(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 571 356**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.04.2004 E 04300192 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.02.2016 EP 1471685**

(54) Título: **Supresión de trampas de SNMP para gestor de red**

(30) Prioridad:

11.04.2003 US 411263

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.05.2016

(73) Titular/es:

ALCATEL LUCENT (100.0%)
148/152 route de la Reine
92100 Boulogne-Billancourt, FR

(72) Inventor/es:

GASPARD, MOISE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Supresión de trampas de SNMP para gestor de red

Campo de la invención

La presente invención se refiere a gestión de red en sistemas de comunicación y más particularmente a sistemas y procedimientos para proteger que se sobrecarguen los sistemas de gestión de red por trampas de eventos de SNMP recibidas desde nodos de red.

Antecedentes de la invención

El protocolo de gestión de red simple (SNMP) está basado en un modelo de gestor/agente en el que el agente requiere software mínimo. El SNMP, desarrollado 1988 se ha convertido en el estándar de facto para gestión de interconexión de red. Puesto que representa una solución sencilla que requiere poco código para implementar, numerosos distribuidores han podido crear agentes de SNMP a sus productos. Generalmente, SNMP es extensible permitiendo de esta manera a los distribuidores añadir fácilmente funciones de gestión de red a sus productos existentes. SNMP también separa la función de gestión de la arquitectura de los dispositivos de hardware lo que amplía la base de soporte de múltiples distribuidores.

La mayoría de la potencia de procesamiento y de almacenamiento de datos implicada en el protocolo de SNMP reside en el sistema de gestión mientras que un subconjunto complementario de estas funciones reside en el sistema gestionado. Para conseguir este objetivo de ser simple SNMP incluye un conjunto limitado de comandos y respuestas manuales. El sistema de gestión emite mensajes get, get next y set para recuperar variables de objetos únicos o múltiples o para establecer el valor de una única variable. El agente gestionado envía un mensaje de respuesta para completar el mensaje get, get next o set. El elemento gestionado envía una notificación de evento denominada una trampa al sistema de gestión para identificar la aparición de condiciones tales como umbrales que superan un valor predeterminado. En resumen hay cinco operaciones primitivas en concreto get, get next, get response, set y trap.

Las trampas son mensajes asíncronos que notifican a los gestores de SNMP de eventos significativos que han tenido lugar en el agente o en el nodo. Las trampas se envían sin solicitar a los gestores de SNMP que están configurados para recibirlas.

Será evidente para un experto en la materia que las trampas de eventos pueden identificar problemas potenciales con nodos de red particularmente si el sistema de gestión recibe un gran número de trampas desde un nodo particular. Será también evidente para un experto en la materia que tales trampas pueden usarse por un atacante malicioso para interrumpir servicios proporcionados por el sistema de gestión de red.

Un procedimiento de detección de intrusión se describe en el documento US 2003/0061514 A1. Una tasa de generación de alerta de un sistema de detección de intrusión se compara con una tasa de generación de alerta umbral, y se modifica un elemento de un conjunto de firma del sistema de detección de intrusión dependiendo de la comparación para reducir la tasa de generación de alerta.

El documento JPH07183932 desvela un sistema de informe de eventos de acuerdo con el que se emite un periodo de supresión o una liberación de supresión desde un terminal de control dependiendo de la transición entre estados de disponibilidad de supervisión en tiempo real o no disponibilidad de dicho terminal de control, que, cuando está disponible, está recibiendo eventos desde dispositivos gestionados.

El Centro de Coordinación CERT® ha emitido la advertencia sobre deficiencias potenciales en el protocolo de SNMP, entre otros, que pueden aprovecharse para ataques maliciosos. Una solución propuesta por CERT para defenderse frente a tales ataques implica identificar el nodo ofensivo (es decir el generador de las trampas de eventos de SNMP excesivas) y desactivar SNMP en ese nodo, si es posible. Desafortunadamente, esto no es una opción para NMS puesto que ya no podría gestionar más ese nodo, y esto sería inaceptable para el proveedor de red.

Otra fuente de la industria significativa de servicios de SNMP trata este problema correlacionado ciertos tipos de trampas de modo que pueda evitarse la diseminación de trampas duplicadas de estos tipos. Esta técnica se aplica a ciertos tipos de trampas convencionales, por ejemplo, trampas de enlace activo/inactivo, etc. Desafortunadamente, este enfoque está limitado puesto que no trata trampas no convencionales, por ejemplo trampas de eventos desconocidos, que produce que un NMS agote recursos significativos para analizarlas.

