ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

"DESARROLLO DE UNA PLATAFORMA MULTIVENDOR DE NETWORKING PARA LA EVALUACION DE INTEROPERABILIDAD DE PROTOCOLOS ROUTING IGP Y EGP"

TRABAJO DE TITULACIÓN

Tipo: PROYECTO TÉCNICO

Presentado para optar el Grado Académico de:

INGENIERA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTORA: MAGALY ALEXANDRA HIDALGO ARIAS

DIRECTOR: ING. ALBERTO ARELLANO AUCANCELA.

Riobamba-Ecuador

2019

Yo, Magaly Alexandra Hidalgo Arias, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otros autores están debidamente citados y referenciados.

Como autora asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 15 de julio de 2019

Magaly Alexandra Hidalgo Arias

060409552-1

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del trabajo de titulación certifica que: El trabajo de titulación: **DESARROLLO DE UNA PLATAFORMA MULTIVENDOR DE NETWORKING PARA LA EVALUACION DE INTEROPERABILIDAD DE PROTOCOLOS ROUTING IGP Y EGP**, de responsabilidad de la señorita Magaly Alexandra Hidalgo Arias, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación quedando autorizada su presentación.

ING. WASHINGTON LUNA
DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA _____ _____

ING. PATRICIO ROMERO
DIRECTOR DE LA ESCUELA DE INGENIERIA ELECTRÓNICA, TELECOMUNICACIONES Y REDES _____ _____

ING. ALBERTO ARELLANO
DIRECTOR DE TESIS _____ _____

ING. VINICIO RAMOS
MIEMBRO DEL TRIBUNAL _____ _____

DEDICATORIA

El presente trabajo de titulación quiero dedicárselo a mi amado Hijo Thiago Didier que, con cada sonrisa, cada abrazo y cada consuelo me dio valor para jamás rendirme en la vida, mi pequeño siempre serás el más hermoso angelito que llego a mi vida y le doy gracias a Dios por estar a mi lado. Se lo dedico además a mis padres que pese a todo siempre han estado a mi lado, mi padre Ángel Gilberto por sus consejos y por ser un honorable hombre, a mi madre María Guadalupe que siempre ha luchado en la vida. A mi hermana Julissa por ayudarme y sustituirme como mama cuando mi hijo lo ha necesitado, mi hermano Joffre por ser como un padre y amigo con mi hijo. A mi tía Lourdes que me ha apoyado en este largo proceso. A mi hermano Henry y su esposa por regalarme 3 hermosas sobrinas y siempre representar un pilar fundamental. Un eterno gracias a mi amiga Karen que siempre ha sido una madre, amiga y pañuelo de lágrimas siempre te llevare en mi corazón. Agradezco infinitamente a mi DIOS por hoy tenerme con salud y cuidar siempre de mi Familia.

Magaly

AGRADECIMIENTO

Agradezco en primer lugar a DIOS por siempre ser ese consuelo en las noches de tristeza, por enseñarme en valor de la vida y cada día más humilde. Hoy sé que sus caminos son perfectos. Te agradezco hijo mío por ser tan bueno y acompañarme en los días buenos y malos, perdóname si fallo, Te amo infinitamente. Agradezco a toda mi familia que siempre ha estado conmigo a pesar de mis faltas, a mis amigos que me han ayudado con sus consejos. A todos los docentes que han acompañado en esta larga travesía en la carrear en especial a mi Tutor Ing. Alberto Arellano por ser mi guía, consejero y amigo. Al Ing. Vinicio Ramos por ayudarme cuando se lo he pedido. Mil gracias a todos no tengo más que amor en mi corazón.

Magaly

TABLA DE CONTENIDO

CAPITULO II

ÍNDICE DE FIGURAS

INDICE DE GRAFICOS

ÍNDICE DE TABLAS

ÍNDICE DE ABREVIATURAS

OSI	Sistema Internacional de Estandarización
ARP	Address Resolution Protocol (Protocolo de resolución de direcciones)
AS	Sistema Autónomo
GUI	Interfaz Gráfica de Usuario
OSPF	Open Shortest Path Firs (Primer Camino mas Corto)
EIGRP	Protocolo de Enrutamiento Puerta de Enlace
RIP	Protocolo de Información de Encaminamiento
IGP	Interior Gateway Protocol (Protocolo de Pasarela Interna)
EGP	Exterior Gateway Protocol (Protocolo de Pasarela Externa)
BGP	Border Gatewey Protocol (Protocolo de enlace fronterizo)
IS-IS	System to Intermediate System
IDP	Proveedor de Identidad
NSAP	Network Service Access Point
TCP	Transmission Control Protocol (Protocolo de control de transmisión)
IP	Internet Protocol (Protocolo de Internet)
MTU	Maximium Transmission Unit (Unidad Máxima de Transmisión)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica del Host)
WPA	Wi-fi Protected Access (Acceso Wi-fi Protegido)
SIP	Session Initiation Protocol (Protocolo de Inicialización de Sesión)
SCCP	Skinny Client Control Protocol (Protocolo Propietario de Terminal)
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)

ÍNDICE DE ANEXOS

RESUMEN

Se desarrolló una plataforma multivendor para evaluar la interoperabilidad de los protocolos de borde interno (IGP) y de borde externo (EGP). Se utilizó el software GNS3 como herramienta de emulación para la implementación de las distintas topologías; además, la máquina virtual VMWare para la instalación de las plataformas de networking como Cisco, Juniper, Mikrotik y Brocade. Para la implementación de la plataforma se utilizaron protocolos que permitan, alta escalabilidad, convergencia y una cantidad alta de enrutadores conectados dentro de la misma red. Al realizar la simulación se emplearon las distintas topologías con configuraciones de enrutamiento como BGP, OSPF y IS-IS. Se realizó 6 pruebas con equipos homogéneos (Cisco-Cisco, Juniper-Juniper y Brocade-Brocade) y heterogéneos en distintos Sistemas Autónomos (AS) 300, 400 y 500, mediante estas pruebas se determinó el grado de interoperabilidad tanto entre equipos de la misma marca como equipos de distintas marcas. Mediante el generador de tráfico Ostinato se inyectaron paquetes TCP con 200 bytes, 800 bytes y 1500 bytes dentro de cada uno de los escenarios de prueba, para comprobar el funcionamiento de la red. Posteriormente, se analizaron los resultados utilizando la herramienta Wireshark, donde se realizó el muestreo en un tiempo aproximado de 30 minutos, en cada una de las topologías. Con los archivos pcap y con el analizador de paquetes se obtuvieron los parámetros como tasa de transferencia, latencia y pérdida de paquetes; además, se analizó la convergencia de la red mediante la tabla de rutas y los mensajes propios de cada topología. Finalmente, se obtuvo que la mayor tasa de transferencia existe en el AS 500 con un 25% más que los otros Sistemas Autónomos, la latencia fue mayor el en AS 300 con un 10% más que los otros AS, la pérdida de paquetes en todas las topologías fueron mínimas. Se concluye que los equipos interoperan adecuadamente en todas las topologías.

PALABRAS CLAVE: <REDES DE COMPUTADORES>, <INTEROPERABILIDAD>, <PLATAFORMA MULTIVENDOR>, <PROTOCOLOS DE ENRUTAMIENTO>, <GNS3 (SOTWARE)>, <SISTEMAS AUTONOMOS>, <PARAMETROS DE RENDIMIENTO>.

ABSTRACT

A multivendor platform was implemented to evaluate the interoperability of the internal edge (IGP) and outer edge (EGP) protocols. The GNS3 software is used as an emulation tool for the implementation of the different topologies. In addition, the VMWare virtual machine for the installation of network platforms such as Cisco, Juniper, Mikrotik and Brocade. For the implementation of the platform the protocols shown are used, high scalability, convergence and a high number of routers connected within the same network. When performing the simulation, different topologies will be used with routing configurations such as BGP, OSPF and IS-IS. Six tests were performed with homogeneous equipment (Cisco-Cisco, Juniper-Juniper and Brocade-Brocade) and heterogeneous in all Autonomous Systems (AS) 300, 400 and 500, through these tests the degree of interoperability was determined both among the equipment the same Brand as teams of different brands. Through the traffic generator, TCP packets with 200 bytes were injected. 800 bytes and 1500 bytes within each of the test scenarios, for the operation of the network. Afterwards, the results will be analysed using the Wireshark tool. where the sampling was done in an approximate time of 00:30:00, in each of the topologies. With the pcap files and with the packet analyser parameters such as transfer rate, latency and packet loss were obtained: in addition, the convergence of the network was analysed through the route table and the messages of each topology. Finally, the highest transfer rate was obtained in the AS 500 with 25% more than the other Autonomous Systems, the latency was higher in the AS 300 with 10% more than the other AS, the packet loss in all the topologies They were minimal. It is concluded that the teams interoperate adequately in all the topologies.

Keywords*:* <COMPUTER NETWORKS> <INTEROPERABILITY>, <MULTIVENDOR PLATFORM>. <ENTRUTAMENT PROTOCOLS (SOTWARE)>, <AUTONOMOUS SYSTEMS>, <RENDIMING PARAMETERS>.

INTRODUCCIÓN

En la actualidad el internet a revolucionado el mundo, como sabemos las redes cada día convergen y se transforman en una herramienta necesaria para la comunicación, como de compartir información, archivos, voz, etc. Todo esto se puede realizar mediante teléfonos o computadoras portátiles sin la necesidad de computadoras gigantescas como hace 30 años de la primera computadora que apareció en el Ecuador un 24 de enero de 1984.

En los últimos años se a incrementado el 13.7% en equipamientos de computadoras portátiles, y 9 de cada 10 hogares poseen al menos un teléfono celular en el Ecuador; donde, en 36% de los hogares a nivel nacional tiene acceso a internet, el 24.5% accede a través de algún medio inalámbrico. Se conoce que el 54.2% de la persona mayor utilizan computadoras, donde Chimborazo ocupa el 15 puesto de las 19 provincias en usos de computadoras. (ENEMDU, 2013, http://www.ecuadorencifras.gob.ec/documentos/webnec/Estadisticas_Sociales/TIC/Resultados_principales_140515.Tic.pdf)

Necesitamos un proceso que nos permita acceder a la información necesaria para realizar trámites, certificados o algún otro documento que necesitamos. Es por ello que en nuestro trabajo de titulación desarrollamos una plataforma para evaluar los protocolos, donde se pueda interoperar con distintas marcas de equipos. En base a esto crear a futuro unas plataformas virtuales donde puedan acceder los usuarios sin la necesidad de acercarse a las instituciones. Un ejemplo de ello es Una Plataforma de interoperabilidad del estado de Perú, donde las empresas particulares o privadas acceden a esta plataforma para brindar sus servicios de manera ágil y actualizada. Hoy en día son más 296 entidades donde 210 ofrecen servicios Web y tiene una interoperabilidad del 99.9% entre las entidades.

ANTECEDENTES

Para mediados de 1980 las empresas empezaron a conectarse a través de la red produciendo un enorme crecimiento en cantidad y tamaño, existía problemas de incompatibilidad de redes. ISO investigó modelos de conexión como la red Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (Systems Network Architecture, SNA) y TCP/IP, a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

En los últimos años muchas empresas han manifestado su interés por crear e integrarse a redes de comunicación, un ejemplo es CNT que brinda servicios de telecomunicaciones. Para que esto pueda ser manejado se crearon protocolos que solucionarían problemas presentados en la red.

Los protocolos de enrutamiento se han usado en redes desde comienzos de la década de los ochenta, debido a la evolución de las redes y su complejidad cada vez mayor han surgido nuevos protocolos. Uno de los primeros protocolos desarrollado fue Routing Protocol Information (RIP).

Que evolucionaria en su nueva versión RIP v2, para abordar las necesidades de redes más amplias se desarrollaron dos protocolos de enrutamiento avanzados. Open Shortest Path First (OSPF) e Intermediate System-to-Intermediate System (IS-IS). Cisco desarrolló el Interior Gateway Routing Protocol (IGRP) y el Enhanced IGRP (EIGRP), que escala bien en implementación de redes de grandes escalas.

BGP es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

Estos protocolos se usan para intercambiar información de enrutamiento entre los Routers, cuando se produce un cambio de topología, este intercambio permite que los Routers aprendan automáticamente sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla en el enlace de red actual.

Una plataforma Multivendor fue desarrollada por la ISO en 1978 para definir claramente la interfaz y los protocolos proporcionando a los usuarios de las redes y que estas estén construidas perfectamente.

Debido a la necesidad de evaluar la red en la FIE utilizaremos una plataforma Multivendor para determinar los algoritmos de enrutamiento, su rendimiento dentro de la red LAN/WAN incluyendo aspectos de seguridad.

FORMULACIÓN DEL PROBLEMA

El desarrollo de la plataforma permitirá evaluar los algoritmos de enrutamiento IGP y EGP más adecuados para el transporte de datos en redes convergentes.

JUSTIFICACIÓN TEÓRICA

La interoperabilidad es la habilidad de que dos o más sistemas puedan intercambiar información.

En Latinoamérica existe el caso más reciente su Proyecto de Gobierno Electrónico 2009, Plataforma de Interoperabilidad del Estado Peruano, teniendo como proyecto piloto un servicio denominado Constitución de Empresas en Línea, en la que intervienen 296 entidades públicas, actualmente en funcionamiento. El proyecto se ejecutó entre los años 2007 y 2011, es un proyecto modelo de interoperabilidad de éxito a estudiar, estrategias empleadas, liderazgo político y técnico, equipos multidisciplinarios, entre otros.

El beneficio que en nuestro país exista interoperabilidad mejoraría las relaciones con los clientes y los servidores, además de aprovechar al máximo la red. Para ellos se cuenta con plataformas comerciales de emulación para la implementación de redes como Mikrotik, Cisco, Brocade y Juniper. Se necesita que estos sistemas cooperen entre si y poder formar una gran entidad que proporcione los recursos necesarios que requieren lo clientes e incluso otras empresas, llevando un mutuo acuerdo de cooperación para que coexista la unión de diferentes entidades proporcionando la información necesaria a los clientes y estos puedan acceder desde cualquier sitio a través de la red.

La información debe ser la requerida por el cliente y por medio de políticas de cada empresa que estos accedan sin la necesidad de acercarse a las instituciones, una plataforma Multivendor de interoperabilidad actualmente no existe en el Estado Ecuatoriano por diversas dificultades de coordinación entre entidades o porque el Estado no apuesta por innovar en tecnología, que es la base

del futuro hoy en día. Muchos tramites aún son antiguos y con poca fiabilidad, además no olvidemos que somos un país en proceso de desarrollo es por el mismo hecho de no contar con la tecnología necesaria para crear nuevos grupos de trabajo.

Evolucionar hoy para que exista un desarrollo tecnológico, aceptando que estamos en una era donde la tecnología inunda los hogares.

JUSTIFICACIÓN APLICATIVA

La necesidad de que hoy en día existan redes que dispongan de una plataforma Networking que nos permita evaluar la interoperabilidad existente entre los diferentes protocolos utilizados, además existen diferentes sistemas informáticos de distintos fabricantes, por ellos, nos obliga a mantener más de un sistema para las tecnologías de integración existes de comunicación. Gracias a este proyecto mejoraríamos la infraestructura tecnológica, optimizamos recursos, con la ayuda de Ostinato que es un generador de tráfico inyectaremos tráfico a la red y Wireshark como analizador de tráfico de paquetes de redes de comunicaciones, donde conoceremos los problemas reales que existen en empresas e instituciones, con esto ayudaremos a profesionales y estudiantes a conocer los verdaderos inconvenientes que existen dentro de una red.

Debemos de tomar en cuenta que en nuestro país no existen equipos de enrutamiento avanzados, la mayoría de centros trabaja con Equipos Cisco, pero en un futuro podremos apostar por la tecnología que cada día avanza a pasos agigantados y conecta a todo el mundo.

Nuestro proyecto pretende dar a conocer el grado de interoperabilidad entre equipos de enrutamiento de diferentes marcas, como ejemplo tenemos Cisco, Juniper, Mikrotik, Brocade cada uno de estos equipos posee sus políticas por ello debemos conocerlas para que estas se puedan conectar. Al crear una plataforma queremos dar a conocer los parámetros de rendimiento que ofrece y sus beneficios a pesar de ser una innovación en el Estado Ecuatoriano ya existe en otros países como Perú donde en la actualidad están afiliadas más de 200 empresas grandes y pequeñas, públicas o privadas. Aplicando esta plataforma desarrollaremos una manera fiable, fácil y sin tantos trámites para obtener algún documento de las empresas que se encuentran dentro de la plataforma.

En un futuro se pueda llevar a cabo un proyecto de esta magnitud en gran escala o pequeña para que sirva como pilar en futuros apostadores por la tecnología. Nuestra plataforma Multivendor de Interoperabilidad dará a conocer el funcionamiento de la red dentro de un sistema autónomo y fuera de él. Además de algunos parámetros de calidad como Ancho de banda, perdida de paquetes entre

otros serán los parámetros más importantes a tomar en cuenta y conoceremos el funcionamiento de los equipos de enrutamiento.

OBJETIVOS

OBJETIVOS GENERAL

Desarrollar una plataforma Multivendor Networking para la evaluación de la interoperabilidad de los protocolos de routing IGP y EGP.

OBJETIVOS ESPECÍFICOS

- Estudiar las plataformas de equipamiento de Networking existentes.
- Verificar el grado de interoperabilidad entre los algoritmos de routing IGP y EGP.
- Desarrollar escenarios de pruebas que simulen redes convergentes acordes a los requerimientos de datos de redes corporativas públicas en la provincia de Chimborazo.
- Realizar un banco de pruebas y verificar el adecuado funcionamiento de los protocolos IGP y EGP seleccionado.

CAPÍTULO I

1. MARCO TEORICO

1.1. Enrutamiento Dinámico

Según el RFC 1058 (Routing Information Protocol), un protocolo existe para intercambiar información con otros hosts, pero este es limitado según el camino que recorra para las actualizaciones o para que el paquete llegue a su destino. De ahí se derivan los IGP y los EGP.

1.1.1. Definición

Los protocolos de enrutamiento permiten descubrir de forma dinámica la estructura de la red, (Ver Figura 1-1), permitiendo adaptarse a los cambios, de tal modo que, si un Router falla o se añade, se agregaran nuevos caminos hacia las redes de destino. Cuando una red destino es alcanzable por varios caminos se debe elegir uno de ellos para enviar el tráfico, a cada camino se le asigna una métrica; el cual se calcula de forma diferente según el algoritmo de enrutamiento utilizado. (Verón, 2010, p.49)

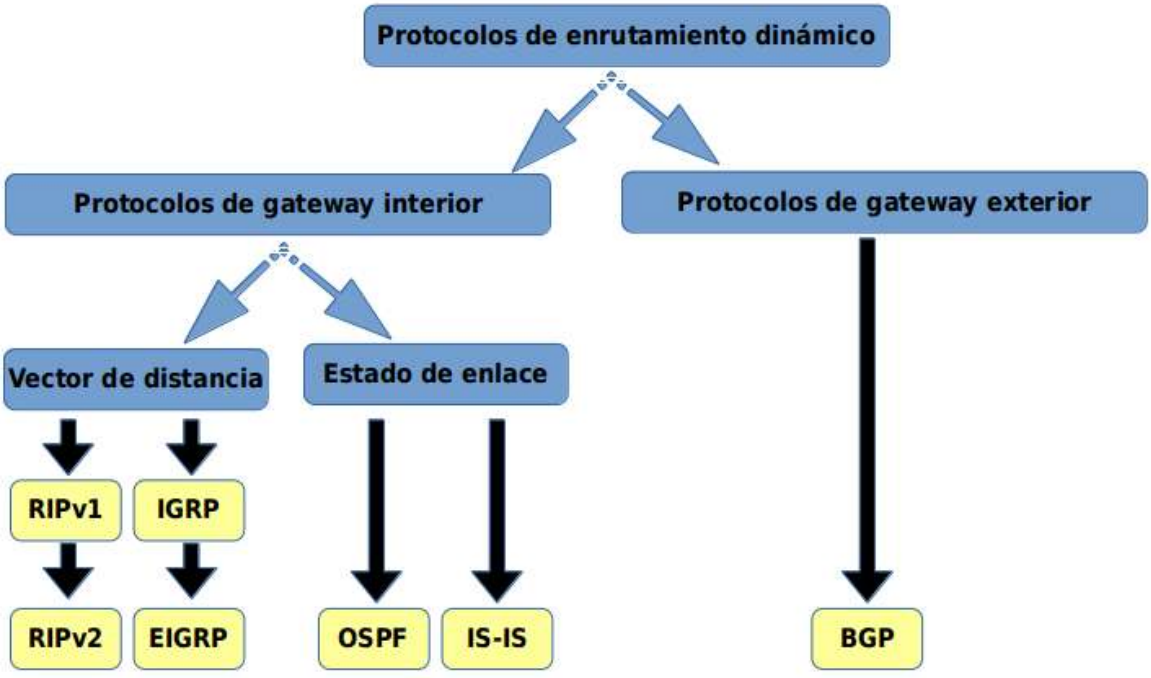

Figura 1-1 Tipos de Enrutamiento

Fuente: (https://planificacionadministracionredes.readthedocs.io/es/latest/Tema10/Teoria.html)

1.2. Protocolo Gateway Interior

Los protocolos de enrutamiento poseen nuevas capacidades en ingeniería de tráfico para crear accesos a puertas de enlace interior; es decir, el camino más corto. Los IGP de estado de enlace calculan la IP para reenviar el tráfico a través de túneles. (N. Shen, 2004, p.1)

1.2.1. IS-IS

IS-IS es uno de un conjunto de estándares internacionales producidos para facilitar la interconexión de sistemas abiertos, es un protocolo de la capa de red. Este protocolo permite que sistemas intermedios dentro de un enrutamiento de dominio intercambien información de configuración. El protocolo de enrutamiento IS-IS intra-dominio está diseñado para soportar grandes dominios de enrutamiento que consiste en muchas combinaciones de subredes, esto incluye enlaces punto a punto, multipunto. Según el RCF 3784, para admitir enrutamientos de dominios grandes se debe organizar jerárquicamente y se divide en áreas administrativas. (D. Oran, 1990, p.2)

1.2.1.1. Protocolo ISO IS-IS

IS-IS ha desarrollado en ISO entornos puros, donde la red se divide en dominios de enrutamiento y estos están definidos por la administración de la red, se establecen algunos enlaces externos. Si un enlace este, marcado como "exterior", no se envían mensajes de enrutamiento IS-IS en este enlace. (R. Callon, 1990, p.5)

OSI IS-IS hace uso del enrutamiento jerárquico de dos niveles (Ver Figura 2-1), los enrutadores de nivel 1 conocen la topología en su área, incluidos todos los enrutadores y sistemas finales. Los enrutadores de nivel 1 no conocen la identidad de enrutadores o destinos fuera de su área, los enrutadores de nivel 1 reenvían todo el tráfico hacia fuera de su área como un nivel 2; del mismo modo los enrutadores del nivel 2 conocen su topología y direccionamiento dentro de su área. (R. Callon, 1990, p.6)

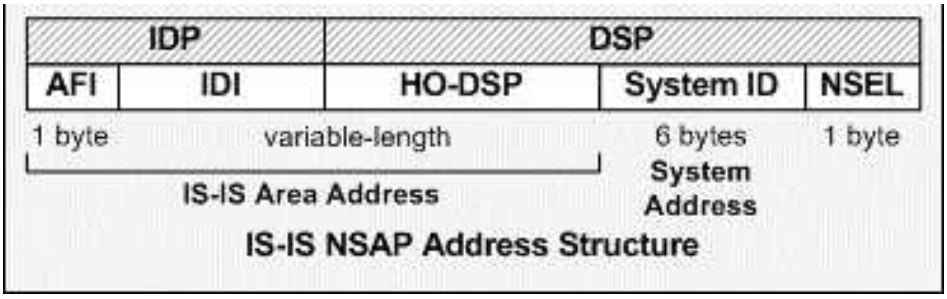

Figura 2-1 Estructura Jerárquica de direcciones ISO

Fuente: (https://www.itcertnotes.com/2012/02/network-service-access-point-nsap.html)

Las direcciones ISO se subdividen en Parte de dominio inicial (IDP) y la parte especifica de dominio (DSP), los IDP es la parte que esta estandarizada con los ISO y especifica el formato. El DSP se subdivide en HO-DSP, un identificador de sistema (ID) y un NSAP selector (SEL), estos identifican tanto el dominio de enrutamiento como el área dentro del dominio de enrutamiento. (R. Callon, 1990, p.6)

1.2.1.2. Características

- Envía paquetes Hello cada 10 segundos
- Sus actualizaciones sincronizan las rutas completas dentro de la topología cada 10 minutos.
- Es un AS dentro de un IGP.
- Es un Protocol de Routing Classless
- Si no obtiene respuesta del vecino dentro de los 30 segundos lo considerara muerto.
- Utiliza VLSM
- La utilización de los recursos el alto.

1.2.1.3. Tipos de enrutadores

Sistemas Intermedios de Nivel 1: Estos nodos se basan en la ID de la dirección ISO, enrutan dentro de un área; ellos conocen la dirección de destino de un paquete, si el destino está dentro del área. Si es así, se dirigen hacia el destino de lo contrario se dirigen al enrutador de nivel 2 más cercano. (R. Callon, 1990, p.7)

Sistema Intermedio de Nivel 2: La ruta de estos nodos se basa en el área de dirección; es decir la combinación de IDP, HO-DSP. Ellos enrutan hacia una área sin tener en cuenta la estructura interna del área, un nivel 2 IS también puede ser un Nivel 1 IS. (R. Callon, 1990, p.7)

1.2.1.4. Formato de la Cabecera de IS-IS

Permite utilizar un único protocolo de enrutamiento para enrutar los paquetes IP y OSI. Cada área será especificada para ser solo de IP, (solo IP puede enrutarse en esa área en particular), solo OSI (Solo el tráfico OSI puede enrutarse en esa área) o dual (tanto el trafico IP como el OSI pueden enrutarse en el área). Esto quiere decir que no se permite la superposición parcial de las áreas OSI e IP, por ejemplo, si un área es solo OSI y otra área es solo IP, entonces no está permitido tener algunos enrutadores en ambas áreas. (R. Callon, 1990, p.9)

La estructura de la dirección IP permiten que las redes se particiones en subredes y estas se subdividan en otras subredes; sin embargo, no existe relación entre direccione de subred IP y áreas IS-IS, incluso si las direcciones IP no son ya pre-asignadas, las direcciones Ip pueden ser asignadas de forma completamente independiente de las direcciones OSI y del área IS-IS. (R. Callon, 1990, p.9)

A continuación, en la Figura 3-1 indicaremos el formato de la cabecera que utiliza IS-IS para el envió de paquetes entro de la red.

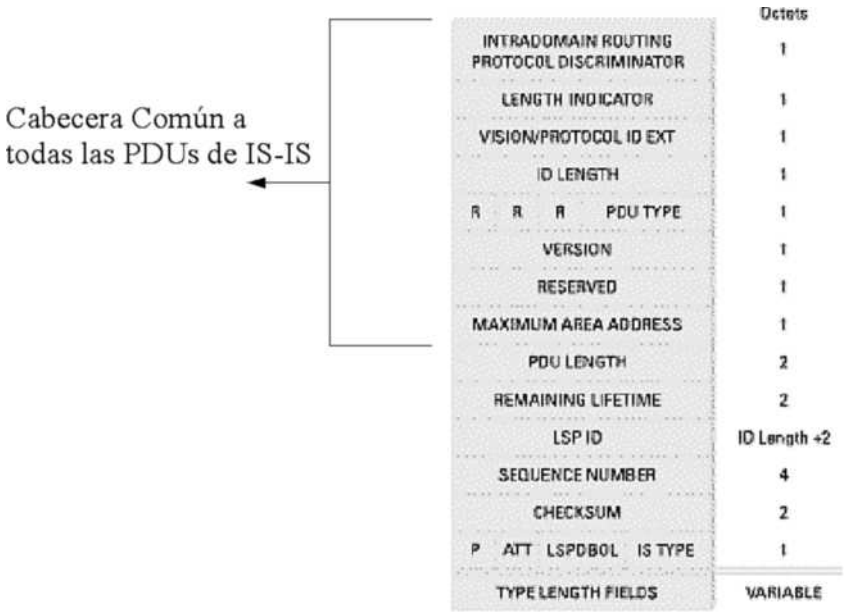

Figura 3-1 Formato de Cabecera de IS-IS

Fuente: (https://www.eduangi.org/node299.html)

1.2.1.5. Tipos de PDU

Los paquetes que transporta IS-IS se clasifican en tres categorías:

- Los paquetes Hello se utilizan para establecer y mantener adyacencia entre nodos (LAN Level-1 – Hello), (LAN Lvel-2 – Hello), (Hello – punto a punto).
- LSPs (Link - State - Packets), se utiliza para distribuir la información de enrutamiento entre nodos IS-IS.
- SNPs(Sequence – Numer – Packets), Se utiliza para controlar los LSPs.

