RIELAC
Revista de Ingeniería Electrónica, Automática y Comunicaciones

Sistema Integrado de Gestión de conmutadores LAN empleando el protocolo SNMP

Damián Ernesto Rodríguez Trujillo, Caridad Emma Anías Calderón, Liz Gámez Picó

RESUMEN / ***ABSTRACT***

El vertiginoso desarrollo tecnológico y creciente ritmo evolutivo de las redes actuales hacen que la gestión sea vital. Sin embargo, la existencia de la gestión heterogénea derivada de la heterogeneidad de las redes de telecomunicaciones provoca, entre otros, ineficiencias y encarecimiento de la operación de las redes. Algunos de los problemas de la gestión heterogénea son: necesidad de tener personal capacitado para operar cada uno de los sistemas de gestión propietarios correspondientes a tecnologías y equipamientos de diferentes fabricantes, trabajar con diferentes protocolos de gestión y enfrentar la diversidad e incompatibilidad de datos que llevan a inconsistencia y hasta posible duplicidad de la información de gestión. En este artículo se presenta el diseño e implementación de un Sistema Integrado de Gestión de conmutadores de red de área local (LAN) empleando el protocolo SNMP. Se revisan brevemente las características del protocolo SNMP, de la MIB de Monitoreo Remoto (RMON) y de la gestión de los conmutadores LAN. Para el diseño del sistema se tuvieron en cuenta requerimientos que consideraran las necesidades actuales de la gestión integrada en las empresas operadoras de servicios de telecomunicaciones. La programación se realizó empleando el lenguaje Python y se dividió en varios módulos: acceso y administración de usuarios; inventario y gestión de conmutadores LAN; estadísticas, eventos y alarmas; y funciones de diagnóstico. Su validación se realizó implementando el sistema en un pequeño escenario de prueba en la red de un operador público de servicios de telecomunicaciones, obteniéndose resultados satisfactorios.

Palabras claves: Gestión integrada de redes, protocolo SNMP, conmutadores LAN, sistemas de gestión.

The vertiginous technological development and increasing evolutionary rhythm of current networks make management vital. However, the existence of heterogeneous management derived from the heterogeneity of telecommunications networks causes, among other things, inefficiencies and increased cost of network operation. Some of the problems of heterogeneous management are: the need to have trained personnel to operate each of the proprietary management systems corresponding to technologies and equipment from different manufacturers, to work with different management protocols and to deal with the diversity and incompatibility of data that they carry. to inconsistency and even possible duplication of management information. This article presents the design and implementation of an Integrated Management System for local area network (LAN) switches using the SNMP protocol. Features of the SNMP protocol, Remote Monitoring MIB (RMON), and LAN switch management are briefly reviewed. For the design of the system, requirements were taken into account that considered the current needs of integrated management in the operating companies of telecommunications services. The programming was done using the Python language and was divided into several modules: user access and administration; LAN switch inventory and management; statistics, events and alarms; and diagnostic functions. Its validation was carried out by implementing the system in a small test scenario in the network of a public operator of telecommunications services, obtaining satisfactory results.

Keywords: Integrated management of networks, SNMP, LAN switches, management systems.

Integrated Management System for LAN switches using the SNMP protocol.

Recibido: 08/09/2022 Aceptado: 02/11/2022

1. -INTRODUCCIÓN

En la actualidad, la complejidad creciente en las redes de telecomunicaciones en productos y servicios de múltiples fabricantes y de diversas tecnologías llevó a la aplicación de técnicas y herramientas que permiten una correcta gestión de los recursos dentro de la red, que la mantenga operativa a niveles adecuados de funcionamiento y monitoreada con la finalidad de conocer su rendimiento, comportamiento de su equipamiento de interconexión y el tráfico que cursa diariamente [1]. Todos estos requerimientos han favorecido la evolución de la gestión de redes y han enfatizado su importancia para llevar a cabo de manera controlada y automatizada los procesos orientados a la correcta operación de las redes, al aumento del grado de satisfacción de los usuarios y a conseguir los objetivos de negocio fijados por las empresas proveedoras de servicios de telecomunicaciones [2].

Por otra parte, los operadores de redes que utilizan varios sistemas de gestión propietarios correspondientes a equipamientos de diferentes fabricantes, enfrentan una gestión de redes compleja [3], ya que deben conocer como operar cada sistema propietario y, lo que es más importante, enfrentar la incompatibilidad de datos de gestión y protocolos, diversidad y hasta posible duplicidad e inconsistencia de la información de gestión y no tener una única visión de toda la red. Esto se conoce como gestión heterogénea la cual impide que la gestión de redes sea efectiva en costo pues incrementa los gastos de operación (OPEX, del inglés *Operational expenditures*) [4].

Sin embargo, es necesario utilizar coherentemente la información que puedan aportar los diferentes recursos gestionados que existan en una red para garantizar la disponibilidad y reducir las fallas y, con ello, el costo de la gestión. Por ello es necesario pasar de soluciones de gestión descentralizadas, aisladas y específicas a centralizadas, integradas y multifabricantes [5].

Los problemas de incompatibilidad y complejidad de la gestión heterogénea también están presentes en la gestión de conmutadores de Red de Área Local (LAN, del inglés *Local Area Network*), de diferentes fabricantes, lo que hace que el objetivo principal de este trabajo sea el diseño e implementación de un Sistema Integrado de Gestión de conmutadores LAN empleando el Protocolo Simple de Gestión de Redes de Internet (SNMP, del inglés *Simple Network Management Protocol*) que considere los requerimientos planteados por los operadores de servicios de telecomunicaciones para solventar los problemas inherentes a la gestión heterogénea.

El resultado final se pretende que sea el desarrollo de un Sistema Integrado de Gestión de conmutadores LAN intuitivo y fácil de manejar que disminuya para los operadores de servicios de telecomunicaciones el uso de recursos humanos, simplifique la gestión, disminuya los costos, emplee una base de datos con información de gestión única y permita obtener una visión integrada de la red, empleando un solo protocolo de gestión.

Para el desarrollo del artículo se parte de las bases teóricas que sustentan la investigación, a continuación, se presenta la propuesta de diseño del sistema y, finalmente, se realiza su implementación en un pequeño escenario de prueba a modo de validación.

2. -GESTIÓN DE CONMUTADORES LAN

La Gestión de Redes se basa en la planificación, instalación, supervisión y control de los elementos que forman una red para garantizar un nivel de servicio de acuerdo a un costo. Su objetivo es mejorar la disponibilidad y rendimiento de las redes y servicios e incrementar su efectividad. La gestión se caracteriza por dos procedimientos básicos: la monitorización y el control de la red y sus recursos, en cada una de sus áreas funcionales: Gestión de Fallos, Gestión de Configuración, Gestión de Contabilidad, Gestión de Desempeño o Prestaciones y Gestión de Seguridad [6].

