ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD: PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

ANÁLISIS COMPARATIVO ENTRE RED DE COMPUTADORAS TRADICIONAL Y RED DEFINIDA POR SOFTWARE: CASO DE ESTUDIO ESPAM MFL

AUTOR:

ALCÍVAR MARCILLO PEDRO ANTONIO

TUTOR:

DR. INF. MARLON R. NAVIA MENDOZA

CALCETA, MAYO 2019

DERECHOS DE AUTORÍA

PEDRO ANTONIO ALCÍVAR MARCILLO, declaro bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____

PEDRO A. ALCÍVAR MARCILLO

CERTIFICACIÓN DE TUTOR

MARLON R. NAVIA MENDOZA, certifica haber tutelado el trabajo de titulación **ANÁLISIS COMPARATIVO ENTRE RED DE COMPUTADORAS TRADICIONAL Y RED DEFINIDA POR SOFTWARE: CASO DE ESTUDIO ESPAM MFL**, que ha sido desarrollado por **PEDRO ANTONIO ALCÍVAR MARCILLO**, previa la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN DE LA UNIDAD DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

_____

DR. INF. MARLON R. NAVIA MENDOZA

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **ANÁLISIS COMPARATIVO ENTRE RED DE COMPUTADORAS TRADICIONAL Y RED DEFINIDA POR SOFTWARE: CASO DE ESTUDIO ESPAM MFL**, que ha sido desarrollado por **PEDRO ANTONIO ALCÍVAR MARCILLO**, previa la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN DE LA UNIDAD DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Dr. Inf. Jorge A. Párraga Álava

MIEMBRO

Dr. Inf. Jorge S. Herrera Tapia

MIEMBRO

Mg. Jessica J. Morales Carrillo

PRESIDENTE

AGRADECIMIENTO

En primer lugar agradecemos a Dios por permitirnos estar redactando estas líneas y continuar despertando a diario;

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de crecer como seres humanos a través de una educación superior de calidad y en la cual hemos forjado nuestros conocimientos profesionales día a día,

A todos los docentes que nos brindaron sus conocimientos y experiencias extra curriculares que solo se obtienen en el campo profesional,

Al personal de la institución que estuvo siempre presto para apoyarnos en las diversas necesidades que se suscitaban en el día a día de clases, de manera particular al departamento de tecnología que nos facilitaron la información necesaria para desarrollar este trabajo,

A nuestros queridos compañeros quienes nos demostraron siempre su amistad sincera, ya que siempre nos apoyamos entre todos, y

De manera muy especial expresamos nuestro agradecimiento a nuestro tutor el Ing. Marlon Navia quien nos brindó una guía acertada no solo en el proyecto de titulación sino también a lo largo del proceso de maestría.

El Autor

DEDICATORIA

Este trabajo lo dedico de manera especial a mi familia de corazón, por soportarme, quererme y estar para mí cuando los he necesitado, sin ustedes nada de esto hubiese sido posible,

A mi madre con la cual intercambiamos momentos terapéuticos, filosóficos o simplemente tonterías que se disfrutan a diario, gracias por enseñarme que la distancia puede llegar a ser tan solo una palabra en el diccionario,

A mi hermano Manuel que aunque por tratar de repararte la computadora de manera remota al final la dejo peor, sabes que te quiero.

Pedro Alcívar Marcillo

CONTENIDO GENERAL

CONTENIDO DE FIGURAS

CONTENIDO DE CUADROS

RESUMEN

Las redes de computadoras son una de las tecnologías que menos cambios significativos han experimentado desde su invención, esta afirmación se sustenta en que protocolos establecidos hace más de 25 años aún continúan vigentes. Por tal motivo, el objetivo de este trabajo fue comparar el paradigma de red tradicional con el modelo de redes definidas por software (Software Defined Network - SDN) en un entorno de red de área local que contaba con servicios propios de una institución de educación superior, para determinar la aplicabilidad de este último paradigma en el entorno analizado. Se implementaron dos entornos de simulación, uno de red tradicional, basada en la red del sector 8 de la ESPAM MFL, y una red SDN con un diseño similar pero con las características propias de este paradigma. Los entornos se implementaron en el simulador de red GNS3. Para agregar los servicios tales como servidor web y aula virtual se integró VirtualBox y VMware al simulador. Para obtener los resultados se implementaron máquinas virtuales en el simulador, las cuales realizaban consultas a los servicios locales y externos. De estas pruebas se obtuvieron la latencia, la variación del retardo y la pérdida de paquetes que fueron capturados por la aplicación de monitoreo de red Smokeping. Basados en los resultados de ambos paradigmas se determinó que SDN tiene la ventaja de requerir menor cantidad de dispositivos de conexión, además los resultados en cuanto al rendimiento, control y administración de la red favorecen la implementación de este modelo en entornos similares.

Palabras clave: Redes de computadoras, redes definidas por software, rendimiento de red, simulación.

ABSTRACT

Computer networks are one of the technologies that have experienced very few significant changes since their invention. This statement is based on the fact that protocols established more than 25 years ago are still valid. For this reason, the goal of this work was to compare, the traditional network paradigm against the software-defined network model (SDN) in a local area network environment which had common services for a higher education institution, to determine the applicability of this last paradigm in the analyzed environment. Two simulation environments were implemented, a traditional network, based on the ESPAM MFL's sector 8 network, and an SDN with a similar design, but with the proper characteristics of this paradigm. The environments were implemented in the GNS3 network simulator. For add the services such as web server and virtual classroom, VirtualBox and VMware were integrated into the simulator. To obtain the results, virtual machines were implemented in the simulator, which consulted the local and external services. From these tests, the latency, jitter, and packet loss were obtained by Smokeping network monitoring application. Based on the results of both paradigms, it was determined that SDN has the advantage of requiring fewer connection devices, as well as the results in terms of performance, control, and administration of the network favor the implementation of this model in similar environments.

Key words: Computer networks, software Defined network, network performance, simulation.

CAPÍTULO I. ANTECEDENTES

1.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

El concepto de Redes Definidas por Software *(Software Defined Networking,* SDN) es una idea que ya se planteaba desde el siglo pasado con iniciativas como *SOFTNET* o *Active Networks* que lograron incluir comandos en el campo de datos de los paquetes transmitidos en la red, que se ejecutaban, a medida que eran recibidos (Roncero, 2014). SDN tiene sus inicios con el proyecto *Ethane* (Barona, Valdivieso, & Guamán, 2014) el cual es comúnmente definido como la separación entre el plano de control y el plano de reenvío de datos. En otras palabras es la administración centralizada de la red por una plataforma de software (Dixon, 2016).

Las principales empresas de tecnología a nivel mundial cuentan con proyectos en ejecución con este paradigma, donde uno de los casos de mayor relevancia es la interconexión entre los centros de procesamiento de datos de Google. Empresas como Facebook y Microsoft son participantes activas en los avances en esta área tanto en el ámbito investigativo como práctico (Roncero, 2014).

A nivel mundial existen investigaciones referentes a casos de estudios de las SDN, (Roncero, 2014) hace énfasis en sus beneficios y los desarrollos en esta área de las empresas importantes del sector de redes tales como: Cisco, Juniper, HP, entre otras. Así mismo, autores como (Rojas, y otros, 2018) cuestionan su aplicación planteándose si el mercado y los administradores de redes están preparados para los cambios que incorpora este paradigma.

Latinoamérica no se ha desentendido de la tecnología SDN, incluso es posible asegurar que cada vez su aportación es mayor a esta área (Ruiz, 2015). Por ejemplo la empresa ISP en Cuba ETECSA, en la cual, se desarrolló un sistema de monitoreo que controla ciertos parámetros de rendimiento y seguridad de la red SDN (Marín, 2016). Otro caso interesante es el que plantea (Duarte & Lobo, 2015) en su estudio sobre la migración de toda la infraestructura de red tradicional a SDN dentro de las instituciones de educación superior, dándole prioridad a las redes inalámbricas.

En el ámbito nacional se considera que la aplicación de las SDN podría tener un impacto importante en el desarrollo de los servicios portadores, es por esta razón que los proveedores de estas infraestructuras en el país tienen muy pendiente la incursión en SDN como eje fundamental para el mejoramiento de la administración y mantenimiento de las redes (Pérez & Marín, 2015).

Dando continuidad al ámbito local se puede mencionar que aunque implementaciones importantes no salten a la vista, varias universidades del Ecuador están inmersas en investigaciones y desarrollo de prototipos para migrar su infraestructura de red tradicional a SDN o, trabajar en entornos híbridos. Una aplicación, que es de relevancia en el país, se da en la Escuela Politécnica Nacional (Bernal & Mejía, 2016), donde detalla la importancia de la selección del controlador (elemento principal de una red SDN) y de la obtención de los resultados en base al simulador Mininet.

En la ESPAM MFL se han desarrollado estudios relacionados al funcionamiento de la red de la institución. En el trabajo de (Vidal, 2016) se hace mención a los problemas que presenta la red en cuanto a su organización y aspectos de configuración, además se atribuyen estos inconvenientes al ser una entidad relativamente joven.

En la maestría en Tecnologías de la Información de la ESPAM MFL se pudo experimentar ciertos inconvenientes en cuanto al rendimiento de la red en el sector en el que se recibían clases, así como también en ciertas áreas circundantes como es el caso de biblioteca, el hotel-laboratorio y el edificio de posgrado. En este sentido amerita explorar opciones que contribuyan el mejoramiento del rendimiento de la red del sector 8 de esta institución.

A pesar de los estudios realizados, donde se han planteado la aplicación de técnicas para mejorar el funcionamiento de la red, no se ha considerado previamente un cambio significativo en la manera en que se gestionan las redes en esta institución, como podría ser la aplicación de SDN. Por lo tanto los autores se hacen la siguiente interrogante: ¿Qué diferencias relacionadas al funcionamiento y rendimiento existirían entre una red tradicional y una SDN aplicadas en la ESPAM MFL?

1.2 JUSTIFICACIÓN

Este estudio resulta muy relevante para los investigadores de redes de computadoras así como también para las organizaciones que se estén planteando mejorar la administración de sus redes, ya que a más de llevar a cabo la comparativa entre el paradigma de red tradicional y SDN en un escenario de red local, se realizó un desarrollo metodológico de las pruebas que puede ser útil para implementar SDN sobre un entorno existente así como también para una instalación totalmente nueva sobre dicho paradigma.

De igual manera este estudio sirve como introducción al concepto de redes definidas por software para quienes deseen incursionar en esta área, brindando ideas simples del funcionamiento de este paradigma, así como también nociones básicas acerca de sus elementos y características más relevantes.

A la hora de contemplar la implementación de redes SDN, el primer aspecto que se debe considerar, por su repercusión es el económico; ya que, no representa una mayor inversión dado que los equipos que se necesitan para gestionar la red son de características básicas. También de manera intrínseca no afecta al ambiente puesto que se utilizan una menor cantidad de dispositivos, además la saturación en dichos equipos es menor como resultado de separar el plano de control (Cordero Vizhñay, 2017).

Tal como plantean varios autores, los cambios tecnológicos generan choques culturales en los entornos que se deciden aplicar, pero de igual manera es necesario concientizar a las personas de los beneficios que podrían brindar soluciones como SDN en el manejo de las redes (Ruiz, 2015).

Finalmente se puede considerar el presente trabajo como un aporte para toda la comunidad estudiantil de la ESPAM MFL, así como también para todas las personas interesadas en el campo de redes y nuevas tecnologías al rededor del mundo, que pretendan demostrar los beneficios de SDN en varios escenarios de infraestructuras de redes de computadoras.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Realizar un análisis comparativo entre una red de computadoras tradicional y el paradigma de SDN, en un entorno de simulación basado en la infraestructura de la red de computadoras del sector 8 de la ESPAM MFL para determinar su aplicabilidad en esta área de la institución.

1.3.2 OBJETIVOS ESPECÍFICOS

- Definir un esquema de trabajo para comparar el paradigma de SDN y el enfoque de red tradicional.
- Obtener los resultados del rendimiento de una red tradicional y del modelo SDN en un ambiente simulado.
- Determinar la aplicabilidad de las redes definidas por software en el entorno analizado, con base en los resultados obtenidos previamente.

1.4 IDEA A DEFENDER

Los resultados del análisis comparativo entre una red tradicional y una red definida por software en un entorno universitario, permitirá determinar su factibilidad de implementación en instituciones de educación superior.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1 REDES DE COMPUTADORAS TRADICIONALES

Se pueden definir a las redes de computadoras como el conjunto de dispositivos tecnológicos que a través de un medio comparten información con otros dispositivos. La concepción de estas redes se basa en la necesidad de comunicarse que tienen las personas y en las nuevas industrias que surgen con el aporte de la tecnología. Se las conoce también como redes de datos, debido a que suelen transportar grandes cantidades de información.

Las redes de computadoras están entre las áreas que menos cambios significativos han experimentado desde la inserción de la tecnología en la sociedad, entendiendo por cambios significativos la manera en que son concebidas, diseñadas, implementadas y administradas. Los autores (Sezer, y otros, 2013) consideran que en una red tradicional el plano de control y el plano de datos se combinan en un nodo de red, asignando al plano de control la labor de configurar el dispositivo y programar la ruta de los paquetes, al contar con el camino definido. Dichos paquetes se envían al plano de datos, donde la data se reenvía mediante controles a nivel de hardware.

Los protocolos de red a menudo se organizan en tres planos: datos, control y administración. El plano de datos consta de los mensajes que generan los usuarios, para transportar dichos mensajes son necesarios protocolos de enrutamiento y conmutación como OSPF y STP. Los mensajes utilizados para este fin se denominan mensajes de control. Tanto el control como la administración pertenecen a la lógica del control de la red (Jain & Paul, 2013).

Para que pueda funcionar la infraestructura de las redes de computadoras son necesarios protocolos y estándares establecidos por las organizaciones pertinentes en la industria tecnológica, los protocolos actualmente se encuentran definidos en la arquitectura TCP/IP que es la líder mundial del sector y los estándares son criterios referentes a los medios de transmisión, los dispositivos y protocolos que soportan la arquitectura de red, dichos estándares los gestionan organizaciones como: ISO, ITU, IETF, IEEE, entre otros.

Las redes de computadoras son implementadas con una serie de equipos que cumplen funciones determinadas, un ejemplo preciso es el que menciona (Nunes, Mendonca, Nguyen, Obraczka, & Turletti, 2014) haciendo referencia a los dispositivos que conforman estas arquitecturas tales como: switches, routers, firewalls, entre otros y sus respectivas funciones en el procesamiento de los datos.

Las políticas de gestión de red suelen ser definidas por el operador de la misma, para luego configurar cada dispositivo en base a los requerimientos de dichas normas. Según (Nunes et al., 2014), está práctica demandará mayores esfuerzos a mayor tamaño de la red, y por este motivo las políticas establecidas rara vez son modificadas.

2.2 REDES DEFINIDAS POR SOFTWARE

Las SDN según (Xia, Wen, Foh, Niyato, & Xie, 2015) son un paradigma de redes emergente, en el que se separa el plano de control del plano de reenvío de datos y además se caracteriza por habilitar la programabilidad de los elementos y eventos de la red (Kreutz, y otros, 2015). En las SDN, los planos de control y datos se separan para reducir la complejidad y el costo de los switches (Jain & Paul, 2013).

Considerando la rigidez de muchas infraestructuras, ya que los dispositivos de redes generalmente son cerrados, patentados e integrados verticalmente; el modelo de red definida por software fomenta que los equipos de conmutación sean simples dispositivos de reenvió de paquetes y se desplace el control y administración de la red a un programa lógicamente centralizado denominado controlador de la red (Kim & Feamster, 2013).

2.2.1 COMPONENTES DE LA ARQUITECTURA SDN

La definición de los componentes de las SDN varía entre uno y otro autor, o pueden diferir en la terminología utilizada para describir los elementos de este paradigma. Como es el caso de (Kreutz, y otros, 2015) y (Xia et al., 2015), ambos estudios mencionan en diferentes términos las capas del modelo SDN, pero coinciden en que este paradigma consta de 3 planos o capas (Figura 1).

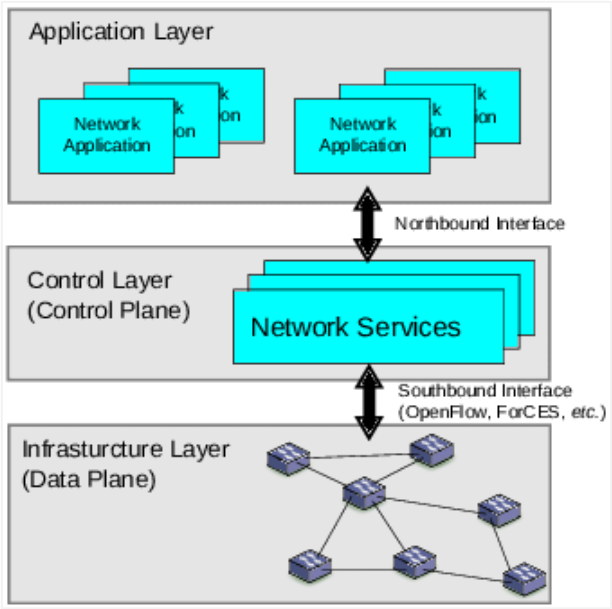

Figura 1. Arquitectura en capas de SDN

Fuente: (Braun & Menth, 2014)

Los trabajos antes mencionados hacen referencia a los elementos que conforman las capas de la arquitectura SDN, especificando en el plano de datos a todos los dispositivos de reenvió de paquetes sean estos físicos o virtuales, en el plano de control se implementan todas las soluciones de controladores disponibles y en la capa de administración se especifican todas las aplicaciones desarrolladas para la gestión de la red.

2.2.2 CONTROLADOR

En su gran mayoría las SDN se implementan basadas en el uso de un controlador, este actúa como una especie de cerebro de la red y facilita a los administradores una visión de todos los dispositivos conectados. También es el encargado de ejecutar acciones en respuesta a eventos inesperados y de realizar el monitoreo de la infraestructura (Calloni, y otros, 2018).

La administración central de la red que se menciona en SDN se basa en el uso de un controlador de red, siendo este considerado el elemento principal de dicho paradigma y a su vez un punto único de falla en la arquitectura (Mousavi & St-Hilaire, 2015). Así mismo, en la comparativa realizada por (Shalimov, Zuikov, Zimarina, Pashkov, & Smeliansky, 2013) se concluye que muchos de los controladores no están listos para trabajar en producción.

2.2.3 OPENFLOW

OpenFlow es una tecnología propuesta para estandarizar la forma en que un controlador se comunica con los dispositivos de red de una arquitectura SDN. Este protocolo permite a los investigadores probar nuevas ideas en un entorno de producción, así mismo, incluye capacidades de análisis de tráfico basado en software, actualización dinámica de reglas de reenvío, control centralizado y abstracción de flujo (Lara et al., 2014).

La tecnología comúnmente utilizada en implementaciones de SDN es el protocolo OpenFlow, el cual es avalado por la Open Networking Fundation - ONF junto con los fabricantes que respaldan esta iniciativa. OpenFlow es la propuesta para estandarizar la comunicación entre el controlador con los equipos de reenvío de tráfico (Lara, Kolasani, & Ramamurthy, 2014), adicionalmente la ONF ha creado documentación que contribuye en la configuración de un switch OpenFlow y sus tablas de flujo.

Según (Braun & Menth, 2014) la arquitectura OpenFlow consta de tres bases, las cuales son: la red se constituye de dispositivos de reenvío de paquetes compatibles con OpenFlow, el plano de control lo conforman uno o varios controladores OpenFlow y por último se necita un canal seguro para conectar los equipos de reenvío con el plano de control.

En términos de seguridad se menciona que la especificación original de OpenFlow requería que el canal entre los controladores y los conmutadores estuviera protegido mediante TLS. Sin embargo las especificaciones posteriores hasta las versiones actuales hacen que TLS sea opcional, enviando todo el tráfico de comunicación entre el controlador y los equipos de conmutación en texto plano (Benton, Camp, & Small, 2013).

2.2.4 TABLAS DE FLUJO

Las tablas de flujo son el elemento principal del que están constituidos los dispositivos pertenecientes al plano de datos, según (Barona, Valdivieso, & Guamán, 2014) estas son numeradas secuencialmente y el proceso de revisión empieza desde la tabla 0.

En el trabajo de (Giraldo & Echeverry, 2018) se explica que si un switch no cuenta con una entrada en sus tablas de flujo (en redes tradicionales conocidas como tablas CAM), o el paquete recibido no coincide con ninguna de las entradas existentes, dicho paquete será enviado al controlador de la red con la finalidad que se indique como se debe conmutar ese tráfico y en caso de no encontrar una acción en el controlador se procede a eliminarlo.

Las tablas de flujo en el paradigma SDN tienen la misma limitante que las tablas CAM (TCAM) en las redes tradicionales, es decir, se encuentran limitadas por su tamaño. En este aspecto se han desarrollado varias propuestas para solventar este inconveniente (Banerjee & Kannan, 2014).

La idea de Tag-In-Tag es un enfoque que reemplaza las entradas de flujo por dos capas de etiquetas más simples y más cortas para permitir mayor una cantidad de entradas en las tablas de flujo e incluso reducir el consumo energético hasta en un 80% aproximadamente en comparación con un conmutador habilitado para SDN no optimizado (Banerjee & Kannan, 2014).

2.2.5 EJEMPLOS DE IMPLEMENTACIÓN

En relación al término de redes definidas por software no se ha formado una definición consistente con respecto a esta tecnología. Los académicos combinan los atributos de SDN con los de la virtualización de redes y los usuarios no entienden los beneficios en su totalidad. Por lo tanto, el establecimiento de SDN como tecnología ampliamente adoptada más allá de los laboratorios y las implementaciones asiladas requiere una brújula para navegar por la multitud de ideas y conceptos que conforman este paradigma en la actualidad (Jarschel, Zinner, Hoßfeld, Tran-Gia, & Kellerer, 2014).

Todo lo que se ha redactado hasta este momento se refiere a una descripción de SDN y sus principales diferencias con las redes de computadoras tradicionales, pero es vital mencionar casos de uso en entornos reales de este paradigma, tal como lo hace el trabajo de (Giraldo & Echeverry, 2018) , el cual sirve de sustento para la aplicación de SDN en la implementación de redes de computadoras y además fortalece el soporte bibliográfico de este trabajo.

Los ejemplos de aplicación de la tecnología SDN pueden también ser considerados desde el enfoque de los entornos o servicios en la red, en la investigación realizada por (Jarschel, Zinner, Hoßfeld, Tran-Gia, & Kellerer, 2014) se enfatiza en el comportamiento de las SDN en los procesos de enrutamiento, balanceo de carga, administración de la red, entre otros.

