(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 304 251**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04727273 .7**
(86) Fecha de presentación : **14.04.2004**
(87) Número de publicación de la solicitud: **1735983**
(87) Fecha de publicación de la solicitud: **27.12.2006**

(54) Título: **Procedimiento y sistema para la gestión de la distribución de contenidos en redes de comunicación.**

(45) Fecha de publicación de la mención BOPI:
01.10.2008

(45) Fecha de la publicación del folleto de la patente:
01.10.2008

(73) Titular/es: **Telecom Italia S.p.A.**
Piazza Degli Affari 2
20123 Milano, IT

(72) Inventor/es: **Maffione, Eugenio Maria y**
Gambaro, Giovanni

(74) Agente: **Ponti Sales, Adelaida**

DESCRIPCIÓN

Procedimiento y sistema para la gestión de la distribución de contenidos en redes de comunicación.

Campo de la invención

La presente invención se refiere a la distribución de contenidos en redes de comunicación.

La presente invención se ha desarrollado prestando una atención específica a la posible aplicación en un escenario de Internet, por ejemplo para controlar el acceso a contenidos de medios en aquellos contextos operativos en los que se utilizan una o más tecnologías "verticales" para distribuir y tener acceso a contenidos de medios en una red móvil o fija.

Descripción de la técnica relacionada

En los últimos años, los servicios disponibles a través de Internet y/o de redes corporativas y basados en la distribución de contenidos de medios (especialmente de tipo multimedia) han adquirido una importancia significativa. Esto es posible tanto por la disponibilidad de anchos de banda de transmisión mayores para el acceso, como por el aumento continuado del número y los tipos de contenidos disponibles para la distribución.

Además de los contenidos Web tradicionales, otros contenidos multimedia "enriquecidos" como por ejemplo la emisión de vídeo (tanto bajo demanda como en directo) proporcionan ahora servicios que son particularmente importantes para los usuarios (enseñanza a distancia, difusión a través de Internet, vídeo bajo demanda, etc.). Este escenario se va enriqueciendo continuamente debido a los nuevos tipos de contenidos que soportan típicamente las plataformas verticales proporcionadas por proveedores específicos y especializados: ejemplos de las mismas son las plataformas para juegos bajo demanda y para aplicaciones bajo demanda.

Los contenidos se proporcionan desde un centro de servicio proveedor de contenido (CP) a un sitio de usuario (US) donde se encuentra un solicitante de contenido (CR), a través de una red N (acceso + servicio metropolitano + transporte).

Como norma, para permitir que un servicio se encuentre disponible para la distribución, es necesario que los contenidos, el servidor de contenido CP y el solicitante de contenido CR cumplan condiciones específicas en términos de compatibilidad. En la práctica los componentes situados en las localizaciones de extremo (esto es el servidor CP y el solicitante CR) deben utilizar aplicaciones de programa que se corresponden/son compatibles con una tecnología común.

Por dicha razón, incluso si se hace referencia solamente a contenidos de flujo de datos, existen diferentes tipos de tecnología como las que se describen en "Windows Media 9 Series Deployment Guide", Microsoft, diciembre de 2002, páginas 47-51, o en "Helix Universal Server Administration Guide, Version 9.0", Real Networks, 19 de mayo de 2003, páginas 247-299.

Cada una de dichas tecnologías se caracteriza por prestaciones específicas en términos de plataformas disponibles (por ejemplo terminal móvil, ordenador personal, agenda electrónica, módulo de sobremesa), el programa disponible con el servidor y los mecanismos de autorización correspondientes.

Dicha aproximación se ha definido como "vertical" por el hecho de que mientras que un usuario final puede tener instalado en su sistema un programa nativo adaptado para "leer" por lo menos una tecnología de contenidos, la tarea más importante se localiza en el centro de servicio CP. De hecho, el centro de servicio debe estar equipado con servidores de distribución así como con procedimientos de autorización y sistemas dedicados específicamente a cada tecnología que debe soportar el centro.

En la figura 1 se muestra una disposición típica que se define como "centralizada". Dicha disposición comprende esencialmente dos bloques funcionales que se encuentran situados físicamente en puntos diferentes:

- por un lado, el solicitante de contenido CR comprende un terminal de usuario y un programa relacionado cargado en el mismo, encontrándose ambos componentes en el lugar del usuario (comprenden posiblemente un teléfono móvil), y

- por otro lado, el centro de servicio CP comprende baterías de servidores 10, 12 dispuesto cada uno para proporcionar un conjunto dado de servicios respecto a una tecnología dada, dependiendo del número de solicitudes simultáneas que se deben gestionar. Cada batería 10, 12 tiene asociado un servidor de autorización respectivo 10a, 12a, así como una base de datos de autorizaciones correspondiente 10b, 12b. Cada conjunto que comprende una batería de servidores, el servidor de autorización correspondiente y la base de datos asociada se define como una "granja de contenido".

Brevemente, en la disposición centralizada que se muestra en la figura 1 el centro de servicio CP deberá comprender, necesariamente, un número de diferentes granjas de contenido correspondientes al número de tecnologías diferentes que debe soportar el centro.

En referencia específicamente a las tecnologías de Microsoft y de Real Networks mencionadas anteriormente, una disposición como la que se representa en la figura 1 requiere procedimientos y mecanismos respectivos diferentes para la gestión de las autorizaciones para el acceso a los contenidos respectivos. Estos procedimientos y mecanismos no son compatibles directamente: por ejemplo, el acceso y/o la autorización pueden controlarse por medio de módulos insertados propietarios que realizan controles sobre el sistema de archivos que almacena los contenidos de las direcciones IP de los usuarios que acceden al sistema.

En otras tecnologías, la autorización se basa en la comprobación de una tabla externa, que puede comprender un simple fichero de texto, una base de datos en un formato propietario o una base de datos abierta de SQL (lenguaje de consulta estructurado).

Para resumir, una disposición como la que se muestra en la figura 1 no requiere solamente que las baterías o bancos de servidores 10, 12 se dediquen unívocamente a una única tecnología de contenidos: de hecho la misma separación no es aplicable también a los procedimientos y sistemas que realizan las tareas de autorización. Éstos requieren componentes de gestión y control especializados y dedicados a cada una de las tecnologías, siendo de hecho cada componente incompatible con componentes homólogos en las demás tecnologías que puedan encontrarse en el centro de servicio.

Esto significa entre otros que cuando se añade al centro una nueva tecnología de distribución de contenidos, no existe ninguna posibilidad práctica de aprovechar ningún equipo ya instalado y beneficiarse por tanto de ningún factor de escala.

Debido a la perspectiva cada vez más amplia de nuevos tipos de contenidos (juegos bajo demanda, aplicaciones bajo demanda, etc.) y a la posible oferta de nuevas soluciones verticales por parte de los proveedores tecnológicos, los componentes y procedimientos software/hardware de autorización corren el riesgo de convertirse en un problema real para los proveedores que gestionan centros de servicio.

Además de estas arquitecturas centralizadas basadas en el concepto de centro de servicio, recientemente se ha ido trazado una evolución hacia la disposición que se muestra en la figura 2. Se trata esencialmente de una disposición que se denomina red de distribución de contenidos (CDN).

En un contexto de CDN (como se describe, por ejemplo, en “Cisco ACNS 5.1 Caching And Streaming Configuration Guide, Release 5.1”, 2003, Cisco, páginas 227-270, parte de texto número OL-4070-01), servidores periféricos designados como servidores “alternativos” 14 toman el lugar de los servidores centralizados de la disposición de la figura 1. Los servidores alternativos se encuentran situados físicamente más cercanos a los usuarios (por lo que la red N que se muestra en la figura 2 comprende esencialmente la red de acceso y de servicio metropolitano y en general no comprende ya propiamente la red de transporte). De esta forma, los servidores alternativos 14 se encuentran en situación de distribuir los contenidos explotando un ancho de banda mayor.

En la disposición que se muestra en la figura 2, cualquier solicitud realizada por el solicitante de contenido CR se reencamina por medio de un sistema central (encaminador de contenido designado CDNCR) hacia un servidor 14 en el cual se encuentran disponibles los contenidos solicitados. Dicho servidor 14 se selecciona como el más adecuado en términos de recursos disponibles y de “distancia” a través de la red. Después de dicho procedimiento de reencaminado (encaminamiento de contenido), el procedimiento de acceder a los contenidos del servidor alternativo seleccionado es esencialmente análogo al procedimiento que tiene lugar en la disposición de la figura 1.

En una realización típica, la arquitectura CDN pertenece y es administrada por un operador de red que ofrece a diferentes proveedores de contenido la posibilidad de utilizar la infraestructura CDN para facilitar la distribución y entrega de los contenidos respectivos.

Una característica típica de los servidores alternativos 14 en una CDN es que no se dedican a una sola tecnología de contenido: se designan de hecho para dar servicio simultáneamente a solicitudes de diferentes tipos de contenidos (por ejemplo Real, Windows Media, etcétera). En consecuencia, se comportan esencialmente como servidores de tecnología múltiple debido a su capacidad de integrar los componentes de servicio de las diferentes tecnologías, permitiendo de esta forma que dichos componentes coexistan dentro de un mismo servidor alternativo 14.

La arquitectura de CDN que se muestra en la 2 no se encuentra exenta de un cierto grado de complejidad. Además de problemas de factor de escala relacionados con la gestión de los procedimientos de autorización para las diferentes tecnologías utilizadas (con la necesidad resultante de disponer de un módulo de autorización 14a específico para cada tecnología específica), aparece un problema adicional debido a la posibilidad de que los contenidos de cada servidor alternativo 14 estén relacionados con diferentes proveedores de contenidos, con diferentes reglas de autorizaciones/licencias.

Esto de hecho añade complejidad al procedimiento de autorización de acceso, haciendo prácticamente imposible gestionar de forma precisa y “granular” los criterios y procedimientos de autorización a los contenidos que hacen disponibles los diferentes proveedores de contenidos. Añadir nuevas tecnologías de contenido (como juegos bajo demanda o aplicaciones bajo demanda) a una arquitectura distribuida como se muestra en la figura 2 puede resultar todavía más complejo que en el caso de la disposición centralizada que se muestra en la figura 1.

De hecho, en las dos arquitecturas que se muestran en las figuras 1 y 2, el control del acceso a los contenidos se convierte en una cuestión crítica tanto para el operador de red como para el proveedor de contenidos, especialmente en lo que respecta a la tarificación por parte del operador. Esto se hace particularmente evidente si se considera el caso de un servicio que, basándose en una subscripción al servicio mismo, proporciona un acceso no diferenciado a los contenidos. Éste puede ser el caso típico de una subscripción a un servicio de ADSL residencial. Cuando se pasa desde dicho servicio a un acceso basado en pago anticipado donde la tarificación se diferencia en función de los contenidos específicos solicitados (como puede ser el caso para el acceso con pago previo a través de un teléfono móvil), la posibilidad de detectar en condiciones de tiempo real - es decir en el momento en el que se realiza la solicitud - posibles intentos de acceso fraudulento se convierte en una cuestión estratégica (si no vital).

El posible control en tiempo real no se encuentra de por si relacionado unívocamente con la intervención en tiempo real contra las aproximaciones fraudulentas. De hecho un operador puede decidir - bajo circunstancias específicas - tolerar un intento fraudulento durante una cierta cantidad de tiempo, mientras se reserva el derecho de tomar la acción más adecuada en vistas, por ejemplo, a aproximaciones de comercialización específicas.

A este respecto, la mayoría de las disposiciones de técnica anterior se basan en aproximaciones en las que se proporciona un dispositivo de control adaptado para actuar de forma transparente sobre el flujo de datos entre el usuario y el servidor que proporciona el servicio mientras realiza un control de acceso basándose en ciertas reglas internas.

Por ejemplo, en “Cisco Content Service Switch Basic Configuration Guide, Version 7.20”, marzo de 2003, Cisco, capítulos 3 y 5, parte de texto número 78-13886-05, se describe un conjunto de dispositivos, que se designan como CSS (conmutador de servicio de contenido), adaptado para operar sobre el flujo de datos entre un cliente y un servidor. Los dispositivos definen reglas estáticas que se aplican al tráfico cliente/servidor. Éstas se adaptan para aplicarse a grupos de clientes (de ciertas subredes o direcciones IP, servidores con ciertas direcciones IP o dominios DNS), tipos de contenidos (por ejemplo extensión de nombre de fichero o URL), basándose en listas definibles previamente configuradas en varios dispositivos. Sobre la base de dichas reglas (programadas desde el exterior), el dispositivo analiza el tráfico y decide la forma en la que se va a gestionar, esto es si cierto tráfico se transmitirá sin modificaciones, se filtrará para bloquear el tráfico o dirigirlo a destinos alternativos (este es el caso típico cuando el servicio es incapaz de acceder a ciertos contenidos).

Dichos dispositivos requieren necesariamente que las reglas de autorización se encuentren establecidas con anterioridad en los dispositivos mismos. Ésta resulta ser una solución crítica por lo menos por dos razones.

Una primera razón se relaciona con el número máximo de autorizaciones que se pueden configurar. Este número puede alcanzar fácilmente un valor muy alto, generalmente mayor que la capacidad del sistema mismo (25.000 reglas en conjunto), debiéndose tomar en consideración todas las combinaciones posibles de usuario/contenido. En una realización típica, se pueden definir 100 listas de acceso denominadas listas de control de acceso (ACL) adaptada cada una para incluir - como máximo - 254 “cláusulas”. Dentro de cada cláusula existe la posibilidad de definir un único usuario y un único contenido o grupos de usuarios y/o de contenidos. En la práctica, todos estos grupos son en si mismos estáticos y no ayudan de ninguna forma en la composición de las reglas.

Un segundo factor crítico consiste en el hecho de que configurar con anterioridad dichas reglas no permite el control dinámico de las autorizaciones. No es posible habilitar o inhabilitar a cierto usuario respecto a ciertos contenidos dependiendo de una condición que puede variar rápidamente y externamente al dispositivo mismo por ejemplo como resultado de la activación de una subscripción nueva, agotamiento del crédito, adquisición de crédito nuevo, campañas de promoción.

En WO-A-99/57866 se describe un sistema de redireccionamiento de datos para redirigir datos de usuario sobre la base de un conjunto almacenado de reglas. La aproximación correspondiente se basa en un representante (proxy) de aplicación. Esto es particularmente engorroso en términos de requerimientos de dispositivo, por el hecho de que requiere un módulo de aplicación de emulación para cada servicio/tecnología soportado por el sistema. Se requiere por tanto un módulo de programa dedicado, dependiente de la tecnología, para cada tecnología a tratar. Un problema adicional es que dicho módulo de programa específico puede no estar disponible para la integración en el sistema. Éste puede ser el caso cuando las tecnologías de distribución de contenido involucradas son tecnologías propietarias, una situación bastante corriente por ejemplo en juegos bajo demanda o aplicaciones bajo demanda.

Otra disposición alternativa se describe en un número de documentos asignados a Nomadix, Inc., como en US-B-6 130 892, US-B-6 636 894, WO-A-01/31886 o WO-A-02/35797.

La solución de Nomadix se puede aplicar a la red de acceso para filtrar los contenidos distribuidos por una arquitectura de distribución de contenidos por medio de satisfacer tres requerimientos básicos:

- analizar el paquete solicitado desde el solicitante de contenido, sin requerir módulos de programa adicionales dedicados al protocolo o a la tecnología de distribución de contenido,

- transmitir y recibir la solicitud de autorización enviada hacia un servidor externo, y

- hacer actuar la autorización por medio de la posibilidad de negar o redirigir la solicitud original del usuario (lo cual sin embargo requiere módulos de programa específicos para el redireccionamiento de la aplicación).

Además del problema de escalabilidad de la aplicación, relacionado con el redireccionamiento, el dispositivo Nomadix presenta un número de puntos críticos respecto a la utilización de servicios de distribución de contenidos en los contextos que se han considerado.

Como primer punto, el dispositivo Nomadix se encuentra situado en la red de acceso del operador de telecomunicaciones. Esto resulta ser un impedimento de la implementación grave para el operador. Esto es particularmente cierto en el caso de una red fija, por el hecho de que requiere un gran número de dispositivos en comparación con otras disposiciones en las que la localización es más cercana a la fuente de distribución (esto es junto al sitio de contenido de la CDN o al centro de servicio en una arquitectura centralizada).

En segundo lugar, el dispositivo Nomadix controla y bloquea la solicitud que procede del cliente. Como resultado, el tiempo involucrado en el proceso de recibir la solicitud del cliente, obtener autorización en un sistema centralizado, proporcionar una respuesta subsiguiente y de hecho transmitir la solicitud puede ser tan largo que dé lugar a una expiración de la aplicación, en el sitio del solicitante de contenido o en el servidor de contenido. Dicha disposición no se encuentra adaptada para su utilización en un contexto móvil en el cual el cumplimiento de requerimientos de tiempo real es vital para asegurar la seguridad contra comportamientos fraudulentos mientras que, por otro lado, las latencias de transmisión no pueden ser inferiores.

Finalmente en lo que respecta a la contabilidad de soporte de servicio del dispositivo Nomadix, éste realiza un registro de contabilidad basándose exclusivamente en las solicitudes de contenido. En el caso de una anormalidad en la respuesta del servidor de distribución, ésta puede dar como resultado una señalización falsa (y tarificación incorrecta) puesto que no existe la posibilidad de proporcionar una contabilidad del tiempo en el que los contenidos se distribuyeron efectivamente puesto que no se detecta la finalización de la entrega.

Objeto y resumen de la presente invención

Existe por tanto la necesidad de crear disposiciones adaptadas para superar las limitaciones de la disposición de la técnica anterior considerada anteriormente por medio de añadir por ejemplo otras funciones adaptadas para contabilizar, mientras se proporciona un mecanismo de autorización (y contabilidad) en tiempo real adaptado para controlar el acceso a los contenidos. Específicamente, existe la necesidad de crear disposiciones en las que criterios de control dinámicos independientes de la tecnología permitan un alto grado de libertad al seleccionar la "granularidad" de la acción de control. Esto permitirá referirse libremente en ese respecto a parámetros como la agrupación lógica de contenidos por subred/URL/usuario en una combinación seleccionada libremente por medio de actuar indiferentemente tanto sobre el flujo de solicitud como sobre el flujo de respuesta (contenidos que se distribuyen) proporcionando en paralelo un soporte más global para propósitos de contabilidad.

El objeto de la presente invención es proporcionar una disposición que satisface estas necesidades.

Según la presente invención este objetivo se alcanza por medio de un procedimiento que presenta las características que se establecen en las reivindicaciones siguientes. La presente invención se refiere también a un sistema correspondiente, a una red relacionada y a un producto programa de ordenador que se puede cargar en la memoria de por lo menos un ordenador y que comprende partes de código de programa para la realización de las etapas del procedimiento de la presente invención cuando se ejecuta en un ordenador. Como aquí se utiliza, la referencia a un producto programa de ordenador de este tipo es equivalente a la referencia a un medio legible por un ordenador que contiene instrucciones para controlar un sistema de ordenador para coordinar la realización del procedimiento de la presente invención. La referencia a "por lo menos un ordenador" se refiere evidentemente a poner de manifiesto la posibilidad de que la presente invención se implemente de forma distribuida/modular.

Una realización preferida de la presente invención es por tanto un sistema para la gestión de transacciones en una red de comunicación, en el cual las transacciones comprenden por lo menos una solicitud de un contenido dado dependiente de la tecnología realizada por un solicitante a por lo menos un servidor. El sistema funciona basándose en una lista de acceso a contenido que comprende cláusulas de permiso/denegación de servicio que regulan el acceso de los solicitantes a los contenidos proporcionados por el servidor. Se proporciona un módulo de procesado configurado para detectar la solicitud dependiente de la tecnología, y extraer a partir de la misma información que identifica al solicitante que realiza la solicitud y el contenido solicitado. De esta forma se puede generar una entrada de acceso a contenido independiente de la tecnología adaptada para comprobarse con la lista de acceso a contenido para derivar información de permiso/denegación referida a la solicitud detectada. La solicitud se gestiona como función de la información de permiso/denegación derivada y por tanto por ejemplo i) se transmite al servidor, o ii) se descarta o se dirige a un destino alternativo. El acceso a los diferentes contenidos distribuidos se controla por tanto de forma independiente de las tecnologías específicas que se utilizan para la distribución de los contenidos de medios.

La disposición que aquí se describe se encuentra por tanto adaptada para realizar una acción de control respecto a cualquiera de los siguientes parámetros:

- el tipo de contenidos (imagen, fichero, flujo de vídeo, páginas Web),

- el tipo de protocolo utilizado para la distribución de contenidos al usuario (http, https, http progresivo, mms, rtsp, ftp, etc.),

- la arquitectura de distribución (servidor centralizado, servidores alternativos o CDN),

- el tipo de cliente que solicita la entrega de contenidos (ordenador personal, módulo de sobremesa, teléfono móvil, etc.),

- el tipo de conectividad IP (inalámbrica, GPRS, Ethernet, etc.).

