ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA / TECNOLOGÍAS DE LA INFORMACIÓN

ANÁLISIS DE METODOLOGÍAS PARA LA AUTOMATIZACIÓN DE REDES PARA EoT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

JOSÉ ANDRÉS SANDOVAL RIVERA
jose.sandoval02@epn.edu.ec

DIRECTOR: CARLOS ROBERTO EGAS ACOSTA
carlos.egas@epn.edu.ec

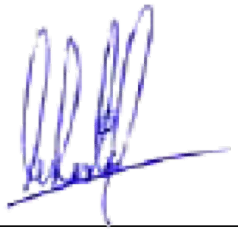
DMQ, Abril 2023

CERTIFICACIONES

Yo, José Andrés Sandoval Rivera declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

José Andrés Sandoval Rivera

Certifico que el presente trabajo de integración curricular fue desarrollado por José Andrés Sandoval Rivera, bajo mi supervisión.



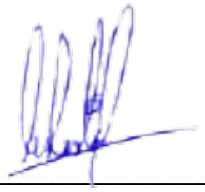
Dra. Carlos Roberto Egas Acosta

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JOSÉ ANDRÉS SANDOVAL RIVERA



CARLOS ROBERTO EGAS ACOSTA

AGRADECIMIENTO

Brindo Agradezco a mi madre por darnos todo lo necesario, a mi hermana y a mí, siendo ella quien supo criar y cuidar a sus dos hijos sin ayuda de nadie, tuvo que ser firme con nosotros pero todo con el fin de vernos llegar lejos, nunca nos faltó nada y gracias a ella he podido llegar a esta etapa de mi vida, agradezco a mi hermana por siempre confiar en mí, por apoyarme y cuidarme pese a tener peleas, siempre hemos cuidado el uno del otro y agradezco mucho a la vida haberme dado una madre y hermana como ellas, agradezco a Paola Zamora, una de las mujeres más importantes en mi vida quien me ayudo a crecer de forma profesional y personal, haciéndome una mejor persona.

José Andrés Sandoval Rivera

ÍNDICE DE CONTENIDOS

RESUMEN

El presente Trabajo de Integración estudia y analiza las metodologías de la automatización de redes, al momento existen varias formas de automatización cada una con sus respectivas especificaciones, el presente documento tiene como fin de inferir el mejor uso para la aplicación en el Internet de Todas las Cosas.

En el primer capítulo se mencionan las principales metodologías de la automatización de redes en dicho capitulo destacan la automatización por equipos, script y software también se cuenta con dos ejemplos de cada una de las metodologías para un mejor entendimiento de estas, aquí también se señala las redes SDN y las redes basadas en la intención, demostrando que el usuario tiene varias opciones de automatización.

A lo largo del segundo capítulo se compara los dos ejemplos dados en el capítulo anterior de cada metodología, esto nos permite obtener características comunes de cada metodología ya que los representantes de su metodología comparten características similares y todas las metodologías comparten características comunes.

Finalmente, se describe las características generales de una automatización optima, además, también se señala las características específicas de cada metodología y las deficiencias esto permite al lector inferir que metodología es la óptima para un cada especifico de automatización.

PALABRAS CLAVE: Automatización, Programación, PnP, Software, EoT, SDN, redes basadas en la intención.

ABSTRACT

This Curricular Integration Peper studies and analyzes the network automation methodologies, now there are several forms of automation each with their respective specifications, the purpose of this document is to infer the best use for the application in internet of everything.

In the first chapter the main methodologies of network automation are mentioned, in said chapter automation by equipment, script and software stand out, there are also two examples of each of the methodologies for a better understanding of these, here the SDN networks and intent-based networks, demonstrating that the user has several automation options.

Throughout the second chapter, the two examples given in the previous chapter of each methodology are compared, this allows us to obtain common characteristics of each methodology since the representatives of their methodology share similar characteristics and all the methodologies share common characteristics.

Finally, the general characteristics of an optimal automation are described, in addition, the specific characteristics of each methodology and the deficiencies are also indicated, this allows the reader to infer which methodology is optimal for each specific automation.

KEYWORDS: Automation, PnP, Software, EoT, SDN, Intent-Based Networking.

1 INTRODUCCIÓN

El desarrollo de la tecnología ha ayudado al ser humano reduciendo tareas y minimizando el esfuerzo requerido para las mismas, de los grandes logros para la tecnología ha sido las telecomunicaciones y redes de información, desde el primer teléfono pasando por la creación de internet e incluso llegando a comunicaciones satelitales, las redes de información son parte fundamental del desarrollo humano y la integración de más dispositivos y personas a la red ha generado que se desarrollé más tecnologías y estudios enfocamos a las redes y sobre todo a la automatización de tareas, comenzamos con el internet de las cosas ahora hablamos del internet de todo, el cual integra la conexión inteligente de personas, procesos, datos y cosas, y para su automatización disponemos de varias opciones proporcionados por varios proveedores pero que se pueden agrupar en tres grandes ramas, cada una de esas ramas puede desarrollarse ampliamente, sin embargo, se analizara sus principales características, deficiencias y limitantes para su aplicabilidad.

1.1 OBJETIVO GENERAL

Investigar formas de automatizar las redes, agrupar dichas formas de automatización en principales metodologías y analizar las metodologías existentes para la automatización de redes en el internet de todo y definir sus principales características, ventajas, desventajas y aplicabilidad.

1.2 OBJETIVOS ESPECÍFICOS

1. Investigar sobre el estado actual de la automatización para redes EoT, en base a los principales proveedores en materia de redes de información.
2. Investigar las metodologías de automatización de Redes de Datos, definir las metodologías en base a las soluciones proporcionadas por varios proveedores.
3. Analizar comparativamente las metodologías para la automatización de Redes, destacando principalmente sus características, ventajas y deficiencias.
4. Analizar la aplicabilidad de las metodologías en redes, en base a sus principales limitantes.

1.3 ALCANCE

El Grupo de Investigación del Internet de Todas la Cosas (EoT) del DETRI, tiene como objetivos el desarrollo de tecnologías para la automatización de redes en el Internet de Todas las Cosas, del cual forma parte el Internet de las Cosas (IoT). Dentro de las tecnologías utilizadas en la actualidad, está la automatización de las redes. La automatización de la red se está convirtiendo en una necesidad en el campo de las Tecnologías de la información a nivel del Ecuador aplicadas al Internet de Todas las cosas, por lo cual es un tema relevante para la carrera de ingeniería en TI de la EPN. Hay cientos de tareas monótonas diarias que se pueden automatizar, desde implementaciones de red, donde los interesados son los estudiantes de la carrera de Tecnología Superior en Redes y Telecomunicación, administración, orquestación de aplicaciones, tema de importancia para los estudiantes de Tecnología Superior en Desarrollo de Software e ingeniería en software, seguridades hasta el monitoreo. Es evidente que, en las certificaciones de redes ofrecidas por las más importantes compañías relacionadas con la fabricación de equipos para redes de datos, se están redirigiendo hacia la automatización las redes lo que valida la necesidad de que los estudiantes tengan conocimientos más profundos de la automatización de las redes y puedan desenvolverse adecuadamente en el ámbito profesional y para obtener esto los docentes de la EPN deben estar preparados y capacitados. La automatización de redes Internet de las Cosas, es un reto en la actualidad, especialmente en los casos en donde estas redes utilizan nodos que operan a baterías y tienen limitaciones de cómputo. En el presente proyecto se pretende entender los conceptos de la automatización de redes para su aplicación al Internet de Todas las Cosas, y preparar al estudiante para afrontar las necesidades de automatización de las redes, para lo cual es necesario estudiar tecnologías aplicadas a la automatización de redes y cómo pueden ser utilizadas en redes Internet de las Cosas.

A. Fase Teórica

Estudiar la automatización de Redes, se recolectará información sobre la automatización de redes, se leerá el contenido, se inferirá que fuentes son confiables, de preferencia archivos IEEE, sin embargo, cualquier información al respecto ayudará a esclarecer la automatización.

Estudiar la programabilidad de Redes, se investigará que lenguajes de programación son mejores para la programabilidad, se analizará el contenido relacionado al tema, y se desarrollará un resumen de este.

B. Fase de Planteamiento

Estudiar la automatización de Redes, se recolectará información sobre la automatización de redes, se leerá el contenido, se inferirá que fuentes son confiables, de preferencia archivos IEEE, sin embargo, cualquier información al respecto ayudará a esclarecer la automatización.

Estudiar la programabilidad de Redes, se investigará que lenguajes de programación son mejores para la programabilidad, se analizará el contenido relacionado al tema, y se desarrollará un resumen de este.

Investigar sobre el estado actual de la automatización para redes Internet de las Cosas, se investigará información relevante del estado actual de Internet de las Cosas, para proseguir con el estado actual de la automatización y su relación entre las Internet de las Cosas.

Investigar las metodologías de automatización de Redes de Datos, en una primera fase de investigación se encontró relevancia entre 3 metodologías de la automatización de redes las mismas que se mencionaron en la sección de descripción del componente y se desarrollaran las mismas.

C. Fase de Implementación

Analizar comparativamente las metodologías para la automatización de Redes, entre las que están la automatización por equipos, programa de automatización y script de programación para la automatización.

D. Fase de Evaluación

Analizar la aplicabilidad de las metodologías en redes, se analizará una a una las tres metodologías encontradas, de encontrar otra metodología a parte de las 3 se analizará del mismo modo.

Se indicará que metodología es mejor, la misma que se recomendará para su aplicabilidad en redes y la enseñanza de esta.

1.4 MARCO TEÓRICO

En el **Apartado 1.4.1,** se analiza el estado actual de la automatización de redes. En el Apartado 1.4.2, se señala lo correspondiente al Internet de todas las cosas. Continuando

con el Apartado 1.4.3 que describe la automatización en el ámbito de las redes, en los Apartados siguientes se señalan las metodologías.

1.4.1 ESTADO ACTUAL DE LAS METODOLOGÍAS DE AUTOMATIZACIÓN DE REDES APLICADAS AL INTERNET DE LAS COSAS

El Informe sobre el estado de la automatización de redes, SoNAR, State of Network Automation Report, por sus siglas en inglés, tiene como objetivo proporcionar información sobre el viaje general hacia la automatización, comprender cómo y cuándo las empresas están adoptando este camino, Los resultados muestran que los tres segmentos de proveedores de servicios de comunicaciones, proveedores de la nube y empresas se encuentran en diferentes etapas de madurez de automatización. Mientras que aproximadamente una cuarta parte de cada segmento está comenzando a automatizarse más allá de la CLI con secuencias de comandos básicas, lo que en sí mismo muestra que la automatización de la red es una tendencia duradera. Un 24 % de los proveedores de la nube dicen que usan la automatización en la producción en todos los lugares de la red, aunque casi el 40 % son bastante nuevos en la automatización y la han estado usando durante menos de 3 años.

En 2019, el impulsor tecnológico más común fue la mejora de la seguridad, pero para el 2020 todos los segmentos indican que el principal impulsor para automatizar es reducir el trabajo duro y repetitivo (esfuerzo) A partir de ahí, los segmentos clasifican los impulsores tecnológicos de manera muy diferente. Ambos tipos de proveedores de servicios dicen que escalar la eficiencia operativa de la red es el segundo impulsor tecnológico más importante En cuanto a los desafíos relacionados con la automatización, al igual que en 2019, el mayor desafío para todos los segmentos es la falta de tiempo para aprender en el trabajo. Pero a partir de ahí, cada segmento clasifica los desafíos de manera diferente. Con un 61 %, los proveedores de la nube informan que el miedo a cometer un error en la producción es igualmente desafiante, lo que pasa a ocupar el segundo lugar entre los profesionales de redes empresariales mientras tanto, los proveedores de servicios de comunicaciones se enfrentan a diferentes desafíos con la automatización. El 64 % no tiene los conocimientos necesarios para acceder a la capacitación y casi la misma cantidad: el 64 % dice que los equipos de red más antiguos dificultan la automatización.

Después de ver por qué estos tres tipos de usuarios de la red automatizan las operaciones de la red y sus desafíos, la conclusión es ineludible son muy diferentes. Es por eso por lo que se analiza los resultados relacionados con las operaciones de red por separado para empresas, proveedores de servicios de comunicaciones y proveedores de la nube.[8].

1.4.2 INTERNET DE TODAS LAS COSAS

El Internet de Todas las Cosas amplía el concepto del Internet de las Cosas (IoT) las cuales se basan en las comunicaciones de una máquina a otra máquina (M2M) con el fin de describir un sistema con mayor grado de complejidad que además engloba personas y procesos.

