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

"**Emulación de la red avanzada CLARA"**

TRABAJO RECEPCIONAL
PARA OBTENER EL TÍTULO DE LICENCIADO EN
INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

PRESENTA:

José Joaquín Sánchez Trejo

Director del trabajo recepcional

M. en C. José Ignacio Castillo Velázquez

México, D.F. Mayo, 2015.

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©

ÍNDICE

Página.

AGRADECIMIENTOS

Agradezco infinitamente a mis padres, Benito Sánchez Mexica y María Domitila Trejo Galán, así como a mi hermana Yazmín Sánchez Trejo por su apoyo incondicional durante todo el proceso de mi formación profesional como ingeniero. Y como muestra principal, deposito en sus manos el presente trabajo que representa a demás de esfuerzo y sacrificios, un paso más en mi carrera profesional.

Mi agradecimiento también va dirigido a la Universidad Autónoma de la Ciudad de México, por haberme aceptado ser parte de ella y abierto las puertas de su seno científico para estudiar una carrera profesional, así como a los diferentes profesores que brindaron sus conocimientos y apoyo para concluir mi formación profesional.

De manera muy especial agradezco a mi director, el M. en C. José Ignacio Velázquez, por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico. Sus orientaciones, su manera de trabajar, su persistencia y su motivación han sido fundamentales para mi formación como ingeniero. Él ha inculcado en mí un sentido de seriedad, responsabilidad, rigor académico sin los cuales no podría tener una formación completa como ingeniero.

Para finalizar, también agradezco a los lectores, la M. en C. Magali Cortez Vázquez, el M. en C. Joel Yazbek Buendía Gómez, la Mtra. Rita Xóchitl Vázquez Padilla y al Capitán Ingeniero Juan Manuel Hernández Carrizosa de la Escuela Militar de Transmisiones de la Secretaria de la Defensa Nacional por sus observaciones, sugerencias y revisión del presente trabajo.

RESUMEN

En 1969 se iniciaron las primeras conexiones de ARPANET (Advanced Research Projects Agency Network) con tres universidades y un centro de investigación, las cuales serían el inicio de internet1, concepto que fue determinado en 1995 cuando el gobierno de los Estados Unidos decide dejar formalmente el control del backbone de internet.

Para 1996 se inicia el proyecto de Internet2 en EEUU, a través de la Corporación Universitaria para el desarrollo de Internet Avanzado, el cual inició con 34 universidades; su objetivo era el desarrollo de tecnología avanzada de internet con fines de investigación y educación. Permitía ejecutar proyectos de investigación desarrollados por universidades y centros de investigación que demandaban un ancho de banda mayor al de internet comercial. Las velocidades de transmisión en sus enlaces eran de 2.4 Gbps en un inicio y al 2013 ya contaban con enlaces a 100 Gbps. En este contexto, la red CLARA (Colaboración Latinoamérica de Redes Avanzadas) provee una infraestructura a las diferentes redes nacionales para realizar proyectos de investigación y educación que permitan el desarrollo de internet2. Las primeras conexiones se realizaron en el 2004 y a más de una década el backbone a incrementado la velocidad de transmisión en sus enlaces ya que para el 2013 estaba formada por 13 países y enlaces a velocidades de trasmisión de 2.5 Gbps en el anillo que cierran los países de Panamá, Chile, y Brasil.

En el presente documento se describe la red CLARA eligiendo como referencia la infraestructura de la topología 2013, con el objetivo de analizar la transmisión del backbone configurado con el protocolo OSPF utilizando routers Ciscos 7200 con IOS reales, con los cuales se realiza la segunda aproximación y se obtienen resultados del análisis en la transmisión y en la configuración del protocolo muy cercanos a los reales.

INTRODUCCIÓN

Las redes de telecomunicaciones, se han convertido en parte fundamental para la investigación, la educación y el avance tecnológico, a partir de que se realizó la primera conexión entre dos computadoras en 1965 por el doctor Lawrencen G. Roberts, al conectar la computadora TX-2, construida con transistores, contaba con lectora fotoeléctrica de cinta de papel y cinta magnética para el almacenamiento, situada en Massachusetts en el MIT (Massachusetts Institute of Technology) con la Q-32 ubicada en Santa Mónica California en el SDC (System Develoment Corporation), que utilizaban la tecnología de conmutación de circuitos [1,2].

A partir de este logro tecnológico, se fueron construyendo las teorías y estándares que permitieron seguir con el desarrollo de las redes de datos. Una de las tecnologías que permitió que las redes se estandarizaran y que pudieran tener una transmisión de información más eficiente, fue la conmutación de paquetes, que ha sido hasta ahora fundamental para que operen las redes de datos, desde la implementación en la red ARPANET (Advanced Research Projects Agency Network) y durante el desarrollo de ésta, conocida actualmente como internet1 [1].

Internet1 es el resultado del avance tecnológico que ha revolucionado el mundo de las telecomunicaciones, proporcionando diferentes servicios que son parte de las tareas que a diario realizamos, como la difusión de información a través de la red; con el aumento de los dispositivos electrónicos cada vez son más los usuarios que se conectan a internet, la tendencia del uso de internet continuará creciendo. internet1 representa uno de los proyectos más exitosos en tecnología de los últimos 44 años, realizado por investigadores e ingenieros, lo cual también permitió desarrollar otras redes de nueva generación cuyo ejemplo más emblemático es internet2 [1].

Internet2 es una red avanzada de nueva generación, es el resultado del desarrollo y evolución del internet1; esta nueva tecnología de redes de computadoras ha permitido transmitir datos más rápido que en internet comercial. La interconexión de las redes avanzadas de los países de Latinoamérica se realizó a través de la red CLARA(Colaboración Latinoamericana de Redes Avanzadas), la cual evolucionó las telecomunicaciones de Latinoamérica al implementar una red avanzada de nueva generación para la interconexión de los diferentes países a internet2; su infraestructura de backbone permite realizar proyectos de investigación que demandan una velocidad de transmisión superior a internet1 y conecta únicamente a universidades y centros de investigación, separándolos del tráfico que se presenta en la red de internet comercial [3,4].

La infraestructura de CUDI (Corporación Universitaria para el Desarrollo de Internet), que es internet2 en México, sigue evolucionando por lo que es importante conocer los protocolos, velocidades de transmisión, los equipos y servicios con los que cuenta el backbone de la red CLARA, por lo ya mencionado uno de los objetivos del presente trabajo es realizar un análisis del backbone, a través de un simulador y emulador, para revisar la operación del protocolo, las velocidades de transmisión y los tiempos de respuesta al enviar información entre los routers, la información que se presenta nos permitirá tener un mejor conocimiento de estas tecnologías de transmisión de datos y del funcionamiento del bakbone de la red avanzada de Latinoamérica.

En el capítulo I se hace una revisión de las etapas del nacimiento de internet1 y de internet2 en EEUU. En el capítulo II se describirá el nacimiento y la evolución de la red CLARA en Latinoamérica que será la base para la construcción de las nuevas generaciones de redes avanzadas (En un futuro podría llamarse la internet3) de Latinoamérica. En el capítulo III se hace una revisión de los protocolos de ruteo y se profundiza

en el protocolo OSPF (Open Shortest Path First) que se configura para realizar el análisis del backbone de la red avanzada CLARA. En el capítulo IV se realiza un análisis del backbone utilizando la herramienta de simulación Packet Tracer como primera aproximación. En el capítulo V se realiza un análisis del backbone de la red avanzada CLARA, utilizando el emulador GNS3 (Graphic Network Simulator) como una segunda aproximación más cercana a la real, para validar los parámetros y el funcionamiento del protocolo OSPF en la red, así como el funcionamiento del backbone en cuanto a transmisión y tiempos de respuesta. Finalmente una de las conclusiones que se presenta en el trabajo es la capacidad que tiene el emulador GNS3, para poder analizar el backbone de la red avanzada CLARA, ya que cuenta con routers ciscos 7200 de bakcbone y se trabaja directamente con las IOS (Internetwork Operating System) de equipos reales, lo cual nos permite obtener en el análisis resultados como si se estuviera trabajando con equipos reales [4].

CAPÍTULO I EL NACIMIENTO DE INTERNET

Los principales fechas que marcaron el desarrollo de internet1 iniciaron en 1969, fecha en que se realizaron las principales conexiones de ARPANET conectando tres universidades y un centro de investigación, y hasta 1995 cuando el gobierno de los EEUU decide terminar el control de la infraestructura de internet1, a través de estos años se realizaron grandes aportaciones que permitieron la evolución de internet1 como la tecnología de conmutación de paquetes que es fundamental para la transmisión de datos en internet1. La capacidad de internet1 era insuficiente, para soportar los proyectos de educación e investigación que requerían un mayor ancho de banda; En respuesta a esta demanda y como resultado de la evolución de internet1, se crea internet2. La red fue desarrollada en EEUU conectando inicialmente centros de supercómputo, para que posteriormente se sumaran universidades y centros de investigación, a través de los conectores GigaPoP (Gigabit Point of Presence) que se encuentran distribuidos a lo largo de EEUU, los cuales son puntos de acceso a la red que soportan transferencias de al menos 1 Gbps.

En las diferentes etapas que marcaron el desarrollo de internet1, se aportaron sin duda una gran cantidad de teorías y de investigación, que marcaron una nueva era en las comunicaciones como se indica en las etapas I, II y III que se describe a continuación [5].

1.1 Etapa I: 1962-1983

En 1962 JCL Licklider escribió un documento, en el cual mencionaba la idea de realizar una red de computadoras que serian conectadas a través de diferentes zonas geográficas llamada Thinking centers (centros pensantes), ya trabajando para ARPA (Advanced Research Projects Agency), Licklider escribió, las primeras líneas sobre la creación de una red global de computadoras a la cual la llamó Red Galáctica [6].

A Leonard Kleinrock, Donald Davies y Paul Baran (EEUU) se les considera como los creadores de la conmutación de paquetes, con estas aportaciones ya se estaba realizando lo que predijo Licklider, ya que él mencionaba en sus documentos que se tardaría entre 10 y 15 años para llegar a tener la red global de computadoras, una vez que la tecnología permitiría el crecimiento de la interconexión entre computadoras. En 1963 se creó la conmutación de paquetes, teoría que hace posible la comunicación entre equipos de cómputo a través de una red centralizada. Esta teoría permitió que los datos fueran divididos en fragmentos de paquetes para que viajaran a través de diferentes rutas, para llegar a su destino y ser ensamblados nuevamente formando los datos enviados, es decir, la información podía tomar diferentes caminos para que pudieran llegar a un mismo destino [5].

En 1964 Paul Baran [EEUU] creó la primera red de comunicaciones distribuida, que se podía conectar con diferentes nodos, en la cual se divide la información en segmentos de 1024 bits y se agregó un encabezado para el enrutamiento, que es reconstruido por el receptor del paquete, en este mismo año Donald Watts Davies [UK], (quien también desarrolló un sistema como Baran) describió a los bloques de datos como "conmutación de paquetes". En 1966 ARPA que ya trabajaba con conmutación de paquetes, emprendió un proyecto para conectar a todas las universidades de EEUU, mientras las comunicaciones fueron cambiando de tecnología analógica a digital y se presentaban las propuestas de la velocidad de transmisión para ser usada en el diseño de ARPANET que eran de 2.4 Kbps a 56 Kbps.

Nuevas iniciativas se presentaban por parte de ingenieros e investigadores en esta primera etapa, por lo que en 1968 después de una planeación en las especificaciones de ARPANET, DARPA (The Defense Advanced Research Projects Agency) presentó un proyecto para que se desarrollara uno de los componentes claves de internet1, el IMP (Interface Message Processor) que trabajaría como uno de los equipos que hoy se

conoce como routers; el proyecto fue ganado e implementado por el grupo BBN (Richard Bolt, Leo Beranek y Newman).

Debido al desarrollo de la primera teoría de conmutación de paquetes y su enfoque en el análisis, diseño y medición, el centro de medición en UCLA (University of California, Los Angeles) fue seleccionado para ser el primer nodo de ARPANET. En septiembre de 1969 BBN instaló el primer IMP en UCLA a estas conexiones se sumaron el SRI, UCSB (University of California, Santa Barbara**)** y la de UTAH (University of Utah); para el 5 de diciembre de 1969 ya estaba operando la red en las 4 instituciones. En retrospectiva, el desarrollo de la ARPANET fue quizá el avance más significativo en las telecomunicaciones. En la figura 1-1 se indica el esquema de las primeras cuatro instituciones conectadas [1].

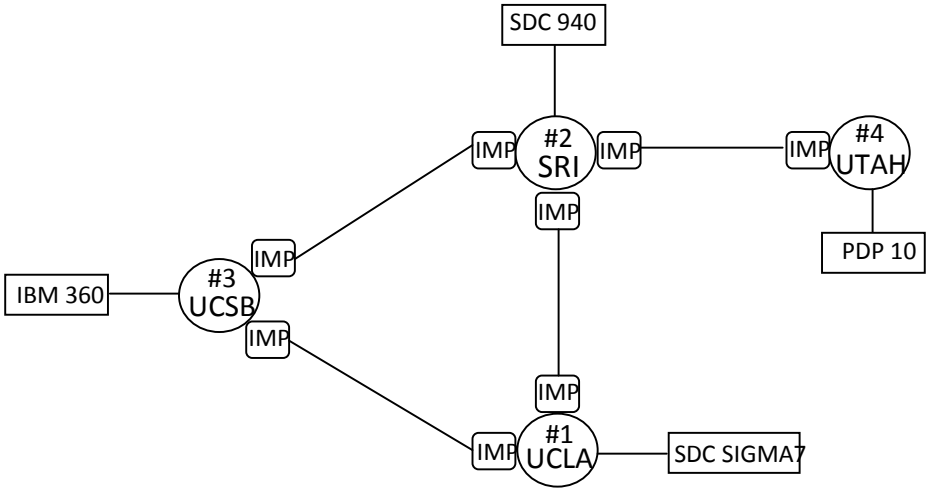


Figura 1-1 Esquema del Proyecto ARPANET, 1969 con cuatro nodos: (UCLA, SRI, UCSB y UTAH). Diagrama propio con base en referencia [7].

Después de la conexión de los primeros nodos a la red ARPANET se definieron algunos estándares de protocolos de red por parte de diferentes grupos de científicos. En 1970 el NWG (Network Working Group), donde se encontraba Vinton Cerf, desarrolló el protocolo inicial de ARPANET Host-to-Host, llamado NCP (Network Control Protocol), éste se terminó de implementar en los host de Internet durante el periodo de 1971 a 1972 [1].

A medida que se implementaban nuevas mejoras a la infraestructura y se solucionaban problemas técnicos como de programación y operación de ARPANET, ésta iba creciendo en el números de nodos conectados a la red, ya que cada vez era menos complicada la conexión de las computadoras, de igual forma iba creciendo en otros lugares del mundo, en donde ya estaban creando sus propias redes de forma paralela al desarrollo de ARPANET [7].

En 1971 ARPANET entró en servicio en 15 sitios de una red, pero tuvo una baja tasa de empleo. En 1972 Robert Kahn y Lawrence Roberts decidieron demostrar las capacidades de ARPANET para las telecomunicaciones en la ICCC (International Conference on Computer Communications) de IEEE (The Institute of Electrical and Electronics Engineers) en Washington DC, causando una gran impresión e impacto en los asistentes de la conferencia, lo cual se vio reflejado en el incremento del uso de la red, ya que después de la presentación se incrementó la red en un 67 %. Aunque los arquitectos de ARPANET, Robert Kahn y Vinton Cerf, la crearon inicialmente con la idea de facilitar el compartir recursos mediante el acceso remoto a archivos, con el gran auge que se presentó, debido a la aplicación del correo electrónico, los contratistas de la red generaron la primera compañía de comunicaciones por paquetes, Telnet Communications Corporation, para que fuera la primera red en llegar al mercado, dando servicio inicialmente a 7 ciudades de EEUU en 1975 [5].

Para el año de 1973 Vinton Cerf organizó un seminario para el diseño del protocolo huésped TCP (Transmission Control Protocol), en 1975 fue aprobada y liberada la primera versión. Se realizaron pruebas en el año de 1977 con enlaces satelitales y ARPANET seguía creciendo, ya contaba con 59 nodos como se indica en la figura 1-2, seguían incrementándose los equipos conectados a la red y con ello se empezó a incrementar la cantidad de tráfico a través de la red [5].

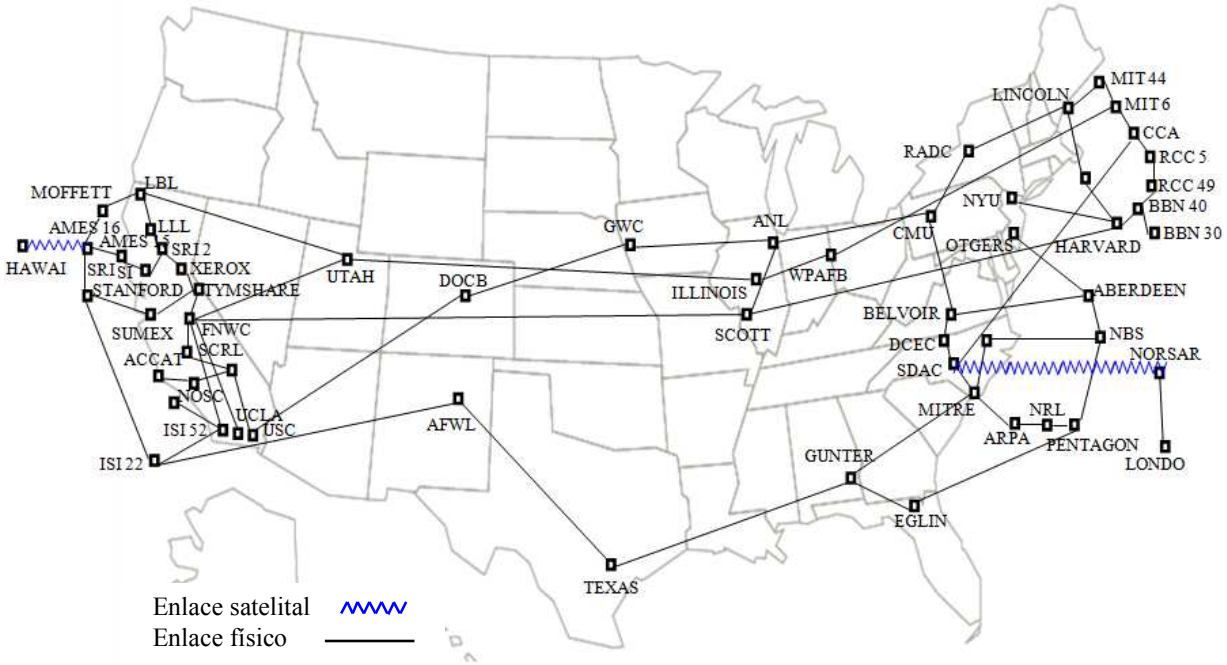


Figura 1-2 Conexión de 59 nodos a la red ARPANET, con dos enlaces satelitales uno a *Hawaii* y otro a *Noruega*, 1977. Diagrama propio con base en referencia [8].

En 1978 el protocolo TCP se dividió en dos componentes un protocolo *Host to Host* dentro de redes (TCP) y un protocolo de internet, al cual lo llamaron protocolo TCP/IP IP (Internet Protocol) era el encargado de pasar paquetes individuales de host a switch o entre switches, mientras que TCP se encargaba de ordenar tales paquetes y de proveer conexión a los host. El protocolo de Internet IP del conjunto de protocolos TCP/IP contiene información de los paquetes para que puedan ser direccionados a su destino, su función es transmitir los paquetes a través de un conjunto de redes interconectadas, pasando por diferentes dispositivos de red, los cuales son host y routers conectados a Internet, para el reenvió de los paquetes, dividendo la información en pequeños fragmentos que serán reconstruidos en el receptor. Cada paquete contiene información que permite identificar al destinatario y al emisor, agregando una dirección IP al encabezado del paquete, estas direcciones se pueden subdividir para crear subredes. Las direcciones de IP versión 4 son de 32 bits, cada una de estas se divide en dos partes principales: el número de red y la otra parte es la dirección del host, permite tener

aproximadamente cuatro mil millones de direcciones, lo cual apareció en la década de los 70, suficiente para que todos los equipos se conectaran a internet1 [9].

En 1981 se reemplazó el protocolo NCP por TCP/ IP en todos los host de ARPANET y fue hasta 1983 cuando lo hicieron posible. En este mismo año de 1983 se presentaron dos acontecimientos importantes que marcaron el desarrollo de ARPANET, la red militar MILNET (Military Network), decidió separarse de la red académica, por lo que todo estaba listo para comercializar una red civil con el protocolo TCP/IP. Durante este año, Robert Melcalfe desarrolló Ethernet en el Centro de Investigación Xerox Palo Alto, el cual implementó un protocolo de acceso al medio CSMA-CD (Carrier Sense Multiple Access with Collision Detection), mismo que detectaba las colisiones en el canal de comunicación, tecnología que durante los siguientes años se convertiría en un estándar mundial de redes de datos. En 1984 ya se contaba con 100 universidades y centros de investigación conectados a ARPANET, por otra parte Compuserve, America Online y Prodigy daban servicio comercial en línea vía modem a los usuarios de PC (Personal Computer) [9].

1.2 Etapa II 1985-1990

En 1985 la NSF (National Science Foundation) creó la red llamada NSFNET (The National Science Foundation Network), la cual tendría como objetivo conectar cinco supercomputadoras, que posteriormente se unirían a ARPANET y a finales de este mismo año el número de servidores conectados a la red era de 2,000. En 1987 la NSF implementó su backbone T1 (Estándar para la transmisión digital de voz y datos, a una velocidad de transmisión de 1.544 Mbps) entre los centros de supercomputación con 24 RT-CP (RISC Technology Personal Computer), implementados por IBM (International Business Machines) como routers, en este mismo año ya contaba con 10,000 nodos, luego entonces aumentó la velocidad de transmisión a T3 (44.77 Mbps) en su backbone [5,10,11].

En la figura 1-3 se indican los nodos de San Diego, Boulder, Urbana, Pittsburgh, Princeton e Ithaca conectados al backbone de NSFNET, así como los nodos que en ese año estaban conectados al backbone de ARPANET.

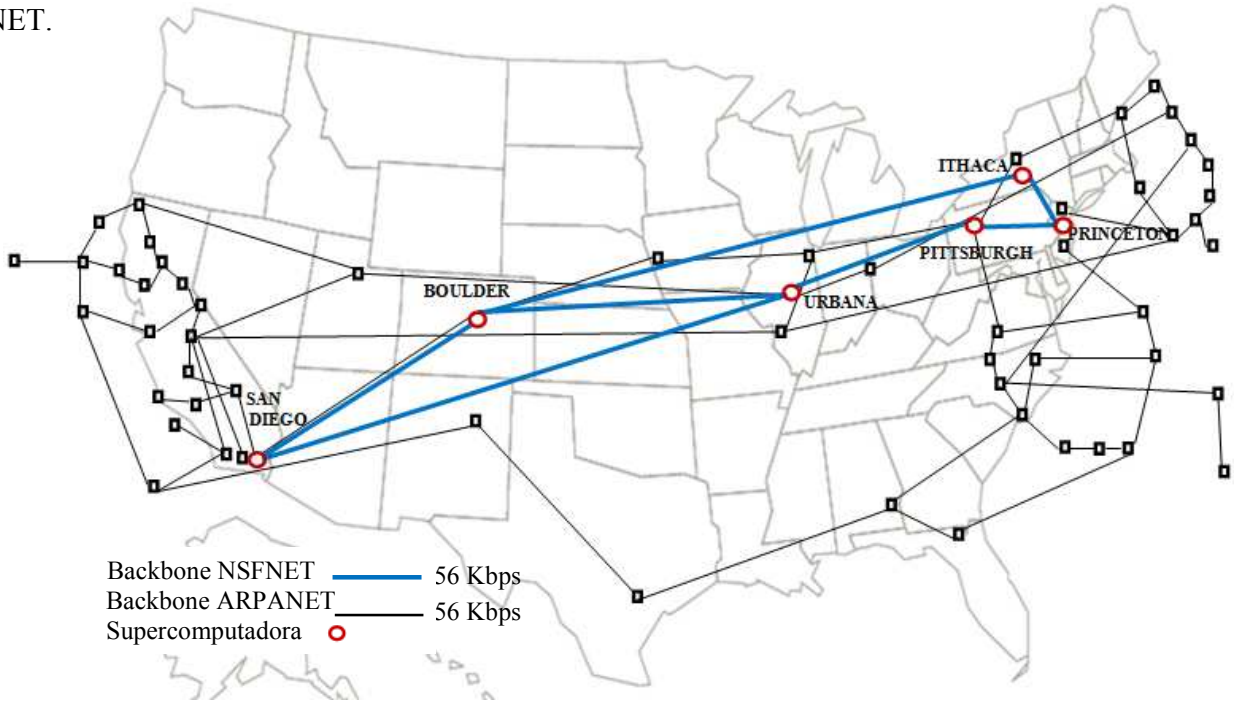


Figura 1-3 Backbone de la red NSFNET con 6 nodos ,1988. Diagrama propio con base en referencia [8].

En 1990 ARPANET dejó de existir y la NSFNET (National Science Foundation Network) tomó su lugar por lo que se convirtió en lo que sería el backbone de Internet. En este mismo año la Universidad de Minnesota introdujo el sistema Gopher (Programa informático que permitió facilitar el acceso a internet1) Mientras tanto el avance más significativo de esta etapa se realizó en diciembre del mismo año por Tim Berners Lee del CERN (European Organization for Nuclear Research) en Europa quien desarrollo la World Wide Web (versión 1) [5].

1.3 Etapa III 1991-1995

En 1991 la NSF determinó que el control de internet1 pasaría a los ISP (Internet Service Provider) quienes operarían su propio backbone, de esta manera los usuarios de la red se conectarían a los ISP, para que estos los interconectaran al Internet comercial. Mientras tanto en 1993 la NSF creó INTERNIC (Internet

Network Information Center), el cual determina la administración y los servicios de Internet, a través de directorios de dominios, En este mismo año la NCSA (National Center For Supercomputing Applications) de la Universidad de Illinois desarrolló una versión mejorada de visor de la web (web browser) llamado Mosaic, el primer sistema que permitía visualizar imágenes a color como parte de la página web, cuando la NCSA lanzó oficialmente Mosaic en noviembre del mismo año 40,000 usuarios ya tenían una copia del *browser*, para la primavera de 1994 ya habían descargado 1,000,000 usuarios la aplicación. Para el mismo 1994 NCSA desarrolló la versión comercial de Mosaic llamada Netscape, a partir de entonces gracias a la web y a los visualizadores web (browser) se popularizó Internet [5,10].

El 30 de Abril de 1995 el gobierno de los EEUU, terminó formalmente el control sobre la infraestructura de Internet. La privatización abrió la Internet a un segmento mucho mayor de la opinión pública estadounidense, con esto ya se podían ofrecer servicios comerciales en línea. En la figura 1-4 se indica el backbone de la NSFNET y de ARPANET al año de 1995 [5].

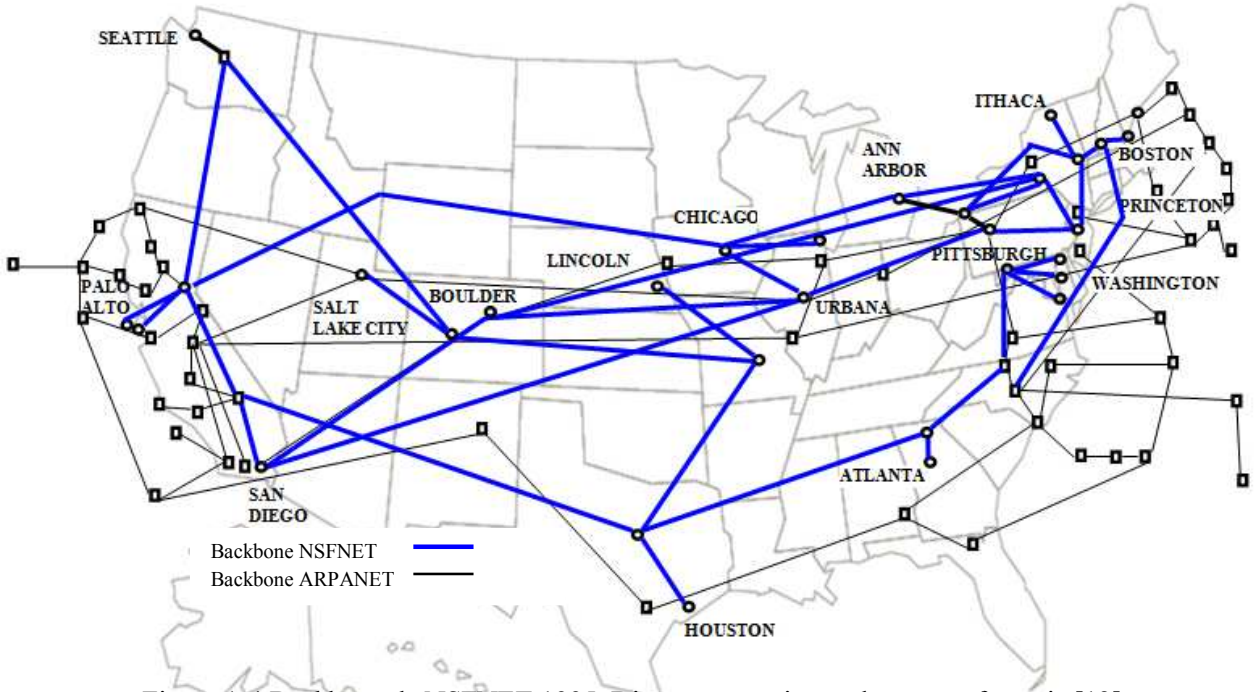


Figura 1-4 Backbone de NSFNET 1995. Diagrama propio con base en referencia [12].

1.4 El nacimiento de las Redes Avanzadas: Internet2

Una vez que en 1995 se creó internet comercial (internet1), el ancho de banda no era suficiente para realizar proyectos en los que se demandaba un ancho de banda mayor a lo que ofrecía ésta red. Al llegar a su máxima capacidad en cuanto a velocidad de transmisión se refiere, estudiantes e investigadores de las diferentes universidades ya no podían realizar tareas en esta red para el desarrollo e innovación de sus diferentes centros de investigación, así como para dar el siguiente paso en la evolución de Internet, por lo que se decidió implementar una red de datos que estaría conectada a través de las diferentes universidades [13].

En octubre de 1996 se inició el proyecto de internet2, el cual fue desarrollado y administrado por UCAID (University Corporation for Advanced Internet Development), el cual inició con la conexión de 34 universidades de EEUU para facilitar y fomentar la colaboración entre instituciones académicas, empresas y el gobierno; su objetivo era el desarrollo de tecnología avanzada de Internet y aplicaciones con fines de investigación y educativas, que permitieran ejecutar los proyectos de los diferentes centros de investigación, con la infrastructura de la NSF y la MCI (Microwave Communications, Inc). Estos formarían la VBNS (The very high-speed Backbone Network Service), que sería el inicio del backbone de internet2, dado que la Internet comercial era la internet1 [3,13,14].

El despliegue del backbone de ABILENE (Es una red alta velocidad que integran el backbone de internet2) se inició en 1998 en colaboración con Qwest Communications[1], Nortel Networks (Kit SONET) hoy extinta, Cisco System (routers 7200 y 12008) y la Universidad de Indiana (Operaciones de Red). En este año ABILENE la integraban 133 universidades, su arquitectura la integraban conectores GigaPop que serían un punto de acceso de red que soportarían transferencias de al menos 1 Gbps, estos se conectarían directamente

[1] Empresa de servicios de SONET (Synchronous Optical Network) Y DWD (Dense Wavelength Division Multiplexing)

con el core de ABILENE. También serían un punto de agregación para la conectividad regional para interconectar a las Universidades o a las diferentes redes regionales como se indica en la figura 1-5 [13,15].

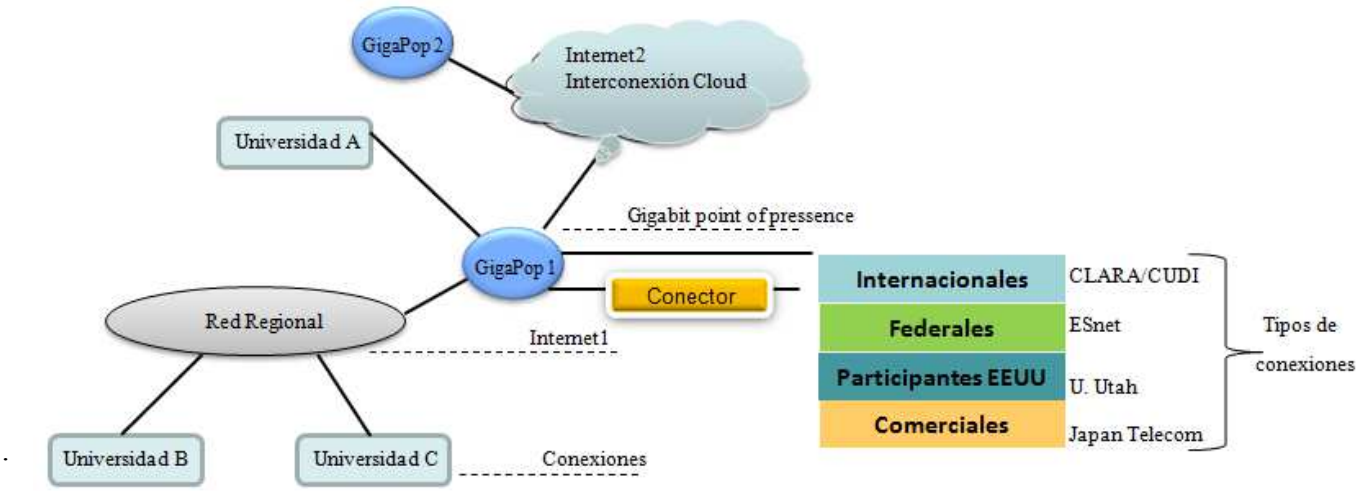


Figura 1-5 Arquitectura de internet2, Diagrama propio con base en referencia [15].

La red contaba con nueve routers centrales (más tarde se amplió a diez), interconectados por enlaces troncales de OC(Optical Carrier)-48 POS (Packet Over SONET) y OC-12 POS, que más tarde se actualizaron, cada router central se interconectaba a dos o tres routers del backbone. Por lo tanto los miembros del internet2 ya podían conectar a través de dos formas, podrían hacerlo directamente al conectarse a un *core router* directamente o través de un GigaPop regional, el cual era identificado como conector, ya que la mayoría de estos se unen a la red de internet2 a través de un enlace OC-3 u OC-12 utilizando IP/ATM (Asynchronous Transfer Mode**)** POS, también se conectarían utilizando OC-48 POS o 1 Gbps Ethernet, el factor límite para el último era la distancia entre conector y el router del backbone de ABILENE. En la figura 1-6 se indican los primeros routers conectados al backbone de ABILE en el año de 1998 [13].

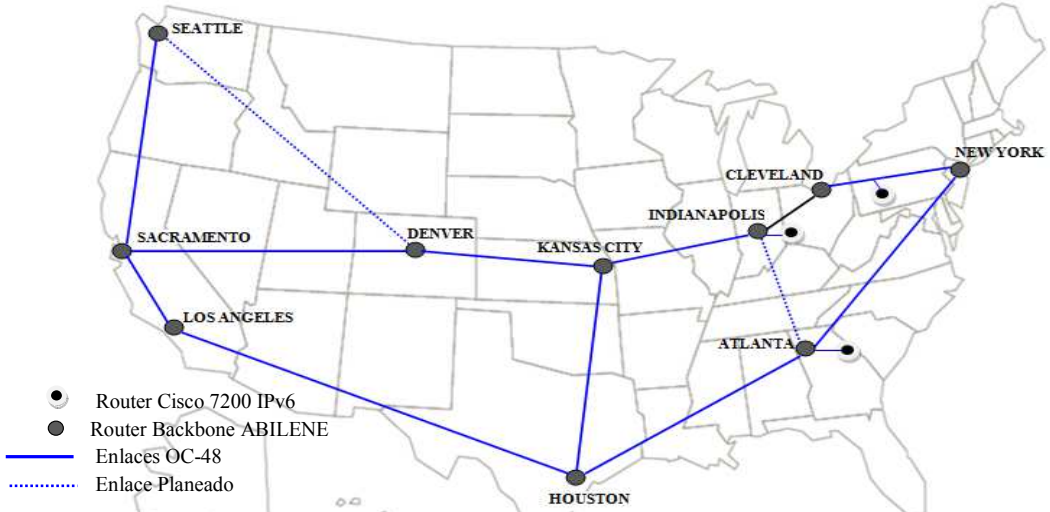


Figura 1-6 Backbone de ABILENE con 10 core routers 1998. Diagrama propio con base en referencia [16].

Otro backbone que integraba el core de internet2 era el de la red VBNS, que para el año de 1999 contaba con 16 conmutadores de backbone ATM, FORES ASX-100 con 16 puertos OC-12, que permitían las conexiones de los enlaces a velocidades de 622 Mbps, así como un enlace entre equipos Juniper M40 a 2.4 Gbps, enlaces de 45 Mbps entre equipos Cisco, enlaces a velocidades de 155 Mbps entre el backbone de la red y los equipos Cisco 7507 y Ascend AGR 400 como se indica en la figura 1-7 [17,18].

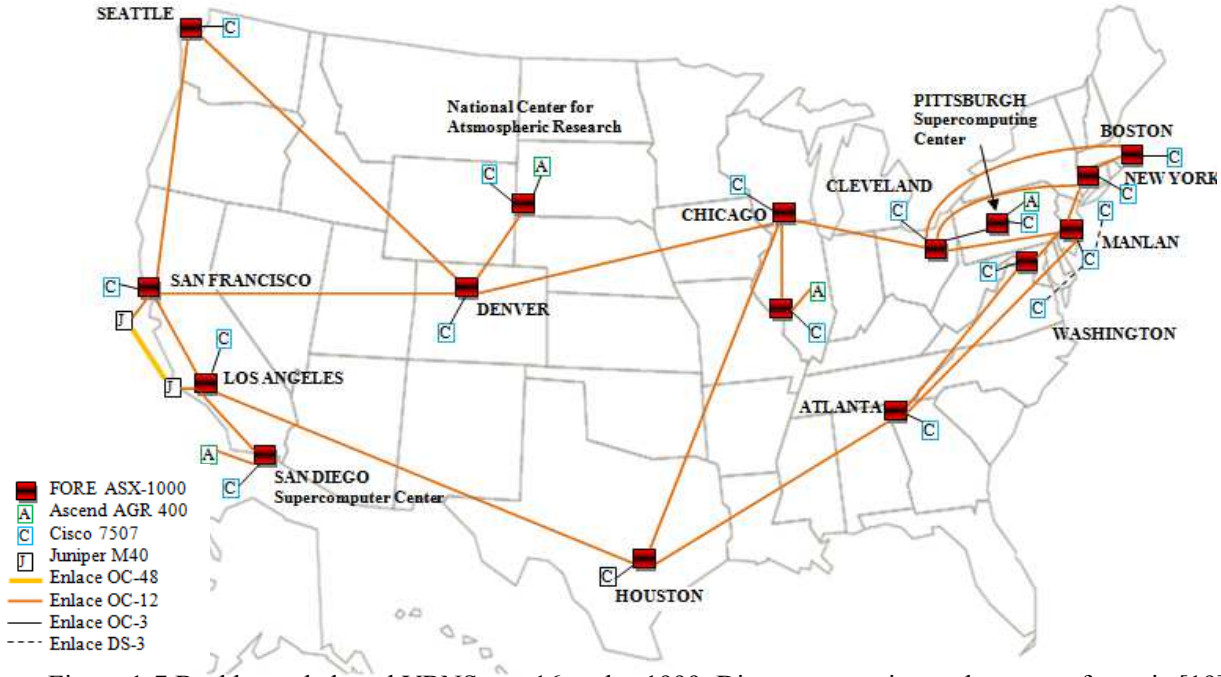


Figura 1-7 Backbone de la red VBNS con 16 nodos 1999. Diagrama propio con base en referencia [19].

El backbone de internet2 está formado por la infraestructura del backbone de las red VBNS y la de ABILENE, en los cuales los equipos de cada una de las redes se encuentran distribuidos en EEUU, para la interconexión de los dos backbones a través de routers core y de GigaPoP, como se indica en la figura 1-8.

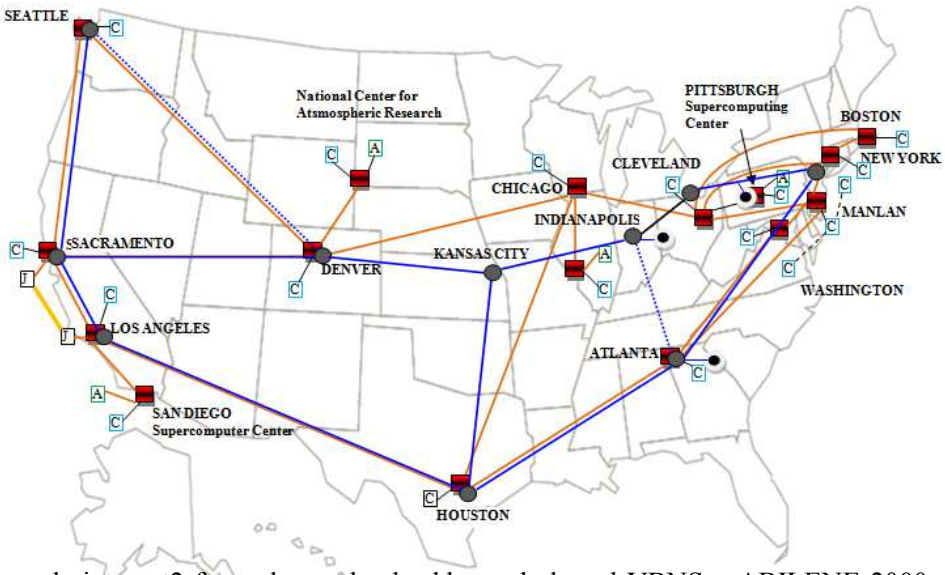


Figura 1-8 Backbone de internet2 formado por los backbone de la red VBNS y ABILENE 2000. Con un total de 26 nodos. Diagrama propio con base en referencia [16,19].

