UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE TELECOMUNICACIONES

ANÁLISIS DE IMPLEMENTACIÓN DE UNA RED SDN EN EL CAMPUS SUR DE LA UNIVERSIDAD POLITÉCNICA SALESIANA

Trabajo de titulación previo a la obtención del Título de ingeniero en telecomunicaciones

AUTORES: MILTON FIDEL CHAMORRO ARMIJOS
JHOSTIN ANDRÉS LÓPEZ VALLEJO

TUTOR: JUAN CARLOS DOMÍNGUEZ AYALA

Quito – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, **Milton Fidel Chamorro Armijos** con documento de identificación N° 1726790742 y **Jhostin Andres López Vallejo** con documento de identificación N° 1724972128; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 7 de marzo del año 2022

Atentamente

Milton Fidel Chamorro Armijos
1726790742

Jhostin Andrés López Vallejo
1724972128

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, **Milton Fidel Chamorro Armijos** con documento de identificación No. 1726790742 y **Jhostin Andres López Vallejo** con documento de identificación No. 1724972128, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: "Análisis De Implementación De Una Red SDN En El Campus Sur De La Universidad Politécnica Salesiana", el cual ha sido desarrollado para optar por el título de: Ingeniero en telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 7 de marzo del año 2022

Atentamente,

Milton Fidel Chamorro Armijos
1726790742

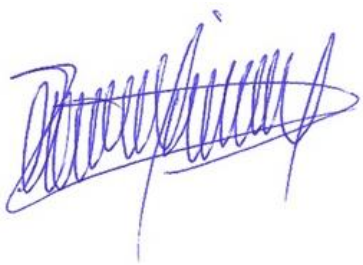
Jhostin Andrés López Vallejo
1724972128

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, **Juan Carlos Domínguez Ayala** con documento de identificación N° 1713195590, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE IMPLEMENTACIÓN DE UNA RED SDN EN EL CAMPUS SUR DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, realizado por **Milton Fidel Chamorro Armijos** con documento de identificación N° 1726790742 y por **Jhostin Andres López Vallejo** con documento de identificación N° 1724972128, obteniendo como resultado final el trabajo de titulación bajo la opción de Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 7 de marzo del año 2022

Atentamente,



Ing. Juan Carlos Domínguez Ayala, Mgtr.

1713195590

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el presente proyecto técnico se busca analizar el funcionamiento de una red SDN en el entorno actual de la Universidad Politécnica Salesiana, la cual posee una red jerárquica en producción y esta será una base para poder comprobar los resultados de la red actual con los resultados de una red administrada por software, esto se logrará realizando una simulación de las dos redes y realizar las pruebas necesarias de su servicio, funcionalidad y administración.

La red SDN contendrá una estructura similar a la red actual del campus sur de la UPS y la cual se busca obtener un desarrollo en cuanto a administración, además considerando el progreso que han tenido las infraestructuras de redes en el mercado actual, también se aborda el incremento de la demanda y de soluciones por parte de los estudiantes y del equipo que trabaja en la universidad.

Los simuladores que han desarrollado cada una de las marcas que se dedican a la fabricación de los equipos de red, se convierten en las mejores opciones para poder simular y comprobar las funcionalidades de cada una de las redes a evaluar. Estos simuladores en la actualidad ya cuentan con las herramientas necesarias como modelos de equipos, protocolos de comunicación, conexiones de último desarrollo, etc.

Los parámetros de la calidad de servicio de una red serán los que regirán esta evaluación de redes y son los que nos respaldarán al momento de brindar un veredicto al concluir con el desarrollo del presente proyecto, concluyendo con determinar con datos reales que puntos fuertes abarca una red SDN comparada con una red jerárquica y poder realizar las recomendaciones necesarias para la implementación de esta en la Universidad Politécnica Salesiana

ABSTRACT

In this technical project we seek to analyze the operation of an SDN network in the current environment of the Salesian Polytechnic University, which has a hierarchical network in production, and this will be a basis to be able to check the current results with the results of a managed network by software, by simulating the two networks and performing the necessary tests of their functionality and administration service.

The SDN network will contain a structure like the current network of the UPS south campus, and which seeks to obtain a development in terms of administration and growth of the same, considering the progress that network infrastructures have had in the market in the Currently, the increase in demand and solutions by students and the team that works at the university to provide a better service in the institution is also addressed.

The simulators that have been developed by each of the brands that are dedicated to the manufacture of network equipment, are defined in the best options to be able to simulate and check the functionalities of each of the networks to be evaluated. These simulators currently already have the necessary tools such as equipment models, communication protocols, state-of-the-art connections, etc.

The parameters of the quality of service of a network will be the ones that will govern this evaluation of networks and are the ones that will support us when giving a verdict at the end of the development of this project, concluding with determining with real data what strong points a network encompasses. SDN network compared with a hierarchical network and to be able to make the necessary recommendations for the implementation of this in the Salesian Polytechnic University.

INTRODUCCIÓN

Las redes SDN pueden ser consideradas el siguiente paso en cuanto a infraestructura de redes, ya que ha logrado un avance en los sistemas que permiten automatizar los equipos y es lo que se probará en este proyecto técnico, dando un avance simulado a la red de la Universidad Politécnica Salesiana que se encuentra en la actualidad en funcionamiento y demostrando los beneficios y percances que se pueden presentar al usar una estructura administrada por software.

La red actual tiene algunos años en función y considerando el avance de la tecnología que ha sido exponencial en los últimos años, se debe considerar migrar también la red a una estructura más actual y más avanzada, que permita tener nuevas opciones en cuanto a administración se refiere, usando nuevos protocolos y trabajando con los sistemas antiguos ya que esta es una integración de nuevas habilidades tanto a nivel de equipos más avanzados, como una administración más sencilla por parte del equipo técnico encargado.

El desarrollo de cada parte del proyecto se detallará a lo largo de este documento y se buscará ser lo más claro posible en la explicación detallada de cada proceso desarrollado para llegar a las conclusiones y posteriores recomendaciones y que estas sean totalmente comprendidas por todos los lectores del proyecto técnico.

CAPÍTULO 1
ANTECEDENTES

En el presente capitulo se plateará el problema, cuya resolución será el desarrollo de este texto, se presentará la justificación para realizar el proyecto técnico, se plantearán los objetivos que se alcanzarán al concluir la investigación, además se detallará las técnicas utilizadas en el desarrollo del proyecto. La comparación con la red actual en producción de la Universidad Politécnica Salesiana será un punto de referencia para poder reconocer y analizar puntos importantes, además de verificar que los objetivos planteados sean completados exitosamente.

1.1 Planteamiento del problema

En la actualidad, vivimos en un mundo inundado por la tecnología en cada aspecto de nuestra vida, si nos enfocamos en las grandes industrias, las mismas que requieren de un sistema de red que cumpla con los requerimientos necesarios para continuar su productividad ininterrumpida por parte de su sistema de redes. Para este estudio, el enfoque será a la industria de la educación, el campus sur de la Universidad Politécnica Salesiana de la capital, la misma es una entidad dedicada a la formación de nuevos profesionales, y ya que su demanda que presenta en cuanto a recursos de una red de calidad es diaria por la cantidad de usuarios que manejan en este campus dedicado en su totalidad a las ingenierías, es muy importante para el sistema educativo de la unidad educativa.

Tomando en cuenta los puntos presentados en el párrafo anterior, y además de tomar en cuenta el desarrollo de todas las tecnologías incluyendo las infraestructuras de redes, se requiere un análisis de un aparentemente nuevo tipo de administración de

redes, la cual tiene por nombre, SDN (Software Defined Network en sus siglas en ingles), esta forma de administración le da una nueva organización en cuanto a planos de control y datos, y otros aspectos positivos y negativos que serán desarrollados y analizados a lo largo de este documento.

La red actual de la universidad es un modelo antiguo pero que se mantiene en funciones activas en la mayoría de los sistemas de redes, ya que se le puede considerar la base actual para implementar una red administrada, estas redes tienen el nombre de redes jerárquicas. Estas redes poseen una estructura tradicional, contienen los dispositivos finales o host, siguiendo con equipos de acceso, equipos de administración en capa 2 y 3, equipos de Core y por último la conexión a red pública con el proveedor de servicios.

En las redes tradicionales se realiza una administración por equipo, esto quiere decir que el administrador encargado debe configurar cada equipo que se pondrá en ejecución con la red para que pueda conocer sus recursos y las normas que debe seguir en los casos específicos que determine el personal encargado, este problema busca ser solucionado con la implementación de una red SDN como el siguiente paso en cuando a administración de redes se refiere.

El objetivo de este análisis comparativo es identificar los beneficios de implementar una red SDN en comparación con las redes actualmente en producción de la institución educativa ya que la demanda de esta incrementa por el crecimiento exponencial tanto de usuarios conectados y de las tecnologías en desarrollo.

1.2 Justificación

Las Redes Definidas por Software o SDN (Software Defined Network) constituyen una tecnología en la que se desacopla el plano de datos del plano de control y en la que se emplean controladores, que son los responsables de gestionar la información de reenvío de los conmutadores o switch en redes cableadas. Hoy en día se han desarrollado muchos controladores SDN, tanto de código abierto como comerciales, por lo que uno de los principales aspectos para tener en cuenta en el entorno actual de las Redes Definidas por Software, es cuál controlador elegir para una solución de este tipo. En este artículo se revisan las características más destacadas de los controladores SDN y se precisan algunos elementos para tener en cuenta para su selección y evaluación". (Centeno, A. G., Vergel, C. M. R., Calderón, C. A., & Bondarenko, F. C. C. ,2014)

En el proyecto técnico se buscará realizar una comparación en los parámetros que involucran calidad de servicio en una red y de esta manera poder determinar la diferenciación entre una red jerárquica que se encuentra actualmente en producción de la universidad y una red definida por software, siendo esta última administrada por un elemento llamado controlador, además de contar con otras características importantes como su capacidad de adaptabilidad en cuanto a equipos de diferentes marcas y modelos. En ambos casos las redes serán simuladas y de esta manera se podrá analizar de manera conjunta, sometiendo a pruebas similares y poder obtener los resultados que nos permitirán realizar una tabla de decisión y al concluir se realizará una recomendación sobre la migración de la red en la entidad educativa.

1.3 Objetivos

1.3.1 Objetivo General

Comparar una red tradicional de la Universidad Politécnica Salesiana con una red Software Define Network propuesta, desarrollando una tabla de decisión tomando en cuenta términos tecnológicos, de eficiencia, y económicos y así determinar la factibilidad de mudar la red actual de la UPS a una red orquestada y centralizada en nube (SDN).

1.3.2 Objetivos Específicos

- Revisar la red jerárquica actual de la UPS en el campus sur que nos permita tener un amplio conocimiento del funcionamiento y segmentación de esta.
- Identificar las arquitecturas SDN disponible en el mercado para redes de acceso y controladas en nube.
- Diseñar una topología SDN para la red de la UPS que cumpla con las características de una red robusta, que le permita alcanzar los estándares de servicio.
- Comparar la capacidad de administración de la red jerárquica actual de la universidad con la nueva red SDN propuesta.

1.4 Metodología

Actualmente, en la red de producción de la universidad, tiene un funcionamiento que esta descontinuado, ya que su infraestructura pertenece a las redes que tienen el plano de control y plano de datos dentro de un mismo dispositivo, esto impide que las redes sean autónomas, ya que la arquitectura pertenece a un modelo jerárquico de 3 capas.

Separaremos el plano de control del plano de datos mediante un controlador, este será el encargado de tener el plano de control, el cual administrará las 3 capas del modelo jerárquico empresarial, ya que conmutará a alta velocidad los datos, dará conectividad basada en políticas y dará acceso de grupo de trabajo locales y remotos. Por debajo del controlador SDN se usará un protocolo Open Flow, que será el encargado de enviar la información al plano de datos.

Por medio de simulación encontraremos el mejor mecanismo de SDN basado en controladores y orientaremos la solución a equipos que soporten Open Flow, enfocados en dispositivos de Core, distribución y acceso que respondan a la orquestación de esta.

Mediante una API se automatizará el plano de control de la red SDN, con un mecanismo que nos permita orquestar toda nuestra topología en nube, de esta manera controlar todos los nodos y dispositivos de la red.

Una vez encontrado el mecanismo de SDN basada en controlador y la topología de red que se apegue al mismo, se procederá a realizar una tabla de decisión que abarque las características que se necesita para la migración en el cual se detallará los parámetros comparativos entre el modelo jerárquico empresarial antiguo con los parámetros de SDN simulados.

Para finalizar el proyecto técnico de ingeniería, se recomendará equipos que se apeguen a la mejor solución de infraestructura SDN de manera general para que este proyecto se pueda ejecutar con bases, Cisco, HPE Aruba, etc.

CAPÍTULO 2
MARCO CONCEPTUAL

En el capítulo actual se detallarán los conceptos, normas y parámetros que guiarán el proyecto técnico para una comprensión total del desarrollo de este. Se busca ampliar el concepto de redes definidas por software y concretar el concepto de una red jerárquica para poder diferenciarlas desde su definición, además de mencionar algunos casos de estudios similares o relacionados que fueron desarrollados en los últimos años.

2.1 Redes jerárquicas

Las redes han sido un punto fuerte en cuanto a la evolución tecnológica, desde sus inicios en los cuales se usaban redes sencillas para enviar paquetes por la dirección de su cabecera, hasta la actualidad que tenemos redes inteligentes que necesitan menos de la interacción humanada y pueden hacer análisis muy extensos en pocos segundos, además tener un nivel muy alto de autonomía en cuanto a gestión de recursos y más.

Las redes jerárquicas actuales tienen una arquitectura de red en la cual los nodos tienen a su cargo el procesamiento de datos de manera individual, esto se consigue después de la previa programación de los nodos para cumplir con su propósito, pero si bien se comprenden como redes hechas a la medida tienen una gran desventaja e involucra al desarrollo de las tecnologías.(Mecánica et al., 2015)

El desarrollo de las tecnologías de comunicaciones y la demanda en crecimiento de los recursos para una buena comunicación empieza a ser una gran desventaja para este tipo de redes en la actualidad ya que, si bien en su tiempo de su primera implementación fueron lo más avanzado, ahora tienen mayores retos y presentan dificultades para poder soportar el tráfico necesario sin llegar a la saturación de canales. (Mecánica et al., 2015)

La gestión de redes con una visión de los recursos más amplia, es el requerimiento que las nuevas tecnologías presentan, además de la cantidad y necesidad de recursos tecnológicos por parte de los usuarios está en constante crecimiento, estos aspectos involucran un reto para que las redes puedan satisfacer las exigencias que se presentan y mantener un servicio de buena calidad para los usuarios. (Mecánica et al., 2015)

Las redes actuales se consideraron ideales en su momento ya que ofrecían un sistema hecho a la medida que resolvía los problemas más comunes y estaba preparado para los problemas previstos por el administrador con protocolos, con rutas alternativas que eran programadas por el personal encargado, pero este tiene un punto débil y el cual en la actualidad es un muy importante y es la adaptación a problemas no previstos por los administradores de la red, quiere decir la adaptabilidad de la red para resolver cualquier problema propuesto en la red.

Llegando a este punto, una opción que significa la esperanza para estas redes es la optimización de recursos que contiene la red, ya que, si se observa cualquier red, seguramente se tendrán enlaces o puertos saturados, pero otras rutas se encuentran libres, por esta razón la administración de los elementos de la red es un punto esencial en la actualidad y este documento desarrollará una nueva red que pueda reducir la importancia de estas desventajas en la red.

2.2 Direccionamiento IP de redes

El direccionamiento IP en el mundo de las redes posee una gran importancia, ya que se podrá considerar como el número de identificación de un dispositivo dentro de la red, para poner un ejemplo es como el apellido de un estudiante que le distingue del resto de sus compañeros que poseen un apellido diferente.

El direccionamiento consta de una cantidad limitada de bits, agrupados en 4 bloques de 8 bits cada uno con un total de 32 bits en el direccionamiento IPv4, las mismas tienen una clasificación en 3 grupos, clase A, B, C, D y E, a continuación, se presenta los detalles de cada clase de redes.

2.2.1 Clase A

Para Clase A se tiene que el primer byte entre los números 0 hasta 127, por ejemplo, un Host puede tener la dirección, 125.X.X.5, siendo "X" cualquier valor entre 0 y 255. (Morat, n.d.)

Bits	1	7	24
	0	Red ID	Host ID
	32 Bits		

Ilustración 1 Estructura Direccionamiento Clase A

2.2.2 Clase B

En la Clase B se tiene que en el primer byte se puede obtener los valores desde 128 hasta 191, además los últimos 16 bits están habilitados para direccionar dispositivos

en la red, por ejemplo, 130.100.X.5, siendo “X” cualquier valor entre 0 y 255.(Morat, n.d.)

Bits	2	14	16
	10	Red ID	Host ID
	32 Bits		

Ilustración 2 Estructura Direccionamiento Clase B

2.2.3 Clase C

Para la clase C los tres primeros bits valen 1, 1 y 0 en ese orden, por lo cual el primer bit va desde 192 hasta 223, un ejemplo de dirección de host en esta clase es, 195.200.10.5. (Morat, n.d.)

Bits	3	21	8
	110	Red ID	Host ID
	32 Bits		

Ilustración 3 Estructura Direccionamiento Clase C

2.2.4 Clase D

Clase D, esta clase está destinada para conexiones multicast, su primer byte tiene valores entre 224 y 239, los bits restantes sirven para identificar grupos multicast en la red.(Morat, n.d.)

Bits	4	28
	1110	Multicast
	32 Bits	

Ilustración 4 Estructura Direccionamiento Clase D

2.2.5 Clase E

Está clase se encuentra reservada para su futuro uso y s valor del primer byte va desde los 240 hasta el número máximo que es 255 al llenar los 8 bits de valor 1 en binario. (Morat, n.d.)

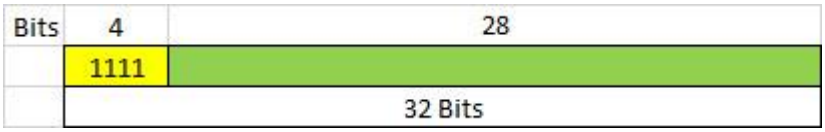


Ilustración 5 Estructura Direccionamiento Clase E

El direccionamiento IP de la versión número 4 ha sido muy usada en los últimos años para direccionar y administrar redes en el mundo entero y aunque tiene un gran problema en la actualidad, el cual es la cantidad de direcciones habilitadas para su uso cada vez se reduce por la alta demanda de equipos que requieren una dirección para poder comunicarse en una red. (Qhwzrun et al., 2011)

Continuando con infraestructuras complejas, al realizar una administración de la red hay una práctica muy utilizada llamada segmentación de la red o Subneteo, que se utiliza para poder de cierta forma partir la red y de esta manera pasar de poseer una red con gran cantidad de host, ahora manejar redes más pequeñas con menos cantidades de host y con usos y políticas diferentes dependiendo del uso que se le dará a este segmento de red, a continuación, se profundizará sobre el tema.

2.2.6 Subneteo

Subneteo hace referencia a la división teórica que se realiza una red en redes de menor cantidad de red o, en otros términos, de máscara más grande, lo cual quiere decir que la cantidad de host es menor en comparación a la red original, para comprender mejor este término mencionaremos un ejemplo. (Morat, n.d.)

Una red 192.168.2.0 tiene una máscara 255.255.255.0, lo cual nos indica que los últimos 8 bits son para poder asignar direcciones a los host, descartando las direcciones 192.168.2.0, 192.168.2.255, ya que son las direcciones de red y de broadcast de esta, tenemos que el ultimo byte puede tener un valor entre 1 y 254, esto si quisiéramos tener una sola red para todos nuestros equipos pero para poder tener un mejor control de los equipos podemos segmentar la red en 8, cada una con 31 direcciones habilitadas en cada subred como se muestra en la siguiente tabla.

Tabla 1 Subneteo Ejemplo 1

Subred	Dirección de red	1era IP utilizable	Ultima IP utilizable	Broadcast
1	192.168.2.0	192.168.2.1	192.168.2.30	192.168.2.31
2	192.168.2.32	192.168.2.33	192.168.2.62	192.168.2.63
3	192.168.2.64	192.168.2.65	192.168.2.94	192.168.2.95
4	192.168.2.96	192.168.2.97	192.168.2.126	192.168.2.127
5	192.168.2.128	192.168.2.129	192.168.2.158	192.168.2.159
6	192.168.2.160	192.168.2.161	192.168.2.190	192.168.2.191
7	192.168.2.192	192.168.2.193	192.168.2.222	192.168.2.223
8	192.168.2.224	192.168.2.225	192.168.2.254	192.168.2.255

2.3 Funciones del servidor

En los simuladores que se pueden encontrar en los diferentes softwares de simulación, se puede implementar algunos servicios en los equipos diseñador para este fin y de esta manera, que el equipo pueda tener una participación lo más parecido a la realidad,

teniendo en cuenta que este es un equipo que contiene mucho del contenido que se presenta a través de una dirección web o dirección IP en una red local.

