(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 286**

(51) Int. CI.:
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07816954 .7**
(96) Fecha de presentación: **25.09.2007**
(97) Número de publicación de la solicitud: **2073432**
(97) Fecha de publicación de la solicitud: **24.06.2009**

(54) Título: **MÉTODO DE LIGAR UN TERMINAL DE ACCESO A UN OPERADOR Y TERMINAL DE ACCESO CORRESPONDIENTE.**

(30) Prioridad:
25.09.2006 CN 200610062834

(45) Fecha de publicación de la mención BOPI:
28.02.2012

(45) Fecha de la publicación del folleto de la patente:
28.02.2012

(73) Titular/es:
Huawei Technologies Co., Ltd.
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:
ZHANG, Ke

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

DESCRIPCIÓN

Método de ligar un terminal de acceso a un operador y terminal de acceso correspondiente.

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo técnico de las líneas de abonados digitales x (xDSL) y, más particularmente, a una tecnología para ligar un terminal de acceso a un operador en un bucle de abonado digital asimétrico (ADSL).

ANTECEDENTES DE LA INVENCIÓN.

Un protocolo de punto a punto (PPP) proporciona un conjunto completo de soluciones para problemas tales como establecimiento de enlace, mantenimiento de enlace, retirada de enlace, negociación de protocolo de capa superior y autenticación. El PPP incluye un protocolo de control de enlace (LCP), un protocolo de control de red (NCP) y un protocolo de autenticación. El protocolo de autenticación incluye principalmente un protocolo de autenticación de contraseña (PAP) y un protocolo de autenticación de desafío mutuo (CHAP).

Un proceso de establecimiento de enlace típico en el PPP se divide en tres fases: una fase de establecimiento, una fase de autenticación y una fase de negociación de red.

El LCP es responsable del establecimiento de un enlace, y en esta fase se selecciona un modo de comunicación básico. Los equipos en dos extremos del enlace retransmiten paquetes de configuración de uno a otro a través del LCP. Una vez que se envía y se recibe el paquete de acuse de recibo de configuración, se completa un intercambio y el LCP entra en un estado abierto.

Durante la fase de autenticación, un cliente envía su información de identidad a un servidor de acceso remoto. En esta fase, se adopta un modo de autenticación seguro para impedir que una tercera parte robe datos o pretenda, como cliente remoto, hacerse cargo de la conexión con el cliente. No tiene que ocurrir un avance de la fase de autenticación a una fase de protocolo de capa de red hasta que se complete la autenticación. Si falla la autenticación, el autenticador deberá saltar a una fase de terminación de enlace.

Los protocolos de autenticación más comúnmente utilizados incluyen PAP y CHAP. El PAP es un simple esquema de autenticación de texto sin cifrar. Cuando un servidor de acceso de red (NAS) requiere que un usuario proporcione un nombre de usuario y una contraseña, el PAP devuelve información del usuario en texto sin cifrar. El CHAP es un esquema de autenticación encriptado capaz de evitar la transmisión de la contraseña real del usuario durante el establecimiento de la conexión. El NAS envía una petición que incluye una ID de sesión y una ristra de desafíos arbitrarios a un cliente remoto. El cliente remoto tiene que utilizar un algoritmo de tratamiento hash unidireccional MD5 para devolver el nombre del usuario y un encriptado del desafío, la ID de sesión y la contraseña del usuario, y en donde el nombre del usuario se envía de una manera no sometida a tratamiento hash.

Después de concluida la fase de autenticación, el PPP emboca diversos NCPs que se seleccionaron durante la fase de establecimiento de enlace. Los NCPs seleccionados resuelven los problemas de protocolo de capa superior en el enlace PPP. Por ejemplo, durante esta fase el protocolo de control IP puede asignar una dirección dinámica a un usuario llamador.

El PPP es uno de los protocolos que se aplican más ampliamente en la red de área amplia (WAN) y es ventajoso por ser sencillo, tener una capacidad de autenticación de usuario y ser capaz de manipular la asignación de IP.

El acceso doméstico por marcación ascendente consiste en establecer un enlace de comunicación entre un cliente y un servidor de acceso de un operador a través del PPP. Con el rápido progreso en la tecnología de acceso de banda ancha se derivan nuevas aplicaciones del PPP. Típicamente, en un modo de acceso de bucle de abonado digital asimétrico (ADSL) el PPP, junto con otros protocolos, deriva nuevos protocolos que satisfacen los requisitos de acceso de banda ancha, por ejemplo PPP sobre Ethernet (PPPoE) y PPP sobre ATM (PPPoA).