Por lo tanto, sería deseable una técnica mejorada para que un NMS responda a trampas de eventos de SNMP excesivas. Los problemas con las soluciones de la técnica anterior son, como se ha analizado anteriormente, que la solución de CERT desactiva SNMP en el nodo ofensivo lo que no es aceptable para un NMS mientras que la segunda solución está limitada a ciertos tipos de trampas convencionales, y no trata trampas no convencionales tales como trampas de eventos desconocidos, que pueden ser particularmente intensivos de analizar en cuanto a procesamiento.

Existe por lo tanto una necesidad de resolver los problemas anteriormente mencionados.

Sumario de la invención

La presente invención se refiere al problema de proteger un Sistema de Gestión de Red (NMS) de que se sobrecargue por trampas de eventos SNMP excesivas desde un nodo de red. La causa de las trampas excesivas podría ser un ataque de Denegación de Servicio (DoS) en el nodo de red, o posiblemente un fallo en el nodo que produce mensajería de eventos de SNMP excesiva.

La invención protege el NM de una inundación de mensajes de SNMP de cualquier tipo, no solamente mensajes convencionales como en la técnica anterior.

La invención protege eficazmente el NM de atraques maliciosos en nodos de red, tales como ataques de DoS, y alerta a un operador de la situación de modo que puedan tomarse acciones correctivas. De manera similar, la invención protege al NM de nodos con fallos que generan una cantidad excesiva de trampas de eventos de SNMP. La invención moderará también la carga de SNMP en el NM cuando se reinicien los nodos. Esta carga podría ser de otra manera bastante grande si varios nodos reinician simultáneamente.

De acuerdo con un aspecto de la presente invención se proporciona un procedimiento como se reivindica en la reivindicación 1.

De acuerdo con un segundo aspecto de la presente invención se proporciona un sistema como se reivindica en la reivindicación 13. Se cubren realizaciones preferidas mediante las reivindicaciones dependientes adjuntas.

Breve descripción de los dibujos

Las características y ventajas de la invención se harán más evidentes a partir de la siguiente descripción detallada de la realización o realizaciones preferidas con referencia a los diagramas adjuntos en los que:

La Figura 1 es un diagrama de red de alto nivel que muestra elementos de la invención;

La Figura 2 es un gráfico de ejemplo de trampas de evento recibidas en un nodo;

La Figura 3 es un segundo gráfico de ejemplo; y

La Figura 4 es un diagrama de flujo que muestra etapas del procedimiento que implementa la invención.

Descripción detallada de la invención

La Figura 1 representa una red simplificada que comprende tres nodos de red (A, B y C) interconectados para formar una red de comunicaciones con enlaces a un NMS para gestión de red y servicios. Cada uno de los nodos comunica la aparición de eventos al NMS usando mensajes de trampa de eventos de SNMP, por ejemplo enlace activo/inactivo. El NMS puede solicitar también información desde los nodos, usando mensajes “get” de SNMP, o configurar recursos en los nodos, usando mensajes “set” de SNMP, entre otras funciones. Cuando una trampa de evento es de tipo desconocido (también conocido como trampa de evento desconocida), se requiere procesamiento adicional por el NMS para analizar la trampa sobre trampas de eventos conocidas convencionales. Por lo tanto, los ataques de DoS que son particularmente eficaces por su fin ilícito son aquellos que producen que se genere excesivo número de trampas de eventos desconocidas por un nodo. La recepción de cientos de miles de trampas de eventos desconocidas por segundo podría “ocupar” completamente un NMS.

De acuerdo con la invención se proporciona un NMS con la capacidad de bloquear trampas de eventos de SNMP desde otro procesamiento en el NMS cuando la tasa de llegada de las trampas desde un nodo particular supera un umbral predeterminado. Esta capacidad se denomina como la característica de supresión de trampa.

