PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN



DISEÑO Y SIMULACIÓN DE UNA RED DE TRES CAPAS EN GNS3 PARA LA CREACIÓN DE VLANS CON HERRAMIENTAS DE AUTOMATIZACIÓN DE PYTHON

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR
PASTRANO IBARRA OSCAR DAVID

TUTOR
MGTR. EDISON MORA

QUITO, 2022

DEDICATORIA

A mis padres, mis hermanas, familiares y amigos que estuvieron a mi lado brindándome su apoyo incondicional les dedico este logro importante en mi vida.

AGRADECIMIENTO

Agradezco a mis padres, mis hermanas y familiares que por sus sacrificios, esfuerzo y apoyo hicieron este sueño realidad. A la PUCE y a todos los docentes que durante mis estudios se convirtieron en guías y ejemplos para mi vida personal y profesional. Un agradecimiento especial a aquellos que participaron en mi proyecto de titulación e influyeron de manera directa en la culminación de mi carrera de grado: Mgtr. Charles Escobar, Mtgr. Edison Mora, PhD. Henry Roa, Mgtr. Suyana Arcos, PhD. Susana Masapanta, Ing. Xavier Vásquez, PhD. Nelson Salgado y Mgtr. Damián Nicolalde.

RESUMEN

El mundo de las redes de computadores evoluciona a pasos agigantados y lo hace cada vez acercándose a las distintas aplicaciones de virtualización, de monitoreo y de automatización. Muchas empresas pueden aprovechar y beneficiarse de este tipo de software, pero si no cuentan con los recursos para adquirirlas están un paso por detrás de la competencia. Gracias a Python: a las herramientas de código abierto y las librerías que se encuentran en constante desarrollo se puede implementar software que permita automatizar y monitorear procesos en infraestructura de red y para ello se utiliza una simulación de topología jerárquica de tres capas con el desarrollo de una aplicación que crea VLANs y configura una serie de protocolos de forma automática.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS III

ÍNDICE DE TABLAS V

CAPÍTULO I: INTRODUCCIÓN 1

1.1. Justificación 1

1.2. Planteamiento del problema 1

1.3. Objetivo General 2

1.4. Objetivos Específicos 2

1.5. Antecedentes 3

1.6. Alcance 5

1.7. Metodología 5

CAPITULO II: FUNDAMENTACIÓN TEÓRICA 6

2.1 Diseño de redes 6

2.1.1. Red de campus 6

2.1.2. Topología jerárquica 7

2.2. Switching 9

2.3. Routing 10

2.3.1. OSPF 12

2.4. DHCP 12

2.5. VTP 13

2.6. Spanning Tree Protocol, STP 13

Capitulo III: Implementación 15

3.1. Requerimientos Iniciales 15

3.2. Topología 18

3.3. Configuración de protocolos 21

3.3.1. Capa de Core 21

3.3.2. Capa de Distribución 23

3.3.3. Capa de Acceso 25

3.4. Software de Automatización 26

3.5. Pruebas de funcionamiento 28

Capitulo IV: Conclusiones y Recomendaciones 36

5.1. Conclusiones 36

5.2. Recomendaciones 37

REFERENCIAS 39

ÍNDICE DE FIGURAS

Figura 1 7

Figura 2 8

Figura 3 15

Figura 4 16

Figura 5 17

Figura 6 17

Figura 7 18

Figura 8 20

Figura 9 20

Figura 10 26

Figura 11 27

Figura 12: 27

Figura 13: 27

Figura 14 28

Figura 15 29

Figura 16 29

Figura 17 30

Figura 18 30

Figura 19 31

Figura 20 32

Figura 21 32

Figura 22 33

Figura 23 33

Figura 24 34

Figura 25 35

ÍNDICE DE TABLAS

Tabla 1 10

Tabla 2: 11

Tabla 3 19

CAPÍTULO I: INTRODUCCIÓN

1.1. JUSTIFICACIÓN

Hace dos décadas el mundo de las redes de computadoras podía considerarse una elite ya que se debía contar físicamente con equipos de red para adquirir conocimientos y experiencia. Esto se lograba solamente con una inversión económica considerable o con un puesto de trabajo en el área de infraestructura. Gracias a software como Cisco Packet Tracer y GNS3 se puede, de manera gratuita, poner en práctica los conocimientos teóricos sobre redes. Se aprovecha esta ventaja y se plantea ir un paso más allá mediante la implementación de una topología jerárquica usada en el sector empresarial.

Mediante esta simulación se configurarán los protocolos de red más relevantes para las comunicaciones entre dos redes LAN. La evolución tecnológica permite que cada vez más usuarios estén conectados a internet por lo que la disponibilidad es un factor crítico. Para minimizar los riesgos de caídas de la red se desarrollan técnicas de redundancia que también son consideradas en el proyecto. Se considera además la importancia del uso de herramientas de automatización para un uso eficiente de los recursos de las organizaciones de sin importar su tamaño.

1.2. PLANTEAMIENTO DEL PROBLEMA

La escalabilidad de la infraestructura de red es un reto al que deben enfrentarse las empresas desde sus inicios. Definir el número de dispositivos, marcas y topología es crucial ya que de ello depende la capacidad de crecimiento de la red. Las empresas deben garantizar la disponibilidad de las comunicaciones de red a sus usuarios a la vez que mantienen una estructura definida cuando se añadan dispositivos a la infraestructura. Por ello, la topología jerárquica es una de las opciones más usadas por las empresas.

Existen las opciones de dos y tres capas de acuerdo al tamaño de la organización, siendo la última la más costosa y compleja, aunque brinda mayores beneficios. Esta topología cuenta con las capas de core, distribución y acceso con varios dispositivos en cada una de ellas. Normalmente los protocolos implementados se repiten en todos los equipos de la misma capa. Puede convertirse en una tarea repetitiva e incrementar la probabilidad de cometer errores a medida que se agregan equipos en la red.

No todas las empresas pueden administrar este tipo de topologías debido a los recursos que se requieren. Aquellas que cuenten con un capital importante pueden adquirir software de administración y monitoreo para así facilitar el control de su red. Lamentablemente para las organizaciones que no puedan adquirir este tipo de software las tareas como creación de VLANS y visualización de las configuraciones de los equipos pueden tomar varias horas por dispositivo. Si existen varias localidades cada tarea se dificulta aún más.

1.3. OBJETIVO GENERAL

Diseñar y simular una red de tres capas en GNS3 para la creación de VLANs con herramientas de automatización de Python

1.4. OBJETIVOS ESPECÍFICOS

- Identificar cada uno de los componentes que se requieren para la implementación de una red de tres capas.
- Analizar la topología de red que conecta dos LAN de modelo jerárquico de tres capas mediante el software GNS3.
- Aplicar conceptos y herramientas de automatización mediante scripts de Python para la creación de VLANs en una topología de tres capas.

1.5. ANTECEDENTES

El presente trabajo está enfocado en las topologías que pueden ser encontradas en el sector empresarial donde se busca alta disponibilidad de los servicios mediante equipos con conexiones redundantes. Una configuración compleja que requiere de muchos recursos, pero permite a la organización escalar su red de manera más rápida. Por otra parte, el departamento técnico debe enfrentarse a distintos retos entre los cuales se encuentran los procesos repetitivos y es ahí donde las herramientas automatización juegan un papel vital ya que ahorran tiempo y permiten que la organización retome su ritmo de funcionamiento normal en menor tiempo cuando se presentan problemas. Por ello se toma como referencia trabajos previos como son:

Una propuesta de nueva plataforma de gestión de redes para la programación y automatización de redes con implementación en GNS3 donde Boumezrag A. (2020) desarrolla una aplicación por consola que denomina “Plataforma de administración de red” usada para configurar equipos en la red con una topología implementada en un entorno virtual. Desarrolla una comparación entre las distintas alternativas para las tareas de automatización que finalmente finaliza con su elección en base a la capacidad de personalización y adaptación de scripts de Python con la librería Netmiko. Muestra las ventajas y la necesidad de implementar un proceso de automatización para configurar equipos que una empresa en base a la cantidad de los mismos puede llegar a ser inmanejable o generar problemas.

Automatización y abstracción de redes usando métodos de programación con Python elaborada por Mihaila, Balan, Cupren y Sandu (2017) que identifican la constante evolución tecnológica y como esta afecta a las organizaciones a la hora de administrar sus equipos de red ya que pueden provenir de distintos fabricantes y requieren optimizar el tiempo en el que el personal configura y pone en funcionamiento estos equipos. Consideran también la

importancia que se brinda a la virtualización y como las Redes Definidas por Software buscan que las herramientas de automatización permitan a las empresas optimizar el uso de sus recursos. Realizan una comparativa entre las herramientas Paramiko, Netmiko y Napalm para finalizar con los beneficios que obtendrían las organizaciones al implementar estos procesos.

Automatización de procesos en redes de datos mediante programación en Python, trabajo realizado por Gallegos y Mayorga (2020) pero forma parte de un proyecto de gran escala que junta a varios profesionales de varias universidades del país y dan como resultado al "Libro de investigación apropiación, generación y uso edificador del conocimiento de estudiantes sentipensantes" dirigido por la Universidad Israel y EDIPE. El trabajo busca promover el uso de las nuevas tecnologías y la adaptación de procesos automatizados para la configuración de los equipos de red.

Se enfocan en las tareas mecanizadas que la mayoría de organizaciones realizan y como los scripts de Python pueden ayudar a optimizar tiempo y recursos mediante librerías que permiten enviar varios comandos a varios dispositivos a la vez. Analizan además tareas de criptografía para proteger los archivos de configuración de accesos no autorizados, así como también identificación de errores que pueden producirse a la hora de ejecutar las tareas de automatización.

Finalmente se considera el proyecto Automatización de procesos en redes de datos mediante programación en Python por Conde (2020) desarrollado principalmente para dar a conocer las herramientas disponibles para automatización en el área de redes y como el uso de la consola de comandos o CLI ralentiza los procesos de configuración en las organizaciones. Desarrolla también a modo de guía una introducción a las librerías más usadas de Python, así como también los modos de conexión disponibles en conjunto con las ventajas y desventajas de cada una.