La combinación de SDN y la Virtualización de las funciones de red (Network Function Virtualization - NFV) están pasando la fase de euforia de su evolución y avanzan hacia una nueva fase en la que comienzan a surgir barreras y desafíos. En la evolución de esta tecnología se deriva el hecho de que los usuarios pasan de las preguntas básicas de comprensión de los beneficios potenciales de SDN y NFV hacia preguntas más profundas sobre cómo estas nuevas tecnologías pueden implementarse de manera realista en sus propias redes (Perrin & Hubbard, 2013)

En Ecuador, en la Escuela Politécnica Nacional se implementó un prototipo de red SDN, para lo cual se habilitaron dispositivos LINKSYS del modelo WRT54GL con el firmware de OpenWRT para obtener el soporte del protocolo OpenFlow, de esta manera se lograron enviar las peticiones al servidor del controlador de la red (Floodlight). (Chico, Mejía, & Bernal, 2013).

En el ambiente de red tradicional hay programas para simular los escenarios de pruebas, con fines de evaluación. De igual manera, para crear simulaciones de redes SDN existen varias aplicaciones que les permiten a los administradores de red conocer en detalle el funcionamiento de este paradigma. Los simuladores de SDN son muy variados y en ocasiones pueden integrarse con sistemas de virtualización para implementar servicios y darle un nivel superior de realismo a las pruebas o para compartir los recursos de cómputo.

2.3 SIMULADORES DE REDES

En ocasiones se encuentran implementaciones de redes que perjudican el rendimiento y la escalabilidad de la misma, para reducir estos inconvenientes resulta útil la utilización de un simulador que permita realizar las pruebas necesarias para determinar el mejor escenario y tecnología a implementar.

En internet se pueden encontrar varias herramientas que permiten crear simulaciones de redes, pero muchas de estas no se integran con aplicaciones de virtualización, lo que dificulta el desarrollo de pruebas donde se implementen sistemas y equipos de diversos fabricantes.

A continuación se detalla una lista de los simuladores de red más populares en el mercado como son: GNS3 (GNS3, 2018), Packet Tracer (Netacad, 2018), Mininet (Mininet, 2018) y ns-3 (De Oliveira, Shinoda, Schweitzer, & Prete, 2014) (ns-3, 2018). En el Cuadro 1 se ha realizado una comparativa en torno a las características de las herramientas de simulación mencionadas.

Cuadro 1. Comparativa entre simuladores de redes.

Simuladores / Características	GNS3	Packet Tracer	Mininet	ns-3
Software Libre	**Si**	**Si**	**Si**	**Si**
Open Source	**Si**	**No**	**Si**	**Si**
Versión para Windows	**Si**	**Si**	**No**	**Si**
Versión para Linux	**Si**	**Si**	**Si**	**Si**
Modo simulación	**Si**	**Si**	**Si**	**Si**
Modo emulación	**Si**	**No**	**No**	**Si**
Sistema IOS funcional	**Si**	**No**	**No**	**No**
Funcionalidad de wifi	**No**	**Si**	**Si**	**Si**
Escalabilidad	**Si**	**Si**	**Si**	**Si**
Compatibilidad con controladores reales	**Si**	**No**	**Si**	**No**
Soporte de interfaz gráfica de usuario	**No**	**Si**	**Si**	**No**
Modelamiento de tráfico	**No**	**Si**	**No**	**Si**
Integración con software de virtualización	**Si**	**No**	**No**	**No**
Conexión con entornos reales	**Si**	**No**	**No**	**No**

Fuente: Los Autores.

Tal como lo demuestran muchos trabajos acerca de SDN en todo el mundo, el simulador preferido por los investigadores es sin duda alguna Mininet, por la facilidad de implementación en máquinas virtuales que en ocasiones ya están configuradas para crear los entornos de redes SDN. Sin embargo, según (Cassongo, 2016), este simulador no proporciona un verdadero rendimiento y calidad que se asemeje a una red real.

Es importante saber que existe diferencia entre un simulador y un emulador de redes, el emulador es una herramienta que ejecuta una copia exacta del sistema operativo de red (generalmente consumen mayor cantidad de recursos del equipo en que se instala), mientras que un simulador está diseñado para tener una semejanza con un sistema operativo de red. Considerando estos aspectos resulta un desafío para estas herramientas el análisis de resultados de rendimiento obtenidos mediante la transmisión de datos (Cassongo, 2016).

Así mismo el autor antes citado considera irónico que GNS3 tenga en sus siglas la palabra “simulador”, ya que no solo se encarga de simular redes completas, sino que también es utilizado por muchos usuarios para emular los IOS de cisco y sistemas operativos de red de otros proveedores, otro aspecto diferenciador es la incorporación con máquinas virtuales reales.

2.4 HERRAMIENTAS DE VIRTUALIZACIÓN

La virtualización es el proceso de compartir recursos tales como: memoria RAM, procesador, almacenamiento, entre otros, para hacer posible la ejecución de un sistema o servicio en una máquina virtual. Estas máquinas virtuales pueden ejecutarse a la vez sobre un computador mediante el uso de un hipervisor, los cuales se encuentran de dos tipos: los nativos o de tipo 1 que se ejecutan directamente sobre el hardware y los de tipo 2 o alojados que necesitan de un sistema operativo base para ejecutarse (Andrade, 2016).

En el Cuadro 2 se muestran varios sistemas de virtualización que se pueden encontrar en internet y sus características principales. Vale mencionar que la comparativa realizada entre las herramientas de virtualización solo consta de hipervisores del tipo alojados, ya que los hipervisores nativos incluyen una capa adicional de virtualización si se instalan sobre un sistema operativo.

Entre las características más relevantes de la virtualización se pueden mencionar: provee un entorno favorable para pruebas, posibilita la recuperación inmediata de máquinas virtuales, brinda múltiples herramientas para simular entornos reales, entre otros. Estás y otras opciones están sujetas a cada solución de virtualización y sus diferentes versiones.

Cuadro 2. Comparativa entre sistemas de virtualización.

Hipervisores / Características	VirtualBox	VMware Workstation	KVM	Virtual PC
Tipo	**2**	**2**	**2**	**2**
Conocimiento requerido	**Bajo**	**Medio**	**Medio**	**Bajo**
Driver para S.O. virtualizado	**Si**	**Si**	**No**	**Si**
Software libre	**Si**	**Si**	**Si**	**Si**
Open Source	**Si**	**No**	**Si**	**No**
Soporte de red modo puente	**Si**	**Si**	**Si**	**Si**
Versión para Linux	**Si**	**Si**	**Si**	**No**
Versión para Windows	**Si**	**Si**	**No**	**Si**
Integración con simuladores	**Alta**	**Media**	**Baja**	**Media**
Instantáneas (Snapshots)	**Si**	**Si**	**Si**	**Si**
Ejecuta VMs en simultaneo	**Si**	**Si**	**Si**	**Si**

Fuente: Los Autores.

2.5 APLICACIONES DE MONITOREO DE REDES

Los autores (Delgado, Dulce, & Toledo, 2016) describen a breves rasgos como las redes de computadoras eran consideradas una tecnología de bajo impacto y un elemento al que se le daba poca importancia en las organizaciones, además el monitoreo se consideraba algo sencillo y que en caso de presentarse fallas en la red, la corrección no se presentaba como un punto crítico que necesitase solución inmediata.

Para desarrollar un plan de monitorización en una red es necesario entender el funcionamiento de las mismas y como se gestionan, también es menester tener en cuenta que el uso de políticas y manuales de procedimientos son de ayuda para los administradores, tal como indican (De Bruijn & Ten Heuvelhof, 2018) en su libro. Además los sistemas, software y métodos utilizados para la gestión de las redes deben ser analizados y aplicados según lo demande el escenario de implementación (Washington, DC: U.S. Patente nº 9,077,611, 2015).

En el cuadro 3 se realiza la comparativa entre varios de los mejores sistemas de monitoreo de software libre que se pueden encontrar en el mercado, para este proyecto no se consideraron herramientas privativas por el corto periodo de ejecución del mismo.

Cuadro 3. Comparativa entre las aplicaciones de monitoreo de redes

Características \ Aplicaciones	Smokeping	Cacti	Zabbix	Nagios
Administración web	**Si**	**Si**	**Si**	**Si**
Soporte	**No**	**No**	**Comercial**	**Comercial**
Software Libre	**Si**	**Si**	**Si**	**Si**
Open Source	**No**	**No**	**No**	**Si**
Habilitar HTTPS	**No**	**No**	**Si**	**Si**
Complejidad de despliegue	**Media**	**Media**	**Baja**	**Alta**
Versión para Linux	**Si**	**Si**	**Si**	**Si**
Versión para Windows	**No**	**Si**	**No**	**Si**
Idiomas inglés y español	**No**	**No**	**Si**	**Si**

Fuente: Los Autores.

Las herramientas de monitoreo de red en su mayoría utilizan agentes en todos los nodos que desean monitorear, por esta razón se afirma que Smokeping es una solución especialmente buena, ya que no requiere que se instalen agentes en la red (Estados Unidos Patente nº 11/796,092., 2007).

(Vera, 2016) En su investigación indica varios parámetros que contribuyen al mejoramiento de la infraestructura de red de la ESPAM MFL, basándose en el levantamiento de la información concerniente al volumen de tráfico que soporta la red. Este trabajo demuestra en parte la importancia de implementar una herramienta de monitoreo de red para brindar soporte a eventualidades y prevenir posibles fallos en la infraestructura.

Los trabajos de (Vera, 2016) y (Vidal, 2016) coinciden en varias de las causas que provocan los inconvenientes al acceder a los servicios implementados dentro de la red de la ESPAM MFL, así mismo plantean como una de las medidas para solucionar dichos fallos la configuración de políticas de calidad de servicio en la red.

CAPÍTULO III. DESARROLLO METODOLÓGICO

3.1 METODOLOGÍA

En el presente trabajo se aplicó el método bibliográfico para la recolección de información sobre los paradigmas de redes que se estudiaron. De igual manera se utilizó el método experimental para la obtención de los resultados mediante la implementación de los escenarios de cada modelo de red y la posterior comparativa de rendimiento.

La parte experimental de este trabajo se sustentó en entornos simulados, en los que se definieron los parámetros para realizar el análisis comparativo entre los paradigmas antes mencionados. Además basándose en dichos parámetros, se escogieron las aplicaciones necesarias para crear las simulaciones.

Para una mejor comprensión del desarrollo de este proyecto investigativo, a continuación se detallan los pasos que se realizaron en este trabajo, en base a los objetivos planteados:

- Definición del esquema de trabajo:
    - Establecer los parámetros y métricas para realizar las pruebas.
    - Búsqueda de información de las herramientas a utilizar, donde se aplicó el método bibliográfico.
    - Levantamiento de información del entorno de la universidad para diseñar los escenarios según cada paradigma.
- Obtención de resultados de la simulación:
    - Instalación de las herramientas seleccionadas.
    - Configuración de los entornos de simulación.
    - Ejecución de las simulaciones.
- Determinación de aplicabilidad en el entorno analizado:
    - Tabulación de datos obtenidos en las pruebas.
    - Comparación entre los resultados obtenidos de cada uno de los paradigmas analizados.

En la ejecución de las pruebas primero se utilizaron varias herramientas (ApacheJMeter, NetFlow generator, Slowloris, entre otras), las cuales enviaban solicitudes de conexión a los servicios pero ninguna pudo generar la sobrecarga deseada en la red para obtener los resultados, por esta razón se realizaron consultas mediante el protocolo ICMP hacia los servicios desde todos los host virtuales de la red.

Las pruebas consistieron en generar peticiones desde un PC de cada una de las redes LAN hacia los servicios instalados en la zona desmilitarizada (DMZ) por un periodo de tiempo determinado (3 horas), mientras que la aplicación de monitoreo de red estuvo analizando el tráfico y capturando los parámetros con sus respectivas métricas previamente establecidas. Vale mencionar que además de los servicios implementados de manera local se realizaron consultas al webmail y página principal de la ESPAM MFL (que están fuera del campus) para observar la variación de resultados en las consultas realizadas hacia el exterior de la red.

La idea de utilizar ICMP mediante el comando ping para realizar las pruebas se llevó a cabo en base a la simplicidad del proceso, las estadísticas que brindan las consultas de ping y el hecho de ejecutar las consultas desde los diferentes segmentos de LAN que fueron simulados, además para evitar agregar más equipos desde VirtualBox los cuales generan mayor consumo de recursos.

El protocolo simple de administración de red (Simple Network Management Protocol – SNMP) fue considerado en principio para realizar las pruebas, pero se determinó que muchos de los parámetros que brinda este protocolo no eran requeridos y además aumentaba la complejidad de la instalación de los escenarios, sin brindar beneficios tan significativos.

La obtención de datos se la realizó en base a la observación de los parámetros capturados por el sistema de monitoreo de red (latencia, jitter y pérdida de paquetes), de los cuales se obtuvo la media aritmética para su presentación. Luego dichos datos fueron tabulados y analizados para ratificar o desmentir la idea a defender de esta investigación.

Así mismo, para determinar la aplicabilidad de SDN en el entorno de estudio, se tomó en cuenta los resultados de la simulación, y se realizó un breve análisis de la necesidad de equipos adicionales para la implementación.

3.2 ENTORNOS DE SIMULACIÓN

Para la elaboración de esta investigación se desarrollaron dos escenarios: uno con el modelo de red de SDN y el otro bajo el modelo de red tradicional, los diseños topológicos de ambos esquemas fueron muy similares en cuanto a la estructura física y lógica, las diferencias que presentaron estuvieron sujetas al modelo de implementación y configuración de los equipos de cada paradigma.

Las herramientas que se utilizaron en esta investigación se pueden categorizar en 3 áreas: simulador de red, sistemas de virtualización y aplicaciones de monitoreo de red, además de manera complementaria se instalaron servicios como: web, DNS y Moodle para mejorar la simulación del entorno de estudio.

3.2.1 SELECCIÓN DEL SIMULADOR DE RED

La selección de la herramienta para realizar la simulación de los entornos de red se sustentó en que la implementación de los escenarios de estudio sean idénticos o muy similares a la arquitectura real implementada en el sector 8 de la ESPAM MFL. Por este motivo se utilizó GNS3 como herramienta de simulación, ya que permite la integración de varias marcas y modelos de dispositivos de red cuya característica facilita la creación de una infraestructura heterogénea tal y como se contempla en la red existente en el sector 8.

Finalmente se justifica el uso de GNS3 sobre Mininet porque este último es un simulador que al ser implementado en una máquina virtual hace uso de otra capa de drivers. Packet Tracer no está considerado en este proyecto porque no permite la creación de redes SDN y además no se integra con máquinas virtuales, otra herramienta que está considerada entre las mejores para entornos SDN es Estinet (Wang, Chou, & Yang, 2013) pero al ser comercial existe poca documentación sobre su uso y la curva de aprendizaje es elevada.

3.2.2 SELECCIÓN DE LOS SISTEMAS DE VIRTUALIZACIÓN

Los sistemas de virtualización utilizados en la implementación de los laboratorios fueron elegidos en base a la capacidad de integración con el simulador de red (GNS3), además solo fueron consideradas las aplicaciones de virtualización del tipo alojados (instalados en un sistema operativo) ya que para la ejecución de este proyecto no eran convenientes sistemas nativos sobre los cuales al implementar las herramientas se genera otra capa de drivers.

VMware Workstation es un hipervisor que tiene la capacidad de integrar máquinas virtuales con GNS3, además puede realizar la función de servidor para gestionar imágenes de sistemas operativos de red así como también aportar con los recursos que se le asignen a la máquina virtual en la que es implementado (Mohtasin, y otros, 2016), En este proyecto se lo utilizó para brindar recursos de hardware a la herramienta de simulación de redes.

En este proyecto se utiliza VirtualBox para la creación de los servicios que brinda la universidad (aula virtual, sitio web, DNS y telefonía IP), ya que este hipervisor es una solución de software libre que se integra de manera muy sencilla al simulador de red.

3.2.3 SELECCIÓN DE LA APLICACIÓN DE MONITOREO

La selección de la herramienta de monitoreo estuvo basada en los parámetros que afectan el rendimiento de una red, según la investigación de (Sharma & Gandole, 2013) el ancho de banda es uno de los elementos que inciden en la velocidad de una red, de igual manera brindan relevancia a la latencia y consideran la perdida de paquetes como el factor de mayor influencia.

Los autores antes citados sustentan que Smokeping es una herramienta ideal para medir el rendimiento de las redes de datos, por motivo que se encarga de graficar los niveles de latencia, perdida de paquetes y la fluctuación de fase (jitter) que se logren identificar en los equipos de una arquitectura. Además, tiene la facultad de integrarse con otros complementos que le permiten incrementar sus funciones de monitoreo.

Existen muchas herramientas de monitoreo de redes, unas enfocadas a servicios como Zabbix, Observium, Nagios, PRTG, pero Smokeping es una aplicación simple de instalar, administrar y de bajo consumo de recursos que además se ajustó a las necesidades de este trabajo. Por estos motivos se la eligió para las pruebas.

3.2.4 ESCENARIO 1 – RED TRADICIONAL

Este laboratorio se implementó bajo el modelo jerárquico de tres capas (núcleo, distribución y acceso) propuesto por Cisco, las configuraciones referentes a la comunicación entre los dispositivos de la red se realizaron buscando el mayor grado de similitud posible con la red del sector 8 de la ESPAM MFL.

La infraestructura implementada bajo el modelo de red tradicional se elaboró de la siguiente manera: se utilizó un appliance de la marca mikrotik que es soportado por GNS3 para simular el equipo del proveedor de internet, el cual se conecta a un router similar que cumple la función de conectar las redes LAN de la institución con la WAN.

La red core del sector 8 está conformada por switches de la marca TP-LINK y routers mikrotik y TP-LINK, para simular los switches TP-LINK se utilizó un switch básico que facilita el simulador con características de VLAN, interfaces 10/100, entre otras, mientras que para los routers de dicha marca se usó un appliance de openWRT teniendo en cuenta que los modelos de equipos que tiene la institución fuese posible realizar el cambio de firmware.

En lo concerniente a las redes LAN de los edificios que conforman el sector 8 (posgrado, computación, hotel y biblioteca), estas se encuentran estructuradas con su respectivo router (en ocasiones 2 o 3, según la distribución en cada edificio), switches de acceso y varios puntos de acceso inalámbrico (estos últimos no se implementaron en la simulación ya que la herramienta GNS3 no brinda esa característica).

Por último, se implementaron los servicios de la DMZ a los cuales se hace referencia en el apartado 3.2., para realizar las pruebas que se ejecutaron de manera local.

3.2.5 ESCENARIO 2 – SDN

La red definida por software debería presentar diferencias con la red tradicional en el modelo de implementación, mientras que se aplica el modelo jerárquico de 3 capas de Cisco para la red tradicional, en SDN uno de los modelos más comunes es el diseño de *leaves and spine* (hojas y columna vertebral [tronco]). Sin embargo, para hacer una comparación más objetiva, se ha tratado de no cambiar demasiado el diseño…

El modelo antes mencionado consiste en implementar un controlador principal el cual va a estar conectado a todos los equipos de forwarding, este tipo de conexión generalmente varía según la dimensión de la red y la distancia a la que están conectados los equipos, pero para este ejemplo en particular se mantendrá hasta cierto punto el diseño de la red convencional para que la comparativa de rendimiento entre ambos paradigmas sea más equitativa.

En tanto a los equipos, sistemas y servicios que complementan la infraestructura fueron los mismos que se utilizaron en el enfoque de red tradicional (teniendo en cuenta la disminución en el uso de los dispositivos de red), al igual que los procesos a realizar para obtener los resultados del rendimiento del paradigma de redes definida por software.

Los elementos que se agregan en la red SDN son los controladores OpenDayLight y Floodlight, así como también la aplicación OpenFlow Manager que se encarga de gestionar las tablas de flujo de los dispositivos de reenvío de tráfico, Según (Khattak, Awais, & Iqbal, 2014) OpenDayLight es un proyecto de código abierto soportado por IBM, Cisco, Juniper, VMware y otros proveedores de redes importantes. Esta solución es una plataforma de controlador SDN implementada en java y puede instalarse en cualquier sistema operativo que soporte java.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 RESULTADOS

La obtención de los resultados está orientada a brindar respuesta a los objetivos plantados en el presente proyecto, para el cumplimiento de cada objetivo se realizaron varias actividades las cuales se pueden categorizar en 3: implementación de las simulaciones de los paradigmas de redes, evaluación del desempeño de dichos paradigmas mediante el software de monitoreo y evaluación de los resultados obtenidos de la herramienta de monitoreo.

4.1.1 ESQUEMAS DE TRABAJO

Para realizar el análisis comparativo entre las SDN y las redes convencionales basándose en la red del sector 8 de la ESPAM MFL, el primer paso consistió en diseñar una topología de red tan similar como fuese posible a la infraestructura que se planteó como objeto de estudio, tal como se muestra en la Figura 2.

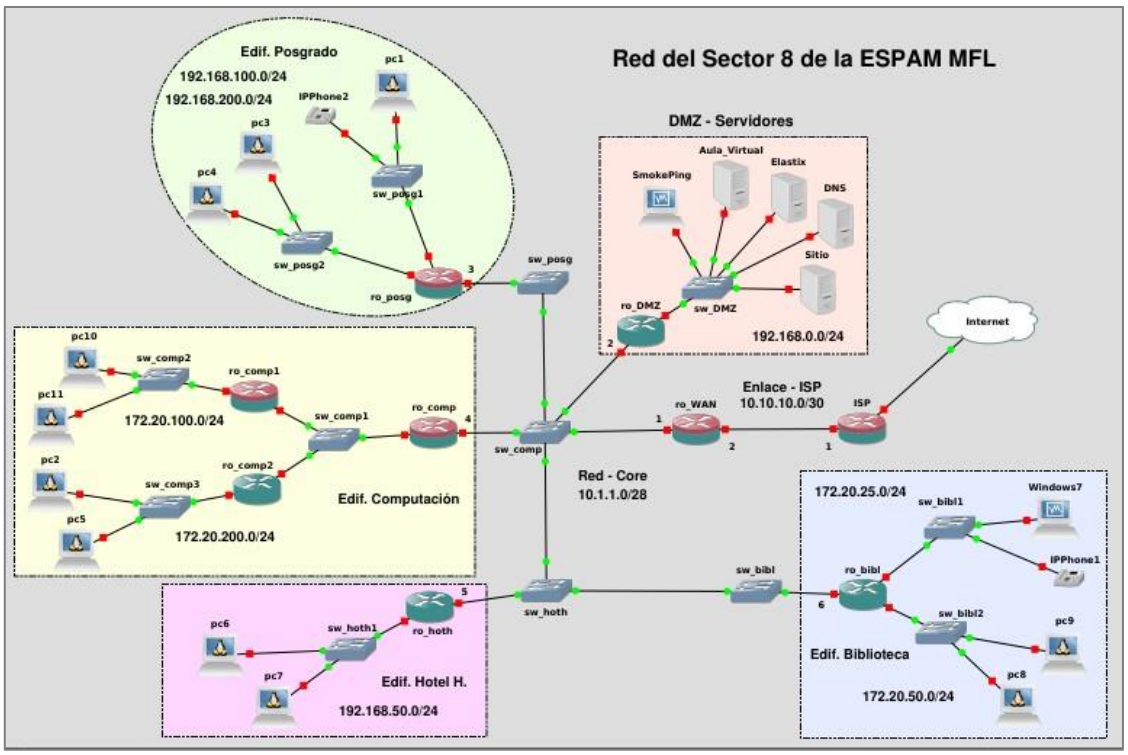

Figura 2. Diseño de la topología de la red actual del sector 8 de la ESPAM MFL

Fuente: Los Autores

En la Figura 3 se muestra la simulación de una propuesta de red bajo el paradigma de SDN, en la misma se pueden observar los cambios planteados para este modelo y sus diferencias con el modelo anterior. Es importante mencionar que en este modelo los equipos de WAN y el ISP son routers comunes, mientras que los demás son dispositivos de reenvío de paquetes.