En el 2002 se realizó la segunda etapa de la red ABILENE en la que los ingenieros del NOC (Network Operations Center) determinaron que el software del sistema con soporte IPv6, era muy robusto como para implementarlo en los equipos Ciscos 12008, esto permitió implementar una red de doble pila IPv4/IPv6, en la cual los host conectados a través de un enlace, mantenían actualizadas las dos tabla de enrutamiento, para las dos direcciones de red. Los primeros routers que se actualizaron fueron los de Indianapolis y Kansas City con el fin de realizar pruebas entre las redes conectadas al Gigapop de Indiana [13].

Para el año 2002 ABILENE contaba con 221 participantes, entre los que se encontraban conectados universidades y centros de investigación, 58 conectores, 50 conexiones a diferentes redes, dentro de las cuales estaban las redes federales que integran a internet2 como DREN (Defense Research and Engineering Network) , ESnet (The Energy Sciences Network) y NREN (National Research and Education Network). En la figura 1-9 se indican el backbone de ABILENE, las velocidades con las que operaban los enlaces a través

de la infraestructura de la red, las cuales eran de OC-3 (155Mbps) POS/ATM, OC-12 (622Mbps) POS/ATM, OC-48 (2.4Gbps) POS/GigEthernet. También se indican los nodos core del backbone, los conectores de las universidades y redes regionales, las conexiones de capa 2, los identificadores de los diferentes participantes de ABILENE, los puntos de conexión a las redes internacionales como CUDI, GEANT (Es la red pan-European de investigación y educación que interconecta las NREN en Europa), CAnet (Canadian Network for the Advancement of Research), sólo por mencionar algunas, las futuras conexiones y las conexiones a la red a través de EEUU, como se indica en la figura 1-9 [13,19].

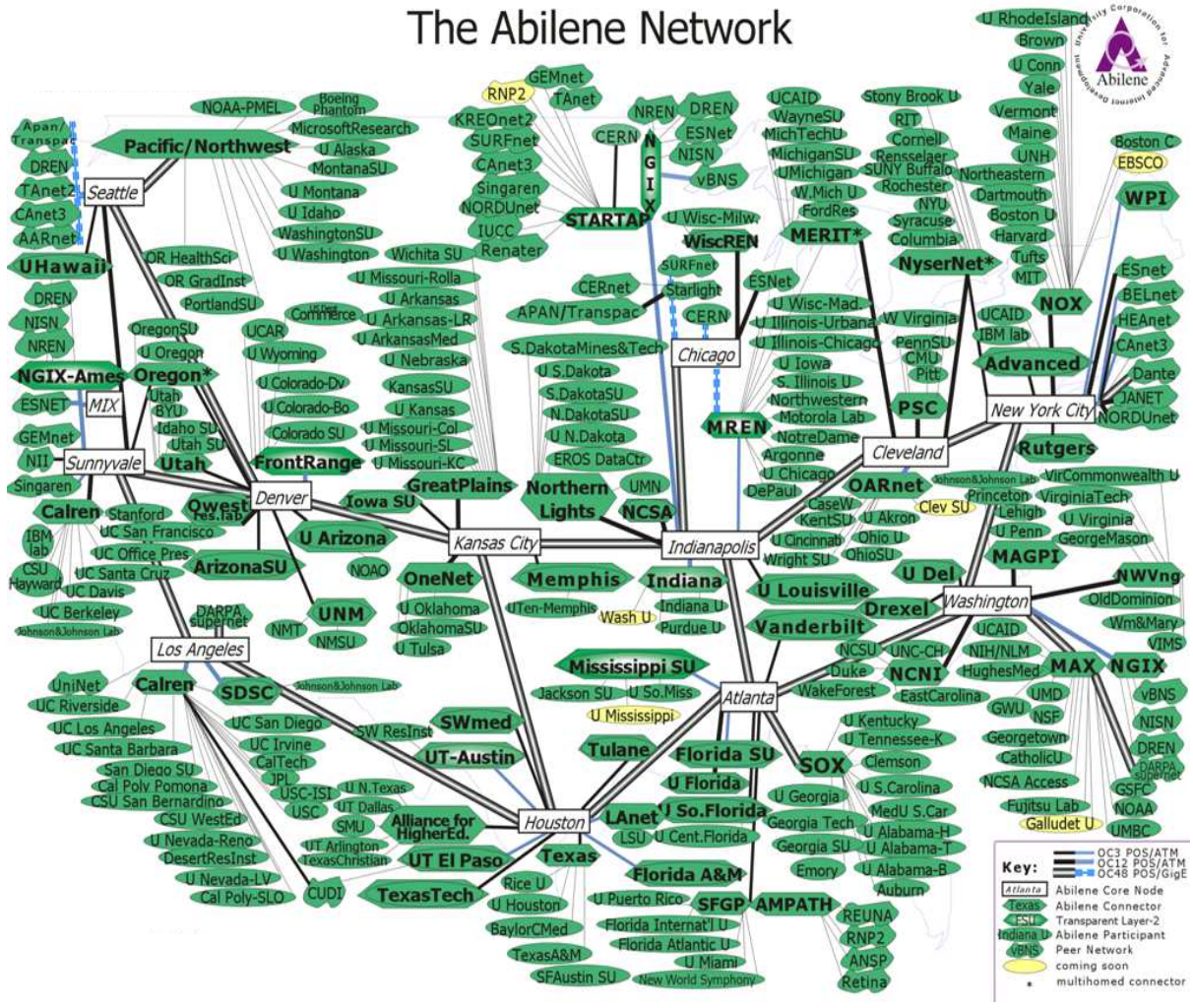


Figura 1-9 Redes académicas conectadas a 13 nodos del backbone de ABILENE, 2002 Diagrama con base en referencia [19].

En 2003 el backbone de ABILENE transmitía a OC-192 (9.4Gbps), contaba con 11 nodos conectados a través de las instituciones de EEUU, así como las conexiones a las diferentes redes de internet2 del mundo. En San Diego y el Paso Texas se encuentran los nodos que permiten la conexión de internet2 en EEUU a CUDI, que es internet2 en México. En New York se conecta a SINET (Science Information Network), en Washington a GEANT y en Miami a RETINE (Red Nacional de Investigación y Educación de Argentina), como se indica en la figura 1-10 [20,21].

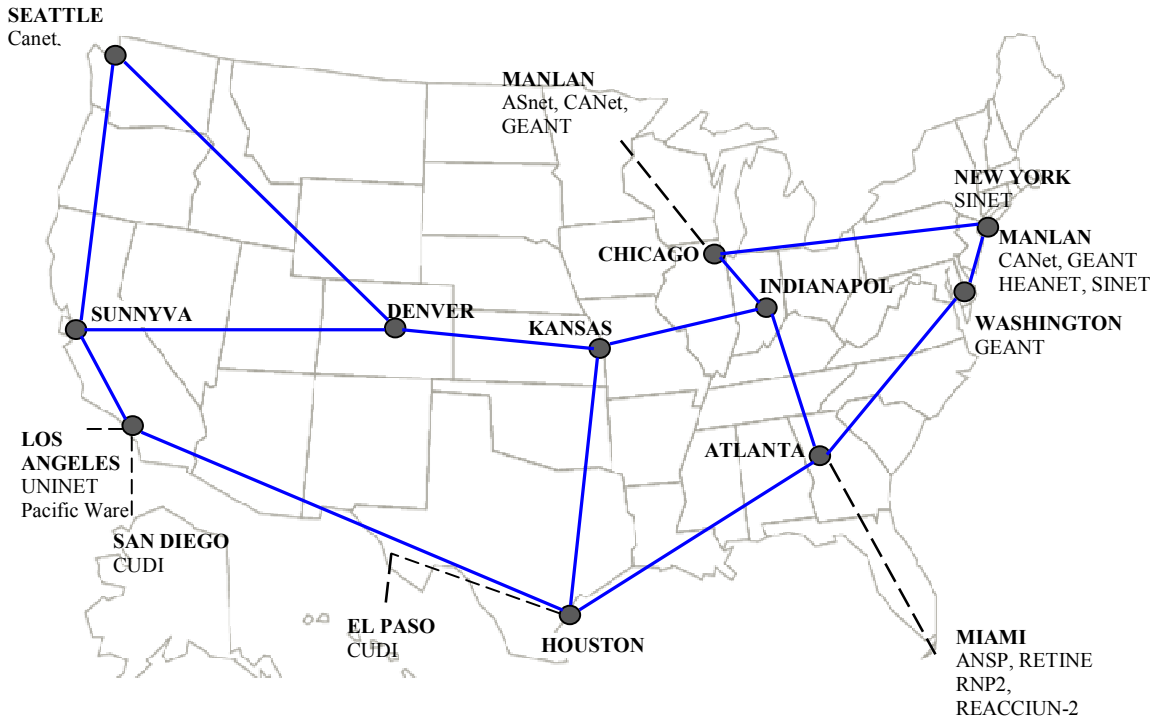


Figura 1-10 Backbone con 11 nodos conectados a Abilene 2003, obsérvese que ya no aparece Cleveland y Mix. Diagrama propio con base en referencia [21].

Para el 2013 el backbone de internet2 operaba a una velocidad de 100 Gbps utilizando una red DCN (Dynamic Circuit Network), una tecnología avanzada que permite la asignación de circuitos de datos en la red de fibra óptica y fiber chanel, en sus diferentes centros de datos conectados a internet2 y actualmente está formada por 212 universidades de Estados Unidos y otras 60 compañías tecnológicas como Comsat, Microsoft, Intel y AMD.

La infraestructura de internet2 se encuentra dividida en tres niveles, en cada uno de estos se ofrecen diferentes servicios y conexión a los usuarios [23].

1.4.1 Nivel 3

El nivel 3 se refiere a los servicios que ofrece internet2 a nivel de red, por lo que una institución que se conecta a través de esta capa, estará directamente conectado al backbone de internet2, lo cual permitirá conectarse a diferentes nodos del backbone, con poca latencia y dando un número menor de saltos al conectarse a los diferentes nodos de internet2. Con un ancho de banda de 5 Ghz con dos enlaces, 10 Ghz con uno o dos enlaces y 100 Ghz con un enlace, podemos ver este nivel como la capa3 core del modelo de las capas de Cisco System, ya que estos servicios de red se proporcionan estando conectados directamente al core de la red, nos permite conectarnos directamente con redes nacionales de investigación y las diferentes redes globales que se encuentran conectadas a internet2, también se pueden realizar conexiones a la capa2.

Los servicios de capa 3 se presentan directamente en el backbone de internet2 y sólo algunas instituciones se conectan directamente a estos nodos, como se indica en la figura 1-11 [23,24].

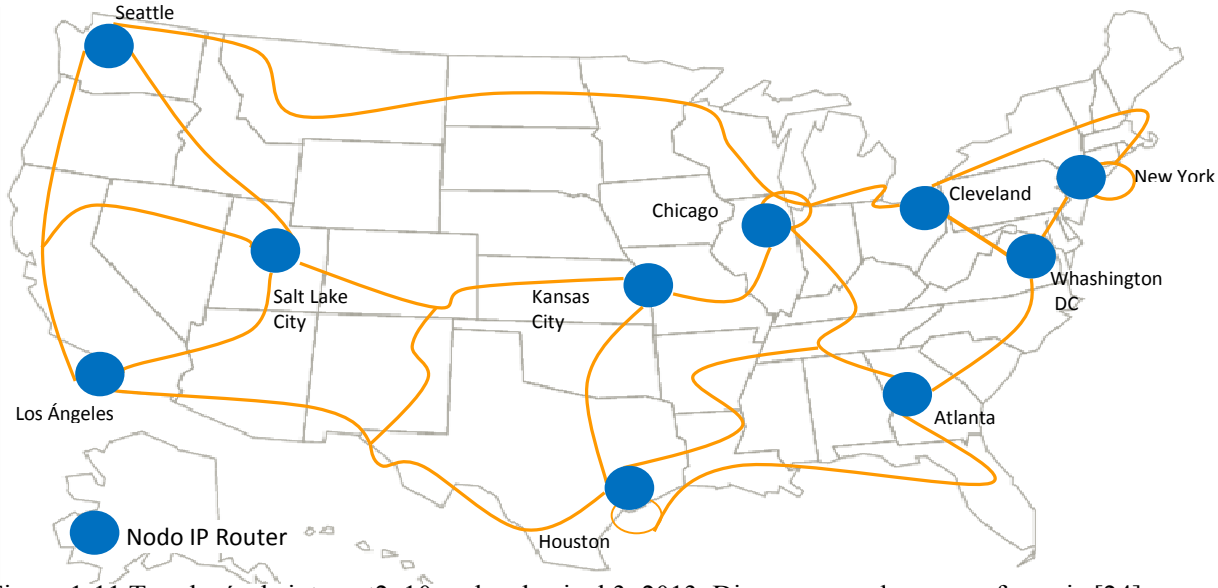


Figura 1-11 Topología de internet2, 10 nodos de nivel 3, 2013. Diagrama con base en referencia [24].

1.4.2 Nivel 2

El nivel 2 se refiere a los servicios que se ofrecen a los usuarios conectados a este nivel, la principal característica de esta capa es la de permitir la creación de VLAN (Virtual Local Area Networks) a los usuarios, haciendo uso de la infraestructura de internet2 también proporciona la conexión de un switch de agregación, por lo que podemos ver esta capa como la capa 2 de distribución. En el nivel 2 se encuentra los nodos que son un intermediario entre los usuarios de internet2 y del backbone, en este nivel de capa 2 se pueden realizar VLAN, para conectarse con cualquier universidad de investigación, tanto nacional como global que estén conectadas a internet2, el ancho de banda puede variar de 10 Ghz hasta 100 Ghz. Los nodos se pueden identificar como de distribución, ya que no están conectados directamente al backbone de Internet y los servicios que se ofrecen en este nivel son diferentes a los del nivel 1 y 3, como se indica en la figura 1-12 [32,25].

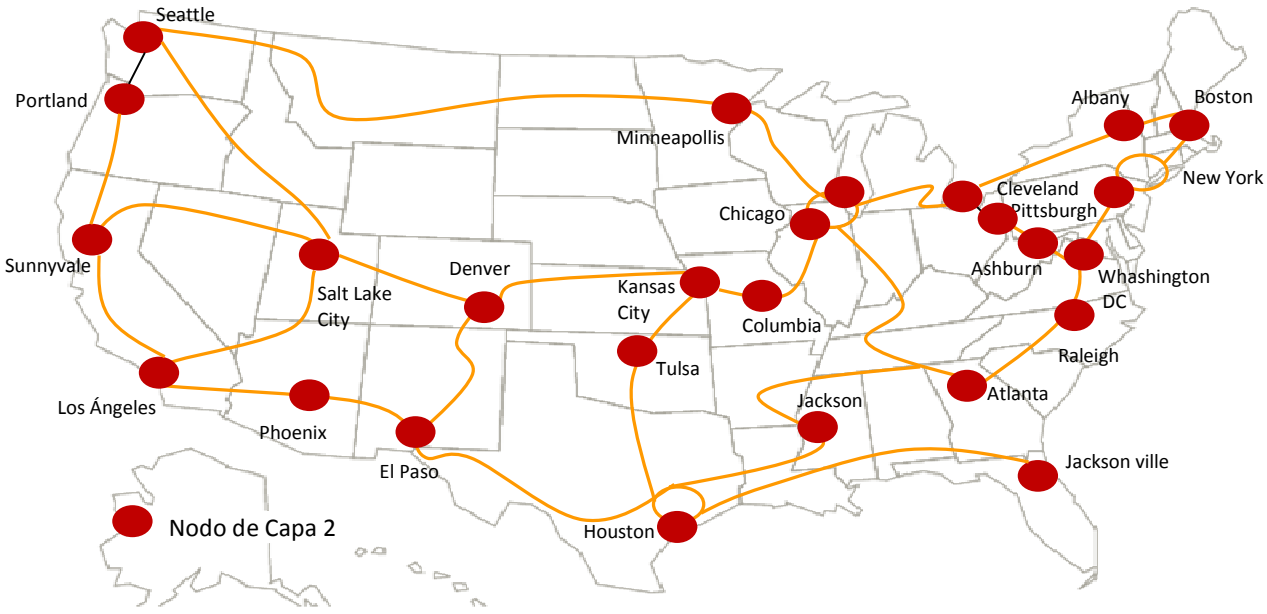


Figura 1-12 Topología de internet2, 26 nodos de nivel 2, 2013. Diagrama con base en referencia [25].

1.4.3 Nivel 1

La capa 1 se refiere a los servicios de los usuarios finales, los cuales sólo pueden hacer una red local, para aumentar el números de usuarios que serán conectados a internet2, sin tener las características de servicios que se describieron en las capas 2 y 3, por ello a la capa 1 la conocemos como capa de acceso [23].

En el nivel 1 proporciona un opción para las conexiones de usuarios finales a internet2, los cuales pueden contar con conexiones de 10 Ghz a 100 Ghz, también proporcionan un conjunto de herramientas especializadas y rentables, para poder crear nuestra red de alta velocidad, este nivel esta identificado por los nodos de los usuarios que requieren de un acceso a internet2, sin contar con los servicios que se ofrecen en los niveles de capa 2 y 3. En la figura 1-13 se indica la topología en donde se identifican los nodos del nivel l y los diferentes centros educativos y de investigación conectados a ellos, a través de la infraestructura de internet2 [26].

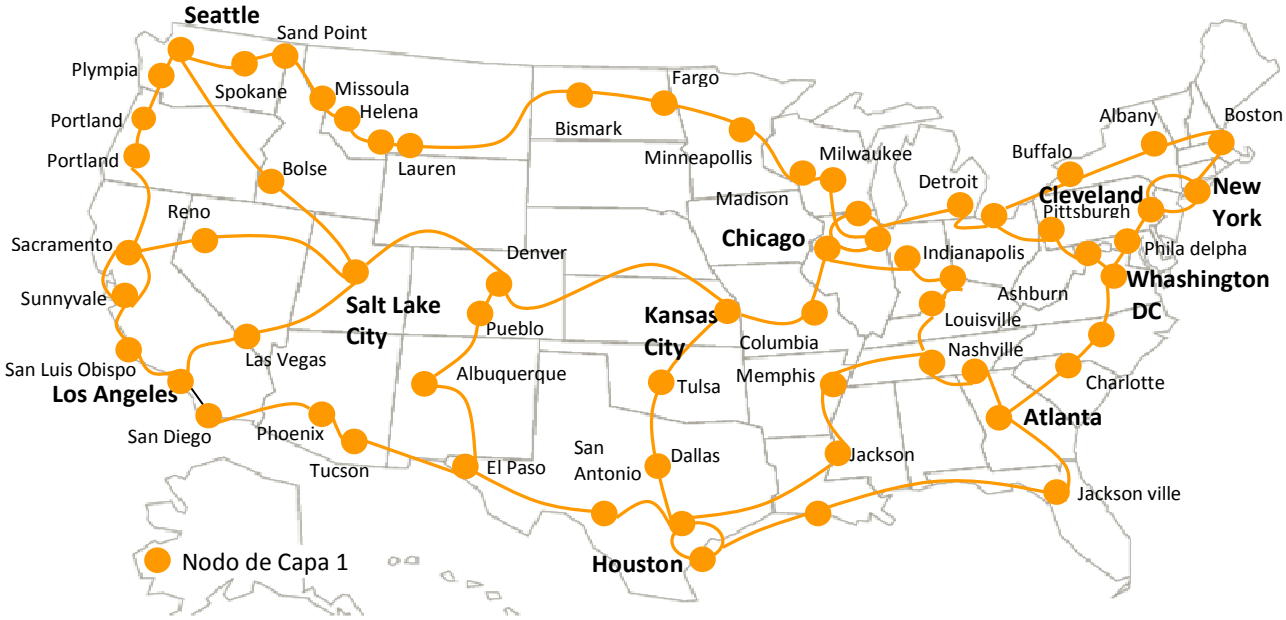


Figura 1-13 Topología de internet2, 63 nodos de nivel 1, 2013.Diagrama con base en referencia [26].

En la figura 1-14 se presenta la topología de la infraestructura de internet2 del 2013, en la cual se indican los nodos que proporcionan servicios en el nivel 3, las conexiones en los diferentes estados del país que proporcionan servicios en la capa 2 y los nodos que proporcionan servicios en la capa 1 [27].

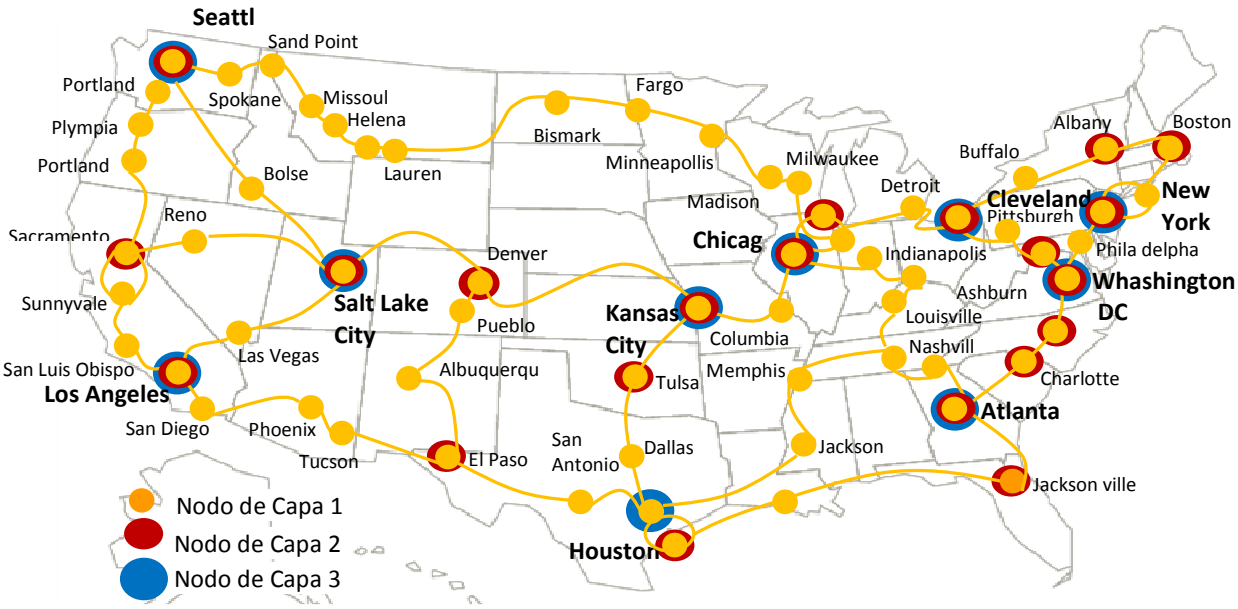


Figura 1-14 Topología de la infraestructura de internet2, en el que se incluyen los nodos de las 3 capas 2013. Diagrama con base en referencia [27].

La tecnología de la red nacional de fibra óptica de internet2 de 100 Gbps y el centro de operaciones de red NOC proporcionan un conjunto de servicios estratégicos para los líderes en la educación superior, el gobierno y la investigación para ofrecer a sus usuarios la solución de red más confiable de alta capacidad. El backbone cuenta con 17 routers juniper MX960 con soporte para la capa avanzada 3; 21 switches con soporte para servicios de red en la capa avanzada 2; 8.8 Tbps de capacidad en fibra óptica, Velocidad de 100 Gbps en las capas 2 y 3 [27].

1.5 Comparación del backone de internet1 con internet2

En la figura 1-2 se indicó el backbone de ARPANET después de 8 años del inicio en 1969, que más tarde pasaría a ser internet1, las primeras instituciones que se conectaron fueron las Universidades y centros de investigación, después se incremento el número de nodos hasta llegar a 59 nodos en el año de 1977. En la figura 1-10 se indica el backbone de internet2 después 7 años del inicio en 1996, contaba con 11 nodos conectados, el inicio de esta red avanzada fue muy similar al inicio del internet1, en cuanto a las instituciones conectadas, internet2 inició con la conexión de universidades y centros de investigación al igual que internet1, a diferencia de internet1 que no contaba con conexiones a redes avanzadas, ya que en el año de 1997 aún no se contaban con las redes avanzadas, otra característica importante son las primeras conexiones que se realizaron en zonas geográficas donde ya se contaba con una nodo directamente conectado al backbone de internet1, como es el caso de Houston, las rutas de los enlaces del backbone de internet2 son muy similares a las rutas del backbone de internet1.

Comparar el backbone de internet1 e internet2, nos permite identificar aspectos importantes para poder hacer una proyección de cómo sería la siguiente evolución en los próximos años de internet2, ya que la evolución de inetrnet1 se realizó por la demanda que tenían los proyectos de investigación en enviar grandes cantidades de información que no se podía realizar en internet1, de la misma forma los proyectos que actualmente se ejecutan en internet2 llegarán a requerir una cantidad mayor de recursos para ejecutarse y en un futuro internet2 tendrá que evolucionar para ofrecer velocidades de transmisión que requieran los proyectos de investigación.

CAPÍTULO II RED AVANZADA EN LATINOAMÉRICA

La red avanzada en Latinoamérica provee una infraestructura a las diferentes redes nacionales de investigación y educación para que puedan desarrollar aplicaciones y proyectos que permitan la evolución de Interenet2, así como la ejecución de los proyectos creados por universidades y centros de investigación. Las primeras conexiones de la red CLARA se realizaron en el 2004 y a más de una década ha pasado por una serie de cambios en su backbone al conectar redes nacionales como CUDI en México, así como el aumento de velocidades de transmisión en sus diferentes enlaces, los cuales al inicio de la infraestructura eran de 155 Mbps y al año del 2014 ya se contaba con enlaces de 10 Gbps, los cambios llevaron a la evolución de una red totalmente óptica: CLARA2, con las nuevas velocidades de transmisión en los enlaces de la red, el backbone soporta servicios y proyectos como las mallas computacionales que requieren de una mayor capacidad en la trasmisión de datos. En este capítulo se presentan las etapas de la evolución de la red CLARA en cuanto a su infraestructura de backbone se refiere, características de las velocidades de transmisión de sus enlaces, lo servicios de la red, características de ingeniería de tráfico y un diagrama de la topología de CLARA al primer semestre del 2013 con las conexiones de las diferentes redes nacionales de investigación y educación.

2.1 El Nacimiento de la Red CLARA

Desde la creación de internet2 en EEUU se crearon algunas redes avanzadas en Latinoamérica como CUDI en México, por lo que en diciembre del 2003 se creó legalmente CLARA, pero es hasta el 2004, cuando se realizan las primeras conexiones de la infraestructura [28].

La red CLARA es un Sistema de Colaboración Latinoamericana que emplea redes Avanzadas, para su principal objetivo, la educación, investigación e innovación. Esta red de Latinoamérica tiene como principal actividad, proveer una infraestructura avanzada para realizar proyectos de investigación, que permitan trabajar

en conjunto con los diferentes países interconectados a la red de Centroamérica y Sudamérica, para poder participar en conjunto en el desarrollo de investigación de las diferentes aplicaciones de innovación internet2, que se desarrollan en la universidad de los países de Latinoamérica. Los nuevos proyectos que se desarrollan en universidades requieren de una infraestructura como la red CLARA, que permita ofrecer servicios a una tasa de transmisión superior a las de Internet comercial. internet2 ofrecer un mayor ancho de banda para las necesidades que demandan los centros de investigación, para la ejecución de bases de datos, video conferencia en tiempo real y capacidad de procesamiento a altas velocidades [29].

Sin duda, para el proyecto ALICE (América Latina Interconectada con Europa) administrado por DANTE (Delivery of Advanced Network Technology to Europe) que coordina la I+E (investigación paneuropea y la educación), la creación de las NREN en favor de investigación, fue uno de los grandes logros al poder establecer los PoP (Puntos de Presencia). Para conectar a los primeros países al backbone de CLARA, en el 2004, los enlaces fueron STM-1 (155Mbps), estos países fueron: México (Tijuana), Panamá (Panamá), Chile (Santiago), Argentina (Buenos Aires), Brasil (Sao Paulo) y Venezuela (Caracas), con estos países se cerraba el anillo de CLARA, dejando las conexiones de los nodos, para que se sumaran posteriormente los siguientes países. Así el año de 2004 fue el año en que se puso en operación la red con los primeros países de Centro y Sudamérica, como se indica en la figura 2-1 [29,30].

En abril del 2005 se integró Uruguay a través del punto de presencia de Buenos Aires, para mediados de este año, ya se contaba con 7 países, en el mismo mes se conectó Perú a través del punto de presencia de Chile, para el mes de septiembre se integraron Costa Rica, Guatemala y el Salvador [4].

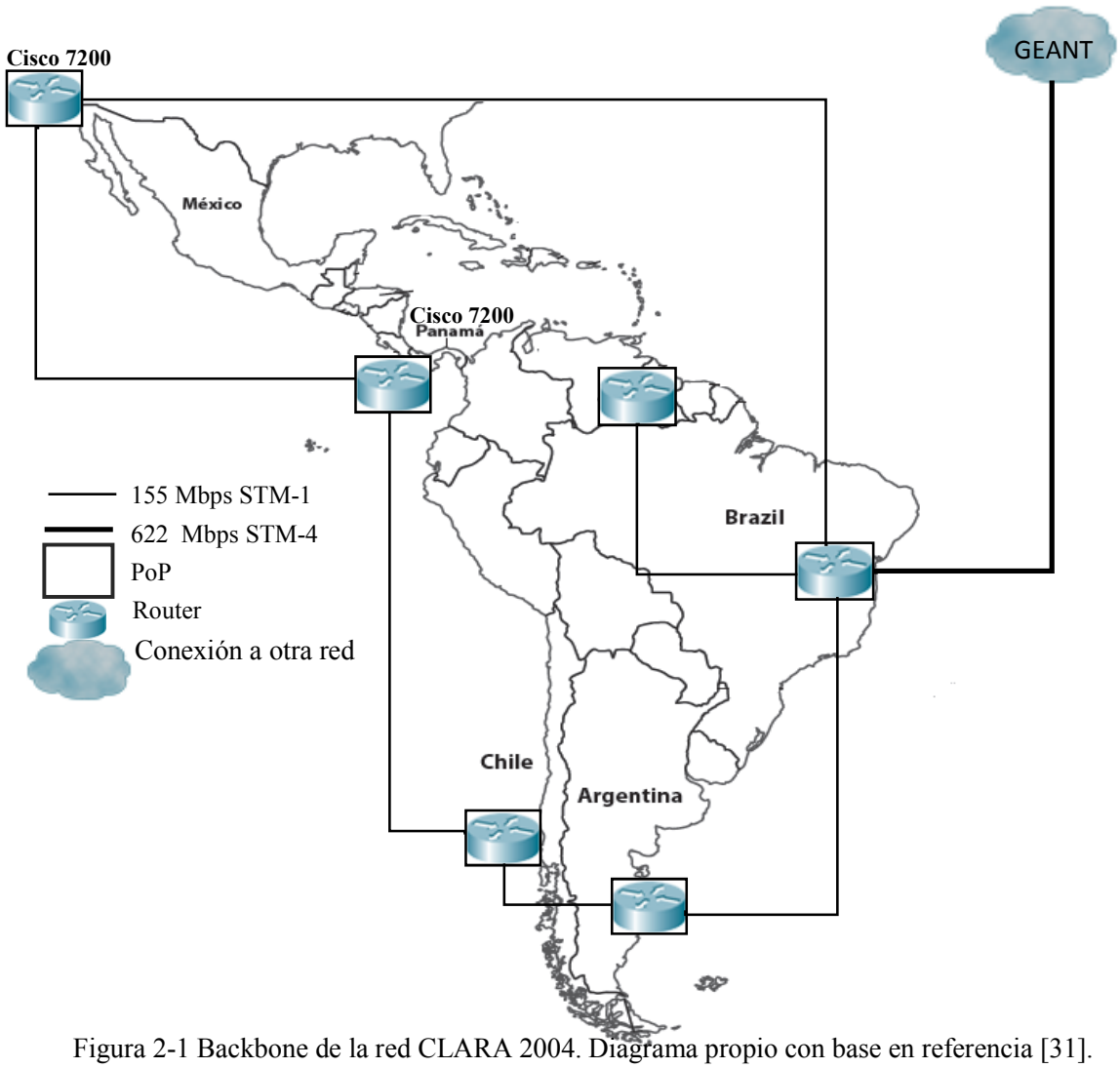


Figura 2-1 Backbone de la red CLARA 2004. Diagrama propio con base en referencia [31].

2.2 CLARA en 2006

La interconexión de los países de Centro y Sudamérica a través de una red de alta velocidad, era el precedente de uno de los proyectos más importantes en cuanto a la interconexión de una nueva tecnología se refiere, para el proyecto de ALICE y DANTE, se presentaba la red CLARA como la primera red de investigación de alta velocidad de Latinoamérica, por lo que durante este año se presentaron diferentes eventos en el que se mencionaba CLARA como un proyecto de innovación y desarrollo para la investigación, de Centro y Sudamérica [32].

Durante el 2006 se presentaban proyectos en los cuales la red estaría participando para interconectarse con otras redes, tal fue el caso del proyecto WHREN/LILA (Western Hemosphere Research and Education Network/Links Interconnecting Latin América), el cual había sido aprobado por la NSF, este permitiría que la red CLARA aumentará la capacidad de transporte de datos, conectando Tijuana con San Diego, lo que permitiría conectar el nodo de CLARA con CENIC (Corporation for Education Network Initiatives of California) con una enlace de fibra obscura y Sao Paulo y Miami.

Específicamente en el NAP (Network Access Point) de las Américas (El NAP es un punto de intercambio de servicios de telecomunicaciones, donde confluyen los cables submarinos más importantes de la región), que permitiría la conexión a otras redes de EEUU a una velocidades de 1.2 Gbps vía LANautilus (Latin American Nautilus U.S.A. Inc.), contando ya con la conexión a San Diego red CLARA se conecta a PW(Pacific Wave), el cual es un proyecto entre CENIC y PNWGP (Pacific Northwest Gigapop) esta es una infraestructura que permite conectar a las universidades y centros de investigación para compartir el backbone de las instituciones de educación e investigación de los países de la cuenca del pacífico y del mundo. De esta manera CLARA accede a PW a través de uno de sus tres nodos que se encuentran en los Ángeles California a una velocidad de 1 Gbps, con el apoyo de CENIT, ya que la conexión de CLARA sólo llegaba a San Diego y como se requería llevar la conexión de red CLARA hasta los Ángeles, para llegar a conectarse a PW y es ahí donde CENIT proporciona su infraestructura de fibra óptica y poder ser parte del intercambio de tráfico de capa2, que se realiza mediante VLAN locales entre las diferentes redes para luego intercambiar tráfico.

Una de las características con las que cuenta CLARA, al ser parte de la red PW, es que permite establecer acuerdo de intercambio de tráfico en un tiempo corto, configurando BGP (Border Gateway Protocolo) con varias redes que se encuentran en el punto de intercambio Los Angeles–PW [32].

En el 2006 se consolidó la organización de CLARA integrado por el NOC (Centro de Operaciones de la Red), NEG (Grupo de Ingeniería de RedCLARA), TEC (Comisión Técnica de CLARA). Los países que ya estaban conectados en ese año fueron México (PoP), Panamá (PoP), Chile (PoP), Argentina(PoP), Brasil (PoP), Venezuela, Uruguay (2005), EEUU (PoP), Guatemala, El Salvador, Nicaragua, Colombia, Ecuador y Perú. En la figura 2-2 se indica el backbone de la red CLARA, el cual contaba con un enlace de 1 Gbps de Brasil a Miami y una nueva conexión a la red Pacific Wave con una enlace de transmisión de 2.5 Gbps.

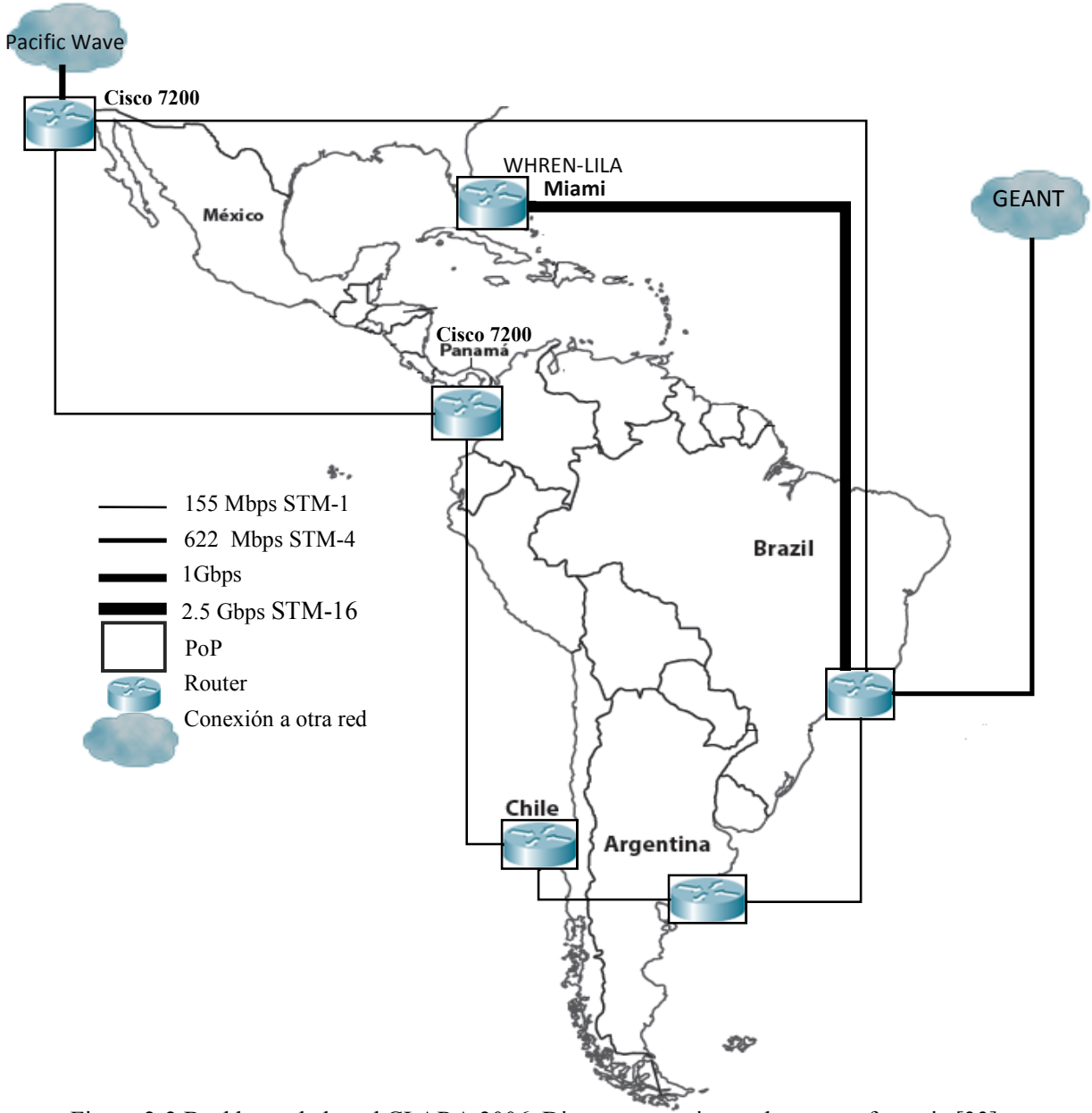


Figura 2-2 Backbone de la red CLARA 2006. Diagrama propio con base en referencia [33].

2.3 CLARA 2007-2009

Para el 2007 se presentaron cambios en la infraestructura del backbone de CLARA, en donde se agregó un nuevo nodo en el NAP de las Américas, en este nodo se instaló un enlace a Panamá, ya que lo que se pretendía era tener una conexión de Miami a Centro América que representaría el enlace principal de conexión entre Centroamérica y Sudamérica, permitiendo a provechar rutas más cortas y reduciendo costos en la operación, a este cambio se le sumaron las conexiones que se realizaron de Panamá a El salvador y Guatemala a una velocidad de 10 Mbps, también se eliminó el enlace directo de Sao Paulo Tijuana. El nuevo nodo que se implementó en Miami fue conectado al proyecto WHREN/LILA a través de una VPN, así el enlace de Miami que se conectaba a la red CLARA hasta Sao Paulo cerrarían el anillo del backbone con la interconexión de Argentina, Chile y Panamá. En el 2008 se realizó el cambio de la velocidad de conexión entre los enlaces de CEDI (Ecuador) de 10 Mbps a 16 Mbps, RENATA (Colombia) de 13 Mbps a 45 Mbps RAGIE (Guatemala) de 10 Mbps a 18 Mbps, a estos cambios del backbone se sumó la conexión del país de Costa Rica el 27 de Noviembre del mismo año con una velocidad de 155 Mbps. Además se incrementó la velocidad de de transmisión implementado un enlace de fibra óptica a una velocidad de 10 Gbps entre Argentina y Chile, con esto la topología de la red vuelve a tener cambios [34,35].

Para 2008 el backbone de Red CLARA contaba con nueve enrutadores principales, conectados en una topología punto a punto. Cada nodo principal representaba un punto de presencia (PoP) para la red. Ocho de ellos se localizaban en países de Latinoamerica: Sao Paulo (Brasil), Buenos Aires (Argentina), Santiago (Chile), Lima (Perú), Guayaquil (Ecuador), Bogotá (Colombia), Panamá (Panamá) y Tijuana (México). El noveno está en Miami (MIA – EEUU). Además de la conexión con la red paneuropea GANT2, y en EEUU con la red WHREN-LILA, como se indica en la figura 2-3.

