Diseño de sistema de monitoreo simple para redes de gran escala

Design of a simple monitoring system for large-scale networks

ARTICLE HISTORY

Received 14 May 2020
Accepted 06 June 2020

Vanessa Napa
Facultad de Ingeniería Eléctrica y Electrónica
Escuela Politécnica Nacional
Quito, Ecuador
vanessa.napa@epn.edu.ec

Luis Urquiza-Aguiar
Departamento de Electrónica,Telecomunicaciones y Redes de Información
Escuela Politécnica Nacional
Quito, Ecuador
luis.urquiza@epn.edu.ec

Xavier Calderón-Hinojosa
Departamento de Electrónica,Telecomunicaciones y Redes de Información
Escuela Politécnica Nacional
Quito, Ecuador
xavier.calderon@epn.edu.ec

Diseño de sistema de monitoreo simple para redes de gran escala

Design of a simple monitoring system for large-scale networks

Vanessa Napa
Facultad de Ingeniería Eléctrica y Electrónica
Escuela Politécnica Nacional
Quito, Ecuador
vanessa.napa@epn.edu.ec

Luis Urquiza-Aguiar
Departamento de Electrónica,Telecomunicaciones y Redes de Información
Escuela Politécnica Nacional
Quito, Ecuador
luis.urquiza@epn.edu.ec

Xavier Calderón-Hinojosa
Departamento de Electrónica,Telecomunicaciones y Redes de Información
Escuela Politécnica Nacional
Quito, Ecuador
xavier.calderon@epn.edu.ec

Resumen — Actualmente, existen muchas herramientas de administración de redes que tratan de monitorizar dispositivos de diferentes casas fabricantes. Sin embargo, ninguna de ellas permite automatizar las tareas de monitoreo que se realizan en la red. Para solventar este problema, se propone un sistema a medida que verifica automáticamente los archivos de configuración de los equipos de red para que los técnicos puedan dedicar su tiempo a solucionar los fallos encontrados, lo que dará como resultado un uso más eficiente de sus días de trabajo. El sistema de monitoreo propuesto se desarrolla para la red WAN de la Corporación Nacional de Telecomunicaciones (CNT EP) de Ecuador, en el cual se utiliza dos formas para el análisis automático de los registros de configuración: 1) mediante el uso interactivo de comandos que se pueden usar en cualquiera de los dispositivos, independientemente de su marca. 2) mediante el uso de los objetos MIB de Cisco, que son la mayoría de los dispositivos de la red. El sistema se desarrolló utilizando software gratuito y nuestro sistema lleva a cabo la supervisión automática de la red en 14 horas, lo que representa una reducción en el tiempo de aproximadamente el 94%.

Palabras clave — Gestión de red, Monitoreo de red, SNMP, Bash, Expect, WordPress

Abstract *— Currently, there are network management tools that try to monitor devices from different manufacturers. However, none of them allow you to automate the monitoring tasks carried out on the network. To tackle this problem, we propose a tailored system that automatically checks the networking devices' configuration files. In this way, the technicians can spend their time resolving the faults found, resulting in a more efficient use of their workdays. The proposed monitoring system was developed for the WAN of Corporación Nacional de Telecomunicaciones (CNT EP) of Ecuador, in which two forms are used for the automatic analysis of configuration records: 1) by interactive use of commands that can be used in any of the devices, independently of his brand. 2) by using the MIB objects of Cisco, which are most of the network devices. The system was developed using free software and the whole, automatic network monitoring is carried out by our system in 14 hours, which represents a reduction in time of approximately 94%.*

Keywords — Network Management, Network Monitoring, SNMP, Bash, Expect, WordPress

ISSN: 1390 -9266 – 2020 LAJC

1 INTRODUCCIÓN

El monitoreo de una red implica advertir de forma preventiva y oportuna la presencia de cualquier tipo de dificultades que puedan interferir en el correcto desempeño de los servicios que dicha red ofrece. En el mercado mundial existen muchas herramientas de administración de redes que tratan de monitorizar dispositivos de diferentes casas fabricantes. Herramientas comerciales como: Mg-Soft, WhatsUp Gold, Tivoli, Open View, etc. Así mismo, existen herramientas de libre distribución como: Nagios, NET-SNMP, Brother, etc. Todas las herramientas trabajan con el protocolo SNMP y permiten obtener datos de los dispositivos de una red. Pero, específicamente ninguna de ellas proporcionan una herramienta que permita automatizar las tareas que se realizan en una empresa.

Actualmente el área de O&M IP_MPLS de CNT EP cuenta con los sistemas de administración CISCO ANA (Active Network Abstraction), U2000 y SAM (Service Aware Manager), los cuales son propietarios de las marcas CISCO, HUAWEI Y ALCATEL, respectivamente. Estas herramientas entre sus múltiples ventajas permiten la gestión de dispositivos de red. Mediante el revisión de forma automatizada de eventos producidos en los equipos, los tres mencionados sistemas detectan fallas en los equipos y muestran alertas en el caso de ser meritorio, siempre basados en parámetros propios de cada fabricante. La red IP_MPLS de CNT EP está conformada por un conjunto extenso de equipos de las marcas anteriormente mencionadas. Los tres softwares de administración son adquiridos a un costo significativo (miles de dólares) y solamente pueden monitorear hasta un determinado número de elementos de red.

Los objetivos que satisface el sistema de monitoreo propuesto en este artículo envuelven características de redundancia en los métodos de obtención de los registros de configuración, escalabilidad al poder funcionar adecuadamente en un número mayor de equipos, eficiencia al realizar el análisis respectivo en un tiempo considerablemente menor en comparación al tiempo empleado en realizar el mismo proceso de forma manual, versatilidad para integrar en una mismo sistema el análisis de varios fabricantes de equipos de conectividad y finalmente presentar los resultados, mediante una visualización completa y ordenada de los resultados obtenidos en el análisis.

El resto de artículo está organizado de la siguiente forma: en la sección 2, se describen los conceptos básicos necesarios acerca de cómo funciona una red MPLS, tomando como base la estructura de la red IP-MPLS de la CNT. Además, se incluye información acerca del protocolo SNMP y la forma en como éste es utilizado para la extracción segura de información de los elementos de red. Luego, la sección 3, presenta la situación actual del proceso conocido como Rutinas de Mantenimiento llevado a cabo por el área de Operación & Mantenimiento de las plataformas IP-MPLS. En la sección 4 se detallan los requerimientos que debe cumplir el sistema para posteriormente definir el diseño del mismo. En la sección 5, se presenta una breve descripción de la parte más relevante de la implementación del sistema de monitoreo. Se describe la estructura general de la programación de los scripts que realizarán el análisis de los parámetros de configuración de los equipos que conforman la red IP-MPLS. Después de ello, la sección 6, da una visión general de las pruebas de funcionamiento realizadas y se describe los pasos a seguir en caso de que se presenten dificultades en el servidor en el cual el sistema de monitoreo fue desplegado. Finalmente, las conclusiones y recomendaciones son presentadas en la sección 7.

