(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 435 574**

(51) Int. CI.:

***H04L 12/24*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.09.2009 E 09815626 (8)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2013 EP 2326047**

(54) Título: **Método para configurar y gestionar terminales y dispositivo terminal**

(30) Prioridad:

**28.09.2008 CN 200810169526**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**20.12.2013**

(73) Titular/es:

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

(72) Inventor/es:

**CHAI, XIAOQIAN y**
**TIAN, LINYI**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Método para configurar y gestionar terminales y dispositivo terminal

**Campo de la tecnología**

La presente invención está relacionada con el campo de las tecnologías de comunicaciones y, más en particular, con un método para la configuración y gestión de terminales, y con un dispositivo terminal.

**Antecedentes de la invención**

Con el aumento de los servicios de comunicaciones móviles, la complejidad de los terminales móviles aumenta continuamente, y la demanda para la gestión y configuración por el aire (OTA) de los terminales móviles, se hace cada vez más urgente. Con el fin de conseguir una gestión OTA segura de los terminales móviles, la Alianza de Móviles Abiertos (OMA) ha desarrollado un protocolo para la Gestión de Dispositivos (DM), que proporciona principalmente un conjunto de mecanismos de comunicaciones basados en la sesión, entre un servidor de gestión y un terminal gestionado, incluyendo un mecanismo de la sesión de gestión, la seguridad de la sesión de gestión, el formato y restricción del mensaje de gestión en una sesión de gestión, y el modelo de datos – Objeto de Gestión (MO). Con el fin de realizar funciones específicas de gestión en el terminal, se ha desarrollado un modelo de datos de aplicaciones – Objeto de Gestión, por ejemplo un Objeto de Gestión de Actualización de Firmware (FUMO) y un Objeto de Gestión de Componentes de Software (SCOMO), sobre la base del protocolo DM.

Un dispositivo terminal que admita la función DM de OMA debe tener un cliente DM (software), que sea responsable de la resolución del protocolo DM de OMA, de la gestión de la sesión, y de la seguridad de la sesión. El dispositivo que admite la función DM de OMA debe incluir además una estructura de datos – Árbol de Gestión de Dispositivos (DMT), donde la DMT organiza todos los objetos de gestión disponibles en el dispositivo conjuntamente, y todos los nodos de la DMT pueden ser localizados por una exclusiva Identidad de Recursos Unificados (URI).

El DM de OMA completa la gestión por medio de dos procesos: Uno es un proceso de configuración inicial (Arranque), para configurar un dispositivo desde un estado inmanejable a un estado manejable, configurando principalmente una cuenta en el servidor, y también puede ser configurada la información tal como los parámetros de conexión; y el otro es un proceso de gestión para completar la gestión subsiguiente.

En la implementación de la presente invención, el inventor averigua que la técnica anterior tiene al menos los siguientes defectos técnicos. En la técnica anterior, el terminal no puede determinar si una configuración es adecuada para el terminal durante la configuración, y el terminal no puede realizar la configuración eficazmente. Al mismo tiempo, el terminal necesita realizar la negociación o intenta determinar qué versión de protocolo se utiliza para iniciar una sesión, lo cual hace que la sesión sea más compleja. Además, durante la gestión subsiguiente, el terminal puede tener múltiples trozos de información de autenticación, y es más bien difícil que el servidor y el terminal determinen que se utiliza la misma información de autenticación para un mensaje de disparo de la sesión, aumentando así la dificultad de que el terminal autentique el mensaje de disparo de la sesión. Además, el terminal solamente puede autenticar y procesar un solo mensaje de configuración de parámetros, de manera que la eficiencia es muy baja, y la carga en el terminal y en el servidor es muy grande.

La Sesión Iniciada por Notificación de Gestión de Dispositivos OMA, 23-02-2007, divulga el paquete de Iniciación de Notificación de Gestión de Dispositivos OMA desde el servidor. Un servidor de gestión puede utilizar esta capacidad de notificación para provocar que el cliente inicie una conexión de vuelta al servidor de gestión.

Los Objetos Estandarizados de Gestión de Dispositivos de OMA, 09-02-2007, divulga un conjunto de objetos de gestión. Los objetos se definen utilizando el Marco de Descripciones de Dispositivos DM de OMA.

El Arranque de Gestión de Dispositivos de OMA, 09-02-2007, define cómo un dispositivo DM de OMA se lleva desde un estado “limpio” a un estado en el que es capaz de iniciar una sesión de gestión con un servidor suministrado para la gestión.

La Versión 1.1 del Contenido de Aprovisionamiento de OMA, 20-07-2004, define la codificación del contenido por el que los parámetros de configuración son presentados al cliente WAP en el marco de aprovisionamiento.

La Seguridad de Gestión de Dispositivos de OMA, 26-02-2007, proporciona una descripción de la seguridad de la capa de transporte, la seguridad de la capa de aplicaciones, etc. También describe los mecanismos de seguridad que se utilizan para proporcionar la integridad, la confidencialidad y la autenticación.

El documento WO2008/060042 divulga una transmisión segura de un mensaje de gestión de dispositivos a través de un canal de difusión (BCAST), por el cual el servidor de BCAST puede transmitir con seguridad un mensaje de gestión de dispositivos que incluye un valor de autenticación para una pluralidad de terminales, a través de un canal unidireccional BCAST, y consecuentemente no se requiere que los terminales usen un canal independiente para autenticar el mensaje de gestión de dispositivos recibido desde el servidor BCAST.

El documento WO2008/022195 divulga un servidor de gestión de dispositivos que utiliza protocolos de transporte tanto de punto a punto como de difusión, para gestionar a distancia una pluralidad de dispositivos electrónicos. El servidor utiliza extensiones para un protocolo de gestión de dispositivos estándar para acceder, a través de un protocolo de transporte punto a punto, información de gestión de dispositivos en la memoria del dispositivo electrónico. La información de gestión de dispositivos permite que el dispositivo electrónico reciba información utilizando el protocolo de transporte de difusión.

**Sumario de la invención**

Los modos de realización de la presente invención proporcionan un método y un sistema para la configuración y gestión de terminales.

Un método de configuración y gestión de terminales, proporcionado por un modo de realización de la presente invención incluye los pasos siguientes.

Se configura una cuenta del servidor DM en un terminal, donde la cuenta del servidor DM incluye un identificador del servidor DM e información de autenticación.

Se genera un mensaje de configuración, basado en el protocolo DM, por medio del servidor DM, donde el mensaje de configuración transporta el identificador del servidor DM, una versión del protocolo usado, una orden de gestión, un valor objetivo de la configuración, e información de autenticación de la identidad del servidor DM, donde el mensaje de configuración se utiliza para la configuración o gestión de parámetros, el valor objetivo de la configuración es un objeto de gestión, y el transporte del valor de la configuración objetivo en el mensaje de configuración incluye específicamente: la secuencia del objeto de gestión, proporcionando un camino virtual al objeto de gestión secuenciado.

El mensaje de configuración es recibido por el terminal a través de un canal de difusión. La información de autenticación se extrae desde la cuenta del servidor DM, de acuerdo con el identificador del servidor DM, y el mensaje de configuración es autenticado utilizando la información de autenticación.

Si la autenticación tiene éxito, se determina un camino básico en el DMT del terminal, de acuerdo con el camino virtual del mensaje de configuración, donde el servidor DM tiene el derecho de ejecutar la orden de gestión transportada en el mensaje de configuración bajo el camino básico, que fue decidido determinando el derecho al control de acceso del servidor DM a un nodo objetivo de gestión en el DMT del terminal, de acuerdo con el identificador del servidor DM, y la orden de gestión transportada en el mensaje de configuración es ejecutada basándose en el derecho al control de acceso.

Un modo de realización de la presente invención proporciona además un sistema para la configuración y gestión de terminales, donde el sistema incluye un servidor DM, un cliente de difusión y un cliente DM.

El servidor DM está adaptado para generar un mensaje de configuración que está basado en un protocolo DM, donde el mensaje de configuración transporta un identificador de servidor DM del servidor DM, una versión del protocolo usado, una orden de gestión, un valor objetivo de la configuración, una información de autenticación de la identidad del servidor DM, donde el mensaje de configuración se utiliza para la configuración o gestión de parámetros, el valor objetivo de la configuración es un objeto de gestión, y el transporte del valor objetivo de la configuración del mensaje de configuración incluye específicamente: la secuencia del objeto de gestión, proporcionando un camino virtual al objeto de gestión secuenciado.

El cliente de difusión está adaptado para recibir un mensaje de configuración entregado a través de un canal de difusión, identificar el mensaje de acuerdo con el tipo de mensaje de configuración, y reenviar el mensaje al cliente DM.

El cliente DM está adaptado para autenticar el servidor DM de acuerdo con el identificador del servidor DM y un tipo de autenticación que son transportados en el mensaje de configuración, determinar un camino básico en el Árbol de Gestión de Dispositivos, DMT, del terminal, de acuerdo con el camino virtual del mensaje de configuración, si la autenticación tiene éxito, donde el servidor DM tiene el derecho de ejecutar la orden de gestión transportada en el mensaje de configuración bajo el camino básico, que fue decidido determinando, de acuerdo con el identificador del servidor DM, un derecho al control de acceso del servidor DM a un nodo de gestión objetivo en el DMT del terminal, y ejecutar, basándose en el derecho al control de acceso, la orden de gestión transportada en el mensaje de configuración.

