UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

Colegio de Ciencia y Tecnología

"EMULACIÓN DE LA CONECTIVIDAD Y GESTIÓN DE LAS REDES AVANZADAS DE ÁFRICA"

TESIS

Que para obtener el título de:

Licenciado en Ingeniería en Sistemas Electrónicos y de Telecomunicaciones

Presenta:

Luis Carlos Revilla Melo

Director:

M. en C. José Ignacio Castillo Velázquez

Ciudad de México, agosto de 2020

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

AGRADECIMIENTOS

Agradezco a mi Universidad por brindarme la oportunidad de formar parte de ella como Universitario, así también a mis Profesores que me apoyaron durante toda mi Formación Académica. Y en especial a mi Director de Tesis, el M. en C. José Ignacio Castillo Velázquez, quien se tomó el tiempo y espacio para guiarme durante todo este trayecto. A mis lectores les agradezco por tomarse el tiempo en leer y revisar la presente Tesis, así como sus apreciables correcciones para el mejoramiento de la misma. Después de años de esfuerzo, sacrificios, dedicación; desvelos, alegrías, tristezas y grandes satisfacciones; llegó el momento de mirar hacia atrás y ver el camino recorrido y poder decir: “Gracias a todos y por todo”.

DEDICATORIA

A mis Padres Hermilo e Irene

Por darme la vida, por su apoyo en todo momento, por creer en mí, por brindarme la oportunidad de estudiar y conseguir una Carrera Profesional a costa de sacrificios, por sus consejos, por sus valores, por la motivación constante que me han permitido ser una persona de bien. Y aunque ya no estés físicamente Mamá, te llevaré siempre en mi corazón y sé que en donde te encuentres te sentirás orgullosa de mi por el logro que eh obtenido.

A mis Hermanos Jorge, Julio Cesar, Israel, Erick y Oscar Alberto

Por sus consejos, apoyo, ánimo y ser el ejemplo en mi vida de perseverancia y constancia siempre.

A mí Esposa Alma Delia Hernández Bruno

Por su gran amor y cariño, por compartir su tiempo conmigo, por haber estado en los momentos difíciles, por apoyarme y darme ánimos cuando más lo necesitaba; y darme la dicha de ser padre de un hermoso hijo; mi pequeño primogénito Carlos Alexander, quien es mi motivo y mi impulso de superación personal y profesional que me hace ser mejor cada día.

Índice

Resumen

La red avanzada de NREN (*National Research and Education Networks*), desarrolla la nueva era de redes de computadoras que brindan soporte a la información generada por los proyectos de investigación, en las universidades y centros de investigación. El término “redes avanzadas”, se caracteriza por poseer enlaces de alta capacidad que soportan los 100 Gbps, utilizando equipos de alta tecnología y, uso de nuevos protocolos que permiten ejecutar aplicaciones en tiempo real [10].

Por lo que ahora nos damos a la tarea de conocer un poco el continente de África, estableció un registro de Internet en Malasia (1997), dónde se llevó a cabo un comité directivo para trabajar en la estructura y el plan de negocios de AFRINIC (*African Network Information Center).* En abril de 2005, ICANN (*Internet Corporation for Assigned Names and Numbers*) acreditó a AFRINIC como el quinto registro regional de Internet.

La misión de AFRINIC es proporcionar una distribución profesional y eficiente de los recursos numéricos de Internet y fortalecer el autogobierno de África.

Con la finalidad de conocer y entender el funcionamiento del **backbone** AFRICACONNECT2, se realizó la emulación de la conectividad y de la gestión de dicho **backbone**, en su versión actualizada 2019, utilizando las herramientas de emulación en GNS3, se utilizaron 29 **routers** c7200 de Cisco que conforman el **backbone**. Se configuró a cada uno de ellos con el protocolo de enrutamiento OSPFv3 y el protocolo de gestión SNMPv3.

Para desarrollar la emulación de la conectividad y de la gestión, se utilizó un equipo laptop con un procesador: Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz. El consumo de recursos en la emulación fue del 99% del procesador y 94% (12 GB) de memoria RAM. El tiempo establecido desde la ejecución de GNS3 hasta tener todo el **backbone** y sus 29 **routers** habilitados fue de 40 minutos. Como productos además de la tesis de licenciatura se obtuvo un artículo como publicación internacional indexada a Scopus.

Abstract

The advanced network of NREN (*National Research and Education Networks*), develops the new era of computer networks that support the information generated by research projects, in universities and research centers. The term “advanced networks” is characterized by having high capacity links that support 100 Gbps, using high-tech equipment and using new protocols that allow applications to be executed in real time [10].

So now we have the task of knowing a little about the continent of Africa, established an Internet registry in Malaysia (1997), where a steering committee was carried out to work on the structure and business plan of AFRINIC (*African Network Information Center*). In April 2005, ICANN (*Internet Corporation for Assigned Names and Numbers*) accredited AFRINIC as the fifth regional Internet registry.

The mission of AFRINIC is to provide a professional and efficient distribution of Internet numerical resources and strengthen the self-government of Africa. In order to know and understand the operation of the AFRICACONNECT2 backbone, the connectivity and management emulation of said backbone was performed, in its updated 2019 version, using the emulation tools in GNS3, 29 Cisco c7200 routers were used that make up the backbone. Each of them was configured with the OSPFv3 routing protocol and the SNMPv3 management protocol.

To develop the emulation of connectivity and management, a laptop computer with a processor was used: Intel (R) Core (TM) i7-5500U CPU @ 2.40GHz. The resource consumption in the emulation was 99% of the processor and 94% (12 GB) of RAM. The time established from the execution of GNS3 to have all the backbone and its 29 routers enabled was 40 minutes. Aditionally to this bacheluor thesis an international conference paper indexed at Scopus was accepted to be published.

Contexto del proyecto ADVNETLAB y este trabajo de tesis

El ADVNETLAB (*Advanced Networking Laboratory*) en la UACM fue fundado en 2013, una vez que hubo interés por parte de los estudiantes de ISET acerca del tema de las redes avanzadas. Desde entonces se ha desarrollado una metodología ADVNETLAB con la que se dirigen las tesis y otros proyectos, Desde 2015 a la fecha se han titulado 13 estudiantes de licenciatura bajo la metodología ADVNETLAB; desde nuestro laboratorio ADVNETLAB, hemos producido 11 tesis con 12 estudiantes de telecomunicaciones, 16 articulos en revistas y procedings de IEEE indexados en SCOPUS con 11 de aquellos 13 quienes trabajaron bajo la metodología ADVNETLAB. A estos productos se adicionan otros 6 artículos indexados para una aportación total de 23 articulos SCOPUS a favor de la UACM. También se desarrolló UTILCON, un sistema de gestión de congresos o seminarios u otro tipo de eventos académicos, registrado ante el Instituto Nacional de Derechos de Autor, ya que en México los sistemas de software no son patentables como sí lo son en otros países.

En esta ocasión se presenta para 2020 Luis Carlos Revilla (ANL13) con el trabajo correspondiente al estudio vía emulación del backbone de la red avanzada africana bajo IPv6 en su topología más actualizada, para el cual se ponen a prueba su conectividad y gestión; tal y como sucede en los centros de operaciones de red de las compañías provedoras de internet. Nunca en ADVNETLAB se había abordado. Luis es uno de los primeros de ISET en presentar examen profesional a distancia en la UACM como adecuación ante la pandemia del COVID 19. Le expreso mis felicitaciones por su trabajo concluido.

M. en C. José Ignacio Castillo Velázquez

Director de tesis - 30 de julio de 2020

CAPÍTULO 1

Introducción

La Internet o también conocida como la red de datos más grande del mundo es sin duda una verdadera revolución en la sociedad moderna. Ya que ha tenido un crecimiento exponencial hasta nuestros días, marcando un gran cambio en las actividades económicas, sociales y culturales. La Internet permite la comunicación a millones de personas a través del e-mail, mensajes, redes sociales o video llamadas, desde cualquier parte del mundo, la cual es parte fundamental de la investigación, educación y avances tecnológicos. Sin embargo, es importante conocer sus inicios y hacia dónde se dirige.

1.1 Los primeros años de las redes de datos y su consolidación

Desde la aparición de los primeros circuitos electrónicos, pasaron por la invención de los relés, bulbos y transistores hasta los circuitos integrados, se había trabajado con la tecnología de conmutación de circuitos; ésta es la que se usaba en las redes telefónicas analógicas y digitales. En 1961 Leonard Kleinrock, en EEUU, modificó radicalmente la idea de los métodos de conmutación de circuitos a la conmutación de mensajes (*message switching*) con su artículo: *Information flow in large communications nets.*

En 1964 Paul Baran, en EEUU, construyó la primera red de comunicaciones distribuida, la cual se podía conectar con varios nodos. Donald Watts Davies, en el Reino Unido, también desarrolló un sistema como Baran, acuñó el término “paquete” y “conmutación de paquetes”, para describir los “bloques de datos” y el protocolo del manejo de mensajes en los dos sistemas indicados. Ambas ideas se incorporaron en la ARPANET (*Advanced Research Projects Agency NETwork*).

En 1966 ARPA (*Advanced Research Projects Agency*) usó conmutación de paquetes y los primeros resultados concretos se obtuvieron en 1969, una vez que se tenían los primeros IMP (*Interfaz Message Processor*), con computadoras de tercera generación se conectaron 2 computadoras: la SDS Sigma 7 desde el nodo 1 en UCLA (*University of California-Los Angeles*), hacia la SDS 940 en el nodo 2 en SRI (*Standford Research Institute en California*) en septiembre de 1969. Luego se les unió la IBM 360/75 en el nodo 3 en UCSB (*University of California-Santa Barbara*) en octubre y finalmente se integró la DEC-PDP-10 como nodo 4 en la Universidad de Utah en octubre de 1969. Con esto nació la primera MAN (*Metropolitan Área Network*), la cual fue construida por ARPANET, la red precursora de lo que hoy conocemos como la Internet. En la figura 1 se muestra la disposición física de ARPANET [1, 2].

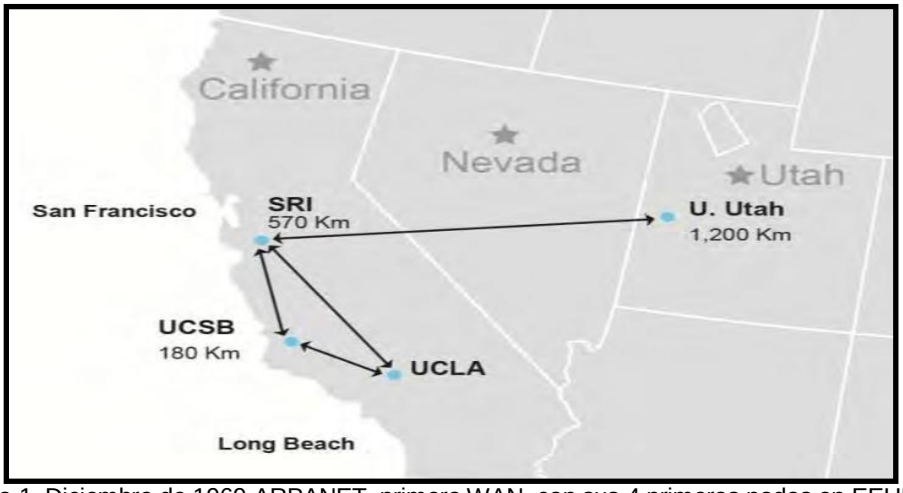


Figura 1. Diciembre de 1969 ARPANET, primera WAN, con sus 4 primeros nodos en EEUU [3].

En 1969 se creó el NCP (*Network Control Protocol*) protocolo que proveía las bases para la aplicación de la transferencia de archivos al comunicar los nodos de ARPANET, mismo que estuvo funcionando desde 1969 hasta 1973, cuando se le sustituyó por TCP (*Transmission Control Protocol*). En Septiembre de 1969 se definió el protocolo TELNET, el cual formaba parte del NCP como un subsistema definido como el Network Subsystem for Time Sharing Host. Un host se definió como cualquier computadora conectada a una red; y para emplear una user-host (terminal-host) remota como si fuera una terminal en un server –host (servidor), con ello se definió el modelo cliente servidor [4].

En diciembre de 1970 ARPANET contaba con 13 nodos y ya comunicaba a las dos costas de EEUU. En 1971 ARPANET tenía 18 nodos y no se dieron cambios radicales.

En 1972 nació el FTP (*File Transfer Protocol*) protocolo para la transferencia de archivos entre computadoras conectadas remotamente, y el e-mail para la transmisión de mensajes de correo electrónico, ambos se convirtieron en los más populares [5].

El éxito de ARPANET fue tal que se planearon importantes cambios; la Sección de Ciencias de la Computación de la NSF (*National Science Fundation*) creó su propia red, la CSNET (*Computer Science Network*) a semejanza de ARPANET. La CSNET fue un proyecto de 1981 a 1985, que comunicaba centros de computación en EEUU, así como universidades, centros de gobierno e industriales y centros de investigación de Europa y Asia. También en 1981 la RFC 801 planteó la necesidad de realizar el cambio de NCP a TCP (TCP /IP (*Internet Protocol*)), el cual se realizó el 1 de enero de 1983.

Para 1984 ya había tal cantidad de servidores que se inventó el DNS (*Domine Name Systems*) para poder organizar a tales servidores en dominios y hacer la resolución de direcciones IP, para hacerlos más fáciles de acceder. Por su parte la NSF quiso replicar el éxito de la CSNET dentro de todas sus áreas, por lo que la NSF decidió crear la red NSFNET. Mientras tanto ISO (*International Organization for Standardization*) liberó su primer estándar, ISO/OSI (*Open Systems Interconnection*) 7498 como un modelo de referencia básico para sistemas abiertos de redes de datos [6].

Para 1988 mientras ARPANET contaba con sus 45 nodos, la NSFNET contaba con 13 nodos y su backbone se comunicaba vía un enlace para voz y datos que se componía de 24 canales DS0 (*Digital Signal*). Cada DS0 tiene un ancho de banda de 64Kbps, lo que da por resultado un enlace de 1.5 Mbps llamado DS1 o T1 (T1-Carrier) o E1 fuera de EEUU. Toda la red consistía en una colección de AS (*Autonomous System*) de modo que cada AS se administra vía una única entidad que tiene un determinado control técnico y administrativo de la infraestructura, en ese entonces todo EEUU conformaba un único AS. En este punto ya había gran claridad respecto de interconectar infraestructura de la red de datos dentro de un mismo AS y otro tema era interconectar 2 o más AS. De este modo, en junio del mismo año, se liberó el estándar del RIP (*Routing Information Protocol*), un protocolo que trabaja dentro de un mismo AS, es decir, un protocolo de tipo IGP (*Interior Gateway Protocol*). RIP permitía el intercambio de información de ruteo entre gateways y host, para lo que empleaba algoritmos de tipo “vector-distancia” como el Bellman-Ford; RIP se empleaba para interconectar redes de “tamaño moderado” que usaran tecnologías “razonablemente homogéneas”; RIP se genera con base en el programa **routed** que se había implementado en el sistema operativo UNIX, distribución BSD (*Berkeley Software Distribution*), para comunicar gateways entre sí desde 1970. Por otro lado para interconectar un AS con otro AS se empleaba el protocolo EGP (*Exterior Gateway Protocol*) entre otros, para ese mismo año ya se les llamaba “protocolos de enrutamiento inter-AS”. En la figura 2 se muestra el Backbone de la NSFNET de 1988 [7].

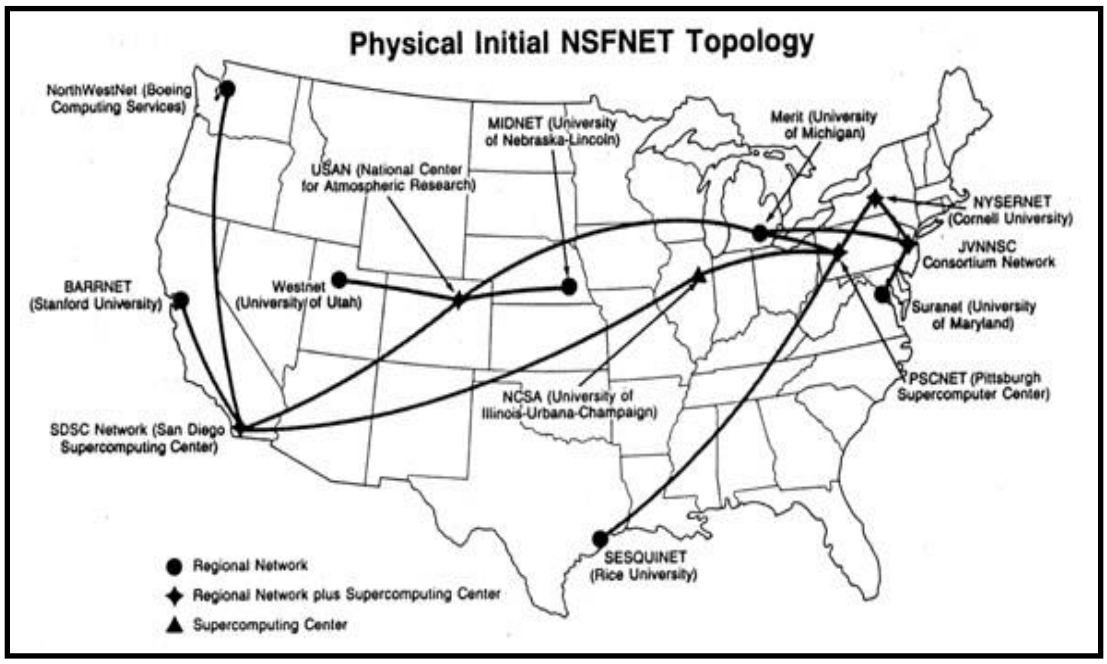


Figura 2. Backbone de la NSFNET de 1988 [8].

Para 1995 el crecimiento de Internet era exponencial, ya contaba con más de 100,000 redes tanto públicas como privadas tan solo dentro de EEUU, de modo que para el 30 de abril de 1995 la NSFNET queda desarticulada para desaparecer y dejar su lugar a la "Internet Comercial" que todos conocemos actualmente, de modo que los usuarios se conectarían con su ISP (*Internet Service Provider*) y él los conectaría a Internet, de modo que el gobierno de EEUU puso fin al control de la infraestructura de su red abriendo la puerta al sector privado, mientras que la Internet tenía para julio de 1995 un total de 23,500 sitios web [9]. En la figura 3 se muestra el resumen de la línea del tiempo para las grandes redes hasta la llegada de "Internet Comercial".

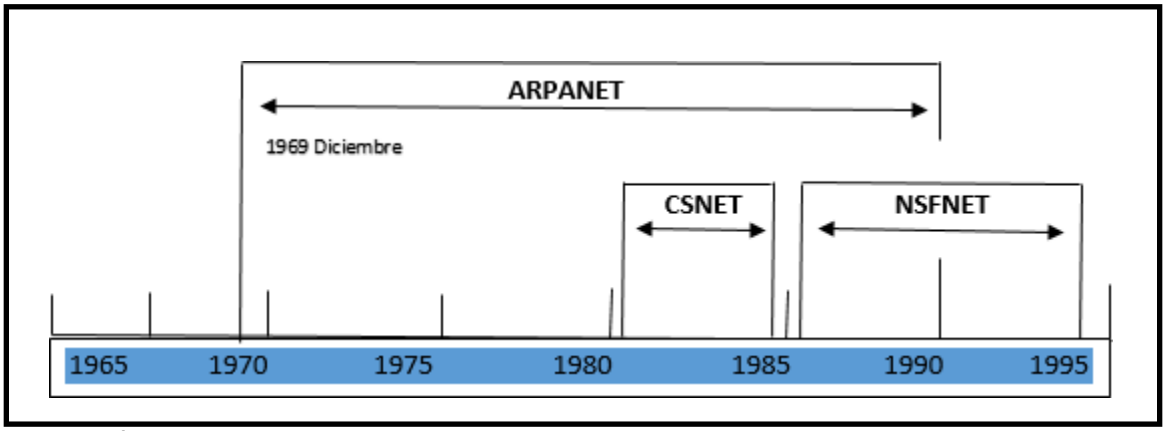


Figura 3. Línea de tiempo de 25 años para las redes grandes {WAN[MAN(LAN)]} previas a la Internet (Propia con base en referencia [9]).

1.2 Redes Avanzadas

(GÉANT, NREN, CANARIE, CUDI, AFRICACONNECT2)

GÉANT es la red de datos paneuropea que interconecta a las organizaciones nacionales de redes de investigación y educación de Europa con un alto ancho de banda y alta velocidad [10].

Las NREN (*National Research and Education Networks*), desarrollan la nueva era de redes de computadoras que brindan soporte a la información generada por los proyectos de investigación. El término “redes avanzadas”, es asignado a la infraestructura utilizada para proveer conexión a universidades e instituciones, dedicadas a la investigación científica. La infraestructura se caracteriza por poseer enlaces de alta capacidad que soportan los 100 Gbps (*Gigabits por segundo*), utilizando equipos de alta tecnología y, uso de nuevos protocolos que permiten ejecutar aplicaciones en tiempo real [10]. Así también CANARIE es el socio federal en la Red Nacional de Investigación y Educación de Canadá, que proporciona conectividad interprovincial e internacional [11].

En la consolidación de ARPANET en 1990 y NSFNET en 1995, surgió un nuevo intento para desarrollar una Internet que permanezca dentro de universidades y centros de educación o investigación, lo que se llamaría la Internet 2, la cual nació en 1996. En México, Internet 2 está coordinado por el CUDI [Consorcio Universitario para el Desarrollo de Internet 2]. El CUDI nació el 8 de abril de 1999, el cual su objetivo es: Promover y coordinar el desarrollo y difusión de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo de México, enfocadas al desarrollo científico y educativo de la sociedad mexicana [12].

Por lo que a continuación, nos damos a la tarea de conocer un poco sobre la Red Avanzada llamada AfricaConnect2, que se encuentra localizada en el continente africano.

1.3 Redes avanzadas en África

El proyecto AfricaConnect tuvo un presupuesto total de 14.75 millones de euros para un periodo de cuatro años (2011-2015), con un 80% de los fondos aportados por el EDF (*European Development Fund*) tras un acuerdo entre la secretaría África Caribe-Islas del Pacífico (ACP) y la Comisión Europea (CE), cuya finalidad principal es fomentar el desarrollo de las NREN`s en otros países y dar continuidad al siguiente proyecto AfricaConnect2 [13].

AfricaConnect bajo la perspectiva de una red de Internet de alta capacidad nivel mundial, tiene como objetivo beneficiar a investigadores, educadores y estudiantes de África Meridional y Oriental para participar en proyectos de Investigación y Desarrollo con su contraparte en Europa y otros países en el mundo.

AfricaConnect2 (2015 - 2019) y su sucesor de AfricaConnect (2011-2015), es un proyecto de redes de investigación y educación que tiene como objetivo conectar a los socios de la red nacional de investigación y educación participantes a través de la red GÉANT África.

AfricaConnect2 es una red cofinanciada por la Unión Europea, la cual procede de los resultados del proyecto AfricaConnect que contribuyó a la creación de UbuntuNet, la red troncal regional que interconecta las NREN y las conecta con otras redes regionales, como la red paneuropea GÉANT.

AfricaConnect2 se basa en los logros del proyecto EUMEDCONNECT desde el 2004, la cual es una red de investigación y educación de la región mediterránea y vinculada con GÉANT.

El proyecto AfricaConnect2 es una iniciativa entre la Comisión Europea, GÉANT y tres organizaciones regionales o redes regionales que apoyan la red local de investigación y educación en África, las cuales están agrupadas en “clusters” [13]:

A. Alianza UbuntuNet (Cluster 1)

B. WACREN (Cluster 2)

C. ASREN (Cluster 3)

Las redes ASREN y WACREN son administradas, financiadas, y operadas por la organización GÉANT, y Alianza UbuntuNet, gestionada por UbuntuNet [14].

1.3.1 Alianza UbuntuNet

Alianza UbuntuNet es una asociación regional de NREN en África Oriental y Meridional, inició en el 2005 con 5 redes, las cuales fueron: MAREN (Malawi), MoRENet (Mozambique), KENET (Kenia), RwEdNet (Ruanda) y TENET (Sudáfrica). El objetivo principal de Alianza UbuntuNet, es asegurar la conectividad internacional a través de GÉANT con una alta velocidad y accesible para la comunidad africana de investigación y educación, a un ancho de banda en Gbps. De igual manera, compartir recursos, acceso y uso de las TIC's entre las NREN africanas [15, 16]. En la tabla 1, se muestran los 15 socios de UbuntuNet Alliance:

NREN	Nombre	País/Status	Conectividad
BERNET	Red de Investigación y Educación de Burundi	Burundi/operacional	*Espera a conexión/local
eb@le	Eb @ le – RDC	República Democrática del Congo/operacional	*Espera a conexión/local www.ubuntunet.net/ebale
EthERNet	Red Etíope de Educación e Investigación.	Etiopía/operacional	*Espera a conexión/local www .ethernet.edu.et
Kenet	Red de Educación de Kenia www.kenet.or.ke	Kenia/operacional	1 Nairobi<>London (1.24Gbps) 2 Nairobi<Amsterdam (2.5Gbps, 620Mbps) 1 Nairobi<>Fujira (620Mbps) 1 Nairobi<>J`Burg (150Mbps)
IRENALA	IRENALA – Madagascar	Madagascar/ Operacional	*Espera a conexión/local www.irenala.edu.mg
MAREN	Red de Investigación y Educación de Malawi	Malawi/operacional	*Espera a conexión/local www.maren.ac.mw
morenet	Red de Investigación y Educación de Mozambique	Maputo Mozambique/ Operacional	1 UbuntuNet Alliancea 1 London-UbuntuNet Alliance www.ubuntunet.net/morenet
Rwednet	Ruanda Red de Educación e Investigación.	Rwanda/no operacional	Sin dato alguno
SREN	Red Somalí de Investigación y Educación	Somalia/no operacional	**En espera a conexión www.somaliren.org
SudREN	Red de Investigación y Educación de Sudán	Sudán/operacional	**En espera a conexión Ubuntunet/local www.sudren.edu
TENET	Red de educación terciaria e investigación de Sudáfrica.	Sudáfrica/operacional	2 London-UbuntuNet (10Gbps) www.tenet.ac.za
TERNET	Red de Educación e Investigación de Tanzania.	Tanzania/operacional	1 London-UbuntuNet (155Mbps) www .ternet.or.tz
RENU	Red de Investigación y Educación para Uganda.	Uganda/operacional	1 London-Amsterdam hacia GEANT (1 Gbps) www.renu.ac. ug
XNet	Xnet Development Alliance Trust – Namibia	Namibia/operacional	*Espera a conexión/local www.ubuntunet.net/xnet
ZAMREN	Red de Investigación y Educación de Zambia.	Zambia/operacional	1 UbuntuNet Alliance (1 Gbps) www.zamren.zm

Tabla 1. UbuntuNet Alliance cubre las regiones del este y sur de África [16].

1.3.2 WACREN

WACREN (*West and Central African Research and Education Network*), es la Red Nacional de Investigación y Educación de África Occidental y Central que comenzó en 2006 con la participación de 10 países y la Asociación de Universidades Africanas.

Como objetivo WACREN es ser una red de clase mundial para la comunidad de Investigación y Educación de África Occidental y Central, y compartir recursos con la red GÉANT [17, 18].

Actualmente, los 10 miembros y socios que participan en WACREN, se muestran en la tabla 2:

NREN.	Nombre.	País/Status.	Conectividad.
	Red de Educación e Investigación de Benin (RerBenin)	Benin / no operacional	**En espera a conexión
	Red Interuniversitaria de Camerún (ICN)	Camerún / no operacional	**En espera a conexión www.minesup.gov.cm
	Gabón Red de Investigación y Educación (GabonREN)	Gabón / Operacional	*Espera a conexión/local www.enseignement-superieur.gouv.ga
	Red Académica y de Investigación de Ghana (GARNET)	Ghana / operacional	*Espera a conexión/local http://garnet.edu.gh
	Red de Telecomunicaciones de la Costa de Marfil para la Enseñanza y la Investigación (RITER)	Costa de Marfil / operacional	*Espera a conexión/local www.riter.ci
	Red Nacional de Educación e Investigación de Malí (MaliREN)	República de Malí / operacional	*Espera a conexión/local www.maliren.ml
	Níger Red Nacional de Investigación y Educación (NigerREN)	Níger / operacional	*Espera a conexión/local *Vecino Nigeria,NgREN cluster www.niger-ren.ne
	La Red Nigeriana de Investigación y Educación (NgREN)	Nigeria / operacional	*Espera a conexión/local ngren.edu.ng
	Red para la Educación Superior y la Investigación de Senegal (snRER)	Senegal / operacional	*Espera a conexión/local *Potencial enlace a Paris http: // snrer .edu.sn /
	Red de Educación e Investigación de Togo (Togo-RER)	Lomé Togo / operacional	*Espera a conexión/local www.togorer.tg

Tabla 2. WACREN de África Occidental y Central [18].

1.3.3 ASREN

La Red de Investigación y Educación de los Estados Árabes (ASREN – *Arab States Research and Education Network*) fue lanzada en 2010 bajo los auspicios de la Liga de los Estados Árabes y de la Alianza Global de las Naciones Unidas para las TIC y el Desarrollo (GAID), para promover la conectividad en la región norte de África, para servir a una población de más de 250 millones de personas.

La red ASREN está vinculada con la red GÉANT y EUMEDCONNECT3, la cual es una red de investigación y educación de 7 países del sur del Mediterráneo (Argelia, Egipto, Jordania, Marruecos, Palestina, Siria y Túnez), y conectada con Internet2 en los Estados Unidos y con otras redes regionales del mundo [19, 20].

En la tabla 3, se muestra los 4 países miembros participantes de ASREN:

NREN	Nombre	País/Status	Conectividad
	Red Argelia de investigación(ARN)	Argelia/operacional	1 GEANT (2.5Gbps) 777Mbps área local www.arn.dz
	Centro de Computación Al Khwarizmi (CCK)	Túnez/operacional	1 GEANT (20-100Gbps) 1 AfricaConnect2(1Gbps) www. cck.rnu.tn
	Red de universidades egipcias (EUN)	Egipto/operacional	1 Internet2 (1 Gbps) *1Gbps área local www.eun.eg
	Marruecos Académico y de investigación de red de área amplia (MARWAN)	Marruecos/operacional	*Espera a conexión www.cnrst.ma

Tabla 3. NREN`s de África del Norte [21]

1.3.4 AfricaConnect2

La red paneuropea GÉANT se conecta a la red UbuntuNet (UbuntuNet Alliance) a través de los routers UbuntuNet London y Ámsterdam que proporcionan un enlace de punto a punto de 10 Gbps para el tráfico IP.

De los cuatro países de África del Norte, la conectividad internacional de Argelia se proporciona a través de la red EUMEDCONNECT3, mientras que Egipto se interconecta directamente con GÉANT vía Ámsterdam. En la figura 7, se muestra el mapa de las NREN's en África a partir del 1 de julio de 2015 y válida hasta 2019 [21].

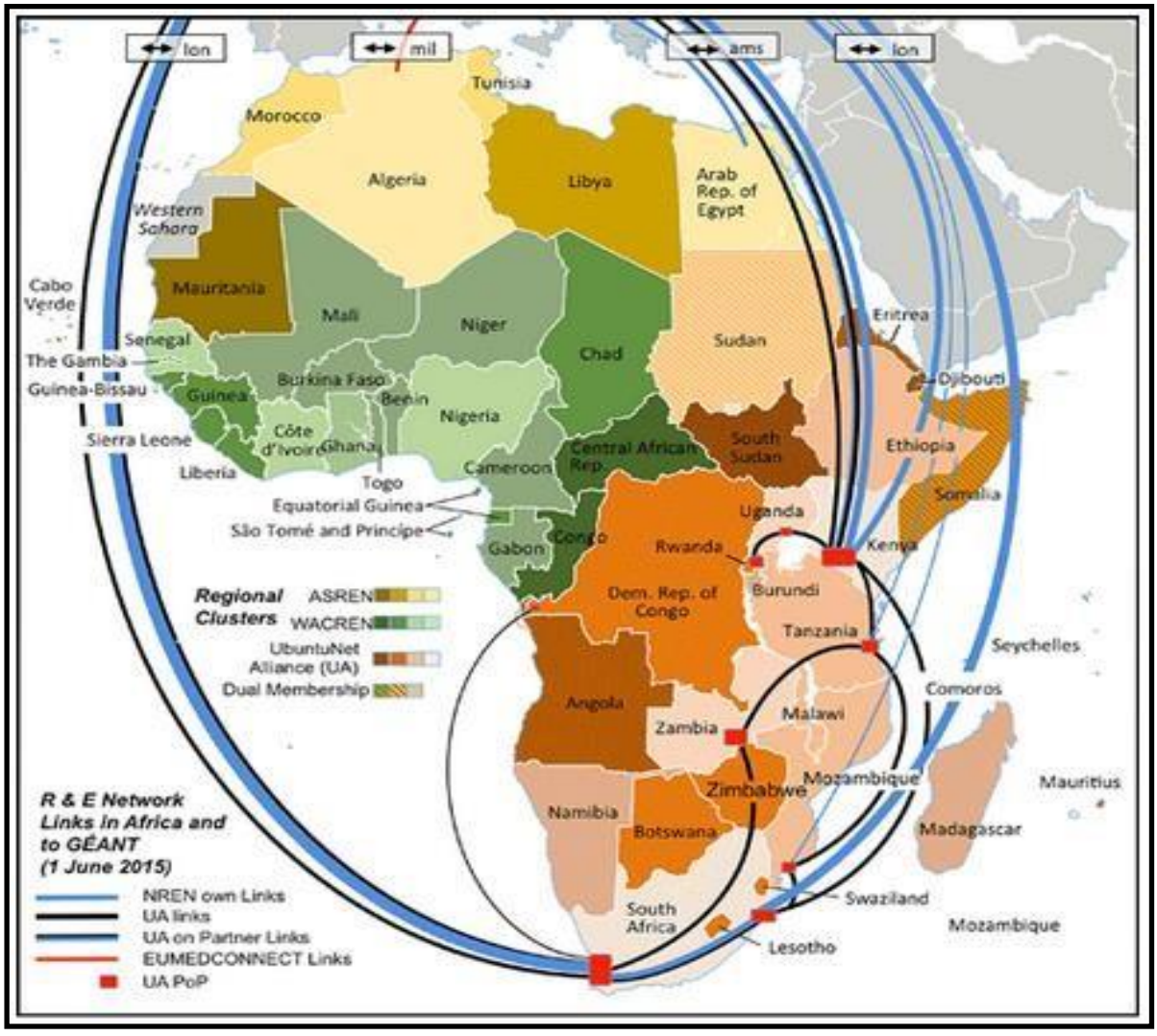


Figura 7. Mapa de conectividad de AfricaConnect2, válida hasta 2019 [22].

Esta topología se usará para el desarrollo de la presente tesis, ya que se eligió por comodidad y para el estudio de la conectividad y gestión de las redes avanzadas en África.

1.4 Objetivo y Justificación

1.4.1 Objetivos

- **General**: Desarrollar las habilidades que me permitan desempeñarme como un administrador de redes WAN, a través del estudio de la gestión de las redes avanzadas en África, realizando la emulación de la misma.
- Desarrollar las habilidades para manejar al emulador GNS3
- Manejar adecuadamente los protocolos de enrutamiento y gestión usados en redes avanzadas.
- Conocer las capacidades y limitaciones del emulador GNS3

1.4.2 Justificación

Se realiza la emulación del funcionamiento de la red avanzada del continente africano, para estudiar la infraestructura de las redes avanzadas, considerando los equipos de backbone, protocolos de enrutamiento y gestión, y las herramientas necesarias y adecuadas para realizar una adecuada administración de redes de alto rendimiento.

