(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 366 649**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05814017 .9**
(96) Fecha de presentación : **30.11.2005**
(97) Número de publicación de la solicitud: **1830512**
(97) Fecha de publicación de la solicitud: **05.09.2007**

(54) Título: **Método y dispositivo para poner en práctica una autentificación de dominio y de privilegio de acceso a red.**

(30) Prioridad: **04.12.2004 CN 2004 1 0097786**

(45) Fecha de publicación de la mención BOPI:
24.10.2011

(45) Fecha de la publicación del folleto de la patente:
24.10.2011

(73) Titular/es: **HUAWEI TECHNOLOGIES Co., Ltd.**
Huawei Administration Building, Bantian, Longgang District, Shenzhen Gu, CN

(72) Inventor/es: **Jin, Tao**

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Método y dispositivo para poner en práctica una autenticación de dominio y de privilegio de acceso a red.

CAMPO DE LA INVENCIÓN

La presente invención se refiere a tecnologías de acceso a red en el campo de la comunicación y de la informática, en particular, a un método y un dispositivo para poner en práctica una autenticación de dominio y una autenticación de privilegio de acceso a red.

ANTECEDENTES DE LA INVENCIÓN

La mayor parte de las redes de empresas existentes y las redes de área local relacionadas utilizan un sistema de dominio. Por ejemplo, numerosas redes de empresa emplean el Controlador de Dominio Primario de Windows de Microsoft Company. Para dispositivos de red, de una red de empresa, se podrían necesitar proporcionar algunos controles de servicios, que incluyen que un usuario introduzca diferentes nombres y contraseñas del usuario para obtener diferentes privilegios de acceso a red, en donde los nombres y contraseñas del usuario necesitan introducirse por el propio usuario. Puesto que un controlador de dominio se utiliza en la red de empresa, el usuario ha de transmitir la autenticación de dominio cuando desee acceder a algunos recursos de redes internos. De este modo, el usuario necesita introducir, de nuevo, un nombre y contraseña de usuario correspondientes.

Por lo tanto, Microsoft Company establece una solución de autenticación simple, de una sola vez, en la que el nombre y la contraseña del usuario se introducen en el sistema de Windows solamente una vez. El ordenador se registra inicialmente en la red según la información de identidad de dominio del usuario y luego se registra en el dominio. De este modo, el usuario puede obtener una identidad válida y un privilegio de acceso de la red y del dominio, simultáneamente, introduciendo el nombre y la contraseña del usuario solamente una vez. Un modo de conexión en red (*networking*) típico se representa en la Figura 1 y su flujo de autenticación se representa en la Figura 2. Los procesos primarios son como sigue:

1. Se realiza un procesamiento de pre-autenticación, que se refiere a varias preparaciones antes de una autenticación, tales como obtener una dirección IP, realizar una negociación de capa de enlace, etc.

2. Un sistema de petición de autenticación envía una petición de autenticación que contiene la información de identidad del usuario a un dispositivo de control de autenticación. La información de identidad del usuario puede ser el nombre y la contraseña del usuario o una tarjeta inteligente, tal como una tarjeta SIM con la identidad del usuario. En la solución de Microsoft, la información de identidad de dominio, tal como nombre de usuario del dominio, cuenta, etc. se puede utilizar también como información de identidad del usuario para una autenticación de red.

3. Después de que el dispositivo de control de autenticación obtiene la información de identidad del usuario, una petición de autenticación se envía a un servidor de autenticación. El servidor de autenticación es una entidad lógica, que suele ser independiente del dispositivo de control de autenticación, pero puede ser también una parte del dispositivo de control de autenticación.

4. El servidor de autenticación obtiene directamente la información de identidad del usuario almacenada desde un controlador de dominio o desde un sistema de almacenamiento correspondiente, tal como un Directorio Activo, etc. el motivo es que la red y el dominio utilizan la misma información de identidad del usuario.

5. El servidor de autenticación compara la información de identidad del usuario contenida en la petición de autenticación con la información de identidad del usuario almacenada. Si la identidad del usuario se determina que es válida, se reenvía un resultado de éxito de la autenticación. Si se determina que la identidad del usuario no es válida, se reenvía un resultado de fallo de la autenticación.

6. El dispositivo de control de autenticación reenvía la información del resultado del éxito o fallo de la autenticación al sistema de petición de autenticación. Si la autenticación es un éxito operativo, indica que el sistema de petición de autenticación obtiene un privilegio de acceso a red válido y el dispositivo de control de autenticación puede realizar una autorización, contabilización y control de acceso, etc. en el usuario. Si falla la autenticación, indica que el usuario no obtiene un privilegio de acceso a red válido y el dispositivo de control de autenticación no concederá un correspondiente privilegio de acceso válido para al usuario.

7. Si la autenticación es un éxito operativo, un cliente de Windows envía automáticamente una petición de autenticación de dominio al controlador de dominio.

8. El controlador de dominio compara la información de identidad del usuario soportada en la petición de autenticación de dominio con la información de identidad del usuario almacenada en el controlador de

dominio o en un correspondiente sistema de almacenamiento, tal como Directorio Activo, etc. Si se determina que la identidad del usuario es válida, se reenvía un resultado de éxito operativo de autenticación. Si se determina que la identidad del usuario no es válida, se reenvía un resultado de fallo de la autenticación. A continuación, se reenvía la información del resultado de éxito, o fallo, de la autenticación de dominio al cliente de Windows.

El flujo anterior es un flujo esquemático para el proceso de autenticación. En los protocolos prácticos, es probable que los procesos de petición y de respuesta presenten una pluralidad de procesos.

En los protocolos de autenticación prácticos, en la solución proporcionada por Microsoft Company, se pueden utilizar dos métodos de autenticación, PPPoE y 802.1 x, entre el sistema de petición de autenticación y el dispositivo de control de autenticación. El protocolo de Servicio de Autenticación Remota Telefónica de Usuario (RADIUS) se utiliza entre el dispositivo de control de autenticación y el servidor de autenticación.