El PPPoE es una manera de ejecutar el PPP sobre la red Ethernet para efectuar el acceso de autenticación de usuario utilizando los recursos Ethernet. El PPPoE no solo protege los recursos Ethernet del lado del usuario, sino que satisface también los requisitos de acceso xDSL, y pasa a ser asi el estándar técnico más ampliamente aplicado entre los actuales modos de acceso xDSL.

En la actual tecnología de comunicaciones el xDSL ha pasado a ser la corriente principal de acceso de banda ancha para familiar y empresas de pequeña escala. Una tecnología de línea de abonado digital (DSL) es una tecnología de transmisión a alta velocidad para transmitir datos a través de un par telefónico retorcido, es decir, un par retorcido no apantallado (UTP), y el xDSL incluye el ADSL, la línea de abonado digital de muy alta tasa de bits (VDSL), la línea de abonado digital ISDN (IDSL) basada en la red digital de servicios integrados (ISDN) y la línea de abonado digital de un solo par y alta tasa de bits (SHDSL), etc.

La manera más común para el acceso xDSL es registrándose en una red de operador a través de marcación ascendente PPPoE. En este caso, el terminal de acceso opera usualmente en dos modos: el modo de ruta y el modo de puente.

En el modo de ruta la marcación ascendente PPPoE es iniciada por un módem. El módem obtiene una dirección IP de red pública y asigna direcciones IP de red privada a los equipos, tales como ordenadores personales (PCs), en una red doméstica. El módem proporciona también un servicio de ruta directa.

En el modo de puente la marcación ascendente PPPoE es iniciada por un PC o un enrutador en una red doméstica. El iniciador de marcación ascendente obtiene una dirección IP y el módem proporciona solamente una vía de datos sin reenvío de datos ni realización de algún otro procesamiento.

El término módem se refiere aquí a un terminal de acceso para el modo de acceso xDSL, tal como una unidad terminal remota (RTU) o una pasarela doméstica (HGW).

Actualmente, para atraer más usuarios de xDSL, la mayoría de los operadores recompensan a los abonados del servicio con terminales de acceso gratuito. Sin embargo, debido a la competencia entre los operadores, algunos operadores pueden adoptar una política preferencial de “acceso con un módem” (es decir, el usuario puede acceder a una red a través de un terminal de acceso autoproporcionado) para extraer recursos de usuario de otros operadores. Por tanto, un usuario puede recibir un terminal de acceso gratuito de un operador y acceder a la red de otro operador por medio de “acceso con un módem”, dando así como resultado una perversa competencia entre los operadores.

Los operadores, especialmente los que recompensan a los abonados con terminales de acceso gratuito, esperan que haya una forma razonable de ligar un terminal de acceso con la red de acceso, para restringir técnicamente que los usuarios utilicen el terminal de acceso a redes de acceso de otros operadores y proteger así sus propios beneficios. Sin embargo, no se ha proporcionado hasta ahora ninguna solución en este campo.

El documento EP 0840480 A2 muestra un método de autenticación. Un verificador genera un número aleatorio y lo transmite a un demandante. El demandante ejecuta una conversión de datos utilizando una clave y transmite el resultado de vuelta al verificador. El verificador ejecuta la misma conversión de datos y compara el resultado con el resultado recibido del demandante. Si los dos resultados son diferentes, el verificador no autoriza al demandante. El sistema de autenticación se utiliza para una unidad de disco óptico a fin de autenticar un dispositivo de reproducción de imagen.

SUMARIO DE LA INVENCIÓN

Por consiguiente, la presente invención se dirige a un terminal de acceso y a un método para ligar el terminal de acceso a un operador a fin de resolver el problema de ser incapaz de ligar un terminal de acceso a un operador que proporciona el terminal de acceso.

Para conseguir el objetivo anterior, la presente invención adopta las soluciones técnicas siguientes.

Se proporciona un método para ligar un terminal de acceso a un operador, que incluye los pasos siguientes:

enviar, por el terminal de acceso, un paquete portador de información privada a un servidor de acceso de banda ancha (BAS);

recibir, por el terminal de acceso, un paquete de respuesta devuelto por el BAS, en donde el paquete de respuesta lleva información privada encriptada obtenida por el BAS de acuerdo con un algoritmo de encriptado convenido;

encriptar, por el terminal de acceso, la información privada utilizando el algoritmo de encriptado convenido; y

comparar, por el terminal de acceso, la información privada encriptada obtenida por el terminal de acceso utilizando el algoritmo de encriptado convenido con la información privada encriptada llevada en el paquete de respuesta, y si las dos son diferentes, terminar un proceso de marcación ascendente hacia el BAS o retirar un enlace con el BAS.