2 ANTECEDENTES

A continuación, se describen los conceptos acerca de la gestión de redes utilizados en el desarrollo del sistema, Así también se describe las configuraciones más significativas de la red IP-MPLS, de la CNT EP.

2.1 Gestión de redes

Gestionar una red implica advertir y diagnosticar problemas para posteriormente dar soporte en el menor tiempo posible. Una adecuada gestión de red, conlleva a que los tiempos de inactividad, causados por un funcionamiento erróneo o a su vez por un rendimiento inadecuado de los equipos sean reducidos, ya que si alguno de estos eventos es pasado por alto podría afectar la forma en la que el cliente percibe el servicio contratado y en consecuencia significar pérdidas económicas [1].

Uno de los protocolos ampliamente difundidos dentro del campo de telecomunicaciones y redes es SNMP (Simple Network Management Protocol). SNMP es un protocolo de capa de aplicación que tiene un conjunto de características especialmente diseñadas para la gestión de redes levantadas sobre la arquitectura de red TCP/IP. Sus bases radican en un modelo de cliente-servidor y se lo utiliza con frecuencia para facilitar el intercambio de información entre dispositivos de red. SNMP maneja los conceptos de agente y gestor. Un agente es un programa dentro del equipo que se encarga de la administración de un conjunto de datos denominado MIB (Management Information Base). Otro programa llamado gestor es similar a una aplicación del tipo cliente, éste genera peticiones hacia la MIB y procesa las respuestas asociadas [2]. La MIB, contiene información almacenada de forma jerárquica en una estructura de árbol. Está conformada por una secuencia de números que representan objetos. Un objeto es una entidad que hace una abstracción de los recursos del dispositivo a ser gestionado y tiene un identificador único (OID, Object Identifier).

2.2 Modelo jerárquico de tres capas

Diseñar una red de forma jerárquica ayuda a los administradores a tener un mejor monitoreo y control de la misma, lo cual se consigue al dividir la red en capas con funciones específicas. Al ser una estructura modular, recuperar la red después de una falla se vuelve una acción fácil de efectuar. El modelo jerárquico tradicional usado para redes extensas consta de tres capas: Core, Distribución y Acceso [3]

Acceso.- Es la interfaz de comunicación entre la red y los dispositivos finales de usuario.

Distribución.- Punto de asociación de múltiples switches de la capa de acceso, agrega los datos provenientes de la misma para su enrutamiento hacia el destino final.

Core.- Es el núcleo de la red. Su función principal es conmutar grandes cantidades de tráfico a la mayor velocidad posible de manera confiable. Es el medio de comunicación entre los elementos de la capa de distribución. La Fig. 1, es un esquema de diseño jerárquico de redes

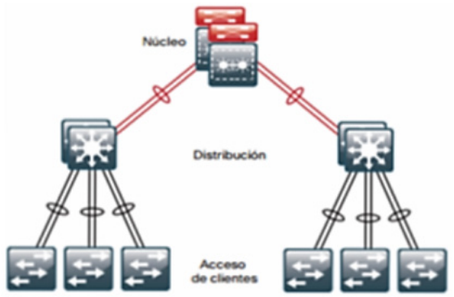

Fig. 1 Esquema del modelo jerárquico de tres capas

2.3 Redes MPLS

La tecnología MPLS fue diseñada como una solución que otorga un trato adecuado a aplicaciones tolerantes al retardo y aplicaciones en tiempo real [4]. MPLS discrimina entre diferentes clases de servicio (CoS - Class of Service) y las administra mediante el uso de ingeniería de tráfico. Adicionalmente, estas redes reciben y dan trato a tráfico multiprotocolo. MPLS, es un mecanismo de conmutación que usa etiquetas para el reenvío de paquetes aprovechando lo mejor de la capa 2 y un rápido enrutamiento mediante características de capa 3; siendo considerado un protocolo de capa 2,5.

En la arquitectura de una red MPLS se distinguen dos dispositivos principales: LER (Label Edge Router) y LSR (Label Switched Router). Los LER también conocidos como PE (Provider Edge) o E-LSR (Edge Label Switching Router), están situados en el borde de la red y son los encargados de asignar/retirar las etiquetas a los paquetes al entrar/salir de la red, son los únicos que realizan funciones de enrutamiento. Los LSR se encuentran intermedios entre los enrutadores de borde, tienen como función el transporte de los paquetes hacia el PE destino.

2.4 Red IP-MPLS de la Corporación Nacional de Telecomunicaciones CNT EP.

La CNT, tiene una amplia red de equipos de telecomunicaciones, la cual está conformada por redes de menor tamaño, subdivididas y administradas en referencia a la función que desempeña dentro del contexto global, una de estas redes basada en tecnología MPLS.

El área de operación y mantenimiento de la de la red IP-MPLS de CNT EP, es la encargada de mantener la disponibilidad de los servicios en dicha red. La red IP-MPLS está estructurada en base al modelo jerárquico de tres capas. La Tabla I, muestra las marcas y número de equipos pertenecientes a cada capa.

TABLE I. NÚMERO APROXIMADO DE EQUIPOS DE LA RED IP-MPLS POR FABRICANTE

CAPA	FABRICANTE	NÚMERO DE EQUIPOS
ACCESO	CISCO	980
	HUAWEI	330
	ALCATEL	160
AGREGACIÓN	CISCO	500
CORE	CISCO	30

La disponibilidad de una red depende en gran parte de la fiabilidad en el funcionamiento de los equipos, es por esta razón que, el departamento O&M IP-MPLS efectúa un proceso denominado Rutinas de Mantenimiento. Este proceso se encarga de verificar el estado operativo de cada uno de los equipos que conforman la red IP-MPLS.

3 RUTINAS DE MANTENIMIENTO OPERACIÓN & MANTENIMIENTO DE LA PLATAFORMA IP-MPLS

Rutina de mantenimiento, es un proceso cuyo objetivo es la revisión periódica de los registros operacionales de los equipos que conforman la red IP-MPLS, con la finalidad de reducir los problemas que pueden presentarse en los mismos. Este proceso actualmente es realizado de forma manual por el personal del área en más de 2000 elementos de conectividad. Se debe considerar que las configuraciones o parámetros analizados dependen de la función que el equipo efectúe dentro de la red. Esta tarea se realiza en un tiempo promedio de siete minutos por equipo y representa un coste global estimado de 234 horas. En contexto, esto significaría que se emplee seis técnicos a tiempo completo (8 horas) de forma continua durante una semana para efectuar el proceso de verificación del funcionamiento de todos los equipos.

Las rutinas de mantenimiento implica la realización de las siguientes actividades en cada uno de los dispositivos:

• Autenticarse en el equipo.

• Digitar el comando que muestre la información a verificar.

• Revisar detalladamente cada uno de los parámetros relevantes de la información mostrada.

• Discriminar entre un funcionamiento adecuado, una alerta o una falla en la configuración.

• Dar soporte en el caso de ser necesario.
En cada capa de la red son analizados parámetros relevantes en cuanto a la función que dicha capa cumple, sin embargo los siguientes parámetros son comunes para las tres capas.

