CAPITULO VI. SISTEMA DE DETECCIÓN Y DIAGNÓSTICO DE FALLAS EN REDES LAN COMO ALTERNATIVA DE TOMA DE DECISIONES DE LOS ADMINISTRADORES DE RED.

Autores:

Mitchell Vásquez Bermúdez, Mgs.
Universidad Agraria del Ecuador. Universidad de Guayaquil
mvasquez@uagraria.edu.ec,

Karla Maribel Galarza Ayala, Mgs.
Universidad Agraria del Ecuador
karly.galarza@gmail.com

Jorge Hidalgo Larrea, Mgs.
Universidad Agraria del Ecuador
jhidalgo@uagraria.edu.ec

María Del Pilar Avilés Vera, Mgs.
Universidad Agraria del Ecuador
maviles@uagraria.edu.ec

INTRODUCCIÓN

La gestión de administración de redes suele ser la parte más importante y crítica dentro de todas las actividades que realizan los administradores de red, debido a que su control debe ser constante y se debe contar con una plataforma de comunicación estable para la adecuada gestión de los ordenadores que se encuentran conectados a la red.

Para el administrador de red solucionar un fallo puede tomarle un tiempo considerable más aún identificar que originó el problema de la red. El problema puede tener varias causas desde software mal configurado o infraestructura mal colocada como por ejemplo un cable de red, esto sin contar que el administrador no podrá estar monitoreando permanentemente la red.

Cuando existen problemas y fallos en la red, su principal síntoma es el bajo rendimiento de toda la red. En la mayoría de organizaciones donde no se encuentra un sistema para el monitoreo, no siempre es el administrador el que se entera del error, sino el usuario que al usar un recurso se da cuenta que este no está disponible.

Se puede mencionar cuando el usuario final utiliza una computadora para el servicio de internet y compartición de archivos con otros usuarios, observa en su funcionamiento un bajo rendimiento, lentitud o anomalías en sus tareas, lo que conllevaría al administrador de red tardarse horas e inclusive días para encontrar el problema. Si sucediera este mismo inconveniente a la red de una Pyme, implicaría un crecimiento de los problemas y las consecuencias también.

Para la gestión de fallos en una red se necesita una gran cantidad de información que permita analizar y deducir los síntomas que al ser comparados en el sistema pueda reducir el número de posibles soluciones que se tendrá para resolver el inconveniente.

Existen en la actualidad diferentes herramientas que sirven de ayuda para los administradores de redes, pero estos sistemas debido a su complejidad y difícil comprensión al momento de tratar de solucionar un fallo, suelen no ser los más eficientes, si bien es cierto facilitan la obtención de problemas que están ocurriendo, no brindan una rápida y correcta solución a la persona encargada de la red y su administración.

Las fallas en una topología de red y las dificultades que se presentan al momento de brindar soluciones, requieren de un análisis de las capas del modelo OSI, desde la capa física hasta la capa de aplicación siendo esta la más compleja para resolver los problemas. Si la falla proviene de una aplicación es una tarea difícil de reconocer y resolver por el administrador de red debido a que éstas son utilizadas de diferentes maneras por un computador y el conocimiento de la forma de trabajar del programa puede ser el causante del bloqueo o pérdida de acceso a la red. Por ejemplo Gemikonakli, Gemikonakli, & Bavan (2009) consideran que:

> La capa inferior de problemas se entiende bien, mientras que los problemas en la capa de aplicación son complejos, depende de la aplicación, y distintas una de otra. La razón de esto puede ser las dificultades encontradas en la modelización del razonamiento, relativa a una colección de conocimiento, o de la naturaleza del problema a ser resuelto (p. 1).

El sistema de detección y diagnóstico de fallas en redes LAN, es una ayuda para el monitoreo y a su vez al existir una falla en algún dispositivo de la red, mostrará alternativas de soluciones sobre la falla que haya sucedido de esa manera es una ayuda para la toma de decisiones de los administradores de red, para que pueda corregir la fallas y dejar en funcionamiento la red.

