Monitoreo en la red avanzada CLARA : Emulación

por Adrian Alberto Martínez Cárcamo

Fecha de entrega: 19-feb-2019 09:14a.m. (UTC-0800)
Identificador de la entrega: 1080330012
Nombre del archivo: nezCarcamo_ISET_Monitoreo_en_la_red_avanzada_CLARA_Emulaci_n.pdf (8.29M)
Total de palabras: 32207
Total de caracteres: 160240

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

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Monitoreo en la red avanzada CLARA: Emulación

TESIS

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A:

ADRIÁN ALBERTO MARTÍNEZ CÁRCAMO

DIRECTOR:

M. EN C. JOSÉ IGNACIO CASTILLO VELÁZQUEZ

Ciudad de México, agosto de 2018.

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

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Agradecimientos

*En primer lugar, a **Dios** por haberme dado la vida, por acompañarme y guiarme en todo momento, por su fidelidad a través de los años y sobre todas las cosas su amor y misericordia. Te agradezco por todo lo que has hecho y todo lo que harás.*

*A mis **padres** por haberme ayudado en esta larga travesía, por haber creído en mí y apoyarme en todas y cada una de mis decisiones. Por la posibilidad de tener una excelente educación y por ser un gran ejemplo en mi vida, gracias por aportarme los valores con los que hasta hoy he enfrentado la vida. Gracias por ayudarme a convertirme en la persona que soy ahora. Siempre están en mi mente*

*A mi **hermana** por darme la oportunidad de crecer a su lado y ser mejor día a día. Por apoyarme incondicionalmente, por su paciencia y oraciones.*

*A mi **abuela y familia** por siempre estar ahí cuando los necesito, por representar la unidad familiar y ser la base de mis comportamientos ante la sociedad. Por el apoyo moral, formativo, financiero, motivacional y espiritual. Les agradezco de corazón.*

*A **Yadira Aguirre Guzmán** por todo su apoyo y amor incondicional desde antes de iniciar esta carrera, por haberme adoptado como parte de su familia y darme lo mejor de su ser todo el tiempo. Por sus enseñanzas para el futuro.*

*A mi director de tesis **José Ignacio Castillo Velázquez** por sacar lo mejor de mí, por motivarme e inculcar el deseo de superación con cada una de sus conversaciones y enseñanzas, por ese ejemplo de mejora continua y superación día con día. Por ese cambio de perspectiva ante la vida con el cual me quedare para el futuro.*

*A mis **profesores** por aportarme el conocimiento el cual aplicare en mi vida laboral, por esas enseñanzas a través de mi vida estudiantil, gracias por su paciencia esfuerzo y dedicación que me mostraron durante todo este ciclo.*

*A la **Universidad Autónoma de la Ciudad de México** por permitirme terminar una carrera, por abrirme las puertas y hacerme parte de esta casa de estudios de la cual*

estoy muy orgulloso. Agradezco por el apoyo otorgado para la impresión y empastado del presente trabajo recepcional.

A mis **compañeros de carrera** “muéganos” por hacer que esta etapa sea muy divertida y muy relajada, gracias por su compañerismo, les deseo éxito en todo lo que emprendan.

A Paul, George, John y Ringo por ser una gran influencia en mi vida, por darme un mensaje en el cual siempre hay esperanza y amor, gracias por esa música que ha sido fuente de inspiración en mi vida.

Por ultimo a Adrian, gracias por ayudarme cuando lo he necesitado. Me ayudas más de lo que piensas que lo haces, espero que puedas llegar a saber lo agradecido que estoy contigo. Muchas gracias de nuevo.

"He peleado la buena batalla, he acabado la carrera, he guardado la fe." 2 Timoteo 4:7

"He peleado la buena batalla, he acabado la carrera, he guardado la fe." 2 Timoteo 4:7

”There are places I remember
All my life though some have changed
Some forever, not for better
Some have gone and some remain

All these places have their moments
With lovers and friends I still can recall
Some are dead and some are living
In my life I've loved them all”

In my life - The Beatles- Rubber Soul 1965

RESUMEN

La red avanzada CLARA es una red creada para la educación e investigación, tiene diversos tipos de aplicaciones, por ejemplo: nanotecnología, energías renovables, bibliotecas digitales, biotecnología, astronomía, ICT (Grids/Mallas computacionales), biodiversidad, entre otras. Dicha red tiene presencia en Latinoamérica interconectando 14 países, sus principales características son los enlaces de muy alta velocidad de entre los 300 Mbps a 100 Gbps, y los equipos de backbone de alta capacidad de enrutamiento. Debido a lo anterior se consideró hacer un estudio a detalle de la conectividad y gestión en la red CLARA por lo que se simuló en Packet Tracer y emuló en GNS3 la red en cuestión. Para ello, se configuraron los equipos correspondientes a la topología más reciente de 2017 con base en los protocolos OSPF y SNMP.

OSPF es un protocolo que permite comunicar routers que pertenezcan a diferentes áreas, por lo cual, es ideal para este tipo de redes en donde se tiene un dominio para backbone y diferentes dominios para las redes que se conectarán en un futuro.

Por otra parte SNMP tiene la función de informar los acontecimientos que pasan en los dispositivos de una red en tiempo y forma, por lo que es un protocolo fundamental en la gestión de cualquier red y por ende es tomado en cuenta en el presente estudio.

La simulación y emulación se realizó en una computadora de escritorio con sistema operativo Windows 7 Ultimate, con procesador AMD FX(tm)-6100 Six-Core Processor a 3.3 GHz y memoria RAM de 8.00 GB (7.50 GB utilizable). La simulación requirió del empleo del 6% de procesador y 36% de memoria; por su parte el emulador requirió de 71% del procesador y 88% de memoria.

Algunas de las limitantes de Packet Tracer es que no cuenta con IOS reales para los routers de Cisco por lo cual utiliza routers genéricos, análogamente SNMP está limitado y no es aprovechado como en las condiciones reales, mientras que GNS3 trabaja con IOS y modelos de routers originales, así como, con máquinas virtuales.

Este proyecto me permitió obtener las habilidades básicas para administrar y configurar la red avanzada CLARA con IOS reales, además de observar en tiempo real los paquetes que circulaban a través de la red y recibir notificaciones de eventos que sucedían en tiempo real.

PALABRAS CLAVES: Redes avanzadas, emulación, gestión, protocolos de enrutamiento, red CLARA.

Capítulo 1 Introducción a las redes de datos

La Internet o también conocida como la red de datos más grande del mundo es sin duda el invento más trascendental de nuestros tiempos ya que desde su creación se dio una revolución histórica en cuanto a la comunicación de la raza humana y esto provocó un cambio radical en el mundo entero. La Internet permite a millones de personas que se comuniquen ya sea por e-mail, mensajes, redes sociales, llamadas telefónicas en línea o video llamadas, es decir, permite que el mundo entero se conecte desde cualquier parte del mundo, de igual manera es parte fundamental en la investigación, en la educación y en los avances tecnológicos. Sin embargo, la Internet no apareció de la nada: es importante conocer sus inicios para saber hacia dónde se dirige y cómo orientarlo para el bien de la raza humana.

1.1 Los primeros años de las redes de datos

La primera idea detrás de las redes de datos la tuvo un profesor del MIT (Massachussets Institute of Technology) llamado Joseph Carl Robnett Licklider, quien en su trabajo pionero titulado "Man Computer Symbiosis" o "Simbiosis del hombre y la computadora" de 1960, decía que las computadoras deberían ser desarrolladas con el objetivo de permitir que los hombres y las computadoras cooperaran en la toma de decisiones y en el control de situaciones difíciles. En otras palabras, promovía una interacción directa entre el hombre y la computadora. Según Licklider las computadoras permitirían una mejor comunicación si había una conexión entre ellas siendo así más eficaces y como consecuencia se compartiría mejor la información entre la gente [1].

En Julio de 1961 en el MIT un estudiante graduado llamado Leonard Kleinrock publicó una tesis de doctorado sobre la teoría de conmutación de mensajes. Dicha teoría permitía hacer un uso eficiente en los enlaces físicos de una red ya que se establecía un intercambio de bloques de información con un tamaño específico entre dos puntos, es decir, un emisor y un receptor [2].

Años más tarde, en 1964 fue creada la primera red distribuida de comunicaciones por Paul Baran, la cual dividía la información en segmentos de 1024 bits y se podía conectar con diferentes nodos. Fue el inicio de la "conmutación de paquetes", el cual se convirtió en un método de envío de datos a través de una red [3].

En 1966 Robert Taylor de ARPA (Advanced Research Projects Agency) tuvo la necesidad de comunicar terminales tontas separadas para acceder a las computadoras desde centros de investigación diferentes, Taylor tuvo la idea de que una terminal tonta podía ser suficiente si todas las computadoras estuvieran en una red común; pensaba que no era bueno tener diferentes terminales tontas para comunicar diferentes computadoras, sino que era mejor una terminal que se pudiera comunicar con diferentes computadoras, como se muestra en la figura 1.1 [4].

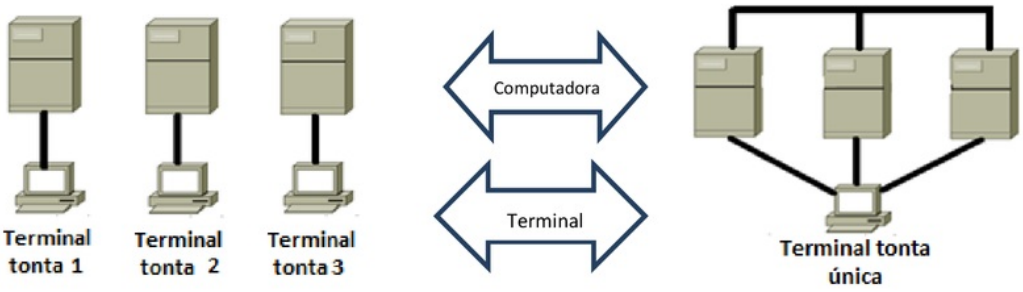


Figura 1.1. Idea de Robert Taylor previo a la creación de ARPANET. Diagrama propio con base en la referencia. [4]

Taylor consiguió financiamiento del gobierno para su proyecto y reclutó a Lawrence Roberts para hacer el trabajo, ya que Roberts había realizado la primera conexión experimental entre dos computadoras en el instituto de Massachusetts.

En 1969 se creó ARPANET, la cual estaba basada en computadoras de propósito especial llamados IMP (Interface Messagge Processor), mostrado en la figura 1.2. Los IMP eran nodos de conmutación de paquetes que se usaban para interconectar redes [5].

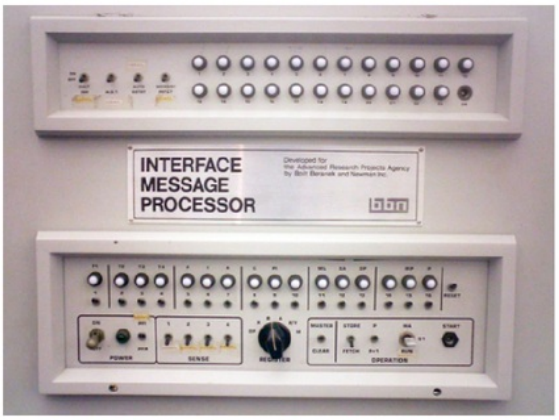


Figura 1.2 Interface Message Processor. Diagrama tomado de la referencia [6].

El plan para ARPANET era conectar a la red varios IMP idénticos en donde cada uno estaría unido a diferentes tipos de mainframes: Sigma 7 para UCLA (University of California, Los Angeles), SDC 940 para SRI (Stanford Research Institute), una IBM 360/75 para UCSB (University of California, Santa Barbara) y una PDP-10 en la Universidad de Utah; con esto se tenían los primeros cuatro nodos de ARPANET [7] [8]. Figura 1.3.

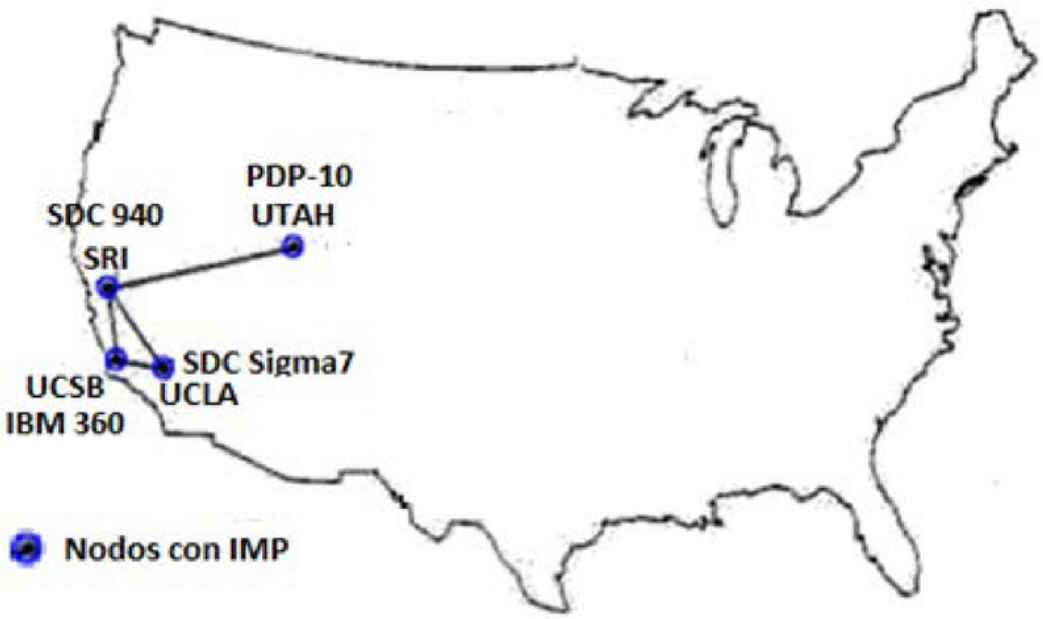


Figura 1.3 Primeros cuatro nodos de ARPANET en 1969. Diagrama propio con base en la referencia [9].

Durante los años siguientes las computadoras se añadieron rápidamente a la red de ARPANET. En diciembre de 1970 se finalizó el primer protocolo *host a host* de ARPANET llamado NCP (Network Control Program), el cual fue creado por el NWG (Network Working Group), utilizado hasta 1973 porque no tenía la capacidad para hacer frente a las redes y máquinas de la creciente ARPANET debido a que sólo conocía el IMP de destino. Por ello, se necesitaba hacer un cambio al protocolo dado que NCP no tenía un control de errores de extremo a extremo porque ARPANET era considerada la única red que existía y era tan confiable que ningún control de errores sería necesario por parte de los host.

En 1973 Robert Khan decidió desarrollar una nueva versión del protocolo, que conocería las necesidades de un entorno de red más allá de ARPANET. Khan le pidió a Vinton Cerf, quien era miembro del NWG, que trabajara con él en el diseño del protocolo TCP/IP (Transfer Control Protocol/ Internet Protocol), ya que Cerf estuvo involucrado en el diseño y en el desarrollo del original NCP. Con la ayuda de Cerf y el enfoque de las comunicaciones de Khan hicieron equipo para establecer los detalles de lo que se convertiría en el protocolo TCP/IP [10].

Cabe recalcar que para el año de 1977 ARPANET seguía creciendo llegando a 59 nodos en todo EUA, como se muestra en la figura 1.4, y así como los equipos de la red, incrementaba de igual manera el tráfico entre la misma [11].

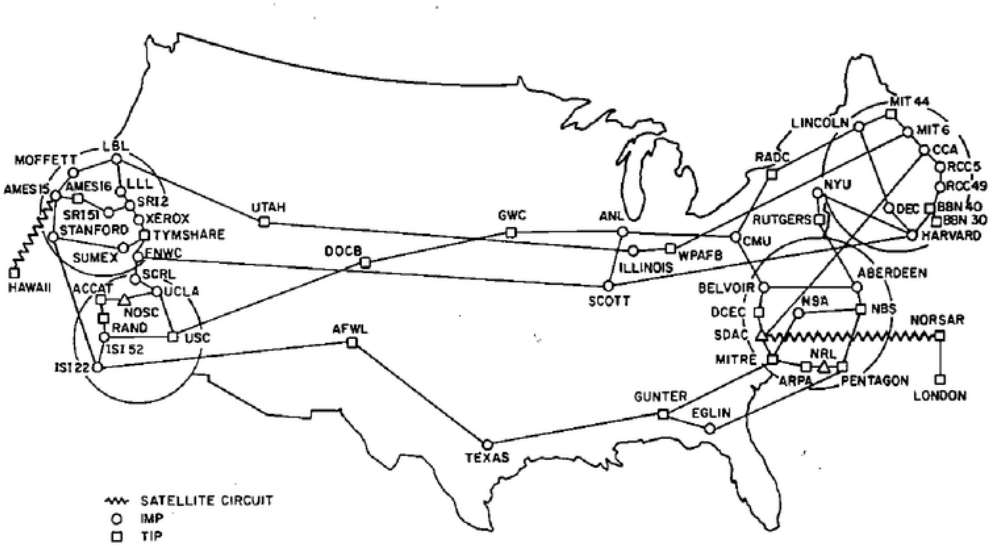


Figura 1.4 ARPANET en 1977. Diagrama propio con base en la referencia [9].

En 1978 TCP se dividió en dos componentes: uno fue el de TCP, que era un protocolo de *host* a *host,* y el IP que es un protocolo de interconexión que se encargaba de pasar paquetes individuales de *host a switch* o entre *switches* [11]. El protocolo TCP/IP permitía a las redes interconectarse, de manera que las computadoras en las redes que conocían el protocolo podían ser capaces de comunicarse a través de las redes mediante un gateway.

El gateway era un dispositivo que permitía tener comunicación de todas y cada una de las redes y podía encapsular paquetes provenientes de computadoras en paquetes que fueran a redes subyacentes [12].

En 1980 con la ayuda de la NSF (National Science Foundation) se creó la CSNET (Computer Science Network), cuyo propósito general era tener los beneficios de ARPANET para sus departamentos de ciencias de la computación e institutos de investigación que no podían conectarse directamente a ARPANET [13].

En 1983 TCP/IP fue adoptado como un estándar universal marcando un logro en el desarrollo de la Internet la cual se define como una red común con diferentes redes interconectadas y protocolos de comunicación iguales para todos los dispositivos [14].

En ese mismo año Robert Metcalfe desarrolló Ethernet: un estándar que implementa el protocolo de acceso al medio CSMA-CD (Carrier Sense Multiple Access- Colition Detected). CSMA-CD detecta las colisiones en un mismo canal de comunicación. Este protocolo junto con el estándar serían adoptados por las redes actuales.

1.2 Consolidación de las redes de datos

En 1985 la NSF quería replicar el éxito de la CSNET, es por ello que nació la NSFNET con el objetivo de conectar seis nodos: en San Diego el NCAR (National Center for Atmospheric Research), la Universidad de Illinois, la Universidad de Pittsburgh, el JVNC (John von Neumann Center) en Nueva Jersey, la Universidad de Cornell en Nueva York; concentrándolos en sus centros de supercomputadoras de grado académico para crear un backbone con la intención de conectarlos a ARPANET como se muestra en la figura 1.5 [3].

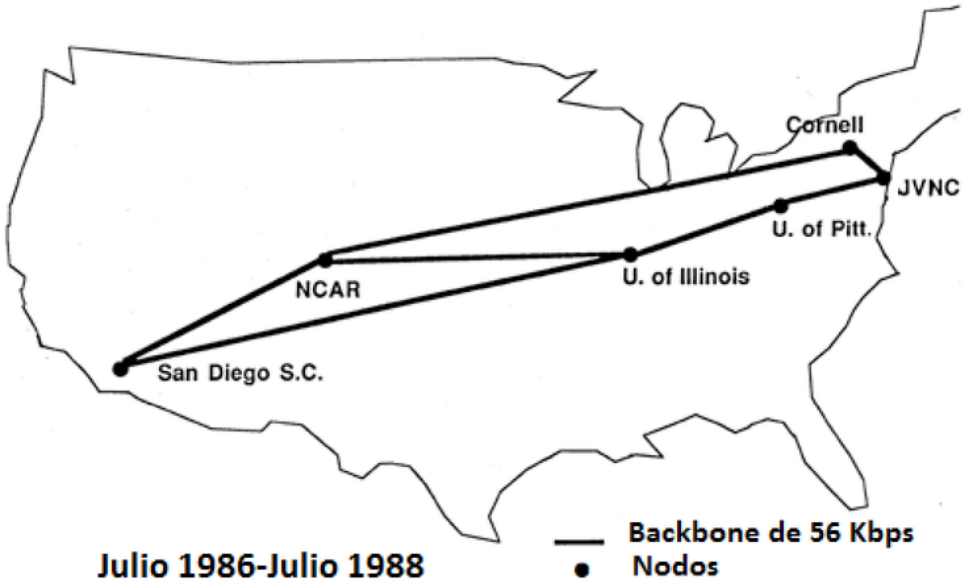


Figura 1.5 Backbone de la NSFNET. Diagrama con base en la referencia [9].

En 1987 la NSF implementó un backbone T-1 ideal para la transmisión digital de voz y datos a una velocidad de 1.544 Mbps como se muestra en la figura 1.6.

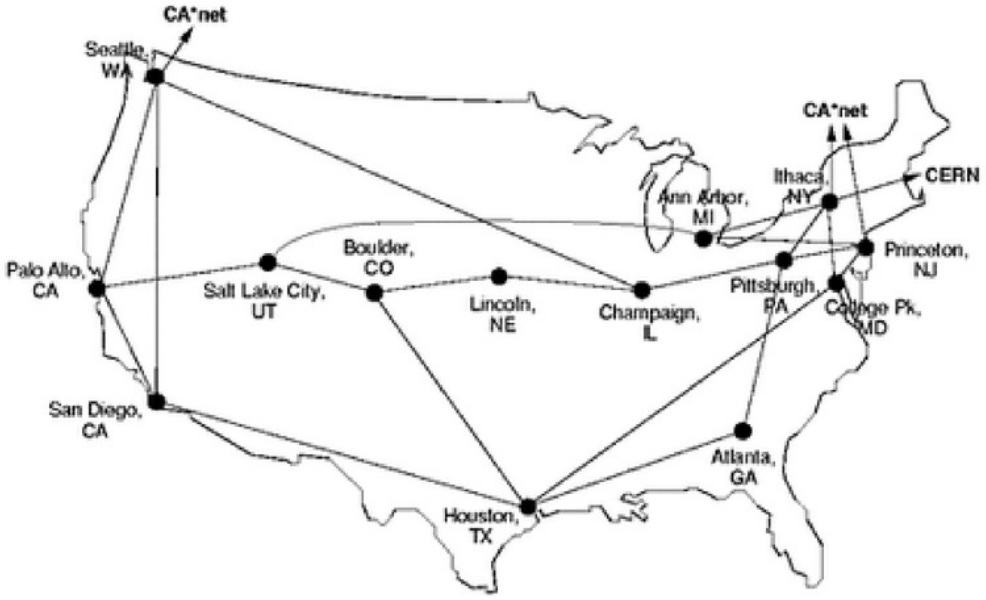


Figura 1.6 Backbone T-1 de la NSFNET en 1987. Diagrama con base en la referencia [9].

Dado que el proyecto crecía de manera exponencial, se decidió expandir la capacidad de la red y se aumentó la velocidad de transmisión a T-3 con capacidad de 44.77 Mbps, como se muestra en la figura 1.7.

Figura 1.7 Backbone T-3 de la NSFNET 1989. Diagrama con base en la referencia [9].

En 1990 ARPANET desapareció y la NSFNET tomó su lugar. Por ello, el desarrollo y el crecimiento se centraron en esta última. Ese mismo año, World Wide Web fue desarrollado por Tim Bernes Lee de la Organización Europea para la Investigación Nuclear o también conocida como CERN [15].

1.3 Inicio de la Internet comercial

En 1991 ya había 3 tipos de niveles de redes: el nivel de backbone, el nivel de distribución y el nivel de acceso. El nivel de backbone de la NSFNET, que estaba compuesto de varios AS (Autonomous Systems), conocido como *core*; el nivel de redes regionales, compuestas por un sólo AS, conocido como nivel de distribución, y el nivel de las redes de las universidades y centros de investigación, conocido como nivel de Acceso [11].

Análogamente la NSF extendió un plan para que el servicio de la Internet fuera tomado por los ISP (Internet Service Provider), quienes operarían sus propios backbones. Los suscriptores de los ISP conectarían sus computadoras a redes de área local a uno de estos backbones y permitirían la interconexión a través de sus sistemas hacia la Internet comercial.

En 1993 la NCSA (National Center for Supercomputing Applications) de la Universidad de Illinois lanzó la primera versión de un visor web llamado *Mosaic,* el cual era el primer *browser* que permitió la visualización de imágenes a color como parte de la página web. Para 1994 *Mosaic* era un éxito: ya lo habían descargado un millón de usuarios. La versión comercial de *Mosaic* se llamó Netscape y así se popularizó la Internet. Finalmente, en 1995 con el crecimiento exponencial de la Internet la NSFNET desapareció y dio paso a la Internet comercial tal y como lo conocemos ahora [16].

En 1995 la FNC (Federal Networking Council) aprobó por unanimidad una resolución oficial para definir el término Internet, la cual decía lo siguiente [17]:

> "Internet" se refiere al sistema de información global que:
>
> (i) Está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de Internet (IP) o en sus extensiones;
>
> (ii) Es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP y
>
> (iii) Emplea, provee, o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas descritas por la FNC

1.4 Redes avanzadas

Este capítulo se centra en definir e identificar las redes avanzadas correspondientes al continente americano así como las diferencias concernientes a capacidad de cada una de ellas, particularmente en la red CLARA (Consorcio Latinoamericano de Redes Avanzadas) para un análisis más detallado de la misma ya que a esta se enfoca este documento, sin embargo, también se establece una breve revisión de las otras redes avanzadas en el continente americano.

Una red avanzada es una red de alta velocidad que permite a científicos, investigadores, académicos, profesores y estudiantes colaborar al compartir información y herramientas mediante una serie de interconexiones de redes [18]. A diferencia de la Internet comercial, estas redes forman un área reservada única y exclusivamente para las comunidades de educación e investigación. Las redes avanzadas sirven para dos propósitos fundamentales:

1) Apoyar el trabajo de investigadores y académicos mediante la provisión de una infraestructura de comunicación de datos de gran capacidad (ancho de banda), lo que permite la rápida transferencia de grandes cantidades de datos, y
2) Ser una poderosa herramienta de investigación al proveer una plataforma sobre la que investigadores e innovadores pueden desarrollar y probar nuevos servicios y tecnologías de red.

1.4.1 Redes Avanzadas en el continente americano

Las redes avanzadas en el continente americano que se abordarán en el presente capítulo son las siguientes:

Red avanzada	País o división geográfica
CANARIE (Canadian Network for the Advancement of Research, Industry and Education)	CANADA
Internet2	ESTADOS UNIDOS DE AMÉRICA
CLARA (Cooperación Latino Americana de Redes Avanzadas)	LATINOAMÉRICA

Tabla 1. 1 Redes avanzadas del continente americano

1.4.2 CANARIE

En la década de los 80 las universidades de Canadá crearon una red la cual interconectaba a las computadoras de los distintos campus pero a velocidades bajas. Esta red fue llamada NetNorth. En 1989 los administradores de NetNorth decidieron adoptar la tecnología emergente que se estaba dando en EUA, propiamente en ARPANET, la cual era el estándar TCP/IP. El paso al estándar TCP / IP fue apoyado por el Consejo de Investigación Nacional de Canadá (CNRC), quien acordó ayudar a financiar una nueva red nacional y formó un comité de planificación que emitió una solicitud RFP (Request for Proposal) de propuestas para crear esta nueva red. La propuesta ganadora fue la de la Universidad de Toronto, la cual contaba con contribuciones de IBM Canadá y el operador de telecomunicaciones local INSIC (Interactive Netcasting Systems Inc). De esta manera en 1990 surgió la nueva red llamada CA*NET Networking Inc [19].

La red CA*NET interconectaba redes regionales, las cuales se muestran en la tabla 1.2:

Localidad	Nombre de red regional
British Columbia	BCNet
Alberta	ARNet
Saskatchewan	SASK#Net
Manitoba	MBNet
Ontario	Onet
Quebec	RISQ
New Brunswick	NBNet
Prince Edward Island	PEINet
Nova Scotia	NSTIN
Newfoundland	NLNet

Tabla 1.2 Redes regionales conectadas a CA*NET

De igual forma, CA*NET proveía tres conexiones hacia la NSFNet de EUA, las cuales estaban en Vancouver, Toronto y Montreal [20].

Las conexiones originales de CA*NET tenían una velocidad de 56 Kbps, pero con el incremento del tráfico en la Internet en 1991 se tuvo la necesidad de incrementar la capacidad de la red. En enero de 1993 el gobierno federal anunció el nacimiento de CANARIE, una organización creada para estimular la investigación y el desarrollo industrial con instalaciones de red de banda ancha. El proyecto inicialmente contó con 3 fases. En la primera fase una de las iniciativas de CANARIE era actualizar el

backbone de CA*NET hasta una capacidad de T-1 ó 1.54 Mbps. Para la segunda fase en 1995 se tuvo una nueva actualización del backbone ahora hasta una capacidad T-3 ó 45 Mbps. Finalmente, en la tercera fase a finales de los 90, cuando ya había una infraestructura de red totalmente actualizada, el gobierno se retiró del proyecto dando paso a la investigación y desarrollo industrial por parte de las universidades [21].

Actualmente (2016) CANARIE apoya la innovación creando comunidades de investigación y educación en Canadá con una red para transmitir datos con una alta velocidad de 100 Gbps, figura 1.8. Más de 19,000 Km de fibra óptica se conectan a más de un millón de usuarios en 1,100 instituciones de Canadá incluidas: universidades, colegios, hospitales y laboratorios de gobierno. Además, CANARIE administra el programa de financiación de investigación ya que proporciona fondos para su comunidad. Esta financiación ayuda a desarrollar plataformas de investigación y componentes que aceleran la invención, el desarrollo de software y permite una amplia utilización de la infraestructura digital [22].

Figura 1.8 Backbone CANARIE 2016 con enlaces de 100 Gbps. Diagrama con base en la referencia [23].

1.4.3 Internet 2

Después de la aparición de la Internet comercial en 1995 y el deseo de los investigadores para recuperar las capacidades de alta velocidad que disfrutaban antes de la privatización de la Internet, el primero de octubre de 1996, 34 líderes universitarios se reunieron en Chicago con la esperanza de establecer capacidades de red para avanzar en la investigación, educación e Internet comercial global. Derivado de esa reunión se creó el proyecto Internet2 el cual se ha convertido en la columna vertebral de la comunidad de investigación y educación de EUA [24].

El proyecto Internet2 fue soportado bajo el respaldo de la UCAID (University Corporation Advanced Internet Development). El objetivo de Internet2 era el desarrollo de tecnología de Internet y aplicaciones orientadas a la investigación y educación para que de esta manera fuera posible el desarrollo de proyectos en centros de investigación y universidades [25].

En 1997 los líderes de Internet2 hacen uso de los GigaPOPs (gigabit points-of-presence), los cuales eran puntos de acceso a la red, que soportaban una velocidad de al menos 1 Gbps y aprovecharon los vBNS (very high speed Backbone Networks Service) de la NSF y la MCI (Microwave Communications Inc,). De esta manera los vNBS sirvieron como el backbone inicial de Internet2 [24].

En 1998 se anunció la red ABILENE, nombrada así por el lugar geográfico donde se construyó: Abilene, Kansas. La creación de dicha red se hizo posible por una asociación con Qwest Communications, Cisco Systems y Nortel Networks. En ese mismo año la Universidad de Indiana ofreció el Centro de Operaciones de Red (NOC) de Abilene y contribuyó en gran medida a su ingeniería y despliegue. La red de Abilene contaba con 133 universidades conectadas a ella. En la figura 1.9 se muestra el backbone inicial de Abilene [24] [26].

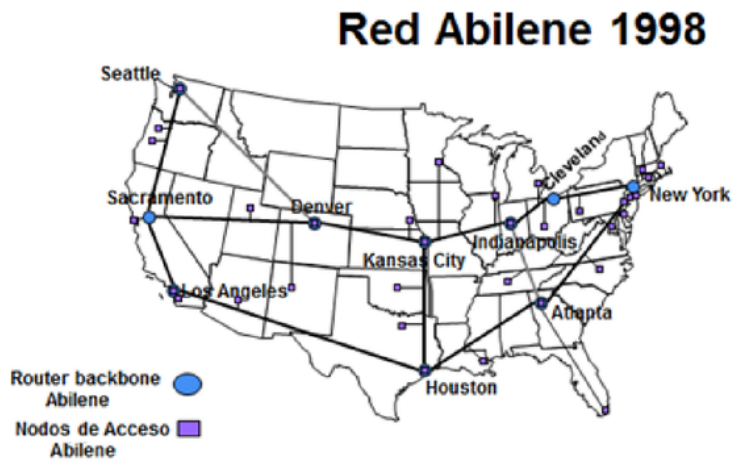


Figura 1.9. Backbone de Abilene 1998. Diagrama propio con base en la referencia. [24]

En febrero de 1999 la red Abilene de Internet2 se puso en marcha bajo el objetivo de extender las fronteras de la investigación y la educación. El backbone de Internet2 incluía alrededor de 21 000 km de fibra óptica con una velocidad de 2.4 Gbps. A finales de año, más de 70 miembros de Internet2 se unieron a Abilene [24].

En 2002 el backbone de Internet2 Abilene comenzó con su primer gran actualización a 10 Gbps con la cual se hacia 4 veces mayor la velocidad de la red. La actualización también contempló la próxima actualización de IP, es decir, IPv6 para direccionamiento futuro, aunque también trabajaba de manera paralela con IPv4. Con esta actualización, Abilene proporcionaba capacidades avanzadas de red a más de 200 universidades a miembros y miles de investigadores afiliados en todo el país; y se interconectó con más de otras 20 redes nacionales de investigación y educación de alto rendimiento de todo el mundo [26].

1.4.4 Infraestructura de Internet2

La infraestructura de Internet2 desde 2013 se divide en niveles. Hay 3 tipos de niveles, los cuales ofrecen diferentes servicios y conexiones [27].

- El nivel 3 (backbone) ofrece un servicio de conexión a nivel del backbone, es decir, el núcleo de la red, por lo que la velocidad es muy rápida ya que se manejan cantidades grandes de información. El ancho de banda es de 100 Gbps.
- En el nivel 2 (distribución) se encuentran los nodos que son intermediarios a los usuarios y el backbone, cuyo ancho de banda dedicado al usuario que varía de 10 Gbps a 100 Gbps.
- En el nivel 1 (acceso) se encuentran los nodos que llegan a los usuarios finales los cuales pueden administrar el ancho de banda en su red local. En este nivel se tiene un ancho de banda que varía de 10 Gbps hasta 100 Gbps.

Al tomar en cuenta los 3 niveles se puede presentar la topología de la infraestructura de Internet2 del 2013, figura 1.10.

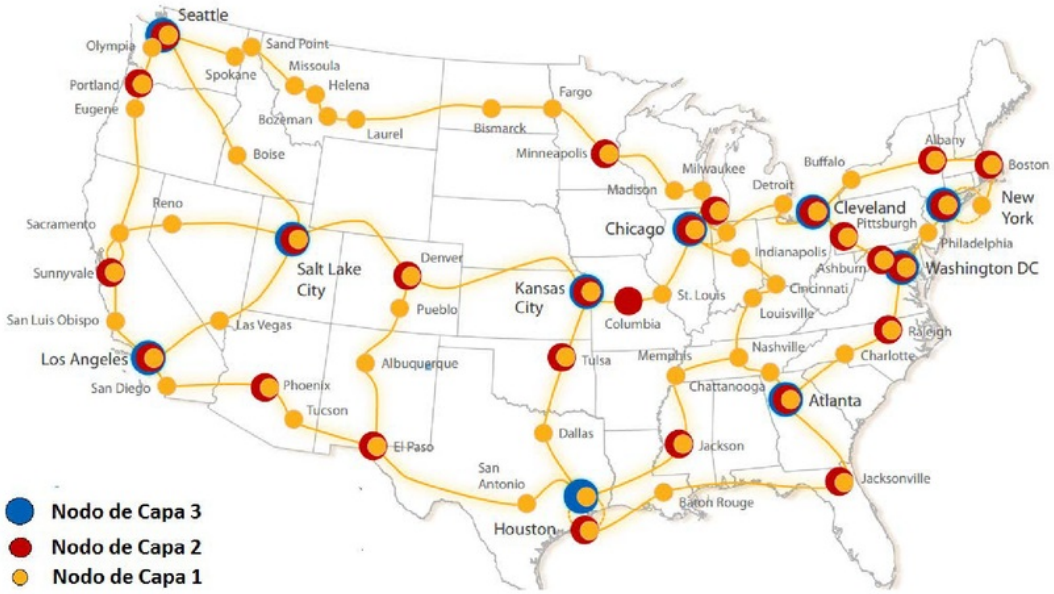


Figura 1.10 Infraestructura de Internet2 2013. Diagrama con base a la referencia [28].

1.5. Red CLARA

La red CLARA es una red avanzada que desde 2004 ha provisto una infraestructura para que las redes nacionales de los países latinoamericanos puedan desarrollar aplicaciones y proyectos creados por universidades y centros de investigación. CLARA se conecta con otras redes avanzadas y centros de investigación alrededor del mundo. En 2005 CLARA contaba con 12 miembros asociados en Latinoamérica. En esta sección se abordan los inicios, desarrollo y evolución de CLARA en los últimos años.

1.5.1 Antecedentes de CLARA

En una reunión en España organizada por DANTE (Delivery of Advanced Network Technology to Europe), la cual es una organización sin fines de lucro dedicada a organizar los servicios internacionales de redes avanzadas para la comunidad de investigación y académica europea, se presentó un estudio llamado CAESAR (Connecting All European and South Latin American Researchers). Dicho estudio tenía el objetivo central de analizar las posibilidades de interconexión directa entre la red de investigación paneuropea GÉANT y sus equivalentes nacionales en América Latina.

CAESAR fue financiado por la Comisión Europea a través de la Dirección General para las Tecnologías de la Sociedad de la Información (EC DG TSI). Posteriormente se convocó a un taller en Toledo, España, para tratar la problemática de la interconexión continental, a este llamado acudieron líderes de las organizaciones dedicadas al desarrollo de redes de investigación y educación de 12 países. El resultado de esta reunión fue que los representantes de 12 redes latinoamericanas se comprometieron a cooperar en la creación y organización de una infraestructura regional para la investigación, la educación y la innovación. Dichas redes fueron: RNP (Rede Nacional de Ensino e Pesquisa, Brasil),– PanNet (Red Académica y de Investigación Nacional, Panamá), CUDI (Corporación Universitaria para el Desarrollo de la Internet, México), RETINA (Red Teleinformática Académica, Argentina), BolNet (Red Boliviana de Comunicación de Datos, Bolivia), REUNA (Red Universitaria Nacional, Chile), RAU (Red Académica Uruguaya, Uruguay), RedUniv (Red Universitaria, Cuba), UNA/CNC (Universidad Nacional de Asunción, Paraguay), RAICES (El Salvador) y Red Científica Peruana (Perú) [29].

1.5.2 El proyecto ALICE

En junio de 2003 inició formalmente el proyecto ALICE (America Latina Interconectada con Europa) con una inversión de € 12.5 millones de los cuales, 10 millones los aporto la Unión Europea y 2.5 millones los socios latinoamericanos. De esta forma, el proyecto ALICE fue un financiamiento de Europa para Latinoamérica con el fin de crear una infraestructura de redes de investigación en América Latina e

interconectarla con su par europea GÉANT mediante el protocolo de Internet (IP). ALICE dio como plazo hasta 2006 para alcanzar la conectividad del continente americano con el europeo, dicho plazo se extendió hasta 2008 ya que los objetivos del financiamiento cada vez tomaban más forma [29].

1.5.3 Nacimiento de CLARA

Mientras Internet2 y CANARIE estaban en pleno desarrollo, en 2003 tras una reunión en Valle de Bravo México, se tuvo la idea inicial para la formación de CLARA. Después de esta reunión, la idea de la organización de redes latinoamericanas se consolidó y se transformó en la organización CLARA, la cual se conserva hasta la actualidad. La constitución formal de CLARA fue acordada el 9 de junio de 2003 en una reunión en México y fue registrada como organización internacional sin fines de lucro en Uruguay el 23 de diciembre del mismo año [29] [30].

Algunos objetivos de CLARA en ese momento fueron:

1. Coordinar entre redes nacionales académicas en América Latina con otras regiones
2. Cooperar para el fomento del desarrollo científico y tecnológico
3. Planificar e implementación de servicios de red para interconexiones regionales
4. Desarrollar una red regional que interconecte redes nacionales académicas y de investigación, misma que deberá ser operada por sus asociados
5. Crear una organización no gubernamental que represente los intereses de las organizaciones conectadas a esta red

La primera etapa de la instalación de la red CLARA tuvo lugar a finales de 2004 cuando se conectaron los primeros seis nodos de la red, los cuales incluían a Argentina, Brasil, Chile, México, Panamá y Venezuela, además de una conexión hacia Europa con GÉANT.

Cabe resaltar que gracias al proyecto WHREN/LILA (Western Hemosphere Research and Education Network/ Links Interconnecting Latin America) CLARA se conectó a EUA con el objetivo de establecer una conexión directa entre las redes académicas y de investigación entre Latinoamérica y Norteamérica. El nodo de Tijuana en México y el de Brasil se interconectaban con las ciudades de San Diego y Miami para tener un acceso hacia la red avanzada Internet 2. Mientras que los enlaces en la red CLARA eran de 155 Mbps, los enlaces mencionados anteriormente que se conectaban con Internet 2 soportaban hasta 1.2 Gbps, como se muestra en la figura 1.11 [31].

Figura 1.11. Enlaces proporcionados por WHREN/LILA para conexión de CLARA con EUA en 2004. Diagrama tomado de la referencia [31].

En 2005 se integraron más redes avanzadas a CLARA, dichas redes fueron la CR2Net de Costa Rica, la RAAP (Red Académica Peruana), RAICES (Red Avanzada de Investigación Ciencia y Educación Salvadoreña), RAGIE (Red Avanzada Guatemalteca para la Investigación y Educación), RedUNIV de Cuba y finalmente RAU (Red Académica de Uruguay). Con esto, hasta ese año se contaba con 12 países que conformaban a la red CLARA.

Para el año de 2006 CLARA ya era una red con 14 países de Latinoamérica conectados, ese año se conectaron a CLARA países de Centroamérica como Guatemala, El Salvador, Nicaragua y Panamá, además de países de América del sur

como Ecuador y Colombia también se agregaron. De esta manera, CLARA tenía presencia tanto en Norteamérica, Centroamérica y Sudamérica con 16 nodos y 17 enlaces que iban desde los 34 Mbps hasta los 2.5 Gbps como se muestra en la figura 1.12. [32]

Figura 1.12. Topología de la Red CLARA 2006. Diagrama con base en la referencia [32].

1.5.4 Consolidación de CLARA

A principios de 2007 la red CLARA tenía una organización más consolidada ya que este año se integró el NOC (Network Operation Center), el cual se encargó de la administración, control, monitoreo y operación diaria de la infraestructura y funciones físicas que constituyen el backbone de la red CLARA. Con el objetivo de garantizar un rendimiento óptimo en la red y sus interconexiones, el NOC de CLARA se estableció físicamente en México y fue administrado por la red avanzada CUDI. Posteriormente, fue trasladado a Chile y actualmente es administrado por la red avanzada REUNA (Red Universitaria Nacional) en el mismo país, en cuanto a su funcionamiento el NOC depende del comité técnico de CLARA cuyo propósito es mantener la red latinoamericana a la vanguardia en servicios avanzados en redes IP [33].

Con el fin de optimizar recursos, en febrero de 2007 CLARA instaló un nuevo nodo en las instalaciones del NAP (Network Access Point) de las Américas en Miami, dichas instalaciones cuentan con una gran calidad técnica que permitiría asegurar que el nodo se encuentre activo un 99.999% del tiempo. Al nuevo nodo se instalaron conexiones a Panamá (155 Mbps), el Salvador (10 Mbps) y Guatemala (10 Mbps). Adicionalmente, se eliminó el enlace directo de Sao Paulo a Tijuana.

El nuevo nodo de Miami fue conectado al nodo del proyecto WHREN/LILA en la misma ciudad para después, mediante un enlace privado virtual (VPN), hacer una conexión entre Sao Paulo-Panamá-Santiago de Chile-Buenos Aires-Sao Paulo [34].

En 2008 tres redes aumentaron la capacidad de sus accesos a la red CLARA, CEDIA de Ecuador pasó de 10 Mbps a 22.5 Mbps, RENATA (Red Nacional Académica de Tecnología Avanzada) de Colombia pasó de 13 Mbps a 45 Mbps y por último RAGIE de Guatemala pasó de 10 Mbps a 18 Mbps. En la figura 1.13 se muestran los cambios que hubo en la red CLARA entre los años 2007 y 2008, con 23 nodos y 24 enlaces.

Figura 1.13. Topología de CLARA hasta 2008. Diagrama con base en la referencia [35].

En 2008 finalizó el proyecto ALICE y debido al éxito que alcanzó se dio inicio inmediatamente al proyecto ALICE2, ahora la Comisión Europea firmó un contrato por € 18 millones para la realización del mismo. Esta nueva iniciativa consolidaría y

extendería la Red CLARA en América Latina, mejorando así la conectividad entre los investigadores latinoamericanos y europeos.

Para 2009 el proyecto ALICE2 tomó más forma y se propusieron los siguientes objetivos [36].

1. Crear una red CLARA2 cuya infraestructura sea fundamentalmente óptica, con costos de mantenimiento bajos, lo que la haga sustentable en el tiempo
2. Hacer de CLARA una organización ampliamente inclusiva que incorpore paulatinamente a todos los países de la región y que favorezca la extensión de las NRENs (National Research and Education Networs)
3. Apoyar el desarrollo de las NRENs por la vía de capacitar a sus técnicos y cuadros gerenciales, así como a las comunidades de usuarios

1.5.5 Red CLARA2

En 2009 la red CLARA2 comenzó su instalación, dicha red pretendía que en su infraestructura se tuviera una red completamente óptica con enlaces mucho más rápidos. CLARA2 incorporó nuevas características de las que sobresalen enlaces múltiples con una capacidad de hasta 10 Gbps que van de *Santiago de Chile, Chile-Buenos Aires, Argentina-Porto Alegre, Brasil.* Por otro lado en Centroamérica se instaló otro enlace de 2.5 Mbps que conectaba a El Salvador y Guatemala [36].

En 2011 se incrementaron algunos enlaces entre los miembros de CLARA, esto marcó un crecimiento considerable en la amplitud del ancho de banda del backbone. A principios de año se concluyó la activación del enlace de respaldo de 1 Gbps para el enlace de 10 Gbps Buenos Aires – Santiago, el enlace entre Panamá y Miami se amplía de 155 Mbps a 1 Gbps. Por otro lado, se estableció un enlace entre Santiago y Panamá, iniciándose la implementación de un anillo STM-4 (622 Mbps) para Sao Paulo - Santiago – Panamá – Sao Paulo. Con esto, la red CLARA multiplicó por 4 la capacidad de sus enlaces en esos PoP. Para finales de año se incrementaron a 622 Mbps los enlaces entre Guayaquil - Lima, Bogotá- Caracas y Caracas-Panamá: la capacidad mínima de Red CLARA pasó de 155 a 622 Mbps [37].

Para el año de 2012 el proyecto ALICE2 finalizó, dicho proyecto permitió a la Red CLARA alcanzar un estado de madurez como institución e infraestructura, entre sus resultados más destacados se obtuvieron un enlace de 2.5 Gbps de CLARA a GÉANT, además de la implementación del primer tramo de fibra óptica de Centroamérica entre San José (Costa Rica) y Ciudad de Panamá (Panamá).

A finales de año, la implementación de la red de fibra óptica en Centroamérica activó la instalación de un enlace por tierra de 1 Gbps por medio de Ethernet entre San Salvador (El Salvador) y San José (Costa Rica), con lo que se incrementó la capacidad de tráfico que se extiende entre San José – Managua – San Salvador. Es importante mencionar que un nodo de la red se ubicó en Nicaragua la cual se conectó en 2013. Por último, en este año se conectó la red del Caribe [38].
En 2013 se instalaron otros dos enlaces de fibra óptica, el primero a 10 Gbps entre Buenos Aires en Argentina y Porto Alegre en Brasil. Y el segundo con una capacidad de 2.5 Gbps entre Lima en Perú y Antofagasta en Chile.

1.5.6 Características técnicas de CLARA en 2014

El backbone de la red CLARA está compuesto por diez nodos router principales, conectados en una topología punto-a-punto. Cada nodo principal representa a un PoP para la red CLARA, siete de ellos están ubicados en un país de América Latina - São Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Caracas (CCS - Venezuela), Panamá (PTY - Panamá), dos en EUA: Miami (MIA - Estados Unidos) y Washington (WSG - Estados Unidos) y uno en Europa (MAD-España) el cual se conecta con GÉANT. Todas las conexiones de las redes nacionales latinoamericanas a la Red CLARA son a través de uno de estos nodos.

A nivel de capacidad, la red CLARA tiene una infraestructura entre los nodos de América Latina mencionados en la modalidad de IRU (Irrestrictible Right of Use) a 10 o 15 años. En este modelo la Red CLARA tiene fibra oscura en Centroamérica pasando por Panamá, Costa Rica, Nicaragua, Honduras, El Salvador, Guatemala y México, una troncal de 10 Gbps entre Santiago (Chile) y Buenos Aires (Argentina), así como un enlace de 10 Gbps entre Buenos Aires (Argentina) y Porto Alegre (Brasil). Cuando una RNIE latinoamericana hace conexión con CLARA, lo hace a través de uno de los diez nodos de su troncal; esta conexión le brinda a estas redes y a sus miembros (clientes) acceso a la red CLARA, otorgándoles un punto de intercambio como se indica en la figura 1.14 [42].

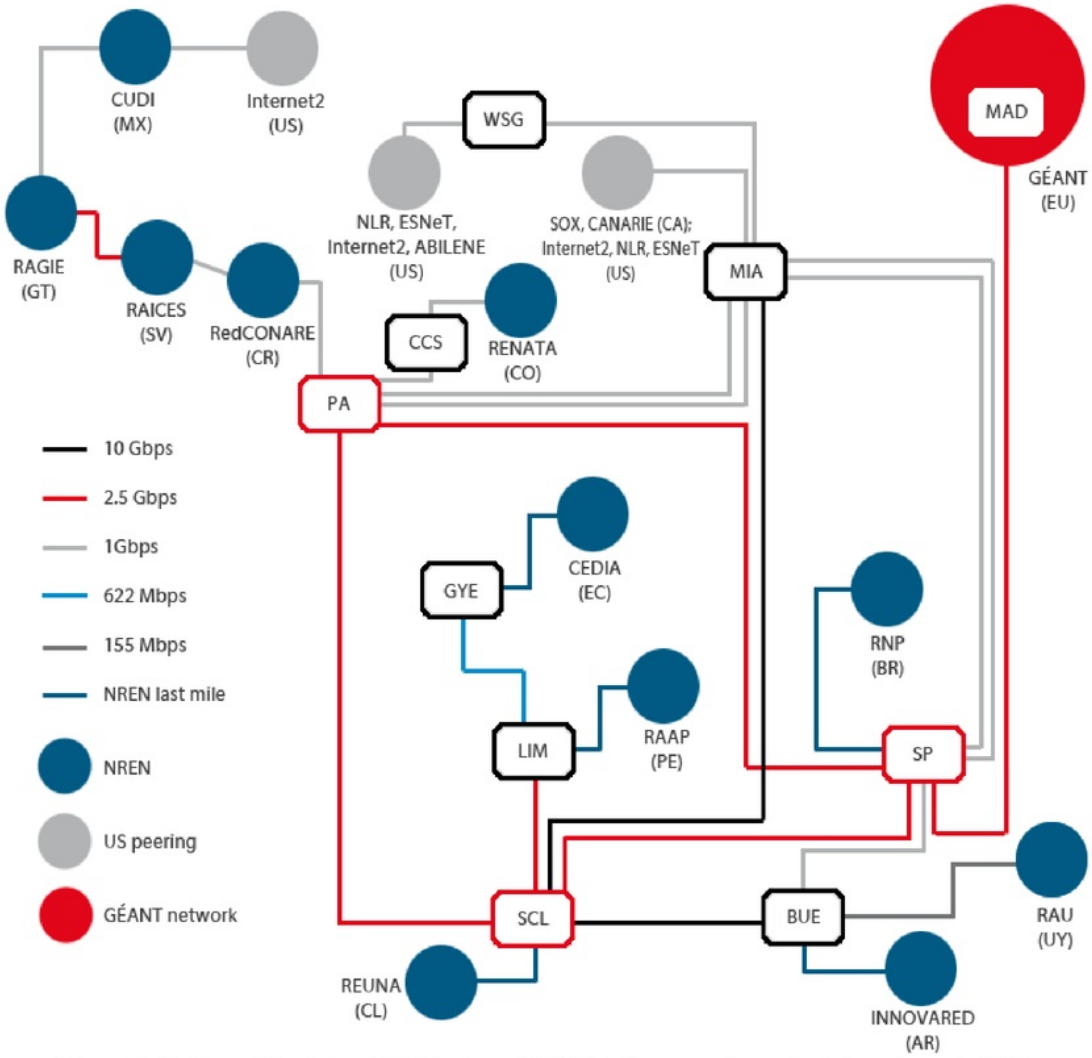


Figura 1.14. Conexión de las NREN a la red CLARA. Diagrama tomado de la referencia [42].

