42

Fecha de presentación: diciembre, 2020
Fecha de aceptación: febrero, 2021
Fecha de publicación: marzo, 2021

IMPLEMENTACIÓN

DE UNA RED DEFINIDA POR SOFTWARE QUE PERMITA BRINDAR SERVICIO DE VoIP SEGUROS

IMPLEMENTATION OF A SOFTWARE DEFINED NETWORK THAT MAKES IT POSSIBLE TO PROVIDE SAFE VoIP SERVICE

Bryon Wladimir Oviedo Bayas[1]
E-mail: boviedo41@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-5366-5917
Emilio Rodrigo Zhuma Mera[1]
E-mail: ezhuma@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-3086-1413
Génesis Katherine Bowen Calero[1]
E-mail: genesis.bowen2015@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-3702-0203
Bryan Sleyter Patiño Maisanche[1]
E-mail: bryan.patino2015@uteq.edu.ec
ORCID: https://orcid.org/0000-0003-2723-0204
[1] Universidad Técnica Estatal de Quevedo. Ecuador.

Cita sugerida (APA, séptima edición)

Oviedo Bayas, B. W., Zhuma Mera, E. R., Bowen Calero, G. K., & Patiño Maisanche, B. S. (2021). Implementación de una red definida por software que permita brindar servicio de VoIP seguros. *Revista Universidad y Sociedad*, 13(2), 389-396.

RESUMEN

Es un nuevo paradigma al escuchar hablar de las redes SDN (Redes definidas por software), son más agiles, escalables y dinámicas, para un mejor aumento de programación y automatización. Presenta algunas ventajas una de ella es la reducción de costos operativos, mejora en el rendimiento de la red, su arquitectura es abierta lo que permite una mejor variedad de proveedores para las empresas que deseen migrar a estas redes. El presente proyecto está enfocado a la implementación de una red definida por software (SDN) que permita brindar servicio de VoIP seguros. Es por ello que uno de sus objetivos es analizar e identificar cuáles son los controladores y protocolos utilizados en las redes SDN y seleccionar el más acorde al proyecto de investigación. Se propone realizar el diseño e implementación de una red, en un ambiente físico. Los equipos que se utilizaran en la red SDN, consiste en un Routerboard y teléfonos IP, el cual va a permitir la interconectividad de los mismos y accesibilidad a Internet. En este escenario de prueba se plantea efectuar métricas, para medir la latencia, rendimiento, ancho de banda, entre otros. También se pretende evaluar la seguridad, que presenta la red SDN a través de la tecnología VoIP, para ello se realizará ataques de seguridad para comprobar su vulnerabilidad. Y por último se discutirá los resultados obtenidos y se expondrá las conclusiones y recomendaciones acerca de los objetivos propuestos.

Palabras clave: Redes definidas por software, OpenFlow, controladores, VoIP, OpenDayLight.

ABSTRACT

It is a new paradigm to hear about SDNs (Software Defined Networks), they are more agile, scalable and dynamic, for a better increase of programming and automation. It presents some advantages one of them is the reduction of operational costs, improvement in the performance of the network, its architecture is open what allows a better variety of suppliers for the companies that want to migrate to these networks. This project is focused on the implementation of a software defined network (SDN) to provide secure VoIP service. That is why one of its objectives is to analyze and identify which are the controllers and protocols used in the SDNs and to select the most appropriate for the research project. It is proposed to carry out the design and implementation of a network, in a physical environment. The equipment that will be used in the SDN network, consists of a routerboard and IP phones, which will allow the interconnectivity of them and accessibility to the Internet. In this test scenario, metrics are proposed to measure latency, performance, bandwidth, among others. It is also intended to evaluate the security, which presents the SDN network through VoIP technology, for this purpose security attacks will be carried out to check its vulnerability. Finally, the results obtained will be discussed and the conclusions and recommendations regarding the proposed objectives will be presented.

Keywords: Software defined networks, OpenFlow, controllers, VoIP, OpenDayLight.

INTRODUCCIÓN

Actualmente el área tecnológica se desarrolla a pasos agigantados al pasar los años. Con la llegada de las redes de quinta generación, las empresas tienen un gran reto y tratan de implementar equipos y diferentes tecnologías que estén a la vanguardia, y por supuesto que satisfagan a sus clientes (Orgaz, 2019).