Al crecer la complejidad en las redes de datos e incrementarse los requerimientos en su disponibilidad y rendimiento se hizo necesario el desarrollo de nuevos y mejores protocolos, y procedimientos que permitan extraer, colectar, transferir, almacenar y reportar información de gestión proveniente de los elementos gestionados.

El protocolo SNMP, es un protocolo de capa de aplicación de la arquitectura de redes de Internet (conocida como TCP/IP) utilizado para intercambiar información de gestión entre agentes (en los nodos gestionados) y gestores. Los componentes básicos de SNMP son: gestor SNMP, agentes SNMP en los dispositivos gestionados y Bases de Información de Gestión (MIB, del inglés *Management Information Base*) [7,8]. La Fig. 1 muestra la interacción gestor-agente del protocolo SNMP.

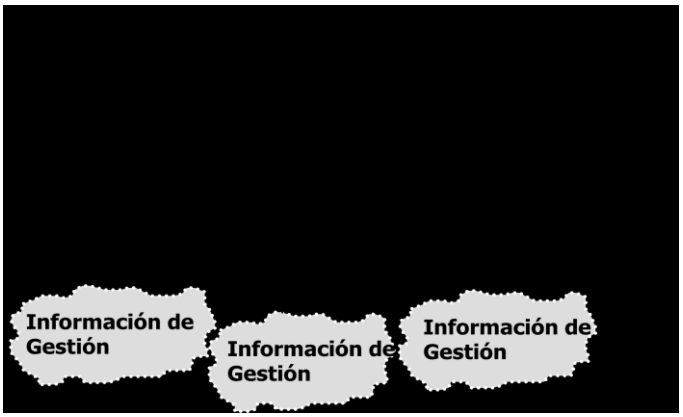

Figura 1

Interacción gestor-agente en SNMP

El gestor SNMP solicita al agente información específica del elemento de red y procesa la información según sea necesario para el Sistema de Gestión de Red (NMS, del inglés *Network Management System*) [9]. Cada agente SNMP mantiene una MIB que contiene la información de gestión del dispositivo gestionado, el cual es supervisado y controlado desde los gestores a través de comandos SNMP básicos. Las MIB se componen de objetos gestionados, identificados mediante el nombre Identificador de Objeto (OID, del inglés *Object Identifier*), que son organizados jerárquicamente en lo que se conoce como árbol MIB [10].

Existen varias MIB que pueden ser gestionadas empleado SNMP: estándar, experimental y propietaria. En esta última se encuentra la información de gestión que definen los diferentes fabricantes para gestionar su equipamiento.

Dentro de las MIB estándar se encuentra la MIB de Monitoreo Remoto (RMON, del inglés *Remote Monitoring* o SMON, del inglés *Switch Monitoring*) [8,11]. Esta MIB fue desarrollada para respaldar el monitoreo y el análisis de segmentos LAN que se encontraban alejados de un sitio central de gestión, siendo una especificación estándar de la industria que proporciona gran parte de la funcionalidad que ofrecen los analizadores de red patentados. Con RMON se puede supervisar una subred como un todo sin tener que estar sondeando a cada dispositivo que se encuentre en ella. Para ello en cada subred debe existir un agente o sonda RMON que es configurado por los gestores para recoger la información de monitoreo que requieren. En los agentes RMON se precisa la información a filtrar y capturar, y las alarmas a emitir a partir de definir, entre otros, la variable de interés y sus valores umbrales. Esto hace más eficiente la gestión. La Fig. 2 muestra parte del árbol de registro de la MIB estándar RMON versión 1 y 2.

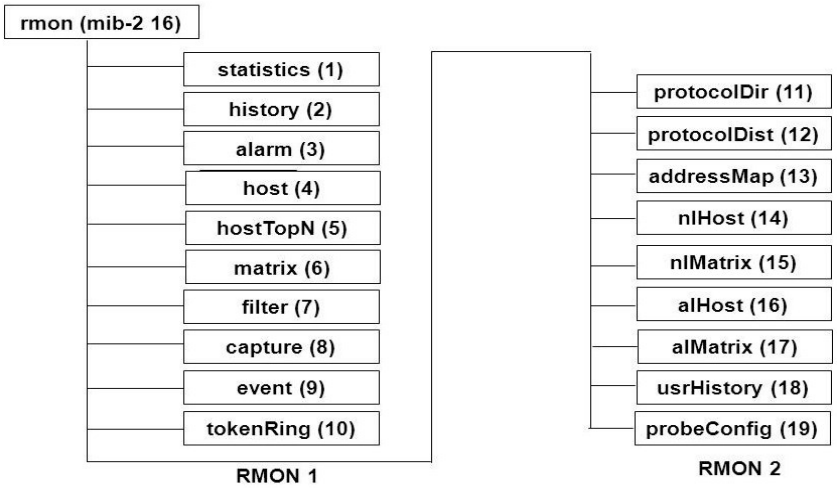

Figura 2

MIB RMON v1 y v2

Se han desarrollado varios sistemas para la gestión automatizada de redes conocidas por la efectividad de su funcionamiento en el control y monitoreo de equipos de interconexión, y otros elementos de red, que en su mayoría emplean el protocolo SNMP. Estos sistemas de gestión se evalúan, fundamentalmente, teniendo en cuenta si son de software libre o propietario; su forma de representación de datos; las alarmas y gráficos que muestran; su nivel de escalabilidad; el manejo que hacen de los agentes de monitoreo; la visualización de la topología de red y el envío de notificaciones.

Hoy en día la inmensa mayoría de los conmutadores LAN son gestionables y pueden configurase para ofrecer al personal de administración una adecuada gestión de ellos. Muchos están diseñados para cargas de trabajo intensas y soporte de grandes cantidades de tráfico por lo que en su despliegue necesitan configuraciones personalizadas. La mayoría de proveedores implementan la gestión de sus conmutadores a través de SNMP.

Algunos aspectos gestionables de los conmutadores LAN son: Redes de Área Local Virtual (VLAN, del inglés *Virtual Local Area Network*), seguridad, autenticación/control de acceso, visibilidad del cableado, monitorización del rendimiento de la red, Calidad de Servicio (QoS, del inglés *Quality of Service*), compatibilidad con el Protocolo de Árbol de Extensión Rápido (RSTP, del inglés *Rapid Spanning Tree Protocol*) o sus variantes, redundancia y reflexión de puertos [12].