1.5.7 CLARA en 2016-2017

En los últimos 3 años CLARA ha tenido actualizaciones destacables empezando en 2014 por el incremento de la capacidad del enlace entre el PoP de la Red CLARA en Sao Paulo (Brasil) y el de GÉANT en Londres (Inglaterra) a 5 Gbps, lo que beneficia a las comunidades de investigación de América Latina y sus colaboraciones con sus pares en Europa.

Por otra parte, se activó la nueva conexión de 2.5 Gbps entre Guatemala y Tapachula, México (es importante mencionar que el nodo de Tijuana fue reemplazado por el de Tapachula), completando así el enlace de fibra obscura que la red CLARA adquirió para conectar los países centroamericanos: México, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica y Panamá [39].

Las últimas actualizaciones de la red CLARA se llevaron a cabo el 2017, a principios de año se realizó el cambio en la capacidad de los enlaces troncales de 2.5 Gbps entre Santiago (Chile), Panamá (Panamá) y Sao Paulo (Brasil), a enlaces de 10 Gbps entre dichos países [40].

En 2017 la red CLARA cuenta con 12 miembros los cuales se muestran en la tabla 2.3 [29].

País	Red Avanzada
Argentina (AR)	INNOVA RED
Brasil (BR)	RNP
Colombia (CO)	RENATA
Costa Rica (CR)	RedCONARE
Chile (CL)	REUNA
Ecuador (EC)	CEDIA
El Salvador (SV)	RAICES
Guatemala (GT)	RAGIE
México (MX)	CUDI
Perú (PE)	RAAP
Uruguay (UY)	RAU
Venezuela (VE)	REACCIUN

Tabla 1.3 Redes conectadas a CLARA hasta 2017.

Dichos miembros se conectan de acuerdo a la topología mostrada en la figura 1.15.

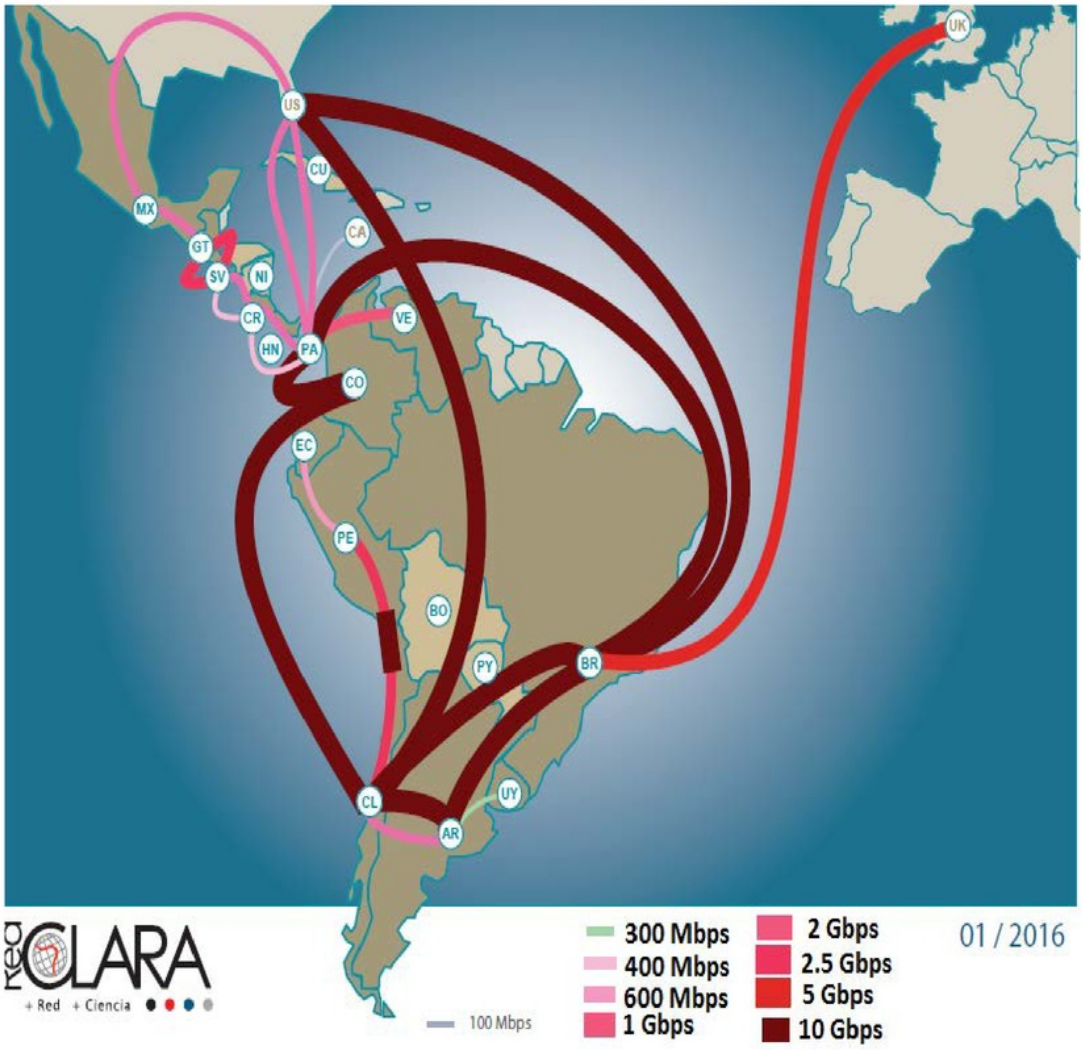


Figura 1.15. Topología de la red CLARA en 2016. Diagrama tomado de la referencia [40].

De igual manera en el 2017 se aumentaron los enlaces de El Salvador – Costa Rica, Costa Rica – Panama de 1 Gbps a 2.5 Gbps, se eliminaron los enlaces de Miami a Panamá ambos de 1 Gbps y se cambiaron por un enlace de 10 Gbps, por último, se aumentó la capacidad del enlace de Miami a Porto Alegre de 10 Gbps hasta 100 Gbps. Por lo que la topología de 2017 se presenta en la figura 1.16.

Figura 1.16. Topología de la red CLARA en 2017. Diagrama tomado de la referencia [41].

Capítulo 2 Protocolos de enrutamiento y gestión

Para lograr que la información fluya o viaje de una red a otra debemos considerar ciertos parámetros y conceptos que hagan esto posible. Todo ello es considerado en los protocolos de enrutamiento ya que estos determinan cuál es la mejor ruta para enviar paquetes entre diferentes redes. Para la presente tesis y debido al protocolo de enrutamiento que utilizaremos, la mejor ruta será aquella que presenta un menor costo del enlace. Para fijar esto, se utiliza una métrica, la cual es información que recopila el router como ancho de banda, estado de enlaces, tipos de enlaces; y les establece un valor. La métrica se utiliza para determinar qué ruta es más factible cuando existe más de un camino al mismo destino. Para complementar esto, los protocolos de enrutamiento se basan en algoritmos matemáticos, los cuales realizan los cálculos para obtener las mejores rutas. Los algoritmos utilizados y aplicados a las redes por los diferentes protocolos de enrutamiento son Dijkstra y Bellman-Ford. En el presente capítulo se hace una clasificación general de los protocolos de enrutamiento y se profundiza en dos de ellos RIP (Routing Information Protocol) y OSPF (Open Shortest Path First). Es preciso indicar que el protocolo que se utiliza para la simulación y emulación de la red CLARA es OSPF.

Por otra parte, los protocolos de gestión sirven para que los administradores de red puedan tener un control de lo que ocurre en la red. En el presente capítulo se abordará SNMP, el cual es el protocolo de gestión más común para la administración de redes. SNMP permite consultar los diferentes elementos que hay en la red y de esta manera poder identificar los problemas que afectan a las redes por ejemplo un enlace caído, un dispositivo que no funciona o bien si la información no está siendo enviada y recibida de manera adecuada.

2.1 Tipos de enrutamiento

Antes de introducir los protocolos y algoritmos de enrutamiento es importante definir qué es un router. Un router es una computadora con un sistema operativo diseñado especialmente para el envió de paquetes, se encarga de interconectar dos o más redes y elige la ruta óptima para enviar paquetes entre las redes [43].

Al referirnos al enrutamiento es necesario hablar primero de la capa de red, la cual tiene la función de mover paquetes desde un host emisor hacia un host receptor. Para hacer eso se necesitan dos funciones que son el reenvío de paquetes y el enrutamiento:

1. Reenvío de paquetes. Cuando un paquete llega al enlace de entrada de un router, el router debe mover el paquete hacia el enlace de salida adecuado. El

reenvió se refiere a la acción local del router de transferir un paquete desde una interfaz de entrada hacia una interfaz de salida.

2. Enrutamiento. La capa de red debe determinar la ruta tomada por los paquetes, es decir, cómo fluyen de un emisor a un receptor. Los algoritmos que se encargan de calcular estas rutas son llamados algoritmos de enrutamiento. El enrutamiento es el proceso que involucra a la red y determina las rutas de extremo a extremo que los paquetes toman desde su origen hasta su destino. Para poder enviar los paquetes los routers tienen que conocer la dirección destino además de los routers vecinos con el objetivo de aprender la mejor ruta para alcanzar a cada red remota.

Para determinar el mejor camino y enviar un paquete el router cuenta con una tabla de enrutamiento la cual elabora obteniendo datos de los routers conectados directamente, los routers vecinos o los routers directamente proporcionados por el administrador de red, la tabla de enrutamiento mantiene un registro de las mejores rutas posibles a las direcciones de las redes de destino, así como las métricas asociadas con estas rutas. Generalmente una tabla de enrutamiento es confundida con la tabla de reenvío, la diferencia es que una tabla de reenvío contiene únicamente las rutas que son elegidas por el algoritmo de enrutamiento como rutas preferidas para el reenvío de paquetes, mientras que en la tabla de enrutamiento se almacenan datos de una forma más general para el reenvió de paquetes [44].

Existen dos tipos de rutas en la tabla de enrutamiento: las que están directamente conectadas a la red y las que están remotamente conectadas. Las rutas remotas sólo pueden llegar a otras redes enviando los paquetes a otro router. Este tipo de rutas se agregan a la tabla de enrutamiento utilizando un protocolo de enrutamiento dinámico o estático [43].

- El enrutamiento estático está compuesto por rutas a redes que un administrador de red agrega y configura manualmente.
- El enrutamiento dinámico son rutas a redes remotas que se aprendieron automáticamente por el router. Es el proceso en el que los protocolos de enrutamiento comunican el router de origen con los routers vecinos. De esta forma, los routers se actualizan mutuamente con base en las redes que conocen. Si se produce un cambio en la red, los protocolos de enrutamiento dinámico informan automáticamente a todos los integrantes de esa red los cambios que hay en la misma.

En la tabla 2.1 se muestran las ventajas y desventajas del enrutamiento dinámico y estático [42].

Tipo de enrutamiento	Ventajas	Desventajas
Estático	• Hay un uso mínimo de ancho de banda entre los routers ya que, al no utilizar protocolos de enrutamiento, no se necesita de gran cantidad de ancho de banda para el envió de actualizaciones automáticas. • Seguridad, ya que el administrador sólo permite el enrutamiento a ciertas redes.	• El administrador debe conocer realmente la red y cómo cada router está conectado para poder configurar las rutas correctamente. • Si se agrega una nueva red el administrador debe agregar una ruta a esta en todos los routers
Dinámico	• Es más fácil de implementar ya que la configuración de las rutas en la tabla de enrutamiento se hace de forma automática.	• Hay un uso considerable en el CPU del router. • Utiliza ancho de banda en los enlaces de la red ya que requiere de la realización y envió de actualizaciones automáticas.

Tabla 2.1. Ventajas y desventajas en enrutamiento estático y dinámico.

2.2 Algoritmos de enrutamiento

Para que el enrutamiento sea posible es necesaria la ejecución de los algoritmos de enrutamiento. Los algoritmos de enrutamiento intercambian y calculan la información que se utiliza para configurar las tablas de reenvío. El algoritmo de enrutamiento determina los valores que se fijan en las tablas de reenvío de los routers. El propósito de un algoritmo de enrutamiento es simple: dado un conjunto de routers con enlaces que conectan a los routes entre sí, un algoritmo de enrutamiento encuentra un "buen" camino desde el router de origen hacia el router de destino. Regularmente, una buena ruta es la que tiene el menor costo como se había indicado al inicio del presente capítulo.

Existen dos tipos de algoritmos de enrutamiento: el centralizado y el descentralizado. El centralizado es un algoritmo que se ejecuta en un sitio central (nodo central) y

descarga información de enrutamiento a cada uno de los routers. Por otro lado en el descentralizado en el que todos los nodos son iguales y cada router envía y recibe información de enrutamiento. En cualquier caso, un router recibe mensajes del algoritmo de enrutamiento, los cuales se utilizan para configurar su tabla de reenvío. La interacción entre los algoritmos de enrutamiento y las tablas de reenvío se muestra en la figura 2.1

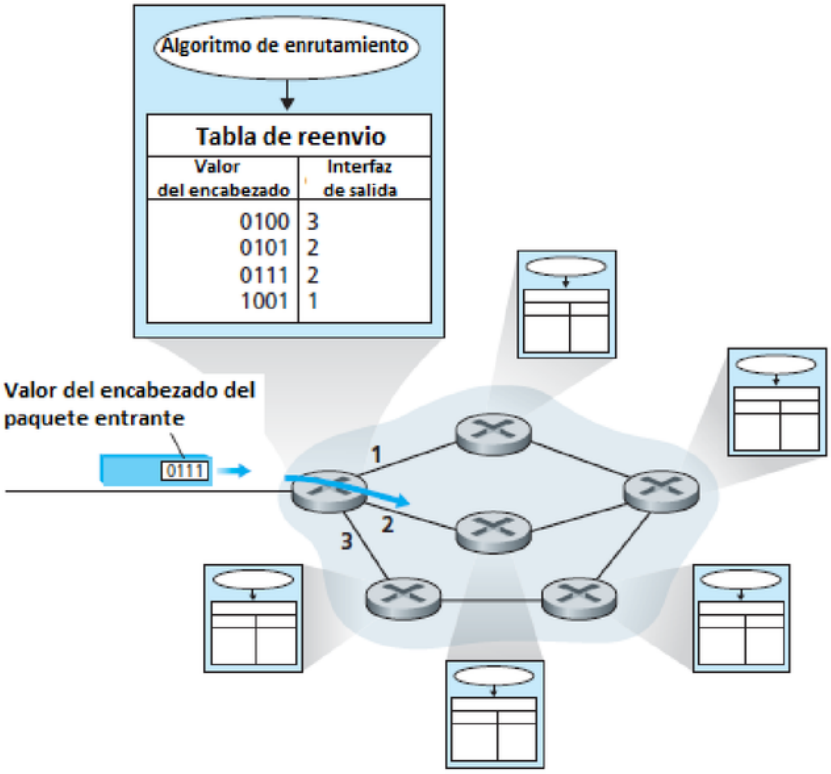


Figura 2.1 Interacción entre los algoritmos de enrutamiento y las tablas de reenvío. Los algoritmos de enrutamiento determinan valores en la tabla de reenvió. Diagrama tomado de la referencia [44].

Los algoritmos de enrutamiento tienen una parte matemática la cual está relacionada con la teoría de grafos. Los algoritmos matemáticos Bellman-Ford y Dijkstra se apoyan en la teoría de grafos para poder encontrar la mejor ruta en una red [45] [46].

Una forma en que podemos clasificar a los algoritmos de enrutamiento es en globales o descentralizados.

2.2.1 Algoritmos de enrutamiento global

Un algoritmo de enrutamiento global o centralizado calcula la ruta de menor costo entre un router de origen y un router destino utilizando el conocimiento completo y global que tiene sobre la red. En otras palabras, el algoritmo toma la conectividad entre todos los nodos y todos los costos de los enlaces como entradas. El cálculo se

ejecuta en un sitio o puede ser replicado en varios sitios ya que un algoritmo global debe tener la información completa acerca de la conectividad y costos de los enlaces, en las redes este tipo de algoritmos son conocidos como algoritmos de *estado-enlace* ya que el algoritmo debe tener en cuenta el costo de cada enlace en la red [44].

2.2.1.1 Algoritmo de estado-enlace

En un algoritmo de estado de enlace, la topología de red y todos los costos de enlace son conocidos. En la práctica esto se logra haciendo que cada nodo transmita paquetes de estado de enlace a todos los otros nodos en la red (broadcast). Con cada paquete de estado de enlace que contiene las identidades y los costos de sus enlaces vecinos, debido al broadcast que se hace, cada nodo puede ejecutar el algoritmo de estado enlace y calcular por sí mismo el conjunto de rutas de menor costo como cualquier otro nodo. Este tipo de algoritmo es adecuado para usarse en redes grandes, además utiliza el algoritmo matemático Dijkstra. El protocolo de enrutamiento OSPF del cual se hablará más adelante utiliza este tipo de algoritmo para el cálculo de rutas [47].

2.2.2 Algoritmos de enrutamiento descentralizado

En un algoritmo de enrutamiento descentralizado el cálculo de la ruta de menor costo se realiza de manera distribuida. Ningún nodo en la red tiene información completa acerca de los costos de todos los enlaces de red. En su lugar, cada nodo comienza solo con conocimiento de los costos de sus propios enlaces directamente vinculados, después a través de un proceso de cálculo e intercambio de información con sus nodos vecinos un nodo calcula la ruta de menor costo a un destino o conjunto de destinos. El algoritmo de enrutamiento descentralizado utilizado en las redes es el algoritmo de vector-distancia llamado así porque cada nodo contiene un vector de estimaciones de los costos y distancias hacia otros nodos de la red [44].

2.2.2.1 Algoritmos de vector-distancia

En un algoritmo de vector distancia los routers envían actualizaciones de rutas periódicas a los vecinos que están directamente conectados, se dice que un algoritmo de vector-distancia es distribuido, iterativo y asíncrono:

- Distribuido. Cada nodo recibe cierta información de uno o varios vecinos que están conectados directamente a él, realiza cálculos y luego redistribuye los resultados de sus cálculos a sus vecinos.
- Iterativo. Este proceso continúa hasta que no se intercambie más información entre los vecinos.

- Asíncrono. No requiere que todos los nodos operen al mismo tiempo, cada nodo puede enviar información de manera aislada.

Este tipo de algoritmos es adecuado para usarse en redes pequeñas o interiores, además utiliza el modelo matemático aplicado a la teoría de grafos de Bellman Ford.

El protocolo de enrutamiento RIPV1 y RIPV2 del cual se hablará más adelante utiliza este tipo de algoritmo para el cálculo de rutas [47].

2.3 Protocolos de enrutamiento

Las redes utilizan los protocolos para cumplir con el envió de paquetes a otras redes. Un protocolo define el formato y el orden de los mensajes intercambiados entre dos o más entidades comunicantes, así como las medidas adoptadas en la transmisión y / o recepción de un mensaje u otro evento [44].

Existen dos tipos de protocolos de enrutamiento utilizados en las redes: el IGP (Interior Gateway Protocol) y el EGP (Exterior Gateway Protocol). Los IGP se usan para el intercambio de información de enrutamiento con otros routers que estén en el mismo Sistema Autónomo (AS). Un AS es una colección de redes bajo un mismo dominio administrativo que tiene un control y gestión propios. [11]. Algunos ejemplos de IGP son RIPv1, RIP v2, IGRP, EIGRP, OSPF, IS-IS. Los EGP son usados para conectar a uno o más AS. Un ejemplo de EGP es BGP [48].

Es importante hacer una clasificación global de algoritmos de enrutamiento y protocolos revisados ya que se hace énfasis en este documento en los protocolos de enrutamiento dinámicos, como se muestra en la figura 2.2.

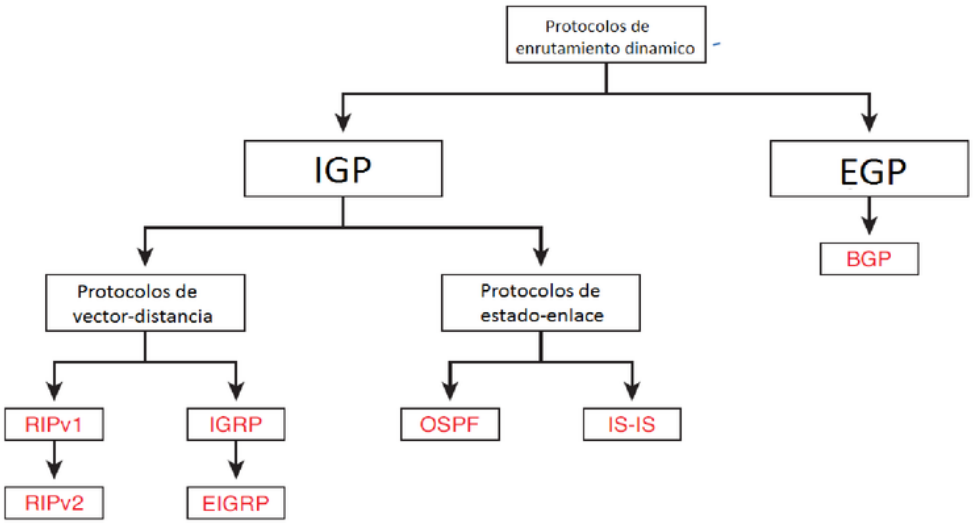


Figura 2.2 Esquema general de los protocolos de enrutamiento dinámicos. Diagrama propio con base en la referencia [43].

Antes de introducir los protocolos que utilizaré para la emulación de la red CLARA es importante hablar de algunos parámetros que son parte fundamental en el funcionamiento de los mismos:

1. Métrica. Se utiliza cuando un destino tiene más de una ruta. Para seleccionar el mejor camino, el protocolo de enrutamiento debe ser capaz de evaluar y diferenciar entre los caminos disponibles. Para ello se utiliza una métrica. La métrica consta de 6 parámetros listados a continuación:
   a. Costo: Valor determinado por el IOS o por el administrador de la red para indicar una preferencia hacia una determinada ruta.
   b. Ancho de banda: Influye en la selección de rutas prefiriendo la ruta con el ancho de banda más alto.
   c. Delay: Considera el tiempo que tarda un paquete en recorrer un camino.
   d. Conteo de saltos. Cuenta el número de routers que un paquete debe recorrer.
   e. Carga: Considera la utilización del tráfico de un enlace determinado.
   f. Confiabilidad: Evalúa la probabilidad de un fallo de enlace, calculado a partir del recuento de errores de interfaz o errores anteriores del enlace.

2. Distancia administrativa. Si tenemos varios protocolos de enrutamiento en un router debemos diferenciar que protocolo está actualizando la tabla de enrutamiento. La distancia administrativa es un valor entero de 0 a 255. Cuanto más bajo es el valor, más preferida es la ruta del protocolo de enrutamiento. Una distancia administrativa de "0" es la más preferida, ya que se considera que un router está conectado directamente a la red. Una distancia administrativa de 255 significa que la ruta no es confiable. Es un parámetro que define la fiabilidad en una ruta.

2.3.1 Routing Information Protocol (RIPv1)

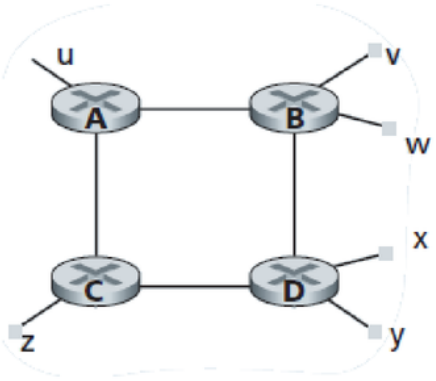
RIPv1 es un protocolo de enrutamiento de vector-distancia basado en el algoritmo de Bellman-Ford. Los algoritmos de vector distancia fueron utilizados desde los inicios de ARPANET. Los orígenes de RIP se tienen en un protocolo de Xerox llamado GIP (Gateway Information Protocol), este protocolo se usaba para intercambiar información de enrutamiento entre redes o sistemas autónomos. Más tarde en 1982 la Universidad de Berkeley desarrollo una variante llamada "routed" misma que pasó a la distribución de software de Unix de Berkeley compatible con TCP/IP. Esta variante tenía como principal característica un temporizador que limitaba a 30 segundos como máximo su actualización.

Por otro lado, diferentes proveedores hacían sus implementaciones del GIP, es por eso que Charles Hedrick en 1988 reconociendo la necesidad de estandarizar el protocolo escribió el RFC 1058 en el cual documentó la existencia del protocolo y especificó algunas mejoras en base al GIP [49].

2.3.1.1 Características de RIPv1

RIP es un protocolo perteneciente a la familia IGP, está diseñado para redes pequeñas dentro de un AS. Al ser un protocolo de vector-distancia está basado en el algoritmo Bellman-Ford y busca la mejor ruta mediante el conteo de saltos como parte de su métrica, esto significa que cada enlace que conecta un router con otro es considerado un salto y tiene un costo de 1, de esta forma cualquier router intermedio que se atraviesa entre el origen y el destino de una ruta es considerado un salto. Al considerar sólo saltos, RIP no toma en cuenta factores como tráfico o ancho de banda. Sin embargo, RIP sólo considera 15 saltos como máximo para llegar a un destino [49].

RIP utiliza el término salto, el cual es el número de subredes recorridas a lo largo de la ruta más corta desde el router de origen hacia la subred de destino. En la figura 2.3 se observa un ejemplo de un AS con seis subredes, así como una tabla que indica el número de saltos desde el router de origen (router A) hasta cada una de las subredes.



Destino	Saltos
u	0
v	2
w	2
x	3
y	3
z	2

Figura 2.3 Conteo de saltos en un AS. Diagrama con base en la referencia [44].

RIP tiene como objetivo permitir que los hosts y routers intercambien información para el cálculo de rutas en una red. A continuación, se enlistan las principales características de RIP [47]:

- Saltos. RIP utiliza saltos como única métrica. Las rutas con saltos superiores a 15 se consideran inaccesibles.
- Actualizaciones por disparo. Cuando RIP detecta que una red es inaccesible lanza una actualización que indica que la red es inaccesible para dar paso a

otra característica llamada “holddown” la cual determina si la ruta es inaccesible mediante un timer.

- Balanceo de carga. Si hay la posibilidad de enviar la información por varios caminos con el mismo costo se balanceará el tráfico con la técnica de “round-robin” que asigna tiempos para el envío por turnos.
- La distancia administrativa de RIPv1 es 120.
- Timers. RIP utiliza ciertos timers o temporizadores para su rendimiento.
  - Temporizador de actualización de ruta. Establece actualizaciones periódicas de enrutamiento normalmente de 30 segundos, en las que el router envía una información de enrutamiento a todos los vecinos.
  - Temporizador de ruta inválida (Hold down). Determina el periodo de tiempo que debe pasar, generalmente de 90 segundos, para que un router determine que una ruta no es válida o inaccesible.

2.3.1.2 Limitaciones de RIPv1

RIPv1 es un protocolo con algunas limitaciones como se mencionó anteriormente, pertenece a la familia de los IGP por lo cual su uso es para redes pequeñas. Las limitaciones de RIPv1 son las siguientes [49]:

1) El protocolo está limitado a las redes cuyo camino más largo implica 15 saltos. Por lo que no es aplicable en redes grandes.
2) El protocolo depende de “contar hasta el infinito” para resolver ciertas situaciones inusuales. Supongamos que se envían actualizaciones sin respuesta o sin encontrar un destino (bucles), esto implicaría un desperdicio de ancho de banda o uso excesivo en el CPU del router por lo que infinito debe traducirse en un valor de 16 saltos para que el bucle termine.
3) Este protocolo utiliza métricas fijas para comparar entre rutas alternativas. Esto no es apropiado en situaciones en las que las rutas necesitan ser escogidas con base en parámetros en tiempo real, como por ejemplo retardo medido, confiabilidad del enlace o carga.
4) El protocolo se define como con clase (Classfull), esto significa que solo trabaja con las direcciones de red y no envía la máscara de subred durante las actualizaciones de enrutamiento, debido a esto todos los routers deben tener la misma máscara de subred. RIPv1 solo trabajará con las redes de clase A, B y C.

2.3.1.3 Formato de mensajes de RIP

RIP es un protocolo con base en UDP (User Datagram Protocol) por lo que cada host que utiliza RIP tiene un proceso de enrutamiento que envía y recibe datagramas así como mensajes de actualizaciones por el puerto UDP 520. Para el enrutamiento de los paquetes, RIPv1 tiene un encapsulamiento como se muestra en la figura 2.4. [49]

Encabezado enlace de Datos	Encabezado del paquete IP	Encabezado del segmento UDP	Mensaje RIP

Figura 2.4 Encapsulamiento de RIP. Diagrama propio con base en referencia. [43]

1) *Encabezado de enlace de datos*: Posee las direcciones MAC de origen y destino.
2) *Encabezado del paquete IP*: Posee las direcciones IP de origen y destino.
3) *Encabezado del segmento UDP*: Posee los puertos de origen y destino, cada uno de 520.
4) *Mensaje RIP*: Contiene el tipo de mensaje, si es solicitud (1) o r espuesta (2); la versión del RIP que se utiliza ya sea 1 o 2; un identificador para la familia de direcciones, generalmente de 2 para IP; y la métrica que se utiliza que es el conteo de saltos. En cualquiera de las versiones RIP se pueden tener hasta 25 rutas, por lo que el mensaje puede aumentar su tamaño hasta 512 bytes.

A continuación se detalla más a fondo el formato de mensaje de RIPv1 presentado en la figura 2.5. En donde los campos están agrupados por octetos (8 bits).

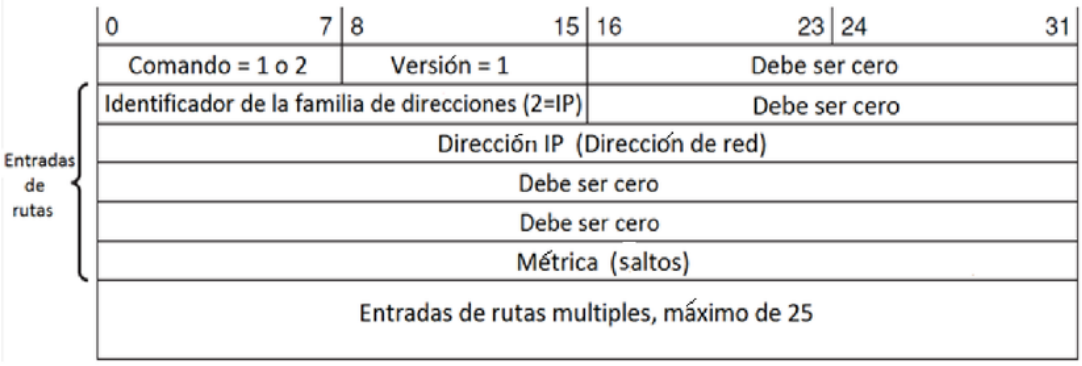


Figura 2.5. Formato del mensaje en RIPv1. Diagrama propio con base en referencia [48].

2.3.1.4 Tabla de enrutamiento de RIPv1

Cada host que implementa el protocolo RIPv1 tiene una tabla de enrutamiento, dicha tabla tiene una entrada para cada destino al que se puede acceder a través de RIPv1. Es importante que la tabla de enrutamiento de RIPv1 tenga al menos la siguiente información [49].

a. La dirección IP de destino, es decir, la red final a la que se desea acceder.
b. Una métrica, la cual representa el costo total de llevar un datagrama desde el router origen hasta el router destino. Como se comentó anteriormente, esta métrica en RIPv1 son saltos, es decir los saltos totales desde el router de origen hasta el router destino.

c. Siguiente salto o el siguiente router sobre el cual un paquete pasa para llegar a su destino, este será necesariamente un router vecino.
d. Un indicador o bandera para mostrar que la información sobre la ruta ha cambiado recientemente.
e. Temporizadores, los cuales indican el tiempo transcurrido desde que se ha recibido la última actualización de una ruta.

2.3.1.5 Funcionamiento de RIPv1

RIP utiliza dos tipos de mensajes especificados en el campo *Comando* los cuales son: mensaje de solicitud y mensaje de respuesta. Cada interfaz configurada por RIP envía un mensaje de petición al arrancar, solicitando que todos los vecinos que estén utilizando RIP envíen sus tablas de enrutamiento completas. Un mensaje de respuesta se envía de vuelta por los vecinos. Cuando el router solicitante recibe las respuestas éste evalúa cada entrada de la ruta y si una entrada de ruta es nueva, el router receptor instala la ruta en su tabla de enrutamiento, al contrario, si la ruta ya está en la tabla, la entrada existente se reemplaza si la nueva entrada tiene un mejor recuento de saltos. Entonces, el router de destino envía una actualización por disparo (triggered update), que son actualizaciones de la tabla de enrutamiento que se envían de manera inmediata en respuesta a un cambio en el enrutamiento. La actualización por disparo contiene información de todas las interfaces de RIP habilitadas para que de esta forma los vecinos estén informados de las nuevas rutas [50] [43].

El funcionamiento de RIP se ejemplifica en las figuras 2.6 a 2.8.

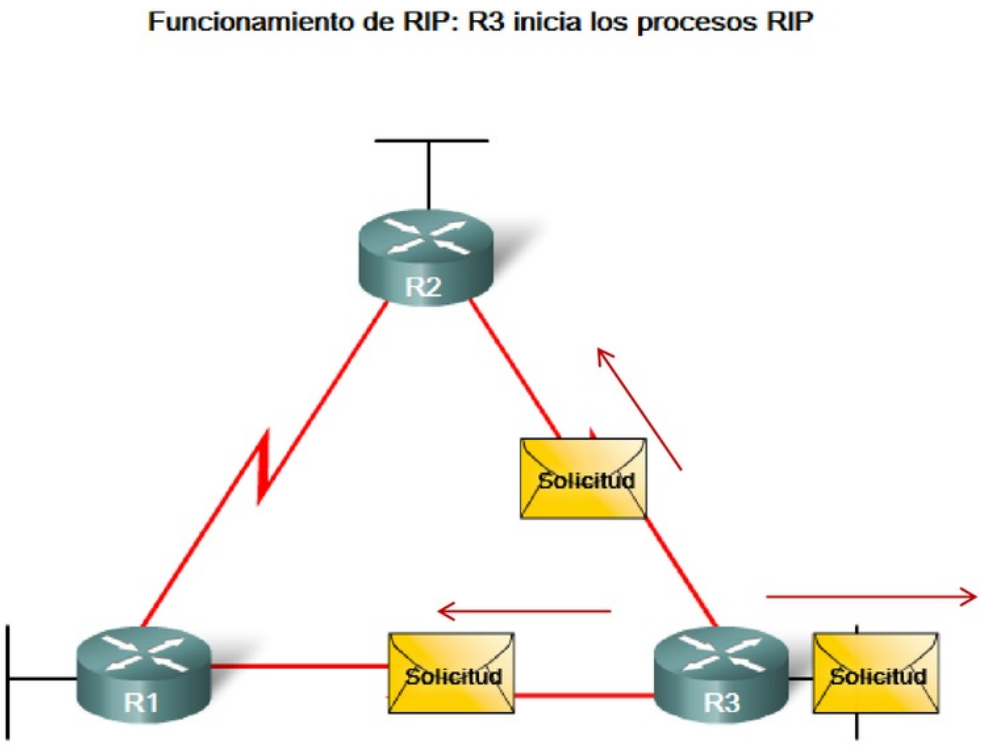


Figura 2.6. R3 envía un mensaje de solicitud a los vecinos. Diagrama con base en referencia [50].

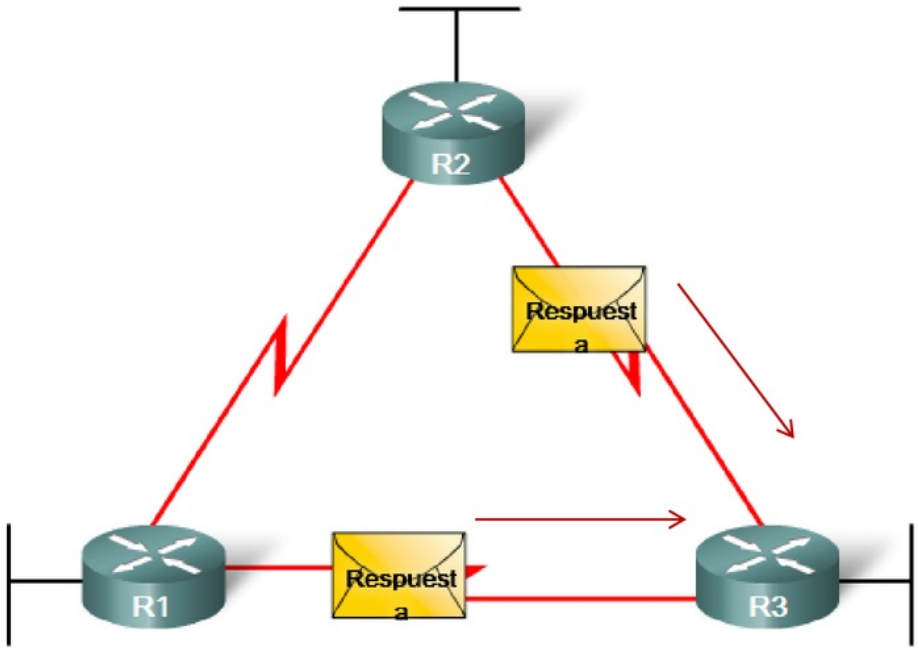


Figura 2.7 Los vecinos envían un mensaje de respuesta a R3. Diagrama con base en referencia [50].

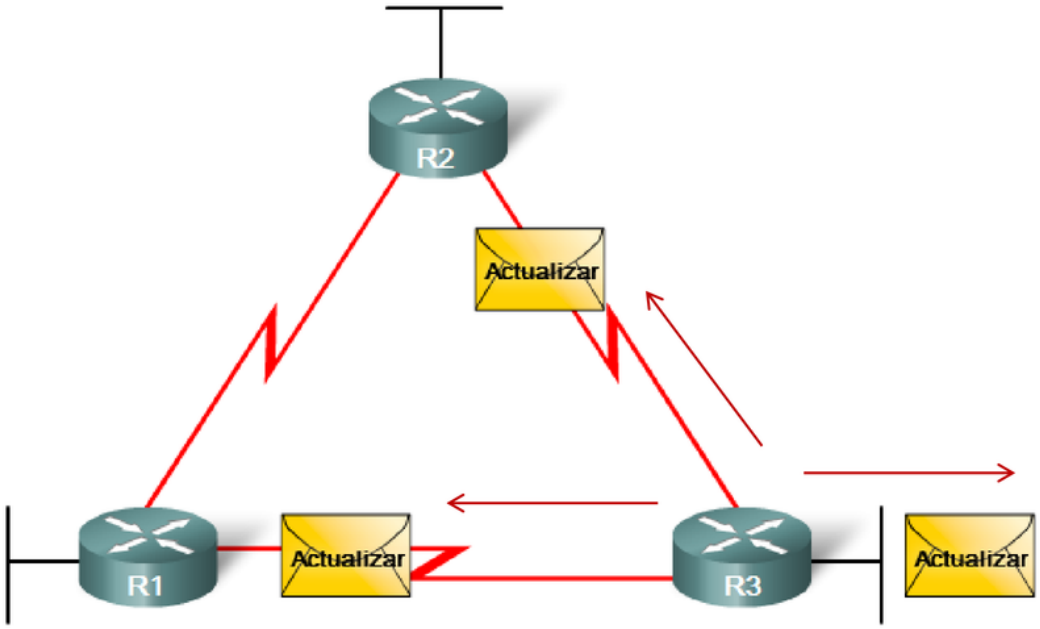


Figura 2.8 R3 envía mensajes de actualización a sus vecinos. Diagrama con base en referencia [50].

El proceso es simple ya que R3 envía una solicitud a sus routers vecinos, después los routers vecinos envían una respuesta a R3, por último, R3 envía actualizaciones a sus routers vecinos.

2.3.2. RIP v2

Diez años después de haberse publicado la primera versión de RIP, G. Malkin publicó la estandarización de RIPv2 en noviembre de 1998 en el RFC 2543. Esto para enfrentar las limitaciones que tenía la primera versión y hacer mejoras al protocolo. La primera versión de RIP tenía ciertas limitantes ya que no consideraba la interacción entre sistemas autónomos, no contaba con autenticación lo cual era algo inseguro y la más importante que no admitía el *subneting* entre redes ya que era un protocolo con clase, esto era un verdadero problema a la hora de comunicar dos topologías diferentes con máscaras de subred diferentes.

RIPv2 tiene las mismas características funcionales que la primera versión, sin embargo, hay ciertos cambios que son importantes de mencionar [47]:

a. Utilización de máscaras de subred, por lo que ya se pueden usar VLSM (Variable Lenght Subnet Mask) y puede haber una comunicación entre diferentes redes de diferentes topologías.
b. Envío de actualizaciones de tablas de enrutamiento de RIP mediante la dirección de multicast 224.0.0.9
c. Inclusión de RIPv2 en las bases de información de gestión (MIB)

d. Autenticación para la transmisión de información entre vecinos.

2.3.2.1. Formato del mensaje RIPv2

El formato de protocolo en la versión 2 de RIP es un poco diferente ya que se agregan algunos campos como:

a. Etiqueta de ruta. Se trata de un atributo asignado a una ruta cuyo uso previsto es proporcionar un método de separación de rutas para redes dentro del dominio de enrutamiento de RIP con respecto de rutas que pueden haber sido importadas de un EGP u otro IGP.
b. Máscara de subred. Permite que una máscara de 32 bits se incluya en la entrada de ruta de RIP. De esta manera, el router receptor ya no depende de la máscara de subred de la interfaz entrante ni de la máscara con clase al determinar la máscara de subred para una ruta, lo que permite intercambiar información con otras redes con diferente máscara de subred.
c. Siguiente salto. La dirección del siguiente salto se usa para identificar una dirección del siguiente salto mejor que la dirección del router emisor, si es que existe. Es la dirección IP donde se deben enviar los paquetes. El soporte para las direcciones del siguiente salto permite optimizar las rutas en un entorno que utiliza múltiples protocolos de enrutamiento.

RIPv2 entra dentro de los protocolos de enrutamiento sin clase, esto quiere decir que las máscaras de subred se incluyen en las actualizaciones de enrutamiento, lo que hace que RIPv2 sea más compatible con el *subnetting* del direccionamiento IP que la primera versión. En la figura 2.9 se muestra el mensaje de formato de RIPv2 [51] [52].

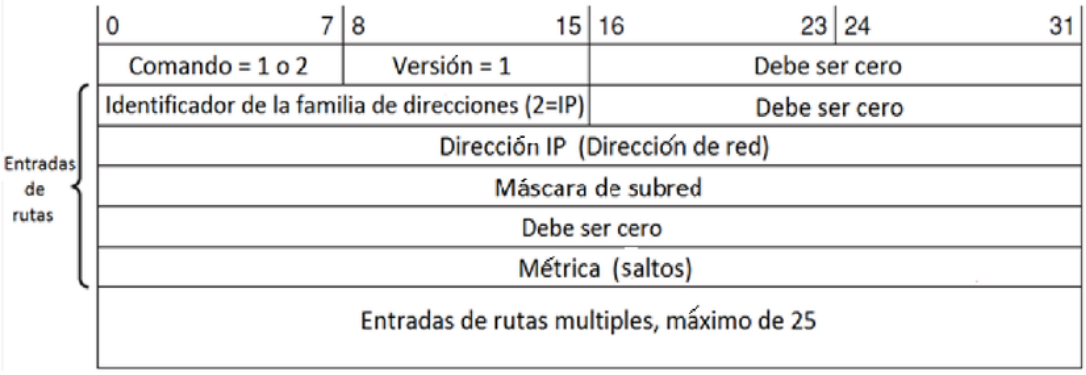


Figura 2.9. Formato del mensaje RIPv2. Diagrama propio con base en la referencia [49].

2.3.2.2 Autenticación de RIPv2

La autenticación de RIPv2 es muy importante ya que permite que haya seguridad cuando se transmitan los mensajes entre los routers. Un problema de seguridad de

cualquier protocolo de enrutamiento es la posibilidad de aceptar actualizaciones de enrutamiento no válidas. La fuente de estas actualizaciones de enrutamiento no válidas puede provenir de un atacante que intenta maliciosamente irrumpir en la red o trata de capturar paquetes engañando al router para que envíe sus actualizaciones al destino incorrecto. Cuando existe autenticación en RIPv2 el formato del mensaje agrega unos campos especiales que se muestran en la figura 2.10.

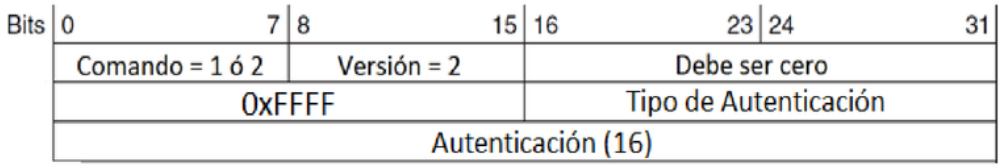


Figura 2.10. Campos agregados en el formato del mensaje de RIPv2. Diagrama propio con base a la referencia [51].

Como se puede observar se agrega un valor hexadecimal de 0xFFFF el cual señala que se ha activado la autenticación en RIPv2. Actualmente, el único tipo de autenticación es la contraseña simple de 2 octetos. Los 16 octetos restantes contienen la contraseña de texto sin formato o texto plano como se conoce en criptografía [51].

2.4 OSPF (Open Shortest Path First)

OSPF es un protocolo de enrutamiento que se clasifica dentro de los IGP. Esto significa que distribuye información de enrutamiento entre routers pertenecientes a un Sistema Autónomo único. El protocolo OSPF tuvo sus inicios en octubre de 1989 en el RFC 1131 con su primera versión. OSPFv1 fue experimental y nunca fue implementada ya que se realizó para reemplazar a RIPv1. El protocolo OSPF, en ambas versiones, se basa en algoritmos de estado-enlace, particularmente en el algoritmo matemático de Dijkstra [53].

Dado que la primera versión fue experimental, en 1991 salió la segunda versión del protocolo en el RFC 1247, la cual fue aplicada a las redes y en 1998 se publicó una actualización a dicha versión con el RFC 2328. A continuación, se presentan las características de estas dos últimas versiones de RFC [54] [55].

2.4.1 Características OSPFv2

OSPF a diferencia de RIP permite una mayor escalabilidad ya que no tiene el problema de los 15 saltos de RIP por otro lado OSPF para el cálculo de costos y rutas óptimas tiene en cuenta factores tales como el ancho de banda con lo cual permite elegir el camino más rápido de acuerdo a la velocidad del enlace [54].

Debido a su naturaleza de estado-enlace, los routers configurados con OSPF mantienen un resumen común de la red e intercambian su información de enlaces

desde un inicio hasta los cambios que ocurren en la red. OSPF tiene las siguientes características [55] [48]:

a. Escalabilidad. Ya que permite un modelo jerárquico que es posible conseguir mediante la utilización de distintas áreas, las cuales se mencionan en la sección 2.4.8.
b. Distancia administrativa de 110.
c. Conocimiento total de la topología de red. Como es un algoritmo de enrutamiento global tiene la información completa de la conectividad y costos.
d. Enrutamiento menos costoso. Permite configurar los costos de camino basándose en cualquier combinación de parámetros que tenga la red. Por ejemplo, ancho de banda, retraso (delay), y costo.
e. Sin limitaciones en la métrica de enrutamiento. Mientras que RIP restringía la métrica de routing a 16 saltos, OSPF no tiene restricción alguna a este respecto ya que no utiliza saltos sino ancho de banda.
f. Enrutamiento de múltiples caminos. Permite la utilización de múltiples caminos de igual costo que conectan a los mismos puntos. Se pueden utilizar estos caminos para conseguir un equilibrio (balancear la carga) lo que resulta en un uso más eficiente del ancho de banda de la red.
g. Enrutamiento de área. Al contar con un enrutamiento especifico, es decir, en un área determinada, disminuye los recursos (memoria y ancho de banda de la red) consumidos por el protocolo y proporciona un nivel adicional de protección en el proceso de enrutamiento.
h. Máscaras de subred de longitud variable (VLSM). Permiten fraccionar una dirección IP en subredes de tamaño variable, conservando el espacio de dirección IP.
i. Autenticación de enrutamiento. Proporciona seguridad adicional al proceso de enrutamiento.
j. Rápida convergencia. Ya que a diferencia de RIP solo se actualizan las rutas que han sido modificadas y estás son distribuidas por la red de forma rápida.

2.4.2 Formato del mensaje en OSPFv2

Para su enrutamiento la porción de datos de un mensaje OSPF se encapsula en un paquete. Antes de mostrar el encapsulamiento de OSPF se presentan los 5 tipos de mensajes que OSPF utiliza ya que dependiendo del mensaje será el formato del mensaje OSPF. Los tipos de mensajes se muestran en la tabla 2.2 [43].

Tipo	Nombre del paquete	Descripción
0x01	Hello	Es utilizado para establecer y mantener la adyacencia con otros routers vecinos que estén utilizando OSPF

0x02	DBD (DataBase Description)	Contiene una lista abreviada de la base de datos del Router de estado-enlace. Es decir, controla la sincronización de la base de datos entre routers.
0x03	LSR (Link-State Request)	Es una solicitud para más información acerca de una entrada DBD
0x04	LSU (Link-State Update)	Se usa para dar respuesta a las LSR así como para anunciar nueva información. Envía los registros de estado enlace específicamente solicitados
0x05	LSAck (Link-State Acknowledgement)	Confirma la recepción de una LSU y reconoce los demás tipos de paquetes

Tabla 2.2 Tipos de mensaje OSPF.

En la figura 2.11 se muestra el encapsulamiento de OSPF [43].

Encabezado de enlace de datos	Encabezado del paquete IP	Encabezado del paquete OSPF	Información específica del tipo de paquete OSPF

Figura 2.11. Encapsulamiento de OSPF. Diagrama propio con base en la referencia [43].

a. Encabezado de enlace de datos: Posee las direcciones MAC de origen y destino. La dirección MAC destino es multicast y puede ser 01-00-5E-00-00-05 o bien 01-00-5E-00-00-06.
b. Encabezado del paquete IP: Posee las direcciones IP de origen y destino. Esta última es una dirección multicast 224.0.0.5 o bien 224.0.0.6. El campo que indica el protocolo dentro del encabezado IP es 89 para OSPF.
c. Encabezado del paquete OSPF: Se incluyen el ID del router y el ID del área que se está configurando.
d. Información específica del tipo de paquete OSPF. Este campo de datos puede incluir uno de cinco tipos de mensajes OSPF vistos al inicio de la sección.

