

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 577 777**

51 Int. Cl.:

H04L 29/08 (2006.01)

H04L 12/835 (2013.01)

H04L 12/819 (2013.01)

H04L 12/823 (2013.01)

H04L 12/46 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **12.06.2012 E 12731618 (0)**

97 Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2721785**

54 Título: **Transferencia de datos**

30 Prioridad:

15.06.2011 GB 201110009

15.06.2011 EP 11275096

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

18.07.2016

73 Titular/es:

**BAE SYSTEMS PLC (100.0%)
6 Carlton Gardens
London SW1Y 5AD, GB**

72 Inventor/es:

**FOUNTAIN, JAMES GRAHAM;
EISSA, RANIA HAMDÍ y
HUDSON, PETER NOBLE**

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 577 777 T3

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

DESCRIPCIÓN

Transferencia de datos

La presente invención se refiere a la transferencia de datos.

5 Las redes de conmutación de paquetes se han considerado durante mucho tiempo como una manera de proporcionar sistemas, incluyendo sistemas de aviónica, con conectividad y anchos de banda muy grandes, evitando los cuellos de botella y las limitaciones asociadas con los protocolos de multiplexación por división de tiempo (TDM, time division multiplexing), tales como MIL-STD-1553B y STANAG 3910. Estos protocolos TDM comparten recursos de red mediante planificar transferencias consecutivamente, lo que requiere un nivel significativo de coordinación
10 entre los diferentes orígenes de datos. Esta coordinación de las transmisiones sobre la red no es generalmente un problema cuando la red está basada en un medio compartido. En este caso, puede ser utilizada una función de control centralizada, tal como un controlador de bus, para controlar todas las transmisiones y asegurar que no hay conflictos. Sin embargo, esta coordinación puede ser un problema muy importante en las redes de conmutación de paquetes. Esto se debe a que, en las redes de conmutación de paquetes, dicha función de control centralizada es difícil de implementar (y sería extremadamente restrictiva, si fuera posible), y la distribución de una función de este tipo requiere una sincronización ajustada de toda la red y, por lo tanto, limita severamente los mecanismos de planificación que pueden ser utilizados en un sistema de este tipo.

Una opción utilizada normalmente en los protocolos de redes comerciales de conmutación de paquetes, tal como Ethernet, es permitir a todos los usuarios transmitir en cualquier momento. Se utilizan entonces colas FIFO para almacenar tráfico en memoria tampón en los recursos compartidos siempre que las cargas sean temporalmente mayores de lo que puede asumir el recurso. Sin embargo, estas memorias tampón tendrán siempre una capacidad limitada para afrontar los picos de tráfico, debido a su tamaño finito. Por lo tanto, si se sobrecargan, es decir, los picos de tráfico son demasiado grandes o duran demasiado, el recurso se congestiona, la memoria tampón se desborda, y por consiguiente se pierden datos. Incluso cuando la memoria tampón no se desborda, se puede llenar tanto que el retardo a su través sea excesivo. Siendo, en general, ambas situaciones inaceptables en sistemas en tiempo real.

Un procedimiento conocido para impedir esta congestión es limitar los anchos de banda del tráfico que comparte los recursos y predecir la carga máxima o la utilización de la memoria tampón que esto provocará. A continuación se pueden comparar las previsiones con los tamaños reales de las memorias tampón para mostrar si es o no posible un desbordamiento, y el retardo provocado por esta utilización puede ser empleado para mostrar si las transferencias pueden o no retardarse demasiado.

El almacenamiento en memoria tampón introduce un retardo adicional que no se produce en los protocolos TDM; sin embargo, este retardo es muy pequeño en comparación con los retardos que se pueden producir en los orígenes cuando los recursos están compartidos mediante TDM, por ejemplo, cuando los datos esperan su ranura de tiempo de transmisión asignada, lo que puede llegar al intervalo de transmisión de los datos (por ejemplo, 20 ms para transferencias de datos de 50 Hz). Dado que, en las redes comerciales de conmutación de paquetes, los usuarios pueden transmitir en cuanto los datos están preparados, estas redes no sufren dichos retardos de transmisión.

El conocido protocolo ATM es, en muchos sentidos, adecuado para el transporte de datos en sistemas en tiempo real, dado que tiene todas las propiedades necesarias para encaminar el tráfico de manera determinista y limitar los anchos de banda. Esto permite predecir las cargas en recursos compartidos y los subsiguientes retardos. ATM realiza este encaminamiento utilizando canales virtuales (VCs, Virtual Channels), que son "conductos" orientados a la conexión que transportan los datos a lo largo de caminos deterministas. El mecanismo utilizado para limitar los anchos de banda en ATM es la compartición de tráfico basada en hardware en el origen, y la vigilancia del tráfico en la red: la vigilancia del tráfico en la red fija de manera efectiva el tamaño del conducto que es un VC, y la compartición del tráfico en el origen garantiza que el origen no intenta mandar demasiados datos en este conducto.

Aunque ATM puede proporcionar transferencia de datos determinista, no se ha difundido significativamente más allá de su nicho de mercado en las infraestructuras de telecomunicaciones, en parte debido a que la complejidad del hardware en las interfaces de red las hace considerablemente más costosas que las interfaces equivalentes Fast/Gigabit Ethernet. Al mismo tiempo, Ethernet es un protocolo de red de conmutación de paquetes de utilización mucho más generalizada, virtualmente ubicua, en el sector comercial. Por lo tanto, es deseable aprovechar la amplitud de componentes, tal como placas de procesador, etc., que incorporan ya interfaces para el protocolo Ethernet. Esto puede reducir los costes iniciales de los sistemas de aviónica y reducir los costes de titularidad reduciendo problemas de obsolescencia y facilitando mejoras de rendimiento, es decir, proporcionando mayores anchos de banda de la red.

55 Las redes Ethernet que tengan que transportar este tipo de datos deterministas, en algunos casos, existirán ya y estarán ya transportando tráfico no controlado o de mejor esfuerzo cuando surjan los requisitos de soportar transferencias de datos deterministas. Como resultado, los protocolos que permitan que una red de este tipo satisfaga requisitos de datos deterministas tendrán que ser aplicados después de su inicio; la única otra alternativa

sería contemplarlos inicialmente, por ejemplo con interfaces modificados/a medida, con la expectativa de que estos requisitos surjan en algunos datos posteriores. Por lo tanto, es importante que el proceso de actualizar una red existente tenga el mínimo impacto posible sobre el sistema y sobre el tráfico de mejor esfuerzo existente previamente, es decir, no debería ser necesario modificar subsistemas que no tengan que participar en estas nuevas transferencias. Adicionalmente, en algunos casos, será necesario demostrar la seguridad de los datos, es decir, que es auténtica y resistente a modificación o acceso no autorizado.

Puede haber ventajas significativas si los sistemas y subsistemas pueden utilizar más mecanismos de planificación avanzada que el ejecutivo cíclico, tal como planificación preferente basada en prioridades. Existen ventajas asimismo en sistemas que soportan reutilización del software, si se pueden realizar transferencias de datos a la frecuencia natural de la aplicación, que puede no estar relacionada armónicamente con otras frecuencias de aplicación. Por ejemplo, añadiendo una aplicación que tiene una frecuencia natural de 60 Hz a un sistema en el que la mayor parte de las aplicaciones funcionan a 50 Hz y subarmónicos de éstos, lo que es una tarea difícil cuando se utiliza planificación cíclica.

Por lo tanto, es deseable que cualquier transferencia de datos determinista utilice interfaces Ethernet estándar; permita transferencia de datos con requisitos de seguridad, fiabilidad y/o puntualidad; pueda ser aplicada a redes existentes con el mínimo impacto, es decir, permita que el tráfico no controlado, heredado, siga utilizando la red y soporte la máxima variedad posible de mecanismos de planificación, y pueda demostrar previamente que se satisfacen estos requisitos deterministas. Son requisitos opcionales la resistencia a fallos del sistema, es decir, sobre-transmisión por subsistemas, y a fallos de red, es decir, errores de los componentes de la red -conmutadores, interfaces de red y cables.