En la bibliografía referente al tema aparecen algunas soluciones de sistemas desarrollados de código abierto o propietarios, que permiten integrar la gestión de los conmutadores LAN de la red. En [13] comparan tres formas de configurar los dispositivos de red: interfaz de usuario orientada a comandos (CLI, del inglés *Command Line Interface*) no estándar, SNMP estándar y el protocolo de configuración de red (NETCONF, del inglés *Network Configuration Protocol*), donde resumen que SNMPv1, 2, 2c y 3 se ha utilizado principalmente para el monitoreo de la red y muy raramente para la configuración de dispositivos de red con sus comandos SET; que el uso de la interfaz CLI no estándar ha demostrado ser una solución muy compleja e ineficaz, especialmente con un desarrollo rápido y una mayor complejidad en el área de redes informáticas; y que NETCONF define la solución estándar para la interfaz de usuario CLI orientada a comandos para la configuración de dispositivos de red de diferentes proveedores.

NETCONF [14] define un mecanismo estándar para la interfaz CLI utilizada para la configuración de dispositivos de red de diferentes vendedores [15] y para obtener información del dispositivo y manipular o actualizar ficheros de configuración. Se basa en el uso de un protocolo de transporte orientado a la conexión, en la mayoría de los casos TCP, que puede utilizarse de manera segura a través de túneles de Acceso Remoto Seguro (SSH, del inglés *Secure Shell*). NETCONF utiliza un modelo de comunicación basado en Llamadas a Procedimientos Remotos (RPC, del inglés *Remote Procedure Call*) y el cliente puede ser un script o una aplicación típica corriendo dentro de un software gestor de red.

El modelado de datos para la información de gestión es imprescindible en la gestión automatizada de redes [16]. NETCONF emplea el lenguaje de modelado de datos de nueva generación (YANG, del inglés *Yet Another Next Generation*) [17], que se conoce desde hace tiempo, empieza a estar en los portafolios de algunos fabricantes, y se utiliza en las Redes Definidas por Software (SDN, del inglés *Software Defined Networking*) y con TOSCA (del inglés *Topology and Orchestration Specification for Cloud Applications*) para el desarrollo de funciones de red virtual (VNF, del inglés *Virtual Network Functions*). YANG define una jerarquía de datos que pueden ser usados para operaciones base como: configuración, estado de datos, RPC y notificaciones. Esto permite una completa descripción de los datos que son enviados entre un cliente y un servidor NETCONF [2].

Por su parte, el trabajo recogido en [1], propone un sistema multiagente desarrollado con la librería PySNMP de Python, basado en capas, con tres tipos de agentes para la recolección, análisis y presentación de los datos, con el objetivo de monitorear los dispositivos centrales de la red de un campus (enrutadores, conmutadores LAN y otros), permitiendo la incorporación de diferentes protocolos, además de SNMP, con capacidad de personalización de los agentes, lo cual complica el sistema de gestión.

En [18] no se utiliza SNMP, se emplean interfaces de programación de aplicaciones (API del inglés *Application Program Interface*) para lograr la integración de la gestión, método empleado en la actualidad pero que es algo más complicado pues usualmente requiere un elemento intermedio para el acoplamiento de las interfaces de los diferentes elementos de la red. En [19] se hace referencia al modelo de un sistema ligero y escalable, el cual utiliza métricas, recopilación, almacenamiento, presentación y alertas para notificar al administrador de la red de dispositivos o procesos con mal comportamiento a través de un sondeo basado en SNMP, eliminando la curva de aprendizaje necesaria para la mayoría de los sistemas de monitoreo de código abierto, sin embargo deja de considerar varias funcionalidades de gestión importantes.

Otra herramienta de interés es DeviceView [20], solución de código abierto para la gestión de conmutadores LAN. Esta herramienta fue integrada al NMS de código abierto Nagios para facilitar y centralizar las tareas de gestión, lo cual evita que el administrador de red que la usa tenga que manipular las herramientas de gestión de cada fabricante facilitando la

visualización de la información de los conmutadores, de las VLANs, la gestión de cambios y la monitorización remota. Esto provoca que su uso requiera la instalación y operación de Nagios.

Además de los sistemas antes mencionados, existen otros de código abierto (ejemplo: *Zabbix*, *Cacti*, *Icinga*, *Elastic Stack*), y las soluciones propietarias (por ejemplo: *Tivoli* de IBM, *ProactiveNet Performance Manager* de BMC, *Unified Infraestructure Management* de *Computer Asociates*, *Magellan Network Management System* de *Imagine Communications*, *Cisco Monitoring* de Cisco y *OpManager* de *ManageEngine*), que son utilizados para gestionar no solo conmutadores LAN, sino también impresoras, enrutadores, servidores, entre otros elementos de red. Estas soluciones, al cubrir varias funcionalidades en el mismo sistema, generalmente requieren un trabajo complejo y exhaustivo para la instalación y configuración, y para la gestión de los recursos de red por parte del operador. Además, las soluciones propietarias son costosas, no se tiene acceso al código y se deben licenciar para su uso y actualización en ambientes empresariales o académicos. Si el tema costo y la independencia tecnológica es un factor decisivo que influye negativamente en la selección del sistema, el uso de estas soluciones no es recomendable.

Lo más requerido por los operadores de redes que deben gestionar múltiples conmutadores LAN, usualmente en un área extensa, es un sistema integrado de gestión, que sea relativamente simple y de código abierto para ejecutarlo, estudiarlo, cambiarlo y redistribuir copias de acuerdo a sus necesidades. Las preferencias del administrador de red, los requerimientos funcionales de la empresa y las necesidades técnicas de la red, deben permitir agregar, actualizar o eliminar funcionalidades al sistema. Precisamente, en este trabajo se realiza el desarrollo e implementación de un Sistema Integrado de Gestión de Conmutadores LAN con las características antes mencionadas.

3.- DISEÑO DEL SISTEMA INTEGRADO DE GESTIÓN DE CONMUTADORES LAN (*SIGCLAN*)

3.1.- ESQUEMA GENERAL

Como premisa para el diseño del Sistema Integrado de Gestión de conmutadores LAN, se desarrolló una herramienta o aplicación que permitiera a los administradores de redes acceder de manera remota y segura al sistema, a través de *internet* o de la *intranet* de la entidad, utilizando para ello un navegador *web*. Esto facilita mucho el trabajo de gestión ya que, el administrador no necesita estar en la ubicación de la red para interactuar con el sistema de gestión.

En el desarrollo del Sistema Integrado de Gestión de conmutadores LAN se consideraron los siguientes requerimientos:

- Poseer interfaz gráfica y amigable para mostrar la información de gestión y el comportamiento de diferentes parámetros de hardware y software.
- Exigir autenticación de todos los usuarios y establecer control de acceso al sistema.
- Realizar descubrimiento, monitoreo y control de los conmutadores LAN de la red.
- Configurar y obtener variadas estadísticas de tráfico, así como información de eventos y alarmas provenientes de los segmentos de red que interconecten los conmutadores LAN.
- Permitir el diagnóstico básico de los conmutadores LAN empleando los comandos de *ping* y *tracer route*.