Una vez visto el encapsulamiento de OSPF es importante ver el formato del paquete OSPF, para esto se hace énfasis en el encabezado del paquete OSPF así como en el campo de Información específica del tipo de paquete OSPF. En la figura 2.12 se ejemplifica el formato del mensaje OSPF [55].

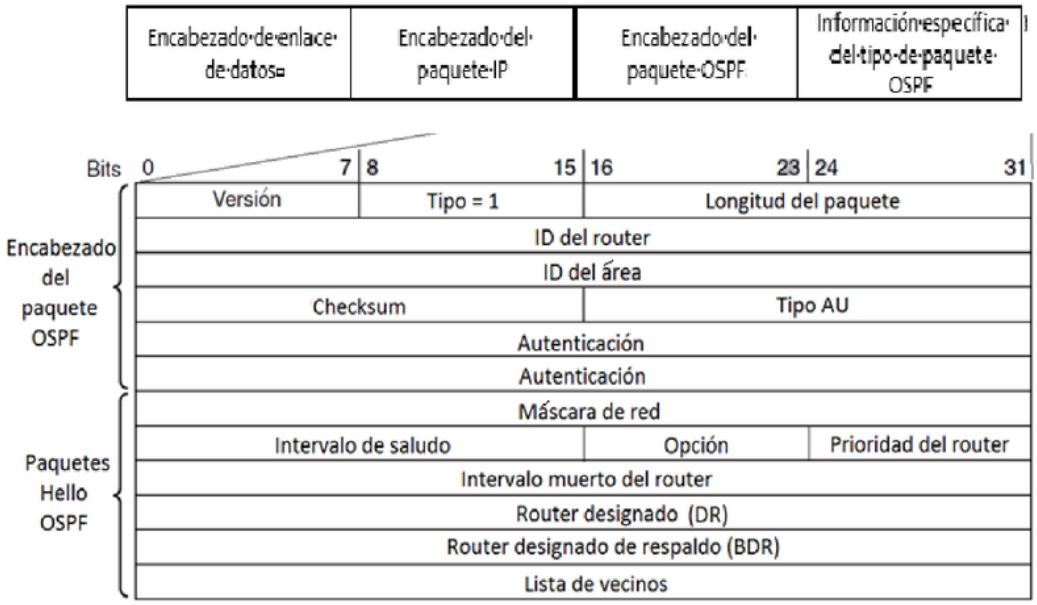


Figura 2.12. Formato de mensaje OSPF. Diagrama con base en la referencia [43].

Encabezado del paquete OSPF

(i) Versión. Especifica la versión de OSPF que se está utilizando.
(ii) Tipo. Especifica el tipo de paquete OSPF: Hello (1), DBD (2), LSR (3), LSU (4), LSAck (5)
(iii) ID del Router. ID del router de origen.
(iv) ID del área: Área en la que se originó el paquete.
(v) Longitud del paquete. Longitud del paquete OSPF incluyendo cabecera.
(vi) Checksum. Suma de verificación del paquete OSPF. Comprueba la integridad del paquete.
(vii) Tipo AU. Tipo de autenticación utilizada. Asegura que la autenticación sea la misma para ambos extremos.

Información contenida en el paquete Hello OSPF:

(i) Máscara de red: máscara de subred asociada con la interfaz emisora.
(ii) Intervalo de saludo: Cantidad de segundos entre los paquetes de saludo del router emisor. Generalmente 10.
(iii) Prioridad del router utilizada en la elección de DR/BDR (la cual se analizará más adelante)
(iv) Router designado (DR). ID del router del DR si existe. Cabe puntualizar que el DR es responsable de actualizar todos los demás routers OSPF cuando ocurre un cambio en la red, es decir, cuando se agregan más routers a la red.

(v) Router designado de respaldo (BDR). ID del router del BDR si existe. El BDR supervisa al DR y reemplaza a DR si el DR actual falla.

(vi) Lista de vecinos. Enumera la ID de los routers OSPF que han sido agregados a la red y tienen una comunicación bidireccional entre sí.

(vii) Opción. Se utiliza para redes que no son multi-acceso por ejemplo Frame Relay.

2.4.3 Funcionamiento de OSPF

OSPF se basa en el establecimiento de una adyacencia entre vecinos, para esto se envían paquetes Hello a través de la dirección multicast 224.0.0.5 y se descubre la vecindad entre los routers. Estos mensajes se envían cada 10 segundos. Una vez que haya una comunicación entre vecinos se pueden intercambiar las actualizaciones de enrutamiento, las cuales se almacenan en la tabla de enrutamiento [43].

Cuando los routers tienen conocimiento de toda la topología, se produce una adyacencia completa, para seguir teniendo esa adyacencia se siguen mandando paquetes Hello.

Para que haya una adyacencia es indispensable que los routers tengan en común tres parámetros: el tipo de la red ya sea de acceso múltiple, punto a punto ó una red de acceso múltiple sin broadcast (X.25, Frame Relay o ATM); el intervalo muerto, generalmente de 40 segundos para redes de acceso múltiple o punto a punto y 120 segundos para redes de acceso múltiple sin broadcast, es el periodo que espera el router antes de declarar al vecino inalcanzable; y el intervalo de saludo de 10 segundos para las redes de acceso múltiple y 30 segundos para las redes acceso múltiple sin broadcast [47].

La adyacencia es muy importante ya que permite saber si algún router se ha caído, esto se determina si el router ya no envía paquetes Hello. Por otra parte, debido a que los routers están sincronizados, si hay algún cambio lo comunicarán automáticamente. La adyacencia permite una convergencia más rápida porque entre los vecinos existe una comunicación permanente. El funcionamiento del paquete Hello llevado a cabo por el protocolo OSPF se muestra en la figura 2.13.

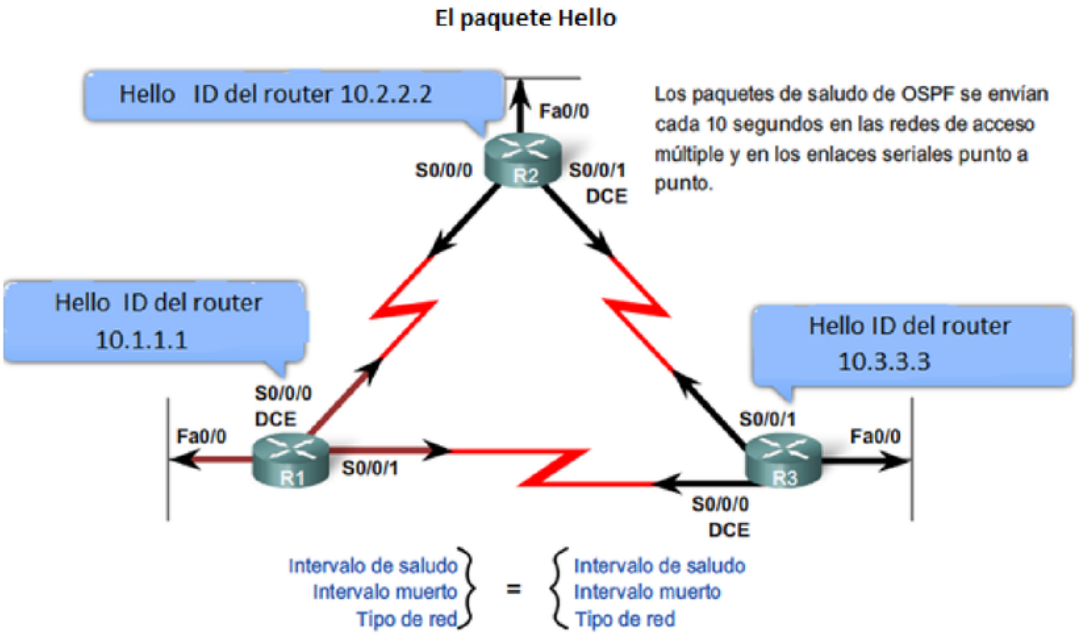


Figura 2.13. Funcionamiento del mensaje Hello y coincidencia de valores para formar una adyacencia. Diagrama con base en la referencia [50].

2.4.4 Funcionamiento de OSPF en un área

Como se había mencionado en la sección 2.4.1, OSPF puede funcionar en un entorno de áreas múltiples, es decir, OSPF permite que las redes contiguas y los host sean agrupados. A dicho grupo, junto con los routers que tienen interfaces a cualquiera de las redes incluidas, se le considera como un área. Cada área ejecuta una copia separada del enrutamiento de estado del enlace, esto significa que cada área tiene su propia base de datos del enrutamiento de estado enlace.

La topología de un área es invisible desde el exterior del área. Por el contrario, los routers internos de una zona dada no saben nada de la topología detallada del área externa. Este aislamiento del conocimiento entre áreas permite que el protocolo efectúe una reducción significativa en el tráfico del enrutamiento. El enrutamiento en un Sistema Autónomo se da en dos niveles, si la fuente y el destino de un paquete residen en la misma área, se utiliza el enrutamiento intra-área, si la fuente y el destino están en diferentes áreas se utiliza enrutamiento inter-área [55].

El funcionamiento de OSPF en un área inicia con el descubrimiento de un vecino y la creación de la adyacencia mediante la utilización de los paquetes Hello. Cuando un nuevo router es añadido a la red se intercambian paquetes Hello y la información de enrutamiento, con esto se construye una tabla de enrutamiento. Para esto se utilizan diferentes tipos de mensajes de petición y respuesta los cuales se muestran en la

tabla 2.2 de la sección 2.4.2. Además, se hace uso de una serie de estados de interfaces para formar la base de datos de OSPF. Los estados son los siguientes [55]:

Los primeros tres estados sirven para establecer una vecindad y adyacencia inicial:

1) Down. Es el estado inicial de una conversación entre vecinos. Eso indica que no se ha recibido información reciente del vecino. Se está a espera de iniciar el siguiente estado.
2) Init. En este estado, un paquete Hello ha sido visto por un vecino. Sin embargo, la comunicación bidireccional no se ha establecido con el vecino.
3) 2-way. En este estado, la comunicación entre los dos routers es bidireccional. Esto ha sido asegurado por la operación del protocolo Hello. Este es el estado más avanzado del establecimiento de adyacencia inicial.

Los estados siguientes sirven para establecer un intercambio de rutas:

4) Exstart. El objetivo de este estado es decidir qué router es el maestro y que otro será el esclavo, el maestro será el que tenga el router ID más alto y empezará a transmitir datos, por otro lado el esclavo quedará en espera de la recepción del mensaje enviado por el maestro.
5) Exchange. En este estado el router utiliza paquetes DBD, para enviarle al otro router su información de la base de datos de estado enlace.
6) Loading. Si el router receptor necesita más información de la que ya ha recibido, deberá solicitar más mediante un mensaje LSR, de esta manera el primer router contestará con un mensaje LSU.
7) Full. En este estado los enrutadores vecinos son totalmente adyacentes. Estas adyacencias aparecerán ahora en los LSAck del router.

Para ejemplificar lo anterior se presenta la figura 2.14.

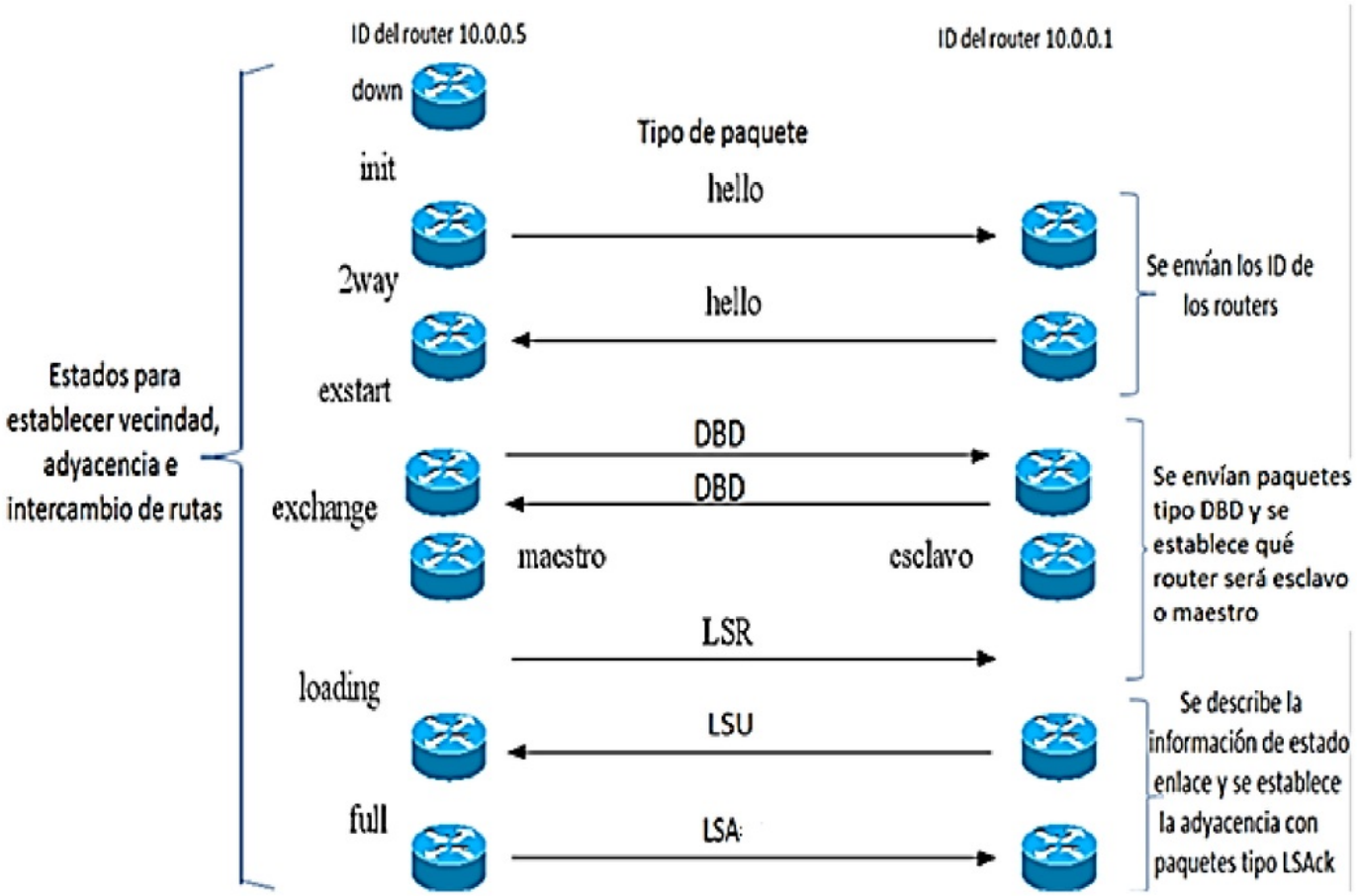


Figura 2.14. Descubrimiento de vecindad, adyacencia y rutas entre routers. Diagrama propio con base en la referencia [47].

2.4.5 Métrica en OSPF [43] [50]

A principios de la sección referente a OSPF se estableció que tenía una métrica diferente a RIP. Debido a que OSPF no utiliza saltos debe considerar otros parámetros, es por eso que en OSPF se manejan costos como métricas. Un costo se asocia con el resultado de la ecuación (1) del ancho de banda de cada interfaz del router. De igual forma el costo puede ser configurado por el administrador del sistema. Cuanto más bajo sea el costo, más probabilidad hay de que la interfaz sea utilizada para enviar tráfico de datos. El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino. Un parámetro común para el cálculo del costo es el ancho de banda de la interfaz. La fórmula utilizada para calcular el costo es la siguiente:

$$Costo = Ancho\ de\ banda\ de\ referencia / Ancho\ de\ banda\ de\ la\ interfaz \quad (1)$$

Donde

Ancho de banda de referencia: es por defecto 10^8 o 100 Mbps. El ancho de banda de referencia puede modificarse para adaptarse a redes con enlaces más rápidos que 100 Mbps.

Ancho de banda de la interfaz: es variable dependiendo la velocidad del enlace de la interfaz.

En la tabla 2.3 se muestran los anchos de banda de diferentes enlaces que existían cuando se desarrolló el RFC de OSPF.

Tipo de interfaz (BW)	Asignación de costo
Giga Ethernet	10^8 / 1000000000 ➔1
Fast Ethernet	10^8 / 100000000 bps ➔ 1
Ethernet	10^8 / 10000000 bps ➔ 10
E1	10^8 / 2 048 000 bps ➔ 48
T1	10^8 / 1 544 000 bps ➔ 64
128 kbps	10^8 / 128 000 bps ➔ 781
64 Kbps	10^8 / 64 000 bps ➔ 11562
56 Kbps	10^8 / 56 000 bps ➔ 1785

Tabla 2.3. Cálculo de los costos con diferentes tipos de enlaces.

2.4.6 Topologías OSPF

OSPF define 5 tipos de topologías para su enrutamiento, las cuales se describen a continuación.

a) Acceso múltiple con broadcast. En este tipo de redes OSPF envía tráfico de multicast, es necesario establecer un DR y un BDR. Algunos ejemplos son LAN Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface). En la figura 2.15 se muestra un ejemplo de red de acceso múltiple con broadcast [45].

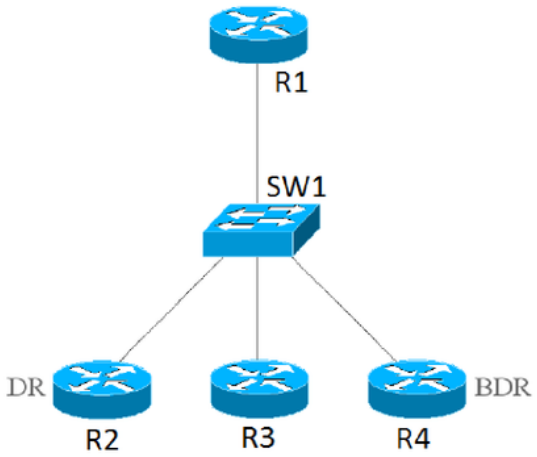


Figura 2.15. Topología acceso múltiple con broadcast. Diagrama con base en la referencia [47].

b) Punto a punto. Se utiliza cuando el router está conectado directamente a otro. Por ejemplo, una conexión es serie. En la figura 2.16 se ejemplifica dicha conexión.

Figura 2.16. Topología punto a punto vía serial. Diagrama con base en la referencia [45].

c) NBMA (Non Broadcast Multi Access). También conocida como acceso múltiple sin broadcast, se apoya en enlaces punto a punto ya sea parciales o totales ya que OSPF envía un broadcast para cada uno de los enlaces. Requiere una configuración manual de DR, BDR y de los vecinos. Un ejemplo de NMBA es Frame Relay. Como se muestra en la figura 2.17.

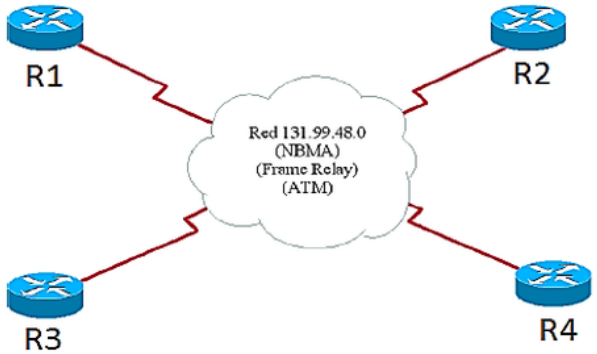


Figura 2.17. Topología NMBA o de acceso múltiple sin broadcast. Diagrama con base en la referencia [47].

d) Punto a multipunto. En esta topología una interfaz (R3) se conecta a múltiples interfaces (R4, R2, R1) mediante Frame Relay, en esta topología no existe el DR y BDR. En la figura 2.18 se muestra un ejemplo de la topología punto a multipunto.

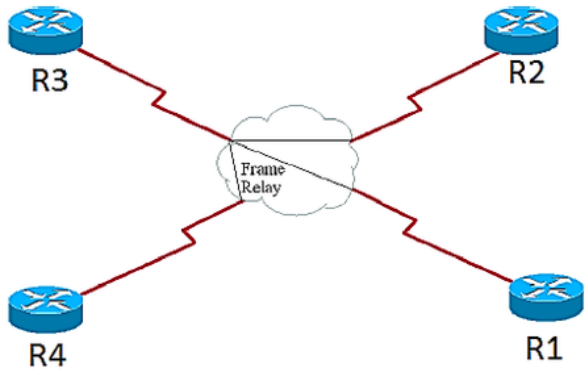


Figura 2.18. Topología punto a multipunto. Diagrama con base a la referencia [47].

e) Enlaces virtuales. Son conexiones virtuales que no tienen ninguna conexión con el área de backbone. OSPF trata a estos enlaces como conectados al área 0, ya que se crean túneles en el enlace virtual.

2.4.7 OSPF en múltiples áreas

La utilización de áreas es posible en OSPF gracias a la naturaleza del protocolo que es de estado enlace y el enrutamiento jerárquico, esto permite que los routers compartan la misma información de sus bases de datos, lo que da pauta a la utilización de áreas ya que se considera jerárquico. Un área en OSPF es una colección de routers que ejecutan el protocolo con una base de datos común. Un área es una división de un AS, si dividimos la red en áreas se reduce el tráfico en la red, así como la cantidad de procesamiento y uso de memoria de los routers. En OSPF el área 0 está reservada para el backbone por lo que no puede usarse para otro fin [43].

La utilización de múltiples áreas se da porque una única área ya no es lo suficientemente manejable o por que se espera un crecimiento en la red.
Para el enrutamiento OSPF en múltiples áreas se tienen diferentes tipos de routers que hacen posible que la información fluya de un área a otra [56] [47]:

1. Routers internos. Todos los routers dentro de un área disponen de exactamente la misma base de datos de estados de enlace, estos son conocidos como routers internos (IR). Todas sus interfaces están en la misma área.
2. Router de backbone. Los routers que corresponden a varias áreas y que conectan dichas áreas al área de estructura básica se denominan routers de borde de área (ABR). Sus interfaces están en diferentes áreas. Este tipo de

routers permite el resumen de direcciones IP, es decir, reduce un rango de direcciones IP a una sola para que la tabla de enrutamiento sea más corta y se optimicen los recursos de los routers.

3. ASBR (Autonomous System Border Route). Conecta la red OSPF con una red externa. Es un router que intercambia información de enrutamiento con routers pertenecientes a otros AS.

La figura 2.19 muestra una topología de red con 2 áreas con routers internos (IR) y una de backbone con routers de backbone (ABR) así como un AS que proporciona acceso a Internet.

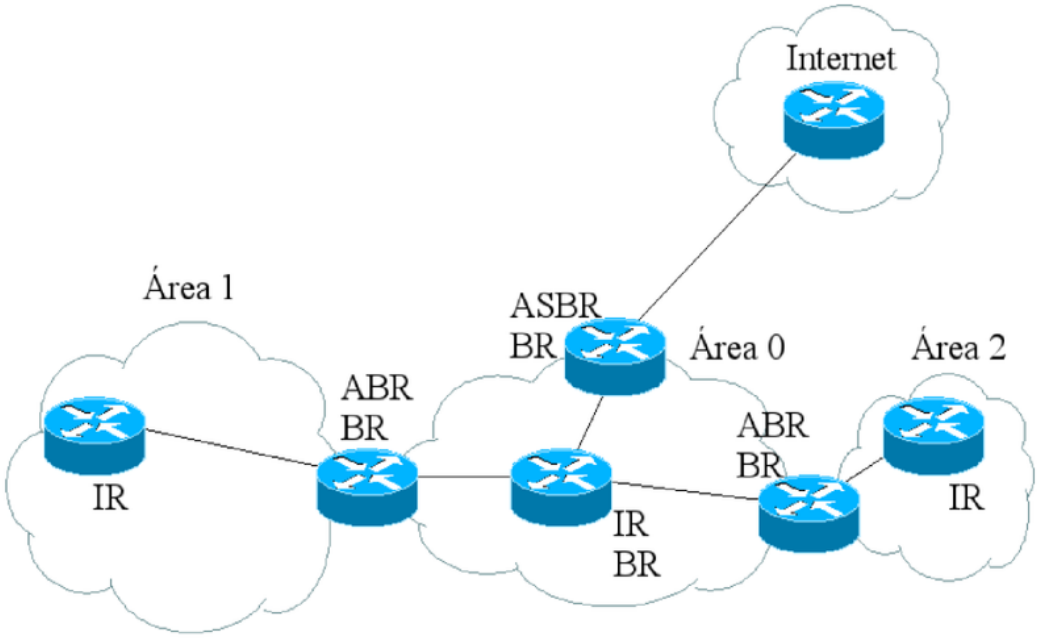


Figura 2.19. Topología de red con múltiples áreas. Diagrama con base en la referencia [47].

2.4.8 Tipos de áreas en OSPF

En OSPF existen 6 tipos de áreas que pueden ser utilizadas de acuerdo a los diferentes tipos de topologías o características de los routers y enlaces.

El número de routers por área es variado basado en los factores de la red, pero según Cisco es recomendable utilizar sólo 30 routers por área. Por otro lado es recomendable que un router no debe estar en más de 3 áreas [56].

Para presentar los tipos de áreas en OSPF es necesario introducir los tipos de LSA (Link-state Advertisement) que maneja OSPF. Los LSA son mensajes de estado-enlace que OSPF envía para la construcción de la base de datos de los estados de enlaces. Los LSA son de diferentes tipos dependiendo del tipo de Router que se utilice, dichos routers fueron descritos en la pasada sección. En la tabla 2.4 se muestran los diferentes tipos de LSA y su descripción [56].

Tipo de LSA	Descripción
1	LSA de Router
2	LSA de red
3 y 4	LSA de tipo resumen
5	LSA Externas
6	LSA de multicast
7	LSA para NSSA (Not-So-Stuby-Area)
8	LSA de atributos externos para BGP
9, 10 o 11	LSA opacas

Tabla 2.4 Tipos de LSA

a) LSA tipo 1. Son generados por todos los routers en un área para describir los enlaces que están directamente conectados, figura 2.20.

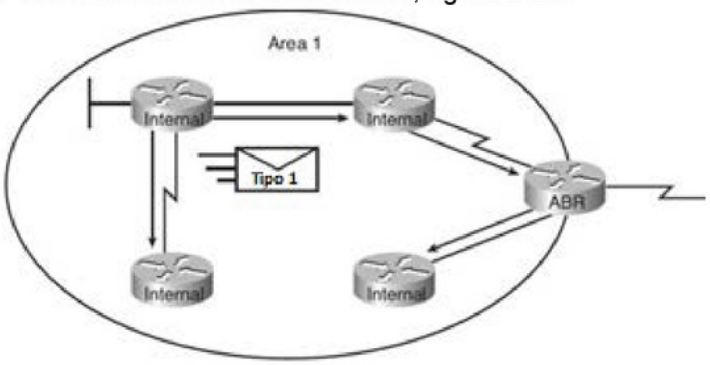


Figura 2.20. LSA de tipo 1. Diagrama tomado de la referencia [56].

b) LSA tipo 2. Un LSA de tipo 2 enumera cada uno de los routers conectados que componen el área, incluyendo el DR así como la máscara de subred del enlace. Los LSA de tipo 2 nunca cruzan el límite de un área, figura 2.21.

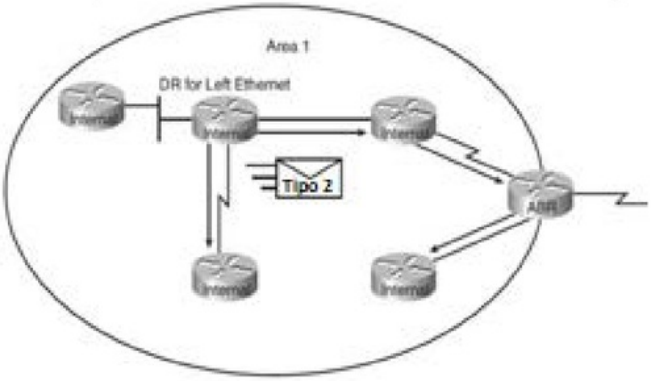


Figura 2.21. LSA de tipo 2. Diagrama tomado de la referencia [56].

c) LSA tipo 3. Son enviados de un área a otra a través de los ABR, describen su conexión del ABR con su área y publica las rutas asociadas de una manera más resumida, figura 2.22.

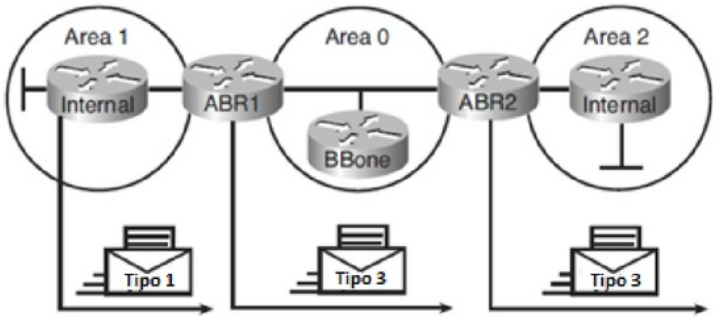


Figura 2.22. LSA de tipo 3. Diagrama tomado de la referencia [56].

d) LSA de tipo 4. Es generado por el ABR del área de origen para anunciar un ASBR hacia todas las demás áreas de un AS, figura 2.23.

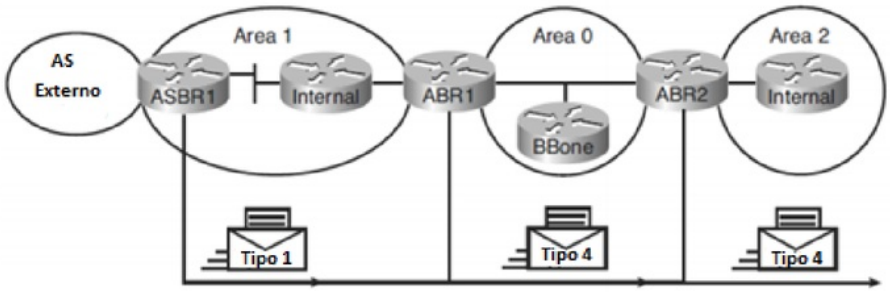


Figura 2.23. LSA de tipo 4. Diagrama tomado de la referencia [56].

e) LSA de tipo 5. Es Utilizado por el ASBR de origen para anunciar redes de otros AS, figura 2.24.

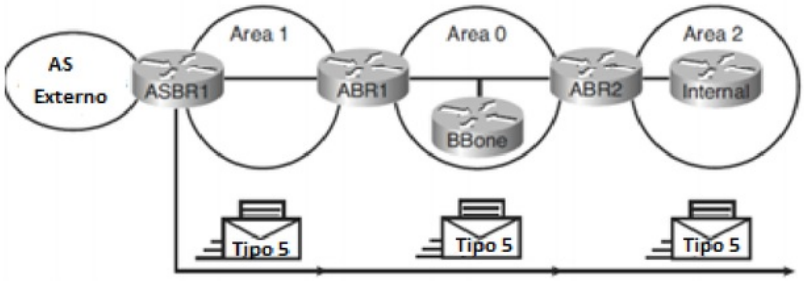


Figura 2.24. LSA de tipo 5. Diagrama tomado de la referencia [56].

f) LSA de tipo 6. Son diseñadas especialmente para multicast.

g) LSA de tipo 7. Generadas por un ASBR dentro de un área NSSA, la cual es una área que permite añadir rutas externas de forma limitada en dicha zona para describir las rutas redistribuidas en la NSSA. Los LSA de tipo 7 se traducen en LSA de tipo 5 cuando sale de la NSSA, figura 2.25.

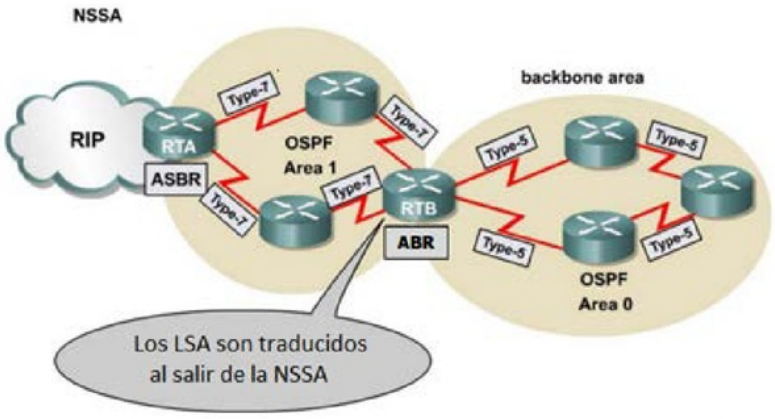


Figura 2.25. LSA de tipo 7. Diagrama tomado de la referencia [56].

h) LSA de tipo 8. Son exclusivos para transportar información BGP (Border Gateway Protocol) dentro de un dominio OSPF.

i) LSA de tipo 9, 10 y 11. Son exclusivos para usos futuros particularmente MPLS (Multiprotocol Label Switch)

Una vez definidos los tipos de LSA podemos introducir los tipos de áreas en OSPF [56].

1) Área Backbone. Son áreas especiales para backbone, se le conoce como área de tránsito y es identificada como área "0".
2) Área Estándar o comúnmente área. Es un área con características básicas, permite actualización de enlaces y el resumen de rutas, dicho resumen permite enviar diferentes rutas a través de una sola publicación de ruta, con este resumen se puede ahorrar ancho de banda y procesamiento de la CPU. Es importante mencionar que las áreas de tipo estándar se dividen a su vez en 4 tipos de áreas llamadas áreas stub. En la figura 2.26 se muestra la interacción entre áreas de backbone y áreas estándar.

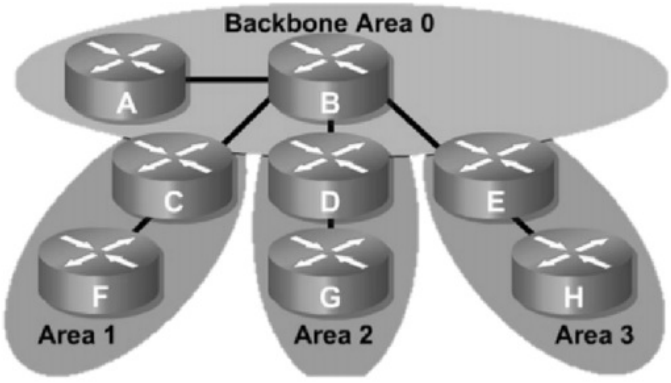


Figura 2.26. Diagrama propio con base en la referencia [56].

2.5 Protocolo de gestión SNMP

En los primeros días de las redes compartidas, cuando las redes de computadoras eran artefactos de investigación en lugar de una infraestructura fuerte utilizada casi por cada persona alrededor del mundo como lo es ahora la Internet, la gestión de red era prácticamente desconocida. Cada vez que un administrador de red encontraba un problema en la red sólo bastaba ejecutar algunos comandos ping para localizar la fuente del problema y luego modificar la configuración del sistema, reiniciar software o cambiar hardware, o simplemente llamar a un colega para comprobar la consola en la sala de máquinas.

A medida que la Internet e Intranets (redes privadas) han crecido comenzando desde redes pequeñas transformándose a una gran infraestructura global, de igual forma la necesidad de gestionar de manera más sistemática el enorme número de componentes de hardware y software dentro de estas redes se ha vuelto más importante.

La gestión de redes consiste en la monitorización, el sondeo, configuración, evaluación, análisis y control de los recursos de una red, todo esto para hacer que la red sea más eficiente y sea capaz de dar un mejor servicio al usuario [57].

Antes de SNMP (Simple Network Management Protocol), la mayoría de los dispositivos de red tenían una gestión como elementos individuales, y sólo se podían administrar con un software patentado que dependía del proveedor, de esta manera se presentó una falta de funcionalidad e interoperabilidad, esto se tradujo en implementaciones de gestión excesivamente complejas ya que se requería el uso de muchos sistemas de gestión y así, para los administradores de red la resolución de problemas se tornó muy difícil debido a que no contaban con la posibilidad de tener una vista completa de la red.

2.5.1 Historia y componentes de SNMP

SNMP surgió a partir de un protocolo anterior; Simple Gateway Monitoring Protocol (SGMP), el cual define algunos elementos tales como tipo de interfaces y el estado de las mismas, el protocolo de ruteo que se está usando así como el tipo de ruta, ya sea local o remoto [58].

Es entonces que a finales de 1980 con el apoyo de la IETF, SNMPV1 se diseñó para tener un mayor control en las redes complejas de múltiples proveedores. Simple Network Management Protocol es un protocolo estándar de Internet para administrar dispositivos en redes IP como switches, impresoras en redes IP, routers, etc. En otras palabras es un protocolo estándar que se encarga de monitorear hardware y software de cualquier marca y cualquier sistema operativo. SNMP parte del protocolo TCP/IP y utiliza UDP como protocolo de transporte. Los principales componentes de

SNMP son: el administrador de SNMP, el agente SNMP y los dispositivos administrados. En la figura 2.27 se muestran los componentes básicos de SNMP.

Figura 2.27. Componentes básicos de SNMP [59].

En SNMP el usuario recibe alertas a través de una estación de administración también llamada solución de monitoreo que a su vez extrae estadísticas de rendimiento de servidores y dispositivos de red, el administrador de SNMP envía una solicitud al agente que a su vez pasa la solicitud a los dispositivos administrados. Estos dispositivos responden a las solicitudes en espera y envían los resultados necesarios al administrador SNMP como se muestra en la figura 2.28 [59].

Figura 2.28 Diagrama típico de la arquitectura SNMP dentro de una red IP [59].

2.5.2 Funcionamiento SNMP

Para entender mejor el funcionamiento se explican a detalle los componentes de SNMP [59].

A. **Los dispositivos administrados:** pueden ser cualquier tipo de dispositivo de red que está presente en la misma, tales como routers, switches , firewall, sensores de temperatura, UPS; también puede ser cualquier servidor físico o virtual y cualquier sistema operativo. En resumen, cualquier dispositivo que pertenezca a una red IP y un agente SNMP.

B. **El agente SNMP:** cada fabricante de hardware configura el agente SNMP en el dispositivo administrado, la principal responsabilidad es recolectar información administrativa sobre su entorno local. El agente SNMP almacena y recupera información tal y como se definió en la MIB (Management Information Base), que es una base de datos a través de la cual se tiene acceso a la información para la gestión y es el fabricante quien posee la MIB de un dispositivo. La MIB es una estructura de datos que describe a los elementos de la red SNMP como una lista de objetos de datos. De esta forma el agente SNMP indica al administrador cuándo se produce un evento.
Algunos ejemplos de agentes SNMP pueden ser los dispositivos Cisco los cuales incluyen el agente SNMP de Cisco, los sistemas operativos Unix y Linux que vienen equipados con paquetes NET-SNMP y en los sistemas operativos Windows el agente SNMP está deshabilitado por defecto pero se puede habilitar.

C. **Administrador SNMP,** tambien conocido como NMS (Network Management System): la función del administrador SNMP es recolectar información administrativa de los agentes SNMP de los dispositivos administrados y almacenarla de una manera más legible, puede ser cualquier protocolo de monitoreo de red como Opmanager o Solarwinds. De igual forma puede ser cualquier solución de monitoreo de red como NMS (Network Management System) el cual ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados, y EMS (Elements Management Systems) [59].

Por otro lado los parámetros de SNMP son:

- **Una OID** (Object Identificator) que es un identificador de objeto y cuenta con los siguientes atributos:
  i. Puede reunir información acerca de un dispositivo con SNMP activado.
  ii. Se identifica por nombres denominados nombres de objeto.
  iii. Cada OID tiene un tipo de dato que puede ser un valor de contador, una cadena de caracteres, un entero o un valor de medida.
  iv. El nivel de acceso es de lectura/escritura.
  v. Puede proporcionar cierta variedad de información como por ejemplo: estado de la interfaz, trafico Rx-Tx, errores, información del proceso como ruta, ID, CPU, memoria total utilizada o disponible, y espacio en disco total utilizado o disponible.
  vi. Cada uno de ellos es un OID ya que tiene un nombre de objeto y cada OID tiene diferentes tipos de datos.
  vii. Los OID se definen en las MIB cada uno es único y especifico a un dispositivo.
  viii. Son escalares o tabulares al igual que la disponibilidad del sistema que es escalar y la información de interfaz es tabular.
  ix. Los OID normalmente se presentan como una lista de puntos enteros.

- **Una MIB** (Management Information Base) es una base de información gestionada que tiene las siguientes características [59]:
  i. Es un conjunto de OID.
  ii. El agente de SNMP del dispositivo administrado mantiene una base de datos de información que describe los parámetros de este dispositivo. Algunos ejemplos de estos parámetros son: CPU, memoria, discos, procesos, estadísticas de interfaz, etc.
  iii. El agente SNMP recupera el valor de la información requerida de la MIB cuando el administrador SNMP lo requiere.
  iv. Define los objetos gestionados que un administrador de SNMP puede requerir del agente SNMP, en otras palabras es un conjunto de preguntas que un administrador SNMP puede preguntar al agente.
  v. Está compuesta por objetos gestionados que se identifican mediante un OID.
  vi. Hay dos tipos de MIB; pueden ser estándares como RFC y MIB personalizadas o privadas como las que proveen los fabricantes de dispositivos como Cisco, HP, Huawei, Juniper, Alcatel-Lucent, etc.

2.5.3. Diagrama de árbol de una MIB

A continuación se muestra el diagrama de árbol de una MIB en donde se pueden apreciar las ramificaciones que hay entre los diferentes niveles, el árbol MIB comienza en el nivel raíz y en el nivel ISO es donde comienzan las ramificaciones hacia los distintos niveles. Con base en el árbol de la figura 2.29 se puede encontrar el OID para la Sun-Platform-MIB. Siguiendo las ramificaciones del árbol se tiene: 1.3.6.1.4.1.42.2.70.101 que es equivalente a ISO.org.dod.Internet.Private.enterprises.sun.products.Sunfire.sun-platform-MIB [59].

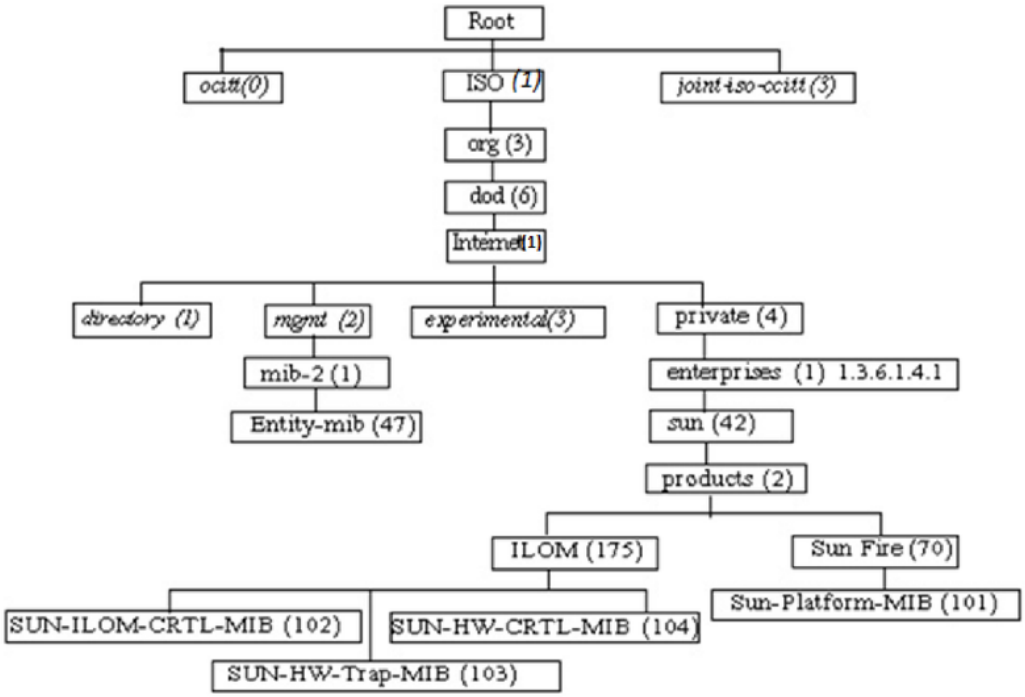


Figura 2.29. Diagrama de árbol de una MIB [59].

2.5.4 Trap SNMP

Las Trap son notificaciones asíncronas, enviadas desde el agente SNMP al administrador que informan sobre los eventos que suceden en el dispositivo administrado, es decir, se usan para capturar errores e indicar dónde se encuentran. Estas incluyen el SysUpTime actual, un OID que identifica el tipo de Trap y enlaces de variables opcionales [60].

Con el fin de capturar como Trap eventos específicos en el dispositivo administrado, es importante especificar la dirección de destino de las Trap que deben recolectarse. Las MIB contienen las variables de configuración de Trap, las Trap escuchan en el puerto 162 UDP.

2.5.5 Mensaje SNMP

12

En el mensaje SNMP podemos diferenciar claramente tres campos:

- Versión: version del protocolo SNMP, v.1, v.2 o v.3
- Comunity: la función de este campo es enviar junto con la tarea que se pretende llevar a cabo una identificación básica del usuario. Su fin es controlar el acceso no autorizado a un dispositivo SNMP.
- Protocol Data Unit (PDU): en el espacio PDU son anotadas las peticiones que el usuario quiere efectuar sobre un dispositivo -operaciones SNMP- y los

mensajes desde el agente hacia el usuario. En la figura 2.30 se muestran los diferentes tipos de mensajes de SNMP.

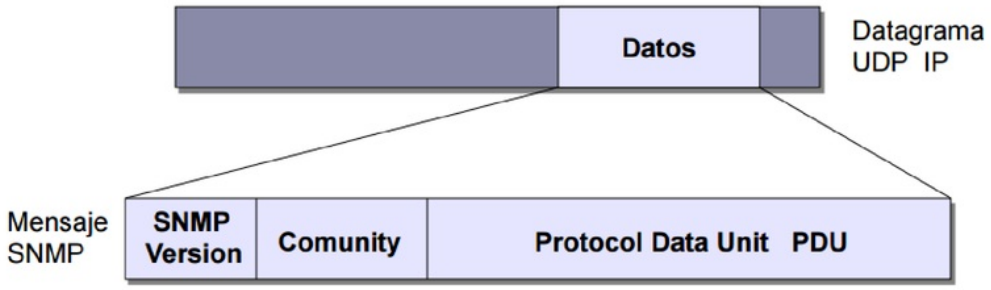


Figura 2.30. Mensaje SNMP (parece diferente letra)

2.5.6 Comunicación SNMP

El proceso de comunicación SNMP se ejemplifica en la figura 2.31, dicho proceso comienza con el administrador SNMP el cual recibe Trap o informes y reune toda la información de desempeño del agente SNMP en el dispositivo gestionado (servidor, router, switch, PC), cada dispositivo cuenta con un agente SNMP y éste tiene definiciones en administración y una base de datos en forma de MIB.

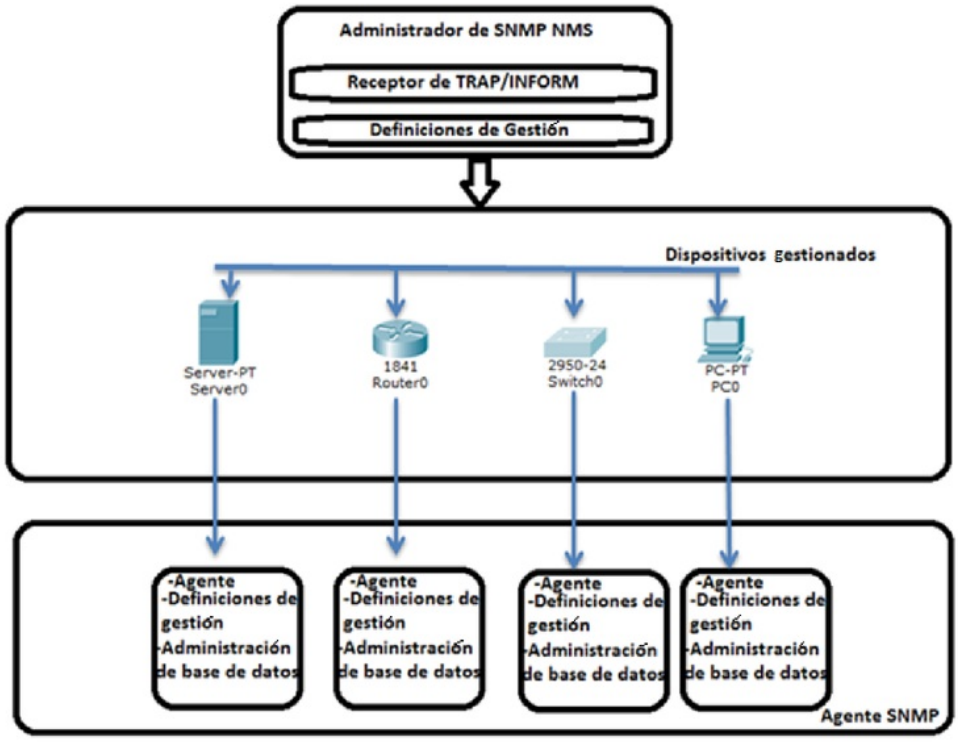


Figura 2.31. Diagrama de comunicación SNMP.

2.5.7 Versiones de SNMP

Actualmente existen 3 tipos de versiones SNMP que se describen a continuación:

2.5.7.1 SNMP v1

Es la implementación inicial de SNMP, opera sobre protocolos y servicios tales como: UDP, IP, Appletalk-Datagramas Delivery Protocols (DDP), CLNS (Connectionless-mode Network Service), entre otros. Es ampliamente utilizado y es el protocolo de red de facto, está disponible desde 1988. SNMP es un protocolo de Petición/Respuesta, el sistema de gestión de red emite una solicitud y los dispositivos gestionados devuelven respuestas [57] [59]. Este comportamiento se implementa usando una de las operaciones de protocolo siguientes:

GET: es utilizada por los NMS para recuperar el valor de una o más instancias de un agente. Si el agente que responde a la operación GET no puede proporcionar valores para todos los objetos de petición de una lista, no regresa ningún valor.

GETNEXT: es utilizada por el NMS para recuperar el valor del siguiente objeto de una tabla o lista dentro de un agente.

SET: es usada por el NMS para establecer los valores de objetos dentro de un agente.

Las desventajas de SNMP v1 son la autenticación de la fuente del mensaje y la protección de estos mensajes de la divulgación y la colocación de los controles de acceso sobre la base de datos MIB. En cuestiones de seguridad SNMPv1 utilizaba solo una forma de seguridad que eran los *nombres de comunidad*, los cuales son similares a las contraseñas ya que los agentes se pueden configurar para responder a las consultas recibidas solamente por los nombres de comunidad aceptadas.

2.5.7.2 SNMP v2

Fue diseñado en 1993, las operaciones GET, GETNEXT y SET son las mismas que en la primera versión. Es una modificación de la versión 1, en esta versión se incorporan 2 nuevas operaciones:

GETBULK tiene mejoras en el desempeño y seguridad en las comunicaciones entre administradores. Es usada por los NMS para recuperar eficientemente grandes bloques de datos.

INFORM: permite a un NMS enviar información del Trap a otro NMS. En esta versión si el agente reacciona a las operaciones GETBULK y no puede proporcionar valores para todas las variables de una lista, proporcionará resultados parciales.

En cuestiones de seguridad SNMPv2 trajo más seguridad adicional, en primer lugar todo el paquete a excepción de la dirección destino está cifrado. Dentro de los datos cifrados están el nombre de la comunidad y la dirección IP de origen [61] [62].

2.5.7.3 SNMP v3

En 2002, debido a la escasa seguridad principalmente en la autenticación y privacidad se produjo SNMP v3 ya que se necesitaba un protocolo de gestión de red más seguro. Esta versión agrega mejoras en la seguridad y en la comunicación remota [63].

