(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 776 475**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.10.2010 PCT/CN2010/077882**

(87) Fecha y número de publicación internacional: **28.07.2011 WO11088695**

(96) Fecha de presentación y número de la solicitud europea: **19.10.2010 E 10843735 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2019 EP 2512089**

(54) Título: **Método y sistema para acceder a una red a través de un equipo público**

(30) Prioridad:

20.01.2010 CN 201010002849

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2020

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

YAN, ZHENGQING;
ZHANG, SHIWEI y
FU, TAO

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para acceder a una red a través de un equipo público

Campo técnico

La presente invención se refiere a los campos de comunicaciones móviles e Internet, y más especialmente, a un método y sistema para acceder a una red en un equipo público. Se conocen tecnologías relacionadas a partir de los documentos EP 2 051 473 A1, US 2009/0258637 A1 y US 2008/066190 A1.

Antecedentes de la técnica relacionada

Cuando un usuario accede a la red en equipo público en la red de Protocolo de Internet (IP) existente, él/ella usa directamente la dirección IP del equipo público para comunicarse con otros usuarios, y las agencias de supervisión de redes no pueden rastrear y localizar a los usuarios que acceden a la red en el equipo público. Por ejemplo, en la red existente, necesita enseñarse una tarjeta de ID para acceder a la Internet, pero la mayoría de cibercafés aún no pueden verificar la autenticidad de los documentos, e incluso aunque no exista un documento legal, un usuario puede navegar por la red con un cierto documento público proporcionado por los cibercafés, que provoca muchas dificultades para que las agencias de supervisión de redes rastreen y localicen.

Además, en la red existente, ya que la dirección IP tradicional tiene la ambigüedad de identificación y ubicación, se permite que los usuarios inicien se sesión en sus propias cuentas empresariales, tales como correo electrónico, banca en línea y así sucesivamente, en el equipo público, pero no pueden conseguir la vinculación de la capa de red IP y los servicios de capa de aplicación para el usuario, una vez que se pierde una cuenta, puede provocar al usuario una gran pérdida. Si la vinculación de la capa de red IP y los servicios de capa de aplicación para el usuario se consiguen con la tecnología IP tradicional, cuando un usuario accede a la red en el equipo público, debido a la diferencia de las direcciones IP de capa de red, el usuario no será capa de acceder a sus servicios de capa de aplicación. Para los agentes de supervisión de redes, ya que la cuenta no puede vincularse con el IP del usuario, la supervisión sobre el usuario también se ha debilitado.

En resumen, la tecnología IP tradicional actual tiene los siguientes problemas:

1, ya que la dirección IP tradicional tiene la ambigüedad de identificación y ubicación, las agencias de supervisión no pueden rastrear y localizar de forma eficiente a los usuarios que acceden a la red en el equipo público, que no únicamente tiene un riesgo sino también tiene dificultades para restringir actividades ilegales y criminales;
2, además, la ambigüedad de identificación y ubicación de la dirección IP tradicional también hace que los usuarios no puedan vincular la capa de red IP con los servicios de capa de aplicación, que no puede proteger de forma efectiva la seguridad de los servicios de capa de aplicación.

Sumario de la invención

El problema técnico a resolver en la presente invención es proporcionar un método y sistema para acceder a una red en equipo público para localizar y rastrear de forma eficiente usuarios que acceden a la red en el equipo público en una red de separación de localizador e identificador de abonado.

Para resolver el problema anteriormente mencionado, la presente invención proporciona un método, según se define en la reivindicación de método independiente 1. Un método, para acceder a una red en equipo público a aplicar a una red de separación de localizador e identificador de abonado, que comprende:

después de que nodo de servicio de servicio (ASN) recibe un mensaje de solicitud de acceso a red desde un usuario en equipo público, el ASN envía el mensaje de solicitud de acceso a red a un centro de autenticación (AC), en el que, el mensaje de solicitud de acceso a red comprende al menos la cuenta y contraseña del usuario;
el AC verifica la validez de la cuenta y la contraseña, si se pasa la verificación, envía el identificador de acceso (AID) del usuario al ASN; y
después de que el ASN recibe dicha AID del usuario, el ASN envía el AID del usuario al equipo público, el equipo público toma el AID del usuario como un AID virtual y usa el AID virtual para enviar y recibir mensajes del usuario.

Preferentemente, después de que el ASN recibe dicha AID del usuario, el ASN realiza asociación en el AID del usuario para establecer una relación de correspondencia del AID del usuario y el identificador de encaminamiento (RID) del ASN y notificar la relación de correspondencia al registro de identificación y ubicación (ILR) de dicho usuario.

Preferentemente, después de que el ASN recibe el AID del usuario, el ASN establece una tabla de correspondencia del AID del usuario y el AID del equipo público.

Preferentemente, al mismo tiempo que el ASN establece la tabla de correspondencia del AID del usuario y el AID del equipo público, el ASN establece el atributo del AID del usuario como un AID virtual, y consulta la tabla de

correspondencia cuando se recibe un mensaje que toma el AID virtual como una dirección de origen o una dirección de destino para adquirir el AID del equipo público, y recoge y factura el tráfico del equipo público.

Preferentemente, el ASN prohíbe que el equipo público gestionado acceda a otros usuarios o equipos a excepción del AC.

Preferentemente, el ASN prohíbe que el equipo público gestionado acceda a otros usuarios o equipos a excepción del AC de la siguiente forma:

dicho ASN registra el AID del equipo público gestionado; cuando se recibe un mensaje, si la dirección de origen del mensaje es el ID registrado y la dirección de destino no es el AID del AC, o la dirección de destino del mensaje es el ID registrado y la dirección de origen no es el AID del AC, descarta este mensaje.

Preferentemente, después de que el usuario accede a la red en el equipo público y está en línea en la red, cuando dicho usuario se desconecta,
dicho usuario envía una solicitud de desconexión en el equipo público, y el ASN envía la solicitud de desconexión al AC;
después de que el AC borra el estado en línea del usuario en la red, el AC envía una respuesta de solicitud de desconexión al ASN;
el ASN elimina la asociación en el usuario, y solicita al ILR que borre la relación de correspondencia del AID del usuario y el RID del ASN; al mismo tiempo, el ASN borra la tabla de correspondencia del AID del usuario y el AID del equipo público y envía la respuesta de solicitud de desconexión al equipo público; y
después de que el equipo público recibe la respuesta de solicitud de desconexión, el equipo público borra dicha AID del usuario virtual.

Preferentemente, la cuenta y contraseña del usuario se preasignan por un gestor de red, o se adquieren enviando información de identificación personal en línea; y al mismo tiempo de la asignación de la cuenta, se asigna al usuario un AID vinculado.

Preferentemente, el método también comprende:
después de que el ASN recibe el mensaje de solicitud de acceso a red, el ASN analiza si el mensaje de solicitud de acceso a red viene o no del equipo público, si el mensaje de solicitud de acceso a red no es desde el equipo público, el ASN envía el mensaje de solicitud de acceso a red al AC, y reenvía la respuesta de acceso a red desde el AC al iniciador del mensaje de solicitud de acceso a red.

La presente invención proporciona también un sistema, según se define en la reivindicación de sistema independiente 10. Un sistema, para acceder a una red en equipo público a aplicar a una red de separación de localizador e identificador de abonado, que comprende: nodos de servicio de acceso (ASN), equipo público y un centro de autenticación (AC), en el que,
dicho ASN se establece para, después de recibir un mensaje de solicitud de acceso a red enviado por un usuario en el equipo público, enviar el mensaje de solicitud de acceso a red al AC, en el que, el mensaje de solicitud de acceso a red comprende al menos la cuenta y contraseña del usuario; y después de que se recibe dicho identificador de acceso (AID) del usuario enviado al AC, enviar el AID del usuario al equipo público;
dicho AC se establece para, después de que se recibe el mensaje de solicitud de acceso a red del usuario, verificar la validez de dichas cuenta y contraseña en el mensaje de solicitud, si se pasa la verificación, enviar el AID del usuario al ASN;
el equipo público se establece para, enviar el mensaje de solicitud de acceso a red al ASN de acuerdo con la cuenta y contraseña introducidas por el usuario, y después de recibir el AID del usuario enviado por el ASN, tomar el AID del usuario como un AID virtual y usar el AID virtual para enviar y recibir los mensajes del usuario.