• Porcentaje de procesamiento de CPU.- El objetivo es, verificar que los niveles de procesamiento no superen los límites establecidos, ya que podrían suscitarse falencias en el rendimiento del dispositivo.

ISSN: 1390 -9266 – 2020 LAJC

• Parámetros de entorno.- Los parámetros de entorno permiten obtener información acerca del estado del hardware del equipo en referencia a condiciones de temperatura, estado operativo de fuentes de poder y ventiladores.

• UTC: Fecha local actual.- Todos los equipos de la red IP-MPLS están conectados a un servidor, el cual posibilita una comunicación remota con dichos elementos. Este servidor está configurado con el estándar de tiempo universal UTC (Universal Time Coordinated), el mismo que se sincroniza con el tiempo medio de Greenwich a partir de las mediciones de la rotación de la Tierra [5] . Es necesario tener concordancia servidor-equipo en cuanto a la fecha configurada, lo cual posibilitará en caso de ser necesario realizar procesos masivos en un día en particular.

A continuación, son descritos los parámetros específicos analizados en cada una de las capas de la red IP-MPLS

3.1 Capa de Acceso

La capa de acceso de la red IP-MPLS de la CNT EP, está conformada por equipos de las marcas Alcatel, Cisco y Huawei. Dentro de esta capa son considerados para el análisis los siguientes parámetros.

• Protocolo Múltiple de Árboles de Expansión.- Su siglas MST (Multiple Spanning Tree), la función de este protocolo es que, en cada instante exista un único camino entre dos equipos. Dentro de este protocolo se analizan dos características. La primera de ellas es la configuración de instancias y de región asociada, como segunda característica es analizado el rol que cumple el equipo dentro de la estructura de MST, al ser equipos que trabajan en capa de acceso, su rol bajo ninguna circunstancia puede actuar como Raiz (Root).

• Virtual Trunking Protocol.- Este protocolo permite administrar de forma eficaz las VLANs dentro de un dominio de equipos, transmitiendo los cambios hechos en un dispositivo hacia los demás dentro de su dominio. Los equipos de acceso deben estar configurados en modo Transparente, en este modo los cambios hechos en un equipo de acceso no son replicados a los demás dispositivos dentro del dominio VTP.

3.2 Capa de Distribución

La capa distribución está conformada por equipos Cisco, los mismos han sido agrupados de acuerdo a la nomenclatura que usa esta casa fabricante: Cisco Series 7600, Cisco ME Series 3600X/3800X, Cisco Series 900 y Cisco IOS XR (ASR Series 9000).

Debido a que en base a cada clasificación los parámetros a analizarse difieren, se ha optado por definir parámetros generales, parámetros comunes y parámetros específicos.

1) Parámetros generales

Dentro de los parámetros generales se encuentran:

• Tráfico en los puertos: sesiones SPAN.- SPAN (Switched Port Analizer), es una tecnología propietaria de Cisco. Posibilita la duplicidad de paquetes y su captura en una localidad distinta al puerto destino, mediante el levantamiento de sesiones consideradas “parásitas” en el dispositivo. Por lo tanto, es necesario comprobar que ningún puerto esté siendo monitoreado por este tipo de sesiones.

• Descripción de las interfaces.- Es necesario tener información de cada uno de los interfaces que tiene el dispositivo. Dentro de esta información está el destino del enlace, el ancho de banda asignado al mismo y el servicio asociado a dicho puerto. Es común que se realicen migraciones o cancelaciones de servicios, por lo que se precisa tener un seguimiento del estado de los servicios asignados con el fin de conocer las interfaces que están libres y asignarles un nuevo uso.

• Interfaces configuradas con ISIS.- Intermediate System to Intermediate System, es un protocolo de estado de enlace de implementación sencilla. Funciona de manera estable, lo que lo hace robusto en redes de gran tamaño. Permite convergencia rápida y alta escalabilidad. Además, mediante IS-IS se puede implementar enrutamiento jerárquico y enrutamiento multiarea. Cuenta con características para la implementación de Ingeniería de Tráfico. Los parámetros comunes son analizados en referencia a la Tabla II.

ISSN: 1390 -9266 – 2020 LAJC

TABLE II. PARÁMETROS EN COMÚN ENTRE SERIES DE EQUIPOS CISCO EN LA CAPA DISTRIBUCIÓN

PARÁMETRO A SER ANALIZADO		SERIE
MST	Rol del equipo dentro del protocolo	7600 3600X/3800X IOS XR
	Estado operativo de los puertos	900
Políticas de servicio	Concordancia de ancho de banda política-interfaz	7600 3600X/3800X
	Paquetes descartados en las interfaces configuradas con políticas de servicio.	900 IOS XR
Estado operativo de objetos referentes a direccionamiento IP: Tracks		7600 3600X/3800X

• MST. - Dentro de este protocolo se analiza el rol que cumple el dispositivo dentro de cada una de las instancias. MST. Cabe mencionar que al ser equipos de capa distribución, el rol de los dispositivos debe ser de Raíz (root). Otra característica para análisis es el estado operativo de los puertos, cada uno de los puertos debe estar en estado Forwarding, el mismo que hace alusión a que todas las tramas entrantes por dicho puerto están siendo reenviadas de acuerdo a las direcciones MAC destino aprendidas.

• Políticas de calidad de servicio. - Una de las causas de la pérdida de paquetes se debe a que el flujo de datos es dirigido desde un enlace de gran ancho de banda hacia otro de ancho de banda menor. Esto a su vez, puede ser el resultado de que el ancho de banda configurado en la interfaz carece de concordancia con al ancho de banda requerido en la política de servicio. Así mismo, es necesario tener información acerca de la existencia de paquetes descartados, con la finalidad de tomar medidas y se posibilite que la mayor cantidad de datos enviados a través de la red lleguen a su destino.

• Estado operativo de objetos referentes a direccionamiento IP: Tracks.- Los Tracks, hacen alusión a un proceso levantado en el equipo. Estos procesos son conocidos como objetos, un objeto puede ser el estado de un protocolo en una interfaz, parámetros de enrutamiento ip o la accesibilidad que tenga el equipo para ser alcanzado por sus vecinos. Se debe verificar que el estado de cada Track sea “Up” y que el intervalo de tiempo transcurrido después de la última actualización de estado sea mayor a una hora.

2) Parámetros específicos analizados: Cisco Series 7600

• Fuentes de Poder. - Se recomienda que todos los equipos tengan dos fuentes de poder, una activa y una en stand-by; ambas de iguales valores de potencia y corriente.

• Estado de arranque y registro de configuración. - Al cargar el IOS en un equipo, la imagen de este se almacena automáticamente en el sup-bootdisk del dispositivo. Si el equipo no encuentra una imagen de IOS válida, entonces no podrá arrancar. El equipo dispone de un disco de respaldo llamado slave-supbootdisk, que actúa en el caso de que el disco principal presente dificultades en su operación. Es por esto que es necesario verificar que ambos discos contengan la imagen del IOS.

