para ser implementado en el firmware de un enrutador que proporciona una mayor seguridad a bajo coste ya que funciona, sustancialmente, a nivel de la capa 2 del modelo OSI. El enrutador descrito incorpora diversos niveles de seguridad en el que comprende una primera etapa (1) de detección de direcciones MAC (10), una segunda etapa (2) de autorización de direcciones MAC (10), una tercera etapa (3) de autorizaciones de usuarios para dicha dirección MAC y protecciones de más alto nivel opcionales como, por ejemplo, una cuarta etapa (3) de restricciones horarias, una quinta etapa (5) de restricciones adicionales tales como bloqueo de puertos, protocolos, páginas web, entre otros.

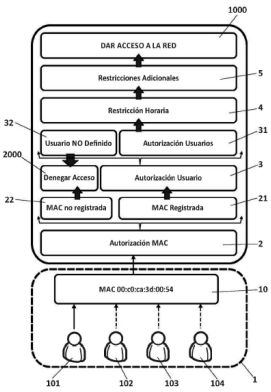

FIG. 1

ES 2 552 675 A1

MÉTODO DE ENRUTAMIENTO CON SEGURIDAD Y AUTENTIFICACIÓN A NIVEL DE TRAMAS

D E S C R I P C I Ó N

OBJETO DE LA INVENCIÓN

La presente invención da a conocer un método de enrutamiento de señales en una red de datos. Más específicamente, la presente invención da a conocer un método de enrutamiento que incorpora mejoras de seguridad a nivel de tramas (capa 2 del modelo OSI, por las siglas de la expresión inglesa “Open System Interconnection”, en español “Sistema de Interconexión Abierto”).

ANTECEDENTES DE LA INVENCIÓN

Son conocidos en la técnica diversos métodos de enrutamiento de señales e, incluso, algunos de dichos mecanismos incorporan complejos algoritmos de seguridad para que la interconexión entre los dispositivos de una red sea únicamente para los usuarios que deberían formar parte de la misma.

Habitualmente, dicha identificación de usuarios se realiza a nivel de la capa 3 del modelo OSI, es decir, mediante direcciones IP (por las siglas de la expresión inglesa “Internet Protocol”, en español “Protocolo de Internet”) o en capas superiores a esta. Por tanto, los dispositivos encargados del enrutamiento y la previa identificación de seguridad, deben contar con dispositivos capaces de interpretar, como mínimo, datos a nivel de la capa 3 del modelo OSI.

Además, la identificación a partir de direcciones IP resulta insuficiente para garantizar la identificación de un usuario en cuanto a que cualquier usuario mediante un dispositivo cualquiera puede configurar su dirección IP sin necesidad de tener un conocimiento extensivo en redes de ordenadores. Esto hace que las direcciones IP sean fácilmente suplantables.

Para solucionar estos problemas de la técnica anterior, se han desarrollado diversos métodos de comunicación para mejorar la seguridad de los enrutadores existentes. En particular, el documento EP1170925 da a conocer un método de comunicación entre dispositivos que utiliza

vectores de acceso almacenados en una tabla de direcciones en el que los vectores comprenden datos indicativos de si la dirección MAC (por las siglas de la expresión en inglés “Media Access Control”, en español “Control de Acceso al Medio”) de un nodo puede comunicarse con la dirección MAC de otro. En definitiva, este documento da a conocer un método que detecta si un nodo tiene permiso para enviar información a otro en base a las direcciones MAC de ambos nodos pero no da a conocer la posibilidad de utilizar estas direcciones MAC para acceder a una red determinada.

Por otra parte, el documento US8316438 da a conocer un sistema en el que un ordenador personal, que dispone de una dirección MAC determinada, al enviar datos a un Gateway pasan por un adaptador de red que determina los permisos para transmisión de información para dicho ordenador portátil y realiza el bloqueo de dicha señal o, por el contrario, permite la transferencia de datos. Por tanto, este documento da a conocer que es posible disponer de un adaptador de red intermedio de bajo coste que funciona en la capa 2 del modelo OSI para filtrar la entrada de usuarios a la red. Sin embargo, entre otros problemas, la red requeriría la incorporación de múltiples adaptadores de red para efectuar este filtrado y la configuración de un nuevo usuario requeriría reconfigurar todos los adaptadores de red del sistema, lo que hace que el sistema sea poco práctico. Además, bastaría con hacerse con un ordenador cuya dirección MAC esté incorporada en los adaptadores de red para acceder a la misma.

