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

Colegio de Ciencia y Tecnología

Gestión de la red avanzada GEANT - AFRICACONNECT bajo entorno de máquina real limitado

T E S I S

Que para obtener el título de:

Licenciadas en Ingeniería en Sistemas Electrónicos y de Telecomunicaciones

Presentan:

Fernández Tinoco Diana Laura

Rosas Suárez Itzel Iliana

Director:

M. en C. José Ignacio Castillo Velázquez

Ciudad de México, noviembre de 2021.

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©

DEDICATORIAS

"Tuyos son, Señor la grandeza y el poder, la gloria, la victoria y la majestad. Tuyo es todo cuanto hay en el cielo y en la tierra. Tuyo también es el reino, y tú estás por encima de todo. De ti proceden la riqueza y el honor; tú lo gobiernas todo. En tus manos están la fuerza y el poder, y eres tú quien engrandece y fortalece a todos. Por eso, Dios nuestro, te damos gracias, y a tu glorioso nombre tributamos alabanzas" 1ª Crónicas 29:11-13

Doy gracias a Dios, por su gran amor, por haberme guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad, ya que este trabajo implica mucho más que un esfuerzo personal, porque no he llegado hasta aquí por mis propias fuerzas, por esto y más, no cesan mis ganas de decir que es gracias a Ti que esta meta está cumplida.

Agradezco tanto a mis padres Joaquín Fernández y Leticia Tinoco, que son mi más grande admiración, por su apoyo incondicional, su entrega, su esfuerzo y dedicar su vida entera a nosotros. A ti Papá, que a pesar de tu partida eres mi inspiración para seguir adelante, cuánto anhelaría que estuvieras celebrando este momento a mi lado, pero te has ido, y sé que hubieras estado orgulloso de mí. Te agradezco tantas cosas, fuiste un gran pilar en la familia, un gran ejemplo, un hombre de casa, trabajador, nunca nos faltó nada, nos diste todo, y a todos por igual, de ti aprendí a tener la fuerza, la valentía, la persistencia, de ti aprendí a entender que nada es para siempre, tengo tantas palabras que expresarte, pero ya no estás aquí para leerlas, ahora sólo me queda dedicar este trabajo en tu honor, mientras tanto, y con gran esperanza lo digo, te veré pronto papá. TE AMO. A ti Mamá, recuerdo cuando siempre nos decías: "querer es poder", y ahora lo he logrado gracias a tus consejos, a tu apoyo, a tu compañía, a todas esas veces que me arrancaste las hojas para que lo hiciera bien, ahora lo entiendo y sé que todo eso dio frutos, y si he persistido es gracias a toda esa entrega que me brindaste. Eres una gran motivación en mi día a día, siempre cuidaré de ti, TE AMO.
"Muchas mujeres han realizado proezas, más tú sobrepasas a todas" Proverbios 31:29

Gracias le doy a Dios por mis hermanos Carlos, Thalía y Yibran que son parte importante de mi vida. Hemos pasado por momentos de felicidad, de emoción, de tensión, de angustia y de tristeza, pero siempre juntos. Gracias por llenar mi vida de grandes

momentos, por todo lo que hemos compartido, por todo el apoyo brindado. He aprendido y sigo aprendiendo de ustedes. Son una bendición para mi vida, los amo.

A mi cuñado Artemio Castillo, por el gran apoyo que me brindaste al regalarme mi laptop, fue donde pude realizar gran parte de mis trabajos a lo largo de mi carrera y ahora hacer posible la realización de mi tesis. A mi cuñada Mariana Hernández por sus palabras de aliento y motivación que siempre tiene para mí, y ser tan buena persona conmigo. Gracias a ambos, porque han estado en muchos de los buenos y malos momentos con mi familia.

A mi sobrino Yosmar Castillo por ser la alegría de la familia, llegaste como una bendición de Dios en los momentos más difíciles, y eres una maravillosa adición a nuestras vidas. Eres una alegría para mi corazón y eres un regalo precioso, te amo Yos.

Agradezco, a mi director de tesis M. en C. José Ignacio Castillo Velázquez, por haber creído en mí, por su paciencia y dedicación para dirigir esta tesis y compartir conmigo su conocimiento. Usted, Mtro. José Ignacio Castillo Velázquez es una parte fundamental de este logro, sin su guía académica no hubiera sido posible obtener mi título profesional.

También deseo agradecer al Ing. Ricardo Galindo Reyes, por brindarme su apoyo al prestarme una laptop cuando lo llegué a necesitar durante la carrera, por sus apoyos personales y académicos, lo tengo presente y lo aprecio mucho.

A Itzel Rosas, quien durante la carrera fue y sigue siendo mi compañera y amiga, agradezco que estemos compartiendo este logro juntas, por los momentos de esfuerzos, logros y luchas, también agradezco a mis amigos: Martha Navarro, Javier Mejía, Christian Aguirre y Jesús Mendoza quienes me han brindado su gran y sincera amistad, por todos los buenos momentos que pasamos juntos durante nuestra estancia en la Universidad, gracias.

Diana Laura Fernández Tinoco

DEDICATORIAS

Esta tesis se la dedico a mis padres Delia Suárez y Odilon Rosas, no hay palabras suficientes para expresarles lo agradecida que estoy con ustedes, siempre me han cuidado, guiado e impulsado para dar lo mejor de mi, aunque a veces solo me quería rendir, ustedes siempre han sido mi motor, gracias por su apoyo incondicional, que día con día me dan, son un claro ejemplo de que el querer es poder, los admiró y amó con todo mi corazón, sin su apoyo en todo sentido este logro no hubiese sido posible.

A Epifania Castro por enseñarme la nobleza que te caracterizaba, siempre me guiaste y aconsejaste en todo, gracias por la confianza que constantemente me brindaste, siempre te extrañare abuela, un abrazo al cielo, te amo.

A Amador Rosas, por cuidarme en los malos momentos, por guiarme y no dejarme caer cuando todo se veía gris, te amo hermano.

A mi sobrino Jorge Rosas porque tu llegada iluminó a la familia, el tenerte cerca me genera inspiración, curiosidad y optimismo, gracias por irradiar tantas cosas positivas, te amo mi querido georgi.

A Jorge Mata, por siempre estar para mí apoyándome, motivándome y brindando los mejores consejos, te lo agradezco amor, por incluso sacarme una sonrisa cuando las cosas no iban bien.

A mi amiga y compañera de tesis Diana Fernández, le agradezco los buenos y malos momentos que hemos compartido, por que hemos aprendido una de la otra, tanto personal como profesionalmente, el construir esta tesis contigo fue un gusto, también quiero agradecer a mis amigos, en especial a Samantha Haquet, Miguel Castañeda, Nohemi Dominguez y Rocio Cadena, por los momentos que hemos pasado juntos, por el apoyo y ánimos que me brindaron.

Una dedicatoria especial a mi director de tesis el M. en C. José Ignacio Castillo Velázquez, por ser un gran profesor que me inspiró, me transmitió sus conocimientos y creyó en mí como alumna, maestros como usted no se consigue en todos lados y tuve la suerte de encontrarme con sus enseñanzas, muchas gracias por su incondicional apoyo y aporte profesional, el cuál fue esencial para la culminación de esta tesis y de mi carrera profesional.

Itzel Iliana Rosas Suárez

AGREDECIMIENTOS

Agradecemos a nuestra casa de estudios, la Universidad Autónoma de la Ciudad de México (UACM), por brindarnos un lugar donde nos formamos con los conocimientos y habilidades para poder desarrollarnos como profesionistas, también agradecemos a todos los profesores que nos impartieron clases y plasmaron su conocimiento y sabiduría en nosotras, en especial a nuestro director de tesis el M. en C. José Ignacio Castillo Velázquez por su apoyo, entusiasmo, dedicación, tiempo, ayuda e interés, en toda nuestra trayectoria como profesor y ahora como nuestro director de tesis, por siempre impulsarnos a dar lo mejor de nosotras, y enseñarnos que el estudio es una variable constate en nuestras vidas.

A nuestros lectores de tesis Dr. Adolfo Horacio Escalona Buendía, Ing. Ricardo Galindo Reyes y al Dr. Gerardo Abel Laguna Sánchez por tomarse el tiempo de revisar nuestro trabajo, sus valiosos comentarios y sus conocimientos compartidos.

RESUMEN

Las redes avanzadas tanto africana AfricaConnect y europea Geant ofrecen una infraestructura troncal de Internet avanzada a 72 países dedicados a la investigación y educación, y se encuentran interconectados a través de tres países africanos y tres países europeos, teniendo tres enlaces de comunicación entre ellos para su conectividad total.

Las citadas redes avanzadas están evolucionando en el tiempo, desarrollando una mejor infraestructura con mayor ancho de banda y capacidades de equipos. La red avanzada africana conecta a 29 países en tres redes avanzadas nacionales, UBUNTUNET, WACREN y ASREN con velocidades de conexión de 100 Gbps, mientras que la red avanzada europea, integra a 43 países con infraestructura de red que le permite ofrecer velocidades de conexión de entre 100 a 500 Gbps.

Para analizar estas redes avanzadas, se requiere de emuladores de gran capacidad, que permitan agregar routers de alto rendimiento, por lo que se utilizó GNS3 como emulador, ya que cuenta con Dynamips y Quick Emulator (QUEMU) como motores de virtualización, y hasta ahora está enfocado a la educación y la investigación, a diferencia de un simulador cuyo enfoque es solo educativo, ya que está limitado en aproximaciones a gran escala y no cuenta con equipos de backbone (ver apéndice A).
En esta emulación se evaluó la conectividad y la gestión de la red empleando los protocolos correspondientes a IPv6.

Este trabajo es particularmente pertinente debido a que hay poca información publicada, por lo que resulta de gran interés para Advanced Networking Laboratory (ADVNETLAB) de la Universidad Autónoma de la Ciudad de México (UACM), además son de gran relevancia para el análisis por parte de los Internet Service Provider (ISP), tal que este trabajo tiene por objetivo describir el funcionamiento de la integración de la red AfricaConnect y Geant, bajo el protocolo de comunicaciones IPv6.

La emulación del backbone AfricaConnect y Geant se realizó en una computadora de escritorio MacOS Catalina. Debido a estas características surgieron limitaciones en el encendido de toda la topología, ya que demoró 50 min llevando el equipo a límite usando

el 100 % del CPU y el 80.3 % de la RAM, a pesar de esto la emulación se ejecutó exitosamente.

ABSTRACT

The advanced African network AfricaConnect and the European Geant offer an advanced Internet backbone infrastructure in 72 countries dedicated to research and education. They are interconnected through three African countries and three European countries, having three communication links between them for their connectivity, which are evolving over time, developing a better infrastructure with greater bandwidth and equipment capabilities. The African advanced network connects 29 countries in three national advanced networks, which are UBUNTUNET, WACREN, and ASREN with connection speeds of 100 Gbps, while the European advanced network integrates 43 countries with network infrastructure, which allows it to offer speeds of connection from 100 to 500 Gbps.

To analyze these advanced networks, high-capacity emulators are required, which allow adding high-performance routers, which is why (Graphical Network Simulator-3) GNS3 was used as an emulator, since it has Dynamips and Quick Emulator (QUEMU) as virtualization engines, and so far, it is focused on education and research, unlike a simulator whose focus is only educational, since it is limited in large-scale approaches and does not have backbone equipment (see appendix A).

In this emulation, network connectivity and management were evaluated using the protocols corresponding to IPv6.

This work is particularly important because there is little published information, so it is of great interest to the Advanced Networking Laboratory (ADVNETLAB) of the Autonomous University of Mexico City (UACM), and they are also of great relevance for analysis by part of the Internet Service Provider (ISP), such that this work aims to describe the operation of the integration of the AfricaConnect and Geant network, under the IPv6 communications protocol.

The AfricaConnect and Geant backbone emulation was performed on a macOS Catalina desktop computer. Due to these characteristics, limitations arose in the powerup of the entire topology, since it took 50 min to bring the equipment to the limit using 100% of the CPU and 80.3% of the RAM, despite this the emulation was executed successfully.

ESTRUCTURA DE LA TESIS

Este trabajo está compuesto de 6 capítulos. El primero cuenta con la descripción breve sobre la importancia de las Redes Avanzadas (RA) y objetivos tanto generales como específicos. El segundo capítulo se aborda a manera de resumen sobre el nacimiento y evolución de las redes de datos, así mismo se enfoca en la historia e integración de las redes avanzadas AfricaConnect y Geant. El tercer capítulo está destinado a los protocolos, la primera parte aborda los protocolos de enrutamiento como Open Shortest Path First Protocol version 3 (OSPFv3) y Border Gateway Protocol version 4 (BGP4), mientras que en la segunda el protocolo de gestión Simple Network Management Protocol version 3 (SNMPv3). En el cuarto capítulo se presenta la metodología para la integración de la emulación de la red africana y europea, así también se aborda qué equipos son necesarios para la emulación, además se agregaron las tablas de direccionamiento y sus respectivas configuraciones. El quinto capítulo está reservado para la discusión de los resultados propios tanto de la conectividad como de la gestión y su análisis. Finalmente, el capítulo seis se presentan las conclusiones. Se adicionan 6 apéndices relacionados a capítulos anteriores como un complemento.

PRÓLOGO

En la UACM, los primeros egresados titulados de ISET se lograron en 2012. El ADVNETLAB en la UACM fue fundado en 2013 en el campus SLT por quien suscribe José Ignacio Castillo Velázquez, con recursos propios, no de la UACM, una vez que hubo masa crítica de egresados de ISET e interés sobre el tema de redes avanzadas. Con base en mi experiencia en universidades (UTM, UPAEP, BUAP, UAM, UDEFA, UACM) y empresas (DICINET, IFE, REDUNO-TELMEX, Data Center Dynamics) desarrollé la metodología ADVNETLAB, la cual está en constante reajuste y con la que se dirigen las tesis y otros proyectos.

Desde 2015 a la fecha se han titulado 15 estudiantes de licenciatura bajo la metodología ADVNETLAB, hemos producido 14 tesis con 15 estudiantes de telecomunicaciones (ANL-1 al ANL-15), 12 de la UACM México y 3 de la UNAS Perú. Desde ADVNETLAB se han publicado 24 artículos indexados en SCOPUS, tanto en redes avanzadas como en seguridad informática, software y educación; 15 de ellos publicados con los ahora ingenieros. Se desarrolló UTILCON, un sistema de gestión de congresos o seminarios u otro tipo de eventos académicos gratuito en línea y en español, 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 trabajos anteriores en ADVNETLAB se han abordado desde 2013 a 2018 la conectividad y gestión para las redes avanzadas CUDI, CLARA, Internet2, CANARIE, REUNA, Geant, AfricaConnect y Multicast bajo protocolos IPv4. Desde 2018 a la fecha se trabaja en las actualizaciones al estudio de redes avanzadas, bajo protocolos IPv6 y SDN, así como el estudio de redes regionales y la interconexión entre éstas para incrementar así el nivel de complejidad. En esta ocasión se presentan Itzel Iliana Rosas Suárez y Diana Laura Fernández Tinoco (ANL16 y ANL17) con el trabajo correspondiente a la Emulación de la gestión de las redes avanzadas europea y africana con IPv6, bajo sus topologías más actualizadas, para el cual se ponen a prueba la conectividad y gestión de las redes avanzadas con las que se unen dos continentes, como sucede en los centros de operaciones de red de que involucran a varias compañías proveedoras de internet alrededor del mundo.

Mis felicitaciones a las señoritas Rosas y Fernández por el trabajo concluido y porque terminaron en 10 meses efectivos, culminando en junio de 2021 para un aproximado de 1,500 hrs, cuando desde 2013 a la fecha en ADVNETLAB los tiempos que tomaron las 13 tesis anteriores fueron de entre 12 y 17 meses efectivos para un aproximado de 2,000 hrs. Este trabajo lo iniciamos en 2020 y lo desarrollamos bajo las condiciones de la pandemia de COVID-19, lo cual obligó a abordar el proyecto sumando recursos económicos de las estudiantes para actualizar su computadora para poder abordar el trabajo. Finalmente, el pasado 16 de agosto recibimos la carta aceptación de un artículo producto de la tesis, el cual se publicará el congreso internacional IEEE ETCM 2021 indexada a Scopus.

M. en C. José Ignacio Castillo Velázquez

Director de tesis - Agosto de 2021

ÍNDICE

CAPÍTULO 1. INTRODUCCIÓN

1.1 INTRODUCCIÓN

Las Redes Avanzadas denominadas como Segunda Internet, permiten interconectarse entre sí con varias redes alrededor del mundo, las RA son importantes para el desarrollo de nuevas tecnologías. El uso de estas redes permiten a los científicos, investigadores y académicos experimentar nuevos protocolos y desarrollos tecnológicos. Por otra parte, no todas las instituciones podrían conectarse a este tipo de redes, por su alto costo. Para ser parte de una RA se debe contar con un fuerte fondo de inversión para poder actualizar su infraestructura, estas redes avanzadas ofrecen un backbone con gran ancho de banda y gran disponibilidad, dado que son redes apartadas de la internet comercial por lo que representan un tráfico diferente y es poco probable que pierdan datos confidenciales.

Cada red avanzada ha ido evolucionando según su localidad, con actualizaciones independientes, han surgido dos grandes Redes Nacionales de Investigación y Educación (NREN) en los continentes africano y europeo, como AfricaConnect y Geant.

La infraestructura de backbone de estas redes avanzadas es propiedad de algunas empresas de Internet Service Provider. En estas redes, cada ISP utiliza protocolos de enrutamiento, como OSPF con algoritmo Dijkstra para la conexión y SNMP para el monitoreo y la administración, entre otros protocolos. En este trabajo nos hemos interesado en el estudio de las topologías AfricaConnect2 y Geant. AfricaConnect2 es resultante de la integración del backbone de tres redes avanzadas en África. Las 28 NREN africanas están integradas por Red Regional de Investigación y Educación de África Oriental y Meridional (UBUNTENET), Investigación de África Occidental y Central y Education Network (WACREN) e Investigación y Educación de los Estados Árabes Network (ASREN), con ancho de banda promedio de 100 Mbps. Ahora bien, Geant está integrada por 50 NREN europeas, operando con un ancho de banda de hasta 500 Gbps. Ambas redes avanzadas se encuentran conectadas al mundo mediante el BGP [1].

A diferencia de otros trabajos realizados dentro del laboratorio ADVENTLAB, en este trabajo, se desarrolló una emulación GNS3 donde se verificó conectividad en la red, la interconexión entre sistemas autónomos y finalmente la administración de la topología AfricaConnect2 - Geant en la que se aplicaron los protocolos IPv6 como OSPFv3, SNMPv3 y BGP-4. Gracias a este último, se pueden interconectar sistemas autónomos, por lo cual la topología tiene un mayor grado de complejidad, debido a la adición de la

configuración de redistribución, con el fin de que los sistemas autónomos alcancen conectividad. Estas características son muy útiles para los administradores de red que trabajan en un centro de operaciones de red (NOC) o una empresa ISP.

Para comprender mejor la importancia y los beneficios de las NREN, a continuación, se presentarán algunos proyectos existentes en estas redes.

1.1.1 AfricaConnect2

Tanzania Education and Research Network **(TERNET) supera las barreras de la enseñanza y el aprendizaje global** - Este proyecto busca una moderna enseñanza y aprendizaje para la educación superior con el fin de mantenerse en contacto con otros campus asociados en diferentes partes del mundo, por ejemplo la Universidad Aga Khan es una de las 67 instituciones miembros de la NREN de Tanzania, miembro de la Alianza UBUNTUNET que opera la Red UBUNTUNET, interconectando NREN en toda la región y con otras redes troncales regionales, como Geant en Europa [2].

WACREN forja alianzas estratégicas para apoyar a las mujeres en las Tecnologías de la Información y de la Comunicación (TIC) – Este proyecto tiene como objetivo brindar oportunidades y estrategias para que las mujeres mejoren sus habilidades de programación, por lo que se lanzó su primer evento Women in WACREN bajo el tema "Computación física con Python". Otros de los aspectos importantes es erradicar los prejuicios inconscientes y las normas culturales que afectan la preparación y las experiencias de las mujeres, en el campo [3].

Protección de los recursos del suelo en Zambia – Este proyecto permite a los investigadores obtener rápidamente grandes conjuntos de datos a través del acceso a Internet de alta velocidad para comprender con precisión los procesos físicos, químicos y biológicos del suelo. Los resultados de análisis más rápidos les permiten monitorear la degradación del suelo y ayudar a proporcionar información sobre políticas de gestión sostenible de la tierra [4].

1.1.2 GEANT

Física de partículas – Geant hace posible que los científicos puedan colaborar permitiendo que se lleven a cabo experimentos como el Gran Colisionador de Hadrones que produce cada vez mayores cantidades de datos para compartirse en todo el mundo [5].

Espacio – Geant hace posible que los científicos observen simultáneamente la misma área del cielo a través de múltiples telescopios alrededor del mundo y la última tecnología de radioastronomía proporciona la vista más detallada del universo hasta la fecha. Los siguientes tres proyectos forman parte del proyecto Espacio: el proyecto ORIENTplus entrega resultados cósmicos por por ejemplo, tormentas magnéticas o llamaradas, reacciona con la atmósfera y se convierte en 'lluvias cósmicas', que pueden desempeñar un papel en la formación de nubes y el cambio climático mediante el estudio de los rayos gamma, proyecto EXPReS hace interconexión de telescopios remotos para permitir la observación en tiempo real y el proyecto NEXPReS hace una mejora de las técnicas de astronomía para un mejor estudio del universo [6].

Salud y Medicina - Con la ayuda de la red Geant, la comunidad de investigación biomédica puede compartir datos y trabajar juntos, investigar enfermedades específicas en múltiples regiones del mundo, los médicos pueden comparar métodos de tratamiento y los investigadores pueden encontrar patrones en condiciones clínicas. Se encuentran involucrados algunos proyectos como: Geant y NeuGRID, que permiten el diagnóstico precoz de enfermedades neurodegenerativas, Geant y outGRID, que respalda una infraestructura de red de neurociencia global; Geant y DECIDEN, que mejora la calidad de vida de las personas que padecen la enfermedad de Alzheimer [7]. Se abordarán más detalles de las redes avanzadas en el capítulo 2.

1.2 JUSTIFICACIÓN

La razón del estudio de las redes avanzadas nació del interés de poder profundizar en la información sobre las RA, ya que es un tema poco estudiado, teniendo en cuenta que la información disponible es escasa. Anteriormente se han estudiado las redes avanzadas de México, Chile, EEUU, Canadá, toda Latinoamérica, toda América, África y Europa bajo protocolos IPv4, en algunos casos solo se han realizado las configuraciones y arreglos

necesarios para probar la conectividad, pero en otros se ha agregado la gestión [8, 9, 10, 11, 12, 13, 14, 15, 16].

Previamente en ADVNETLAB en el año 2020 se ha presentado un trabajo para AfricaConnect y otro para Geant bajo IPv6, sin embargo, el presente trabajo también es considerado de interés para ADVNETLAB ya que va más allá en la complejidad de los trabajos anteriores, al interconectar a las dos redes continentales [17, 18]. Por lo tanto, aumenta la complejidad en el número de routers de backbone, también se hace necesario usar un protocolo adicional a los casos anteriores como es BGP-4, tal que permita interconectar ambos sistemas autónomos. Además, se requerirá de mayores capacidades de procesador y memoria para el equipo físico en el que se hace la emulación correspondiente, así como se exigirá más del propio programa de emulación. Estos dos últimos factores son quizás el principal reto para el trabajo.

1.3 OBJETIVO GENERAL

De acuerdo al área de conocimiento de las telecomunicaciones se generan habilidades técnicas y no técnicas. Las habilidades técnicas se basan en formar administradores de redes Wide Area Network (WAN) como Internet para proveer la capacidad de poder entender, comprender probar, analizar y desarrollar redes que serán administradas únicamente por compañías ISP como el backbone de redes avanzadas. De tales en México solo existen 10 a la fecha, y solamente 2 de ellas proveen servicios de redes avanzadas para las instituciones de educación superior y centros de investigación.

Las habilidades técnicas se desarrollarán al emular el funcionamiento de una red avanzada con alto requerimiento de recursos computacionales para evaluar su conectividad y gestión. La red bajo estudio se conforma por la unión de las redes avanzadas de Europa (Geant) y las de África (AfricaConnect) a nivel de backbone. La emulación de la correspondiente red avanzada resultante necesitará del empleo de emulador, máquinas virtuales y otras herramientas. Las habilidades no técnicas por desarrollar son: el trabajo en equipo, la planeación, disciplina y la aplicación de mejores prácticas al desarrollar proyectos bajo la metodología ADVNETLAB.

1.4 OBJETIVOS ESPECÍFICOS

- Estudiar, analizar y emular la conectividad y gestión del backbone de AfricaConnect2 y Geant interconectados como sistemas autónomos utilizando los protocolos OSPFv3 y BGP-4 para el enrutamiento dentro y fuera de los sistemas autónomos y SNMPv3 para la gestión bajo IPv6.
- Poner a prueba al emulador GNS3 y a nuestros equipos de cómputo bajo una topología de red compleja.
- Desarrollar las habilidades de un administrador para redes WAN.
- Desarrollar habilidades de análisis y síntesis de la información.

CAPÍTULO 2. REDES AVANZADAS

2.1 NACIMIENTO Y EVOLUCIÓN DE LAS REDES DE DATOS

En la primera generación de redes en la Research Project Agency NETwork Advanced (ARPANET) v1 se desarrollaron una serie de eventos importantes. ARPA, en el año 1966 usó conmutación de paquetes de acuerdo a las aportaciones de Paul Baran y Donald Watts Davis e inició un proyecto para conectar a las universidades de EEUU. En 1969 se crearon los primeros 4 nodos de ARPANET que conectaron a University of California-Los Ángeles (UCLA), University of California-Santa Barbara (UCSB), Standford Research Institute en California (SRI) y University of Utah (U.Utah). Donde la comunicación se hizo por la red telefónica a 56 Kbps vía Public Switching Telephonic Network (PSTN), también se utilizó el protocolo Network Control Protocol (NCP) que proveía las bases para la aplicación de la transferencia de archivos al comunicar los nodos de ARPANET. En la figura 1.2 se muestra la interconexión de los 4 primeros nodos de la estructura física de ARPANET con sus respectivas computadoras de tipo mainframe, es importante mecionar que la fibra óptica fue inventada en 1970, pero estas tecnologías debía perfeccionarse hasta que en 1983 se hizo comercialmente viable para su implementación en la telefonía de EEUU [19].

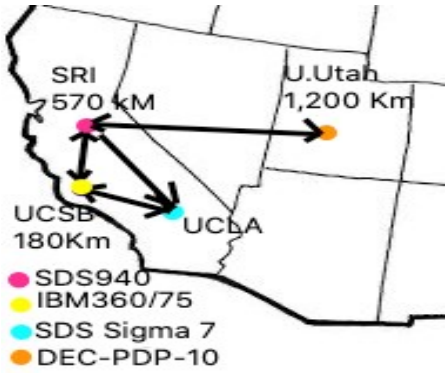


Figura 1.2. Primeros 4 Nodos ARPANET y sus respectivas computadoras [19].

En la segunda generación de redes en la ARPANET v2, para en el año de 1981, nació la red Computer Science Network (CSNET) quién también dio parte a conectar las principales universidades de los EEUU, centros de investigación de Asia, Europa y centros de gobierno e industrias. Para el año de 1983 ARPANET se quedó con un menor número de nodos al separarse de la red Militar Network (MILNET), para este mismo año se conectó CSNET con ARPANET. Al ver la National Science Foundation (NSF) que

CSNET se conectó de manera exitosa con ARPANET creó la National Science Fundation Network (NSFNET) que nacería para el año de 1985, con el objetivo de formar una red de redes con intención académica conectada a la red ARPANET, donde se logró conectar 100 universidades y centros de investigación en EEUU y Europa. Otro hecho importante es que en el año de 1984 se contaba con más servidores, por lo que se inventó el Domine Name Systems (DNS) para poder organizarlos en dominios y hacer las resoluciones de las direcciones IP. Por lo que para el año 1988 se liberó el estándar de Routing Information Protocol (RIP), el cual es un protocolo de tipo Internal Gateway Protocol (IGP), es decir, trabaja dentro de un Autonomous System (AS) y para el año de 1989 se liberó el protocolo BGP para conectar a los AS, a su vez se liberó Open Systems Interconnection (OSI) - Sistema de Interconexión Abierto de (ISO) y hasta 1990 ARPANET dejaría su lugar a NSFNET.

Para la tercera generación se inició la transición de banda ancha, dada la demanda de servicio que el backbone de la NSFNET provocó debido al crecimiento de sus nodos, ya que para el año de 1991 había aumentado a 16 nodos y podía conectar a más de 3500 redes. De igual manera, para este mismo año nació el Comercial Internet eXchange (CIX) proyecto que después traería ventajas a la NSFNET para el libre intercambio de tráfico que tendría entre las redes comerciales, lo cual propició a la idea de la Internet comercial. Por otro lado en 1993 National Center for Supercomputing Applications (NCSA) liberó el primer (Web Browser) llamado Mosaic, de la Universidad Ilinois, por lo que también habría que decir que para 1995 creció la Internet de una forma exponencial, y fue la pauta para que la NSFNET desapareciera y tomara su lugar la Internet comercial. Los ISP serían el medio que conectaría a los clientes con la Internet y se dio lugar a los protocolos de enrutamiento, a la arquitectura de sistemas autónomos, a los routers, al protocolo TCP/IPv4 y el direccionamiento por clases. A manera de resumen en la figura 2.2 se muestra las fechas más relevantes desde el nacimiento de ARPANET hasta Internet comercial [19, 20]

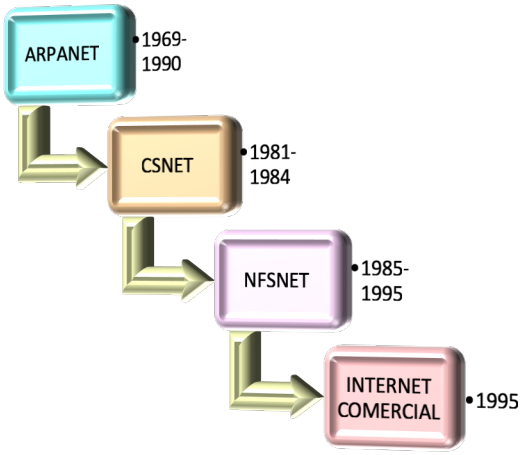


Figura 2.2. Evolución de las redes [19].

La cuarta generación tiene como datos relevantes la presentación del protocolo IPv6, para el año de 1998 a partir de esto, éste se probo funcionalmente en el 2000 con la red avanzada Internet 2. Se da lugar a IPv6 debido a la creciente demanda de usuarios conectados a Internet, donde en los años de 1981 al 2012, se notó el crecimiento de Internet de manera exponencial, por lo que para el año 1981, había menos de 1000 usuarios conectados a Internet, mientras que para el 2012 llegó hasta los 2,300 millones de usuarios conectados a ésta, mismo año en el que hubo cambios en los browsers.

Por otro lado, cuando se creó ARPA, NSFNET e Internet comercial existía un sistema de neutralidad en la red, es decir los usuarios podían acceder a una misma velocidad y sin ningún costo, pero en el año 2008 la economía de EUA y mundial se estancó y había que sacar dinero de algún lado, por lo que cambió a un sistema de no neutralidad, es decir se redujeron algunos servicios a los usuarios, no permitiendo el acceso para todos, al menos que pagaran por ello. Las empresas que invierten en la infraestructura de telecomunicaciones como AT&T, Verizon COMCAST en EUA, no son las que más dinero obtienen de ella, sino empresas como las Facebook, Amazon, Google, Apple (FAGA) por sus productos de software.

En la Tabla 1.2 se presentan las características más importantes de las generaciones de redes de datos [19, 20].

Características y generaciones de las redes datos:

Generación	Enrutamiento	Familia de protocolos	Ejemplo de red	Fecha
1	IMP	NCP	ARPANET	(1969-1982)
2	Gateway	TCP/IP	ARPANET/MILNET	(1983-1990)
3	Routers	TCP/IPv4	CSNET/NSFNET/INTERNET COMERCIAL/INTERNET 2	(1990-2011)
4	Routers	TCP/ IPv4/IPv6	INTERNET COMERCIAL/INTERNET2	(2012 -)

Tabla 1.2. Generaciones de redes de acuerdo a sus características [20].

2.2 REDES AVANZADAS

El uso de las redes avanzadas está destinado solo para el uso académico, es decir no para uso comercial y utilizandose sólo para fines cientificos y de investigación. En el año de 1969 ARPANET nació como un proyecto de Red Académica, ya que fue la primera red entre universidades.

Con el paso de los años se desarrollaron Redes Académicas de Orden Mundial como Internet2, CANARIE, DANTE, Geant, AfricaConnect2, CUDI, CLARA entre otras, que son consorcios u organizaciones sin ánimo de lucro, estos conforman una red Red Académica de Alta Velocidad (RAAV) a través de un conjunto de instituciones que deciden interconectarse a través de enlaces de comunicación de gran capacidad, además ponen en contacto a sus investigadores para procesos de investigación y colaboración. De esta forma es que en la actualidad es posible encontrar aplicaciones y servicios como Telemedicina, videoconferencias, acceso a recursos remotos, laboratorios virtuales, bibliotecas digitales, mayores capacidades de almacenamiento y procesamiento en equipos de cómputo etc., con el fin de desarrollar aplicaciones de tipo científico, tecnológico y social.

Este tipo de redes representan una oportunidad para el crecimiento de nuestro país, así como lo fue con la llegada de las telecomunicaciones digitales, que fueron las bases para evolucionar hacia una red académica sustentada con los desarrollos de la conmutación de paquetes que se consolida en lo que ahora conocemos como Internet.

No se pueden dejar de lado las RAAV, ya que con ellas sucederán adelantos muy importantes para la ciencia y la tecnología generados por investigadores y académicos de todo el mundo [21].

2.3 RED AVANZADA AFRICACONNECT2

AfricaConnect2 se basa en tres redes existentes divididas en áreas geográficas (o "clúster") como son: África oriental y meridional, Norte de África y África occidental y central. El objetivo general de AfricaConnect2 es contribuir a la reducción de la brecha digital, para contar con suficientes recursos de las TIC y fomentar el desarrollo sostenible en África. También apoya el desarrollo de redes de Internet de alta capacidad para la investigación y educación en África. Por otro lado posibilita conexiones con la red paneuropea, que ofrece una puerta de entrada para colaboraciones globales en investigación y educación.

AfricaConnect2 es un proyecto que comenzó en el 2015 y terminó en el 2019, esta se ha sustentado en el trabajo realizado por los proyectos EUMEDCONNECT (2004 – 2005) y AfricaConnect (2011 - 2015) que han contribuido a apoyar la creación y puesta en marcha de redes de investigación y educación (REN) de alta capacidad en África. Para esto, AfricaConnect2 contó con un financiamiento de 26.6 millones de euros, de los que 20 millones fueron aportados por la Dirección General de Cooperación Internacional y Desarrollo de la Comisión Europea (DG DEVCO). Los fondos restantes (6.6 millones de euros) los aportaron los socios africanos.

Cabe mencionar que se aprovecharon los resultados de proyectos anteriores para contribuir a mejorar el desarrollo del capital humano en África, de modo que se consolidó AfricaConnect3, por lo que se aceleró a partir de la pandemia COVID-19 iniciando en febrero del 2020, dado que se dio un incremento a las demandas de herramientas de comunicación, así como Geant4-3N se aceleró bajo las mismas circunstancias. [22] Este proyecto estará soportado por AfricaConnect2 conformado por 29 NREN africanas como son:

UBUNTUNET conformado por 15 NREN

WACREN conformado por 10 NREN

ASREN conformado por 4 NREN

UBUNTUNET es la red que pertenece al Grupo 1 de África oriental y meridional, y están organizadas bajo Ubuntu Net, la red troncal regional que interconecta las NREN y las conecta a otras redes regionales.

El socio Ubuntu Net Alliance es la asociación regional de NREN en África, que fue creada en el 2005 con el fin de asegurar la conectividad a la internet de alta velocidad para la

comunidad africana de investigación y educación, también es el implementador de este grupo que tiene la responsabilidad administrativa, financiera y de operaciones técnicas. El objetivo es consolidar y expandir la red Ubuntu Net existente, adoptando nuevos servicios de infraestructura electrónica así como mejorar la interconectividad entre los participantes en redes de investigación y educación (REN) en África y su conectividad con la investigación y redes de educación en todo el mundo así como con Internet en general; desarrollar el conocimiento y las habilidades de los profesionales de las TIC en estas instituciones; y proporcionar servicios auxiliares relacionados con las REN.

WACREN es la red que pertenece al Grupo 2 África occidental y central, esta red regional comenzó en el 2006 con AfNOG que es una comunidad de Ingenieros que cooperan e intercambian información para impulsar y operar la infraestructura de Internet en África y en Internet global, organizado por AAU (Asociación de Universidades Africanas). Fue un requisito indispensable desarrollar la capacidad organizativa y técnica dentro de los países que constituyen las NREN para considerarla como una red viable.
En marzo 2011 en la ciudad de Dakar por la iniciativa de la RENU (Unidad de Redes de Investigación y Educación) de la asociación AAU se estableció la primera juta directiva de WACREN con los representantes de los 11 países de África Occidental y África Central.

En julio del 2013 en la ciudad de Abuja celebraron su primera reunión anual en la que las partes interesadas de WACREN nombraron un director ejecutivo, eligieron un presidente de la junta y establecieron un comité de búsqueda para la nominación de los miembros, por lo que para agosto de este mismo año el proceso se consolidó y ahora se compone de 6 miembros incluido el Chief Executive Officer (CEO). Los objetivos de WACREN son interconectar redes nacionales de investigación y educación en África Occidental y Central para formar una red regional de investigación y educación con la misión de construir y operar infraestructura de red de clase mundial; desarrollar la provisión de servicios de vanguardia y promover la colaboración entre comunidades de investigación y educación nacionales, regionales e internacionales; así como desarrollar la capacidad de la comunidad NREN en la región.

TANDEM es un proyecto que tiene como objetivo facilitar el diálogo entre WACREN, los usuarios finales, las NREN y los institutos de investigación y educación superior de

la región de África occidental y central. TANDEM, a su vez ayuda a WACREN a lograr sus objetivos y poder participar en el proyecto de AfricaConnect2.
ASREN es la red que pertenece al Grupo 3 del Norte de África esta es la Red de Educación e Investigación de los Estados Árabes, es una organización internacional sin fines de lucro, registrada en Dusseldorf, Alemania, el 3 de junio de 2011, y es la asociación de las NREN junto con socios estratégicos que tienen por objetivo implementar, gestionar y ampliar infraestructuras electrónicas panárabes sostenibles y conectar las instituciones árabes entre ellas y con el mundo a través de redes de comunicaciones de datos de alta velocidad. Estas redes permitirán compartir y acceder a una variedad de servicios y aplicaciones de investigación. A su vez, ASREN facilita la colaboración y cooperación entre los investigadores y académicos de la región árabe aumentando la disponibilidad y accesibilidad de los recursos de conocimiento para estudiantes e investigadores, promoviendo el desarrollo de contenidos árabes y su disponibilidad, facilitando el intercambio de conocimientos y los procesos de transferencia en toda la región con socios en Europa y en todo el mundo.

En la figura 3.2 se observa la conectividad de la red AfricaConnect del año 2015, pero es importante mencionar que sigue vigente hasta el año 2021 y es proporcionada por International Bank for Reconstruction and Development/The World Bank, actualmente disponible en la página oficial de AfricaConnect2, así como sus respectivos países que lo integran que se muestran en la tabla 2.2 [23].

