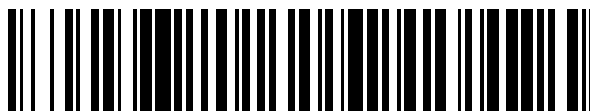


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 531 253**

51 Int. Cl.:

H04L 29/06 (2006.01)

G06F 21/00 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **05.10.2007** **E 07820986 (3)**

97 Fecha y número de publicación de la concesión europea: **26.11.2014** **EP 2084879**

54 Título: **Sistema seguro para transferir datos entre dos equipos**

30 Prioridad:

06.10.2006 FR 0608788

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2015

73 Titular/es:

**THALES (100.0%)
45 RUE DE VILLIERS
92200 NEUILLY SUR SEINE, FR**

72 Inventor/es:

**ALCOUFFE, FABIEN;
WEBER, ERIC y
QUENTIN, ANTOINE**

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 531 253 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema seguro para transferir datos entre dos equipos

La invención se refiere a un sistema seguro para la transferencia de informaciones entre dos equipos (denominados arbitrariamente A y B). El sistema es monodireccional en el sentido 'A hacia B' y asegura de ese modo la no transmisión (voluntaria o no) de informaciones físicas y/o lógicas de 'B hacia A'.

El sistema seguro se utiliza, por ejemplo entre dos equipos que tengan unos niveles de confidencialidad diferentes con el fin de permitir unas transferencias en un sentido mientras se impiden fugas eventuales de información en el sentido opuesto.

Una aplicación posible pero no limitativa de la invención es su integración en el seno de un cable destinado a interconectar dos ordenadores de manera monodireccional.

Se aplica en cualquier sistema en el que se desee restringir la circulación o la transmisión de información en un sentido.

El procesamiento de informaciones sensibles conduce a veces a compartimentar los sistemas. De manera práctica, estas compartimentaciones provocan problemas cuando se trata de intercambiar unas informaciones entre estos sistemas.

Se tolera a veces sin embargo efectuar unos intercambios de información en un sentido preciso mientras que se prohíben los intercambios en el otro sentido.

Por ejemplo, en el campo de la defensa, se tolera la circulación de informaciones en un equipo de nivel de seguridad bajo hacia un equipo que tenga un nivel de seguridad más elevado mientras que los intercambios en el sentido opuesto están prohibidos.

En otro caso de aplicación, una compañía desea poder poner unos recursos a disposición de unos usuarios por Internet evitando cualquier riesgo de ataques que remonten la Internet hacia la red de la compañía (por ejemplo la difusión de virus).

Existen también en el comercio unos dispositivos que realizan unas conversiones de protocolo (por ejemplo, los convertidores USB hacia Ethernet, RJ 12, RS232, IR, Bluetooth, SCSI, DB 15).

Existen también unos cables de interconexión entre equipos informáticos que constituyen un enlace entre estos equipos que permite la difusión bidireccional de datos.

Se encuentran así numerosas soluciones de programas que permiten filtrar las transferencias de informaciones, tales como los programas cortafuegos. Sin embargo, estas soluciones no aseguran una monodireccionalidad física y presentan como riesgo la posibilidad de que se sobrepase la protección.

Aunque puedan ser eficaces, las soluciones de la técnica anterior presentan algunos inconvenientes de los que se presentan algunos en el presente documento a continuación.

Las soluciones de transferencia monodireccional a base de interfaces Ethernet se conciben para interconectar unas redes. Para ello, necesitan generalmente la implementación de un cierto número de equipos tales como unos servidores (encargados de soportar la importante carga de programación provocada por poner servicios a disposición del conjunto de los usuarios de una red); esto convierte a estas soluciones en voluminosas y costosas.

Al utilizar cada aplicación su propio protocolo, es necesario generar la adaptación monodireccional de cada uno de entre ellos en particular.

