Revista Cubana de Ciencias Informáticas
ISSN: 1994-1536
ISSN: 2227-1899
Editorial Ediciones Futuro

Peña Casanova, Mónica; Lauriano da Silva, Joaquim;
Febles Díaz, Orestes; Anías Calderón, Caridad

Sistema Para Detección Y Aislamiento De Fallas

Revista Cubana de Ciencias Informáticas, vol. 12, núm. 2, 2018, Abril-Junio, pp. 58-73
Editorial Ediciones Futuro

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Tipo de artículo : Artículo original
Temática: Tecnologías de la información y las telecomunicaciones
Recibido: 31/08/2017 | Aceptado: 22/03/2018

SISTEMA PARA DETECCIÓN Y AISLAMIENTO DE FALLAS

FAIL DETECTION AND ISOLATION SYSTEM

Msc. Mónica Peña Casanova[1*], Lic. Joaquim Lauriano da Silva[2]; Dr. Orestes Febles Díaz[3], Dra. Caridad Anías Calderón[4]

[1] Universidad de las Ciencias Informática, Cuba. monica@uci.cu

[2] Universidad Agostinho Neto, Angola. joaquim.laurianoo@gmail.com

[3] Unión de Informáticos de Cuba, Cuba. ofebles@uic.cu

[4] Universidad Tecnológica de La Habana, Cuba. cacha@tesla.cujae.cu

[*] **Autor para correspondencia**: monica@uci.cu

Resumen

Actualmente existen una gran cantidad de soluciones encaminadas a detectar y corregir fallas, de manera temprana, en el equipamiento activo de las redes. Estas funcionan solo a partir del monitoreo de la red y no están exentas de generar falsos positivos o múltiples alarmas que desorientan a los administradores sobre el origen y la localización de las fallas. La detección tardía implica la degradación de los servicios que se ofrecen provocando el incumplimiento de los acuerdos de nivel de operación y de servicio. Las herramientas existentes, resultan insuficientes para correlacionar el impacto asociado a la ocurrencia de fallas para automatizar las tareas relacionadas a la solución de las mismas. El presente trabajo propone un sistema para la disminuir la degradación de los servicios a partir de la detección temprana de los síntomas relacionados con la ocurrencia de las fallas en el equipamiento activo, minimizando el impacto en los usuarios. El sistema incorpora una arquitectura de Gestión Basada en Políticas que permite la corrección automatizada de las fallas disminuyendo la afectación en los servicios. Además, agiliza la localización de las fallas a través de la aplicación de un algoritmo de detección de cambios al análisis de parámetros en variables de las MIB del equipamiento activo de redes. El mismo permite el análisis panorámico de la red empleando un modelo de detección de anomalía basado en grafos, que además considera, el control de los activos y la estructura de la red almacenados en una Base de Datos de Gestión de Configuración.

Palabras clave: Gestión de fallas, gestión de redes basada en políticas, PBNM, gestión de configuración

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Abstract

Nowadays we can find several solutions for early faults detection and correction in active network equipment. These are network monitoring based mechanisms, but they could provoke false positives or generate multiple alarms that would disorient managers about the failure´s origin. Delayed detection implies the degradation of the services offered, causing non-compliance of service level agreements and operations. The existing tools are insufficient to correlate the impact associated with the occurrence of failures for automating tasks related to their solution. This paper presents a system to reduce the degradation of services; from the early detection of the symptoms related to the occurrence of failures in the active equipment, minimizing the impact in users. The system incorporates a Policy Based Management architecture that allows automatic correction of failures, reducing the interruption of the services. In addition, it speeds up the location of faults through the application of an algorithm of changes detection in the analysis of parameters in IBM variables of the active equipment of networks. It allows the panoramic analysis of the network using a graph based anomaly detection model, which also considers the control of the assets and the network structure stored in a Configuration Management Database.

Keywords: *configuration management, fault management, PBNM, policy based network management*

Introducción

En la medida que las organizaciones informatizan sus procesos y se hacen más dependientes de las tecnologías, aumenta el impacto que la degradación de los servicios telemáticos y el incumplimiento de los niveles de operación, provocados por las fallas en las infraestructuras Tecnologías de la Información (TI) pueden provocar en las mismas. De ahí que la gestión de fallas debe realizarse de manera temprana, tomando rápidas decisiones correctivas, basadas en la evaluación del impacto de los daños en el equipamiento provoca en las organizaciones. Múltiples esfuerzos se realizan en torno a la gestión de fallas, que incluye acciones de monitoreo para la detección, aislamiento de estas y acciones de control para la corrección de problemas. (Hassett 2016).