DESCRIPCIÓN DE LA INVENCIÓN

Por tanto, existe una necesidad de incorporar un sistema de seguridad que, por una parte, represente un bajo coste computacional y, por otra, aumente la seguridad de las redes bloqueando los usuarios no autorizados y permitiendo que dicha tabla de usuarios se pueda actualizar fácilmente.

La presente invención da a conocer un método de enrutamiento que se puede incorporar en el enrutador mediante su firmware y que, al funcionar a nivel de la capa 2 del modelo OSI representa un bajo coste computacional y permite mejorar ostensiblemente las prestaciones de los enrutadores actuales sin necesidad de modificar las redes existentes añadiendo nuevo hardware.

La presente invención da a conocer un método de enrutamiento de señales en un enrutador

que comprende:

- medios de conexión a una serie de dispositivos;
- una tabla de direcciones de usuarios permitidos; y
- una tabla de autorización de usuarios;

en el que la tabla de direcciones de usuarios permitidos comprende direcciones MAC de dispositivos con permiso de acceso a la red, y en el que la tabla de autorización de usuarios comprende una serie de datos de identificación de usuarios permitidos relacionados a, al menos una, dirección MAC y que comprende las etapas de:

a) determinar la dirección MAC del dispositivo que se pretende conectar al enrutador;
b) identificar si la dirección MAC determinada en la etapa a) está en la tabla de direcciones de usuarios permitidos; y
c) otorgar un nivel de acceso a la red;

en el que si en la etapa b) se identifica que la dirección MAC está en la tabla de direcciones de usuarios permitidos, se inicia una etapa b1) de lectura de los datos de identificación de usuarios permitidos para dicha dirección MAC a partir de la tabla de autorización de usuarios y un etapa b2) de identificación del usuario en la que se solicitan al dispositivo datos de identificación de usuario y compara dichos datos de identificación de usuario con los datos leídos en la etapa b1).

En cuanto a los niveles de acceso, la presente invención contempla tres niveles principales: un primer nivel de denegación de acceso en el que se impide completamente el acceso a la red; un segundo nivel de autorización parcial en el que se otorga acceso a, al menos, parte de la red, por ejemplo únicamente a intranet; y un tercer nivel en el que se otorga acceso total a la red. Sin embargo, en el ámbito de la presente invención se pueden incorporar otros tipos de niveles sin alejarse del ámbito de protección de la presente invención.

Preferentemente, la presente invención contempla que si, en la etapa b), se identifica que la dirección MAC no corresponde a ninguna de las direcciones de la tabla de direcciones de usuarios permitidos, en la etapa c) se deniega el acceso a la red.

Preferentemente, si en la etapa b) se identifica que la dirección MAC corresponde a una de las direcciones de la tabla de direcciones de usuarios permitidos y en la etapa b2) se identifica que datos de identificación de usuario corresponden con uno de los datos de identificación leídos en

la etapa b1), en la etapa c) se otorga acceso a, al menos, parte de la red.

Además, en el determinado caso en que la dirección MAC del equipo no corresponda con ninguna de las direcciones dispuestas en la tabla de direcciones de usuarios permitidos o que los datos de identificación del usuario leídos en la etapa b1) no correspondan con los datos de identificación de usuarios permitidos almacenados en la tabla de autorización de usuarios para la dirección MAC del usuario, en la etapa c) se otorga un acceso restringido a la red o, incluso, se podría denegar el acceso (2000) a la red.

En cuanto al acceso restringido a la red, este acceso restringido se puede interpretar, particularmente, como únicamente la recepción de datos, únicamente el acceso a intranet (por ejemplo, para conectarse con impresoras, escáner, etc.) y/o únicamente para envío de datos sin recepción de los mismos.