De manera más general, su volumen, su coste y su complejidad hacen de estas soluciones una respuesta poco adaptada a un enlace entre dos puestos únicamente.

Además, estas soluciones en su funcionamiento normal, se conectan, en cada lado, a la altura de la red y no del puesto. En el caso de que se implementen estas soluciones para un enlace monodireccional al puesto, se utiliza la interfaz frecuentemente única de Ethernet de éste. Es entonces muy posible estar a la vez conectado a la red local y a la solución.

El documento D1 de Tenix PTY Limited titulado "Interactive Link Data Diode" XP 2444389 describe un diodo de infraestructura, es decir destinado conectar dos redes que no están destinadas a una utilización entre dos puestos.

El documento D2 de Tenix titulado "Network Separation for Information Asset Protection White Paper" XP2444390 presenta una arquitectura en la que la utilización de un elemento que asegura la monodireccionalidad de los flujos se somete a la utilización de servidores de un lado y otro. Esto no es posible en el caso de un enlace entre dos puestos.

El documento D4 WO 2005/119462 divulga un sistema para relajar de manera selectiva la información de un computador de una red hacia otro computador de una clasificación inferior. Una operación de control permite efectuar esta "relajación" de la información.

- 5 El documento D3 WO 96/30840 divulga un medio para controlar los flujos de informaciones entre una primera red que tiene un nivel de clasificación dado más elevado que el nivel de clasificación de una segunda red y que comprende un conmutador para permitir el funcionamiento del sistema en dos estados.

La invención se basa, particularmente, en una adaptación del protocolo en el seno del enlace entre los dos equipos. Se parte de un protocolo por ejemplo bidireccional, tal como el protocolo USB o cualquier otro protocolo, que permita la transferencia de datos, se adapta este protocolo en un protocolo monodireccional, aquel que se desee.

- 10 Se puede utilizar cualquier protocolo utilizado en el campo de las transmisiones de informaciones.

La idea de la presente invención consiste particularmente en proporcionar un sistema que se presenta, por ejemplo, bajo la forma de un cable equipado con conectores USB o en anglosajón "Firewire" o de cualquier otra conectividad que permita la conexión en un equipo, asegurando a la vez la transferencia monodireccional de las informaciones y la compatibilidad a la altura de los protocolos de intercambio utilizados por los equipos.

- 15 La invención se refiere a un dispositivo que permita conectar al menos dos puestos informáticos, teniendo un primer puesto informático un nivel de confidencialidad A y teniendo un segundo puesto informático un nivel de confidencialidad B, dialogando los dos puestos informáticos con el exterior utilizando un protocolo bidireccional USB caracterizado porque comprende al menos los elementos siguientes:

- 20 • un soporte que permite la transmisión de los datos entre el primer puesto informático A y el segundo puesto informático B,
- un medio de conexión USB del soporte con el equipo A y un medio de conexión USB del soporte con el equipo B, los datos transmitidos por el puesto A transitan a través de la conexión USB hasta un módulo de gestión USB,
- unos módulos A y B que permiten la adaptación monodireccional del protocolo de transmisión utilizado, y la transmisión de los datos en un sentido monodireccional,
- 25 • permitiendo dicho módulo A la adaptación monodireccional del protocolo bidireccional de transmisión utilizado, y la transmisión de los datos en un sentido monodireccional comprende:
 - un primer módulo adaptado para realizar las adaptaciones lógicas del protocolo bidireccional en un protocolo monodireccional, y
 - un segundo módulo adaptado para realizar la adaptación física de los protocolos, y
 - 30 • un emisor E, y
- porque el módulo B que permite la adaptación bidireccional del protocolo monodireccional de transmisión utilizado y la transmisión de los datos en un sentido monodireccional comprende:
 - un primer módulo de adaptación lógica del protocolo monodireccional en un protocolo bidireccional y
 - un segundo módulo de adaptación física que comprende un receptor R,
 - 35 • dichas comunicaciones son bidireccionales entre el módulo de gestión del protocolo y dichos primeros módulos,
 - dichas comunicaciones son monodireccionales entre dichos primeros módulos y dichos segundos módulos.