1.6. ALCANCE

El proyecto tiene un alcance descriptivo por lo que se centra en diseñar y simular una topología jerárquica de tres capas en el software GNS3 en la que se implementará un proceso de automatización para la creación de VLANs. La topología estará formada por dos redes LAN interconectadas por un enlace principal. Se usarán imágenes de switches multicapa con sistema operativo Cisco iOS y vpc's para probar la comunicación entre las dos redes. La implementación de varios protocolos en la topología serán la base para el uso de las herramientas de automatización con Python.

Debido a las prestaciones del equipo donde se desarrolla el proyecto, no se podrán agregar más elementos a la simulación para que su funcionamiento sea fluido. Se configurará una máquina virtual que será el único equipo de administración de la red y también servirá de servidor de la aplicación web para automatizar la creación de VLANs. Los switches de la capa de acceso cuentan con cuatro tarjetas de red donde solo una está libre para la creación de una única VLAN mediante el software desarrollado.

1.7. METODOLOGÍA

El estudio se realiza utilizando un enfoque cuantitativo deductivo que comienza con el análisis de las fuentes bibliográficas que en lo posterior se traslada a un caso particular. Se analizan los protocolos de red necesarios para comunicar dos redes LAN además de las herramientas necesarias para llevar a cabo una simulación. Una vez se definan los elementos que implican el área de investigación seleccionada, se aplicarán para deducir su funcionamiento en el caso específico de creación de VLANs de manera automática en una topología jerárquica de tres capas.

CAPITULO II: FUNDAMENTACIÓN TEÓRICA

2.1 DISEÑO DE REDES

Como lo explican expertos de Cisco en una de sus publicaciones de la serie “Diseños Validados por Cisco” se pueden llegar a considerar a las redes de computadoras como sistemas de fontanería. En cierto modo tiene validez usar esta analogía debido a las similitudes entre el fluido del agua y los electrones a través de las tuberías y los cables respectivamente. Pero diseñar un sistema de distribución de agua conlleva analizar el tamaño de la edificación, las personas que lo utilizarán, mecanismos de protección, etc. al igual que en las redes de computadoras, (Cisco CVD, 2020). El diseño seleccionado debe contemplar la mayor cantidad de eventos riesgosos y plantear soluciones preventivas y correctivas.

Para las organizaciones la información es uno de sus activos más importantes y su integridad depende de la red. Por ello, la topología definida debe ser lo más confiable y segura posible. La versatilidad es otro aspecto importante ya que la red requiere cambiar y adaptarse de acuerdo a la situación economía de la empresa, (Cisco CVD, 2020). Para el diseño de una topología se pueden considerar los siguientes conceptos:

2.1.1. Red de campus

Horn (s.f.) describe a las redes de campus como un conjunto de redes LAN distribuidas en la misma área geográfica. Sin importar su tamaño, la característica principal es la conectividad entre varias edificaciones. Destaca además la versatilidad que brinda para realizar modificaciones a la red de acuerdo a las necesidades de los usuarios. Al tratar la red como un conjunto de LANs su administración es más sencilla.

El término hace referencia principalmente a un campus universitario, que consta de varios edificios y construcciones, ocupando un espacio considerable. A pesar de estar formado por varias facultades y departamentos todos pertenecen a la misma institución,

(Merriam-Webster, s.f.). A pesar de ello, cada edificio tiene su propia infraestructura y la comunicación se mantiene en la edificación siempre y cuando no se requiera enviar o recibir datos a otro departamento o facultad. De esta manera se aprovecha al máximo el potencial de cada red LAN y se utiliza de forma eficiente la capacidad de velocidad de transmisión, (Cloudflare, s.f.).

2.1.2. Topología jerárquica

Cuando en una organización crece el número de usuarios y requiere conectar varios departamentos, una de las soluciones más populares para el diseño de la red es la topología jerárquica. Consiste en agrupar dispositivos y segmentar la carga de trabajo en grupos o capas. Esta distribución brinda mejoras y ventajas a la hora de desplegar y administrar la red. De esta forma el diseño se puede replicar en todas las localidades de una organización o campus con la capacidad de escalabilidad y adaptabilidad que brinde los mayores beneficios, (Cisco CVD, 2013).

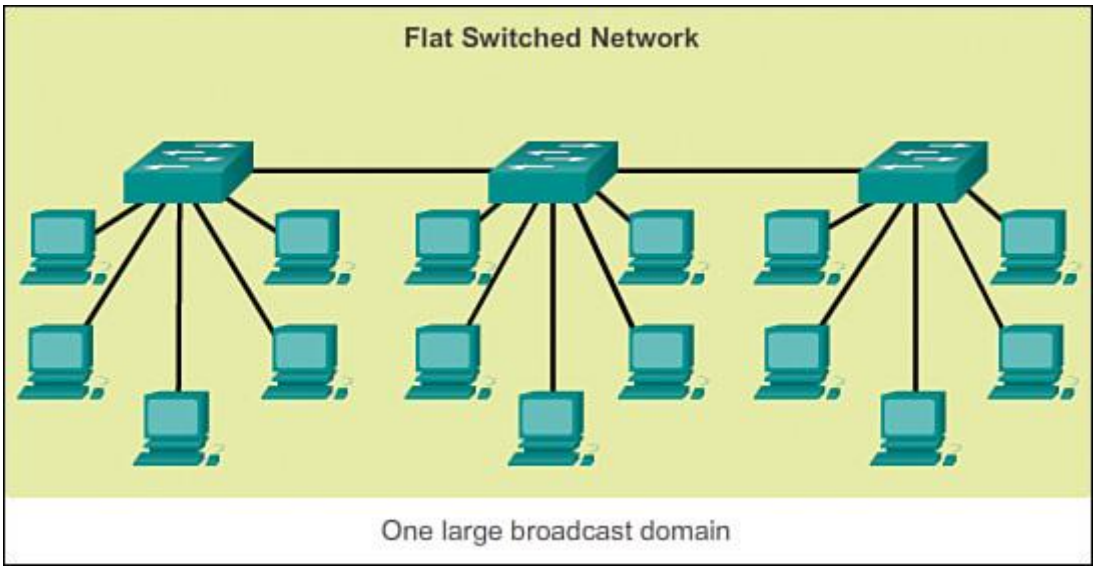
Por lo general, el tamaño de una red empresarial se clasifica por el número de dispositivos conectados y son:

- Redes Pequeñas: Conectan hasta 200 dispositivos
- Redes Medianas: Conectan entre 201 y 100 dispositivos
- Redes Grandes: Conectan a más de 1000 dispositivos

Cuando una red supera los 100 usuarios conectados, la administración puede llegar a ser demandante y compleja si su topología usa un diseño “Plano de switches” como se muestra en la figura 1. Es un diseño que agrega hubs o switches de manera continua conforme se incorporan más dispositivos. Esta topología es propensa a sufrir fallas críticas de comunicación y problemas de administración altamente complejos, estos eventos los resuelve la topología jerárquica representada en la figura 2, (Cisco Press, 2014).

Figura 1

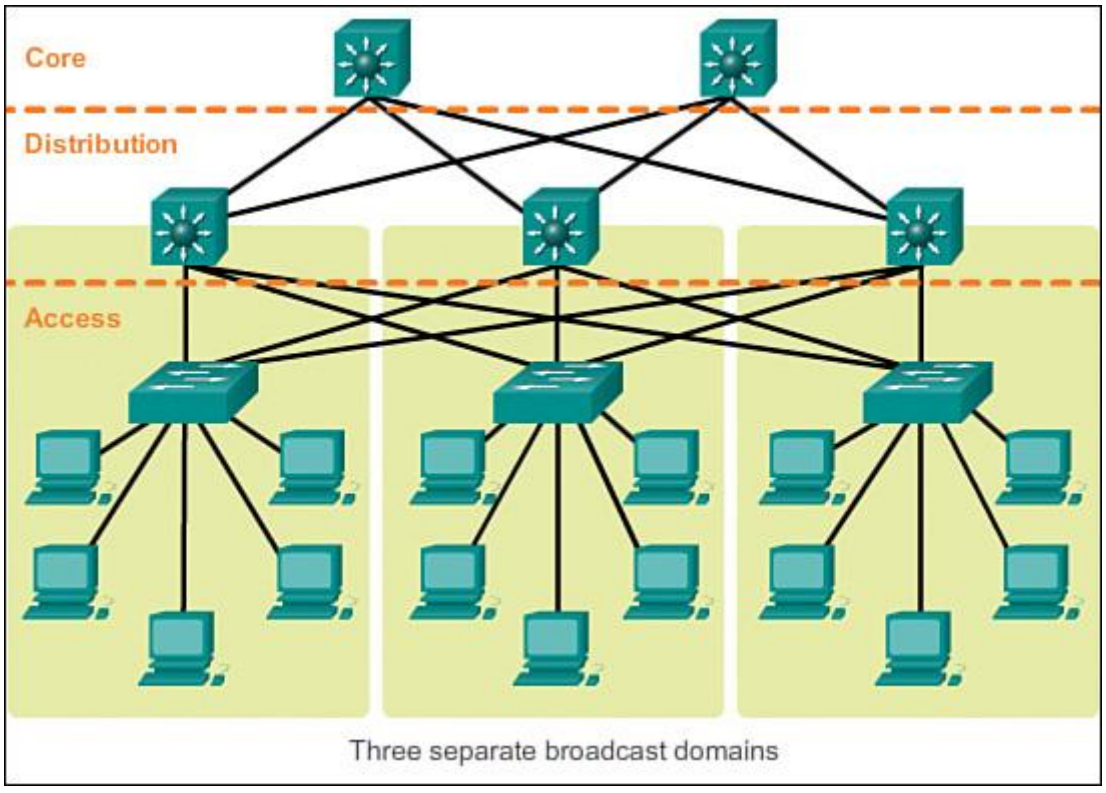
Topología con diseño Plano de Switches



Fuente: Cisco Press. (2014)

Figura 2

Topología con diseño Jerárquico



Fuente: Cisco Press. (2014)

Se describen a continuación cada una de las capas de la topología jerárquica:

Capa de Acceso: Por lo general se colocan switches de capa 2 con la mayor cantidad de puertos posible ya que en estos equipos se conectan los dispositivos de usuario final. Aquí se configuran los puertos de acceso para todas las VLAN que el diseño de la red lo requiera. También se realizan configuraciones para filtrar el tráfico, mejorar el rendimiento y optimizar el uso de los enlaces, (Ariganello & Barrientos, 2014).

