(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 276 021**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03290242 .1**
(86) Fecha de presentación : **31.01.2003**
(87) Número de publicación de la solicitud: **1335565**
(87) Fecha de publicación de la solicitud: **13.08.2003**

(54) Título: **Procedimiento y dispositivo para el tratamiento de paquetes de datos.**

(30) Prioridad: **12.02.2002 FR 02 01705**

(45) Fecha de publicación de la mención BOPI:
**16.06.2007**

(45) Fecha de la publicación del folleto de la patente:
**16.06.2007**

(73) Titular/es: **FRANCE TELECOM**
**6, place d'Alleray**
**75015 Paris, FR**

(72) Inventor/es: **Paul, Olivier;**
**Gombault, Sylvain;**
**Laurent Maknavicius, Maryline;**
**Lattmann, Joel;**
**Duret, Christian y**
**Guesdon, Hervé**

(74) Agente: **Lehmann Novo, María Isabel**

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).



Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

## DESCRIPCIÓN

Procedimiento y dispositivo para el tratamiento de paquetes de datos.

La presente invención concierne a un procedimiento de tratamiento de paquetes de datos según reglas aplicadas a cada paquete de datos, en función de datos contenidos en ese paquete.

La misma concierne más particularmente a un procedimiento de configuración de un dispositivo de memoria particular utilizado para el tratamiento de paquetes de datos.

La solicitud de patente FR-A-2 812 491, publicada el 1ro de febrero de 2002, divulga un dispositivo de control de acceso para redes ATM. Ese dispositivo comprende un controlador de acceso que configura analizadores de tráfico para tratar una a una las células portadoras del tráfico ATM. Los analizadores de tráfico proceden por análisis del contenido de las células portadoras de tráfico ATM asociando sus referencias de encaminamiento por medio de una memoria asociativa de tipo Trie. Tales dispositivos pueden también ser utilizados en enrutadores IP, dispositivos de seguridad ("Firewall"), dispositivos de medida del tráfico, etc. Según esas aplicaciones, el tratamiento asignado a cada paquete de datos puede ser un direccionamiento de ese paquete, una modificación de datos de ese paquete, el registro de una información establecida a partir de ese paquete, o, de forma general, una acción determinada a partir del contenido de ese paquete.

El interés de la utilización de una memoria de tipo Trie es permitir un análisis rápido y en un orden cualquiera de partes de los contenidos de las células portadoras de tráfico. Tal memoria y su utilización en el análisis de paquetes de datos son descritas en la solicitud de patente EP-A-1 030 493 publicada el 23 de agosto de 2000.

La configuración de la memoria Trie es llevada a cabo al nivel del gestor de control de acceso.

Un objetivo de la presente invención es obtener una configuración de esta memoria que permite asignar un tratamiento apropiado a cada paquete de datos en función de partes de su contenido.

La invención propone un procedimiento de configuración de una memoria asociativa de tipo Trie para el tratamiento de paquetes de datos en función de un conjunto de reglas. La memoria Trie es utilizada para el análisis de cadenas binarias situadas en emplazamientos determinados de cada paquete de datos. Cada regla atribuye una acción a un paquete en función de los valores de dichas cadenas binarias. La memoria Trie comprende registros compuestos por un número determinado de células elementales para recibir referencias respectivas.

Según la invención, el procedimiento, definido en la reivindicación 1, comprende una etapa en el curso de la cual se traduce el conjunto de reglas en un árbol de análisis de los paquetes, comprendiendo nodos repartidos en etapas sucesivas respectivamente asociados a los emplazamientos considerados en un orden determinado, arcos, y hojas que corresponden a acciones atribuibles por las reglas. Cada arco tiene un nodo de partida y un punto de llegada que consiste en un nodo de la etapa siguiente de aquella del nodo de partida como una hoja. La primera etapa comprende un único nodo racimo. Cada arco del árbol está asociado a un campo de valores de cadena binaria que puede aparecer en el emplazamiento asociada a la etapa de su nodo de partida. El árbol de análisis define así caminos que consisten cada uno en una sucesión de n arcos, n siendo un número entero al menos igual a 1, tal que el punto de llegada de cada arco de un camino además del último arco sea el nodo de partida del arco siguiente de dicho camino, y que el punto de llegada del último arco del camino sea una hoja que corresponde a una acción atribuida después del conjunto de reglas a cada paquete que tiene, en los n emplazamientos respectivamente asociados a las etapas de los nodos de partida n arcos del camino, valores de cadena binaria que caen en los n campos respectivamente asociados a dichos arcos.

El procedimiento comprende además una etapa en el curso de la cual se asigna un grupo de registros de la memoria Trie que incluye un registro portador en cada nodo del árbol de análisis que pertenece a una etapa asociada a un emplazamiento, y se registra en las células de ese grupo de registros de las referencias de manera que analizando a partir del registro portador el valor de cadena binaria contenida en dicho emplazamiento en un paquete, se obtiene una referencia final que depende de qué campo contiene dicho valor entre los campos de valores asociados a los arcos que tienen dicho nodo como nodo de partida y de manera que:

- si el arco asociado al campo que contiene dicho valor tiene como punto de llegada una hoja que corresponde a una acción, la referencia final designa dicha acción como siendo atribuida al paquete, y

- si el arco asociado al campo que contiene dicho valor tiene otro nodo de la etapa siguiente como punto de llegada, la referencia final designa dicho otro nodo para proseguir analizando el valor de cadena binaria contenida en el paquete en el emplazamiento asociado a dicha etapa siguiente.

Tal modo de configuración de la memoria Trie ofrece una gran flexibilidad para tomar en cuenta una gran diversidad de reglas de clasificación del tráfico, que pueden corresponder a diversas acciones a emprender sobre los paquetes de datos en función del contenido de los emplazamientos analizados. Los caminos del árbol corresponden a gráficos de análisis que son recorridos por medio de operaciones de indización y de direccionamiento indirecto en la memoria Trie así configurada.

Tal organización de la estructura de análisis permite garantizar que la duración del análisis de un paquete de datos cualquiera está limitada por un límite superior fijado para el análisis considerado. Este límite corresponde a la altura del árbol de análisis, es decir al número de campos a analizar. Esto permite al operador de una red de comunicación que utiliza la invención realizar un tratamiento en tiempo real de los paquetes de datos que se presentan a la entrada del analizador de tráfico, otorgando medios de análisis suficientes.

Según la invención, el orden considerado en la etapa de construcción del árbol de análisis resulta ventajosamente de una clasificación de los emplazamientos operado después del inventario de intervalos elementales. Para cada uno de los emplazamientos, se definen intervalos elementales consecutivos que cubren valores de cadena binaria que pueden aparecer en este emplazamiento, cada intervalo elemental siendo tal que la acción atribuida por cada una de las reglas no sea modificada por un cambio, en el interior de dicho intervalo elemental, del valor de la cadena binaria situada en dicho emplazamiento en un paquete tratado. La clasificación de los emplazamientos es entonces operada en un orden tal que el emplazamiento para el cual el mayor número de intervalos elementales ha sido definido sea colocado de último. Se puede específicamente escoger los emplazamientos en el orden de los números crecientes de intervalos elementales.

Una ventaja de tales clasificaciones de emplazamiento reside en la minimización del tamaño de la memoria Trie necesaria para el análisis del contenido de cada paquete de datos, a partir del cual una acción es atribuida a cada paquete después del conjunto de reglas. Así, un gran número de paquetes de datos correspondientes a una variedad importante de acciones atribuidas a cada uno de ellos puede ser tratado con una operación única de análisis de los contenidos de esos paquetes.

En general, una memoria Trie se presenta bajo la forma de una tabla cuyas líneas, llamadas registros, comprenden un número fijo de células, por ejemplo 4, 8, 16 o 32 células. El tamaño de la memoria Trie corresponde entonces al número de registros de esta memoria. La presente invención permite por lo tanto reducir el número de registros necesarios para efectuar un análisis dado del contenido de los paquetes de datos.

El procedimiento de configuración de la memoria Trie de la invención comprende la trascripción del árbol de análisis en esta memoria bajo la forma de referencias inscritas en las células de la memoria. Un árbol de análisis voluminoso requiere en general una memoria Trie de tamaño tanto más grande. Es por consiguiente ventajoso concebir el árbol de análisis y su trascripción de forma de reducir el tamaño necesario de la memoria Trie.

El número de etapas de nodos del árbol de análisis corresponde al número de emplazamientos en el interior de los paquetes de datos en los cuales son leídas las cadenas binarias.

Se puede determinar un límite superior de la dimensión del árbol de análisis de la forma siguiente. La primera etapa del árbol de análisis comprende el nodo racimo como único nodo. La segunda etapa del árbol de análisis comprende un número de nodos a lo máximo igual al número de intervalos elementales definidos por el emplazamiento colocado en primer lugar según el orden retenido para los emplazamientos. El número de nodos de la tercera etapa del árbol de análisis es igual a lo máximo al producto de los dos números de intervalos elementales respectivamente definidos por los dos emplazamientos a los cuales están asociadas las dos primeras etapas de nodos. De forma recurrente, el número de nodos de una etapa cualquiera del árbol de análisis asociado a un emplazamiento dado es inferior o igual al producto de los números de intervalos elementales respectivamente definidos para todos los emplazamientos que preceden al emplazamiento al cual está asociada la etapa considerada según el orden de clasificación de los emplazamientos.

Si N designa el número de emplazamientos de cadenas binarias definidas en los paquetes de datos sobre los cuales está basado el análisis de los paquetes, el número de nodos de la última etapa del árbol de análisis es por lo tanto inferior al producto de los (N - 1) números de intervalos elementales correspondientes a los (N - 1) primeros emplazamientos según el orden de clasificación de los emplazamientos. Dicho de otra forma, es inferior al valor igual al producto de todos los números de intervalos elementales dividido por el número de intervalos elementales del último emplazamiento según este orden. Este valor constituye por lo tanto un límite superior al número de nodos de la última etapa del árbol de análisis, que corresponde a un límite superior del tamaño de la memoria Trie necesaria. Para intervalos elementales fijados para todos los emplazamientos, este límite superior es el más pequeño cuando el orden de clasificación de los emplazamientos es tal que está colocado en lo último de los emplazamientos para el cual el mayor número de intervalos elementales ha sido definido.

En ciertas aplicaciones del procedimiento según la invención, las cadenas binarias alojadas en dichos emplazamientos son números o valores que comprenden números. Es entonces particularmente cómodo definir los intervalos elementales respetando una relación de orden entre esos números, o utilizando una relación de orden adaptada a la estructura de los valores alojados, para permitir una configuración rápida de la memoria Trie.

En un modo de realización preferido del procedimiento según la invención, la traducción del conjunto de reglas en un árbol de análisis es tal que al menos un nodo del árbol de análisis sea el punto de llegada de varios arcos salidos de nodos de partida distintos de la etapa precedente. Ese modo de realización permite una compresión de las estructuras de clasificación definidas en la memoria Trie que provoca una ganancia espacial importante en esta memoria.

Para esto, se asocia en cada nodo del árbol de análisis además del racimo del árbol de análisis un sub-árbol. Este sub-árbol tiene un racimo constituido por dicho nodo y está compuesto por nodos, arcos y hojas reunidos a partir

de dicho nodo al lo largo de diferentes caminos que pasan por dicho nodo. La traducción del conjunto de reglas es entonces operado de forma tal que el árbol de análisis no incluye primer y segundo sub-árboles teniendo racimos distintos y tales que se puedan aparear sus nodos respectivos, sus arcos respectivos y sus hojas respectivas, de tal manera que cada nodo del primer sub-árbol sea apareado a un nodo del segundo sub-árbol perteneciendo a la misma etapa, que cada hoja del primer sub-árbol sea apareada a un a hoja del segundo sub-árbol correspondiente a una misma acción, y que dos arcos apareados de los primero y segundo sub-árboles tengan nodos de partida apareados y puntos de llegada apareados y que sean asociados al mismo campo de valores.

Según una formulación particular de las reglas del conjunto, cada regla es definida por una acción e intervalos de valores correspondientes respectivamente a algunos al menos de los emplazamientos, y atribuye dicha acción a los paquetes que tienen, en dichos emplazamientos, valores de cadenas binarias que caen respectivamente en dichos intervalos. Para un tratamiento genérico de todas las reglas, se ha recurrido a la siguiente precaución: cuando, para un emplazamiento dado, una regla no presenta intervalo explícito, un intervalo le es adicionado que corresponde a este emplazamiento y que comprende el conjunto de los valores de cadenas binarias que pueden ser alojadas en paquetes de datos en este emplazamiento.