Preferentemente, el sistema también comprende un registro de identificación y ubicación (ILR),
el ASN también se establece para, después de que dicha AID del usuario se recibe, realizar asociación en dicha AID del usuario para establecer una relación de correspondencia de dicho AID del usuario y el identificador de encaminamiento (RID) del ASN, y notificar la relación de correspondencia al ILR del dicho usuario;
dicho ILR se establece para guardar la relación de correspondencia del AID del usuario y el RID del ASN; y, después de recibir una solicitud de consulta de relación de correspondencia iniciada por otro ASN de acuerdo con el AID del usuario, devolver el RID que corresponde al AID del usuario al ASN que inicia solicitud de consulta.

Preferentemente, el ASN también se establece para, después de recibir dicho AID de usuario, establecer la tabla de correspondencia del AID del usuario y el AID del equipo público.

Preferentemente, el ASN también se establece para, establecer el atributo del AID del usuario como un AID virtual, y cuando se recibe un mensaje que toma el AID virtual como una dirección de origen o de destino, consultar la tabla de correspondencia para adquirir el AID del equipo público, y recoger y facturar tráfico del equipo público.

Preferentemente, el ASN también se establece para, prohibir que equipo público gestionado acceda a otros usuarios

o equipos a excepción del AC.

Preferentemente, el ASN también se establece para, después de que se recibe la solicitud de desconexión del usuario, enviar la solicitud a dicho AC; y después de recibir una respuesta de solicitud de desconexión, eliminar la asociación en el usuario, y solicitar al ILR que borre la relación de correspondencia del AID del usuario y el RID del ASN, al mismo tiempo, eliminar la tabla de correspondencia del AID del usuario y el AID del equipo público, y enviar la respuesta de solicitud de desconexión al equipo público;

el AC también se establece para, después de recibir la solicitud de desconexión y borrar el estado en línea del usuario en la red, enviar una respuesta de solicitud de desconexión al ASN; el equipo público también se establece para, después de que se recibe la respuesta de solicitud de desconexión, borrar el AID del usuario virtual.

La solución de implementación anteriormente mencionada se basa en la red de separación de localizador e identificador de abonado, y la singularidad del AID del usuario se adopta en toda la red para conseguir el usuario que acceda a la red en el equipo público. En comparación con la red IP tradicional existente, las ventajas de la red de separación de localizador e identificador de abonado puede usarse completamente cuando se aplica la solución de implementación anteriormente mencionada, y los usuarios que acceden a la red en el equipo público pueden rastrearse y localizarse de forma efectiva sobre la base de la singularidad del AID en toda la red.

Breve descripción de los dibujos

La Figura 1 es un diagrama de la arquitectura de la SILSN de acuerdo con una realización de la presente invención.

La Figura 2 es un diagrama de flujo de un usuario que accede a la red en el equipo público de acuerdo con una realización de la presente invención.

La Figura 3 es un diagrama de flujo del reenvío de mensajes cuando un usuario está en línea en el equipo público de acuerdo con una realización de la presente invención.

La Figura 4 es un diagrama de flujo del ASN que procesa los mensajes desde el equipo público de acuerdo con una realización de la presente invención.

La Figura 5 es un diagrama de flujo de un ASN procesando mensajes desde otro ASN de acuerdo con una realización de la presente invención.

La Figura 6 es un diagrama de flujo del usuario desconectándose de acuerdo con una realización de la presente invención.

La Figura 7 es un diagrama de flujo de un usuario solicitado una cuenta en el equipo público de acuerdo con una realización de la presente invención.

Realizaciones preferidas de la presente invención

Para resolver el problema de la ambigüedad de la identificación y ubicación en la dirección IP tradicional existente, la presente invención proporciona una arquitectura de sistema de una Red de Separación de Localizador e Identificador de abonado (SILSN) mostrada en la Figura 1, en la Figura 1, el sistema de SILSN consiste en nodos de servicio de acceso (ASN), usuarios, el centro de autenticación (AC) 11, el centro de información de identificador (IIC) 12, el Registro de Identificación y Ubicación (ILR) 13, y así sucesivamente.

Entre los mismos, el ASN es principalmente responsable del acceso del usuario, y emprender la facturación, conmutación y otras funciones; el ILR se establece para emprender el registro de ubicación del usuario e identificación de identificador y localizador, así como la función de consulta de ubicación; el AC es responsable de verificar el acceso del usuario; el IIC es responsable de almacenar la información de identificación del usuario.

Existen dos tipos de identificación en la arquitectura de SILSN anteriormente mencionada: identificador de acceso (AID) e identificador de encaminamiento (RID). En el que, el AID es el identificador del usuario, este identificador se asigna únicamente a este usuario y es único en toda la red, y este identificador puede ser único e invariable en la transmisión de red, y cuando el usuario se mueve en la red, el AID se mantiene invariable y es único en toda la red. Los usuarios encaminan los mensajes con sus RID de ASN asociados. Se ha de observar que el identificador de identidad y el identificador de ubicación podrían tener nombres diferentes en diferentes de arquitecturas SILSN, pero los fundamentos son los mismos.

La SILSN anteriormente mencionada tiene la siguiente característica: ningún usuario en esta red puede acceder hasta que pasa una rigurosa verificación. Cada usuario transporta su propio AID en los paquetes enviados en una diversidad de servicios, y cada paquete enviado por el usuario debe verificarse por ASN para garantizar que el paquete de datos enviado por el usuario transporta el identificador de acceso del usuario, por lo tanto, un usuario no puede hacerse

pasar por el AID de otro usuario para acceder a la red, y este identificador de acceso permanece invariable cuando se transmite en la red, y cuando el usuario se mueve o conmuta, el identificador no cambiará.

En el ejemplo mostrado en la Figura 1, los usuarios Usuario 1 y Usuario 2 tienen sus identificadores de acceso únicos AID1 y AID2, el Usuario 1 y el Usuario 2 acceden a la red con el ASN1 y el ASN2 respectivamente. En el que, el Usuario 2 accede a la red normalmente, es decir, el Usuario 2 usa su propio equipo de usuario (UE) para acceder a la red, y el AID de su UE es el AID que el Usuario 2 usa para vincular con los servicios. Sin embargo, el Usuario 1 accede a la red en el equipo público, ya que el AID del equipo público no es el AID propiedad del Usuario 1, no puede vincularse con los servicios de aplicación del usuario.

Para la SILSN anteriormente mencionada, para resolver el problema, la idea de implementación básica de la presente invención es como se indica a continuación: el gestor de red guarda la cuenta del usuario, contraseña y AID en el AC, el usuario usa sus propias cuenta y contraseña para acceder a la red; el AC verifica la cuenta y contraseña del usuario, después de que el usuario se autentica, el AC envía el AID del usuario al ASN y el equipo público; y toma el AID del usuario que se vincula con la cuenta como un AID virtual para vincular al equipo público.

Por lo tanto, puede conseguirse la vinculación del AID del Usuario 1 y los servicios de aplicación. Se ha de observar que la cuenta del usuario podría asignarse directamente por el gestor de red, o aplicarse por el usuario a través de enviar su información personal en línea en la red pública. Mientras la cuenta se asigna, se asignará un AID para vincular con la cuenta.

Más específicamente, la presente invención usa la siguiente solución para abordar el problema de acceso a la red en el equipo público basándose en la SILSN:

después de que el ASN recibe el mensaje de solicitud de acceso a red enviado por el usuario en el equipo público, envía el mensaje de solicitud al AC y el mensaje de solicitud de acceso a red comprende al menos la cuenta y contraseña del usuario;

el AC verifica la validez de dicha cuenta y contraseña, si se pasa la verificación, envía el AID del usuario al ASN;

el ASN envía el AID del usuario al equipo público, y el equipo público toma dicha AID del usuario como un AID virtual y usa el AID virtual para enviar y recibir los mensajes del usuario.

