(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 311 614**

(51) Int. Cl.:
H04L 12/00 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02747631 .6**
(96) Fecha de presentación : **03.05.2002**
(97) Número de publicación de la solicitud: **1502384**
(97) Fecha de publicación de la solicitud: **02.02.2005**

(54) Título: **Método y sistema en una red de comunicaciones para asignar y cambiar direcciones de nivel de enlace.**

(45) Fecha de publicación de la mención BOPI:
16.02.2009

(45) Fecha de la publicación del folleto de la patente:
16.02.2009

(73) Titular/es: **Nokia Siemens Networks Oy**
Karaportti 3
02610 Espoo, FI

(72) Inventor/es: **Pietilainen, Antti y**
Pohjola, Olli-Pekka

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Método y sistema en una red de comunicaciones para asignar y cambiar direcciones de nivel de enlace.

La presente invención se refiere al cambio de las direcciones de entidades en una red de comunicaciones.

Cuando se están transfiriendo datos a través de una red de comunicaciones, con frecuencia resulta importante proteger los datos para que no acceda a los mismos una persona no autorizada. Frecuentemente los datos se cifran para evitar que sean leídos por alguien que no disponga de una clave para descifrarlos. A este tipo de acceso no autorizado (en inglés *hacking*) hostil de datos de otro usuario también se le puede denominar rastreo (en inglés *sniffing*) o interceptación (en inglés *eavesdropping*). Sin embargo, además de los propios datos, existe otra información auxiliar que puede ser útil para una persona no autorizada que tenga acceso a la red. La misma podría incluir información sobre el tipo, la temporización o la cantidad de tráfico que se está enviando a entidades particulares en la red: puede proporcionar pistas que podrían ayudar a un pirata informático a violar la seguridad de la red, o, en una red comercial, podría revelar información comercial sensible sobre el nivel al que se está utilizando la red.

Los problemas de protección contra el acceso a datos e información auxiliar son especialmente importantes en redes de medios compartidos. En una red de medios compartidos, varias entidades están conectadas entre sí mediante un enlace de datos común, y a través del enlace se emiten por difusión general datos destinados a una o más de las entidades. Si se desea que solamente una de las entidades reciba ciertos datos, entonces se puede usar un esquema de difusión general y selección. Para implementar este esquema, cada entidad tiene una dirección de nivel de enlace en la red y los datos se transmiten conjuntamente con la dirección de nivel de enlace de la entidad a la que están destinados. Cuando una entidad reconoce que su dirección de nivel de enlace es transmitida conjuntamente con una cantidad de datos, decodifica esos datos.

La patente US nº 6.028.933 describe un método para cifrar datos a través de una red de acceso múltiple de medios compartidos. Este documento sugiere la mejora de la seguridad mediante un cifrado total de todos los bits de sentido descendente.

Las redes de medios compartidos ofrecen una forma rentable de implementar una red para proporcionar a varios nodos acceso a un recurso tal como Internet. En una situación de este tipo, la red puede comprender un transceptor individual de alta velocidad en un nodo de acceso o concentrador, que sea capaz de comunicarse con muchos nodos en las instalaciones de los consumidores. Un bus individual compartido de alta velocidad conecta el concentrador a los nodos de los consumidores (conocidos también como nodos satélite). Los nodos satélite necesitan una interfaz de alta velocidad para recibir información a través del enlace, aunque el resto del conjunto electrónico en los nodos satélite puede ser más lento y por lo tanto relativamente económico. La red puede adoptar cualquier topología adecuada, por ejemplo, en estrella, en árbol, anular, en bucle o lineal. Como todos los nodos están conectados al mismo bus de alta velocidad, los mismos pueden escuchar el tráfico que no está destinado a ellos. Incluso si los datos están cifrados, un nodo oyente podría detectar información auxiliar que podría resultar valiosa: por ejemplo, podría identificar cuántos datos van dirigidos a cada una de las otras entidades y cuándo son enviados. Adicionalmente, si el oyente quisiera leer comunicaciones dirigidas a un nodo en particular, podría interceptar transmisiones que van dirigidas a ese nodo y almacenarlas para su descifrado posteriormente usando un ordenador potente.

Las redes inalámbricas de medios compartidos corren especialmente el riesgo de sufrir esta forma de monitorización ya que resulta difícil evitar el acceso físico al canal de datos. Por ejemplo, en las redes LAN inalámbricas IEEE802.11b cualquier receptor compatible dentro del alcance del concentrador puede escuchar transmisiones destinadas a otras entidades en la red.