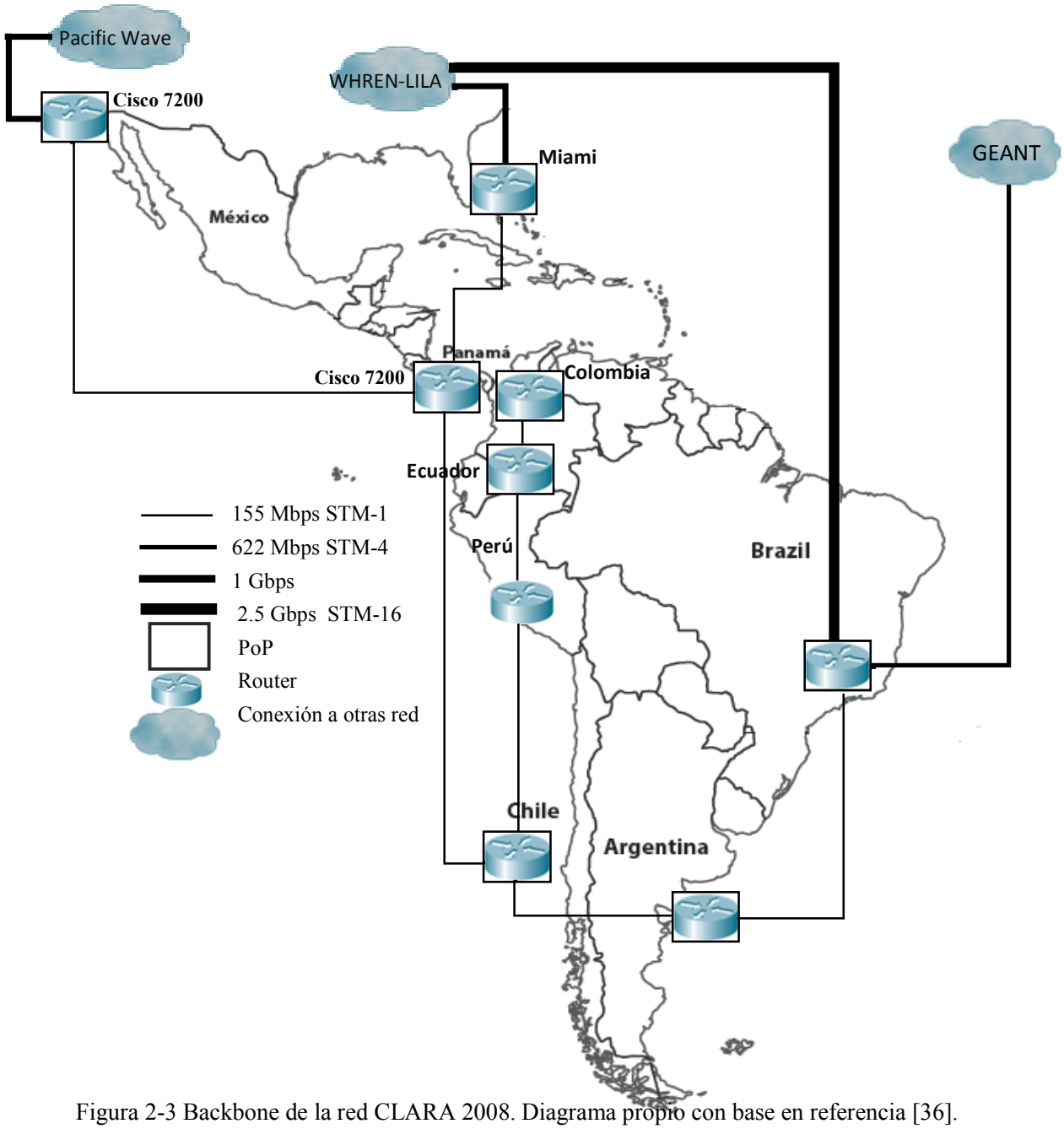


Figura 2-3 Backbone de la red CLARA 2008. Diagrama propio con base en referencia [36].

Para el 2009 la red continuó sumando países a la conexión de a la infraestructura de CLARA, así mismo la infraestructura de la red siguió evolucionando con la implementación del proyecto de ALICE2, que tenía como objetivo cambiar la infraestructura por una red completamente óptica, se inició el proyecto con un plan de trabajo, en el cual se describieron los cambios que se presentarían en el año 2010.

2.4 CLARA2

CLARA2 es la evolución de la infraestructura de red a una completamente óptica, en la cual se incrementó la tasa de transmisión, los servicios a nivel de circuitos virtuales en capa 2 y no solamente a nivel IP y la implementación de fibra óptica a través de todos los enlaces de backbone. El proyecto inició en el 2010 con la implementación del primer enlace de fibra óptica de 10 Gbps entre Santiago (Chile) y Buenos Aire (Argentina).

Para el 2011 el backbone de CLARA seguió incrementando su capacidad al implementar nuevos enlaces y al aumentar su ancho de banda, con la implementación del enlace de respaldo de 1 Gbps de Argentina a Chile, la actualización del enlace de Miami a Panamá de 155 Mbps a 1 Gbps, con otro enlace STM-4 de Chile a Panamá, posteriormente se implementaron los enlaces entre Chile-Brasil y Panamá, con la actualización del enlace de 155 Mbps a 622 Mbps de Ecuador a Perú, Colombia a Venezuela y Panamá, estos cambios fueron el inicio de la evolución del backbone de la red CLARA a red CLARA2 .

En la figura 2-4 se indica el backbone con las nuevas implementaciones de fibra óptica, así como los enlaces que se actualizaron que permitieron aumentar la capacidad del backbone de la red CLARA en el año 2011, la fibra óptica de mayor capacidad en cuanto a velocidad de transmisión se refiere, se encuentra entre el nodo de Chile y Argentina y los otros enlace de fibra óptica de 1 Gbps se encuentran entre los nodos de Panamá a el nodo de Miami, de Miami a Brasil y de México a Pacific Wave.

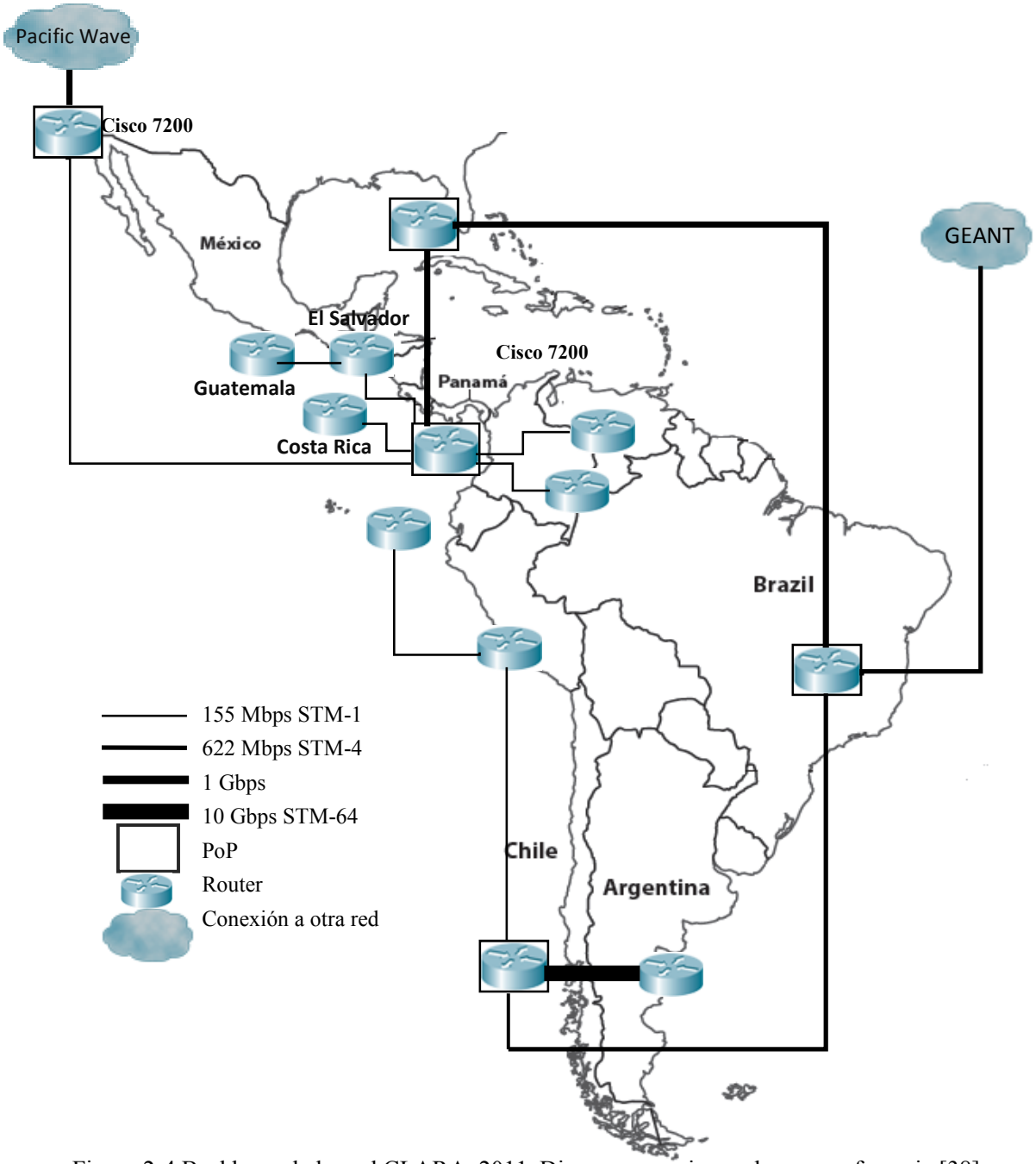


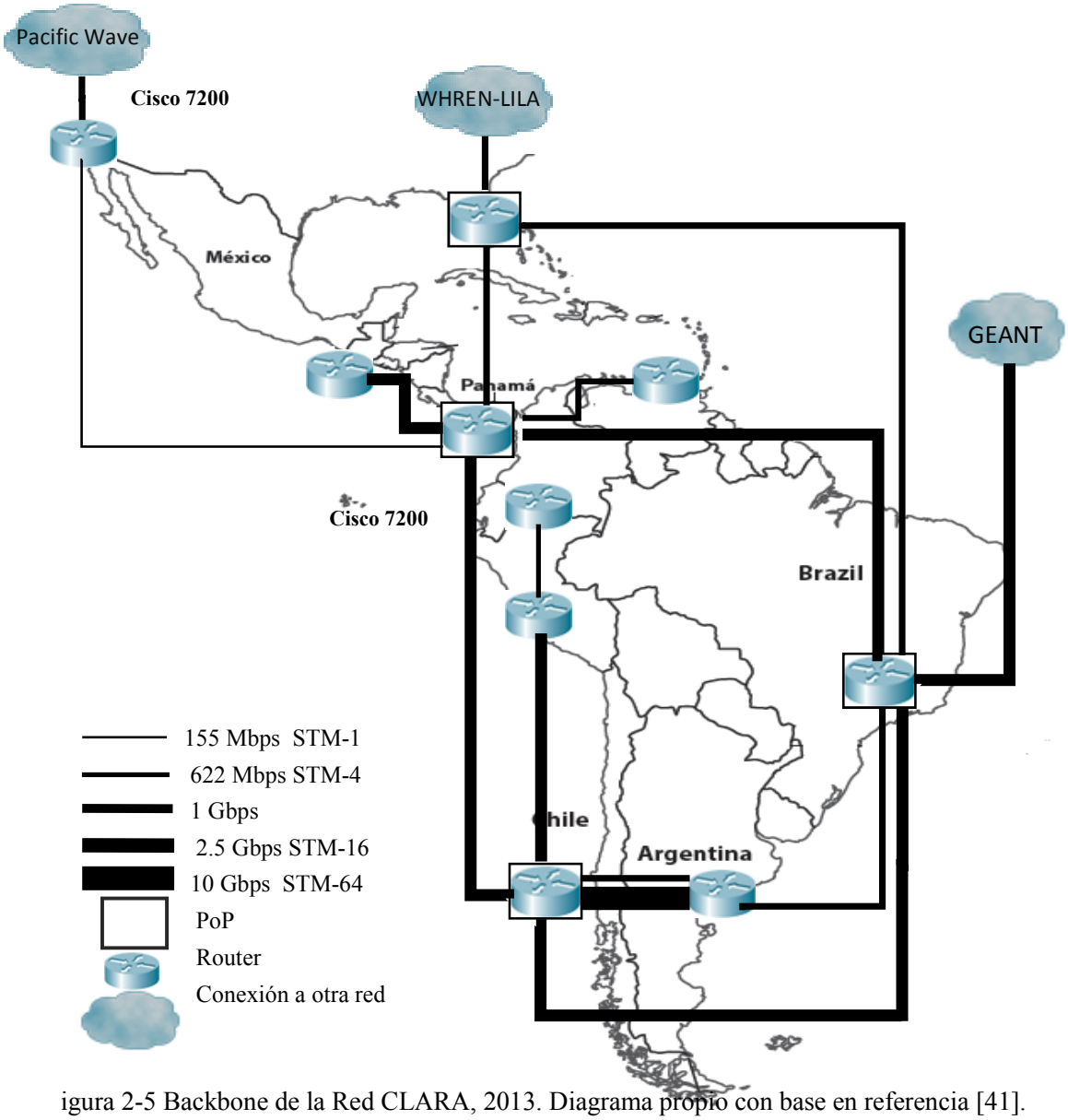
Figura 2-4 Backbone de la red CLARA 2011. Diagrama propio con base en referencia [38].

Para el año 2012 la infraestructura de la red sufrió otros cambios, debido al avance tecnológico en su topología, al continuar con el proyecto de la expansión de la fibra óptica terrestre para aumentar el ancho de banda, lo cual marcaría una evolución importante de CLARA, para la investigación, innovación y la

educación en Latinoamérica, implementado una enlace de 2.5 Gbps a GEANT, que anteriormente su velocidad de transmisión era de 622 Mbps, también la transmisión de información en el enlace a C@ribNet con tecnología Ethernet a 45 Mbps teniendo comunicación con la red Avanzada del Caribe.[39].

También se realizó la primera implementación del enlace de fibra óptica de San José(Costa Rica) y la Ciudad de Panamá (Panamá) a una velocidad de 1 Gbps y un enlace de 1 Gbps Ethernet entre San Salvador (El Salvador) y San José (Costa Rica), dejando un nodo en Nicaragua para su futura conexión con CLARA, en el 2013 se finalizó el cierre de la red óptica con el establecimiento de dos enlaces, uno a 10 Gbps entre Buenos Aires (Argentina) y Porto Alegre (Brasil), y uno a 2.5 Gbps entre Lima (Perú) y Antofagasta (Chile) [39].

Así, para 2013, la red CLARA, estaba formada por 13 países: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Panamá, Perú, Uruguay, Venezuela y se pretendía que en los próximos años se sumaran los países de: Bolivia, Cuba, Honduras, Nicaragua y de Paraguay. El backbone de la red CLARA lo integraban diez nodos ruteadores principales, conectados en una topología punto-a-punto. Cada nodo principal (IP - Protocolo Internet) representa a un PoP (Punto de Presencia) para RedCLARA, nueve de ellos están ubicados en un país de América Latina Sao Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Bogotá (BOG - Colombia), Panamá (PTY - Panamá), San Salvador (El Salvador) y Tijuana (TIJ - México) y el décimo, en Miami (MIA - Estados Unidos), como se indica en la figura 2-5 [40].



igura 2-5 Backbone de la Red CLARA, 2013. Diagrama propio con base en referencia [41].

A nivel de capacidad, RedCLARA tiene una infraestructura entre los nodos de Latinoamérica mencionados, en la modalidad de IRU (Irrestrictible Right of Use) a 10 o 15 años. En este modelo RedCLARA tiene fibra oscura (Fibra óptica que no está iluminada para transmitir información) 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 una velocidad de transmisión de 10 Gbps entre Buenos Aires (Argentina) y Porto Alegre (Brasil). [39]

Cuando una RNIE (Redes Nacionales de Investigación y Educación) latinoamericana hace conexión con RedCLARA, 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 RedCLARA, otorgándoles un Punto de Intercambio [40].

A continuación se presenta la figura 2-6, en donde se indica la evolución que ha tenido la red CLARA desde su implementación en el 2003 hasta el 2013, respecto a las diferentes velocidades de los enlaces. Los años más significativos de su evolución fueron del 2011 al 2013, ya que se alcanzaron velocidades mayores a 1 Gbps.

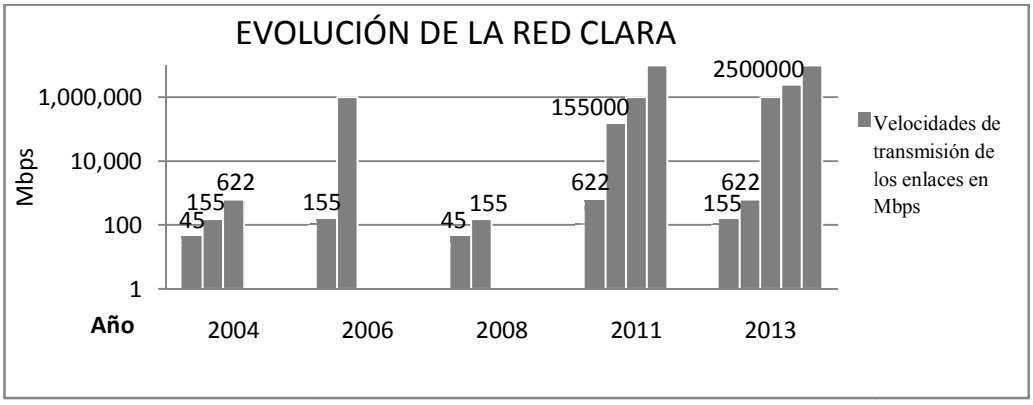


Figura 2-6 Evolución de la velocidad de los enlaces CLARA del 2004 al 20013. Gráfica propia con base en referencias [31,32,35].

La red CLARA proporciona servicios para la creación y el apoyo a las comunidades de investigación latinoamericanas, estos permiten a las comunidades comunicarse, compartir información, encontrar socios en otros países, recibir alertas de fondos de financiamiento, entre otros. Todos, servicios orientados a fortalecer la educación y la investigación. Los servicios de la red CLARA al año 2013, se indican en la tabla 2-1.

SERVICIOS DE LA RED CLARA
Multicast IPV4 y Multicast IPv6
Disponibilidad de Ancho de Banda
Mediciones
Servicios específicos para proyectos: Grids (Mallas Computacionales) y otro
Portal de servicios para las comunidades de investigación como: entorno social para comunidades, videoconferencias de escritorio(VC Espresso), Wikis, alertas de fondos de investigación, entre otros

Tabla 2-1 Servicios de la red CLARA [40].

La red CLARA cuenta con soporte de ingeniería, el cual permite administrar el backbone de la red a través del NOC, así como los grupos de sistemas de Ingenieros y el grupo de ingenieros de red, los cuales se encargan las actividades de la infraestructura del backbone de CLARA, como se indica en la tabla 2-2.

CARACTERÍSTICAS DE INGENIERIA DE TRÁFICO Y OPERACIÓN DE LA RED CLARA
Red CLARA posee una infraestructura con múltiples caminos a las redes internacionales, para lo cual se ha desarrollado una ingeniería de red para la selección de la ruta óptima, usando protocolos de IGP (Interior Gateway Protocol) y EGP (Exterior Gateway Protocol).
El NOC (Network Operations Center) se encuentra ubicado en Santiago de Chile y ofrece servicios de mantenimiento correctivo en la modalidad 7x24.
Existen, adicionalmente, dos áreas de ingeniería y una de soporte a servicios. Las areas mencionadas son: El SEG (Systems Engineering Group), Network Engineering Group y el VNOC (Videoconference Network Operations Center).

Tabla 2-2 Características de la red CLARA [40].

En la figura 2-7 se indica el bacckbone de la red clara con las conexiones de las diferentes redes nacionales de investigación y educación de los diferentes países conectados de Latinoamérica.

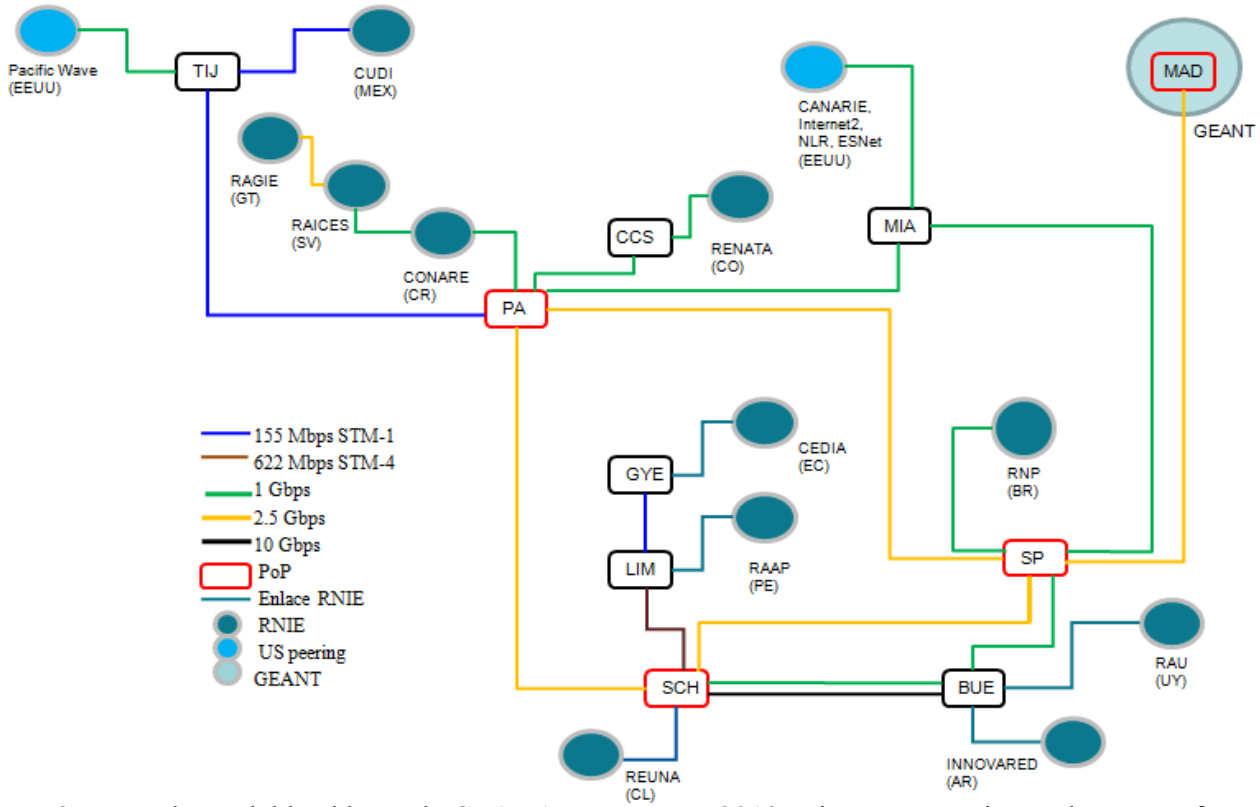


Figura 2-7 Topología del backbone de CLARA con NREN, 2013, Diagrama propio con base en referencia [39, 41].

CAPÍTULO III PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de ruteo determinan las mejores rutas, para transmitir los datos enviados de una red a otra, su tabla de ruteo es calculada a través de los algoritmos de ruteo, dependiendo del protocolo que se utilice el algoritmo puede ser Bellman-Ford o Dijkstra, que realizan los cálculos para obtener las mejores rutas, los protocolos hacen uso del costo como métrica, esta utiliza parámetros como el ancho de banda del enlaces, tipo de enlaces, dependiendo del protocolo que se esté utilizando son los parámetros que se consideran para el cálculo del costo. Los protocolos de ruteo, se clasifican en IGP que a su vez se subdividen en vector-distancia, los cuales son RIP (Routing Information Protocol) V1, RIP V2, IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) y en Estado-Enlace que son OSPF e IS-IS (Intermediate System to Intermediate System), otra clasificación es EGP dentro de esta se encuentra el protocolo BGP que es utilizando para el enrutamiento de paquetes entre los sistemas autónomos. En este capítulo se realiza una revisión general de los protocolo IRP, RIPV2, IGRP, EIGRP, IS-IS, BGP y profundizando más en el protocolo OSPF, que es el que se configura, para realizar el análisis del presente documento..

3.1 Enrutamiento

El enrutamiento de paquetes, se refiere al envió de paquetes de un dispositivo de red a otro dispositivo en una red diferente, este envió de información se realiza a través de los routers que estarán conectados en la infraestructura, para que permitan la interconexión de las diferentes redes. Para poder enviar paquetes, los dispositivos tendrán que conocen la dirección destino, los routers vecinos a partir de los cuales se puede aprender la mejor ruta para cada red remota, mantener y verificar la información de enrutamiento.

El router aprende sobre las redes remotas de los routers vecinos, construyendo una tabla de enrutamiento que describe cómo encontrar las redes remotas. Si la red está conectada directamente, el router

sabrá cómo llegar a la red, de lo contrario el router deberá saber cómo llegar a la red remota, ya sea con enrutamiento estático o dinámico [42].

a) Enrutamiento estático.

   La configuración de las rutas en la tabla se realiza de forma manual, esto puede tener algunas ventajas, lo cual reduce el uso del ancho de banda, ya que no se actualiza su tabla periódicamente, pero una de sus desventajas es que si se tienen muchos routers, se tendrían que configurar cada uno de ellos manualmente y se perdería mucho tiempo, si un enlace dejara de funcionar, se tendrían que configurar nuevamente los routers afectados por el enlace manualmente [42].

b) Enrutamiento dinámico.

   La configuración de las rutas en las tablas de ruteo del router se hace de forma automática, pero una de sus ventajas es que no se tienen que actualizar las rutas de forma manual a través de todos los routers de la red. La desventaja es que como se requiere que se realicen las actualizaciones de forma automática se tendía que enviar paquetes de actualización constantemente. Para validar el estado de las rutas y si se presentará algún cambio en la topología de la red, se realizaría la actualización de forma dinámica, esto llevaría hacer uso de más ancho de banda a través de todos los enlaces de la red [42].

Los protocolos de enrutamiento dinámico, permiten a los routers anunciar y aprender dinámicamente las rutas, determinan qué rutas están disponibles, actualizan las tablas de enrutamiento de forma automática cuando cambia la topología, determinan cual es la mejor ruta a un destino. Dentro de sus objetivos esta descubrir redes remotas y mantener la información de enrutamiento actualizada seleccionando la mejor ruta a las redes de destino, estos protocolos cuentan con un algoritmo de ruteo, que determinan la parte lógica, a través de un conjunto de pasos finitos que se ejecutan de manera ordenando, para calcular la mejor ruta entre

la red, así como realizar todos los cálculos necesarios para obtener las métricas. Los algoritmos más empleados en el enrutamiento de redes de datos son Bellman-Ford y Dijkstra. Si se desea mayor información acerca de los algoritmos de enrutamientos consultar el apéndice A.

3.2 Protocolos IGP

Los protocolos de enrutamiento internos, son los que se utilizan para determinar la rutas óptimas, dentro de una red de una misma organización o que actúan en un AS (Autonomous System) que es un conjunto de routers que intercambia información de redes mediante un protocolo de enrutamiento común y que generalmente son administrados por una misma entidad. Los protocolos internos son: RIP V1, RIP V2, IGRP EIGRP, OSPF IS-IS [48].

3.2.1 Vector-distancia

Los protocolos internos se pueden clasificar en vectores de distancia y de estado de enlaces, los de vector de distancia utilizan el algoritmo Bellman-Ford, mediante el cual se calcula la mejor ruta a través de toda la topología de la red, este cálculo lo realiza asignándole un costo o métrica al enlace entre dos routers, basando en el número de saltos [48].

El primer protocolo de vector de distancia fue implementado por la compañía Xerox en su protocolo GIP (Gateway Information Protocol) dentro de la arquitectura XNS (Xerox Network System). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos, más tarde la Universidad de California en Berkeley creó una variante llamada “routed”, tenía como modificaciones el campo de direccionamiento más flexible, así como un temporizador de 30s, para limitar el tiempo máximo de actualización. El GIP se integró a UNIX con la finalidad de que pudiera ser portable [49].

3.2.1.1 RIP V1

El protocolo RIP que fue desarrollado en 1988 utiliza el algoritmo Bellman-Ford, para el cálculo de sus rutas, el cual ha sido utilizado para los cálculos de enrutamiento en redes de computadoras desde los primeros días de la ARPANET, fue utilizado durante mucho tiempo desde su desarrollo, en sus diferentes variantes. El protocolo RIP está basado en los algoritmos utilizados por ARPANET desde el año 1969 [48].

RIP es útil para trabajar en redes pequeñas, en redes donde no se tengan que dar más de 15 saltos entre los routers, por lo que es inadecuado para grandes redes, ya que cuando el valor es mayor a 15, el protocolo establece en su costo o métrica de valor 16, que determina que la ruta es inalcanzable, por lo que se define como un protocolo de ruteo interior. RIP permite realizar actualizaciones de la tabla de rutas cada 30 s y si durante 180 s no se ha recibido actualizaciones, el protocolo determina esa ruta como inalcanzable. El tiempo de eliminación, el cual se refiere a que después de 300 s se eliminan todas las rutas inalcanzables cuyo costo sea de 16 en la tabla de ruteo [48].

RIP es un protocolo basado en UDP (User Datagram Protocol**)**. Cada host que utiliza RIP tiene un proceso de enrutamiento que envía y recibe datagramas en el puerto UDP 520. Las consultas específicas y solicitudes de depuración pueden ser enviados desde puertos que no sean 520, pero que se dirigen al puerto 520 de la máquina de destino [48].

El mensaje del protocolo RIP V1 contiene una serie de campos, en los cuales se establecen diferentes parámetros, para identificar el tipo de mensaje que se está enviando, el campo *command* que identifica el tipo de mensaje puede tener el parámetro 1 para solicitud y 2 para respuesta. EL campo *version*, se refiere a la versión del protocolo que se está utilizando, 1 para versión 1 y 2 para versión 2. El campo *IP Address Family of net 1* se establece el valor 2 para solicitar una dirección IP y 0 para solicitar una tabla de ruteo. *El campo IP*

address es la dirección del router destino. El campo *Hop Distance Metric* guarda el número de saltos entre 1 y 16. En la figura 3-1 se indican los diferentes campos del mensaje RIPV1 [48].

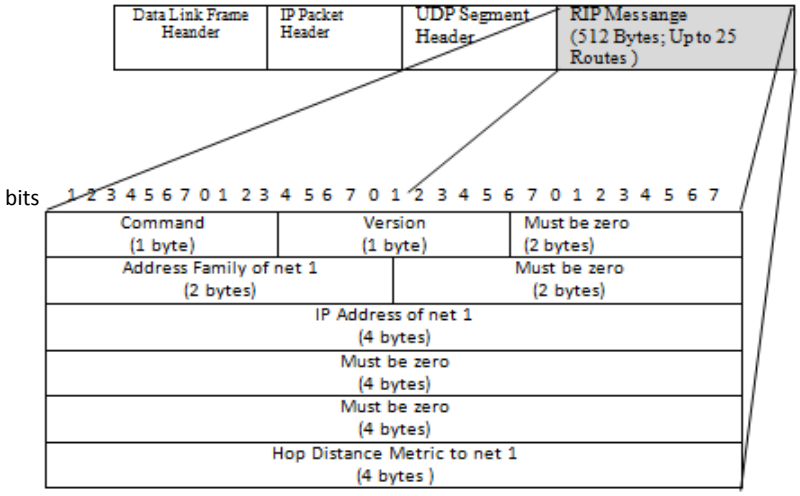


Figura 3-1 Formato de mensaje del Protocolo RIP V1 [45].

El algoritmo RIP V1 es un protocolo *Classfull* o con clase, esto se refiere a que no envía la máscara de subred durante las actualizaciones de enrutamiento, sólo la dirección de red, por lo que todos los routers de la red deberán de tener la misma submáscara de red. Cuando un router envía una actualización sólo recibe la dirección de red y con esta información se determina a qué clase de red pertenece. Puede ser alguna de las clases A 1.XXX.XXX.XXX - 126.XXX.XXX.XXX, B 128.001.XXX.XXX - 191.254.XXX.XXX y C 192.000.001.XXX – 223.255.255.XXX [48].

3.2.1.2 RIP V2

La versión 2 del Protocolo RIP, se publicó en noviembre de 1998 por G. Malkin, la cual establece una serie extensiones, que permiteron mejorar al protocolo, ya que en la versión 1 no se contaba con autenticación, ni se podía trabajar con topologías de red que tuvieran diferentes máscara de subredes. Entonces aprovechando el espacio de almacenamiento de información en el formato del mensaje RIP V1, se anexaron

algunos campos que permitieron mejorar el protocolo y modificar el nuevo formato del mensaje del protocolo RIP V2, como se indica en la figura 3-2 [51].

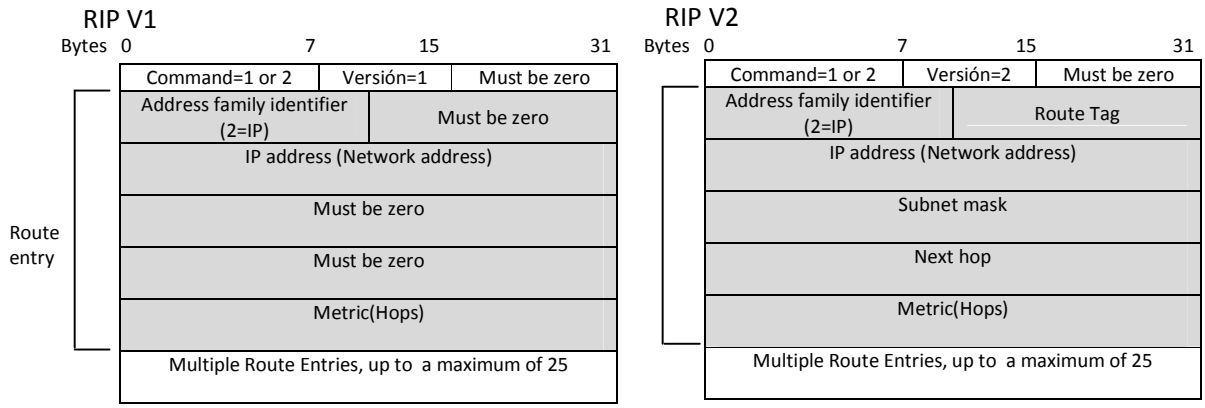


Figura 3-2 Diferencia de campos de los protocolos RIP V1 Y RIPV2. Con base en referencia [52].

Las extensiones que se agregaron a la versión 2 del protocolo RIP, para mejorar el funcionamiento del protocolo son las siguientes: [51].

a) *Autentication.* Este campo que se agregó a la nueva versión de RIP, permite agregar seguridad durante la transmisión de mensajes entre los routers, ya que estarán protegidos por una contraseña en ambos dispositivos al enviar o recibir paquetes, actualmente el único tipo de autenticación es una contraseña y es de tipo 2, si no hay autenticación en el mensaje el campo *Address Family Identifier* el parámetro de 0XFFFF de lo contrario se anexará al mensaje un formato de autenticación con una conjunto de parámetros.
b) *Route Tag*. La etiqueta de la ruta de campo (RT) es un atributo asignado a una ruta que debe preservarse. El uso previsto de la etiqueta de ruta es proporcionar un método de separación de RIP "interna" (rutas para las redes en el dominio de enrutamiento RIP) y de rutas RIP "externos", que pueden haber sido importados de un EGP u otro IGP.

c) *Subnet Mask*. El campo *Máscara de subred* contiene la máscara de subred que se aplica a la dirección IP para obtener la porción no host de la dirección. Si este campo es cero, entonces no hay una máscara de subred.

d) *Next Hop*. La dirección IP del siguiente router al cual se le enviará la información, para que pueda llegar al host destino.

e) *Multicasting*. Con el fin de reducir la carga innecesaria en los host que no escuchan los mensajes RIP-2, una dirección de multidifusión IP se utiliza para transmisiones periódicas. La dirección de multidifusión IP es 224.0.0.9.

f) *Queries*. Si un router RIP-2 recibe una solicitud RIP-1, se debe responder con una RIP-1 Response. Si el router está configurado para enviar sólo RIP-2 mensajes, no deben responder a una solicitud RIP-1.

3.2.1.3 IGRP

Otro protocolo de vector de distancia es el IGRP, que fue desarrollado a mediados de 1980 por Cisco System, que tenía como objetivo crear un protocolo robusto, con todas las características de un protocolo de vector de distancia, para que operara dentro de los AS este tipo de protocolos pertenece a los IGP [56].

En esta misma fecha el protocolo RIP era el protocolo más popular de ruteo utilizado dentro de las redes pequeñas y medianas de los AS. Aunque RIP era un protocolo utilizado por muchas redes en ese momento, ya estaba siendo sobrepasado por el crecimiento de las redes de los diferentes AS. Con el crecimiento de las redes se observó que una de las características que limitaba a RIP era su métrica por el número de saltos, ya que estaba limitado a no más de 15 saltos entre los router de la topología de la red. De esta manera se limitaba la conexión de más routers en la red; debido a esta limitación y en respuesta a las necesidades que requerían las redes en este momento Cisco System desarrolló IGRP; fue desarrollado en

consecuencia a las limitaciones que presentaba el protocolo RIP y a las necesidades que requerían los AS de un protocolo de ruteo interno [56].

El número máximo de saltos de IGRP es de 100 por defecto y 255 configurables, su distancia administrativa es de 100, utiliza una métrica compuesta que se calcula mediante la factorización de valores matemáticos ponderados por retardo de red, ancho de banda, fiabilidad y carga IGRP ofrece una amplia gama de sus indicadores. La fiabilidad y la carga, por ejemplo, pueden tomar cualquier valor entre 1 y 255. El ancho de banda puede tomar valores que reflejan velocidades desde 1200 bps hasta 10 Gbps, mientras que el parámetro de retardo puede tomar cualquier valor entre 1 y 224 [56].

Los parámetros que utiliza IRGP para calcular su métrica es el retardo que es la cantidad de tiempo que pasa cuando se envía un mensaje desde el origen hasta su destino a través de una ruta, suponiendo una red no cargada, el retardo se mide en décimas de microsegundos, el ancho de banda se calcula con la expresión $\frac{10^7}{BW}$, la fiabilidad que se refiere a la actual tasa de error es una fracción de los paquetes que llegan al destino sin error, así como a los enlaces que no han caído. La carga que es la ocupación del canal, nos indica cuánto del ancho de banda está actualmente en uso, sí en un enlace se está transmitiendo demasiada información, entonces la línea de transmisión estará cargada, el protocolo realizará el cálculo y lo guardará para verificar la línea y determinar otra que este menos cargada. [56].

La métrica se obtiene realizando el cálculo con la expresión 3-1.

$$Métrica = \left[K1 \cdot BW + \frac{K2 \cdot BW}{256 - load} + K3 \cdot delay \right] \bullet \left(\frac{K5}{reliability + K4} \right)$$

Expresión 3-1 Cálculo de la métrica del protocolo IGRP.[56].

Las variables K1,K2,K3,K4 y K5 se pueden modificar, el protocolo establece inicialmente los valores K1=K3=1 y K2=K4=K5=0, entonces tendremos la expresión reducida, como se indica en la ecuación 3-2.

$$\text{Métrica} = BW + delay$$

Expresión 3-2 Expresión reducida, por los valores iníciales que establece el protocolo IGRP.

Los tiempos o temporizadores que utilizan para realizar el control de las rutas actualizadas son: *Update* envía el contenido de la tabla de ruteo cada 90 s. *Invalid* la cual marca una ruta como inválida si no se obtiene un mensaje de actualización en 3x*Update*. El parámetro *Flush* elimina las rutas de las tablas marcadas con el parámetro *Invalid* cada 7x*Update*. El parámetro *Holddown* no acepta cambios de una ruta modificada en 3xUpdate más 10 [56].

3.2.1.4 EIGRP

EIGRP es un protocolo desarrollado por Cisco System que sólo se puede encontrar en los routers de la marca que desarrolló el protocolo, a principios de 1990 como una evolución y respuesta a las limitaciones que se presentaban en su protocolo antecesor el IGRP. Con la nueva versión se permitió tener un protocolo de enrutamiento escalable que permitiera el uso de VLSM (Variable Length Subnet Mask) y de CIRD (Classless Inter-Domain Routing), no envía actualizaciones periódicas, permite la autenticación con password o con MD5 (Message-Digest Algorithm) que es un algoritmo criptográfico de 128 bits, automatiza las redes y permite el balanceo de cargas con igual número de métricas, su dirección multicast es 224.0.010.

Las características del protocolo EIGRP son: Dualidad, redes de bucles, actualizaciones incrementales, direccionamiento de multicas para actualizaciones, protocolo vector de distancia avanzado, tabla de routing libres de bucles, soporte para diferentes tecnologías, convergencia rápida, utilización de ancho de banda reducido y configuración sencilla. EIGRP utiliza la métrica compuesta de ancho de banda retardo, confiabilidad y carga, pero los protocolos de ruteo sólo utilizan el retardo y el ancho de banda en forma predeterminada, para realizar el cálculo de la ruta más próxima, en cuanto al algoritmo que utiliza el protocolo

IGRP, sabemos que es Bellman-Ford, pero para la nueva versión Cisco implementó el protocolo DUAL (Algoritmo de Actualización por Difusion), el cual empezó a operar en los IOS versión 12.2 (13)T y 12.2 (R1S4) [58].

El Algoritmo DUAL opera de forma diferente al algoritmo utilizado por los protocolos de ruteo de vector de distancia que utilizan los protocolos RIP e IGRP, por lo que las actualizaciones se realizan constantemente en un intervalo de tiempo muy pequeño. Por otra parte DUAL no envía actualizaciones periódicas y las entradas de las rutas son válidas todo el tiempo a menos que se presente un problema con el enlace en la topología de la red. En cuyo caso, se enviará sólo la actualización con la información del enlace que esta inalcanzable y no toda la tabla con las diferentes rutas de la red, para la supervisión de los enlaces EIGR utiliza un protocolo liviano. Sólo los cambios en la información de enrutamiento, tales como un nuevo enlace o un enlace que ya no está disponible, producirán una actualización de enrutamiento [58].

El encabezado de paquete EIGRP contiene un conjunto de campos, algunos de los cuales tiene una longitud de 0 o 32 bits. Su estructura está formada por el encabezado, que contiene los campos *Versión*, C*ódigo de operación*, *Checksum*, *Señalización*, *Secuencia* y *ACK*, el mensaje EIGRP que está formado por los campos número de sistema autónomo y TLV como se indica en la Figura 3-3. A continuación se listan los diferentes campos del mensaje IGRP.