El protocolo de transmisión es un protocolo bidireccional del tipo USB, el soporte de transmisión comprende un cable que comprende en cada uno de sus extremos un conector USB.

- 40 La invención se refiere también a un procedimiento que permita conectar al menos dos puestos informáticos, teniendo un primer puesto informático un nivel de confidencialidad A y teniendo un segundo puesto informático un nivel de confidencialidad B, dialogando los dos puestos informáticos con el exterior utilizando un protocolo caracterizado porque comprende al menos una etapa de transmisión de los datos del primer puesto de nivel de confidencialidad A hacia el segundo puesto de nivel de confidencialidad B a través de un módulo de adaptación de protocolo que traduce un protocolo bidireccional en un protocolo monodireccional utilizado para la transferencia de los datos.

El dispositivo según la invención asegura particularmente la ausencia de fugas de informaciones desde el equipo B hacia el equipo A. El sistema ofrece una solución portátil y un reducido volumen.

En el caso de un cable, utiliza los puertos USB y/o Firewire de los puestos informáticos a los que se conecta, lo que deja libre acceso a los otros puertos, por ejemplo los puertos Ethernet.

- 50 La compatibilidad con los protocolos utilizados (USB o Firewire o cualquier otro protocolo que permita la conexión en el equipo) es completa y no necesita por lo tanto ninguna modificación de los equipos en cuanto que generan ese protocolo.

Es más simple de implementar que los sistemas alternativos conocidos en la técnica anterior y no requiere especialista para su instalación o su administración.

Otras características y ventajas de la presente invención surgirán mejor con la lectura de la descripción a continuación, dada a título ilustrativo y en ningún caso limitativo con unas figuras adjuntas que representan:

- 5 • la figura 1, una disposición del dispositivo según la invención,
- la figura 2, diferentes módulos que pueden ser integrados en el dispositivo según la invención, y
- la figura 3, una variante de realización de la invención.

La figura 1 ilustra la conexión de dos puestos informáticos (puesto A y puesto B) por medio de un cable que implementa la invención y que utiliza unas interfaces USB. El cable está equipado con un dispositivo 10 que asegura por un lado el respeto de los protocolos utilizados para la conexión del cable a los puestos informáticos (en este caso el protocolo USB en los dos lados) y por otro lado la circulación de unas informaciones de manera monodireccional desde el puesto A hacia el puesto B. La transmisión monodireccional se asegura debido a que uno de los módulos 3.2a está equipado con un emisor E y el otro 3.2b está equipado con un receptor R.

El dispositivo comprende diferentes módulos:

- 15 [1] Un módulo de gestión 1 del protocolo bidireccional con el puesto A, que asegura el funcionamiento estándar del protocolo bidireccional USB entre el cable 5 y el puesto A. Este módulo genera particularmente las confirmaciones necesarias para el buen funcionamiento del protocolo.
- [2] Un módulo de gestión 2 del protocolo bidireccional con el puesto B que asegura el funcionamiento estándar del protocolo bidireccional USB entre el cable 6 y el puesto B.
- 20 [3] Dos módulos 3a, 3b que tienen como función una adaptación monodireccional de estos dos protocolos entre los dos módulos de gestión 1, 2 citados anteriormente.

El módulo 3a comprende por ejemplo un primer módulo 3.1a que tiene por función realizar las adaptaciones lógicas del protocolo USB, por ejemplo, protocolo monodireccional; y el módulo 3.2a que tiene por función la adaptación física de los protocolos. Este módulo 3.2a comprende un emisor E.

25 El módulo 3b comprende, de manera idéntica, un módulo 3.1b de adaptación lógica del protocolo monodireccional en un protocolo USB o incluso en un protocolo bidireccional y un módulo 3.2b de adaptación física que comprende un receptor R.