Para concluir, en las soluciones técnicas proporcionadas en modos de realización de la presente invención, cuando se realiza la configuración inicial, de acuerdo con la información de la versión del protocolo admitida o correspondiente con el servidor correspondiente y transportada en el fichero de configuración, el terminal puede identificar una versión del protocolo correspondiente a un fichero de configuración, de manera que el terminal puede determinar si el paquete es adecuado para el terminal, y de esa manera realizar una configuración correcta. Cuando

el terminal es capaz de admitir una pluralidad de versiones de protocolo, el terminal puede determinar, de acuerdo con la información de la versión del protocolo admitida o correspondiente al servidor correspondiente y transportada en el paquete de configuración, un protocolo que debería ser usado para la comunicación con el servidor, eliminando así el problema del aumento del tráfico de comunicaciones debido a diferentes versiones de protocolo.

Además, a través del método de configuración de parámetros en lotes, se pueden completar eficazmente la entrega segura de las operaciones generales de gestión por lotes, tal como la configuración de parámetros, mejorando así la eficiencia del funcionamiento, reduciendo la ocupación del canal, y aligerando la carga del servidor.

**Breve descripción de los dibujos**

La figura 1 es un diagrama esquemático que ilustra un diagrama de flujo de la configuración de terminales, de acuerdo con un modo de realización de la presente invención;

La figura 2 es un diagrama esquemático que ilustra un diagrama de flujo de la configuración de terminales, de acuerdo con un modo de realización de la presente invención;

La figura 3 es un diagrama esquemático que ilustra un diagrama de flujo de la configuración de terminales, de acuerdo con otro modo de realización de la presente invención;

La figura 4 es un diagrama esquemático que ilustra un diagrama de flujo de la configuración de terminales, en un modo de difusión, de acuerdo con un modo de realización de la presente invención;

La figura 5 es una vista esquemática estructural de un terminal, de acuerdo con un modo de realización de la presente invención; y

La figura 6 es una vista esquemática estructural de un sistema de configuración de parámetros, de acuerdo con un modo de realización de la presente invención.

**Descripción detallada de los modos de realización**

Los modos de realización de la presente invención proporcionan un método para la configuración y gestión de terminales, donde el método se describe con referencia a algunos ejemplos de modos de realización.

En el DM de OMA, un DMT de un terminal es un interfaz entre un servidor DM (en adelante denominado servidor) y el terminal. Con el fin de establecer una sesión de gestión entre el servidor y el terminal y completar la autenticación de la capa de aplicaciones, antes de realizar la gestión subsiguiente, un dispositivo necesita transitar desde un estado inmanejable a un estado manejable, y en el DM del OMA, el proceso es denominado configuración inicial (Arranque), y es principalmente para configurar la información de la cuenta en el servidor para el terminal.

Haciendo referencia a la figura 1, un método para la configuración y gestión de terminales de acuerdo con un primer modo de realización de la presente invención incluye los pasos siguientes.

En el paso S01, se adquiere un fichero de configuración, donde el fichero de configuración transporta información de la cuenta en el servidor e información de la versión del protocolo de la sesión admitida o seleccionada por un servidor correspondiente a la cuenta del servidor.

Específicamente, el fichero de configuración es adquirido en un modo PULL, y antes de adquirir el fichero de configuración, se adquiere primero una dirección del fichero de configuración, y después se adquiere el fichero de configuración de acuerdo con la dirección. Si la dirección es una dirección de solicitud, se envía un mensaje de solicitud a la dirección solicitada para adquirir el fichero de configuración, donde el mensaje de solicitud transporta además uno o más de los siguientes: un identificador del terminal, información del abonado al servicio, un código de autenticación de la identidad del abonado, información del dispositivo y una versión DM admitida, y el servidor selecciona el fichero de configuración, de acuerdo con la información transportada y entrega el fichero de configuración al terminal.

El fichero de configuración incluye la información de la versión del protocolo de la sesión admitida por el servidor correspondiente.

En el paso S02, la información de la cuenta del servidor en el fichero de configuración adquirido, es configurada sobre un DMT del terminal.

El método de configuración es: determinar una posición en el DMT, y establecer la correspondencia en la información de la cuenta del servidor determinada para que sea un caso en la posición de Objeto de Gestión en la Cuenta de Gestión de Dispositivo (DMAcc).

Si el fichero de configuración adquirido incluye la información de la versión del protocolo de la sesión admitida por el

servidor correspondiente, se extrae la información de la versión del protocolo de la sesión, se determina si la cuenta del servidor es adecuada para el terminal, y se configura la cuenta cuando la cuenta es adecuada para el terminal. Se establece una correspondencia en la información de la versión del protocolo de la sesión para que sea un valor o un campo de un nodo-hoja del caso del Objeto de Gestión de la DMAcc.

En el paso S03, basándose en la cuenta configurada del servidor, se establece una sesión de gestión con el servidor, y se realiza la gestión y configuración subsiguientes en el terminal.

Tras haber completado la configuración, el terminal puede establecer una sesión de gestión con el servidor. La sesión de gestión puede ser disparada por el terminal o por el servidor. Si la sesión es disparada por el servidor, la información de la cuenta configurada debe incluir información de autenticación utilizada por un mensaje de disparo de la sesión, con el fin de utilizar la información de autenticación para autenticar el mensaje de disparo de la sesión. Con el fin de completar la autenticación, se necesita diseñar un tipo de autenticación por adelantado, o el mensaje de disparo transporta un tipo de autenticación o un nombre de autenticación, se predetermina una regla de determinación del tipo de autenticación, y se determina el tipo de autenticación de acuerdo con la regla, de manera que el terminal autentica el mensaje de disparo de acuerdo con el tipo de autenticación.

Después de haber completado la configuración, cuando se inicia la sesión de gestión, el terminal puede determinar, de acuerdo con la información de la versión del protocolo de la sesión en correspondencia con la DMAcc del DMT y la versión del protocolo admitida por el terminal, una versión de protocolo de sesión adecuado para el terminal y el servidor, e iniciar un mensaje de solicitud de sesión de acuerdo con la versión del protocolo de la sesión.

En este modo de realización, se puede identificar una versión de protocolo correspondiente a un fichero de configuración, de acuerdo con la información de la versión del protocolo admitida o correspondiente a un servidor correspondiente y transportada en el fichero de configuración, de manera que el terminal puede determinar un protocolo que deba ser utilizado para la comunicación con el servidor, de manera que se realice una configuración correcta, eliminando así el problema del aumento de tráfico de las comunicaciones debido a diferentes versiones del protocolo.

Haciendo referencia a la figura 2, un método para la configuración y gestión de acuerdo con un segundo modo de realización incluye los pasos siguientes.

En el paso S11, se adquiere un fichero de configuración, donde el fichero de configuración transporta uno o más trozos de información de la cuenta del servidor, y al mismo tiempo transporta la información de la versión del protocolo de la sesión admitida o seleccionada por un servidor correspondiente a cada información de cuenta. Además, la información de la versión del protocolo de la sesión es transportada en la correspondiente información de cuenta del servidor, y la información de la versión del protocolo de la sesión es uno o más valores de la versión del protocolo.

El método de adquisición incluye lo siguiente: un dispositivo terminal lee el fichero de configuración construido en una tarjeta de Módulo de Identidad del Abonado (SIM)/Módulo de Identidad Universal del Abonado (USIM), o bien el dispositivo terminal adquiere el fichero de configuración desde una entidad externa, a través de un interfaz local (tal como Bluetooth, Infrarrojos, y USB), o un lado de la red empuja el fichero de configuración al dispositivo terminal en un modo PUSH, o bien el terminal solicita el fichero de configuración desde el lado de la red en un modo PULL.

El método para solicitar el fichero de configuración en el modo PULL incluye los pasos siguientes.

1) El terminal adquiere una dirección del fichero de configuración. La información de la dirección puede ser almacenada, sin estar limitado a ello, en una tarjeta SIM/USIM por adelantado, por medio de un emisor de tarjetas SIM/USIM. Cuando se adquiere la dirección, la información de encriptado de seguridad puede ser adquirida también, donde la información de encriptado de seguridad es para que el terminal realice subsiguientemente en el fichero de configuración, la autenticación de la integridad del contenido y la confidencialidad, y puede ser un certificado en el servidor.

2) El terminal adquiere el fichero de configuración de acuerdo con la dirección, que es específicamente como sigue.

Si la dirección es un Localizador de Recursos Universales (URL) del fichero de configuración, el terminal descarga directamente el fichero de configuración, por ejemplo, utilizando un Protocolo de Transferencia de Hipertexto (HTTP).

Si la dirección es una dirección de solicitud (es decir, una dirección de acceso del servidor, donde se solicita a través de la dirección de acceso el fichero de configuración desde el servidor), el terminal envía, a la dirección solicitada, un mensaje de solicitud para adquirir el fichero de configuración, donde el mensaje de solicitud puede ser un mensaje HTTP, y puede transportar uno o más de lo siguiente: un identificador del terminal (tal como la Identidad Internacional del Equipo Móvil (IMEI) y el Número de Serie Electrónico (ESN)), información de abonado al servicio (tal como un identificador público de usuario), un código de autenticación de la identidad del abonado (información

asignada por el lado de la red al abonado, para identificar la identidad del abonado, por ejemplo, un código de autenticación de la identidad, después de haber sido solicitado por el usuario a través del identificador público, entregado por el lado de la red al terminal a través del Servicio de Mensajes Cortos (SMS) u otros medios), información del dispositivo (tal como el tipo de dispositivo, la versión del sistema operativo, la versión del firmware), y una versión DM admitida. Tras recibir el mensaje de solicitud, el servidor identifica la identidad del terminal de acuerdo con la información transportada y selecciona un fichero de configuración adecuado para el terminal, donde el fichero de configuración está organizado en el formato del Perfil de Aprovisionamiento de Clientes o el Perfil de Objetos de Gestión, y entrega el fichero de configuración al terminal, tras realizar el proceso de integridad y confidencialidad en el fichero de configuración.