En la red jerárquica se utilizó algunos de los servicios que presenta la Universidad Politécnica Salesiana, como son, DHCP para los equipos, Email, HTTP/S y DNS para los usuarios, para que se pueda tener una mejor experiencia y poder analizar la respuesta y el tráfico en estos procedimientos en el desarrollo de este documento, a continuación, hablaremos un poco sobre estos servicios que presta el servidor.

2.3.1 DHCP

DHCP o Dynamic Host Configuration Protocol en sus siglas en inglés, es un protocolo el cual permite el direccionamiento IP de forma automática de los equipos que tiene a su alcance, esto permite a los equipos finales obtener una dirección IP dentro de la misma red a la cual se han conectado de manera alámbrica o inalámbrica y formar parte de ella y permitirle la comunicación con toda la red y el servidor que brinda DHCP será el encargado de brindar una dirección IP a los equipos que lo soliciten y en el rango que tenga disponible. (Pengaruh PMA, PMDN, TK, 2020)

2.3.2 Email

Email o correo electrónico , es un servicio prestado a varios usuarios que desean comunicarse por medio de la red, estos son agregados a un servidor que contiene todas sus credenciales y un dominio que los identifica en que servidor se encuentra almacenada su información por ejemplo se tiene @outlook.com, que pertenece a Microsoft, o @gmail que pertenece a Google, estos le permiten comunicarse con otros usuarios de este u otros dominios por medio de las plataformas de correo de cada

empresa y que ayuda en la transferencia de archivos por medio de red pasando por el servidor como intermediario y lograr la comunicación.

2.3.3 HTTP / HTTPS

HTTP (Hypertext Transfer Protocol en sus siglas en inglés) es un protocolo que se basa en el envío de archivos, sobre todo este se relaciona con las solicitudes de un esquema cliente-servidor, en el cual el cliente solicita un servicio y el servidor envía una respuesta a esta. HTTP se envía por una única conexión TCP y la solicitud es enviada en un formato llamado URI (Uniform Resourse Identifier en sus siglas en inglés), este proporciona cierta información para poder localizar y acceder al servidor que cuenta con el recurso que se solicita.(Http, 2020)

HTTPS (Hypertext Transfer Protocol Secure en sus siglas en inglés), básicamente es HTTP sobre TLS, este cambia a un sistema mucho más seguro y confiable, cuanta con autenticación, confidencialidad e integridad en el transporte de los datos en el medio.(Http, 2020)

2.3.4 DNS

DNS o Domain Name System, es un servicio el cual relaciona la dirección IP con un nombre legible de texto plano, lo cual facilita la interacción del usuario con el servidor por medio de una palabra como nombre en lugar de conocer la dirección IP de este servidor al cual requiere enviarle un mensaje de solicitud de sus servicios y este brinde una respuesta. Este protocolo se usa mucho para las páginas web y la dirección de correo electrónico.(Magazine & Usenix, 2000)

2.4 Software Defined Networks (SDN)

Las redes SDN son la respuesta a los problemas de la red jerárquica, ya que forman un conjunto de servicios que le permiten trabajar de una forma dinámica, rápida y sobre todo escalable, este último punto le permite mantenerse como la red más eficiente en la actualidad por algunos años, evitando convertirse en obsoleta muy rápidamente. (Mecánica et al., 2015)

Además, las SDN son un gran inicio para el crecimiento y desarrollo de redes futuras, estás poseen características de flexibilidad, capacidad de ser programadas, gestión y rentabilidad dentro de las redes.

Esencialmente las redes SDN logran ser una oportunidad frente a muchos problemas por su estructura en la red, la razón principal es que separa el plano de control del plano de datos, ya que estos estaban unidos en la mayoría de los dispositivos administrables de la red, por esta razón han separado los planos, asignándole el plano de control a un equipo que lo conoceremos como el controlador que es un equipo central en la red y la cual contendrá todo lo relacionado a control de la red, y el plano de datos continuará en cada uno de los equipos de la red.(Pereira & Gamess, 2017)

Las redes definidas por software le permiten al administrador tener un sistema de respuesta muy eficaz el cual previamente el programará en un lenguaje de alto nivel y que cumpla con las demandas de la red, y logrará que su red reduzca la dependencia de la intervención humanada para poder realizar algunos cambios en su forma de administrar los recursos, por ejemplo, el ancho de banda.(Mecánica et al., 2015)

SDN al igual que otras redes han tenido un desarrollo a lo largo de los años y este empezó con el desarrollo del internet y ha evolucionado con redes complejas,

separación de los planos de control y datos y finalmente su último punto de desarrollo se encuentra en el desarrollo de Open Flow y la interfaz de programación.(Pereira & Gamess, 2017)

Para Concluir con la definición de las redes SDN, el plano de control y el plano de datos trabajarán en equipos separados, el control lo tendrá el controlador bajo las normas o funciones programadas por el administrador en la API en un lenguaje de programación de máquina, estas serán transmitidas por el protocolo Open Flow a los switches o a los dispositivos conectados y les asignaran recursos dependiendo la demanda de la red en ese momento y en ese momento el plano de datos y el plano de control trabajaran juntos si la necesidad del equipo lo demanda.

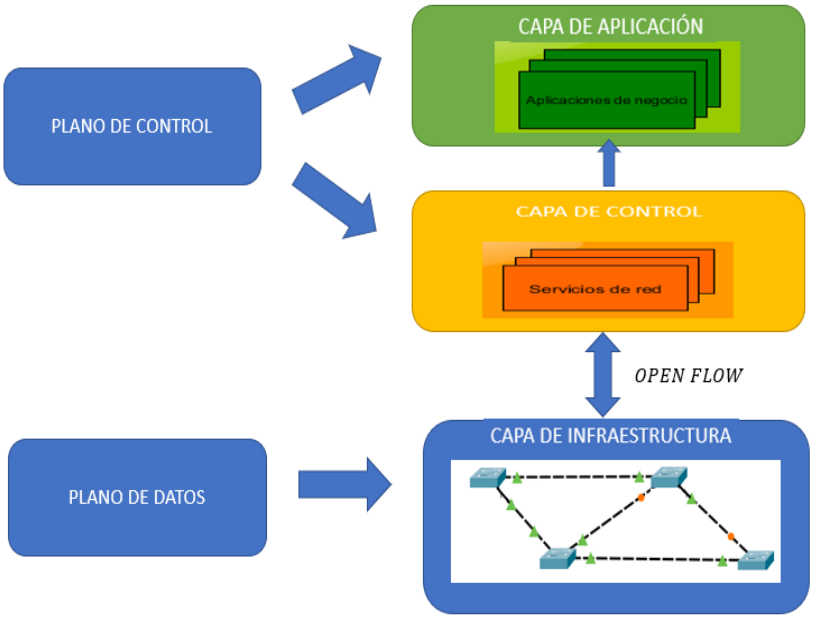


Ilustración 6 Distribución de red SDN

La ilustración previa indica cómo está distribuida la arquitectura SDN debido a que el plano de datos y el plano de control se separan y esto a su vez se distribuye en 3 capas.

2.4.1 Capa de infraestructura

La primera capa de infraestructura es donde entran los dispositivos físicos de la red como, switches, routers, Host (computadoras), los cuales se separan del plano de control para interactuar en el plano de datos ya que se comunican y delegan el control de estos mediante el protocolo Open Flow a un controlador el cual es el encargado de administrar y gestionar de una manera centralizada toda la información desde la capa de control.(Zeng et al., 2020)

En esta capa es donde se realiza la conmutación de los dispositivos aplicando inteligencia artificial ya que los paquetes entrantes de los equipos intermedios van directamente al controlador para que su Heider sea revisada y se pueda obtener un status de errores que pueda contener la misma, así mismo de manera ordenada todos los paquetes son enviados al controlador par que mediante tablas sean analizadas y sean reenviados a los destinos correspondientes, a esto se le denomina hardware de reenvío.

2.4.2 Capa de control

La segunda capa de infraestructura SDN es una de las más primordiales ya que se dedica a monitorear y gestionar los flujos en el controlador SDN de manera centralizada.

En la parte intermedia de la infraestructura SDN es donde se encuentra el sistema operativo de la red ya que gestiona la capa de arquitectura y la capa de aplicación con protocolos y políticas en los cuales se puede aplicar programación para que todos los elementos de la red tengan una convergencia en sus diferentes aplicaciones y dispositivos, en resumen, es donde está el control total de la infraestructura

Esta capa es programable debido a que se puede automatizar los flujos de gestión para que la red sea inteligente y pueda corregirse a sí misma en caso de errores, las redes SDN deben tener una tendencia a la automatización y es por lo que la programación juega un papel importante.

2.4.3 Capa de aplicación

La tercera capa de infraestructura SDN ubicada al norte es donde el controlador interactúa con las aplicaciones por medio de un Api que es la interfaz de Aplicación Programática, la misma que permite realizar al sistema operativo diferentes acciones conectándola con lo que el administrador de red lo necesite.(Centeno et al., 2014)

La capa de aplicación utiliza programas con inteligencia artificial que fueron desarrollados con lenguajes de programación, lo interesante en esta capa es que se puede seguir desarrollando aplicaciones de acuerdo con las necesidades de los usuarios ya que los controladores aceptan protocolos de Open Source y esto ayuda a que la administración y gestión sea inteligente en los equipos que soportan SDN, dependiendo de la solución y requerimiento del usuario final.

Un ejemplo de aplicación es implementar en una red una Api que nos ayude a tener un servicio de red ininterrumpido el cual se aplica inteligente artificial por medio de algoritmos para detectar problemas como cuellos de botella y que automáticamente los paquetes de la red puedan tomar otro camino para llegar a su destino final, esto se implementaría en el controlador y se lo aplicaría para todos los dispositivos de red.

2.4.4 Controlador

En una arquitectura SDN uno de los dispositivos primordiales que es el encargado de crear e implementar, ejecutar, distribuir las decisiones es un controlador debido a que es el cerebro de la arquitectura.(Centeno et al., 2014)(Zeng et al., 2020)

Este equipo es también conocido como el control plane de la infraestructura por que se comunican a la data plane al sur y al norte de una red SDN por medio del protocolo Open Flow, esto hace que la red sea centralizada desde un solo dispositivo, en la actualidad los controladores están tendiendo a ser implementados en nube esto hace que los costos operativos y de infraestructura se reduzcan debido a que el controlador puede ser un software y no en un equipo físico como tal.(Zeng et al., 2020)

Los fabricantes de controladores SDN para redes LAN, WLAN, DATACENTER están tendiendo a mantener sus controladores centralizados en una sola plataforma convergente, Cisco por su parte tiene su propio controlador en nube y físico al igual que HPE-Aruba que, si funcionan con Apis propietarias y también de tipo Open Source, en este caso quien se junta más a las soluciones de código abierto es HPE-ARUBA porque se integra con diferentes plataformas.

Hay diferentes implementaciones de controladores. Desde un simple software que dinámicamente añada y suprima flujos, donde el administrador controla toda la red de switches Open Flow y es el responsable del proceso de todos los flujos hasta una implementación con múltiples administradores, cada uno con diferentes cuentas y passwords, que les permite gestionar diferentes conjuntos de flujos. Es lo que se podría asimilar a virtualizar una red con múltiples propietarios.(Zeng et al., 2020)

2.5 Open Flow

Open Flow es un protocolo de comunicación para redes SDN, esta es una de las principales herramientas que hace posible el separar el plano de datos y el plano de control entre los dispositivos que admiten y trabajan con este protocolo, el cual es el más utilizado para este tipo de redes administradas por un controlador en nube. (Al-Somaidai, 2014)

Este protocolo en los últimos años ha aumentado su importancia en la administración de redes, a un nivel en la cual se ha considerado usar este protocolo en la infraestructura de Google, pero esto trae consigo una adaptabilidad de redes actuales y redes con estructuras tradicionales y evitar que esta diferencia sea un problema para el consumidor de sus servicios.(*Open Flow Vulnerability Assessment Enhanced Reader.Pdf*, n.d.)

Si bien este protocolo esta aun en desarrollo al igual que las redes SDN, su seguridad aun es un tema de estudio y el cual se buscará prontas respuestas teniendo en cuenta la importancia de este protocolo en las nuevas redes definidas por software, ya que este le permite transmitir la información del estado de la red para que el controlador pueda evaluar y responder según las reglas o procedimientos programados en la API que está en el dispositivo de control. (*OpenFlow Vulnerability Assessment Enhanced Reader.Pdf*, n.d.)

2.6 Application Programming Interfaces (API)

API se traduce como interfaz de programación de aplicaciones, con una interfaz que visualmente no se diferencia de otras utilizadas en software libre, esta permitirá la comprensión de los dispositivos externos con el controlador, además de tener la programación que usará el controlador para brindar una respuesta a las solicitudes que realicen los equipos de la red.(Pereira & Gamess, 2017)

Esta API contiene todas las normas, leyes y respuestas programadas por el administrador y el cual desarrollara esta aplicación dependiendo de las necesidades de su red, además te poder tener un control total de su red y tener una administración que pueda responder y resolver problemas que se presenten en la red, si el controlador tiene en su programación una respuesta oportuna para el inconveniente que se presentó, eso beneficia a la efectividad y confiabilidad de la red ya que tiene una administración autónoma, aunque no en su totalidad, ya que aún necesita del administrador para desarrollar su programación y resolver problemas extraños al sistema.

2.7 Hewlett-Packard-Enterprise (HPE)

HPE inicio después de la separación que obtuvo de HP, el cual se dedicó a la infraestructura facilitando así a las empresas el cual necesitaba no solo comercializar impresoras, ordenadores sino una manera de la administración de la información y software.(Industrial, 2018)

HPE unió a Aruba con el objetivo de brindar servicio de soporte de internet por el cual SDN ha conseguido un correcto funcionamiento ya que se caracteriza por la capacidad, diseño y eficiencia, considerando la herramienta Standard Open Flow y Brocade

Hewlett- Packard sostenida por ONF (Open Networking Foundation) organización creada por el usuario para el desarrollo de Software.(Fabrizio, 2018)

Cuando hablamos de Brocade nos referimos a uno de los primeros en utilizar Open Flow también caracterizado por el uso de modo híbrido, el cual va a permitir que en un solo puerto pueda incorporar el switching, routing y el Open Flow. Siendo así un gestionador de datos y de almacenamiento en red.(Zeng et al., 2020)

2.7.1 Controlador SDN VAN HPE

Este controlador de SDN HP Virtual Application Networks (VAN) es apto para desarrollar y administrar el plano de control de equipos ampliando la posibilidad de mayor control e interacción para beneficio de la red. A continuación, las siguientes características del controlador:

El controlador es una estructura por interfaces abierta programable, el cual nos indica que el Software da acceso a HP para la aplicación de SDN, con el fin del funcionamiento más eficiente y eficaz. El controlador HP VAN SDN da acceso al implemento de aplicaciones y la mecanización con Protocolos Open Flow brindando así control manejable y centralizado que nos permita verificar la ruta donde se está enviando la información sea larga o corta.(Wallace et al., 2016)

La accesibilidad y escalabilidad del software del controlador SDN HP Virtual Application Networks (VAN) está planificado para la adecuada productividad y funcionamiento de la respectiva red.(Wallace et al., 2016)

El SDN HP Virtual Application Networks caracterizado también por la seguridad altamente eficiente para el uso de los usuarios, siendo un controlador responsable de una conexión segura.(Wallace et al., 2016)

Para el manejo del controlador hay dos topologías de red como en la ilustración 7 (control centralizado) tenemos el control centralizado, en este el controlador es enlazado directamente a un switch esto nos permite observar de la red, también la administración del ancho de banda y organización inteligente del mismo, para esta topología se puede utilizar un solo software para uso de la red.

Con respecto a la figura a continuación (Control distribuido) tenemos el controlador distribuido, el cual podemos ver que hay varios controladores en diferentes puntos de los instrumentos de la red, esta topología es implementada cuando tenemos una gran variedad de redes.(BARRIOS, 2014)

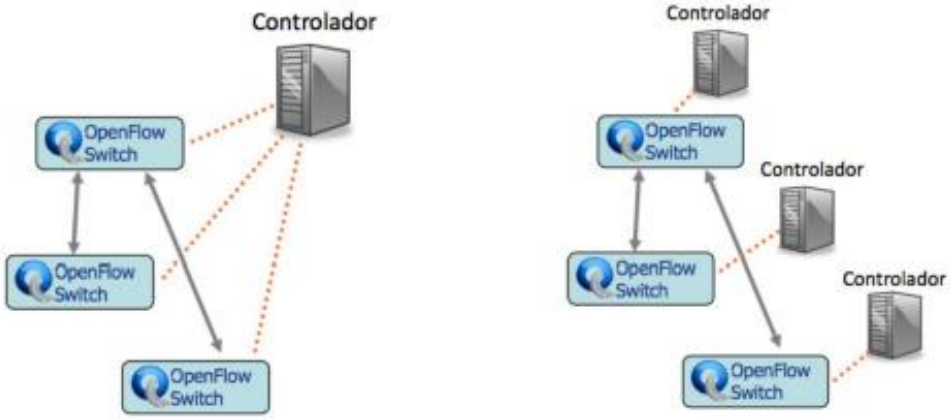


Ilustración 7 Topologías de red con controlador en operación. (BARRIOS, 2014)

El controlador debe utilizar un tipo de enrutamiento puede ser de flujo o enrutamiento de agregación.

2.7.2 Enrutamiento Por Flujo

El flujo se ordena mediante números empezado en 0 el cual es desarrollado en el controlador el cual cada paquete es recibido para la inspección de cada detalle de la tabla de flujo.

Cada tabla de flujos contiene una entrada el cual tiene otro acceso para la categoría de los flujos. En el controlador va a presentar varias conductas caracterizadas por lo siguiente:

2.7.2.1 Controlador de Reactivo

En el caso que no se use una tabla de flujo por un tiempo acordado este provoca la reiniciación y el acceso a nuevos paquetes de entrada. Cada flujo y controlador conlleva tiempo para su configuración, si en tal caso ocurriera una desconexión o falla en el controlador, el switch puede dar una ventaja quedándose con la última actualización antes hecha.(BARRIOS, 2014)

2.7.2.2 Control Proactivo

Antes de la configuración de tablas de flujo se puede dar a conocer que elementos deben estar implementados para el manejo del controlador, por otra parte, si se hallara una desconexión del controlador no se vería afectado la ruta de su señal.(BARRIOS, 2014)

2.8 Aruba Central

Es la integración de inteligencia artificial el cual está comprendido por el acceso rápido para la administración, mantenimiento y distinción los dispositivos de cada usuario desde un solo panel. Con Aruba Central podemos optimizar el tiempo de administración de los equipos porque tenemos una plataforma centralizada para todos los dispositivos como Switches, Access Points entre otros si estos elementos de la infraestructura están centralizados se puede desarrollar ajustes o control en la misma.

Aruba AIOps es una ventaja que viene con Aruba central el cual proporciona alertas sobre lo que está pasando en la red LAN para así brindar mayor seguridad en tiempo real y también puede crear informes donde se encuentran alguna falla y esta emite una alerta al administrador de red para que pueda visualizar y atender a la necesidad de la red de manera remota sin necesidad de asistir al sitio. (Soluci, 2019)

2.8.1 Arquitectura Spine and Leaf

Este tipo de topología está diseñado para dar una mayor conectividad de los switches, a través del centro de redes llegar a obtener una mejor escalabilidad y eficiencia. Esta arquitectura Leaf-Spine se espera que implementen las empresas pequeñas ya que podemos enlazar todos los switches de acceso a un switch de interconexión, es decir que un servidor puede conectarse con otros servidores a través de una ruta de switches de interconexión entre dos switches de acceso.(Henri, 2018)

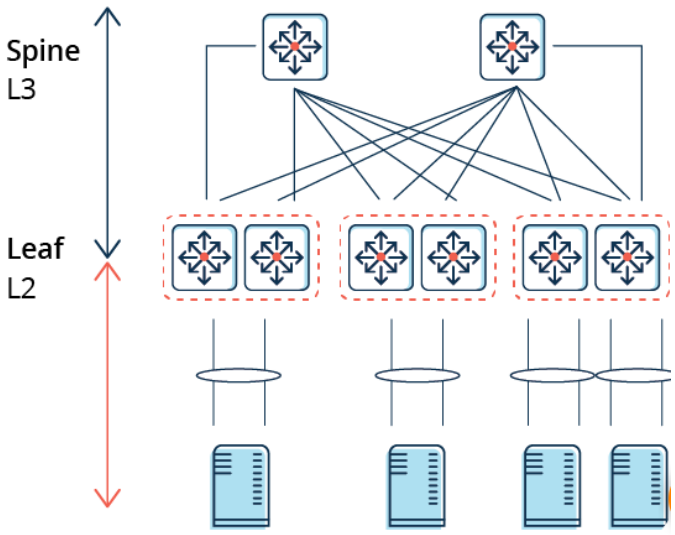


Ilustración 8 Arquitectura Spine and Leaf ((*1) New Messages!*, n.d.)