Una de las soluciones a estos problemas es que los consumidores u operadores de redes que estén preocupados por la privacidad usen un enlace dedicado entre el concentrador y cada nodo. No obstante, esta opción resulta económicamente costosa.

Por lo tanto, existe una necesidad de mejorar la seguridad de redes consiguiendo que resulte más difícil que un oyente acceda a datos auxiliares sobre el uso de la red.

Según uno de los aspectos de la presente invención, se proporciona un sistema de comunicaciones que comprende: una pluralidad de nodos de comunicación conectados mediante un enlace de datos; un controlador de comunicaciones para asignar direcciones de nivel de enlace a los nodos de comunicación con lo cual los nodos se pueden identificar para las comunicaciones a través del enlace; estando dispuesto el controlador de comunicaciones para cambiar de vez en cuando las direcciones asignadas a cada nodo de comunicación y transmitir la dirección recién asignada al nodo respectivo de forma cifrada.

De la forma más preferida, el controlador de comunicaciones está dispuesto para cambiar las direcciones de vez en cuando durante un periodo mientras está teniendo lugar la comunicación con los nodos a través del enlace de datos. Dicha comunicación puede ser discontinua, y de la forma más preferida es una comunicación basada en paquetes. Dicha comunicación puede ser adecuadamente una comunicación de datos de tráfico entre el controlador de comunicaciones y el o cada nodo.

El enlace de datos es preferentemente un enlace de datos compartido. El enlace de datos compartido se comparte entre los nodos de manera que cualquier nodo conectado al enlace de datos tiene acceso a comunicaciones a través del enlace. De forma adecuada, cada nodo está dispuesto para interpretar únicamente las comunicaciones a través del nodo que van dirigidas al mismo. El enlace de datos puede adoptar cualquier topología adecuada. El enlace de datos puede ser, por ejemplo, un enlace por cable o un enlace inalámbrico.

En las reivindicaciones subordinadas se exponen otros aspectos de la invención.

A continuación se describirá la presente invención a título de ejemplo haciendo referencia a los dibujos adjuntos.

En los dibujos:

la figura 1 es un diagrama esquemático de un sistema de transmisión de datos, que muestra componentes de un concentrador y un terminal de forma detallada.

En el sistema de transmisión de datos de la figura 1, existe una red en la que se implementan procedimientos para inhibir el acceso por parte de un oyente a datos auxiliares sobre el uso de la red. A dispositivos receptores en la red se les asignan direcciones de nivel de enlace para ser usadas en la red, y las direcciones de nivel de enlace se cambian de vez en cuando de manera que resulta problemático para un oyente determinar qué entidades tiene qué direcciones. Esto significa que resulta difícil para el oyente obtener información auxiliar sobre el uso de la red. Para complementar la seguridad de este procedimiento, se usan también procedimientos adicionales, que se describen de forma más detallada posteriormente.

En la figura 1, se presenta una red mostrada de forma general con la referencia 1, que comprende un concentrador 2 y un conjunto de nodos satélite 3. Uno de los nodos satélite: 3a, se muestra más detalladamente que los otros. Los nodos satélite están conectados al concentrador mediante un bus compartido de datos de alta velocidad 4. El concentrador 2 está conectado a recursos de datos adicionales, por ejemplo, una memoria local de datos 5 e internet 6.

En la práctica, los nodos satélite podrían ser, por ejemplo, ordenadores personales o cajas de adaptación de televisores dispuestos para recibir datos desde el bus de datos. El bus de datos podría ser un enlace de fibra óptica instalado en las instalaciones de los consumidores. En lugar de un bus de datos, los medios compartidos pueden comprender una interfaz inalámbrica tal como, por ejemplo, una interfaz de radiocomunicaciones u óptica.

En la figura 1 se muestran más detalladamente componentes del concentrador 2 y uno de los nodos 3a. El concentrador comprende una interfaz 10 mediante la cual está conectado a los recursos de datos de sentido ascendente 5, 6; y una interfaz 11 mediante la cual está conectado al bus de datos 4. La interfaz 10 podría ser un conmutador de Ethernet o un encaminador IP. La interfaz 11 podría ser un transceptor óptico. Los datos que pasan entre las interfaces 10 y 11 pasan a través de un conversor 12, que funciona bajo el control de un controlador de enlace 13. El controlador de enlace tiene una memoria 14 en la que mantiene un registro de la información necesaria para la comunicación en la red con cada uno de los nodos 3. Este comprende, para cada uno de los nodos 3, una lista de: la dirección de nivel de enlace en la red 1 que está asignada a ese nodo, y la(s) clave(s) de cifrado/descifrado asignada(s) a ese nodo. También se puede almacenar otra información para soportar protocolos de seguridad adicionales, por ejemplo, la dirección MAC del nodo respectivo.

