



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 367 629**

51 Int. Cl.:
H04L 12/46 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **03739963 .1**

96 Fecha de presentación : **20.06.2003**

97 Número de publicación de la solicitud: **1646188**

97 Fecha de publicación de la solicitud: **12.04.2006**

54 Título: **Procedimiento para el aislamiento de seguridad de servicios de red Ethernet.**

45 Fecha de publicación de la mención BOPI:
07.11.2011

45 Fecha de la publicación del folleto de la patente:
07.11.2011

73 Titular/es: **ZTE CORPORATION**
ZTE Building, South Hi-Tech Road
Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

72 Inventor/es: **Jia, Minghong;**
You, Yong y
Xu, Lingbo

74 Agente: **Carpintero López, Mario**

ES 2 367 629 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

Procedimiento para el aislamiento de seguridad de servicios de red Ethernet

Campo técnico

5 La presente invención se refiere a un procedimiento para el aislamiento de seguridad de servicios de Ethernet, particularmente a la realización de una Red Privada Virtual (VPN) sobre Ethernet de Capa 2, que es utilizado por los proveedores de servicios de telecomunicaciones para proporcionar servicios de Ethernet.

Antecedentes de la invención

10 Ethernet se aplicó originalmente en red de área local (LAN), cuyos usuarios son principalmente usuarios los internos de una empresa, lo que significa que el número de usuarios es más bien pequeño. Cuando el número de usuarios es mayor, se utiliza mayor nivel de equipamiento para realizar la conexión de una pluralidad de redes Ethernet.

Con el rápido desarrollo y la extensa aplicación de Ethernet, también se aplica a la red de área ancha (WAN). Para cumplir con la exigencia de un mayor desarrollo, VLAN (en referencia a IEEE 802.1Q) se introduce en la tecnología de Ethernet. VLAN se utiliza para el aislamiento de seguridad para restringir el área de difusión de los datos.

15 El documento de solicitud de patente EP1318631A2 divulga los procedimientos de resolución de direcciones utilizados en la red privada virtual (VPN). Según este documento, se transmite un mensaje de petición de resolución de dirección por un primer dispositivo de borde cliente (CE) en los circuitos virtuales de capa 2 de su interfaz de borde proveedor (PE). El mensaje de petición de resolución de direcciones incluye la dirección de capa 3 asignada a un segundo dispositivo CE de la VPN. En respuesta a la recepción del mensaje de petición de este tipo en el
20 segundo dispositivo CE, se devuelve un mensaje de respuesta de a resolución de dirección al primer dispositivo CE. En respuesta a la recepción de este mensaje de respuesta, el primer dispositivo CE cartografía la dirección de capa 3 asignada al segundo dispositivo CE a un identificador de LAN virtual del circuito virtual de capa 2 en el que se recibe el mensaje de respuesta.

25 El documento US2003110268A1 divulga un servicio de red privada virtual (VPN) prestado a través de una infraestructura de red compartida que incluye dispositivos interconectados de borde proveedor (PE) que tienen interfaces de borde cliente (CE). Algunas de las interfaces CE se asignan a una VPN que soporta LAN virtuales. Una correspondencia entre una interfaz CE y una LAN virtual se aprende sobre la base de tramas etiquetadas recibida en esta interfaz CE y que incluye un identificador de esta LAN virtual. El proceso de aprendizaje permite la detección de pares de interfaces CE que corresponden a una LAN virtual común. Cuando se da tal detección, se
30 establece un circuito virtual en la infraestructura de red compartida entre los dispositivos PE que tienen estas interfaces CE, y posteriormente se utiliza para las tramas de envío que incluyen el identificador de la VLAN virtual común

El documento US2003037163A1 divulga un procedimiento de comunicación: el procesamiento para la designación de un proveedor de servicio, autenticación de usuarios y asignación de direcciones IP, se realiza intercambiando
35 tramas de gestión entre un terminal de usuario y un proveedor de servicios a través de una red de acceso; y las principales tramas de señal tienen cada una una forma de IPOE y que contiene una dirección de fuente de capa 2 del terminal de usuario se intercambian entre el terminal del usuario y el proveedor de servicios a través de la red de acceso. Las tramas de gestión tienen una forma que puede ser objeto de discriminación por parte de las principales tramas de señal en la Capa 2, y la red de acceso contiene información sobre correspondencias entre
40 direcciones de fuente de Capa 2 y redes privadas virtuales. La red de acceso reconoce una de las redes privadas virtuales conectadas al proveedor de servicios, sobre la base de la dirección fuente de capa 2 contenida en cada trama principal de señal, y transfiere las tramas principales de señal a la Capa 2 por puentes MAC.