2.9 Cisco DNA Center

Cisco DNA son las siglas para abreviar a Cisco Digital Network Architecture es una controladora desarrollada por la empresa del mismo nombre Cisco, esta permite el diseño de nuevas redes basadas en SDN, este equipo de control trabaja con los equipos de su infraestructura como AP, switches, routers, políticas, analíticas y además facilita la configuración inicial de tareas operativas, también posee una interfaz amigable con los administradores menos experimentados y de esta manera tener un ahorro en tiempo y una disminución en la complejidad de una administración de los recursos de la red, además de tener el benefició de ser editable para que cada usuario pueda acoplar la herramienta para que trabaje con los requerimientos de cada red. (Thesis, 2019)

DNA Center es una plataforma la cual contiene una interfaz web y varias interfaces de programación de aplicaciones más conocidas como API, las cuales ayudaran a la automatización y a la simplificación de procesos dentro de la red, permitiendo así a los

administradores segmentar de una manera más efectiva los recursos de la red y de esta manera incrementar la productividad de la red, esto se logra con un trabajo coordinado de DNA Center y Cisco SD-Access ya que esta última es una herramienta puede automatizar las políticas de acceso de los usuarios con el fin de que las empresas tengan un mayor control. (Thesis, 2019)

2.10 Cisco SD-Access

Cisco SD-Access traducido al español significa “Acceso definido por software”, es una solución de la empresa Cisco que trabaja en las arquitecturas de red de la controladora Cisco DNA para redes definidas por software, esta herramienta realiza una separación automática de tráfico, diferenciando que este sea de usuarios, de dispositivos y aplicaciones, esto se puede lograr con la red actual y no tener que invertir en un rediseño, este es el resultado de lograr la separación de la capa de datos y de la capa de control de los equipos, de igual manera y como se ha mencionado anteriormente como un beneficio de redes SDN, el automatizar procesos en la red involucra una mayor eficiencia de la misma, ya que reduce la intervención humana por un sistema casi autónomo en su totalidad. (Ponce Yumbato, 2020)

Su enfoque está en un sistema de red autónomo en su administración ya que este controlará desde las tareas más sencillas, hasta tareas como monitoreo, resolución de problemas en la red, alarmas, configuración de puertos y políticas, etc. Trabajando juntamente con Cisco DNA como controladora de los equipos en una red administrada por software se logra un control casi total de la red en producción y una garantía para

los usuarios de una red de calidad que brinde los servicios necesarios para tener una experiencia de calidad al usar la red y sus recursos. (Ponce Yumbato, 2020)

2.11 MININET

En cuanto a redes SDN tenemos un sistema avanzado con una gran capacidad autónoma de autogestión de recursos por lo cual lo convierte en una nueva topología muy poderosa, pero a su vez muy costosa hablando en el punto económico por esta y muchas razones se han desarrollado emuladores para estas redes, los cuales permitirán experimentar con un entorno lo más real posible para que el personal tenga un dimensionamiento claro de lo que necesita para implementar esta red definida por software.(Valencia et al., 2015)

En el campo de las redes definidas por software existen muchas investigaciones que se han desarrollado, las mismas han buscado software de simulación para poder completar la indagación que cumplan con los objetivos en cuando a redes SDN.(Nielsen, 2009)

Al simular una red SDN nos permitirá, evaluar, corregir y comprobar el rendimiento de los equipos en la red, además de establecer todos los estándares o protocolos que se usaran para el correcto funcionamiento de la red ya en producción, además de poder simular escenarios complejos que pueden o no existir en las industrias.

El emulador Mininet es un software que nos permite realizar simulaciones con un ambiente casi real, es de código abierto lo cual le permite ser editado para un mejor uso y además de ser rápidamente configurable. Este emulador puede realizar variar redes de un solo núcleo del sistema operativo, además tiene la habilidad de utilizar la

red real de nuestro ordenador, lo que le permite interactuar con equipos reales de nuestra red.(Valencia et al., 2015)

Mininet contiene en su catálogo de equipos, switches, hosts, controladores y enlaces entre estos y al ser un emulador, las prestaciones son muy altas, ya que no se necesitan los equipos físicos para poder realizar pruebas, además de tener grandes cualidades como flexibilidad, escalabilidad e interactividad, lo cual elevan su valor en el sector de softwares para simular redes SDN.(Nielsen, 2009)

2.12 Cisco Packet Tracer

Packet Tracer es un simulador muy poderoso y usado en la actualidad para la simulación de redes con equipos de la marca Cisco, además según la definición que encontramos en su página web es: “Este laboratorio virtual es una forma interactiva de practicar habilidades de redes, IoT y ciberseguridad, ¡sin necesidad de hardware! Utilice Packet Tracer como entorno de aprendizaje para cursos, aprendizaje a distancia, capacitación profesional, planificación del trabajo o simplemente para divertirse.”.(Tarkaa et al., 2017)

Este simulador ya tiene algunos años en el mercado y ha tenido un desarrollo junto con su tecnología, lo cual en cada versión lanzada se implementa y se mejoran las herramientas que presta este software para que el entorno de simulación sea cada día más real para el administrador, además de proporcionar un catálogo de equipos muy extenso y con administración total de los equipos simulados.

En las últimas actualizaciones Packet Tracer ha empezado a implementar las herramientas para poder simular una red definida por software, ya que como se

mencionó en el anterior párrafo, el desarrollo de su plataforma de simulación está coordinada con el avance tecnológico que tiene Cisco como empresa de soluciones de redes y su administración.(Ghaliya Alfarsi, 2020)

CAPÍTULO 3
DISEÑO, SIMULACIÓN Y MEDICIÓN

En este capítulo se detallará el proceso de simulación de la red jerárquica que se encuentra en producción en el campus sur de la Universidad Politécnica Salesiana y de la red definida por software en relación con los requisitos y estructura actual de la institución, además de identificar la complejidad de cada una para lograr una simulación completa y lo más real posible, además se enlistarán los equipos utilizados para la simulación para obtener un dimensionamiento amplio al momento de comparar y realizar las evaluaciones en capítulos siguientes.

3.1 Revisión de la red jerárquica de la UPS

Para esta sección, se mantuvieron algunas sesiones con uno de los ingenieros a cargo, de esta manera logramos un amplio conocimiento sobre la dimensión de la red, su estructura actual de producción. La red de la UPS tiene una segmentación para su mejor administración, los modelos de los equipos que están en este momento en la infraestructura y las capas que se deben considerar en el diseño de la red, todos estos puntos serán explicados a continuación.

La red de la Universidad es 172.17.x.x /16, esta red contiene 32.767 direcciones habilitadas para Host, sin contar con la primera y la última dirección que tienen otra función, esta red contiene una gran capacidad por ser máscara de 16 bits. Para un mejor manejo y control de la red, esta fue segmentada para poder organizar los equipos en cada uno de los bloques de la universidad y también para que la seguridad de la red

sea mayor, esta separación de la red se realizó en relación con la necesidad de la universidad y se realizará el mismo proceso de segmentación según la necesidad en la simulación, a continuación se muestra la topología lógica y física de la red actual de la institución.

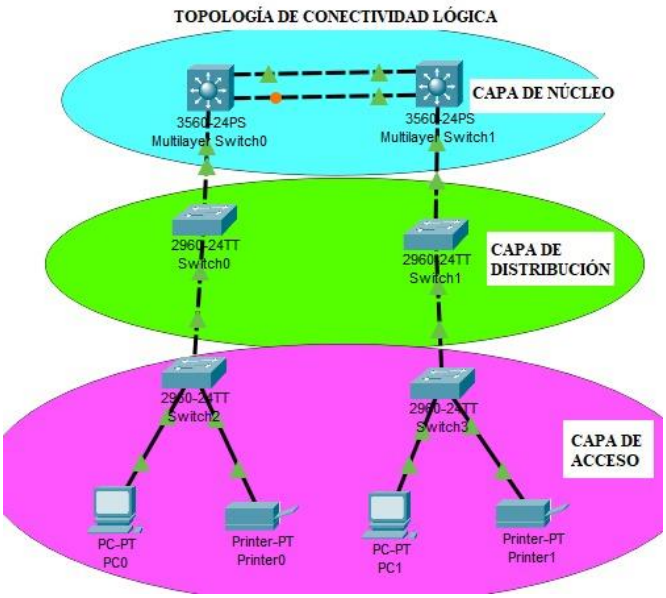


Ilustración 9 Topología Lógica de la Universidad Politécnica Salesiana

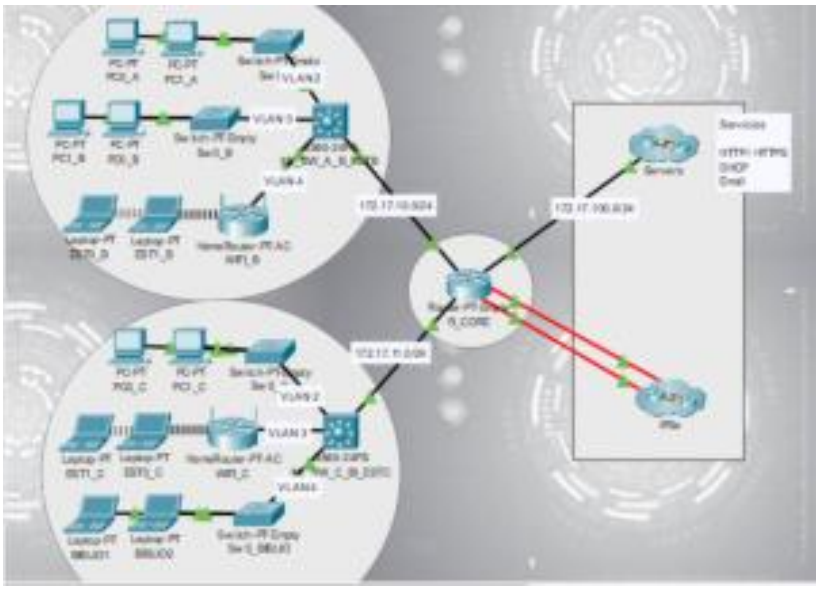


Ilustración 10 Topología Física de la Universidad Politécnica Salesiana

Los equipos que se encuentran en ese momento en producción en su mayoría son de la empresa Cisco, los modelos de los equipos son 2960, 2960X, 3560, 3750, todos estos equipos son switches encargados de la conexión y el transporte de datos dentro de toda la red, además de tener una administración en capa 2 y capa 3 de la red jerárquica, dentro de la simulación se busca mantener un solo modelo ya que su funcionamiento en la red es similar y también para poder generar una estructura más comprensiva para el lector.

3.2 Diseño de la red jerárquica

En la presente sección se describirá la planificación y el diseño de la red, previo a la simulación, en este punto se realiza el estudio de equipos en cuanto a cantidades y distribución, también se detallará la segmentación de la red y la asignación de direcciones a cada equipo en la infraestructura.

3.2.1 Subneteo de la red

El Subneteo como fue explicado en el capítulo anterior, es una técnica que sirve para segmentar una red grande en redes de menor tamaño y este proceso se realizará a la red actual de la UPS, que es la red 172.17.0.0, con máscara 255.255.0.0, y con lo cual buscaremos crear redes de 254 host que posee una máscara de 24 bits, a continuación, se muestra una tabla con el Subneteo que se generó con las direcciones IPv4.

Tabla 2 Subneteo de Red de la UPS

Subred	Dirección de Red	1era Dir. Host	Ultima Dir. Host	Máscara
1	172.17.1.0	172.17.1.1	172.17.1.254	255.255.255.0
2	172.17.2.0	172.17.2.1	172.17.2.254	255.255.255.0
3	172.17.3.0	172.17.3.1	172.17.3.254	255.255.255.0
4	172.17.4.0	172.17.4.1	172.17.4.254	255.255.255.0
5	172.17.5.0	172.17.5.1	172.17.5.254	255.255.255.0
6	172.17.6.0	172.17.6.1	172.17.6.254	255.255.255.0

Con la segmentación realizada, se asignará una subred para cada una de las zonas que serán simuladas en Packet Tracer, las zonas son; Bloque A, Bloque B, Estudiantes Bloq_B, Bloque C, Biblioteca y Estudiantes Bloq_C, y se detalla a continuación, la distribución de las subredes.

Tabla 3 Distribución Subredes - Zonas

Zona	RED	Broadcast	Máscara
Bloque A	172.17.1.0	172.17.1.255	255.255.255.0
Bloque B	172.17.2.0	172.17.2.255	255.255.255.0
Estudiantes Bloq_B	172.17.3.0	172.17.3.255	255.255.255.0
Bloque C	172.17.4.0	172.17.4.255	255.255.255.0
Biblioteca	172.17.5.0	172.17.5.255	255.255.255.0
Estudiantes Bloq_C	172.17.6.0	172.17.6.255	255.255.255.0

3.2.2 Distribución de la red jerárquica

Cada zona en la simulación contará con dos usuarios, ya sean estas computadoras de escritorio o portátiles, además de un switch de paso, que cumplirá con la función de conectar todos los equipos de cada bloque entre sí. Se unirá agruparán 3 zonas en una switch multicapa, el mismo será el encargado de realizar los enlaces virtuales (VLAN), estos equipos que serán 2 saldrán a un router de Core que tendrá una posición central en la red, a este también se conectan los dos proveedores de servicios o ISP, además de los servidores locales del campus, esta implementación en el simulador se explicará más adelante.

Los switch Multicapa son del modelo “3560-24PS”, este modelo permite un control de capa 2, realizar Vlan para poder separar a cada bloque con su propia subred y que tengan su propia comunicación con el resto de los equipos sin pertenecer a la misma subred, esto se realiza para tener una mejor administración de los equipos de red.

Para cubrir la capa 3 de control tenemos un router modelo “Router-PT-Empty”, en el cual se realizó la tabla de enrutamiento de todas las subredes, además la cantidad de redes para esta simulación es pequeña, por lo cual, se trabajó sin protocolos de enrutamiento, además este modelo también fue usado para poner en red a los dos ISP que contiene la universidad y aunque no tienen participación ya que es una evaluación local es importante su consideración dentro de la topología de red.

En relación con los servicios, se utilizaron dos servidores, modelo Packet Tracer “Server-PT”, el cual permite tener los servicios de manera local, por ejemplo, DHCP para cada subred, página web con HTTP, DNS para la navegación de los usuarios y correo electrónico de manera local con los usuarios conectados al servidor.

3.2.3 Cantidad de equipos de la red jerárquica

Para comenzar la simulación en Packet Tracer se usa un documento en blanco del software para empezar a trabajar, a continuación, se muestra una tabla con las cantidades y modelos de los equipos que se utilizaron en la simulación.

Tabla 4 Cantidades y modelos en la simulación

Modelo	Descripción	cantidad
PC-PT	Computadoras de escritorio	6
Laptop-PT	Computadoras portátiles	6
Switch-PT	Switch de paso	5
HomeRouter-PT-AC	switch de paso Wifi	2
3560-24PS	Switch Multicapa	2
Router-PT-Empty	Routers	3
Server-PT	Servidores	2

3.3 Simulador para la red jerárquica

En el área de la simulación de redes existen una gran cantidad de emuladores, cada uno con su diferenciador en el mercado y por lo cual los usuarios deciden utilizarlos para algún trabajo en específico, para la simulación de la red jerárquica, se utilizará el simulador de redes llamado Packet Tracer en el sistema operativo de Windows.

3.3.1 Software de simulación Cisco Packet Tracer

Esta aplicación funciona en el sistema operativo Windows que es en el más común utilizado en ordenadores de consumo, en este caso se instaló la última versión

encontrada hasta la fecha, la cual es, Packet Tracer 8.1.0, no se necesita instalar herramientas adicionales por lo cual la instalación ha concluido.

Por su interfaz completa y sus herramientas la convierten en un simulador potente en el campo de redes, por lo cual esta aplicación es óptima para desarrollar la red jerárquica del presente proyecto técnico.

3.3.2 Simulación de la red jerárquica de la Universidad Politécnica Salesiana

En este punto se describirá el proceso de simulación de la red jerárquica de la UPS campus sur, Subneteo de la red utilizada en la actualidad, equipos utilizados, procesos de conexión de equipos, políticas y protocolos implementados y el levantamiento de servicios de manera local por los servidores del campus.

La simulación se dividirá en dos secciones a partir de un elemento central que será el router de core, a la derecha de este equipo se colocarán los servidores y los dos routers que se consideran como ISP´s, y a su izquierda se colocan primero los elementos más cercanos al router que son los dos switches multicapa, siguiendo los switches de paso para finalmente colocar en agrupaciones de 2, los equipos finales, a continuación se muestra una tabla con el contenido de cada agrupación y los nombres de los equipos finales que se colocarán, tomando en cuenta que cada agrupación es una zona que se mencionó en anteriores párrafos.

Tabla 5 Equipos y Nombres por Zonas

Bloque A	Bloque B	Estudiantes Bloq_B	Bloque C	Biblioteca	Estudiantes Bloq_C
PC0_A (PC-PT)	PC0_B (PC-PT)	EST0_B (Laptop-PT)	PC0_C (PC-PT)	BIBLIO1 (Laptop-PT)	EST0_C (Laptop-PT)
PC1_A (PC-PT)	PC1_B (PC-PT)	EST1_B (Laptop-PT)	PC1_C (PC-PT)	BIBLIO2 (Laptop-PT)	EST1_C (Laptop-PT)

Después de organizar los equipos en la pantalla del simulador se deben añadir los módulos necesarios para la conexión en los equipos que se requieran, se debe apagar el equipo y reemplazar el módulo arrastrándolo con el mouse. Comenzando desde los equipos de host, tenemos las laptops de las zonas de "Estudiantes Bloq_B", estos equipos tienen que cambiar el puerto RJ-45 por una antena para su conexión Wifi, y existen varios módulos para poder habilitar está opción en el equipo la que se eligió en este caso es la antena "WPC300N", a continuación, se muestra una imagen del equipo.

Ilustración 11 Laptop de Cisco Packet Tracer con antena WPC300N

Continuando con los switches de paso, “Switch-PT-Empty”, tienen la característica en la simulación de tener 10 ranuras para adicionar puertos dependiendo de la necesidad de la red, en este caso se añaden 8 puertos RJ-45 de FastEthernet, “PT-SWITCH-NM-1CFE”, y los dos restantes se añadirán 2 puertos RJ-45 de GigaEthernet, “PT-SWITCH-NM-1CGE”, el switch de paso con los puertos se muestra en la siguiente ilustración.

Ilustración 12 Puertos RJ-45 en Switch de paso de Packet Tracer

En cuanto a los switches multicapa, no se requiere ningún modulo adicional, se utilizarán los 24 puertos integrados por default en su diseño, los puertos se indican en la siguiente ilustración.

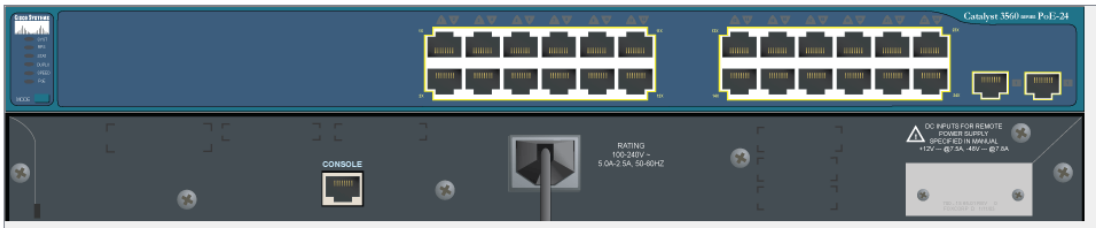


Ilustración 13 Switch Multicapa de 24PS de Packet Tracer

En cuando al router central que será utilizado, posee 10 slots para la integración de los puertos necesarios, en este caso al ser un router necesita una gran variedad de conexiones, por esta razón se le agregó 4 puertos RJ-45 de FastEthernet, 1 puerto de fibra de FastEthernet, 1 puerto serial, 1 puerto de fibra de GigaEthernet, 3 puertos RJ-45 de GigaEthernet.

Ilustración 14 Router Core de Packet Tracer

Por último, en los servidores no se debe alterar su diseño, ya que para esta simulación los puertos por defecto son los ideales para poder trabajar, estos son un puerto RJ-45 de FastEthernet y un puerto RJ-45 de GigaEthernet.

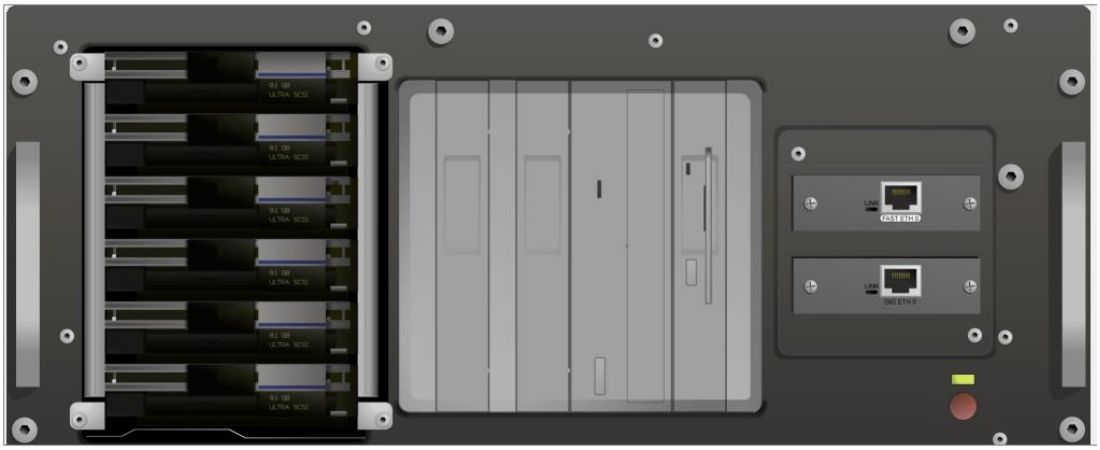


Ilustración 15 Servidor de Packet Tracer

Con esto se concluye la edición de los equipos que serán utilizados en la simulación, los mismos que en el subtítulo siguiente serán conectados y habilitados para su funcionamiento en la red.