Aunque la información de identidad del usuario necesita introducirse solamente una vez cuando la solución anterior se utiliza para la autenticación, debe añadirse un servidor de autenticación RADIUS y el dispositivo de control de autenticación ha de proporcionar una autenticación punto a punto (PPP) con MS-CHAP (Protocolo de Autenticación por Desafío Mutuo de Microsoft) o una autenticación tipo 802.1x. Además, el método existente tiene requisitos estrictos sobre el dispositivo relacionado tal como un terminal de usuario, dispositivo de red y servidor de autenticación etc. Por ejemplo, actualmente, sólo se puede utilizar el servidor de autenticación proporcionado por Microsoft Company y unos pocos servidores de autenticación que pueden acceder a un Directorio Activo (AD, que es una clase de base de datos proporcionada por Microsoft Company para almacenar información tal como información del usuario, información del dominio, etc.). Sin embargo, no se puede utilizar numerosos servidores de autenticación existentes en la red.

El documento D1 (US20040168090) describe un sistema y método para delegar un proceso de autenticación de usuario, para una aplicación conectada en red, a un proxy de autenticación. Una aplicación, conectada en red, puede pedir a un usuario que proporcione información de autenticación para poder acceder a la aplicación. A la recepción de esta información de autenticación desde el usuario, el lado del cliente de la aplicación, conectada en red, envía la información al lado del servidor de la aplicación conectada en red. A continuación, el lado del servidor de la aplicación puede determinar un agente de autenticación apropiado, asociado con el usuario, para delegarle el proceso de autenticación. Por ejemplo, para cada usuario de aplicación, el lado del servidor de la aplicación puede mantener información asociada con el usuario, tal como el empleador del usuario. A continuación, la aplicación puede poner en correspondencia esta información del empleador con un agente de autenticación que opera en el dominio de la red del empleador y el proceso de autenticación se puede delegar, entonces, a este agente de autenticación.

SUMARIO DE LA INVENCIÓN

La invención da a conocer un método y un dispositivo para poner en práctica una autenticación de dominio y una autenticación de privilegio de acceso a red para resolver la limitación en aplicaciones prácticas debido a requisitos estrictos en el terminal de usuario, el dispositivo de red y el servidor de autenticación utilizando el método de autenticación existente.

Para resolver la limitación anterior, la invención da a conocer las soluciones técnicas siguientes.

Un método para poner en práctica la autenticación de dominio y la autenticación de privilegio de acceso a red, que comprende:

la recepción, por un dispositivo de control de seguimiento, de una petición de autenticación de dominio desde un terminal de usuario;

el envío, por el dispositivo de control de seguimiento, de la petición de autenticación de dominio a un controlador de dominio; la recepción, por el dispositivo de control de seguimiento, de un resultado de autenticación de dominio desde el controlador de dominio, en el que se realiza una autenticación de dominio en el terminal de usuario en función de la petición de autenticación de dominio y

la determinación, por el dispositivo de control de seguimiento, de si la autenticación de dominio en el terminal de usuario resulta ser un éxito operativo para obtener el privilegio de acceso del dominio válido en función del resultado de autenticación de dominio; si el terminal de usuario tiene éxito operativo para obtener el privilegio de acceso válido del dominio, la obtención de un privilegio de acceso a red correspondiente al terminal de usuario y la autorización del terminal de usuario para acceder a la red; de no ser así, la prohibición al terminal de usuario de acceder a la red.

En donde:

El dispositivo de control de seguimiento realiza un seguimiento y analiza todos los mensajes de autenticación de

dominio entre el terminal de usuario y el controlador de autenticación de dominio, durante la autenticación de dominio.

El dispositivo de control de seguimiento obtiene directamente el privilegio de acceso a red correspondiente al usuario desde el propio dispositivo, o el dispositivo de control de seguimiento obtiene el privilegio de acceso a red correspondiente al usuario desde otro dispositivo de red.

Cuando el dispositivo de control de seguimiento determina que se necesita una contabilización en el usuario, se da instrucciones a un servidor de contabilización designado para iniciar la contabilización después de determinar que la autenticación de dominio del usuario presenta un éxito operativo.

Un dispositivo de control de seguimiento, que comprende:

un módulo de gestión de dispositivos para gestionar cada uno de los módulos en el dispositivo; un módulo de gestión de ruta para gestionar una ruta de mensajes; un módulo de gestión de usuarios para gestionar la información y privilegio del usuario y un módulo de reenvío de mensajes para enviar un mensaje desde un puerto de entrada del dispositivo a un puerto de salida, en donde el dispositivo comprende, además:

un módulo de análisis sintáctico de mensajes para analizar un mensaje de autenticación de dominio enviado por el módulo de reenvío de mensajes y para guardar la información de usuario en el módulo de gestión de usuarios y

un módulo de procesamiento de mensajes para configurar un privilegio de acceso a red para el usuario en función de un mensaje de éxito de una autenticación de dominio, lo que significa que el usuario tuvo éxito operativo para obtener un privilegio de acceso válido del dominio, analizado por el módulo de análisis sintáctico de mensajes y para prohibir al usuario el acceso a la red, en función de un mensaje de fallo de autenticación de dominio, lo que significa que el usuario falló en la obtención de un privilegio de acceso válido del dominio, analizado por el módulo de análisis sintáctico de mensajes .

El módulo de procesamiento de mensajes está basado en el módulo de gestión de usuarios.

La invención presenta las ventajas operativas siguientes:

1. Registrándose solamente una vez, el usuario puede obtener automáticamente el privilegio de acceso a red y el privilegio de dominio después de que sea positiva la autenticación de dominio. De este modo, esto facilita el uso para los usuarios y mejora, en gran medida, la disponibilidad.

2. En comparación con el método de autenticación de dominio existente, el método para la autenticación de dominio según la invención tiene menos procesos y más alta eficiencia de la autenticación.