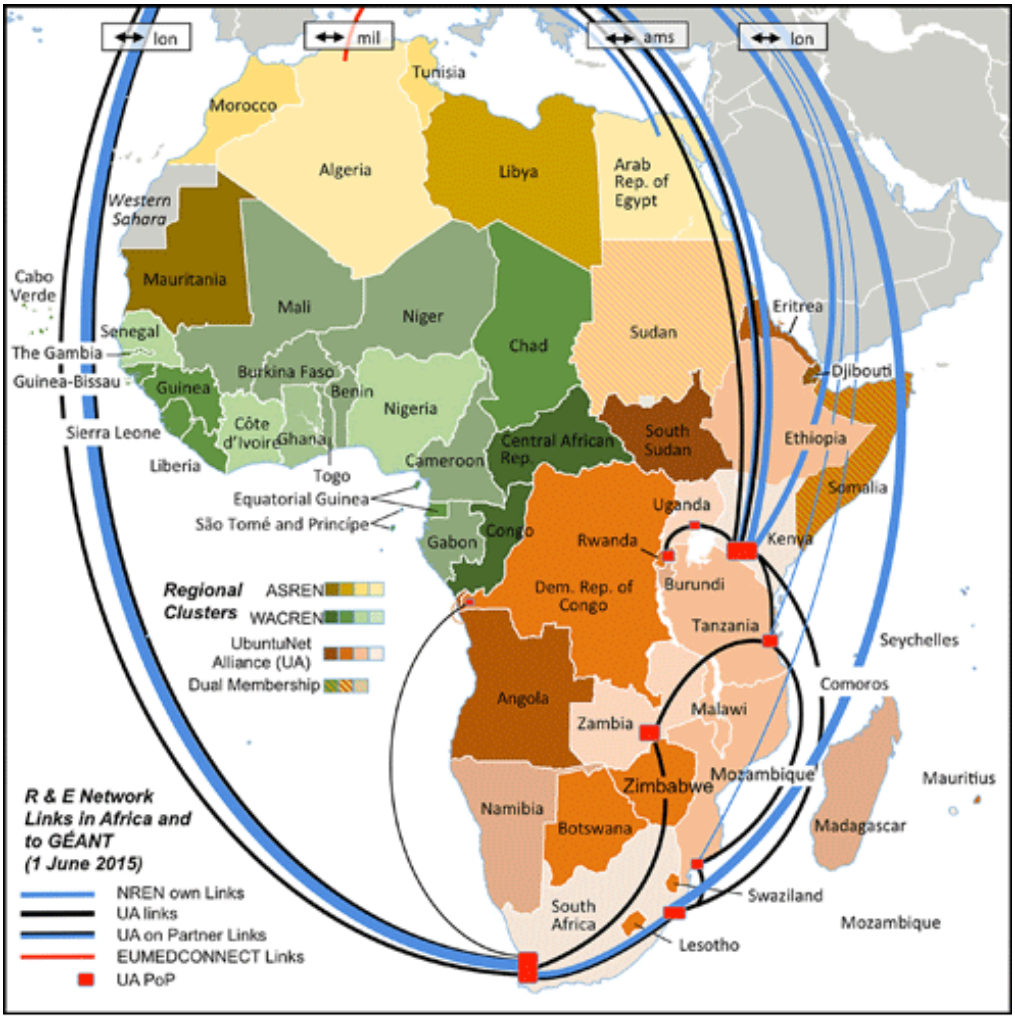


Figura 3.2. Topología AfricaConnect2 [24].

Burundi	**Congo Democratic Republic**	**Ethiopia**	**Kenya**	**Madagascar**	**Mali**	**Maputo Mozambique**
Rwanda	Somalia	Sudan	South Africa	Tanzania	Uganda	Namibia
Zambia	Benin	Cameroon	Gabon	Ghana	Ivory Coast	Mali Republic
Niger	Nigeria	Senegal	Togo	Algeria	Tunisia	Egipto
Morocco						

Tabla 2.2. Países miembros de AfricaConnect2.

2.4 RED AVANZADA GEANT4 -2

En el 2014 las asociaciones TERENA Y DANTE unificaron fuerzas para realizar el proyecto Geant, atendiendo las políticas de restructuración por parte de la comunidad de las NREN europeas, bajo una estructura de gobernanza unificada.

El Proyecto Geant ha evolucionado a través de GN1, GN2, GN3, GN3plus y GN4-1. La fase del proyecto GN4-2, comenzó el 1 de septiembre de 2017 al 31 de diciembre de 2018, generación que se introducirá en esta tesis; cabe mencionar que el 1 de enero de 2019 se introdujeron los proyectos GN4-3 y GN4-3N, pero debido a la COVID-19 aumentó la demanda de aplicaciones y servicos como: acceso a plataformas académicas, videoconferencias, laboratorios virtuales, bibliotecas digitales, entre otras, generando un aceleramiento en éstas dos últimas versiones de Geant, donde se esforzaron en la realización de actualizaciones en la medida de lo posible [25].

El proyecto Geant permite el desarrollo de las comunidades de investigación de Europa y del mundo. El responsable de la creación de Geant es DANTE que es una organización inglesa establecida en Cambridge con el fin de gestionar los servicios de redes avanzadas para la comunidad investigadora y académica europea, además de ser el coordinador del consorcio Geant. La red Geant interconecta las NREN europeas, opera a velocidades de hasta 500 Gbps y llega a más de la mitad de los países del mundo, ofreciendo los niveles más altos de capacidad y seguridad que requieren los usuarios de investigación y educación. El proyecto Geant ofrece numerosos servicios y aplicaciones proporcionando una conectividad de alta velocidad necesaria para compartir, acceder y procesar grandes volúmenes de datos, para respaldar y mejorar las opciones de conectividad disponibles como son: monitoreo de red, mejora del desempeño, confianza e identidad, seguridad, servicios de nube y movilidad.

El proyecto GN4-2 cuenta con dos periodos, el primer periodo inició el 1 de mayo del 2016 y finalizó el 31 de agosto del 2017, operando a una velocidad de 100Gbps. Contando con un total de 41 países de Europa y sus alrededores en su red. El segundo periodo se dio el 1 septiembre de 2017 al 21 de diciembre de 2018 como se muestra en la figura 4.2, operando a una velocidad de 500 Gbps conectando a un total de 43 países europeos en su red, los cuales se muestran en la tabla 3.2. El objetivo de la red GN4-2 es mantenerse separada de la Internet comercial, a fin de que sea sólo para usuarios de investigación y

educación. Esta red continúa ofreciendo un rendimiento rentable y extremadamente alto para todos los usuarios, al mismo tiempo refuerza la posición de Europa a la vanguardia de la investigación.

La red Geant posibilita el avance de proyectos garantizando un acceso equitativo a la red de investigación en infraestructuras y recursos de infraestructura electrónica en Europa, por esto es que han existido varias actualizaciones de la red [26].

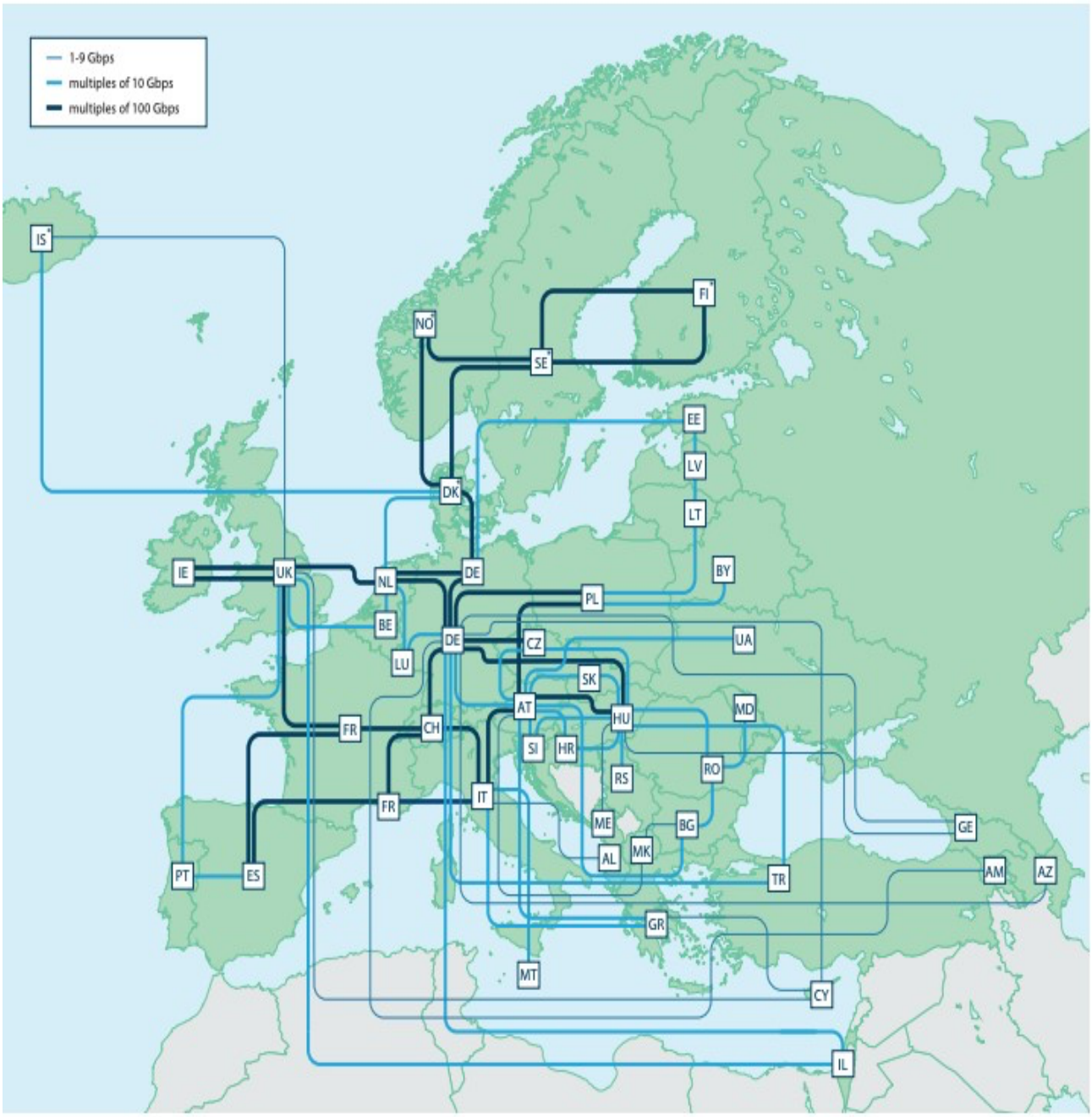
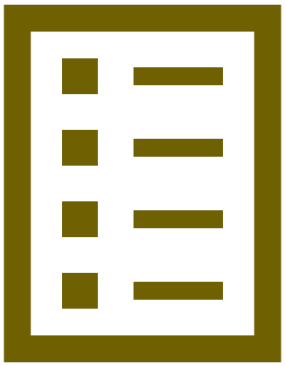


Figura 4.2. Red Geant4-2, año 2018. [27]

AL- **Albania**	BE- **Belgium**	CY- **Cyprus**	EE- **Estonia**	GE- **Georgia**	IE- **Ireland**	LT- **Lithuania**	ME- **Montenegro**	NO- **Norway**	KS- **Serbia**	TR- **Turkey**
AM- **Armenia**	**BG-** Bulgaria	**CZ-** Czech Republic	**ES-** Spain	**GR-** Grece	**IL-** Israel	**LU-** Luxembourg	**MK-** F.Y.R Macedonia	**PL-** Poland	**SE-** Sweden	**UK-** United Kingdom
AT- **Austria**	**BY-** Belarus	**DE-** Germany	**FL-** Finland	**HR-** Croatia	**LS-** Iceland	**LV-** Latvia	**MT-** Malta	**PT-** Portugal	**SI-** Slovenia	**UK-** Ukraine
AZ- **Azerbajian**	**CH-** Switzerland	**DK-** Denmark	**FR-** France	**HU-** Hungary	**IT-** Italy	**MD-** Moldavia	**NL-** Netherlands	**RO-** Romania	**SK-** Slovakia	

Tabla 3.2. Países miembros de la topología GN4-2 [9].



CAPÍTULO 3. PROTOCOLOS

3.1 IPv6 COMO SUCESOR DE IPv4

En 1983 fue puesto en marcha el protocolo IPv4, el cual tiene un direccionamiento de 32 bits, por lo que permite un número máximo de 4.294.967.296 (2^{32}) direcciones IP diferentes, en el tiempo en que se desarrolló, se creía que la cantidad de direcciones era suficiente para identificar todas las computadoras en la red y soportar el surgimiento de nuevas subredes, no obstante, con el rápido crecimiento de la Internet surgió el problema de la escasez de las direcciones IPv4, hasta ahora se estima que las dos terceras partes de las direcciones que ofrece este protocolo ya están asignadas, lo que originó la creación de una nueva generación del protocolo IP, por lo que para el año de 1998 fue presentado IPv6, una nueva versión del Protocolo de Internet, diseñado como el sucesor de IPv4 que actualmente se encuentra en uso, este nuevo estándar mejorará el servicio a nivel global. El direccionamiento IPv6 está formado por:

$2^{128} = 340 \times 10^{36}$ direcciones de redes diferentes [28].

3.1.1 Cambios principales entre IPv6 e IPv4:

Capacidades de direccionamiento ampliadas: IPv6 aumenta el tamaño de la dirección IP de 32 bits a 128 bits, lo que permite direcciones IP únicas y prácticamente ilimitadas, por lo que se incrementa el espacio de direcciones permitiendo identificar un mayor número de dispositivos en la red y la mejora de la escalabilidad del enrutamiento “multicast”, no obstante, también se agregó un nuevo tipo de direccionamiento “anycast”.

Simplificación del formato de encabezado: Algunos campos de encabezado de IPv4 se han eliminado o se han hecho opcionales, con el fin de reducir el costo de procesamiento de los paquetes en los routers.

Soporte mejorado para extensiones y opciones: Los cambios del encabezado base IP permiten un enrutamiento más eficiente y una mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de etiquetado de flujo: Se agrega una nueva capacidad para permitir la identificación de paquetes pertenecientes a determinados "flujos" de tráfico.

Capacidades de autenticación y privacidad: se agregaron encabezados de extensión para admitir autenticación, integridad y la confidencialidad de los datos para IPv6 [29].

3.1.2 Direccionamiento IPv6

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Hay tres tipos de direcciones [30]:

1. ***Unicast:*** Esta dirección identifica una única interfaz, donde el paquete es enviado a una dirección de unidifusión que se entrega a esa única interfaz.

2. ***Anycast:*** Dirección que identifica un conjunto de interfaces donde el paquete es enviado a una dirección anycast que se entrega a una de las interfaces identificadas por esa dirección (la "más cercana", según la medida de distancia de los protocolos de enrutamiento), es decir, de 'una' a 'una de muchas'.

3. ***Multicast:*** Al igual que la dirección anycast, identifica un conjunto de interfaces, donde el paquete es enviado a una dirección de multidifusión que se entrega a todas las interfaces identificadas por esa dirección, hay que resaltar que no existen las direcciones de difusión (broadcast) para IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast, es decir, de 'una' a 'muchas'.

3.1.3 Representación de IPv6

Es importante mencionar la sintaxis de la representación de IPv6, hay 2 formas convencionales para representar direcciones IPv6 como cadenas de texto:

1. La forma convencional es X: X: X: X: X: X: X: X, donde las X son los valores hexadecimales de 16 bits de la dirección, es decir cuenta con una longitud de 128 bits.
Ejemplo:

2001: FAB8: ABCD: 1237: EFAD: 1F4F: 7136: 8230

2. Debido a algunos métodos para asignar ciertos estilos de las direcciones de IPv6, será común que las direcciones contengan cadenas largas de cero bits. una sintaxis especial está disponible para comprimir los ceros.

Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo:

2001: FAB8: ABCD:0000: EFAD: 1F4F: 7136: 8230

2001: FAB8: ABCD: : EFAD: 1F4F: 7136: 8230

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos, la compresión sólo se permite en uno de ellos. Así, son representaciones posibles de una misma dirección: 2001: FAB8: 0000: 0000: 0000: 0000: 7136: 8230 las siguientes:

2001: FAB8: 0000: 0000: 0000 : : 7136: 8230
2001: FAB8 :0:0:0:0: 7136: 8230
2001: FAB8 :0: :0: 7136: 8230
2001: FAB8 : : 7136: 8230

Estas direcciones son válidas y significan lo mismo.
Ejemplo de cuando una dirección no es válida:
A1DF: :CA98: :321F
No es considerada válida porque no queda claro cuántos grupos nulos hay en cada lado [30].

3.1.4 Formato de encabezado IPv6

En la figura 1.3 se muestra el formato del encabezado IPv6 el cual tiene algunos cambios respecto al formato del encabezado IPv4 para hacerlo más simple con tan solo 8 campos y con un tamaño fijo de 40 bytes, más flexible en cuanto a la extensión por medio del encabezado adicional como el identificador de flujo y más eficiente respecto al costo de procesamiento de los paquetes. Estos cambios permiten que el tamaño total del encabezado IPv6 sea cuatro veces mayor de la versión anterior, es decir, teniendo un direccionamiento de 128 bits [29].

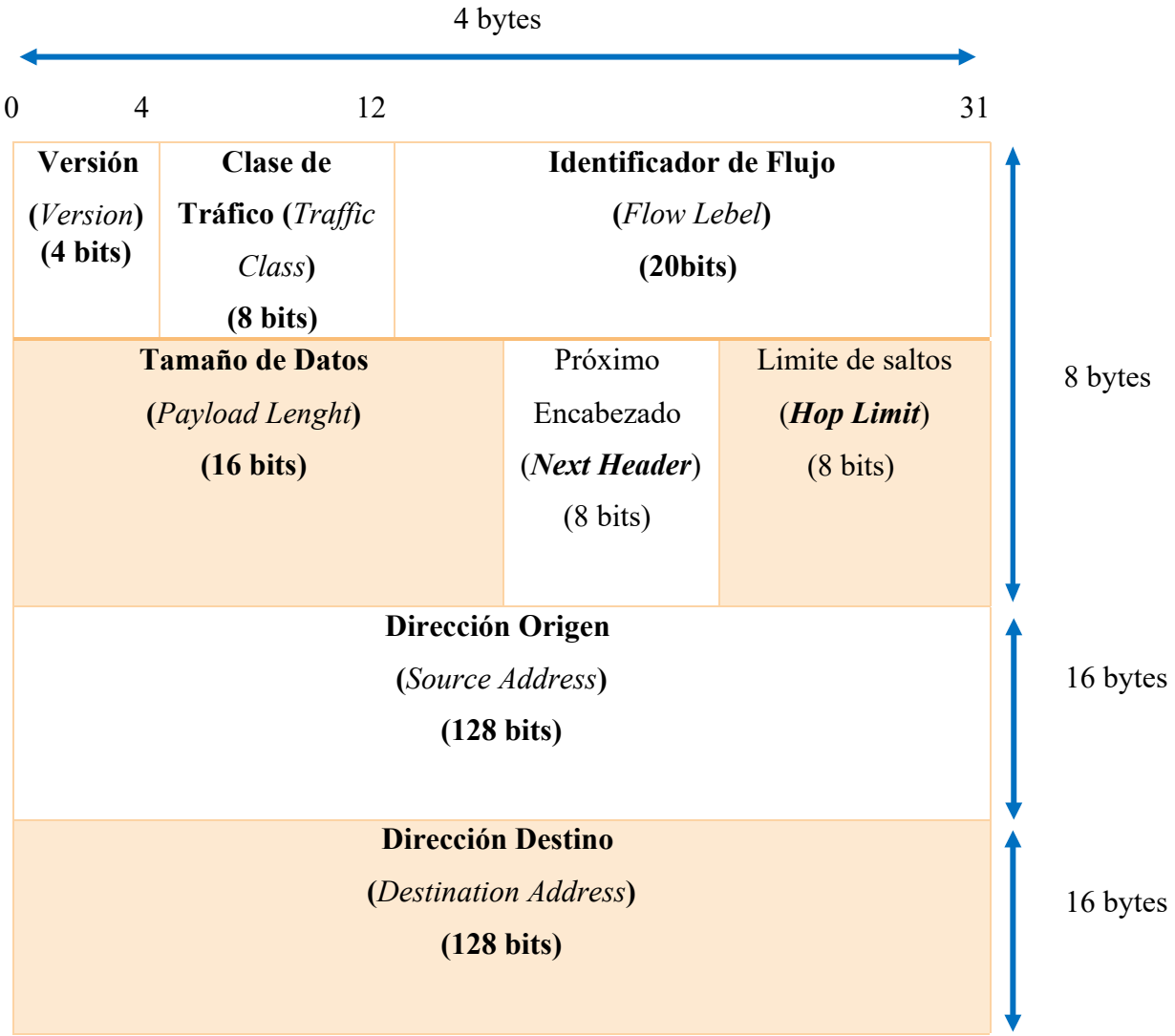


Figura 1.3. Formato de encabezado IPv6 [29].

A continuación, se explica cada uno de los campos del formato:

***Versión**:* Este campo identifica la versión del Protocolo de Internet, para este caso el valor es 6, por IPv6.

Traffic Class: Este campo identifica y diferencia los paquetes de enrutamiento por clases de servicios o prioridad según sea el caso.

Flow Label: Este campo permite que el router identifique el tipo de flujo (capa 3) ISO/OSI, de cada paquete.

Payload Lenght: Este campo indica el tamaño, en bytes, de los datos enviados, ligado con el encabezado IPv6.

Next Header: Identifica el encabezado que sigue al encabezado de IPv6 e indica los valores de los encabezados de extensión.

Hop Limit: Contador que se decrementa en 1 por cada nodo que reenvía el paquete, el paquete se descarta si el límite de saltos se reduce a cero.
Source Address: Indica el origen del paquete.
Destination Address: Indica el destino del paquete.

3.2 PROTOCOLO DE ENRUTAMIENTO OSPFv2

El protocolo de enrutamiento de estándar abierto Open Shortest Path First (OSPF), toma este nombre dado que se puede implementar para diferentes plataformas, este busca encontrar la ruta más corta, por lo que emplea el algoritmo Shortest Path First (SPF) de Dijkstra, que soporta una mejor convergencia en la red respecto del resto de los protocolos, es decir, qué tan rápido se actualizan las tablas para que todos los routers tengan la misma información. Una de las ventajas de OSPF, es el tipo de algoritmo que soporta redes más grandes con una métrica o coste establecido por el propio fabricante, a diferencia del protocolo RIP que emplea el algoritmo Bellman-Ford, el cuál soporta redes más pequeñas recordando que su métrica es de 15 saltos. El protocolo OSPF fue diseñado para aplicarse dentro de un Sistema Autónomo (AS), por lo tanto, es de tipo IGP, así que cada router dentro del AS debe contener una base de datos idéntica, de manera que a partir de esa BD se calcula una tabla de ruteo, vía la construcción del Shortest Path Tree (SPT). La versión 2 de OSPF para IPv4 (32 bits) apareció en el año de 1998 y la versión 3 de OSPF para IPv6 (128 bits) apareció en el año 2018. En la figura 2.3 se muestra el formato de encabezado OSPFv2 [31, 32].

Características generales de OSPF:

1. Se clasifica por áreas, lo que hace que se puedan utilizar muchas redes. Un router de núcleo Router Backbone (BR) se ubica dentro del área 0, pero un router cuyas interfaces están conectadas dentro de un área que no es el área 0 se le considera un router interno Internal Router (IR), con respecto al router de frontera de área Area Border Router (ABR) interconecta las distintas áreas. En cuanto al router de enlace de sistema autónomo Autonomous System Boundary Router (ASBR) interconecta un AS con otro AS, en tal caso OSPF se conecta a un proceso de enrutamiento externo, que intercambia información con ese proceso.
2. Debido a la clasificación por áreas, se reduce el tamaño de las tablas de enrutamiento, empleando un resumen de rutas por cada router.

3. Envía las actualizaciones de las rutas solamente cuando se le es requerido, por esta razón, se reduce el ancho de banda.
4. Utiliza una base de datos de enlace-estado (Link State), no genera bucles, es decir, no existe una repetición de datos, ya que un router anuncia a su router vecino si tiene su información de su base de datos, sino la tiene, se la envía y continua el proceso.
5. Para hacer más seguras las redes soporta autentificación.
6. Soporta una ejecución de enrutamiento sin clases, es decir incluyen la información de la máscara de subred con la dirección de red en las actualizaciones de routing.
7. Para reducir el impacto en los equipos y routers que no estén activos, utiliza el direccionamiento multicast [33].

3.2.1 Formato de encabezado OSPFv2

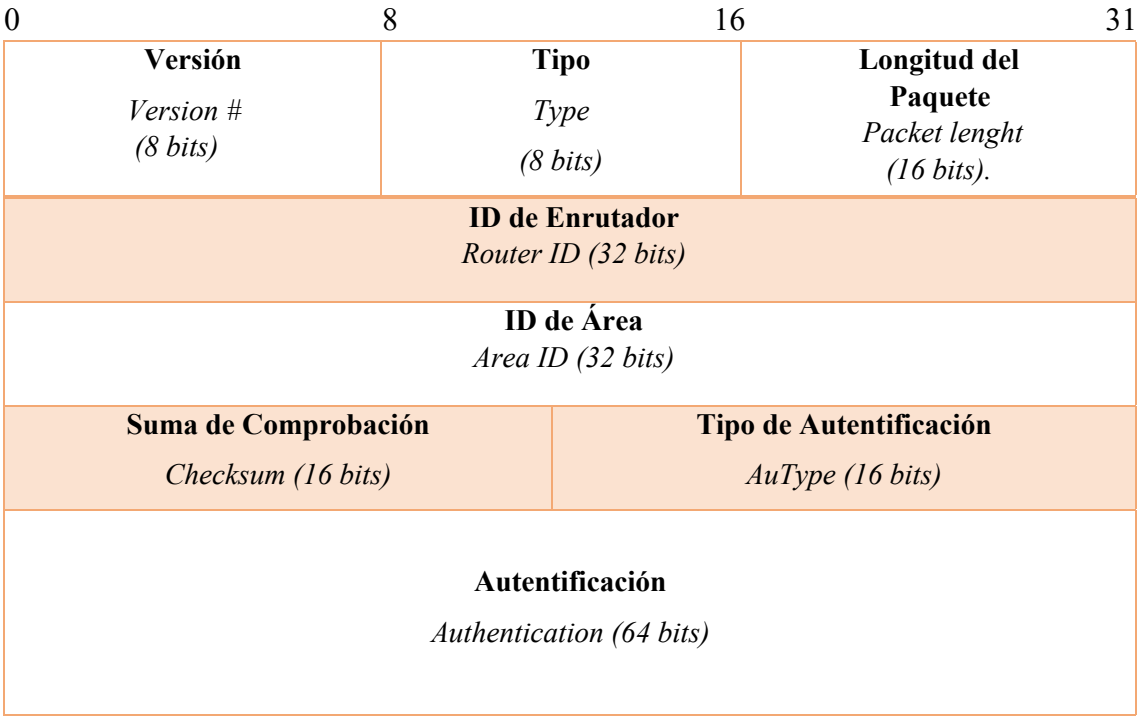


Figura 2.3. Encabezado OSPFv2 [31].

A continuación, se explica cada uno de los campos del formato:

Versión #: Indica el tipo de versión de OSPF

Type: Indica los 5 tipos de paquetes o mensajes OSPF:

1. *Hello:* Descubre los vecinos y establece adyacencias.
2. *Database Description* (DBD): Resume el contenido de la base de datos.
3. *Link State Request* (LSR): Solicitud de información de estado de un enlace especifico durante la fase de intercambio de información entre dos routers.

4. *Link State Update* (LSU): Actualiza la base de datos y envía información específica sobre el estado del enlace.
5. *Link State Acknowledgment* (LSAck): Reconocimiento de flooding (inundación, es decir es la repetición desmesurada de algún mensaje en un corto espacio de tiempo en la red).

Packet lenght: La longitud del paquete del protocolo OSPF.

Roter ID: La ID del router es el que origina los paquetes OSPF.

Área ID: Identifica el área a la que pertenece el router. Todos los paquetes OSPF están asociados con un área única, por ejemplo el 0.0.0.0. es el valor que está reservado para el área de backbone.

Checksum: Es el valor de comprobación de IP estándar de todo el contenido del paquete.

AuType: Identifica el procedimiento de autenticación que se utilizará para el paquete (no autenticación, autenticación simple, autenticación SHA).

Authentication: Son claves y métodos a un sistema, los cuales pueden contener texto plano o encriptación [31].

En relación a las características de OSPF, se explica la clasificación de los routers como se indica en la figura 3.3, de manera que se pueda comprender la segmentación de una red como se muestra en la figura 4.3.

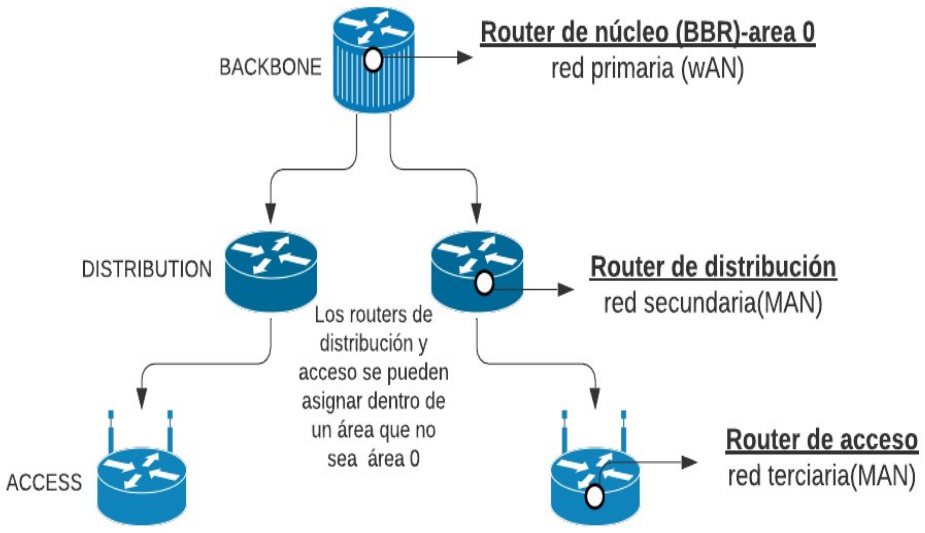


Figura 3.3. Clasificación de Routers.

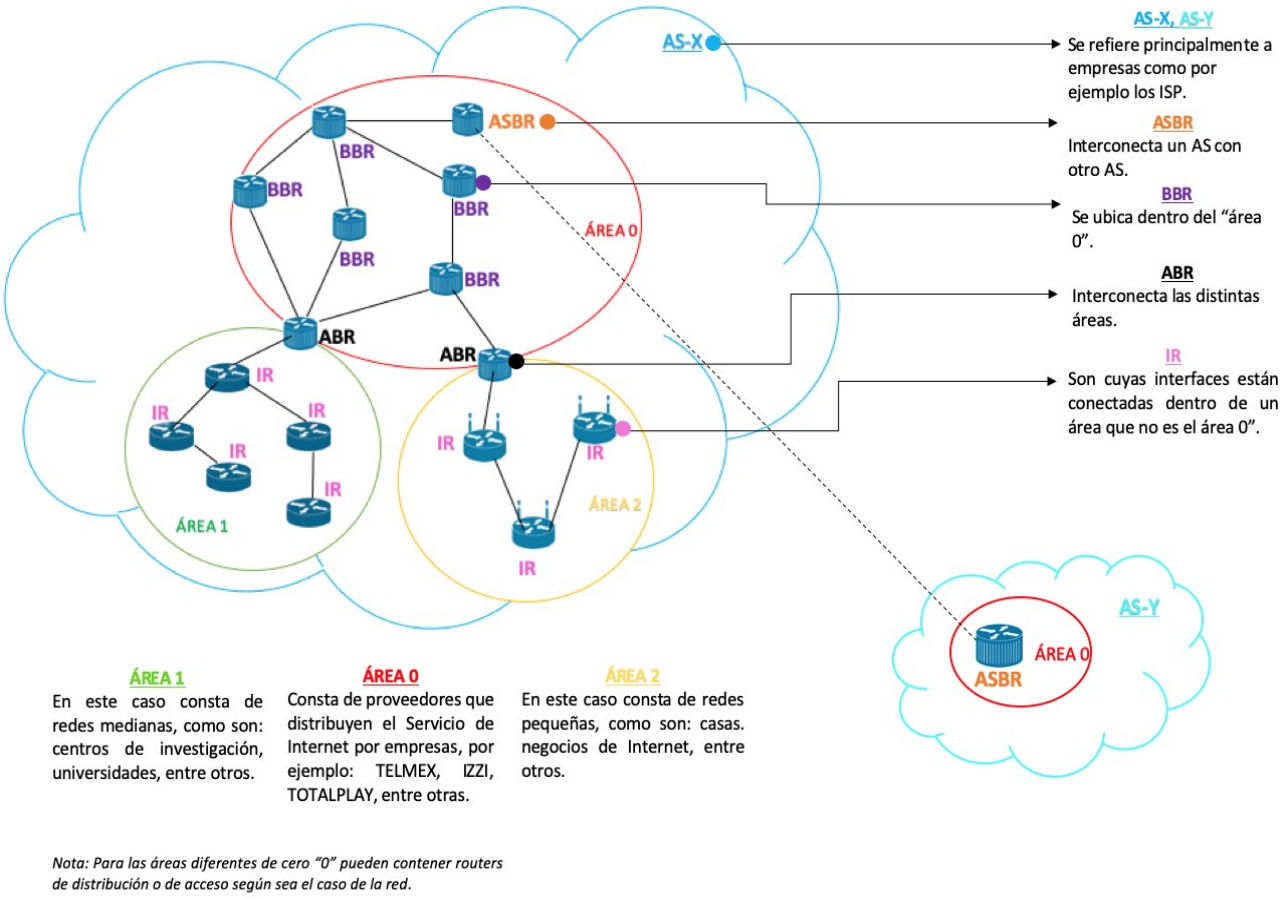


Figura 4.3. Representación de la segmentación por áreas en OSPF.

Una de las características de OSPF es que puede reducir el tráfico y la saturación en la red, para esto cada router tomará un rol, dependiendo del entorno si es una red Peer 2 Peer, es decir una comunicación directa o de acceso múltiple.

Una red de acceso múltiple es un segmento donde tenemos más de dos routers, dependiendo del entorno, el router actuará de una manera u otra en la topología, esto debido al protocolo, así que OSPF designa un router Designed Router (DR) cuya función consiste en llevar a cabo el intercambio de LSU entre todos los miembros que conforman una red para intercambiar datos, por lo que cada dispositivo envía su información de enrutamiento solo a este router DR, además se encargará de reenviar esta información a los vecinos restantes.

El protocol OSPF también designa un router Backup Designeted Router (BDR), el cual se conoce como router designado de respaldo. El BDR cumplirá los deberes del DR en caso de que el DR falle, este también realiza las retransmisiones que puedan ser necesarias en sustitución del DR.

Los routers que no se configuran como DR ni como BDR se designan como "Drother", los cuales se limitan al intercambio de paquetes LSU con el DR, esto significa que todos

los routers Drother en la red de accesos múltiples siguen recibiendo paquetes hello en todos los otros routers, de esta manera, éstos conocen a todos los routers de la red [34].

3.2.2 Costo OSPF

OSPF utiliza el costo como métrica, y no se encuentra descrito en los RFC que definen al protocolo OSPF, es por esto que está definido por el propio fabricante. Este protocolo utiliza una métrica para establecer una mejor ruta de un paquete por medio de una red. Una métrica indica la congestión de datos que implica enviar paquetes a través de una interfaz determinada.

El costo de una ruta es descrito por una única métrica adimensional, y es inversamente proporcional al ancho de banda de la interfaz, la fórmula utilizada para calcular el costo de OSPF es:

$$Costo = \frac{ancho\ de\ banda\ de\ referencia}{ancho\ de\ banda\ de\ la\ interfaz}$$

El ancho de banda de referencia predeterminado es 10^8 es lo mismo que (100 Mb/s - 100 000 000).

$$Costo = \frac{100\ 000\ 000\ bps}{ancho\ de\ banda\ de\ la\ interfaz\ en\ bps}$$

En la tabla 1.3 se indica el cálculo de costos para diferentes tipos de interfaces, dado que el ancho de banda de referencia predeterminado se establece en 100 Mb/s, las interfaces Fast Ethernet, Gigabit Ethernet comparten el mismo costo "1", es decir, el costo del enlace es mínimo. Por lo tanto, entre mayor sea la congestión y retraso en la ruta de los paquetes, mayor es el costo, así como las interfaces Serial e Ethernet. Por el contrario, cuanto mayor es el ancho de banda de la interfaz, menor es el costo y la ruta es mejor [35].

Tipo de interfaz y ancho de banda	Ancho de Banda de referencia en bps	Ancho de Banda de la interfaz en bps	Costo	
Gigabit Ethernet 1 Gbps	100 000 000	1 000 000 000	**1**	Estandarización de costo mínimo.
Fast Ethernet 100 Mbps	100 000 000	100 000 000	**1**	
Ethernet 10 Mbps	100 000 000	10 000 000	10	
Serial 64 Kbps	100 000 000	64 000	1562	

Tabla 1.3. Valores de costo en base al tipo de interfaz.

El costo de una ruta determinada se calcula sumando los costos de todas las interfaces encontradas a lo largo de esa ruta. Se mantiene un registro de los costos sumados hasta el destino conocido en el árbol de ruta más corta de OSPF.

3.3 PROTOCOLO DE ENRUTAMIENTO OSPFv3

Este protocolo se desarrolló como una nueva versión aplicable sobre entornos (IPv6). Su modo de operar coincide con la de su antecesor OSPFv2 en aspectos como son: estado de enlace, algoritmo de routing (SPF), métrica (costo), áreas, tipos de paquetes OSPF, mecanismos de descubrimiento de vecinos (message Hello), proceso de elección del DR/BDR y el router ID [32].
En la tabla 2.3 se mencionarán algunas diferencias entre estas versiones.

	OSPFv2	**OSPFv3**
Anuncio de rutas	Redes IPv4	Prefijos IPv6
Dirección de origen	Dirección IPv4 de origen	Dirección IPv6 link-local
Dirección de destino	Opción de: ✔ Dirección IPv4 de unidifusión de vecino. ✔ Dirección de multidifusión 224.0.0.5 de todos los routers OSPF. ✔ Dirección de multidifusión 224.0.0.6 del DR/BDR.	Opción de: ✔ Dirección IPv6 link-local de vecino. ✔ Dirección de multidifusión FF02::5 de todos los routers OSPFv3. ✔ Dirección de multidifusión FF02::6 de DR/BDR.
Anuncio de redes	Configurado con la instrucción ***network***	Configurado con la instrucción de configuración de interfaz **ipv6 ospf** id-proceso **área** id-area
Routing de unidifusión IP	El routing de unidifusión IPv4 está habilitado de manera predeterminada	El reenvió de unidifusión IPv6 no está habilitado de manera predeterminada. Se debe configurar la instrucción de configuración global **ipv6 unicast-routing**
Autentificación	Texto no cifrado y MD5	Autentificación IPv6

Tabla 2.3. Diferencias entre OSPFv2 y OSPFv3 [32, 34].

Nota: Las direcciones mencionadas en la tabla 2.3 son asignadas individualmente por IANA (Internet Assigned Numbers Authority) y designadas para multidifusión.

3.4 PROTOCOLO DE ENRUTAMIENTO BGP-4

Border Gateway Protocol (BGP) fue definido por primera vez en el año 1989, su actualización a BGP-2 se dio en 1990, para 1991 llegó BGP-3, y finalmente en 1995 se actualizó a BGP-4.