Para una formulación tal de las reglas, se asocia un subconjunto de reglas de cada nodo de un punto (p+1)esima etapa del árbol de análisis, p siendo un número entero mayor que 0. Dicho subconjunto está compuesto por reglas del conjunto tales que cada intervalo de valores corresponde a un emplazamiento asociado a una de las p primeras etapas del árbol teniendo un recubrimiento no vacío con el campo de valores asociado al arco de cada camino que pasa por dicho nodo y que tiene su nodo de partida en dicha etapa.

Se asocia al nodo racimo un subconjunto constituido por el conjunto de las reglas.

La traducción del conjunto de reglas comprende entonces las etapas siguientes, para cada nodo de la p-esima etapa asociada a un primer subconjunto de reglas:

- determinar campos de valores que cubren valores de cadena binaria que pueden aparecer en el p-esimo emplazamiento según dicho orden, cada campo siendo tal que la acción atribuida para cada una de las reglas del primer subconjunto no sea modificada por un cambio, en el interior de dicho campo, del valor de la cadena binaria situada en el p-esimo emplazamiento en un paquete tratado; y

- para cada uno de dichos campos de valores:

  - generar un arco asociado a dicho campo, que tiene dicho nodo de la p-esima etapa por nodo de partida;

  - detectar cada regla del primer subconjunto que es definida por al menos un intervalo de valores que incluye dicho campo;

  - si ninguna regla es detectada, asignar una hoja del árbol correspondiente a una acción por defecto como punto de llegada de dicho arco;

  - si para cada regla detectada, ningún intervalo de valores corresponde a uno cualquiera de los emplazamientos siguiendo el p-esimo emplazamiento según dicho orden, asignar una hoja del árbol correspondiente a una acción de una regla detectada como punto de llegada de dicho arco;

  - si para al menos una regla detectada, un intervalo de valores corresponde a uno de los emplazamientos siguiendo el p-esimo emplazamiento según dicho orden, asignar un nodo de la (p+1)esima etapa del árbol como punto de llegada de dicho arco, dicho nodo de la (p+1)esima etapa estando asociado a un segundo subconjunto compuesto por reglas detectadas del primer subconjunto.

Prioridades pueden ser respectivamente otorgadas a las reglas del conjunto. En ese caso, cuando varias reglas son detectadas y cada uno de sus intervalos de valores no corresponden a uno de los emplazamientos siguiendo el p-esimo emplazamiento, la acción correspondiente a la hoja del árbol asignada a dicho arco es aquella de una de las reglas detectadas, seleccionada sobre la base de las prioridades otorgadas.

A fin de evitar que el árbol de análisis no comprenda sub-árboles que tengan racimos respectivos distintos y donde se puede aparear, entre ellos, los nodos, arcos y hojas que pertenecen respectivamente a cada uno de ellos, se ejecutan las etapas siguientes cuando se ha detectado al menos una regla que tiene un intervalo de valores que corresponde a uno de los emplazamientos siguiendo el p-esimo emplazamiento:

- buscar si ya ha sido generado un nodo de la (p+1)esima etapa del árbol asociada al segundo subconjunto;

- si la búsqueda se detiene, generar un nodo tal en la (p+1)esima etapa;

- si la búsqueda identifica un nodo de la (p+1)esima etapa, asignar el nodo identificado como punto de llegada de dicho arco.

La presente invención concierne también a un dispositivo de tratamiento de paquetes de datos definido en la reivindicación 11, que comprende una memoria asociativa de tipo Trie y un controlador adaptado para llevar a cabo un procedimiento de configuración de la memoria Trie tal como el definido anteriormente. Esos dispositivos pueden específicamente ser utilizados en las aplicaciones siguientes.

- el encaminamiento por una red de comunicación de paquetes de datos en función de reglas de encaminamiento aplicadas a paquetes;

- el control de acceso a una red de comunicación por paquetes de datos en función de reglas de control de acceso a esa red aplicados a esos paquetes;

- la adquisición de informaciones concernientes a los paquetes de datos transmitidos por una red de comunicación.

Los paquetes de datos pueden ser específicamente de células ATM portadoras de tramas AAL 5 o de los paquetes IP.

Otras particularidades y ventajas del procedimiento de la presente invención aparecerán en la descripción a continuación de ejemplos de realización no limitativos, con referencia a los dibujos anexos, en los cuales:

- la figura 1 es un esquema sinóptico de un dispositivo de control de acceso en el cual es realizado el procedimiento de la invención;

- la figura 2 es una tabla que describe las informaciones tratadas por los analizadores de tráfico del dispositivo de la figura 1;

- la figura 3 representa un árbol de análisis resultante de dos reglas particulares aplicadas a pares de números (x, y), y que no utiliza la presente invención;

- la figura 4 representa un segundo árbol de análisis correspondiente a las reglas dadas para el árbol de análisis de la figura 3, utilizando la clasificación de los emplazamientos según la presente invención;

- la figura 5 representa un árbol de análisis que resulta de tres reglas particulares aplicadas a tripletes de números (x, y, z), y que no utiliza la presente invención;

- la figura 6 representa un segundo árbol de análisis correspondiente a las reglas dadas para el árbol de análisis de la figura 5, utilizando la clasificación de los emplazamientos según la presente invención;

- la figura 7 representa un tercer árbol de análisis correspondiente a las reglas dadas para el árbol de análisis de la figura 5, utilizando además reagrupamientos de sub-árboles según la presente invención;

- la figura 8 es un esquema sinóptico de las etapas de creación de un nuevo arco según el modo de realización preferido del procedimiento de la invención;

- la figura 9 representa un cuarto árbol de análisis correspondiente a las reglas dadas para el árbol de análisis de la figura 5, utilizando la clasificación de los emplazamientos y el método de creación de los arcos de la figura 8.

La estructura de un dispositivo de control de acceso dispuesto entre dos redes de transmisión ATM ("Asynchronous Transfert Mode"), en el cual puede ser llevado a cabo el procedimiento de la presente invención, es descrito en detalle en la solicitud de patente WO 0209367, publicada el 31 de enero de 2002. Como es indicado en la figura 1, un dispositivo de control de acceso puede estar compuesto por dos partes principales 1,2 que cooperan con un conmutador ATM 3. La primera parte 1 está dedicada a la toma en cuenta de una política de control de acceso y al análisis de la señalización ATM. El resultado de este análisis es utilizado para construir dinámicamente una configuración. Esta es utilizada por la segunda parte 2 para proporcionar un servicio de control de acceso basado en las informaciones transportadas en las células ATM. Esta segunda parte 2 es capaz de recuperar las informaciones de nivel ATM, IP y transporte a fin de decidir si una comunicación debe ser autorizada o prohibida. La configuración del conjunto se realiza por medio de un lenguaje único.

La parte 1 puede ser realizada por medio de una estación de trabajo, tal como una estación comercializada por la sociedad Sun Microsystem, Inc. El analizador de señalización 4 es el elemento de esta parte 1 que efectúa las acciones de control de acceso al nivel de la señalización ATM en combinación con el gestor de control de acceso 7.

La parte 2 puede ser realizada por medio de una estación de tipo PC que funciona por ejemplo con el sistema de explotación Solaris x86. Esta estación está equipada con tarjetas 20, 21 de análisis en tiempo real de las células ATM, o analizadores de tráfico, a continuación llamadas tarjetas IFT ("IP Factor Translator"), que aseguran las acciones de control de acceso célula ATM por célula ATM.

A fin de permitir la expresión de políticas de control de acceso, se utiliza un Lenguaje de Definición de Política de Control de Acceso (ACPDL, "Access Control Policy Description Language"). La definición de la ACPDL está basada en el Lenguaje de Descripción de Política (PDL) en curso de definición en el seno del grupo de trabajo que trabaja sobre las políticas en la IETF (ver J. Strassner, y otros, "Policy Framework Definition Language", draft-ietf-policy-framework-pfdl-00.txt, Internet Engineering Task Force, 17 noviembre 1998). En ese lenguaje, una política es definida por un conjunto de reglas, cada regla estando constituida por un conjunto de condiciones y por una acción que es ejecutada cuando el conjunto de condiciones es cumplido. La expresión siguiente (expresada en el formalismo Backus Naur, BNF) describe la forma general de una regla:

Regla ::= IF <Conditions> THEN <Action>

Todas las condiciones tienen la misma estructura genérica expresada a continuación por medio del formalismo BNF:

Condition ::= <ACCESS CONTROL PARAMETER> <RELATIONAL OPERATOR> <VALUE>

En función del nivel en la pila de protocolo, varios tipos de parámetros de control de acceso pueden ser utilizados:

- al nivel ATM, los parámetros interesantes son descritos en el artículo de O. Paul, y otros, "Manageable parameters to improve access control in ATM networks", HP-OVUA Workshop, Rennes, Francia abril de 1998. Entre estos, se puede seleccionar el tipo de tráfico, los identificadores de conexión, las informaciones de direccionamiento, los descriptores de QoS y los descriptores de servicio;

- al nivel de transporte, la mayor parte de los parámetros considerados son aquellos que son utilizados habitualmente para realizar la filtración de los paquetes en los enrutadores filtrantes (por ejemplo las informaciones de direccionamiento, los puertos fuente y destino, los revestimientos en el caso de las conexiones TCP, etc.);

- al nivel de aplicación, dos parámetros genéricos son considerados: el identificador del usuario de la aplicación así como el estado de aplicación;

- informaciones temporales son igualmente incluidas a fin de especificar cuando una regla debe ser aplicada.

Las acciones tienen igualmente una estructura genérica (notación BNF):

Action ::= <ACTION> <ACTION LEVEL> <LOG LEVEL>

Una acción se descompone en tres partes. La primera indica si la comunicación descrita por las condiciones debe ser autorizada o prohibida. El parámetro <ACTION LEVEL> corresponde a la capa protocolar en la cual debe ser efectuada la acción. La última parte describe la importancia acordada al evento de control de acceso y permite la clasificación de los resultados.

El siguiente párrafo muestra como el lenguaje ACPDL puede ser utilizado a fin de expresar un ejemplo de servicio de control de acceso. En este ejemplo, cada equipo es identificado por su dirección fuente (IP_SRC_ADDRESS) y su dirección destino (IP_DST_ADDRESS). El servicio WWW es identificado por los puertos fuente (SRC_PORT) y destino (DST_PORT). La segunda línea de accionamiento dada en el ejemplo es utilizada para prohibir las solicitudes de conexión sobre el puerto WWW de una estación interna.

```
IF (IP_SRC_ADDRESS = 192.165.203.5 255.255.255.255) AND
(IP_DST_ADDRESS = 0.0.0.0 0.0.0.0) AND (SRC_PORT > 1023)
AND (DST_PORT = 80) THEN PERMIT TRANSP_CONNECTION;
IF (IP_SRC_ADDRESS = 0.0.0.0 0.0.0.0) AND
(IP_DST_ADDRESS = 192.165.203.5 255.255.255.255) AND
(SRC_PORT = 80) AND (DST_PORT > 1023) AND (TCP_FLAG <>
SYN) THEN PERMIT TRANSP_CONNECTION ;
```

La política de control de acceso es definida por el oficial de seguridad por medio de una interfase hombre-máquina (IHM) 6 de la estación 1, utilizando el lenguaje ACPDL. La misma es utilizada para configurar las dos partes del controlador. Sin embargo esta política no puede ser utilizada directamente para las dos herramientas de control de acceso 4, 20/21. El gestor 7 es el módulo que permite resolver ese problema traduciendo la política de control de acceso en órdenes de configuración para las dos herramientas.

Ese proceso de traducción puede ser dividido en dos partes principales. La primera es la traducción de la política en tres configuraciones estáticas:

- al nivel de la señalización ATM, esta configuración comprende una descripción de las comunicaciones que deben ser controladas. Cada comunicación es descrita por un conjunto de elementos de información (IE) y por una acción (Autorizar o Prohibir). Esta configuración es enviada al analizador de señalización 4;

- al nivel TCP/IP la configuración comprende una descripción de los paquetes que deben ser controlados. Esta parte de la política puede ser genérica, lo que significa que las reglas que son descritas no son dedicadas a una conexión ATM particular. Esta parte puede también ser anexada a una conexión ATM por la expresión de condiciones que portan sobre los identificadores de conexión;

- al nivel célula ATM, la configuración comprende una descripción de las células ATM que deben ser controladas. Esas células son divididas según campos que las mismas pueden contener. El conjunto de los valores que cada campo puede tomar es descrito por un árbol. Esta configuración es enviada a las tarjetas IFT 20, 21.