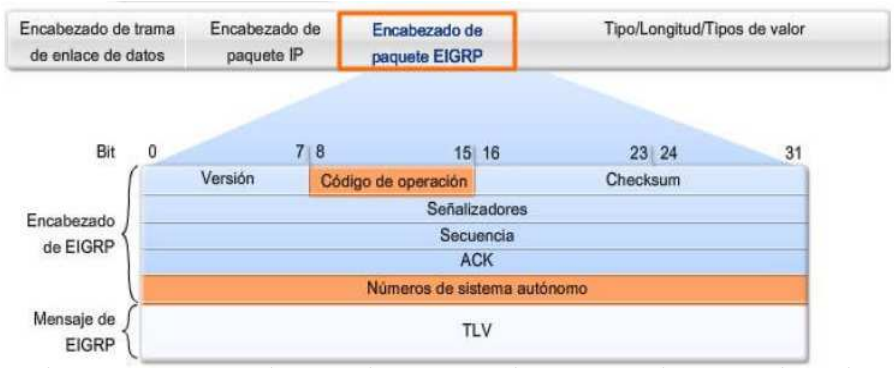


Figura 3-3 Formato de mensaje EIGRP. Diagrama con base en referencia [59].

a) Código de operación: Se refiere al tipo de mensaje que se está enviando, el protocolo EIGRP utilizan los mensajes actualización (1), consulta (3), repuesta (4) y saludo (5), para realizar sus diferentes operaciones de envió y recepción de información a lo largo de toda la topología de red [58].
b) Número de Sistema Autónomo: es el número, con el cual se identifica un proceso de enrutamiento EIGRP, a diferencia del protocolo RIP, este permite ejecutar diferente instancia de EIGRP en los routers de cisco. El número AS nos permite identificar diferentes procesos o instancias ejecutadas por el protocolo EIGRP.

3.2.2 Estado-enlace.

Los protocolos de estado-enlace, permiten mantener sus tablas de ruteo de forma libre de bucles, esta tabla también debe ser precisa. Este tipo de protocolos envían sus actualizaciones de forma periódicas, solamente cuando la red se está implementado por primera vez, o cuando se presenta un problema en uno de los enlaces y este deja de funcionar; las actualizaciones se envian a través de multicast. Estos tipos de protocolos mantienen en cada uno de sus routers el árbol completo de la topología de la red, con las rutas más próximas, requieren de un mayor recurso de CPU y de memoria. Estos son adecuados para ser usados en grandes redes, permiten realizar actualizaciones de tablas locales, estas se realizan en la tabla topológica, las cuales son modificadas por todas las actualizaciones que se van produciendo por la red [49].

Los protocolos de estado de enlace ejecutan el algoritmo Dijkstra, para obtener la tabla de ruteo actualizada, seleccionan la mejor ruta de acuerdo al cálculo de la métrica, el valor de la métrica viene especificado por el fabricante del router, pero se puede modificar. Los protocolos de estado-enlace son: OSPF (Open Shortest Path First) e IS-IS (Internal System Internal System) [49].

Una de las características de los protocolos estado-enlace que la diferencia de los protocolos de estado-distancia, es la forma en que mantienen registrada sus rutas. En los protocolos estado-distancia, la tabla de ruteo está formada por las rutas de cada uno de sus vecinos; mientras que los protocolos de estado-enlace, en cada uno de los routers, se tiene una tabla de ruteo con toda las rutas de la topología de la red, la cual se construye al formarse el árbol de la topología de la red [58].

3.2.2.1 OSPF (Open Shortest Path First)

El protocolo OSPF es un protocolo de ruteo de estado de enlace, el inicio de su desarrollo fue en 1987 por el grupo de trabajo de OSPF, el IETF (Grupo de trabajo de Ingeniería de Internet), para estas fechas Internet estaba formada por universidades y centros de investigación de EEUU, para 1989 se desarrolló la versión OSPFV1 del protocolo en el RFC 1131 para entonces ya se contaba con dos versiones diferentes, una para equipos *routers* y otra para estaciones de trabajo UNIX, esta última terminó siendo un proceso en los sistemas que ejecutaban UNIX, el cual fue conocido como GATED. La versión OSPV1 fue experimental ya que nunca se implementó. En 1991 se liberó la versión OSPFV2 por John Moy escrita en el RFC 1247, la cual presentaba mejoras a la primera versión, la actualización de la versión 2 se realizó en 1998 y se escribió en el RFC 2328, esta es la versión más reciente de OSPF para IPV4, ya que en 1999 se liberó una nueva versión OSPFV3, para trabajar con IPV6 en el RFC 2740 [49,60].

OSPF fue desarrollado para remplazar las limitaciones que presentaba el protocolo RIP. Durante los inicios del las redes y del Internet, era un protocolo de ruteo eficiente, pero a medida que fueron creciendo las redes, sus limitaciones en la cantidad de saltos que utilizaba como métrica para el cálculo de la ruta más corta, ya no era suficiente para mantenerse en grandes redes, es por eso que OSPF se desarrolló para trabajar de forma eficiente en las grades redes de datos, ya que como protocolo de estado de enlace, permite trabajar en

redes más grandes utilizando el concepto de área para realizar la escalabilidad, converge más rápido y utiliza el ancho de banda como métrica, para calcular la ruta más corta a diferencia del protocolo RIP [60].

Las principales características de OPSF son las siguientes:

- Protocolo de estado de enlace
- Enrutamiento sin clase
- Escalabilidad
- Ancho de banda como métrica
- Rápida convergencia
- Distancia administrativa de 110
- Contiene todas las rutas de la topología de la red en cada router

El formato de mensaje del protocolo OSPF se encapsula en el campo *Encabezado del paquete OSPF* y en el campo *Datos específicos del Tipo de Paquete OSPF* como se indica en la figura 3-4. En el primer campo permite identificar la cabecera del mensaje OSPF y en el segundo campo se almacenan parámetros de valores más concretos de la información que se va a enviar dentro del mensaje OSP [61].

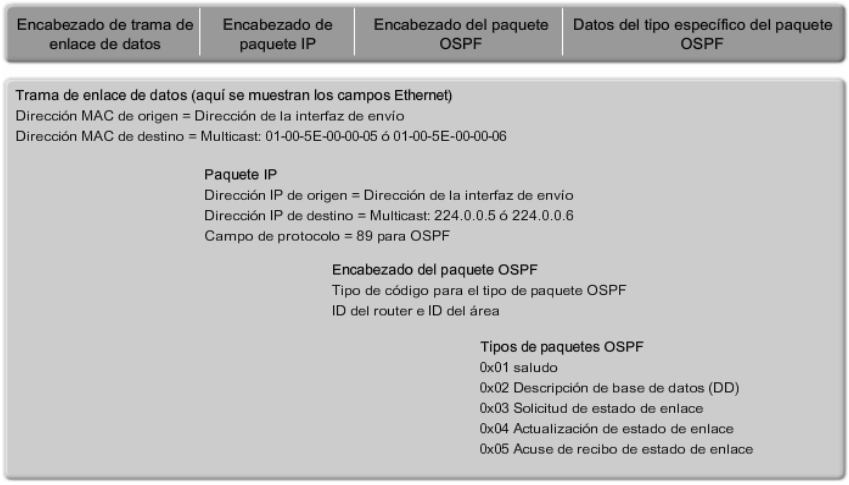


Figura 3-4 Mensaje OSPF encapsulado. Diagrama con base en referencia [61].

A diferencia de otros protocolos de ruteo que utilizan UDP o TCP para la transmisión de su mensaje, en el encabezado de paquete IP también se establecen los parámetros de *IP origen* y la dirección *IP destino*, que es una dirección multicast las cuales son 224.0.0.5 o 224.0.0.6 y en el campo de *Encabezado de trama de enlace de datos*, se almacenan los parámetros de *Dirección MAC (Media Access Control) de origen* y *Dirección MAC de destino multicast*, las cuales pueden ser 01-00-5E-00-00-05 o 01-00-5E-00-00-06, como se indica en la figura 3-4 [61].

El formato del mensaje OSPF se encuentra dividido en dos partes: Encabezado del paquete OSPF y Datos específicos del paquete OSPF, dentro de estos campos se encuentran los parámetros que conforman al mensaje OSPF como se indica en la figura 3-5.

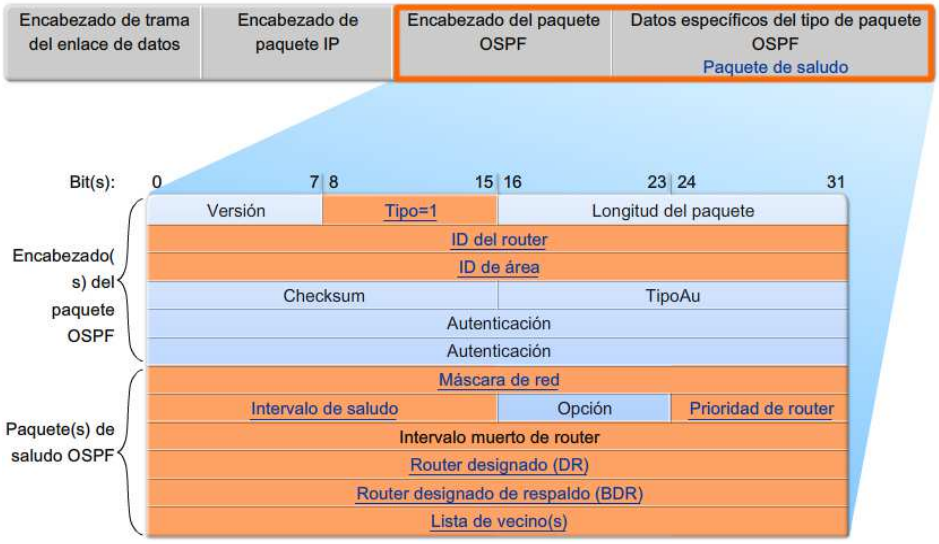


Figura 3-5 Formato del mensaje OSPF encapsulado en una trama. Diagrama con base en [61].

Los parámetros que contiene el encabezado del formato OSPF se describen a continuación, así como los del tipo de paquete. En la figura 3-5 se indican los parámetros del tipo de paquete corresponden al tipo de mensaje *hello*.

Los parámetros del encabezado del formato del mensaje OSPF son los siguientes:

Tipo de paquete OSPF: Pueden ser uno de los cinco diferentes paquetes que puede enviar el protocolo OSPF, cada mensaje está representado por un número que describe el tipo de mensaje.

ID del Router: Que es el identificador del router de origen.

ID del área: Se refiere al área en la que se originó el paquete.

Version: Versión del protocolo OSPF.

Longitud del paquete: Longitud del paquete OSPF incluyendo cabecera.

Checksum: Suma de comprobación de todo el paquete incluyendo OSPF incluyendo el campo de autentificación.

TipoAu: Tipo de autenticación utilizada.

Autenticacion: Es una campo que se utiliza para la seguridad entre los sistemas

Los parámetros del tipo de paquete OSPF (paquete de saludo) son los siguientes:

Máscara de red: Asociada a la interfaz emisora.

Intervalo de de saludo: Es la cantidad de segundos entre los paquetes de saludo del router emisor.

Prioridad del router: Utilizado en la elección de DR/BDR.

Router designado (DR): Es el ID del router DR.

Router designado de respaldo (BDR): Se refiere al ID del router BDR.

Lista de vecinos: Es una lista de los ID de los routers vecinos.

Opción: Utilizado en rede que no son de multiaccesos. Dead = 120 y Hello= 30s

OSPF utiliza 5 tipos diferentes de mensajes para su operación y mantenimiento de los estados de enlace, estos son los siguientes: [49].

1. Hello: Se utilizan para establecer y mantener la adyacencia con otros routers OSPF.
2. DBD (Database Description): Descripción de bases de datos o DDPs (Database Description Packets) incluye una lista abreviada de la base de datos de estado de enlace del router.
3. LSR (Link State Request): Solicitud para información específica.
4. LSU (Link-State Update): los paquetes de Actualización de estado de enlace se utilizan para responder las LSR y para anunciar nueva información con los LSA (Link-State Advertisement).
5. LSAck (Link-State Acknowledgement): Confirmar la recepción de LSU.

Los tipos de mensajes LSU son utilizados, para realizar las actualizaciones de enrutamiento OSPF, cada uno de estos mensajes puede contener diferentes tipos de notificaciones LSA.

Los routers sólo pueden intercambiar mensajes entre sus vecinos, si se establece una adyacencia, si los routers tienen el mismo valor de intervalo de saludo, intervalo muerto y tipo de red.

El intervalo de saludo que utiliza el protocolo OSPF, para controlar el envió de mensajes hello entre los routers de la red, se envía cada 10 segundos en redes de acceso múltiple y punto a punto y cada 30 segundos en redes NBMA (Non-Broadcast Multiple Access Network), Frame Relay, X.25 y ATM (Asynchronous Transfer Mode). Los mensajes hello generalmente son enviados a través de la dirección multicast 224.0.0.5.

El intervalo muerto es el periodo que el router esperará para recibir un paquete de saludo antes de declarar el vecino inalcanzable. Cisco utiliza como valor predeterminado cuatro veces el tiempo del mensaje hello, para las redes multiacceso con broadcast y punto a punto es de 40 s, para las redes multiacceso sin broadcast es de 120 s. Sí los dos routers tienen los mismos valores en los parámetros que les permite

establecer la adyacencia, estos pasan por una serie de estados en los que se ejecutan diferentes tipos de mensajes para la obtención de la información de todos los estados de enlace de la red para formar su base de datos.

Los diferentes tipos de estados son los siguientes:

1. *Down*: El proceso OSPF no ha empezado a intercambiar información con ningún vecino está esperando a entrar en el siguiente estado [61].

2. *Int*: Cuando una interfaz recibe su primer mensaje hello (1), entonces el router entra en estado Init.

3. *Two-Way*: El router entra en este estado, en el momento en que se ve en una de las actualizaciones de uno de sus vecinos.

4. *Exstart*: Cuando el router utiliza paquetes de tipo (2), estos se envían cuando se establece la relación maestro esclavo, el maestro será el que tenga el Router ID (IP) más alta y será quien empiece a transmitir datos, el esclavo quedará en espera de la recepción del mensaje enviado por el maestro.

5. *Exchange*: Cuando el router entra en este estado utiliza paquetes de tipo 2, para enviarle al otro router su información de estado de enlace (Dos vecinos descubren el mapa de la red).

6. *Loading*: Cuando se recibe un paquete de tipo 3 y responde con un tipo de paquete 4 que describe la información de estado de enlace.

7. *Completa*: cuando termina el estado loading, los routers están en una adyacencia completa. Cada router mantiene una lista de sus vecinos adyacentes, llamada base de datos de adyacencia.

En la figura 3-6 se indica los estados por los que pasa cada uno de los routers, en cado uno de los procesos en los que envían una serie de mensajes, desde el establecimiento de la adyacencia hasta la obtención de la información de los estados de enlaces, para crear su base de datos [49].

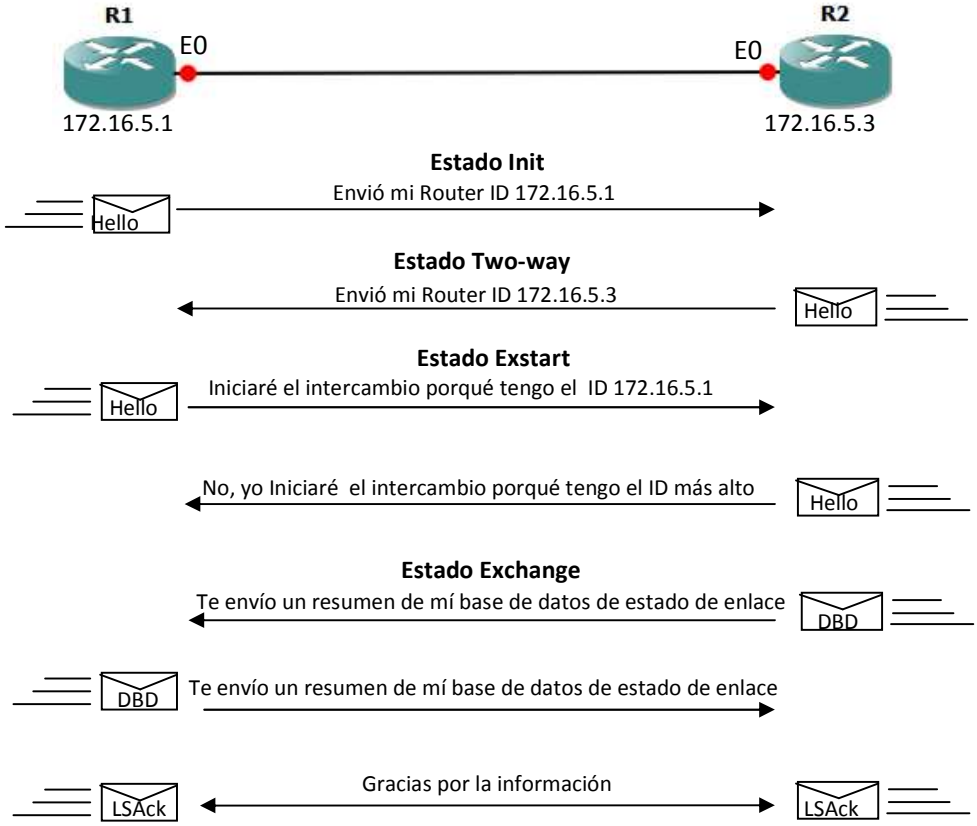


Figura 3-6 Descubrimiento de rutas entre los routers. Diagrama con base en referencia [49].

En la figura 3-7, se describen los estados entre los dos routers vecinos, cuando se solicita información detallada sobre una ruta, a través del mensaje LSU, el router con la dirección IP 172.16.5.3 envía un mensaje de respuesta LSU a la petición del router R1, para que finalmente el router R1 envié un mensaje ASAck al router R2.

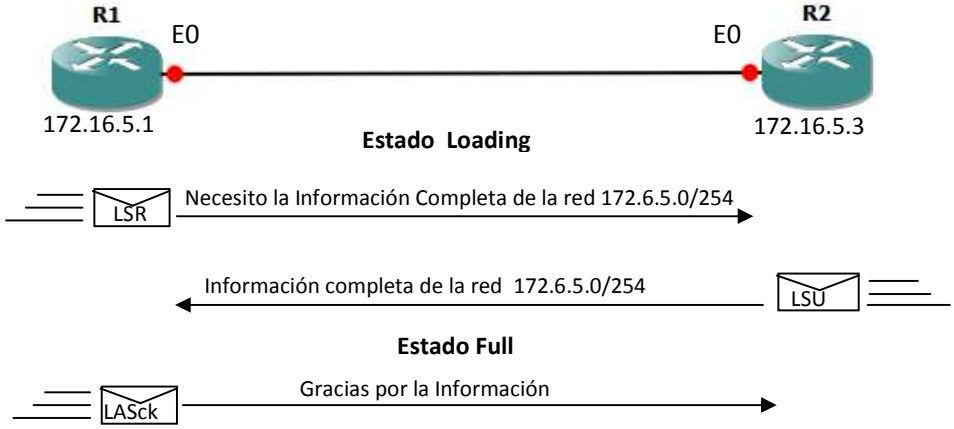


Figura 3-7 Solicitud de información específica entre dos routers. Diagrama con base en referencia [49].

El protocolo OSPF utiliza como métrica el costo y lo calcula con la expresión matemática 3-3, la cual es un cociente, de dividir 10^8 entre el ancho de banda del enlace. Se pueden tener diferentes enlaces en una red, con diferentes valores de anchos de banda, para un enlace con un ancho de banda de 128 Kbps, su valor de costo calculado será de 781, como se indica en la expresión 3-4.

$$\text{Costo} = \frac{10^8}{BW}$$

Expresión 3-3. Operación para el cálculo del costo. Cociente con base en referencia [61].

$$\text{Costo} = \frac{10^8}{128X10^3} \longrightarrow 781 \text{ serial } 128 \text{ kbps}$$

Expresión 3-4 Cálculo del costo para un enlace de 128 Kbps. Cociente con base en referencia [61].

El protocolo permitirá realizar balance de carga, con lo cual la información se enviará por los dos enlaces de transmisión, alternando el envió de la información por los dos enlaces.

Los anchos de banda para diferentes enlaces de red se indican en la tabla 3-3, se puede observar que el valor máximo de costo es de *Fast Ethernet*, por lo que si se tienen enlaces con un ancho de banda mayor en la topología de red, el protocolo establecerá el valor del costo en 1.

Tipo de interfaz	Asignación de costo
Fast Ethernet	10^8/100000000 bps → 1
Ethernet	10^8/10000000 bps → 10
E1	10^8/2048000 bps → 48
T1	10^8/1544000 bps → 64
128 Kbps	10^8/128000 bps → 781
64 Kbps	10^8/64000 bps → 1562
56 Kbps	10^8/56000 bps → 1785

Tabla 3-3. Cálculo de costo con diferentes enlaces. Tabla con base en referencia [61].

Si tenemos una topología de red en donde los *routers* están conectados punto a punto como se indica en el figura 3-8 en donde los enlaces tienen diferente valor de costo, en los enlaces que tienen diferentes anchos de banda, sí se desea calcular el costo desde el *router* R1 hasta la red 10.10.10.0/24, el protocolo calculará el costo sumando el valor de los enlaces que están entre el origen que es R1 y la red destino, para este ejemplo la suma del costo es de 65, como se muestra en el recuadro, en donde aparece el valor 110 que corresponde a la distancia administrativa seguido del costo acumulado.[61].

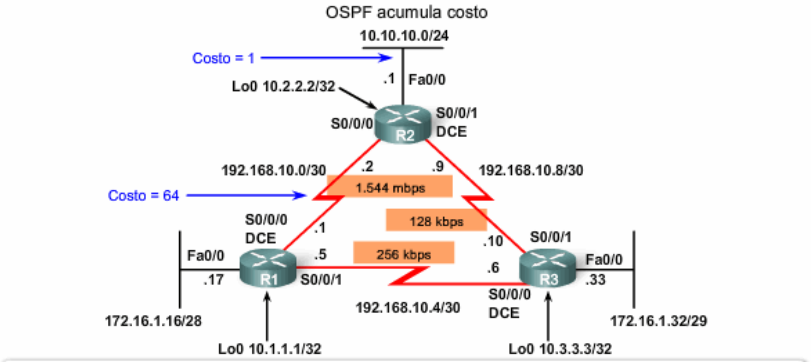
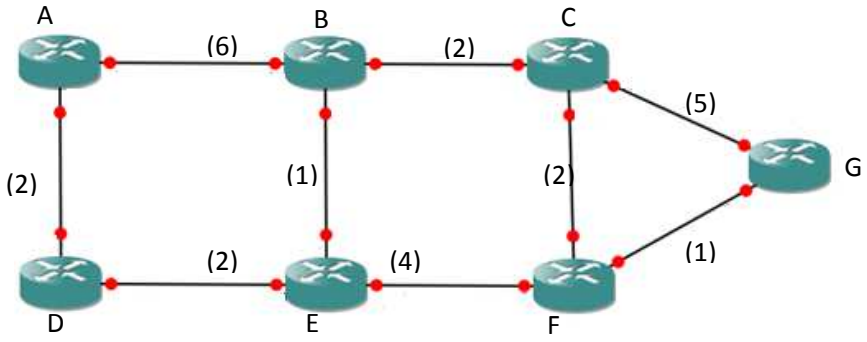


Figura 3-8 Costo acumulado del *router* R1 a la red 10.10.10.0. Diagrama con base en referencia [61].

Después de que los routers ejecutan el protocolo OSPF para obtiener los estados de los enlace de toda la topología y los almacene en una base de datos, se ejecuta el algoritmo Dijkstra conocido como SPF (Shortest Path First), el cual calcula el camino más corto en un grafo ponderado, este sólo funciona con grafos que no tienen pesos negativos a diferencia del algoritmo Bellman-Ford. Hace uso de la teoría de grafos, para poder realizar el cálculo de los costos menores, basado en el estado de enlace de las aristas, para poder determinar la ruta más corta [61].

En la figura 3-9 se indica una topología de red con el valor de costo en cada uno de sus enlaces, como por ejemplo el enlace que se encuentra conectado entre el router A y el router B, en donde su valor de costo es de (6). Cada uno de los router almacena los costos de los enlaces a los que se encuentra conectado directamente, por ejemplo el router B está conectado directamente a tres enlaces que tienen como valor de

costo (2), (1) y (6) [47].



A	B	C	D	E	F	G
B(6)	A(6)	B(2)	A(2)	B(1)	C(2)	C(5)
D(2)	C(2)	F(2)	E(2)	D(2)	E(4)	F(1)
	E(1)	G(2)	-	F(4)	G(1)	-

Figura 3-9 Costos de los enlaces en la topología de red. Diagrama propio con base en referencia [47].

Dijkstra construye un árbol topológico, con las rutas más cortas de la red en cada uno de los routers, para que el protocolo OSPF pueda generar la base de datos de ruteo. El algoritmo primero obtener los valores de costo de los enlaces a los que está conectado directamente, para el caso del router C se inicializa el árbol como se indica en la figura 3-10, posteriormente obtiene los costos que están conectados directamente a una de las ramas del árbol, como se indica en el árbol B), si los valores de costos que se agregan a las ramas, son menores a los que ya se tenían de un mismo router se elimina y se mantiene el enlace del router de menor costo como se indica en l árbol C) donde se eliminó el valor G (5), para que sólo quedara el valor G (3), finalmente el árbol topológico queda como el árbol D). Como se indica en la figura 3-10 [47].

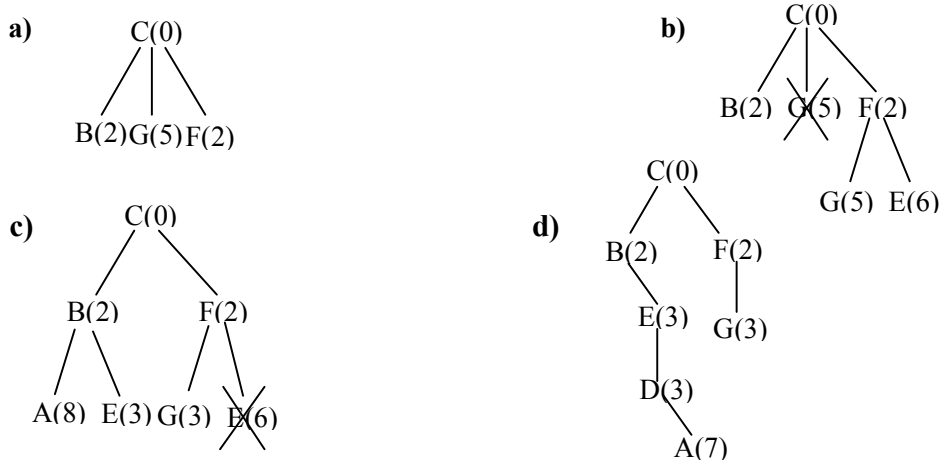


Figura 3-10 Construcción del árbol topológico, para encontrar la mejor ruta. Diagrama con base es referencia [47].

Después de generar el árbol OSPF, el protocolo genera la base de datos de ruteo, que tendrá las rutas más cortas de la topología de red, que fueron calculadas de acuerdo a su costo que realiza el cálculo considerando su ancho de banda de cada enlace de la red. En resumen el procedimiento para la generación de la mejor ruta se puede describir en cuatro procedimientos: Generación de la base de datos de los estados de enlace, ejecución del algoritmo Dijktra o SPF (Shortest Path Firs), generación de el árbol topológico y generación de la tabla de ruteo que se construye con los valores obtenidos de la base de datos topológica.

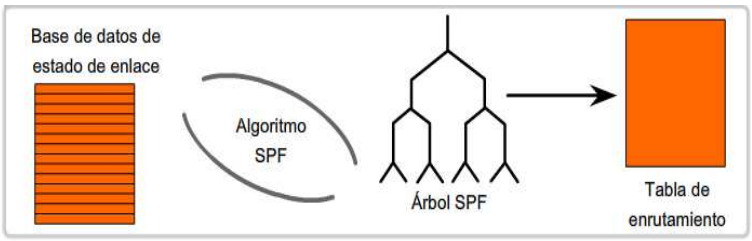
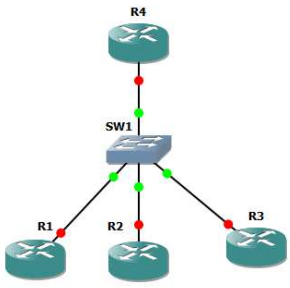
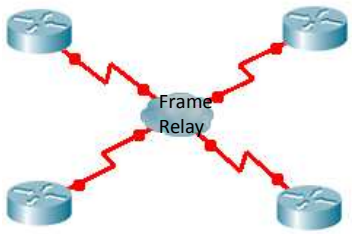


Figura 3-11 Procedimiento, para obtener la tabla de enrutamiento. Diagrama con base en referencia [61].

OSPF permite trabajar con diferentes tipologías de redes, las cuales pueden ser broadcast de acceso múltiple, punto a punto, punto a multipunto, NBMA y enlaces virtuales, como se indica en la figura 3-12.

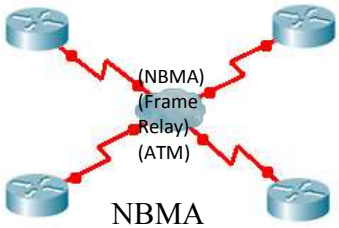


Broadcast de accesos múltiples.



Punto a multipunto.

Punto a punto



NBMA

3-12 Tipos de redes que define el protocolo OSPF. Diagrama con base en referencia [49].

Las cinco 5 topologías que define OSPF se describen a continuación:

a) Punto a punto: En esta configuración los routers se encuentran conectados físicamente a otros routers, un ejemplo de esta configuración podrían ser rouetrs conectados a través de un cable serial, como se indica en la figura 3-12.
b) Acceso Múltiple con Broadcast: Las redes Ethernet o FDDI **(**Fiber Distributed Data Interface**),** en el entorno de OSPF envía trafico de multicast, por lo que se establece un DR (Designated Router) y un BDR (Backup Designated Router).
c) Punto a multipunto: En esta configuración física de la topología, una interfaz se conecta a múltiple interfaces, no existe elección de DR y BDR
d) NBMA: requiere una configuración especial, ya que físicamente requiere enlaces punto a punto, de forma parcial o total mallada. OSPF envía un broadcast por cada uno de sus enlaces . Se requiere una configuración manual de DR, BDR y de los vecinos. El DR será el encargado de generar los LSAs para los nodos de la red.

e) Enlaces virtuales: es una conexión virtual al área remota que no tiene ninguna conexión con el área del backbone. OSPF tratará a estos enlaces como directamente conectados al área 0, ya que se crearán túneles a través del enlace virtual [49].

En la topología de Brodcast de acceso múltiple se presenta un problema de flooding, cuando todos los routers establecen sus adyacencias con sus vecinos, al estar conectados a sus enlaces físicos directamente, estos envían sus LSAs a cada uno de sus vecinos, lo que ocasiona que se saturen los enlaces y con esto el ancho de banda de cada uno se reduzca ocasionando problemas en la comunicación de los enlace de red y que el protocolo trabaje de forma ineficiente, ya que su principal característica de OSPF es calcular las mejores

rutas de la red considerando el mayor ancho de banda de los enlaces. En la figura 3-13 se puede observar las adyacencias que se establecen entre los routers de una topología de acceso múltiple con broadcast.

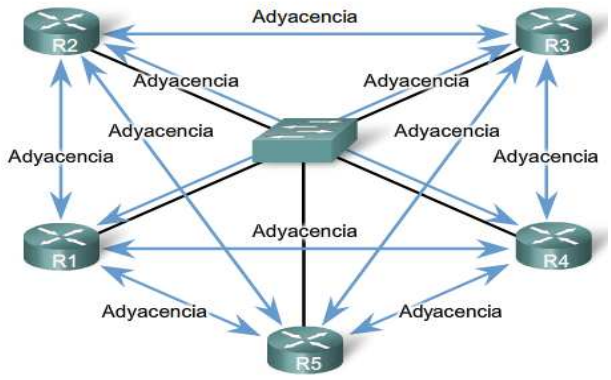


Figura 3-13 Adyacencia en una red broadcast de acceso múltiple. Diagrama con base en referencia [61].

En la figura 3-14 se indica cómo después de que se establece la adyacencia entre los router, envían cada uno sus mensajes a todos los routers, saturan los enlaces al iniciar el protocolo OSPF o cuando hay un cambio en la topología, se indica como el router R2 de la topología a) envía un mensaje LSA a todos los routes, en este caso no se presentan problemas, pero si todos envían sus mensajes LSA al mismo tiempo, se presenta tráfico de paquetes, saturando los anchos de banda de los enlaces de la red, como se indica en la topología b) [61].

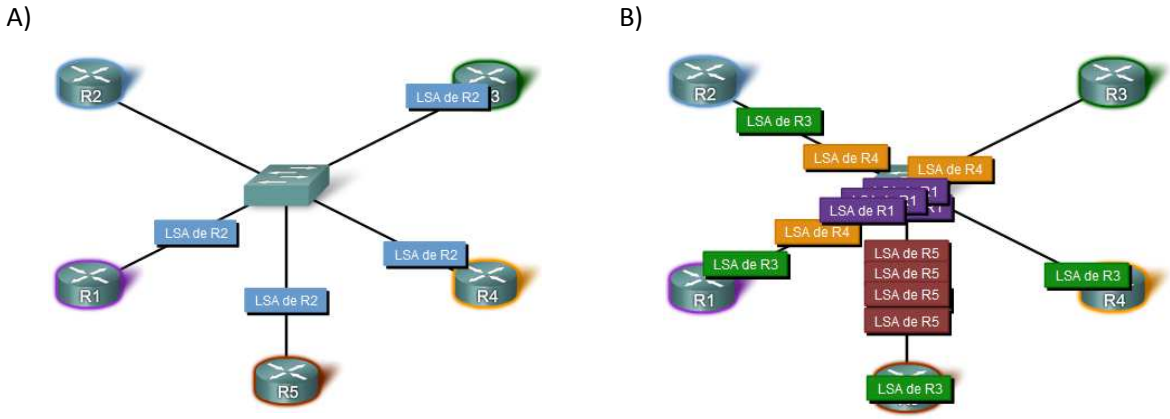


Figura 3-14 Saturación de los enlaces en una topología de broadcast de acceso múltiple. Diagrama con base en referencia [61].

Para solucionar el problema de flooding en las redes de acceso múltiple con broadcast, OSPF establece un router como DR el cual se encargará de la administración de los mensajes enviados por los demás routers de la red, se encargará de recibir los LSA de los routers y reenviarlos a todos los demás router de la red, atraves de la dirección 224.0.0.05 multicast.

El BDR es un router que será designado, como de respaldo si llegar a fallar el router DR, el BDR tomará el control y se establecerá como DR, realizando todas las funciones del Designated Router, recibe mensajes del DR y de los Drothers.

Los Drothers son los router que configura OSPF, los cuales sólo enviaran mensajes LSA al DR y al BDR, a través de la dirección multicast 224.0.0.6.

En la figura 3-15 se indica una topología en donde se encuentra configurado por el protocolo OSPF un router DR, uno como BDR y tres routers como drother. En la topología A se envía un mensaje LSA, el cual puede contener información de sus estados de enlace, para propagarlos a través de los demás routers de la red, el envió se hace del R1 al DR y al BDR como se puede ver, después de recibir el LSA el RB lo reenvía a través de su dirección boradcas 224.0.0.5 a todos los routers de la topología y es recibido por los Drother, como se indica en la topologíab B).

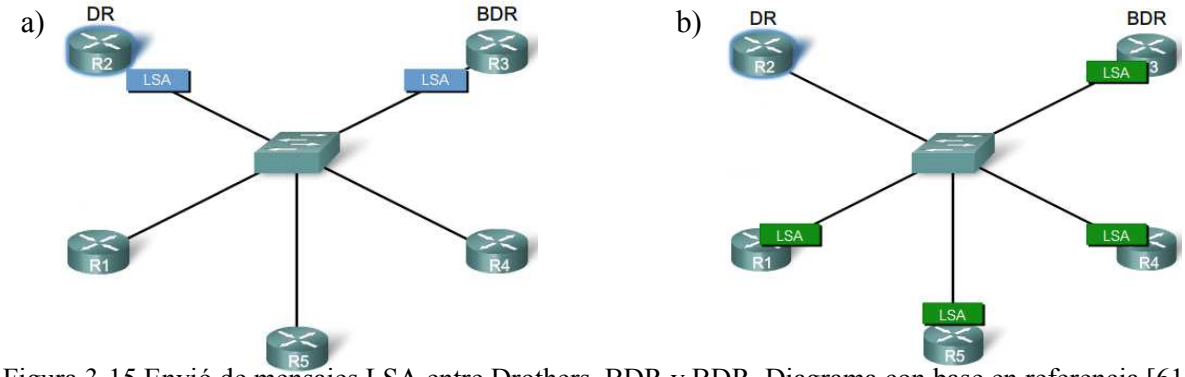


Figura 3-15 Envió de mensajes LSA entre Drothers, BDR y BDR. Diagrama con base en referencia [61].

OSPF determinar el router DR y BDR, de a cuerdo a la siguiente lista de consideraciones:

1. DR: Router con la prioridad más alta de interfaz OSPF.

2. BDR: Router con la segunda prioridad más alta de interfaz OSPF.

3. Si las prioridades de la interfaz OSPF son iguales, la ID del router más alta se utiliza para desempatar.

Los drothers se determinan estableciendo su prioridad en 0

3.2.2.1.1 Multi-Área

En los inicios del protocolo OSPF, las redes donde se implementaba no eran tan grandes, a través de los años el número de equipos fue incrementado, así como las redes de datos, esto permitió que se definieran nuevas configuraciones en la topologías lógicas y físicas donde se implementaría el protocolo OSPF, las nuevas definiciones asignadas a los dispositivos de red y a las configuraciones lógicas del protocolo, permitieron que el protocolo trabajara de una manera más eficiente al reducir el número de equipos en la red a 50 equipos máximo, al dividir las red de un AS en áreas, en las cuales los routers no deberían de estar conectados a más de 3 áreas, con estas mejoras se reduce el tráfico en la red, la cantidad de procesamiento y el uso de memoria en cada uno de los routers, ya que si se tiene una base de datos topológica muy grande, se requerirá de una mayor procesamiento y un mayor uso de memoria, lo que haría más lento el funcionamiento del protocolo OSPF en cada routers de la topología [62].

Los diferentes tipos de routers con los que se puede implementar una topología OSPF multitarea son los siguientes:

a) Router Interno: Todas las interfaces se encuentran conectados a un router vecino que se encuentra dentro de la misma área.

b) bRouter Backbone: Una o más de sus interfaces están conectadas al área backbone

ABR(Area Border Router): Dos de sus interfaces como mínimo están conectadas a dos áreas diferentes, puede tener una interfaz conectada a una área y otra al backbone (area 0).

- Tiene una base topológica para cada una de la áreas a las que está conectado.
- Permite enrutar tráfico entre diferentes áreas.
- Permite el resumen de direcciones IP (resume un grupos de direcciones IP en una sola)

c) ASBR (Autonomous System Border Router): Una de sus interfaces se encuentra conectada a otro Autonomous System, permite distribuir las rutas externas de otros AS con protocolos de ruteos que no son OSPF y también permite resumen de rutas [63].

En la figura 3-16, se indica una topología, la cual tiene 3 aéreas diferentes, un switch y 4 routers en la área 1 se encuentra un router de tipo interno conectado al router ABR-2, el cual está conectado a la área 0 backbone, el router ABR-1 se conecta al área 51 y al backbone, el router ASBR está conectado al Backbone, al Internet y aun Autonomous System que utiliza como protocolo de ruteo EIGRP [63].

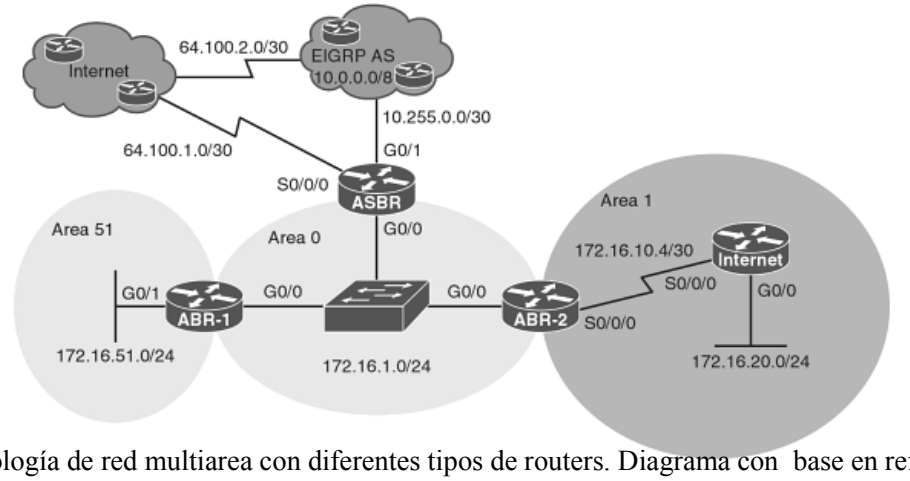


Figura 3-16 Topología de red multiarea con diferentes tipos de routers. Diagrama con base en referencia [63].

Las LSA son publicaciones de estado-enlace utilizadas por el protocolo OSPF que son enviados para la construcción de la base de datos de estados de enlaces, dependiendo del tipo de routers se utilizan distintos

tipos de LSA para utiliza la información de los estados de enlace. Los diferentes tipos de LSAs e indican en la tabla 3-4

Tipo de LSA	Descripción
1	LSA de Router
2	LSA de Red
3 y 4	LSA de Tipo resumen
5	LSAs Externas
6	LSAs de Multicast
7	NSSAs para NSSA
8	LSA de atributos externos para BGP
9, 10 o 11	LSA opacas

Tabla 3-4 Tipos de LSAs. Tabla en base a referencia [61].

a) LSA de Router tipo 1 (Intra área)

Generadas por cada router que se encuentran dentro de una misma área, describe el estado de los enlaces directamente conectados, las LSA de router no salen del area a la que pertenece el enlace, las rutas aprendidas mediante este tipo de LSA se marcan como tipo O.

Cada LSA de este tipo contiene información sobre sus enlaces directamente conectados que pueden ser de tipo:

Tipo de Enlace	Descripción	ID de estado de enlace
1	Conexión punto a punto a un router	ID del roueter vecino
2	Conexión a una red de transito	IP de DR
3	Conexión a una red de area stup	IP/máscara de subred
4	Enlace virtual	ID del roueter vecino

Tabla 3-5 Tipos de LSA de router. Tabla con base en [64].