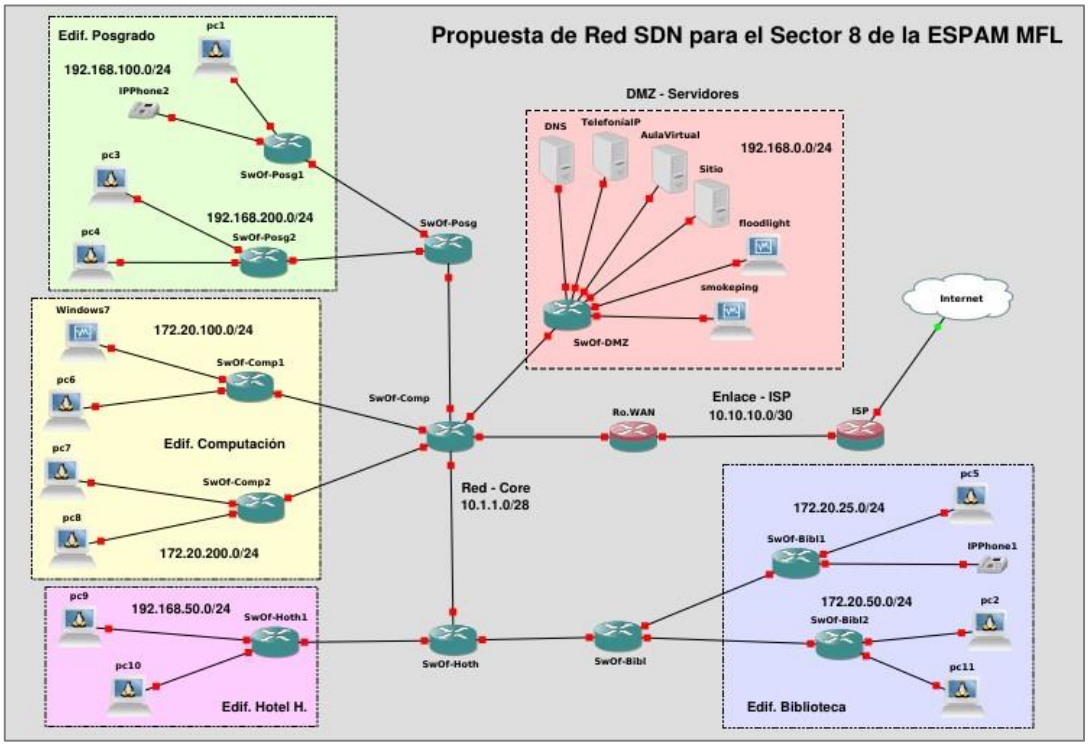

Figura 3. Diseño de la topología de red SDN propuesta para el sector 8 de la ESPAM MFL
Fuente: Los Autores

4.1.2 TABULACIÓN DE RESULTADOS

Para obtener los resultados del análisis comparativo entre el rendimiento de un entorno de red tradicional y un escenario de red creado bajo el paradigma de SDN, se realizaron consultas a través del protocolo ICMP a dos de los servicios locales en la red simulada y dos servicios reales de la ESPAM MFL.

Los equipos de los cuales se obtuvieron los resultados del rendimiento fueron una PC virtual por cada red LAN simulada (7 en total), además las gráficas obtenidas del sistema de monitoreo pueden ser consultadas en el anexo 1 y 2 de este documento. En el Cuadro 4 se registraron los valores obtenidos por Smokeping al realizar las pruebas, Así mismo se resaltan los mejores valores (menores) de cada prueba realizada.

Cuadro 4. Registro de latencia y jitter, obtenido del sistema de monitoreo en ambos paradigmas de red.

Equipos / Paradigmas	PC1	PC2	PC3	PC4	PC5	PC6	PC7
SDN MOODLE LOCAL							
Max. Latencia	5,80	6,50	5,30	4,80	8,30	7,20	8,90
Min. Latencia	4,30	4,10	3,40	3,60	4,70	5,50	5,60
Media	5,05	5,30	4,35	**4,20**	6,50	6,35	7,25
Fluctuación	1,50	2,40	1,90	**1,20**	3,60	1,70	3,30
SDN WEB LOCAL							
Max. Latencia	6,30	9,00	5,00	4,80	7,10	9,90	8,10
Min. Latencia	4,40	5,50	3,50	3,50	4,80	5,70	5,30
Media	5,35	7,25	4,25	**4,15**	5,95	7,80	6,70
Fluctuación	1,90	3,50	1,50	**1,30**	2,30	4,20	2,80
SDN WEB ESPAM MFL							
Max. Latencia	6,60	5,60	4,60	5,30	5,60	5,20	5,40
Min. Latencia	3,90	4,00	3,40	3,40	4,00	3,90	3,80
Media	5,25	4,80	**4,00**	4,35	4,80	4,55	4,60
Fluctuación	2,70	1,60	**1,20**	1,90	1,60	1,30	1,60
SDN MAIL ESPAM MFL							
Max. Latencia	6,00	6,60	7,50	6,90	7,30	6,60	6,30
Min. Latencia	4,00	4,30	4,40	4,00	4,60	4,40	4,00
Media	**5,00**	5,45	5,95	5,45	5,95	5,50	5,15
Fluctuación	2,00	2,30	3,10	2,90	2,70	**2,20**	2,30
TRADICIONAL MOODLE LOCAL							
Max. Latencia	6,40	7,20	10,90	10,00	6,90	6,30	7,90
Min. Latencia	4,20	4,40	7,40	5,40	4,10	3,90	4,40
Media	5,30	5,80	9,15	7,70	5,50	**5,10**	6,15
Fluctuación	**2,20**	2,80	3,50	4,60	2,80	2,40	3,50
TRADICIONAL WEB LOCAL							
Max. Latencia	6,40	6,40	10,50	11,10	6,90	7,90	6,60
Min. Latencia	4,10	4,50	6,20	6,80	3,90	4,30	4,50
Media	**5,25**	5,45	8,35	8,95	5,40	6,10	5,55
Fluctuación	2,30	**1,90**	4,30	4,30	3,00	3,60	2,10
TRADICIONAL WEB ESPAM MFL							
Max. Latencia	6,20	7,10	6,70	7,30	4,90	5,70	6,30
Min. Latencia	4,20	4,50	4,70	5,00	3,40	4,10	4,20
Media	5,20	5,80	5,70	6,15	**4,15**	4,90	5,25
Fluctuación	2,00	2,60	2,00	2,30	**1,50**	1,60	2,10
TRADICIONAL MAIL ESPAM MFL							
Max. Latencia	6,30	6,00	7,80	9,20	6,50	7,60	6,20
Min. Latencia	3,90	3,80	5,30	5,90	3,70	5,20	4,10
Media	5,10	**4,90**	6,55	7,55	5,10	6,40	5,15
Fluctuación	2,40	2,20	2,50	3,30	2,80	2,40	**2,10**

Fuente: Los Autores

En el Cuadro 5 se registran los datos referentes a la latencia obtenidos de realizar ping desde las PC virtuales instaladas en cada una de las redes LAN simuladas hacia todos los servicios que se ejecutaron las consultas, en este cuadro al igual que en el anterior se encuentran resaltados los mejores valores (menores) de cada prueba.

Cuadro 5. Registro de la latencia obtenida en cada PC, mientras se ejecutaba la consulta a los diferentes servicios.

Equipos / Paradigmas	PC1	PC2	PC3	PC4	PC5	PC6	PC7
SDN MOODLE LOCAL							
Media	7,09	7,34	5,79	**5,36**	7,40	7,97	7,83
SDN WEB LOCAL							
Media	9,23	9,20	**7,38**	7,44	9,52	10,80	9,41
SDN WEB ESPAM MFL							
Media	230,72	230,44	**230,15**	231,30	230,90	231,02	230,67
SDN MAIL ESPAM MFL							
Media	202,98	202,90	**202,38**	202,73	202,87	203,22	202,39
TRADICIONAL MOODLE LOCAL							
Media	7,58	7,33	9,35	9,18	**6,35**	6,93	6,77
TRADICIONAL WEB LOCAL							
Media	7,44	**7,16**	10,34	10,32	7,31	7,20	7,64
TRADICIONAL WEB ESPAM MFL							
Media	266,82	266,47	270,23	270,66	268,13	**266,34**	266,72
TRADICIONAL MAIL ESPAM MFL							
Media	181,52	183,88	184,29	185,13	181,00	183,66	183,36

Fuente: Los Autores

A continuación se presenta el análisis de los datos obtenidos de la herramienta de monitoreo, los cuales están clasificados por cada servicio al que se ejecutaron las consultas.

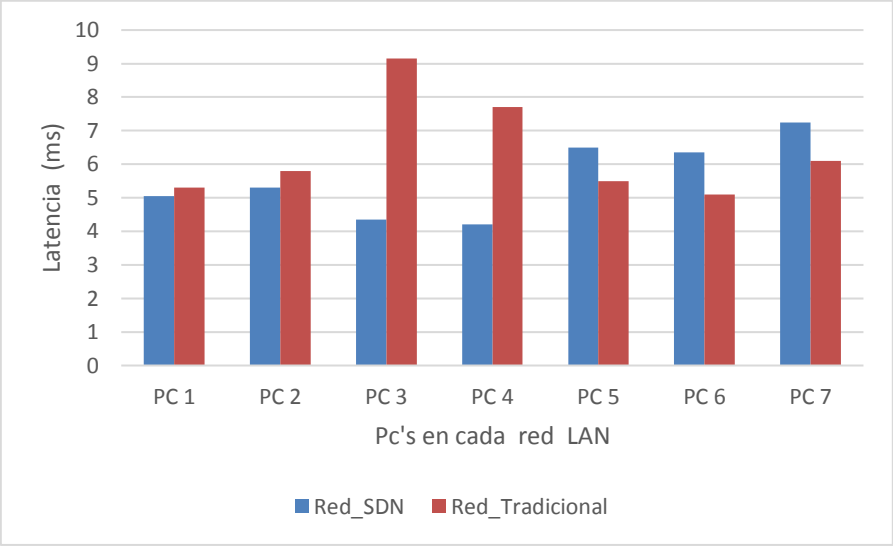

Figura 4. Comparación de latencia hacia el aula virtual, entre paradigma de redes

Fuente: Los Autores

En la Figura 4 se muestran los valores correspondientes a la media de la latencia generada al realizar consultas ICMP al servicio de aula virtual local, los equipos con más saltos de red hacia el sistema de monitoreo muestran latencia elevada, esta idea aplica para ambos paradigmas con picos de 9,15 ms en el entorno de red convencional y 4,2 ms en SDN.

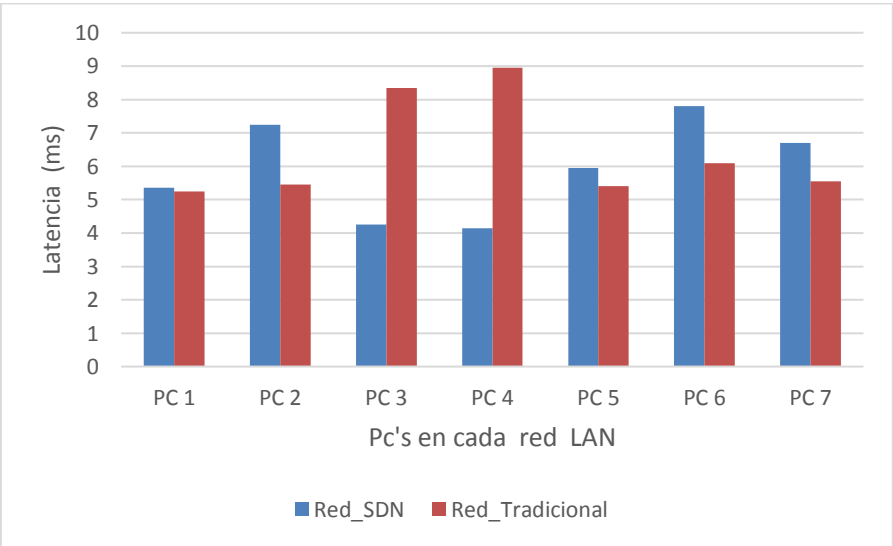

Figura 5. Comparación de latencia hacia el sitio web local, entre paradigma de redes

Fuente: Los Autores

La Figura 5 muestra los valores correspondientes a la media de la latencia generada al realizar consultas ICMP al sitio web instalado de manera local, al igual que en caso anterior los puntos más altos de latencia se encuentran en los equipos con más saltos hacia el sistema de monitoreo y los picos están en la red tradicional con 8,95 ms y el menor en SDN con 4,15 ms.

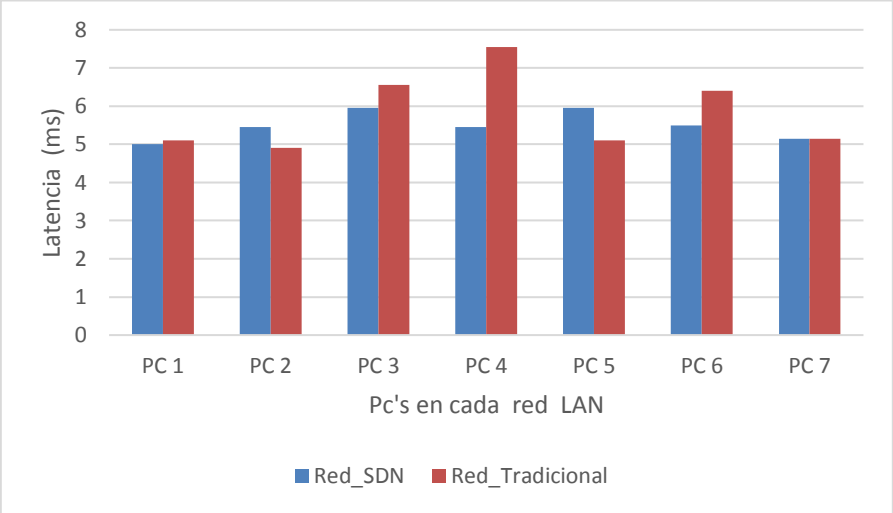

Figura 6. Comparación de latencia hacia el webmail de la ESPAM MFL, entre paradigma de redes

Fuente: Los Autores

En la Figura 6 se muestran los valores de la media de la latencia generada al realizar consultas ICMP al servidor de webmail de la ESPAM MFL, además se puede constatar menor variabilidad en SDN cuando se realizan consultas fuera de la red y coincidencia de ambos paradigmas en la PC 7 con 5,15 ms.

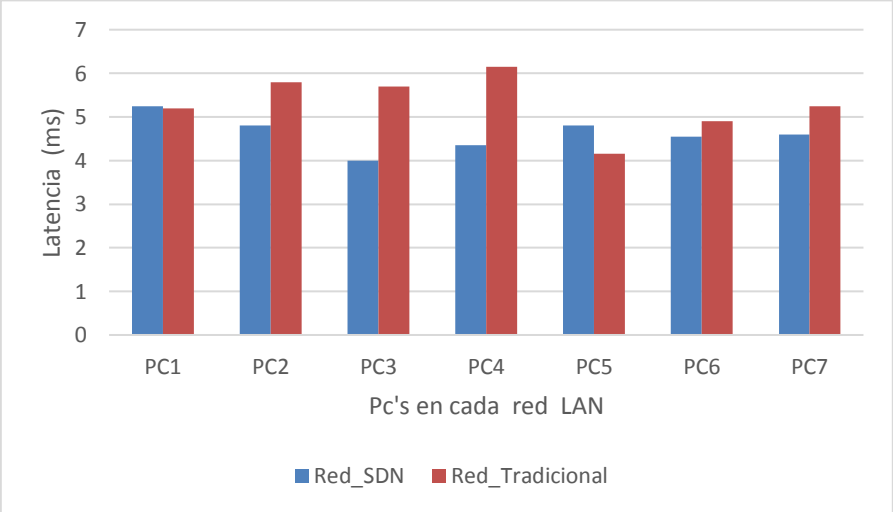

Figura 7. Comparación de latencia hacia el sitio web de la ESPAM MFL, entre paradigma de redes

Fuente: Los Autores

En la Figura 7 se muestra al igual que el caso anterior mayor estabilidad en SDN y solo la PC 5 de la red tradicional está por debajo de SDN, el pico de latencia en esta prueba lo tiene la red tradicional con 6,15 ms y el menor valor es de la PC 3 de SDN con 4 ms.

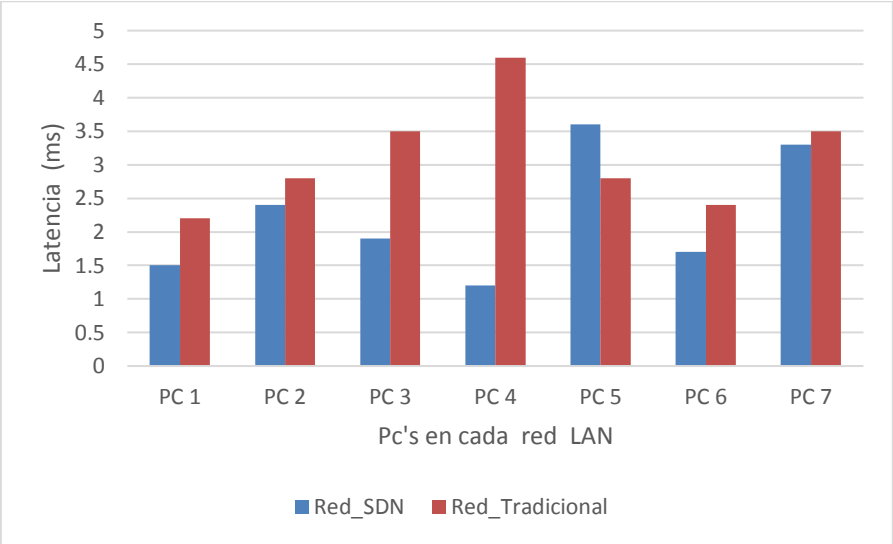

Figura 8. Comparación de jitter hacia el aula virtual, entre paradigma de redes
Fuente: Los Autores

La Figura 8 muestra los valores correspondientes al jitter encontrado en las PC de cada red LAN simulada, para este caso todos los valores de la red SDN son menores a la red tradicional a excepción de la PC 5, el pico de menor valor se da en SDN con 1,2 ms y el valor más alto está en la red tradicional con 4,6 ms.

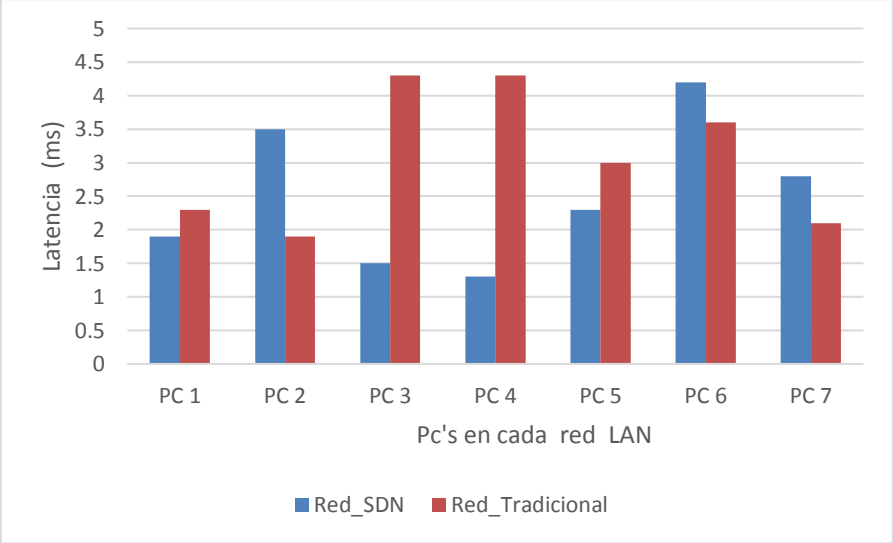

Figura 9. Comparación de jitter hacia el sitio web local, entre paradigma de redes
Fuente: Los Autores

La Figura 9 muestra los valores del jitter encontrados al realizar consultas ICMP al sitio web local, además SDN continúa mostrando mayor cantidad de valores inferiores que la red tradicional, teniendo como pico las PC 4 y 5 de este paradigma con 4,3 ms y el menor valor corresponde a SDN con 2,3 ms.

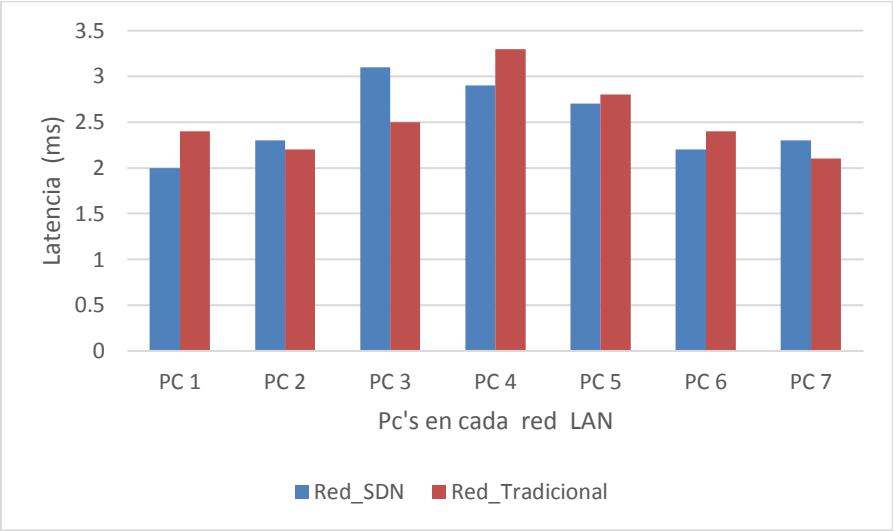

Figura 10. Comparación de jitter hacia el servidor de webmail de la ESPAM MFL, entre paradigma de redes
Fuente: Los Autores

La Figura 10 muestra los valores del jitter encontrados al realizar consultas ICMP al webmail de la ESPAM MFL, los valores obtenidos de esta prueba son los más equivalentes entre ambos paradigmas y a su vez los más bajos, el pico mayor es en la red tradicional con 3,3 ms y el menor en SDN con 2 ms.