3. La invención no establece exigencias extras sobre el dispositivo de control de seguimiento y el controlador de dominio. Un servidor de autenticación no necesita añadirse, ni se requiere que el dispositivo soporte las autenticaciones similares a PPP CHAP o 802.1 x. Por lo tanto, el método de autenticación de la invención no está limitado en las aplicaciones prácticas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama esquemático que representa la conexión en red típica para la autenticación de red y la autenticación de dominio en el sistema Windows según la técnica anterior;

La Figura 2 es un diagrama de flujo de autenticación en donde un usuario se registra primero en la red por su información de identidad de dominio y a continuación, se registra en el dominio según la técnica anterior;

Figura 3 es un diagrama esquemático que representa una conexión en red para poner en práctica una autenticación, según una forma de realización de la invención;

La Figura 4 es un diagrama estructural esquemático de un dispositivo de control de seguimiento, según una forma de realización de la invención y

La Figura 5 es un diagrama de flujo para poner en práctica una autenticación según una forma de realización de la invención.

DESCRIPCIÓN DETALLADA DE LA FORMA DE REALIZACIÓN

Haciendo referencia a la Figura 3, para poner en práctica un procesamiento uniforme de una autenticación de dominio y un control del privilegio de acceso a red, la invención modifica el dispositivo de control de autenticación de la técnica anterior, a un dispositivo de control de seguimiento mediante el cual se efectúa el seguimiento de una

autenticación de dominio en un terminal de usuario durante un proceso completo y se obtiene directamente un privilegio de acceso a red del usuario y se configura en función de un resultado de autenticación de dominio.

Haciendo referencia a la Figura 4, el dispositivo de control de seguimiento comprende principalmente lo que sigue:

un módulo de reenvío de mensajes, que envía un mensaje desde un puerto de entrada a un puerto de salida correspondiente según un mecanismo de conmutación o un mecanismo de reenvío de encaminamiento. Un mensaje de autenticación de dominio necesita enviarse a un módulo de análisis sintáctico de mensajes para su análisis sintáctico. En condiciones normales, el módulo de reenvío de mensajes puede enviar directamente un mensaje de autenticación de dominio que no necesita modificarse. Sin embargo, en algunos casos, por ejemplo, para el mensaje de autenticación de dominio, se necesita añadir, suprimir o modificar alguna información, el mensaje de autenticación de dominio necesita reconstruirse y luego enviarse. Por lo tanto, el módulo de reenvío de mensajes reconstruye, además, el mensaje de autenticación de dominio obtenido y a continuación, envía el mensaje reconstruido.

el módulo de análisis sintáctico de mensajes, que realiza el análisis sintáctico del mensaje de autenticación de dominio y guarda una información de usuario obtenida en un módulo de gestión de usuarios. Cuando una parte de atributos necesite añadirse, suprimirse o modificarse en el mensaje de autenticación de dominio, el módulo de análisis sintáctico de mensajes necesita, además, reconstruir el mensaje de autenticación de dominio;

el módulo de gestión de usuarios, que gestiona la información de red básica del usuario, tal como IP, MAC (Control de Acceso Multimedia), VLAN (Red de Área Local Virtual) etc., registra la información de autenticación de dominio y el estado de autenticación del dominio al que pertenece el usuario y da instrucciones a un servidor de contabilización correspondiente para realizar una contabilización cuando se necesita sobre el usuario;

un módulo de procesamiento de mensajes, que está incorporado, además, en el módulo de gestión de usuarios (no representado en la Figura 4), para obtener y configurar un privilegio de acceso a red para el usuario, cuando el módulo de análisis sintáctico de mensajes analiza el mensaje de autenticación de dominio del usuario, y para controlar el privilegio de usuario.

Un módulo de gestión de dispositivos y un módulo de gestión de ruta, que son responsables para varias gestiones en un dispositivo y una ruta, en función del modo existente.

Existen interfaces de interacción de información de gestión entre el módulo de gestión de dispositivos y los módulos de reposo y el módulo de reenvío de mensajes determina cómo enviar un mensaje por el módulo de gestión de encaminamientos y el módulo de gestión de usuarios.

Un privilegio de acceso a red de un usuario se puede pre-configurar manualmente en el módulo de gestión de usuarios del dispositivo de control de seguimiento y obtenerse directamente por el dispositivo de control de seguimiento. El privilegio de acceso a red se puede enviar también por otros dispositivos en la red. Dicho de otro modo, un privilegio de acceso a red de un usuario se puede pre-configurar y guardar en otros servidores. El dispositivo de control de seguimiento puede efectuar la petición de un privilegio de acceso a red desde los otros servidores, cuando se requiera y a continuación, los otros servidores envían el privilegio de acceso a red al dispositivo de control de seguimiento mediante un protocolo o los otros servidores asignan, de modo dinámico, el privilegio de acceso a red al usuario y a continuación, envían el privilegio de acceso a red al dispositivo de control de seguimiento, por intermedio de un protocolo, después de recibir la petición desde el dispositivo de control de seguimiento. Los atributos de autorización del usuario se pueden modificar también en línea por este método. Los servidores pueden emplear protocolos tales como un protocolo de Servicio de Autenticación Remota Telefónica de Usuario (RADIUS), protocolo de Servicio de Política Abierta Común (COPS), etc. y envía el privilegio de acceso a red en cumplimiento con RFC2865/RFC2866/RFC2869, etc.

Haciendo referencia a la Figura 5, los procesos de autenticación detallados son como sigue.

Proceso 1: Se realiza un procesamiento de pre-autenticación, que comprende principalmente varias preparaciones antes de una autenticación, tales como obtener una dirección de IP, realizar una negociación de enlace y así sucesivamente.

Proceso 2: Un usuario se registra en un dominio introduciendo información de usuario en un terminal de usuario y envía una petición de autenticación de dominio a un controlador de dominio.

Proceso 3: Un dispositivo de control de seguimiento analiza la petición de autenticación de dominio después de recibirla y luego, envía la petición de autenticación de dominio a un controlador de dominio.

El análisis de la petición de autenticación de dominio comprende: el análisis sintáctico de la estructura, atributo y contenido revelado del mensaje de autenticación de dominio y la consulta y registro de una dirección IP de usuario, nombre de usuario, proceso de autenticación de dominio y su estado.

Proceso 4: El controlador de dominio compara la información de identidad del usuario contenida en la petición de autenticación con la información de identidad del usuario almacenada en el controlador de dominio o, su sistema de almacenamiento correspondiente, tal como Directorio Activo, etc. Si se determina que la identidad del usuario es válida, se reenvía un resultado de éxito de la autenticación. Si se determina que la identidad de usuario no es válida, se reenvía un resultado de fallo de la autenticación.