En cuanto a la usabilidad, el sistema debe ser fácil de utilizar por los usuarios que no estén familiarizados con el mismo, permitiendo su asimilación en un corto plazo de tiempo; mostrar al usuario un diseño homogéneo e intuitivo en todas sus pantallas. Además, debe ofrecer rápida respuesta a las operaciones, pantallas poco cargadas, mínimo acceso a la base de datos, y no realización de consultas redundante. También el sistema debe ser escalable, permitir mejoras sistemáticas y la inclusión de nuevas funcionalidades, ser portable y seguro.

La información de gestión que se requiere para realizar las funciones de gestión previstas en el *SIGCLAN* es obtenida de los conmutadores LAN empleando el protocolo SNMP, que permite el acceso a los objetos gestionados existentes en las MIBs.

La Fig. 3 muestra un esquema general del Sistema Integrado de Gestión de Conmutadores LAN (*SIGCLAN*) que se propone para dar respuesta a los requerimientos descritos anteriormente. En dicho sistema se han considerado un conjunto de módulos que implementan varias áreas funcionales de la gestión, con vistas a simplificar su diseño y programación.

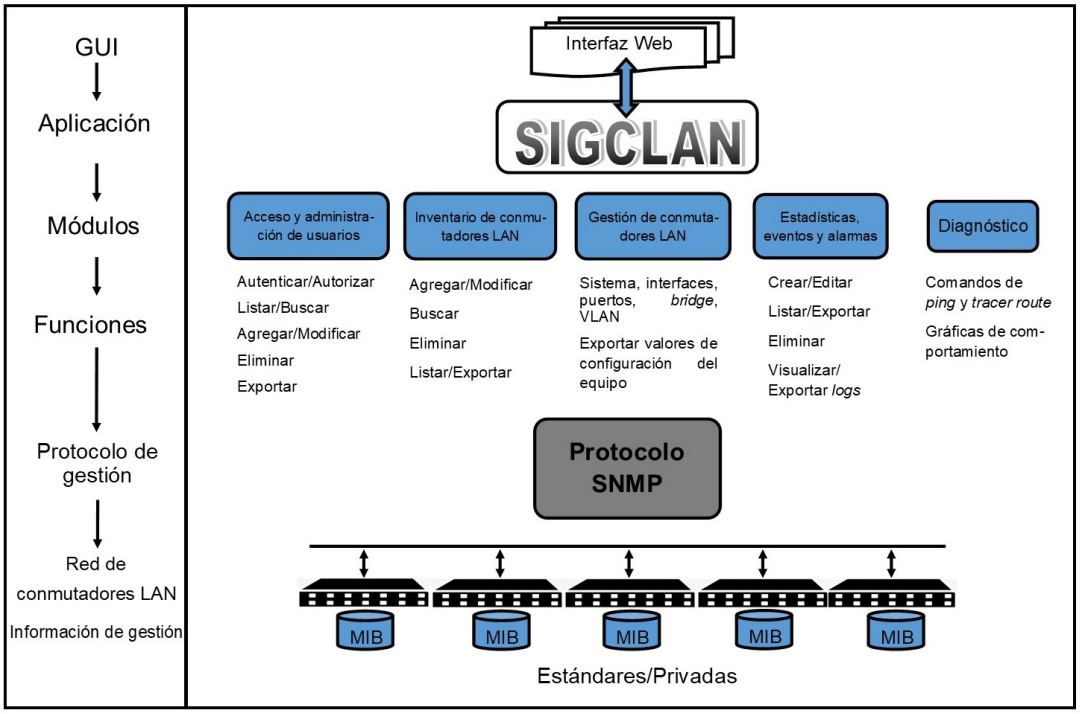

Figura 3

Esquema general del Sistema Integrado de Gestión de conmutadores LAN (*SIGCLAN*) [Desarrollo propio]

3.2.- PROGRAMACIÓN DE LOS MÓDULOS DEL *SIGCLAN*

La programación de los módulos de gestión mostrados en el esquema general del *SIGCLAN*, se realizó para trabajar sobre el sistema operativo Windows y se utilizaron las siguientes herramientas libres y de código abierto:

- Entorno de Desarrollo Integrado (IDE, del inglés *Integrated Development Environment*) *Visual Studio Code*, herramienta que tiene soporte nativo para gran variedad de lenguajes y posibilidad de configuración de interfaces de acceso a terminales y ofrece detalles de los problemas. Se puede encontrar fácilmente documentación y ayuda en foros y sitios relacionados.
- Python, utilizado por ser un lenguaje de programación de alto nivel, que brinda portabilidad y una baja curva de aprendizaje, además de una fuerte comunidad de desarrolladores.
- Librerías auxiliares para el trabajo con algunas de las funciones de Python y PySNMP [21], una librería de código abierto e implementación gratuita del protocolo SNMP en este lenguaje .
- Django, como marco de trabajo *web* de alto nivel escrito en Python, que permite el desarrollo de sitios *web* seguros y mantenibles.
- PostgreSQL, seleccionada como sistema gestor de bases de datos relacional orientada a objetos y de código abierto, la cual brinda la potencia y robustez necesaria para el tipo de aplicación que se propone.

Las funciones principales de Python utilizadas en la programación fueron:

1. Funciones de ejecución de programas externos, utilizadas para iniciar, parar servicios y ejecutar ciertos comandos del sistema. Por ejemplo, el comando de ping del módulo “Diagnóstico” del sistema se hace a través de una llamada a los subprocesos de Windows.
2. Funciones de PostgreSQL, para la manipulación de la información de la base de datos.
3. Funciones SNMP para el servicio del protocolo en sus distintas versiones, o sea: *get*, *get next*, *get bulk*, *set*, *traps*, *inform*, *response*.

Para el empleo de Django en el *SIGCLAN* tuvo presente que es un marco de trabajo o *framework* del tipo Modelo-Plantilla-Vista (MTV, del inglés *Model-Template-View*). Las plantillas contienen las decisiones relacionadas a la presentación del lado del cliente. Las vistas contienen la lógica del negocio que accede al modelo de datos y la delega a la plantilla apropiada, comportándose como un puente entre los modelos y las plantillas. En la Fig. 4 se observa el funcionamiento de trabajo de Django en el desarrollo de la aplicación *SIGCLAN*.