3.3.3 Conexión y configuración de equipos

En este título se conectarán y se configurarán todos los equipos para que puedan tener una comunicación entre todos los dispositivos de la red, por lo cual se iniciará con una lista de los equipos y nombres que se le asignarán en la topología para identificarlos.

Tabla 6 Tabla de equipos y nombres de la topología

Modelo	Nombre
PC-PT	PC0_A
PC-PT	PC1_A
PC-PT	PC0_B
PC-PT	PC1_B
PC-PT	PC0_C
PC-PT	PC1_C
Laptop-PT	EST0_B
Laptop-PT	EST1_B
Laptop-PT	EST0_C
Laptop-PT	EST1_C
Laptop-PT	BIBLIO1
Laptop-PT	BIBLIO2
Switch-PT	SW0_A
Switch-PT	SW0_B
Switch-PT	SW0_C
Switch-PT	SW0_BIBLIO
Switch-PT	SW0_Servers
HomeRouter-PT-AC	WIFI_B
HomeRouter-PT-AC	WIFI_C
3560-24PS	ML_SW_A_B_ESTB
3560-24PS	ML_SW_C_BI_ESTC
Router-PT-Empty	R_CORE
Router-PT-Empty	ISP1
Router-PT-Empty	ISP2
Server-PT	Server-UPS
Server-PT	Server-AVAC

Se iniciará con la conexión partiendo del router R_CORE, el cual tendrá las siguientes conexiones con cable de cobre, el puerto Fa0/0 al puerto Fa0/5 de

ML_SW_A_B_ESTB, el puerto FA1/0 al puerto Fa0/4 de ML_SW_C_BI_ESTC, el puerto Gig0/9 al puerto Gig9/1 de SW0_Servers. Las próximas conexiones serán con los routers de los ISP´s con cable de fibra, el puerto Gig6/0 al puerto Gig4/0 de ISP2 y finalmente el puerto Gig4/0 al puerto Gig4/0 de ISP1.

Continuando con el lado derecho de la topología, se conectará los switches multicapa con los switches de paso y routers Wifi que se pueden considerar como Access Point, las conexiones se realizarán con cable de cobre, el puerto Fa0/2 al puerto Fa2/1 de SW0_A, el puerto Fa0/3 al puerto Fa2/1 de SW0_B Y finalmente el puerto Fa0/4 al puerto 0/0 de WIFI_B.

Para el segundo switch multicapa se tienen conexiones similares al explicado anteriormente, las conexiones se harán con cable de cobre, el puerto Fa0/3 al puerto Fa2/1 de SW0_C, el puerto Fa0/2 al puerto Fa2/1 de SW0_BIBLIO Y finalmente el puerto Fa0/1 al puerto 0/0 de WIFI_B.

Siguiendo el orden la conexión de los equipos finales con los switches de paso, no son de gran importancia ya que pueden conectarse en cualquier puerto de estos equipos, y en cuanto a los equipos Wifi se debe conectar a la red inalámbrica respectiva con el nombre y la contraseña de este.

Al concluir con todas las conexiones de los equipos se pueden configurar las direcciones IPv4, ya sea por medio de la interfaz gráfica o por medio de CLI de los equipos, en esta ocasión se empezará el enrutamiento de los equipos con direcciones IP fijas, los cuales serán, los switches multicapa, los routers, y los servidores, de acuerdo al proceso de Subneteo realizado en la tabla 3, se asignarán direcciones IP a los equipos como se muestra en la siguiente tabla, además de configurar Vlan en los equipos respectivos.

Tabla 7 Enrutamiento IP de cada Equipo

VLAN2 (ML_SW_A_B_ESTB)		
Gateway (R_CORE)	172.17.1.1	Estática
PC0_A	172.17.1.10	DHCP
PC1_A	172.17.1.11	DHCP
VLAN3 (ML_SW_A_B_ESTB)		
Gateway (R_CORE)	172.17.2.1	Estática
PC0_B	172.17.2.10	DHCP
PC1_B	172.17.2.11	DHCP
VLAN4 (ML_SW_A_B_ESTB)		
Gateway (R_CORE)	172.17.3.1	Estática
EST0_B	172.17.3.10	DHCP
EST1_B	172.17.3.11	DHCP
VLAN2 (ML_SW_C_BI_ESTC)		
Gateway (R_CORE)	172.17.4.1	Estática
PC0_C	172.17.4.10	DHCP
PC1_C	172.17.4.11	DHCP
VLAN3 (ML_SW_C_BI_ESTC)		
Gateway (R_CORE)	172.17.5.1	Estática
BIBLIO1	172.17.5.10	DHCP
BIBLIO2	172.17.5.11	DHCP
VLAN4 (ML_SW_C_BI_ESTC)		
Gateway (R_CORE)	172.17.6.1	Estática
EST0_C	172.17.6.10	DHCP
EST1_C	172.17.6.11	DHCP
Servidores		
Gateway (R_CORE)	172.17.100.1	Estática
Server-UPS	172.17.100.2	Estática
Server-AVAC	172.17.100.3	Estática
Proveedores de servicio		
Gateway (R_CORE)	172.17.12.1 172.17.13.1	Estática
ISP1	172.17.12.2	Estática
ISP2	172.17.13.2	Estática

Se creó Vlan en los equipos indicados en la tabla, además se les asigna las direcciones estáticas a los equipos que las poseen, para los equipos finales que poseen su dirección por medio de DHCP, ese servicio ya proporcionara los servidores cuando se habilite este.

Para el enrutamiento, en la simulación se usará enrutamiento estático ya que no existe gran cantidad de subredes además de demostrar una de las formas básicas de enrutamiento que se ha mantenido durante muchos años, realizando el enrutamiento en su totalidad para que la comunicación sea exitosa con todos los equipos de red, el enrutamiento se da en el equipo R_CORE y se muestra a continuación.

```
     172.17.0.0/24 is subnetted, 10 subnets
C       172.17.1.0 is directly connected, FastEthernet0/0.2
C       172.17.2.0 is directly connected, FastEthernet0/0.3
C       172.17.3.0 is directly connected, FastEthernet0/0.4
C       172.17.4.0 is directly connected, FastEthernet1/0.2
C       172.17.5.0 is directly connected, FastEthernet1/0.3
C       172.17.6.0 is directly connected, FastEthernet1/0.4
C       172.17.11.0 is directly connected, FastEthernet0/0
C       172.17.12.0 is directly connected, GigabitEthernet4/0
C       172.17.13.0 is directly connected, GigabitEthernet6/0
C       172.17.100.0 is directly connected, GigabitEthernet9/0
```

Ilustración 16 Enrutamiento estático en R_CORE

3.3.4 Habilitar servicios

Para tener un entorno más real, se habilitarán los servicios en los dos servidores de la topología, comenzando por el DHCP el cual asignará direcciones IPv4 a los equipos finales, el rango de asignación será desde la 10ma dirección habilitada, por ejemplo, para la red del bloque A que es la 172.17.1.0, la primera dirección habilitada para host por DHCP será 172.17.1.10, ya que suelen reservar las primeras direcciones para equipos con direcciones estáticas y de gran importancia en la red.

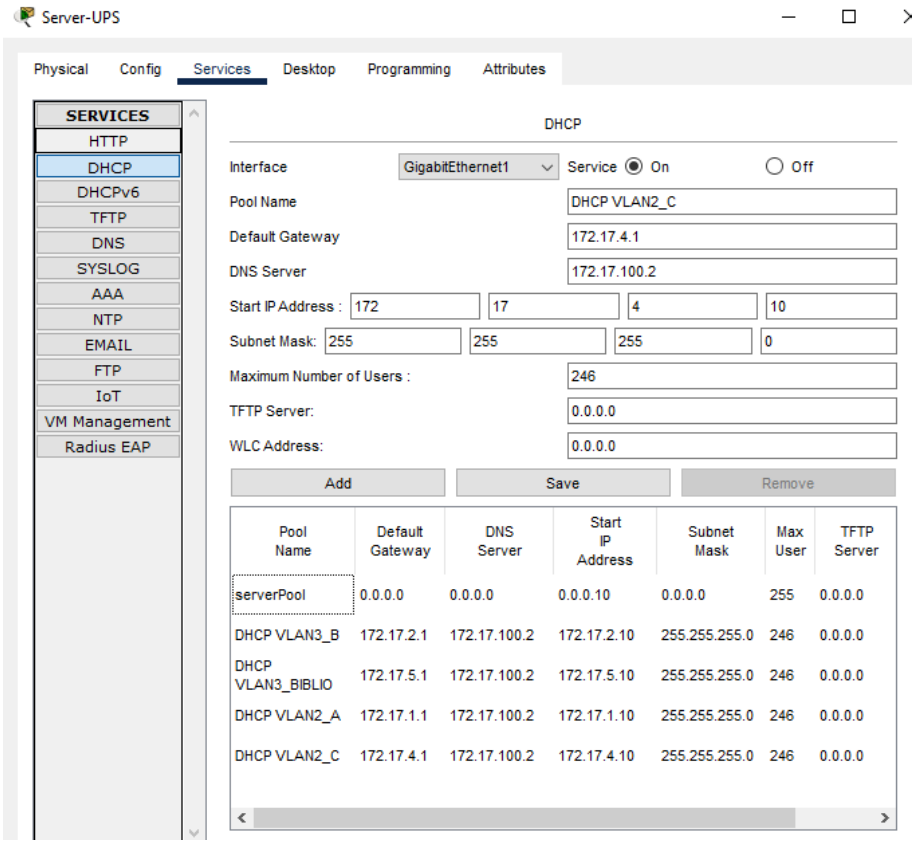


Ilustración 17 Configuración DHCP para Vlan 2 del bloque C

El servidor encargado del DHCP para cada red se detalla en la siguiente tabla.

Tabla 8 Servidores DHCP y las redes para asignación

SERVER-UPS	Inicio	Final
Bloque A	172.17.1.10	172.17.1.254
Bloque B	172.17.2.10	172.17.2.254
Bloque C	172.17.4.10	172.17.4.254
BLIBLIOTECA	172.17.5.10	172.17.5.254

SERVER-AVAC	Inicio	Final
Estudiantes Bloq_B	172.17.3.10	172.17.3.254
Estudiantes Bloq_C	172.17.6.10	172.17.6.254

El servicio de HTTP es muy importante para poder hacer uso de los recursos del mismo, se habilitará en el equipo y en la sección de “índex” cagará una imagen, en Server_UPS una imagen de la página de la Universidad y en Server_AVAC una

imagen de la página de AVAC, para que se pueda ver desde las computadoras de los usuarios, además se activará el servicio de DNS, en el cual se asignará la dirección IP, para el servidor de UPS se usaran los nombres, www.ups.com y ups, además, para el servidor AVAC se utilizarán los nombres, www.avac.com y avac, la respuesta al buscar por web service "ups" debe ser como se muestra en la imagen a continuación.

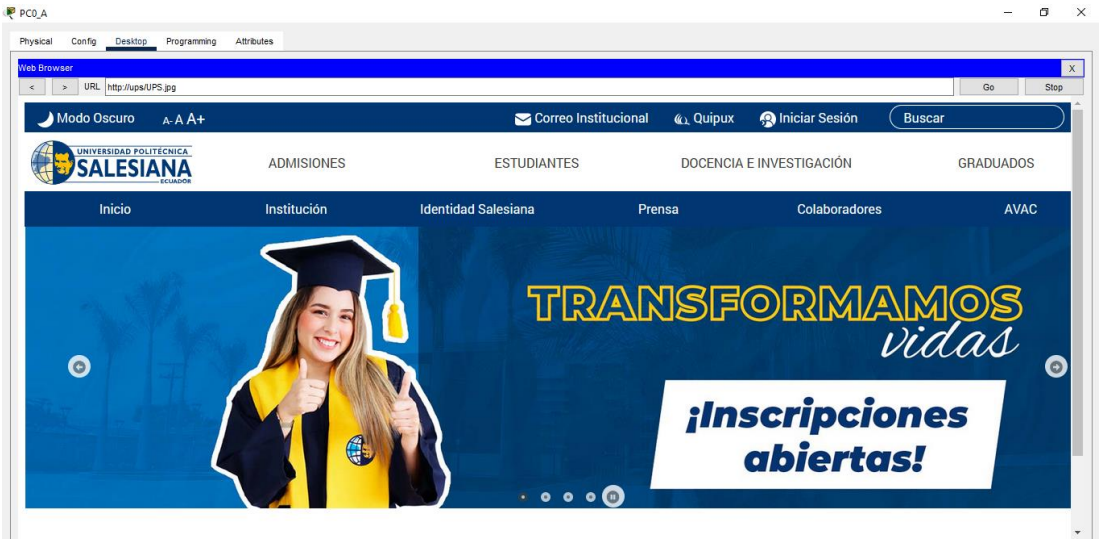


Ilustración 18 Web Service de PC0_A - búsqueda de UPS

Por último activa el servicio de correo para que puedan comunicarse los usuarios finales por medio de correo electrónico, con ayuda del servidor y de los usuarios creados en este, el dominio a usar será, @ups.edu.ec para todos los usuarios, además se usa como nombre el mismo del equipo final, por ejemplo, la computadora PC0_A, tiene el correo, PC0_A@ups.edu.ec y con el cual se puede enviar correos electrónicos al resto de usuarios, algunas pruebas realizadas se muestran a continuación.

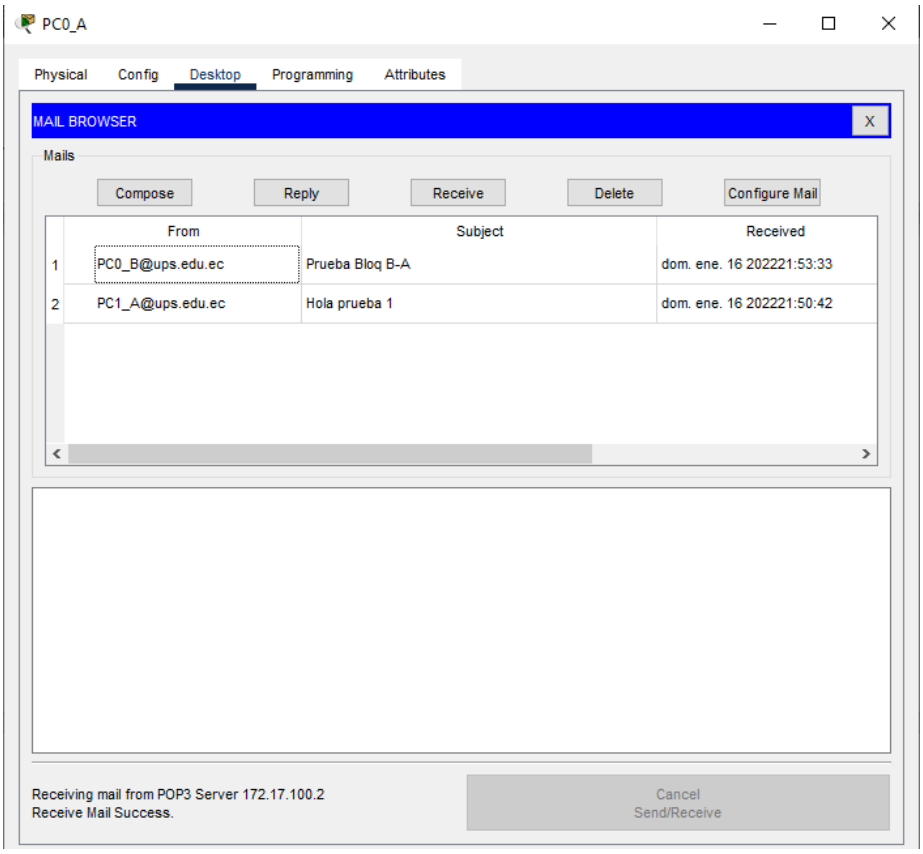
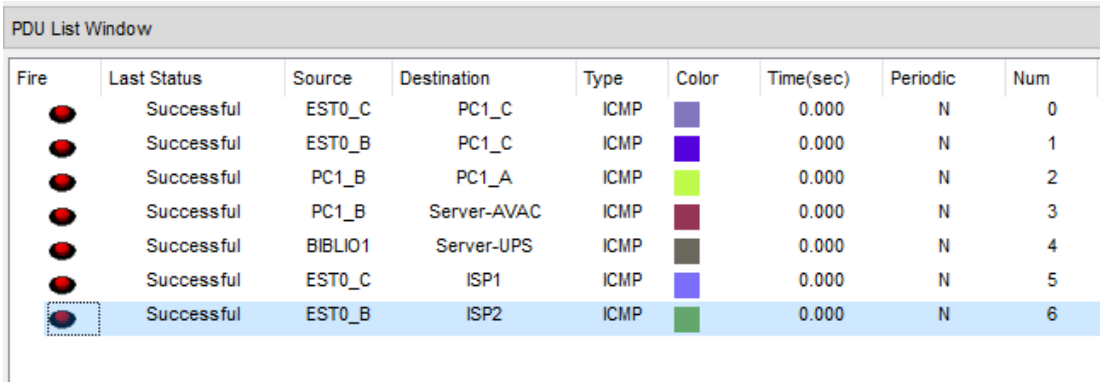


Ilustración 19 PC0_A Bandeja de entrada de correos

Para concluir con la simulación se realizarán algunas pruebas de ping, a pesar de que ya se puede observar la comunicación entre los equipos PC y Servers, pero esta es una confirmación de que las rutas están correctamente configuradas y la red puede comunicarse con todos los equipos.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	EST0_C	PC1_C	ICMP		0.000	N	0
	Successful	EST0_B	PC1_C	ICMP		0.000	N	1
	Successful	PC1_B	PC1_A	ICMP		0.000	N	2
	Successful	PC1_B	Server-AVAC	ICMP		0.000	N	3
	Successful	BIBLIO1	Server-UPS	ICMP		0.000	N	4
	Successful	EST0_C	ISP1	ICMP		0.000	N	5
	Successful	EST0_B	ISP2	ICMP		0.000	N	6

Ilustración 20 Pruebas de conexión Packet Tracer

Finalmente encapsulamos los bloques para tener una mejor organización en la topología simulada y se muestra a continuación la red jerárquica resultante, después de todo el proceso detallado en este título.

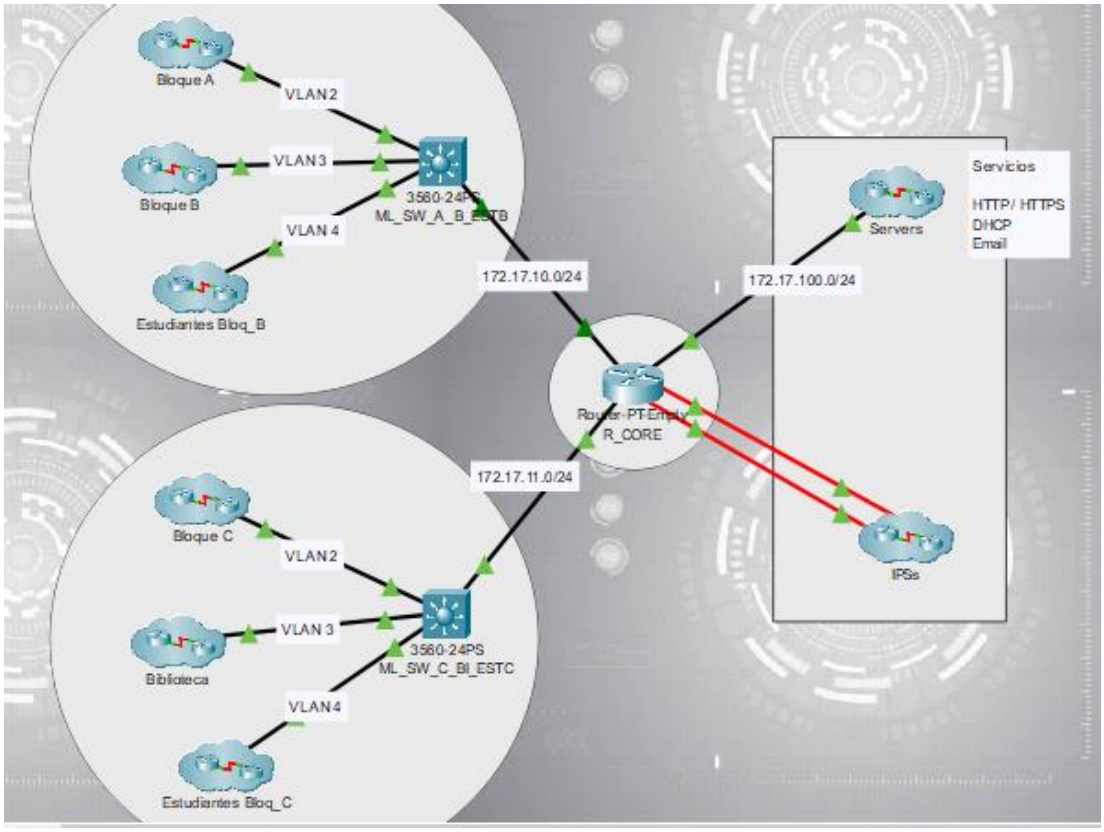


Ilustración 21 Red Jerárquica utilizada

3.4 Arquitectura SDN con controladora en nube disponible en el mercado

En el mercado varios fabricantes están trabajando con la automatización y desarrollo para que las redes SDN pasen a ser una tecnología mandataria, a continuación, se diseñará una red SDN con dispositivos reales y vigentes en el mercado ecuatoriano.