Adicionalmente, después de que el AC verifica la validez de dicha cuenta y contraseña, envía un mensaje de respuesta de acceso a red al ASN, y si se pasa la verificación, el AID del usuario se transporta en el mensaje de respuesta de acceso a red;
después de que el ASN recibe el mensaje de respuesta de acceso a red que contiene el AID, realiza asociación en el AID del usuario, y establece la relación de correspondencia del AID del usuario y el RID del ASN, y notifica la relación de correspondencia al ILR del dicho usuario; y establece una tabla de correspondencia del AID del usuario y el AID del equipo público.

Adicionalmente, si se pasa la verificación, el ASN también establece el atributo del AID del usuario como un AID virtual.

Adicionalmente, el usuario introduce su cuenta y contraseña en el equipo público, y envía un mensaje de solicitud de acceso a red al ASN, y el mensaje de solicitud de acceso a red comprende al menos la cuenta y contraseña del usuario;
el ASN evalúa si el mensaje de solicitud de acceso a red viene o no del equipo público, si es que sí, realiza asociación en el AID del usuario si se recibe el mensaje de respuesta de acceso a red que pasa la verificación, y establece la tabla de correspondencia del AID del usuario y el AID del equipo público; si el mensaje no viene del equipo público, el mensaje únicamente necesita reenviarse al AC para verificar, y el mensaje de respuesta de acceso a red recibido se reenvía al iniciador de la solicitud de acceso a red.

Adicionalmente, el ASN prohibirá que el equipo público acceda a los usuarios a excepción del AC.

A continuación, se describirá en detalle adicional la implementación del esquema técnico de la presente invención con combinación de los dibujos adjuntos y realizaciones específicas. Se ha de observar que el contenido de la presente invención puede explicarse con las siguientes realizaciones, pero el contenido de la presente invención no se limita a las siguientes realizaciones.

La Figura 2 muestra el proceso de un usuario que accede a la red con su cuenta en el equipo público. El usuario introduce su propia cuenta en el equipo público, e introduce la contraseña para solicitar acceder a la red. La información de aplicación se envía al AC para procesar, el AC consulta para adquirir la contraseña de la cuenta así como el AID de acuerdo con la cuenta. A continuación, el AC usa la información de cuenta consultada para verificar la autenticidad de la cuenta y contraseña enviadas por el usuario para verificar si la solicitud de acceso a red desde el usuario puede aceptarse o no. Si la verificación es satisfactoria, el AC envía el AID del usuario al equipo público del usuario. El proceso específicamente comprende las siguientes etapas.

S200, el Usuario introduce su cuenta y contraseña en el equipo público y envía un mensaje de solicitud de acceso a red al ASN, y el mensaje de solicitud de acceso a red comprende la cuenta y contraseña del usuario.

En este documento, el AID de origen del mensaje es el AID del equipo público, y el AID de destino es el AID del AC;

S210, el ASN recibe el mensaje de solicitud de acceso a red del usuario desde el equipo público, y reenvía el mensaje al AC para procesar.

En esta etapa, el ASN necesita evaluar si el mensaje de solicitud de acceso a red viene o no del equipo público, si el mensaje no viene del equipo público, por ejemplo, un acceso doméstico normal a través de un PC o UE, el usuario transporta su propio AID en la solicitud de acceso a red, el ASN envía la solicitud al AC para verificar, y después de que se recibe la solicitud de acceso a red response desde el AC, si se pasa la verificación, el ASN realiza directamente asociación en el AID del usuario. La diferencia de acceder en el equipo público es que, el AC únicamente necesita devolver el mensaje de respuesta indicando si se pasa la verificación o no, mientras el AID del usuario no necesita enviarse; el ASN tampoco necesita establecer la tabla de correspondencia del AID del usuario y el AID del equipo público.

S220, después de que el AC recibe el mensaje de solicitud de acceso a red del usuario desde el equipo público, el AC verifica la validez de la cuenta y contraseña en el mensaje de solicitud, por ejemplo, extrae la cuenta y contraseña del usuario en el mensaje de solicitud, y compara las mismas con la correspondiente cuenta y contraseña almacenadas en el AC, si son consistentes, la verificación es satisfactoria, de lo contrario la verificación falla.

S230, el AC envía a acceso de red mensaje de respuesta de solicitud al ASN, y el mensaje transporta el AID del usuario.

S240, después de que el ASN recibe desde el mensaje de respuesta de verificación de acceso a red del usuario desde el AC, si se pasa la verificación, el ASN realiza la asociación en el AID del usuario, y establece la relación de correspondencia <AID, RID> con el propio RID del ASN, y al mismo tiempo, establece la tabla de correspondencia de AID en forma de <AID, RID> para el usuario y el equipo público, opcionalmente, el ASN establece el atributo de AID del usuario como el AID del usuario virtual; si no se pasa la verificación, el ASN directamente reenvía al mensaje de respuesta de verificación de acceso a red desde el AC.

S250, después de que el equipo público recibe el mensaje de respuesta de autenticación de acceso a red, el equipo público toma el AID del usuario como un AID virtual en su propio sistema si se pasa la autenticación, y todo el comportamiento de red del usuario en el equipo público toma el AID virtual como el AID de origen.

Por ejemplo, cuando el usuario accede al servidor de Protocolo de Transferencia de Archivos (FTP), el AID de origen en el mensaje de solicitud de acceso enviado es el AID virtual.

S260, el ASN notifica la relación de correspondencia <AID, RID> del usuario al ILR.

En la que, el propósito del usuario estableciendo una relación de correspondencia <AID,RID> con el ASN y notificando la relación al ILR es para explicar que el usuario se asocia al ASN para facilitar que los otros usuarios y el ASN consulten el ILR de la correspondiente información de RID basándose en el AID del usuario y, a continuación, enviar los mensajes al ASN de acuerdo con la información de RID consultada.

S270, después de que el ILR graba o actualiza la relación de correspondencia <AID, RID> del usuario, devuelve y notifica el mensaje de respuesta de relación de correspondencia al ASN.

Posteriormente, después de que el ILR recibe la solicitud de consulta de la relación de correspondencia del usuario desde otro ASN, devuelve el RID que corresponde al AID del usuario al lado de consulta, es decir, el ASN que inicia la solicitud de consulta.

Se ha de observar que, en las etapas anteriormente mencionadas, las S260 y S270 podrían implementarse antes de la S250, y el orden de la implementación depende del método de implementación dentro del ASN.

La Figura 3 es un diagrama de flujo del reenvío de mensajes cuando el usuario está en línea en el equipo público. El comportamiento en línea del usuario en el equipo público es básicamente consistente con el comportamiento en línea del usuario en su propio equipo, que está en línea con los requisitos de rastreo y localización de los gestores de red y agencias de supervisión en los usuarios, mientras tanto, también resuelve el problema de vincular el AID de capa de red de usuario y los servicios de capa de aplicación. La diferencia reside en que el ASN necesita recoger el tráfico del equipo público para conseguir la gestión del equipo público. El proceso específicamente comprende las siguientes etapas.

S300, el Usuario 1 envía un mensaje de solicitud de comunicación al Usuario 2 en el equipo público, y el AID de origen

en el paquete es el AID virtual (el AID del Usuario 1).

En la que, además de su propio AID, el sistema del equipo público también permite que los usuarios que acceden satisfactoriamente a la red en el equipo público asocien sus AID al equipo público. En otras palabras, cuando el AID del usuario se asocia al equipo público, el AID usado por el equipo público para enviar y recibir mensajes es el AID del usuario virtual, en lugar del propio AID del equipo público. Cuando el usuario sale de la red, el AID virtual también se borra y, a continuación, el AID usado por el equipo público para enviar y recibir mensaje es su propio AID.

S310, después de que el ASN1 recibe un mensaje desde el equipo público y encuentra que el AID de origen es el AID virtual de acuerdo con el atributo del AID del usuario asociado establecido por el ASN, el ASN1 usa el AID para consultar el AID del Usuario 1 y la tabla de correspondencia de AID del equipo público para consultar y adquirir el AID del equipo público y a continuación recoge el tráfico del equipo público.

S320, el ASN1 consulta el ILR del correspondiente RID (RID del ASN2) de acuerdo con el AID de destino, es decir, el AID del Usuario 2, en el mensaje de solicitud de comunicación del Usuario 1, y toma el RID del ASN1 como el RID de origen, y encapsula el RID del ASN2 en el mensaje como el RID de destino, y encamina y reenvía el mensaje al ASN2.