Este tipo de redes es muy importante ya que dan soporte a proyectos de investigación y educación regionales o mundiales en áreas como la medicina, espacio, educación, física de partículas, astronomía, etc.

1.4.3 Trabajos previos realizados en Advnetlab, que se han publicado desde el 2016-2019

1. Routing algorithms Applied to an advanced academic network know as CUDI, 2016 [23]
2. Emulation for CLARA's operation, the advanced network for Latin America, 2016 [24]
3. Emulation of backbone's connectivity and management for the advanced network in Latin America: 2016's topology [25]
4. Emulation of the connectivity of backbone and management for the layer 3 service of INTERNET2: 2016 topology [26]
5. IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network, 2018 [27]
6. An Approach to Management Assessment for GEANT Backbone Using GNS3 for SNMPv3, 2018 [28]
7. Use of GNS3 Cloud Environment for Network Management Emulation when Comparing SNMP vs Syslog Applied Over an Advanced Network, 2019 [29]
8. Management Emulation for Advanced Networks Interconection in all America: 2019 topology [30]

CAPÍTULO 2

Protocolos.

En este capítulo se aborda un determinado detalle del protocolo IPv6, el protocolo de enrutamiento OSPF y el protocolo de gestión SNMP, los cuales se usarán en el presente proyecto.

2.1 Internet Protocol, Versión 6 (IPv6)

IPv6: La versión 6 de IP (IPv6) es una nueva versión del Protocolo de Internet, diseñado como el sucesor de la versión 4 de IP (IPv4). Los cambios de IPv4 a IPv6 caen principalmente en las siguientes categorías [31, 32]:

- **Capacidades de direccionamiento expandidas:** IPv6 aumenta el tamaño de la dirección IP de 32 bits a 128 bits, para admitir más niveles de jerarquía de direccionamiento, un número mucho mayor de nodos direccionables y una configuración automática de direcciones más simple. La escalabilidad del enrutamiento de multicast se mejora al agregar un campo de "alcance" a las direcciones de multicast. Además se define un nuevo tipo de dirección llamada "dirección anycast".

- **Tipos de direcciones:**
  Dirección **unicast**: comunicación a un nodo específico con dirección única.
  Dirección **broadcast**: comunicación a todos los nodos de la red.
  Dirección **multicast**: comunicación a todos los nodos de un grupo que tienen la misma dirección de grupo.
  Dirección **anycast**: comunicación a un nodo de un grupo que tienen la misma dirección de grupo.

- **Simplificación del formato de encabezado:** Algunos campos de encabezado de IPv4 se han eliminado o se han hecho opcionales, para reducir el costo de procesamiento de casos comunes del manejo de paquetes y para limitar el costo de ancho de banda del encabezado de IPv6.

- **Soporte mejorado para extensiones y opciones:** Los cambios en la forma en que se codifican las opciones del encabezado IP permiten un reenvío más eficiente, límites menos estrictos en la duración de las opciones y una mayor flexibilidad para introducir nuevas opciones en el futuro.

- **Capacidad de etiquetado de flujo:** Se agrega una nueva capacidad para habilitar el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para los cuales el remitente solicita un manejo especial, como la calidad no predeterminada de servicio o servicio "en tiempo real".

- **Capacidades de autenticación y privacidad:** Las extensiones para admitir la autenticación, la integridad de los datos y la confidencialidad de los datos (opcional) se especifican para IPv6.

A.- Formato de encabezado de IPv6

En la figura 8 se muestra el formato de encabezado IPv6

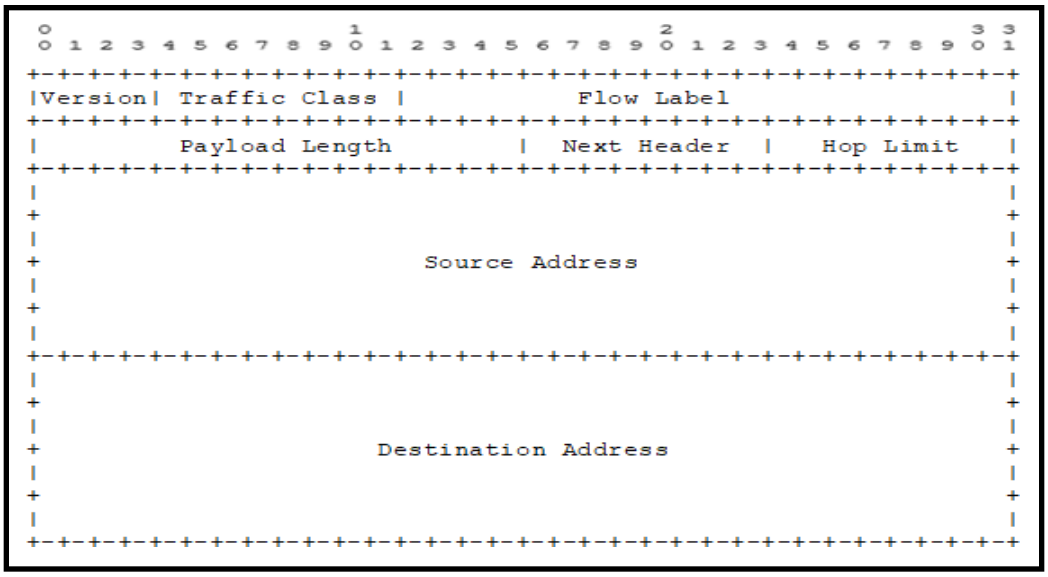


Figura 8. Formato de encabezado IPv6 [31].

Versión: Número de versión del protocolo de Internet de 4 bits.

Clase de tráfico: Campo de clase de tráfico de 8 bits.

Etiqueta de flujo: Etiqueta de flujo de 20 bits.

Longitud de carga útil: Entero sin signo de 16 bits. Longitud de carga útil de IPv6, es decir, el resto del paquete que sigue a este encabezado de IPv6, en octetos. (Tenga en cuenta que cualquier encabezado de extensiones se considera parte de la carga útil, es decir, se incluye en el recuento de longitudes.)

Siguiente encabezado: Selector de 8 bits. Identifica el tipo de encabezado que sigue inmediatamente el encabezado de IPv6. Utiliza los mismos valores que el campo Protocolo IPv4.

Límite de salto: Entero sin signo de 8 bits. Disminuido en 1 por cada nodo que reenvía el paquete. El paquete se descarta si el límite de salto se reduce a cero.

Dirección de la fuente: Dirección de 128 bits del originador del paquete.

Dirección de destino: Dirección de 128 bits del destinatario deseado del paquete (posiblemente no sea el destinatario final, si hay un encabezado de enrutamiento). [31]

B.- Cabeceras de extensión IPv6

En IPv6, la información opcional de la capa de Internet se codifica en encabezados separados que se pueden colocar entre el encabezado de IPv6 y el encabezado de la capa superior en un paquete. Hay un pequeño número de dichos encabezados de extensión, cada uno identificado por un valor distinto de siguiente encabezado. Como se ilustra en los siguientes ejemplos, un paquete IPv6 puede llevar cero, uno o más encabezados de extensión, cada uno identificado por el campo siguiente encabezado del encabezado anterior. [31]

En la figura 9 se muestran ejemplos de encabezados:

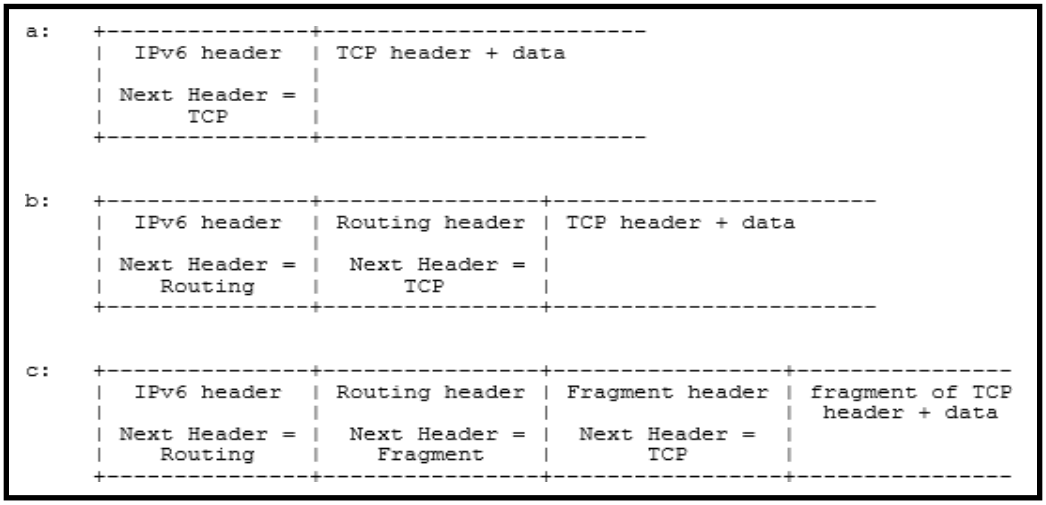


Figura 9. Encabezados de IPv6 [31].

Con una excepción, los encabezados de extensión no son examinados ni procesados por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete llega al nodo (o cada uno de los conjuntos de nodos, en el caso de multidifusión) identificado en el campo **Dirección de destino** del Encabezado IPv6. Ahí, la demultiplexación normal en el campo **Siguiente encabezado** del encabezado IPv6 invoca al módulo para procesar el primer encabezado de extensión, o el encabezado de la capa superior si no hay un encabezado de extensión presente. Por lo tanto, los encabezados de extensión deben procesarse estrictamente en el orden en que aparecen en el paquete; un receptor no puede, por ejemplo, escanear un paquete buscando un tipo particular de encabezado de extensión y procesar ese encabezado antes de procesar todos los anteriores [31].

La excepción mencionada en el párrafo anterior, es el salto por encabezado de opciones de salto, que lleva información que debe ser examinada y procesada por cada nodo a lo largo de la ruta de entrega de un paquete, incluyendo los nodos de origen y destino. El encabezado Opciones de salto por salto, cuando esté presente, debe seguir inmediatamente el encabezado de IPv6. Su presencia se indica mediante el valor cero en el campo: **Siguiente encabezado**, del encabezado IPv6 [31].

Si, como resultado del procesamiento de un encabezado, se requiere un nodo para continuar al siguiente encabezado, pero el valor del siguiente encabezado en el encabezado actual no es reconocido por el nodo, debe descartar el paquete y enviar un parámetro de ICMP mensaje de problema a la fuente del paquete, con un valor de Código ICMP de 1 (*tipo de encabezado siguiente no reconocido*) y el campo del puntero de ICMP que contiene el desplazamiento del valor no reconocido dentro del paquete original. Se debe realizar la misma acción si un nodo encuentra un valor de **Siguiente encabezado**, de cero en cualquier encabezado que no sea un encabezado de IPv6 [31].

Cada encabezado de extensión es un múltiplo entero de 8 octetos de longitud, con el fin de mantener la alineación de 8 octetos para los encabezados posteriores. Los campos de varios octetos dentro de cada encabezado de extensión se alinean en sus límites naturales, es decir, los campos de ancho *n* octetos se colocan en un múltiplo entero de *n* octetos desde el inicio del encabezado, para n=1, 2, 4 u 8 [31].

Una implementación completa de IPv6 incluye la implementación de los siguientes encabezados de extensión:

- Hop-by-Hop Options
- Routing (Type 0)
- Fragment
- Destination Options
- Authentication
- Encapsulating Security Payload

C.- Orden del encabezado de extensión

Cuando se usa más de un encabezado de extensión en el mismo paquete, se recomienda que esos encabezados aparezcan en el siguiente orden:

- IPv6 header
- Hop-by-Hop Option header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Playload header
- Destination Options header
- Upper-layer header

D: Representación de texto de direcciones IPv6

Hay tres formas convencionales para representar direcciones IPv6 como cadenas de texto:

- La forma preferida es x:x:x:x:x:x:x:x, donde las **x** son los valores hexadecimales de las ocho partes de 16 bits de la dirección [32].

Ejemplos: **FEDC:BA98:7654:3210:FEDC:BA98:7654:3210**

1080:0:0:0:8:800:200C:417ª

Tenga en cuenta que no es necesario escribir los ceros iniciales en un campo individual, pero debe haber al menos un número en cada campo.

- Debido a algunos métodos de asignación de ciertos estilos de IPv6 direcciones, será común que las direcciones contengan cadenas largas de cero bits. Para facilitar la escritura de direcciones que contengan cero bits, hay disponible una sintaxis especial para comprimir los ceros. El uso de "::" indica varios grupos de 16 bits de ceros. El "::" solo puede aparecer una vez en una dirección. El "::" también se puede usar para comprimir los ceros iniciales y / o finales en una dirección [32].

Por ejemplo, las siguientes direcciones:

1080:0:0:0:8:800:200C:417A	unicast
FF01:0:0:0:0:0:0:101	multicast
0:0:0:0:0:0:0:1	loopback
0:0:0:0:0:0:0:0	unspecified

Se puede representar como:

1080::8:800:200C:417A	unicast
FF01::101	multicast
::1	loopback
::	unspecified

- Una forma alternativa que a veces es más conveniente cuando se trata de un entorno mixto de nodos IPv4 e Pv6 es: x:x:x:x:x:x:dddd, donde las *x* son los valores hexadecimales de los seis partes de bits de la dirección, y las *d* son los valores decimales de las cuatro partes de 8 bits de orden inferior de la Dirección. (representación estándar de IPv4) [32].

Ejemplos:

0:0:0:0:0:0:13.1.68.3 **::13.1.68.3**

O en forma comprimida:

0:0:0:0:0:FFFF:129.144.52.38 **::FFFF:129.144.52.38**

2.2 Protocolos de enrutamiento RIP:

El enrutamiento dentro de las redes de datos es de suma importancia ya que los routers son los encargados de transferir paquetes de una red origen-destino. Un router es conocido como enrutador o encaminador de paquetes, tal que el router desempeña la función de interconectar dos o más redes y elige el mejor de los caminos o rutas entre ellas. Existen dos tipos de enrutamientos:

- (*Interior Gateway Protocol*): El protocolo de enlace interno fue diseñado para uso dentro de un sistema autónomo (AS), como por ejemplo: **RIPv1**, **RIPv2**, **RIPng**, **OSPFv1**, **OSPFv2** y **OSPFv3**.
- (*Exterior Gateway Protocol*): El protocolo de enlace externo fue diseñado para su uso entre múltiples sistemas autónomos (AS), por ejemplo: **BGP** (*Border Gateway Protocol*).

2.2.1 RIPv1

El RIP (*Routing Information Protocol*) es un protocolo de puerta de enlace interna o IGP (*Interior Gateway Protocol*) utilizado por los routers, también es conocido como un protocolo de enrutamiento con clase, es decir, basado en las clases de direcciones IP. Este protocolo es importante por ser uno de los primeros en implementarse y servir de base para la evolución de los protocolos de enrutamiento dinámico [33].

RIP: No soporta subredes ni CIDR (*Classless Inter-Domain Routing*, estándar para la interpretación de direcciones IP). Tampoco incluye ningún mecanismo de autentificación de los mensajes [33].

A.- Características básicas del protocolo RIPv1:

- Es un protocolo de enrutamiento vector-distancia.
- Utiliza el algoritmo Bellman-Ford.
- La máxima métrica válida es de 15 saltos, mayores que 15 son inalcanzables.
- Se transmiten mensajes cada 30 segundos (Actualizaciones).
- Sus mensajes se encapsulan en un segmento UDP (User Datagram Protocol) con direcciones de puerto 520 tanto en origen como en destino.
- Tiene asignada una distancia administrativa de 120.
- Utiliza el formato de mensaje Broadcast.

B.- Formato del paquete RIPv1:

El formato de datagramas que contiene información de la red. Los tamaños de campo se dan en octetos, a menos que se especifique lo contrario. Los campos contienen enteros binarios, en orden normal de Internet con el primer octeto más significativo [33].

En la figura 10 se muestra el formato de paquete RIP con encabezado. Cada marca de verificación representa un bit.

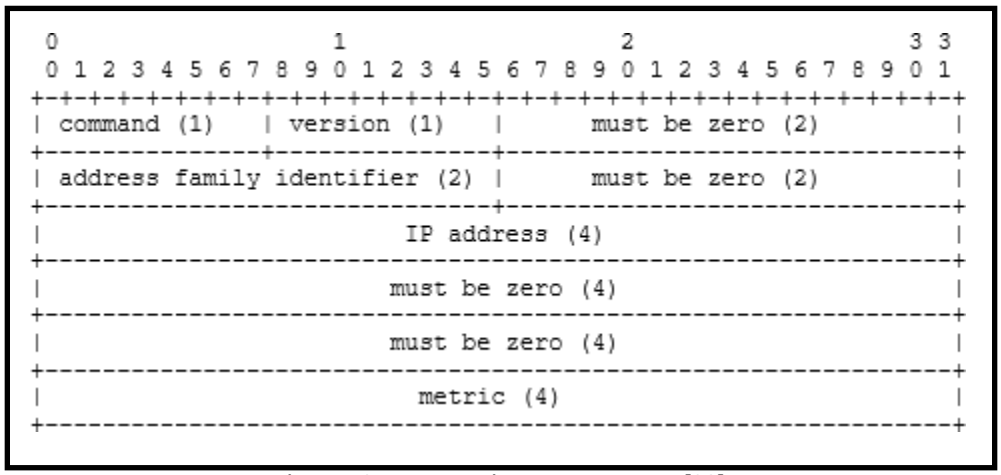


Figura 10. Formato de Paquete RIPv1 [33].

2.2.2 RIPv2

Soporta subredes *Classless Inter-Domain Routing* y VLSM (*Variable Length Subnet Masks*). Soporta autenticación utilizando uno de los siguientes mecanismos: no autenticación, autenticación mediante contraseña, autenticación mediante contraseña codificada mediante MD5 (*Message-Digest Algorithm 5*) [34].

A.- Características básicas de RIPv2:

- RIPv2 es una versión mejorada de RIPv1.
- Utiliza el algoritmo Bellman-Ford.
- La máxima métrica válida es de 15 saltos, mayores que 15 son inalcanzables.
- Se transmiten mensajes cada 15 segundos (Actualizaciones).
- Hay un mecanismo de autenticación (No permite que los router que usen RIPv1 lean los mensajes de RIPv2).
- Utiliza el formato de mensaje Multicast.
- Sus mensajes se encapsulan en un segmento UDP con direcciones de puerto 520 tanto en origen como en destino.

B.- Formato del paquete RIPv2:

El mismo formato de encabezado se utiliza para los mismos mensajes de RIP y RIPv2. El la figura 11 se muestra el formato para la entrada de ruta de 20 octetos.

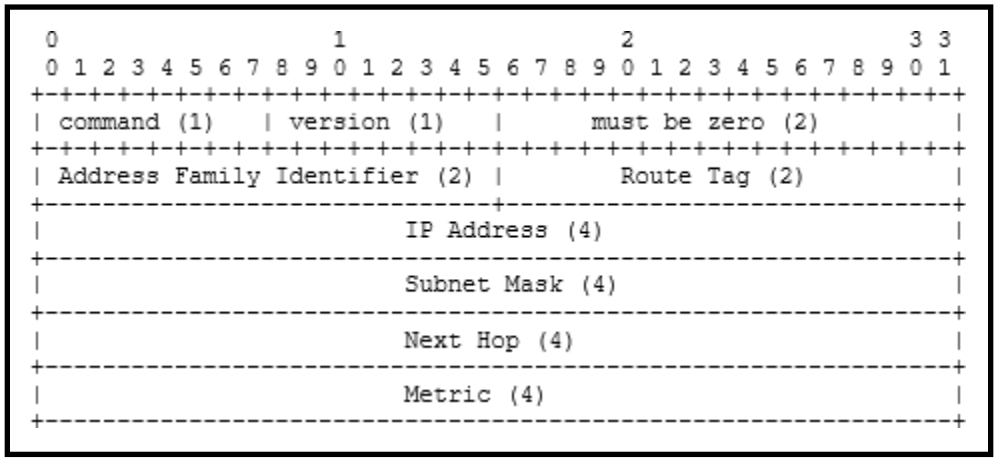


Figura 11. Formato de Paquete RIPv2 [34].

2.2.3 RIPng

RIPng (*Routing Information Protocol next generation*): El avance de la implementación de IPv6 exige que, no sólo conozcamos la versión actual del protocolo de direccionamiento de capa de red, sino también los protocolos de enrutamiento asociados al mismo.

IPv6 es un protocolo de enrutamiento completamente diferente de IPv4. En consecuencia los protocolos de enrutamiento IP que se utilizan en el entorno tradicional no son aplicables en redes IPv6. Por esto, son necesarios protocolos de enrutamiento específicos que respondan a la nueva arquitectura de IPv6 [35].

A.- Características básicas de RIPng:

- Protocolo de enrutamiento de vector-distancia.
- Básicamente es una actualización de RIPv2.
- Número máximo de saltos: 15
- Utiliza el puerto 521 de UDP para las comunicaciones.

B.- Funciones avanzadas de RIPng:

- Puede generar rutas por defecto.
- Permite la implementación de tags (etiquetas) en las rutas.
- Soporta redistribución de rutas originadas en otros protocolos o estáticas.
- Se requiere definir manualmente una métrica al redistribuir rutas dentro de RIPng.

C.- El formato del paquete RIPng con encabezado, se muestra en la figura 12.

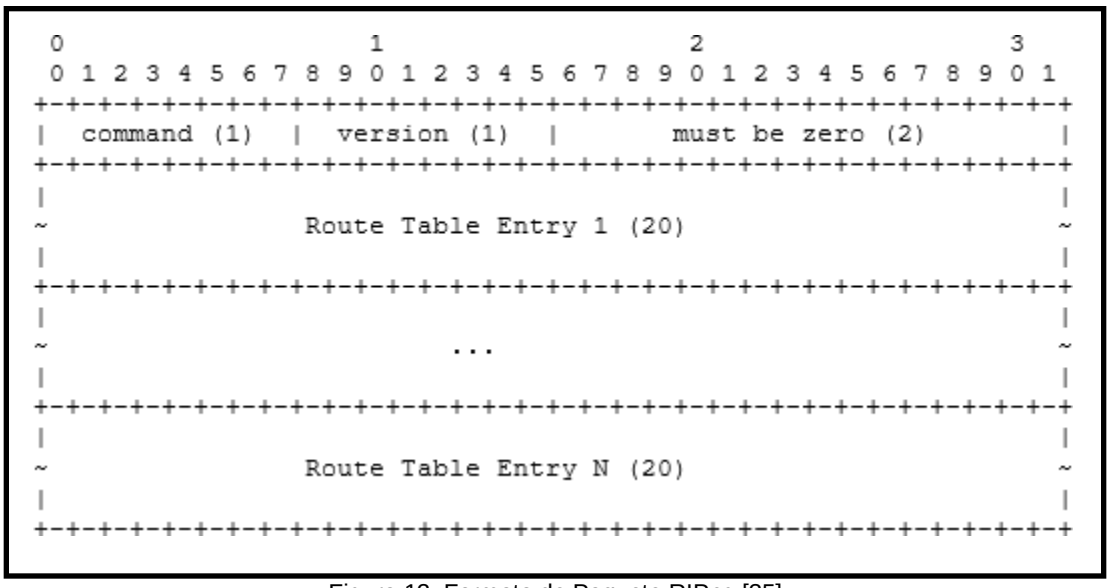


Figura 12. Formato de Paquete RIPng [35]

D.- El formato de entrada de la tabla de ruta RIPng, se muestra en la figura 13.

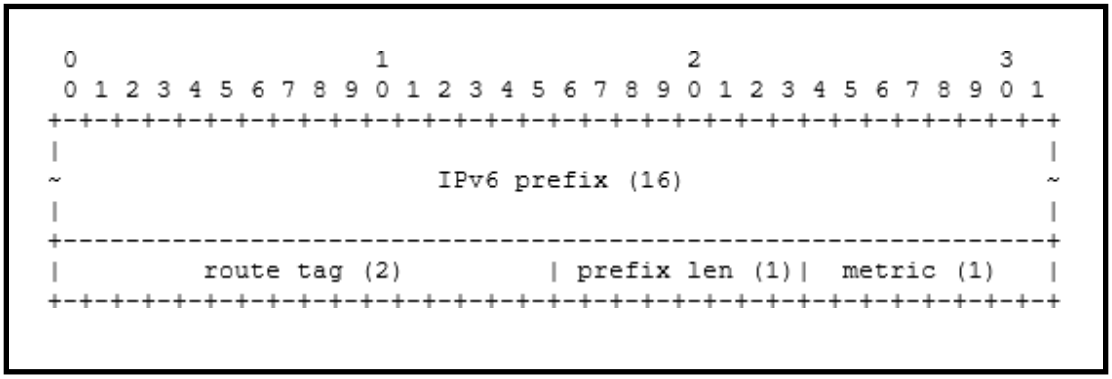


Figura 13. Formato de entrada de la tabla de ruta RIPng [35].

2.3 Protocolo de enrutamiento OSPF

En OSPF existen 3 tipos de versiones, las cuales son: OSPF, OSPFv2 y OSPFv3.

2.3.1 OSPF

El OSPF (*Open Shortest Path First*) es un protocolo de enrutamiento de estándar abierto, el cual emplea el algoritmo SPF (*Shortest Path First*) de Dijkstra para soportar una mejor convergencia en la red respecto del resto de los protocolos existentes. Debido a que es un estándar abierto, éste se puede implementar para diferentes plataformas, los fabricantes por lo general agregan a la base características extendidas por lo que en ocasiones algunas características podrían no quedar soportadas entre distintos fabricantes. OSPF fue diseñado para ejecutarse dentro de un AS, por lo que es un IGP, en la que cada router mantiene una base de datos idéntica, la cual describe la topología del AS y a partir de esa BD se calcula una tabla de **routeo** vía la construcción del SPT (*Shortest Path Tree*). La versión 1 apareció en 1989 y la versión 2 apareció en 1999 [36, 37]. Cabe mencionar que OSPF es uno de los protocolos soportados por la tecnología MPLS (*Multi-Protocol Label Switching*).

A.- Características básicas de OSPF:

- Emplea una base de datos de enlace-estado para eliminar los posibles “bucles de enrutamiento”.
- Soporta un comportamiento de enrutamiento sin clase (En la actualidad, la mayoría de las redes requieren protocolos de enrutamiento porque usan la técnica VLSM (*Variable Length Subnet Mask*)).
- Usa un resumen de rutas para reducir el tamaño de las tablas de enrutamiento.
- Reduce el ancho de banda requerido, al enviar las actualizaciones de las rutas solamente cuando se le es requerido.
- Emplea paquetes multicast para reducir en impacto en los equipos y routers que no estén activos en un determinado momento.
- Soporta autenticación para hacer más seguras las redes.
- Emplea áreas, lo cual permite usar muchas redes y una única “área 0”.

Un *backbone router* (router de núcleo) BR es un router que se encuentra dentro del “área 0”, mientras que un router interno es un router cuyas interfaces están conectadas dentro de un área que no es el área 0”. Para interconectar las distintas áreas se emplean los *Area Border Router*- router de frontera de área (ABR) y para interconectar un AS con otro se emplean los *Autonomous System Boundary Router*- router de enlace de sistema autónomo (ASBR), en este caso un router OSPF se conecta a un proceso de enrutamiento externo, el cual intercambia información con

ese proceso; todos estos tipos de routers se muestran de acuerdo a la función descrita en el diagrama de la figura siguiente.

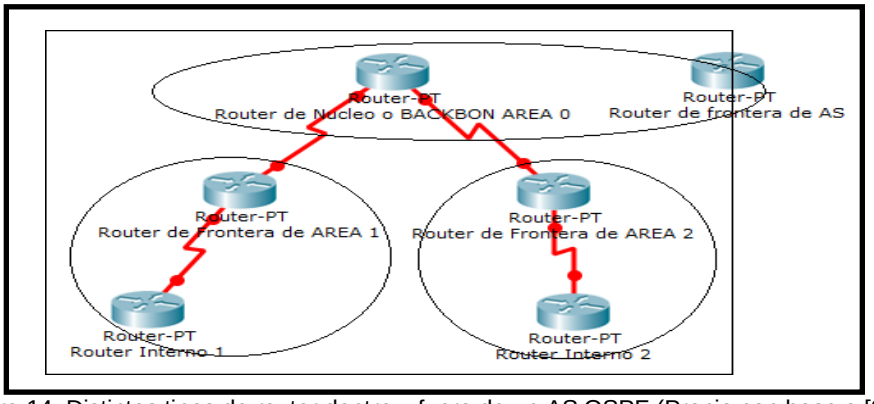


Figura 14. Distintos tipos de router dentro y fuera de un AS OSPF (Propia con base a [38]).

Los paquetes OSPF contienen 9 campos: *Version number*, *Type* (*Data Type*- tipo de dato), *Packet lengh* (bytes), *Router ID* (*source*-fuente del paquete), *Area ID* (*source*-fuente del paquete), *Checksum*, *authentication type*, *Authentication y Data*. Como se indica en la figura 11.

En el caso de los datos, pueden existir 5 tipos de datos o mensajes: *Hello* (lista de vecinos conocidos), DBD (contiene un resumen de la base de datos de los enlaces de estado –*Link State*), LSR, LSU y LSAck (paquete vacío). Como los que se describen en las figuras (12-16) [36, 37].

2.3.2 OSPFv2

Puede “etiquetar” rutas y propagar esas etiquetas por otras rutas, además, una red OSPF se puede descomponer en redes más pequeñas. Ejemplos:

- **Área Backbone**: También denominado “área 0”, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).
- **Área stub:** Es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.
- **Área not-so-stubby:** También conocida como NSSA (*Not-so-stuby área*), constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas [37].

A.- En la figura 15 se muestra el formato de encabezado del paquete OSPFv2.

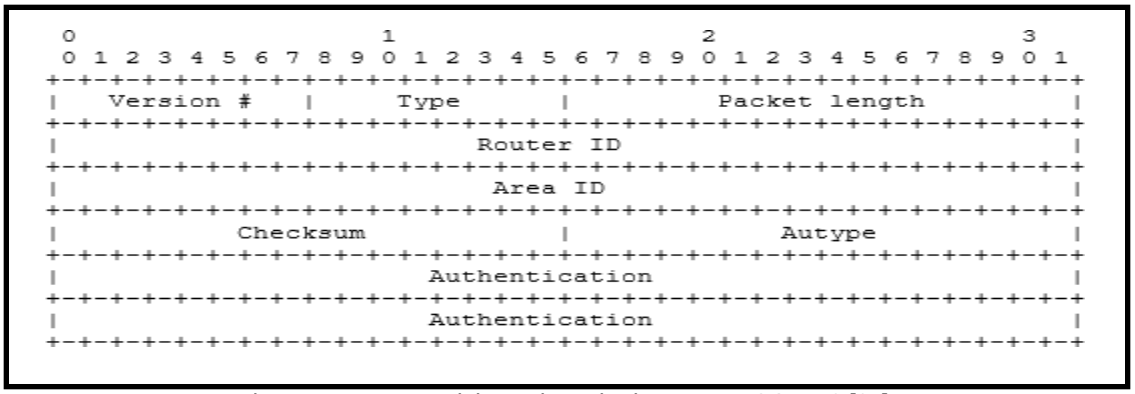


Figura 15. Formato del encabezado de paquete OSPFv2 [37].

B.- El protocolo OSPFv2 utiliza cinco tipos de paquetes que lo caracterizan:

- **Paquete Hello**: Descubre quienes son los vecinos.

El **Paquete Hello**, son paquetes OSPF de tipo 1. Estos paquetes se envían periódicamente en todas las interfaces (incluidos los enlaces virtuales) para establecer y mantener relaciones de vecinos. Además, los Hellos son multidifusión en las redes físicas que tienen una capacidad de difusión o multidifusión, lo que permite el descubrimiento dinámico de enrutadores vecinos. En la figura 16 se muestra el **Paquete Hello**, con encabezado. [37]

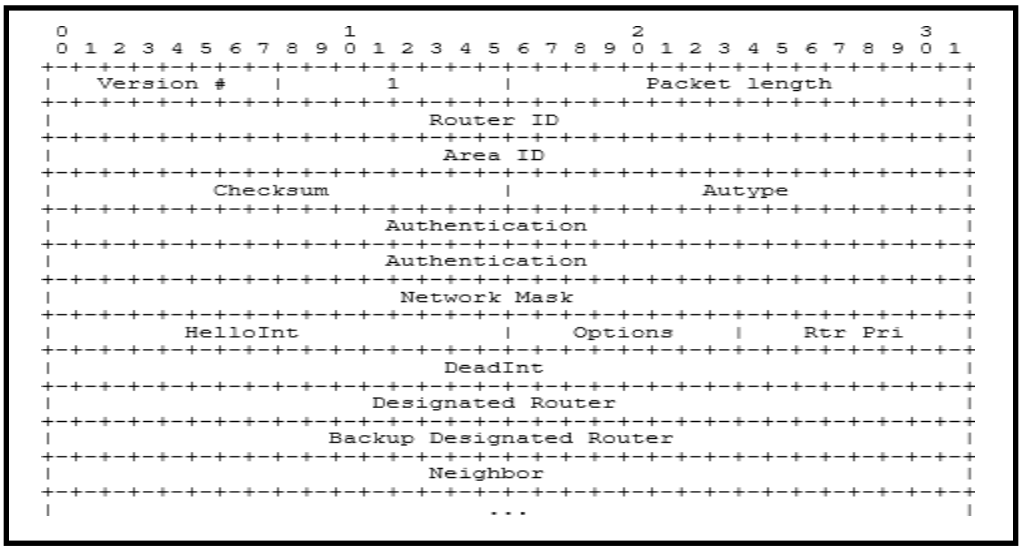


Figura 16. “Paquete Hello” OSPFV2 [37].

- **Network Mask**: La máscara de red asociada a esta interfaz. Por ejemplo, si la interfaz es a una red de clase B cuyo tercer byte se utiliza para subnetting, la máscara de red es 0xffffff00
- **HelloInt**: El número de segundos entre los paquetes de saludo de este enrutador.
- **Options**: Las capacidades opcionales soportadas por el router.

- **Rtr Pri**: Prioridad de enrutador de este enrutador. Utilizado en la elección del enrutador designado (de respaldo). Si se establece en 0, el enrutador no será elegible para convertirse en enrutador designado (de respaldo).
- **DeadInd**: El número de segundos antes de declarar un enrutador silencioso hacia abajo.
- **Designated Router**: La identidad del enrutador designado para esta red, en la vista del enrutador de publicidad. El enrutador designado se identifica aquí por su dirección de interfaz IP en la red. Se establece en 0 si no hay un enrutador designado [37].

➢ **Paquete DBD** (*DataBase Description*): Anuncia qué actualizaciones tiene la base de datos

El **Paquete DBD**, es un paquete OSPF de tipo 2. Este paquete se intercambia cuando se está inicializando una adyacencia. Describe los contenidos de la base de datos topológica. Se pueden usar múltiples paquetes para describir la base de datos. Para este propósito se utiliza un procedimiento de encuesta de respuesta. Uno de los enrutadores está designado como maestro, el otro como esclavo. El maestro envía los **Paquetes de Descripción de la Base de Datos** (sondeos) que son reconocidos por los **Paquetes de Descripción de la Base de Datos** enviados por el esclavo (respuestas). Las respuestas están vinculadas a las encuestas a través de los números de secuencia de los paquetes. En la figura 17 se muestra el **Paquete DBD** [37].