Los equipos de telecomunicaciones tienden a evolucionar con el tiempo, todo esto para brindar un mejor servicio. La comunicación a nivel mundial exige cada vez una mejor calidad en servicios y es ahí donde las infraestructuras antiguas están quedando obsoletas. Las nuevas tecnologías como Internet de las cosas (IoT), Inteligencia artificial, telefonía IP, aplicaciones inteligentes; entre otras, requieren mejor calidad en los servicios que prestan las redes, los mismos que provocan cambios en las configuraciones, administración de equipos y en muchas ocasiones en medios de comunicación.

La telefonía surgió de la necesidad de tener un medio para que las personas se comuniquen (Aguirre Paz, 2005). En décadas pasadas solo existía la telefonía fija, pero con el desarrollo del internet y las redes de telecomunicaciones, todos los servicios analógicos han migrado a ser digitales. La telefonía evolucionó de fija (análoga) a telefonía IP (digital); es decir, que la voz se comprime y se transmite por la misma red de datos mediante el protocolo IP (Moyolema Tenegusniay, 2015). Este cambio causó grandes beneficios a las empresas porque disminuyeron los gastos destinados a llamadas telefónicas; también, se redujeron los costos de implementación de equipos y de instalación, debido a que solo tienen que disponer de una red de datos para tener servicios VoIP (Caldera & Suazo, 2011).

Al implementar más de un servicio en la red, ésta necesita un mayor ancho de banda; por ello, en la actualidad este tipo de servicios se está implementando sobre redes definidas por software (SDN), que es un nuevo concepto de arquitectura de red en la cual se facilita la gestión de la misma, ya que es escalable y toda su inteligencia se encuentra en un controlador central (Seyeon Jeong, 2016).

Todo lo anteriormente descrito se puede evidenciar en el proyecto de investigación denominando “Análisis de redes SDN utilizando Mininet e implementación de un Deep Packet Inspector” realizado por Li, et al. (2016), en el cual, se implementó un inspector de paquetes desarrollado en lenguaje Java para detectar y marcar paquetes que se encuentren en la red que permite dividir el tráfico VoIP y Web y que éste pueda ser utilizado para diversas funcionalidades y garantizar que exista calidad de servicio.

De igual manera, en el trabajo de investigación realizado por Flores Moyano (2018), se propuso diseñar una arquitectura para la gestión de redes residenciales mediante el uso de funciones de virtualización y redes definidas por software, en la cual se utilizan aplicaciones para uso de usuarios que gestionan servicios residenciales tales como el consumo de internet y servicio telefónico. Además, el investigador incluye funcionalidades de administración de tráfico para que servicios en línea como videos en alta definición y juegos tengan un rendimiento óptimo.

En el Ecuador existen varios estudios referentes a redes definidas por software y su implicación con servicios de VoIP. Moscoso Clerque (2016), indica en su estudio que se desarrolla una aplicación para tener calidad de servicio priorizando tráfico en una red definida por software. La aplicación se desarrolló bajo lenguaje Java y se ejecutó junto con el controlador Floodlight, las pruebas consistieron en realizar llamadas telefónicas y enviar paquetes que saturen la red permitiendo que la aplicación implemente calidad de servicio y no se afecte la llamada.

Por otro lado, se cuenta con un estudio denominado “Despliegue de una red SDN aplicando el protocolo MPLS y generando políticas de QoS para servicios de telefonía IP” realizado por Fernández & Ulloa (2016). En este trabajo los autores plantean un laboratorio de pruebas en una red SDN con el controlador OpenDayLight, en el cual se gestionan y administran todos los aspectos concernientes a equipos que envían paquetes y también se implementa el protocolo de transporte MPLS. Además, el servicio VoIP es implementado sobre una nube con tecnología de virtualización OpenStack en el cual se aplican pruebas para verificar la calidad de servicio.

Por lo antes expuesto, se puede determinar que es factible proponer un proyecto de investigación que permita diseñar e implementar una red definida por software para brindar servicios de VoIP seguros. La implementación de este servicio en la red SDN se realizará creando y configurando VLANs sobre equipos físicos que contengan el protocolo OpenFlow (Lara, et al., 2014). En esta red se garantizará la seguridad y confiabilidad en él envió paquetes mediante la integración de algoritmos de encriptación; también, se evaluará la calidad de servicio en la trasmisión de VoIP (Tablas 1 y 2).

