Evaluación del rendimiento de una red LAN y una red WAN tradicional bajo el estándar IEEE 802.3 y la norma RFC 3031 en un entorno simulado, aplicando procesos SDN.

Daniel Stiven Quintero Londoño
Juan Diego Medina Rojas

Trabajo de grado presentado como requisito para optar al título de:
Ingeniero de Telecomunicaciones.

Asesor(es)
Msc. Bayron Jesit Ospina Cifuentes

Instituto Tecnológico Metropolitano - ITM
Facultad de Ingenierías
Departamento Antioquia
Medellín, Colombia
2021

RESUMEN

Este trabajo de grado evalúa el *performance* de una red basada en el estándar *IEEE 802.3* para la *LAN* y *RFC 3031* para la *WAN* con referencia en el estándar *ITU Y.1564* y *KPI* (Indicadores de rendimiento*)* establecidos sobre un entorno simulado. Actualmente muchas empresas solo tienen en cuenta un parámetro de medición que es la disponibilidad omitiendo los demás factores de medición que pueden impactar sus servicios y aplicaciones que funcionan sobre la red; es importante definir los *KPI* que permitan conocer el estado real con el objetivo de ofrecer una mejor percepción de calidad de servicio al usuario final, también, permitiendo cambiar el funcionamiento de administración de red de forma reactiva a preventiva. Se aplica una configuración basada en procesos de *SDN* (Redes definidas por software) sobre una red *legacy* (redes tradicionales), que permita conmutar los paquetes dependiendo la calidad de los enlaces para cumplir con las necesidades del negocio, garantizando la mayor disponibilidad y rendimiento. La configuración de red se apoya en el protocolo de enrutamiento *BGP*. Se implementa distintos *scripts* que permitan automatizar la evaluación de la red emulando procesos *SDN*, donde se pueda tener visibilidad del estado de la red por parte del centro de operación de red (*NOC*) o administrador para detectar proactivamente la presencia de incidencia, problema o cambio. La metodología en la que se desarrolla el proyecto es *Design Thinking*. A la red *legacy* y *overlay* se les realiza pruebas de rendimiento donde se obtienen resultados que, aunque son afectados por los recursos del computador se logra evidenciar mejores *KPIs*, *Jitter (6 ms inferior en la red legacy)* y *Bandwidth garantizando en promedio 1 Mbps* en la red *overlay y legacy 800 Kbps*. Al final del trabajo se anexa las diferentes configuraciones realizadas sobre los dispositivos, se realiza el análisis, comparación de las pruebas y los resultados.

Palabras clave: *KPI*, *Legacy*, *MPLS*, *Overlay*, *SDN*, Simulación.

RECONOCIMIENTOS

Queremos expresar nuestro agradecimiento primero a Dios por permitirnos tener la voluntad, la inteligencia y el coraje para emprender este proyecto, luego a nuestros familiares, esposas, padres y madres por su apoyo incondicional, sus sabios consejos, amor y siempre creer en nosotros, por último, a nuestro asesor de trabajo de grado Bayron Jesit Ospina por sus enseñanzas y largas jornadas de asesoría, también, a todas las personas que colaboraron en nuestra formación universitaria, profesores, jefes de programa, personal administrativo y académico del ITM.

ACRÓNIMOS

ARPANET Red de computadoras del departamento de defensa de Estados Unidos
ATM Modo de transferencia asíncrona
BGP Protocolo de puerta enlace de frontera
CEF Cisco Express *Forwarding*
CSMA/CD Acceso múltiple con detección de portadora y detención de colisiones
CSMA/CA Acceso múltiple con detección de portadora con evitación de colisiones
D-ITG Generador de tráfico para medir redes informáticas
DCSP Punto de código de servicios diferenciados
DMVPN Red privada virtual multipunto dinámica
DWDM Multiplexado denso por división en longitudes de onda.
FEC Clase de equivalencia de reenvío
GNS3 Simulador de red gráfico
IAAS Infraestructura como servicio
IBN Redes basadas en intención.
ICPM Paquete del protocolo IP que guarda información del tráfico IP.
IETF Grupo de trabajo de ingeniería de Internet.
IP Protocolo de internet.
IPERF Herramienta para hacer pruebas en redes informáticas.
IPSLA Medición de red IP activa.
ITU Unión Internacional de Telecomunicaciones.
IOT Internet d las cosas.
IWAN CISCO WAN Inteligente.
KPI Indicador Clave de rendimiento.

LAN Red de área Local.
LDP Protocolo de distribución de etiquetas.
MACA Acceso múltiple con prevención de colisiones.
MPLS Conmutación de etiquetas multiprotocolo.
NAT Traslaciones de direcciones de red.
*NBAR R*econocimiento de aplicaciones basado en red.
OSI Modelo de interconexión de sistemas abiertos*.*
PaaS Plataforma como servicio.
PERT-CPM Técnica de revisión y evaluación de programas.
PFR Encaminamiento del funcionamiento de CISCO.
RSTP Protocolo de prevención rápida de *loops.*
SasS Software como servicio.
SDH/SONET Red óptica síncrona.
SDN Redes definidas por software.
SD-WAN WAN Definida por Software.
SLA Acuerdos de niveles de servicio.
SSH *Secure Shell* programa de gestión remota.
SR Segment routing.
TDM Acceso múltiple por división de tiempo.
VLAN Virtual LAN.
VRF Enrutamiento virtual y de reenvío.
WAN Red de área amplia.
WAAS Servicios de aplicaciones de área amplia de CISCO.

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCIÓN

1.1 GENERALIDADES

Una red en informática es la interconexión de múltiples equipos sin importar su lugar físico con el objetivo de comunicarse entre sí para compartir datos y ofrecer servicios (cisco.com, 2020). Existen diferentes tipos de redes que se clasifican según su área geográfica de cobertura, una red *LAN* o de área local conecta equipos dentro de un área reducida como un edificio o habitación, por otra parte, una red *WAN* agrupa redes *LAN* que se encuentran en diferentes ubicaciones o lugares. Para establecer una comunicación se requiere vincular el *software* y aplicaciones terminales con el *hadware* y la infraestructura física, *Ethernet* es una tecnología para redes de datos que vincula el *software* y el *hardware*. *Ethernet* permite a través de cables de redes *LAN* el intercambio de datos entre equipos terminales, estos dispositivos establecen conexiones mediante protocolos de comunicación, el protocolo actual y más extendido para ello es IEEE 802.3 (ionos.es, 2018), sin embargo, el crecimiento de la Internet ha convertido al protocolo *IP* en el protocolo base en la redes de telecomunicaciones debido a que está en capa 3 del modelo *OSI* y únicamente está orientado a servicios y no a la conexión, requiere trabajar en conjunto con otros protocolos como *UDP* o *TCP* en la capa 4 del modelo *OSI* para que los paquetes puedan ser enviados, además, se requiere para garantizar altas necesidades de ancho de banda, calidad de servicio y mayores velocidades de conmutación en el nivel 2 del modelo *OSI* también conocido como capa de enlace, es por ello, que luego de trabajar sobre *ATM*, *SDH/SONET* y *DWDM* la *IETF* establece la RFC 3031 o también conocido como *MPLS* para unificar las soluciones de conmutación de nivel 2 y proporcionar características de redes orientadas a la conexión a redes no orientas a la conexión, al final entrega los beneficios de la ingeniería de tráfico del modelo IP, escalabilidad, diseños sencillos y opera sobre cualquier tecnología de nivel de enlace.

Las redes *WAN* tradicionales conectan usuarios ubicados en diferentes lugares con aplicaciones alojadas en servidores de centros de datos, garantizando seguridad y conectividad por medio de circuitos *MPLS*, pero con la llegada de la NUBE, los altos volúmenes de tráfico y requerimientos de calidad de servicio han aparecido nuevos conceptos como *SDN*, en esta tecnología se desvincula el control de la red del *hadware*, para ello, se le da a una aplicación o *software* las características para ser el controlador de

la red, de esta manera se logra manejar el tráfico de forma más flexible y eficiente en general para redes corporativas o empresariales con el propósito de cumplir los acuerdos niveles de servicio.

1.2 PROBLEMA ABORDADO Y JUSTIFICACIÓN

Cuando en las empresas no se cuantifica ni cualifica la calidad de prestación del servicio de la red y solo se mide la disponibilidad se realiza una medición superficial, omitiendo que también pueden ser afectados los servicios por degradaciones, intermitencias, saturaciones entre otras eventualidades que pueden generar retrasos de los procesos laborales, por lo tanto, no se tienen contractualmente definidos los parámetros *KPI* de medición para garantizar la calidad del servicio 7x24x365 o en el horario que se pacte en el acuerdo de prestación de servicio con los operadores correspondientes. Por ello, deben ser establecidos *SLA* donde se definan la calidad de servicio prestado, la forma de medir y evaluar el rendimiento que responda a las necesidades de cada compañía teniendo presente que pueden ser ajustados o modificados.

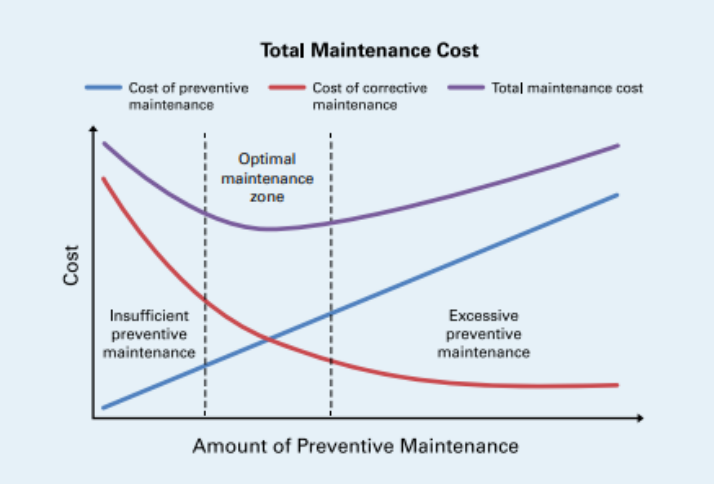
Al no tener definidos unos *SLA* que integren la calidad de prestación del servicio se omite las penalizaciones y sanciones contra el prestador del servicio por incumplimientos, lo que conlleva a posibles pérdidas de dinero o resarcimientos a las organizaciones, esto depende de la operación de cada empresa, por ejemplo, se puede establecer la multa por incumplimiento de los *SLA* técnicos como multa = días de atraso * valor mensual de servicios total* porcentaje máximo del valor del contrato (Web.integra.cl, 2014). La gestión de compensación y costos que deban asumir los proveedores de servicio depende de las condiciones de cada contrato.

Las organizaciones que tienen la idiosincrasia de realizar mantenimientos de forma reactiva y no preventiva ocasionan afectación en sus servicios, estos pueden ser evitados mediante uso del monitoreo, mantenimiento preventivo, correcta configuración de los dispositivos de red y evaluación de puntos de fallas. Para lograr esto es necesario integrar múltiples herramientas que permitan mantener una visibilidad en tiempo real del estado de la red, teniendo presente los estándares existentes; todo esto con el objetivo de brindar la mejor experiencia y calidad de servicio al usuario final.

Un estudio realizado en la revista *The Newsletter of Risktec Solutions* (Spring, 2017). Titulado "EMIT *Optimisation – Getting more out of existing equipment for less*" muestra la optimización de los costos de mantenimiento preventivo comparado con el correctivo como se observa en la Figura 1.

Figura 1.

Optimización de los costos de mantenimiento. Fuente: EMIT optimisation – getting more out of existing equipment for les (p. 1).



Nota: Se deduce que el costo total de mantenimiento es el costo de mantenimiento preventivo más el correctivo, también, que la zona de mantenimiento óptima es donde se logra el equilibrio de los dos costos.

Al realizar un mantenimiento preventivo se considera necesario en este proyecto una evaluación del rendimiento de una red *LAN* y *WAN* tradicional, además serán introducidos algunos aportes de conceptos de *SDN* con el propósito de mostrar las ventajas de conmutación que proveen estos nuevos conceptos junto con protocolos como *DMVPN* y *BGP*.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Evaluar el rendimiento de una red *LAN* y una red *WAN* tradicional (*legacy*) bajo el estándar IEEE 802.3 y la norma RFC 3031 en un entorno simulado, aplicando procesos *SDN*.

1.3.2 OBJETIVOS ESPECIFICOS

- Implementar la red *LAN* en el estándar IEEE 802.3 y la red *WAN* bajo la norma RFC 3031 en un entorno simulado bajo las plataformas GNS3, *Proxmox* o *Vmware* para aplicar procesos de *SDN* en redes *legacy*.
- Definir *SLA*, *KPI*, políticas de enrutamiento, procedimientos de monitoreo y administración de TI (Tecnologías de la información) que permitan una conmutación automática de la red.
- Evaluar el rendimiento de las redes diseñadas con referencia en el estándar ITU Y.1564 y *KPI* planteadas en el escrito bajo diferentes escenarios.
- Documentar los procesos, configuraciones y resultados obtenidos en el desarrollo del trabajo.

1.4 ORGANIZACIÓN DEL TRABAJO DE GRADO

Este proyecto tiene una fase inicial la cual incluye la introducción donde se exponen de forma general los temas importantes del proyecto, se aborda la problemática que se busca abordar y la justificación del proyecto, así como los objetivos del trabajo de grado. En la segunda fase del trabajo de grado se presenta el marco teórico donde se inicia con los antecedentes relevantes al proyecto, se expone cada uno de los temas que se consideran importantes para que el lector comprenda los términos y el cumplimiento de los objetivos. Luego se aborda las métricas, umbrales y *KPI* que serán evaluados según el estándar Y.1564,

se definen las políticas de enrutamiento, después se muestra el diseño e implementación de la red *WAN* y *LAN* del proyecto en la plataforma *GNS3*. Al final se muestran los resultados obtenidos en las pruebas con las herramientas de evaluación *IPERF* y *D-ITG* en la red *legacy* y aplicando conceptos de *SDN*. En la tercer y última fase del proyecto se presentan las conclusiones del proyecto, las recomendaciones y los trabajos futuros, así como las referencias tomadas en cuenta y se anexa los archivos de configuración.