Capa de Distribución: Esta formada por switches multicapa ya que es el primer equipo que interconecta el tráfico de los equipos de la capa inferior. La característica principal son los puertos de alta velocidad ya que este nivel es el canal intermedio de la topología y aquí se realizan configuraciones de calidad de servicio y lista de control de acceso, (Ariganello & Barrientos, 2014).

Capa de Core: Se utilizan solamente switches multicapa con conexiones redundantes y de las más altas prestaciones. Esta capa se encarga de la conexión entre las redes existentes en una zona del campus con el exterior o las redes públicas. Se busca principalmente tres características en este nivel: alta velocidad de transmisión, tolerancia a fallas y fácil escalabilidad, (Cisco Press, 2014).

2.2. SWITCHING

VLAN: El término LAN (Red de área local, Local Área Network) hace referencia a un conjunto de dispositivos conectados entre sí mediante un enlace común. Los elementos de una LAN pueden agruparse de manera lógica mediante VLANs (Red de Área Local Virtual) con el mismo hardware. Son consideradas redes LAN que se pueden administrar con políticas diferentes entre ellas. La ventaja principal es la seguridad ya que el tráfico está aislado en cada VLAN permitiendo formar redes más robustas, (Abdulahad, 2018).

El proceso de creación de VLANs consiste en asignar los puertos físicos del switch a la VLAN definida en la topología. Se puede realizar de forma individual o a través de rangos de puertos. Aquellos que tengan acceso a equipos de usuario final serán denominados puertos

de acceso y el resto como puertos troncales, (Empson, 2016). Se muestra a continuación los comandos para crear una VLAN y asignar sus puertos.

Tabla 1

Comandos para la asignación de puertos a una VLAN

Forma individual	
Switch (config) # interface fastethernet 0/1	Accede al modo de configuración de la interfaz
Usando rangos	
Switch (config) # interface range fastethernet 0/1-9	Accede al modo de configuración del rango de interfaces
Creación de la VLAN	
Switch (config-if) # switchport mode access	Configura el puerto en modo acceso
Switch (config-if) # switchport access vlan 10	Asigna el puerto a la vlan 10

Fuente: Empson, 2016

La creación de VLANs se puede realizar solamente en switches, ya sean de capa 2 que trabajan con direcciones MAC o switches multicapa que pueden trabajar con direcciones IP. A diferencia de los obsoletos HUB, un switch envía información a los dispositivos conectados, pero sin interferir en el tráfico de otros equipos. Han evolucionado tanto que pueden ser usados como routers o como switches debido a las funciones incorporadas y la velocidad de transmisión ya que cuentan con puertos multigigabit. Actualmente incorporan características de firewalls dedicados, machine learning y demás ventajas que son aprovechadas por las redes empresariales, (Cisco, 2022).

2.3. ROUTING

Es el proceso en el que un router calcula la mejor ruta para direccionar el tráfico de una red a otra. Se considera el número de saltos intermedios, la velocidad de transmisión, la calidad de los enlaces, etc. para seleccionar la ruta por la cual se enviarán los paquetes. Almacenan información sobre las rutas hacia las redes con las que puede trabajar en un espacio de memoria llamado Tablas de enrutamiento. La información que maneja puede ser

estática o dinámica y existen varios protocolos con características específicas para cada situación, (Cloudflare, 2022).

Las tablas de enrutamiento también se conocen como Información Base de Enrutamiento (RIB, Routing Information Base). En cuanto al enrutamiento estático se puede realizar de forma Default o por Defecto en donde se redirige todo el tráfico por un solo router, normalmente utilizada en redes pequeñas con pocos dispositivos. También se puede realizar agregando de forma manual las rutas y sus destinos en la RIB cuando la topología es pequeña. Por otro lado, mediante el enrutamiento dinámico, la información se almacena mediante cálculos automáticos de algoritmos y protocolos existentes, (Vardy, .2015).

Un router decide la mejor ruta para direccionar los paquetes basándose en los valores de la Distancia Administrativa (AD, Administrative Distance). Son valores preestablecidos entre 0 y 255, mientras el valor es más bajo significa que la ruta es más confiable y rápida. Aunque la configuración de enrutamiento estático toma más tiempo que realizarlo de forma dinámica, es el tipo de enrutamiento que cuenta con el segundo menor valor de AD, por lo tanto, un router siempre dará prioridad a esta ruta por encima de las disponibles mediante enrutamiento dinámico, (Carthern et al., 2015). Se muestra a continuación los valores de AD y los protocolos de enrutamiento disponibles:

Tabla 2:

Protocolos de enrutamiento y valores de la distancia administrativa (AD).

Protocolo	AD
Interfaz conectada	0
Ruta Estática	1
EIGRP	5
BGP Externo	20
BGP Interno	90
IGRP	100
OSPF	110

IS-IS	115
RIP	120
EGP	140
ODR	160
EIGRP Externo	170
EIGRP Interno	200
Desconocido	255

Fuente: Carthern et al, 2015

2.3.1. OSPF

Permite realizar enrutamiento dinámico y se encuentra en la categoría de protocolos de “Estado de Enlace” o “Ruta más rápida primero, Shortest path first” y utiliza el algoritmo Dijkstra, uno de los más importantes en la teoría de grafos. Es un protocolo que no está asociado ni le pertenece a ninguna organización por lo que su uso se extiende a nivel mundial y puede ser implementado en la mayoría de dispositivos sin importar su fabricante. Es el remplazo directo del protocolo RIP superando ampliamente su rendimiento, capaz de trabajar con VLSM brindando una administración de direcciones eficaz y el uso de áreas de enrutamiento que ayudan a reducir el impacto en el rendimiento del CPU y memoria del dispositivo, (Doyle, 2005). Sus características y ventajas sobre otros protocolos fueron las que influyeron para elección de OSPF como el protocolo de enrutamiento dinámico en la implementación del proyecto.

2.4. DHCP

Cada dispositivo dentro de una red requiere de un identificador único e irrepetible para comunicarse con los demás equipos, este identificador se denomina dirección IP (Internet Protocol). Cuando la topología es reducida se pueden asignar direcciones IP de forma manual sin mayores inconvenientes. Realizar este proceso manual en una red de campus no es viable por el tiempo que tomaría y los inconvenientes que puede causar cuando la red esté en funcionamiento. Por ello existe el protocolo DHCP para encargarse de la

asignación de direcciones de forma automática junto con información adicional como la máscara de la red y la puerta de enlace, (Microsoft Docs, 2021).

En los routers de Cisco y de otros proveedores se puede habilitar la funcionalidad de servidor DHCP con la posibilidad de modificar varios parámetros, (Carthern et al. 2015), como:

- Dirección IP
- Mascara de red
- Puerta de enlace
- Tiempo mínimo de conexión
- Tiempo de caducidad de la IP
- Servidor DNS
- Nombre del dominio

2.5. VTP

VTP (VLAN Trunking Protocol) es un protocolo que funciona en la capa de enlace de datos y permite administrar las VLAN que se encuentren en un Dominio VTP o VTP Domain. VTP ayuda al administrador de la red a reducir el riesgo de cometer errores o crear inconsistencias con la información de las VLANs como nombres duplicados o números fuera de rango. Por lo general se lo implementa en switches de capa 2 o multicapa y requiere de conexiones troncales para replicar la información de las VLANs existentes (Cisco Catalyst Guide, s.f.). Es de gran utilidad ya que las configuraciones principales serán enviadas y almacenadas en los demás equipos reduciendo el uso de los recursos, pero por otra parte se debe tener cuidado ya que un error puede generar que la falla se replique en toda la red.

2.6. SPANNING TREE PROTOCOL, STP

Cuando existen conexiones en bucle con switches se puede provocar que el tráfico se transmita de forma infinita saturando la red y provocando una caída del rendimiento. El

protocolo STP evita estos bucles bloqueando interfaces y así los paquetes viajen sin interrupciones debido a este tipo de conexiones. Los bucles son necesarios en las topologías ya que permiten incrementar la redundancia y la tolerancia a fallas, pero es de vital importancia implementar el protocolo STP para evitar problemas en la transmisión de datos. Su funcionamiento se basa en la selección de un equipo denominado “Root Bridge” donde todos sus puertos están activados para enviar y recibir información mientras que en el resto de puertos de los demás equipos se calcula mediante un valor de prioridad cuales serán bloqueados para evitar bucles, (Carthern et al. 2015).