El concentrador 2 puede realizar una traducción de direcciones de manera que los nodos 3 se representen para los recursos de sentido ascendente mediante la dirección del concentrador.

Cuando se van a enviar datos desde la interfaz 10 a uno de los nodos satélite, los mismos se hacen pasar al conversor 12 que funciona bajo el control del controlador de enlace 13 para formar un mensaje con vistas a su transmisión a través del enlace 4. El controlador de enlace proporciona al conversor la dirección de nivel de enlace del nodo de destino y la clave de cifrado para las transmisiones hacia ese nodo. El conversor cifra los datos usando la clave de cifrado y forma el mensaje para que sea dirigido hacia la dirección del nodo. A continuación, el mensaje se traslada a la interfaz 11.

Cuando se van a enviar datos desde la interfaz 11 a un recurso de sentido ascendente, los mismos se trasladan al conversor 12 que funciona bajo el control del controlador de enlace 13 para formar un mensaje para su transmisión de sentido ascendente. El conversor informa al controlador de enlace sobre la dirección de nivel de enlace desde la que se enviaron los datos. El controlador de enlace recupera de la memoria 14 la clave de descifrado apropiada y la proporciona al conversor. A continuación, el conversor descifra los datos usando la clave de descifrado y traslada los datos a la interfaz 11.

En cada nodo satélite 3 existe un controlador transceptor 16. El controlador transceptor 16 incluye una memoria 17 que almacena la dirección de nivel de enlace y la(s) clave(s) de cifrado/descifrado asignada(s) al modo. El controlador transceptor está conectado a un selector de datos 18 y a una unidad de cifrado/descifrado 19. El controlador transceptor 16 informa al selector de datos 18 sobre la dirección asignada al nodo. El selector de datos monitoriza datos en el enlace 4 en relación con mensajes dirigidos a ese nodo. Todos estos mensajes se trasladan a la unidad de cifrado/descifrado 19. La misma descifra los mensajes usando la clave de descifrado que le ha proporcionado el controlador transceptor 16 y, a continuación, traslada los datos para su uso local (véase enlace 20). Cuando, a través del enlace 20, se reciben datos para su transmisión a través del enlace 4, los datos pasan a la unidad de cifrado/descifrado 19, que cifra los datos

usando la clave de cifrado (según la ha proporcionado el controlador transceptor 16) del nodo y a continuación los traslada al concentrador 2 a través del enlace 4.

El concentrador 1 incluye también un controlador de seguridad de enlace 15. El controlador de seguridad del enlace adapta al funcionamiento de la red a través del bus de datos 4.

El controlador de seguridad de enlace controla la asignación de direcciones de nivel de enlace a los nodos 3. El controlador de seguridad de enlace tiene un grupo de direcciones disponibles para él y almacena un registro de las que han sido asignadas a nodos 3. Cuando un nodo nuevo se conecta a la red, al mismo se le asigna una de las direcciones no asignadas del grupo. Adicionalmente, de vez en cuando el controlador de seguridad del enlace cambia las direcciones asignadas a los nodos. Realiza esta acción seleccionando otra dirección no asignada del grupo, trasladándola al nodo cuya dirección se va a cambiar y, a continuación, almacenando esa dirección como asignada y la dirección previamente asignada a ese nodo como no asignada. Cuando se asigna una dirección a un nodo, el mismo la almacena en la memoria 17 y, a continuación, la usa tal como se ha descrito anteriormente.

Cuando el controlador de seguridad de enlace 15 asigna una dirección a un nodo, transmite esa dirección al nodo de forma cifrada, por medio del sistema de cifrado previamente establecido usando las unidades 11 y 18. De este modo, los nodos que están escuchando en el enlace 4 no pueden determinar la dirección nueva asignada al nodo. Esto puede resultar imposible cuando se asigna por primera vez al nodo una dirección ya que, en esa fase, puede que no se haya establecido el cifrado para ese nodo. En esa situación, el controlador de seguridad asigna la dirección inicial del nodo en una transmisión simple y, a continuación, una vez que se ha establecido el cifrado, asigna otra dirección a través del canal cifrado.