El envío de un paquete portador de información privada al BAS incluye, además, enviar, por el terminal de acceso, un paquete de protocolo de control de enlace (LCP) al BAS, en donde el paquete LCP lleva la información privada.

La recepción de un paquete de respuesta devuelto por el BAS incluye, además, recibir, por el terminal de acceso, un paquete de respuesta LCP del BAS, en donde el paquete de respuesta LCP lleva la información privada encriptada obtenida por el BAS al encriptar la información privada utilizando el algoritmo de encriptado convenido.

Se proporciona un terminal de acceso que incluye un módulo de transmisión de información privada y un módulo de procesamiento de determinación.

El módulo de transmisión de información privada está adaptado para enviar un paquete portador de información

privada a un BAS y recibir un paquete de respuesta devuelto por el BAS. El paquete de respuesta lleva información privada encriptada obtenida por el BAS de acuerdo con un algoritmo de encriptado convenido.

El módulo de procesamiento de determinaciones está adaptado para determinar si la información privada encriptada llevada en el paquete de respuesta es idéntica o no a la información privada encriptada obtenida por el terminal de acceso utilizando un algoritmo de encriptado convenido, y si no es así, terminar un proceso de marcación ascendente hacia el BAS o retirar un enlace con el BAS.

El paquete es un paquete de protocolo de control de enlace (LCP) y el paquete de respuesta es un paquete de respuesta LCP.

Para superar las deficiencias de la técnica anterior se tiene que, según la presente invención, durante la interacción de un módem y un BAS este BAS recibe un paquete del módem, encripta la información privada en el paquete utilizando un algoritmo convenido y luego devuelve la información privada encriptada al módem mediante un paquete de respuesta LCP. El módem encripta la información privada original utilizando el algoritmo convenido y compara la información privada encriptada con la información privada encriptada devuelta por el BAS. Si las dos son diferentes, se termina un proceso de marcación ascendente PPPoE o se retira un enlace establecido. Las soluciones técnicas de la presente invención pueden impedir efectivamente que el usuario utilice un terminal de acceso proporcionado por el operador considerado para acceder a redes de otros operadores, a fin de evitar una perversa competencia entre los operadores. Además, la presente invención se consigue simplemente sin cambiar el modo de interconexión en red o el hábito del usuario, y no tiene una demanda extra de distribución de servicios.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de flujo de una primera realización según la presente invención;

La figura 2 es un diagrama de flujo de una segunda realización según la presente invención; y

La figura 3 es una vista estructural esquemática de un terminal de acceso según una realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

La presente invención proporciona un terminal de acceso y un método para ligar el terminal de acceso a un operador.

Según la presente invención, durante la interacción de un módem y un servidor de acceso de banda ancha (BAS) el BAS recibe un paquete del módem, encripta información privada en el paquete utilizando un algoritmo convenido y devuelve luego la información privada encriptada al módem mediante un paquete de respuesta LCP. El módem encripta la información privada original utilizando el algoritmo de encriptado convenido y compara la información privada encriptada con la información privada encriptada devuelta por el BAS. Si las dos son diferentes, se termina un proceso de marcación ascendente PPPoE o se retira un enlace establecido.

En primer lugar, es necesario extender una entrada de opción definida por el usuario en un protocolo de control de enlace (LCP) para transportar información privada en un paquete LCP y realizar una autenticación del BAS. Esta entrada de opciones tiene que ser identificable en los dos extremos del PPP.

Un formato de la entrada de opciones es como se muestra en la Tabla 1 siguiente. En el formato un campo de Tipo representa el tipo de un parámetro privado y puede ser, por ejemplo, 0x66; un campo de Longitud representa la longitud del parámetro privado; y un campo de Datos se define como el contenido del parámetro privado y puede ser, por ejemplo, una ristra de caracteres.