En el método anterior, el servidor identifica la identidad del terminal de acuerdo con el código de autenticación de la identidad del abonado y la información de abonado al servicio; y el servidor selecciona el fichero de configuración adecuado para el terminal, de acuerdo con el identificador del terminal, la información del dispositivo, la información de abonado al servicio, o la versión DM admitida.

El método PULL puede ser utilizado para adquirir cualquier fichero de configuración para la configuración inicial DM de OMA.

Con el método PULL, el correspondiente fichero de configuración del servidor puede ser actualizado directamente después de haber actualizado el servidor o después de averiguar que la información configurada es errónea, de manera que el fichero de configuración entregado al terminal es el último, eliminando así el coste de notificar al terminal y de volver a entregar un nuevo fichero de configuración cuando el servidor configura el fichero de configuración al terminal por adelantado y se averigua que le información de la cuenta es errónea o que el servidor se ha actualizado.

En el paso S12, se extrae la información de la versión del protocolo de la sesión admitida o seleccionada por el servidor y transportada en el fichero de configuración.

En el paso S13, basándose en la información de la versión del protocolo de la sesión extraída y en la versión del protocolo admitida por el propio terminal, se decide si la cuenta del servidor es adecuada para el terminal, y se configura la información de la cuenta del servidor si la cuenta del servidor es adecuada para el terminal.

Además, la decisión sobre si la cuenta del servidor es adecuada para el terminal, incluye el paso siguiente.

Se determina si la versión del protocolo admitida por el terminal se corresponde con la versión del protocolo de la sesión extraída (si ambas partes admiten múltiples versiones, se determina si los conjuntos de la versión admitida tienen una intersección). Si la versión del protocolo admitida por el terminal no se corresponde con la versión del protocolo de la sesión extraída, se determina que la cuenta no es adecuada para el terminal, y si existe otra información de la cuenta, se busca continuamente una cuenta adecuada en el servidor; si no existe otra información de la cuenta, el proceso de configuración termina. Si la versión del protocolo admitida por el terminal es la correspondiente a la versión del protocolo de la sesión extraída, se determina que la cuenta del servidor correspondiente al elemento es adecuada para el terminal. Si el mismo servidor en el mismo fichero de configuración tiene múltiples cuentas de servidor adecuadas para el terminal, se selecciona para la configuración una cuenta de servidor que admita la última versión del protocolo.

Específicamente, la configuración puede incluir los pasos siguientes.

Se determina una posición en un DMT, se establece una correspondencia entre la información de la cuenta del fichero de configuración con un caso de la posición en el Objeto de Gestión de DMAcc, y se establece una correspondencia en uno o más valores de la versión del protocolo transportados en la información de la cuenta para que sea un valor o campo de un valor de uno o más nodos-hoja del caso del Objeto de Gestión de DMAcc. Si existen otros objetos de gestión relacionados (por ejemplo, objetos de gestión de parámetros de conexión), se establece también una correspondencia en los objetos de gestión relacionados con respecto al DMT. Los derechos de obtención, sustitución, eliminación de los nodos de los objetos de gestión de la correspondencia son concedidos al servidor correspondiente de la cuenta del servidor.

En el paso S14, después de que la configuración haya tenido éxito, cuando se necesita establecer una sesión de gestión, el terminal determina, de acuerdo con la información de la versión del protocolo de la sesión cuya correspondencia se ha establecido sobre la DMAcc en el DMT y la versión del protocolo admitida por el terminal, una versión del protocolo de la sesión adecuado para el terminal y el servidor, e inicia un mensaje de solicitud de acuerdo con la versión del protocolo de la sesión.

El paso de determinar la versión del protocolo de la sesión adecuada para el terminal y el servidor puede ser: determinar una intersección del conjunto de versiones del protocolo admitida por el terminal y el conjunto de versiones del protocolo de la sesión de la DMAcc, si la intersección incluye solamente una versión del protocolo, determinar el inicio de la sesión con esta versión del protocolo, y si la intersección incluye múltiples versiones del

protocolo, se selecciona la última versión para iniciar la sesión. El servidor utiliza como respuesta la misma versión del protocolo, y subsiguientemente utiliza el protocolo para la interacción. Si el servidor desea utilizar un protocolo de otra versión para la sesión, se puede efectuar la negociación en sesiones subsiguientes.

Con el método para transportar la información de la versión del protocolo de la sesión admitida o seleccionada por el servidor en la información de la cuenta del servidor, de acuerdo con los modos de realización de la presente invención, antes de configurar la cuenta del servidor para el terminal, el terminal puede determinar por adelantado si el servidor es adecuado para el terminal, evitando así configurar una cuenta en el servidor no adecuada para el terminal y reduciendo el subsiguiente coste del proceso y, al mismo tiempo, la versión del protocolo admitida por el servidor habilita también al terminal para determinar una versión de protocolo de la sesión adecuada, antes de iniciar la sesión, reduciendo así el coste de la negociación subsiguiente sobre la versión del protocolo de la sesión.

Después de haber configurado la información de la cuenta en el servidor, se puede establecer una sesión de gestión entre el servidor y el terminal. La iniciación de la sesión de gestión puede ser iniciada activamente por el terminal, o iniciada por el servidor. Si la sesión de la gestión es iniciada activamente por el terminal, el terminal se conecta directamente al servidor y envía un mensaje de solicitud para solicitar una sesión, donde el mensaje de solicitud puede implementarse basándose en un protocolo tal como el HTTP, el Protocolo de Sesión Inalámbrica (WSP), el Intercambio de Objetos (OBEX), o un Protocolo de Inicio de Sesión (SIP). Si la sesión de gestión es iniciada por el servidor, como el servidor apenas puede conectarse directamente con el terminal, un método común utilizado es que el servidor entregue y envíe un mensaje de disparo de la sesión al terminal, a través del SMS, de un Impulso del Protocolo del Aplicaciones Inalámbricas (WAP Push), o un impulso de SIP (SIP Push), donde el mensaje de disparo transporta información tal como la información de autenticación de la identidad del servidor, el identificador del servidor, el identificador de la sesión, y el iniciador de la sesión, y el terminal inicia una solicitud de sesión de acuerdo con el mensaje de disparo para establecer la sesión de gestión con el servidor. La información de la cuenta del servidor configurada puede tener múltiples trozos de información de autenticación correspondientes a diferentes tipos de autenticación. Los tipos de autenticación incluyen por ejemplo syncml:auth-basic, y syncml:auth-md5, y el terminal adopta un tipo de autenticación para generar la información de autenticación, y el tipo de autenticación adoptado puede ser un tipo de autenticación preferido designado en la cuenta configurada. Si no se designa un tipo de autenticación preferido en la cuenta del servidor configurada, se puede utilizar el tipo de autenticación negociado por la última sesión. Si el servidor considera que el tipo de autenticación adoptado por el terminal no es adecuado, el servidor puede enviar un Reto al terminal para designar un nuevo tipo de autenticación.

El mensaje de disparo de la sesión enviado por el servidor incluye un compendio y un mensaje de disparo (disparo), donde el compendio es un compendio MD5 y el método de generación es como sigue.

Compendio = H (B64 (H (identificador-servidor:contraseña)):código al azar: B64 (H (disparo)))

Aquí, H es una función de cifrado MD5, identificador-servidor es un identificador del servidor, código al azar es un número aleatorio de ataque anti-respuesta, B64 es una función de codificación de Base64, y contraseña es una contraseña de autenticación.

Como el terminal puede tener múltiples trozos de información de autenticación, y el servidor y el terminal no tienen un mecanismo de negociación, el servidor y el terminal apenas pueden utilizar la contraseña y el código al azar de la misma información de autenticación para procesar el mensaje de disparo durante la interconexión, aumentando así la dificultad de proceso para el terminal. Al mismo tiempo, como se debe utilizar un número aleatorio en el mensaje de disparo para impedir los ataques de reproducción, se necesita mantener la información de autenticación que tiene un código al azar para el mensaje de disparo. Después de haber configurado los parámetros, se puede procesar el mensaje de disparo utilizando los métodos siguientes.

Método 1: Se designa por adelantado la información de autenticación (correspondiente a un cierto tipo de autenticación) determinada por el mensaje de disparo (incluyendo lo estandarizado). La información de autenticación debe tener una contraseña y un número aleatorio, y puede no tener un nombre de usuario, y se puede utilizar la información de autenticación correspondiente al tipo de autenticación syncml:auth-md5 o syncml:auth-MAC. Si el terminal y el servidor admiten el mensaje de disparo para disparar la sesión de gestión, la información de autenticación debe existir en la información de la cuenta del servidor, configurada por el terminal, es decir, un nodo AppAuth de un caso de DMAcc correspondiente a la cuenta del servidor en el DMT debe tener información de autenticación con un valor AAuthType del tipo de autenticación.