El documento US2006/002370 describe una arquitectura del plano de control/plano de transporte para controlar una red portadora formada por conmutadores Ethernet. Los conmutadores de borde de la portadora pueden estar separados lógicamente en una única función de núcleo de borde de proveedor (PE, Provider edge) y una o varias de borde de PE. La función de núcleo de PE puede ser utilizada para encapsular tráfico de Ethernet entrante procedente del cliente utilizando encapsulación tipo MAC y para reenviar el tráfico encapsulado a través de la red portadora. Las etiquetas VLAN se utilizan para proporcionar separación de clientes en el núcleo PE lógico, teniendo cada diferente sitio de cliente conectado a cada conmutador de borde una etiqueta VLAN única. El núcleo PE lógico de un conmutador de borde encapsula cada trama de Ethernet en otra trama de Ethernet utilizando la dirección MAC del conmutador de borde como la dirección de origen y la dirección MAC del punto de salida apropiado (la dirección de destino). En el núcleo PE del conmutador de borde, las tramas originales son despojadas de su encapsulación y enviadas sobre un enlace de comunicaciones por medio del borde PE del conmutador de borde a un conmutador de cliente. Cada conmutador, al recibir una trama de Ethernet en un puerto, difunde dicha trama de Ethernet en cada uno de los otros puertos. El proceso se repite a medida que la trama es recibida por otros conmutadores. De este modo, la trama se difunde a través de toda la red. Se proporciona la funcionalidad de autoaprendizaje de direcciones MAC para mejorar la eficiencia de la configuración en redes Ethernet conmutadas. Las tramas de Ethernet tienen direcciones MAC de origen y destino correspondientes a sus conmutadores Ethernet de origen y destino. Cuando una trama de Ethernet emitida por un conmutador de origen es recibida por un conmutador Ethernet receptor intermedio o de destino, el conmutador receptor observa el puerto en el que la trama se ha recibido y la dirección de origen de la trama. El conmutador receptor construye a continuación una tabla de reenvío para su utilización en la futura conmutación de tramas. La etiqueta VLAN definida en IEEE 802.1 q se aplica de tal modo que los conmutadores Ethernet de la red portadora están al tanto de la VLAN 802.1 q pero están configurados para utilizar una combinación de dirección de destino y etiqueta VLAN para reenviar tráfico de datos. Esto se consigue preferentemente reutilizando las capacidades existentes en cada conmutador Ethernet para almacenar tablas de reenvío independientes para cada etiqueta VLAN configurada, actuando la etiqueta VLAN como un mapeo (o indexación) para tablas de reenvío.

El documento WO2006/070197 da a conocer un esquema de comunicaciones para configurar una red que comprende una serie de aparatos de conmutación conectados, comprendiendo el esquema: determinar en un plano de control valores de campo de cabecera de índice para identificar tráfico sin conexión recibido en aparatos de conmutación para los que se debe establecer una conexión entre un nodo de origen y un nodo de destino; dotar a cada aparato de conmutación necesario para implementar una conexión, de información del plano de control, permitiendo dicha información alimentar las tablas de reenvío de datos de conmutación con dichos valores de campo de cabecera de índice en asociación con puertos de salida del aparato de conmutación; y desactivar cualquier otra funcionalidad en dicho aparato de conmutación que pueda alimentar las tablas de reenvío de datos con información de índice asociada con dichos puertos de salida del aparato de conmutación necesario para establecer dicha conexión. Las tablas de reenvío de los aparatos de conmutación están dotadas directamente de información de direcciones asociada con puertos salientes de los aparatos de conmutación. En algunas realizaciones, el plano de control alimenta las entradas en la tabla de reenvío con, por lo menos, otro campo de cabecera Ethernet además del campo de dirección de destino, y asocia además una VLAN con un puerto saliente, o de salida del conmutador. Este ID de la VLAN se utiliza para extinguir entre múltiples trayectorias a través de la red de comunicaciones.

El documento US2005/157737 describe una red que incluye un nodo de borde configurado para definir comportamientos por salto, utilizando un conjunto de bits en una cabecera Ethernet de una trama, y un nodo central configurado para recibir la trama y para reenviar la trama de acuerdo con los comportamientos por salto.

El documento US 7 369 495 se refiere a un procedimiento y un dispositivo de red para compartir ancho de banda entre un grupo de clases de tráfico para una interfaz. El ancho de banda se puede asignar, por lo menos, a una clase de tráfico de una primera prioridad para la interfaz. Por lo menos parte del ancho de banda no utilizado de dicha por lo menos una clase de tráfico puede ser asignado, por lo menos, a otra clase de tráfico de una segunda prioridad para la interfaz.

En el documento US2003/0154259 se dispone un servicio VPN a través de una infraestructura de red compartida que comprende una serie de dispositivos de borde de proveedor interconectados que tienen interfaces de borde de cliente. Algunos de los interfaces CE están asignados a un VPN que soporta una serie de redes de área local virtuales (VLANs, virtual local area networks) y están dispuestos para intercambiar unidades de datos de tráfico con dispositivos CE. Cada unidad de datos de tráfico incluye un identificador VLAN. Se establece por lo menos una conexión virtual en la infraestructura de red compartida entre dos interfaces CE de dispositivos PE diferentes, asignados a dicho VPN, para reenviar dichas unidades de datos de tráfico incluyendo un identificador VLAN. Dicha conexión virtual (VC, virtual connection) tiene un identificador determinado a partir de dicho identificador VLAN, y un identificador de dicha VPN.

El documento US2004/0213254 da a conocer un procedimiento para dar servicio a extremos de abonado utilizando LAN virtual en ATU-R (ADSL Termination Unit - Remote, unidad de terminación ADSL -remota) de ADSL, que utiliza VLAN para generar una serie de conexiones virtuales en una conexión ADSL, acopla equipos de cada extremo de abonado a una serie de puertos de entrada/salida (I/O) de abonado en ATU-R, añade una central de conmutación en la ATU-R para identificar datos etiquetados en las conexiones virtuales, conecta cada extremo de abonado en las conexiones virtuales con la central de conmutación a través de Ethernet, y asigna cada puerto I/O de abonado en la central de conmutación a una de las conexiones virtuales con una etiqueta diferenciadora.

Ninguna de las publicaciones de patente mencionadas en lo anterior propone específicamente designar un dispositivo informático como el único origen de datos sobre VC en una red del mismo modo que la presente invención, y por lo tanto no resuelve los problemas técnicos relacionados con la seguridad y la congestión que se describen en la presente memoria.

Las realizaciones de la presente invención están destinadas a solucionar por lo menos algunos de los problemas explicados anteriormente y proporcionan a la transferencia de datos requisitos de fiabilidad, puntualidad, seguridad y/o tolerancia a fallos, a través de una red Ethernet de conmutación de paquetes, en paralelo con datos ordinarios, de mejor esfuerzo, y utilizando interfaces de red Ethernet estándar. Las realizaciones pueden utilizar VCs para un transporte fiable, seguro y/o puntual de datos sobre una red Ethernet gigabit conmutada de dúplex completo que utiliza el protocolo de red de área local virtual (VLAN) para identificar los VCs y el protocolo de clase de servicio (CoS, Class of Service) para separar los datos de estos VCs respecto de otros datos que no tienen dichos requisitos. Las realizaciones pueden ser utilizadas para demostrar a un cliente o a un organismo de certificación que las transferencias de datos entre interfaces Ethernet estándar en una red Ethernet conmutada satisfarán siempre sus requisitos de seguridad (el emisor puede confiar en que los datos van sólo a donde deberían, y el receptor puede confiar en que estos proceden solamente de donde deberían), fiabilidad (que los datos no se perderán debido a las consecuencias de otro tráfico, es decir, no puede haber congestión, en la red) y/o puntualidad (que los datos llegan dentro de un plazo límite especificado, con respecto a su tiempo de transmisión).

De acuerdo con un primer aspecto de la presente invención, se da a conocer un sistema de transferencia de datos que incluye:

por lo menos un dispositivo de conmutación configurado, durante su utilización, para transferir datos, directa o indirectamente, entre una serie de dispositivos informáticos,

en el que dicho por lo menos un dispositivo de conmutación está configurado para proporcionar una serie de VLAN dentro de las cuales se puede configurar un canal virtual (VC) por medio de datos de VC transmitidos como tramas de Ethernet etiquetadas con una etiqueta VLAN,

siendo encaminados los datos de VC a través de dicho por lo menos un dispositivo de conmutación, de acuerdo con un campo de ID de VLAN de la etiqueta VLAN de dicha trama; caracterizado porque cada una de dichas VLAN está configurada como un respectivo VC al recibir datos de VC desde un dispositivo informático designado como el único origen de datos de VC sobre el VC respectivo, y porque se determina un encaminamiento fijo y predeterminado de la trama mediante la configuración de dicho por lo menos un dispositivo de conmutación.