Adicionalmente, el enrutador puede comprender una variable de control adicional que se basa en una tabla de restricciones y una etapa e) en la que para al menos uno de los usuarios de la tabla de autorización de usuarios, se disponen unas restricciones de acceso. Dichas restricciones pueden ser, por ejemplo, una restricción de acceso horario en las que, en la etapa c) se permite acceso a la red, una restricción a páginas web en las que, en la etapa c) se deniega acceso a al menos una página web, una restricción de protocolos, en la que en la etapa c) se deniega la comunicación mediante, al menos un, protocolo (por ejemplo, el protocolo FTP, cuyas siglas provienen de la expresión en inglés “File Transfer Protocol”), una restricción de puertos, en la que en la etapa c) se deniega la comunicación mediante, al menos un, puerto, etc.

Por otra parte, la presente invención también se refiere a un enrutador que ejecuta un método de enrutamiento del tipo explicado anteriormente.

DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo

siguiente:

La figura 1 muestra una vista esquemática de un flujo de comunicaciones en una realización preferente de la presente invención.

La figura 2 muestra un diagrama de flujo que indica el funcionamiento de un método de enrutamiento según la presente invención.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

La figura 1 muestra una realización preferente de la presente invención. En particular, la figura 1 muestra una primera realización en la que el enrutador se encuentra conectado a una serie de dispositivos usuarios (101, 102, 103, 104), disponiendo cada uno de dichos dispositivos usuarios (101, 102, 103, 104) una dirección MAC.

Inicialmente, el enrutador de la figura 1 detecta, en una primera etapa (1) la dirección MAC (10) del dispositivo activo (101), esto es, uno de los dispositivos de la serie de dispositivos usuarios (101, 102, 103, 104) que pretende hacer uso de la red. Posteriormente, en una segunda etapa (2) realiza una autorización de la dirección MAC (10) del dispositivo activo (101), es decir, determina si la dirección MAC (10) de dicho dispositivo corresponde con alguna de las direcciones MAC almacenadas en una tabla de direcciones de usuarios permitidos del enrutador. Si se realiza la autorización MAC (21), es decir, se determina que la dirección MAC (10) del dispositivo corresponde con alguna de las direcciones almacenadas en el enrutador, entonces se procede a dar paso a una tercera etapa (3) en la que se realiza una autorización de usuario. En caso contrario, se deniega el acceso (2000).

En dicha tercera etapa (3) se pretende identificar al usuario que está haciendo uso del equipo autorizado para entrar a la red, sin embargo, en realizaciones particulares de la presente invención, esta autorización no es necesaria para todas las direcciones MAC de los dispositivos usuarios en cuanto a que habrá dispositivos como, por ejemplo, impresoras, fax, escáner, etc. para los que no hace falta realizar esta autorización de usuario.

Sin embargo, la presente invención contempla que el enrutador comprende una tabla de autorización de usuarios en la que, para al menos una de las direcciones MAC almacenadas

en la tabla de direcciones de usuarios permitidos, se dispone de al menos un nombre de usuario y una contraseña para identificar, además del equipo que se conecta a la red, al usuario que está haciendo uso de ese equipo.

De manera que si se ha realizado la identificación del usuario (31), se procede a una cuarta etapa (4) de restricción horaria y, en caso de una identificación incorrecta (31) se procede a denegar el acceso (2000) a la red.

En cuanto a la cuarta etapa (4) de restricción horaria, la realización de la figura 1 contempla que para al menos uno de los usuarios exista un parámetro de restricción horaria que puede ser implementado como un parámetro adicional de la tabla de autorización de usuarios o como una tabla independiente de restricciones horarias.