Tabla 1. Recursos de Hardware.

Cantidad	Hardware	Descripción
2	Computadora Portátil	Dell Inspiron '15,6 2,90 GHz Intel Core i7-7500U 8 GB RAM 4 GB Tarjeta de video Radeon HP Intel Core i3-4010U 4 GB RAM
2	Impresora	Epson L365 Series Epson L355 Series
1	SSD	Samsung 860PRO 1TB
1	RouterBoard	Microtik RB11UiAS-RM
1	Switch	HPE OfficeConnect 1920S

Tabla 2. Recursos del Software.

Software	Descripción
Sistemas Operativos	• Windows 10 • Ubuntu 18.04
Programas de Oficina	• Paquete de Office de Microsoft
Software de trabajo	• OpenDaylight • VirtualBox • Elastix • 3CX • Wimbox
Otros	• Gantt Project • Wireshark • Advanced IP Scanner • Prezzi

DESARROLLO

Etapa 1 – Identificación de controladores y protocolos que pueden ser implementados en una red SDN.

A continuación, en esta etapa se detallará cuáles son los controladores y protocolos y que función cumple.

Identificación de protocolos SDN

En la tabla 3, se indican los protocolos algunos de ellos, ya existentes con cada uno de sus fabricantes o desarrolladores, que funciones realizan cada uno de ellos, con el objetivo de determinar cuál es el que mejor se adapta a las necesidades para la implementación de la red SDN.

En el mercado ya han desarrollado equipos basado con OpenFlow, es el protocolo predominante para las redes SDN, aunque se están diseñando arquitecturas utilizado otros métodos de comunicación, tales como los protocolos: BGP, MPLS-TP, NETCONF, XMPP.

Tabla 3. Protocolo de las redes SDN.

PROTOCOLO	DESARROLLADO POR	FUNCIÓN
Border Gateway Protocol (BGP)	Estandarizado por la RFC.	Permite el intercambio de información entre hosts de Gateway en la red.
Perfil de Transporte - Multiprotocol Label Switching (MPLS-TP)	Internet Engineering Task Force (IETF)	Diseñado como una tecnología de capa de red en redes de transporte.
NETCONF	Internet Engineering Task Force (IETF)	Resuelve problemas que existen con los protocolos SNMP y la CLI.
Protocolo de Presencia y Mensajería Extensible (XMPP)	Jeremie Miller	Mensajería instantánea, distribución de la información y detección en línea.
OpenFlow	Universidad de Stanford y California	Permite el accesibilidad directa y manipulación entre los dos planos.

De acuerdo a las necesidades de la red SDN se seleccionó el protocolo OpenFlow. Presenta muchas ventajas que sobresale de otros protocolos, esto es gracias a las organizaciones principales como la ONF (OpenNetworking, 2020), que ofrece mejoras en cuanto a sus actualizaciones para un buen desempeño en una red SDN.

Este permite la accesibilidad directa y manipulación de los planos de datos de los dispositivos y el plano de control, además ofrece un mayor ancho de banda, permite una configuración automatizada de la red el cual conlleva a reducir gastos de operación y menor inactividad ante fallos con la red.

Identificación de controladores SDN

El controlador es el núcleo central de la arquitectura SDN (Escobar Ordoñez, 2015). Es por ello, se han tomado en cuenta seis controladores, de los cuales se analizará cada una de las características, para identificar que controlador es el más acorde al diseño de la red SDN (Tabla 4).

Tabla 4. Controladores SDN.

CARACTERÍSTICA	CONTROLADORES					
	NOX	**POX**	**BEACON**	**ONOS**	**Ryu**	**OpenDayLigth**
Soporte	OpenFlow v1.0	OpenFlow v1.0	OpenFlow v1.0	OpenFlow v1.0/v1.3	OpenFlow v1.0/v1.3	OpenFlow v1.0/v1.4
Lenguaje	C++	Python	Java	Java	Python	Java
Plataformas	Linux	Linux, Mac Os, Windows	Linux, Mac Os, Windows	Linux	Linux	Linux, Mac Os, Windows
Código abierto	Si	Si	Si	Si	Si	Si
Interfaz gráfica	Python + QT4	Python + QT4	Web	Web	Web	Web
API	No	No	No	Si	Si	Si
Documentación	Media	Baja	Buena	Media	Media	Media