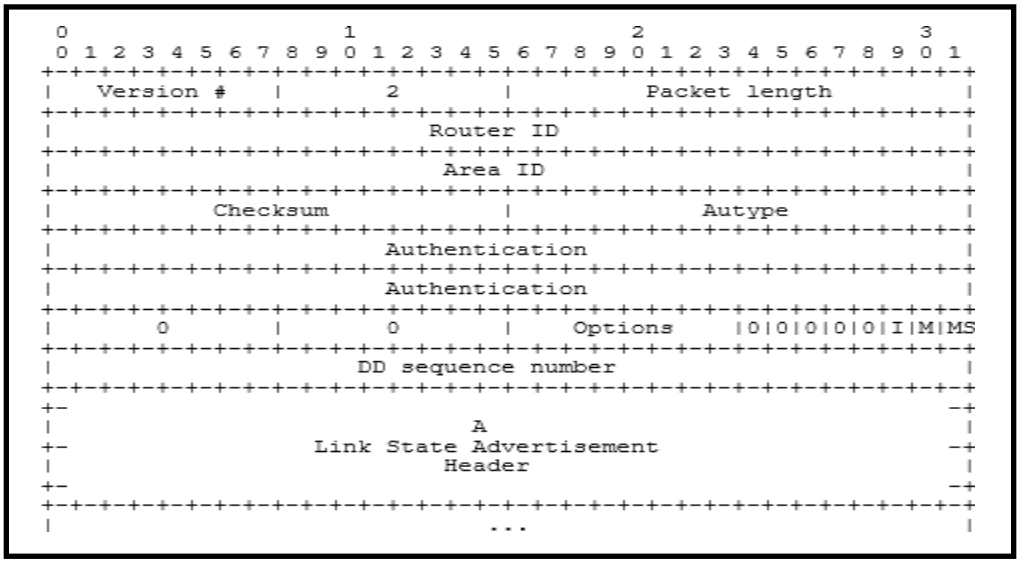


Figura 17. “Paquete DBD” OSPFV2 [37].

- **0**: Estos campos están reservados. Deben ser 0.
- **Options**: Las capacidades opcionales soportadas por el router.
- **I-bit**: El bit inicial. Cuando se establece en 1, este paquete es el primero en la secuencia de descripciones de la base de datos.

- **M-bit**: El bit más. Cuando se establece en 1, indica que hay más base de datos.
- **MS.bit**: El bit maestro/ esclavo. Cuando se establece en 1, indica que el enrutador es el maestro durante el proceso de intercambio de base de datos. De lo contrario, el enrutador es el esclavo.
- **DD sequence number**: Se utiliza para secuenciar la colección de paquetes de descripción de base de datos. El valor inicial (indicado por el bit de inicio que se establece) debe ser único. El número de secuencia se incrementa hasta que se envía la descripción completa de la base de datos.

El resto del paquete consiste en una lista (posiblemente parcial) de las piezas de la base de datos topológica. Cada anuncio de estado de enlace en la base de datos se describe por su encabezado de estado de enlace. [37]

- **Paquete LSR** (*Link-State Request*): Solicita información de la base de datos.

El **Paquete LSR**, es un paquete OSPF de tipo 3. Después de intercambiar los **Paquetes de Descripción de la Base de Datos** con un enrutador vecino, un enrutador puede encontrar qué partes de su base de datos topológica están desactualizados. El paquete de solicitud de estado de enlace se utiliza para solicitar las partes de la base de datos del vecino que están más actualizadas. Es posible que se necesiten varios paquetes de solicitud de estado de enlace. El envío de paquetes de solicitud de estado de enlace es el último paso para que aparezca una adyacencia. En la figura 18 se muestra el **Paquete LSR** [37].

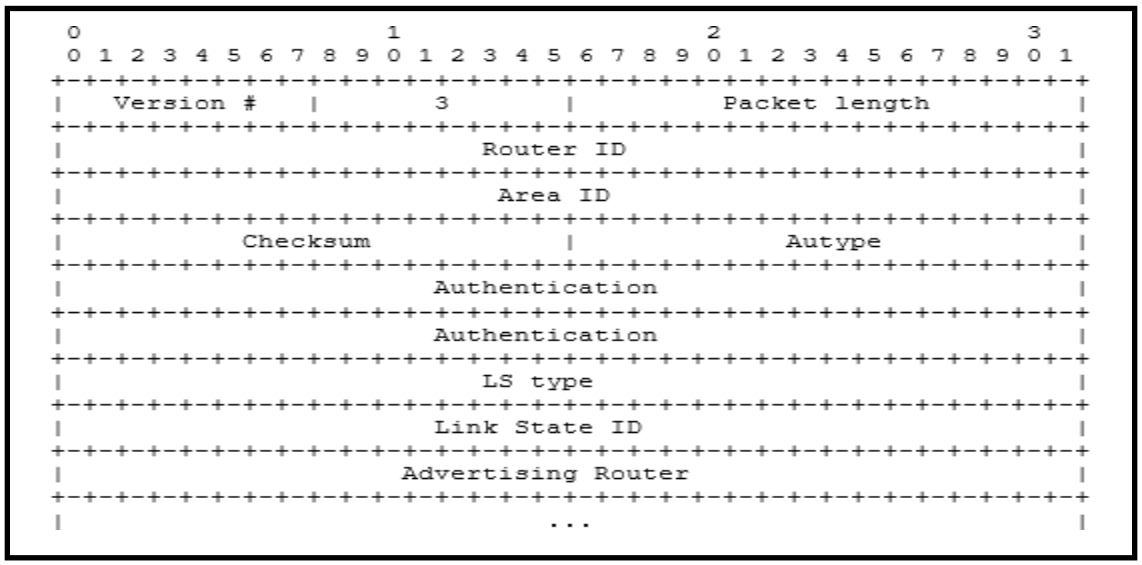


Figura 18. “Paquete LSR” OSPFv2 [37].

Cada anuncio solicitado se especifica por su tipo de LS, ID de estado de enlace y enrutador de publicidad. Esto identifica de forma única el anuncio, pero no su instancia. Los paquetes de solicitud de estado de enlace se entienden como solicitudes para la instancia más reciente (cualquiera que sea) [37].

- **Paquete LSU** (*Link State Update*): Proporciona la actualización de la base de datos.

El **Paquete LSU**, es un paquete OSPF de tipo 4. Éste paquete implementa *Flooding* de anuncios de estado de enlace. Cada paquete de actualización de estado de enlace lleva una colección de anuncios de estado de enlace un salto más lejos de su origen. Se pueden incluir varios anuncios de estado de enlace en un sólo paquete. Como en la figura 19 se muestra el **Paquete LSU** [37].

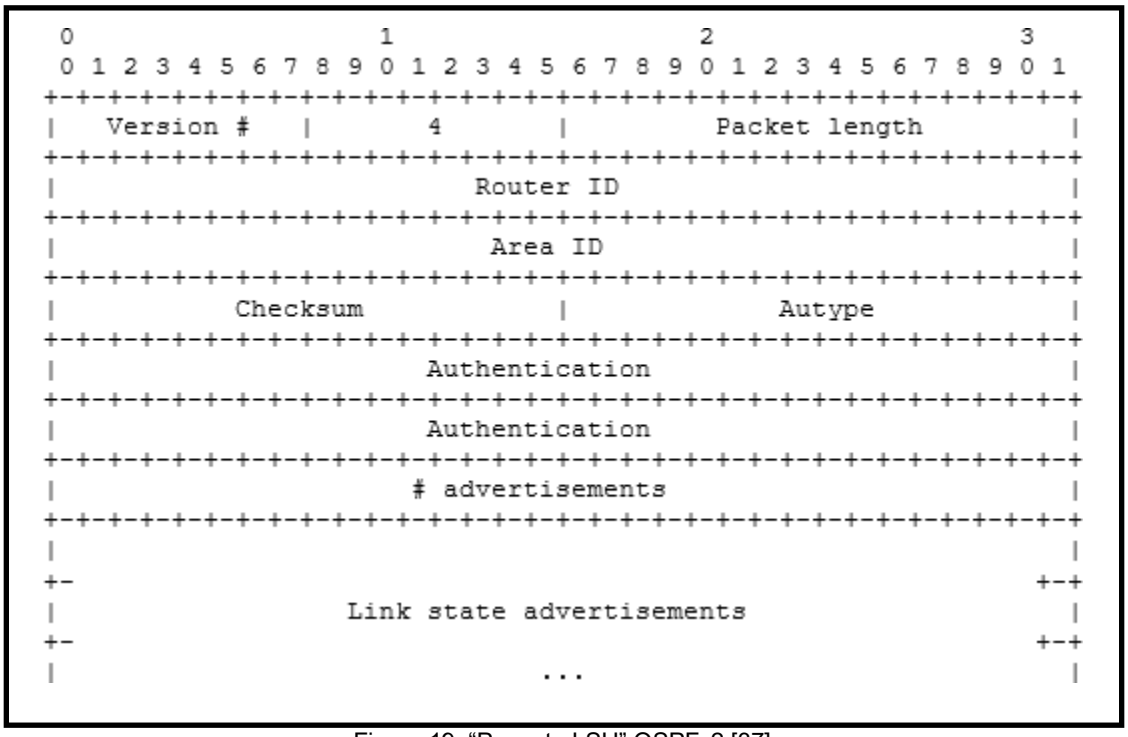


Figura 19. “Paquete LSU” OSPFv2 [37].

- **# advertisements**: El número de anuncios en estado de enlace incluidos en esta actualización.

El cuerpo del paquete de actualización de estado de enlace consiste en una lista de anuncios de estado de enlace. Cada anuncio comienza con un encabezado común de 20 bytes, el encabezado del anuncio de estado del enlace. De lo contrario, el formato de cada uno de los cinco tipos de anuncios de estado de enlace es diferente [37].

- **Paquete LSAck** (*Link-State acknowledgment*): Confirma la recepción de la actualización del estado del enlace.

El **Paquete LSAck**, es un paquete OSPF de tipo 5. Para que *Flooding* de anuncios de estado de enlace sea confiable, los anuncios *Flooding* se reconocen explícitamente. Este reconocimiento se logra mediante el envío y la recepción de **Paquetes de Reconocimiento de Estado de Enlace**. Múltiples anuncios en estado de enlace pueden ser reconocidos en un solo paquete [37]. Como en la figura 20**.**

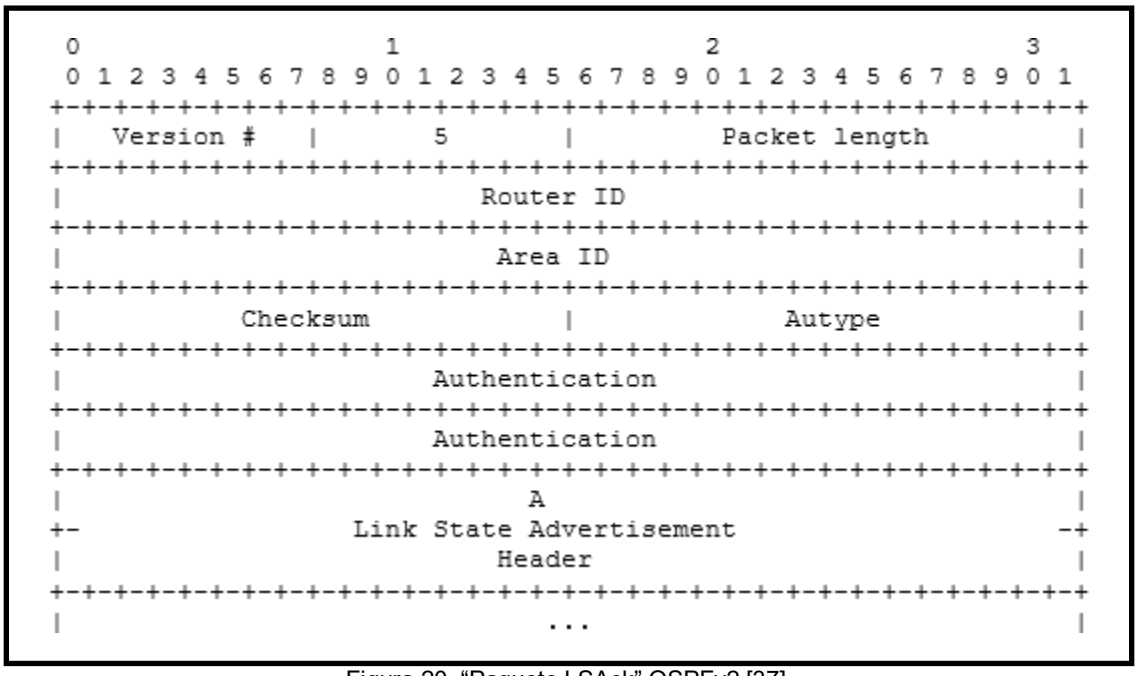


Figura 20. “Paquete LSAck” OSPFv2 [37].

El formato de este paquete es similar al del paquete de descripción de datos. El cuerpo de ambos paquetes es simplemente una lista de encabezados de anuncios de estado de enlace.

Cada anuncio de estado de enlace reconocido se describe por su encabezado de estado de enlace. Contiene toda la información necesaria para identificar de forma única tanto el anuncio como la instancia actual del anuncio [37].

2.3.3 OSPFv3

Es la actualización de OSPFv2, en la cual se realizaron las modificaciones para la versión 6 del Protocolo de Internet (IPv6). Los mecanismos fundamentales de OSPF (*Flooding*, elección de DR, soporte de áreas, cálculos de SPF, etc.) permanecen sin cambios. Sin embargo, algunos cambios han sido necesarios, ya sea debido a cambios en la semántica de protocolo entre IPv4 e IPv6, o simplemente para controlar el aumento del tamaño de la dirección de IPv6.

Los cambios entre OSPFv2 y OSPFv3 son los siguientes: Las semánticas de direccionamiento se han eliminado de los paquetes de OSPF y de los LSA. Se han creado nuevos LSA para transportar prefijos y direcciones IPv6. OSPF ahora se ejecuta por enlace, en lugar de por subred IP. Se ha generalizado el alcance de *Flooding* para LSAs. La autenticación se ha eliminado del propio protocolo OSPF, así como los campos relacionados con la autenticación se han eliminado del área OSPF y las estructuras de la interfaz. Confiando en el encabezado de autenticación de IPv6 y la encapsulación de la carga útil de seguridad [39].

A.- Uso de direcciones de enlace local:

Las direcciones de enlace local de IPv6 se utilizan en un sólo enlace, para fines de descubrimiento de vecinos, configuración automática, etc. Los enrutadores de IPv6 no reenvían datagramas de IPv6 que tienen direcciones de origen de enlace local. Las direcciones unicast locales de enlace se asignan desde el rango de direcciones IPv6 FF80 / 10 [39].

B.- Cambios de formato de paquetes:

OSPF para IPv6 se ejecuta directamente sobre IPv6. Aparte de esto, toda la semántica de direccionamiento ha sido eliminada de los encabezados de paquetes OSPF, por lo que es esencialmente “independiente del protocolo de red”. Todas las direcciones y la información ahora están contenidas en los diversos tipos de LSA solamente.

C.- El encabezado del paquete OSPFv3:

Cada paquete OSPF comienza con un encabezado estándar de 16 bytes. Junto con los encabezados IPv6 que encapsulan, el encabezado OSPF contiene toda la información necesaria para determinar si el paquete debe ser aceptado para su posterior procesamiento [39].

D.- En la figura 21 se muestra el formato del encabezado del paquete OSPFv3:

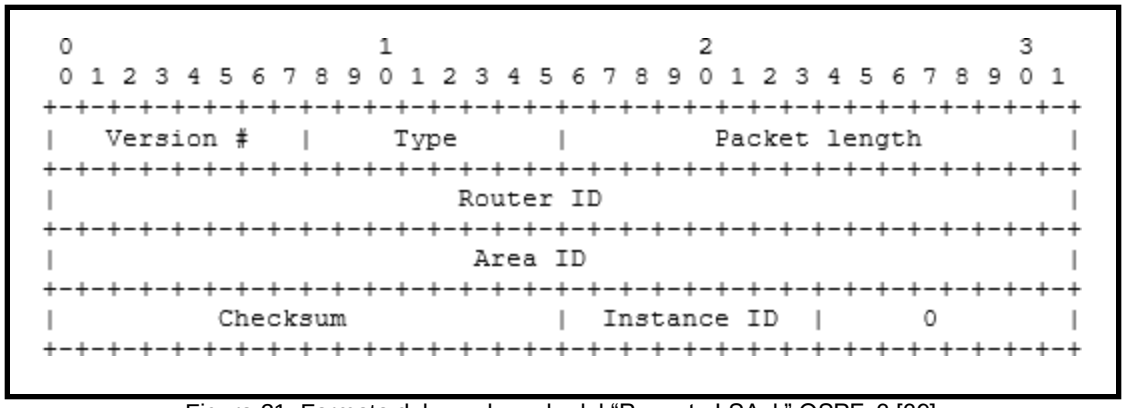


Figura 21. Formato del encabezado del "Paquete LSAck" OSPFv3 [39].

E.- El protocolo OSPFv3 (IPv6) utiliza cinco tipos de paquetes que lo caracterizan al igual que en OSPFv2 (IPv4).

A continuación, tendremos los 5 tipos de paquetes con sus respectivas actualizaciones para IPv6 [39].

- **Paquete Hello**: Descubre quienes son los vecinos. Ver figura 22:

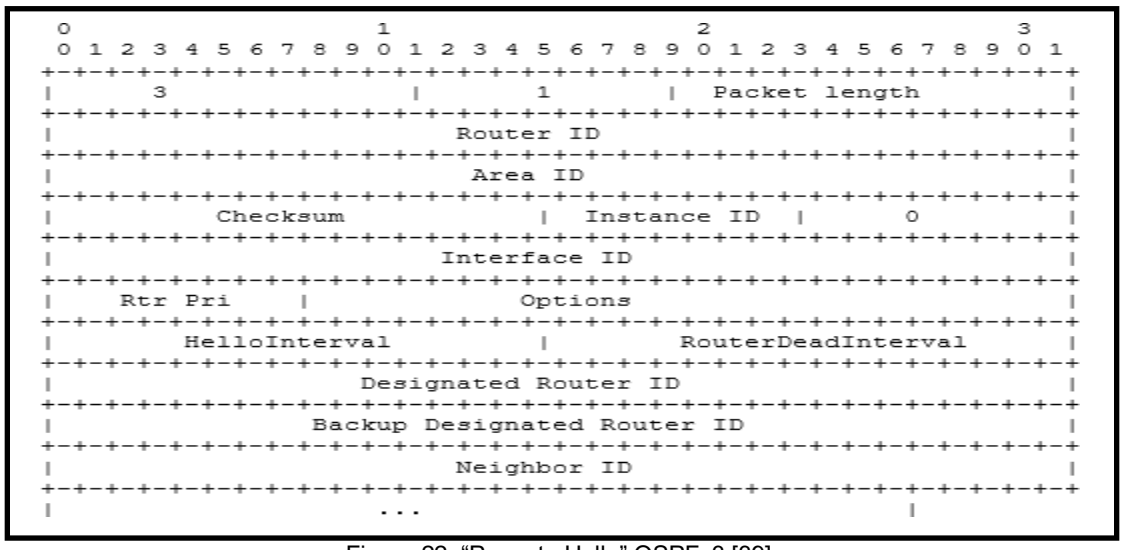


Figura 22. "Paquete Hello" OSPFv3 [39].

- **Interface ID**: Número de 32 bits que identifica de forma única esta interfaz entre la colección de las interfaces de este enrutador.
- **HelloInterva**l: El número de segundos entre los paquetes de saludo de este enrutador.
- **RouterDeadInterval**: El número de segundos antes de declarar un enrutador silencioso o inhabilitado.
- **Designated Router ID**: La identidad del Router designado para esta red, en la vista del enrutador emisor. El enrutador designado se identifica por su ID de enrutador. Se establece en 0.0.0.0 si no hay un enrutador designado.

- **Backup Designated Router ID**: La identidad del enrutador designado de respaldo para esta red, en la vista del enrutador emisor. El enrutador designado de respaldo se identifica por su ID de enrutador IP. Se establece en 0.0.0.0 si no hay un enrutador designado de respaldo.
- **Neighbor ID**: Las ID del enrutador de cada enrutador desde el cual se han visto recientemente paquetes de saludo válidos en la red. Recientemente significa en los últimos segundos *RouterDeadInterva*l. [39]

➢ **Paquete DBD** (*DataBase Description*): Anuncia qué actualizaciones tiene la base de datos. Como en la figura 23:

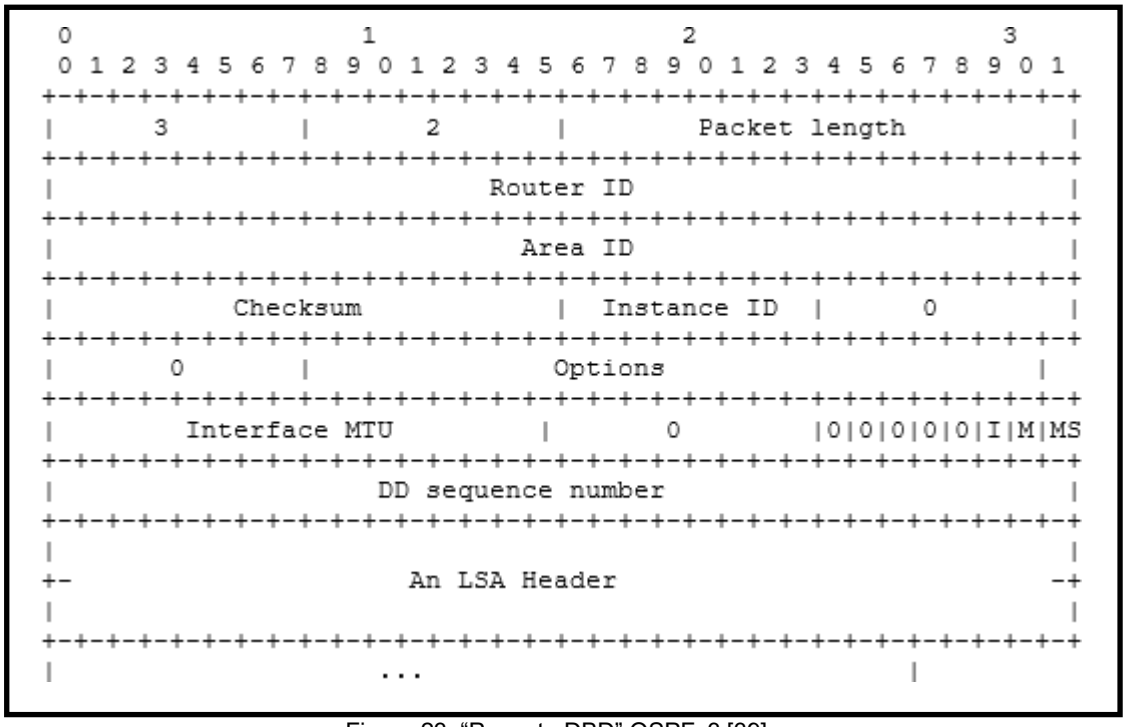


Figura 23. “Paquete DBD” OSPFv3 [39].

- **Interface MTU**: El tamaño en bytes del datagrama IPv6 más grande que se puede enviar. Fuera de la interfaz asociada, sin fragmentación. La interfaz MTU debe establecerse en 0 en los paquetes de descripción de la base de datos enviados a través de enlaces virtuales [39].

- **Paquete LSR** (*Link-State Request*): Solicita información de la base de datos. Como en la figura 24:

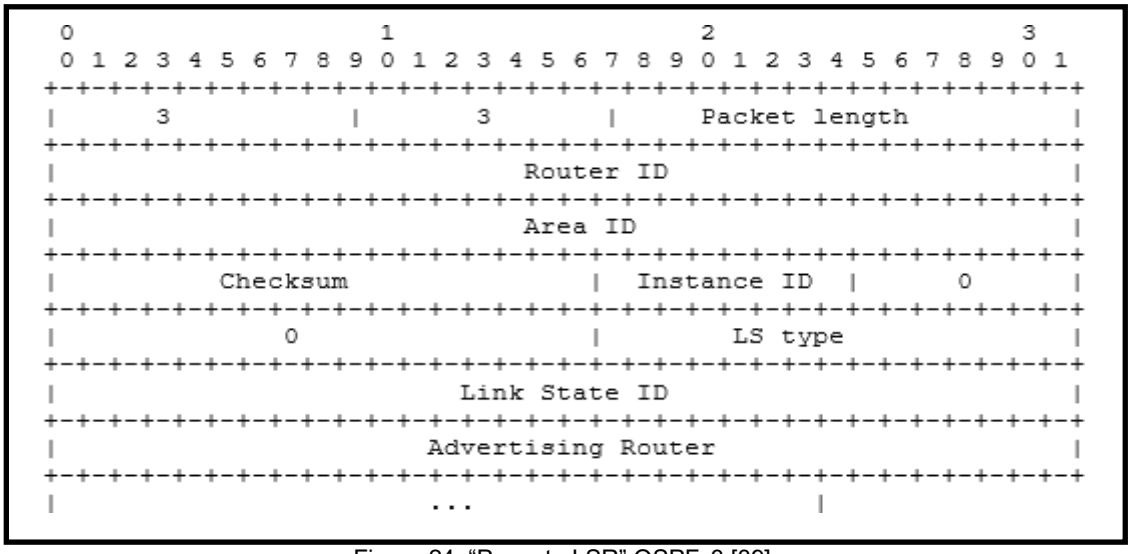


Figura 24. "Paquete LSR" OSPFv3 [39].

- Cada LSA solicitado se especifica por su tipo LS, ID de estado de enlace y enrutador de Advertising. Esto identifica de forma única la LSA, pero no su instancia. Los paquetes de solicitud de estado de enlace se entienden como solicitudes para la instancia más reciente (cualquiera que sea) [39].

- **Paquete LSU** (*Link State Update*): Proporciona la actualización de la base de datos. Como en la figura 25:

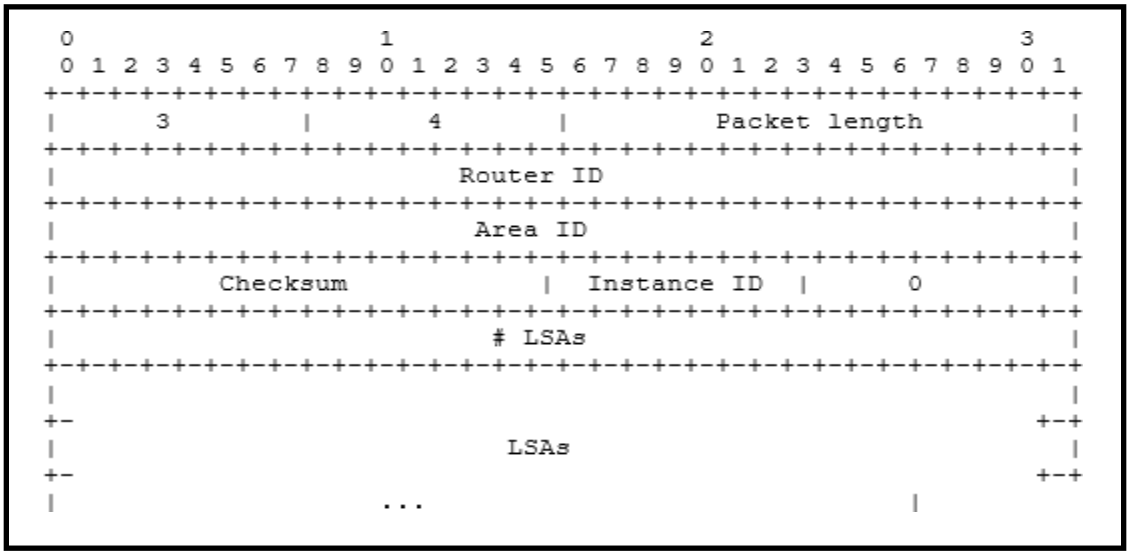


Figura 25. "Paquete LSU" OSPFv3 [39].

- **# LSAs**: El número de LSA incluidos en esta actualización.
- El cuerpo del paquete de actualización del estado de enlace consiste en una lista de LSA. Cada LSA comienza con un encabezado común de 20 bytes.

- **Paquete LSAck** (*Link-State Acknowledgment*): Confirma la recepción de la actualización del estado del enlace. Como en la figura 26:

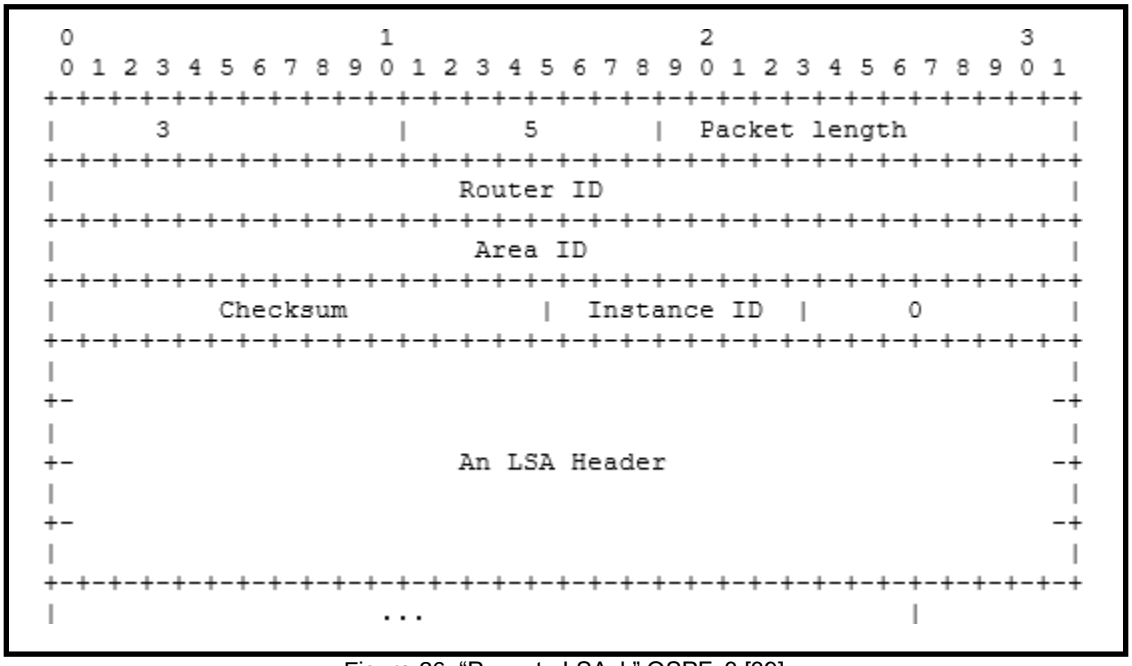


Figura 26. “Paquete LSAck” OSPFv3 [39].

- Cada LSA reconocida se describe por su encabezado LSA. Contiene toda la información necesaria para identificar de forma única tanto la LSA como la instancia actual de la LSA [39].

2.4 Protocolo de gestión SNMP

En SNMP existen 3 tipos de versiones, las cuales son: SNMPv1, SNMPv2 y SNMPv3.

2.4.1 SNMPv1

El SNMP (*Simple Network Management Protocol*) es un protocolo que se desarrolló para permitir que los administradores puedan administrar los nodos, servidores, las estaciones de trabajo, los routers, los switches y los dispositivos de seguridad, en una red IP. Permite a los administradores de red gestionar el rendimiento de la red, encontrar y resolver problemas de red, y planifiquen el crecimiento de la red [40].

SNMP: Es un protocolo de capa de aplicación que proporciona un formato de mensaje para la comunicación entre administradores y agentes. El sistema SNMP consta de tres elementos:

- Administrador de SNMP
- Agentes SNMP (nodo administrado)
- Base de información de administración (MIB)

A.- Funcionamiento del SNMP.

Los agentes SNMP que residen en los dispositivos administrados recopilan y almacenan información sobre los dispositivos y su funcionamiento. El agente almacena esta información localmente en la MIB. El administrador SNMP luego usa el agente SNMP para tener acceso a la información dentro de la MIB [40].

Existen dos solicitudes principales de administrador de SNMP: get y set.

- **get**: Recupera un valor de una variable específica.
- **set**: Almacena un valor en una variable específica.

B.- Especificación del protocolo SNMP.

El protocolo de gestión de red es un protocolo de aplicación mediante el cual las variables de la MIB de un agente pueden ser inspeccionadas o alteradas.

La comunicación entre entidades de protocolo se realiza mediante el intercambio de mensajes, cada uno de los cuales está total e independientemente representado dentro de un sólo datagrama UDP. Un mensaje consta de una versión, identificador, un nombre de comunidad SNMP y una unidad de datos de protocolo (PDU). Una entidad de protocolo recibe mensajes en el puerto UDP 161 en el host con que se asocia para todos los mensajes, excepto para aquellos que informan *traps* (es decir, todos los mensajes excepto aquellos que contienen la PDU de *traps*). Los mensajes que informan capturas deben recibirse en el puerto UDP 162 para su posterior procesamiento. Una implementación de este protocolo no necesita aceptar

mensajes cuya longitud exceda los 484 octetos. Sin embargo se recomienda que las implementaciones admitan datagramas más grandes siempre que sea posible [40].

C.- Operaciones soportadas en la información de gestión

El SNMP modela todas las funciones del agente de administración como alteraciones o inspecciones de variables. Por lo tanto, una entidad de protocolo en un host lógicamente remoto (posiblemente el propio elemento de red) interactúa con el agente de administración residente en el elemento de red para recuperar (*get*) o alterar (*set*) variables. Esta estrategia tiene al menos dos consecuencias positivas:

- Tiene el efecto de limitar el número de funciones de administración esenciales realizadas por el agente de administración: una operación para asignar un valor a una configuración específica u otro parámetro y otra para recuperar dicho valor.

- Un segundo efecto de esta decisión es evitar la introducción en el soporte de definición de protocolo para comandos de gestión imperativos: el número de comandos de este tipo aumenta en la práctica, y la semántica de dichos comandos es en general arbitrariamente compleja.

La estrategia implícita en el SNMP es que la supervisión del estado de la red en cualquier nivel de detalle significativo se realiza principalmente mediante el sondeo de la información apropiada por parte del centro o los centros de supervisión. Un número limitado de mensajes no solicitados (*traps*) guían el tiempo y el enfoque del sondeo.

D.- Trap de un SNMP

Las *traps* son mensajes no solicitados por el administrador, pero enviados por cualquiera de los nodos para alertar al administrador de SNMP sobre una condición o un evento en la red. Algunos ejemplos de las condiciones de *trap* incluyen, entre otros, la autenticación incorrecta de usuarios, los reinicios, el estado del enlace (activo o inactivo), el seguimiento de direcciones MAC, el cierre de una conexión TCP, la pérdida de conexión a un vecino u otros eventos importantes [40].

2.4.2 SNMPv2

Es una evolución de SNMPv1. Agrega y mejora algunas operaciones de protocolo. La operación de traps de SNMPv2, por ejemplo, tiene la misma función que la utilizada en SNMPv1, pero emplea un formato de mensaje diferente y está diseñado para sustituir las traps de SNMPv1 [41].