1.2.2. OSPF

OSPF es un protocolo de Enrutamiento de Internet, es una puerta de enlace interna esto significa que distribuye información de enrutamiento entre enrutadores que pertenecen a un único sistema Autónomo. El protocolo OSPF ha sido diseñado según RFC 1583, expresamente para el entorno de internet, incluido el soporte explícito de subredes IP. (J. Moy, 1991, p.2)

1.2.2.1. Introducción

OSPF enruta paquetes IP basados únicamente en la dirección IP, es un protocolo de enrutamiento dinámico detecta rápidamente los cambios topológicos en el AS y calcula nuevas rutas sin bucles después de un periodo de convergencia. Es un protocolo basado es SPF, cada enrutador mantiene una base de datos describiendo la topología del sistema autónomo, donde todos los enrutadores ejecutan exactamente el mismo algoritmo. (J. Moy, 1991, p.2)

OSPF calcula rutas separadas para cada tipo de servicio, además de la configuración flexible de subredes IP. Todos los intercambios de protocolos OSPF están autenticados, esto significa que solo los enrutadores confiables pueden participar en el enrutamiento del sistema Autónomo. (J. Moy, 1991, p.3)

1.2.2.2. Mensajes en OSPF

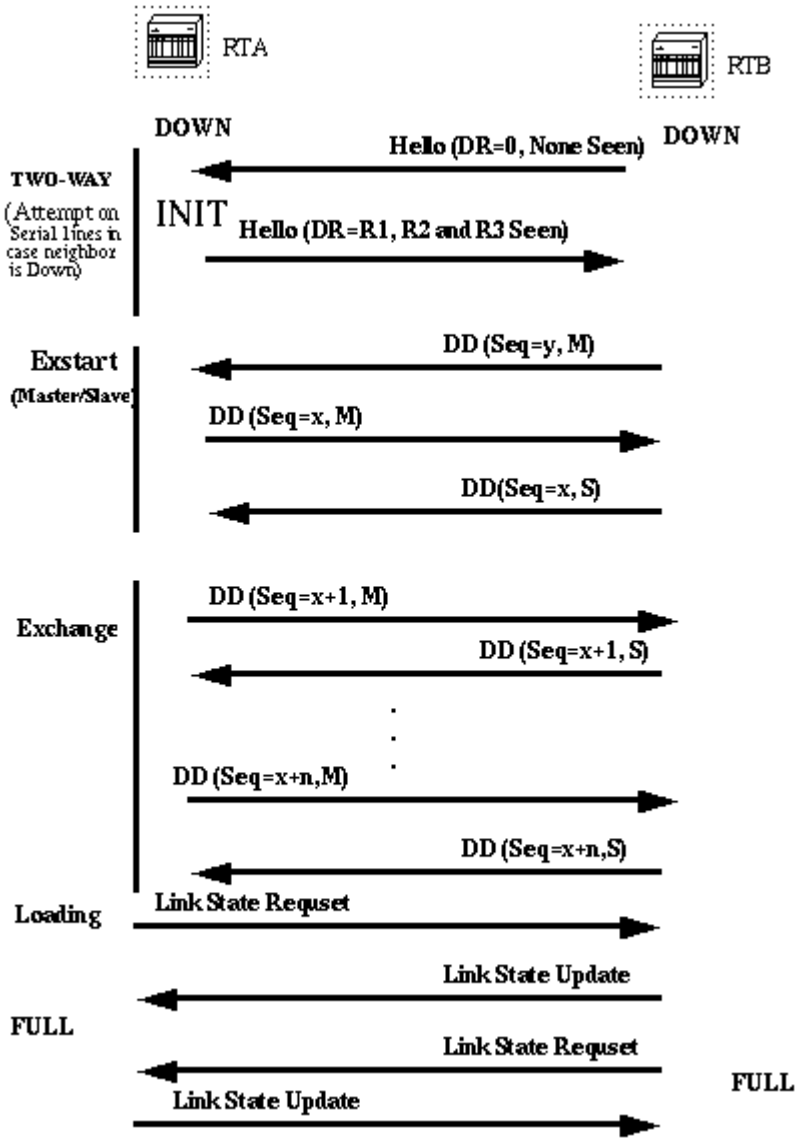

Figura 4-1 Mensajes OSPF

Fuente: (https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html)

En la Figura 4-1 se observa los estados de los Routers, en Exstart se establece una relación maestro / esclavo esto se utiliza para determinar estados link (LSA). En el estado intercambio, se intercambian paquetes de descripción (DD), donde el encabezado proporciona suficiente información de todos los paquetes transmitidos y recibidos dentro del protocolo OSPF. (Cisco, 2005, https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html)

1.2.2.3. Características

- Enrutador

Un conmutador de paquete de protocolo de internet de tercer nivel.

- Sistema Autónomo

Grupo de enrutadores que intercambian información de enrutamiento a través de un protocolo de enrutamiento denominado AS.

- ID de Enrutador

El numero de 32 bits asignado a cada enrutador que ejecuta el protocolo OSPF, identifica de manera única el enrutador dentro de un Sistema Autónomo.

- Mascara de Red

Un número de 32 bits que indica el rango de direcciones IP que residen en una red/subred, se muestra las máscaras de red como número hexadecimales.

- Redes de Acceso Múltiple

Esas redes físicas que admiten el archivo adjunto de múltiples enrutadores, cada par de enrutadores en dicha red se supone que es capaz de comunicarse directamente.

- Interfaz

La conexión entre un enrutador y una de sus redes conectadas. Una interfaz tiene información de estado asociada a ella, que es obtenida a partir de los protocolos subyacentes de nivel inferior y el enrutamiento si una interfaz de una red tiene asociado una única red IP y mascara.

- Proximidad

Una relación formada entre enrutadores vecinos seleccionados para el propósito de cambiar información de enrutamiento. No todos los pares de enrutadores vecinos de vuelven adyacentes.

- Anuncio de entado de Enlace

Describe el estado local de un Enrutador o red. Esto incluye el estado de las interfaces del enrutador. Los anuncios del estado de enlace recopilados de todos los enrutadores y redes forman la base de datos topológica del protocolo.

- Hello Protocolo

La parte del protocolo OSPF utilizada para establecer y mantener relaciones vecinas. En redes de acceso múltiple, el protocolo Hello también puede descubrir dinámicamente los enrutadores vecinos.

- Enrutador Designado

Cada red de acceso múltiple que tiene al menos dos enrutadores conectados tiene un enrutador designado. El enrutador designado genera un estado de enlace para la red de acceso múltiple y tiene otra responsabilidad en la ejecución del protocolo reduce la cantidad de tráfico del protocolo de enrutamiento.

1.2.2.4. Tipos de Redes Físicas

- Redes Punto a Punto

Una red que se une a un solo par de enrutadores.

- Redes de Transmisión

Redes que admiten dos o más enrutadores conectados con la capacidad de dirigir un solo mensaje físico a todos los enrutadores conectados, se descubre nuevos enrutadores vecinos dinámicamente en las redes que utilizan el Protocolo Hello de OSPF. El protocolo Hello aprovecha la capacidad de transmisión en el uso de Multicast.

- Redes no Transmitidas

Son redes que admiten dos o más enrutadores, pero que no tiene capacidad de transmisión, debido a esto se necesita información de configuración para el correcto funcionamiento del protocolo Hello. Dos enrutadores unidos por una red punto a punto están conectados directamente por un par de bordes, uno en cada dirección.

Las interfaces punto a punto no necesitan la asignación de direcciones IP, la representación gráfica de redes punto a punto es diseñado para que las redes no numeradas puedan ser compatibles de forma natural.

1.2.2.5. Formato de Cabecera

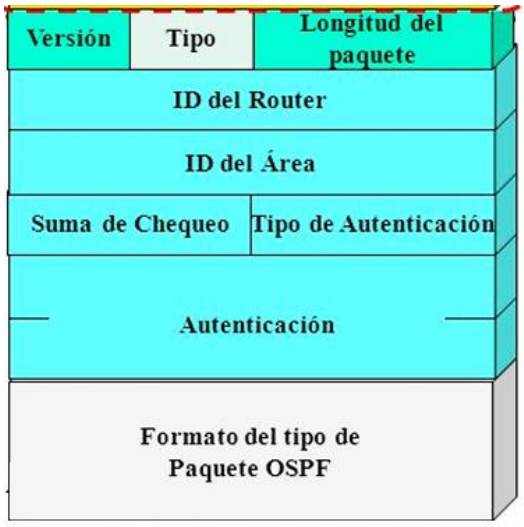

Figura 5-1 Formato de Cabecera OSPF

Fuente: (https://slideplayer.es/slide/16764/)

Los tipos de paquetes del formato de OSPF se encapsulan del siguiente modo (Ver Figura 5-1).

- Tipo 1: Hello

Es quien descubre nuevos router y los mantiene como vecinos.

- Tipo 2: DBD (Data Base Description)

Es quien describe el contenido de la base de datos de la topología.

- Tipo 3: LSR (Link Stare Request)

Descarga todo el registro que se halla en la Base de datos.

- Tipo 4: LSU (Link State Update)

Es la que se encarga de actualizar la base de datos.

- Tipo 5: LSA (Link State Acknowled)

Es el reconocimiento de los paquetes de estado de enlace.

1.2.3. RIP V1

1.2.3.1. Introducción

Es un protocolo simple que se actualiza cada 30 segundos, trabaja bien en redes pequeñas. El problema con Rip se encuentran en los tiempos de convergencia que son muy elevados para redes grandes. RIP es un protocolo de una clase de algoritmos conocidos como Vector Distancia según la (RFC 1058), está diseñado para ser utilizado en internet basado en IP.

El internet está en una serie de redes conectadas por puertas de enlace, las redes pueden ser punto a punto o redes más complejas como Ethernet. Las puertas de enlace se presentan con datagramas de IP dirigidos a algún host; donde el enrutamiento es el método por donde el host o la puerta de enlace deciden a donde enviar el datagrama. (C. Hedrick, 1988, p.3)

1.2.3.2. Limitaciones del Protocolo

Este protocolo no resuelve todos los problemas de enrutamiento, en redes homogéneas de tamaño moderado. El protocolo está limitado en redes cuyo camino más largo implica 15 saltos, este diseño básico del protocolo es inapropiado para redes más grandes. Si el administrador del sistema elige usar costos más grandes el límite superior de 15 saltos puede convertirse en un problema.

Este protocolo usa métricas fijas para comparar rutas alternativas, no es apropiado para rutas donde necesita ser elegido en base a parámetros en tiempo real ya que existe retraso.

1.2.3.3. Formato de Cabecera de RipV1

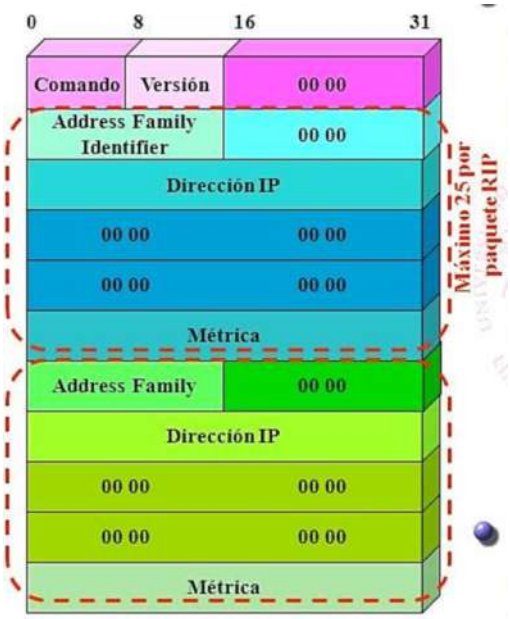

Figura 6-1 Formato de Cabecera RipV1

Fuente: (https://slideplayer.es/slide/16764/)

Cuando cualquier host que utiliza RIP tiene interfaces con una o más redes, esto se conoce como conexión directa; por ello, el protocolo se basa en el acceso a cierta información sobre cada una de estas redes.

La métrica para una red conectada directamente se establece en las implementaciones de RIP (Ver Figura 6-1), nos muestra el formato del mensaje que transporta RIP; además, las implementaciones también pueden optar por permitir que el administrador del sistema también ingrese rutas adicionales. Es muy probable que sean rutas hacia los hosts o redes fuera del alcance del sistema de enrutamiento.

1.2.4. RIP V2

1.2.4.1. Introducción

Según (RFC 2453), RIP es un protocolo de enrutamiento basado en el algoritmo Bellman-Ford, este algoritmo se ha utilizado para el enrutamiento en redes de computadoras desde los primeros días de

ARPANET. En una red internacional como Internet se utiliza varios protocolos de enrutamiento para toda la red, la red se organizará con una colección de sistemas autónomos y estos son administrados por una sola identidad. El protocolo de enrutamiento utilizado dentro de un AS se conoce como protocolo de puerta de enlace Interior (IGP); además de otro protocolo de puerta de enlace exterior (EGP). Rip fue Diseñado para trabajar como un IGP en AS de tamaño moderado, no está destinado para entornos más complejos. (G. Malkin, 1998, p.4)

RIP está diseñado para ser utilizado en internet basado en IP. Las redes pueden ser punto a punto, enlaces o redes más complejas como Ethernet o Token ring. El enrutamiento es el método por el cual el host decide donde enviar el datagrama directamente al destino, si este destino está en una de las redes que están directamente conectadas al host o enrutador; sin embargo, cuando el destino no está directamente conectado el host o enrutador intenta enviar el datagrama a un enrutador que esté más cerca del destino. (G. Malkin, 1998, p.5)

1.2.4.2. Características

Mientras RIP versión 2 comparte los mismos algoritmos básicos que RIP versión 1, admite varias funciones nuevas que son: etiquetas de ruta externa, mascara de subred, direcciones del siguiente salto y autenticación.

1.2.4.3. Seguridad

El protocolo RIP básico no es un protocolo seguro, para llevar RIP versión 2 con protocolos más modernos se ha incorporado una autenticación extensible que proporciona mejoras al protocolo.

1.2.4.4. Mascara de Subred

Las máscaras de Subred de RIP mejoran el protocolo, su información hace que RIP sea más útil en varios entornos y permite el uso de variedad de máscaras de subred. Las máscaras de subred son necesarias para implementar el direccionamiento dentro de la red.

1.2.4.5. Próximas Direcciones de Salto

El soporte para próximas direcciones de salto permite la optimización de rutas en un entorno que usa múltiples protocolos de enrutamiento. Por ejemplo, si RIP versión 2 se está ejecutando en una red

junto con otro IGP, y el enrutador ejecuto ambos protocolos, entonces ese enrutador podría indicar a otros enrutadores RIP versión 2 un mejor próximo salto.

1.2.4.6. Formato de Cabecera de RIPv2

Los mensajes de cabecera de RIP incluyen un máximo de 25 entradas (Ver Figura 7-1), de 20 bytes que contiene el destino, el siguiente salto, la métrica y la máscara.

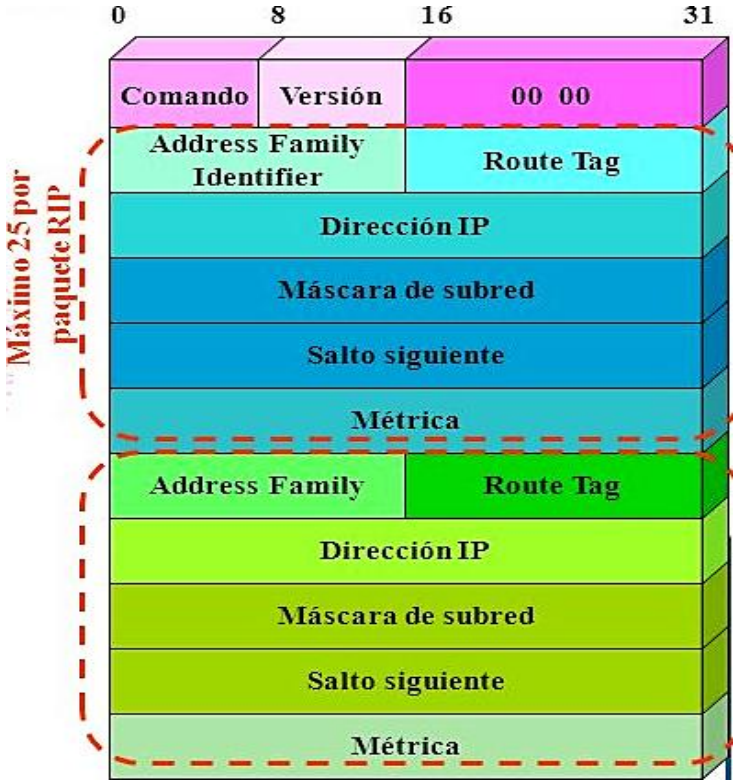

Figura 7-1 Formato de Cabecera RipV2

Fuente: (https://slideplayer.es/slide/16764/)

1.2.4.7. Mensajes RipV2

Los mensajes RIP son transportados por datagramas UDP en el puerto 520 como se puede observar en la Figura 8-1. Estos mensajes pueden ser de petición y de respuesta.

- Petición: Es alguien que recién se agrega a la red y desea información acerca del encaminamiento.
- Respuesta: Se envía actualizaciones de la tabla de enrutamiento, en un mensaje ordinario se envía cada 30 segundos donde se comunica algún cambio en la tabla entre otras características.

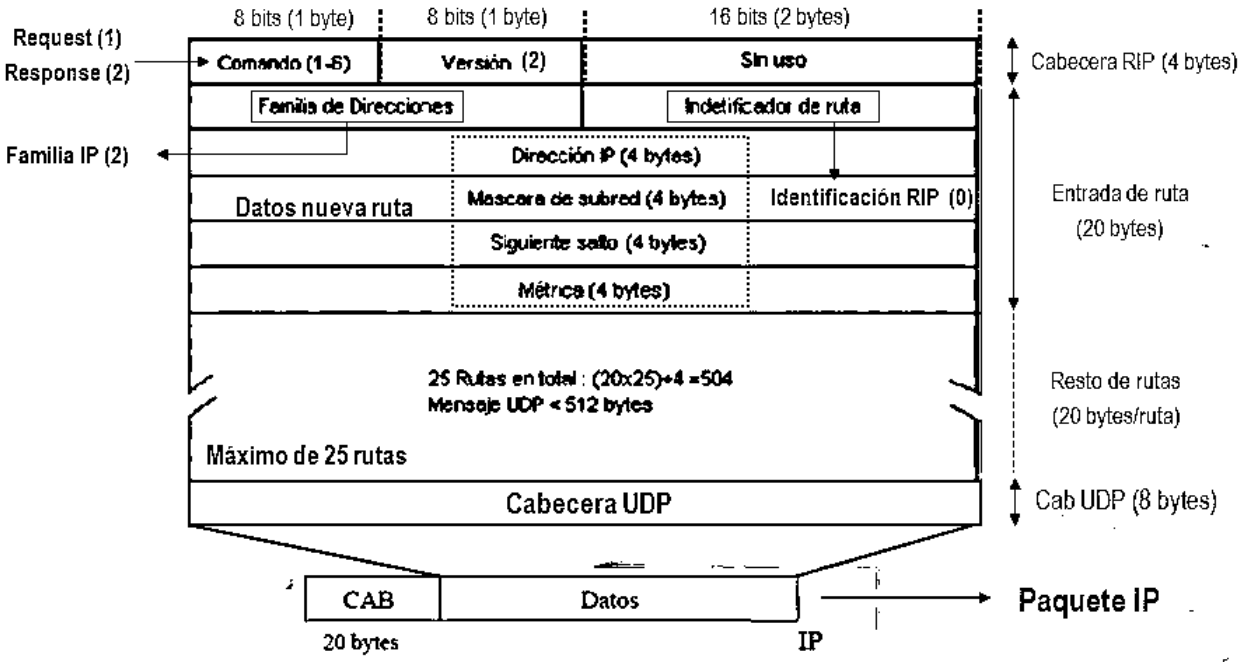

Figura 8-1 Formato de Mensajes RipV2

Fuente: (https://slideplayer.es/slide/1661098/)

1.2.5. EIGRP

1.2.5.1. Introducción

El enrutador de la puerta de enlace interior, (RFC 7868), es un protocolo diseñado y desarrollado por Cisco Systems. Este protocolo permite que todos los enrutadores involucrados en un cambio de topología para sincronizarse al mismo tiempo, los enrutadores no afectados por el cambio de topología no están involucrados en el recalculo. (D. Savage, 2016, p.5)

1.2.5.2. Paquetes EIGRP

EIGRP utiliza 5 clases de paquetes:

- Paquetes Hello
- Paquetes Query
- RESPONDER Paquetes
- SOLICITAR Paquetes
- ACTUALIZACION de Paquetes

Los paquetes EIGRP se encapsulan directamente en una capa de red de IPv4 o IPv6; mientras, EIGRP es capaz de usar encapsulación adicional. No se admite fragmentación del protocolo de capa de red, y EIGRP intentara evitar un tamaño máximo de paquetes que excedan la interfaz MTU enviando múltiples paquetes que son menores o igual a los paquetes del tamaño MTU. (D. Savage, 2016, p.21)

1.2.5.3. Terminología

- Estado Activo: El estado de una ruta local en un enrutador desencadenada por cualquier evento hace que todos los vecinos que proporcionan la ruta actual de menor costo fallen la verificación de condición de viabilidad.

- Topología de Base: Un enrutamiento de dominio que representa una vista física de la topología de la red, consiste en los dispositivos conectados y los segmentos de la red.

- Distancia Calculada: La distancia total a lo largo de una ruta desde el enrutador actual a una red de destino vecino en particular se calcula utilizando la distancia reportada de ese vecino y el costo de enlace entre los dos enrutadores.

- Computación Difusa: Un cálculo distribuido en el único nodo inicial comienza delegando subtareas de computación a sus vecinos que, a su vez, recursivamente delega tareas adicionales incluyendo el esquema de señalización permitiendo que el nodo de inicio detecte que el cálculo ha terminado mientras se evitan las terminaciones falsas.

- DUAL: El algoritmo libre de bucle utilizado en vectores distancia o estado de enlace proporciona un cálculo difuso de una tabla de enrutamiento. Funciona muy bien en presencia de múltiples cambios de topología con poca sobrecarga.

- Distancia Factible: Definido como la métrica total menos conocida para un destino del enrutador actual desde la última transición de estado activo a pasivo.

- Distancia Reportada: Para un destino particular, el valor que representa el enrutador destino según lo anunciado en todos los mensajes que llevan información de enrutamiento RD no es equivalente a la distancia actual del enrutador al destino y puede ser diferente en el proceso de recalculo del camino.

1.2.5.4. Operación de EIGRP

Ancho de Banda en enlaces de baja velocidad

EIGRP se limita a usar no más del 50% de ancho de banda informando por una interfaz el ritmo de intervalos de los paquetes. Si en ancho de bando no coincide con el físico EIGRP puede:

- Genere más tráfico de lo que la interfaz puede manejar, posiblemente ocasionando caídas, lo cual perjudica el rendimiento.
- Generar gran tráfico lo cual produce que quede poco ancho de banda restante para los datos del usuario. Para controlar tales transmisiones de define un temporizador de estimulación de interfaz en EIGRP.

1.2.5.5. Paquetes HELLO

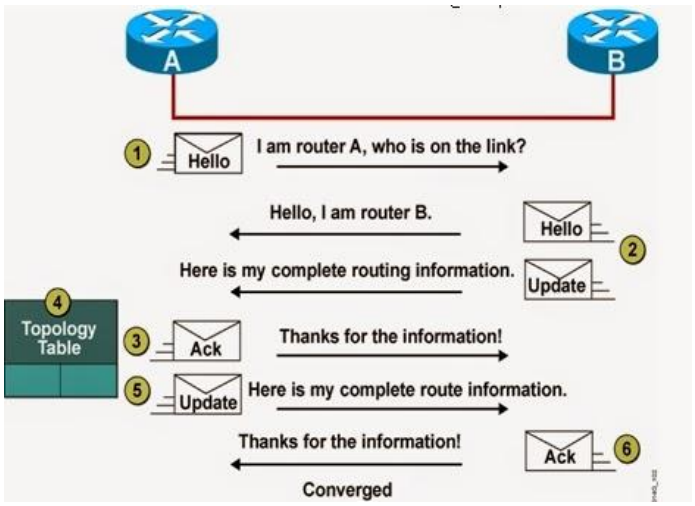

Figura 9-1 Paquetes Hello en EIGRP

Fuente: (http://ccnp-jncis-en-espanol.blogspot.com/2015/03/2-protocolos-de-enrutamiento.html)

Cuando inicia EIGRP el enrutador comienza a empaquetar cualquier interfaz en la que EIGRP este habilitado. Paquetes Hello (Ver Figura 9-1), incluirá la métrica EIGRP configurada, esto obliga a que los usos de las métricas sean constantes en todo el internet. También se incluye en el paquete HELLO un tiempo de espera, este valor indica a todos los receptores el periodo de tiempo valido en segundos. El tiempo de espera predeterminado será tres veces el intervalo HELLO, que serán transmitidos cada 5 segundos por defecto. (D. Savage, 2016, p.35)

Figura 10-1 Cabecera en EIGRP

Fuente: (https://es.slideshare.net/proventujavier/eigrp-27793963)

En la cabecera de EIGRP dependerá del tipo de mensaje (Ver Figura 10-1), algunos envían Multicast y otros unicast.

- Opcode: Especifica el tipo de paquete.
- Checksum: Se aplica a todo el paquete excepto la cabecera IP.
- Flags: El bit de inicialización que comunica con los vecinos.
- ACK y Sequence: son los portadores de mensajes fiables.
- AS Number: Identifica el proceso EIGRP.

1.3. Protocol Gateway Exterior

EGP se utiliza para intercambiar información de acceso a la red que pertenece a la misma o diferentes sistemas autónomos. Un sistema autónomo podría consistir en una única puerta de enlace, ya que su único propósito en conectar la red local al resto de internet; y no está destinado para manejar cualquier tráfico que no pertenece a la red local particular. Su propósito es permitir que uno o más sistemas autónomos se utilicen como medios de transporte en el tráfico que se origina en otros sistemas. (Eric C, 1982, p.2)

1.3.1. BGP

Según RFC 4271 (A Border Gateway Protocol), BGP es un sistema Inter-autónomo su función es interconectar Router fronterizos para que estos compartan información de red con otros Routers BGP, en esta información se incluye la ruta completa del AS (sistema Autónomo), que tráfico se debe transitar para alcanzar estas redes. Esta información es suficiente para construir un gráfico de AS, realizando conectividad desde la cual los bucles de enrutamiento pueden ser limitados y algunas políticas se pueden aplicar. BGP ejecuta un protocolo de transporte confiable, esto elimina la necesidad de implementar fragmentación, la retro-transmisión y cualquier esquema de autenticación. El mecanismo de notificación de error usado en BGP asume que el protocolo de transporte admite un cierre, es decir que todos los paquetes pendientes serán entregados antes del cierre. (Y. Rekhter, 1990, p.3)

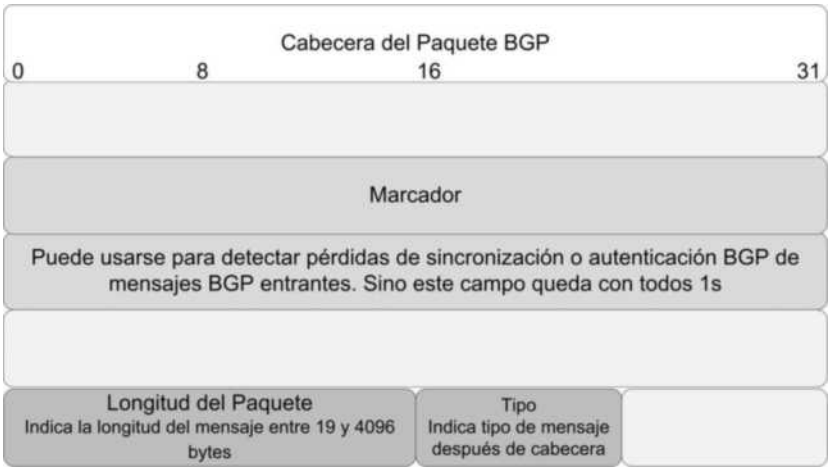

Figura 11-1 Cabecera de BGP

Fuente: (S. Pérez, 2017, https://www.researchgate.net/figure/Cabecera-de-Paquete-BGP_fig63_312029712)

Dos sistemas forman una conexión de protocolo de transporte entre ellos, intercambian mensajes al abrir y confirmar los parámetros de conexión. (Ver Figura 11-1). El flujo de datos inicial es toda la tabla de enrutamiento de BGP, los hosts ejecutan los Border Gateway Protocol no necesitan ser enrutadores. Un host sin enrutamiento podría intercambiar información de enrutamiento con enrutadores a través de EGP o incluso un protocolo de enrutamiento interior, este host no enrutador podría usar BGP para intercambiar información de enrutamiento con otro sistema autónomo. (Y. Rekhter, 1990, p.4)

Si un AS particular tiene múltiples BGP y proporciona tránsito de servicio a otros AS, se debe tener cuidado para garantizar una vista de enrutamiento dentro de un AS. Una vista consiste el interior de las rutas de un AS son proporcionadas por el protocolo de enrutamiento interior, las conexiones entre BGP de diferentes AS se conocen como “Enlaces Externos” y las conexiones entre BGP del mismo AS se conoce como “Enlace Internos”.