Una vez analizado cada una de las características se seleccionó el controlador que se adapte mejor al proyecto de investigación, como lo es OpenDayLight. Este ofrece una plataforma compatible con SDN (Moreno & Zambrano, 2018). Además, cuenta con una plataforma de abstracción de servicios, esto es ventajoso para los desarrolladores porque pueden crear aplicaciones con cualquier protocolo sin ningún inconveniente, de la misma manera en diferentes equipos.

Etapa 2 – Implementación de la red SDN en un escenario físico.

En esta etapa se realizó el diseño de la red SDN. Este diseño fue implementado en el Laboratorio de Redes de la FCI, el escenario consiste en un router Mikrotik RB11UiAS-RM, un switch HPE OfficeConnect 1920S, dos teléfonos IP YEALINK T20P y una laptop (Dónde estará el controlador) (Figura 1).

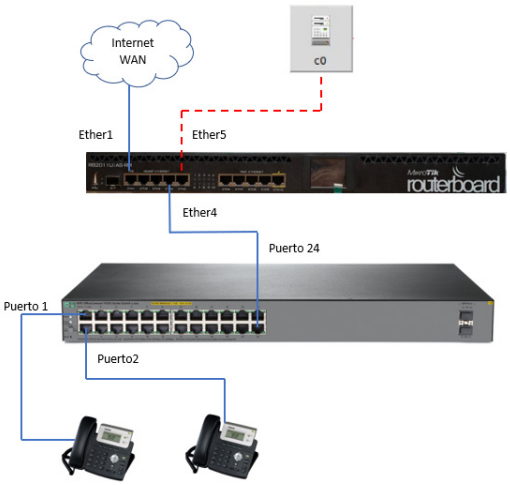

Figura 1. Diseño de la Red SDN.

Para comenzar, se necesita descargar el software "WinBox", el cual permitirá la conexión con el equipo para su respectiva configuración. Es necesario comprobar la conectividad (cableado) del router con el pc. Se ejecuta el programa y de preferencia se ingresa mediante la MAC Address del dispositivo (Otra forma, es con la IP del router que inicialmente tiene 192.168.88.1). Se tendrá dos tipos de redes: la WAN estará en el puerto 1 del Mikrotik y la LAN con una IP 192.168.2.1 en el router. Dentro de la red LAN se brindarán a los puertos direcciones DHCP, con la finalidad que exista interconectividad y servicio de internet (esto último si se desea, caso contrario se omite).

Para los teléfonos se configuró la central telefónica en Elastix. En una máquina virtual, uno de los requisitos es una IP pública, para esta investigación, se dio la IP 192.168.2.249 que está dentro del rango de la red LAN creada. Se abre el navegador y se coloca la dirección 192.168.2.249:5001 para ejecutar el 3CX el cual proviene de Elastix para la configuración de las extensiones que se otorgarán a los teléfonos IP.

Extensión 1001 fue asignada al teléfono Telematica2 con el cual se identifica, y como id de llamada tiene el nombre de root2.

Extensión 1002 fue asignada al teléfono Telematica3 con el cual se identifica, y como id de llamada tiene el nombre de root3 (Figura 2).

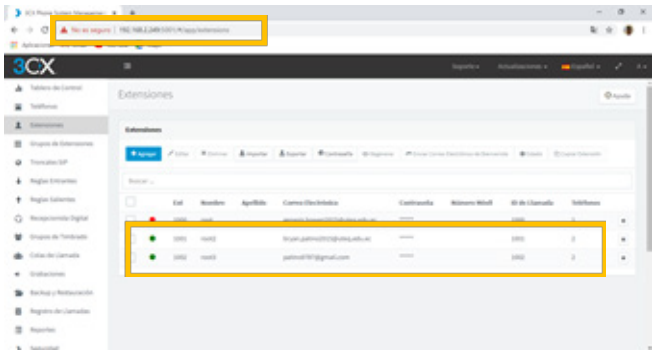

Figura 2. Configuración de las extensiones en 3CX para los teléfonos IP.