A continuación, se ha desarrollará un TDR (Términos de referencias mínimos) en la marca HPE-Aruba, en base a la experiencia y requerimientos mínimos que se necesita para la implementación de dicha red para un escenario de campus empresarial, en el cual se detallará una breve descripción de los equipos, con las diferentes necesidades y características que se necesita para implementar soluciones reales SDN.

SWITCH CORE		SWITCH AGREGACIÓN	
Descripción	Especificaciones técnicas mínimas: - Switch modular - Al menos 6 bahías de medio ancho para módulos I/O - L2/L3/L4 - Fuentes de poder redundantes - Soporte interfaces 1G /10G / 40G - Soporte interfaces 1000Base-T POE+ - Soporte de interfaces RJ-45 Multi Gigabit 1/2,5/5/10Gb POE+	**Descripción**	Especificaciones técnicas mínimas: - Switch L2/L3 básico - IPv4/IPv6 con enrutamiento estático, RIPv1/v2, OSPF, PIM, PBR - 48 puertos 1000Base-T - Con 4 puertos 10GbE SFP+
	Especificaciones técnicas		**Especificaciones técnicas**
Cantidad	2 /Para un escenario de Alta disponibilidad	Cantidad	8
Características Generales		**Características Generales**	
Tipo	Modular	Tipo	Stand-alone
Capas	Switch de capa 2, 3, 4.	Capas	Switch de capa 2, 3 básico
Soporte de módulos de administración	El equipo debe incluir al menos dos (2) bahías para módulos de administración. Los módulos de administración deben operar al menos en modo activo/pasivo.		
Soporte de módulos de I/O	El equipo debe incluir al menos seis (6) bahías de medio ancho para módulos de Entrada/Salida (I/O).	Stacking	Capacidad de conectarse en stack con otros equipos de la misma serie: - Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. - El stack debe ser capaz de crecer al menos hasta cuatro (4) equipos de la misma serie. - El stack debe poder ser configurado utilizando interfaces uplink de 1G o 10G
Stacking	Capacidad de conectarse en stack con otro equipo igual: - Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. - El stack debe ser capaz de crecer al menos hasta dos (2) equipos iguales.	Rendimiento	Al menos: - Rendimiento: 112 Mpps - Capacidad de conmutación: 176 Gbps.

Ilustración 22 Términos técnicos de referencia para implementar una topología SDN

Rendimiento	Al menos: - Rendimiento: 571,4 Mpps - Capacidad de conmutación: 960 Gbps.	Latencia	En 1 Gbps menor a 3,8 us. En 10 Gbps menor a 1.6 us.
Latencia	En 1 Gbps menor a 2,8 us, en 10Gbps menor a 1,8 us, y en 40Gbps menor a 1,5 us.	Memoria	Al menos: - RAM: 1 GB - Buffer compartido: 12.38 MB.
Memoria	Al menos: - RAM: 4 GB - Flash: 16 MB.		
Sistema Operativo	El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.	Sistema Operativo	El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.
Administración y Monitoreo		**Administración y Monitoreo**	
Acceso y configuración	Al menos vía: - Línea serial de comandos (CLI) - Telnet - HTTP - SSH v2	Acceso y configuración	Al menos vía: - Línea serial de comandos (CLI) - Telnet - HTTP/HTTPS - SSH v2

Ilustración 23 Términos técnicos de referencia para implementar una topología SDN

Requerimientos L2		**Requerimientos L2**	
MAC address table	64000 direcciones MAC	MAC address table	32768 direcciones MAC
VLANs	Al menos: - Soporte de 4094 VLAN ID. - 4094 VLANs simultáneas. - GVRP y MVRP.	VLANs	Al menos: - Soporte de 4094 VLAN ID. - 2000 VLANs simultáneas. - GVRP y MVRP.
Servicios y Funcionalidades para L2	Al menos: - VxLAN	Tramas	Soporte de tramas de hasta 9220 bytes.
Protocolos y Estándares	Al menos: - IEEE 802.1Q. - IEEE 802.1v. - IEEE 802.1w. - IEEE 802.1p. - IEEE 802.1X. - IEEE 802.3u. - IEEE 802.3x. - IEEE 802.3ab. - IEEE 802.3ad.	Protocolos y Estándares	Al menos: - IEEE 802.1Q. - IEEE 802.1v. - IEEE 802.1w. - IEEE 802.1p. - IEEE 802.1X. - IEEE 802.3u. - IEEE 802.3x. - IEEE 802.3ab. - IEEE 802.3ad.
Listas de Acceso	Listas de control de acceso (ACL) en todos los puertos: - ACLs por hardware que operen a la velocidad del cobre. - Parámetros configurables de Capa 2, Capa 3 y Capa 4. - ACL para IPv6. - ACLs basadas en identidad de los usuarios, para facilitar la integración con sistemas de Control de Acceso a la red (NAC)	Listas de Acceso	Listas de control de acceso (ACL) en todos los puertos: - ACLs por hardware que operen a la velocidad del cobre. - Parámetros configurables de Capa 2, Capa 3 y Capa 4. - ACL para IPv6. - ACLs basadas en identidad de los usuarios, para facilitar la integración con sistemas de Control de Acceso a la red (NAC)
Voice VLAN	Manejo de VLAN de voz.	Voice VLAN	Manejo de VLAN de voz.

Ilustración 24 Términos técnicos de referencia para implementar una topología SDN

Requerimientos L3		Requerimientos L3	
Protocolos enrutados	Al menos: - IPv4 - IPv6	Protocolos enrutados	Al menos: - IPv4 - IPv6
Tamaño de las tablas	Al menos: - 256 entradas para rutas estáticas. - 10000 entradas para rutas RIP IPv4 y 5000 entradas para rutas RIPng. - 10000 entradas , 16 áreas y hasta 128 interfaces para OSPFv2.	Tamaño de las tablas	Al menos: - OSPF: 200 rutas (un ID de área) - RIP routes: 10000 rutas - ARP: 25000 entradas (para IPv4 e IPv6)
Protocolos para IPv4	Al menos: - Enrutamiento: estático. - Enrutamiento Inter-Vlan. - RIPv1, RIPv2 y OSPF configurado como acceso - BGP	Protocolos para IPv4	Al menos: - Enrutamiento: estático. - Enrutamiento Inter-Vlan. - RIPv1, RIPv2 y OSPF configurado como acceso - Policy-based Routing - VRRP
Protocolos para IPv6	Al menos: - Enrutamiento: estático. - RIPng - OSPFv3	Protocolos para IPv6	Al menos: - Enrutamiento: estático. - VRRP
DHCP	Soporte para asignar direccionamiento IP dinámico mediante protocolo DHCP	DHCP	Soporte para asignar direccionamiento IP dinámico mediante protocolo DHCP
QoS		**QoS**	
Colas para QoS	Al menos 8 colas por puerto.	Colas para QoS	Al menos 8 colas por puerto.
Control de tormentas	Limitación de ancho de banda	Control de tormentas	Limitación de ancho de banda
Seguridad		**Seguridad**	
Autenticación	Soporte de: - Autenticación por dirección MAC - Radius - TACACS+ - Autenticación basada en WEB.	Autenticación	Soporte de: - Autenticación por dirección MAC - Radius - Autenticación basada en WEB.
Servicios de seguridad	Al menos: - Guest VLAN. - VLAN privada - VLAN isolation para tráfico no IP. - DHCP protection. - Dynamic ARP protection. - Filtrado de puerto origen, para permitir que únicamente puertos específicos se comuniquen con otros.	Servicios de seguridad	Al menos: - Guest VLAN. - VLAN privada - VLAN isolation para tráfico no IP. - DHCP protection. - Dynamic ARP protection. - Filtrado de puerto origen, para permitir que únicamente puertos específicos se comuniquen con otros. - IP multicast snooping.
SDN		**SDN**	
SDN	Soporte al menos OpenFlow v1.3.	SDN	Soporte al menos OpenFlow v1.3.

Ilustración 25 Términos técnicos de referencia para implementar una topología SDN

Después de organizar el TDR para la ejecución del proyecto, usando una herramienta para la simulación y cotizaciones de equipos que requiere la red del campus con todos sus componentes, llamada Intangui Iris y en la cual se realizará la simulación en una solución con Aruba Networks.

En primer lugar, como se puede observar en la siguiente ilustración, se separó la capa de administración de los equipos en sitio, ya que se puede implementar en una controladora en nube privativa de la marca llamada Aruba Central, que es la encargada de administrar monitorear y crear políticas desde una plataforma centralizada, este se encargará de brindar seguridad realizando tareas de mantenimiento y administración de toda la topología con funcionalidades avanzadas, sin la necesidad de tener un equipo extra como un Firewall o controladora física.

Para la adquisición de esta controladora en nube, se realiza mediante la adquisición de un licenciamiento perpetuo para cada dispositivo de red, que necesita ser dado de alta en la controladora, adicional los equipos los cuales serán administrados de manera centralizada deben soportan Open Flow y Vxlan que son protocolos de comunicación para que funcione SDN dentro de esta controladora en Nube.

Ilustración 26 Licenciamiento Aruba Central

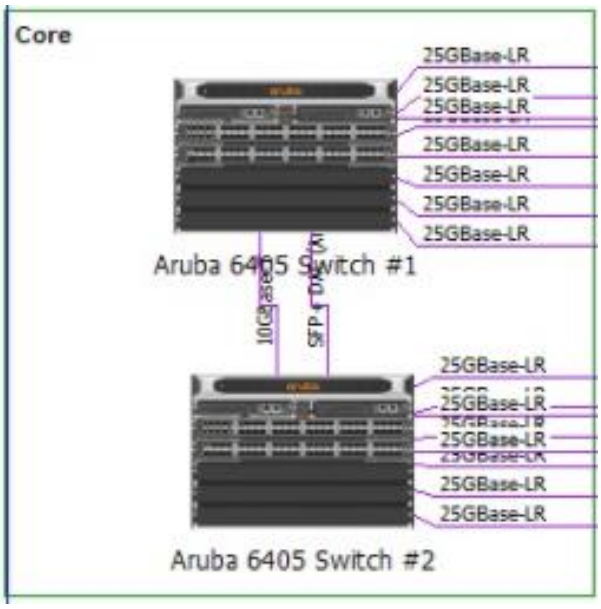


Ilustración 27 Core Switches 6404 OS-CX

Como se puede visualizar en la ilustración anterior, el escenario consta de dos Switches tipo chasis Aruba 6405 en alta disponibilidad, para que si un enlace falla, el otro quede de Back Up, el Backbone entre ambos consta de un enlace por fibra óptica a 10 Gbps por puertos SFP+ en los cuales se coloca transceivers, que permitan hacer stacking entre los enlaces Uplink, esto permitirá que ambos equipos funcionen como un solo elemento lógico y multipliquen su capacidad de conmutación, al igual que su rapidez de envío y ancho de banda.

Para que se pueda comunicar los Switches tipo chasis en alta disponibilidad Core o Spine a la capa de agregación o Leaf, se necesita puertos que funciones en QSFP28 que es la nomenclatura para slots que soportan transceivers a 10/25 Gbps en este caso como se necesita un ancho de banda amplio y para prevenir pérdidas por la gran demanda de dispositivos finales que se conectan en la misma, se usan enlaces por fibra óptica para que el Backbone entre Spine and Leaf sea de 25 Gbps.

En la capa de agregación cada Switch de la topología de igual manera estará conectado en escenarios de alta disponibilidad, de esta manera, si un enlace es amenazado por mucha saturación o pérdidas, para evitar que los equipos estén fuera de servicio, ya que, tendrá un enlace de Back Up.

Ilustración 28 Switches Aruba 6300F para cada bloque - Aruba AP-515

Ilustración 29 Switches Aruba 6300F para cada bloque - Aruba AP-515

Para finalizar se agregaron Access Points, por motivo del uso de dispositivos cableados, al igual que equipos inalámbricos que utilizan la red de la institución, estos equipos inalámbricos no necesitan una controladora, ya que, puede ser administrados desde el servicio en nube que ofrece la marca, Aruba Central, estos equipos son energizados por Power Over Ethernet Class4 con enlaces a 1 Gbps por los puertos del Switch.

Consideraciones importantes dentro del diseño de la topología SDN:

Ilustración 30 Guía de diseño Spine and Leaf (Núcleo- Agregación)

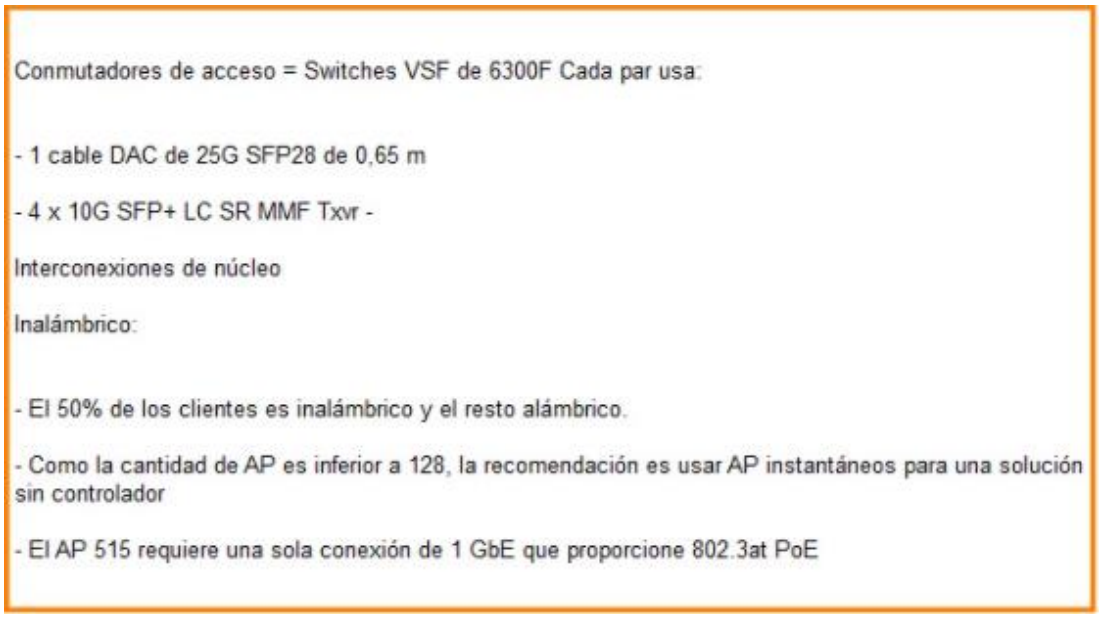


Ilustración 31 Consideraciones Switch Acceso y equipos inalámbricos

Para finalizar se indicará una aproximación de precios de la topología diseñada en este título, la cual satisface las necesidades de la Universidad Politécnica Salesiana del campus sur, siendo está administrada por una controladora en nube. La plataforma de la marca Aruba permite la obtención de estos valores, se tiene en consideración que los precios pueden variar de acuerdo con costos de importación, margen de ganancias de la empresa en donde se haga la adquisición, al igual que impuestos cambios de moneda, todos los equipos que se muestran en el diseño están homologados por el Arcotel, organismo regulatorio en el país, es decir pueden ser usados en cualquier escenario en Ecuador y en la región.

El Boom final contiene equipos, cables, transceivers, fuentes redundantes, Access Points, Switches, Licenciamientos, Controladora todos los componentes de la red están detallados con su número de parte comercial, dentro de cada segmento de la topología como se muestra a continuación.

Part Number	Description	Unit Price	Quantity	Sub Total
BLOQUE A- WC 1				
Q9H63A	Aruba AP-515 (US) Unified AP	$1.301,40	10	$13.014,00
HC4J8E	Aruba 1Y FC NBD Exch AP-515 SVC [for Q9H63A]	$58,30	10	$583,00
JL665A	Aruba 6300F 48G CL4 PoE 4SFP56 Switch	$12.829,32	2	$25.658,64
JL665A ABA	INCLUDED: Power Cord - U.S. localization	incl.	2	
HR5U1E	Aruba 1Y FC NBD Exch 6300F 48 PoE SVC [for JL665A]	$634,51	2	$1.269,02
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for JL665A]	$1.070,00	2	$2.140,00
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	4	$25.266,40
R0M46A	Aruba 50G SFP56 to SFP56 0.65m DAC Cable	$490,00	1	$490,00
BLOQUE B - WC 2				
Q9H63A	Aruba AP-515 (US) Unified AP	$1.301,40	10	$13.014,00
HC4J8E	Aruba 1Y FC NBD Exch AP-515 SVC [for Q9H63A]	$58,30	10	$583,00
JL665A	Aruba 6300F 48G CL4 PoE 4SFP56 Switch	$12.829,32	2	$25.658,64
JL665A ABA	INCLUDED: Power Cord - U.S. localization	incl.	2	
HR5U1E	Aruba 1Y FC NBD Exch 6300F 48 PoE SVC [for JL665A]	$634,51	2	$1.269,02
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for JL665A]	$1.070,00	2	$2.140,00
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	4	$25.266,40
R0M46A	Aruba 50G SFP56 to SFP56 0.65m DAC Cable	$490,00	1	$490,00
BLOQUE C - WC 3				
Q9H63A	Aruba AP-515 (US) Unified AP	$1.301,40	10	$13.014,00
HC4J8E	Aruba 1Y FC NBD Exch AP-515 SVC [for Q9H63A]	$58,30	10	$583,00
JL665A	Aruba 6300F 48G CL4 PoE 4SFP56 Switch	$12.829,32	2	$25.658,64
JL665A ABA	INCLUDED: Power Cord - U.S. localization	incl.	2	
HR5U1E	Aruba 1Y FC NBD Exch 6300F 48 PoE SVC [for JL665A]	$634,51	2	$1.269,02
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for JL665A]	$1.070,00	2	$2.140,00
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	4	$25.266,40
R0M46A	Aruba 50G SFP56 to SFP56 0.65m DAC Cable	$490,00	1	$490,00

Ilustración 32 Boom SDN arquitectura ARUBA

BLOQUE G - WC 4				
Q9H63A	Aruba AP-515 (US) Unified AP	$1.301,40	10	$13.014,00
HC4J8E	Aruba 1Y FC NBD Exch AP-515 SVC [for Q9H63A]	$58,30	10	$583,00
JL665A	Aruba 6300F 48G CL4 PoE 4SFP56 Switch	$12.829,32	2	$25.658,64
JL665A ABA	INCLUDED: Power Cord - U.S. localization	incl.	2	
HR5U1E	Aruba 1Y FC NBD Exch 6300F 48 PoE SVC [for JL665A]	$634,51	2	$1.269,02
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for JL665A]	$1.070,00	2	$2.140,00
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	4	$25.266,40
R0M46A	Aruba 50G SFP56 to SFP56 0.65m DAC Cable	$490,00	1	$490,00
CONTROLADORA EN NUBE ARUBA CENTRAL				
JL639AAE	Aruba NetEdit Single Node 1yr Sub E-STU	$63,72	10	$637,20
JY925AAE	Aruba Central Device Management 1 Token 1 Year Subscription E-STU [discontinued]	$0,00	50	$0,00
JZ402AAE	Aruba ClearPass NL AC 1K CE E-LTU	$21.000,00	2	$42.000,00
H9XH2E	Aruba 1Y FC SW CP NL AC 1K CE E-L SVC [for JZ402AAE]	$1.848,00	2	$3.696,00
JZ438AAE	Aruba ClearPass NL OB 1K USR E-LTU	$29.750,00	2	$59.500,00
H9XK2E	Aruba 1Y FC SW CP NL OB 1K USR E-L SVC [for JZ438AAE]	$2.616,90	2	$5.233,80
JZ474AAE	Aruba ClearPass NL OG 1K EP E-LTU	$18.000,00	2	$36.000,00
H9XF2E	Aruba 1Y FC SW CP NL OG 1K EP E-L SVC [for JZ474AAE]	$1.588,40	2	$3.176,80
CORE				
R0X26A	Aruba 6405 Switch	$15.453,66	1	$15.453,66
HL8M1E	Aruba 1Y FC NBD Exch 6405 SVC [for R0X26A]	$2.142,14	1	$2.142,14
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for R0X26A]	$1.070,00	1	$1.070,00
R0X35A	Aruba 6400 1800W Power Supply with C16 Inlet Adapter	$2.860,86	4	$11.443,44
R0X35A B2E	INCLUDED: NEMA 6-20 220V NA Power Cord	incl.	4	
R0X31A	Aruba 6400 Management Module	$10.302,06	1	$10.302,06
R0X44A	Aruba 6400 48p 10G/25G SFP28 Module	$57.238,86	1	$57.238,86
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	8	$50.532,80
R0X44A	Aruba 6400 48p 10G/25G SFP28 Module	$57.238,86	1	$57.238,86
JL563A	Aruba 10GBASE-T SFP+ RJ45 30m Cat6A Transceiver	$2.104,60	1	$2.104,60
R0X26A	Aruba 6405 Switch	$15.453,66	1	$15.453,66
HL8M1E	Aruba 1Y FC NBD Exch 6405 SVC [for R0X26A]	$2.142,14	1	$2.142,14
H8XE6E	HPE Aruba 6xxxN8xxx Install Swt SVC [for R0X26A]	$1.070,00	1	$1.070,00
R0X36A	Aruba 6400 3000W Power Supply with C20 Inlet Adapter	$4.578,06	4	$18.312,24
R0X36A B2E	INCLUDED: NEMA 6-20 220V NA Power Cord	incl.	4	
R0X31A	Aruba 6400 Management Module	$10.302,06	1	$10.302,06
R0X44A	Aruba 6400 48p 10G/25G SFP28 Module	$57.238,86	1	$57.238,86
JL486A	Aruba 25G SFP28 LC LR 10km SMF Transceiver	$6.316,60	8	$50.532,80
R0X44A	Aruba 6400 48p 10G/25G SFP28 Module	$57.238,86	1	$57.238,86
JL563A	Aruba 10GBASE-T SFP+ RJ45 30m Cat6A Transceiver	$2.104,60	1	$2.104,60
	Quote Total			$845.849,68

Ilustración 33 Boom SDN arquitectura ARUBA

3.5 Diseño de la red SDN para la Universidad

En el presente título se realizará el diseño de la red definida por software, esta debe cumplir con una estructura similar a la red jerárquica, además de tener la capacidad de generar una administración completa y centralizada, con una estructura de redes SDN y que le permita cubrir la demanda de la transmisión de datos entre todos los equipos de la red.