Basándose en la información de autenticación designada por adelantado, el servidor genera un mensaje de disparo y entrega el mensaje de disparo al terminal a través de otros canales diferentes al de la sesión DM. El terminal extrae el identificador del servidor en el mensaje de disparo, y después lee la contraseña y el número aleatorio de la información de autenticación determinada en el caso del Objeto de Gestión de DMAcc, correspondiente al identificador del servidor configurado en el DMT, utiliza el identificador del servidor, la contraseña y el número aleatorio para generar un compendio MD5 para autenticar la validez y la integridad del mensaje de disparo (el algoritmo de generación es el mismo que el algoritmo de generación DIGEST (compendio) descrito anteriormente), e

inicia una solicitud de sesión para el servidor tras haber tenido éxito con la autenticación. Si se necesita usar la autenticación de la capa de aplicaciones, se utiliza un tipo de autenticación preferido en la información de la cuenta del servidor en la solicitud de la sesión, para generar la información de autenticación. Si no existe un tipo de autenticación preferido en la información de la cuenta, para efectuar la autenticación se utiliza el tipo de sesión usado con éxito en la última sesión.

Método 2. Se extrae el formato del mensaje para añadir un tipo de autenticación o un campo del nombre de la autenticación. El valor del campo del tipo de autenticación se corresponde con el valor del nodo AAuthType bajo el nodo AppAuth sobre el Objeto de Gestión DMAcc, y el valor del campo del nombre de autenticación es el correspondiente al valor del nodo AAuthName bajo el nodo AppAuth sobre el Objeto de Gestión DMAcc. El campo puede ser ampliado en una cabecera del mensaje (trigger-hdr) o un cuerpo de mensaje (trigger-body) del mensaje de disparo. Como el valor del tipo de autenticación es largo, puede ser codificado, y el campo ampliado por el mensaje de disparo transporta solamente el código, y puede transportar también directamente el valor del tipo de autenticación. Basándose en la extensión, el servidor transporta el tipo de autenticación o el nombre de la autenticación utilizado por el servidor en el mensaje de disparo entregado al terminal. Con el fin de admitir la extensión, la información de la cuenta del servidor configurada por el terminal debe incluir la información de autenticación correspondiente al tipo de autenticación o al nombre de la autenticación utilizado por el mensaje de disparo.

Basándose en el tipo de autenticación o en el campo del nombre de autenticación transportado en el mensaje de disparo, tras recibir el mensaje de disparo enviado por el servidor a través de otros canales diferentes al de la sesión DM, el terminal extrae el identificador del servidor y el tipo de la autenticación o la información del nombre de la autenticación en el mensaje de disparo, y después lee la contraseña y el número aleatorio de la información de autenticación correspondiente al tipo de autenticación o al nombre de la autenticación en el caso del Objeto de Gestión DMAcc correspondiente al identificador del servidor configurado en el DMT, utiliza el identificador del servidor, la contraseña y el número aleatorio para generar un compendio MD5 para autenticar la validez y la integridad del mensaje de disparo (el algoritmo de generación es el mismo que el algoritmo de generación DIGEST descrito anteriormente, y se puede utilizar también el nombre de la autenticación para sustituir el identificador del servidor en el algoritmo de generación del DIGEST, al tiempo que se mantienen inalterados otros elementos del algoritmo), e inicia una solicitud de sesión al servidor tras haber tenido éxito la autenticación. Si se necesita usar la autenticación de la capa de aplicaciones, se utiliza en la solicitud de la sesión un tipo de autenticación preferido en la información de la cuenta del servidor para generar la información de la autenticación. Si no existe un tipo de autenticación preferido en la información de la cuenta, para efectuar la autenticación se utiliza el tipo de sesión utilizado con éxito en la última sesión.

Método 3. El tipo específico de la información de autenticación utilizada por el servidor y el terminal no está limitado, pero la información de la cuenta del servidor configurada por el terminal debe incluir al menos un tipo de autenticación que tenga un código al azar. Al mismo tiempo, se predetermina una regla de determinación (incluyendo lo estandarizado) y el terminal y el servidor seleccionan un tipo de autenticación para el mensaje de disparo de la sesión, de acuerdo con la regla de determinación. Como tanto el servidor como el terminal conocen el tipo de autenticación incluido en la información de la cuenta del servidor, pueden habilitarse los dos para seleccionar el mismo tipo de autenticación basándose en la regla de determinación del tipo de autenticación. La regla de determinación del tipo de autenticación puede ser: efectuar una secuencia de los tipos de autenticación que tengan un código al azar (por ejemplo, de acuerdo con las prioridades), y seleccionar un tipo de autenticación de acuerdo con la secuencia.

Basándose en la regla de determinación predeterminada, el servidor determina un tipo de autenticación adecuado entre los tipos de autenticación de la información de la cuenta del servidor configurada para el terminal para generar un mensaje de disparo, y entrega el mensaje de disparo a través de otros canales diferentes al de la sesión DM. Por ejemplo, si la regla de determinación es “seleccionar syncml:auth-md5 y syncml:auth-MAC en secuencia”, la cuenta del servidor debe incluir uno de los dos tipos de autenticación y, en funcionamiento, el servidor determina el tipo de autenticación de acuerdo con el método siguiente: si la información de la cuenta del servidor incluye la información de autenticación del tipo de autenticación de syncml:auth-md5, el tipo de autenticación se determina que es el tipo de autenticación para el mensaje de disparo de la sesión; si la información de la cuenta del servidor no incluye la información de autenticación, del tipo de autenticación de syncml:auth-md5, syncml:auth-MAC, se determina que es el tipo de autenticación para el mensaje de disparo de la sesión.

El terminal extrae el identificador del servidor en el mensaje de disparo, y después determina, basándose en la misma regla de determinación, un tipo de autenticación del caso del Objeto de Gestión DMAcc correspondiente al identificador del servidor configurado en el DMT, lee la contraseña y el número aleatorio del tipo de autenticación, utiliza el identificador del servidor, la contraseña y el número aleatorio, para generar un compendio de MD5 para autenticar la validez y la integridad del mensaje de disparo (el algoritmo de generación es el mismo que el algoritmo de generación DIGEST descrito anteriormente), e inicia una solicitud de sesión al servidor tras haber tenido éxito con la autenticación. Si se necesita usar la autenticación de la capa de aplicaciones, se utiliza un tipo de autenticación preferido en la información de la cuenta del servidor en la solicitud de la sesión, para generar la información de

autenticación. Si no existe un tipo de autenticación preferido en la información de la cuenta, se utiliza el tipo de sesión utilizado con éxito en la última sesión, para efectuar la autenticación.

Método 4: El tipo de información de autenticación utilizado por el servidor y el terminal no está limitado, pero la información de la cuenta del servidor configurada por el terminal debe incluir al menos un tipo de autenticación que tenga un código al azar.

Basándose en la información de autenticación ilimitada, el servidor selecciona un tipo de autenticación que tiene un código al azar para generar un mensaje de disparo, y entrega el mensaje de disparo al terminal a través de otros canales diferentes al de la sesión DM.

El terminal extrae el identificador del servidor en el mensaje de disparo, y después lee la contraseña y el número aleatorio de un cierto tipo de autenticación que tenga un código al azar desde el caso del Objeto de Gestión DMAcc correspondiente al identificador del servidor configurado en el DMT, y utiliza el identificador del servidor, la contraseña y el número aleatorio para generar un compendio de MD5 para autenticar la validez e integridad del mensaje de disparo (el algoritmo de generación es el mismo que el algoritmo de generación DIGEST descrito anteriormente). SI falla la autenticación, se selecciona otro tipo de autenticación que tenga un código al azar para re-autenticar el mensaje de disparo, hasta que la autenticación tenga éxito o se hayan probado todos los tipos de autenticación que tengan un código al azar. Después de que la autenticación haya tenido éxito, se inicia una solicitud de sesión en el servidor. Si se necesita usar la autenticación de la capa de aplicaciones, se utiliza en la solicitud de la sesión un tipo de autenticación preferido en la información de la cuenta del servidor, para generar la autenticación. Si no existe un tipo de autenticación preferido en la información de la cuenta, se utiliza el tipo de sesión utilizado con éxito en la última sesión, para efectuar la autenticación.

En el método para procesar el mensaje de disparo, la información de la cuenta del servidor configurada puede transportar o no la información de la versión del protocolo de la sesión admitida o seleccionada por el servidor. El método puede ser usado también para el proceso del mensaje de disparo después de la configuración de la cuenta del servidor o de la Sincronización de Datos (DS) de OMA.

A través del método para procesar el mensaje de disparo, el servidor y el terminal están habilitados para usar la misma información de autenticación para procesar el mensaje de disparo durante la interconexión, reduciendo así la dificultad del proceso del terminal y, al mismo tiempo, se asegura que el cliente y el servidor que admiten el mensaje de disparo pueden siempre seleccionar la información de autenticación que tiene un número aleatorio, realizando así la función del mecanismo de ataque anti-reproducción del mensaje de disparo.

Un método de configuración de terminales de acuerdo con un tercer modo de realización de la presente invención es para conseguir la configuración y gestión por lotes basándose en la configuración de la cuenta. Como se ilustra en la figura 3, el método incluye los pasos siguientes.