BGP-4 es un protocolo de puerta de enlace exterior estandarizado External Gateway Protocol (EGP), se considera un protocolo de enrutamiento de vector-ruta y no se creó para enrutar dentro de un Autonomous System (AS), sino para enrutar entre los AS, además, mantiene una tabla de enrutamiento separada basada en la ruta AS más corta y varios otros atributos, a diferencia de las métricas IGP como la distancia o el costo. La idea detrás de los Autonomous System es que las redes no se preocupen por los detalles internos de otras redes. Por su parte, este protocolo es aplicable sobre entorno IPv6, y es la implementación estándar actual de BGP. Un router puede aprender rutas IPv6 por medio de diferentes orígenes como son los IGP antes mencionados. Cada ruta que no es de origen OSPF, es considerada como una ruta externa OSPF. Para importar rutas externas dentro de OSPF, un router debe tener al menos una interfaz configurada con OSPF y conocer por lo menos una red que no sea OSPF. Este router es llamado router de frontera de sistema autónomo - Autonomous System Border Router (ASBR) y su modo de operación coincide con la de su antecesor BGP-3, en efecto es utilizado principalmente para conectar una red de área local a una red externa, para obtener acceso a Internet o para conectarse a otras organizaciones.

La función principal de un sistema de BGP es intercambiar información de las redes accesibles con otros sistemas BGP. Esta red proporciona la información de accesibilidad, incluye información sobre la ruta completa de sistemas autónomos (AS) que se debe transitar para llegar a estas redes, usando TCP como su protocolo de transporte confiable y el puerto TCP 179 para establecer sus conexiones [36, 37]. En a la figura 5.3 se muestra el uso de protocolos internos y externos, para el caso de estudio de esta tesis.

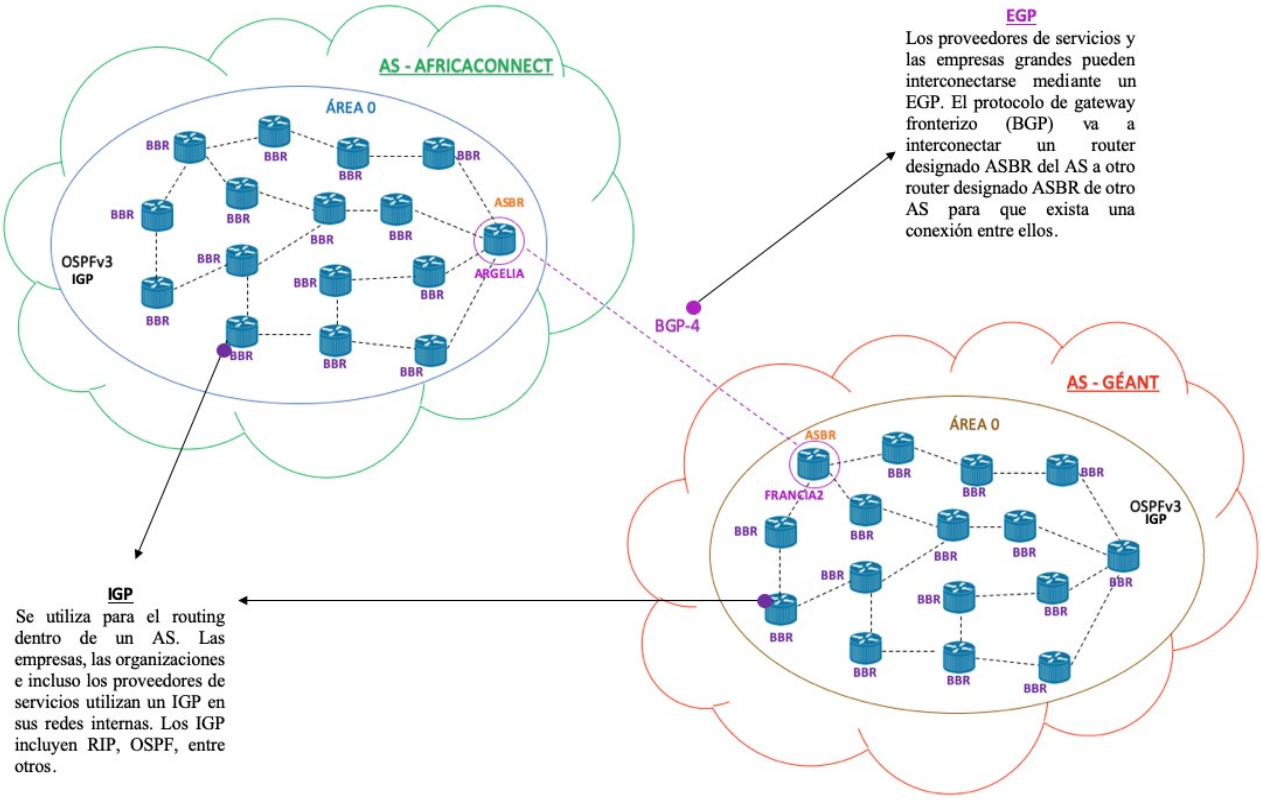


Figura 5.3. Representación del uso de BGP.

3.4.1 Formato del encabezado del mensaje BGP-4

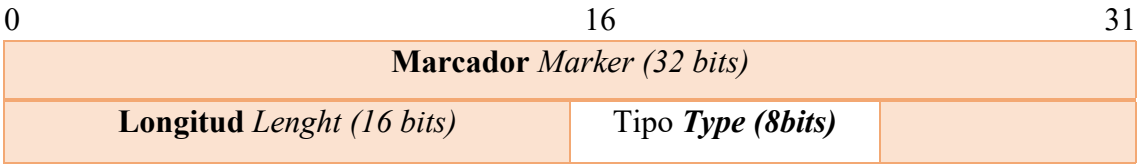


Figura 6.3. Formato del encabezado del mensaje BGP [37].

A continuación, se explica cada uno de los campos del formato que se muestran en la figura 6.3:

Marker: Contiene un valor que el receptor del mensaje puede utilizar para detectar la pérdida de sincronización entre un par de pares BGP y para autentificar los mensajes BGP entrantes.

Lenght: Indica la longitud total del mensaje, incluido el encabezado, en octetos. No se permite "relleno" de datos adicionales después del mensaje, por lo que el campo Longitud debe tener el valor más pequeño requerido dado el resto del mensaje.

Type: Indica alguno de los 4 tipos de mensaje BGP:

1. *Open (abrir sesión):* Se envía tras el establecimiento de la conexión TCP, su función es informar a los routers vecinos acerca de la versión BGP utilizada, el número de AS y el número de identificador de proceso BGP. Una vez enviado este mensaje, el proceso BGP se queda en espera de recibir mensajes de tipo Keepalive.
2. *Keepalive (mantener conexión):* Sirven para mantener viva la conexión, básicamente es la confirmación de un mensaje Open.
3. *Notification (notificación):* Sirven para notificar el cierre tanto de una sesión BGP como el cierre de la conexión TCP.
4. *Update (actualización):* Son aquellos que utilizan los routers para propagar la información de enrutamiento, este tipo de mensajes se envían solo cuando existe un cambio en la red y su recepción genera la activación de un proceso BGP en el que se actualizarán las tablas de enrutamiento y se actualizarán a los vecinos [37].

3.5 PROTOCOLO DE GESTIÓN DE RED SNMP

Simple Network Management Protocol (SNMP) es un protocolo de gestión utilizado para la supervisión, transferencia y recopilación de la información de los dispositivos conectados a la red, además, tiene una amplia variedad de tipos de software como programa de gestión SNMP por ejemplo, Power SNMP, iReasoning, entre otros. SNMP, se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP.

3.5.1 SNMPv2

A diferencia de SNMPv1, ésta permite una arquitectura de contadores de 64 bits, pero envía datos críticos mediante caracteres de texto sin cifrar, por lo que representa una desventaja en términos de seguridad. Cuando un usuario utiliza SNMPv2, suele tratarse de SNMPv2c, que representa la versión de la comunidad ("c" community) [38].

Actualmente existen tres versiones principales de SNMP: SNMPv1, SNMPv2 y SNMPv3. Las tres son muy parecidas, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión, En la figura 7.3 se muestran las características en común y generales de SNMP.

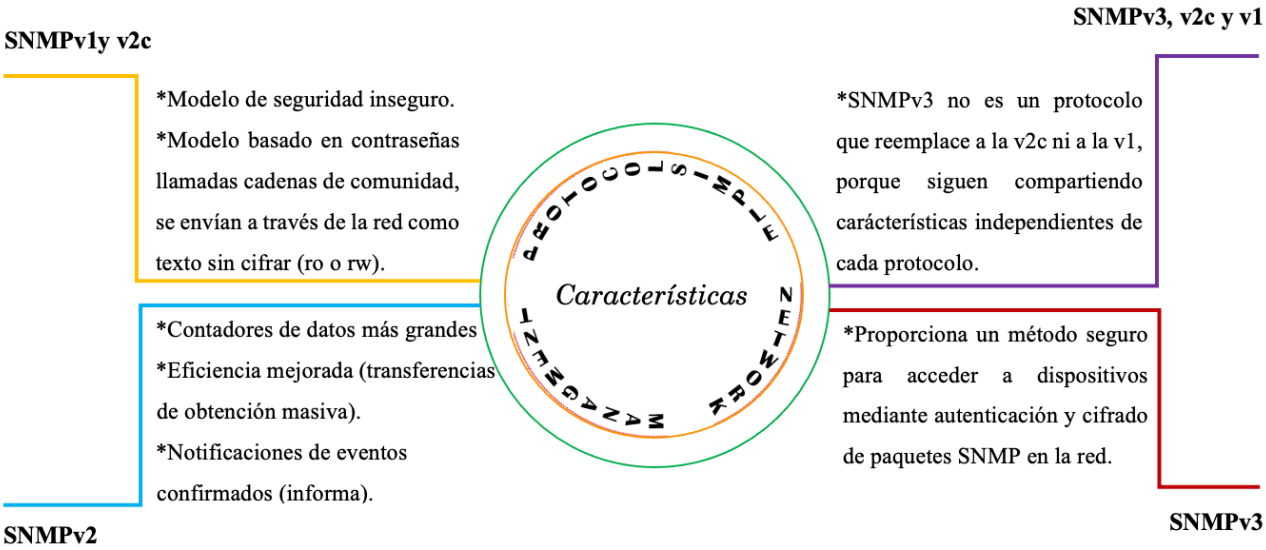


Figura 7.3. Características generales de SNMP [39, 38].

3.5.1.1 Funcionamiento de SNMP

La gestión de una red involucra regular y modificar la configuración de los dispositivos de red, es decir los **elementos a gestionar** y tendrán como huésped un **agente**. El protocolo de administración SNMP se utiliza para comunicar las **estaciones de gestión de la red** y los agentes en los elementos a gestionar de la red. Un sistema de gestión SNMP contiene:

1. **Administrador de SNMP:** Controla la administración y gestión de una red.
2. **Estación de gestión de la red:** Network Managment System (NMS), esta es una aplicación encargada de interrogar a un agente para pedir información del mismo, así como modificarlas según sean sus necesidades.
3. **Agente:** Es un módulo de software que habita dentro de un dispositivo y se ejecuta todo el tiempo. Este agente utiliza SNMP para transferir información al sistema de gestión.
4. **Elementos a gestionar:** switches, routers (dispositivos de enrutamiento).

El hecho de que los proveedores estén dispuestos a implementar agentes en muchos de sus productos hace que la gestión del sistema o el trabajo del administrador de red sea más sencillo.

El agente proporciona la información de gestión al NMS realizando un seguimiento de varios aspectos del dispositivo. Por ejemplo, el agente en un router es capaz de realizar un seguimiento del estado de cada una de sus interfaces para saber cuáles están activos y cuáles no, el tiempo de operación del router, la visualización del estado del enlace para saber si están activos o no, verificar el nombre del router e incluso modificarlo, entre otras acciones.

El NMS puede consultar el estado de cada una de las acciones mencionadas anteriormente que se realizan en un router: cuando el agente nota que algo está mal puede enviar un mensaje de “trap o trampa” al NMS, el mensaje trap es originado por el agente y se envía al NMS, donde se manejará apropiadamente. A modo de ejemplo en la figura 8.3 se muestra un diagrama UML de la relación de un agente-router y un NMS.

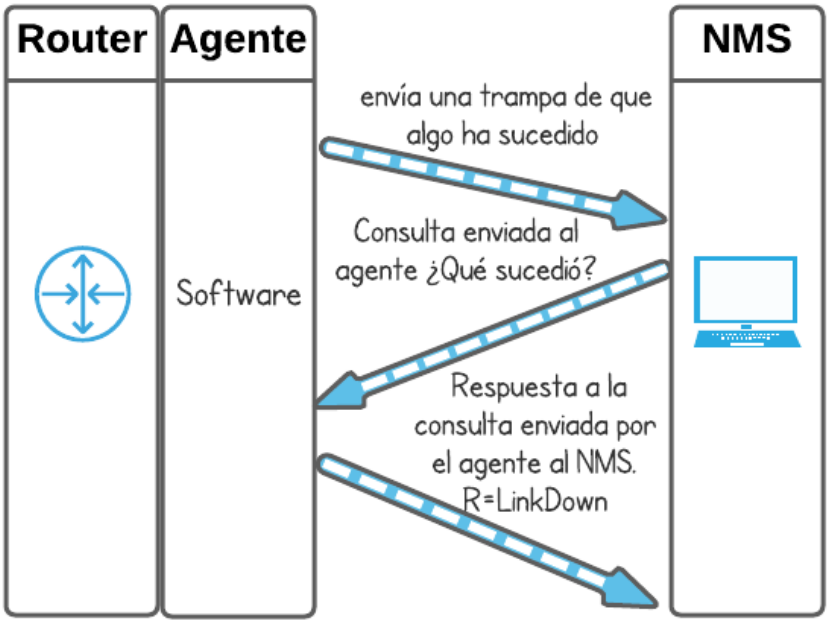


Figura 8.3. Diagrama de UML entre la relación de un agente-router y un NMS.

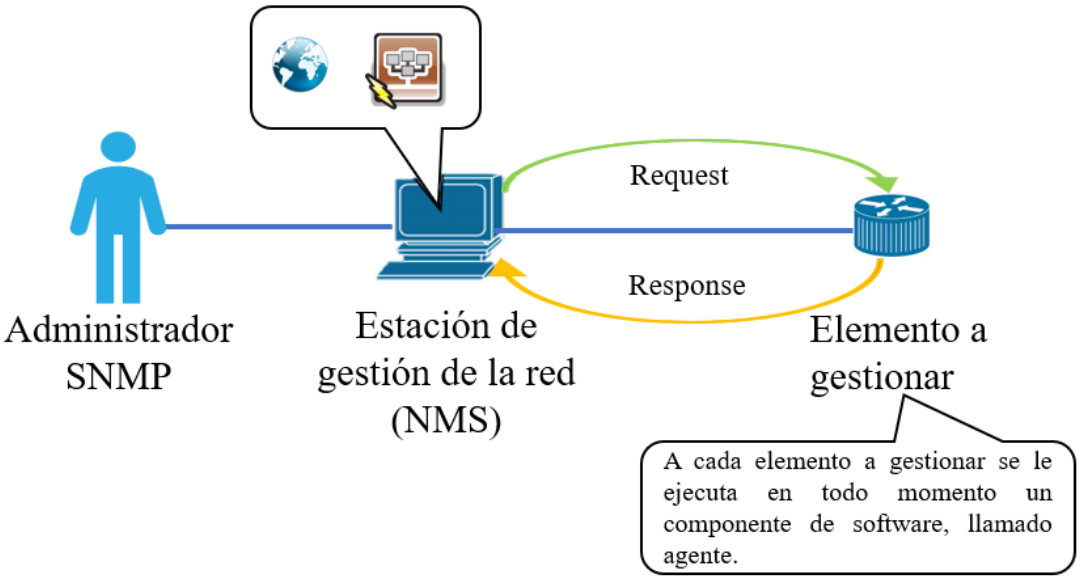


Figura 9.3. Elementos que conforman la gestión de una red.

Como se muestra en la figura 9.3, la comunicación entre la **estación de gestión de la red** y los **elementos a gestionar** se puede comparar con la típica comunicación cliente–servidor, es decir "petición- respuesta". Para ejemplificar, en la figura 10.3 se muestra el diagrama de casos de uso, donde se tiene un *programa de gestión SNMP* como sistema.

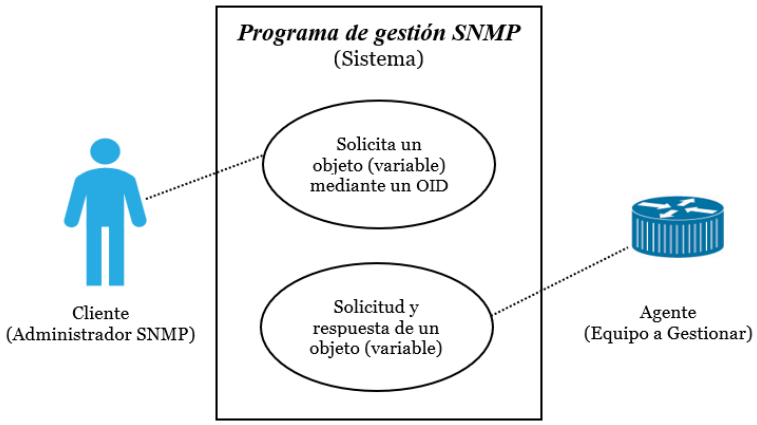


Figura 10.3. Diagrama de caso de uso para el sistema de programa de gestión SNMP.

Nota: Es importante mencionar que el Object IDentifier (OID) es el que identifica de forma única a un objeto administrado en la red vía SNMP.

3.5.1.2 Mensajes SNMP

SNMP permite el intercambio de información a través de la red entre la estación de gestión y el agente en forma de mensajes SNMP. Cada mensaje incluye un número de versión que indica la versión de SNMP, un nombre de comunidad utilizado en el intercambio, y uno de los cinco tipos de Protocol Data Units (PDU) definidos: GetRequest, GetNextRequest, SetRequest, GetResponse y Trap.

Las tramas tienen el siguiente formato:

Version	***Community***	***SNMP PDU***

Figura 11.3. Formato de la trama SNMP

A continuación, se explica cada uno de los campos del formato que se muestran en la figura 11.3:

Version: Número de versión de protocolo que se está utilizando ya sea SNMPv1, SNMPv2 o SNMPv3.
Community: Controla el acceso no autorizado a un dispositivo SNMP.
SNMP PDU: Contenido de la Unidad de Datos de Protocolo, depende de la operación que se ejecute.

A continuación, se describen los campos del tipo de dato PDU mostrado en la figura 12.3:

PDU Type	*Request ID*	*Error- status*	*Error- Index*	*Variable Blindings*

Figura 12.3. Formato PDU

A continuación, se explica cada uno de los campos del formato:

PDU Type: Indica el tipo de PDU.

Estos cinco mensajes proporcionan información necesaria para el monitoreo de la red, además realizan la comunicación entre un agente SNMP y un mensaje NMS (Network Managment System).

1. *Get-Request:* Este mensaje de petición la inicia el NMS, que envía la solicitud al agente, el agente solicita el valor especificó de un objeto en la MIB y lo procesa lo mejor que puede. En respuesta a un tipo GetRequest, el paquete contiene los datos o valores solicitados (ver figura 13.3).

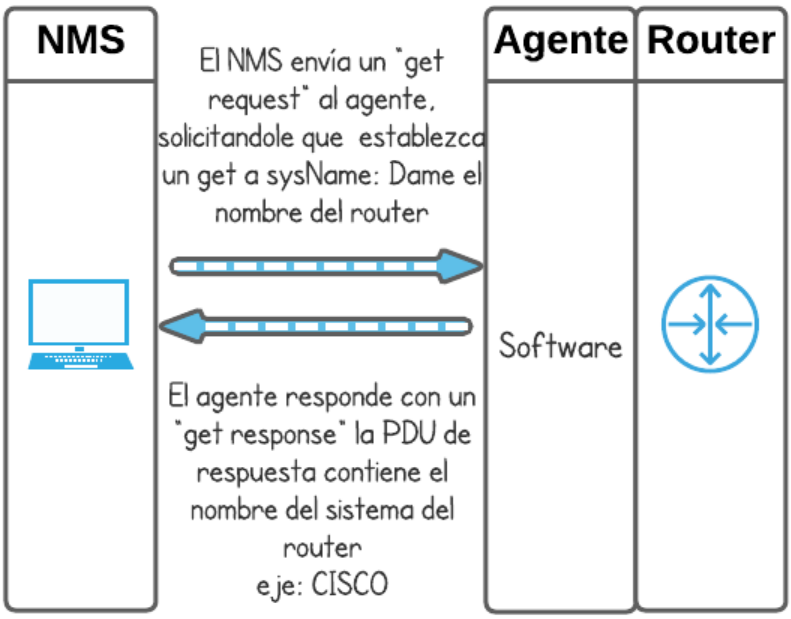


Figura 13.3. Diagrama UML de actividades Get-Request.

2. *Get-Next-Request:* Este tipo de mensaje lo envía el NMS para descubrir la información disponible desde el dispositivo, al iniciar el OID 0. El administrador, puede comenzar enviando una solicitud de los siguientes datos disponibles hasta que no haya más. De ahí que, los usuarios pueden descubrir todos los datos.

3. *Set-Request:* Este tipo de mensaje se utiliza para actualizar y administrar la configuración entre otros ajustes. El administrador inicia la instrucción para establecer o cambiar el valor de un objeto gestionado a modo de confirmación de que el Set-Request se ha completado exitosamente por medio del agente SNMP. Así también un Set-Request incorrecto podría afectar gravemente tanto a los sistemas como a las configuraciones de la red (ver figura 14.3).

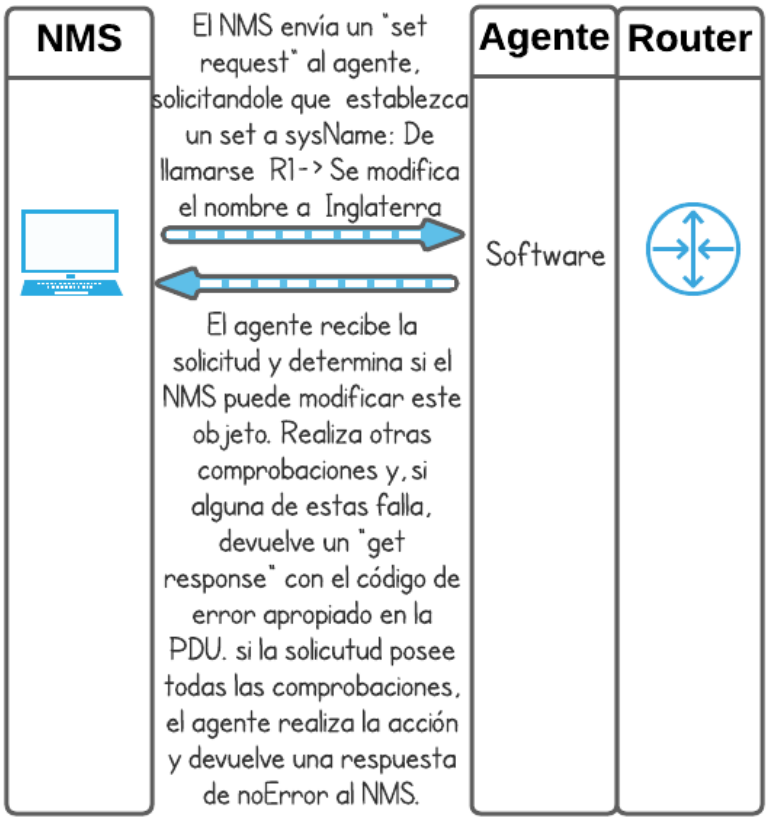


Figura 14.3. Diagrama UML de actividades Set-Request.

noError (0): No hubo problemas para realizar la solicitud.

4. *Get-Response:* La respuesta es el mensaje que un agente de dispositivo envía tras una solicitud del administrador.

5. *Trap*: Un mensaje de trap es la forma en que el agente le dice al NMS que algo a ocurrido, por lo que advierte al administrador sobre un ingreso incorrecto de la autentificación, que el estado del enlace este deshabilitado o exista un fallo repentino de una tarjeta del elemento a gestionar, entre otros (ver figura 15.3)[38].

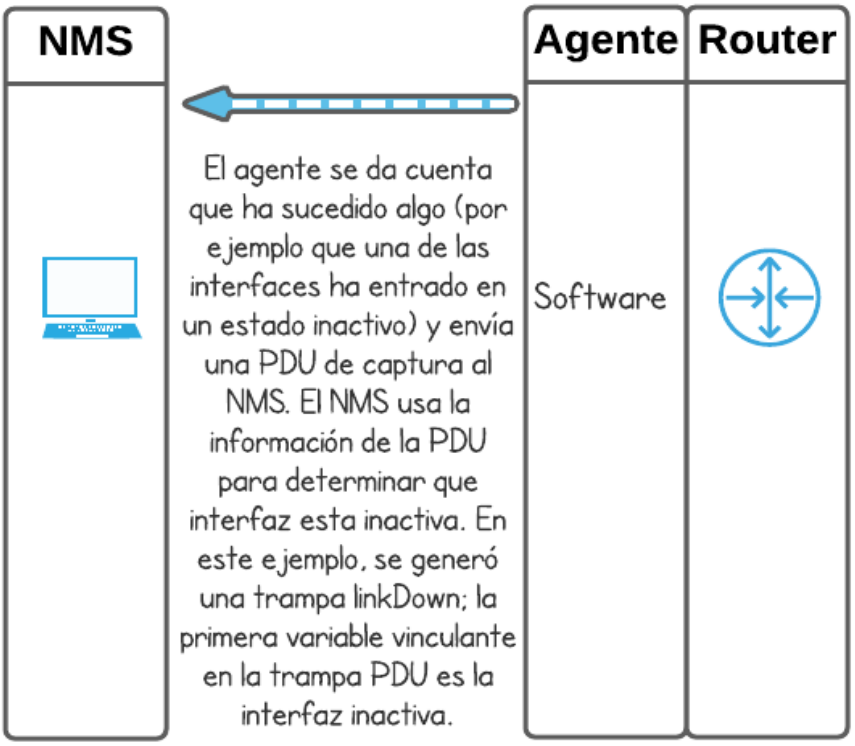


Figura 15.3. Diagrama UML de actividades traps.

Request ID: Utilizado para diferenciar las distintas peticiones, añadiendo a cada una de ellas un único identificador.

Error- status: Indica que ha ocurrido una excepción durante el procedimiento de una petición, sus valores posibles son: NoError(0), tooBig(1), noSuchName (2), badValue (3), readOnly (4), genErr (5).

A continuación se mostrarán los estados de error SNMP en la tabla 3.3.

Mensajes de Error SNMPv1	Descripción
NoError (0)	No existe problemas para realizar la solicitud
tooBig (1)	La respuesta a su solicitud fue demasiado grande para ajustar en una respuesta
noSuchName (2)	Petición a un agente que obtuviera o estableciera un OID que no pudo encontrar; es decir, el OID no existe
badValue (3)	Un objeto de read-write o de solo write se estableció en un valor inconsistente.

readOnly (4)	Este error generalmente no se usa, ya que es equivalente al error noSuchName.
genErr (5)	Error general, es decir, si ocurre un error, pero no coincide con los anteriores, se emite un genErr

Tabla 3.3. Estado de error SNMP.

Los mensajes de error SNMPv1 no son suficientes, una propuesta de solución a este problema fue SNMPv2 que define respuestas de error adicionales válidas para las operaciones get, set, get-next, get-bulk, siempre y cuando tanto el agente como el NMS admitan SNMPv2. Algunos mensajes de error de este son: noAccess(6), wrongType(7), wrongLength(8), wrongEncoding(9), wrongValue (10), entre otros.

Error-Index: Si no es cero indica que la variable de la petición es errónea.

Variable Blindings: Es una lista de nombres de variables y sus correspondientes valores [40].

Existen otros dos PDU de SNMP que solo son para la versión dos y tres:
GetBulkRequest - PDU: La respuesta solicitada contendrá tantos datos como permita la solicitud. Esencialmente es una forma de efectuar varias GetNextRequest a la vez, permitiendo a los usuarios generar una lista de todos los datos y parámetros disponibles.
InformRequest - PDU: Permiten que un administrador de SNMP determine qué tipo de problema detectó el agente SNMP remoto. Dependiendo del error detectado, el motor de SNMP puede intentar enviar un mensaje corregido. De no ser posible, puede enviar una indicación del error a la aplicación en cuyo nombre se emitió la solicitud SNMP fallida [41].

3.5.1.3 Transferencia de mensajes SNMP

El gestor de red SNMP trabaja en la capa de aplicación (capa 5) del modelo TCP/IP, utilizando el protocolo de datagramas de usuario (UDP) para transferir los mensajes. Para que la supervisión tenga éxito, es necesario que los paquetes UDP puedan trasladar del agente al administrador, por lo que hay que configurar específicamente el router para permitir que dichos paquetes atraviesen redes más amplias.

Los agentes SNMP reciben solicitudes UDP usualmente por el puerto 161 pero no implica que no puedan solicitarse desde cualquier otro puerto. Los agentes envían "mensajes de traps" a través del puerto 162, y el administrador de SNMP también las recibe por el mismo puerto [40].

3.5.1.4 MIB (Managment Information Base-Base de Información Gestionada)

El MIB es una estructura de datos que describe a los elementos de la red SNMP como una lista de objetos de datos. En una MIB cada objeto recibe una definición que describe sus propiedades dentro del dispositivo a gestionar. Se accede a los objetos utilizando el protocolo SNMP [42].

Para que se comuniquen con éxito la estación de gestión (NMS) y un elemento a gestionar en la red, es necesario conocer qué OID están disponibles. Esta es la razón por la cual existen las MIB, y por qué son tan útiles para los administradores del sistema. Todos los objetos que hay que supervisar en un dispositivo dado deben conocer las MIB de dicho dispositivo, por lo cual los administradores deben asegurarse de que todas las MIB necesarias estén almacenadas tanto en los dispositivos agentes SNMP, así como en la estación de gestión.

En la figura 16.3 se muestra el árbol de Internet de acuerdo a sus OID y el nombre del objeto correspondiente. Los siguientes ejemplos OID se propusieron con base en lo realizado en esta tesis.

3.5.1.5 OID (Object IDentifier-Identificador de Objetos)

Es un número que identifica de manera única a un objeto utilizado en la red SNMP. Cada parte de la información de administración que se puede obtener a través de SNMP se trata individualmente por su OID, éste a su vez ayuda a los administradores a identificar y supervisar los objetos que tienen en su red y, de ese modo, lograr que la supervisión sea significativa.

Un Object IDentifier (OID) se representa como una secuencia de enteros positivos en la que cada entero corresponde con un nodo en la estructura del árbol de la Managment Information Base (MIB). Este tipo de dato identifica 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** (iso (**1**), org (**3**), dod (**6**), Internet(**1**)), y el árbol MIB a su vez se compone de un **subárbol** de Internet, como se muestra en la tabla 4.3, compuesta de 6 subárboles que se describen brevemente:

Subárbol	Descripción
directorio (1)	Describe como se deben usar las direcciones OSI en Internet
mgmt (2)	Identifica objetos estándar registrados por la IANA (Internet Assigned Numbers Authority)
experimental (3)	Objetos de uso experimental empleados por el IETF, al convertirse en estándar se trasladan al mgmt (2)
private (4)	Objetos definidos por un único grupo (por lo general un proveedor o vendor. ejemplo Cisco). 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.

Tabla 4.3. Descripción del subárbol.

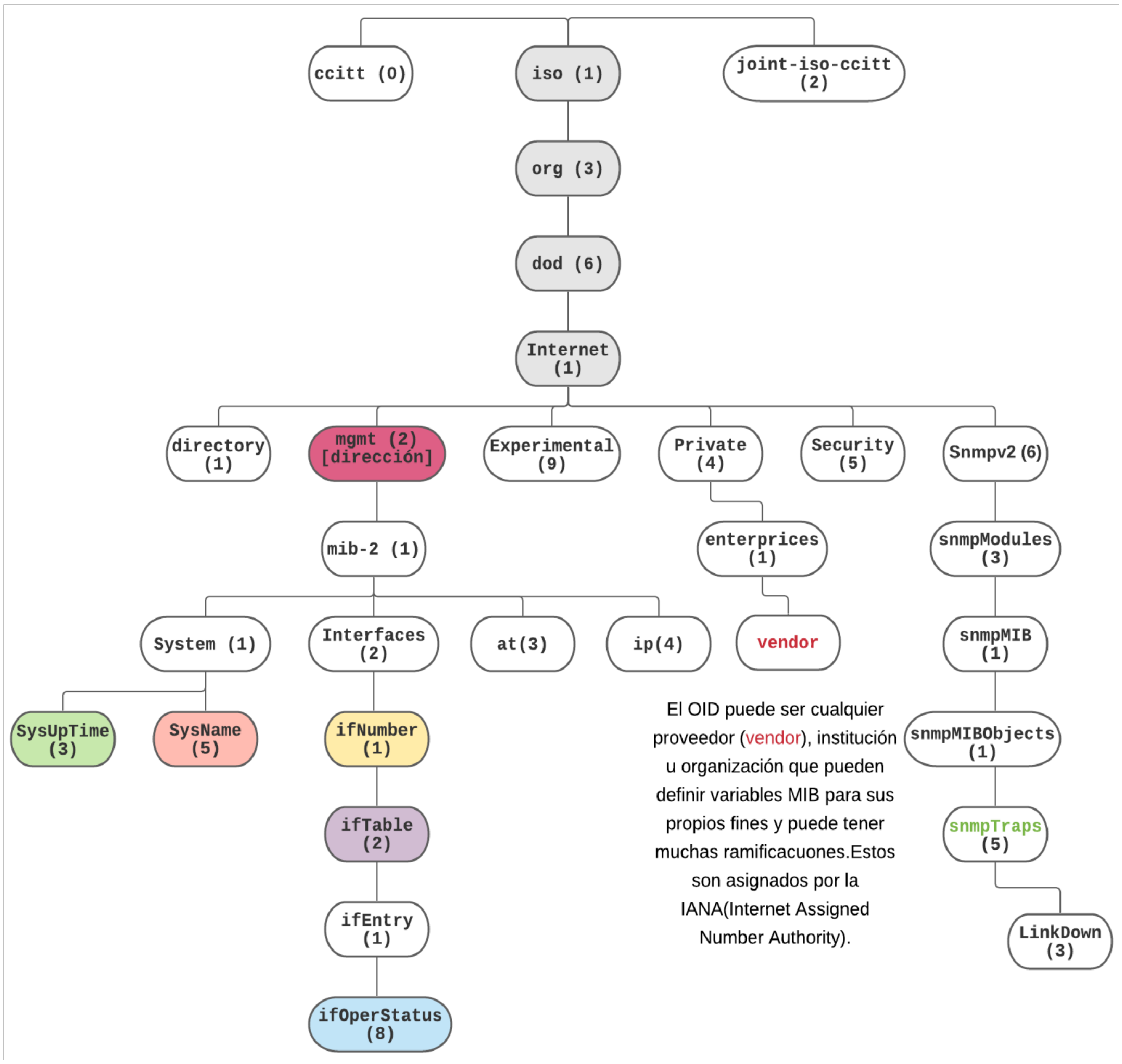


Figura 16.3. Árbol de Internet de acuerdo a su OID [42].

3.5.1.6 Tipos de MIBs: Públicas y Privadas

Públicas: Son aquellas que están definidas mediante estándares y se caracterizan por proporcionar información general de cualquier sistema de comunicaciones. Un ejemplo de MIB pública más conocida es la MIB-II, esta está soportada por los agentes SNMP y contiene información sobre el dispositivo a gestionar.
Privadas: Son aquellas definidas por los fabricantes para gestionar sus dispositivos, en este caso puede ser cualquier proveedor "Vendor".

Para un router, los típicos objetos OID de interés considerados en esta tesis se muestran en la tabla 5.3.

Variable OID	OID	Cadena de comunidad	Descripción	Operación
SysName	1.3.6.1.2.1.1.5	read and write	Nombre asignado administrativamente, esto es, el nombre de dominio completo del nodo, es decir el nombre del router.	GET/SET
ifNumber	1.3.6.1.2.1.2.1	read	El número de interfaces de red presentes en el sistema.	GET
SysUpTime	1.3.6.1.2.1.1.3	read	El tiempo desde que se reinicializó por última vez la parte de administración de red del sistema.	GET
ifOperStatus	1.3.6.1.2.1.2.2.1.8	read	El estado operativo actual de la interfaz.	GET
ifTable	1.3.6.1.2.1.2.2	read	El número de entradas viene dado por el valor de "ifNumber".	GET

Tabla 5.3. Variables OID de SNMP a gestionar.

Otras variables que se pueden consultar en el árbol de MIB-II se presentan en la tabla 6.3.

Nombre del subárbol	OID	Descripción
system (1)	1.3.6.1.2.1.1	Define una lista de objetos que pertenecen al funcionamiento del sistema, como el tiempo de actividad del sistema, el contacto del sistema, y nombre del sistema.
interfaces (2)	1.3.6.1.2.1.2	Realiza un seguimiento del estado de cada interfaz, en un elemento a gestionar. El grupo de interfaces monitorea qué interfaces están activadas o desactivadas, así como octetos enviados y recibidos, errores, etc.

at (3)	1.3.6.1.2.1.3	El grupo de traducción de direcciones (@) está obsoleto y se proporciona solo para compatibilidad con versiones anteriores, Probablemente se eliminará de MIB-III.
ip (4)	1.3.6.1.2.1.4	Realiza un seguimiento de muchos aspectos de IP, incluido el enrutamiento de IP.
icmp (5)	1.3.6.1.2.1.5	Realiza un seguimiento de errores ICMP.
tcp (6)	1.3.6.1.2.1.6	Rastrea, entre otras cosas, el estado de la conexión TCP (por ejemplo, cerrado, escucha, sysSent, etc.)
udp (7)	1.3.6.1.2.1.7	Rastrea estadísticas UDP, datagramas de entrada y salida, etc.
egp (8)	1.3.6.1.2.1.8	Realiza un seguimiento de varias estadísticas sobre EGP y mantiene una tabla de vecinos de EGP.
transmission (10)	1.3.6.1.2.1.10	Actualmente no hay objetos definidos para este grupo, pero otros MIB específicos de medios se definen utilizando este subárbol.
snmp (11)	1.3.6.1.2.1.11	Mide el rendimiento de la implementación SNMP subyacente en la entidad gestionada y rastrea información como el número de paquetes SNMP enviados y recibidos.

Tabla 6.3. Descripción del árbol MIB-II

3.5.1.7 SMI (Structure of Management Information)

Los socios de comunicación en una conversación SNMP son la entidad gestora y los dispositivos administrados. Ambos envían y reciben mensajes que contienen información de gestión a través de la red a través de SNMP, sin importar qué sistemas operativos, lenguajes de programación y compiladores estén involucrados.

Para lograr la independencia de los sistemas operativos, lenguajes de programación y otros tipos de componentes que generan incompatibilidad, se necesita liberar SNMP y por esto es importante una estructura estandarizada y ampliamente, conocida como SMI. [43,44].

3.5.2 SNMPv3

Esta versión incluye mejoras a SNMPv2c y aporta soluciones de seguridad como cuentas de usuarios, autentificación y cifrado de paquetes de datos opcional. Dadas estas mejoras, SNMPv3 se convierte en la versión de SNMP recomendada en términos de seguridad. No obstante, también se dificulta su configuración, sin dejar de lado que necesita mucha más potencia de procesamiento, concretamente cuando se supervisa en intervalos cortos en que se genera una gran cantidad de mensajes SNMP. Permite a los administradores un

alto mantenimiento de la red, así como resolver problemas que puedan surgir en la misma. En la figura 17.3 se muestran las características más relevantes de esta versión.