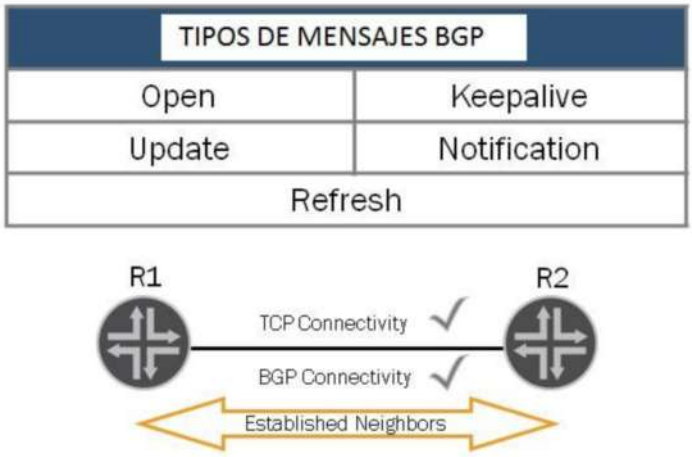

Figura 12-1 Mensajes de BGP

Fuente: (http://ccnp-jncis-en-espanol.blogspot.com/2016/03/capitulo-13-border-gateway-protocol.html)

Los mensajes se envían a través de una conexión de protocolos de transporte confiable, un mensaje se procesó solo después de haberse recibido completo. El tamaño máximo del mensaje es de 4096 octetos, el mensaje más pequeño puede ser enviado con un encabezado BGP (Ver Figura 12-1), sin porción de datos. (Y. Rekhter, 1990, p.5)

- Open: Se inicia la sesión BGP que contiene información del vecino.
- Update: Envía información a los nodos.
- Keepalive: Para verificar el temporizador.
- Notificacion: Se envía cuando algún nodo falla o un mensaje.
- Refresh: Envia las actualizaciones de las rutas.

Los mensajes de BGP determinan el camino y las rutas alcanzables.

1.4. Redes Convergentes

La convergencia se da cuando toda la tabla de enrutamiento tiene información completa y precisa sobre la red, el tiempo de convergencia es el tiempo que tarda un router en compartir la información, calcular sus mejores rutas y actualizar sus tablas.

Los Routers comparten información entre sí, pero deben calcular de forma independiente los impactos del cambio de topología en sus propias rutas. Las propiedades de convergencia incluyen:

- Velocidad de Propagación de Información de Enrutamiento
- Calculo de Rutas Optimas

Los protocolos de enrutamiento pueden clasificarse en base a la velocidad de convergencia; cuanto, más rápido sea la velocidad de convergencia mejor será el protocolo.

1.5. Parámetros de Rendimiento

1.5.1. Rendimiento

Específica la cantidad de datos que es transmitido a través de la red, el rendimiento es medido después de la transmisión de datos porque el sistema añade retardo causado por limitaciones del procesador. El rendimiento varía con el tiempo durante la transmisión de datos debido al tráfico y a la congestión, la información de las cabeceras de las tramas (direcciones de origen y destino, parámetros para intercambio de información, código para chequeo de errores, entre otros) reduce el rendimiento. (D. Bustamante, 2019, https://www.academia.edu/10963565/PARAMETROS_DE_CALIDAD_DE_SERVICIO_CALIDAD_DE_SERVICIO_QoS)

1.5.2. Retardo

El retardo de propagación es el que se origina por recorrer un paquete una distancia en cierto tiempo. Depende de los saltos que realiza el paquete hasta llegar a su destino y por ello también dependerá del protocolo.

1.5.3. Ancho de Banda

Es una velocidad o tasa a la que se introduce bits dentro de la red; además, de un rango de frecuencias que representa la manera en la que puede variar una señal.

1.5.4. Latencia

La variabilidad de la latencia en un problema, algunos protocolos dependen del tiempo. Es posible que las aplicaciones futuras sean sensibles a la latencia, la latencia se mide desde el primer bit real enviado y el tiempo que se demora en llegar a su destino.

1.6. Interoperabilidad

La capacidad de un sistema de información para comunicarse y compartir datos documentos e información, mediante la interconexión libre, automática y transparente sin dejar de utilizar en ningún momento la interfaz del sistema propio. (LF. Gomez, 2009, p.2)

La interoperabilidad debe estar basada en estándares abiertos para que se pueda comunicar con todo su entorno. La interoperabilidad se manifiesta por medio de:

- La capacidad de los sistemas para trabajar entre sí en tiempo real o programado.
- La capacidad del Software para trabajar en diferentes sistemas.
- La capacidad de los datos de ser intercambiados entre diferentes sistemas.

1.7. Plataformas de Enrutamiento

Para conocer las tendencias en tecnologías analizamos los equipos de enrutamiento según el cuadrante de Gartner, donde basado en dos criterios como la integridad y la capacidad de ejecución. Es una empresa que está encargada de la investigación de las nuevas tendencias tecnológicas dentro del mercado y los equipos más óptimos según sus características A continuación analizaremos cada uno de los equipos de enrutamiento.

1.7.1. Juniper

1.7.1.1. Introducción

Juniper Networks comercializa productos de redes, que son utilizados por proveedores de servicios ISP que sirve para enrutar el tráfico de internet. Juniper se diversifica en tres aplicaciones, en enrutadores centrales, de borde y para tráfico móvil, se enfocaron en los enrutadores de borde ya que las ISP acumulaban mucho ancho de banda en el núcleo. El primer producto de conmutación de Juniper fue EX 4200, en el 2008 siendo un conmutador de red mejorado en latencia y rendimiento que en sus características era menos robusto. En febrero del 2011, Juniper presento QFabric una metodología de protocolo para transferir datos a través de una red utilizando una sola capa de red. En el 2014 se realizó varias mejoras de software y hardware para los enrutadores Juniper, incluidas aplicaciones de software para ISP que se puede utilizar para proporcionar servicios basados en internet para los consumidores. (Infochannel, 2016, http://www.infochannel.info/juniper-networks-mejora-caracteristicas-en-ruteadores-mx)

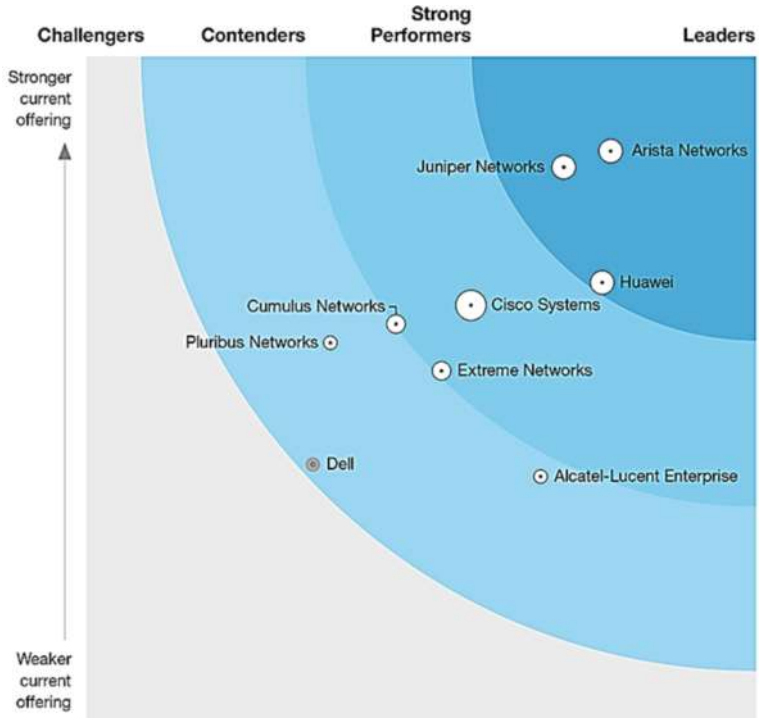

Figura 14-1 Juniper Cuadrante de Gartner

Fuente: (http://www.junipernetworksblog.com/gartner-reconoce-juniper-como-lider-en-el-cuadrante-magico-para-redes-de-centro-de-datos-en-2018)

Según los análisis realizados se determina que Juniper será una plataforma a futuro, gracias a sus estándares abiertos y alto rendimiento en redes corporativas. Ver Figura 14-1

1.7.1.2. Características

- Las aplicaciones de distribuirán por medio de nubes hibridas, se adapta según las necesidades.
- Ofrece una seguridad de extremo a extremo, automatiza las políticas evitando que existan cyber ataques.
- Organización entre entornos Multivendor complejos, permite una adecuada administración de los equipos, con estándares abiertos.
- Alto rendimiento, para Juniper sus aplicaciones de red cubren todas las necesidades en centros de datos de gran volumen optimizando los servicios IP.
- Servicios y Políticas, posee dispositivos virtuales; además, su configuración hibrida se extiende hasta las redes corporativas.
- Cooperación Tecnológica, Juniper se alinea a los estándares mundiales dando soluciones a múltiples proveedores proporcionando flexibilidad a sus clientes.

1.7.2. Brocade

Brocade establece las bases para una arquitectura de servicios de red flexible, fácil de usar y alto rendimiento capaz de satisfacer las demandas actuales y futuras de la red. Brocade aumenta la escalabilidad y posee agilidad entre los enrutadores de núcleo.

Según análisis del cuadrante de Gartner Brocade se ubica entre los productos innovadores (Ver Figura 15-1), ofrece buenas funcionalidades y un número considerable de productos en el mercado.

Figura 15-1 Brocade Cuadrante de Gartner

Fuente: (http://www.computing.es/infraestructuras/informes/1034794001801/cuadrante-magico-gartner-application.1.html)

1.7.2.1. Características

- Se ajusta rápidamente al cambio de la red y el tráfico.
- Facilita el camino entre la nube y sus usuarios finales con una arquitectura que simplifica sus operaciones y brinda visibilidad de tráfico.
- Habilita redes definidas por software con soporte para OpenFlow, al mismo tiempo que incrementa el reenvió tradicional de la capa 2 y capa 3.

1.7.3. Cisco

Cisco es un líder innato (Ver Figura 15-1), tanto en la seguridad que ofrece como el posicionamiento en el mercado. Es una base de red solida centrada en la seguridad y eficiencia de la misma. Analiza minuciosamente las amenazas y ejecuta protecciones de seguridad para proteger las organizaciones de inminencias conocidas, desconocidas y emergentes. Permite automatización mediante la arquitectura integrada, trabajo conjunto a diversas herramientas para la detección más rápida, bloqueo y respuesta. (G. Rittenhouse, 2018, https://gblogs.cisco.com/la/sc-geeritt-cisco-lider-en-firewalls-de-redes-empresariales-segun-el-cuadrante-magico-de-gartner-2018-para-firewalls-de-redes-empresariales/).

Figura 16-1 Cisco Cuadrante de Gartner

Fuente: (https://www.linkedin.com/pulse/gartner-data-center-networking-2016-roberto-fraile)

1.7.3.1. Funciones

- Comunicación en la capa 2 y capa 3.
- Encapsulamiento MPLS a través de Ethernet
- El receptor que maneja la dirección de tráfico esta bifurcado para permitir la funcionalidad de no bloqueo.

1.7.4. Mikrotik

1.7.4.1. Introducción

Mikrotik es una empresa que se fundó en 1996 para desarrollar enrutadores y sistemas ISP inalámbricos, ahora posee hardware y software para la conectividad a internet. Tiene un sistema de software RouterOS que proporciona gran estabilidad, controles para todo tipo de interfaces de datos y enrutamiento.

1.7.4.2. Características

- Estabilidad
- Control
- Flexibilidad

Además, Mikrotik soporta rutas estáticas con varios protocolos de enrutamiento, en IPv4 puede trabajar con RIPv1 y v2, OSPF v2 y BGP v4. Un componente importante de Mikrotik es Winbox, que es un administrador de las direcciones que maneja Mikrotik dentro de sus configuraciones.

1.8. Generadores y Analizadores de Trafico

1.8.1. Analizadores de Paquetes y de Red

Existen muchas herramientas que recolectan el tráfico de la red y la mayoría de ellas utilizan pcap, que son sistemas similares a Unix.

Un rastreador de paquetes es una herramienta útil que le permite implementar la política de capacidad de red de su empresa como beneficios obtenemos:

- Identificar enlaces congestionados.
- Identificar las aplicaciones que generan más tráfico.
- Recopilar datos para el análisis predictivo.
- Destacar picos y valles en la demanda de la red.

Las acciones que se realicen dependerán del presupuesto de las empresas rastreando los paquetes que permitirán dirigir nuevos recursos para ampliar la capacidad de la red. Si no es así la detección de paquetes ayudara a configurar el tráfico priorizando las aplicaciones, redimensionando las subredes, redireccionando el tráfico, limitando el ancho de banda en aplicaciones específicas.

1.8.1.1. Tipos de Trafico de Red

El análisis de tráfico requiere una comprensión completa de cómo funciona la red, existen dos clases de tráfico el ARP Y DHCP. Cuando se trabaja a nivel empresarial la mayor parte se centra en el flujo de tráfico y no en el contenido del paquete; entonces, determinamos que lo más importante dentro de una red empresarial será evitar los cuellos de botella en el rendimiento.

1.8.1.2. Cómo funcionan los Analizadores de Redes y Paquetes

Las características más importantes de un Analizador de paquetes son los datos que viajan a través de la red, un dispositivo de rastreo copia todos los datos y los guarda en un archivo. La información recopilada puede ser de gran importancia como datos del administrador de la red codificada, si la carga útil de paquetes no este encriptada permitirá que cualquier persona que obtenga esta información pueda verla, es por ellos que muchos analizadores de paquetes están limitados a copiar solo información de encabezado.

1.8.2. Analizador Wireshark

Es una de las herramientas más conocidas entre los sistemas de administración, es un analizador de paquetes, recopila los datos luego los analiza en un solo lugar en un archivo pcap. Wireshark le permite cargar un archivo existente y empezar a capturar el tráfico de la red, opcionalmente puede especificar filtros para reducir la cantidad de datos. Si no especifica los filtros Wireshark recopilara todos los datos de la red.

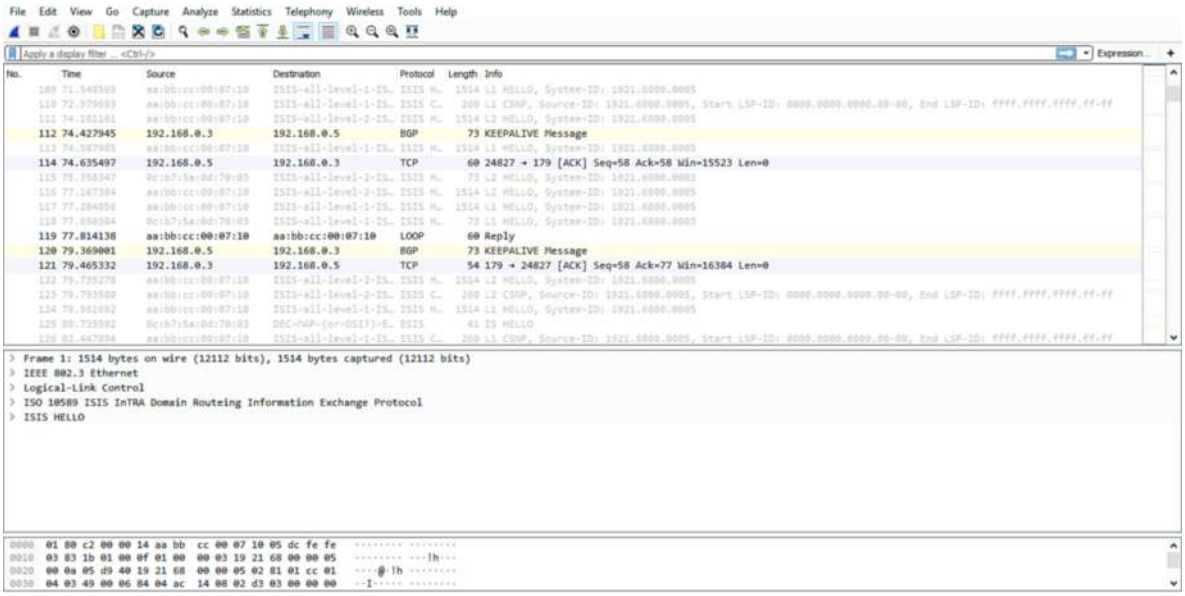

Figura 17-1 Interfaz de Wireshark

Fuente: (https://www.researchgate.net/figure/Screenshot-of-wire-shark_fig2_220902180)

1.8.2.1. Características

- Inspección profunda con cientos de protocolos.
- Captura en vivo y analiza fuera de línea.
- Multiplataforma: se ejecuta el Windows, Unix, Linux, Solaris y muchos más.
- Los datos de red capturados se pueden explorar a través de una GUI.
- Análisis extenso en VoIP.
- Los archivos comprimidos capturados son descomprimidos sobre la marcha.
- Los datos en vivo se pueden leer desde Ethernet, IEEE 802.11, PPP/ISAKMP, Kerberos, WPA Y WPA2.

1.8.3. Analizador Stellcenter

Es un analizador de protocolos que acelera el análisis de paquetes de red y la creación de informes de archivos de seguimiento de gran tamaño mediante una interfaz gráfica de usuario y una amplia selección de vistas de análisis predefinidas.

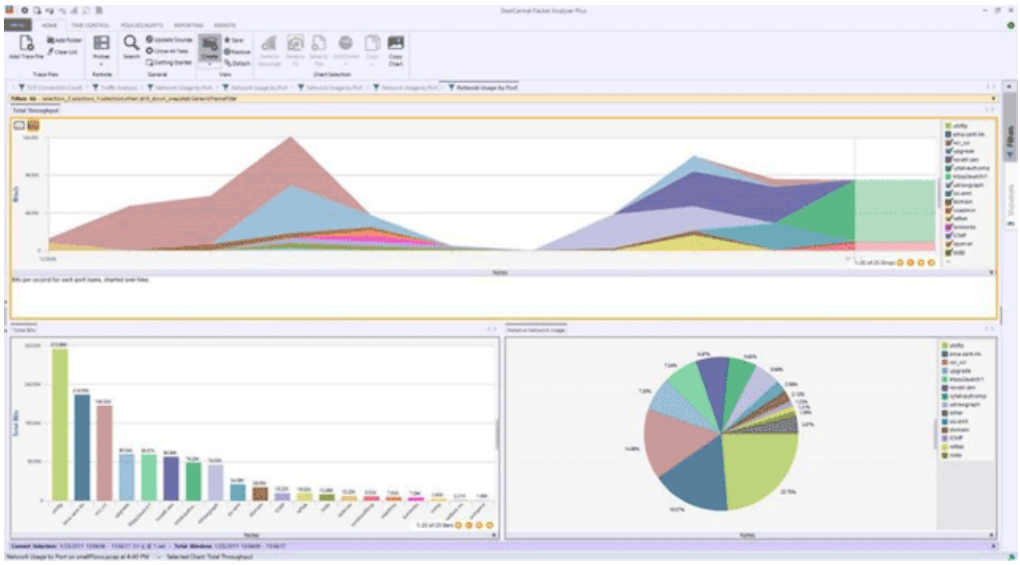

Figura 18-1 Interfaz de StellCenter

Fuente: (https://www.riverbed.com/mx/products/steelcentral/steelcentral-packet-analyzer.html)

1.8.3.1. Características

- Identifica y Soluciona con rapidez problemas con el desempeño de las aplicaciones y las redes.
- Se puede analizar gracias a su integración con Wireshark.
- Vistas de análisis completas para la solución de problemas de forma visual.
- Decodificaciones para VoIP (SIP, H323, SCCP).
- Aislamiento de transiciones específicas para el análisis sin conexión.

1.8.4. Generador Ostinato

Ostinato es un potente generador de tráfico de código abierto recreando escenarios mediante la generación de dispositivos en una plataforma de estudio, basados en ciertas estructuras de paquetes específicos. Su interfaz gráfica de usuario es fácil de usar y su flexibilidad, el NIC de computadora portátil de usuario puede inyectar el tráfico directamente. Por lo tanto, no es necesario esperar a que un dispositivo disponible genere tráfico.

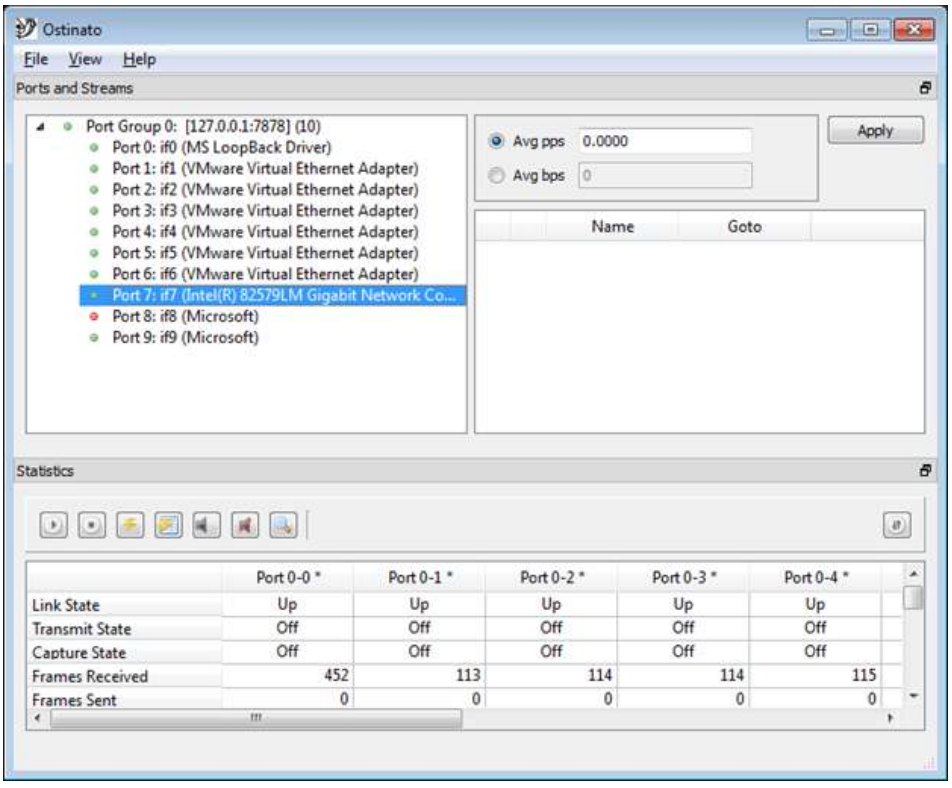

Figura 19-1 Interfaz de Ostinato

Fuente: (https://community.cisco.com/t5/networking-documents/easy-traffic-generator-works-with-gns3/ta-p/3160775)

1.8.4.1. Características

- Útil para pruebas de carga de red y pruebas funcionales.
- Uso a través de GUI o API de Python.
- Crea y configura múltiples flujos.
- Configurara velocidades de flujo de paquetes.
- Estadísticas y tasas de recepción / transmisión a nivel de interfaz para monitoreo y medición de red en tiempo real.
- Emulación de dispositivo de red, para múltiples Host IP para ayudar en la simulación del tráfico de la red.

CAPITULO II

2. DESARROLLO DE UNA PLATAFORMA MULTIVENDOR DE PROTOCOLOS ROUTING IGP Y EGP.

Para determinar la plataforma Multivendor que permita emular protocolos IGP y EGP analizaremos algunos aspectos fundamentales (Ver Figura 1-2).

2.1. Metodología para la Implementación de una Plataforma Multivendor

Figura 1-2. Diagrama de la Metodología

Realizado por: (Hidalgo Magaly. 2019)

En este capítulo se justifica la elección de las plataformas Networking, los protocolos de enrutamiento dentro de la topología y las pruebas de interoperabilidad. Para ello realizamos las siguientes pruebas entre equipos Homogéneos y Heterogéneos de la siguiente forma:

Utilizamos 3 topologías entre equipos Cisco-Cisco, Juniper-Juniper y Brocade-Brocade configurados con OSPF y 1 Escenario entre equipos Cisco, Juniper, Mikrotik y Brocade configurando OSPF y IS-IS con IPv4, donde determinarnos la interoperabilidad.

2.2. Selección de la Herramienta de Simulación

Para una mejor comprensión de las herramientas de simulación haremos una breve descripción de cada una de ellas.

2.2.1. VIRL

Es una potente plataforma de simulación de Cisco, posee máquinas virtuales que ejecutan los mismos sistemas operativos de red que los enrutadores y conmutadores físicos. Tiene un motor de configuración que puede construir una configuración completa de Cisco. (Cisco, 2018, https://learningnetworkstore.cisco.com/virlfaq/aboutVirl)

2.2.1.1. Características

- Posee Imágenes Oficiales de Cisco: posee un conjunto completo de imágenes legales y con licencia con nuevos sistemas operativos.
- Configuración Automática: Utiliza Autonetkit para crear configuraciones de arranque.
- Potente y Portátil: Sus redes virtuales son flexibles donde puede vincular dispositivos físicos.
- Acceso Libre: Presenta nuevas funciones y actualizaciones periódicamente para mejorar la experiencia de simulación.
- ASAV: Presenta máquinas virtuales ASAv, IOSvL2 facilitando el aprendizaje y conmutación.

2.2.2. EVE-NG

La plataforma EVE-NG Pro permite crear pruebas virtuales para entornos de capacitación dentro de empresas. Es el primer software de emulación Multivendor, donde sus opciones de administración

sea una mejor opción para ingenieros sin las políticas de seguridad corporativa ya que puede ejecutarse en un entorno totalmente aislado.

2.2.2.1. Características

- Posee enlaces activos, donde obtiene una respuesta inmediata de los puertos.
- Soporta 1024 nodos por laboratorio.
- Consola HTML para gestionar EVE.
- Posee configuraciones de importación y exportación desde la PC local.
- Captura de Wireshark integrada con multi configuraciones para un solo laboratorio.
- Temporizador de laboratorio para autoformación.
- Soporte para google Cloud EVE PRO.
- Plantilla personalizada para nodos propios.

2.2.3. GNS3

GNS3 es un emulador para topologías de red de gran tamaño y por sus aplicaciones lo utilizaremos para implementar nuestra plataforma Multivendor en base además de las siguientes características:

2.2.3.1. Características

La Emulación

GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales. Considerando que es una plataforma donde se puede incluir casos reales virtualizados, para conocer el funcionamiento de redes corporativas.

Simulación

GNS3 simula las características reales de un dispositivo como Routers de diferentes marcas, trabaja en la capa 2 pero nos permite conocer funcionamiento de equipos en capas más altas y poder interactuar con esos equipos.

2.2.3.2. Ventajas

- No hay limitación en la cantidad de dispositivos compatibles (la única limitación es su hardware: CPU y memoria)

- Admite todas las imágenes VIRL (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASAv)
- Soporta entornos de múltiples proveedores.
- Dispositivos descargables, pre-configurados y optimizados disponibles para simplificar la implementación
- Soporte nativo para Linux sin la necesidad de software de virtualización adicional
- Software de múltiples proveedores disponible gratuitamente.

2.2.3.3. Desventajas

- Las imágenes de Cisco deben ser suministradas por el usuario (descargue desde Cisco.com, o compre una licencia VIRL o copie desde un dispositivo físico).
- No es un paquete independiente, pero requiere una instalación local de software (GUI).
- GNS3 puede verse afectado por la configuración y las limitaciones de su PC debido a la instalación local (configuración de firewall y seguridad, políticas de la computadora portátil de la empresa, etc.)