Proceso 5: El dispositivo de control de seguimiento determina si la autenticación de dominio presenta un éxito operativo en función del resultado de la autenticación. Si la autenticación es positiva, se obtiene el privilegio de acceso a red correspondiente al usuario y se configura el privilegio correspondiente y de no ser así, se prohibirá al usuario el acceso a red.

Después de determinar que la autenticación de dominio en el usuario presenta un éxito operativo, si se necesita una contabilización en el usuario, el dispositivo de control de seguimiento da instrucciones a un servidor de contabilización, tal como un servidor RADIUS o un servidor de FTP/TFTP (Protocolo de Transferencia de Ficheros/ Protocolo de Transferencia de Ficheros Trivial) etc. para iniciar la contabilización.

Proceso 6: El dispositivo de control de seguimiento envía un mensaje al terminal de usuario. Si la autenticación es un éxito operativo, significa que el terminal de usuario obtiene simultáneamente un privilegio de acceso válido del dominio y de la red. Si la autenticación presenta un fallo operativo, significa que el usuario no obtiene un privilegio de acceso válido y el dispositivo de control de seguimiento no concede un privilegio de acceso a red válido correspondiente al usuario.

El flujo representado en la Figura 5 es un proceso de autenticación esquemático. En los protocolos prácticos, la petición y la respuesta pueden tener una pluralidad de procesos. El dispositivo de control de seguimiento sigue el resultado de autenticación de dominio durante el proceso de autenticación de dominio completo. Dicho de otro modo, desde la petición de autenticación de dominio de un usuario, todos los mensajes de varios protocolos de autenticación de dominio, tales como peticiones y respuestas, son objeto de seguimiento, se obtiene y analiza la información y se registran, cuando se necesita, la información del usuario y su estado.

En los protocolos prácticos de autenticación de dominio, es el protocolo de NTLM (Windows NT LAN Manager) en Windows NT 4.0, pero puede ser los protocolos NTLM, Kerberos o los protocolos de Autorización de Pasarela Distribuida (DPA) siguiendo Windows 2000. Para el dispositivo de control de seguimiento, puede seguir y analizar todos los protocolos de autenticación de dominio que incluyen, sin limitación, a los protocolos de NTLM, Kerberos y DPA.

Cuando el dispositivo de control de seguimiento constata que está terminada una sesión (una parte de los protocolos de autenticación de dominio puede terminar la sesión correspondiente), termina un límite de tiempo de la autenticación de dominio (algunas autenticaciones de dominio tienen un límite de tiempo), el usuario inicia una nueva petición o el usuario se encuentra desconectado fuera de línea por un protocolo de capa de aplicación o de red, se da instrucciones al servidor de conteo para interrumpir su funcionamiento.

Un proceso de cómo supervisar el proceso de autenticación de dominio por el dispositivo de control de seguimiento se ilustrará ahora tomando, la autenticación de dominio de Kerberos, a modo de ejemplo. El Kerberos es una clase de mecanismo de autenticación orientado a un sistema abierto para proporcionar un servicio de terceros, de confianza, para la comunicación de red. El Kerberos proporciona un mecanismo de cifrado eficaz, por medio del cual un terminal de usuario y un servidor pueden confirmar la identidad de ambos, incluso en un entorno de conexión de red insegura. Además, todas las comunicaciones subsiguientes son objeto de cifrado después de que se transmita la autenticación de identidad mutua. Dicho de otro modo, durante la puesta en práctica, se configura una base de datos de claves de los sistemas que se comunican con el servidor de terceros de confianza, que se mantiene en dicho servidor. Solamente Kerberos y los sistemas con los que se comunica poseen una clave privada. De este modo, se establece una conexión de comunicación de red, de confianza, por la clave privada y una clave de sesión, que se crea durante la autenticación. Un proceso de autenticación de dominio de Kerberos es como sigue.

Proceso 1: Cuando un usuario se registra inicialmente en Windows NT (p.e. controlador de dominio), el SSP (Puerto de Servicio de Seguridad) de Kerberos del terminal de usuario obtiene un así denominado “vale de concesión de vales” (TGT) de Kerberos inicial y Windows NT almacena el TGT en una memoria intermedia de licencias del terminal de usuario como una parte del entorno de registro del usuario.

Proceso 2: Cuando un programa de terminal de usuario intenta acceder a un servicio de red en un servidor, el terminal de usuario constata si hay una licencia de cesión válida para acceder al servidor en su memoria intermedia de licencias cuando opere el terminal de usuario. Si no existe ninguna licencia de cesión válida, el terminal de usuario envía una petición a un centro de distribución de claves para solicitar una licencia de cesión para acceder al servidor y a continuación, memoriza localmente la licencia de cesión solicitada.

Proceso 3: La licencia de cesión se envía al servidor cuando el terminal de usuario establece una conexión de

iniciación con el servidor.

Proceso 4: El servidor verifica la licencia de cesión. Puesto que una parte de la licencia de cesión se ha cifrado utilizando una clave compartida entre el servidor y el centro de distribución de claves y existe una copia de la clave compartida en la memoria intermedia cuando se ejecuta Kerberos en el lado del servidor, el servidor puede verificar directamente el terminal de usuario sin necesidad de conectarse con el servicio de autorización en el centro de distribución de claves. Cuando el terminal de usuario necesita también verificar la identidad del servidor, el servidor tiene en cuenta una marca de tiempo (*time stamp*) recibida, realiza el cifrado de la marca de tiempo después de tener en cuenta la clave de sesión y a continuación, envía la marca de tiempo cifrada al usuario. El usuario determina la identidad del servidor realizando un proceso de descifrado con el uso de la clave de sesión después de la recepción de un mensaje correspondiente.

Existe una clave de sesión que sólo se conoce por el terminal de usuario y el servidor después de que sus identidades sean mutuamente verificadas. De este modo, todas las comunicaciones subsiguientes se pueden proteger por la clave de sesión.