• Porcentaje de uso de recursos de hardware para reenvío de tramas y paquetes. - Es necesario conocer el porcentaje de uso de recursos de hardware empleados para el reenvió de tramas y paquetes. Esta información es almacenada en una base de información denominada EARL (Encoded Address Recognition Logic), mediante un proceso centralizado se permite el reenvío de tramas y paquetes, basado en las direcciones MAC aprendidas. El dispositivo se basa en dichos datos para tomar las decisiones de conmutación [6].

• Recursos usados para brindar QoS. - Dentro de una red extendida que permite el flujo de una gran variedad de servicios contratados por diversos clientes, es necesario saber la cantidad de recursos usados para la asignación de políticas que permiten brindar una adecuada calidad de servicio a cada requerimiento.

• Porcentaje de uso de los recursos de fábrica. - Al ser dispositivos cuya función principal es la de conmutar tráfico hacia diferentes destinos, se vuelve imprescindible conocer el porcentaje de uso de los recursos que están siendo utilizados para lograr dicho objetivo. De esta manera si se superara un umbral predeterminado administrativamente, se deberá tomar una acción, con el fin de garantizar la disponibilidad de los servicios.

3) Parámetros analizados en equipos Cisco ME Series 3600X y 3800X.

• Etiquetas utilizadas para VPN (Virtual Private Network) capa 3.- La configuración de VPN de capa 3, proporciona seguridad extra al encapsular paquetes mediante etiquetado. El número de etiquetas usadas debe estar por debajo de un valor referencial, con el fin de no colapsar la capacidad del dispositivo.

• Etiquetas utilizadas para tráfico unicast IP v4.- Es necesario conocer el número de etiquetas utilizadas para aplicaciones unicast en direccionamiento IP v4, esta información es almacenada en la tabla TCAM (Ternary Content Adressable Memory), esta tabla se encuentra subdividida en regiones llamada Nile.

4) Parámetros analizados en equipos Cisco ASR Series 900

• Etiquetas y rutas usadas en conmutación avanzada CEF. - Cisco Express Forwarding (CEF), es una técnica que permite una conmutación más rápida usando la tabla de enrutamiento FIB (Forwarding Information Base). Es importante conocer el número de etiquetas utilizadas dentro de esta tabla.

• Uso de memoria en la tabla TCAM. - Dentro de la tabla TCAM existe un número de etiquetas específico para tráfico unicast, multicast y etiquetas con las que se puede brindar calidad de servicio. Es necesario conocer estos valores con el fin de no sobrepasar los límites y conocer la disponibilidad de etiquetas que puedan ser asignadas a nuevos requerimientos.

5) Parámetros analizados en equipos Cisco ASR Series 9000 IOS XR.

• Estado de dispositivos programables de campo FPD.- Los dispositivos programables de campo FPD (Field Programmables Devices), son elementos que se implementan en las tarjetas de los enrutadores o conmutadores. Estos dispositivos le proporcionan al equipo de red, características adicionales como por ejemplo las que se encuentran dentro de un FPGA. La reprogramación hace referencia a una actualización de software que se basa en lograr una compatibilidad del FPD con el sistema operativo del enrutador o del conmutador. Los FPD se reprograman en caliente y de forma independiente.

• Tráfico en periodos de congestión. - Es importante analizar el comportamiento del dispositivo en cuanto al reenvío de paquetes en periodos de congestión. WRED Drop (Weidhted Random Early Detection), es el parámetro que indica el número de paquetes descartados debido a falta de capacidad en el buffer.

3.4 Capa Core

Los equipos que conforman esta capa cuentan con las mismas características de los dispositivos ASR 900 IOS XR, presentados en la capa de agregación, por consiguiente, la mayor parte de parámetros a ser analizadas fueron ya descritos.

Los parámetros en común entre los equipos agregación ASR Series 900 y los equipos de la capa de Core son:

• Descripción de las interfaces.
• Interfaces configuradas con ISIS.
• Paquetes descartados en las interfaces configuradas con políticas de servicio.
• Estado de dispositivos programables de campo FPD.
• Como parámetro adicional en estos equipos es necesario verificar el estado del protocolo BGP, en cuanto a la recepción de prefijos.
• Prefijos Recibidos en BGP (Border Gateway Protocol).- Para BGP es indispensable que la información que se intercambia entre sistemas autónomos (AS) sea confiable y que ayude a obtener detalles de la red dentro de la cual se está operando. Esto se hace posible a través del intercambio de prefijos entre los AS.

ISSN: 1390 -9266 – 2020 LAJC

4 DISEÑO DEL SISTEMA

En la actualidad la mayor parte de dispositivos en el mundo, que trabajan con IP (Internet Protocol) tienen como parte de su plataforma un repositorio MIB que permite la monitorización de estos, utilizando diferentes herramientas de administración denominadas NMS (Network Management System). Es por eso que existen objetos MIB's que tienen información relacionada a la plataforma del dispositivo y por ende información del protocolo MPLS, facilitando de esta forma el sondeo de las características que tienen los dispositivos de redes en relación a MPLS y con esta información los administradores de una red pueden solucionar los problemas que se presenten en la red de cualquier empresa. Por tanto, la información de monitoreo de un equipo de red puede ser extraída de forma automática con un conjunto de herramientas adecuado. Esta sección describe los componentes del sistema propuesto

La metodología usada para el diseño del sistema se basa en las siguientes actividades:

• Análisis de la situación actual de la Empresa y toma de requerimientos del sistema en base a los criterios de los técnicos.
• Selección de las herramientas software a utilizar y elaboración de los diagramas de flujo del programa a implementar.
• Se realiza la codificación de cada una de las soluciones planteadas.
• Finalmente, se realizan las pruebas de funcionalidad del software en la Empresa y se procede a realizar las correcciones de los errores encontrados y las mejoras planteadas por los técnicos de CNT.

4.1 Requerimientos del sistema

El sistema software deberá ser capaz de satisfacer los siguientes requerimientos:

• Las entradas del sistema deberán ser obtenidas de manera fiable y automática.

• Los parámetros especificados dentro del proceso de Rutinas de Mantenimiento deberán ser analizados de manera automática en todos los equipos de la red IP-MPLS.

• La salida resultante debe ser concisa y confiable.

• El sistema debe ser diseñado de manera que pueda adecuarse a necesidades futuras, es decir, en caso de que posteriormente se consideren nuevos parámetros a revisar, estos podrán ser incluidos sin la necesidad de un cambio drástico en la estructura del sistema.

• El sistema debe ser multimarca, lo que permitirá abarcar en una única plataforma cualquier dispositivo de red independientemente de su fabricante. No estará limitado por las políticas impuestas de uno u otro propietario, convirtiendo al sistema en una herramienta de monitoreo multiplataforma.

4.2 Elementos y Herramientas utilizadas en el Sistema

El sistema constará de tres elementos claves: Servidor, Base de Datos y un Gestor de Contenido para la visualización de los resultados.

1) Servidor

Este elemento será la interfaz equipo-sistema que posibilitará dos tareas principales:

• Obtención de los registros operacionales y de eventos de los elementos de red.- La obtención de registros es una de las partes fundamentales que realiza el sistema, es por esto que se han considerado dos alternativas para su realización, el objetivo es que la herramienta desarrollada sea adaptable y robusta.