S330, después de que el ASN2 recibe el mensaje anteriormente mencionado, el ASN2 desencapsula el RID y reenvía el mensaje de solicitud de comunicación del Usuario 1 al Usuario 2.

S340, el Usuario 2 contesta la solicitud de comunicación del Usuario 1, la dirección de origen en el mensaje de respuesta es el AID del Usuario 2, y la dirección de destino es el AID del Usuario 1;

S350, después de que el ASN2 encapsula el RID de origen (el RID del ASN2) y el RID de destino (el RID del ASN1) en el mensaje de respuesta, el ASN2 reenvía el mensaje al ASN1.

Este ejemplo se describe tomando el Usuario 1 que inicia la comunicación con el Usuario 2 como un ejemplo. Si el Usuario 2 inicia una comunicación con el Usuario 1, el ASN2 consulta el ILR para adquirir el correspondiente RID del ASN1 de acuerdo con la dirección de destino, es decir, el AID del Usuario 1, en el mensaje de solicitud de comunicación del Usuario 2, encapsula el mismo en el mensaje, y reenvía y encamina el mensaje al ASN1, el proceso de comunicación es similar a este ejemplo y no se repite en este punto.

S360, después de que el ASN1 recibe el mensaje desde el ASN2, el ASN1 comprueba y encuentra que el AID de destino es el AID virtual, y usa el AID para consultar el AID del Usuario 1 y la tabla de correspondencia de AID del equipo público para consultar y adquirir el AID del equipo público y recoge el tráfico del equipo público.

S370, después de que el ASN1 elimina el RID encapsulado en el mensaje, el ASN1 reenvía el mensaje de respuesta del Usuario 2 al Usuario 1.

En este punto, finaliza el proceso del usuario reenviando el mensaje en el equipo público.

Se ha de observar, que el ASN1 usa el AID del Usuario 1 y la tabla de correspondencia de AID del equipo público para consultar y adquirir el AID del equipo público y, a continuación, recoge el tráfico es únicamente una de las funciones. Las funciones pueden conseguirse por el ASN1 de acuerdo con la tabla de correspondencia de AID no se limitan a la recogida de tráfico, también comprenden grabar la ubicación específica del Usuario 1 que accede a la red, facturar el equipo público, y otras funciones.

La Figura 4 muestra el proceso del ASN que procesa los mensajes desde el equipo público. En este ejemplo, el ASN necesita comprobar si el AID de origen es el AID del equipo público o no, si es que sí, necesita prohibir que el equipo público acceda directamente al destino de un no AC. El proceso específicamente comprende las siguientes etapas.

S400, el ASN recibe un mensaje desde el equipo público (tal como los PC en el cibercafé).

S410, el ASN extrae el AID de origen en el mensaje, y evalúa si es el AID del equipo público o no, si es que sí, continuar a S420; de lo contrario, continuar a S430.

En la que, el ASN consulta para adquirir el AID de origen de acuerdo con la lista que incluye todos los AID en el ASN y, a continuación, evalúa si el AID de origen es el equipo público o no consultando el atributo del AID de origen. Podría existir una diversidad de atributos de AID, tal como el atributo del equipo público anteriormente mencionado, así como el AID virtual, el AID que necesita redirigirse y así sucesivamente.

Además, el AID también podría evaluar si el AID de origen anteriormente mencionado es el equipo público o no a través de una diversidad de otras formas, por ejemplo, el ASN registra los AID de todos los equipos públicos en el mismo y guarda individualmente los mismos como la lista de AID del equipo público; cuando se recibe un mensaje, el ASN evalúa si el AID de origen es el equipo público o no de acuerdo con la lista de AID del equipo público registrada, y así sucesivamente. No se listan uno a uno en este punto.

S420, el ASN evalúa si el destino del mensaje es el AC o no, si es que sí, continuar a la S470, y reenvía el mensaje normalmente; de lo contrario, continuar a la etapa S460, y descartar el mensaje;

S430, si el AID no es el AID del equipo público, el ASN evalúa si el atributo de AID es el usuario virtual o no, es decir, si el AID es el AID virtual para el usuario que accede a la red en el equipo público o no, y si es que sí, continuar a S440; de lo contrario, continuar a S470 y reenvía normalmente el mensaje.

S440, de acuerdo con el AID virtual para el usuario que accede a la red en el equipo público, se comprueba si existe o no la correspondiente tabla de correspondencia de AID con el AID del equipo público, si existe la tabla de correspondencia de AID, continuar a S450; de lo contrario, continuar a S460, y descartar el mensaje.

S450, el ASN recoge el tráfico del equipo público de acuerdo con la tabla de correspondencia de AID consultada, y continuar a la etapa 470.

S460, el mensaje se descarta; y finaliza el proceso.

S470, el mensaje se reenvía normalmente. Se ha de observar que se salta la S470 de la etapa S420, S430 o S450.

En este punto, finaliza el proceso del reenvío de mensajes desde el equipo público por el ASN.

La Figura 5 muestra el proceso del ASN procesando un mensaje desde otro ASN. En este ejemplo, el ASN necesita comprobar si el AID de destino es el AID virtual del usuario que accede a la red en el equipo público o no. El proceso específicamente comprende las siguientes etapas.

S500, el ASN recibe un mensaje desde otro ASN.

S510, el ASN extrae el AID de origen y el AID de destino en el mensaje, y evalúa si el AID de destino es el AID del equipo público o no, si es que sí, continuar a S520; de lo contrario, continuar a S530.

S520, el ASN evalúa si el mensaje viene desde el AC o no, si es que sí, continuar a S570, y reenvía normalmente el mensaje; de lo contrario, continuar a la etapa S560, y descartar el mensaje.

S530, el ASN evalúa si el AID de destino del mensaje es el AID virtual para el usuario que accede a la red en el equipo público o no, y si es que sí, continuar a la S540; de lo contrario, continuar a S570 y reenvía normalmente el mensaje.

S540, si el AID de destino del mensaje es el AID virtual del usuario que accede a la red en el equipo público, el ASN comprueba si tiene la tabla de correspondencia de AID con el AID del equipo público o no de acuerdo con el AID virtual, si es que sí, continuar a S550; de lo contrario, continuar a S560, y descartar el mensaje.

S550, el ASN recoge el tráfico del equipo público de acuerdo con el AID del equipo público, continuar a la etapa 570.

S560, el mensaje se descarta; y finaliza el proceso.

S570, el ASN reenvía el mensaje normalmente. Se ha de observar que la S570 está precedida de las etapas S520, S530 o S550.

En este punto, se completa el proceso del ASN procesando el mensaje desde otro ASN.

La Figura 6 es el proceso del usuario desconectándose. El usuario ha accedido a la red en el equipo público y está en línea, cuando el usuario necesita desconectarse, él/ella envía una solicitud de desconexión al AC, todos del AC, el ILR y el ASN se requieren para borrar la grabación asociada con el AID del usuario. El proceso específicamente comprende las siguientes etapas.

S600, el usuario 1 que accede la red en el equipo público envía una solicitud de desconexión al AC a través del ASN.

S610, el ASN recibe la solicitud de desconexión del Usuario 1 y reenvía la misma al AC para procesar.

S620, el AC recibe la solicitud de desconexión desde el Usuario 1 y borra el estado en línea del Usuario 1 en la red.

S630, el AC envía una respuesta de solicitud de desconexión al ASN para notificar el ASN para borrar la información relacionada de Usuario 1.

S640, el ASN recibe el mensaje de respuesta de solicitud de desconexión desde el AC, elimina la asociación de AID del Usuario 1 y, al mismo tiempo, borra la tabla de correspondencia de AID del AID del Usuario 1 y el AID del equipo público.

S650, el ASN notifica la actualización de relación de correspondencia <AID, RID> del Usuario 1 al ILR, y solicita que el ILR borre la relación de correspondencia <AID,RID>.

S660, el ILR elimina la relación de correspondencia <AID, RID> del Usuario 1, y envía una respuesta de borrado de relación de correspondencia al ASN.