Cada entidad SNMP tiene un identificador SNMP_ENGINE_ID, esto hace que la comunicación sea únicamente posible si la entidad SNMP conoce la identidad de su par. SNMPv3 soporta modelos de seguridad y contiene especificaciones para USM (User Security Model) es decir para un modelo de seguridad basado en usuario y el modelo de control de acceso VACM (View-based Control Model) para el control de acceso. Esta versión introduce la posibilidad de configurar dinámicamente el agente SNMP, esta configuración permite agregar, eliminar y modificar las entradas de configuración de forma local o remota. Los mecanismos estándar de comunicación disponibles en el modelo de seguridad basado en usuarios son:

- Comunicación sin autenticación y privacidad – NoAuthNoPriv
- Comunicación con autenticación y sin privacidad – AuthNoPriv
- Comunicación con autenticación y privacidad – Auth Priv

El USM protege al usuario contra 4 amenazas: *modificacion de la información, información falsa (enmascaramiento), modificación de secuencia de mensajes y revelación de información* [63].

Los protocolos de autenticación soportados en USM son: MD5 (Message Digest Algorithm), SHA (Security Hash Algorithm) y los protocolos de privacidad soportados son: CBC_DES (Data Encrytion System in Cipher Block Changing), CFB_AES_128 (Advanced Encryption System Cipher Feedback) [65].

2.5.7.3.1 Características de SNMPv3

Brinda un entorno seguro para la administración de sistemas, cubriendo los siguientes aspectos:

A. Procedimiento de sincronización de tiempo la cual facilita la autenticación de la comunicación entre las entidades SNMP.

B. Framework MIB SNMP el cual facilita la configuración remota y la administración de la entidad SNMP.
C. MIB USM para el módulo de seguridad de usuarios las cuales facilitan la configuración remota y la administración de los módulos de seguridad.
D. MIB VACM las cuales facilitan la configuración remota y la administración de los módulos de control de acceso.
E. Brinda objetivos de seguridad que incluyen protección contra la modificación de la información, modificación en el flujo de mensajes, difusión, etc.

Esta versión de SNMP trata los problemas relacionados con las implementaciones a gran escala de SNMP, los registros de actividad y la administración de fallas, además se enfoca principalmente en la seguridad a través de la encriptación y autenticación de la información de igual forma en la administración mediante originadores de notificaciones y re-direccionadores de proxy para una mejor gestión.

La implementación de SNMPv3 cuenta con una seguridad muy fuerte en lo que respecta a la confidencialidad debido a que previene la intromisión de fuentes no autorizadas a la integridad porque asegura que un paquete no está alterado y a la autenticación ya que verifica que el mensaje es recibido desde una fuente valida [63].

2.5.8 Comandos básicos de SNMP

A continuación se explican los comandos básicos de SNMP que son utilizados por las herramientas de monitoreo:

i. GET: recupera un valor del dispositivo gestionado. Por ejemplo get SysName, get sysUptime, get sysLocation.
ii. GET NEXT: recupera el valor del siguiente OID.
iii. GET BULK: recupera información voluminosa por ejemplo una “ifTable”.
iv. SET: modifica o asigna un valor a un parámetro.
v. Trap: se inician por el agente al administrador SNMP ante la ocurrencia de un evento por ejemplo un enlace o el estado del ventilador de alguno de los dispositivos administrados.
vi. INFORM: como Trap, también incluye información del administrador SNMP.
vii. RESPONSE: comando que se utiliza para llevar los valores o la señal de acciones dirigidas por el administrador de SNMP.

Capítulo 3. Metodología para la simulación y emulación de la red avanzada CLARA

En el presente capítulo se explica de una manera general el funcionamiento de la red avanzada CLARA, para esto se utiliza el software gratuito de Cisco Packet Tracer; cabe señalar que este software tiene sus limitaciones ya que no tiene interfaces reales que se usan en CLARA, tampoco tiene modelos de routers de backbone, esto es entendible ya que el software es para fines pedagógicos, sin embargo, es una herramienta suficiente para simular de forma general cualquier esquema de red.

Antes de comenzar con la metodología para la simulación y emulación de la red avanzada CLARA es importante puntualizar ciertas diferencias entre el simulador y emulador para esto se presenta la tabla 3.1 con las ventajas y desventajas de Packet Tracer y GNS3.

	Packet Tracer	GNS3
Software Gratuito	√	√
Código abierto	X	√
Windows/Linux	√	√
IOS reales	X	√
Catalyst Switches	√	X
Routers Cisco	X	√
WIFI	√	X
VOIP	√	√
SNMP	Limitado	√
GUI	√	X
CLI	√	√
Recursos PC	Normales	Superiores

Tabla 3.1. Comparación de características entre Packet Tracer y GNS3.

Con base en lo anterior se pueden tener ciertas expectativas que permiten saber las limitantes, ventajas y desventajas de cada uno para así hacer una simulación y emulación adecuada respecto a las características que ofrece GNS3 y Packet Tracer.

La primera parte de la simulación corresponderá al armado físico de la red en Packet Tracer. Es importante puntualizar que la topología de red que se simula es la de 2017 y para ello se utilizan routers genéricos ya que no hay equipos de backbone en el simulador. Es importante aclarar que no existen interfaces superiores a 1 Gbps en el simulador por lo que solo me limitaré a utilizar velocidades de 100 Mbps y 1 Gbps. La segunda parte corresponderá al direccionamiento lógico, donde se realiza un subnetting de red clase C para las direcciones IP, para esto se toma una porción del rango de direcciones IP privadas que van de 192.168.0.1 a 192.168.255.254 con máscara de subred 255.255.255.0. Por último se utiliza el protocolo de enrutamiento OSPF para entablar la conectividad de la red y ver los paquetes y mensajes vistos en el capítulo anterior.

Debido a la diversidad en los enlaces de la red CLARA, no será posible en la simulación tener los valores reales de éstos, sin embargo, se aprovechan los recursos que tiene este simulador para hacer una aproximación que permita la conectividad y el funcionamiento básico de la red.

3.1 Simulación en Packet Tracer.

Para la simulación de la red CLARA con topología de 2017 se utiliza una computadora de escritorio con las s características técnicas mostradas en la tabla 3.2.

Atributo	Descripción
Procesador	AMD FX(tm)-6100 Six-Core Processor a 3.3 GHz
Memoria RAM	8.00 GB (7.50 utilizable)
Tipo de sistema	Sistema operativo de 64 bits
Sistema operativo	Windows 7 Ultimate

Tabla 3.2 Características técnicas del equipo de cómputo.

De igual forma las características técnicas de los recursos del software que se utiliza se muestran en la tabla 3.3.

Recurso del software	Característica
Cisco Packet Tracer	Versión 6.1.0.0120
Routers	Tipo Genérico. IOS del software Versión 12.2(28)
Interfaces	Serial desde 1200 bps hasta 4 Mbps Ethernet 10 Mbps Fast Ethernet 100 Mbps Fibra Óptica 1 Gbps

Tabla 3.3 Características técnicas del software Packet Tracer y de las interfaces que maneja.

3.1.1 Conexión física de la red en Packet Tracer para la simulación

Para empezar con la conexión física se debe tomar en cuenta el tipo de interfaz para asignar las velocidades de transmisión y poder aproximarlas adecuadamente. La red CLARA cuenta con 16 nodos activos y 5 nodos los cuales todavía no están unidos a la red (Nicaragua, Honduras, Cuba, Bolivia y Paraguay). Con base en las características técnicas de la tabla 4.2 se utiliza routers genéricos para cada nodo activo de la red CLARA, así como conexiones de fibra óptica para las interfaces mayores o iguales a 1 Gbps, y de cable cruzado para las interfaces menores a 1 Gbps. Los nodos activos son los siguientes:

São Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Montevideo (Mdeo - Uruguay), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Bogotá (BOG - Colombia), Caracas (Car - Venezuela), Panamá (PTY - Panamá), San José (San José – Costa Rica), San Salvador (El Salvador), Guatemala (Guatemala), Tapachula (Tap - México)- y Miami (MIA - Estados Unidos), Londres (UK)

En la tabla 3.4 se muestran los enlaces reales de la red, mismos que serán utilizados en Packet Tracer.

#	Enlace	Velocidad real	Velocidad en el simulador y emulador
1	Tapachula (México) --- Miami (Estados Unidos)	1 Gbps	1 Gbps
2	Tapachula (México) --- Guatemala (Guatemala)	2.5 Gbps	1 Gbps
3	Guatemala (Guatemala) --- San Salvador (El Salvador)	2.5 Gbps	1 Gbps
4	San Salvador (El Salvador)---San José (Costa Rica)	400 Mbps	100 Mbps
	San Salvador (El Salvador)---San José (Costa Rica)	2.5 Gbps	1 Gbps
5	San José (Costa Rica)--- PTY (Panamá)	400 Mbps	100 Mbps
	San José (Costa Rica)--- PTY (Panamá)	2.5 Gbps	1 Gbps
6	Miami (Estados Unidos) --- PTY (Panamá)	10 Gbps	1 Gbps
7	Miami (Estados Unidos) --- São Paulo (Brasil)	100 Gbps	1 Gbps
8	Miami (Estados Unidos) --- Santiago (Chile)	10 Gbps	1 Gbps
9	PTY (Panamá) --- São Paulo (Brasil)	10 Gbps	1 Gbps
10	PTY (Panamá) --- Bogotá (Colombia)	10 Gbps	1 Gbps
11	PTY (Panamá) --- Caracas (Venezuela)	2 Gbps	1 Gbps
12	Bogotá (Colombia) --- Santiago (Chile)	10 Gbps	1 Gbps
13	Guayaquil (Ecuador) --- Lima (Perú)	600 Mbps	100 Mbps
14	Lima (Perú) --- Santiago (Chile)	2.5 – 10 Gbps	1 Gbps
15	Santiago (Chile) --- São Paulo (Brasil)	10 Gbps	1 Gbps
16	Santiago (Chile) --- Buenos Aires (Argentina)	10 Gbps	1 Gbps
	Santiago (Chile) --- Buenos Aires (Argentina)	1 Gbps	1 Gbps
17	Buenos Aires (Argentina) --- Montevideo (Uruguay)	300 Mbps	100 Mbps
18	Buenos Aires (Argentina) --- São Paulo (Brasil)	10 Gbps	1 Gbps
19	São Paulo (Brasil) --- Londres (UK)	5 Gbps	1 Gbps

Tabla 3.4. Comparativa entre enlaces reales y los enlaces a utilizar en Packet Tracer. Diagrama propio con base en la referencia [41]

Como se puede ver en la tabla 3.4 de los 9 tipos de interfaces reales sólo se utilizan 2 que son las que da el simulador para aplicarlas en la simulación. De esta forma la topología de la red quedó como se muestra en la figura 3.1.

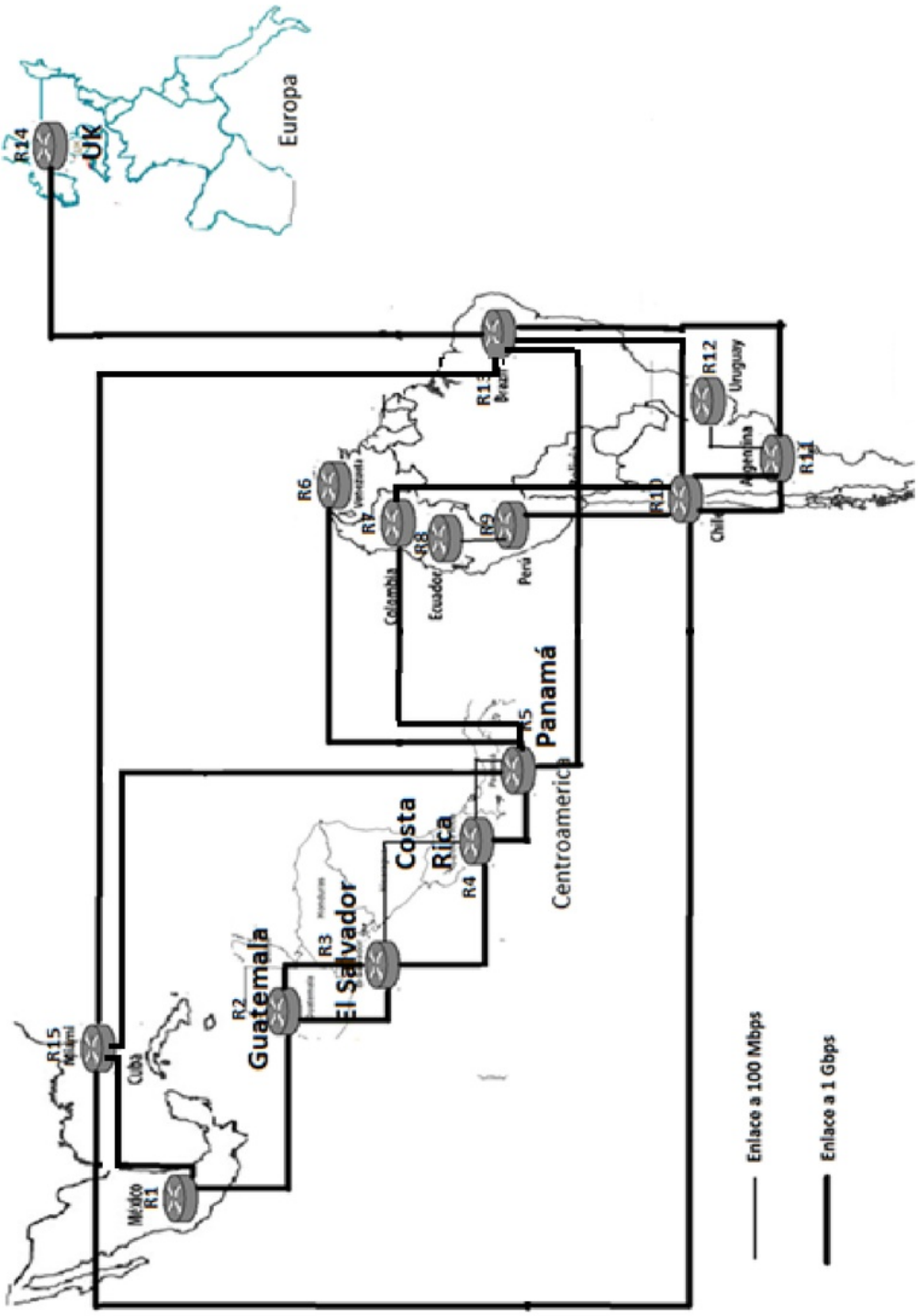


Figura 3.1. Topología de la red CLARA en 2017 a simular en Packet Tracer. Diagrama propio con base en la referencia. [41]

3.1.2 Direccionamiento IP

Para obtener la conectividad lógica de la red se realiza un subnetting de clase C con direcciones privadas de red las cuales se toman del rango ***192.168.0.0 hasta 192.168.255.0***, así mismo se determinan al menos 6 hosts para cada router, esto para asegurar futuras conexiones en los routers.

Por lo anterior se parte de la subred 192.168.4.0/24 y se establecen las subredes tomando los primeros 5 bits del último octeto y se utilizan los 3 restantes para los host. Con lo anterior tenemos una máscara de subred de 29 bits lo cual garantiza 32 subredes con 6 direcciones de host para cada una de ellas. El procedimiento se indica en la tabla 3.5.

Dirección IP de Red Clase C privada	192.168.4.0 / 255.255.255.0
Máscara de subred en binario	11111111.11111111.11111111.11111000 Máscara de subred 29 bits — 3 bits para host
Número de hosts por subred	$2^3 - 2$= 8-2= 6 ➔6 hosts por subred
Número total de subredes	2^5=32 ➔32 Subredes
Red y máscara de subred en decimal	192.168.4.0 / 29 255.255.255.248
Máscara de Wildcard	255.255.255.255 -255.255.255.248 0 .0 .0 .7

Tabla 3.5 Proceso para establecimiento de subredes y hosts por subred de la dirección de red IP 192.168.4.0/24

La tabla 3.6 muestra las subredes que se utilizan en la simulación y posteriormente en la emulación. Cumpliendo con la tabla 3.4 en la cual se especifican 6 direcciones IP de hosts para cada subred, se utiliza la dirección IP base 192.168.4.0 y una máscara de subred 255.255.255.248 ó /29. Para direcciones externas de los host y gateway, para cada router en los diferentes países se utiliza la dirección IP base 192.168.5.0 y una máscara de subred 255.255.255.248 ó /29.

# Enlace	Dirección de subred	Máscara de subred	Primer host utilizable	Último host utilizable	Dirección de broadcast
1	192.168.4.0/29	255.255.255.248	192.168.4.1	192.168.4.6	192.168.4.7
2	192.168.4.8/29	255.255.255.248	192.168.4.9	192.168.4.14	192.168.4.15
3	192.168.4.16/29	255.255.255.248	192.168.4.17	192.168.4.22	192.168.4.23
4	192.168.4.24/29	255.255.255.248	192.168.4.25	192.168.4.30	192.168.4.31
	192.168.4.32/29	255.255.255.248	192.168.4.33	192.168.4.38	192.168.39
5	192.168.4.40/29	255.255.255.248	192.168.4.41	192.168.4.46	192.168.4.47
	192.168.4.48/29	255.255.255.248	192.168.4.49	192.168.4.54	192.168.4.55
6	192.168.4.56/29	255.255.255.248	192.168.4.57	192.168.4.62	192.168.4.63
7	192.168.4.64/29	255.255.255.248	192.168.4.65	192.168.4.70	192.168.4.71
8	192.168.4.72/29	255.255.255.248	192.168.4.73	192.168.4.78	192.168.4.79
9	192.168.4.80/29	255.255.255.248	192.168.4.81	192.168.4.86	192.168.4.87
10	192.168.4.88/29	255.255.255.248	192.168.4.89	192.168.4.94	192.168.4.95
11	192.168.4.96/29	255.255.255.248	192.168.4.97	192.168.4.102	192.168.4.103
12	192.168.4.104/29	255.255.255.248	192.168.4.105	192.168.4.110	192.168.4.111
13	192.168.4.112/29	255.255.255.248	192.168.4.113	192.168.4.118	192.168.4.119
14	192.168.4.120/29	255.255.255.248	192.168.4.121	192.168.4.126	192.168.4.127
15	192.168.4.128/29	255.255.255.248	192.168.4.129	192.168.4.134	192.168.4.135
16	192.168.4.136/29	255.255.255.248	192.168.4.137	192.168.4.142	192.168.4.141
	192.168.4.144/29	255.255.255.248	192.168.4.145	192.168.4.150	192.168.4.151
17	192.168.4.152/29	255.255.255.248	192.168.4.153	192.168.4.158	192.168.4.159

18	192.168.4.160/29	255.255.255.248	192.168.4.161	192.168.4.166	192.168.4.167
19	192.168.4.168/29	255.255.255.248	192.168.4.169	192.168.4.174	192.168.4.175
Direcciones para los host y gateway para cada router					
R1 MEX	192.168.5.0/29	255.255.255.248	192.168.5.1	192.168.5.6	192.168.5.7
R2 GUA	192.168.5.8/29	255.255.255.248	192.168.5.9	192.168.5.14	192.168.5.15
R3 SV	192.168.5.16/29	255.255.255.248	192.168.5.17	192.168.5.22	192.168.5.23
R4 CR	192.168.5.24/29	255.255.255.248	192.168.5.25	192.168.5.30	192.168.5.31
R5 PAN	192.168.5.32/29	255.255.255.248	192.168.5.33	192.168.5.38	192.168.5.39
R6 VEN	192.168.5.40/29	255.255.255.248	192.168.4.41	192.168.4.46	192.168.4.47
R7 COL	192.168.5.48/29	255.255.255.248	192.168.4.49	192.168.4.54	192.168.4.55
R8 EC	192.168.5.56/29	255.255.255.248	192.168.4.57	192.168.4.62	192.168.4.63
R9 PE	192.168.5.64/29	255.255.255.248	192.168.4.65	192.168.4.70	192.168.4.71
R10 CH	192.168.5.72/29	255.255.255.248	192.168.4.73	192.168.4.78	192.168.4.79
R11 ARG	192.168.5.80/29	255.255.255.248	192.168.5.81	192.168.5.86	192.168.5.87
R12 UY	192.168.5.88/29	255.255.255.248	192.168.5.89	192.168.5.94	192.168.5.95
R13 BR	192.168.5.96/29	255.255.255.248	192.168.5.97	192.168.5.102	192.168.5.103
R14 UK	192.168.5.104/29	255.255.255.248	192.168.5.105	192.168.5.110	192.168.5.111
R15 MIA	192.168.5.112/29	255.255.255.248	192.168.5.113	192.168.5.118	192.168.5.119

Tabla 3.6 Subredes a utilizar en la simulación y emulación.

Una vez que ya establecimos las subredes, es preciso determinar la asignación de éstas a cada uno de los enlaces descritos en la tabla 3.4 por lo que en la tabla 3.7 se establecen las subredes específicamente para cada enlace, la conexión de las interfaces tanto físicas y lógicas así como las direcciones IP para dichas interfaces.

# Enlace	Subred	Interconexiones	Interfaces físicas Interconexiones	Interfaces lógicas Interconexiones
1	192.168.4.0	R1(Mex)⇔R15(Mia)	G7/0⇔G7/0	192.168.4.1-⇔ 192.168.4.2
2	192.168.4.8	R1(Mex)⇔R2(Gua)	G8/0⇔G8/0	192.168.4.9⇔192.168.4.10
3	192.168.4.16	R2(Gua)⇔R3(SV)	G7/0⇔G7/0	192.168.4.17⇔192.168.4.18
4	192.168.4.24	R3(SV)⇔R4(CR)	G8/0⇔G8/0	192.168.4.25⇔192.168.4.26
	192.168.4.32	R3(SV)⇔R4(CR)	Fa9/0⇔Fa0/0	192.168.4.33⇔192.168.4.34
5	192.168.4.40	R4(C.R)⇔R5(Pan)	Fa9/0-⇔Fa9/0	192.168.4.41⇔192.168.4.42
	192.168.4.48	R4(C.R)⇔R5(Pan)	G7/0⇔G7/0	192.168.4.49⇔192.168.4.50
6	192.168.4.56	R15(Mia)⇔R5(Pan)	G8/0⇔G8/0	192.168.4.57⇔192.168.4.58
7	192.168.4.64	R15(Mia)⇔R13(Br)	G1/0⇔G1/0	192.168.4.65⇔192.168.4.66
8	192.168.4.72	R15(Mia)⇔R10(CL)	G9/0⇔G8/0	192.168.4.73⇔192.168.4.74
9	192.168.4.80	R5(Pan)⇔R13(Br)	G1/0⇔G7/0	192.168.4.81⇔192.168.4.82
10	192.168.4.88	R5(Pan)⇔R7(CO)	G0/0⇔G1/0	192.168.4.89⇔192.168.4.90
11	192.168.4.96	R5(Pan)⇔R6(Ven)	G2/0⇔G1/0	192.168.4.97⇔192.168.4.98
12	192.168.4.104	R7(Co)⇔R10(CL)	G7/0⇔G1/0	192.168.4.105⇔192.168.4.106
13	192.168.4.112	R8(EC)⇔R9(PE)	Fa0/0⇔Fa0/0	192.168.4.113⇔192.168.4.114
14	192.168.4.120	R9(PE)⇔R10(CL)	G7/0⇔G7/0	192.168.4.121⇔192.168.4.122
15	192.168.4.128	R10(CL)⇔R13(Br)	G6/0⇔G6/0	192.168.4.129⇔192.168.4.130
16	192.168.4.136	R10(CL)⇔R11(Arg)	G3/0⇔G7/0	192.168.4.137⇔192.168.4.138
	192.168.4.144	R10(CL)⇔R11(Arg)	G2/0⇔G8/0	192.168.4.145⇔192.168.4.146
17	192.168.4.152	R11(Arg)⇔R12(UY)	Fa0/0⇔Fa0/0	192.168.4.153⇔192.168.4.154
18	192.168.4.160	R11(Arg)⇔R13(Br)	G2/0⇔G8/0	192.168.4.161⇔192.168.4.162
19	192.168.4.168	R13(Br)⇔R14(UK)	G0/0⇔G1/0	192.168.4.169⇔192.168.4.170

Tabla 3.7 Asignaciones de las direcciones IP a las interfaces de los routers, para simulación y emulación.

3.1.3 Configuración en Packet Tracer

Después de tener la conexión física y la asignación de las subredes a cada enlace es tiempo de configurar las subredes en los routers del simulador, para esto lo primero que se configura es el nombre y la seguridad de cada router, es decir, las contraseñas. En la figura 3.2 se muestra la utilización de los comandos utilizados que se usaron para el router de México, mismos que se utilizaron para cada uno de los routers.

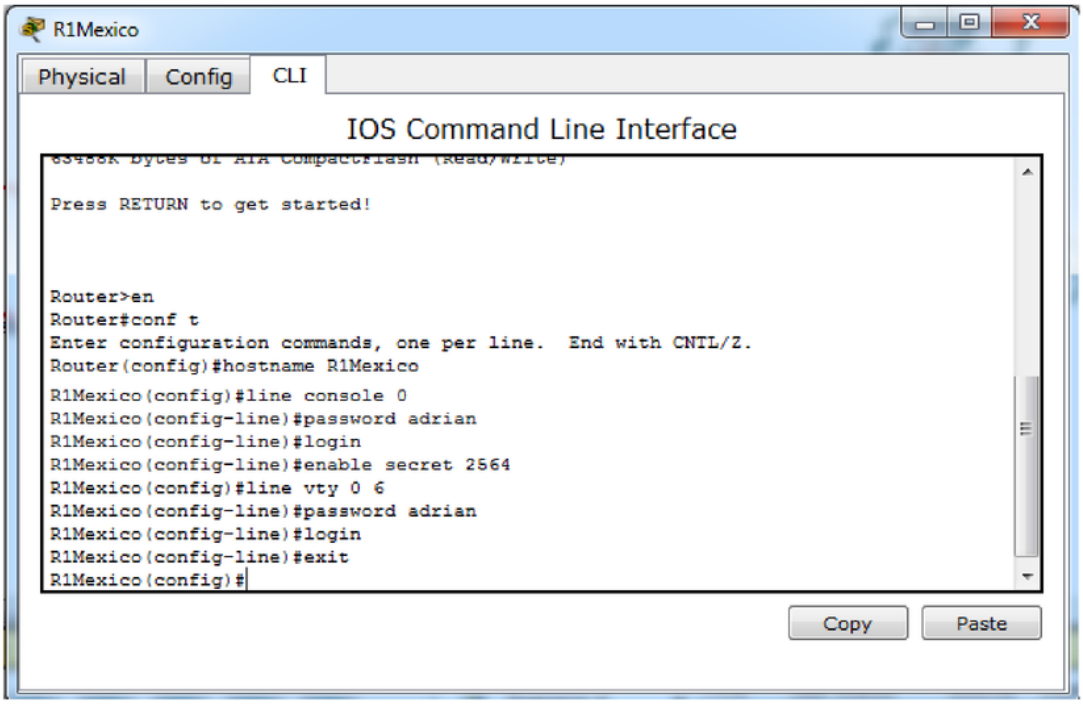


Figura 3.2 Configuración del nombre y la seguridad en el Router de México.

Una vez configurados todos los routers como en la figura 3.2 se procede a configurar las direcciones IP para cada uno de los enlaces con base en la tabla 3.6. Se destaca que todos los enlaces son de fibra óptica, a excepción de 4 enlaces: R3(SV)-R4(CR), R4(C.R)-R5(Pan), R8(EC)-R9(PE), R11(Arg)-R12(UY).

Ahora que los routers tienen una configuración básica se procede a configurar las direcciones IP para cada uno de los enlaces punto a punto, para esto con base en la tabla 3.6 que contiene las direcciones IP para cada una de las interfaces de cada router. En la figura 3.3 se muestra la asignación de direcciones IP mediante los

comandos correspondientes al router de México, este procedimiento será el mismo para cada uno de los routers restantes.

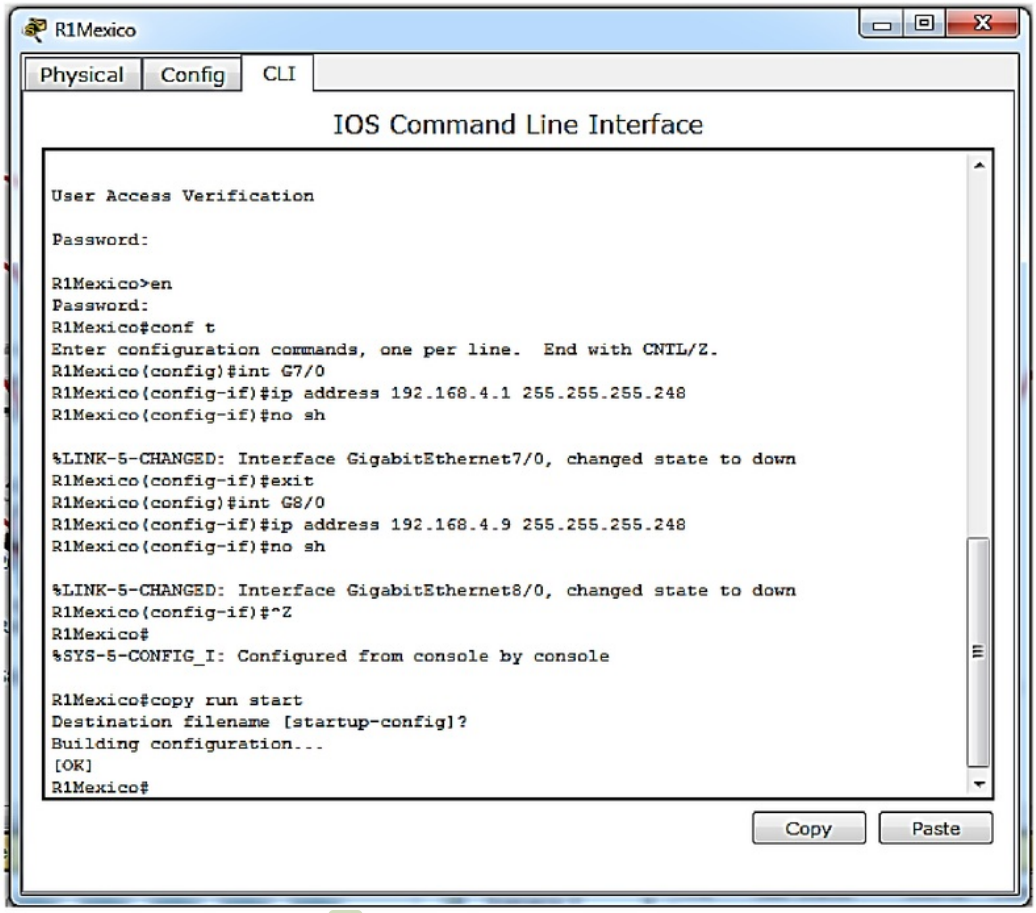


Figura 3.3. Configuración de direcciones IP a cada una de las interfaces del router de México.

En la figura 3.4 se observan todas las interfaces configuradas en cada uno de los routers del simulador con base en la tabla 3.6.

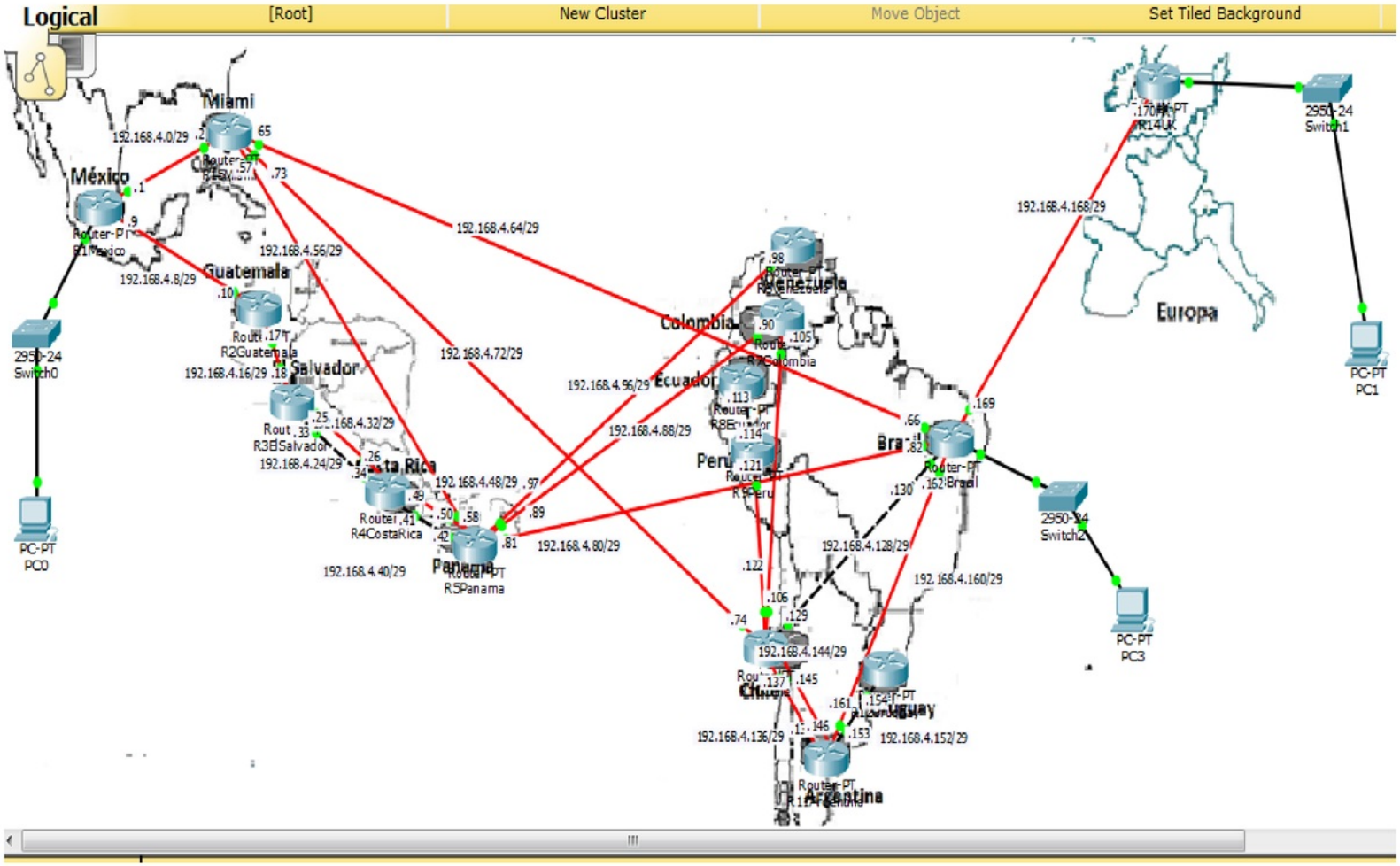


Figura 3.4. Interfaces asignadas a una dirección IP en el simulador.

Hasta este punto tenemos conectividad tanto física como lógica, sin embargo, no hay un protocolo de enrutamiento configurado para hacer llegar paquetes desde un router a otro. Es por ello que se utiliza el protocolo de enrutamiento OSPF para tener una conectividad global con todos los routers.

3.1.4 Configuración del protocolo de enrutamiento OSPF para la simulación en Packet Tracer

Para configurar el protocolo OSPF es necesario conocer qué subredes están conectadas a los routers directamente. Debido al mayor número de subredes que tiene conectadas, se toma el Router de Panamá para ejemplificar la configuración del protocolo OSPF. El proceso y los comandos a utilizar son los mismos que en las figuras 3.5 y 3.6 tomando en cuenta que sólo cambiarán las subredes conectadas directamente dependiendo cada router. Hay que enfatizar que dado que los routers en la simulación representan el backbone de CLARA es necesario configurarlos como área 0 en la sintaxis de los comandos para OSPF.

Para empezar se utiliza el comando "*show ip route*" para ver qué redes están conectadas directamente al router. El router de Panamá tiene 6 subredes conectadas mismas que deberán ser incluidas en la configuración del protocolo OSPF, como se indica en la figura 3.5. En donde la sintaxis para configurar el protocolo OSPF es la siguiente:

router ospf "ID del proceso"

network "Dirección IP red conectada al router" "máscara de wildcard" "área de proceso"

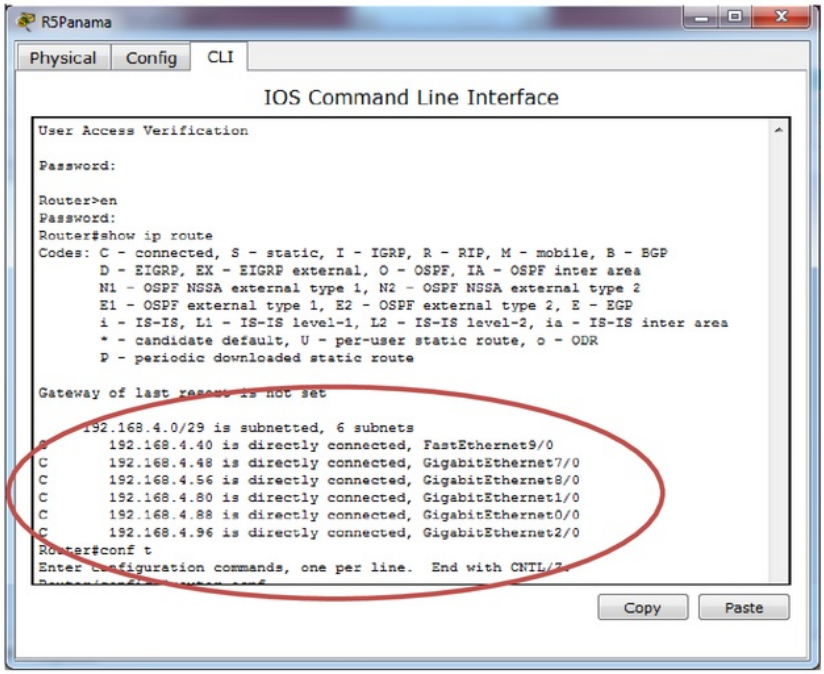


Figura 3.5. Número de subredes conectadas al router de Panamá.

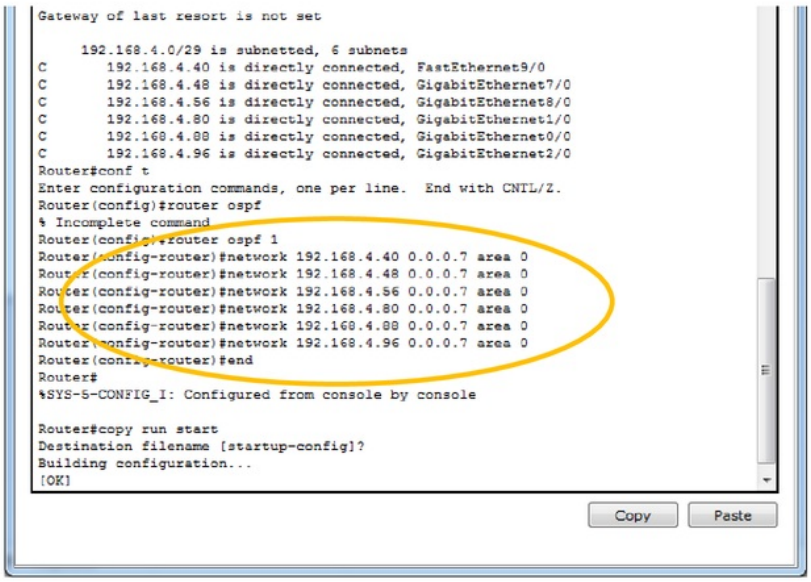


Figura 3.6. Configuración de OSPF en el router de Panamá.

3.1.5 Configuración de SNMP en Packet Tracer

Conforme una red va creciendo en dispositivos ésta se hace más compleja, de igual forma los recursos que ofrece son mayores, es por ello que hay que poner atención especial a la gestión, esto sirve para tener un control mayor sobre la red. En esta sección se configura SNMP en los routers de la red CLARA para contar con una gestión apropiada.

3.1.5.1 Activación del protocolo SNMP en CLARA mediante Packet Tracer

La configuración de SNMP comienza siempre en los routers, SNMP solicíta establecer un nombre de comunidad de lectura y escritura para establecer diversos parámetros mediante una MIB browser de una PC. En la figura 3.7 se muestra la configuración de SNMP que se utiliza para todos los routers; se toma como referencia el router de Panamá, nótese en dicha figura los comandos ***snmp-server community*** *nombre de la comunidad* ***ro*** (nombre de comunidad con privilegios sólo de lectura) y ***snmp-server community*** *nombre de la comunidad* ***rw*** (nombre de comunidad con privilegios sólo de escritura).

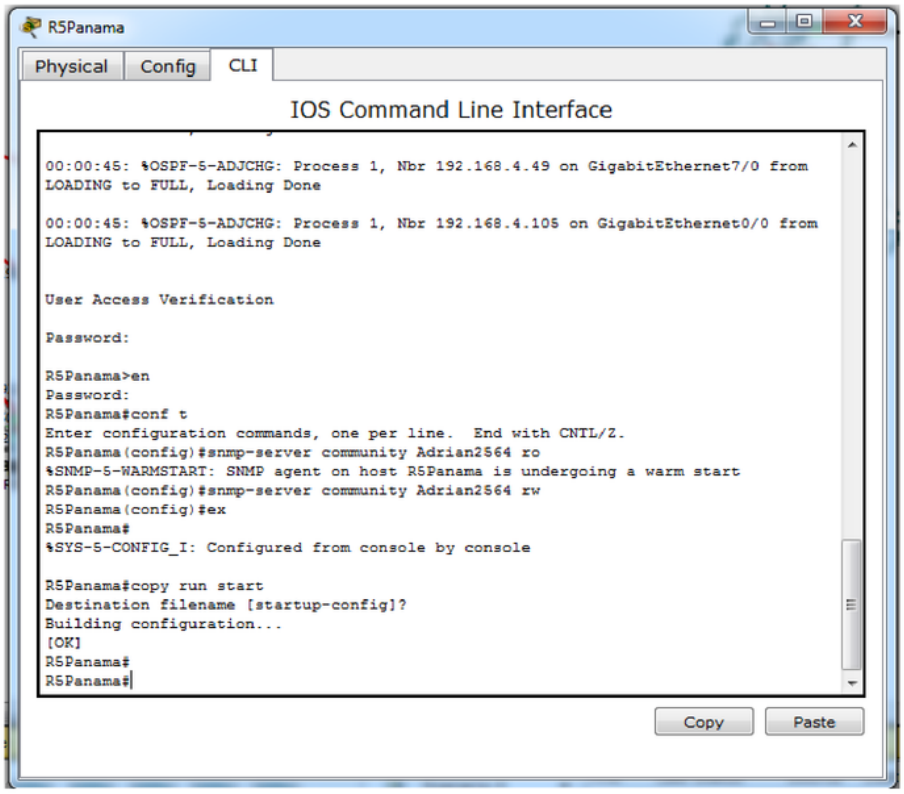


Figura 3.7 Configuración general de SNMP que será utilizada en todos los routers de la simulación.

3.2 GNS3

Para tener una aproximación más real de la red CLARA se utiliza el emulador GNS3 el cual fue creado en 2006. GNS3 utiliza el emulador de routers Dynamips. La ventaja que tiene usar GNS3 es que se pueden utilizar los routers de backbone así como los IOS (Internetwork Operating Systems) correspondientes, ya que GNS3 trabaja con IOS reales.

El subneting para la emulación de la red será el mismo que se utiliza en Packet Tracer por lo que solo cambiarán las interfaces lógicas de los routers. Es importante precisar que los routers en GNS3 trabajan con puertos Fast Ethernet y Gigabit Ethernet por lo que al igual que Packet Tracer sólo se tendran enlaces con velocidades de 100 Mbps y 1 Gbps.

Una herramienta importante de GNS3 es el analizador de paquetes Wireshark el cual permite examinar los tipos de paquetes OSPF en tiempo real.

Para la emulación de la red CLARA se utiliza una computadora de escritorio con las características técnicas de la tabla 3.1.

Al emular con GNS3 se está buscando tener una aproximación más cercana a la realidad con respecto de Packet Tracer, para esto es importante configurar algunos parámetros básicos de GNS3 para tener un rendimiento óptimo, ya que GNS3 utiliza muchos recursos que pueden entorpecer la emulación.

3.2.1 Configuración básica de GNS3

Como cualquier software de uso libre se debe ir a la página oficial de GNS3 (https://gns3.com/) y bajar la versión que sea útil, en este caso se usó la versión 2.0.1 misma que se actualizó por última vez en mayo de 2017.

Una vez instalado GNS3 lo primero que se configura son las imágenes de los routers, mismas que dependiendo del modelo de router que se vaya a trabajar se pueden encontrar en Intenet. Para añadir las imágenes a GNS3 se usa el menú Edit -> Preferences, de ahí se selecciona *Dynamips-> IOS routers ->New* y se busca la imagen que se va a añadir como se muestra en la figura 3.8. Para la presente emulación se usan imágenes del router 7200 de Cisco ya que es un router usado para conexiones de backbone, además es el router con mayor capacidad en GNS3.

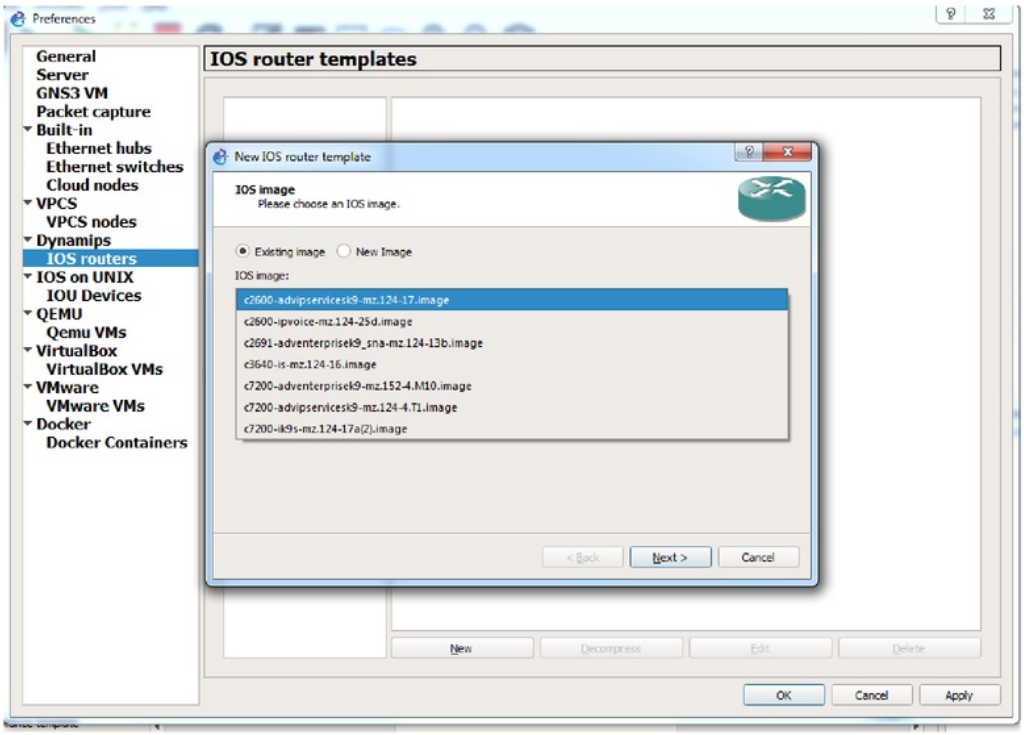


Figura 3.8. Forma de agregar las imágenes de los routers en GNS3.

Debido a la naturaleza y exactitud de GNS3 hay un uso de recursos muy alto, es por eso que GNS3 cuenta con una opción llamada IDLE-PC, la cual permite optimizar el uso de recursos de GNS3, esto se traduce en ahorro de consumo de procesador y uso de memoria RAM. La figura 3.9. Muestra la opción de IDLE-PC la cual busca automáticamente un valor de optimización encontrado por el emulador.

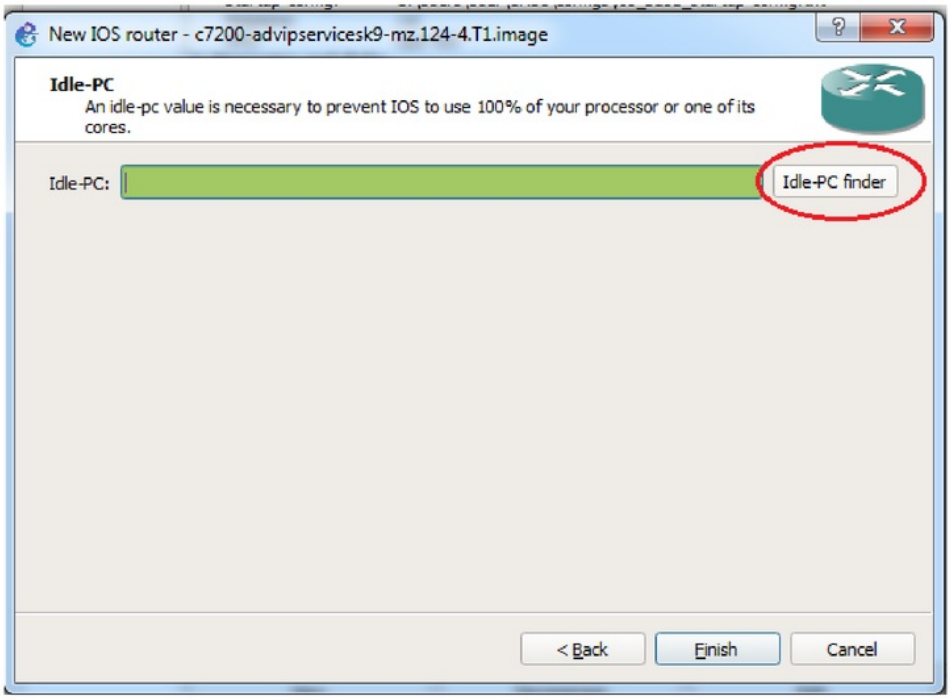


Figura 3.9. Asignación del IDLE-PC.

Una vez agregado aparece en la pestaña de routers como se muestra en la figura 3.10.

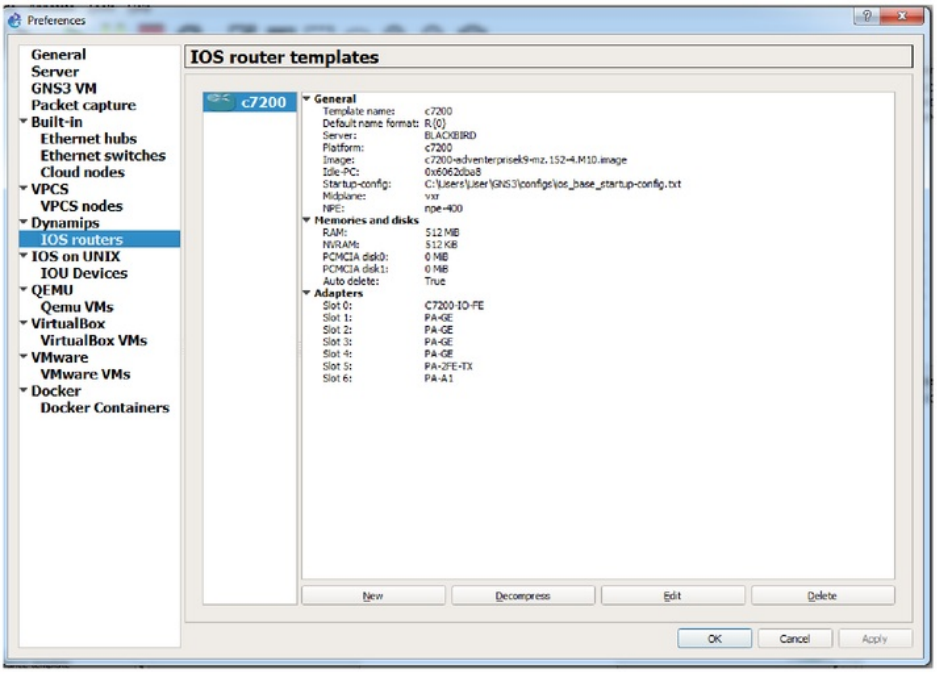


Figura 3.10. Imagen del router 7200 añadida correctamente.

GNS3 permite trabajar con módulos de máquinas virtuales, por lo que se agregan las máquinas virtuales para que funcionen como agentes SNMP. La figura 3.11 muestra que el software añadió correctamente las máquinas virtuales, es importante mencionar que el proceso es el mismo que cuando se añadieron los routers, para la emulación se usó Vmware con una imagen de Windos 7 ya que es compatible con el administrador SNMP que en este caso es PowerSNMP.