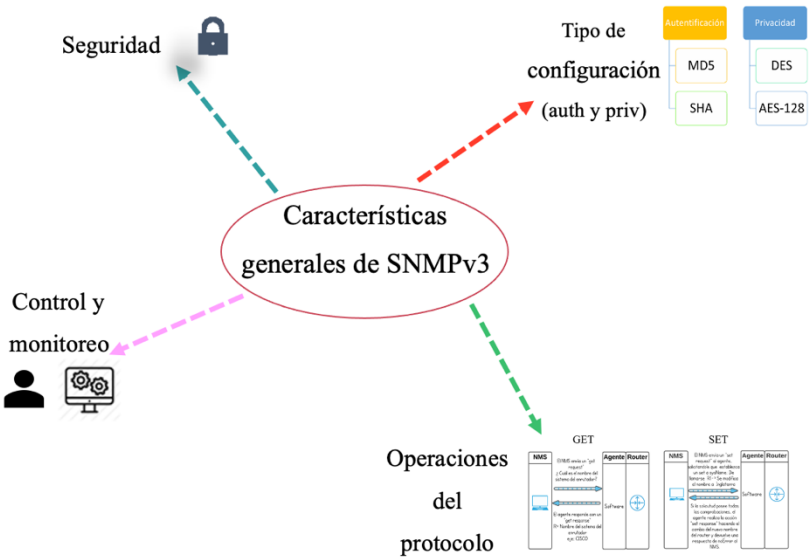


Figura 17.3. Características SNMPv3.

Como se ha mencionado, esta versión asegura la integridad del mensaje mediante el cifrado, y para conseguirlo SNMPv3 lo define en dos bloques [45]:

USM (User based Security Model): Define la estructura de usuarios e información necesaria para el cifrado y la autentificación. Esto se realiza entregando claves secretas, para la autentificación a través de los protocolos MD5 o SHA y para el cifrado a través de los algoritmos DES-CBC o AES-128.

VACM (View based Access Control Model): Se encarga de comprobar si el usuario tiene permitido el acceso a la lectura-escritura de determinados objetos, además describe los privilegios que tiene cada usuario USM.

SNMPv3 admite todas las operaciones definidas por las versiones 1 y 2. Con respecto a la seguridad está ha sido la mayor debilidad de SNMP desde el comienzo de la versión 1 y 2, ya que estas equivalen a nada más que a una contraseña entre una entidad gestora y un agente. Un administrador de red debe saber que las contraseñas de texto sin cifrar no proporcionan ninguna seguridad real, así que la versión 3 de SNMP resuelve los problemas de seguridad que tanto han afectado a las versiones anteriores. El cambio más importante para SNMPv3 es que abandona el concepto de entidad gestora y agente, por lo que ahora serán llamados entidades SNMP, cada entidad constará de un motor SNMP y de una o más aplicaciones SNMP.

3.5.2.1 Motor SNMPv3

El motor se compone de 4 piezas que proporcionan una mayor seguridad:

Dispatcher: el trabajo del despachador es enviar y recibir mensajes, intenta determinar la versión de cada mensaje recibido, que pueden ser v1, v2 o v3 y, si la versión es compatible, entrega el mensaje al procesador de mensajes del subsistema. Este también envía mensajes SNMP a otras entidades.

Message Processing Subsystem: el subsistema de procesamiento de mensajes. Su función es preparar los mensajes que se enviarán, y extrae datos de los mensajes recibidos. Un procesamiento de mensajes del sistema puede contener varios módulos de procesamiento de mensajes, por ejemplo, un subsistema puede tener módulos para procesar SNMP v1, solicitudes v2 y v3. Por otro lado, pueden contener un módulo para otros modelos de procesamiento, aunque aún no se han definido.

The Security Subsystem: El subsistema de seguridad proporciona servicios de autentificación y privacidad. La autentificación utiliza cadenas de comunidad, es decir son contraseñas de texto no cifrado, estas autentican el acceso a los objetos MIB. (SNMPv1 y v2), la autentificación basada en usuarios SNMPv3 está sustentada en los algoritmos Message Digest 5 (MD5) o Secure Hash Algorithm (SHA) para autentificar a los usuarios. El servicio de privacidad utiliza el algoritmo Data Encryption Standard (DES) para cifrar y descifrar mensajes SNMP, actualmente DES es el único algoritmo utilizado, aunque pude agregar otros en el futuro.

The Access Control Subsystem: El subsistema de control de acceso es el encargado de controlar el acceso a objetos MIB. Puede controlar a qué objetos un usuario puede acceder, así como a las operaciones que se le admite realizar en esos objetos [46].

CAPÍTULO 4. METODOLOGÍA

Dado que nuestro objetivo es el estudio de la conectividad y gestión de las redes avanzadas de Europa y África en la actualidad, en la figura 1.4 se muestra el diagrama que integra ambas redes. Las tres redes africanas UBUNTUNET Alliance, WACREN y ASREN conforman AfricaConnect2 en la actualidad y se asocian con Geant-4 en su segunda extensión actualmente. Los socios involucrados aprovecharán las sinergias para garantizar la cobertura [47].

Figura 1.4. Integración de AfricaConnect2 y Geant-4. [48]

4.1 EQUIPO NECESARIO PARA LA EMULACIÓN

En cuanto al sistema donde se realizó la emulación, cumple con los requerimientos para soportar la topología propuesta en esta tesis, ya que cuenta con las siguientes características: Procesador Intel Core i5 de 4 núcleos CPU 2.7 GHz, Memoria RAM de 16 GB, S.O. MacOS Catalina v 10.15.7. Cabe aclarar que teníamos 8 GB en RAM y tuvimos que actualizar a 16 GB en RAM.

4.2 TOPOLOGÍA PARA LA EMULACIÓN DE LAS REDES AVANZADAS DE ÁFRICA Y EUROPA.

Para lograr nuestro objetivo fue necesario integrar las redes AfricaConnect y Geant, se tomó la topología de backbone de cada red, para África desde 2015 a la fecha 2021 y para Europa desde 2018 a la fecha 2021. El número total de routers configurados en la topología AfricaConnect - Geant fue de 78 routers de backbone modelo c7200, además se utilizaron 3 routers de cada continente para la interconexión entre Autonomous Systems, la manera en que fueron distribuidos fue la siguiente:

África: Sudáfrica, Argelia y Kenia.
Europa: Inglaterra 2, Francia 2 y Alemania_DE3.

La interconexión entre Autonomous Systems de estos países es: Sudáfrica - Inglaterra 2, Argelia - Francia 2 y Kenia - Alemania_DE3.

La Internet Assigned Numbers Authority (IANA) asigna el Autonomous System Number (ASN) concreto de cada red, siendo estos: AfricaConnect dividido en 3 redes avanzadas y sus ASN correspondientes son: 36944 para UBUNTUNET, 37288 para WACREN y 199354 para ASREN, a su vez Geant tiene un ASN asignado de 20965, ver la figura 6.4. Los ASN se obtuvieron de la página ASRank [49].

Para esta topología se hizo la emulación en el programa GNS3 v 2.2.10, en el cual se agregaron routers Cisco c7200 y se utilizó la imagen (IOS): ***c7200-advipservicesk9-mz.150-1.M.image*** (ver la figura 2.4), para emular routers de backbone, ya que un emulador tiene el objetivo de comportarse exactamente igual que un router original, con

lo cual el emulador supera a los simuladores. En cuanto a los routers, se le agregaron 7 slots Gigabit Ethernet (GbE) como se indica en la figura 3.4. Para la interconexión con todos los routers, también se agregaron 2 computadoras virtuales, una conectada en África y otra en Europa, con un sistema operativo Windows 10 para la administración de la red, (ver figura 5.4). En el caso del enrutamiento dentro del AS de cada red avanzada (AfricaConnect - Geant) se configuró el protocolo OSPFv3 para IPv6, en cuanto al enrutamiento entre sistemas autónomos se configuró el protocolo BGPv4. Además, para la gestión de la red se configuró el protocolo SNMPv3, siendo que GNS3 no tiene integrado un MIB BROWSER, así que se instalaron dentro de la máquina virtual los programas PowerSNMP y iReasoning, como comparativas utilizadas para realizar pruebas de gestión en la red. Finalmente se instaló Wireshark en la máquina real, que se ejecuta en GNS3 como analizador de red.

GNS3 es un software gratuito que permite emular, configurar, probar y solucionar problemas de redes de cualquier tamaño.

Incorporación de routers y máquinas virtuales en GNS3.

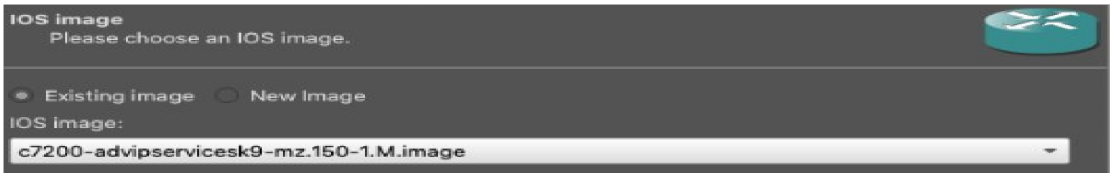


Figura 2.4. Imagen IOS para router de backbone c7200

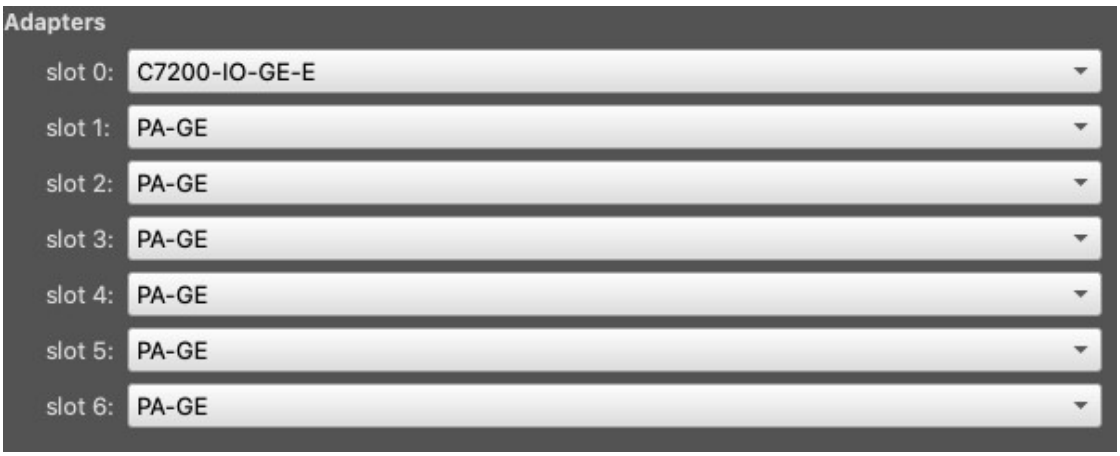


Figura 3.4. Slots disponibles en el router c7200.

Decidimos activar el idle, como se muestra en la figura 4.4, para evitar que GNS3 al ejecutar y virtualizar los equipos, se consuman tanto la memoria RAM como el procesador (número de núcleos que contenga), del equipo físico.

En esta topología, se utilizaron 2 máquinas virtuales en las que se les instalaron los programas de gestión PowerSNMP y iReasoning, las cuales tienen por nombre (VM_Marruecos y VM_Finlandia).

Figura 4.4. Activación Idle-PC.

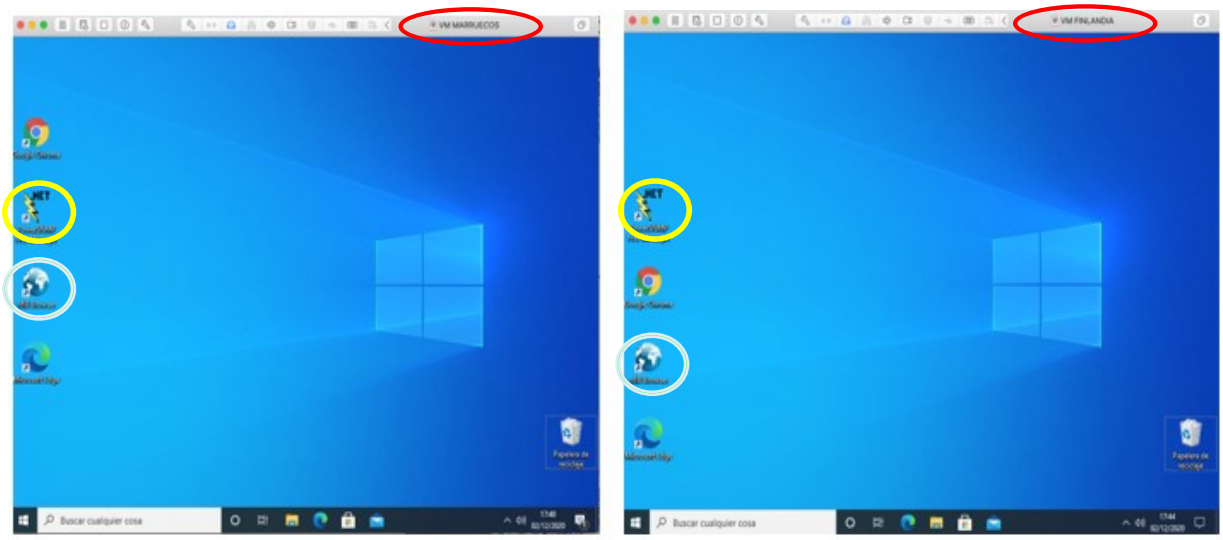


Figura 5.4. Máquinas Virtuales Windows 10 en Marruecos y Finlandia.

4.2.1 REDES AVANZADAS AfricaConnect- Geant

Una vez instalados los routers de backbone y las máquinas virtuales necesarias para la emulación, se implementarón en el emulador las redes Geant-4 y AfricaConnect2 interconectadas bajo la topología de backbone, como se muestra en la figura 6.4, en la cual se observa que estas se interconectan mediante 3 enlaces, en las que participan 6 routers de backbone a los cuales conocemos como Autonomous System Boundary Router (ASBR) circulados en color rosa.

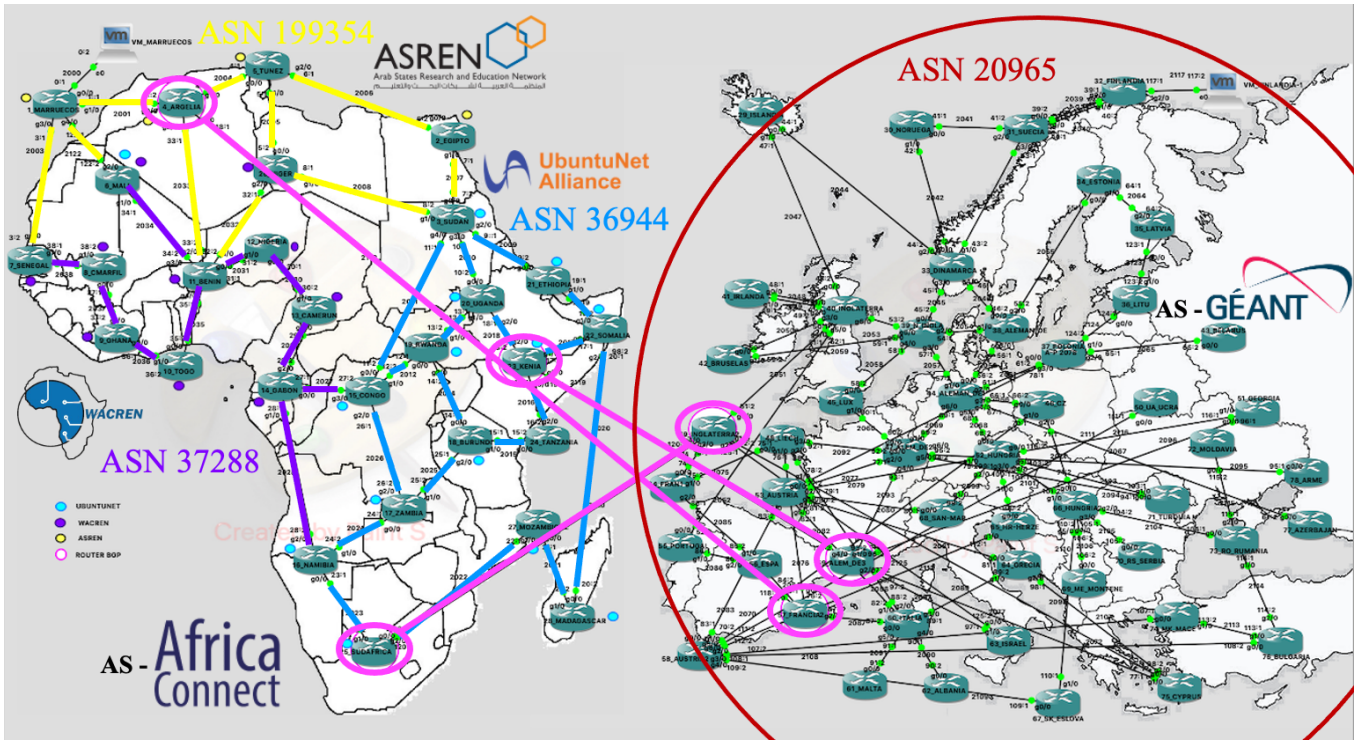


Figura 6.4. Integración de la Topología AfricaConnect – Geant.

Las direcciones que componen esta topología están divididas como se muestra en la tabla 1.4:

AfricaConnect2	Geant
2000: :/64 – 2038: :/64	2039: :/64 - 2125: :/64

Tabla 1.4. Intervalos de direcciones seccionadas respecto a cada AS.

Nota: Estos intervalos de direcciones no cuentan precisamente con la numeración continua de principio a fin.

4.2.2 Red avanzada AfricaConnect

La red avanzada de África es AfricaConnect, la cual conecta las redes nacionales en 29 países que está dividida en 3 grupos como se muestra en la figura 7.4:

- **Grupo 1:** África oriental y meridional:

  UBUNTUNET *(Red Regional de Investigación y Educación de África Oriental y Meridional):* cubre Burundi, República Democrática del Congo, Etiopía, Kenia, Madagascar, Mali, Maputo Mozambique, Ruanda, Somalia, Sudán, Sudáfrica, Tanzania, Uganda, Namibia y Zambia.

● **Grupo 2:** África occidental y central

WACREN *(Investigación de África Occidental y Central y Education Network):* cubre Benín, Camerún, Gabón, Ghana, Costa de Marfil, República de Malí, Níger, Nigeria, Senegal y Togo.

● **Grupo 3:** Norte de África

ASREN *(Investigación y Educación de los Estados Árabes Network):* cubre Argelia, Túnez, Egipto y Marruecos.

Dado que el router MALÍ se comparte con la red UBUNTUNET y la red WACREN existen un total de 28 routers de backbone c7200 en la red de AfricaConnect.

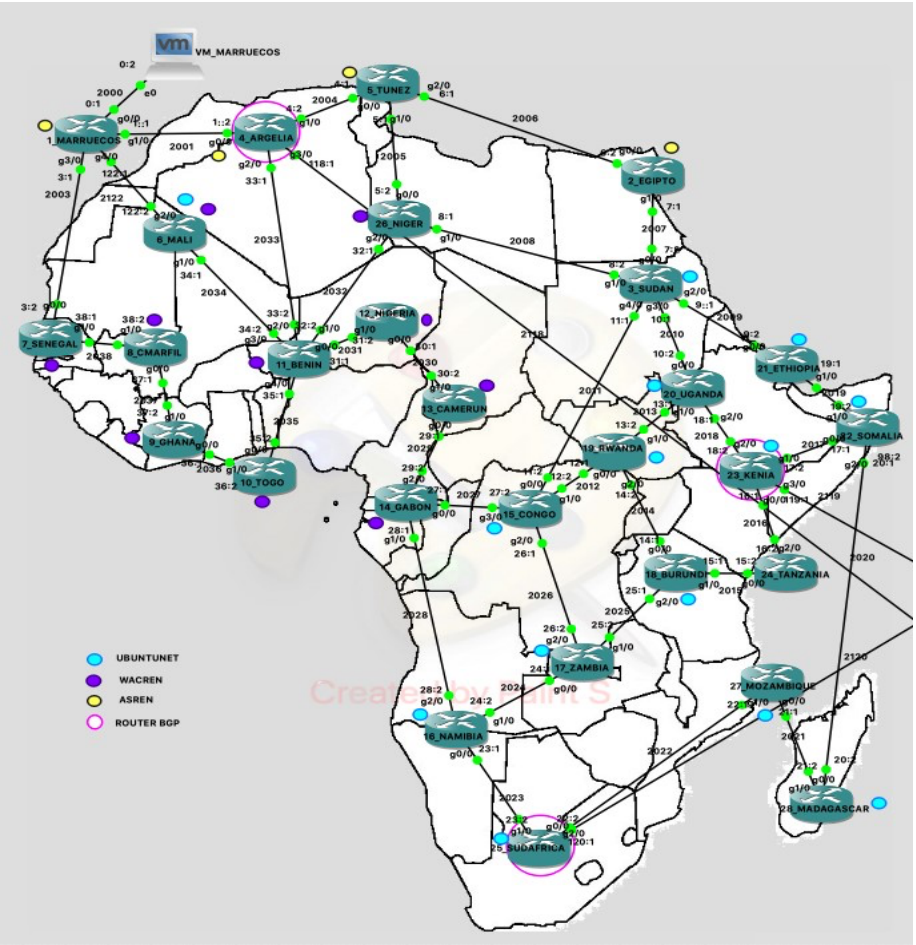


Figura 7.4. Topología de AfricaConnect2 en 2021.

4.2.3 Red avanzada GEANT

Es la red avanzada para Europa, que integra redes para 43 países. Se agregaron 7 routers más, debido al número limitado de interfaces que contiene el router C7200 los cuales fueron:

3 en ALEMANIA, 1 en INGLATERRA, 1 en AUSTRIA, 1 en HUNGRIA y 1 en FRANCIA.

Por lo tanto, la red Geant consta de 50 routers de backbone c7200 en su totalidad como se muestra en la figura 8.4.

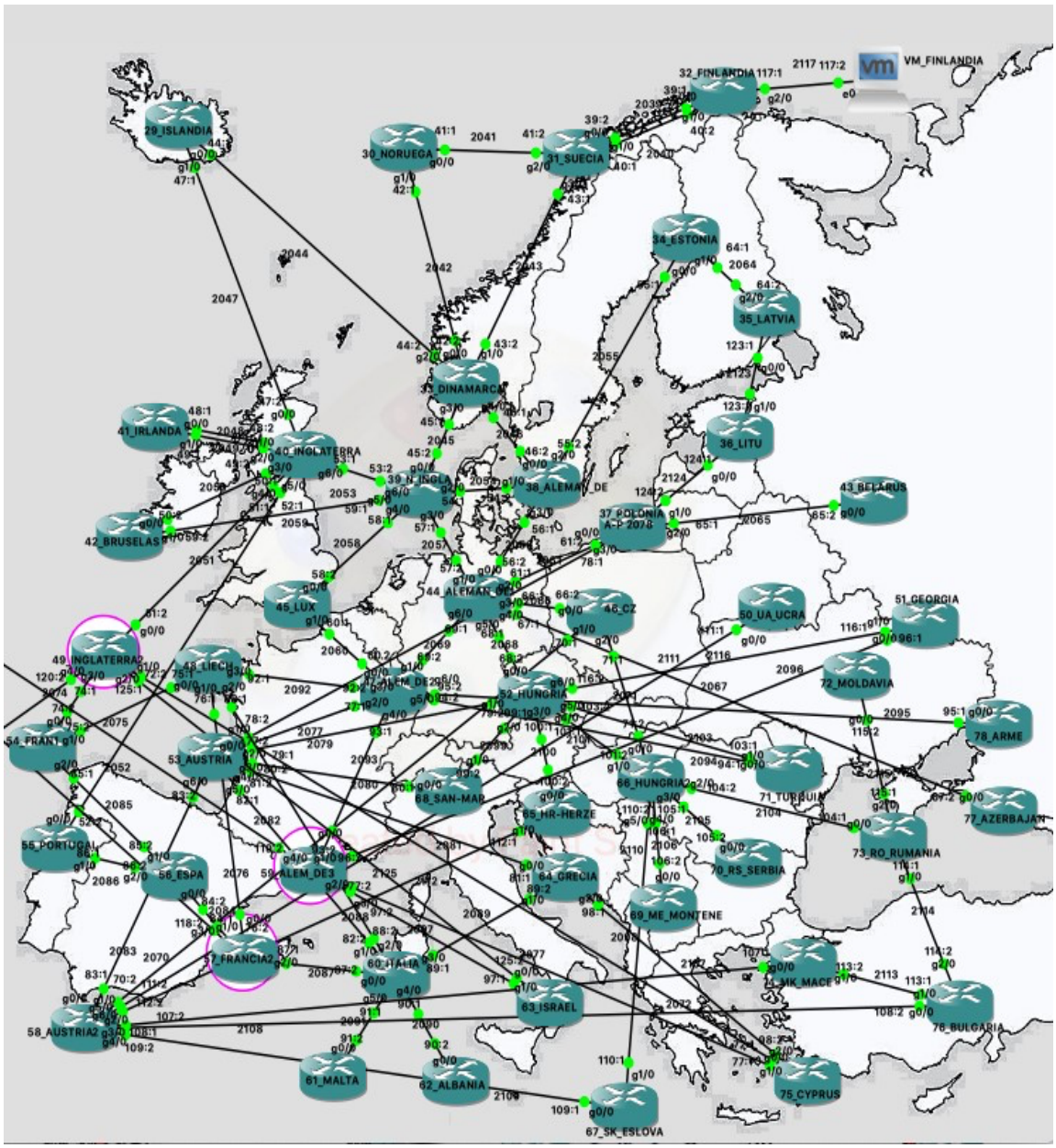


Figura 8.4. Topología Geant4-2 en 2021.

4.3 TABLA DE DIRECCIONES IP AfricaConnect – Geant

Ahora bien, como se muestra en la figura 7.4 se configuró cada uno de los routers con una dirección de red, mediante la cual se establece una comunicación entre ellos, además se configuró una Virtual Machine (VM) mediante el programa VMware Fusion, y se conectó al router Marruecos, para realizar la gestión de la red.

El router ID es un identificador de 32 bits definido por el formato IPv4, este se utilizará como identificador OSPF, es decir, solo se utilizará como etiqueta, no como dirección IPv4, es importante mencionar que, aunque el router ID se utilice para el formato de IPv4 también sirve para IPv6.

En la tabla 24, se muestran las direcciones de red IPv6 que se utilizaron en cada segmento que une a los routers, indicando a manera de resumen 28 enlaces, sin embargo, ésta realmente considera un total de 37 enlaces que conectan a los 28 routers que conforman a la topología AfricaConnect2; la tabla completa se puede consultar en el Apéndice C.

Red	**Dirección de red IPv6**	**Routers asociados AfricaConnect**	**Dirección IPv6 de** Routers **asociados**	**Router ID**
1	2001::/64	MARRUECOS	2001::1/64	1.1.1.1
		ARGELIA	2001::2/64	4.4.4.4
2	2122::/64	MARRUECOS	2122::1/64	1.1.1.1
		MALI	2122::2/64	6.6.6.6
3	2033::/64	ARGELIA	2033::1/64	4.4.4.4
		BENIN	2033::2/64	11.11.11.11
4	2005::/64	TUNEZ	2005::1/64	5.5.5.5
		NIGER	2005::2/64	26.26.26.26
5	2006::/64	NIGER	2006::1/64	26.26.26.26
		SUDAN	2006::2/64	3.3.3.3
6	2035::/64	BENIN	2035::1/64	11.11.11.11
		TOGO	2035::2/64	10.10.10.10
7	2036::/64	TOGO	2036::2/64	10.10.10.10
		GHANA	2036::1/64	9.9.9.9
8	2038::/64	CMARFIL	2038::2/64	8.8.8.8
		SENEGAL	2038::1/64	7.7.7.7
9	2003::/64	SENEGAL	2003::2/64	7.7.7.7

		MARRUECOS	2003::1/64	1.1.1.1
10	2035::/64	TOGO	2035::1/64	10.10.10.10
		BENIN	2035::2/64	11.11.11.11

Tabla 2.4. Direcciones para los routers asociados a la red AFRICACONECT, parte 1-3.

Por lo que respecta a, la red Geant de la figura 7.4 se configuró cada uno de los routers con una dirección de red, mediante la cual se establece una comunicación entre ellos, además se configuró una Virtual Machine mediante el programa VMware Fusion, y se conectó al router Finlandia, para realizar la gestión de la red.

En la tabla 3.4, se muestran las direcciones de red IPv6 que se utilizaron en cada segmento que une a los routers, indicando a manera de resumen 50 enlaces, sin embargo, esta realmente considera un total de 77 enlaces que conectan a los 50 routers que conforman a la topología Geant; la tabla completa se puede consultar en el Apéndice D.

Red	Dirección de red IPv6	Routers asociados Geant	Dirección IPv6 de routers asociados	router ID
1	2047::/64	ISLANDIA	2047::1/64	29.29.29.29
		INGLATERRA	2047::2/64	40.40.40.40
2	2048::/64	INGLATERRA	2048::2/64	40.40.40.40
		IRLANDA	2048::1/64	41.41.41.41
3	2043::/64	IRLANDA	2043::1/64	41.41.41.41
		INGLATERRA	2043::2/64	40.40.40.40
4	2059::/64	BRUSELAS	2059::2/64	42.42.42.42
		N. INGLATERRA	2059::1/64	39.39.39.39
5	2054::/64	N. INGLATERRA	2054::1/64	39.39.39.39
		ALEMANIA_DE	2054::2/64	38.38.38.38
6	2046::/64	ALEMANIA_DE	2046::2/64	38.38.38.38
		DINAMARCA	2046::1/64	33.33.33.33
7	2042::/64	DINAMARCA	2042::2/64	33.33.33.33
		NORUEGA	2042::1/64	30.30.30.30
8	2041::/64	NORUEGA	2041::1/64	30.30.30.30
		SUECIA	2041::2/64	31.31.31.31
9	2039::/64	SUECIA	2039::2/64	31.31.31.31

		FINLANDIA	2039::1/64	32.32.32.32
10	2040::/64	FINLANDIA	2040::2/64	32.32.32.32
		SUECIA	2040::1/64	31.31.31.31

Tabla 3.4. Direcciones asociadas a la red Geant, parte 1-5

En cuanto a la comunicación entre Autonomous Systems fue necesario configurar los routers con una dirección de red IPv6 y un tipo de enrutamiento BGP-4 como se muestra en la tabla 4.4.

Routers AfricaConnect2	**Routers de GÈANT**	**Dirección IPv6 de los routers asociados**		**Direccionamiento BGP-4**
Sudáfrica - Inglaterra 2		2120::1/64	2120::2/64	✓
Argelia - Francia 2		2118::1/64	2118::2/64	✓
Kenia - Alemania_DE3		2119::1/64	2119::2/64	✓

Tabla 4.4. Direcciones IPv6 asociadas para la interconexión entre Autonomous Systems.

4.4 CONFIGURACIÓN DE INTERFACES, PROTOCOLOS DE ENRUTAMIENTO Y DE GESTIÓN

1. **Configuración de interfaz y asignación de IP**

Para la configuración de una interfaz en GNS3 se debe tener claro qué tipo de interfaz se va a configurar, en este caso se configuró un interfaz de tipo Giga Ethernet, para los 78 routers de backbone. A manera de ejemplo se tomó el router de Argelia (ver figura 9.4) para la habilitación de sus 4 interfaces, como se muestra en la figura 10.4.

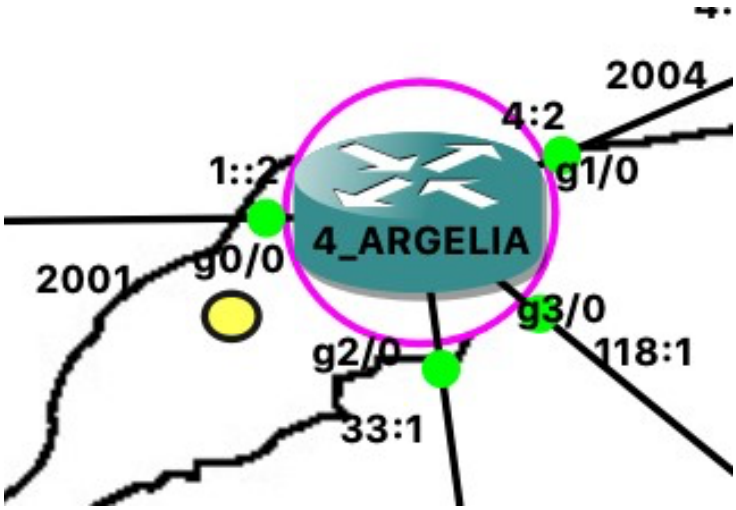


Figura 9.4. Router Argelia.

```
4_ARGELIA#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4_ARGELIA(config)#ipv6 unicast-routing
4_ARGELIA(config)#int g0/0
4_ARGELIA(config-if)#no shutdown
4_ARGELIA(config-if)#ipv6 address 2001::2/64
4_ARGELIA(config-if)#exit
4_ARGELIA(config)#int g2/0
4_ARGELIA(config-if)#no shutdown
4_ARGELIA(config-if)#ipv6 address 2033::1/64
4_ARGELIA(config-if)#exit
4_ARGELIA(config)#int g3/0
4_ARGELIA(config-if)#no shutdown
4_ARGELIA(config-if)#ipv6 address 2118::1/64
4_ARGELIA(config-if)#exit
4_ARGELIA(config)#int g1/0
4_ARGELIA(config-if)#no shutdown
4_ARGELIA(config-if)#ipv6 address 2004::2/64
4_ARGELIA(config-if)#
```

Figura 10.4. Habilitación de interfaces y configuración de ip del router Argelia.

2. **Configuración de OSPF:**

Tomando como ejemplo los routers Argelia y Francia2 de la figura 11.4, se muestra la configuración para el enrutamiento dinámico OSPFv3 para IPv6. Para esto se debe tener en cuenta el número de Sistema Autónomo (ASN) que va a anunciar la ruta. En el capítulo 4 mencionamos los ASN reales, pero para efectos prácticos en este caso asignamos el 1 para el AS AfricaConnect y el 2 para el AS Geant, así respectivamente el resto de los router se configurarán según corresponda a la topología.

Por otra parte, se configuró la redistribución BGP en OSPF debido a que se quiere lograr que las tablas de enrutamiento puedan compartir las rutas internas y externas en todos los routers.

Es importarte mencionar que la interfaz g3/0 del router Argelia no contará con la configuración de OSPF, mientras la que interconecta a la interfaz g3/0 del router de frontera Francia2 sí, esto es debido a que si ambas contaran con la configuración de OSPF existiría un traslape de información de rutas, debido a su conexión directa. Los 4 routers restantes identificados como routers de frontera BGP fueron configurados de igual forma.

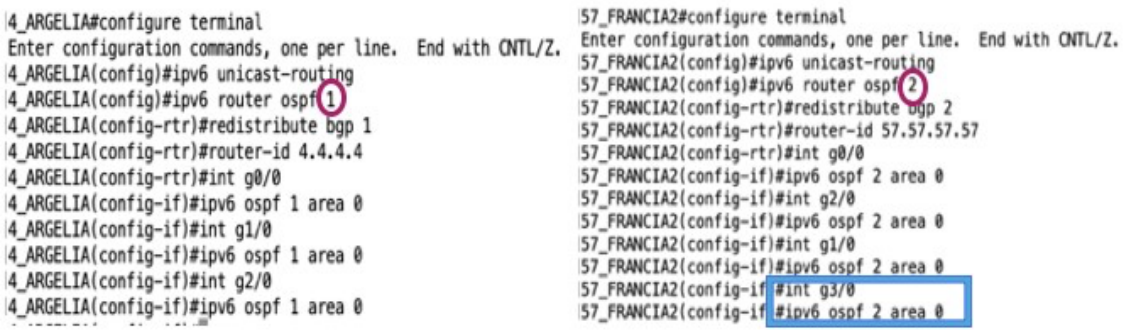


Figura 11.4. Configuración OSPFv3.

3. Configuración BGP y Redistribución de Rutas

En la figura 12.4 se muestra la interconexión del router Argelia ubicado en el AS-AfricaConnect, contiguo al router Francia2 del AS-Geant. Posteriormente en la figura 13.4 se representa la configuración de enrutamiento BGP-4 para IPv6, en donde habilitamos la familia de direcciones IPv6. Así también dentro de esta sub-configuración habilitamos la interfaz vecina con la instrucción **neighbor** y la configuración de la instrucción **network** que son las redes propias del router origen y la redistribución de rutas OSPF en BGP debido a que se quiere lograr que las tablas de enrutamiento puedan compartir las rutas internas y externas en todos los routers.

La redistribución de rutas sirve para que el protocolo BGP anuncie a OSPFv3 las rutas externas que tiene para ciertas redes y a su vez OSPF va anunciar a BGP las rutas internas que se puedan alcanzar dentro del Sistema Autónomo. Con esto, BGP podrá anunciar todas las rutas a otro AS asociado dentro de todas las rutas que hay en los Sistemas Autónomos, gracias al intercambio de información que hay entre las tablas BGP y OSPF es como un Sistema Autónomo puede saber lo que tiene otro Sistema Autónomo y las rutas que queremos utilizar con el fin de generar la conectividad entre estos.

Por su parte, los 4 routers restantes marcados con un círculo rosa e identificados como routers de frontera BGP fueron configurados de igual forma, según corresponde con la topología.

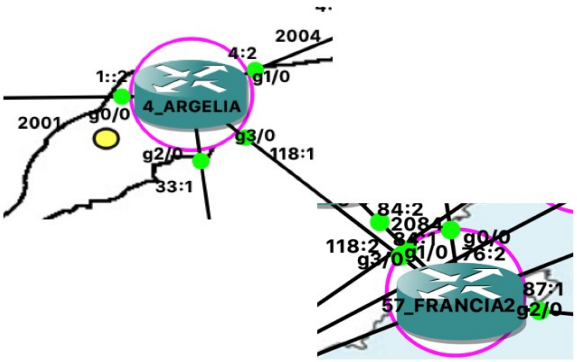


Figura 12.4. Configuración BGP router Argelia, contiguo al router Francia2.

```
4_ARGELIA(config)#router bgp 1
4_ARGELIA(config-router)#bgp router-id 4.4.4.4
4_ARGELIA(config-router)#no bgp default ipv4-unicast
4_ARGELIA(config-router)#neighbor 2118::2 remote-as 2
4_ARGELIA(config-router)#address-family ipv6
4_ARGELIA(config-router-af)#neighbor 2118::2 activate
4_ARGELIA(config-router-af)#redistribute ospf 1
4_ARGELIA(config-router-af)#network 2001::/64
4_ARGELIA(config-router-af)#network 2004::/64
4_ARGELIA(config-router-af)#network 2033::/64
```

```
57_FRANCIA2(config)#router bgp 2
57_FRANCIA2(config-router)#bgp router-id 57.57.57.57
57_FRANCIA2(config-router)#no bgp default ipv4-unicast
57_FRANCIA2(config-router)#neighbor 2118::1 remote-as 1
57_FRANCIA2(config-router)#address-family ipv6
57_FRANCIA2(config-router-af)#neighbor 2118::1 activate
57_FRANCIA2(config-router-af)#redistribute ospf 2
57_FRANCIA2(config-router-af)#network 2076::/64
57_FRANCIA2(config-router-af)#network 2084::/64
57_FRANCIA2(config-router-af)#network 2087::/64
```

Figura 13.4. Configuración BGP-4 en Argelia - Francia2

Nota: El número de procesos mencionados en la sección "*Configuración de OSPF*" también son utilizados para el protocolo BGP

4. Creación de una máquina virtual en VMware Fusion importada a GNS3

Se utilizaron 2 máquinas virtuales para prueba de conectividad y gestión por lo que se configuraron como Network Management Systems, utilizando aplicaciones como PowerSNMP y iReasonig MIB Browser

Procedimiento:

a) Iniciar el programa VMware Fusion (para ver instalación de este programa ir al Apéndice B).

b) Ubicarse en la ventana emergente y colocarse en la pestaña + y seleccione **Nuevo**.

c) Aparece un cuadro con la leyenda **Seleccione el método de instalación**.

d) Encuentre el archivo de imagen de disco de instalación de sistema operativo y arrástrelo y suéltelo en **Instalar desde disco o imagen**.

e) Se iniciará el asistente **Crear una máquina virtual nueva**.

f) Haga clic en **Continuar**.