Entre las soluciones que han sido desarrolladas para la detección, localización y aislamiento de fallas en la red, se destaca el empleo de: máquinas de estado finito (Hassett 2016), métodos estadísticos, aproximaciones basadas en reglas, ajustes de patrones, redes neuronales, lógica fuzzy y teoría de grafos (Matsumoto 2016, Chenaru 2016). Los resultados alcanzados a través de las mismas solo han proporcionado una vista local de la falla, y por lo tanto no

pueden describirla, hasta que sus consecuencias son visibles, de ahí que sea necesario complementarlos con mecanismos para la localización, los cuales son responsables del análisis de las alarmas generadas por los componentes de la red proponiendo posibles hipótesis sobre la causa de la falla (Souza 2016).

La ejecución de acciones correctivas que minimicen el impacto de las fallas en la organización sigue dependiendo del nivel de experticia del equipo de administración de redes, de ahí que persiste la necesidad de automatizar dichas acciones. (Youssfi 2014).

El presente artículo propone un sistema para disminuir efectivamente la degradación de los servicios en el equipamiento activo de la red a través de la automatización de la detección y aislamiento de fallas, facilitando la localización temprana de los síntomas que preceden a la ocurrencia de estas y automatizando la aplicación de medidas de control, reduciendo los tiempos de recuperación y el impacto de las fallas.

Metodología computacional

En los últimos años muchas soluciones han sido desarrolladas para la detección, localización y aislamiento de fallas en la red (Mohiuddin 2016). La detección de fallas puede entenderse como una indicación en línea de que algún componente de la red está funcionando incorrectamente. Estos componentes solo tienen una vista local de la falla, y por lo tanto no pueden describir la falla, hasta que sus consecuencias son visibles (Kleinsteuber 2016, Mohiuddin 2016).

Los algoritmos para la detección de fallas están divididos en dos categorías; los basados en el patrón de la anomalía y los basados en el comportamiento normal de la red. Los basados en el patrón de la anomalía requieren tener un conocimiento previo sobre las fallas para su posterior modelación, lo que no siempre es posible debido a la propia complejidad de los entornos de red, de ahí de que nuevos tipos de fallas pueden ocurrir sin ser detectadas (Chu 2015).

En el caso de los algoritmos basados en el comportamiento normal de la red, se crea un perfil que almacena los parámetros de funcionamiento normal en el equipamiento activo de la red, a partir de lo cual se definen los Acuerdos de Nivel de Operación y Servicio. Los desvíos de este perfil representan las anomalías, o sea los síntomas asociados a la ocurrencia de una falla, estos se detectan a partir de algoritmos de detección de cambios. Entre los algoritmos de detección de cambios se destaca el propuesto por Thottan y Ji. (Roy 2014, Bhuyan 2014). Este algoritmo resulta eficiente para detectar fallas a nivel de equipos de interconexión, ya que analiza los componentes de la red de forma individual y genera alarmas, presentando insuficiencias a la hora de evaluar propagación de las anomalías para evaluar el impacto de las fallas.(Ji 2003, M. Thottan 2010)

En una red de computadoras, una única falla puede generar varias alarmas, lo que frecuentemente dificulta el aislamiento de la causa primaria de esta. Algunas de las técnicas que permiten la localización o aislamiento de la causa raíz de la falla son: los sistemas basados en reglas, la teoría de grafos y algoritmos que se desarrollan considerando la estructura de la red. Los sistemas basados en reglas presentan insuficiencias para la adaptación a nuevos problemas que no forman parte de la base de datos, lo que requiere el incremento constante de reglas y dificulta su manutención. Los grafos, que representan las relaciones de dependencia entre los componentes de la red y permiten la modelación de la propagación, pueden ser adicionados en la base de conocimiento para mejorar la capacidad de diagnóstico y adaptación a nuevos problemas. La definición de un modelo propagación de anomalías no es sencillo y se pueden ignorar anomalías no previstas durante el diseño. (Matsumoto 2016, Chenaru 2016).

En el modelo de detección de anomalías en redes de computadoras propuesto por Zarpelão, la estructura de la red se representa por medio de un grafo, donde cada vértice representa uno de los dispositivos en la red y los bordes representan los enlaces entre estos dispositivos. En él se hace la correlación de las alarmas, lo cual permite visualizar la propagación de los síntomas sobre la red (Amaral 2010, Oliveira 2014, Kawakani 2016).

Una vez representada la estructura de la red y los enlaces de los dispositivos, es preciso correlacionarlo con los atributos de cada uno de ellos, determinar sus relaciones, así como los servicios que soportan para facilitar la toma de decisiones, en el momento que sea preciso, y aplicar políticas. Para lograr lo anterior, es necesario integrar al modelo a una Base de Datos de Gestión de Configuración (Cruz-Hinojosa 2016). Al correlacionar la estructura de la red obtenida a partir de la aplicación del modelo de Zarpelão con la Base de Datos de Gestión de Configuración, se puede evaluar el impacto de la propagación de los síntomas en la red, facilitando la toma de decisiones. (Sánchez 2013).