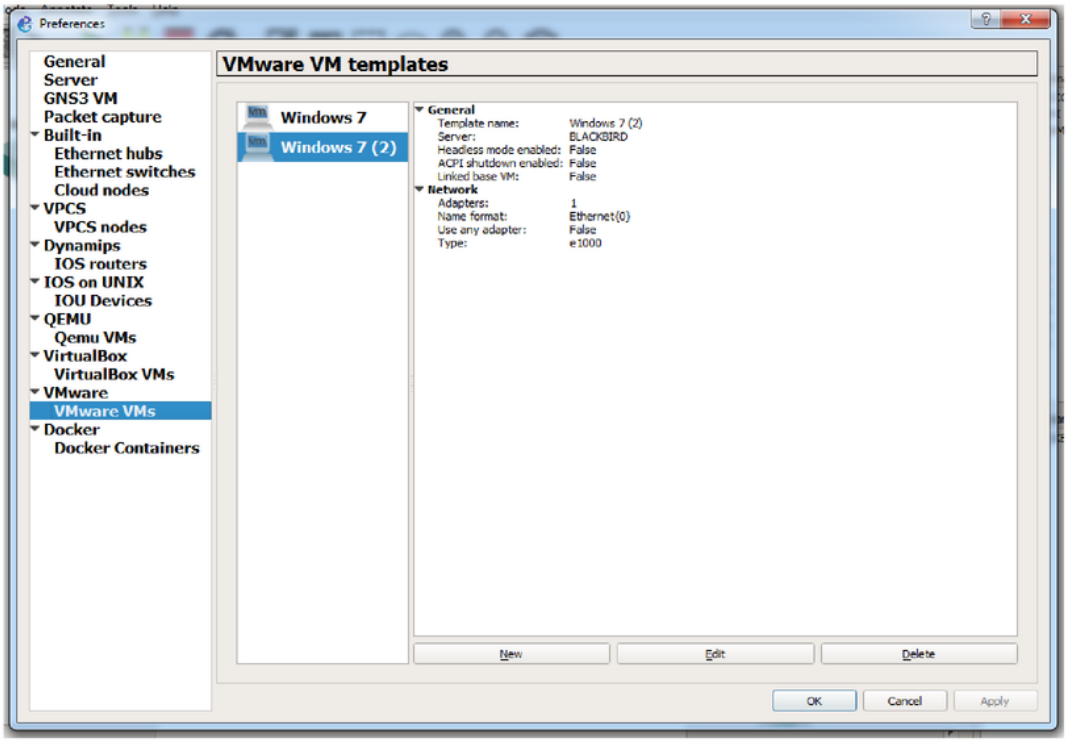


Figura 3.11. Imagen de máquina virtual Windows 7 añadida correctamente.

Por último una herramienta fundamental con la que cuenta GNS3 es Wireshark, el cual realiza una captura de paquetes que permite observar los paquetes que pasan por los enlaces Ethernet que conectan a los routers de la red CLARA. Esta herramienta se instala automáticamente al momento de instalar GNS3.

GNS3 no cuenta con switches originales, por lo cual, se utiliza un router que añadimos como switch aprovechando sus puertos Ethernet. Para esto hay que cambiar el símbolo, en la opción change Symbol se busca un símbolo de switch Ethernet como se muestra en la figura 3.12.

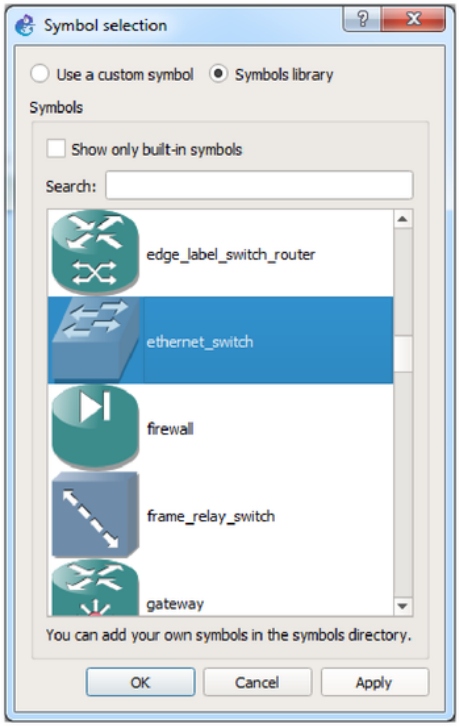


Figura 3.12. Switch agregado en GNS3.

En la figura 3.13 se muestra el área de trabajo de GNS3 en la cual se resaltan 5 recuadros los cuales tienen las siguientes funciones:

1. Node Types. En esta ventana se toman los dispositivos que se utilizan en las emulaciones, esta ventana cuenta con routers, switches, PC y las conexiones que se utilizan para conectar los dispositivos.
2. Área de trabajo. En esta ventana se crean las topologías de forma gráfica.
3. Topology Summary. Muestra un recuadro con los detalles de los dispositivos, es decir, si están encendidas o apagadas.
4. Servers Summary. Esta ventana indica el uso de CPU y de memoria RAM que ocupa GNS3.
5. Mensajes y errores que ocurren durante la emulación.

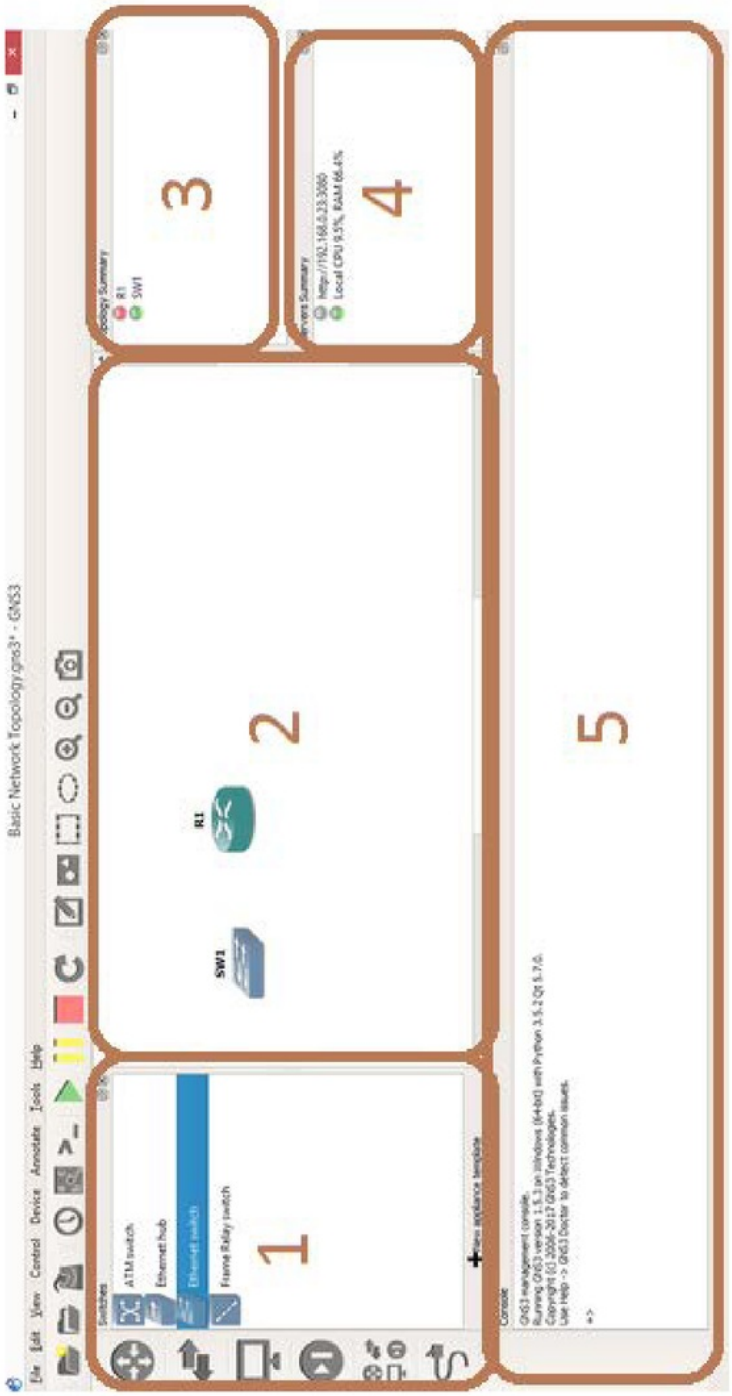


Figura 3.13. Área de trabajo de GNS3.

3.2.2 Conexión física de la red en GNS3

Ahora se procede a agregar los routers y hacer la conexión física con base en la topología 2017, la cual se muestra en la figura 3.14.

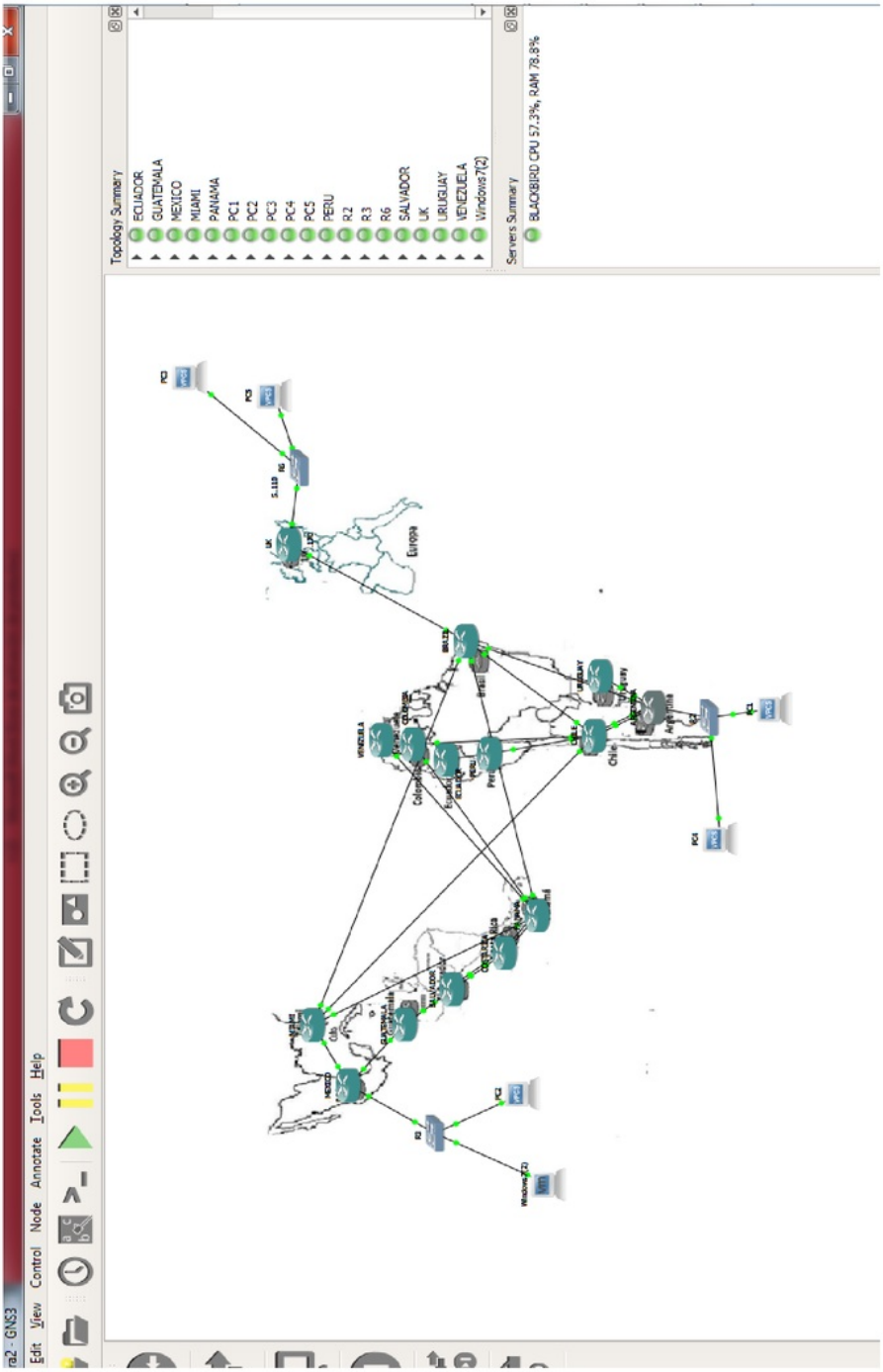


Figura 3.14. Conexión física de la red CLARA en GNS3

De igual forma, la tabla de interfaces cambia un poco con respecto a la de Packet Tracer, es decir, sólo cambian algunos valores de la columna de interfaces físicas, la tabla 3.8 muestra la asignación de interfaces.

# En la-ce	Subred	Interconexiones	Interfaces físicas de Interconexión.	Interfaces lógicas de Interconexiones
1	192.168.4.0	R1(Mex)⇔R15(Mia)	G0/0⇔G0/0	192.168.4.1-⇔ 192.168.4.2
2	192.168.4.8	R1(Mex)⇔R2(Gua)	G1/0⇔G0/0	192.168.4.9⇔192.168.4.10
3	192.168.4.16	R2(Gua)⇔R3(SV)	G0/0⇔G0/0	192.168.4.17⇔192.168.4.18
4	192.168.4.24	R3(SV)⇔R4(CR)	G1/0⇔G0/0	192.168.4.25⇔192.168.4.26
	192.168.4.32	R3(SV)⇔R4(CR)	Fa0/0⇔Fa0/0	192.168.4.33⇔192.168.4.34
5	192.168.4.40	R4(C.R)⇔R5(Pan)	Fa0/0-⇔Fa0/0	192.168.4.41⇔192.168.4.42
	192.168.4.48	R4(C.R)⇔R5(Pan)	G1/0⇔G1/0	192.168.4.49⇔192.168.4.50
6	192.168.4.56	R15(Mia)⇔R5(Pan)	G1/0⇔G1/0	192.168.4.57⇔192.168.4.58
7	192.168.4.64	R15(Mia)⇔R13(Br)	G1/0⇔G1/0	192.168.4.65⇔192.168.4.66
8	192.168.4.72	R15(Mia)⇔R10(CL)	G3/0⇔G5/0	192.168.4.73⇔192.168.4.74
9	192.168.4.80	R5(Pan)⇔R13(Br)	G4/0⇔G0/0	192.168.4.81⇔192.168.4.82
10	192.168.4.88	R5(Pan)⇔R7(CO)	G3/0⇔G0/0	192.168.4.89⇔192.168.4.90
11	192.168.4.96	R5(Pan)⇔R6(Ven)	G0/0⇔G0/0	192.168.4.97⇔192.168.4.98
12	192.168.4.104	R7(Co)⇔R10(CL)	G3/0⇔G1/0	192.168.4.105⇔192.168.4.106
13	192.168.4.112	R8(EC)⇔R9(PE)	Fa0/0⇔Fa0/0	192.168.4.113⇔192.168.4.114
14	192.168.4.120	R9(PE)⇔R10(CL)	G1/0⇔G4/0	192.168.4.121⇔192.168.4.122
15	192.168.4.128	R10(CL)⇔R13(Br)	G2/0⇔G3/0	192.168.4.129⇔192.168.4.130
16	192.168.4.136	R10(CL)⇔R11(Arg)	G1/0⇔G3/0	192.168.4.137⇔192.168.4.138
	192.168.4.144	R10(CL)⇔R11(Arg)	G0/0⇔G2/0	192.168.4.145⇔192.168.4.146
17	192.168.4.152	R11(Arg)⇔R12(UY)	Fa1/0⇔Fa0/0	192.168.4.153⇔192.168.4.154
18	192.168.4.160	R11(Arg)⇔R13(Br)	G0/0⇔G2/0	192.168.4.161⇔192.168.4.162
19	192.168.4.168	R13(Br)⇔R14(UK)	G1/0⇔G0/0	192.168.4.169⇔192.168.4.170

Tabla 3.8. Interfaces para la emulación en GNS3.

3.2.3 Configuración en GNS3

Al igual que en la simulación con Packet Tracer se configuran las subredes y direcciones IP en cada uno de los routers del emulador, para esto primero se configura el nombre y la contraseña de los routers, el user y password serán los mismos que en la simulación de Packet Tracer. En la figura 3.15 se muestran los comandos de configuración que se utilizaron. Se repite el procedimiento en los demás routers de la red.

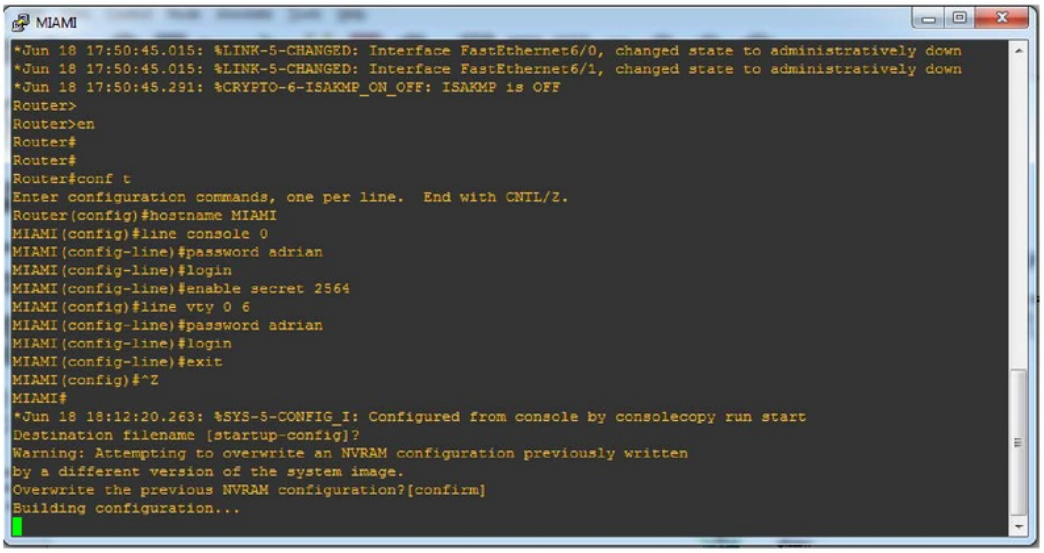


Figura 3.15. Configuración de nombre y contraseñas en el router de Miami.

Una vez configurados el nombre del router y las contraseñas, se procede a configurar las direcciones IP de cada una de las interfaces de los routers, para esto se utiliza la tabla 3.7 con las mismas direcciones que en Packet Tracer. En la figura 3.16 se muestran los comandos para configurar las redes IP en los routers. Es importante mencionar que sólo se muestran los comandos para el router de México, sin embargo, el procedimiento es el mismo para los demás routers.

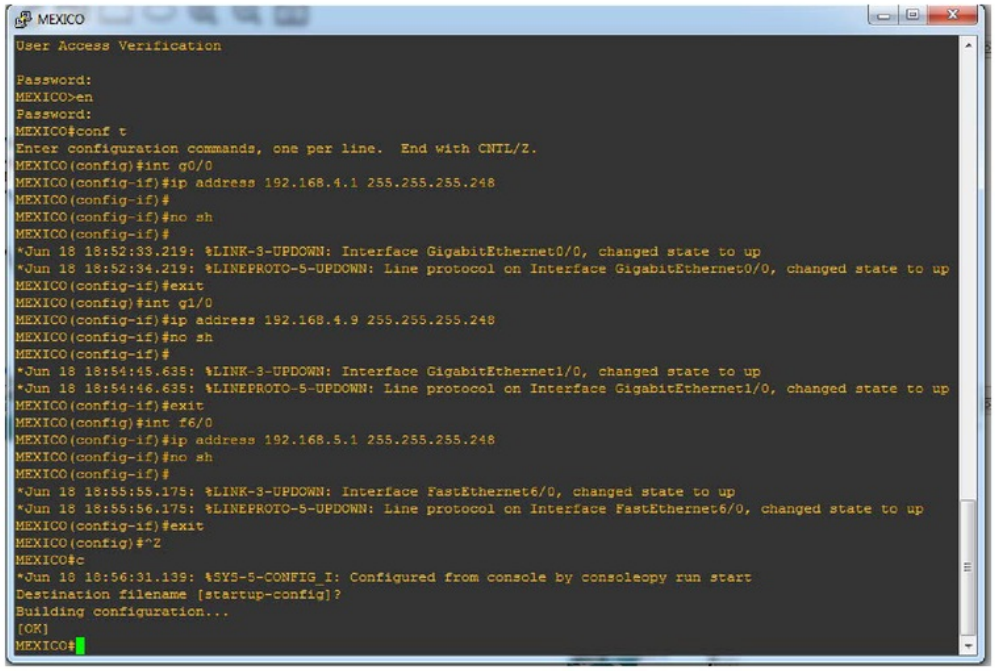


Figura 3.16. Comandos para asignación de direcciones IP en el router de México.

3.2.4 Configuración del protocolo de enrutamiento OSPF en GNS3

Con todas las subredes configuradas de la red CLARA, es posible configurar OSPF para establecer adyacencias entre los routers, lo que permitirá un enrutamiento que tome el camino más corto para llegar a su destino. Para ejemplificar la configuración y sintaxis de los comandos de OSPF se toma como referencia el router de Panamá ya que tiene el mayor número de enlaces. El proceso no varía con respecto de Packet Tracer por lo que se usan los mismos comandos, los cuales servirán para configurar el protocolo en cada uno de los routers, por lo que se deberán tomar en cuenta las subredes que corresponden a cada router. Dado que los routers que conforman CLARA son routers de backbone, OSPF se deberá configurar en cada router como área cero (backbone).

La configuración de OSPF se realiza en dos partes, lo primero que hay que tomar en cuenta son las redes que están directamente conectados al router, para esto se utiliza el comando *show ip route*. Como se puede observar en la figura 3.17 el router de Panamá tiene 6 subredes, dichas subredes deberán tomarse en cuenta al configurar el protocolo OSPF.

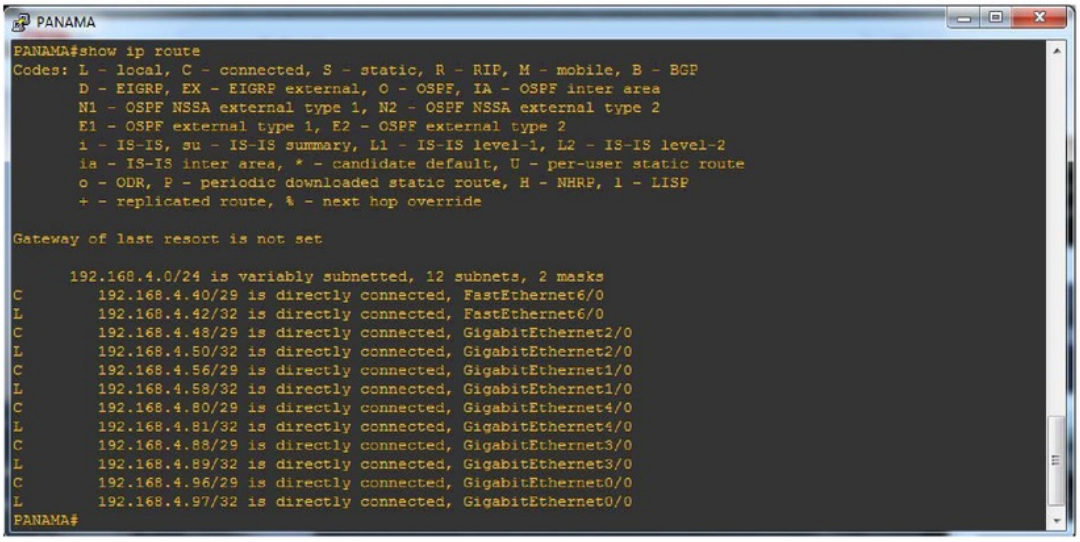


Figura 3.17. Número de subredes conectadas al router de Panamá.

Ahora que se conocen las subredes conectadas se procede a configurar OSPF, en la figura 3.18 se ejemplifica la configuración de OSPF con la sintaxis siguiente:

router ospf "ID del proceso"

network "Dirección IP red conectada al router" "máscara de wildcard" "área de proceso"

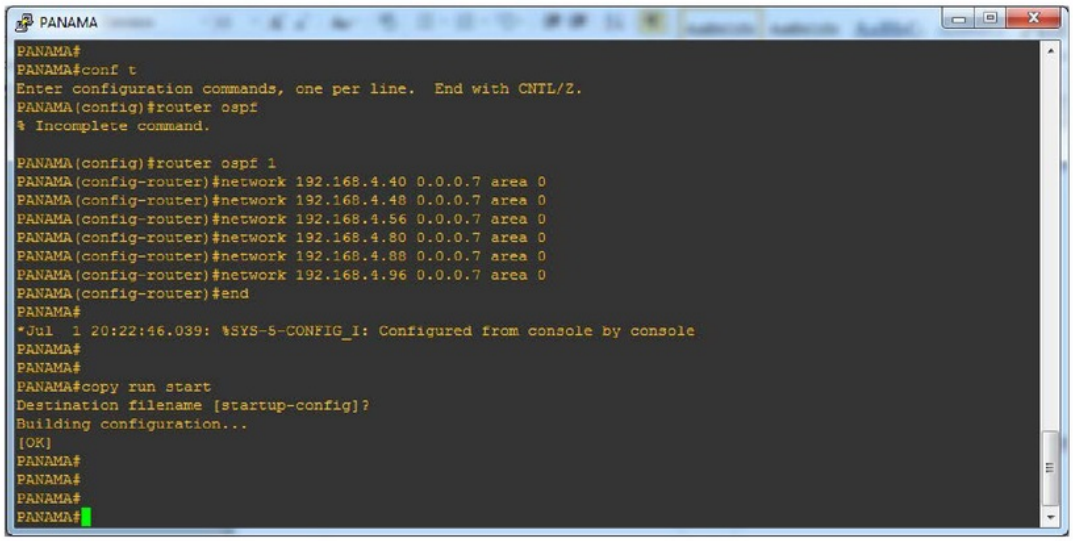


Figura 3.18. Configuración de OSPF en el router de Panamá.

3.2.5 Configuración del protocolo de gestión SNMP

Una parte medular en la gestión de una red es el protocolo SNMP, el cual ayuda a tener un control y conocimiento sobre ésta para poder detectar fallos o donde se requiera mantenimiento ya que permite establecer variables relacionadas con el estado y configuración de los hosts como routers, switches y equipos de usuarios. SNMP hace un sondeo a los agentes para obtener datos mediante los Trap SNMP como se explicó en el capítulo 2. Para configurar SNMP se utiliza el router de México y Argentina.

3.2.5.1 Configuración de administrador SNMP

Lo primero que se establece es el administrador de red (PC Mex-Windows7) y los agentes SNMP (Switch S3 y router de Argentina). Para establecer el administrador de red se utiliza el programa SNMP manager el cual se muestra en la figura 3.19.

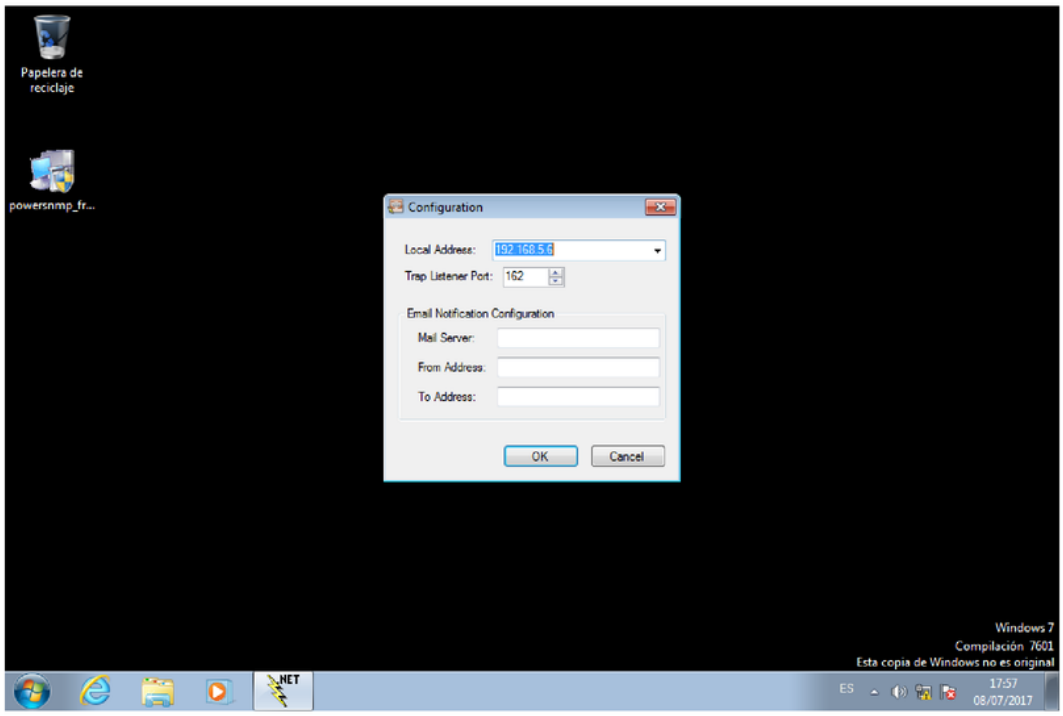


Figura 3.19. SNMP Manager ejecutado desde la máquina virtual Windows 7.

El programa SNMP Free Manager requiere establecer la dirección IP del administrador, la cual en nuestro caso es 192.168.5.6. Esta dirección es por la que va a escuchar lo que pasa en la red.

3.2.5.2 Configuración del agente SNMP

A continuación se configura el agente SNMP el cual se encargara de enviar las Trap al administrador SNMP. Para configurar el agente se utilizan los comandos que se muestran en la figura 3.20.

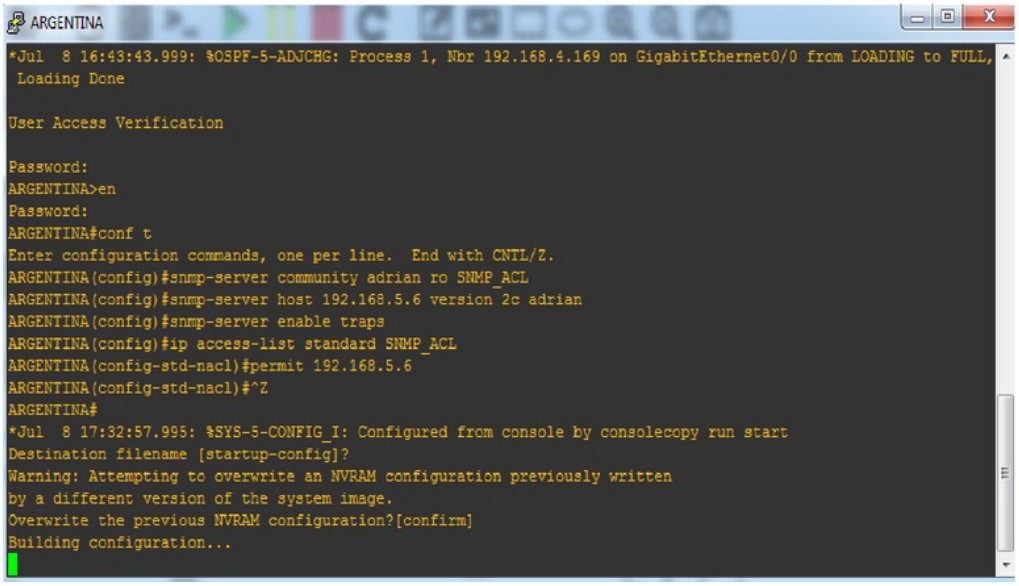


Figura 3.20. Configuración del agente SNMP en router de Argentina

Con esto se ha configurado la conectividad y gestión tanto en Packet Tracer como en GNS3, por lo cual falta comprobar dichas configuraciones, lo cual se realizará en el siguiente capítulo.

Capítulo 4 Análisis de resultados para la simulación y emulación de la red avanzada CLARA

El objetivo del presente capítulo es realizar un análisis de la simulación con Packet Tracer y GNS3 en dos aspectos clave, la conectividad y la gestión de la red. La conectividad de la red es fundamental en cualquier red que esté en funcionamiento ya que una red sin conectividad sería prácticamente inoperante, por otro lado la gestión es un complemento que ayuda a supervisar que la red esté operando correctamente y permite tener información en tiempo y forma de cualquier dispositivo, para esto se utiliza SNMP, el cual ha sido abordado en el capítulo 2.

4.1 Resultados en Packet Tracer

4.1.1 Establecimiento de adyacencias

Una vez configurado el protocolo OSPF en los routers y como complemento para ver cómo se establece la relación de adyacencia, se toma el router de Brasil para que al momento de configurar el protocolo OSPF tenga la relación de adyacencia con los demás routers a los cuales se les configuró el protocolo OSPF previamente. La figura 4.1 muestra el proceso de establecimiento de adyacencias entre routers.

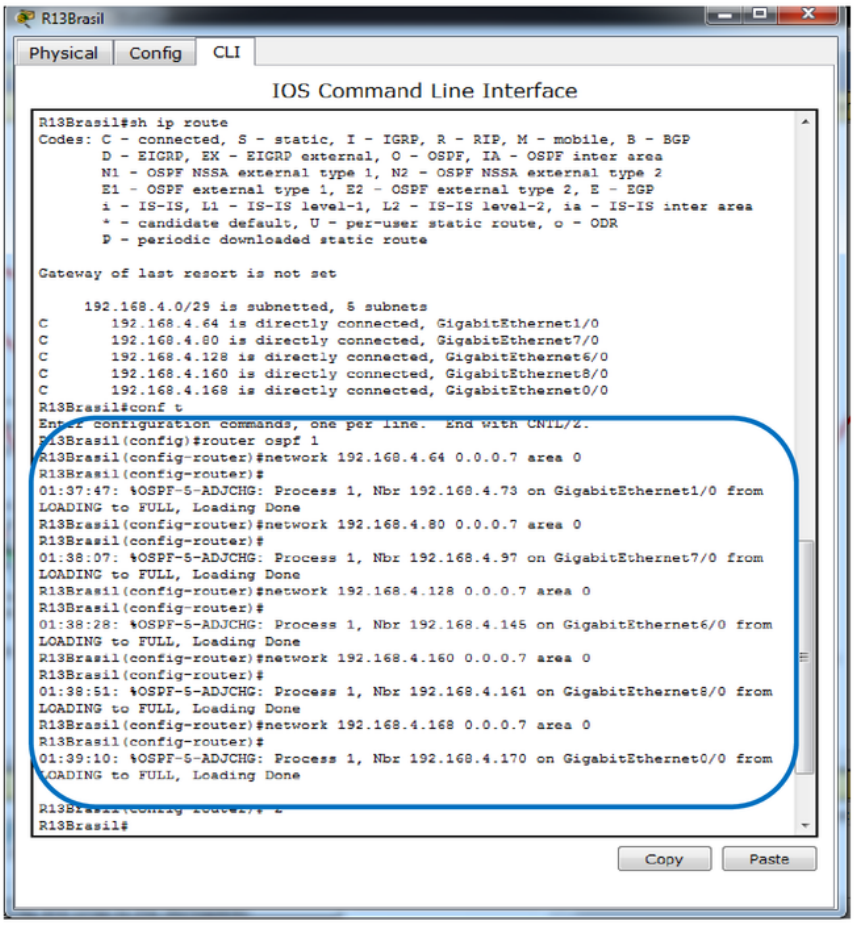


Figura 4.1 Establecimiento de adyacencias entre el router de Brasil y sus routers vecinos.

Como se puede observar el router de Brasil ha encontrado una adyacencia con sus routers vecinos (R14UK, R15Miami, R5Panamá, R13Chile, R11Argentina), con esto tiene una conectividad completa y ya se pueden mandar paquetes con sus routers vecinos y por ende a través de toda la red. Para verificar lo anterior OSPF establece una topología lógica la cual se utiliza para llegar a cualquier router es por esto que asigna rutas gateway para lograrlo. Con el comando ***show ip protocol*** se muestra el protocolo de enrutamiento que se está utilizando, las subredes de los enlaces de los vecinos que están directamente conectados, así como las rutas gateways y el tiempo de sus actualizaciones, esto para que el administrador de red cuente con los elementos necesarios para comprobar si los enrutadores vecinos están siendo reconocidos y si otros routers están ejecutando el mismo protocolo. La figura 4.2 muestra el comando *show ip route* a detalle.

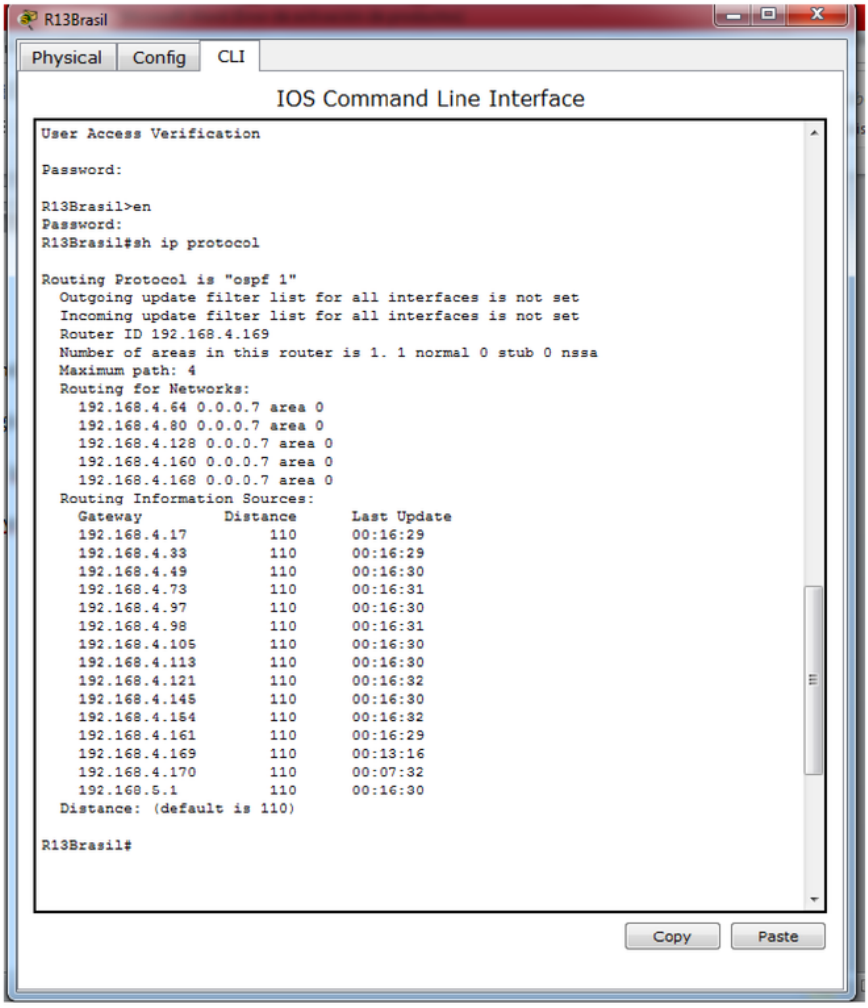


Figura 4.2. Gateways de toda la red y subredes directamente conectadas al router de Brasil.

4.1.2 Verificación de los routers vecinos

Otra forma de ver a los vecinos que tiene un router configurado con OSPF es mediante el comando ***show ip ospf neighbor*** el cual muestra el ID del router vecino, el estado de la adyacencia, la cual será completa si se configuró adecuadamente el protocolo en ambos extremos; el tipo de configuración de interfaces ya sea DR, BDR o Drother; el "dead time", el cual es el tiempo en el que un destino se considera inalcanzable y por último la prioridad, teniendo en cuenta que cuando ésta es cero el router no se convierte en DR o BDR ya que no hay adyacencia, cuando esta va de 1 a 255 el router se puede convertir en DR o BDR dependiendo su ID [66].
Para clarificar mejor lo anterior se toma como ejemplo el router de Panamá y se aplica el comando descrito, como se muestra en la figura 4.3.

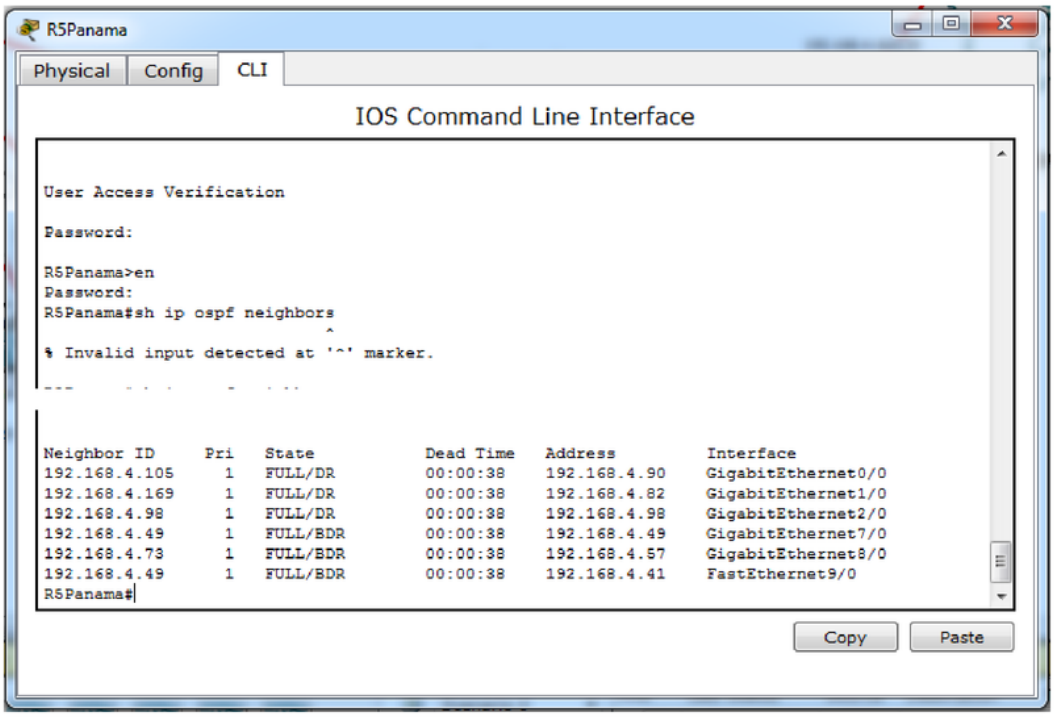


Figura 4.3 Verificación de adyacencia con el comando show ip ospf neighbor.

Como se puede observar se tienen los ID de los routers vecinos o routers de siguiente salto, al comparar con la figura 4.4 se pueden ver las direcciones IP de los neighbor ID (direcciones IP de los routers por donde saldrán los paquetes que se envíen desde el router de Panama), así como las direcciones IP que señala en la columna Address de la figura 4.3 (routers con los que está directamente conectado el router de Panamá), estas IP están dentro de la red de cada enlace.

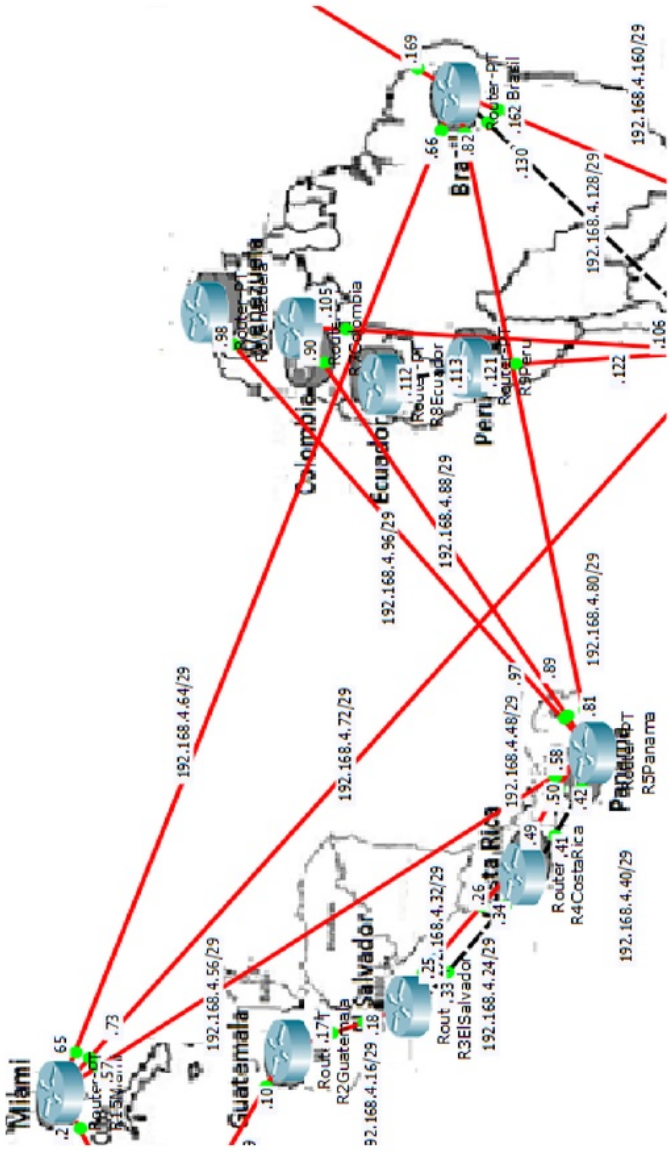


Figura 4.4. Direcciones IP que respaldan la adyacencia mostrada en la figura 4.3 en el router de Panamá.

4.1.3 Rutas y costo configuradas por OSPF

Una vez comprobada la adyacencia se pueden percibir qué rutas hay disponibles para llegar a cualquier dispositivo en la red, mediante el comando ***show ip route*** se pueden observar las diferentes redes aprendidas por los routers mediante el protocolo OSPF. Se toma nuevamente el router de panamá para ejecutar dicho comando como se muestra en la figura 4.5.

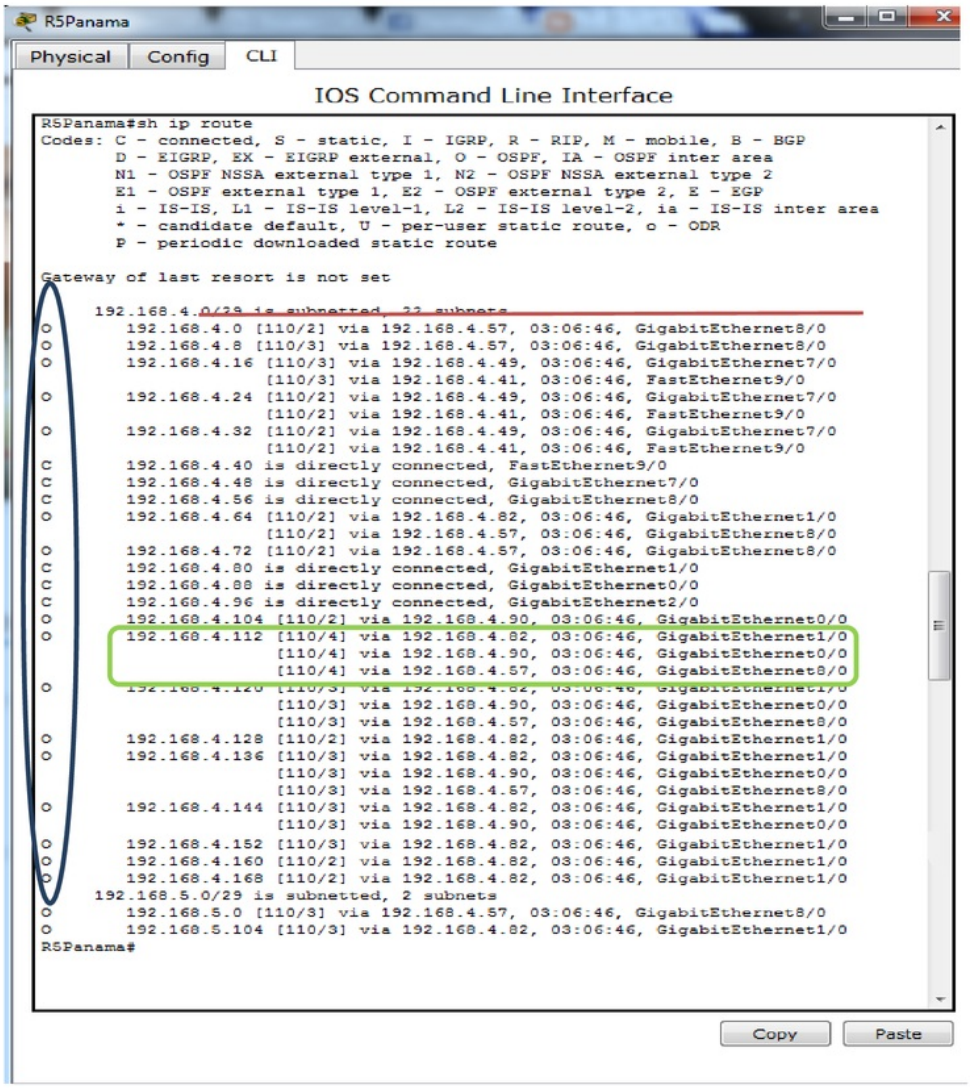


Figura 4.5. Comando *show ip route*.

Como se puede observar en el ovalo vertical se tienen todos los enlaces ejecutando el protocolo OSPF (O) además de los enlaces directamente conectados (C). Se

tienen 22 subredes /29 en total. Se toma como ejemplo la dirección IP 192.168.4.0 (línea roja), la cual es la subred del enlace de México a Miami, ésta es alcanzable vía la interfaz G8/0 del router de Miami cuya dirección IP es 192.168.4.57, el costo es de 2 ya que pasa por 2 enlaces con un costo de 1 para llegar a su destino. Cabe aclarar que cualquier enlace igual o mayor a 100 Mbps tendrá un costo de 1, esto con base en la tabla 3.3. Por otro lado si queremos llegar a la subred 192.168.4.112, la cual corresponde al enlace entre **Ecuador y Perú**, es alcanzable de **tres** formas (área rectangular figura 4.5), la primera es vía la interfaz G1/0 del router de Brasil cuya dirección IP es 192.168.4.82 con un costo de 4. La segunda es vía la interfaz G0/0 del router de Colombia cuya dirección IP es 192.168.4.90 con un costo de 4. La tercera es vía la interfaz G8/0 del router de Miami cuya dirección IP es 192.168.4.57 con un costo de 4. Al tener estas tres rutas un costo de 4 el administrador de red podría, de ser necesario modificar el costo para optimizar los recursos ya que como tenemos diferentes rutas con el mismo costo, OSPF podrá tomar diferentes caminos para llegar a un mismo destino. Dado que en este caso todos costos son iguales hay dos alternativas, la primera implica dejarlas así en caso de que un enlace no funcione tener otra ruta con el mismo costo, la segunda es asignar costos de tal manera que el enrutamiento se haga por enlaces pre-establecidos por el administrador de red. Para empezar, hay que comprobar el costo de los enlaces analizados en el enlace de Panamá en el ejemplo anterior. Para ello, se utiliza el comando *show int G1/0* para conocer el ancho de banda de la interfaz, el cual se muestra en la figura 4.6.

```
R5Panama#sh int G1/0
GigabitEthernet1/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0040.0b45.5c53 (bia 0040.0b45.5c53)
  Internet address is 192.168.4.81/29
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

Figura 4.6. Verificación de ancho de banda de la interfaz G1/0.

Al aplicar la fórmula de la tabla 2.3 nos da que el costo es 0.1 lo cual converge a 1. En la figura 4.7 se puede verificar el costo de la interfaz. El mismo procedimiento aplica a los otros dos enlaces.