3.5.1 Planificación de direccionamiento IP de la red

Previo a una implementación SDN, se recomienda realizar una topología virtual, en la cual, se pueda visualizar una arquitectura de tipo Spine-Leaft que se encarga de tener equipos en capa 3 que son los encargados de la distribución de la red y Leaf que son equipos encargados de la capa de acceso para los dispositivos finales. A continuación, se mostrará el direccionamiento IP que usamos para dicha topología:

Tabla 9 Direccionamiento Vlan

DIRECCIONAMIENTO IP VLAN				
SW ACCESO BLOQUE A				
EQUIPO	VLAN	DIRECCIÓN IP	RED	MASCARA
PC9	10	DHCP	192.16.10.0	255.255.255.0
PC10	20	DHCP	192.16.10.0	255.255.255.0
SW ACCESO BLOQUE B				
PC11	20	DHCP	192.168.20.0	255.255.255.0
PC12	30	DCHP	192.168.30.0	255.255.255.0
		SW ACCESO BLOQUE C		
PC17	10	DHCP	192.168.10.0	255.255.255.0
PC18	30	DHCP	192.168.30.0	255.255.255.0
SW ACCESO BLOQUE D				
PC13	100	DHCP	192.168.100.0	255.255.255.0
PC14	110	DHCP	192.168.110.0	255.255.255.0

	SW ACCESO BLOQUE E			
PC15	110	DHCP	192.168.110.0	255.255.255.0
PC16	120	DHCP	192.168.120.0	255.255.255.0
SW ACCESO BLOQUE G				
PC13	110	DHCP	192.168.110.0	255.255.255.0
PC14	120	DHCP	192.168.120.0	255.255.255.0

Para el enrutamiento de las direcciones IP de los equipos, se adjunta en la siguiente tabla el enrutamiento implementado en la topología.

Tabla 10 Direccionamiento IP

Router central			
INTERFAZ	RED	IP	MASCARA
GIG 0/0/0	192.168.70.0	192.168.70.2	255.255.255.0
GIG 0/0/1	192.168.80.0	192.168.80.2	255.255.255.0
SwitchDistribucion1			
INTERFAZ	RED	IP	MASCARA
GIG 1/0/1	192.168.70.0	192.168.70.1	255.255.255.0
GIG 0/0/1	192.168.80.0	192.168.60.1	255.255.255.0
GIG 1/0/7	192.168.140.0	192.168.140.1	255.255.255.0
GIG 1/0/5	192.168.60.0	192.168.60.1	255.255.255.0
GIG 1/0/6	192.168.40.0	192.168.40.1	255.255.255.0
SwitchDistribucion2			
INTERFAZ	RED	IP	MASCARA
GIG 1/0/5	192.168.60.0	192.168.60.2	255.255.255.0
GIG 1/0/1	192.168.80.0	192.168.80.1	255.255.255.0
GIG 1/0/6	192.168.160.0	192.168.160.1	255.255.255.0
Controladora			
INTERFAZ	RED	IP	MASCARA
GIG 0	192.168.140.0	192.168.140.2	255.255.255.0
Server DCHP BLOQUES A-B-C			
INTERFAZ	RED	IP	MASCARA
Fa 0	192.168.40.0	192.168.40.50	255.255.255.0
ServerDCHP BLOQUES D-E-G			
INTERFAZ	RED	IP	MASCARA
Fa 0	192.168.160.0	192.168.160.50	255.255.255.0

3.6 Software de simulación para redes SDN

3.6.1 Prueba de simulación con Mininet

El proceso de instalación de Mininet que se realizó para este proyecto técnico fue el siguiente:

- Elegir una aplicación para poder levantar una máquina virtual en el ordenador, en este caso se utilizó VirtualBox por la experiencia previa en el sistema de estudio de la carrera, esta aplicación permite la creación de máquinas virtuales con diferentes sistemas operativos y con la asignación de recursos del ordenador.
- Se crea una máquina virtual con el sistema operativo Linux con una distribución llamada Ubuntu 20, se le asignan los recursos a la máquina virtual, memoria RAM 4096 Mb y disco duro 50Gb para almacenamiento.
- Cuando se inicie la máquina virtual, se utilizará una ventana del terminal para instalar la aplicación Mininet, también se instalará la aplicación Python 3 y Git en sus últimas versiones.

Esta opción fue descartada como simulador ya que el controlador OpenDayLight diseñado para administrar redes SDN, no logro tener un enlace con Mininet por lo cual se tiene que encontrar la solución a este problema, ya sea caso de librerías por actualizaciones en el sistema operativo o la versión de Mininet, se considera esto un tema de estudio para ser desarrollado en el futuro.

3.6.2 Elección de simulador para la red definida por software

Por los puntos antes mencionados y ya que el simulador de Cisco Packet Tracer, en sus últimas versiones ya ha integrado el uso de controladoras para la implementación

en las simulaciones de redes SDN, resulta una mejor opción, por esta razón se realizó la instalación en este simulador.

Considerando que la topología de la red diseñada en la marca HPE-Aruba, maneja un concepto similar al que se realizará en el simulador Cisco Packet Tracer de la red SDN, se simplificará la explicación de la configuración y del diseño de la topología presentada en los siguientes subtítulos.

3.7 Simulación de la red definida por software

En este título se desarrollará la simulación de la red SDN en el software Packet Tracer, enfrentando un entorno similar al de la red actual de la Universidad Politécnica Salesiana del campus sur de la ciudad de Quito, además de integrar los equipos que una red SDN requiere para su correcto funcionamiento, resaltando el rol que cumple el controlador en la infraestructura de la red administrada por software presentada, todo el proceso se detallará a continuación.

3.7.1 Configuración en los equipos de la simulación

Se configurarán todos los equipos como se explica en las tablas de direccionamiento IP detalladas anteriormente, asignando direccionamiento IP a los dispositivos correspondientes y configuraciones necesarias para que la topología pueda converger, con ayuda de comandos de verificación, se podrá visualizar las configuraciones que se han implementado dentro de cada dispositivo

```
SwitchDsitribucin1>enable
SwitchDsitribucin1#sh running-config
```

Ilustración 34 Comando ejecutado para visualización

En este caso se muestra las configuraciones realizadas en un Switch de Acceso, Switch Multilayer capa 3 y el Router Central en los cuales se ejecutan comandos para dar de alta las direcciones IP, además crear un enrutamiento dinámico, Vlan y también comandos para que la topología cree los caminos y rutas necesarias para que los paquetes viajen, a continuación se mostrarán las configuraciones realizadas en los equipos antes mencionados.

```
interface GigabitEthernet1/0/1
no switchport
ip address 192.168.70.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,20,30
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,20,30
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 10,20,30
switchport mode trunk
!
```

Ilustración 35 Configuración Switches Multicapa

```
interface GigabitEthernet1/0/5
no switchport
ip address 192.168.60.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/6
switchport access vlan 40
interface GigabitEthernet1/0/7
no switchport
ip address 192.168.140.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan10
mac-address 0090.0cc3.7901
ip address 192.168.10.1 255.255.255.0
ip helper-address 192.168.40.50
!
```

Ilustración 36 Configuración Switches Multicapa

```
interface Vlan20
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.40.50
!
interface Vlan30
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.40.50
!
interface Vlan40
ip address 192.168.40.1 255.255.255.0
!
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.70.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
!
```

Ilustración 37 Configuración Switches Multicapa

```
!
interface GigabitEthernet0/0/0
ip address 192.168.70.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
ip address 192.168.80.2 255.255.255.0
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 192.168.70.0 0.0.0.255 area 0
network 192.168.80.0 0.0.0.255 area 0
!
```

Ilustración 38 Configuración Router Central

```
!
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/3
switchport access vlan 30
switchport mode access
switchport nonegotiate
!
```

Ilustración 39 Configuración Switches de acceso

2.7.2 Integración y configuración del controlador

Después de ejecutar los comandos en todos los dispositivos de la topología y ver que la red converge, se añadirá un controlador SDN que posee Cisco Packet Tracer en sus

dispositivos para la simulación, en la siguiente ilustración se puede observar el dispositivo físico.

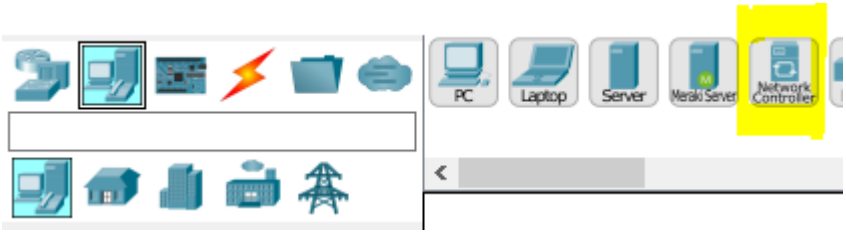


Ilustración 40 Controlador SDN

Para activar el Network Controller, dentro del simulador Cisco Packet Tracer se debe ingresar en la barra de herramientas en Options>Preferences>Miscellaneous y activar Enable External Access for Network Controller REST API esto habilita para que el simulador pueda comunicarse con un API externa como un cliente REST y pueda ser utilizada interna y externamente para diferentes aplicaciones.

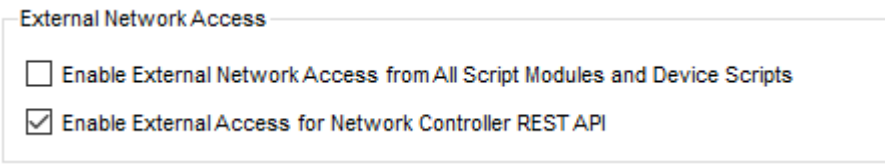


Ilustración 41 Opción para habilitar la opción para visualizar la controladora con REST API externa

Añadir el controlador SDN a la topología previamente realizada, dar de alta la dirección IP de la red 192.168.140.2/24 que corresponde a la segunda IP utilizable para dicha red y colocar el default Gateway 192.168.140.1/24 más cercano para que el dispositivo de red pueda ubicarse en la topología y pertenezca visible, para que posterior pueda ser gestionado.

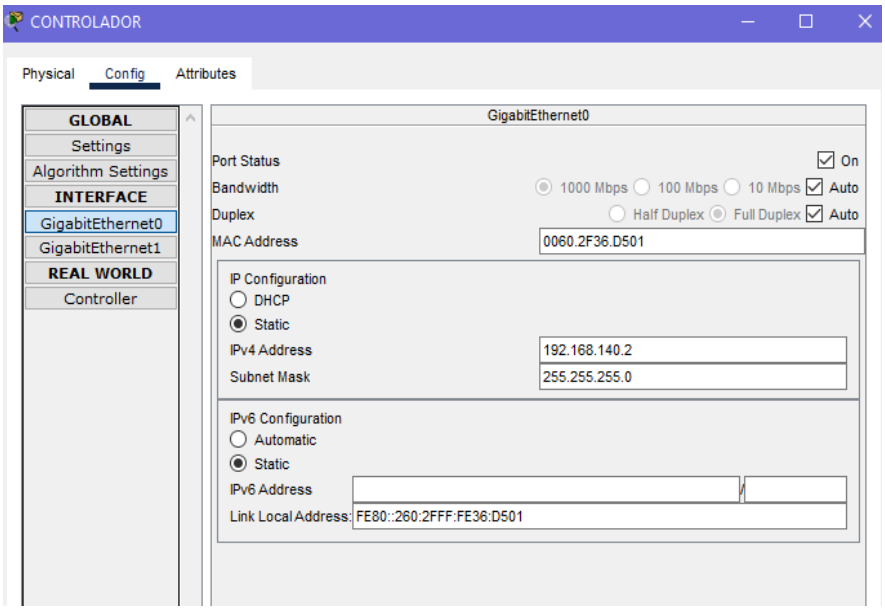


Ilustración 42 Direccionamiento IP Controller

La interfaz que se coloca en el controlador es la Gig0 la misma que debe ser conectado por cable de cobre a la interface Giga 1/0/7 del SwitchDistribucion1, a continuación, se observa una imagen ilustrativa de la misma.

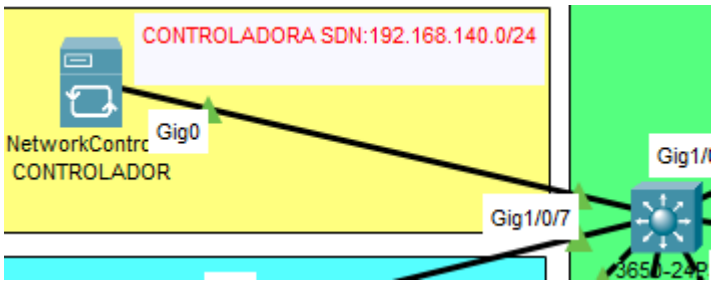


Ilustración 43 Controlador SDN en producción

Cuando el controlador SDN ya está en producción y con el direccionamiento IP se puede utilizar sus funcionalidades, en primer lugar, se accede a una computadora se ingresa en la opción de Web Browser para tipear la IP de la controladora, ya que, esta

se conecta de manera remota, si la interfaz se muestra en un Dashboard visual dentro del Web Browser del Pc quiere decir que toda la red converge y que las interfaces de red fueron colocadas correctamente.

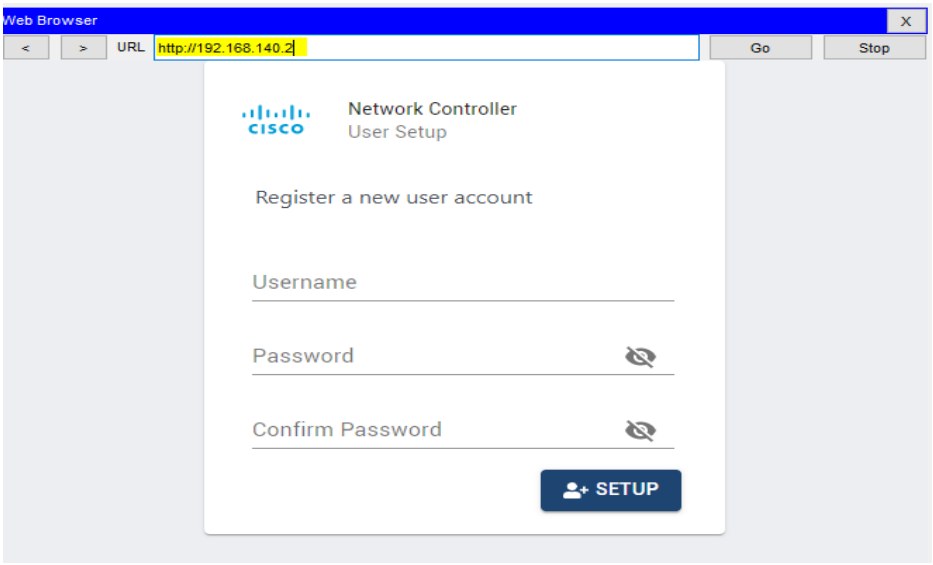


Ilustración 44 Dashboard inició de sesión

Una vez iniciada la sesión, se muestra la interfaz gráfica de la controladora cuando se ingresa por primera vez el dispositivo pide crear una cuenta para la autenticación y registro, para la simulación de este proyecto se ha colocado un username: sdn y Password: 1234, la recomendación técnica es siempre crear las credenciales de hasta 8 caracteres.

Después de autenticarse e ingresar a la controladora en su dashboard se despliega toda la información en la cual se puede acceder a toda la topología ya que esta controladora identifica todos los dispositivos intermedios y Hosts de la red por medio de protocolo Open Flow para poder administrar y gestionar de manera centralizada.

3.7.2 Funciones de la controladora para la administración de la red

A continuación, para verificar el funcionamiento de la controladora se genera un ticket como credencial que sirve para que el equipo pueda identificar y descubrir los equipos de la red y generar una nueva herramienta de cliente basada en flujos para poder implementar configuraciones dentro del equipo como se muestra a continuación.

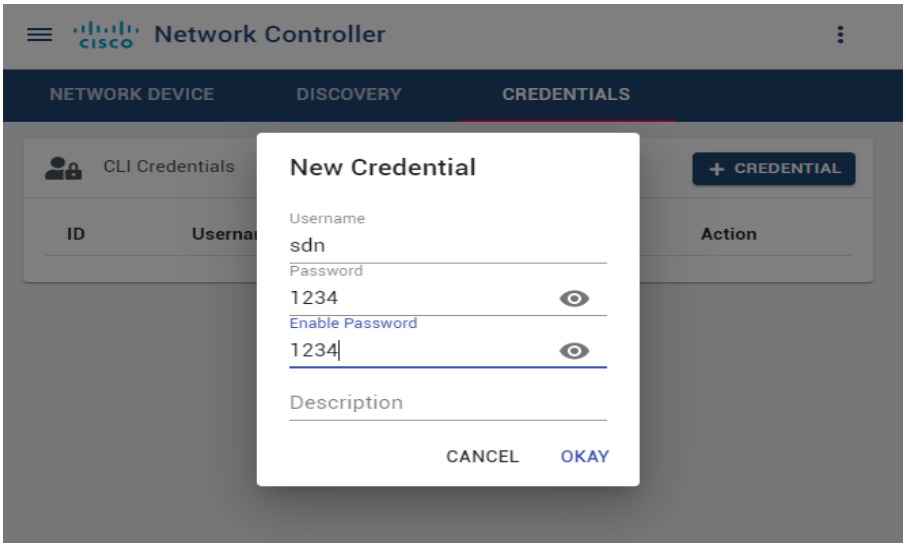


Ilustración 45 Credentíal SDN Controladora

Después de generar la credencial en el equipo, el controlador puede descubrir los elementos de la red utilizando la herramienta Discover con esta herramienta se puede analizar y visualizar las interfaces de red y Mac address de los equipos incluido los Host name, entre otros, esta herramienta envía un mensaje en Broadcast para que pueda entender y analizar los caminos de la red, al igual, que identifica toda la topología sin necesidad de ingresar manualmente los equipos al controlador.

Para configurar esta funcionalidad se debe colocar un nombre, también la IP del primer host o Default Gateway que esté más cercano del controlador y también escoger la credencial que previamente fue creada como nos indica la siguiente imagen.