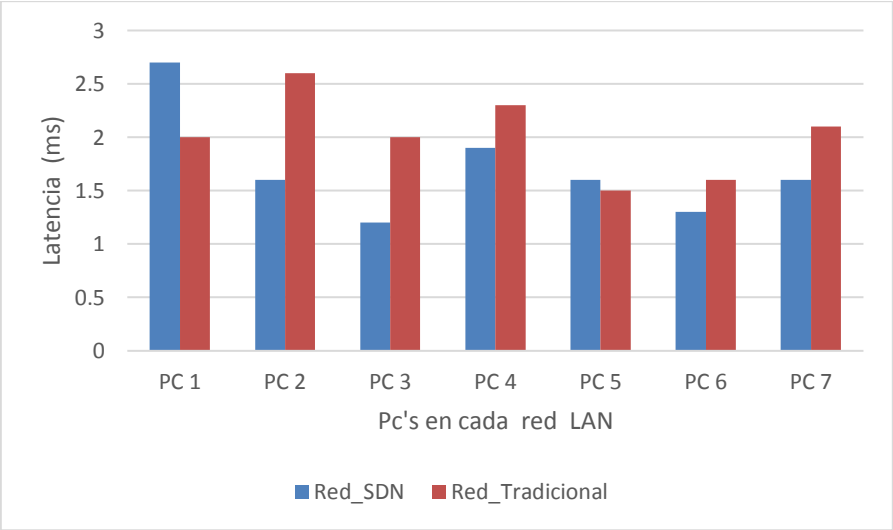

Figura 11. Comparación de jitter hacia el sitio web de la ESPAM MFL, entre paradigma de redes
Fuente: Los Autores

En la Figura 11 se muestran los valores correspondientes al jitter encontrado en los equipos de las redes LAN que ejecutaron las pruebas, este es el único caso en que el pico de mayor valor se encuentra en SDN con un valor de 2,7 ms, de igual manera el pico de menor valor también se encuentra en SDN en la PC 3 con un valor de 1,2 ms.

En base a los resultados obtenidos se logró constatar que los paradigmas de redes analizados tienen en común ciertos comportamientos, por ejemplo: En la red tradicional se obtuvieron los mayores niveles de latencia en los equipos que estaban separados del sistema de monitoreo por mayor cantidad de routers, de igual manera en SDN la latencia fue mayor en las equipos que estaban a mayor distancia de la aplicación de monitoreo.

4.1.3 FACTIBILIDAD DE APLICACIÓN

En consecuencia de los resultados obtenidos en puntos anteriores se puede determinar que es factible implementar el paradigma de redes SDN en el sector 8 de la ESPAM MFL, atendiendo los aspectos de diseño y configuración que se proponen en este trabajo.

Para mencionar los aspectos que favorecen la aplicación de una red SDN para el Sector 8 de la ESPAM MFL se puede considerar la importante disminución de equipos utilizados, teniendo en la red convencional un total de 22 equipos entre switches y routers, mientras que la topología con el modelo SDN cuenta con apenas 14 equipos entre dispositivos de reenvió de tráfico y routers (Cuadro 6), este aspecto no solo favorece a la administración y operatividad de la red sino también al ahorro de recursos de la institución.

Cuadro 6. Requerimiento de equipos de red y aplicaciones en cada paradigma.

Equipos / Paradigma	Routers	Switches	Equipos de reenvío	Servidores
Red Tradicional	**9**	**13**	**0**	**5**
Red SDN	**2**	**0**	**12**	**6**

Fuente: Los Autores

Cabe indicar, que los Switches considerados en el Cuadro 6, se pueden reutilizar como Equipos de reenvío en SDN. Esto implicaría que no se necesita adquirir este último tipo de equipos de forma adicional.

El uso del controlador de la red en complemento con una aplicación para la gestión de las tablas de flujo que se ejecutan en los dispositivos de reenvío favorece el control y configuración centralizado de la red, además de proveer altos niveles de programabilidad en la misma. Como respaldo a la factibilidad de implementación de SDN en el escenario de redes estudiado, a continuación se presenta una gráfica comparativa entre ambos paradigmas de red.

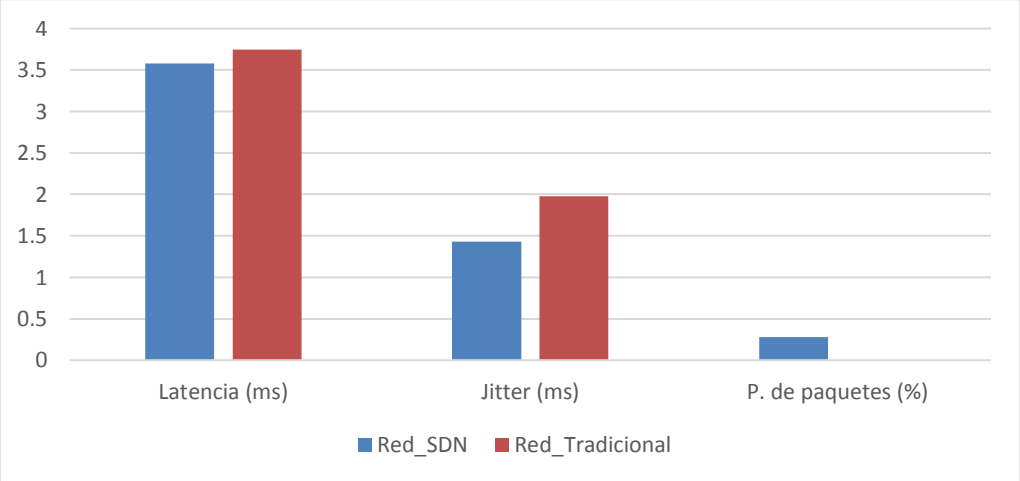

Figura 12. Promedios de latencia, jitter y pérdida de paquetes en ambos paradigmas de red.
Fuente: Los Autores

En la Figura 12 se puede observar como el paradigma de red SDN presenta ventajas en cuanto al promedio calculado entre los mejores valores (menores) correspondientes a la latencia y al jitter que se obtuvieron de las pruebas realizadas en el escenario de estudio, así mismo, se observa una pérdida de paquetes en SDN del 0,28% el cual se dio cuando los dispositivos de reenvío de datos aún desconocían las rutas de los datos definidas en las tablas de flujo.

Como acción complementaria a una posible implantación de SDN en la red del sector 8 de la ESPAM MFL se debe establecer como mandatorio la capacitación al personal de TI para garantizar se lleven a cabo las actividades correspondientes al proceso de implementación y administración de la red bajo el paradigma antes mencionado.

Los datos que se encuentran en el Cuadro 4 y Cuadro 5 respectivamente están detallados en el Anexo 1 y Anexo 2, los cuales contienen las gráficas que se obtuvieron del sistema de monitoreo Smokeping, así como también las estadísticas de los resultados de ping ejecutados hacia los servicios.

4.2 DISCUSIÓN

Las redes definidas por software se han convertido en una tecnología de red eficiente con la capacidad de adaptarse a la naturaleza cambiante de las futuras funciones de red y las aplicaciones inteligentes tal como sustentan (Sezer, y otros, 2013) en su investigación, esta capacidad de adopción está acompañada de reducción de costes en la infraestructura y administración simplificada, este criterio es compartido por los desarrolladores de este trabajo.

Una de las principales ventajas de las redes SDN que se mencionan en este trabajo son sus bases en protocolos y estándares abiertos, criterio que es compartido por autores como (Rojas, y otros, 2018) y (Sezer, y otros, 2013). De igual manera este beneficio conlleva ciertos inconvenientes como por ejemplo: la incompatibilidad existente entre diversos protocolos SDN, las características de funcionalidades exclusivas definidas por los proveedores de soluciones de redes, lo que conlleva a estar sujetos a marcas al pensar en la escalabilidad de la red para obtener mayores índices de productividad en la infraestructura.

Como aporte al párrafo anterior se menciona que el nivel de complejidad que conlleva la migración de una infraestructura de red tradicional hacia el paradigma SDN puede resultar bastante alto, ya que en primera instancia siempre se está sujeto a la tecnología existente y la compatibilidad que pueda ofrecer con protocolos de SDN. Por otra parte está la opción de contar equipos compatibles con firmwares libres que faciliten la migración.

Existe una fuerte tendencia a utilizar la Mininet para crear las topologías basadas en el modelo SDN, pero desde el punto de vista de los autores de este trabajo dicha herramienta no proporciona las características en cuanto a desempeño y calidad de una red real, idea que es compartida con el trabajo de (Cassongo, 2016), el cual argumenta que la funcionalidad de esta aplicación está limitada por el CPU y la cantidad de memoria que cuente el equipo.

La elección de una herramienta que permita simular redes definidas por software resulta en ciertas ocasiones algo controversial por motivo que cada investigador tiene sus preferencias, en este aspecto resulta muy interesante la integración que realizan (Laponina & Sizov, 2017) en su trabajo, el cual consiste en analizar las posibilidades de migrar redes tradicionales a SDN utilizando como herramienta de simulación Mininet que a su vez se integra con una red convencional implementada en GNS3.

Existen varias investigaciones que sustentan la aplicación de las SDN, aunque en términos generales enfocan su aplicación en el contexto de los centros de datos o en redes WAN. Según (Al-Najjar, Layeghy, & Portmann, 2016) este paradigma también resulta aplicable y efectivo para la implementación de un balanceador de carga. Además, los autores de este trabajo sostienen que la aplicación del paradigma SDN en entornos de redes LAN pueden resultar beneficioso sustentado su uso con los estudios necesarios.

Esta investigación se puede considerar como un aporte a la aplicabilidad de las SDN en entornos de redes LAN y particularmente en escenarios que se brinden servicios relacionados con instituciones de educación superior, esta idea también es respaldada por (Duarte & Lobo, 2015) en su investigación sobre la factibilidad de aplicación de una red SDWLAN (Software Defined Wireless Local Area Network) en un campus universitario.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Este trabajo ha permitido realizar la comparación entre los paradigmas de una SDN y una red tradicional, para el caso de una red de datos de una universidad.
- El paradigma de SDN plantea un mejoramiento en el esquema de red analizado desde su diseño, al reducir la cantidad de equipos de red necesarios para el funcionamiento de la red utilizada en este estudio.
- Los resultados del rendimiento de ambos paradigmas muestran como la red definida por software presenta ligeramente mejor rendimiento que la red tradicional, para el caso del entorno y topologías analizados, así mismo en el caso de SDN se presentaron pérdidas de paquetes en dos pruebas por el desconocimiento de la ruta de destino en primera instancia.
- En la red tradicional se obtuvieron los mayores niveles de latencia en los equipos que estaban separados del sistema de monitoreo por mayor cantidad de routers, de igual manera en SDN la latencia fue mayor en los equipos que estaban a mayor distancia de la aplicación de monitoreo pero separados por dispositivos de reenvió de datos.
- Este trabajo fomenta ligeramente la aplicación de redes SDN en entornos de LAN y particularmente en entornos de instituciones de educación superior
- La administración de la red SDN se simplifica mediante el uso del controlador de la red y como complemento se tiene la aplicación que se encarga de la manipulación de las tablas de flujo en los dispositivos de reenvío de tráfico de la red.
- El esquema que se simuló bajo el paradigma de SDN en este proyecto puede considerarse como una red híbrida, ya que varios equipos se mantuvieron funcionando de manera tradicional y sin la administración mediante el controlador de la red.

5.2 RECOMENDACIONES

- Al considerar implementar un entorno de SDN es importante tener en cuenta la tecnología existente en la entidad para obviar gastos innecesarios en la compra de equipos.
- La implementación de SDN también conlleva una revisión exhaustiva de las tecnologías presentes en el mercado para conocer las capacidades de cada una y adquirir aquella que más se ajuste a las necesidades de la implementación.
- La selección de un controlador para la red definida por software se debe considerar un proceso muy importante, ya que, cada aplicativo tiene características y capacidades diferentes, además se puede escoger entre varias soluciones de software libre así como también soluciones comerciales integradas con el hardware.
- Para implementar características de SDN se recomienda que se realice de manera paulatina y segura, o gestionar capacitaciones para el personal de TI que solventen los conocimientos generales de este paradigma y aseguren la administración básica de la red mediante dicho paradigma de redes.
- En este trabajo se utilizó un appliance de openWRT del simulador para que el diseño de la red SDN se base en la implementación tradicional, pero es recomendable por facilidad e integración utilizar el appliance de openvswitch que también está incluido en la herramienta de simulación.

BIBLIOGRAFÍA

Al-Najjar, A., Layeghy, S., & Portmann, M. (2016). Pushing SDN to the end-host, network load balancing using OpenFlow . *IEEE international conference on pervasive computing and communication*, 1-6.

Andrade, L. C. (2016). *Análisis e implementación de cloud computing utilizando la plataforma de software libre owncloud.* Quito: Universidad de las Américas.

Banerjee, S., & Kannan, K. (2014). Tag-in-tag: Efficient flow table management in sdn switches. *In 10th International Conference on Network and Service Management (CNSM) and Workshop* , 109-117.

Barona, L., Valdivieso, L., & Guamán, D. (2014). Una Nueva alternativa a mininet: Emulación de una red definida por software usando VNX. *IX Congreso de Ciencia y Tecnología ESPE, 9*, 193 - 199.

Benton, K., Camp, L. J., & Small, C. (2013). OpenFlow vulnerability assessment. *In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* , 151-152.

Bernal, I., & Mejía, D. (2016). Las redes definidas por software y los desarrollos sobre esta temática en la Escuela Politécnica Nacional. *Revista Politécnica, 37*(1), 11.

Braun, W., & Menth, M. (2014). Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices. *Future Internet*, 302-336.

Calloni, J. C., Fernandes Macedo, D., Montejano, G. A., Silva, V. F., Silva, E. D., Scarello, E., & Paez, S. (2018). Modelo para la interoperabilidad entre controladores de redes definidas por software. *XX Workshop de Investigadores en Ciencias* (págs. 716-720). Red de Universidades con Carreras en Informática.

Cassongo, A. B. (2016). The comparison of network simulators for SDN. . *Новітні інформаційні системи та технології-Modern information system and technologies*.

Chico, J. C., Mejía, D., & Bernal, I. (2013). Implementación de un prototipo de una Red Definida por Software (SDN) empleando una solución basada en hardware. *Escuela Politécnica Nacional*, 356-365.

Cordero Vizhñay, C. F. (2017). *Diseño y despliegue de funciones de red virtualizadas (NFV) usando redes definidas por software (SDN) dentro de una infraestructura virtual, aplicando balanceo de carga y seguridad distribuida en IPv6.* Cuenca: Universidad Politécnica Salesiana.

Cordray, C., Link, D., Chart, R., & Ginter, K. (2015). *Washington, DC: U.S. Patente nº 9,077,611.*

De Bruijn, H., & Ten Heuvelhof, E. (2018). *Management in networks.* Londres: Routledge.

De Oliveira, R. L., Shinoda, A. A., Schweitzer, C. M., & Prete, L. R. (2014). Using mininet for emulation and prototyping software-defined networks. . *IEEE Colombian Conference*, 1-6.

Delgado, J. K., Dulce, E. R., & Toledo, R. A. (2016). La importancia del monitoreo en redes de datos. . *boletin Informativo CEI*, (págs. 50 - 51). Colombia.

Dixon, J. (4 de Mayo de 2016). *Software defined networking. Infosecwriters.* Recuperado el 28 de Julio de 2018, de http://www.infosecwriters.com/Papers/JDixon_SDN.pdf

Duarte, G. E., & Lobo, R. J. (2015). Emulación de escenarios virtuales, en una SDWLAN (software defined wireless local area network), de un campus universitario. *Ingeniería al Día, 1*(2), 69 - 85.

Giraldo, M. R., & Echeverry, A. M. (2018). Redes de datos definidas por software-SDN, arquitectura, componentes y funcionamiento. *Journal de Ciencia e Ingenierıa*, 55-61.

GNS3. (10 de Septiembre de 2018). Obtenido de GNS3: https://www.gns3.com/software

Intriago, R. W. (2017). *Estudio del protocolo Openflow usando el modelo de red definida por software (software defined networks). Caso de estudio la Universidad Técnica de Manabí.* Quito: PUCE.

Jain, R., & Paul, S. (2013). Network virtualization and software defined networking for cloud computing: a survey. *IEEE Communications Magazine*, 24-31.

Jarschel, M., Zinner, T., Hoßfeld, T., Tran-Gia, P., & Kellerer, W. (2014). Interfaces, attributes, and use cases: A compass for SDN. *IEEE Communications Magazine*, 210-217.

Khattak, Z. K., Awais, M., & Iqbal, A. (2014). Performance evaluation of OpenDaylight SDN controller. *IEEE international conference on parallel and distributed systems (ICPADS)*, 671-676.

Kim, H., & Feamster, N. (2013). Improving network management with software defined networking. *IEEE Communications Magazine*, 114-119.

Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 14-76.

Laponina, O. R., & Sizov, M. R. (2017). Laboratory bench for testing the integration capabilities of SDN networks and traditional networks. *International Journal of Open Information Technologies*, 3-12.

Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network innovation using openflow: A survey. . *IEEE communications surveys & tutorials*, 493-512.

Marín, M. Y. (2016). *Plataforma de pruebas para evaluar el desempeño de las redes definidas por software basadas en el protocolo Openflow.* Cuba: Universidad Central" Marta Abreu" de Las Villas. Facultad de Ingeniería Eléctrica.

Mininet. (10 de Septiembre de 2018). Obtenido de Mininet: http://mininet.org/overview/

Mohtasin, R., Prasad, P. W., Alsadoon, A., Zajko, G., Elchouemi, A., & Singh, A. K. (2016). Development of a virtualized networking lab using GNS3 and VMware workstation. *International Conference on Wireless Communications*.

Mousavi, S. M., & St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. *IEEE Magazine*, 77-81.

Netacad. (10 de Septiembre de 2018). Obtenido de Netacad: https://www.netacad.com/es/courses/packet-tracer

ns-3. (10 de Septiembre de 2018). Obtenido de ns-3: https://www.nsnam.org/

Nunes, B. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. . *IEEE Communications Surveys & Tutorials*, 1617-1634.

Pérez, G. C., & Marín, M. F. (2015). Redes definidas por software: Solución para servicios portadores del Ecuador. *Investigation Research Review*, 41-63.

Perrin, S., & Hubbard, S. (2013). Practical Implementation of SDN & NFV in the WAN. *White paper, Heavy Reading*, 1-11.

Rojas, E., Doriguzzi-Corin, R., Tamurejo, S., Beato, A., Schwabe, A., Phemius, K., & Guerrero, C. (2018). Are we ready to drive software-defined networks? A comprehensive survey on management tools and techniques. *ACM Computing Surveys* .

Roncero, H. O. (2014). *Software defined networking.* Barcelona: Universidad Politécnica de Cataluña.

Ruiz, Q. A. (2015). *Estado del arte redes definidas por software (SDN).* Pereira: Universidad Católica de Pereira.

Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, 36-43.

Shalimov, A., Zuikov, D., Zimarina, D., Pashkov, V., & Smeliansky, R. (2013). Advanced study of SDN/OpenFlow controllers. . *In Proceedings of the*

9th central & eastern european software engineering conference in russia.

Sharma, S. U., & Gandole, Y. B. (2013). Understanding network latency in thin client environment. *IJESIT*, 4.

Titus, T. G. (2007). *Estados Unidos Patente nº 11/796,092.*

Vera, V. J. (2016). *Mejoramiento de los enlaces de datos y de la infraestructura de red del campus de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López .* Quito.

Vidal, L. J. (2016). *Diseño una propuesta de mejoramiento en la infraestructura de red de datos en la ESPAM MFL con calidad de servicio.* Quito.

Wang, S. Y., Chou, C. L., & Yang, C. M. (2013). EstiNet openflow network simulator and emulator. *IEEE Communications Magazine*, 110-117.

Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*, 27-51.

ANEXOS

ANEXO 1: CAPTURAS DE LOS DATOS OBTENIDOS EN LA HERRAMIENTA DE MONITOREO EN EL PARADIGMA DE SDN

PRUEBAS DE MONITOREO DEL ENFOQUE SDN AL MOODLE LOCAL

En estas pruebas se evaluó el rendimiento del modelo de red SDN mientras se realizaban consultas de ping al servidor de aula virtual instalado de manera local en la simulación.