Es importante destacar la estructura y funcionamiento de software de monitoreo de código abierto como Snort un IPS, sniffer de paquetes y detector de intrusos mostrando un nivel de flexibilidad al momento de almacenar ssus informes tanto en archivos de texto como en bases de datos; de la misma forma el HIDS detecta anomalías en las actividades de los equipos que en un momento determinado pueden representar un riesgo para la red.

Entre las características significativas que permiten configurar incidentes especialmente sobre el ruido se presenta a la plataforma OSSEC para una variedad de sistemas operativos Linux, Windows. Mac y dispositivos portátiles. Otra colección de herramientas de código abierto es OSSIM (Open Source Security Information Management) que ayudan a los administradores de red en muchos aspectos de seguridad, sin embargo, presenta manejo de incidentes filtrando la información a través de sensores detectando anomalías en direcciones MAC, en servicios, en paquetes; construyendo una base de datos con información de la red facilitando la detección de anomalías en el comportamiento.

Este artículo presenta se propone un sistema para la detección de fallos en redes LAN, que permita, mediante reglas, detectar las fallas que suceden en una red

mostrando una respuesta como alternativa de solución para que el administrador ahorre tiempo en el momento de resolver los problemas que se presenten en la red.

6.1. Fallas en Redes LAN.

El estudio se enfoca a una red LAN, como primer punto se debe recordar a que se denomina las redes LAN. Una red LAN (Local Área Network) o también llamada red de área local, "está compuesta por un conjunto de computadoras que se conectan entre sí en un área geográficamente limitada (5 km de distancia), como edificio, una fábrica o un campo universitario" (Herrera Perez, 2003, pág. 121).

Los fallos que pueden darse dentro de una red, Mohamed (2009) define que "Cualquier estado excepcional que puede tener lugar en una capa determinada de red se denomina evento de red. Los fallos de red (una clase especial de eventos de red) se manifiestan a sí mismos en forma de alarmas (o síntomas)" (pág. 3). Oates (1995) considera que "Una falla es simplemente un mal funcionamiento de algún componente de la red, ya sea hardware o software" (pág. 3). Por mencionar ejemplos comunes, cada vez que no hay internet, correo electrónico, lentitud en la trasferencia de archivos o cuando las aplicaciones se cierran inesperadamente pueden considerarse como un fallo.

Tipos de fallas en la red.

Benítez, Solano, Cárdenas, y Garcia (2008) Consideran que "La clasificación de fallos en los sistemas de tiempo variable es todavía un problema abierto" (pág. 1). No obstante, una forma de clasificar los fallos puede ser por el tiempo de duración, lo que nos da tres tipos de fallos:

- Fallas permanentes
- Fallas intermitentes
- Los fallos transitorios.

Las fallas permanentes son fáciles de entender y existen en la red hasta que sean reparadas. Ejemplos de tales fallas incluyen: un cable roto, tarjeta de interfaz de mal funcionamiento. Ocurren fallas intermitentes de manera discontinua y periódica y tienden a causar el fracaso de los procesos actuales, y por lo tanto da lugar a la máxima degradación en el nivel de servicio durante un corto período de tiempo.

Los fallos transitorios momentáneamente causan degradación menor en el servicio, y ya que a menudo enmascarados por la gestión de los servicios públicos no son observables al usuario (Mohamed, 2009, p. 4).

“Algunas fallas pueden ser directamente observables, es decir, hay los problemas y síntomas en el mismo tiempo. Sin embargo, muchos tipos de fallos no son observables debido a su naturaleza intrínsecamente inobservable” (Steinder & Sethi, 2004, p. 166).

Sistemas de Gestión de Red.

En cuanto a una conceptualización de la gestión de redes se puede expresar que es “El conjunto de actividades destinadas a garantizar el control, la supervisión y la administración de los diferentes elementos que constituyen una red para que la comunicación tenga lugar” (Hinojosa, Madruñero, & Ortega, 2001, p. 14).