El controlador de seguridad de enlace determina cuándo cambiar las direcciones asignadas a nodos. Lo puede hacer de forma aleatoria o seudoaleatoria, o periódica. Se prefiere que cambie las direcciones de los nodos de una en una a intervalos aleatorios. El tiempo entre cambios de dirección se puede seleccionar convenientemente para equilibrar el aumento de seguridad que se obtiene a partir del cambio de dirección con el tráfico y el procesamiento adicionales implicados en un cambio de dirección. Esto dependerá de las condiciones de la red.

El controlador de seguridad de enlace selecciona direcciones nuevas de forma aleatoria o seudoaleatoria de entre el grupo de direcciones.

Como consecuencia de estas características, alguien que esté escuchando en el enlace 4 no puede realizar un seguimiento fácilmente sobre qué dirección se asigna a qué nodo. Por lo tanto, no puede monitorizar qué volumen de tráfico se está trasladando hacia qué nodo.

Cuando se cambia una dirección, se actualiza la memoria 14. Existen dos opciones. Si el nodo cuya dirección se cambia va a mantener la misma clave de cifrado que tenía antes, entonces la lista de la memoria 14 se actualiza para asociar la dirección nueva de ese nodo a su clave o par de claves anterior. Alternativamente, la clave de cifrado del nodo se puede cambiar al mismo tiempo que se cambia su dirección. En ese caso, el registro almacenado en la memoria 14 para la dirección anterior se elimina, y se añade un registro nuevo para asociar la dirección nueva a la clave o par de claves nuevo.

Para proporcionar seguridad adicional, el concentrador 2 puede estar dispuesto para transmitir datos hacia los nodos en un orden aleatorio o seudoaleatorio. Los datos se envían a los nodos en unidades discretas, tales como tramas o paquetes. Cuando se van a transmitir dichos datos hacia los nodos, el orden en que se envían las unidades lo determina de forma aleatoria (o seudoaleatoria) el concentrador 2. A continuación, el orden en el que los modos van dirigidos es sustancialmente impredecible para un oyente en el enlace. Esto proporciona una seguridad adicional.

La red tiene otra característica de seguridad. El generador de tráfico 21 es capaz de generar tráfico espurio que se puede transportar a través del enlace 4. Realiza esto durante los tiempos en los que el enlace, si no, estaría en reposo. El tráfico espurio puede tener cualquier contenido, aunque convenientemente es aleatorio o seudoaleatorio. El tráfico espurio se forma en mensajes dirigidos, como otro tráfico a través del enlace, aunque va dirigido a direcciones que no están asignadas, de manera que no es recogido por ninguno de los nodos. El resultado de esto es que un oyente en el enlace no puede decir cuánto tráfico hay en el enlace, ya que el enlace aparece como si estuviera utilizado en su totalidad o casi en su totalidad todo el tiempo.

Los sistemas antes descritos se implementan de la forma más conveniente en redes por conmutación de paquetes, aunque también se podrían usar en redes de otros tipos.

Una de las plataformas adecuadas para implementar los sistemas antes descritos es la Red Óptica Pasiva de Ethernet (EPON) que está siendo normalizada actualmente en el grupo de trabajo Ethernet en la Primera Milla (EFM) IEEE802.3ah.

Ethernet PON es una red de punto-a-multipunto usada para enviar tramas de Ethernet. Se ha planificado el uso del método de difusión general y selección para el tráfico de sentido descendente y un método de acceso múltiple por división de tiempo para el tráfico de sentido ascendente. Habrá una dirección PHY ID que se usará en la emisión por

difusión general de tramas de Ethernet hacia nodos de destino y con la cual los nodos de destino pueden seleccionar las tramas que deberían decodificar. La PHY ID estará incluida en el comienzo de una trama de Ethernet. La estructura de la trama de Ethernet será entonces:

PHY ID

DIRECCIÓN MAC

---CAMPOS---

---DATOS---

---OTROS CAMPOS---

Se debe cifrar toda la información excepto la PHY ID. La PHY ID es un identificador que identifica qué nodo va a recibir la trama. De este modo, la PHY ID indica también qué clave de cifrado y descifrado se van a usar para la trama.