Durante un proceso de negociación LCP o en un paquete de latidos LCP el módem genera una ristra de caracteres aleatorios, pone la ristra de caracteres aleatorios en la entrada de opciones y envía la entrada de opciones al BAS. El BAS encripta la ristra de caracteres aleatorios utilizando un algoritmo particular (por ejemplo, el BAS puede encriptar la ristra de caracteres aleatorios utilizando un nombre de usuario como clave, y devuelve la ristra de caracteres encriptada al módem a través de la entrada de opciones anterior. El módem encripta la ristra de caracteres aleatorios anteriormente generada utilizando un algoritmo de encriptado convenido y compara el resultado con la ristra de caracteres aleatorios encriptada devuelta por el BAS. Si las dos son idénticas, esto indica que el módem y el BAS utilizan el mismo algoritmo de encriptado y que el módem es proporcionado por el operador de la red de acceso; si las dos son diferentes, esto indica que el módem y el BAS utilizan algoritmos de encriptado diferentes y que el módem no es proporcionado por el operador de la red de acceso; por tanto, se desconecta la conexión PPP.

Tabla 1

Tipo	Longitud	Datos
66	xxx	Ristra de caracteres

La soluciones técnicas se describen en detalle más abajo mediante realizaciones con referencia a las figuras adjuntas.

Realización 1: identificación de una red a acceder por información privada en un modo de ruta

En el modo de ruta se inicia por un módem un proceso de marcación ascendente PPPoE. El módem genera aleatoriamente una ristra de caracteres de datos, pone la ristra de caracteres aleatorios en la entrada de opciones y añade la entrada de opciones a un paquete LCP.

Al recibir el paquete LCP, un BAS encripta la ristra de caracteres de datos y devuelve la ristra de caracteres de datos encriptada al módem mediante un paquete de respuesta. El módem encripta la ristra de caracteres de datos anteriormente generada utilizando un algoritmo de encriptado convenido con el BAS y compara la ristra de caracteres de datos encriptada con el campo de Datos devuelto por el BAS. Si los dos son diferentes, el módem retira el enlace con el BAS.

Se toma como ejemplo un paquete de latidos PPP para ilustrar el proceso anterior, y el diagrama de flujo es como se muestra en la figura 1.

1. Después de establecida una conexión, el módem envía un paquete de latidos portador de una opción definida por el usuario con una opción TIPO=66 al BAS y general aleatoriamente una ristra de caracteres de Datos “123456”.

2. El BAS encripta la ristra de caracteres de Datos “123456” para generar “abcdef”.

3. El BAS devuelve un paquete de respuesta de latidos portador de una opción definida por el usuario con una opción TIPO=66 y Datos=abcdef.

4. El módem encripta “123456” con un algoritmo de encriptado convenido con el BAS y determina si el resultado es “abcdef” o no. Si no es así se realiza el paso 5.

5. El móden retira el enlace con el BAS.

Realización 2: identificación de una red a acceder por información privada en un modo de puente

En el modo de puente se inicia por un PC un proceso de marcación ascendente PPPoE y se añade un punto de detección PPP en el flujo de procesamiento del puente para interceptar y analizar sintácticamente paquetes PPP. Si el paquete es un paquete de datos ascendente, el módem inserta un parámetro extendido en el paquete original y envía el paquete al BAS para su autenticación. Si el paquete es un paquete de datos descendente, el módem verifica primero el paquete y luego extrae el parámetro extendido y envía el paquete al PC.

Asimismo, se toma como ejemplo un paquete de latidos PPP para ilustrar el proceso anterior, y el diagrama de flujo es como se muestra en la figura 2.

1. El PC envía un paquete de latidos al BAS. El módem, al detectar el paquete PPP, intercepta y analiza sintácticamente el paquete, inserta una opción definida por el usuario con una opción TIPO=66 en el paquete de latidos. Los datos aleatoriamente generados son “123456” y el módem reenvía los datos al BAS.

2. El BAS se encripta “123456” para generar “abcdef”.

3. El BAS devuelve un paquete de respuesta de latidos que lleva una opción definida por el usuario con una opción TIPO=66 y Datos=abcdef.

4. El módem intercepta el paquete de respuesta de latidos, extrae la ristra de caracteres de datos del paquete, encripta “123456” utilizando un algoritmo de encriptado convenido y determina si el resultado es “abcdef” o no. Si no lo es, se realiza el paso 5.

5. El módem desecha el paquete de respuesta de latidos.

6. Cuando el PC no recibe que el paquete de respuesta de latidos, el PC retira automáticamente el enlace con el BAS.

La figura 3 muestra una estructura de un terminal de acceso de acuerdo con una realización de la presente invención. El terminal de acceso incluye un módulo de generación y encriptado de información privada, un módulo de transmisión de información privada y un módulo de procesamiento de determinación.

El módulo de generación y encriptado de información privada está adaptado para generar una ristra de caracteres aleatorios como información privada del terminal de acceso y para encriptar la ristra de caracteres aleatorios utilizando un algoritmo de encriptado convenido.