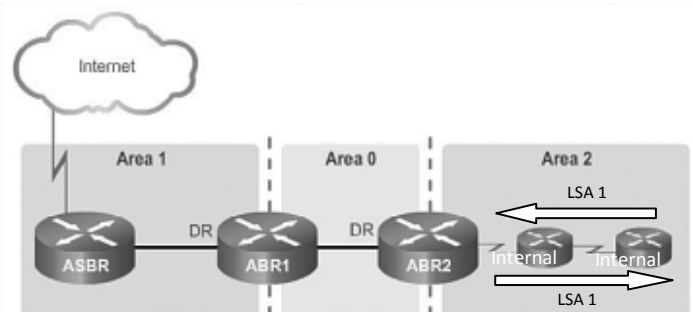


Figura 3-17 LSA de tipo 1 en una topología con OSPF. Diagrama con base en [64].

b) LSA de Red tipo 2 (Intra área)

Esta tipo de LSA es generado en redes broadcast multiacceso y en redes NBMA, entre la conexión de los routers DR, BDR y Drorhers, el DR es quien genera las LSA de tipo 2, las cuales describen un conjunto de routers conectados a un mismo segmento físico que no salen de la area en la que se encuentra el citado enlace de red. Este tipo de LSA es marcada por el protocolo como tipo O. En la figura 3-18 se indican las LSAs dentro de una topología de red.

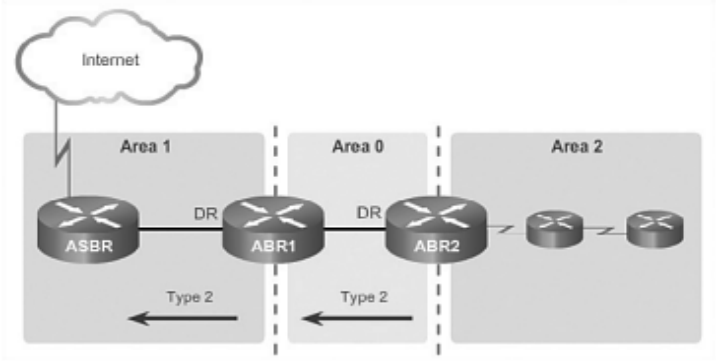


Figura 3-18 LSA de tipo 3 en una topología con OSPF. Diagrama con base en referencia [64].

c) LSA de Resumen tipo 3 (Inter área)

Son generadas por el BGR, para ser enviadas de una área a otra, a través de los ABR, las cuales describen la conexión del ABR con su área, publican las rutas asociadas a una área de manera resumida. Las rutas aprendidas mediante este tipo de mensajes son marcadas por el protocolo como OIA (OSPF Inter Área).

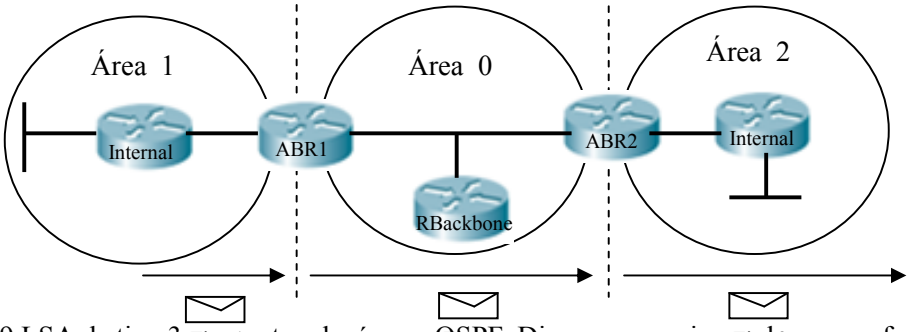


Figura 3-19 LSA de tipo 3 en una topología con OSPF. Diagrama propio con base en referencia [65].

d) LSA de Resumen tipo 4 (Inter área)

Esta es generada por un ABR, la cual es enviada al área de backbone, la LSA contiene información acerca de la alcanzabilidad de ASBR dentro del área, es enviada a través del backbone al resto de los ABR de la topología de la red. Las rutas son marcadas por el protocolo OSPF como tipo IA (Inter Área).

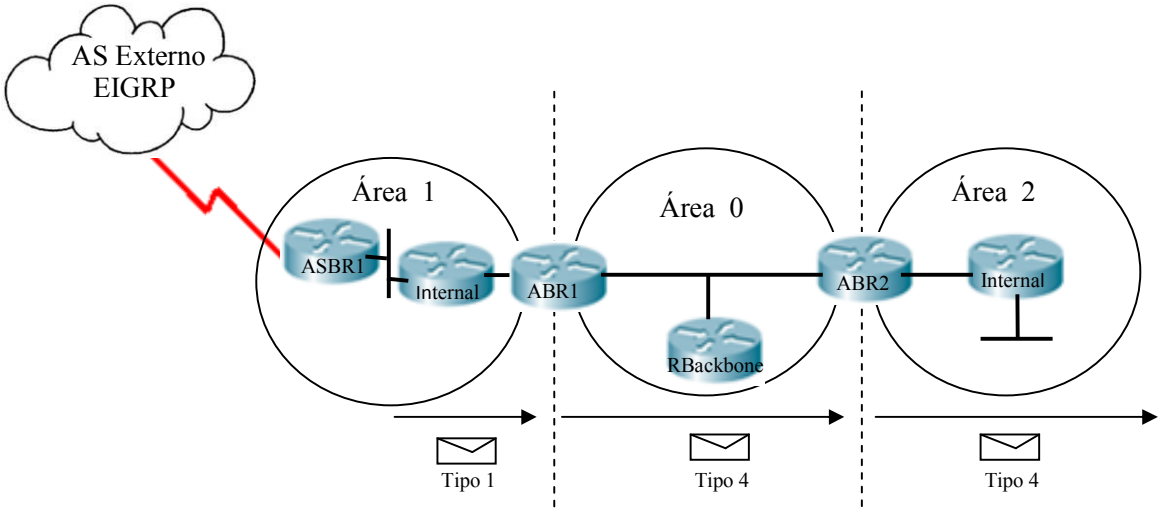


Figura 3-20 LSA de tipo 4 en una topología con OSPF. Diagrama propio con base en referencia [65].

e) LSA Externas de tipo 5 (Inter área externa).

Las LSA de tipo 5 son generadas por ASBR, estas describen rutas fuera del sistema autónomo, las cuales fluyen a través de todo el sistema autónomo, excepto por las stubby(no acepta LASs para la distribución de rutas externas, tales como rutas desde orígenes no OSPF) y las totally stubby áreas(Es una área propietaria de Cisco que no acepta rutas de sistemas autónomos externos)

Las rutas son marcadas por el protocolo OSPF como tipo E2O (OSPF External Type 2)

Las LSA describen las rutas fuera del AS. Existen dos tipos de Externanl Link:

E1 publica el costo total para alcanzar al destino (costo externo + conste interno)

E2 solo publica el costo externo (costo asignado en la redistribución)

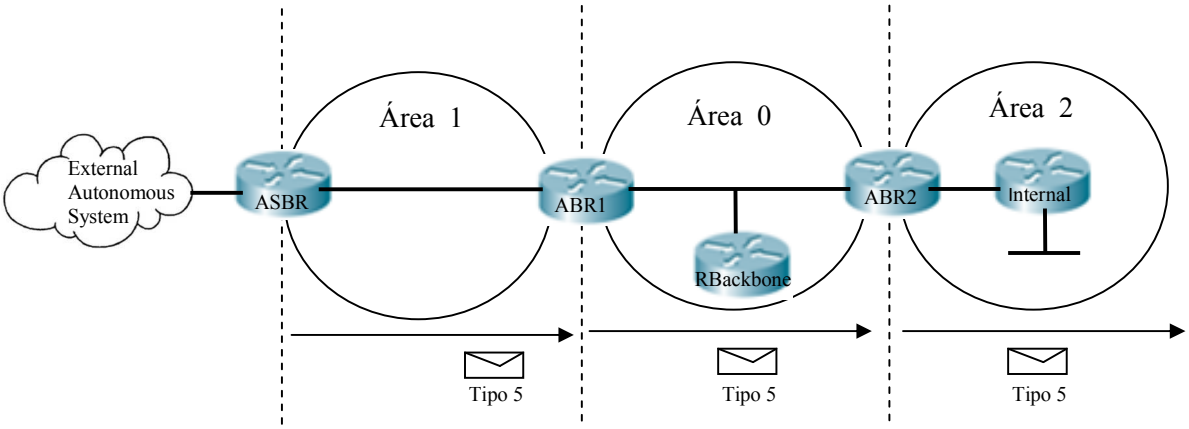


Figura 3-21 LSA de tipo 5 en una topología con OSPF. Diagrama propio con base en referencia [65].

f) LSA de tipo 8

LSA especiales utilizadas para la conexión de BGP ocnOSPF

g) LSA de tipo 9, 10 y 11

Llamadas también LSAs opacas

Diseñadas para usos futuros especialmente para MPLS (Multiprotocol Label Switching).

3.2.2.1.2 Resumen de Rutas

El resumen permite enviar varias rutas, a través de una sola publicación de ruta, cuando se configura el proceso OSPF de manera correcta, afecta de manera directa al consumo de ancho de banda, memoria y CPU consumidos por el protege a los routers de los recalculos de sus rutas y cambios en la tabla de enrutamiento, como la ejecución de OSPF consume mucho procesamiento de la CPU, un buen diseño del direccionamiento jerárquico así como un adecuado resumen son completamente necesarios en OSPF [65].

Los dos tipos de resumen de rutas son los siguientes:

a) Inter-área: El resumen se realiza en ABR y se hace utilizando LSAs de tipo 3.

Se aplica a las rutas que hacen referencia a la propia area

No se aplica a las rutas externas

Deben configurarse redes contiguas

b) External: Se realiza en los ASBR utilizando las LSAs de tipo 5.

Se aplica a rutas que se han prendido mediante redistribución.

Es importante asegurarse que los rangos de las direcciones IP que se resumieron sean contiguos.

En la figura 3-22 se indican las rutas que se resumieron en la dirección 200.9.0.0/16 por el router ASBR, la rutas externas son generadas por el protocolo de ruteo RIP que pertenece a la área externa y en el router ABR se realiza el resumen de rutas internas perteneciente al área 1, las culas se reasumen en la dirección 192.168.16.0/22.

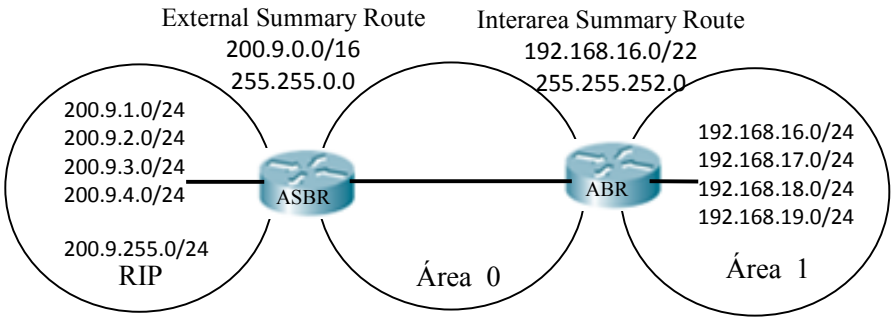


Figura 3-22 Ejemplo de resumen de rutas. Diagrama propio con base en referencia [65].

3.2.2.1.3 Tipos de áreas en OSPF

El protocolo OSPF en su configuración jerarquía, define diferentes tipos de áreas, en una topología de red, las cuales se describen a continuación:

a) Estándar: Área que permite la actualización de enlaces, resumen de rutas internas y externas

b) Backbone: Tambien identificada como area 0, en todas las topología de OSPF se encuentra una área backbone, tiene las mismas características de una área estándar.

c) Stub Área: Esta área permite el resumen de direcciones IP, no acepta LASs para la distribución de rutas externas, tales como rutas desde orígenes no OSPF, si los routers requieren enrutar información fuera de del Sistema Autonomo OSPF, por ejemplo de los protocolos RIP EIGRP, el router ARB distribuirá la ruta por defecto (0.0.0/0), a través de todos los routers internos del area Stub, que se utiliza para alcanzar otras redes externas. En el área Stub no se permiten ASBR pero sí el router hace la función de ASBR y ABR al mismo tiempo, entonces sí lo permitirá, no acepta LSAs 4 y 5

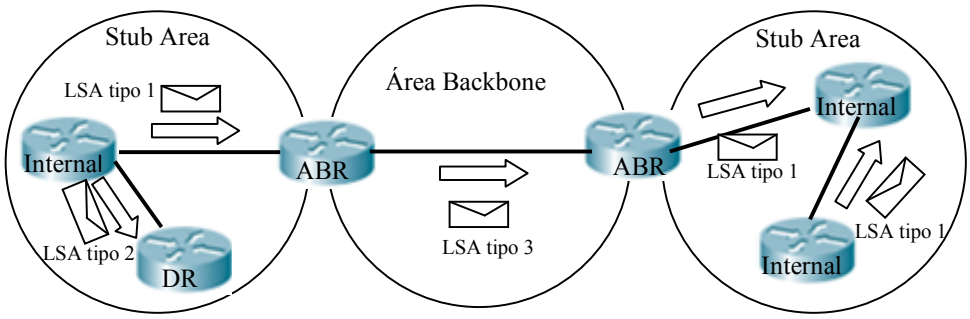


Figura 3-23 Áreas Stub con LSAs permitidas. Diagrama propio con base en referencia [65].

d) Totally Stubby Area: Es una área propietaria de Cisco y no acepta rutas de sistemas autónomos externos (redistribución) o rutas sumarizadas desde otras áreas internas del sistema autónomo. Al igual que en las áreas Stub, los ABR envían una ruta por defecto para todas las rutas externas y sumarizadas (esa es la diferencia con Stub). No se permiten ASBR (a menos que el ABR sea al mismo tiempo un ASBR), no acepta las LSAs 3, 4 y 5.

e) NSSA (Not So Stubby Area) Permite la distribución de las LSAs de tipo 7, no acepta información de rutas externas al sistema autónomo OSPF, al igual que la area Stup, estas rutas las remplaza por una ruta por defecto originada en el ABR, a diferencia de la area Stup NSSA si acepta ASBR que se conecta directamente con otros protocolos de ruteo como por ejemplo RIP e EIGRP. EL ASRB envía su información de la ruta a través de una LSAs de tipo 7, esta sólo es visible o aceptable a través de la área NSSA, cuando la LSAs de

tipo 7 llega a un ABR, para distibuirla dentro de su área, este traduce la LSAs a tipo 5, para poderla enviar a los rouetrs de la área. No acepta las LSAs de tipo 4 y 5.

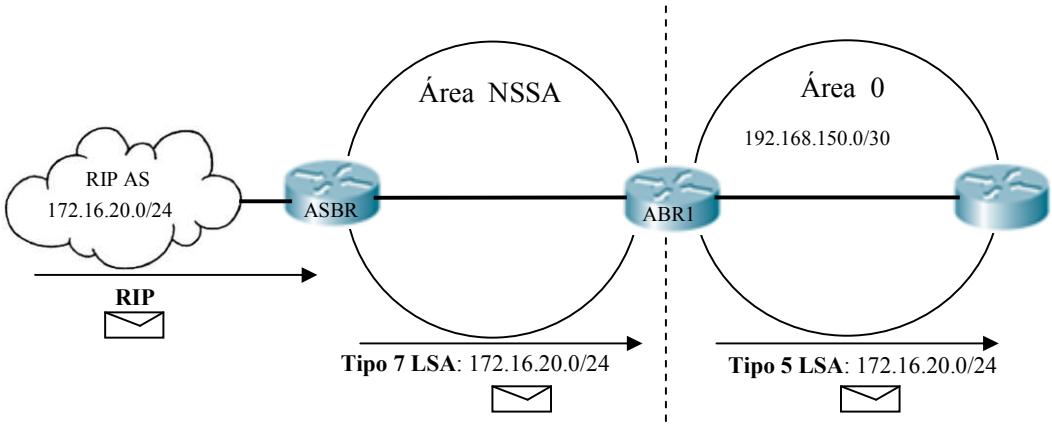


Figura 3-24 Áreas NSSA con LSAs permitidas. Diagrama propio con base en referencia [65].

f) Totally Stubby Stubby NSSA: Esta área también es propietaria de Cisco System que al igual que Totally Stubby Area no permite rutas externas ni sumarizadas, pero si permite un ASBR al igual que la área NSSA. No acepta rutas externas aprendidas mediante LSAs 4 y 5 ni LSAs de tipo 3, solamente reconoce rutas intra-area, la ruta por defecto, se propaga la ruta por defecto en la área, el ABR tiene que ser configurado con el parámetro no-summary, para evitar que se propaguen rutas de tipo 3 dentro del NSSA.

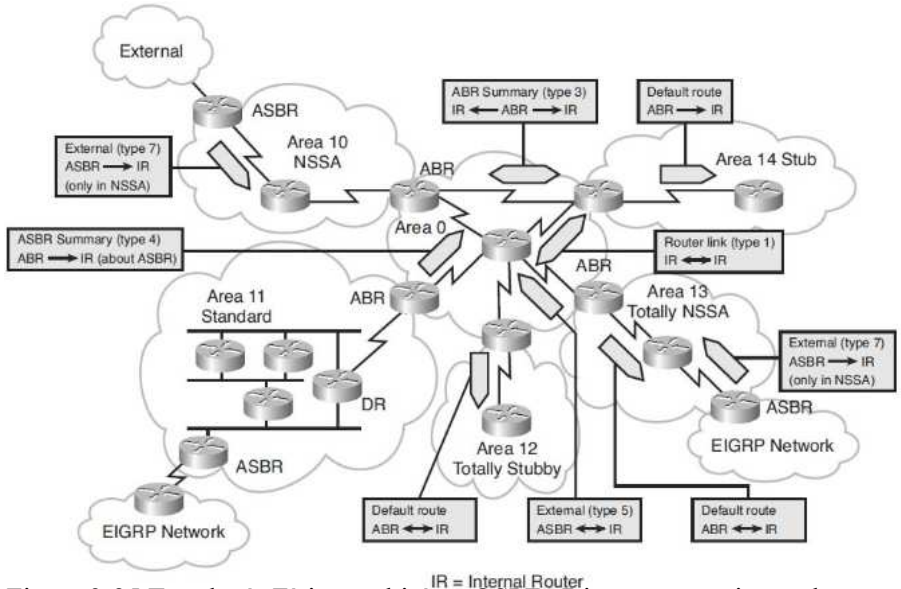


Figura 3-25 Topología Física multi-área OSPF . Diagrama propio con base en referencia [65].

En la tabla 3-6 se muestra un resumen de los tipos de áreas que se pueden definir al implementar el protocolo OSPF, así como las notificaciones de estados de enlaces permitidos y el tipo de rutas no permitidas en cada una de las áreas en los niveles jerárquicos de una topología con miliáreas.

Tipo de Área	Acepta Rutas dentro de la área (0)	Acepta Rutas desde otras área (O IA)	Aceptadas Rutas externas (O E1 y O E2)	Permite ASBR	Propietaria De Cisco System	Tipo de LSAs que permite	Tipo de LSAs que no acepta
Estaandar	Si	Si	Si	Si	No	1,2,3,5	4,6,7
Backbone	Si	Si	Si	Si	No	1,2,3,5,4,7	6
Stub	Si	Si	No (Utiliza ruta por defecto)	No	No	1,2,3	4,5
Totally stubby	Si	No (Utiliza ruta por defecto)	No (Utiliza ruta por defecto)	No	Si	1,2	3,4,5
NSSA	Si	Si	No (Utiliza ruta por defecto)	Si	No	7	4,5
Totally Stubby NSSA	Si	No (Utiliza ruta por defecto)	No (Utiliza ruta por defecto)	Si	Si	7	3,4,5

Tabla 3-6 Descripción de las rutas y LSAs que aceptan las diferentes áreas en una topología multi-área. Tabla con base en referencia [65].

3.2.2.2 Protocolo IS-IS

EL protocolo IS-IS fue desarrollado por DEC (Digital Equipment Corporation*)* y suscrito por ISO (International Organization for Standardization) en 1980, para que fuera el protocolo de ruteo de ISO, ya que se requería de un protocolo no propietario con un esquema de direccionamiento grande, así como un esquema de direccionamiento jerárquico y eficiente que permitiera una convergencia rápida, precisa y eficiente. IS-IS es un protocolo de estado de enlace, ya que utiliza el algoritmo Dijkstra para calcular la ruta más próxima, también realiza un árbol de toda la topología de red, en cada uno de sus routers, divide la red en niveles jerárquicos al igual que OSPF, a diferencia de el protocolo OSPF que es implementado como una solución empresarial IS-IS es implementado como una solución para los ISP. Otra de sus principales características de este protocolo, es que opera en la parte superior de la capa 2 a diferencia de OSPF que opera en la capa 3, IS-

IS es un protocolo con su propio paquete de capa 3, en redes broadcast todos los IS (Internal System) mantienen adyacencia entre ellos [49].

El protocolo IS-IS establece una estructura jerárquica de dos niveles, en los cuales se identifican los *router* de a cuerdo al nivel de jerarquía al que pertenecen, la descripción de estos *routers* son los de Nivel 1: Estos *routers* se establecen en el nivel 1 y sólo se comunican dentro de la área para encontrar la mejor ruta. *Router* Nivel2: Este se comunica en el segundo nivel y busca el área al cual pertenece un IS o ES (External System) de destino.

Hay un tercer *router* el cual es de nivel 1-2, el cual lo podemos identificar como nivel 3, este permite que se comuniquen los *routers* de nivel 1 con los de nivel 2, por lo que tendrán una tabla de rutas del nivel1 como del nivel2. En la figura 3-26 se indica una topología de red con sus diferentes *routers* de nivel L1, L 2 y L1-2.

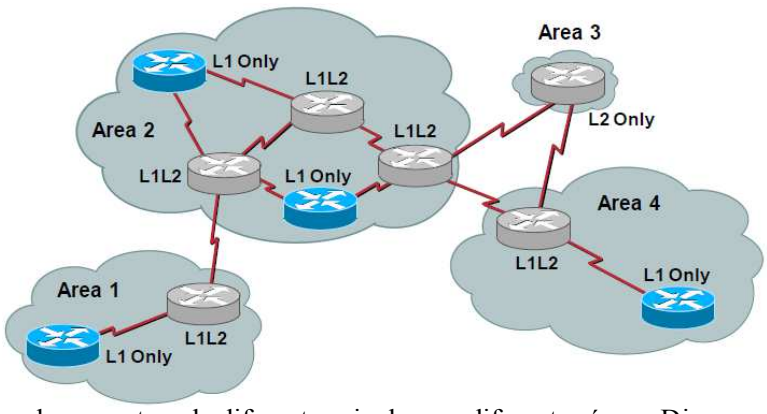


Figura 3-26 Topología de red con routers de diferentes niveles, en diferentes áreas. Diagrama con base en referencia [49].

Para el enrutamiento de los paquetes se requiere que cada uno de los routers se identifique a lo largo de la topología de la red con una dirección ISO, la cual puede ser NSAP (Network Servicie Access Point) y NET (Network Entity Tittle), estas direcciones pueden ser del tamaño de 8 y 20 bytes de longitud y se dividen en tres partes: ÁREA que se utiliza para enrutar entre áreas utilizando routing Nivel 2. ID Se utiliza para enrutar

mensajes de un host o un *router* dentro de la área utilizando routing Nivel 1. SEL: Se utiliza para enrutar a una entidad en el host o en el ES (End System).

Esta dirección se divide en dos partes en IDP (Initial Domaint Part) que es utilizado para enrutar el dominio o el AS, identifica la organización, la cual es responsable del resto de la estructura del direccionamiento, dentro de este campo se encuentra AFI (Authority and Format IDentifier) que es el primer octeto del campo y IDI (Initial Domain Identifier) es la subrogación del AFI. El segundo campo en el que se divide es el DSP (Domain Specific Part) que se utiliza para enrutar dentro del AS y este a su vez se subdivide en DSP (High Order) que se refiere al área dentro del AS, System ID que puede tener un valor entre 1 y 8 octetos, que puede ser la dirección MAC. Esta dirección ISO se subdividen en NETs: Es la dirección de un host, donde el valor del campo NSEL es 0x00, esta es básicamente NSAP con el campo NSEL a 0x00. Como se puede indicar en la figura 3-27, la cual tiene una MAC de AA:00:03:01:16:CD

IDP		DSP		
AFI (1 octeto)	IDI	High Order DSP	System ID (1-8 octetos)	NSEL (1 octeto)
47.		0005.	aa00.0301.16cd	0
AREA			ID	SEL

Figura 3-27 Campos de una dirección NET. Diagrama con base en referencia [49].

NSAP Son direcciones que describen el área, el host y al destino a quien se va enviar la información. En la figura 3-28 se indica una topología de red, formada por un conjunto de routers, los cuales, están identificados a través de toda la red por una dirección NET, la parte que esta remarcada en itálica nos indica el identificador del área o nivel y el resto de la dirección nos indica la MAC del router.

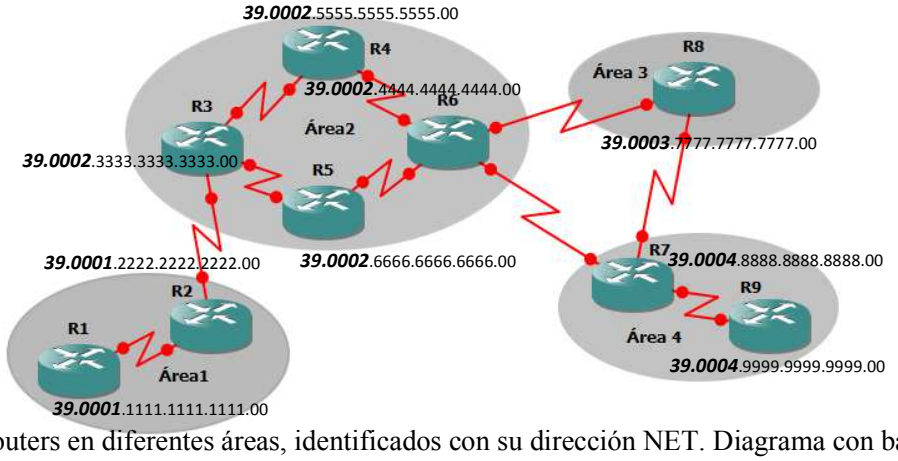


Figura 3-28 Routers en diferentes áreas, identificados con su dirección NET. Diagrama con base en referencia [49].

IS-IS a diferencias de los otros protocolos de ruteo, no utiliza el protocolo TCP/IP para el envió de los paquetes ya que uti

liza ISO, en la tabla 3-7 se puede ver la diferencia que hay entre ISO e IP.

ISO	IP
IS (Intermediate System)	Router
ES (End System)	Host
CLNS (Connectionless Network Service)	IP/UDP stack + applications running onn top of UDP
CLNP (Connectionless NetworkProtocol)	IP
NSAP (Network Service Access Point)	IP address + TCP/UDP port
NET NSAP Address where NSEL	IP address
PDU(Protocol Data Unit)	Packet
LSP(Link State PDU)	LSA in OSPF

Tabla 3-7 Diferencia de parámetros de ISO e IP. Tabla con base en referencia [49].

3.3 Protocolos EGP

Los protocolos Exterior Gateway son los que permiten comunicarse entre los Sistemas Autónomos, a diferencia de los IGP, que se comunican dentro de los AS, dentro de estos protocolos podemos citar el protocolo BGP, que a su vez se clasificado en IBGP (Internal Border Gateway Protocol) y EBGP (External Border Gateway Protocolo) los cuales permitirán el paso de paquetes entre los enlaces de los diferentes sistema autónomos, la clasificación de cada uno de estos se determina de a cuerdo a su configuración y a la función que realiza, para el enrutamiento de la información entre las redes de los Sistema Autónomo [49].

3.3.1 BGP

El protocolo BGP fue desarrollado a finales de 1980 como una solución, para que se pudieran enrutar paquetes a través de los diferentes AS, por lo que es definido como un protocolo EGP ya que se encarga del direccionamiento del tráfico de los diferentes redes interconectadas entre diferentes Sistemas Autónomo. Este protocolo es utilizado por los diferentes proveedores de Internet para comunicar sus sistemas directamente con el backbone de Internet. BGP se basa en un vector de distancia. Actualmente es utilizada la versión 4 del protocolo en los AS la cual ha estado funcionando en Internet desde 1990 [47].

La implementación del protocolo BGP se basa en TCP utilizando el puerto 179 para establecer las conexiones entre los sistemas de los AS, su distancia administrativa es de 200, soporta VLSM, CIDR y resumen de rutas, realiza actualizaciones completas al establecerse la conexión, si se presenta una actualización en la topología de la red se activa un mensaje para realizar una actualización de los cambios en la red, permite utilizar direccionamiento jerárquico, así como la capacidad de manipular el flujo de tráfico, lo que permite que la red pueda crecer. El protocolo cuenta con su propia tabla de ruteo, sin embargo, es capaz de compartir y preguntar sobre la tabla de ruteo IP interior, permite modificar el flujó de tráfico haciendo uso de atributos, una de sus principales características es su actualización que permite asegurar la fiabilidad de transporte al actualizar y sincronizar la tabla de ruteo [49].

BGP puede es implementado entre Sistemas Autónomos como un protocolo de pasarela exterior, el cual es llamado EBGP o dentro de los AS, cuando es configurado de esta forma se utiliza para llevar información exterior entre *routers* EBGP que se encuentran en el mismo AS y es llamado IBGP. En la figura 3-29 se indican estos dos tipos de configuraciones del protocolo BGP en los diferentes *routers* [49].

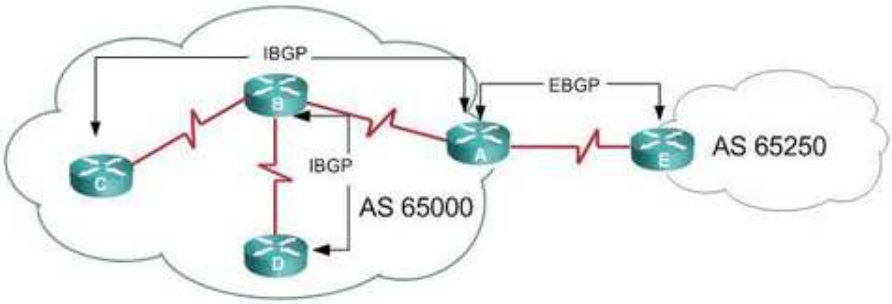


Figura 3-29. BGP Configurado como IBGP y EBG en dos As diferentes. Diagrama con base en referencia [66].

Cada mensaje que se envía tiene un tamaño fijo de cabecera, los mensajes a demás de los campos principales de identificación pueden o no contar con los datos que se encuentran después de la cabecera. El máximo tamaño del mensaje puede ser de 1024 bytes y el mínimo es de 8 bytes. Los campos que contiene la cabecera se indican en la figura 3-30 [66].

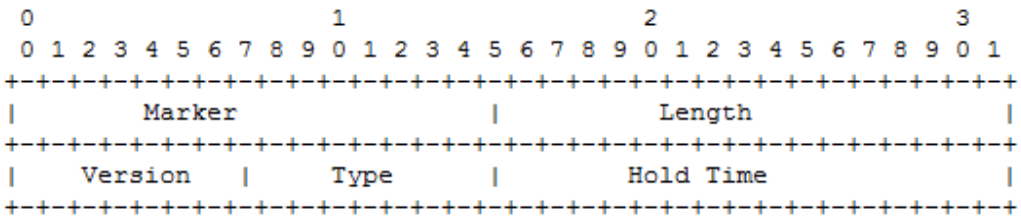


Figura 3-30 Cabecera de los mensajes BGP. Diagrama con base en referencia [67].

Donde el campo *Marker de 16 bits* se utiliza para marcar el inicio de un mensaje y para controlar la sincronización de los paquetes, cuando estos se envían en varios bloques, este campo revisa si los segmentos pertenecen al mismo conjunto de información. *Length 16 bits* indica la longitud total del mensaje incluyendo el encabezado. *Version de 8 bits* se refiere a la versión del protocolo BGP que se está ejecutando. *Type 8 bits* este parámetro indica el tipo de mensaje, los cuales se representan por uno de los siguientes números: 1 *Open*, 2 *Update*, 3 *Notification*, 4 *Keepalive* y *open confirm*. *Hold Time de 16 bits* es el tiempo en segundo después de recibir un mensaje Keepalive BGP o BGP Update antes de determinar el enlace como inalcanzable. La forma en que se ejecuta el procedimiento de la actualización de rutas a través del protocolo, primero establece una conexión entre los *routers* a través de un enlace, esto se realiza a través del protocolo TCP, después

intercambian mensajes para abrir y confirmar los parámetros de conexión , el flujo de datos inicial es toda la tabla de ruteo BGP, se envían actualizaciones periódicas para actualizar las rutas, así como mensajes de mantenimiento de conexión, se envían también mensajes de notificaciones los cuales se ejecutan cuando se presenta un error o cuando se modifican los enlaces de la topología de la red [67].

Tabla comparativa de protocolos de ruteo.

CATRACTERISTICAS	RIP1	RIP2	IGRP	EIGRP[2]	OSPF	IS-IS	BGP[1]
Enrutamiento interior	✓	✓	✓	✓	✓	✓	-
Enrutmaiento exteriro	-	-	-	-	-	-	✓
Vector de distancia	✓	✓	✓	✓			✓
Estado de enlace	-	-	-	-	✓	✓	-
Soporta Classful	✓	-	✓	-	-	-	-
Soporta Classless	-	✓	-	✓	✓	✓	✓
Soporta VLSR	-	✓	-	✓	✓	✓	✓
Soporta CIRD	-	✓	-	✓	✓	✓	✓
Métrica saltos	✓	✓	-	-	-		
Métrica ancho de banda	-	-	-	-	✓		
Métrica ancho de banda retardo	-	-	✓	✓	-		
Métrica atributos de ruta	-	-	-	-	-	-	✓
Autentificación	-	✓		✓	✓		
Sumarización automática	✓	✓		✓	-	-	✓
Sumarización manual	-	✓		✓	✓	✓	✓
Año	1988	1994	1985	1992	1991	1990	1995
Intercambio de Información enrutamiento	Entire table Broadcast 255.255.255.255 Update:30s	Entire table Multicast 255.0.0.9 Update: 30s	Entire Broadcast 255.255.255.255 Update: 90s	Partial Update Multicast 224.0.0.10 Event-Update	PArtial Update Multicast 224.0.0.5 y 6 Event-Updtae		
Distancia Administrativa	120	120	100	90/90/170	110		[3]
Protocolo de transporte	UDP	UDP	UDP	RTP	NO		
Número de puerto	-	520 UDP		-	-	-	179 TCP
Número de protocolo	-	-		88	110	124	20/200
Tiempo de Convergencia	Lenta	Lenta		Muy rápido	Rápida	Rápido	Muy lento
Tamaño de red	Pequeño	Pequeño		Grande	Grande	Grande	Muy grande
Tipos de paquetes	Query Update	Query Update		Hello Update Query Reply Ack	Hello DBD LSR LSU LSAck	Hello Link State Sequence	Open Keepalive Update Notificaci on
Temporizadores	Update Invalid Holddown Flush	Update Invalid Holddown Flush		Hello Holdtime Active	Hello Dead Interval	CSNP Hello Holding LSP Retransmit	ConectRet ry Hold time Keepalive

Tabla 3-8 Características de los diferentes protocolos de ruteo.

1. BGP también se conoce como un protocolo de vector de ruta.

2. En EIGRP, la AD es de 5 para rutas sumarizadas, 90 para rutas internas y 170 para rutas externas (redistribuídas dentro de EIGRP)

3. En BGP, la AD para las sesiones BGP externas (EBGP) es de 20 y para las internas (IBGP) es 200

CAPÍTULO IV SIMULACIÓN DEL BACKBONE DE LA RED CLARA

Como primera aproximación de la red avanzada CLARA se utilizó el simulador de Packet Tracer de Cisco System, el cual no cuenta con equipo de backbone, por lo cual se utilizaron routers genéricos con interfaces de red a velocidades de 1 Gbps y 100 Mbps, así como interfaces seriales, se configuraron los routers del backbone con subredes, las cuales se crearon a partir de una dirección IP clase C, se activó el protocolo OSPF en cada uno de los routers para realizar pruebas de validación de parámetros OSPF y de transmisión de información, se realizaron pruebas de tiempo de respuesta al enviar información entre los routers, también se forzó el simulador, para determinar hasta qué punto se puede trabajar en el simulador con redes avanzadas como la red CLARA, ya que Packet Tracer tiene limitaciones, al no contar con equipo de backbone y velocidades de transmisión menores no mayores a 1Gbps en las interfaces de red. En este capítulo se realiza la simualación de la red avanzada CLARA utilizando un simulador como primera aproximación, se configuran los routers de cada uno de los nodos de la red, se realizan pruebas, para validar la configuración del protocolo OSPF y la transmisión de la información a través de sus diferentes enlaces, se hace uso de las herramientas de simulación para analizar los diferentes mensajes enviados por el protocolo OSPF a los routers

El proceso de simulación se inició con la determinación de la clase de red que se utilizó en la topología, así como los tipos de router, el número de direcciones IP, el tipo de enlace, para aproximarlo a la velocidad de transmisión de la topología de la red, y también el tipo de interfaces de red en cada uno de los routers.

Los routers, se determinaron de acuerdo a la cantidad y tipo de interfaces que soportan, así como la versión del IOS, lo que permitió trabajar con la versión 2 del protocolo OSPF. Para el escenario de la topología de red CLARA, se realizó la simulación con 10 router genéricos que soportaron hasta 10 interfaces de fibra óptica de 1 Gbps o interfaces seriales de 128 Kbps, con una versión de IOS de 12.2 (28).

Como el Backbone de la Red CLARA cuenta con enlaces de 155 Mbps, 622 Mbps y 11 enlaces de fibra óptica y para que la simulación fuera lo más aproximado a la red CLARA, se determinó simular los enlaces de 155 Mbps y 622 Mbps con interfaces seriales de 128 Kbps y para los enlaces de fibra óptica se realizó la aproximación con interfaces de fibra óptica de 1 Gbps, en la simulación se conectaron 2 enlaces seriales y el resto con fibra óptica, como se indica en la tabla 4-1.

Recurso para la Simulación	Especificaciones Técnicas
Software PacketTracer	Version 5.3.0
Router Genéricos	IOS 12.2(28), soporte para 10 Interfaces
Interfaz Serial/Enlace	Velocidad de 128Kbps
Interfaz de Fibra Óptica/Enlace	Velocidad de 1Gbps
Sistema Operativo	Windows Vista32 bits Service Pack 2
Procesador	AMD Athlon Dual Core 2.2 GHz
Memoria	4 GB

Tabla 4-1 Recursos utilizados en la simulación.

4.1 Cálculo de direcciones IP

Como la topología de la red CLARA, está en configuración punto a apunto, se requiere de dos direcciones IP que se encuentren dentro de una red o de subred, para que se conecten lógicamente y se comuniquen ambos routers, realizando este análisis se determinó crear subredes de una red de clase C 192.168.10.0/24, ya que se consideraron sólo dos direcciones IP de host, una dirección de subred y una dirección de broadcast. El procedimiento que se realizó para el cálculo las subredes se describe a continuación.

De la dirección 192.168.10.0/24, se tomaron 6 bits para la máscara de subred de los 8 que se tienen para el número de host, con lo que se obtuvo una máscara de subred de 30 bits, para 62 subredes con 2 direcciones de host para cada subred como se indica a continuación.

Red clase C 192.168.10.0
255.255.255.0

11111111.11111111.11111111.11111100
Mascara de subred 30 bits Host

Número de subredes 2^6-2= 64 – 2 = 62 subredes

Número de host por subred 2^2 -2= 4 -2 = 2

192.168.10.0/30
Mascara de subred decimal 255.255.255.252

255.255.255.255
- 255.255.255.252

Máscara de wildcard 0 . 0 . 0 . 3

Después de obtener las subredes que serían utilizadas en la simulación de la red CLARA, se determinó cómo serían asignadas a lo largo de la topología. En la tabla 4-2 se indican la direcciones de subredes, las direcciones IP de hosts y las direcciones de broadcast.

Dirección de Subred	Direcciones IP de hosts	Dirección de Broadcast
192.168.10.0/30	192.168.10.1 – 192.168.10.2	192.168.10.3
192.168.10.4/30	192.168.10.5 – 192.168.10.6	192.168.10.7
192.168.10.8/30	192.168.10.9 – 192.168.10.10	192.168.10.11
192.168.10.12/30	192.168.10.13 – 192.168.10.14	192.168.10.15
192.168.10.16/30	192.168.10.17 – 192.168.10.18	192.168.10.19
192.168.10.20/30	192.168.10.21 – 192.168.10.22	192.168.10.23
192.168.10.24/30	192.168.10.25 – 192.168.10.26	192.168.10.27
192.168.10.28/30	192.168.10.29 – 192.168.10.30	192.168.10.31
192.168.10.32/30	192.168.10.33 – 192.168.10.34	192.168.10.35
192.168.10.36/30	192.168.10.37 – 192.168.10.38	192.168.10.39
192.168.10.40/30	192.168.10.41 – 192.168.10.42	192.168.10.43
192.168.10.44/30	192.168.10.45 – 192.168.10.46	192.168.10.47
192.168.10.48/30	192.168.10.49 – 192.168.10.50	192.168.10.51
192.168.10.52/30	192.168.10.53 – 192.168.10.54	192.168.10.55

Tabla 4-2 Subredes utilizadas en la simulación de la red CLARA.

Al obtener las subredes, se realizó un diagrama de la tipología de red, para determinar cómo serían asignadas las subredes a lo largo de todos los enlaces de la red, para determinar el identificador del nombre de

host, el tipo y la cantidad de interfaces para cada router, así como los diferentes tipos de enlaces con sus velocidades, que se aproximen a los valores reales de la transmisión. En la figura 4-1 se indica el diagrama que se utilizó como referencia, para realizar la configuración del backbone de la red CLARA en el simulador.