En el paso S31, se configura una cuenta de servidor DM en un terminal, donde la cuenta del servidor DM incluye un identificador del servidor e información de autenticación de un servidor, donde la información de autenticación es la misma para todos los terminales.

En el paso S32, se recibe un mensaje de configuración (para la configuración o gestión de parámetros) generado al utilizar un protocolo DM a través de un canal de difusión, donde la cabecera del mensaje de configuración transporta el identificador del servidor, una versión del protocolo usado, y la información de autenticación de la identidad del servidor, que es la misma para todos los terminales.

En el paso S33, se determina si el terminal admite la versión del protocolo utilizada por el mensaje de configuración, y si el terminal admite la versión del protocolo utilizado por el mensaje de configuración, el mensaje de configuración se autentica de acuerdo con el identificador del servidor y la información de autenticación de la identidad del servidor.

En el paso S34, si la autenticación tiene éxito, se determina un camino básico (es decir, un camino básico en un DMT del terminal), de acuerdo con la información del camino virtual (es decir, la información del camino virtual en el DMT del terminal) de un objeto de gestión del mensaje de configuración, y el camino determinado debe satisfacer la condición siguiente: El servidor correspondiente al identificador del servidor transportado tiene el derecho de ejecutar una orden de gestión en el mensaje de configuración bajo el nodo del DMT del terminal, y la orden de gestión transportada en el mensaje de configuración se ejecuta bajo el camino básico.

Al igual que para el servidor, algunas tareas de configuración o tareas de gestión no necesitan diferenciar los terminales, por ejemplo, para la configuración de los parámetros de conexión, pues se configuran los mismos valores de los parámetros para todos los terminales. La configuración de los parámetros de conexión puede ser realizada para múltiples terminales al mismo tiempo, y la demanda para la interacción no es intensa. Para tales tareas, con el fin de reducir la ocupación del canal y aligerar la carga del servidor, se puede adoptar un modo de difusión/multidifusión.

Un método de configuración basado en el modo de difusión (similar al modo de multidifusión, y similar a la distribución de otras tareas de gestión por lotes), de acuerdo con un cuarto modo de realización, se describe a continuación con referencia a la figura 4.

En el paso S41, se configura una cuenta en el servidor DM para la gestión, a través de un canal de difusión sobre un DMT de un terminal, donde el servidor DM es responsable de generar un mensaje DM (es decir, un mensaje de configuración basado en un protocolo DM) para la configuración a través del canal de difusión. La cuenta incluye un identificador del servidor e información de autenticación del servidor, donde la información de autenticación es la misma para todos los terminales, y se puede utilizar un certificado de un servidor DM para completar la autenticación unidireccional (es decir, el terminal autentica el servidor DM). La cuenta puede incluir además una dirección de informes o un identificador del servidor de informes de un mensaje de gestión entregado a través del canal de difusión, para que el terminal informe un resultado de un proceso del mensaje DM recibido a través del canal de difusión. La configuración de la cuenta del servidor DM puede ser completada de las maneras siguientes.

En el paso S41a), se completa la configuración de la cuenta del servidor DM durante la configuración inicial, y la información de la cuenta se transporta en un fichero de configuración inicial adquirido por el terminal, y en correspondencia con un DMT del terminal durante la configuración.

En el paso S41b), se establece una sesión DM con el terminal, a través de otro servidor DM, y la cuenta del servidor se añade al DMT durante la sesión.

En al paso S42, tras haber completado la configuración, el servidor configurado genera un mensaje de configuración basado en el protocolo DM para la difusión, donde el mensaje de configuración transporta el identificador del servidor, una versión del protocolo usado, la información de autenticación de la identidad del servidor, una orden de gestión DM, y un valor objetivo de la configuración. El identificador del servidor es transportado en un elemento <Fuente>/<LocName> de la cabecera del mensaje, y el identificador se utiliza por el terminal para autenticar el servidor, y se utiliza también por el terminal para decidir sobre un derecho al control de acceso (es decir, la Lista de Control de Acceso (ACL)) del servidor a un nodo objetivo de gestión en el DMT. El valor de la configuración objetivo puede ser un objeto de gestión (consistente en uno o más nodos de gestión), y el método para transportar el valor de la configuración objetivo en el mensaje de configuración incluye, específicamente: efectuar la secuencia del objeto de gestión, proporcionar un camino virtual "./Inbox" para el objeto de gestión secuenciado, donde el camino relativo es el correspondiente a un objeto de gestión con un identificador de urn:oma:mo:oma-dm-inbox:1.0 en el DMT del terminal. El camino virtual instruye al terminal para que determine un camino básico de significación práctica (es decir, un camino básico en el DMT) de acuerdo con la situación del DMT, y para ejecutar la orden de gestión DM sobre el valor de configuración, basándose en el camino básico y en la ACL. En este caso, la orden de gestión DM es una orden de Añadir o Sustituir. Un ejemplo del mensaje se ofrece a continuación.

```
<SyncML xmlns='SYNCML:SYNCML1.2'>
  <SyncHdr>
    <VerDTD>1.2</VerDTD>
    <VerProto>DM/1.2</VerProto>
<Objetivo><LocURI>IMEI:493005100592800</LocURI></objetivo>
<Fuente>
 <LocURI>http://www.syncml.org/mgmt-server</LocURI>
<LocName><!--identificador del servidor, para que el terminal identifique el servidor para la autenticación y, al mismo tiempo, decidir sobre el derecho a la ACL→<LocName>
</Fuente>
<Cred>
  <Meta><Tipo xmls="syncml:metinf"><!--tipo de autenticación →</Tipo>
      <Format  xmlns='syncml:metinf'><!-- formato de información de autenticación--></Formato></Meta>
<Data><!-- valor de la información de autenticación --></Data>
    </Cred>
  </SyncHdr>
  <SyncBody>
```

```
<Añadir>
<CmdID>1</CmdID><!-- para que el terminal vuelva a un estado -->
<Item>
 <Objetivo><LocURI>./Inbox</LocURI></Objetivo>
        <Meta>
            <Format xmlns='syncml:metinf'>xml</Format>
            <Type
xmlns='syncml:metinf'>application/vnd.syncml.dmtnds+xml</Type>
        </Meta>
        <Data>
          <MgmtTree xmlns='syncml:dmddf1.2'>
            <VerDTD>1.2</VerDTD>
            <Node>
                <NodeName>MMS</NodeName>
                <RTProperties >
                    <Format><node/></Format>
                    <Type> <DDFName><!-- MOID --></DDFName></Type>
      </RTProperties>
      <Nodo><!-- contenido de subnodo -->< Nodo>
                </Node>
              </MgmtTree>
            </Data>
          </Item>
    <Add>
  </SyncBody>
</SyncML>
```

El servidor envía el mensaje de configuración generado y el tipo de mensaje (el tipo de mensaje DM es: application/vnd.syncml.dm+xml) a una Aplicación de Servicio BCAST (BSA), una Distribución/Adaptación de Servicio BCAST (BSD/A), o una Distribución/Adaptación de Servicio del sistema de Distribución de Difusión (BDS SD/A).

En el paso S43, el BSA, el BSD/A o el BDS SD/A cifra el contenido y envía el mensaje de configuración y el tipo de mensaje de configuración a un cliente de difusión a través de una red de difusión.

En el paso S44, tras recibir el mensaje de configuración, el cliente de difusión descifra el contenido del mensaje de configuración, y después determina, de acuerdo con el tipo de mensaje de configuración, un cliente al cual se ha de entregar el mensaje de configuración, y entrega el mensaje de configuración a un cliente DM.

El cliente DM procesa el mensaje de configuración y el método específico del proceso es como sigue.

En el paso S44a), se decide sobre si el terminal admite la versión del protocolo utilizada por el mensaje de configuración, y si el terminal admite la versión del protocolo utilizada por el mensaje de configuración, se efectúa el paso siguiente.

En el paso S44b, se extrae el identificador del servidor y el tipo de autenticación del mensaje, y después se autentica

el mensaje de configuración utilizando la información de autenticación del tipo de autenticación de la cuenta correspondiente al identificador del servidor configurado por el terminal, que es específicamente como sigue: El terminal extrae la información de autenticación en el correspondiente Objeto de Gestión DMAcc desde el DMT del terminal, de acuerdo con el identificador del servidor y el tipo de autenticación, utiliza la información de autenticación para generar los datos de autenticación, y compara si los datos de autenticación son los mismos que la información de autenticación de la identidad del servidor transportada en el mensaje de configuración y, si los datos de autenticación son los mismos que en la información de autenticación de la identidad del servidor transportada en el mensaje de configuración la autenticación tiene éxito; si los datos de autenticación son diferentes a la información de autenticación de la identidad del servidor transportada en el mensaje de configuración, la autenticación falla. Después de que la autenticación haya tenido éxito, se efectúa el paso siguiente.

En el paso S44c), el terminal aprende, de acuerdo con el "./Inbox" del mensaje de configuración, que el terminal necesita determinar un camino básico en el DMT, y determina un camino básico adecuado en el DMT, donde el camino básico debe satisfacer la condición siguiente: El servidor DM tiene el derecho de ejecutar la orden de gestión del mensaje de configuración bajo el camino básico. Un método para juzgar si el servidor DM tiene el derecho de ejecutar la orden de gestión en el mensaje de configuración bajo el camino básico es: determinar, de acuerdo con el identificador del servidor transportado en el mensaje de configuración, la orden de gestión transportada en el mensaje de configuración, y la ACL del nodo de gestión de DMT correspondiente al camino básico determinado, y si la ACL incluye el elemento de la orden de gestión, y el elemento incluye el identificador del servidor, se indica que el servidor DM tiene ese derecho.