Se configurará la VLAN 200 dentro del router y del switch administrable para la comunicación de la telefonía IP. Habilitando los puertos 1 y 2 para la conexión con los teléfonos IP (Included y Untagged) y el puerto 24 para la comunicación entre el switch (Included y Tagged) y el router (puerto openflow) (Figura 3).

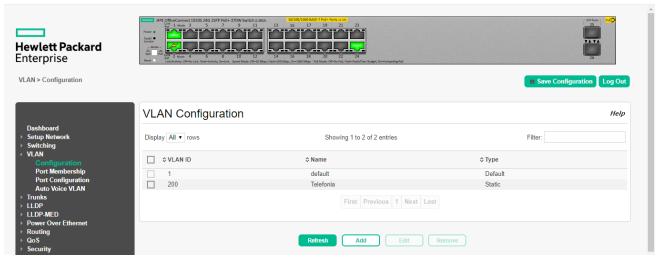

Figura 3. Configuración de la VLAN en el Switch.

Se necesitará el paquete OpenFlow, descargado de la página de Mikrotik e instalado dentro del router. OpenFlow brinda tres opciones: Switches, Flows y Ports. En Switches se configuró al router como switch OpenFlow, asignándole la IP del controlador 192.168.2.250. En Ports se añadió al puerto (puerto 4 cuyo puerto tiene el nombre de telemática 2) designado a OpenFlow (Figuras 4 y 5).

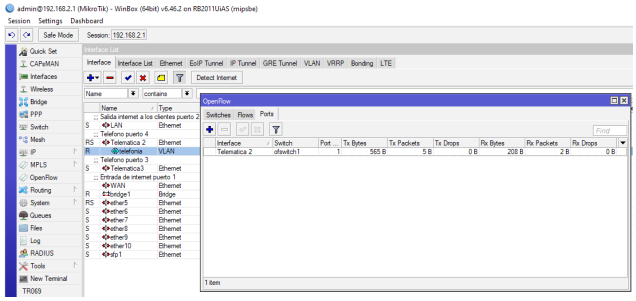

Figura 4. VLAN y OpenFlow añadidos al puerto 4.

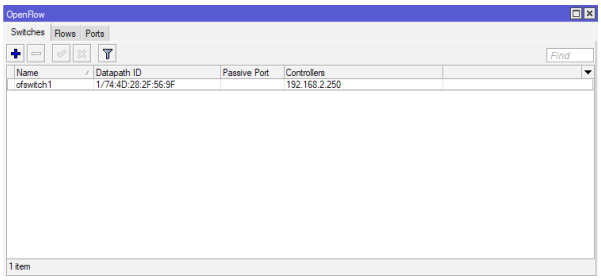

Figura 5. Configuración del router como Switch OpenFlow.

Se instala Ubuntu en el VirtualBox (máquina virtual, IP 192.168.2.250), se descarga e instala el controlador OpenDayLight, cuya versión fue 0.4.0-Beryllium. Para ingresar al controlador desde el modo gráfico, se abrió una pestaña en el navegador, se le coloco la siguiente dirección 192.168.2.250:8181/index.html Cargará el controlador pidiendo autenticación (Figura 6).

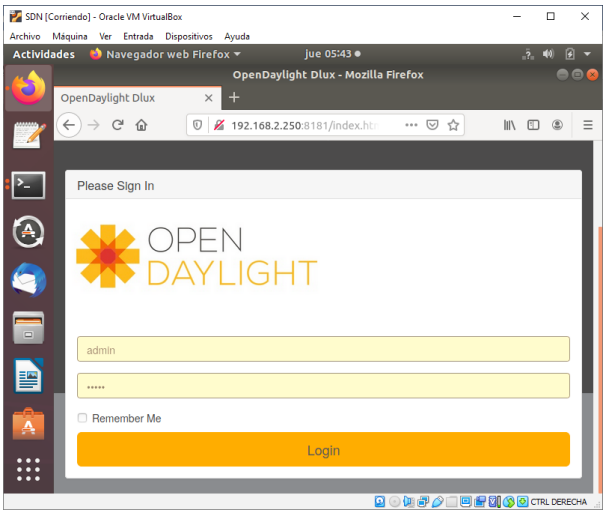

Figura 6. Ingreso al controlador OpenDayLight mediante Ubuntu.