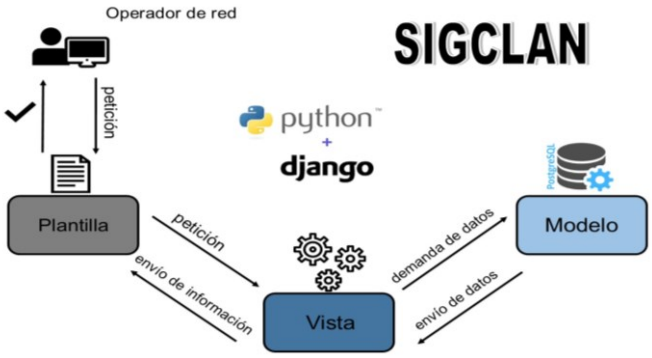

Figura 4

Patrón MTV de Django en *SIGCLAN* [Desarrollo propio]

Es de vital importancia para el desarrollo con calidad del sistema *SIGCLAN* minimizar la ocurrencia de errores y garantizar que la información gestionada sea coherente en cada momento, en función de lograr que el sistema sea confiable. Para lograr esto, en los formularios de entrada de datos se validan los campos y se comprueba que los de uso obligatorio no queden en blanco, evitando así la entrada de información incorrecta. En caso de producirse algún error, el sistema lo notifica al administrador de red y no realiza ninguna acción; a nivel de los modelos se definen dichas validaciones para garantizar que los campos tomen los valores acorde a su tipo y función.

Para facilitar el desarrollo de *SIGCLAN* se utilizó el paquete de la base de datos PostgreSQL para Python psycopg2 y, además pgAdmin, una aplicación de diseño y manejo de bases de datos para su uso con PostgreSQL.

El *SIGCLAN* está diseñado para responder a las necesidades de información de los administradores de red, desde una simple consulta SQL, hasta el acceso a bases de datos complejas, como sería el caso de los datos registrados en la red de conmutadores LAN de una empresa proveedora de infraestructura de telecomunicaciones que posee alcance nacional.

Uno de los aspectos fundamentales en el desarrollo del *SIGCLAN* es la manipulación de la información registrada en la base de datos PostgreSQL mediante Python. Por ello, el diseño de la base de datos debe asegurar que los datos persistentes del sistema sean almacenados de manera estable y segura, así como establecer el comportamiento que estos deben tener implementado en la base de datos, a través de sus representaciones lógicas y físicas.

Para el trabajo con la base de datos y la programación de los módulos del sistema, se definieron los modelos de datos Usuarios, Dispositivos, Interfaces, Estadísticas, Eventos, Logs, Alarmas, Puertos y VLAN. La Fig. 5 muestra el modelo de datos Inetrfaces.

```
32  class Interfaces(models.Model):
33      ipiface=models.CharField(max_length=15)
34      ID=models.IntegerField(null=True, blank=True)
35      descripcion=models.CharField(max_length=250, null=True, blank=True)
36      alias=models.CharField(max_length=200, null=True, blank=True)
37      tipo=models.CharField(max_length=100, null=True, blank=True)
38      conector=models.CharField(max_length=100, null=True, blank=True)
39      mtu=models.CharField(max_length=100, null=True, blank=True)
40      velocidad=models.CharField(max_length=100, null=True, blank=True)
41      estado_op=models.CharField(max_length=100, null=True, blank=True)
42      estado_admin=models.CharField(max_length=100, null=True, blank=True)
43      pktin=models.CharField(max_length=100, null=True, blank=True)
44      pktout=models.CharField(max_length=100, null=True, blank=True)
45      promiscuo=models.CharField(max_length=100, null=True, blank=True)
```

Figura 5

Modelo de datos Interfaces [Desarrollo propio]

3.3.- DISEÑO DE LAS INTERFACES DEL *SIGCLAN*

La primera interfaz que aparece en el *SIGCLAN* es la que permite la autenticación y autorización de los usuarios, utilizando para ello los campos usuario y contraseña. Esta interfaz forma parte del módulo Acceso y administración de usuarios del sistema. De acuerdo al tipo de usuario (administrador o súper administrador) que se suministre, así será la próxima interfaz que ofrecerá *SIGCLAN*. Si el usuario ingresado no existe en la base de datos del sistema, aparece una notificación de error y nuevamente se mostrará la interfaz inicial de autenticación.

Una vez que un usuario autorizado ingresa al *SIGCLAN*, en cualquier interfaz que se le presente encontrará, a la izquierda, un menú vertical con las funcionalidades incorporadas al sistema. A la derecha hallará una sección dinámica de resultados que mostrará la información en tablas y formularios de acuerdo con la opción que se seleccione. Además, el sistema ofrecerá cuadros de alertas y de confirmación, al igual que etiquetas de información que ayudan al usuario a comprender sus funcionalidades.

El *SIGCLAN* posee principalmente dos páginas: la principal y generalidades del sistema; y la de gestión de conmutadores LAN, donde aparecen las particularidades del conmutador LAN que se seleccione entre los que están incorporados al sistema.

Página principal y generalidades del sistema.

Esta página de datos muestra las opciones siguientes:

- Listado de conmutadores LAN
- Diagnóstico general
- Administración de usuarios

Por ejemplo, la opción Listado de conmutadores LAN corresponde al módulo Inventario de conmutadores LAN gestionado por *SIGCLAN*. Esta opción muestra la tabla que se muestra en la Fig. 6 donde aparece la información correspondiente a las características de los conmutadores LAN incorporados al sistema: fabricante, dirección IP, dirección de Control de Acceso al Medio (MAC, del inglés, *Media Access Control*), ubicación, cantidad de puertos; y la implementación del acrónico informático Crear, Leer o Listar, Editar o Actualizar y Eliminar (CRUD, del inglés *Create, Read, Upgrade and Delete*).

Figura 6

Opción Listado de conmutadores LAN [Desarrollo propio]

En la opción Ver el sistema muestra una imagen del conmutador LAN seleccionado, el uso de CPU y memoria, la temperatura y tiempo de actividad del conmutador LAN, e información general del mismo, como descripción, nombre, contacto, ubicación, dirección IP, MAC, cantidad de puertos e interfaces, y nombre de la comunidad SNMP. Estos elementos se obtienen de la lectura, con el comando SNMP *get*, de los OID correspondientes al grupo system de la MIB-2, y algunos OID de la *Bridge* MIB y las MIB privadas, dependiendo del fabricante del conmutador LAN seleccionado.

Página de Gestión de conmutadores LAN

Esta página de gestión muestra las siguientes opciones:

- Información general del conmutador LAN
- Interfaces
- Puertos
- *Bridge*
- VLAN

- RMON, que despliega un menú con otras opciones: Estadísticas, Eventos y Alarmas.
- Diagnóstico

El diseño de la opción de menú Interfaces del sistema *SIGCLAN* se muestra, como ejemplo, en la Fig. 7, la que corresponde con las variables del modelo de datos presentado en la figura 5.