En el paso S44d), la orden de gestión del mensaje de configuración se ejecuta bajo el camino básico.

El proceso de ejecución es específicamente como sigue: Si la orden de gestión transportada en el mensaje de configuración es Add (añadir), el objeto de gestión secuenciado se añade bajo el camino básico determinado del DMT (para configurar un nuevo valor de parámetro). Si ya existe un nodo de gestión bajo el camino completo, se juzga si se utiliza el mismo parámetro, y si se usa el mismo parámetro, la operación Add falla; si se usan parámetros diferentes, se renombra el nodo raíz del objeto de gestión a configurar, y el objeto de gestión se añade tras haber sido renombrado. Si la orden de gestión transportada en el mensaje de configuración es Replace (sustituir), el objeto de gestión secuenciado transportado en el mensaje de configuración se utiliza para actualizar el objeto de gestión existente bajo el camino básico determinado del DMT (para actualizar el valor del parámetro existente). Si no existe un nodo de gestión bajo el camino básico, la operación Replace falla.

Tras la configuración, el método incluye además un paso de activación del parámetro configurado.

En el paso S45 (que es opcional), tras haber ejecutado la orden de gestión en el mensaje de configuración (con éxito o con fallo), el cliente adquiere la dirección de informes o el identificador del servidor de informes incluido en la cuenta del servidor configurada. Si se adquiere la dirección de informes, se genera un mensaje HTTP u otro mensaje correspondiente y es enviado a la dirección de informes. Si se adquiere el identificador del servidor de informes, el terminal establece una sesión de gestión DM con el servidor correspondiente al identificador del servidor, e informa un resultado de la ejecución durante la sesión de gestión DM, donde el resultado de la ejecución informada incluye, por ejemplo, no tener derechos, versión incompatible y ejecución con éxito.

Durante la configuración, se puede completar eficazmente la configuración que no requiere diferenciar los terminales, utilizando el mecanismo DM, que no solamente puede asegurar la seguridad (la autenticación de la identidad del servidor y el control del derecho de acceso), sino también satisfacer los requisitos de localización de objetos de gestión de diferentes estructuras DMT e informes del resultado de la configuración, de manera que se puede completar de manera segura y eficaz la configuración de parámetros en lotes basándose en DM, mejorando así la eficiencia de la operación, reduciendo la ocupación del canal y aligerando la carga del servidor.

Haciendo referencia a la figura 5, un terminal 500 de acuerdo con un modo de realización de la presente invención incluye una unidad 510 de adquisición de ficheros de configuración, una unidad 520 de determinación de cuentas del servidor, una unidad 530 de configuración, una unidad 540 de proceso, una unidad 550 de determinación de la versión de la sesión, y una unidad 560 de autenticación de mensajes de disparo.

La unidad 510 de adquisición de ficheros de configuración está adaptada para adquirir un fichero de configuración. La unidad de adquisición incluye una unidad PULL para adquirir el fichero de configuración en un modo PULL. Cuando se adquiere el fichero de configuración, la unidad PULL envía, a un servidor de adquisición, una solicitud de adquisición que transporta información del terminal. El fichero de configuración puede transportar además información de la cuenta del servidor, y la información de la cuenta del servidor incluye información de la versión del protocolo de la sesión admitida por el servidor correspondiente.

La unidad 520 de determinación de la cuenta del servidor está adaptada para extraer la información de la versión del protocolo de la sesión y determinar si la cuenta del servidor es adecuada para el terminal, basándose en la información de la versión del protocolo de la sesión y una versión del protocolo admitido por el terminal.

La unidad 530 de configuración está adaptada para configurar la información de la cuenta del servidor determinada sobre un DMT del terminal, cuando se determina que la cuenta del servidor es adecuada para el terminal.

La unidad 540 de proceso está adaptada para establecer, basándose en la cuenta del servidor configurada, una sesión de gestión entre el terminal y el servidor, y efectuar la configuración y gestión subsiguientes en el terminal, durante la sesión.

La unidad 550 de determinación de la versión de la sesión está adaptada para determinar, cuando se inicia la sesión de gestión, de acuerdo con la información de la versión del protocolo de la sesión, en correspondencia con una DMAcc en el DMT y con la versión del protocolo admitida por el terminal, una versión de protocolo de la sesión adecuada para el terminal y para el servidor; y la unidad 540 de proceso inicia un mensaje de solicitud de la sesión de acuerdo con la versión del protocolo de la sesión.

La unidad 560 de autenticación del mensaje de disparo está adaptada para autenticar un mensaje de disparo utilizando el tipo de autenticación designado por adelantado, un tipo de autenticación o un nombre de autenticación transportado en el mensaje de disparo, o un tipo de autenticación determinado de acuerdo con una regla predeterminada, donde la información de autenticación correspondiente al tipo de autenticación o al nombre de la autenticación está incluido en la información de la cuenta configurada.

Para concluir, en las soluciones técnicas de la presente invención, cuando se efectúa la configuración inicial, el terminal puede identificar, de acuerdo con la información de la versión del protocolo admitida o correspondiente a un servidor correspondiente y transportada en el paquete de configuración, una versión del protocolo correspondiente a un paquete de configuración, de manera que el terminal puede determinar si el paquete es adecuado para el terminal, para poder realizar una configuración correcta. Cuando el terminal tiene capacidad para admitir una pluralidad de versiones de protocolo, el terminal puede determinar, de acuerdo con la información de la versión del protocolo admitida o correspondiente al servidor correspondiente y transportada en el paquete de configuración, un protocolo que deba ser utilizado para la comunicación con el servidor, eliminando así el problema de aumentar el tráfico de las comunicaciones debido a diferentes versiones de protocolo.

Haciendo referencia a la figura 6, un sistema para la configuración por lotes de acuerdo con un modo de realización de la presente invención, incluye un servidor DM, un cliente de difusión y un cliente DM.

El servidor DM está adaptado para generar un mensaje de configuración basado en un protocolo DM, para ser entregado a través de un canal de difusión, donde el mensaje de configuración transporta un identificador del servidor DM e información de autenticación. El servidor DM está conectado a un BSA o a un BSD/A o BDS SD/A, para entregar el mensaje de configuración, y el canal de la entrega es un canal de difusión.

El cliente de difusión está adaptado para recibir un mensaje entregado a través del canal de difusión, identificar el mensaje de acuerdo con el tipo de mensaje, y reenviar el mensaje al cliente DM.

El cliente DM está adaptado, de acuerdo con el identificador del servidor y un tipo de autenticación que son transportados en el mensaje de configuración, para completar la autenticación de la identidad del servidor DM que genera el mensaje de configuración, determinar, de acuerdo con el identificador del servidor DM, un derecho al control de acceso del servidor DM a un nodo objetivo de gestión en un DMT de un terminal, determinar un camino básico adecuado en el DMT basándose en el derecho al control de acceso, donde el camino determinado debe satisfacer la condición siguiente: El servidor correspondiente al identificador del servidor transportado tiene el derecho de ejecutar una orden de gestión en el mensaje de configuración bajo el nodo, y ejecutar la orden de gestión transportada en el mensaje de configuración bajo el camino básico.

A través del método de configuración por lotes, se puede completar eficazmente la entrega segura de las operaciones de gestión general por lotes, tal como la configuración de parámetros, mejorando así la eficiencia de la operación, reduciendo la ocupación del canal, y aligerando la carga del servidor.

Obviamente, las personas con experiencia normal en la técnica deben comprender que las unidades o pasos de la presente invención pueden ser realizados con un dispositivo informático universal, y pueden ser integrados en un solo dispositivo informático, o distribuidos en una red consistente en una pluralidad de dispositivos informáticos. Opcionalmente, las unidades o pasos pueden ser realizados utilizando un código de programa ejecutable del dispositivo informático, por tanto las unidades o pasos se almacenan en un dispositivo de almacenamiento y se ejecutan en el dispositivo informático, o bien se realizan siendo fabricados en módulos de un circuito integrado (IC) respectivamente, o fabricando múltiples unidades o pasos entre ellos en un solo módulo de IC. Por tanto, la presente invención no está limitada a ninguna combinación específica de hardware y software.

Finalmente, debe indicarse que los anteriores modos de realización se ofrecen meramente para describir las soluciones técnicas de la presente invención, pero no pretenden limitar la presente invención. Debe entenderse por las personas de experiencia normal en la técnica, que aunque la presente invención ha sido descrita en detalle con referencia a los modos de realización, se pueden hacer modificaciones a las soluciones técnicas descritas en los

modos de realización, o se pueden hacer sustituciones equivalentes a algunas características técnicas de las soluciones técnicas, mientras que tales modificaciones o sustituciones no se apartan del alcance de la solución técnica de acuerdo con los modos de realización de la presente invención.