45 El documento EP1244254A divulga un sistema de clasificación VLAN y de etiquetado para un nodo de conmutación. Durante la clasificación VLAN, se asigna un paquete de entrada se asigna a una VLAN de acuerdo con un modo de clasificación seleccionable a partir de modos, PASO, FUERZA y PROTOCOLO. En el modo PASO, el paquete es asignado a una VLAN asociada con un ID de VLAN del paquete. En el modo FUERZA, el paquete es asignado a una VLAN asociada con un puerto de entrada. En el modo PROTOCOLO, el paquete es asignado a una VLAN asociada con un tipo de protocolo del paquete. Durante el etiquetado de VLAN, se modifica o no un
50 identificador de VLAN en un paquete de salida de acuerdo con un modo de etiquetado seleccionable desde un modo PASO, FUERZA y ELIMINAR. En el modo de PASO, el ID de VLAN en el paquete se mantiene tal como se recibió. En el modo FUERZA, el ID de VLAN en el paquete se sustituye por un ID de VLAN en el cual se clasificó en el paquete entrante. En modo ELIMINAR, el ID de VLAN del paquete se elimina sin sustitución.

Sin embargo, la reciente introducción de la tecnología VLAN está orientada hacia la empresa, la cual es eficaz y eficiente para la Ethernet de una empresa. Si un proveedor de servicios utiliza una VLAN para realizar aislamiento

de seguridad de los servicios de Ethernet en la prestación de servicios a varias empresas, se producirán los siguientes problemas:

- la configuración de VLAN proporcionada por el proveedor de servicio puede entrar en conflicto con la configuración original de la empresa VLAN;
- 5 - una empresa tiene muchos servicios VLAN, algunos de los cuales no tiene una identificación válida de antemano;
- demasiados ajustes de VLAN podrían hacer que la administración fuese demasiado complicada o incluso no administrable;
- 10 - hay un número limitado de ID de VLAN, teóricamente, un dispositivo puede soportar 4.096 VLAN simultáneamente, las cuales son compartidas por todos los usuarios, dando como resultado un número insuficiente de VLAN;
- la tecnología de conmutación de capa 2 que emplea VLAN solamente lleva a cabo el aislamiento de datos, pero no aplica realmente todo el puente virtual en la tabla de direcciones MAC, y
- 15 - dos interfaces en dispositivos tradicionales de capa 2 no se pueden conectar en bucle, lo cual es menos es menos mensurable.

Sumario de la invención

El objetivo de la presente invención es solucionar el problema de que la aplicación de VLAN se limita a Al servicio de Ethernet a una sola empresa, solucionar el problema de aislamiento de seguridad al que se enfrentan los proveedores de servicios cuando prestan servicios de Ethernet/VLAN a una pluralidad de empresas, y proporcionar un procedimiento para realizar tecnología VPN sobre Ethernet de capa 2. Con este procedimiento, la invención puede proporcionar un puente virtual completo para hacer que la transferencia de datos sea transparente y mejorar la capacidad operativa y la mensurabilidad de los servicios Ethernet.

La solución técnica de la presente invención es como sigue:

Un procedimiento para realizar aislamiento de seguridad de servicios de Ethernet, que comprende las siguientes etapas:

- 1) añadir un segmento adicional en una trama Ethernet para identificar diferentes servicios de usuario, el segmento consiste en n bytes y n tiene un valor ligado al formato del segmento;
- 2) introducir un servicio de usuario en las redes de datos de un proveedor de servicios, y añadir un ID de usuario al segmento adicional de la trama Ethernet que soporta el servicio de usuario;
- 30 3) procesar conmutación/ruta;
- 4) borrar el ID de usuario y restablecer la trama Ethernet cuando el servicio de usuario sale de las redes de datos, en las cuales cuando el servicio de usuario es procesado en alguna interfaz física, el ID de usuario del servicio de usuario se compara con el ID de usuario de la interfaz física, si los dos ID coinciden, el servicio de usuario quedará garantizado, de otro modo se descartará el servicio.

35 En la etapa 2), el servicio de usuario que entra en una interfaz física se marca con un cierto formato por un ID de usuario asignado a la interfaz física que conecta el servicio de usuario.