Según la recomendación de la UIT-T iin P. 900, propone parámetros para asociar una escala de calificación según la percepción del usuario. En la mayoría de los casos se presentan escalas crecientes que van desde 0 hasta 5. La percepción promedio no debe superar el umbral de 3.5 que se considera una calidad aceptable. Para determinar valores en nuestra plataforma definiremos solo 3 valores que son:

0	Excelente
1	Buena
2	Muy buena

Para determinar la herramienta de simulación analizaremos las características de cada una de ellas, y según los distintivos de nuestra PC evaluaremos la mejor opción a escoger. Los dos factores más importantes que tomaremos en cuenta será la Memoria RAM y el tipo de Licencia de los simuladores. Observamos la Tabla 2-2.

Tabla 1-2: Herramientas de Simulación

SIMULADORES	VIRL	GNS3	EVE-NG
Escalabilidad	Alta	Alta	Alta
Procesador	4 Núcleos Lógicos	2 Núcleos Lógicos	4 Núcleos Lógicos
Memoria RAM	12GB	4GB	8GB
Almacenamiento	70 GB	1 GB	40 GB
Sistema Operativo	Unix/Linux y Windows	Windows , Linux	Windows, Mac OS X, Linux
Licencia	Pagada	Libre	Pagada
Versión	. VMware Fusion Pro v5.02	2.1.20	LTS 18.04.1!

Realizado por: HIDALGO, Magaly, 2019

En la Tabla 3-2 se asignará valores de 0, 1, 2; donde 0 representa deficiente para la implementación, 1 representa intermedio y 2 como excelente, estas variables son cualitativas con respecto a cada uno de los simuladores.

Tabla 2-2: Valorización de las Herramientas de Simulación

SIMULADORES	VIRL	GNS3	EVE-NG
Escalabilidad	1	2	2
Procesador	1	2	1
Memoria RAM	0	2	1
Almacenamiento	0	2	1
Sistema Operativo	2	2	2
Licencia	1	2	1
Versión	2	2	2

TOTAL	7	14	10

Realizado por: HIDALGO, Magaly, 2019

GNS3 en una herramienta fácil de utilizar para simular redes de gran tamaño es por eso que analizaremos las características que necesita nuestra PC para la Instalación. Además de que su licencia es libre, el Consumo de memoria RAM dependerá de los equipos que implementemos dentro de la topología, pero GNS3 según las características que más adelante conoceremos es la adecuada para nuestra Plataforma Networking.

Tabla 3-2: Requerimientos de GNS3

GNS3			
Características	**Requerimientos Mínimos**	**Requerimientos Recomendados**	**Requerimientos Óptimos**
Sistema Operativo	Windows 7,8,10 (64 bits)	Windows 7 y Linux (64 bits)	Linux (64 bits)
Procesador	2 o más núcleos	4 o más núcleos AMD/RV1 or Intel VT-X/EPT	I7 CPU
Virtualización	Requiere Extensiones	Requiere Extensiones	Requiere Extensiones
Memoria	4GB RAM	16 GB RAM	32 GB RAM
Espacio Disco	1GB	Disco de Estado Solido (SDD) 35 Gb	Disco de Estado Solido (SDD) 80 Gb

Fuente: (https://telectronika.com/articulos/que-es-gns3/)
Realizado por: HIDALGO, Magaly, 2019

Para simular la plataforma Networking nos basamos en los requerimientos Mínimos ya que nuestra PC es una Intel Core i5 de Séptima Generación con Tarjeta gráfica y Activada la Virtualización. Procedemos a la Instalación de GNS3 con el VMware.

Para la implementación de nuestra plataforma utilizamos el VM local GNS3 2.1.20 que ejecuta la máquina virtual, usando un software de virtualización como VMware o VirtualBox, esta instalación encontramos en al ANEXO B.

2.3. Protocolos de Enrutamiento

Para determinar los protocolos que se configuraran dentro de los AS, limitaremos sus características a las más importantes como la cantidad de Routers conectados, las métricas. Estas serán determinantes al momento de escoger el protocolo de enrutamiento. Observamos la Tabla 5-2.

Tabla 4-2: Características de los protocolos de Enrutamiento

GNS3				
PROTOCOLO	OSPF	IS-IS	EIGRP	RIP v2
Métricas	Ancho de Banda y Menor Costo	Menor Costo y Ancho de Banda	Ancho de Banda, Retardo, Confiabilidad.	Conteo de Saltos, Menor es Mejor.
Convergencia	Rápida	Muy Rápida	Muy Rápida	Lenta
Distancia Administrativa	110	115	90 Interno 170 Externo	120
Actualizaciones	Admite resumen de rutas y divide la red en áreas.	No, envía actualizaciones cuando se produce un cambio en la topología.	Envía una actualización solamente con la información a los Routers vecinos.	Actualizaciones cada 30 segundos por Multicast.
Sin Clase	Si	Si	Si	Si
Protocolo Tipo	Estado de Enlace	Estado de Enlace	Vector Distancia y Estado de Enlace.	Vector-Distancia
Cantidad de Router Máxima	50 Router por Área	1024	255	30
Función	Interior	Interior/Exterior	Interior	Interior
# Máximo de Saltos	Sin limite	200	224	15

Fuente: (http://www.redespracticas.com/?Njs=t&pag=txtEnrutamientoNociones.php)
Realizado por: HIDALGO, Magaly, 2019

Se asigna valores de 0, 1, 2 donde 0 es deficiente o antiguo, 1 es probable de implementar y 2 es excelente. En la Tabla 6-2 mostramos los resultados obtenidos según las comparaciones de las características de cada una de los protocolos de enrutamiento.

Tabla 5-2: Valorización a las Características de los protocolos de Enrutamiento

GNS3				
PROTOCOLO	OSPF	IS-IS	EIGRP	RIP v2
Métricas	2	2	1	1
Convergencia	2	2	2	1
Distancia Administrativa	2	2	1	2
Actualizaciones	2	2	1	1
Sin Clase	2	2	2	2
Protocolo Tipo	2	2	2	1
Cantidad de Router Máxima	2	2	1	1
Función	1	2	1	1
# Máximo de Saltos	2	2	2	1
TOTAL	17	18	13	11

Realizado por: HIDALGO, Magaly, 2019

Para la creación de nuestra topología escogimos dos protocolos de enrutamiento IS-IS y OSPF por las siguientes ventajas.

- IS-IS tiene una convergencia más rápida y admite aproximadamente 500 dispositivos conectados dentro de su área según la empresa a la que pertenecen.
- OSPF admite entre unos 100 dispositivos.
- OSPF puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.
- OSPF divide un Sistema Autónomo en áreas y las mantiene separadas para disminuir el tráfico de direccionamiento.
- IS-IS en un protocolo estándar ISO que admite protocolos como CLNS, IP e IPX mientras que OSPF admite IP.

- IS-IS utiliza paquetes de protocolo más pequeños para transportar información de enrutamiento.
- IS-IS soporta gran número de Routers conectados dentro de una topología de red, al igual que OSFPF no tiene límite con un máximo de 50 por área. Debido a estas características esenciales dentro de nuestra plataforma escogimos estos dos protocolos para realizar nuestra simulación.

Por estas características que son similares escogimos utilizar estos dos protocolos dentro de nuestra plataforma, sus características y su fácil codificación nos permiten manipular mejor los equipos.

2.4. Plataformas Networking

Al momento de utilizar GNS3 como simulador se nos limitan las Plataformas Networking, por ello se estableció las 4 Plataformas como se muestra en la Tabla 7-2 debido a la compatibilidad con las herramientas de emulación. En la página oficial de GNS3 (**https://gns3.com)** se muestra las versiones actualizadas de cada una de las herramientas.

Tabla 6-2 Plataformas Networking

CARACTERISTICAS	JUNIPER	CISCO	MIKROTIK	BROCADE
RAM	512 MB	256 MB	128 MB	512 MB
Nombre y Versión	Juniper_vMX-1	IOU1	MikroTik-1	Brocade-1
Tipo de Consola	Telnet	Telnet	Telnet	Telnet
CPUs	2	1	1	1
Tipo	Paravirtualized Network I/O (virtio-net-pci)	Intel Gigabit Ethernet (e1000)	Paravirtualized Network I/O (virtio-net-pci)	Intel Gigabit Ethernet (e1000)
Puertos	8	4	5	8
Rendimiento	3G/4G LTE	2Gbps	2.5 a 5.8 Gb	10 Gb

Sistema Operativo	Junos	Cisco IOS XE	Kernel Linux v2.6	Red abierta x86

Realizado por: HIDALGO, Magaly, 2019

Las características tomadas en cuenta son variables cualitativas y cuantitativas que me permiten conocer algunos parámetros como el manejo e instalación de estas Plataformas.

2.5. Parámetros de Rendimiento

Los parámetros de rendimiento que utilizaremos dentro de la Plataforma de Networking será la Tasa de Transferencia, la Latencia y la pérdida de paquetes, estos nos proporcionaran información más detallada acerca de cómo trabaja la red. Además, estos parámetros serán utilizados para recabar información acerca de los protocolos utilizados.

2.5.1. Tasa de Transferencia

La tasa de transferencia dentro de nuestra plataforma nos ayudara a medir el rendimiento de la red y cuan interoperable es esta. Para ello se realizó 3 pruebas inyectando tráfico con 200 bytes, 800 bytes y 1500 bytes. Según la Tabla 7-2 nos muestra una valorización de la tasa de trasferencia. Esta valorización la mediremos según la ITU-T G.993.2 VDSL2 en rápida; es decir, la tasa de transfería es baja, normal y lenta cuando se demore la red en descargar o subir datos a la red.

Tabla 7-2: Valoración de la Tasa de Transferencia

Tasa de Transferencia	
0.5 Mbps a 1.1 o 2.2 Mbps	Rápida
2.2 a 9 Mbps	Normal
9 a 10 Mbps	Lenta

Realizado por: HIDALGO, Magaly, 2019

2.5.2. Latencia

La latencia es el tiempo que tarda un paquete de datos en viajar de un nodo a otro. Para determinar este parámetro dentro de nuestra topología realizaremos pruebas enviando 200 bytes, 800 bytes y 1500 bytes dentro de la red propuesta.

En la Tabla 8-2 se muestra una valorización que utilizaremos para conocer la latencia de la Plataforma Networking y como la calificaremos. Para nuestro análisis la utilización deberá ser mínima según la Norma UIT-T G.114, es decir entre 4.4 ms y 78.2, por cada uno de los protocolos.

Tabla 8-2: Valoración de la Latencia

Latencia	
< 15 ms	Excelente
16 a 50 ms	Buena
50 a 78.2 ms	Mala

Realizado por: HIDALGO, Magaly, 2019

2.5.3. Perdida de Paquetes

Es la diferencia de paquetes entre los transmitidos y los recibidos, este puede ser medido de forma unidireccional según sean los equipos; además, de otros factores como físicos o el congestionamiento de la red que hacen que algún paquete se pierda.

Según la observación de nuestra plataforma determinaremos una valoración en los paquetes perdidos dentro de la red como se observa en la Tabla 9-2 donde obtenemos el porcentaje en perdida de paquetes desde el origen hasta llegar a su destino, cabe aclarar que según la T-REC-Y.1541-200602 nos expresa hasta un máximo del 10% en perdida de paquetes es aceptable.

Tabla 9-2: Pérdida de Paquetes dentro de una red.

Paquetes en la Red	
Paquetes Perdidos en Datos	**Valoración**
0% al 0.9%	Excelente

1% al 1.9%	Bueno
2% al 3.9%	Mala
4% al 10%	Muy Mala

Realizado por: HIDALGO, Magaly, 2019

Además de los parámetros expuestos anteriormente y sus valorizaciones podemos obtener un análisis de la pérdida de paquetes mediante la siguiente formula:

$$Perdidas = \frac{\#\ Paquetes\ Ingresados}{\#\ Paquetes\ Transmitidos}$$

2.6. Topología de Red.

Para la implementación de la Plataforma Networking utilizamos 20 Routers; donde, 8 son equipos Cisco, 5 Juniper, 2 Brocade, y 5 Mikrotik. Además de un Servidor, 2 Host que simularan a los usuarios y 2 Ostinato que inyectaran tráfico a la red; creamos 3 Sistemas Autónomos configurados internamente con OSPF y IS-IS. (Ver Figura 2-2)

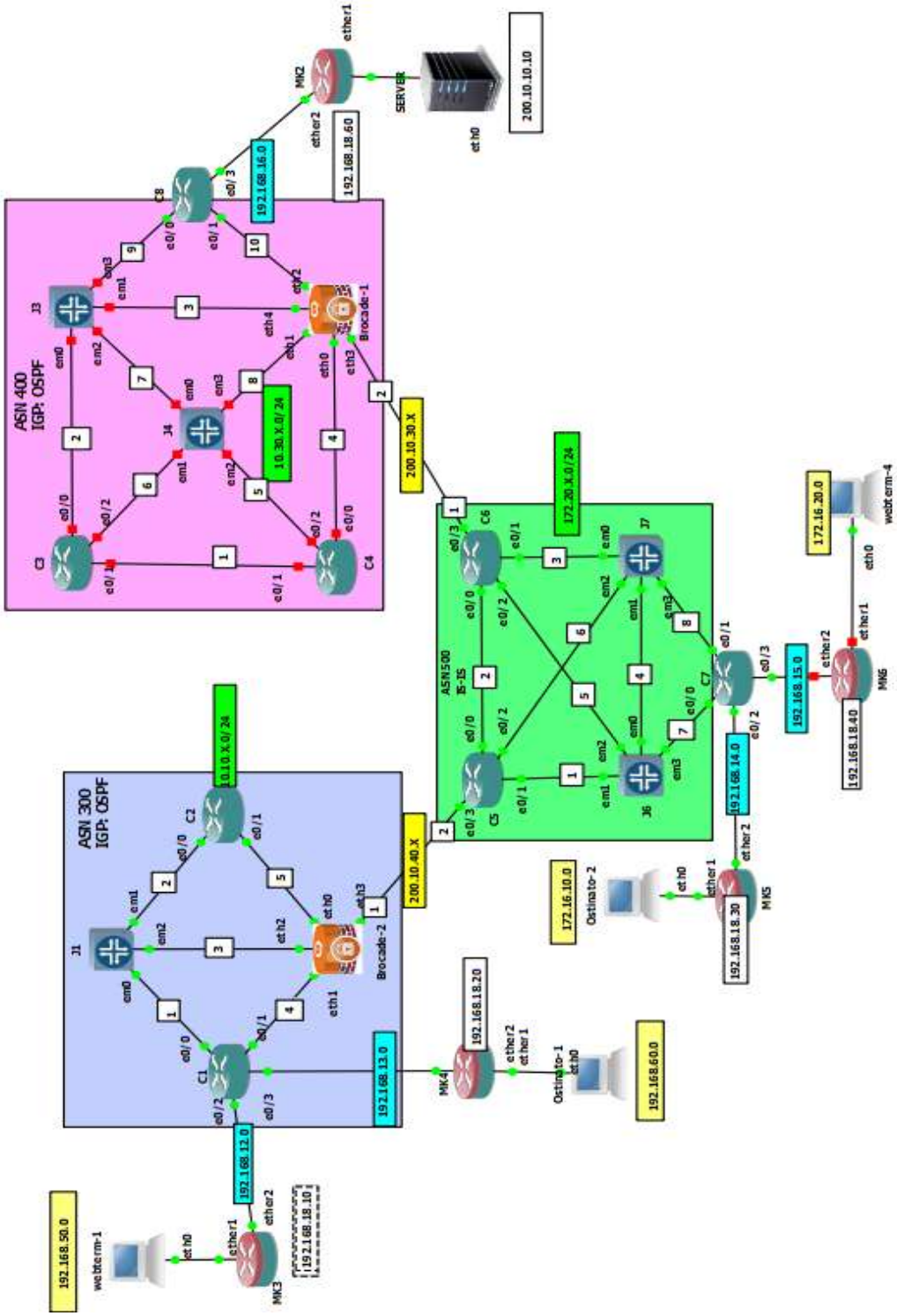

Figura 2-2. Plataforma Multivendor

Realizado por: (Hidalgo Magaly. 2019)

2.6.1. Sistema Autónomo de la Plataforma Multivendor

El Sistema Autónomo en nuestra plataforma nos permite dividir distintos escenarios reales implementados virtualmente con distintas administraciones, con las características de grandes redes. Utilizamos un Router fronterizo cuya función será de intercambiar tráfico y sirva de medio de comunicación entre diferentes protocolos en diferentes sistemas Autónomos.

2.7. Plan de Direccionamiento

Tabla 10-2 Plan de Direccionamiento

ADMINISTRADOR	INTERFAZ	DIRECCION IP	MASCARA DE RED	GATEWAY	ID
C1	e 0/0	10.10.1.1	255.255.255.0		1.1.1.1
	e 0/1	10.10.4.1	255.255.255.0		
	e 0/2	192.168.12.1	255.255.255.0		
	e 0/3	192.168.13.1	255.255.255.0		
J1	em0	10.10.1.2	255.255.255.0		3.3.3.3
	em1	10.10.2.1	255.255.255.0		
	em2	10.10.3.1	255.255.255.0		
C2	e 0/0	10.10.2.2	255.255.255.0		2.2.2.2
	e 0/1	10.10.5.1	255.255.255.0		
	e 0/2	200.10.20.1	255.255.255.0		
Brocade-2	eth0	10.10.5.2	255.255.255.0		4.4.4.4
	eth1	10.10.4.2	255.255.255.0		
	eth2	10.10.3.2	255.255.255.0		
	eth3	200.10.40.1	255.255.255.0		
C3	e 0/0	10.30.2.1	255.255.255.0		5.5.5.5
	e 0/1	10.30.1.1	255.255.255.0		
	e 0/2	10.30.6.1	255.255.255.0		
C4	e 0/0	10.30.4.1	255.255.255.0		6.6.6.6
	e 0/1	10.30.1.2	255.255.255.0		
	e 0/2	10.30.5.1	255.255.255.0		
J3	em0	10.30.2.2	255.255.255.0		7.7.7.7

	em1	10.30.3.1	255.255.255.0		
	em2	10.30.7.1	255.255.255.0		
	em3	10.30.9.1	255.255.255.0		
Brocade-1	eth0	10.30.3.2	255.255.255.0		8.8.8.8
	eth1	10.30.4.2	255.255.255.0		
	eth2	10.30.8.1	255.255.255.0		
	eth3	10.30.10.1	255.255.255.0		
	eth4	200.10.30.2	255.255.255.0		
J4	em0	10.30.7.2	255.255.255.0		9.9.9.9
	em1	10.30.6.2	255.255.255.0		
	em2	10.30.5.2	255.255.255.0		
	em3	10.30.8.2	255.255.255.0		
C5	e 0/0	172.20.2.1	255.255.255.0		192.168.0.1
	e 0/1	172.20.1.1	255.255.255.0		
	e 0/2	172.20.6.1	255.255.255.0		
	e 0/3	200.10.10.2	255.255.255.0		
C6	e 0/0	172.20.2.2	255.255.255.0		192.168.0.4
	e 0/1	172.20.3.1	255.255.255.0		
	e 0/2	172.20.5.1	255.255.255.0		
	e 0/3	200.10.30.1	255.255.255.0		
J6	em0	172.20.4.1	255.255.255.0		192.168.0.2
	em1	172.20.1.2	255.255.255.0		
	em2	172.20.5.2	255.255.255.0		
	em3	172.20.7.1	255.255.255.0		
J7	em0	172.20.3.2	255.255.255.0		192.168.0.3
	em1	172.20.4.2	255.255.255.0		
	em2	172.20.6.2	255.255.255.0		
	em3	172.20.8.1	255.255.255.0		
C7	e 0/0	172.20.7.2	255.255.255.0		192.168.0.5
	e 0/1	172.20.8.2	255.255.255.0		
	e 0/2	192.168.14.1	255.255.255.0		
	e 0/3	192.168.15.1	255.255.255.0		
C8	e 0/0	10.30.9.2	255.255.255.0		10.10.10.10
	e 0/1	10.30.10.2	255.255.255.0		
	e 0/2	192.168.17.1	255.255.255.0		
	e 0/3	192.168.16.1	255.255.255.0		

MK2	ether1	200.10.10.0	255.255.255.0		
	ether2	192.168.16.2	255.255.255.0		
MK3	ether1	192.168.50.1	255.255.255.0		
	ether2	192.168.12.2	255.255.255.0		
MK4	ether1	192.168.60.1	255.255.255.0		
	ether2	192.168.13.2	255.255.255.0		
MK5	ether1	172.16.10.1	255.255.255.0		
	ether2	192.168.14.2	255.255.255.0		
MK6	ether1	172.16.20.1	255.255.255.0		
	ether2	192.168.15.2	255.255.255.0		
WEBTERM1	eth0	192.168.50.10	255.255.255.0	192.168.50.1	
Ostinato 1	eth0	192.168.60.10	255.255.255.0	192.168.60.1	
Ostinato 2	eth0	172.16.10.10	255.255.255.0	172.16.10.1	
WEBTERM4	eth0	172.16.20.10	255.255.255.0	172.16.20.1	
SERVER	eth0	200.10.10.10	255.255.255.0	200.10.10.1	

Realizado por: (Hidalgo Magaly. 2019)

2.8. Pruebas de Interoperabilidad en equipos Homogéneos

Para medir el grado de interoperabilidad en nuestra Plataforma Networking lo realizaremos mediante 6 pruebas que serán entre equipos homogéneos y entre equipos heterogéneos, como se puede observar en la Tabla 11-2.

Tabla 11-2 Pruebas entre equipos Homogéneos

Equipos Homogéneos	
Prueba 1	Cisco-Cisco
Prueba 2	Brocade - Brocade
Prueba 3	Juniper - Juniper

Realizado por: (Hidalgo Magaly. 2019)

Estas pruebas se dividirán en dos segmentos, el primero es la convergencia de la red, este será analizado con la tabla de rutas y los tipos de mensajes que se envían dentro de la topología. En el segundo segmento se toma en cuenta algunos parámetros de rendimiento como la latencia, perdida

de paquetes, tasa de transferencia y estos nos indicaran que tan interoperables son los equipos de la misma marca.

2.8.1. Prueba 1: Cisco

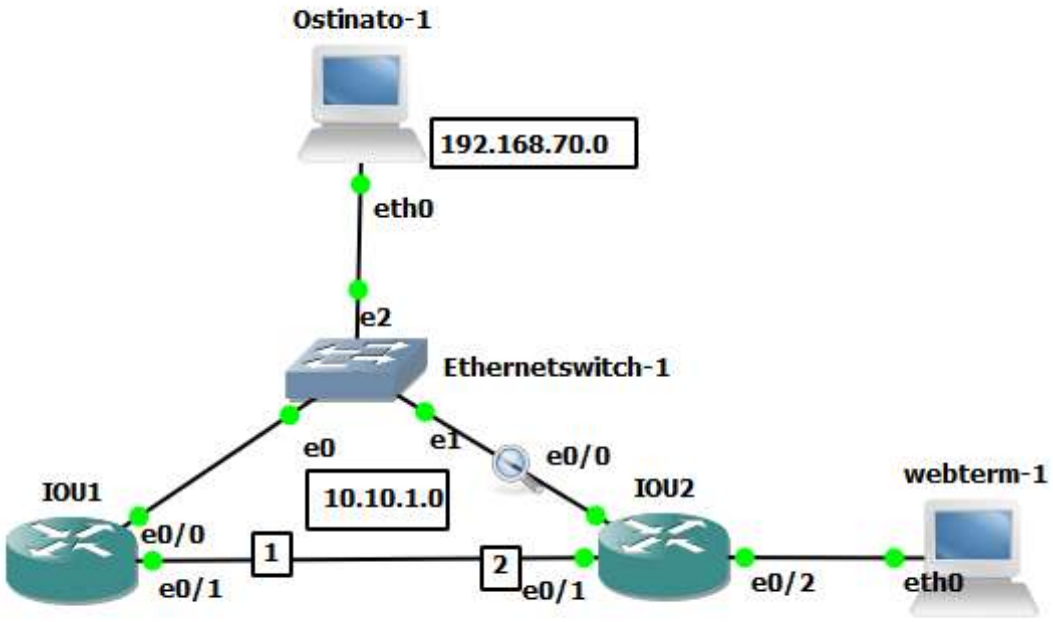

Figura 3-2. Interoperabilidad Cisco

Realizado por: (Hidalgo Magaly. 2019)

Para determinar la interoperabilidad entre equipos Cisco-Cisco inyectaremos trafico TCP por medio de Ostinato. (Ver Figura 3-2)

Para determinar la interoperabilidad entre equipos Cisco tomamos en cuenta los siguientes parámetros.

- Latencia
- Tasa de Transferencia
- Perdida de paquetes
- Convergencia (Tabla de Rutas y mensajes)

Mediante el Generador de Trafico Ostinato inyectamos paquetes TCP con una cantidad de 200 Bytes, 800 Bytes y 1500 Bytes, configurando el Protocolo OSPF a todas las plataformas de enrutamiento, conoceremos el funcionamiento de equipos homogéneos y el grado de interoperabilidad entre estos.

2.8.2. Prueba 2: Brocade

En la Figura 4-2 se puede observar la topología que utilizaremos para comprobar la interoperabilidad entre equipos Brocade-Brocade.

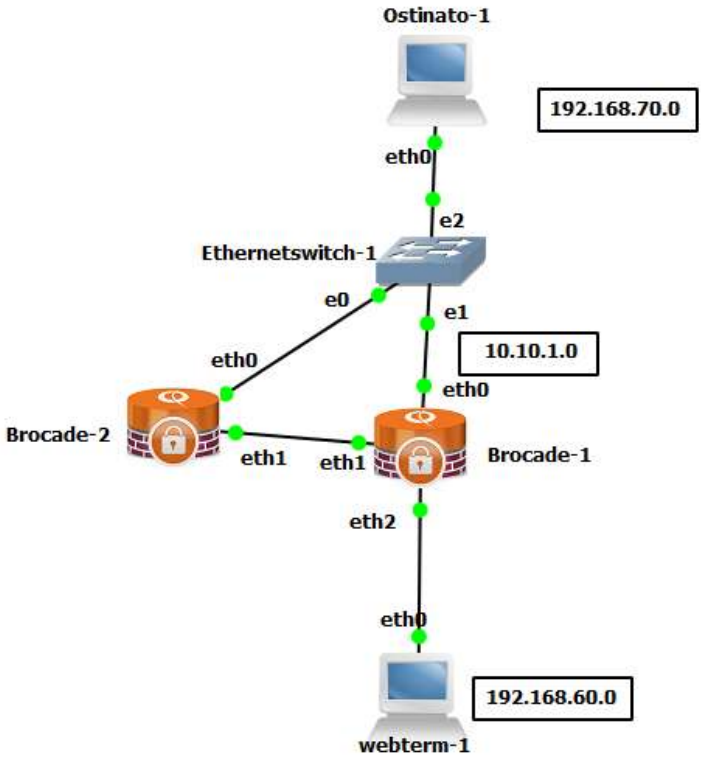

Figura 4-2. Interoperabilidad Brocade

Realizado por: (Hidalgo Magaly. 2019)

Para la configuración de equipos Brocade utilizamos el protocolo OSPF, que generalmente es utilizado casi en todas las empresas como un protocolo piloto; además en el escenario se inyecto tráfico, mediante Ostinato enviamos 200 Bytes, 800 Bytes y 1500 Bytes a la red. En el Capítulo 3 analizaremos los parámetros de rendimiento que existió en los Equipos de Enrutamiento Brocade.

2.8.3. Prueba3: Juniper

Topología de la red en equipos Juniper-Juniper. Ver Figura 5-2.

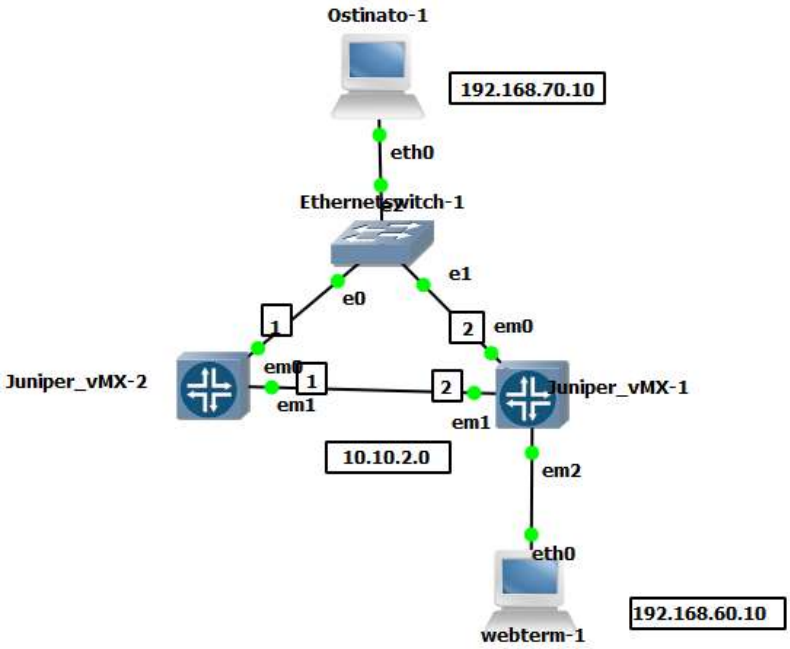

Figura 5-2. Interoperabilidad Juniper.