Una realización que se prefiere particularmente de la presente invención proporciona la presencia de un componente de control centralizado (que funciona como servidor de contenido y de reglas de seguridad) adaptado para verificar en condiciones de tiempo real las autorizaciones de usuario/contenidos para gestionar de forma unitaria las autorizaciones para todas las tecnologías y tipos de contenido (actuales y futuros). Éste opera primariamente sobre el identificador de usuario y sobre la referencia al contenido solicitado, unificando de esta forma el procedimiento de autorización.

Además, se proporciona preferiblemente por lo menos un dispositivo de red que funciona como una pasarela de acceso condicional a contenido (DCCA). Dicha pasarela se puede adaptar para realizar, para todas las tecnologías de contenido (actuales y futuras) las siguientes funciones:

- análisis transparente de tráfico, por medio de reforzar una lógica de control bilateral para la solicitud, actuando sobre las solicitudes mismas o actuando sobre el tráfico de retorno hacia el usuario, mientras también se tiene en consideración - a todos los niveles (enlace de datos, red, transporte y aplicación) - la información derivada de las mismas. Este análisis se define como “transparente” puesto que se realiza sin modificar la arquitectura IP, y es capaz de actuar en una disposición de conmutador/puente (nivel 2 de la pila OSI);

- recibir y transmitir solicitudes de autorización hacia el componente de control central, sobre la base de un formato unitario para todos los tipos de componentes, por medio de identificar el contenido solicitado y el usuario de una forma totalmente independiente de las características específicas de las tecnologías adaptadas para distribuir contenidos (tipo de contenidos, protocolo, cliente, servidor, arquitectura, conectividad);

- reforzar la autorización del flujo con una aproximación bilateral por medio de detener el flujo de la solicitud sin retransmitirla al servidor de contenido (por ejemplo en un control de línea que actúa sobre la solicitud) o por medio de bloquear el flujo de retorno hacia el solicitante de contenido (por ejemplo control retardado activo en la respuesta), mientras se controla el flujo mismo para soportar la función de contabilidad;

- posiblemente redirigir la solicitud, mientras se realiza el control sobre la solicitud, basándose en los mismos criterios transparentes considerados para los propósitos de análisis, modificando por tanto la referencia a los contenidos solicitados contenida en la carga útil de los paquetes mientras se mantiene activa la sesión de comunicación establecida con el servidor de contenido, sin la intervención de ningún módulo de programa dedicado específicamente a una tecnología dada.

Una realización preferida de la disposición que aquí se describe proporciona que el dispositivo de red en cuestión se disponga en la conexión hacia la batería o banco de servidores de contenido del centro de servicio, por encontrarse situado junto a la misma o encontrándose dispuesto en la conexión hacia los servidores alternativos en cada sitio en una arquitectura CDN situándose en el sitio mismo. De esta forma la disposición resultante es significativamente más eficiente en comparación con aquellas disposiciones basadas en la situación en un punto de acceso a la red misma: esta última disposición puede sin embargo implementarse todavía si apareciese la necesidad.

Para resumir, la disposición que se describe aquí cumple todas las necesidades posibles de control dinámico de acceso a contenido que se han listado anteriormente.

Específicamente, la disposición que se describe aquí proporciona una solución que es:

- totalmente transparente respecto a la arquitectura de distribución de contenidos, al cliente y al contenido así como a la arquitectura IP utilizada, debido entre otros a la posibilidad de funcionar como una disposición de conmutador/puente;

- escalable, por el hecho de que la parte dedicada a procesar la autorización (de forma centralizada) es distinta de la parte que se dedica a la acción de activación/filtrado;

- de naturaleza altamente granular puesto que permite una definición de los permisos de acceso a los contenidos basándose en cualquier elemento de información adaptado para derivarse a nivel de enlace de datos, red, transporte y aplicación;

- altamente configurable, puesto que permite la gestión en tiempo real de autorizaciones de acceso tanto sobre la base de la solicitud de contenido como actuando de forma retardada sobre el flujo de retorno, siendo compatible por tanto con servicios basados en contenidos de nuevos tipos que solicitan tarificación en tiempo real, como aquellos basados en pago previo, mientras es compatible con latencias de conectividad no despreciables; e

- independiente del proveedor, por el hecho de que puede soportar fácilmente nuevos protocolos y tecnologías de contenido sin requerir módulos de programa adicionales, mientras se encuentra en situación de interceptar cualquier protocolo de solicitud (y el flujo de retorno relacionado) así como de gestionar de forma unitaria las solicitudes de autorización y los eventos de contabilidad hacia un servidor centralizado.

Breve descripción de las figuras

A continuación se describirá la presente invención, a modo de ejemplo solamente, con referencia a las figuras adjuntas, en las cuales:

- las figuras 1 y 2 se han descrito anteriormente de forma breve,

- la figura 3 es un diagrama de bloques que representa, por medio de la utilización de esencialmente el mismo esquema de las figuras 1 y 2, la estructura básica de la disposición que aquí se describe,

- las figuras 4 a 6 representan de forma esquemática la aplicación del esquema básico que se muestra en la figura 3 a diferentes contextos de funcionamiento,

- la figura 7 es un diagrama de flujo de alguna lógica básica de control adaptada para implementarse en la disposición que aquí se describe,

- la figura 8 es un diagrama de bloques que representa el flujo de datos correspondientes al diagrama de flujo de la figura 7,

- la figura 9 es otro diagrama de flujo que representa una lógica de control alternativa adaptada para implementarse en la disposición que aquí se describe,

- la figura 10 es un diagrama de bloques que representa el flujo de datos correspondiente al diagrama de flujo de la figura 9,

- las figuras 11 y 12 son diagramas de bloques lógicos representativos del control de permisos como se implementa en el marco de la disposición que aquí se describe,

- las figuras 13 a 17 son diferentes diagramas de bloques que representan el funcionamiento de varios módulos involucrados en diferentes fases de funcionamiento de la disposición que aquí se describe,

- la figura 18 representa una estructura de acceso a contenidos adaptada para gestionar una solicitud de contenido y el posible redireccionamiento de la misma en la disposición que aquí se describe, y

- las figuras 19 y 20 son ejemplos de realizaciones prácticas posibles de la disposición que aquí se describe.

Descripción detallada de realizaciones preferidas de la presente invención

La figura 3 de las figuras adjuntas muestra una localización posible de los componentes de un sistema como aquí se describe respecto a otros objetos y elementos implicados en el funcionamiento del mismo. En términos generales, las partes, los componentes o los elementos idénticos, similares o equivalentes a partes, componentes y elementos homólogos ya descritos en relación con las figuras 1 y 2 se designan por medio de las mismas letras y/o números de referencia.

Específicamente, la disposición de la figura 3 comprende una pasarela 20 (que se define de aquí en adelante como pasarela de acceso condicional dinámico a contenido o DCCA) que se dispone sobre la ruta de conexión entre el solicitante de contenido CR y el sitio de usuario US y una disposición de servidor de contenido 26 (adaptada para configurarse según diferentes disposiciones, como se detallará mejor más adelante) situado en el sitio de distribución de contenido 24.

La pasarela 20 se configura para realizar un número de funciones como activación, permiso, filtrado, tratamiento y reinyección sobre el tráfico que la atraviesa. La pasarela 20 se configura para cooperar con un servidor 22 que juega el papel de servidor de reglas y seguridad de contenidos. Éste se sitúa en el nivel de control de la red, por ejemplo en un centro de servicio del operador de telecomunicaciones que gestiona la red. El servidor 22 tiene la tarea principal de validar las solicitudes entrantes y posiblemente activar mecanismos de contabilidad específicos.

Los bloques que representan al solicitante de contenidos CR y al sistema servidor de contenidos 26 se representan por medio de líneas de puntos puesto que representan elementos preexistentes de la arquitectura.

Las figuras 4 a 6 muestran cómo los elementos básicos representados en la figura 3 se pueden disponer de formas distintas con varias arquitecturas adaptadas para distribuir contenidos de medios.

Específicamente, la disposición que se muestra en la figura 4 se refiere a una arquitectura centralizada en la que la pasarela DCCA 20 se dispone "delante" de las baterías/bancos de servidores de contenidos 10, 12 ya tratados en relación con la figura 1.

La pasarela 20 y el servidor de reglas y seguridad de contenidos 22 son dos componentes situados en el centro de servicio proveedor de contenidos 24, es decir el centro de servicio para la distribución de contenidos. En este caso, el elemento de conectividad representado por la red N comprende normalmente la red de acceso, (a la cual se encuentran conectados el solicitante de contenido CR y el proveedor de contenido 24), la red metropolitana, y la red de transporte en el caso de conexiones de larga distancia.

La figura 5 por el contrario se refiere a una arquitectura de distribución basada en CDN. En este caso la pasarela 20 se dispone delante de los servidores alternativos 14 dispuestos en cada sitio de la red de distribución de contenido (por ejemplo en los puntos de presencia metropolitana). Por el contrario, el servidor de reglas y seguridad de contenidos 22 se dispone en el centro de servicio del operador de la red de distribución de contenido, posiblemente junto a los demás componentes de control de dicha red, como el encaminador de contenido de CDN 23.

En dicho caso, el punto de localización óptimo para la pasarela 20 es, como se ha indicado, delante del servidor alternativo (o la batería/banco de servidores alternativos) que entregan los contenidos. Son posibles otras localizaciones, pero es posible que puedan convertir al sistema de control en más vulnerable a intentos por parte de usuarios de operar fraudulentamente por medio de rodear la pasarela de control.

La figura 6 se refiere a una arquitectura "genérica" que comprende servidores 28 dispuestos en diferentes localizaciones de la red y que descienden hasta dueños diferentes. En este caso, la pasarela 20 tiene la función de filtrar y controlar todo el tráfico en la fuente, concretamente en la proximidad del punto de acceso a la red que utiliza el solicitante de contenido CR.

La disposición que aquí se describe no se encuentra en modo alguno limitada a la utilización posible de una arquitectura habilitada por CDN o una arquitectura que utiliza un centro de servicio. De hecho, esta disposición se encuentra adaptada para funcionar en conexión con arquitecturas "mixtas", donde aparece la necesidad de autorización/habilitación de un usuario para recibir un servicio proporcionado por uno o más servidores mientras se proporciona el soporte necesario para la contabilidad.

La siguiente descripción de una realización preferida de la disposición que aquí se describe se referirá principalmente a una posible implementación en un escenario de CDN, es decir a un contexto genérico de arquitectura CDN. A este respecto, en referencia a la figura 5, el concepto de servidor alternativo debe entenderse en su significado más general de un "conjunto de" servidores que proporcionan un servicio de contenidos, mientras que el encaminador de contenido 23 se puede substituir por otros sistemas, por ejemplo un DNS (servidor de nombres de dominio) o encontrarse ausente.

De hecho, los elementos básicos de las disposiciones que aquí se describen, en concreto la pasarela 20 (que realiza las acciones de activación, filtrado y redireccionado) y el servidor de reglas y seguridad de contenidos 22 (que comprueba los derechos de acceso a los contenidos en condiciones de tiempo real después de la solicitud por parte de la pasarela 20 y proporciona el resultado a la misma pasarela 20) son independientes del tipo de arquitectura y - lo que es más importante - de la tecnología utilizada en la cadena de solicitante de contenido CR/servidor de contenido 24. Esto significa que cualquier acceso al servidor alternativo 14 puede ser interceptado por la pasarela 20 y procesado por medio de la ejecución de las funciones consideradas anteriormente.

Los mecanismos de activación y filtrado implementados por la pasarela 20 se pueden configurar basándose en una descripción y alcanzar un nivel de granularidad a nivel de un nombre de dominio o un contenido único. Este mecanismo se implementa por medio de listas de acceso de contenido (ACL) designadas por descriptores de lista que se describirán en detalle a continuación con referencia a la figura 18.

Un filtro ACL controla por medio de cláusulas de permiso/denegación los siguientes elementos: direcciones IP de origen y destino + máscara de subred + identificación VPN, tipo de protocolo de transporte (TCP/UDP), puerto de comunicación (origen/destino) y referencia al contenido solicitado.

Los filtros ACL se mantienen al nivel de la pasarela 20, que funciona basándose en la interceptación de la solicitud de usuario y se activan (en un modo permitir/denegar) como resultado de la validación de la habilitación realizada por el servidor 22. Esto se basa en transmitir los atributos del identificador de usuario (por ejemplo la dirección IP), el contenido del servicio (por ejemplo el URL) y, posiblemente, los atributos correspondientes del servidor alternativo 14 que proporciona el servicio.

La pasarela 20 de la figura 5 intercepta el tráfico de usuario (solicitud de contenidos multimedia, los cuales - como regla - son "dependientes de la tecnología"), de forma transparente, esto es sin afectarlo o modificarlo. La pasarela extrae de cada solicitud dependiente de la tecnología los contenidos para los cuales se ha configurado la gestión, es

decir la dirección IP del CR del solicitante, el URL asociado con el contenido solicitado, la dirección IP del servidor alternativo, y las características del protocolo utilizado.

Estos datos se utilizan para crear (como se detalla mejor a continuación en referencia a la figura 18) una entrada de contenido de acceso (ACL) "independiente de la tecnología", para la cual se solicita validación accediendo al servidor 22. El servidor 22 comprueba las credenciales del usuario respecto a la solicitud realizada y deriva una información correspondiente de permiso/denegación.

Cuando el usuario se encuentra habilitado ("permitido"), el flujo de datos desde el usuario hasta el servidor alternativo y desde el servidor alternativo hasta el usuario permanece inalterado.

Si el usuario no se encuentra habilitado ("denegación") para recibir el contenido solicitado, pueden producirse por lo menos dos intervenciones diferentes.

Como primera opción, se puede bloquear la solicitud de cliente, es decir la solicitud no se retransmite al servidor alternativo 14 que proporciona el servicio.

Como opción alternativa, se puede bloquear el flujo de descenso (desde el servidor alternativo hasta el cliente).

Específicamente, en referencia al diagrama de flujo de la figura 7, la referencia 100 indica una etapa en la que la pasarela 20 extrae del tráfico enviado por el solicitante de contenido CR hacia el servidor 14 (tráfico que se indica como 1 en la figura 8) la dirección IP (ES) y los URL. estos datos extraídos se someten en la etapa 102 a una comprobación de la aptitud del usuario.

El resultado de dicha comprobación se espera en la etapa 104 y en la etapa 106 se realiza una prueba final. Si la prueba da un resultado positivo (usuario habilitado - "permitir") la solicitud respectiva se transmite al servidor alternativo 14 en una etapa 108.

En el caso en el que la comprobación de la etapa 106 entregue un resultado negativo (usuario no habilitado - "denegación"), la solicitud se descarta/redirige en una etapa 110.

Más concretamente, los números de referencia 1 a 6 de la figura 8 identifican la secuencia de tiempo de los diferentes flujos de tráfico. Específicamente, dicha secuencia presenta las siguientes etapas:

- la solicitud desde el solicitante de contenido CR se transmite a la pasarela 20 (flujo 1),

- la pasarela 20 intercepta la solicitud (mientras que el resto del tráfico la atraviesa sin alteración) y dispone la solicitud en una condición de espera sin transmitirla al servidor alternativo 14. Mientras tanto, la pasarela 20 prepara una solicitud para el servidor 22 que comprende las referencias del solicitante (dirección IP) y el contenido solicitado, que a continuación se transmite al servidor 22 (flujo 2),

- el servidor 22 realiza la comprobación de la aptitud del usuario respecto a los contenidos solicitados y responde a la pasarela 20 por medio de un mensaje de permitido/denegado (flujo 3),

- si el resultado es positivo, la pasarela 20 retransmite la solicitud original al servidor alternativo 14 (flujo 4); en caso contrario puede descartar la solicitud o retransmitirla de forma modificada (dentro del marco de la misma sesión TCP). Además, puede establecer una ACL interna para optimizar solicitudes posteriores;

- el servidor alternativo responde a la solicitud recibida (flujo 5), y

- el flujo de respuesta atraviesa la pasarela 20 hacia el solicitante de contenido (flujo 6). Esta forma de funcionamiento permite el redireccionamiento en línea de los contenidos.

Las figuras 9 y 10 describen la aproximación alternativa que ya se ha considerado anteriormente.

En este caso, después de extraer (en la etapa 100) la información referente a la aptitud del usuario y pasarla al servidor 22 para su verificación (en una etapa 102), la disposición alternativa que se considera en las figuras 9 y 10 hace que se envíe la solicitud de usuario (en una etapa 112) como un paquete de usuario al servidor 14 sin alterarse en ningún modo. De esta forma, el servidor 14 puede empezar a proporcionar al usuario el servicio solicitado. Esto ocurre en la etapa 114 que continúa (por lo menos) mientras se recibe desde el servidor 22 el resultado de la comprobación realizada en la etapa 102.

En este punto se comprueba la aptitud del usuario en una etapa 116.

Si la etapa 116 entrega un resultado positivo, el sistema evoluciona hasta la etapa 118 de "no hacer nada", dejando de esta forma que el servidor 14 continúe la etapa 114 entregando así el contenido al CR solicitante.

Si, por el contrario, la comprobación de la etapa 116 entrega un resultado negativo, se transmite una señal de bloque al servidor 114 interrumpiendo de esta forma la entrega del servicio al CR solicitante.

De nuevo, en el diagrama de la figura 10, los diferentes flujos de información se indican por medio de números de referencia que identifican su secuencia temporal.

Específicamente, en la disposición de la figura 10:

- la solicitud de usuario se transmite a la pasarela 20 (flujo 1),

- la pasarela 20 intercepta la solicitud (mientras que el resto del tráfico la atraviesa de forma inalterada) y dispone la solicitud en una condición de espera sin transmitirla al servidor alternativo 14. Mientras, la pasarela prepara una solicitud para el servidor 22 que comprende las referencias del solicitante (dirección IP) y del contenido solicitado, que a continuación se transmite al servidor 22 (flujo 2),

- al mismo tiempo la solicitud se transmite (inalterada) al destino final, que es el servidor 14 (flujo 3),

- el servidor 14 empieza a satisfacer la solicitud, enviando de vuelta tráfico de respuesta (flujo 4),

- el tráfico de respuesta pasa de forma inalterada desde la pasarela 20 hacia el CR solicitante de contenido (flujo 5),

- después de comprobar la habilitación del usuario respecto a los contenidos solicitados, el servidor 22 responde a la pasarela 20 por medio de un mensaje de permitido/denegado (flujo 6).

En el caso de permiso, la pasarela 20 no realiza ningún tipo de operación; por el contrario, en el caso de denegación, inserta un filtro que bloquea el flujo de respuesta desde el servidor alternativo 14 al CR solicitante de contenido (cortando de esta forma los flujos 4 y 5).

La ventaja de esta disposición alternativa consiste en que permite controlar la habilitación del usuario también en aquellas situaciones en las que la latencia de transmisión y la posible expiración de la aplicación son críticas. Éste puede ser típicamente el caso en una red móvil.

La figura 11 es un diagrama de bloques de ejemplo de una posible estructura interna del servidor 22. En la realización de ejemplo que se muestra, el servidor 22 es esencialmente un sistema que accede a diferentes bases de datos para identificar, basándose en operaciones de relación de base de datos, las reglas a aplicar a un usuario dado respecto a un contenido dado.

Por supuesto es posible contemplar diferentes implementaciones de este tipo de servidor. Las realizaciones alternativas pueden basarse posiblemente en servidores del tipo de autenticación, autorización, contabilidad (AAA) como los que se conocen como sistemas RADIUS, TACACS, TACACS+, DIAMETER u otros sistemas como los servidores LDAP, adaptados para detectar el perfil de usuario y decidir si se puede autorizar o no cierta solicitud procedente de una pasarela.

En la realización de ejemplo que se muestra, el servidor 22 comprende tres bases de datos, en concreto:

- una base de datos de identidad de usuarios 30 que contiene la información referente a los usuarios (que se encuentran en línea o no),

- una base de datos de contenidos 32 que contiene la información referente a los contenidos disponibles y gestionados por el sistema (por ejemplo el URL respectivo, dominio alojado, proveedor de contenido, coste, duración, etcétera), y

- una base de datos de reglas de contenido 34 que contiene la información de habilitación del contenido para los usuarios individuales (o grupos de usuarios).

Como se muestra en la figura 11, un único servidor 22 puede cooperar con diferentes pasarelas 20, comprendidas en una CDN. Como se explicará a continuación, la pasarela 20 se configura para detectar la información relativa al solicitante (como la dirección IP), el contenido solicitado (como el URL respectivo) y posiblemente la dirección del servidor alternativo hacia el cual se dirigía la solicitud.

El número de referencia 36 designa en conjunto la lógica principal del servidor 22, que comprende entre otros un módulo de comprobación ACL 38 así como un controlador de pasarela 40.

Basándose en los objetos de información recibidos desde la o cada pasarela 20, se interroga al módulo de comprobación ACL 38 para determinar la “consistencia” del acceso al contenido respecto a la aptitud del usuario.