Un fichero en el NMS define ciertos parámetros necesarios para supresión de trampa. El primer parámetro activa, o desactiva, la característica de supresión de trampa. El valor por defecto es activado. El siguiente parámetro es la tasa de llegada de trampas máxima por nodo para todos los tipos de trampas. El valor por defecto de este parámetro es de 100 trampas/segundo. La realización preferida usa el mismo valor de tasa de llegada para todos los nodos y tipos de trampas. Sin embargo, sería posible especificar tasas de llegadas separadas por tipo de trampa y por tipo de nodo en otras realizaciones. El siguiente parámetro es la latencia de supresión de trampa, que especifica la cantidad de tiempo que la trampa se bloqueará desde un nodo ofensivo después de que ese nodo ha superado la tasa de llegada de trampas máxima. El valor por defecto para este parámetro es 100 segundos. Un parámetro final es el tiempo de antigüedad, que especifica la cantidad de tiempo que los registros de un nodo se mantendrán por la característica. Para cada nodo, este tiempo se mide desde el tiempo de la última trampa desde ese nodo. El valor de tiempo de antigüedad por defecto es de 100 minutos.

En operación normal, las trampas recibidas desde cualquier nodo particular no deberían superar la tasa de llegada de trampas máxima. Para cada nodo, mientras que la tasa de llegada de trampas real es menor que la tasa de llegada de trampas máxima, las trampas desde ese nodo se reenvían a procedimientos de nivel superior en el NMS

que tiene registrado para recibir trampas. Ejemplos de estos procedimientos son el procedimiento de Auto-descubrimiento y el procedimiento de Vigilancia de Alarma (GGP). El número de trampas recibidas desde cada nodo se cuenta durante un intervalo predefinido (por ejemplo 10 segundos) por un contador para determinar la tasa de llegada de trampas para cada nodo. La duración del intervalo podría definirse también mediante un parámetro en el fichero de parámetros, y de esta manera podría ser programable.

Cuando un nodo supera la tasa de llegada de trampas máxima todas las trampas adicionales de ese nodo se interrumpen (es decir, no se reenvían) durante una duración especificada mediante el parámetro de latencia de supresión de trampa (por ejemplo 100 segundos). Esta ocurrencia se registra y puede notificarse opcionalmente a procedimientos tales como el procedimiento de vigilancia de alarma (GGP), de modo que un operador de red puede tomar la acción correctiva apropiada (por ejemplo establecer un cortafuegos, ejecutar diagnóstico en el nodo ofensivo, etc.). Después de que ha pasado la duración de las trampas de bloqueo, el NMS empieza a reenviar trampas recibidas desde el nodo siempre que no superen la tasa de llegada de trampas máxima, de otra manera las trampas se bloquean como anteriormente y el procedimiento se repite.

Las Figuras 2 y 3 muestran gráficos de ejemplo de trampas de eventos recibidas desde un nodo. En la Figura 2 en el tiempo cero segundos las trampas de eventos recibidas desde el nodo empiezan a aumentar drásticamente, que podría ser el resultado de un reinicio del nodo. Las trampas por segundo aumentan rápidamente a 200 trampas/segundo antes de estabilizarse, y permanecen en esa tasa durante cinco segundos. Por lo tanto, después de aproximadamente cinco segundos el número total de trampas recibidas es de 1.000 trampas. Suponiendo una duración para la característica de supresión de trampa de 5 segundos significa que la tasa de llegada de trampas calculada es de 200 trampas/segundo. Por lo tanto, el NMS bloqueará todas las trampas de eventos adicionales desde este nodo durante la duración especificada por el parámetro de latencia de supresión de trampa, por ejemplo, 100 segundos. El troceo bajo la curva en la Figura 2 indica las trampas bloqueadas. Estas trampas de eventos pueden reconciliarse (recuperarse desde el nodo) mediante el NMS en un momento más tarde.

La Figura 3 muestra otro ejemplo de llegadas de trampas en el NMS. En este caso el nodo que envía las trampas envía un número muy grande de trampas a intervalos repetidos. Esto podría deberse a algún fallo que produce reinicios continuos o a partir de un ataque de DoS. El NMS bloquea todas las trampas de eventos recibidas desde el nodo después de que se supera la tasa de llegada de trampas, y durante la duración especificada mediante el parámetro de latencia de supresión. La característica de supresión de trampas alerta a un operador de esta condición de modo que pueden tomarse las acciones apropiadas.