En realizaciones que comprenden una serie de dichos dispositivos de conmutación, cada uno de dichos dispositivos de conmutación puede utilizar troncalizado de VLAN para permitir la transmisión sobre, y la recepción desde una serie de VLAN, permitiendo de ese modo que se conecten juntos dicha serie de dispositivos de conmutación. En este caso, la etiqueta VLAN de una de dichas tramas se introduce o se retira externamente de dicho por lo menos un dispositivo de conmutación.

Una mencionada etiqueta VLAN puede utilizar cualquier valor de ID de protocolo de etiqueta (TPID, Tag Protocol ID) disponible y puede designar por lo menos uno de dichos dispositivos informáticos diferente a dicho único dispositivo informático de origen como por lo menos un destino para los datos de VC. Alternativamente, cuando los datos de VC

tienen requisitos de seguridad, el VC se puede limitar a dicho dispositivo informático designado como único destino para los datos de VC (con el fin de evitar que los destinos reciban datos espurios de destinos diferentes, con fallos o maliciosos, tal como puede ocurrir en las VLAN convencionales).

5 En las salidas de dicho por lo menos un dispositivo de conmutación, los VCs se pueden asignar a una memoria tampón de VC y encaminarse a través de la misma. El encaminamiento a través de la memoria tampón de VC puede ser por medio del protocolo CoS descrito en IEEE 802.1d, y compañía. Se puede utilizar un punto de código de prioridad (PCP, Priority Code Point) en la etiqueta VLAN con el fin de identificar los datos de VC para encaminamiento a través de la memoria tampón de VC. La memoria tampón deberá recibir prioridad sobre todas las demás memorias tampón asociadas con la salida de un mencionado dispositivo de conmutación, de tal modo que no se transmita ningún otro tráfico (por ejemplo, no crítico) desde la salida cuando la memoria tampón de VC contiene alguna trama de datos Ethernet.

10 Cada mencionado VC será asignado a un ancho de banda máximo. Dicho por lo menos un dispositivo de conmutación puede utilizar mensajes de control de tráfico que limitan cada mencionado VC individualmente a su mencionado ancho de banda máximo asignado, por ejemplo, retardando y/o rechazando cualquier tráfico que exceda este límite (determinado, por ejemplo, por llegar demasiado cerca de la trama anterior del mismo VC, en base al ancho de banda y a la fluctuación tolerada para dicho VC). Esto se puede realizar, por ejemplo, utilizando los conocidos algoritmos de cubo de permisos ("token bucket") o de cubo con fugas ("leaky bucket").

15 A continuación se puede calcular un nivel máximo de llenado para cada una de las mencionadas memorias tampón de VC, y el nivel máximo de llenado se puede comparar con tamaños reales de las memorias tampón para evitar, o reducir la probabilidad de congestión dentro de, o entre las memorias tampón asignadas a los VCs. Los retardos extremo a extremo para los VCs se pueden asimismo calcular, utilizando los niveles de llenado para las memorias tampón a través de las cuales son encaminados, y comparar con cualesquiera requisitos de plazo límite para los VCs.

20 Dicho por lo menos un dispositivo informático puede comprender, por ejemplo, unidades de aviónica reemplazables en línea (LRUs, Avionic Line Replaceable Units).

Normalmente, las VLAN comprenderán VLAN IEEE 802.1q. La serie de conmutadores estarán configurados normalmente para proporcionar una red Ethernet gigabit conmutada de dúplex completo IEEE 802.3.

25 De acuerdo con otro aspecto de la presente invención, se da a conocer una red de comunicaciones que incluye un sistema de transferencia de datos sustancialmente tal como se describe en la presente memoria, que incluye por lo menos un dispositivo de conmutación y una serie de dichos dispositivos informáticos.

De acuerdo con otro aspecto de la presente invención, se da a conocer un procedimiento para proporcionar transferencia de datos entre dispositivos informáticos, incluyendo el procedimiento:

30 configurar por lo menos un dispositivo de conmutación, en uso, para transferir datos, directa o indirectamente entre una serie de dispositivos informáticos, en el que dicho por lo menos un dispositivo de conmutación está configurado para proporcionar una serie de VLAN dentro de la cual se puede configurar un canal virtual (VC) por medio de datos de VC transmitidos como tramas de Ethernet etiquetadas con una etiqueta VLAN,

35 siendo encaminados los datos de VC a través de dicho por lo menos un dispositivo de conmutación, de acuerdo con un campo de ID de VLAN de la etiqueta VLAN de dicha trama; caracterizado porque cada una de dichas VLAN está configurada como un respectivo VC al recibir datos de VC desde un dispositivo informático designado como el único origen de datos de VC sobre el VC respectivo, y porque se determina un encaminamiento fijo y predeterminado de la trama mediante la configuración de dicho por lo menos un dispositivo de conmutación.

40 Aunque la invención se ha descrito en lo anterior, se extiende a cualquier combinación inventiva de características expuestas en lo anterior o en la siguiente descripción. Si bien en la presente memoria se describen en detalle realizaciones ilustrativas de la invención haciendo referencia a los dibujos adjuntos, se debe entender que la invención no se limita a estas realizaciones precisas. Siendo así, resultarán evidentes para los expertos en la materia muchas modificaciones y variaciones. Además, se contempla que una característica particular descrita ya sea individualmente o como parte de una realización, se pueda combinar con otras características descritas individualmente, o con partes de otras realizaciones, incluso si dichas otras características y realizaciones no hacen mención a la característica particular. Por lo tanto, la invención se extiende a dichas combinaciones específicas no descritas.

45 La invención se puede llevar a cabo de diversas maneras y, solamente a modo de ejemplo, se describirán realizaciones de la misma, haciéndose referencia a los dibujos adjuntos, en los cuales:

la figura 1 muestra esquemáticamente una red de comunicaciones que incluye una serie de dispositivos de conmutación configurados para transferir datos entre una serie de dispositivos informáticos, y

55 la figura 2 muestra el formato de una trama de Ethernet.

Haciendo referencia a la figura 1, se muestra un sistema de comunicaciones que incluye un conjunto de dispositivos de conmutación 102A - 102C. Cada dispositivo de conmutación está conectado a por lo menos un dispositivo informático 104A - 104F, que puede ser un dispositivo informático convencional, por ejemplo unidades de aviónica reemplazables en línea (LRU), y puede ser configurable para actuar como un equipo anfitrión en red. Los componentes del sistema se utilizan para proporcionar una red Ethernet gigabit conmutada de dúplex completo IEEE 802.3, en la que se utilizan una serie de VLANs, tal como se describe en IEEE 802.1 q, y compañía, como VCs para la transferencia de datos. Los equipos anfitriones en este sistema pueden, mediante la utilización de troncalizado VLAN, estar capacitados para la transmisión y recepción desde una serie de VLAN.

Una VLAN está configurada como un VC con un origen de datos críticos de entre los dispositivos informáticos 104. Estos datos son transmitidos en la forma de tramas de Ethernet etiquetadas con una etiqueta VLAN, que puede utilizar cualquier valor TPID disponible. El VC puede tener una serie de destinos para estos datos. Sin embargo, cuando los datos tienen requisitos de seguridad, el VC se puede limitar a un único destino entre los dispositivos informáticos 104 para evitar que los destinos reciban datos espurios desde orígenes diferentes, con fallos o maliciosos, tal como puede ocurrir en las VLAN. Estos VCs/VLANs, son encaminados por medio de uno o varios dispositivos de conmutación 102 en su ID de VLAN (que está contenida dentro de la etiqueta VLAN, tal como se explica a continuación) y tienen caminos fijos y predeterminados. La predeterminación de los caminos está contenida dentro de la configuración de dichos uno o varios dispositivo de conmutación.