Cisco dio origen al concepto de Internet de todo, quien propone como definición Internet de Todas las Cosas como "la conexión inteligente de personas, procesos, datos y cosas". Esto se debe a que, en el Internet de las cosas, las comunicaciones se establecen entre máquinas, IoT y M2M, se las puede considerar como sinónimos. El concepto de internet de todo más extenso integra, las comunicaciones entre maquina a máquina, interacciones de máquina a persona conocidas como M2P y comunicaciones de persona a persona apoyada por tecnología desarrollada en telecomunicaciones, dicha relación se la conoce como P2P.

El Internet de las cosas incluye todo tipo de objeto o entidad física o virtual la cual tenga la propiedad de ser direccionable y con la factibilidad de transmitir datos sin intervención de una persona a máquina. El internet de todo adiciona lo mencionado y también incluye todo el campo de las comunicaciones e interacciones implementadas por el usuario y asociadas en su totalidad con los dispositivos en red.[1].

El Internet de las cosas es un término utilizado para describir la conexión de dispositivos electrónicos comunes a Internet. Esto permite que estos dispositivos se comuniquen entre sí y con otros dispositivos y sistemas a través de una red global. El Internet de las cosas se ha convertido en una tecnología cada vez más importante en nuestra sociedad moderna, ya que permite la automatización de procesos y la recopilación de datos en una variedad de campos, desde la industria hasta el hogar.

La relación entre el Internet de las cosas y el Internet de Todo se basa en la conectividad. El Internet de Todas las Cosas se refiere a la conexión de todas las cosas, incluyendo personas, procesos, datos y dispositivos, a través de Internet. Esto permite una mayor interconexión y comunicación entre diferentes sistemas y dispositivos, lo que a su vez permite una mayor eficiencia y automatización en una variedad de campos.

El IoT es una parte importante del Internet de Todas las Cosas y en la actualidad los dos términos se utilizan de manera similar y para las mismas aplicaciones, ya que proporciona la conectividad física entre los dispositivos y la red global. Al conectar dispositivos como sensores, dispositivos de control y electrodomésticos a Internet, se pueden recopilar y analizar datos en tiempo real, lo que permite una mayor comprensión de los procesos y

una mayor capacidad para automatizarlos. Esto tiene un gran impacto en campos como la industria, la salud, el transporte y el hogar.

Sin embargo, a medida que se conectan más dispositivos a Internet, también se plantean preocupaciones sobre la privacidad y la seguridad. Con la recopilación de datos masiva, existe el riesgo de que los datos personales sean vulnerables a ataques y violaciones de privacidad. Además, al conectar dispositivos críticos, como sistemas de control de infraestructura, a Internet, existe el riesgo de que los ataques cibernéticos puedan tener consecuencias graves. Es importante que se desarrollen medidas de seguridad adecuadas para proteger los datos y los sistemas conectados.

1.4.3 AUTOMATIZACIÓN DE REDES

La automatización es el proceso donde una o varias tareas se repiten un número indefinido de veces, para comenzar ese proceso se debe definir una orden de inicio y dependiendo del requerimiento se debe dar una orden de fin o a su vez tener un método para detener el proceso, gracias al avance tecnológico varios sistemas o procedimientos pueden ser automatizados, optimizando tareas, reduciendo tiempos de ejecución minimizando recursos laborales.

Las redes nacen como la conexión entre dos dispositivos, en un principio teléfonos, mediante un cable de cobre, ubicados a cierta distancia con el fin de comunicar 2 personas, hoy en día las redes no abarcan solo la conexión de dos teléfonos y menos aún entre un cable de cobre, actualmente se dispone de computadores, celulares, tabletas, relojes que se conectan entre cables de cobre, fibra, red inalámbrica, nos enfrentamos a un mundo donde todo está conectado y la administración de dichas conexiones de vuelven más complejas.

El propósito de automatizar las redes se basa en reducir la complejidad que administrar una red conlleva, hacer que las tareas repetitivas no las haga el usuario de las redes, que independientemente del dispositivo conectado funcione correctamente sin la necesidad de realizar algún cambio al dispositivo o a la red, ya hay procesos en redes que se han automatizado, un ejemplo del mismo son los servidores DHCP, los cuales asignan una IP al usuario de la red, ese proceso es trasparente para el usuario y es uno de las tareas más básicas para una conexión en la red, entre los principales beneficios de la automatización de redes destacan las siguientes:

- Reducción de la cantidad de problemas.
- Costos más bajos.
- Mayor resistencia de red.

- Reducción del tiempo de inactividad de la red.
- Aumento de la fuerza de trabajo estratégica.
- Mejor perspectiva y control de la red.[2]

1.4.4 METODOLOGÍAS PARA LA AUTOMATIZACIÓN

Podemos separar la automatización de redes en tres grandes metodologías, cada uno de ellos con sus ventajas y desventajas, la primera y una de las más conocidas es mediante equipos de red, seguida de la metodología mediante scripts, la cual es más utilizada por quienes tienen un amplio conocimiento en lenguajes de programación y por último la metodología mediante software, para las siguientes secciones se describe con mayor desglose cada una de ellas para un mejor entendimiento de estas.

1.4.4.1 Automatización Mediante Equipos

Para esta sección se toma de ejemplo dos grandes empresas en la fabricación de equipos de red, Cisco y Juniper, los cuales cuentan con un amplio desarrollo es la industria, Cisco con aproximadamente 37 años en el mercado y Juniper con un aproximado de 26 años al momento del desarrollo del presente documento, ambas empresas reconocidas a nivel mundial.

Junos Space es una solución integral de gestión de redes que ayuda a simplificar con la automatización de la gestión de los dispositivos de conmutación (switch), enrutamiento (router) y seguridad como firewall de Juniper. Junos Space consta de una plataforma de gestión de red para la gestión de elementos profundos y FCAPS, aplicaciones de gestión plug-and-play para reducir costos y aprovisionar nuevos servicios rápidamente, y un SDK programable para la personalización de la red. Con cada uno de estos componentes funcionando de forma coherente, Junos Space ofrece una solución unificada de orquestación y administración de red para ayudarlo a administrar de manera más eficiente la nueva red.[3]

Cisco desarrolló DNA Center, la cual es un dispositivo físico en 3 presentaciones integrados con una solución de software. La solución recibe datos en forma de transmisión de telemetría proveniente de cada dispositivo (switch, router, Access Point y dispositivo WiFi) en la red. Los datos brindan a Cisco DNA Center información en tiempo real para todas las funcionalidades que realiza para la automatización de redes.[4].

1.4.4.2 Automatización Mediante Scripts

La automatización de redes mediante scripts es una técnica que consiste en utilizar lenguajes de programación para automatizar tareas y procesos relacionados con las redes. Los scripts son un conjunto de comandos que se ejecutan en secuencia para llevar a cabo una tarea específica, como la configuración de dispositivos de red, la monitorización de estado de red, o la gestión de políticas de seguridad.

La automatización de redes mediante scripts tiene varios beneficios. En primer lugar, permite una mayor eficiencia en la administración de redes, ya que los scripts pueden ser utilizados para automatizar tareas que de otra manera serían tediosas o repetitivas de realizar manualmente. Además, los scripts pueden ser programados para realizar tareas específicas de manera precisa y sin cometer errores humanos.

En segundo lugar, la automatización de redes mediante scripts también ayuda a mejorar la seguridad de las redes. Los scripts pueden ser utilizados para automatizar la configuración de seguridad de los dispositivos de red y para implementar políticas de seguridad de manera automática. Esto ayuda a proteger las redes contra ataques y violaciones de seguridad.

Además, la automatización de redes mediante scripts también ayuda a mejorar la escalabilidad y flexibilidad de las redes. Los scripts pueden ser utilizados para automatizar la configuración y el despliegue de dispositivos de red, lo que permite una mayor escalabilidad y flexibilidad en la gestión de las redes.

Sin embargo, existen algunos desafíos asociados con la automatización de redes mediante scripts. Uno de ellos es la complejidad, ya que escribir un script puede ser un desafío para aquellos sin experiencia en programación o en redes. Además, los scripts también pueden ser vulnerables a errores y ataques cibernéticos si no se escriben y se mantienen de manera adecuada.

Python destaca como el principal lenguaje de programación para la automatización de redes y existen varias librerías con la funcionalidad básica o inicial para dicho propósito entre ellas esta Paramiko, Netmiko NAPALM. En principio las bibliotecas de código abierto están diseñadas para simplificar la administración de SSH, se ocupa principalmente de recopilar resultados de los comandos show y de realizar cambios de configuración, tiene como objetivo lograr ambas operaciones y hacerlo en un conjunto muy amplio de plataformas de red de varios proveedores, incluidos Cisco, Arista y Juniper Networks.

Entrando en un ámbito de simulación se encuentra Mininet, quien permite simular redes SDN, tanto con una interfaz gráfica como con programación en Python.[5].

1.4.4.3 Automatización Mediante Scripts

La automatización de redes mediante software es una técnica que consiste en utilizar programas especializados para automatizar tareas y procesos relacionados con las redes. Estos programas, conocidos como software de automatización de redes, ofrecen una interfaz gráfica de usuario (GUI) o una interfaz de línea de comandos (CLI) para configurar y controlar dispositivos de red, monitorear el estado de la red, y automatizar la implementación de políticas de seguridad.

La automatización de redes mediante software tiene varios beneficios. En primer lugar, permite una mayor eficiencia en la administración de redes, ya que los administradores de redes pueden automatizar tareas repetitivas y tediosas mediante el uso de software especializado. Esto libera tiempo para que los administradores se enfoquen en tareas más críticas, como el desarrollo y la seguridad.

En segundo lugar, la automatización de redes mediante software ayuda a mejorar la seguridad de las redes. Los programas de automatización de redes pueden ser configurados para implementar políticas de seguridad automáticamente y monitorear el estado de la red para detectar posibles amenazas. Esto ayuda a proteger las redes contra ataques y violaciones de seguridad.

Además, la automatización de redes mediante software también ayuda a mejorar la escalabilidad y flexibilidad de las redes. Los programas de automatización de redes pueden ser utilizados para automatizar la configuración y el despliegue de dispositivos de red, lo que permite una mayor escalabilidad y flexibilidad en la gestión de las redes.

Sin embargo, existen algunos desafíos asociados con la automatización de redes mediante software. Uno de ellos es el costo, ya que el software de automatización de redes puede ser costoso. Además, la implementación y el uso de software de automatización de redes requieren un cierto nivel de conocimiento técnico y experiencia en redes.

Como un ejemplo de la automatización esta los equipos “plug and play”, PnP, que se puede entender como “Conectar y usar”, el más básico de dichos equipos son las flash memory, las cuales al ser conectadas se pueden usar para almacenar información sin una previa acción por parte del usuario, sin embargo, para que dichos dispositivos puedan ser usados debe haber una previa estandarización y configuración de parte de los fabricantes, tanto del computador como del fabricante de la flash memory, en redes pasa algo similar, se puede adquirir equipos los cuales no tengas o tengan poca intervención de configuración para su uso, lo que se considera como un inicio en la automatización.

Configuración plug and play de Cisco, en sus routers serie RV34x, En el entorno Small Business se integró la compatibilidad Plug and Play con FindIT, la cual actúa como un servidor Plug and Play. PnP ayuda a simplificar significativamente la implementación de

imágenes o configuraciones de los dispositivos de red cada que un dispositivo se integra a la red, esto es conocido como implementación de configuración sin intervención o con poca intervención.[6]

2 METODOLOGÍA

En el presente Capítulo se detalla las metodologías de automatización existentes y destacas en los últimos años, cada uno con 2 ejemplos para su aplicabilidad en un ambiente real.

2.1 ANALISIS

En la presente sección de detalla las tres principales metodologías para la automatización de redes, con productos existentes en el mercado, comenzando con la metodología por equipos, mediante Cisco PnP y Junos Space, se analiza la automatización mediante scripts, entre Netmiko y Paramiko, terminando con automatización por software con Cisco DNA.

Se omite como pasos para la automatización de redes el análisis de escalabilidad de la red, ya que es un paso fundamental y prioritario para cualquier aplicación de redes de telecomunicación.

2.1.1 AUTOMATIZACIÓN POR EQUIPOS

Para aplicar una automatización por equipo es necesario tener en cuenta la limitación física que puede presentar el equipo y las consideraciones a tomar para su aplicabilidad, entre dichas limitaciones se encuentra:

A. Número de puertos

Si bien en el mercado existen varias opciones de equipos con diversos números de puertos, como principales características a tomar en cuenta son los medios de trasmisión, por fibra o cable de cobre, y que equipos son compatibles con la automatización acompañado de un análisis de la escalabilidad que la empresa, cliente o usuario tendrá con el trascurso de los años.