Lo siguiente establece las etapas de procedimiento implicadas al implementar el algoritmo de acuerdo con la invención.

1) el sistema de gestión de red (NMS) arranca y lee el estado de configuración de supresión de trampas.
2) el NMS activa el algoritmo de supresión de trampas (basándose en el estado de configuración de supresión de trampas). Si el estado de supresión de trampas está desactivado, no se hace supresión de trampas y a continuación las trampas pasarán.
3) el algoritmo de supresión de trampas lee su configuración y actualiza todos los parámetros requeridos: *latencia de supresión de trampas (en s.), tiempo de antigüedad de supresión de rampas* (e*n s.*)*, contador de supresión de trampas y tasa de llegada de supresión de trampas.*
4) el algoritmo de supresión está completamente configurado y listo para procesar trampas.
5) primera trampa recibida desde un nodo; el algoritmo de supresión de trampas notifica al administrador y proporciona descripción, una descripción breve acerca del emisor (el nodo de envío): dirección de IP del nodo y el tiempo en el que se enviaron las trampas.
6) el NSM mantiene registros del nodo que envía trampas: *el número de trampas enviadas hasta ahora, el primer tiempo y el último tiempo que se envió la trampa.*
7) el algoritmo de supresión de trampas evalúa (calcula) la tasa de envío de trampas
8) parar el procesamiento de trampas desde ese nodo cuando la tasa de envío de trampas es superior a la esperada (basándose en un umbral: la tasa de llegada de supresión de trampas).
9) notifica al administrador de modo que pueda tomarse acción adicional.
10) el algoritmo de supresión de trampas inicia el temporizador de latencia de trampa para ese nodo.
11) reanudar el procesamiento de trampas para ese nodo cuando el tiempo de latencia de trampas se agota (la latencia de trampas actual para el nodo se compara frente a la latencia de trampa configurada)
12) el administrador de red recibe notificación de esto.
13) si ese mismo nodo deja de enviar trampas durante un periodo de tiempo mayor o igual al tiempo de antigüedad del nodo, entonces el algoritmo envejece el nodo. El registro en la etapa 7 para ese nodo se borra.

La Figura 4 es un diagrama de flujo simplificado que representa las etapas de procedimiento del algoritmo.

El algoritmo cuando se implementa de acuerdo con la invención bloquea de manera eficaz que un nodo malicioso envíe tráfico indeseado al NSM. Permite también al administrador del NMS detectar qué nodo está enviando eventos de trampas al NSM. La primera vez que un nodo está enviando una trampa al NSM, el algoritmo, notifica al administrador del NMS independientemente de la tasa de trampas. El administrador de NSM puede realizar doble comprobación de los nodos que están enviando trampas. Cuando el NSM ya no gestiona el nodo se elimina de los

registros. El algoritmo permite la configuración de todos los parámetros requeridos para la supresión de trampas y aumenta la eficacia del NMS. Se anticipa que el algoritmo facilitará el uso de una alarma genérica tal como X.733 el formato de alarma convencional de facto en la industria. El algoritmo de la invención conduce a mayor eficacia de sistema en que únicamente se mantiene un registro de parámetros predefinidos para cada nodo gestionado para fines de supresión de trapas. Estos parámetros son: cálculo de tasa de llegada de trampas, cálculo de latencia de supresión de trampas y cálculo de tiempo de envejecimiento de nodo. De acuerdo con la invención el algoritmo sirve para notificar a la administración del NMS en las siguientes circunstancias:

- ♦ cuando un nodo envía una trampa la primera vez,
- ♦ cuando se bloquea la recepción de trampas
- ♦ cuando se reanuda la recepción de trampas
- ♦ cuando se envejece un nodo

El resultado es que los ataques tales como DoS e interrupciones de red se han de detectar y se han de tomar las etapas para superar los problemas que se derivan de ellos.

Las realizaciones presentadas son únicamente ejemplares y los expertos en la materia apreciarían que pueden realizarse variaciones a las realizaciones anteriormente descritas sin alejarse del alcance de la invención. El alcance de la invención se define únicamente por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento de supresión, en un sistema de gestión de red, de mensajes de trampas de eventos del protocolo de gestión de red simple, SNMP, desde nodos de red (A, B, C) en una red de comunicación, comprendiendo el procedimiento:

- contar, en el sistema de gestión de red, mensajes de trampa de eventos recibidos desde cada nodo de red (A, B, C) durante un intervalo de tiempo; y **caracterizado porque** el procedimiento comprende adicionalmente la etapa de:
- en respuesta a que el recuento supere un umbral, ignorar todos los mensajes adicionales de trampa de eventos enviados por ese nodo de red (A, B, C) al sistema de gestión de red hasta que se haya agotado un periodo de supresión predeterminado.