La arquitectura para gestión de más amplio uso para el monitoreo del equipamiento activo de redes es sin dudas SNMP (*Simple Network Management Protocol*, por sus siglas en inglés), la cual se basa en la interrelación de tres componentes básicos: un gestor, un agente, y una base de datos de información de gestión o MIB (*Management Information Base*, por sus siglas en inglés). Cada agente almacena datos de gestión en la MIB y responde a las preguntas del gestor SNMP (Jae-Young Kim 2016).

Debido a la complejidad y el gran tamaño de los entornos de red actuales, se hace necesaria la automatización de las tareas de control, siendo la gestión basada en políticas una de las técnicas empleadas en este contexto. El *Internet Engineering Task Force* (IETF) propuso una arquitectura de gestión de red basada en políticas (*Policy Based Network Management*, por sus siglas en inglés) que permite automatizar la aplicación de medidas de control sobre la red en función de las condiciones dinámicas de la propia red (Odagiri 2014). En esta arquitectura está compuesta por una

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Herramienta de gestión de políticas, un contenedor de políticas, un punto de ejecución de políticas y un punto de decisión de políticas (Haddadou 2012, Odagiri 2014)

Resultados y discusión

Propuesta de sistema de detección y aislamiento temprano de fallas en el equipamiento activo de la red

El sistema de detección y aislamiento de fallas tiene como objetivo mantener el control de los activos de la red, conocer de la estructura de la misma, detectar anomalías que tienen implicación en su rendimiento y evitar su propagación sobre esta, además debe permitir, crear políticas para evitar que las anomalías causen la interrupción de los servicios de la red.

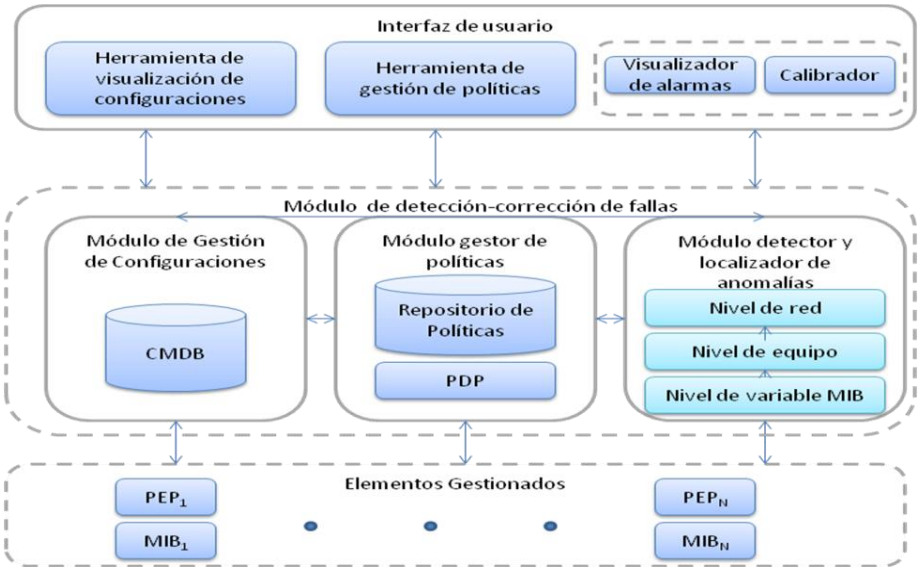

Figura 1 - Arquitectura del sistema de detección y aislamiento de fallas en la red

Para lograr su objetivo, conforme ilustra la figura 1, la arquitectura posee tres módulos, organizados de tal forma que la comunicación entre ellos permite prevenir efectivamente la degradación del funcionamiento de los elementos gestionados:

- Módulo de gestión de configuraciones, en la que se mantiene la información de los activos de la red, y el conocimiento de la estructura del equipamiento activo.
- Módulo detector y localizador de anomalías, en el que se detectan las anomalías que tienen implicación en el rendimiento de la red, se localiza la raíz y visualiza su propagación sobre la red.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

- Módulo gestor de políticas, es en el que se crean las políticas para evitar que las anomalías causen la interrupción de los servicios de la red.

Módulo base de datos de gestión de configuraciones

El módulo base de datos de gestión de configuraciones es el elemento base del sistema. Su inclusión, tiene como finalidad resolver la deficiencia en el control de inventario de los activos del equipamiento activo de la red (hardware y software), facilitando la localización física de equipos, así como su vinculación con los servicios de red que soportan, elemento importante en la toma de decisiones y para la ejecución de políticas.