- Si va a instalar el sistema operativo desde un archivo de imagen, compruebe que el archivo de imagen está en un directorio al que puede acceder el sistema host.
- Si va a instalar el sistema operativo desde un disco físico, inserte el disco de instalación del sistema operativo en su Mac.

g) Finalizar

El proceso de instalación se realizó tal cual se describe en la sección *procedimiento.* En la figura 14.4, se muestra la creación de las dos máquinas virtuales.

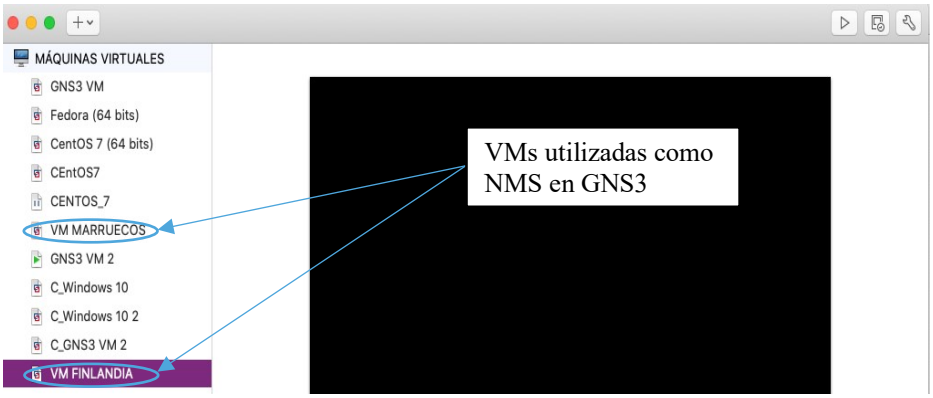


Figura 14.4. Creación de las máquinas virtuales VM_Marruecos y VM_Finlandia.

Una vez creadas las máquinas virtuales se configura la memoria RAM y el procesador. Hay que mencionar que la máquina real les asigna recursos a las máquinas virtuales, estos recursos se dividen de la siguiente manera: de los 4 núcleos de procesador, se le asignaron dos núcleos a la VM _Finlandia y uno a la VM_Marruecos. En cuanto a memoria RAM, de los 16 GB se les asignan 1024MB a cada máquina virtual, lo que es el mínimo recomendado para que estas puedan ser ejecutadas. En la figura 15.4 se muestran las asignaciones mencionadas de la máquina virtual Finlandia.

Figura 15.4. Asignación de recursos de una VM.

Por otra parte, se configuró la Network Interface Card (NIC) de la máquina virtual con S.O Windows 10 (ver figura 16.4), de la siguiente manera:

1. Encender máquina virtual desde GNS3
2. Inicio → panel de control → Conexiones de red
3. Propiedades de Ethernet o Seleccionar Protocolo de Internet versión 6 (IPv6) ○ Propiedades: Protocolo de internet versión 6 (TCP/IPv6) ○ Agregar la dirección IPv6, mascara de subred y el Gateway. Finalmente, se tiene que desactivar el firewall para evitar problemas de conectividad como se muestra en la figura 17.4.

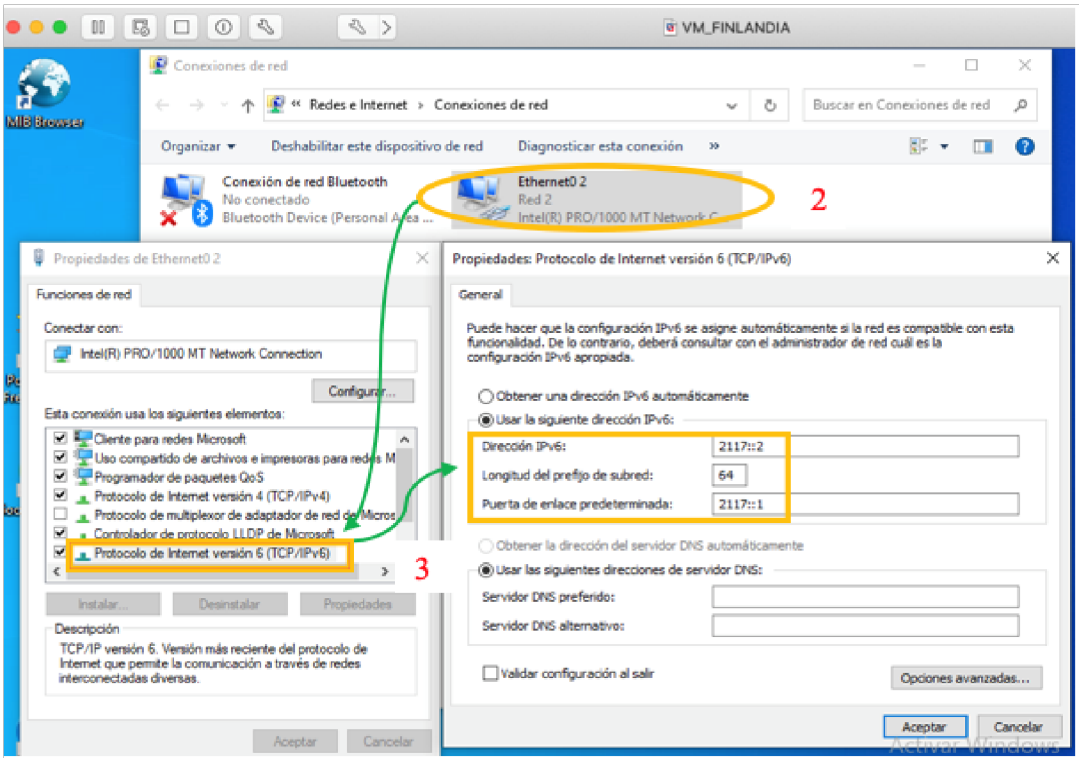


Figura 16.4. Configuración de la NIC para la máquina virtual VM_Finlandia.

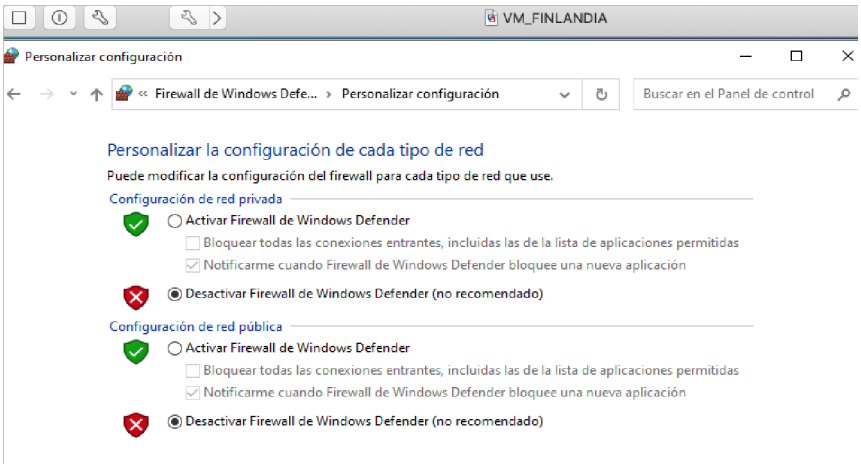


Figura 17.4. Deshabilitación del firewall en la máquina virtual.

Nota: Este procedimiento se hace para ambas máquinas virtuales.

5. **Vinculación de las máquinas virtuales de VMware Fusion a GNS3**

Para poder importar una máquina virtual con GNS3 se realizan los siguientes pasos:

1. Abrir GNS3→ seleccionar la pestaña **preferencias.**
2. Ir a la sección **VM ware VM templates** o Elegir pestaña **nueva,** elegir el **tipo de servidor "local o GNS3"** o Elegir la máquina virtual, previamente cargada en VMware fusion o Finalizar la carga de la máquina virtual.

El proceso de vinculación se realizó tal cual se menciona anteriormente como se observa en las figuras 18.4 y 19.4.

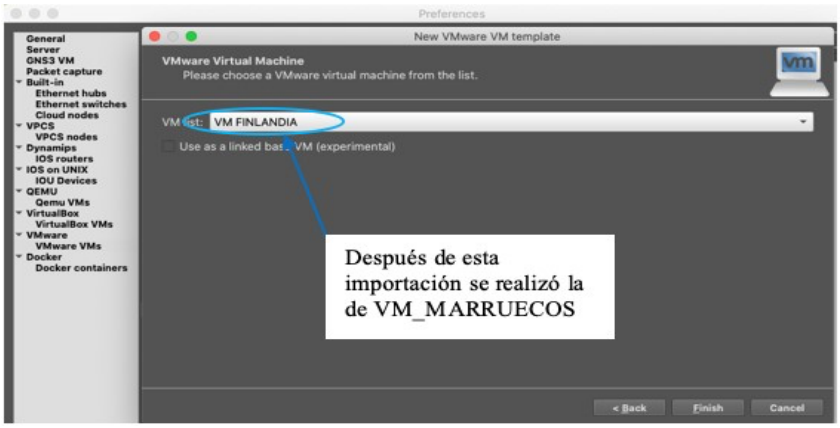


Figura 18.4. Importación de máquina virtual de VMware a GNS3.

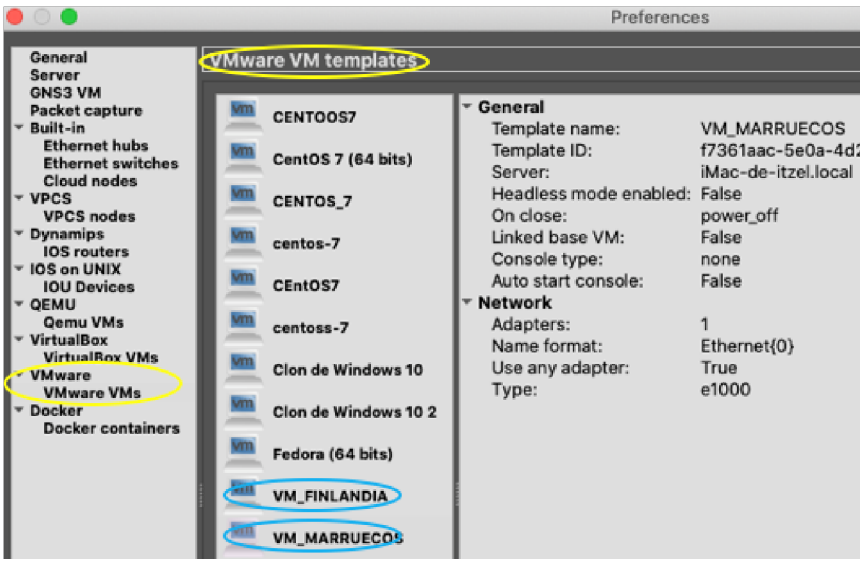


Figura 19.4. Finalización de importación de máquinas virtuales.

6. Configuración de SNMP de la topología AFICACONNECT-GEANT en GNS3

Una vez configurado el enrutamiento en la emulación, se prosigue a configurar SNMP en cada uno de los dispositivos a gestionar. Para esta emulación se utilizaron dos estaciones de gestión, una conectada al router Marruecos y otra conectada al router Finlandia (ver figura 20.4), donde se pueden utilizar cualesquiera de las dos, para realizar la gestión eligiendo alguno de los 78 dispositivos a gestionar mostrados en la figura 6.4.

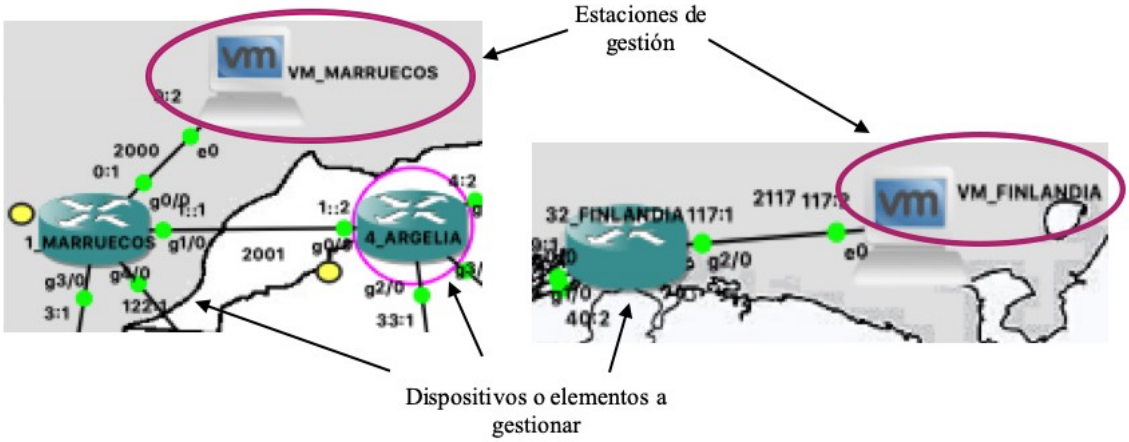


Figura 20.4. Elementos de gestión.

Una vez teniendo instaladas las máquinas virtuales en la topología AfricaConnect-Geant, se les instalaron los softwares de gestión PowerSNMP y iReasoning MIB Browser. Por consiguiente, se activó el router que lleva por nombre Argelia y por medio de la terminal se configuró SNMP de la siguiente manera:

1. Ingresar a la terminal en modo súper usuario.
2. Declarar el comando del protocolo SNMP.
3. Declarar el nombre del grupo llamado como **afgen.**
4. Agregar el nombre del usuario llamado **UACM,** así como el grupo, el tipo de versión **v3**, escoger el tipo de autentificación **sha** identificado como **dian20** y el tipo de privacidad con el cifrado **DES** con contraseña **itzel20.**
5. Finalmente, se habilitaron los mensajes para traps.

A continuación, en la figura 21.4 se mostrarán los 5 pasos anteriores para la configuración del router Argelia utilizando el protocolo SNMPv3. Cabe mencionar que este proceso se repite para los 78 routers de la topología.

```
4_ARGELIA(config)#snmp-server community afgen ro
4_ARGELIA(config)#snmp-server community afgen rw
4_ARGELIA(config)#snmp-server group afgen v3 priv
4_ARGELIA(config)#$ user UACM afgen v3 auth sha dian20 priv des itzel20
4_ARGELIA(config)#snmp-server enable traps
```

Figura 21.4. Configuración de SNMPv3.

En relación a la configuración de SNMPv3, también se configuraron los agentes en las máquinas virtuales como se muestra en la figura 22.4,

1. Para esto abrir la máquina virtual; → abrir software **"PowerSNMP".**
2. Seleccionar pestaña **Discover;** → seleccionar pestaña **SNMP Agents;** → aparece ventana emergente **Discover SNMP Agents.**
3. Agregar la dirección del agente, (ver figura 23.4).
4. Agregar las propiedades del agente como se muestra en la figura 24.4; → se descubre el agente, (ver figura 23.4)**.**
5. finalmente se detectan los agentes de los routers de la topología mostrados en la parte izquierda de la figura 25.4.

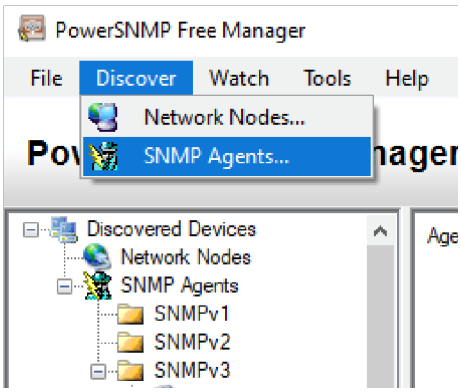


Figura 22.4. Añadir agente mediante SNMP Agents.

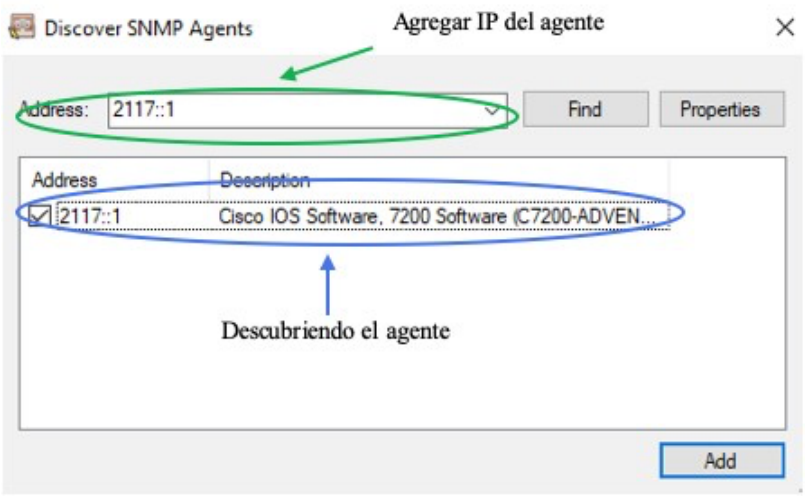


Figura 23.4. Agregar y descubrir el agente con dirección 2117::1.

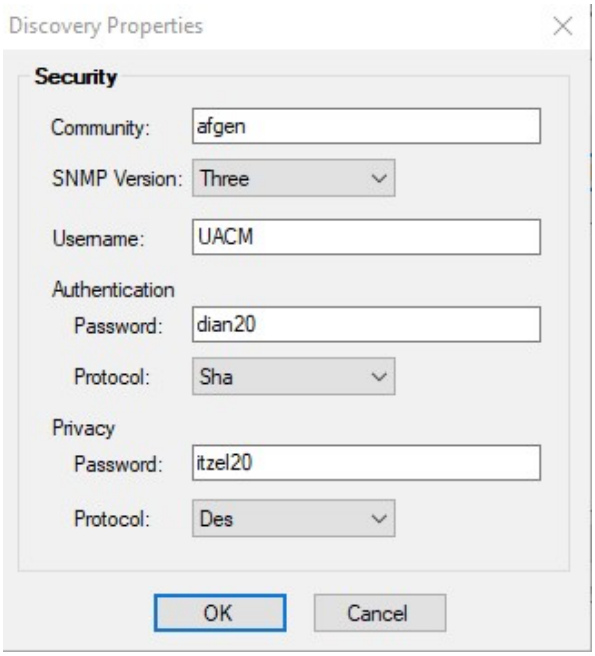


Figura 24.4. Propiedades del agente.

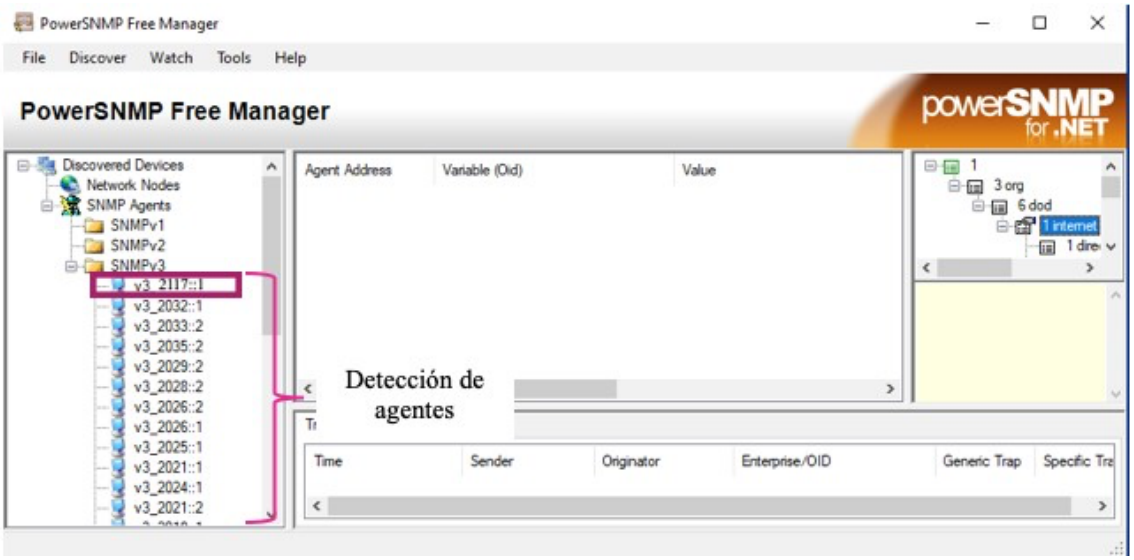


Figura 25.4. Detección de agentes en Power SNMP Free Manager.

Asimismo, se configuraron los agentes en el software iReasonig MIB Browser, una vez instalada la aplicación en nuestra máquina virtual, se procede a abrir la misma:

1. Ir a file; →ir agente; →aparece pestaña emergente **Advanced Properties of SNMP Agent.**
2. Elegir versión **"v3";** →agregar la dirección IP del agente a descubrir; → seleccionar el puerto 161.
3. En la parte de autentificación y privacidad agregar parámetros del agente para tener acceso a la información, como se muestra en la figura 26.4.

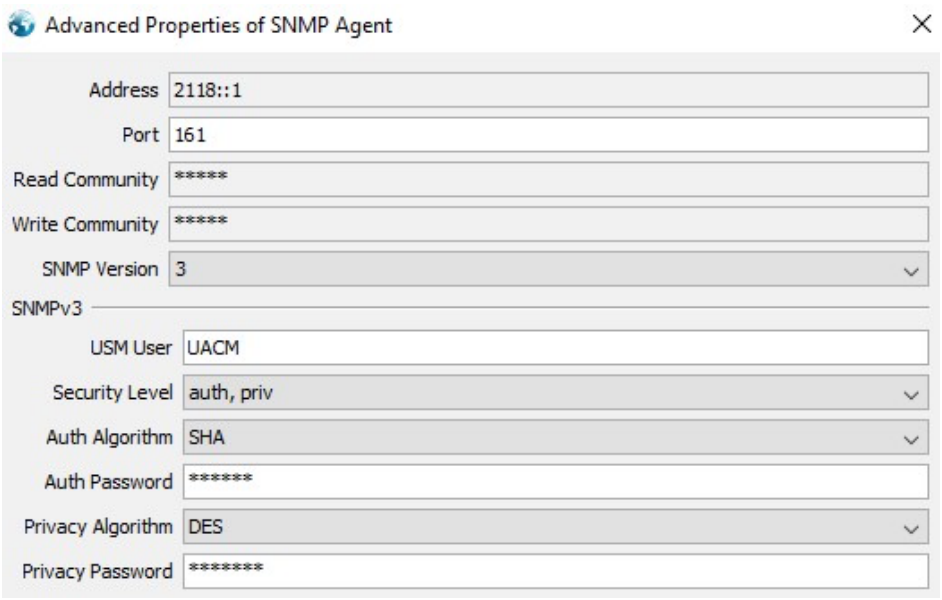


Figura 26.4. Propiedades y descubrimiento del agente con IP 2118::1.

CAPÍTULO 5. RESULTADOS

5.1 RESULTADOS DE CONECTIVIDAD

En esta sección se hablará sobre los resultados de la conectividad entre los routers de las redes avanzadas en cuestión y de cómo funcionaron los protocolos de enrutamiento OSPFv3 y BGP-4, para corroborar la correcta configuración de estos.

5.1.1 Conectividad al interior de los AS usando OSPF.

En esta sección se utilizó la instrucción **show ipv6 route ospf** para comprobar la correcta ejecución del protocolo de enrutamiento OSPFv3. Por ejemplo, se verificó que en el router Argelia, existieran todas las rutas internas **O** de OSPF, pertenecientes a su AS AfricaConnect2, contando con un total de 38 redes como se muestra en la figura 1.5. De igual manera se verificó que en el router de Francia2, existieran todas las rutas internas **O** pertenecientes a su AS Geant, contando con un total de 76 redes como se muestra en la figura 2.5.

Como se presentó en la *sección 3.2:* IGP tiene la capacidad de relacionarse al interior de una organización en un AS. Los protocolos de enrutamiento de gateway interior más conocidos son OSPF, EIGRP y RIP.

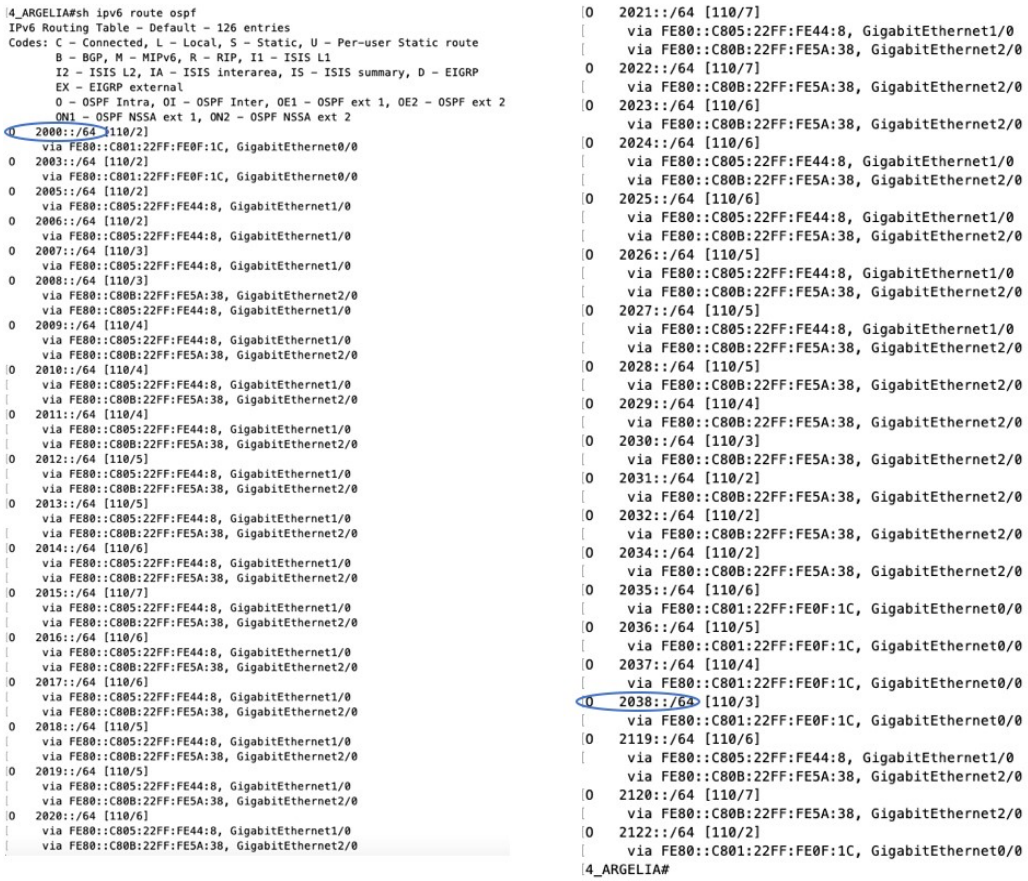


Figura 1.5. Tabla de enrutamiento del router Argelia.

```
57_FRANCIA2#sh ipv6 route ospf
IPv6 Routing Table - Default - 126 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2039::/64 [110/8]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2040::/64 [110/7]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2041::/64 [110/7]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2042::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2043::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2044::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2045::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2046::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2047::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2048::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2049::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2050::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2051::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2052::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2053::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2054::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2055::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2056::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2057::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2058::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2059::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2060::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2061::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2062::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2064::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2065::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2066::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2067::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2068::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2069::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2070::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2071::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2072::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2074::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2075::/64 [110/2]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2077::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2078::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2079::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2080::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2081::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2082::/64 [110/2]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2083::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2085::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2086::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2088::/64 [110/2]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2089::/64 [110/2]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2090::/64 [110/2]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2091::/64 [110/2]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2092::/64 [110/2]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2093::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2094::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2095::/64 [110/3]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2096::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2097::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2098::/64 [110/3]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2099::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2100::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2101::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2103::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2104::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2105::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2106::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2107::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2108::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2109::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2110::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2111::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2112::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2113::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2114::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2115::/64 [110/6]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2116::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2117::/64 [110/8]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2123::/64 [110/5]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2124::/64 [110/4]
     via FE80::C83C:28FF:FE00:8, GigabitEthernet2/0
O   2125::/64 [110/4]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
```

La representación del óvalo azul significa el rango de direcciones, donde se corrobora que pertenecen a su AS interno correspondiente, usando OSPF.

Recordando : AfricaConnect 2000: :/64 – 2038: :/64
Geant 2039: :/64 – 2125: :/64
Estos rangos de direcciones no cuentan precisamente con la numeración continua de principio a fin.

Figura 2.5. Tabla de enrutamiento del router Francia2.

5.1.2 Resultado del protocolo de enrutamiento dinámico OSPF para rutas internas y rutas externas aprendidas mediante OSPF vía BGP.

En este punto se tomarán como ejemplo los routers Marruecos para AfricaConnect y Estonia para Geant. Estos tienen configurado el protocolo de Gateway interior OSPF el cual tienen por objetivo interconectar a sus propios Autonomous Systems considerados como de área 0 o de backbone. Estos son routers identificados como BBR, para ver más detalles ir a la figura 9. Cabe destacar que todos los routers BBR fueron configurados con el protocolo de Gateway interior OSPF.

Se analizó un router BBR por cada AS. En el caso de AfricaConnect se tomó como ejemplo el router Marruecos y para Geant se tomó el router Estonia. Se utilizó la instrucción **show ipv6 route** para obtener las tablas de enrutamiento y estudiarlas de manera independiente para identificar todas aquellas redes internas **O** y compartidas **OE2**, como se muestra en las figuras 3.5 y 4.5. En el caso del router Marruecos, se pueden apreciar las 38 redes que puede alcanzar dentro de su propio AS **AfricaConnect**, así como las 76 redes aprendidas mediante OSPF vía BGP, identificadas mediante OE2, es decir todas aquellas direcciones que también son OSPF, pero pertenecen al otro AS **Geant**, no al propio.
En el caso del router Estonia, se pueden apreciar las 76 redes que puede alcanzar dentro de su propio AS **Geant**, así como las 38 redes aprendidas mediante OSPF vía BGP, es decir, todas aquellas direcciones que también son OSPF, pero pertenecen al otro AS **AfricaConnect**. Se pueden ver las diferencias en estas rutas en función de cada uno de los términos que se describen a continuación:

- **O** – Se identifican todas aquellas redes que puede alcanzar, construidas mediante OSPF dentro de una misma área, para este caso dentro del área 0 o de backbone.
- **C** – Son aquellas redes que están conectadas directamente al router.
- **L** – Identifica que la ruta es link-local. Cuando la interfaz se configura con una dirección IP y se activa, creará automáticamente una red de enlace local.
- **OE2** – Describe las redes que puede alcanzar, aprendidas mediante OSPF vía BGP. Para consultar las tablas completas ir al Apéndice F.

AS- Africa Connect2

```
1 MARRUECOS#sh ipv6 route
IPv6 Routing Table - Default - 126 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2000::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2000::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001::/64 [0/0]
     via GigabitEthernet1/0, directly connected
L   2001::1/128 [0/0]
     via GigabitEthernet1/0, receive
C   2003::/64 [0/0]
     via GigabitEthernet3/0, directly connected
L   2003::1/128 [0/0]
     via GigabitEthernet3/0, receive
O   2004::/64 [110/2]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2005::/64 [110/3]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2006::/64 [110/3]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2007::/64 [110/4]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2008::/64 [110/4]
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2009::/64 [110/5]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2010::/64 [110/5]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2011::/64 [110/5]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2012::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2013::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2014::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2015::/64 [110/8]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2016::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2017::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2018::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2019::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2020::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2021::/64 [110/8]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2022::/64 [110/8]
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2023::/64 [110/7]
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2024::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2025::/64 [110/7]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2026::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2027::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2028::/64 [110/6]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2029::/64 [110/5]
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
O   2030::/64 [110/4]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2031::/64 [110/3]
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
O   2032::/64 [110/3]
     via FE80::C806:22FF:FE49:38, GigabitEthernet4/0
     via FE80::C804:22FF:FE41:8, GigabitEthernet1/0
```

AS- Géant

```
34 ESTONIA#sh ipv6 route
IPv6 Routing Table - Default - 123 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2000::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2001::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2003::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2004::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2005::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2006::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2007::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2008::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2009::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2010::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2011::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2012::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2013::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2014::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2015::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2016::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2017::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2018::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2019::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2020::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2021::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2022::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2023::/64 [110/1]
OE2 2024::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2025::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2026::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2027::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2028::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2029::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2030::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2031::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2032::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2033::/64 [110/1]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2034::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2035::/64 [110/6]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2036::/64 [110/5]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2037::/64 [110/4]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
OE2 2038::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2039::/64 [110/5]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2040::/64 [110/4]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2041::/64 [110/4]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2042::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2043::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2044::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2045::/64 [110/3]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2046::/64 [110/2]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2047::/64 [110/4]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2048::/64 [110/4]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2049::/64 [110/5]
     via FE80::C826:26FF:FE39:38, GigabitEthernet0/0
O   2050::/64 [110/4]
```

O – Direcciones pertenecientes al AS- Géant (dentro de su AS son identificadas como IGP).

OE2 – Direcciones externas pertenecientes al AS- Africaconnect2 (dentro de su AS son identificadas como IGP)

Figura 3.5. Tablas de enrutamiento Marruecos y Estonia para el protocolo de ruteo IGP parte 1/4.

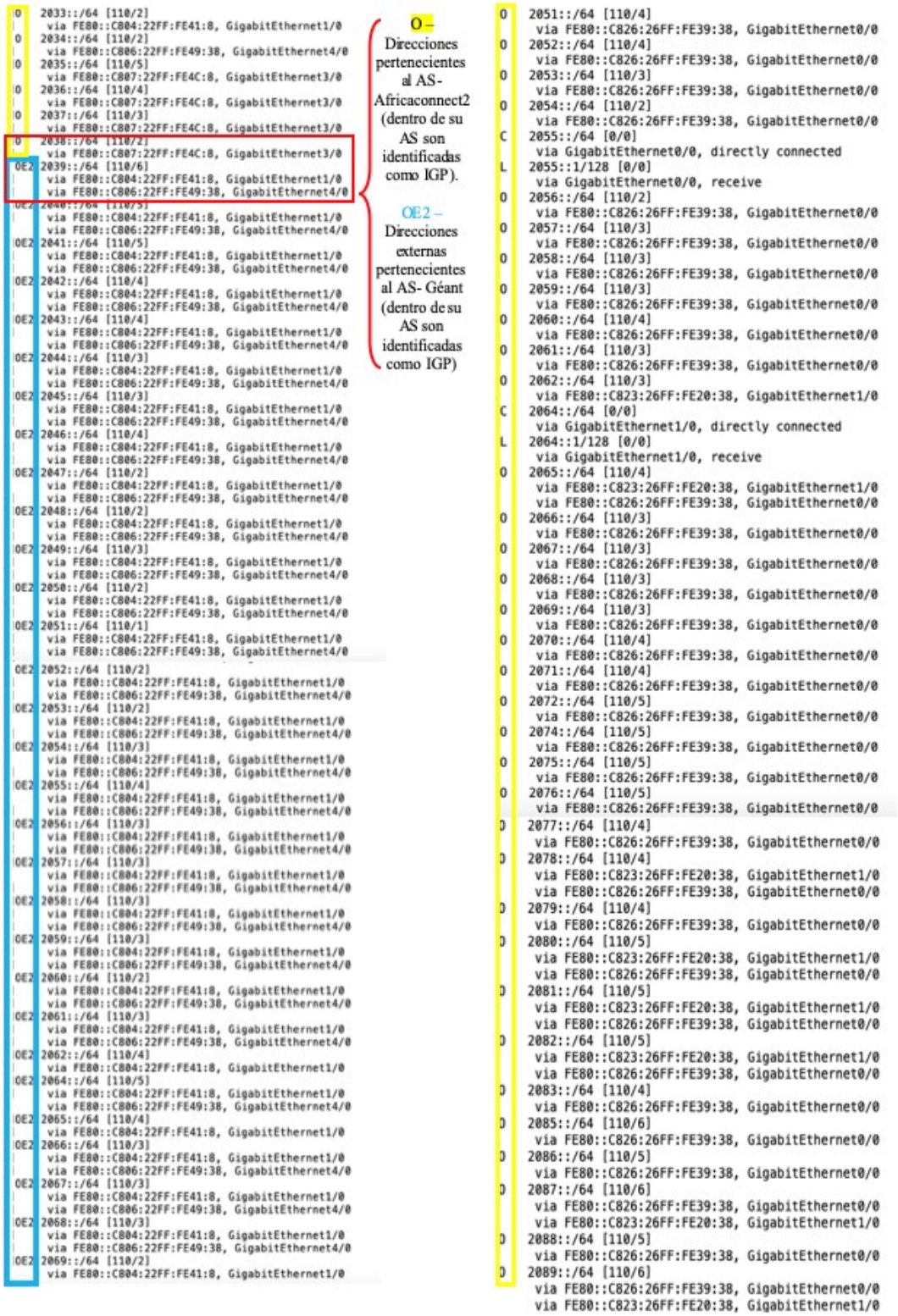


Figura 4.5. Tablas de enrutamiento Marruecos y Estonia para el protocolo de ruteo IGP parte 2/4.

5.1.3 Resultado de la conectividad al exterior de los AS para rutas internas, externas y su redistribución aprendidas mediante BGP.

En este punto se tomarán como ejemplo los routers Argelia para AfricaConnect y Francia2 para Geant, que a diferencia de los routers Marruecos y Estonia, éstos tienen configurado el protocolo BGP y son identificados como ASBR que tienen por objetivo interconectar Autonomous Systems de área 0 o de backbone, para ver más detalles ir a la figura 5.3.

Con la instrucción **show ipv6 route** se comprobaron ambas tablas de enrutamiento en las cuales se aprecian todas aquellas redes aprendidas mediante el protocolo OSPF e identificadas por la letra **O**, es decir en el caso del router Argelia contendrá todas las redes de su propio AS AfricaConnect. Mientras que el router Francia2 contendrá todas las redes de su propio AS Geant, además todas las redes del AS Geant estarán contenidas en la tabla de enrutamiento del router Argelia, mientras que todas las redes del AS AfricaConnect estarán contenidas en la tabla de enrutamiento del router Francia2, ambas aprendidas mediante el protocolo BGP e identificadas por la letra **B**, como se muestra en la figura 5.5 y 6.5.
Para consultar las tablas completas ir al Apéndice G.

Como se presentó en la *sección 3.4:* los EGP utilizan el protocolo de enrutamiento dinámico BGP, son comúnmente conocidos como routers de frontera o de borde, los cuales se encuentran al extremo de cada sistema autónomo, en el caso de esté trabajo se puede identificar en la topología mediante un círculo de color rosa, además se caracterizan por tener la capacidad de establecer vínculos entre sistemas autónomos, ya que pueden coexistir en su funcionamiento varios protocolos IGP dentro de los EGP. Estos sistemas autónomos tienen una administración por separado.