**REIVINDICACIONES**

1. Un método para la configuración y gestión de terminales, que comprende:

configurar (S31) una cuenta del servidor de Gestión de Dispositivos DM en un terminal, donde la cuenta del servidor DM comprende un identificador del servidor DM e información de autenticación;

generar, por medio del servidor DM, un mensaje de configuración basado en un protocolo DM, donde el mensaje de configuración transporta el identificador del servidor DM, una versión del protocolo usado, una orden de gestión, un valor de la configuración objetivo, e información de autenticación de identidad del servidor, donde el mensaje de configuración se usa para la configuración o gestión de parámetros, y donde el valor de la configuración objetivo es un objeto de gestión, y el transporte del valor de la configuración objetivo en el mensaje de configuración incluye: efectuar una secuencia del objeto de gestión, proporcionando un camino virtual al objeto de gestión secuenciado;

recibir (S32) en el terminal, a través de un canal de difusión, el mensaje de configuración, extrayendo (S33) la información de autenticación desde la cuenta del servidor DM de acuerdo con el identificador del servidor DM, y autenticar el mensaje de configuración utilizando la información de autenticación;

determinar un camino básico en el Árbol de Gestión del Dispositivo, DMT, del terminal, de acuerdo con el camino virtual del mensaje de configuración, si la autenticación tiene éxito, juzgando si el servidor DM tiene el derecho de ejecutar la orden de gestión transportada en el mensaje de configuración bajo el camino básico, determinando (S34), de acuerdo con el identificador del servidor DM, un derecho al control de acceso del servidor DM a un nodo de gestión objetivo en el DMT del terminal, y

ejecutar, basándose en el derecho al control de acceso, la orden de gestión transportada en el mensaje de configuración.

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

determinar, de acuerdo con la información de la versión del protocolo usado, transportada en el mensaje de configuración, si el terminal admite el mensaje de configuración, y si el terminal admite el mensaje de configuración, autenticar el mensaje de configuración.

3. Un sistema para la configuración y gestión de terminales, que comprende:

un servidor de Gestión de Dispositivos, DM, adaptado para generar un mensaje de configuración basado en un protocolo DM, donde el mensaje de configuración transporta un identificador del servidor DM, una versión del protocolo usado, una orden de gestión, un valor de la configuración objetivo, e información de autenticación de la identidad del servidor DM, donde el mensaje de configuración se utiliza para la configuración o gestión de parámetros, donde el valor de la configuración objetivo es un objeto de gestión, y el transporte del valor de la configuración objetivo del mensaje de configuración incluye específicamente: efectuar una secuencia del objeto de gestión, proporcionando un camino virtual para el objeto de gestión secuenciado;

un cliente de difusión, adaptado para recibir un mensaje de configuración entregado a través de un canal de difusión, identificar el mensaje de acuerdo con el tipo de mensaje de configuración, y reenviar el mensaje al cliente DM; y

un cliente DM, adaptado para autenticar el servidor DM de acuerdo con el identificador del servidor DM y un tipo de autenticación, que son transportados en el mensaje de configuración, determinar un camino básico en el Árbol de Gestión de Dispositivos, DMT, del terminal, de acuerdo con el camino virtual del mensaje de configuración, si la autenticación tiene éxito, donde el cliente DM está adaptado para juzgar si el servidor DM tiene el derecho de ejecutar la orden de gestión transportada en el mensaje de configuración bajo el camino básico, determinando, de acuerdo con el identificador del servidor DM, un derecho al control de acceso del servidor DM a un nodo de gestión objetivo en el DMT del terminal, y ejecutar, basándose en el derecho al control de acceso, la orden de gestión transportada en el mensaje de configuración.

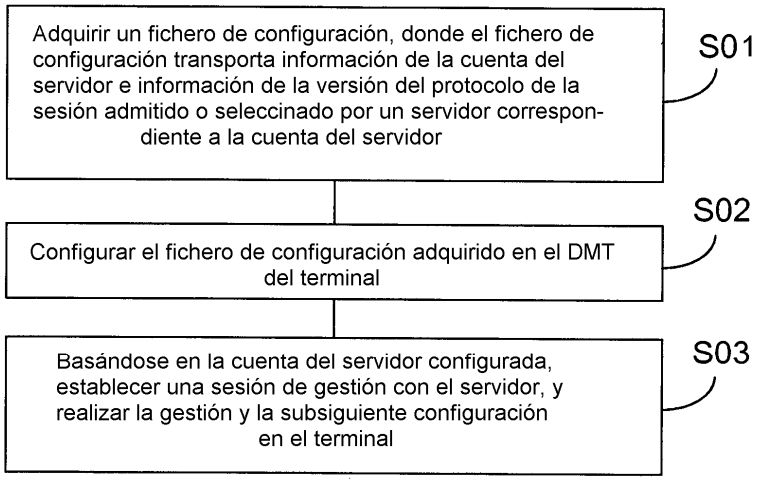
Adquirir un fichero de configuración, donde el fichero de configuración transporta información de la cuenta del servidor e información de la versión del protocolo de la sesión admitido o seleccinado por un servidor correspondiente a la cuenta del servidor
S01
Configurar el fichero de configuración adquirido en el DMT del terminal
S02
Basándose en la cuenta del servidor configurada, establecer una sesión de gestión con el servidor, y realizar la gestión y la subsiguiente configuración en el terminal
S03

FIG. 1

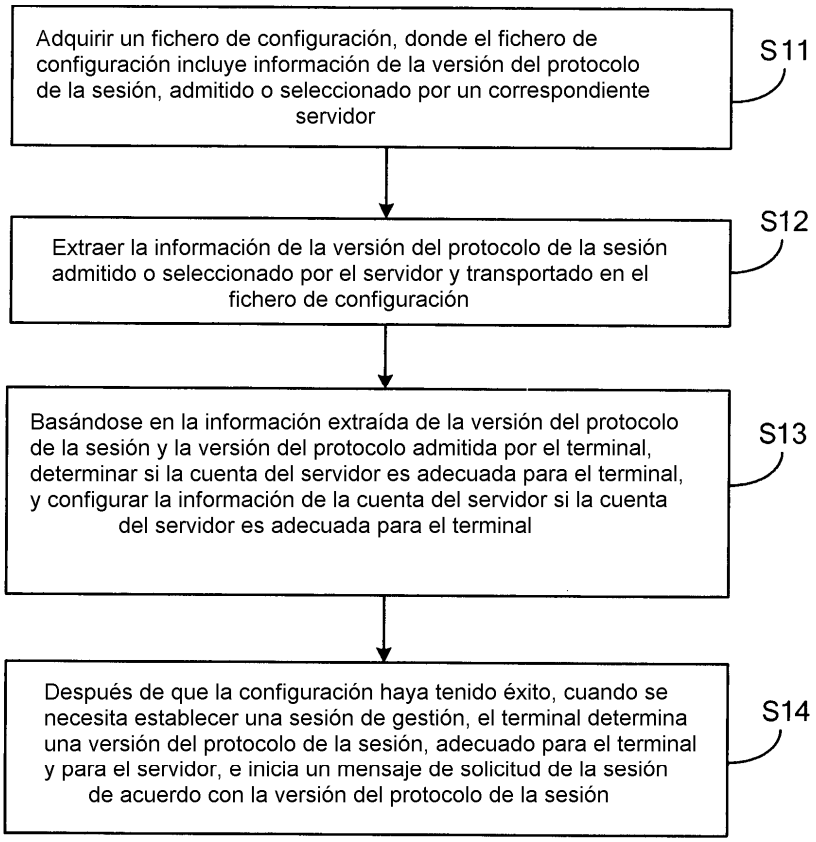
Adquirir un fichero de configuración, donde el fichero de configuración incluye información de la versión del protocolo de la sesión, admitido o seleccionado por un correspondiente servidor
S11
Extraer la información de la versión del protocolo de la sesión admitido o seleccionado por el servidor y transportado en el fichero de configuración
S12
Basándose en la información extraída de la versión del protocolo de la sesión y la versión del protocolo admitida por el terminal, determinar si la cuenta del servidor es adecuada para el terminal, y configurar la información de la cuenta del servidor si la cuenta del servidor es adecuada para el terminal
S13
Después de que la configuración haya tenido éxito, cuando se necesita establecer una sesión de gestión, el terminal determina una versión del protocolo de la sesión, adecuado para el terminal y para el servidor, e inicia un mensaje de solicitud de la sesión de acuerdo con la versión del protocolo de la sesión
S14

