(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 595 927**

(51) Int. CI.:

H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.12.2013 E 13382563 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.08.2016 EP 2890087**

(54) Título: **Sistema de notificación de dispositivos de abonados en redes de ISP**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.01.2017

(73) Titular/es:

TELEFÓNICA S.A. (100.0%)
C/ Gran Vía 28
28013 Madrid, ES

(72) Inventor/es:

PASTOR PERALES, ANTONIO AGUSTÍN;
MARTÍN GÓMEZ, GERMÁN y
GARCÍA PUERTO, M. MAR

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema de notificación de dispositivos de abonados en redes de ISP

Campo de la invención

La presente invención tiene su aplicación en el sector de las telecomunicaciones, y se refiere especialmente a mecanismos de notificaciones para abonados de un Proveedor de Servicios de Internet (ISP).

Antecedentes de la invención

Hay diferentes mecanismos que pueden ser usados por un ISP para comunicar con un abonado/cliente/usuario. La siguiente lista identifica las soluciones existentes más comunes:

- Procedimientos en línea basados en la propia red de acceso del ISP
  - Notificación al navegador de la Red, que intercepta el tráfico del HTTP e inyecta un título o página de entrada (página de inicio).
    - Notificación de Jardín Vallado, que redirige el tráfico de navegación de la Red a un portal del ISP que limita el acceso a solamente algunos dominios (portal del ISP, descarga de antivirus, etc.)
    - Mensajería instantánea
    - Correo electrónico
    - Alerta de pantalla de televisión
    - Medios Sociales: Muchas redes sociales proporcionan mensajería privada y directa a usuarios, que puede ser usada para las notificaciones
- Procedimientos fuera de línea (procedimientos analógicos o digitales, sin una relación directa con la conectividad del abonado al ISP)
    - Llamada telefónica
    - Correo postal
    - Fax
    - Servicio de Mensajes Cortos (SMS)

Sin embargo, estas técnicas de notificaciones existentes no garantizan que las notificaciones lleguen al dispositivo de usuario y sean vistas por el usuario. Más en particular:

- Correo electrónico. Es posible que la dirección de correo electrónico no sea usada por el abonado, que esté clasificada como correo no deseado (SPAM), etc.
- Llamada telefónica. Para un ISP una llamada telefónica tiene limitaciones con relación a las horas adecuadas y la disponibilidad del abonado.
- Correo postal. Las notificaciones de correo postal pueden tardar demasiado tiempo.
- Mensajería instantánea y Medios sociales. La falta de estandarización de soluciones de mensajería instantánea, e incluso de soluciones vinculadas a tipos de acceso de red (móvil o fija) aumenta la complejidad y reduce la capacidad de enviar una notificación. Además, muchos sistemas de mensajería instantánea no garantizan la entrega ni aplican mecanismos de acuse de recibo.
- Servicio de Mensajes Cortos (SMS). Como las llamadas telefónicas, tiene limitaciones en términos de tiempos aceptables, y también carece de mecanismos para confirmar que los mensajes se han leído (errores de dispositivo, falta de espacio, servicios de SMS no enviados).
- Notificación al navegador de la Red. Es necesario que el cliente use un navegador estándar de la Red. Además, la mayoría de los navegadores integran complementos para bloquear publicidad o por motivos de seguridad, que podrían interferir con el mecanismo de notificación.
- Jardín Vallado. Estas soluciones pueden afectar a otros dispositivos en el lugar de residencia/negocio, teniendo un impacto sobre el servicio (llamadas de emergencia, vigilancia, interrupción de negocio).

Además, algunos de estos sistemas de notificación plantean interrogantes al abonado respecto de la autenticidad del remitente (correo electrónico, llamadas telefónicas) que reducen el éxito de notificación y requieren un segundo mecanismo de notificación para que el abonado valide la información. Si la identidad del dispositivo de usuario al que se envía la notificación no es conocida, puede haber problemas para ver el mensaje (por ejemplo, en pequeñas pantallas, navegadores incompatibles, etc.). En general, la ausencia de inteligencia y una medida de la fiabilidad del

sistema de notificación reducen la fiabilidad de cualquiera de estos propios mecanismos de notificación.

Existen tecnologías para identificar dispositivos en base a los protocolos de red usados por los mimos. Por ejemplo:

- Huella digital: Es un procedimiento que permite la identificación de un dispositivo de red en base a su pila de comunicación. Este mecanismo identifica el sistema operativo y las aplicaciones a partir del análisis de la información que fluye a través de la red. Como su nombre sugiere, está basado en conseguir un conjunto de patrones de comportamiento observados en los paquetes que genera para formar una "huella digital" que lo identifica de manera unívoca. Usa firmas basadas en los valores de campos de cabecera presentes en paquetes de red, y en cómo se rellenan estos valores. La huella digital puede ser bien pasiva, si solo analiza tráfico existente, o bien activa, si envía tráfico al dispositivo para forzarle a generar tráfico. En la Huella Digital Activa, se envían paquetes al dispositivo y se analizan sus respuestas. En la Huella Digital Pasiva, los paquetes enviados por el dispositivo son analizados escuchando directamente la red local.

Existen otras tecnologías que permiten la identificación remota de protocolos y aplicaciones que están siendo usados por un dispositivo:

- DPI (Inspección profunda de paquete): Esta tecnología lleva a cabo una inspección completa del paquete más allá de su cabecera. El objetivo de la DPI es buscar habitualmente incumplimientos de protocolos para identificar virus, correo no deseado, intrusiones, etc., así como efectos estadísticos. El análisis del tráfico de red por la DPI se centra en la parte de datos y aplicaciones de los paquetes que circulan a través de la red, más allá de la cabecera del protocolo.
- IDS (Sistema de detección de intrusiones): Es un sistema que analiza el tráfico de red para descubrir indicaciones de ataques o intrusiones.
- Escáneres de red: Estos programas rastrean todos los puertos de un dispositivo para descubrir cuáles están abiertos y qué aplicaciones son escuchadas. Son capaces de conseguir las versiones de aplicaciones y sus posibles vulnerabilidades. Un escáner de red se aplica a un programa de ordenador que identifica nodos, protocolos y servicios de red. Esta información puede ser usada para identificar el dispositivo.

Además, muchos protocolos incluyen parámetros específicos que facilitan la identificación del tipo y versión de aplicación (Usuario-Agente en HTML, Código de Estado en SMTP, etc.).

Existen también tecnologías que permiten la conectividad entre la red del ISP y el dispositivo de usuario situado en la red de abonado:

- NAT (Traducción de Direcciones de Red): Mecanismo en tiempo real que permite al enrutador del abonado traducir las direcciones de IP internas de red del abonado a la IP pública asignada por el ISP al cliente.
- Enrutamiento de puerto: Mecanismo que permite la redirección de un puerto en un segmento de red a otro puerto. Esta tecnología hace que sea posible establecer una conexión a un dispositivo en la red interna desde el exterior.
- uPnP (Enchufar y Usar universal): Familia de protocolos de comunicación que permite que dispositivos de red descubran de manera dinámica la presencia de otros dispositivos y establezcan una conexión entre sí.
- PCP (Protocolo de Control de Puertos): Protocolo de comunicación, especificado por el documento RFC6887, que permite la comunicación con el nodo de red que proporciona el NAT para abrir o redirigir puertos.
- Redirección de la Red: También conocida como redirección de URL, es un mecanismo del protocolo HTTP para indicar a un cliente del HTTP que consulte otro URL o dirección cuando el cliente realiza la primera solicitud del HTTP. Los códigos de estado 30x realizan la redirección al nivel del protocolo HTTP.

Estas diferentes soluciones, que permiten la identificación de dispositivos de usuario y su comunicación con la red del ISP, tienen varios problemas para garantizar que las notificaciones lleguen al dispositivo de usuario.

Por ejemplo, el uso generalizado de direccionamiento privado, especificado por el documento RFC1918 y con soporte de tecnologías de NAT para proporcionar acceso a Internet a abonados, requiere el uso compartido del direccionamiento público entre los dispositivos del abonado e incluso entre abonados, y dificulta la identificación exacta del destino de la notificación. El agotamiento del direccionamiento público IPv4, haciendo que los ISP compartan las direcciones IPv4 disponibles entre abonados por una aplicación de NAT adicional, hace que sea incluso más compleja la identificación de abonados y dispositivos desde el exterior de la red local del abonado.

Por otra parte, las técnicas de huella digital que analizan tráfico de red según los parámetros de dispositivo relacionados con protocolos de red tales como DHCP, TCP, UDP, ICMP o IP, pierden eficacia y precisión cuando se usan fuera del segmento de red (LAN) donde el dispositivo de usuario está situado, tal como la red del ISP o Internet. Además, los tiempos de latencia son parámetros que permiten la categorización de Sistemas Operativos.

La recepción de notificaciones enviadas desde el exterior de la red local del abonado, usada en algunas soluciones, necesita configuraciones de red adicionales para permitir que el tráfico llegue al dispositivo, tal como la adaptación de la NAT (enrutamiento de puertos, uPnP, PCP, etc.) o el uso de Cortafuegos en el CPE (Equipo de instalaciones del cliente) del abonado. En esta situación, la solución de notificación se complica ya que implica a los dispositivos

de red intermedios y a las políticas de seguridad.

Otros ejemplos de sistemas de usuario de notificación se describen a continuación.

El documento US 2013/0046880 A1 define un mecanismo de notificación a una base de abonado del ISP en redirección de la Red. Sin embargo, no garantiza asiduidad de tráfico ni la correcta adaptación a cualquier dispositivo.

El documento US 6459913 B2 describe un sistema de alerta unificado a un abonado con diferentes procedimientos de notificación. Sin embargo, está exclusivamente basado en un perfil generado de abonado, es decir, requiere que el abonado indique qué dispositivos estarán disponibles, y sus características, así como el nivel de prioridad, según sus preferencias. Estas necesidades de nivel de prioridad no concuerdan con la fiabilidad de entrega, dado que es un juicio subjetivo del abonado.

El documento US 7243130 B2 describe un procedimiento de selección de notificación que deduce el interés y la localización del usuario basándose en información de múltiples investigaciones en contexto de uso. Sin embargo, este procedimiento no tiene en cuenta el interés del ISP porque la información llegue al abonado con la máxima garantía, lo cual no siempre concuerda con el interés del abonado (por ejemplo, el abonado no debería interesarse por una alarma debida a violaciones de acuerdos vinculantes con el ISP). Además, el procedimiento divulgado en el documento US 7243130 B2 requiere una configuración y un inventario previos, que sean capaces de deducir, basándose en el tráfico de red, qué dispositivos existen, y también necesita que se configure una investigación específica, puesto que la información del nivel de atención se obtiene de manera automática a partir de la red.