Dentro del cuadro de controls aparecerá el Swicth OpenFlow con los Host (teléfonos IP) conectados, en este caso, hay dos teléfonos conectados al switch.

Host: 00:15:65:43:55:e1 ip:192.168.2.248 conectado al puerto 1

Host: 00:15:65:47:71:71 ip:192.168.2.100 conectado al puerto 2 (Figura 7).

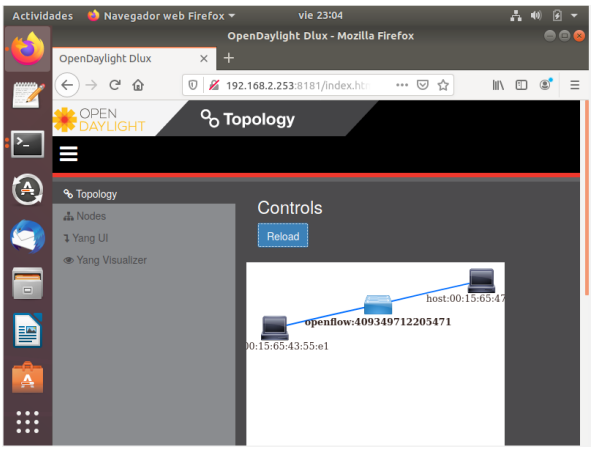

Figura 7. Topología de la red SDN.

Los resultados obtenidos en este proyecto para los diferentes parámetros, fueron tomadas de las herramientas que brinda el router Mikrotik para escaneo y monitoreo de las redes.

Latencia

Para esta métrica de evaluación, se hicieron varias pruebas de conectividad utilizando la herramienta Ping (Running) propia de Mikrotik, para verificar el retardo de los paquetes en llegar a su destino, a continuación, se dará de ejemplo una de las pruebas realizadas, dando a conocer los resultados.

En la Figura 8, se observa la prueba realizada a la dirección 192.168.2.100.

Se obtuvo un resultado óptimo, con 208 paquetes enviados y la misma cantidad recibida, dando a conocer que no hubo pérdidas de paquetes en el transcurso de la transmisión, con un retardo de 5ms en el paquete #56 y 0ms en los paquetes restantes.

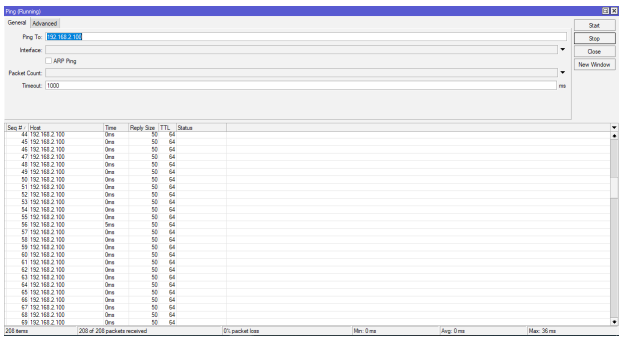

Figura 8. Ping (Running).

En la Figura 9, se observa la prueba realizada a la dirección 192.168.2.248.

Se obtuvo un resultado óptimo, con 242 paquetes enviados y la misma cantidad recibida, dando a conocer que no hubo pérdidas de paquetes en el transcurso de la transmisión, con un retardo de 1ms en 3 paquetes transmitidos y 0ms en los paquetes restantes.

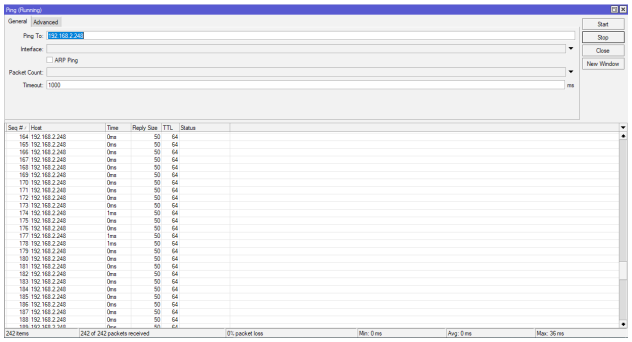

Figura 9. Ping (Running).