6.2. Modelo de Gestión OSI.

El modelo OSI ha establecido la gestión de red en diferentes áreas funcionales: La gestión de la configuración, gestión de fallos, gestión del rendimiento, gestión de la seguridad y gestión de la contabilidad. “Uno de los objetivos de categorizar las tareas de gestión de red es facilitar la popularización en el diseño e implementación de herramientas de gestión de red” (Oates, 1995, p. 1).

Elementos en un sistema de gestión de red

Dentro de un sistema de gestión de red, existen básicamente 4 elementos principales, el gestor, el agente, el objeto gestionado y los protocolos.

- Gestor: “Estaciones gestoras (NMS, Network Management Station), nodo en el que se ejecuta la aplicación gestora de red (NMA, Network Management Application). Interactúan con los operadores humanos, son los clientes que piden información a los agentes” (Martín & Léon , 2002, p. 4).
- Agente: Se considera agente al “software de administración de red que se encuentra en un nodo administrado. Este posee una base de datos local de información de administración, denominada MIB” (Molero, 2010, p. 9). El agente tiene como función responder las órdenes enviadas por el gestor.
- MIB: “Es un conjunto de definiciones de uno o varios recursos formados por clase de objetos gestionados, acciones, notificaciones, atributos, sintaxis, etc.” (Barba, 1999, pág. 76). Stallings (2004) menciona que “La MIB funciona como un conjunto de puntos de acceso en el agente para la estación del gestión (por ejemplo, todos los puentes tienen los mismos objetos de gestión)” (p. 264).
- Objeto gestionado: Puede ser cualquier nodo en la red, como por ejemplo un pc, impresora, host, router, tarjeta de red, etc.
- Protocolos: Son los encargados de establecer la comunicación entre los objetos y agentes, estos protocolos varían dependiendo del modelo utilizado, como definición se puede citar lo siguiente “especificación formar que define los procedimientos que han de seguirse cuando se transmiten o reciben datos, los protocolos definen el formato, tiempo, secuencia y verificación de errores usados en la red” (Dyson, 1997, p. 190).

    - Protocolo TCP (Transmission Control Protocol o protocolo de control de transmisión), Aznar en su texto indica lo siguiente:

TCP es protocolo orientado a conexión, que ofrece un servicio de flujo (stream) de bytes. Permite establecer una conexión fiable, para lo cual precisa una etapa

previa de conexión y una posterior de desconexión a la transmisión de datos. La unidad de información que se transmite se denomina segmento.

Cuando TCP emite un segmento, mantiene un temporizador esperando su asentimiento por el otro extremo. Si expira el temporizador se reenvía el segmento. Si TCP recibe datos del otro extremo de la conexión, emite un asentimiento. Los segmentos TCP son enviados como datagramas IP, por tanto, pueden llegar desordenados. Este problema lo soluciona TCP reordenándolos en el destino. Podría ocurrir asimismo que un segmento TCP llegara duplicado al destino, en este caso TCP eliminaría las redundancias presentadas. Además, TCP proporciona un control de flujo (tamaño de la ventana), adecuando un emisor rápido con un receptor lento. (Aznár López, 2004, p. 34)

- IP (Internet Protocol o protocolo Internet) Es el trabajo de la capa IP interactuar con estas capas más bajas, al tiempo que presenta un esquema de direccionamiento de red uniforme a las capas por encima de ella. La capa IP prepara los datos enviados a él por los protocolos más altos para transmisión a través de una red lógica específica, teniendo en cuenta cosas tales como la longitud del paquete, la estructura de direccionamiento de hardware y cómo los datos deben dividirse en varios paquetes. (Gilmer 2012, p. 1).