En consecuencia, el módulo de comprobación 38 realiza las siguientes tareas:

- identificar al usuario basándose en los atributos respectivos que se han pasado desde la pasarela 20 (por ejemplo utilizando la dirección IP para derivar a partir de una tabla el nombre de usuario del usuario habilitado, encontrándose dicha función actualmente disponible en un número de sistemas AAA); esto ocurre como resultado de acceder a la base de datos de identificación de usuario 30,

- identificar posibles macro-familias con las cuales se encuentra relacionado el contenido solicitado así como información adicional pertinente (por ejemplo la duración o el ancho de banda solicitado), por medio de acceder a la base de datos de contenido 32, y

- verificar las habilitaciones asociadas con el usuario respecto a las agregaciones de contenido relacionadas con el contenido solicitado, por medio de acceder a la base de datos de reglas de contenido 34.

El resultado de dicha operación, que puede ser de permiso o denegación, se transmite desde el control de pasarela 22 hasta la pasarela solicitante 20.

Por ejemplo, en dicho caso los árboles de las bases de datos asociados comprenden:

Base de datos 30 de identidad de usuario

Dirección IP	**NombreUsuario**	**Crédito**
10.10.10.10	Usuario1	10 Euros
10.10.10.11	Usuario2	1 Euro
10.10.10.12	Usuario3	1 Euro

Base de datos 32 de contenido

Referencia a contenido	**Duración**	**Coste**	**Macrofamilias**
www.milan.it/ultimigoal.rm	120	1 •	deporte, fútbol
www.rai.it/montalbano1.rm	2500	2 •	ficción
www.formula1.it/monza.rm	500	1 •	deporte, automovilismo

Base de datos 34 de reglas de contenido

ClaveNombreUsuario	**Macrofamilia**
Usuario1	ficción
Usuario2	fútbol
Usuario3	deporte

Los siguientes pares solicitud/respuesta pueden producirse desde/hacia la pasarela solicitante 20

Solic(10.10.10.10,www.milan.it/ultimigoal.rm)=>Resp(Negación: contenido no permitido)

Solic(10.10.10.11,www.milan.it/ultimigoal.rm)=>Resp(Permitido, durante 120 segundos)

Solic(10.10.10.12,www.milan.it/ultimigoal.rm)=>Resp(Negación, por crédito insuficiente)

Solic(10.10.10.12,www.formula1.it/monza.rm)=>Resp(Permitido, durante 500 segundos)

En consecuencia, junto con la respuesta, el servidor 22 puede transmitir a la o cada pasarela 20 algunos elementos de información adicional derivados de las bases de datos consultadas. Estos pueden comprender por ejemplo la duración del contenido (que se convierte en el tiempo de vida de la ACL misma), el crédito residual, u otra información útil para controlar la entrega del servicio.

Como regla, será generalmente suficiente transmitir hacia la pasarela solicitante 20 solamente el mensaje de permiso/denegación asociado adecuadamente con la solicitud original.

De forma similar, la etapa en la que se comprueban las agregaciones del contenido en macrofamilias se puede realizar si la base de datos de reglas de contenidos 34 aloja reglas a nivel de contenido individual (URL) y no a nivel de macrofamilias. De esta forma, se puede lograr un nivel máximo de granularidad en el control del acceso a los contenidos.

Se apreciará que, preferiblemente, la función de gestión de las ACL activas y el almacenamiento de las mismas no los proporciona el servidor 22 sino la pasarela respectiva 20, por medio de implementar simplemente dos órdenes:

- ObtenerACL por parte de la pasarela 20, y

- EstablecerACL por parte de un servidor 22.

En otras realizaciones, puede ser útil implementar un servidor 22 adaptado para almacenar ACL creadas de forma centralizada para permitir un reinicio subsiguiente en el caso de eventos de fallo por parte de la pasarela 20. Preferiblemente, en dicho tipo de arquitectura, se proporciona una orden adicional del tipo:

- RealinearACL por parte tanto de la pasarela 20 como del servidor 22, que se encarga de transmitir desde la pasarela 20 y hacia el servidor 22 las ACL disponibles localmente (por ejemplo para asegurar el reinicio después de un fallo en dicho componente), o viceversa (desde el servidor 22 hacia cada pasarela 20, selectivamente).

- DescartarACL desde la pasarela 20 hacia el servidor 22 después de la expiración del tiempo de vida de la ACL misma.

La figura 12 destaca la estructura interna de la pasarela 20, mientras que las figuras siguientes 13 a 17 detallan el funcionamiento de la misma.

En la realización de ejemplo que se muestra, la pasarela 20 se implementa como un componente separado. Sin embargo, teniendo en cuenta lo que se ha descrito anteriormente, y en vistas al resto de la presente descripción, se hará evidente que las funciones realizadas por la misma, en concreto la activación, filtrado, reglas y redireccionamiento (tratamiento + reinyección) de paquetes se pueden implementar en forma de módulos agregados asociados con otros dispositivos de red como un conmutador de red, un conmutador de contenido, un dispositivo de encaminamiento o directamente con uno o más servidores alternativos.

El sistema se dispone sobre una pluralidad de capas, dos de las cuales (la inferior y la superior) comprenden esencialmente interficies de red 50 y 52 que cooperan con el solicitante de contenido CR y el servidor alternativo, respectivamente, más una interficie adicional 54 hacia el servidor 22.

Las capas intermedias comprenden esencialmente una capa inferior 56 a nivel de núcleo y un nivel más alto 58 a nivel de contenidos de aplicación.

En la capa de núcleo 56 la función básica de un núcleo tipo Unix se dispone para tratar redes, puentes y filtros a nivel IP (hasta el nivel 4).

Una implementación típica de la capa 56 comprende todas las funciones típicas situadas actualmente en la disposición FreeBSD como se encuentra en el IPFW (cortafuegos IP) de una disposición FreeBSD.

Específicamente, se incluyen los siguientes elementos:

- un módulo de filtro IP 60 con un sub-módulo asociado 60a de control correspondiente al que se confía la tarea de filtrado (hasta el nivel 4) de los paquetes IP. Este módulo funciona con paquetes puenteados entre dos interficies de red destacados por el nivel inferior, y un sub-módulo de desviación 62 y un sub-módulo de reinyección 64. El módulo 62 tiene la tarea de redirigir paquetes de Ethernet (tramas) hacia una aplicación de sistema a nivel de usuario para su procesado. El módulo 64 tiene la tarea de reinyectarlos, siempre por medio de una aplicación de sistema a nivel de usuario, con nuevo el cálculo del código de corrección cilíndrica (CRC) para el envío correcto hacia la red. Estos módulos 62 y 64, que actualmente no se encuentran disponibles para interficies puenteadas, se pueden activar también para el tráfico puenteado modificando de forma correspondiente el núcleo básico de FreeBSD.

Las referencias 66 y 68 designan dos bases de datos que alojan reglas estáticas de IP y reglas dinámicas de IP, respectivamente.

Utilizar FreeBSD como base para dicho sistema operativo de la pasarela 20 presenta un número de ventajas.

En primer lugar, permite realizar cortafuegos IP transparentes por medio de puenteado. Además, realiza las acciones de filtrado y activación a nivel de núcleo con un rendimiento mejorado. Existe la posibilidad de implementar mecanismos selectivos de desviación relacionados con las reglas de cortafuegos para transmitir paquetes específicos hacia una o más tomas de núcleo conectadas a una aplicación de espacio de usuario.

Además, existe la posibilidad en FreeBSD de realizar un mecanismo de reinyección de paquetes por medio de las tomas de núcleo consideradas anteriormente. Esto permite que una aplicación de espacio de usuario trate exclusivamente aquellos paquetes identificados específicamente por las reglas de cortafuegos por medio de aceptar, modificar, rechazar o tratar de forma retardada el flujo de retorno.

Además, FreeBSD es un programa disponible gratuitamente, por lo que la parte de cortafuegos sigue los desarrollos actuales en la programación de código fuente abierto, mientras que se preserva la parte de nivel de aplicación. Fácilmente se pueden realizar los cambios posibles que se requieren en la red a nivel de núcleo para hacer que las funciones de desviación/reinyección estén disponibles también para los paquetes puenteados.

Finalmente, las implementaciones TCP de la BSD se consideran actualmente como la pila TCP más robusta que existe en un contexto Unix.

El módulo lógico principal 58 comprende un número de sub-módulos de aplicación. Estos comprenden un módulo de análisis 70 que realiza el análisis (nivel 7) de los paquetes recibidos desde el módulo de desviación del núcleo 62 por medio de extraer la dirección IP y el URL (o, más generalmente, las referencias útiles para la autorización), mientras se instancia también la solicitud de autorización enviada al servidor 22 (a través de la interficie 54) y se gestiona la respuesta correspondiente por medio de reforzar las reglas de filtrado por medio de órdenes enviadas al sub-módulo de control del núcleo 60a. Esto comporta esencialmente la presencia de un sub-módulo de control de reglas 72 y un sub-módulo solicitante de reglas 76. La posible manipulación del paquete de solicitud y el control del sub-módulo de reinyección del núcleo 64 se realizan por medio de un sub-módulo de tratamiento de paquetes 74. Específicamente, el sub-módulo de control de reglas 72 realiza la acción de temporización para las ACL y la posible eliminación de las mismas después de la expiración del tiempo de abandono establecido por el servidor 22.

La capa lógica principal 58 de la pasarela 20 coopera además con dos depósitos de información 78 y 80.

El depósito anterior, que se designa como 78, comprende esencialmente los ajustes de configuración de la pasarela 20. Estos se refieren esencialmente a:

- reglas estáticas para activar las solicitudes y determinar los protocolos, los puertos y los atributos característicos de los paquetes sobre los cuales se investiga la información de contenido (igual como se utilizan por parte del filtro IP 60 para el filtrado de nivel 4);

- reglas de separación en el marco de Ethernet para localizar la información de IP y URL que van a utilizar los sub-módulos 70 para propósitos de análisis; y

- reglas de redireccionamiento posible basadas en protocolo, dominio o tipo de denegación (por ejemplo crédito insuficiente, habilitación no disponible, etcétera) para su utilización posible por parte del sub-módulo de tratamiento 74 para substituir el URL o la solicitud original procedente del usuario por un destino alternativo. Se apreciará que un destino alternativo de este tipo se transmite al servidor alternativo dentro de la misma sesión TCP. Por otro lado, esto asegura su existencia en el servidor mientras que por otro lado se mejora la eficiencia del sistema mismo.

El depósito 80 comprende esencialmente las listas de acceso de contenido local (ACL), que describen en el nivel 7 el filtrado activo en cierto momento y realizan un mapeado con las reglas correspondientes a nivel 4 de los módulos de filtrado IP 60 almacenadas en la base de datos 68 de reglas dinámicas de IP.

La fase de configuración de la pasarela 20 se detalla mejor en la figura 13 en la cual se destacan mediante líneas de puntos los módulos/sub-módulos implicados directamente.

Esencialmente, la parte principal de la fase de configuración tiene lugar en la pasarela 20 antes de utilizar el sistema. De hecho, la configuración del servidor 22 se limita a indicar las referencias para la conexión a la(s) pasarela(s) y bases de datos utilizadas. Se asumirá de forma general que éstas se encuentran ya cargadas anteriormente con la información necesaria como se ha indicado anteriormente.

Esencialmente, la fase de configuración de la pasarela 20 comprende un número de etapas de establecimiento de la configuración.

Una primera etapa de configuración comprende establecer la dirección del servidor 22 y los puertos correspondientes para la información para solicitar autorización (por lo menos una dirección IP de usuario y URL) y recibir las respuestas correspondientes (como denegación/permiso o agotamiento de tiempo). Este proceso es esencialmente simétrico respecto a la configuración realizada sobre el servidor 22. Lo siguiente es un ejemplo de esto:

CP&SSERVER = 10.10.15.156

ServerCommPort = 22222

NetworkCommPort = 33333

En una etapa subsiguiente de establecimiento de la configuración, se incluye la definición de las interficies físicas para el control y el puenteado, en concreto aquellas interficies por medio de las cuales la pasarela 20 recibe información y se comunica con el servidor 22 y el solicitante de contenido CR así como con el servidor alternativo.

Ejemplos de esto son:

DCCAControllf = fxp2

TowardsUserlf = fxp0

TowardsContentlf = fxp1

Subsiguientemente, la lógica estática de filtrado/activación a nivel 4 (reglas IP estáticas) se establece para implementarse por parte del módulo de filtro IP 60 sobre los paquetes entre las dos interficies puenteadas. Estos comprenden preferiblemente todas las tramas de interés para capturar la solicitud de usuario (y preferiblemente solamente dichas tramas) para cada protocolo sobre el cual se va a implementar la función. Esto indica también el puerto de desviación a nivel de núcleo donde los módulos 70 (análisis L7) y 74 (tratamiento de paquete) pueden recibir y reinyectar paquetes a través del puente entre el solicitante de contenido CR y el servidor alternativo. Dichos ajustes pueden comprender también aquellas configuraciones relacionadas con el bloqueo de las respuestas actuales para el protocolo. Por ejemplo, en el caso del protocolo Real de RealNetworks esta configuración puede comprender:

TriggerL4DivertRule = divert 11111 tcp from any to any 554,7070,7071 in via fxp1 established

InitL4FilterRule = deny udp from any to any 6979-7170 in via fxp0

A continuación, la lógica de análisis de nivel 7 se establece para extraer la referencia al contenido a transmitir al servidor 22 para propósitos de autorización. Esto se produce por medio de señalar el patrón de prefijo a buscar dentro de la trama (sin tomar en consideración el código de caracteres adoptado), dispuesto antes de la cadena referida a los contenidos. En el caso de Real esto puede tomar la forma:

TriggerL7PrefixString = “PLAY rtsp://”

A continuación, la lógica de tratamiento de paquete para propósitos de aceptación/denegación de paquete se establece para cada protocolo que se gestiona de una posible manera diferente para cada dominio hospedado. Se apreciará que en este caso, para los protocolos indicados, la pasarela 20 adoptará una lógica de filtrado del tipo activo sobre la solicitud como se indica en las figuras 7 y 8. En el caso de Real esto puede ser:

ReinjectAccept = <none>

ReinjectDeny = sorry.rm (para dominio hospedado = “rai.cdn.telecomitalia.it”

ReinjectDeny = please_subscribe.rm (para dominio hospedado = “cnn.cdn.telecomitalia.it”)

Como alternativa a la regla indicada anteriormente, la plantilla de regla a nivel 4 se establece para insertarse automáticamente en el caso de aceptación o se establece como negación para la gestión de la acción de filtrado activo retardado sobre la respuesta. Bastante a menudo, estas reglas son simplemente en forma de negación de una regla que se establece como InitL4FilterRule, que se instancia adecuadamente entre la dirección IP del solicitante de contenido CR y la dirección IP del servidor alternativo indicadas en la solicitud. Si la plantilla es diferente una definición útil puede ser:

TemplateAcceptRule = accept udp 6979-7170

que en el caso de aceptación produce la inserción (por parte del módulo de control de reglas 72) de una regla de nivel 4 para ser gestionada por el filtro de IP 60 del tipo:

accept udp from <Surrogate Server> to <Content Requester> 6970-7170 in via <TowardsContentIf>

y similarmente para la negación

TemplateDenyRule = deny udp 6970-7170

En los ejemplos de configuración que aquí se han dado esto puede convertirse en superfluo puesto que cae dentro de las reglas estáticas de la base de datos 66.

Las figuras 14 a 16 destacan los componentes de la pasarela 20 que entran en juego durante diferentes fases del funcionamiento de la pasarela 20.

Específicamente, la figura 14 destaca los componentes de la pasarela 20 que realizan la acción de activación de la solicitud.

En primer lugar, por medio de las reglas contenidas en la base de datos 66, la trama ("dependiente de la tecnología") procedente del solicitante de contenido CR se analiza a nivel 4 por parte del módulo de filtrado IP 60. Si es de interés, en lugar de transmitirse directamente (por parte del filtro IP 60) hacia la interficie 52 del servidor alternativo, la trama se intercepta y se transmite a través de sub-módulo 62 hacia el módulo de análisis 70 en el nivel de aplicación.

Por medio de utilizar las reglas de separación sobre el paquete contenido en la base de datos 78 (específicamente en lo que se refiere al prefijo de protocolo) el módulo de análisis 70 transmite hacia el solicitante de reglas 76 el conjunto que comprende:

- <los atributos de identificador del solicitante de contenido>
- <los atributos de identificador del contenido solicitado>
- <los atributos de identificador del servidor alternativo>

Este conjunto puede de hecho limitarse a la dirección IP del usuario y al URL así como a la dirección IP del servidor alternativo.

Se apreciará que de esta forma se realiza un mecanismo de autorización unitario que es "tecnológicamente independiente", es decir totalmente independiente de la tecnología de distribución de contenidos utilizada en la red.

El diagrama de la figura 15 destaca el componente de la pasarela 20 que implementa la comunicación hacia el servidor 22. Esta actividad se gestiona completamente por medio del módulo solicitante de reglas 76 que realiza las tareas de:

- empaquetar la solicitud utilizando los datos contenidos en el módulo de análisis 70, y

- transmitir la solicitud utilizando el puerto de comunicación 52 hacia el servidor.

Simultáneamente, el módulo 76 gestiona las respuestas procedentes del servidor. Estas respuestas (típicamente en forma de mensajes de aceptación/denegación teniendo posiblemente asociadas algunas características adicionales relativas al contenido como la duración, el ancho de banda solicitado, etcétera) se transmiten a los módulos de aplicación. Estos módulos gestionan la creación de reglas de filtrado dinámico (por medio del módulo de control de reglas 72) y el tratamiento de paquete (por medio del módulo de tratamiento de paquete 74).

En ausencia de respuesta desde el servidor 22 dentro de un cierto período de expiración, el módulo solicitante de reglas 76 fuerza reglas por defecto establecidas por el administrador, como aquellas que pretenden evitar la entrega del contenido.

Una fase de filtrado subsiguiente causa que la información se haga pasar o no desde el solicitante de contenido CR hasta el servidor alternativo y viceversa. Por esta razón los elementos que se destacan en la figura 16 (una vez más destacados por medio de líneas de puntos) dan lugar a una estructura interna de soporte, contenida en la lista de acceso a contenido (ACL) designada actualmente de la base de datos 80. Esta estructura describe las cláusulas de permitir/denegar activas para un usuario dado y un contenido dado y otros atributos útiles para el filtrado a nivel 7. Estas cláusulas se refieren además a una cláusula de nivel 4 gestionada por el módulo de filtro IP 60 y los sub-módulos relacionados.

La figura 18 describe el posible trazado para la memorización de las listas de acceso de contenido ACL dentro de la pasarela 20. Una estructura de este tipo se puede utilizar también dentro del servidor 22 para centralizar al almacenamiento de las ACL existentes.

Como se ha descrito anteriormente, una lista ACL define parámetros para una conexión/solicitud. Basándose en los mismos se pueden definir reglas para aceptar o denegar el acceso a ciertos recursos de red.

La figura 18 es un ejemplo de los campos de información que se utilizan para implementar la lógica de decisión (lógica de filtrado) dentro de la pasarela 20. En el caso de ejemplo que se muestra en la figura 18, los campos que se indican tienen el siguiente significado/función:

- Acción: describe la acción a realizar en presencia de ciertos parámetros de conexión (aceptar/denegar);

- IP origen e IP destino: representan la dirección IP de las entidades que establecen la conexión y comprenden, si es necesario, información referente a la identidad de la red privada virtual (VPN) y la máscara de subred;

- Protocolo: identifica el tipo de protocolo de transporte que se utiliza para la conexión (TCP/UDP);

- Puerto de entrada y puerto de salida: definen los puertos lógicos que se utilizan para la comunicación entre los procesos que establecen la conexión;

- D.H.: representa el dominio hospedado del cual se ha solicitado contenido (por ejemplo cdn.telecomitalia.it);

- Contenido: identifica el URL del contenido concreto solicitado como resultado de la conexión (por ejemplo: /recent/promo.asf);

- TTL: define el tiempo de validez de la cláusula de ACL, más allá del cual se eliminará dicha cláusula automáticamente.

La figura 16 destaca los componentes utilizados por la pasarela 20 para permitir el control de la solicitud por medio de establecer una acción de filtrado retardado que actúa sobre la respuesta como se presenta en las figuras 9 y 10.

En dicho caso, el módulo de tratamiento de paquete 74 transmite el paquete de solicitud hacia la interficie de salida 52 sin ninguna modificación. Para hacerlo, es activado inmediatamente por el módulo de solicitud de reglas 76 antes de transmitir la solicitud hacia el servidor alternativo.

La mayoría de la actividad la realiza el módulo de control de reglas 72. Este módulo recibe la información requerida por el módulo de solicitud de reglas 76 basándose en los criterios establecidos en el nivel de configuración para un protocolo dado por medio de interactuar con el módulo de control de filtro IP 60. El módulo de control de reglas 72 tiene la tarea de mantener/revisar las ACL contenidas en la base de datos 80, especialmente en lo que respecta a la función de gestión de los valores de TTL de las reglas.