En el Proceso 1, el dispositivo de control de seguimiento puede obtener la información que indica que TGT se obtiene con éxito operativo (lo que significa que la autenticación en el terminal de usuario se transmite por el controlador de dominio). Mientras tanto, el privilegio correspondiente al usuario se puede obtener y controlar configurando de forma estática u obteniendo, de forma dinámica, el privilegio y así sucesivamente. Por lo general, todos los privilegios correspondientes al usuario se obtienen en este proceso.

En el Proceso 2 o en el Proceso 4, el dispositivo de control de seguimiento puede obtener el resultado de autenticación para obtener un servicio por el terminal de usuario, obtener y controlar el privilegio correspondiente al usuario configurando de forma estática u obteniendo, de forma dinámica, el privilegio y así sucesivamente. De forma estricta, el resultado de autenticación en el usuario debe obtenerse en el Proceso 4, pero, de forma imprecisa, se puede obtener en el Proceso 2. En general, un privilegio de un servicio correspondiente a un usuario se configura en este proceso.

En los procesos anteriores, se puede iniciar una operación de contabilización, mientras se obtiene una licencia (que incluye TGT y la licencia de servicio). Un tiempo válido de la licencia se incluye, además, en el mensaje, mientras se obtiene la correspondiente licencia. Por lo tanto, la contabilización se interrumpe cuando termina el tiempo válido de la licencia o cuando el usuario se encuentra desconectado fuera de línea.

De este modo, según la invención, el usuario necesita registrarse para iniciar sesión en el dominio solamente una vez y a continuación, se puede obtener automáticamente el privilegio de acceso a red después de que se transmita la autenticación de dominio. Lo anterior facilita el uso para los usuarios y mejora, en gran medida, la disponibilidad. Además, las soluciones técnicas, según la invención, resuelven la limitación en aplicaciones prácticas debido a requisitos estrictos en el terminal de usuario, utilizando el dispositivo de red y el servidor de autenticación el método de autenticación existente.

Otras ventajas y modificaciones serán evidentes para los expertos en esta materia. Por lo tanto, la invención en sus más amplios aspectos no está limitada a los detalles específicos y formas de realización representativas aquí representadas y descritas. En consecuencia, se pueden realizar diversas modificaciones y variaciones sin desviarse, por ello, del alcance de protección de la invención, según se define por las reivindicaciones adjuntas y sus equivalentes.

REIVINDICACIONES

1. Un método para poner en práctica una autenticación de dominio y una autenticación de privilegio de acceso a red, que comprende:

la recepción, por un dispositivo de control de seguimiento, de una petición de autenticación de dominio desde un terminal de usuario (2);

el envío, por el dispositivo de control de seguimiento, de la petición de autenticación de dominio a un controlador de dominio (3);

la recepción, por el dispositivo de control de seguimiento, de un resultado de autenticación de dominio desde el controlador de dominio, en donde una autenticación de dominio, en el terminal de usuario, se realiza en función de la petición de autenticación de dominio (4) y caracterizado porque:

la determinación, por el dispositivo de control de seguimiento, de si la autenticación de dominio, en el terminal de usuario, es positiva, o no, para obtener un privilegio de acceso válido del dominio en función del resultado de autenticación de dominio; si el terminal de usuario tiene éxito operativo para obtener el privilegio de acceso válido del dominio, la obtención de un privilegio de acceso a red correspondiente al terminal de usuario y la autorización al terminal de usuario para acceder a red; en caso contrario, la prohibición al terminal de usuario de acceder a red (5).

2. El método según la reivindicación 1, que comprende, además: el envío, por el dispositivo de control de seguimiento, del resultado de autenticación de dominio al terminal de usuario (6).

3. El método según la reivindicación 1 o 2, en donde el dispositivo de control de seguimiento sigue y analiza todos los mensajes de autenticación de dominio entre el terminal de usuario y el controlador de autenticación de dominio durante la autenticación de dominio.

4. El método según la reivindicación 1, en donde el dispositivo de control de seguimiento obtiene directamente el privilegio de acceso a red correspondiente al terminal de usuario desde el propio terminal.

5. El método según la reivindicación 1, en donde el dispositivo de control de seguimiento obtiene el privilegio de acceso a red correspondiente al terminal de usuario desde otro dispositivo de red.

6. El método según la reivindicación 5, en donde la obtención por el dispositivo de control de seguimiento del privilegio de acceso a red correspondiente al terminal de usuario desde otro dispositivo de red, comprende además:

la recepción, por el dispositivo de control de seguimiento, del privilegio de acceso a red que está preconfigurado para el terminal de usuario correspondiente desde el otro dispositivo de red, después de que el otro dispositivo de red reciba una petición desde el dispositivo de control de seguimiento o

la recepción, por el dispositivo de control de seguimiento, del privilegio de acceso a red que se asigna dinámicamente al terminal de usuario, después de que el otro dispositivo de red reciba la petición desde el dispositivo de control de seguimiento.

7. El método según la reivindicación 1, en donde cuando el dispositivo de control de seguimiento determina que se necesita una contabilización en el terminal de usuario, se da instrucciones a un servidor de contabilización designado para iniciar la contabilización después de determinar que la autenticación de dominio en el terminal de usuario es positiva.

8. El método según la reivindicación 7, en donde cuando el dispositivo de control de seguimiento constata que una sesión de usuario se termina por un protocolo de autenticación de dominio, que ha terminado un límite de tiempo de autenticación de dominio en el terminal de usuario, que el terminal de usuario envía una nueva petición o que el usuario está desconectado fuera de línea, da instrucciones al servidor de contabilización para interrumpir su operación.