Esta restricción horaria pretende que, en el enrutador, se disponga de permisos determinados para cada uno de los usuarios, por ejemplo, uno de los usuarios debe tener acceso únicamente durante parte de la jornada laboral a ciertos recursos como impresoras, etc. para organizar el trabajo en una oficina o, en otro ejemplo, se puede disponer de un control infantil de manera que si se accede con la contraseña de un usuario infantil solo se tiene acceso a internet hasta una hora determinada y, una vez se excede dicha hora, se tiene un acceso restringido a los recursos. En el caso del control infantil, este acceso restringido a recursos puede ser, por ejemplo, que no se tiene acceso a internet pero sí a los recursos de la red interna tales como impresoras, escáner, etc.

Adicionalmente, la presente invención contempla que, además de la restricción horaria, el método de la presente invención permite incorporar mecanismos adicionales de restricción como, por ejemplo, una quinta etapa (5) en la que se disponen restricciones adicionales, tales como, restringir el acceso mediante ciertos puertos, protocolos de comunicación, a ciertas páginas web, entre otros.

Una vez se ha definido el nivel de acceso para el usuario y si se determina que no dispone de restricción alguna se le puede otorgar acceso a la red (1000). En caso contrario, se deniega el acceso (2000)

La figura 2 muestra un diagrama de flujo de una segunda realización de la presente

invención.

En dicha realización, se dispone una primera etapa (1) de entrada de datos, en esta caso, se disponen como entradas al diagrama de flujo la dirección MAC del dispositivo que pretende conectarse a la red, y datos de configuración que comprenden una tabla de direcciones de usuarios permitidos, una tabla de autorización de usuarios y, en este ejemplo particular, se dispone una tabla de restricción horaria y una tabla de restricciones adicionales.

Una vez se detectan los datos de entrada, se procede a una segunda etapa (2) de autorización MAC en la que se determina si la dirección MAC de la primera etapa (1) corresponde con una de las direcciones MAC de la tabla de direcciones de usuarios permitidos. Si dicha dirección MAC corresponde a una de las direcciones almacenadas en la tabla de direcciones de usuarios permitidos, mediante un primer operador de decisión (200), la dirección MAC corresponde (202) con una de las direcciones almacenadas, se procede a una tercera etapa (3) de autorización de usuarios. Si se determina que la no-correspondencia (201) de la dirección MAC con las direcciones almacenadas, se procede a denegar el acceso (2000) a la red.

En la tercera etapa (3) se procede a realizar la autorización del usuario, es decir, se realiza al usuario una interrogación de un par nombre de usuario-contraseña. Posteriormente, si el par nombre de usuario-contraseña corresponden con los almacenados en la tabla de autorización de usuarios para dicha dirección MAC se determina la autenticación (303) del usuario y, de lo contrario, se determina que no se ha autenticado un usuario autorizado y se puede proceder de dos maneras diferentes, una primera forma de actuación (301) en la que se da acceso restringido (3000) al usuario, por ejemplo, únicamente a intranet y, una segunda forma de actuación (302) en la que procede a denegar el acceso (2000) a la red por no-autenticación.

Tras la autenticación (303) del usuario se procede a determinar si para dicho usuario se ha definido alguna restricción horaria mediante una cuarta etapa (4). De allí mediante un operador lógico de decisión se determina que es un usuario con restricción horaria para lo que se puede escoger una primera actuación (401) denegando el acceso o una segunda actuación (402) otorgando un acceso restringido (3000) al usuario.

Si se determina que es un usuario sin restricción horaria se procede a autorizar (403) el acceso sin restricciones horarias para el usuario.

Finalmente, la presente invención contempla una quinta etapa (5) de restricciones adicionales en la que se determina si para dicho usuario hay restricciones adicionales. Si se determina la existencia de una restricción adicional (501) se otorga acceso restringido (3000) al usuario y si es un usuario para el cual se ha determinado la no-existencia de restricciones adicionales (502) se otorga acceso a la red (1000).

Con el fin de otorgar mayor claridad a la presente descripción, la definición de acceso restringido (3000) a la red se refiere a que existe un bloqueo parcial (301), por ejemplo, se otorga acceso únicamente a internet, se deniega el acceso a protocolos determinados (por ejemplo, FTP), se deniega el acceso a determinadas páginas web, se bloquean ciertos puertos, etc. Adicionalmente, cuando se menciona que se deniega el acceso (2000) se refiere a que se realiza un bloqueo total (2001) impidiendo la comunicación del usuario, tanto con los dispositivos de la red, como con una red externa tal como internet.