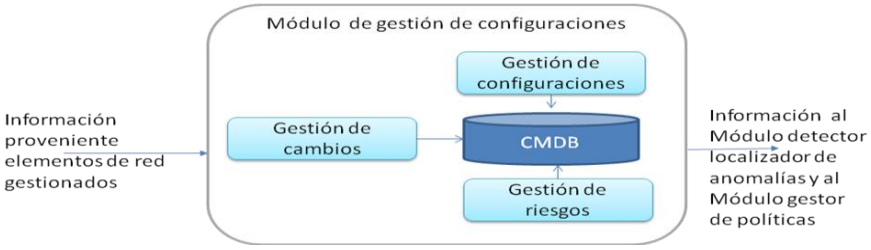

Figura 2 – Grupos de funcionalidades del módulo de gestión de configuraciones

Como se observa en la figura 2, sobre su estructura operan los demás módulos. Obtiene información proveniente de los elementos gestionados y entrega información a Módulo detector localizados de anomalías y al Módulo gestor de políticas, que este utiliza para la evaluación de condiciones. No siendo suficiente tener una lista de los activos de la red, el control inventario se extiende hasta el mantenimiento del registro actualizado de todos los activos y sus características, las interrelaciones entre ellos, los riesgos asociados a cada uno de ellos, los cambios efectuados en la red y la representación de la topología.

A tal efecto, el módulo CMDB provee funcionalidades de los procesos gestión de configuraciones, de cambios y de riesgos, conforme ilustra la Figura Cumpliendo estas funcionalidades, el módulo CMDB permite verificar el cumplimiento de las políticas para llevar a cabo los controles de activos. Sobre los activos controlados por este módulo operan los módulos detector y localizador de anomalías y el gestor de políticas.

Módulo detector y localizador de anomalías

El Módulo detector y localizador de anomalías es responsable de detectar los síntomas asociados a la ocurrencia de posibles fallas en la red.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

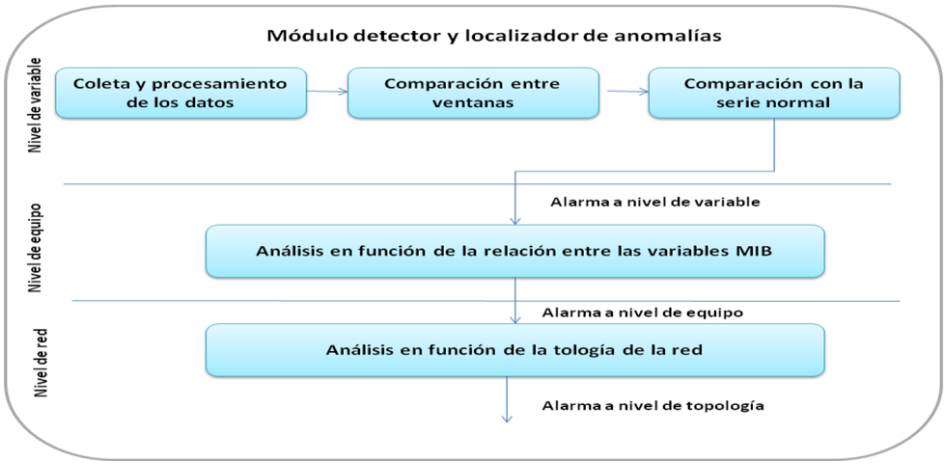

Figura.3 – Niveles de análisis y flujo de información en el Módulo detector y localizador de anomalías

Su función dentro de la arquitectura, es proveer un enfoque de análisis distinto a la evaluación de los parámetros de QoS y rendimiento físico de los equipos, en la detección de los síntomas y permitir visualizar la propagación de los síntomas sobre la red. Lo anterior implica la detección temprana de la falla y la localización de la raíz. Para cumplir con su propósito, en el módulo detector y localizador de anomalías se hace un análisis en tres niveles, respectivamente: a nivel de variable MIB, a nivel de equipo y a nivel de la topología de red. En la figura 3 se observan, los diferentes niveles de análisis para este módulo, así como las tareas que se ejecutan en cada uno de ellos, el análisis a nivel de variable MIB se realiza mediante la implementación del algoritmo de detección de cambios propuesto por Tottan& Yi y en los restantes niveles de análisis se emplea el modelo de detección de anomalías en redes de computadoras desarrollado por Zarpelão. Este modelo no incluye la fuente de datos sobre la topología de la red, para lo cual se concibe, como parte de este trabajo, el uso de una CMDB, lo cual permitirá, además de la obtención del dispositivo raíz de los síntomas que se propagan sobre la red, el conocimiento de las características del mismo y su localización física.

A. Análisis a nivel de variable MIB

El análisis a nivel de variable MIB se realiza a través del algoritmo propuesto por Tottan& Yi. Se efectúan dos etapas, en la primera, se hace la recopilación y procesamiento de los datos y en la segunda, a través de métodos estadísticos, se verifica si existen o no anomalías.

La primera etapa consiste en la observación con una periodicidad ajustable por el administrador, de los valores de las variables MIB. Estos valores son cambiantes en el tiempo y forman series temporales no estacionarias. Estas series temporales son divididas en segmentos estacionarios, los que se modelan utilizando un proceso auto regresivo y se

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

aplica una prueba de hipótesis basado en la razón verosimilitud generalizada (Lozano 2016, González-Betanzos 2015), entre ventanas de tiempo adyacentes para detectar los cambios bruscos entre las dos series. En caso de detectarse dichos cambios se generan alarmas a nivel de variable MIB.