A.- En la figura 27 se muestra el formato de mensaje SNMPv2:

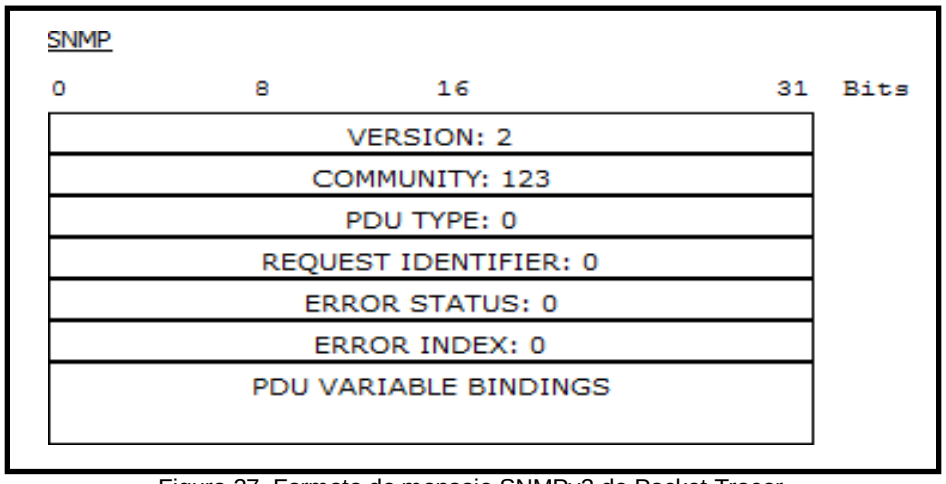


Figura 27. Formato de mensaje SNMPv2 de Packet Tracer.

B.- Componentes del marco SNMPv2:

Un sistema de gestión contiene: varios (potencialmente muchos) nodos, cada uno es una entidad de procesamiento, denominado agente, que tiene acceso a la instrumentación de administración; al menos una estación de gestión; y, un Protocolo de administración, utilizado para transmitir información de administración entre los agentes y las estaciones de administración. Las operaciones del protocolo se llevan a cabo bajo un marco administrativo que define las políticas de autenticación, autorización, control de acceso y privacidad.

Las estaciones de gestión ejecutan aplicaciones de gestión que supervisan y controlan los elementos gestionados. Los elementos gestionados son dispositivos como hosts, enrutadores, servidores de terminal, etc., que se monitorean y controlan mediante el acceso a su información de administración [42].

C.- Protocolo de operaciones de SNMPv2:

Proporciona el intercambio de mensajes que transmite información de gestión entre los agentes y las estaciones de gestión. La forma de estos mensajes es un mensaje “contenedor” que encapsula una Unidad de Datos de Protocolo (PDU). El propósito del Protocolo de Operaciones para el documento SNMPv2 es definir las operaciones del protocolo con respecto al envío y recepción de las PDUs [42].

D.- Asignaciones de transporte en SNMPv2:

El protocolo de administración, versión 2 del Protocolo Simple de Administración de Redes, se puede usar en una variedad de conjuntos de protocolos. El propósito de las asignaciones de transporte para el documento SNMPv2, es definir cómo se asigna SNMP a un conjunto inicial de dominios de transporte. Otras asignaciones se pueden definir en el futuro.

Aunque se definen varias asignaciones, la asignación a UDP es el mapeo preferido. Como tal, para proporcionar el mayor nivel de interoperabilidad, sistemas que eligen desplegar otros mapeos. El SNMP también debe proporcionar servicio de proxy a la asignación UDP [42].

E.- El marco administrativo basado en la comunidad SNMPv2:

El propósito de un marco administrativo es definir una infraestructura a través de la cual se pueda realizar una gestión efectiva en una variedad de configuraciones y entornos. Especificados como parte o como extensiones de un marco administrativo son mecanismos de seguridad utilizados para lograr un nivel de administración definido de manera administrativa [42].

3.1.2 SNMPv3

Es un protocolo de interoperabilidad basado en estándares para la gestión de red. Asimismo, el SNMPv3 proporciona el acceso seguro a los dispositivos mediante una combinación de autenticación y encriptación de los paquetes a través de la red. Algunas características de SNMPv3 son: Seguridad del mensaje, autenticación y encriptado.

El SNMPv3 trabaja esencialmente en el sistema de seguridad, incluyendo autenticación, privacidad y control de acceso, así como la administración del protocolo para realizar configuraciones remotas. El SNMPv3 utiliza el USM (*User-Based Security Model* – Modelo de Seguridad Basado en Usuario), el mecanismo genera un acuse de recibo del mensaje, y garantiza que éste no fue modificado durante su trayecto, para ello, utiliza el protocolo de autenticación: HMAC-MD5-96 o el HMAC-SHA-96, el cual utiliza una función hash criptográfica en conjunto con una llave de encriptación como MD5 (*Message-Digest Algorithm 5*- Algoritmo de Resumen del Mensaje 5) o SHA-1 (*Secure Hash Algorithm*- Algoritmo de Hash Seguro). Además, SNMPv3 difunde los mensajes dentro de un intervalo de tiempo en el que agente y gestor garantizan la velocidad del mensaje, si después de transcurrido dicho intervalo de tiempo se recibe un mensaje, este se considera erróneo y se desecha, por lo que este procedimiento es para proporcionar seguridad de nivel de mensaje SNMP, además del intervalo de tiempo, cada mensaje lleva una codificación extra utilizando el algoritmo CBC (*Cipher Block Chaining*, construido por el algoritmo *Data Encryptation Standard*, conocido como DES-56).

Por otra parte también podemos conocer el CBC-DES como cifrado simétrico, que es el primer protocolo de privacidad que se utiliza el USM en el protocolo SNMPv3, también trabaja con una Base de información de administración (MIB) para monitorear/administrar de forma remota los parámetros de configuración en los dispositivos de red [43].

A.- Motor SNMP

Proporciona servicios para enviar y recibir mensajes, autenticar, cifrar mensajes y controlar el acceso a objetos gestionados. Existe una asociación uno a uno entre un motor SNMP y la entidad SNMP que lo contiene [43, 44].

El motor contiene:

1. Sólo hay un despachador en un motor SNMP. Permite soporte concurrente de múltiples versiones de mensajes de SNMP en el motor SNMP. El despachador lo hace a través de:

- Enviar y recibir mensajes SNMP a / desde la red.
- Determinar la versión de un mensaje SNMP e interactuar con el correspondiente Modelo de Procesamiento de Mensajes.
- Proporcionar una interfaz abstracta para aplicaciones SNMP para entrega de un PDU a una aplicación.
- Proporcionar una interfaz abstracta para aplicaciones SNMP que le permite enviar una PDU a una entidad SNMP remota.

2. Un subsistema de procesamiento de mensajes es responsable de preparar mensajes para enviar y extraer datos de mensajes recibidos, también contiene múltiples modelos de procesamientos de mensajes como se muestra en la figura 28.

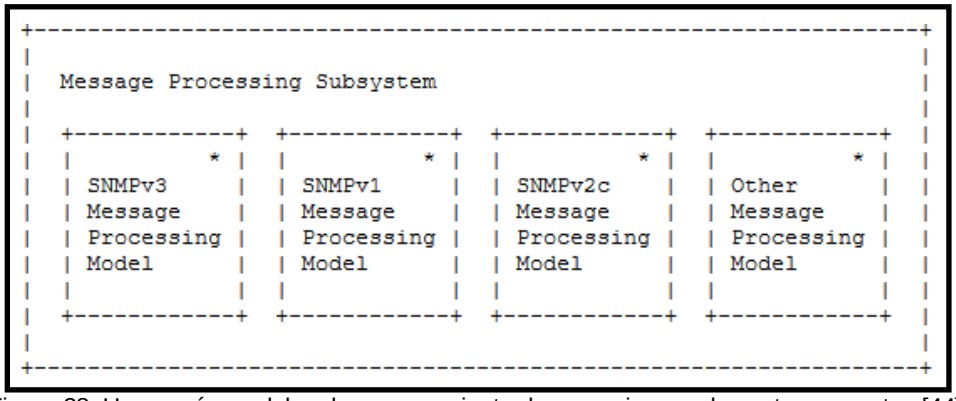


Figura 28. Uno o más modelos de procesamiento de mensajes pueden estar presentes [44].

3. Un subsistema de seguridad proporciona servicios de seguridad como autenticación y privacidad de los mensajes y potencialmente contiene varios modelos de seguridad como se muestra en la figura 29.

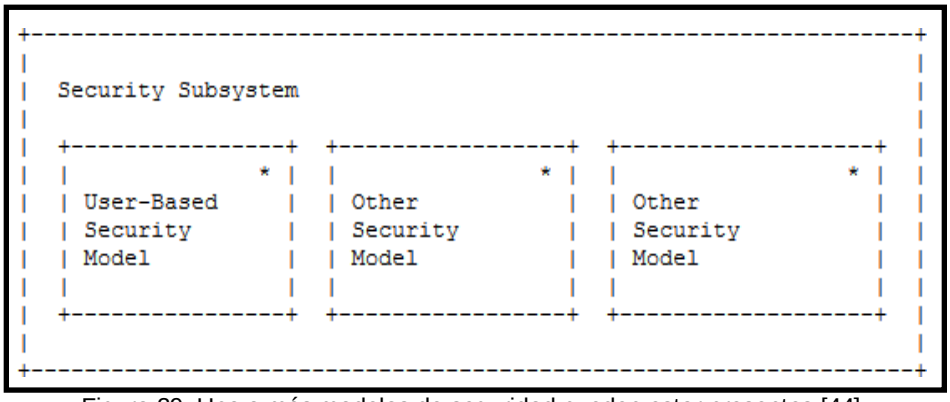


Figura 29. Uno o más modelos de seguridad pueden estar presentes [44].

4. Un subsistema de control de acceso proporciona servicios de autorización por medio de uno o más modelos de control de acceso. Como se muestra en la figura 30.

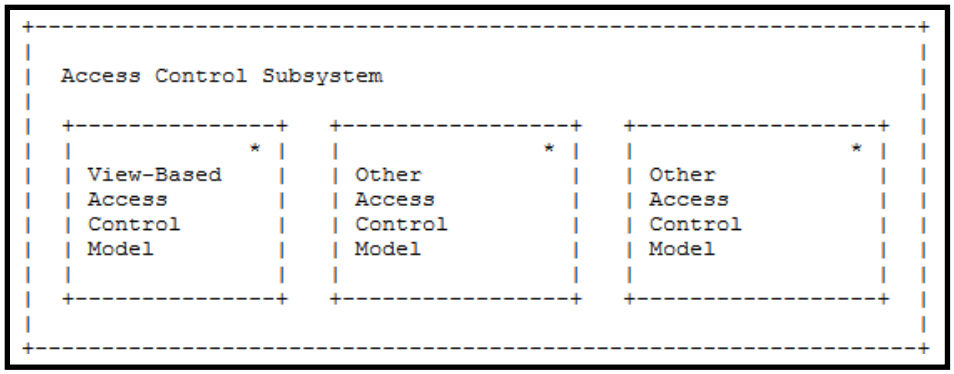


Figura 30. Subsistema de control de acceso [44].

B.- SNMP Manager

Una entidad SNMP que contiene uno o más aplicaciones de generador de comandos y / o receptor de notificaciones (junto con su motor SNMP asociado) se ha denominado: “Administrador SNMP”. Como se muestra en la figura 31.

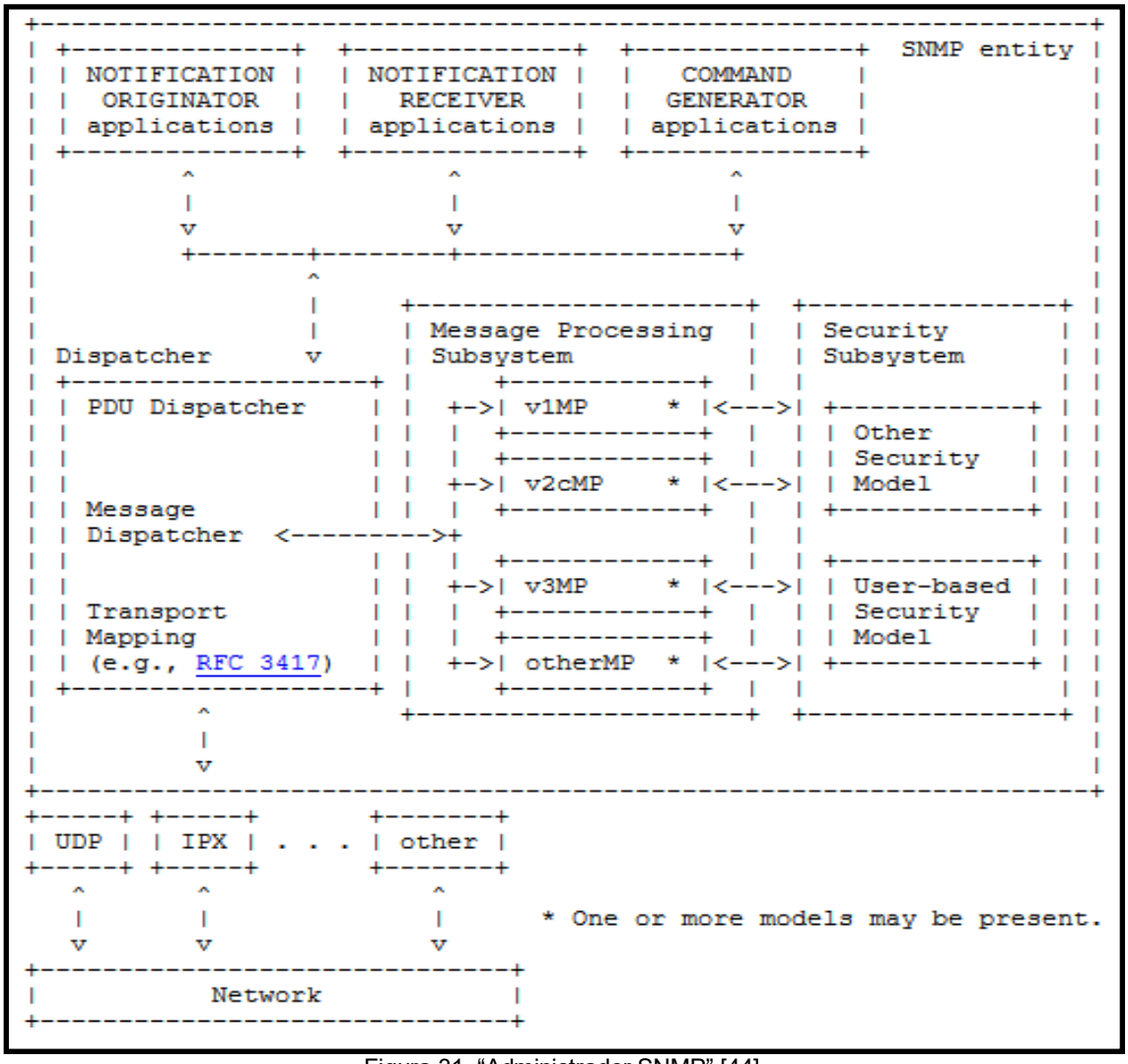


Figura 31. “Administrador SNMP” [44].

C.- SNMP Agent

Una entidad SNMP que contiene una o más aplicaciones de respuesta de comando y / o creador de notificaciones (junto con su motor SNMP asociado) se ha denominado: “Agente SNMP”. Como se muestra en la figura 32.

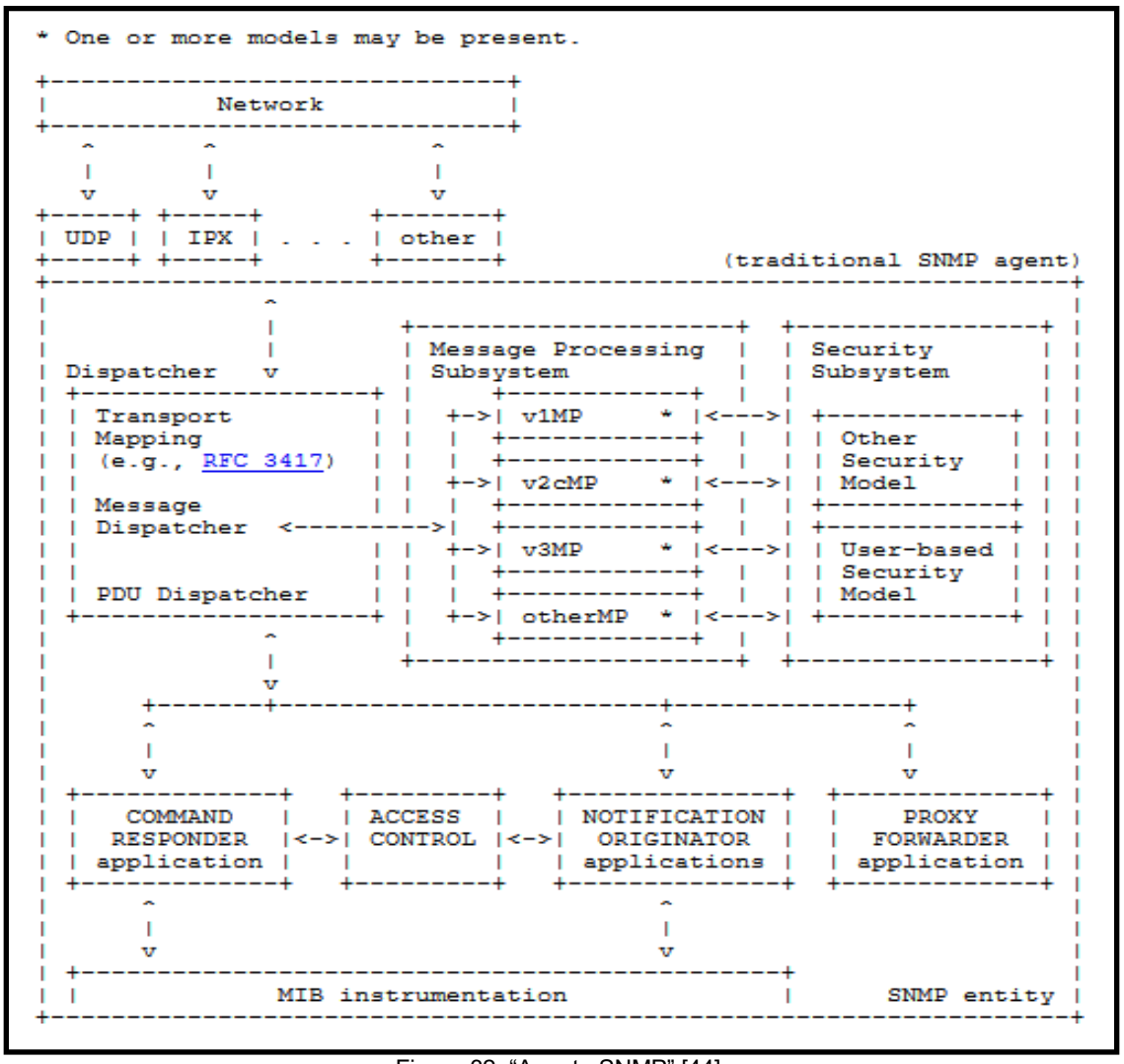


Figura 32. “Agente SNMP” [44].

D.- Estructura de la información de gestión – SMI

La SMI (*Structure of Management Information*) – Estructura de la Información de Gestión, el estándar especifica la forma en cómo se debe agrupar y nombrar la información de gestión. Cada objeto debe tener un nombre único, una sintaxis mediante la cual se escribe la MIB y una codificación, también define los datos que serán permitidos. En otras palabras, la SMI define la arquitectura con la cual se describe la MIB [45].

La arquitectura SMI contiene los siguientes elementos:

- **Identificadores de objetos (OID):** cada variable en SNMP tiene un identificador único, ya sea mediante un nombre (iso.org.dod.internet.mgm.mib-2) o en forma numérica (1.3.5.1.2.1). Los identificadores se establecen en orden jerárquico.

- **Tipos de objetos:** SMI define los tipos de objetos a utilizar como enteros, nulo, cadena de octetos e identificador de objetos. Para ello utiliza la notación ASN.1 (*Abstract Syntax Notation One* – Notación Sintáctica Abstracta 1. Lenguaje estandarizado por CCITT y la ISO), para definir la sintaxis sobre datos de aplicaciones, los cuales una vez aprobados se convierten en estándar.

- **Método de codificación de objetos:** Utiliza una cadena de octetos bajo el método BER (*Basic Encoding Rules* – Regla de Codificación Básica), que incluye tipo, etiqueta, longitud y valor para codificar a cada objeto junto con sus valores, para transmitirlos dentro de los paquetes SNMP.

E.- Base de datos de Información de Gestión – MIB

El MIB es una estructura de datos que describe a los elementos de la red SNMP como una lista de objetos de datos. Para monitorear dispositivos SNMP, el gestor SNMP debe compilar el archivo MIB para cada tipo de equipo en la red. Un OID se representa como una secuencia de enteros positivo en la que cada entero corresponde con un nodo particular en el árbol. Y este tipo de dato da un medio para identificar un objeto de gestión y relaciona su lugar en la jerarquía de objetos. Los identificadores de objetos de Internet empiezan con 1.3.6.1 y el subárbol de Internet (1) tiene 6 subárboles que se describen brevemente [46]:

- **directorio(1):** Describe como se debe usar las direcciones OSI en Internet.
- **mgmt(2):** Identifica objetos estándar registrados por la IANA (*Internet Assignet Numbers Authority*).
- **experimental(3):** Objetos de uso experimental empleados por el IETF, al convertirse en estándar se trasladan al mgmt(2).
- **privada(4):** Objetos definidos por un único grupo (por lo general un vendedor). Tiene un subárbol empresa(1) que permite a las empresas registrar sus objetos de red.
- **seguridad(5):** Aspectos de seguridad.
- **snmpv2(6):** Se reserva para tareas de gestión del SNMPv2, incluye información de objetos para dominio de transporte, y módulos de identificación.

En la figura 33 se observa el árbol identificador de objetos para objetos de Internet(1), en la que se indican 3 subárboles de donde parten algunos TRAP (mensaje de SNMP publicado por un agente que indica un evento o falla, es un código de programa que se usa para capturar errores e indicar dónde es que éste se encuentra) muy importantes para denotar eventos en la red.

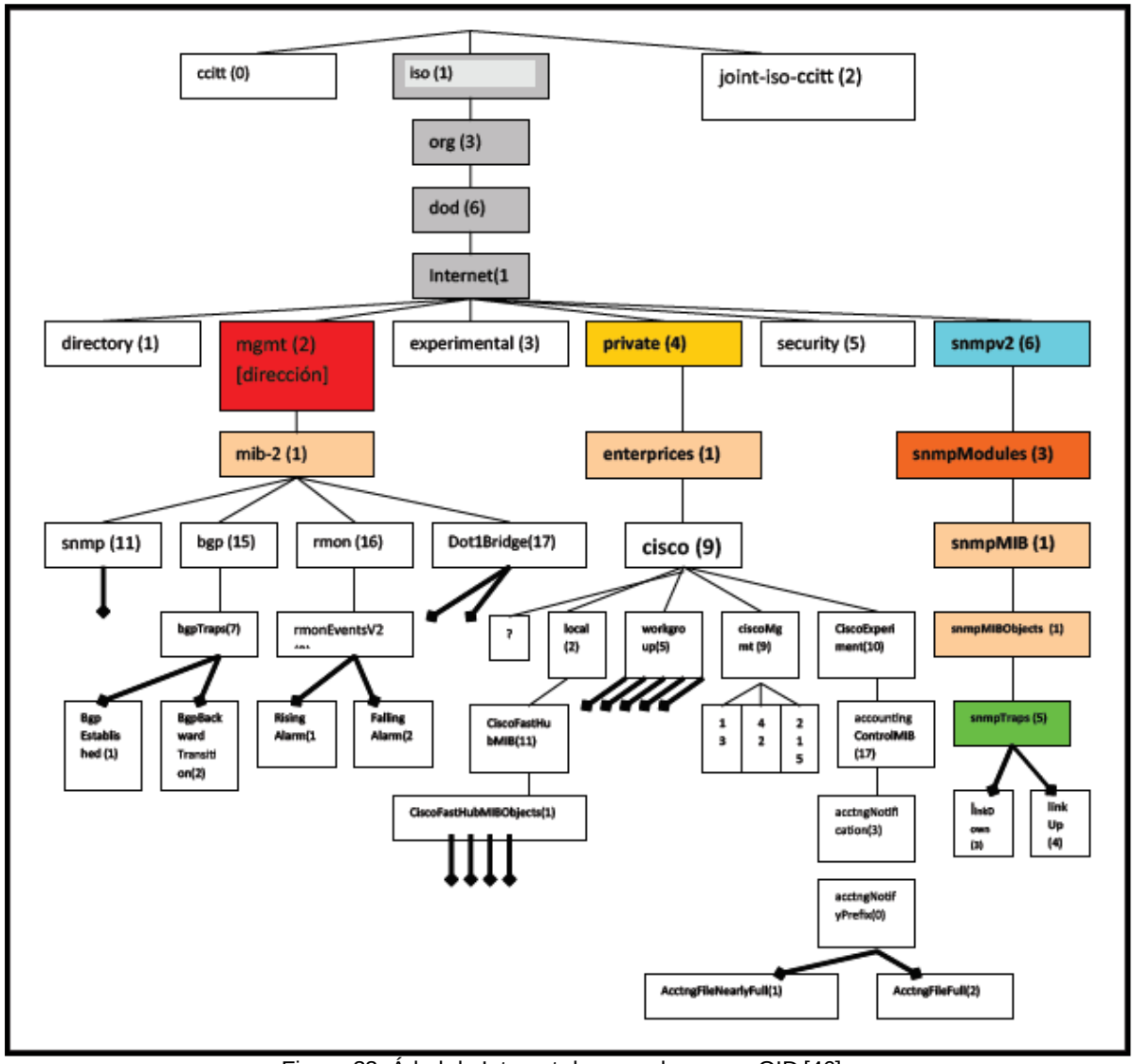


Figura 33. Árbol de Internet de acuerdo con su OID [46].

CAPÍTULO 3

Metodología para la emulación de la red AfricaConnect2.

3.1 Diferencia entre Simulador y Emulador

Packet Tracer es un simulador gráfico de redes, desarrollado por Cisco como herramienta de entrenamiento para sus estudiantes. El simulador provee un entorno gráfico para crear topologías de red y configurar los dispositivos utilizados. Además, ofrece realizar el análisis de los procesos ejecutados en el programa, convirtiendo así a la computadora donde se ha instalado, en un laboratorio de redes de datos [47]. Y GNS3 es un software emulador de IOS (*Internetwork Operating System* – Sistema Operativo de Interconexión), es un programa que crea una plataforma virtual, sobre la cual se ejecutan programas diseñados para otras plataformas distintas a las que se ejecutan en una computadora. Por ejemplo, en una computadora con algún tipo de S.O. (Sistema Operativo), se puede crear una máquina virtual cuyo S.O. sea de otra plataforma como: Ubuntu, Fedora, Windows 7 o Windows 10.

3.2 Recursos

GNS3 (*Graphical Networks Simulator* - Simulador de Red Grafica) es un software emulador de IOS de Routers Cisco, ASA Firewalls y Juniper. Está basado en Dynamips (emulador de routers Cisco), Dynagen (es un front-end para Dynamips) y PEMU (emulador de Cisco PIX firewall basado en Qemu), permite diseñar topologías de red para emularlas lo más cercano a la realidad, utilizando IOS de routers reales [48]. Por lo que después de instalar el emulador de GNS3, se procede a descargar los IOS del router c7200 [49], con éste tipo de router se realizará la emulación de conectividad y de gestión para AfricaConnect2. También se instala la aplicación de Oracle VM VirtualBox [50], versión 6.0.10, dentro de VirtualBox se instala una máquina virtual (VM) con S.O. Windows 10 con arquitectura de 64 bits [51]. Así también se instala en la VM la aplicación de Power SNMP Free Manager, versión 2.0 [52], y por último se instala la aplicación de iReasoning MIB Browser [53], versión 12, con la cual podremos llevar a cabo la emulación de gestión en AfricaConnect2.

3.3 Especificaciones técnicas para la emulación de la conectividad y de la gestión.

Para desarrollar la emulación de conectividad y gestión, se utilizó un equipo marca DELL, en el cual se ejecuta el sistema operativo Windows 10 con arquitectura de 64 bits, con las siguientes características:

- Procesador: Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz. Cuenta con 2 núcleos y 4 procesadores lógicos.
- Memoria instalada (RAM): 12 GB

En Windows 10 se instaló GNS3 versión 2.1.20, con licencia GLPv3 (*General Public License* – Licencia Pública General), versión más reciente hasta el momento para ejecutarse en plataformas de 64 bits.

3.4 Procesos para la conectividad de AfricaConnect2

Configurar una red de datos es funcional únicamente cuando se le ha configurado un protocolo de enrutamiento a cada uno de los routers que la conforman. De esta manera se garantiza que exista comunicación entre los distintos equipos de dicha red, con la finalidad de que establezcan relación de vecinos, para construir sus tablas de enrutamiento y, con ello, poder realizar la transmisión de paquetes de un punto a otro. Partiendo de esta idea, se utilizará el emulador GNS3 y las herramientas de análisis y diseño.

El diseño sobre GNS3 para las pruebas de emulación de conectividad y gestión se muestra en la figura 34.

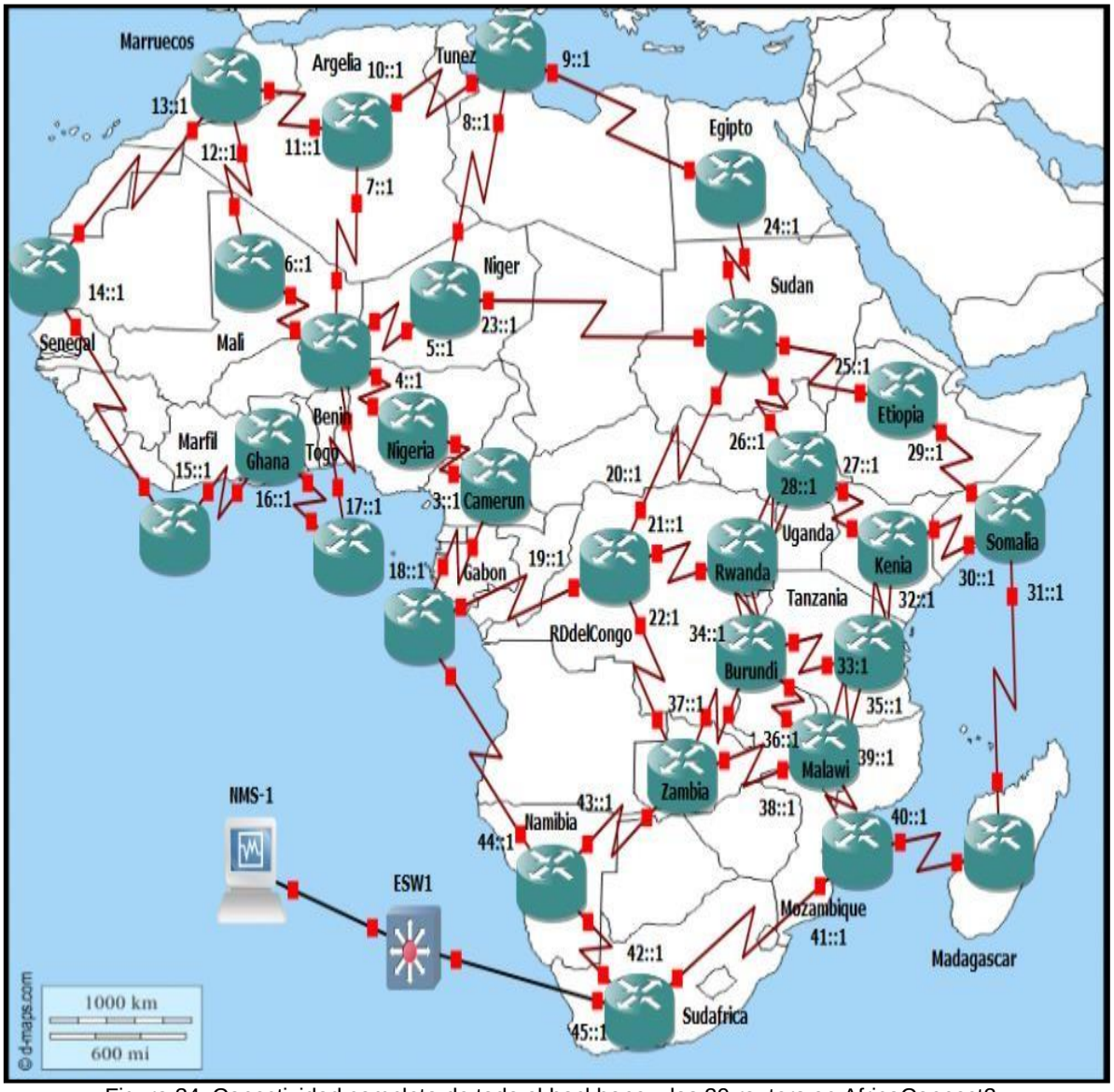


Figura 34. Conectividad completa de todo el backbone y los 29 routers en AfricaConnect2.

Cada uno de los 43 enlaces que conectan a los 29 routers que conforman la topología de AfricaConnect2 de la figura 34 deben utilizar una dirección de red, mediante la cual se puede establecer la comunicación entre dichos routers. En la tabla 4 se muestran las direcciones de red utilizadas en cada segmento que une a los routers. Las direcciones de red utilizadas están dentro del rango: 2019:3:3:3::1/64 al 2019:45:45:45::2/64. Obsérvese en sombreado aquellos routers con mayor número de enlaces y la conexión de la máquina virtual NMS1.

Enlaces	Direcciones de red
Argelia – Benín	2019:7:7:7::1/64
Argelia – Túnez	2019:10:10:10::1/64
Argelia - Marruecos	2019:11:11:11::1/64
Benín – Nigeria	2019:4:4:4::2/64
Benín – Níger	2019:5:5:5::2/64
Benín – Mali	2019:6:6:6::2/64
Benín – Argelia	2019:7:7:7::2/64
Benín – Togo	2019:17:17:17::2/64
Burundi - Tanzania	2019:33:33:33::2/64
Burundi - Rwanda	2019:34:34:34::1/64
Burundi - Malawi	2019:36:36:36::2/64
Burundi - Zambia	2019:37:37:37::2/64
Camerún - Nigeria	2019:3:3:3::1/64
Camerún - Gabón	2019:18:18:18::2/64
Egipto – Túnez	2019:9:9:9::2/64
Egipto – Sudan	2019:24:24:24::1/64
Etiopia – Sudan	2019:25:25:25::1/64
Etiopia - Somalia	2019:29:29:29::1/64
Gabón - Camerún	2019:18:18:18::1/64
Gabón - RDdelCongo	2019:19:19:19::2/64
Gabón - Namibia	2019:44:44:44::2/64
Ghana – Marfil	2019:15:15:15::2/64
Ghana – Togo	2019:16:16:16::1/64
Kenia – Uganda	2019:27:27:27::2/64
Kenia - Somalia	2019:30:30:30::2/64
Kenia - Tanzania	2019:32:32:32::1/64
Madagascar - Somalia	2019:31:31:31::2/64
Madagascar - Mozambique	2019:40:40:40::2/64
Malawi - Tanzania	2019:35:35:35::2/64
Malawi - Burundi	2019:36:36:36::1/64
Malawi - Zambia	2019:38:38:38::1/64
Malawi - Mozambique	2019:39:39:39::1/64
Mali – Benín	2019:6:6:6::1/64
Mali - Marruecos	2019:12:12:12::2/64
Marfil - Senegal	2019:14:14:14::2/64
Marfil – Ghana	2019:15:15:15::1/64

Tabla 4. Direcciones de enlace que conforman la topología de AfricaConnect2, parte 1/3.