S670, el ASN envía un mensaje de respuesta satisfactoria de desconexión al equipo público, y borra el AID del Usuario 1 virtual asociado al equipo público.

En este punto, finaliza el proceso del usuario desconectándose.

La Figura 7 muestra el proceso del usuario registrando una cuenta en el equipo público. En la condición que el gestor de red permite, el usuario puede rellenar su información personal real en el equipo público, y directamente envía una aplicación de registro de cuenta. La información personal real del usuario se recoge y guarda por el gestor de red en el IIC por adelantado, y se usa para verificar la autenticidad de la aplicación de cuenta enviada por el usuario en línea. El proceso específicamente comprende las siguientes etapas.

S700, el usuario rellena su información personal, tal como número de ID, domicilio, empresa, contraseña y así sucesivamente, y envía un mensaje de aplicación de registro de cuenta al AC.

S710, el ASN reenvía el mensaje de aplicación de registro de cuenta al AC.

S720, el AC recibe el mensaje de aplicación de registro de cuenta, y de acuerdo con el número de ID en este mensaje, consulta el IIC de la información personal real del usuario.

S730, el IIC devuelve la información personal real del Usuario consultada al AC.

S740, el AC usa la información personal real del usuario consultada desde el IIC para verificar si el mensaje de registro de cuenta enviado por el usuario es válido o no, si es válido (por ejemplo, la información de identidad enviada por el usuario en línea, tal como el número de ID, el nombre, la contraseña y así sucesivamente, es consistente con la correspondiente información proporcionada por el IIC, es decir, es válida), el AC asigna una cuenta, una contraseña y un AID al usuario.

S750, el AC envía un mensaje de respuesta de solicitud de registro al ASN.

S760, el ASN asocia el AID del usuario, y establece una tabla de correspondencia con el AID del equipo público, y notifica la relación de correspondencia al ILR.

S770, el ASN envía el mensaje de respuesta de registro que transporta el AID del usuario al usuario, si el registro es satisfactorio, el AID del usuario se virtualiza en el AID del equipo público. Ya que a continuación, el AID de todo el comportamiento de red del usuario es este AID virtual.

Los expertos en el campo pueden entender que todas o parte de las etapas del método anteriormente mencionado se completan por el programa ordenando el hardware relacionado, y el programa puede almacenarse en un medio de almacenamiento legible por ordenador, tal como una memoria de solo lectura, disco o CD-ROM. Opcionalmente, todas o parte de las etapas en las realizaciones anteriormente mencionadas podrían también implementarse con uno o más circuitos integrados. Por consiguiente, cada módulo/unidad en las realizaciones anteriormente mencionadas puede implementarse en forma de módulos funcionales de hardware o software. La presente invención no se limita a ninguna forma particular de combinaciones de hardware y software.

La anterior descripción es únicamente las realizaciones preferidas de la presente invención, y no se usa para limitar la presente invención, y para los expertos en el campo, la presente invención podría tener una diversidad de modificaciones y cambios. Cualquier cambio, sustituciones equivalentes y mejoras hechos dentro de los principios de la presente invención según se definen en las reivindicaciones debería comprenderse dentro del alcance de protección de la presente invención.

Aplicabilidad industrial

El método y sistema para acceder a la red en el equipo público proporcionados en la presente invención usan la singularidad del AID del usuario en toda la red para conseguir que el usuario acceda a la red en el equipo público, las ventajas de la red de separación de localizador e identificador de abonado pueden usarse completamente cuando se aplica la solución de implementación anteriormente mencionada, por lo tanto los usuarios que acceden a la red en el equipo público pueden rastrearse y localizarse de forma efectiva sobre la base de la singularidad del AID en toda la red.

REIVINDICACIONES

1. Un método para acceder a una red en equipo público, que se aplica a una red de separación de localizador e identificador de abonado, y comprendiendo el método:

después de que un nodo de servicio de servicio, ASN, recibe (S200) un mensaje de solicitud de acceso a red desde un usuario en equipo público, el ASN envía (S210) el mensaje de solicitud de acceso a red a un centro de autenticación, AC (11), en el que el mensaje de solicitud de acceso a red comprende al menos una cuenta y una contraseña del usuario, y el equipo público se refiere a ordenadores públicos en Internet;
el AC (11) verifica (S220) la validez de la cuenta y la contraseña, si se pasa la verificación, envía (S230) un identificador de acceso, AID, del usuario al ASN, en el que el AID del usuario es único en toda la red; y
después de que el ASN recibe el AID del usuario, el ASN envía (S250) el AID del usuario al equipo público, el equipo público usa el AID del usuario para enviar y recibir mensajes del usuario.

2. El método de la reivindicación 1, en el que el método también comprende:
después de que el ASN recibe el AID del usuario, el ASN realiza (S250) asociación en el AID del usuario para establecer una relación de correspondencia del AID del usuario y un identificador de encaminamiento, RID del ASN, y notifica la relación de correspondencia a un registro de identificación y ubicación, ILR, (13) del usuario.

3. El método de la reivindicación 2, en el que el método también comprende:
después de que el ASN recibe el AID del usuario, el ASN establece (S250) una tabla de correspondencia del AID del usuario y un AID del equipo público.

4. El método de la reivindicación 3, en el que el método también comprende:
al mismo tiempo que el ASN establece la tabla de correspondencia del AID del usuario y el AID del equipo público, el ASN establece el atributo del AID del usuario como un AID virtual, y consulta (S310) la tabla de correspondencia cuando se recibe un mensaje que toma el AID virtual como una dirección de origen o una dirección de destino para adquirir el AID del equipo público, y recoge y factura tráfico del equipo público.

5. El método de una cualquiera de las reivindicaciones 1 a 4, en el que el método también comprende:
el ASN prohíbe que el equipo público gestionado acceda a otros usuarios o equipos a excepción del AC (11).

6. El método de la reivindicación 5, en el que
el ASN prohíbe que el equipo público gestionado acceda a otros usuarios o equipos a excepción del AC (11) de la siguiente forma:

el ASN registra el AID del equipo público gestionado;
cuando se recibe un mensaje, si la dirección de origen del mensaje es el ID registrado y la dirección de destino no es el AID del AC (11), o la dirección de destino del mensaje es el ID registrado y la dirección de origen no es el AID del AC (11), descarta este mensaje.

7. El método de la reivindicación 2 o 3, en el que el método también comprende: después de que el usuario accede a la red en el equipo público y está en línea en la red, cuando el usuario se desconecta,
el usuario envía (S600) una solicitud de desconexión en el equipo público, y el ASN envía (S610) la solicitud de desconexión al AC (11);
después de que el AC (11) borra (S620) el estado en línea del usuario en la red, el AC (11) envía (S630) una respuesta de solicitud de desconexión al ASN;
el ASN elimina (S640) la asociación en el usuario, y solicita que (S650) el ILR (13) borre la relación de correspondencia del AID del usuario y el RID del ASN; al mismo tiempo, el ASN borra (S640) la tabla de correspondencia del AID del usuario y el AID del equipo público y envía la respuesta de solicitud de desconexión al equipo público; y después de que el equipo público recibe la respuesta de solicitud de desconexión, el equipo público borra el AID virtual del usuario.

8. El método de una cualquiera de las reivindicaciones 1 a 4, en el que la cuenta y la contraseña del usuario se preasignan por un gestor de red, o se adquieren enviando información de identificación personal en línea; y al mismo tiempo de la asignación de la cuenta, se asigna al usuario un AID vinculado.

9. El método de la reivindicación 1, en el que el método también comprende:
después de que el ASN recibe el mensaje de solicitud de acceso a red, el ASN analiza si el mensaje de solicitud de acceso a red viene o no del equipo público, si el mensaje de solicitud de acceso a red no es desde el equipo público, el ASN envía el mensaje de solicitud de acceso a red al AC (11), y reenvía la respuesta de acceso a red desde el AC (11) al iniciador del mensaje de solicitud de acceso a red.