En la etapa 3), basado en el ID de usuario, se mantiene una única tabla de direcciones MAC para cada ID de usuario mediante el aprendizaje y la búsqueda de direcciones MAC, se genera un único árbol de expansión en la interfaz física incluida en cada ID de usuario para formar un puente virtual real, en dichos puente virtual, las direcciones MAC idénticas se pueden utilizar en tablas de direcciones MAC de diferentes ID de usuario.

En la etapa 3), se genera un único árbol de expansión para cada ID de usuario para evitar una tormenta de difusión.

En la etapa 3), los usos de ID de VLAN para diferentes ID de usuario están completamente aislados, y un usuario también puede usar las ID de VLAN para realizar el aislamiento de red interna.

45 En la etapa 3), en las interfaces físicas que conectan el servicio de usuario, el aislamiento de servicio interno se fija según que el ID de VLAN sea o no utilizado mediante la elección de vías de utilización del ID de VLAN a través de la gestión de redes.

En la etapa 3), un modo de servicio multidifusión única puede ser proporcionado para cada ID de usuario, en el cual el modo de servicio multidifusión comprende un modo de protocolo de multidifusión dinámica y un modo de configuración de multidifusión estática;

5 el modo de protocolo de multidifusión dinámica significa que una interfaz de servicios en el servicio multidifusión es determinado por el protocolo de multidifusión dinámica, y el protocolo de multidifusión dinámica comprende el protocolo ICMP y el protocolo GMRP(Véase RFC 2236 e IEEE 802.1q);

El modo de configuración multidifusión estática determina la interfaz de servicios en el servicio multidifusión por configuración manual del usuario mediante gestión de redes.

10 En la etapa 3) cada ID de usuario configura el modo de servicio de multidifusión por la gestión de red. El modo de servicio incluye el modo de protocolo multidifusión dinámica y el modo de configuración multidifusión estática.

En la etapa 2) un ID de usuario es asignado a cada interfaz física. Cuando se introduce en la interfaz, se etiqueta un servicio mediante un ID de usuario. E ID de usuario permanece sin cambios en toda la red hasta que el servicio salga de la interfaz y alcance un dispositivo de usuario. A continuación el ID se elimina y finalmente el servicio alcanza el dispositivo de usuario. Por este medio se transfiere de manera transparente un servicio.

15 El segmento adicional en la trama Ethernet usa el siguiente formato: formato compatible con MPLS, formato VLAN apilable o formato personalizado para realizar una conexión entre una pluralidad de dispositivos.

Se establecen opciones de configuración en las interfaces físicas a través de la gestión de red para proporcionar formatos compatibles con MPLS, VLAN apilable y personalizados al segmento adicional en la trama Ethernet.

20 El procedimiento de aislamiento de servicio según la presente invención tiene las siguientes características en comparación con las presentes técnicas VLAN (IEEE 802.1Q): realizar un puente virtual de función plena sin tener en cuenta la VLAN en el servicio de usuario; reducir la complejidad de administración y mejorar la independencia de los dispositivos; poder adaptarse a los servicios Ethernet proporcionados por los proveedores de servicios de telecomunicaciones.

Este procedimiento tiene los siguientes efectos:

- 25 1. El proveedor de servicio no necesita conocer la configuración VLAN original del cliente. La configuración VLAN original no necesita ser cambiada.
2. El cliente puede cambiar sus configuraciones VLAN libremente. Puede modificar o añadir el servicio con la ayuda del proveedor de servicio. El servicio de usuario no necesita tampoco tener un ID de VLAN.
3. El proveedor de servicio solamente configura el ID de usuario, que es sencillo de realizar.
- 30 4. Si se usan n bits de ID de usuario, se pueden albergar segundos usuarios. Cada usuario puede usar 4096 VLAN independientemente, lo cual soluciona el problema del número de VLAN.
5. aprendiendo la dirección MAC y el ID de cliente, se puede realizar un puente virtual completo en la tabla de direcciones MAC.
6. Se pueden configurar diferentes servicios de multidifusión según los requisitos de cliente.
- 35 7. Se mejora la mensurabilidad de los dispositivos de conmutación de capa 2. Con la realización del puente virtual anterior, se puede ensayar un dispositivo construyendo un canal de ensayo de servicio entre una pluralidad de puentes virtuales.