CAPITULO III: IMPLEMENTACIÓN

3.1. REQUERIMIENTOS INICIALES

El software base para la implementación del proyecto es GNS3 para la simulación de la red jerárquica y VirtualBox para la administración de las máquinas virtuales. Las especificaciones del equipo donde se ejecuta el proyecto definen el límite de las prestaciones de la simulación, la cantidad de memoria y la velocidad de lectura/escritura del disco duro son de vital importancia para el correcto funcionamiento de la implementación. Se detalla a continuación las características más relevantes del equipo utilizado:

- Procesador Intel i7 UVL 2 núcleos 3ra generación
- Memoria RAM 12GB DDR3
- Disco Duro 500GB 7200RPM

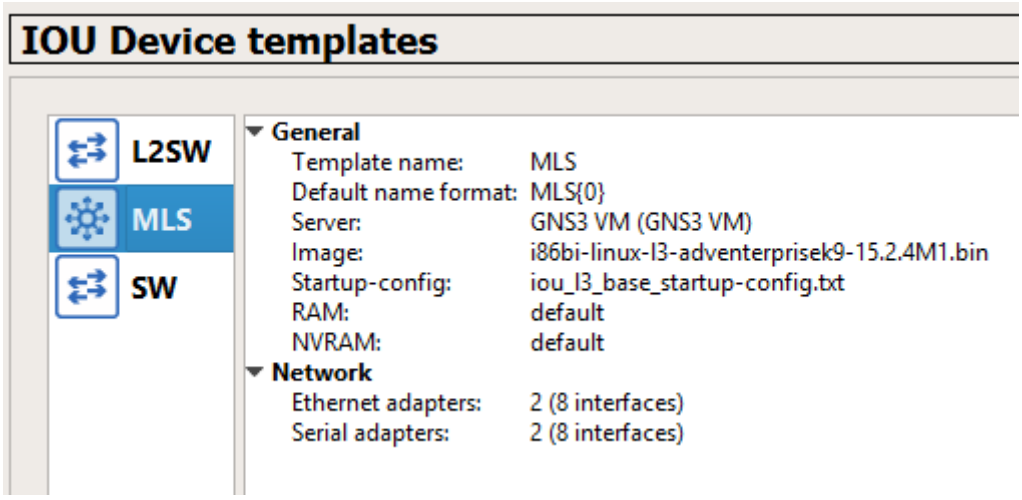
En cuanto a los detalles del software implicado además de las aplicaciones para simulación de redes y virtualización se detallan las versiones a continuación:

- Windows 8.1 x64
- GNS3 2.1.21 x64
- Oracle VirtualBox 6.1.28

La topología requiere de imágenes con el sistema operativo Cisco iOS y que cuenten con las funcionalidades necesarias para las configuraciones de red definidas previamente. Se cargan en GNS3 dos archivos que son utilizados para simular los equipos de cada capa de la red.

Figura 3

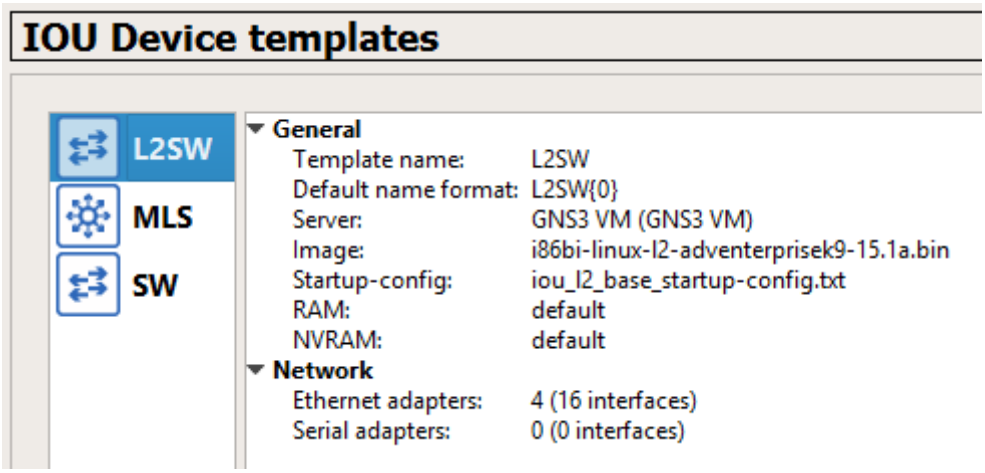
Información del archivo correspondiente a la imagen de un Switch multicapa de Cisco



Fuente: Autor

Figura 4

Información del archivo correspondiente a la imagen de un Switch capa 2 de Cisco

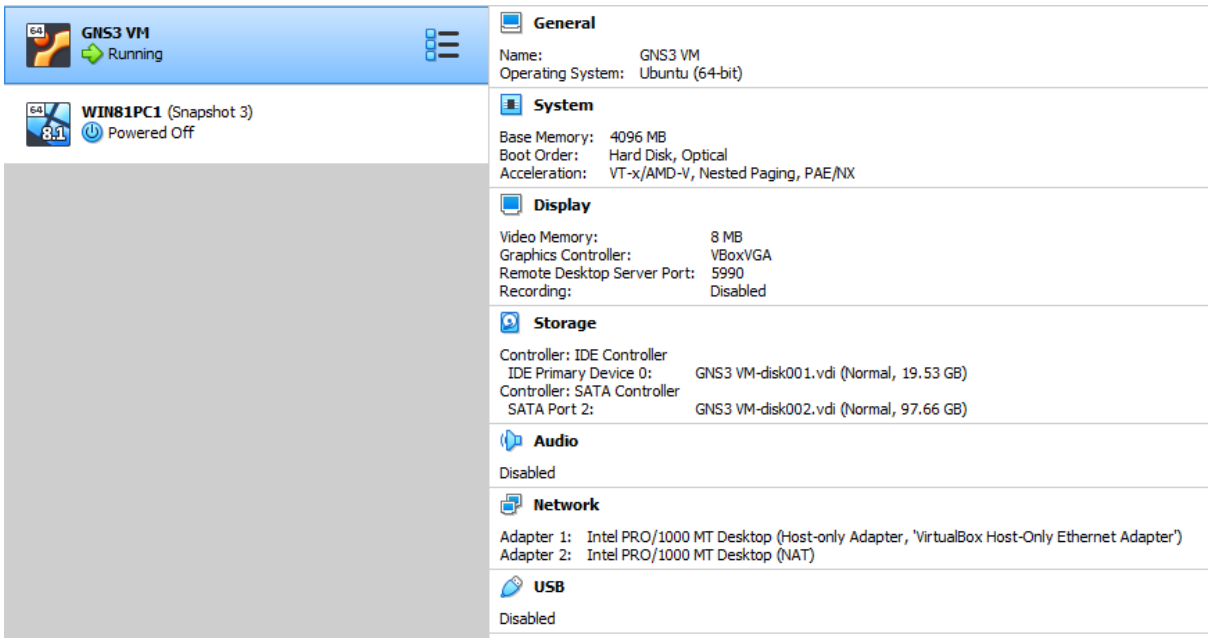


Fuente: Autor

Para mejorar el rendimiento de GNS3 y para utilizar la imagen de un switch multicapa se requiere de una máquina virtual del mismo software para que se encargue de la carga de trabajo de los equipos de red y así optimizar la simulación, (GNS3 Docs, s.f.). Se recomienda el uso del software de virtualización de VMware por sus prestaciones y características, pero consumen más recursos del hardware empleado. La parte medular del proyecto se encuentra en la simulación y automatización de la red por lo que VirtualBox brinda las características básicas necesarias para llevar a cabo la implementación del proyecto.

Figura 5

Máquina virtual de GNS3 cargada en VirtualBox

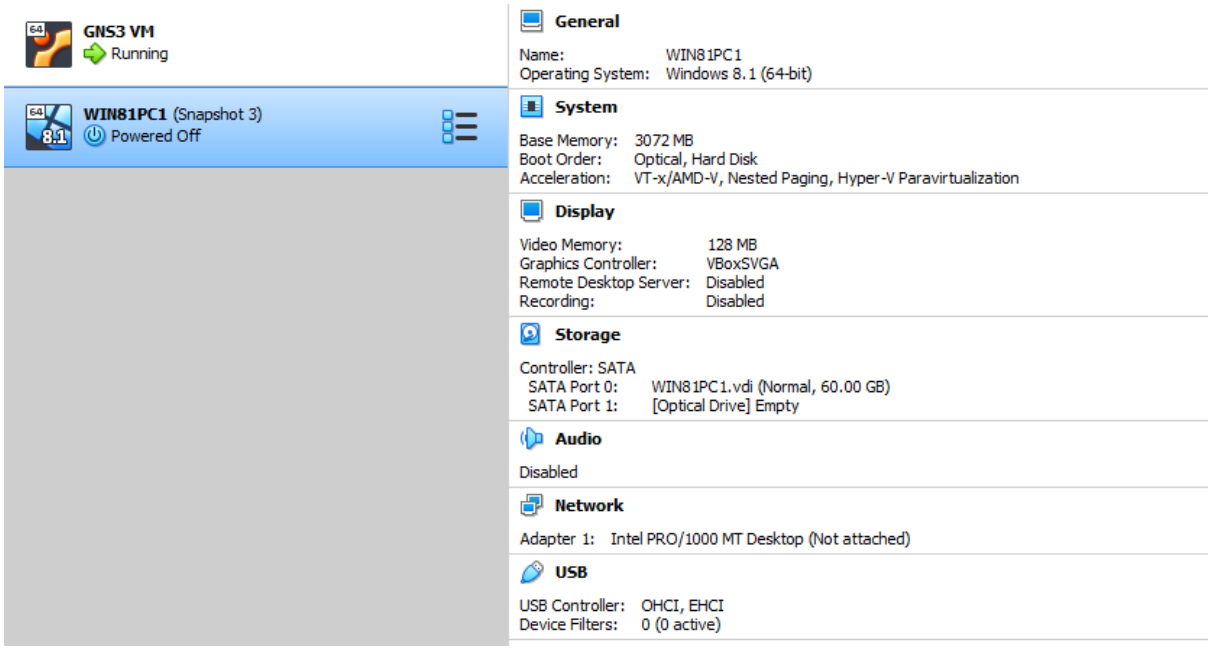


Fuente: Autor

Se utiliza una máquina virtual adicional que se designa como equipo de administración de la red. Contiene además la aplicación de automatización desarrollada que tiene acceso a todos los dispositivos de la topología. Como recomendación de buenas prácticas y prevención de errores se debe instalar una aplicación por máquina virtual, pero motivos prácticos en este caso coexisten dos en una MV. Los recursos asignados a este equipo se detallan en la siguiente figura:

Figura 6

Máquina virtual para la administración de la red y ejecución de la aplicación de automatización