REIVINDICACIONES

1. Método de enrutamiento de señales en un enrutador que comprende:

- medios de conexión a una serie de dispositivos (101, 102, 103, 104);
- una tabla de direcciones de usuarios permitidos; y
- una tabla de autorización de usuarios;

en el que la tabla de direcciones de usuarios permitidos comprende direcciones MAC (10) de dispositivos con permiso de acceso a la red caracterizado porque la tabla de autorización de usuarios comprende una serie de datos de identificación de usuarios permitidos relacionados a, al menos una, dirección MAC (10) y porque comprende las etapas de:

a) determinar la dirección MAC (10) del dispositivo que se pretende conectar al enrutador;
b) identificar si la dirección MAC (10) determinada en la etapa a) está en la tabla de direcciones de usuarios permitidos; y
c) otorgar o denegar un nivel de acceso a la red;

en el que si en la etapa b) se identifica que la dirección MAC (10) está en la tabla de direcciones de usuarios permitidos, se inicia una etapa b1) de lectura de los datos de identificación de usuarios permitidos para dicha dirección MAC (10) a partir de la tabla de autorización de usuarios y un etapa b2) de identificación del usuario en la que se solicitan al dispositivo datos de identificación de usuario y compara dichos datos de identificación de usuario con los datos leídos en la etapa b1).

2. Método, según la reivindicación 1, caracterizado porque si, en la etapa b), se identifica que la dirección MAC (10) no corresponde a ninguna de las direcciones de la tabla de direcciones de usuarios permitidos, en la etapa c) se deniega el acceso (2000) a la red.

3. Método, según la reivindicación 1, caracterizado porque, si en la etapa b) se identifica que la dirección MAC (10) corresponde a una de las direcciones de la tabla de direcciones de usuarios permitidos y en la etapa b2) se identifica que datos de identificación de usuario corresponden con uno de los datos de identificación leídos en la etapa b1), en la etapa c) se otorga acceso a, al menos, parte de la red

4. Método, según la reivindicación 1, caracterizado porque en la etapa c) se otorga un acceso restringido (3000) a la red.

5. Método, según la reivindicación 4, caracterizado porque el acceso restringido (3000) a la red comprende únicamente la recepción de datos.

6. Método, según la reivindicación 1, caracterizado porque el enrutador comprende una tabla de restricciones y porque comprende una etapa e) en la que para al menos uno de los usuarios de la tabla de autorización de usuarios, se disponen unas restricciones de acceso.

7. Método, según la reivindicación 6, caracterizado porque dichas restricciones comprenden una restricción de acceso horario en las que, en la etapa c) se otorga acceso (1000) a la red.

8. Método, según la reivindicación 6, caracterizado porque dichas restricciones comprenden una restricción a páginas web en las que, en la etapa c) se deniega acceso a al menos una página web.

9. Método, según la reivindicación 6, caracterizado porque dichas restricciones comprenden una restricción de protocolos, en la que en la etapa c) se deniega la comunicación mediante, al menos un, protocolo.

10. Método, según la reivindicación 9 caracterizado porque el al menos un protocolo es el protocolo FTP.

11. Método, según la reivindicación 6, caracterizado porque dichas restricciones comprenden una restricción de puertos, en la que en la etapa c) se deniega la comunicación mediante, al menos un, puerto.