Marruecos - Argelia	2019:11:11:11::2/64
Marruecos - Mali	2019:12:12:12::1/64
Marruecos - Senegal	2019:13:13:13::1/64
Mozambique - Malawi	2019:39:39:39::2/64
Mozambique - Madagascar	2019:40:40:40::1/64
Mozambique - Sudáfrica	2019:41:41:41::1/64
Namibia - Sudáfrica	2019:42:42:42::2/64
Namibia - Zambia	2019:43:43:43::1/64
Namibia - Gabón	2019:44:44:44::1/64
Níger – Benín	2019:5:5:5::1/64
Níger – Túnez	2019:8:8:8::2/64
Níger – Sudan	2019:23:23:23::1/64
Nigeria - Camerún	2019:3:3:3::2/64
Nigeria – Benín	2019:4:4:4::1/64
RDdelCongo - Gabón	2019:19:19:19::1/64
RDdelCongo - Sudan	2019:20:20:20::1/64
RDdelCongo - Rwanda	2019:21:21:21::1/64
RDdelCongo - Zambia	2019:22:22:22::1/64
Rwanda- RDdelCongo	2019:21:21:21::2/64
Rwanda - Uganda	2019:28:28:28::2/64
Rwanda - Burundi	2019:34:34:34::2/64
Senegal - Marruecos	2019:13:13:13::2/64
Senegal – Marfil	2019:14:14:14::1/64
Somalia - Etiopía	2019:29:29:29::2/64
Somalia – Kenia	2019:30:30:30::1/64
Somalia - Madagascar	2019:31:31:31::1/64
Sudáfrica - Mozambique	2019:41:41:41::2/64
Sudáfrica - Namibia	2019:42:42:42::1/64
Sudáfrica – NMS-1	2019:45:45:45::1/64
Sudan - RDdelCongo	2019:20:20:20::2/64
Sudán – Níger	2019:23:23:23::2/64
Sudán – Egipto	2019:24:24:24::2/64
Sudán – Etiopia	2019:25:25:25::2/64
Sudán – Uganda	2019:26:26:26::2/64
Tanzania – Kenia	2019:32:32:32::2/64
Tanzania - Burundi	2019:33:33:33::1/64
Tanzania – Malawi	2019:35:35:35::1/64
Togo – Ghana	2019:16:16:16::2/64
Togo – Benín	2019:17:17:17::1/64
Túnez – Níger	2019:8:8:8::1/64
Túnez – Egipto	2019:9:9:9::1/64
Túnez – Argelia	2019:10:10:10::2/64

Tabla 4. Direcciones de enlace que conforman la topología de AfricaConnect2, parte 2/3.

Uganda – Sudán	2019:26:26:26::1/64
Uganda – Kenia	2019:27:27:27::1/64
Uganda - Rwanda	2019:28:28:28::1/64
Zambia - RDdelCongo	2019:22:22:22::2/64
Zambia - Burundi	2019:37:37:37::1/64
Zambia - Malawi	2019:38:38:38::2/64
Zambia - Namibia	2019:43:43:43::2/64
NMS-1 - Sudáfrica	2019:45:45:45::2/64

Tabla 4. Direcciones de enlace que conforman la topología de AfricaConnect2, parte 3/3.

Para poder distinguir la procedencia de las rutas al realizar la consulta de alguna de las tablas de enrutamiento, a cada uno de los 29 routers se les asignó un identificador en formato de dirección IPv4. En la tabla 5 contiene el identificador para cada router, además, todo el backbone se encuentra en el "área 0".

Router	**Identificador**
Argelia	1.1.1.1
Túnez	2.2.2.2
Egipto	3.3.3.3
Níger	4.4.4.4
Marruecos	5.5.5.5
Senegal	6.6.6.6
Malí	7.7.7.7
Benín	8.8.8.8
Marfil	9.9.9.9
Ghana	10.10.10.10
Togo	11.11.11.11
Nigeria	12.12.12.12
Camerún	13.13.13.13
Gabón	14.14.14.14
RDdelCongo	15.15.15.15
Sudán	16.16.16.16
Etiopía	17.17.17.17
Uganda	18.18.18.18
Rwanda	19.19.19.19
Kenia	20.20.20.20
Somalia	21.21.21.21
Burundi	22.22.22.22
Tanzania	23.23.23.23
Zambia	24.24.24.24
Malawi	25.25.25.25
Mozambique	26.26.26.26
Madagascar	27.27.27.27
Namibia	28.28.28.28
Sudáfrica	29.29.29.29

Tabla 5. Asignación de número de identificador.

El enlace entre los routers utilizados en GNS3 se estableció mediante la conexión de interfaz F.O. (Fibra Óptica), la cual nos brinda 1Gbps, conexión máxima permitida en GNS3. Como se muestra en la figura 35.

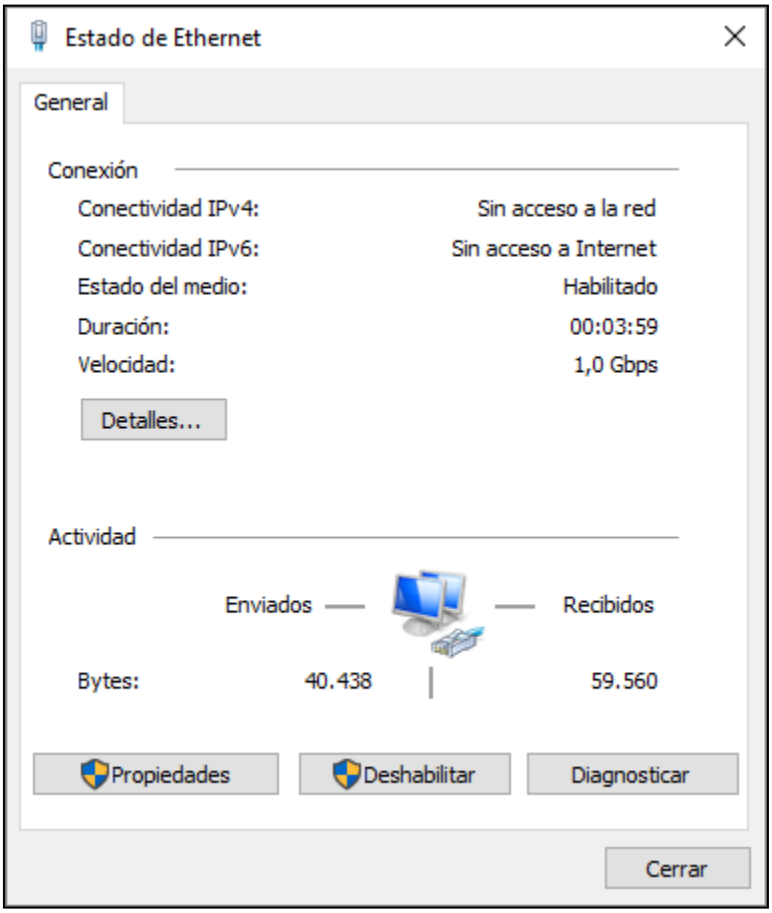


Figura 35. Conexión máxima permitida de 1Gbps.

Para lograr que los 29 routers c7200 construyan sus tablas de enrutamiento, se les configuró las interfaces que mantienen conexión con sus vecinos, asignándoles una dirección de red, de acuerdo a las consideraciones de la tabla 4. En la figura 36 muestra la configuración de una de las interfaces del router Gabón.

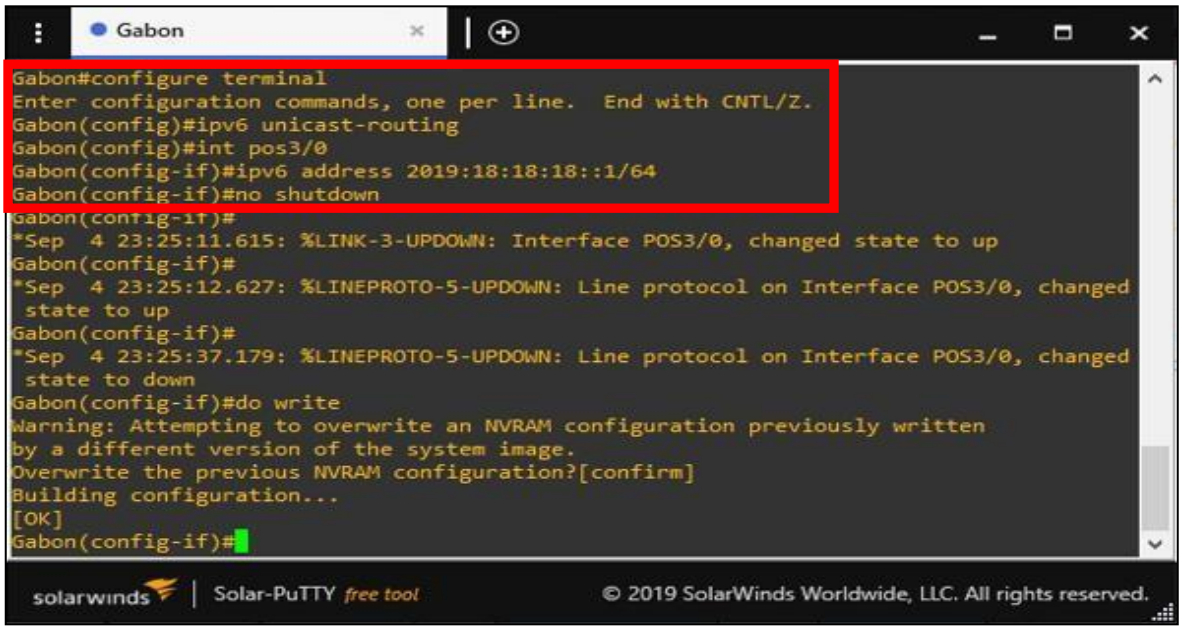


Figura 36. Configuración de una de las interfaces del router Gabón.

De ésta manera se configuran todos los enlaces de F.O. para cada uno de los 29 routers. El siguiente paso es activar el protocolo de enrutamiento OSPFv3 en el router correspondiente, como se muestra en la figura 37.

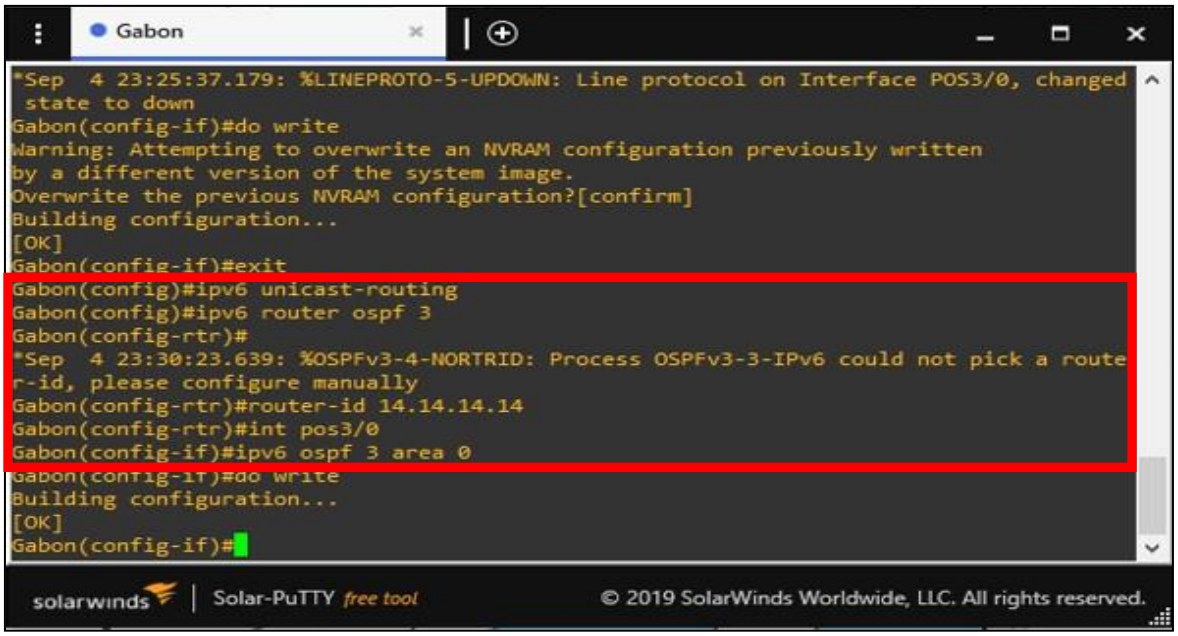


Figura 37. Configuración de OSPFv3 en el router Gabón.

De ésta manera también se configura el router vecino Camerún, como se muestra en la figura 38.

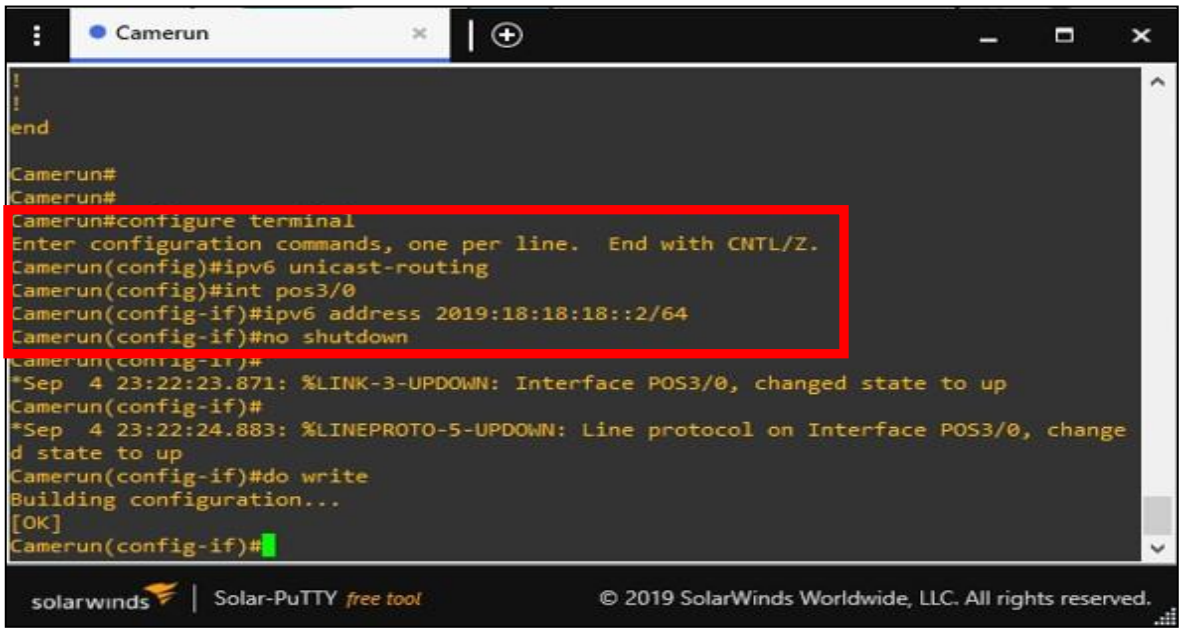


Figura 38. Configuración de una de las interfaces del router vecino Camerún.

También se configura el protocolo de enrutamiento OSPFv3 para el router vecino: Camerún, como se muestra en la figura 39.

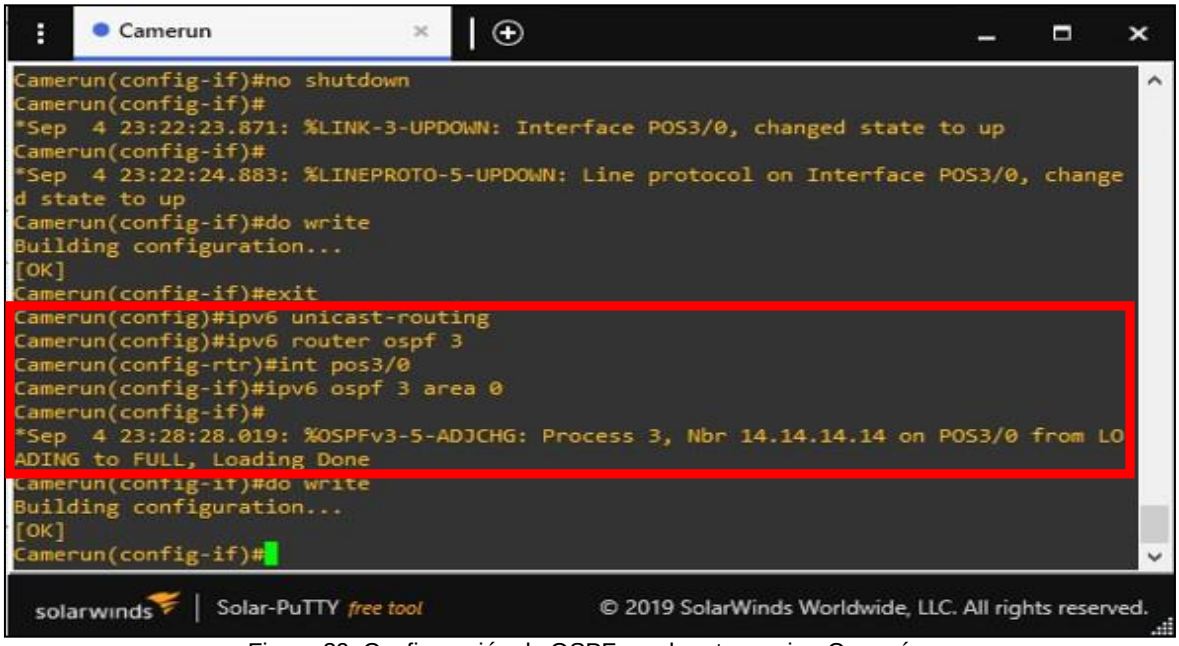


Figura 39. Configuración de OSPF en el router vecino Camerún.

De ésta manera nos podemos dar cuenta que ya están en comunicación el router Gabón y Camerún, ya que al momento de configurar el protocolo de enrutamiento OSPFv3 en el router de Camerún, nos indica que ya tenemos un vecino con un número de identificador (Nbr 14.14.14.14), como se muestra en la figura 39.

3.5 Proceso de configuración para la gestión de routers

Para poder llevar a cabo la gestión, primero se tuvo que configurar el protocolo de gestión SNMPv3 en cada uno de los 29 routers. Además de asignar los permisos de grupo establecido como: **AFRICA**, para poder acceder a la información de gestión, se toma como ejemplo el router Argelia. Para realizar la configuración como se muestra en la figura 40.

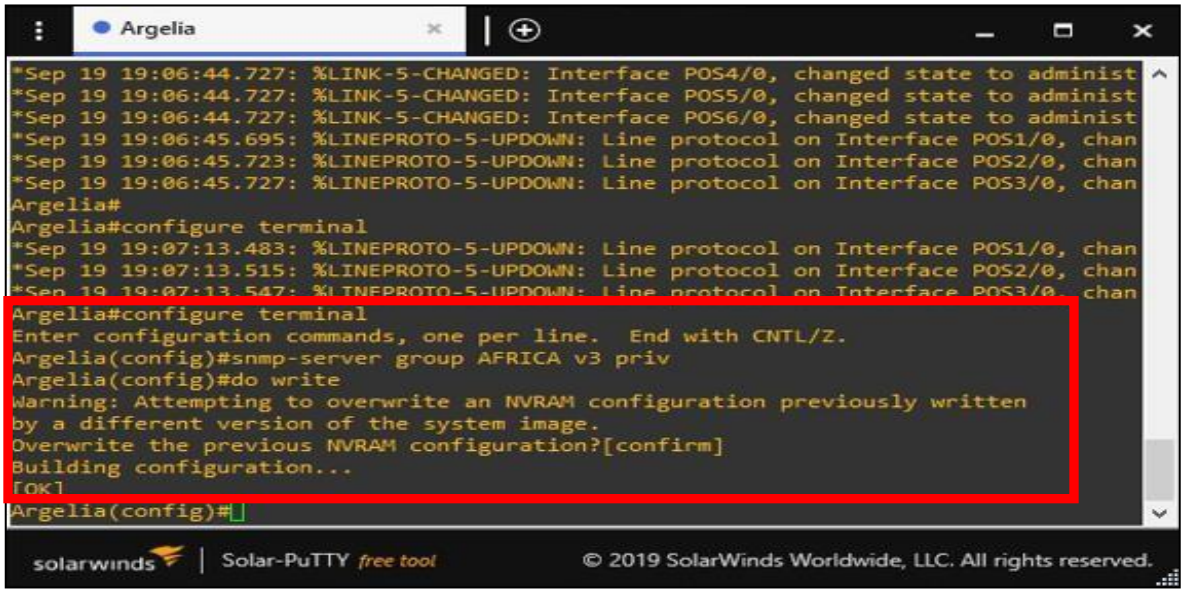


Figura 40. Configuración del protocolo de gestión SNMPv3.

Posteriormente se procedió a configurar el nombre del usuario del administrador de red, así también se asignó la dirección de interfaz del host que opera como gestor de la red. Como se muestra en la figura 41.

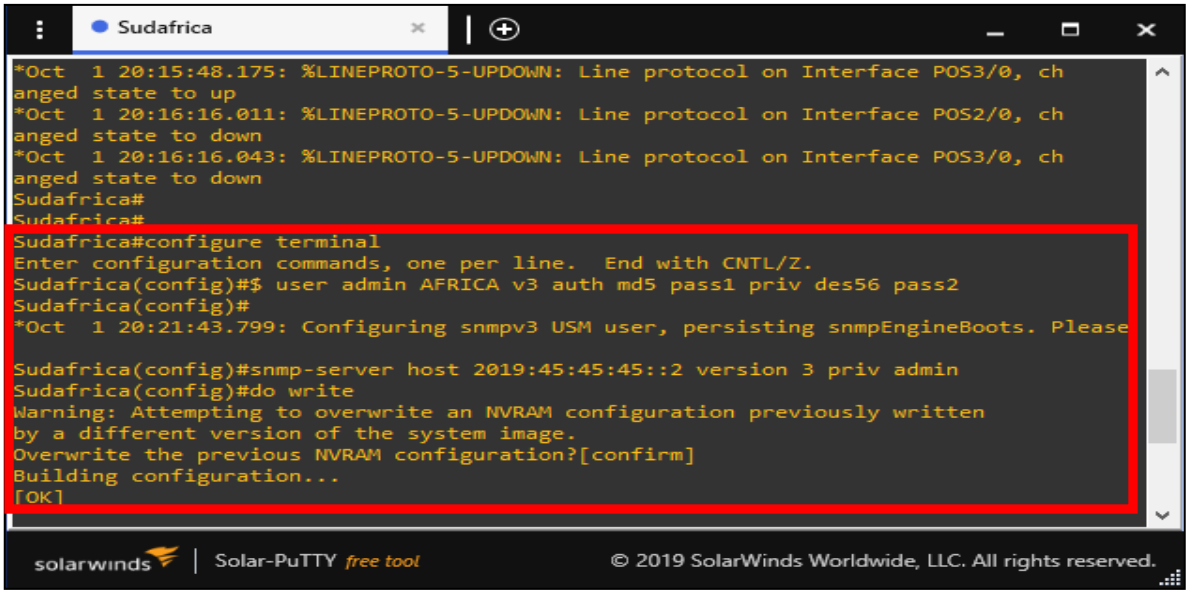


Figura 41. Configuración del nombre de usuario como administrador de red y la dirección de interfaz del host gestor de red.

En la figura 42 se puede validar la configuración correcta de los parámetros para nombre de usuario y nombre del grupo.

Figura 42. Configuración correcta de los parámetros para nombre de usuario y nombre de grupo.

3.6 Prueba de gestión de la red AfricaConnect2

Para monitorear de manera correcta y de forma segura nuestra red de AfricaConnect2, se utilizó el software PowerSNMP Free Manager, para tener comunicación constante entre la estación de gestión de red y los agentes configurados.

Una vez que se logró la configuración del protocolo de gestión SNMP en el agente del router, se realizó la configuración para los mensajes de Get, Set y Trap de SNMP, -Se enciende la máquina virtual llamada NMS, -Se abre PowerSNMP Free Manager para agregar los routers gestionados, -Seleccionamos SNMP Agents, -Add Agent. Como se muestra en la figura 43.

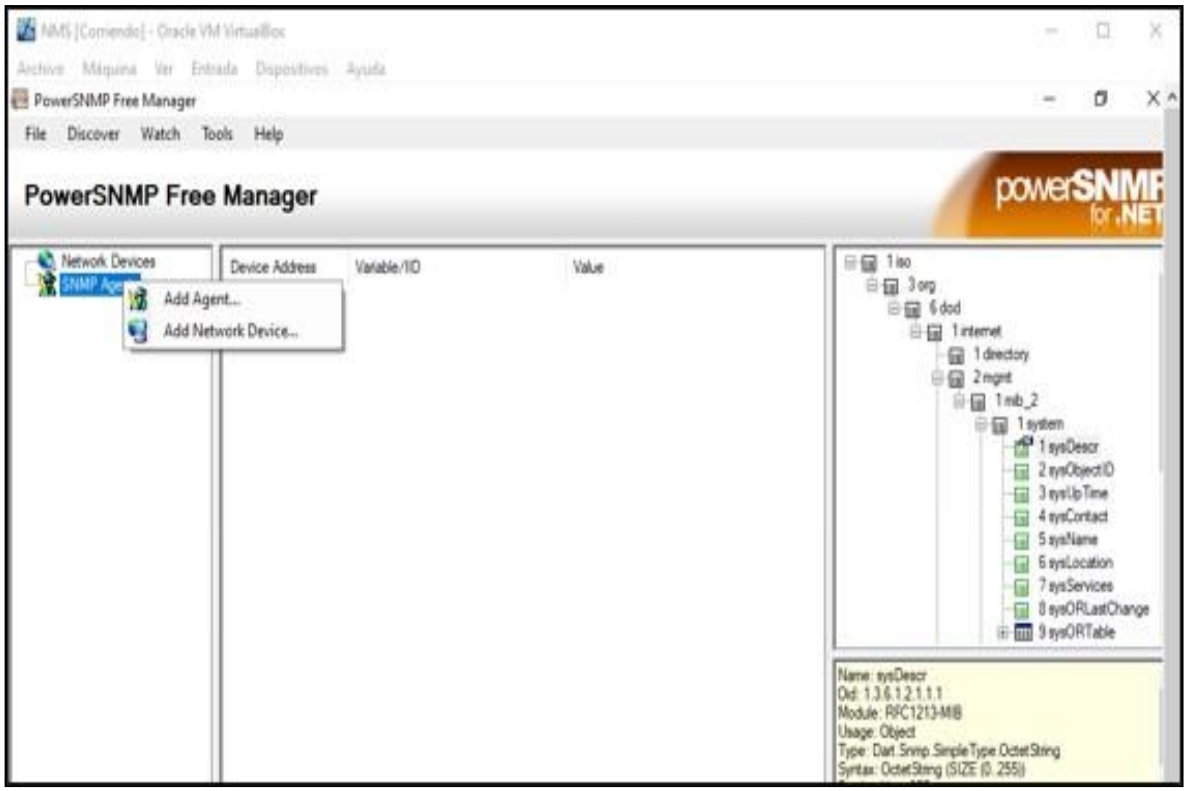


Figura 43. Forma de agregar un Agente al PowerSNMP Free Manager.

Posteriormente se configuró el agente, agregando la IPv6: 2019:45:45:45::1, que corresponde al router gestionado, puerto 161, versión 3, comunidad group, nombre de usuario, tipo de autenticación y privacidad para contraseña y protocolo. Como se muestra en la figura 44.

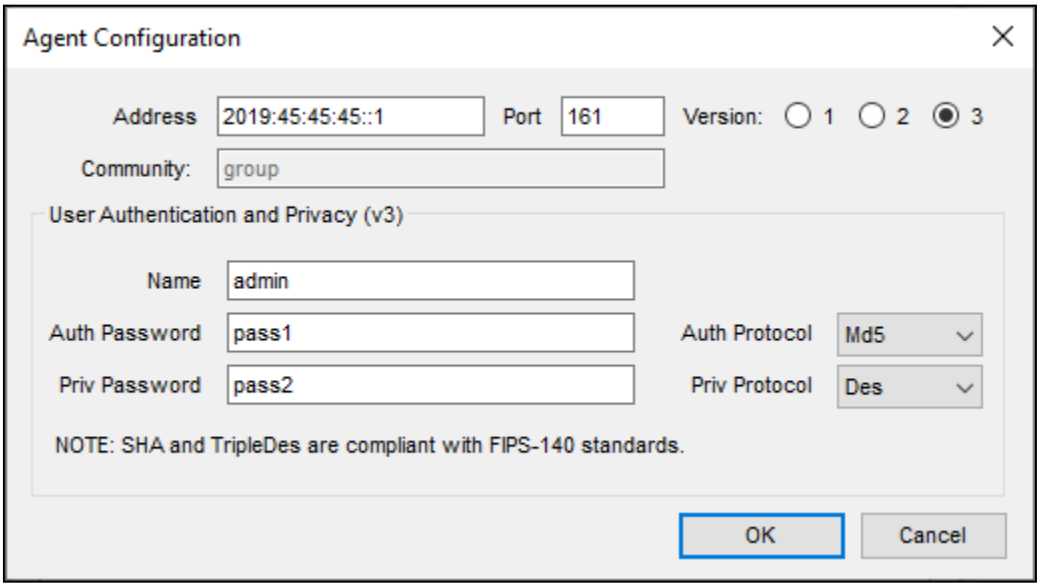


Figura 44. Parámetros configurados en el agente agregado.

De esta manera, una vez configurado los parámetros del agente, la aplicación PowerSNMP realiza la localización del mismo, indicándonos dirección, nombre y descripción. Como se muestra en la figura 45.

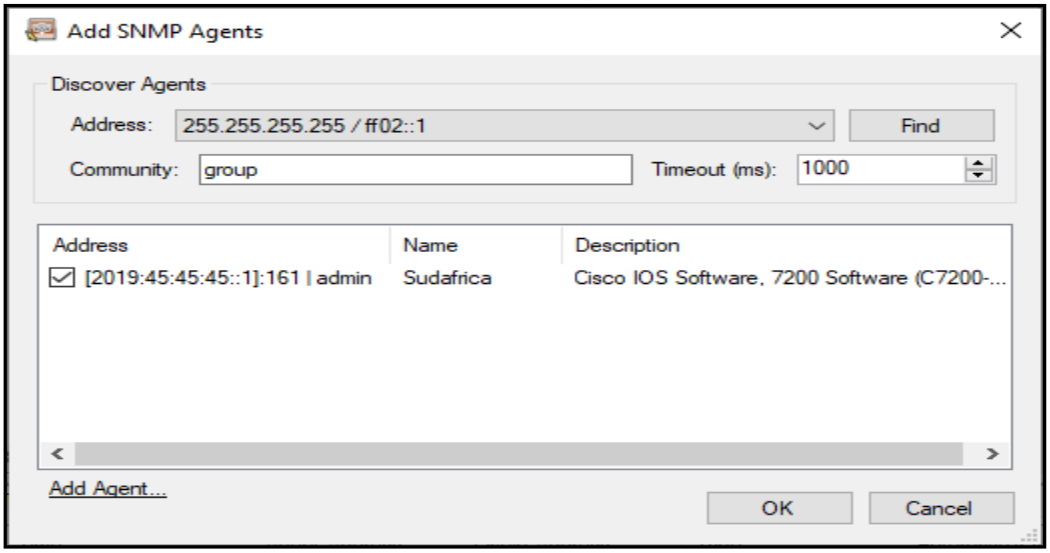


Figura 45. Detección del Agente Sudáfrica.

Para validar que efectivamente nos permita gestionar cualquier router de la red, se toma como ejemplo el router Sudáfrica. – En la parte superior izquierda de la aplicación PowerSNMP Free Manager, nos posicionamos en el subárbol sysName y enseguida dar click derecho y elegir la opción de consulta. Nos arroja un pequeño recuadro en donde nos muestra la dirección del router y el nombre como se muestra en la figura 46. De esta manera podemos validar que se puede llevar acabo la gestión, ya sea para la opción de sysName, sysDesc, sysUpTime, interfaces-ifNumber, ifOperStatus o lo que se requiera gestionar de la red.

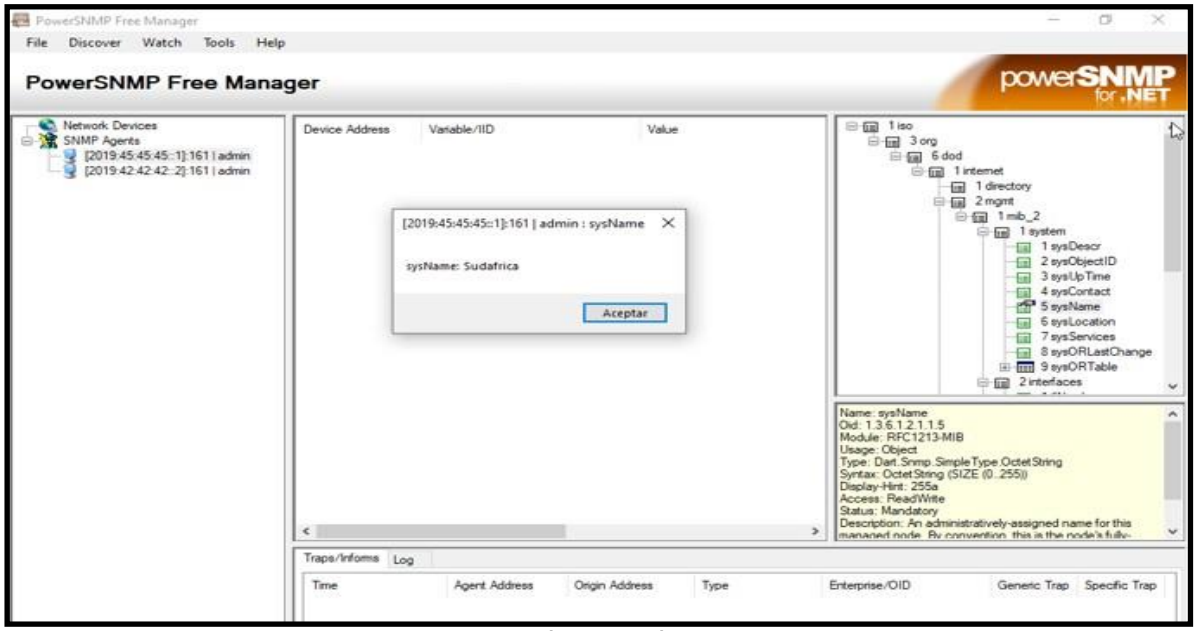


Figura 46. Gestión del subárbol sysName.

Finalmente se agregan los 29 agentes a gestionar, como se muestra en la figura 47.