B. Velocidad

Ligado con el número de puertos y sobre todo por el medio de trasmisión, si bien la fibra óptica ha tenido un amplio despliegue, los dispositivos finales estas conectados de forma inalámbrica o por cable UTP.

C. Versión

No todas las versiones de firmware o sistema operativo que maneje el proveedor de equipos son compatibles con otros proveedores o incluso con sus respectivas soluciones de automatización.
para un mejor análisis se tomará en cuenta 2 soluciones en automatización por equipos.

2.1.1.1 JUNIPER JUNOS SPACE

Es la plataforma centralizada desarrollada para la orquestación y la administración de dispositivos y servicios de red a través de un único panel de cristal.
Ofrece un modelo de red abstracto que se puede extender a terceros a través de una API RESTful con varias funciones. Los usuarios pueden acceder a sus capacidades a través de una interfaz gráfica de usuario Web 2.0 que utiliza flujos de trabajo basados en humanos y divulgación incremental para brindar visibilidad y control específicos del alcance y centrados en el operador.[9], en la Figura 2.1. se muestra el equipo Juniper JA2500

Figura 2. 1. Equipo Juniper JA2500

Para su implementación en necesario seguir las siguientes indicaciones:

A. Requisitos Básicos de Implementación

Cada dispositivo de la estructura utiliza la interfaz eth0 para todas las comunicaciones entre nodos dentro de la estructura. En cada dispositivo, puede elegir usar una interfaz separada (eth3) para todas las comunicaciones entre el dispositivo y los dispositivos administrados, como se muestra en la **Figura 2.1.**

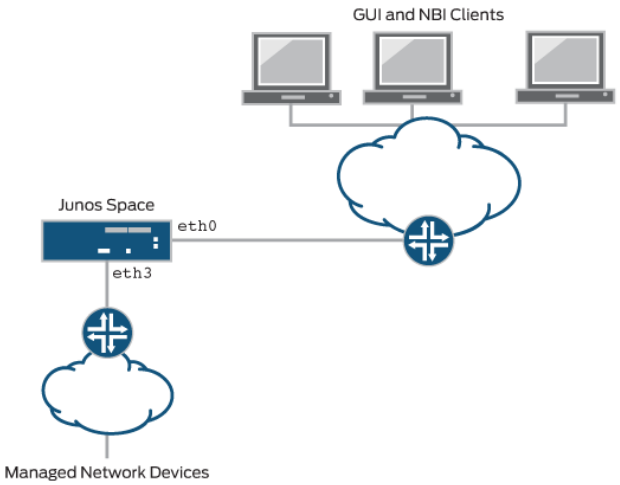


Figura 2. 2. Uso de Dos Interfaces Ethernet para toda la Conectividad IP

Se requiere lo siguiente cuando implementa un tejido de Junos Space:

- Conectividad o prueba de ping a la dirección IP de la puerta de enlace predeterminada.
- Las direcciones IP asignadas a la interfaz eth0 en los dos primeros dispositivos de la estructura deben estar en la misma subred.
- La dirección IP virtual configurada en el primer dispositivo de la estructura debe estar en la misma subred que la interfaz eth0 en los dos primeros dispositivos.
- Los paquetes de multidifusión deben poder enrutarse entre todos los nodos.
- Todos los dispositivos de la estructura deben usar la misma fuente NTP externa para garantizar una configuración de hora uniforme en todos los dispositivos de la estructura. Debe especificar la fuente NTP en cada dispositivo antes de agregar el dispositivo a la estructura.
- Todos los nodos del tejido ejecutan la misma versión del software

B. Configuración de Conectividad de Red para Junos Space

Un dispositivo Junos Space dispone de cuatro interfaces Ethernet RJ45 10/100/1000 que se denominan eth0, eth1, eth2 y eth3, como se muestra en la **Figura 2.1.** Al implementar el dispositivo, se debe asegurar que tenga conectividad IP con lo siguiente:

- Dispositivos en su red administrada.
- Equipos de escritorio, portátiles y estaciones de trabajo desde los que los usuarios de Junos Space acceden a la interfaz de usuario de Junos Space, así como a sistemas externos que alojan clientes de northbound interface, NBI por sus siglas en inglés.
- Otros dispositivos que forman un tejido Junos Space junto con este dispositivo.

Junos Space le permite utilizar dos de las cuatro interfaces Ethernet: eth0 y eth3. Las otras dos interfaces Ethernet están reservadas para uso futuro.

El escalamiento es un factor importante que considerar al automatizar redes porque puede afectar la eficiencia y la capacidad de la red a medida que crece. La automatización de redes puede ayudar a facilitar el escalamiento, ya que permite una configuración uniforme y consistente de los dispositivos de red, lo que a su vez puede mejorar la escalabilidad y la flexibilidad de la red.

Sin embargo, es importante considerar el escalamiento al planificar y diseñar la automatización de redes. Por ejemplo, es posible que sea necesario ajustar la infraestructura de la red para manejar el tráfico adicional generado por un aumento en el número de dispositivos y usuarios. También es importante asegurarse de que las herramientas y tecnologías utilizadas para la automatización sean escalables y puedan adaptarse a una red en constante crecimiento.

Además, es importante considerar el escalamiento al monitorear la red. La automatización puede ayudar a detectar y solucionar problemas de rendimiento antes de que afecten negativamente a los usuarios, pero es importante asegurarse de que los procesos de monitoreo sean escalables y puedan manejar un aumento en la cantidad de datos y dispositivos.

Permite elegir una de las siguientes opciones para configurar interfaces para conectividad IP:

- Utilizar la interfaz eth0 para toda la conectividad de red del dispositivo, como se muestra en la **Figura 2.3.**

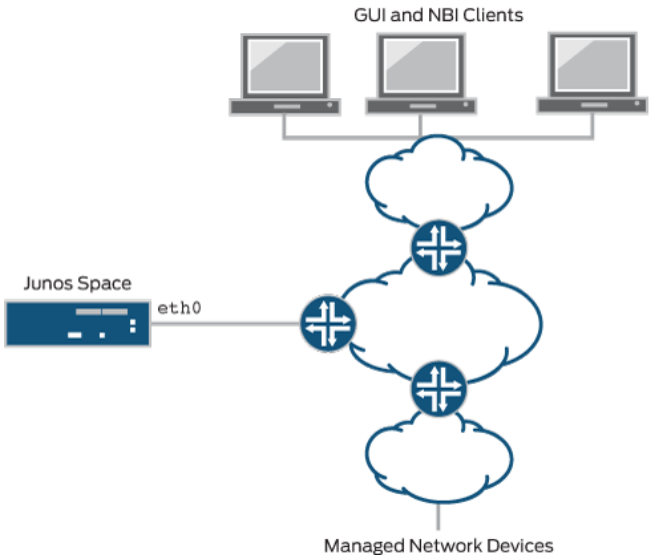


Figura 2. 3 uso de una sola interfaz Ethernet para toda la conectividad IP

- Utilizar la interfaz eth0 para la conectividad de red con los clientes de la interfaz de usuario de Junos Space y otros dispositivos en la misma estructura, y use la interfaz eth3 para la conectividad de red con dispositivos administrados, como se muestra en la **Figura 2.2.**

C. Adición de nodos a Junos Space

Se debe tener asignada la función de usuario Administrador del sistema para poder agregar nodos a una estructura de Junos Space. Los nodos se agregan a una estructura de Junos Space desde la página Agregar nodo de estructura (Plataforma de administración de red > Administración > Estructura > Agregar nodo de estructura). Para agregar un nodo a una estructura, especifique la dirección IP asignada a la interfaz eth0 del nuevo nodo, un nombre para el nuevo nodo y (opcionalmente) una fecha y hora programadas para agregar el nodo a la estructura. El software Junos Space maneja automáticamente todos los cambios de configuración necesarios para agregar el nodo a la estructura. Después de agregar el nuevo nodo al tejido, puede monitorear el estado del nodo desde la página Tejido (Plataforma de administración de red > Administración > Tejido).[10]

2.1.1.2 CISCO DIGITAL NETWORK ARCHITECTURE (DNA)

Cisco DNA Center es una solución de software que reside en el dispositivo Cisco DNA Center. La arquitectura de red digital de Cisco es una arquitectura abierta, extensible e impulsada por software que acelera y simplifica las operaciones de red, al mismo tiempo que reduce los costos y el riesgo. Proporciona una estructura de red única que funciona con inteligencia profunda y seguridad integrada para brindar automatización y seguridad en toda su organización a escala. Cisco DNA Automation and Assurance se basa en un controlador de redes definidas por SDN.[11]

Cisco DNA Center está respaldada por tres dispositivos de hardware diferentes como los que se muestran en la **Figura 2.4.**

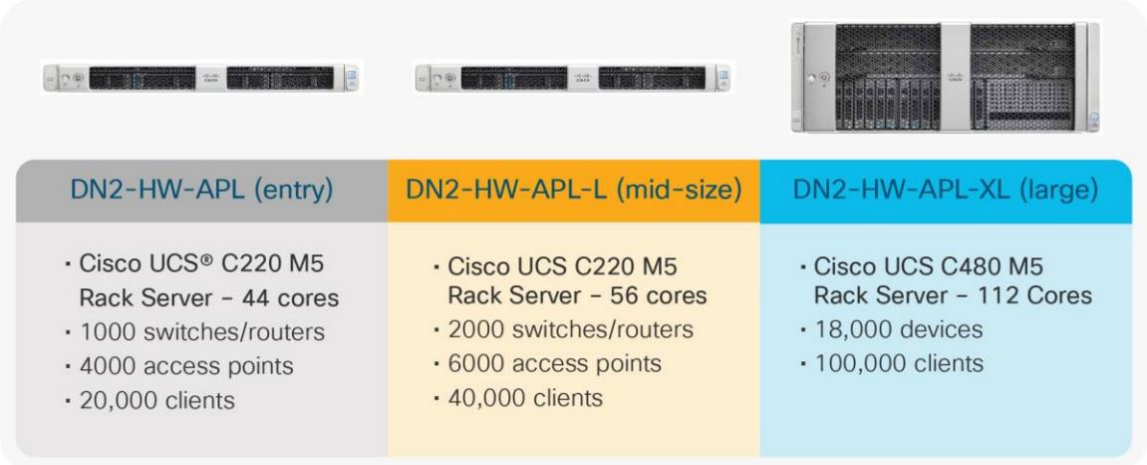


Figura 2. 4. Equipos para Cisco DNA

Para su implementación se debe realizar los siguientes pasos:

A. Planificar la Implementación

Tabla 2. 1. Flujo de Trabajo para Planificación

Acción	Flujo de trabajo de planificación
Descripción	
Antes de instalar y configurar el dispositivo Cisco DNA Center, se debe seguir los siguientes pasos de planificación y adquirir la información necesaria de la red a implementar, al finalizar los pasos se procede a la instalación física del dispositivo.	
Pasos complementarios	
Revisar los requerimientos de cableado estructurado y conmutación recomendados para los dos tipos de instalación que proporciona el dispositivo, independiente y de clúster. Reunir el direccionamiento IP, las subredes y toda la información pertinente al tráfico IP, la cual será configurada en el dispositivo. Disponer de una solución específica para proporcionar acceso a los recursos basados en la web. Para el tráfico de Cisco DNA, se requiere reconfigurar las políticas y los firewalls de seguridad.	

Tabla 2. 2. Conexiones de cable para Interfaz

Acción	Conexiones de cable de interfaz
Descripción	
Para la funcionalidad de Cisco DNA se debe conectar los puertos a un switch que proporcione acceso a la red. El mínimo requerimiento necesario es configurar las interfaces de puerto Enterprise e Intracluster.	

Tabla 2. 3. Direcciones IP y Subredes Requeridas

Acción	Direcciones IP y subredes requeridas
Descripción	
Cada puerto por utilizar se le debe asignar una dirección IP por lo cual, es necesario asegurar que la red disponga de suficientes direcciones IP. Dependiendo de si está instalando el dispositivo como un clúster de un solo nodo, como un nodo principal o secundario.	

URL de Internet requeridas y nombres de dominio calificados: Para seguridad del usuario, las direcciones URL requieren acceso seguro y nombres de dominio completos (FQDN).