Se pueden transferir datos críticos sobre estos VCs solamente desde el origen autorizado y solamente a los destinos autorizados. Sin embargo, esto aplicará solamente cuando la configuración de los conmutadores de red sea adecuadamente segura. Específicamente, la configuración del conmutador o conmutadores a través de los cuales se encaminan los VCs deben estar limitadas para evitar ataques de salto VLAN, por ejemplo, doble etiquetado y suplantación del conmutador, y puede ser modificada solamente por medios autorizados. Es probable que los límites en las configuraciones incluyan requisitos tales como que ninguna salida del conmutador mediante la cual son encaminados uno o varios VCs puede retirar etiquetas VLAN. Es probable que los límites sobre los medios de configuración incluyan, por ejemplo, que no se pueda utilizar el protocolo de troncalizado dinámico o el protocolo de registro de VLAN múltiple para modificar las VLAN que se utilizan como VCs (lo que impide que los VCs con datos críticos sean objeto de ataques de suplantación del conmutador), y los procedimientos de configuración de los conmutadores para las VLAN utilizadas de este modo deben ser adecuadamente seguros. Puede existir asimismo el requisito de que las interfaces de equipos anfitriones que reciben estos datos críticos sobre VCs de VLAN reciban solamente tramas de Ethernet que están etiquetadas con etiquetas VLAN, incluyendo cualesquiera datos no críticos que puedan tener que recibir, donde las VLAN utilizadas para los datos no críticos serán de menor prioridad (tendrán un valor PCP menor) que las de datos críticos (lo que evitará que las salidas de conmutador conectadas a estos equipos anfitriones tengan que retirar etiquetas VLAN por defecto desde datos no críticos, e impide por lo tanto que los equipos anfitriones y los VCs de datos críticos sean objeto de ataques de doble etiquetado).

Para los VCs que están configurados con un único origen y un único destino, las limitaciones sobre cómo son encaminados los VCs a través del conmutador o conmutadores, es decir, utilizando el ID de VLAN, asegurarán que los datos recibidos por el destino deben proceder del origen previsto: no se permitirá que las tramas que contienen el ID de VLAN correcto que son transmitidas por equipos anfitriones diferentes, erróneos o maliciosos, se unan a este VC, en virtud de no haber datos de encaminamiento suministrados al conmutador para las entradas a las que están conectados dichos equipos anfitriones erróneos o maliciosos. Por lo tanto estos VCs son, exceptuando circunstancias que implican fallos en los conmutadores de red y/o en el esquema de protección de datos incorporado en el estándar Ethernet, inmunes a ataques de suplantación de datos.

Los dispositivos de conmutación 102 pueden ser conmutadores centrales y conmutadores de subsistemas, que satisfacen los requisitos básicos de soporte para IEEE 802.1 q (incluyendo troncalizado VLAN), y para IEEE 802.1p, que permiten por lo menos dos niveles de prioridad con memorias tampón independientes para cada uno, y teniendo la memoria tampón de tráfico de alta prioridad, prioridad simple sobre la inferior. Las especificaciones del soporte de IEEE 802.1 q son que los conmutadores tienen que ser configurables de tal modo que las tramas que lleguen a un puerto desde el equipo anfitrión conectado etiquetadas con una ID de VLAN específica, sean encaminadas solamente a un subconjunto de los otros puertos del conmutador. En el caso ideal, el conjunto de puertos a los que se encamina un ID de VLAN dado se debería especificar en cada entrada, es decir, el ID de puerto incrementa el ID de VLAN. Sin embargo, en común con la utilización normal de VLAN en redes COTS (commercial off the shelf, disponibles en el mercado), es aceptable que la asociación se realice configurando estos otros puertos para que tengan estas tramas encaminadas a los mismos. Siendo la diferencia que el primer procedimiento permitiría una reutilización limitada de IDs de VLAN dentro de un conmutador.

Los dispositivos de conmutación 102 tienen asimismo que ser configurables de tal modo que las tramas no etiquetadas que llegan a un puerto desde el equipo anfitrión conectado se puedan etiquetar internamente con un ID de VLAN por defecto/nativo específico para dicho puerto, y de tal modo que las tramas encaminadas internamente a éstos desde otros puertos que están etiquetados con un ID de VLAN por defecto/nativo, específico para dicho puerto, puedan ser despojadas de sus etiquetas antes de la retransmisión.

Los dispositivos de conmutación 102 proporcionan asimismo funcionamiento a velocidad de hilo, es decir, proporcionan un ancho de banda de conmutación central que es por lo menos igual a la suma de los anchos de

banda de entrada. Utilizan almacenamiento en memoria tampón compartido, centralizado, o memorias tampón de salida individuales, y utilizan conmutación de almacenamiento y reenvío. El funcionamiento a velocidad de hilo asegurará que no hay ningún almacenamiento en memoria tampón de entrada en los conmutadores que pueda conducir a un bloqueo de cabeza de línea. La utilización de memorias tampón compartidas/centralizadas o de salida permite que las utilizaciones de las memorias tampón sean calculadas y comparadas con los tamaños disponibles de las memorias tampón. El requisito de conmutación de almacenamiento y reenvío asegura que las tramas no son reencaminadas en IDs de VLAN corruptos, etc.

Los dispositivos de conmutación 102 se pueden configurar fuera de la plataforma, o fuera de banda mediante un único subsistema en la plataforma. Pueden asimismo ser configurados en banda mediante algún procedimiento adecuadamente seguro, por ejemplo el conocido protocolo simple de administración de red. En todos los casos, se desactivarán otros medios no utilizados de configuración de conmutadores, específicamente la configuración autónoma de VLAN y la vigilancia de tráfico, incluyendo DTP y MVRP, es decir, los VCs implementados mediante los procedimientos descritos en la presente memoria serán equivalentes a los denominados VCs permanentes (PVCs, Permanent VCs) utilizados en redes ATM en lugar de a los denominados VCs conmutados (SVCs, Switched VCs).

Los dispositivos de conmutación 102 se configuran para proporcionar implementaciones de Ethernet, de red de conmutación de paquetes de dúplex completo. Se apreciará que el sistema mostrado en la figura es sólo un ejemplo, y que el número y la disposición de dispositivos de conmutación e informáticos puede variar. Por ejemplo, la arquitectura más simple posible comprende una estrella, con cada equipo anfitrión 104 en red conectado a uno de los puertos de un solo dispositivo de conmutación (éste puede estar duplicado, por ejemplo, para redes redundantes). Cuando hay más equipos anfitriones para interconectar de los que pueden estar conectados oportunamente a un único conmutador, pueden ser utilizados múltiples conmutadores. Estos conmutadores se pueden conectar conjuntamente, para permitir a un equipo anfitrión conectado a uno comunicar con equipos anfitriones conectados a otro. Estos enlaces entre conmutadores pueden entonces limitar las transferencias, si existe la necesidad de un número significativo de conexiones entre equipos anfitriones en uno y equipos anfitriones en otros. Esto se puede simplificar utilizando conexiones de mayor ancho de banda para estos enlaces entre conmutadores, es decir, utilizando Ethernet de 10 gigabits en una red generalmente Ethernet gigabit.

Si están interconectados más de dos dispositivos de conmutación 102, esto puede entonces crear anillos: por ejemplo, A conecta con B, que conecta con C, que conecta con A, etc. Dichos anillos en un solo dominio de difusión, pueden hacer que el tráfico de difusión se regenere repetidamente y, generalmente, inundan la red. Una solución conocida es utilizar el protocolo rápido de árbol de expansión para detectar dichos bucles y desconectar uno de los enlaces en el bucle, rompiéndolo de ese modo e impidiendo la acumulación de datos de difusión. Para los VCs de VLAN descritos en la presente memoria, se supone que estarán configurados sin bucles o bien que se utilizará el protocolo de múltiples árboles de expansión para romper cualesquiera bucles formados. Éste puede ser asimismo un potencial procedimiento de implantación de redundancia de red, con la salvedad de que puede tardar por lo menos 3 segundos en reactivar un enlace si hubiera un fallo de capa física.