4.2 Selección y conexión de los dispositivos en el simulador

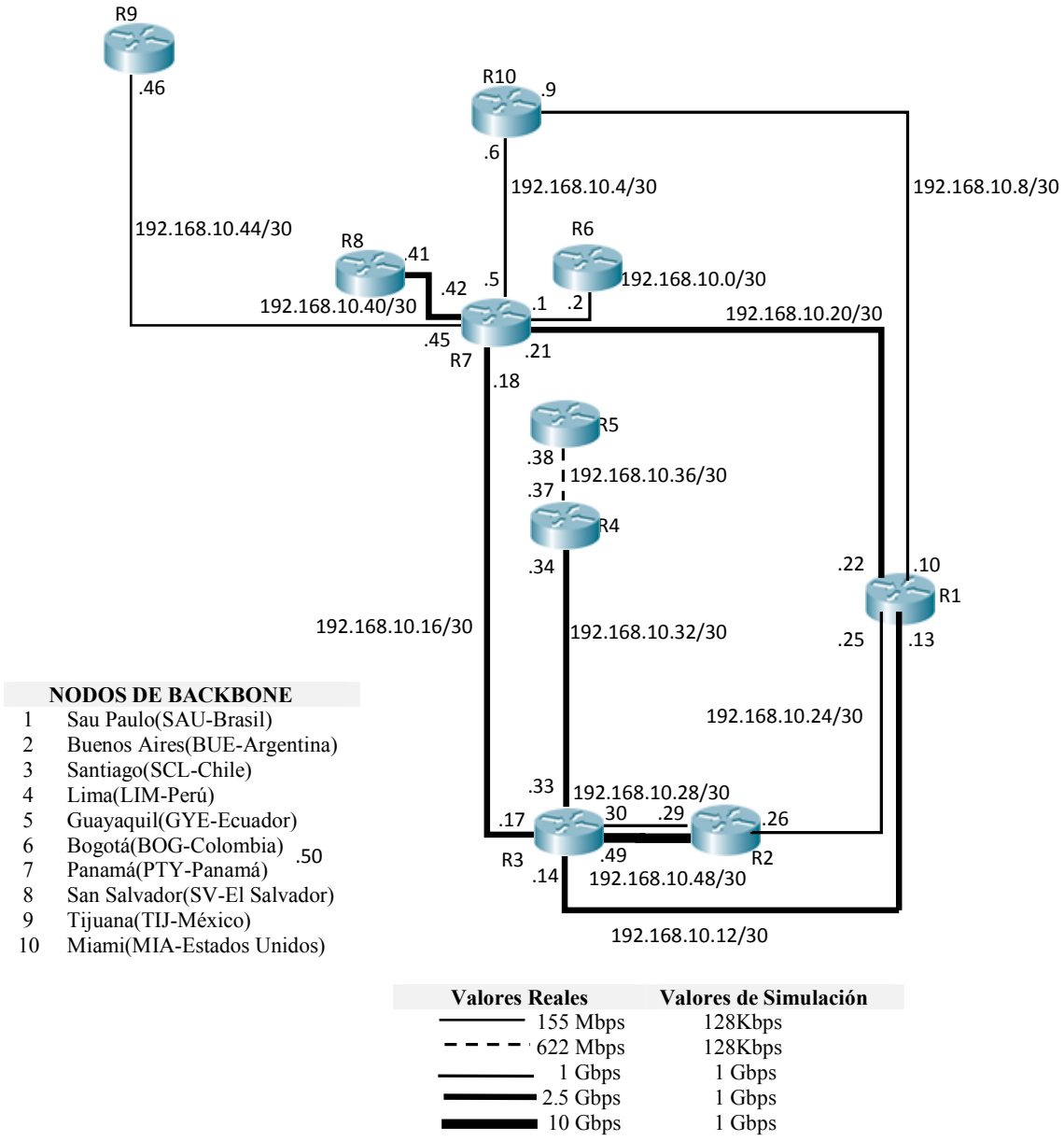


Figura 4-1 Diagrama de la topología, que se implementó en el simulador. Diagrama propio con base en referencia [40].

La configuración de la red, se realizó con los dispositivos e interfaces más aproximadas que nos permitió utilizar el simulador, también hay que subrayar que la topología es una configuración punto a punto, en la mayor parte de sus enlaces utiliza cable de fibra óptica y sólo en 2 se utilizan enlaces seriales, ya que la velocidades de transmisión son de 155 Mbps y 622 Mbps.

En el simulador se eligieron los routers para cada país que conforman el backbone de CLARA, el simulador Packet Tracer no cuenta con routers core como el 7200, por lo que se determinó trabajar con un router genérico, que permitió anexar más de 5 interfaces de fibra óptica de 1 Gbps, que es la máxima velocidad para interfaces de fibra óptica, que se puede utilizar en el simulador, que fueron las que se agregaron al router de Panamá. Otra consideración importante en la selección del router fue el IOS, los cuales cuentan con la versión 12.2 (28) que permiten trabajar con el protocolo OSPF V2.

Después de seleccionar un router genérico con las características que ya se mencionaron, se agregó de fondo un mapa de Latinoamérica en la área de trabajo del simulador, para colocar los routers sobre cada país y se tenga una referencia de la zona geográfica, se coloca cada uno de los routers con la cantidad de interfaces necesarias ya sea de fibra óptica o serial, después se eligió el medio de transmisión para cada enlace de la red, utilizando cables de fibra óptica y sólo dos seriales.

Al tener todos los routers conectados, se agregaron etiquetas con la subred a la que pertenece cada enlace en los routers se agregaron identificadores con nombre del router y en cada uno de las interfaces de los routers se agregaron los últimos octetos de la dirección IP en decimal, que se les asignó a la interfaz de red.

En la figura 4-2 se indica la topología de red CLARA generada en el simulador Packet Tracer, así como sus etiquetas que identifican la subred a las que pertenece el enlace y las direcciones IP que se les asignó a cada una de las interfaces de la red.

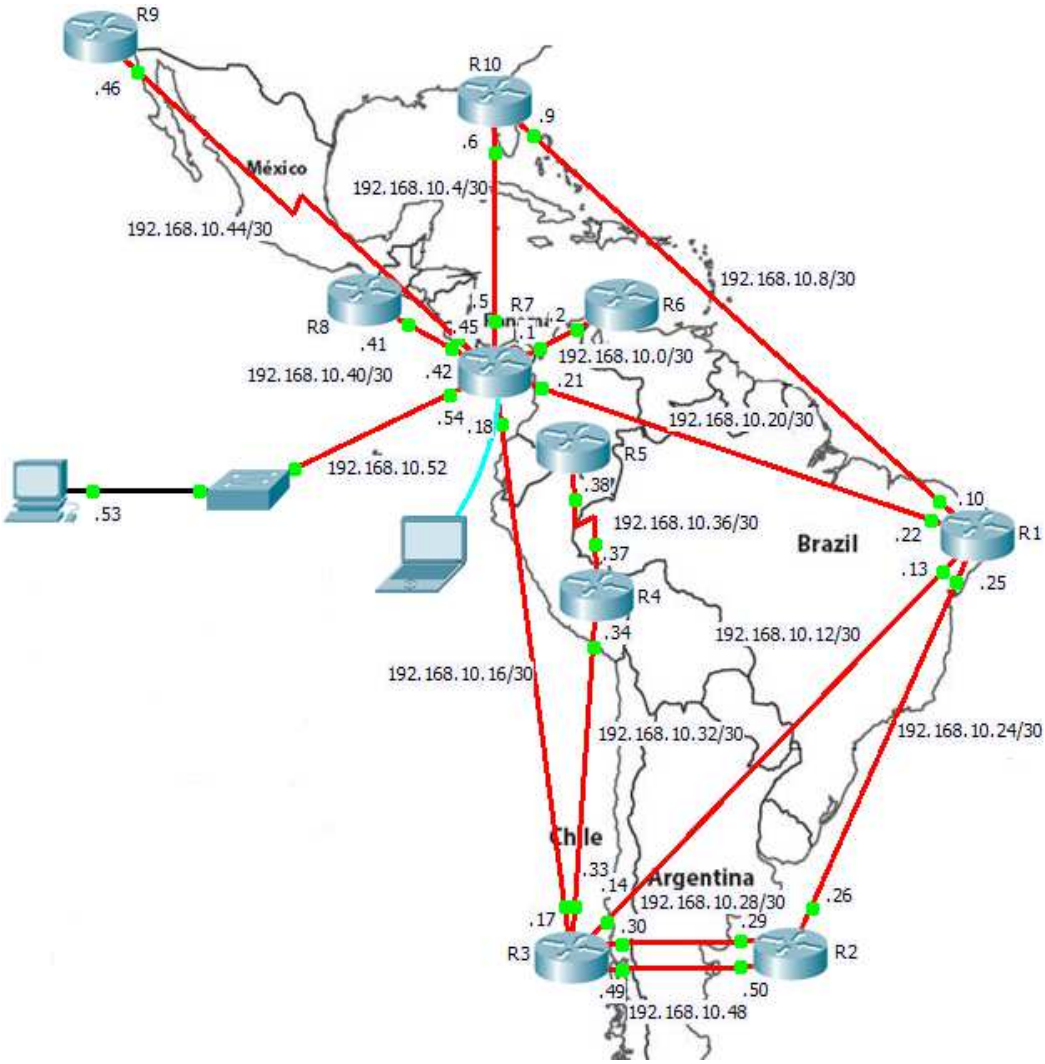


Figura 4-2 Diagrama de la topología en el simulador. Diagrama propio con base en referencia [68].

4.3 Configuración del protocolo OSPF

La configuración de los routers se inició con la configuración del router de Panamá, asignándole un nombre de host, el cual fue el identificador que aparece en el diagrama de la figura 4-2 más el nombre del país al que pertenece el router, después se configuró cada uno de las tarjetas de red, asignándoles su dirección IP, su máscara de subred para su activación, como se indica en la tabla 4-3.

```
Router>enable
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R7Panama
R7Panama(config)#int gi1/0
R7Panama(config-if)#ip address 192.168.10.42 255.255.255.252
```

Tabla 4-3 Configuración de direcciones IP

Se activó el protocolo OSPF, indicando el número de proceso, las subredes a las que se conectó directamente el router con su máscara de *wildcar* y el área, a todas las subredes se les asignó el área 0, ya que el router se configuró dentro de una área backbone como se indica en la tabla 4-4.

```
R7Panama(config)#router ospf 1
R7Panama(config-router)#network 192.168.10.0 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.4 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.16 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.20 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.40 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.44 0.0.0.3 area 0
R7Panama(config-router)#network 192.168.10.52 0.0.0.3 area 0
R7Panama(config-router)#
```

Tabla 4-4 Configuración de subredes al router de Panamá

Después de activar el protocolo OSPF y agregar cada una de las subredes, se validó que el router ya contara con las subredes configuradas, se validó el parámetro de Router ID, como se describió en la teoría del protocolo OSPF, el router asigna la direción IP mayor de sus interfaces, como se indica en la tabla 4-5 al ejecutar el comando *sh ip protocl*.

```
R7Panama#sh ip protocol
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.54
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
    192.168.10.16 0.0.0.3 area 0
    192.168.10.20 0.0.0.3 area 0
    192.168.10.40 0.0.0.3 area 0
    192.168.10.44 0.0.0.3 area 0
    192.168.10.52 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
```

Tabla 4-5 Subredes asignadas al router de Panamá

Se puede ver que al ejecutar el comando *sh ip protocol*, se muestra el parámetro Router ID 192.168.10.45, como se describe en la teoría del protocolo OSPF, estableciendo la dirección IP mayor de todas sus interfaces como Router ID, también se mostraron todas las subredes que se agregaron, el campo de Gateway se encontró vacío, ya que aún no se habían configurado los router vecinos a los que se conectó R7Panama. En la figura 4-3 se indican las subredes a las que se conectó el nodo de Panamá, la dirección IP de sus interfaces y los enlaces de sus vecinos.

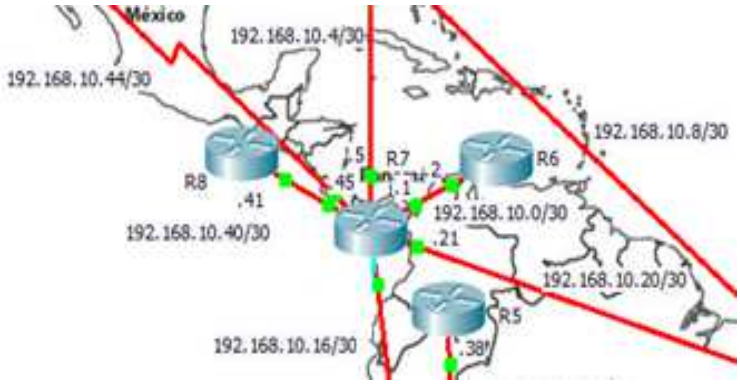


Figura 4-3 Subredes a las que se conectó directamente el router de Panamá. Diagrama propio con base en [68].

La configuración del ancho de banda se realizó en cada una de las interfaces de los routers al ejecutar el comando *bandwidth*, ya que en la topología de los enlaces de la red CLARA, se tienen diferentes velocidades de transmisión. La configuración se realizó, para que el algoritmo Dijkstra realice el cálculo más aproximado del costo, al ejecutar el protocolo OSPF, como se indica en la tabla 4-6.

```
R9Mexico#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R9Mexico(config)#int se1/0
R9Mexico(config-if)#bandwidth 155000
```

Tabla 4-6 Configuración de ancho de banda

Los cambios que se realizaron con el comando *bandwidth,* sólo afectaron el cálculo del costo al ejecutarse el algoritmo Dijkstra, en cada enlace y no la velocidad de transmisión de la interfaz donde se realizó la modificación.

El procedimiento de la configuración del protocolo OSPF y la validación de las subredes que se realizó en el nodo de Panamá, se aplicó a cada uno de los routers de la topología, tomando como referencia las susbredes y direcciones IP, así como los nombre de los routers, que se describieron en el diagrama de referencia para la simulación. En la tabla 4-7 se indican las subredes y direcciones IP en cada uno de los nodos del Backbone de la red CLARA.

Nombre del Nodo	Interfaz	Dirección IP	Mascra de Subred	Gateway
R1Brasil	Gig0/0	192.168.10.10	192.168.10.8	192.168.10.9
	Gig1/0	192.168.10.13	192.168.10.12	192.168.10.14
	Gig2/0	192.168.10.25	192.168.10.24	192.168.10.26
	Gig3/0	192.168.10.22	192.168.10.20	192.168.10.21
R2Argentina	Gig0/0	192.168.10.29	192.168.10.28	192.168.10.30
	Gig1/0	192.168.10.26	192.168.10.24	192.168.10.25
	Gig2/0	192.68.10.50	192.168.10.48	192.168.10.49
R3Chile	Gig0/0	192.168.10.17	192.168.10.16	192.168.10.68
	Gig1/0	192.168.10.33	192.168.10.32	192.168.10.34
	Gig2/0	192.168.10.30	192.168.10.28	192.168.10.29
	Gig3/0	192.168.10.14	192.168.10.12	192.168.10.13
	Gig4/0	192.168.10.49	192.168.10.48	192.168.10.50
R4Peru	Se0/0	192.168.10.37	192.168.10.36	192.168.10.38
	Gi1/0	192.168.10.32	192.168.10.34	192.168.10.33
R5Ecuador	Se0/0	192.168.10.38	192.168.10.36	192.168.10.37
R6Colombia	Gi0/0	192.168.10.2	192.168.10.0	192.168.10.1
R7Panama	Se0/0	192.168.10.45	192.168.10.44	192.168.10.46
	Gig1/0	192.168.10.42	192.168.10.40	192.168.10.41
	Gig2/0	192.168.10.5	192.168.10.4	192.168.10.6
	Gig3/0	192.168.10.1	192.168.10.0	192.168.10.2
	Gig4/0	192.168.10.18	192.168.10.16	192.168.10.17
	Gig5/0	192.168.10.21	192.168.10.20	192.168.10.22
	Gig7/0	192.168.10.54	192.168.10.52	-
R8Salvador	Gig0/0	192.168.10.41	192.168.10.40	192.168.10.42
R9Mexico	Se1/0	19.168.10.46	192.18.10.44	192.168.10.45
R10EEUU	Gig0/0	192.168.10.6	192.168.10.4	192.168.10.5
	Gig9/0	192.168.10.9	192.168.10.8	192.168.10.10

Tabla 4-7 specificaciones de las subredes y direcciones IP asignadas a cada una de las interfaces, en los diferentes routers del backbone de la red CLARA.

4.4 Validación de parámetros OSPF y transmisión

Al habilitar el protocolo OSPF en cada uno de los nodos de la backbone de CLARA, se validó que registraran sus direcciones de Gateway, ya que al ejecutar anteriormente este protocolo no se visualizaban las direcciones debido a que no estaban configuradas las interfaces de los vecinos que estaban conectados directamente a cada router. Al ejecutar el comando *sh ip protocol* en el router de panamá, se pudo ver que tenía cuatro direcciones Gateway, las cuales se refieren a las interfaces de los vecinos que estaban directamente conectados al nodo de Brasil, también se muestra sus distancia administrativa, como se indica en la tabla 4-8.

```
R1Brasil#sh ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.25
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
    192.168.10.12 0.0.0.3 area 0
    192.168.10.20 0.0.0.3 area 0
    192.168.10.24 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.9         110      00:09:50
    192.168.10.14        110      00:09:52
    192.168.10.26        110      00:09:52
    192.168.10.21        110      00:09:52
  Distance: (default is 110)
```

Tabla 4-8 Subredes y Gateways asignadas al router de Brasil.

Continuando con la validación de las conexiones, se validó que nuestro router de Brasil haya establecido la adyacencia con sus vecinos de Argentina, Chile, Panamá y EEUU esto lo validamos al ejecutar el comandos *sh ip ospf neighbor*, que muestra campos con información de los equipos vecinos, la primera columna nos indicó el Router ID del vecino, para el vecino de Argentina es de 92.168.10.9; en la segunda

columna se indica la prioridad de la interfaz que puede ser 0; el estado para este vecino es completo lo cual significa que se estableció adecuadamente la adyacencia y ambos comparten la misma tabla de estados de enlace; también se muestra el tipo de configuración de las interfaces, las cuales pueden ser Drother, DR o BDR; el tiempo restante antes de determinar el enlace como inalcanzable; la dirección IP de la interfaz del vecino a la que el router de Brasil está directamente conectada, la cual es 192.168.10.26 y finalmente la interfaz del router de Brasil con la que se conecta directamente al vecino de Argentina que en este caso es Gig3/0, como se indica en la tabla 4-9.

```
R1Brasil#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.9      0   FULL/DROTHER    00:00:33    192.168.10.9    GigabitEtherne
t0/0
192.168.10.33     0   FULL/DROTHER    00:00:39    192.168.10.14   GigabitEtherne
t1/0
192.168.10.50     0   FULL/DROTHER    00:00:33    192.168.10.26   GigabitEtherne
t2/0
192.168.10.45     1   FULL/BDR        00:00:35    192.168.10.21   GigabitEtherne
t3/0
```

Tabla 4-9 Parámetros de los vecinos a los que se conecta el router de Brasil.

Se puede ver que se estableció la adyacencia con cada uno de los vecinos a los que se conectó directamente el nodo de Brasil, después se validó que el router contará con todas las rutas de los diferentes enlaces del backbone de CLARA, antes de realizar una prueba de transmisión. Para esto ejecutamos el comando *sh ip route*, el cual mostró una lista de todas y cada una de las subredes de la topología de la red, al inicio de la información nos indica que hay 14 subredes que se realizaron de la dirección 192.18.10.0, al inicio de cada subred muestra con una letra el identificador, que determina cómo se alcanza la subred, ***c*** para las interfaces conectadas y ***o*** para indicar que se alcanza vía protocolo ospf, se muestra la distancia administrativa, así como el costo y finalmente a través de cuál dirección IP se puede alcanzar la subred, como se indica a en la tabla 4-10.

```
R1Brasil#sh ip route
Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 14 subnets
O       192.168.10.0 [110/2] via 192.168.10.21, 03:48:30, GigabitEthernet3/0
O       192.168.10.4 [110/2] via 192.168.10.9, 03:48:30, GigabitEthernet0/0
                     [110/2] via 192.168.10.21, 03:48:30, GigabitEthernet3/0
C       192.168.10.8 is directly connected, GigabitEthernet0/0
C       192.168.10.12 is directly connected, GigabitEthernet1/0
O       192.168.10.16 [110/2] via 192.168.10.14, 03:48:30, GigabitEthernet1/0
                      [110/2] via 192.168.10.21, 03:48:30, GigabitEthernet3/0
C       192.168.10.20 is directly connected, GigabitEthernet3/0
C       192.168.10.24 is directly connected, GigabitEthernet2/0
O       192.168.10.28 [110/2] via 192.168.10.14, 03:48:30, GigabitEthernet1/0
                      [110/2] via 192.168.10.26, 03:48:30, GigabitEthernet2/0
O       192.168.10.32 [110/2] via 192.168.10.14, 03:48:30, GigabitEthernet1/0
O       192.168.10.36 [110/3] via 192.168.10.14, 01:41:56, GigabitEthernet1/0
O       192.168.10.40 [110/2] via 192.168.10.21, 03:48:30, GigabitEthernet3/0
O       192.168.10.44 [110/2] via 192.168.10.21, 01:03:05, GigabitEthernet3/0
O       192.168.10.48 [110/2] via 192.168.10.14, 03:48:30, GigabitEthernet1/0
                      [110/2] via 192.168.10.26, 03:48:30, GigabitEthernet2/0
O       192.168.10.52 [110/2] via 192.168.10.21, 03:48:30, GigabitEthernet3/0
```

Tabla 4-10 Tabla del router de Brasil con las mejores rutas para alcanzar todas las subredes del la topología de CLARA.

Se envió una prueba de transmisión del router de R1Brasil, a los nodos de México, El Salvador y Ecuador, como el router cuenta con la tabla de ruteo de todas las subredes de los enlaces, no se presentaron problemas durante la prueba. Después de ejecutar el comando *ping* se obtuvo la información de la tabla 4-11.

```
R1Brasil#ping 192.168.10.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/11 ms

R1Brasil#ping 192.168.10.38

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.38, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 10/11/14 ms

R1Brasil#ping 192.168.10.41

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.41, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/6/9 ms
```

Tabla 4-11 Tiempo de respuesta al ejecutar el comando ping.

Se configuró la computadora conectada a el nodo de Panamá con los siguientes parámetros: IP 192.168.10.53 Mascara de subred 255.255.255.252 y Gateway 192.168.10.54. La primera prueba que se ejecutó con el comando tracert, el cual nos mostró las direcciones IP de las diferentes interfaces de acuerdo a la trayectoria que recorrió el mensaje de prueba, en la segunda prueba se utilizó el comando ping el cual reportó el tiempo de respuesta en ms de los mensajes que se enviaron. La dirección IP de destino fue la 192.168.10.30 del router de Ecuador, desde la computadora hacia ecuador es el que más lejos esta, como se indica en la tabla 4-12.

```
PC>tracert 192.168.10.38

Tracing route to 192.168.10.38 over a maximum of 30 hops

  1    11 ms     8 ms     10 ms    192.168.10.54 Panamá
  2    42 ms     28 ms    9 ms     192.168.10.17 Chile
  3    16 ms     16 ms    10 ms    192.168.10.34 Perú
  4    20 ms     19 ms    30 ms    192.168.10.38 Ecuador
```

```
PC>ping 192.168.10.38

Pinging 192.168.10.38 with 32 bytes of data:

Reply from 192.168.10.38: bytes=32 time=26ms TTL=252
Reply from 192.168.10.38: bytes=32 time=19ms TTL=252
Reply from 192.168.10.38: bytes=32 time=22ms TTL=252
Reply from 192.168.10.38: bytes=32 time=17ms TTL=252
```

Tabla 4-12 Tiempo de respuesta al ejecutar el comando ping desde la PC de la topología de CLARA.

Después de las pruebas de comunicación se revisaron las métricas, para un enlace de fibra óptica y para otro serial, para el caso del enlace serial se revisó el router de México, el comando que se ejecutó fue *sh int se1/0*.

Al ejecutar el comando se observó que el ancho de banda de una línea serial en el simulador de Packet Tracer es de 155000 Kbps. Ya que se obtuvo el ancho de banda, se comprobó el valor de costo para esta interfaz con la expresión que utiliza OSPF, después se ejecutó el comando *sh ip ospf int se1/0*, para comparar los dos resultados, el que se calculó manualmente y el que calcula el protocolo, para validar el cálculo del costo del enlace, como se indica en la tabla 4-13.

```
R9Mexico#sh int se1/0
Serial1/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.46/30
  MTU 1500 bytes, BW 155000 Kbit, DLY 20000 usec,
```

$$Costo = \frac{10^8}{155000X10^3} = 1$$

```
  R9Mexico#sh ip ospf int se1/0
  Serial1/0 is up, line protocol is up
    Internet address is 192.168.10.46/30, Area 0
    Process ID 1, Router ID 192.168.10.46, Network Type POINT-TO-POINT, Cost: 1
    Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

Tabla 4-13 Cálculo de la métrica en el router de México.

Se realizó el mismo procedimiento para los enlaces de fibra óptica, en los cuales se mostró el valor del costo que fue de 1, esto es porque todo valor de ancho de banda mayor a 10^8 bits, se le asignó como costo el valor 1, como se indica en la tabla 4-14.

```
R1Brasil#sh int gi0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.9721.734a (bia 0001.9721.734a)
  Internet address is 192.168.10.10/30
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

$$Coste = \frac{10^8}{10^9} = 1$$

```
R1Brasil#sh ip ospf int gi0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.10/30, Area 0
  Process ID 1, Router ID 192.168.10.25, Network Type BROADCAST, Cost: 1
```

Tabla 4-14 Cálculo de la métrica en el router de Brasil.

Después de validar los costos de los diferentes enlaces, se revisó la suma de los costos, la validación se realizó desde el router de México hasta el router de Ecuador donde la suma fue de 4, ya que el cáculo de la métrica considera un enlace de México a Panamá con una valor de 1, de Panamá a Chile con un costo de 1, de Chile a Perú con un costo de 1, ya que son enlaces de fibra óptica y de Perú a Ecuador de 1, el valor acumulado se obtuvo, por el protocolo OSPF que calculó la ruta más corta de menor costo, como se indica en la tabla 4-15.

```
      192.168.10.0/30 is subnetted, 14 subnets
O        192.168.10.0 [110/2] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.4 [110/2] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.8 [110/3] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.12 [110/3] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.16 [110/2] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.20 [110/2] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.24 [110/3] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.28 [110/3] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.32 [110/3] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.36 [110/4] via 192.168.10.45, 00:39:31, Serial1/0
O        192.168.10.40 [110/2] via 192.168.10.45, 00:39:31, Serial1/0
```

Tabla 4-15 Ruta más corta de México a Ecuador.

El la figura 4-4 se indican dos diagramas en los que sólo aparecen los enlaces que se recorren durante la trayectoria para llegar al nodo de ecuador desde el nodo de México, en el primer diagrama se indican los costos de cada uno de los enlaces de la trayectoria, para el cálculo del costo acumulado, esta ruta fue calculada por el algoritmo Dijkstra, al ser ejecutado por el protocolo OSPF, es la ruta más corta para llegar a Ecuador, para validar que es la ruta más corta, en el segundo diagrama se trazó otra ruta que se identificó como ruta alterna, se puede ver que el costo acumulado es de 5, es un valor mayor a la ruta del primer gráfico que es de 4, si se presentara algún problema en el enlace de Panamá a Chile del primer gráfico, se calcularía la ruta del segundo diagrama que sería la segunda ruta con el menor costo acumulado.

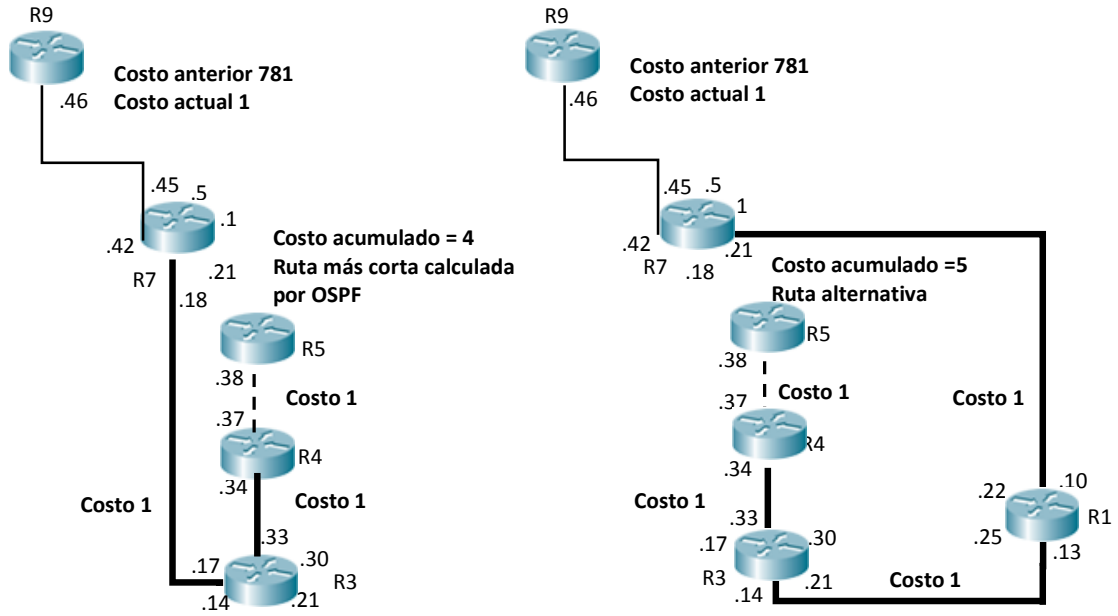


Figura 4-4 Costo acumulado de la ruta más corta y de la ruta alterna. Diagrama propio en base a referencia [40].

Los routers del backbone de CLARA se conectaron en una configuración punto a punto, por lo que se esperaba, una configuración lógica punto a punto, pero sólo las interfaces seriales obtuvieron esta configuración, ya que las interfaces de los routers que se conectaron con fibra óptica, fueron configuradas como una topología de brocadcast de acceso múltiple, en cada una de las interfaces de fibra óptica, el protocolo OSPF las configuró como tipo DR, BDR o Drother.

Después de que el protocolo configurará las interfaces de red, se decidió realizar modificaciones, de tal manera que no se presentaran problemas de comunicación entre los enlaces del Backbone, estas configuraciones se aplicaron al nodo de Brasil, donde se determinó que todas sus interfaces de red quedaran configuradas como DR, de acuerdo a la topología de la red y a la forma en que están conectados los enlaces de la red, el único router, que si llegara a presentar problemas y quedara inhabilitado, todos los demás nodos del backbone tendrían comunicación sin que sus enlaces fueran afectados. El router que se determinó para que uno de sus enlaces se configurara como BDR fue el de panamá que pasaría a tipo DR, si llegara a fallar el router de Brasil, permitiendo tener redundancia entre routers, para mantener la conectividad en todos los enlaces del backbone de la red CLARA.

La configuración que se realizó a todas las interfaces del router de Brasil fue la del cambio de prioridad a 5, para que su configuración de estado quedara como DR, ya que el protocolo OSPF toma el número mayor de prioridad para establecer la interfaz como DR y si son iguales lo determina con la dirección IP mayor de las interfaces, como se indica en la figura 4-5.

```
R1Brasil(config)#int gi0/0
R1Brasil(config-if)#ip ospf priority 5
```

ESTADO DE INTERFACES

Router	IP	Estado	Priority
R1	.10	DR	5
	.13	DR	5
	.22	DR	5
	.25	DR	5

Figura 4-5 Estado de las interfaces del router R1Brasil.Diagrama propio con base en referencia [68].

Después de modificar el valor de prioridad a cada una de las interfaces de red, se validó el valor del estado, donde cambio a DR., como se indica en la tabla 4-16.

```
R1Brasil#sh ip ospf  interface gi0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.10/30, Area 0
  Process ID 1, Router ID 192.168.10.25, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 5
```

Tabla 4-16 Validación del parámetro priority en el router de Brasil.

Otra conexión que es revisó fue el nodo de Perú, el cual tiene una interfaz serial y de fibra óptica, para que no se presentaran problemas con la comunicación del nodo de Chile, se configuró su interfaz de fibra como Drother, con esta configuración el router obtuvo su tabla de ruteo de todos los enlaces de la topología de red sin problemas. Sus dos interfaces quedaron configuradas como se indica a en la figura 4-6.

ESTADO DE INTERFACES

Router	IP	Estado	Priority
R4	.34	Drother	0
	.37	Point to Point	-

Figura 4-6 Estado de las interfaces del router de Perú. Diagrama propio con base en referencia [68].

En la figura 4-7 se indican los estados de todas las interfaces de los routers del backbone de la red CLARA, así como su prioridad, su dirección IP y las interfaces y estados de los vecinos conectados a cada uno de los routers. Se puede ver que cada interfaz de red que fue configurada como Drother está conectada directamente a una interfaz configurada como DR y las que están configuradas como BDR también están conectadas a interfaces DR, no hay interfaces de estados Drother conectados a otra del mismo estado, ni DR conectados a otra del mismo estado o BDR, el protocolo OSPF no permite que se conecten ya que presentarían problemas y no sería posible comunicarse entre los los routers.

Como se indica en la figura 4-7 tenemos más de un router con estados de interfaces DR, los cuales son los nodos de Brasil, Chile y Panamá, estas configuraciones permitieron mantener la transmisión de la información con el protocolo OSPF, en todo el Backbone de la red CLARA.

ESTADO DE INTERFACES

Router	IP	Estado	Priority	IP Vecinos	Estado
R1	.10	DR	5	.9	Drother
	.13	DR	5	.14	Drother
	.22	DR	5	.21	BDR
	.25	DR	5	.26	Doither
R2	.26	Drother	0	.25	DR
	.29	Drother	0	.30	DR
	.50	Drother	0	.49	DR
R3	.14	Drother	0	.13	DR
	.17	Drother	0	.18	DR
	.30	DR	1	.29	Drother
	.33	DR	2	.34	Drother
	.49	DR	1	.50	Drother
R4	.34	Drother	0	.33	DR
	.37	Point to Point	-	.38	Point to Point
R5	.38	Point to Point	-	.37	Point to point
R6	.2	Drother	0	.1	DR
R7	.1	DR	1	.2	Drother
	.5	DR	1	.6	Drother
	.18	DR	3	.17	Drother
	.21	BDR	1	.22	DR
	.42	DR	1	.41	Drother
	.45	Point to Point	-	.46	Point to Point
R8	.41	Drother	0	.42	DR
R9	.46	Point to Point	-	.45	Point to Point
R10	.9	Drother	0	.10	DR
	.6	Drother	0	.5	DR

Figura 4-7 Configuración de los estados de las interfaces de los routers del Backbone. Diagrama propio con base en referencia [68].

Se validó la transmisión de información desde cada uno de los routers y a través de una computadora conectada a Panamá, también se validaron algunos parámetros del protocolo OSPF, después se realizaron pruebas de transmisión desde las herramientas del simulador y se realizó la depuración de paquetes que envía el protocolo OSPF para actualizar las tabla de los estados de enlace.

4.5 Pruebas de OSPF

Se realizó una prueba enviando un mensaje del nodo de Brasil al de Argentina que nos permitió ver el funcionamiento del mensaje hello OSPF, en la figura 4-8 se indica el mensaje OSPF que se encuentra en el nodo de Brasil, que será enviado de la DR 192.168.10.13, a través de la dirección 224.0.0.5

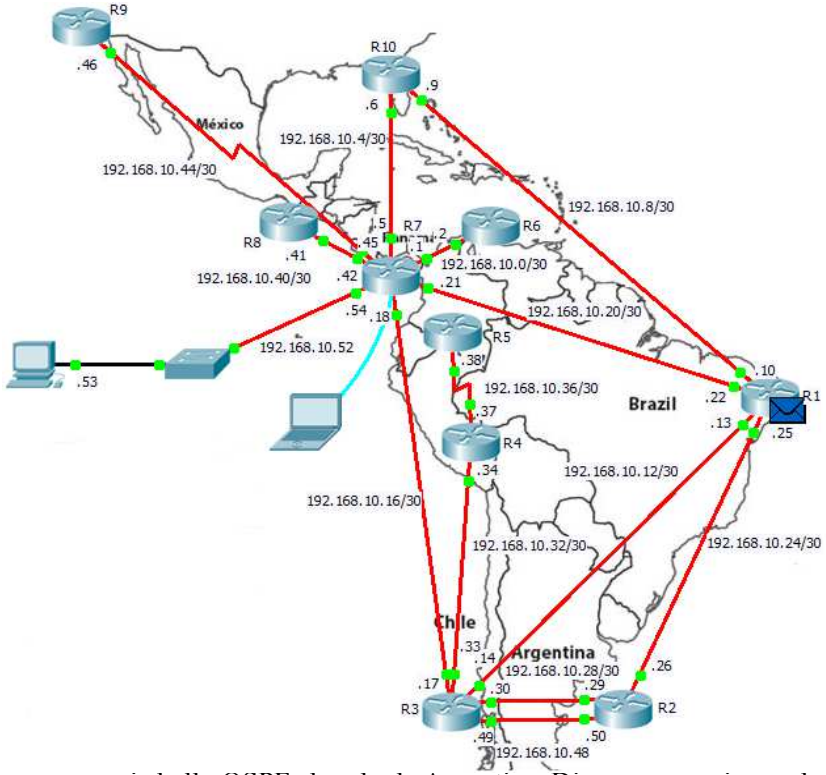


Figura 4-8 Envió de un mensaje hello OSPF al nodo de Argentina. Diagrama propio con base en referencia [68].

El encabezado del paquete de capa 3 muestra la dirección IP origen la cual es la 192.168.10.13; la dirección destino IP multicast que es la 224.0.0.5; los parámetros del mensaje OSP hello nos muestra la versión del protocolo que es la 2; el tipo de mensaje 1 que corresponde al tipo de mensaje hello; la longitud del paquete 45; la IP del Router ID, como estamos en el nodo del Brasil su dirección mayor de IP es la 192.168.10.25; el área a la que pertenece el router que es backbone 0, para todos los routers, la suma de verificación y la autentificación son 0; la máscara de subred que es 255.255.255.252; el intervalo del mensaje

hello que es 10 s; opción y prioridad de router tiene el valor de 0; el dead interval es 40; la dirección IP del router DR la cual es 192.168.10.25; la dirección IP de un router BDR, como la interfaz del router desde donde se va enviar el mensaje solo está conectada a otra interfaces que es Drother; la dirección IP de BDR es 0 y la dirección del vecino es 192.168.10.33, por que el router de Chile tiene más de una interfaz en estado DR, como se indica en la figura 4-9.

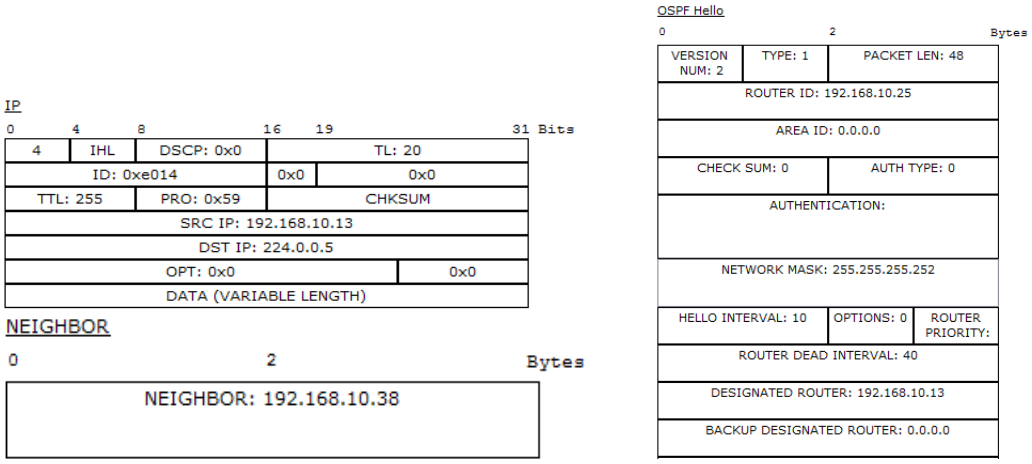


Figura 4-9 Parámetros del mensaje de salida hello OSPF de la interfaz 192.168.10.13 DR del nodo de Brasil. Diagrama con base en referencia [68].

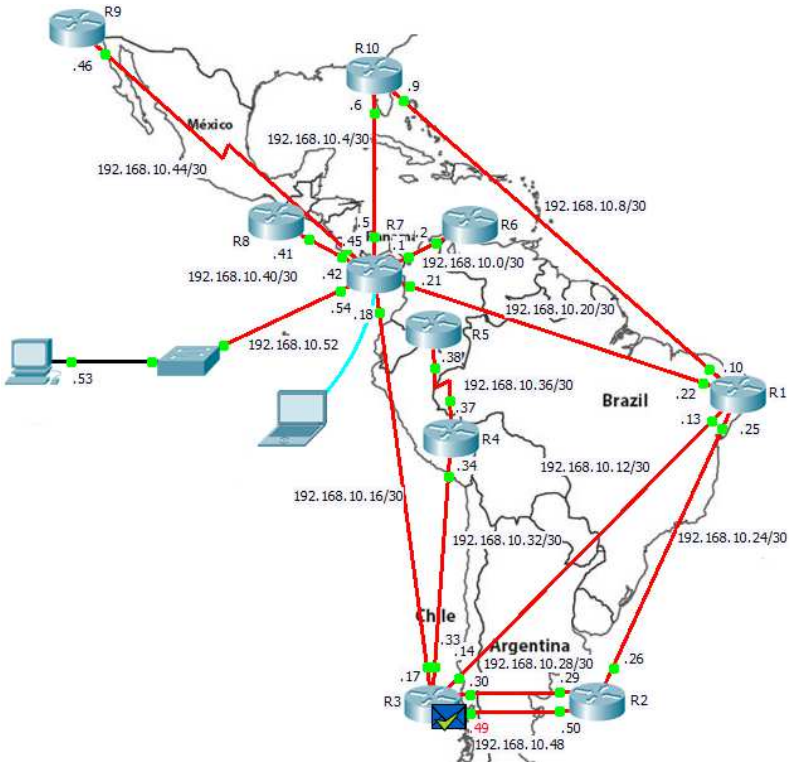


Figura 4-10 Mensaje recibido por el nodo de Argentina. Diagrama propio con base en referencia [68].