2. MARCO TEÓRICO

2.1 ANTECEDENTES

Cuando hablamos de redes de área local los ingenieros de redes piensan en *Ethernet*, esta nació en 1970 cuando *Norman Abramson* trabajaba en *Alohanet*, posteriormente Robert Metcalfe en 1973 realizaba el trabajo de grado doctoral sobre cómo aumentar el rendimiento del protocolo *Aloha* y así comenzaría a forjarse la que con el tiempo sería la tecnología aceptada comercialmente como principal herramienta de interconexión de redes. (*Guimi*, 2009)

Los proveedores de servicio con el tiempo han aprovechado las ventajas de *Ethernet* para ofrecer servicios y se ha hecho necesario la evaluación con interfaces Ethernet que soportan hasta 25 *Gbps* y la monitorización de estas redes para cumplir con los servicios ofrecidos. Hoy en día no hay una palabra unánime o un protocolo estándar para la evaluación del rendimiento de redes *Ethernet* como se especifica en *UIT-T* Y.1563 o Y.1564. Antes de esta recomendación se utilizaba la "Metodología de evaluación comparativa de *IETF* para dispositivos de interconexión de red", también conocido como IETF RFC 2544. (*Davantel*, 2016)

Al principio de la década de 1990 la mayoría del tráfico de red se mantenía en la red *LAN* porque los servicios se agrupan en un edificio, por los enlaces *WAN* normalmente se transferían datos de servicios de correo o de acceso a Internet. Con el tiempo se ha visto un incremento en el tráfico *WAN* y principalmente hacia Internet debido al auge de aplicaciones en internet, nubes *IAAS*, *SasS*, *PaaS*, surgimiento de Movilidad, *IOT,* Video HD, Automatización, *Streaming*, Colaboración etc., a su vez ha evidenciado un aumento en la cantidad de usuarios o clientes conectados, por lo que se requieren mayores anchos de

banda y la necesidad de mejorar todas las tecnologías que ayudan a brindar la conectividad a estos servicios. (CISCO, 2019)

Debido a la necesidad y a las exigencias que los usuarios y empresas demandan cada vez más de las redes, *CISCO System* a través del tiempo también ha evidenciado la necesidad de mejorar y hacer más eficiente el proceso de *forwarding* en el *Router* con el objetivo de mejorar el rendimiento y disminuir la latencia de enrutamiento, hacia 1980 *Process Switching* era la técnica utilizada para enrutar paquetes, pero esta se basaba en realizar todo el proceso del reenvió (recorrer la tabla de enrutamiento *RIB*, identificar interfaz de salida y realizar el *frame rewrite* paquete por paquete utilizando los recursos de CPU (Software), lo cual hacia el proceso demasiado lento y poco óptimo. (Learningnetwork.com, 2019)

Por tal motivo se desarrolló *Fast Swtiching* el cual permitiría procesar el primer paquete (en CPU) y los resultados de su búsqueda almacenarlos en cache, para ser utilizados en paquetes posteriores (Tabla de reenvío de *Hardware*), con ello se reducían los tiempos de cálculo y se optimiza el uso de recursos; este método, aunque mejoraba el proceso de reenvió, tenía carencias que lograban impactar en la latencia de enrutamiento debido a que cuando había un aumento de paquetes con destinos desconocidos se tiene que realizar *process switching* con el primer paquete y volver almacenar en cache la búsqueda, además que después de un tiempo se refresca el cache de los equipos. (CISCO.com, 2005)

Por las limitantes que se presentaron en *Fast Switching* y teniendo en cuenta que el proceso que impacta significativamente los recursos del dispositivo es la búsqueda del mejor camino para un destino, teniendo presente que en el proceso debe identificar interfaz de salida y realizar *frame rewrite*, fue necesario innovar hacia el método *CEF*.

Las tecnologías de la *WAN* también han presentado una evolución demasiado importante, todas con el objetivo de brindar una mayor eficiencia en la red y satisfacer las necesidades que los usuarios han ido generando; iniciando desde la conmutación por circuitos hasta utilizar la conmutación de paquetes. Desde la aparición de *ARPANET* (1969), posteriormente se utilizó la multiplexación por división de tiempo *TDM* (1985), luego se crearon dos tecnologías a nivel de transporte en capa 2 muy significativas como fueron *Frame Relay* (1990) y *ATM* (1995), siendo consideradas la primera evolución de la *WAN*, debido a que permitían la conmutación de paquetes. *MPLS LDP* (2005) el estándar que marcó significativamente y se convirtió fundamental en las redes de transporte para permitir una conectividad más eficiente, apoyándose de la capacidad de programación ofrecida por la capa 3 y la rapidez de la capa 2, el cual fue mejorado con *Seameless MPLS (*2010).

Debido a la necesidad de identificar y utilizar mejor los recursos a nivel *WAN* y siendo considerado una evolución natural, se desarrolló *IWAN* el cual es un compendió de múltiples tecnologías que permiten hacer más eficiente la *WAN* y brindan inteligencia al reenvió de paquetes. Gracias a ello surgió *SDN* (redes definidas por software) donde ya se intenta abarcar una mejora en la transmisión de datos, que a la vez logre facilitar la implementación de redes *LAN* (*SD-ACESS*) y *WAN* (*SD-WAN*), está tecnología va muy de la mano del tema de programación de redes. Ligado a esto nace *Segment Routing* para la red de transporte con lo cual se logra una mayor eficiencia que la ofrecida por *MPLS*.

La importancia de las tecnologías *SDN* reside en permitir soluciones a los problemas de aumento de consumo de ancho de banda, optimización de la conectividad y aplicaciones en la nube, seguridad de la *WAN* y automatización con administración por separado del plano de datos del de control. Todas estas tecnologías han sido mostradas a partir del nuevo siglo alguna de ellas CISCO como *Meraki SD-WAN*, *IWAN* y *Viptela*, sin embargo, la industria de las telecomunicaciones continúa utilizando implementaciones tradicionales.

Actualmente se viene abordando el nuevo concepto de redes *IBN* (redes basadas en intención o intuitivas) (2019) y a nivel de la red de transporte *SRv6* (*VXLAN*, *OTV* y *EVPN* se convierten en tecnologías desfasadas para *SRv6*) (2019) la cual es basada completamente en IPv6.

2.2 MÉTRICAS, UMBRALES Y KPI

Los *KPI* son características que indican el rendimiento mínimo que debe tener el tráfico. Los *KPI* que se abordan en el trabajo de grado son el *Jitter*, *Bandwidth*, retraso de ida y vuelta (*RTT*) y pérdida de paquetes.

Se define a nivel numérico el funcionamiento de la infraestructura de red que no se debe superar o se debe garantizar, con el objetivo de brindar una correcta prestación de servicios y aplicaciones de acuerdo con los siguientes parámetros.

2.2.1 CRITICIDAD DEL NEGOCIO

Es definido con la intención de categorizar las diferentes severidades de las sucursales, está debe estar basada en el impacto que genere a la entidad o empresa que contrata un servicio; se definen las severidades de sucursales o sedes así:

0: *Centro de datos*.

1: Sucursales de volumen crítico de operación.

2: Sucursales de volumen medio de operación.

3: Sucursales de impacto bajo en la operación.

2.2.2 TIPOS DE SITIO POR ZONA GEOGRÁFICA

Se definen las zonas de acuerdo con la ubicación de las sedes así:

Zona 0: Son las sedes ubicadas áreas metropolitanas y ciudades capitales

Zona 1: Son las sedes ubicadas en ciudades secundarias de cada departamento

Zona 2: Son las sedes ubicadas en las demás ciudades del país.

Se definen a continuación las métricas de medición de servicio con respecto a disponibilidad de servicio, *RTT* (*Round Trip Delay*), ancho de banda, pérdida de paquetes y *Jitter*.

2.2.3 JITTER

La fluctuación de paquete (*Frame Delay Variation*) o más conocido en inglés como *Packet Jitter* hace referencia a la variabilidad en el tiempo de llegada de paquetes. Cuando los paquetes viajan a través de una red a menudo se ponen en colas y se envía en ráfagas hacia el próximo salto lo que resulta en trasmisiones aleatorias y recepciones en intervalos irregulares, su valor aceptable para datos se establece en menores a 10 milisegundos. En la Tabla 1 se muestra los valores de *Jitter* definidos.

Tabla 1

Tabla de Jitter. Fuente: Autores

Tipo	*Zona 0*	*Zona 1*	*Zona 2*
Voz	<=3 ms	<=5 ms	<=8 ms
Datos	NA	NA	NA

Nota: Los tiempos de Jitter se expresan en milisegundos

2.2.4 BANDWIDTH (ANCHO DE BANDA)

El ancho de banda o *Bandwidth* es la cantidad de datos o información que puede transportarse por una red en un instante de tiempo determinado, normalmente la unidad de medida de los datos es el *bit* o los *bytes* y se expresa el ancho de banda en *Mbps* (*Megabits* por segundo) o *Kbps* (*Kilobits* por segundo). Por razones prácticas se define un ancho de banda máximo de un *Megabit* en la red simulada para evitar saturación o perdida de información por capacidad de los recursos disponibles. Los valores de configuración de *Threshold* definidos se muestran en la Tabla 2.

Tabla 2

Tabla de Threshold. Fuente: Autores

Parámetro	*Threshold*	*Duration*
Inbound Utilization	80%	300 sec (5 min)
Outbound Utilization	80%	300 sec (5 min)
In Errors	2%	300 sec (5 min)
Out Errors	2%	300 sec (5 min)
In Discarded	5%	300 sec (5 min)
Out Discarded	5%	300 sec (5 min)

2.2.5 RETRASO DE IDA Y VUELTA (RTT)

El *RTT* se define como el tiempo transcurrido en milisegundos que un paquete IP de 100 *bytes* toma en el tránsito de ida y vuelta entre dos sitios que pertenecen a la misma red *MPLS*, esto se ilustra en la tabla 3.

Tabla 3

RTT. Fuente: Autores

Tipo	RTD (ms) Zona 0	RTD (ms) Zona 1	RTD (ms) Zona 2
Datos	<100	<100	<200

Nota: Los tiempos de RTT se expresan en milisegundos

2.2.6 PÉRDIDA DE PAQUETES

La pérdida de paquetes es el máximo número de paquetes perdidos por extremo, con relación a la totalidad transmitida, por unidad de tiempo.

La pérdida de paquetes se define como la relación entre la cantidad de paquetes entregados por la red del oferente para su recepción y la cantidad total de paquetes enviados por protección a la red, medidos por enlace en forma porcentual, se definen de acuerdo con su prioridad como se muestra en la Tabla 4. Su fórmula de cálculo es:

(cantidad de paquetes perdidos / cantidad de paquetes transmitidos) *100

Tabla 4

Pérdida de paquetes. Fuente: Autores

Tipo	Pérdida de Paquetes
Datos Prioridad Alta	<=0.1%
Datos Prioridad Media	<=0.5%
Datos Prioridad Baja	<=0.7%
Datos Mejor Esfuerzo	<=1.0%

2.3 MONITOREO

El monitoreo es un servicio clave en telecomunicaciones, debido a que permite cumplir con el objetivo de supervisar los equipos y servicios aprovisionados, además que ayuda a asegurar el *performance* y cumplimiento de los niveles de servicios acordados (*SLAs*), debe contar con la notificación y escalamiento a un centro de gestión, realizar diagnósticos iniciales y brindar acciones necesarias para normalizar los servicios.

Para poder realizar el monitoreo de red, supervisión de rendimiento y administración de red es necesario implementar una serie de herramientas (*hardware*/*software*) y protocolos, que permitan cumplir con múltiples características que se deben tener:

- Monitoreo del 100% de dispositivos de telecomunicaciones.
- Monitoreo de red de extremo a extremo.
- Detección proactiva y reactiva de fallas.
- Identificación ágil y eficaz de puntos de fallas.
- Monitoreo de performance (*RDD*, *Jitter*, *Packet Loss*, *Bandwith Througput*).
- Permita realizar mediciones de *performance*.
- Detección de degradación de servicio o desvió de la calidad en el servicio de red respecto a los niveles de servicio pactado.
- Análisis de tráfico.
- Contar con alertas de incidentes y eventos, las cuales sean notificados utilizando algún medio como *sms (mensaje de texto)*, e-mail o web.
- Generación de informes y que mantenga una data histórica no inferior a 6 meses.
- Almacenamiento de *logs (registros de eventos)*.
- Gestión centralizada de *Backups* y archivos de configuración de los dispositivos de red.

(Autores,2021).

2.4 ADMINISTRACIÓN DE TI

Las personas administradoras de TI son las encargadas de realizar tareas de mantenimientos proactivos, mantenimientos correctivos, verificación, pruebas operativas y de *performance* sobre toda la infraestructura con el objetivo de garantizar el correcto funcionamiento en todo momento de los servicios, además deben cumplir con la atención, análisis, hallazgo de causa raíz y brindar una solución definitiva de los incidentes y problemas que suceden sobre las plataformas de telecomunicaciones.

Para realizar una correcta administración se debe contar con tareas de soporte y actividades de mantenimiento de la infraestructura, además de disponer con las herramientas adecuadas; siempre buscando garantizar los niveles de servicio requeridos.

Entre las tareas a realizas son:

- Gestionar incidentes y solicitudes escalados.
- Soporte y configuración de equipos de red (*Swiches*, *Router*).
- Garantizar la disponibilidad de los servicios de *LAN* de acuerdo con los marcos de calidad y niveles de servicio acordados con la empresa.