La figura 17 destaca los componentes de la pasarela 20 que entran en juego durante la fase en la que se reinyecta una solicitud modificada. Como se ha descrito anteriormente esto corresponde a la solución alternativa que se considera en las figuras 7 y 8.

Las dos opciones se pueden configurar para un único protocolo y permiten obtener diferentes características dependiendo de las necesidades del operador. Dos factores básicos a este respecto se representan por medio de una sensibilidad mayor/menor a los retardos de la respuesta por parte del servidor y el tiempo de expiración de la aplicación, o la personalización menor/mayor de la gestión de las negativas a la solicitud.

En este último caso, el módulo de tratamiento de paquete 74 realiza la mayor parte de la actividad relacionada. Dependiendo de la respuesta (aceptación/denegación) recibida del solicitante de reglas 76, el módulo de tratamiento de paquete 74 determina si y de qué forma el paquete de solicitud original (todavía en “espera”) se va a reinyectar en el nivel de núcleo para transmitirse al servidor alternativo.

En dicho caso, la creación de una ACL local conduce a la optimización de cualquier solicitud subsiguiente del mismo tipo, por medio de crear un tipo de memoria intermedia evitándose de esta forma consultas continuadas al servidor.

Una ventaja básica de esta disposición se encuentra en el hecho de que permite el redireccionamiento en línea del paquete hacia los denominados “destinos de disculpa” (estos son normalmente en forma de páginas html, películas u otros, dependiendo del tipo de solicitud), mientras se mantiene la conexión TCP con el servidor alternativo activo y sin requerir la presencia de un módulo de programa de emulación para cada tecnología que se quiere gestionar.

Las realizaciones prácticas de la pasarela 20 se concentran en un sistema en el cual la acción de activación, y la acción de filtrado subsiguiente, se realizan con un alto grado de granularidad, especialmente en relación con cada uno de los contenidos solicitados por un usuario específico.

A ese respecto, se han considerado tanto i) las disposiciones que se comportan como representante para los servicios de contenido, como ii) las disposiciones que realizan filtrado a nivel de puenteado, por medio de evaluar sus características en términos de transparencia respecto al impacto del agente - o el componente que juega el papel del agente - sobre la red (lo que se denomina cortafuegos "transparente").

Como extensión añadida, los componentes de activación y filtrado se pueden considerar por separado para extender el análisis también a aquellos sistemas de análisis de paquetes e inspección de paquetes existentes en sistemas de filtrado de red que son suficientemente configurables y granulares.

Finalmente, se consideran varios modos posibles de tratamiento/reinyección de paquetes.

Una primera observación es que FreeBSD y Linux ofrecen la posibilidad de filtrar paquetes IP hasta nivel 4, redireccionándolos a una toma de núcleo mientras se permite también la gestión a nivel de aplicación. Esta capacidad se explota por parte de muchos sistemas de análisis de red. Adicionalmente, FreeBSD ofrece la posibilidad de transmitir paquetes IP que satisfacen una regla de cortafuegos dada hacia una aplicación de usuario que puede decidir si dichos paquetes se van a modificar o reinyectar en la red (regla de derivación). En este caso, el sistema se encarga de reensamblar de forma correcta las tramas Ethernet.

Adicionalmente, tanto FreeBSD como Linux ofrecen la posibilidad de configurar un par de interficies de red en un modo puenteado. Esta disposición, sin embargo, no ofrece ya la posibilidad de derivar los paquetes.

El análisis de paquetes no solicita necesariamente la disponibilidad de un representante de capa de aplicación. El análisis se puede realizar a través de los mecanismos de análisis de las expresiones regulares (el denominado "análisis cruzado"), como utilizan típicamente los sistemas de detección de intrusos. Ciertos sistemas de detección de intrusos proporcionan un mecanismo de activación si se detecta una firma definida anteriormente al comparar el paquete de Ethernet.

Otros sistemas utilizan el mecanismo de firma para realizar una conformación inteligente de los paquetes, funcionando a nivel 7.

El diagrama de bloques de la figura 19 destaca las varias fases del funcionamiento de la disposición que aquí se describe sin referirse de forma expresa a la situación de los módulos en el interior de los diferentes dispositivos.

En una etapa 100 un paquete 100 entra en la pasarela DCCA 20.

En una etapa 102 el análisis de nivel 4 (por ejemplo de dirección, protocolo y puertos) detecta ciertos paquetes a redirigir (derivar) hacia el análisis de nivel 7. Los paquetes que no son filtrados por la regla de nivel 4 siguen (después de algunos controles posibles basados en otras reglas de nivel 4 para otros protocolos en el bloque 102), un flujo de puente típico a través del bloque 118 de forma inalterada.

El análisis de nivel 7 se representa por medio de un bloque 106.

En la realización de ejemplo que aquí se describe este análisis se realiza en terreno del usuario y no a nivel de núcleo. En cualquier caso, dicho análisis determina las características de la solicitud y transmite la solicitud de autorización al módulo de autorización (bloque 108). En la realización de ejemplo que aquí se describe esto es implementado por el servidor 22. En cualquier caso, el análisis de nivel 7 puede requerir la autorización temporal de la solicitud (en el caso del modo de funcionamiento basado en autorización retardada con control de respuesta). En dicho caso, el dispositivo puede establecer una regla basada en el tiempo.

La fase de establecimiento de regla se representa por medio de un bloque 110. Esto comporta normalmente reglas de activación para habilitar el tráfico en dos direcciones y, generalmente, otras reglas relacionadas que permiten la gestión de la contabilidad sobre el tráfico de respuesta (esto es realizado normalmente por un módulo externo que se designa como 112).

La fase de autorización que se realiza en el módulo 108 puede dar lugar (por ejemplo, como resultado de una respuesta negativa) a un redireccionamiento en línea de la solicitud actuando sobre la fase de redirección (bloque 114).

Subsiguientemente, la fase de reinyección 104 reinserta el paquete sometido anteriormente a una acción de derivación (modificado posiblemente como resultado de la redirección). Finalmente, en una etapa que se designa como 116 el paquete (derivado o reinyectado) abandona el dispositivo.

La figura 20 muestra el tráfico de red de entrada (solicitud de contenido multimedia), interceptado y filtrado a nivel de núcleo (por medio de reglas de cortafuegos IP) y conducido a un espacio de usuario. Allí, módulos JAVA se encargan de la tarea de autorización de solicitudes y de reinyectar el tráfico a nivel de núcleo para dar servicio a la solicitud de forma tradicional.

Como se ha indicado, una localización preferida de la pasarela 20 es delante del servidor. De esta forma, se puede controlar el servidor por medio de asegurar que el camino de red para alcanzarlo, comenzando desde cualquier cliente considerado, es - por necesidad - solamente uno, pasando a través del dispositivo.

En otro caso, un núcleo FreeBSD 4.8 se puede modificar para asegurar que algunos sub-componentes de la orden ipfw (relacionados con la derivación y reinyección de los paquetes hacia y desde el nivel de aplicación) pueden funcionar correctamente también con los paquetes puenteados.

Las solicitudes por parte de los usuarios finales se interceptan en la interficie de entrada de red y se hacen pasar, a través de la pila de protocolo de red, al módulo de núcleo (cortafuegos IP) para el filtrado de paquetes. Dicho módulo analiza y filtra el tráfico de red por medio de establecer reglas del tipo:

0400 accept from 192.168.0.1 22222 to 192.168.0.2 33333 tcp in via fxp0 established

Donde el primer parámetro representa el identificador de la regla del cortafuegos IP, el segundo la acción a realizar (permitir/denegar/derivar), seguido por las direcciones IP del origen y el destino y los puertos lógicos respectivos, el protocolo de transporte, la interficie de entrada para el tráfico y, en el caso considerado (protocolo TCP) el control de la bandera SYS para controlar si se establece o no la conexión.

El cortafuegos IP ofrece una función adicional que permite transmitir tráfico que satisface las condiciones de la regla hacia el espacio de usuario utilizando un conector específico (DIVERT_SOCKET). De esta forma, cualquier tarea de procesado relacionada con el tráfico de red se puede desplazar al nivel de aplicación.

Para dicho propósito, es suficiente indicar la opción “divert” (desviar) como campo de acción en la regla de cortafuegos IP:

0400 divert 44444 from 192.168.0.1 to 192.168.0.2 33333 tcp via fxp0 established

Esto indica también el puerto lógico de la toma de desviación (44444) hacia la cual se debe transmitir el tráfico de red que satisface la regla.

Un módulo desarrollado en C (C_a_JAVA) asegura la interficie adecuada de las tomas de desviación con las aplicaciones JAVA para analizar y procesar la solicitud procedente del nivel de núcleo.

Por ejemplo, una disposición de este tipo se puede aplicar a tráfico ICMP (del tipo solicitud de eco) utilizando, como regla del cortafuegos IP para la interceptación:

0400 divert 44444 from 192.168.2.2 to 192.168.2.1 icmp in via fxp1 icmptype 8

Esto tiene el propósito de interceptar las solicitudes ICMP desde el cliente en la interficie “fxp1”, haciendo pasar dichos paquetes a un módulo de programa JAVA que escucha al puerto “44444” para la salida de vídeo de paquetes de datos y reinyectar el tráfico en la interficie de salida (fxp0).

De esta forma el filtro es transparente al cliente solicitante, mientras que intercepta correctamente (y posiblemente imprime) los paquetes ICMP sobre una salida estándar.

Se realizaron experimentos alternativos utilizando el protocolo “mmst” (mmst sobre transporte TCP) utilizando como regla del cortafuegos IP:

0400 divert 44444 from 192.168.2.2 to 192.168.2.1 tcp in via fxp1 established

Esto tiene el propósito de interceptar todos los paquetes de datos que solicitan contenidos multimedia del servidor de Windows Media™ (sesiones TCP con establecer: SYN = 0), haciéndolos pasar a un módulo de programa JAVA en el espacio de usuario para la salida de vídeo y la reinyección dentro del tráfico en la interficie de salida (fxp0).

El flujo de audio/vídeo se dejó inalterado durante el proceso de interceptación y reinyección. Durante la operación, es posible visualizar los URL contenidos dentro de la solicitud procedente del servidor. Por medio de comunicarse con el servidor de seguridad, el módulo JAVA del agente comprueba si la dirección IP que ha solicitado un contenido dado se habilita para recibir el contenido del URL solicitado.

En dicho caso, el tráfico desviado hacia un espacio de usuario se reinyecta a nivel del núcleo utilizando las tomas de desviación y la solicitud se transmite subsiguientemente a través de las interficies de salida a los dispositivos de almacenamiento pertinentes.

En el caso en el que la prueba realizada por el módulo JAVA entregue un resultado negativo, existen dos posibilidades:

- el tráfico se descarta o redirige hacia una página de disculpa (lógica positiva),

- en otro caso el tráfico se reinyecta a nivel de núcleo y se permite que llegue a los dispositivos de almacenamiento mientras que se bloquea el flujo de respuesta procedente de las memorias intermedias (lógica negativa).

El redireccionamiento del tráfico de red desde el espacio de núcleo hasta el espacio de usuario a través de las tomas de desviación se hace posible modificando el módulo de núcleo relacionado con el cortafuegos IP. Esto realiza originariamente un control de la consistencia de los paquetes IP antes de la operación de desviación (que por tanto no se permite sobre paquetes no IP). La modificación elimina este tipo de control, permitiendo de esta forma la posibilidad de realizar una acción de desviación sobre tramas de Ethernet “puras”.

La disposición que aquí se describe autoriza solicitudes utilizando el paradigma PULL: el usuario avanza la solicitud; ésta se intercepta directamente o se intercepta el flujo asociado, y se generan finalmente listas de control sobre un sistema de red.

Adicionalmente, el mecanismo intercepta la solicitud o el flujo de retorno identifica un evento de comienzo de contabilidad, concretamente el comienzo de la entrega. Subsiguientemente, la generación automática de la entrada de las listas de control conduce al sistema de la red a monitorizar la actividad generando posiblemente otros tipos de registros de utilización (espera y paro). La información disponible comprende todos los elementos que permiten la tarificación, en concreto:

- tarificación basada en consumo, gracias a los datos de tráfico capturados de la entrada de la lista de control,

- tarificación basada en tiempo, gracias a la gestión de los eventos de comienzo y paro, y

- tarificación basada en evento/contenido, gracias a la indicación de la referencia a los contenidos.

De esta forma, se da al operador la posibilidad de realizar la tarificación basándose en el tráfico realizando así la tarificación por tiempo en servicios en directo, la tarificación por evento en servicios de vídeo bajo demanda y similares, mientras se resta el componente de tráfico de la cantidad total para evitar una doble tarificación.

Esta disposición se puede aplicar de forma transparente a diferentes arquitecturas de distribución de contenidos (tanto centralizadas como descentralizadas).

La misma disposición se puede utilizar, sin el mecanismo de activación, para realizar autorizaciones basadas en el paradigma PUSH, por medio del aprovisionamiento previo por parte de un servidor central basándose en lógica de control no activada directamente por la red, sino activada por aplicaciones externas.

El paradigma PULL es significativo por el hecho de que proporciona ciertas mejoras “sobre la marcha” al servicio de distribución de contenido. Esto se realiza de forma completamente transparente respecto a los dos puntos de extremo involucrados, en concreto el solicitante de contenido CR y el servidor que proporciona el servicio. Basándose en las características del dispositivo de activación/filtrado y de las funciones de control proporcionadas posiblemente por un servidor externo, se puede utilizar la disposición que aquí se describe para otros propósitos.

Ejemplos de esto son los siguientes.

Soporte para calidad de servicio (QoS) dinámica. Siguiendo una solicitud de acceso a cierto contenido, el servidor 22 puede detectar los requerimientos específicos y generar una solicitud de reserva hacia el sistema de gestión de QoS, para el ancho de banda solicitado y para la duración del contenido, utilizando el servidor alternativo y el solicitante de contenido como punto de extremo. Alternativamente, existe la posibilidad de comunicarse directamente con la pasarela 20 para etiquetar las tramas de retorno desde el servidor de contenido con el nivel de servicio correspondiente.

Alternativamente, la misma disposición se puede utilizar para soportar portales de aplicación externos, por medio de controlar y autorizar, de forma transparente, el acceso por parte de terceras partes a los contenidos de un portal, sin la necesidad de proporcionar esta función de forma nativa.

Todavía alternativamente, se puede utilizar la misma disposición para el redireccionamiento de forma controlada de solicitudes a atributos prefijados en tiempo real. Esto conduce a un mecanismo de redireccionamiento de las solicitudes de usuario por medio de reconstruir desde el inicio el URL. De esta forma, una solicitud se puede adaptar según atributos específicos del usuario y criterios dados que se pueden derivar a partir de sistemas externos como:

- información en tiempo real relativa a la localización para cambiar, por ejemplo, una solicitud para www.restaurants.it a restaurants.it/Milan;

- dependiendo de la hora del día, pudiendo transformar una solicitud del tipo www.rai.it/lastnews en una solicitud más general como rai.it/eveningnews;

- dependiendo del ancho de banda disponible, transformando una solicitud del tipo www.trailer.it/mickey en una solicitud www.trailer.it/30Kb/mickey;

- dependiendo de las características del terminal de usuario. Esto puede basarse por ejemplo en detectar un contenido de red móvil por medio de la dirección IP y el identificador IMEI (identidad internacional de equipos móviles) mientras se deriva a partir de los mismos características específicas del terminal (pantalla, capacidades, etc.). Una solicitud genérica para un cierto contexto se puede transformar de esta forma en una solicitud adaptada a las características del equipo receptor.

Como regla, el mecanismo de interceptación y filtrado disponible con la pasarela 20 evalúa ciertas características en tiempo real, mientras permite que se tome una decisión sobre la mejor forma de servir el contenido de la solicitud.

Una pasarela como se ha descrito arriba se puede implementar, opcionalmente:

- directamente en el servidor alternativo (cluster),

- directamente en un elemento de red comprendido en el flujo de tráfico entre el usuario y el servidor (cluster),

- por medio de un dispositivo dedicado insertado de forma transparente en la infraestructura de red en el flujo de tráfico entre el usuario y el servidor alternativo (cluster), considerándose esta última una realización preferida.

El servidor de seguridad que implementa el mecanismo de verificación sobre el acceso se puede implementar opcionalmente:

- como una derivación de un servidor AAA genérico con una conexión de acceso hacia las capacidades del usuario respecto al contenido,

- como una derivación de un servidor de seguridad genérico con un módulo insertado similar, y

- como un sistema dedicado para vigilancia de contenido de seguridad, considerándose ésta actualmente la realización preferida.

El dispositivo se dispone preferiblemente, y todavía preferiblemente se dispone conjuntamente, con el servidor de contenido (centro de servicio o sitios CDN). Como alternativa, se puede disponer en una red de acceso, aguas abajo del primer dispositivo IP existente.

Es por tanto evidente que, sin perjuicio de los principios básicos de la presente invención, pueden variar los detalles y realizaciones de la misma, también de forma significativa, respecto a como se ha descrito, a modo de ejemplo solamente, sin salir del ámbito de la presente invención como se define en las siguientes reivindicaciones.

Referencias citadas en la presente descripción

Esta lista de referencias citadas por el solicitante es solamente para la conveniencia del lector. No forma parte del documento de Patente Europea. Aunque se ha prestado gran atención a la recopilación de las referencias, no se pueden descartar errores u omisiones y la Oficina Europea de Patentes declina cualquier responsabilidad respecto a la misma.

Documentos de patente citados en la presente descripción

- WO 9957866 A [0031]
- WO 0131886 A [0032]
- US 6130892 B [0032]
- WO 0235797 A [0032]
- US 6636894 B [0032]

Literatura no de patente citada en la presente descripción

- Windows Media 9 Series Deployment Guide. *Microsoft*, diciembre de 2002, páginas 47-51 [0007]
- Helix Universal Server Administration Guide, Version 9.0. *Real Networks*, 19 de mayo de 2003, páginas 247-299 [0007]
- Cisco ACNS 5.1 Caching And Streaming Configuration Guide, Release 5.1, 2003, páginas 227-270 [0018]

REIVINDICACIONES

1. Procedimiento para la gestión de transacciones en una red de comunicaciones, comprendiendo dichas transacciones por lo menos una solicitud dependiente de la tecnología de un contenido dado realizada por un solicitante (CR) a por lo menos un servidor (14), comprendiendo el procedimiento las etapas de:

- hacer disponible una lista de contenido de acceso (80) que comprende cláusulas de permiso/denegación de acceso que regulan el acceso de dicho solicitante (CR) a los contenidos proporcionados por dicho por lo menos único servidor (14),

- detectar (56) dicha solicitud dependiente de la tecnología,

- extraer (58) de dicha solicitud dependiente de la tecnología informaciones que identifican al solicitante (CR) que realiza la solicitud y al contenido que se solicita,

- generar (58) a partir de las informaciones extraídas de dicha solicitud dependiente de la tecnología una entrada de acceso a contenido correspondiente independiente de la tecnología,

- comprobar (22) dicha entrada en dicha lista para deducir información de permiso/denegación referente a la solicitud detectada, y

- gestionar dicha solicitud en función de dicha información deducida de permiso/denegación, **caracterizado** por el hecho de que dicha gestión de dicha solicitud comprende, indiferentemente de dicha información deducida de permiso/denegación, la etapa de transmitir (116) dicha solicitud detectada a dicho por lo menos único servidor (14) y, en función de dicha información deducida de permiso/denegación, realizar las etapas alternativas de:

  - i) bloquear la transacción asociada con dicha solicitud detectada, si la información de permiso/denegación indica que el solicitante no está autorizado, o

  - ii) dejar continuar la transacción asociada con dicha solicitud, si la información de permiso/denegación indica que el solicitante está autorizado.

2. Procedimiento según la reivindicación 1, **caracterizado** por el hecho de que dicha etapa de bloqueo se realiza por medio de bloquear un flujo de datos de respuesta (4, 5) desde dicho por lo menos único servidor (14) al solicitante (CR) que realiza dicha solicitud detectada.

3. Procedimiento según cualquiera de las reivindicaciones 1 y 2, **caracterizado** por el hecho de que dicha etapa de bloqueo se retarda (114) respecto a la deducción de dicha información de permiso/denegación.

4. Procedimiento según la reivindicación 1, 2 o 3, **caracterizado** por el hecho de que dicha entrada de acceso a contenido comprende:

- atributos de identificación del solicitante (CR) que realiza la solicitud detectada,

- atributos de identificación del contenido solicitado, y

- atributos de identificación de dicho por lo menos único servidor (14) al cual se realiza la solicitud.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por el hecho de que comprende la etapa de proporcionar una función de pasarela (20) entre dicho solicitante (CR) y dicho por lo menos único servidor (14).

6. Procedimiento según la reivindicación 5, **caracterizado** por el hecho de que comprende las etapas de:

- configurar dicha función de pasarela (20) para realizar por lo menos una de dichas etapas de detectar, extraer, generar y gestionar, y

- asociar a dicha función de pasarela (20) una función de servidor de reglas de contenido (22) para realizar dicha etapa de comprobación.