La segunda parte del proceso de configuración tiene lugar cuando una solicitud de conexión es recibida por el analizador de señalización 4. Una vez que el proceso de control de acceso ha sido realizado, el analizador de señalización 4 envía al gestor 7 las informaciones necesarias para efectuar la configuración dinámica de las tarjetas IFT 20, 21. Las informaciones proporcionadas por el analizador de señalización 4 comprenden:

- los identificadores de conexión VPI y VCI ("Virtual Path Identifier", "Virtual Channel Identifier");

- las direcciones ATM fuente y destino;

- un descriptor de servicio (Classical IP over ATM (CLIP), Applications natives ATM). Cuando una capa adicional es utilizada por encima del modelo ATM, el analizador de señalización 4 proporciona igualmente la encapsulación (con o sin encabezamiento SNAP/LLC);

- la dirección de la comunicación.

En un ambiente CLIP, el gestor 7 utiliza las direcciones ATM fuente y destino para encontrar las direcciones IP correspondientes. Esta traducción es efectuada por medio de un fichero que describe las correspondencias entre direcciones IP y ATM. La misma puede también utilizar un servidor de resolución de dirección (ATMARP).

El gestor 7 trata a continuación de encontrar una correspondencia entre las direcciones IP y las reglas genéricas de control de acceso de nivel TCP/IP. El subconjunto de reglas obtenido es instanciado con las direcciones IP y asociado a las otras informaciones (direcciones, encapsulación, identificadores de conexión, dirección). Este conjunto de informaciones es utilizado por el gestor a fin de construir el árbol de análisis que será utilizado para configurar las tarjetas IFT, y es conservado durante toda la vida de la conexión. Al cierre de la conexión, el gestor 7 recibe una señal del analizador de señalización 4 para reconfigurar eventualmente las tarjetas IFT 20, 21 borrando las informaciones relativas a la conexión. El gestor destruye seguidamente las informaciones asociadas a la conexión.

El analizador de señalización 4 reposa en dos funciones. La primera es la dirección de los mensajes de señalización que provienen de las redes interna y externa hacia un filtro que pertenece al analizador 4. La segunda es la capacidad de descomponer los mensajes de señalización según la especificación UNI 3.1 de la ATM Forum ("ATM User-Network Interface Specification, Versión 3.1", ATM Forum, Julio 1994) y transmitir o suprimir esos mensajes en función de la configuración de control de acceso proporcionada por el gestor 7.

La estación 1 está provista con dos tarjetas de interfase ATM 8, 9 respectivamente unidas a dos interfases 12, 13 del conmutador 3. Las otras interfases representadas del conmutador 3 son denotadas 10 (red interna), 11 (red externa), 14 y 15 (tarjetas IFT 20 y 21).

Para redirigir la señalización, el conmutador ATM3 es configurado de forma de dirigir los mensajes de señalización hacia la estación 1. Esta configuración puede ser realizada desactivando el protocolo de señalización sobre las interfases 10, 11, 12 y 13. Un canal virtual (VC) debe ser seguidamente construido entre cada par de interfases para cada canal de señalización. Los canales de señalización son por ejemplo identificados por un identificador de canal virtual (VCI) igual a 5.

Con la configuración precedente, los mensajes de señalización que provienen de la red externa son dirigidos hacia la interfase 13 de la estación 1 mientras que los mensajes que provienen de la red interna son dirigidos hacia la interfase 12.

Cuando los mensajes de señalización son recibidos por el analizador de señalización 4, estos son descompuestos en elementos de información según la especificación UNI 3.1. Los elementos de información son seguidamente descompuestos en informaciones elementales tales como las direcciones, los identificadores de conexión, la referencia de llamada, los descriptores de servicio y los identificadores de servicio. El analizador 4 busca seguidamente si el mensaje puede estar asociado a una conexión existente por medio del tipo de mensaje y de la referencia de llamada. Si

la conexión es nueva, un descriptor de conexión que contiene esas informaciones es construido. Cuando la conexión existe ya, el descriptor de conexión es actualizado. El descriptor de conexión está asociado al estado de la conexión y a la interfase de origen. Este es identificado por un identificador de conexión. El descriptor es seguidamente enviado al filtro del analizador de señalización 4 a fin de ser analizado.

Cuando el filtro del analizador de señalización 4 recibe un descriptor de conexión, compara los parámetros que describen la conexión con el conjunto de las comunicaciones descritas por la política de control de acceso. Si una correspondencia es encontrada, el filtro aplica la acción asociada a la comunicación. En el caso contrario, aplica la acción por defecto que es prohibir la conexión. Cuando la acción consiste en una prohibición, el filtro destruye el descriptor de conexión. En el caso contrario, envía el descriptor de conexión a un módulo de construcción de los mensajes. Cuando el descriptor de conexión indica que un mensaje CONNECT ha sido recibido, un subconjunto de los parámetros del descriptor de conexión es enviado al gestor 7 como se indicó anteriormente:

- los identificadores de conexión VPI/VCI, obtenidos a partir del IE “Connection Identifier”;
- las direcciones ATM fuente y destino, proporcionadas por las IE “Called Party Identifier” y “Calling Party Identifier”;
- los descriptores de servicio, obtenidos a partir de las IE “Broadband Higher Layer Identifier (BHLI)” y “Broadband Lower Layer Identifier (BLLI)”;
- la dirección, proporcionada por el número de interfase asociada al descriptor de conexión.

Cuando el descriptor de conexión indica la recepción de un mensaje RELEASE_COMPLETE, que completa la liberación de una conexión, el descriptor de conexión es de nuevo enviado al gestor 7. Las comunicaciones entre el gestor 7 y el filtro de señalización pueden hacerse de forma clásica por medio de un segmento de memoria compartido y de señales.

Las tarjetas IFT consideradas aquí para la realización de la invención son del tipo descrito en la solicitud europea EP1030493 depositada el 9 de febrero 2000 por la solicitante, y publicada el 23 de agosto 2000. Las mismas están basadas en la utilización de una memoria asociativa de tipo Trie para el análisis de partes del contenido de células ATM, y para la atribución, a cada célula de una misma trama, de una acción definida por la política de control de acceso. Esas tarjetas poseen las características remarcables siguientes:

- permiten el análisis de la primera célula de cada trama AAL5 (“ATM Adaptation Layer no. 5”) y la modificación de las células correspondientes en función del análisis;
- pueden funcionar a la velocidad de 622 Mbits/s gracias a un procedimiento rápido y flexible de análisis;
- el plazo introducido por el análisis puede ser limitado y depende de la configuración de la tarjeta;
- pueden ser configuradas dinámicamente sin interrumpir el proceso de análisis;
- son integrables en equipos de tipo PC bajo Solaris.

La figura 2 describe las informaciones que pueden ser analizadas por las tarjetas IFT 20, 21 en el caso de los protocolos CLIP (CLIP1) y CLIP sin encapsulación SNAP-LLC (CLIP2). Las cámaras UD y TD indican el comienzo de los segmentos de datos para los protocolos UDP y TCP, respectivamente. Esto significa que, en el caso general, las tarjetas IFT tienen acceso a las informaciones de nivel ATM, IP, TCP, UDP y en algunos casos de nivel de aplicación. Sin embargo es necesario notar que los campos opcionales que pueden encontrarse en el paquete IP no son representados. La presencia de esos campos (de longitud variable) puede rechazar las informaciones de nivel TCP o UDP en la segunda célula ATM.

Como en el caso de la señalización, la primera parte del proceso de control de acceso al nivel de célula ATM consiste en redirigir el tráfico que proviene de las redes interna y externa hacia las tarjetas IFT 20, 21. Sin embargo, en ese caso, la configuración debe preservar la configuración realizada para el control de la señalización. A modo de ejemplo, los canales virtuales identificados por un valor de VCI igual a 31 son voluntariamente dejados libres para permitir al conmutador ATM 3 rechazar las células ATM que pertenecen a una comunicación que debe ser prohibida. El conmutador ATM 3 es entonces configurado a fin de crear un canal virtual para cada valor de VCI diferente de 5 y de 31 entre cada par de interfase (10, 14) y (11, 15).

Las tarjetas IFT consideradas solamente permiten el análisis de flujos unidireccionales. Esto significa que los flujos que provienen de las redes interna y externa deben estar separados. Esta operación es particularmente simple en el caso de una capa física de tipo Mono Modo Fiber utilizada por las tarjetas ya que las fibras de emisión y de recepción están físicamente separadas.

La segunda parte del proceso de control de acceso es la configuración de las tarjetas IFT 20, 21 para que las mismas proporcionen el servicio de control de acceso deseado. Como es indicado precedentemente, esta configuración

es realizada por el gestor 7. Las tarjetas IFT han sido concebidas al principio para ser administradas a distancia por varios gestores. Un soporte lógico apropiado 27 (demo RPC) es entonces utilizado en la estación 2 para poner en serie las solicitudes dirigidas al circuito de accionamiento 28 (driver) de las tarjetas 20, 21. Del lado del gestor 7, una librería da acceso a las funciones de configuración. Esta librería traduce las llamadas locales en llamadas a distancia en la estación 2. Las comunicaciones entre los dos equipos se hace por ejemplo a través de de una red dedicada de tipo Ethernet.

La configuración de las memorias Trie de las tarjetas 20, 21 se basa en una descripción de las comunicaciones a controlar bajo la forma de árboles. Cada rama del árbol describe el valor codificado de una cadena binaria, por ejemplo de 4 bits, que puede ser encontrada durante el proceso de análisis. Ese proceso consiste en recorrer la porción de célula ATM a analizar por rodajas de 4 bits sucesivas que sirven para acceder al contenido de la memoria Trie incluso en cada tarjeta IFT. Un árbol de análisis, construido a partir de una instrucción de control de acceso proporcionado por el gestor 7, corresponde a un encadenamiento dado de rodajas de 4 bits encontrados en emplazamientos determinados recorriendo la célula ATM. El racimo del árbol corresponde a un portero que es reconocido para comenzar el análisis del árbol. Ejemplos de árboles de análisis y de configuraciones resultantes de memorias Trie de tarjetas IFT son ahora presentadas.

De forma general, cada emplazamiento a analizar, o campo, comprende un número de bits fijo para la dimensión de ese campo, por ejemplo 32 bits. Su análisis por rodajas es efectuado de forma de que los valores que puede revestir cada lonja corresponde a las células elementales de uno o varios registros de la memoria Trie utilizada. Un cuarteto que puede tomar $2^4$=16 valores, es específicamente adaptado a una memoria Trie donde cada registro comprende 16 células elementales. Varios registros, incluso un gran número de registros, son entonces necesarios para el análisis de un campo, según la dimensión de ese campo con relación al número de células elementales de un registro.

El análisis de un campo comprende en general los análisis de un gran número de rodajas de bits, encadenados sucesivamente hasta la siguiente por el análisis de otro campo de la misma trama, o hasta la obtención de una acción atribuida a la trama analizada por la política de control de acceso. Por cuestiones de simplicidad y de claridad de ilustración de la invención, aunque esto no corresponde a una situación real, los ejemplos presentados a continuación solo comprenden cada uno un solo cuarteto para cada campo sobre el cual se hace el análisis. Por las mismas razones de simplicidad y de claridad, el número de reglas consideradas y el número de campos tomados en consideración para el análisis son muy reducidos, mientras que una política de control de acceso real puede comprender numerosas reglas de acceso que inducen a un gran número de campos de información de control de protocolo.

Un primer ejemplo es dado para los dos campos x y y leídos en las células ATM, representados por pares (x, y). Las cadenas binarias leídas en los campos x y y son cuartetos representados por números hexadecimales comprendidos entre 0 y F.

Las reglas consideradas, en número de dos, son las siguientes:

- Regla Re1: si $x \geq 7$ y $3 \leq y \leq 8$, entonces se efectúa una acción A1;

- Regla Re2: si $2 \leq x \leq B$ y $y \geq 3$, entonces se efectúa una acción A2.

La regla Re1 es supuesta prioritaria con relación a la regla Re2, aunque la acción A1 es efectuada solo cuando la misma es atribuida simultáneamente a la acción A2 a un mimo par (x, y), respectivamente para cada regla. Si la condición de alguna de las dos reglas Re1 y Re2 no es satisfecha por un par (x, y) dado, entonces una acción por defecto O es atribuida a ese par.

Las acciones A1, A2 y O pueden ser simples acciones de rechazo (“DENY”) o de aceptación (“PERMIT”) de las tramas. Las mismas pueden también corresponder a acciones más complejas, tal como el seguimiento del control de acceso por el examen de otros parámetros tales como campos autorizados atribuidos a un destinatario de la trama considerada.