Realizado por: (Hidalgo Magaly. 2019)

Los Equipos Juniper en nuestro país son muy pocos utilizados, no se conoce una cifra exacta de la cantidad que exista en la actualidad, pero aun así haremos un análisis de su grado de interoperabilidad, generamos tráfico por medio de Ostinato enviamos 200 Bytes, 800 Bytes y 1500 Bytes. Se creará un análisis de los parámetros de rendimiento y la convergencia de la red a través de la tabla de rutas y los mensajes que transporta la red.

2.9. Pruebas de Interoperabilidad en Equipos Heterogéneos

Para determinar el grado de interoperabilidad entre equipos de distintas marcas realizaremos 3 pruebas, cada una de ellas es de un AS diferente (Ver Tabla 12-2). Se dividirán en dos segmentos:

- El primero será verificar la convergencia de la red, esto lo realizaremos con las tablas de rutas y los tipos de mensajes que se envían dentro de la topología.

- El segundo será analizando algunos parámetros de rendimiento como la perdida de paquetes, la tasa de transferencia y la latencia.

Tabla 12-2 Pruebas entre equipos Heterogéneos

Equipos Heterogéneos	
Prueba 4	(Cisco – Brocade – Juniper – Mikrotik) AS 300
Prueba 5	(Cisco – Brocade – Juniper – Mikrotik) AS 500
Prueba 6	(Cisco – Brocade – Juniper – Mikrotik) AS 400

Realizado por: (Hidalgo Magaly. 2019)

A continuación, presentaremos los escenarios con las pruebas que se realizaran en los diferentes AS.

2.9.1. Prueba 4: AS 300

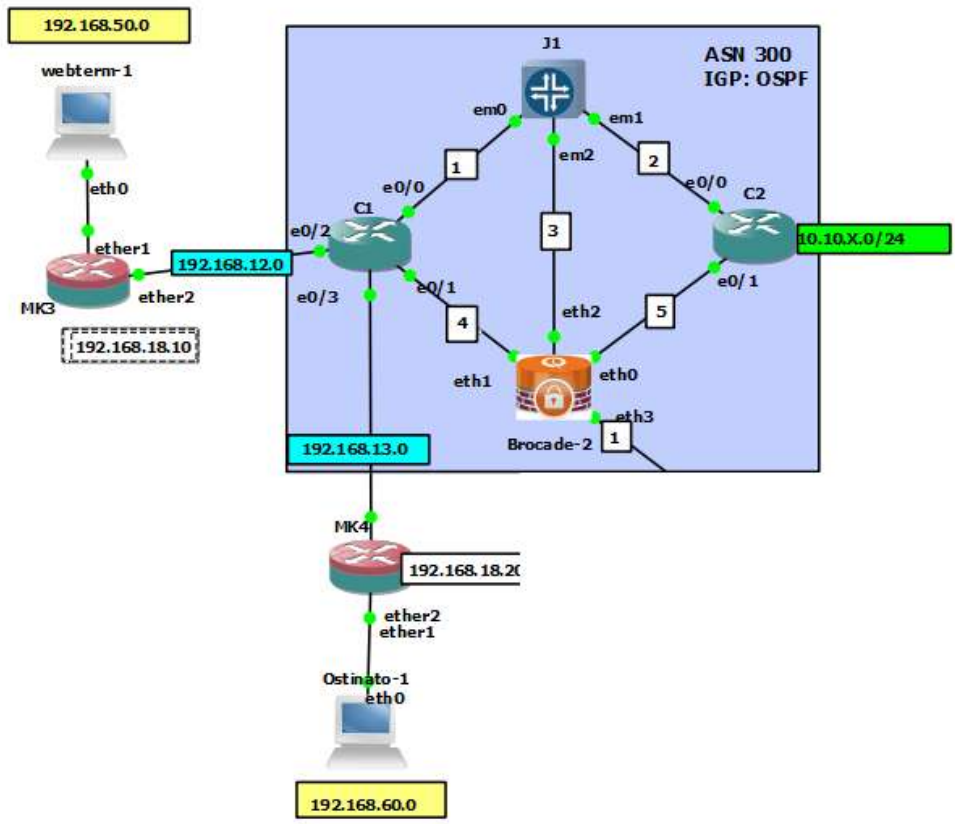

Figura 6-2. AS 300

Realizado por: (Hidalgo Magaly. 2019)

En este escenario realizaremos pruebas de Interoperabilidad, utilizando equipos de enrutamiento de distintas marcas (Juniper, Cisco, Mikrotik y Brocade). Mediante Ostinato se simulará el funcionamiento de una red corporativa y se podrá determinar 2 parámetros como Latencia y Perdida de paquetes. Además de la convergencia a través de las Tablas de enrutamiento y los mensajes Hello.

Para la Figura 6-2 observamos el escenario con un AS 300 donde se configuro el protocolo OSPF v2 en IPv4, utilizaremos BGP y dentro de la red IBGP en el equipo Cisco que será nuestro intermediario. Una vez comprobada su conectividad, inyectamos tráfico y enviamos 200 bytes, 800 bytes y 1500 bytes en paquetes TCP en un tiempo aproximado de 00:30:11.

2.9.2. Prueba 5: AS 500

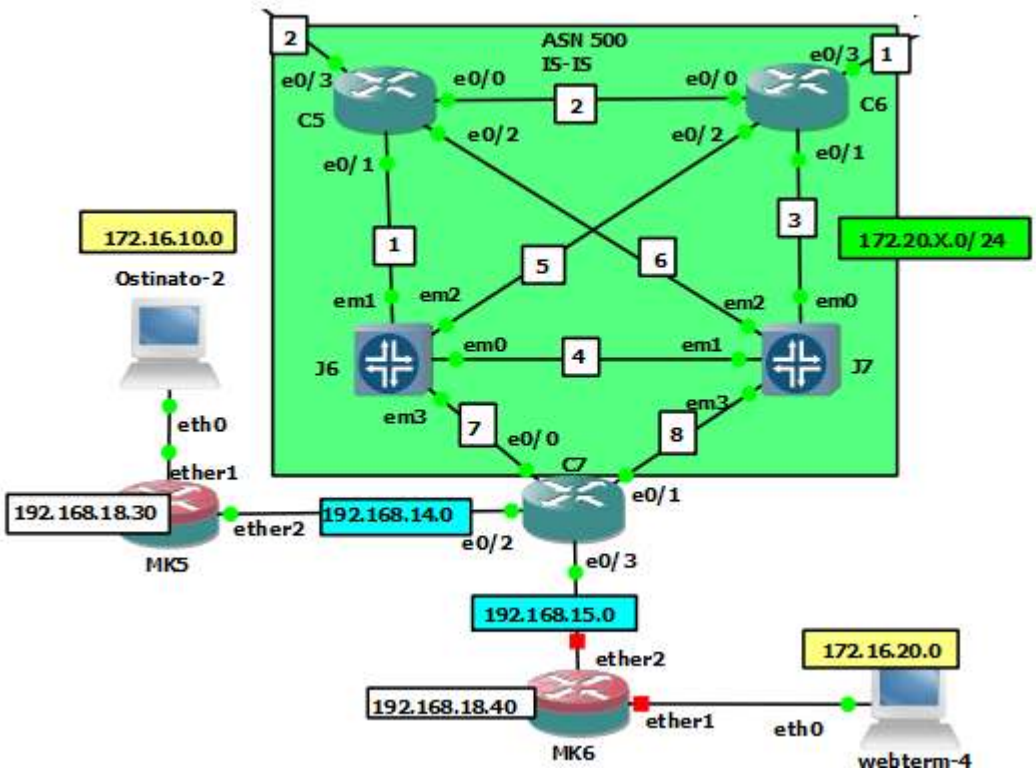

Figura 7-2. AS 500

Realizado por: (Hidalgo Magaly. 2019)

Para el AS 500 utilizamos el protocolo IS-IS generalmente utilizado dentro de las grandes redes por su alto grado de Escalabilidad ver Figura 7-2. Para esta topología creamos equipos de enrutamiento

como Cisco, Juniper, Mikrotik configurados en IPv4 y un generador de tráfico que inyectaba paquetes TCP dentro de la red, en este caso tenemos 2 Routers fronterizos como el Cisco 5 y el Cisco 6 en los que se configuro BGP y en el equipo Juniper 6, Juniper 7 y Cisco 7 IBGP para que este actualice la tabla de enrutamiento y pueda transitar los paquetes sin ningún problema.

El tiempo de muestreo fue de 00:41:19, en este lapso transitaron una cantidad de 3765 paquetes dentro de IS-IS, cabe aclarar que no solo transitaran paquetes TCP por Ostinato sino BGP e IS-IS que son propios de la topología.

2.9.3. Prueba 6: AS 400

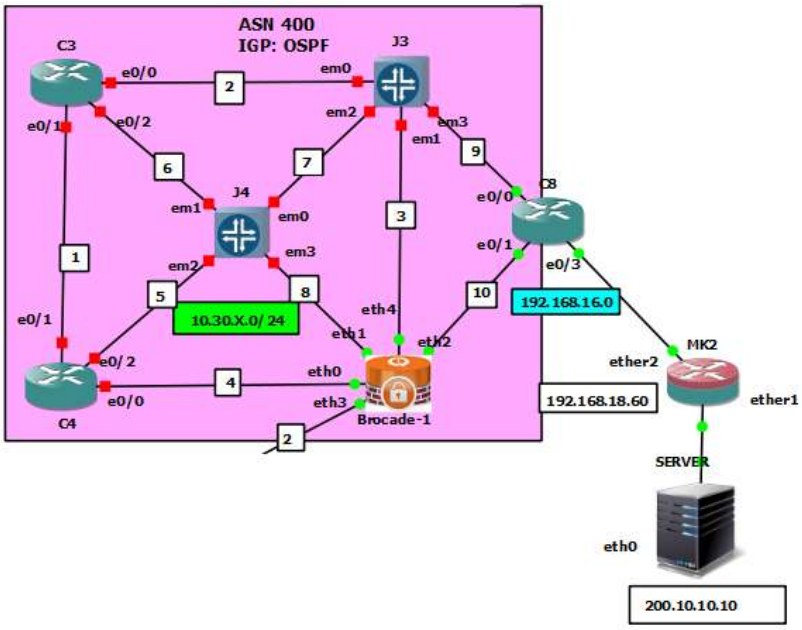

Figura 8-2. AS 400

Realizado por: (Hidalgo Magaly. 2019)

Para nuestra última topología que es el AS 400 ver Figura 8-2, utilizamos equipos de enrutamiento como Cisco, Brocade, Mikrotik y Juniper. El servidor está en la topología y nos permitirá el acceso a internet dentro de la red, una cosa muy importante es que en este escenario no tenemos un generador de tráfico como Ostinato; que inyecto paquetes TCP en 200 bytes, 800 bytes y 1500 bytes.

La red Transmite paquetes TCP, BGP, IS-IS y OSPF, aquí realizaremos un análisis de los paquetes perdidos y la latencia que ocupa este escenario.

2.10. Pruebas de Rendimiento

2.10.1. Prueba 7: Generador de Trafico Plataforma Multivendor

Ostinato es un generador de Tráfico que permite inyectar paquetes TCP de forma que simule redes corporativas. Para ellos se debe configurar la cantidad de paquetes y el destino como se muestra en la Figura 9-2:

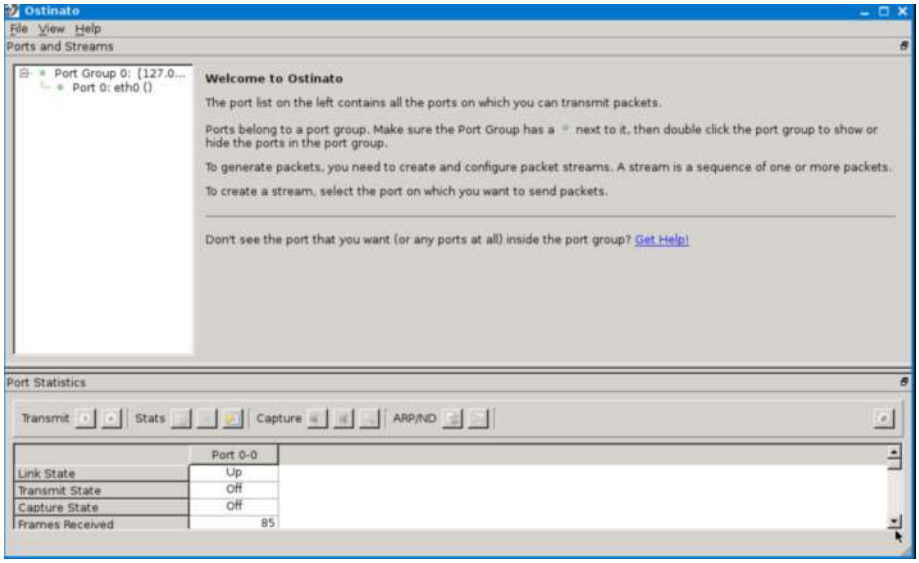

Figura 9-2. Interfaz de Ostinato

Realizado por: (Hidalgo Magaly. 2019)

Cuando encendemos Ostinato nos pregunta el puerto que vamos a configurar y por el cual enviamos tráfico a la red, en nuestro escenario escogemos el puerto Cero enlazado a la eth0 y al lado derecho escogemos New Stream como se ve en la Figura 10-2:

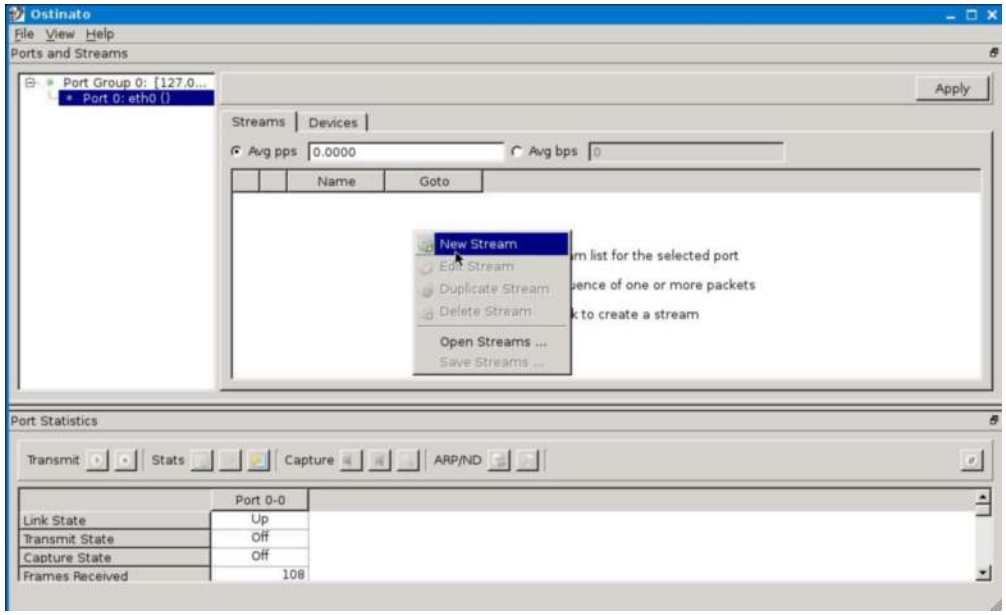

Figura 10-2. New Stream Ostinato

Realizado por: (Hidalgo Magaly. 2019)

Ahora proporcionamos los datos que requiere Ostinato como la selección del protocolo (IPv4), los datos del protocolo es decir el destino y el origen. Ver figura 11-2. En la pestaña Stream control controlamos la cantidad de paquetes y el tiempo, esto puede ser opcional si no tenemos una medida exacta de los paquetes transportados.

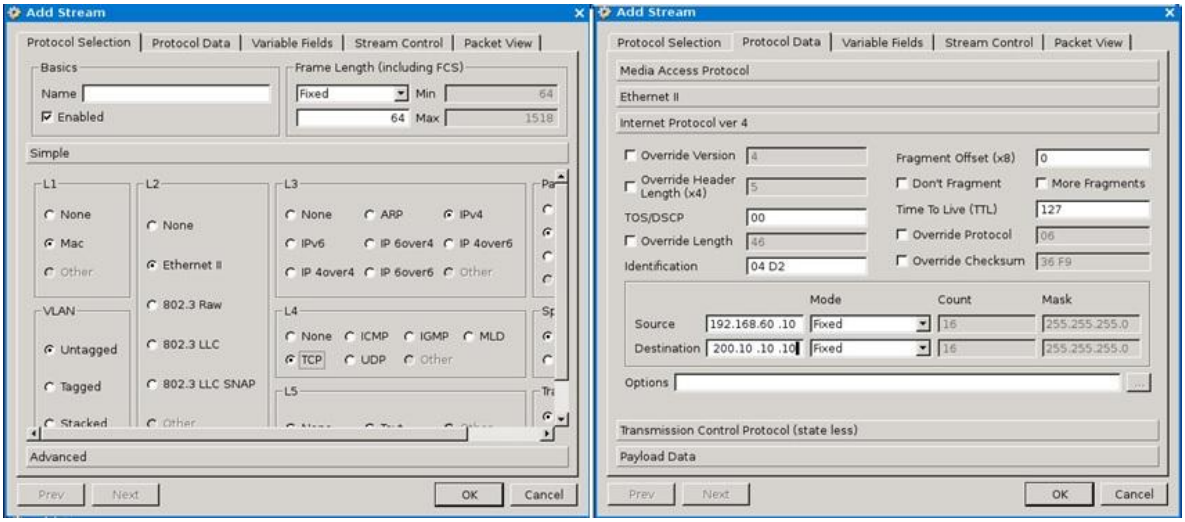

Figura 11-2. Configuración interna de Ostinato

Realizado por: (Hidalgo Magaly. 2019)

Una vez realizada las configuraciones en Ostinato 1 y Ostinato 2, estos generaran paquetes TCP en tramas de 200 bytes, 800 bytes y 1500 bytes, donde con la ayuda de Wireshark capturamos los paquetes transmitidos a través de la red en un tiempo aproximado de 00:30:00 para todas los AS.

CAPITULO III

3. ANALISIS DE RESULTADOS

3.1. Resultados Equipos Homogéneos

Los equipos Homogéneos dentro de nuestra red son aquellos con la misma marca y características físicas, como memoria RAM. Analizaremos esencialmente 3 marcas de equipos CISCO, JUNIPER Y BROCADE, en el Capítulo 2 realizamos los escenarios y estos fueron los resultados que obtuvimos de cada uno de los equipos de enrutamiento.

3.1.1. Resultado1: Cisco

Emulamos una topología de red que me permita analizar el flujo de datos que se transporta a través de la red, donde se requiere conocer la convergencia y el rendimiento. Se analizó el tipo de mensajes que se envían dentro del protocolo, la tabla de rutas que es muy importante para determinar el grado de interoperabilidad, la tasa de transferencia, perdida de paquetes y la latencia de la red. Estas pruebas se realizaron entre equipos de las mismas marcas y equipos combinados.

A continuación, verificaremos los resultados obtenidos entre equipos Cisco-Cisco y el grado de Interoperabilidad que existe.

3.1.1.1. Convergencia

Para determinar el grado de Convergencia se tomará en cuenta dos factores importantes como es la Tabla de Rutas y los Mensajes que se envían dentro del protocolo configurado.

- Tabla de rutas

La tabla de rutas nos muestra los nodos conectados y sus direcciones, así se determina que existe interoperabilidad entre estos, ya que se observa en la Figura 1-3 las direcciones con /32 son las de Ipv4 que transportara los paquetes donde contienen la información propia de la red y la requerida por los usuarios.

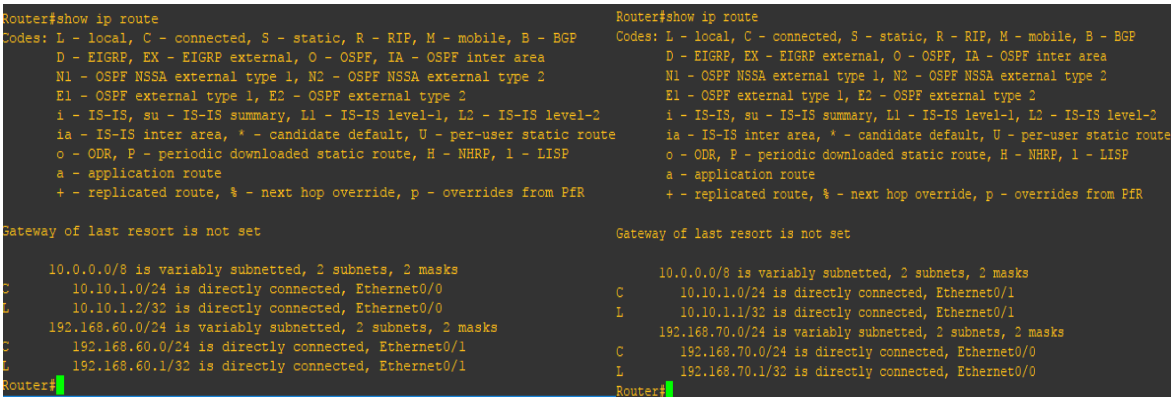

Figura 1-3. Display Routing Table Cisco

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes del Protocolo

Los mensajes que se intercambian dentro del protocolo nos ayuda a conocer que existe interoperabilidad , ya que estos son mensajes que envian peticiones en intervalos exactos, si un router no tiene el mismo intervalo estos no se comunicaran ni existira intercambio de informacion de forma keepalive, ademas debe coincidir el indicador de area entre los paquetes Hello. (Ver Figura 2-3)

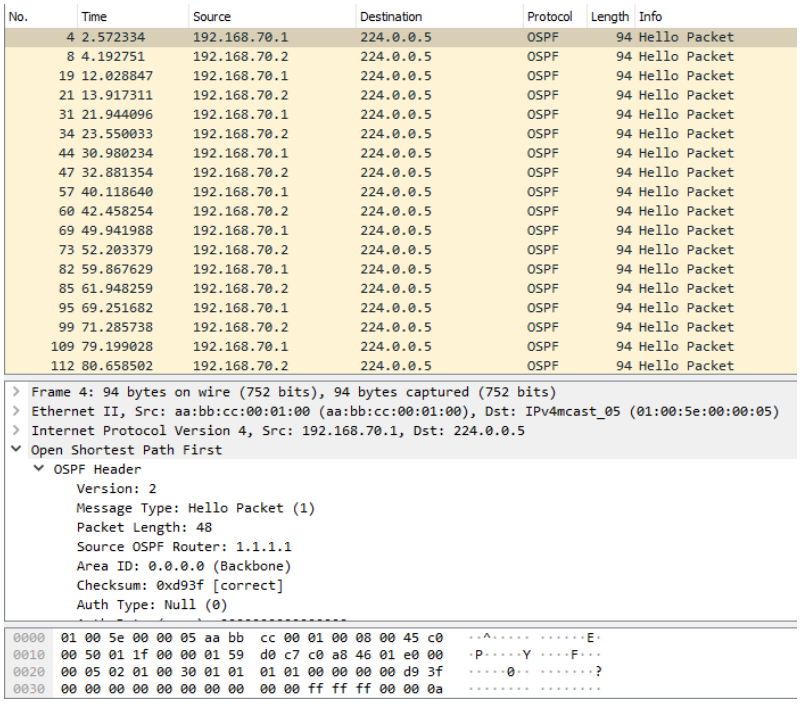

Figura 2-3. Mensajes Cisco

Realizado por: (Hidalgo Magaly. 2019)

3.1.1.2. 3.1.1.2. Rendimiento

Una forma más explícita de determinar el grado de interoperabilidad entre equipos Cisco – Cisco es analizando sus parámetros de rendimiento como se Observa en la Tabla 1-3 donde determinamos la latencia, tasa de transferencia y la perdida de paquetes en 200 bytes, 800 bytes y 1500 bytes.

Tabla 1-3 Resultados Interoperabilidad Cisco

Características	200 Bytes	800 Bytes	1500 Bytes
Tasa de Transferencia	327 bits/s	397.5 bits/s	402.36 bits/s
Perdida de paquetes	0.01%	0.01%	0.01%
Latencia	5.74 bits/s	4.87 bits/s	6.47 bits /s
Payload	0.897 bits/s	0.547 bits/s	0.674 bits/s
Tiempo de Muestreo	00:30:17	00:30:12	00:30:06

Realizado por: (Hidalgo Magaly. 2019)

3.1.2. Resultado 2: Juniper

Se realizo una prueba entre Equipos Networking de la misma marca, es este caso especifico Juniper-Juniper. Conoceremos el funcionamiento de una red convergente y el flujo de datos que atraviesa por la misma, se determino parametros como la tasa de transferencia, perdida de paquetes y la latencia.

3.1.2.1. Convergencia de la Red

Para analizar la Convergencia de la red se verifica por medio de la tabla de Rutas y los Mensajes que se envian dentro de la topologia.

- Tabla de Rutas

La tabla de rutas almacenara cualquier nodo que se encuentra conectado, por esta razon realizamos un run show route dentro de los equipos Juniper y determinamos que estos actualizan sus tablas y proporcionan informacion necesaria al router vecino para que este tenga acceso a las direcciones ip

que conoce el sistema. (Ver Figura 3-3). La Tabla de rutas intercambia informacion con los dispositivos que se encuentra concetados, es decir interoperan entre vecinos.

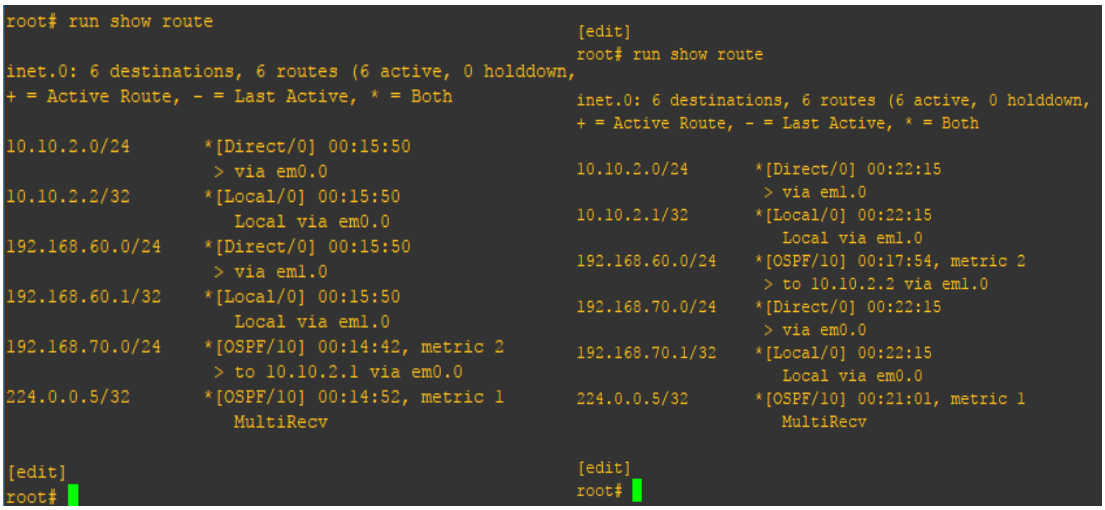

Figura 3-3. Display Routing Table Juniper

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes del Protocolo

El nucleo del sistema en la tabla de rutas envia mensajes constantemente para formar adyacencias, donde esta comparte informacion bidireccional entre ambos equipos. Gracias a estos mensajes entre se comprueba que existe interoperabilidad entre dos Routers y que estos intercambia paquetes de datos. (Ver Figura 4-3).