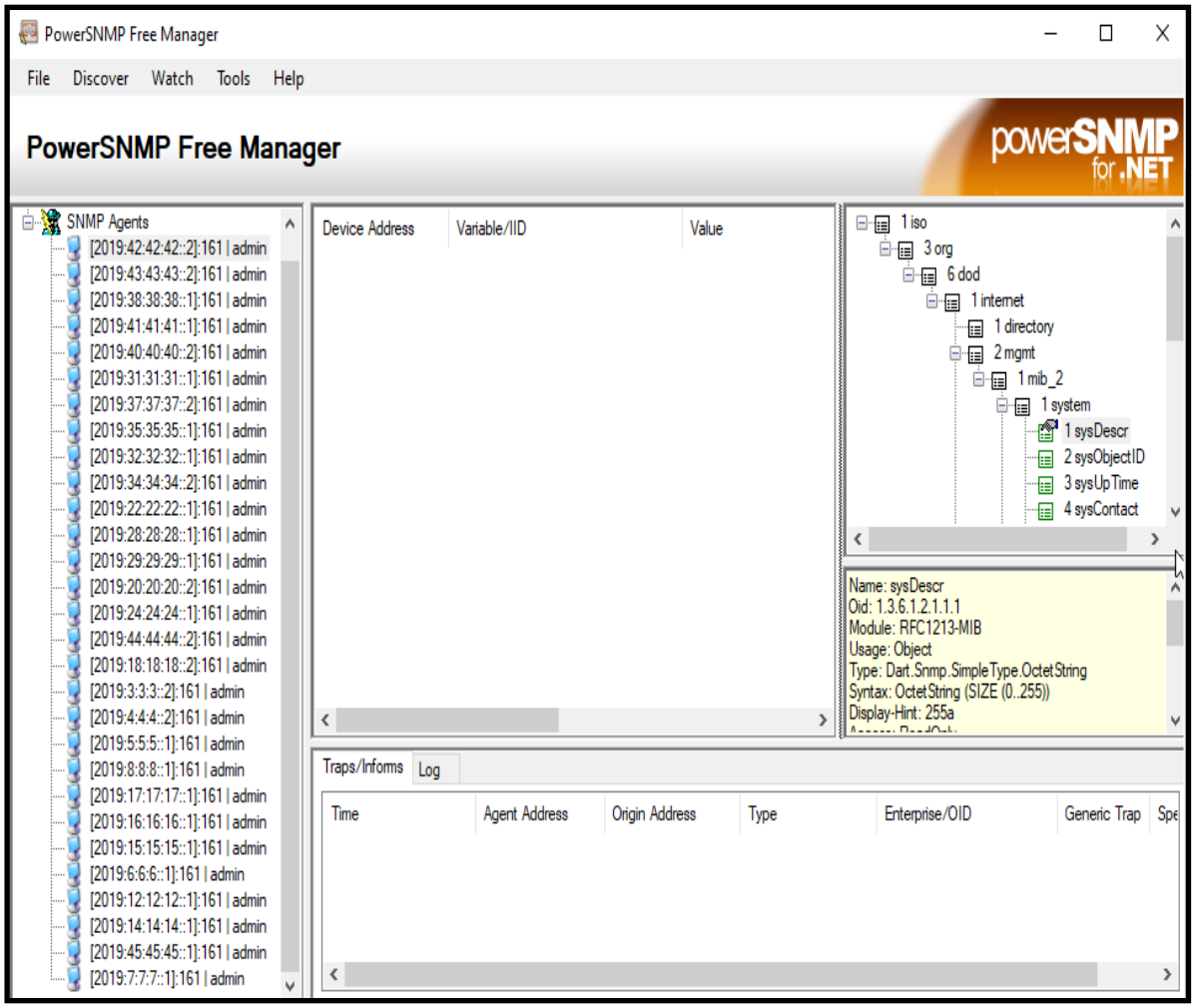


Figura 47. Agentes agregados para gestionar.

CAPÍTULO 4

Resultados de la emulación de la conectividad y de la gestión.

4.1 Resultados de la conectividad

Para indicar la conectividad de los primeros 14 routers (ASREN y WACREN), se realiza un ping desde la interfaz: 2019:18:18:18::2/64 del router Camerún a la interfaz: 2019:18:18:18::1/64 del router Gabón. Como se muestra en la figura 48.

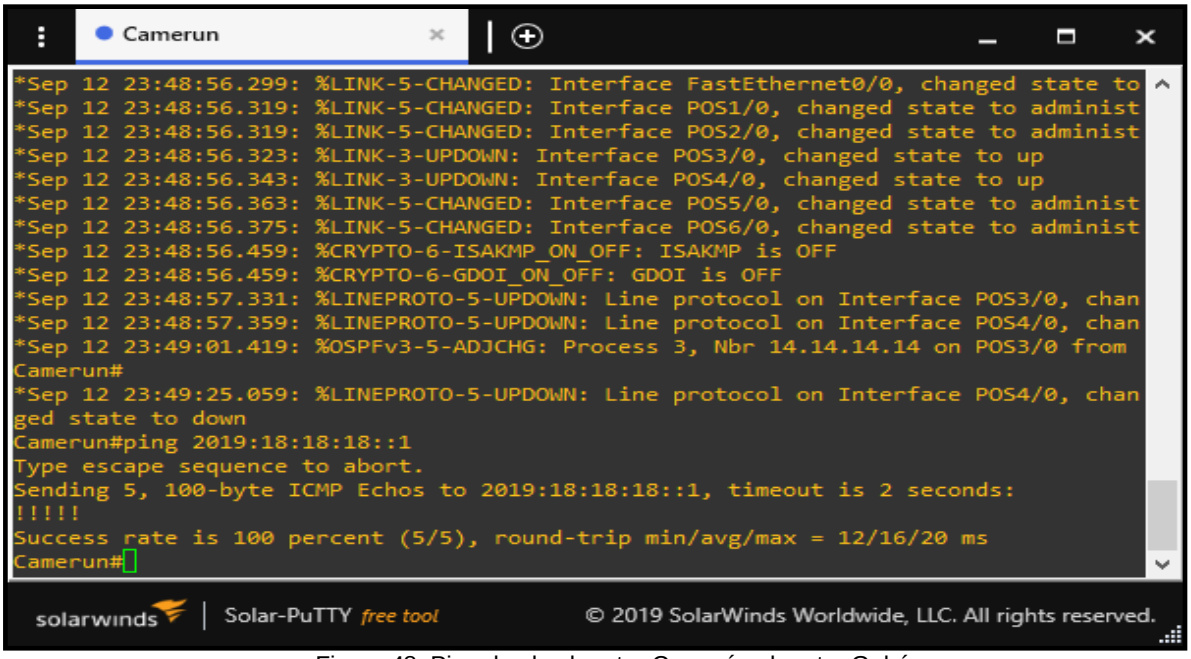


Figura 48. Ping desde el router Camerún al router Gabón.

En la figura 49 se muestra el consumo de Memoria y CPU del emulador, para los socios de África del Norte (ASREN), África Occidental y Central (WACREN).

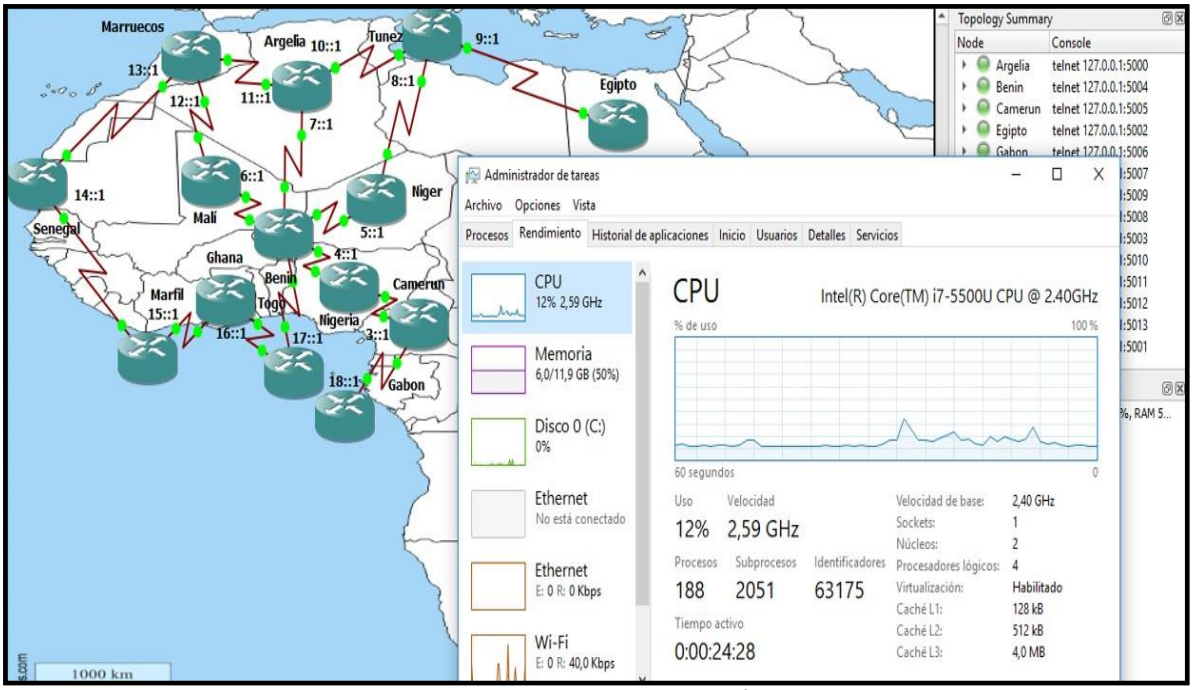


Figura 49. Consumo de memoria y CPU de la emulación de ASREN y WACREN.

Para confirmar la conectividad de los primeros 14 routers (ASREN y WACREN), se realizan 3 ping a los routers: Argelia, Egipto y Senegal, desde el router Gabón. Como se muestra en la figura 50.

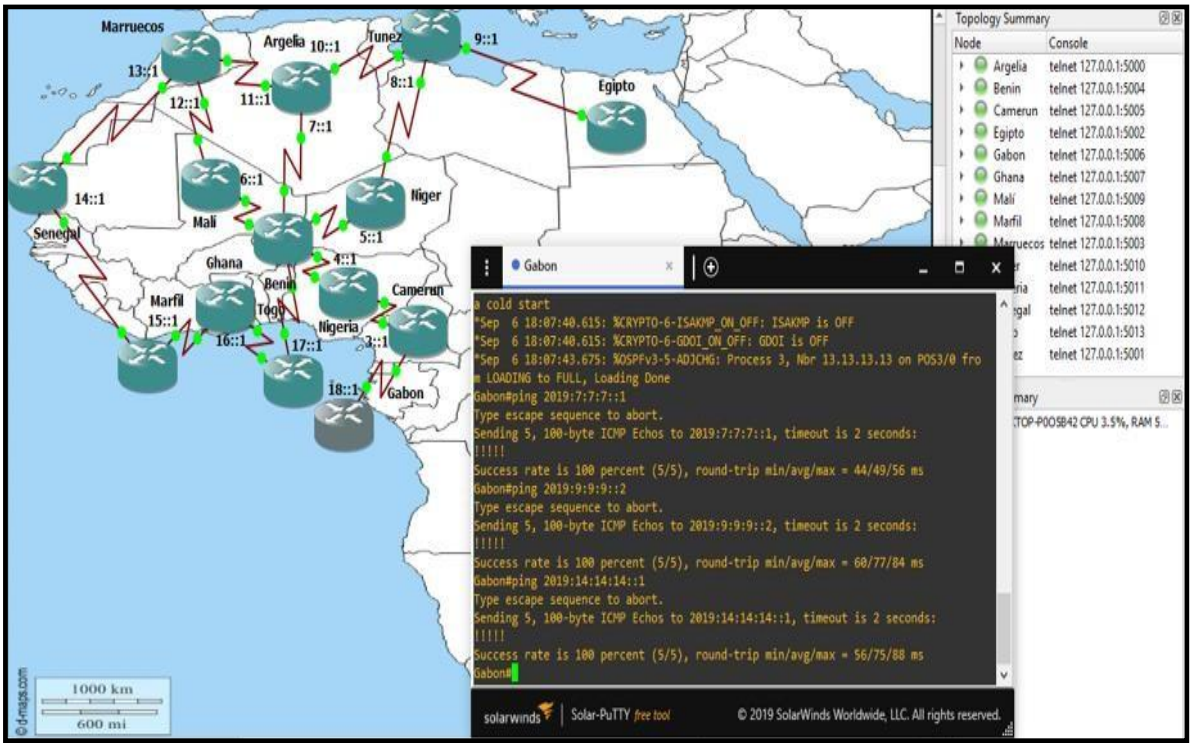


Figura 50. Ping a los routers: Argelia, Egipto y Senegal.

En la figura 51 se muestra la conectividad completa de los 29 routers de AfricaConnect2, así como también el rendimiento de nuestra VM NMS-1.

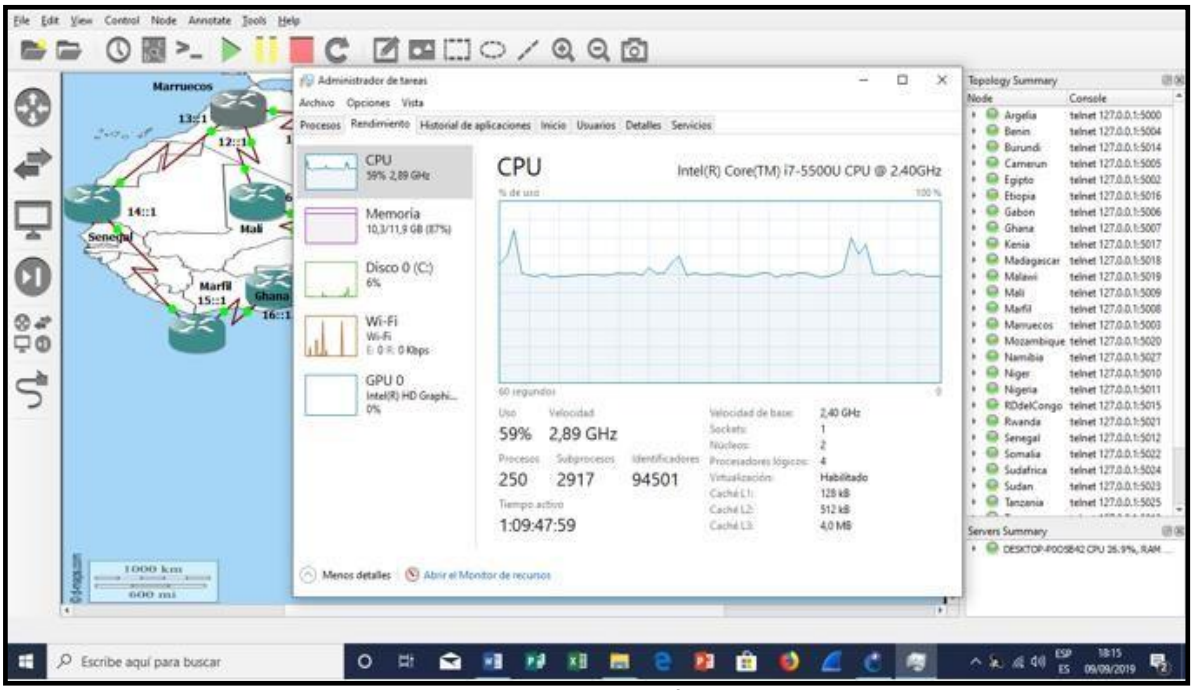


Figura 51. Consumo de memoria y CPU de la emulación de los 29 routers de AfricaConnect2.

En la figura 52 se realiza 1 ping a los routers: Senegal, Túnez, Egipto, Etiopia y Madagascar, desde el router Sudáfrica. Esto para validar la conectividad completa de los 29 routers.

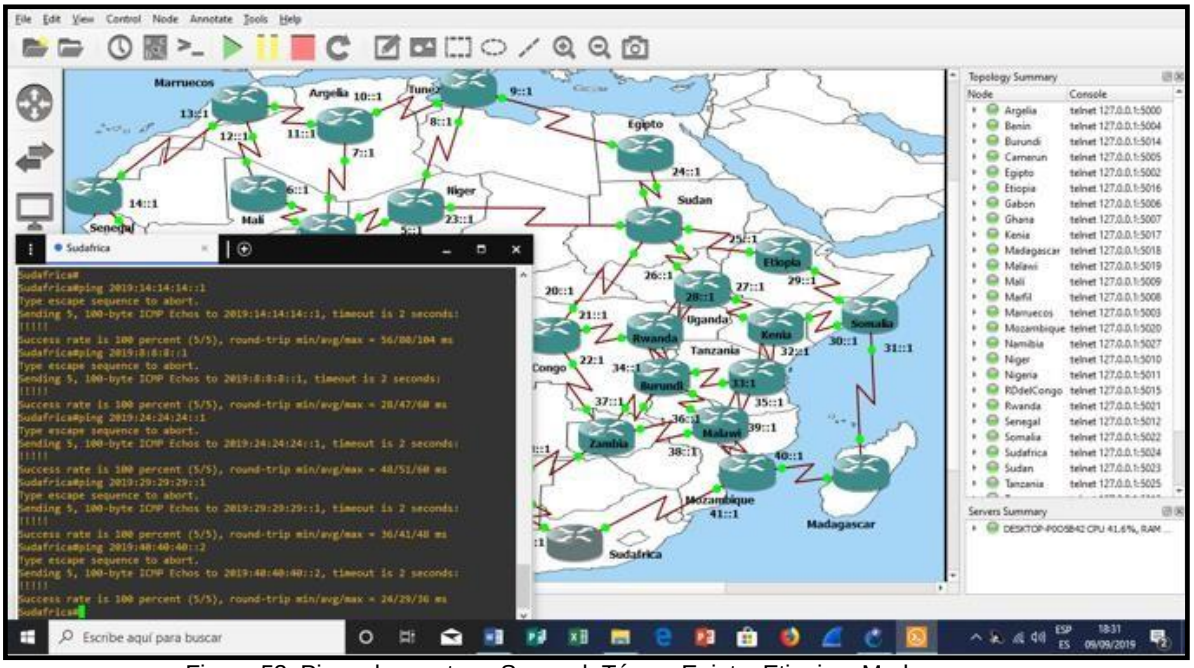


Figura 52. Ping a los routers: Senegal, Túnez, Egipto, Etiopia y Madagascar.

Otra forma de verificar que los routers han establecido relación de vecinos es a través del análisis de la tabla de enrutamiento, en la cual deben aparecer por lo menos las rutas de los routers vecinos. La tabla se consigue a través del mando “show ipv6 route”, la cual se ejecuta mediante el router Sudáfrica. Ver figura 53.

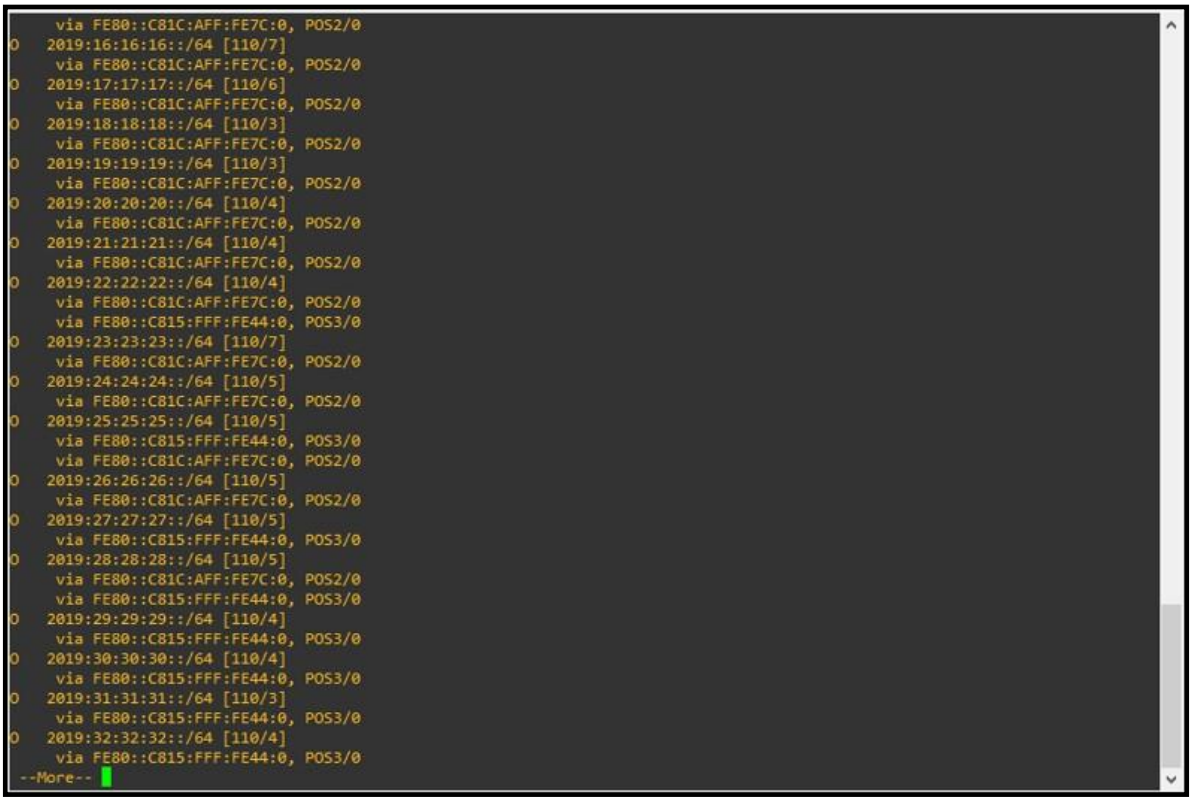
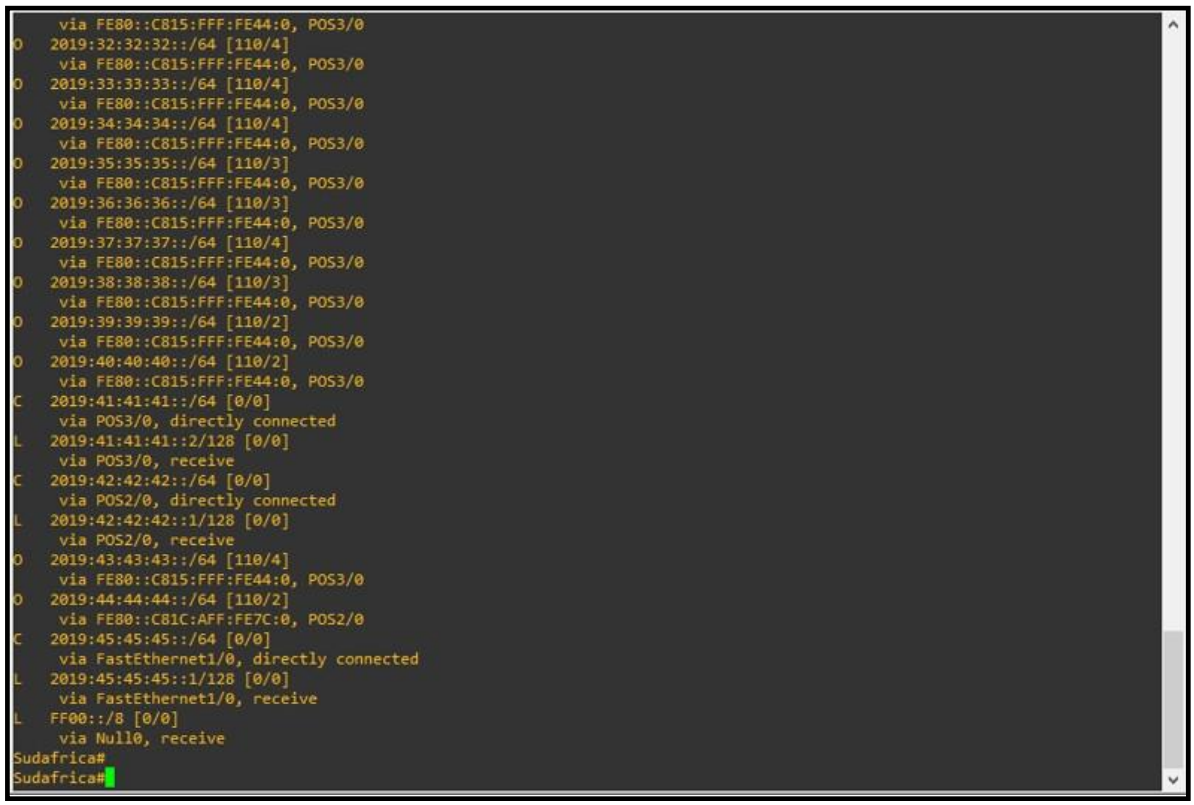


Figura 53. Tabla de enrutamiento del router Sudáfrica, parte 2/3.



En la figura 54 se indica la conectividad habilitando a todo el backbone y la VM NMS-1 en AfricaConnect2.

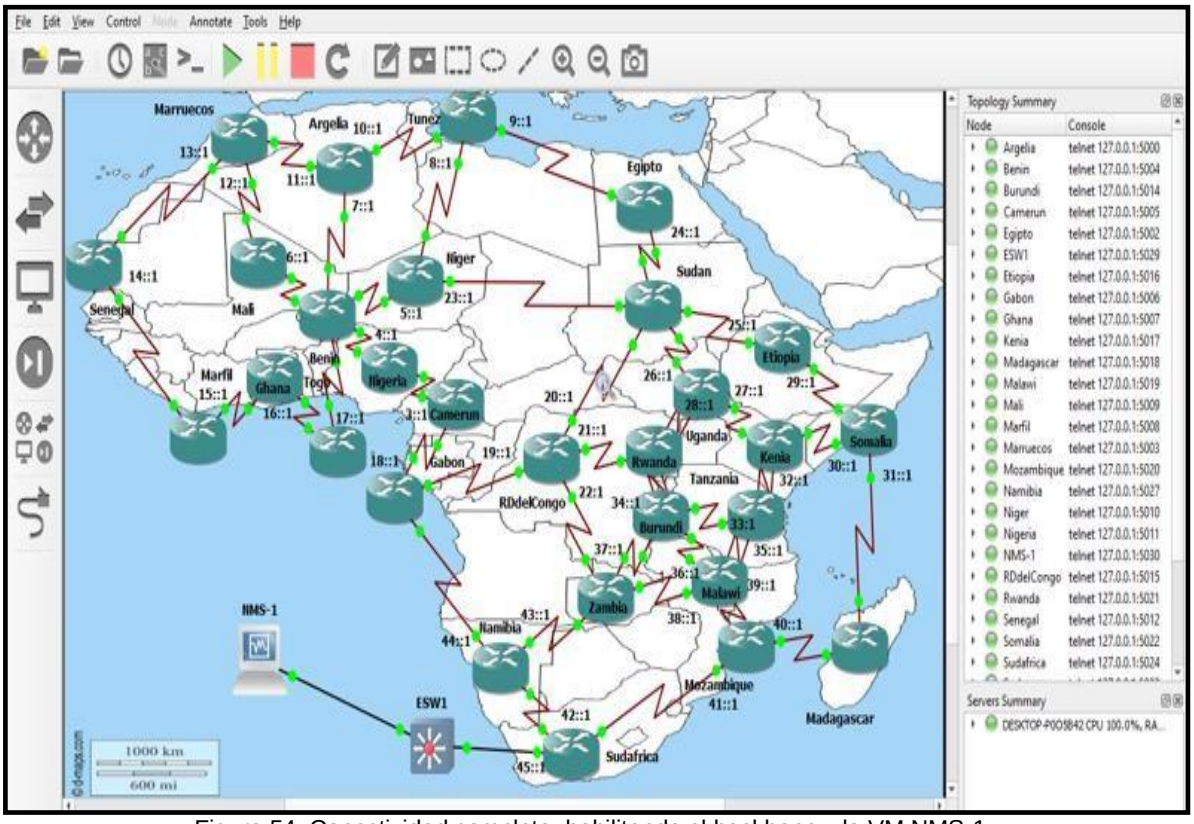


Figura 54. Conectividad completa, habilitando el backbone y la VM NMS-1.

En la figura 55 se indica el consumo de memoria una vez que se ha habilitado a todo el backbone y la VM NMS-1 en AfricaConnect2.

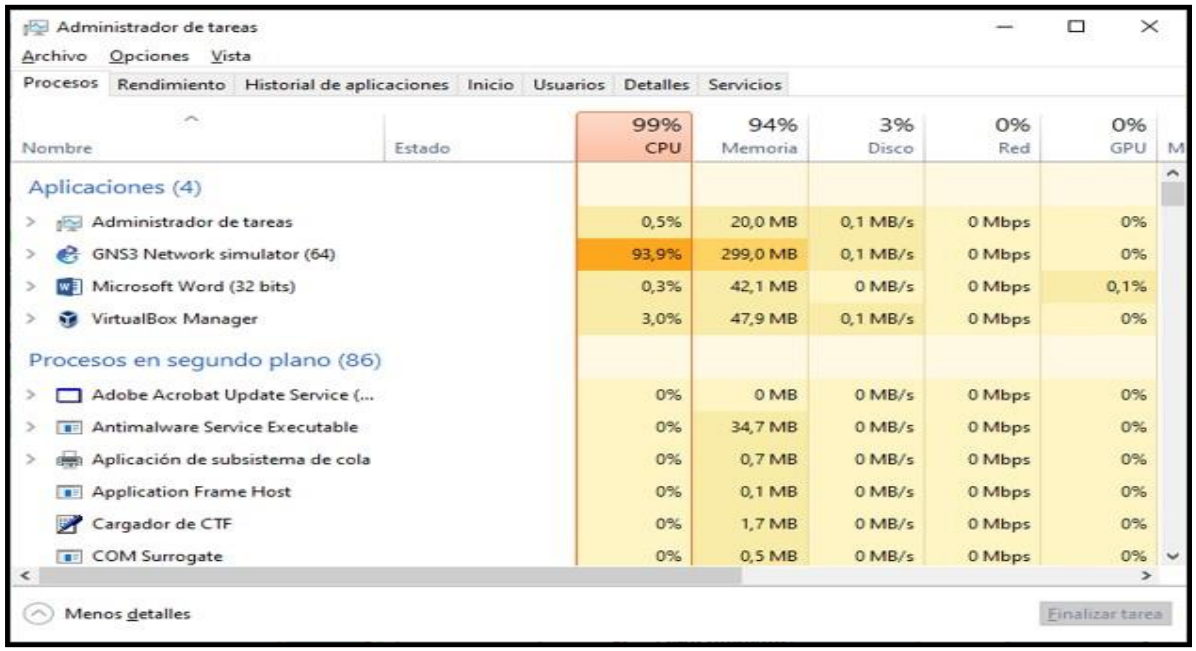


Figura 55. Consumo de Memoria y CPU, para la emulación de AfricaConnect2.

En la figura 56 se muestra la captura de los 5 tipos de paquetes OSPFv3 generados por los routers Sudán y RDdelCongo, a través de la aplicación Wireshark.

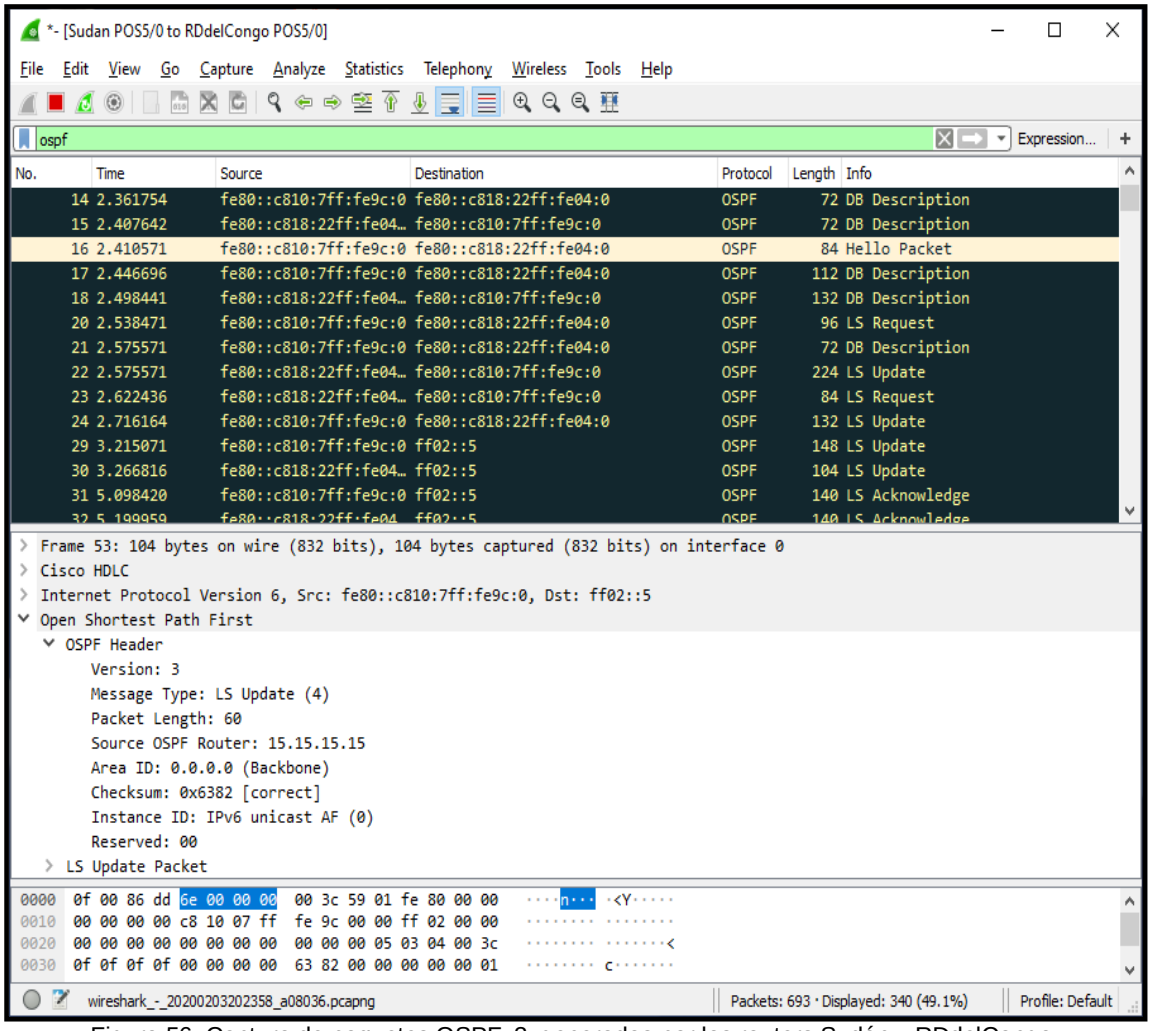


Figura 56. Captura de paquetes OSPFv3, generados por los routers Sudán y RDdelCongo.

4.2 Resultados de la gestión

Para indicar los resultados de la gestión, utilizamos la aplicación de iReasoning MIB Browser. Una vez instalado la aplicación en nuestra VM (NMS), procedemos a abrir la misma. –En el apartado de Address se coloca la IP de nuestro router Sudáfrica. -En el apartado Advanced se ingresan los parámetros del Agente para tener acceso a la información de gestión como se muestra en la figura 57. Así también se realiza el mismo proceso para el router Túnez.