Las soluciones actuales envían a ciegas notificaciones al usuario, es decir, sin la seguridad de que la notificación ha sido recibida o vista por el abonado. Por lo tanto, hay necesidad en el estado de la técnica de un procedimiento y un sistema para enviar notificaciones a un dispositivo dentro de la red de IP de un abonado del Proveedor de Servicios de Internet, que seleccione el protocolo o el mecanismo que proporcione mayores garantías de ser recibido o percibido por el usuario.

El documento 2010/312852 A1 describe un dispositivo para procesar notificaciones de aplicaciones, a transmitir a los terminales de comunicación de los usuarios. Este dispositivo analiza la notificación de la aplicación a fin de determinar i) cómo y a qué hora debe ser transmitido el contenido de la notificación de la aplicación a un terminal del usuario, ii) qué parte del contenido debe ser usado y iii) cómo debe ser usada esa parte por el terminal. Este análisis de la notificación de la aplicación tiene en cuenta información de usuario y de contexto, parámetros de notificación de aplicaciones y características del terminal de usuario.

Sumario de la invención

La presente invención resuelve los problemas mencionados anteriormente y soluciona limitaciones de funcionamiento de la técnica anterior, explicadas anteriormente, divulgando un procedimiento y un sistema que permiten la identificación del tipo de dispositivo de abonado (usuario) a notificar, y seleccionar el protocolo de comunicación óptimo para enviar una notificación a dicho dispositivo de usuario en la red del ISP.

En una realización preferente, la presente invención permite determinar un tipo de dispositivo de usuario seleccionado a partir del ordenador, teléfono celular, tableta, televisor inteligente, etc., por no citar más que unos pocos, pero también determina la Aplicación del Sistema Operativo que se ejecuta en el dispositivo del usuario. Además, la presente invención es capaz de descubrir si el dispositivo de usuario está activo, bien de manera pasiva o de manera activa (es decir, inyectando tráfico en el segmento de red del abonado).

La presente invención selecciona y gestiona el mejor mecanismo para enviar la notificación al dispositivo de usuario determinado, basándose en la información que circula a través del segmento de red del abonado.

El procedimiento y el sistema propuestos para enviar notificaciones a abonados del ISP son capaces de decidir si las notificaciones se envían usando el mecanismo más fiable seleccionado por el procedimiento propuesto o si el envío de notificaciones se delega en la red del ISP de manera que el ISP pueda usar otros canales fuera de línea, tales como llamadas telefónicas, correo postal, etc., si el procedimiento propuesto lo considera más fiable que los mecanismos detectados.

En una posible realización de la invención, se genera un inventario de los diferentes dispositivos del abonado, y se asocia a los mejores mecanismos de notificación para cada uno de los mismos.

Un primer aspecto de la presente invención se refiere a un procedimiento para enviar notificaciones a abonados de una red de un ISP, teniendo cada abonado uno o más dispositivos conectados a al menos una red de área local de abonado, que comprende las siguientes

En un segundo aspecto de la presente invención, se divulga un sistema para enviar mensajes de notificaciones o alertas a dispositivos del abonado, que está integrado en una red del IP. El sistema está definido en la reivindicación 1.

Este sistema comprende componentes de hardware y software para gestionar alertas o notificaciones a los dispositivos de un abonado del ISP, identificar las posibles soluciones tecnológicas disponibles, analizar el tráfico de red local del abonado y seleccionar el mecanismo de entrega más adecuado para el abonado, haciéndose cargo el propio sistema de la entrega local o delegando la tarea en sistemas externos del ISP.

Un último aspecto de la presente invención se refiere a un programa de ordenador que comprende medios de código de programa de ordenador, adaptados para llevar a cabo las etapas del procedimiento descrito, cuando dicho programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en el terreno, un circuito integrado específico de la aplicación, un microprocesador, un micro-controlador o cualquier otra forma de hardware programable.

El procedimiento según los aspectos de la invención descritos anteriormente tiene una serie de ventajas respecto de la técnica anterior, que se pueden resumir como sigue:

- mayor fiabilidad en la entrega de notificaciones, puesto que la presente invención garantiza el uso de un medio/protocolo que es usado regularmente por el dispositivo,
- flexibilidad para adaptarse a las diferentes soluciones técnicas,
- inteligencia para realizar un auto-inventario de los mecanismos de notificación y establecer prioridades,
- uso del tráfico real desde el dispositivo del abonado en el algoritmo de decisión para seleccionar el mejor mecanismo de entrega de notificación,
- eficiencia de uso solamente del mecanismo adecuado, en lugar de varias tecnologías simultáneas (por ejemplo llamada telefónica más correo postal),
- ahorros de operadores, ya que los mecanismos de notificación más caros son sustituidos por procedimientos de menor coste.

Estas y otras ventajas se pondrán de manifiesto a la luz de la descripción detallada de la invención.

Descripción de los dibujos

Con el fin de ayudar a entender las características de la invención, según una realización práctica preferente de la misma y para complementar esta descripción, las siguientes figuras se añaden como parte integrante de la misma, teniendo un carácter ilustrativo y no limitativo:

la figura 1 muestra un diagrama de bloque de un sistema para enviar notificaciones a dispositivos de abonado en una red de un ISP, según una realización preferente de la invención.

La figura 2 muestra un diagrama de bloques de flujo de comunicación entre un gestor de consultas y el resto de componentes del sistema anterior, según una realización preferente de la invención.

La figura 3 muestra un diagrama de bloques del flujo de comunicación entre una base de datos de contactos y el resto de componentes del sistema anterior, según una realización preferente de la invención.

La figura 4 muestra un diagrama de bloques del flujo de comunicación entre los componentes de un detector de dispositivos en el sistema anterior y el resto de componentes de este sistema, según una realización preferente de la invención.

La figura 5 muestra un diagrama de bloques de un componente analizador del detector de dispositivos y el flujo de comunicación entre otros componentes restantes de este detector de dispositivos, según una realización preferente de la invención.

La figura 6 muestra un diagrama de bloques de un componente creador del detector de dispositivos y el flujo de comunicación entre otros componentes restantes de este detector de dispositivos, según una realización preferente de la invención.

La figura 7 muestra un diagrama de bloques del flujo de comunicación entre los componentes de un notificador en el sistema anterior y el resto de componentes de este sistema, según una realización preferente de la invención.

La figura 8 muestra un escenario de red para una aplicación del sistema que envía notificaciones de alertas a dispositivos de abonado en una red de un ISP, según un posible caso de uso de la invención.

La figura 9 muestra un escenario de red de un equipo virtual de instalaciones de cliente en la red del ISP para la aplicación del sistema que envía notificaciones de alerta a los dispositivos de abonado, según otro posible caso de uso de la invención.

La figura 10 muestra un escenario de red con diferentes tipos de dispositivos de abonado para la aplicación del sistema que envía diferentes notificaciones de alerta a cada tipo de dispositivo de abonado, según un posible caso de uso adicional de la invención.

La figura 11 muestra un escenario de red de una empresa para la aplicación del sistema que envía mensajes de notificación a los abonados, según un posible caso de uso adicional de la invención.

Realización preferente de la invención

Evidentemente, las realizaciones de la invención se pueden aplicar en varias plataformas arquitectónicas, sistemas operativos y servidores, dispositivos, sistemas o aplicaciones. Cualquier disposición o aplicación arquitectónica presentada en el presente documento está provista solo con fines ilustrativos y de comprensión, y no está destinada a limitar aspectos de la invención.

Es dentro de este contexto que las diversas realizaciones de la invención se presentan ahora con referencia a las figuras 1 a 11.

La figura 1 presenta un diagrama de bloques de la arquitectura de sistema que aplica la notificación propuesta a abonados del ISP, incluyendo sus componentes principales y la interacción entre los mismos. El sistema (111) está integrado en una red de un ISP y comprende medios para comunicar con el operador (100) de red del ISP y con la red de área local (120) a los cuales están conectados los dispositivos (121) de la red del abonado. El sistema (111) propuesto comprende, además, los siguientes componentes:

- gestor de consultas (11): recibe y distribuye las solicitudes de notificación (101) desde el operador de red (100). Busca (104) en una base de datos de contactos (14) si hay o no contactos disponibles para el dispositivo (121) o dispositivos de un abonado y, en caso afirmativo, informa (102) al notificador (12); en caso contrario, pide al detector (13) una búsqueda activa (103). Finalmente, supervisa e informa al ISP sobre el proceso de estado y notificación,
- base de datos de contactos (14): es un repositorio que almacena información sobre la manera de contactar con un dispositivo (121), los mecanismos disponibles, y las prioridades y la fiabilidad de cada mecanismo,
- detector (13): hace el inventario de dispositivos de red (121) del abonado e identifica los mecanismos disponibles (107) en la base de datos de contactos (14) para notificar alertas al dispositivo basándose en el análisis del tráfico (105) de la red de área local (120) del abonado. Finalmente, asigna prioridades (106) a cada mecanismo de notificación, basándose en el tráfico de red analizado y las pruebas realizadas por componentes específicos del detector (13) descritos anteriormente,
- notificador (12): selecciona (108), a partir de los mecanismos disponibles almacenados en la base de datos de contactos (14), uno o más mecanismos con mayor prioridad, es decir, con mayor probabilidad de ser vistos por el usuario, emite la notificación (109, 110), bien localmente, es decir enviando la alerta directamente (109) a la red de área local (120) alterando el tráfico de usuario para notificar la alerta sin necesidad de agentes locales en el dispositivo (121), o bien, cuando no es posible o eficaz, informa a un sistema externo de red (110) con un identificador adecuado para realizar la notificación. Finalmente, mantiene el estado del proceso de notificación.