2. El procedimiento como se define en la reivindicación 1, en el que el periodo de supresión empieza desde un momento en el que se supera el umbral, después de que el agotamiento del sistema de gestión de red reanuda mensajes de procesamiento enviados por ese nodo de red (A, B, C).

3. El procedimiento como se define en la reivindicación 1, en el que el intervalo de tiempo es un intervalo predeterminado.

4. El procedimiento como se define en la reivindicación 1, en el que el intervalo de tiempo es programable.

5. El procedimiento como se define en la reivindicación 1, en el que el umbral se especifica en función de cada nodo.

6. El procedimiento como se define en la reivindicación 1, en el que el umbral se especifica basándose en el tipo de nodo (A, B, C) desde el que se reciben las trampas.

7. El procedimiento como se define en la reivindicación 1, en el que el umbral se especifica de acuerdo con el tipo de mensaje de trampa de evento recibido desde el nodo de red (A, B, C).

8. El procedimiento como se define en la reivindicación 1, en el que los mensajes de trampa de eventos ignorados de otra manera se someten a una característica de antigüedad que incluye el registro de los mensajes de trampa de eventos ignorados de otra manera, en el que los registros se mantienen para cada nodo (A, B, C) que está enviando mensajes de trampa de eventos de modo que puede volverse a aplicar la función de supresión de trampa a aquellos nodos (A, B, C), y en el que los registros que pertenecen a cualquier nodo dado (A, B, C) se borran después de un tiempo límite basándose en el tiempo del último mensaje de trampa de evento recibido desde que se ha agotado ese nodo (A, B, C) sin que se haya recibido ningún mensaje de trampa de eventos adicional.

9. El procedimiento como se define en la reivindicación 1, en el que el sistema de gestión de red registra selectivamente todos los nodos (A, B, C) que han superado su umbral de tasa de llegada de trampas.

10. El procedimiento como se define en la reivindicación 1, en el que el sistema de gestión de red proporciona selectivamente una notificación con respecto a los nodos (A, B, C) que han superado su umbral de tasa de llegada de trampas.

11. El procedimiento como se define en la reivindicación 10, en el que la notificación es una alarma.

12. El procedimiento como se define en la reivindicación 10, en el que la notificación alerta a un operador de que un nodo (A, B, C) ha superado el umbral de modo que puede tomarse una acción correctiva.

13. Un sistema de supresión, en un sistema de gestión de red, de mensajes de trampas de eventos del protocolo de gestión de red simple, SNMP, recibidos desde nodos de red (A, B, C) en una red de comunicación, comprendiendo el sistema

- un contador, en el sistema de gestión de red, para contar mensajes de trampa de eventos recibidos desde cada nodo de red (A, B, C) durante un intervalo de tiempo; y **caracterizado porque** el sistema comprende adicionalmente:
- medios, en respuesta a que el recuento supere un umbral, para ignorar todos los mensajes de trampa de eventos adicionales enviados por ese nodo de red (A, B, C) al sistema de gestión de red hasta que se haya agotado un periodo de supresión predeterminado.

14. El sistema como se define en la reivindicación 13, en el que el intervalo de tiempo tiene un valor predeterminado.

15. El sistema como se define en la reivindicación 13, en el que el intervalo de tiempo es programable.

16. El sistema como se define en la reivindicación 13, que incluye adicionalmente medios para registrar información relativa a mensajes de trampa de eventos que se han recibido en el sistema de gestión de red después de que se ha superado el intervalo de tiempo.

17. El sistema como se define en la reivindicación 16, que tiene medios heredados de supresión de trampa a un límite de tiempo establecido para bloquear mensajes de trampa de eventos después de que se ha superado el intervalo de tiempo.

18. El sistema como se define en la reivindicación 17, que tiene medios de antigüedad para establecer unos parámetros en cuanto a cuánto tiempo se retiene la información de registro.