En la figura 4-10 se indica, la recepción del mensaje hello enviado desde la interfaz 19.168.1.13 del router de Brasil, el cual llegó a la dirección 192.168.10.14, es importante mencionar que dentro de los parámetros del mensaje no está la dirección IP 192.168.10.14, esto es porque la interfaz 192.168.10.13 que está configurada en estado DR, envía el mensaje a la dirección broadcast 224.0.0.5, pero sólo le llega el mensaje hello OSPF a la interfaz 192.168.10.14 configurada en estado Drother del router de Chile, porque es la única interfaz que está directamente conectada a la interfaz DR 192.168.1.13 del router de Brasil.

Se puede ver el mensaje en el router de Chile, lo que indica que el router recibió el mensaje sin problema, los parámetros del encabezado del paquete IP, y del mensaje hello siguen siendo los mismos de la figura 4-9. En la figura 4-11 se indica un nuevo menaje hello OSPF, que se encuentra en el nodo de Perú, que será enviado al nodo de Ecuador a través de la interfaz serial con la dirección IP 192.168.10.37.

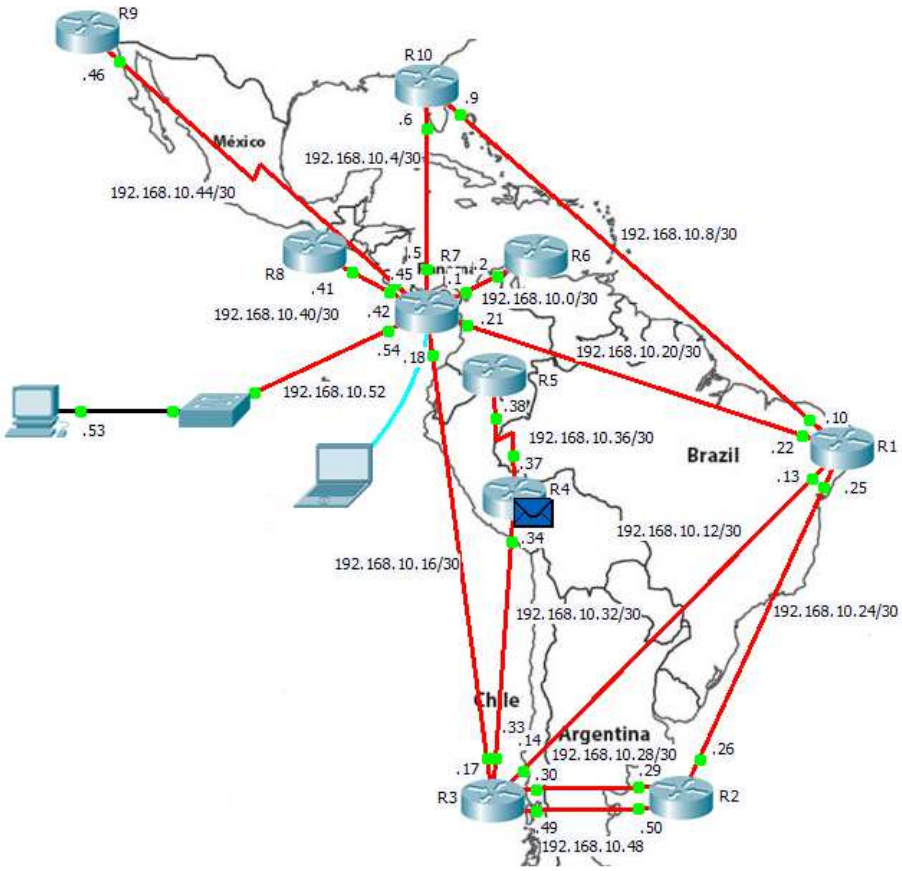


Figura 4-11 Envió de un mensaje hello OSP al nodo de Ecuador. Diagrama propio con base en referencia [68].

En la figura 4-12 se indican los parámetros de un encabezado IP del mensaje que se envió al router de Ecuador, como se puede ver los parámetros similares a los de la figura 4-19, sólo cambia la dirección de origen, que ahora es 192.168.10.37, en el formato del mensaje 3.

En el mensaje OSPF hello, los parámetros que son diferentes son el Router ID que es 192.168.10.37 y la dirección IP del router designated 0, porque la interfaz por la que se enviará el mensaje es serial, la configuración que estableció el protocolo OSPF para estos enlaces es de punto a punto y no como una red de brocadcast de acceso múltiple, donde se establece un DR, BDR y un Drother, la dirección IP de vecino es 192.168.10.38. En la figura 4-13 se indica como el mensaje OSPF llegó al router de Ecuador.

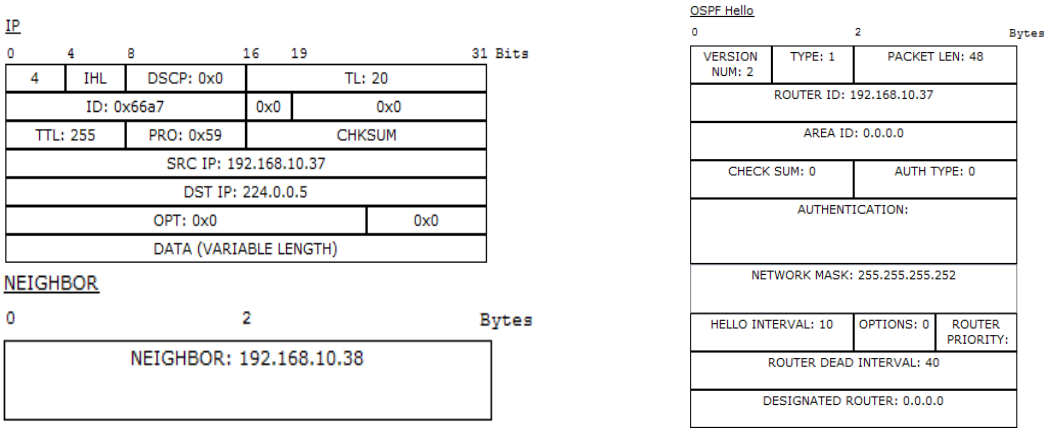


Figura 4-12 Parámetros del mensaje de salida hello OSPF del nodo de Perú. Diagrama con base en referencia [68].

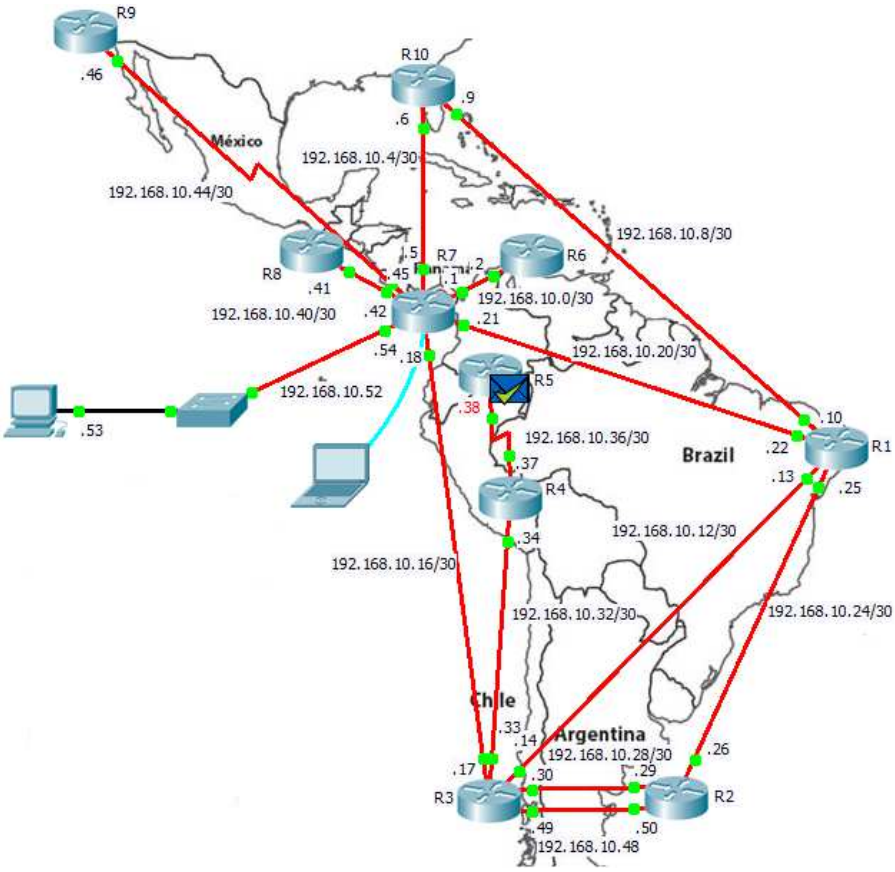


Figura 4-13 Mensaje OPSF hello recibido en el nodo de Ecuador. Diagrama propio con base en referencia [68].

Continuando con las pruebas, del funcionamiento del protocolo OSPF en el backbone de CLARA, se conectó una laptop al router de Panamá, a través de la interfaz de consola, para visualizar los resultados de depuración de mensajes OSPF. Al ejecutar el comando *debug ip packet,* se pueden ver los parámetros que se utilizan para el envío de mensajes de un router. Para el primer mensaje que se visualizó, los parámetros y sus valores son los siguientes: IP origen: 192.168.10.1(local); dirección de origen: 224.0.0.5 (gig3/0); su longitud del mensaje que es de 20; el tipo de envió que es multicast, después de este mensaje; el receptor 192.168.10.2, ya que el mensaje se envió a Colombia; la dirección IP destino que es la 224.0.0.5; la longitud del mensaje que es de 20 y finalmente rcvd2 indica que el nodo con dirección 192.168.10.2 aceptó el mensaje que se le envió, como se indica en la tabla 4-17.

```
R7Panama#debug ip packet
Packet debugging is on
R7Panama#
IP: s=192.168.10.1 (local), d=224.0.0.5 (GigabitEthernet3/0), len 20, sending br
oad/multicast

IP: s=192.168.10.2 (GigabitEthernet3/0), d=224.0.0.5 len 20, rcvd 2

IP: s=192.168.10.54 (local), d=224.0.0.5 (GigabitEthernet7/0), len 20, sending b
road/multicast

IP: s=192.168.10.18 (local), d=224.0.0.5 (GigabitEthernet4/0), len 20, sending b
road/multicast

IP: s=192.168.10.46 (Serial0/0), d=224.0.0.5 len 20, rcvd 2

IP: s=192.168.10.45 (local), d=224.0.0.5 (Serial0/0), len 20, sending broad/mult
icast
```

Tabla 4-17 Parámetros de los diferentes mensajes que se envían a los vecinos de Panamá.

Continuando con la depuración de paquetes de OSPF, se ejecutó el comando *debug ip ospf eventn*, para ver los mensajes que permiten establecer la adyacencia entre los vecinos, como se indica en la tabla 4-18.

```
R7Panama# no debug ip ospf eventn
02:13:24: OSPF: Rcv hello from 192.168.10.33 area 0 from GigabitEthernet4/0 192.
168.10.17

02:13:24: OSPF: End of hello processing

02:13:24: OSPF: Rcv hello from 192.168.10.25 area 0 from GigabitEthernet5/0 192.
168.10.22

02:13:24: OSPF: End of hello processing

02:13:24: OSPF: Rcv hello from 192.168.10.9 area 0 from GigabitEthernet2/0 192.1
68.10.6

02:13:24: OSPF: End of hello processing

02:13:25: OSPF: Rcv hello from 192.168.10.2 area 0 from GigabitEthernet3/0 192.1
68.10.2

02:13:25: OSPF: End of hello processing

02:13:25: OSPF: Rcv hello from 192.168.10.41 area 0 from GigabitEthernet1/0 192.
168.10.41
```

Tabla 4-18 Mensaje OSPF hello enviado a los diferentes vecinos de Panamá.

Al ejecutar el comando se mostrarón los parámetros de los mensajes hello que son enviados al router Panamá, desde las diferentes interfaces que están conectadas directamente al router, los parámetros son: tiempo en que recibe el mensaje el router, para el primer mensaje es 2:13:24; el protocolo, indica desde que

Router ID se recibió el mensaje, la dirección IP es 192.168.10.33; la área 0, la interfaz y dirección IP desde donde se envió el mensaje que es la Gig4/0 con IP 192.168.10.17, en este caso la dirección del Router ID y la dirección IP de origen y la dirección IP de la interfaz de origen, ya no son las mismas. En el tiempo 2:13:25 se indica otro mensaje que es recibido por el nodo de Panamá, en este mensaje las dirección de origen IP 192.168.10.41 y la dirección IP 192.168.10.41 de la interfaz de origen son iguales, esto es porque el mensaje se está enviando desde el nodo El Salvador y el router sólo tiene una interfaz de red, que está directamente conectada al nodo de Panamá, por lo que esa dirección fue asignada al parámetro Router ID. Después de terminar el proceso del envió del mensaje el protocolo indica con un mensaje que el proceso del mensaje hello a finalizado.

El protocolo OSPF envía cada 10 s los mensajes hello, este tiempo se validó durante la depuración de los eventos, en el siguiente listado de eventos se puede ver en el tiempo 2:13:35, diez minutos después de haber enviado su mensaje hello al nodo de El Salvador lo envía de nuevo, de esta forma se validó el tiempo de envió de los mensajes hello en el Backbone de la red CLARA, como se indica en la tabla 4-19.

```
02:13:34: OSPF: Rcv hello from 192.168.10.33 area 0 from GigabitEthernet4/0 192.
168.10.17

02:13:34: OSPF: End of hello processing

02:13:34: OSPF: Rcv hello from 192.168.10.25 area 0 from GigabitEthernet5/0 192.
168.10.22

02:13:34: OSPF: End of hello processing

02:13:34: OSPF: Rcv hello from 192.168.10.9 area 0 from GigabitEthernet2/0 192.1
68.10.6

02:13:34: OSPF: End of hello processing

02:13:35: OSPF: Rcv hello from 192.168.10.2 area 0 from GigabitEthernet3/0 192.1
68.10.2

02:13:35: OSPF: End of hello processing

02:13:35: OSPF: Rcv hello from 192.168.10.41 area 0 from GigabitEthernet1/0 192.
168.10.41
```

Tabla 4-19 Mensaje OSPF hello enviado después de 10s a los diferentes vecinos de Panamá.

CAPÍTULO V EMULACIÓN DEL BACKBONE DE LA RED CLARA

Como una segunda aproximación de la red CLARA se utilizó el emulador GNS3, el cual nos permite trabajar con equipo de backbone como el router 7200, también con las IOS directamente que se utilizan en los equipos reales. Al realizar las configuraciones en el backbone de la red CLARA se ejecutan diferentes comandos para validar los diferentes parámetros del protocolo OSPF, así como la comunicación entre los routers haciendo uso de la herramienta de *wireshark*, a diferencia del simulador en el emulador podemos analizar las LSAs que envía el protocolo entre las interfaces de los routers, también se mide el consumo de recursos utilizados de la PC donde se está realizando la emulación, ya que GNS3 consume más recursos que el simulador Packet Tracer, que puede llegar a inhibir el sistema, esto se soluciona con la activación del parámetro IDLE-PC (Proceso que consume la menor cantidad de recursos de memoria y procesador) que sólo se activa en la emulación de los routers de Cisco, este parámetro permite reducir el consumo de los recursos del procesador y la memoria para que sea utilizada de una manera eficiente y no se dispare el consumo de los recursos, Al emular el backbone de CLARA con GNS3 nos permitió acercarnos más a los valores reales, por lo que se tiene una buena aproximación del backbone. En este capítulo se presenta la emulación de la red avanzada CLARA utilizando en GNS3, se realizan una análisis de su backbone en sus diferentes routers y sus enlaces, para revisar la configuración del protocolo OSPF, la transmisión de la información y los tiempos de respuesta en el envío de la información entre los routers, así como la medición del consumo de la memoria y procesador del simulador.

5.1 GNS3

El software que se utilizó para la emulación de la red avanzada CLARA fue el GNS3, es un emulador de redes de datos, que permite crear entorno de redes virtuales y topologías complejas, que son integrados con simuladores de IOS de los equipos Cisco Systems y JunOS Juniper. El inicio del desarrollo del emulador fue en el 2006 por Jeremy Grossmann, cuando trabajaba en su tesis de maestría [69].

5.1.1 Arquitectura

- Dynamips: Es un emulador de routers, que permite emular diferentes plataformas hardware usando imágenes del sistema operativo Cisco System en un mismo host, las plataformas que emulan se encuentra entre los routers 1700,2600,3700 y 7200. También permite emular switches Ethernet, Frame-Relay y ATM con funcionalidades básica. El emulador de switch de dynamips no es capaz de emular switches, ni de la familia Cisco Catalyst ni Juniper Ex, sino que provee una versión limitada de un switch. Dynamips tampoco es capaz de emular Firewalls PIX, para ello se usa el emulador PEMU a través de Dynagen. Otra característica de operación de dynamips es la de grandes consumos de CPU y de memoria RAM (Random Access Memory), cuando se realiza una emulación, para poder solucionar este problema, se ejecuta la opcón IDLE-PC, el cual sólo se activa en los dispositivos de la familia de Cisco System y no para los de Juniper, el procedimiento permite reducir la cantidad de consumo de CPU en cada emulación, lo que permite que se tenga un consumo más eficiente de los recursos del equipo en el que se ejecuta GNS3 [70].

- Dynagen: Es un *front-end* basado en texto para Dynamips escrito por Gren Anzelli que proveer la administración, mediante CLI (Command Line Interface) de las plataformas emuladas por Dynamips haciendo más fácil su uso. Usa el modo "Hypervisor" para comunicarse con Dynamips y ambas pueden correr en la misma o en ambas PC, simplifica la gestión de las redes virtuales ya que implementa comandos para listar, iniciar, parar, reiniciar, suspender, reanudar los diferentes dispositivos emulados, además determina los valores de IDLE-PC y realiza captura de paquetes.

- Network File: Es un archivo escrito usando sintaxis INI(INI File Syntax), que almacena la configuración de todos los dispositivos de la red de la topología virtual a simular como son los routers switches, las interconexiones entre ellos y las posiciones de los objetos en el diagrama, así como las

etiquetas. El archivo especifica valores tan concretos como los NIO (Descriptores de los Adaptadores de Red) que se encargan de la conexión con equipos reales a los puertos [70].

5.1.2 Herramientas

- QEMU: Es un programa de vitalización de código libre, es utilizado para ejecutar IOS de Cisco ASA ,PIX e IDS, y en el también se puede implementar JUNOS con QEMU emula un sistema informático completo incluyendo procesador y varios periféricos, es usado para proveer hosting virtuales a varios ordenadores virtuales en un único ordenador. QEMU puede a arrancar varios sistemas operativos como Linux, Microsoft Windows, DOS y BSD así como varias plataformas de hardware, incluyendo x86, AMD64, Alpha, Mips y Sparc.

- Virtual Box: Es una aplicación open source de visualización, es una de las herramienta más usada por su interfaz amigable ya que tiene versiones instalables en multitud de Sistemas operativos incluyendo Linux, Windows, Mac. Actualmente se compone de un servicio que maneja las máquinas llamado VboxManage y de varios entornos gráficos o terminales para acceder a las máquinas, también incorpora un modulo PHP, para crear un servidor web donde se muestra la misma interfaz de aplicación y las máquinas virtuales, que son creadas y gestionadas desde el entorno gráfico o directamente desde la línea de comandos mediante VboxManager [70].

- Wireshark: Es una herramienta para la captura de paquetes que pasan a través de los enlaces de comunicaciones de las topologías de red que se realizan en GNS3, como los enlaces Ethernet y seriales. Pueden ser almacenados en archivos *libcap*, para que posteriormente sean interpretados por la aplicación *tcpdump*.

- Simuladores de PC GNS3: Permite a demás de los dispositivos de red la incorporación de PCs en las topologías de redes creadas en el simulador estas simulaciones se pueden realizar con el programa VPC (Virtual PC Simulator) que usa puertos UDP para la comunicación entre el simulador y cada uno de los PCs simulados [70].

En la figura 5-1 se indica la área de trabajo del simulador GNS3, en la cual se puede observar las diferentes áreas de trabajo con las que cuenta, para la emulación de los dispositivos de red.

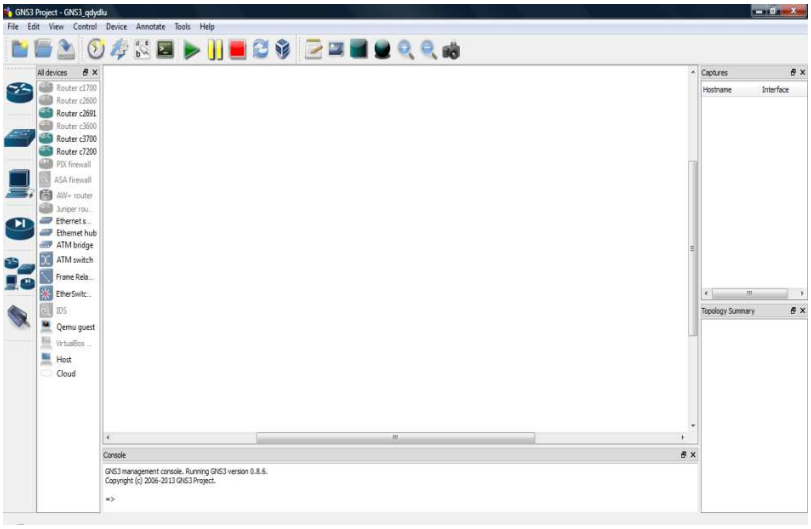


Figura 5-1 Área de trabajo del simulador GNS3. Esquema con base en referencia [71].

5.2 Configuración de los equipos de la red CLARA

La configuración de los equipos de la red avanzada CLARA en la emulación, se realizó con las direcciones IP, que se calcularon en el capítulo IV de la simulación, en el cual se determinaron las direcciones IP clase C, siguiendo el diagrama de simulación que se realizó, donde se indican los routers a utilizar, las direcciones IP asignadas a cada interfaz, las velocidades de los enlaces y las subredes a las que se conectaron cada router del backbone de la red CLARA, como se indica en la Figura 4-2.

La selección del tipo de router fue de acuerdo a las especificaciones técnicas que se requerían, para las diferentes interfaces, que permitieran aproximar a los valores reales en cuanto a la velocidad de transmisión y el ancho de banda, después de realizar una evaluación de los routers que utiliza el emulador GNS3 se determinó utilizar el router de Cisco System 7200 con IOS 12.14, ya que inicialmente se había seleccionado la versión del IOS 12.12, pero presentaba problemas al momento de emular el IOS, ya que no soportaba interfaces de 1G bps que son las que se requieren en la mayor parte de los routers, para la emulación del backbone de la red avanzada CLARA.

Después de seleccionar el router se le asignó a cada uno, las interfaces requeridas, de acuerdo al tipo de nodo que representaría dentro de la red y de los enlaces a los que estarían conectado, en la figura 5-2 se indican las tres diferentes interfaces que se seleccionaron en los diferentes routers.

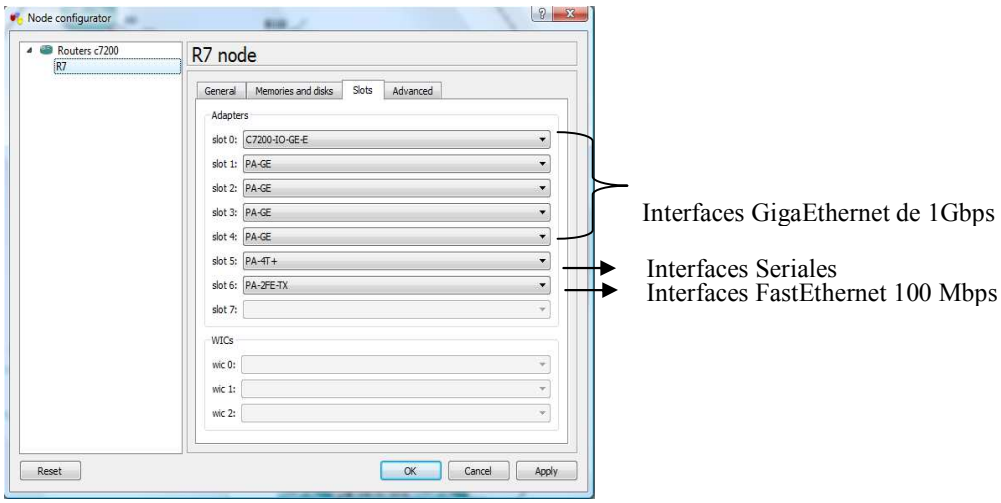


Figura 5-2 Asignación de interfaces de red al nodo 7 de Panamá. Diagrama con base en [71].

Continuando con la configuración, de la red CLARA para la emulación, después de la asignación de interfaces a los routers, se realizó la conexión de los enlaces en las interfaces de cada uno de los routers, como GNS3 no permite trabaja con enlaces mayores a 1 Gbps, en los enlaces en los que se requería de 2.5 Gbps, se trabajó con enlaces de esta velocidad, de igual forma para los enlaces de 155 Mbps y 622 Mbps se emularon

con enlaces seriales a velocidades aproximadas a las reales, el ancho de banda se cambió después de que se configuró el protocolo OSPF en la red, esto para que el protocolo tenga valores exactos de los anchos de banda reales, para que realice el cálculo del costo de manera exacta a los de los enlaces reales y se tenga un funcionamiento del protocolo OSPF más eficiente.

Después de conectar los enlaces en cada una de la interfaces de los routers, se indicó a lo largo de la topología de la red las direcciones IP, el Identificador del router y las subredes a las que se encuentran conectadas cada uno de los routers, como se indica en la figura 5-3.

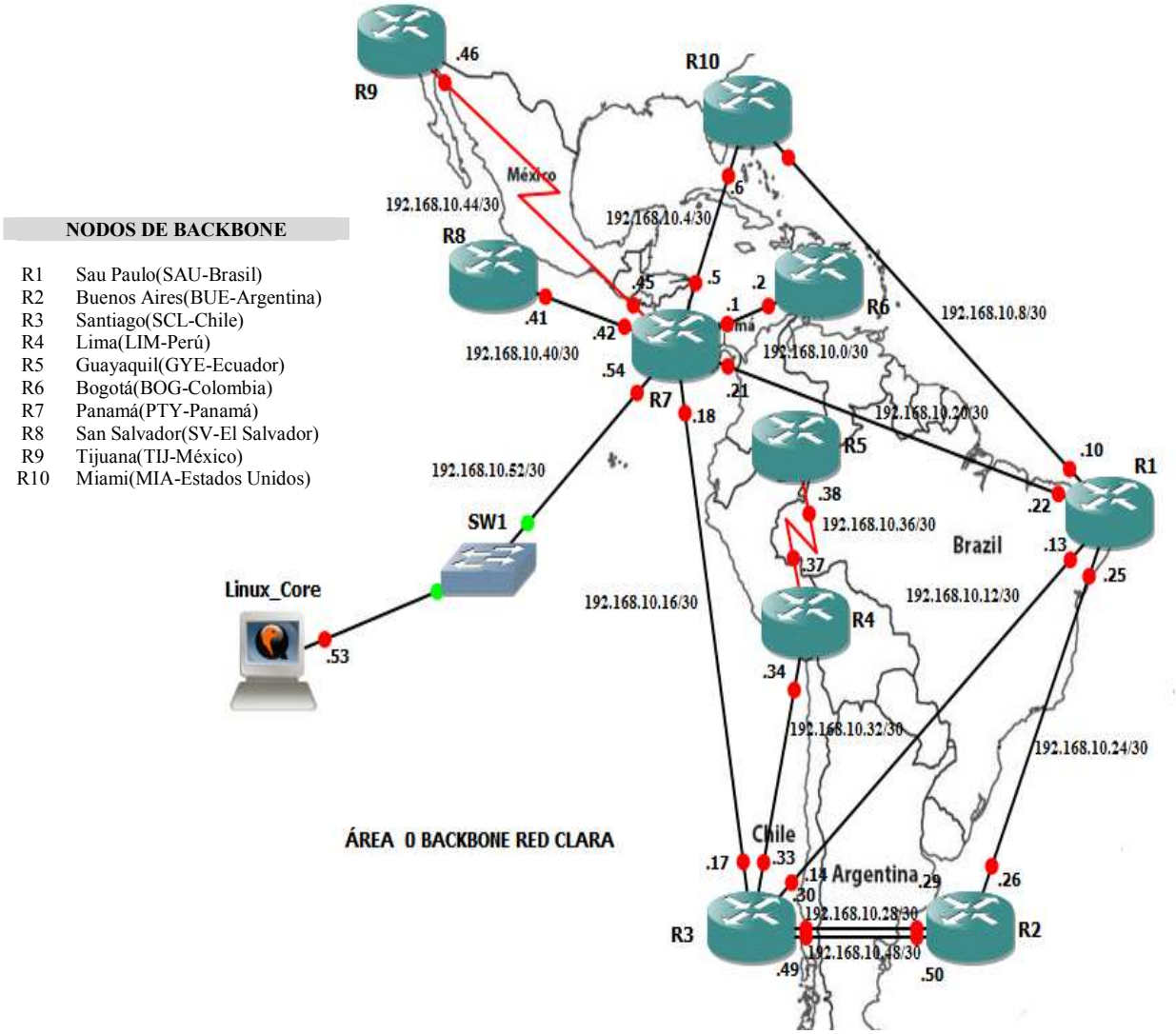


Figura 5-3 Topología del backbone de la red CLARA a emular en GNS3. Diagrama con base en referencia [71].

Después de conectar los enlaces, se continúo con la configuración de la PC que se encuentra conectada al nodo de Panamá en la cual se ejecutó una versión de Linux Tiny Core 2.6.33.3, versión en la que no se cuenta con la interfaz gráfica, para ejecutar las diferentes instrucciones del sistema operativo, los comandos son ejecutados a través del CLI en la cual se ejecutó el comando *root@box:~# ifconfig eth0 192.168.10.53 netmask 255.255.255.252*, para configurar la dirección IP del equipo y el comando *root@box:~# route add default gw 192.168.10.54 eth0* para configurar la dirección IP del Gateway

La ejecución del comando *ifconfig* y *route*, con sus diferentes parámetros de red, para que la PC pueda conectarse al nodo de Panamá. El comando *ifconfig* es utilizado para asignarle a la interfaz eth0 de la PC una dirección IP y una máscara de subred y la instrucción route es utilizada para asignarle la dirección IP de Gateway. Primero se configuró la dirección IP en cada una de las interfaces de los routers con el comando *ip address*, como se indica en la tabla 5-1, se configuró el protocolo OSPF y se agregaron las rubredes al routers como se indica se indica en la tabal 5-2.

```
R1Brasil#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1Brasil(config)#int gi0/0
R1Brasil(config-if)#ip address 192.168.10.10 255.255.255.252
R1Brasil(config-if)#no shutdown
R1Brasil(config-if)#_
```

Tabla 5-1 Configuración de dirección IP.

```
R1Brasil#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1Brasil(config)#router ospf 1
R1Brasil(config-router)#network 192.168.10.8 0.0.0.3 area 0
R1Brasil(config-router)#network 192.168.10.20 0.0.0.3 area 0
R1Brasil(config-router)#network 192.168.10.12 0.0.0.3 area 0
R1Brasil(config-router)#network 192.168.10.24 0.0.0.3 area 0
R1Brasil(config-router)#_
```

Tabla 5-2 Configuración del protocolo OSPF.

Al validar la asignación de las diferentes subredes que se agregaron con el comando *sh ip protocol,* como se indica en la tabla 5-3, se pueden ver las cuatro subredes que fueron agregadas al nodo R1Brasil, el

campo de Gateway se encuentra sin direcciones IP, por ser el primer router que se activó para configurarse, las interfaces de sus vecinos a las que está conectado aún no están activadas ni configuradas, después de que se configuren los routers vecinos y de ejecutar el comando, se mostraran las direcciones IP de Gateway.

```
R1Brasil#sh ip protocol
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.54
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
    192.168.10.12 0.0.0.3 area 0
    192.168.10.20 0.0.0.3 area 0
    192.168.10.24 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

R1Brasil#_
```

Tabla 5-3 Subredes asignadas al router de Brasil en la emulación.

Se ejecutó el comando *ip route*, como se indica en la tabla 5-4 para validar que interfaces del router están directamente conectadas las subredes. En el listado que se muestra se puede ver sólo conexiones directas, ya que como se mencionó anteriormente este es el primer router que se configuró.

```
R1Brasil#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 5 subnets
C       192.168.10.8 is directly connected, GigabitEthernet0/0
C       192.168.10.12 is directly connected, GigabitEthernet2/0
C       192.168.10.20 is directly connected, GigabitEthernet1/0
C       192.168.10.24 is directly connected, GigabitEthernet3/0
R1Brasil#_
```

Tabla 5-4 Direcciones IP asignadas a las interfaces del router de Brasil.

Como se puede ver en las instrucciones anteriores, los comandos y el procedimiento durante la configuración de los routers, fueron los mismos que se realizaron en el capítulo de simulación a diferencia de

que en la emulación se trabaja directamente con los IOS de los routers, otra de las diferencias, es que se realizó la configuración para activar la conexión vía remota, para medir el tiempo de respuesta de los routers esde una conexión remota en cada uno de los routers, la configuración se realizó ejecutando los siguientes comandos, como se indica en la tabla 5-5.

```
R7Panama#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R7Panama(config)#line vty 0 4
R7Panama(config-line)#login local
R7Panama(config-line)#exit
R7Panama(config)#username admin secret cisco
R7Panama(config)#enable secret clara
R7Panama(config)#
```

Tabla 5-5 Configuración del acceso remoto en el router de Panamá.

Las configuraciones se replicaron en cada uno de los routers del backbone de forma ascendente de acuerdo al nombre del router, el primer router que se configuró fue el router R1Brasil y el último en configurarse fue el router R10EEUU.

Otro parámetro que se configuró en los enlaces del backbone de CLARA fue el ancho de banda de los enlaces seriales para que se emularan con los valores reales de transmisión, el primer enlace va del nodo Ecuador al nodo de Colombia, el cual tiene una velocidad de transmisión de 622 Mbps y el otro va del nodo de Panamá al nodo de México a una velocidad de 155 Mbps, así como algunos enlaces de fibra óptica con velocidades de transmisión de 2.5 Gbps y 10G bps. El comando que se utilizó para realizar la modificación fue *bandwidth* como se indica en la tabla 5-6.

```
R5Ecuador#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R5Ecuador(config)#int se2/0
R5Ecuador(config-if)#bandwidth 622000
R5Ecuador(config-if)#_
```

Tabla 5-6 Configuración del ancho de banda.

Es importante mencionar que el cambio que se realizó en los enlaces, sólo fueron considerados para que el protocolo OSPF realizara el cálculo del costo, que es el valor que utiliza el protocolo como métrica y no es considerado para la velocidad de transmisión de los dispositivos ni para los enlaces.

Continuando con la configuración en los dispositivos del backbone de red CLARA, se modificaron la prioridad en algunos dispositivos de red de los routers, para que la topología quedará configurada como en la simulación, en la tabla 5-7 se indica cómo se modificó el parámetro de prioridad.

```
R1Brasil#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1Brasil(config)#int gi0/0
R1Brasil(config-if)#ip ospf priority 5
R1Brasil(config-if)#_
```

Tabla 5-7 Configuración del parámetro prioridad.

Los equipos quedaron configurados como en el capítulo IV con la misma dirección IP y mismas subredes, la diferencia es que ahora se trabaja con routers de backbone cisco 7200, se trabaja directamente con los IOS de los routers y con una PC que emula el sistema Operativo Linux, por lo que es importante reportar las características técnicas del los sistemas operativos que se emulan en la topología de la red CLARA.

En la tabal 5-8 se indica las características de los equipos que fueron asignados a la topología de la red CLARA para su emulación, en la que se describen algunos parámetros de los dispositivos como versión de IOS, modelo de de router, tipo de dispositivo, ID y sistema operativo.

Nombre	Dispositivo	Mod	S.O	Ver.	Interfaz	Dirección IP	Subred	Gateway
R1Brasil	Router	7200	IOS	12.4	Gig0/0	192.168.10.10	192.168.10.8	192.168.10.9
					Gig1/0	192.168.10.22	192.168.10.20	192.168.10.21
					Gig2/0	192.168.10.13	192.168.10.12	192.168.10.14
					Gig3/0	192.168.10.25	192.168.10.24	192.168.10.26
R2Argentina	Router	7200	IOS	12.4	Gig0/0	192.168.10.26	192.168.10.24	192.168.10.25
					Gig1/0	192.168.10.29	192.168.10.28	192.168.10.30
					Gig2/0	192.68.10.50	192.168.10.48	192.168.10.49
R3Chile	Router	7200	IOS	12.4	Gig0/0	192.168.10.14	192.168.10.12	192.168.10.13
					Gig1/0	192.168.10.30	192.168.10.28	192.168.10.29
					Gig2/0	192.168.10.49	192.168.10.48	192.168.10.50
					Gig3/0	192.168.10.33	192.168.10.32	192.168.10.34
					Gig4/0	192.168.10.17	192.168.10.16	192.168.10.18
R4Peru	Router	7200	IOS	12.4	Gi0/0	192.168.10.34	192.168.10.32	192.168.10.33
					Se2/0	192.168.10.37	192.168.10.36	192.168.10.38
R5Ecuador	Router	7200	IOS	12.4	Se2/0	192.168.10.38	192.168.10.36	192.168.10.37
R6Colombia	Router	7200	IOS	12.4	Gi0/0	192.168.10.2	192.168.10.0	192.168.10.1
R7Panama	Router		IOS	12.4	Gig0/0	192.168.10.42	192.168.10.40	192.168.10.41
					Gig1/0	192.168.10.5	192.168.10.4	192.168.10.6
					Gig2/0	192.168.10.1	192.168.10.0	192.168.10.2
					Gig3/0	192.168.10.21	192.168.10.20	192.168.10.22
					Gig4/0	192.168.10.18	192.168.10.16	192.168.10.17
					Se5/0	192.168.10.45	192.168.10.44	192.168.10.46
					F6/0	192.168.10.54	192.168.10.52	-
R8Salvador	Router	7200	IOS	12.4	Gig0/0	192.168.10.41	192.168.10.40	192.168.10.42
R9Mexico	Router	7200	IOS	12.4	Se1/0	19.168.10.46	192.18.10.44	192.168.10.45
R10EEUU	Router	7200	IOS	12.4	Gig0/0	192.168.10.9	192.168.10.8	192.168.10.10
					Gig1/0	192.168.10.9	192.168.10.4	192.168.10.5
Linux_Core	PC	-	Tiny Core	2.6.33 .3	E0	192.168.10.53	192.168.10.52	192.168.10.54
SW1	Switch	-	-	-	1	-	-	-
					2	-	-	-

Tabla 5-8 Características técnicas y direcciones IP de los dispositivos que integran la topología en la simulación de la Red CALRA.

5.3 Validación de los parámetros del protocolo OSPF

Para la validación de los parámetros del protocolo OSPF, se prendieron cada uno de los dispositivos de la topología de la red iniciando por la PC Linux_Core y continuando con los routers de manera ascendente iniciando por R1Brasil y finalizando por R10EEUU. Como se indica en la figura 5-4.

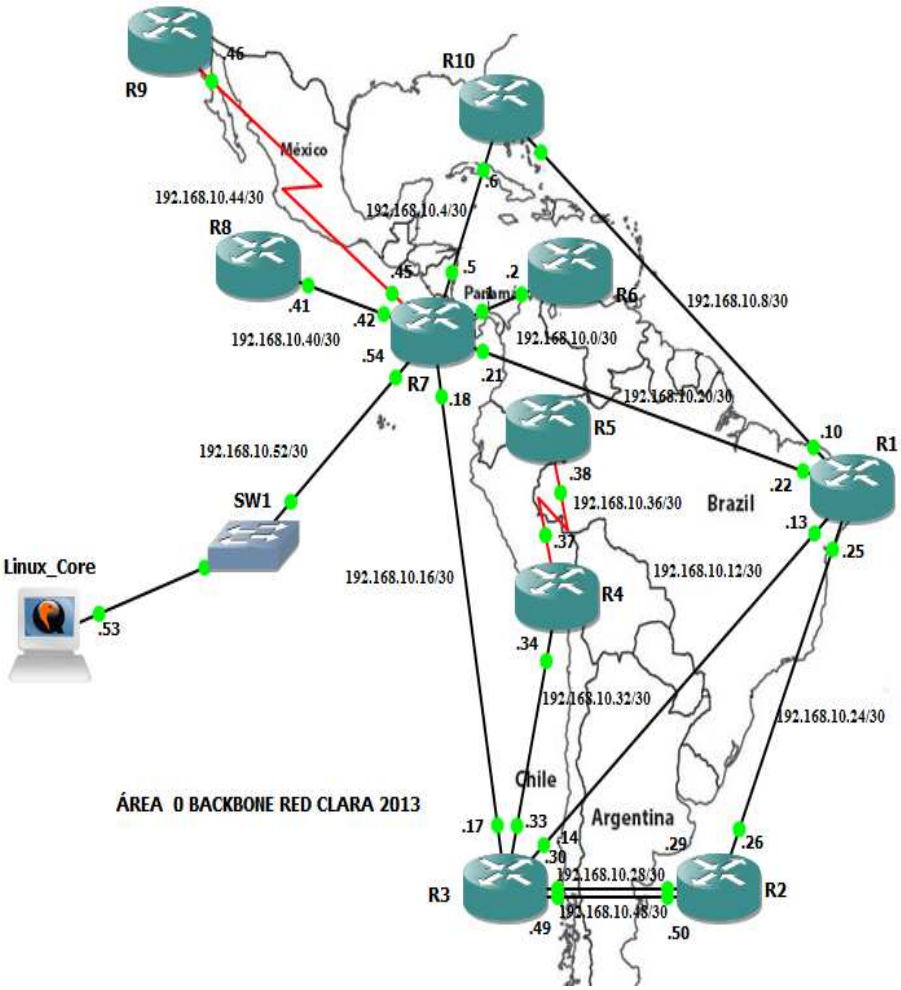


Figura 5-4 Topología del Backbone de la red CLARA, con todos sus dispositivos prendidos para l emulación en GNS3. Diagrama con base en [71].

En la área de trabajo del emulador se encuentra la topología de la red CLARA con todos las interfaces activas, de la PC, el switch y los routers, se muestra un indicador verde cuando están prendidas y uno rojo cuando las interfaces están apagadas.