Breve descripción de los dibujos

- 40 - la figura 1 es el cuatro esquemático del ensayo de servicio usando el procedimiento según la presente invención;
- la figura 2 es el diagrama de flujo de una realización según la presente invención;
- la figura 3 es el cuadro esquemático del soporte de la VLAN de cliente usando el procedimiento según la presente invención;
- la figura 4 es el cuadro esquemático de uso del ID de usuario para realizar el aislamiento de servicio;
- 45 - La figura 5 es el formato de cuadro de VLAN de Ethernet;

- La figura 6 es el formato de cuadro VLAN apilable;
- La figura 7 es el formato de cabeza de cuadro MPLS.

Descripción detallada de la invención

Un procedimiento de aislamiento de servicios Ethernet según la presente invención comprende lo que sigue:

- 5 Se añade un segmento adicional a una trama Ethernet, y el dato en el segmento se define como un ID de usuario que consiste en n byte para identificar una red de datos de proveedor de servicio, en consecuencia la trama Ethernet se cambia. Cuando el usuario sale de la red de datos, se restablece la trama Ethernet al estado original.

- 10 En primer lugar, se asigna un ID de usuario a la interfaz física que conecta el servicio de usuario, para marcar el ID de usuario al servicio que entra en la interfaz física. A continuación, cuando un servicio entra en una interfaz física, el ID de usuario del servicio se compara con el ID de usuario de la interfaz. Si los dos ID coinciden, el servicio quedará garantizado.

Usando el ID de usuario, un dispositivo Ethernet se convierte en una pluralidad de redes Ethernet virtuales, y todas las redes Ethernet virtuales funcionan de forma independiente, sin interferir entre sí.

- 15 Debido a la presencia del ID de usuario, se puede mantener una única tabla de direcciones MAC para cada cliente aprendiendo y buscando la dirección de ID + MAC de usuario. Mientras tanto, se usa un único árbol de expansión en la interfaz física incluida en cada ID de usuario. Asimismo, se puede usar una multidifusión independiente para cada ID de usuario, lo cual incluye multidifusión dinámica y multidifusión estática. En consecuencia, se genera un puente virtual real. Con este puente virtual, diferentes usuarios pueden usar la misma dirección MAC y diferentes configuraciones de protocolo de multidifusión dinámica o multidifusión estática respectivamente.

- 20 En la figura 1, se realiza un ensayo de bucle en dos dispositivos. Aquí (a, b) se refieren a interfaces, a es un número de dispositivo bajo prueba, mientras que b es un número de interfaz. (1, 1), (1, 2), (2, 1), (2, 2) son el ID de usuario N, (1, 3), (1, 4), (2, 3), (2, 4) es el ID de usuario M, N#M Un servicio de un dispositivo de ensayo entra en primer lugar (1, 1), aquí está marcado con el ID de usuario N, a continuación, el mismo servicio sale (1, 2) y entra (2, 1), luego sale (2, 2), donde se elimina el ID de usuario N. El servicio que sale (2, 2) entra a continuación (2, 4), donde se marca con el ID de usuario M; a continuación, el mismo servicio sale (2, 3) y entra (1, 4); a continuación sale (1,3) y entra en el dispositivo de ensayo, donde el ID de usuario M se elimina. La misma función se puede realizar de forma inversa.

- 30 En la figura 2, un servicio se marca con el ID de usuario en primer lugar en la entrada, y luego pasa a través de conmutador/ruta; al mismo tiempo el ID de usuario + dirección MAC se aprenden y se buscan. Cuando el servicio procesado a través del conmutador/ruta llega a la salida, el ID de usuario del servicio se compara con el ID de usuario de la interfaz. Si dos ID no coinciden entonces se descartará el servicio.

En la figura 3, la red de servicio de cliente está marcado con un ID de usuario. Un servicio n de VLAN se transfiere de 2, 3 a 1, mientras que un servicio m de VLAN se transfiere de 1 a 2, 3. La VLAN entre las interfaces 2 y 3 interfaces ayuda a aislar los datos para que no se mezclen.

- 35 La figura 4 es una conexión WAN típica. Las diferentes líneas se refieren a diferentes servicios aislados por ID de usuario. Los servicios con diferentes ID de usuario no se mezclan. Cada ID de usuario tiene un único árbol de expansión, lo que ayuda a evitar tormenta de difusión. El uso de ID de VLAN entre los diferentes ID de usuario está completamente aislado. Un cliente puede elegir utilizar ID de VLAN para aislar servicios internos o no usarlos.