En un sistema de este tipo, el proceso para cambiar la PHY ID para implementar la función de cambio de dirección del controlador de seguridad 15 según se ha descrito anteriormente es:

1. Se envía una orden "PHY ID Nueva" al nodo de destino cuya dirección se va a cambiar. La orden se envía en una trama que se direcciona usando la PHY ID actual (antigua) del nodo y se cifra usando la clave de cifrado apropiada para ese nodo. La orden incluye, en la parte cifrada de la trama, la PHY ID nueva para el nodo. Esta PHY ID nueva está vinculada a la clave de cifrado existente, aunque la clave también se podría cambiar al mismo tiempo (en la misma orden que se da instrucciones al nodo para cambiar la dirección), para aumentar adicionalmente la seguridad.

2. En el nodo de destino, la orden se identifica como dirigida al mismo, y es descifrada e interpretada. A continuación, el nodo de destino adopta la PHY ID nueva y, si estuviera presente, la clave de cifrado nueva.

La presente invención se implementa preferentemente a través de un enlace de datos compartidos, ya que en esa situación puede proporcionar ventajas adicionales, aunque también se podría implementar a través de enlaces de otros tipos. El enlace de datos podría ser cualquier forma adecuada de canal de datos.

Por la presente, el solicitante da a conocer de forma aislada cada característica individual descrita en el presente documento y cualquier combinación de dos o más de dichas características, en la medida que estas características o combinaciones puedan ser llevadas a la práctica basándose en la presente memoria descriptiva como un conjunto y teniendo en cuenta el conocimiento general común de los expertos en la materia, con independencia de si dichas características o combinaciones de características resuelven cualquier problema dado a conocer en el presente documento, y sin limitación al alcance de las reivindicaciones. El solicitante indica que aspectos de la presente invención pueden constar de cualquiera de estas características individuales o combinaciones de características. A la vista de la descripción anterior, resultará evidente para un experto en la materia que se pueden realizar varias modificaciones dentro del alcance de la invención que queda definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Sistema de comunicaciones (1), que comprende:

una pluralidad de nodos de comunicación conectados mediante un enlace de datos;

un controlador de comunicaciones (13) para asignar direcciones de nivel de enlace a los nodos de comunicación con lo cual los nodos se pueden identificar para las comunicaciones a través del enlace;

estando dispuesto el controlador de comunicaciones (13) para cambiar de vez en cuando las direcciones asignadas a cada nodo de comunicación (3) y transmitir de forma cifrada al nodo respectivo la dirección recién asignada.

2. Sistema de comunicaciones según la reivindicación 1, en el que las comunicaciones a través del enlace comprenden una parte de dirección que indica la dirección del de los nodos al que va dirigida la comunicación respectiva y una parte de carga útil.

3. Sistema de comunicaciones según la reivindicación 2, en el que la parte de dirección no está cifrada.

4. Sistema de comunicaciones según la reivindicación 2 ó 3, en el que la parte de carga útil está cifrada.

5. Sistema de comunicaciones según cualquiera de las reivindicaciones anteriores, en el que las comunicaciones a través del enlace son en forma de paquetes de datos.

6. Sistema de comunicaciones según cualquiera de las reivindicaciones anteriores, en el que el sistema de comunicaciones comprende una unidad de distribución de datos (2) conectada entre el enlace de datos (4) y por lo menos una fuente externa de datos para reenviar datos desde la fuente de datos hacia los nodos a través del enlace de datos.

7. Sistema de comunicaciones según la reivindicación 6, en el que la unidad de distribución de datos está dispuesta para reenviar los datos hacia los nodos en un orden aleatorio o seudoaleatorio.

8. Sistema de comunicaciones según la reivindicación 6 ó 7, en el que la unidad de distribución de datos (2) comprende un generador de tráfico (21) que está dispuesto para, por lo menos en algunos tiempos en los que, si no, no estaría transmitiendo datos a los nodos, transmitir a través del enlace comunicaciones direccionadas a una dirección que no está asignada a ninguno de los nodos.

9. Sistema de comunicaciones según cualquiera de las reivindicaciones anteriores, en el que un nodo (3) está dispuesto para almacenar la dirección asignada al mismo y para ignorar comunicaciones sobre el canal de datos direccionadas a direcciones que no sean esa dirección.

10. Sistema de comunicaciones según cualquiera de las reivindicaciones anteriores, en el que el enlace es un enlace de Ethernet.

11. Sistema de comunicaciones según la reivindicación 10, en el que las direcciones de nivel de enlace son direcciones PHY ID de Ethernet.