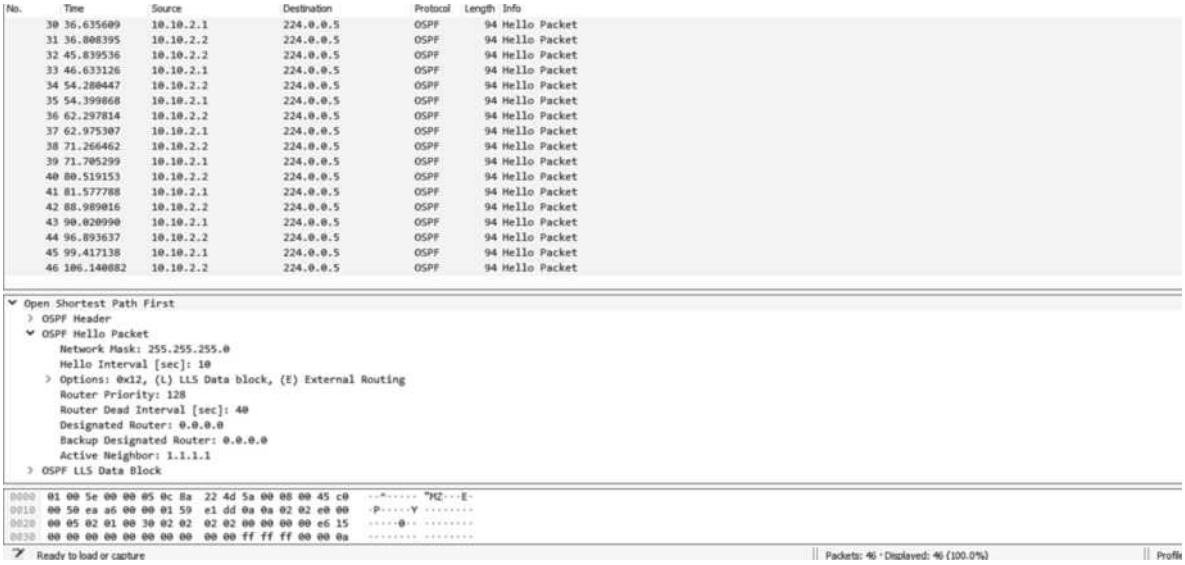

Figura 4-3. Mensajes Juniper

Realizado por: (Hidalgo Magaly. 2019)

3.1.2.2. Rendimiento

Entre los equipos Juniper que es una marca no muy reconocida, pero de alto rendimiento se realizó las pruebas para determinar su grado de interoperabilidad y obtuvimos el siguiente resultado que se observa en la Tabla 2-3.

Tabla 2-3 Resultados Interoperabilidad Juniper

Características	**200 Bytes**	**800 Bytes**	**1500 Bytes**
Tasa de Transferencia	320 Bits/s	175.47 Bits/s	200 bits /s
Perdida de paquetes	0.1%	0.1%	0.1%
Latencia	9.15 ms	8.4 ms	13.13 ms
Payload	1.1 bits/s	0.9 bits /s	1.025 bits/s
Tiempo de Muestreo	00:30:12	00:30:09	00:30:50

Realizado por: (Hidalgo Magaly. 2019)

3.1.3. Resultado 3: Brocade

Los equipos Brocade es uno de los líderes en el mercado para infraestructuras grandes, para medir su interoperabilidad realizamos una simulación enviando paquetes desde el generador Ostinato hacia la red.

Se analizará la convergencia de la red y su rendimiento para conocer el grado de interoperabilidad que existe entre equipos de las mismas Marcas.

3.1.3.1. Convergencia

En la convergencia de la red se quiere analizar la tabla de rutas de Brocade y los tipos de mensajes que se envían dentro de la topología.

- Tabla de Rutas

En la Figura 5-3 se observa la tabla de rutas de los dispositivos que están conectados, son interoperables porque comparten información de direcciones.

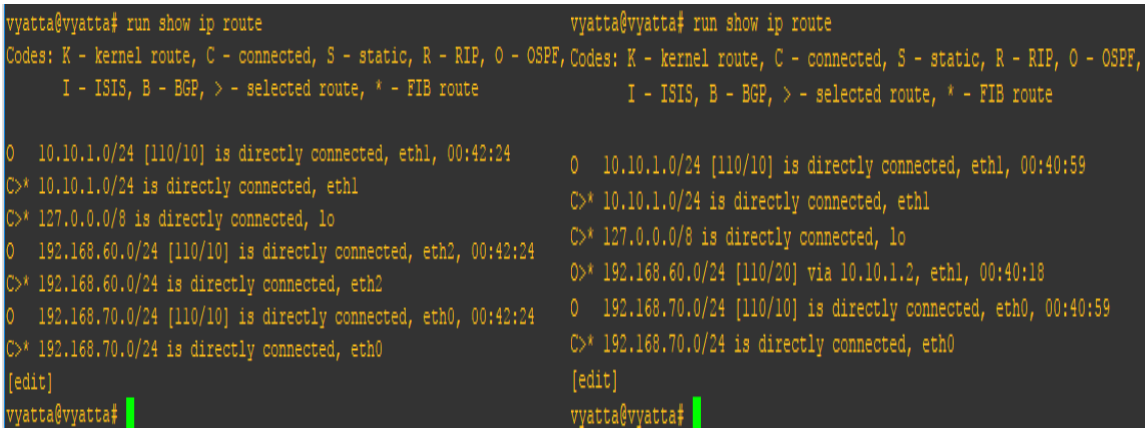

Figura 5-3. Display Routing Table Brocade

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes del Protocolo

Una vez que se comprueba que intercambia mensajes dentro del protocolo se da una adyacencia es decir compartes base de datos con información del paquete. Todo este proceso se da cuando existe interoperabilidad entre los Routers y sus vecinos (Ver Figura 6-3), mensajes que intercambian toda la información que se requiera.

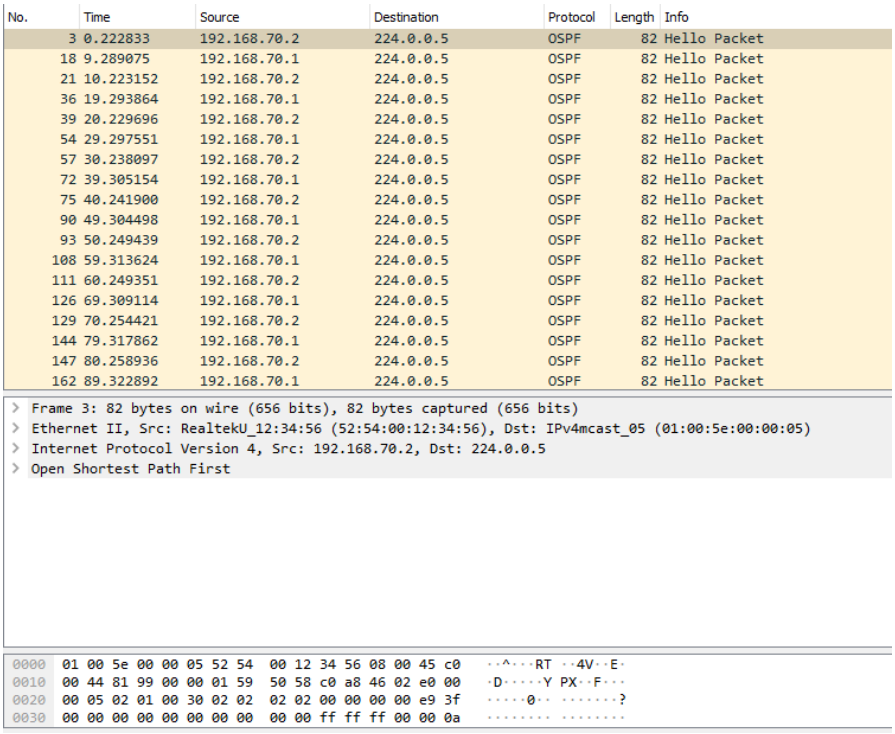

Figura 6-3. Mensajes Brocade

Realizado por: (Hidalgo Magaly. 2019)

3.1.3.2. Rendimiento

Una forma más detallada de analizar el rendimiento de la red es conocer ciertos parámetros como la latencia, la tasa de transferencia y la perdida de paquetes que nos ayudar a conocer cuan interoperables son los equipos de la misma marca como en este caso es Brocade-Brocade. Observamos la Tabla 3-3.

Tabla 3-3 Resultados Interoperabilidad Brocade

Características	**200 Bytes**	**800 Bytes**	**1500 Bytes**
Tasa de Transferencia	182.93 bits/s	259.87 bits/s	355.20 bits/s
Perdida de paquetes	0.01%	0.01%	0.01%
Latencia	5.14 ms	5.49 ms	5.014 ms
Payload	0.747 bits/s	0.91bits/s	0.845 bits/s
Tiempo de Muestreo	00:31:00	00:30:14	00:30:31

Realizado por: (Hidalgo Magaly. 2019)

3.1.4. Resultado Final Equipos Homogéneos

Se determina que los equipos homogéneos alcanzan una latencia mínima, sea Cisco Juniper o Brocade. Además, la pérdida de paquetes tiende a cero y la tasa de transferencia oscila entre 180 y 400 bits/s.

3.2. Resultado Equipos Heterogéneos

3.2.1. Resultado 4: AS 300

En este Sistema Autónomo 300 recopilaremos las deducciones de las pruebas de tráfico generadas por Ostinato anteriormente y obtendremos los resultados necesarios para comprender el funcionamiento de la red. Se divide en dos segmentos: La convergencia y el Rendimiento.

3.2.1.1. Convergencia AS 300

Para determinar la convergencia en la Tabla de rutas se realizó un Show ip route Ver Figura 14-3, donde nos muestra toda la información acerca de los equipos conectados dentro de la red. Además del tiempo que tardo el compartir la información y la actualización, también dependerá del protocolo que se utilizó, en este caso se observará el tiempo de convergencia con el protocolo OSPF.

- Tabla de Rutas

En el Sistema Autónomo 300 tenemos dos Routers de gran importancia que es el Cisco 1 donde se configuro IBGP y el Brocade 2 que se configuro BGP.

Brocade 2 es el router fronterizo de este AS, se realizó un show ip route en el Cisco 1 donde nos muestra toda la tabla de rutas (Ver Figura 7-3), además de la dirección del servidor (200.10.10.0)

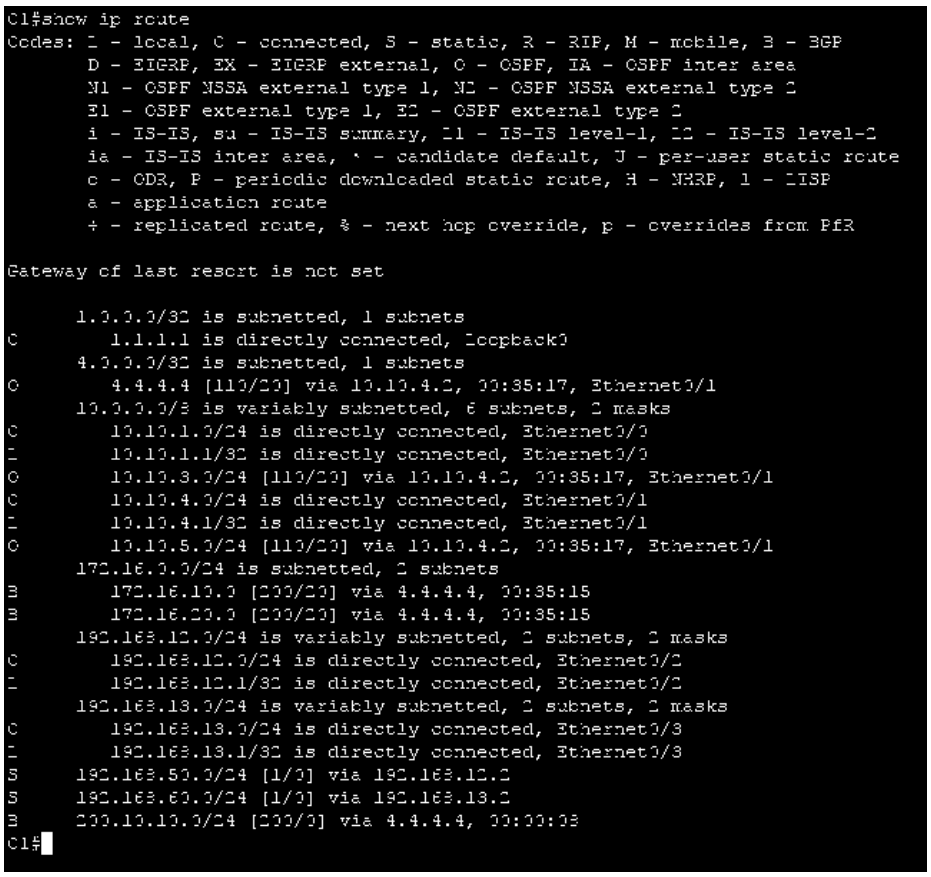

Figura 7-3. Display Routing Table C1

Realizado por: (Hidalgo Magaly. 2019)

La Tabla de rutas del equipo Brocade 2 de igual forma que en Cisco 1 realizamos un run show ip route y nos muestra la información acerca de la tabla de rutas de las que están directamente conectadas y de las que están por medio de Subnetted.

En la Figura 8-3 se observa que Brocade 2 conoce las direcciones del servidor (200.10.10.0), además de los Host (192.168.50.0 y 192.168.60.0).

Figura 8-3. Display Routing Table Brocade 2

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes del Protocolo

Otro segmento de la convergencia de la red será conocer el tipo de mensajes que se envían dentro de la topología (Ver Figura 9-3), en este caso tenemos mensajes Hello propios de OSPF, Keepalive, ACK. Determinamos que existe interoperabilidad ya que se comunican los Routers por medio de un mensaje enviado y mensaje de respuesta.

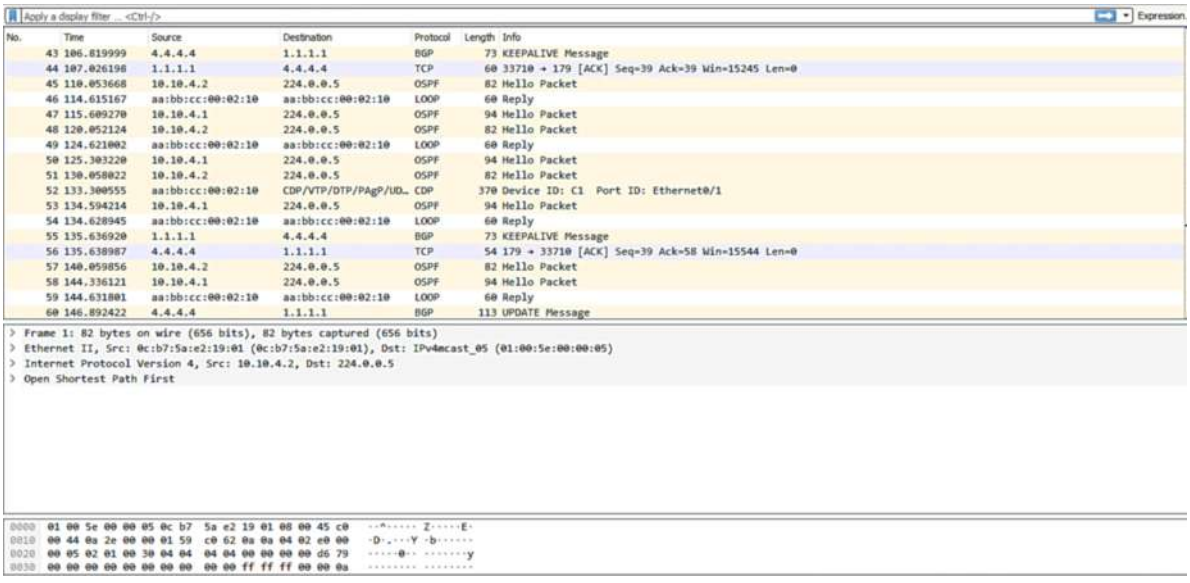

Figura 9-3. Mensajes AS 300

Realizado por: (Hidalgo Magaly. 2019)

3.2.1.2. Rendimiento AS 300

En la Tabla 4-3 especificamos algunas características del AS 300 como la tasa de transferencia, la perdida de paquetes entre otras. Estos nos ayudaran a comprender mejor el grado de interoperabilidad dentro de esta topología.

Tabla 4-3 Resultados Interoperabilidad AS 300

Características	200 Bytes	800 Bytes	1500 Bytes
Tasa de Transferencia	348,27 bits/s	354,13 bits/s	540.14 bits/s
Perdida de paquetes	0%	0.01%	0%
Latencia	9.899 ms	7.377 ms	8.295 ms
Payload	8.40 Bits/s	8.40 Bits/s	8.40 Bits/s
Tiempo de Muestreo	00:30:13	00:32:15	00:30:12

Realizado por: (Hidalgo Magaly. 2019)

3.2.2. Resultado 5: AS 500

En el Sistema Autónomo 500 por medio de Wireshark analizaremos los resultados recopilados en las pruebas de conectividad y transporte de datos que anteriormente generamos por Ostinato. Uno de los principales requisitos son las pruebas de ping entre el sistema y el servidor.

3.2.2.1. Convergencia AS 500

Utilizaremos dos factores para determinar la convergencia de la red: Tabla de Rutas y Mensajes dentro de la Topología, y para los parámetros será la latencia, pérdida de paquetes y la tasa de transferencia.

- Tabla de Rutas

Para conocer si existe interoperabilidad se realizó un show ip route, donde nos indica si la tabla de rutas conoce los caminos por donde transportar los paquetes dentro de la red, es así que observando la Figura 10-3 nos muestra las rutas conectadas directamente además de la que están por Subnetted. Debe tener la dirección del servidor (200.10.10.0) para que puedan los demás equipos tener acceso, ya que C6 es un router fronterizo donde está configurado BGP.

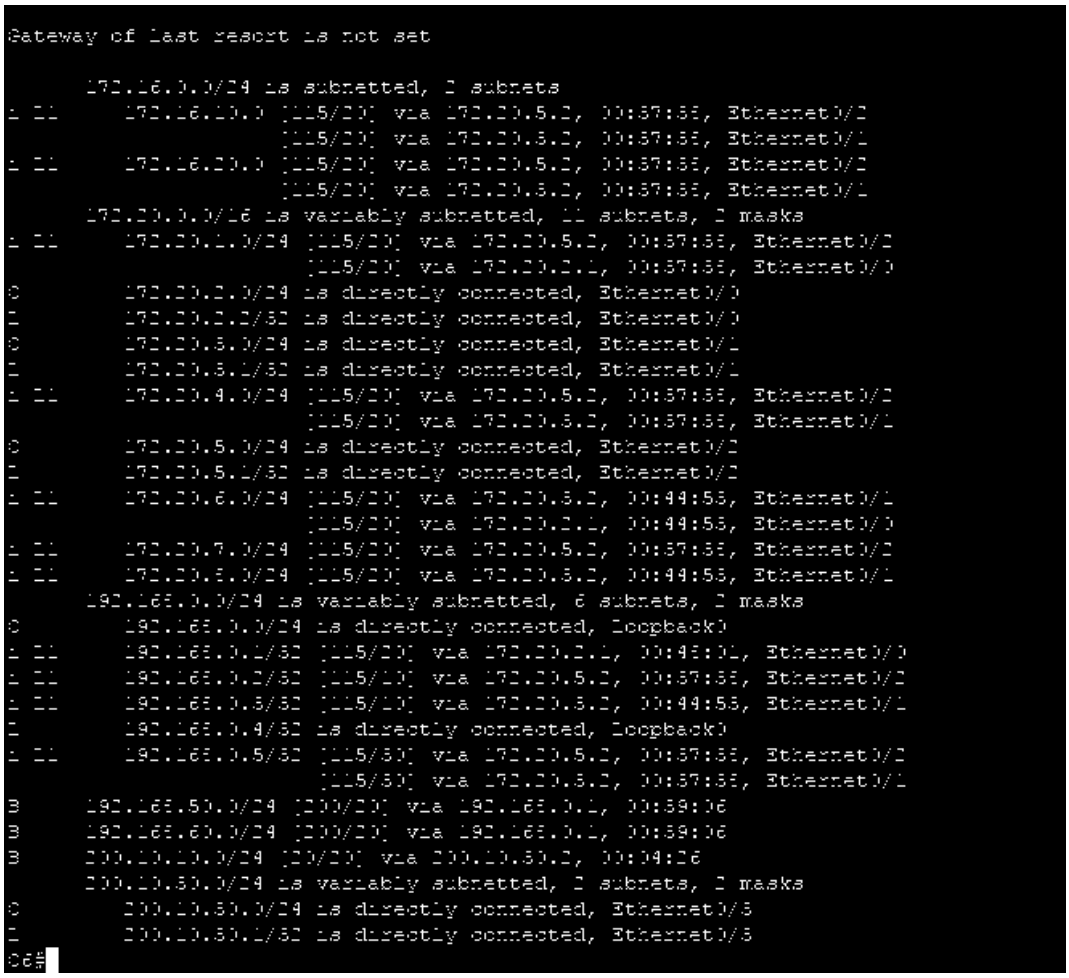

Figura 10-3. Display Routing Table C6

Realizado por: (Hidalgo Magaly. 2019)

De igual forma al anterior C5 es un Router fronterizo que debe tener la información necesaria para que los hosts accedan al servidor; además, de las métricas. Ver Figura 11-3 nos indica las rutas directamente conectadas y las que no lo están.

```
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
i L1     172.16.10.0 [115/20] via 172.20.6.2, 00:38:39, Ethernet0/2
                     [115/20] via 172.20.1.2, 00:38:39, Ethernet0/1
i L1     172.16.20.0 [115/20] via 172.20.6.2, 00:38:39, Ethernet0/2
                     [115/20] via 172.20.1.2, 00:38:39, Ethernet0/1
      172.20.0.0/16 is variably subnetted, 11 subnets, 2 masks
C        172.20.1.0/24 is directly connected, Ethernet0/1
L        172.20.1.1/32 is directly connected, Ethernet0/1
C        172.20.2.0/24 is directly connected, Ethernet0/0
L        172.20.2.1/32 is directly connected, Ethernet0/0
i L1     172.20.3.0/24 [115/20] via 172.20.6.2, 00:45:22, Ethernet0/2
                       [115/20] via 172.20.2.2, 00:45:22, Ethernet0/0
i L1     172.20.4.0/24 [115/20] via 172.20.6.2, 00:38:39, Ethernet0/2
                       [115/20] via 172.20.1.2, 00:38:39, Ethernet0/1
i L1     172.20.5.0/24 [115/20] via 172.20.2.2, 00:38:39, Ethernet0/0
                       [115/20] via 172.20.1.2, 00:38:39, Ethernet0/1
C        172.20.6.0/24 is directly connected, Ethernet0/2
L        172.20.6.1/32 is directly connected, Ethernet0/2
i L1     172.20.7.0/24 [115/20] via 172.20.1.2, 00:38:39, Ethernet0/1
i L1     172.20.8.0/24 [115/20] via 172.20.6.2, 00:45:22, Ethernet0/2
      192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
i L1     192.168.0.0/24 [115/20] via 172.20.2.2, 00:49:03, Ethernet0/0
C        192.168.0.1/32 is directly connected, Loopback0
i L1     192.168.0.2/32 [115/10] via 172.20.1.2, 00:38:39, Ethernet0/1
i L1     192.168.0.3/32 [115/10] via 172.20.6.2, 00:45:22, Ethernet0/2
i L1     192.168.0.5/32 [115/30] via 172.20.6.2, 00:38:39, Ethernet0/2
                        [115/30] via 172.20.1.2, 00:38:39, Ethernet0/1
B     192.168.50.0/24 [20/20] via 200.10.40.1, 00:40:01
B     192.168.60.0/24 [20/20] via 200.10.40.1, 00:40:01
B     200.10.10.0/24 [200/20] via 192.168.0.4, 00:05:21
      200.10.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.10.40.0/24 is directly connected, Ethernet0/3
L        200.10.40.2/32 is directly connected, Ethernet0/3
C5#
```

Figura 11-3. Display Routing Table C5

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes de la Topología

En la Figura 12-3 se muestra los paquetes que se transportan a traves de la red, para determinar el grado de interoperabilidad analizamos los paquetes (Keepalive, ACK, Hello.CSNP), estos son los que mantienen a sus vecinos informados si existe algun cambio en la topologia. Todo estos mensajes que se intercambiar nos indica que existe comunicación entre equipos por lo tanto interoperabilidad.

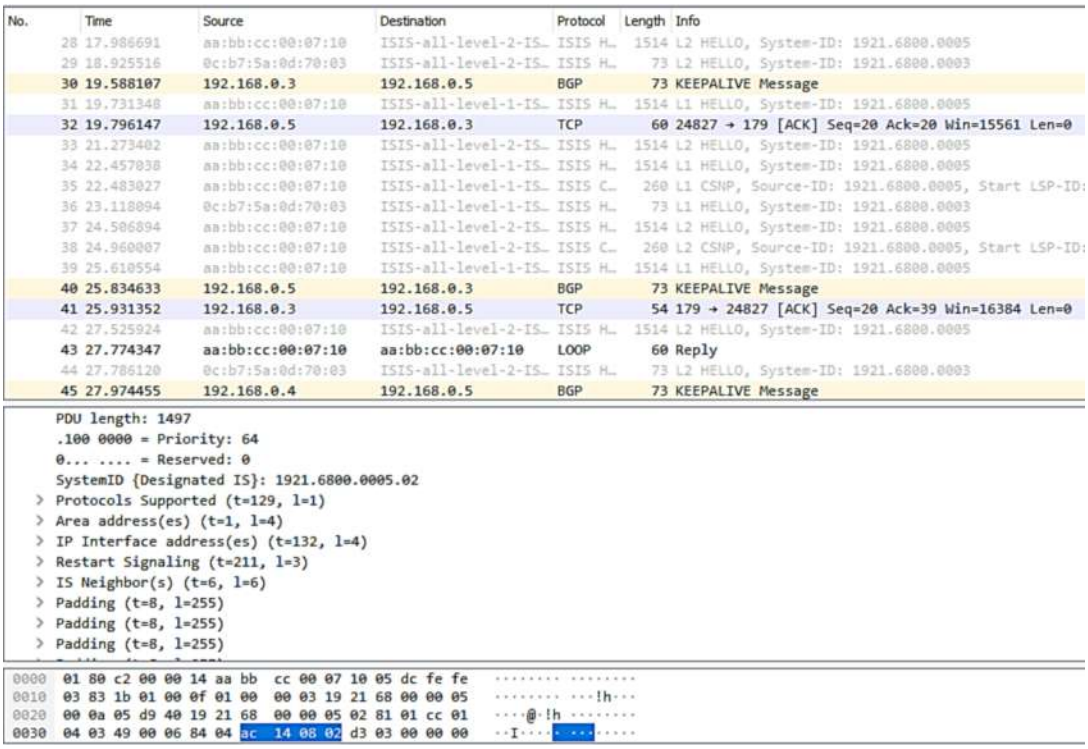

Figura 12-3. Mensajes AS 500

Realizado por: (Hidalgo Magaly. 2019)

3.2.2.2. Rendimiento AS 500

Por medio de Ostinato generamos trafico dentro de la red, para se realizo un muestreo de 00:30:00 aproximadamente con una cantidad de 200 bytes, 800 bytes y 1500 bytes respectivamente con paquetes TCP; donde, no solo transitaran paquetes TCP sino BGP, IS-IS, OSPF y propios de la red

Para determinar analiticamente los datos proporcionador por Wireshark observamos la Tabla 7-3 donde nos proporcina una informacion detallada del tiempo de transmision de los paquetes; ademas, de otras caracteristicas importantes dentro del AS 500.

Tabla 5-3 Resultados Interoperabilidad AS 500

Características	200 Bytes	800 Bytes	1500 Bytes
Tasa de Transferencia	12240 bits/s	12330 bits/s	9500 bits/s

Perdida de paquetes	0.01%	0.01%	0.01%
Latencia	8.507 ms	6.715 ms	9.045 ms
Payload	13.33 bits/s	12.53 bits/s	19.33 bits/s
Tiempo de Muestreo	00:32:17	00:30:49	00:30:20

Realizado por: (Hidalgo Magaly. 2019)

3.2.3. Resultado 6: AS 400

Como resultado de la prueba 6 en el AS 400 se determinará al igual que las anteriores pruebas la convergencia de la red por medio de la tabla de rutas y los mensajes, también el rendimiento y los parámetros a tomar en cuenta serán la latencia, tasa de transferencia y la perdida de paquetes.