— La primera alternativa es mediante un proceso definido por Cisco basado en CISCO-CONFIG-COPY-MIB. Ésta última es un conjunto de archivos que entre otras funciones permite copiar archivos de configuración pertenecientes a un agente SNMP hacia y desde la red. En este caso el dispositivo gestionado (con su agente) es cada uno de los equipos Cisco de la red IP-MPLS y sus archivos de configuración son transferidos vía TFTP hacia el servidor. La información contenida en la MIB (Management Information Base), se encuentra alojada de forma jerárquica mediante los OID (Object

Indentifiers Device). Cada objeto identifica una variable que puede ser configurada o leída a través del protocolo SNMP. Para poder ejecutar este procedimiento es necesario que los equipos tengan configurado una comunidad SNMP privada con permisos de lectura y escritura.
— El segundo mecanismo usa una ejecución interactiva de comandos, a partir de la función de Linux EXPECT. Este mecanismo emula un diálogo entre el usuario y el elemento de red a través del servidor, pudiendo ser usado en equipos de cualquier fabricante [7].

• Almacenamiento y administración de las bases de datos y tablas necesarias para el adecuado funcionamiento del sistema.

2) Bourne Again Shell

Bash es un shell que interpreta comandos introducidos por el usuario, éstos también pueden ser leídos y/o ejecutados de manera secuencial desde un archivo llamado Script.
Algunas de sus características y funciones se mencionan a continuación:

• Edición de línea de comandos.

• Redireccionamiento de entradas y salidas para controlar y filtrar información.

• Control absoluto del entorno de los procesos.

• Ejecución de comandos desde el teclado o desde ficheros (Scripts).

• Lenguaje de programación con una amplia gama de variables, operadores, matrices, estructuras de control de flujo, funciones, definición de alias, etc.

• Control y ejecución de procesos en primer y segundo plano.

• Historial ilimitado de los comandos ejecutados.

El software está desarrollado en base a CentOS, una distribución de Linux que utiliza Bash.

3) WordPress

Es un CMS (Content Management System) o gestor de contenidos. Se trata de un software de código abierto que permite administrar de manera dinámica contenido escrito en lenguajes que pueden ser entendidos por un servidor, entre estos lenguajes figuran PHP y MySQL.
Este gestor permite crear fácilmente páginas web de todo tipo sin escribir código en html. Separa el contenido y el diseño de una página web, permitiendo cambiar el diseño sin afectar la información del sitio web.
Es una herramienta gratuita que funciona a partir de una base de datos en donde es almacenada la información del sitio web, y de un servidor en el cual se encuentra alojado.
El sistema de monitoreo utiliza WordPress para publicar los resultados de la ejecución automática de las Rutinas de Mantenimiento.

4) Base de Datos

Una base de datos es una entidad que puede almacenar gran cantidad de información de manera estructurada [8]. MariaDB y MySQL, son los dos softwares libres de gestión de bases de datos más ampliamente difundidos.

MariaDB al igual que MySQL, utiliza un lenguaje estructurado de consulta interactiva denominado SQL (Structured Query Language). Los comandos que utiliza este lenguaje de programación permiten la creación, almacenamiento, manipulación y consulta de información alojada en una base de datos. La información de una base de datos es organizada en tablas. En las tablas generadas por un SGDB, los datos se almacenan en filas y columnas, de manera de que no se presente redundancia en la información.

El servidor que se utilizará en el sistema cuenta con la base de datos ´ommpls´ dentro de la cual la tabla ´maestro´ es de característica estática. En esta tabla se almacena información de todos y cada uno de los equipos de la red IP-MPLS. Entre esta información se encuentran: nombre del dispositivo, dirección IP, marca, modelo del equipo, rol dentro de la red IP-MPLS, si el dispositivo está o no en proceso de mantenimiento, entre

ISSN: 1390 -9266 – 2020 LAJC

otras. Varios de estos parámetros serán consultados por el sistema de monitoreo de manera frecuente.

Después de realizar el proceso de análisis, los resultados generados por el sistema se almacenarán en una tabla denominada ´reporte´. Este reporte será de característica dinámica debido a que el sistema actualizará dicha tabla semanalmente. Sin embargo, una vez que el reporte semanal se genere, se hará una copia del mismo en una tabla estática dentro de la base de datos ´reportes_rutinas´, esta copia será identificada con la fecha en la cual el sistema fue ejecutado con el fin de disponer de un historial de los resultados del análisis.

4.3 Estructura del sistema

En la sección Rutinas de Mantenimiento, se puede observar que los parámetros a ser analizados varían en base al rol que los equipos desempeñan dentro de la red, a su fabricante y en ciertas ocasiones a la serie del dispositivo. A partir de esta premisa se han clasificado los equipos de la red en siete grupos. La Tabla III, muestra esta clasificación.

TABLE III. AGRUPACIÓN DE EQUIPOS DE LA RED IP-MPLS

CAPA	GRUPO
ACCESO	CISCO
	HUAWEI-ALCATEL
AGREGACIÓN	CISCO Series 7600
	CISCO Series 3000
	CISCO Series 900
	Cisco IOS XR (ASR Series 9000)
CORE	Cisco IOS XR (ASR Series 9000)

Dentro de la estructura del sistema serán creados siete scripts independientes en función a la clasificación de la Tabla III. Cada script constará de cuatro partes principales que son: filtrado de equipos de acuerdo con las características de cada grupo, obtención de registros de operación, análisis de parámetros e inserción de resultados globales en la tabla 'reporte'.

En la Fig. 2 se puede apreciar un diagrama de flujo de la forma en cómo está estructurado el sistema de monitoreo

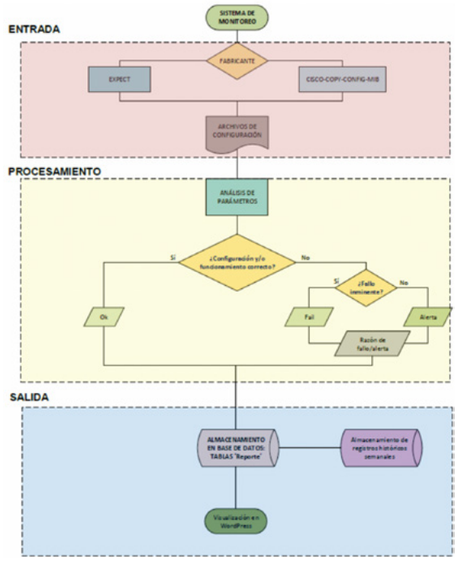

Fig. 2 Estructura del diseño del sistema de monitoreo

En un inicio se pueden observar las Entradas, éstas abarcan los registros operacionales y de eventos obtenidos de cada equipo. El procesamiento de la información consta en realizar el análisis de cada uno de los parámetros especificados dentro de las Rutinas de Mantenimiento. Este análisis se hará por medio de scripts de código escritos en BASH. Los posibles resultados del análisis de cada parámetro son los siguientes:

• "OK": En el caso de que el comportamiento del equipo sea correcto.
• "FAIL": Si fue detectada una falla que requiera soporte de un técnico.
• "NA" (No Aplica): En situaciones que el parámetro analizado no sea requerido en determinado equipo.
• "Warning": Cuando se considere que el resultado del análisis no requiera soporte inmediato, pero deban ser tomadas precauciones.
• "No Data": En circunstancias por las que no se obtuvo la información de entrada, de igual modo se detallará el motivo de este evento.