B. Análisis a nivel de equipo

Realizado el análisis en el nivel de variable, se hace el análisis a nivel de equipo, con el objetivo de determinar si las alarmas generadas a nivel de variable MIB corresponden a una anomalía o no. Para la obtención de la relación entre dichas variables se utilizaron dos conjuntos que representan la relación asociadas al transporte de datos en los niveles de enlace, red y transporte, respectivamente los grupos *interface*, *ip*, *tcp* y *udp* de una MIB.

Forman parte del primer conjunto, el conjunto de entrada de datos en el dispositivo las variables: *IfInOctets*, *IpInReceiveds* y *tcpInSegs.* Del segundo conjunto que representa la salida de datos del dispositivo forman parte las variables: *IfOutOctets*, *IpOutRequest* y *TcpOut.* Se utiliza un grafo direccionado G= (V, E) para representar la relación entre las variables MIB en cada uno de los conjuntos, donde cada vértice V representa la variable MIB analizada y los bordes E representan la relación entre las mismas. Cada borde en este grafo es representado por el par ordenado (x, y). El sentido de los bordes representa el sentido en que una anomalía se puede propagar dentro de cada conjunto, y de acuerdo al tipo de equipo, existe un conjunto de variables definidas como iniciales y otras como finales.

```
    Programa principal
1.  Inicio
2.      Para cada v ∈ (V_i ∩ V_a) haga
3.          BusquedaProfundidad(v)
4.  Fin Programa
    Procedimiento BusquedaProfundidad(v)
5.  Inicio
6.      Marcar v como visitado
7.      Empilar v en P
8.      Si (v ∈ V_f) entonces
9.          Anomalía detectada;
10.     Para cada (v' ∈ C(v)) haga
11.         Si v' no esta marcado entonces
12.             BusquedaProfundidad(v')
13.     Fin para
14.     Desenfilar P
15. Fin procedimiento
```

Figura.4 - Correlación de alarmas a nivel de variable MIB

Teniendo en cuenta el sentido de propagación de una anomalía en cada uno de los conjuntos, la correlación entre las alarmas a nivel de variable MIB es realizada de la siguiente forma:

- Cuando es generada una alarma para una de las variables del conjunto, se verifica si existen alarmas para las demás variables del conjunto.

- Si se comprueba la existencia de alarmas para todas las variables del mismo conjunto, significa que hay una anomalía que se propaga sobre este conjunto.
- En el caso de que se haya identificado la ocurrencia de la anomalía para determinado conjunto, es generada una alarma a nivel de equipo para el respectivo conjunto.

El proceso de correlación es descrito por el algoritmo de búsqueda a profundidad de la figura 4 en que se tiene como entradas las alarmas de nivel de variable MIB y como salida las alarmas a nivel de equipo. Donde Vi es el conjunto de variables definidas como iniciales, Vf es el conjunto de variables MIB definidas como finales, conjunto de variables con alarmas, P es la pila utilizada en la búsqueda a profundidad, C (v) es la función que retorna todas las variables que son adyacentes y que presentan alarmas. La presencia de alarmas a nivel de equipo, da lugar al análisis a nivel de topología de la red.

C. Análisis a nivel de topología de la red

El análisis a nivel de topología de la red, tiene como objetivo presentar el escenario de propagación de las anomalías sobre la red, para lo cual, se extrae la topología de la red de la CMDB, y se utilizan grafos para representar la misma. Cada dispositivo en la red es representado por un vértice del grafo y los enlaces entre ellos son los bordes. Una anomalía puede tener inicio, fin o encaminarse en uno de los dispositivos. La estructura del grafo que representa la topología de la red, permite obtener una visualización de la propagación de una anomalía sobre vértices adyacentes. Finalmente se hace una correlación temporal de las alarmas a nivel de dispositivo, y de acuerdo a la topología de la red, de manera tal que se obtiene una representación de la propagación de la anomalía sobre la red. El análisis de propagación de anomalías sobre la red, facilita que el administrador visualice sobre qué servicios impactarán esas anomalías y de acuerdo a su experiencia aplique medidas de control. El módulo gestor de políticas permite a la automatización de estas medidas de control.