3.2.3.1. Convergencia AS 400

- Tabla de Rutas

Para determinar la convergencia de Tablas de enrutamiento realizamos un run show ip route en el Brocade 1 donde nos muestra todas las rutas directamente o no conectadas. Ver Figura 13-3 podemos observar que conoce las direcciones de las rutas, una de las más importantes seria la ruta que conecta con los demás AS (200.10.30.0).

```
[edit]
vyatta@vyatta# run show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O   8.8.8.8/32 [110/10] is directly connected, lo, 00:07:27
C>* 8.8.8.8/32 is directly connected, lo
O>* 10.10.10.10/32 [110/11] via 10.30.10.2, eth2, 00:06:41
O   10.30.3.0/24 [110/10] is directly connected, eth4, 00:07:27
C>* 10.30.3.0/24 is directly connected, eth4
O   10.30.4.0/24 [110/10] is directly connected, eth0, 00:07:27
C>* 10.30.4.0/24 is directly connected, eth0
O   10.30.8.0/24 [110/10] is directly connected, eth1, 00:07:27
C>* 10.30.8.0/24 is directly connected, eth1
O>* 10.30.9.0/24 [110/20] via 10.30.10.2, eth2, 00:06:41
O   10.30.10.0/24 [110/10] is directly connected, eth2, 00:06:43
C>* 10.30.10.0/24 is directly connected, eth2
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.10.0/24 [20/20] via 200.10.30.1, eth3, 00:07:18
B>* 172.16.20.0/24 [20/20] via 200.10.30.1, eth3, 00:07:18
B>* 192.168.50.0/24 [20/0] via 200.10.30.1, eth3, 00:07:18
B>* 192.168.60.0/24 [20/0] via 200.10.30.1, eth3, 00:07:18
O>* 200.10.10.0/24 [110/20] via 10.30.10.2, eth2, 00:06:40
C>* 200.10.30.0/24 is directly connected, eth3
[edit]
vyatta@vyatta#
```

Figura 13-3. Display Routing Table Brocade 1

Realizado por: (Hidalgo Magaly. 2019)

En la Figura 14-3 que es del Cisco que se encuentra en el AS 400 debe conocer todas las rutas incluidas las del servidor (200.10.10.0), además de los hosts que están dentro de la red (192.168.50.0, 192.168.60.0, 172.16.20.0 y 172.16.10.0). Por ello determinamos que coexiste interoperabilidad entre en la plataforma ya que existe comunicación y se comparten información dentro de la topología.

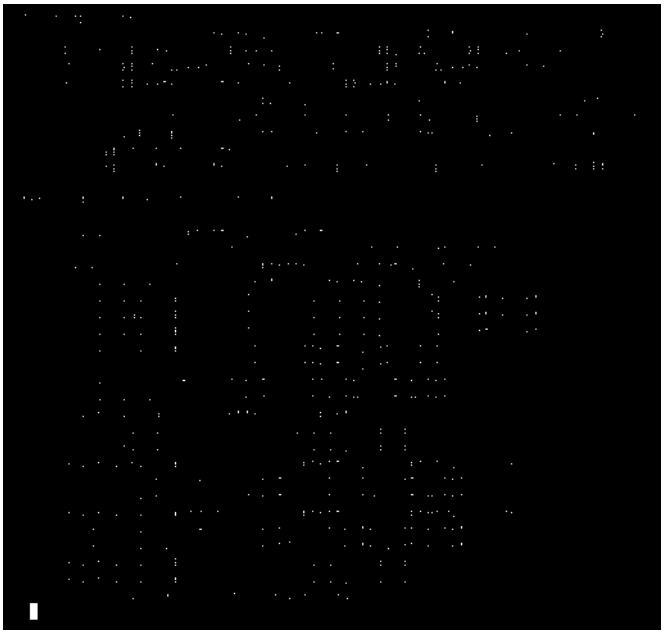

Figura 14-3. Display Routing Table C8

Realizado por: (Hidalgo Magaly. 2019)

- Mensajes del Protocolo

En la Figura 15-3 nos muestra los tipos de mensajes que se transporta dentro de la red (Keepalive, ACK, Hello), esto determina que si existe interoperabilidad dentro del AS 400. Por esta red transportan paquetes propios de AS 400 y además de los AS 300 Y 500 que están conectados por medio de BGP.

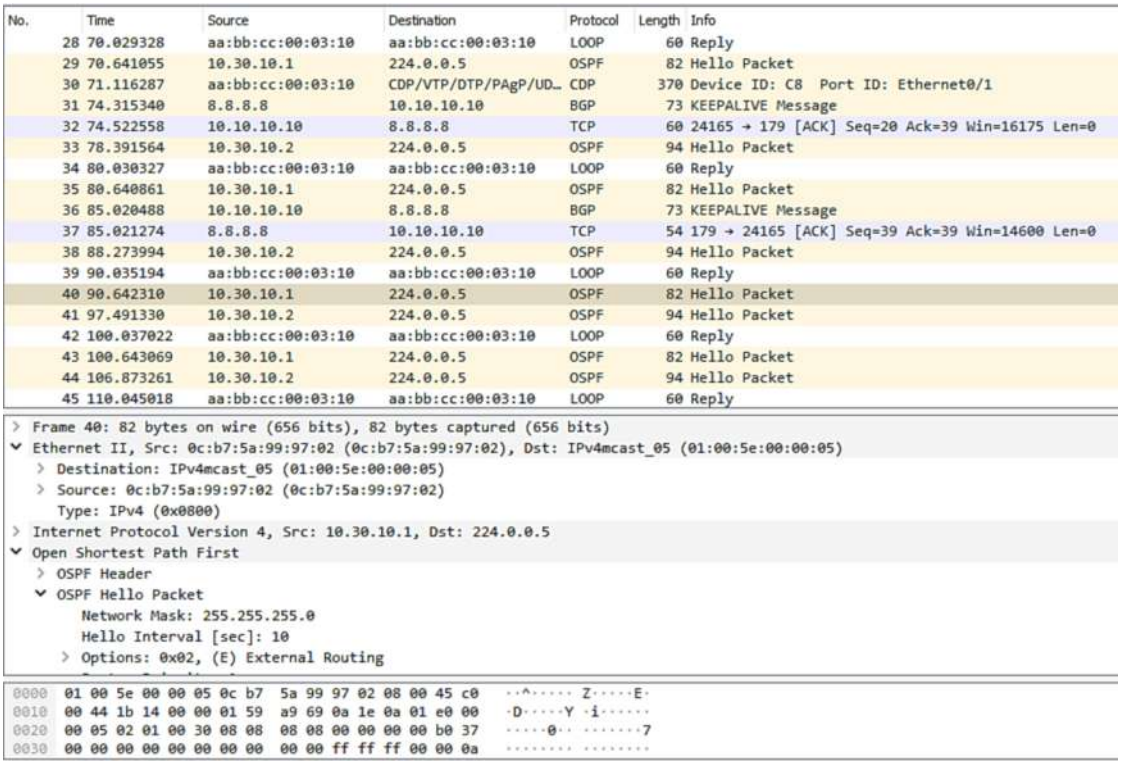

Figura 15-3. Trafico AS 400

Realizado por: (Hidalgo Magaly. 2019)

3.2.3.2. Rendimiento AS 400 con IPv4

Para analizar el tráfico que se generó en el AS 400 detallamos estos datos recopilados por Wireshark en una Tabla 10-3 donde determinamos los bytes transportados el tiempo entre otros detalles que utilizaremos para determinar el ancho de banda y la perdida de paquetes. Se transmitió por medio de Ostinato 3766 paquetes TCP.

Tabla 6-3 Resultado Interoperabilidad AS 400

Características	200 Bytes	800 Bytes	1500 Bytes
Tasa de Transferencia	368.27 bits/s	436.40 bits/s	389.73 bits/s
Perdida de paquetes	0%	0%	0%
Latencia	6.8 ms	9.4 ms	7.02 ms
Payload	8.40 bits/s	8.40 bits/s	8.40 bits/s
Tiempo de Muestreo	00:30:46	00:30:10	00:30:30

Realizado por: (Hidalgo Magaly. 2019)

3.2.4. Resultado Final Equipos Heterogéneos

3.2.4.1. Tasa de Transferencia

La tasa de transferencia será el ancho de banda real que se transmite a través de la topología, en nuestra plataforma observamos la Figura 16-3, 17-3, 18-3, donde nos muestra en graficas la tasa de transferencia de cada AS de la plataforma Multivendor.

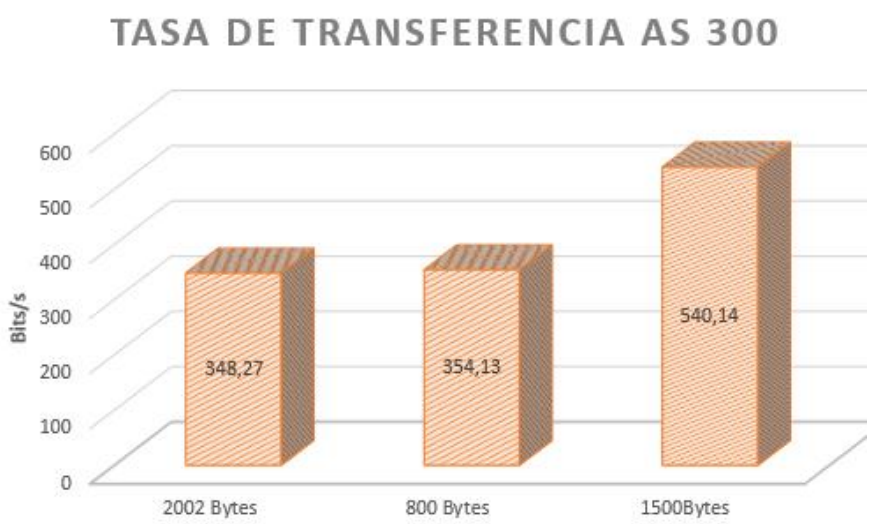

Grafico 1-3. Tasa de Transferencia AS 300

Realizado por: (Hidalgo Magaly. 2019)

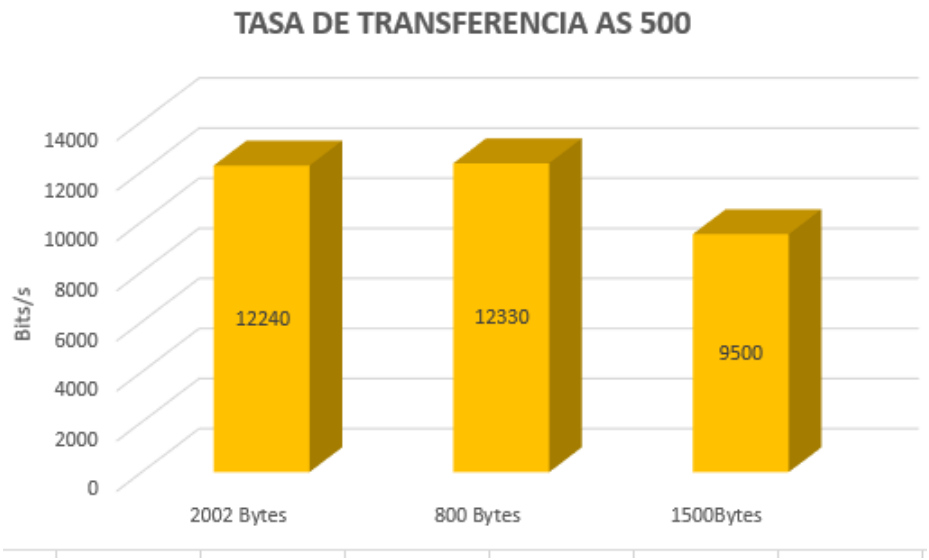

Grafico 2-3. Tasa de Transferencia AS 500

Realizado por: (Hidalgo Magaly. 2019)

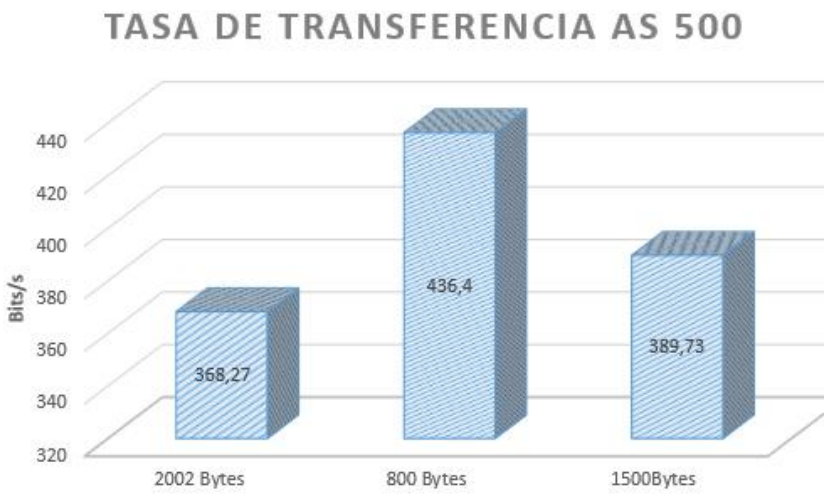

Grafico 3-3. Tasa de Transferencia AS 400

Realizado por: (Hidalgo Magaly. 2019)

3.2.4.2. Latencia

Un parámetro fundamental al momento de comprobar interoperabilidad en nuestra plataforma será medir la latencia donde se dice que si la latencia es mayor de 150ms será calificada como pésima. Para nuestro caso la latencia es mínima ya que se ha trabajado solo con datos, como se observa en la Figura 19, 20, 21-3 con una carga de 200 bytes, 800 bytes y 1500 bytes, existe mayor latencia en el AS 300.

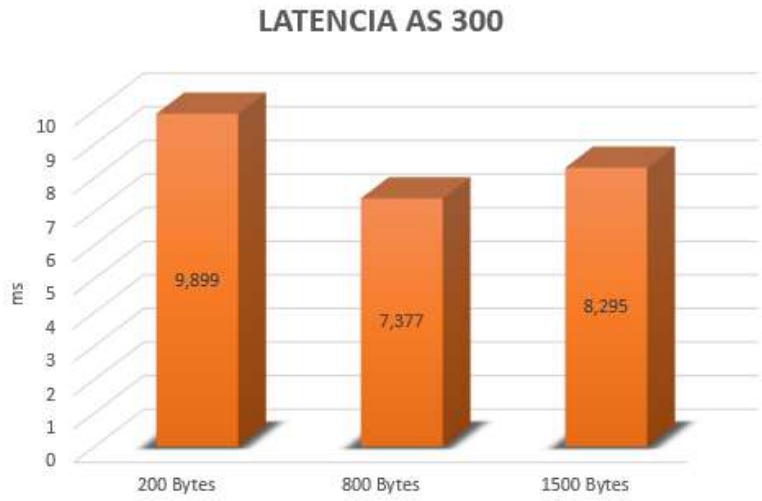

Grafico 4-3. Latencia AS 300

Realizado por: (Hidalgo Magaly. 2019)

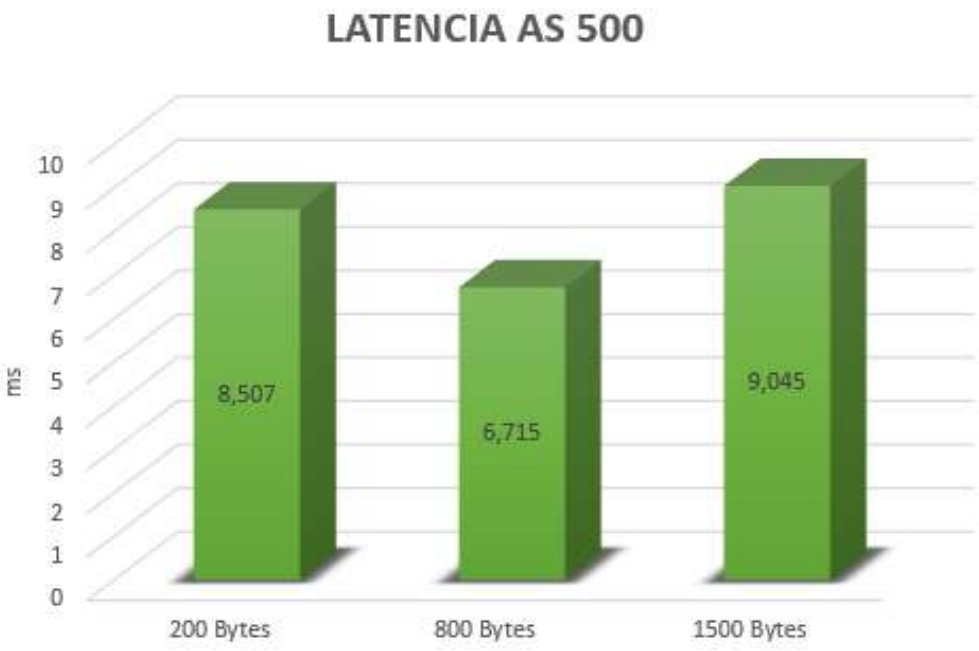

Grafico 5-3. Latencia AS 500

Realizado por: (Hidalgo Magaly. 2019)

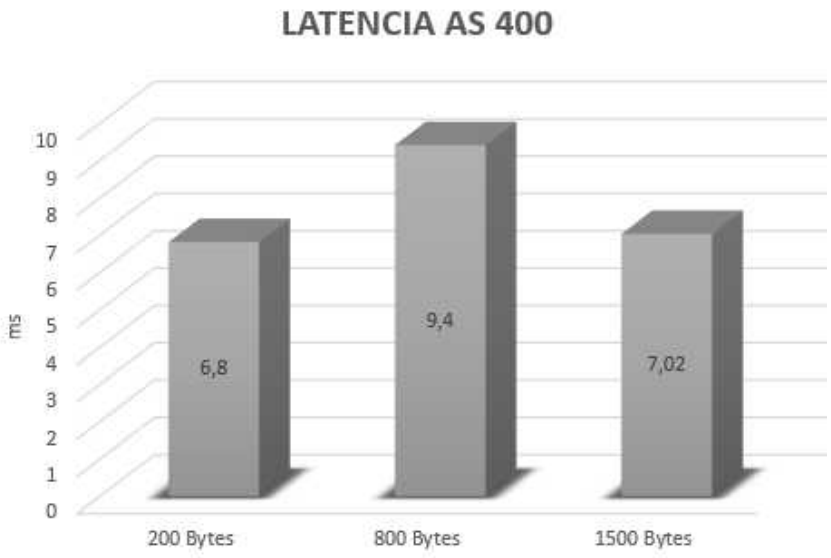

Grafico 6-3. Latencia AS 400

Realizado por: (Hidalgo Magaly. 2019)

3.2.4.3. Perdida de Paquetes

Según los resultados obtenidos la perdida de paquetes es mínima para toda la plataforma lo que nos ayuda a comprobar que tan interoperables seria nuestra plataforma trabajando con diferentes plataformas Networking. En la Figura 22-3 nos muestra en conjunto la perdida de paquetes dentro de toda la topología.

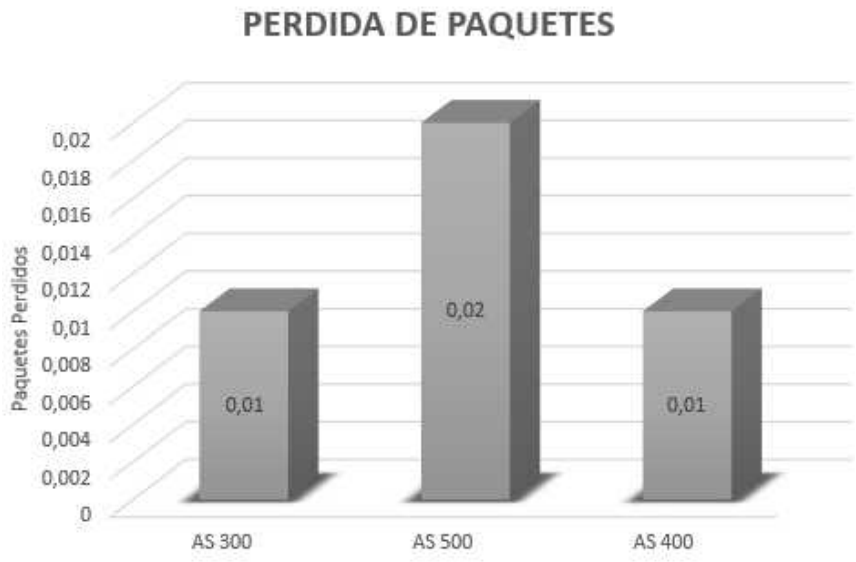

Grafico 7-3. Pérdida de Paquetes AS 300, 400 y 500

Realizado por: (Hidalgo Magaly. 2019)

3.3. Resultados de Interoperabilidad Plataforma Multivendor

3.3.1. Resultados Finales de la Interoperabilidad Plataforma

Como resultado de interoperabilidad (Ver Figura 24-3), entre las diferentes marcas de equipos tenemos que optimizamos el intercambio de Informacion por medio de diferentes AS, que se interconectar en base a protocolos y sus politicas. En nuestra Plataforma se muestra que existe comunicación y ahora podemos realizar un analisis de como funciona

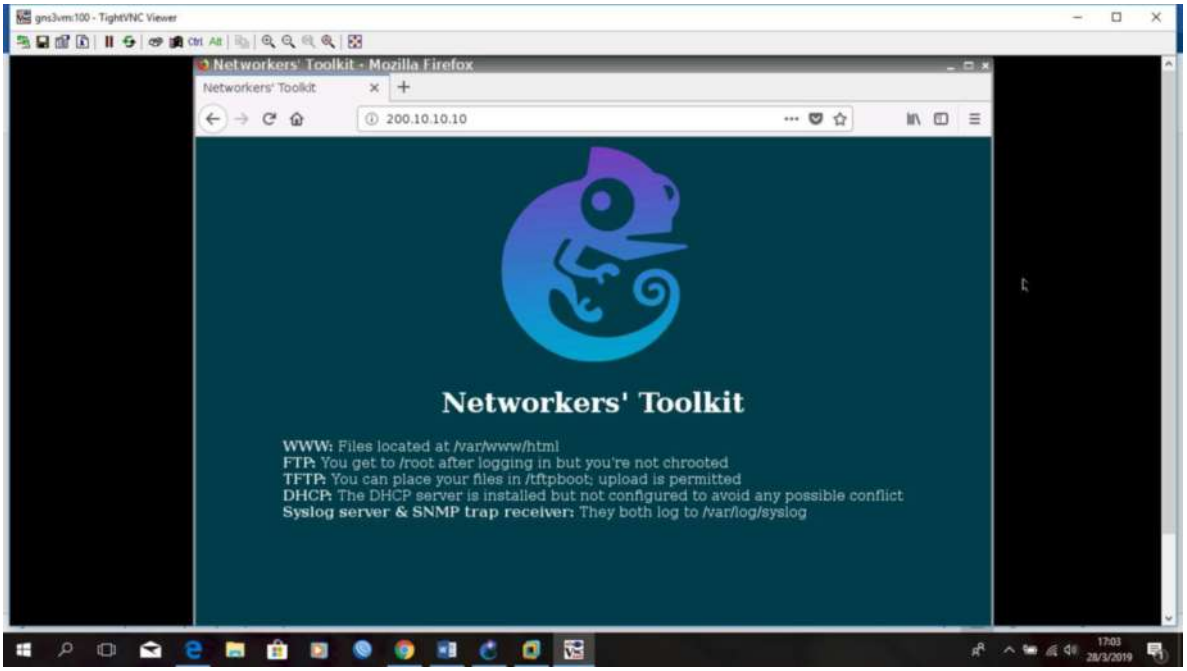

Figura 16-3. Servidor

Realizado por: (Hidalgo Magaly. 2019)

El hecho que desde cualquier equipo se acceda al servidor nos comprueba que nuestra Plataforma a dado con los requerimientos para que en un futuro se implemente este sistema de manera física y se pueda conectar diferentes sistemas y ofrecer servicios que ayuden en un bien común.

CONCLUSIONES

Se determinó que las plataformas de equipamiento Networking que más aceptación poseen en el mercado son Cisco como líder, Juniper, Brocade y Mikrotik, analizamos sus características; además, de su grado de interoperabilidad, trabajando conjuntamente con equipos homogéneos y heterogéneos.

Para Verificar el Grado de Interoperabilidad entre los algoritmos IGP y EGP, se configuro diferentes sistemas Autónomos dentro de una misma topología de red. Se analizó el ancho de banda y la perdida de paquetes dentro de cada uno de los AS.

La utilización de la herramienta GNS3 nos permitió simular redes convergentes existentes en la actualidad, aunque no trabajen con los equipos de innovación pudimos determinar el comportamiento de una red de gran tamaño, sin la necesidad que tener los equipos físicamente logramos comprobar las ventajas y desventajas de diferentes AS conectados.

Realizamos un banco de 6 pruebas para determinar el adecuado funcionamiento de la red, ya que mediante Ostinato inyectamos tráfico a la plataforma para simular una red corporativa, se configuro los protocolos IS-IS y OSPF dentro de los AS y BGP como el protocolo de transporte para comunicar los AS.

Para determinar la interoperabilidad de la Plataforma tomamos en cuenta 3 parámetros que fueron la tasa de transferencia, la latencia y la perdida de paquetes; además, se realizaron pruebas inyectando 200 bytes, 800 bytes y 1500 bytes. Concluimos que el Sistema Autónomo que más tasa de transferencia ocupa es el AS 500 con un 30% más que los otros AS.

De determino la latencia dentro de la topología y como resultado se obtuvo que el AS 300 tiene un porcentaje del 10% mayor al resto de Sistemas.

El desarrollo de una Plataforma de Interoperabilidad de procesos integrados dentro de un AS ayuda a la cooperación de servicios públicos, en línea a través de internet o por telefonía móvil. Planificando el uso de recursos en las entidades del estado como su crecimiento y desarrollo, ayudaríamos a controlar la información que se proporciona al cliente sea legible y verídica.

La creación de una plataforma no solo será un crecimiento en la tecnología sino ayudará a mejorar los servicios públicos del estado.

RECOMENDACIONES

Para la implementación de la plataforma algo muy importante es el equipo que utilizaremos para la simulación, ya que su memoria RAM mínima deberá ser de 8Gb ya que los protocolos de enrutamiento que implementaremos dentro de GNS3 poseen su propia capacidad de almacenamiento.

Recomendamos la utilización de protocolos de enrutamiento como IS-IS y OSPF para la creación de grandes topologías ya que estos permites varios dispositivos conectados al mismo tiempo y se asegurara que la red no colapse.

Se debe analizar cada una de las plataformas de simulación, así como los protocolos a implementar descubrir sus características y ventajas para la implementación de la topología de la red.

A mayor ancho de banda se asegurará que la red no se haga lenta, es por ello que se recomienda que las empresas cuyos fines sean la de ofrecer servicios públicos posea un amplio acceso de internet.

Es recomendable ejercer normas para la legalización de las empresas que compongan este sistema ya que deben existir políticas de cada empresa y se debe respetar según los datos de información que proporcionen.

BIBLIOGRAFIA

HEDRICK, C.," Routing Information Protocol (RIP)". *Network Working Group*, (1988). pp. 4-10.

REKHTER, Y. ; HARES, S. ; LI, T.," A Border Gateway Protocol 4 (BGP)". *Standards Track*, (2006). pp. 6-15.

SAVAGE, D. ; MOORE, S. ; SLICE, D. ; PALUCH, P.," Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)". *Informational*, (2016). pp. 5-18.

MALKIN, G.," Rip Version 2 (RIP)". *Standarda Track*, (1998). pp. 5-12.

MOY, J.," OSPF Version 2 (OSPF)". *Standards Track* (1994). pp. 5-88.

SMIT, H. ; LI, T.," Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)". *Informational*, (2004). pp. 2-12.

CISCO., *Cisco* [en línea]. Birmingham: Cuadrante Magico de Gartner. 2018. gblogs. Disponible en: https://gblogs.cisco.com/la/sc-geeritt-cisco-lider-en-firewalls-de-redes-empresariales-segun-el-cuadrante-magico-de-gartner-2018-para-firewalls-de-redes-empresariales/.

DUFFY, M., *Puppet Reporting and Monitoring* [en línea]. First. Birmingham - Mumbai. 2014. ISBN 9781783981427. Disponible en: https://gblogs.cisco.com/la/sc-geeritt-cisco-lider-en-firewalls-de-redes-empresariales-segun-el-cuadrante-magico-de-gartner-2018-para-firewalls-de-redes-empresariales/.

DZERKALS, U., EVE-NG Professional Cookbook. , 2017. p. 197.

EDUREKA, DevOps Tools: Configuration Management & Deployment. [en línea]. 2017. [Consulta: 5 enero 2019]. Disponible en: https://www.slideshare.net/EdurekaIN/chef-vs-puppet-vs-ansible-vs-saltstack-configuration-management-tools-comparison-edureka.