El sistema mostrado comprende componentes existentes del protocolo estándar Ethernet: utilización de controladores estándar de dispositivos y sistema operativo COTS, etc. Los presentes inventores han investigado los estándares Ethernet y han descubierto que aparentemente había un medio de implementar VCs ya presente en IEEE 802.1q: redes de área local virtuales (puente) (VLAN). Inicialmente, esto se consideró una manera de implementar un equivalente plenamente COTS del conocido protocolo AFDX utilizando el ID de VLAN en lugar del ID de VLink. Sin embargo, después de comprender que esto requeriría actualizar las redes existentes de tal modo que todo el tráfico utilizara VLAN, los inventores comprendieron que se podría utilizar la clase de servicio (CoS) IEEE 802.1p para permitir separar el tráfico en las VLAN respecto del tráfico de mejor esfuerzo así como entre éstos, si éste tráfico de mejor esfuerzo es asignado a una prioridad menor, o la tiene por defecto.

La figura 2 muestra el formato de una trama 200 etiquetada VLAN, que incluye una etiqueta VLAN 202 de 4 octetos. Las tramas de Ethernet transmitidas en una VLAN se identifican por un valor específico 204 del ID de VLAN de 12 bits en la etiqueta 202, que se introduce en la trama de Ethernet delante del campo Ethertype. Otro campo 206 PCP de 3 bits indica una de 8 clases de servicio. El indicador de formato canónico (CFI, Canonical Format Indicator) 208 de un solo bit no se utiliza en esta realización. Cierta pequeña cantidad de datos de soporte, por ejemplo, respuestas a solicitudes del protocolo de resolución de direcciones o del protocolo de descubrimiento de vecinos, pasarán/pueden pasar desde el destino o destinos al origen y ser etiquetados asimismo con el ID para la VLAN asociada con el VC.

Las VLAN convencionales fueron desarrolladas para interconectar grupos de equipos anfitriones como si estos, y solamente estos, estuvieran acoplados al mismo dominio de difusión, independientemente de su emplazamiento físico. Por lo tanto, una VLAN tiene los mismos atributos que una LAN física, pero permite que los equipos anfitriones se agrupen juntos lógicamente incluso si no están situados en el mismo conmutador de red. Varias de estas VLAN pueden compartir un mismo dominio físico, por ejemplo, estar conectadas al mismo conmutador físico, estando cada una aislada respecto de las otras. Los dispositivos de conmutación que soportan VLAN IEEE 802.1 q, hacen esto mediante un conjunto de conmutadores virtuales, uno para cada VLAN, estando asociados los puertos del conmutador físico con una serie de estos conmutadores virtuales de VLAN.

- Normalmente, los conmutadores que soportan VLAN transforman tráfico no etiquetado en una VLAN por defecto a su llegada, es decir, añaden una etiqueta que indica ID 1 de VLAN y, generalmente, retiran esta etiqueta en la transmisión. Pueden estar configurados asimismo para añadir una etiqueta con un valor diferente de ID de VLAN en un puerto, encaminar solamente VLAN con esta etiqueta a dicho puerto, y retirarlas en la transmisión. Esto permite que un equipo anfitrión conectado a dicho puerto esté en una VLAN pero, al ignorarlo, haciendo el conmutador todo el trabajo. Esto se conoce como VLAN basadas en puertos y conmutación de VLAN basada en puertos. Por lo tanto, el equipo anfitrión conectado a este puerto está en la VLAN asociada con el puerto, pero ignorándolo, y no tiene que ser compatible con IEEE 802.1q, etc., dado que ni añade etiquetas VLAN a sus transmisiones ni recibe ninguna trama etiquetada. Sin embargo, no es así como se utilizan las VLAN en la presente realización.
- Los presentes inventores consideraron que cada VLAN estando aislada de todas las demás en una conmutación VLAN basada en puertos es una limitación en la que existe la necesidad de conectar un equipo anfitrión a múltiples VLAN, por ejemplo, cuando este equipo anfitrión es un servidor, etc., o cuando es necesario conectar conjuntamente múltiples conmutadores, soportando cada uno una fracción de una o varias VLAN. Por lo tanto, decidieron utilizar otro modo de funcionamiento conocido, denominado troncalizado VLAN. En este modo, los puertos de conmutador se pueden asociar con múltiples VLAN, y pueden dejarlas etiquetadas cuando transmiten estas tramas. Un equipo anfitrión conectado a un puerto de troncalizado tiene entonces que añadir y retirar las propias etiquetas VLAN, y puede simultáneamente transmitir y recibir desde múltiples VLAN. Es así como se utilizan las VLAN para tráfico determinista en la presente realización.
- En la presente realización, se asume siempre que la conmutación de VLAN que llevan datos deterministas es utilizando troncalizado VLAN para los datos deterministas, y que las etiquetas VLAN que identifican estas VLAN no deberían nunca ser introducidas o retiradas por el conmutador. Como resultado de esta conmutación virtual, una VLAN (troncalizada) que se utiliza para transportar solamente un tipo de datos, donde se utiliza solamente un equipo anfitrión como el origen nominal de este tipo de datos y todos los otros equipos anfitriones conectados son entonces destinos de este tipo de datos, pasa a ser, en todos los aspectos significativos, un VC.
- Dado que las VLAN son encaminadas a través de un conmutador virtual, en lugar de a través una central virtual, el encaminamiento de tráfico identificado con una VLAN es modificado asimismo por la dirección de destino MAC. De este modo, una trama identificada con una VLAN y que contiene una dirección MAC específica irá solamente al puerto asociado con la VLAN y conectado con la dirección MAC especificada. Sin embargo, se puede utilizar una dirección MAC de difusión, cuando la trama se transmita a todos los puertos asociados con la VLAN (excepto aquel en el que se recibe).
- Tal como se ha indicado anteriormente, el campo 202 ID de VLAN tiene solamente 12 bits de tamaño, lo que limita el número de VCs identificados por separado a 4094 (un par de valores están reservados). Si es necesaria la identificación de los VCs para mantener consistencia a través de todo el sistema, y ésta es la única identificación, entonces esto significa solamente 4094 VCs en todo el sistema. Sin embargo, este sería un límite artificial debido a que los valores de ID de VLAN pueden ser reutilizados. Con los conmutadores compatibles con VLAN de COTS, el límite real es que no puede haber más de 4094 VCs encaminados a través de ningún conmutador. Por lo tanto, en las redes mayores, los diferentes VCs que son encaminados a través de diferentes conmutadores pueden reutilizar el mismo ID. Se podrían satisfacer entonces requisitos para la identificación única de datos utilizando, por ejemplo, un ID de tipo de mensaje en la carga útil.
- Los dispositivos de conmutación que son compatibles con la CoS de IEEE 802.1 p se pueden configurar para transmitir tráfico etiquetado IEEE 802.1q a través de memorias tampón de salida independientes. Esto se puede realizar configurando el origen para establecer el valor PCP en la etiqueta a un valor alto (por ejemplo, 7) y configurando el conmutador para asociar esta clase de servicio con la memoria tampón de alta prioridad. Los conmutadores se pueden configurar asimismo para dar servicio a estas memorias tampón de alta prioridad, con estricta prioridad sobre la memoria tampón utilizada para el tráfico de mejor esfuerzo, que puede estar configurada por defecto a una prioridad menor. De este modo, cuando llega a una salida una trama priorizada etiquetada, se transmitirá con un retardo provocado solamente por el otro tráfico de alta prioridad y como mucho por una trama de baja prioridad (si había una recién empezada cuando llega la primera trama de alta prioridad).
- A la salida de cada dispositivo de conmutación 102, los VCs se asignan a una memoria tampón y se encaminan a través de la misma, por ejemplo, utilizando el protocolo de clase de servicio (CoS) descrito en IEEE 802.1d, y compañía. Esta memoria tampón recibe una prioridad simple sobre todas las demás memorias tampón asociadas con la misma salida del conmutador, de tal modo que no se transmite ningún otro tráfico (por ejemplo, no crítico) desde dicha salida cuando existe alguna trama de datos Ethernet contenida en la memoria tampón de VC.
- Cada VC se puede asignar a un ancho de banda máximo que puede utilizar. Los conmutadores de red pueden utilizar medidas de control de tráfico que limitan individualmente cada VC a su ancho de banda asignado, por ejemplo retardando y/o rechazando cualquier tráfico que exceda este límite, determinado, por ejemplo, por llegar demasiado cerca de la trama anterior del mismo VC, en base al ancho de banda y a la fluctuación tolerada para dicho VC. Esto se puede realizar, por ejemplo, utilizando los algoritmos conocidos de cubo de permisos o de cubo con fugas, o un equivalente, es decir, un algoritmo que limite estrictamente la frecuencia de datos nominal y la fluctuación máxima del tráfico en un VC de VLAN individual, independientemente entre cada entrada y las memorias

tampón. Los requisitos específicos para el rango y la resolución del ancho de banda (intervalo nominal) y la tolerancia a la fluctuación pueden variar. Sin embargo, el rango en el intervalo nominal (que es equivalente al espacio de asignación de ancho de banda de AFDX) debería abarcar intervalos desde por lo menos 12 μ s y hasta un segundo. La tolerancia a la fluctuación debería abarcar un rango desde cero y hasta, por lo menos, varios milisegundos (que se asume es suficiente para jerarquías de conmutadores de múltiples niveles hasta por lo menos una profundidad de 4 capas).