9. Un dispositivo de control de seguimiento, que comprende: un módulo de gestión de dispositivo (401) para gestionar cada uno de los módulos en el dispositivo; un módulo de gestión de ruta (402) para gestionar una ruta de mensajes; un módulo de gestión de usuarios (403) para gestionar informaciones y privilegios de usuarios y un módulo de reenvío de mensajes (404) para enviar un mensaje desde un puerto de entrada del dispositivo a un puerto de salida, que comprende además:

un módulo de análisis sintáctico de mensajes (405) para analizar un mensaje de autenticación de dominio enviado por el módulo de reenvío de mensajes y guardar la información del usuario en el módulo de gestión de usuarios y caracterizado porque:

un módulo de procesamiento de mensajes para configurar un privilegio de acceso a red para el usuario en función de un mensaje de autenticación de dominio positivo, lo que significa que el usuario ha tenido éxito operativo en obtener un privilegio de acceso válido del dominio, analizado por el módulo de análisis sintáctico de mensajes o para prohibir al usuario el acceso a red en función de un mensaje de autenticación de dominio negativo, lo que significa que el usuario no ha obtenido el privilegio de acceso válido del dominio, analizado por el módulo de análisis sintáctico de mensajes.

10. El dispositivo de control de seguimiento según la reivindicación 9, en donde el módulo de procesamiento de mensajes está construido en el módulo de gestión de usuarios (403).

11. Un sistema para poner en práctica una autenticación de dominio y una autenticación de privilegio de acceso a red, que comprende un terminal de usuario (301), un controlador de dominio (302) y un dispositivo de control de seguimiento (303), en donde:

el terminal de usuario (301) envía una petición de autenticación de dominio al controlador de dominio (302);

el controlador de dominio (302) realiza una autenticación de dominio en el terminal de usuario (301) en función de la petición de autenticación de dominio y reenvía un resultado de autenticación de dominio al dispositivo de control de seguimiento (303) y
caracterizado porque:

el dispositivo de control de seguimiento (303) está destinado para determinar si la autenticación de dominio en el terminal de usuario (301) es positiva, o no, para obtener un privilegio de acceso válido del dominio en función del resultado de autenticación de dominio; si el terminal de usuario (301) tiene éxito operativo para obtener el privilegio de acceso válido del dominio, para obtener un privilegio de acceso a red correspondiente al terminal de usuario (301) y para autorizar al terminal de usuario (301) el acceso a red y en caso contrario, prohibir al terminal de usuario (301) el acceso a red.

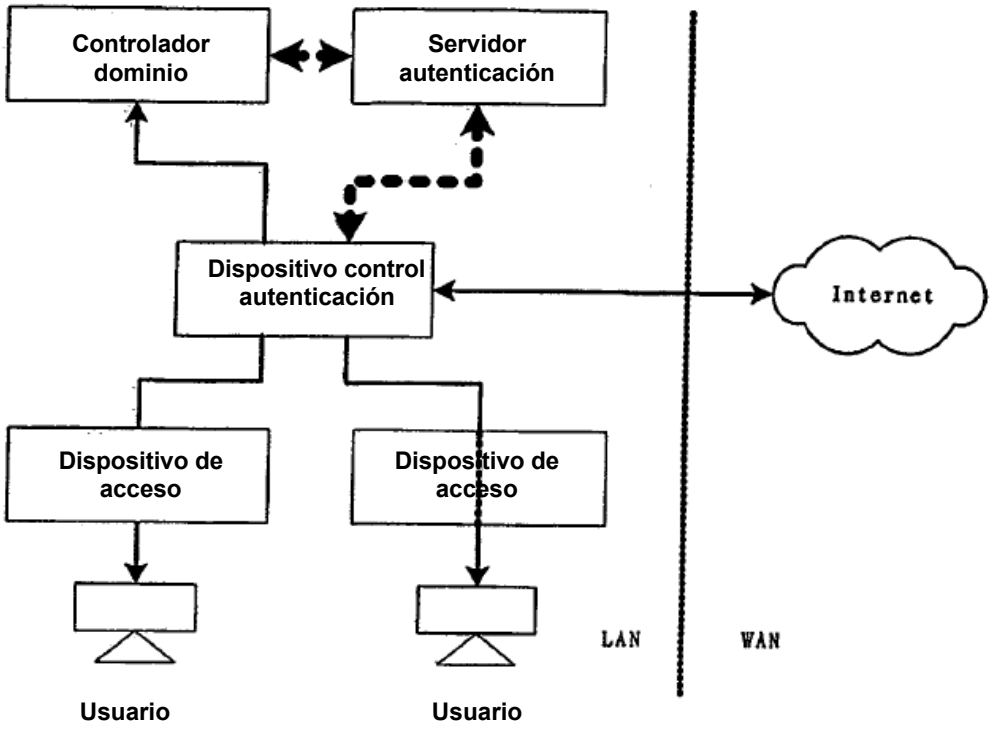
Controlador dominio
Servidor autenticación
Dispositivo control autenticación
Internet
Dispositivo de acceso
Dispositivo de acceso
LAN
WAN
Usuario
Usuario