- Solucionar los problemas relacionados con los ámbitos *LAN* en el menor tiempo posible.
- Identificación de fallas, causa raíz e implementación de soluciones definitivas.
- Elaborar y presentar los informes.
- Diseño y mejora de balanceo de tráfico entre canales *WAN*.
- Actualización de *IOS* de los dispositivos de red.
- *Backup* de la configuración de los equipos de red.
- Análisis de vulnerabilidades a nivel de red (Topología, Esquemas recomendados (Buenas prácticas según el fabricante)).
- Análisis de esquemas de seguridad para el acceso y funcionamiento de la red (*ACLs*, Acceso SSH, Integración *Radius*, 802.1x).

(Autores,2021).

2.5 EVALUACIÓN Y ANALISIS DEL RENDIMIENTO DE REDES ETHERNET

Son actividades realizadas por los administradores de redes, las cuales pueden ser pruebas activas y pasivas, el objetivo es determinar el estado de rendimiento de la red a nivel de enlaces, dispositivos y cableados, para garantizar el cumplimiento de los acuerdos de niveles de servicios contratados.

Las pruebas activas consisten en inyectar tráfico dentro de la red o enviar paquetes a servidores para validar los tiempos de respuesta, el *throughput*, variación de llegada de paquetes, entre otros parámetros.

Las pruebas no invasivas o pasivas son análisis de flujos de tráfico y escucha de tráfico sin realizar la modificación de ningún parámetro y sin enviar paquetes.

Luego de realizar las pruebas deben ser analizadas y comparadas estas con la métricas y umbrales establecidos para determinar el *performance* de la infraestructura y determinar si es requerido algún mantenimiento correctivo o preventivo.

2.5.1 RECOMENDACIÓN UIT-T Y.1564

Y.1564 define una metodología para probar servicios basados en *Ethernet* en la etapa de activación del servicio, se aplica a la conectividad punto a punto y punto a multipunto, no define arquitecturas de red *Ethernet* o servicios y supone un equipo de prueba dedicado a las metodologías de pruebas.

En la recomendación, el ancho de banda está referido al perfil de ancho de banda y los parámetros (*SLA*) que están referidos al criterio de aceptación del servicio (SAC). (ITU, 2016)

2.5.2 PRUEBAS ADICIONALES

Se consideran pruebas adicionales las que están por fuera de las recomendadas en la UIT Y.1564, ya que estas no proporcionan información necesaria para que un servicio no funcione como se esperaba en la capa de transporte o 4 del modelo OSI. El IEFT y varios proveedores de servicio trabajaron en un marco estandarizado para las pruebas de rendimiento TCP, dicha metodología fue estandarizada en la RFC 6349. En caso de requerir conocer la causa de un mal rendimiento en capas superiores del modelo OSI, se dispone de herramientas como *iPerf* y *D-ITG*. (Autores,2021)

2.6 REDES

Se contempla la descripción de los tipos de redes presentes en el proyecto.

2.6.1 RED UNDERLAY

Es la red base física de la red *overlay*, en la cual se basa la conectividad para el soporte del transporte de los datos.

2.6.2 RED LEGACY

Es la red tradicional la cual está conformada por equipos activos, enrutadores, *switchs*, equipos terminales y protocolos de red con la intención de ofrecer conectividad o comunicación en áreas de trabajo.

2.6.3 RED OVERLAY

Estará conformada por túneles *DMVPN, VRF* y protocolos de enrutamiento, con el objetivo de mantener el plano de control y plano de datos, permitiendo la segmentación de tráfico.

2.6.7 MPLS

MPLS se define como un protocolo de conmutación de etiquetas, aunque esto no quiere decir que no pueda transmitir o recibir paquetes IP nativos si una interfaz tiene activo el protocolo. Este ofrece soporte de redes privadas virtuales (*VPN*), ingeniería de tráfico (TE), *QoS* y (*AToM*).

Para la implementación de redes *MPLS* se escogen principalmente protocolos de *Links-State* (Estado de enlace) como *OSPF* (*Open Shortest Path First*) porque este permite a los nodos tener información completa de la topología y además brinda información a *LDP* (*Label Distribution Protocol*) para poder crear y anunciar los *label bindings* (etiquetas), la creación de etiquetas depende de los prefijos aprendidos en la tabla de enrutamiento del dispositivo; *BGP* (*Border Gateway Protocol*) tiene su propio mecanismo interno de distribución de etiquetas. (CISCO, 2005).

2.6.7 SDN

Las *SDN* (redes definidas por *software*) que a diferencia de las redes tradicionales separan el plano de control del plano de datos y utilizan un controlador o equipo de gestión centralizado (*Feamster*, 2013).

Más allá de esta importante ventaja que define el futuro y presente de las redes, las redes definidas por *software* permiten que cada dispositivo aprenda y tome decisiones de reenvió de tráfico, definidas por los controladores, políticas de enrutamiento y estado del

performance de los enlaces, además de la administración desde un equipo central, programabilidad y despliegue rápido de nuevas soluciones.

2.7 DIAGRAMA LÓGICO DE LA RED OVERLAY Y LEGACY

Se presenta en la Figura 2 el diagrama lógico de la red *legacy* y en la Figura 3 el diagrama lógico de la red *overlay*, en esta se presenta una *WAN MPLS* conformada por un *router* P (*Provider Router*) central y cuatro *router* PE (*Povider Edge*) de frontera, además, se tendrán dos sedes, una el centro de datos y otra la sede principal con las redes *LAN* que serán descritas en otros capítulos.

Figura 2

Diagrama lógico de la red Legacy. Fuente: Autores.

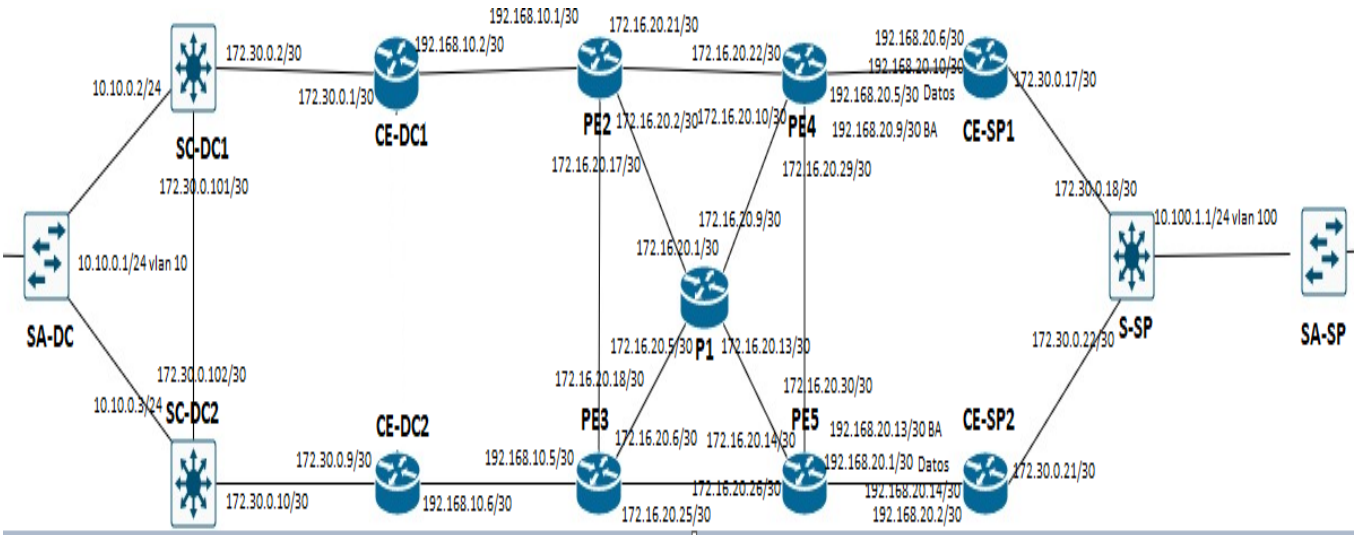
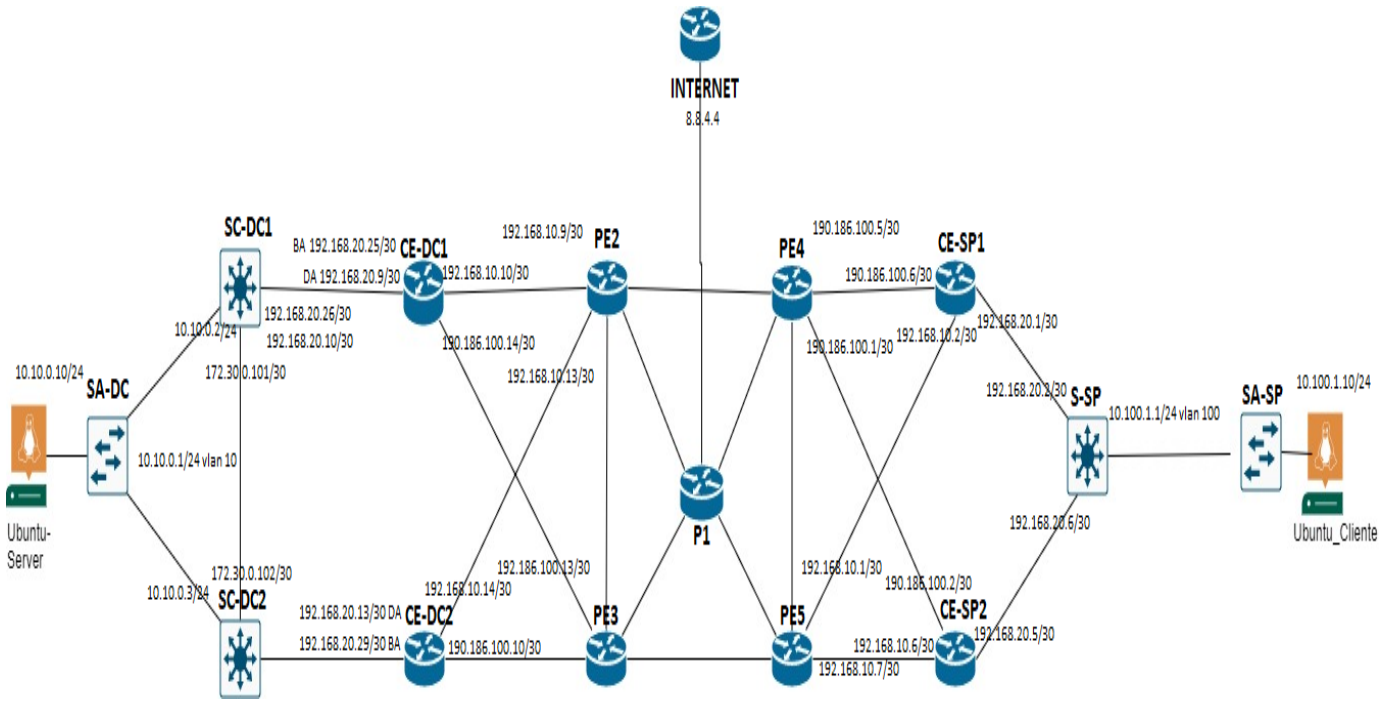


Figura 3

Diagrama lógico de la red Overlay. Fuente: Autores.



2.8 DISEÑO DE LA RED WAN

Se realiza el planteamiento de una solución la cual proporciona una plataforma de red *WAN* con conceptos de *SDN*, que permita a las empresas implementar una arquitectura escalable, segura y enfocada a cumplir los objetivos del negocio.

2.8.1.1 PLANO DE CONTROL

Es la configuración de una *VRF* por la cual se transporta el tráfico de gestión de los *routers* donde se permita la administración central, separando del tráfico de datos del usuario.

2.8.1.2 PLANO DE DATOS

Es una malla de túneles *IPSec* punto a punto entre los enrutadores, estos túneles se forman automáticamente entre los nodos en la red, los enrutadores crean dinámicamente las claves de cifrado *IPSec* locales que se distribuyen a los otros *router* y las cuales se cambian dinámicamente en ciertos intervalos de tiempo.

Cuando los paquetes destinados a la *LAN* se reciben en un túnel de los *router*, los paquetes se descifran y se enrutan al segmento de *LAN* correspondiente.

El comportamiento de la malla completa podría ser restringido a atreves de configuraciones, mediante la cual se limitará enlaces en la malla.

El enrutamiento se realizará mediante el protocolo *BGP* hacia la red *overlay* y hacia la red LAN, para permitir redistribución automática de las siguientes rutas que se aprenden localmente o de sus pares de enrutamiento del lado de servicio:

- Conectadas.
- Estáticas
- Rutas dinámicas.

2.8.2 DEFINICIÓN DE *VRF* PARA LA SOLUCIÓN PROPUESTA

Para poder cumplir con las soluciones propuestas es requerido una segmentación granular de tráfico mediante el uso de *vrf*. Cada *vrf* descrita en la Tabla 5 tiene su propia tabla de reenvió que proporciona aislamiento dentro del *router*; con lo cual se puede imponer una separación inherente entre servicios, transporte y administración.

Tabla 5

VRF. Fuente: Autores.

Nombre de *vrf*	**Descripción**
lan-corporativa	Data/voz/video

global	Tráfico de internet

2.8.3 POLÍTICAS DE ENRUTAMIENDO DE APLICACIONES

Para optimizar el rendimiento de los servicios y mejorar la experiencia de usuario en las aplicaciones de voz, datos y video, es requerido la clasificación, marcado, asignación de ancho de banda, priorización de aplicaciones, selección de rutas según los acuerdos de nivel de servicio (*SLA*) e ingeniería de tráfico, configuradas en los *CEdge* de cada sede. Estas políticas son configuradas para influir y establecer preferencias de rutas en las tablas de reenvió y toma de decisiones de enrutamiento en los enrutadores *CEdge*, están basadas en la aplicación según la clasificación del tráfico y el marcado *DCSP (Differentiated Services Code Point)*, para selección de la mejor ruta determinada según los requisitos de *KPI* especificados en el documento, los cuales son *Jitter*, *RTT* y ancho de banda.