12. Enrutador que ejecuta un método de enrutamiento según cualquiera de las reivindicaciones 1 a 11.

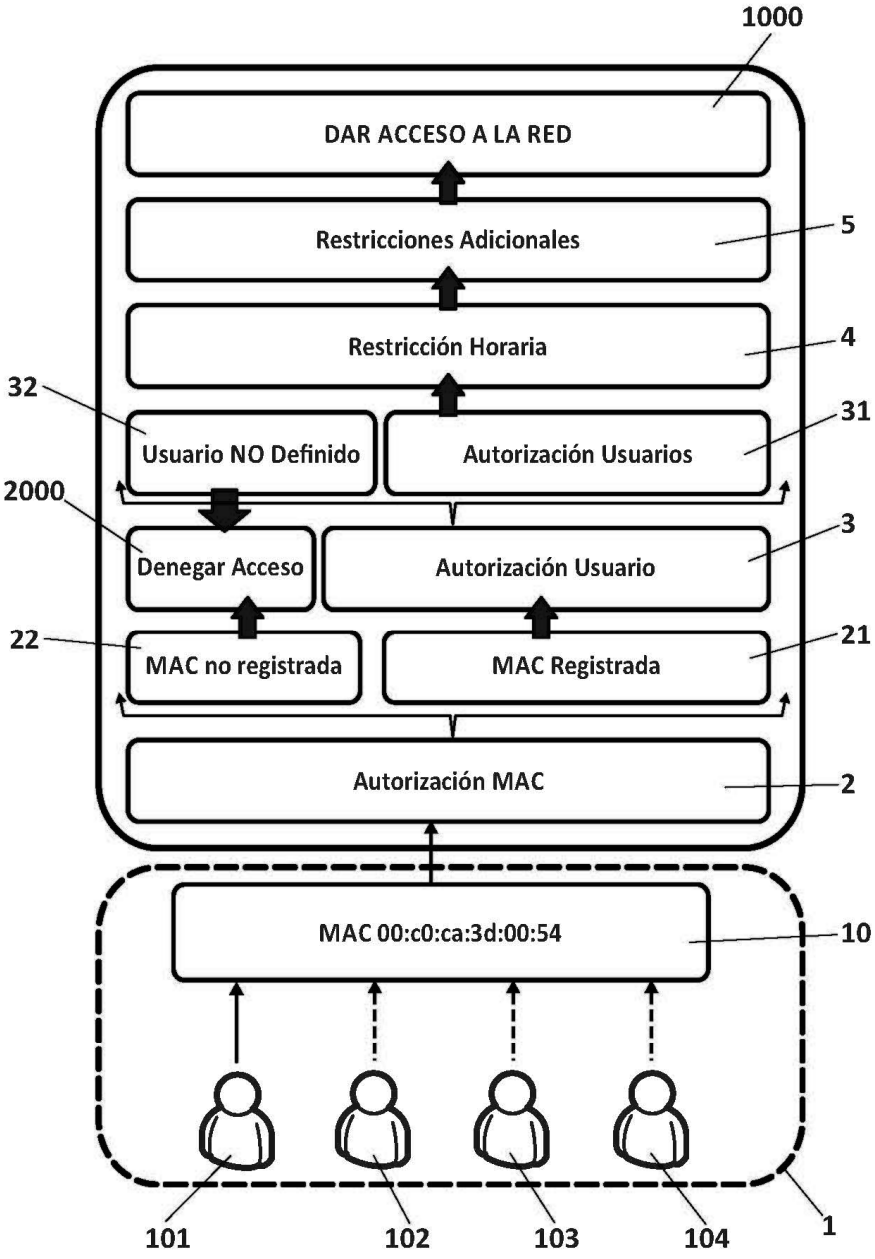
1000
DAR ACCESO A LA RED
Restricciones Adicionales
5
Restricción Horaria
4
32
Usuario NO Definido
Autorización Usuarios
31
2000
Denegar Acceso
Autorización Usuario
3
22
MAC no registrada
MAC Registrada
21
Autorización MAC
2
MAC 00:c0:ca:3d:00:54
10
101
102
103
104
1