Fuente: Autor

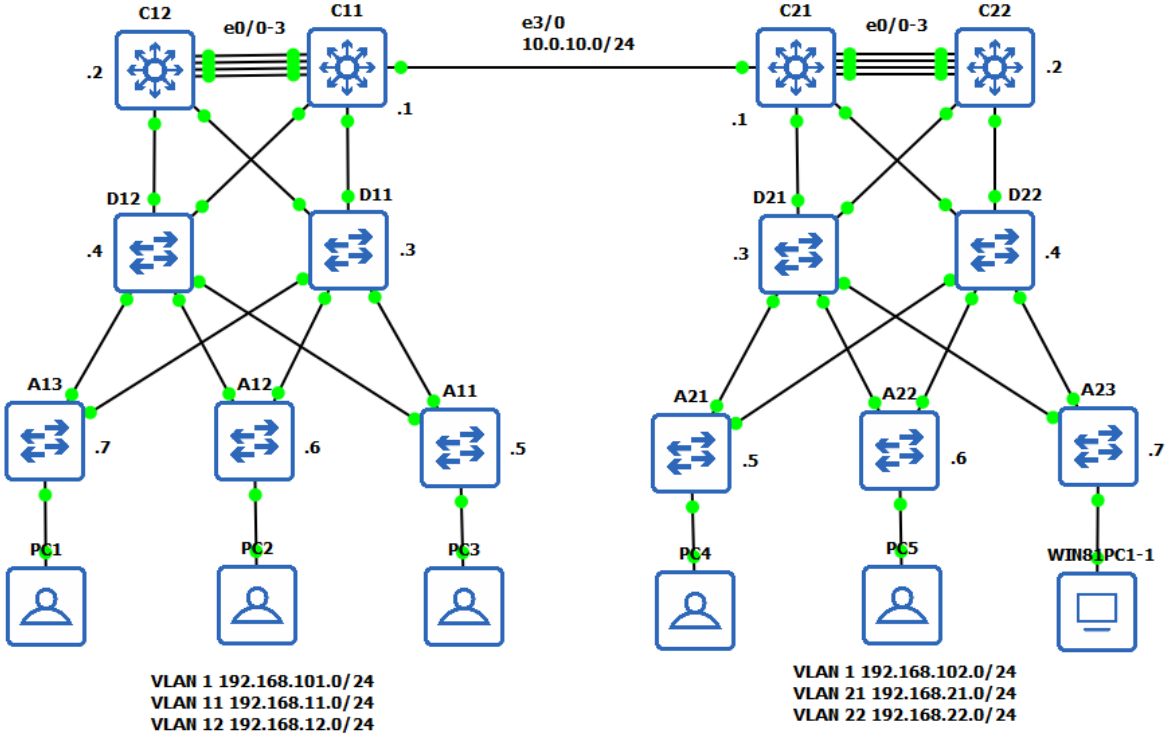
3.2. TOPOLOGÍA

Consta de dos redes LAN denominadas LAN 1 a la izquierda y LAN 2 a la derecha en la figura 7. Se utilizan 4 switches multicapa en el primer nivel o Core, 4 switches capa 2 en el nivel de Distribución y 6 switches capa 2 en el nivel de Acceso.

Los equipos identificados con el nombre PC desde el número 1 hasta el 5 son VPC (Virtual Personal Computer) que cuenta con las funcionalidades básicas para probar la conectividad en la red. Se les puede agregar una dirección IP de forma estática y dinámica, en este caso serán configuradas con el protocolo DHCP implementado en el equipo de Core de cada LAN. La máquina virtual principal que cuenta con el software de automatización se denomina WIN81PC1 y está conectada en el último switch de acceso de la red LAN 2.

Figura 7

Topología de la red implementada en GNS3



Fuente: Autor

La nomenclatura utilizada para nombrar los equipos en la topología se describe a continuación:

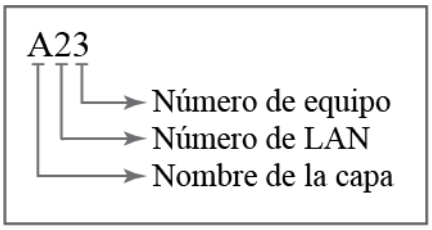


Tabla 3

Descripción de nomenclatura usada en los equipos de la topología

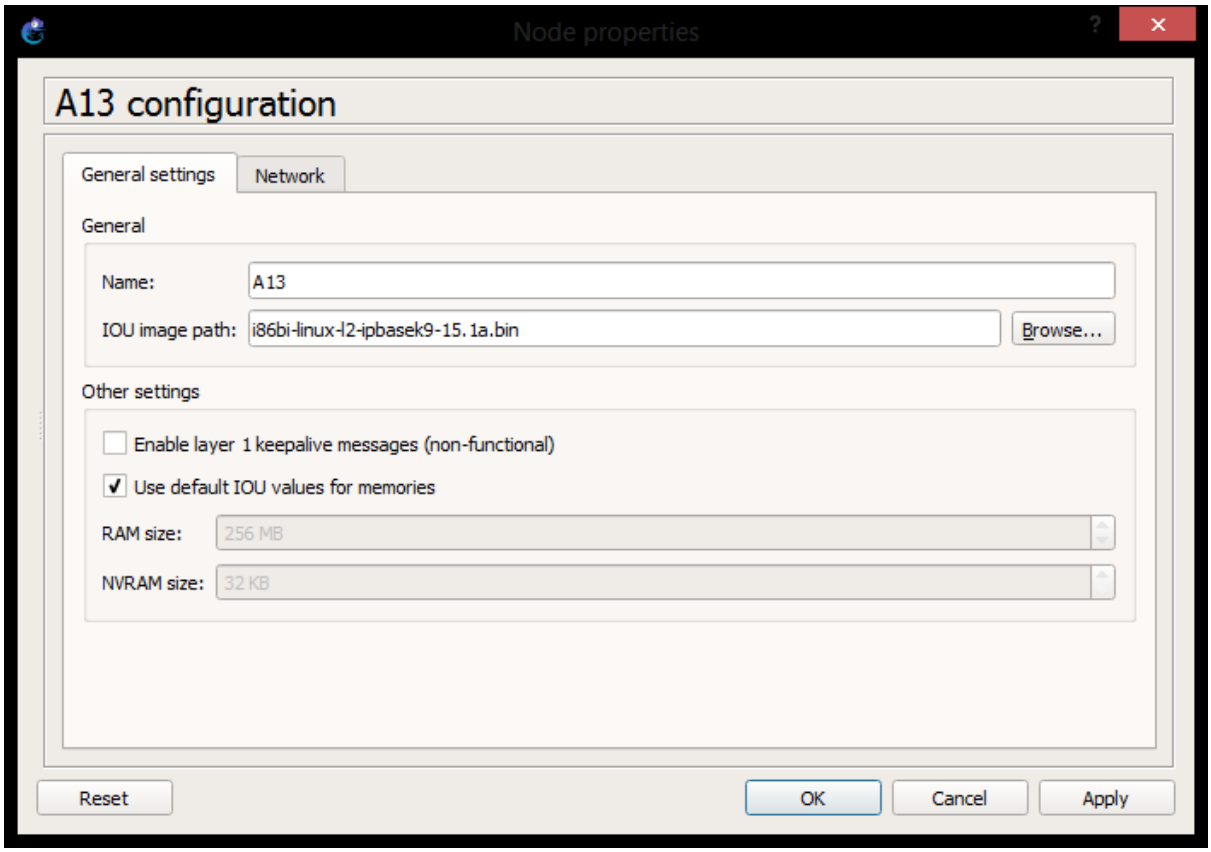
Capa	Core	C
	Distribución	D
	Acceso	A
LAN	1	
	2	

Fuente: Autor

Los dispositivos de red funcionan con las configuraciones por defecto solo con la modificación del icono que los representa. En cuanto a los equipos de la capa de acceso se requiere de 4 tarjetas de red donde cada una tiene una funcionalidad especifica. La primera NIC se utiliza para las conexiones con los dispositivos de red mientras que las demás corresponden a cada VLAN.

Figura 8

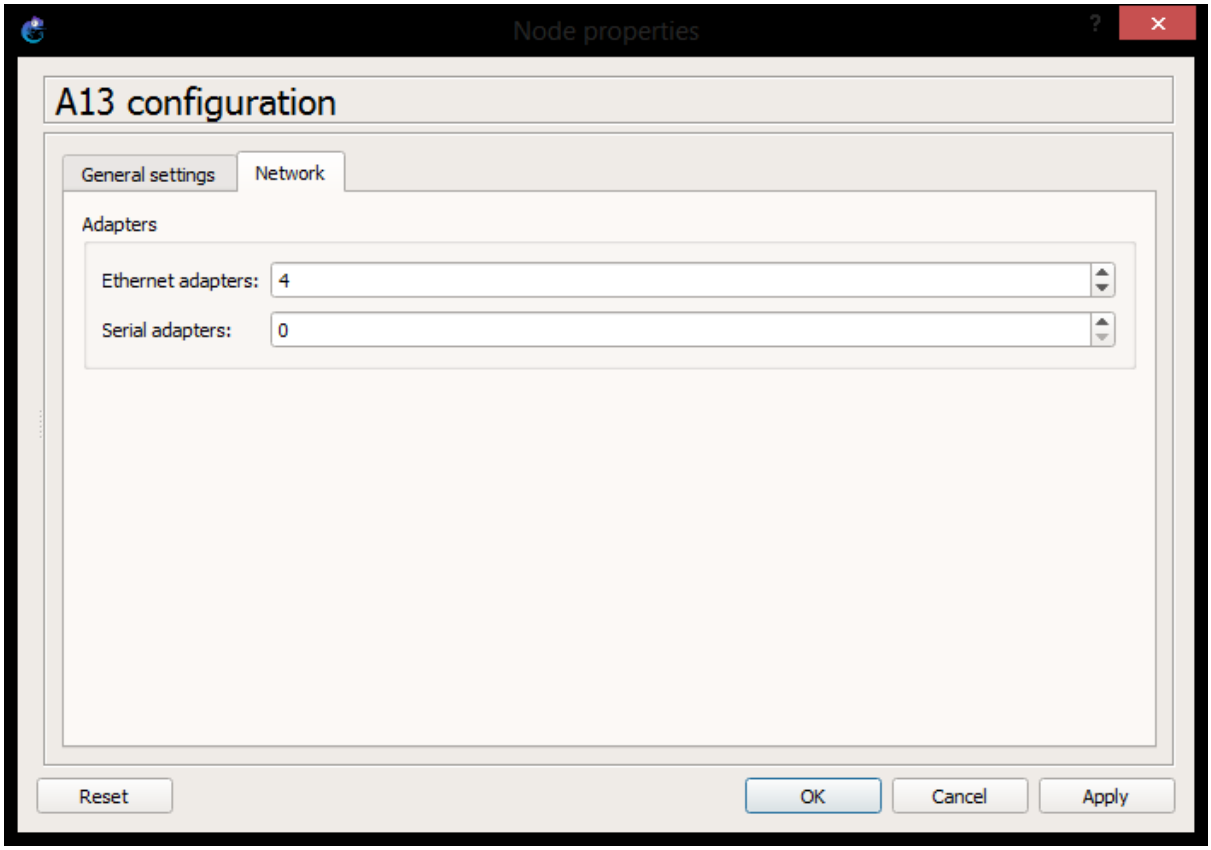
Configuración básica de switch de acceso 3 de la red LAN 1