```
R5Panama#sh ip ospf int G1/0

GigabitEthernet1/0 is up, line protocol is up
  Internet address is 192.168.4.81/29, Area 0
  Process ID 1, Router ID 192.168.4.97, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
```

Figura 4.7. Validación del costo.

Dado que todos los enlaces son superiores a 100 Mbps tenemos que todos los enlaces tendrán un costo de 1. El siguiente paso es ver las rutas que toma el protocolo OSPF para llegar al enlace que conecta Ecuador y Perú, como se mencionó hay tres formas para llegar a dicho enlace. En las figuras 4.8 a 4.10 se muestran las tres rutas, mismas que se pueden constatar con la figura 4.4.

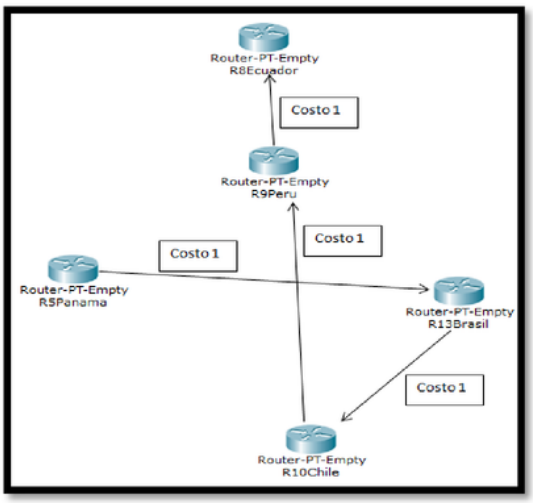


Figura 4.8 Primer ruta para llegar al router de Ecuador.

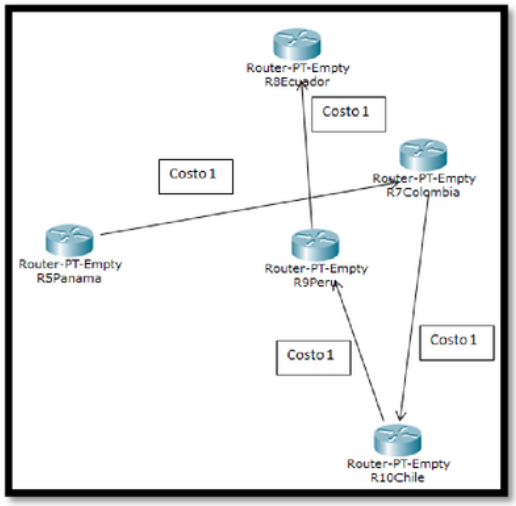


Figura 4.9 Segunda ruta para llegar al router de Ecuador.

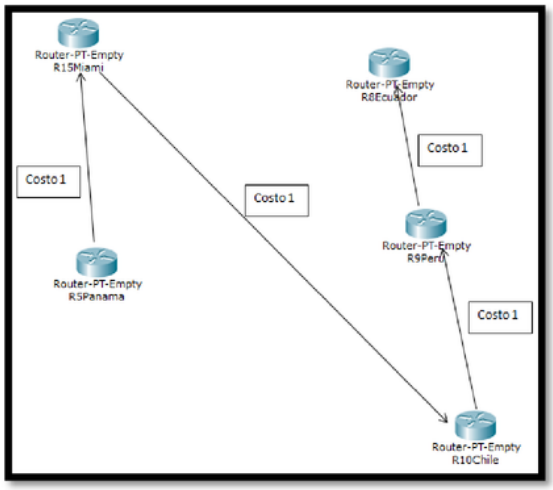


Figura 4.10. Tercera ruta para llegar al router de Ecuador.

4.1.4 Rutas y costos configurados por el administrador de red

Ahora bien, si se necesita que se envíen los datos sólo por una de esas tres rutas es ahí donde se configura otro costo a algún enlace de las otras dos rutas para que de esta forma solo haya una ruta del nodo de Panamá al de Ecuador. Supongamos que se elige la ruta de Colombia, es decir la de la figura 4.9, esto por cuestiones geográficas sabemos que es la ruta más corta, no así OSPF, el cual sólo maneja costos. Para arreglar esto se configura el costo a las interfaces de las subredes de Brasil (G8/0) y Miami (G1/0) para asegurar que la única ruta sea la de la subred de

Colombia, esto mediante el comando *ip ospf cost 2.* Como se muestra en la figura 4.11.

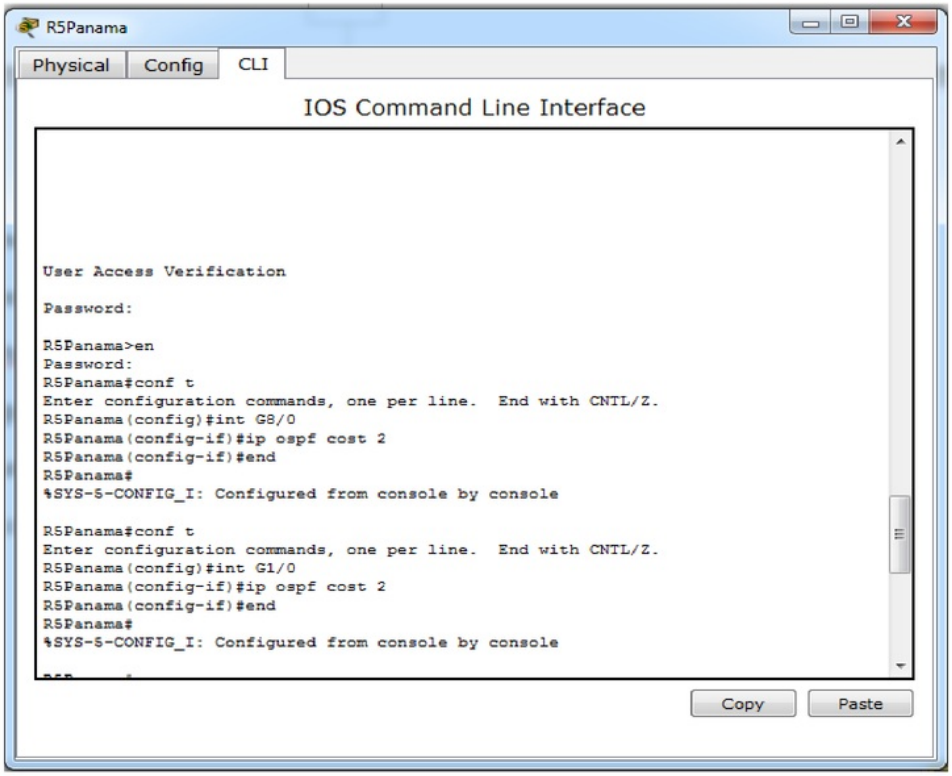


Figura 4.11. Configuración del costo a las interfaces de Brasil y Miami.

Para corroborar la configuración anterior se usa el comando *show ip ospf interface.* Como se muestra en la figura 4.12.

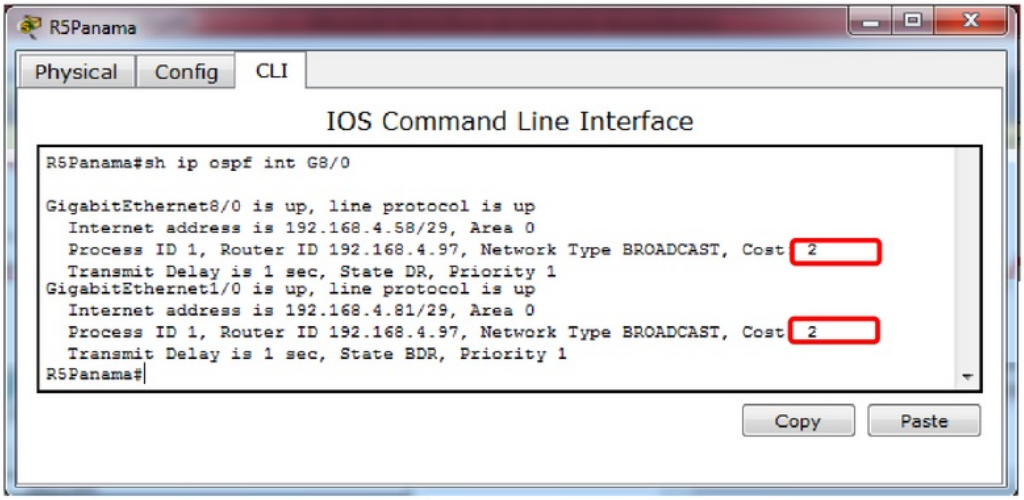


Figura 4.12. Información del nuevo costo de los enlaces de Brasil y Miami.

Ahora bien, debido a la configuración anterior debería quedar solo una ruta para llegar a la subred del enlace de Ecuador a Perú, como se muestra en la figura 4.13 al utilizar el comando ***show ip route***. Si comparamos la figura 4.5 y la 4.13 se ve que las rutas que llegaban al enlace de Ecuador a Perú cambiaron, ya que en efecto con la reasignación de los costos, ahora solo queda una ruta (vía la interface 192.168.4.90) en vez de las tres rutas que originalmente se contemplaban.

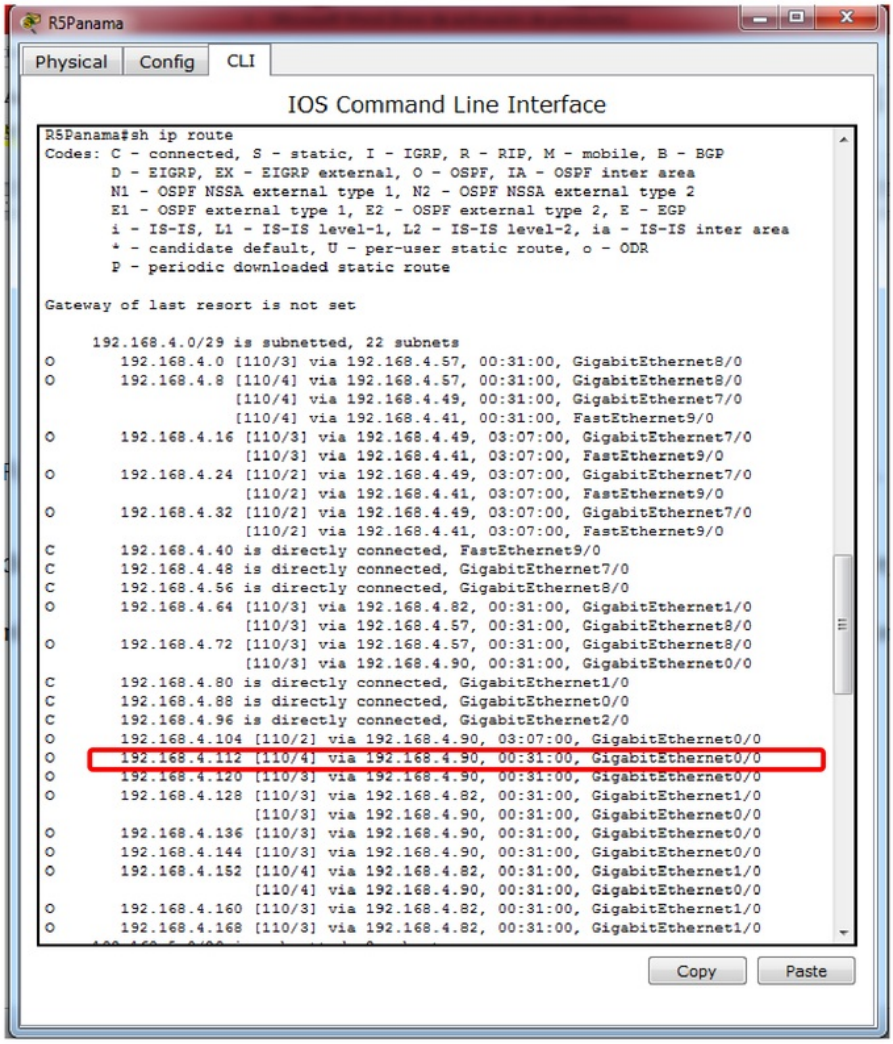


Figura 4.13. Ruta única para llegar a la subred que comprende el enlace de Perú – Ecuador.

4.1.5 Pruebas de conectividad en la simulación de la red CLARA

Para realizar las pruebas de conectividad se añadió un switch y una PC en el router de México, al de Brasil y al de UK. Para añadir las subredes que contendrán a las PC en ambos routers, con base a la tabla 3.5, la subred correspondiente a México es la

192.168.5.0/29, la 192.168.5.96/29 corresponde a Brasil y 192.168.5.104/29 para UK. Por lo que para las PC se tiene la información de la tabla 4.1.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
PC0 (MEX)	Fa0/0	192.168.5.2	255.255.255.248	192.168.5.1
PC3(BR)	Fa0/0	192.268.5.98	255.255.255.248	192.268.5.97
PC2(UK)	Fa0/0	192.168.5.106	255.255.255.248	192.168.5.105

Tabla 4.1. Asignación de direcciones IP y gateways a las PC de Brasil y México.

Una vez asignadas las direcciones es necesario comprobar las conexiones mediante el comando ***ping***, el cual se ejecuta desde ambas PC. En la figura 4.14 se muestra el ping desde la PC de México a Brasil.

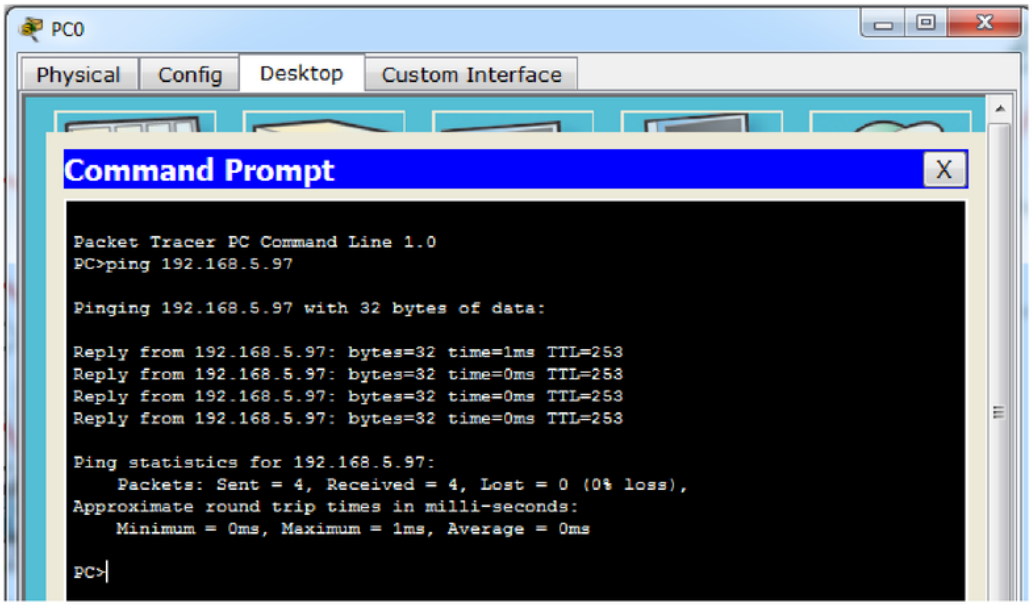


Figura 4.14. Ping desde el router de México a Brasil.

En la figura 4.15 se muestra el ping desde Brasil a UK.

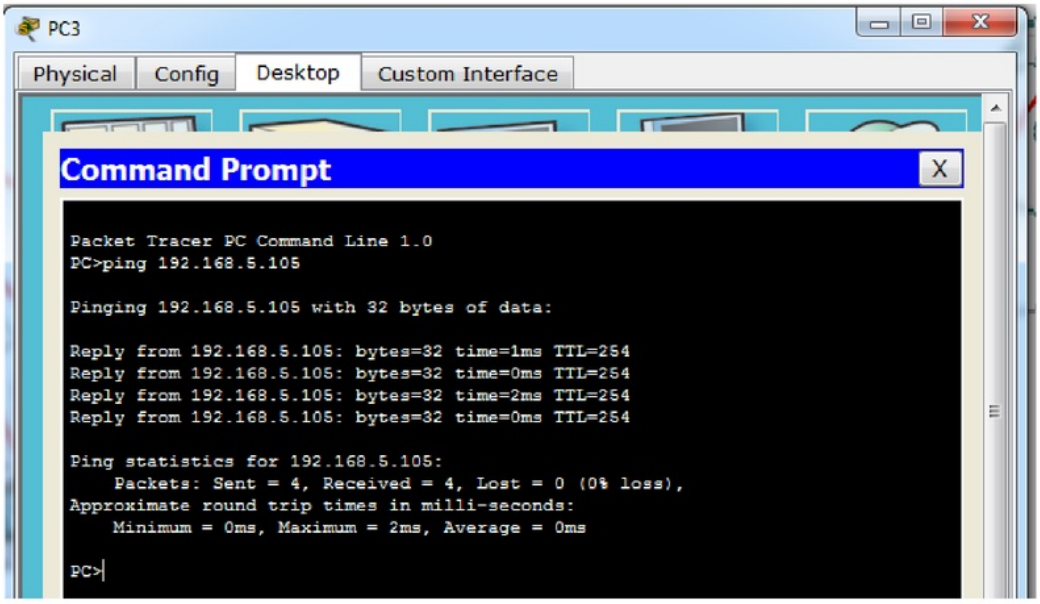


Figura 4.15. Ping desde el router de Brasil a UK.

Por último en la figura 4.16 se muestra el ping de UK a México.

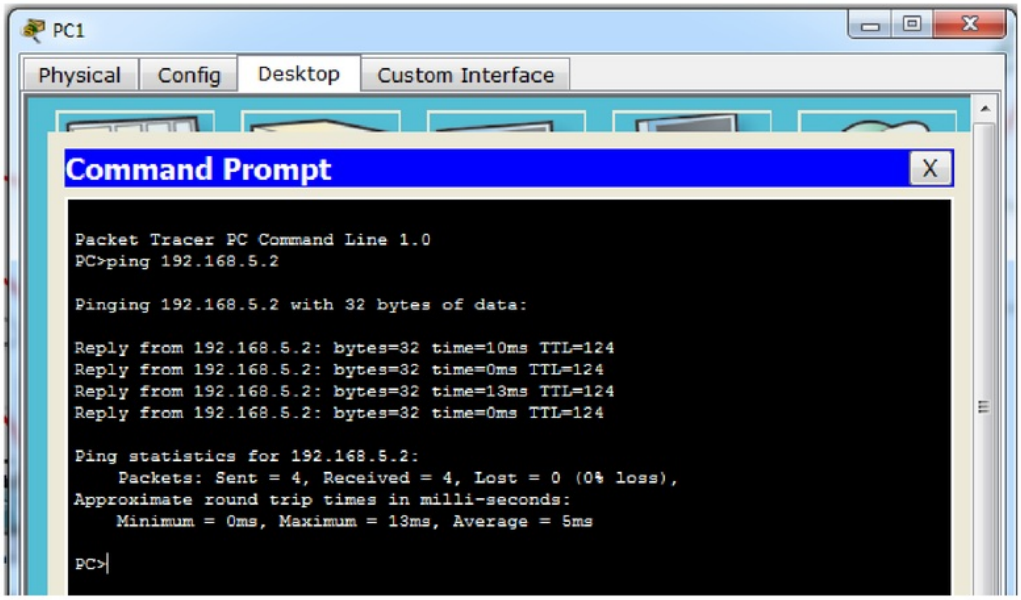


Figura 4.16. Ping de UK a México.

En las figuras anteriores se observa que hay conectividad entre los routers con un tiempo de respuesta entre 1 y 13 ms.

4.1.6 Paquetes OSPF en Packet Tracer

Dado que las actualizaciones de OSPF son automáticas Packet Tracer no permite mandar un paquete OSPF manualmente. Para ver un paquete OSPF en Packet Tracer se debe editar el filtro para de esta manera sólo queden paquetes OSPF. Como se observa en la figura 4.17.

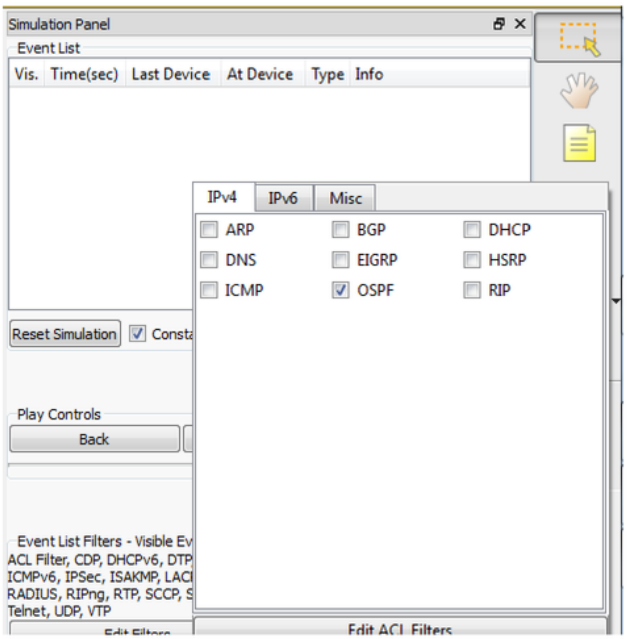


Figura 4.17. Filtrado de paquetes OSPF.

Una vez aplicado el filtro solo se usa la opción capture/forward para ver cómo se van enviando los paquetes Hello, esto evidentemente solo entre routers vecinos. En la figura 4.18 se muestra un paquete enviado de Miami a Brasil. Por lo tanto el paquete a analizar será el de Brasil.

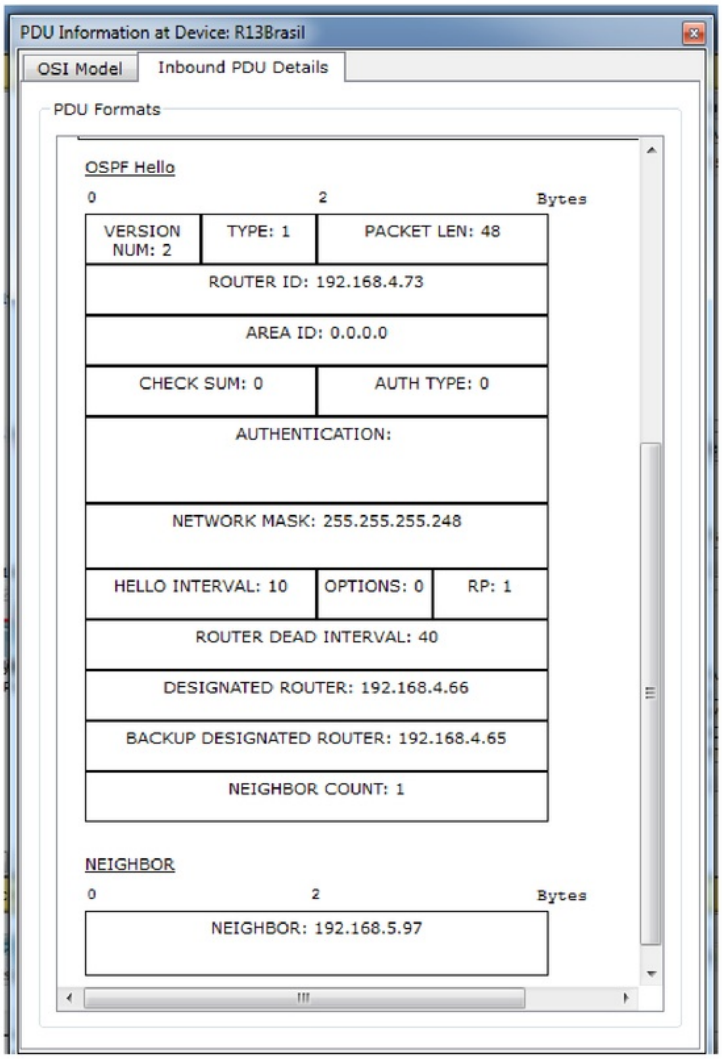


Figura 4.18. Detalles paquete OSPF.

El paquete OSPF Hello revela diferente tipo de información relacionada al protocolo y a la red en la que se está ejecutando. Este paquete es muy parecido al de la figura 4.18. En la tabla 4.2 se describen los parámetros del paquete.

Parámetro	Valor	Significado
Versión	2	Versión de OSPF
Tipo	1	Tipo de paquete OSPF 1 para Hello
Packet lenght	48	Tamaño del paquete
Router ID	192.168.4.73	Dirección IP del router ID en este caso la dirección IP más grande en el router de Miami
Area ID	0.0.0.0	El área que se configuró. Cero para backbone
Checksum	0	No hay suma de verificación de errores
Auth Type	0	No hay algún tipo de autenticación
Authentication	Sin valor	
Network Mask	255.255.255.248	La máscara de subred. Del enlace de Brasil a Miami
Hello Interval	10	Intervalo de saludo entre los routers expresado en segundos
Options	0	Opciones en los paquetes Hello, LSA y BD para soportar una combinación de capacidades de coexistir en un único Sistema Autónomo
Router Priority	1	Prioridad del router
Router Dead	40	Tiempo para que el router se considere inalcanzable
Designed Router	192.168.4.66	Router designado o router principal, para que represente el punto de recolección y distribución de las LSA enviadas y recibidas y de esa forma evitar la saturación de LSA en toda la red. En este caso es el mismo a través de su interfaz G1/0
Backup Designed Router	192.168.65	Router principal de respaldo. El de Miami a través de su interfaz 1/0
Neighbor Count	1	El número Identificador de un router vecino
Neighbor	192.168.4.97	Este ID es utilizado para descubrir y responder a nuevos routers. En este caso en el router de Panama a través de su interfaz G2/0

Tabla 4.2. Descripción de los parámetros del paquete OSPF.

4.1.7 Pruebas SNMP en Packet Tracer

Ahora que ya está configurado el protocolo SNMP es posible ver distintas características que ofrece el entorno de Packet Tracer, lo primero es saber si hay una red de gestión activa, para esto se establece en la PC0 con dirección IP 192.168.5.2, que se encuentra en el router de México, para acceder desde ella hacia el router de UK con dirección IP 192.168.4.170 (R14UK), esto con la finalidad de ver los parámetros que muestra SNMP en el simulador. A continuación se muestra el proceso para acceder al router de UK. En la figura 4.19 se muestra el ingreso a la MIB browser desde el PC0.

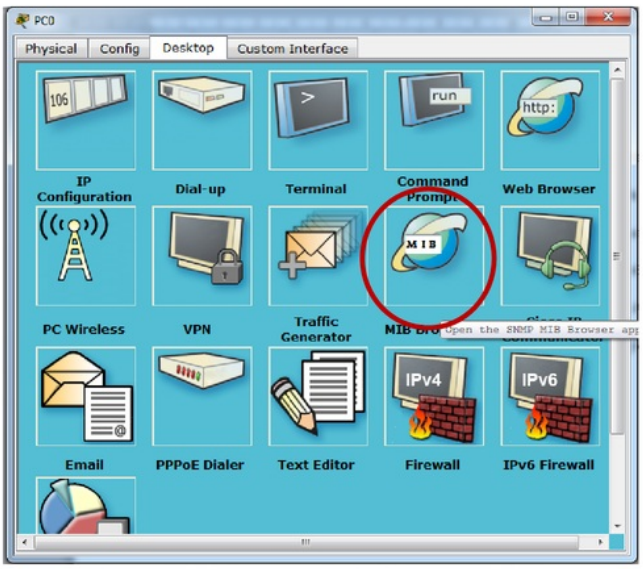


Figura 4.19. Acceso a la MIB desde la PC0.

En la MIB Browser se puede configurar la IP del router hacia el cual se desea acceder, el nombre de comunidad de lectura y escritura que se estableció en la activación de SNMP, así como la versión que se utilizara. En la figura 4.20 se muestra la configuración del MIB Browser.

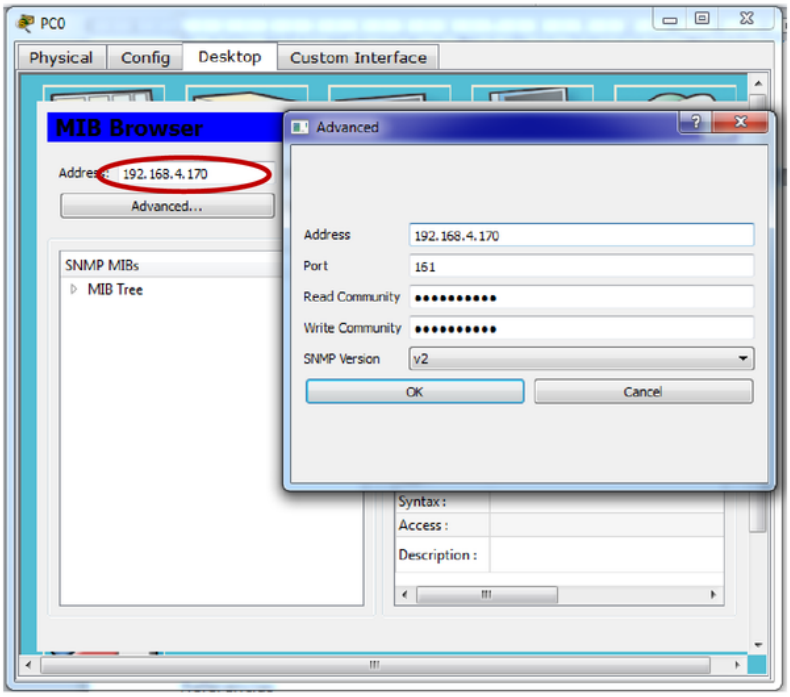


Figura 4.20. Configuración del MIB Browser.

Una vez configurada la MIB Browser, se tiene en efecto acceso a la MIB del router, la cual muestra el conjunto de OID con las que cuenta el router. Por ejemplo, si queremos ver la información del sistema (sysDescr) del router, se accede mediante el OID correspondiente como se ve en la figura 4.21 y después se selecciona la operación ***Get*** y se selecciona Go. La figura 4.21 muestra diversos parámetros que son dignos de examinar. Primero se tiene en el apartado result table el OID, el cual muestra un árbol MIB parecido al que nos referimos en la figura 2.29, aquí el árbol MIB es compuesto por el OID .1.3.6.1.2.1.1.1.0, el nombre de este OID es *Sysname* y, como se puede ver en la región roja de la figura, muestra información del sistema como el tipo de hardware del router, el IOS del router, la versión del software, etc.

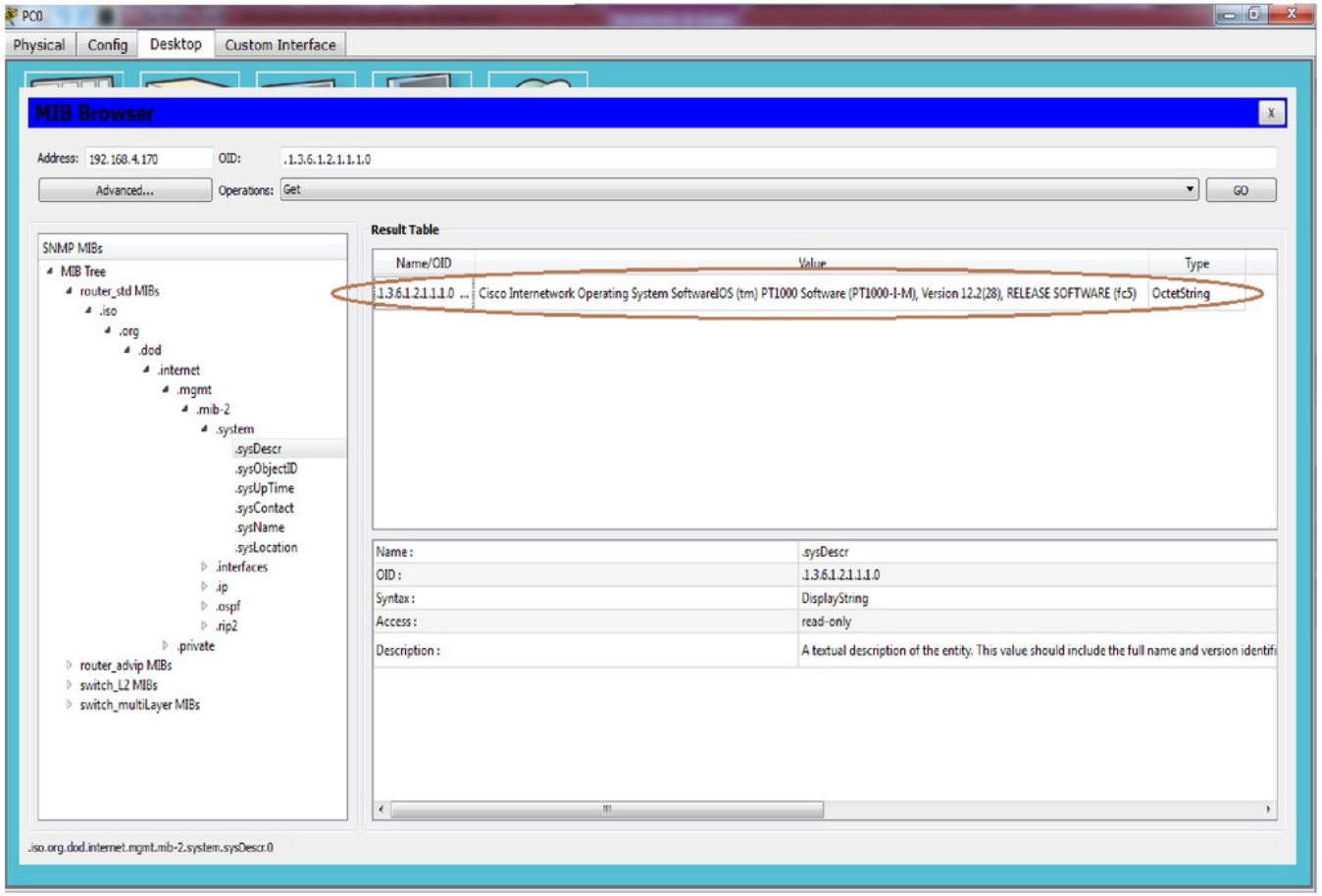


Figura 4.21. OID para sysDescribe.

Otro OID relevante es el de ifDescribe el cual permite ver las interfaces con las que cuenta el router de UK. Ver figura 4.22.

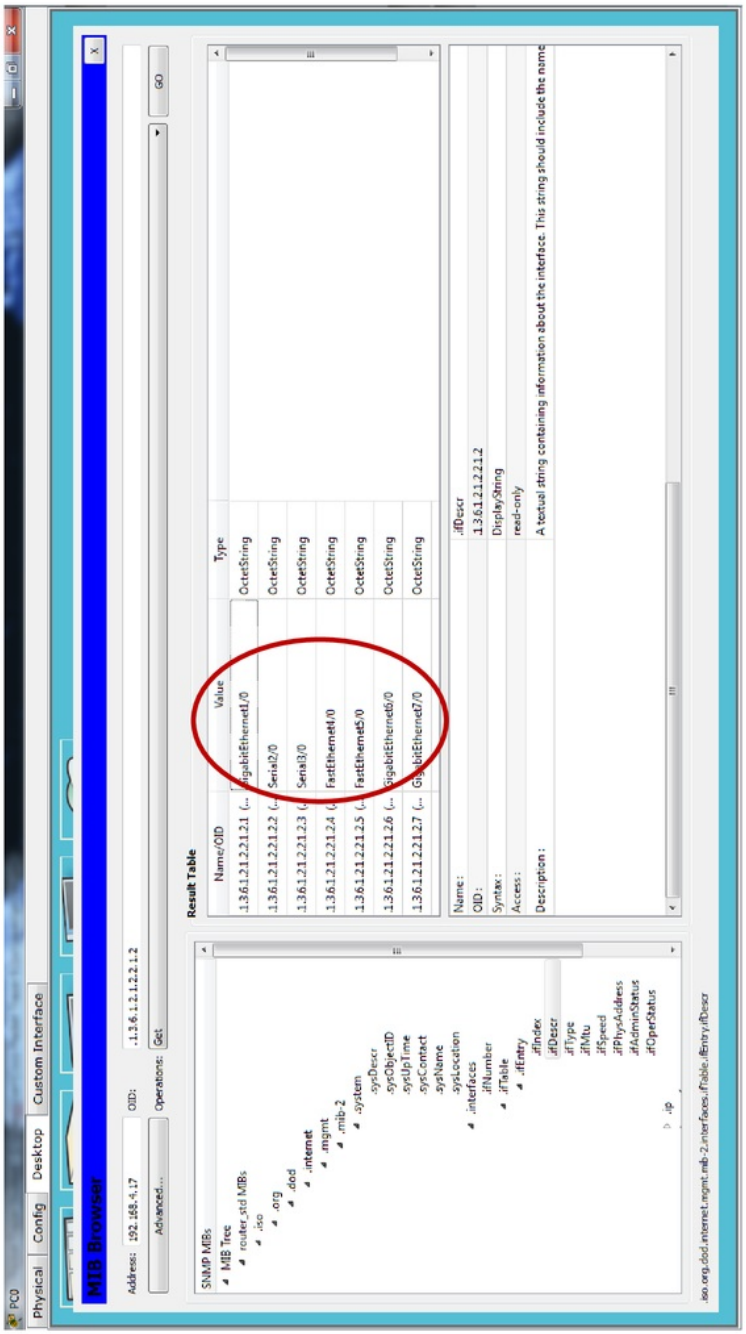


Figura 4.22. OID ifDescribe.

Por otra parte el OID ipRouteDest muestra las subredes que se han configurado en toda la red, como se ve en la figura 4.23.

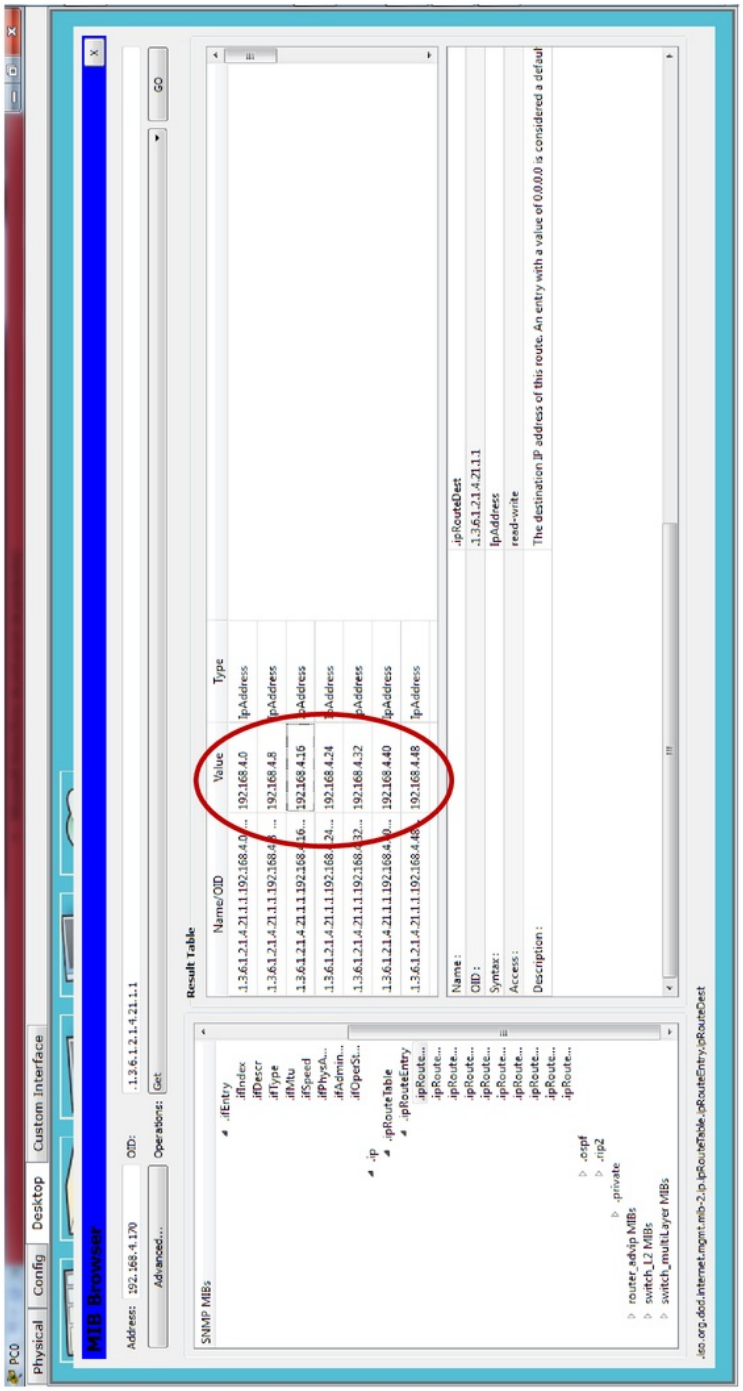


Figura 4.23. OID ipRouteDest.

El OID sysName muestra el nombre del router en este caso R14UK. Ver figura 4.24.

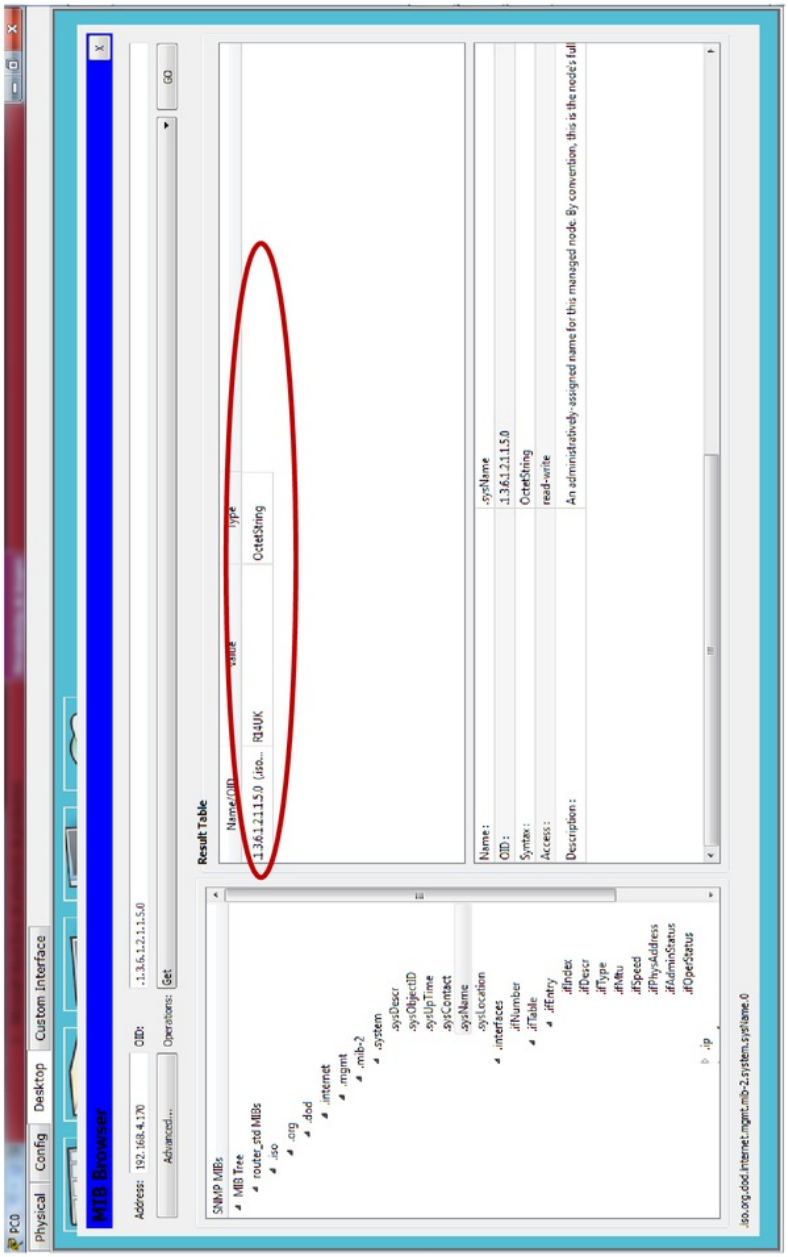


Figura 4.24 OID sysName.

Una aplicación muy común es cuando se quiere cambiar un valor de un parámetro desde una PC. Por ejemplo, si el NOC de la red CLARA se encontrará en México, se podría cambiar el nombre del router de UK desde el NOC. En Packet Tracer se hace de la siguiente manera: para empezar se elige la opción sysUpName, después en la pestaña operations se cambia la opción de get a ***set*** para de esta forma poder cambiar el parámetro correspondiente. En la figura 4.25 se ejemplifica lo anterior.

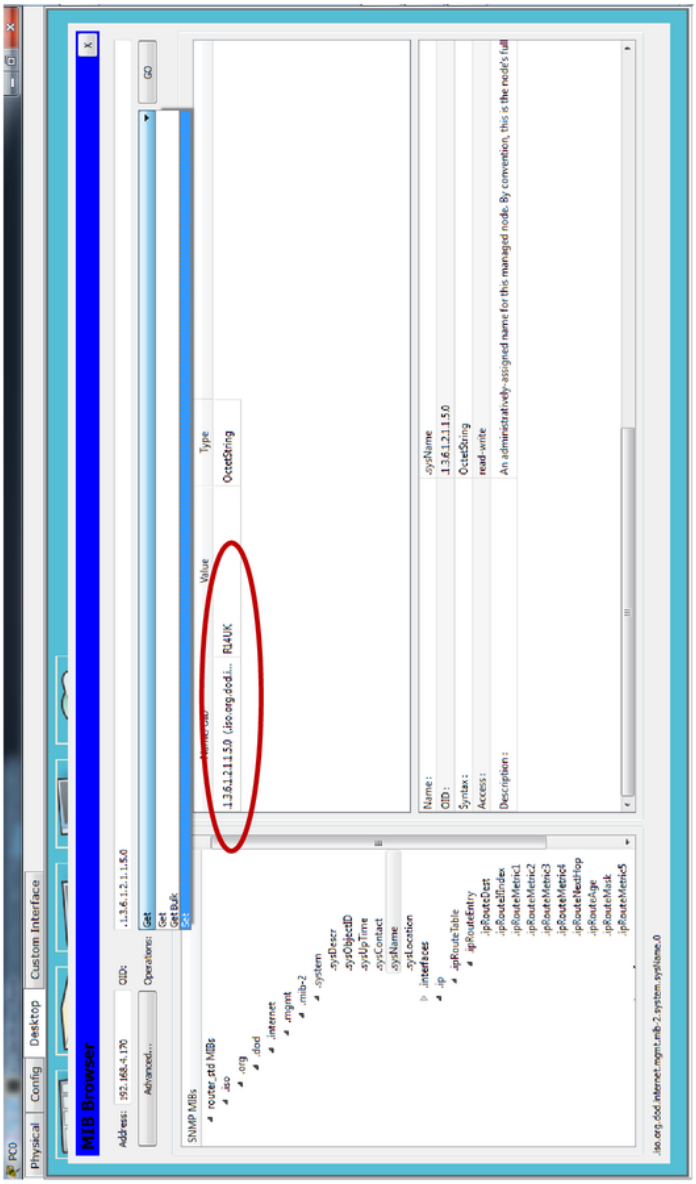


Figura 4.25. Operador set en sysName.

Al presionar GO debemos cambiar el data type el cual será OctecString, para poder ponerle un nombre. En este caso el nuevo nombre será R14UnitedKingdom. En la figura 4.26 se ejemplifica lo anterior.

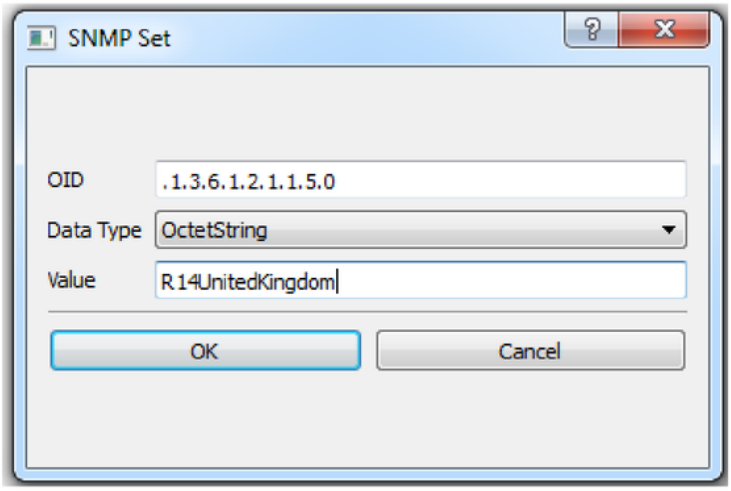


Figura 4.26. Configurador operador set.

Para corroborar lo anterior se puede ir al router de UK y observar el cambio de configuración del nombre. Como se muestra en la figura 4.27 es diferente con respecto a la figura 4.24.

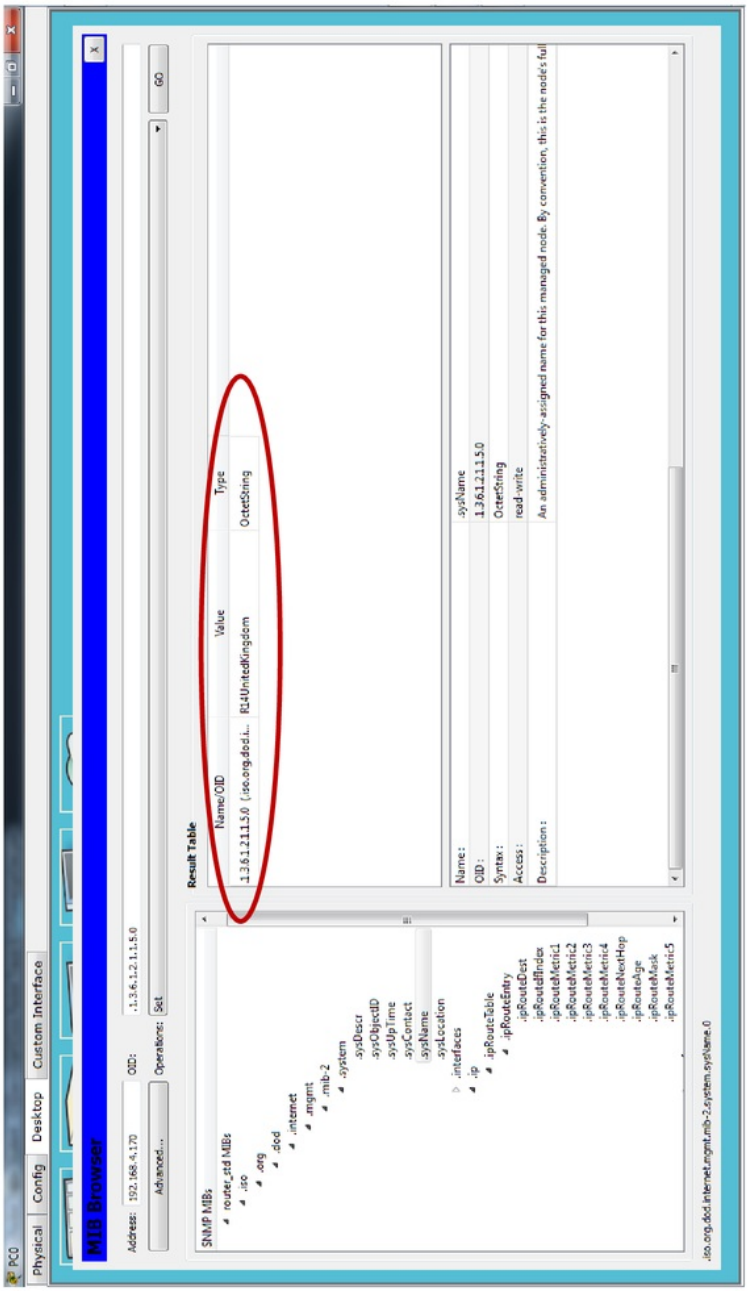


Figura 4.27. Cambio del nombre del router de UK.

Por último es importante conocer la diferencia en lo que se refiere a uso de recursos, por lo que es preciso saber los recursos que la simulación en Packet Tracer ha consumido, esto durante el envió de mensajes entre los routers desde UK hasta México, para esto se utiliza la opción de administrador de tareas de Windows que permite conocer el uso de CPU y de memoria RAM. En la figura 4.28 se muestra el uso de recursos en Packet Tracer.

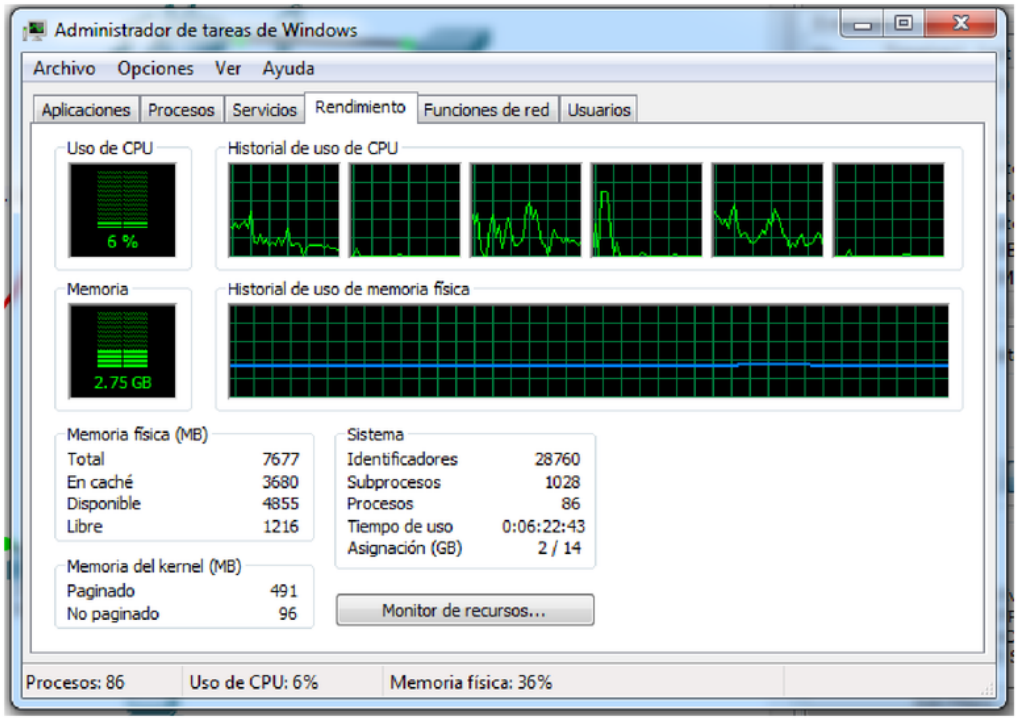


Figura 4.28. Uso de recursos de la simulación en Packet Tracer.

Como se puede observar hay un uso total de CPU del 6 % el cual está divido en cada uno de los núcleos del procesador, p0or otro lado hay un uso de memoria RAM de 2.75 GB equivalente a un 36% del total con el que cuenta el equipo.

4.2 Análisis de resultados en GNS3

4.2.1 Establecimiento de adyacencias en GNS3

Cuando se configura OSPF cada router establece una adyacencia con su router vecino, esto hace que se tenga conocimiento completo y global de toda la red y que entre todos los routers se tenga una topología general que servirá para calcular el camino más corto de las rutas. En la figura 4.29 se muestra el procedimiento de formación de adyacencias en cada interfaz del router de Chile.

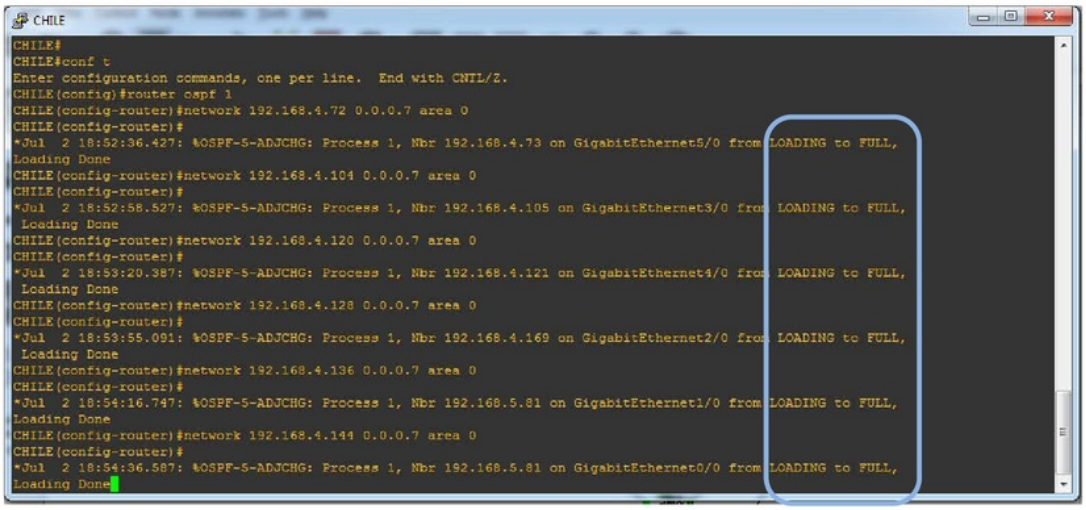


Figura 4.29. Establecimiento de adyacencias entre el router de Chile y sus vecinos.

El establecimiento de adyacencias ocurre solo cuando se ha configurado OSPF en los routers vecinos. En la figura anterior podemos observar cómo cambia el estado del router de LOADING a FULL, con esto se tiene una conectividad completa del router con sus vecinos. Para verificar la información que OSPF tiene de toda la red, OSPF asigna rutas gateway para llegar a cualquier router que se encuentre en la red. En la figura 4.30 se muestran las subredes de los enlaces vecinos que están directamente conectados, de igual forma se observan las rutas gateway, esto es posible de notar mediante el comando *show ip route*. Para ejemplificar lo anterior se toma como referencia el router de Chile.

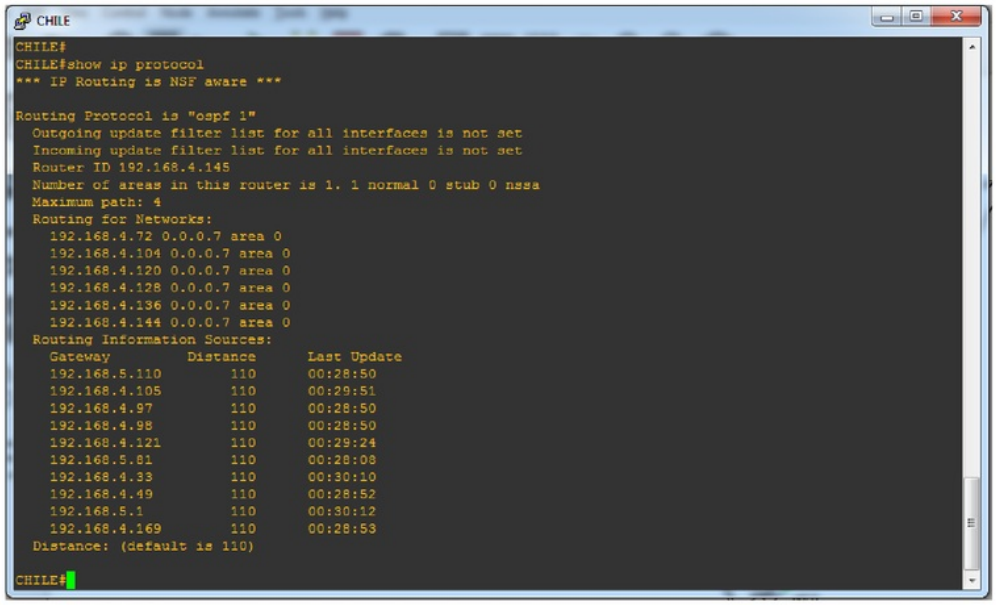


Figura 4.30. Gateways de toda la red y subredes directamente conectadas al router de Chile.

4.2.2 Verificación de los routers vecinos

Para asegurarnos que OSPF está bien configurado, en los vecinos se puede usar el comando *show ip ospf neighbor,* el cual muestra el ID del router vecino, el estado de la adyacencia que será FULL si se configuró adecuadamente en ambos extremos, el tipo de configuración de interfaces ya sea DR, BDR o Drother; el dead time y por último la prioridad. En la figura 4.31 se muestra el comando descrito.

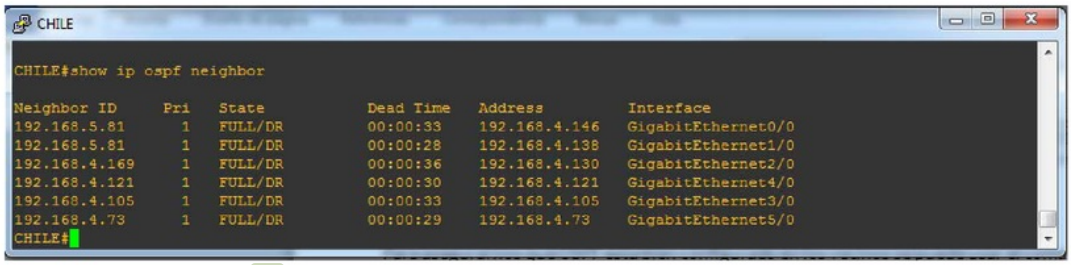


Figura 4.31. Verificación de adyacencia con el comando *show ip ospf neighbor*.

4.2.3 Rutas y costos en OSPF

Cuando ya se han establecido las adyacencias es posible ver qué rutas tiene OSPF disponibles para llegar a sus diferentes destinos y a través de qué subredes, para observar lo anterior se ejecuta el comando *show ip route*, la figura 4.32 muestra dicho comando así como las subredes configuradas y el costo que toma llegar a los diferentes posibles destinos.

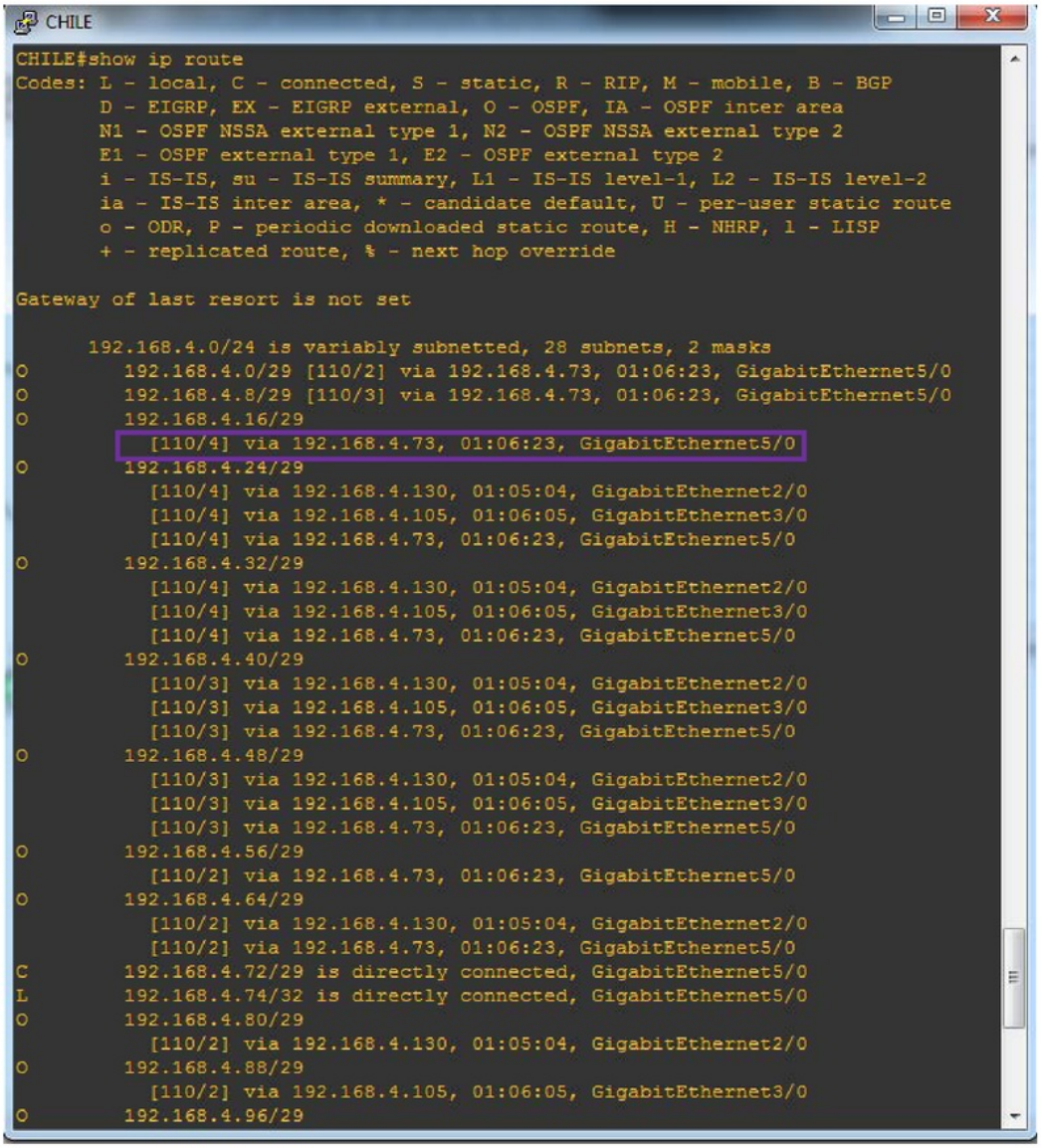


Figura 4.32. Comando show ip route.

De manera general este comando indica que desde el router actual no es posible llegar a una determinada red desde una interfaz del router a través de una dirección IP en un gateway vecino. Por ejemplo, con base en la figura anterior, si queremos llegar desde el router de Chile hacia el router de México llegaremos a la subred destino 192.168.4.0/29 (subred que contempla el enlace de México - Miami) por la dirección IP 192.168.4.73 (router Miami) a través de la interfaz GigabitEthernet 5/0 (interfaz que contempla el enlace de Chile - Miami) en el router de Chile. Cabe mencionar que el costo será de 2.

Las rutas y costos configurados por el administrador de red usan la misma metodología que en Packet Tracer desarrollada en la sección 4.1.4.

4.2.4 Pruebas de conectividad en GNS3

Para las pruebas de conectividad se utilizan tres PC en los routers de México, Argentina y UK debido a que son puntos medulares en la red CLARA, para esto se utilizan el comando ping para verificar la conectividad entre México➔Argentina; Argentina ➔ UK y por último UK ➔México, con base en la tabla 4.3.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
PC Virtualizada (MEX)	Fa0	192.168.5.6	255.255.255.248	192.168.5.1
PC4(ARG)	Fa0	192.268.5.85	255.255.255.248	192.268.5.81
PC3 (UK)	Fa0	192.168.5.107	255.255.255.248	192.168.5.110

Tabla 4.3. Direcciones IP correspondientes a las PC de UK, Argentina y México.

Primero se ejecuta el comando ping desde México (PC Windows 7) hasta Argentina (PC4), la figura 4.33 muestra la conectividad entre las PC mencionadas.

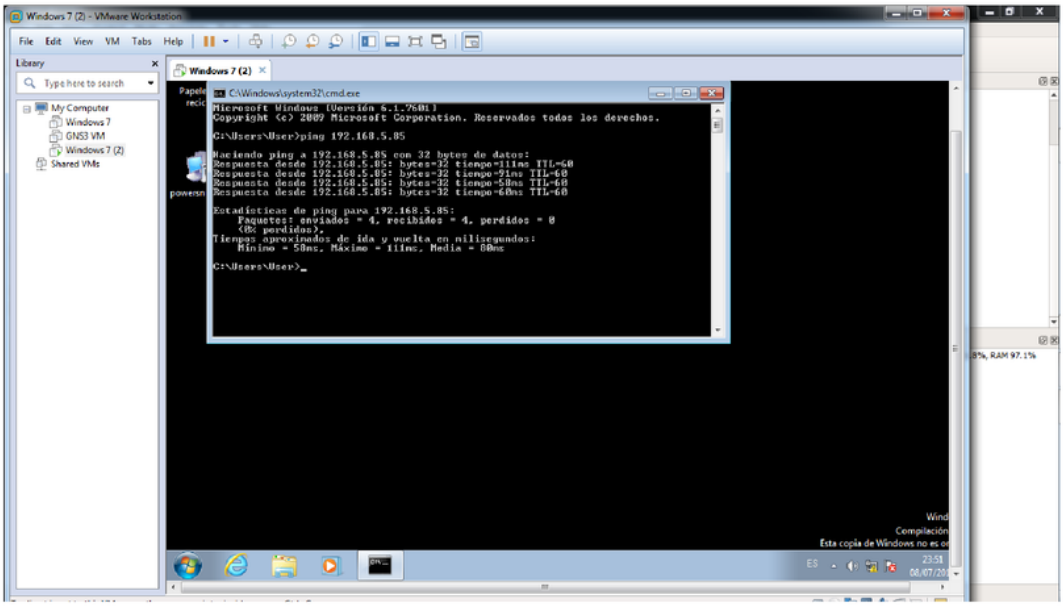


Figura 4.33. Ping desde la PC de México hasta la PC de Argentina.

En la figura 4.34 se muestra el ping desde la PC4 de Argentina a la PC3 de UK.

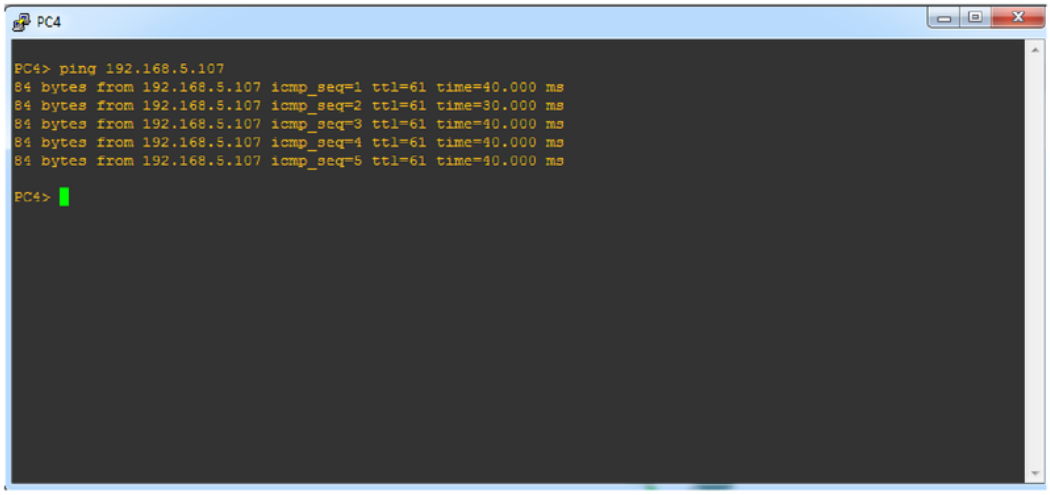


Figura 4.34. Ping desde la PC de Argentina hasta la PC de UK.

En la figura 4.35 se muestra el ping desde la PC3 de UK hasta la PC (Windows 7) de México.