FIG. 1

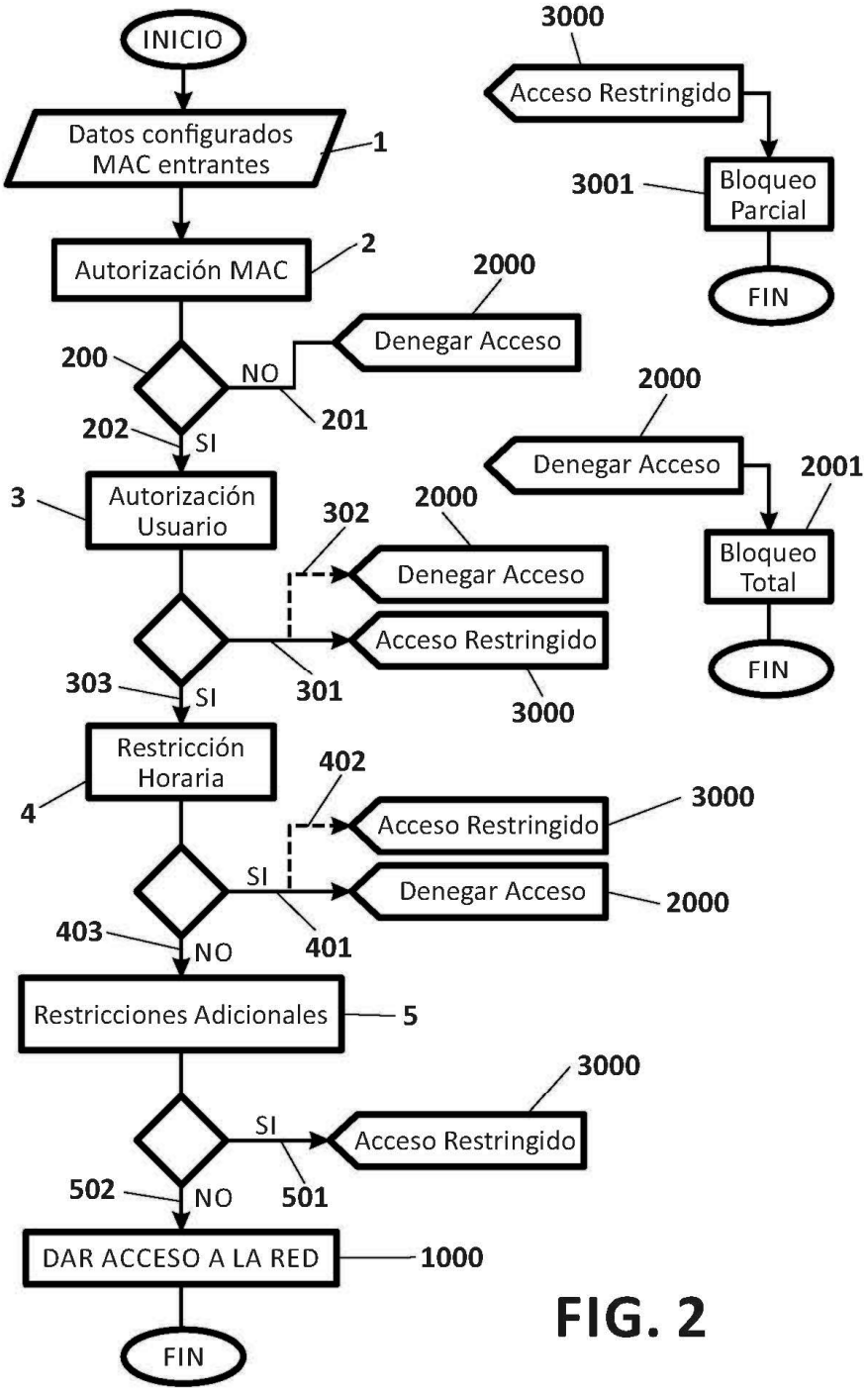
INICIO
Datos configurados MAC entrantes
1
Autorización MAC
2
200
NO
Denegar Acceso
2000
201
202
SI
3
Autorización Usuario
302
2000
Denegar Acceso
Acceso Restringido
3000
301
303
SI
4
Restricción Horaria
402
Acceso Restringido
3000
SI
Denegar Acceso
2000
401
403
NO
Restricciones Adicionales
5
3000
SI
Acceso Restringido
501
502
NO
DAR ACCESO A LA RED
1000
FIN
3000
Acceso Restringido
3001
Bloqueo Parcial
FIN
2000
Denegar Acceso
2001
Bloqueo Total
FIN

FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201430822

(22) Fecha de presentación de la solicitud: 29.05.2014

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W12/06*** (2009.01)
G06F21/00 (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2003220994 A1 (ZHU CHUNRONG) 27.11.2003, descripción: párrafos 11-15; reivindicación 4; figura 2.	1-12
A	US 2006137005 A1 (PARK CHANG-HWAN) 22.06.2006, todo el documento.	1-12
A	US 2008209071 A1 (KUBOTA MAKOTO) 28.08.2008, todo el documento.	1-12
A	US 7568092 B1 (ENGLUND PAER MARTIN) 28.07.2009, todo el documento.	1-12
A	EP 2667664 A1 (COMCAST CABLE COMM LLC) 27.11.2013, todo el documento.	1-12
A	US 7574202 B1 (TSAO ROBERT et al.) 11.08.2009, todo el documento.	1-12

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
08.09.2015	M. Muñoz Sánchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, H04W, G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 08.09.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-12	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-12	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2003220994 A1 (ZHU CHUNRONG)	27.11.2003
D02	US 2006137005 A1 (PARK CHANG-HWAN)	22.06.2006
D03	US 2008209071 A1 (KUBOTA MAKOTO)	28.08.2008
D04	US 7568092 B1 (ENGLUND PAER MARTIN)	28.07.2009
D05	EP 2667664 A1 (COMCAST CABLE COMM LLC)	27.11.2013
D06	US 7574202 B1 (TSAO ROBERT et al.)	11.08.2009

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: el documento D01 divulga un método de control de acceso a redes de ordenadores a través de un dispositivo de cómputo móvil. El control final del acceso lo lleva a cabo el servidor de administración de cuentas, de usuario, (pár. 11) que utiliza para la autenticación la dirección MAC del dispositivo que solicita acceso así como el identificador de usuario y su contraseña (pár. 12, pár. 15). Las diferencias entre el contenido técnico de la reivindicación 1 y el método divulgado en el documento D01 se refieren a detalles de implementación:

- Uno de dos tablas de datos relativas a los usuarios (direcciones y autorización)
- Comprobación secuencial de dirección MAC y de datos de identificación

La primera diferencia es una forma comúnmente conocida para establecer correspondencias entre tuplas de valores de variables resultando entonces evidente para el experto en la materia.
La segunda diferencia no supone un efecto técnico distinto a la comprobación de las 2 condiciones en otro orden (primero la información de identificación) o de forma simultánea y se considera una mera alternativa. Así esta segunda diferencia también resulta evidente para el experto en la materia.
En conclusión el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley 11/86 de patentes.

Reivindicación 12: el enrutador reivindicado (no definido explícitamente sino por su capacidad de ejecución del método reivindicado) comprendería características totalmente análogas a la combinación del servidor de administración de cuentas de usuario y la red wireless de acceso en sí (punto de acceso) del documento D01 en lo que a autenticación se refiere. Por tanto, las diferencias de implementación generales se consideran una mera traslación natural del ámbito de un servidor y punto de acceso al ámbito concreto de un enrutador siendo entonces evidentes para el experto en la materia.
En conclusión el documento D01 afecta a la actividad inventiva de la reivindicación 12 según el art. 8.1 de la Ley 11/86 de patentes.

Reivindicaciones dependientes

Reivindicaciones 2-11: las restricciones reivindicadas impuestas a un dispositivo con acceso parcial a la red protegida por el enrutador son algunas de las comunes aplicadas por los sistemas de control de acceso en redes de dispositivos de cómputo resultando entonces evidentes para el experto en la materia. A modo de ejemplo, en los documentos D02, D03, D04, D05 y D06 pueden observare unas cuantas.
En conclusión el documento D01 afecta a la actividad inventiva de las reivindicaciones 2-11 según el art. 8.1 de la Ley 11/86 de patentes.