Teniendo presente que ciertas aplicaciones son más sensibles a los niveles de deterioro de transporte *WAN*, es beneficioso seleccionar ciertas rutas para este tipo de tráfico, por tal motivo se preferirá el tráfico de video y *VoIP* en la ruta de *MPLS* que garantiza los *SLA* para el tráfico en tiempo real, mientras el tráfico masivo como correo electrónico o acceso a recursos compartidos funcionarían bien en la ruta de Internet.

2.9 DESCRIPCIÓN DE SOLUCIÓN RED LAN SEDE PRINCIPAL UNDERLAY Y OVERLAY

La solución propuesta para la red LAN, es una infraestructura *underlay* sin aplicar conceptos de *SD-ACCES* (LAN definida por software), *IBN* y seguridad como CISCO ISE (*CISCO Identity*

Services Engine) donde se tiene políticas centralizadas de acceso a la red, porque desborda el alcance del trabajo de grado, pero si buenas prácticas para garantizar disponibilidad y escalabilidad, con el objetivo de cumplir a los *SLAs* contratados por las empresas.

Para la red *overlay* se aplicarán los siguientes conceptos en el diseño de las redes con el objetivo de garantizar siempre el cumplimiento de los acuerdos de niveles de servicio y *KPI* contratados como la utilización de *embedded event manager (EEM)*, el cual es un subsistema que permite identificar eventos de red en tiempo real y automatización integrada en dispositivos *CISCO*, *Spanning-tree portfast* en un *switch* para cambiar rápidamente del estado *blocking* al modo de *forwarding* saltándose los estados *listenning* y *learning*, a su vez el protocolo de enrutamiento dinámico *BGP* que permite manipulación de las tablas de enrutamiento mediante la utilización de los atributos que este brinda y la implementación de túneles *DMVPN*. En la red LAN se emula un dispositivo VSS que permite que dos equipos físicos independientes sean vistos como una sola entidad lógica, brindando una mayor eficiencia administrativa y disponibilidad de red.

2.10 LAN CENTRO DE DATOS UNDERLAY Y OVERLAY

Actualmente las empresas pueden contratar servicios de *collocation* y *hosting* en los centros de datos de terceros dedicados a ofrecer un excelente desempeño, además de los múltiples servicios ofertados en *cloud*; debido a las ventajas que estos ofrecen, que son costosas para ser asumidas en una implementación por las compañías, se puede validar las ofertas brindadas a nivel de centro de datos teniendo en cuenta la calificación *TIER* (Sistema de clasificación de centros de datos inventado por *uptime institute*) y las necesidades de la organización. A nivel de red en el centro de datos sería una excelente opción que cuente con una arquitectura *spine* and *leaf* que mejora el rendimiento de *switching* de paquetes y

permite la utilización de todos los enlaces al no hacer uso del protocolo *STP* para evitar bucles de capa 2.

La red *LAN* de *Centro de datos underlay* que se configura para el desarrollo del trabajo de grado, es una arquitectura de *core* colapsada, con protocolo de enrutamiento *BGP*, *spanning tree* y protocolo *HSRP* para darle redundancia de puerta de enlace, con el objetivo de realizar la simulación, debido a que no es fácil simular una arquitectura *spine* and *leaf* debido a los equipos y licenciamientos requeridos.

Para la red *overlay* se implementa la tecnología de CISCO *EEMM*, *IPSLA* y túneles *DMVPN*, con el objetivo de brindar mayor *performance,* control de tráfico y resiliencia ante fallas.

2.10.1 VLAN Y DIRECCIONAMIENTO DEL CENTRO DE DATOS

Se configurarán *VLAN* como se muestra en la Tabla 6 debido a que nos permite mitigar el riesgo de tormentas de *broadcast*, brindan seguridad y se pueden asignar por tipo de tráfico.

Tabla 6

Vlan sede centro de datos. Fuente: Autores.

Descripción	VLAN ID
***Vlan* Servidores de producción**	10
***Vlan* de servidores de pruebas**	20
***Vlan* de servidores de desarrollo**	30
***Vlan* de replicación**	40

***Vlan* de gestión**	50
***Vlan* WAN**	60

En la tabla 7 se presenta el direccionamiento IP de la sede del centro de datos relacionada con la *vlan* correspondiente en el *Centro de datos*.

Tabla 7

Direccionamiento IP redes del Centro de datos. Fuente: Autores.

Direccionamiento IP	Mascara	*Vlan*
10.10.0.0	255.255.255.0	10
10.11.0.0	255.255.255.0	20
10.12.0.0	255.255.255.0	30
10.13.0.0	255.255.255.0	40
10.14.0.0	255.255.255.0	50
172.30.0.0	255.255.255.248	60

2.9.5.5 VLAN Y DIRECCIONAMIENTO DE LA SEDE PRINCIPAL

Se configurarán *vlan* para la sede principal que se muestran en la Tabla 8.

Tabla 8

VLAN sede principal. Fuente: Autores

Descripción	VLAN ID	Observación
***Vlan* usuarios**	100	*Vlan* de datos por piso

***Vlan* de voz**	110	*Vlan* de voz por piso
***Vlan* de gestión**	120	General
***Vlan* de CCTV**	130	General
***Vlan* de servidores**	140	General

En la Tabla 9 se muestra el direccionamiento asociado en la *LAN* de la sede principal para cada *vlan* configurada.

Tabla 9

Direccionamiento IP de la sede principal. Fuente: Autores.

Direccionamiento IP	Mascara	Descripción	*Vlan*
10.100.1.0	255.255.255.0	Red usuarios Piso 1	100
10.100.2.0	255.255.255.0	Red voz piso 1	110
10.100.100.0	255.255.255.0	Red de gestión	120
10.100.101.0	255.255.255.224	Red CCTV	130
10.9.0.0	255.255.255.0	Red *loopbacks*	
172.30.0.16	255.255.255.252	Red WAN	60

2.10 DESARROLLO DE DMVPN

Se definen los *router* CE-DC1 y CE-DC2 como *DMVPN Hub*, donde se crean los túneles para el canal de datos e Internet para comunicarse con los *router* CE-SP1 y CE-SP2 por el transporte del túnel. Las configuraciones que se mostrarán a continuación para CE-DC1 también aplican para CE-DC2. Se debe identificar la interfaz de origen del tráfico del túnel, configurar el túnel como un túnel *GRE* multipunto, asociar la IP local del transporte, habilitar *NHRP* sobre los túneles y si desea, se le puede añadir seguridad mediante llaves de conexión *Ike* e *IPsec*.

Se debe asociar la interfaz de cada túnel *DMVPN* a la *VRF* local del servicio para la actualización de las tablas de enrutamientos locales y eliminar los problemas de enrutamiento recursivo. Por ello, dentro de cada túnel se asocia un *vrf forwarding* a la *vrf lan-services*.

Previamente se debe configurar el enrutamiento en todos los *router* de la red y debe estar configurado el *core MPLS*. Se utilizan rutas por defecto hacia los *router* P del *core MPLS* y se crea un *NAT* (*Network Address Translation*) para la conexión hacia Internet, a su vez, los *router* CE y P tienen establecidas sesiones *BGP* para el intercambio de prefijos de red donde se redistribuyen los prefijos directamente conectados y estáticos.

La configuración de *DMVPN* del proyecto se muestra en la Figura 4 y 5.

Figura 4

Configuración DMVPN Hub en CE-DC1. Fuente: Autores.

```
interface Tunnel0
 description To-DMVPN-DATOS
 vrf forwarding lan-service
 ip address 172.30.0.1 255.255.255.248
 no ip redirects
 ip mtu 1440
 ip nhrp map multicast dynamic
 ip nhrp network-id 111
 ip nhrp redirect
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet1/0.1500
 tunnel mode gre multipoint
interface Tunnel1
 description To_DMVPN-INTERNET
 vrf forwarding lan-service
 ip address 172.30.0.9 255.255.255.248
 no ip redirects
 ip mtu 1440
 ip nhrp network-id 222
 ip nhrp redirect
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet2/0.1600
 tunnel mode gre multipoint
```

Figura 5

Configuración BGP en CE-DC1. Fuente: Autores.

```
router bgp 65100
 bgp router-id 10.9.0.4
 bgp log-neighbor-changes
 neighbor 192.168.20.26 remote-as 65300
 neighbor 192.168.20.26 version 4
 neighbor 192.168.20.26 timers 11 33
 !
 address-family ipv4
  neighbor 192.168.20.26 activate
  neighbor 192.168.20.26 default-originate
  neighbor 192.168.20.26 allowas-in
  neighbor 192.168.20.26 soft-reconfiguration inbound
 exit-address-family
 !
 address-family ipv4 vrf lan-service
  redistribute connected
  redistribute static
  neighbor 172.30.0.2 remote-as 65001
  neighbor 172.30.0.2 version 4
  neighbor 172.30.0.2 timers 11 33
  neighbor 172.30.0.2 activate
  neighbor 172.30.0.2 default-originate
  neighbor 172.30.0.2 soft-reconfiguration inbound
  neighbor 172.30.0.10 remote-as 65001
  neighbor 172.30.0.10 version 4
  neighbor 172.30.0.10 timers 11 33
  neighbor 172.30.0.10 activate
  neighbor 172.30.0.10 default-originate
  neighbor 172.30.0.10 soft-reconfiguration inbound
  neighbor 192.168.20.10 remote-as 65300
  neighbor 192.168.20.10 version 4
  neighbor 192.168.20.10 timers 11 33
  neighbor 192.168.20.10 activate
  neighbor 192.168.20.10 soft-reconfiguration inbound
 exit-address-family
'
```

En la Figura 6 se muestra la configuración de rutas por defecto y *NAT* para la conectividad por el túnel de internet.

Figura 6

Rutas por defecto y NAT en CE-DC1. Fuente: Autores.

```
ip nat translation timeout 5400
ip nat inside source list Cx-Internet interface GigabitEthernet2/0.1600 overload
ip route 0.0.0.0 0.0.0.0 190.186.100.13 name INTERNET
ip route 192.168.10.0 255.255.255.0 192.168.10.9 name DATOS
ip route vrf lan-service 0.0.0.0 0.0.0.0 192.168.20.10 name Default
'
```

Para la configuración del cliente *DMVPN* se debe probar conectividad en la red *Overlay* y se configura una IP de transporte para el túnel correspondiente como se muestra en la Figura 7.

Figura 7

Configuración de túnel DMVPNl cliente en CE-SP1

```
interface Tunnel0
 description To-DMVPN-DATOS
 vrf forwarding lan-service
 ip address 172.30.0.2 255.255.255.248
 no ip redirects
 ip mtu 1440
 ip nhrp map 172.30.0.1 192.168.10.10
 ip nhrp map multicast 192.168.10.10
 ip nhrp network-id 111
 ip nhrp nhs 172.30.0.1
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet1/0.1500
 tunnel mode gre multipoint
!
interface Tunnel1
 description To-DMVPN-INTERNET
 vrf forwarding lan-service
 ip address 172.30.0.10 255.255.255.248
 no ip redirects
 ip mtu 1440
 ip nhrp map 172.30.0.9 190.186.100.14
 ip nhrp map multicast 190.186.100.14
 ip nhrp network-id 222
 ip nhrp nhs 172.30.0.9
 ip nhrp shortcut
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet2/0.1600
 tunnel mode gre multipoint
```

2.11 DESARROLLO DE IPSLA

Con *IPSLA* (*Internet protocol service level agreement*) se busca medir los parámetros de *KPI* establecidos, así como verificar las mejores rutas debido a la degradación de uno de estos parámetros. La configuración se muestra en la Figura 8.

Figura 8

Configuración IPSLA en CE-SP1. Fuente Autores.

```
ip sla auto discovery
ip sla 10
 icmp-echo 172.30.0.1 source-interface Tunnel0
 vrf lan-service
 frequency 300
 timeout 1000
 threshold 150
ip sla schedule 10 life forever start-time now
ip sla 11
 udp-jitter 172.30.0.1 16384 source-ip 172.30.0.2 num-packets 20
 tos 46
 vrf lan-service
 frequency 300
 timeout 1000
 threshold 100
ip sla schedule 11 life forever start-time now
ip sla 20
 icmp-echo 172.30.0.9 source-interface Tunnel1
 vrf lan-service
 frequency 300
 timeout 1000
 threshold 150
ip sla schedule 20 life forever start-time now
ip sla 21
 udp-jitter 172.30.0.9 16384 source-ip 172.30.0.10 num-packets 20
 tos 46
 vrf lan-service
 frequency 300
 timeout 1000
 threshold 100
ip sla schedule 21 life forever start-time now
ip sla reaction-configuration 10 react rtt threshold-value 200 150 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 11 react jitterAvg threshold-value 100 90 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 11 react packetLossSD threshold-value 10 6 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 20 react rtt threshold-value 200 150 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 21 react packetLossSD threshold-value 10 6 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 21 react jitterAvg threshold-value 100 90 threshold-type immediate action-type trapOnly
no cdp log mismatch duplex
```

A su vez se configura el receptor de tráfico *IPSLA* en los *router* CE conectados al otro lado del *core MPLS* como se muestra en la Figura 9.

Figura 9

Configuración IPSLA en CE-DC1. Fuente: Autores.

```
ip sla auto discovery
ip sla 1
 icmp-echo 8.8.4.4 source-interface GigabitEthernet1/0.1600
ip sla schedule 1 life forever start-time now
ip sla logging traps
ip sla responder
no cdp log mismatch duplex
```

Se podría realizar una implementación de *IPSLA* dinámico para el cambio de rutas y tráfico, sin embargo, debido a limitaciones de *hadware* en el presente trabajo no es posible inyectar tráfico en la red para simular degradación.

2.12 HERRAMIENTAS DE EVALUACIÓN Y ADMINISTRACIÓN DE TI

Las herramientas de evaluación y administración de TI que se utilizarán son *IPerf* y *D-ITG*.