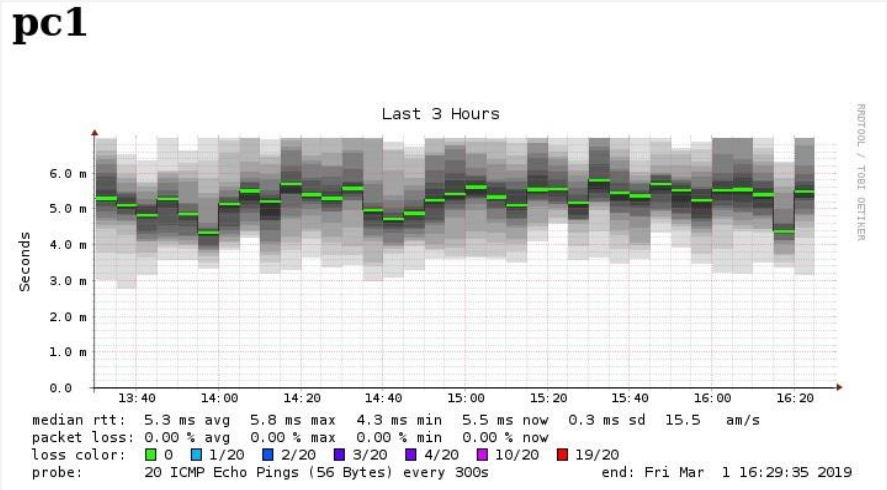

Figura 12. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

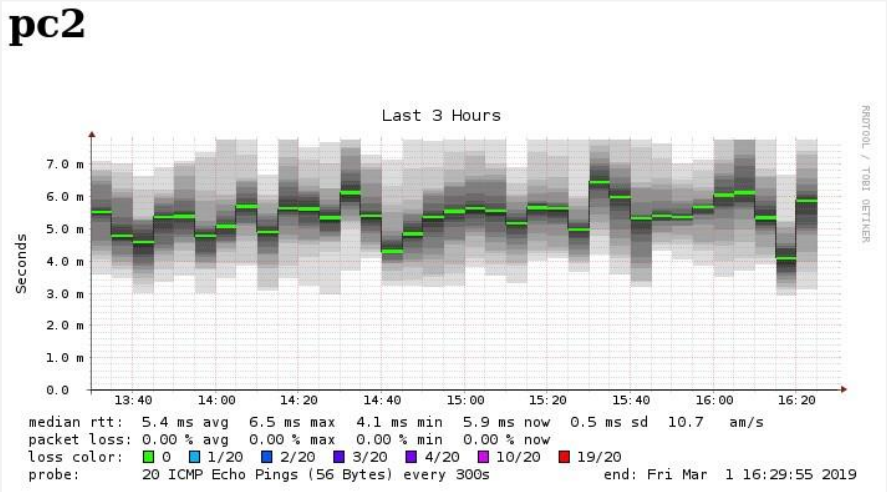

Figura 13. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

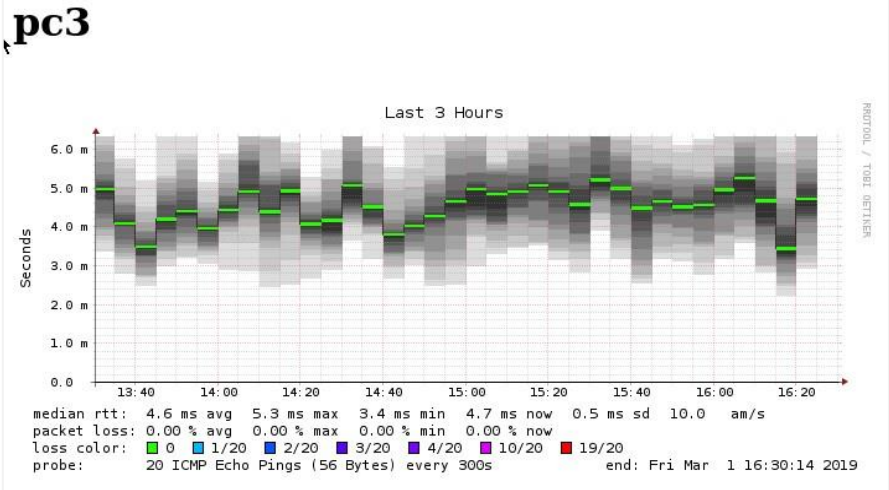

Figura 14. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

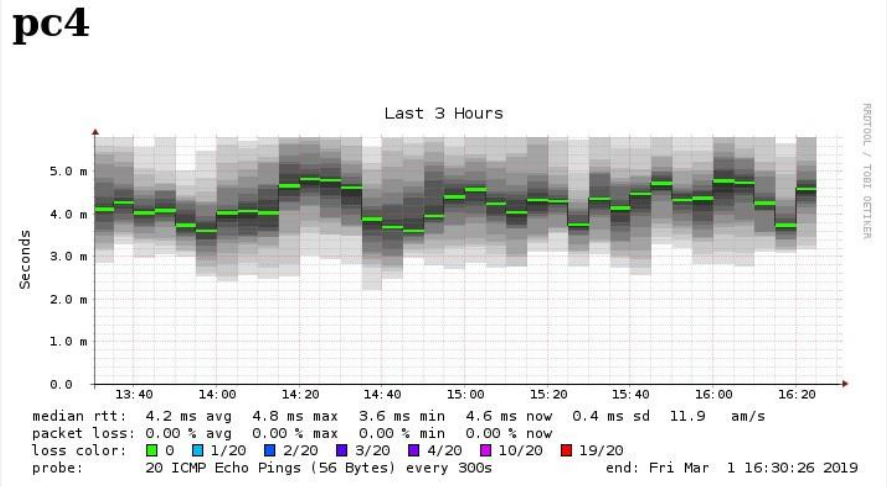

Figura 15. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

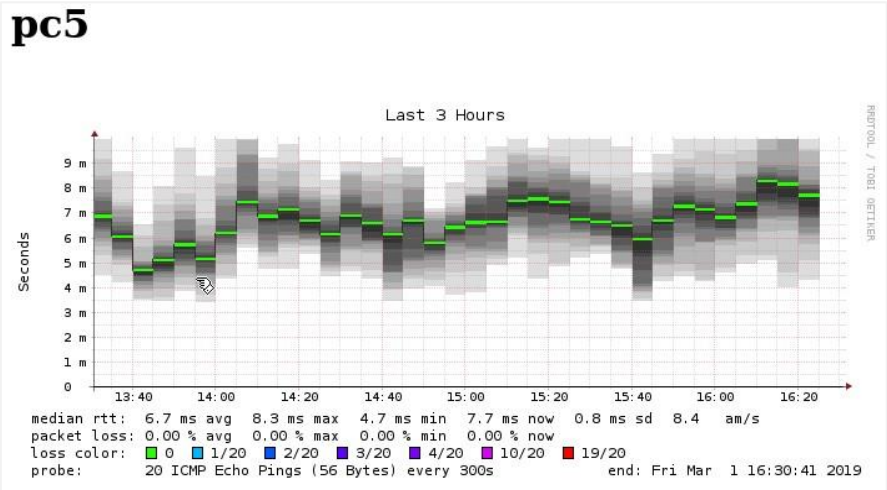

Figura 16. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

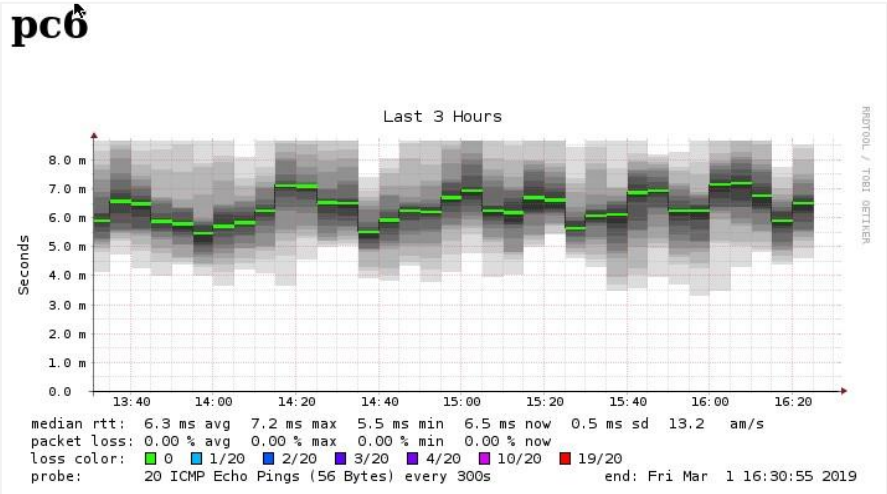

Figura 17. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

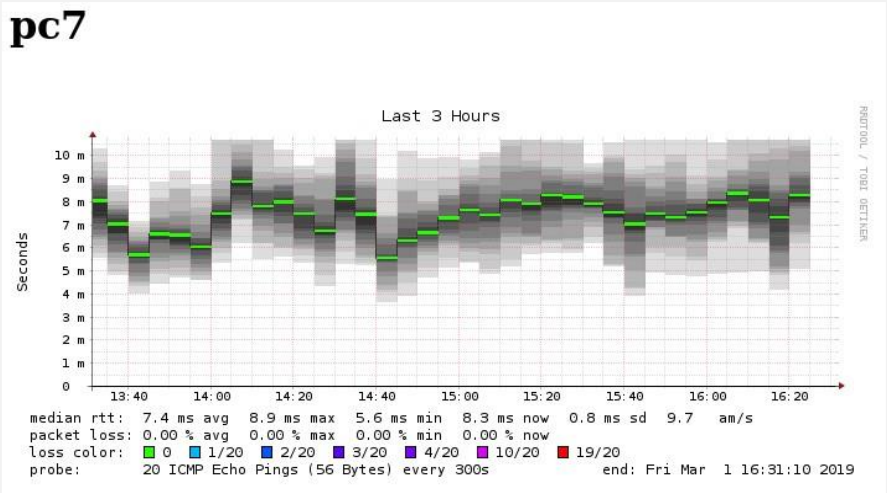

Figura 18. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE SDN AL SITIO WEB LOCAL

Estas pruebas reportaron pérdidas de paquetes, al iniciar la transmisión de los paquetes ICMP, este comportamiento a veces es común en redes SDN que basan su tráfico en la transmisión de flujo ya que en primera instancia las entradas de las tablas de flujo desconocen el origen y el destino de los paquetes.

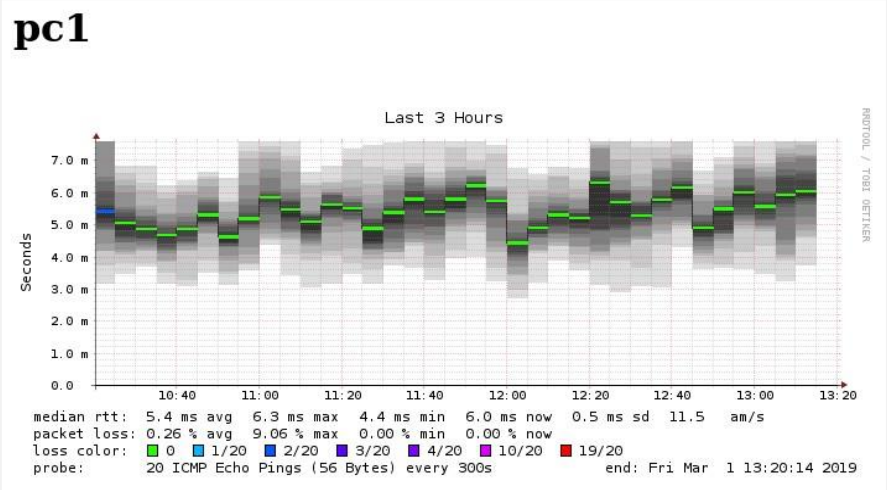

Figura 19. Medición de latencia entre PC 1 y el sitio web local
Fuente: Los Autores

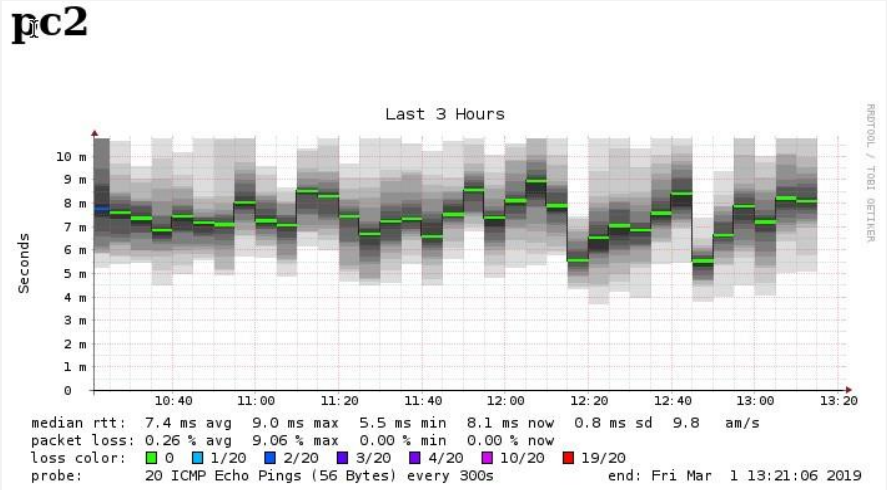

Figura 20. Medición de latencia entre PC 2 y el sitio web local
Fuente: Los Autores

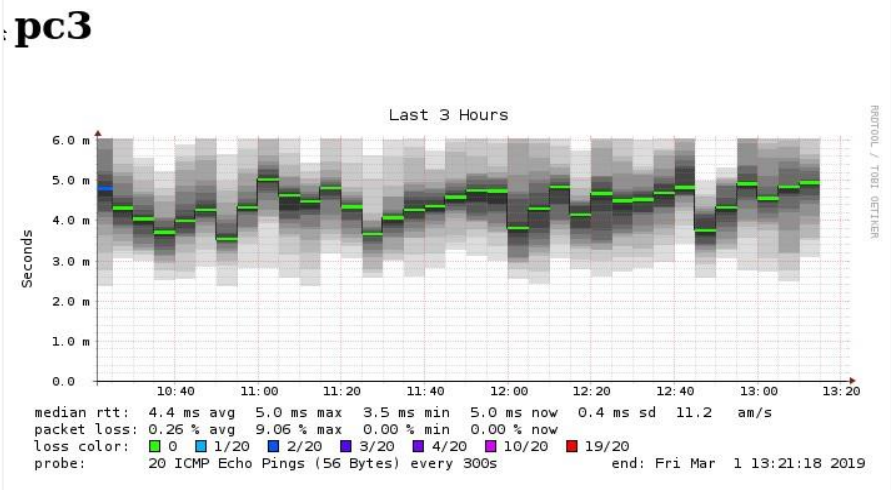

Figura 21. Medición de latencia entre PC 3 y el sitio web local
Fuente: Los Autores

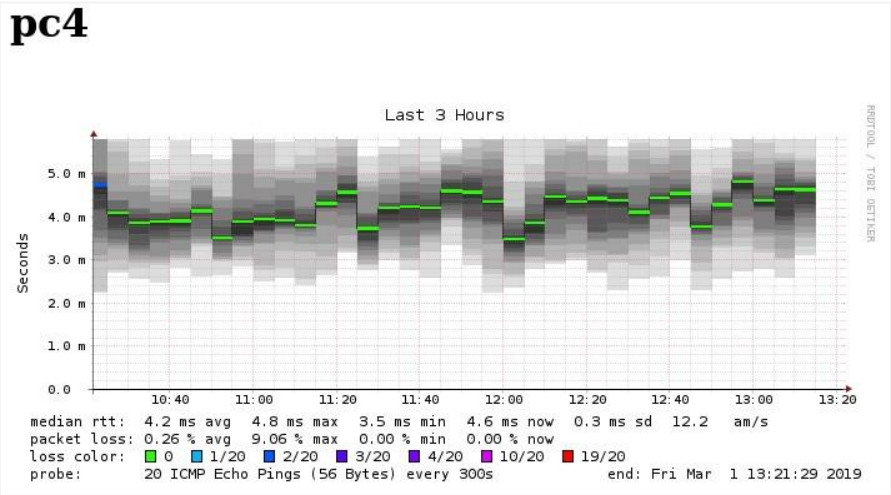

Figura 22. Medición de latencia entre PC 4 y el sitio web local
Fuente: Los Autores

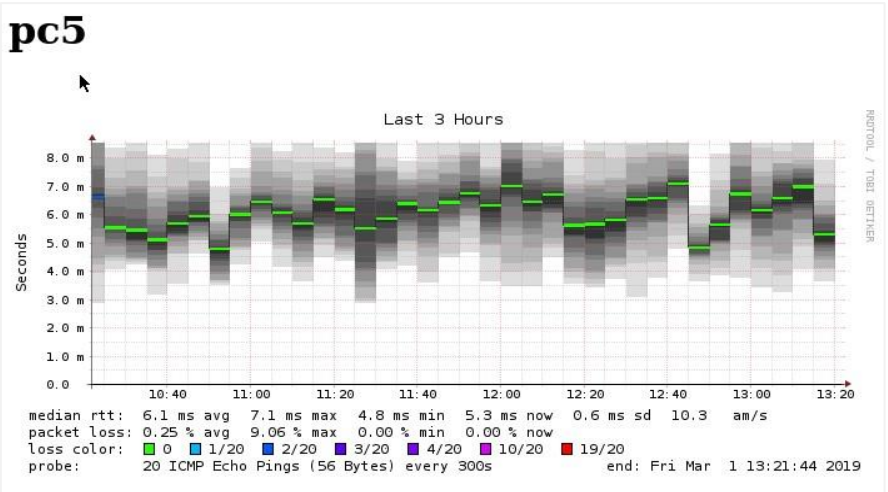

Figura 23. Medición de latencia entre PC 5 y el sitio web local
Fuente: Los Autores

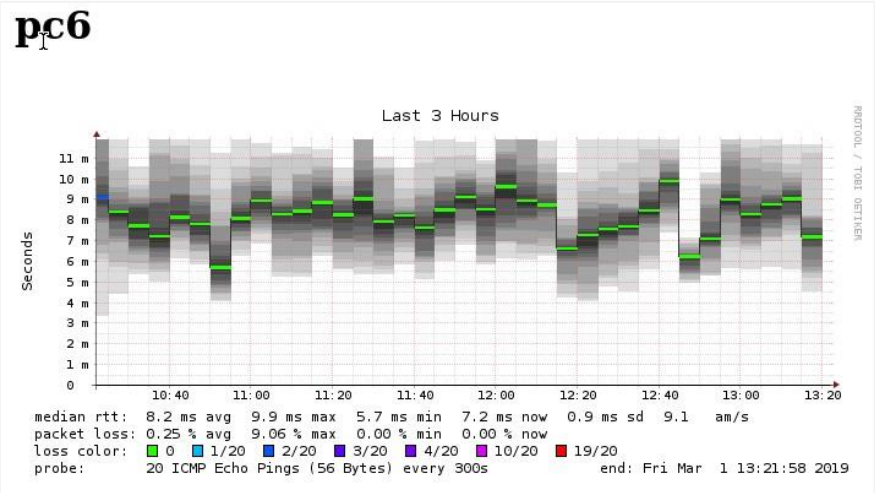

Figura 24. Medición de latencia entre PC 6 y el sitio web local
Fuente: Los Autores

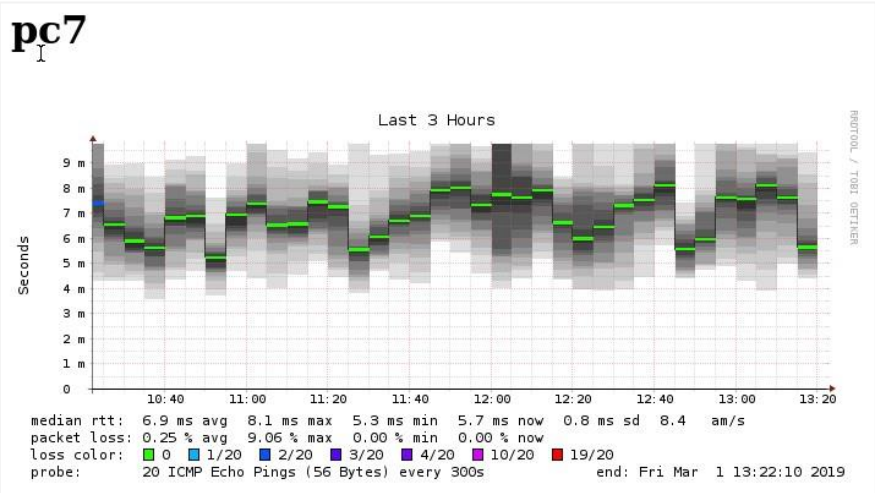

Figura 25. Medición de latencia entre PC 7 y el sitio web local
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE SDN AL SITIO WEB DE LA ESPAM MFL

Estas pruebas también presentaron perdidas de paquetes situación que se puede justificar de igual forma que en las pruebas anteriores, ya que, aunque las PC se estén conectando a un servicio externo el Smokeping monitorea los equipos mediante las entradas de las tablas de flujo.