La acción de rechazo o de aceptación es codificada por medio de un nodo particular que provoca el fin del análisis y reenvía el identificador de conexión que será atribuido a todas las células de la trama AAL 5 correspondiente. La acción “DENY” es codificada dirigiendo la trama hacia el canal no configurado (VCI 31) al nivel del conmutador 3. El VCI 31 es así utilizado como cesto de basura VCI para botar todas las células ATM no conformes a la política de seguridad. La acción “PERMIT” es codificada dejando el identificador de conexión sin cambio.

El conjunto de números que pueden ser leídos en el campo x es repartido por las reglas Re1 y Re2 según los 4 intervalos siguientes: $x < 2$, $2 \leq x < 7$, $7 \leq x \leq B$ y $x > B$. De forma análoga, el conjunto de números pueden ser leídos en el campo y está repartido según los 3 intervalos siguientes: $y < 3$, $3 \leq y \leq 8$ y $y > 8$.

Un árbol de análisis que resulta de la aplicación de dos reglas Re1 y Re2 a los pares (x, y) es representado en la figura 3, analizando primero el valor de x, y luego el valor de y. El nodo racimo 100 representa el punto de partida del análisis de los pares (x, y). Tres nodos 101, unidos cada uno al nodo racimo 100 por un arco 130, corresponde a resultados del análisis del valor de x con relación a los 4 intervalos identificados para x. Nodos 102, u hojas del árbol de análisis, unidos a los nodos 101 por arcos 131, corresponden respectivamente por los resultados precedentes

del análisis del valor de x a los resultados del análisis del valor de y con relación a los 3 intervalos identificados para y. Para algunos valores de x, por ejemplo $x < 2$, el análisis de los pares (x, y) no necesita análisis del valor de y para determinar la acción atribuida por las reglas Re1 y Re2. En ese caso, un arco 131 une directamente una hoja 102 al nodo racimo 100. En otros casos, $2 \leq x < 7$ y $x > B$, el análisis del valor de y no hace intervenir todos los límites de intervalos definidos para y. En efecto, algunos intervalos definidos para y pueden ser reunidos cuando estos corresponden a las mismas acciones respectivas atribuidas por las dos reglas.

Líneas 110 y 111 indican respectivamente las hojas 102 para las cuales la acción A2 y/o la acción A1 es atribuida por las reglas Re2 y Re1, consideradas separadamente. En fin, en función de la prioridad de esas acciones, una línea 120 indica la acción AA que corresponde a cada hoja 102 resultante de la aplicación de las dos reglas Re1 y Re2 combinadas. Así, la línea 120 retoma la línea 111 completándola por la acción A2 para aquellas hojas 102 para las cuales la línea 110 atribuye la acción A2 mientras que la línea 111 no le atribuye ninguna acción. Además, la línea 120 atribuye la acción por defecto O a las hojas 102 consideradas en cada una de las líneas 110 y 111.

Se utiliza una memoria Trie cuyos registros sucesivos R0, R1, R2, ... comprenden todos seis células elementales. Un ejemplo de configuración de esta memoria Trie correspondiente al árbol de análisis de la figura 3 es el siguiente:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R0 | O | O | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 |
| R1 | O | O | O | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R2 | O | O | O | A1 | A1 | A1 | A1 | A1 | A1 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R3 | O | O | O | A1 | A1 | A1 | A1 | A1 | A1 | O | O | O | O | O | O | O |
| R4 | | | | | | | | | | | | | | | | |
| R5 | | | | | | | | | | | | | | | | |

En esta configuración de la memoria Trie, el registro portero R0 es atribuido al análisis del valor de x, y los registros R1, R2 y R3 al análisis del valor de y. R0 es por lo tanto el registro por el cual el análisis de cada par (x, y) es comenzado. Según el valor de x del par (x, y) analizado, el registro R0 reenvía a uno de los registros R1, R2 o R3 para el seguimiento del análisis. Este último registro indica entonces, en función del valor de y del par (x, y) analizado, la acción a efectuar asociada a la hoja 102 del árbol de análisis en la cual termina el camino que corresponde a los resultados sucesivos de los análisis de x y y. Según esta configuración, 4 registros de memoria Trie son necesarios para permitir el análisis de todos los pares posibles (x, y).

Analizando primero el valor y, y luego el valor x, para la aplicación de las mismas reglas Re1 y Re2, se obtiene un árbol de análisis tal como el representado en la figura 4. Referencias idénticas entre las figuras 3 y 4 corresponden a significados idénticos. En la figura 4, los nodos intermedios 103 corresponden a los resultados del análisis del valor de y, efectuado primero, cuando el análisis del valor de x debe ser efectuado seguidamente. Para cada par de números (x, y), este árbol indica un mismo resultado de aplicación de las reglas Re1 y Re2, bajo la forma de la acción AA indicada por la línea 120.

Aplicando, a partir el árbol de análisis de la figura 4, el mismo método que precedentemente para la configuración de la memoria Trie, se obtiene:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R0 | O | O | O | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| R1 | O | O | A2 | A2 | A2 | A2 | A2 | A1 | A1 | A1 | A1 | A1 | A1 | A1 | A1 | A1 |
| R2 | O | O | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | O | O | O | O |
| R3 | | | | | | | | | | | | | | | | |
| R4 | | | | | | | | | | | | | | | | |

Así, la clasificación según la invención de los dos emplazamientos x y y permite, en este ejemplo, reducir en un registro el tamaño de la memoria Trie necesaria para permitir la aplicación de las mismas reglas de tratamiento.

Un segundo ejemplo concierne a un conjunto de reglas aplicadas a tripletes de números (x, y, z) cada uno de esos números siendo también un número hexadecimal:

- Regla Re1: si $x \geq A$ y $3 \leq z \leq 8$, entonces se efectúa una acción A1;

- Regla Re2: si $x > 5$ y $2 \leq y \leq 9$ y $z \geq 6$, entonces se efectúa una acción A2;

- Regla Re3: si $3 \leq x \leq C$, entonces se efectúa una acción A3.

En este ejemplo la relación de prioridad entre las tres reglas es: Re2 > Re1 > Re3. Sólo la acción más prioritaria es finalmente asignada a cada triplete, entre las acciones atribuidas para cada una de las tres reglas. Una acción por defecto O es también atribuida a una tripleta (x, y, z) que satisface las condiciones de alguna de las tres reglas.

Estas tres reglas definen 5 intervalos para el campo x: $x < 3$, $3 \leq x \leq 5$, $5 < x < A$, $A \leq x \leq C$, y $x > C$, 3 intervalos para el campo y : $y < 2$, $2 \leq y \leq 9$, y $y > 9$, y 4 intervalos para el campo z : $z < 3$, $3 \leq z < 6$, $6 \leq z \leq 8$, y $z > 8$.

La figura 5 representa un árbol de análisis correspondiente a las tres reglas Re1, Re2 y Re3 precedentes, analizando primero el valor de x, y luego el valor de y, y finalmente el valor de z. Este árbol de análisis es construido de la misma forma que los árboles de las figuras 3 y 4. Las referencias 100 y 120 poseen los significados ya introducidos. Nodos 104 corresponden a los resultados del análisis del valor de x que no permiten determinar directamente la acción indicada para cada regla, a saber $5 < x < A$, $A \leq x \leq C$ y $x > C$. Igualmente, nodos 105 que corresponden a los resultados del análisis del valor de y cuando el análisis de los tripletes debe ser todavía continuado para el análisis del valor de z. Según los caminos, las hojas 106 del árbol de análisis están unidas por arcos directos a los nodos 100, 104 o 105.

Líneas 112, 113 y 114 indican, para cada una de las hojas 106, las acciones respectivamente indicadas para cada una de las tres reglas, tomadas en el orden de prioridad creciente. Una línea 120 designa la acción final asignada a cada tripleta (x, y, z) en función de la prioridad entre las acciones indicadas por las tres reglas.

Se utiliza, por ejemplo, también una memoria Trie de seis células elementales por registro. En ese caso, la configuración de la memoria Trie, según ese primer árbol de análisis, necesita tantos registros como nodos 100, 104 o 105, o sea 9 registros en total.

Un ejemplo de configuración de esta memoria Trie correspondiente al árbol de análisis de la figura 5 es el siguiente:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R0 | O | O | O | A3 | A3 | A3 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 6 | 6 | 6 |
| R1 | A3 | A3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A3 | A3 | A3 | A3 | A3 | A3 |
| R2 | A3 | A3 | A3 | A3 | A3 | A3 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R3 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 |
| R4 | A3 | A3 | A3 | A1 | A1 | A1 | A1 | A1 | A1 | A3 | A3 | A3 | A3 | A3 | A3 | A3 |
| R5 | A3 | A3 | A3 | A1 | A1 | A1 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R6 | 7 | 7 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 7 | 7 | 7 | 7 | 7 | 7 |
| R7 | O | O | O | A1 | A1 | A1 | A1 | A1 | A1 | O | O | O | O | O | O | O |
| R8 | O | O | O | A1 | A1 | A1 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R9 | | | | | | | | | | | | | | | | |
| R10 | | | | | | | | | | | | | | | | |

De forma análoga, la figura 6 representa un árbol de análisis correspondiente a las reglas Re1, Re2 y Re3 analizando primero el valor de y, luego el valor de z, y, por último, aquel de x, conforme al orden creciente del número de intervalos definidos respectivamente para x, y y z. Dos nodos intermedios 107 corresponden a los resultados del análisis de los

valores de y, efectuado en primer lugar, y seis nodos intermedios 108 a los resultados del análisis de los valores de z, efectuado seguidamente.

En el árbol de análisis de la figura 6, los sub-árboles que corresponden a los resultados de los análisis de y y luego z siguientes [(y < 2 o y > 9) y (z < 3 o z > 8)] por una parte, y [2 ≤ y ≤ 9 y z < 3] por otra parte, son homólogos. Igualmente para los sub-árboles [(y < 2 o y > 9) y 3 ≤ z ≤ 8] por una parte, y [2 ≤ y ≤ 9 y 3 ≤ z < 6] por otra parte. Además, en la figura 6, las acciones AA atribuidas en función del valor de x, según la línea 120, para valores de y y z tal que [2 ≤ y ≤ 9 y 6 ≤ z ≤ 8] por una parte y [2 ≤ y ≤ 9 y z > 8] por otra parte son idénticos. El árbol de análisis de la figura 7 corresponde entonces a aquel de la figura 6 reagrupando los sub-árboles homólogos.

La configuración de la memoria Trie, según este último árbol de análisis, necesita tantos registros como nodos 100, 107 o 108, o sea 6 registros en total. Así, 3 registros de memoria Trie han sido economizados con relación a la configuración de la memoria Trie sacada del árbol de análisis de la figura 5. Un ejemplo de configuración de la memoria Trie que corresponde al árbol de análisis de la figura 7 es:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R0 | 1 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 1 | 1 | 1 | 1 | 1 | 1 |
| R1 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| R2 | O | O | O | A3 | A3 | A3 | A3 | A3 | A3 | A3 | A3 | A3 | A3 | O | O | O |
| R3 | O | O | O | A3 | A3 | A3 | A3 | A3 | A3 | A3 | A1 | A1 | A1 | A1 | A1 | A1 |
| R4 | 2 | 2 | 2 | 3 | 3 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| R5 | O | O | O | A3 | A3 | A3 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 | A2 |
| R6 | | | | | | | | | | | | | | | | |
| R7 | | | | | | | | | | | | | | | | |

La figura 8 detalla las diferentes etapas de la creación de un nuevo arco de árbol de análisis según el modo de realización preferido del procedimiento de la invención que evita, desde la construcción del árbol de análisis, la creación de sub-árboles homólogos. Se trata de determinar el punto de llegada de un nuevo arco sacado de n nodo NP de una p-esima etapa del árbol de análisis, y asociado a un campo D determinado para el emplazamiento $E_p$ asociado a la p-esima etapa.

El método descrito es aplicado de forma recurrente a cada etapa del árbol de análisis, tomado según el orden de los emplazamientos respectivamente asociados a las etapas. Este método genera los nodos del árbol de análisis, al mismo tiempo que atribuye a cada nodo creado un subconjunto de reglas. Así, antes de la aplicación del presente método al nodo NP, un subconjunto $\{R_j\}$ de reglas es ya asociado a ese nodo, j siendo un número entero de enumeración.

Se supone que cada regla $R_j$ atribuye una acción cuando, para algunos emplazamientos, la cadena binaria leída en este emplazamiento está comprendida en un intervalo de valores especificado por esta regla. Esta forma de reglas $R_j$ corresponde a aquella de los ejemplos precedentes.