AS-AfricaConnect2 **AS-Geant**

```
4_ARGELIA#sh ipv6 route
IPv6 Routing Table - Default - 126 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2000::/64 [110/2]
     via FE80::C801:22FF:FE0F:1C, GigabitEthernet0/0
C   2001::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001::2/128 [0/0]
     via GigabitEthernet0/0, receive
O   2003::/64 [110/2]
     via FE80::C801:22FF:FE0F:1C, GigabitEthernet0/0
C   2004::/64 [0/0]
     via GigabitEthernet1/0, directly connected
L   2004::2/128 [0/0]
     via GigabitEthernet1/0, receive
O   2005::/64 [110/2]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
O   2006::/64 [110/2]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
O   2007::/64 [110/3]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
O   2008::/64 [110/3]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
O   2009::/64 [110/4]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2010::/64 [110/4]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2011::/64 [110/4]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2012::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2013::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2014::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2015::/64 [110/7]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2016::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2017::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2018::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2019::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2020::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2021::/64 [110/7]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2022::/64 [110/7]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2023::/64 [110/6]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2024::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2025::/64 [110/6]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2026::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2027::/64 [110/5]
     via FE80::C805:22FF:FE44:8, GigabitEthernet1/0
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2028::/64 [110/5]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2029::/64 [110/4]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2030::/64 [110/3]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2031::/64 [110/2]
     via FE80::C80B:22FF:FE5A:38, GigabitEthernet2/0
O   2032::/64 [110/2]
```

```
57_FRANCIA2#sh ipv6 route
IPv6 Routing Table - Default - 126 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2000::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2001::/64 [20/0]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2003::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2004::/64 [20/0]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2005::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2006::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2007::/64 [20/3]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2008::/64 [20/3]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2009::/64 [20/4]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2010::/64 [20/4]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2011::/64 [20/4]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2012::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2013::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2014::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2015::/64 [20/7]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2016::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2017::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2018::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2019::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2020::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2021::/64 [20/7]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2022::/64 [20/7]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2023::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2024::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2025::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2026::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2027::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2028::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2029::/64 [20/4]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2030::/64 [20/3]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2031::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2032::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2033::/64 [20/0]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2034::/64 [20/2]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2035::/64 [20/6]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2036::/64 [20/5]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2037::/64 [20/4]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
B   2038::/64 [20/3]
     via FE80::C804:22FF:FE41:54, GigabitEthernet3/0
O   2039::/64 [110/8]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2040::/64 [110/7]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2041::/64 [110/7]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2042::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2043::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2044::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2045::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2046::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2047::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2048::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2049::/64 [110/6]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
O   2050::/64 [110/5]
     via FE80::C830:26FF:FEB0:1C, GigabitEthernet0/0
```

Figura 5.5. Tabla de enrutamiento Argelia y Francia2 para el protocolo de ruteo EGP parte 1/3

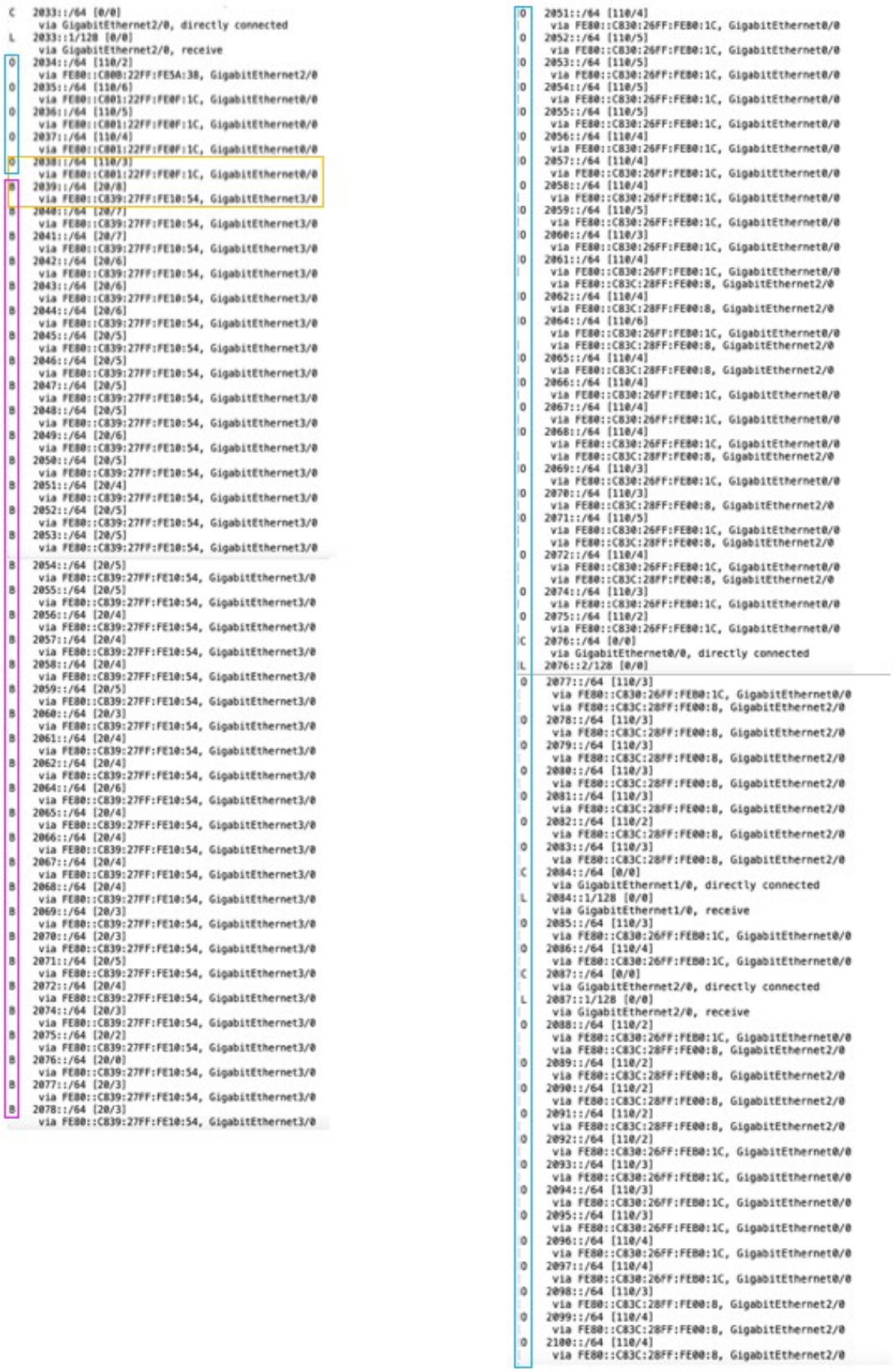


Figura 6.5. Tabla de enrutamiento Argelia y Francia2 para el protocolo de ruteo EGP parte 2/3.

Por lo tanto, para reafirmar lo dicho anteriormente, en las tablas de enrutamiento de los routers Argelia y Francia2 se llevó a cabo el protocolo BGP, asumiendo que un AS informe a otro sobre las redes que puede alcanzar a partir de este. Asimismo, estos routers de backbone denominados ASBR de un mismo AS deben intercambiar información BGP para conocer las mismas rutas externas e internas, identificadas con color rosa y azul como se muestras en las figuras 5.5 y 6.5.

Para comprobar todas las direcciones de OSPF dentro de la tabla de enrutamiento BGP, en la figura 7.5 se muestra la información sobre las conexiones del protocolo de puerta de enlace fronterizo, donde se utilizó la instrucción **show bgp ipv6**.
Para consultar la tabla completa ir al Apéndice H.

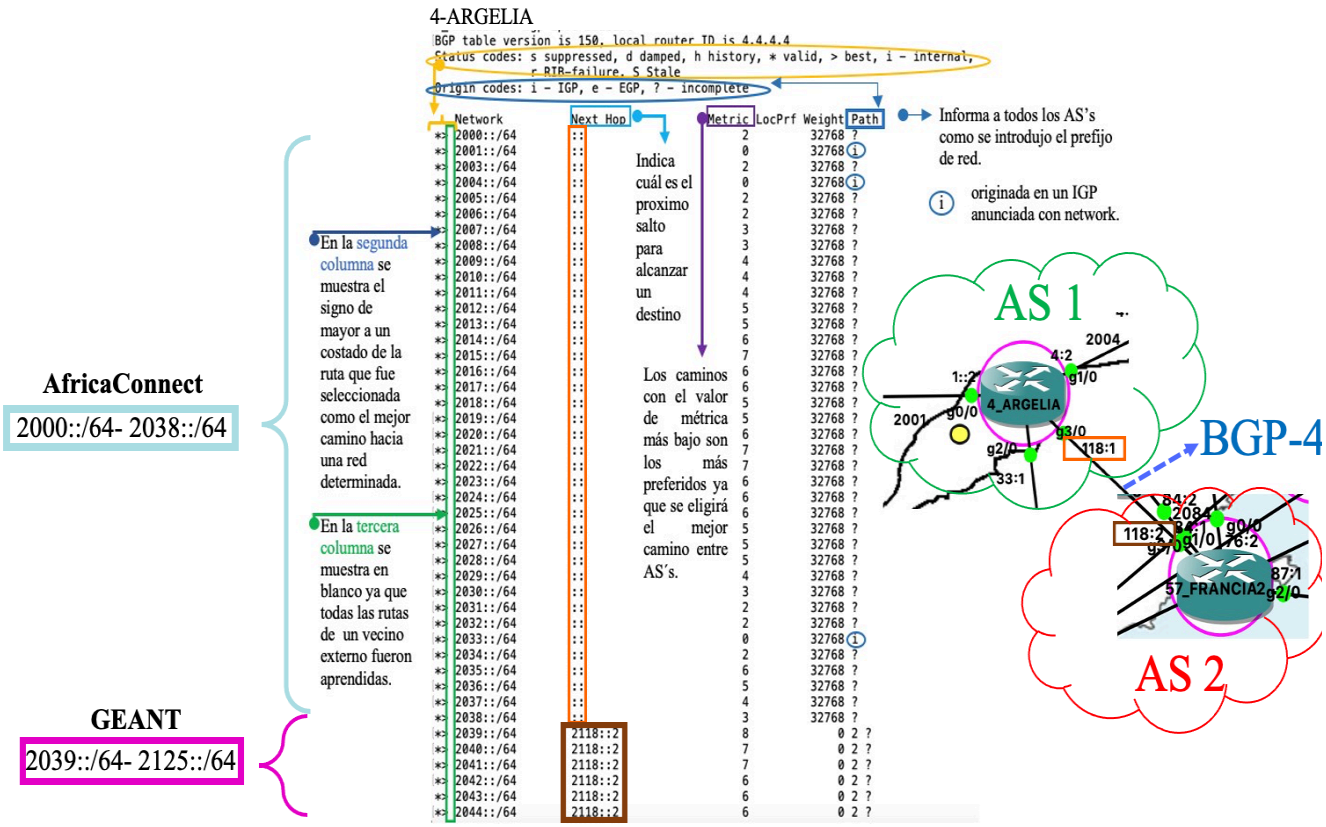


Figura 7.5. Verificación de la tabla BGP IPv6, parte 1/2.

Analizando la figura 7.5 del router Argelia que pertenece al AS AfricaConnect2 tiene un intervalo de direcciones IPv6 (2000::/64 - 2038::/64) teniendo como próximo salto para alcanzar un destino la dirección (::), es decir es la interfaz con dirección 2118::1 propia del router Argelia, además es la que tiene salida a BGP para poder comunicarse con el otro AS Geant. Por otro lado el router Argelia también detectó el intervalo de direcciones (2039::/64 – 2125::/64) que pertenecen al AS Geant y tienen como próximo salto la dirección 2118::2, la cual indica que el router externo Francia2 originó la ruta, así mismo tiene salida a BGP.

En la misma figura también se pueden observar la sección path que contiene algunos prefijos detectados con la letra i, el cual indica si la ruta ha sido aprendida por un protocolo IGP (es la ruta interior al AS del router origen que se ha configurado con la instrucción network o redistribute), es decir, son las direcciones propias al router Argelia. Ahora bien, el símbolo de "?" indica que se ha aprendido de una forma distinta (normalmente por redistribución en BGP de una ruta dinámica). Cabe señalar que el primer intervalo de direcciones del AS AfricaConnect2 pertenecen al proceso 1, mientras que el intervalo de direcciones del AS Geant pertenecen al proceso 2 como se puede observar en la figura 7.5.

La instrucción **show bgp ipv6 unicast summary**, que se ejecuta en la figura 8.5 sirve para verificar el estado de los vecinos. En este caso el vecino que se muestra es Francia2 del AS **Geant**.

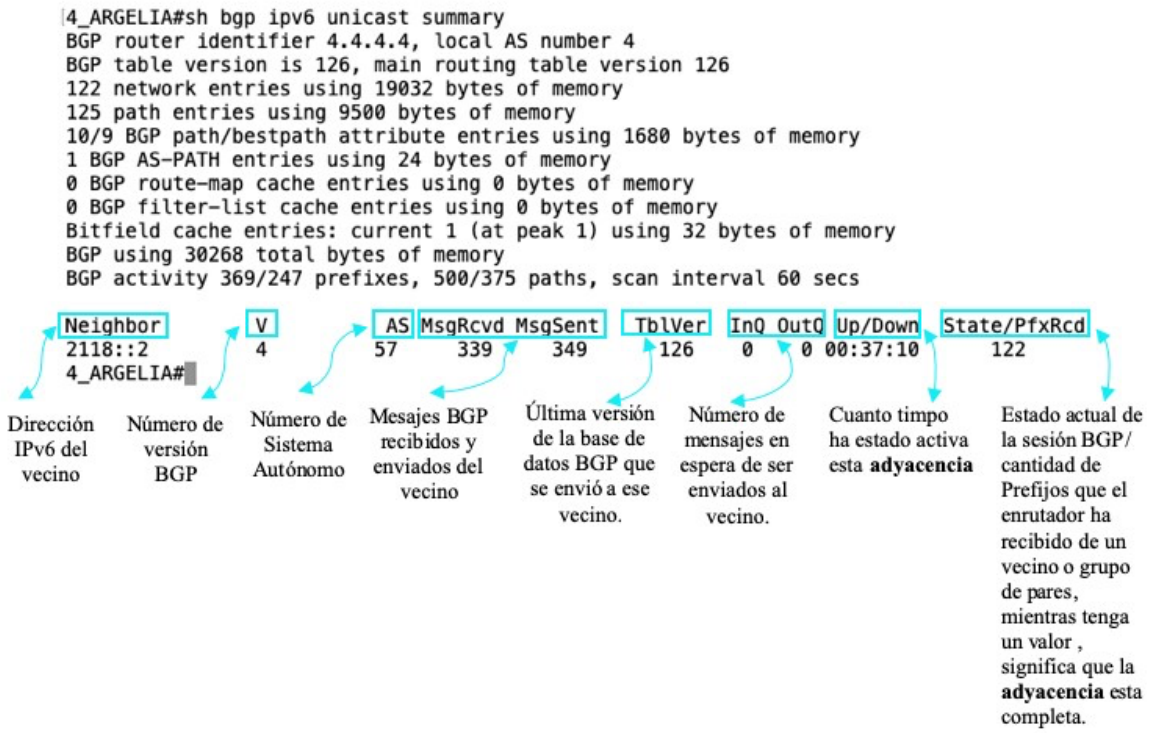


Figura 8.5. Visualización del campo BGP IPv6.

5.2 PRUEBA DE CONECTIVIDAD PARA LA RED AVANZADA AfricaConnect2-Geant4-2

Con respecto a los resultados de la prueba de conectividad de la red, fue necesario corroborar que las configuraciones de enrutamiento fueron correctas. Para esto se utilizó la herramienta llamada *ping*, la cual nos permite saber si existe o no conectividad mediante el protocolo Internet Control Message Protocol (ICMP). En la figura 9.5 se muestra la prueba de conectividad donde se eligieron los routers Finlandia y Marruecos que son los más lejanos de cada AS, con la finalidad de saber si existe conectividad en toda la topología. Además, se puede observar un envío de paquetes con la tasa (5/5), es decir cinco enviados y cinco recibidos, así como el tiempo de vida de cada paquete, por lo tanto, se demuestra que la conectividad es exitosa. En caso de no tener conectividad, se mostrarían paquetes perdidos, por ejemplo, cinco enviados y cero recibidos (5/0). Así también se puede visualizar la ejecución de la herramienta *traceroute* la cual muestra la ruta más corta, para llegar al router destino. Además, se puede visualizar en la figura 10.5 la prueba de conectividad exitosa desde la VM Marruecos a la VM Finlandia y hacia sus routers contiguos.

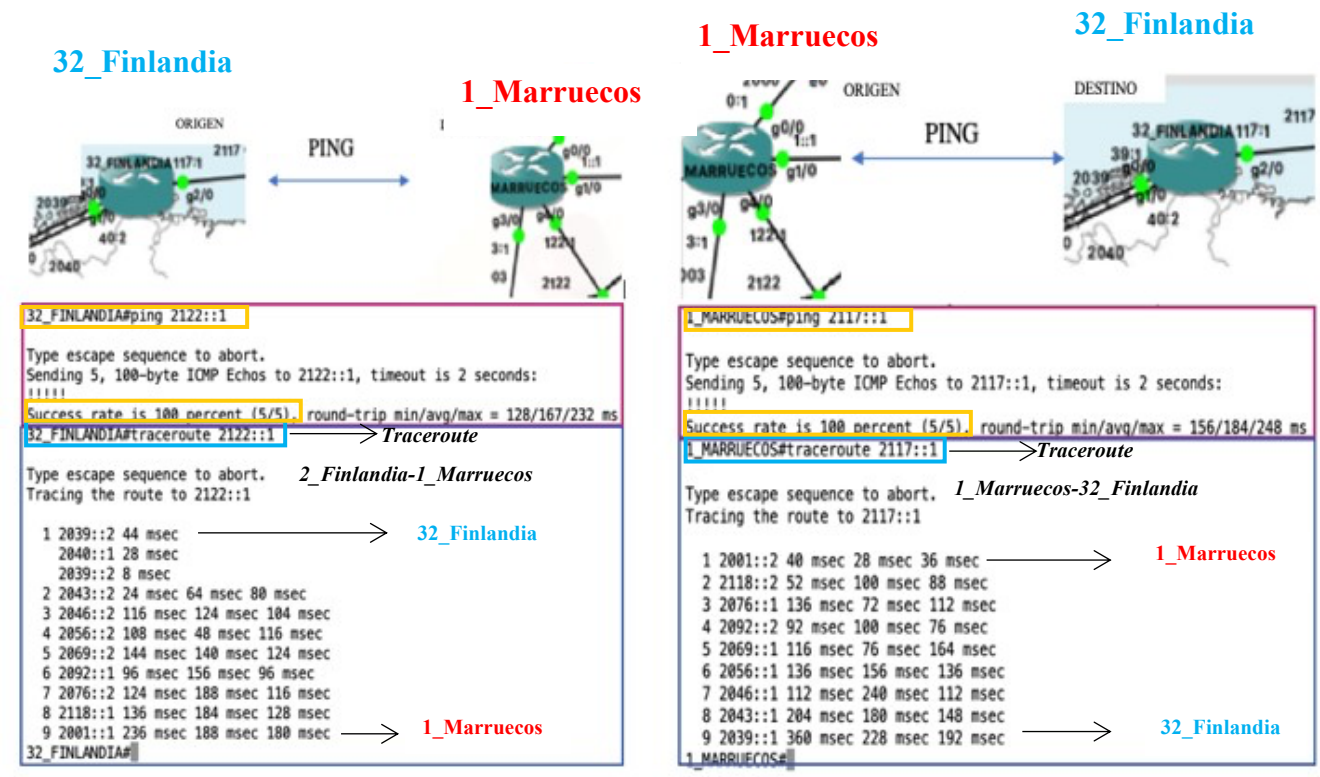


Figura 9.5. Prueba de conectividad y traceroute entre routers.

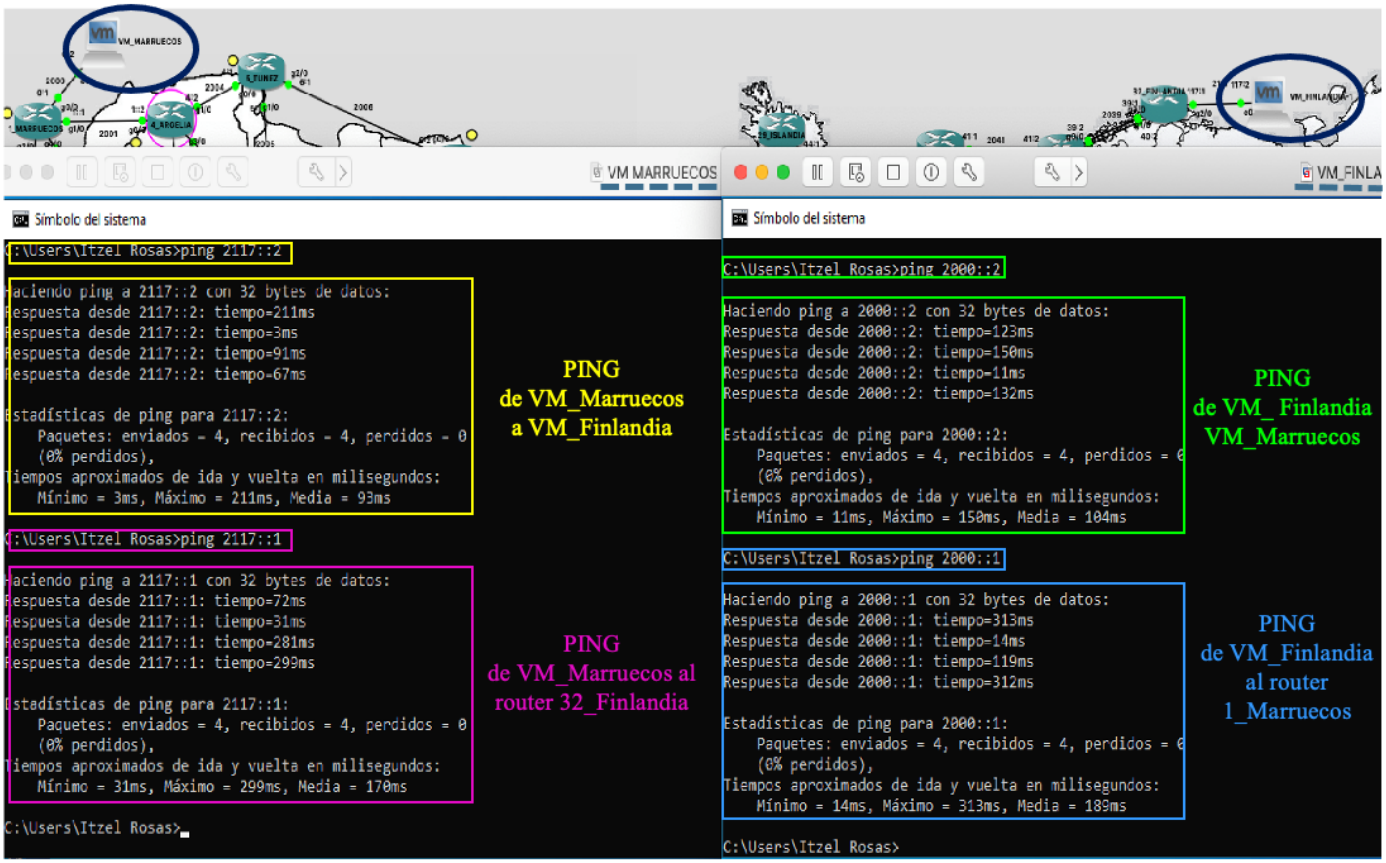


Figura 10.5. Prueba de conectividad de VM Marruecos a VM Finlandia.

5.3 RESULTADOS DE PRUEBA DE GESTIÓN

Teniendo la configuración SNMP, dentro de cada router es posible gestionarlos por medio de cualquier estación de gestión (NMS). Una vez dentro de esta, se abre el software iReasonig, se ingresa la dirección IP y los parámetros del dispositivo a gestionar, así mismo se elige la versión 3 a utilizar. Una vez que la sesión lista, se puede apreciar el árbol MIB. En este se podrá elegir qué variable del dispositivo se quiere gestionar, entonces que, se procede a realizar la gestión para todos los routers. Para esta tesis se eligieron 5 variables para gestionar los 78 routers, como son **sysName, IfNumber, SysUpTime, ifOperStatus e ifTable** las cuales se mostrarán a continuación: Para esta prueba de gestión, se seleccionó el agente de enrutador de cada uno de los routers de la topología y luego se eligió la variable **sysName**, que nos dio el nombre de los routers, como se muestra en la figura 11.5, para visualizar la tabla completa (ver apéndice E).

Nota: Es importante mencionar que con el software PowerSNMP no fue posible realizar la gestión con algunas variables, a pesar de que la configuración de los agentes fue exitosa, por lo que se optó por utilizar el software iReasonig.

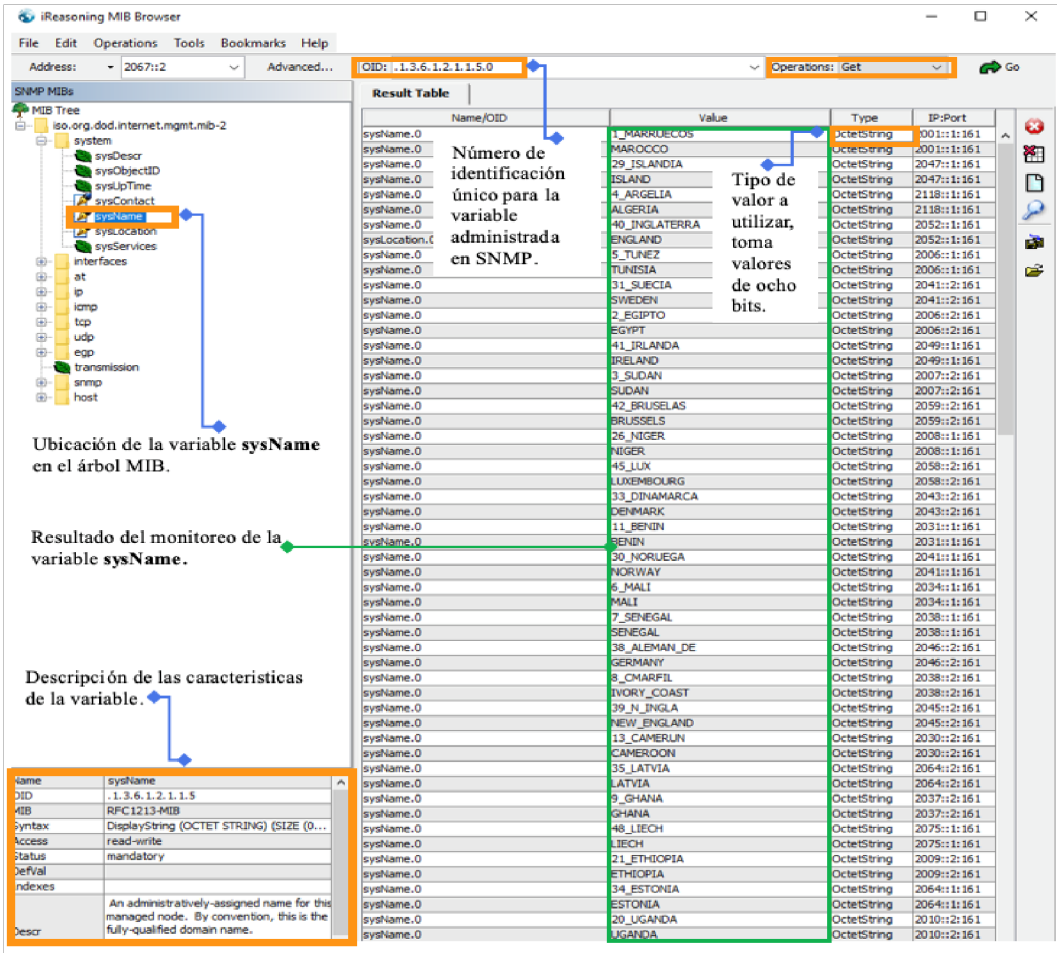


Figura 11.5. Monitoreo de la variable sysName para los 78 routers, parte 1/3.

Cuando se administra un router, algo que se quiere saber es la cantidad de interfaces que tiene el router, con la variable **IfNumber** se puede saber el número de interfaces que contiene cada uno de los 78 routers de la topología, como se muestra en la figura 12.5.

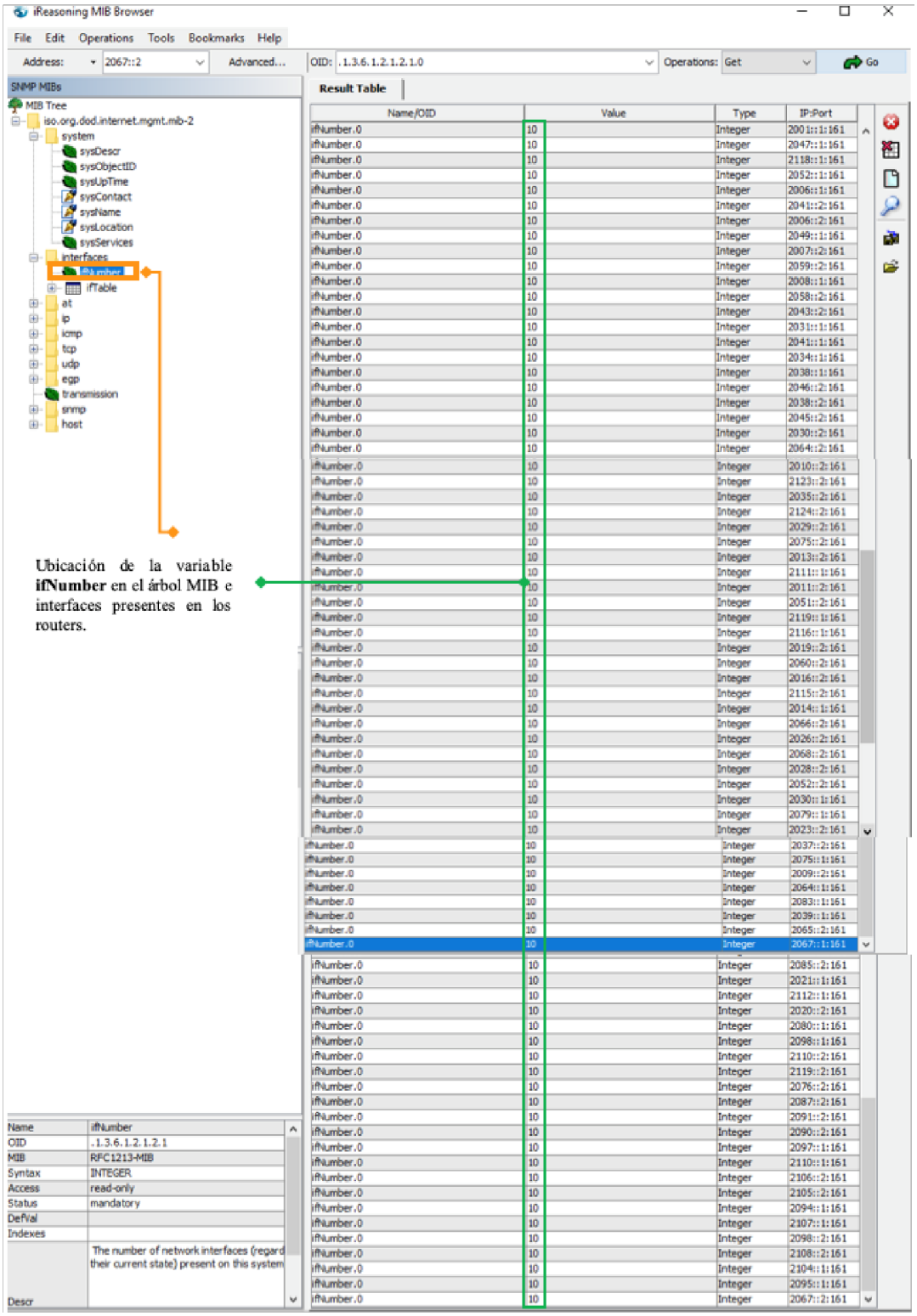


Figura 12.5. Monitoreo de la variable IfNumber para los 78 routers.

Otra de las variables de interés a gestionar en un router es **SysUpTime**, para saber el tiempo de operación en el que un router estuvo encendido, como se muestra en la figura 13.5. Esta prueba se hizo para los 78 routers.

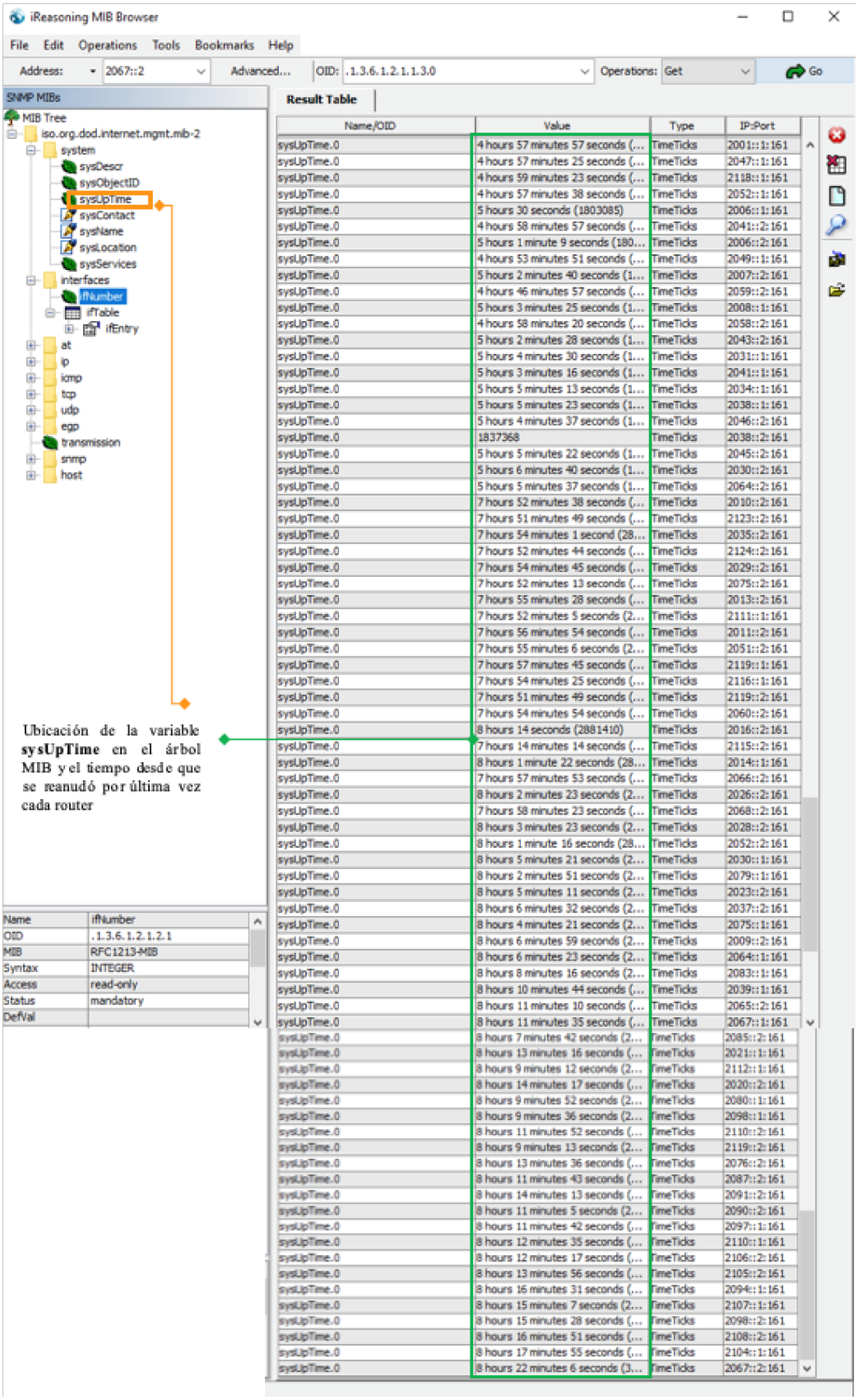


Figura 13.5. Monitoreo de la variable SysUpTime para los 78 routers.

Con el fin de saber si las interfaces se encuentran activas o no, se utilizó la variable **ifOperStatus**, para los 78 routers como se muestra en la figura 14.5.

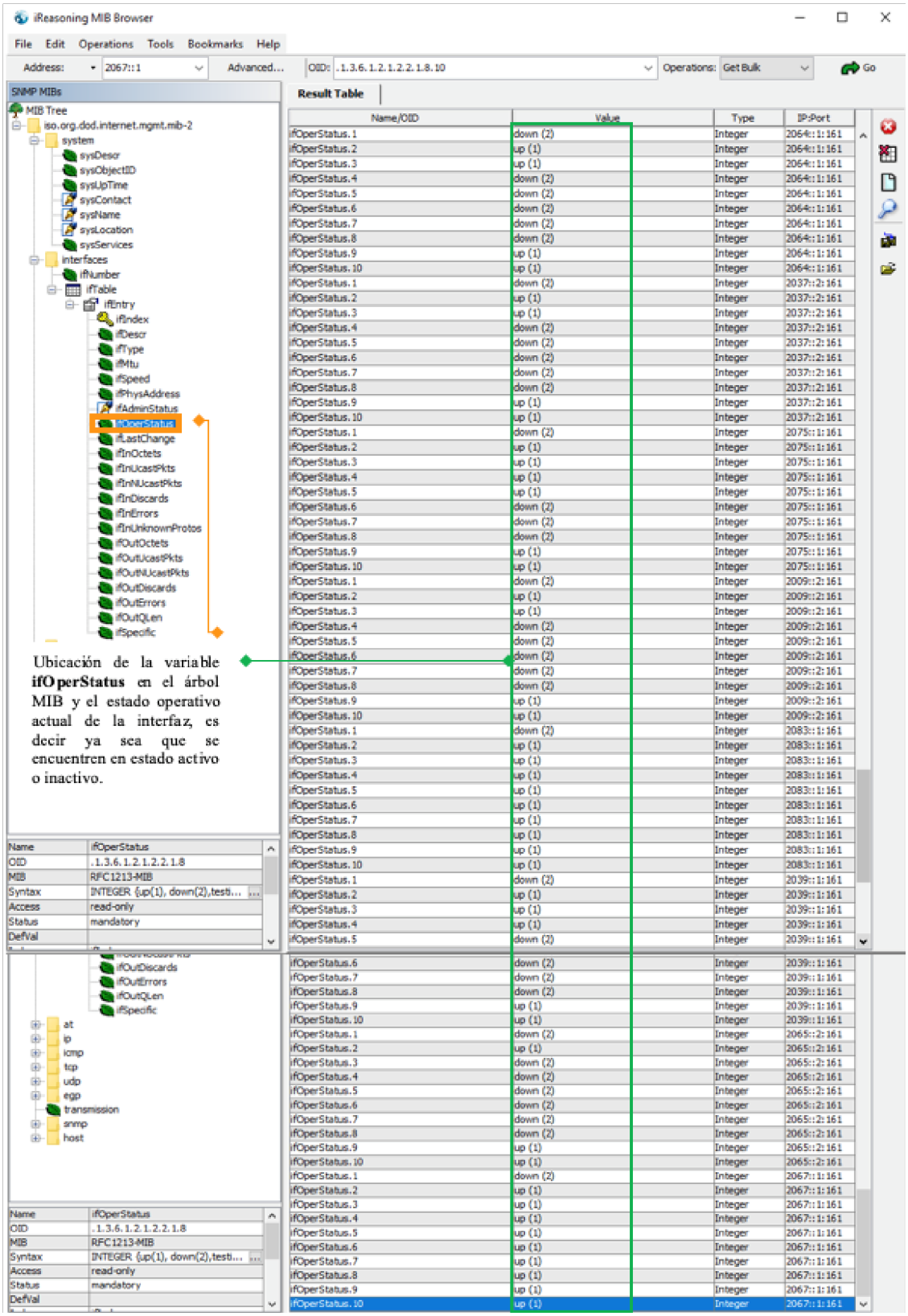


Figura 14.5. Monitoreo de la variable ifOperStatus para los 78 routers.

Finalmente se gestionó la variable **ifTable** únicamente para tres routers (Alemania_DE3, Bulgaria, Austria2) de la topología, en donde se indican las características de las interfaces que despliega ifNumber, como se muestra en la figura 15.5.