Fuente: Autor

Figura 9

Configuración de las tarjetas de red del switch de acceso 3 de la red LAN 1



Fuente: Autor

3.3. CONFIGURACIÓN DE PROTOCOLOS

3.3.1. Capa de Core

Los protocolos principales del nivel son DHCP, OSPF, InterVLAN Routing y Port Channel. La configuración realizada en este nivel permite la comunicación entre los dispositivos de la LAN 1 y también permite que el tráfico sea redireccionado hacia la LAN 2 donde además se encuentra el equipo de administración de la red. Se muestra a continuación los comandos empleados en el switch de core 1:

conf t
hostn C11
ip domain-name puce.com
crypto key genera rsa
1024
ip ssh version 2
username cisco privil 15 passw cisco

line vty 0 4

login local

transport input all

exit

spa mode rapi

int r e1/0-3

sw tr encap dot

sw mode tru

exit

ip dhcp exclud 192.168.11.0 192.168.11.10

ip dhcp exclud 192.168.12.0 192.168.12.10

ip dhcp pool Net11

netw 192.168.11.0 255.255.255.0

defa 192.168.11.1

ip dhcp pool Net12

netw 192.168.12.0 255.255.255.0

defa 192.168.12.1

exit

vlan 11

name NET11

vlan 12

name NET12

exit

int vlan 11

ip addr 192.168.11.1 255.255.255.0

no shut

int vlan 12

ip addr 192.168.12.1 255.255.255.0

no shut

exit

ip routing

spa vlan 11 root primary

spa vlan 12 root primary

vtp mode server

vtp domain Puce1
vtp passw puce1
int e3/0
no sw
ip addr 10.0.10.1 255.255.255.252
exit
int vlan 1
ip addr 192.168.101.1 255.255.255.0
no shut
exit
router ospf 1
netw 192.168.11.0 0.0.0.255 area 0
netw 192.168.12.0 0.0.0.255 area 0
netw 10.0.10.0 0.0.0.3 area 0
netw 192.168.101.0 0.0.0.255 area 0
exit
do wr
int r e0/0-3
channel-group 1 mode desirable
sw tru encap dot
sw mode tru
exit
int port-channel 1
sw tru encap dot
sw mode tru
exit
do wr

3.3.2. Capa de Distribución

Los equipos del nivel intermedio redirigen el tráfico enrutado en la capa de core y sea entre las VLAN existentes o de la red LAN 2. Su funcionamiento base se centra en los puertos troncales y la configuración de STP. Es un componente principal en cuanto a la

redundancia de los enlaces. Se muestra a continuación los comandos utilizados en un switch del nivel:

conf t
hostn D11
ip domain-name puce.com
crypto key genera rsa
1024
ip ssh version 2
username cisco privil 15 passw cisco
line vty 0 4
login local
transport input all
exit
spa mode rapi
int r e0/0-3
sw tru encap dot
sw mode tru
int r e1/0-3
sw trun encap dot
sw mode trun
exit
no ip routing
vtp mode client
vtp domain Puce1
vtp passw puce1
int vlan 1
ip addr 192.168.101.3 255.255.255.0
no shut
exit
ip default-gateway 192.168.101.1
do wr

3.3.3. Capa de Acceso

Los dispositivos de acceso tienen sus puertos asignados a las dos VLAN creadas previamente, mientras que los puertos de la última tarjeta de red están libres y serán usados para la automatización. El software fue desarrollado con esta consideración y la automatización se enfoca en la creación de una VLAN usando los puertos libres mencionados. Se muestra a continuación los comandos de un equipo de la capa de acceso:

conf t
hostn A11
ip domain-name puce.com
crypto key genera rsa
1024
ip ssh version 2
username cisco privil 15 passw cisco
line vty 0 4
login local
transport input all
exit
spa mode rapi
int r e0/0-3
sw tru encap dot
sw m tr
int r e1/0-3
sw m a
sw a vlan 11
spa portf
int r e2/0-3
sw m a
sw a vlan 12
spa portf
exit
no ip routing
vtp mode client

vtp domain Puce1

vtp passw puce1

int vlan 1

ip addr 192.168.101.5 255.255.255.0

no shut

exit

ip default-gate 192.168.101.1

do wr

3.4. SOFTWARE DE AUTOMATIZACIÓN

Mediante la aplicación Netmiko se realiza la conexión a los dispositivos de red mediante el protocolo SSH configurado inicialmente. Cuando el software accede al dispositivo se procede con el envío de los comandos para su ejecución, este proceso se realiza de forma secuencial por lo que se lo realiza mediante un arreglo de cadenas de texto. Esta tarea se lleva a cabo en una función llamada “set_cmd” definida de la siguiente manera:

Figura 10

Función que permite la conexión y envío de comandos de configuración al dispositivo de red

```
def set_cmd(ip, cmdset):
    cisco_dev = {
        'device_type': 'cisco_ios',
        'host': ip,
        'username': 'cisco',
        'password': 'cisco'
    }

    print('\n#################################################')
    print(f'Configuration of device: {cisco_dev["host"]} ')
    print('#################################################\n')
    net_con = ConnectHandler(**cisco_dev)
    cmd_resp = net_con.send_config_set(cmdset)
    net_con.write_channel('exit\n')
```

Fuente: Autor

El proceso de automatización se realiza mediante un bucle for que accede de manera individual a los dispositivos y envía el conjunto de comandos que corresponda de acuerdo a

la capa en la que se encuentre. Las sentencias más relevantes que realizan este proceso son dos:

Figura 11

Sentencias que iteran y acceden a los equipos de red aplicando la configuración respectiva

```
for dip in part:
    set_cmd(dip, config_ports(numVlan))

run_cmd(coreip, config_core(numVlan, nameVlan))
```

Fuente: Autor

Este proceso toma la información cargada en un archivo de extensión ".py" que contiene funciones con parámetros que reciben la información ingresada por el usuario:

Figura 12:

Función que modifica la configuración de los puertos de los switches de la capa de acceso en base a los datos ingresados por el usuario

```
def config_ports(a):
    return [
        'int r e3/0-3',
        'sw mode a',
        f'sw a vlan {a}',
        'span portf'
    ]
```

Fuente: Autor

Figura 13:

Función que modifica la configuración del equipo principal de la capa de Core en base a los datos ingresados por el usuario.

```
def config_core(vnum, vname):
    return [
    f'ip dhcp exclud 192.168.{vnum}.0 192.168.{vnum}.10',
    f'ip dhcp pool Net{vnum}',
    f'netwo 192.168.{vnum}.0 255.255.255.0',
    f'default 192.168.{vnum}.1',
    'exit',
    f'vlan {vnum}',
    f'name {vname}',
    'exit',
    f'int vlan {vnum}',
    f'ip addr 192.168.{vnum}.1 255.255.255.0',
    'no shut',
    'exit',
    'router ospf 1',
    f'netw 192.168.{vnum}.0 0.0.0.255 area 0',
    'exit'
]
```

Fuente: Autor

3.5. PRUEBAS DE FUNCIONAMIENTO

La aplicación se desarrolló con herramientas de Python en su totalidad. Se define un entorno virtual que contiene las librerías necesarias para la ejecución del proyecto y se mantiene aislado de procesos del sistema operativo. Se activa el entorno virtual creado y se ejecuta la aplicación:

Figura 14

Consola cmder con los comandos para la activación y ejecución de la aplicación.

```
C:\Users\DellVm\Documents\networkApp01 (master)
λ .\env01\Scripts\activat
'.\env01\Scripts\activat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\DellVm\Documents\networkApp01 (master)
λ .\env01\Scripts\activate.bat

C:\Users\DellVm\Documents\networkApp01 (master)
(env01) λ python main.py
 * Serving Flask app 'app' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: on
 * Running on http://127.0.0.1:5000 (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 851-174-872
```

Fuente: Autor

Página de inicio de la aplicación que muestra los campos para ingresar el número y el nombre de la VLAN además del desplegable para seleccionar la red en la que se creará la nueva VLAN.

Figura 15

Pantalla de inicio de la aplicación



Fuente: Autor

En el apartado de configuración se puede seleccionar del desplegable todos los equipos de red para visualizar los protocolos configurados.