Rendimiento y Performance

En esta evaluación se utilizó la visualización de las interfaces para el monitoreo de la red del Mikrotik para obtener resultados del rendimiento, dando como resultados una transmisión y recepción de velocidad de 891 kbps, siendo estos 53 paquetes enviados y 53 recibidos.

Teniendo caminos rápido con una velocidad de 432bps y una recepción de 488bps, con 1 paquete enviado y uno recibido, concluyendo que es óptima la red SDN (Figura 10).

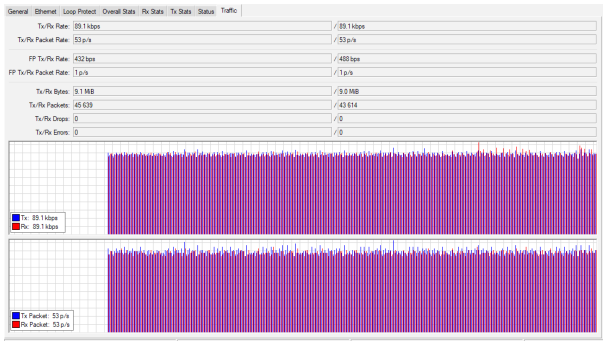

Figura 10. Rendimiento y Performance.

Caso contrario fue sin el controlador OpenFlow dónde hubo discrepancia tanto en la transmisión y recepción de velocidad de los paquetes como se puede observar en la Figura 11.

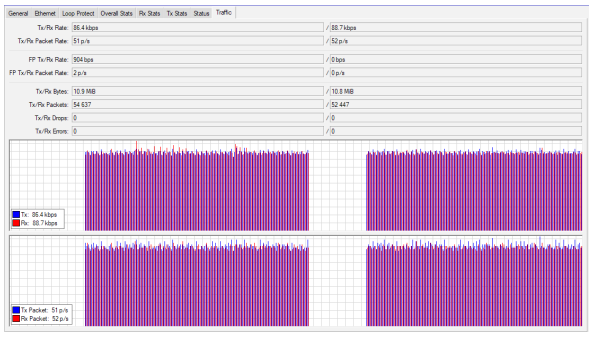

Figura 11. Rendimiento y Performance en una red sin OpenFlow.

Seguridad

Para prevenir ataques a la red, se optó por una medida de seguridad que ofrece las VLAN, comúnmente conocida como el Enmascarado. Dónde el administrador de la red, debe conocer cada una de las direcciones IP, porque a cada dispositivo que se conecte se le asignará una IP estática, y se habilitará un puerto dentro del switch, como se observa en la Figura 12, hay dos puertos asignados para los teléfonos y 1 que se conectará del router con el switch.

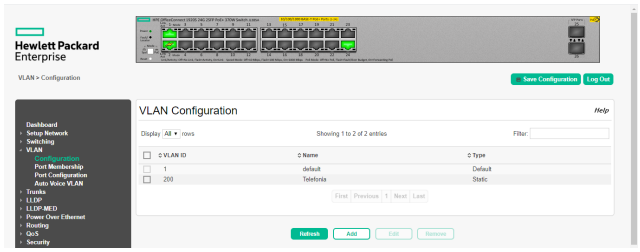

Figura 12. Habilitación del puerto 1 y 2 para los teléfonos IP.

Es decir, cualquier persona que se conecte a la red o al switch, no tendrá acceso, porque no se está generando una IP para aquel host.

Ventajas:

- No tener dirección IP para la realización de los ataques, incluso usando herramientas de búsquedas de IP como lo demuestra la Figura 13.
- Aunque tuviera una IP, el puerto donde está conectado no está habilitado para la transmisión de datos.
- La VLAN creada tiene un ID, y es otro número que se tiene que descubrir en casa de querer hackear la red.

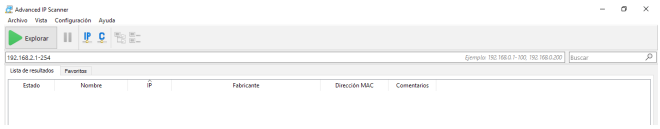

Figura 13. Advanced IP para el escaneo de la red.

Entre otras ventajas, Mikrotik permite implementar reglas para los usuarios. Es decir, se puede implementar reglas que envíen a una lista negra a las direcciones o host que emitan repetidas solicitudes hacia el servidor, logrando así que esta IP o host no vuelva más a aparecer en el listado de dispositivos conectados en la red.