- Protocolo SNMP: El protocolo simple de administración de redes, “SNMP opera en la parte superior del protocolo de Datagrama de Usuario (UDP), un protocolo sin conexión que no garantiza datagrama de entrega” (Oates, identificación de fallos en redes de computadoras: Una revisión y un nuevo enfoque, 1995, p. 6). “Protocolo simple de administración de redes (SNMP) es muy útil para un administrador de red, lo que les permite gestionar y controlar varios aspectos de forma remota el dispositivo de red” (Faircloth, Kit de herramientas de codigo libre para pruebas de penetracion, 2011, p. 261).

Arquitectura del protocolo SNMP para gestión de red

Este protocolo al ser destinado para la administración y gestión de los dispositivos de redes, es realmente necesario usarlo en el desarrollo del sistema, ya que la mayoría de dispositivos de red como router, switch, host, etc. vienen con la configuración de fábrica SNMP para que puedan ser gestionados por un NMS, además porque es más sencillo de implementar y trabaja con un agente por medio del cual se comunicará el estado de los diferentes dispositivos conectados a la red.

Las especificaciones que se usa para SNMP son:

- **RFC 1155:** Sintaxis y semántica para definir los objetos gestionados en la MIB.
- **RFC 1213:** Contiene las definiciones de los objetos contenidos en la MIB basadas en TCP/IP.
- **RFC 1157:** Define el protocolo para acceder a los objetos y gestionarlos.

6.3 Modelo de gestión de red OSI.

El modelo de Gestión de Red OSI (Open Systems Interconnection (Interconexión de Sistemas Abiertos). “El Modelo OSI es más potente y general que el modelo de Internet, para lo cual sacrifica simplicidad” (Oates, 1995, p. 5).

“En el modelo OSI, los gestores y agentes utilizan un transporte fiable para comunicarse a través de asociaciones entre los procesos de la capa de aplicación” (Oates, 1995, p. 7).

Modelo TMN

El modelo TMN Telecommunications Management Network “El término Red de Gestión de Telecomunicaciones (TMN, Telecommunications Management Network) fue introducido por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T,

ITU Telecommunication Standarization Sector), y está definido en la recomendación M.3010" (Hinojosa et al., 2001, pág. 27). Este es más utilizado en el área de comunicaciones, sobre todo para los grandes operadores de redes.

Gestión de fallos.

La forma en el que el administrador de red se da cuenta de una falla es mediante un sistema de alamas o notificaciones. Por lo general la mayoría de sistemas de gestión utilizan este método. Esta gestión "debe ser capaz de detectar problemas y evaluar su gravedad, además ha de permitir establecer niveles de alarma personalizados, indicando la causa más probable del fallo" (Caballero, 1998, p. 179). En todo caso se puede distinguir algunos pasos básicos para la gestión de fallos de red, los cuales vendrían siendo:

- La identificación de fallos: Este primer paso es el que avisa de la presencia de un comportamiento anormal dentro de la red, existen herramientas como ping, este "envía un paquete desde una dirección origen hasta una dirección destino, permitiendo saber si hay conexión entre ambas, cual es el tiempo que tarda el paquete ida y vuelta y si hay pérdidas de paquetes" (Universidad Gerardo Barrios, 2010, p. 208). Otras herramientas como ipconfig, tracert también ayudan en este paso.
- El diagnóstico de fallos: En esta etapa se analizan las características como el tipo, tamaño y causa del fallo para luego determinar la acción correctiva necesaria.
- La reparación de fallos: Se ejecuta las posibles acciones a tomar, ya sea aislando el fallo, o reparando el área afectada. Oates (1995, p. 2) determina estos pasos en tareas de la siguiente manera:

  La sub tarea identificación de fallo que implica la detección de una problemática desviación del comportamiento normal que se ha producido y la identificación de su naturaleza. Diagnóstico de fallo consiste en determinar la causa raíz de un problema identificado y la corrección de fallo es la formulación de un curso de acción que se compromete a reparar el problema. Estas sub tareas son realizadas según el tipo de sistema de gestión de fallos que se aplique.