Tabla 2. 4. Puertos de Red Requeridos

Acción	Puertos de red requeridos
Descripción	
Se debe asegurar de que los puertos estén abiertos para los flujos de tráfico hacia y desde el dispositivo, dichos puertos pueden ser abiertos mediante una puerta de enlace o configurando el firewall.[11] Información de configuración requerida: Durante el proceso de configuración, el dispositivo solicitará, además de las direcciones IP y subredes.	
Información Requerida	
Nombre de usuario de Linux. Contraseña de Linux. Semilla de generación de contraseña (opcional). Frase de contraseña del administrador. Contraseña de usuario de Cisco IMC. Dirección IP del nodo principal.	

Tabla 2. 5. Información de Configuración Inicial

Acción	Información de configuración inicial
Descripción	
Al finalizar la configurado los dispositivos, es necesario iniciar sesión en el dispositivo Cisco DNA Center y completar los pasos de configuración fundamentales.	
Información Requerida	
Contraseña nueva para el superusuario administrador Credenciales de Cisco.com Credenciales de la cuenta inteligente de Cisco Credenciales y URL del administrador de direcciones IP URL, puerto y credenciales del proxy Usuarios de Cisco DNA Center	

B. Instalar el Dispositivo

Para la instalación del equipo se debe tener en cuenta lo siguiente:

- Revisar las advertencias y pautas de instalación
- Revisar los requisitos del rack
- Conectar y encender el dispositivo
- Comprobar los LED

C. Configuración del Dispositivo Mediante el Asistente Maglev

El dispositivo dispone de dos modos de funcionamiento para su implementación en la red los cuales son:

Standalone, para pruebas y entornos de red no muy amplios, esta opción es preferente también para implementaciones iniciales. Al elegir el presente modo como implementación inicial, el dispositivo permite añadir más dispositivos con el fin de crear un clúster. Al configurar un host independiente, debe ser el primer nodo o nodo principal en el clúster.

Clúster, Como un nodo que pertenece a un clúster de tres nodos. Para el presente modo, entre los host todos los servicios y datos están siendo compartidos. Este modo es preferente en implementación de red amplias. Si se elige el modo de clúster como implementación inicial, es necesario terminar de configurar el nodo principal antes de configurar los nodos secundarios.

2.1.2 AUTOMATIZACIÓN POR SCRIPT

Si bien la automatización por scripts es básica, ya que no cuenta con un análisis para la optimización de la red, cumple con la función de evitar las tareas repetitivas en la parte de gestión y administración de redes, enfocando su desarrollo en la configuración de dispositivos y presentación de comandos básicos en CLI, como el comando show.

La presente metodología cuenta con limitación física, considerando el procesador de equipo, RAM y memoria, y tiene limitaciones de sistema operativo ya que no todas las versiones tienen el mismo rendimiento al momento de ejecutar los scripts.

2.1.2.1 SCRIPTS CON NETMIKO

Es una biblioteca, desarrollada en Python, de múltiples proveedores para simplificar las conexiones CLI a distintos dispositivos de red, tiene como objetivo recopilar resultados de los comandos show y de realizar cambios de configuración esto lo hace en un conjunto muy amplio de plataformas. Busca hacer esto mientras abstrae el control de estado de bajo

nivel (es decir, elimina la coincidencia de patrones de expresiones regulares de bajo nivel en la medida de lo práctico).[12]
Como pasos para la implementación tenemos:

A. Preparación del Entorno

Se requiere de un computador con sistema operativo Ubuntu para su mejor desempeño, la misma debe tener salida a internet para descargar las librerías necesarias para la implementación de Netmiko, se procede a instalar python3 y la librería Netmiko, habilitando en todos los dispositivos la conexión por SSH.

B. Creación de Script

Un Dispositivo: Se importa la librería netmiko, se crea una variable que contendrá un diccionario donde se especifica la información del dispositivo (dirección IP, credenciales SSH). Luego de la conexión al dispositivo, switch o router, se envía el comando «show ip int brief» para imprimirlo en pantalla. Se puede crear una lista de comandos de configuración para enviarla al dispositivo, para crear VLANs se hace uso del bucle for, se puede observar un ejemplo de código en la **Figura 2.5.** con su respectiva ejecución en la **Figura 2.6.**

Figura 2. 5. Ejemplo de script para un dispositivo

Aquí hay algunas ventajas de programar automatización de redes en Python:

Sintaxis fácil de leer y escribir: Python tiene una sintaxis fácil de leer y escribir, lo que facilita el desarrollo de scripts para automatización de redes.

Gran cantidad de bibliotecas: Python tiene una gran cantidad de bibliotecas y módulos disponibles que se pueden utilizar para automatizar tareas en redes. Por ejemplo, la biblioteca Paramiko se puede utilizar para automatizar la conexión SSH a dispositivos de red, mientras que la biblioteca PySNMP se puede utilizar para interactuar con dispositivos SNMP.

Multiplataforma: Python se puede utilizar en una amplia variedad de plataformas, incluyendo Windows, Linux y macOS. Esto lo hace muy conveniente para la automatización de redes en entornos heterogéneos.

Facilidad para realizar pruebas y depuración: Python es un lenguaje interpretado que permite la realización de pruebas y depuración en tiempo real, lo que facilita la identificación de errores y la resolución de problemas.

Amplia comunidad de usuarios y soporte: Python tiene una amplia comunidad de usuarios y un gran soporte en línea, lo que lo hace muy conveniente para obtener ayuda y recursos adicionales para la automatización de redes.

Flexibilidad: Python es un lenguaje de programación flexible que se puede utilizar para desarrollar una amplia variedad de aplicaciones, desde scripts sencillos hasta aplicaciones de gran escala. Esto lo hace muy conveniente para la automatización de redes, ya que se pueden adaptar los scripts a diferentes situaciones y necesidades.

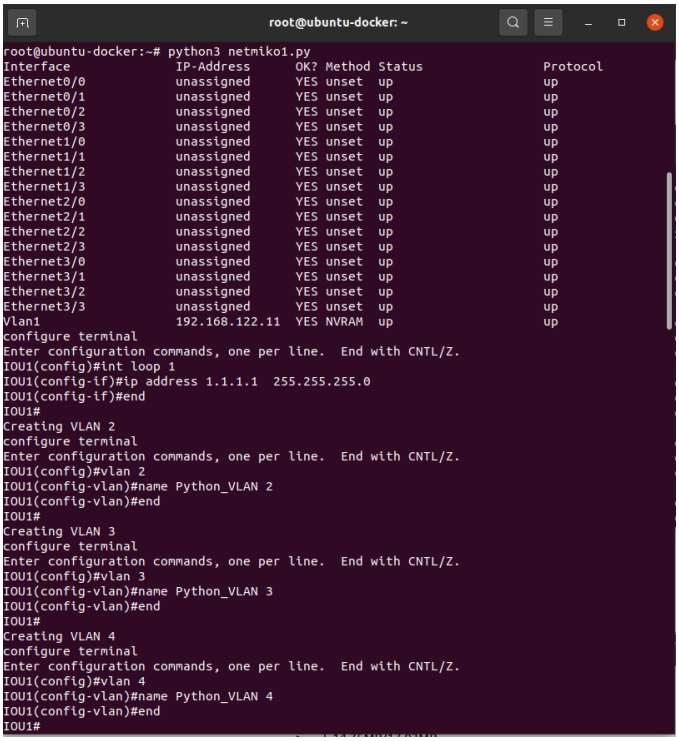


Figura 2. 6. Ejecución del script para un dispositivo

Varios dispositivos: Para varios dispositivos de la topología se puede crear un script, creando las variables que contienen el diccionario con la información de cada dispositivo, se crea una variable donde se especifica una lista de los dispositivos, a los cuales se aplicara el bucle for para crear las vlans, se puede observar un ejemplo de código en la **Figura 2.7.**

Figura 2. 7. Ejemplo de script para varios dispositivos

Variación de Script: Netmiko permite crear un script para abrir un archivo donde se ubica las configuraciones que el usuario o administrador desee, el archivo de configuración se aplicará para cada dispositivo que se defina en el script, se puede observar un ejemplo de script en la **Figura 2.8.** con su respectiva ejecución en la **Figura 2.9.**

Figura 2. 8. Ejemplo de script con modificación

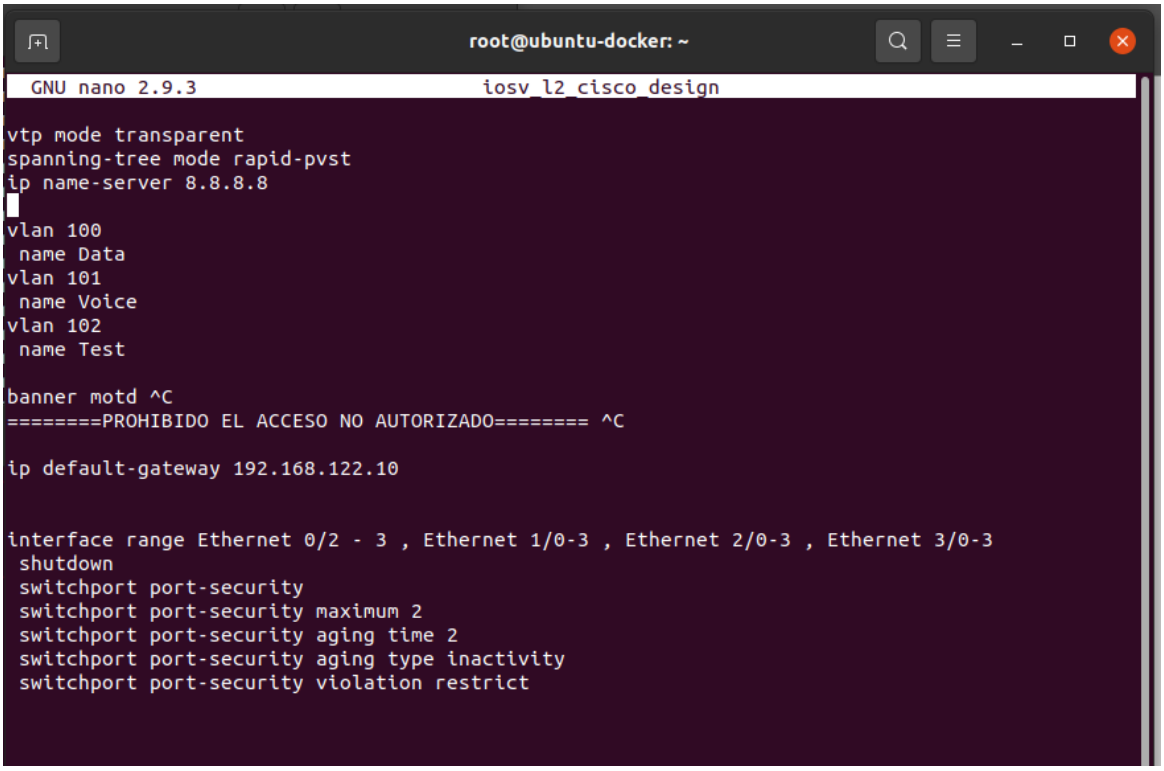


Figura 2. 9. Ejecución de scrpt modificado.

Varios dispositivos y variación de Script: Netmiko permite modificar el script para configurar más dispositivos y utilizar más archivos de configuración, de la misma manera que los anteriores scripts, se define una variable para cada dispositivo, donde se coloca un diccionario con información de los dispositivos, permite especificar el archivo que se usara para la configuración de cada dispositivo. En este tipo de script se puede usar varios archivos de configuración.

C. Ejecución del Script

Su ejecución es sencilla, solo requiere de utilizar el comando "python3 nombre_del_archivo.py", siempre se debe generar un script con tipo de archivo .py.

2.1.2.2 SCRIPTS CON PARAMIKO

Paramiko es una implementación de Python, del protocolo SSHv2, que proporciona funcionalidad tanto de cliente como de servidor. Proporciona la base para la biblioteca Fabric de SSH, se usa para ejecutar comandos de shell remotos o transferir archivos.[13]

A. Deficiencias

Citando a la página web de Paramiko en su sección preguntas frecuentes tenemos su mayor deficiencia "Desafortunadamente, el tiempo de desarrollo voluntario y el acceso a

plataformas no convencionales son limitados, lo que significa que solo podemos admitir implementaciones estándar de OpenSSH, como las que se encuentran en la distribución promedio de Linux (así como en Mac OS X y *BSD).” Esto representa una gran limitante al momento de implementarlo en redes con dispositivos Cisco o Juniper.