Figura 1

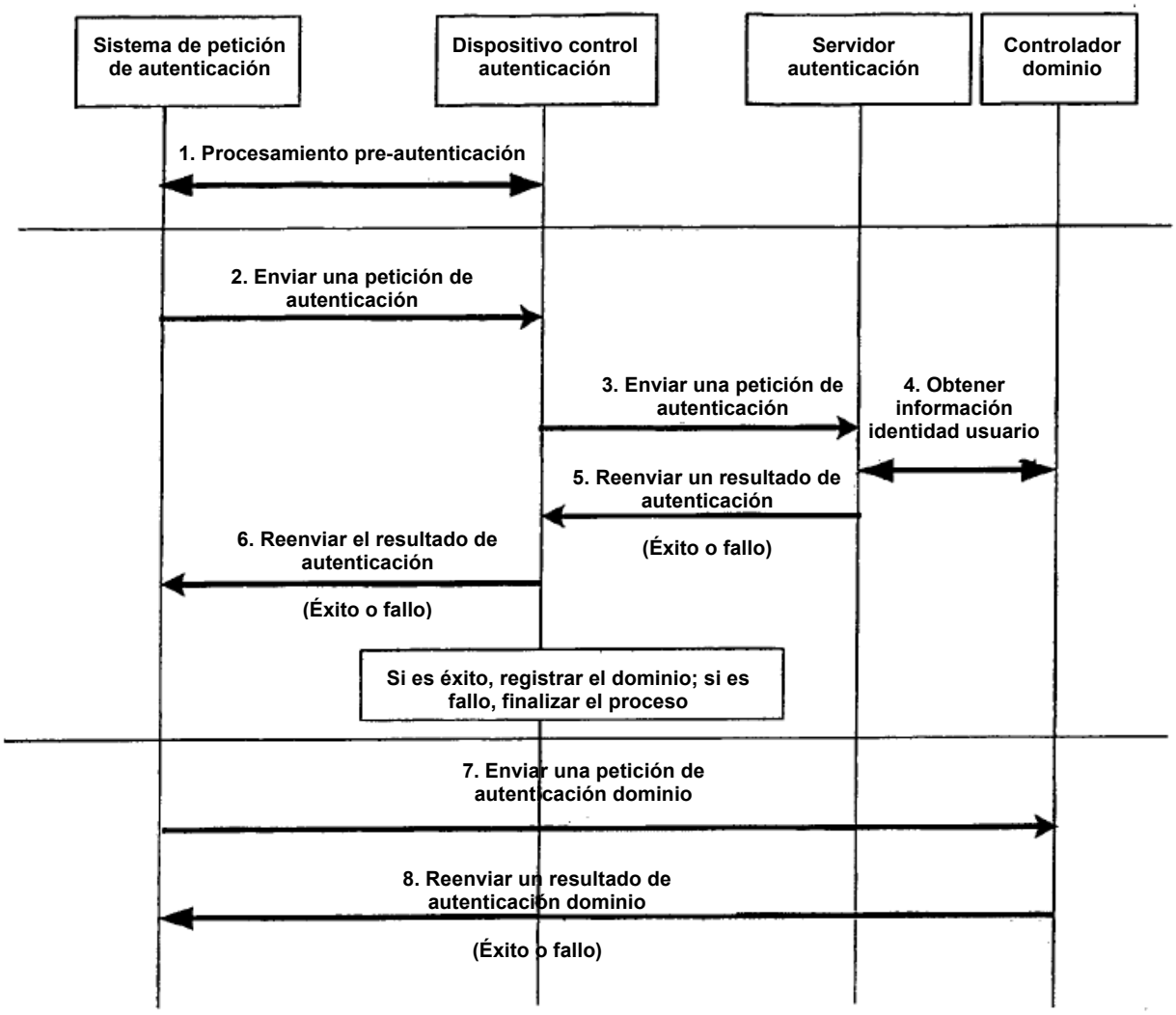
Sistema de petición de autenticación
Dispositivo control autenticación
Servidor autenticación
Controlador dominio
1. Procesamiento pre-autenticación
2. Enviar una petición de autenticación
3. Enviar una petición de autenticación
4. Obtener información identidad usuario
5. Reenviar un resultado de autenticación
(Éxito o fallo)
6. Reenviar el resultado de autenticación
(Éxito o fallo)
Si es éxito, registrar el dominio; si es fallo, finalizar el proceso
7. Enviar una petición de autenticación dominio
8. Reenviar un resultado de autenticación dominio
(Éxito o fallo)