En una primera interrogación 200, se buscan aquellas reglas $R_j$ cuyo intervalo contiene el campo D para el cual el arco asociado está en curso de creación. Si ninguna de las reglas $R_j$ posee un intervalo que contiene el campo D, entonces el punto de llegada del arco es una hoja 102, 106 asociada a la acción definida por defecto O, según la etapa 201.

En caso positivo, la segunda interrogación 210 consiste en buscar entre las reglas $R_{j1}$ identificadas durante la etapa 200, las reglas $R_{j2}$ donde al menos un intervalo corresponde a un emplazamiento $E_q$ posterior al emplazamiento $E_p$ según el orden de clasificación de los emplazamientos. Si ninguna de las reglas $R_{j1}$ posee un intervalo que corresponda a un emplazamiento posterior $E_p$, entonces (etapa 211) el punto de llegada del arco es una hoja 102, 106 asociada a la acción de la regla más prioritaria entre las reglas $R_{j1}$ identificadas en la etapa 200.

En el caso donde las reglas $R_{j2}$ son identificadas durante la etapa 210, se busca entonces, en una etapa 220, si un nodo $NP^{+1}$ ya creado en la etapa (p+1) del árbol de análisis está asociado a un subconjunto $\{R_{j2}\}$ de las reglas identificadas. En caso afirmativo, ese nodo es el punto de llegada del nuevo arco sacado del nodo NP (etapa 222). En caso negativo, un nuevo nodo $NP^{+1}$ es creado en la etapa (p+1) y asociado al subconjunto $\{R_{j2}\}$ de las reglas identificadas durante la etapa 210 (etapa 221).

Este análisis es repetido por cada uno de los campos D determinados por el emplazamiento $E_p$, a fin de establecer el arco sacado del nodo NP asociado a cada uno de ellos. El mismo es seguidamente repetido de forma idéntica para

un nodo a continuación de la p-esima etapa del árbol de análisis, hasta un agotamiento de los nodos de esta etapa. Finalmente, el mismo es también reiterado para todos los nodos de la etapa siguiente (p+1), de forma de continuar la construcción del árbol de análisis.

Este método de creación de nuevos arcos es realizado para la construcción de un cuarto árbol que corresponde a las reglas dadas con referencia a la figura 5. De igual manera que para la figura 6, los emplazamientos son clasificados según el orden objeto de la invención. El árbol resultante es representado en la figura 9.

Para cada nodo del árbol es indicado el subconjunto de las reglas $\{R_{j2}\}$ asociadas a ese nodo. Para las hojas 106, la línea 121 indica las reglas $R_{j1}$ que determinan, en función de sus prioridades relativas, las acciones asociadas a esas hojas e indicadas por la línea 120.

Los diferentes ejemplos de configuración de memoria Trie detallados en esta solicitud de patente muestran el interés de la invención por la configuración de una memoria Trie. Este procedimiento, gracias a la clasificación de los emplazamientos, eventualmente combinado con el reagrupamiento de los sub-árboles de análisis homólogos, permite reducir el número de registros necesarios de una memoria Trie utilizada para asignar a células ATM de las acciones designadas por reglas fijas. Las reducciones obtenidas en los ejemplos presentados están en relación con la simplicidad de esos ejemplos. Para políticas de control de acceso reales, las reducciones obtenidas por la aplicación de los mismos principios pueden ser consecuentes, según el caso, en función del número de reglas, del número y del tamaño de los campos considerados y de los intervalos elementales asociados a los campos.

En la práctica, la configuración de la memoria Trie según la invención es efectuada a medida de la introducción de nuevas reglas, o de la supresión de reglas, al nivel del gestor del control de acceso. Ese gestor comprende un módulo de compilación que construye y modifica los árboles de análisis en función de las actualizaciones de reglas introducidas, antes de modificar la configuración existente de la memoria Trie.

## REIVINDICACIONES

1. Procedimiento de configuración de una memoria asociativa de tipo Trie para el tratamiento de paquetes de datos en función de un conjunto de reglas, la memoria Trie siendo utilizada para el análisis de cadenas binarias situadas en emplazamientos determinados de cada paquete de datos, cada regla atribuyendo una acción (110-114) a un paquete en función de los valores de dichas cadenas binarias, la memoria Trie comprendiendo registros compuestos por un número determinado de células elementales para recibir referencias respectivas, el procedimiento comprendiendo las etapas siguientes:

a- para cada uno de dichos emplazamientos, se definen intervalos elementales consecutivos que cubren valores de cadena binaria que pueden aparecer en dicho emplazamiento, cada intervalo elemental siendo tal que la acción (110-114) atribuida para cada una de las reglas no sea modificada por un cambio, en el interior de dicho intervalo elemental, del valor de la cadena binaria situada en dicho emplazamiento en un paquete tratado;

b- se inventarían los intervalos elementales definidos para cada emplazamiento y se clasifican los emplazamientos en un orden tal que el emplazamiento para el cual el mayor número de intervalos elementales ha sido definido sea colocado de último;

c- se traduce el conjunto de reglas en un árbol de análisis de los paquetes que comprenden nodos (100, 101, 103-105, 107, 108) repartidos en etapas sucesivas respectivamente asociadas a los emplazamientos considerados en dicho orden, arcos (130, 131), y hojas (102, 106) que corresponden a acciones (120) atribuibles por las reglas, la primera etapa del árbol comprendiendo un único nodo (100) llamado racimo del árbol de análisis,

cada arco teniendo un nodo de partida asociado a un emplazamiento y un punto de llegada que consiste en un nodo de la etapa siguiendo aquella del nodo de partida como en una hoja, y cada arco estando asociado a un campo respectivo de valores de cadena binaria posibles a dicho emplazamiento,

el árbol de análisis que define los caminos que consisten cada uno en una sucesión de n arcos (130, 131), n siendo un número entero al menos igual a 1, el primer arco de la sucesión teniendo pro nodo de partida el racimo del árbol de análisis,

el punto de llegada de cada arco de un camino además del último arco siendo el nodo de partida del arco siguiente de dicho camino, y que el punto de llegada del último arco del camino siendo una hoja (102, 106) que corresponde a una acción atribuida después del conjunto de reglas a cada paquete que tiene, en los n emplazamientos respectivamente asociados a las etapas de los nodos de partida n arcos del camino, valores de cadena binaria que caen en los n campos respectivamente asociados a dichos arcos;

d- se asignan un grupo de registros de la memoria Trie incluyendo un registro portero a cada nodo (100, 101, 103-105, 107, 108) del árbol de análisis que pertenece a una etapa asociada a un emplazamiento, y se registra en las células de dicho grupo de registros referencias tales que analizando a partir del registro portero el valor de cadena binaria contenida en dicho emplazamiento en un paquete, se obtiene una referencia final que depende de qué campo contiene dicho valor entre los campos de valores asociados a los arcos que tienen dicho nodo como nodo de partida y tal que:

si el arco asociado (131) al campo que contiene dicho valor tiene como punto de llegada una hoja (102, 106) que corresponde a una acción (120), la referencia final designa dicha acción como siendo atribuida al paquete, y

si el arco (130) asociado al campo que contiene dicho valor tiene otro nodo (101, 103-105, 107, 108) de la etapa siguiente como punto de llegada, la referencia final designa dicho otro nodo para proseguir analizando el valor de cadena binaria contenida en el paquete en el emplazamiento asociado a dicha etapa siguiente.

2. Procedimiento según la reivindicación 1, según el cual, durante la etapa b, se clasifican dichos emplazamientos en el orden de los números crecientes de intervalos elementales.

3. Procedimiento según la reivindicación 1 o 2, según el cual, los intervalos elementales definidos para cada emplazamiento comprenden límites de intervalo, y según el cual cada límite de intervalo corresponde al cambio de una acción (110-114) atribuible por al menos una regla.

4. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el cual la traducción del conjunto de reglas es tal que al menos un nodo del árbol de análisis sea el punto de llegada de varios arcos sacados de nodos de partida distintos de la etapa precedente.

5. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el cual un sub-árbol está asociado a cada nodo del árbol de análisis además del racimo del árbol de análisis, dicho sub-árbol teniendo un racimo constituido

por dicho nodo y estando compuesto por nodos, arcos y hojas reunidas a partir de dicho nodo a lo largo de los diferentes caminos que pasan por dicho nodo, y en el cual la traducción del conjunto de reglas es operada de forma tal que el árbol de análisis no incluya primer y segundo sub-árboles teniendo racimos distintos y tal que se pueda aparear sus nodos respectivos, sus arcos respectivos y sus hojas respectivas, de tal manera que cada nodo del primer sub-árbol sea apareado a un nodo del segundo sub-árbol perteneciendo a una misma etapa, que cada hoja del primer sub-árbol sea apareada a una hoja del segundo sub-árbol correspondiente a una misma acción, y que dos arcos apareados de los primer y segundo sub-árboles tengan nodos de partida apareados y puntos de llegada apareados y sean asociados al mismo campo de valores.

6. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el cual cada regla del conjunto es definida por una acción e intervalos de valores que corresponden respectivamente a algunos al menos de los emplazamientos, y atribuye dicha acción a los paquetes que tienen, en dichos emplazamientos, valores de cadenas binarias que caen respectivamente en dichos intervalos.

7. Procedimiento según la reivindicación 6, en el cual se asocia un subconjunto de reglas a cada nodo de una (p+1) esima etapa del árbol de análisis, p siendo un número entero mayor que 0, dicho subconjunto estando compuesto por reglas del conjunto tales que cada intervalo de valores correspondiente a un emplazamiento asociado a una de las p primeras etapas del árbol tenga un recubrimiento no vacío con el campo de valores asociado al arco de cada camino que pasa por dicho nodo y teniendo su nodo de partida en dicha etapa.

8. Procedimiento según la reivindicación 7, en el cual se asocia al nodo racimo un subconjunto constituido por el conjunto de reglas, y en el cual la traducción del conjunto de reglas comprende las etapas siguientes para cada nodo de la p-esima etapa asociada a un primer subconjunto de reglas:

- determinar campos de valores que cubren valores de cadena binaria que pueden aparecer en el p-esimo emplazamiento según dicho orden, cada campo siendo tal que la acción atribuida por cada una de las reglas del primer subconjunto no sea modificada por un cambio, en el interior de dicho campo, del valor de la cadena binaria situada en el p-esimo emplazamiento en un paquete tratado; y

- para cada uno de dichos campos de valores:

  - generar un arco asociado a dicho campo, que tiene dicho nodo de la p-esima etapa por nodo de partida;

  - detectar cada regla del primer subconjunto que es definida por al menos un intervalo de valores que incluye dicho campo;

  - si ninguna regla es detectada, asignar una hoja del árbol correspondiente a una acción por defecto como punto de llegada de dicho arco;

  - si para cada regla detectada, ningún intervalo de valores corresponde a uno cualquiera de los emplazamientos siguiendo el p-esimo emplazamiento según dicho orden, asignar una hoja del árbol correspondiente a una acción de una regla detectada como punto de llegada de dicho arco;

  - si para al menos una regla detectada, un intervalo de valores corresponde a uno de los emplazamientos siguiendo el p-esimo emplazamiento según dicho orden, asignar un nodo de la (p+1)esima etapa del árbol como punto de llegada de dicho arco, dicho nodo de la (p+1)esima etapa estando asociado a un segundo subconjunto compuesto por reglas detectadas del primer subconjunto.

9. Procedimiento según la reivindicación 8, en el cual prioridades son respectivamente asignadas a las reglas del conjunto, y en el cual cuando varias reglas son detectadas y ninguno de sus intervalos de valores corresponde a uno de los emplazamientos siguiendo el p-esimo emplazamiento, la acción correspondiente a la hoja del árbol asignada a dicho arco es aquella de una de las reglas detectadas, seleccionada sobre la base de las prioridades asignadas.

10. Procedimiento según la reivindicación 8 o 9, en el cual se ejecutan las etapas siguientes cuando se ha detectado al menos una regla que tiene un intervalo de valores correspondiente a uno de los emplazamientos siguiendo el p-esimo emplazamiento:

- buscar si ya ha sido generado un nodo de la (p+1)esima etapa del árbol asociada al segundo subconjunto;

- si la búsqueda se detiene, generar un nodo tal en la (p+1)esima etapa;

- si la búsqueda identifica un nodo de la (p+1)esima etapa, asignar el nodo identificado como punto de llegada de dicho arco.