DUT es un dispositivo bajo ensayo.

- 40 Una realización según la presente invención se describe con sigue:

Etapas 1: Marcar un servicio con un ID de usuario.

- 45 Un ID de usuario se puede establecer para cada interfaz física. Cuando el servicio entra en la interfaz, en primer lugar se marca con el ID de usuario que se mantendrá sin cambios en toda la red hasta que el servicio sale de la interfaz y llega al dispositivo de usuario. A continuación el ID de usuario se elimina y el servicio alcanza el dispositivo de usuario. En consecuencia, el servicio se transfiere de manera transparente.

Etapas 2: Aislamiento del servicio

Cada interfaz física tiene un ID de usuario configurable por el usuario. Cuando el servicio necesita salir de la interfaz, el ID de usuario del servicio se compara con el ID de usuario de la interfaz. Si los dos ID no coinciden, se descarta el servicio.

Etapa 3: Realización de un puente virtual real

Si el dispositivo es un puente de conmutación, añadir el ID de usuario para el aprendizaje y la búsqueda de la dirección MAC generará una única tabla de direcciones MAC para cada ID de usuario. Se puede ejecutar un único árbol de expansión para cada ID de usuario y se puede también ejecutar una única multidifusión para cada ID de usuario. La multidifusión única incluye un protocolo multidifusión dinámica y una configuración de multidifusión estática. En consecuencia, la interfaz para cada identificador de usuario funciona como un puente virtual real.

El diagrama de flujo del procedimiento anterior se muestra en la Fig. 2.

Etapa 4: Aislamiento del servicio interno de usuario mediante el uso de ID de VLAN

Un usuario puede realizar una VLAN en un dispositivo mediante configuración. Con el ID de usuario, la VLAN se limita a las interfaces dentro de los dispositivos marcados con el ID de usuario. En consecuencia, no interferirá con otro servicio de usuario. Un usuario puede también no utilizar VLAN y sólo transferir el servicio de VLAN de forma transparente.

El diagrama de flujo del procedimiento anterior se muestra en la figura. 3.

Una pluralidad de servicios pueden ser aislados de manera flexible por las técnicas descritas anteriormente, mostradas en la figura. 4.

5. Realización del formato de trama

Al cambiar un formato de trama Ethernet, la norma internacional se debería tener en cuenta ya que tanto la compatibilidad como la interconectividad deberían ser concernida. De otro modo, los dispositivos de diferentes fabricantes no podrán funcionar juntos. Si no hay una norma internacional específica, se deberían considerar problemas tales como formato compatible con MPLS y formato de VLAN apilable. Si un dispositivo se puede conectar a una pluralidad de diferentes dispositivos, las opciones de configuración se pueden establecer en las interfaces para soportar formatos diferentes. Las opciones de configuración de ID de usuario pueden incluir: no usar, usar el formato MPLS, usar el formato de VLAN apilable, y usar el formato personalizado.

Las figuras 5, 6 y 7 muestran los formatos opcionales de trama.

La figura 5 muestra el formato de trama de VLAN definido por el estándar IEEE 802.1Q, en el que 0x8100 es el ID de trama de VLAN, 0XXXXX son los datos del ID de VLAN, en los que P, C y V, P se refieren a las prioridades de 0-7; C es el tipo de LAN, 0 es Ethernet, 1 es el anillo testigo. V es el ID de VLAN con un valor de 0 a 4095.

La figura 6 muestra el formato de trama utilizado por VLAN apilable. 0x9100 es el ID de VLAN y apilables y 0XXXXX son los datos de la ID de VLAN, cuya definición es la misma que la del ID de VLAN. Todas los otros ajustes son iguales a los de la IEEE 802.1Q.

La figura 7 muestra el formato de trama MPLS definido por RFC2236. ID es el ID de MPLS. Exp es para el almacenamiento y el uso del ensayo. EOS muestra si está al final de la pila de MPLS. TTL es el tiempo de vida

REIVINDICACIONES

1.- Procedimiento para realizar aislamiento de seguridad de servicios de Ethernet, **caracterizado porque** comprende:

- 5 (1) añadir un segmento adicional en una trama Ethernet para identificar diferentes servicios de usuario, consistiendo el segmento en n bytes y teniendo n un valor ligado al formato del segmento;
- (2) introducir un servicio de usuario en redes de datos de un proveedor de servicios, y añadir un ID de usuario al segmento adicional de la trama Ethernet que soporta el servicio de usuario;
- (3) procesar conmutación/ruta; y
- 10 (4) borrar el ID de usuario y restablecer la trama Ethernet cuando el servicio de usuario sale de las redes de datos, en las cuales cuando el servicio de usuario es procesado en alguna interfaz física, el ID de usuario del servicio de usuario se compara con el ID de usuario de la interfaz física, si los dos ID coinciden, el servicio de usuario quedará garantizado, de otro modo se descartará el servicio.