El módulo de transmisión de información privada está adaptado para enviar un paquete portador de la información privada a un BAS y recibir un paquete de respuesta devuelto por el BAS. El paquete de respuesta lleva información privada encriptada obtenida por el BAS de acuerdo con un algoritmo de encriptado convenido.

El módulo de procesamiento de indeterminación está adaptado para determinar si la información privada encriptada llevada en el paquete de respuesta es idéntica o no a una información privada encriptada obtenida por el terminal de acceso utilizando el algoritmo de encriptado convenido, y si no lo es, terminar un proceso de marcación ascendente haciael BAS o retirar un enlace con el BAS.

Será evidente para los expertos en la materia que pueden hacerse diversas modificaciones y variaciones en la estructura de la presente invención sin apartarse del alcance o espíritu de dicha invención. En vista de lo anterior, se pretende que la presente invención cubra modificaciones y variaciones de esta invención siempre que éstas caigan dentro del alcance de las reivindicaciones siguientes y sus equivalentes.

REIVINDICACIONES

1. Un método para ligar un terminal de acceso a un operador, **caracterizado** porque comprende:

enviar, por el terminal de acceso, un paquete de protocolo de control de enlace LCP portador de información privada ("123456") a un servidor de acceso de banda ancha BAS;

recibir, por el terminal de acceso, un paquete de respuesta LCP del BAS, en donde el paquete de respuesta LCP lleva información privada encriptada ("abcdef") obtenida en el BAS al encriptar la información privada utilizando un algoritmo de encriptado convenido;

encriptar, por el terminal de acceso, la información privada utilizando el algoritmo de encriptado convenido; y

comparar, por el terminal de acceso, la información privada encriptada ("abcdef") obtenida por el terminal de acceso utilizando el algoritmo de encriptado convenido con la información privada encriptada llevada en el paquete de respuesta, y si las dos son diferentes, terminar un proceso de marcación ascendente hacia el BAS o retirar un enlace con el BAS,

en donde el paquete LCP es un paquete de latidos de protocolo de punto a punto (PPP).

2. El método según la reivindicación 1, **caracterizado** porque, antes de enviar el paquete LCP portador de la información privada al BAS, dicho método comprende además:

interceptar, por el terminal de acceso, un paquete LCP enviado al BAS desde un cliente e insertar la información privada en el paquete LCP interceptado.

3. El método según la reivindicación 2, **caracterizado** porque la terminación del proceso de marcación ascendente hacia el BAS o la retirada del enlace con el BAS comprende además:

desechar, por el terminal de acceso, el paquete de respuesta LCP; y

terminar el proceso de marcación ascendente o retirar el enlace, por el cliente, cuando no se recibe el paquete de respuesta LCP.

4. El método según la reivindicación 1 ó 2, **caracterizado** porque la información privada es portada por una entrada de opciones del paquete LCP.

5. El método según una cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque la información privada es una ristra de caracteres aleatoriamente generada por el terminal de acceso.

6. Un terminal de acceso, **caracterizado** porque comprende:

un módulo de transmisión de información privada adaptado para enviar un paquete portador de información privada ("123456") a un servidor de acceso de banda ancha BAS y recibir un paquete de respuesta devuelto por el BAS, en donde el paquete de respuesta lleva información privada encriptada ("abcdef") obtenida por el BAS de acuerdo con un algoritmo de encriptado convenido; y

un módulo de procesamiento de determinación adaptado para determinar si la información privada encriptada llevada en el paquete de respuesta es idéntica o no a una información privada encriptada ("abcdef") obtenida por el terminal de acceso utilizando un algoritmo de encriptado convenido, y si no lo es, terminar un proceso de marcación ascendente hacia el BAS o retirar un enlace con el BAS;

en donde el paquete es un paquete de protocolo de control de enlace LCP, el paquete de respuesta es un paquete de respuesta LCP y el paquete LCP es un paquete de latidos de protocolo de punto a punto PPP).

7. El terminal de acceso según la reivindicación 6, **caracterizado** porque comprende además:

un módulo de generación y encriptado de información privada adaptado para generar una ristra de caracteres aleatorios como la información privada del terminal de acceso y para encriptar la ristra de caracteres aleatorios utilizando un algoritmo de encriptado convenido.

8. El terminal de acceso según la reivindicación 6 ó 7, en el que el terminal de acceso es una unidad de terminal remota (RTU) o una pasarela doméstica (HGW).