2.12.1 IPERF

Iperf fue desarrollado por NLANR / DAST para medir el rendimiento máximo de ancho de banda TCP y UDP. Permite el ajuste de varios parámetros y características e informa el *bandwidth*, *delay jitter*, and *packet loss*. (code.google.com, 2014)

2.12.2 D-ITG

D-ITG (*Distributed* Internet *Traffic Generator*) es una plataforma capaz de producir tráfico a nivel de paquete replicando con precisión los procesos estocásticos. *D-ITG* admite la generación de tráfico IPv4 e IPv6 y es capaz de generar tráfico en la capa de red, transporte y aplicación. (traffic.comics.unina.it, 2012)

2.12.3 MODO DE USO DE LAS HERRAMIENTAS

En el servidor *centos-server* se ejecutan los siguientes comandos para cada una de las herramientas de evaluación del rendimiento, también se describe cada uno de estos

Para *IPERF*:

iperf -s -u -i 10 -m

Opciones del comando
-s: Se refiere a que es el servidor de la conexión.
-u: Especifica que la prueba se realiza con protocolo UDP.
-i 10: Intervalo de la prueba
-m: Muestra el MSS (MTU - TCP/IP *header*)

Para D-ITG

ITGSend -T UDP -a 10.10.0.11 -c 100 -C 1315 -t 1000 -l sender.log
Opciones del comando
-T UDP: especifica que la prueba se realiza con protocolo UDP.
-a: Especifica dirección del servidor
-c 100: especifica los tamaños de los paquetes.
-C 1315: especifica los paquetes por segundo
Se configura –c 100 y –C 1315 debido a que 100 bytes= 0,0008 Megabits, este valor multiplicado por 1315 es igual a aproximadamente 1,062 Megabits por segundo, que hace una tasa de transferencia similar a la utilizada en iperf.
-t 1000: especifica la duración de la prueba de 10 segundos.
-l sender.log: especifica el archivo donde guarda los resultados.

En el servidor *centos-client* e se ejecutan los siguientes comandos para cada una de las herramientas de evaluación del rendimiento, también se describe cada uno de estos

Para *IPERF*:

iperf -c 10.10.0.11 -u -b 1M -f k
Opciones del comando
-c: especifica que es el cliente de la conexión
-u: especifica que la prueba se realiza con protocolo UDP.
-b: para enviar durante el tiempo de la prueba máximo un Megabits/segundo.
-f k: para mostrar los resultados en Kilobits.

Para D-ITG:

ITGRecv -l receive.log: Establece el equipo como el servidor de la conexión y guarda los resultados de las pruebas en el archivo receive.log.

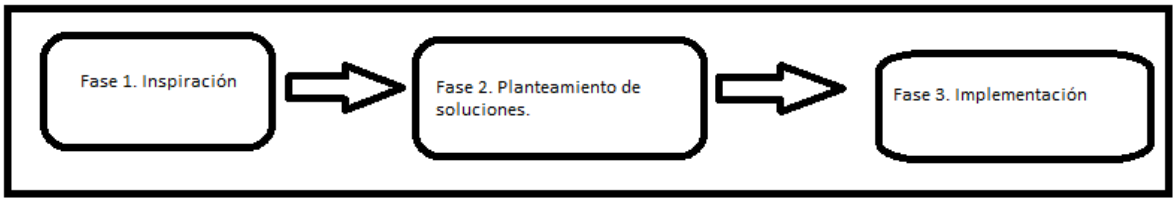
ITGDec receive.log: Decodifica la información alojada en el archivo receive.log y muestra en la pantalla los resultados de la prueba.

3. METODOLOGÍA

A continuación, se explica las actividades realizadas utilizando como referencia el método *Design Thinking* en cada fase de la metodología se expone cómo se desarrolla todos los objetivos planteados como se muestra en la Figura 10.

Figura 10

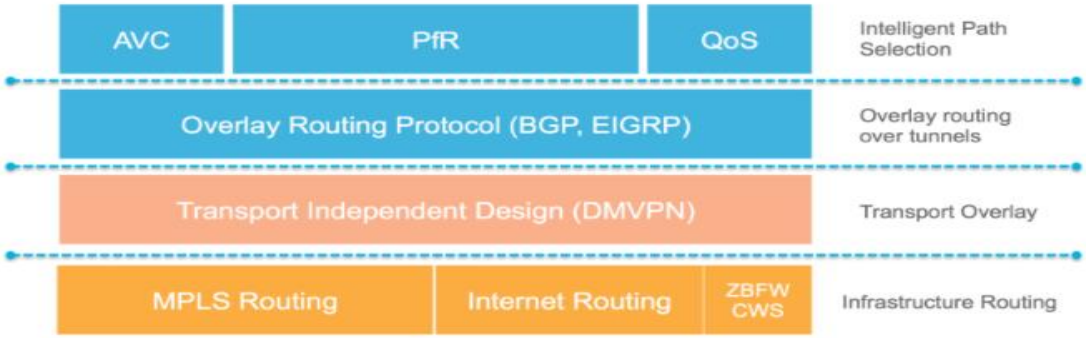
Fases de la metodología. Fuente: Autores.



- Fase 1 o de inspiración: En esta fase se realiza una observación, búsqueda e investigación de información considerada útil para el desarrollo del trabajo de grado, allí se tiene en cuenta todo lo referente principalmente a nuevas tecnologías para la *WAN y para la LAN,* se recopila los documentos sobre todo vía web donde se encuentran archivos recientes referentes a tecnologías como *SD-ACCES* e información del protocolo de transporte *DMVPN*, el método de selección inteligente *PFR*, la infraestructura *MPLS* y el protocolo de enrutamiento *BGP* teniendo en cuenta las capas de la tecnología *IWAN* que se muestran en la Figura 11.

Figura 11

Capas de Iwan. Fuente: relaxnetwork.wordpress.com



En esta etapa también se define la topología general de la red, las herramientas de virtualización escogidas que son *GNS3* y *Vmware Workstation*, los recursos mínimos de CPU y RAM que se requieren y las imágenes ISO CISCO para el proyecto.

- Fase 2 o de planteamiento de soluciones: Tomando en cuenta la información recopilada en la fase 1, se define una estrategia para la selección definitiva de la topología de red donde se toma la decisión de tener 2 sedes, una principal y otra el centro de datos con un *core MPLS*, una vez definida la topología, el protocolo de enrutamiento *BGP*, también, se definen los *KPI* a evaluar y los parámetros mínimos o requerimientos del sistema. Por último, se implementa una red *legacy* y luego una red con conceptos de *SDN* para tener puntos de comparación y demostrar que es mucho mejor en la implementación final del proyecto.
- Fase 3 o Implementación: Diseñado en GNS3 junto con *VMware Workstation* una red *legacy* para la red LAN de *Centro de datos* y la red *LAN* de la sede principal interconectadas mediante una infraestructura de red *MPLS*, luego se procede a utilizar las herramientas de evaluación *iperf*, *ping* y D-ITG mediante el uso de *scripts* para obtener datos sobre el estado de la red luego de responder a fallas en los enlaces, esto con la intención de abordar todas las posibles fallas que se puedan presentar en la topología y medir el rendimiento de la red bajo estas incidencias, finalmente se diseña la red con conceptos de *SDN*, una vez más se obtienen mediante las herramientas de evaluación mencionadas los datos necesarios para conocer el rendimiento de la red respondiendo a puntos de falla y así se tiene cómo

comparar el diseño final de la red con la red *legacy* para presentar los resultados y conclusiones.

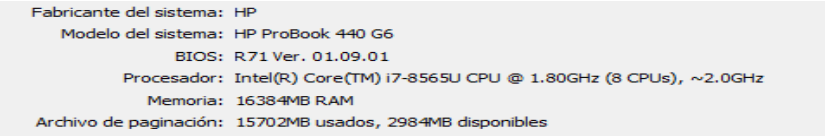
4. RESULTADOS Y DISCUSIÓN

4.1 SIMULACIÓN

La simulación se realiza en un equipo portátil HP *Probook* con las siguientes características que se muestran en la Figura 12.

Figura 12

Características de computador donde se realizan simulaciones. Fuente: Autores.



4.1.1 DISPOSITIVOS

En la tabla 10 se referencian los dispositivos utilizados para la creación del laboratorio de pruebas virtualizado.

Tabla 10

Dispositivos. Fuente: Autores.

Referencia	Descripción	Ubicación
CISCO 7200 Series	Diseñados para plataformas de interconexión de datos, soportan *QoS*, múltiples protocolos y métodos de multiplexación. Es un *router* de alto rendimiento con diferentes interfaces que proporcionan e ideal para los ISP	Core *MPLS* router P, PE y CE
Dispositivos IOU L2 Y L3	Son *Switch* virtualizados de CISCO con las interfaces y rendimiento para aplicaciones empresariales.	Ubicados en la interconexión de la *MPLS* y la LAN de casa sede.

4.1.2 GNS3

Se implementa la red *legacy* y *MPLS* simuladas en el software GNS3 versión 2.1.21 utilizando IOS CISCO C7200 *Version* 15.2(4) M y IOU L2 *Version* 15.2.

Para la simulación de servidores con sistema operativo Ubuntu 16.04 y servidor GNS3 se utiliza software de simulación *VMware WorkStation*.

Para la integración a nivel de red entre el GNS3 y *Vmware WorkStation* se realiza configuración con tarjetas de red virtuales, pudiendo configurar cada servidor en el segmento de red deseado.

En la Figura 13 se muestra la implementación de la red *legacy* en el *software* de simulación *GNS3* y en la Figura 14 la implementación de la red *overlay*, donde se puede observar las sedes (principal y *Centro de datos*) y la red de *core MPLS*, además, los servidores *Linux* conectados e integrados para la evaluación de rendimiento a realizar.

Figura 13

Implementación de la red legacy en GNS3. Fuente: Autores.

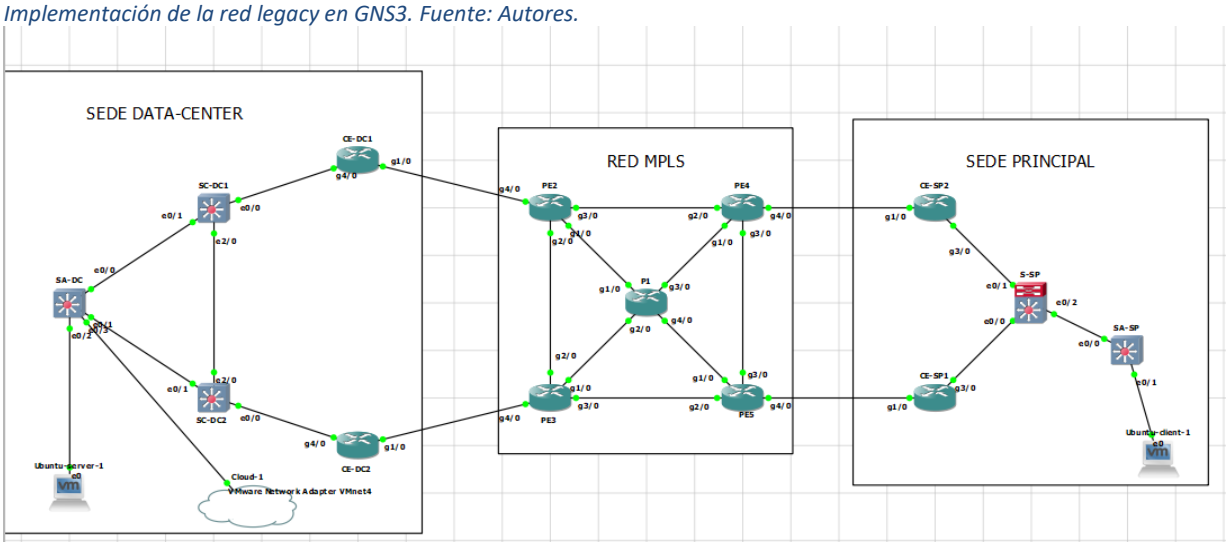
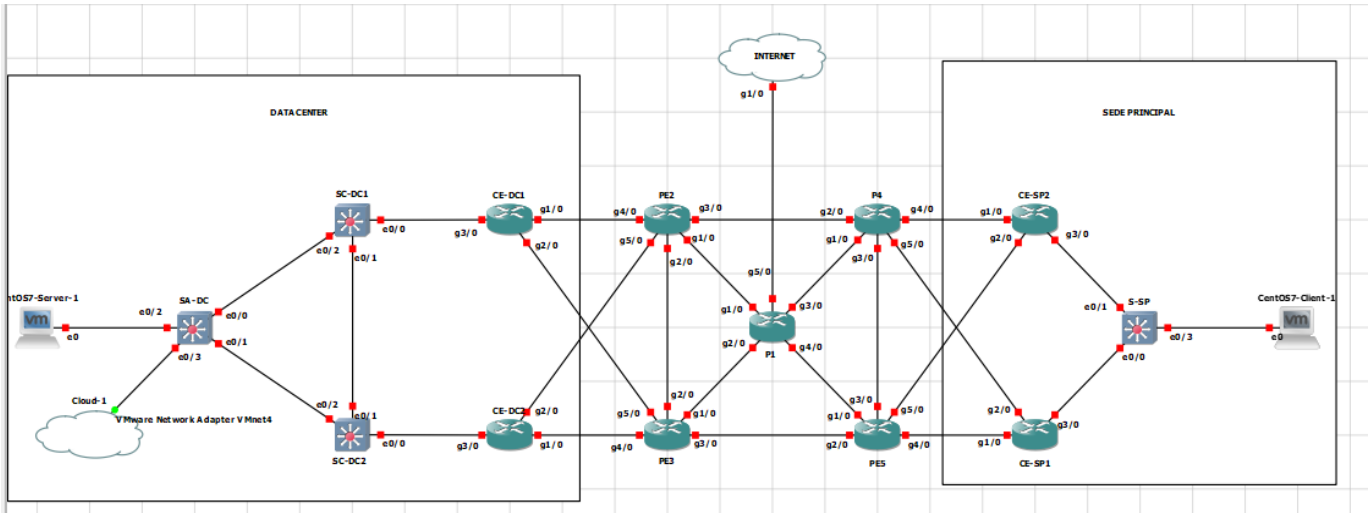


Figura 14

Implementación de la red Overlay en GNS3. Fuente: Autores



4.2 PROCESOS SDN A LA RED LEGACY

Al aplicar procesos de *SDN* a la red *legacy* el objetivo es configurar una red *overlay* (La red de transporte) donde no sea necesario configurar un protocolo de enrutamiento dinámico, ya que solo se requiere rutas por defecto en los *CEdge* hacia los PE, para tener conectividad *WAN* entre estos. El protocolo de enrutamiento dinámico se requiere sobre la red *underley* para compartir dinámicamente las tablas de enrutamiento de las redes locales de cada sede.