6.4 Sistemas activos y pasivos para gestionar fallos en redes.

Los sistemas de gestión de red utilizan diferentes técnicas o métodos para administrar los fallos, estos sistemas se pueden dividir en dos grupos:

- **Sistemas activos:** Se denominan así a los sistemas basados en sondas, estos muestran datos de la red gestionada de forma activa usando herramientas de software dedicado denominadas sondas. “El monitoreo activo implica el envío de tráfico a una red para probar su comportamiento. Este tráfico se envía en forma de sonda, que puede variar de sondas simples, tales como los pings a transacciones de prueba complejos” (Natu & Sethi, 2006, p. 1).

- **Sistemas pasivos:** Los sistemas de gestión de fallos pasivos son sistemas basados en la correlación de alarma o alertas. “Una alerta consiste de una notificación sobre la ocurrencia de un evento especifico, que puede o no representar un error. Un reporte de alerta es un tipo de reporte de evento, usado en el transporte de informaciones de alerta” (Valderrama, 2001, p. 168). Por lo general estos sistemas son utilizados por redes de gran tamaño, por su alto costo de implementación, también interviene la decisión de cada administrador, sin embargo, para las redes LAN sigue existiendo un vacío en este aspecto.

6.5 Funcionamiento del sistema.

El sistema de gestión y detección de problemas en una red LAN está conformado por cinco módulos:

1. Configuración.
2. Monitoreo
3. Fallos detectados
4. Historial de fallas
5. Nuevo conocimiento

El **Módulo Configuración**, nos permite la configuración de la red LAN, dentro del módulo existe la opción de detectar equipos la que permite buscar los equipos que conforman la red. Es opción nos mostrara cuadro dialogo donde el administrador de red debe estableceremos el rango de direcciones IP a detectar automáticamente. El sistema detectará todos los equipos automáticamente y aparecerá un mensaje del sistema indicando el proceso de carga de los equipos que están conectados en la red, para ser monitoreados, cuando este cargado al 100% se acepta las IP encontradas. Una vez detectados los equipos, se presentará en pantalla, la dirección IP, el nombre del equipo, tipo, la dirección MAC, y su estado, es decir, si el host se encuentra apagado o encendido. Además, este módulo permita agregar un host manualmente.

El **Módulo Monitoreo**, nos permite ver los dispositivos activos en la red. Este módulo se divide en dos subprogramas. El primer subprograma nos muestra la información de los dispositivos de la red tales como los host conectados a la red: la dirección IP, nombre de la máquina y estado (si el host está activo se mostrara un icono color verde en caso contrario de color gris). Además, se puede visualizar la información de utilización del CPU, el número de proceso que está ejecutando, y el uso de la memoria RAM de los dispositivos conectados. El segundo subprograma nos muestra la información de los problemas surgidos hasta el momento, para iniciar el monitoreo se ejecuta el subprograma dará inicio a las consultas del estado de cada host y al encontrase un problema notificará la siguiente información: La dirección IP del host donde sucede el problema, el nombre del problema, la fecha y hora en que se encontró el problema y estado del problema encontrado. Cuando el problema este resuelto se guarda en el historial de fallos.

El **Módulo Fallos detectados**, nos permite obtener información detallada de los fallos de los dispositivos de la red, ayudará a mostrar alternativas de soluciones de los problemas que ocurrieron en la red LAN.

El **Módulo historial de fallas,** nos permite visualizar el estado de los dispositivos de la red así como las fallas que tuvieron cada uno de ellos. Además, el historial de fallos puede ser buscado por un rango determinado de fechas. Existe la opción de obtener un reporte de los fallos en pdf y Excel.

El **Módulo nuevo conocimiento,** en la cual se introducirán problemas nuevos que han ocurrido, las misma que deben ser ingresadas por una sola vez por el experto en administración de redes. El administrador de red para la creación de reglas debe ingresar un nombre del problema y la descripción detallada del problema. Este módulo tiene la opción llamada regla alternativa la cual se relaciona con una lista de problema la cual se relacionará una posible solución. El módulo también tiene la opción de mantenimiento de reglas, que permite modificar los valores que están ya definidos en el archivo de clip.