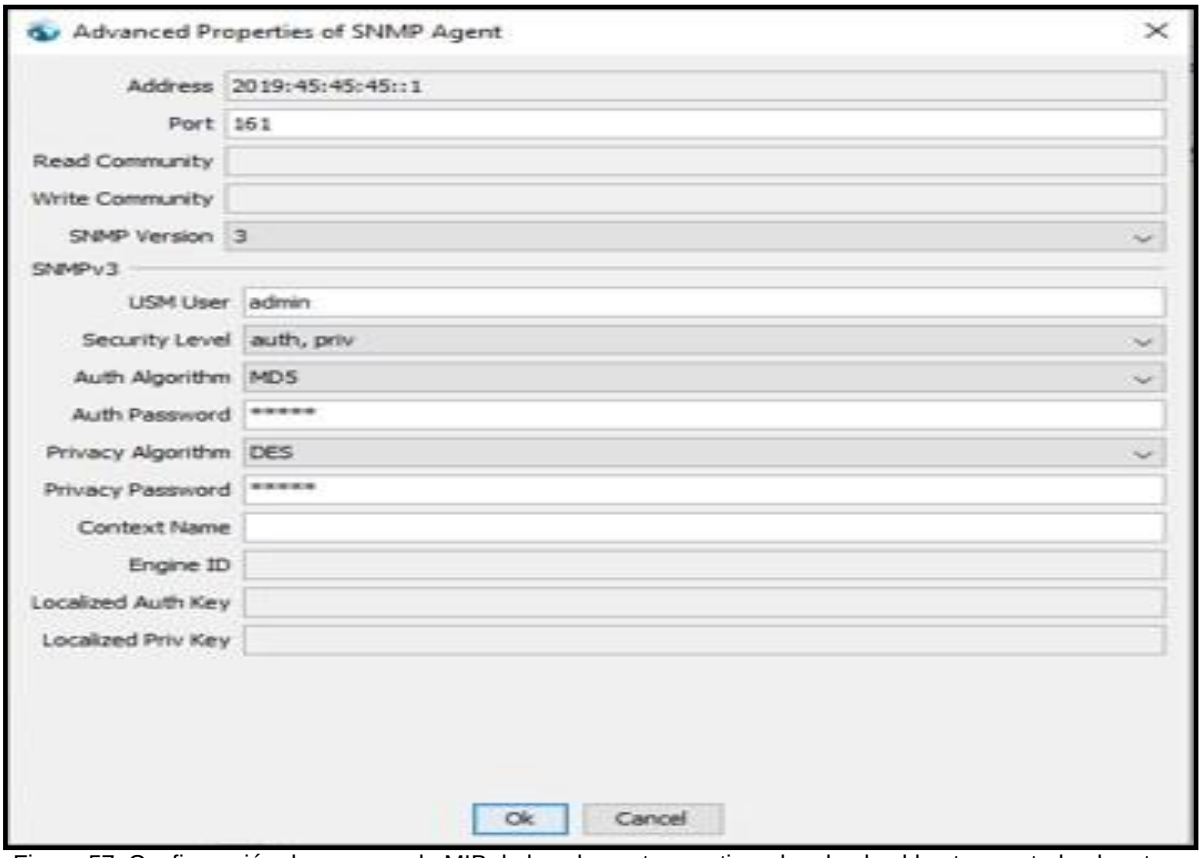


Figura 57. Configuración de acceso a la MIB de los elementos gestionados desde el host conectado al router Sudáfrica.

Para los resultados de la emulación de gestión, se toman las siguientes 6 variables, para el router Sudáfrica y Túnez:

1. sysName
2. ifNumber
3. ifTable
4. ifDescr
5. ifOperStatus
6. sysUpTime

4.2.1 sysName para el router Sudáfrica

En la figura 58 muestra el valor contenido en la variable sysName, el valor de la variable se obtiene mediante la operación Get.

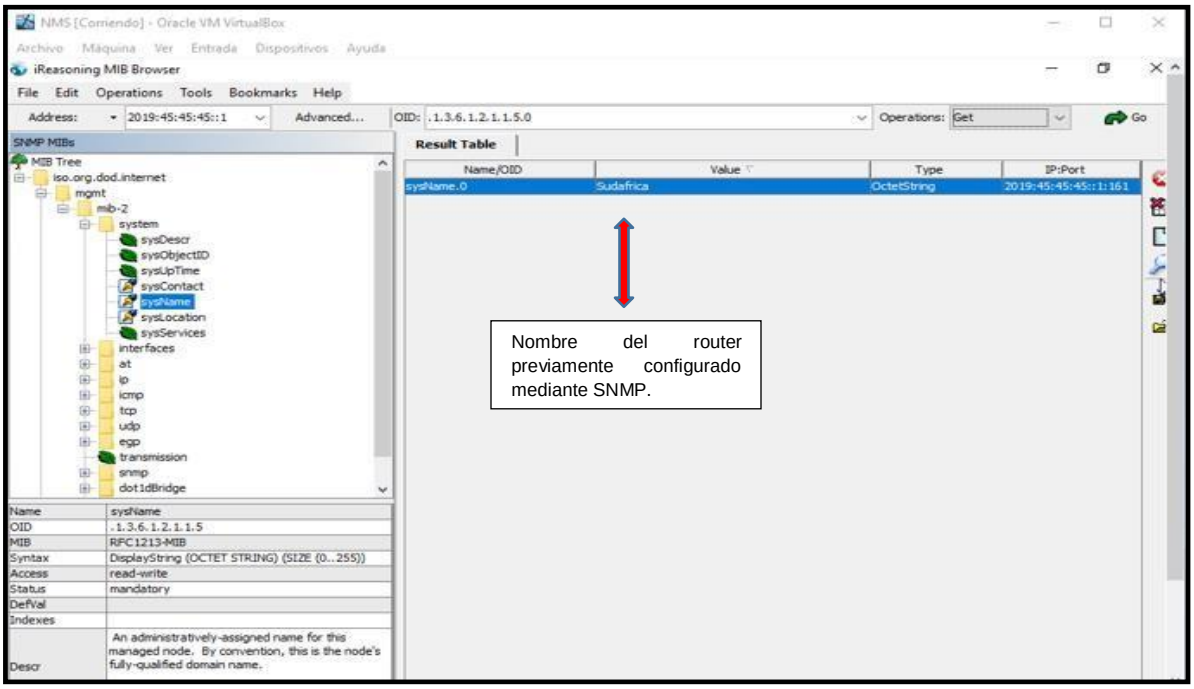


Figura 58. Monitoreo de la variable sysName.

4.2.2 ifNumber para el router Sudáfrica

En la figura 59 muestra el valor de la variable ifNumber, obtenido mediante la operación Get.

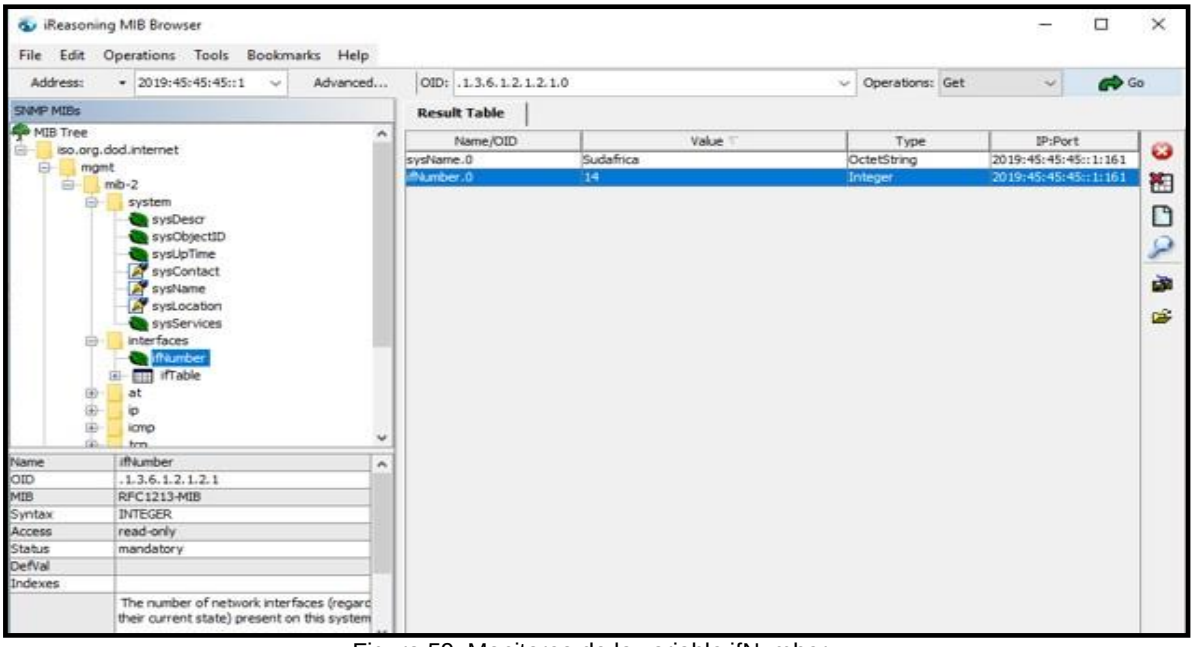


Figura 59. Monitoreo de la variable ifNumber.

4.2.3 ifTable para el router Sudáfrica

En la figura 60 muestra los valores de la variable ifTable, obtenidos mediante la operación Table-View.

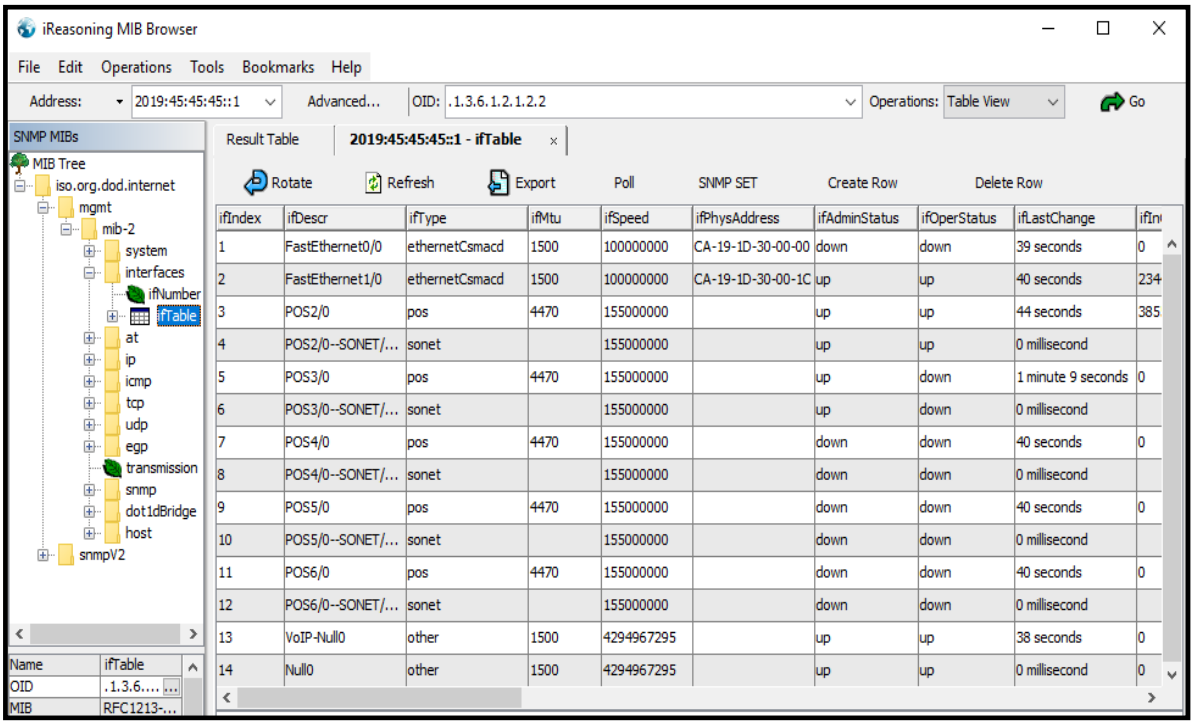


Figura 60. Monitoreo de la variable ifTable, parte 1/3.

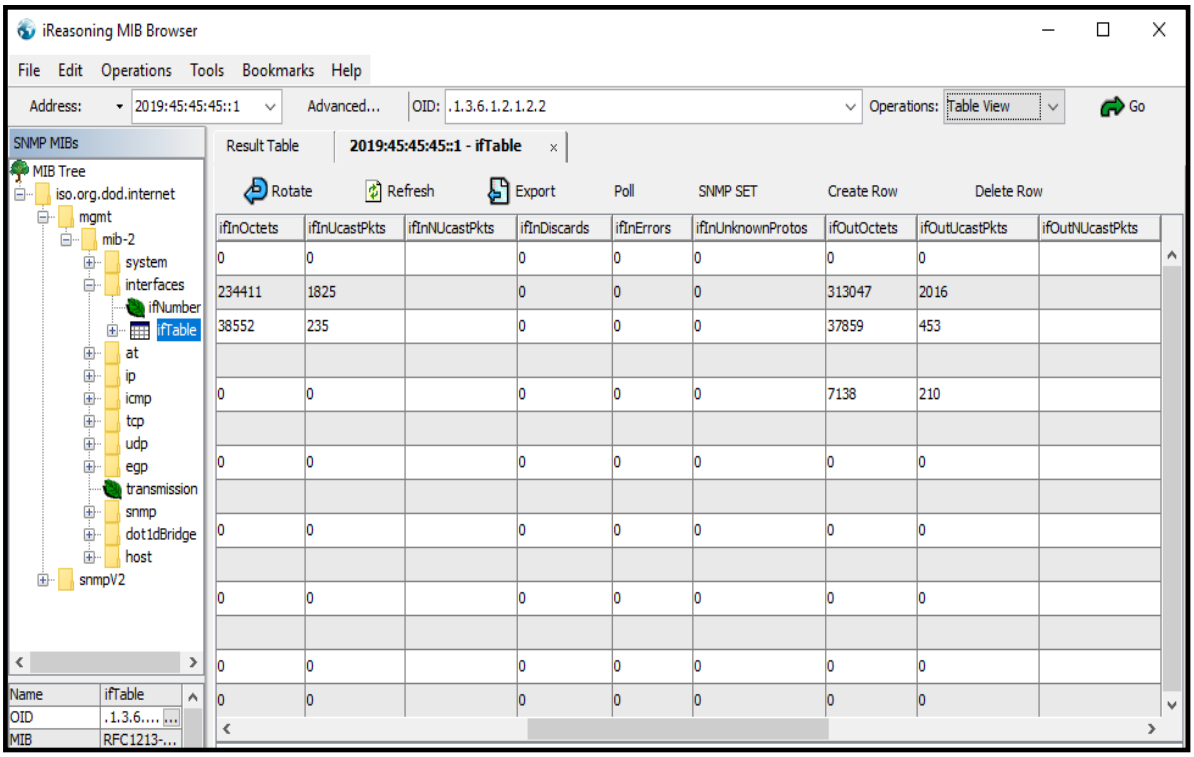


Figura 60. Monitoreo de la variable ifTable, parte 2/3.

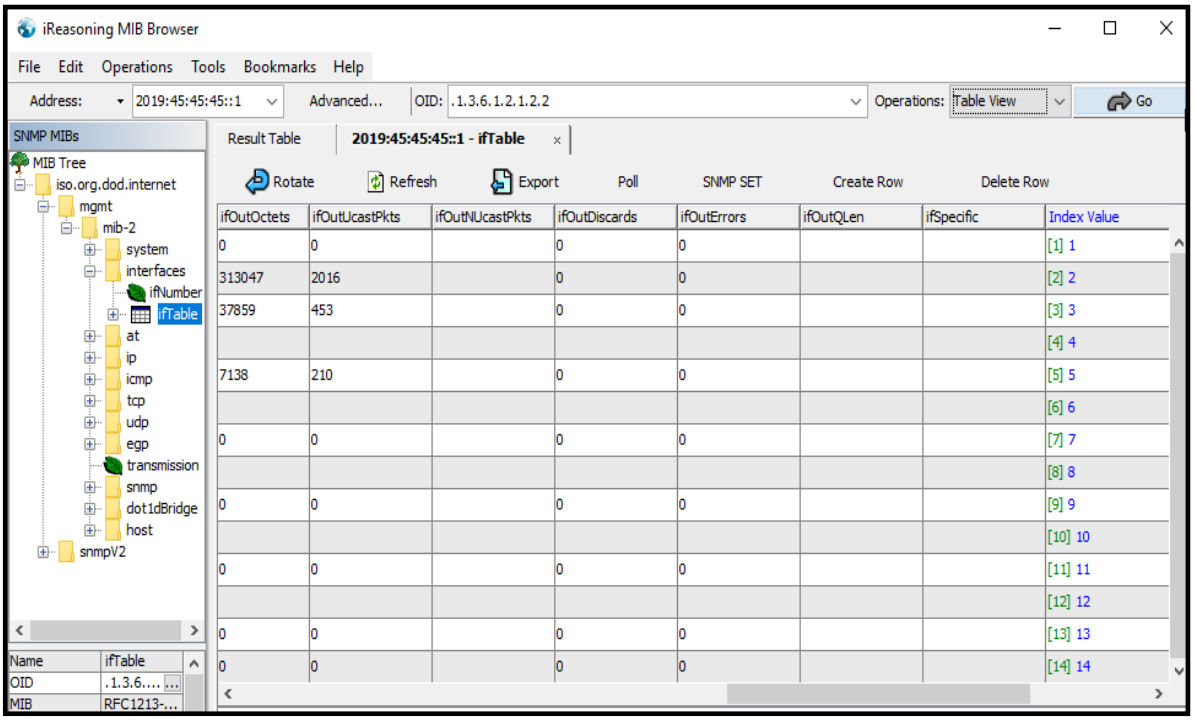


Figura 60. Monitoreo de la variable ifTable, parte 3/3.

4.2.4 ifDescr para el router Sudáfrica

En la figura 61 muestra los valores de la variable ifDescr, obtenidos mediante la operación Get.

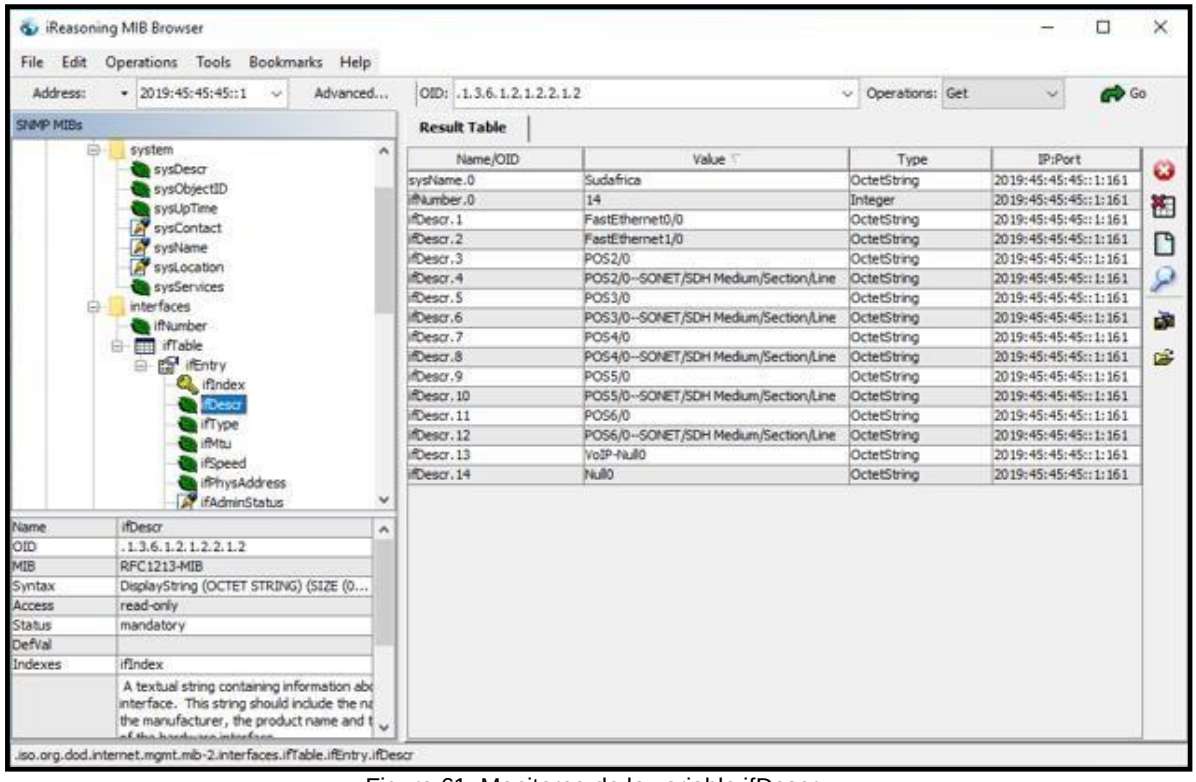


Figura 61. Monitoreo de la variable ifDescr.

4.2.5 ifOperStatus para el router Sudáfrica

En la figura 62 muestra los valores de la variable ifOperStatus, obtenidos mediante la operación Get.

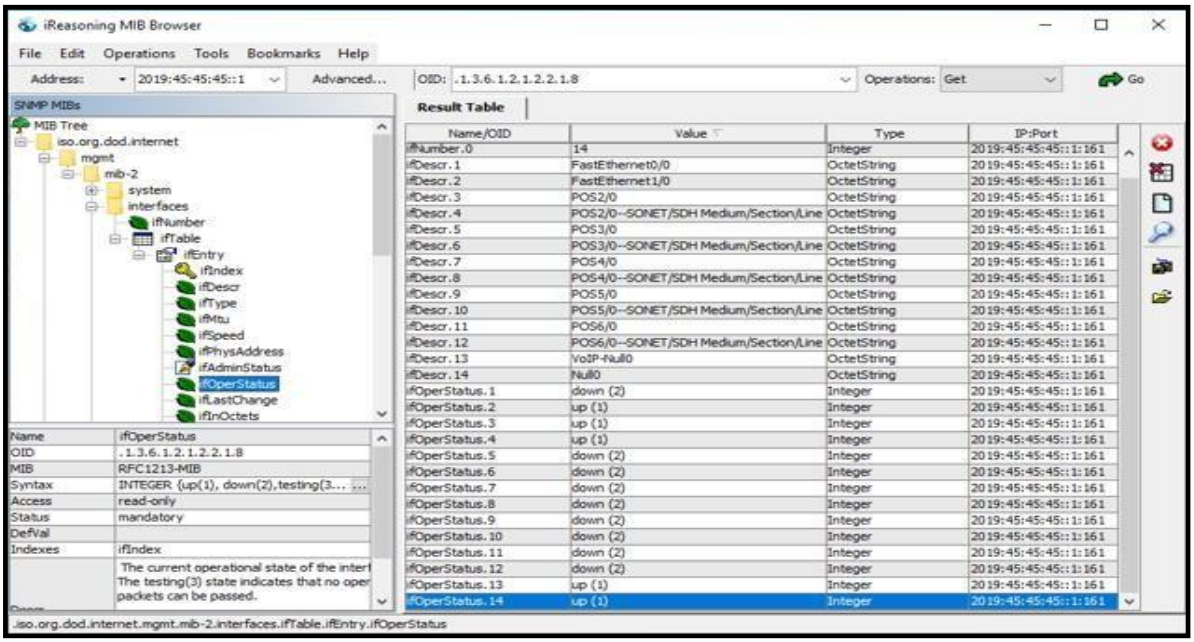


Figura 62. Monitoreo de la variable ifOperStatus.

4.2.6 sysUpTime para el router Sudáfrica

En la figura 63 muestra el valor de la variable sysUpTime, obtenido mediante la operación Get.

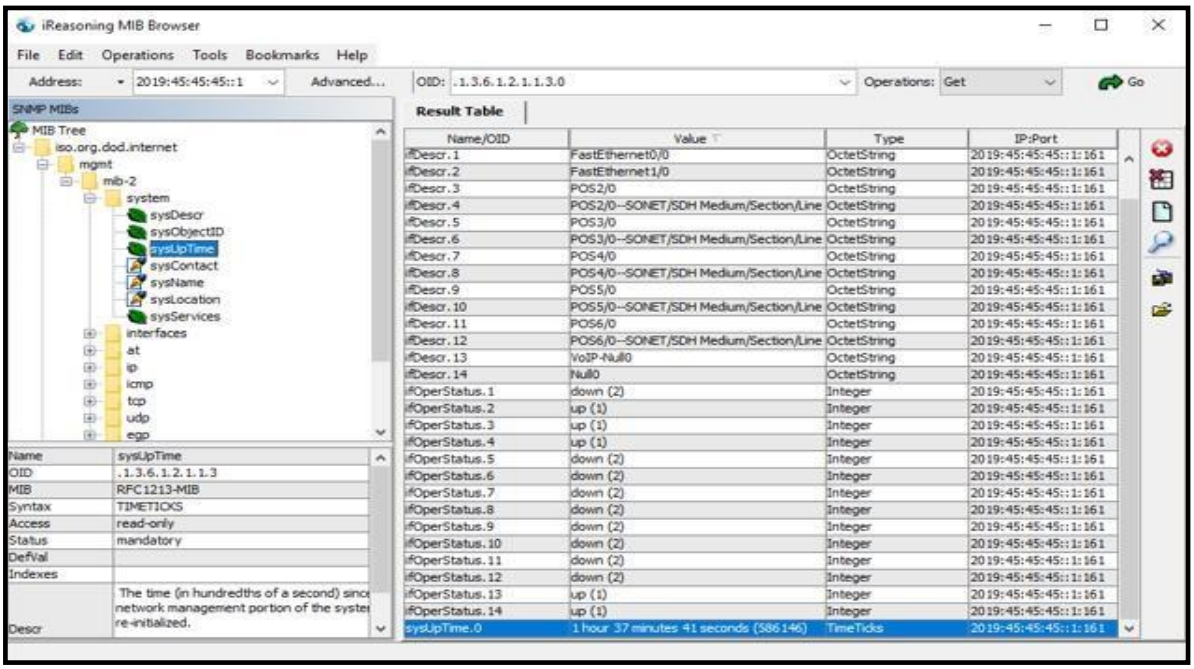


Figura 63. Monitoreo de la variable sysUpTime.

4.2.7 sysName para el router Túnez

En la figura 64 muestra el valor contenido en la variable sysName, el valor de la variable se obtiene mediante la operación Get.

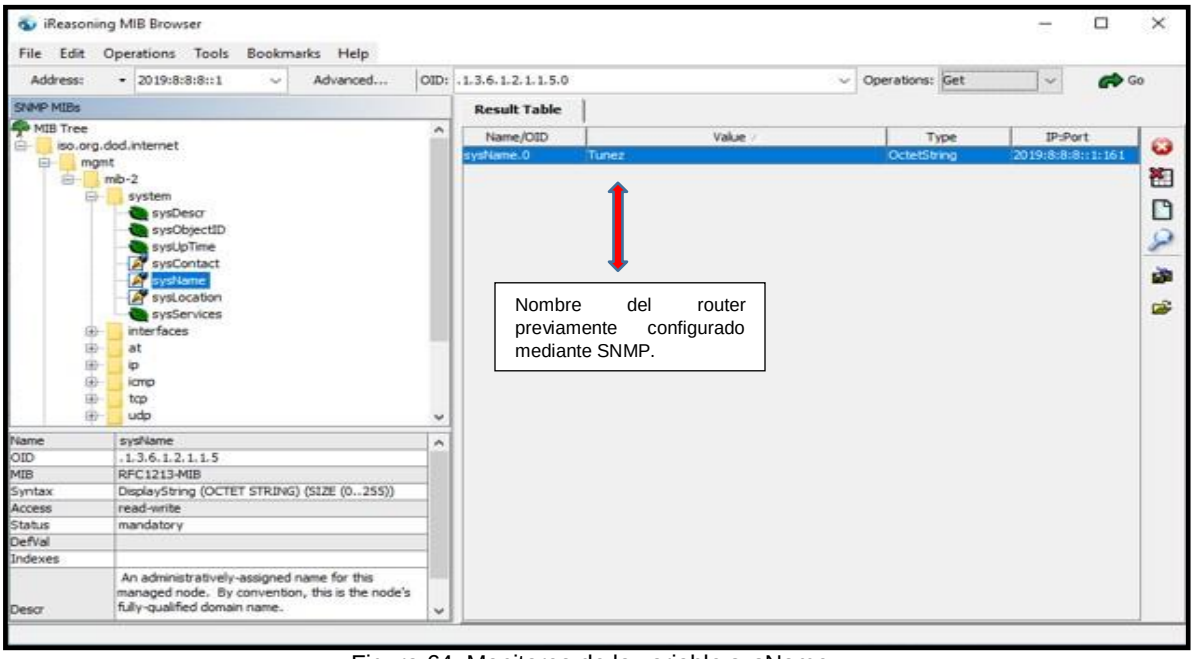


Figura 64. Monitoreo de la variable sysName.

4.2.8 ifNumber para el router Túnez

En la figura 65 muestra el valor contenido en la variable ifNumber, el valor de la variable se obtiene mediante la operación Get.

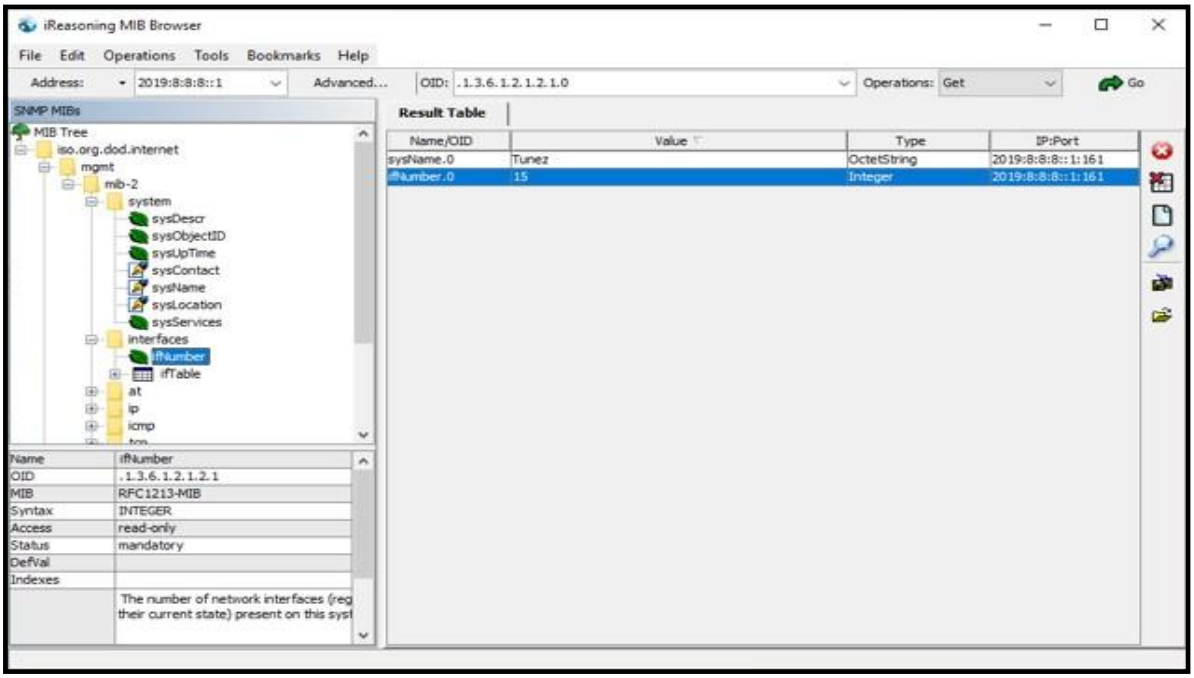


Figura 65. Monitoreo de la variable ifNumber.

4.2.9 ifTable para el router Túnez

En la figura 66 muestra los valores de la variable ifTable, obtenidos mediante la operación Table-View.

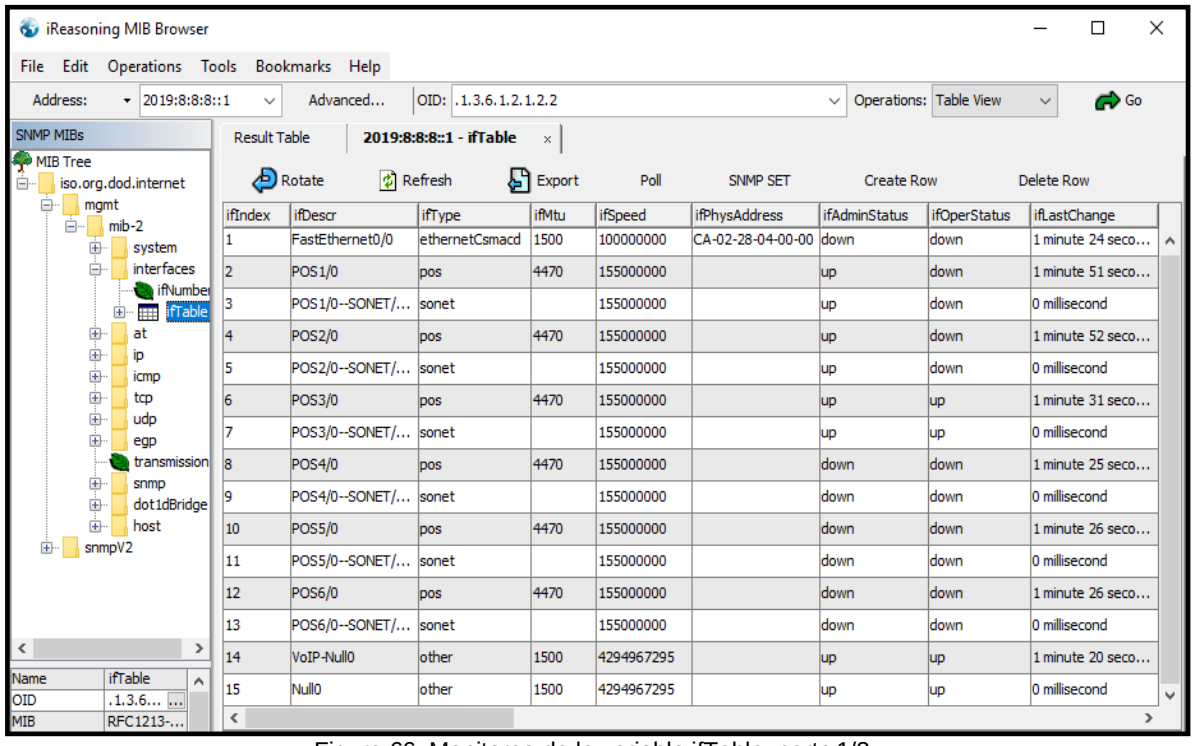


Figura 66. Monitoreo de la variable ifTable, parte 1/3.

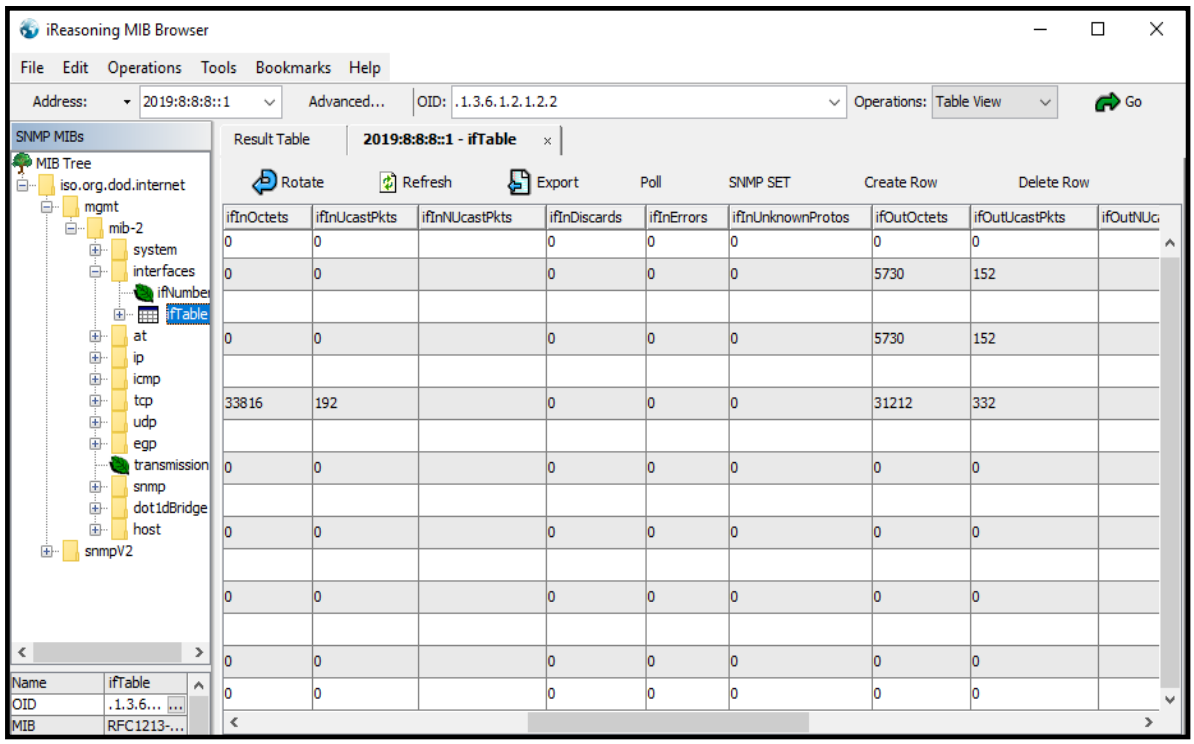


Figura 66. Monitoreo de la variable ifTable, parte 2/3.