En el desarrollo del trabajo de grado se configura el protocolo de enrutamiento dinámico *IBGP* entre los *router* de *Core* y *E-BGP* entre los *CEdge - router* de *core*, además entre el *Hub* and *Spoke* en la red *Overlay* para la conectividad de las sedes y centro de datos, se escogió el protocolo de enrutamiento *BGP* debido a que permite realizar modificaciones a la tabla de enrutamiento con el objetivo de realizar conmutaciones automáticas gracias a sus algoritmos de escogencia de rutas con atributos ya que brinda la posibilidad de manejar el tráfico *inbound* y *outbound* a conveniencia. Al momento de realizar configuraciones para la implementación del protocolo *PFR* en los *router's CEdge* con el controlador *master*, se identifica una limitante del protocolo PFR con respecto a *BGP*, debido a que se requiere *IBGP* en la red *LAN* para poder realizar las modificaciones en la tabla *RIB*, para así, modificar

la entrada y salida del tráfico debido a que *PFR* logra manipular la tabla de enrutamiento de *BGP* mediante el atributo de *local preference* y como se realizó la configuración de *E-BGP* entre los *CEdge* y *router's* de Core no es posible implementar *PFR* en la simulación, en su lugar, se aplica escogencia de rutas entre los *CEdge* y los *router* de *core* mediante manipulaciones de *BGP* e *IPSLA* para conocer el estado de la red, saber cuáles son las mejores rutas y obtener resultados en tiempo real de las mediciones de los *KPI*.

La red se automatiza mediante *BGP*, la conmutación del tráfico de enlaces principales a enlaces *Backups* al presentarse caídas o fallas tanto para el servicio de datos como para internet, permitiendo obtener resiliencia ante fallas, pero no se cuenta con conmutación por estado de enlaces a nivel de degradación del servicio.

La conmutación automática se logra utilizando los atributos de BGP como el *Weitgh* y AS-PATH ya sea directamente hacia el *peer* o mediante la utilización de *route-map*, además se apoya en *embedded event manager* (*EEMM*) de CISCO para automatizar tareas dependiendo del registro del log.

Con el objetivo de tener conocimiento del estado real de los enlaces, se configura *IP-SLA* en los *router* de la sede remota, los cuales son capturados mediante un *script* en el servidor; además, se desarrolla scripts para captura de *bakcup* de los dispositivos de red y múltiples scripts que permiten la ejecución automatizada del desarrollo de las pruebas de rendimiento con los softwares *D-ITG, iperf* e *icmp*.

4.3 *SCRIPTS*

Se describen los diferentes *scripts* desarrollados en el trabajo de grado, con el objetivo de automatizar tareas y pruebas que permitan una administración más ágil de la plataforma de red. En los anexos esta la configuración de los scripts.

4.3.1 PROGRAMACIÓN DE SCRIPT DE BACKUP

El script ubicado en el centro de datos para realización de *backup* automático de los equipos de red utiliza la librería *expect* que permite la conexión con equipos remotos, *shell* de *bash*, lenguaje de programación *perl* y *crontab*, para permitir la automatización.

Se utilizan 3 archivos para lograr la automatización.

- **Archivo equipos_telnet.pl:** El cual lee la lista de dispositivos a realizar los *backups* y ejecuta para cada equipo el script de *expect*, y brinda dos salidas con la información de configuración del equipo de red y un log para validar la ejecución correcta de los *backups*.

- **Archivo equipos_red.txt:** Contiene una lista de las *IP* y *hostname* de los equipos de red.

- **Archivo equipos_red. ex:** Es el script que se conecta al equipo de red y ejecuta las instrucciones requeridas para la creación del *backup* y posteriormente cierra la conexión con el dispositivo.

4.3.2 PROGRAMACIÓN DE SCRIPT PARA EJECUCIÓN REMOTA

Se crea un *script* que permite la conexión remota con otro servidor y la ejecución de comandos, este se compone del script cliente y script servidor.

Script servidor cxremote.pl: Abre la conexión hacia el servidor remoto y es invocado en los scripts que requieren ejecutar comandos en un servidor destino, luego de la ejecución del comando termina la conexión.

Script en servidor cliente cxremoted.pl: Habilita el puerto de conexión en *listening*, el cual será utilizado por el script servidor y tiene definidos cuales comandos o scripts se pueden ejecutar, al final cierra la conexión y brinda una salida en el servidor.

Los scripts permitidos para ser ejecutados son guardados en un directorio llamados *cmd* y relacionados en el archivo *txt* de nombre comandos.

4.3.3 PROGRAMACIÓN DE SCRIPT DE PRUEBAS DE PING

Se crea script para pruebas de ping con el objetivo de evaluar el RTT, el cual genera 100 paquetes *icmp request* desde el servidor *centos-client* y son organizados los resultados para ser almacenados en el archivo de *excel* Pruebas HA donde serán almacenados los datos de las pruebas de rendimiento.

4.3.4 PROGRAMACIÓN DE SCRIPT PARA PRUEBAS DE *IPERF* Y D-ITG

Son *scripts* los cuales se apoyan en el script de conexión remota para ejecutar comandos en modo cliente servidor.

El *script* **tooliperf.sh** fue desarrollado para realizar pruebas de *iperf* automatizadas, y muestra los resultados en pantalla, ejecuta comandos en el servidor y en el equipo cliente.

El script **toolDITG.sh** fue desarrollado para realizar pruebas de D-ITG automatizadas, y muestra los resultados en pantalla, ejecuta comandos en el servidor y en el equipo cliente.

4.3.5 PROGRAMACIÓN DE SCRIPT PARA CONSULTAS DE PRUEBAS IPSLA EN LOS ROUTER CISCO

Se crean múltiples scripts mediante *expect* para conectarse a los *router* CISCO *wan* y obtener el resultado de las pruebas *IPSLA* ejecutadas en los mismos, para posteriormente mostrar el resultado en pantalla.

4.4 DESARROLLO DE LAS PRUEBAS

Las pruebas que se realizan en el proyecto se detallan en las Tablas 11, 12, 13, 14 y 15 allí se enumeran cada una de ellas para ser identificadas de forma fácil y se describe la tarea asociada a cada prueba.

Las pruebas realizadas en la sede principal para la red legacy se muestran en la Tabla 11, las pruebas en la sede Centro de datos para la red legacy se muestra en la Tabla 12. Así mismo, en la Tabla 13 y 14 están las pruebas para la red overlay donde se aplican los conceptos de SDN tanto para la sede principal como en el Centro de datos respectivamente. En la tabla 15 se muestra las pruebas sobre de conectividad sobre la red Overlay.

En la red legacy solo se hacen pruebas sobre el canal de datos, para la red overlay se tiene dos canales, el de datos y uno de internet. Todas las pruebas parten de una interrupción de un enlace o tramo de la red, donde se evalúa el impacto que esta incidencia tiene en la red de acuerdo con los KPI establecidos y otra parte de la prueba es cuando se normaliza la interrupción o incidencia en uno de los enlaces de la red y allí se realiza otra evaluación para identificar el comportamiento de la red al ser solucionados los puntos de falla.

Tabla 11

Pruebas realizadas en la sede principal red Legacy. Fuente: Autores.

Número de Prueba	Tarea
1	Deshabilitar canal de datos de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
2	Normalizar canal de datos de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
3	Deshabilitar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
4	Normalizar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
5	Deshabilitar canal de datos de S-SP
	Pruebas de conectividad y tabla de Enrutamiento
6	Normalizar canal de datos de S-SP

	Pruebas de conectividad y tabla de Enrutamiento
7	Deshabilitar canal de datos de S-SP
	Pruebas de conectividad y tabla de Enrutamiento
8	Normalizar canal de datos de S-SP
	Pruebas de conectividad y tabla de Enrutamiento

Tabla 12

Pruebas realizadas en el Centro de datos red legacy. Fuente: Autores

Número de Prueba	**Tarea**
1	Deshabilitar canal de datos de CE-DC1
	Pruebas de conectividad y tabla de Enrutamiento
2	Normalizar canal de datos de CE-DC1
	Pruebas de conectividad y tabla de Enrutamiento
3	Caída de equipo CE-DC1
	Pruebas de conectividad y tabla de Enrutamiento
4	Normalizar equipo CE-DC1
	Pruebas de conectividad y tabla de Enrutamiento
5	Deshabilitar canal de datos de CE-DC2
	Pruebas de conectividad y tabla de Enrutamiento
6	Normalizar canal de datos de CE-DC2
	Pruebas de conectividad y tabla de Enrutamiento
7	Caída de equipo SC-DC1
	Pruebas de conectividad y tabla de Enrutamiento
8	Normalizar equipo SC-DC1
	Pruebas de conectividad y tabla de Enrutamiento
9	Caída de equipo SC-DC2
	Pruebas de conectividad y tabla de Enrutamiento
10	Normalizar equipo SC-DC2
	Pruebas de conectividad y tabla de Enrutamiento

Tabla 13

Pruebas realizadas en la sede principal red Overlay. Fuente: Autores.

Número de Prueba	Tarea
1	Deshabilitar canal de datos de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
2	Normalizar canal de datos de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
3	Deshabilitar canal de Internet de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
4	Normalizar canal de Internet de CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
5	Deshabilitar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
6	Normalizar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
7	Deshabilitar canal de Internet de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
8	Normalizar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
9	Apagar router WAN CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento
10	Deshabilitar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
11	Normalizar canal de datos de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
12	Deshabilitar canal de Internet de CE-SP2
	Pruebas de conectividad y tabla de Enrutamiento
13	Normalizar canal de Internet de CE-SP2 y encender *router* WAN CE-SP1
	Pruebas de conectividad y tabla de Enrutamiento

Tabla 14

Pruebas realizadas sede Centro de datos red Overlay. Fuente Autores.

Número de Prueba	Tarea
1	Deshabilitar canal de datos de CE-DC1
2	Normalizar canal de datos de CE-DC1
3	Deshabilitar canal de Internet de CE-DC1

4	Normalizar canal de Internet de CE-DC1
5	Apagar router WAN CE-DC1
6	Deshabilitar canal de datos de CE-DC2
7	Normalizar canal de datos de CE-DC2
8	Deshabilitar canal de Internet de CE-DC2
9	Normalizar canal de Internet de CE-DC2 y encender *router* WAN CE-DC1
10	Apagar router Core SC-DC1
11	Encender router Core SC-DC1

Tabla 15

Pruebas de conectividad red Overlay. Fuente Autores.

Número de Prueba	Tarea
1	Deshabilitar canal de Internet de CE-DC1
2	Normalizar canal de Internet de CE-DC1

De acuerdo con cada escenario realizado para la evaluación del rendimiento, se toman resultados mediante pruebas de ping, *jitter*, *bandwidth* y *packet Loss* utilizando las herramientas *IPERF y D-ITG.* Además, se validan los cambios ocasionados por cada prueba en las tablas de enrutamiento, para observar cómo se afecta a esta, comprobando que hay conmutación automática en la red, a su vez se observan y guardan los tiempos de conmutación para validar el tiempo de afectación del servicio.

4.4.1 ARCHIVO DE TOMA DE DATOS DE LAS PRUEBAS

Se toman los resultados de las pruebas de evaluación del rendimiento, esto se publica como un anexo del trabajo de grado, se diseñan 19 escenarios para la red *legacy* y 26 escenarios para la red *overlay*, para tomar tiempos de conmutación, métricas de rendimiento, resultados de los *KPIs* mediante las herramientas de pruebas adicionales que son *Iperf* y *D-ITG*.

4.5 COMPARACIONES DE LOS RESULTADOS OBTENIDOS

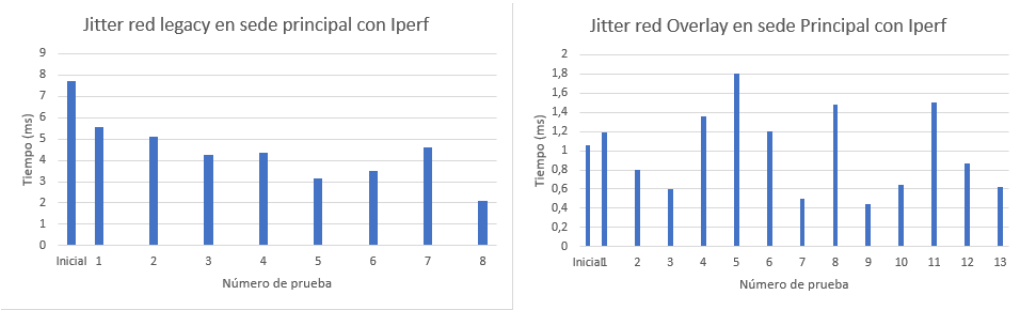
Se presentan a continuación las comparaciones de los resultados relevantes del proyecto con la intención de analizar los datos de forma gráfica y sacar conclusiones al comparar los resultados en la red *legacy* con los resultados de la red *overlay*.