Módulo gestor de políticas

El módulo gestor de políticas se encarga de la automatización de las tareas de control, permite las definiciones de políticas teniendo en cuenta las alarmas a nivel de dispositivo y su propagación sobre la red y su impacto sobre los principales servicios que se prestan sobre ella.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

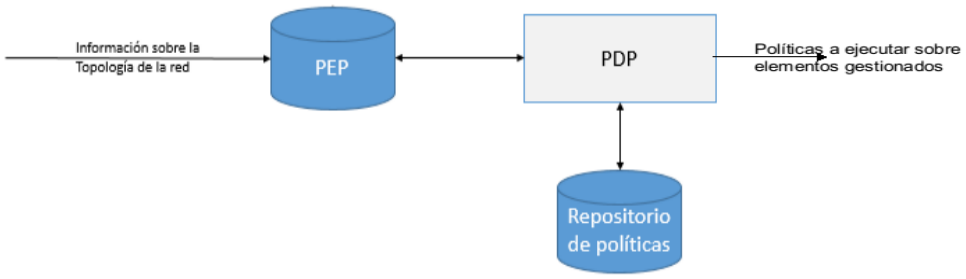

Figura.5 – Modulo Gestor de Políticas

La figura 5 representa el funcionamiento de este módulo. Este se comunica con el módulo de gestión de configuraciones solicitando información de los dispositivos que componen la red, los cuales corresponden a los puntos de ejecución de políticas. La aplicación de políticas sobre los PEP depende de las alarmas que provee el módulo detector y localizador de anomalías, las cuales reflejan el estado de los PEP. La aplicación conjunta de algoritmos para el diagnóstico de fallas en la red y la PBNM permite la elaboración de políticas teniendo en cuenta los síntomas asociados a las fallas, añadiendo al proceso de gestión de red tradicional, la capacidad de toma de decisiones, y permitiendo finalmente la ejecución de estas sobre los dispositivos de red.

Despliegue de la arquitectura en un entorno simulado

Para la validación de la arquitectura, se desplegó un entorno de prueba simulado. Se utilizó GNS3 como la herramienta simuladora de red, la cual permite el trabajo con otros programas para lograr la emulación de dispositivos de redes reales, creando una plataforma que permite el fácil diseño de topologías de redes complejas (Antunes 2015).

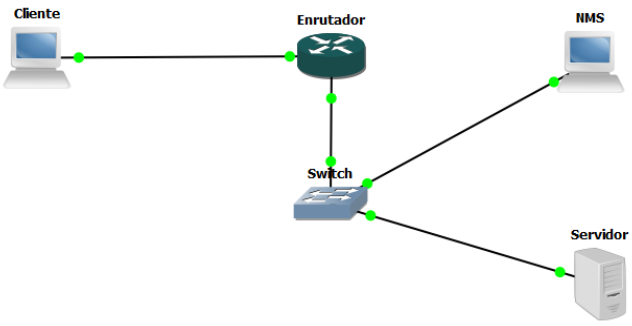

Figura.6 –Topología de la red creada con GNS3

La figura 6 representa la topología creada en el GNS3 con los equipos presentes en Tabla 1. Tanto en la máquina NMS como en el enrutador fueron instalados y configurados agentes SNMP.

Tabla 1 Equipos de la topología simulada con GNS3

Nombre de equipo	Descripción.

Cliente	En él se simula la generación del tráfico anómalo en la red utilizando la herramienta Ostinato que permite la generación de gran volumen de datos con los protocolos TCP, UDP e ICMP.
Servidor	Recibe el tráfico anómalo proveniente del cliente.
NMS	Es la estación de gestión donde se encuentra el sistema de detección y aislamiento de fallas
Enrutador	Responsable por el encaminamiento de paquetes entre Cliente y Servidor
Switch	Switch que conecta las máquinas Servidor y NMS a la red

Se adoptó la CMDB ITOP para realizar las funcionalidades referentes al módulo base de datos de gestión de configuración, debido a que la misma cumple con casi todos los requisitos funcionales para este módulo y, es de distribución libre y de código abierto, lo que permite su extensibilidad (Allqui 2015).

Tabla 2 Pruebas realizadas

Número del test	Tipo de Condición	Alarmas Generadas	Clasificación
1	FNR	0	Positivo
2	FNR	0	Positivo
3	FAR	2	Positivo
4	FNR	0	Positivo
5	FAR	2	Positivo

En la tabla 2 se presenta el resultado de las pruebas realizadas. La prueba consiste en la evaluación del comportamiento del sistema bajo las siguientes condiciones:

- Funcionamiento normal de la red (FNR), en el que la red opera sin grandes cantidades de tráfico.
- Funcionamiento anormal de la red (FAR), en el que se genera grandes cantidades de tráfico en determinado punto de la red para simular el comportamiento anormal que tienen implicación en el rendimiento de la red.

. Cada prueba realizada tiene una de las siguientes clasificaciones:

- Positivo: cuando el resultado de la prueba es exactamente el esperado en función del tipo de condición.
- Negativo**:** cuando el resultado de la prueba realizada no es el esperado para el tipo de condición definida.

La prueba dos se realizó con el objetivo de evaluar la calibración del sistema de detección y aislamiento de fallas, esta calibración deberá realizarse por parte del administrador que opera la red en función de las necesidades de esta.