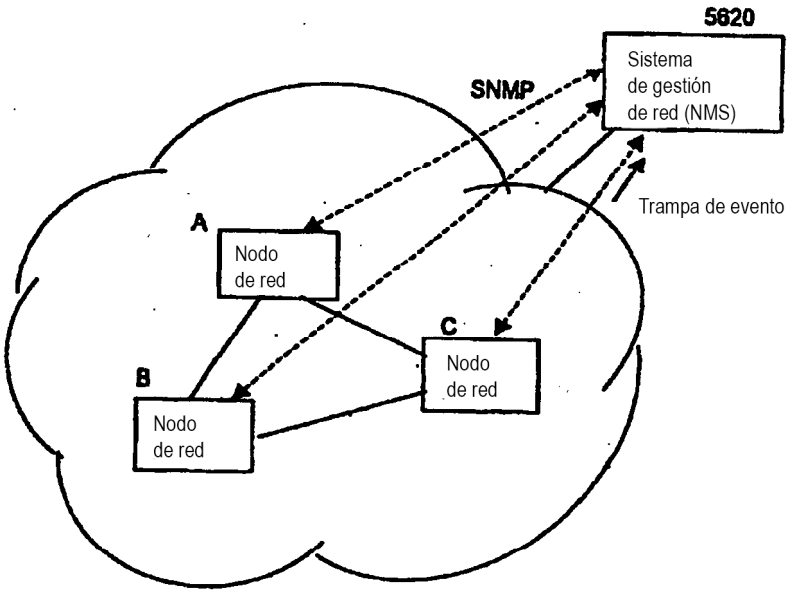
5820
Sistema
de gestión
de red (NMS)
SNMP
Trampa de evento
A
Nodo
de red
B
Nodo
de red
C
Nodo
de red

FIG. 1

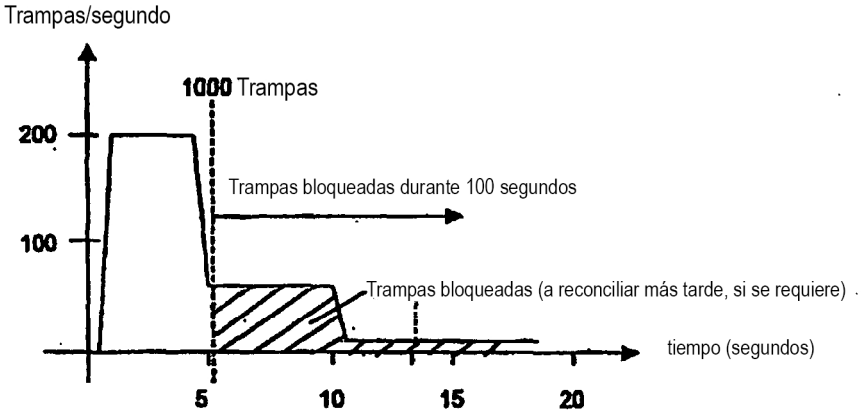
Trampas/segundo
1000 Trampas
200
100
Trampas bloqueadas durante 100 segundos
Trampas bloqueadas (a reconciliar más tarde, si se requiere)
tiempo (segundos)
5
10
15
20

FIG. 2

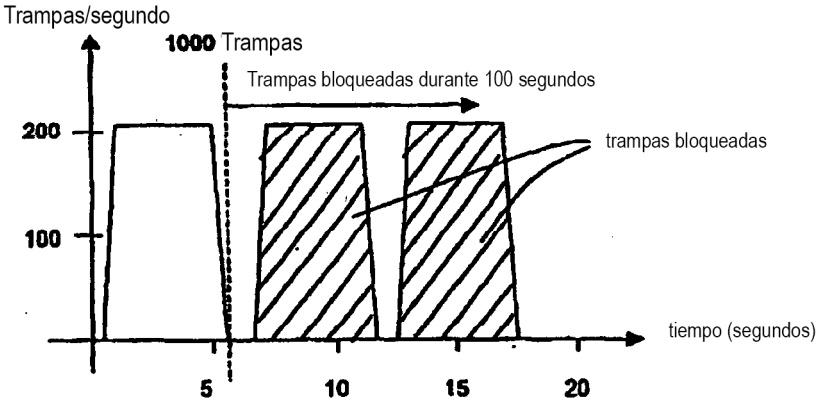
Trampas/segundo
1000 Trampas
Trampas bloqueadas durante 100 segundos
200
100
trampas bloqueadas
tiempo (segundos)
5
10
15
20