La figura 2 muestra más en detalle el gestor de consultas (11) y su flujo de configuración con el resto de componentes del sistema (111). El gestor de consultas (11) es el punto de entrada del sistema (111), puesto que recibe solicitudes de notificación (101) desde el operador de red (100) para entregar un mensaje de notificación o alerta. Estas solicitudes incluyen el contenido del mensaje a notificar y el dispositivo o dispositivos a los cuales está destinado el mensaje y, optativamente, comprende parámetros adicionales tales como el nivel de prioridad, el tiempo de activación y desactivación, el número de intentos y el tiempo de espera máximo. El dispositivo de destino (121) puede ser identificado por su dirección de IP, la Dirección de MAC, o el nombre del dispositivo de alojamiento, y esta identificación del dispositivo proporciona conectividad en la red de área local (120) del abonado. La identificación del dispositivo se usa para consultar (201) la base de datos de contactos (14) que almacena las capacidades de notificación para verificar la existencia del dispositivo de destino (121) y los mecanismos de notificación válidos. El gestor de consultas (11) envía (202) la solicitud de notificación, con la información recuperada desde la base de datos de contactos (14) y según los condicionamientos de parámetros, al notificador (12), solo si ha encontrado al menos un mecanismo de notificación disponible para el dispositivo de destino (121). Si no se especifica un dispositivo en la solicitud de notificación, existe la posibilidad de notificar a todos los dispositivos identificados y encontrados en la base de datos de contactos (14). En caso de que no haya ningún dispositivo resultante de la consulta a la base de datos de contactos (14), la solicitud de notificación avanza o es transmitida (203) al detector (13) para iniciar una búsqueda activa del dispositivo o dispositivos. Periódicamente, el gestor de consultas (11) consulta la base de datos de consultas (14) para comprobar la existencia de nuevos mecanismos de notificación disponibles para la solicitud, o el estado de la notificación al dispositivo y, según el resultado o los errores, tal como la imposibilidad del detector (13) para obtener un mecanismo de notificación, el gestor de consultas (11) genera una respuesta (204) del sistema (111) al Operador de red (100), comprendiendo la respuesta (204), respectivamente, los mecanismos de notificación disponibles, si los hubiere, asociados al o a los dispositivos de destino, o un informe de errores, si lo hubiere.

La figura 3 muestra más en detalle la base de datos de contactos (14) y su flujo de comunicación con el resto de componentes del sistema (111). La base de datos de contactos (14) aplica el almacenamiento de toda la información necesaria para la operación del sistema (111). La información almacenada comprende principalmente:

– estado de procesos de notificación (141), de manera que los procesos de notificación de funcionamiento puedan ser consultados, con información acerca de su estado y resultado,
– inventario de dispositivos (142), que es un inventario dinámico de los dispositivos (121) del abonado en la red de área local (120) del abonado, enriquecido con información recibida desde el detector (13), que incluye las características del dispositivo, por ejemplo, la dimensión de pantalla, sistemas operativos, protocolos de red disponibles, aplicaciones con detalles sobre volumen de tráfico y frecuencia de uso,
– datos de mecanismos de notificación (143) disponibles, que incluyen, para cada dispositivo, detalles sobre el protocolo de transporte a usar y el valor de fiabilidad del mecanismo obtenido por el detector (13). En caso de que un mecanismo de notificación no esté disponible para el dispositivo, se establece el valor de fiabilidad en cero para indicar que dicho mecanismo de notificación no puede ser usado.

Esta base de datos de contactos (14) interactúa con el resto del sistema (111) como sigue: la base de datos de contactos (14) recibe datos de mecanismos de notificación (143) disponibles, relativos a los mecanismos de notificación descubiertos por el detector (13), así como información (32) procedente del inventario de dispositivos (142), ya que los dispositivos (121) del abonado son descubiertos por el detector (13). El notificador (12) informa (33), actualizando el estado de procesos de notificación (141), acerca del proceso de notificación interno en la red de área local (120) del abonado o su delegación, para mantener informados a los sistemas externos del Operador de red (100) sobre el funcionamiento interno del sistema (111). El gestor de consultas (11) consulta (34) la disponibilidad de dispositivos y mecanismos de notificación para cada solicitud que recibe y, periódicamente, consulta el estado de las notificaciones para informar al Operador de red (100) sobre el resultado. Finalmente, la base de datos de contactos (14) recibe información desde el Operador de red (100) para enriquecerse con datos de red (35) desde la red de área local (120) del abonado no accesible al detector (13), e información sobre el mecanismo de notificación fuera de línea con soporte por parte del Operador de red (100), junto con su grado de fiabilidad.

La figura 4 muestra más en detalle el detector (13) del sistema (111) y sus componentes, interactuando con el resto de componentes del sistema (111). El detector (13) comprende los siguientes componentes:

– descubridor (131): este componente escucha el tráfico en la red de área local (120 del abonado, por cable o inalámbrica, y hace inventario en la base de datos de contactos (14) de todos los nuevos dispositivos (121) del abonado que están conectados. También inicia la búsqueda de un dispositivo, previa solicitud, y verifica la accesibilidad y el estado: en línea/fuera de línea. Con este fin, se basa en tecnologías pasivas (uso de modalidad promiscua en las interfaces de red por cable o modalidad de monitor en interfaces de red inalámbricas, y tráfico de difusión y multidifusión, usado por muchos dispositivos para conectarse a la red), y tecnologías activas (tales como el Protocolo de Resolución de Direcciones –ARP- o la inyección de tráfico de Descubrimiento de Vecinos –ND-),
– analizador (132): su fin es caracterizar todos los nuevos dispositivos (121) del abonado previamente detectados por el Descubridor (131). Este componente ejecuta varias pruebas en paralelo, seleccionando información útil y almacenándola en la base de datos de contactos (14). Esta caracterización incluye múltiples parámetros tales como el tipo de dispositivo, por ejemplo PC, teléfono celular, televisor inteligente, tableta, etc., sistema operativo y versión, protocolos de red activos, y aplicaciones en ejecución, entre otros. La tecnología usada se basa en la combinación de varias técnicas, cada una de las cuales es parte del estado de la técnica y no el objeto de la presente invención, y que son, por ejemplo:
    - escaneado de red: localización de puertos, protocolos abiertos en los dispositivos (121) del abonado,
    - huella digital pasiva (escuchar el tráfico en diferentes protocolos) y huella digital activa (enviar tráfico específico) de manera que, en función de los parámetros de paquetes de tráfico, se obtenga una firma que identifica el sistema operativo y su versión,
    - escaneado de vulnerabilidades: pruebas sobre protocolos abiertos para identificar versiones de dispositivos vulnerables y utilizarlas para obtener más información sobre el dispositivo.

    Inspección profunda de paquetes (DPI): el analizador (132) está configurado entre el dispositivo y la Pasarela de red para ver todo el tráfico de un dispositivo. Esta configuración puede ejecutarse mediante el ISP, actuando a distancia sobre el equipo de red, o incluso mediante el uso de técnicas del hombre en el medio –MITM- por el propio Analizador (132), puesto que está conectado al segmento de red. Esta tecnología proporciona detalles sobre el tipo y versión de las aplicaciones usadas en algunos protocolos, mejorando la caracterización.

De este modo, el Analizador (132) combina estas herramientas para extraer información, relativa a soluciones de notificación, que es exclusivamente relevante para un Operador de red del ISP (100). Además, el Analizador (132) recoge información estadística relativa a dos parámetros: volumen de tráfico generado por cada aplicación a lo largo del tiempo y frecuencia de uso de cada aplicación, estimada a partir del tráfico observado en las aplicaciones. Esta información estadística recogida por el Analizador (132) es usada por el siguiente componente, el Creador (133), para predecir grados de fiabilidad de los mecanismos de notificación disponibles.
– Creador 8133): Este componente identifica los mecanismos de notificación que el Operador de red del ISP (100) puede usar con cada dispositivo y decide el valor/grado de fiabilidad de cada uno de los mismos. Mientras este componente no pueda establecer la confianza en un procedimiento de notificación de

dispositivo específico, tal procedimiento de notificación no se puede usar.

El detector (13) analiza de manera continua el tráfico de red para identificar y clasificar los mecanismos de notificación disponibles, de manera que la información esté a disposición del resto de componentes del sistema (111) con los cuales el detector (13) interactúa, como se muestra en la figura 4. El proceso realizado por el detector (13) se enciende cuando el gestor de consultas (11) solicita una búsqueda (41) para un mecanismo de notificación a un dispositivo específico (121) del abonado que es desconocido, o cuando el Descubridor (131) descubre un nuevo dispositivo (121) del abonado mientras escucha el tráfico (42) en la red de área local (120) del abonado. La información relativa a la identificación de dispositivo y el estado de accesibilidad se actualizan periódicamente (43) en la base de datos de contactos (14). El Analizador (132) consulta (44) periódicamente la base de datos de contactos (14) para conocer los dispositivos descubiertos (121) del abonado y, para los mecanismos de notificación disponibles asignados a los nuevos dispositivos (121) del abonado en la base de datos de contactos (14), el Analizador (132) recoge información estadística (45) de la red de área local (120) del abonado. A su vez, el Analizador (132) almacena (46) esta información estadística y los datos de caracterización de los dispositivos (121) del abonado en la base de datos de contactos (14), de manera que el Creador (133) pueda usar toda esta información. Finalmente, el Creador (133) es responsable de la lectura de la información que esté disponible sobre un dispositivo (121) del abonado desde la base de datos de contactos (14) y de la asignación (47) de los mecanismos de notificación y su grado de fiabilidad a cada dispositivo (121) del abonado.

La figura 5 muestra cómo el analizador (132) funciona e interactúa con el Creador (133). El Analizador (132) usa el escaneado de red (51), no afectando el tráfico normal de usuario (52) a la Pasarela doméstica (HGW). Para un análisis más completo, el tráfico es encaminado (53) a través del Analizador (132), después de llevar a cabo una Inspección profunda de paquetes (DPI). Finalmente, se genera información estadística (151), a partir del tráfico escaneado (152) y observado a través de la Inspección profunda de paquetes (DPI), y suministrado (54) al Creador (133) de manera que pueda estimar la fiabilidad de los mecanismos de notificación.

La figura 6 muestra cómo el Creador (133) funciona e interactúa con los otros componentes del detector (13) y la base de datos de contactos (14). El Creador (133) estima un valor de fiabilidad o índice de confiabilidad (60) combinando datos relativos a la disponibilidad de los dispositivos descubiertos (61) por el descubridor (131), la frecuencia y el volumen de tráfico (62) para los mecanismos de notificación que han sido identificados por el analizador (132). Este índice de confiabilidad (60) está incluido en los datos de mecanismos de notificación (143) asociados a los mecanismos de notificación disponibles, almacenados en la base de datos de contactos (14).