Las comunicaciones son bidireccionales, 4, entre el módulo de gestión del protocolo USB y el módulo 3.1, monodireccional, 7, entre el módulo 3.1 y el módulo 3.2 y bidireccionales, 8, entre el módulo 3.2 y el módulo de gestión 2 del protocolo USB.

Unos conectores, 9, de tipo USB en este ejemplo de realización, equipan los cables 5 y 6.

Además de estos módulos, se puede encontrar un cierto número de módulos, representados funcionalmente en la figura 2 y que ofrecen ciertas o varias de las funciones siguientes:

- 35 • Un módulo 10 de gestión de las velocidades a la altura de la adaptación 'Protocolo USB - Protocolo monodireccional' que permite limitar la velocidad del enlace monodireccional mediante la 'solicitud' al puesto bajo de reducir la velocidad en el enlace USB,
- Un módulo 11 de gestión de la redundancia de los datos transmitidos con el fin de disminuir las probabilidades de mala transmisión (o de no transmisión) de los datos en el seno del enlace monodireccional,
- 40 • Un módulo 12 de gestión de control de redundancia cíclica (de tipo CRC) que permite una verificación de la integridad de los datos recibidos a la altura del módulo 'Adaptación de Protocolo monodireccional - Protocolo USB'.
- Un módulo 13 de gestión de la autenticación del usuario.

La alimentación del sistema según la invención se efectúa, o bien mediante la utilización de una fuente exterior, o bien utilizando las fuentes de alimentación disponibles a través de las interfaces utilizadas (por ejemplo, utilización de las alimentaciones dispensadas por el bus USB).

Una vez conectado el cable 5, 6 al puesto A por un lado y al puesto B por otro lado, el sistema funciona en la forma descrita en el presente documento a continuación (caso de la utilización de la invención en el seno de un cable que utiliza unas interfaces USB para establecer un enlace monodireccional entre dos puestos informáticos A y B en el sentido del puesto A hacia el puesto B).

50 Los datos transmitidos por el puesto A transitan a través de la conexión 5 USB hasta un módulo 2 de gestión USB sobre el cable.

A continuación, el módulo 3.1a de adaptación del protocolo USB hacia un protocolo monodireccional, hace transitar estos datos hacia el módulo 3.1b de adaptación de protocolo monodireccional hacia el protocolo USB. Esto se puede realizar de varias maneras diferentes (de las que se dan ciertas de ellas a título de ejemplo y no de limitación):

- Recuperación de las tramas USB que se transmiten tal cual sin modificación por el módulo de adaptación,
- Re-encapsulado de las tramas USB en un protocolo propietario o no (pero necesariamente monodireccional) para una emisión a través del enlace monodireccional,
- Recuperación de los datos solamente (sin las informaciones ligadas al protocolo USB) para una emisión tal cual a través del enlace monodireccional,
- Re-encapsulado de los datos solamente (sin las informaciones ligadas al protocolo USB) en un protocolo propietario o no (pero necesariamente monodireccional) para una emisión a través del enlace monodireccional.

Estas acciones se pueden efectuar al vuelo (utilización de memorias tampón únicamente referenciadas como 10 en la figura 3) o en varios momentos por medio de un paso de los datos por unas memorias 11 intermedias de referencia. Finalmente, los datos así recepcionados por el módulo de adaptación 'protocolo monodireccional - protocolo USB' se emiten hacia el módulo de gestión USB que se encarga entonces de transmitirlos hacia el puesto B respetando el protocolo USB.

Los dos módulos de gestión del protocolo USB tienen igualmente el encargo de generar el reconocimiento del cable por los dos puestos A y B.

- 15 Sin salirse del ámbito de la invención, el procedimiento y dispositivo descrito en el presente documento anteriormente se aplican a cualquier sistema que requiera la transferencia de informaciones en un sentido determinado y una adaptación del protocolo utilizado para la transmisión de informaciones.