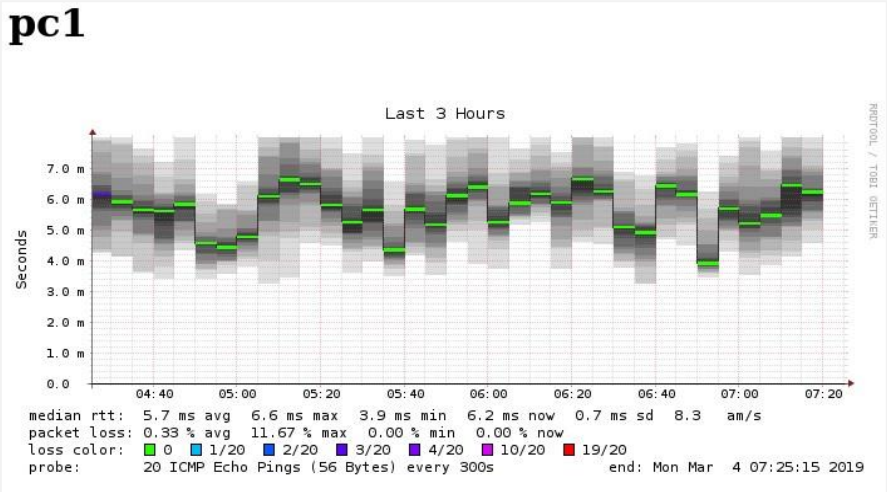

Figura 26. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

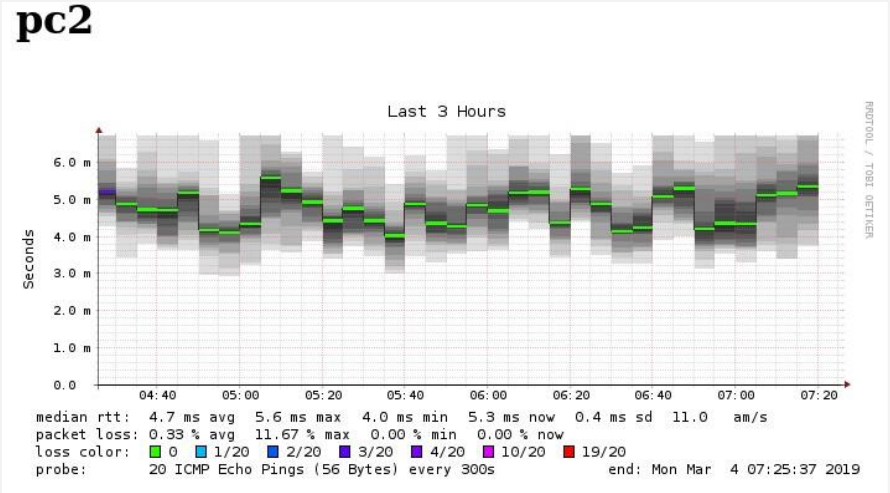

Figura 27. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

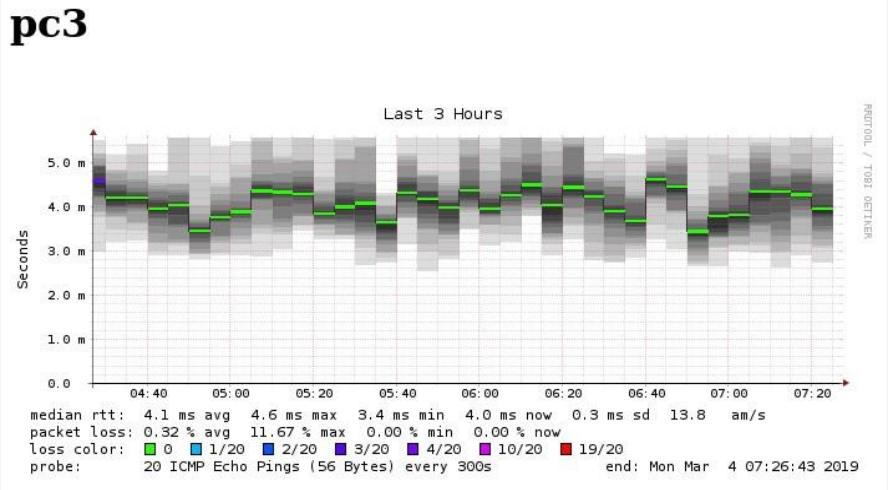

Figura 28. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

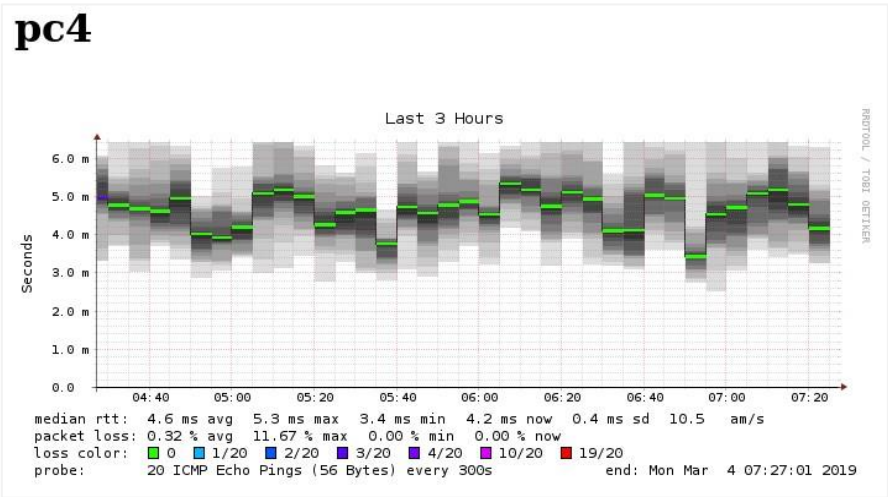

Figura 29. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

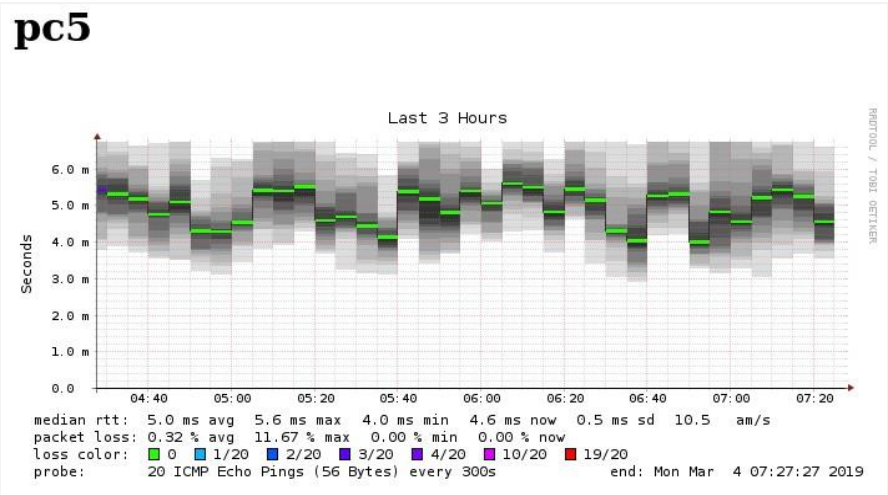

Figura 30. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

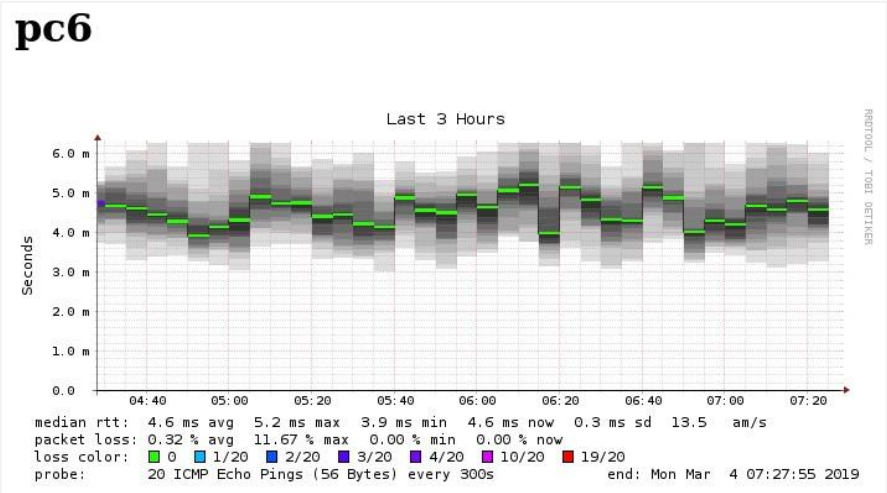

Figura 31. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

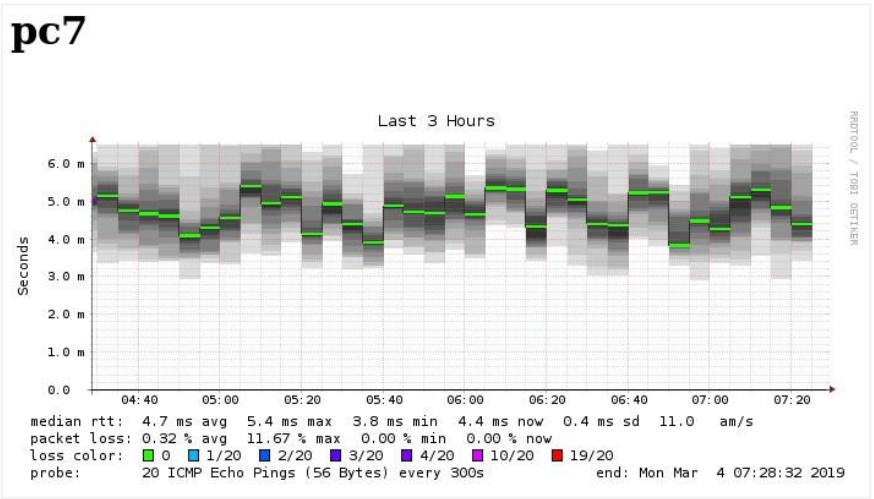

Figura 32. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE SDN AL WEBMAIL DE LA ESPAM MFL

En estas pruebas se evaluó el rendimiento del modelo de red SDN mientras se realizaban consultas de ping al servidor de webmail real de la ESPAM MFL.

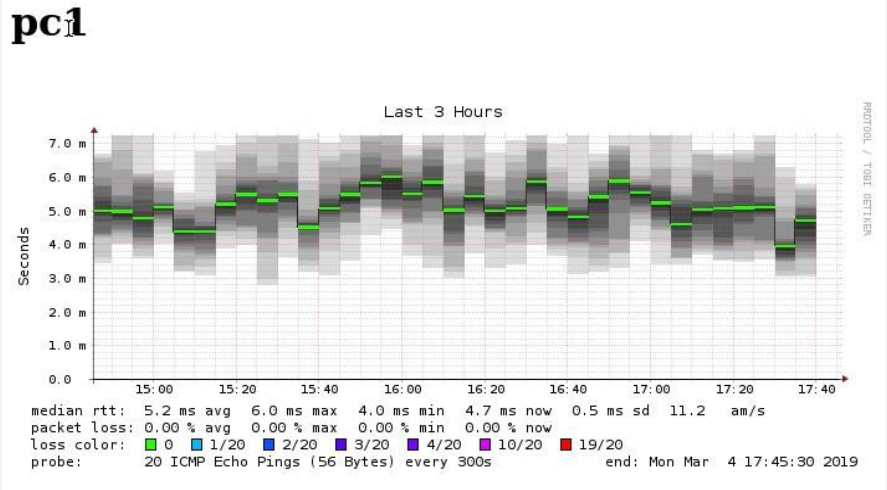

Figura 33. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

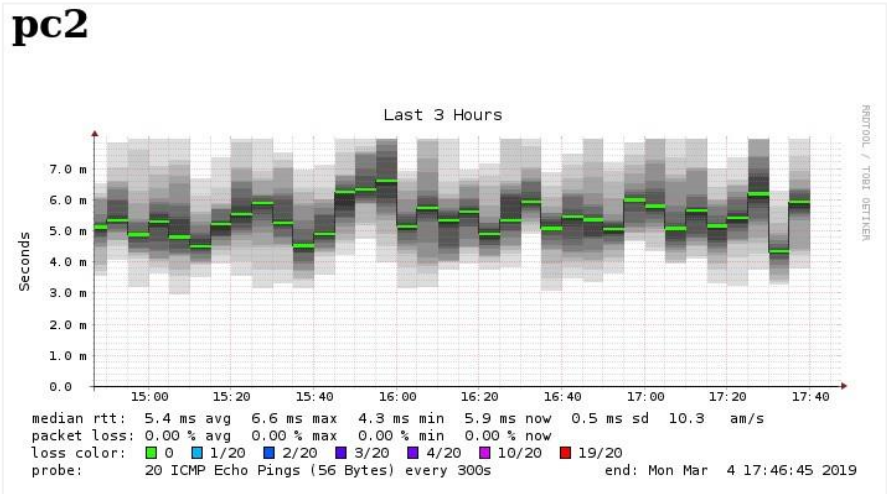

Figura 34. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

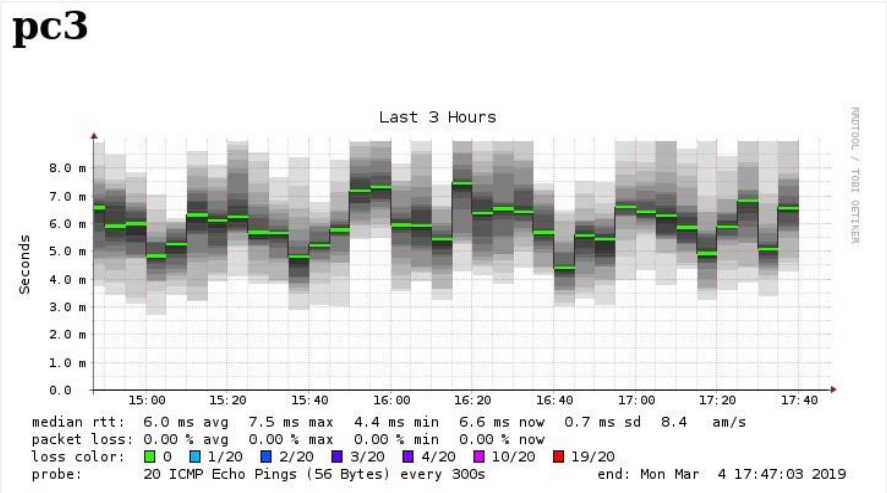

Figura 35. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

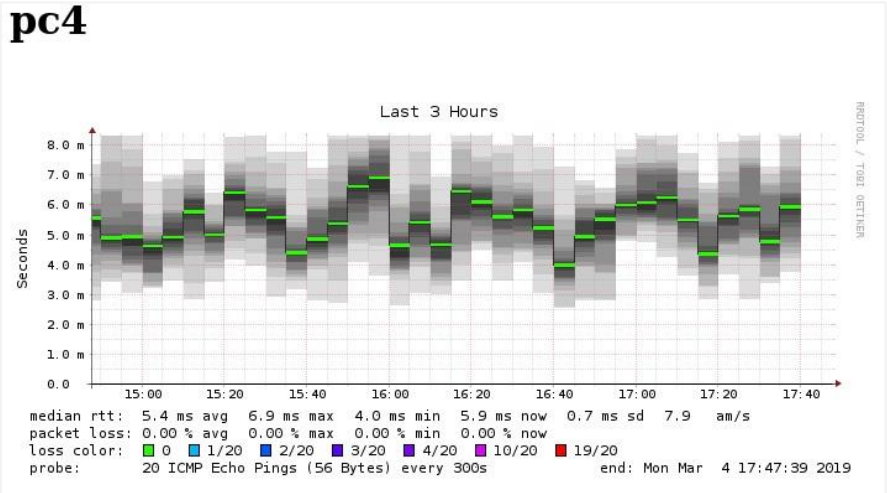

Figura 36. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

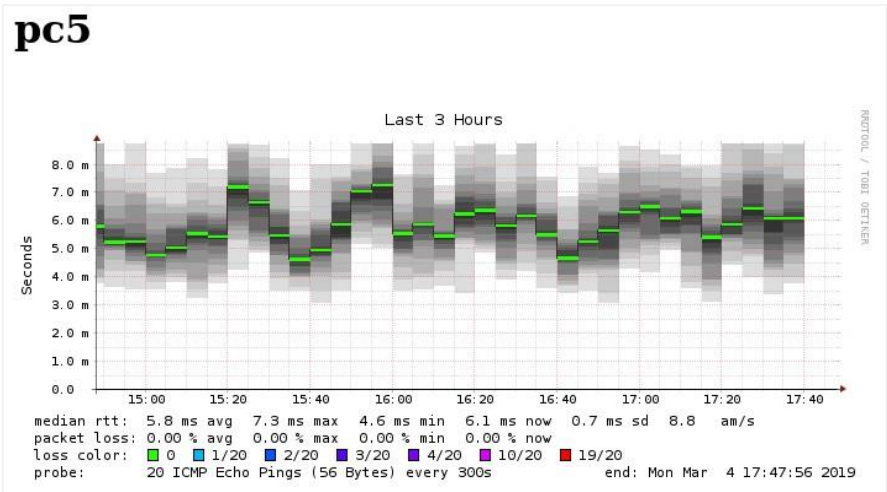

Figura 37. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

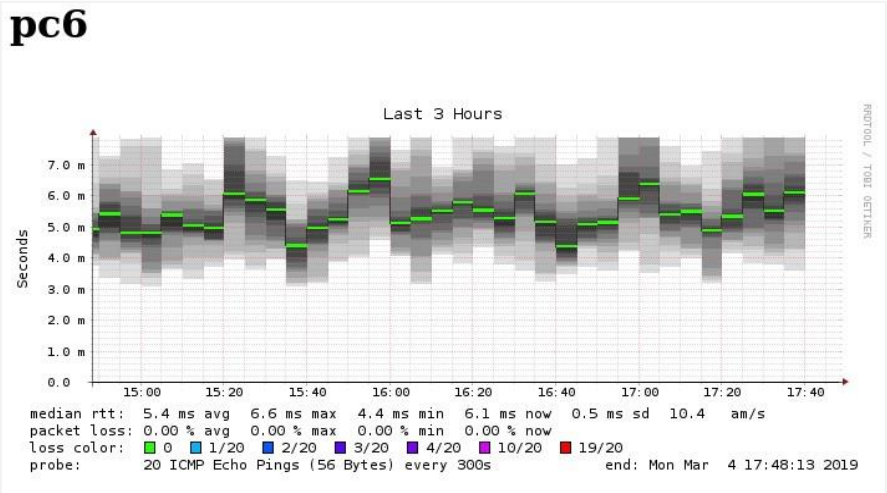

Figura 38. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

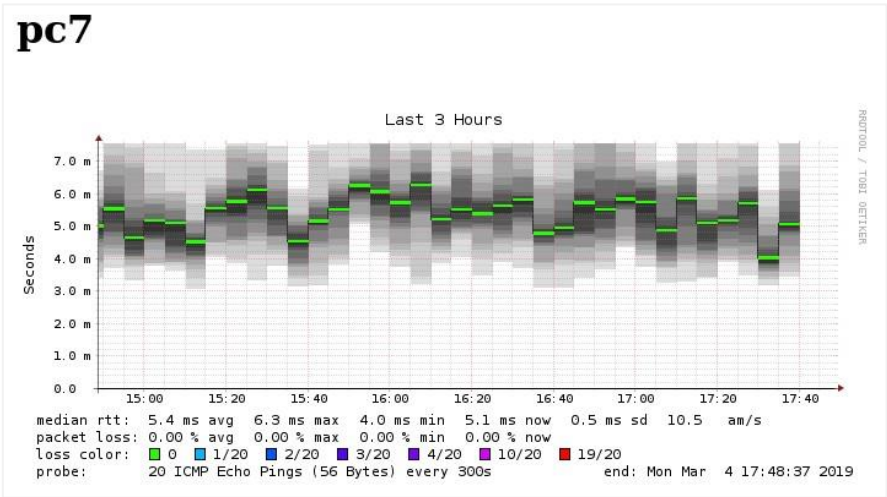

Figura 39. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

ANEXO 2: CAPTURAS DE LOS DATOS OBTENIDOS EN LA HERRAMIENTA DE MONITOREO EN EL PARADIGMA DE RED TRADICIONAL

PRUEBAS DE MONITOREO DEL ENFOQUE TRADICIONAL AL MOODLE LOCAL

En estas pruebas se evaluó el rendimiento del modelo de red tradicional mientras se realizaban consultas de ping al servidor de aula virtual instalado de manera local en la simulación.

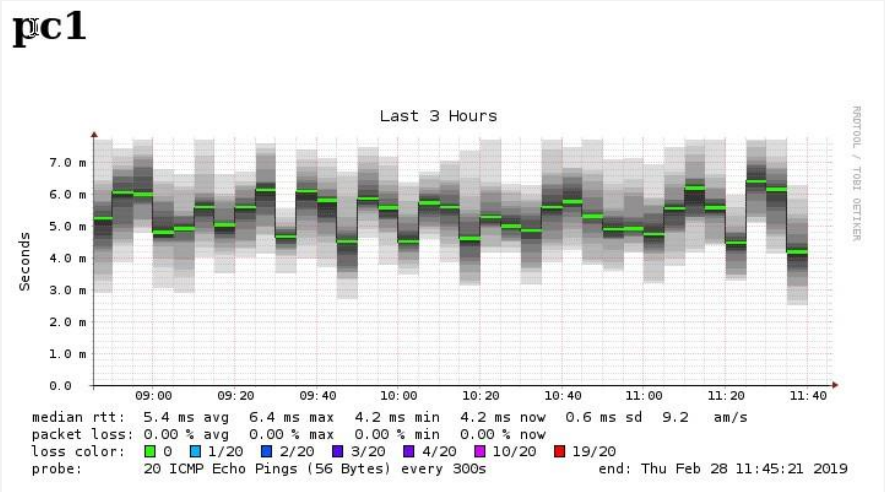

Figura 40. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

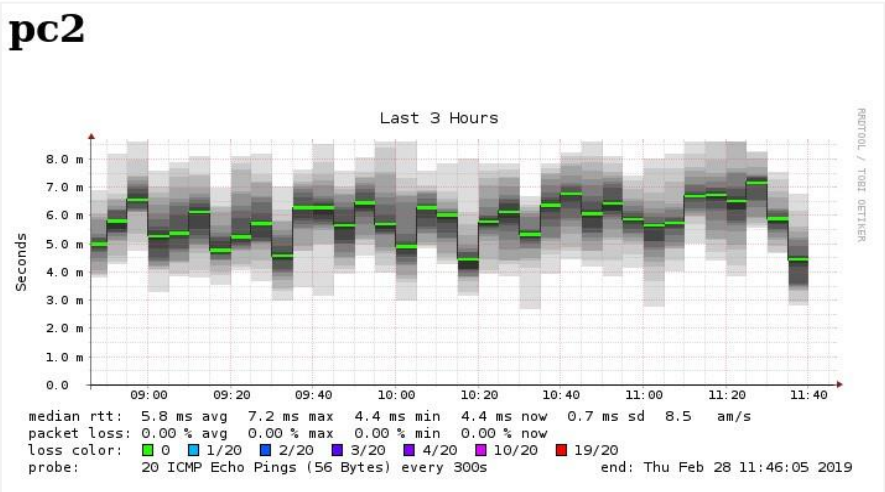

Figura 41. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

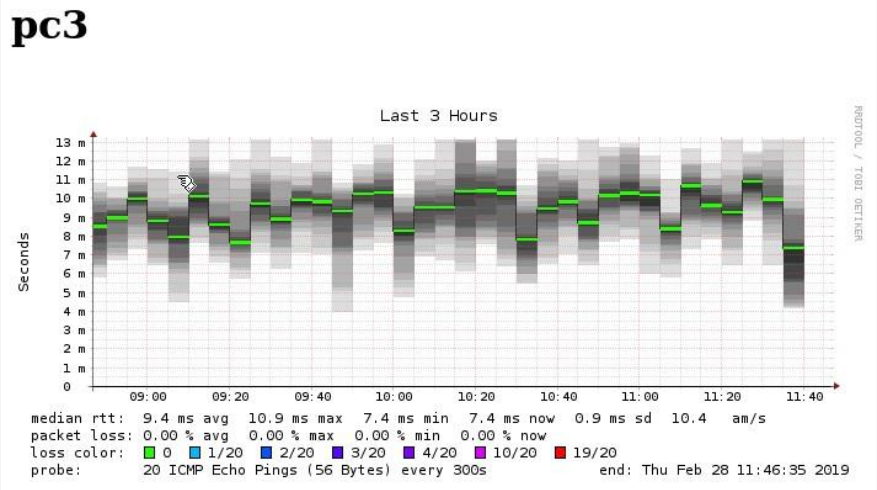

Figura 42. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

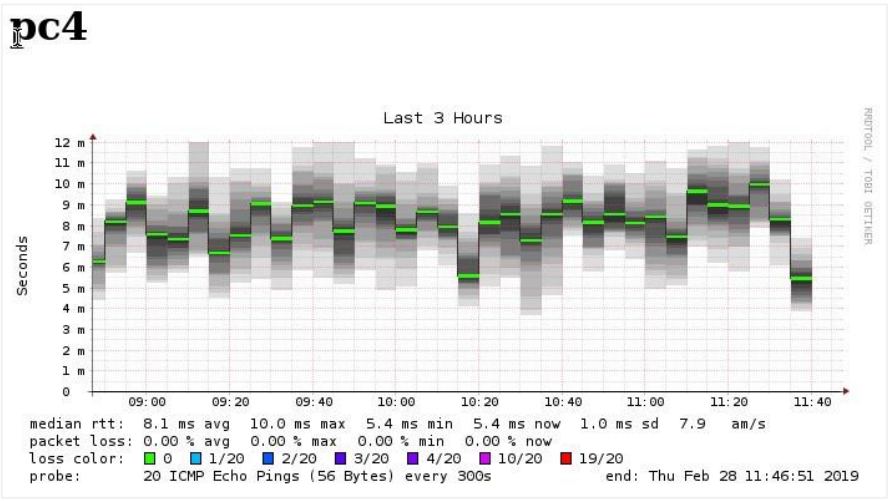

Figura 43. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

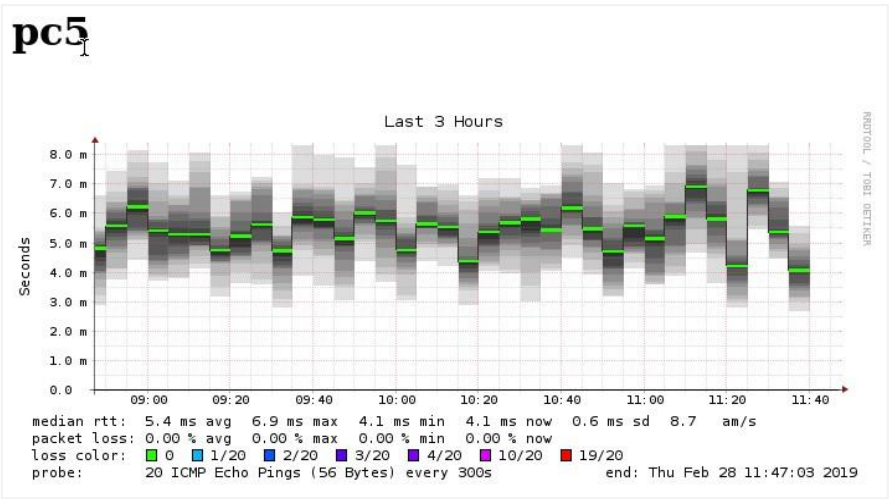

Figura 44. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

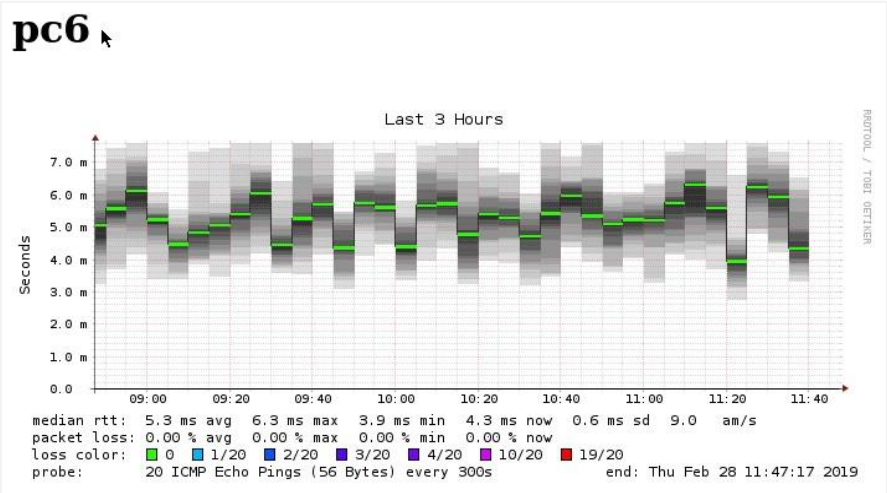

Figura 45. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

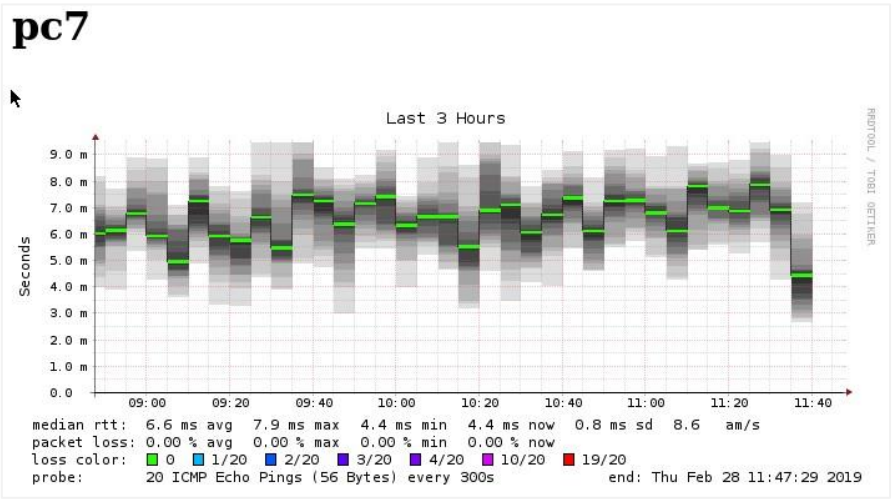

Figura 46. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE TRADICIONAL AL SITIO WEB LOCAL

En estas pruebas se evaluó el rendimiento del modelo de red tradicional mientras se realizaban consultas de ping al sitio web instalado de manera local en la simulación.