10. Un sistema para acceder a una red en equipo público, que se aplica a una red de separación de localizador e identificador de abonado, comprendiendo el sistema: nodos de servicio de acceso, ASN, equipo público y un centro de autenticación, AC (11), en el que
el ASN se establece para, después de recibir un mensaje de solicitud de acceso a red enviado por un usuario en el

equipo público, enviar el mensaje de solicitud de acceso a red al AC (11), en el que el mensaje de solicitud de acceso a red comprende al menos una cuenta y una contraseña del usuario; y después de que se recibe un identificador de acceso, AID, del usuario enviado por el AC (11), enviar el AID del usuario al equipo público, en el que el AID del usuario es único en toda la red;
el AC (11) se establece para, después de que se recibe el mensaje de solicitud de acceso a red del usuario, verificar la validez de la cuenta y contraseña en el mensaje de solicitud, si se pasa la verificación, enviar el AID del usuario al ASN;
el equipo público se establece para enviar el mensaje de solicitud de acceso a red al ASN de acuerdo con la cuenta y contraseña introducidas por el usuario, y después de recibir el AID del usuario enviado por el ASN, usar el AID del usuario para enviar y recibir mensajes del usuario, en el que el equipo público se refiere a ordenadores públicos en Internet.

11. El sistema de la reivindicación 10, en el que el sistema también comprende un registro de identificación y ubicación, ILR (13),
el ASN también se establece para, después de que se recibe el AID del usuario, realizar asociación en el AID del usuario para establecer una relación de correspondencia del AID del usuario y un identificador de encaminamiento, RID, del ASN y notificar la relación de correspondencia al ILR (13) del usuario;
el ILR (13) se establece para, guardar la relación de correspondencia del AID del usuario y el RID del ASN; y, después de recibir una solicitud de consulta de relación de correspondencia iniciada por otro ASN de acuerdo con el AID del usuario, devolver el RID que corresponde al AID del usuario al ASN que inicia solicitud de consulta.

12. El sistema de la reivindicación 10, en el que
el ASN también se establece para, después de recibir el AID del usuario, establecer la tabla de correspondencia del AID del usuario y un AID del equipo público.

13. El sistema de la reivindicación 12, en el que
el ASN también se establece para establecer el atributo del AID del usuario como un AID virtual, y cuando se recibe un mensaje que toma el AID virtual como una dirección de origen o de destino, para consultar la tabla de correspondencia para adquirir el AID del equipo público, y recoger y facturar tráfico del equipo público.

14. El sistema de una cualquiera de las reivindicaciones 10 a 13, en el que el ASN también se establece para prohibir que equipo público gestionado acceda a otros usuarios o equipos a excepción del AC (11).

15. El sistema de la reivindicación 13, en el que
el ASN también se establece para, después de que se recibe la solicitud de desconexión del usuario, enviar la solicitud al AC (11); y después de recibir una respuesta de solicitud de desconexión, eliminar la asociación en el usuario, y solicitar al ILR (13) que borre la relación de correspondencia del AID del usuario y el RID del ASN, al mismo tiempo, eliminar la tabla de correspondencia del AID del usuario y el AID del equipo público, y enviar la respuesta de solicitud de desconexión al equipo público;
el AC (11) también se establece para, después de recibir la solicitud de desconexión y recibir el estado en línea del usuario en la red, enviar una respuesta de solicitud de desconexión al ASN;
el equipo público también se establece para, después de que se recibe la respuesta de solicitud de desconexión, borrar el AID virtual del usuario.

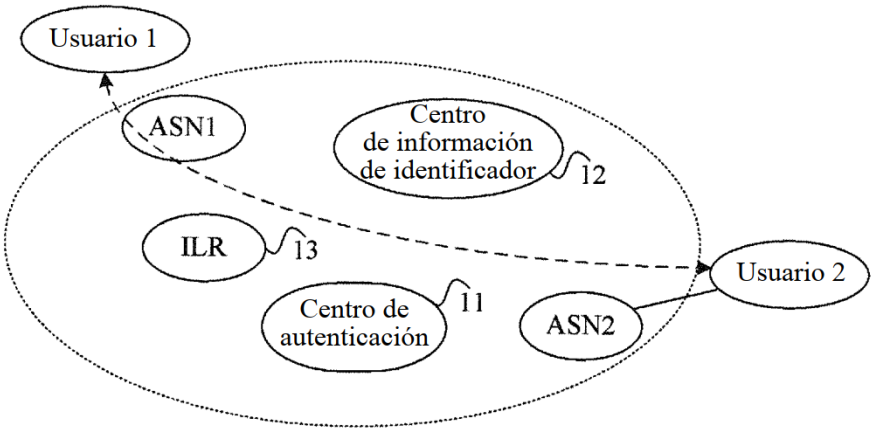
Usuario 1
ASN1
Centro de información de identificador
12
ILR
13
Usuario 2
Centro de autenticación
11
ASN2

FIG. 1

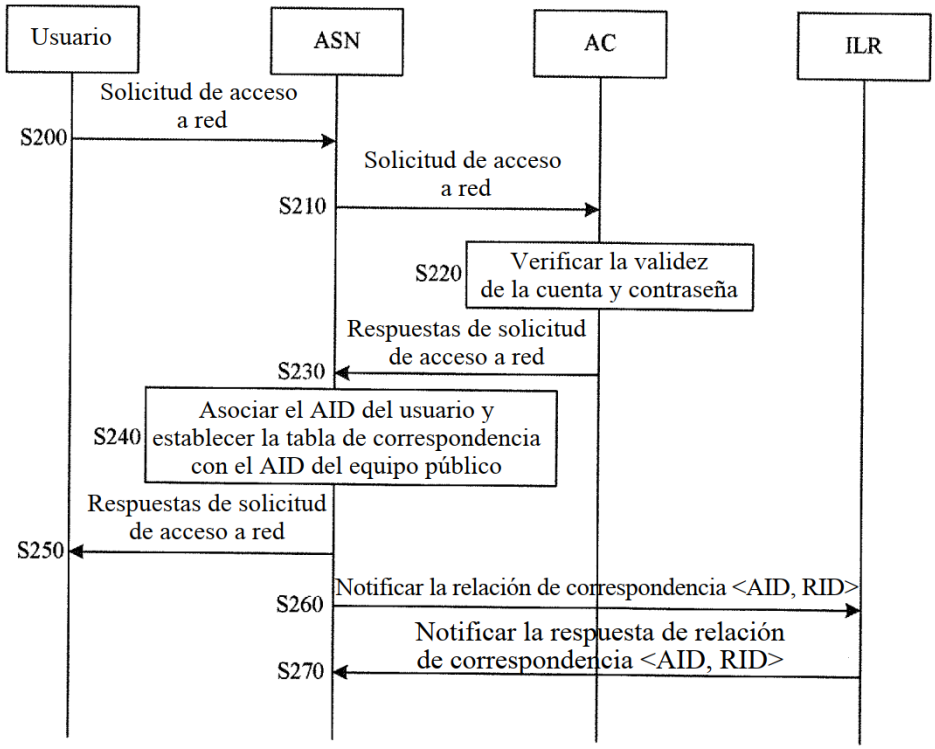
Usuario
ASN
AC
ILR
Solicitud de acceso a red
S200
Solicitud de acceso a red
S210
S220
Verificar la validez de la cuenta y contraseña
Respuestas de solicitud de acceso a red
S230
S240
Asociar el AID del usuario y establecer la tabla de correspondencia con el AID del equipo público
Respuestas de solicitud de acceso a red
S250
Notificar la relación de correspondencia <AID, RID>
S260
Notificar la respuesta de relación de correspondencia <AID, RID>
S270