Simplificando, los algoritmos de cubo de permisos y de cubo con fugas miden la frecuencia promedio en la que llegan datos en un VC y la variación en torno a ésta, esencialmente, cuánto antes llegan respecto de cuando deberían, en base al ancho de banda nominal. Básicamente, las tramas deberían llegar a la frecuencia nominal, pero algunas pueden llegar anticipadamente, debido a la fluctuación. Sin embargo, si llega más de la fluctuación esperada antes de un "tiempo de llegada ideal" (obtenido a partir de la frecuencia nominal), tiene que haber sido transmitida demasiado pronto, es decir, en un ancho de banda demasiado alto, o haber fluctuado más de lo permitido, y por lo tanto es abandonada por la función de vigilancia de tráfico para proteger la memoria tampón.

Sin embargo, este procedimiento propuesto para la tolerancia a fallos del sistema (vigilancia del tráfico en las entradas del conmutador), no está soportado por los protocolos Ethernet actuales, por lo menos no en relación con VLAN y CoS. No obstante, las funciones que proporcionan esta característica en las presentes realizaciones están contenidas íntegramente dentro del conmutador o conmutadores de la red central. Por lo tanto, estas características se puede implementar mientras que se siguen utilizando solamente características estándar de Ethernet en los subsistemas. Esto significa modificar el conmutador o conmutadores de la red central donde se requiera tolerancia a fallos del sistema, pero dado que habrá muchos menos de éstos que subsistemas, esto será aceptable en la mayor parte de los casos.

Para asegurar que estas funciones de vigilancia del tráfico no rechazan tráfico legítimo, el límite de ancho de banda al que se vigila un VC se puede ajustar algo mayor que el ancho de banda asignado para el VC, es decir, el ancho de banda que se permite al origen utilizar en el VC. Análogamente, el límite de fluctuación se puede ajustar algo mayor que la suma de las variaciones en la planificación en el origen del VC y los retardos entre el punto en el que está planificada la transmisión y la función de vigilancia, lo que tiene que incluir cualquier variación en el retardo entre la entrada del conmutador y la función de vigilancia. Sin embargo, este retardo puede ser difícil de medir por separado, ya sea como parte de caracterización o validación frente a especificación. De este modo, puede ser necesario utilizar un valor sobrestimado, por ejemplo, la variación en retardo entre la entrada y la salida del conmutador, lo que incluye necesariamente retardos que preceden a la función de vigilancia y retardos que la suceden.

Los retardos a través de los conmutadores comprenderán dos tipos independientes: un tipo que depende del tráfico que fluye a través del conmutador (y, por lo tanto, específico del sistema y de la configuración de la red), y un tipo que, aunque de naturaleza potencialmente variable, no depende del tráfico que fluye a través del conmutador y, por lo tanto, se puede caracterizar por separado respecto de una configuración. Mediante la especificación apropiada de los dispositivos de conmutación, por ejemplo, con funcionamiento a velocidad de hilo y memorias tampón de salida o bien una memoria tampón centralizada y compartida que se puede modelizar como un conjunto de memorias tampón de salida virtuales asociadas, cada una, con una salida de conmutador específica, es posible asegurar que el almacenamiento en memoria tampón en el conmutador asociado con las salidas de conmutador es la única fuente de retardos que dependen de los flujos de tráfico y, además, que estos retardos dependen solamente del tráfico encaminado a través de la salida con la que está asociada la memoria tampón.

Como una consecuencia de la predeterminación de los caminos y de las limitaciones aplicadas a los anchos de banda de los VCs, se pueden predecir los niveles de llenado para, y los consiguientes retardos provocados por las memorias tampón del conmutador en la red. Los niveles de llenado máximos, ya sea en valores absolutos o con una probabilidad de ocurrencia, se pueden comparar entonces con los tamaños reales de las memorias tampón con el fin de asegurar que no puede haber congestión dentro de, o entre las memorias tampón asignadas a los VCs, o que la congestión tiene solamente una cierta probabilidad de ocurrencia. Por lo tanto, el transporte de estas tramas con etiquetas VLAN sobre un VC, excepto pérdidas debidas al ruido y a fallos de componentes dentro de sus caminos o equipos anfitriones que exceden los anchos de banda asignados de otros VCs, será completamente fiable o, cuando los niveles de llenado predichos sean probabilísticos, tendrá una cierta probabilidad de éxito.

Dado que el ancho de banda de cada VC se puede limitar a un nivel conocido, es posible, utilizando procedimientos conocidos, por ejemplo cálculo de redes o un procedimiento equivalente, predecir por adelantado cuál puede ser el nivel máximo de llenado de cada una de las memorias tampón en la red para un conjunto dado de VCs. Estos valores se pueden comparar a continuación con los tamaños de memorias tampón disponibles con el fin de comprobar que no puede haber congestión, es decir, que las memorias tampón no se pueden desbordar en ningún caso, o que existe una probabilidad suficientemente baja de que lo hagan. Esto se puede utilizar para demostrar la fiabilidad de las transferencias. Los retardos que estas memorias tampón pueden llegar a provocar se pueden asimismo calcular al mismo tiempo, y combinados con los otros retardos, que se pueden caracterizar por separado respecto del conjunto de VCs que comparten los recursos de red, para proporcionar los retardos máximos extremo a extremo, o valores cuya superación tenga una probabilidad lo suficientemente baja. Estos se pueden comparar a

continuación con cualesquiera requisitos del plazo límite para transferencias de datos puntuales, para demostrar que se cumplirán.

5 El retardo máximo provocado por las memorias tampón en el camino de un VC se puede añadir a continuación a los retardos no dependientes del tráfico para el mismo camino con el fin de proporcionar un retardo máximo extremo a extremo en transporte, a través de la red. Análogamente, las variaciones en estos retardos se pueden sumar para el camino de un VC con el fin de proporcionar una fluctuación máxima en la entrega de las tramas de Ethernet que llevan los datos críticos. Estos VCs proporcionan por lo tanto rendimiento en tiempo real.

10 La utilización del control del tráfico en los conmutadores de red para limitar las transmisiones en los VCs asegurará que, exceptuando en circunstancias que involucren fallos de los conmutadores de red y/o del esquema de protección de datos incorporado en el estándar Ethernet, los niveles de llenado y los retardos máximos predichos provocados por las memorias tampón en los conmutadores no se superarán incluso en situaciones en las que los equipos anfitriones que transmiten sobre otros VCs excedan sus anchos de banda asignados. Las previsiones de que no habrá congestión y de los retardos máximos extremo a extremo, exceptuando las circunstancias que se acaban de enumerar, seguirán siendo válidas incluso en dichas situaciones. Por lo tanto estos VCs son, exceptuando las
15 circunstancias que se acaban de enumerar, inmunes a ataques de denegación de servicio que provocan la congestión y la subsiguiente pérdida de datos en la salida del conmutador de la memoria tampón.