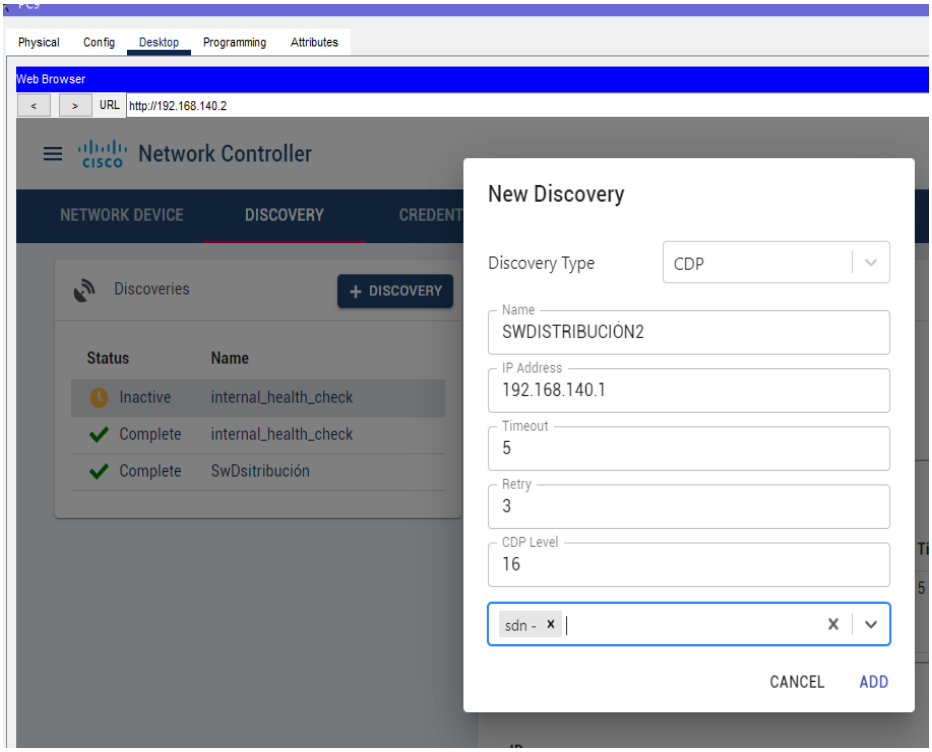


Ilustración 46 Panel de descubrimiento de dispositivos

Cuando se añade el descubrimiento a la controladora, automáticamente comienza la búsqueda y entra en un estado de inactividad hasta que se complete el proceso, esto lleva un tiempo, ya que, tiene que analizar todos los saltos y añadir toda la información a la memoria del dispositivo como nos indica la siguiente ilustración, una vez que ya se completa la información el status de la búsqueda nos indica que todo se ha realizado con éxito y se puede ingresar para visualizar toda la información.

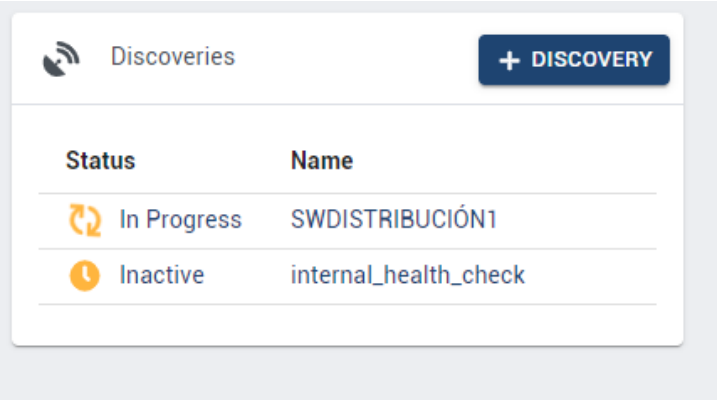


Ilustración 47 Búsqueda de dispositivos

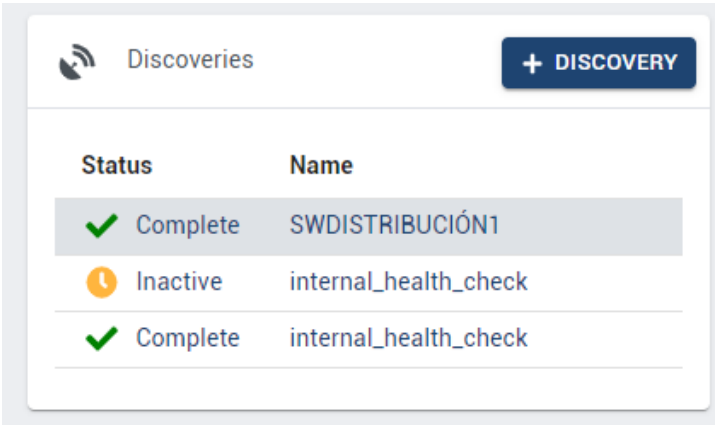


Ilustración 48 Status completo

Cuando el proceso de búsqueda y descubrimiento se completa la controladora ya tiene noción y conocimiento de todos los dispositivos que están dentro de la red, ya que se han añadido correctamente la información y además puede reconocer estados, ver la salud de la red y como es su comportamiento por medio de la API del controlador como se muestra en la siguiente imagen.

Discovered Devices

	Hostname	Type	IP	Reachability Status
			0.0.0.0	Unreachable
	SwitchDsitribucin1	MultiLayerSwitch	192.168.10.1	Unreachable
	PC17	Pc	192.168.10.10	Reachable
	PC9	Pc	192.168.10.12	Reachable
	SwitchDsitribucin2	MultiLayerSwitch	192.168.100.1	Unreachable
			192.168.100.11	Unreachable
	SwitchDsitribucin2	MultiLayerSwitch	192.168.110.1	Unreachable
			192.168.110.11	Unreachable
			192.168.110.12	Unreachable
			192.168.110.13	Unreachable
	SwitchDsitribucin2	MultiLayerSwitch	192.168.120.1	Unreachable
			192.168.120.11	Unreachable
			192.168.120.12	Unreachable
	SwitchDsitribucin1	MultiLayerSwitch	192.168.140.1	Unreachable
	SwitchDsitribucin2	MultiLayerSwitch	192.168.160.1	Unreachable
			192.168.160.50	Unreachable

Ilustración 49 Dispositivos Descubiertos

Después de implantar la controladora dentro de la topología ya se puede dar uso de esta, además nos indica una información extensa y hace que la administración total de la topología sea bastante intuitiva. A continuación, se hará el respectivo análisis y resultados de las funcionalidades del controlador aplicando métricas como Ping, caminos, políticas y también se, mostrará la inteligencia artificial con la que cuenta el dispositivo ante la tolerancia a fallos ya que se dará de baja un enlace y el propio dispositivo nos indicará una alerta cuando este deje de funcionar.

Está topología hace que una arquitectura SDN cumpla con las métricas y toda la carga no se acumule en un solo dispositivito esto evitara que no exista un solo camino y el escenario siempre tenga una disponibilidad alta, en la siguiente imagen se muestra el escenario en el cual la arquitectura SDN se implementó en Cisco Packet Tracer para el funcionamiento y procedimiento del mismo.

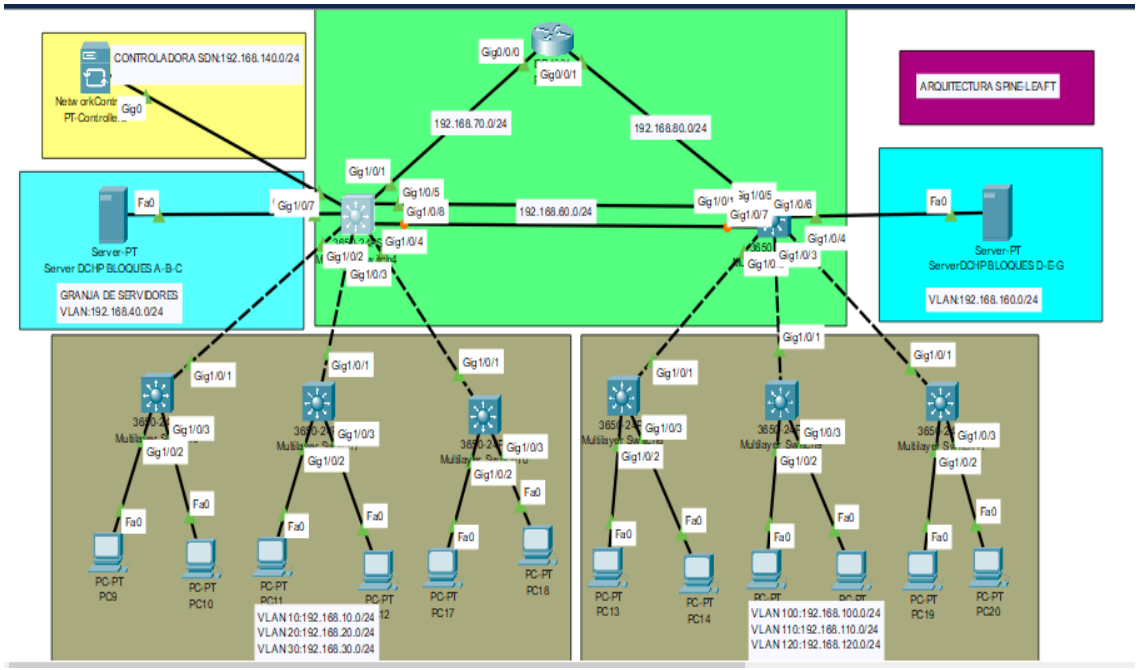


Ilustración 50 Red SDN -Spine-Leaf

3.8 Prueba de envío de paquetes

En esta sección se mostrará un gráfico comparativo del comportamiento de las redes, después de realizar unas pruebas de envío de paquetes, en la cual se midió el tiempo que se necesita para enviar un mensaje y obtener una respuesta del receptor hacia el emisor en la simulación, se comenzó con objetivos relativamente cercanos y continuando con dispositivos más lejanos en la topología.

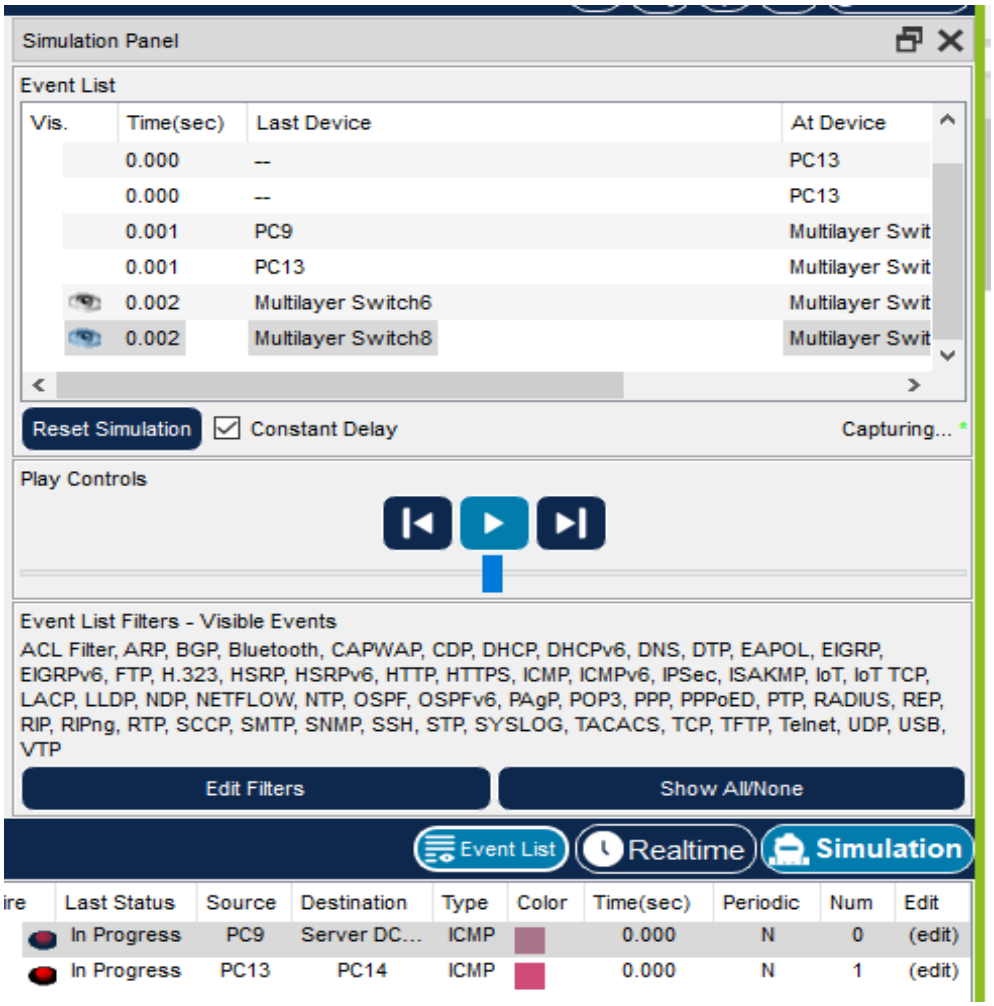


Ilustración 51Simulación de envío de paquetes

CAPÍTULO 4

ANÁLISIS DE RESULTADOS

En el presente capitulo se realizará un análisis de los resultados obtenidos en el capítulo anterior, realizando una comparación entre las dos redes, resaltando los detalles más importantes que demanda una red en la actualidad.

El funcionamiento de una red jerárquica empresarial está dado por el plano de control y el plano de datos todo en un dispositivo de red, esto hace que la red como tal no sea inteligente y su administración sea en sitio y no de una manera remota o centralizada, esto ocasiona defectos y costes altos de productividad para cualquier empresa.

En la simulación realizada se pudo constatar que la red SDN es necesaria para alivianar la carga de la infraestructura ya que separa el control de la data que circula en la red , únicamente un dispositivo será el encargado de gestionar y administrar los equipos de toda la topología, esto habilita la opción de optimización de tiempo y costos para el personal de TI.

Para el análisis de la red SDN se realizó un descubrimiento de toda la red y se observa que no todos los dispositivos de la red pueden ser ubicados ya que son 14 hosts y solo encontró a 7 los cuales son del bloque A, B, C y los del bloque D, E, G no pueden ser encontrados, esta alerta nos emite el controlador directamente sin necesidad de ir a los dispositivos y mirar su configuración que nos indicará que es lo que sucede con el dispositivo como se muestra a continuación.

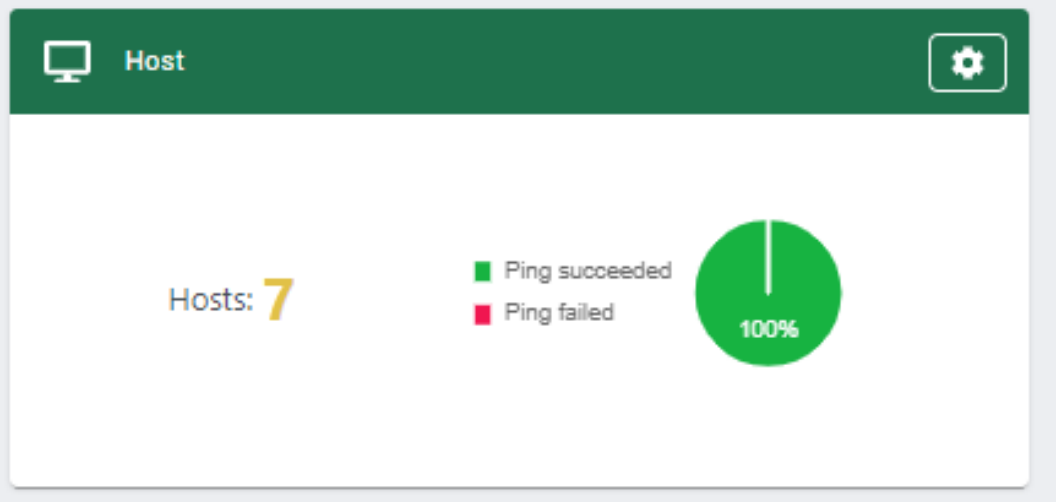


Ilustración 52Hosts encontrados en la topología

A continuación, como se explicó previamente se puede observar que los dispositivos encontrados se enlistan dentro del controlador dando así un detalle a profundidad de sus entradas MAC, IP, Hostame y Tipo es aquí donde nos damos cuenta que los dispositivos del bloque A, B, C si fueron reconocidos por el controlador, esto quiere decir que el protocolo Open Flow está operativo.

Host

	Host Device			
	MAC	**IP**	**Hostname**	**Type**
	000A.F3E8.AE64	192.168.40.50	Server DCHP BLOQUES A-B-C	Server
	0000.0CD3.3934	192.168.10.10	PC17	Pc
	0002.4AB4.E651	192.168.30.12	PC18	Pc
	0040.0B73.E4B6	192.168.20.11	PC11	Pc
	0090.2B6E.379B	192.168.30.11	PC12	Pc
	0004.9A9E.224C	192.168.10.12	PC9	Pc

Ilustración 53 Dispositivos Encontrados

Se pueden analizar las características de igual manera entrando en el detalle de cada dispositivo en el controlador , este indica la información de un Host con nombre PC9 que está conectada a una VLAN 10 y sale por la interface Gigabit Ethernet1/0/2 de igual manera indica a que dispositivo de red está conectado, en este caso indica que está conectado a un SwAccesoBloque1, adicional este muestra que es Host de tipo Pc y sobre todo algo muy importante es que el Ping Status es exitoso esto quiere decir que la controladora pudo enviar paquetes e interactuar con el equipo sin que ocurriese pérdidas, a continuación se puede visualizar el detalle del Host en una imagen ilustrativa.

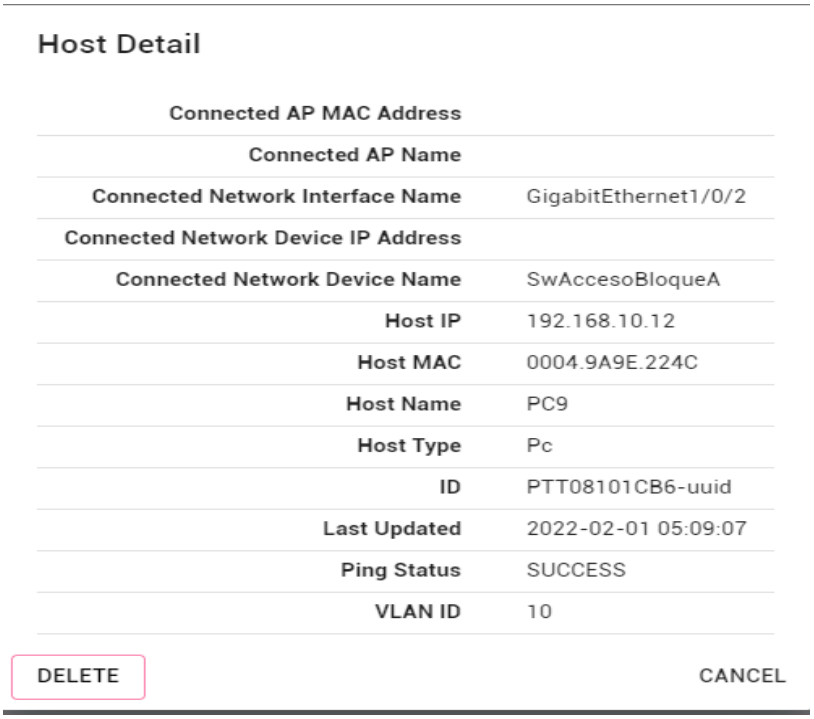


Ilustración 54 Host Detail

Después de visualizar que la controladora no encuentra a los equipos del bloque D,E,G es decir el ping a estos equipos es rechazado nos deja claro que la topología no está convergiendo y es necesario tomar acciones sobre ello, entonces en el estatus la

controladora nos indica que no está creado una ruta entre switches multicapa ya que se está realizando intervlan y esta funcionalidad no está activada, debe ser creada en los equipos de distribución capa 3, por ahora la controladora en el simulador Cisco Packet Tracer no permite crear enrutamiento dinámico entre interfaces que otras controladoras en la práctica real si permiten, es por ello que se procede a crear la ruta de la red de la controladora hasta la red del bloque D,E,G usando el protocolo OSPF de la siguiente manera para luego analizar que sucede con la topología:

```
SwitchDsitribucinl(config)#router ospf 1
SwitchDsitribucinl(config-router)#net
SwitchDsitribucinl(config-router)#network 192.168.140.0 0.0.0.255 area
SwitchDsitribucinl(config-router)#network 192.168.140.0 0.0.0.255 area 0
SwitchDsitribucinl(config-router)#exit
```

Ilustración 55 Configuración enrutamiento dinámico

Después de verificar que el enrutamiento dinámico para los Switches de distribución de la red de la controladora a la red del bloque D, E, G que fue exitoso, se comprueba que automáticamente en la controladora se añaden los equipos faltantes que no se encontraban dentro de la topología, esto quiere decir que la ruta fue exitosa. También como ya se creó la opción de descubrimiento dentro de la controladora automáticamente los dispositivos se cargan dentro del Dashboard, esta herramienta de descubrimiento dentro de la controladora es bastante eficaz porque ayudará a conocer que dispositivos se encuentran dentro de nuestra topología que constantemente envía pruebas de conexión, la información que nos entrega la controladora es la siguiente.