7. Procedimiento según la reivindicación 6, **caracterizado** por el hecho de que comprende la etapa de proporcionar a dicha función de pasarela (20) funciones de interficie (50, 52, 54) con dichos solicitantes (CR) y dicho por lo menos único servidor (14) así como respecto a dicha función de servidor de reglas de contenido (22), respectivamente.

8. Procedimiento según la reivindicación 5, 6 o 7, **caracterizado** por el hecho de que comprende la etapa de proporcionar a dicha función de pasarela (20) una pluralidad de niveles que comprenden:

- un nivel inferior de núcleo (56) dentro de la pluralidad de niveles, que proporciona funciones de tratamiento de red, de derivación y de filtrado de nivel IP relacionadas con la detección de dicha solicitud, y

- un nivel de aplicación (58) por encima del nivel inferior de núcleo dentro de la pluralidad de niveles para realizar dichas etapas de extracción y generación.

9. Procedimiento según la reivindicación 8, **caracterizado** por el hecho de que dicho nivel inferior de núcleo (56) realiza por lo menos una de las etapas de:

- filtrar (60) flujos de datos que se intercambian entre dichos solicitantes (CR) y dicho por lo menos único servidor (14),

- desviar (62) dichos flujos de datos hacia dicho nivel de aplicación, y

- reinyectar (64) dichos flujos de datos dentro de dicha red.

10. Procedimiento según la reivindicación 9, **caracterizado** por el hecho de que comprende la etapa de realizar dicho filtrado como un filtrado de paquetes IP.

11. Procedimiento según la reivindicación 10, **caracterizado** por el hecho de que comprende la etapa de realizar dicho filtrado IP como un filtrado de paquetes IP hasta nivel 4.

12. Procedimiento según la reivindicación 8, **caracterizado** por el hecho de que comprende la etapa de realizar dentro de dicho nivel de aplicación (58) las operaciones de:

- extraer (70) a partir de dicha solicitud informaciones que identifican a dicho solicitante (CR) y al contenido solicitado,

- transmitir (76) dichas informaciones extraídas a dicha función de servidor de reglas de contenido (22), y

- controlar (72, 60a) dicho nivel inferior de núcleo (56).

13. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por el hecho de que comprende la etapa de detectar dicha solicitud sin afectar a dicha solicitud.

14. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por el hecho de que dicha etapa de extracción comprende el análisis de los paquetes comprendidos dentro de dicha solicitud.

15. Procedimiento según la reivindicación 14, **caracterizado** por el hecho de que dicho análisis se realiza en forma de análisis de nivel 7.

16. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por el hecho de que comprende la etapa de generar, basándose en dicha información de permiso/denegación, por lo menos una solicitud de reserva a un sistema de gestión de calidad de servicio (QoS).

17. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por el hecho de que comprende la etapa de redirigir dicha solicitud de usuario por medio de modificar selectivamente un identificador (URL) asociado con la misma.

18. Procedimiento según la reivindicación 1, **caracterizado** por el hecho de que comprende las etapas de:

- detectar información sobre el terminal asociado con el solicitante (CR) que realiza dicha solicitud detectada, y

- modificar dicha solicitud detectada en función de dicha información sobre el terminal asociado con el solicitante (CR).

19. Sistema para la gestión de transacciones en una red de comunicaciones, comprendiendo dichas transacciones por lo menos una solicitud dependiente de la tecnología de un contenido dado realizada por un solicitante (CR) a por lo menos un servidor (14), comprendiendo dicho sistema una lista de acceso de contenido (80) que comprende cláusulas de permiso/denegación de acceso que regulan el acceso de dicho solicitante (CR) a los contenidos proporcionados por dicho por lo menos único servidor (14), y por lo menos un módulo de procesado de solicitud (20, 22) que comprende sub-módulos configurados para:

- detectar (56) dicha solicitud dependiente de la tecnología,

- extraer (58) a partir de dicha solicitud dependiente de la tecnología informaciones que identifican al solicitante (CR) que realiza la solicitud y al contenido solicitado,

- generar (58) a partir de dichas informaciones extraídas de dicha solicitud dependiente de la tecnología una entrada de acceso a contenido independiente de la tecnología correspondiente,

- comprobar (22) dicha entrada en dicha lista para deducir información de permiso/denegación referente a la solicitud detectada, y

- gestionar dicha solicitud en función de dicha información deducida de permiso/denegación, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para realizar, independientemente de dicha información de permiso/denegación deducida, la etapa de transmitir (116) dicha solicitud detectada a dicho por lo menos único servidor (14) y, en función de dicha información de permiso/denegación deducida, realizar las etapas alternativas de:

  - i) bloquear la transacción asociada con dicha solicitud detectada, si la información de permiso/denegación indica que el solicitante no está autorizado, o

  - ii) dejar continuar la transacción asociada con dicha solicitud, si la información de permiso/denegación indica que el solicitante está autorizado.

20. Sistema de la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para realizar dicha etapa de bloqueo por medio de bloquear un flujo de datos de respuesta (4, 5) entre dicho por lo menos único servidor (14) y el solicitante (CR) que realiza dicha solicitud detectada.

21. Sistema según cualquiera de las reivindicaciones 19 o 20, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para realizar dicha etapa de bloqueo como una etapa retardada (114) respecto a la deducción de dicha información de permiso/denegación.

22. Sistema según las reivindicaciones 19, 20 o 21, **caracterizado** por el hecho de que dicha entrada de acceso a contenido comprende:

- atributos de identificación del solicitante (CR) que realiza la solicitud detectada,

- atributos de identificación del contenido solicitado, y

- atributos de identificación de dicho por lo menos único servidor (14) al cual se realiza la solicitud.

23. Sistema según cualquiera de las reivindicaciones 19 a 22, **caracterizado** por el hecho de que comprende una pasarela (20) entre dicho solicitante (CR) y dicho por lo menos único servidor (14).

24. Sistema según la reivindicación 23, **caracterizado** por el hecho de que dicha pasarela (20):

- se configura para realizar por lo menos una de dichas etapas de detectar, extraer, generar y gestionar, y

- dispone de un servidor de reglas de contenido asociado (22) para realizar dicha etapa de comprobación.

25. Sistema según la reivindicación 24, **caracterizado** por el hecho de que dicha pasarela (20) dispone de funciones de interficie (50, 52; 54) con dichos solicitantes (CR) y dicho por lo menos único servidor (14) así como respecto a dicha función de servidor de reglas de contenido (22), respectivamente.

26. Sistema según cualquiera de las reivindicaciones 23 a 25, **caracterizado** por el hecho de que dicha pasarela (20) comprende:

- un nivel inferior de núcleo (56), que proporciona funciones de tratamiento de red, de puenteado y funciones de filtrado de nivel IP relacionados con la detección de dicha solicitud, y

- un nivel de aplicación (58) para realizar dichas etapas de extracción y generación.

27. Sistema según la reivindicación 26, **caracterizado** por el hecho de que dicho nivel inferior de núcleo (56) se configura para realizar por lo menos una de las etapas de:

- filtrar (60) flujos de datos que se intercambian entre dichos solicitantes (CR) y dicho por lo menos único servidor (14),

- desviar (62) dichos flujos de datos hacia el nivel de aplicación, y

- reinyectar (64) dichos flujos de datos dentro de dicha red.

28. Sistema según la reivindicación 27, **caracterizado** por el hecho de que dicha pasarela (20) se configura para realizar dicho filtrado como un filtrado de paquetes IP.

29. Sistema según la reivindicación 28, **caracterizado** por el hecho de que dicho filtrado IP comprende un filtrado de paquetes IP hasta nivel 4.

30. Sistema según la reivindicación 26, **caracterizado** por el hecho de que dicho nivel de aplicación (58) se configura para:

- extraer (70) a partir de dicha solicitud informaciones que identifican a dicho solicitante (CR) y al contenido solicitado,

- transmitir (76) dichas informaciones extraídas a dicha función de servidor de reglas de contenido (22), y

- controlar (72, 60a) dicho nivel inferior de núcleo (56).

31. Sistema según la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para detectar dicha solicitud sin afectar a dicha solicitud.

32. Sistema según la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para analizar los paquetes comprendidos en dicha solicitud.

33. Sistema según la reivindicación 32, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para realizar dicho análisis en forma de análisis de nivel 7.

34. Sistema según la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para generar, basándose en dicha información de permiso/denegación, por lo menos una solicitud de reserva a un sistema de gestión de calidad de servicio (QoS).

35. Sistema según la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para redirigir dicha solicitud de usuario por medio de modificar selectivamente un identificador (URL) asociado con la misma.

36. Sistema según la reivindicación 19, **caracterizado** por el hecho de que dicho por lo menos único módulo de procesado (20, 22) se configura para:

- detectar información referente al terminal asociado con el solicitante (CR) que realiza la solicitud, y

- modificar dicha solicitud detectada como función de dicha información referente al terminal asociado con el solicitante (CR).

37. Red de comunicaciones que comprende un sistema según cualquiera de las reivindicaciones 19 a 36.

38. Producto programa de ordenador que se puede cargar en la memoria de por lo menos un ordenador y que comprende partes de código de programa para realizar el procedimiento según cualquiera de las reivindicaciones 1 a 18.

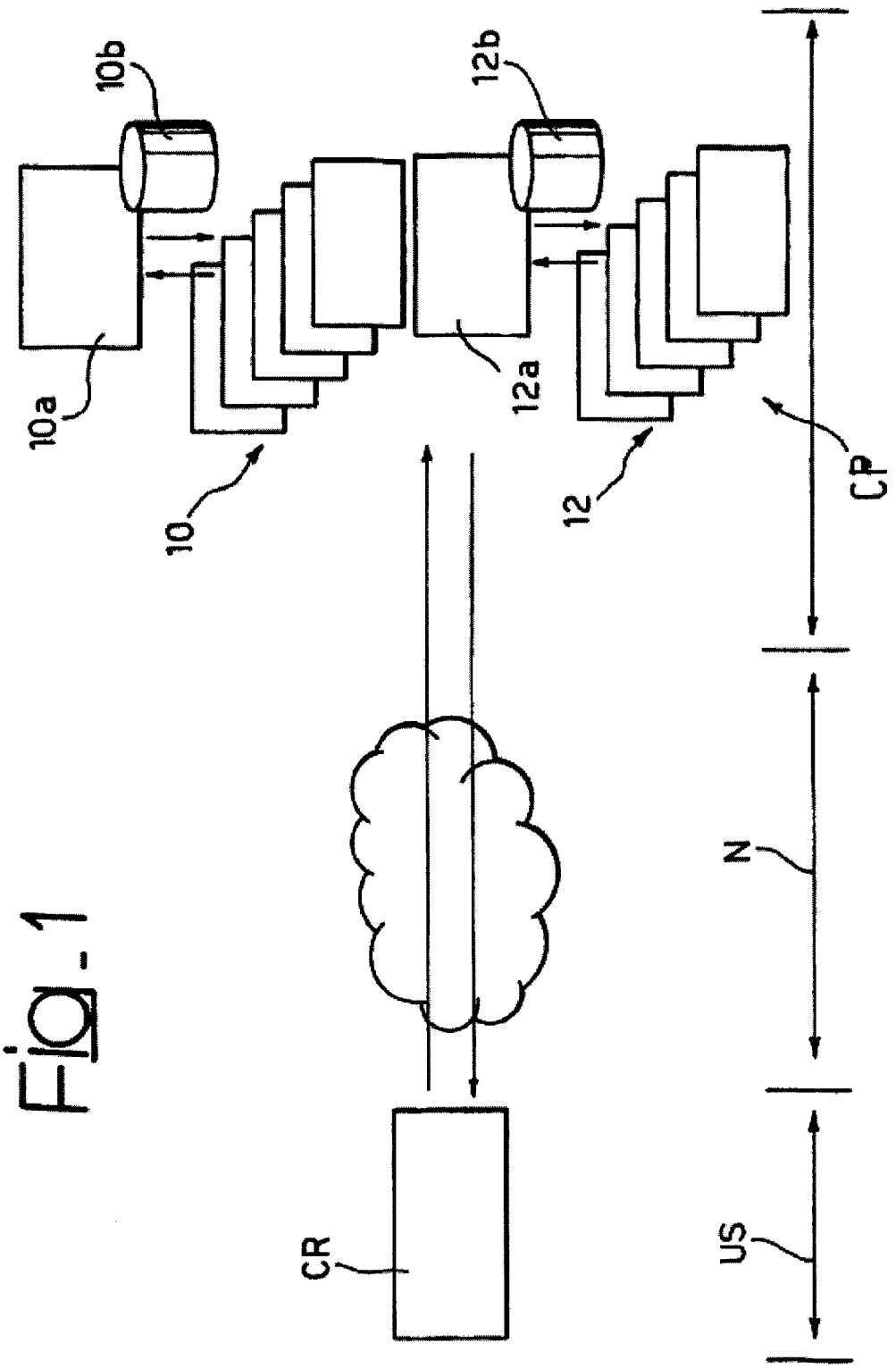
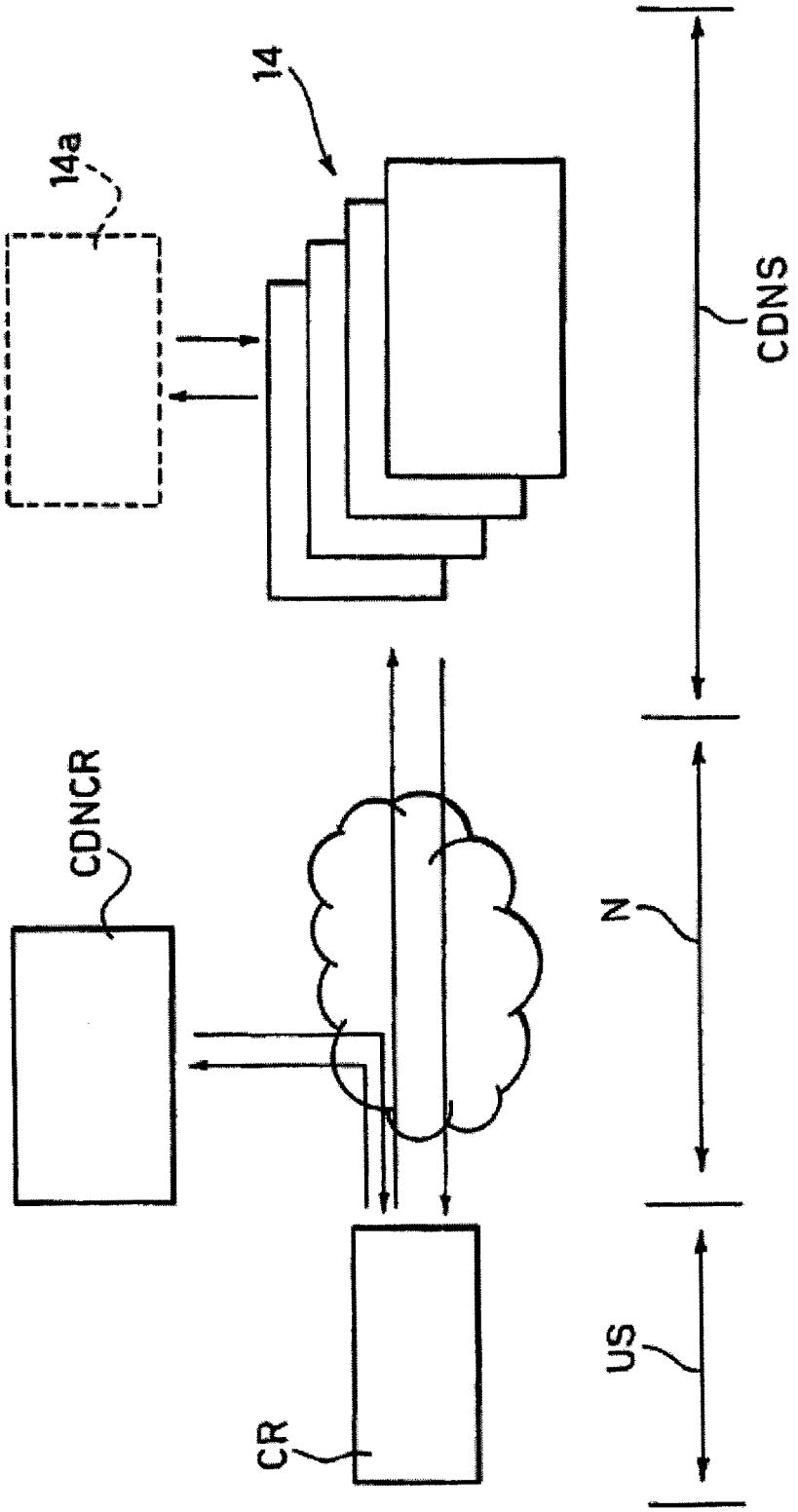