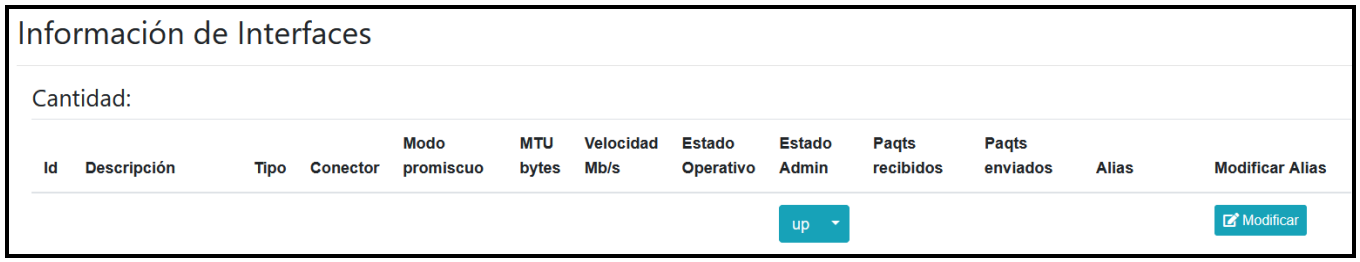

Figura 7

Opción Interfaces del conmutador LAN [Desarrollo propio]

El sistema presenta al usuario una tabla con la relación de interfaces del conmutador LAN seleccionado y sus características asociadas: descripción, tipo, presencia de un conector, estado del modo promiscuo, Unidad Máxima de Transferencia (MTU, del inglés *Maximum Transmission Unit*), velocidad, estado administrativo, estado operativo, paquetes recibidos, paquetes enviados, y alias; así como la opción de modificar el estado administrativo y el alias de las interfaces del conmutador LAN.

Algunos de los campos de la tabla de información de las interfaces del conmutador LAN se obtienen de la lectura de objetos, con la utilización del comando básico SNMP *get-bulk*, del grupo *interfaces* de la MIB-2, y de la ifMIB (como: *ifConnectorPresent*, *ifAlias*, *ifPromiscuousMode*) la cual constituye una extensión del grupo anterior de la MIB-2. La modificación de determinados objetos de estos grupos de la MIB-2 e ifMIB es posible empleando el comando SNMP *set* o *set-bulk*.

Dentro de la opción RMON se desarrollaron funcionalidades relacionadas con la recolección de estadísticas de una o varias de las interfaces del conmutador LAN, obtenidas a través de la lectura de los nodos de información de la tabla *etherStats* del grupo *statistics* de la MIB-RMON. Además, se trabajó con la tabla de control del grupo *events* y *alarm* de dicha MIB, para crear los *triggers* asociados a diferentes parámetros o variables de rendimiento del conmutador LAN. La Fig. 8 muestra el formulario para agregar la recolección de estadísticas en el *SIGCLAN*.

Figura 8

Formulario para agregar la recolección de estadísticas [Desarrollo propio]

4.- IMPLEMENTACIÓN DEL *SIGCLAN* Y RESULTADOS OBTENIDOS

El Sistema Integrado de Gestión de Conmutadores LAN (*SIGCLAN*) desarrollado fue implementado en un pequeño escenario de prueba de la red de un operador público de servicios de telecomunicaciones, estructurada en capas, que transporta el tráfico proveniente del acceso hasta las plataformas de servicio, controladores y otros elementos del núcleo de la red.

El escenario de prueba donde se implementó el *SIGCLAN* está formado por un conmutador LAN en la capa de agregación que conecta dos subredes al *backbone* de la red. Cada una de las cuales posee un conmutador LAN que interconecta en la capa de acceso a los equipos terminales de la red. Se seleccionaron conmutadores LAN de dos fabricantes diferentes, condición imprescindible para validar la integración del sistema diseñado. La Tabla 1 muestra las características de los conmutadores LAN del escenario de prueba. Es necesario destacar que no se muestran las direcciones IP completas para proteger los datos de direccionamiento del operador.

Tabla 1
Características de los conmutadores LAN del escenario

Conmutador LAN	Dirección IP	Comunidad SNMP	
Huawei s3300	152.206.X.1/25	Lectura	PRUEBA
Huawei s2300	152.206.X.69/25	Lectura-escritura	PRUEBA_1
Cisco c2960s	192.168.X.151/24	Lectura-escritura	write

En la Fig. 9 recoge el escenario de prueba representado por los conmutadores LAN y sus interfaces en cada uno de los enlaces entre los dispositivos. También en la figura aparece el servidor *web* donde se encuentra instalado el Sistema Integrado de Gestión de conmutadores LAN desarrollado.

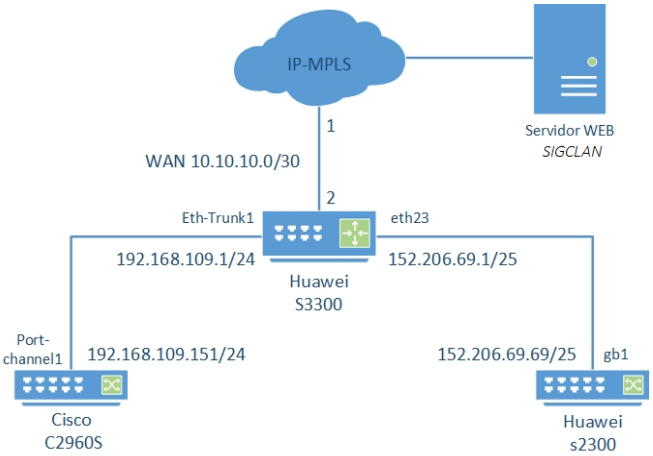

Figura 9
Escenario de prueba [Desarrollo propio]

Para gestionar un conmutador LAN con *SIGCLAN* es necesario, primeramente, realizar el enrutamiento entre la subredes donde se encuentran los conmutadores LAN y la subred del servidor *web* donde está instalado el sistema diseñado; Además, se deben definir las comunidades SNMP de lectura/lectura-escritura para la comunicación SNMP entre el *SIGCLAN* y los agentes de los conmutadores LAN, así como precisar el rango o las direcciones IP de los dispositivos a gestionar. Además, también se deben definir las Listas de Control de Acceso (ACL, del inglés *Access Control List*), como parte de las configuraciones de seguridad de los conmutadores.

La Fig. 10 muestra la página principal y generalidades del *SIGCLAN* correspondiente al escenario de prueba que se está considerando.