Figura 16

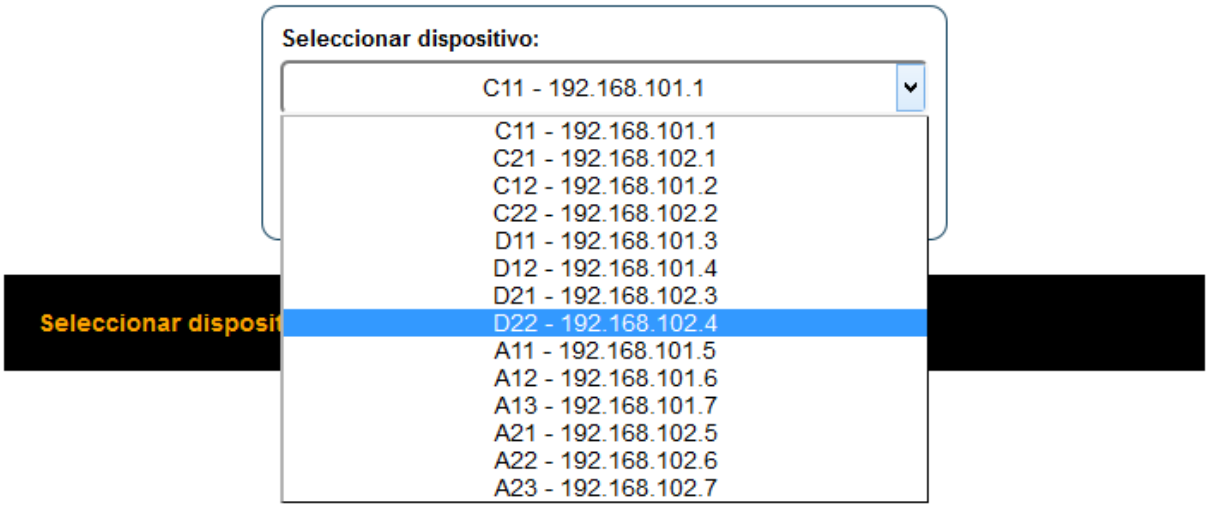
Pantalla que muestra la configuración del equipo seleccionado en la segunda página de la aplicación



Fuente: Autor

Figura 17

Desplegable que muestra los equipos de red conectados y sus respectivas direcciones IP



Fuente: Autor

Figura 18

Información de las VLAN configuradas en el equipo seleccionado

```
##########################################################
  Configuration of device: 192.168.101.1
##########################################################

configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
C11(config)#do show vlan br

VLAN Name                        Status    Ports
---- ----------------------------- --------- -------------------------------
1    default                      active    Et2/0, Et2/1, Et2/2, Et2/3, Et3/1, Et3/2, Et3/3
11   NET11                        active
12   NET12                        active
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

Fuente: Autor

Figura 19

Información de las interfaces configuradas en el equipo seleccionado