En el caso de encontrar fallas en la configuración, se presentará un breve detalle de la información relevante a considerar del equipo. Finalmente, la información obtenida del análisis realizado en cada uno de los scripts será almacenada dentro de la base de datos ommpls; a su vez

se realizará una copia del resultado final del análisis en una base de datos diferente con la finalidad de obtener registros históricos. Todo el contenido de los 'reportes' será visualizado a través de la interfaz de WordPress.

4.4 Scripts

Los scripts desarrollados se escribirán en BASH. Este lenguaje de programación ofrece una amplia gama de comandos con funciones específicas. Los siete scripts implementados son nombrados en la Tabla IV.

TABLE IV. SCRIPTS

CAPA	GRUPO	SCRIPT
ACCESO	CISCO	RTN_AcCisco.sh
	HUAWEI-ALCATEL	RTN_AcHuaAlc.sh
AGREGACIÓN	CISCO Series 7600	RTN_Ag7600.sh
	CISCO Series 3000	RTN_Ag3000.sh
	CISCO Series 900	RTN_Ag900.sh
	CISCO IOS XR (ASR Series 9000)	RTN_Agxr.sh
CORE	CISCO IOS XR (ASR Series 9000)	RTN_Core.sh

5 IMPLEMENTACIÓN DEL SISTEMA

En esta sección se presenta, la estructura global de los siete scripts que realizan el análisis de los parámetros de configuración de los equipos de la red IP-MPLS. Cada uno de ellos consta de cuatro partes fundamentales que son: filtrado de equipos, obtención de información, análisis de parámetros e inserción de resultados globales en la tabla reporte.

En la Fig. 3, se presenta un diagrama de flujo del sistema.

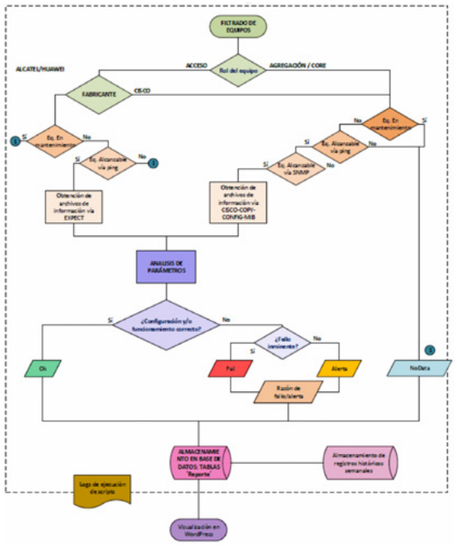

Fig. 3 Scripts: Estructura general

5.1 Filtrado de equipos

Desde la tabla 'maestro' se extraen los dispositivos que cumplen con las características del grupo respectivo. Como ejemplo, dentro del script RTN_Accisco.sh se extraerá la información básica de los equipos de capa acceso y marca CISCO. En la información básica se incluyen datos como: nemónico, dirección IP, modelo, comunidad SNMP, entre otras. Adicionalmente, serán definidas variables que harán referencia a la fecha actual del servidor.

5.2 Obtención de información

Se iniciará declarando variables que harán referencia a cada uno de los datos extraídos desde la tabla 'maestro', tales como: NOMBRE, IP, MODELO, COMUNIDADSNMP, entre otras. Se continuará verificando la comunicación servidor-equipo vías ping y/o SNMP. Posteriormente, se extraerán los archivos de configuración de cada equipo usando uno de los siguientes mecanismos o su combinación:

• CISCO-CONFIG-COPY-MIB (proceso vía SNMP, propietario CISCO)

ISSN: 1390 -9266 – 2020 LAJC

• EXPECT (ejecución interactiva de comandos)
A continuación, se presenta una explicación global de la programación referente a la obtención de información mediante cada uno de estos métodos.

1) CISCO-CONFIG-COPY-MIB

Este proceso hace uso de OIDs, para obtener de forma exitosa los archivos de configuración de cada equipo. Mediante los OIDs se logra lo siguiente:

• Administrar la solicitud de copia de archivos.
• Definir el protocolo para la copia de archivos.
• Especificar que la información a copiar está en el archivo running-config.
• Definir el tipo de archivo a donde se va a realizar la copia.
• Especificar la dirección IP del servidor hacia el cual se va a transferir los archivos.
• El nombre del archivo que contiene la información que se desea copiar.
• Especificar el tiempo que deberá transcurrir desde la petición de copia hasta finalizar el proceso.

El archivo que especifica la información que se desea copiar contiene uno a uno los comandos a ser ejecutados en el equipo.

2) Obtención de archivos de configuración mediante EXPECT

Debido a que el sistema debe ser adaptable, se ha optado por dar una alternativa al uso de SNMP para la extracción de archivos de configuración. Este mecanismo ejecuta de manera interactiva un comando o conjunto de comandos simulando una comunicación técnico-servidor-equipo. La Fig. 4 muestra la programación necesaria. Inicialmente se necesita definir las variables usuario y clave (ln 1-2). En las líneas 3-6 se declaran las variables comando_[1-n], las mismas contendrán la sintaxis de los comandos que permitirán obtener la información de los registros de configuración de los equipos. La sintaxis de los comandos varía de un fabricante a otro.

```
1 usuario=USUARIO
2 clave=PASSWORD
3 comando_1=`echo -e "comado1"`
4 comando_2=`echo -e "comando2\n"`
5 comando_n_menos_uno=`echo -e "comando_n_menos_uno\n"`
6 comando_n=`echo -e "comandon"`
```

Fig. 4 Variables necesarias dentro de EXPECT

Como atributo adicional la marca CISCO permite redireccionar el resultado del comando ejecutado a un archivo específico, como lo muestra el ejemplo siguiente:

```
comando=`echo -e "show spanning-tree | file
tftp://dir_ip/tmp/accisco/stp.axt"`
```

Para los equipos ALCATEL Y HUAWEI, no es posible el redireccionamiento, por lo cual el resultado de la ejecución de los n-1 comandos se almacenará en un único archivo. Cabe mencionar que el comando_n tiene como función terminar la sesión del usuario autenticado. Y es dependiente de la marca del equipo.

5.3 Análisis de parámetros

Esta sección es considerada como el cuerpo del script, debido a que contiene el mayor número de líneas de todo el código. En ella se analizarán uno a uno los parámetros asociados a las Rutinas de Mantenimiento. Por ejemplo, para los equipos de capa acceso y marca CISCO son analizados 5 parámetros, entonces, en el script RTN_Accisco.sh existirán 5 subsecciones de programación.

El sistema consta de 7 scripts, los mismos realizan el análisis del estado operativo de los equipos. Los parámetros a ser analizados varían de acuerdo al modelo y rol que el equipo desempeñe dentro de la red IP-MPLS.