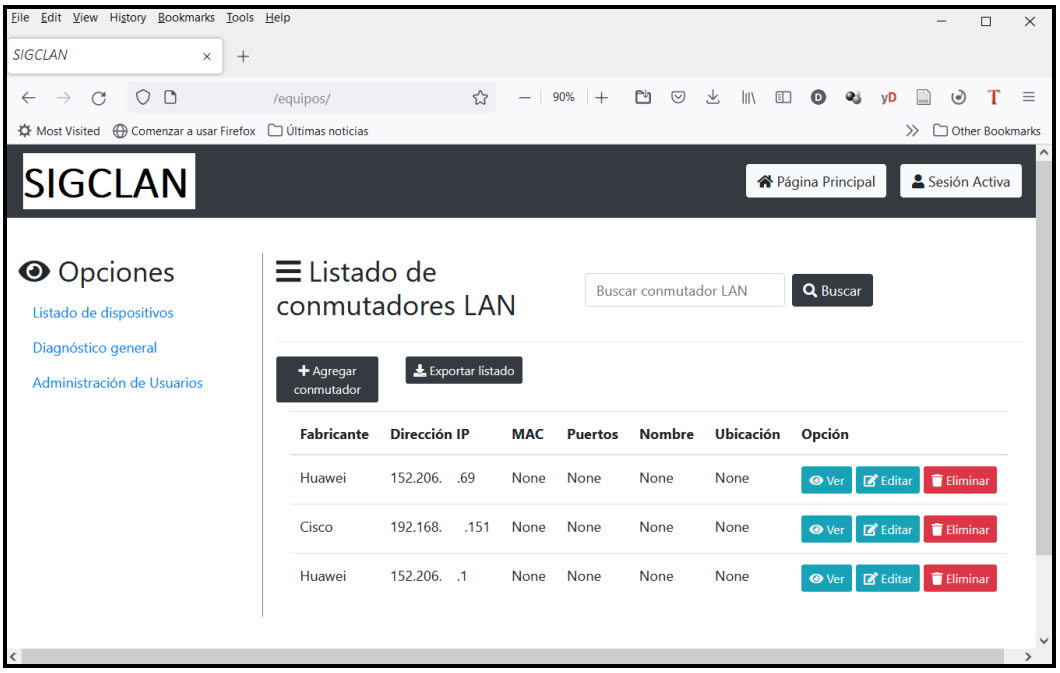

Figura 10

Listado de los conmutadores LAN del escenario

Si se selecciona alguno de los conmutadores LAN del escenario de prueba, automáticamente se muestra en la página de Gestión del sistema la información obtenida a través de SNMP. En la Fig. 11 se ilustra la información correspondiente al conmutador Huawei s3300.

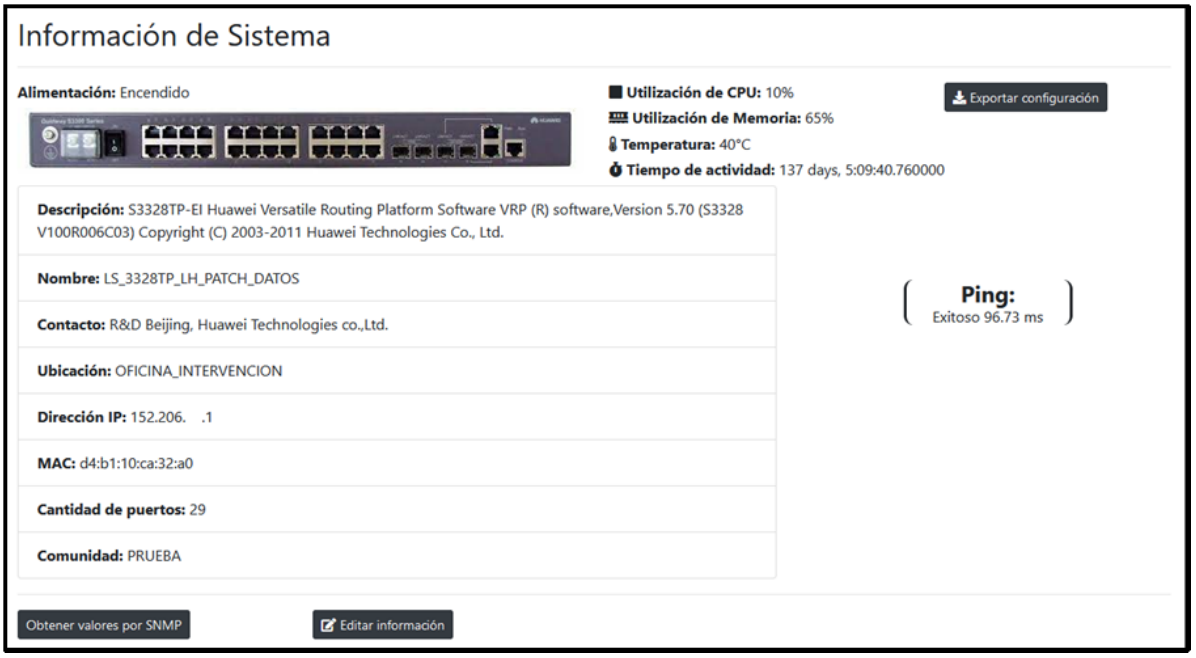

Figura 11

Autodescubrimiento SNMP del conmutador LAN Huawei s3300

Análisis de los resultados obtenidos en la implementación de *SIGCLAN*

La implementación, en la red de un proveedor de servicios públicos, del Sistema Integrado de Gestión de conmutadores LAN desarrollado, permitió comprobar su validez. Se logró realizar, con un grado significativo de estabilidad y confiabilidad, labores de monitorización y control utilizando las funcionalidades desarrolladas. A partir de los resultados obtenidos en las pruebas realizadas se puede esperar que el despliegue del sistema *SIGCLAN* permita efectuar una gestión integrada y proactiva de la red al punto de aspirar a que en la mayoría de las ocasiones las fallas en los conmutadores LAN que se gestionan no lleguen a ser percibidas por los clientes de la red.

En particular, en la implementación del sistema *SIGCLAN* en el escenario de prueba de la red de un operador público de servicios de telecomunicaciones se han obtenido los siguientes resultados:

- Detección de fallas, a través de la monitorización de los conmutadores LAN.
- Elaboración de reportes actualizados e históricos de la disponibilidad y el estado de los conmutadores LAN.
- Acceso en tiempo real, por el personal de administración autorizado, a la información de gestión de los conmutadores LAN, desde cualquier punto de la red empleando una interfaz *web*, lo que les permite actuar con mayor celeridad.

6.- CONCLUSIONES

Los Sistemas Integrados de Gestión de red son cada vez más necesarios para cualquier tipo de organización que opere una red de telecomunicaciones. El diseño e implementación del Sistema Integrado de Gestión de conmutadores LAN, *SIGCLAN*, que se presenta en este artículo dio respuesta al problema y requerimientos planteados ya que con el SIGCLAN es posible gestionar adecuadamente conmutadores LAN de diferentes fabricantes utilizando el estándar de gestión SNMP, código abierto e interfaz gráfica amigable, logrando consistencia en la información de gestión al implementar una única base de datos. De esta forma, contribuye a una mayor eficiencia y eficacia de su operación, lo que disminuye el OPEX y consecuentemente, eleva la calidad de los servicios ofrecidos por los operadores de telecomunicaciones. Además, *SIGCLAN* cumple requerimientos importantes como sistema informático que son: escalabilidad, usabilidad, rendimiento y seguridad.