La invención se puede aplicar al caso del sistema que pone en práctica la conversión óptica de la señal emitida desde el puesto informático A hacia el puesto informático B. En este caso, la caja 3.2a está equipada con un emisor óptico y la caja 3.2b está equipada con un receptor óptico, el soporte de la transmisión está constituido por una fibra óptica.

REIVINDICACIONES

1. Dispositivo que permite conectar al menos dos puestos informáticos, teniendo un primer puesto informático un nivel de confidencialidad A y teniendo un segundo puesto informático un nivel de confidencialidad B, dialogando los dos puestos informáticos con el exterior utilizando un protocolo bidireccional USB **caracterizado porque** comprende al menos los elementos siguientes:
 - un soporte que permite la transmisión de los datos entre el primer puesto informático A y el segundo puesto informático B,
 - un medio de conexión USB (5) del soporte con el equipo A y un medio de conexión USB (6) del soporte con el equipo B, los datos transmitidos por el puesto A transitan a través de la conexión USB (5) hasta un módulo de gestión USB (1),
 - unos módulos A y B (3a, 3b) que permiten la adaptación monodireccional del protocolo bidireccional de transmisión utilizado, y la transmisión de los datos en un sentido monodireccional,
 - permitiendo dicho módulo A (3a) la adaptación monodireccional del protocolo bidireccional de transmisión utilizado, y la transmisión de los datos en un sentido monodireccional comprende:
 - un primer módulo (3.1a) adaptado para realizar las adaptaciones lógicas del protocolo bidireccional en un protocolo monodireccional, y
 - un segundo módulo (3.2a) adaptado para realizar la adaptación física de los protocolos
 - un emisor E, y
 - el módulo (3b) que permite la adaptación bidireccional del protocolo monodireccional de transmisión utilizado y la transmisión de los datos en un sentido monodireccional comprende:
 - un primer módulo (3.1b) de adaptación lógica del protocolo monodireccional en un protocolo bidireccional y
 - un segundo módulo (3.2b) de adaptación física que comprende un receptor R,
 - dichas comunicaciones son bidireccionales, (4, 7), entre el módulo de gestión del protocolo y dichos primeros módulos (3.1a, 3.1b),
 - dichas comunicaciones son monodireccionales, (8), entre dichos primeros módulos (3.1a, 3.1b) y dichos segundos módulos (3.2a, 3.2b).
2. Dispositivo según la reivindicación 1 **caracterizado porque** el módulo (3.1a) de adaptación del protocolo USB hacia un protocolo monodireccional está adaptado para hacer transitar los datos hacia el módulo (3.1b) de adaptación del protocolo monodireccional hacia el protocolo USB utilizando uno de los procedimientos siguientes:
 - Recuperación de las tramas USB que se transmiten tal cual sin modificación por el módulo de adaptación,
 - Re-encapsulado de las tramas USB en un protocolo monodireccional para una emisión a través del enlace monodireccional,
 - Recuperación de los datos solamente sin las informaciones ligadas al protocolo USB para una emisión tal cual a través del enlace monodireccional,
 - Re-encapsulado de los datos solamente sin las informaciones ligadas al protocolo USB en un protocolo monodireccional para una emisión a través del enlace monodireccional.
3. Dispositivo según la reivindicación 1, **caracterizado porque** el protocolo de transmisión es un protocolo bidireccional del tipo USB, el soporte de transmisión comprende un cable que comprende en cada uno de sus extremos un conector USB.
4. Dispositivo según la reivindicación 3, **caracterizado porque** el conjunto comprende un módulo (10) de gestión de las velocidades a la altura de la adaptación "Protocolo USB-Protocolo monodireccional".
5. Dispositivo según una de las reivindicaciones 1 a 3, **caracterizado porque** el soporte de la transmisión está provisto de un módulo (11) de gestión de la redundancia de los datos transmitidos.
6. Dispositivo según una de las reivindicaciones 1 a 3, **caracterizado porque** comprende un módulo (12) de gestión del control de redundancia cíclica.
7. Dispositivo según una de las reivindicaciones 1 a 3, **caracterizado porque** comprende un módulo (13) de gestión de la autenticación de los usuarios.
8. Procedimiento puesto en práctica en un dispositivo según una de las reivindicaciones 1 a 7, que permite conectar al menos dos puestos informáticos, teniendo un primer puesto informático un nivel de confidencialidad A y teniendo un segundo puesto informático un nivel de confidencialidad B, dialogando los dos puestos informáticos con el exterior utilizando un protocolo, **caracterizado porque** comprende al menos una etapa de transmisión de los datos del puesto informático de nivel de confidencialidad A hacia el segundo puesto que tiene un nivel de confidencialidad B a través de un módulo de adaptación de protocolo que traduce un protocolo bidireccional en un protocolo monodireccional utilizado para la transferencia de los datos.