6.6 Funcionamiento de detección de fallo.

El sistema estará monitoreando los dispositivos conectados en la red y recolecta información necesaria de la misma. En el caso que exista algún problema de red en alguna máquina, se comunica al sistema de gestión y revisará cual es el problema sucedido. Si el problema se encuentra, mostrará las alternativas de solución, en caso contrario el sistema da la opción de almacenar el nuevo fallo el cual debe ser ingresado por el experto en redes. Por ejemplo, obtener información detallada del fallo encontrando en una maquina **PROBLEMA DE AUMENTO DE TRÁFICO**, el sistema de detección de fallas mostrará el siguiente mensaje:

Figura 1. Alternativas de Solución.
Fuente: Autores

En el caso de que la detección del fallo no se encuentre como alternativa de solución del sistema, el administrador de red debe ingresarlo como nueva regla.

Figura 2. Creación de Nueva Regla.
Fuente: Elaboración propia.

El sistema tiene un detalle de fallas que han sucedido, donde se identifican el nombre del Problema, descripción de falla, la fecha y hora, en la figura nos presenta los problemas encontrados por el sistema corresponde a problemas comunes de las redes como: conexión al host, problemas de DNS y de saturación de ancho de banda.

Figura 3: Modulo de Historial Fallas.
Fuente: Elaboración propia.

El administrador de red puede obtener información de las fallas ocurridas en la red y revisar el estado de cada uno de los problemas de la misma manera se puede obtener un reporte del historial en Excel como se muestra en la tabla 1.

ID	NOMBRE	DESCRIPCION	FECHA	HORA
75	PROBLEMA DE DNS	El usuario tiene conexión, dirección IP. Sin embargo, no se conecta a aplicaciones o navegador de internet.	02/08/2016	1:19:14
76	PROBLEMA DE CONEXIÓN AL HOST	No se puede encontrar el host en la red, host ha sido desconectado.	24/08/2016	13:59:32
77	PROBLEMA DE DNS	El usuario tiene conexión, dirección IP. Sin embargo, no se conecta a aplicaciones o navegador de internet.	04/09/2016	22:04:12
78	PROBLEMA DE CONSUMO ANCHO BANDA	Alto consumo de ancho de banda en internet	14/09/2016	14:00:25

Tabla 1. Detalle de Historial de fallos Registrados Fallos de la Red.
Fuente: Elaboración propia.

6.7 Metodología

Para la prueba se realizó una simulación con el programa GNS3 donde se diseñó un área de trabajo con una topología de Red LAN (Figura. 4), conexión a internet, direccionamiento IP con rangos de 192.168.1.1 hasta 192.168.1.14: y en el host administrador se instaló el sistema de detección de fallas, el cual monitoreo continuamente los hosts de la red (computadoras e impresoras). Para la

simulación de fallas en nuestro escenario se tuvo que generar las mismas, las cuales fueron monitoreadas y reportadas en el sistema.