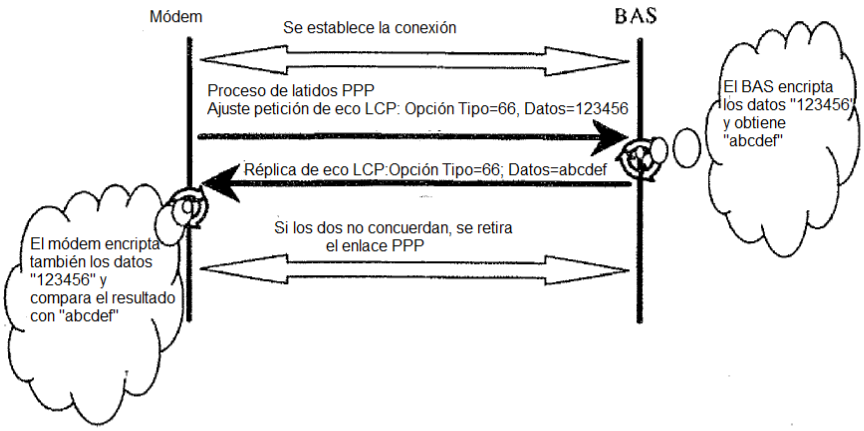
Módem
BAS
Se establece la conexión
Proceso de latidos PPP
Ajuste petición de eco LCP: Opción Tipo=66, Datos=123456
El BAS encripta los datos "123456" y obtiene "abcdef"
Réplica de eco LCP:Opción Tipo=66; Datos=abcdef
El módem encripta también los datos "123456" y compara el resultado con "abcdef"
Si los dos no concuerdan, se retira el enlace PPP

FIG. 1

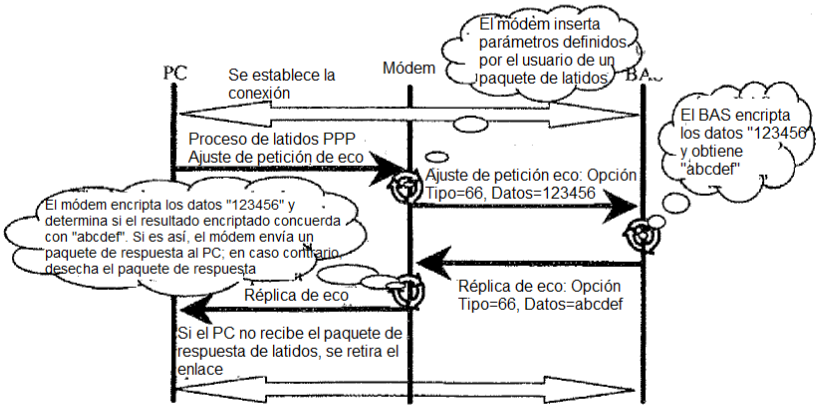
El módem inserta parámetros definidos por el usuario de un paquete de latidos
PC
Se establece la conexión
Módem
BA...
El BAS encripta los datos "123456" y obtiene "abcdef"
Proceso de latidos PPP
Ajuste de petición de eco
Ajuste de petición eco: Opción Tipo=66, Datos=123456
El módem encripta los datos "123456" y determina si el resultado encriptado concuerda con "abcdef". Si es así, el módem envía un paquete de respuesta al PC; en caso contrario, desecha el paquete de respuesta
Réplica de eco
Réplica de eco: Opción Tipo=66, Datos=abcdef
Si el PC no recibe el paquete de respuesta de latidos, se retira el enlace

FIG. 2

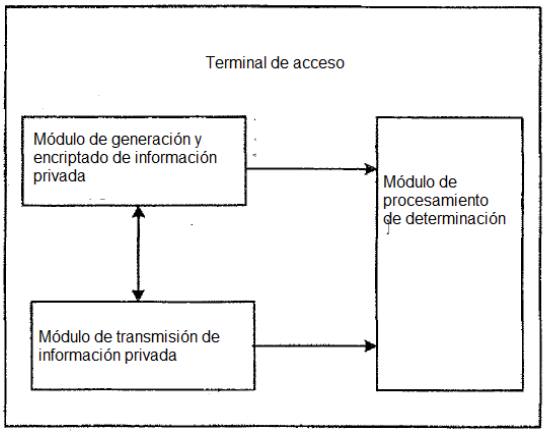
Terminal de acceso
Módulo de generación y encriptado de información privada
Módulo de transmisión de información privada
Módulo de procesamiento de determinación

FIG. 3