FIG. 2

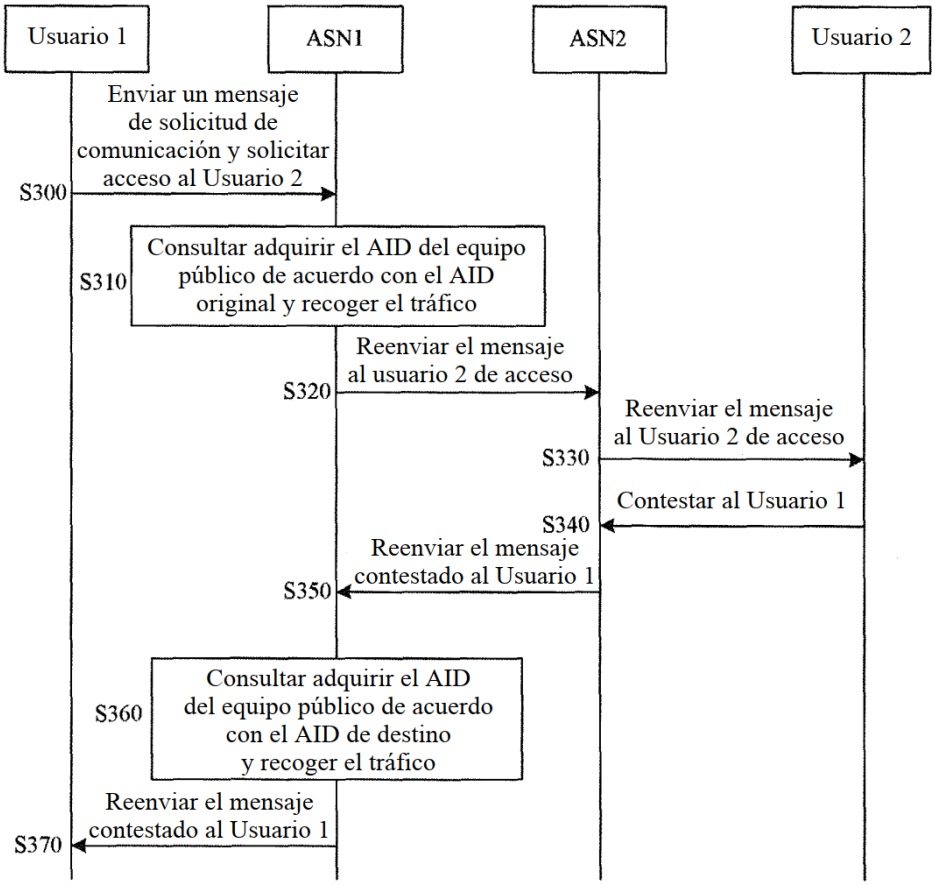
Usuario 1
ASN1
ASN2
Usuario 2
Enviar un mensaje de solicitud de comunicación y solicitar acceso al Usuario 2
S300
S310
Consultar adquirir el AID del equipo público de acuerdo con el AID original y recoger el tráfico
Reenviar el mensaje al usuario 2 de acceso
S320
Reenviar el mensaje al Usuario 2 de acceso
S330
Contestar al Usuario 1
S340
Reenviar el mensaje contestado al Usuario 1
S350
S360
Consultar adquirir el AID del equipo público de acuerdo con el AID de destino y recoger el tráfico
Reenviar el mensaje contestado al Usuario 1
S370

FIG. 3

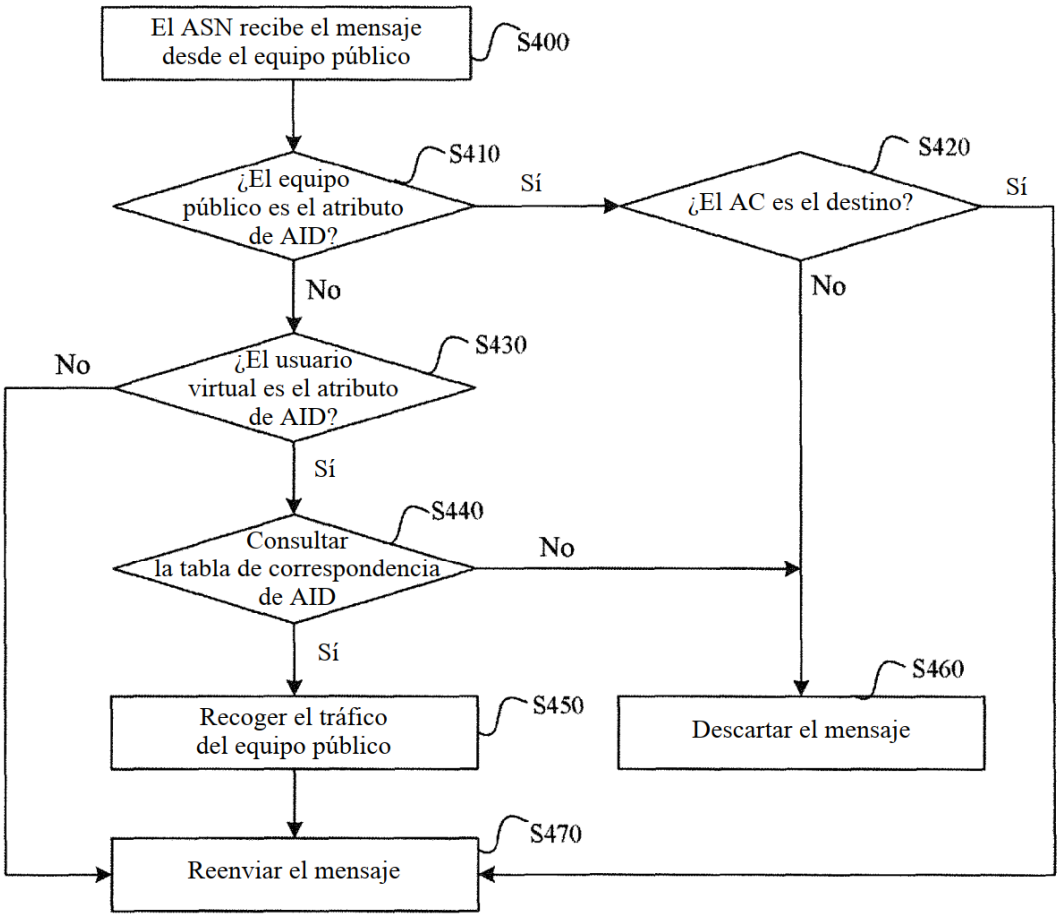
El ASN recibe el mensaje desde el equipo público
S400
¿El equipo público es el atributo de AID?
S410
Sí
¿El AC es el destino?
S420
Sí
No
No
¿El usuario virtual es el atributo de AID?
S430
No
Sí
Consultar la tabla de correspondencia de AID
S440
No
Sí
Recoger el tráfico del equipo público
S450
Descartar el mensaje
S460
Reenviar el mensaje
S470