2.1.3 AUTOMATIZACÍON POR SOFTWARE

En esta sección se indica dos opciones principales para la automatización por software, la primera proporcionada por Cisco una de las más sencillas la automatización por equipos PnP y su administración mediante una interfaz gráfica, mientras que la segunda propone un software más complejo y especializado, cabe recalcar que las implementaciones por software están limitadas al tipo de software a adquirir y el precio de las mismas, ya que mientras más características tenga el software, capacidad para más dispositivos y disponibilidad para el usuario mayor será su precio en el mercado. Si bien se pueden encontrar desarrolladoras de software para la automatización y gestión de red.

2.1.3.1 Definiciones

En el área de automatización mediante software destacan 2 empresas, redhat y vmware las cuales tienen sus respectivas definiciones que se muestran a continuación

A. Redhat

La lógica de programación o lógica programable en la automatización de redes se usa con el fin de gestionar los recursos y servicios de la red, permitiendo que los (NetOps), equipos de operaciones, sean más eficientes y rápidos al momento de integrar, proteger, ajustar y configurar los servicios de las aplicaciones del usuario, que cuando el propio usuario lo realiza por sus propios medios.

En la gestión de redes, eliminar los pasos manuales son el principal motivo de la automatización de redes, uno de estos pasos puede ser el inicio de sesión para la configuración en los elementos de red como los routers, switch, balanceadores de carga o incluso firewalls, este proceso se lo realiza en base de scripts secuenciales, los mismos que son programados en la interfaz de líneas de comandos (CLI) implementados en un software de automatización o en un sistema operativo.

B. VMware

La automatización de red busca maximizar la funcionalidad y eficiencia de la red de manera continua, mediante el uso de software, el cual permite gestionar, aprovisionar y asegurar la red. La virtualización puede ser usada a la par de la automatización de red.

Los administradores de red y departamentos del área de Networking requieren de coherencia y agilidad al momento de gestionar y aprovisionar las aplicaciones nativas en la nube, así como también las aplicaciones tradicionales, estos objetivos se pueden lograr implementando una moderna plataforma de automatización para la red.

2.1.3.2 MOTIVOS PARA AUTOMATIZAR LAS REDES

En décadas, los cambios para gestionar las redes han sido mínimos, el procedimiento normal es crear la red, operarla y mantenerla de forma manual, sin embargo, este procedimiento carece de rapidez al momento de configurar y actualizar la red, sin mencionar los posibles errores que se pueden cometer, es en este ámbito donde la automatización de redes brinda flexibilidad y agilidad al momento de gestionar los recursos y los servicios de red.

2.1.3.3 FUNCIONAMIENTO DE LA AUTOMATIZACIÓN

Este método de automatización se basa en una API que reemplaza las instrucciones proporcionadas por líneas de comandos aplicadas a cada dispositivo de red para su configuración, la API puede ser empleada en lenguajes de programación como Python, Java o Go o invocada directamente. Uno de los aspectos básicos de la automatización son los scripts, las plataformas modernas validan los recursos de red en el trascurso del aprovisionamiento y verifica que la red sea capaz de gestionar las solicitudes de configuración del elemento de red previo a su implementación.

Además de existir varios métodos de automatización de redes, existen varios elementos en la red que pueden ser automatizados, en el método de automatización de redes por software existen 2 derivaciones, la automatización de comandos implementados por CLI y el software de automatización.

Como base, es factible automatizar los dispositivos y elementos de red a través de comandos y/o argumentos de CLI, un ejemplo de esto son los administradores del SO Linux, los cuales pueden utilizar operadores de Bash para secuenciar eventos en función de errores y aciertos de los comandos previos, también los administradores de red o usuarios en general pueden compilar scripts de Shell, los cuales son listas de comandos en archivos de texto.

Las soluciones de software de automatización integran diversas tareas de gestión de red en programas previamente definidos que se pueden aplicar, ejecutar o programar desde el frontend de la solución de software, un ejemplo de lo mencionado es Red Hat Ansible, Automation Platform, dicha solución automatiza la red y sus requerimiento de permisos mediante el empaquetado de interfaces de programación de aplicaciones (API), plugins, inventarios y los módulos en playbooks que los administradores de red pueden analizar, elegir y ejecutar para automatizar tareas de red como la configuración, seguridad, la organización y la preparación de la red, entre otras, en proveedores de servicios como AWS, Microsoft y Cisco.

2.1.3.4 AUTOMATIZACIÓN DE RED INTELIGENTE

La automatización de red nace al utilizar macrodatos y aprendizaje automático para determinar la manera más eficiente de configurar y gestionar la red del usuario con el fin de cumplir los objetivos específicos de la empresa, como nueva era de la automatización tenemos la red inteligente, la cual cuenta con una visión centralizada general de toda la red, permitiéndole determinar el camino más eficiente de funcionabilidad para cumplir los objetivos de la empresa, evitando configurar cada dispositivo o puerto de la red.

2.1.4 REDES DEFINIDAS POR SOFTWARE

Las redes definidas por software, es una solución de automatización que usa controladores desarrollados en software o interfaces de programación (API) para gestionar el tráfico de la red, comunicando la infraestructura de red basada en hardware.

Las redes tradicionales utilizan dispositivos dedicados como routers y switches para gestionar el tráfico en la red, mientras que una SDN permite crear y gestionar una red virtual o una red tradicional basada en hardware mediante un software.

2.1.4.1 FUNCIONAMIENTO DE UNA SDN

Como principio de toda tecnología virtualizada, la SDN desvincula los dos planos fundamentales, el hardware del software, esto ocurre al trasladar el plano de control el cual establece la gestión del tráfico al software, dejando al hardware el plano de datos que se encarga de reenviar el tráfico. Esta solución permite a los administradores de red programar, gestionar y controlar toda o gran parte de la red desde un único panel de control, evitando la configuración y gestión de cada equipo router, switch o firewall.

La arquitectura de las SDN incluye tres componentes principales:

Controlador SDN: La capa de control de la SDN (Red Definida por Software) es la capa centralizada de software que se encarga de tomar decisiones sobre el encaminamiento de datos en la red y de programar los dispositivos de red para que implementen estas decisiones. Esta capa se conoce como el "controlador SDN" y se comunica con los dispositivos de red a través de un protocolo de comunicación especial llamado "Southbound Protocol".

El controlador SDN es el corazón de la arquitectura de la SDN y es el encargado de tomar decisiones sobre cómo se deben enrutar los datos en la red. Para ello, utiliza una base de datos de estado de la red que almacena información sobre la topología de la red, los enlaces disponibles y otras características relevantes. A partir de esta información, el controlador SDN puede calcular rutas óptimas para el tráfico de datos y programar los dispositivos de red para que implementen estas rutas.

Además de tomar decisiones de encaminamiento de datos, la capa de control de la SDN también se encarga de comunicarse con las aplicaciones de red a través de un protocolo de comunicación especial llamado "Northbound Protocol". Esto permite que las aplicaciones de red utilicen la información de encaminamiento y la programación de dispositivos de red para implementar diferentes políticas y funcionalidades de red.

Dispositivos de red: La capa de dispositivos de red de la SDN (Red Definida por Software) incluye los dispositivos que se encargan de la conexión física de los dispositivos de red en la red y de la transmisión de datos entre ellos. En una SDN, estos dispositivos se conocen como "dispositivos inteligentes" o "switches inteligentes" y se programan a través del controlador SDN para implementar las decisiones de encaminamiento de datos tomadas por la capa de control de la SDN.

Los dispositivos de red de la SDN son similares a los dispositivos de red tradicionales, como routers y switches, pero tienen la capacidad de ser programados y controlados de forma más flexible y dinámica. Esto se debe a que están diseñados para trabajar en conjunto con el controlador SDN y aceptar instrucciones desde él para implementar decisiones de encaminamiento de datos.

Aplicaciones de red: Son las aplicaciones que se ejecutan en la capa de control de la SDN y que utilizan la información de encaminamiento y la programación de dispositivos de red para implementar diferentes políticas y funcionalidades de red. La capa de aplicaciones de red de la SDN (Red Definida por Software) incluye las aplicaciones que se ejecutan en la capa de control de la SDN y que utilizan la información de encaminamiento y la programación de dispositivos de red para implementar diferentes políticas y funcionalidades de red. Estas aplicaciones se comunican con el controlador SDN a través de un protocolo de comunicación especial llamado "Northbound Protocol".

Las aplicaciones de red de la SDN pueden ser utilizadas para implementar una amplia variedad de políticas y funcionalidades de red, tales como la optimización del rendimiento de la red, la gestión de la calidad de servicio, la seguridad de la red y muchas otras. Al utilizar la información de encaminamiento y la programación de dispositivos de red proporcionadas por el controlador SDN, las aplicaciones de red de la SDN pueden implementar estas políticas y funcionalidades de manera dinámica y flexible.

2.1.4.2 VENTAJAS DE LAS SDN

Las redes definidas por software (SDN) son un enfoque innovador en el diseño y la administración de redes de computadoras. Algunos de los aspectos que destacan de las SDN son:

A. Mejor control con mayor velocidad y flexibilidad

Evita que los administradores de red programen varios dispositivos de hardware, routers o switch, de forma manual, ya que solo deben programar un controlador basado en software para gestionar el tráfico que fluye en la red, a su vez permite mayor flexibilidad al momento de seleccionar el equipo de las redes, esto debido a que los administradores pueden escoger un protocolo de código abierto y comunicarse con una amplia cantidad de dispositivos a través de un solo panel de control o controlador central.

B. Personalización de la Infraestructura de red

Permite a los operadores o administradores de red la optimización del flujo de datos, al priorizar las aplicaciones que necesitan mayor disponibilidad en la red, esto es factible, ya que los operadores pueden asignar recursos virtuales y/o configurar los servicios de red para modificar la infraestructura de la red en tiempo real desde el controlador central.

C. Seguridad fuerte

Aumentar la visibilidad completa de la red es una de las ventajas más importantes de una red definida por software, permitiendo una visión integral de amenazas a la seguridad. Debido al avance exponencial de los dispositivos inteligentes que se incorporan a la red y a la par al internet, las SDN proporcionan mayor ventaja en comparación a las redes tradicionales. Los operadores y administradores son capaces de crear zonas aisladas para los dispositivos que requieren niveles de seguridad distintos y/o poner en tiempo real en cuarentena a cualquier dispositivo con características de vulnerabilidad, evitando que la red sea afectada.

D. Capa de aplicaciones

Es una parte importante de la automatización de redes que consiste en un conjunto de aplicaciones y funciones que envían instrucciones al controlador SDN. Estas instrucciones pueden incluir solicitudes de recursos o información sobre la propia red y se transmiten a través de APIs. Algunas de las funciones más comunes incluyen la gestión de direcciones IP y el equilibrio de carga de trabajo.

E. Capa de control

se refiere a los controladores SDN, que reciben información de la capa de aplicaciones y la transmiten a los componentes de la red. Los controladores SDN son responsables de determinar cómo enrutar los paquetes de datos y administrar las políticas y el flujo de tráfico. Además, recopilan información de la red de hardware, lo que los convierte en uno de los componentes más importantes de una red definida por software, ya que funcionan como un punto de unión entre la capa de aplicaciones y la capa de infraestructura.

F. Capa de infraestructura

Comprende todos los dispositivos de red físicos, como switches y enrutadores, que se encargan del envío y procesamiento de los datos. Reciben información del controlador SDN para determinar dónde y cómo mover los datos, y recopilan información crítica, como el uso o la tipología de la red, que luego se envía de vuelta a la capa de control.

2.1.4.3 TIPOS DE SDN

SDN (Software-Defined Networking o Red Definida por Software) es un enfoque de red que se basa en la separación del control y el forwarding de la red. Esto permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red se centraliza en un software y puede ser modificado y programado de forma dinámica.

Existen varios tipos de SDN, incluyendo:

A. SDN de capa 2 (Layer 2 SDN)

Se refieren a la implementación de SDN en la capa 2 del modelo OSI (capa de enlace de datos). En este tipo de SDN, el control de la red se basa en el intercambio de tráfico entre dispositivos de red, como switches y hubs.

En una SDN de capa 2, se utilizan técnicas de virtualización de capa 2, como VLANs (Virtual LANs o Redes LAN virtuales), para crear una red virtual encima de la red física subyacente. Esta red virtual se controla mediante una capa centralizada de software y

permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red puede ser modificado y programado de forma dinámica.
Las SDN de capa 2 se utilizan a menudo en entornos de red de pequeña a mediana escala y son especialmente útiles para implementar soluciones de red personalizadas y adaptables a las necesidades específicas de una empresa.