15 2.- Procedimiento según la reivindicación 2, en el cual el servicio de usuario que entra en una interfaz física se marca con un cierto formato por un ID de usuario asignado a la interfaz física que conecta el servicio de usuario.

3.- Procedimiento según la reivindicación 1 o 2, en el cual en la etapa (3):

20 basado en los ID de usuario, se mantiene una única tabla de direcciones MAC para cada ID de usuario mediante el aprendizaje y la búsqueda de direcciones MAC; se genera un único árbol de expansión en la interfaz física incluida en cada ID de usuario para formar un puente virtual real; en dicho puente virtual, las direcciones MAC idénticas se pueden utilizar en tablas de direcciones MAC de diferentes ID de usuario.

4.- Procedimiento según la reivindicación 1, en el cual en la etapa 3):

se genera un único árbol de expansión para cada ID de usuario para evitar una tormenta de difusión.

5.- Procedimiento según la reivindicación 1, en el cual en la etapa 3):

25 los usos de ID de VLAN para diferentes ID de usuario están completamente aislados, y un usuario usa ID de VLAN para realizar el aislamiento de red interna.

6.- Procedimiento según la reivindicación 5, en el cual en la etapa 3):

30 en las interfaces físicas que conectan el servicio de usuario, el aislamiento de servicio interno se fija según que el ID de VLAN sea o no utilizado mediante la elección de vías de utilización del ID de VLAN a través de la gestión de red.

7.- Procedimiento según la reivindicación 1, en el cual en la etapa 3):

se proporciona un modo de servicio multidifusión única para cada ID de usuario, en el cual el modo de servicio de multidifusión comprende un modo de protocolo de multidifusión dinámica y un modo de configuración de multidifusión estática;

35 el modo de protocolo de multidifusión dinámica significa que una interfaz de servicio en el servicio de multidifusión es determinado por el protocolo de multidifusión dinámica, y el protocolo de multidifusión dinámica comprende el protocolo ICMP y el protocolo GMRP(Véase RFC 2236 e IEEE 802.1q);

el modo de configuración multidifusión estática determina la interfaz de servicios en el servicio de multidifusión por configuración manual del usuario mediante gestión de red.

40 8.- Procedimiento según la reivindicación 7, en el cual en la etapa 3) cada ID de usuario configura el modo de servicio de multidifusión por la gestión de red, y el modo de servicio a seleccionar incluye el modo de protocolo multidifusión dinámica y el modo de configuración multidifusión estática.

45 9.- Procedimiento según la reivindicación 1, en el cual en la etapa 2) un ID de usuario es asignado a cada interfaz física, cuando se introduce en la interfaz, se marca un servicio mediante un ID de usuario. El ID de usuario permanece sin cambios en toda la red hasta que el servicio salga de la interfaz y alcanza un dispositivo de usuario, y a continuación el ID se elimina y finalmente el servicio alcanza el dispositivo de usuario, con lo cual el servicio se transfiere de manera transparente.

10.- Procedimiento según la reivindicación 1, en el cual el segmento adicional en la trama de Ethernet usa un formato que incluye formato compatible con MPLS, formato VLAN apilable o formato personalizado para realizar una conexión entre una pluralidad de dispositivos.

5 11.- Procedimiento según la reivindicación 10, en el cual se establecen opciones de configuración en las interfaces físicas a través de la gestión de red para proporcionar formatos compatibles con MPLS, VLAN apilable y personalizados al segmentos adicional en la trama Ethernet.