La figura 7 muestra más en detalle el notificador (12) del sistema (111) y sus componentes, interactuando con el resto de componentes del sistema (111). El notificador (12) comprende los siguientes componentes:

- despachador (12_d): recibe y distribuye solicitudes a los componentes de notificación adecuados, según la disponibilidad tecnológica detectada en la red y los valores de prioridad que han sido determinados,
- sub_notificadores (12_{s1}, …, 12_{sN}): Estos componentes aplican tecnologías de notificación. Cada componente se dedica exclusivamente a una tecnología, tal como la inyección de tramas del HTTP o el envío de texto a través de mensajería instantánea. Los mecanismos de notificación que estos componentes aplican son parte del estado de la técnica y no son el objeto de la presente invención y, como tal, no se describen aquí.

El notificador (12) entra en acción cuando al menos un dispositivo (121) del abonado y un mecanismo de notificación viable para este dispositivo han sido identificados. Entonces, el notificador (12) es activado (71) por el gestor de consultas (11) cuando la base de datos de contactos (14) tiene información sobre el dispositivo identificado (121) del abonado y al menos un mecanismo de notificación disponible. El Despachador (12_d) consulta (72) la base de datos de contactos (14) para recuperar los mecanismos de notificación que están disponibles y seleccionar aquel, o aquellos, con un valor de prioridad superior a un umbral configurable por el operador de red (100). El Despachador (12_d) envía (73) toda la información necesaria para la notificación a uno o más de los Sub_notificadores (12_{s1}, …, 12_{sN}), que, a su vez, entregan (74) el mensaje de notificación al dispositivo o dispositivos (121) implicados del abonado. Cada uno de los Sub_notificadores (12_{s1}, …, 12_{sN}) notifica (75), además, el resultado del proceso de envío y, en algunos casos, en función de la tecnología usada, puede enviar de vuelta un acuse de recibo de la recepción de notificación al operador de red (100). Con toda la información anterior usada, el Despachador (12_d) actualiza (76) la información en la base de datos de contacto (14), de manera que la información actualizada esté disponible para el resto de módulos del sistema (111).

La figura 8 muestra un ejemplo de caso de uso de un escenario de red en el que el sistema (111) puede estar integrado en la red de área local (120) del abonado para aplicar el procedimiento descrito para enviar mensajes de notificación o de alerta a uno o más dispositivos domésticos (121_{d1}, …, 121_{dN}) conectados a una red LAN doméstica, que es la red de área local (120) con la que un abonado de una red de un ISP (800) está comunicado. La red de área local (120) y la red del ISP (800) están comunicadas a través de una pasarela doméstica (HGW). El sistema (111) para la notificación de un mensaje, como una alerta, es proporcionado por el ISP como un dispositivo de HW situado en la red de área local (120), y es gestionado por el ISP mediante un módulo de gestión (801) y la conectividad de red del abonado con la pasarela doméstica (HGW). El sistema (111) proporciona al operador de red (100) de la red del ISP (800) medios para la notificación de alertas a un abonado que tiene que ser consciente de la

alerta para autorizar al operador de red (100) a tomar ciertas acciones, o para que el abonado tome medidas con relación a los dispositivos notificados (121_{d1}, …, 121_{sN}) del abonado. Algunos casos de uso relacionados con alertas de seguridad son avisos de uso inapropiado de la red, tales como generación de correo no deseado o un aviso sobre un dispositivo infectado por un programa malicioso. El sistema (111) recibe una solicitud para notificar una alerta de seguridad (81), por ejemplo, una infección por un programa malicioso, a al menos uno de los dispositivos (121_{d1}, …, 121_{sN}) de abonado, por ejemplo, un primer dispositivo (121_{d1}) del abonado es el especificado para dar la alerta en la figura 8. El sistema (111) recibe la solicitud de notificación desde el módulo de gestión (801) de la red del ISP (800) a través de la pasarela doméstica (HGW) y ejecuta el procedimiento descrito anteriormente: localizar el dispositivo, identificar los mecanismos disponibles (por ejemplo, una inyección de tramas en una página del HTTP usada por el dispositivo, un SMS y una cuenta de correo electrónico activa obtenida que analiza el tráfico en línea), y seleccionar el mecanismo más fiable (inyectar un título del HTTP se estima como el mecanismo más fiable), finalmente lanzar (82) la alerta de notificación redirigiendo e inyectando un mensaje del HTML (83) que comprende la información de alerta (802). En el caso de que el resto de los dispositivos (121_{d1}, …, 121_{sN}) del abonado no sean solicitados para ser notificados, en el ejemplo, puesto que no están afectado por el programa malicioso, ningún mecanismo de notificación está activado (84).

El sistema (111) descrito aquí no se limita a mecanismos de notificación para alertas de seguridad, ya que la presente invención admite notificaciones de cualquier naturaleza, por ejemplo:

- consumo de cuota de un servicio de pago por uso,
- publicidad dirigida a un dispositivo por el Operador.

La figura 9 muestra un ejemplo de caso de uso alternativo de un escenario de red en el que el sistema (111) puede integrarse usando una capacidad de virtualización, es decir, con acceso a una HGW de ancho de banda virtualizado (vCPE), de manera que el tráfico en el nivel OSI 3 sea directamente accesible (91) por el operador de red (100). En este caso, el sistema (111) está situado en la red del ISP (900) en un Entorno Virtual de Ejecución de Software como el divulgado en el documento ES 2386048 B1. El Entorno Virtual de Ejecución de Software proporciona un equipo de red de operador compartido (por ejemplo, recursos para servidores virtualizados) que está conectado lógicamente a la instancia del Puente de Agregación ofrecida por el vCPE de manera que tenga conectividad de Capa 2 con dispositivos domésticos y con la interfaz dirigida al usuario del enrutador doméstico virtual. En este entorno Virtual de Ejecución de Software, el sistema (111) para notificación de alertas funciona siguiendo las mismas etapas mostradas en la figura 8, pero también usando la conectividad de capa 2 (91) de la Pasarela Doméstica de Banda ancha (vCPE) conectada (90) a un conmutador doméstico (HS).

La figura 10 muestra un ejemplo adicional de caso de uso donde la capacidad del sistema (111) se usa para detectar un tipo de dispositivo (1001, 1002, 1003) del abonado. El sistema (111) tiene la capacidad de identificar a través del detector (13) que la vivienda del abonado tiene varios tipos de dispositivos (1001, 1002, 1003) y múltiples opciones de notificación asignadas a los mismos. Por ejemplo, en un posible escenario de red, como se muestra en la figura 10, el operador de red (100) solicita enviar una alerta masiva (1100) a todos los dispositivos (100) del abonado conectados a la red de área local (120) del abonado. El detector (13) puede identificar los diferentes tipos de dispositivos (1001, 1002, 1003) y mecanismos de notificación (1101), por ejemplo: un televisor inteligente (1001), un ordenador de sobremesa (1002) y un teléfono celular (1003). El notificador (12) genera un mensaje de notificación adaptado respectivamente a cada dispositivo (1102, 1102', 1102"). Por ejemplo, el televisor inteligente (1001) ofrece una API (1102) para mostrar mensajes en la pantalla, el ordenador de sobremesa (1002) se usa para la navegación en la Red (1102') y, por lo tanto, se puede usar una redirección de la Red para mostrar un mensaje del HTTP, y el uso de un servidor de SMS (1103) del ISP para enviar alertas del SMS (1102") permite alcanzar celdas telefónicas (1003) con tecnología de 2G.

Esta aplicación puede simplificar la gestión del ISP, ya que los mensajes son independientes del tipo de dispositivo, delegando en el SAS la adaptación inteligente de mensajes, de manera que haya una mayor probabilidad y, por tanto, fiabilidad de observar la alerta.

La figura 11 muestra un caso de uso aplicado donde el sistema (111) es una extensión para un entorno de negocios con múltiples LAN (1111_{d1}, …, 1111_{dN}) a las que los usuarios están conectados con un gran número de dispositivos (1111), deteriorados por el fenómeno BYOD: Trae Tu Propio Dispositivo. La eficacia técnica del sistema (111) puede entenderse gracias al detector (13), que puede supervisar el tráfico de intranet (1112) para detectar e inventariar un gran número de dispositivos (1111). La disposición del sistema (111) en la intranet conectada al tráfico (1113) de diferentes subredes de empresa o LAN (1111_{d1}, …, 1111_{dN}), mediante tecnologías de agregación de VLAN o 802.1Q, o el despliegue de interfaces físicas en cada subred, permite optimizar las notificaciones con un pequeño número de recursos de hardware. Además, el detector (13), como parte del proceso de identificación del mecanismo con más fiabilidad, hace que sea posible clasificar el uso y el volumen de tráfico en la red de empresa y detectar aplicaciones no conformes a la política de la empresa (1114). Como parte de los mecanismos de notificación, el notificador (12) puede, optativamente, extenderse utilizando mecanismos de notificación adicionales (1115) que están disponibles en la empresa, tales como listas de correos electrónicos, tarjetas electrónicas, aplicaciones de cliente en los elementos, etc., para evitar duplicidades y optimizar recursos gracias a la gestión centralizada (1116) del gestor de consulta (11) por el operador de red del ISP (1110).

Cabe señalar que, en este texto, el término “comprende” y sus derivaciones (tales como “comprendiendo”, etc.) no deberían entenderse en un sentido excluyente, es decir, estos términos no deberían interpretarse como que excluyen la posibilidad de que lo descrito y definido pueda incluir elementos, etapas, etc. adicionales.

REIVINDICACIONES

1. Un sistema (111) de notificación de dispositivos de abonado (121, 121_{d1}, 121_{dN}, 1001, 1002, 1003, 1111) en redes de un ISP, Proveedor de Servicios de Internet, que está integrado en una red del IP, estando comunicado el sistema (111) con una red de área local (120) de abonado, y comprendiendo una interfaz con un operador de red (100) de un ISP para recibir (101) al menos una solicitud de notificación que comprende un contenido de notificación y una identidad de al menos un dispositivo de abonado (121) de destino, y estando el sistema (111) **caracterizado por** comprender además:

- una base de datos de contactos (14) que almacena una dirección de contacto de cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111) e identificaciones de mecanismos de notificación disponibles para cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111),

- un gestor de consultas (11) que verifica la dirección de contacto del dispositivo de abonado (121) de destino, y si hay o no mecanismos de notificación disponibles para el dispositivo de abonado (121) de destino en la base de datos de contactos (14), usando la identidad del dispositivo de abonado (121) de destino, y comprendiendo el gestor de consultas (11) medios de envío para enviar una respuesta que indica un estado de la solicitud de notificación a la interfaz del operador de red (100) del ISP;

- un detector (13) que asigna prioridades (106) a cada mecanismo de notificación, en base al tráfico de red analizado, y que comprende:

  - un descubridor (131) para inventariar cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111) en la base de datos de contactos (14), escuchando la red de área local (120) del abonado,

  - un analizador (132) para analizar (105) el tráfico desde la red de área local (120) del abonado,

  - un creador (133) para identificar mecanismos de notificación de cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111) inventariado por el descubridor (131), estimando el creador (133) un índice de fiabilidad (60) para cada mecanismo de notificación identificado, combinando datos con respecto a la disponibilidad (61) de cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111) inventariado por el descubridor (131), la frecuencia y el volumen de tráfico (62) para los mecanismos de notificación identificados por el analizador (132), y almacenando el índice de fiabilidad (60) en la base de datos de contactos (14) como la prioridad asignada al mecanismo de notificación identificado, disponible para cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111);

- un notificador (12) que selecciona (108) al menos un mecanismo de notificación entre los mecanismos de notificación disponibles, si hay mecanismos de notificación disponibles identificados por el creador (133) y almacenados en la base de datos de contactos (14) para el dispositivo de abonado (121) de destino, y comprendiendo el notificador (12) medios de envío para enviar el contenido de la notificación a la dirección de contacto del dispositivo de abonado (121) de destino, usando el mecanismo de notificación seleccionado, si lo hubiera.