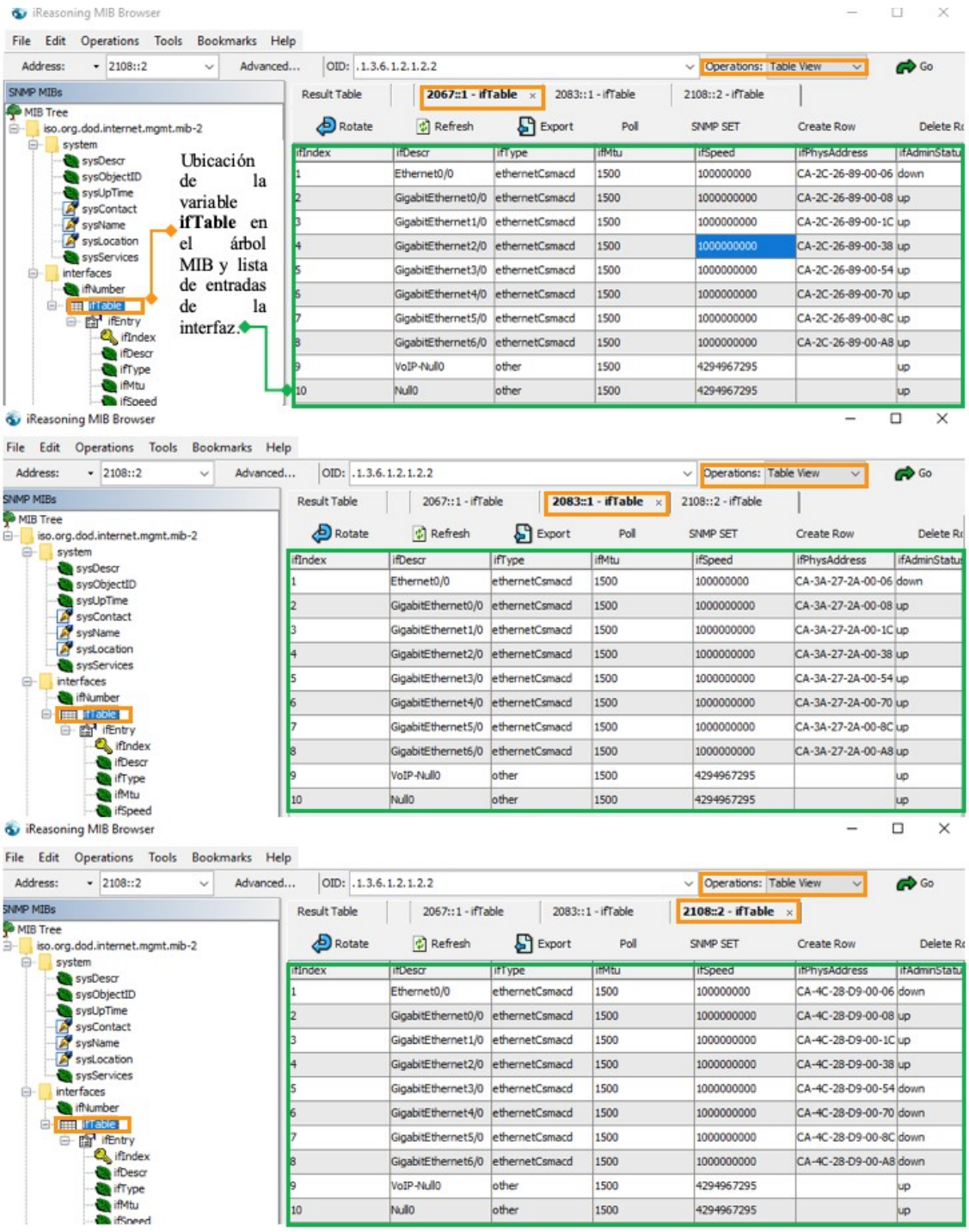


Figura 15.5. Monitoreo de la variable ifTable para los 3 routers.

5.4 ANÁLISIS DE MENSAJES EN LA TOPOLOGÍA AfricaConnect-Geant

En esta sección, se utilizó la herramienta Wireshark como analizador de paquetes, para lograr validar el funcionamiento de toda la red AfricaConnect – Geant y observar el comportamiento en cuanto al flujo de mensajes que pasan por la interfaz, así como cada uno de los mensajes generados. Cabe señalar que no todos los paquetes de datos pueden ser interpretados o capturados debido a la implementación adicional de seguridad que tienen. A continuación, en la figura 16.5 se muestra la captura de pantalla del software Wireshark, con su respectiva explicación de los elementos básicos del entorno de trabajo.

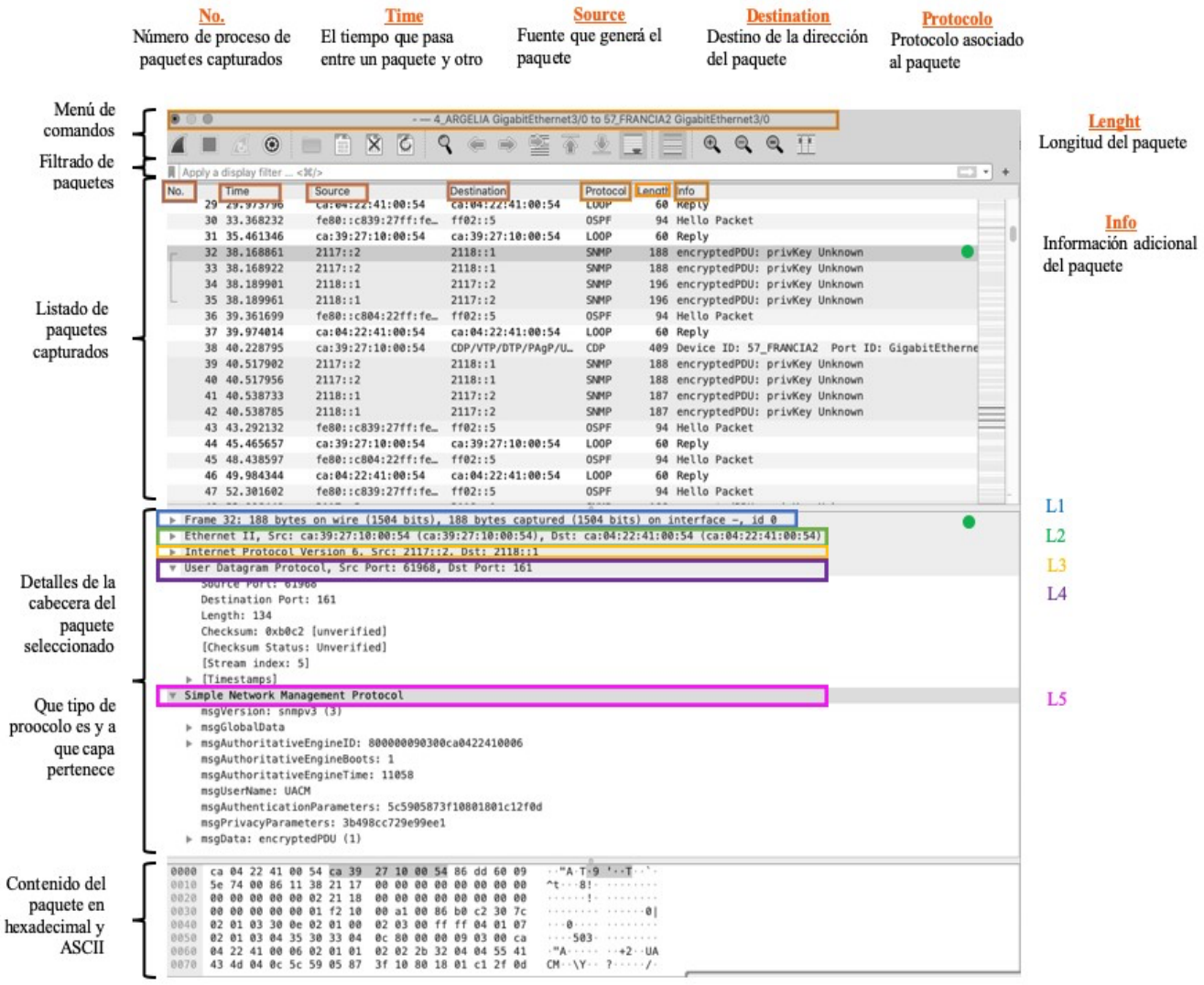


Figura 16.5. Entorno de trabajo del software Wireshark.

Para ejemplificar el análisis de los paquetes, en esta sección supervisaremos los mensajes del protocolo OSPF que pasan por la interfaz Marruecos – Argelia realizando un ping desde la VM_Finlandia al router Marruecos. En la figura 17.5 se observa la lista de paquetes capturados donde se lograron obtener tres de los cinco mensajes OSPF.

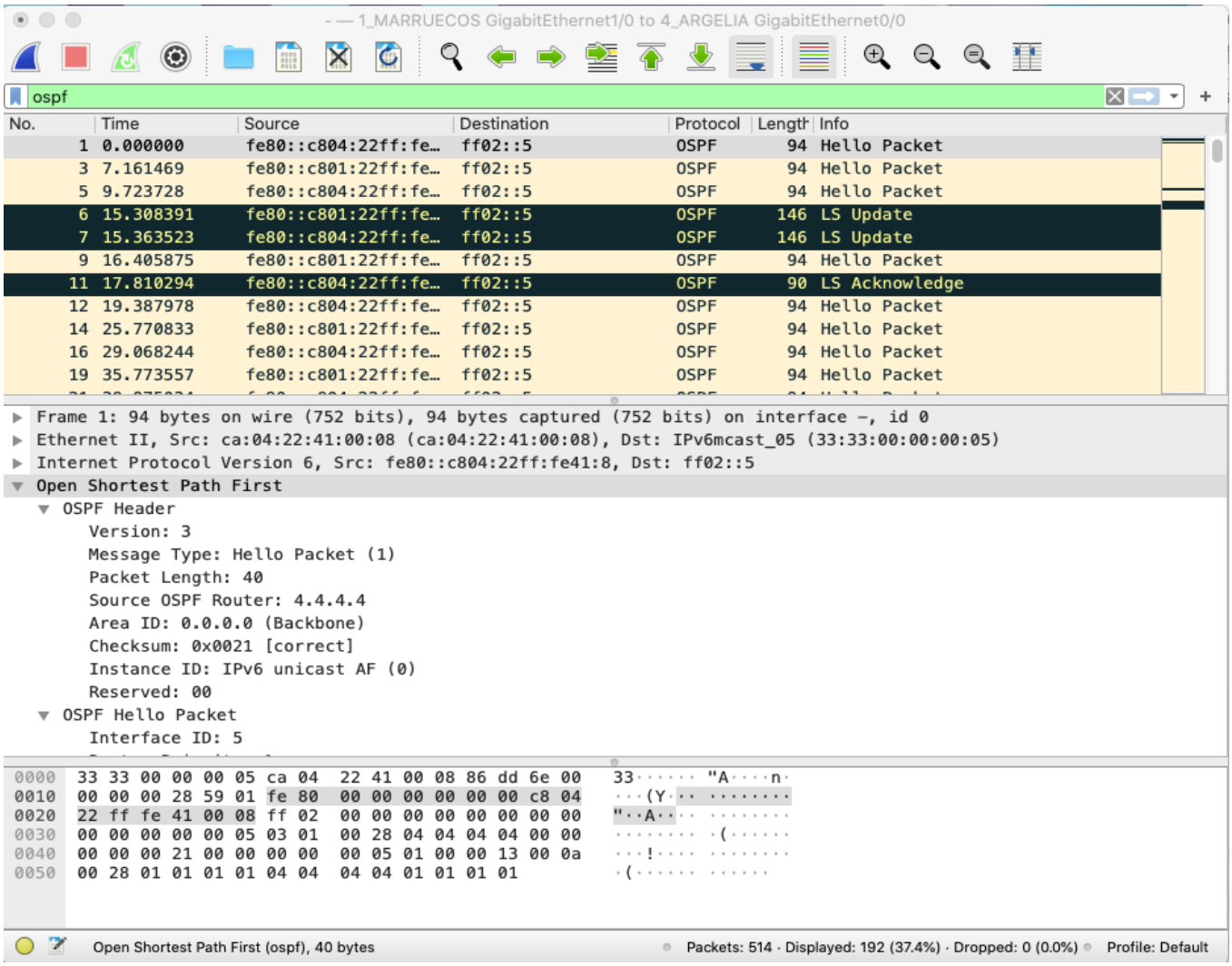


Figura 17.5. Mensajes OSPF visualizados en la interfaz Wireshark.

Posteriormente, se muestran tres de los cuatro mensajes BGP obtenidos en la emulación y analizados con Wireshark desde el enlace Argelia (2118::1) - Francia2 (2118::2) que se muestran en la figura 18.5, 19.5 y 20.5. Se observan en la lista de paquetes los mensajes BGP capturados como son Open, Update y Keepalive, donde se muestran los detalles en la cabecera de cada uno de estos paquetes.

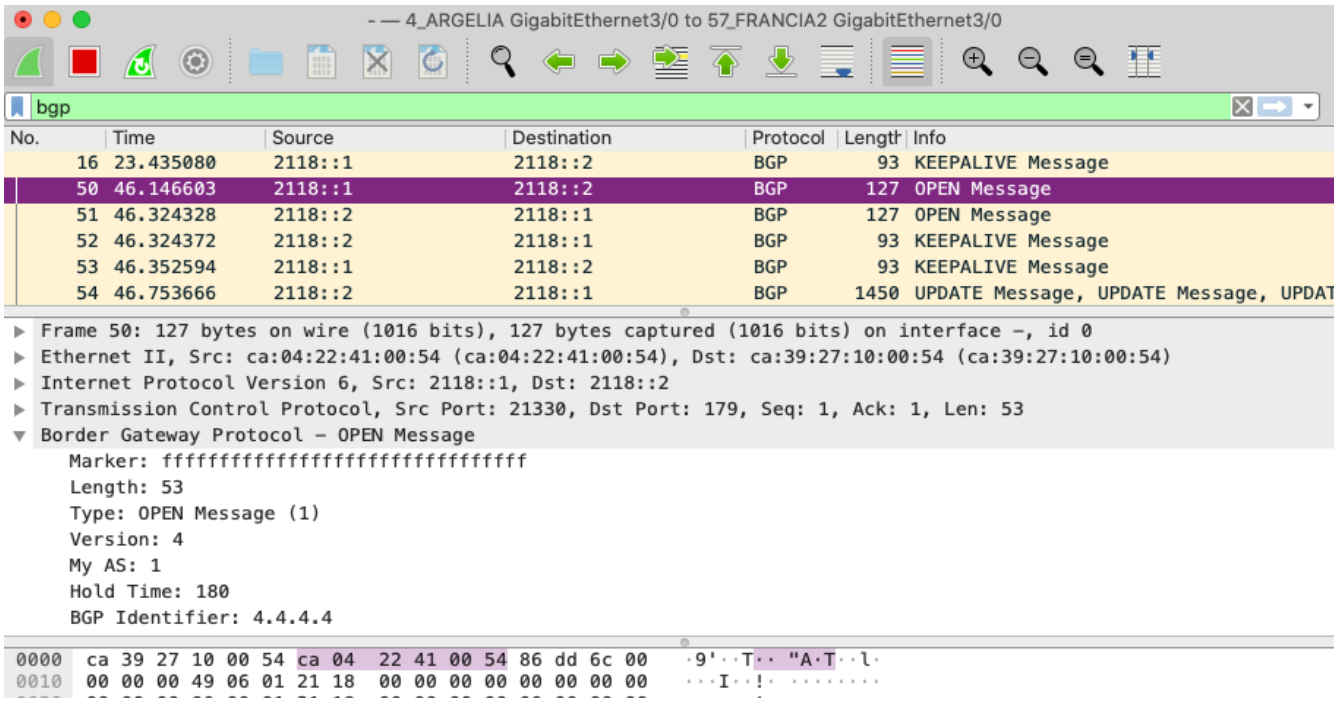


Figura 18.5. Mensaje BGP OPEN.

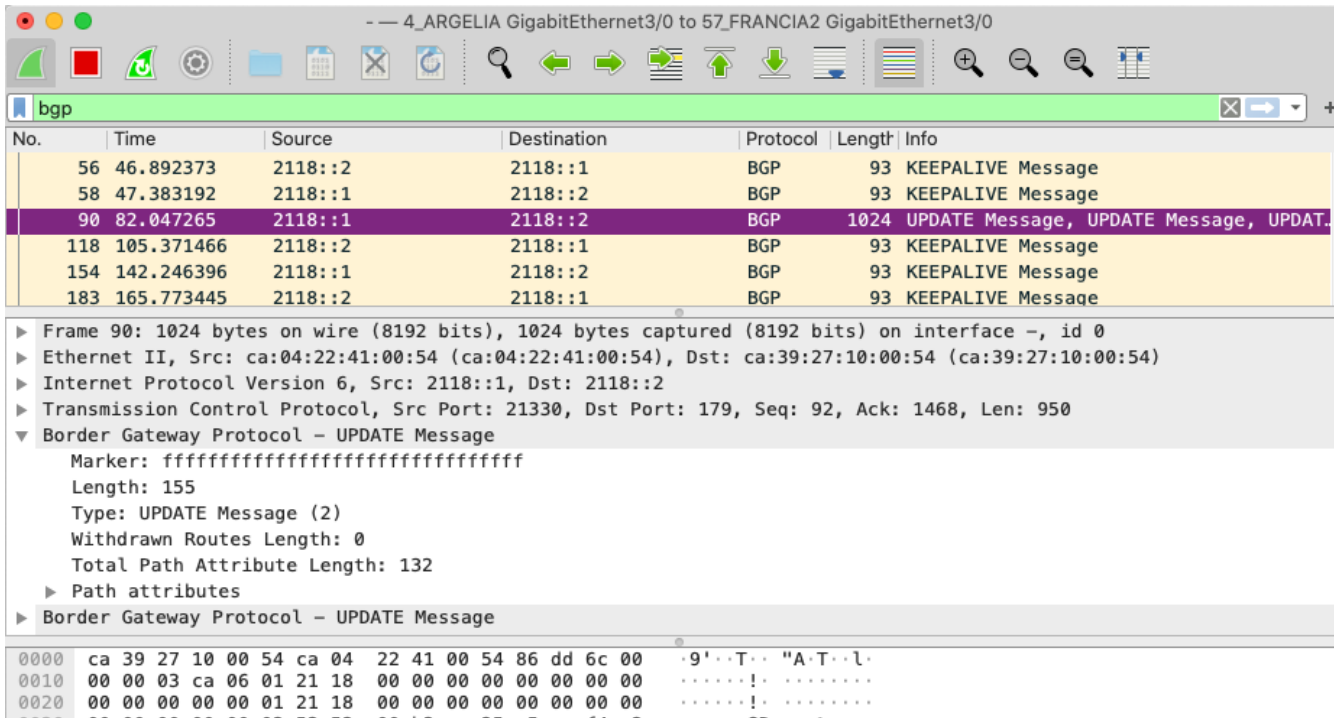


Figura 19.5. Mensaje BGP UPDATE.

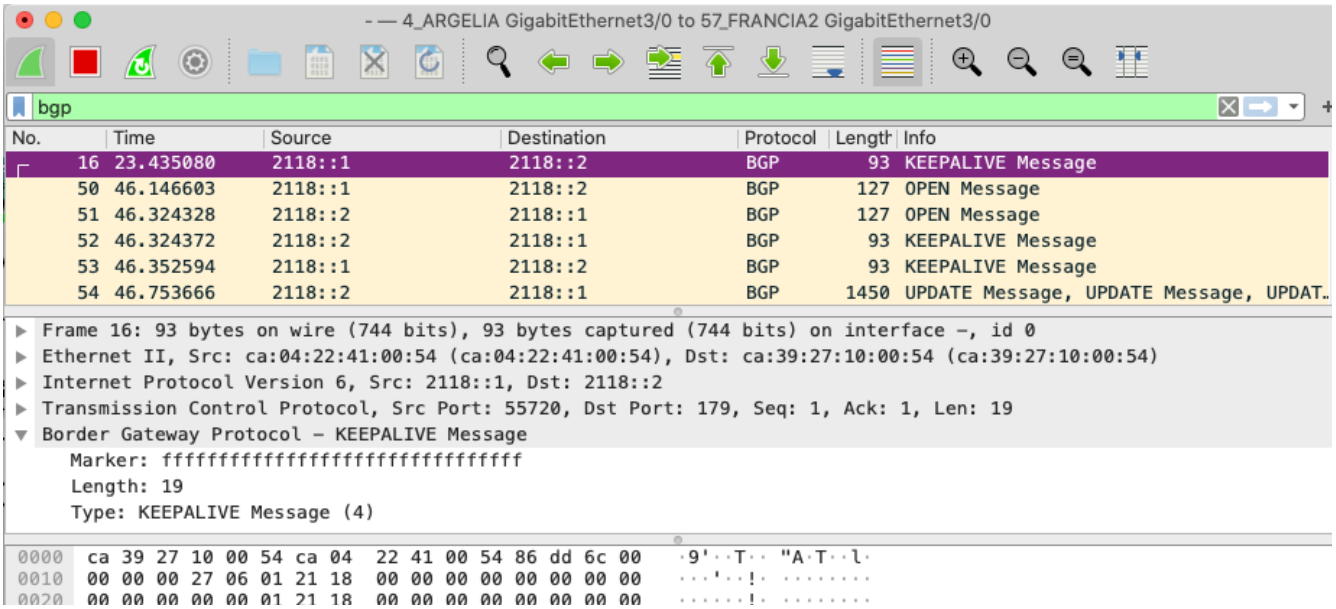


Figura 20.5. Mensaje BGP KEEPALIVE.

Por último, para ejemplificar el análisis del protocolo SNMPv3, se supervisó la interfaz de red Marruecos (2001::1) - Argelia, donde se realizó la gestión desde la VM_Finlandia (2117::2). En la figura 21.5, se muestran la lista de paquetes capturados SNMP y los detalles de la cabecera del paquete que se despliega en Wireshark, el cual corrobora que la información es genuina respecto a lo configurado previamente con el protocolo SNMP en cada router vía CLI.

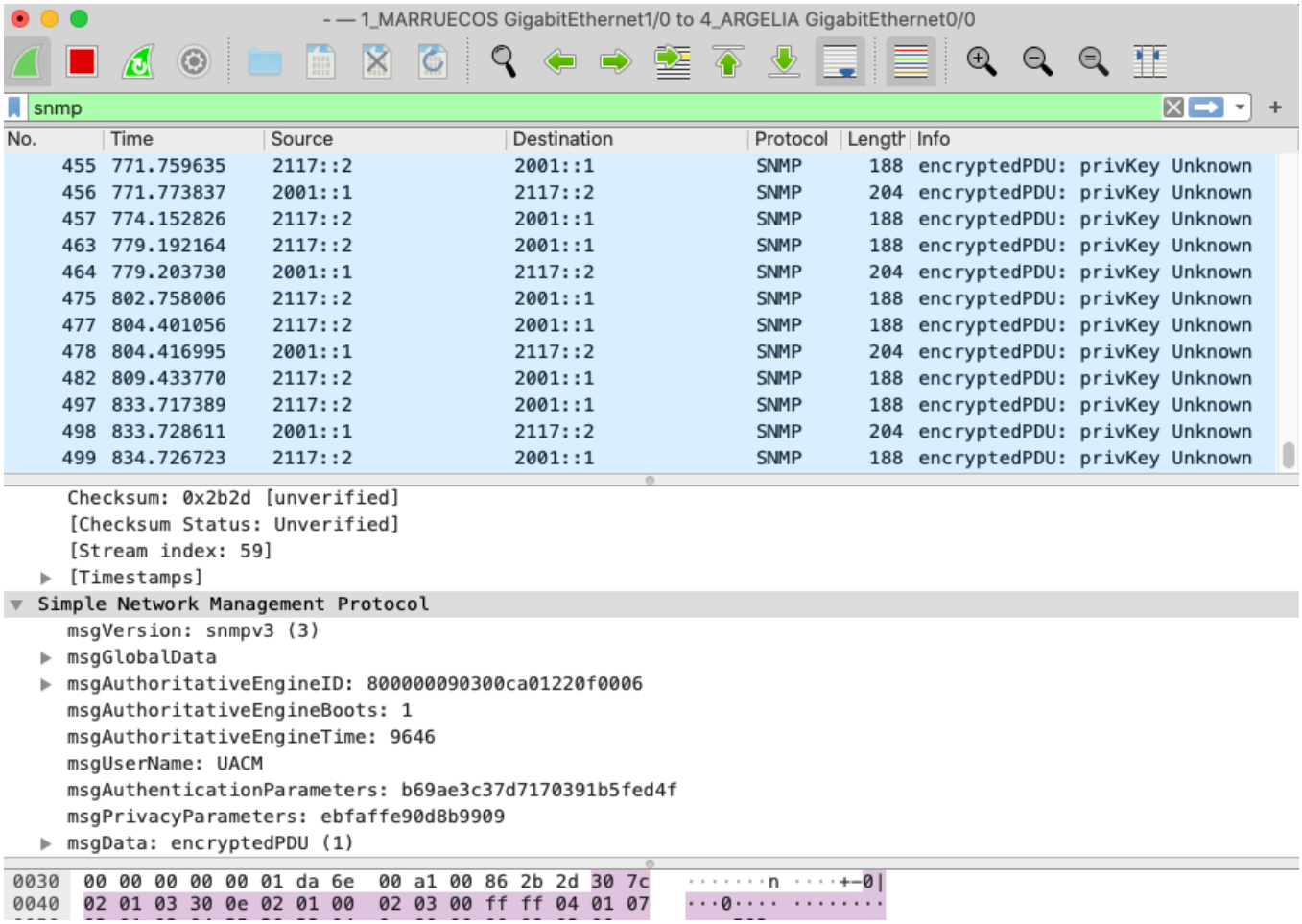


Figura 21.5. Mensajes SNMPv3 visualizados en la interfaz Wireshark.

5.5 RESULTADOS DEL RENDIMIENTO DE LA EMULACIÓN

Se deben tomar en cuenta las características del equipo físico para conocer el consumo de recursos GNS3, sin olvidar que puede ser variado, éste depende de qué tan compleja sea la emulación que se quiera ejecutar. En este caso se utilizó una computadora de escritorio con S.O MacOS Catalina v 10.15.7 con un procesador 2.7 GHz Intel Core i5 de cuatro núcleos y 16 GB en RAM. Debido a que la emulación consume parte de estos recursos, implica en el equipo mayor costo computacional, por lo que se llevó tanto al equipo como a la emulación al límite como se puede ver en la tabla 1.5, donde se puede observar el análisis del consumo de recursos de las redes avanzadas por separado, y posteriormente la consolidación de estas, así como el tiempo que tomó activar la topología completa.

Redes Avanzadas emuladas	Uso de recursos			Tiempo de estabilidad
	CPU (%)	RAM (%)	RAM física (16 GB) RAM usada (GB)	
AfricaConnect2	37.8	54	11.27	16:21 min
Geant4	60.2	71.2	12.06	29:14 min
AfricaConnect2 - Geant4	100	80.3	13.63	50:41 min

Tabla 1.5. Recursos consumidos por GNS3.

Analizando la tabla 1.5 es importante mencionar que el 100% del CPU es debido a la activación de todos los routers de la topología. Se requirió un tiempo para estabilizar la emulación de aproximadamente 50 minutos. Si no se da el tiempo suficiente, el emulador se cierra, colapsando su funcionamiento. En la figura 22.5, se puede ver la caraga de trabajo de los núcleos del CPU donde se alcanzó el 100%.

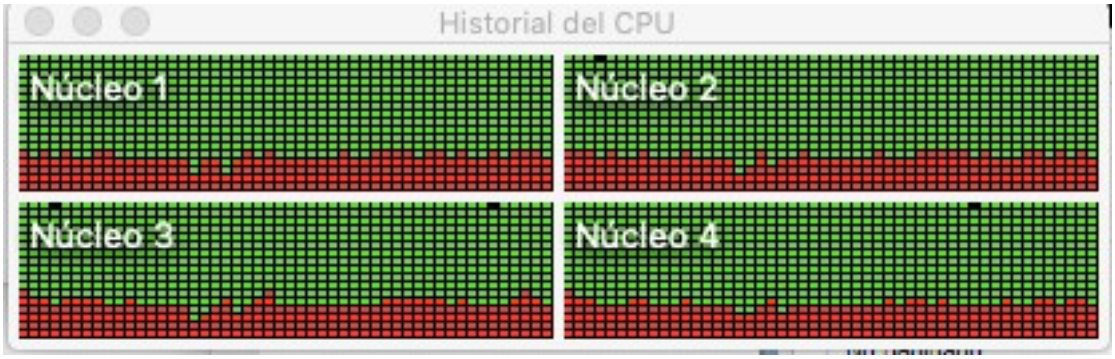


Figura 22.5. Rendimiento del CPU del equipo físico en emulación.

Además, en la tabla 1.5 se muestra el total de recursos que se consumieron en la emulación de la integración de las redes avanzadas la cual fue de 13.63 GB de memoria RAM, es decir muy cercano al total de la RAM física, ya que entre más routers activados se tenga, la exigencia de recursos de la emulación será mayor. En la figura 23.5, se puede ver la demanda de espacio en la RAM la cual se alcanzó el 80.3%.

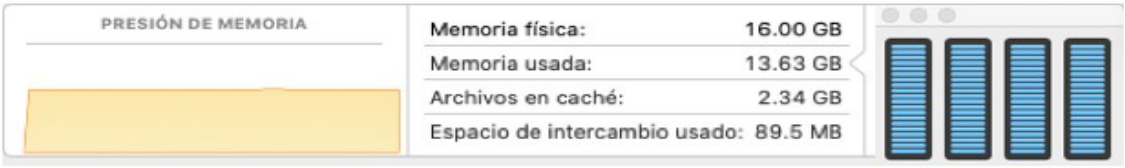


Figura 23.5. Registro de uso de memoria RAM del equipo físico en emulación.

CAPÍTULO 6. CONCLUSIONES

6.1 CONCLUSIONES

Se tuvieron varios retos a los cuales nos enfrentamos, ya que la topología a emular, está compuesta por la unión de dos sistemas autónomos que son AfricaConnect y Geant. Estas son consideradas redes avanzadas, por el tipo de infraestructura tan cara y empresas tan grandes a las que pertenecen en la vida real, pero también la emulación con GNS3 es considerada como una aproximación a la realidad, aunque es muy exigente en cuanto a recursos informáticos, pero aun así fue posible ejecutar estas redes troncales complejas.

Cumpliendo con los objetivos específicos del proyecto:

Se estudió, analizó y emuló la conectividad y gestión del backbone de AfricaConnect2 y Geant interconectando los sistemas autónomos utilizando los protocolos OSPFv3 y BGP-4 para el enrutamiento dentro y fuera de los sistemas autónomos y SNMPv3 para la gestión, todo esto bajo el protocolo IPv6. Se utilizó una computadora de escritorio MacOS Catalina v 10.15.7 con un procesador 2.7 GHz Intel Core i5 de cuatro núcleos y una RAM con 16 GB, para el desempeño de la emulación de la red en cuanto a conectividad y gestión. Con estas características se creó una topología AfricaConnect - Geant compuesta de 78 routers de backbone llegando a utilizar un 100% de RAM con un 80.3% de CPU, demorando 50 min para estabilizarse. Estas características fueron adecuadas para el desempeño de los protocolos utilizados por cada red avanzada, que son OSPFv3 y BGP-4. El primer protocolo se encargó de compartir información de las redes internas de cada AS de manera dinámica, así como el segundo protocolo hizo que hubiera comunicación entre los Sistemas Autónomos. Estos protocolos funcionaron de manera correcta, por lo que la emulación de la conectividad de la integración de estas redes avanzadas fue exitosa. Una vez verificada la conectividad total del backbone de las redes avanzadas, se realizaron actividades de gestión, por lo que se solicitó información desde el NMS a los routers mediante las variables propuestas como: **sysName** que indica el nombre de los routers, **IfNumber** indica el número de interfaces de un router, **SysUpTime** indica el tiempo de operación en el que un router estuvo encendido, **ifOperStatus** indica si las interfaces se encuentran activas o no e **ifTable** indica las características de las interfaces que despliega **ifNumber**,

llegando a obtener información útil para la gestión de la red, de esta manera se comprobó el correcto funcionamiento del protocolo SNMPv3.

- Se puso a prueba al emulador GNS3 y a nuestro equipo de cómputo bajo la topología de red compleja. Se utilizó el emulador GNS3 en su versión 2.2.10 del año 2020 nos permitió crear redes complejas y VMware Fusion en su versión 11.5.5 del año 2020 nos permitió emular máquinas virtuales, pero depende mucho de los recursos del equipo para que este emulador funcione adecuadamente. En nuestro caso es de gran importancia mencionar que nuestro equipo es limitado, por lo que decidimos agregar interfaces de tipo Giga Ethernet (GE) en lugar de Fibra Óptica (POS), para reducir recursos y así disminuir complicaciones en toda la topología, cabe resaltar que en la vida real la tecnología Giga Ethernet tiene algunas limitantes, por lo que no hubiese sido posible implementarla debido a la demanda de recursos en la emulación, por esto es que actualmente se ha adaptado una nueva tecnología de Fibra Óptica por sus múltiples y eficientes características. Por otro lado, cabe señalar que una de las ventajas del emulador GNS3 es que permite ejecutar imágenes IOS, en nuestro caso se requirió utilizar routers de backbone, por lo que se eligió la serie 7200 de Cisco, considerada una de las más estables en GNS3, siempre que use la cantidad correcta de RAM y el valor de idle que ayudará a consumir menos CPU.

  Una de las primeras limitantes que tuvimos al ejecutar este trabajo, fue la capacidad de memoria RAM de 8 GB con la que contaba la máquina a un inicio, ya que el emulador comenzaba a ralentizarse sin ser posible encender toda la topología, por lo que se optó por aumentar la capacidad de memoria a 16 GB para obtener un mejor rendimiento óptimo de ésta, por lo que se adquirieron habilidades desde encontrar las características de la memoria RAM compatible con la versión de la computadora, la instalación de ésta, hasta el desarmado y armado de la máquina. Una segunda, fue la limitante del sistema operativo Mac que utilizamos, ya que no es tan común como otros sistemas operativos como Windows, por la búsqueda de información de la instalación de los softwares, y una tercera fue la limitante de información para la configuración de los protocolos que se implementaron con IPv6.

- Se desarrollaron habilidades de un administrador para redes WAN como son la configuración, la capacidad de probar la conectividad de equipos de red y el monitoreo, por lo que se obtuvo un mayor conocimiento en redes avanzadas, con la intención de llegar a ser administradores de red en un ISP.

- Se desarrollaron habilidades de análisis y síntesis de la información durante el proceso de realización de esta tesis como:

  Trabajo en equipo

  Se obtuvieron buenos resultados ya que desarrollamos las habilidades como son el compromiso, ponerse de acuerdo, coordinación, cooperación, repartición de tareas, planificación, complementación de ideas, entre muchas otras, a fin de lograr nuestro objetivo en común, para esto fue necesario organizar nuestros tiempos.

  Capacidad de análisis y síntesis de la información

  Para la parte de resolución de problemas, nos surgieron algunos inconvenientes tanto en hardware como en software, ya que se presentaron en varias ocasiones durante la realización del proyecto de tesis, por lo que desarrollamos la capacidad de separar la información del problema en partes de un todo, hasta llegar a conocer los elementos fundamentales que lo conforman, con la finalidad de construir una idea precisa, lo que nos ayuda para nuestra vida personal y profesional.

  Habilidades de redacción

  Enfrentamos el reto de expresar idóneamente pensamientos e ideas en la escritura, lo que mejoró nuestros procesos sintácticos, léxicos y textuales.

6.1.1 LOGROS ADICIONALES

El paper titulado *Management of the Continental Advanced Networks Geant and AfricaConnect Joint as Two Autonomous Systems by BGP-4 Under IPv6: Using Limited Resources,* fue aceptado por el Comité de Revisores de Comunicaciones del ETCM 2021, el cuál se publicó en octubre del 2021 por la IEEE (ver apéndice G).

Le agradecemos este logro a nuestro director M. en C. José Ignacio Castillo Velázquez por haber promovido esta tesis y llevarla a un mayor nivel, como lo es este artículo, que ahora se vuelve un documento importante para nuestra carrera profesional.

APÉNDICE A: ¿Qué es GNS3?

Antes de que existiera la virtualización, los ingenieros de redes, administradores y estudiantes tenían que construir laboratorios con hardware físico o alquilar tiempo en un rack. Ambas opciones pueden ser costosas e inconvenientes y limitan los diseños de red disponibles. Ahora, Graphical Network Simulator-3 (GNS3), permite personalizar sus laboratorios de red para satisfacer exactamente sus necesidades, crear proyectos ilimitados usando Cisco y tecnología que no sea de Cisco.

La primera versión de GNS3 se liberó en 2008 y para la versión más estable y gráfica se desarrolló en el año 2011. GNS3 permite características de emulador, ya que cuenta con Dynamips y Quick Emulator como motores de virtualización, a diferencia de un simulador que está limitado en aproximaciones a gran escala y no cuenta con equipos core o backbone. Por lo que GNS3 es considerado un Emulador.

La interfaz gráfica de GNS3 le permite crear laboratorios de red virtualizados con una variedad de routers, switches y computadoras, pero realmente destaca cuando se combina con Cisco IOS. En cuanto a la emulación de routers necesita gran cantidad de recursos de procesamiento y memoria. En muchos casos, el hardware de la computadora no puede cumplir con estos requisitos. GNS3 ofrece la posibilidad de configurar hipervisores externos para delegar esta carga de trabajo.

GNS3 no se limita a imitar los comandos o funciones de Cisco IOS. En su lugar, utiliza una aplicación de hipervisor externo que es una instancia de Dynamips, el cual es un emulador de IOS de quipos Cisco que ejecuta un archivo de imagen IOS real, en su PC. Todos los comandos de configuración provienen de un IOS real y, en teoría, cualquier protocolo o característica que admita una versión de IOS está disponible para usar en sus diseños de red. Esta funcionalidad distingue a GNS3 de programas como RouterSim, Boson NetSim o Virtual Internet Routing Lab (VIRL), que simulan solo entornos, comandos y escenarios limitados con los que trabajar. GNS3 además de poder emular equipos de redes de datos, puede integrar QEMU y máquinas virtuales con VMware Fusion, que ejecutan sistemas operativos como Linux, Windows o Mac.

La virtualización, también requiere una gran cantidad de recursos informáticos. La distribución de esta carga de trabajo requiere que GNS3 se pueda comunicar con una instancia de Vmware Fusion corriendo en la computadora física [51, 52, 53].

APÉNDICE B: Instalación del software VMware Fusion para Mac.

VMware Fusion, permite ejecutar más de 200 sistemas operativos como máquinas virtuales seguras, entre los sistemas operativos que puede utilizar, se incluyen Windows, Linux y MacOS; Fusion asigna los recursos del hardware físico a los recursos de la máquina virtual para que cada máquina virtual tenga su propio procesador, memoria, discos, dispositivos de E/S, etc. Después de instalar Fusion y crear una máquina virtual, puede instalar y ejecutar sistemas operativos completos y sin modificar, así como software de aplicaciones asociadas en la máquina virtual, de la misma forma que en un PC físico.

Para instalar, se ingresa a la página:
https://www.vmware.com/mx/products/fusion/fusionevaluation.html para descargar la versión 11.5.5 para MacOS de VMware Fusión
a. Fusion se instala de la misma forma que otras aplicaciones de Mac OS.

Procedimiento

1. Haga doble clic en el archivo Fusion .dmg para abrirlo.
2. El contenido de la imagen de disco aparece en la ventana de Finder Fusion.
3. En la ventana de Finder, arrastre el icono de VMware Fusion hasta el icono de la carpeta Aplicaciones.
4. Cuando se indique, introduzca el nombre de usuario y la contraseña de su administrador. Fusion está instalado en la carpeta Aplicaciones de su Mac.
5. Finalmente utilizar VMware Fusion.

APÉNDICE C: Direcciones de red IPv6 que se utilizaron para la topología AficaConnect2.

Red	Dirección de red IPv6	Routers asociados AFRICACONNECT	Dirección IPv6 de Routers asociados	Router ID
11	2031: :/64	NEGERIA	2031::2/64	12.12.12.12
		BENIN	2031::1/64	11.11.11.11
12	2030: :/64	CAMERUN	2030::1/64	13.13.13.13
		NIGERIA	2030::2/64	12.12.12.12
13	2029: :/64	GABON	2029::2/64	14.14.14.14
		CAMERUN	2029::1/64	13.13.13.13
14	2011: :/64	CONGO	2011::2/64	15.15.15.15
		SUDAN	2011::1/64	3.3.3.3
15	2028: :/64	NAMIBIA	2028::2/64	16.16.16.16
		GABON	2028::1/64	14.14.14.14
16	2026: :/64	ZAMBIA	2026::2/64	17.17.17.17
		CONGO	2026::1/64	15.15.15.15
17	2014: :/64	BURUNDI	2014::1/64	18.18.18.18
		RWANDA	2014::2/64	19.19.19.19
18	2013: :/64	RWANDA	2013::2/64	19.19.19.19
		UGANDA	2013::1/64	20.20.20.20
19	2010: :/64	UGANDA	2010::2/64	20.20.20.20
		SUDAN	2010::1/64	3.3.3.3
20	2009: :/64	SUDAN	2009::1/64	3.3.3.3
		ETHIOPIA	2009::2/64	21.21.21.21

Tabla 1. Direcciones para los routers asociados a la red AfricaConnect2, parte 2-3.