Fig. 1

Fig.2



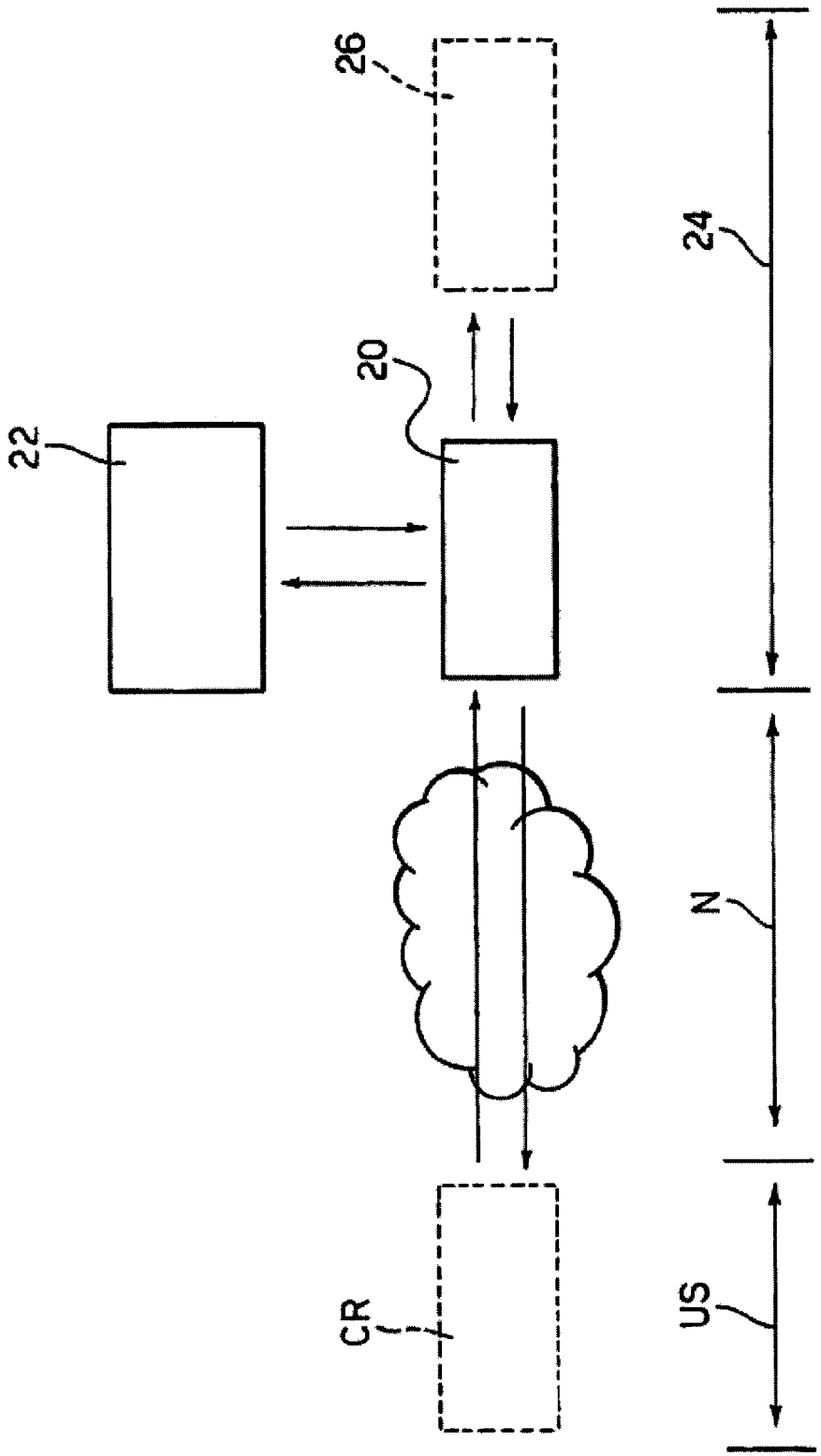


Fig-3

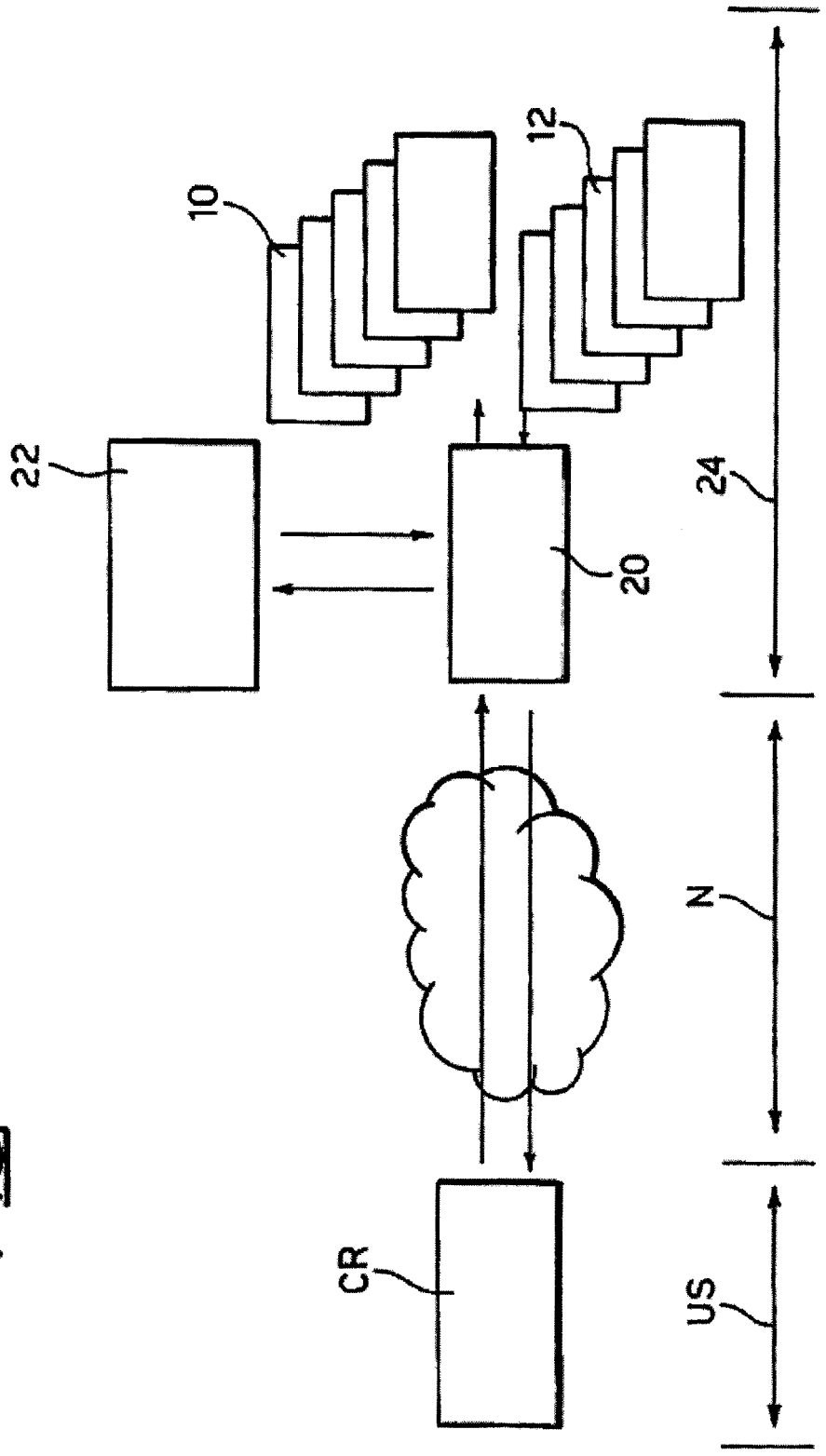


Fig. 4

Fig.5

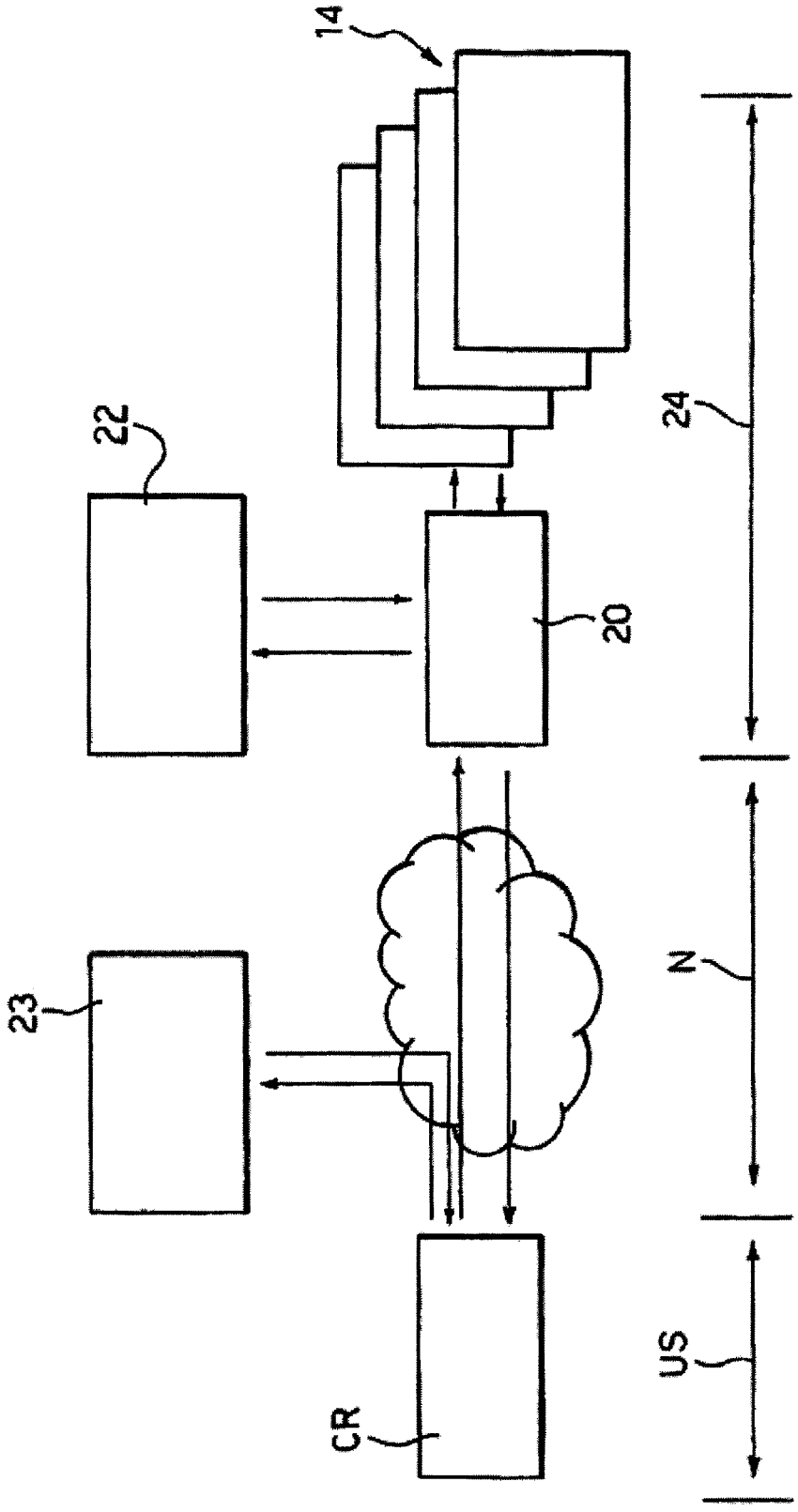
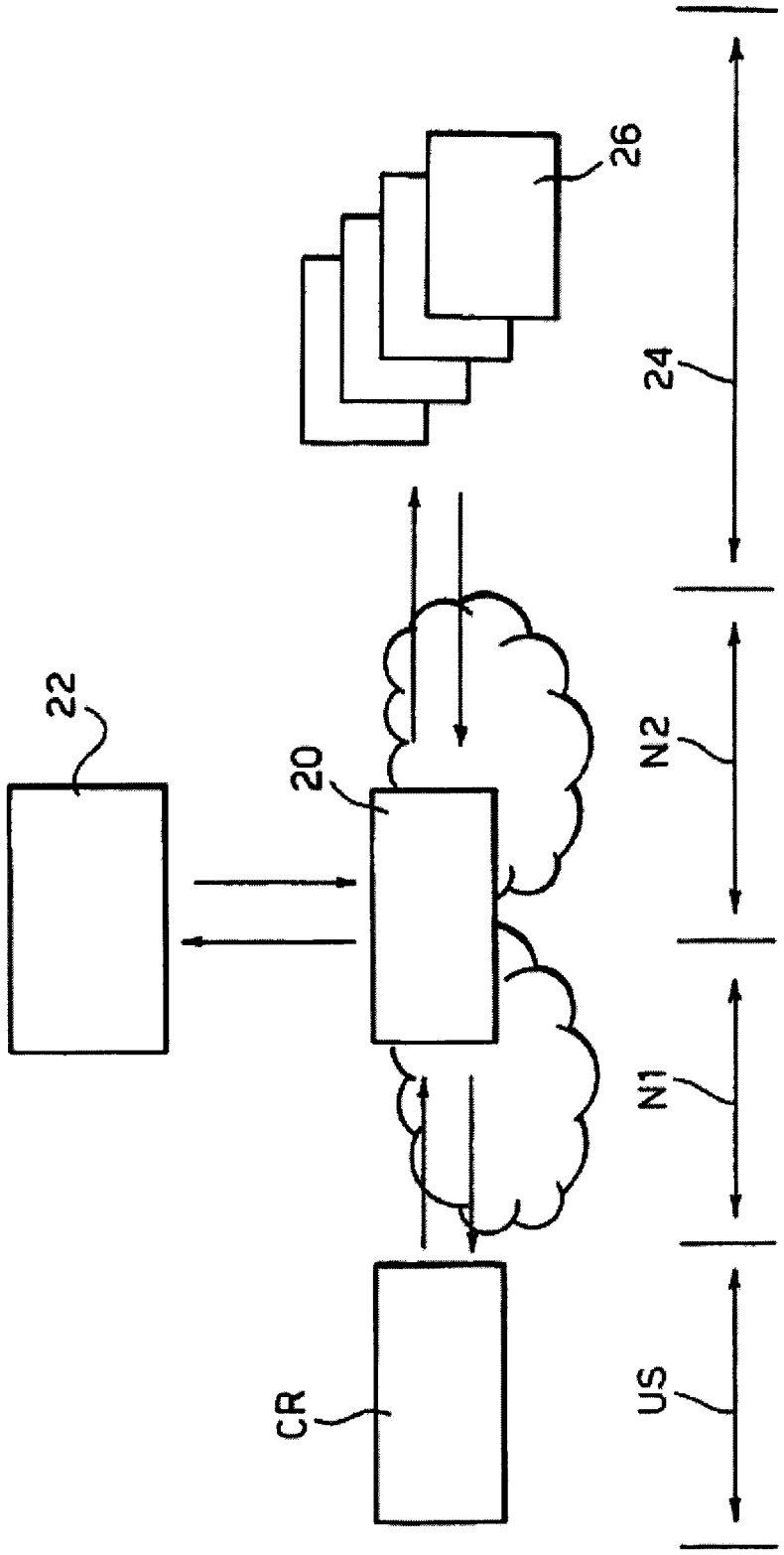