Figura 2

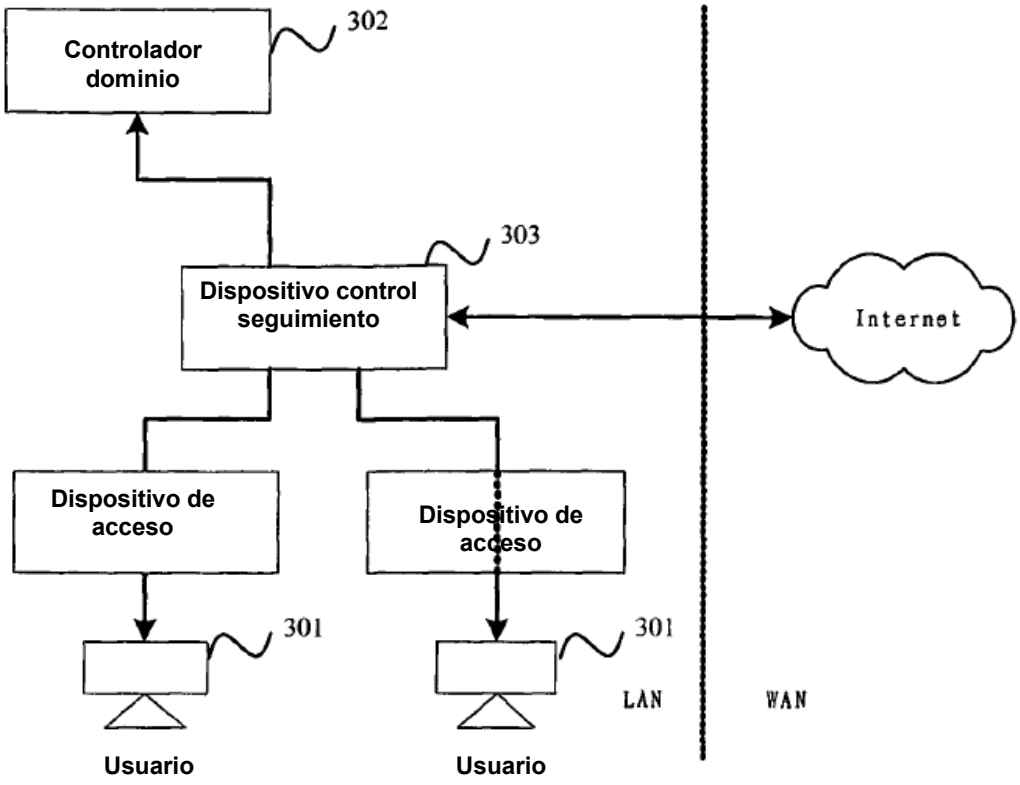

Figura 3

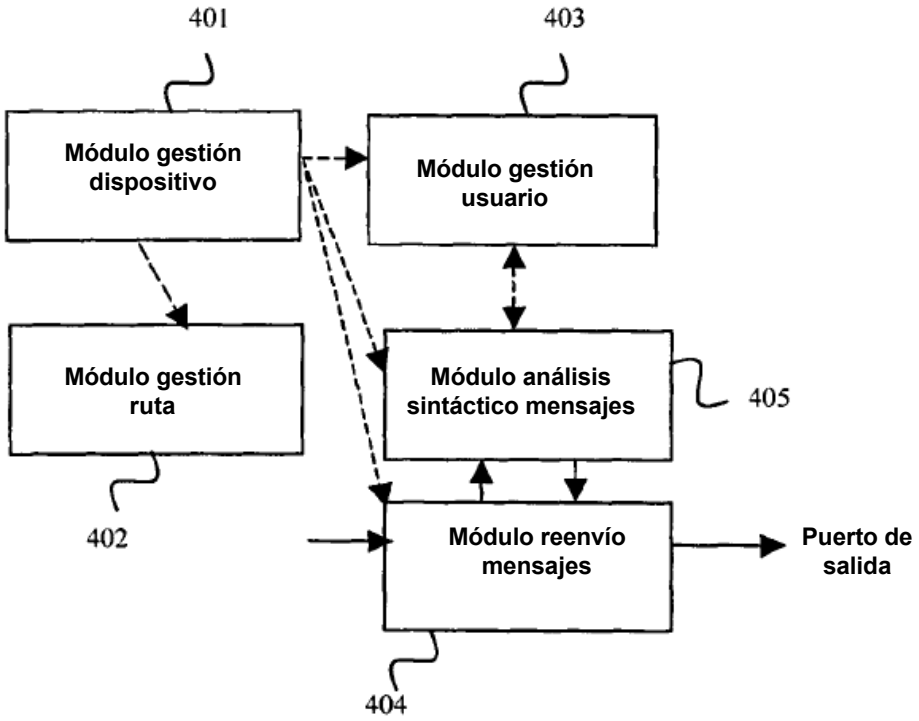

Figura 4

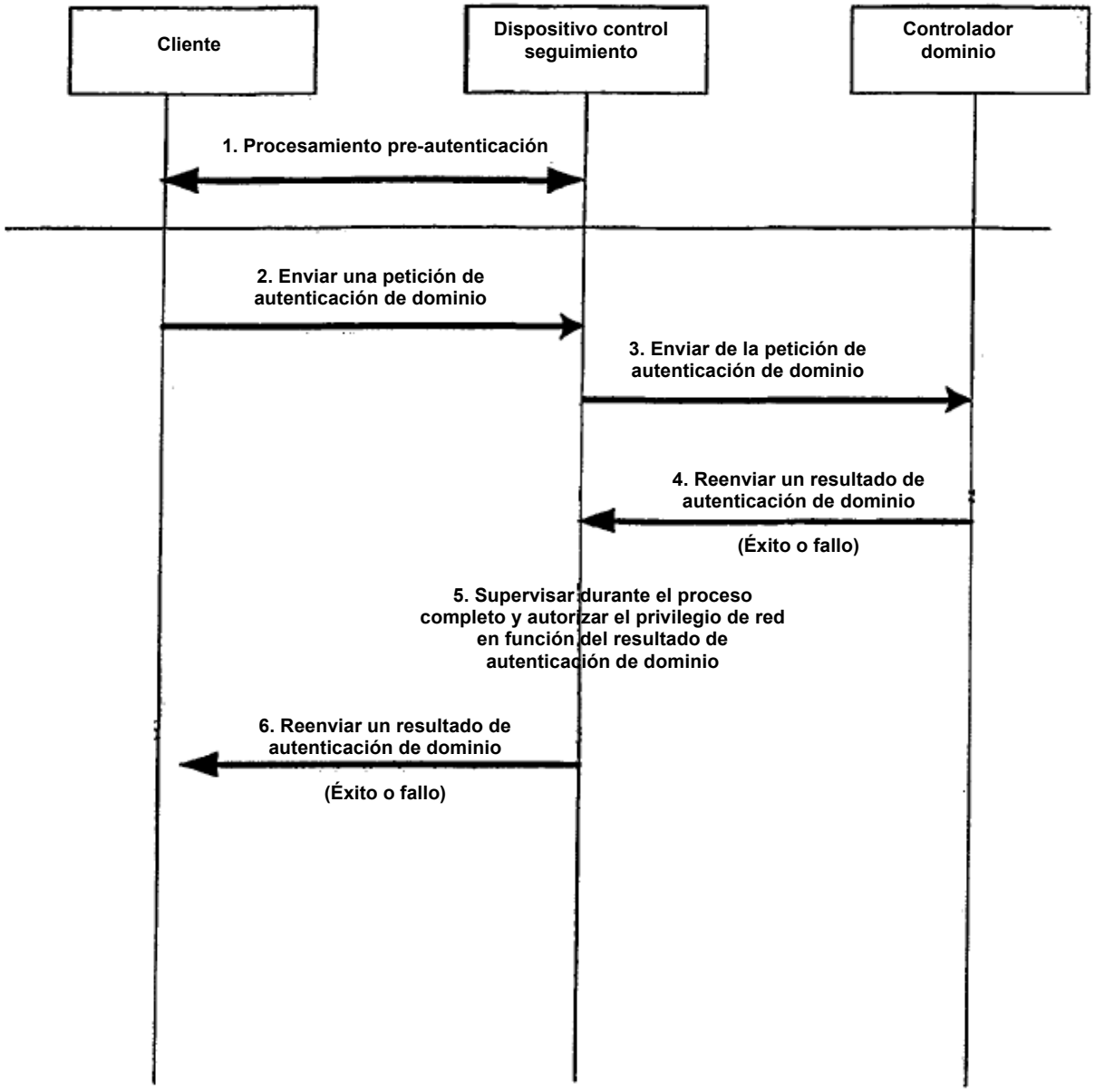
Cliente
Dispositivo control seguimiento
Controlador dominio
1. Procesamiento pre-autenticación
2. Enviar una petición de autenticación de dominio
3. Enviar de la petición de autenticación de dominio
4. Reenviar un resultado de autenticación de dominio
(Éxito o fallo)
5. Supervisar durante el proceso completo y autorizar el privilegio de red en función del resultado de autenticación de dominio
6. Reenviar un resultado de autenticación de dominio
(Éxito o fallo)

Figura 5