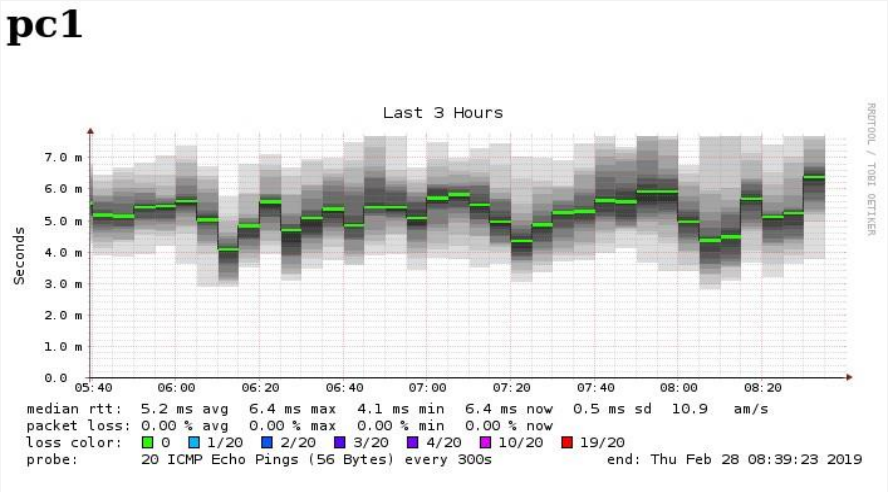

Figura 47. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

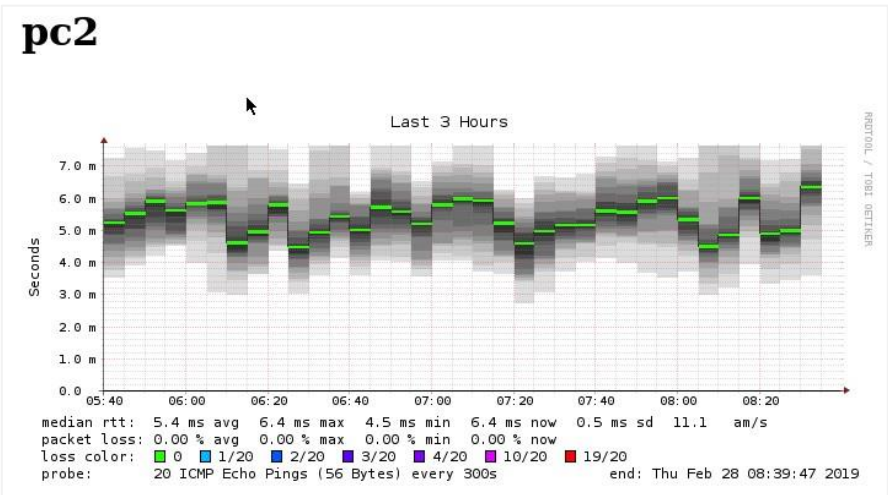

Figura 48. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

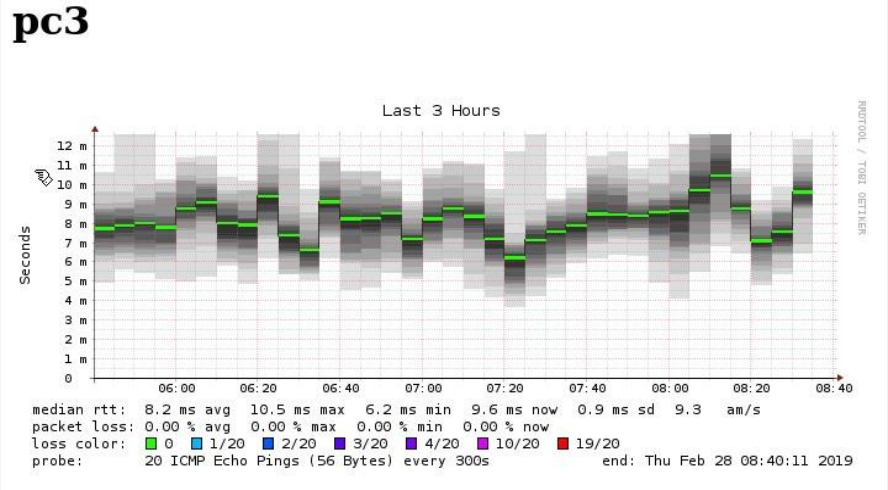

Figura 49. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

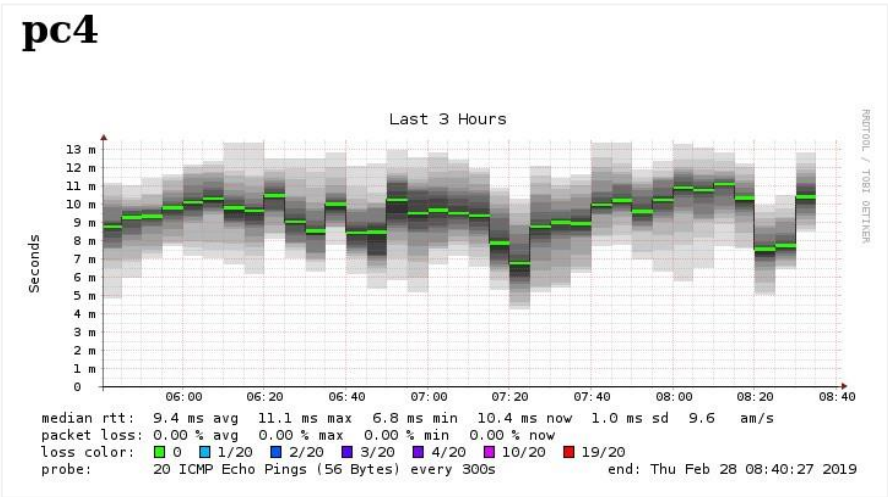

Figura 50. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

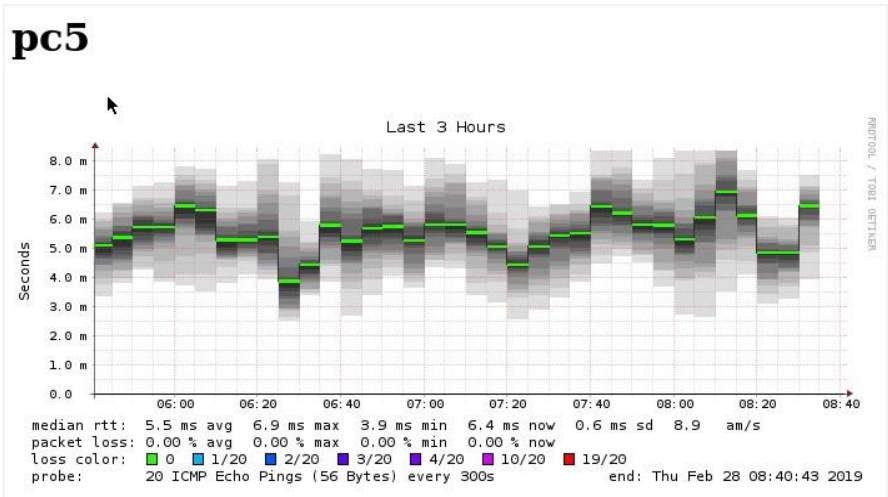

Figura 51. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

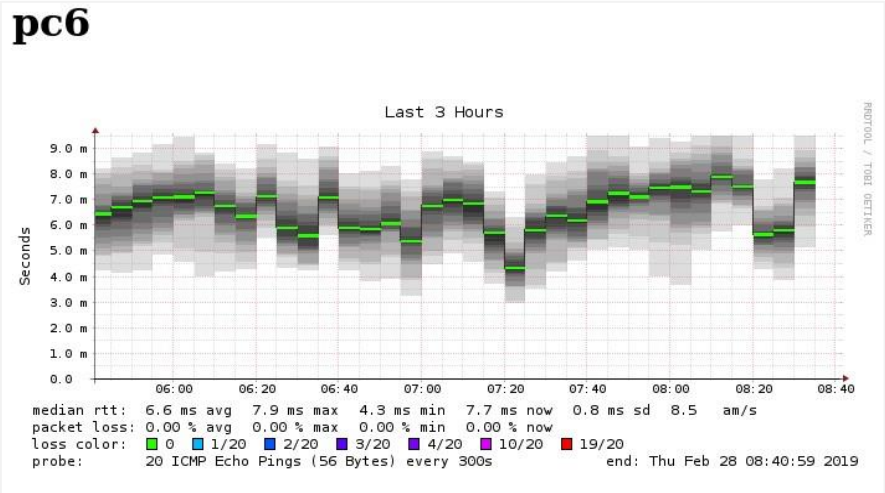

Figura 52. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

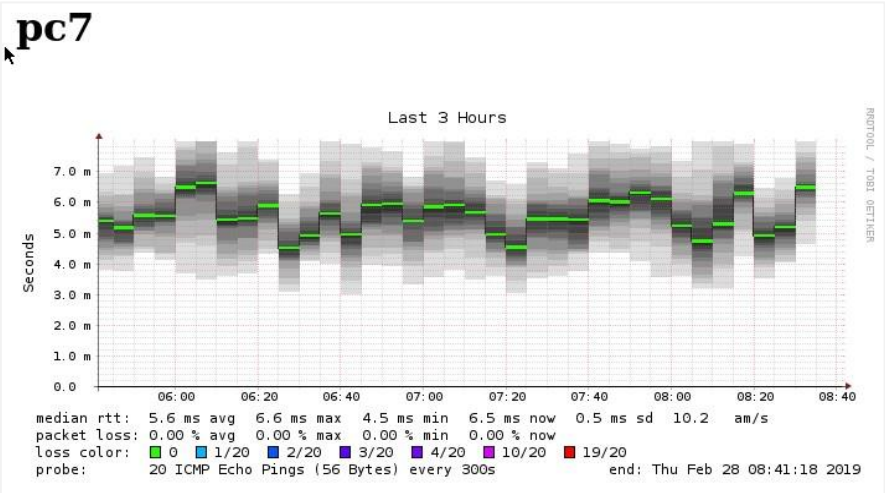

Figura 53. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE TRADICIONAL AL SITIO WEB DE LA ESPAM MFL

En estas pruebas se evaluó el rendimiento del modelo de red tradicional mientras se realizaban consultas de ping al sitio web real de la ESPAM MFL.

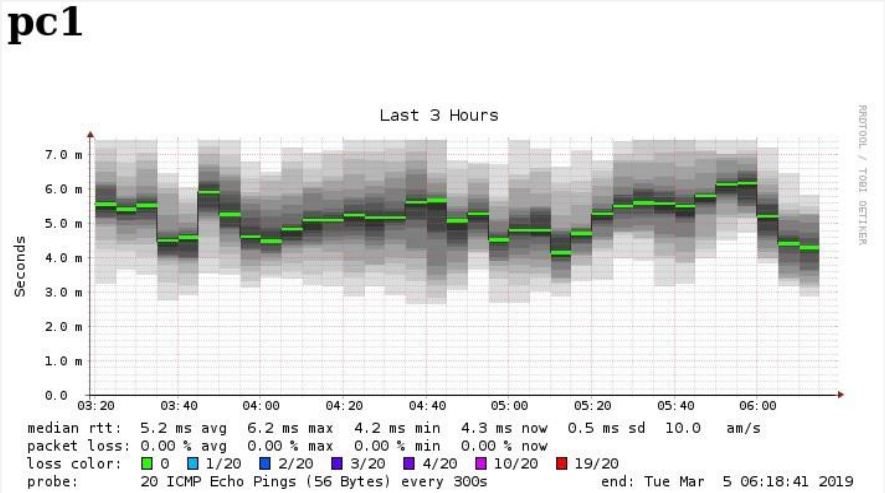

Figura 54. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

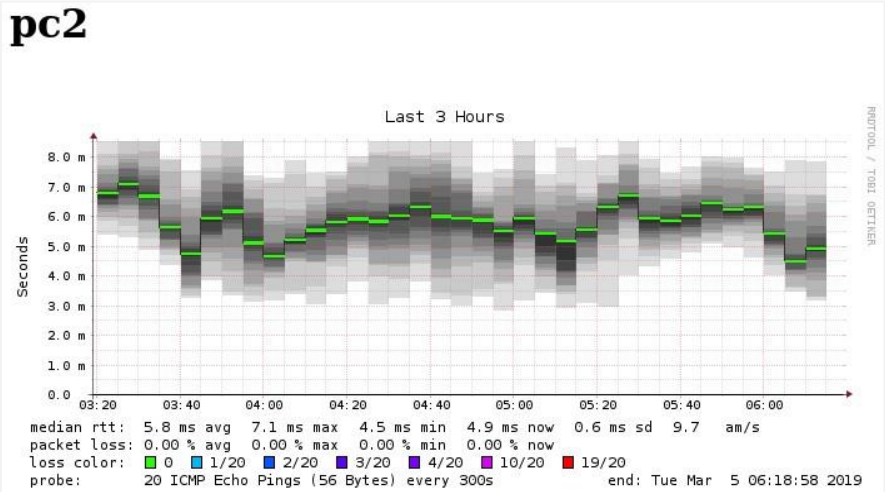

Figura 55. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

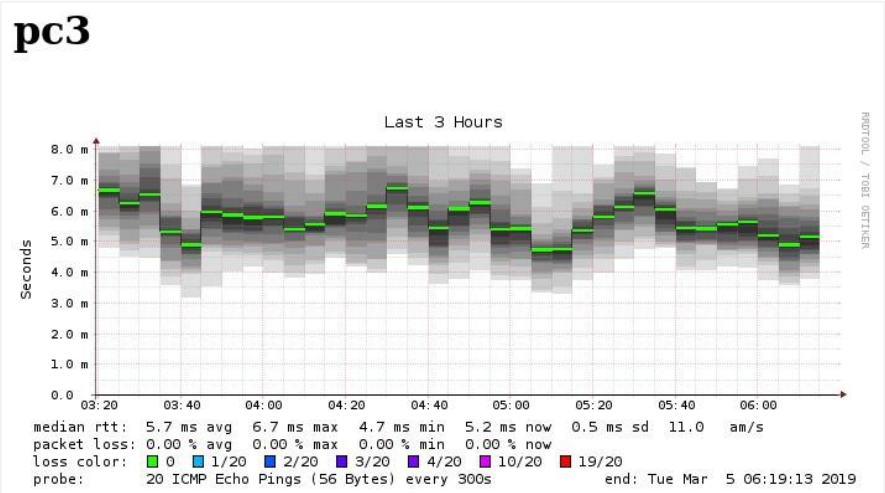

Figura 56. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

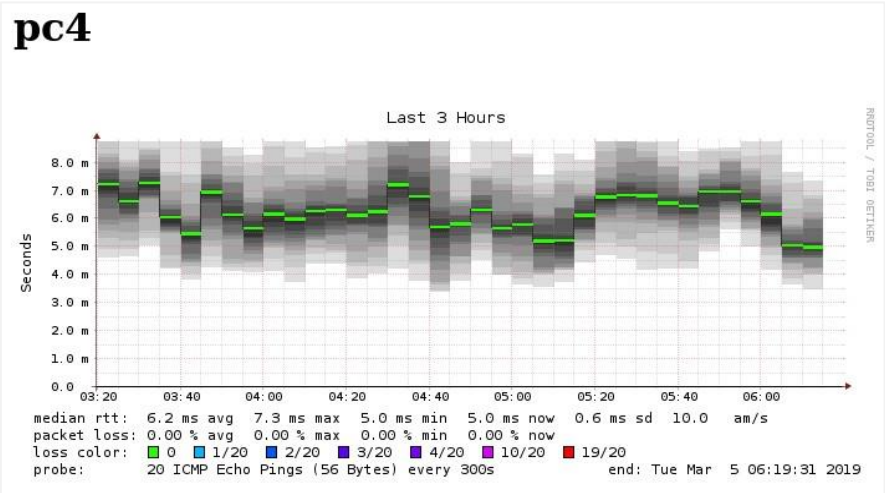

Figura 57. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

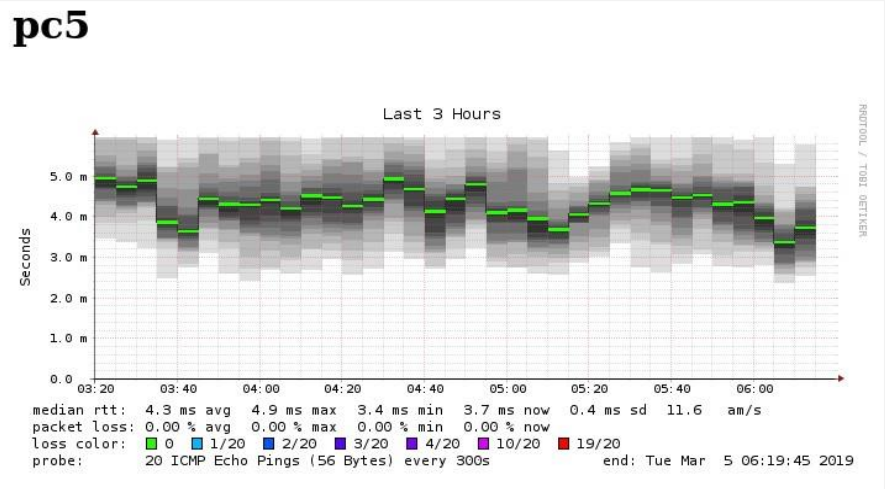

Figura 58. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

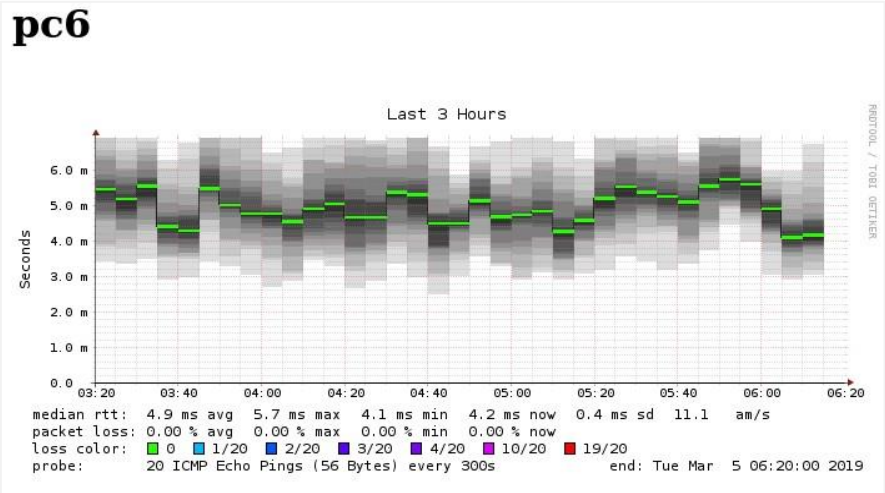

Figura 59. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

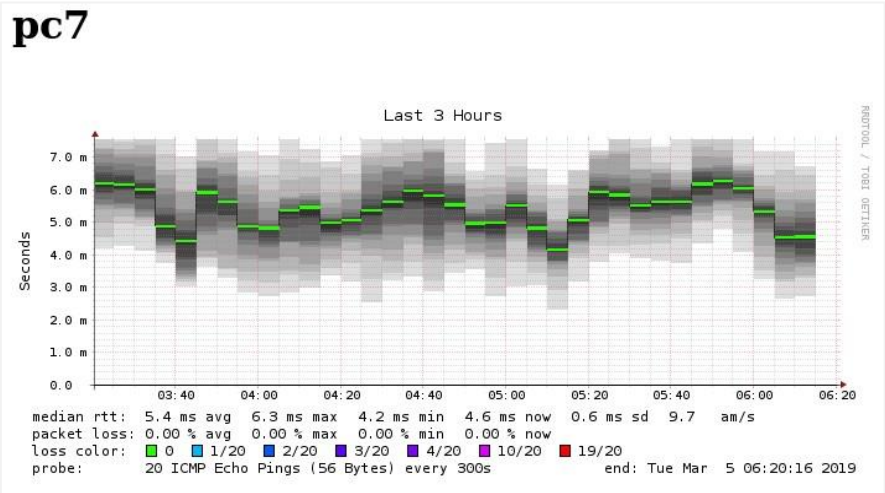

Figura 60. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

PRUEBAS DE MONITOREO DEL ENFOQUE TRADICIONAL AL WEBMAIL DE LA ESPAM MFL

En estas pruebas se evaluó el rendimiento del modelo de red tradicional mientras se realizaban consultas de ping al servidor de webmail real de la ESPAM MFL.