FIG. 2

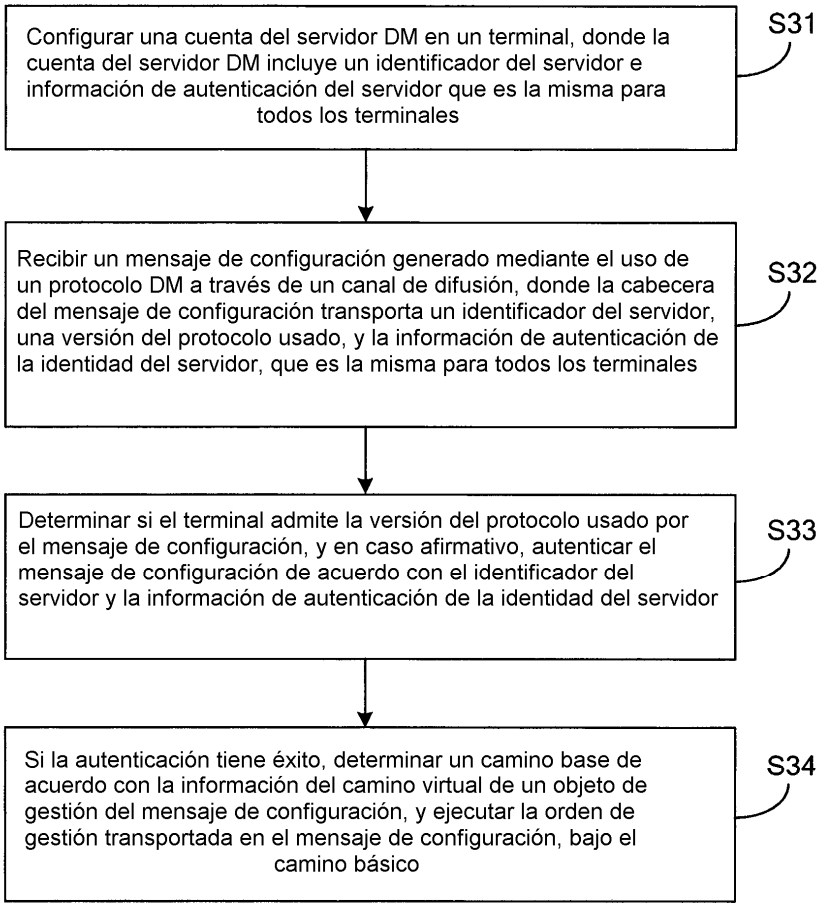
Configurar una cuenta del servidor DM en un terminal, donde la cuenta del servidor DM incluye un identificador del servidor e información de autenticación del servidor que es la misma para todos los terminales
S31
Recibir un mensaje de configuración generado mediante el uso de un protocolo DM a través de un canal de difusión, donde la cabecera del mensaje de configuración transporta un identificador del servidor, una versión del protocolo usado, y la información de autenticación de la identidad del servidor, que es la misma para todos los terminales
S32
Determinar si el terminal admite la versión del protocolo usado por el mensaje de configuración, y en caso afirmativo, autenticar el mensaje de configuración de acuerdo con el identificador del servidor y la información de autenticación de la identidad del servidor
S33
Si la autenticación tiene éxito, determinar un camino base de acuerdo con la información del camino virtual de un objeto de gestión del mensaje de configuración, y ejecutar la orden de gestión transportada en el mensaje de configuración, bajo el camino básico
S34

FIG. 3

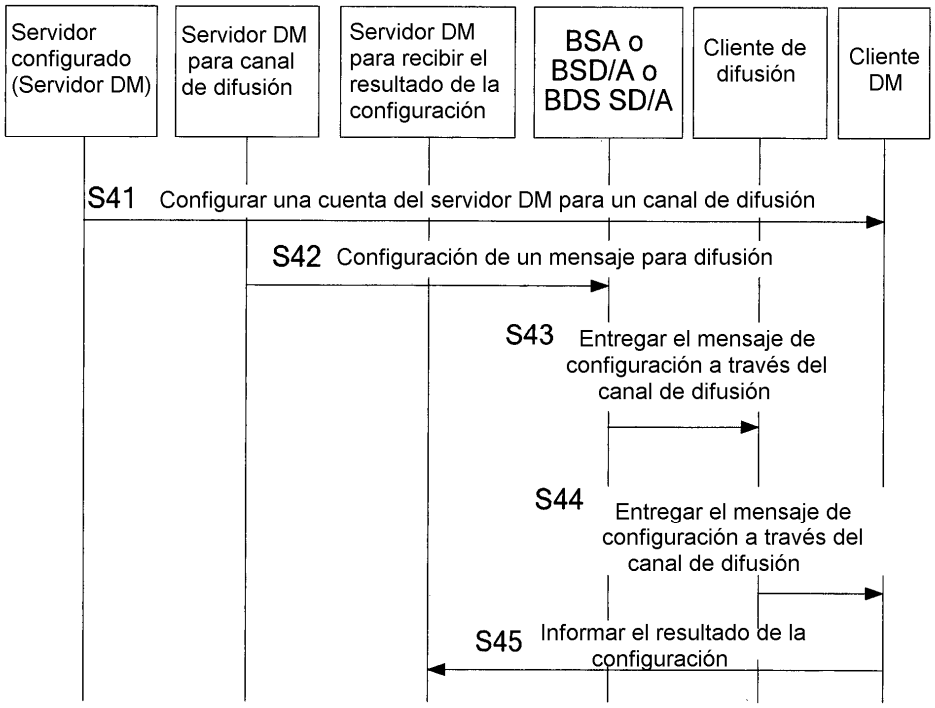
Servidor configurado (Servidor DM)
Servidor DM para canal de difusión
Servidor DM para recibir el resultado de la configuración
BSA o BSD/A o BDS SD/A
Cliente de difusión
Cliente DM
S41 Configurar una cuenta del servidor DM para un canal de difusión
S42 Configuración de un mensaje para difusión
S43 Entregar el mensaje de configuración a través del canal de difusión
S44 Entregar el mensaje de configuración a través del canal de difusión
S45 Informar el resultado de la configuración

FIG. 4

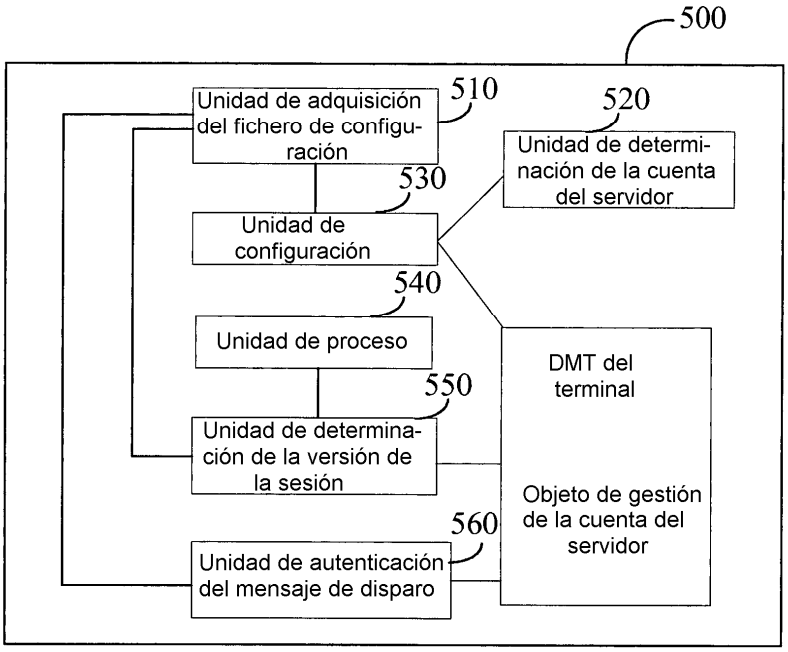
500
Unidad de adquisición del fichero de configuración
510
520
Unidad de determinación de la cuenta del servidor
530
Unidad de configuración
540
Unidad de proceso
DMT del terminal
550
Unidad de determinación de la versión de la sesión
Objeto de gestión de la cuenta del servidor
560
Unidad de autenticación del mensaje de disparo

FIG. 5

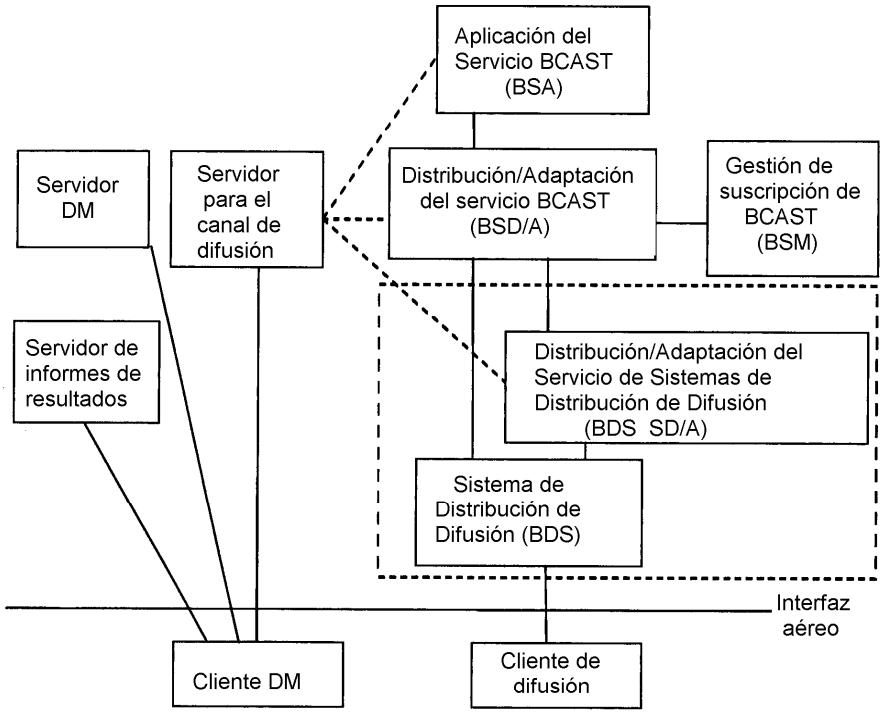
Aplicación del Servicio BCAST (BSA)
Servidor DM
Servidor para el canal de difusión
Distribución/Adaptación del servicio BCAST (BSD/A)
Gestión de suscripción de BCAST (BSM)
Servidor de informes de resultados
Distribución/Adaptación del Servicio de Sistemas de Distribución de Difusión (BDS SD/A)
Sistema de Distribución de Difusión (BDS)
Interfaz aéreo
Cliente DM
Cliente de difusión

FIG. 6