11. Dispositivo de tratamiento de paquetes de datos que comprende una memoria asociativa de tipo Trie y un controlador adaptado para llevar a cabo un procedimiento de configuración de la memoria Trie según una cualquiera de las reivindicaciones precedentes.

12. Dispositivo según la reivindicación 11, en el cual los paquetes de datos son células ATM portadoras de tramas AAL 5.

13. Dispositivo según la reivindicación 11, en el cual los paquetes de datos son paquetes IP.

14. Dispositivo según una cualquiera de las reivindicaciones 11 a 13, dispuesto para el encaminamiento por una red de comunicación de paquetes de datos en función de reglas de encaminamiento aplicadas a dichos paquetes.

15. Dispositivo según una cualquiera de las reivindicaciones 11 a 13, dispuesto para el control de acceso a una red de comunicación por paquetes de datos en función de reglas de control de acceso a esa red aplicadas a dichos paquetes.

16. Dispositivo según una cualquiera de las reivindicaciones 11 a 13, dispuesto para la adquisición de informaciones concernientes a paquetes de datos transmitidos por una red de comunicación.

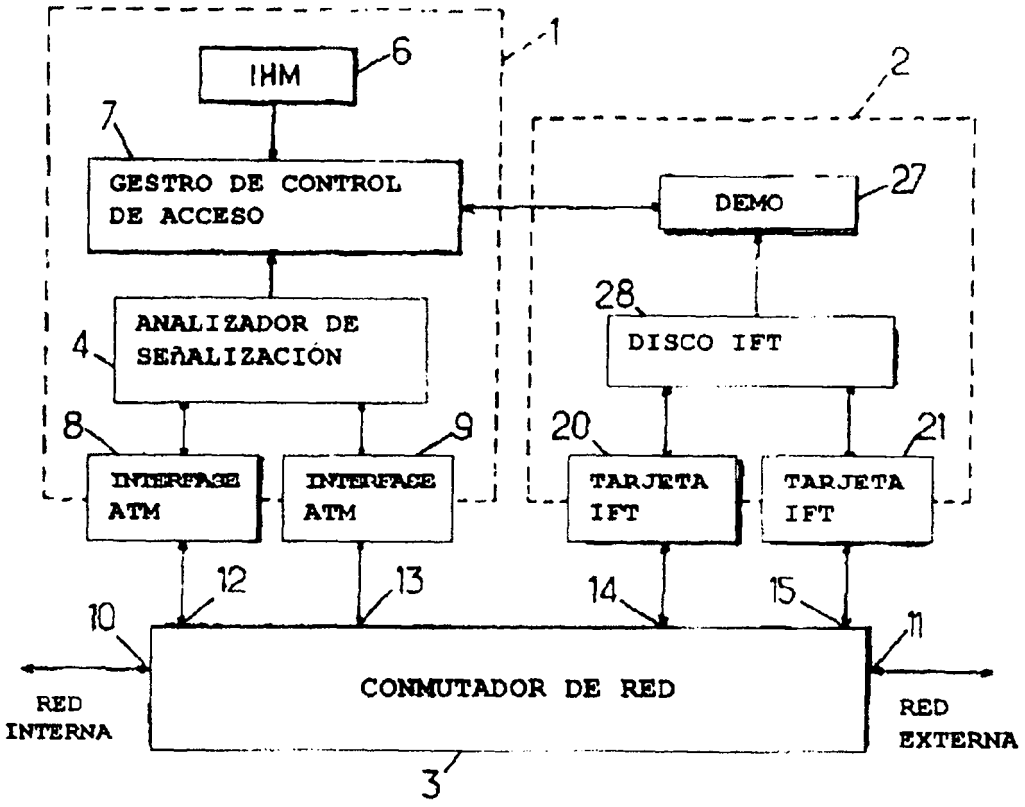

1
2
IHM
6
7
GESTRO DE CONTROL DE ACCESO
DEMO
27
28
DISCO IFT
ANALIZADOR DE SEñALIZACIÓN
4
8
9
20
21
INTERFACE ATM
INTERFACE ATM
TARJETA IFT
TARJETA IFT
12
13
14
15
10
11
CONMUTADOR DE RED
RED INTERNA
RED EXTERNA
3

FIG.1.

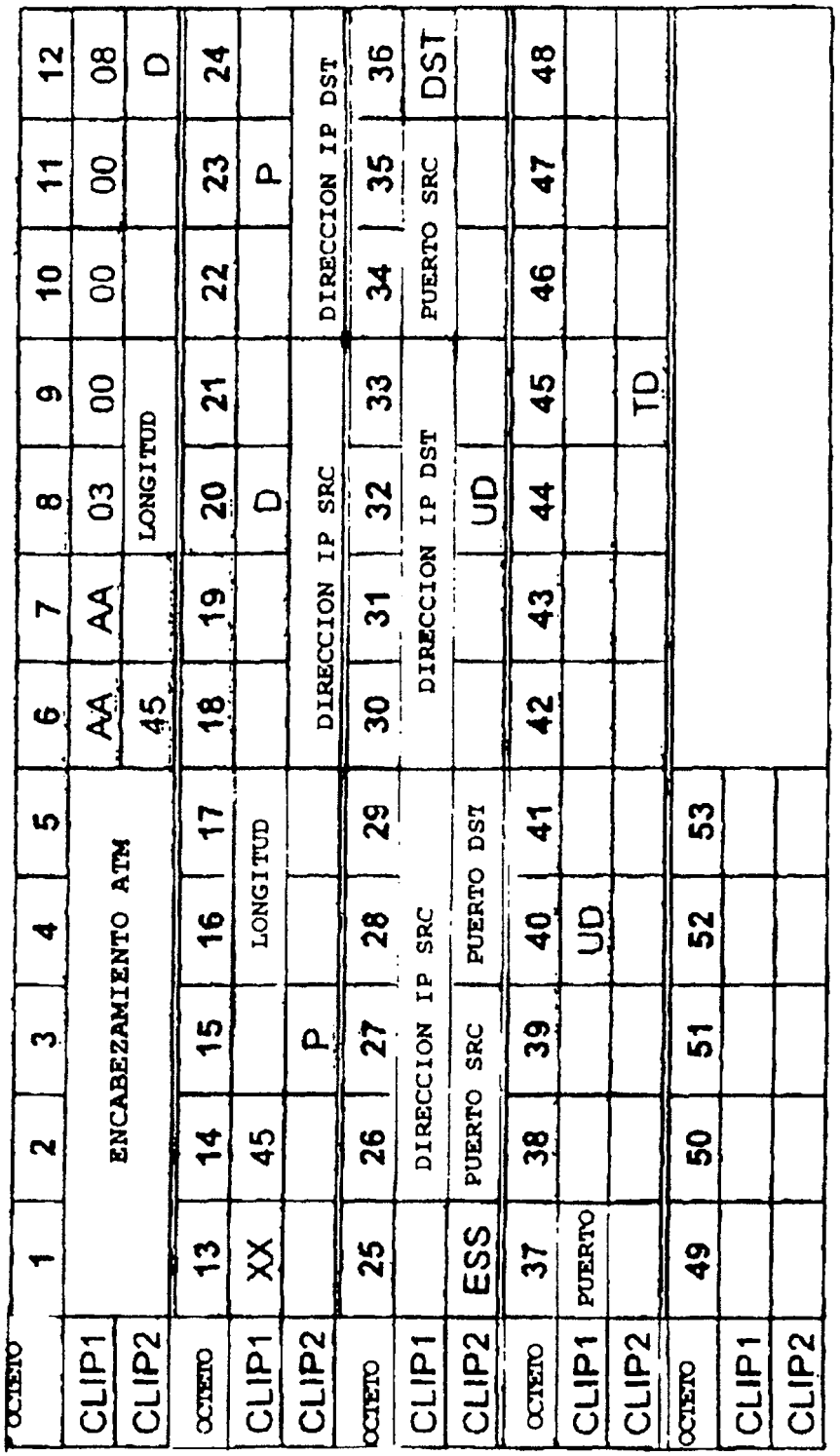

OCTETO
1
2
3
4
5
6
7
8
9
10
11
12
CLIP1
ENCABEZAMIENTO ATM
AA
AA
03
00
00
00
08
CLIP2
45
LONGITUD
D
OCTETO
13
14
15
16
17
18
19
20
21
22
23
24
CLIP1
XX
45
LONGITUD
D
P
CLIP2
P
DIRECCION IP SRC
DIRECCION IP DST
OCTETO
25
26
27
28
29
30
31
32
33
34
35
36
CLIP1
DIRECCION IP SRC
DIRECCION IP DST
PUERTO SRC
DST
CLIP2
ESS
PUERTO SRC
PUERTO DST
UD
OCTETO
37
38
39
40
41
42
43
44
45
46
47
48
CLIP1
PUERTO
UD
CLIP2
TD
OCTETO
49
50
51
52
53
CLIP1
CLIP2

FIG.2

FIG.3.

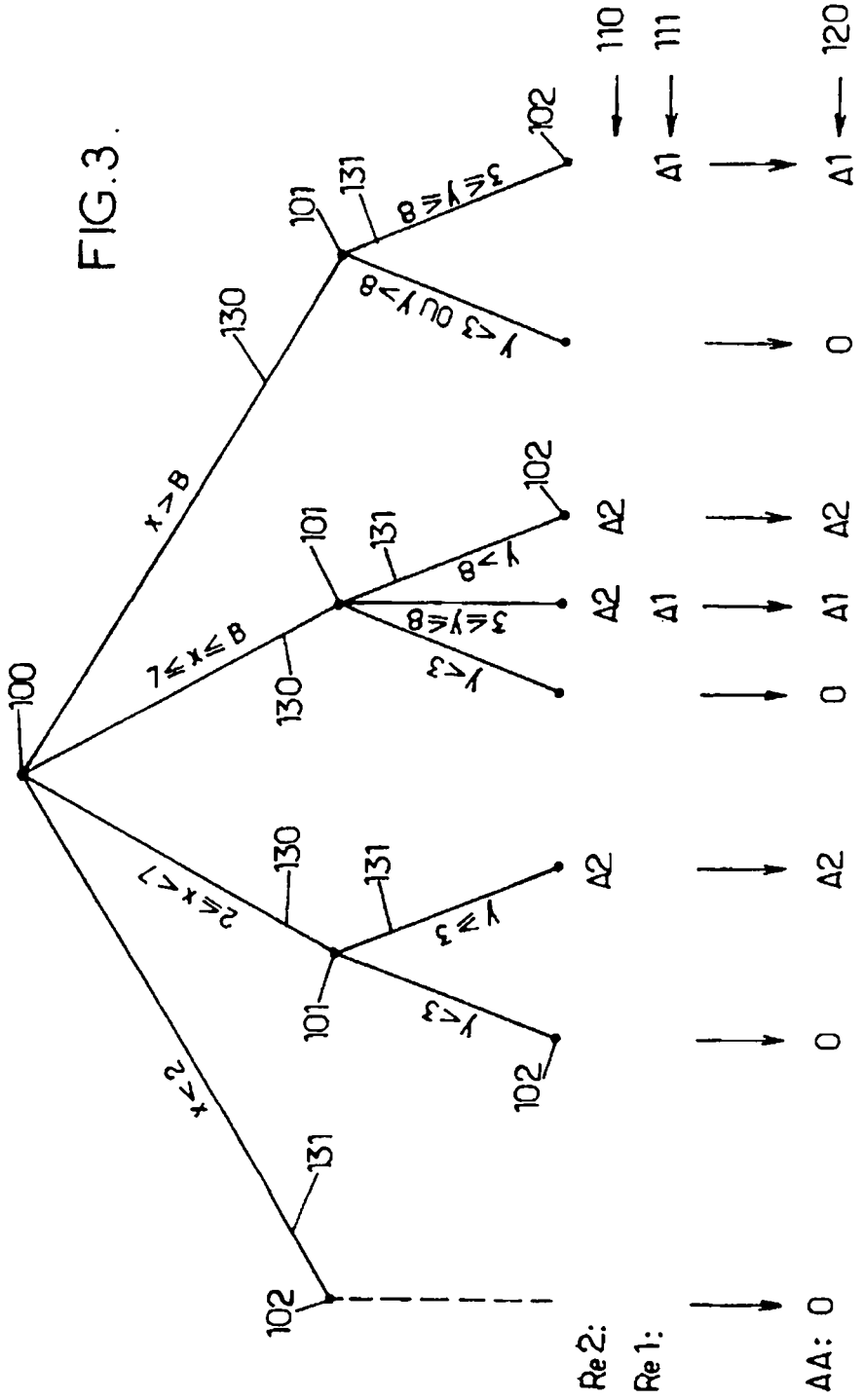

100
x>B
130
101
131
102
3≤Y≤B
Y<3 OU Y>B
110
111
120
A1
A1
A1
0
7≤X≤B
130
101
131
102
Y>B
A2
A2
A2
3≤Y≤B
A1
A1
Y<3
0
0
2≤X<7
130
101
131
102
Y≥3
A2
A2
Y<3
0
0
X<2
131
102
Re 2:
Re 1:
AA: 0

FIG.4.