12. Método para comunicar datos en un sistema de comunicaciones (1), comprendiendo el sistema de comunicaciones una pluralidad de nodos de comunicación conectados mediante un enlace de datos y un controlador de comunicaciones; comprendiendo el método:

el controlador de comunicaciones (13) que asigna direcciones de nivel de enlace a los nodos de comunicación (3) con lo cual los nodos se pueden identificar para comunicaciones a través del enlace;

el controlador de comunicaciones (13) que cambia de vez en cuando las direcciones asignadas a cada nodo de comunicación (3) y transmite de forma cifrada al nodo respectivo la dirección recién asignada.

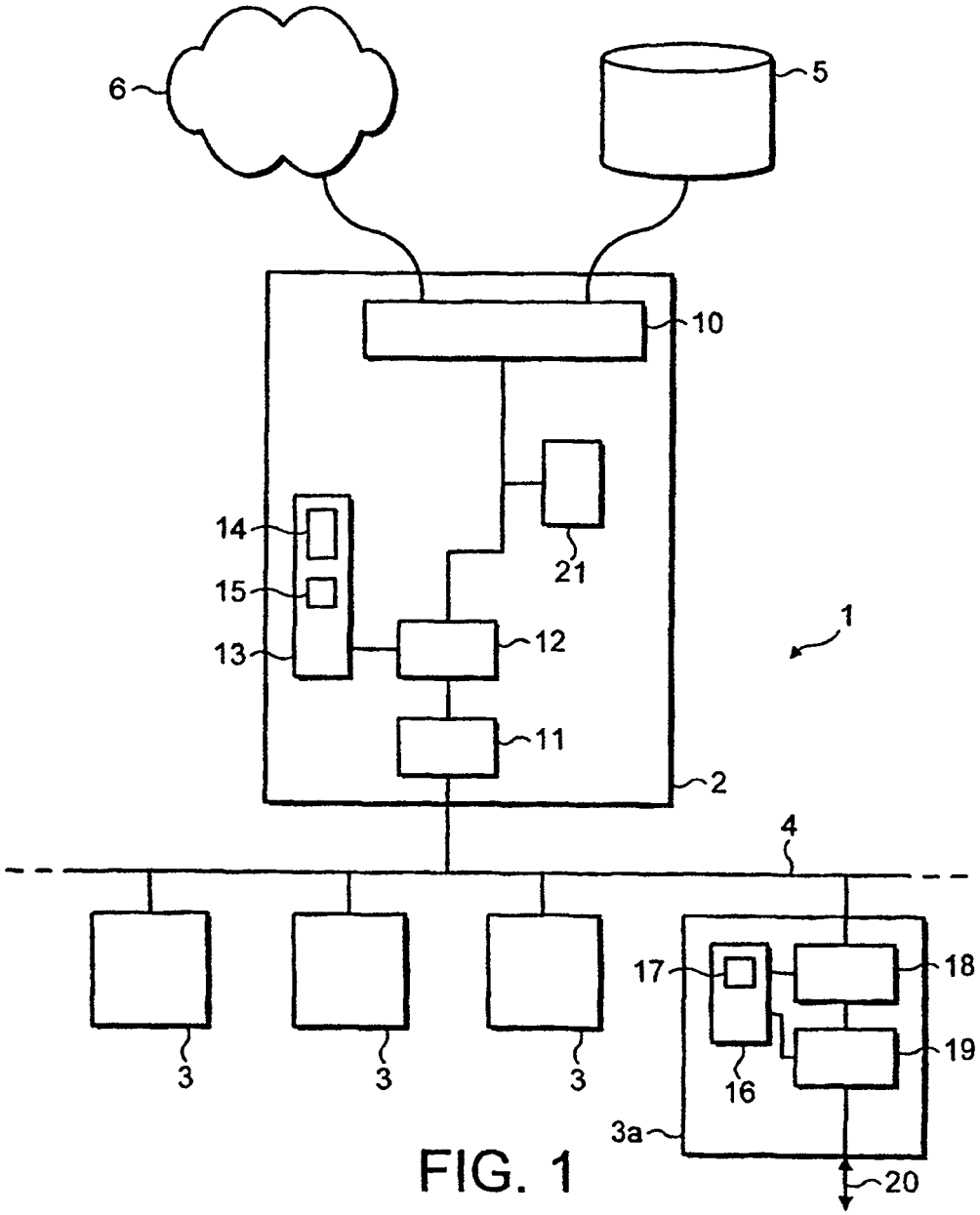

FIG. 1