La sección Análisis de Parámetros consta de n subsecciones que hacen referencia a los n parámetros que se desea analizar. En la Fig. 5, se presenta el diagrama de flujo de la programación que constituirá cada subsección.

5.4 Inserción de resultados globales en la tabla reporte

Previamente una tabla llamada 'reporte' ha sido creada para cada script. Por ejemplo, para RTN_Accisco.sh la tabla es llamada reporte_accisco. En ésta, se insertará la información que identifica al equipo y los resultados del análisis de parámetros.g

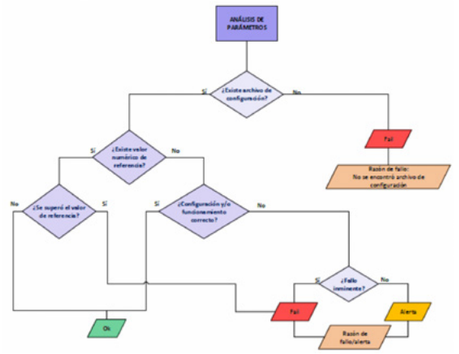

Fig. 3 Scripts: Estructura general

6 PRUEBAS DE FUNCIONAMIENTO Y SOPORTE

Durante el desarrollo de los códigos se realizaron pruebas individuales a cada uno de los scripts para verificar el correcto funcionamiento de los mismos.

6.1 Pruebas individuales realizadas de forma manual

Los siete scripts fueron desarrollados de forma independiente. Para la programación de cada uno de ellos se tomó como referencia los archivos de configuración de un equipo elegido al azar, perteneciente a cada grupo.

Tomando en cuenta esta premisa, las pruebas individuales constan de dos escenarios, el primero de ellos en donde el script es ejecutado solamente para el dispositivo referencial y el segundo en el cual el script se ejecuta para todos los equipos del grupo respectivo. Es necesario recalcar que dentro del primer escenario no se presentaron contratiempos relevantes, por lo cual los incisos siguientes harán referencia a las dificultades más significativas del escenario número dos.

1) Ajustes realizados en cuanto a fallas en la comunicación vía SNMP

Al momento de ejecutar un script para todos los elementos del grupo, se pudo constatar que varios de los equipos no eran mostrados en la salida del sistema. Al analizar los logs resultantes de la ejecución, se determinó que dichas ausencias se debían a la falta de configuración de la comunidad SNMP en el equipo. Este problema fue solucionado mediante el uso de un condicional al final de cada script.

La función del condicional es constatar el establecimiento de la comunicación vía SNMP, en el caso de que esta configuración no exista, se asignará como salida la frase 'Falta configurar comunidad SNMP'. Los valores de registro correspondiente al equipo analizado serán llenados con la palabra 'NoData'.

2) Inconsistencias en la existencia de los archivos a ser analizados

Al analizar de forma minuciosa la salida presentada por el sistema, se observó que, a pesar de no tener problemas de comunicación por el protocolo de gestión SNMP, en ciertas ocasiones se mostraban celdas en blanco. La causa fue la ausencia del archivo de configuración necesario para el análisis del parámetro respectivo. Dicha inexistencia se debe a acciones externas al sistema que influyen en el comportamiento del equipo. Situaciones propias de cada elemento, como: alto procesamiento, reinicio intempestivo y otras, pueden ocasionar este tipo de dificultades.

Para corregir esta clase de falencia, se agregó código al inicio de cada subrutina, para comprobar la existencia del archivo necesario para el análisis de cada parámetro. En el caso de la ausencia de este, en la salida del sistema se mostrará el mensaje "No se encontró el archivo de configuración"; caso contrario se continuará con el análisis normal.

3) Ajustes realizados debido a la variación del formato de la información de los archivos analizados

Los siete grupos en los que han sido clasificados los equipos de la red IP-MPLS, contienen en promedio un número elevado de dispositivos. Existiendo diversidad de modelos en cada uno de ellos.

Gran parte del análisis de parámetros se realiza mediante comparaciones a través de operadores numéricos, esta acción solo puede ser efectuada si los datos a ser evaluados están dentro de esta categoría. Uno de los obstáculos que se presentó de manera recurrente en el segundo escenario de pruebas en el cual se ejecutó el script para todos los equipos del grupo, fue que, la ejecución del script se veía detenida abruptamente debido a inconsistencias en el tipo de datos a ser comparados.

Una vez analizados dichos errores, se concluyó que el formato de la información de los archivos variaba de un modelo a otro. Con el objetivo de solventar esta problemática, se determinó la necesidad de agrupar los equipos por modelos en base al formato de la información obtenida de ellos.

En este punto cabe recalcar que, para cada uno de los parámetros analizados la distinción entre modelos no es necesariamente la misma. Para ciertos análisis la agrupación no es necesaria y en otros puede haber más o menos diferencias. Solventado este tipo de errores, y sin tener evidencia de fallas en los logs de ejecución, se obtuvo la salida esperada de cada uno de los siete scripts.

La forma en la que los técnicos pueden visualizar los resultados se ha diseñado de la forma más sencilla posible, la misma se basa en un código de colores que agiliza la lectura de los resultados. El detalle de colores es el siguiente:

Verde simboliza una configuración adecuada. No se requiere acción de soporte.
Rojo Equipo con fallas en la configuración. Necesidad de soporte inmediato.
Naranja Estado de alerta. El equipo funciona adecuadamente, pero podrían suscitarse fallas a posteriori. Necesidad de soporte en cuanto sea posible.
Azul El análisis del parámetro de configuración no se aplica al dispositivo
Celeste No se obtuvieron datos para ser analizados. Posibles causas: equipo en mantenimiento, inalcanzable vía ping o no se pudo establecer comunicación vía SNMP.

6.2 Prueba paralela de scripts realizada de forma automática

Para la ejecución de esta prueba se utilizó la función CRONTAB, mediante la cual se ejecuta de forma automática un script, que tiene como función ejecutar en segundo plano los siete scripts, correspondientes a las rutinas de mantenimiento. A este último script se lo conocerá como RTN_Todas.sh.

Para la ejecución automática se utiliza la función CRONTAB de Linux. Posterior a analizar los logs de ejecución generados durante esta prueba, se determina el éxito del funcionamiento del sistema. Concluyendo que el sistema es automático y cumple a cabalidad con todos los requerimientos para los cuales fue diseñado.

6.3 Soporte al sistema de monitoreo

El sistema desarrollado consta de tres elementos principales: Servidor, Base de Datos y el Gestor de Contenido WordPress. Al presentarse un desperfecto en el funcionamiento de cualquiera de sus componentes es necesario conocer los pasos para reactivar el sistema en el menor tiempo posible.

1) Recuperación del servidor

Para efectuar este proceso es primordial tener un respaldo de los datos almacenados en el servidor, así como también, es necesario conocer la estructura de directorios sobre la cual funciona el sistema. Al levantar un nuevo servidor se requiere que éste cuente con las mismas características del original o superiores. A continuación, se presentan las características mínimas con las que el servidor debe contar.