Fig.6



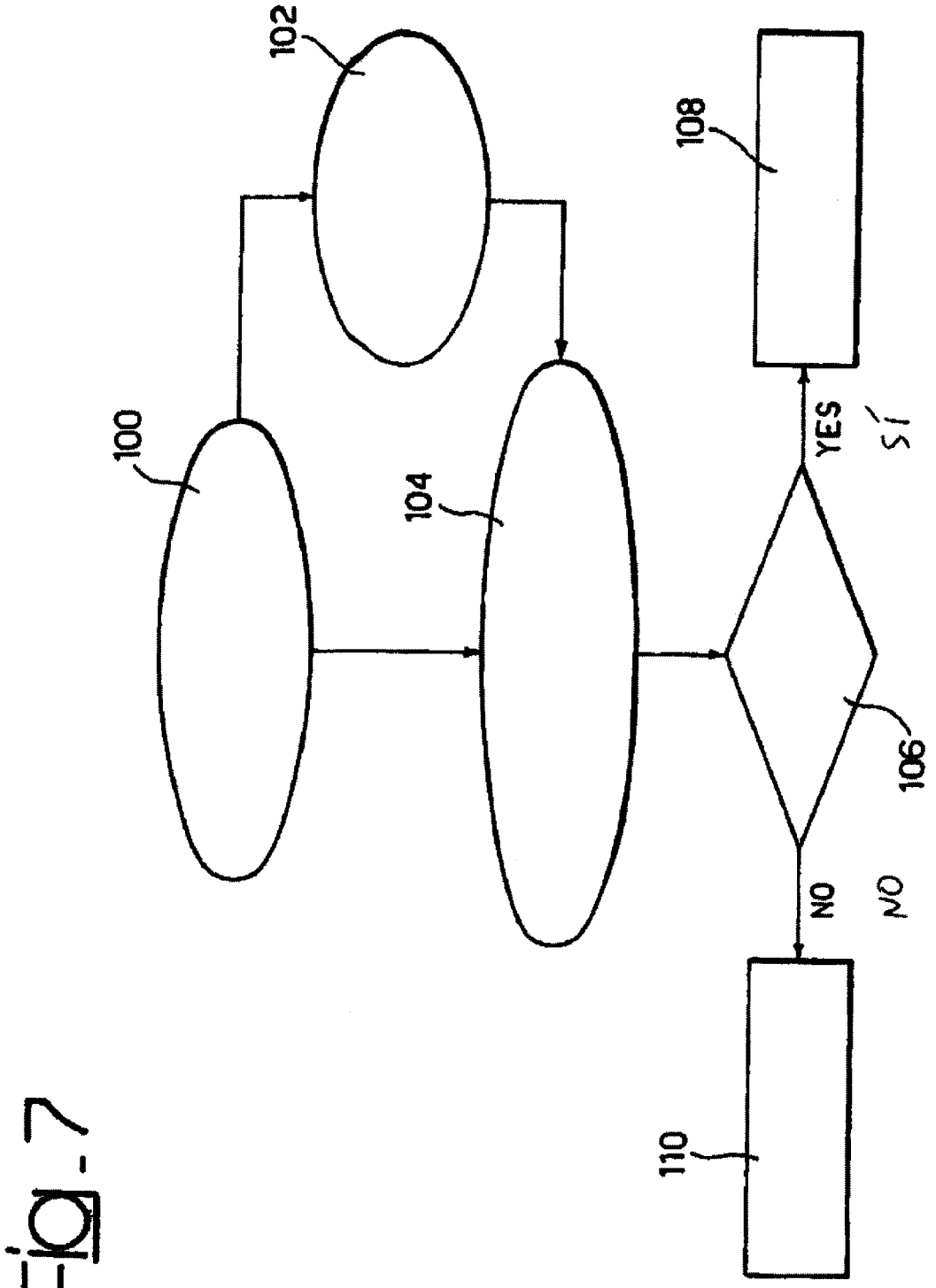


Fig. 7

Fig. 8

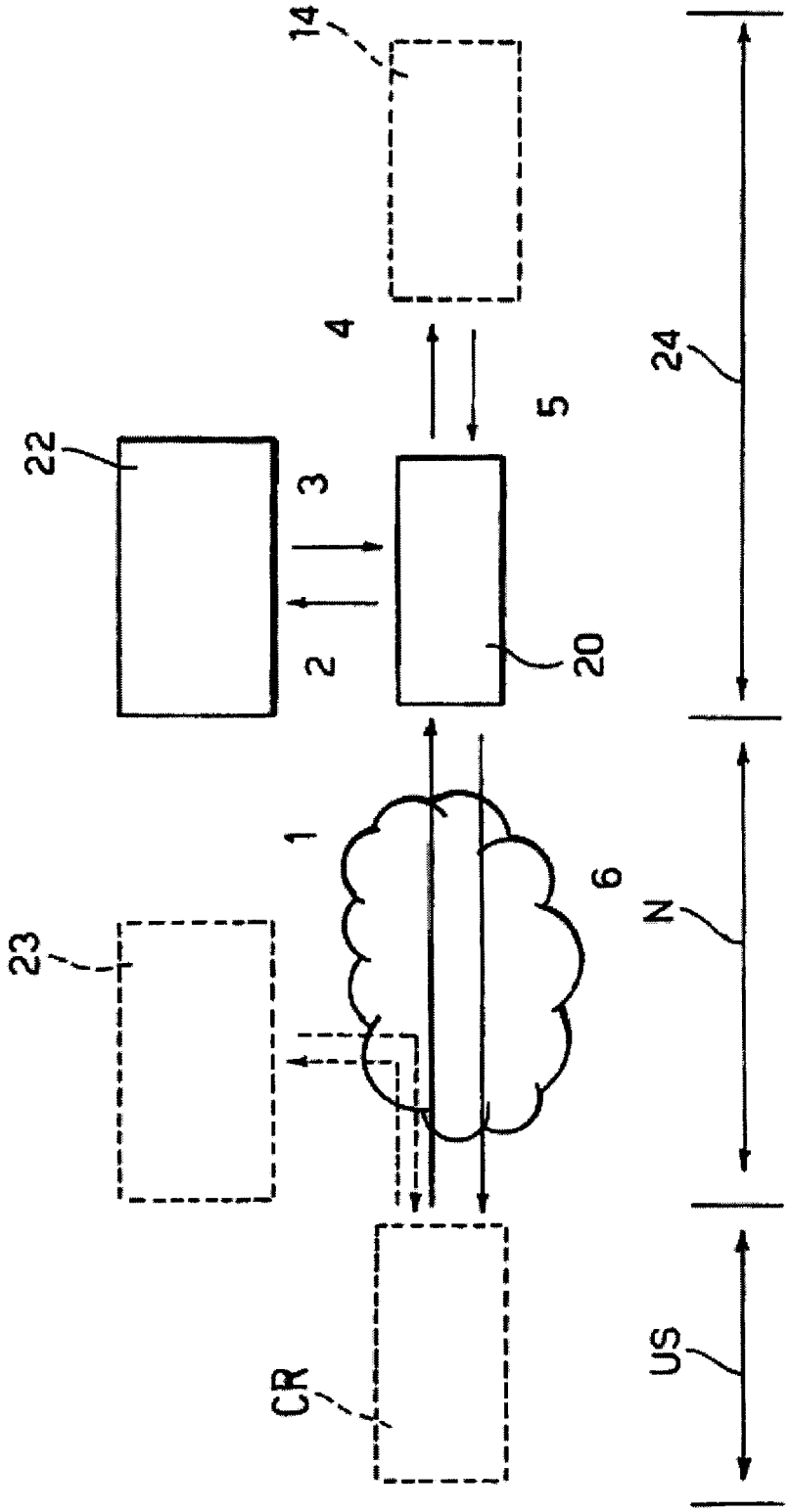


Fig.9

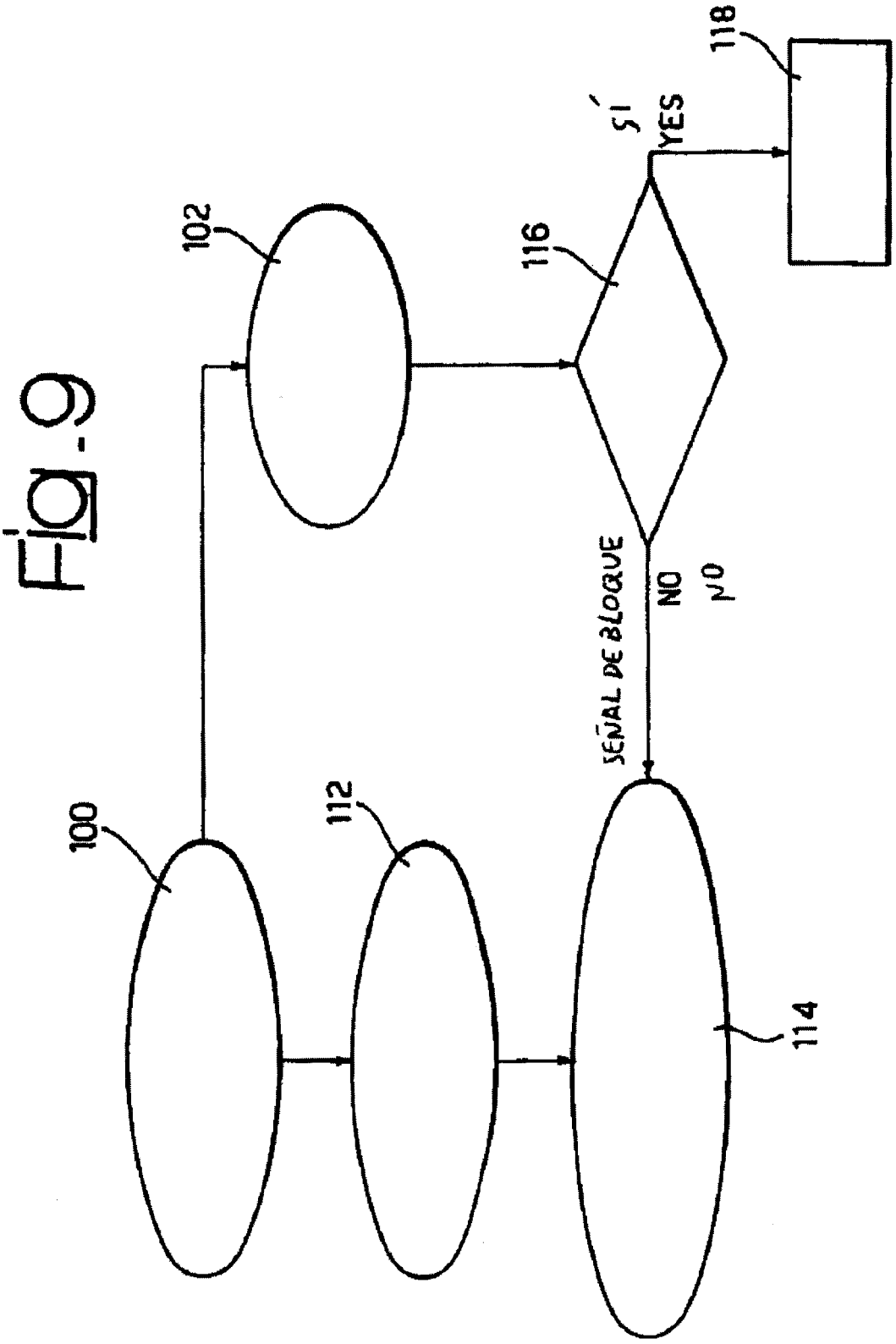
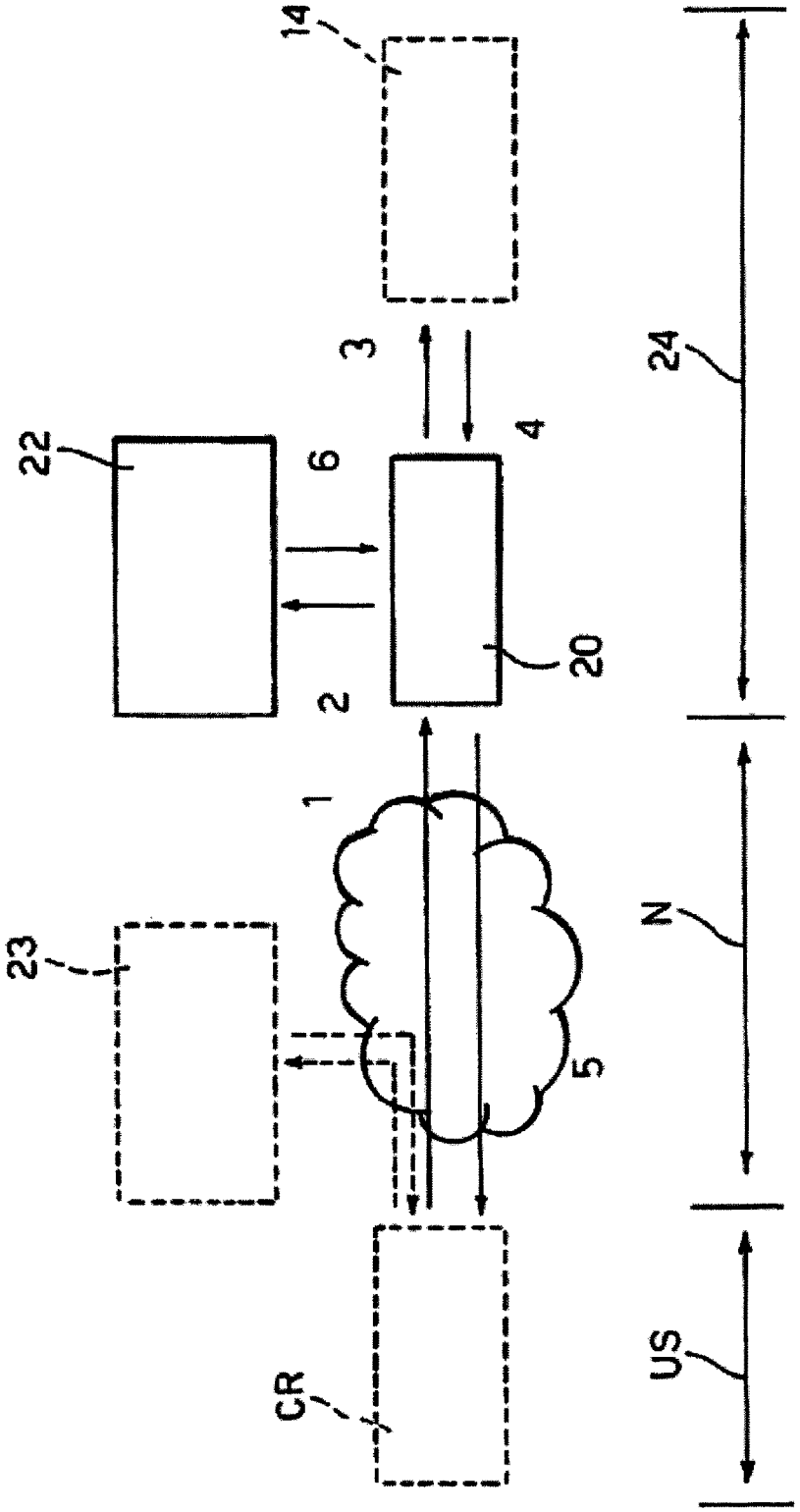


Fig. 10



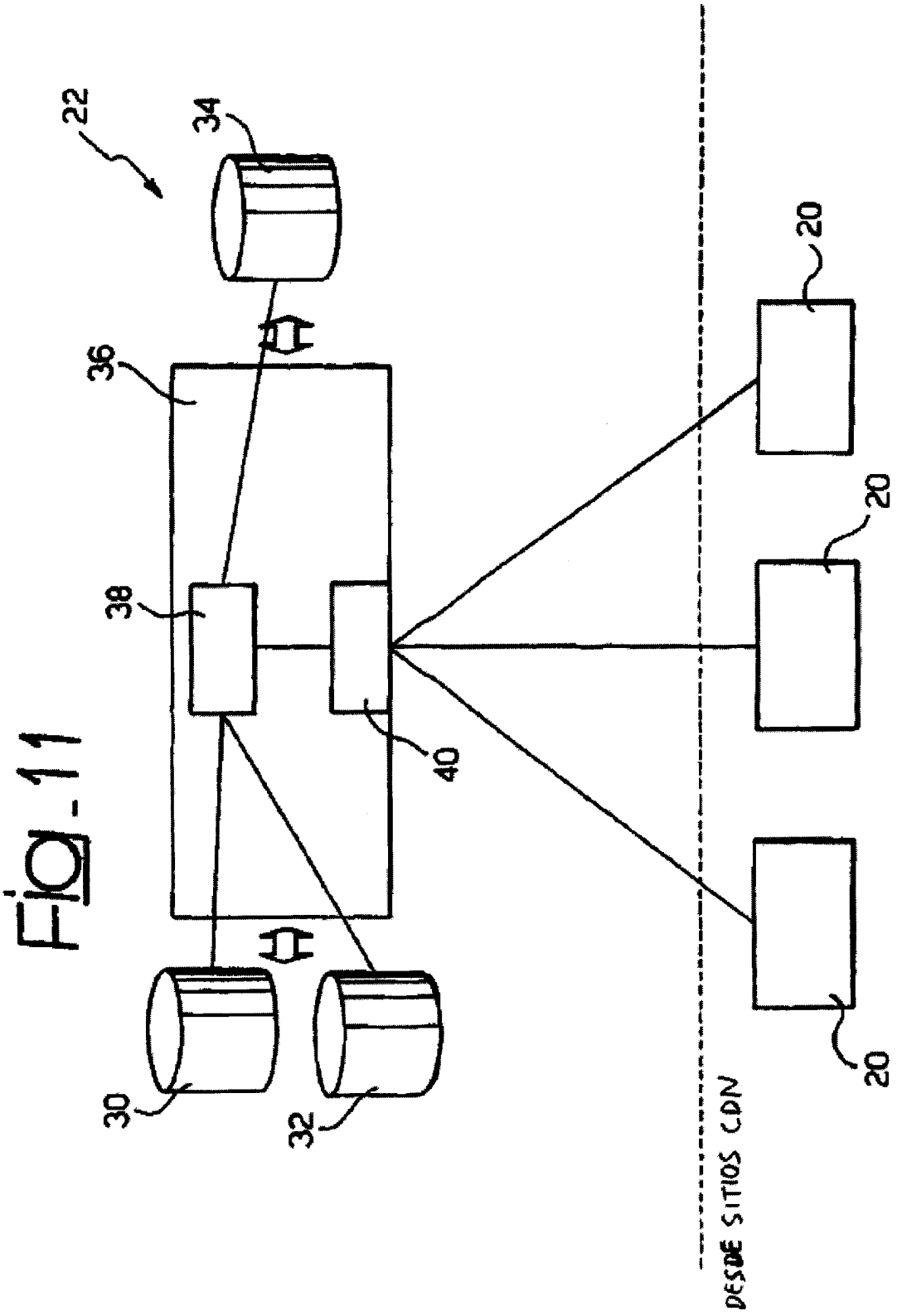


Fig. 11

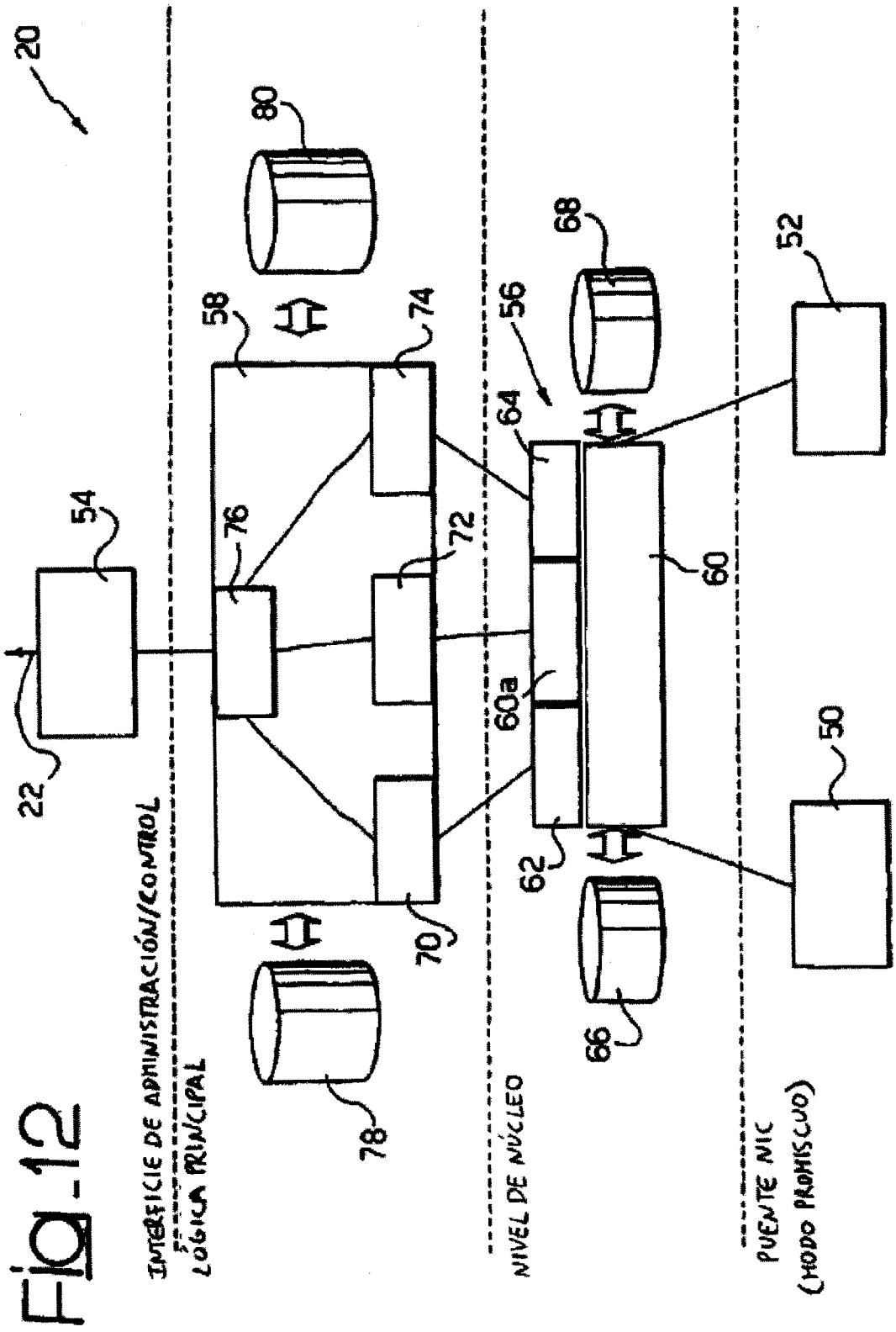

20
22
54
76
58
80
78
72
74
70
64
56
68
66
62
60
60a
52
50
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig-12

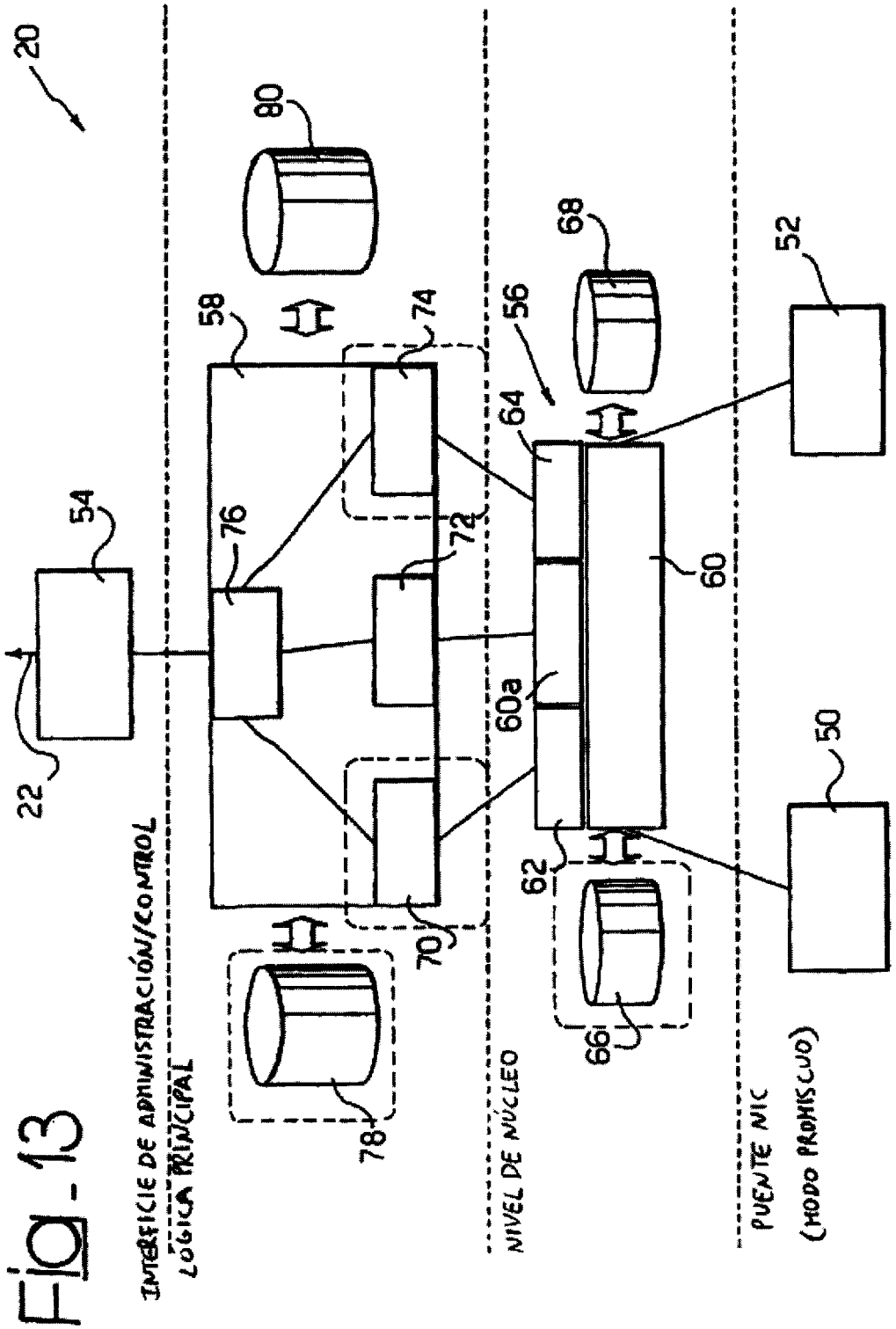

20
80
58
74
56
68
52
54
76
72
64
60
22
60a
50
62
70
66
78
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig. 13

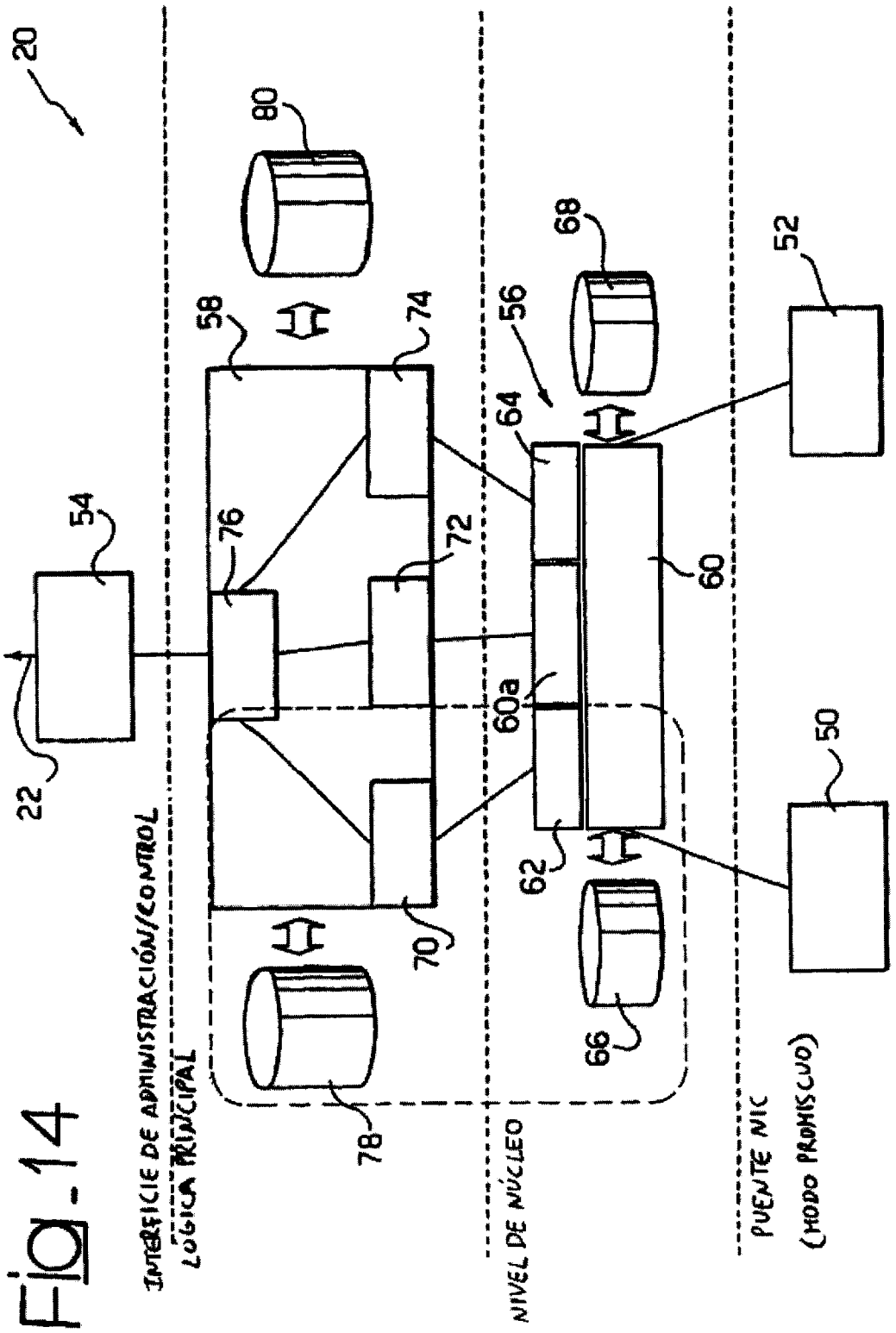

20
80
58
74
56
68
52
54
76
72
64
60
22
60a
50
62
70
66
78
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig. 14