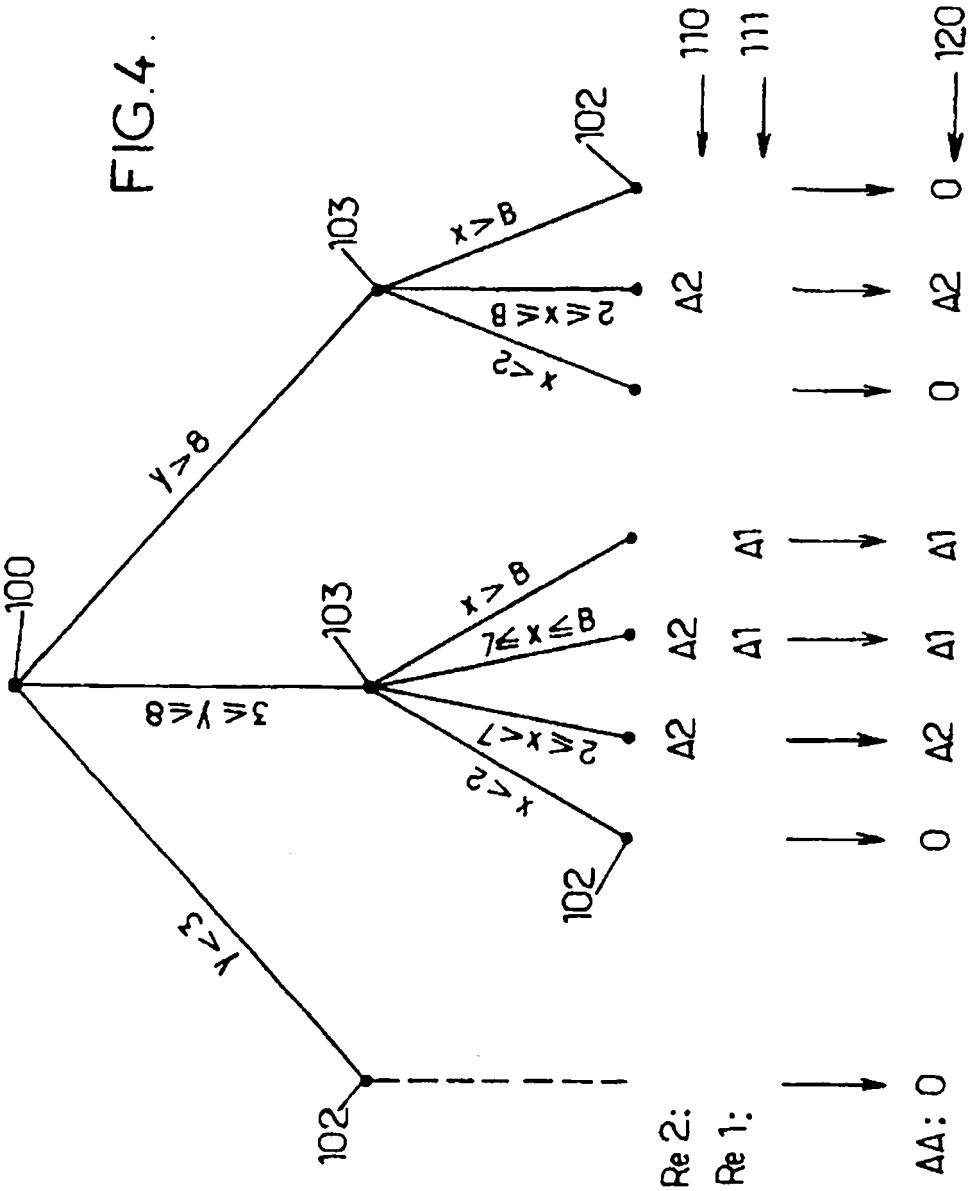

100
102
103
Y<1
1≤Y≤8
Y>8
X<2
2≤X≤7
X>7
X<2
2≤X≤8
X>8
Re 2:
Re 1:
ΔA: 0
Δ2
Δ1
110
111
120
0

FIG.5

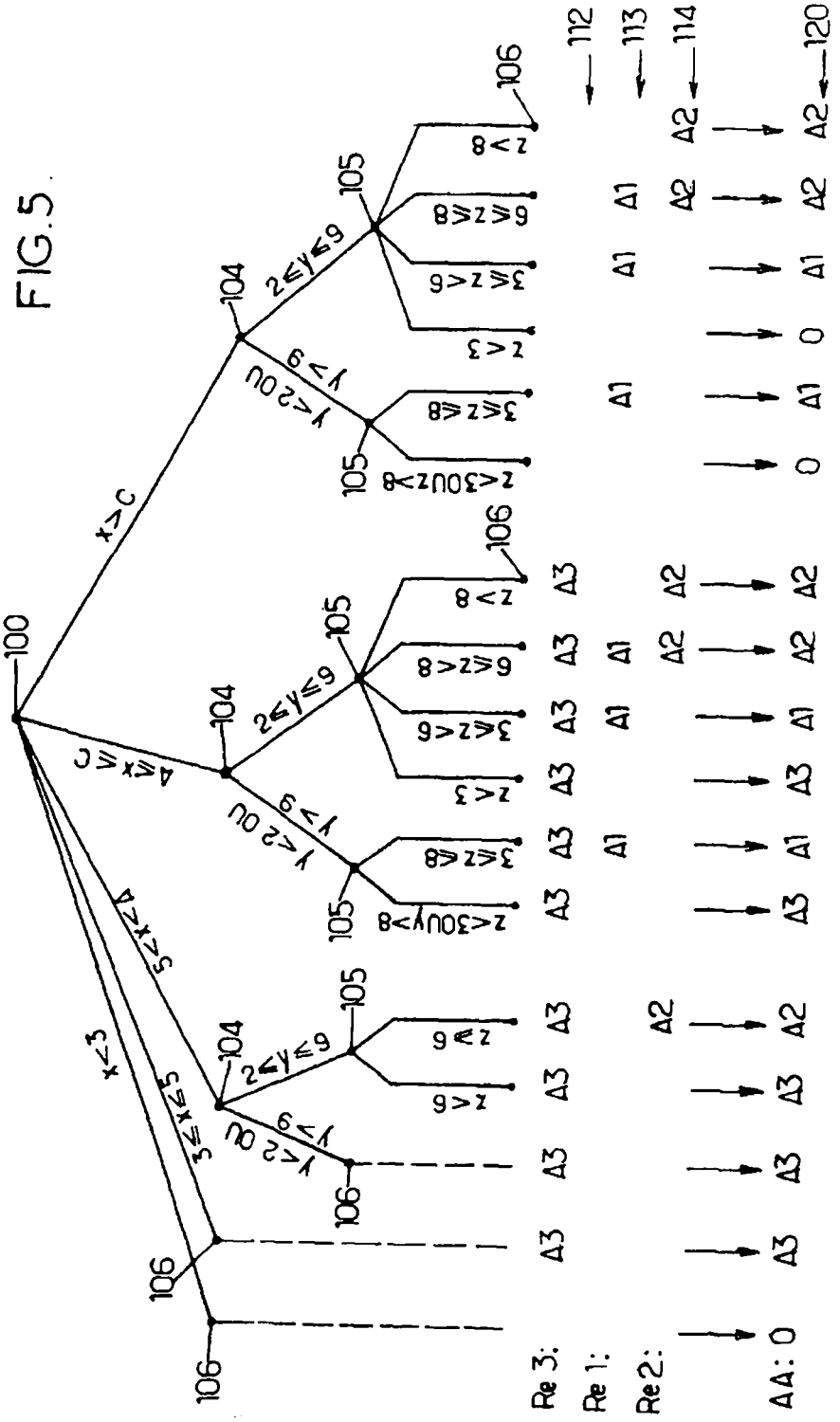

100
x>C
A≤x≤C
x<3
5≤x≤A
3≤x≤5
104
105
106
2≤y≤9
y>9
y<2 ou
z>8
6≤z≤8
3≤z<6
z<3
z<3 ou z>8
3≤z≤8
6≤z<8
z≥6
z<6
112
113
114
120
Re 3:
Re 1:
Re 2:
AA: 0
Δ1
Δ2
Δ3
0

FIG.6.

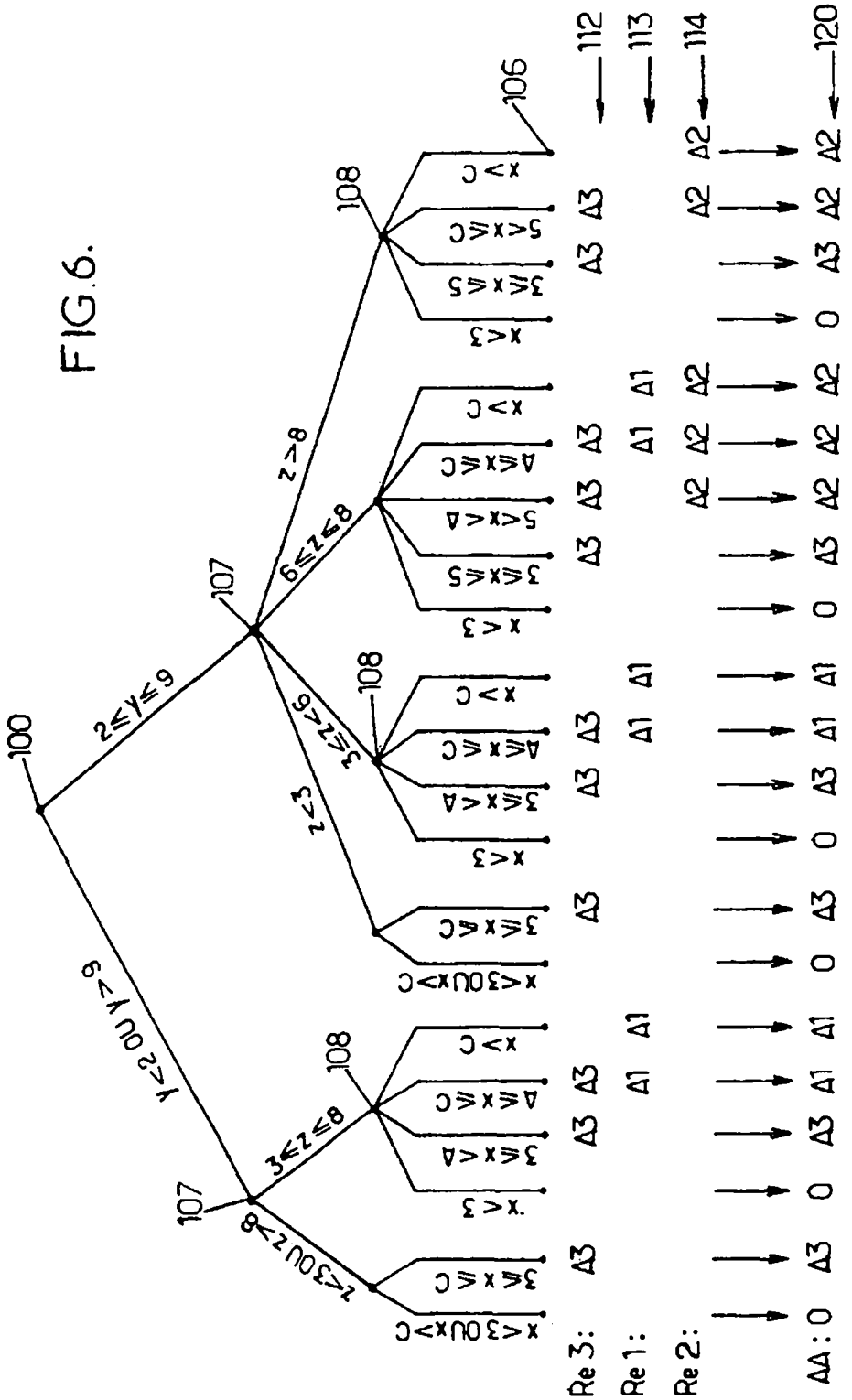
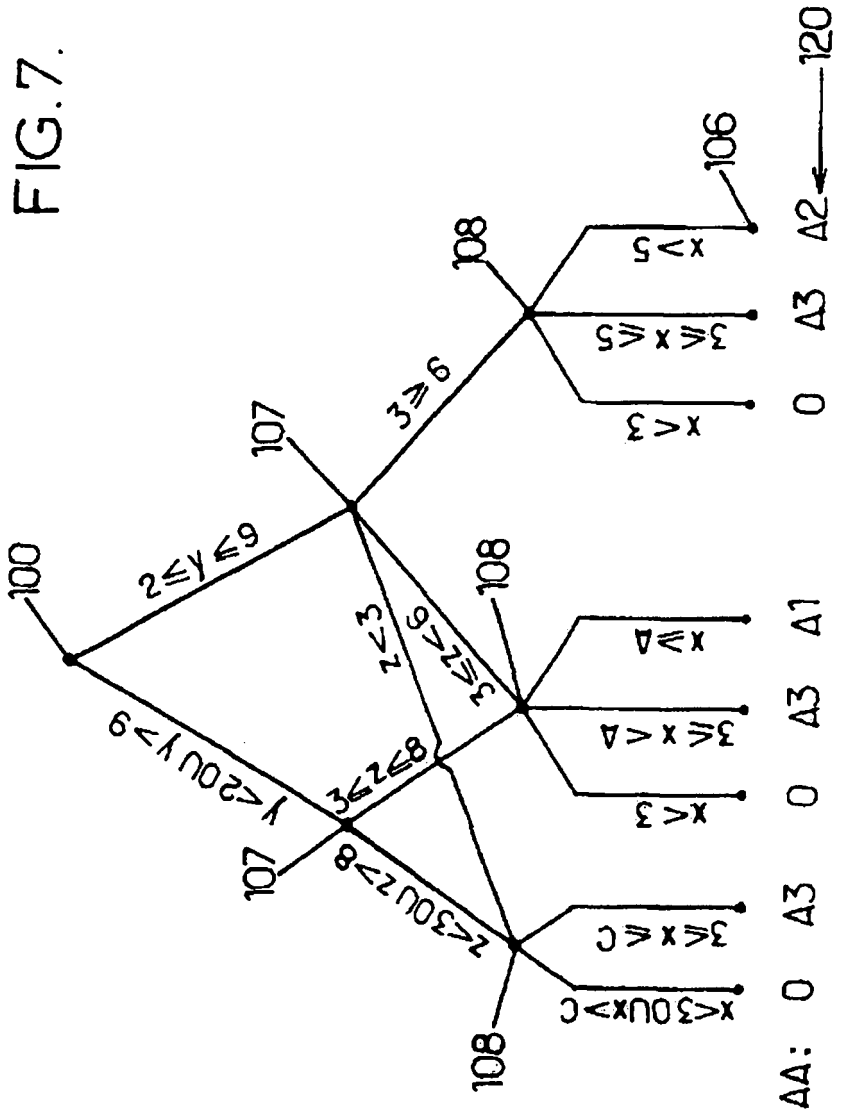