20 Como resultado de utilizar el ancho de banda y las fluctuaciones en el control del tráfico, en lugar de los tiempos de transmisión absolutos para los datos, es posible utilizar una amplia variedad de procedimientos para planificar la transmisión de datos críticos, lo que debería ser un facilitador para utilizar técnicas de planificación avanzadas para las aplicaciones que son los orígenes y los receptores de estos datos. Específicamente, se puede soportar el procedimiento ejecutivo cíclico habitual, así como técnicas más avanzadas tales como planificación basada en prioridad preferente, siempre que sea posible especificar el intervalo mínimo entre transmisiones en un VC determinado. Asimismo, debido a que el sistema descrito en la presente memoria está basado solamente en la utilización de técnicas del dominio de frecuencias en el control y la predicción de rendimientos críticos, las
25 transmisiones pueden utilizar frecuencias de actualización no relacionadas armónicamente. Esto contrasta con procedimientos que utilizan técnicas en el dominio temporal, es decir, sincronizan los tiempos de transmisión sobre toda la red para evitar conflictos en los recursos compartidos (memorias tampón de conmutador). En estos enfoques controlados en el dominio temporal, las frecuencias de transmisión deben ser, esencialmente, subdivisiones de una frecuencia base y, por lo tanto, todas las frecuencias de transmisión están necesariamente relacionadas armónicamente. Por ejemplo, la frecuencia máxima se puede fijar a 50 Hz; en cuyo caso, las únicas frecuencias de transmisión menores que están disponibles serán de 25, 12,5 y 6,25 Hz, etc. Si esto no es así, se producirán entonces conflictos a cierta frecuencia determinada por sus diferentes frecuencias. Sin embargo, en una red que utilice el esquema descrito en la presente memoria, un VC puede utilizar una frecuencia de transmisión de 50 Hz mientras que otro, que puede tener el mismo origen y/o los mismos destinos, puede utilizar 60 Hz.

35 La redundancia de red para proporcionar tolerancia a fallos de la red no está soportada por los protocolos Ethernet actuales. Sin embargo, de nuevo, es posible implementar esta característica, con ciertos costes, pero sin apartarse de la utilización de COTS y de los componentes estándar en el subsistema. Una posible manera de implementar esta clase de redundancia de red sería en la capa de aplicación. Una solución de este tipo consiste en utilizar múltiples VCs, uno a través de cada una de las redes idénticas. Estos múltiples VCs se pueden extender desde las aplicaciones en el origen hasta las aplicaciones en el destino. Las aplicaciones en el destino pueden a continuación
40 extraer datos solamente de uno de estos, por ejemplo, el que los entregue primero. En el contexto de los IMS (integrated modular systems, sistemas modulares integrados) y de la TLS (three layer stack, pila de tres capas), se puede ver que esto hace que la capa de aplicación dependa de la red, dado que no tendría que hacer esto si la propia red fuera tolerante a fallos, etc. Sin embargo, si los requisitos para esta tolerancia a fallos se limitan a una fracción de posibles usuarios, puede ocurrir que soportar redundancia de red en el MSUOSL haga estas capas dependientes de la nueva plataforma, o por lo menos añada a las mismas complejidad más allá de los requisitos generales. En cuyo caso, utilizar múltiples VCs paralelos, a pesar de la funcionalidad adicional en la capa de aplicación, puede ser una solución aceptable.

50 La utilización de componentes existentes de los estándares Ethernet permite al sistema descrito en la presente memoria ser totalmente compatible tanto con hardware COTS como con software COTS. Por ejemplo, tanto VxWorks™ (edición de equipos de red) de Wind River como Integrity de Green Hill soportan IEEE 802.1 q e IEEE 802.1 p. Asimismo, la pila de tres capas (TLS) de IMS utiliza actualmente controladores de dispositivos VxWorks™, y por lo tanto debería proporcionar asimismo el soporte necesario. Greenhills Integrity™ y algunas versiones de Linux proporcionan asimismo soporte para VLAN y CoS. Las realizaciones descritas en la presente memoria pueden ser
55 utilizadas por lo tanto para añadir transferencias de datos deterministas a nuevas implementaciones de red, es decir, sistemas nuevos y actualizaciones de sistemas; y pueden asimismo ser aplicables a sistemas que utilicen redes Ethernet conmutadas (y un OS compatible) existentes, con un mínimo impacto sobre el tráfico existente y el funcionamiento en dichos sistemas. Pueden asimismo permitir la implementación de nuevos sistemas o de nuevas redes sabiendo que dichas transferencias se pueden añadir en un momento posterior sin la necesidad de añadir nuevas interfaces, cuando emerjan, si lo hacen, los requisitos para estas transferencias. Los controladores de dispositivos, etc., para las interfaces de red que no están destinadas a enviar o recibir tráfico determinista no tendrán
60

requisitos especiales adicionales en relación con su utilización en realizaciones del sistema y, por lo tanto, debería ser suficiente cualquier controlador compatible con IEEE 802.3.

Además de proporcionar medios para demostrar que se satisfarán siempre los requisitos de criticidad, las realizaciones descritas en la presente memoria permiten asimismo que las redes Ethernet existentes puedan ser actualizadas para soportar transferencias de datos críticas. Esto se debe a que la realización utiliza solamente los protocolos IEEE 802.1q e IEEE 802.1d para identificar y encaminar los VCs, y para mantener los datos críticos separados del tráfico de Ethernet ordinario, no crítico. Por lo tanto, los sistemas de VCs se pueden implementar utilizando solamente interfaces Ethernet y software de controladores de dispositivos que sean compatibles con los estándares IEEE 802.3-2002 o posteriores, incorporando soporte para VLANs IEEE 802.1q y CoS IEEE 802.1d. Sin proporcionar tolerancia a fallos en los otros equipos anfitriones, puede ser implementado utilizando un conmutador que sea compatible con los estándares IEEE 802.3-2002 o posteriores, incorporando soporte para VLANs IEEE 802.1q y CoS IEEE 802.1d. Estando dichos conmutadores ampliamente disponibles tanto para instalaciones de red comerciales como en forma reforzada para aplicaciones de aviónica, etc. La disposición de tolerancia a dichos fallos del sistema, como transmisión excesiva de datos críticos, requerirá la modificación de los conmutadores utilizados en el sistema, pero no requerirá modificaciones de, o en ninguno de los equipos anfitriones, ni en aquellos que transmiten y reciben utilizando los VCs descritos en la presente memoria ni en los que transmiten y reciben sin utilizarlos, siempre que estos equipos anfitriones y su software soporten VLANs y CoS. Por lo tanto, este procedimiento para soportar sistemas críticos se puede imponer, como un protocolo de aplicación, en una red Ethernet gigabit conmutada de dúplex completo existente, con un impacto mínimo sobre las LRUs de equipos anfitriones existentes, y por lo tanto con costes mínimos.

Los subsistemas en algunas plataformas pueden comprender múltiples módulos y contener pequeños conmutadores para interconectarlos, y conectarlos a uno o varios conmutadores de la red central. Otros pueden comprender un único módulo, y por lo tanto sin conmutación. Estos conmutadores de subsistemas seguirán necesitando separar el tráfico de mejor esfuerzo y el determinista (esto es cierto asimismo para cualquier protocolo de aplicación que añada transferencia determinista a tráfico de mejor esfuerzo, tal como TTE). En el caso de la realización descrita en la presente memoria, esto requiere el soporte tanto para IEEE 802.1 q como para IEEE 802.1 p, dado que tiene que reconocer y utilizar el PCP en la etiqueta VLAN. Para otros protocolos de aplicación, los mecanismos para identificar datos deterministas, y, por lo tanto, cómo determina el conmutador la prioridad del tráfico, son generalmente específicos de los protocolos, y por lo tanto requerirán generalmente un conmutador a medida en este contexto.

Las realizaciones del sistema de transferencia de datos descrito en la presente memoria pueden tener las ventajas siguientes:

- Es económico:
 - Económico de implementar o de añadir como una actualización -los componentes pueden ser COTS o MCOTS.
 - Económico de poseer -seguirá siendo compatible con componentes de subsistemas futuros, es decir, conjuntos de chips Ethernet en tarjetas de procesador, minimizando problemas de obsolescencia asociados con la red.
 - Económico de actualizar una vez implementado -minimiza el impacto de actualización a mayor ancho de banda de capa física (por ejemplo, Ethernet de 10 gigabits) y/o a una red mayor (por ejemplo, múltiples conmutadores).
- Se minimiza el impacto sobre el funcionamiento de sistemas y subsistemas:
 - No prescribe ni proscribire procedimientos de planificación de tráfico -no es necesario planificar cíclicamente o sincronizar transmisiones mediante subsistemas diferentes - soporte directo para procedimientos avanzados de planificación, por ejemplo planificación preferente basada en prioridades.
 - Soporta transferencias acíclicas/espóradas
 - Soporta frecuencias de transferencias no relacionadas armónicamente (no se requieren procedimientos de frecuencias divididas).
- Perfectamente adecuado para sistemas de canalización de información:
 - Los datos se pueden transferir en cuanto sean procesados (con planificación preferente, pueden asimismo ser procesados en cuanto se reciben).
- Bajo impacto frente a cambios -tráfico añadido sin cambios en otros subsistemas:
 - Solamente es necesario recalcular las utilidades de las memorias tampón para confirmar que sigue sin producirse congestión y se siguen cumpliendo los plazos límite.
- Compatible con protocolos estándar de capas superiores, por ejemplo, protocolos de internet (UDP, TCP, etc.).