B. SDN de capa 3 (Layer 3 SDN)

Se refieren a la implementación de SDN en la capa 3 del modelo OSI (capa de red). En este tipo de SDN, el control de la red se basa en el encaminamiento de paquetes entre dispositivos de red, como routers y firewalls.
En una SDN de capa 3, se utilizan técnicas de virtualización de capa 3, como VRFs (Virtual Routing and Forwarding Instances o Instancias de enrutamiento y encaminamiento virtuales), para crear una red virtual encima de la red física subyacente. Esta red virtual se controla mediante una capa centralizada de software y permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red puede ser modificado y programado de forma dinámica.

C. SDN de capa 4 a 7 (Layer 4-7 SDN)

Se refieren a la implementación de SDN en las capas 4 a 7 del modelo OSI (capas de transporte, sesión, presentación y aplicación). En este tipo de SDN, el control de la red se basa en el procesamiento y el enrutamiento de tráfico a nivel de aplicación.
En una SDN de capa 4 a 7, se utilizan técnicas de virtualización de capa 4 a 7, como VSFs (Virtual Service Functions o Funciones de servicio virtual) y VNFs (Virtual Network Functions o Funciones de red virtual), para crear una red virtual encima de la red física subyacente. Esta red virtual se controla mediante una capa centralizada de software y permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red puede ser modificado y programado de forma dinámica.
Las SDN de capa 4 a 7 se utilizan a menudo en entornos de red de gran escala y son especialmente útiles para implementar soluciones de red personalizadas y adaptables a las necesidades específicas de una empresa.

D. SDN abierta

En este primer modelo, los administradores de red utilizan un protocolo (como Open Flow) para la gestión y control de los datos de la red, así como la supervisión de los conmutadores virtuales y físicos.

La SDN abierta (Open SDN) se refiere a la implementación de SDN en la que se utilizan estándares abiertos y protocolos de red para permitir la interoperabilidad entre dispositivos y sistemas de red de diferentes fabricantes. Esto permite a las empresas implementar soluciones de red más flexibles y personalizables, ya que no están atadas a un único fabricante o solución de red.

La SDN abierta también permite una mayor innovación y colaboración en la industria de la red, ya que permite a múltiples fabricantes y desarrolladores trabajar juntos para crear nuevas soluciones y mejorar las existentes. Esto también permite a las empresas adoptar soluciones de red más innovadoras y adaptables a sus necesidades específicas.

E. SDN por API

En este caso, son las interfaces de programación de aplicaciones (APIs) las que controlan el desplazamiento de los datos a través de la red de dispositivos.

La SDN por API (API-based SDN o SDN basada en API) se refiere a la implementación de SDN en la que se utilizan APIs (interfaces de programación de aplicaciones) para permitir la interoperabilidad entre diferentes componentes de la red y para proporcionar una capa de abstracción para la configuración y el control de la red.

En una SDN por API, el control de la red se basa en una capa centralizada de software que se comunica con los dispositivos de red a través de APIs. Esto permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red puede ser modificado y programado de forma dinámica a través de las APIs.

La SDN por API también permite una mayor interoperabilidad entre diferentes componentes de la red, ya que las APIs proporcionan una forma estandarizada de comunicación entre ellos. Esto permite a las empresas implementar soluciones de red más flexibles y personalizables, ya que no están atadas a un único fabricante o solución de red.

En general, la SDN por API es un enfoque muy flexible y personalizable para la implementación de SDN y permite una mayor interoperabilidad y programabilidad de la red.

F. Superposición de SDN

En este modelo, se ejecuta una red virtual sobre una infraestructura de hardware, creando túneles dinámicos. Todo ello sin modificar la red física, ya que la virtual permite reasignar dispositivos y ancho de banda en los diferentes canales.

La superposición de SDN (SDN Overlay) se refiere a la implementación de SDN en la que se crea una capa de red virtual encima de una red existente. Esto se hace utilizando técnicas de virtualización, como VLANs (Virtual LANs o Redes LAN virtuales) y VXLANs (Virtual Extensible LANs o Redes LAN extensibles virtuales).

En una superposición de SDN, se crea una red virtual que está completamente separada de la red física subyacente y se controla mediante una capa centralizada de software. Esto permite una mayor flexibilidad y programabilidad de la red, ya que el control de la red puede ser modificado y programado de forma dinámica.
La superposición de SDN también permite a las empresas implementar soluciones de red más flexibles y personalizables, ya que no están atadas a la red física subyacente y pueden configurar y controlar la red virtual de acuerdo con sus necesidades específicas.

G. SDN híbrida

consiste en combinar una red definida por software con protocolos de red tradicionales, de modo que el SDN asuma una parte del control del tráfico de datos, y los protocolos estándar la otra.
La SDN híbrida (Hybrid SDN) se refiere a la implementación de SDN en la que se combinan diferentes enfoques o tecnologías de SDN para crear una solución de red más compleja y adaptable. Esto permite a las empresas implementar soluciones de red más flexibles y personalizables que se ajusten a sus necesidades específicas.
Por ejemplo, una SDN híbrida podría combinar una superposición de SDN con una SDN de capa 3 para crear una red virtual que se controla mediante una capa centralizada de software y que se basa en el encaminamiento de paquetes entre dispositivos de red. Otra opción podría ser combinar una SDN por API con una SDN de capa 4 a 7 para crear una red que se controla a través de APIs y que se basa en el procesamiento y el enrutamiento de tráfico a nivel de aplicación.

2.1.4.4 CISCO PNP

En esta sección se profundiza la automatización mediante software, comenzando por la implementación de plug and play (PnP). Es de las primeras etapas para la automatización, el conectar un equipo sin preocuparse por la configuración de este facilita el trabajo tanto para el usuario como para el administrador de redes, sin embargo, esto no significa que no haya pasos previos para la aplicar dicho método.

A. FindIT y Network PnP

FindIT es una solución del fabricante de equipos Cisco, el cual descubre automáticamente los productos Cisco Small Business de la red, a su vez muestra la información necesaria para la administración de la red, solucionar problemas y/o agregar un nuevo dispositivo. PnP es una herramienta en el administrador de FindIT para la implementación de Network Plug & Play (Network PnP) sin intervención Cisco.[14]

PnP permite eliminar cargas de trabajo necesarias para la implementación de infraestructuras. Entre dichas cargas se encuentran el aprovisionamiento hasta la detección de dispositivos, permite a los usuarios una ágil implementación de la red desde una interfaz remota. PnP, evita que el usuario configurar los dispositivos uno a la vez y permite, sin la intervención del usuario de red, el aprovisionamiento de firmware o la actualización de la configuración de inicio para los dispositivos dentro de la red a trabajar.[15]

La automatización por equipos de Cisco PnP se sigue el siguiente procedimiento:

Tabla 2. 6. Procedimiento de Automatización.

Procedimiento	Configuración del Router PnP
Para configurar el router en necesario registrar el router en FindIT Manager esto permite que el router admita PnP.	
Pasos del Procedimiento	
En el router se debe Iniciar sesión en la página de configuración web. Ingresar al icono de Configuración del sistema seguido de la opción PnP. En el router se debe habilitar PnP y configurar la opción PnP Transport en Auto lo cual permite detectar automáticamente el servidor PnP esto lo realiza de forma predeterminada. Introducir el nombre de dominio (FQDN) o la dirección IP del administrador FindIT, el puerto 443, es el puerto por default. Aplicar la configuración.	
Procedimiento	Carga de Imagen o Configuración
Pasos del Procedimiento	
Conectar FindIT, se elige la opción Network Plug and Play y se selecciona imagen o configuración. Seleccionar el icono Añadir para cargar el archivo de configuración o imagen. Para subir o cargar, se tiene la opción de arrastrar y soltar, seguido del icono Cargar.[16]	

B. Características y Deficiencias

Cisco indica sus características principales de su producto Network PnP de las cuales se toman las más destacadas para la automatización y de analizan para el cumplimiento de una automatización optima, entre ellas tenemos:

- Descubrimiento y visualización automáticos de información sobre cualquier dispositivo Cisco Small Business en la red, incluido el tipo de dispositivo, el número de serie, la versión de hardware y firmware, y las direcciones IP y MAC.

Las palabras claves son “dispositivos Cisco”, ya que si bien descubre y visualiza de forma automática está limitado por el proveedor al solo permitir dispositivos Cisco y forzando al usuario al desarrollar toda su red con Cisco

- Descubrimiento y visualización automáticos de nuevas actualizaciones de firmware y capacidad para descargar actualizaciones a la PC con solo unos pocos clics.

Si bien el realizar pocos clics ayuda y facilita el trabajo del usuario o administrador de redes no lo automatiza como tal, se considera que entre las principales características para una automatización optima es el evitar dar clics sobre todo en las actualizaciones de los dispositivos.

- Informes básicos, incluidos informes de inventario, mantenimiento y fin de vida útil

El optimizar y mejorar una red se obtiene al generar y analizar informes favoreciendo al usuario el análisis para desarrollar y escalar su red acorde las necesidades.

2.1.4.5 Paragon de Juniper

Como se mencionó al inicio de esta sección la implementación esta esta metodología está condicionada al servicio que la empresa está dispuesto a pagar, al igual que el tamaño y escalamiento de la misma en los siguientes años, su implementación es más sencilla al ser la empresa distribuidora la encargada de ofertar e implementar el software para la automatización, como un ejemplo de este tipo de software se presenta Juniper Paragon, se presentará sus características principales y se analizará sus ventajas y desventajas.

Juniper Paragon Automation es una solución de módulos con aplicaciones de software alojadas de manera nativa en la nube, ofreciendo automatización como un circuito cerrado en entornos multinube y 5G. Permite eliminan tareas y procesos los cuales los realizaría el usuario de la red, esto permite a los equipos de operaciones un trabajo más rápido, eficiente y preciso.

A. Calidad del Servicio de Red en el Punto de Mira

Paragon Automation combina el aprendizaje automático, agentes de prueba y transmisión de telemetría con remediación de ciclo cerrado. Los dispositivos y administradores sabrán si un servicio se ve afectado, en tiempo real, al verificar y analizar el desempeño real del servicio a lo largo de la vida del servicio.

B. Automatización con reconocimiento de Red

La presente solución se creó enfocado a los operadores de red, con cada aplicación diseñada para ser consciente del desempeño de la red y del servicio. Esto incluye capacidades como reconocimiento y mapeo de la topología de red en tiempo real, dando soporte integrado en todos los dominios de red. Juniper Paragon brinda un análisis de causa raíz de varias capas, detecta, examina y mapear los inconvenientes del servicio al dispositivo y desde el dispositivo al servicio.

C. Aprendizaje Automático Adaptado a la Red

Paragon Automation se basa en el algoritmo de aprendizaje automático y en el analisis de red. obtiene, integra y analiza grandes cantidades de datos en tiempo real para brindar una vista de varias dimensiones del estado de la red, dispositivo, y servicio. Para identificar anomalías y comportamientos inusuales utiliza múltiples algoritmos de ML, lo que permite realizar predicciones precisas sobre el futuro comportamiento de dispositivos en la red.

D. Resiliencia y agilidad Nativas en la Nube.

las aplicaciones nativas de la nube de la solución Paragon Automation brindan flexibilidad y elasticidad de la nube a la red, controlando el asiento del conductor para la red WAN en su totalidad. Se puede utilizar como una solución SaaS alojada en la nube, alojada en las instalaciones. Y se puede implementar en clústeres de nodos redundantes dentro de un mismo centro de datos, así como también en múltiples nubes en una arquitectura de escalamiento horizontal altamente confiable y de alta disponibilidad.[7].

2.2 DESARROLLO

En esta sección se exponen las características principales para una correcta automatización de redes basado en el análisis previamente visto, además de una comparativa entre las distintas metodologías y su aplicabilidad en redes con sus respectivos requerimientos.

2.2.1 COMPARATIVA DE METODOLOGÍAS

En la siguiente tabla se nuestras una comparativa de las características con las metodologías de automatización, si la metodología cumple la característica sin excepción se la señala con CUMPLE, sí existe alguna excepción se señala con LIMITADO y se señala con NO CUMPLE si no aplica la característica.