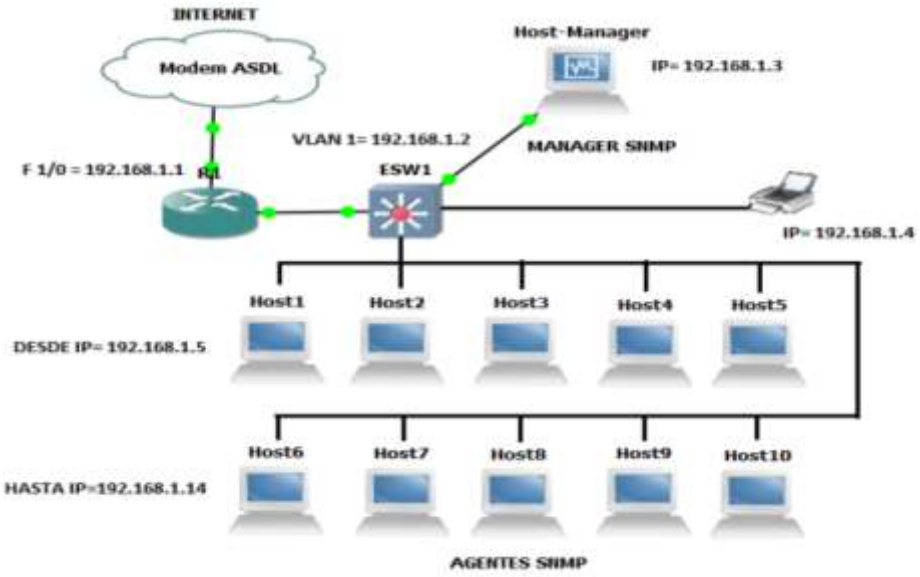

Figura 4. Red LAN.
Fuente: Elaboración propia.

El sistema tiene almacenados los errores comunes en las redes LAN con las alternativas de soluciones, en el caso no se encuentren como fallas comunes, las cuales las alternativas de fallas detectados lo deben ingresar por una sola vez el administrador de red. Las fallas comunes en las redes LAN son las siguientes:

- ✓ Problema de conexión al Host
- ✓ Problemas de comunicación entre Host
- ✓ Problema de duplicación de IP en la Red
- ✓ Problema de conexión a la impresora
- ✓ Problemas de DNS
- ✓ Problema de saturación ancho banda
- ✓ Problema conexión server aplicación
- ✓ Problema de conexión al servidor de correo
- ✓ Agente Socket desconectado

En la tabla 2 y figura 5 se muestran las fallas comunes, las mismas fueron monitoreadas y reportadas en el sistema en un reporte en Excel.

Tabla 2: Simulación de Fallas.

FALLAS COMUNES	PC1	PC2	PC3	PC4	PC5	PC6	PC7	PC8	PC9	PC10
CONEXION AL HOST	10	5	4	4	1	4	8	9	10	30
COMUNICACION ENTRE HOST	4	15	10	5	5	4	7	8	10	10
DUPLICACION DE IP	8	2	1	1	1	1	1	1	1	1
DNS	2	0	0	0	0	1	1	0	0	0
CONEXION A LA IMPRESORA	0	0	1	0	0	0	2	1	0	0
SATURACION ANCHO BANDA	0	0	0	0	0	1	0	0	0	1
CONEXION AL SERVIDOR DE CORREO	0	1	0	0	0	3	0	0	0	2
AGENTES SOCKET DESCONECTADO	20	40	8	7	0	4	7	14	5	7

Fuente: Elaboración propia.

Figura 5. Simulación de Fallas.

Fuente: Elaboración propia.

En el mismo escenario se realizado el monitoreo de la red con una generación de tráfico de paquetes, los cuales se muestra en la figura 6.

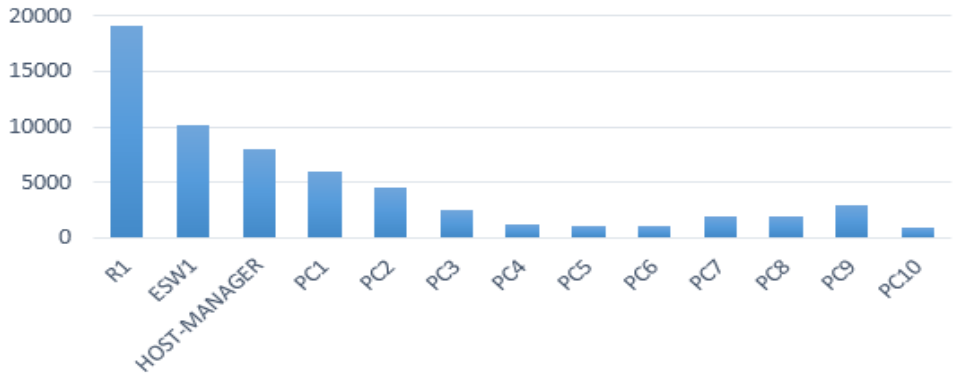

Figura 6. Monitoreo de la red.
Fuente: Elaboración propia.