AGRADECIMIENTOS

Los autores desean agradecer al operador público de servicios de telecomunicaciones que facilitó parte de su red para implementar y validar el *SIGCLAN*.

REFERENCIAS

1. Espinel Villalobos RI, Ardila Triana E, Zarate Ceballos H, Ortiz Triviño JE. Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents. Ingeniería e Investigación. 1 de enero de 2022;42(1):e87564.

2. Park P, Na T, Kim T. Device Independent YANG Auto-generation Mechanism. En: 2021 International Conference on Information and Communication Technology Convergence (ICTC). 2021. p. 1300-5.

3. Laštovička M, Husák M, Sadlek L. Network Monitoring and Enumerating Vulnerabilities in Large Heterogeneous Networks. En: NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. 2020. p. 1-6.

4. Peña-Casanova M, Anias-Calderón C, Peña-Casanova M, Anias-Calderón C. Integración de marcos de referencia para gestión de Tecnologías de la Información. Ingeniería Industrial. abril de 2020;41(1):1-12.

5. Shahjee D, Ware N. Integrated Network and Security Operation Center: A Systematic Analysis. IEEE Access. 2022;10:27881-98.

6. Bracho Tovar G, Rueda Carreño A, MUNIVE M, GUERRA A, Mestre Arzuaga T, OSPINO A, et al. Detección de condiciones anómalas en redes de datos usando bases de información de gestión. Tecnología Interculturalidad y Naturaleza. Bogotá: Grupo Editorial Ibáñez. 2019. 149-199 p.

7. Fedor M, Schoffstall ML, Davin JR, Case JD. Simple Network Management Protocol (SNMP). Internet Engineering Task Force; 1990 may. Report No.: RFC 1157. Disponible en: https://datatracker.ietf.org/doc/rfc1157

8. Boyar O, Özen ME, Metin B. Detection of Denial-of-Service Attacks with SNMP/RMON. En: 2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES). Las Palmas de Gran Canaria, Spain; 2018. p. 000437-40.

9. Zakaria S, Nasir A, Fahmy S, Samsudin N. Development of a Prototype of Open-Source Network Management System. International Journal of Synergy in Engineering and Technology. 1 de diciembre de 2020;1(2):38-45.

10. Matoušek P, Ryšavý O, Polčák L. Unified SNMP Interface for IoT Monitoring. En: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). 2021. p. 938-43.

11. Cole RG, Romascanu D, Kalbfleisch CW, Waldbusser S. Introduction to the Remote Monitoring (RMON) Family of MIB Modules. Internet Engineering Task Force; 2003 ago. Report No.: RFC 3577. Disponible en: https://datatracker.ietf.org/doc/rfc3577

12. Quitiqut T, Bhuse V. Utilizing Switch Port Link State to Detect Rogue Switches. iccws. 2 de marzo de 2022;17(1):272-8.

13. Valenčić D, Mateljan V. Implementation of NETCONF Protocol. En: 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2019. p. 421-30.

14. Enns R, Björklund M, Bierman A, Schönwälder J. Network Configuration Protocol (NETCONF). Internet Engineering Task Force; 2011 jun. Report No.: RFC 6241. Disponible en: https://datatracker.ietf.org/doc/rfc6241

15. Valencic D. Vendors' Implementation of NETCONF Standard on Routers and Switches. En: 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO). 2020. p. 536-41.

16. Peña M, Anías Calderón C. Empleo de modelos de información en arquitectura modificada para gestión de redes y servicios basada en políticas. 1 de octubre de 2018;39:77-88.

17. Björklund M. YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF). Internet Engineering Task Force; 2010 oct. Report No.: RFC 6020. Disponible en: https://datatracker.ietf.org/doc/rfc6020

18. Afsar S, Korbatov A, Matten A. Design and Implementation of Network Operational Management Systems for Integrated and Automated Management of LANs and WANs. JOURNAL OF AGRICULTURE & SOCIAL SCIENCES. 1 de enero de 2005;1(2):156-160.

19. Brattstrom M, Morreale P. Scalable Agentless Cloud Network Monitoring. En: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). 2017. p. 171-6.

20. Linares JR, Cubillos FS, Gutierrez JH, Palacios DM. Gestión gráfica de dispositivos activos de red multivendedor. Ingeniería Solidaria. 1 de enero de 2018;14(24):1-11.

21. Choi B. Python Network Automation Labs: cron and SNMPv3. En: Choi B, editor. Introduction to Python Network Automation: The First Journey. Berkeley, CA: Apress; 2021. p. 629-73. Disponible en: https://doi.org/10.1007/978-1-4842-6806-3_15

CONFLICTO DE INTERESES

No existe conflicto de intereses entre los autores, ni con ninguna institución a la que cada uno está afiliado, ni con ninguna otra institución.
Las opiniones expresadas aquí son únicamente responsabilidad de los autores y no representan la posición de la Institución o las instituciones a las que están afiliados.

CONTRIBUCIONES DE LOS AUTORES

Damián Ernesto Rodríguez Trujillo: Conceptualización de la investigación, diseño del *SIGCLAN*, elección de los *softwares* para la programación y la validación de los resultados. Redacción del borrador original y aceptación de sugerencias para la conformación de la versión final. Revisión de la versión final a presentar.

Caridad E. Anías Calderón: Aportes significativos en la conceptualización de la investigación. Contribución a la idea y organización del artículo. Revisión crítica de cada una de las versiones del borrador y la versión final del artículo a publicar.

Liz Gámez Picó: Contribución a la redacción del documento y revisión crítica de la versión final del artículo.

AUTORES

Damián Ernesto Rodríguez Trujillo, Ingeniero en Telecomunicaciones y Electrónica, Universidad Tecnológica de La Habana CUJAE, La Habana, Cuba E-mail: damiane.rt98@gmail.com ORCID: https://orcid.org/0000-0002-9375-149X. Intereses de investigación: Gestión de redes y servicios.

Caridad E. Anías Calderón, Ingeniera en Telecomunicaciones, Máster en Telemática, Doctora en Ciencias Técnicas, Universidad Tecnológica de La Habana CUJAE, La Habana, Cuba E-mail: cacha@tesla.cujae.edu.cu ORCID: https://orcid.org/0000-0002-5781-6938. Intereses de investigación: redes de telecomunicaciones y gestión de redes y servicios.

Liz Gámez Picó, Ingeniera en Telecomunicaciones, Máster en Telecomunicaciones y Telemática, Universidad Tecnológica de La Habana CUJAE, La Habana, Cuba E-mail: lizgpico@gmail.com ORCID: https://orcid.org/0000-0003-2992-2060. Intereses de investigación: redes de telecomunicaciones y gestión de redes y servicios.