FIG. 3

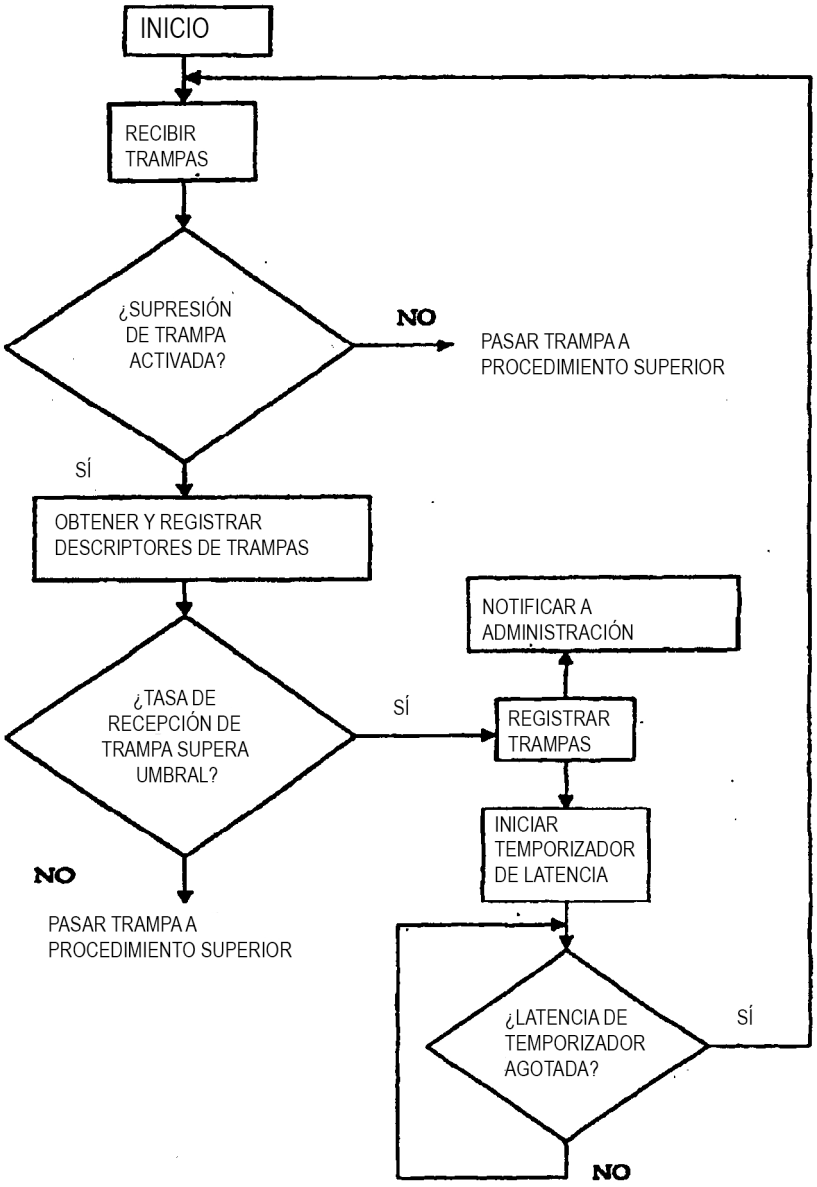
INICIO
RECIBIR TRAMPAS
¿SUPRESIÓN DE TRAMPA ACTIVADA?
NO
PASAR TRAMPA A PROCEDIMIENTO SUPERIOR
SÍ
OBTENER Y REGISTRAR DESCRIPTORES DE TRAMPAS
NOTIFICAR A ADMINISTRACIÓN
¿TASA DE RECEPCIÓN DE TRAMPA SUPERA UMBRAL?
SÍ
REGISTRAR TRAMPAS
INICIAR TEMPORIZADOR DE LATENCIA
NO
PASAR TRAMPA A PROCEDIMIENTO SUPERIOR
¿LATENCIA DE TEMPORIZADOR AGOTADA?
SÍ
NO

FIGURA 4