CONCLUSIONES

El presente trabajo describe el programa de sistema de detección de fallas cuyo objetivo es mejorar la gestión en la solución de las fallas detectadas en una red LAN. El programa permite ayudar a los especialistas en redes para disponer de información de fallas en tiempo real y un medio de alerta al administrador de red. Se realizaron pruebas de simulación de redes, donde se obtuvieron resultados de obtención de fallas y monitoreo de la red.

Se considera que la implementación de un sistema de detección de problemas en redes tiene un tiene efecto positivo en la gestión de los administradores de red, esto lo pudimos comprobar gracias a las respuestas del programa que detalla de manera eficiente las detecciones y soluciones de los problemas en red.

A través de este trabajo investigativo se ha demostrado que el sistema de detección de problemas de red, ayudaría a optimizar el tiempo de inactividad de la misma, mejorando el sistema de trabajo en un centro de cómputo, por lo consiguiente ayudará en el crecimiento y desarrollo de la empresa.

EL software brindará al administrador de la red, una gran herramienta en relación al ahorro de tiempo y facilitará la gestión de fallos en una red, al contar con un sistema que los detecte y presente alternativas de solución al problema.

Para trabajos futuros se debería realizar pruebas con redes inalámbricas y las bases de reglas de fallos deberían adquirir su propio conocimiento, involucrando la idea interesante que se realice un sistema experto de gestión de redes.

REFERENCIAS

Aznár López, Andrés. La red Internet. El modelo TCP/IP. Madrid: España, 2004.
Barba Martí, Antoni. Gestion de Red. Barcelona: UPC, 1999.

Benítez Pérez, Solano González, Cárdenas Flores, y Garciıa Nocetti. FAULT CLASSIFICATION FOR A CLASS OF TIME-VARYING SYSTEMS BY USING OVERLAPPED ART2A NETWORKS. Mexico, 2008.

Caballero, José Manuel . Redes de banda ancha. Barcelona: Marcombo S.A., 1998.

Dyson, Peter. Diccionario de Redes . Colombia: McGRAW-HILL, 1997.

Faircloth, Jeremy. Kit de herramientas de codigo libre para pruebas de penetracion. 2011.

Gemikonakli, E., O. Gemikonakli, y S. Bavan. Red de Monitoreo Inteligente usando un modelo de inferencia conexionista. Liverpool, Reino Unido, 2009.

Gilmer, Brad. Network protocols. 2012.

Herrera Perez, Enrique. Tecnologías y redes de transmisión de datos. Limusa, 2003.

Hinojosa, Víctor Hugo, Luis Alberto Madruñero, y Luis Vicente Ortega. Sistemas de Gestión de Red. Ibarra, 2001.

Martín, Antonio, y Carlos Léon . Gestion de Redes. Sevilla, 2002.

Mohamed, Abduljalil. Deteccion e Identificacion de fallos en redes de computadoras. Waterloo, Ontario, 2009.

Molero, Luis. Planificación y Gestión de Red. Maracaibo, 2010.

Natu, Maitreya, y Adarshpal S. Sethi. «Active Probing Approach for Fault Localization in Computer Networks.» http://ieeexplore.ieee.org/. abril de 2006. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1651276&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1651276 (último acceso: 04 de abril de 2015).

Oates, Tim. identificación de fallos en redes de computadoras: Una revisión y un nuevo enfoque. Massachusetts, 1995.

Steinder, Małgorzata, y Adarshpal S. Sethi. Un estudio de las técnicas de localización de fallos en redes de ordenadores. 2004.

Valderrama, Jose. «Informacion Tecnologica.» Centro de Informacion Tecnologica , 2001.

Universidad Gerardo Barrios. «Universidad Gerardo Barrios El Salvador.» marzo de 2010. http://biblio2.ugb.edu.sv/bvirtual/10063/capitulo6.pdf (último acceso: 4 de abril de 2015).