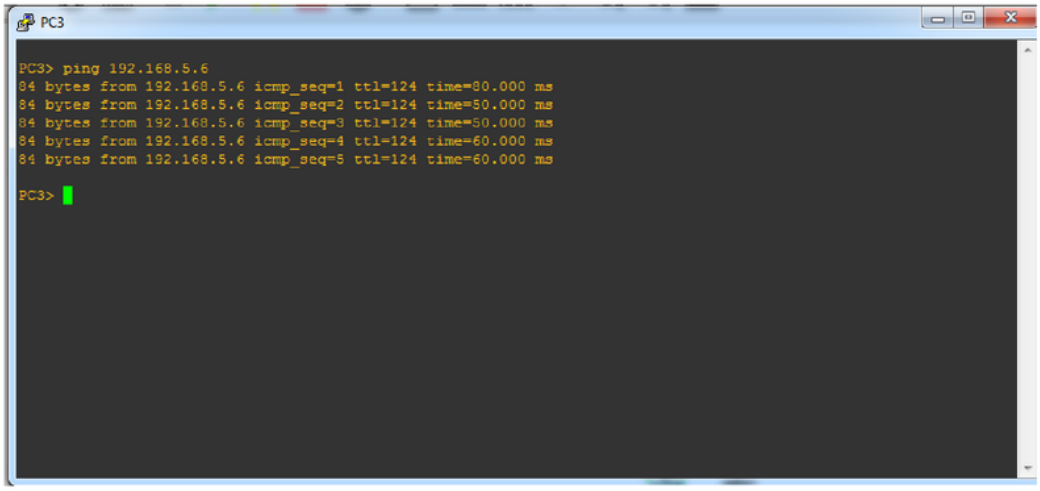


Figura 4.35. Ping desde la PC de Argentina hasta la PC de México.

Con la ejecución de dichos comandos se puede comprobar que hay una conectividad completa en toda la red mediante el protocolo OSPF.

4.2.5 Paquetes OSPF con Wireshark

GNS3 permite hacer uso de una herramienta muy importante para el análisis de paquetes: Wireshark, el cual permite observar paquetes que Packet Tracer no mostraba, por ejemplo las actualizaciones de OSPF, las cuales se muestran a continuación. Para esto, se toma el router de México y Miami para ver los paquetes

que se envían entre este enlace. La figura 4.36 muestra los paquetes enviados entre el router de México y Miami antes de las actualizaciones por ello sólo muestra paquetes Hello y paquetes Reply para verificar la adyacencia.

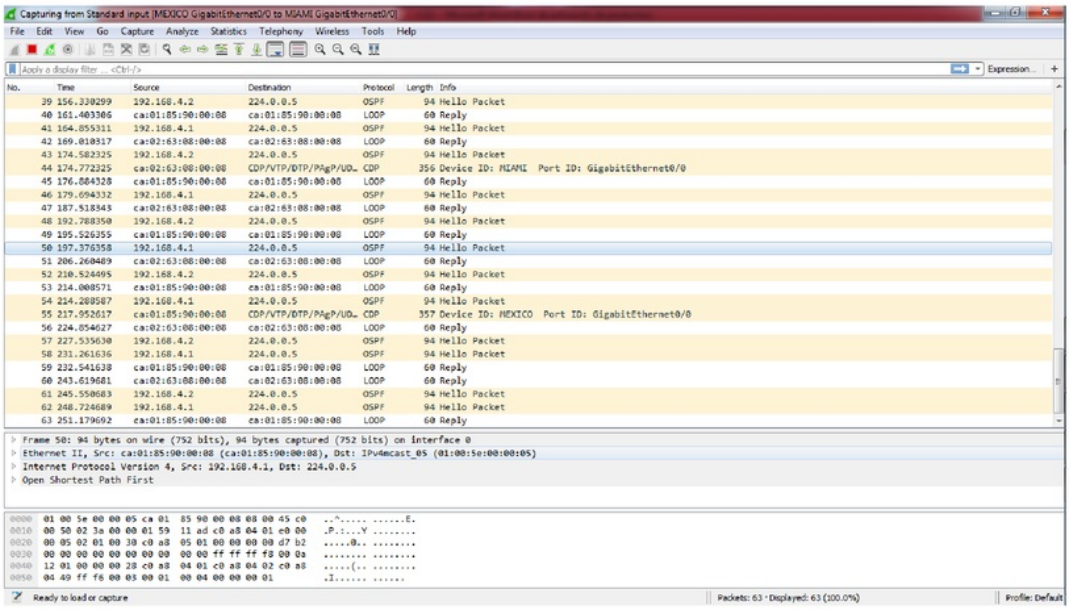


Figura 4.36. Paquetes OSPF entre el enlace de México y Miami.

Posteriormente se apaga intencionalmente la interfaz que conecta el router de Miami con el de México y luego se vuelve a encender para ver las actualizaciones de vecindades de OSPF, como se muestra en la figura 4.37.

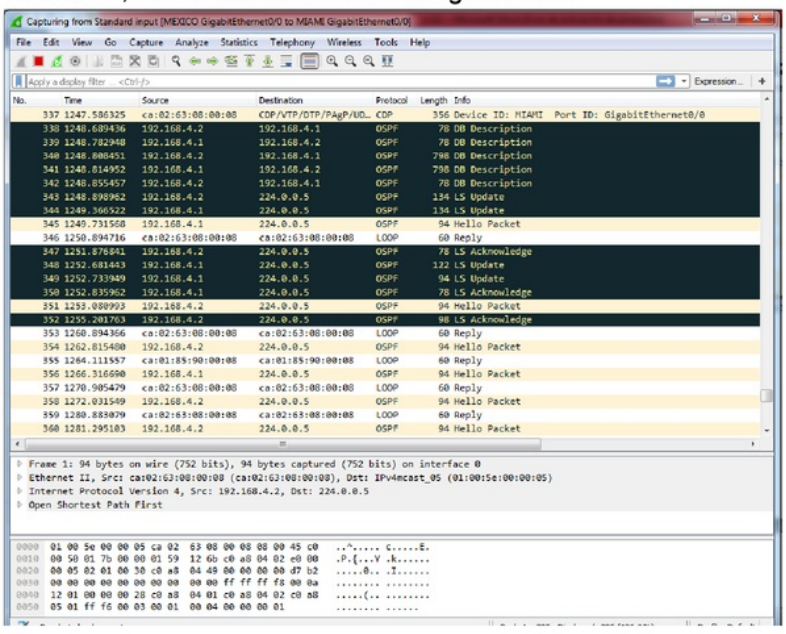


Figura 4.37. Traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.5

Después de encenderlo automáticamente el router de Miami manda un DB Description al router de México. En la figura 4.38 se muestra el paquete con el mensaje DB Description.

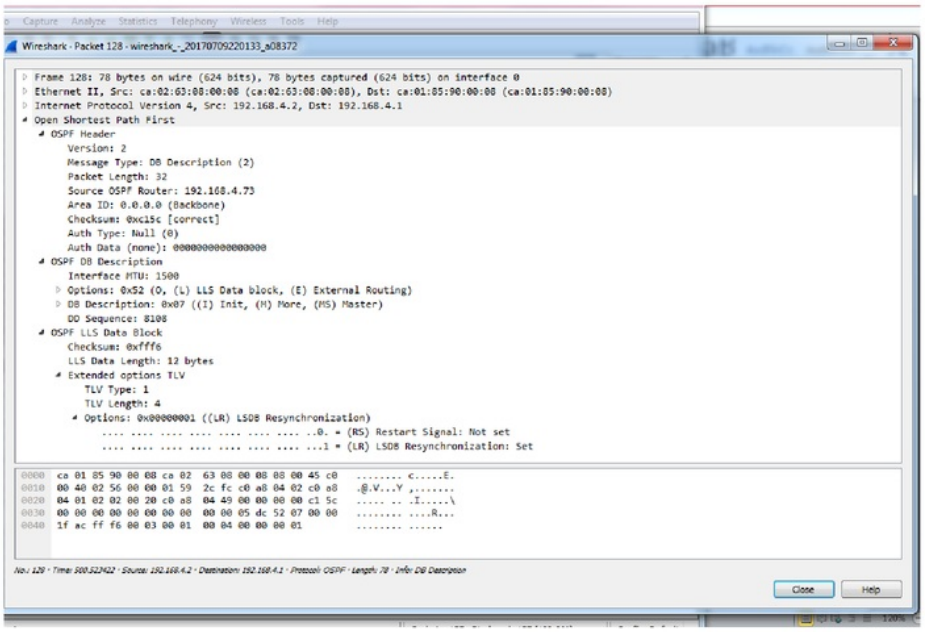


Figura 4.38. Paquete DB Description.

Posteriormente el router de Miami manda un mensaje LSU al router de México. En la figura 4.39 se muestra el paquete con el mensaje LSU.

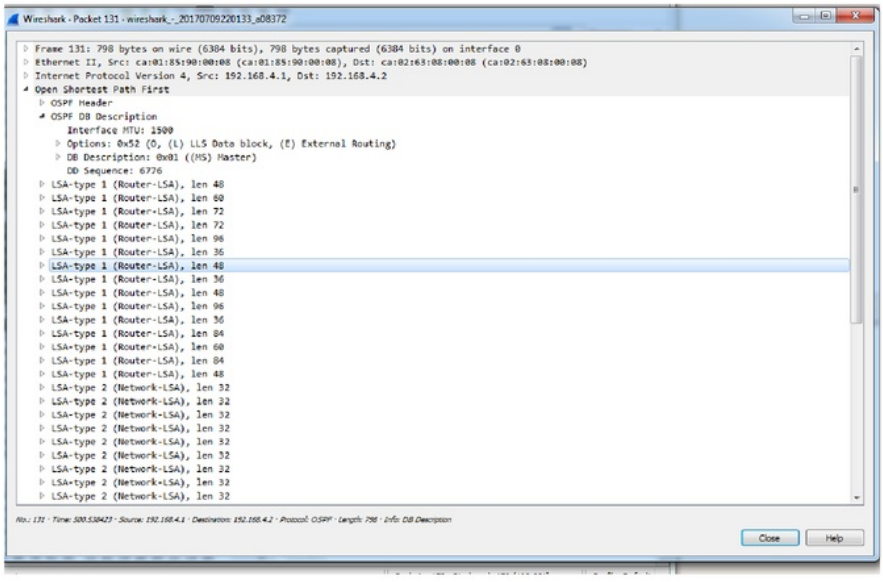


Figura 4.39. Paquete LSU.

Para finalizar el establecimiento de adyacencia el router de Miami envía un LSAck. En la figura 4.40 se muestra el paquete con el mensaje LSAck.

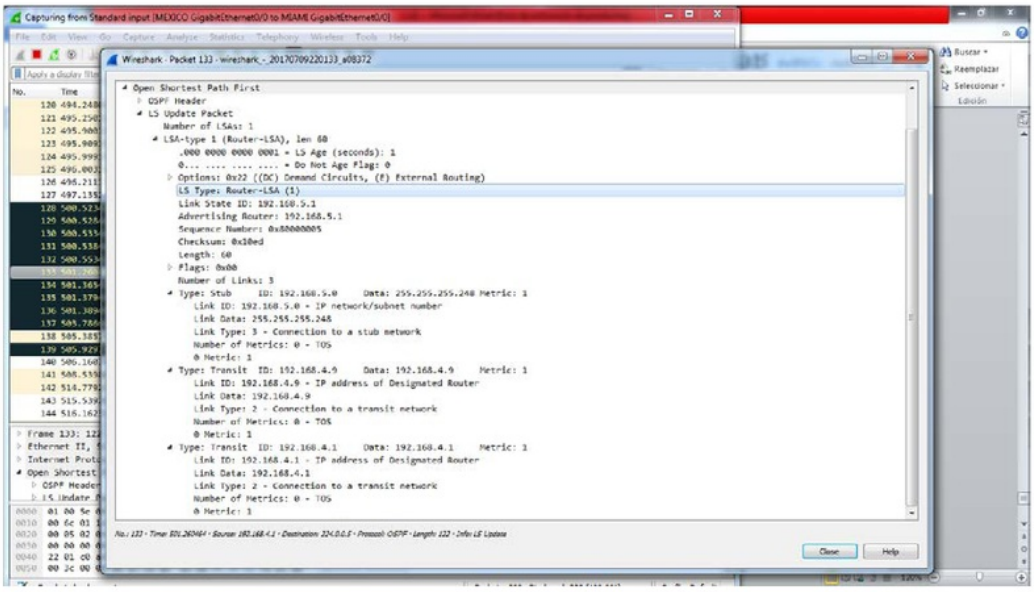


Figura 4.40. Paquete LSAck.

Por último, al hacer un ping entre los routers de México y UK se debe ver reflejado en el analizador de paquetes por lo que se ejecuta un ping desde la Pc de México hasta la PC de UK. La figura 4.41 muestra los paquetes del ping desde México hasta UK, así como la dirección IP desde donde se origina el ping y su dirección destino.

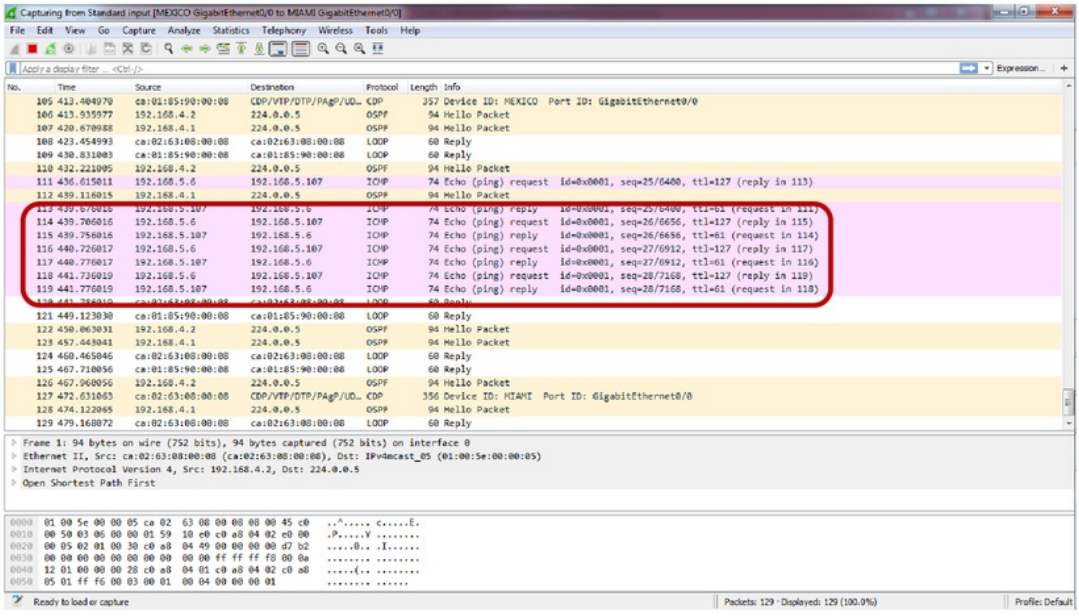


Figura 4.41. Ping desde México a UK.

Para las pruebas de conectividad el uso de recursos en GNS3 fue considerablemente mayor al de Packet Tracer tanto en uso de CPU como en memoria RAM. Esto porque es una aproximación más cercana a la realidad y considera más elementos que en Packet Tracer. Como se muestra en la fiugura 4.42.

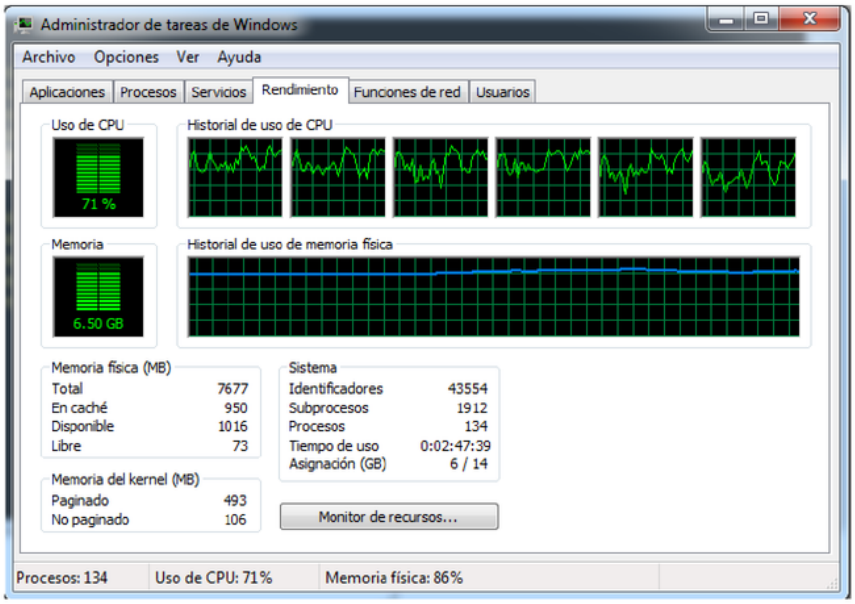


Figura 4.42. Uso de recursos de la emulación en GNS3.

Como se puede observar hay un uso total de CPU del 71 % el cual está divido en cada uno de los núcleos del procesador, por otro lado hay un uso de memoria RAM de 6.50 GB equivalente a un 86% del total con el que cuenta el equipo.

4.2.6 Configuración del protocolo de gestión SNMP

Una parte medular en la gestión de una red es el protocolo SNMP, el cual permite tener un control y conocimiento sobre ésta para poder detectar fallos o donde se requiera mantenimiento ya que permite establecer variables relacionadas con el estado y configuración de los hosts como routers, switches y equipos de usuarios. SNMP hace un sondeo a los agentes para obtener datos mediante los Trap SNMP, como se explicó en el capítulo 3. Para configurar SNMP se utiliza el router de México y Argentina.

4.2.6.1 Configuración de Administrador SNMP

Lo primero que se establece es el administrador de red (PC Mex-Windows7) y los agentes SNMP (Switch S3 y router de Argentina). Para establecer el administrador de red se utiliza el programa SNMP manager el cual se muestra en la imagen 4.43.

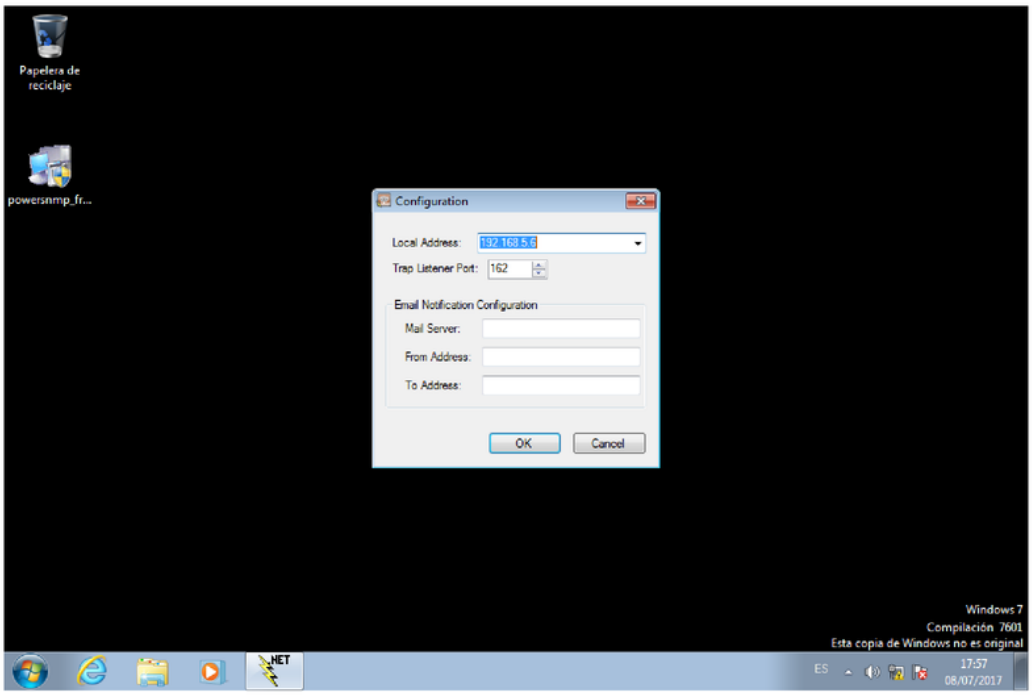


Figura 4.43. SNMP Manager ejecutado desde la máquina virtual Windows 7.

El programa SNMP Free Manager solicita establecer la dirección IP del administrador la cual en este caso es 192.168.5.6, esta dirección es por la que va a escuchar lo que pasa en la red. Con esta configuración el administrador contenido en la PC virtual puede enviar solicitudes a los agentes SNMP contenidos en otros dispositivos de la red.

4.2.6.2 Configuración del agente SNMP

A continuación se configura el agente SNMP el cual se encarga de enviar las Trap al administrador SNMP. Para configurar el agente se utilizan los comandos que se muestran en la figura 4.44.

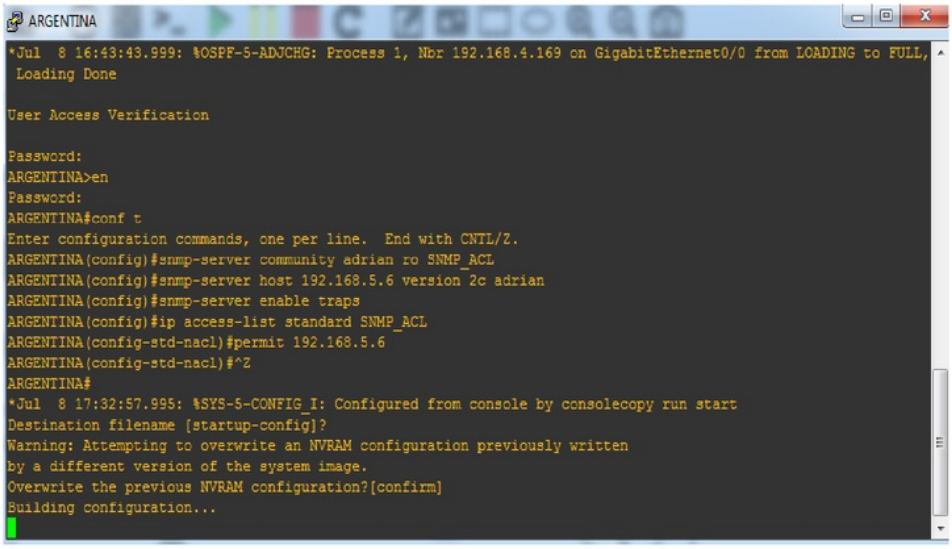


Figura 4.44. Configuración del agente SNMP en el router de Argentina

Debido a la configuración anterior, se puede observar que PowerSNMP Free Manager recibe notificaciones del router de Argentina. Lo anterior se muestra en la figura 4.45.

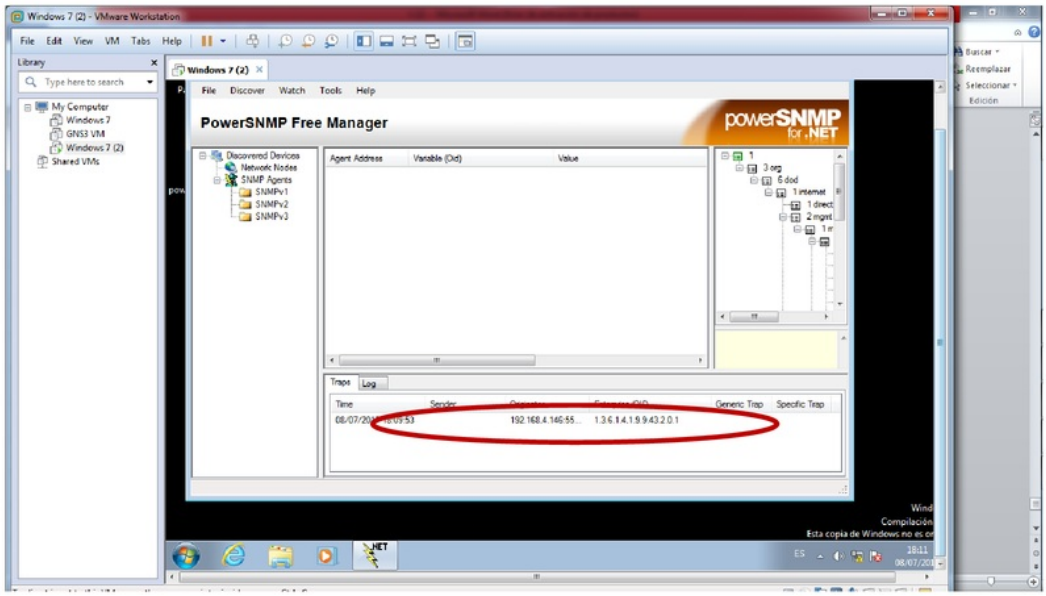


Figura 4.45. Detección de notificaciones desde el router de Argentina.

4.2.6.3 Detección de Agentes SNMP con PowerSNMP Free Manager

Para detectar los agentes SNMP que están configurados, Power SNMP Free Manager los muestra en una ventana llamada **Discover> SNMP Agents** con la dirección 192.168.5.255 y los parámetros establecidos de nombre de comunidad y versión SNMP, como se muestra en la figura 4.46.

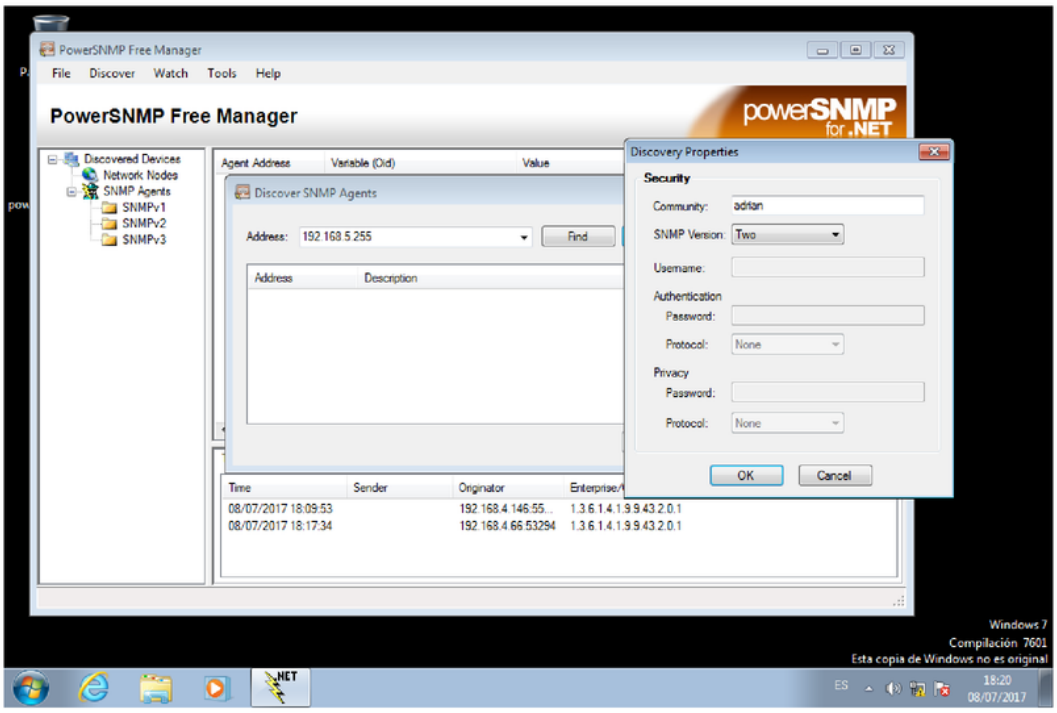


Figura 4.46. Encontrando Agentes SNMP en PowerSNMP Free Manager.

Posteriormente se encuentra el router de Argentina, como se observa en la figura 4.47, y lo establece como agente SNMP.

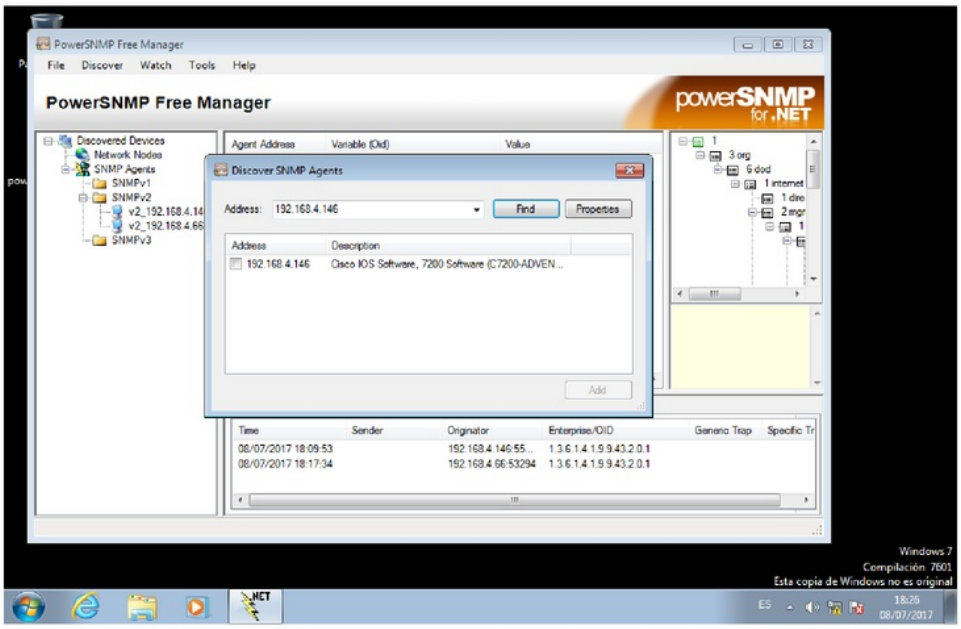


Figura 4.47. Agregación del agente SNMP router de Argentina

4.2.6.4 Trap SNMP analizadas con Wireshark

Al agregar el router de Miami se pueden observar 2 mensajes Trap de SNMP, los cuales se muestran en la figura 4.48, se tienen como origen la dirección IP 192.168.4.2, la cual corresponde al router ya mencionado, y como destino la dirección IP 192.168.5.6, la cual corresponde al administrador SNMP.

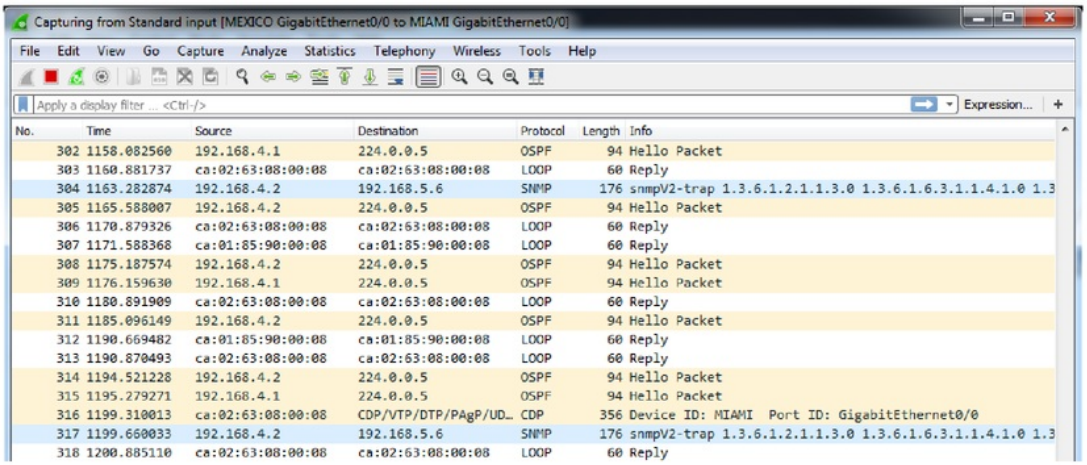


Figura 4.48. Mensajes SNMP con origen en el router de Miami.

Para saber que OID incluye, se selecciona con doble clic en el mensaje y se observan 5 árboles MIB los cuales se descifran con un traductor de OID. La figura 4.49 muestra los OID generados. Esta captura de paquete muestra la versión de

SNMP que se está utilizando, el nombre de comunidad y 5 OID que se traducen posteriormente.

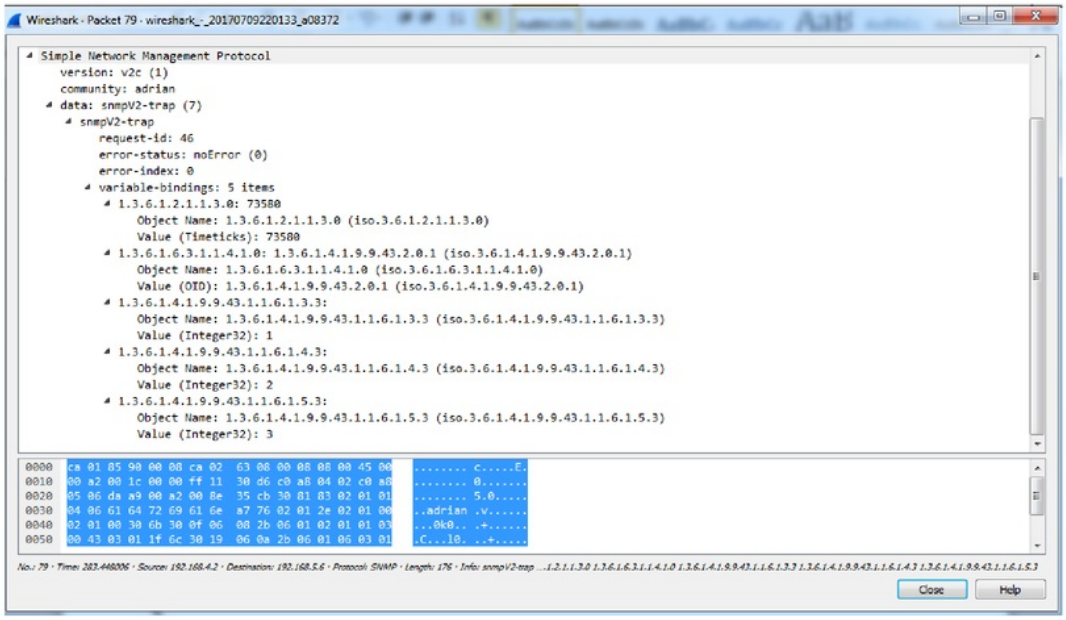


Figura 4.49. OID's generados en el router de Miami.

4.2.6.5 Traducción de los OID

Para traducir los OID se utiliza una página web de Cisco la cual cuenta con una base de datos que contiene los diferentes tipos de OID. En la figura 4.50 se muestra la página que se utiliza.

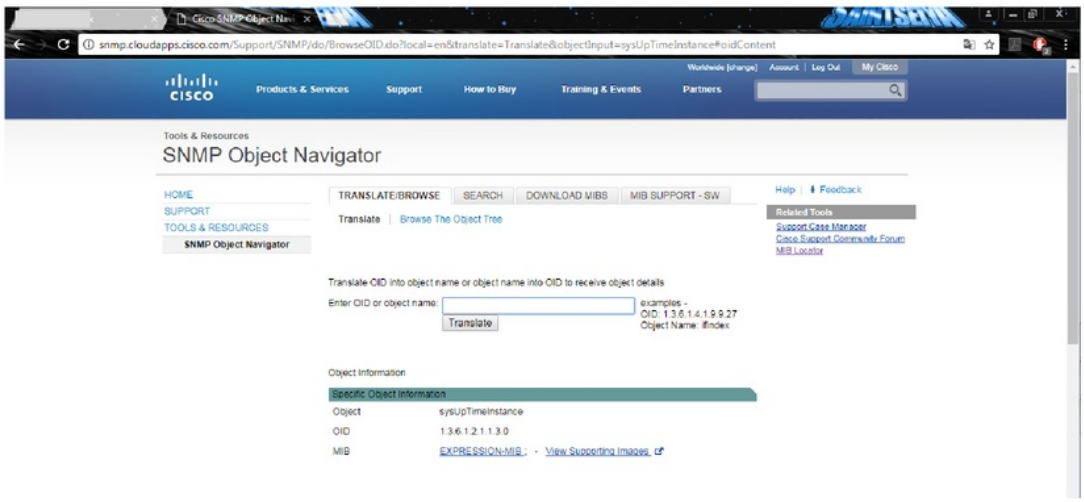


Figura 4.50. Página web de Cisco SNMP Object Navigator.

En la figura 4.51 se muestra la traducción para el OID 1.3.6.1.4.1.9.9.43.2.0.1 el cual es una notificación de que ha ocurrido una reciente configuración en dicho dispositivo.

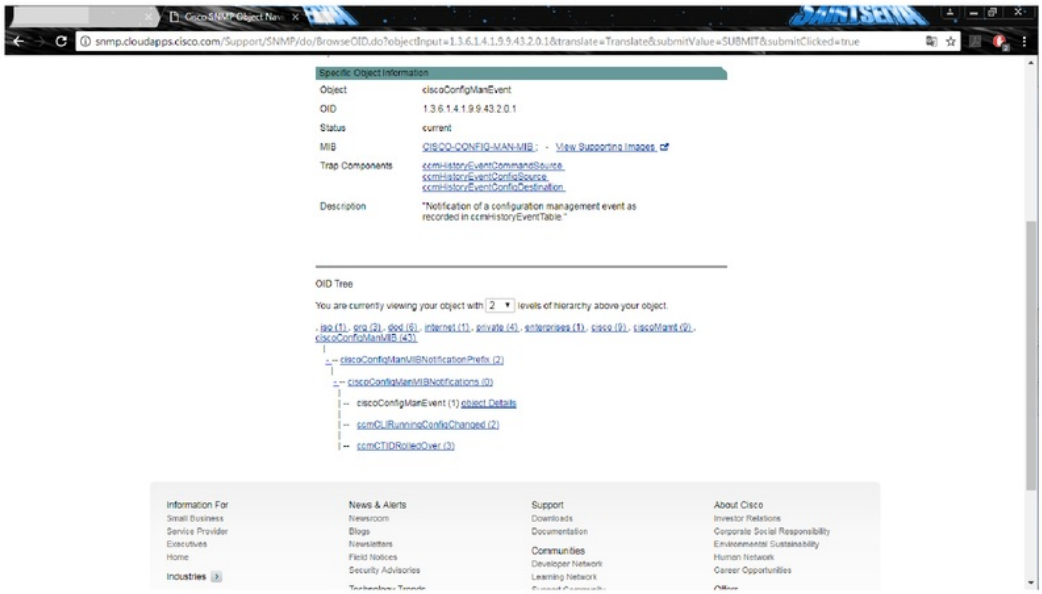


Figura 4.51. Traducción para el OID 1.3.6.1.4.1.9.9.43.2.0.1.

En la figura 4.52 se muestra la traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.3 la cual indica la fuente del comando que incitó el evento.

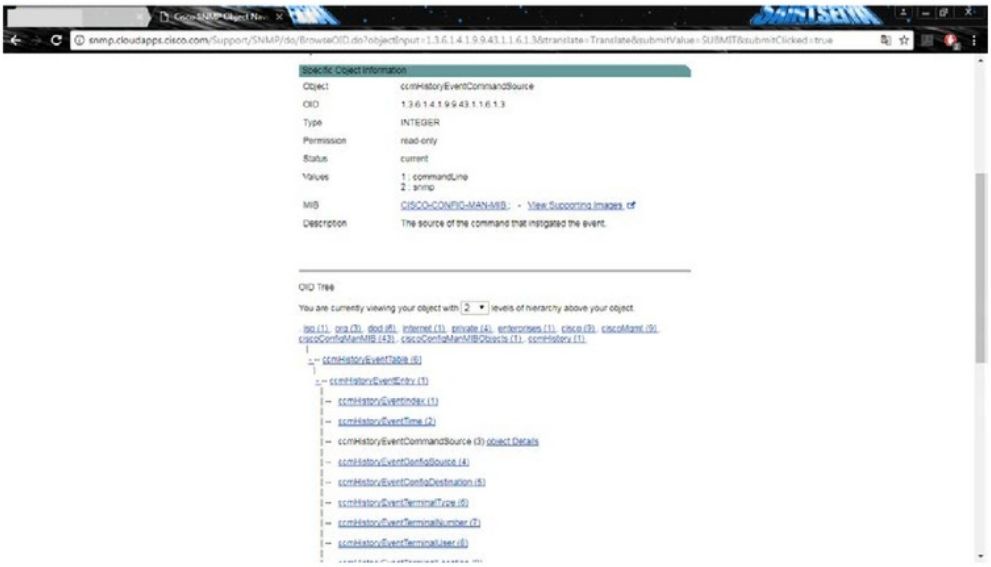


Figura 4.52. Traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.3.

En la figura 4.53 se muestra la traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.4, la cual indica la configuración de origen del dispositivo.

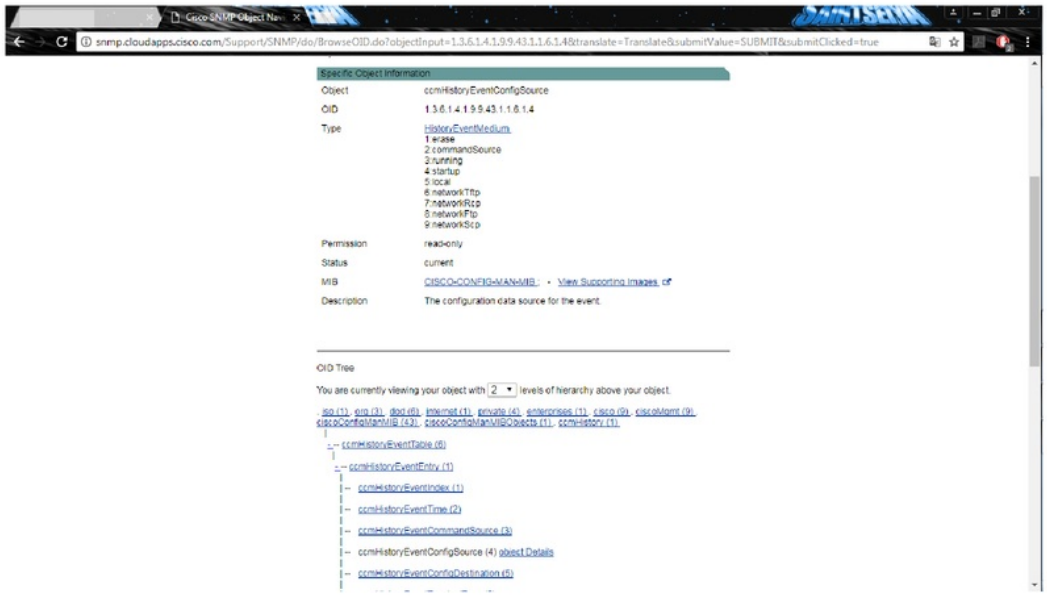


Figura 4.53. Traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.4.

En la figura 4.54 se muestra la traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.4, la cual indica la configuración de destino del dispositivo.

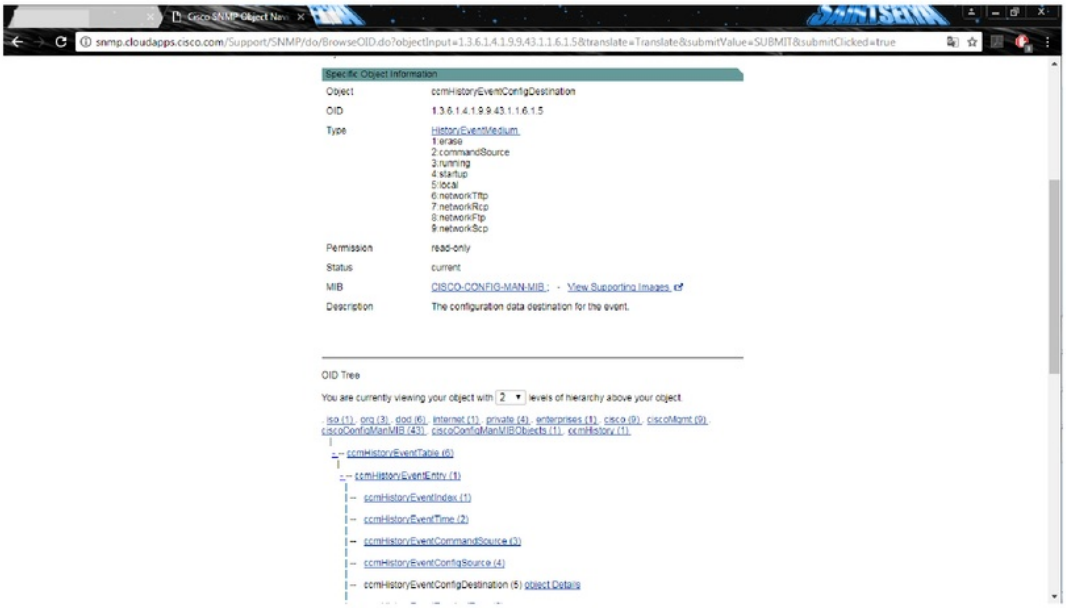


Figura 4.54. Traducción para el OID 1.3.6.1.4.1.9.9.43.1.1.6.1.4.

El administrador SNMP manda una solicitud get-request a los routers que tiene configurados como agentes y posteriormente éstos le responden con un get-response. En este caso manda un get-request al router de Argentina y éste le responde con un get-response. En la figura 4.55 se muestra cuándo el analizador de paquetes identifica los mensajes get-request y get-response.

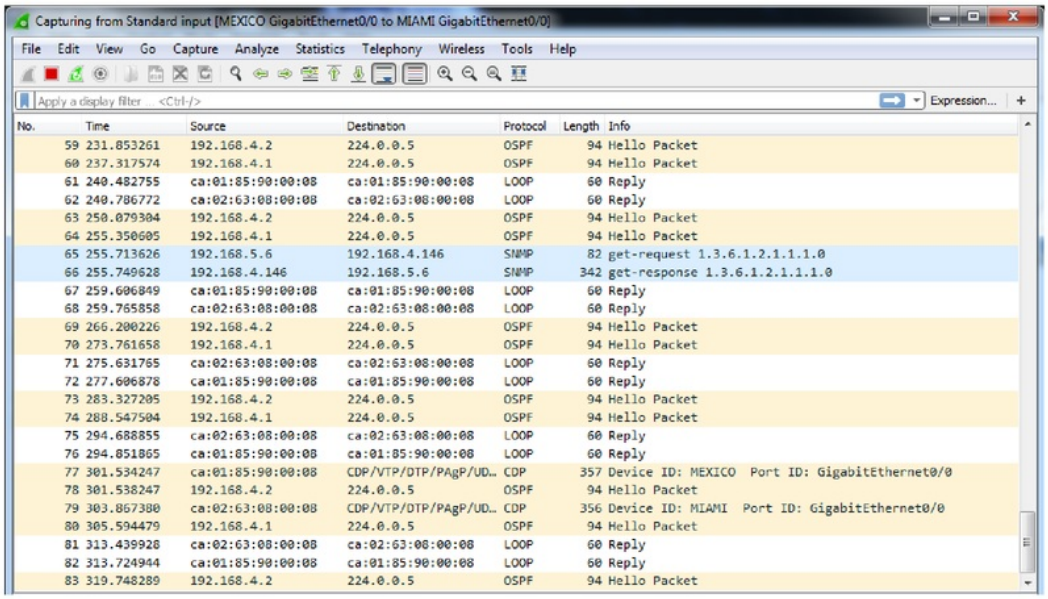


Figura 4.55. Mensajes *get-request y get-response* capturados por Wireshark.

El mensaje *get-request* con OID 1.3.6.1.2.1.1.1.0 cuyo significado es una descripción del router, incluye el nombre del router, la versión del mismo y el software del router. La figura 4.56 muestra el OID mencionado.

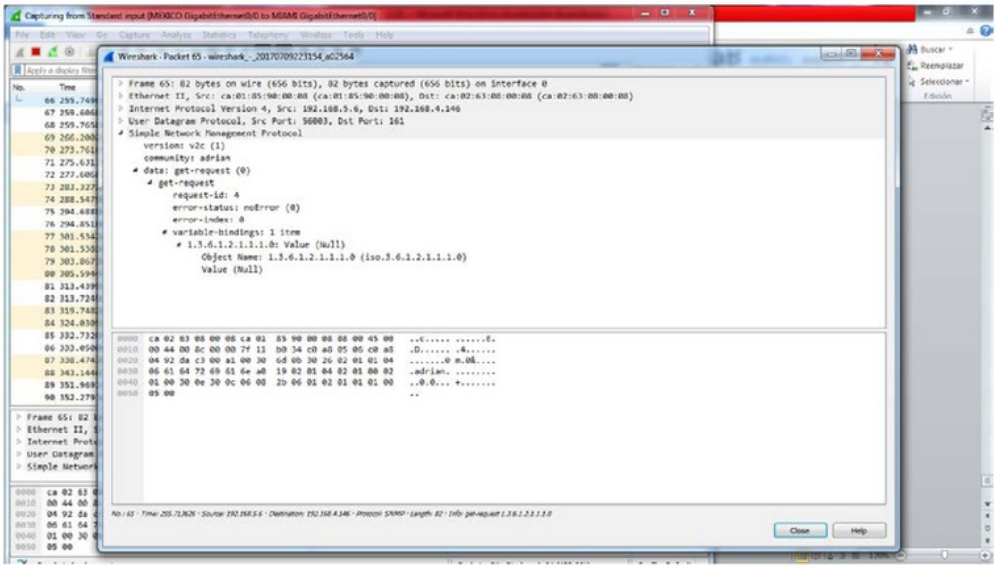


Figura 4.56. Paquete *get-request* desde el administrador SNMP en la PC de México hasta el router de Argentina.

El mensaje *get-response* contiene el mismo OID, esto significa que el administrador SNMP (PC Mexico) requirió el nombre del router de Argentina y éste le respondió proporcionándole el modelo del router, la versión y el sistema operativo que usa. En la figura 4.57 se muestra el paquete *get-response*.

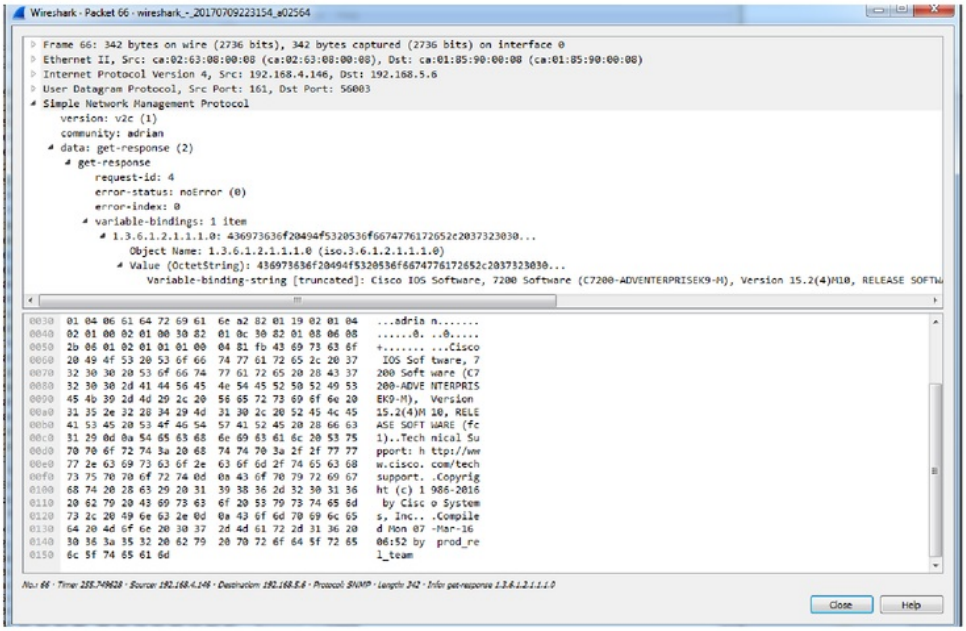


Figura 4.57. Paquete get-response desde el router de Argentina hacia el Administrador SNMP de la PC de México.

4.2.6.6 Pruebas SNMP en GNS3

Para probar SNMP se configura el router de Miami, se enciende una nueva interfaz y le asigna una dirección IP, de igual forma se configura el protocolo OSPF y se observa qué Trap arroja al Administrador SNMP. En la figura 4.58 se muestra la configuración realizada al router de Miami.

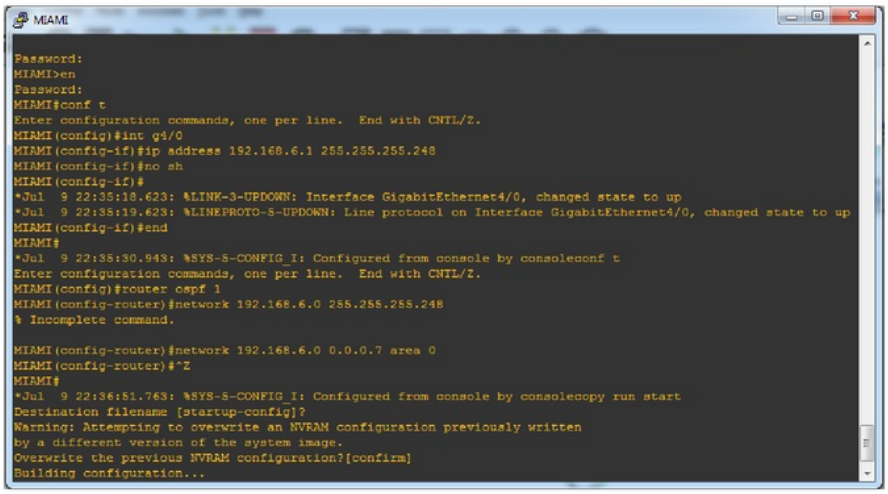


Figura 4.58. Configuración al router de Miami para observar la respuesta del protocolo SNMP.

Como se puede observar en la figura 4.59 se generó un Trap SNMP con origen en el router de Miami y destino en el administrador SNMP (PC de México).

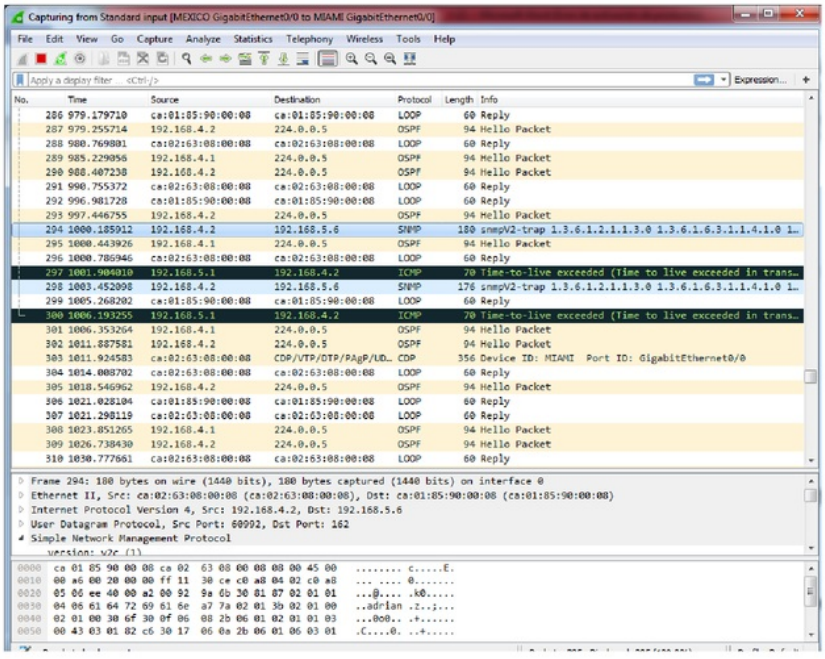


Figura 4.59. Generación de Trap al agregar una configuración del router de Miami.

Al abrir el paquete se muestra una serie de OID como en la figura 4.60.

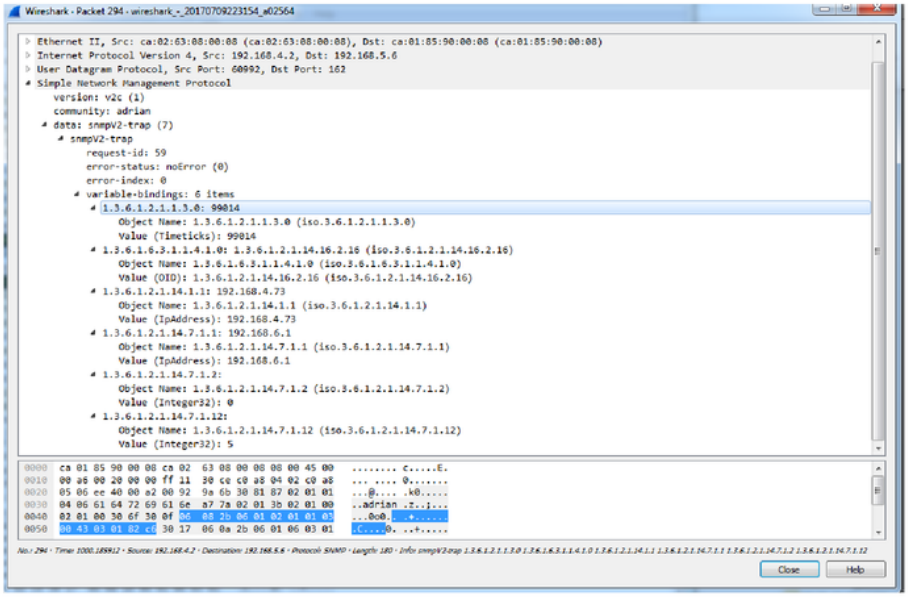


Figura 4.60. OID generados al configurar de nuevo el router de Miami.

Los OID se explican a continuación:

1.- El OID con valor 1.3.6.1.2.1.1.3.0 se refiere a una autenticación que le pone el vendor al dispositivo para distinguirlo de los demás.

2. El OID con valor 1.3.6.1.2.1.14.16.2.16 es un *Trap* de tipo ospfIfStateChange la cual significa que ha surgido un cambio en el estado de una interfaz OSPF. Esta *Trap* se generó porque se configuró el protocolo OSPF en el router de Miami, es por eso que SNMP enseguida lo detectó y se lo envió al administrador OSPF.

3. El OID 1.3.6.1.2.1.14.1.1 se refiere a la dirección IP del router donde se ha configurado OSPF, esta dirección es solo para identificar el router de Miami, en el cual se hizo la configuración.

4. El OID 1.3.6.1.2.1.14.7.1.1 se refiere a la dirección IP que se añadió en el router de Miami y a la cual posteriormente se le configuró OSPF.

5. El OID 1.3.6.1.2.1.14.7.1.2. Se refiere a que dicha dirección IP se ha añadido a la tabla de OSPF.

6. El OID 1.3.6.1.2.1.14.7.1.12. Se refiere a que el estado OSPF ha cambiado de down a up, debido a que se estableció una adyacencia mediante la configuración reciente al router de Miami.

En la ventana de Traps del administrador SNMP se muestran las Trap que van apareciendo conforme surgen los cambios en la red. La figura 4.61 ejemplifica lo anterior.

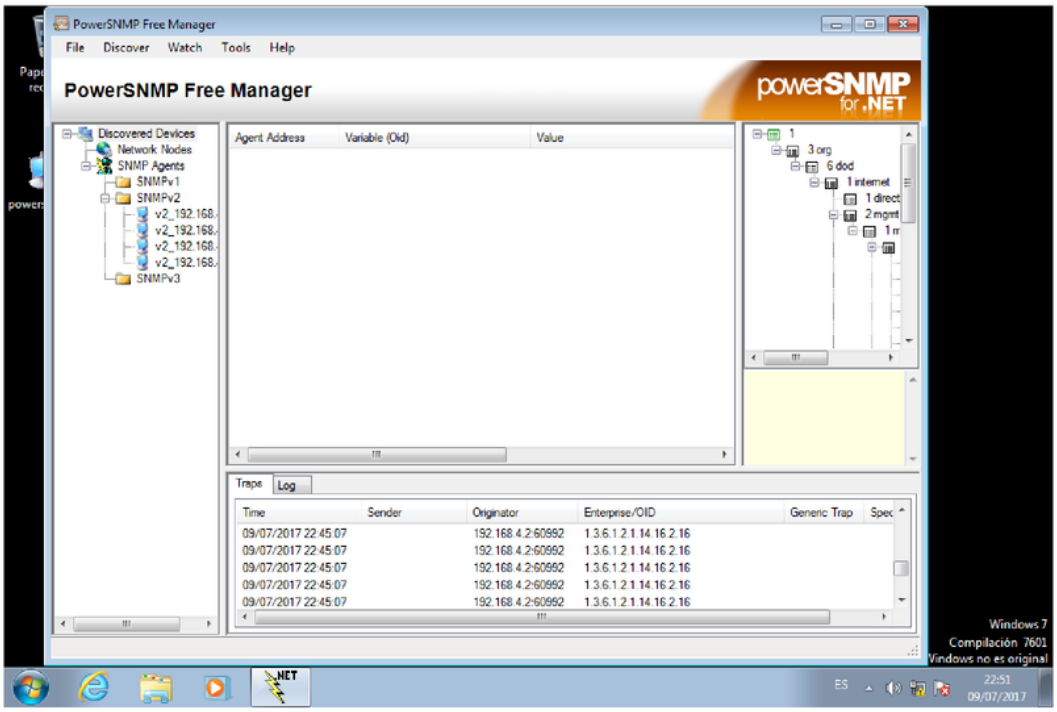


Figura 4.61. Ventana de Traps del Administrador SNMP en la máquina virtual.

Por último se puede ver que al hacer uso de OSPF el consumo aumenta principalmente en la memoria RAM, cabe mencionar que la emulación toma más porcentaje en memoria RAM que en CPU, esto porque el equipo con el que se realizó la emulación tiene un procesador con 6 núcleos que divide las operaciones en cada uno de sus núcleos, mientras que la memoria RAM está contenida en dos slots de 4 GB. En la figura 4.62 se muestra el uso de CPU y de RAM.

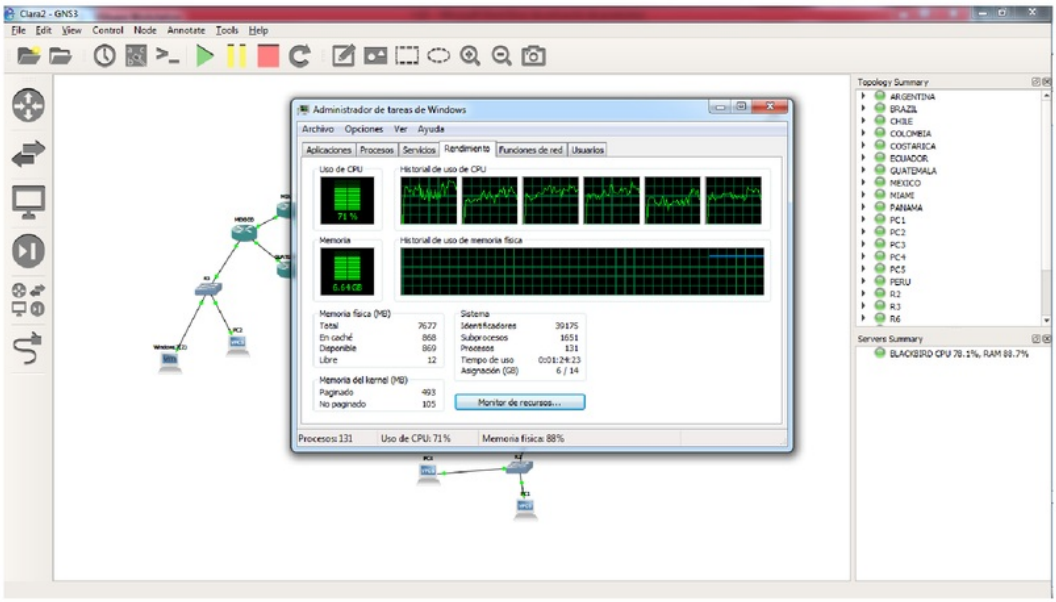


Figura 4.62. Uso final de CPU y memoria RAM.

Capítulo 5 Conclusiones

A lo largo del presente documento se ha podido observar que una red avanzada es y será una importante herramienta para la investigación y educación en sus diferentes campos, es por ello que la red avanzada requiere de un funcionamiento óptimo, confiable en cuanto a conectividad y seguro. Evidentemente, una emulación dista de la realidad por lo que deberíamos de tomar factores en cuenta como costos de equipos, costos de mantenimiento, además de contar con un personal de trabajo especializado.

De esta forma rescatando algunos puntos finales a manera de conclusiones se tiene:

1. La red avanzada CLARA es un logro para toda América Latina, sin embargo, queda mucho por hacer ya que hasta 2017 no todos los países estaban integrados a la misma por lo que, para que todos tengan acceso, debe de haber una disposición e inversión en el ámbito educativo. Por el momento, se puede decir que la red CLARA cumple con sus objetivos iniciales y con el tiempo puede mejorar en aspectos de colaboración, entre más países agregados más universidades interconectadas.

2. OSPF es un protocolo que permite comunicar routers que pertenecen a diferentes áreas debido a que tiene muchas características que contemplan diferentes escenarios entre áreas. Con esto se puede intercambiar información entre un área específica con un área de backbone o bien con un área de otro dominio administrativo (una red externa mediante el ASBR). Por otra parte OSPF, es ideal para este tipo de redes en donde se tiene un dominio para backbone y diferentes dominios para las redes que se conectarán en un futuro.

3. Con base a las características vistas de Packet Tracer y GNS3 se puede concluir que GNS3 tiene un entorno más real lo que permite tener una mejor aproximación de red comparado con Packet Tracer, es por ello que se concluye que GNS3 es más completo que Packet Tracer y sirve para emular redes más complejas con un mejor resultado con respecto a Packet Tracer, de acuerdo a lo siguiente:

   3.1. Wireshark es una herramienta muy útil para el análisis y rastreo de paquetes, esta herramienta que permite ver los paquetes en tiempo real en cualquier enlace de la red; paquetes de conectividad, de enrutamiento y de gestión particularmente SNMP con OID's incluidas fueron los paquetes que predominaron en cada enlace. Dicha herramienta solo funciona en la emulación en GNS3 ya que en Packet Tracer no está disponible.

3.2. Con base en la gestión SNMP cumplió con la función de informar los acontecimientos que pasaban en los routers de la red en tiempo y forma, esto tanto en Packet Tracer como en GNS3. Por otra parte, al hacer algún cambio en un router, por ejemplo configurar una nueva dirección IP, configurar OSPF o desactivar un enlace de la red éste se reflejaba de manera automática tanto en el analizador de paquetes Wireshark como en el Administrador SNMP para el cual tuve que configurar una máquina virtual y cargarle el Administrador SNMP, todo lo anterior sólo es posible en GNS3.

3.3. En lo referente al consumo de recursos tenemos que para la simulación en Packet Tracer se utilizó un total del 6 % de uso de CPU el cual está dividido en cada uno de los 6 núcleos del procesador y un uso de memoria RAM del 36 %. Análogamente en GNS3 tenemos que se utilizó un total del 71 % de uso de CPU el cual está dividido en cada uno de los 6 núcleos del procesador y un uso de memoria RAM del 86 %. La emulación consume mayores recursos de procesador, de igual forma para el caso de la memoria RAM. Por lo que es evidente que en GNS3 tenemos una mejor aproximación de la red y por ende una emulación más cercana a la realidad.