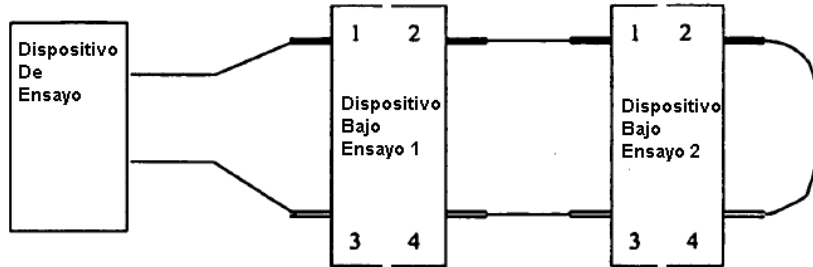


Fig. 1

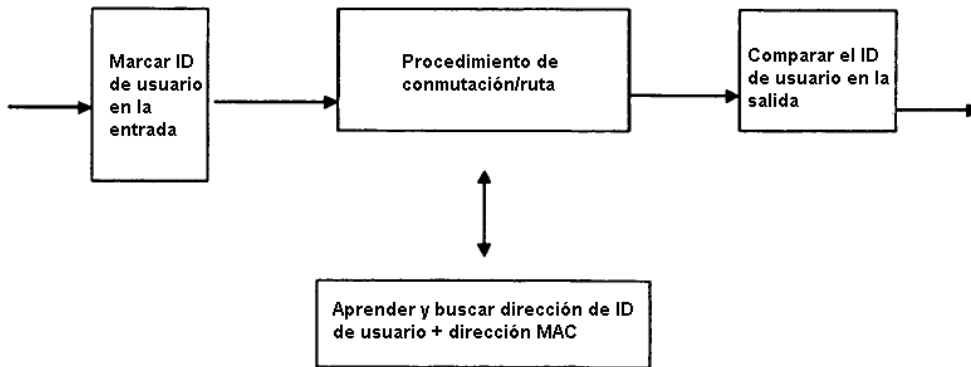


Fig. 2

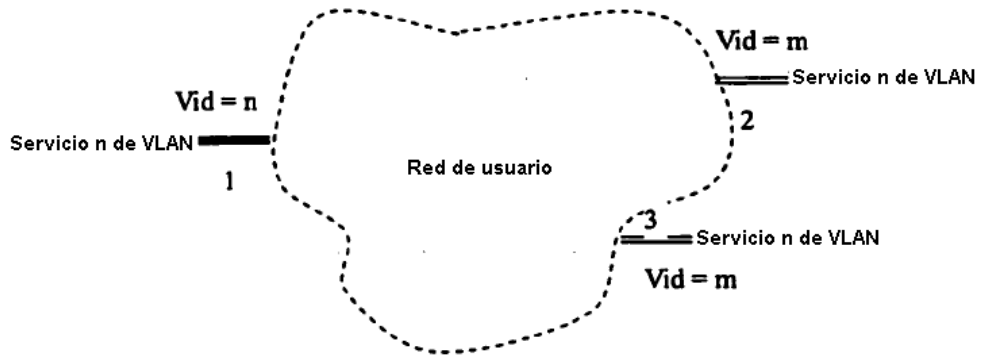


Fig. 3

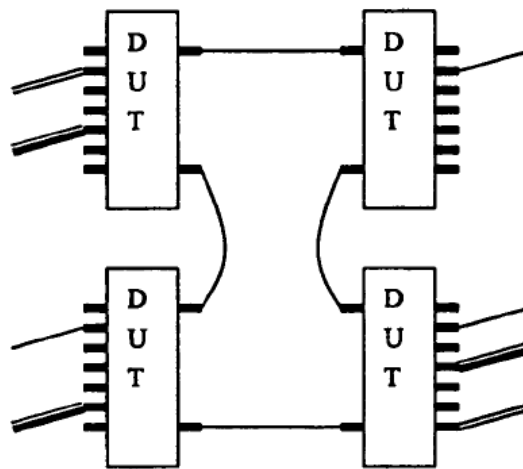


Fig. 4

Dirección destino (6)	Dirección fuente (6)	0x8100	0xXXXX
--------------------------	-------------------------	--------	--------

Formato interno 0xXXXXX.:

P	P	P	C	V	V	V	V	V	V	V	V	V	V	V	V
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Fig. 5

Dirección destino (6)	Dirección fuente (6)	0x9100	0xXXXX	0x8100	0xXXXX
--------------------------	-------------------------	--------	--------	--------	--------

Formato interno 0xXXXXX.:

P	P	P	C	V	V	V	V	V	V	V	V	V	V	V	V
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Fig. 6

Marca (20 bits)	EXP (3 bits)	EOS (1 bit)	TTL (8 bits)
-----------------	--------------	-------------	--------------

Fig. 7