FIG. 4

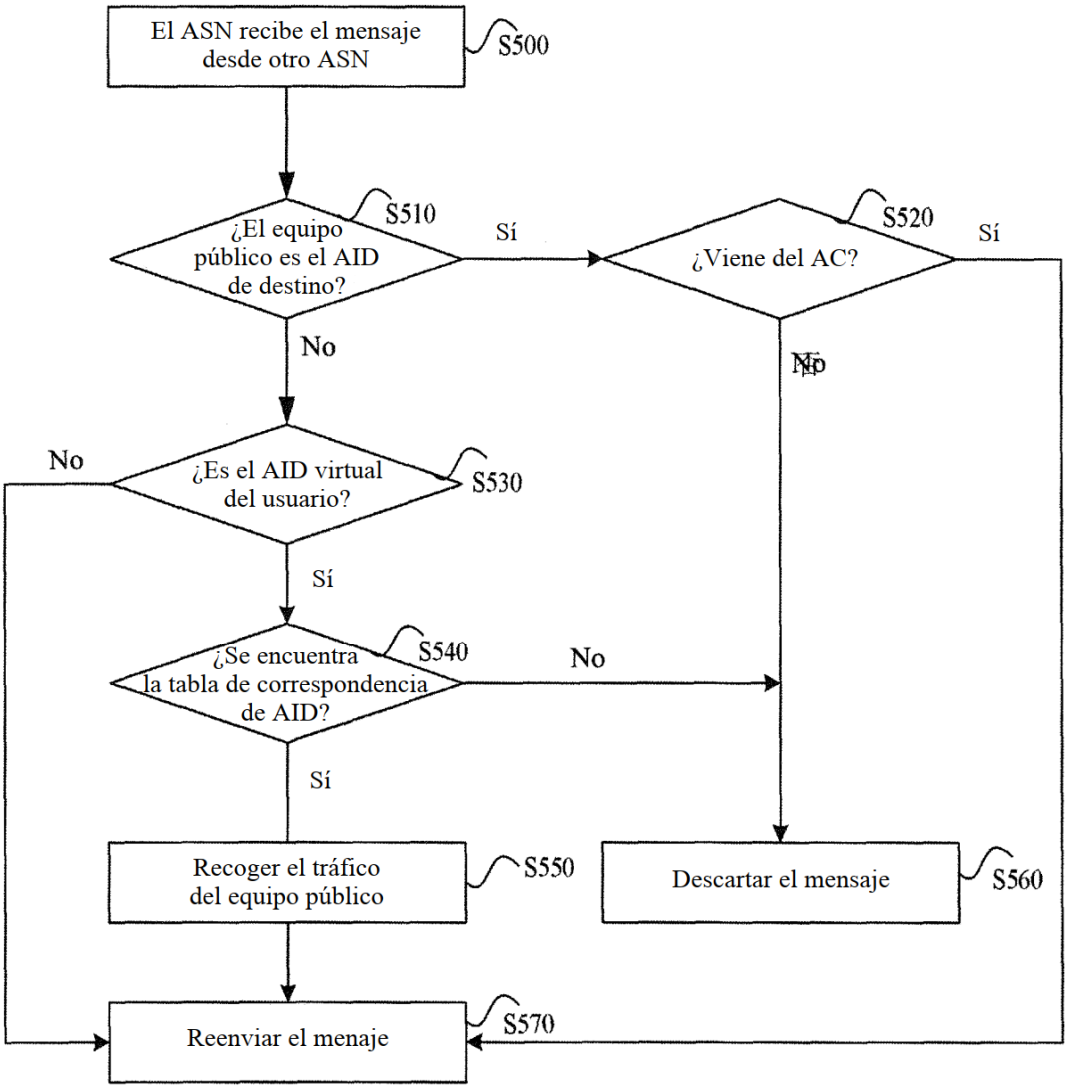
El ASN recibe el mensaje desde otro ASN
S500
¿El equipo público es el AID de destino?
S510
Sí
¿Viene del AC?
S520
Sí
No
No
No
¿Es el AID virtual del usuario?
S530
Sí
¿Se encuentra la tabla de correspondencia de AID?
S540
No
Sí
Recoger el tráfico del equipo público
S550
Descartar el mensaje
S560
Reenviar el menaje
S570

FIG. 5

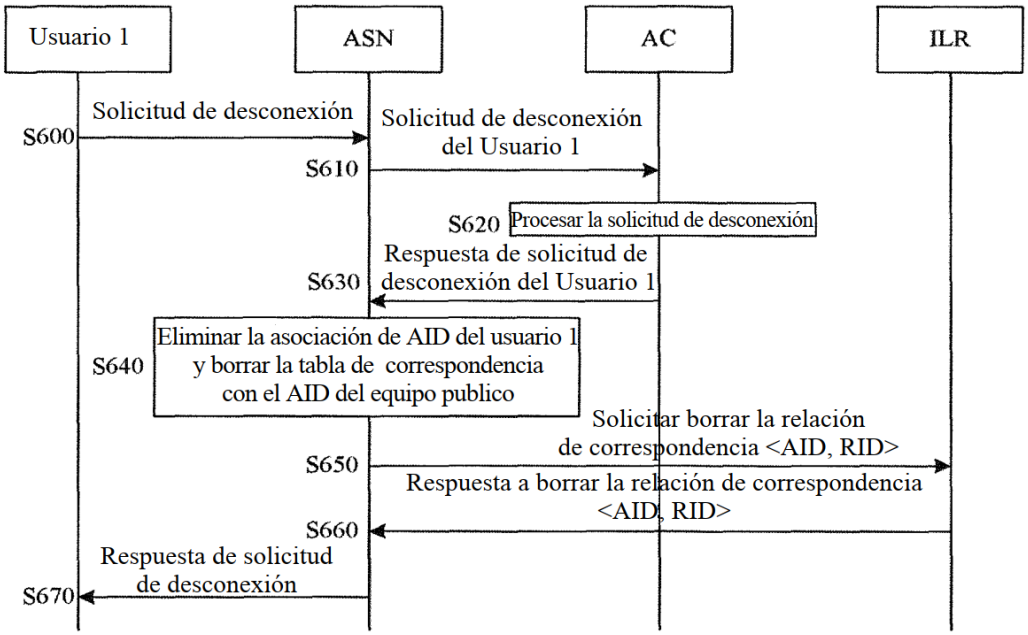
Usuario 1
ASN
AC
ILR
Solicitud de desconexión
S600
Solicitud de desconexión del Usuario 1
S610
S620
Procesar la solicitud de desconexión
Respuesta de solicitud de desconexión del Usuario 1
S630
S640
Eliminar la asociación de AID del usuario 1 y borrar la tabla de correspondencia con el AID del equipo publico
Solicitar borrar la relación de correspondencia <AID, RID>
S650
Respuesta a borrar la relación de correspondencia <AID, RID>
S660
Respuesta de solicitud de desconexión
S670

FIG. 6

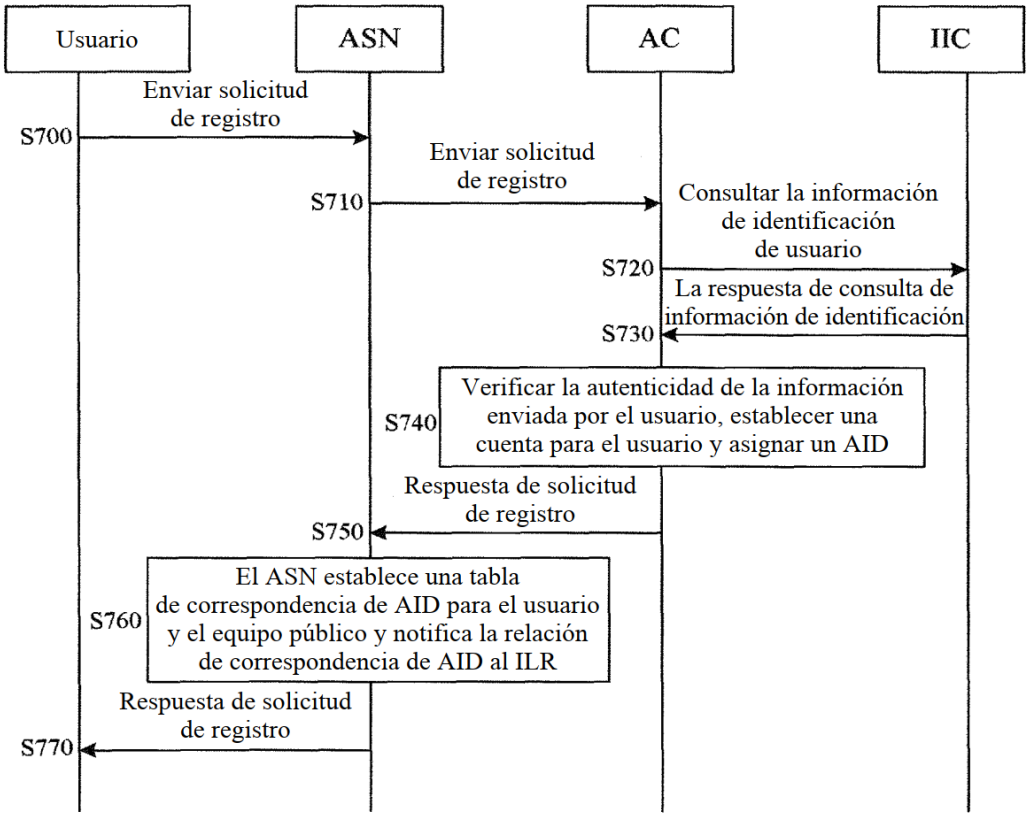
Usuario
ASN
AC
IIC
Enviar solicitud de registro
S700
Enviar solicitud de registro
S710
Consultar la información de identificación de usuario
S720
La respuesta de consulta de información de identificación
S730
S740
Verificar la autenticidad de la información enviada por el usuario, establecer una cuenta para el usuario y asignar un AID
Respuesta de solicitud de registro
S750
S760
El ASN establece una tabla de correspondencia de AID para el usuario y el equipo público y notifica la relación de correspondencia de AID al ILR
Respuesta de solicitud de registro
S770

FIG. 7