2. El sistema (111) de acuerdo con la reivindicación 1, en el que el gestor de consultas (11) distribuye las solicitudes de notificación (101) recibidas desde la interfaz del operador de red (100) del ISP e informa (102) al notificador (12) sobre la dirección de contacto del dispositivo de abonado (121) de destino y los mecanismos de notificación disponibles para el dispositivo de abonado (121) de destino, si los hay verificados con éxito en la base de datos de contactos (14) y, en caso contrario, si la verificación no tiene éxito, solicita al detector (13) una búsqueda activa (103) de mecanismos de notificación y del dispositivo de abonado (121) de destino, analizando (105) el tráfico procedente de la red de área local (120) del abonado.

3. El sistema (111) de acuerdo con cualquiera de las reivindicaciones 1 a 2, que está integrado en la red de área local (120) del abonado.

4. El sistema (111) de acuerdo con cualquiera de las reivindicaciones 1 a 2, que está integrado en una red (900) de un ISP, usando una pasarela doméstica de banda ancha virtualizada (vCPE).

5. El sistema (111) de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que el detector (13) identifica un tipo de cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111) y el notificador (12) genera un mensaje de notificación para enviar el contenido de la notificación, usando el mensaje de notificación el mecanismo de notificación seleccionado, que depende del tipo de cada dispositivo de abonado (121, 121_{d1}, ..., 121_{dN}, 1001, 1002, 1003, 1111).

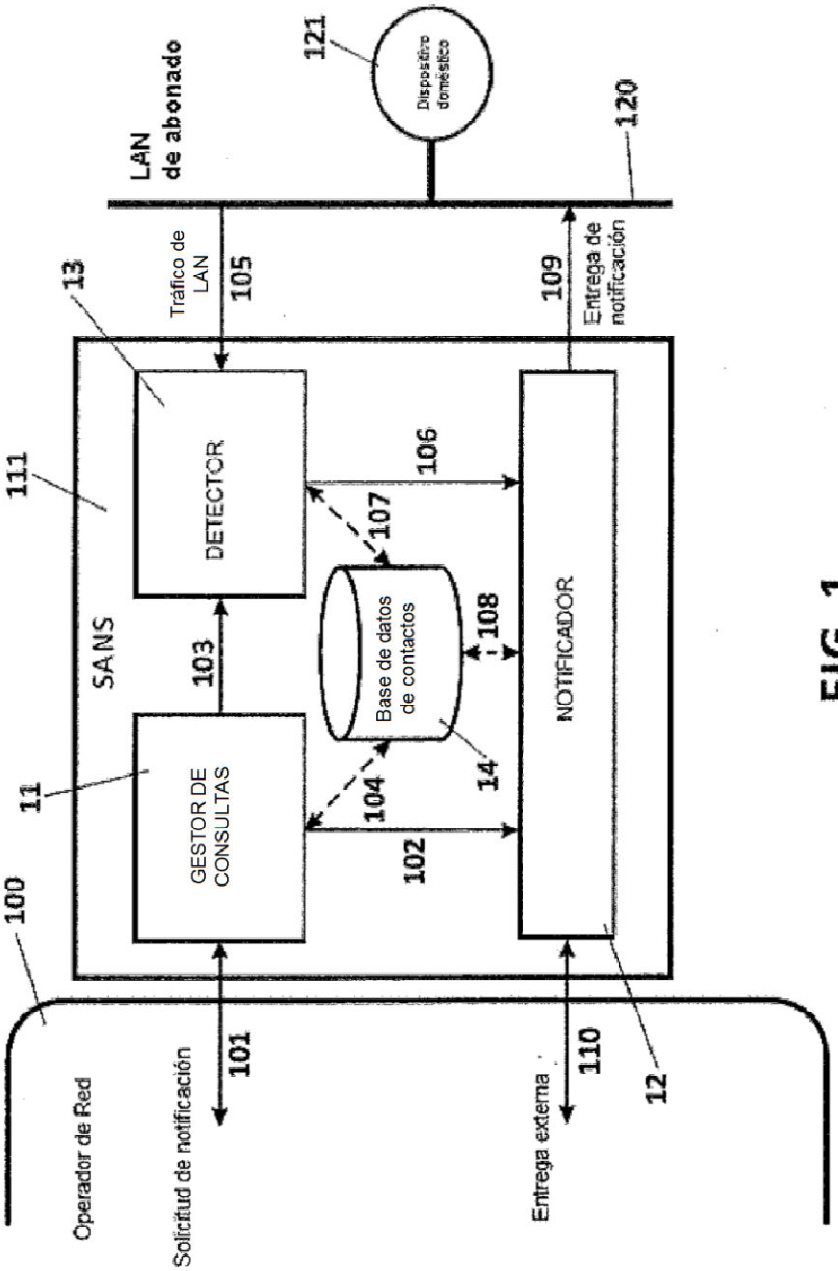
LAN de abonado
121
Dispositivo doméstico
120
Tráfico de LAN
105
109
Entrega de notificación
13
111
DETECTOR
106
107
SANS
Base de datos de contactos
108
103
NOTIFICADOR
11
GESTOR DE CONSULTAS
104
14
102
100
Operador de Red
Solicitud de notificación
101
Entrega externa
110
12

FIG. 1

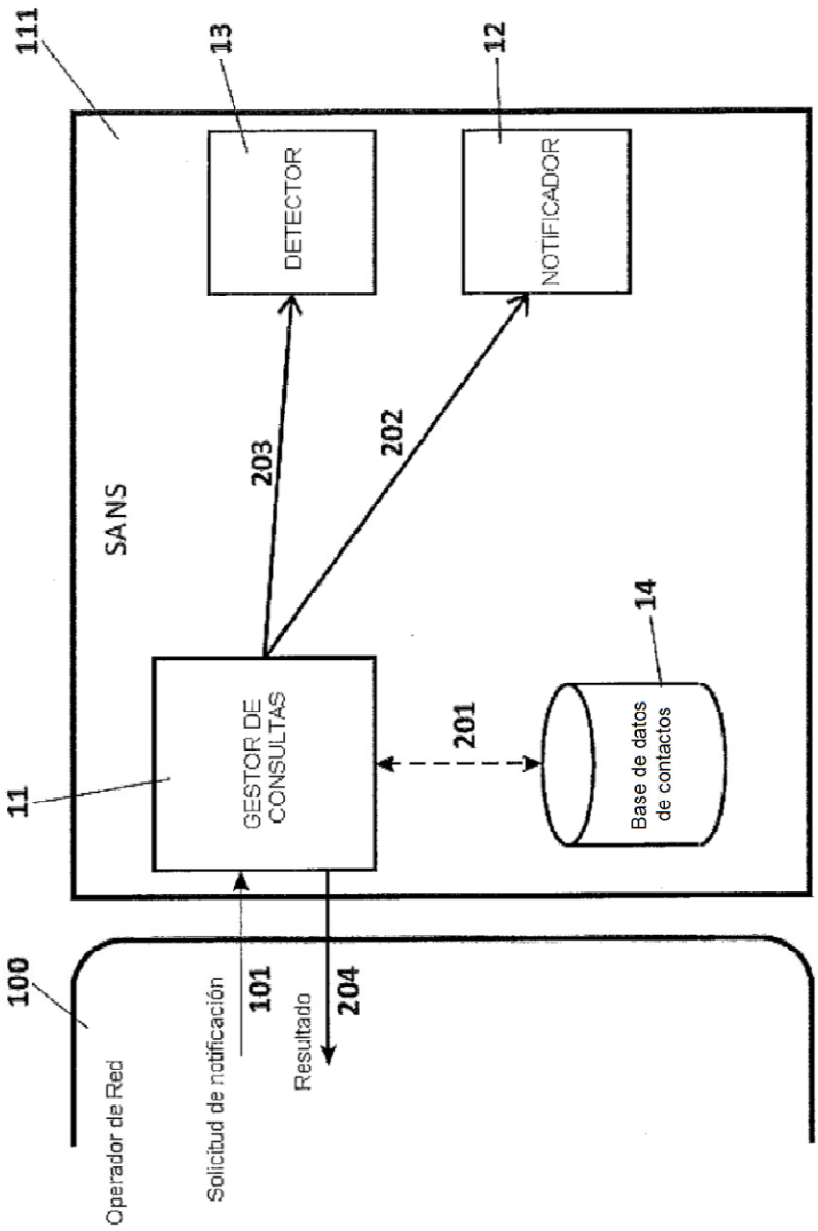
111
13
12
DETECTOR
NOTIFICADOR
SA NS
203
202
14
GESTOR DE CONSULTAS
201
Base de datos de contactos
11
100
Operador de Red
Solicitud de notificación
101
Resultado
204