3.4. Referente a los tiempos de respuesta en conectividad, en el proceso del ping desde los nodos de México a Brasil y desde Brasil a UK fueron mayores en la emulación ya que tenemos aproximadamente 80 ms para GNS3 y 1 ms para Packet Tracer, por otra parte, en la gestión eran inmediatos en ambos. Por lo que es evidente que un proceso del comando ping en GNS3 es mas cercano a la realidad y por consecuencia mas exacto y confiable que en la simulación en Packet Tracer.

3.5. Relativo al arranque del entorno, es decir de la red para que estuviera lista y funcionando en la simulación y emulación se tiene que en Packet Tracer el tiempo de espera es alrededor de dos minutos para que carguen todos los componentes incluyendo las adyacencias en OSPF. Sin embargo, para GNS3 tenemos un tiempo de 15 a 20 minutos incluyendo la iniciación de los routers y de la máquina virtual. Lo cual indica que es un valor mas cercano a la realidad y por ende debería ser mas utilizado por administradores de redes o incluso estudiantes avanzados de redes para planeracion, diseño o resolución de problemas.

4. Se puede afirmar que se cumplió con el objetivo inicial de la presente tesis ya que se consiguió establecer implementar mediante una conectividad totalmente funcional del backbone de la red CLARA, así mismo se consiguió implementar la gestión mediante SNMP para la red CLARA, la cual funcionó satisfactoriamente en tiempo real.

Referencias

[1] J.C.R Licklider “Man-Computer Symbiosis”, IRE transaction on human factors in Electronics, Vol HFE-1 No1, March 1960. Pp 4- 11.

[2] L. Kleinrock MIT “information flow in large communications nets” PhD thesis. Elec Eng Dept, May 1961.Cambridge EUA pp 9-11.

[3] David D. Clark “Brief History of the Internet” Internet Society , Oct 2012, pp 3-10.

[4] Lyon, Matthew; Hafner, Katie . “ Where Wizards Stay Up Late: The Origins Of The Internet” Simon & Schuster. Kindle Edition . 1993, pp 43-52.

[5] DARPA, BBN.“A history of the ARPANET: The First Decade ” APril 1981. Virginia, EUA pp I-2 - II-6

[6] Richards, Mark 1965. “Interface Message Processor”. Consultado Septiembre 2016. Disponible en: http://www.computerhistory.org/revolution/networking/19/407/2086

[7] UCLA, “Birthplace of the Internet, 1969”, IEEE Milestones, IEEE History Center, IEEE, 2009. Virginia EUA. Consultado Septiembre 2016. Disponible en http://ethw.org/Milestones:Birthplace_of_the_Internet,_1969

[8] SRI “Inception of the ARPANET, 1969” IEEE Milestones, IEEE History Center, IEEE, 2009 Consultado Septiembre 2016 Disponible en http://ethw.org/Milestones:Inception_of_the_ARPANET,_1969

[9] National Science Foundation, “NSF and the birth of Internet”, (en línea); EUA, Consultado Octubre 2016. Disponible: https://www.nsf.gov/news/special_reports/nsf-net/home.jsp

[10] V.G. Cerf and R.E. Khan “A protocol for packet network interconnection” IEEE transactions on communication vol.22, issue 5, 1974, pp 637-648

[11] Jose Ignacio Castillo Velazquez, “Redes de datos contexto y evolucion”, 2da edición, Mexico 2016, ed SAMSARA. ISBN: 978-970-94-2915-2.

[12] Institute of Engineering Task Force, RFC 823, “The DARPA Internet Gateway” Sep 1982.

[13] Peter J. Denning, Anthony Hearn, C. William Kern, “History and overview of CSNET” 1983

[14] Institute of Engeneering Task Force, RFC 823,“ NCP/TCP TRANSITION PLAN” Sep 1982.

[15] Tim Berners-Lee, "WWW: Past, Present, and Future", IEEE, Computer Magazine, Vol. 29, No. 10, Oct. 1996. Consultado Octubre 2016. Disponible en: https://www.w3.org/People/Berners-Lee/1996/ppf.html .

[16] IEEE ComSoc, "A brief history of communications", 2002. ISBN: 0-7803-9825-4.

[17] Barry M. Leiner, Vinton G. Cerf, David D. Clark, etal, "Brief History of the Internet" Internet Society , Oct 2012, pp 14.

[18] Red CLARA, Red y Conectividad, (en línea). Consultado octubre 2016. Disponible en: http://www.redclara.net/index.php/red-y-conectividad/redes-avanzadas-en-el-mundo/14-faq-s/3121-para-que-sirve-la-conexion-a-redclara

[19] Miller Gerry, CANARIE "A birthday for Canada's Internet" noviembre 2015 (en línea). Consultado octubre de 2016. Disponible en: https://www.canarie.ca/a-birthday-for-canadas-internet/

[20] Gerry Miller, Gerri Sinclair, David Sutherland, "Regulation of the Internet: A technological perspective". March 1999, pp 17-19

[21] Andy Bjerring, John Demco, Paul Gilmore, etal, CaNet Institute, "A nation goes online". Canadá 2001, pp 110-11

[22] Leslie Regan Shade, "Computer Networking in Canada: From CA*net to CANARIE", (en linea), Canadian Journal of Communications, Vol 19, No 1 (1994). Consultado Octubre 2016. Disponible en: http://www.cjc-online.ca/index.php/journal/article/view/794/700

[23] CANARIE, Conections, "Full speed ahead for the new mandate", (en linea) Sept 2012. Consultado Octubre 2016. Disponible en: https://www.canarie.ca/wp-content/newsletters/Connection_2012_sept_en.html

[24] Internet2, Internet2 Community Timeline, [en línea]; Washington, D.C, EEUU. Consultado: Octubre 2016. Disponible en: http://www.internet2.edu/about-us/internet2-community-timeline/

[25] Nathan Penner, Overview of Internet2, (en linea); EUA, Consultado Octubre 2016, Disponible en: http://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/internet-2/overview.html

[26] Ann O'Beay, Internet2, Advanced Networking, (en linea) Washington D.C, EUA, October 1998. Consultado Octubre 2016. Disponible en: http://www.internet2.edu/presentations/981027-BT-Ann/sld001.htm

[27] Internet2, Advanced Networking. (en linea); Washington, D.C, EUA. Consultado Octubre 2016. Disponible en: http://www.internet2.edu/products-services/advanced-networking/

[28] Internet2, Internet2 Network Topology Infraestructure Topology, (en linea); Washington D.C, EUA, 2013. Consultado Octubre 2016. Disponible en: http://www.internet2.edu/media/medialibrary/2013/07/31/Internet2-Network-Infrastructure-Topology.pdf

[29] Red CLARA y su historia , (en linea); Consultado Octubre 2016. Disponible en: https://www.redclara.net/index.php/somos/sobre-redclara/historia

[30] Alice, About CLARA, (en linea); Consultado Octubre 2016. Disponible en: http://alice1.archive.dante.net/server/show/nav.871.html

[31] María José López Pourailly, "CLARA opens its direct transit to the North American Advanced Networks", DeClara, Year 1 - Nº 1, April 2005, pp 9-10.

[32] Red CLARA, Memoria 2006, pp 20-23, Abril 2007.

[33] María Paz Mirosevic, "CLARA publishes information about the NOC", DeClara, July, 2007, Year 3 - Nº 13 pp 9.

[34] Red CLARA, Memoria 2007, pp 10-11, Abril 2008.

[35] Red CLARA, Memoria 2008, pp 20, Abril 2009.

[36] Red CLARA, Memoria 2009, pp 13-16, Abril 2010.

[37] Red CLARA, Memoria 2011, pp 21, Abril 2012

[38] Red CLARA, Memoria 2012, pp 19, Abril 2013

[39] Red CLARA, Memoria 2014, pp 25, Abril 2015

[40] Red CLARA, Memoria 2015, pp 25, Abril 2016

[41] RedClara, Topología Red CLARA, (En linea) 2017. Consultado marzo 2017. Disponible en: http://dspace.redclara.net/bitstream/10786/1255/1/topology_RedCLARA_basecafe-16.pdf

[42] Red CLARA, Especificaciones técnicas, (En línea) 2014. Consultado octubre 2016. Disponible en: https://www.redclara.net/index.php/red-y-conectividad/descripcion-tecnica

[43] Allan Johnson “Routing Protocols and Concepts CCNA Exploration Labs and Study Guide” Cisco Press 800 East 96th Street Indianapolis, IN 46240 EUA, 2009 ISBN-13: 978-1-58705-575-1

[44] James F. Kurose, Keith W. Ross “Computer Networking: A Top-Down approach” Sixth Edition, Pearson Education, 2013. ISBN-13: 978-0-13-285620-1, pp 2.

[45] Mohd Nayeem Shah, “Implementation of Graph Theory in Computer Networking to Find an Efficient Routing Algorithm” IJIRCCE. Vol. 4, Issue 1, January 2016, pp 12-13.

[46] Jose Ignacio Castillo, Noé Galicia. “Routing Algorithms Applied to an Advanced Academic Network Known as CUDI”. IEEE Latin America Transactions, June 2016, Volume 14 Issue 6.

[47] Eduardo Collado Cabeza, “Fundamentos de Routing”. Mayo 2009. España.

[48] Todd Lammle, CCNA Cisco Certified Study Guide, San Francisco EUA, 2000, 2da Edition, ed. SYBEX Inc. ISBN: 0-7821-2647-2.

[49] C. Hedrick, “A Routing Information Protocol”. RFC 1058. NWG, Rutgers University. June 1988.

[50] Cisco CCNA Exploration v4.0. “Conceptos y protocolos de enrutamiento” Módulo 2.

[51] G. Malkin. “RIP Version 2”. RFC 2453. NWG. Bay Networks. November 1998.

[52] G. Malkin. “RIP Version 2 Carrying Aditional Information”. RFC 1723. NWG. Xylogics Inc. November 1994.

[53] J. Moy “The OSPF Specification” RFC 1131. Proteon Inc. October 1989.

[54] J. Moy. “OSPF Version 2” RFC 1247. Proteon Inc. July 1991.

[55] J. Moy “OSPF Version 2” RFC 2328. Ascend Communications, Inc. April 1998.

[56] Cisco CCNP Route implementing IP Routing. Chapter 3. “Configuring the Open Shorthest Path First Protocol” 2007 – 2010.

[57] IEFT “Vulnerabilities of network control protocols: An example” RFC 789 1981.

[58] Davin, J., J. Case, M. Fedor, and M. Schoffstall, "A Simple Gateway Monitoring Protocol", RFC 1028. November 1987.

[59]. Case J. Fedor M, Schoffstall M. Davin J. “A simple network management Protocol (SNMP)”. RFC 1157. Mayo 1990.

[60] Castillo Velázquez, J. I. El árbol de internet y la estructura de la información de gestión de una red. IEEE Latin America and the Caribbean Newsletter No. 62, 2009. Consultado septiembre 2016. Disponible en: http://ewh.ieee.org/sb/mexico/uacm/jicv/2009_arbolinternet_n62_pp1517.pdf.

[61] J. Case, K. McCloghrie, M. Rose, "Introduction to Community-based SNMPv2" RFC 1901, 1996.

[62] J. Case, K. McCloghrie, M. Rose," Introduction to version 2 of the Internet-standard Network Management Framework" RFC 1441, 1997.

[63] J. Case,R. Mundy, D. Partain, "Introduction and Applicability Statements for Internet Standard Management Framework", RFC 3410, Diciembre 2002.

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

[65] U. Blumenthal, F. Maino, K. McCloghrie " The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826 Junio 2004.

[66] CCNA 3, Modulo 5. "OSPF en redes de accesos múltiples". (Consultado Abril 2017). Disponible en: http://ecovi.uagro.mx/ccna3/course/module5/5.1.2.8/5.1.2.8.html

Monitoreo en la red avanzada CLARA : Emulación

INFORME DE ORIGINALIDAD

13%	12%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.scribd.com Fuente de Internet	2%
2	dspace.redclara.net Fuente de Internet	1%
3	docplayer.es Fuente de Internet	1%
4	repositorio.utp.edu.co Fuente de Internet	1%
5	www.redclara.net Fuente de Internet	1%
6	redclara.net Fuente de Internet	1%
7	dspace.uah.es Fuente de Internet	<1%
8	eduangi.com Fuente de Internet	<1%
9	Submitted to University of Wales central	<1%

	institutions Trabajo del estudiante	
10	fr.scribd.com Fuente de Internet	<1%
11	neutron.ing.ucv.ve Fuente de Internet	<1%
12	www.ccapitalia.net Fuente de Internet	<1%
13	www.slideshare.net Fuente de Internet	<1%
14	repositorio.cepal.org Fuente de Internet	<1%
15	addi.ehu.es Fuente de Internet	<1%
16	renataustaadmon.blogspot.com Fuente de Internet	<1%
17	Submitted to Universidad Internacional Isabel I de Castilla Trabajo del estudiante	<1%
18	virtual.cudi.edu.mx Fuente de Internet	<1%
19	mailweb.udlap.mx Fuente de Internet	<1%
20	web.madritel.es	

	Fuente de Internet	<1%
21	id.scribd.com Fuente de Internet	<1%
22	bibdigital.epn.edu.ec Fuente de Internet	<1%
23	www.mlconsultora.com.ar Fuente de Internet	<1%
24	Submitted to UNAPEC Trabajo del estudiante	<1%
25	kaslab.net Fuente de Internet	<1%
26	www.cicei.ulpgc.es Fuente de Internet	<1%
27	es.wikipedia.org Fuente de Internet	<1%
28	Submitted to UNIV DE LAS AMERICAS Trabajo del estudiante	<1%
29	documents.mx Fuente de Internet	<1%
30	future-internet.eu Fuente de Internet	<1%
31	es.slideshare.net Fuente de Internet	<1%

32	ants.dif.um.es Fuente de Internet	<1%
33	www.buenastareas.com Fuente de Internet	<1%
34	Submitted to Universidad de Valladolid Trabajo del estudiante	<1%
35	www.systemconsultores.com Fuente de Internet	<1%
36	www.ic.gc.ca Fuente de Internet	<1%
37	Submitted to Systems Link Trabajo del estudiante	<1%
38	www.sdominguez.com Fuente de Internet	<1%
39	comuna.cat Fuente de Internet	<1%
40	www.rap.org.pe Fuente de Internet	<1%
41	www.gpi.tsc.uvigo.es Fuente de Internet	<1%
42	www.uoc.edu Fuente de Internet	<1%
43	Submitted to INACAP	

	Trabajo del estudiante	<1%
44	diegocer.blogspot.com Fuente de Internet	<1%
45	www.angelfire.com Fuente de Internet	<1%
46	repositorio.uax.es Fuente de Internet	<1%
47	Submitted to Universidad Manuela Beltrán Virtual Trabajo del estudiante	<1%
48	eduangi.org Fuente de Internet	<1%
49	Submitted to University of Plymouth Trabajo del estudiante	<1%
50	upcommons.upc.edu Fuente de Internet	<1%
51	aic-online.net Fuente de Internet	<1%
52	Submitted to Hodges University Trabajo del estudiante	<1%
53	ruidera.uclm.es Fuente de Internet	<1%
	www2.reacciun.ve	

54	Fuente de Internet	<1%
55	www.oalib.com Fuente de Internet	<1%
56	www.reuna.cl Fuente de Internet	<1%
57	www.flyingabroad.co.uk Fuente de Internet	<1%
58	www.todalaley.com Fuente de Internet	<1%
59	Submitted to Texas A&M University, College Station Trabajo del estudiante	<1%
60	www2.ing.puc.cl Fuente de Internet	<1%
61	www.die.udec.cl Fuente de Internet	<1%
62	www.romaguerratotal.com Fuente de Internet	<1%
63	sepe.rau.edu.uy Fuente de Internet	<1%

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Monitoreo en la red avanzada CLARA : Emulación

INFORME DE GRADEMARK

NOTA FINAL

/0

COMENTARIOS GENERALES

Instructor

PÁGINA 1

PÁGINA 2

PÁGINA 3

PÁGINA 4

PÁGINA 5

PÁGINA 6

PÁGINA 7

PÁGINA 8

PÁGINA 9

PÁGINA 10

PÁGINA 11

PÁGINA 12

PÁGINA 13

PÁGINA 14

PÁGINA 15

PÁGINA 16

PÁGINA 17

PÁGINA 18

PÁGINA 19

PÁGINA 20

PÁGINA 21

PÁGINA 22

PÁGINA 23

PÁGINA 24

PÁGINA 25

PÁGINA 26

PÁGINA 27

PÁGINA 28

PÁGINA 29

PÁGINA 30

PÁGINA 31

PÁGINA 32

PÁGINA 33

PÁGINA 34

PÁGINA 35

PÁGINA 36

PÁGINA 37

PÁGINA 38

PÁGINA 39

PÁGINA 40

PÁGINA 41

PÁGINA 42

PÁGINA 43

PÁGINA 44

PÁGINA 45

PÁGINA 46

PÁGINA 47

PÁGINA 48

PÁGINA 49

PÁGINA 50

PÁGINA 51

PÁGINA 52

PÁGINA 53

PÁGINA 54

PÁGINA 55

PÁGINA 56

PÁGINA 57

PÁGINA 58

PÁGINA 59

PÁGINA 60

PÁGINA 61

PÁGINA 62

PÁGINA 63

PÁGINA 64

PÁGINA 65

PÁGINA 66

PÁGINA 67

PÁGINA 68

PÁGINA 69

PÁGINA 70

PÁGINA 71

PÁGINA 72

PÁGINA 73

PÁGINA 74

PÁGINA 75

PÁGINA 76

PÁGINA 77

PÁGINA 78

PÁGINA 79

PÁGINA 80

PÁGINA 81

PÁGINA 82

PÁGINA 83

PÁGINA 84

PÁGINA 85

PÁGINA 86

PÁGINA 87

PÁGINA 88

PÁGINA 89

PÁGINA 90

PÁGINA 91

PÁGINA 92

PÁGINA 93

PÁGINA 94

PÁGINA 95

PÁGINA 96

PÁGINA 97

PÁGINA 98

PÁGINA 99

PÁGINA 100

PÁGINA 101

PÁGINA 102

PÁGINA 103

PÁGINA 104

PÁGINA 105

PÁGINA 106

PÁGINA 107

PÁGINA 108

PÁGINA 109

PÁGINA 110

PÁGINA 111

PÁGINA 112

PÁGINA 113

PÁGINA 114

PÁGINA 115

PÁGINA 116

PÁGINA 117

PÁGINA 118

PÁGINA 119

PÁGINA 120

PÁGINA 121

PÁGINA 122

PÁGINA 123

PÁGINA 124

PÁGINA 125

PÁGINA 126

PÁGINA 127

PÁGINA 128

PÁGINA 129

PÁGINA 130

PÁGINA 131

PÁGINA 132

PÁGINA 133

PÁGINA 134

PÁGINA 135

PÁGINA 136

PÁGINA 137

PÁGINA 138

PÁGINA 139

PÁGINA 140

PÁGINA 141

PÁGINA 142

PÁGINA 143

PÁGINA 144

PÁGINA 145

PÁGINA 146

PÁGINA 147

PÁGINA 148

PÁGINA 149

PÁGINA 150

PÁGINA 151

PÁGINA 152

PÁGINA 153

PÁGINA 154

PÁGINA 155