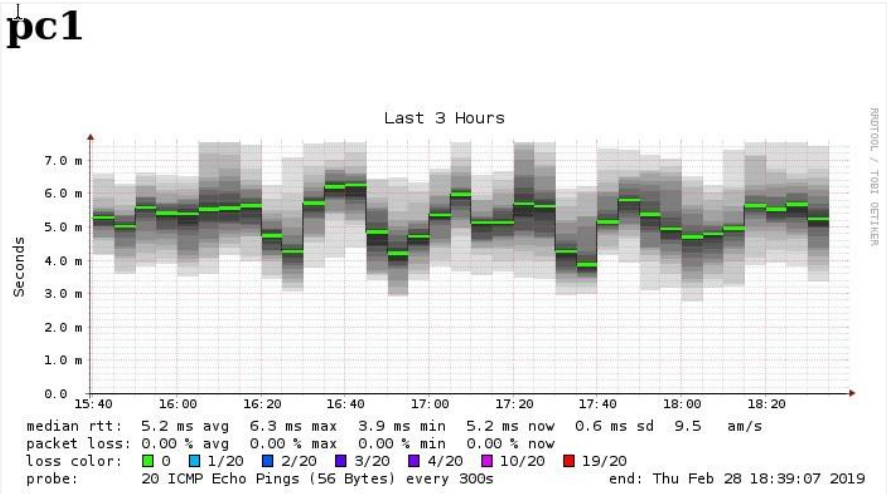

Figura 61. Medición de latencia entre PC 1 y Smokeping
Fuente: Los Autores

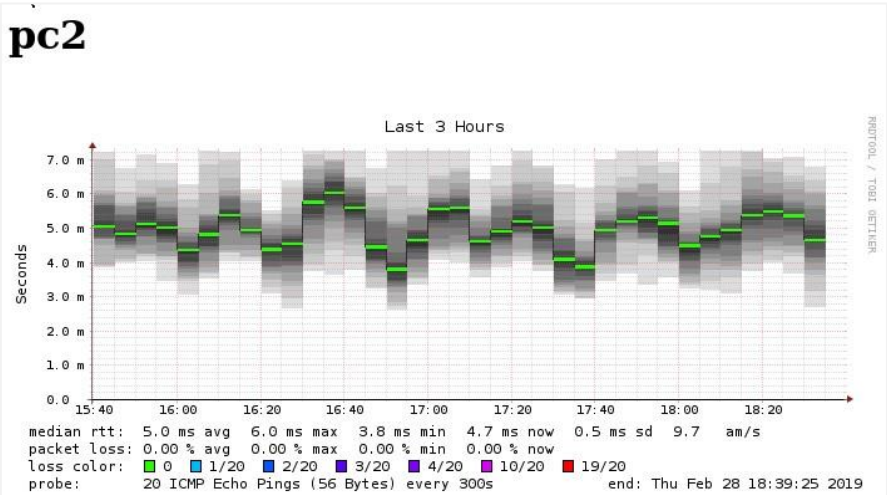

Figura 62. Medición de latencia entre PC 2 y Smokeping
Fuente: Los Autores

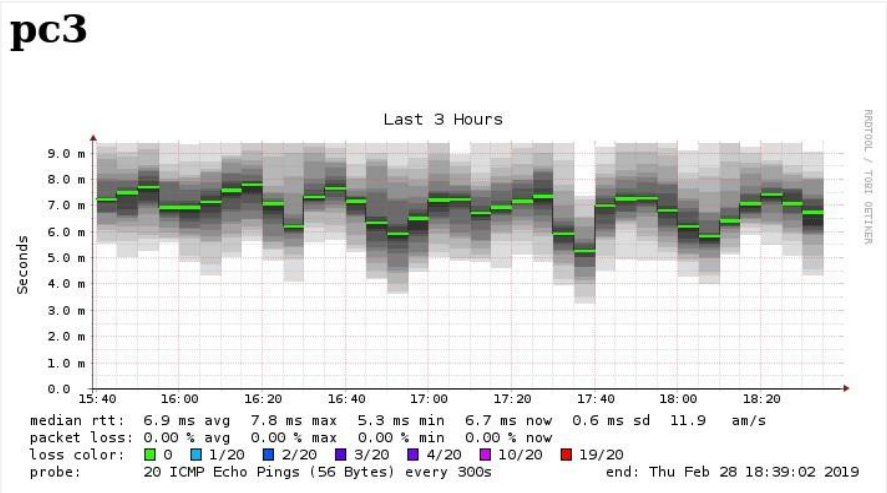

Figura 63. Medición de latencia entre PC 3 y Smokeping
Fuente: Los Autores

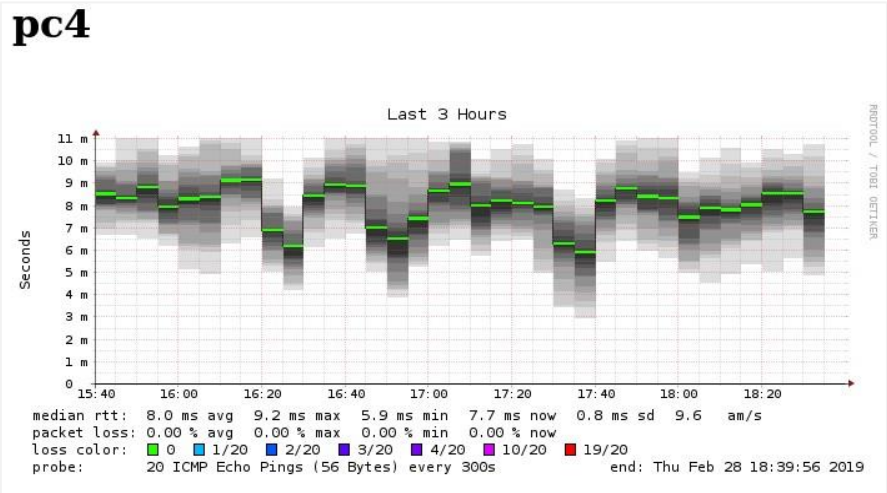

Figura 64. Medición de latencia entre PC 4 y Smokeping
Fuente: Los Autores

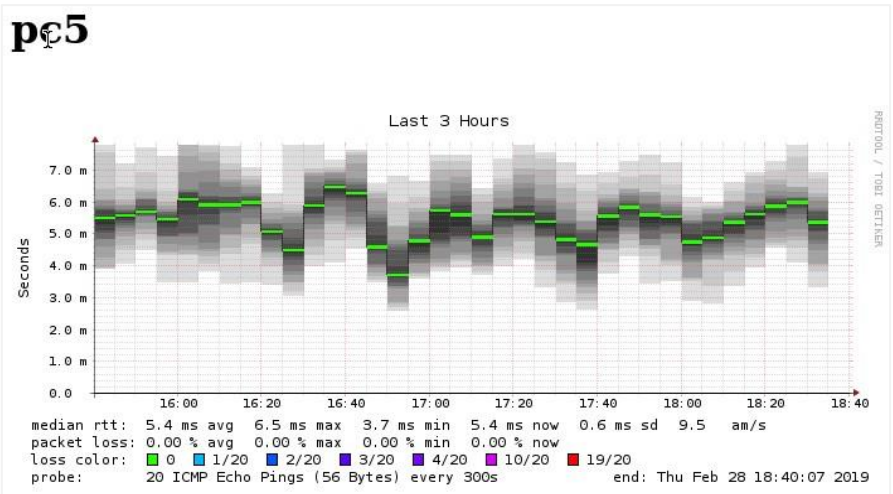

Figura 65. Medición de latencia entre PC 5 y Smokeping
Fuente: Los Autores

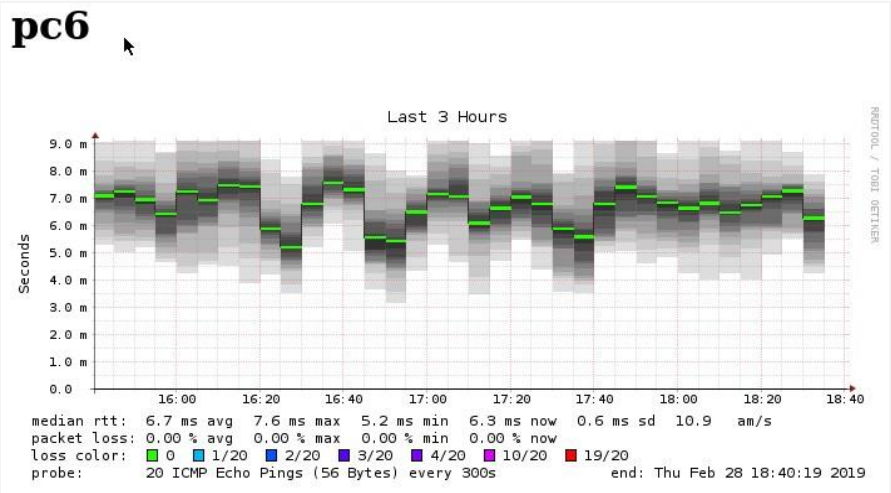

Figura 66. Medición de latencia entre PC 6 y Smokeping
Fuente: Los Autores

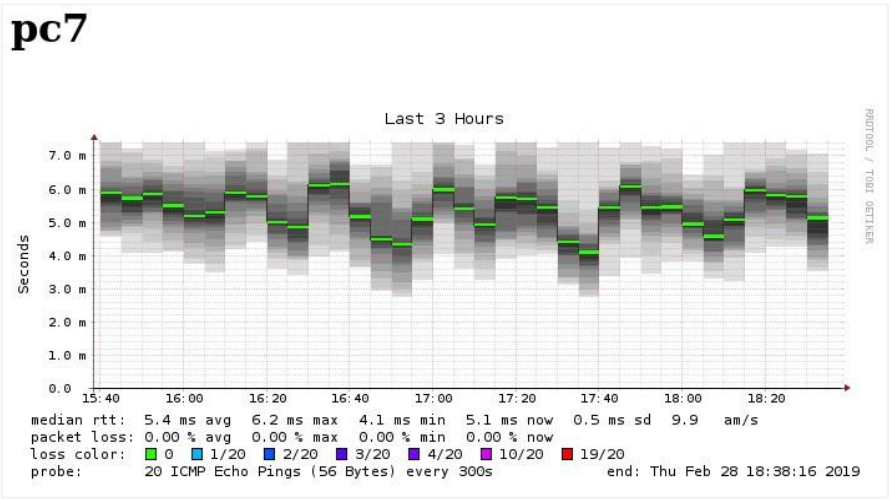

Figura 67. Medición de latencia entre PC 7 y Smokeping
Fuente: Los Autores

ANEXO 3: CAPTURAS DEL CONTROLADOR FLOODLIGHT

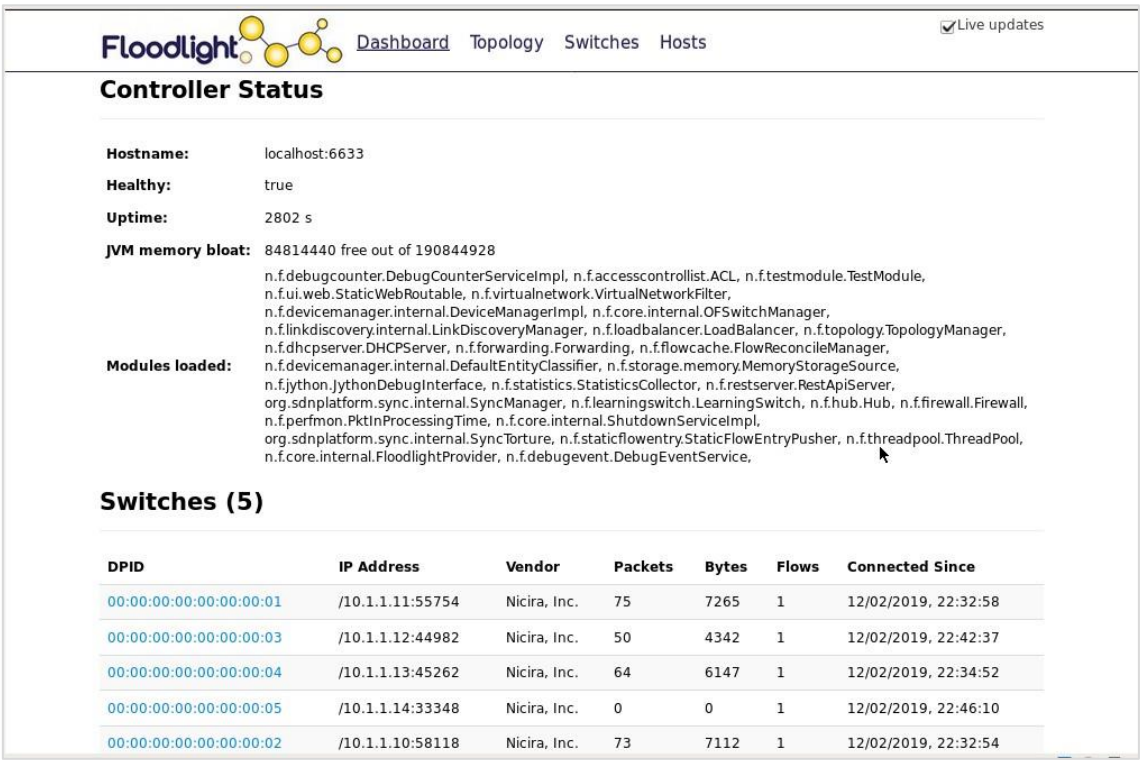

Figura 68. Panel principal del controlador Floodlight
Fuente: Los Autores

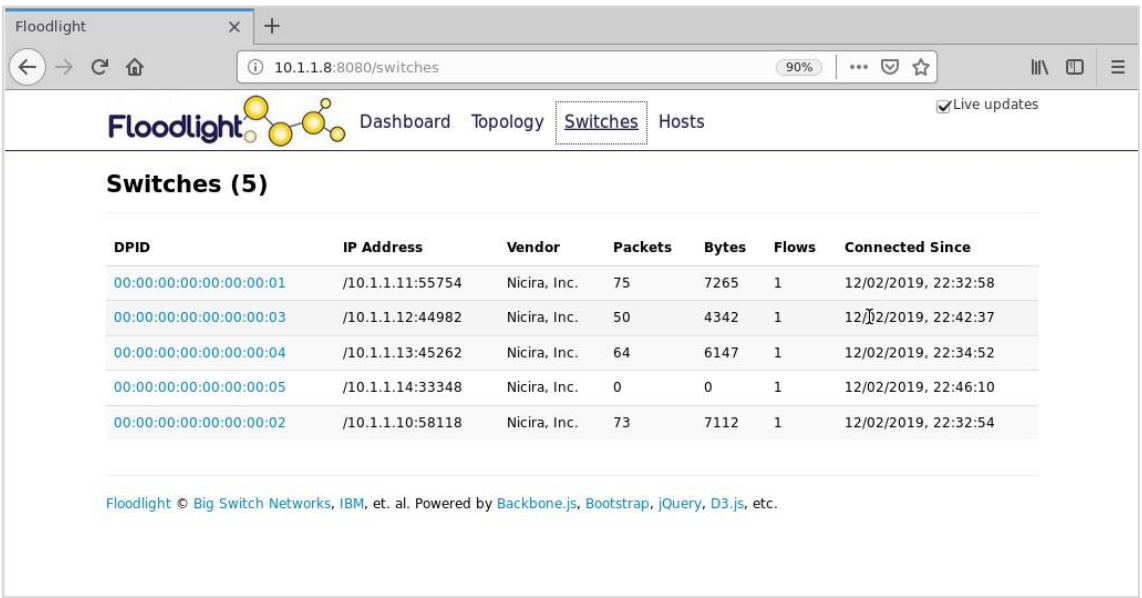

Figura 69. Pestaña de switches del controlador Floodlight
Fuente: Los Autores

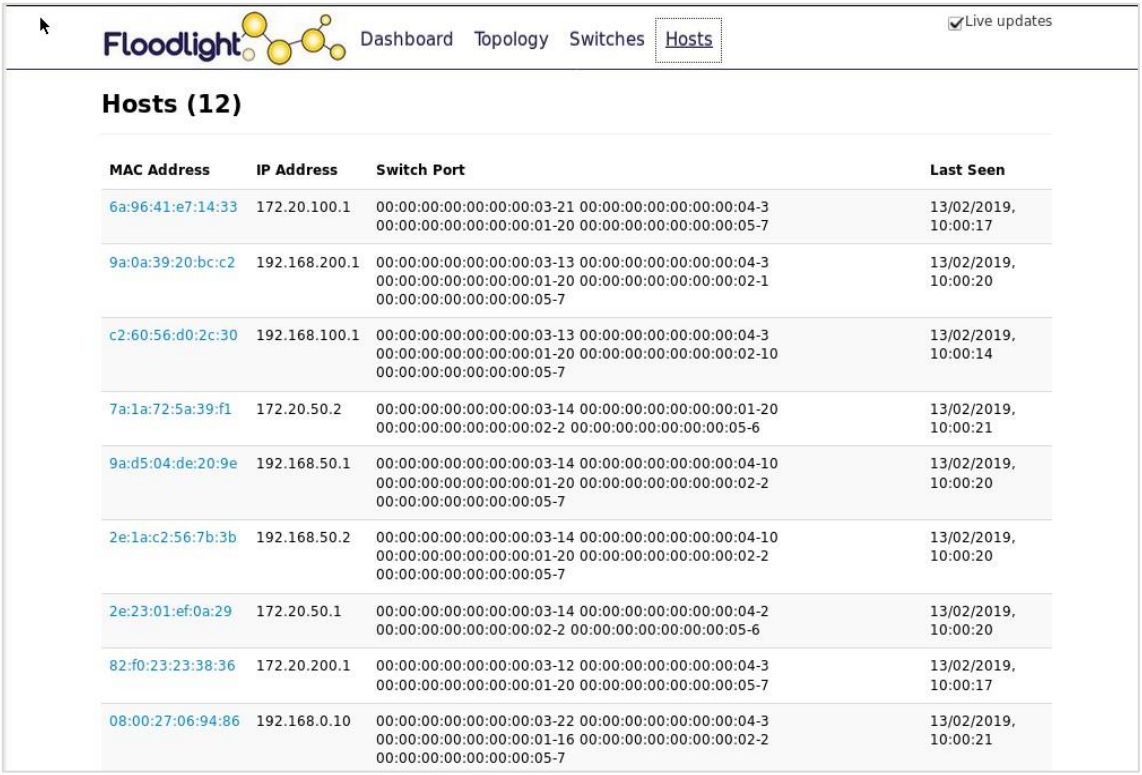

Figura 70. Pestaña de hosts del controlador Floodlight
Fuente: Los Autores

ANEXO 4: GLOSARIO

Active Networks: Iniciativa de investigaciones de lo que hoy son las SDN.

ApacheJmeter: Es un aplicación de código abierto desarrollada en java que sirve para realizar test de carga a sitios web, entre otras funciones.

DNS (Domain Name System): Sistema de Nombres de Dominio sirve para apuntar los dominios al servidor correspondiente, además para traducir la dirección IP, en el nombre del dominio correspondiente.

DMZ (demilitarized zone): Zona desmilitarizada o desprotegida, generalmente se refiere al área de servidores.

ESPAM MFL: Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López"

Estinet: Simulador de redes con características que favorecen la implementación de entornos Linux u redes SDN.

Ethane: Iniciativa de investigaciones de lo que hoy son las SDN.

Firmware: Es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Floodlight: Es un controlador para redes SDN basado en java y que es soportado por su comunidad de desarrolladores.

GNS3 (Graphic Network Simulation): Simulador gráfico de redes

Hipervisor: Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos

ICMP (Internet Control Message Protocol): El protocolo de control de mensajes de Internet es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP)

IEEE (*Institute of Electrical and Electronics Engineers*): Instituto de Ingeniería Eléctrica y Electrónica

IETF (*Internet Engineering Task Force*): Grupo de Trabajo de Ingeniería de Internet

ISO (International Organization for Standardization): Organización Internacional de Estandarización

ITU (*International* Telecommunication *Union*): Unión Internacional de telecomunicaciones

Jitter: Se denomina **jitter** o fluctuación del retardo a la variabilidad temporal durante el envío de señales digitales, una ligera desviación de la exactitud de la señal de reloj. El **jitter** suele considerarse como una señal de ruido no deseada.

Latencia de red: Es la suma de los retardos temporales en una red.

Mininet: Simulador y emulador de redes que sirve para probar implementaciones de redes SDN

Nagios: Sistema de monitoreo de redes.

NetFlow Generator: Herramienta que sirve para simular tráfico de netflow.

NFV (Network Function Virtualization): La Virtualización de las Funciones de Red son un complemento de las SDN y de otras tecnologías.

ns-3: es un simulador de redes basado en eventos discretos. Se usa principalmente en ambientes educativos y de investigación

Observium: Sistema de monitoreo de redes.

ONF (Open Networking Foundation): La Open Networking Foundation es una organización comercial sin fines de lucro

OpenDayLight: El proyecto OpenDayLight es un proyecto de código abierto de colaboración alojado por la Fundación Linux. El objetivo del proyecto es promover la creación de redes definidas por software y la virtualización de las funciones de red

OpenFlow: Es un protocolo que permite a un servidor decirle a los conmutadores de red adónde enviar paquetes

OpenFlow Manager: es una aplicación desarrollada para ejecutarse sobre OpenDayLight para visualizar topologías de OpenFlow (OF), programas de rutas y recopilar estadísticas de OF.

OpenWRT: Es un firmware de software libre para dispositivos de enrutamiento.

OSPF (Open Shortest Path First): Camino más corto primero, es un protocolo de red para encaminamiento jerárquico

Paradigma: Ejemplo o modelo de algo

Plano de control: Es el encargado de gestionar las rutas de los paquetes y las funciones de administración de los equipos.

Plano de datos: Se encarga del reenvío de los datos mediante procesos relacionados por el hardware.

Protocolo: Conjunto de reglas que se emplean en determinadas actividades

PTRG: Sistema de monitoreo de redes.

Red Tradicional: Manera de diseñar, implementar, configurar, y resolver problemas en las redes de computadoras en las que no se separa el plano de control del plano de datos.

Slowloris: El ataque del cliente HTTP Slowloris se basa en abrir muchas peticiones a un servidor web y lanza una petición que nunca acaba

Smokeping: es un monitor de latencias basado en RRDTool, mide el retardo de ICMP y varios servicios como: DNS, SSH, HTTP, SMTP, LDAP, entre otros.

SOFTNET: Iniciativa de investigaciones de lo que hoy son las SDN.

Software Defined Network – SDN: Redes definidas por software, son aquellas en las que se separa el plano de control del plano de datos y se gestionan de manera centralizada.

TLS (Transport Layer Security): protocolos criptográficos que proporcionan autenticación y cifrado de la información entre servidores, máquinas y aplicaciones que operan sobre una red

Zabbix: Sistema de monitoreo de redes.