FIG. 2

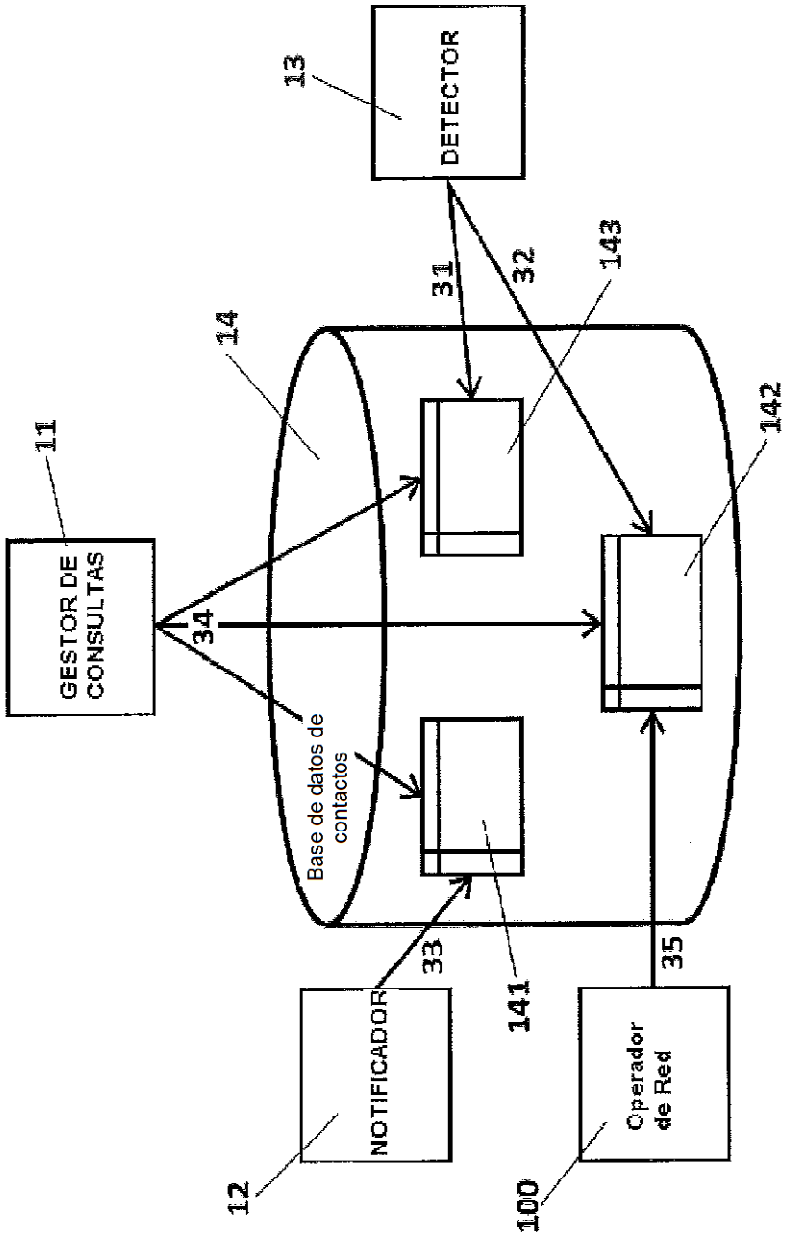
13
DETECTOR
31
32
143
14
142
11
GESTOR DE CONSULTAS
34
Base de datos de contactos
33
141
35
NOTIFICADOR
Operador de Red
12
100

FIG. 3

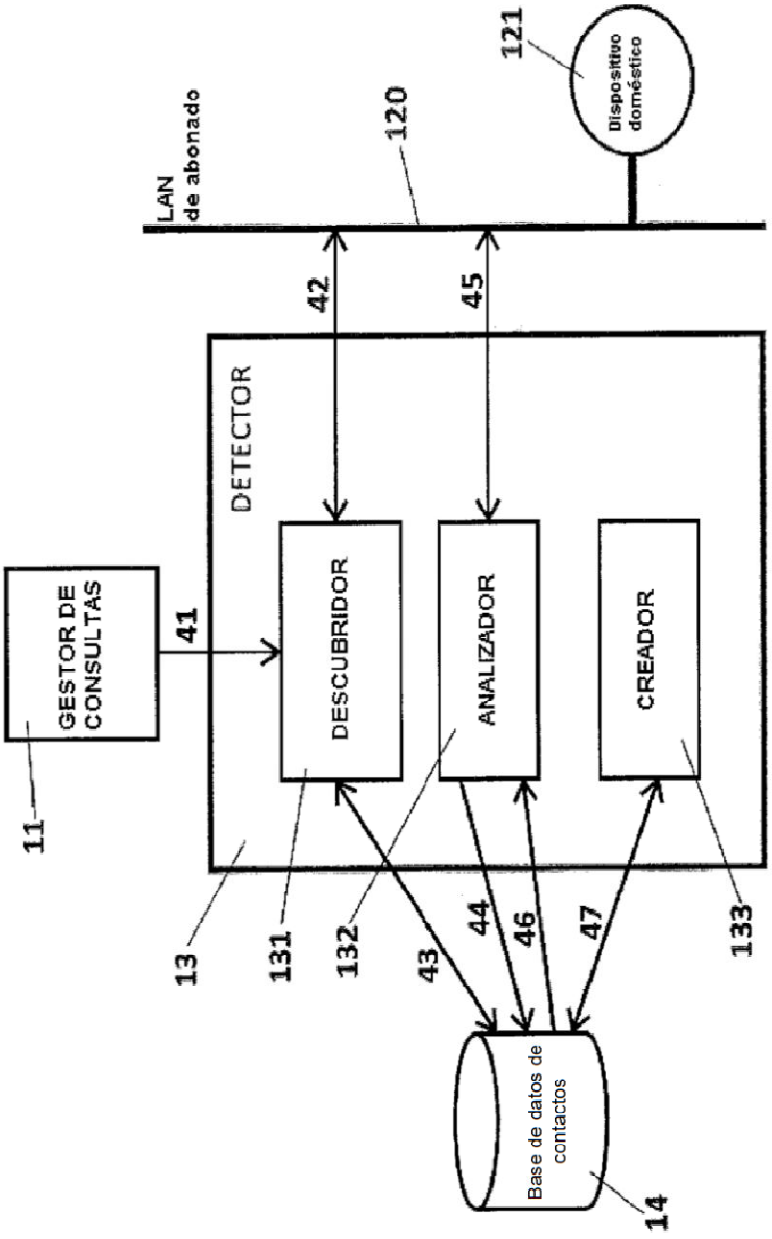
LAN de abonado
120
121
Dispositivo doméstico
42
45
DETECTOR
GESTOR DE CONSULTAS
41
DESCUBRIDOR
ANALIZADOR
CREADOR
11
13
131
132
43
44
46
47
133
Base de datos de contactos
14

FIG. 4

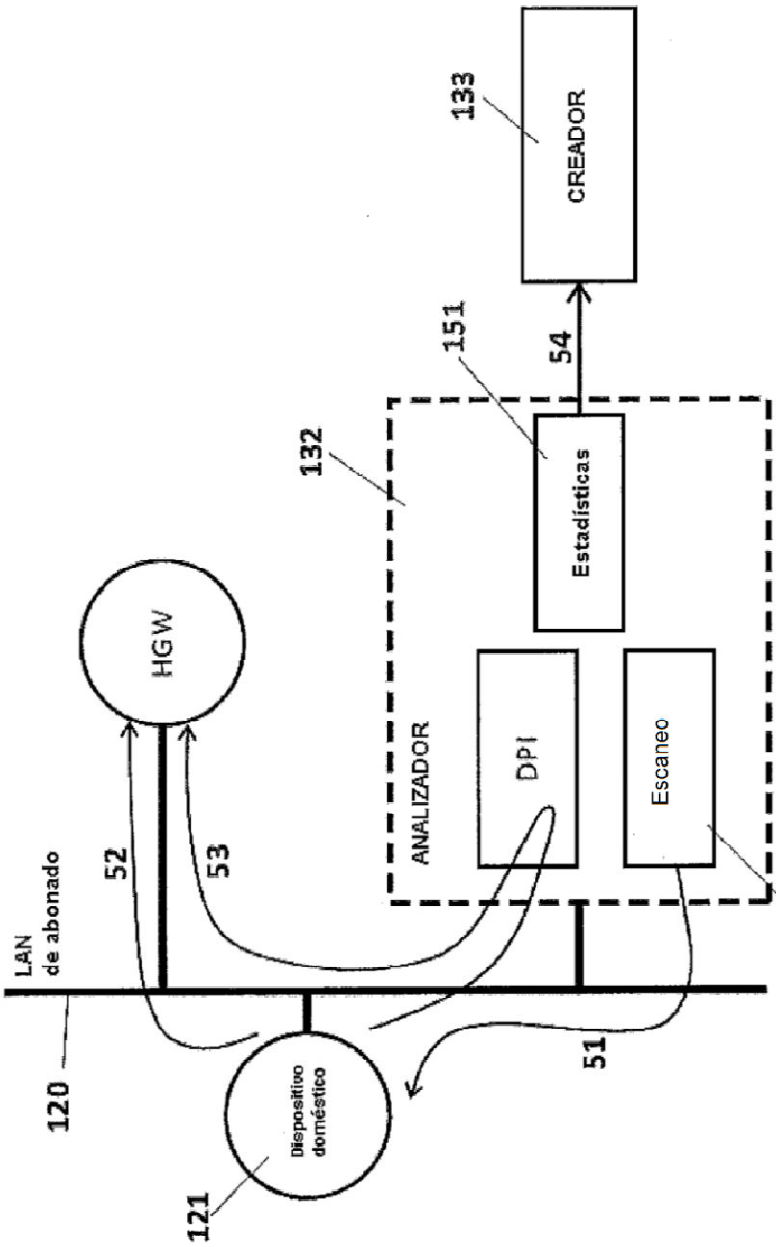
133
CREADOR
151
54
132
Estadísticas
HGW
ANALIZADOR
DPI
Escaneo
52
53
LAN
de abonado
120
Dispositivo
doméstico
121
51
152