4.5.1 COMPARACION DEL JITTER DE LA RED LEGACY CON LA RED OVERLAY CON IPERF

En la Figura 15 se muestra la comparación del *jitter* en la sede principal sobre la red *legacy* y *overlay*, donde se observa en la red *legacy* unos tiempos de *jitter* con límite inferior de 2 ms y superior de 7.7 ms, mientras que los tiempos en la red *overlay* con límite inferior de 0.5 ms y superior de 1.8 ms. Esto demuestra unos resultados óptimos en la red *overlay* para una prestación de servicio.

Figura 15

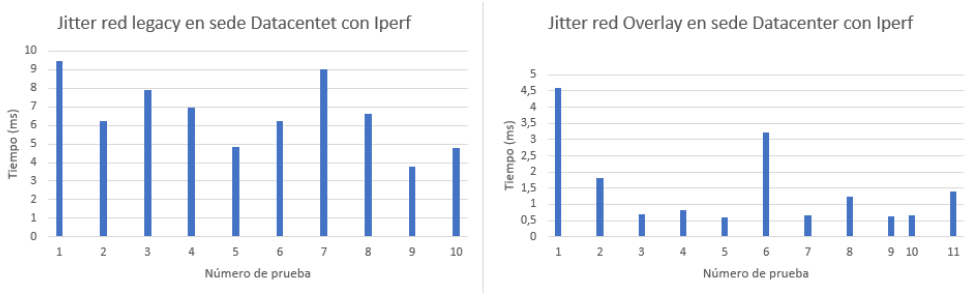
Comparación del jitter en la sede principal entre la red legacy y overlay con Iperf. Fuente: Autores



Al igual que en la Figura 16 se muestra el resultado de las pruebas de *jitter* con *iperf* en las redes *legacy* y *overlay* sobre el *Centro de datos* en los cuales se obtienen en la red *legacy* unos tiempos de jitter con límite inferior de 3.8 ms y superior de 9.5 ms, mientras que los tiempos en la red *overlay* con límite inferior de 0.6 ms y superior de 4.5 ms. Demostrando mejores tiempos en la red *overlay* para el *Centro de datos.*

Figura 16

Comparación del jitter en la sede Centro de datos entre la red legacy y overlay con Iperf. Fuente: Autores

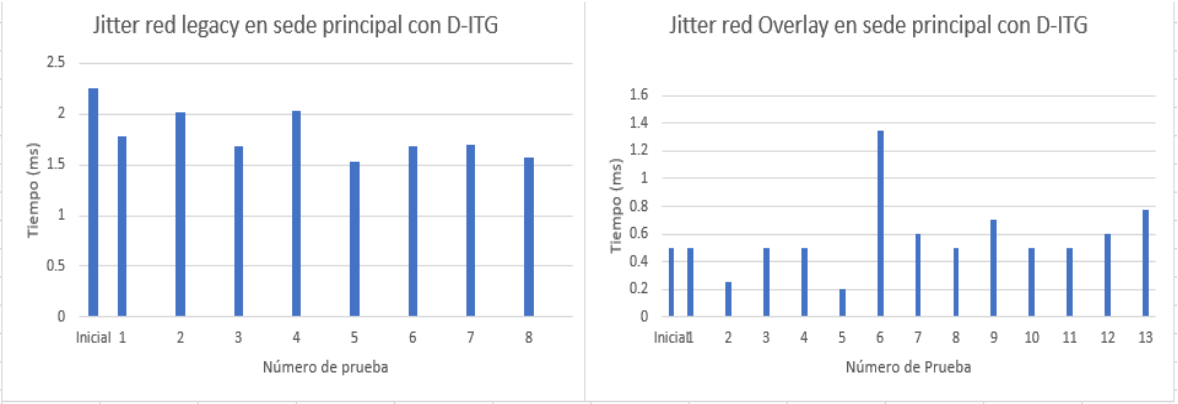


4.5.2 COMPARACION DEL JITTER DE LA RED LEGACY CON LA RED OVERLAY CON D-ITG

En la Figura 17 se muestra las pruebas de *jitter* con *D-ITG* en la sede principal donde se obtiene en la red *legacy* unos tiempos de *jitter* con límite inferior de 1.5 ms y superior de 2.5 ms, mientras que los tiempos en la red *overlay* con límite inferior de 0.5 ms y superior de 1.3 ms.

Figura 17

Comparación del jitter en la sede principal entre la red legacy y overlay con D-ITG. Fuente: Autores

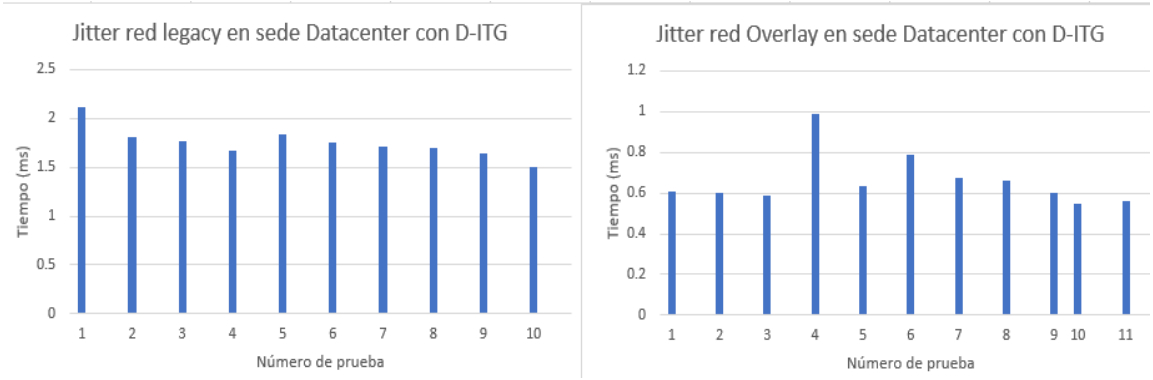


En la Figura 18 se muestra de forma similar las pruebas de *jitter* con *D-ITG* en el *Centro de datos* donde se obtienen en la red *legacy* unos tiempos de jitter con límite inferior de 1.5

ms y superior de 2.3 ms, mientras que los tiempos en la red *overlay* con límite inferior de 0.6 ms y superior de 1 ms.

Figura 18

Comparación del jitter en la sede Centro de datos entre la red legacy y overlay con D-ITG. Fuente: Autores

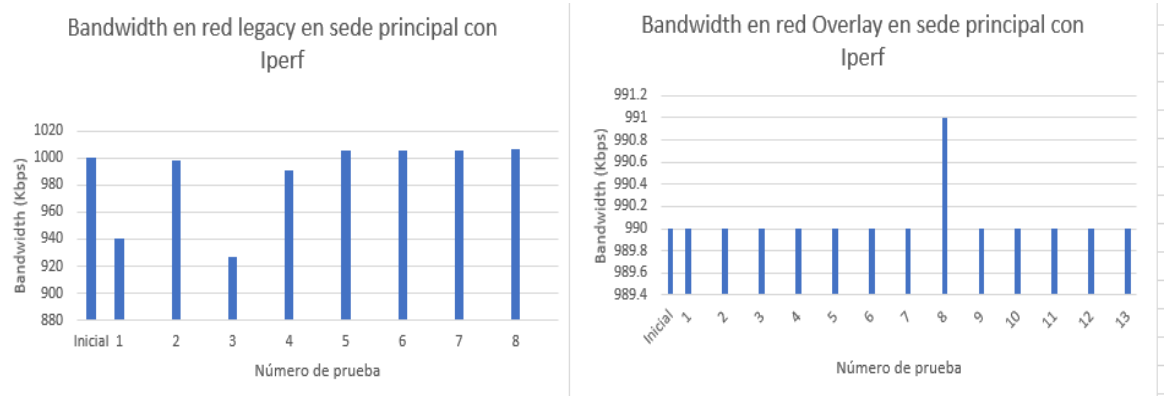


4.5.3 COMPARACION DEL BANDWIDTH DE LA RED LEGACY CON LA RED OVERLAY CON IPERF

En la Figura 19 se muestra las comparaciones de ancho de banda en las pruebas realizadas con *iperf* sobre la sede principal donde se puede evidenciar en términos generales que los resultados de la red *legacy* y *overlay* son diferentes en 10 Kbps lo cual no constituye una diferencia sustancial, además, de mayor estabilidad en los resultados de ancho de banda en la red *overlay*.

Figura 19

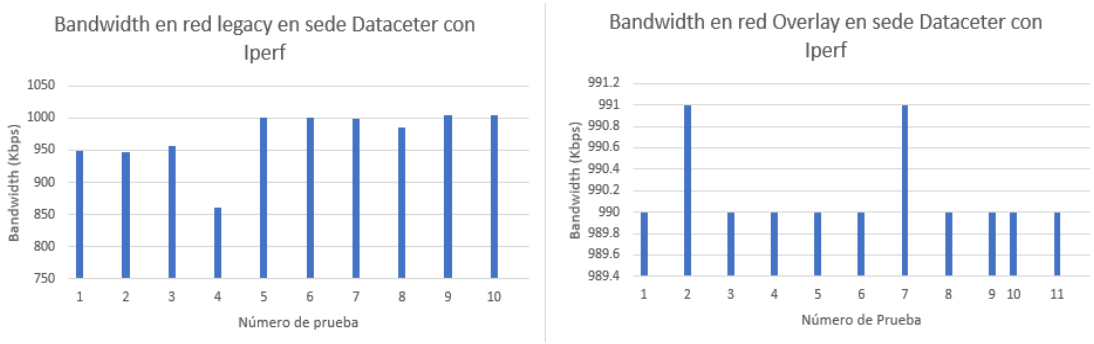
Comparación del Bandwidth en la sede principal entre la red legacy y overlay con Iperf. Fuente: Autores



De forma similar en la Figura 20 se muestra las comparaciones de ancho de banda en las pruebas realizadas con *iperf* sobre la sede *Centro de datos* donde se puede evidenciar en términos generales de nuevo que los resultados de la red *legacy* y *overlay* son diferentes en 10 Kbps lo cual no constituye una diferencia sustancial, además, de mayor consistencia en los resultados de ancho de banda en la red *overlay*.

Figura 20

Comparación del Bandwidth en la sede Centro de datos entre la red legacy y overlay con Iperf. Fuente: Autores



4.5.4 COMPARACION DEL BANDWIDTH DE LA RED LEGACY CON LA RED OVERLAY CON D-ITG

En la Figura 21 y 22 se observan los resultados de ancho de banda tomados con D-ITG en las redes *legacy* y *overlay* sobre la sede principal y *Centro de datos* respectivamente, donde se puede evidenciar que sobre la red *overlay* se garantiza un *bandwidth* de 1 Mbps mientras que en la red *legacy* un máximo de 900 kbps.

Figura 21

Comparación del Bandwidth en la sede principal entre la red legacy y overlay con D-ITG. Fuente: Autores

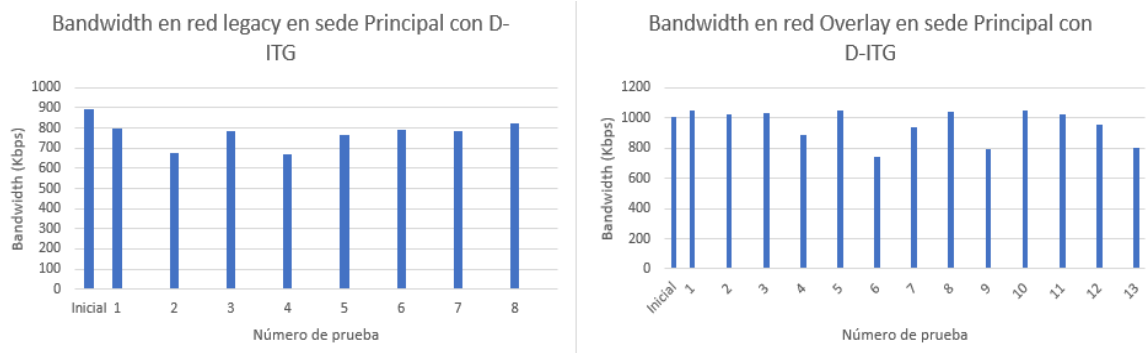
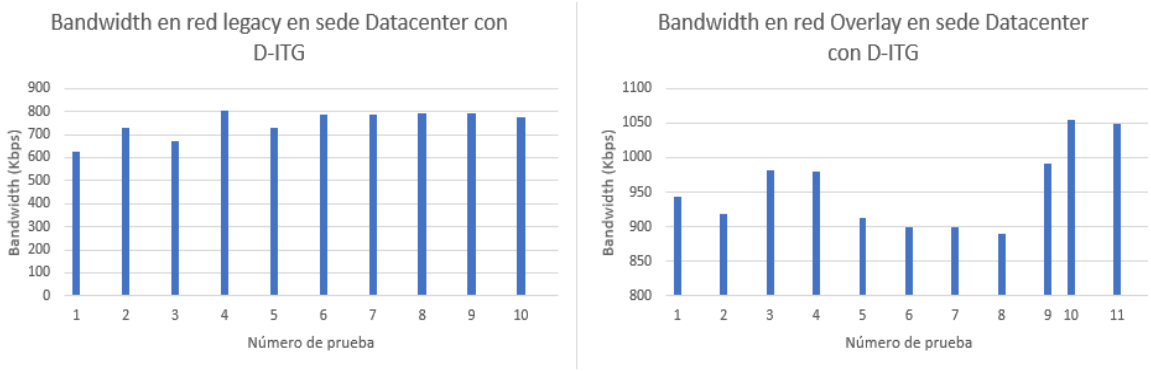


Figura 22

Comparación del Bandwidth en la sede Centro de datos entre la red legacy y overlay con D-ITG. Fuente: Autores



4.5.5 COMPARACION DE RTT DE LA RED LEGACY CON LA RED OVERLAY EN SEDE PRINCIPAL Y CENTRO DE DATOS

En la Figura 23 y 24 se logra evidenciar tiempos muy semejantes de respuesta entre la red *overlay* y la red *legacy* para las pruebas de la sede principal, aunque ambas tienen diferentes picos de respuesta que oscilan entre 50 ms a 190 ms.