100
2≤y≤9
y<2 ou y>9
107
z>8
6≤z≤8
3≤z≤6
z<3
3≤z≤8
z<3 ou z>8
108
106
x>c
5<x≤c
3≤x≤5
x<3
Δ≤x≤c
3≤x<Δ
3≤x≤c
x<3 ou x>c
112
113
114
120
Re 3:
Re 1:
Re 2:
Δ4: 0
Δ3
Δ2
Δ1
0

FIG. 7.


100
2≤y≤9
y<2 OU y>9
z<3
3≤z≤9
3≤z≤8
z<3 OU z>8
107
107
108
108
108
3≥6
x<3
3≤x≤5
x>5
x<3
3≤x<A
x≥A
x<3 OU x>C
3≤x≤C
Δ4: 0
Δ3
0
Δ3
0
Δ1
Δ3
0
Δ2
106
120

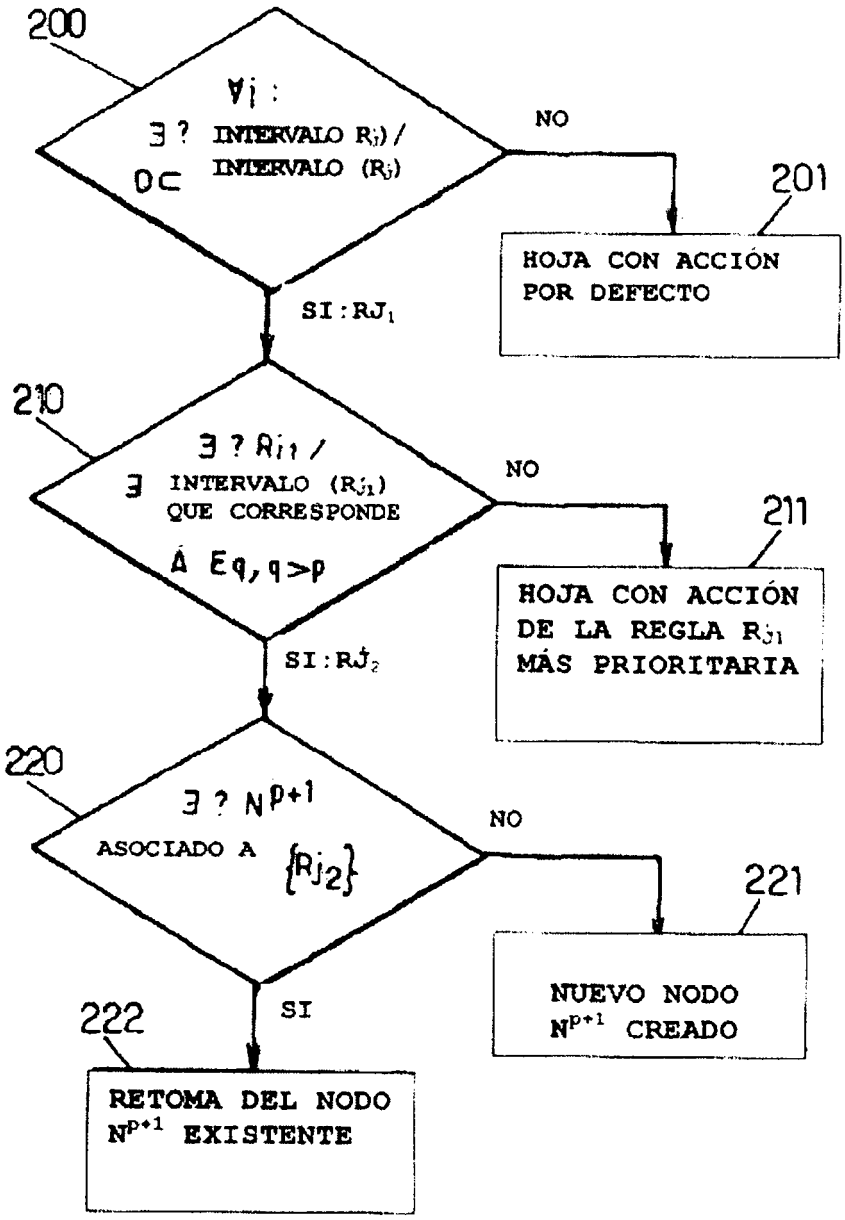
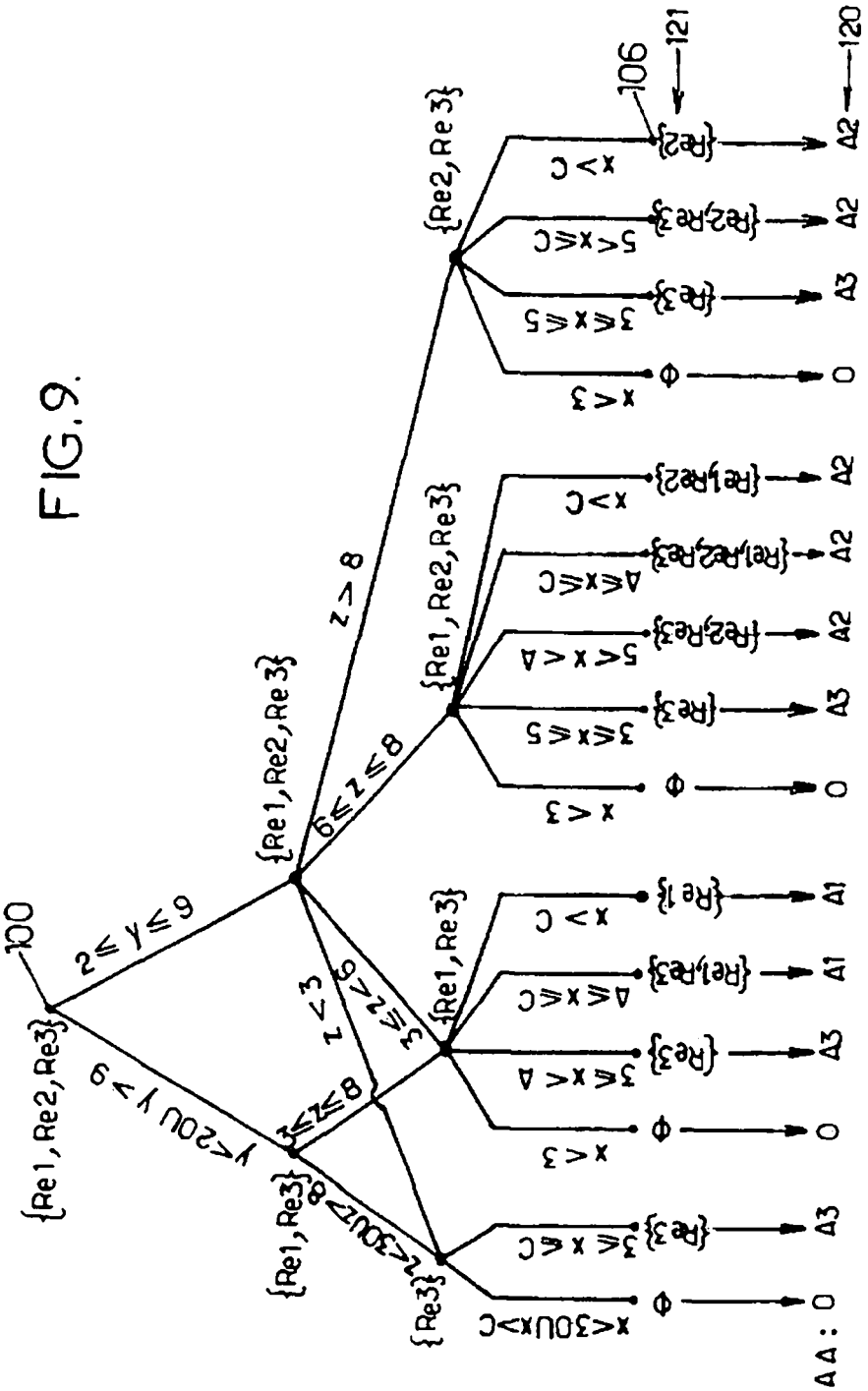

200
∀j :
∃ ? INTERVALO Rj) /
0⊂ INTERVALO (Rj)
NO
201
HOJA CON ACCIÓN POR DEFECTO
SI : RJ1
210
∃ ? Rj1 /
∃ INTERVALO (Rj1) QUE CORRESPONDE
Á Eq, q>p
NO
211
HOJA CON ACCIÓN DE LA REGLA Rj1 MÁS PRIORITARIA
SI : RJ2
220
∃ ? N p+1
ASOCIADO A {Rj2}
NO
221
NUEVO NODO N p+1 CREADO
SI
222
RETOMA DEL NODO N p+1 EXISTENTE

FIG.8.

FIG. 9.


100
{Re1, Re2, Re3}
2≤y≤9
y<2 OU y>9
{Re1, Re3}
z<3
3≤z≤8
z>8
{Re3}
x<3 OU x>C
Φ
0
3≤x≤C
{Re3}
Δ3
x<3
Φ
0
3≤x<Δ
{Re3}
Δ3
Δ≤x≤C
{Re1,Re3}
Δ1
x>C
{Re1}
Δ1
3≤z≤8
{Re1, Re2, Re3}
x<3
Φ
0
3≤x≤5
{Re3}
Δ3
5<x<Δ
{Re2,Re3}
Δ2
Δ≤x≤C
{Re1,Re2,Re3}
Δ2
x>C
{Re1,Re2}
Δ2
z>8
{Re2, Re3}
x<3
Φ
0
3≤x≤5
{Re3}
Δ3
5<x≤C
{Re2,Re3}
Δ2
x>C
106
121
{Re2}
Δ2
120
ΔΔ : 0