FIG. 5

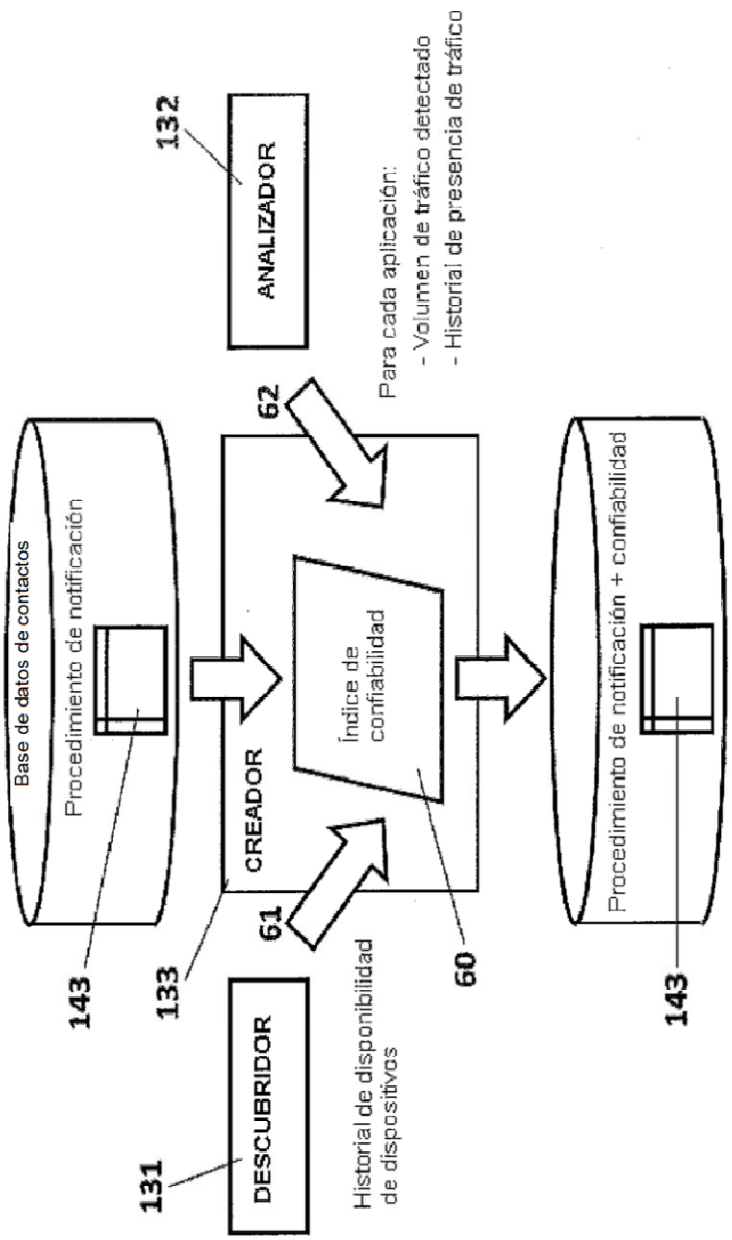
132
ANALIZADOR
62
Para cada aplicación:
- Volumen de tráfico detectado
- Historial de presencia de tráfico
Base de datos de contactos
Procedimiento de notificación
143
133
CREADOR
Índice de confiabilidad
61
60
Historial de disponibilidad de dispositivos
131
DESCUBRIDOR
Procedimiento de notificación + confiabilidad
143

FIG. 6

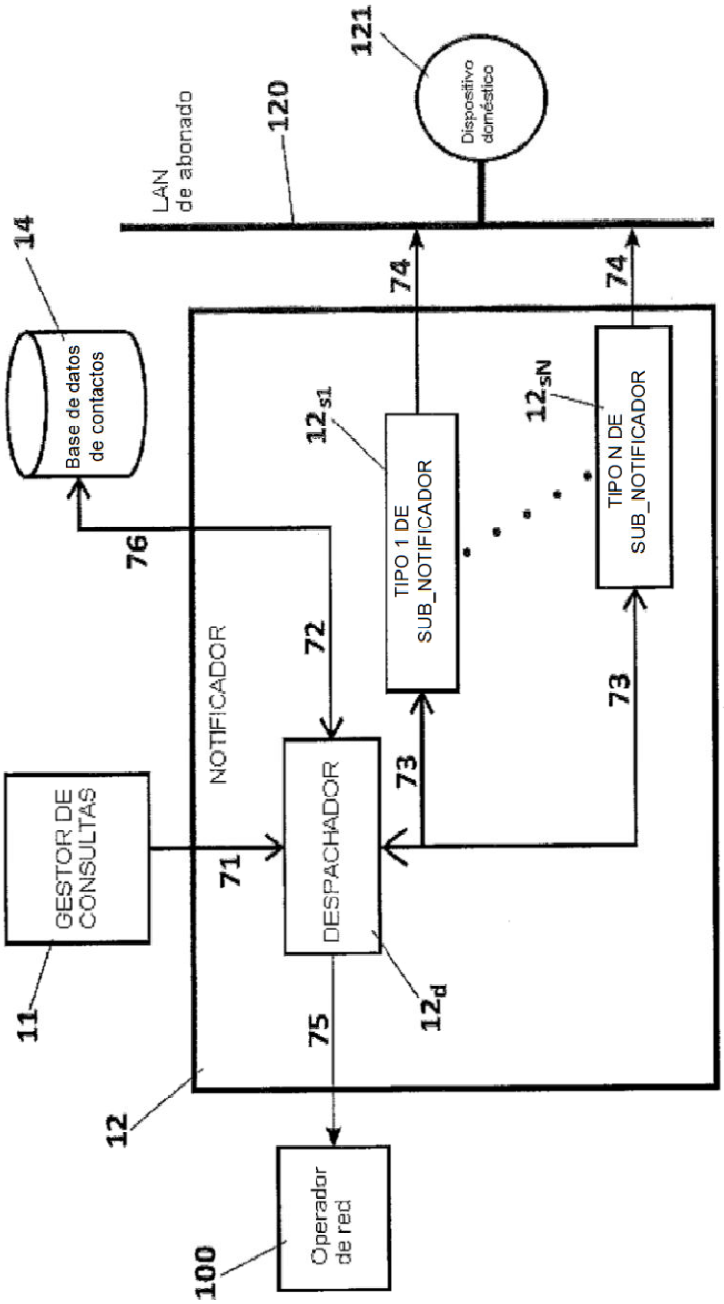
121
Dispositivo doméstico
120
LAN de abonado
14
Base de datos de contactos
74
74
12_{s1}
12_{sN}
TIPO 1 DE SUB_NOTIFICADOR
TIPO N DE SUB_NOTIFICADOR
76
72
73
73
NOTIFICADOR
GESTOR DE CONSULTAS
71
DESPACHADOR
12_d
11
75
12
Operador de red
100

FIG. 7

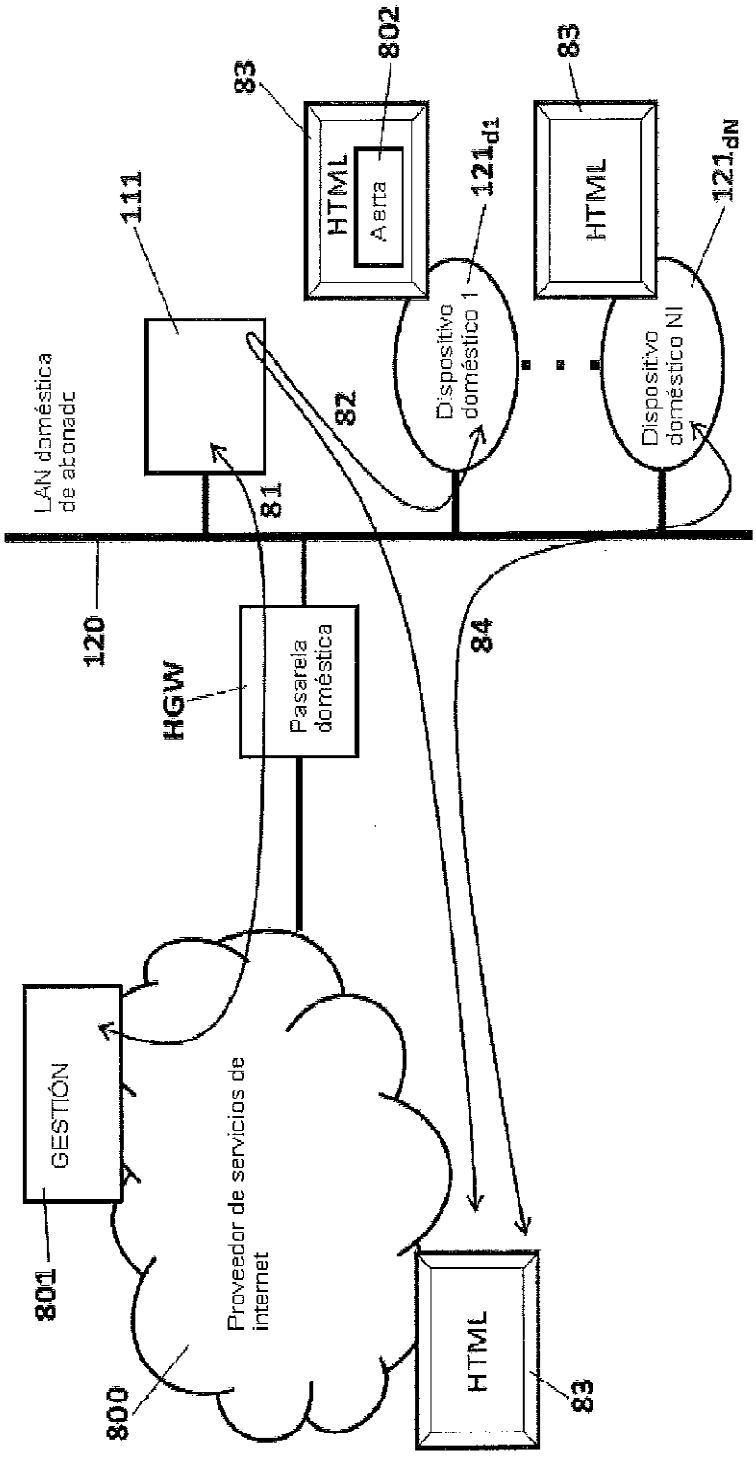
LAN doméstica de abonado
120
111
81
82
83
802
HTML
Alerta
121d1
Dispositivo doméstico 1
121dN
Dispositivo doméstico NI
HGW
Pasarela doméstica
84
GESTIÓN
801
Proveedor de servicios de internet
800
HTML
83