REIVINDICACIONES

1. Un sistema de transferencia de datos, que incluye:
 por lo menos un dispositivo de conmutación (102) configurado, en uso, para transferir datos, directa o indirectamente, entre una serie de dispositivos informáticos (104),
- 5 en el que dicho por lo menos un dispositivo de conmutación está configurado para proporcionar una serie de redes de área local virtuales (VLAN), dentro de las cuales se puede configurar un canal virtual (VC) por medio de datos de VC transmitidos como tramas de Ethernet (200) etiquetadas con una etiqueta VLAN (202),
 siendo encaminados los datos de VC a través de dicho por lo menos un dispositivo de conmutación, según un campo (204) ID de VLAN de la etiqueta VLAN de una mencionada trama; **caracterizado porque:**
- 10 cada mencionada VLAN está configurada como un respectivo VC al recibir datos de VC desde un mencionado dispositivo informático designado como un único origen de datos de VC sobre el VC respectivo, y **porque** el encaminamiento fijo y predeterminado de dicha trama está determinado por la configuración de dicho por lo menos un dispositivo de conmutación.
- 15 2. Un sistema según la reivindicación 1, que incluye una serie de dispositivos de conmutación (102), utilizando cada uno de dichos dispositivos de conmutación troncalizado VLAN para permitir la transmisión sobre, y la recepción desde una serie de VLAN, permitiendo de ese modo que dicha serie de dispositivos de conmutación se conecten conjuntamente.
3. Un sistema según la reivindicación 2, en el que la etiqueta VLAN (202) de una mencionada trama es introducida o retirada externamente de dicho por lo menos un dispositivo de conmutación (1102).
- 20 4. Un sistema según cualquiera de las reivindicaciones anteriores, en el que una mencionada etiqueta VLAN (202) utiliza cualquier valor de ID de protocolo de etiqueta (TPID) disponible y designa por lo menos un mencionado dispositivo informático (104) diferente a dicho único dispositivo informático de origen como por lo menos un destino para los datos de VC.
- 25 5. Un sistema según cualquiera de las reivindicaciones 1 a 3, en el que el VC está limitado a un mencionado dispositivo informático designado como un único destino para los datos de VC, con el fin de evitar que los destinos reciban datos de otros orígenes.
- 30 6. Un sistema según cualquiera de las reivindicaciones anteriores, en el que en una salida de dicho dispositivo de conmutación (102), los VCs pueden ser asignados a, y encaminados a través de una memoria tampón de VC, y el encaminamiento a través de la memoria tampón de VC es por medio de un protocolo de clase de servicio (CoS) de IEEE 802.1d.
7. Un sistema según la reivindicación 6, en el que se utiliza un campo de punto de código de prioridad (PCP) (206) en la etiqueta VLAN (202) para identificar los datos de VC para encaminamiento a través de la memoria tampón de VC.
- 35 8. Un sistema según la reivindicación 7, en el que la memoria tampón de VC recibe prioridad sobre cualesquiera otras memorias tampón asociadas con la salida del dispositivo de conmutación (102), de tal modo que no se transmite ningún otro tráfico desde la salida cuando la memoria tampón de VC contiene alguna trama de datos Ethernet.
9. Un sistema según cualquiera de las reivindicaciones anteriores, en el que se asigna a cada mencionado VC un ancho de banda máximo.
- 40 10. Un sistema según la reivindicación 9, en el que dicho por lo menos un dispositivo de conmutación (102) utiliza medidas de control de tráfico que limitan individualmente cada mencionado VC a su mencionado ancho de banda máximo asignado, por ejemplo retardando y/o rechazando cualquier tráfico que exceda el ancho de banda máximo.
11. Un sistema según la reivindicación 10, en el que la medida de control del tráfico comprende un algoritmo de cubo de permisos o un algoritmo de cubo con fugas.
- 45 12. Un sistema según cualquiera de las reivindicaciones 9 a 11, en el que se calcula un nivel máximo de llenado para cada una de las mencionadas memorias tampón de VC y dicho nivel máximo de llenado se compara con los tamaños reales de las memorias tampón para evitar, o reducir la probabilidad de congestión dentro de, o entre las memorias tampón asignadas a los VCs.
- 50 13. Un sistema según cualquiera de las reivindicaciones anteriores, en el que dicho por lo menos un dispositivo informático (104) comprende una unidad de aviónica reemplazable en línea (LRU).

14. Una red de comunicaciones que comprende un sistema de transferencia de datos según cualquiera de las reivindicaciones anteriores, que incluye por lo menos un dispositivo de conmutación (102) y una serie de los mencionados dispositivos informáticos (104).

5 15. Un procedimiento para proporcionar transferencia de datos entre dispositivos informáticos (104), incluyendo el procedimiento configurar por lo menos un dispositivo de conmutación (102), en uso, para transferir datos, directa o indirectamente entre los dispositivos informáticos utilizando el sistema de transferencia de datos según cualquiera de las reivindicaciones 1 a 13.

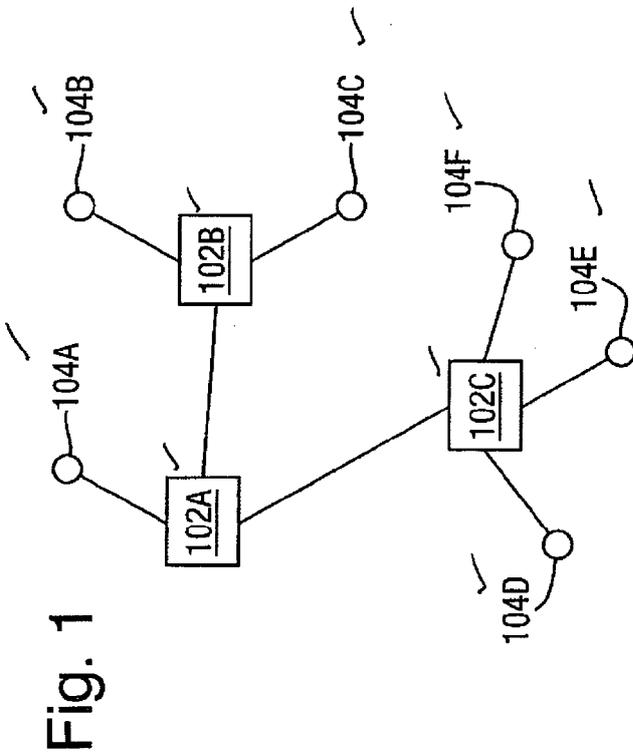


Fig. 1

Fig. 2

Preámbulo	7 octetos de 10101010	Delimitador de inicio de trama	1 octeto de 10101011	Destino MAC	6 octetos	Origen MAC	6 octetos	Etiqueta VLAN		Carga útil (datos y relleno)	CRC32	Espacio entre tramas																		
								<table border="1"> <tr> <td>ID de protocolo de etiquetas</td> <td>P</td> <td>C</td> <td>ID de VLAN</td> <td>C</td> <td>F</td> <td>P</td> <td>I</td> </tr> <tr> <td>2 octetos</td> <td>3</td> <td>1</td> <td>12</td> <td>2</td> <td>1</td> <td>12</td> <td>2</td> </tr> </table>	ID de protocolo de etiquetas	P	C	ID de VLAN	C	F	P	I	2 octetos	3	1	12	2	1	12	2	<table border="1"> <tr> <td>Ether-type o Longitud</td> <td>2 octetos</td> </tr> </table>	Ether-type o Longitud	2 octetos	46-1500 octetos	2 octetos	12 octetos de inactividad
ID de protocolo de etiquetas	P	C	ID de VLAN	C	F	P	I																							
2 octetos	3	1	12	2	1	12	2																							
Ether-type o Longitud	2 octetos																													

Fig. 2