9. Procedimiento según la reivindicación 8, **caracterizado porque** se utiliza como protocolo, el protocolo USB y **porque** comprende al menos las etapas siguientes:

- Recuperación de las tramas USB que se transmiten tal cual sin modificación por el módulo de adaptación,
- Re-encapsulado de las tramas USB en un protocolo propietario o no para una emisión a través del enlace monodireccional,
- Recuperación de los datos solamente (sin las informaciones ligadas al protocolo USB) para una emisión tal cual a través del enlace monodireccional,
- Re-encapsulado de los datos solamente (sin las informaciones ligadas al protocolo USB) en un protocolo monodireccional para una emisión a través del enlace monodireccional.

5

10

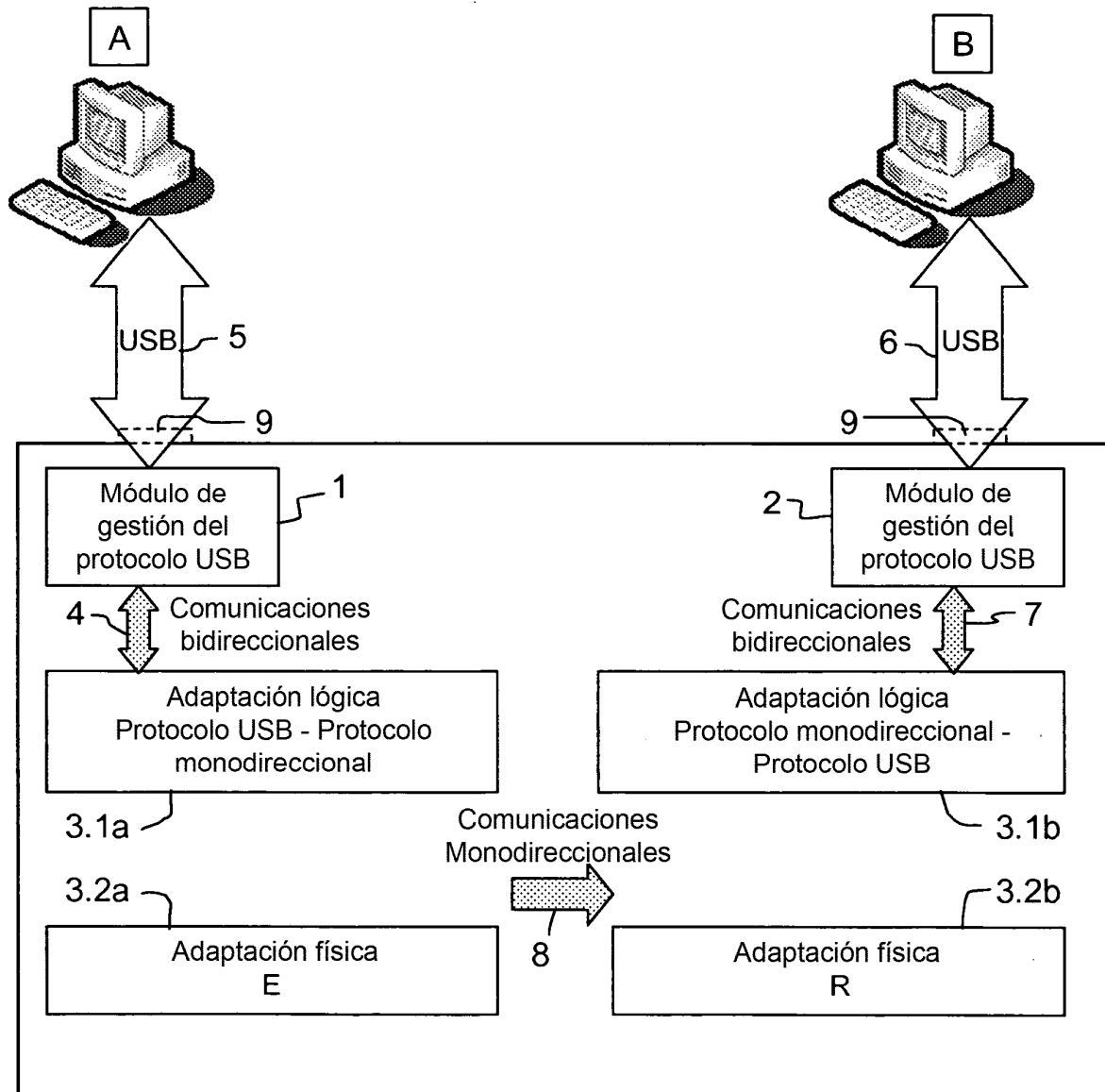


FIG.1

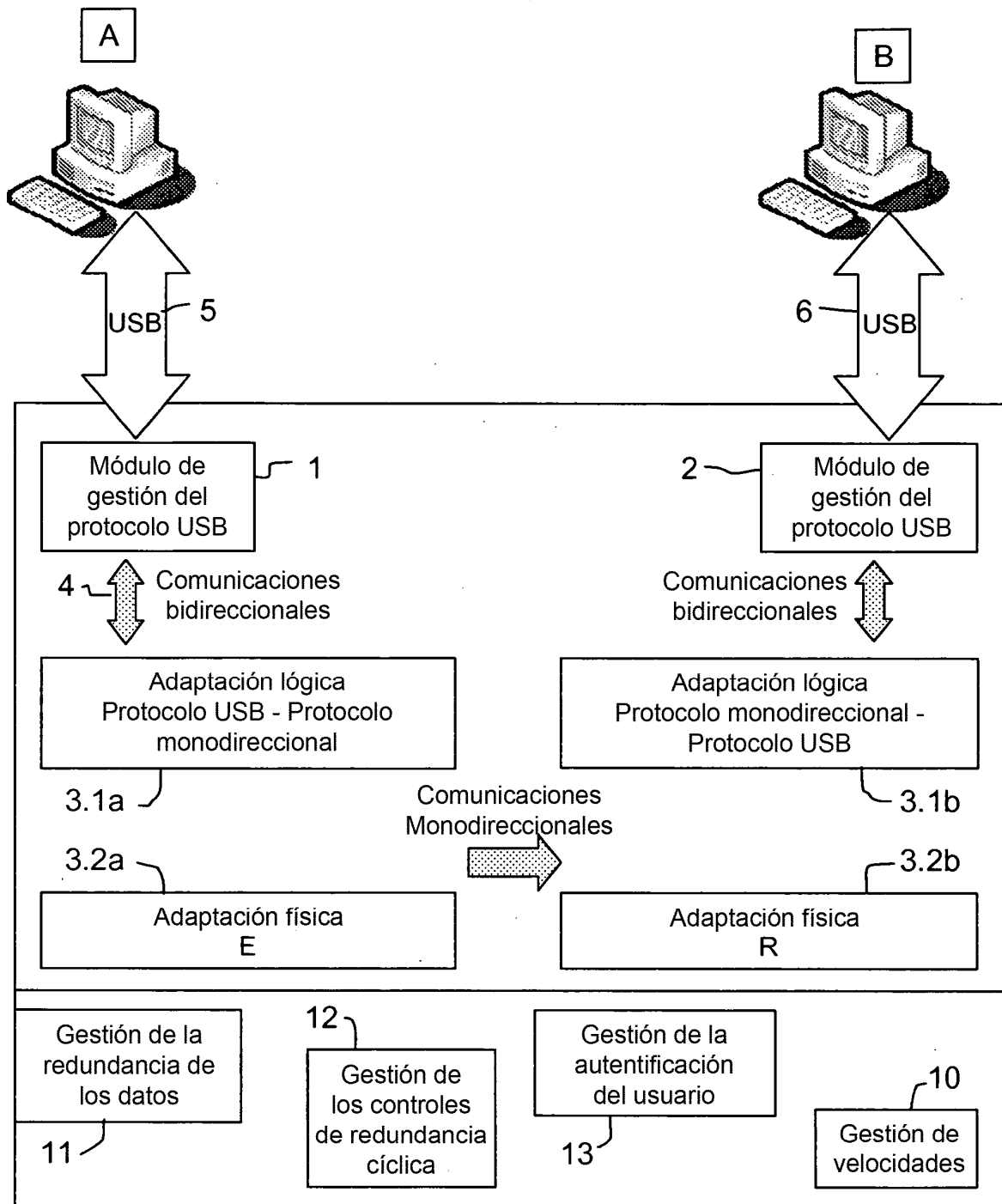


FIG.2

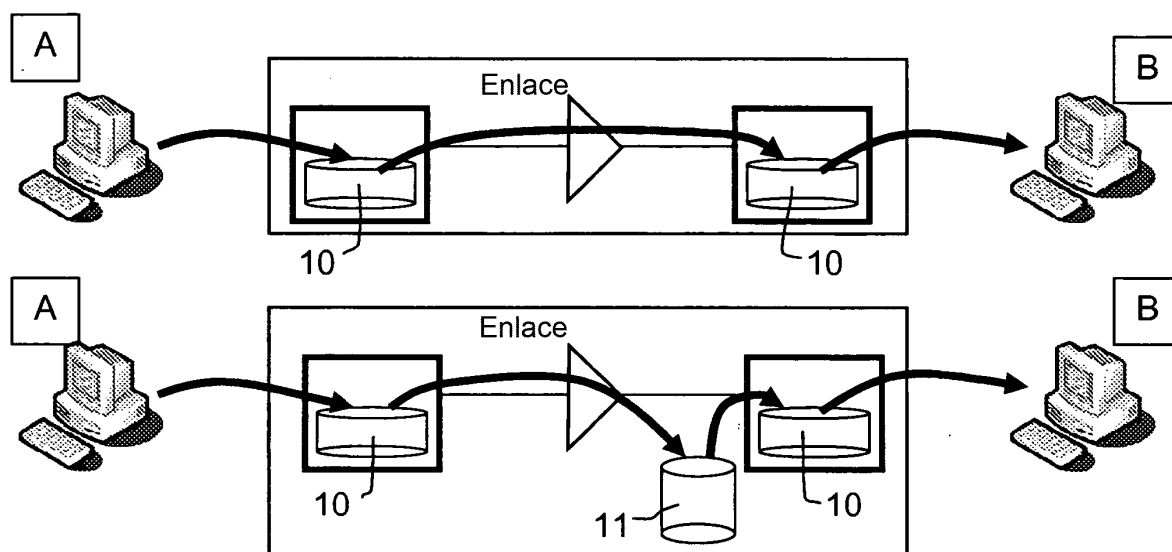


FIG.3