FIG. 8

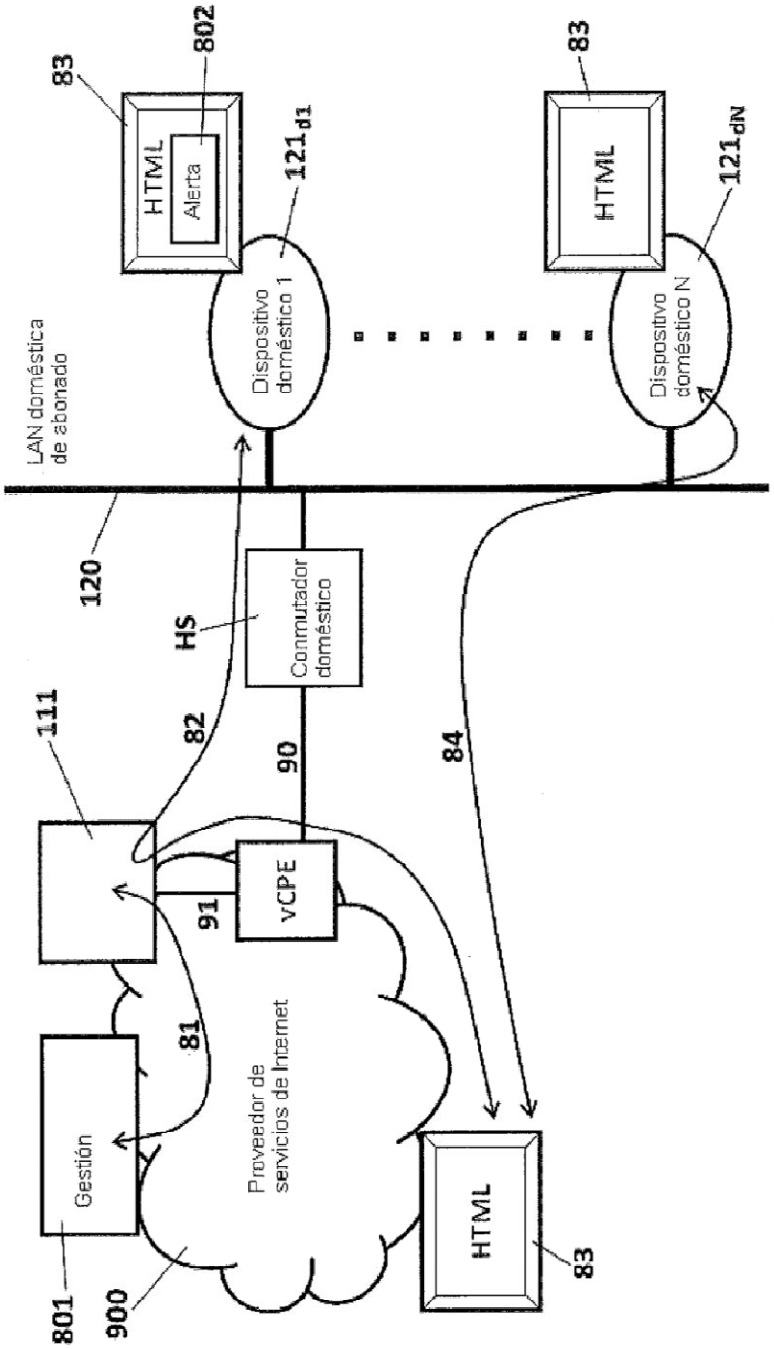
83
802
HTML
Alerta
121d1
Dispositivo doméstico 1
83
HTML
121dN
Dispositivo doméstico N
LAN doméstica de abonado
120
HS
Conmutador doméstico
111
82
90
84
vCPE
91
81
Gestión
Proveedor de servicios de Internet
HTML
83
801
900

FIG. 9

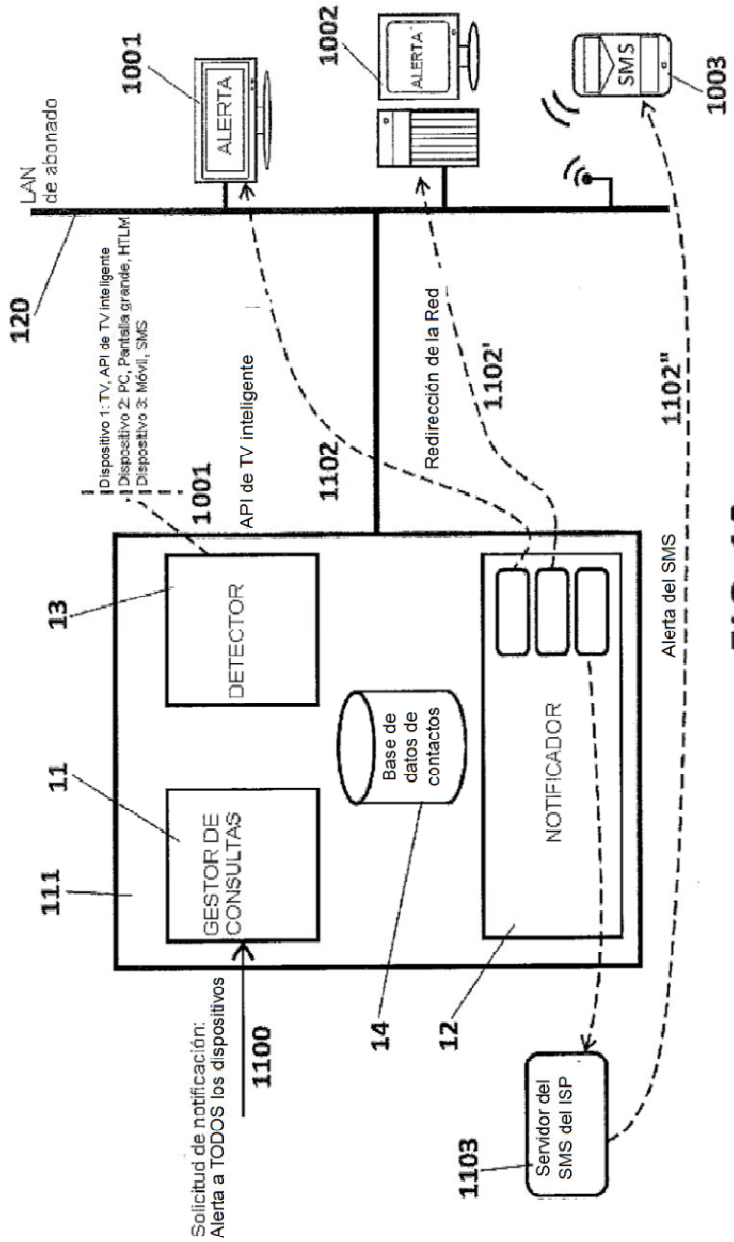
1001
ALERTA
1002
ALERTA
SMS
1003
LAN
de abonado
120
Dispositivo 1: TV, API de TV inteligente
Dispositivo 2: PC, Pantalla grande, HTLM
Dispositivo 3: Móvil, SMS
1001
API de TV inteligente
1102
Redirección de la Red
1102'
1102"
13
DETECTOR
11
GESTOR DE CONSULTAS
111
Base de datos de contactos
NOTIFICADOR
Alerta del SMS
Solicitud de notificación:
Alerta a TODOS los dispositivos
1100
14
12
1103
Servidor del SMS del ISP

FIG. 10

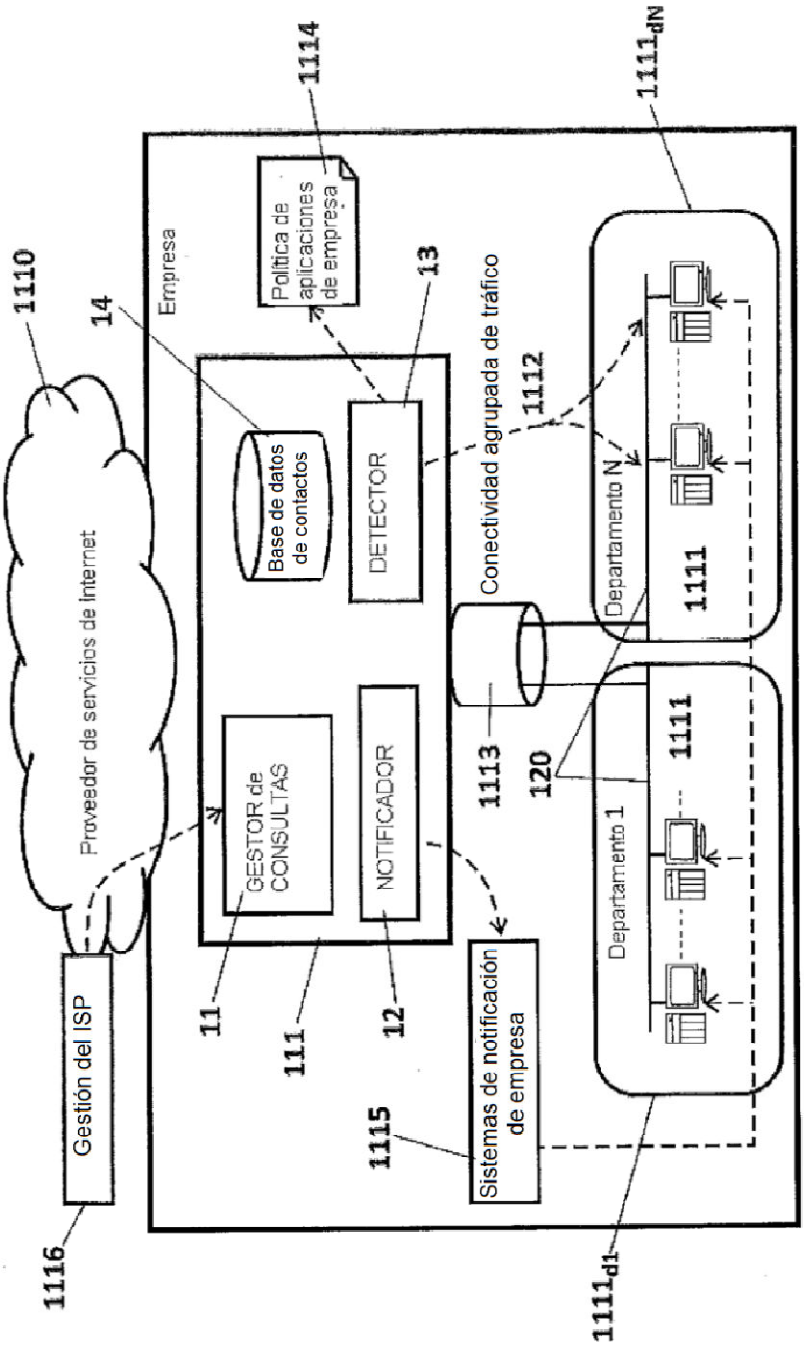
1110
14
Empresa
1114
Política de aplicaciones de empresa
13
1111dN
Base de datos de contactos
DETECTOR
1112
Conectividad agrupada de tráfico
Departamento N
1111
Proveedor de servicios de Internet
GESTOR de CONSULTAS
NOTIFICADOR
1113
120
Departamento 1
1111
11
111
12
1115
Sistemas de notificación de empresa
Gestión del ISP
1116
1111d1

FIG. 11