En la prueba número tres fueron generadas alarmas a nivel de equipo. Las pruebas cuatro y cinco fueron realizadas con las mismas condiciones establecidas con el fin de verificar si el sistema se comportaría de la misma forma.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 2, Abril-Junio, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Figura. 7 Alarma a nivel de topología

La Figura 7 presenta la forma en que las alarmas a nivel de equipo son vistas desde la perspectiva de la topología de la red, como se puede observar, se tiene la información sobre el equipo, que genera el tráfico anómalo, el equipo de destino y la hora.

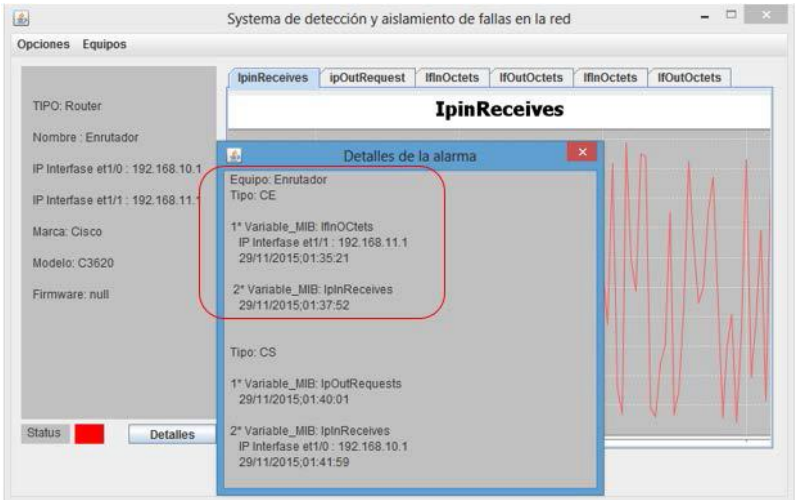

Figura. 8 Detalles de la alarma a nivel de equipo

En las pruebas en que se generaron alarmas a nivel de equipo, las mismas correspondieron a los dos conjuntos de alarmas. Como se puede observar, fueron generadas alarmas de entrada y de salida en el enrutador. Para las alarmas de entrada corresponde al tráfico anómalo que es generado en la subred 192.168.11.0/24 por la máquina Cliente con dirección IP 192.168.11.2 para el puerto del enrutador en esta subred con dirección IP 192.168.11.1. Esta alarma corresponde a la correlación de las alarmas a nivel de variable MIB para las variables *IfInOctets*, e IpInReceives conforme indica el área seleccionada en la figura 8.

La capacidad del sistema de generar alarmas y de visualizarlas desde la perspectiva de red, facilita la localización temprana de fallas, minimizando el impacto de estas en la degradación de los servicios. Por otra parte, su capacidad

de automatizar las tareas de gestión, asociadas a la corrección de las fallas impacta en la mejora de la calidad de los servicios.

Conclusiones

A partir del estudio de los elementos claves para la detección y aislamiento de fallas, se logró la modelación de un sistema para la detección y aislamiento de fallas en el equipamiento activo de la red, presentándose la arquitectura del mismo.

El sistema propuesto incluyó una herramienta que integra las funcionalidades de una base de datos de gestión de configuraciones para el control de los activos de la red, algoritmos proactivos en la detección y aislamiento de fallas en el equipamiento activo de la red, y la automatización de medidas de control empleando una arquitectura de Gestión de Redes Basada en Políticas.

El módulo base de datos de gestión de configuraciones es un elemento clave del sistema, pues permite realizar el control de inventario de los activos de red. En el caso de ocurrir fallas, para cada problema, debe haber un registro en la CMDB conteniendo los CI implicados, causas, síntomas asociados, soluciones temporales, servicios involucrados, niveles de prioridad, urgencia, impacto y estado, lo que facilita la toma de decisiones.

El módulo detector y localizador de anomalías, realiza un análisis a nivel de las variables MIB del equipamiento activo, de manera escalonada, hasta cubrir la topología del sistema, útil para localizar posibles. Además, dicho módulo permite visualizar la afectación de los síntomas en la red y en los servicios que soporta, facilitando la detección temprana de la falla, antes que la misma pueda percibirse por parte de los usuarios.

El módulo gestor de políticas del sistema efectúa la automatización de las tareas de control, para corregir los síntomas asociados a las fallas. Dota al sistema de la capacidad de tomar de decisiones a partir de políticas definidas para la configuración de los elementos activos de red, que se ejecutan en los mismos.

Las pruebas realizadas al sistema en el escenario de red simulado, empleando la plataforma GNS3, permitió verificar que el mismo, previa calibración por parte del administrador, disminuye efectivamente la degradación de los servicios.

Referencias

ALLQUI, V. E. C. (2015). Estudio de operación de los servicios de tecnologías de la información mediante el estándar ITIL con el aplicativo "Software para la Gestión de Incidentes de Tecnologías de la Información" en el Departamento de Sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Santiago de Quero: Facultad de Ingeniería en Sistemas Electrónica e Industrial. Ambato – Ecuador, UNIVERSIDAD TÉCNICA DE AMBATO. Ingeniero en Sistemas Computacionales e Informáticos: p152.