CONCLUSIONES

La investigación sobre los diferentes tipos de controladores y protocolos a usar, ayudó a determinar las herramientas necesarias para realizar las diferentes configuraciones. Una buena elección del controlador OpenDayLight y el protocolo OpenFlow será de gran ayuda para una estable conexión con los equipos.

La prueba fue realizada en un ambiente controlado, determinando que la red tenía menos pérdidas y retardo en cuestión del intervalo de tiempo de los paquetes que a diferencia de una red telefónica sin VLAN y OpenFlow. También se pudo constatar que SDN ocupaba casi toda la capacidad máxima de la velocidad de transmisión. Acorde a la seguridad, se pudo percibir varios tipos de seguridad que en un futuro se pueden implementar en las redes SDN con tecnología Mikrotik.

Dados los resultados obtenidos por el mismo software del router, se logra observar un mayor fluido del tráfico de voz, minimizando la perdida de paquetes y ocupando la máxima capacidad del canal tanto en transmisión, como en recepción, con minorías de tiempo en el retardo de cada paquete, haciendo que la red sea factible en cuanto a la transmisión VoIP.

REFRENCIAS BIBLIOGRÁFICAS

Aguirre Paz, J., & Ortega Castañeda, E. (2005). ***La calidad del servicio como uno de los elementos formadores de imagen. Estudio de caso: Telmex-Maxcom.*** (Tesis de grado). Universidad de las Américas Puebla.

Caldera Palma, J. C., & Suazo Sequeira, W. E. (2011). ***Planeación de un curso especializado en telefonía para profesionales de la industria de telecomunicaciones: Módulo III Telefonía IP.*** Universidad Nacional de Ingeniería.

Escobar Ordoñez, J. A. (2015). ***Control de flujo de una red definida por software usando sensores térmicos.*** UTA.

Fernández, M. M., & Ulloa, R. F. (2016). ***Despliegue de una red SDN aplicando el protocolo MPLS y generando políticas de QoS para servicios de telefonía IP.*** (Trabajo de Titulación). Universidad Politécnica Salesiana.

Flores Moyano, J. R. (2018). ***Contribución a las arquitecturas de virtualización de funciones de red y redes definidas por sotware aplicadas a las redes residenciales con gestión centrada en el usuario.*** (Tesis Doctoral). Universidad Politécnica de Madrid.

Jeong, S., Lee, D., Choi, J., Li, J., & Hong, J. (2016). Application-aware Traffic Management for OpenFlow networks. (Poencia). ***18th Asia-Pacific Network Operations and Management Symposium (APNOMS)***. Seoul, Korea.

Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network Innovation using OpenFlow: A Survey. ***IEEE Communications Surveys & Tutorials, 16(1),*** 493-512.

Li, G., Dong, M., Ota, K., Wu, J., Li, L., & Ye, T. (2016). Deep Packet Inspection Based Application-Aware Traffic Control for Software Defined Networks. (Ponencia). ***IEEE Global Communications Conference (GLOBECOM).*** Washington, USA.

Moreno Palacios, D. R., & Zambrano, A. M. (2018). ***Analisis comparativo del desempeño computacional de una aplicacion distribuida intensiva en datos en redes de dispositivos y redes definidas por software.*** (Trabajo de Titulación). Escuela Politécnica Nacional.

Moscoso Clerque, E. M. (2016). ***Desarrollo de una aplicación para la implementación de calidad de servicio por priorización de tráfico sobre una red definida por software (SDN).*** (Trabajo de Titulación). Escuela Politécnica Nacional.

Moyolema Tenegusniay, S. R. (2015). ***Diseño de un sistema de voz/ip para un call center en el Hospital Docente de la Policía Nacional Guayaquil N° 2.*** (Trabajo de Titulación). Universidad de Guayaquil.

OpenNetworking. (2020). Transforming access and edge networks by collaboratively building next generation mobile and broadband infrastructures, leveraging. ***OpenNetworking ONF***. https://www.opennetworking.org/

Orgaz, C. J. (31 de Mayo de 2019). 3 grandes ventajas que traerá la tecnología 5G y que cambiarán radicalmente nuestra experiencia en internet. ***BBC***. https://www.bbc.com/mundo/noticias-48477358