Tabla 2. 7. Comparativa de Características Principales

CARACTIRISTICA	DISPOSITIVO	SCRIPTS	SOFTWARE
CONTROL CENTRALIZADO	CUMPLE	CUMPLE	CUMPLE
MULTIPROVEEDOR	LIMITADO	CUMPLE	LIMITADO
ESCALABLE	LIMITADO	CUMPLE	LIMITADO
APRENDIZAJE AUTOMATIZADO	LIMITADO	NO CUMPLE	CUMPLE
GESTIÓN AMIGABLE	LIMITADO	NO CUMPLE	CUMPLE
APLICABILIDAD	LIMITADO	NO CUMPLE	CUMPLE

2.2.1.1 EQUIPOS O DISPOSITIVOS

La automatización por dispositivos se ve ampliamente limitado por el dispositivo a implementar, sobre todo por el proveedor, a grandes rasgos el proveedor Juniper se ve limitado por la escalabilidad, debido que en cierto punto se necesitará más de un equipo Junos para escalar la red, mientras que, en el caso de Cisco destaca ya que dispone una solución física implementable a varios niveles cómo se ve en la Figura 2.4, además que cuenta con documentación más detallada para su implementación, sin embargo, está limitado por las características de aprendizaje automático y multiproveedor.

- Utiliza herramientas de automatización de software o hardware específicas para automatizar tareas en dispositivos de red.
- Puede ser más fácil de usar que la automatización por scripts, ya que no requiere habilidades de programación.
- Es más adecuado para redes grandes con un gran número de dispositivos.
- Puede ser más costoso que la automatización por scripts debido a la necesidad de adquirir y mantener equipos de automatización.

2.2.1.2 SCRIPTS

Para el aprendizaje automático se requiere de otras librerías e implementación de código, por lo que no aplica dicha característica, no dispone de una gestión amigable, ya que no dispone de una interfaz gráfica para su implementación, es netamente código, lo que conlleva problemas al momento de aplicar, debido a que se necesita de una persona con conocimientos de programación para aplicar la metodología, entre Netmiko y Paramiko, sobresale Netmiko a su mayor desarrollo e implementación para varios proveedores.

- Permite automatizar tareas mediante el uso de scripts o programas de computadora que se ejecutan en un dispositivo de red.
- Los scripts pueden ser escritos en diferentes lenguajes de programación, como Python, Perl, etc.
- El uso de scripts permite automatizar tareas específicas y personalizadas, que no están disponibles en las herramientas de automatización de equipos.
- Es más adecuado para redes pequeñas o medianas con un número limitado de dispositivos.
- Puede requerir habilidades de programación para crear y mantener los scripts.

2.2.1.3 SOFTWARE

Más que una metodología se la puede considerar una solución de automatización, la cual tienen sus limitantes en la parte financiera, tamaño de la empresa y su escalamiento en próximos años, si bien una empresa puede adquirir un software para la automatización de su red, debe estar consciente de que requerimientos de automatización son necesarios, si los servicios que ofrece el proveedor se ajustan a la empresa y si es un gasto necesario para la misma.

Entre las dos metodologías vistas, Cisco tiene amplias limitantes como el número de dispositivos que soportan PnP y limitado análisis de datos, mientras que Paragon de Juniper dispone de varios servicios para la automatización de redes y análisis de esta con aprendizaje automático.

- Utiliza software específico, como herramientas de automatización de red o plataformas de administración de red, para automatizar tareas en dispositivos de red.
- El software se ejecuta en un dispositivo de red o en una computadora central y se comunica con los dispositivos de red a través de protocolos de red estándar.
- Puede ser más económico que la automatización de redes por equipos debido a la posibilidad de utilizar hardware existente.
- Puede requerir habilidades de programación para crear y mantener los scripts o aplicaciones de automatización.

2.2.1.4 REDES DEFINIDAS POR SOFTWARE

La automatización de redes es un proceso que utiliza tecnologías para simplificar la configuración, el monitoreo y la gestión de redes. Ambos, software y SDN (Software

Defined Networking) son utilizados para automatizar redes, pero ofrecen diferentes enfoques y beneficios.

La automatización de redes mediante software se refiere a la utilización de herramientas de software para configurar y monitorear dispositivos de red, como routers y switches. Estas herramientas suelen ser proporcionadas por los fabricantes de equipos de red y pueden incluir características como la configuración en masa y la automatización de tareas de diagnóstico.

Por otro lado, SDN es un enfoque de red en el que la lógica de control de la red se separa de los dispositivos físicos. En lugar de configurar cada dispositivo individualmente, un controlador SDN centraliza la configuración y el monitoreo de la red, lo que permite una mayor automatización y flexibilidad. SDN también permite una mayor programabilidad de la red, lo que facilita la integración con otras tecnologías como la inteligencia artificial y el aprendizaje automático.

Por lo tanto, la automatización de redes mediante software se enfoca en la configuración y el monitoreo de dispositivos de red individuales, mientras que SDN es un enfoque más generalizado que busca centralizar el control de la red y proporcionar una mayor programabilidad y flexibilidad.

2.2.1.5 REDES BASADAS EN LA INTENCIÓN

La automatización de redes basadas en la intención (también conocida como redes basadas en políticas) es un enfoque similar al SDN, ya que ambos buscan automatizar la configuración y el monitoreo de redes mediante la centralización del control de la red. Sin embargo, hay algunas diferencias clave entre ambos enfoques.

SDN se enfoca en la programabilidad de la red, permitiendo que los desarrolladores escriban aplicaciones para controlar y automatizar la red. En cambio, las redes basadas en la intención se enfocan en la expresión de las necesidades y deseos del usuario en términos de servicios y políticas de red, y luego automatizan la configuración de la red para cumplir esas intenciones.

Otra diferencia es que SDN se enfoca en la separación de la capa de control de la red de los dispositivos físicos, permitiendo una mayor programabilidad y flexibilidad. Mientras tanto, redes basadas en la intención se enfocan en la expresión de las necesidades del usuario y luego automatizando la configuración de la red para cumplir esas necesidades, dando como resultado una mayor eficiencia y seguridad en las redes.

En resumen, SDN y las redes basadas en la intención comparten el objetivo de automatizar la configuración y el monitoreo de redes mediante la centralización del control de la red, pero se enfocan en áreas diferentes: SDN se enfoca en la programabilidad de la red,

mientras que las redes basadas en la intención se enfocan en la expresión de las necesidades del usuario y en la automatización de la configuración de la red para cumplir esas necesidades.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se mostrarán las características generales inferidas de todas las metodologías analizadas en el capítulo 2, seguido de las características específicas y deficiencias.

3.1 RESULTADOS

En esta sección se exponen las características principales para una correcta automatización de redes basado en el análisis previamente visto, además de una comparativa entre las distintas metodologías y su aplicabilidad en redes con sus respectivos requerimientos.

3.1.1 CARACTERISTICAS GENERALES

En base a lo estudiado y expuesto previamente se puede destacar las siguientes características principales, para la automatización de redes.

- Control centralizado: Permite controlar y configurar dispositivos de red de forma remota desde una consola central.
- Escalabilidad: Permite agregar o eliminar dispositivos de red de forma dinámica sin interrumpir el servicio.
- Configuración automática: Permite configurar automáticamente los dispositivos de red según una política predefinida.
- Monitoreo en tiempo real: Permite monitorear el estado de los dispositivos de red y detectar problemas en tiempo real.
- Integración con sistemas de gestión de red: Permite integrar la automatización de redes con sistemas de gestión de red para una visibilidad y control total de la red.
- Automatización de tareas repetitivas: Permite automatizar tareas repetitivas para reducir el tiempo y los errores humanos.
- Multiproveedor: Debe ser capaz de aceptar e implementar varios dispositivos de red, de forma óptima y sin limitantes al momento de implementar.

- Aprendizaje automático: Capacidad de aprender de la red, sin intervención del usuario o administrador, para mejorar su desempeño.
- Gestión amigable: Permite al usuario o administrador, usar la metodología de forma sencilla, de preferencia mediante una interfaz gráfica
- Aplicabilidad: La metodología debe ser fácil de aplicar, administrar y gestionar, con conocimientos básicos de redes y sin conocimientos adicionales.

3.1.2 CARACTERISTICAS Y DEFICIENCIAS POR METODOLOGÍA

En la presente sección se analiza las características de cada una de las metodologías indicadas en el Apartado 2.1.

3.1.2.1 METODOLOGÍA POR EQUIPOS JUNOS SPACE

1. Automatización de infraestructura de red integrada

La plataforma de gestión de red de Junos Space proporciona una gestión centralizada, unificada con una funcionalidad completa de gestión de elementos para una gestión total de los dispositivos de enrutamiento, conmutación y seguridad de Juniper. Las funciones de gestión de elementos de red incluyen.

- Detección de dispositivos, proporciona una interfaz basada en asistente para la detección de dispositivos casi en tiempo real que permite a los operadores administrar rápidamente los dispositivos de red.

El proporcionar una interfaz permite no solo a un administrador de red hacer uso del dispositivo, también permite al usuario con conocimiento básico de redes hacer uso de este.

- Topología, permite a los operadores tener una vista topológica amplia de la red, incluidos los dispositivos de punto final, información de enlace, cuellos de botella y fallas, y relaciones descubiertas entre elementos de red, como dispositivos e interconexiones para dispositivos bajo administración.

El tener una amplia vista de la red permite al usuario y/o administrador de red, tener un mejor control y administración de los dispositivos, gestionando de manera ágil la red y sus flujos.

- Plantillas de configuración, permite la creación de plantillas de configuración basadas en modelos para ayudar a optimizar y escalar las configuraciones de los dispositivos. Incluye GUI basada en esquemas para configuraciones totalmente personalizables y un registro de auditoría para realizar un seguimiento de los

cambios de configuración. Las opciones de plantilla basadas en CLI también están disponibles.

Una plantilla de configuración agilita el procedo de gestión y activación de dispositivos y servicios, dando bases a la automatización de redes y su gestión, tanto por interfaz gráfica como por CLI, permitiendo abarcar varios dispositivos de red.

- Gestión de archivos de configuración, permite una gestión de configuración simplificada que incluye importar, editar, comparar y realizar copias de seguridad/restauración para dispositivos individuales o grupos de dispositivos. Proporciona visibilidad instantánea de la configuración de la red y la correlación de rendimiento, programación de implementación de configuración automatizada, validación para minimizar los errores de sintaxis y formularios de entrada para una fácil creación de definiciones de plantilla y modificación masiva de configuraciones.

Como se trató en el punto anterior las plantillas proporcionan una base para la automatización de rede Junos complementa las plantillas con la automatización de procesos principales.

3.1.2.2 METODOLOGÍA CISCO DNA

Entra las principales características que ofrece el software de Cisco DNA para la automatización de redes destacan las siguientes:

- Gestión centralizada, Diseñe, aprovisione, habilite políticas y asegure los servicios de red a través de una administración centralizada habilitada para la nube.

Uno de los principales desarrollos en tecnología es SaaS, permitiendo gestionar los dispositivos en cualquier parte del mundo a través de la nube, sin embargo, esto está limitado por la solvencia financiera que tenga la empresa

- Automatización, Automatice por completo la infraestructura de la red en función de una política en toda la red de acceso, simplifique y escale las operaciones automatizando la configuración, el aprovisionamiento y la resolución de problemas diarios.

Predicción, otra de las bases fundamentales para la automatización de redes, si un sistema puede predecir el comportamiento esta mejor capacitado para la automatización.

- Plataforma abierta, Optimiza las operaciones de TI, habilita la innovación y alinea la intención comercial al hacer que la red sea abierta y extensible para la integración con otros sistemas y aplicaciones.

Al permitir varios dispositivos amplia la diversidad de la red y permite el escalamiento de esta sin limitantes en dispositivos, sin embargo, la implementación de otros dispositivos fuera de cisco suele ser más complejos y difíciles de implementar

3.1.2.3 METODOLOGÍA POR SCRIPTS

Entre las principales características para la automatización de redes con Netmiko, destacan:

- Multiproveedor, admite un gran conjunto de dispositivos de varios proveedores, entre ellas, dos de las empresas más conocidas, Juniper y Cisco, sin mencionar una amplia lista de dispositivos compatibles.
- Configuración de dispositivos, proporciona métodos para aplicar la configuración desde una lista de comandos o un archivo de comandos.
- Configuración del dispositivo, admite varios métodos para leer la configuración de los dispositivos.

De manera general, Netmiko proporciona al usuario la posibilidad de configurar y visualizar datos relevantes de los equipos, sin embargo, no contempla en análisis de los datos obtenidos, se requiere de una metodología adicional para el análisis de la red, la visualización de esta y su implementación requiere de un usuario o administrador de red con conocimientos de programación en el lenguaje Python.