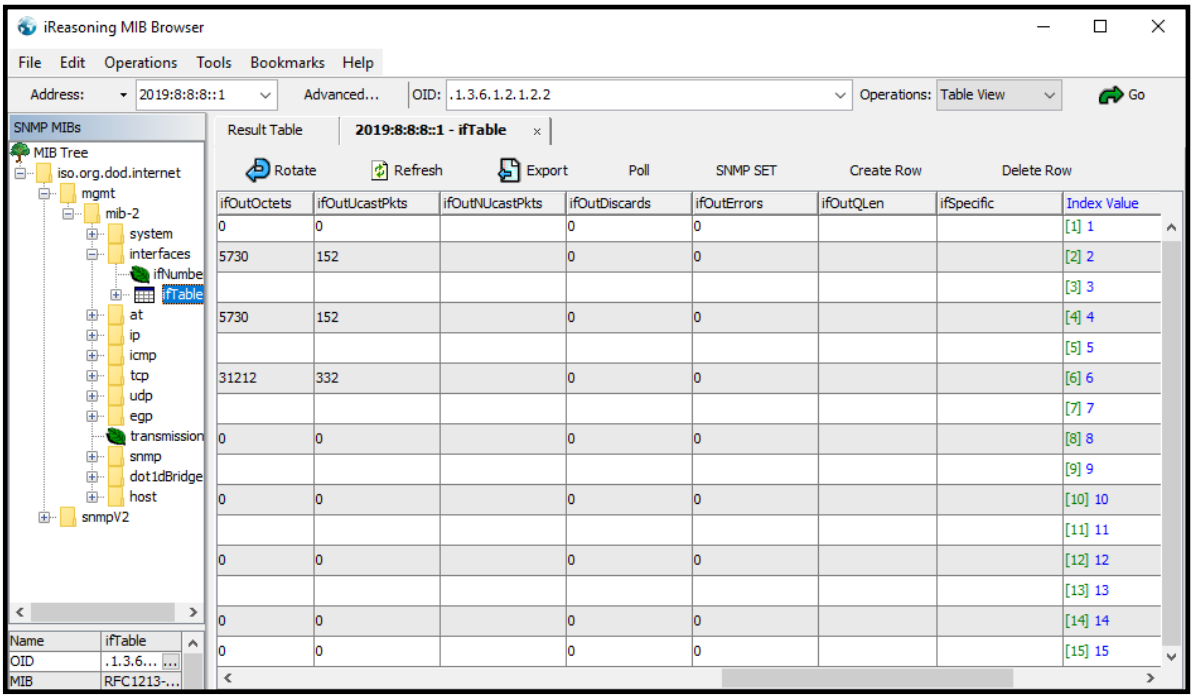


Figura 66. Monitoreo de la variable ifTable, parte 3/3.

4.2.10 ifDescr para el router Túnez

En la figura 67 muestra los valores de la variable ifDescr, obtenidos mediante la operación Get.

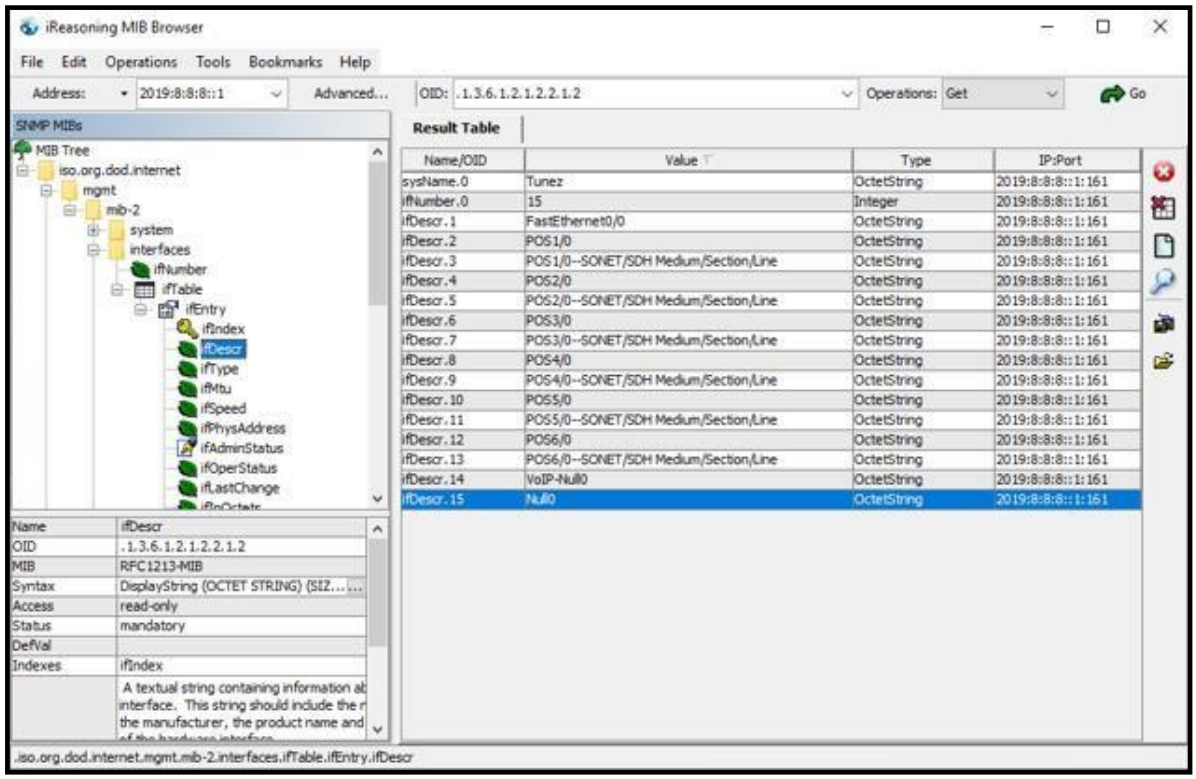


Figura 67. Monitoreo de la variable ifDescr.

4.2.11 ifOperStatus para el router Túnez

En la figura 68 muestra los valores de la variable ifOperStatus, obtenidos mediante la operación Get.

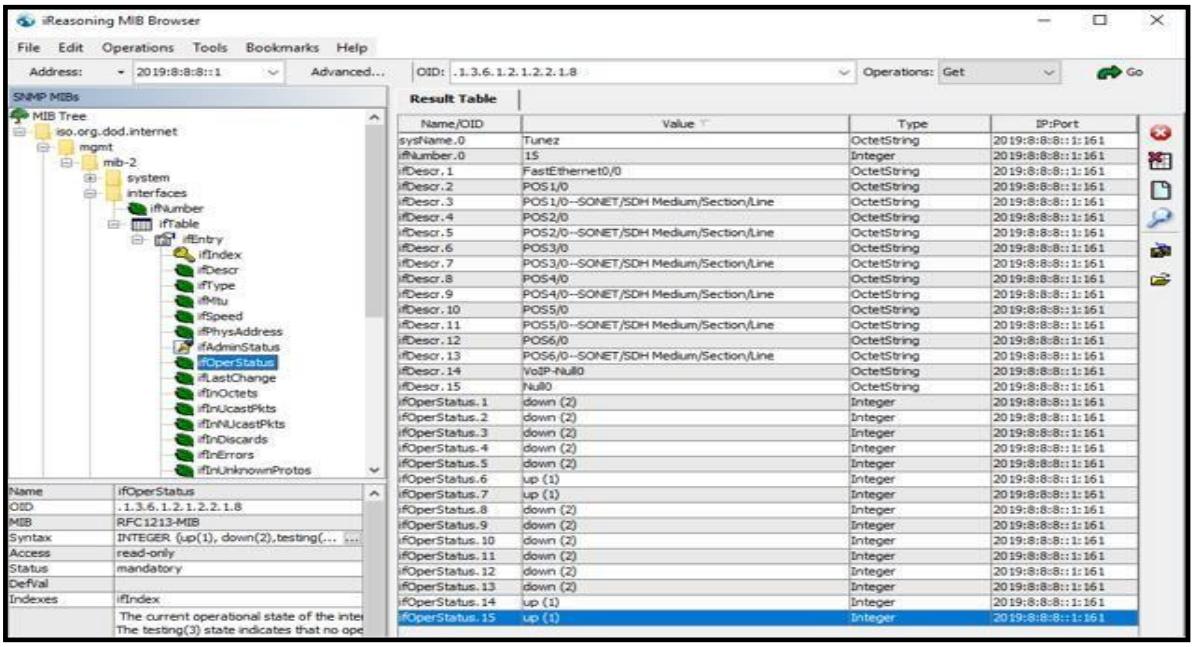


Figura 68. Monitoreo de la variable ifOperStatus.

4.2.12 sysUpTime para el router Túnez

En la figura 69 muestra el valor de la variable sysUpTime, obtenido mediante la operación Get.

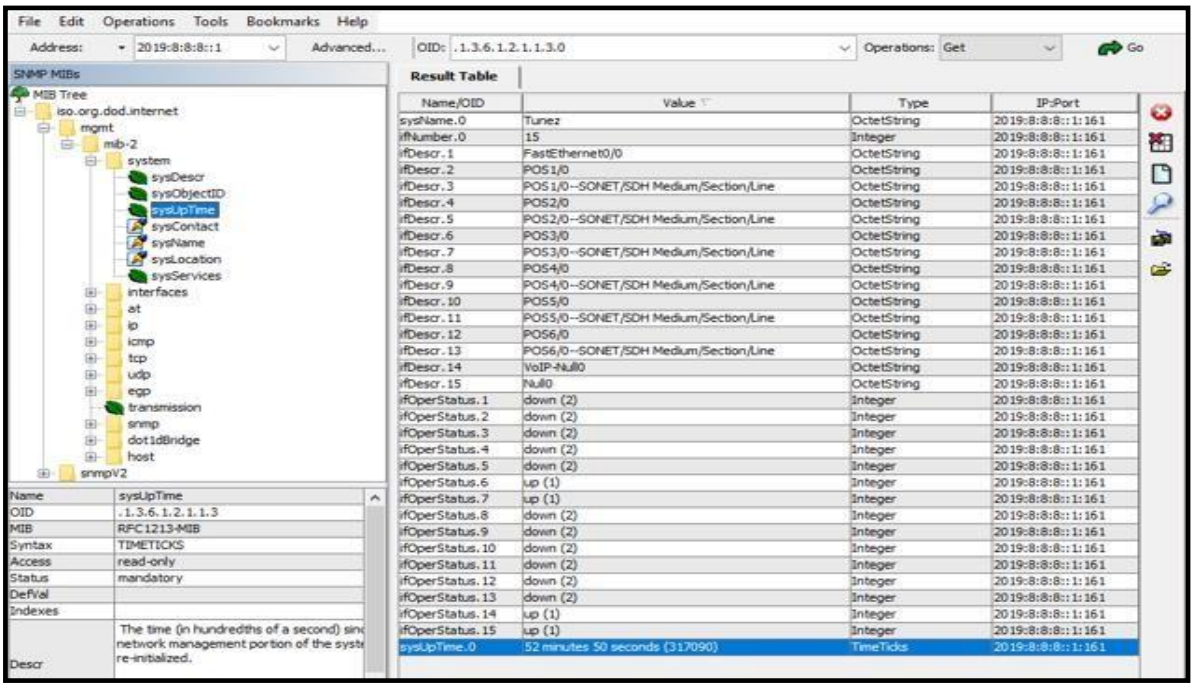


Figura 69. Monitoreo de la variable sysUpTime.

4.3 Paquetes SNMPv3 generados a través de la aplicación de Wireshark

En la figura 70 muestra los paquetes SNMPv3 generados a través de los routers Gabón y Namibia.

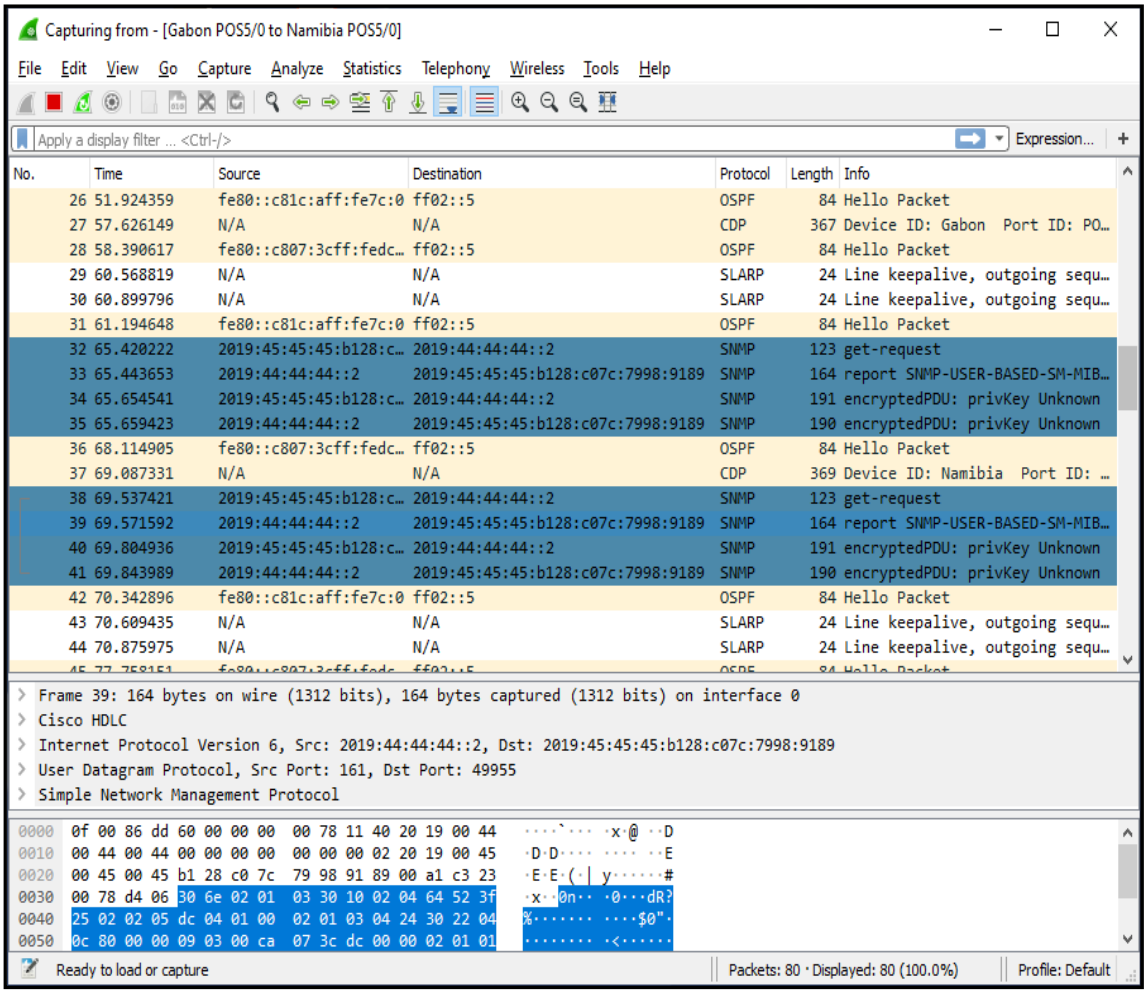


Figura 70. Paquetes SNMPv3

En la figura 71 muestra la descripción del paquete SNMPv3 generado a través del router Gabón y Namibia.

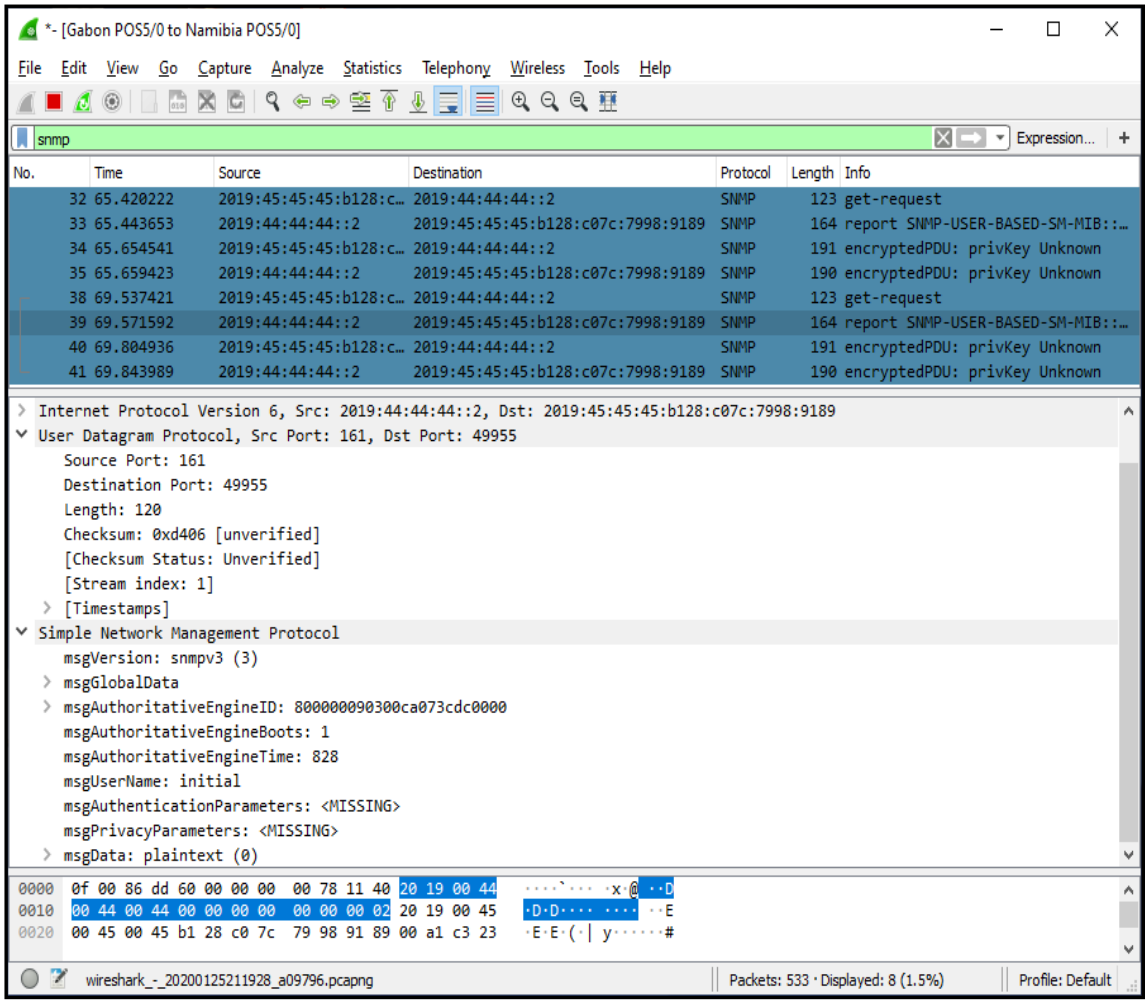


Figura 71. Características del paquete SNMPv3

CAPÍTULO 5

Conclusiones para la emulación de la conectividad y de la gestión.

Esta sección se divide en tres partes conclusiones para la conectividad, para la gestión y logros adicionales como resultados de esta tesis de licenciatura.

5.1.- Conclusiones de la conectividad

- **Enlaces:** Los routers c7200 tipo backbone de Cisco se utilizaron para la conectividad con interfaces de Fibra Óptica, las cuales todos los enlaces tuvieron una conexión máxima permitida por el emulador de 1Gbps, si bien esta velocidad es la utilizada para AfricaConnect2.

- **Estabilidad:** La ejecución del emulador GNS3 en la VM con Windows 10, no presento un nivel estable considerable, ya que al habilitar la primera parte de los routers (ASREN y WACREN), tuvo un consumo de memoria del 50% y la segunda parte fue el habilitar todos los routers (ASREN, WACREN y Alianza UbuntuNet), por lo que el consumo de memoria se disparó al 87% y la conectividad completa con la VM NMS-1 fue del 94% y CPU del 99%. Nuestro equipo tuvo una saturación, la cual se alentó mucho pero aun así se logró realizar la emulación de conectividad de todo el backbone con un tiempo aproximado de 40 a 45 minutos. Para esto se utilizó un equipo laptop marca DELL, con una capacidad de memoria instalada (RAM) de 12 GB, en el cual se ejecuta el sistema operativo Windows 10 con arquitectura de 64 bits.

5.2.- Conclusiones de la gestión

GNS3 nos permite tener un monitoreo completo a través del protocolo de conectividad (OSFPv3) y gestión (SNMPv3), así como la posibilidad de manipular variables remotas desde las unidades gestoras que se hayan indicado, por ejemplo: el gestor, la MIB y agentes. Así como las 6 variables que se tomaron para las pruebas de gestión, para el router Sudáfrica y Túnez. Esto a través de la aplicación iReasoning MIB Browser, las cuales fueron: sysName, ifNumber, ifTable, ifDescr, ifOperStatus y sysUpTime.

Además de poder realizar el monitoreo y manipulación de las 6 variables descritas para la gestión, en PowerSNMP Free Manager e iReasoning MIB Browser fue posible manejar el uso de nombre de usuario, comunidad (public, group), puerto, versión, autenticación y tipo de privacidad al realizar la habilitación o la des-habilitación de la misma a través del agente gestionado. Por lo que el emulador GNS3 nos permite acercarnos un poco a la realidad del funcionamiento de la red AfricaConnect2, al utilizar los routers c7200 de Cisco, ya que se realiza la descarga de los IOS para dicho router.

Por lo tanto se concluye que al poner a prueba las herramientas de emulación para la conectividad y la gestión con las cuales se realizó el análisis de funcionamiento del backbone AfricaConnect2, fueron las esperadas. Comprobando de esta manera, la eficiencia de cada una de ellas y exponiendo sus limitantes como lo fue en los routers, sólo se tuvo 6 slots para la conectividad entre dichos routers, ancho de banda de 1 Gbps, alto consumo del emulador y de la VM.

5.3.- Publicación adicional a tesis de licenciatura

Un logro adicional a la presente tesis de licenciatura es la publicación del artículo:
Management Emulation of Advanced Network Backbones in Africa: 2019 Topology, en proceedings IEEE. Mismo que se encontrara disponible en IEEEXplore y en las bases dedatos de SCOPUS. En las siguientes páginas [103-105] se anexa copia del copyright en el que se autoriza a IEEE la publicación internacional.

IEEE COPYRIGHT AND CONSENT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the IEEE and must accompany any such material in order to be published by the IEEE. Please read the form carefully and keep a copy for your files.

Management Emulation of Advanced Network Backbones in Africa: 2019 Topology.
Prof. Jose-Ignacio Castillo-Velazquez and Mr. Luis-Carlos Revilla-Melo
2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)

COPYRIGHT TRANSFER

The undersigned hereby assigns to The Institute of Electrical and Electronics Engineers, Incorporated (the "IEEE") all rights under copyright that may exist in and to: (a) the Work, including any revised or expanded derivative works submitted to the IEEE by the undersigned based on the Work; and (b) any associated written or multimedia components or other enhancements accompanying the Work.

GENERAL TERMS

1. The undersigned represents that he/she has the power and authority to make and execute this form.
2. The undersigned agrees to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
3. The undersigned agrees that publication with IEEE is subject to the policies and procedures of the IEEE PSPB Operations Manual.
4. In the event the above work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, the foregoing copyright transfer shall be null and void. In this case, IEEE will retain a copy of the manuscript for internal administrative/record-keeping purposes.
5. For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
6. The author hereby warrants that the Work and Presentation (collectively, the "Materials") are original and that he/she is the author of the Materials. To the extent the Materials incorporate text passages, figures, data or other material from the works of others, the author has obtained any necessary permissions. Where necessary, the author has obtained all third party permissions and consents to grant the license above and has provided copies of such permissions and consents to IEEE

You have indicated that you DO wish to have video/audio recordings made of your conference presentation under terms and conditions set forth in "Consent and Release."

CONSENT AND RELEASE

1. In the event the author makes a presentation based upon the Work at a conference hosted or sponsored in whole or in part by the IEEE, the author, in consideration for his/her participation in the conference, hereby grants the IEEE the unlimited, worldwide, irrevocable permission to use, distribute, publish, license, exhibit, record, digitize, broadcast, reproduce and archive, in any format or medium, whether now known or hereafter developed: (a) his/her presentation and comments at the conference; (b) any written materials or multimedia files used in connection with his/her presentation; and (c) any recorded interviews of him/her (collectively, the "Presentation"). The permission granted includes the transcription and reproduction of the Presentation for inclusion in products sold or distributed by IEEE and live or recorded broadcast of the Presentation during or after the conference.
2. In connection with the permission granted in Section 1, the author hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work or Presentation, and releases IEEE from any claim based on right of privacy or publicity.

BY TYPING IN YOUR FULL NAME BELOW AND CLICKING THE SUBMIT BUTTON, YOU CERTIFY THAT SUCH ACTION CONSTITUTES YOUR ELECTRONIC SIGNATURE TO THIS FORM IN ACCORDANCE WITH UNITED STATES LAW, WHICH AUTHORIZES ELECTRONIC SIGNATURE BY AUTHENTICATED REQUEST FROM A USER OVER THE INTERNET AS A VALID SUBSTITUTE FOR A WRITTEN SIGNATURE.

Jose-Ignacio Castillo-Velazquez — **Signature**

28-02-2020 — **Date (dd-mm-yyyy)**

Information for Authors

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author's personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use.The IEEE Intellectual Property Rights office must handle all such third-party requests.
- Authors whose work was performed under a grant from a government funding agency are free to fulfill any deposit mandates from that funding agency.

AUTHOR ONLINE USE

- **Personal Servers.** Authors and/or their employers shall have the right to post the accepted version of IEEE-copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including a link to the article abstract in IEEE Xplore. Authors shall not post the final, published versions of their papers.
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the accepted version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.

6 REFERENCIAS

[1] UCLA, “Birthplace of the Internet, 1969”, IEEE Milestones, IEEE History Center, IEEE, 2009

[2] SRI, “Inception of the ARPANET, 1969”, IEEE Milestones, IEEE History Center, IEEE, 2009

[3] José Ignacio Castillo Velázquez, Redes de datos: Contexto y evolución, Samsara, México, 2016. Capítulo III.1 La primera generación. Pag. 53.

[4] DARPA, RFC 15, Network Subsystem for Time Sharing Host, Sep.1969

[5] DARPA, RFC 354, File Transfer Protocol, 1972

[6] ISO 7498:1984 Open Systems Interconnection – Basic Reference Model: The basic Model, 1984

[7] José Ignacio Castillo Velázquez, Redes de datos: Contexto y evolución, Samsara, México, 2016. Capítulo III.2 La segunda generación. Pag. (57-58).

[8] NSFN, *Physical Initial NSFNET Topology,* [en linea]; [Consulta: 8 marzo 2019] Disponible: https://images.computerhistory.org/internethistory/1988_nsfnet_map.gif

[9] José Ignacio Castillo Velázquez, Redes de datos: Contexto y evolución, Samsara, México, 2016. Capítulo III.3 La tercera generación. Pag. 60.

[10] Royer C. Hermand, Advanced Networking Technology, Estados Unidos, Ed. DIANE Publishing, Junio 1993, pp. 5-13, ISBN: 0-16-041805-4

[11] CANARIE, [en linea]; [Consulta: 23 Jun 2019] Disponible: https://www.canarie.ca/network/nren/

[12] José Ignacio Castillo Velázquez, SWITCHING & ROUTING, Samsara, México, 2016. Capítulo IV.10, Las redes avanzadas: Internet 2 -1996, Pag. 88.

[13] AfricaConnect, Projects [en linea]; [Consulta: 23 Jun 2019] Disponible:

https://www.africaconnect.eu/Pages/Project/Funding.aspx

[14] AfricaConnect2, Approach [en linea]; [Consulta: 23 Jun 2019] Disponible:

https://www.africaconnect2.net/Project/Approach/Pages/Home.aspx

[15] UbuntuNet Alliance, Stories [en linea]; [Consulta: 23 Jun 2019] Disponible:

https://ubuntunet.net/

[16] UbuntuNet Alliance, Members [en linea]; [Consulta: 23 Jun 2019] Disponible:

https://ubuntunet.net/members/

[17] WACREN, About Us, [en linea]; [Consulta: 23 Jun 2019] Disponible:

http://www.wacren.net/en/content/about-us

[18] AfricaConnect2, Partners, [en linea]; [Consulta: 23 Jun 2019] Disponible:

https://www.africaconnect2.net/Partners/African_NRENs/West_and_Central_Africa/Pages/Home.aspx

[19] ASREN, What is ASREN, [en linea]; [Consulta: 28 Jun 2019] Disponible:

http://www.asrenorg.net/?q=content/publications

[20] ASREN, Members, [en linea]; [Consulta: 28 Jun 2019] Disponible:

http://www.asrenorg.net/?q=content/shareholders-0

[21] AfricaConnect2, Partners, [en línea]; [Consulta: 13 Jul 2019] Disponible:

https://www.africaconnect2.net/Partners/African_NRENs/Northern_Africa/Pages/Home.aspx

[22] AfricaConnect2, Network, [en linea]; [Consulta: 13 Jul 2019] Disponible: https://www.africaconnect2.net/Networks/Pages/Home.aspx

[23] J. I. Castillo and N. Galicia, “Routing algorithms applied to an advanced academic network know as CUDI,” *IEEE Latin America Transactions*, vol. 14. no. 6. pp. 2974-2979, June 2016, doi: 10.1109/TLA.2016.7555284

[24] J. Castillo-Velazquez and J. Sánchez-Trejo, “Emulation for CLARA’s operation, the advanced network for Latin America,” *2016 IEEE ANDESCON*, Arequipa, 2016, pp. 1-4. doi:10.1109/ANDESCON.2016.7836205

[25] J. Castillo-Velazquez, D. Serrano-Martinez and A. Morales, “Emulation of backbone’s connectivity and management for the advanced network in Latin America: 2016’s topology,” *2017 Sensors Networks Smart and Emerging Technologies (SENSET)*, Beirut, 2017, pp. 1-4. doi: 10.1109/SENSET.2017.8125029

[26] J. Castillo-Velazquez, D. Serrano-Martinez and A. Morales, “Emulation of the connectivity of backbone and management for the layer 3 service of INTERNET2: 2016 topology,” *2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII),* Managua, 2017, pp. 1-4. doi: 10.1109/CONCAPAN.2017.8278476

[27] J. Castillo-Velazquez, V. R. Cobos Panduro and W. R. Marchand Niño, “IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network,” *2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Lima, 2018, pp. 1-4. doi: 10.1109/INTERCON.2018.8526390

[28] J. Castillo-Velazquez, F. DeLaCruz-Alejandre and M. Huerta, “An Approach to Management Assessment for GEANT Backbone Using GNS3 for SNMPv3,” *2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII)*, San Salvador, 2018, pp.1-6. doi: 10.1109/CONCAPAN.2018.8596667

[29] J. Castillo-Velazquez, E. Ramirez-Diaz and W. R. M. Niño, “Use of GNS3 Cloud Environment for Network Management Emulation when Comparing SNMP vs Syslog Applied Over an Advanced Network,” *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX),* Guatemala City, Guatemala, 2019, pp. 1-6. doi: 10.1109/CONCAPANXXXIX47272.2019.8976995

[30] C. Jose-Ignacio, D. Serrano-Martinez and H. Mónica, “Management Emulation for Advanced Networks Interconection in all America: 2019 topology,” *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, Guatemala City, Guatemala, 2019, pp. 1-6. doi: 10.1109/CONCAPANXXXIX47272.2019.8976946

[31] S. Deering Cisco, R. Hinden Nokia, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.

[32] R. Hinden, S. Deering, IPv6 Addressing Architecture, RFC 2373, July 1998.

[33] RFC 1058 Headrick para RIP Jun 1988

[34] RFC 2453 G. Malkin para RIPv2 November 1998

[35] RFC 2080 Malkin & Minnear RIPng para IPv6 January 1997

[36] DARPA, RFC 1131, The OSPF specification, Oct 1989.

[37] J. Moy, Proteon, Inc. OSPFv2, RFC 1247, July 1991

[38] José Ignacio Castillo Velázquez, SWITCHING & ROUTING, Samsara, México, 2016. Capítulo IV.7.2 OSPF, Pag. 83.

[39] R.Coltun, D. Ferguson, J. Moy, OSPF for IPv6, RFC 2740, December 1999.

[40] M. Fedor, M. Schoffstall, J. Davin, Un protocolo simple de gestión de red (SNMP), RFC 1157, Mayo 1990

[41] U. Blumenthal, F. Maino, K. McCloghrie “The advanced Encryption Standart (AES) Cipher Algorithm in the SNMP User-based Security Model”, RFC 3826 Junio 2004.

[42] J. Case, K. McCloghrie, M. Rose, “Introduction to Community-based SNMPv2”, RFC 1901, 1996.

[43] U Blumenthal, B. Wijnen, “User-based Security Model (USM) for versión 3 of the Simple Network Management Protocol (SNMPv3)” RFC 3414, Diciembre 2002.

[44] DARPA, RFC 3411, Marcos de administración (SNMP), Dic 2002.

[45] M. Rose, “Structure and Identification of Management Information for TCP/IP-based Internets”, RFC 1155, Mayo de 1990.

[46] José Ignacio Castillo, El árbol de Internet y la estructura de información de gestión de una red, IEEE Latin America and the Caribbean Newsletter, Año 20, No.62, pp. 15-17, Abril de 2009, ISSN: 2157-8354.

[47] GNS3 (General Public License – Licencia Pública General), [en linea]; [Consulta: 13 Jul 2019] Disponible: https://gns3.com/software

[48] Cisco IOS, [en línea]; [Consulta 26 Jul 2019] Disponible: https://telectronika.com/descargas/cisco-imagenes-ios-para-gns3-dynamips-y-vm/

[49] VirtualBox, [en línea]; [Consulta 26 Jul 2019] Disponible en: https://www.virtualbox.org/wiki/Downloads

[50] Microsoft, Descarga Windows 10, [en línea]; [Consulta: 26 Jul 2019] Disponible: https://www.microsoft.com/es-mx/software-download/windows10

[51] SNMP, PowerSNMP Free Manager 2.0, [en línea]; [Consulta: 26 Jul 2019] Disponible: https://powersnmp-free-manager.software.informer.com

[52] Cisco Packet Tracer, [en línea]; [Consulta: 05 Sep 2019] Disponible: https://packet-tracer.softonic.com/

[53] iReasoning, [en línea]; [Consulta: 09 Oct 2019] Disponible: https://www.ireasoning.com/download.shtml