Figura 23

Comparación RTT en la sede principal entre la red legacy y overlay. Fuente: Autores

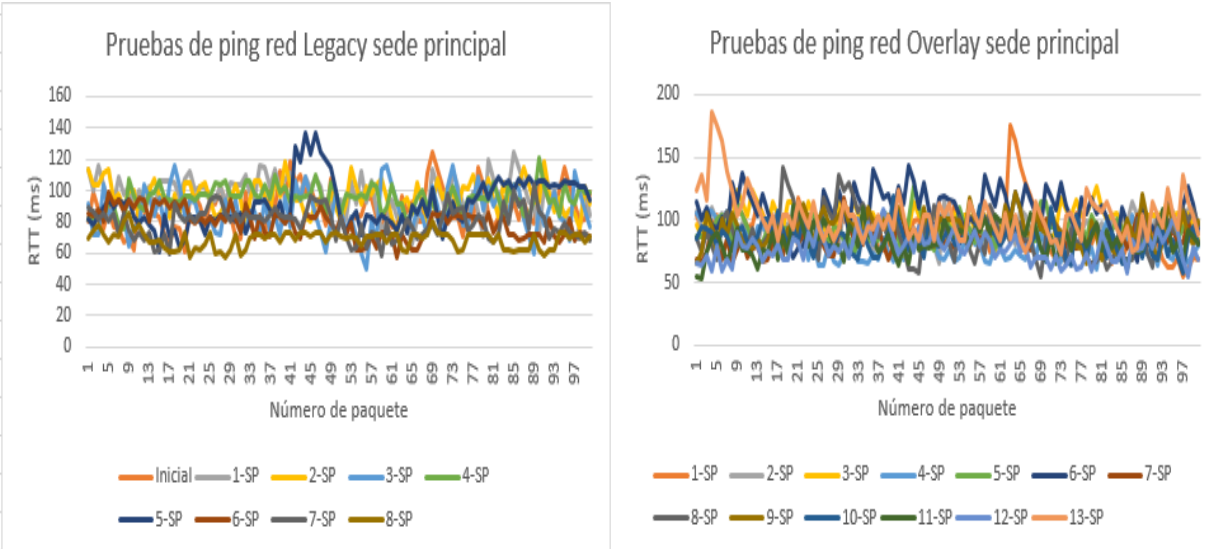
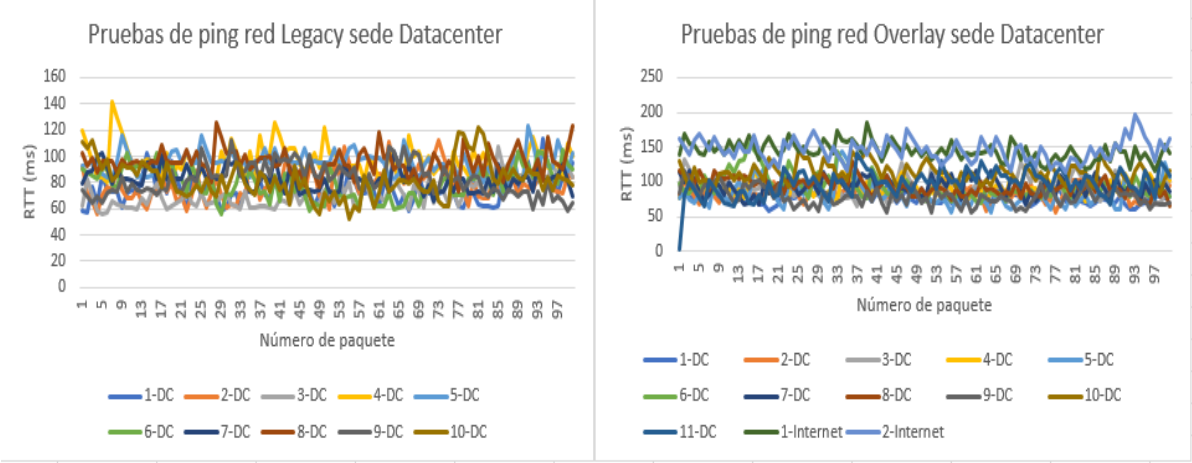


Figura 24

Comparación RTT en la sede Centro de datos entre la red legacy y overlay. Fuente: Autores



5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

5.1 CONCLUSIONES

Aunque la evaluación del rendimiento de la *LAN* y *WAN* en la red *legacy* y la red *overlay* con procesos de *SDN* se afecta por la capacidad de procesamiento del equipo donde fueron virtualizadas las redes, se logra evidenciar en las comparaciones de los resultados obtenidos en el capítulo 4.5 del trabajo de grado, unos mejores *KPI* en la red *overlay* con respecto a la red *legacy,* aunque se debe tener presente que no fue posible compararlos con los valores de KPI obtenidos con los umbrales definidos para *jitter*, *RTT* y *packet loss* debido a la alteración de las pruebas por el rendimiento del computador donde fueron realizadas las pruebas, sin embargo, concluimos que las pruebas sobre redes físicas permiten tener una comparación más concluyente de ambos diseños propuestos y desarrollados en este trabajo de grado. Es importante indicar que se lograron cumplir con todos los objetivos,

aunque de manera limitada en la solución planteada y desarrollada debido a los recursos de hardware requeridos.

Se diseña y configura una red *legacy*, una red *overlay* y *MPLS*, la implementación de las redes se realiza en el software de simulación GNS3 y los servidores son virtualizados utilizando *Vmware Workstation.* Se aplican procesos de *SDN* mediante el desarrollo de scripts que permite automatizar tareas rutinarias, agilizando la obtención de datos de los diferentes dispositivos, como el estado real de los enlaces y del equipo, para toma de decisiones oportunas ya sea para una conmutación automática o manual del direccionamiento de los paquetes, en el desarrollo del trabajo se utilizaron herramientas activas de evaluación de rendimiento lo cual nos permitió evaluar la red bajo diferentes escenarios de forma ágil. Al realizar una correcta configuración de *BGP*, complementándolo con *EEMM* (*Embedded event manager*) de CISCO e *IPSLA* se permite tener conmutaciones automáticas para garantizar continuidad de servicio, con esto se aplica un concepto importante de *SDN* que es garantizar la disponibilidad de servicio, aunque se puede realizar una mejora implementando *pfr*, para lo cual habría que realizar a su vez cambio de protocolo de enrutamiento de *BGP* a *OSPF* para poder tener conmutaciones basados en otras estadísticas como *RTT*, *jitter* y saturación de los enlaces. También, se destaca que debido a la pandemia del Covid 19 del año 2020 no se logró utilizar los equipos y recursos de *hadware* de las instalaciones de la Universidad.

Se realiza la definición de métricas y *KPI* en el trabajo de grado en el titulo 2.2 teniendo como referencia las recomendaciones de la UIT-T Y.1564 con el objetivo de garantizar la mejor prestación del servicio a nivel *LAN* y *WAN*; además se describen en el titulo 2.4 del trabajo de grado las actividades que deben ser realizadas por el personal administrador de TI y en el titulo 2.3 se delimita las características con la cual debe contar una herramienta de monitoreo para garantizar una detención proactiva y reactiva de fallas.

Se realizan diferentes pruebas de evaluación de rendimiento y medición de métricas de *KPI* bajo diferentes escenarios de fallas diseñados con el objetivo de observar el comportamiento de la red *legacy* e *overlay*; en el titulo 4.8 “Comparación de los resultados obtenidos” se logra evidenciar un mejor comportamiento de la red *overlay* para la prestación de servicio, sin embargo, presenta diferentes dificultades en la simulación debido a limitación de recursos de sistema requeridos para la implementación de las redes diseñadas como lo son CPU y RAM, lo cual afecta directamente los resultados de la evaluación del rendimiento, donde se logra evidenciar que bajo el mismo escenario de pruebas se pueden obtener diferentes resultados, por tal motivo las pruebas realizadas no

pueden ser comparadas de forma exacta con los *KPI* y *SLA* definidos en el trabajo de grado; a su vez, se observa en las pruebas de rendimiento entre los servidores virtualizados conectados a la red simulada un alto consumo de procesamiento en el host físico, ocasionando falla en los equipos de red simulados y hasta bloqueo total del host teniendo que recurrir a un reinicio del mismo.

Se logra una documentación muy completa de todos los procesos y configuraciones realizadas en cada uno de los dispositivos en el trabajo de grado, se genera el documento de anexos "FDE-089-Informe-Anexos-TdG-FI-V4" que contiene el análisis de los resultados de todas las pruebas realizadas en la red *legacy* y overlay, además, el archivo Pruebas-HA que contiene solo los resultados de las pruebas realizadas en el trabajo de grado con el objetivo de servir como guía para trabajos futuros y comprender correctamente los procesos *SDN* aplicados a nuestro trabajo y poder realizar mejoras que permitan seguir extendiendo la vida de las redes *legacy*.

5.2 RECOMENDACIONES

Para realizar las pruebas de conmutación basados en el rendimiento del enlace, se hace necesario contar con un laboratorio físico para poder utilizar *software* de generación de paquetes que permita simular degradaciones y fallas de enlaces, como lo es *ostintato*, *tfgen*, *scapy*, entre otros.

Es importante configurar sobre el software de simulación las imágenes correctas y que hemos indicado en el trabajo de grado que permitan simular los dispositivos de red requeridos para una correcta integración con los servidores virtualizados en el software de simulación *VMware WorkStation*.

Se recomienda que durante la implementación de la red *legacy* y *overlay* se esté realizando *backup* sobre los avances de la configuración y guardarlos en diferentes almacenamientos con la intención de evitar pérdidas de información y retrasos en el desarrollo del trabajo.

5.3 TRABAJO FUTURO

Para futuros trabajos de grado sería importante desarrollar la evaluación de rendimiento de una red *legacy* en producción y no simulada, para obtener resultados reales, posteriormente aplicarle procesos de *SDN* a dicha red y realizar una comparación entre los resultados obtenidos, para identificar si se evidencian mejoras en el funcionamiento de la red con nuestra implementación o por el contrario se degrada los servicios que funcionan sobre la misma.

Para redes que no están en producción se pueden utilizar generadores de tráfico o recrear escenarios de degradación de red, para aplicar pruebas que permitan evidenciar el correcto funcionamiento de los procesos de *SDN* aplicados, validando que estas mejoras si ayuden a garantizar óptimo rendimiento y resiliencia ante fallas totales o degradaciones, en una red *legacy*.

En trabajos futuros se puede implementar una aplicación que permita almacenar los datos en una base de datos, posteriormente analizarla, mostrar los datos gráficamente, además, parametrizar umbrales con el objetivo de generar alarmas y notificaciones a las áreas encargadas. Actualmente existen herramientas de monitoreo como *zabbix* que permiten recopilar la información y almacenarla en una base de datos para ser visualizadas en gráficos e históricos.

6. REFERENCIAS

Peixoto, T., & Vieira, A., & Nogueira, M., & Macedo, D. (noviembre del 2018). Does OpenFlow Really Decouple The Data Plane from The Control Plane. *IEEE Symposium on Computers and Communications (ISCC)*. Simposio llevado a cabo en Natal, Brazil.

Feamster, N., & Rexford, J., & Zegura, E. (abril del 2014). The Road to SDN. An intellectual history of programmable networks, Volumen 44 (Número 2), p.5.

D-ITG, Distributed Internet Traffic Generator. (2020). Napoli, Italia. Recuperado de http://traffic.comics.unina.it/software/ITG.

Edgeworth, B., (2017). *CISCO Intelligent WAN (IWAN)*, Indianapolis, Indiana: CISCO Press.

Luciani, J., & Katz, D., & Piscitello, D., & Cole, B., & Doraswamy, N. (abril de 1998). *NBMA Next Hop Resolution Protocol (NHRP)*. Fremont, USA.

CISCO IWAN E Laboratorio. (2020**).** California, USA. Recuperado de https://relaxnetwork.wordpress.com/2017/06/29/primeiro-post-do-blog/

Google Code Archive - Long-Term Storage For Google Code Project Hosting. (2020). California, USA, Recuperado de https://code.google.com/archive/p/iperf.

E.800: Definiciones De Los Términos Relativos A La Calidad De Servicio. (2020). Ginebra, Suiza. Recuperado de https://www.itu.int/rec/T-REC-E.800/es.

Y.1564: Ethernet Service Activation Test Methodology. (2020). Ginebra, Suiza. Recuperado de https://www.itu.int/rec/T-REC-Y.1564/en.

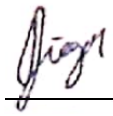
Iwan 2.X Versions And Release Support. (2020). California, USA. Recuperado de https://community.CISCO.com/t5/networking-documents/iwan-2-x-versions-and-release-support/ta-p/3292248.

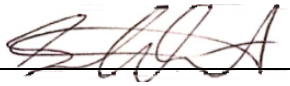
SDN And Controller-Based Networks > Introduction To Controller-Based Networking | CISCO Press. (2020). California, USA. Recuperado de https://www.CISCOpress.com/articles/article.asp?p=2995354&seqNum=2.

Ethernet - Ecured. (2020). La Habana, Cuba. Recuperado de https://www.ecured.cu/index.php?title=Ethernet&oldid=3539156.

Y.1564: SAM Desmitificado. (2020). Madrid, España. Recuperado de https://www.ayscom.com/documentos/D08-00-005_WP_VSAM_A00_SP_draft1.pdf

RFC 3031 - Multiprotocol Label Switching Architecture. (2020). Broomfield, USA. Recuperado de https://datatracker.ietf.org/doc/rfc3031/?include_text=1.

FIRMA ESTUDIANTE S 



FIRMA ASESORES 

FECHA ENTREGA: _____13-07-2021_____