Red	Dirección de red IPv6	Routers asociados AFRICACONNECT	Dirección IPv6 de routers asociados	Router ID
21	2019: :/64	ETHIOPIA	2019::1/64	21.21.21.21
		SOMALIA	2019::2/64	22.22.22.22
22	2020: :/64	SOMALIA	2020::1/64	22.22.22.22
		MADAGASTAR	2020::2/64	28.28.28.28
23	2021: :/64	MADAGASTAR	2021::1/64	28.28.28.28
		MOZAMBIQUE	2021::2/64	27.27.27.27
24	2022: :/64	MOZAMBIQUE	2022::1/64	27.27.27.27
		SUDAFRICA	2022::2/64	25.25.25.25
25	2023: :/64	SUDAFRICA	2023::2/64	25.25.25.25
		NAMIBIA	2023::1/64	16.16.16.16
26	2018: :/64	TAZANIA	2018::2/64	24.24.24.24
		KENIA	2018::1/64	23.23.23.23
27	2017: :/64	KENIA	2017::2/64	23.23.23.23
		SOMALIA	2017::1/64	22.22.22.22
28	2007: :/64	EGIPTO	2007::1/64	2.2.2.2
		SUDAN	2007::2/64	3.3.3.3

Tabla 2. Direcciones para los routers asociados a la red AfricaConect2, parte 3-3.

APÉNDICE D: Direcciones de red IPv6 que se utilizaron para la topología Geant.

Red	Dirección de red IPv6	routers asociados GÉANT	Dirección IPv6 de routers asociados	router ID
11	2064: :/64	ESTONIA	2064::1/64	34.34.34.34
		LATVIA	2064::2/64	35.35.35.35
12	2123: :/64	LATVIA	2123::1/64	35.35.35.35
		LITU	2123::2/64	36.36.36.36
13	21124: :/64	LITU	21124::1/64	36.36.36.36
		POLONIA	21124::2/64	37.37.37.37
14	2065: :/64	POLONIA	2065::1/64	37.37.37.37
		BELARUS	2065::2/64	43.43.43.43
15	2061: :/64	POLONIA	2061::2/64	37.37.37.37
		ALEMANIA_DE1	2061::1/64	44.44.44.44
16	2066: :/64	ALEMANIA_DE1	2066::1/64	44.44.44.44
		CZ	2066::2/64	46.46.46.46
17	2071: :/64	CZ	2071::1/64	46.46.46.46
		HUNGRIA2	2071::2/64	66.66.66.66
18	2105: :/64	HUNGRIA2	2105::1/64	66.66.66.66
		RS_SERBIA	2105::2/64	70.70.70.70
19	2106: :/64	HUNGRIA2	2106::1/64	66.66.66.66
		ME_MONTENE	2106::2/64	69.69.69.69
20	2101: :/64	HUNGRIA2	2101::1/64	66.66.66.66
		HUNGRIA	2101::2/64	52.52.52.52

Tabla 3. Direcciones asociadas a la red Geant, parte 2-5.

Red	Dirección de red IPv6	routers asociados GÉANT	Dirección IPv6 de routers asociados	router ID
21	2114: :/64	BULGARIA	2114::2/64	76.76.76.76
		RO_RUMANIA	2114::1/64	73.73.73.73
22	2104: :/64	RO_RUMANIA	2104::1/64	73.73.73.73
		HUNGRIA2	2104::2/64	66.66.66.66
23	2113: :/64	BULGARIA	2113::1/64	76.76.76.76
		MK_MACE	2113::2/64	74.74.74.74
24	2103: :/64	TURQUIA	2103::1/64	71.71.71.71
		HUNGRIA	2103::2/64	52.52.52.52
25	2115: :/64	MOLDAVIA	2115::2/64	72.72.72.72
		RO_RUMANIA	2115::1/64	73.73.73.73
26	2067: :/64	AZERBAJAN	2067::2/64	77.77.77.77
		ALEMANIA_DE1	2067::1/64	44.44.44.44
27	2095: :/64	ARME	2095::1/64	78.78.78.78
		HUNGRIA	2095::2/64	52.52.52.52
28	2099: :/64	HUNGRIA	2099::1/64	52.52.52.52
		SAN-MAR	2099::2/64	68.68.68.68
29	2116: :/64	GEORGIA	2116::1/64	51.51.51.51
		HUNGRIA	2116::2/64	52.52.52.52
30	2111: :/64	UA_UCRA	2111::1/64	50.50.50.50
		AUSTRIA2	2111::2/64	58.58.58.58

Tabla 4. Direcciones asociadas a la red Geant, parte 3-5.

Red	Dirección de red IPv6	routers asociados GÉANT	Dirección IPv6 de routers asociados	router ID
31	2070: :/64	AUSTRIA2	2070::2/64	58.58.58.58
		CZ	2070::1/64	46.46.46.46
32	2091: :/64	MALTA	2091::2/64	61.61.61.61
		ITALIA	2091::1/64	60.60.60.60
33	2090: :/64	ITALIA	2090::1/64	60.60.60.60
		ALBANIA	2090::2/64	62.62.62.62
34	2109: :/64	SK_ESLOVA	2109::1/64	67.67.67.67
		AUSTRIA2	2109::2/64	58.58.58.58
35	2087: :/64	ITALIA	2087::2/64	60.60.60.60
		FRANCIA2	2087::1/64	57.57.57.57
36	2089: :/64	GRECIA	2089::2/64	64.64.64.64
		ITALIA	2089::1/64	60.60.60.60
37	2098: :/64	GRECIA	2098::1/64	64.64.64.64
		CYPRUS	2098::2/64	75.75.75.75
38	2100: :/64	HR_HERZE	2100::2/64	55.55.55.55
		HUNGRIA	2100::1/64	52.52.52.52
39	2080: :/64	SAN_MAR	2080::1/64	68.68.68.68
		AUSTRIA	2080::2/64	53.53.53.53
40	2077: :/64	AUSTRIA	2077::2/64	53.53.53.53
		ALEMANIA_DE2	2077::1/64	47.47.47.47

Tabla 5. Direcciones asociadas a la red Geant, parte 4-5.

Red	Dirección de red IPv6	routers asociados GÉANT	Dirección IPv6 de routers asociados	router ID
41	2125: :/64	ISRAEL	2125::2/64	63.63.63.63
		INGLATERRA2	2125::1/64	49.49.49.49
42	2074: :/64	INGLATERRA2	2074::1/64	49.49.49.49
		FRAN1	2074::2/64	54.54.54.54
43	2075: :/64	FRAN1	2075::2/64	54.54.54.54
		LIECH	2075::1/64	48.48.48.48
44	2076: :/64	LIECH	2076::1/64	48.48.48.48
		FRANCIA2	2076::2/64	57.57.57.57
45	2084: :/64	FRANCIA2	2084::1/64	57.57.57.57
		ESPA	2084::2/64	56.56.56.56
46	2086: :/64	ESPA	2086::2/64	56.56.56.56
		PORTUGAL	2086::1/64	55.55.55.55
47	2052: :/64	PORTUGAL	2052::2/64	55.55.55.55
		INGLATERRA	2052::1/64	40.40.40.40
48	2093: :/64	ALEM_DE3	2093::2/64	59.59.59.59
		ALEM_DE2	2093::1/64	47.47.47.47
49	2060: :/64	ALEM_DE2	2060::2/64	47.47.47.47
		LUX	2060::1/64	45.45.45.45
50	2058: :/64	LUX	2058::2/64	45.45.45.45
		N_INGLA	2058::1/64	39.39.39.39

Tabla 6. Direcciones asociadas a la red Geant, parte 5-5.

APÉNDICE E: Monitoreo de la gestión de la red mediante la variable SysName para todos los routers de la topología AfricaConnect2-Geant.

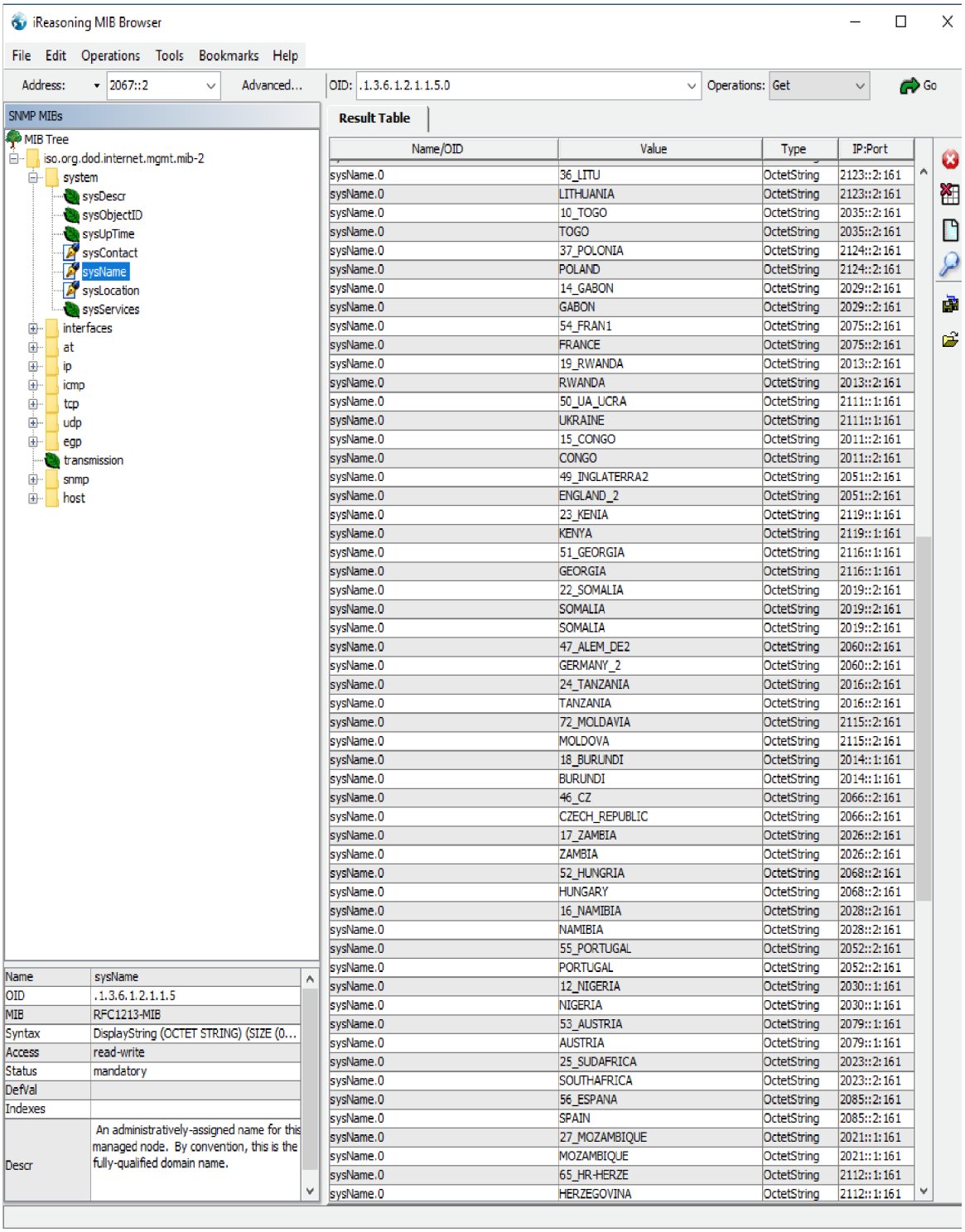


Figura 1. Monitoreo de la variable sysName para los 78 routers, parte 2/3

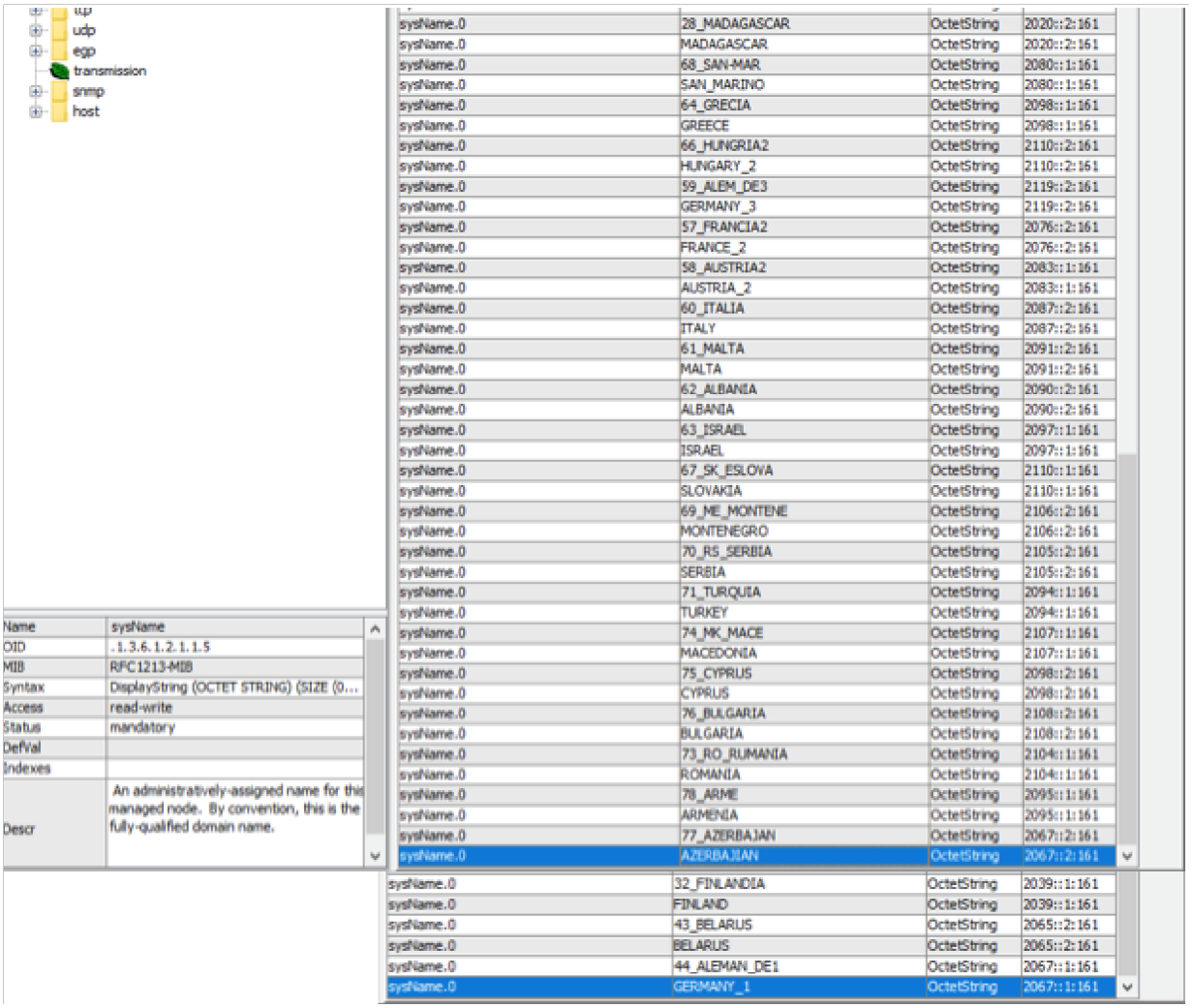


Figura 2. Monitoreo de la variable sysName para los 78 routers, parte 3/3

APÉNDICE F: Resultado del protocolo de enrutamiento dinámico OSPF para rutas internas y rutas externas aprendidas mediante OSPF vía BGP en los routers Marruecos y Estonia.

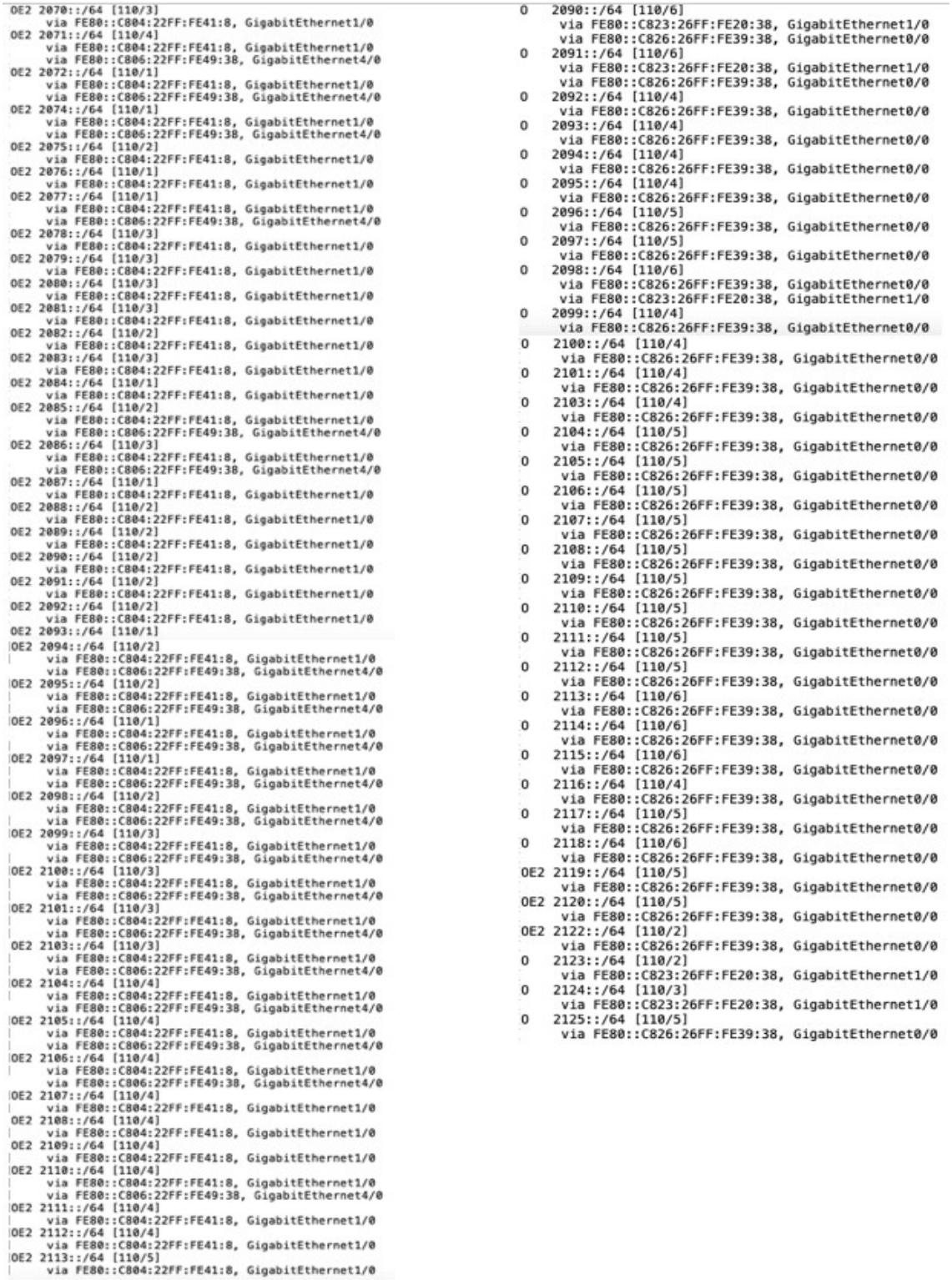


Figura 3. Tablas de enrutamiento Marruecos y Estonia para el protocolo de ruteo IGP parte 3/4.

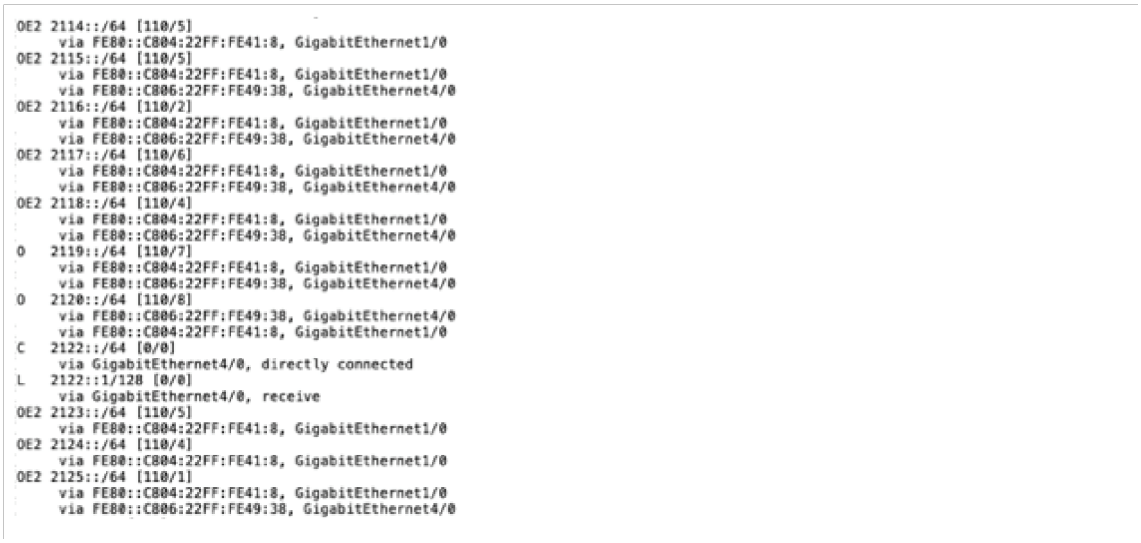


Figura 4.Tablas de enrutamiento Marruecos y Estonia para el protocolo de ruteo IGP parte 4/4.

APÉNDICE G: Resultado del protocolo de enrutamiento dinámico BGP para rutas externas y su redistribución de los routers Argelia y Francia2.

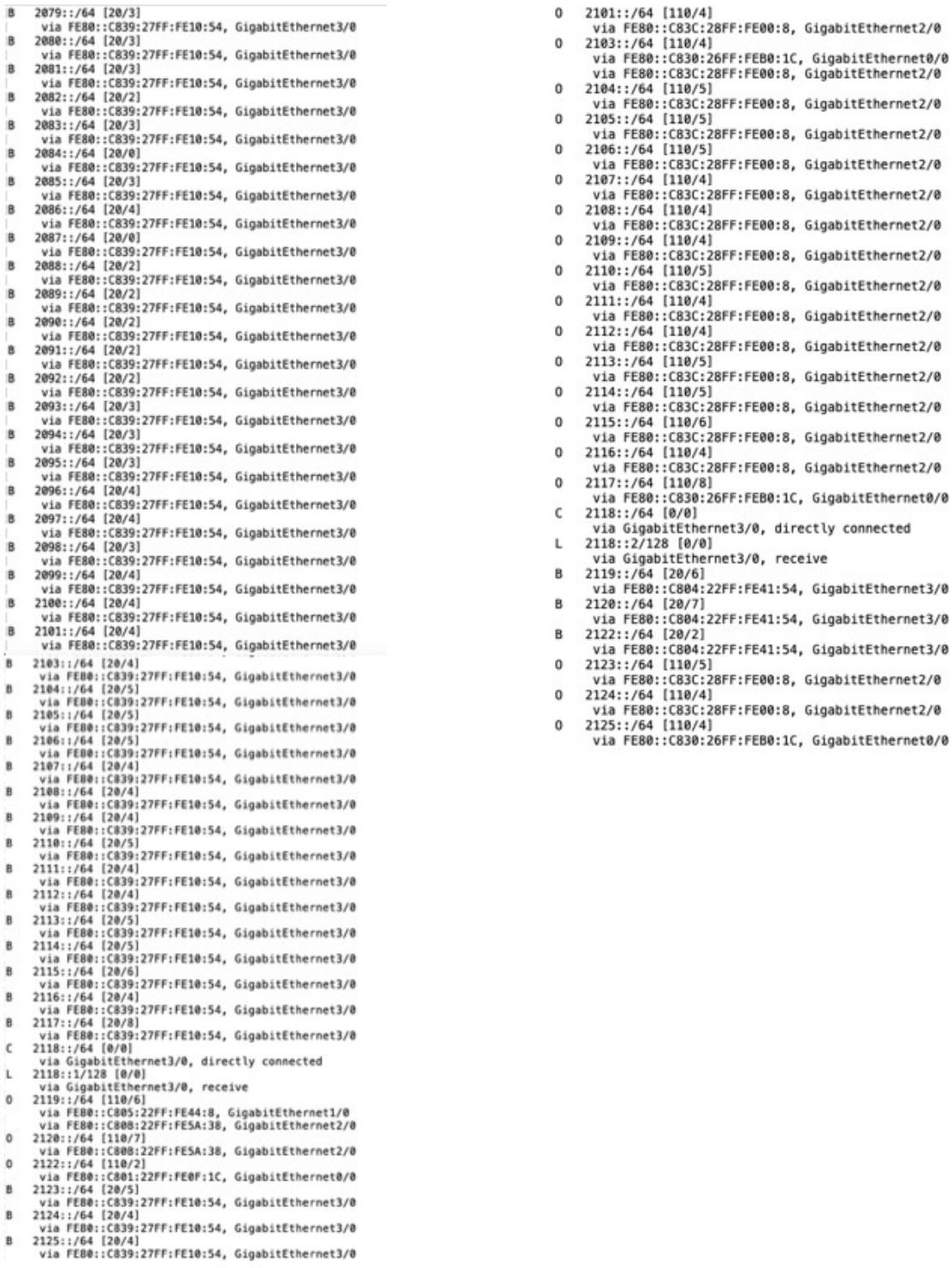


Figura 5. Tabla de enrutamiento Argelia y Francia2 para el protocolo de ruteo EGP parte 3/3.

APÉNDICE H: Verificación de la tabla BGP IPv6 para el router Argelia.

*>	2045::/64	2118::2	5	0 2 ?
*>	2046::/64	2118::2	5	0 2 ?
*>	2047::/64	2118::2	5	0 2 ?
*>	2048::/64	2118::2	5	0 2 ?
*>	2049::/64	2118::2	6	0 2 ?
*>	2050::/64	2118::2	5	0 2 ?
*>	2051::/64	2118::2	4	0 2 ?
*>	2052::/64	2118::2	5	0 2 ?
*>	2053::/64	2118::2	5	0 2 ?
*>	2054::/64	2118::2	5	0 2 ?
*>	2055::/64	2118::2	5	0 2 ?
*>	2056::/64	2118::2	4	0 2 ?
*>	2057::/64	2118::2	4	0 2 ?
*>	2058::/64	2118::2	4	0 2 ?
*>	2059::/64	2118::2	5	0 2 ?
*>	2060::/64	2118::2	3	0 2 ?
*>	2061::/64	2118::2	4	0 2 ?
*>	2062::/64	2118::2	4	0 2 ?
*>	2064::/64	2118::2	6	0 2 ?
*>	2065::/64	2118::2	4	0 2 ?
*>	2066::/64	2118::2	4	0 2 ?
*>	2067::/64	2118::2	4	0 2 ?
*>	2068::/64	2118::2	4	0 2 ?
*>	2069::/64	2118::2	3	0 2 ?
*>	2070::/64	2118::2	3	0 2 ?
*>	2071::/64	2118::2	5	0 2 ?
*>	2072::/64	2118::2	4	0 2 ?
*>	2074::/64	2118::2	3	0 2 ?
*>	2075::/64	2118::2	2	0 2 ?
*>	2076::/64	2118::2	0	0 2 i
*>	2077::/64	2118::2	3	0 2 ?
*>	2078::/64	2118::2	3	0 2 ?
*>	2079::/64	2118::2	3	0 2 ?
*>	2080::/64	2118::2	3	0 2 ?
*>	2081::/64	2118::2	3	0 2 ?
*>	2082::/64	2118::2	2	0 2 ?
*>	2083::/64	2118::2	3	0 2 ?
*>	2084::/64	2118::2	0	0 2 i
*>	2085::/64	2118::2	3	0 2 ?
*>	2086::/64	2118::2	4	0 2 ?
*>	2087::/64	2118::2	0	0 2 i
*>	2088::/64	2118::2	2	0 2 ?
*>	2089::/64	2118::2	2	0 2 ?
*>	2090::/64	2118::2	2	0 2 ?
*>	2091::/64	2118::2	2	0 2 ?
*>	2092::/64	2118::2	2	0 2 ?
*>	2093::/64	2118::2	3	0 2 ?
*>	2094::/64	2118::2	3	0 2 ?
*>	2095::/64	2118::2	3	0 2 ?
*>	2096::/64	2118::2	4	0 2 ?
*>	2097::/64	2118::2	4	0 2 ?
*>	2098::/64	2118::2	3	0 2 ?
*>	2099::/64	2118::2	4	0 2 ?
*>	2100::/64	2118::2	4	0 2 ?
*>	2101::/64	2118::2	4	0 2 ?
*>	2103::/64	2118::2	4	0 2 ?
*>	2104::/64	2118::2	5	0 2 ?
*>	2105::/64	2118::2	5	0 2 ?
*>	2106::/64	2118::2	5	0 2 ?
*>	2107::/64	2118::2	4	0 2 ?
*>	2108::/64	2118::2	4	0 2 ?
*>	2109::/64	2118::2	4	0 2 ?
*>	2110::/64	2118::2	5	0 2 ?
*>	2111::/64	2118::2	4	0 2 ?
*>	2112::/64	2118::2	4	0 2 ?
*>	2113::/64	2118::2	5	0 2 ?
*>	2114::/64	2118::2	5	0 2 ?
*>	2115::/64	2118::2	6	0 2 ?
*>	2116::/64	2118::2	4	0 2 ?
*>	2117::/64	2118::2	8	0 2 ?
*>	2119::/64	::	6	32768 ?
*>	2120::/64	::	7	32768 ?
*>	2122::/64	::	2	32768 ?
*>	2123::/64	2118::2	5	0 2 ?
*>	2124::/64	2118::2	4	0 2 ?
*>	2125::/64	2118::2	4	0 2 ?

Figura 6. Verificación de la tabla BGP IPv6, parte 2/2

APÉNDICE G: Paper accepted by the Reviewers Committee Communications of the ETCM 2021 and Publication.

José Ignacio Castillo Velázquez <ignacio.castillo@uacm.edu.mx>

ETCM 2021 notification for paper 43

ETCM 2021 <etcm2021@easychair.org> 16 de agosto de 2021, 17:05
Para: Jose-Ignacio Castillo-Velazquez <ignacio.castillo@uacm.edu.mx>

Dear Jose-Ignacio Castillo-Velazquez,

We are pleased to inform you that your paper No. 43, title "Management of the Continental Advanced Networks GEANT and AFRICACONNECT Joint as Two Autonomous Systems by BGP-4 Under IPv6: Using Limited Resources" has been accepted by the Reviewers Committee Communications of the ETCM 2021. The Committee informs you that before 30 August 2021, you should make the changes suggested by the reviewers.

In a few days, we will send Camera-Ready instructions: how to use the PDF-Express tool, where you have to upload the approved version, and how to transfer copyright to IEEE.

With Warmest Regards

Mónica Karel Huerta
Technical Program Chair
mhuerta@ieee.org

SUBMISSION: 43
TITLE: Management of the Continental Advanced Networks GEANT and AFRICACONNECT Joint as Two Autonomous Systems by BGP-4 Under IPv6: Using Limited Resources

Figura 7. Aceptación Paper.

Figura 8. Publicación del paper en IEEE.

REFERENCIAS

[1] F. Michael, “The Role and Status of National Research and Education Networks (NRENs) in Africa” de WORLD BANK EDUCATION, TECHNOLOGY & INNOVATION SABER-ICT Technical Paper Series, EEUU, 2016.

[2] AfricaConnect2, “AfricaConnect2.net” AfricaConnect2, 24 Mayo 2018. [En línea]. Available:https://www.AfricaConnect2.net/Users/Case_studies/Pages/TERNET_leaps_barriers.asp x. [Último acceso: 18 Marzo 2021].

[3] R. d. I. y. E. d. Á. O. y. Central, “wacren.net” wacren, 2018. [En línea]. Available: https://wacren.net/en/news/wacren-forges-strategic-partnerships-support-women-ict. [Último acceso: 18 Marzo 2021].

[4] AfricaConnect2, “inthefieldstories.net” in THE FIELD, junio 2016. [En línea]. Available: https://www.inthefieldstories.net/helping-to-map-soil-resources-in-zambia/. [Último acceso: 18 marzo 2021].

[5] Geant, “geant.org” Geant, [En línea]. Available: https://www.geant.org/People/research_communities/Pages/Particle_physics.aspx. [Último acceso: 2021 marzo 20].

[6] Geant, “geant.org” Geant, [En línea]. Available: https://www.geant.org/People/research_communities/Pages/Space.aspx. [Último acceso: 2021 Marzo 20].

[7] Geant, “geant.org” Geant, [En línea]. Available: https://www.geant.org/People/research_communities/Pages/Health_and_medicine.aspx. [Último acceso: 2021 marzo 20].

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

[9] 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 37_{th} Central America and Panama Convention (CONCAPAN XXXVII), 2017, pp. 1-4, doi: 10.1109/CONCAPAN.2017.8278476.

[10] 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), 2017, pp. 1-4, doi: 10.1109/SENSET.2017.8125029XXXVII), 2017, pp. 1-4, doi: 10.1109/CONCAPAN.2017.8278476.

[11] 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), 2018, pp. 1-6, doi: 10.1109/CONCAPAN.2018.8596667.

[12] J. -I. Castillo-Velazquez and M. -I. Trigueros-Galicia, "UTILCON 1.0: A Conference Management System trainer in Spanish with strict refereeing control," 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON), 2019, pp. 1-4, doi: 10.1109/INTERCON.2019.8853831.

[13] 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), 2019, pp. 1-6, doi: 10.1109/CONCAPANXXXIX47272.2019.8976946.

[14] J. Castillo-Velazquez, M. A. Garcia and D. J. S. Martinez, "Hardening as a best practice for WLAN Security Meanwhile WPA3 is released," 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX), 2019, pp. 1-5, doi: 10.1109/CONCAPANXXXIX47272.2019.8977073.

[15] J. -I. Castillo-Velazquez and A. Delgado-Villegas, "GNS3 Limitations when Emulating Connectivity and Management for Backbone Networks: A Case Study of CANARIE," 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2020, pp. 1-4, doi: 10.1109/CCECE47787.2020.9255741.

[16] 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), 2018, pp. 1-4, doi: 10.1109/INTERCON.2018.8526390.

[17] J. -I. Castillo-Velazquez and L. -C. Revilla-Melo, "Management Emulation of Advanced Network Backbones in Africa: 2019 Topology," 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2020, pp. 1-4, doi: 10.1109/CCECE47787.2020.9255779.

[18] J. -I. Castillo-Velazquez, I. Muñoz-Martínez, J. -A. Díaz-Ramírez and E. F. Ordoñez-Morales, "Management Emulation for Geant Advanced Network: 2020 Topology under IPv6," 2020 IEEE ANDESCON, 2020, pp. 1-6, doi: 10.1109/ANDESCON50619.2020.9271972.

[19] J. I. Castillo, Redes de datos: Contexto y evolución, México: SAMSARA, 2019.

[20] J. I. Castillo, Redes de datos: Contexto y evolución, México: SAMSARA, 2016.

[21] I. A. R. Vidal, "Redes Académicas de Educación e Investigación", México, 2019.

[22] C. T. M. G. COMMUNITY, "connect.geant.org" [En línea]. Available: https://connect.geant.org/wp-content/uploads/2020/06/CONNECT-34-Web-PDF.pdf. [Último acceso: 8 DIC 2020].

[23] AfricaConnect2, "AfricaConnect2.net" [En línea]. Available: https://www.AfricaConnect2.net/Pages/Home.aspx. [Último acceso: 10 DIC 2020].

[24] AfricaConect2, "AfricaConnect2.net" [En línea]. Available: https://www.AfricaConnect2.net/Networks/Pages/Home.aspx. [Último acceso: 10 DIC 2020].

[25] Geant, "geant.org" [En línea]. Available: https://www.geant.org/Projects/Geant_Project_GN4-1/Pages/GN41_Supporting_Horizon_2020.aspx. [Último acceso: 11 DIC 2020].

[26] Geant, "geant.org" [En línea]. Available: https://www.geant.org/Projects/Geant_Project_GN4-2/Pages/European_success_story.aspx. [Último acceso: 11 DIC 2020].

[27] Geant, "geant.org" [En línea]. Available: https://www.geant.org/Resources/#maps. [Último acceso: 12 DIC 2020].

[28] W. Stallings, Comunicaciones y redes de Computadoras 7a Edición, Madrid: PEARSON, 2004.

[29] G. Scott, "Guide for Internet Standards Writers" de RFC 2460, June, 1998.

[30] S. D. R. Hinden, “IP Version 6 Addressing Architecture” de RFC 2373, July, 1998.

[31] J. Moy, “OSPF Version 2” de RFC 2328, April,1998.

[32] D. F. J. M. R. Coltun, “OSPF for IPv6” de RFC 5340, July 2008.

[33] J. I. Castillo, Switching & Routing: Introducción, México: SAMSARA, 2016.

[34] R. CISCO, Curso práctico de formación para la certificación CCNA, México: ALFAOMEGA, 2018.

[35] HUAWEI, “What Is OSPF and How Is It Configured?” [En línea]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100082074. [Último acceso: 17

[36] Y. R. K. Lougheed, “A Border Gateway Protocol 3 (BGP-3)” de RFC 1267, October 1991.

[37] S. H. Y. Rekhter, A Border Gateway Protocol 4 (BGP-4), RFC 4271, January 2006.

[38] J. C. K. M. M. R. R. Presuhn, “Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)” de RFC 3416, December 2002.

[39] D. L. S. R. B. W. R. Frye, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework” de RFC 3584, August 2003.

[40] M. F. J. Case. J. Davin, “Simple Network Management Protocol (SNMP)” de RFC 1157, May 1990.

[41] R. P. B. W. J. Case. D. Harrington, “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)” de RFC 3412, December 2002.

[42] J. I. Castillo, “El árbol de Internet y la estructura de información de gestión de una red”, IEEE Latin America and the Caribbean Newsletter, nº No.62ISSN: 2157-8354, pp. pp. 15-17, Abril de 2009.

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

[44] D. P. J. S. K. McCloghrie, “Structure of Management Information Version 2 (SMIv2)” de RFC 2578, April 1999.

[45] J. C. R. M. Partain, “Introduction to Version 3 of the Internet-standard Network Management Framework” de RFC 2570, April 1999.

[46] D.Harrington, “An Architecture for Describing SNMP Management Frameworks” de RFC 2571, EEUU, 1999.

[47] AFRICACONNECT2, “AfricaConnect2.net” [En línea]. Available: https://www.AfricaConnect2.net/Partners/Regional_Networking_organisations/Pages/Ho me.aspx. [Último acceso: 13 DIC 2020].

[48] Geant, “geant.org” [En línea]. Available: https://www.geant.org/Resources/Documents/Geant_at_the_Heart_of_Global_Research_and_Education_Networking_Oct_2019.pdf. [Último acceso: 14 DIC 2020].

[49] U. D. o. H. S. S. a. Technology, “ASRank” [En línea]. Available: https://asrank.caida.org/. [Último acceso: 25 FEBRERO 2021].

[50] K. M. M. R. R. Presuhn. J. Case, “Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)” de RFC 3416, December 2002.

[51] GNS3, 2021. https://www.gns3.com/

[52] Zhang, Y., Liang R., and Ma. H., Teaching Innovation in Computer Network Course for Undergraduated Students with Packet Tarcer, IERI Procedia, 2012.

[53] Julio. C. Turbay. A, “ACTAS TICAL” CCCI, Cartagena de Indias, Colombia, 2013.