- Sistema Operativo: CENTOS 7.2.1611
- Procesamiento: 2.5 GHz
- Memoria RAM: 2 Gbytes
- Servidor web: Apache 2.5.6
- Gestor de Base de datos: MySQL o MariaDB
- Lenguaje de programación: PHP 5.5.16
- Protocolo de gestión SNMP: Habilitado y activo
- Función EXPECT: Habilitado y activo

2) Restauración de Bases de Datos

Como se mencionó en un inicio, es primordial tener respaldos de la información con la cual interactúan los scripts desarrollados, en este caso la base de datos a respaldar es ommpls; para ello se puede utilizar lel siguiente comando, que hace un dump de toda la información contenida en MySQL:

```
mysqldump -u root -p -A > /Ruta/archivo_dump.sql
```


ISSN: 1390 -9266 – 2020 LAJC

Siempre y cuando se tenga este respaldo de forma previa, para la restauración de la información de bases de datos se empleará el siguiente comando:

```
mysql -u root -p nombre_BDD_a_restaurarse < /Ruta/archivo_dump.sql
```

3) Restauración del Gestor de Contenidos

Antes de iniciar una restauración es imprescindible tener un respaldo de la información original, esto se logra mediante el comando:

```
cp /usr/share/wordpress/Ruta_respaldo
```

Los pasos para restaurar el funcionamiento de Wordpress son:

• Verificar que el servidor web esté activo.
• Restaurar directorio WordPress.- Se ejecuta el comando:

```
cp /Ruta_respaldo/wordpress/usr/share/
```

• En el caso de ser necesario se modificará el archivo wp-config.php.

• Finalmente, se creará un enlace simbólico para el directorio wp, mediante el comando:

```
ln -s /usr/share/wordpress/var/www/html/ommpls
```

• donde ommpls es una etiqueta con la cual se apuntará al contenido de la carpeta wordpress.

ISSN: 1390 -9266 – 2020 LAJC

7 CONCLUSIONES

El proceso de rutinas de Mantenimiento que realiza el área O&M apalanca la disponibilidad y funcionamiento normal de los servicios que presta la red de un operador de gran escala como la CNT EP. No obstante, realizar el análisis de configuración de forma manual toma demasiado tiempo y genera retrasos en otras actividades asignadas a cada uno de los técnicos del área. Por otro lado, soluciones propietarias no pueden en muchas cosas gestionar un gran volumen de equipos. Por ello, hemos propuesto un sistema monitoreo sencillo y que utiliza herramientas gratuitas. El sistema toma ventaja de la distribución de los equipos en las capas de la red lo que determina los parámetros a ser monitoreados.

El sistema escala fácilmente en el número de equipos a monitorear y sólo requiere la apropiada adición del nuevo equipo en la tabla maestra y configuración del acceso a los equipos. Actualmente el sistema de monitoreo propuesto monitorea de forma satisfactoria alrededor de 2000 equipos en la red IP/MPLS de CNT. Trabajo futuro de nuestro sistema incluye el desarrollo de nuevas características como generación de respaldos y cambio de configuraciones.

En trabajos futuros, se plantea desarrollar módulos al software propuesto que permita automatizar las mismas tareas, pero de dispositivos de otras casas fabricantes. Además, se plantea añadir otras tareas a través de un perfil de Administrador y el acceso al sistema de monitoreo a través de un teléfono inteligente.

REFERENCIAS

[1] M. Romero, “Gestión de Redes,” [Online]. Available: http://www.dte.us.es/personal/mcromero/docs/gestionderedes.pdf. [Accessed: May. 2014]

[2] IBM, “Gestión de redes,” [Online]. Available: http://www.ibm.com/support/knowledgecenter/es/ssw_aix_6. [Accessed: Jun. 2009]

[3] Cisco Systems, “Resumen de diseño de una red LAN,” [Online]. Available: http://www.cisco.com/c/dam/r/es/la/internet-of everythingioe/assets/pdfs /en05_campus-wireless_wp_cte_es-xl_42333.pdf. [Accessed: Jul. 2009]

[4] I. Minei and J. Lucek, “MPLS-Enabled Applications: Emerging Developments and New Technologies,” England, UK, 2011.

[5] Cisco System, “Identifying Catalyst 5000 EARL Version and Other Common EARL Questions,” [Online]. Available: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-5000-series-switches/1059076.html [Accessed: Oct. 2005]

[6] D. Libes, “Expect: Scripts for controlling interactive proccesses,” [Online]. Available: https://www.usenix.org/legacy/publications/compsystems/1991/spr_libes.pdf [Accessed: May. 2020]

[7] S. Sudarshan, Fundamentos de Sistemas de Bases de Datos, Connecticut, Estados Unidos, McGrawHill, 2011.

[8] Circitor, “CISCO-CONFIG-COPY-MIB,” Cisco routers configuration, [Online]. Available: https://circitor.fr/Mibs/Html/C/CISCO-CONFIG-COPY-MIB.php [Accessed: Aug. 28, 2019]

AUTORES

VANESSA NAPA

Nació en Quito-Ecuador el 9 de Junio de 1991. Realizó sus estudios superiores la Escuela Politécnica Nacional, obteniendo el título de Ingeniera en Electrónica y Telecomunicaciones. Vanessa tiene la certificación CCNA y experiencia en el monitoreo de redes de grandes dimensiones.

LUIS URQUIZA AGUIAR

Ingeniero en Electrónica y Redes de Información por la Escuela Politécnica Nacional (EPN) de Ecuador. Recibió los títulos de Máster y Doctor en Ingeniería Telemática y el de Máster en Estadística e Investigación Operativa por la Universitat Politècnica de Catalunya (UPC) de España en 2012, 2016 y 2018, respectivamente. Tiene la acreditación de Investigador Agregado 2 de la Secretaria Nacional de Educación Superior, Ciencia y Tecnología (SENESCYT). Actualmente se desempeña como profesor auxiliar en el Departamento de Electrónica, Telecomunicaciones y Redes de Información de la EPN y Coordinador del grupo de investigación en Redes Inalámbricas. Sus intereses de investigación se enfocan en la redes vehiculares, redes de 5G y optimización.

ISSN: 1390 -9266 – 2020 LAJC

XAVIER CALDERÓN HINOJOSA

Trabaja en la Escuela Politécnica Nacional (EPN), donde es profesor principal a tiempo completo, ha sido miembro del Consejo del Departamento de Electrónica, Telecomunicaciones y Redes de Información (DETRI), Jefe del Laboratorio de Computación de la Facultad de Ingeniería Eléctrica y Electrónica, Director de Proyectos de Investigación: Semilla y Junior en la EPN; Director y Codirector de Proyectos de Investigación CEPRA de CEDIA (Consorcio Nacional para el Desarrollo de Internet Avanzado) y de Proyectos Internos de la EPN, además, fue Jefe del DETRI. Últimamente ha dirigido el proyecto de investigación relacionado al área Sistemas Inteligentes de Transporte y ha colaborado en un proyecto de investigación relacionado con la accesibilidad a internet en el Ecuador.