AMARAL, A. A., ZARPELÃO, B. B., RODRIGUES, J. J. P. C., MENDES, L. S., PROENÇA JUNIOR, M. L. (2010). Analysing network-wide anomalies using dependency graphs and baseline International Conference on Software, Telecommunications and Computer Networks (SoftCOM)**:** 310 - 314.

ANTUNES, R. E. M. (2015). Automatic network configuration in virtualized environment using GNS3. 10th International Conference on, Cambridge, Cambridge.

BHUYAN, M. H.; BHATTACHARYYA, D. K.; KALITA, Jugal K. Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, 2014, vol. 16, no 1, p. 303-336.

CHENARU, O.D.. (2016). Practical fault management using real-time decision tree analysis. 24th Mediterranean Conference on Control and Automation (MED). Athens**:** 384-389.

CHU, Q. Z. A. T. (2015). "Structure regularized traffic monitoring model for traffic matrix estimation and anomaly detection. Control Conference (CCC). Chinese, Hangzhou**:** 4980-4985.

CRUZ-HINOJOSA, N. J. G.-D.-M., José Antonio. (2016). "Literature review of the situation research faces in the application of ITIL in Small and Medium Enterprises." Computer Standards & Interfaces**48**: 124-138.

HADDADOU, K.; SAMIR; GHAMRI-DOUDANE, Y.; AGOULMINE, N. (2012). "Practical and analytical approaches for designing scalable on-demand policy-based resource allocation in stateless IP networks." International Journal of Network Management**22** (2): 1099-1190.

HASSETT, B. (2016). Recovery from multiple faults in a communications network **US 9331897 B2**.

JAE-YOUNG, K; M.-S. K., WON-KI HONG, TAE-SANG CHOI, YOON-HEE JUNG, AND SUNG-WON SOHN (2016). "Design and Implementation of a Management System for Differentiated Services Using the SNMP Framework." Journal of Communications and Networks, Special Issue on QoS in IP Networks.

JI, M. T. A.. (2003). "Anomaly Detection in IP Networks." IEEE Transactions in Signal Processing. **51** (8).

SÁNCHEZ P., JJ. E. F. V., ANTONIO MORATILLA OCAÑA (2013). "ITIL, COBIT and EFQM: Can They Work Together?" International Journal of Combinatorial Optimization Problems and Informatics**4**: 11.

KAWAKANI, C. T., BARBON JUNIOR, S., MIANI, R. S., CUKIER, M., ZARPELÃO, B. B (2016). Intrusion Alert Correlation to Support Security Management. XII Simpósio Brasileiro de Sistemas de Informação (SBSI). Brasil.

KLEINSTEUBER, H. K. W. K. M. (2016). "Network Volume Anomaly Detection and Identification in Large-scale Networks based on Online Time-structured Traffic Tensor Tracking." IEEE Transactions on Network and Service Management **PP** (99): 1.

LOZANO FORERO, Sébastien (2016). REFINAMIENTO DE PRUEBAS DE HIPÓTESIS ASINTÓTICAS. II Encuentro Colombiano de Educación Estocástica, ISSN 2390-0172, p. 56.

M. THOTTAN, G. L., C. JI (2010). Anomaly Detection Approaches for Communication Networks. Algorithms for Next Generation Networks, Springer-Verlag

MATSUMOTO, A., et al (2016). Fault management system. Fault management server, and non-transitory computer-readable storage medium in which fault management program is stored.

MOHIUDDIN, A. N. M., JIANKUN HU (2016). "A survey of network anomaly detection techniques." Journal of Network and Computer Applications**60**: 19–31.

ODAGIRI, K. S., ISHII, N. AND TAKIZAWA, M. (2014). Functional Experiment of Virtual Policy Based Network Management Scheme in Cloud Environment. 17th International Conference on Network-Based Information Systems, Salermo.

OLIVEIRA, P. H., ZARPELÃO, B. B., KASTER, D. S. (2014). Aumentando o Desempenho de Análises de Dados de Fluxos IP com Bancos de Dados Orientados a Coluna. X Simpósio Brasileiro de Sistemas de Informação (SBSI). Brasil.

ROY, Debdutta Barman; CHAKI, Rituparna.(2014) State of the art analysis of network traffic anomaly detection. En *Applications and Innovations in Mobile Computing (AIMoC)*. IEEE, p. 186-192.

SOUZA, V. S., SE) (2016). METHOD AND ARRANGEMENT FOR FAULT MANAGEMENT IN INFRASTRUCTURE AS A SERVICE CLOUDS Telefonaktiebolaget L M Ericsson (publ) (Stockholm, SE)

YOUSSFI, K. J. B., SOUHAIL ELGHAZI (2014). "A Tool Design of Cobit Roadmap Implementation." (IJACSA) International Journal of Advanced Computer Science and Applications.**5**.