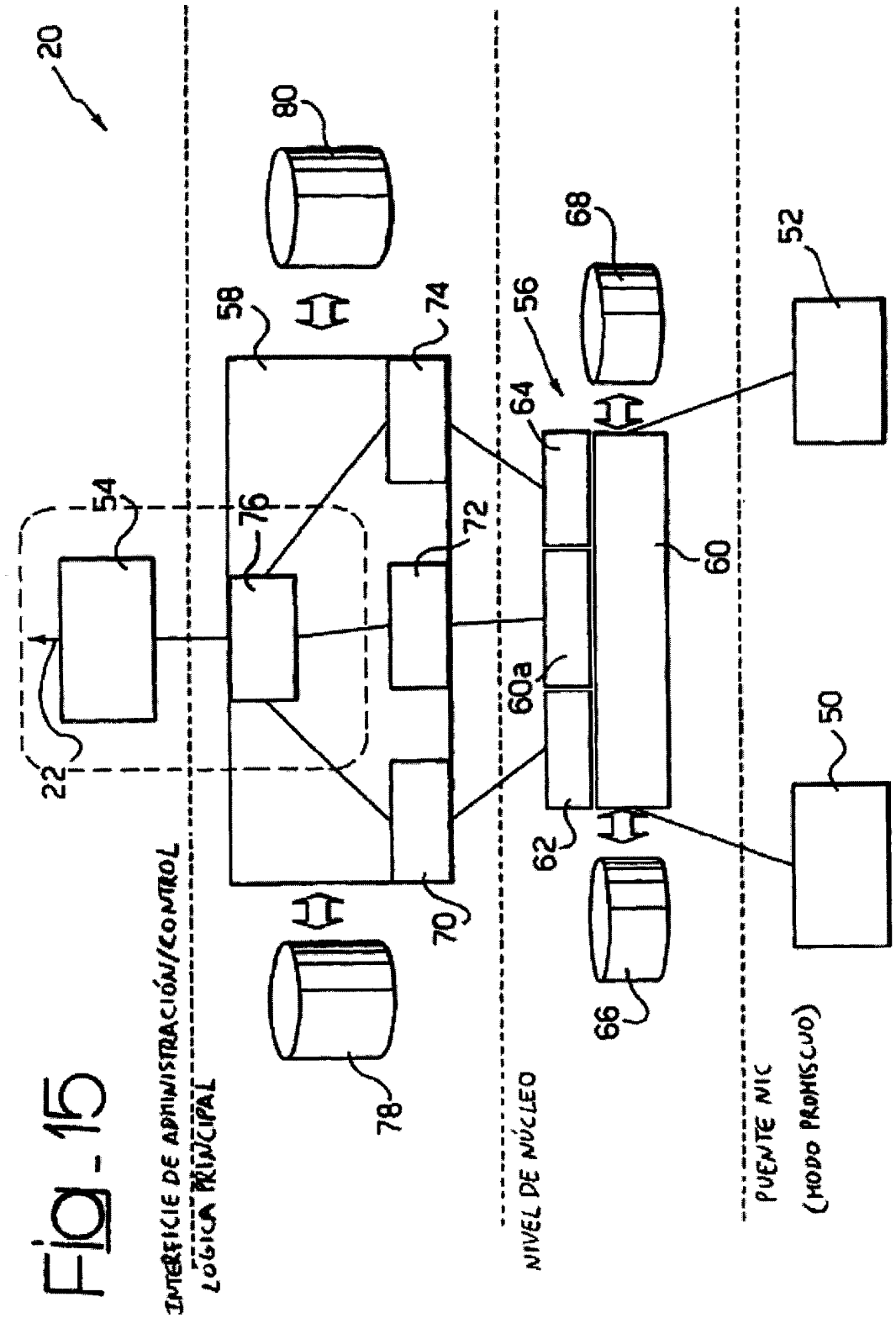

20
80
58
74
68
56
52
54
76
72
64
60
22
60a
50
62
70
66
78
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig. 15

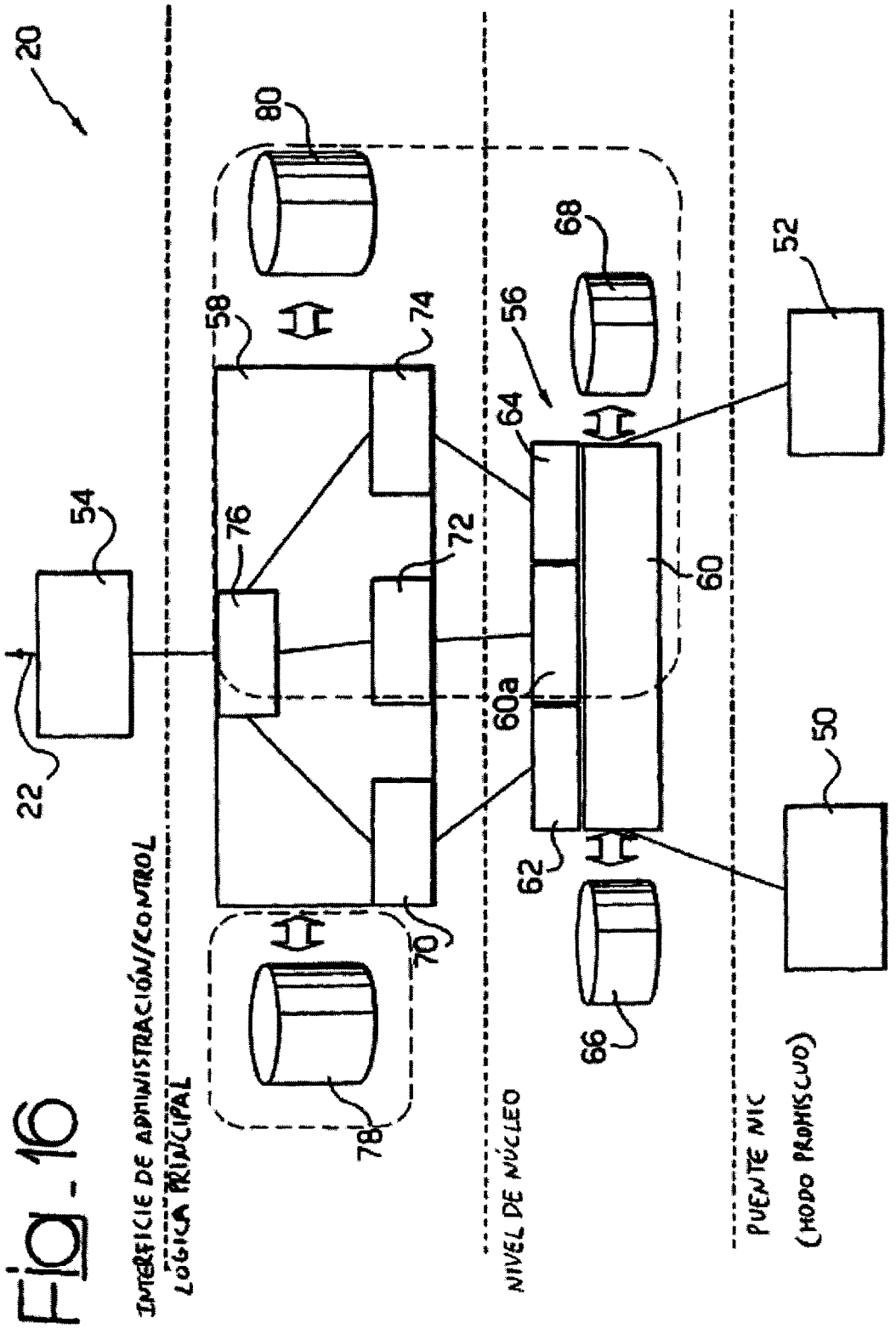

20
80
58
74
68
52
56
64
54
76
72
60
22
60a
50
62
70
66
78
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig. 16

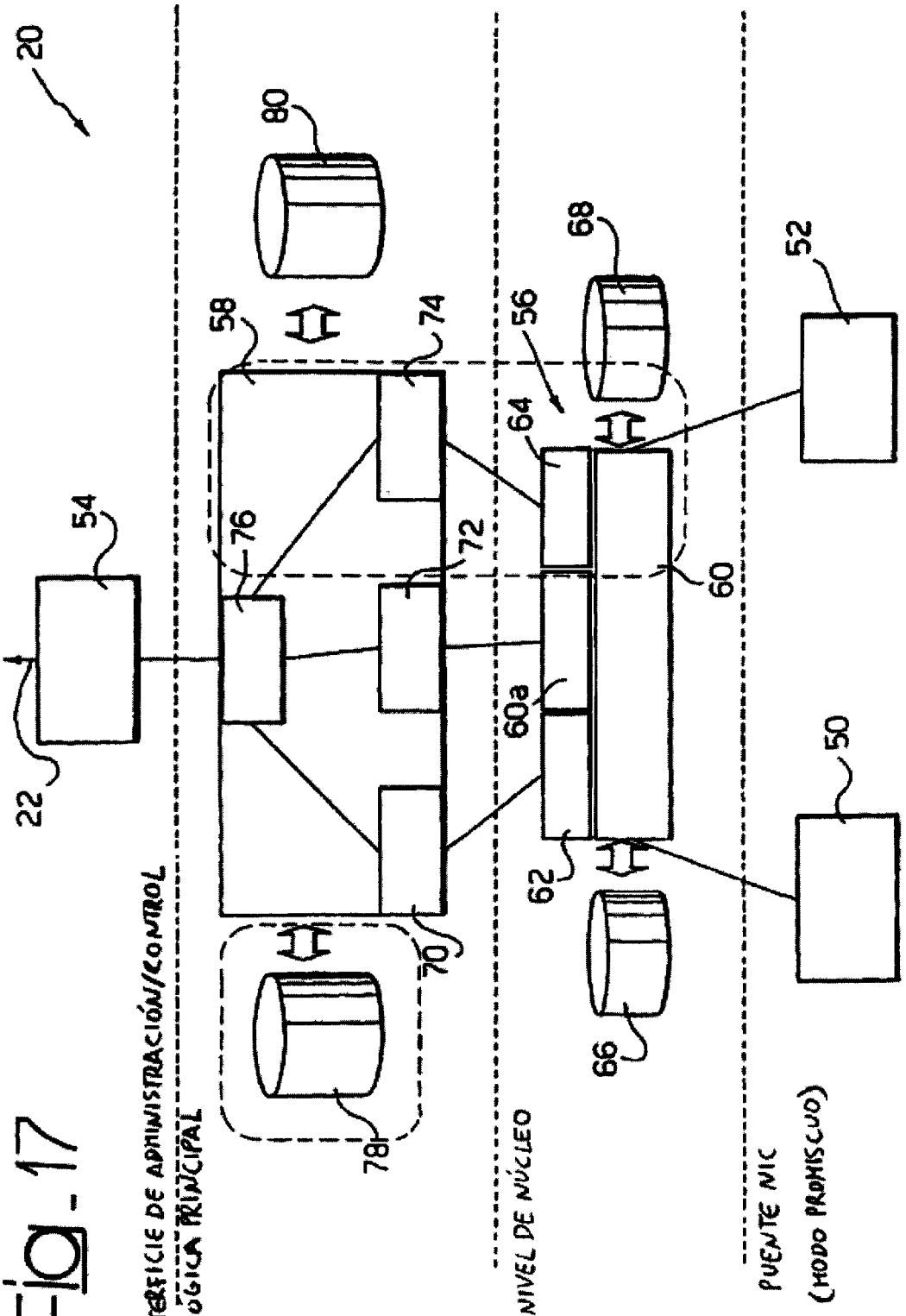
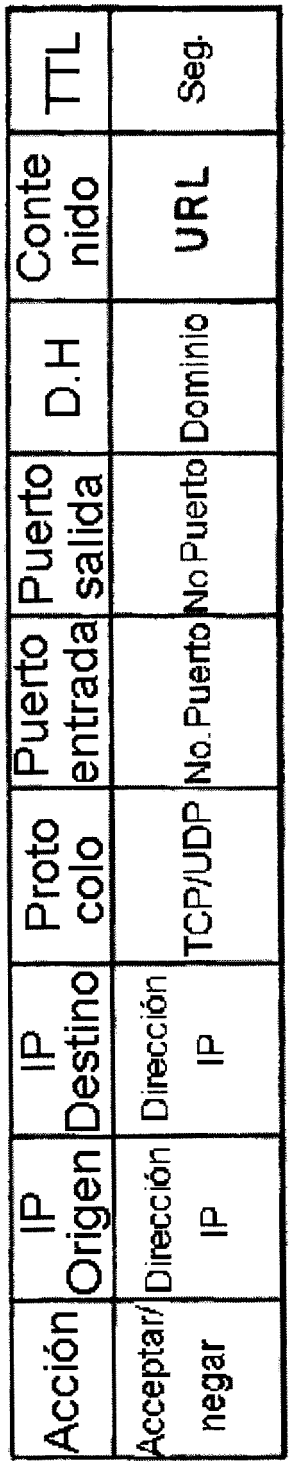

20
22
54
58
74
76
72
70
80
78
64
56
68
60
60a
62
66
52
50
INTERFICIE DE ADMINISTRACIÓN/CONTROL
LÓGICA PRINCIPAL
NIVEL DE NÚCLEO
PUENTE NIC
(MODO PROMISCUO)

Fig. 17

Fig. 18



Acción	IP Origen	IP Destino	Protocolo	Puerto entrada	Puerto salida	D.H	Contenido	TTL
Aceptar/negar	Dirección IP	Dirección IP	TCP/UDP	No. Puerto	No Puerto	Dominio	URL	Seg.

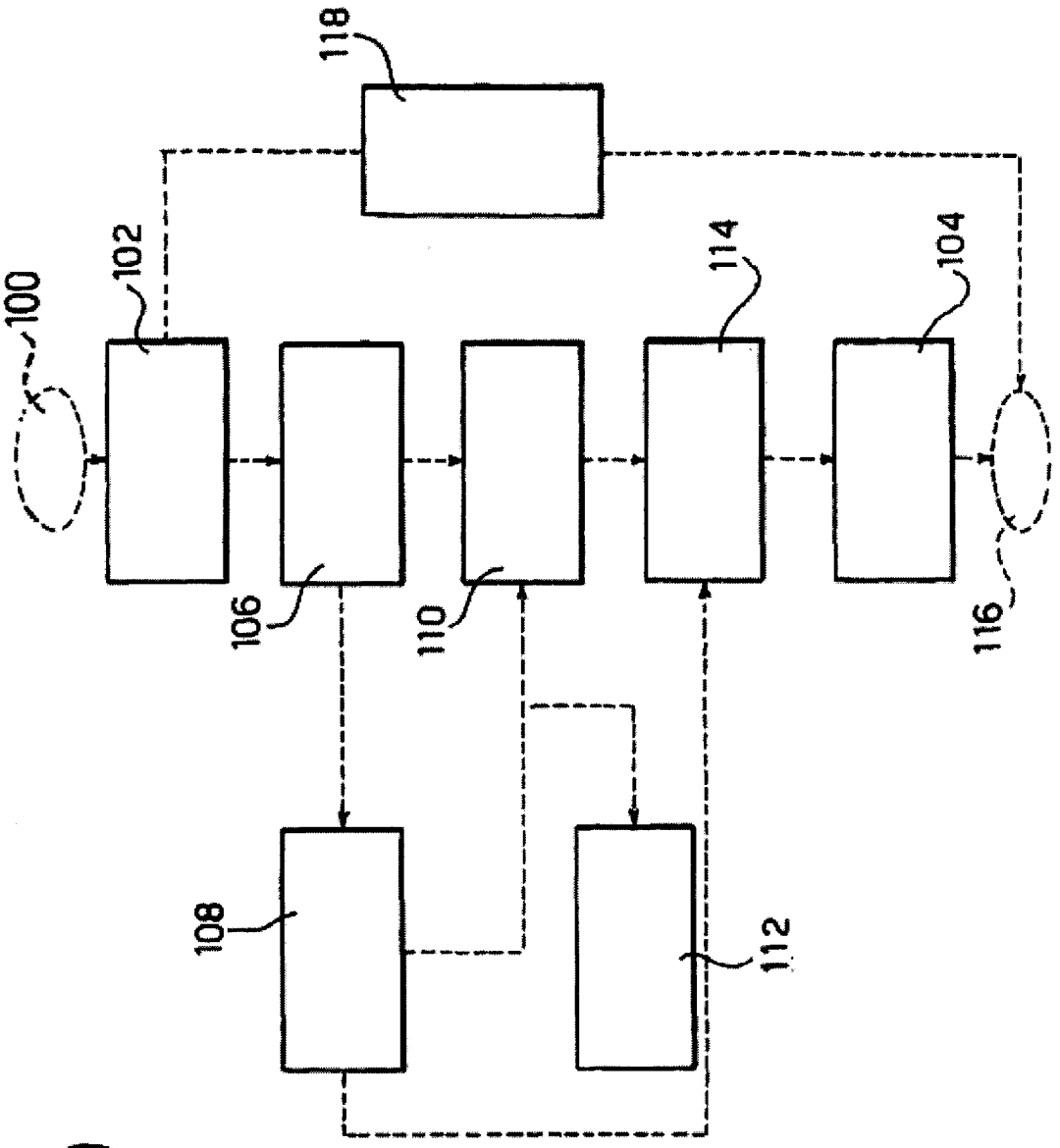
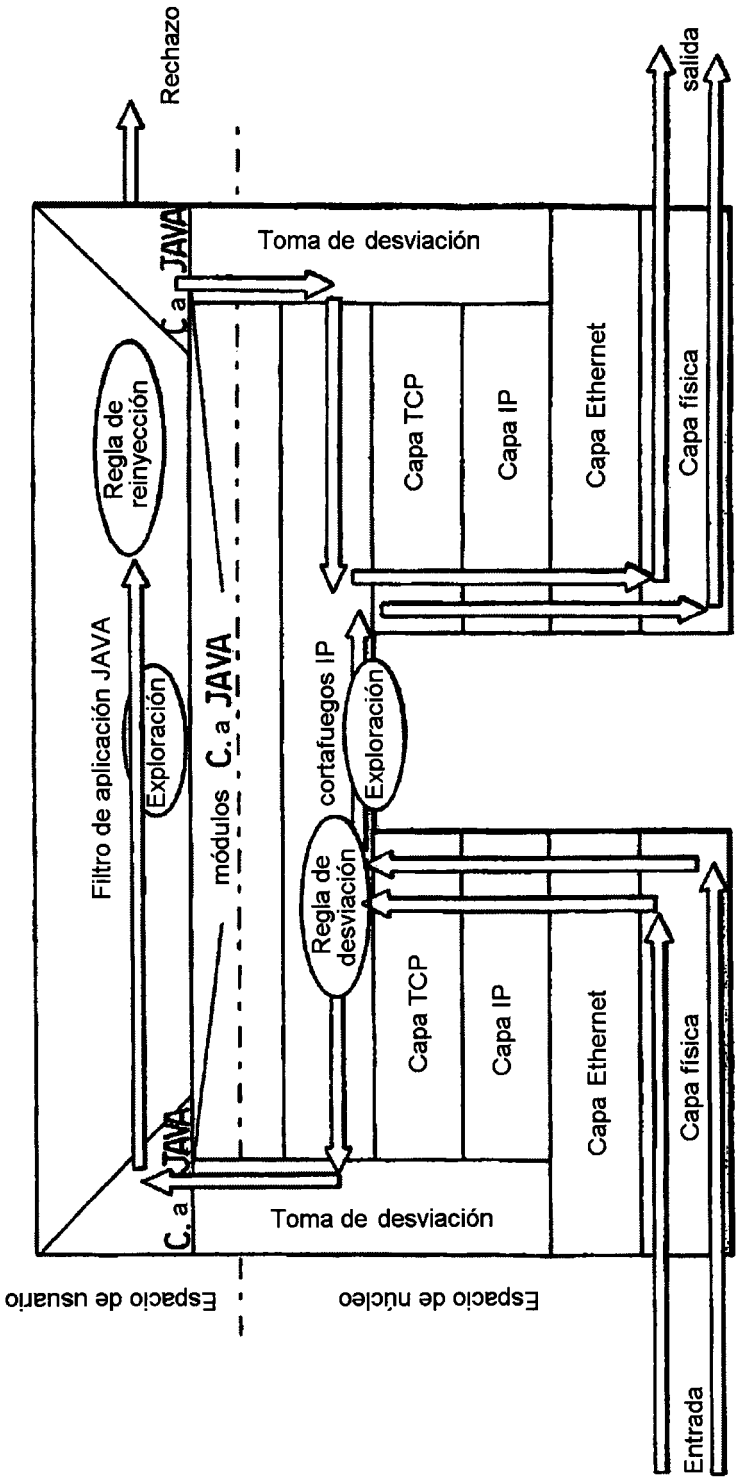


Fig. 19

Fig.20


Rechazo
salida
Toma de desviación
C. a JAVA
Regla de reinyección
Capa TCP
Capa IP
Capa Ethernet
Capa física
Filtro de aplicación JAVA
Exploración
módulos C. a JAVA
cortafuegos IP
Exploración
Regla de desviación
Capa TCP
Capa IP
Capa Ethernet
Capa física
C. a JAVA
Toma de desviación
Espacio de usuario
Espacio de núcleo
Entrada