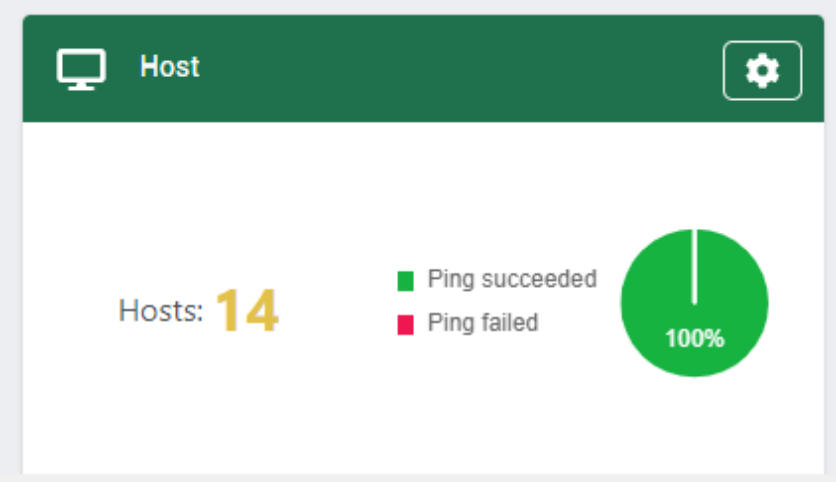


Ilustración 56 Hosts totales en la topología

Host

	Host Device				Connected Network Device		
	MAC	IP	Hostname	Type	IP	Hostname	Port
	000A.F3E8.AE64	192.168.40.50	Server DCHP BLOQUES A-B-C	Server	192.168.70.1	SwitchDsitribucin1	GigabitEthernet1/0/6
	0000.0CD3.3934	192.168.10.10	PC17	Pc		SwAccesoBloqueC	GigabitEthernet1/0/2
	0002.4AB4.E651	192.168.30.12	PC18	Pc		SwAccesoBloqueC	GigabitEthernet1/0/3
	0040.0B73.E4B6	192.168.20.11	PC11	Pc		SwAccesoBloqueB	GigabitEthernet1/0/2
	0090.2B6E.379B	192.168.30.11	PC12	Pc		SwAccesoBloqueB	GigabitEthernet1/0/3
	0004.9A9E.224C	192.168.10.12	PC9	Pc		SwAccesoBloqueA	GigabitEthernet1/0/2
	000C.8579.6488	192.168.160.50	ServerDCHP BLOQUES D-E-G	Server	192.168.80.1	SwitchDsitribucin2	GigabitEthernet1/0/6
	0060.3E3D.E893	192.168.110.13	PC19	Pc		SwAccesoBloqueG	GigabitEthernet1/0/2
	00D0.97D6.1E35	192.168.120.12	PC20	Pc		SwAccesoBloqueG	GigabitEthernet1/0/3
	0001.63AB.7830	192.168.110.11	PC15	Pc		SwAccesoBloqueE	GigabitEthernet1/0/2
	0009.7C6D.2DE0	192.168.120.11	PC16	Pc		SwAccesoBloqueE	GigabitEthernet1/0/3
	0060.7096.4B73	192.168.100.11	PC13	Pc		SwAccesoBloqueD	GigabitEthernet1/0/2
	0010.1152.B64D	192.168.110.12	PC14	Pc		SwAccesoBloqueD	GigabitEthernet1/0/3
	00D0.9785.6D5C	192.168.30.10	PC10	Pc		SwAccesoBloqueA	GigabitEthernet1/0/3

Ilustración 57 Rutas directas que descubre la controladora SDN

Para hacer una prueba de conexión local y no en la controladora también se la puede realizar en los dispositivos finales como son los computadores desde su consola CMD en este caso se hará una prueba de conexión desde un dispositivo final (Host) hasta la controladora para verificar que los bytes que se envían son recibidos:

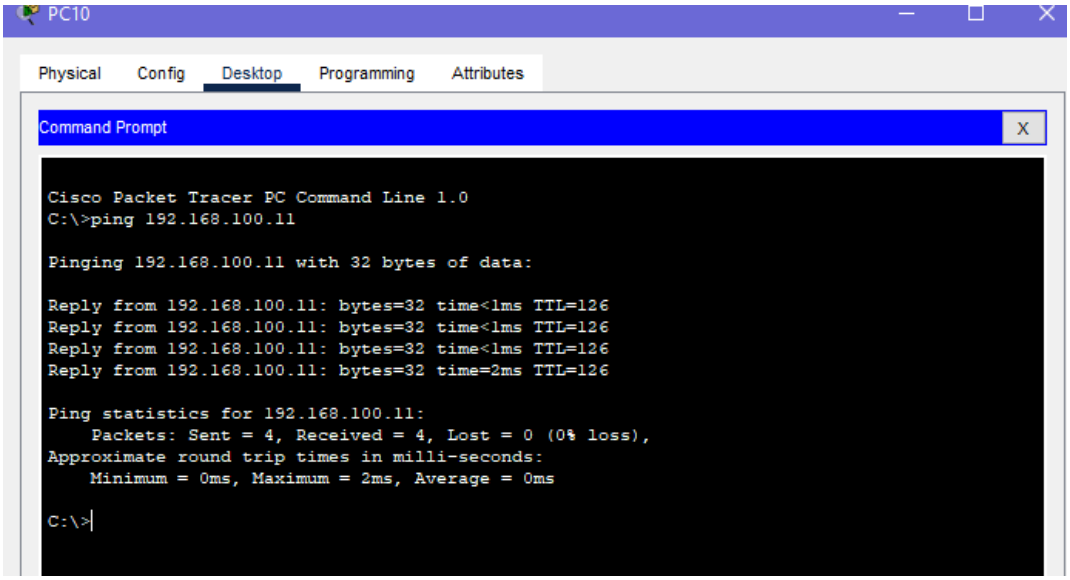


Ilustración 58 Prueba Ping PC- Controller SDN

Como se puede visualizar en la ilustración previa los paquetes enviados desde el PC10 hasta el controller SDN se reciben con éxito es decir que no existe pérdidas en los caminos, el tiempo de vida de los paquetes ha disminuido en 1 salto debido a que se encuentra a 2 conmutadores de distancia.

Adicional la controladora tiene una funcionalidad para visualizar el camino por donde se envía los paquetes como se indica en la siguiente ilustración, esto quiere decir que maneja un algoritmo interno por medio de programación, indica la información necesaria de manera gráfica para saber cómo viajan los paquetes creando una ruta eficaz con tolerancia a fallos y también indicando porque interfaz entra y sale la data desde la fuente hasta el destino.

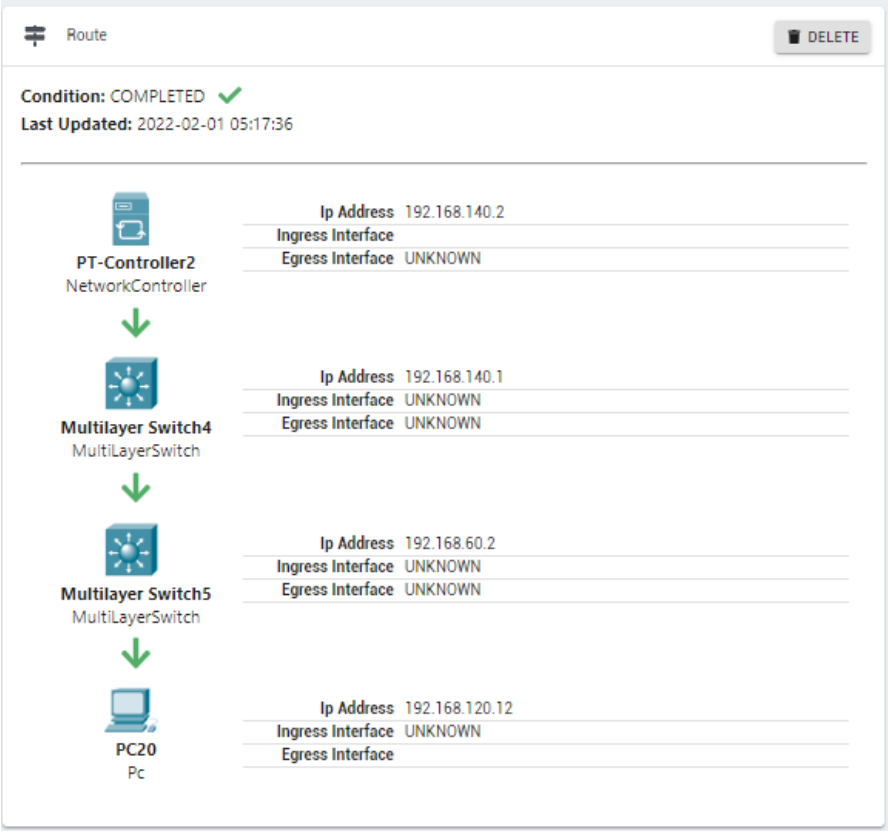
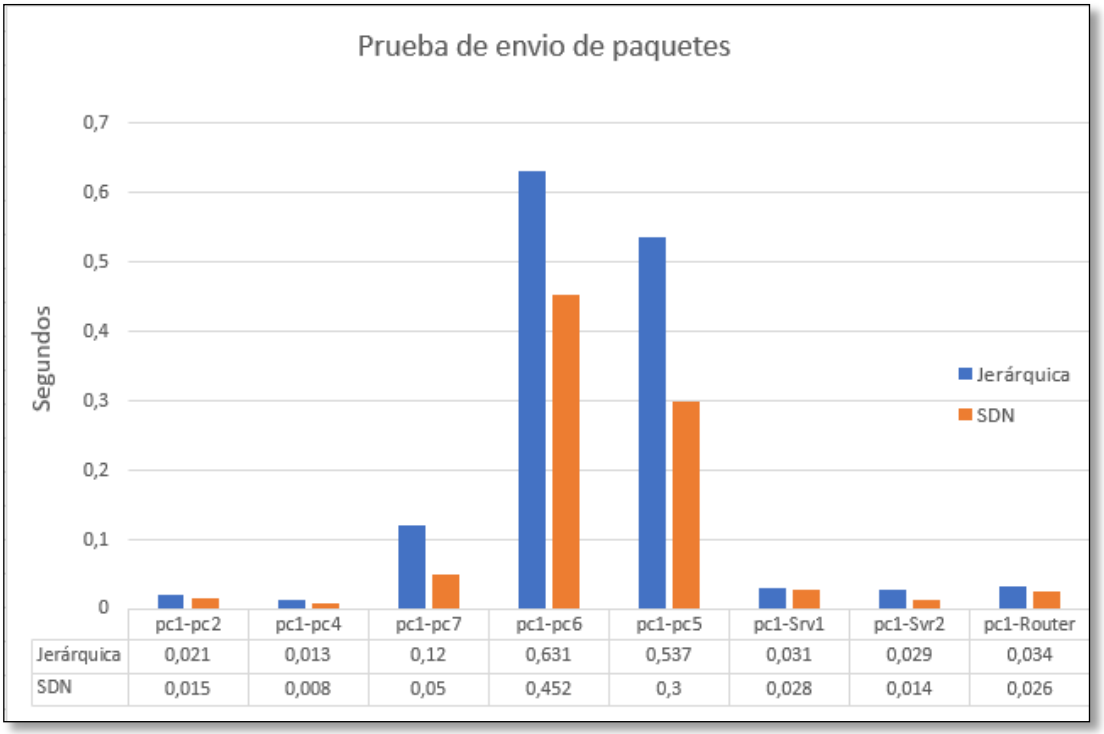


Ilustración 59 Path (Controller -PC 20)

En esta última sección del presente capitulo, se realizará una comparación de las dos redes simuladas, tomando como punto de evaluación la capacidad de administración, según las pruebas antes realizadas dentro del software de simulación en Packet Tracer.

En referencia a calidad de servicio, en un ambiente que podríamos considerar normal podemos observar un buen rendimiento en las dos redes, manteniendo una conexión total entre todos los dispositivos de red, sin pérdida de paquetes en el medio de transmisión, pero la característica que hace resaltar a la red SDN es la información que emite sobre el envío de los paquetes, además de tener un esquema gráfico de los equipos por los cuales fue transmitida la información desde su emisor hasta llegar al receptor, si bien en teoría en la red jerárquica se puede realizar el mismo proceso, el proceso es por individual, se debe entrar a cada equipo de la red para conocer por qué puerto fluyo la transmisión de mensaje pero eso involucra la inversión de una gran cantidad de tiempo a comparación con el utilizado en el controlador.

En el siguiente punto, la administración, es un punto muy importante y si bien en las pruebas tuvieron un rendimiento parecido, la experiencia con la configuración de los equipos explica muchas cosas, ya que si bien ambas cumplen con sus funciones, el proceso para agregar reglas, para administrar equipos de la red es completamente diferente, en la red SDN se hace un control total de los equipos desde un solo punto y se puede distribuir de manera general las reglas realizadas, en la red jerárquica se debe realizar una administración individual y al integrar una nueva regla se debe realizar en cada equipo que involucrará a la nueva regla. Este es uno de los puntos que resaltan en cuanto a administración en la red SDN, ya que en la simulación el controlador permite tener un control general, sin la necesidad de entrar a los equipos, este nuevo equipo integrado a la red realiza todo el trabajo desde un solo punto.



	pc1-pc2	pc1-pc4	pc1-pc7	pc1-pc6	pc1-pc5	pc1-Srv1	pc1-Svr2	pc1-Router
Jerárquica	0,021	0,013	0,12	0,631	0,537	0,031	0,029	0,034
SDN	0,015	0,008	0,05	0,452	0,3	0,028	0,014	0,026

Ilustración 60 Comparación red jerárquica vs SDN

Como se muestra en el último grafico comparativo de envío de paquetes, la velocidad de trasmisión de datos de la red SDN es superior a la velocidad de la red jerárquica debido a la separación de la capa de datos de la capa de control lo cual facilita la transmisión y la determinación de un camino óptimo para lograr una comunicación exitosa.

CAPÍTULO 5
CONCLUSIONES

Al concluir con el desarrollo de las simulaciones planteadas en los objetivos de este proyecto técnico, se pudo tener una compresión completa del funcionamiento de la red jerárquica actual de la Universidad Politécnica Salesiana, considerando todos los aspectos de conexión entre equipos que posee en la actualidad la red.

El estudio de mercado de los sistemas SDN dio a entender sobre el mercado ecuatoriano en redes, para poder tomar la mejor decisión en cuanto a equipos para la red SDN, además de identificar las marcas más importantes en el campo de las redes definidas por software y que se pueden considerar para futuros proyectos.

Después de realizar el análisis de los conceptos de SDN y las aplicaciones de simulación, se ha logrado un amplio conocimiento del funcionamiento y desarrollo de estas redes y aunque aún se considera un campo en desarrollo y de progreso, es una implementación que ya se encuentra en algunas estructuras importantes alrededor del mundo por su desarrollo en cuanto a administración de la red y de todos los recursos de esta.

Con la comparación de las redes simuladas, se concluyó que la administración de la red SDN facilita el trabajo del personal a cargo, como se mostró en los resultados en el capítulo anterior, los beneficios de centralizar el control de toda la red son extensos, además de dar un paso al futuro de las redes y con lo cual generamos un progreso en cuanto a la eficiencia de la red y la optimización de sus recursos, tomando en cuenta que se genera un control con una interfaz sencilla y adaptable para el usuario encargado de su monitoreo.

RECOMENDACIONES

Se recomienda para futuros temas de estudio, analizar equipos que se están desarrollando en base a esta nueva estructura de red, además de expandir los beneficios que con el desarrollo de estos equipos de ser se pueden generar ya que este campo puede tener un gran desarrollo en el futuro y tener equipos diseñados para trabajar bajo estos estándares.

En cuanto a simulación se aconseja empezar por los softwares de simulación conocidos para tener bases del funcionamiento de estos, ya que el tiempo que requiere conocer un nuevo sistema y poder implementar en un tema de estudio es muy extenso y si los simuladores ya conocidos y utilizados en la formación como estudiante contiene todo lo necesario para el desarrollo del estudio se puede considerar en la mejor opción para el desarrollo del estudio.

Recomendamos indagar en los simuladores de software libre y su correcto funcionamiento, ya que, en el campo de las redes, el sistema operativo Linux al ser libre es muy utilizado y por lo cual se debe desarrollar una investigación relacionando las redes de software libre con los simuladores de distribuciones como Ubuntu 20 o superiores que existan en el mercado en el tiempo del estudio.

Si se desea ampliar el tema se sugiere buscar en textos de la IEEE, ya que en estos amplían los conceptos y plantean nuevos problemas que se encuentran en el camino del desarrollo de estas redes que pueden ser temas de estudio para los futuros estudiantes universitarios, además de poder enfocarse en puntos relacionados como el desarrollo de API o de interfaces gráficas para estas controladoras.

REFERENCIAS

(1) New Messages! (n.d.). Retrieved January 31, 2022, from https://www.arubanetworks.com/latam/faq/que-es-la-arquitectura-spine-leaf/

Al-Somaidai, M. B. (2014). Survey of Software Components to Emulate OpenFlow Protocol as an SDN Implementation. *American Journal of Software Engineering and Applications*, *3*(6), 74. https://doi.org/10.11648/j.ajsea.20140306.12

BARRIOS, J. P. R. M. B. (2014). No TitleМини-инвазивные вмешательства под ультразвуковым контролем при эхинококковом абсцессе печени. *Diseño De Un Modelo De Control Interno En La Empresa Prestadora De Servicios Hoteleros Eco Turisticos Nativos Activos Eco Hotel La Cocotera, Que Permitira El Mejoramiento De La Informacion Financiera*, 97.

Centeno, A. G., Manuel, C., Vergel, R., & Calderón, C. A. (2014). Controladores SDN, elementos para su selección y evaluación. *Telemática*, *13*(3), 10–20.

Fabrizio, O. (2018). *Económica para la Implementación de Laboratorio de SDN Escuela de Ingeniería Eléctrica Facultad de Ingeniería*.

Ghaliya Alfarsi. (2020). Using Cisco Packet Tracer to simulate Smart Home. *International Journal of Engineering Research And*, *V8*(12), 670–674. https://doi.org/10.17577/ijertv8is120211

Henri. (2018). 済無No Title No Title No Title. *Angewandte Chemie International Edition, 6(11), 951–952.*

Http, E. (2020). *El protocolo HTTP*.

Industrial, E. (2018). *Estudio de un proceso para innovar y satisfacer la experiencia postventa del cliente Escola Tècnica Superior d ' Enginyeria Industrial de Barcelona*.

Magazine, T. H. E., & Usenix, O. F. (2000). *NOT BE THEME ISSUE : SECURITY edited by Rik Farrow*. *25*(7).

Mecánica, F. DE, por, P., & Diego Cruz Freire Darwin Vinicio Chimbo Chimbo, J. (2015). *Escuela Superior Politécnica De Chimborazo*.

Morat, D. (n.d.). *Esquemas de direccionamiento IP Direccionamiento Classful*. 1–9.

Nielsen, P. (2009). Coastal and estuarine processes. In *Coastal And Estuarine Processes* (pp.

1–360). https://doi.org/10.1142/7114

OpenFlow vulnerability assessment Enhanced Reader.pdf. (n.d.).

Pengaruh PMA, PMDN, TK, dan I. (2020). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*. *2507*(February), 1–9.

Pereira, G., & Gamess, E. (2017). Lineamientos para el Despliegue de Redes SDN/OpenFlow. *Revista Venezolana de Computación*, *4*(2), 21–33. http://www.svc.net.ve/revecom

Ponce Yumbato, G. (2020). *SD- ACCESS, Redes Definidas por Software*. http://localhost:8080/xmlui/handle/123456789/90

Qhwzrun, H., Zlwk, S., Wr, U., Zlwk, Q., Fruuhr, D., & Hgx, X. (2011). *5P] Ls Kl Klzltwl | V Lu Ylklz 07] Jvu*. *8*.

Soluci, G. D. E. L. A. (2019). *DESCRIPCIÓN GENERAL DE LA SOLUCIÓN*.

Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and Simulation of Local Area Network Using Cisco Packet Tracer. *The International Journal of Engineering and Science*, 2319–1813. https://doi.org/10.9790/1813-0610026377

Thesis, T. P. (2019). *Cisco DNA Center Multi Tenant Manager*.

Valencia, B., Santacruz, S., & Padilla, L. Y. B. J. J. (2015). *Mininet : una herramienta versátil para emulación y prototipado de Redes Definidas por Software 1 Mininet : a versatile tool for emulation and prototyping of Software Defined Networking*. *17*, 62–70.

Wallace, B. Y. T. C., Velasco, A., Lay, T., Zhang, J., Tromp, J., Tape, C., Liu, Q., Thompson, E. M., Wald, D. J., Thio, H. K., Kanamori, H., ΤΖΕΦΕΡΗΣ, Π., Razafindrakoto, H. N. T., Martin Mai, P., Mai, P. M., Thingbaijam, K. K. S., Jordan, T. H., Juarez, A., Ji, C., … Lavallée, D. (2016). ΒΙΟΕΚΧΥΛΙΣΗ ΟΞΕΙΔΩΜΕΝΩΝ ΜΕΤΑΛΛΕΥΜΑΤΩΝ ΝΙΚΕΛΙΟΥ ΜΕ ΤΗ ΧΡΗΣΗ ΕΤΕΡΟΤΡΟΦΩΝ ΜΙΚΡΟΟΡΓΑΝΙΣΜΩΝNo Title. *Bulletin of the Seismological Society of America*, *106*(1), 6465–6489. http://www.bssaonline.org/content/95/6/2373%5Cnhttp://www.bssaonline.org/content/95/6/2373.short%0Ahttp://www.bssaonline.org/cgi/doi/10.1785/0120110286%0Ahttp://gji.oxfordjournals.org/cgi/doi/10.1093/gji/ggv142%0Ahttp://link.springer.com/10.1007/s00024-01

Zeng, D., Gu, L., Pan, S., & Guo, S. (2020). Software Defined Networking II: NFV. *SpringerBriefs in Computer Science*, 77–100. https://doi.org/10.1007/978-3-030-32942-6_5