3.1.2.4 METODOLOGÍA POR SOFTWARE

Algunas de las características de las redes definidas por software (SDN) incluyen:

- Centralización del control: En SDN, la inteligencia de la red se mueve de los dispositivos de red físicos a una "capa de control" lógica de software, lo que permite una mayor flexibilidad y programabilidad en la gestión de la red.
- Programabilidad: SDN permite programar y automatizar la configuración de la red a través de lenguajes de programación como Python o Java.
- Separación de control y forwarding: En SDN, la capa de control se separa de la capa de forwarding, lo que permite una mayor flexibilidad y escalabilidad en la gestión de la red.
- Abierto: SDN se basa en estándares abiertos, lo que permite una mayor interoperabilidad y facilidad de integración con otras herramientas y sistemas.
- Virtualización: SDN permite la virtualización de los recursos de red, lo que permite una mayor eficiencia y flexibilidad en el uso de los recursos de red.

- Visibilidad y monitoreo: SDN permite una mayor visibilidad y monitoreo de la red, lo que permite detectar y resolver problemas de manera más rápida.
- Automatización: SDN permite automatizar tareas repetitivas y reducir el tiempo de resolución de problemas.

Algunas de las principales deficiencias de las redes definidas por software (SDN) son:

- Complejidad: La implementación de SDN puede ser compleja y requerir un equipo de desarrollo experimentado en programación y automatización.
- Costo: La implementación de SDN puede ser costosa debido a la necesidad de adquirir nuevos equipos y software especializado.
- Seguridad: Una configuración incorrecta o una vulnerabilidad en el software de control pueden poner en riesgo la seguridad de la red.
- Dependencia del software: SDN es altamente dependiente del software, y un fallo en éste puede afectar el correcto funcionamiento de la red.
- Compatibilidad: Aunque SDN se basa en estándares abiertos, puede haber problemas de compatibilidad entre los diferentes proveedores de software y hardware.
- Escalabilidad: A medida que la red crece, puede ser difícil escalar la implementación de SDN de manera adecuada.
- Cambios en la infraestructura: La implementación de SDN puede requerir cambios significativos en la infraestructura existente de la red, lo que puede ser costoso y tiempo-consumidor.

En esta sección también se considera las características y deficiencias de las redes basadas en la intención, como deficiencias cuanta con las mismas que las SDN mientras que sus principales características son:

- Enfoque en el usuario: La automatización de redes basada en la intención se enfoca en expresar las necesidades y deseos del usuario en términos de servicios y políticas de red, y luego automatizar la configuración de la red para cumplir esas intenciones.
- Eficiencia: Al automatizar la configuración de la red para cumplir las necesidades del usuario, la automatización basada en la intención puede mejorar la eficiencia de la red.
- Seguridad: La automatización basada en la intención puede ayudar a garantizar que la red cumpla con las políticas de seguridad establecidas, lo que aumenta la seguridad de la red.

- Flexibilidad: La automatización basada en la intención permite una mayor flexibilidad en la configuración de la red, ya que se pueden especificar políticas y servicios personalizados.

3.2 CONCLUSIONES Y RECOMENDACIONES

3.2.1 CONCLUSIONES

El análisis fue desarrollado con un estudio previo de las metodologías existentes, seguido de un desglose de las metodologías con ejemplos prácticos con el fin de obtener sus características y desventajas, realizado lo anterior se obtuvo las características principales que se deben considerar el automatizar las redes.

- la automatización de redes en EoT por equipos es una solución fácil de usar, pero puede ser costosa, mientras que la automatización de redes en EoT por software es más económica, pero puede requerir habilidades de programación. Dependiendo de las necesidades de su red, puede utilizar ambos enfoques de forma combinada para obtener los mejores resultados en la automatización de tareas en redes IoT.
- la automatización de redes aplicado a EoT por scripts es más adecuada para tareas específicas y personalizadas, mientras que la automatización de redes aplicado a EoT por software es más adecuada para redes con un gran número de dispositivos IoT y proporciona una interfaz fácil de usar. Dependiendo de las necesidades de su red, puede utilizar ambos enfoques de forma combinada para obtener los mejores resultados en la automatización de tareas en redes IoT.
- Existen varias opciones para automatizar la red, muchas de ellas dispersas por la red, como se desarrolló en este documento se pueden sintetizar en tres tipos de metodologías, automatización por equipos, automatización por scripts o automatización por software, cada una varia acorde la necesidad del cliente y la complejidad de la red.
- La metodología por equipos es útil al tratarse de una empresa grande que disponga de un cuarto de equipos para el correcto mantenimiento y cuidado de estos y que requiera de un análisis de los datos que fluyen por la red.
- La automatización por scripts es adecuada para usuarios o empresas pequeñas que requieran de un monitoreo básico cómo son los comandos “show” o una configuración mínima del equipo, sin olvidar que la persona a cargo debe tener

conocimientos en redes y programación, sobre todo en el lenguaje de programación Python.

- La automatización por software no se considera como tal una metodología ya que el proveedor del software se encarga de realizar el análisis, ofertar y proporcionar el software, su implementación es más sencilla, pero depende mucho de la parte financiera de la empresa.

3.2.2 RECOMENDACIONES

Durante el análisis se infirió distintas recomendaciones tanto en las metodologías como para aplicar las mismas expuestas en el presente documento, dichas recomendaciones con las siguientes:

- Se recomienda indagar más sobre los limitantes que cada una de las metodologías tiene, ya que si bien se menciona a grandes rasgos sus limitantes es favorable indicar más para una correcta implantación y mejor desempeño de cada metodología proporcionada en el presente documento.
- Si bien en la automatización por software se puede encontrar varios productos en el mercado, se recomienda al usuario o administrador de redes que compare las características que el proveedor ofrece con proveedores de marcas conocidas como Cisco y Juniper que tienen varios años en el mercado.
- En la metodología por equipos es recomiendo tener claro como escalará la red durante los años, si el espacio disponible en el cuarto de equipos o rack es el idóneo para la implementación de más equipos y su correcto mantenimiento.
- Como se mencionó previamente automatización por scripts es básica y solo se enfoca a la validación de estado del equipo y configuraciones no tan complejas, al elegir esta metodología se recomienda que el usuario indague más información de librerías que pueden ayudar a analizar la red y crear mejores flujos de red para un mejor desempeño de automatización.
- Lenguaje de programación ampliamente utilizado: Es recomendable utilizar lenguajes de programación ampliamente utilizados como Python o Perl, ya que estos lenguajes tienen una amplia variedad de bibliotecas y recursos disponibles para automatizar tareas de red.
- Protocolos estándar: Asegúrese de utilizar protocolos estándar para comunicarse con los dispositivos IoT, como HTTP, ya que esto garantizará la compatibilidad con la mayoría de los dispositivos IoT.

- Estrategia de prueba y desarrollo: Antes de implementar los scripts en una red en producción, asegúrese de probarlos en un entorno de prueba para detectar y corregir cualquier problema.
- Sistema de control de versiones: Utilice un sistema de control de versiones como Git para controlar y rastrear los cambios en los scripts, lo que facilita la colaboración y el mantenimiento.
- Sistema de automatización de tareas: Utilice un sistema de automatización de tareas como CRON para programar la ejecución de los scripts en una hora específica o periodo de tiempo.
- Herramienta de monitorización: Utilice una herramienta de monitorización para supervisar el rendimiento y el estado de la red IoT y detectar problemas en tiempo real.
- Dispositivos de automatización de redes: Utilice dispositivos de automatización de redes, como controladores de red o gateways, para automatizar tareas en dispositivos IoT. Estos dispositivos pueden proporcionar una interfaz fácil de usar para configurar y controlar los dispositivos IoT.
- Herramienta de gestión de dispositivos: Utilice una herramienta de gestión de dispositivos para configurar y controlar los dispositivos de automatización de redes de forma remota.
- Política de seguridad: Asegúrese de tener una política de seguridad sólida en su lugar para proteger su red IoT contra posibles amenazas.
- Plataforma de administración de red IoT: Utilice una plataforma de administración de red IoT, como AWS IoT o Microsoft Azure IoT, para automatizar tareas en dispositivos IoT. Estas plataformas proporcionan una interfaz fácil de usar para configurar y controlar los dispositivos IoT.

4 REFERENCIAS BIBLIOGRÁFICA

[1] "What is Internet of Everything (Internet de Todas las Cosas)? - Definition from WhatIs.com", IoT Agenda, 2022. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Everything-IoE. [Accessed: 03- Sep- 2022].

[2] "¿Qué es la automatización de red? | Juniper Networks", Juniper Networks, 2019. [Online]. Available: https://www.juniper.net/mx/es/research-topics/what-is-network-automation.html. [Accessed: 03- Sep- 2022].

[3] "Installing and Upgrading Junos Space Software Overview | Juniper Networks", Juniper.net, 2022. [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos-space22.1/junos-space-

getting-started/topics/concept/junos-space-getting-started-applications-installing.html. [Accessed: 03- Sep- 2022].
[4] CISCO, "Cisco DNA Center 2.2.2.0", 2022.
[5] L. Amaya Fariño, J. Arroyo Pizarro, M. Jaramillo Infante, A. Tumbaco Reyes and B. Mendoza Morán, "SDN Redes definidas por Software usando MiniNet", 2022.
[6] P. Support, "Configuración de Plug and Play en los routers serie RV34x", Cisco, 2022. [Online]. Available: https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/Configuring-Plug-and-Play-in-RV34x-series-routers.html. [Accessed: 03- Sep- 2022].
[7] B. Gibbs, S. Varma, S. Hajela and R. Rahim, "Unleash Experience-First Networking with Juniper Paragon Automation | Official Juniper Networks Blogs", Official Juniper Networks Blogs, 2021. [Online]. Available: https://blogs.juniper.net/en-us/service-provider-transformation/unleash-experience-first-networking-with-juniper-paragon-automation. [Accessed: 03- Sep- 2022].
[8] Juniper, "The 2020 State of Network Automation", 2022.
[9] "Plataforma de administración de red de Junos Space | Juniper Networks", Juniper Networks, 2022. [Online]. Available: https://www.juniper.net/mx/es/products/sdn-and-orchestration/junos-space-platform.html. [Accessed: 04- Sep- 2022].
[10] "Junos Space Fabric Deployment Overview | Juniper Networks", Juniper.net, 2022. [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos-space22.1/junos-space-getting-started/topics/concept/junos-space-getting-started-fabric-deploying-overview.html#junos-space-fabric-deployment-overview__d324e73. [Accessed: 04- Sep- 2022].
[11] Paramiko.org. 2022. Welcome to Paramiko! — Paramiko documentation. [online] Available at: <https://www.paramiko.org/> [Accessed 4 September 2022].
[12] PyPI. 2022. netmiko. [online] Available at: <https://pypi.org/project/netmiko/> [Accessed 4 September 2022].
[13] Services, P. and Management, C., 2018. Cisco FindIT Network Discovery Utility Data Sheet. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/small-business-findit-network-discovery-utility/data_sheet_c78-570064.html> [Accessed 4 September 2022].
[14] Support, P. and Center, C., 2022. Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.2.2 - Review the Cisco DNA Center Appliance Features [Cisco DNA Center]. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-2/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_2_2ndGen/m_review_appliance_features_2_2_2_2ndgen.html> [Accessed 4 September 2022].
[15] Support, P. and FindIT, A., 2018. Ahorre tiempo iniciando su próximo proyecto de TI con FindIT y Network Plug and Play. [online] Cisco. Available at: <https://www.cisco.com/c/es_mx/support/docs/smb/cloud-and-systems-management/cisco-findit-network-management/smb5849-save-time-findit-network-pnp.html> [Accessed 4 September 2022].
[16] Support, P., 2019. Configuración de Plug and Play en routers RV160 y RV260. [online] Cisco. Available at: <https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/Configuring-Plug-and-Play-in-RV160-and-RV260-routers.html> [Accessed 4 September 2022].
[17] M. Faris, K. Abdullah, I. Hazwam, R Ruslan, Network Automation using Ansible for EIGRP Network. Universiti Teknologi MARA Perlis Branch, Perlis, 2021.
[18] P. Mihăilă, T. Bălan, R. Curpen, F. Sandu, Network Automation and Abstraction using Python Programming Methods, International Conference on Recent Achievements in Mechatronics, Automation, Computer Science and Robotics, Transylvania, 2017.

[19] D. Rafique, L. Velasco, Machine Learning for Network Automation: Overview, Architecture, Applications [Invited Tutorial], J. Opt. Commun. Netw. 10, D126-D143 (2018).

5 ANEXOS

Los anexos adjuntados como parte complementaria al desarrollo del presente Trabajo de Integración Curricular se observan a continuación:

ANEXO I. Cuadro comparativo de la Automatización.

ANEXO I. Cuadro comparativo de la Automatización