NEUMANN, J.C., *The book of GNS3 : build virtual network labs using Cisco, Juniper, and more*. San Francisco: No Starch Press. 2015. ISBN 978-1-59327-554-9.

OCAMPO ZUÑIGA, A., Emuladores de Red | Networking. [en línea]. 2015. [Consulta: 31 agosto 2018]. Disponible en: https://aocampoz.wordpress.com/2015/05/02/emuladores-de-red/.

STALLINGS, W., Comunicaciones y Redes de Computadores. *Pearson Prentice Hall*, 2004. p. 896.

WELSH, C., *GNS3 Network Simulation Guide* [en línea]. Birmingham: Packt Publishing. 2013. ISBN 1782160809. Disponible en: http://cds.cern.ch/record/1633716.

ANEXOS

ANEXO A

CONFIGURACIONES PRIMER ESCENARIO

Cisco 1

```
C1(config) #int lo0
C1(config) #ip add 1.1.1.1 255.255.255.255
C1(config) #exit
C1(config) #interface e0/0
C1(config-if)#ip address 10.10.1.1
255.255.255.0
C1(config-if)#no shut
C1(config-if)#exit
C1(config) #interface e0/1
C1(config-if)#ip address 10.10.4.1
255.255.255.0
C1(config-if)#no shut
C1(config-if)#exit
C1(config) #interface e0/2
C1(config-if)#ip address 192.168.12.1
255.255.255.0
C1(config-if)#no shut
C1(config-if)#exit
C1(config) #interface e0/3
C1(config-if)#ip address 192.168.13.1
255.255.255.0
C1(config-if)#no shut
C1(config-if)#exit
```

Configuración de OSPF

```
C1(config) #router OSPF 10
C1(config-router)#router-id 1.1.1.1
C1(config-router)#network 10.10.1.0
0.0.0.255 area 0
C1(config-router)#network 10.10.4.0
0.0.0.255 area 0
C1(config-router)#network 192.168.12.0
0.0.0.255 area 0
C1(config-router)#network 192.168.13.0
0.0.0.255 area 0
```

Cisco 2

```
C2(config) #int lo0
C2(config) #ip add 2.2.2.2 255.255.255.255
C1(config) #exit
C2(config) #interface e0/0
C2(config-if)#ip address 10.10.2.2
255.255.255.0
C2(config-if)#no shut
C2(config-if)#exit
C2(config) #interface e0/1
C2(config-if)#ip address 10.10.5.1
255.255.255.0
C2(config-if)#no shut
C2(config-if)#exit
```

Configuración de OSPF

```
C2(config) #router OSPF 10
C2(config-router)#router-id 2.2.2.2
C2(config-router)#network 10.10.2.0
0.0.0.255 area 0
C2(config-router)#network 10.10.5.0
0.0.0.255 area 0
```

Juniper 1

```
J1#set interfaces em0 unit 0 family inet
address 10.10.1.2/24
J1#set interfaces em1 unit 0 family inet
address 10.10.2.1/24
J1#set interfaces em2 unit 0 family inet
address 10.10.3.1/24
J1#commit
```

Configuración de OSPF

```
J1#set routing-options router.id 3.3.3.3
J1#set protocols ospf area 0.0.0.0 interface
em0
J1#set protocols ospf area 0.0.0.0 interface
em1
J1#set protocols ospf area 0.0.0.0 interface
em2
```

Brocade 2

Para accede al Brocade nos pide login: vyatta y su password: vyatta, accedemos a la consola de configuración y escribimos los siguientes códigos:

vyatta @vyatta:~$ configure
vyatta @vyatta # set interfaces loopback lo address 4.4.4.4/32
vyatta @vyatta #set interfaces Ethernet eth0 address 10.10.5.2/24
vyatta @vyatta #set interfaces Ethernet eth1 address 10.10.4.2/24
vyatta @vyatta #set interfaces Ethernet eth2 address 10.10.3.2/24
vyatta @vyatta #set interfaces Ethernet eth3 address 200.10.40.1/24
vyatta @vyatta #commit

Configuración de OSPF

vyatta @vyatta # set protocols ospf parameters router-id 4.4.4.4
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.10.3.0/24
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.10.4.0/24
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.10.5.0/24
vyatta @vyatta #commit

Mikrotik 1

Figura 16-2. Cloud-1 utilizado para configurar Mikrotik
Realizado por: (Hidalgo Magaly. 2019)

Para la Configuración de Mikrotik utilizamos un Cloud-1.

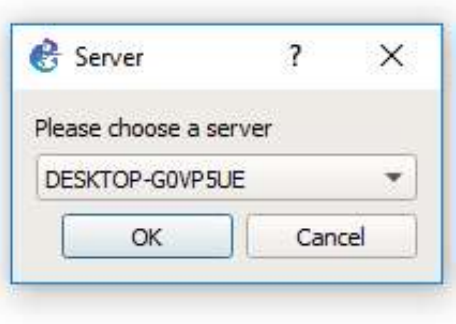

Figura 17-2. Cloud-1 conectado a la PC
Realizado por: (Hidalgo Magaly. 2019)

Automáticamente nos pregunta si nuestro Cloud se conectara con el equipo o la máquina virtual, debemos escoger la Pc para la configuración de Mikrotik. Después procedemos a configurar; este procedimiento realizamos una sola vez ya que por medio de este cloud podemos configurar todos los Mikrotik de nuestra plataforma.

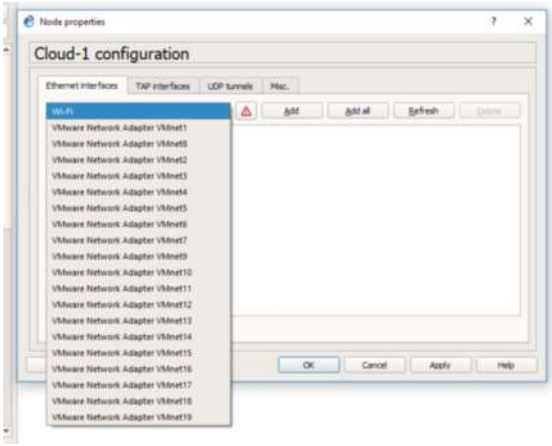

Figura 18-2. Tarjeta Virtual del Cloud-1
Realizado por: (Hidalgo Magaly. 2019)

En la configuración escogemos el VMware Network Adapter VMnet19, ya que esta previamente a sido configurada en la PC para que se conecte con la máquina virtual. Añadimos, aplicamos y colocamos OK.
Como se observa en la Figura 18-2 del primer escenario conectamos a un Switch, y al Mikrotik en la ether6. Encendemos el equipo y esperamos que se cargue.

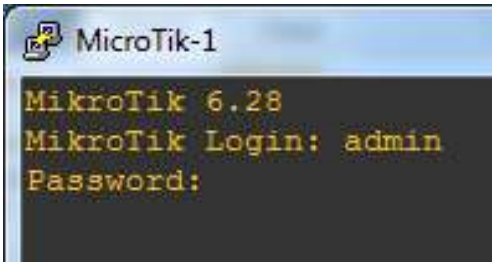

Figura 19-2. Configuración de Mikrotik
Realizado por: (Hidalgo Magaly. 2019)

No tiene password, solo agregamos la dirección IP, la máscara y el Interface 6.
[admin@MikroTik]>ip address add address=192.168.18.10/24 interface=ether6
Después descargamos el WINBOX que es gratuito, por medio de este configuramos y asignamos las direcciones IP con las interfaces; ingresamos la dirección IP asignada anteriormente; es decir 192.168.18.10 y conectamos, como se muestra en la Figura 20-2.

Figura 20-2. WinBox conectado a Mikrotik 192.168.18.10
Realizado por: (Hidalgo Magaly. 2019)

Asignamos las direcciones conectadas a nuestro Mikrotik como esta en la tabla de enrutamiento, aplicamos y aceptamos; así con cada una de las direcciones IP

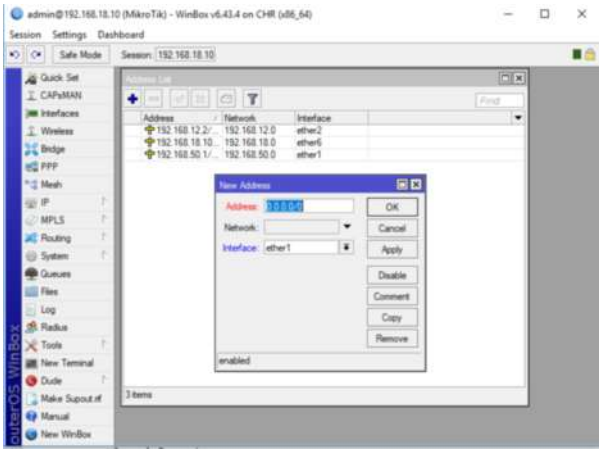

Figura 21-2. WinBox asignado direcciones de Mikrotik
Realizado por: (Hidalgo Magaly. 2019)

WEBTERM 1
Encendemos la PC, y abrimos el Terminal para configurar.

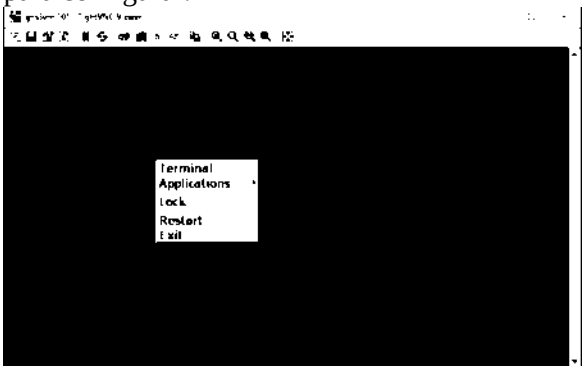

Figura 22-2. WebTerm 1
Realizado por: (Hidalgo Magaly. 2019)

root@webterm-1:~# ifconfig eth0 192.168.50.10 netmask 255.255.255.0
root@webterm-1:~#route add default gw 192.168.50.1

WEBTERM 2

root@webterm-1:~# ifconfig eth0 192.168.60.10 netmask 255.255.255.0
root@webterm-1:~#route add default gw 192.168.60.1

Cerramos el WebTerm y procedemos a realizar una última configuración en el Cisco 1 asignamos rutas por defecto para que pueda distribuir las configuraciones con OSPF.

Otra forma de configurar los WEBTERM es por medio de su configuración interna, no por medio de la consola; además esta configuración quedara grabada, sabemos que al momento de apagar los equipos las configuraciones no se guardan. Por ello seguimos estos sencillos pasos:
Primero Clik derecho sobre WEBTERM1 y seleccionamos configuración:

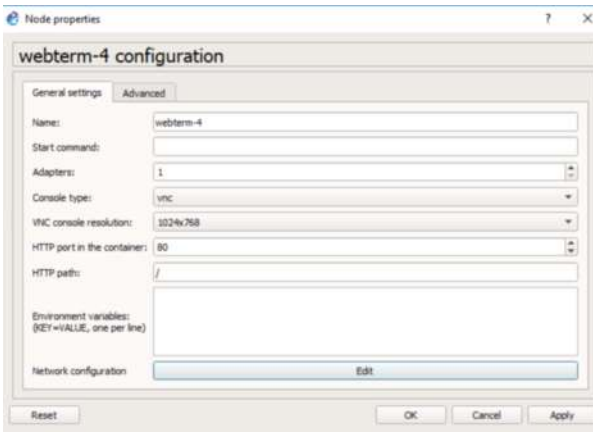

Figura 23-2. Configuración de WebTerm 4
Realizado por: (Hidalgo Magaly. 2019)

Seleccionamos Edit (Network configuration)

```
#
# This is a sample network config uncomment lines to configure the network
#


# Static config for eth0
#auto eth0
#iface eth0 inet static
#               address 192.168.0.2
#               netmask 255.255.255.0
#               gateway 192.168.0.1
#               up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
```

Figura 24-2. Configuración Interna de WebTerm 4
Realizado por: (Hidalgo Magaly. 2019)

Realizamos los siguientes cambios, para guardar la configuración de cada uno de los equipos.

```
#
# This is a sample network config uncomment lines to configure the network
#


# Static config for eth0
#auto eth0
#iface eth0 inet static
#               address 192.168.0.2
#               netmask 255.255.255.0
#               gateway 192.168.0.1
#               up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
 auto eth0
 iface eth0 inet static
address 172.16.20.10
netmask 255.255.255.0
gateway 172.16.20.1
```

Figura 25-2. Configuración definitiva de WebTerm 4
Realizado por: (Hidalgo Magaly. 2019)

WebTerm es una herramienta de red, contiene un navegador web Firefox que me permite ingresar a internet. Por medio de las configuraciones realizadas podemos realizar ping entre los hosts de cada Sistema Autónomo dentro de su red creada; además, estas configuraciones debemos realizar en cada uno de los WebTerm y el Server dentro de la plataforma, con las direcciones, mascara y Gateway previamente asignados.

CONFIGURACIONES SEGUNDO ESCENARIO
Cisco 5
C5(config)# int lo0
C5(config-if)#ip add 192.168.0.1 255.255.255.255
C5(config-if)#exit
C5(config) #interface e0/0
C5(config-if)#ip address 172.20.2.1 255.255.255.0
C5(config-if)#no shut
C5(config-if)#ip router isis
C5(config-if)#exit
C5(config) #interface e0/1
C5(config-if)#ip address 172.20.1.1 255.255.255.0
C5(config-if)#no shut
C5(config-if)#ip router isis
C5(config-if)#exit
C5(config) #interface e0/2
C5(config-if)#ip address 172.20.6.1 255.255.255.0
C5(config-if)#no shut
C5(config-if)#ip router isis

C5(config-if)#exit

Configuración de ISIS
C5(config) #router isis
C5(config-router)#net
49.0006.1921.6800.0001.00
C2(config-if)#exit
C2(config)#

Cisco 6
C6(config)# int lo0
C6(config-if)#ip add 192.168.0.4
255.255.255.255
C6(config-if)#exit
C6(config) #interface e0/0
C6(config-if)#ip address 172.20.2.2
255.255.255.0
C6(config-if)#no shut
C6(config-if)#ip router isis
C6(config-if)#exit
C6(config) #interface e0/1
C6(config-if)#ip address 172.20.3.1
255.255.255.0
C6(config-if)#no shut
C6(config-if)#ip router isis
C6(config-if)#exit
C6(config) #interface e0/2
C6(config-if)#ip address 172.20.5.1
255.255.255.0
C6(config-if)#no shut
C6(config-if)#ip router isis
C6(config-if)#exit
C6(config-if)#ip address 172.20.6.1
255.255.255.0
C6(config-if)#no shut
C6(config-if)#ip router isis
C6(config-if)#exit

Configuración de ISIS
C6(config) #router isis
C6(config-router)#net
49.0006.1921.6800.0004.00
C6(config-if)#exit
C6(config)#

Juniper 6

J6#set interfaces loopback lo address
192.168.0.2/32

J6#set interfaces em0 unit 0 family inet
address 172.20.4.1/24
J6#set interfaces em0 unit 0 family iso
J6#set interfaces em1 unit 0 family inet
address 172.20.1.2/24
J6#set interfaces em1 unit 0 family iso
J6#set interfaces em2 unit 0 family inet
address 172.20.5.2/24
J6#set interfaces em2 unit 0 family iso
J6#set interfaces em3 unit 0 family inet
address 172.20.7.1/24
J6#set interfaces em3 unit 0 family iso
J6#commit

Configuración de ISIS
J6#set interfaces lo0 unit 0 family iso address
49.0006.1921.6800.0002.00
J6#set protocols isis interface em0
J6#set protocols isis interface em1
J6#set protocols isis interface em2
J6#set protocols isis interface em3

Juniper 7
J6#set interfaces loopback lo address
192.168.0.3/32
J7#set interfaces em0 unit 0 family inet
address 172.20.3.2/24
J7#set interfaces em0 unit 0 family iso
J7#set interfaces em1 unit 0 family inet
address 172.20.4.2/24
J7#set interfaces em1 unit 0 family iso
J7#set interfaces em2 unit 0 family inet
address 172.20.6.2/24
J7#set interfaces em2 unit 0 family iso
J7#set interfaces em3 unit 0 family inet
address 172.20.8.1/24
J7#set interfaces em3 unit 0 family iso
J7#commit

Configuración de ISIS

J7#set interfaces lo0 unit 0 family iso address
49.0006.1921.6800.0003.00
J7#set protocols isis interface em0
J7#set protocols isis interface em1
J7#set protocols isis interface em2
J7#set protocols isis interface em3

Mikrotik 5
[admin@MikroTik] >ip address add
address=192.168.18.30/24 interface=ether6

Mikrotik 6
[admin@MikroTik] > ip address add address=192.168.18.40/24 interface=ether6

Una vez asignadas las configuraciones realizamos el mismo procedimiento en el primer escenario asignando las direcciones Ip por medio del WinBox Utilizando el mismo Cloud-1.

WEBTERM 3

root@webterm-1:~# ifconfig eth0 172.16.10.10 netmask 255.255.255.0
root@webterm-1:~#route add default gw 172.16.10.1

WEBTERM 4
root@webterm-1:~# ifconfig eth0 172.16.20.10 netmask 255.255.255.0
root@webterm-1:~#route add default gw 172.16.20.1

CONFIGURACIONES TERCER ESCENARIO
Cisco 3
C3(config)# int lo0
C3(config-if)#ip add 5.5.5.5 255.255.255.255
C3(config-if)#exit
C3(config) #interface e0/0
C3(config-if)#ip address 10.30.2.1 255.255.255.0
C3(config-if)#no shut
C3(config-if)#exit
C3(config) #interface e0/1
C3(config-if)#ip address 10.30.1.1 255.255.255.0
C3(config-if)#no shut
C3(config-if)#exit
C3(config) #interface e0/2
C3(config-if)#ip address 10.30.6.1 255.255.255.0
C3(config-if)#no shut
C3(config-if)#exit

Configuración de OSPF
C3(config) #router OSPF 10
C3(config-router)#router-id 5.5.5.5
C3(config-router)#network 10.30.2.0 0.0.0.255 area 0
C3(config-router)#network 10.30.1.0 0.0.0.255 area 0
C3(config-router)#network 10.30.6.0 0.0.0.255 area 0
C3(config-router)#exit

Cisco 4
C4(config)# int lo0
C4(config-if)#ip add 6.6.6.6 255.255.255.255
C4(config-if)#exit
C4(config) #interface e0/0
C4(config-if)#ip address 10.30.4.1 255.255.255.0
C4(config-if)#no shut
C4(config-if)#exit
C4(config) #interface e0/1
C4(config-if)#ip address 10.30.1.2 255.255.255.0
C4(config-if)#no shut
C4(config-if)#exit
C4(config) #interface e0/2
C4(config-if)#ip address 10.30.5.1 255.255.255.0
C4(config-if)#no shut
C4(config-if)#exit

Configuración de OSPF
C4(config) #router OSPF 10
C4(config-router)#router-id 6.6.6.6
C4(config-router)#network 10.30.4.0 0.0.0.255 area 0
C4(config-router)#network 10.30.1.0 0.0.0.255 area 0
C4(config-router)#network 10.30.5.0 0.0.0.255 area 0
C4(config-router)#exit

Juniper 3
J3#set interfaces loopback lo address 7.7.7.7/32
J3#set interfaces em0 unit 0 family inet address 10.30.2.2/24
J3#set interfaces em1 unit 0 family inet address 10.30.3.1/24
J3#set interfaces em2 unit 0 family inet address 10.30.7.1/24
J3#set interfaces em3 unit 0 family inet address 10.30.9.1/24
J3#commit

Configuración de OSPF
J3#set routing-options router-id 7.7.7.7
J3#set protocols ospf area 0.0.0.0 interface em0
J3#set protocols ospf area 0.0.0.0 interface em1
J3#set protocols ospf area 0.0.0.0 interface em2
J3#set protocols ospf area 0.0.0.0 interface em3
J3#commit

Juniper 4
J3#set interfaces loopback lo address 9.9.9.9/32
J4#set interfaces em0 unit 0 family inet address 10.30.7.2 /24
J4#set interfaces em1 unit 0 family inet address 10.30.6.2/24
J4#set interfaces em2 unit 0 family inet address 10.30.5.2/24
J4#set interfaces em2 unit 0 family inet address 10.30.8.2/24
J4#commit

Configuración de OSPF
J4#set routing-options router-id 9.9.9.9
J4#set protocols ospf area 0.0.0.0 interface em0
J4#set protocols ospf area 0.0.0.0 interface em1
J4#set protocols ospf area 0.0.0.0 interface em2
J4#set protocols ospf area 0.0.0.0 interface em3
J4#commit

Brocade-1

Para accede al Brocade nos pide login: vyatta y su password: vyatta, accedemos a la consola de configuración y escribimos los siguientes códigos:

vyatta @ vyatta :~$ configure
vyatta @vyatta #set interfaces loopback lo address 8.8.8.8/32
vyatta @vyatta #set interfaces Ethernet eth0 address 10.30.4.2/24
vyatta @vyatta #set interfaces Ethernet eth1 address 10.30.8.2/24
vyatta @vyatta #set interfaces Ethernet eth2 address 10.30.10.1/24
vyatta @vyatta #set interfaces Ethernet eth3 address 200.10.30.2/24
vyatta @vyatta #set interfaces Ethernet eth4 address 10.30.3.2/24
vyatta @vyatta #commit

Configuración de OSPF
vyatta @vyatta # set protocols ospf parameters router-id 8.8.8.8
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.30.3.0/24
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.30.4.0/24
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.30.8.0/24
vyatta @vyatta # set protocols ospf area 0.0.0.0 network 10.30.10.0/24
vyatta @vyatta #commit

Cisco 8
C8(config) #int lo0
C8(config-if)#ip add 10.10.10.10 255.255.255.255
C8(config-if)#exit
C8(config) #interface e0/0
C8(config-if)#ip address 10.30.9.2 255.255.255.0
C8(config-if)#no shut
C8(config-if)#exit
C8(config) #interface e0/1
C8(config-if)#ip address 10.30.10.2 255.255.255.0
C8(config-if)#no shut
C8(config-if)#exit
C8(config) #interface e0/2
C8(config-if)#ip address 192.168.17.1 255.255.255.0
C8(config-if)#no shut
C8(config-if)#exit
C8(config) #interface e0/3
C8(config-if)#ip address 192.168.16.1 255.255.255.0
C8(config-if)#no shut
C8(config-if)#exit

Configuración de OSPF
C8(config) #router OSPF 10
C8(config-router)#router-id 10.10.10.10

C8(config-router)#network 10.30.9.0
0.0.0.255 area 0
C8(config-router)#network 10.30.10.0
0.0.0.255 area 0
C8(config-router)#network 192.168.17.0
0.0.0.255 area 0
C8(config-router)#network 192.168.16.0
0.0.0.255 area 0
C8(config-router)#exit

Mikrotik 1
[admin@MikroTik] >ip address add
address=192.168.18.50/24 interface=ether6

Mikrotik 2
[admin@MikroTik] > ip address add
address=192.168.18.60/24 interface=ether6
Una vez asignadas las configuraciones realizamos el mismo procedimiento en el primer escenario asignando las direcciones Ip por medio del WinBox Utilizando el mismo Cloud-1.

SERVER

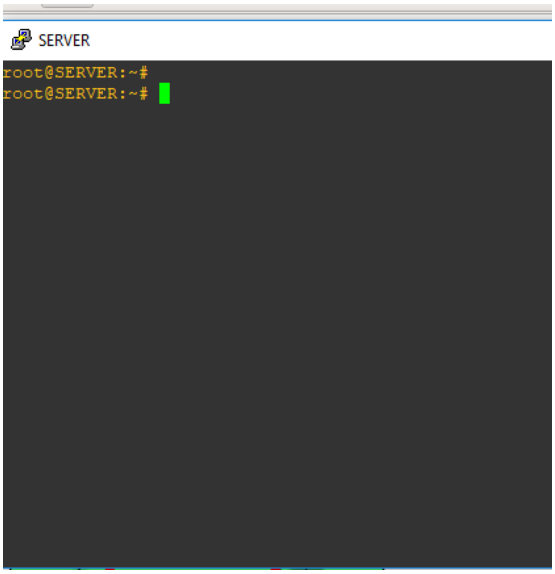

Figura 28-2. Consola de Configuración del SERVER
Realizado por: (Hidalgo Magaly. 2019)

En la consola de configuración añadimos la Dirección IP y el Gateway; con esto, podemos hacer Ping desde cualquier Router hacia el SERVER.
root@SERVER:~# ifconfig ether0
200.10.10.10 netmask 255.255.255.0
Configuración de Rutas Estáticas

C8 con OSPF
C8(config) #router ospf 10
C8(config-router) # router-id 10.10.10.10
C8(config-router) # network 10.30.9.0
0.0.0.255 area 0
C8(config-router) # network 10.30.10.0
0.0.0.255 area 0
C8(config-router) # redistribute static subnets
C8(config-router) #exit

C7 con ISIS
C7config) #router isis
C7(config-router) #ip route 172.16.20.0
255.255.255.0 192.168.15.2
C7(config-router) #ip route 172.16.10.0
255.255.255.0 192.168.14.2
C7(config-router) #no shut
C7(config-router) #redistribute static level_1
C7(config-router) #exit

C1 con OSPF
C8(config) #router ospf 10
C8(config-router) # router-id 1.1.1.1
C8(config-router) # network 10.10.1.0
0.0.0.255 area 0
C8(config-router) # network 10.10.4.0
0.0.0.255 area 0
C8(config-router) # redistribute static subnets
C8(config-router) #exit

Configuración de iBGP y BGP

BGP nos permite intercambiar información entre diferentes sistemas autónomos.

Cisco 8
C8(config) #router bgp 400
C8(config-router) # bgp log-neighbor-changes
C8(config-router) # neighbor 8.8.8.8 remote-as 400
C8(config-router) # neighbor 8.8.8.8 update-source Loopback0
C8(config-router) #exit
C8#wr
Brocade 1
vyatta @vyatta # set protocols bgp 400 parameters router-id 8.8.8.8
vyatta @vyatta # set protocols bgp neighbor 10.10.10.10 remote-as 400

vyatta @vyatta # set protocols bgp neighbor 10.10.10.10 update-source 8.8.8.8
vyatta @vyatta # set protocols bgp neighbor 10.10.10.10 nexthop-self
vyatta @vyatta # set protocols bgp neighbor 200.10.30.1 remote-as 500
vyatta @vyatta #commit

Cisco 8

C8(config) #router bgp 500
C8(config-router) # bgp router-id 192.168.0.4
C8(config-router) # bgp log-neighbor-changes
C8(config-router) # network 172.16.10.0 mask 255.255.255.0
C8(config-router) # network 172.16.20.0 mask 255.255.255.0
C8(config-router) # neighbor 192.168.0.2 remote-as 500
C8(config-router) # neighbor 192.168.0.2 update-source Loopback0
C8(config-router) # neighbor 192.168.0.2 next-hop-self
C8(config-router) # neighbor 192.168.0.3 remote-as 500
C8(config-router) # neighbor 192.168.0.3 update-source Loopback0
C8(config-router) # neighbor 192.168.0.5 remote-as 500
root@J6#set neighbor 192.168.0.1
root@J6#set neighbor 192.168.0.4
root@J6#set neighbor 192.168.0.5
root@J6#commit and-quit

Juniper 7
root@J6#set routing-options autonomous-system 500
root@J6#edit protocols bgp group ibgp
root@J6#set type internal
root@J6#set peer-as 500
root@J6#set neighbor 192.168.0.1
root@J6#set neighbor 192.168.0.4
root@J6#set neighbor 192.168.0.5
root@J6#commit and-quit

C8(config-router) # neighbor 192.168.0.5 update-source Loopback0
C8(config-router) # neighbor 192.168.0.5 next-hop-self
C8(config-router) # neighbor 200.10.30.2 remote-as 400
C8(config-router) #exit

Cisco 8
C8(config) #router bgp 500
C8(config-router) # bgp log-neighbor-changes
C8(config-router) # neighbor 192.168.0.2 remote-as 500
C8(config-router) # neighbor 192.168.0.2 update-source Loopback0
C8(config-router) # neighbor 192.168.0.3 remote-as 500
C8(config-router) # neighbor 192.168.0.3 update-source Loopback0
C8(config-router) # neighbor 192.168.0.4 remote-as 500
C8(config-router) # neighbor 192.168.0.4 update-source Loopback0
C8(config-router) # exit

Juniper 6
root@J6#set routing-options autonomous-system 500
root@J6#edit protocols bgp group ibgp
root@J6#set type internal
root@J6#set peer-as 500

ANEXO B

Instalación de GNS3 y VMware

https://sourceforge.net/projects/gns-3/