```
C11(config)#do show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            10.0.10.1       YES NVRAM  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Port-channel1          unassigned      YES unset  up                    up
Vlan1                  192.168.101.1   YES NVRAM  up                    up
Vlan11                 192.168.11.1    YES NVRAM  up                    up
Vlan12                 192.168.12.1    YES NVRAM  up                    up
C11(config)#end
C11#
```

Fuente: Autor

Una vez ingresados los datos en los campos definidos, se procede con la creación de la VLAN y el proceso correspondiente en el que se configuran una serie de comandos de

manera automática para que la nueva VLAN y los equipos asignados tengan conectividad en la red.

Figura 20

Resultado luego de ingresar los datos de la VLAN y presionar el botón principal

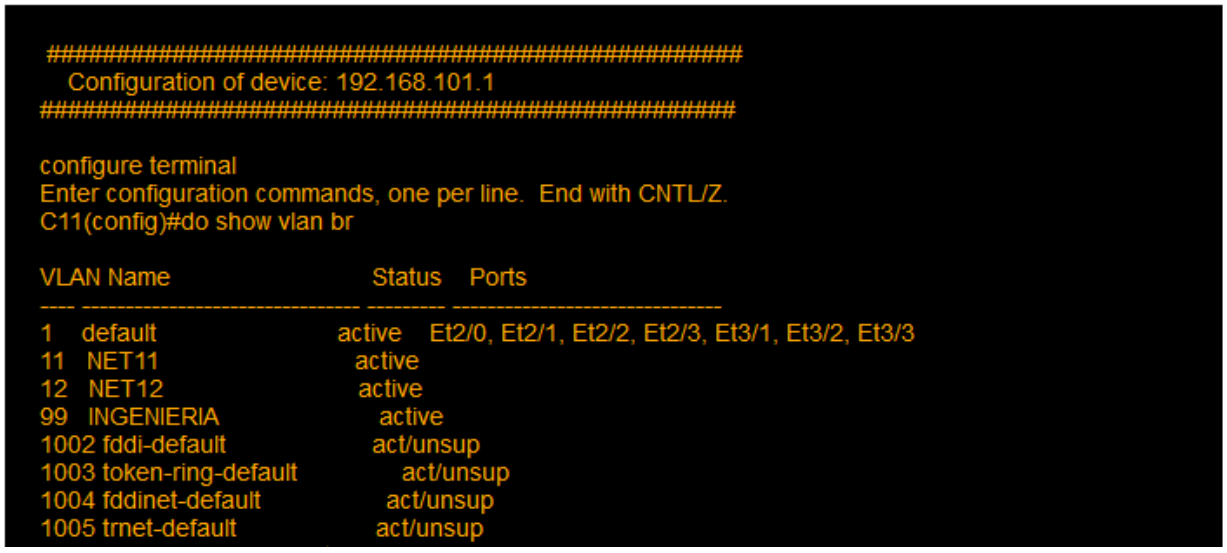


Fuente: Autor

Para verificar que la creación de la VLAN se realizó de forma exitosa se accede nuevamente a la segunda página de la aplicación y se selecciona un dispositivo de la lista.

Figura 21

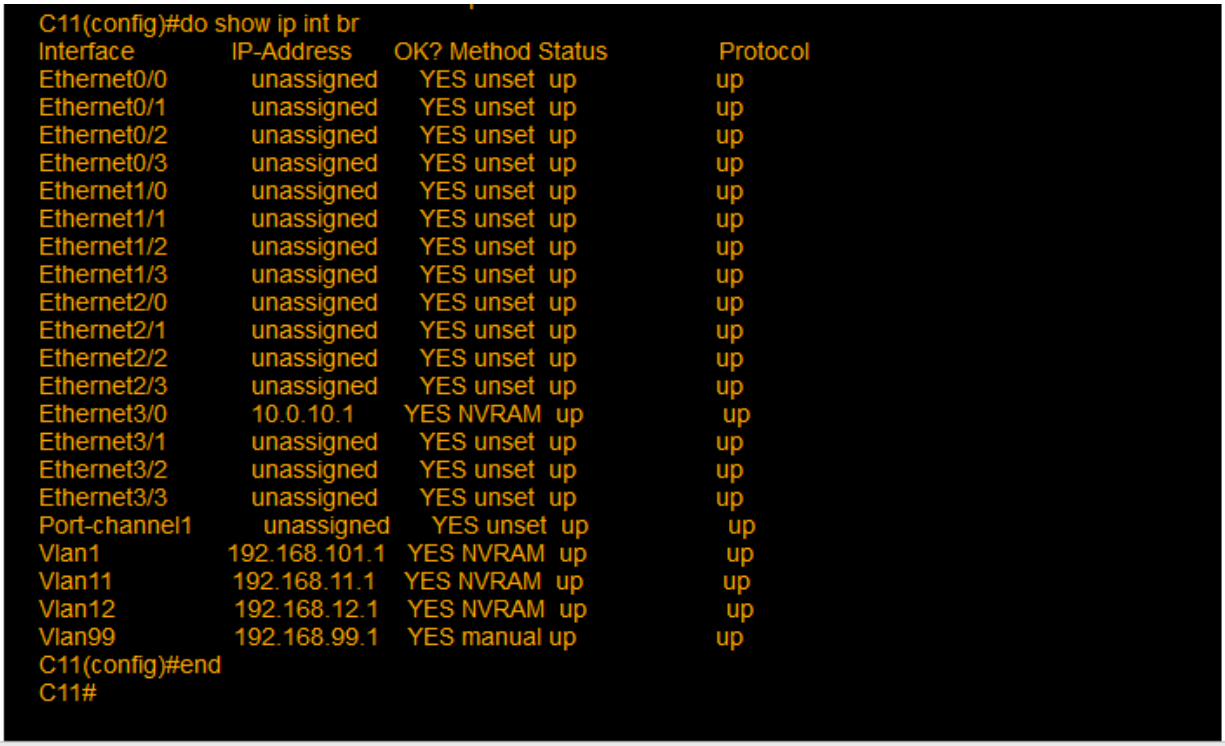
Información de las VLAN creadas en el equipo de Core luego de la automatización



Fuente: Autor

Figura 22

Información de la configuración de las interfaces del equipo de Core luego del proceso de automatización.

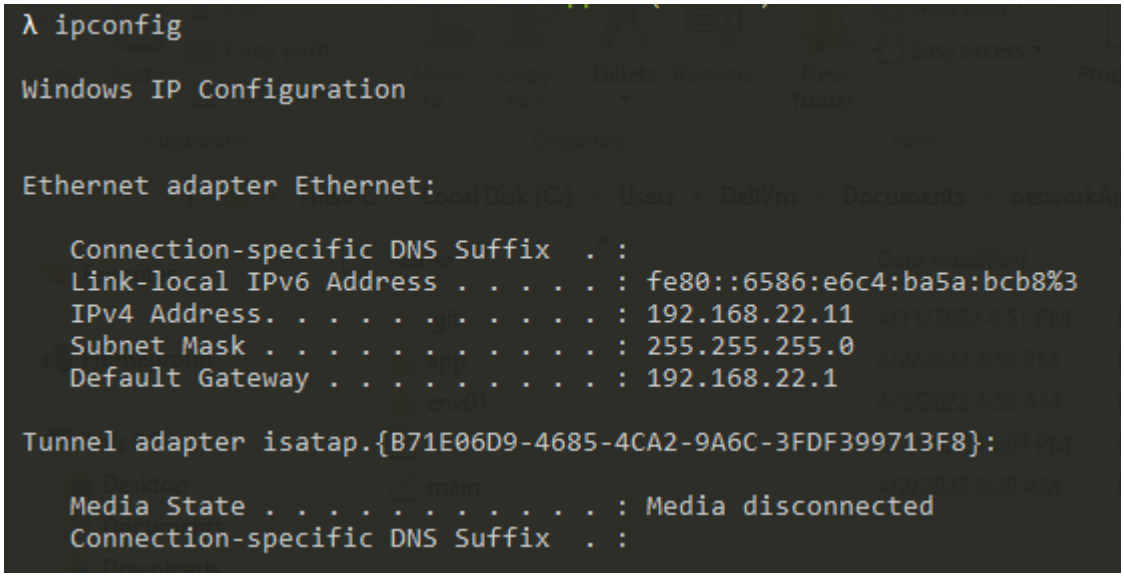


Fuente: Autor

Como verificación final se revisa la dirección IP del equipo de administración para probar la comunicación con la nueva VLAN.

Figura 23

Configuración del adaptador de red del equipo de administración

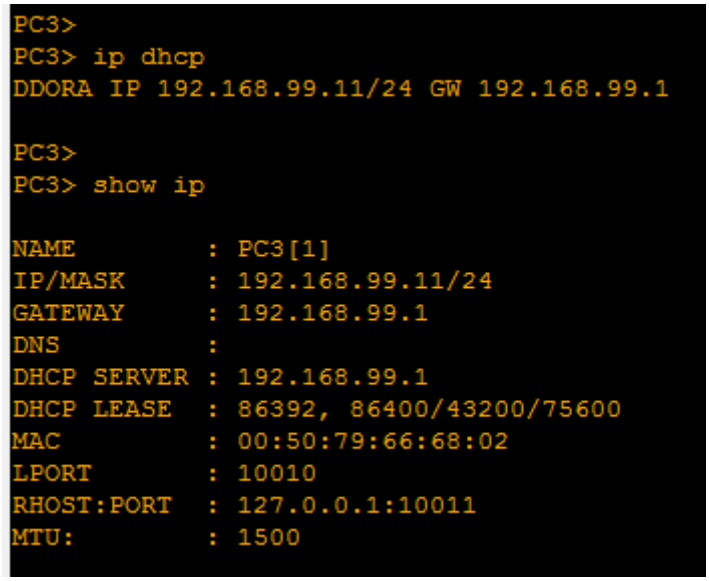


Fuente: Autor

Desde la consola de GNS3 se accede al VPC conectado al puerto de la tarjeta de red que forma parte de la VLAN creada desde la aplicación. Se realiza la petición de dirección IP al servidor de DHCP que es el switch de core principal y mediante el programa “ping” se verifica la conectividad al equipo de administración. Este proceso es satisfactorio y es posible gracias a la configuración de los protocolos de enrutamiento, de gestión de VLANs y de gestión de puertos que se llevan a cabo de forma automática luego de que el usuario crea la VLAN.

Figura 24

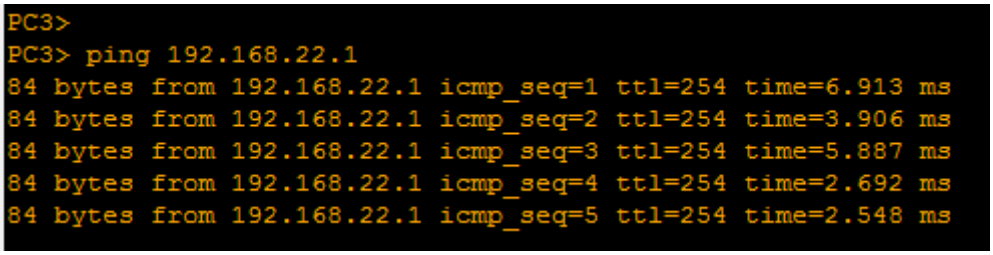
Ejecución de comandos que asignan una IP al equipo VPC de prueba.



Fuente: Autor

Figura 25

Prueba de conectividad entre el VPC conectado a la VLAN creada y el equipo de administración de la red.



Fuente: Autor

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La topología jerárquica de tres capas establece que en el nivel superior se implementen switches multicapa mientras que en los demás niveles se pueden utilizar switches de capa 2. Se diseñó la topología conectando el switch de core principal de cada LAN mediante un solo enlace que no cumplió con los parámetros de alta redundancia establecidos en el resto de la topología. Se concluye también que realizar una conexión de más de un enlace entre los equipos de core requiere de la configuración de un protocolo adicional como HSRP (Hot Standby Router Protocol)
- Para realizar el proceso de automatización se utiliza la única tarjeta de red disponible en los equipos de la capa de acceso. Agregar NIC a cada dispositivo incrementa la cantidad de memoria ram que requiere el equipo de red disminuyendo además el rendimiento de la simulación y la aplicación desarrollada.
- Las librerías existentes para automatización de redes desarrolladas en Python brindan grandes beneficios, pero muchos inconvenientes presentados no están documentados por lo que su solución depende principalmente del desarrollador.
- Para la implementación de Port Channel se debe considerar las interfaces disponibles ya que conectar dos dispositivos con más de un enlace no siempre significa que la velocidad de transmisión será superior. Utilizar varios puertos ethernet o fast ethernet mediante Port Channel no brinda ningún beneficio si se dispone de un puerto Giga Ethernet.
- Luego de la configuración de la topología con todos los protocolos definidos inicialmente, se realizan pruebas de funcionamiento y al finalizar se descartan los cambios efectuados para que la implementación no sufra errores además de llevar a cabo pruebas bajo en el mismo escenario. Se detectó que el nombre de la VLAN creada mediante el software de

automatización se mantiene en el switch de core por lo que se concluye que la imagen del switch guarda esta información sin la necesidad de ejecutar el comando “copy running-config startup-config”.

- En base a las fuentes consultadas y pruebas iniciales realizadas en la aplicación Packet Tracer se pudo verificar que los switches multicapa de Cisco requieren de la activación de la función de enrutamiento, pero las imágenes utilizadas en GNS3 ya tienen esta opción habilitada por defecto. Por lo tanto, se obtuvieron errores en el funcionamiento de la topología hasta que se detectó el estado de esta funcionalidad que solo se requiere en el switch de core principal de cada LAN.

5.2. RECOMENDACIONES

- Se recomienda revisar la mayor cantidad de documentación existente sobre los protocolos a implementar y su compatibilidad con los equipos o imágenes que se utilicen para evitar posibles errores durante el desarrollo del proyecto.
- Utilizar imágenes de tipo IOU Device brindan un rendimiento superior a las imágenes dedicadas de switches multicapa que consumen mayor cantidad de recursos y pueden provocar que la simulación falle si el equipo host no cuenta con mas de 16GB de memoria RAM. Sin embargo, se debe habilitar el acceso a equipos IOU mediante un código generado desde la máquina virtual de GNS3 que tiene cierta complejidad.
- Realizar pruebas de funcionamiento y de integración con las imágenes de los dispositivos de red cargados al simulador GNS3 ya que su funcionamiento y características son reducidas en comparación a los equipos físicos y el análisis de errores puede llevar a conclusiones erróneas sobre las posibles soluciones.
- Los protocolos que se pueden considerar esenciales en la red de una organización están directamente relacionados con switches y routers. En este caso el proyecto fue desarrollado con imágenes de equipos Cisco, pero se recomienda considerar las nuevas

versiones de equipos y sistemas operativos de dispositivos de red. La evolución tecnológica ha mostrado cierta tendencia hacia la optimización de software para automatización y monitoreo que son áreas con gran potencial de desarrollo e investigación.

- El desarrollo de la aplicación de automatización utilizando Python como lenguaje base brinda ventajas en cuanto a rendimiento general, ya que el módulo de conexión a los dispositivos de red y la página web se integran de manera automática sin la necesidad de herramientas adicionales. Pero se recomienda implementar frameworks de frontend, desarrollados principalmente en JavaScript, para mejorar la interacción del usuario con el software desarrollado.

REFERENCIAS

Abdulahad, D. (2018). The Importance of VLANs and Trunk Links in Network Communication Areas. International Journal of Scientific & Engineering Research, 9(9), p11. Recuperado de: https://www.researchgate.net/profile/Dlnya-Aziz-4/publication/327824310_The_Importance_of_VLANs_and_Trunk_Links_in_Network_Communication_Areas/links/5ba69acc299bf13e6045f14f/The-Importance-of-VLANs-and-Trunk-Links-in-Network-Communication-Areas.pdf

Ariganello, E. & Barrientos, E. (2014). Redes Cisco, guía de estudio para la certificación CCNP. Madrid, España: RA-MA, S.A. Editorial y Publicaciones.

Boumezrag, A. (2020). Una propuesta de nueva plataforma de gestión de redes para la programación y automatización de redes con implementación en GNS3. University Mohamed Khider Biskra. Algeria.

Carthern, C., Wilson, W., Rivera, N., & Bedwell, R. (2015). *Cisco Networks. Engineers' Handbook of routing, switching, and security with iOS, NX-OS, and ASA.* New York, United States, Apress Media.

Cisco. (2022). What is network switching? Recuperado de: https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html

Cisco Catalyst Guide. (s.f.). Catalyst 6500 Release 12.2SX Software Configuration Guide. Recuperado de: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html

Cisco CVD. (2013). Campus Wired LAN. Recuperado de: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-CampusWiredLANDesignGuide-AUG13.pdf

Cisco CVD. (2020). Campus LAN and Wireless LAN Solution Design Guide. Recuperado de: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

Cisco Press. (2014). Connecting Networks Companion Guide. Recuperado de: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Cloudflare. (s.f.). ¿Qué es una red de área de campus (CAN)? Recuperado de: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-campus-area-network/

Cloudflare. (2022). What is routing? | IP routing. Recuperado de: https://www.cloudflare.com/learning/network-layer/what-is-routing/

Conde, A. (2020). Automatización de procesos en redes de datos mediante programación en Python. Cataluña, España.

Doyle, J. (2005). CCIE Professional Development Routing TCP/IP, Volume I, Second Edition. Cisco Press.

Empson, S. (2016). CCNA Routing and Switching Portable Command Guide. United States, Indianapolis. Cisco Press.

Gallegos, J., Mayorga, T. (2020). Automatización de procesos en redes de datos mediante programación en Python. Universidad Israel y REDIPE, Quito. Ecuador.

GNS3 Docs. (s.f.). GNS3 setup wizard with the GNS3 VM. Recuperado de: https://docs.gns3.com/docs/getting-started/setup-wizard-gns3-vm/

Horn, U. (s.f.). What is a 5G Campus Network? Recuperado de: https://www.ericsson.com/en/enterprise/cellular-curious/5g-campus-network

Merriam-Webster. (s.f.). Definition of campus. Recuperado de: https://www.merriam-webster.com/dictionary/campus

Microsoft Docs. (2021). Dynamic Host Configuration Protocol (DCHP). Recuperado de: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Mihaila, P., Balan, T., Cupren, R. & Sandu, F. (2017). Automatización y abstracción de redes usando métodos de programación con Python. Transilvania University, Brasov. Romania.

Vardy, A. (2015). Cisco CCNA networking for beginers.