Durante el proceso de encendido de los routers se presentó un problema con los recursos del consumo del procesador y de la memoria RAM en la laptop donde se emuló la topología de la red CLARA, ya que después de encender el tercer router R1Chile el sistema se saturaba por el consumo del procesador, ya que trabajaba al 100% e inhibía la emulación, como se indica en la figura 5-5.

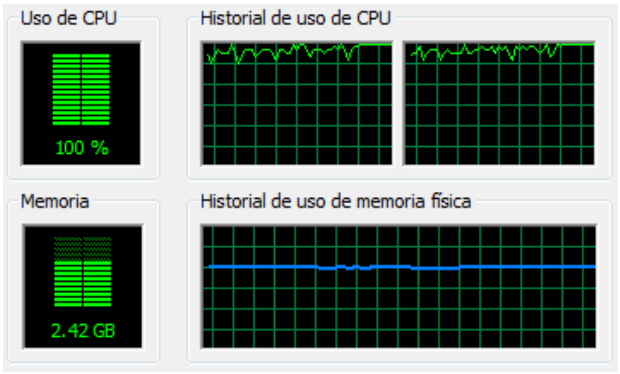


Figura 5-5 Consumo del procesador y de la memoria al encender el router R1chile. Diagrama con base en referencia [72].

Para poder solucionar este problema se ejecutó la opción de IDLE-PC en cada uno de los routers, lo que permitió disminuir el consumo de los recuros de la laptop, para poder seleccionar uno de los valores de la lista calculada por GNS3, los valores que se encuentran marcados por un asterisco, son determinados por el emulador para un correcto funcionamiento, reduciendo el consumos del procesador y la memoria, como se indica en la figura 5-6

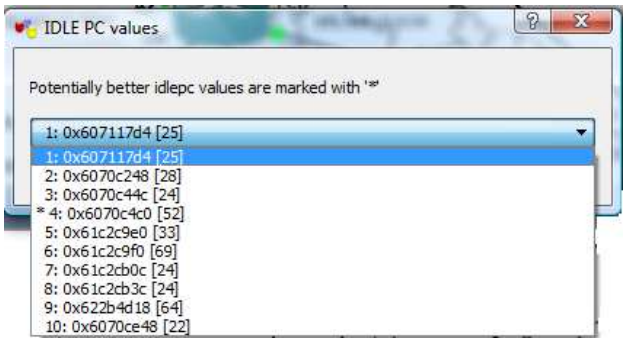


Figura 5-6 Selección del parámetro IDLE-PC, para un bajo consumo de recursos. Diagrama con base en referencia [71].

Durante este proceso de encendido de los routers, se seleccionó el mejor parámetro IDLE-PC, para bajar el consumo de los recursos del sistema y se pudiera continuar con el encendido de todos los routers, después de un tiempo prolongado se logró encender todos los dispositivos de la red con un consumo de recurso de aproximadamente del 50%. En la tabla 5-9 se indica cómo fue aumentando el consumo del

procesador y la memoria durante el proceso del encendido de los dispositivos hasta lograr una ejecución del emulador estable sin que el consumo de los recursos llegara al 100%.

Orden de ON	Dispositivo	Consumo de Memoria	Consumo CPU
1	Linux_Core	2.54 GB	5 %
2	R1Brasil	2.74 GB	15 %
3	R2Argentina	2.84 GB	20 %
4	R3Chile	2.89 GB	27 %
5	R4Peru	3 GB	35 %
6	R5Ecuador	3.15 GB	39 %
7	R6Colombia	3.18 GB	45 %
8	R7Panama	3.24 GB	50 %
9	R8ElSalvador	3.28 GB	60 %
10	R9Mexico	3.30 GB	70 %
11	R10EEUU	3.33 GB	81 %

Tabla 5-9 Consumo de recursos de la laptop durante el proceso del encendido.

Al terminar de encender todos los dispositivos y establecer su parámetro IDLE-PC, después de un tiempo el emulador GNS3 bajo el consumo del procesador y de la memoria, para mantenerlos en los valores que se indica en la figura 5-7.

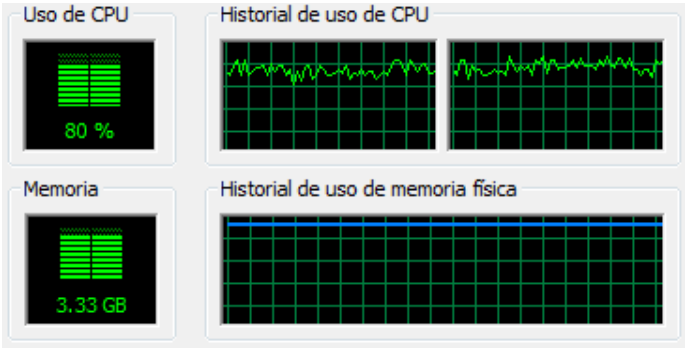


Figura 5-7 Consumo del procesador y de la memoria con la que se realizó la emulación. Diagrama con base en referencia [72].

Después de que el sistema estableció el consumo de los recursos de la laptop, donde se simuló el backbone de la red CLARA, se validaron diferentes parámetros antes de iniciar con las pruebas de transmisión. Se realizó la conexión de los routers conectándose desde la PC Linux_Core vía remota, a través del comando *telnet*, para conectarse a Panamá se ejecutó el comando, que se indica en la tabla 5-10.

```
root@box:~# telnet 192.168.10.54

Entering character mode
Escape character is '^]'.

User Access Verification

Username: admin
Password:
R7Panama>enable
Password:
R7Panama#_
```

```
R7Panama#telnet 192.168.10.17
Trying 192.168.10.17 ... Open

User Access Verification

Username: admin
Password:
R3Chile>enable
Password:
R3Chile#_
```

```
R3Chile#telnet 192.168.10.13
Trying 192.168.10.13 ... Open

User Access Verification

Username: admin
Password:
R1Brasil>enable
Password:
R1Brasil#_
```

Tabla 5-10 Parámetros introducidos en los routers para la conexión vía telnet.

Los primero que se validó fueron las interfaces y sus direcciones IP del nodo de Brasil, como se indica al ejecutar el comado *sh ip int brief*, las subredes asignadas y las direcciones Gateway con el comado *sh ip protocol*, como se indica en la tabla 5-11.

```
R1Brasil#sh ip int brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down

GigabitEthernet0/0         192.168.10.10   YES NVRAM  up                    up

GigabitEthernet1/0         192.168.10.22   YES NVRAM  up                    up

GigabitEthernet2/0         192.168.10.13   YES NVRAM  up                    up

GigabitEthernet3/0         192.168.10.25   YES NVRAM  up                    up

GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down

R1Brasil#_
```

Tabla 5-11 Direcciones IP asignadas a las interfaces del router de Brasil.

Al ejecutar el comando *sh ip protocol* mostró las subredes configuradas en el router, las direcciones IP de los Gateways a los que se conecta y el router ID, como se indica en la tabla 5-12

```
R1Brasil#sh ip protocol
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.25
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
    192.168.10.12 0.0.0.3 area 0
    192.168.10.20 0.0.0.3 area 0
    192.168.10.24 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.37         110      00:49:24
    192.168.10.49         110      00:49:24
    192.168.10.54         110      00:49:24
  Distance: (default is 110)

R1Brasil#_
```

Tabla 5-12 Subredes y Gateways asignado al nodo de Brasil.

Para validar qué vecinos estaban conectados a cada uno de las interfaces del router, la prioridad del enlace y el estado de la interfaz, se ejecutó el comando *sh ip ospf neighbor*, como se indica en la tabla 5-13

```
R1Brasil#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.50     0   FULL/DROTHER    00:00:33    192.168.10.26   GigabitEtherne
t3/0
192.168.10.54     1   FULL/BDR        00:00:35    192.168.10.21   GigabitEtherne
t1/0
192.168.10.49     0   FULL/DROTHER    00:00:39    192.168.10.14   GigabitEtherne
t2/0
192.168.10.9      1   FULL/BDR        00:00:39    192.168.10.9    GigabitEtherne
t0/0
R1Brasil#_
```

Tabla 5-13 Parámetros de los vecinos conectados a Brasil.

Para validar la tabla de las diferentes rutas calculadas por el protocolo OSPF, en la cual también se puede validar la suma de los costos para llegar a una determinada subred como por ejemplo para alcanzar la subred 192.168.10.36 se requiere de un costo de 3 y la ruta seria R3Argentina-R4Peru-R5-Ecuador como se indica al ejecutar el comando *sh ip route*, cualquier otra ruta tomaría un costo mayor de 3 saltos, como por ejemplo la ruta R7Panama-R3Chile-R4Peru-R5Ecuador, para esta ruta el costo sería de un costo de 4, como se indica en la tabla 5-14.

```
R1Brasil#sh ip route_

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 14 subnets
O       192.168.10.32 [110/2] via 192.168.10.14, 01:45:32, GigabitEthernet2/0
O       192.168.10.36 [110/3] via 192.168.10.14, 01:45:32, GigabitEthernet2/0
O       192.168.10.40 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
O       192.168.10.44 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
O       192.168.10.48 [110/2] via 192.168.10.26, 01:45:32, GigabitEthernet3/0
                      [110/2] via 192.168.10.14, 01:45:32, GigabitEthernet2/0
O       192.168.10.52 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
O       192.168.10.0 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
O       192.168.10.4 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
                     [110/2] via 192.168.10.9, 01:45:32, GigabitEthernet0/0
C       192.168.10.8 is directly connected, GigabitEthernet0/0
C       192.168.10.12 is directly connected, GigabitEthernet2/0
O       192.168.10.16 [110/2] via 192.168.10.21, 01:45:32, GigabitEthernet1/0
                      [110/2] via 192.168.10.14, 01:47:53, GigabitEthernet2/0
C       192.168.10.20 is directly connected, GigabitEthernet1/0
C       192.168.10.24 is directly connected, GigabitEthernet3/0
O       192.168.10.28 [110/2] via 192.168.10.26, 01:47:56, GigabitEthernet3/0
                      [110/2] via 192.168.10.14, 01:47:56, GigabitEthernet2/0
R1Brasil#
```

Tabla 5-14 Mejores rutas para alcanzar las diferentes subredes de la topología CLARA desde el nodo de Brasil.

Continuando con la ejecución de los comandos, para la validación de los cambios que se realizaron en el ancho de banda de los enlaces se ejecutó el comando *sh int se1/0* que muestra además del parámetro de ancho de banda la velocidades de las interfaces de GigabitEthernet. En en el listado de la tabla 5-15 se indican los diferentes valores de anchos de banda de las interfaces, con las que se emuló el backbone de la Red CLARA.

```
R9Mexico#sh int se1/0_
 Serial1/0 is up, line protocol is up
   Hardware is M4T
   Internet address is 192.168.10.46/30
   MTU 1500 bytes, BW 155000 Kbit, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
```

```
R5Ecuador#sh int se2/0_
Serial2/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 192.168.10.38/30
  MTU 1500 bytes, BW 622000 Kbit, DLY 20000 usec,
```

```
R3Chile#sh int gi1/0_
GigabitEthernet1/0 is up, line protocol is up
  Hardware is 82543, address is ca07.1128.001c (bia ca07.1128.001c)
  Internet address is 192.168.10.30/30
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
```

```
 R1Brasil#sh int gi2/0_
 GigabitEthernet2/0 is up, line protocol is up
   Hardware is 82543, address is ca04.0554.0038 (bia ca04.0554.0038)
   Internet address is 192.168.10.13/30
   MTU 1500 bytes, BW 2500000 Kbit, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
```

```
R2Argentina#sh int gi2/0_
GigabitEthernet2/0 is up, line protocol is up
  Hardware is 82543, address is ca05.0554.0038 (bia ca05.0554.0038)
  Internet address is 192.168.10.50/30
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
```

Tabla 5-15 Diferentes tipos de ancho de banda que se utilizaron en los enlaces del backbone de CLARA

Otro de los comandos que se ejecutó fue *ip ospf int*, éste nos permitió validad diferentes parámetros del protocolo OSPF entre ellos están la subred a la que está directamente conectada la interfaz, el Id del router, el tipo de red OSPF, el costo, estado, prioridad y área, como se indica en la tabla 5-16.

```
R1Brasil#sh ip ospf int gi0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.10.10/30, Area 0
  Process ID 1, Router ID 192.168.10.25, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 5
  Designated Router (ID) 192.168.10.25, Interface address 192.168.10.10
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1Brasil#_


GigabitEthernet0/0 is up, line protocol is up
  Hardware is i82543 (Livengood), address is ca04.0554.0008 (bia ca04.0554.0008)
  Internet address is 192.168.10.10/30
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

$$Coste = \frac{10^8}{1000000 X 10^3}$$

El valor asignado 1

Tabla 5-16 Validación de la métrica en uno de los enlaces del router de Brasil.

Todos los comandos que se ejecutaron anteriormente en el nodo R1Brasil para validar los parámetros del protocolo OSPF, fueron ejecutados en cada uno de los routers del backbone durante la emulación de la red para conocer las configuraciones que se realizaron en a cada una de las interfaces de los routers y los parámetros del protocolo OSPF que se configuraron.

5.4 Validación de la transmisión en los enlaces de la red CLARA

Para la validación de la transmisión, se estableció la interfaz g4/0 como de captura, en el nodo R7Panamá, para poder capturar los paquetes que se transmiten a través del enlace entre el router de Panamá y Chile, se inicializó la opción de captura en la interfaz, se ejecutó la herramienta de Wireshark y se ejecuto el comando *ping 192.168.10.38* desde la consola de la PC Linux_Core.

Al abrir la herramienta Wireshark se capturaron los paquetes del protocolo OSPF y de ICMP (Internet Control Message Protocol). En la figura 5-8 se indican los paquetes que se capturaron al ejecutar Wireshark, en la columna de origen la dirección IP desde donde se envía el paquete y la dirección IP destino a donde se envía, en la columna de protocolo se muestran los diferentes protocolos a los que pertenece el paquete, los cuales son ICMP y OSPF, también se muestra la longitud y en la columna info se muestra el tipo de paquete que es enviado o recibido.

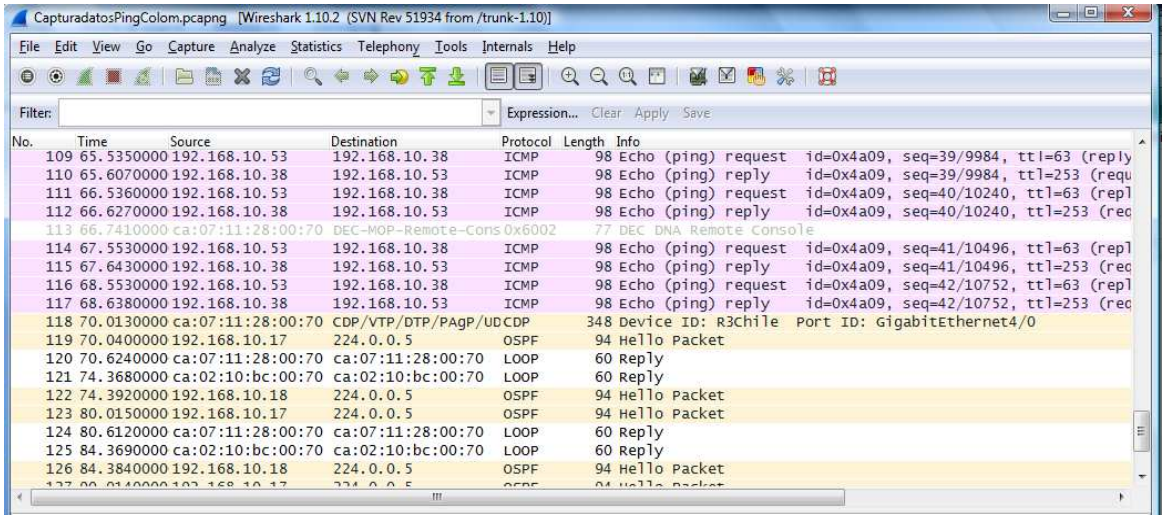


Figura 5-8 Captura de paquetes OSPF e ICMP en Wireshark, que pasan por la interfaz g4/0 del router R7Panama. Diagrama con base en referencia [73].

Los primeros parámetros que se revisaron fueron los del ICMP que se activó al ejecutar el comando ping, en la pantalla de captura de paquetes de Wireshark se pueden ver dos tipos de paquetes ICMP, los cuales son Echo (ping) request, que se envía para hacer una solicitud, esta se realiza desde la dirección IP 192.168.10.53 que fue ejecutada desde la PC Linux_Core y mediante el comando *ping 192.168.10.38*, para el tipo de mensaje de solicitud la dirección origen es 192.168.10.53 y la dirección destino es 192.168.10.38, para el tipo de paquete Echo (ping) reply la dirección origen es 192.168.10.38 que es la dirección del la interfaces del router R5Ecuador y la dirección destino es 192.168.10.53 de la PC Linux_Core como se indica en la figura 5-9.

Time	Source	Destination	Protocol	Length	Info
109 65.5350000	192.168.10.53	192.168.10.38	ICMP	98	Echo (ping) request id=0x4a09, seq=39/9984, ttl=63 (reply
110 65.6070000	192.168.10.38	192.168.10.53	ICMP	98	Echo (ping) reply id=0x4a09, seq=39/9984, ttl=253 (requ

Figura 5-9 Tipos de paquetes ICMP. Diagrama con base en referencia [73].

A continuación se revisaron los paquetes capturados del protocolo OSPF. enviado desde la dirección IP 192.168.10.18 y otro desde la dirección 192.168.10.17, la dirección destino multicast es la 255.0.0.5, estos dos tipos de paquetes fueron capturados a través de la interfaz para capturar los datos que fueron enviados entre los routers, en los cuales se activó el protocolo OSPF, por lo que la interfaz con dirección IP 192.168.10.18 envió el mensajes hello a la dirección 192.168.10.17 y esta misma interfaz también envió mensajes hello a la dirección 192.168.10.18, los mensajes son enviados cada 10 s como se indicó al revisar la teoría del protocolo OSPF, esto se puede ver en la columna time en donde se registra el tiempo en que se capturó el mensaje desde que se inició la captura de paquetes. Para el paquete que se envío del router de Panamá a Chile los tiempos en que se enviaron fueron en 0 s y 10 s, los tiempos en que se enviaron los mensajes desde el nodo de Chile a Panamá fueron 4 s y 14 s, de esta manera se comprueba la parte teórica del envió del mensaje hello cada 10 s, como se indica en la figura 5-10.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.10.17	224.0.0.5	OSPF	94	Hello Packet
2	0.61700000	ca:07:11:28:00:70	ca:07:11:28:00:70	LOOP	60	Reply
3	4.36100000	ca:02:10:bc:00:70	ca:02:10:bc:00:70	LOOP	60	Reply
4	4.37500000	192.168.10.18	224.0.0.5	OSPF	94	Hello Packet
5	9.97500000	ca:07:11:28:00:70	CDP/VTP/DTP/PAgP/UD	CDP	348	Device ID: R3Chile Port ID: GigabitEthernet4/0
6	10.0720000	192.168.10.17	224.0.0.5	OSPF	94	Hello Packet
7	10.6400000	ca:07:11:28:00:70	ca:07:11:28:00:70	LOOP	60	Reply
8	14.3650000	ca:02:10:bc:00:70	ca:02:10:bc:00:70	LOOP	60	Reply
9	14.3830000	192.168.10.18	224.0.0.5	OSPF	94	Hello Packet
10	19.9960000	192.168.10.17	224.0.0.5	OSPF	94	Hello Packet
11	20.6280000	ca:07:11:28:00:70	ca:07:11:28:00:70	LOOP	60	Reply
12	24.3770000	ca:02:10:bc:00:70	ca:02:10:bc:00:70	LOOP	60	Reply
13	24.3910000	192.168.10.18	224.0.0.5	OSPF	94	Hello Packet

10s

Figura 5-10 Captura de paquetes OSPF. Diagrama con base en referencia [73].

Para poder ver los parámetros del mensaje OSPF capturado, seleccionamos una de las cuatro opciones de Wireshark en la que divide la información del protocolo, en la opción de *Frame* se muestra información

como la hora y fecha en que fue capturado el paquete, esta información es generada para todos los protocolos que se muestran en la ventana de captura de paquetes. La opción *Ethernet II*, se refiere a la información de la trama, en las que se muestra la dirección MAC de origen y destino hacia donde se enviará el mensaje. En la opción *Internet Protocol versión 4* muestra información del paquete IP, en la cual se pueden ver los parámetros como la dirección Origen desde donde se envía el mensaje y la dirección destino, así como la dirección destino multicast 254.0.0.5, como se indica en la figura 15-11. Para este ejemplo se revisó el paquete que se envía de la dirección 192.168.10.17 a la interfaz con dirección IP 192.168.10.18 del nodo R7Panama.

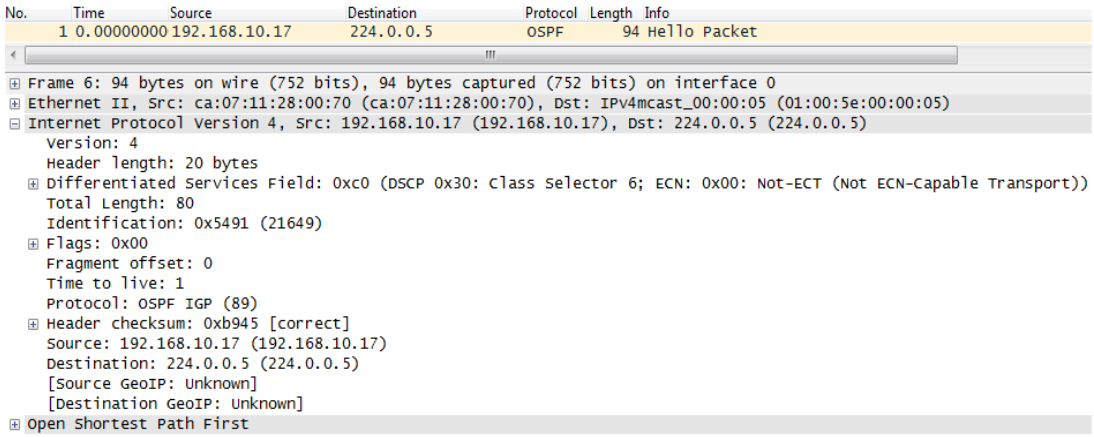


Figura 5-11 Parámetros del protocolo OSPF en un paquete IP versión. Diagrama con base en referencia [73].

Se revisó la opción *Open Shortest Path First* que es donde se encuentran los parámetros específicos del mensajes capturados del protocolo OSPF, en el se indica el tipo de versión del protocolo el cual es 2; el tipo de paquete que es Hello(1) como se indica en la columna de información de la pantalla de captura de paquetes; la longitud de paquete que es de 48; el origen del paquete OSPF; el área que es 0; la suma de verificación; la máscara de subred; el intervalo en que se envía el mensaje como es de tipo hello se envía cada 10s como se indicó en la parte teórica del protocolo OSPF. Así también se pueden ver los parámetro de prioridad; intervalo del mensaje muerto que es de 40 s; la dirección IP del router DR, que es la dirección IP 192.168.10.18 del nodo de R7Panama, ya que fue configurado con este estado y la interfaz del nodo R3Chile con dirección 192.168.10.17 fue configurado como Drother y el ID del router vecino al que está conectada la

interfaz con dirección 192.168.10.17 como se indica en la figura 5-12

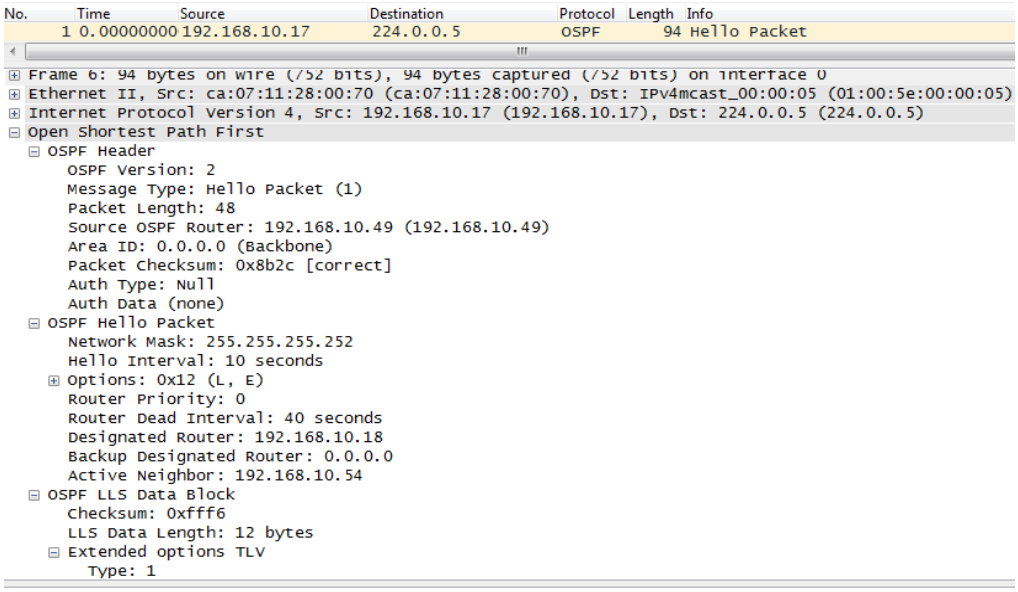


Figura 5-12 Parámetros del protocolo OSPF. Diagrama con base en referencia [73].

Para validar la transmisión de los diferentes paquetes que envía el protocolo OSPF, deshabilitamos la interfaz gi4/0 que tiene asignada la dirección IP 192.168.10.17 para poder ver los paquetes que se envían una sola vez a los routers vecinos después de activarla y revisamos en la pantalla de captura de paquetes los diferentes mensajes que se envían, los cuales son DB, Request, Update y Acknowledge, como se indica en la figura 5-13.

No.	Time	Source	Destination	Protocol	Length	Info
80	270.963000	192.168.10.17	192.168.10.18	OSPF	78	DB Description
81	270.983000	192.168.10.18	192.168.10.17	OSPF	78	DB Description
82	271.013000	192.168.10.17	192.168.10.18	OSPF	138	DB Description
83	271.041000	192.168.10.18	192.168.10.17	OSPF	118	DB Description
84	271.051000	192.168.10.18	192.168.10.17	OSPF	82	LS Request
85	271.053000	192.168.10.17	192.168.10.18	OSPF	78	DB Description
86	271.061000	192.168.10.18	192.168.10.17	OSPF	78	DB Description
87	271.063000	192.168.10.17	192.168.10.18	OSPF	70	LS Request
88	271.073000	192.168.10.17	192.168.10.18	OSPF	178	LS Update
89	271.081000	192.168.10.18	192.168.10.17	OSPF	158	LS Update
90	271.086000	192.168.10.17	192.168.10.18	OSPF	78	DB Description
91	271.096000	192.168.10.18	224.0.0.5	OSPF	94	LS Update
92	271.458000	192.168.10.18	224.0.0.5	OSPF	158	LS Update
93	271.610000	192.168.10.17	224.0.0.6	OSPF	146	LS Update
94	273.191000	192.168.10.17	224.0.0.5	OSPF	94	Hello Packet
95	273.587000	192.168.10.17	224.0.0.6	OSPF	98	LS Acknowledge
96	275.849000	ca:02:12:b0:00:70	ca:02:12:b0:00:70	LOOP	60	Reply
97	275.940000	192.168.10.18	224.0.0.5	OSPF	94	Hello Packet
98	276.088000	192.168.10.18	192.168.10.17	OSPF	158	LS Update
99	276.110000	192.168.10.18	224.0.0.5	OSPF	94	LS Update
100	276.359000	ca:07:09:70:00:70	CDP/VTP/DTP/PAgP/UD	CDP	348	Device ID: R3Ch
101	276.549000	192.168.10.17	192.168.10.18	OSPF	146	LS Update
102	278.619000	192.168.10.17	224.0.0.6	OSPF	98	LS Acknowledge
103	279.992000	ca:07:09:70:00:70	ca:07:09:70:00:70	LOOP	60	Reply
104	281.294000	192.168.10.17	192.168.10.18	OSPF	146	LS Update
105	281.314000	192.168.10.18	192.168.10.17	OSPF	78	LS Acknowledge

Figura 5-13 Captura de diferentes mensajes OSPF. Diagrama con base en referencia [73].

En la figura 5-14 se indican los parámetros de los diferentes mensajes OSPF capturados después de activar la interfaz gi4/0, dentro de los valores del mensaje Request (3), se encuentran el identificador de la LSA que se envía dentro del mensaje OSPF, que son de dos tipos la Router-LSA (1) y la Network-LSA (2), también se muestran los parámetros de los mensajes OSPF de tipo DB Desccription (2), LS Update (4) y LS Acknowledge.

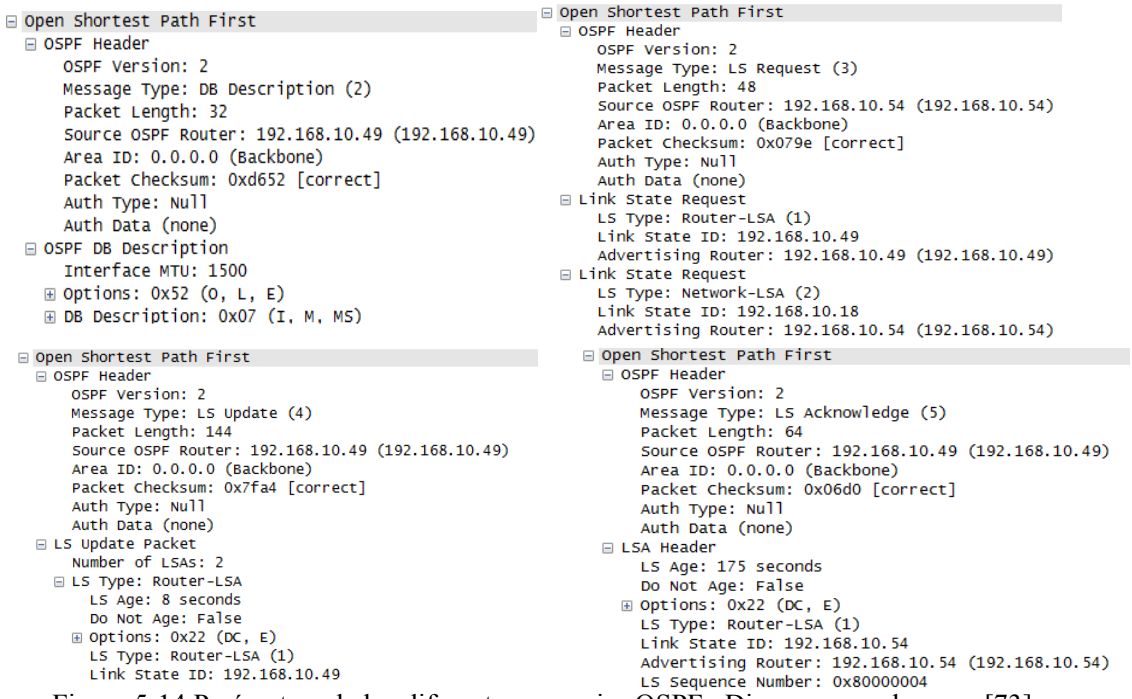


Figura 5-14 Parámetros de los diferentes mensajes OSPF. Diagrama con base en [73].

Con la ejecución del comando *traceroute* desde la PC Linux_Core, se revisó la transmisión entre los nodos de Panamá, Chile, Perú y Ecuador, ya que es una de las rutas más largas desde donde se ejecutó el comando. En la siguiente lista al ejecutar el comando *traceroute* se indican las direcciones IP de las interfaces de los routers, para alcanzar la dirección IP 192.168.10.38, como se indica en la tabla 5-17

```
root@box:~# traceroute 192.168.10.38
traceroute to 192.168.10.38 (192.168.10.38), 30 hops max, 38 byte packets
 1  192.168.10.54 (192.168.10.54)  20.489 ms  16.678 ms  18.038 ms
 2  192.168.10.17 (192.168.10.17)  44.097 ms  28.426 ms  17.728 ms
 3  192.168.10.34 (192.168.10.34)  43.968 ms  49.054 ms  41.766 ms
 4  192.168.10.38 (192.168.10.38)  69.933 ms  65.605 ms  83.003 ms
root@box:~# _
```

Tabla 5-17 Validación de la métrica en uno de los enlaces del router de Brasil.

En la figura 5-15 se indica la mejor ruta que calculó el protocolo OSPF mediante el algoritmo Dijkstra, la cual pasa a través de los routers R7, R3, R4 y finalmente al router R5, con esto se comprobó la transmisión y el cálculo de la mejor ruta.

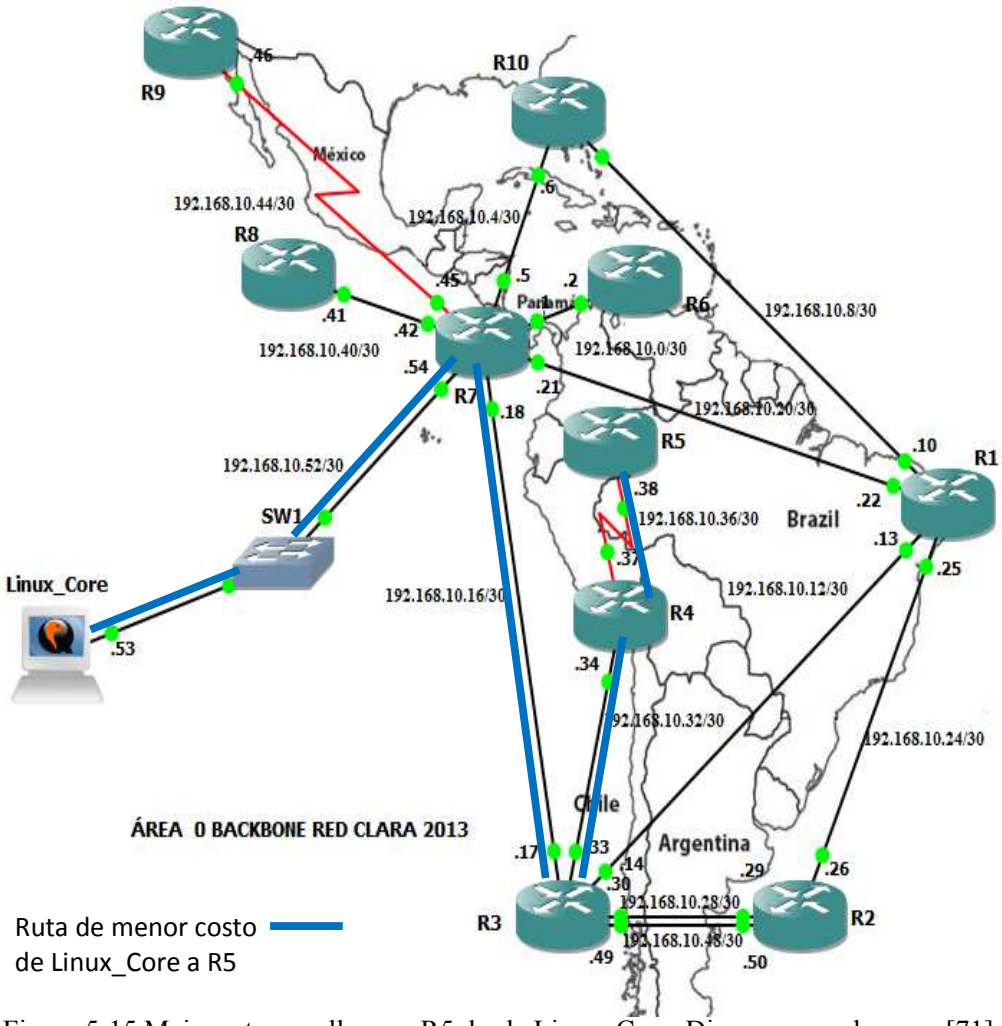


Figura 5-15 Mejor ruta para llegar a R5 desde Linux_Core. Diagrama con base en [71].

En el router de Panamá se ejecutó el comando tracer, que realiza la misma función que el comando traceroute, la lista de direcciones IP de las interfaces son tres, ya que se ejecutó el comando desde el nodo R7Panama como se indica en la tabla 5-18.

```
R7Panama#tracer 192.168.10.38

Type escape sequence to abort.
Tracing the route to 192.168.10.38

  1 192.168.10.17 76 msec 72 msec 12 msec
  2 192.168.10.34 28 msec 36 msec 120 msec
  3 192.168.10.38 104 msec 80 msec 60 msec
R7Panama#*_
```

Tabla 5-18 Tiempos de respuesta al enviar un mensaje al nodo de Ecuador.

Para comprobar el número de salto que realiza el comando *tracer* para alcanzar la dirección IP 192.168.10.38 desde la PC conectada al nodo de Panamá, se ejecutó el comando *sh ip route*, el cual muestra la tabla de rutas, para alcanzar todas las subredes de la topología de la red CLARA, así como su costo, como todos los enlaces tienen costo 1, la suma de los costos para llegar a la subred de 192.168.10.36 es de 3, ya que se alcanza al pasar por 3 enlaces, como se indica en la tabla 5-19.

```
R7Panama#sh ip route_
     192.168.10.0/30 is subnetted, 14 subnets
O       192.168.10.32 [110/2] via 192.168.10.17, 02:08:14, GigabitEthernet4/0
O       192.168.10.36 [110/3] via 192.168.10.17, 02:08:14, GigabitEthernet4/0
C       192.168.10.40 is directly connected, GigabitEthernet0/0
C       192.168.10.44 is directly connected, Serial5/0
O       192.168.10.48 [110/2] via 192.168.10.17, 02:08:14, GigabitEthernet4/0
C       192.168.10.52 is directly connected, FastEthernet6/0
C       192.168.10.0 is directly connected, GigabitEthernet2/0
C       192.168.10.4 is directly connected, GigabitEthernet1/0
O       192.168.10.8 [110/2] via 192.168.10.22, 02:08:14, GigabitEthernet3/0
                     [110/2] via 192.168.10.6, 02:08:14, GigabitEthernet1/0
O       192.168.10.12 [110/2] via 192.168.10.22, 02:08:14, GigabitEthernet3/0
                      [110/2] via 192.168.10.17, 02:08:14, GigabitEthernet4/0
C       192.168.10.16 is directly connected, GigabitEthernet4/0
```

Tabla 5-19 Costo acumulado para alcanzar la subered 192.168.10.36 desde el nodo de Panamá.

Otra de las pruebas de transmisión que se realizaron se muestran en la tabla 5-20 al ejecutar el comando *traceroute* con diferentes direcciones IP, con esto se validó la transmisión de los enlaces de la red.

```
root@box:~#
root@box:~# traceroute 192.168.10.25
traceroute to 192.168.10.25 (192.168.10.25), 30 hops max, 38 byte packets
 1  192.168.10.54 (192.168.10.54)  82.348 ms  30.047 ms  29.380 ms
 2  192.168.10.22 (192.168.10.22)  211.007 ms  52.245 ms  42.218 ms
root@box:~# traceroute 192.168.10.29
traceroute to 192.168.10.29 (192.168.10.29), 30 hops max, 38 byte packets
 1  192.168.10.54 (192.168.10.54)  56.892 ms  53.401 ms  29.072 ms
 2  192.168.10.17 (192.168.10.17)  121.722 ms  58.667 ms  82.490 ms
 3  192.168.10.29 (192.168.10.29)  258.063 ms  112.537 ms  103.703 ms
root@box:~# traceroute 192.168.10.26
traceroute to 192.168.10.26 (192.168.10.26), 30 hops max, 38 byte packets
 1  192.168.10.54 (192.168.10.54)  78.781 ms  36.852 ms  14.592 ms
 2  192.168.10.22 (192.168.10.22)  73.154 ms  53.412 ms  90.595 ms
 3  192.168.10.26 (192.168.10.26)  159.789 ms  103.011 ms  210.098 ms
root@box:~# *_
```

Tabla 5-20 Tiempo de respuesta al enviar un mensaje desde la PC de la topología a diferentes nodos de la red CLARA

Finalmente se ejecutó el comando *ping*, para enviar mensajes de prueba a las direcciones IP 192.168.10.46 al nodo de México, a la dirección IP 192.168.10.38 al nodo de Ecuador y a la IP 192.168.10.41 al nodo de El Salvador, para validar la transmisión y comparar los tiempos de respuesta del mensaje con los resultados obtenidos en la simulación.

Los resultados de la ejecución del comando ping hacia los nodos de México, Ecuador y El Salvador desde Brasil se presenta en la tabla 5-21.

```
R1Brasil#ping 192.168.10.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/68/92 ms
R1Brasil#_


R1Brasil#ping 192.168.10.38

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.38, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/117/180 ms
R1Brasil#_


R1Brasil#ping 192.168.10.41

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.41, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/94/140 ms
R1Brasil#_
```

Tabla 5-21 Tiempo de respuesta al enviar un mensaje desde Brasil a diferentes nodos de la red.

5.5 Consumo de recursos en la emulación de la red CLARA

La emulación del Backbone de la red CLARA se realizó con la versión de GNS3 0.8.6 en una laptop Toshiba Satellite C655 con un procesador AMD Athon(tm) II P340 Dual-Core a 2.20 Ghz, con 4.00 GB de memoria (RAM) y una tarjeta de video ATI Mobility Radeon HD 4200 Series, el sistema operativo en el que se realizó el trabajo fue Windows Vista Home Premium de 32 bits con Service Pack2, como se indica en la figura 5-16

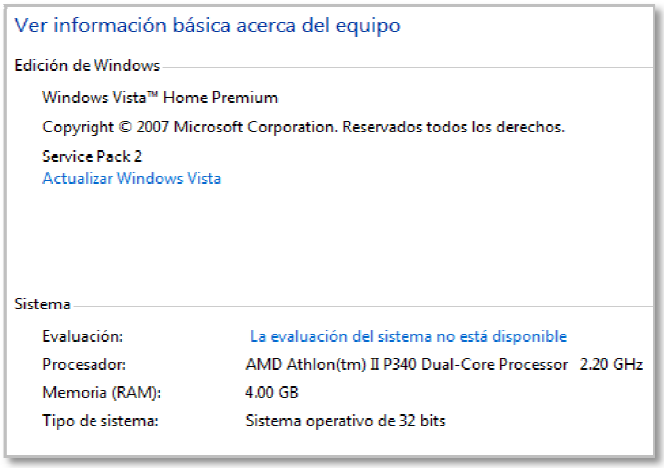


Figura 5-16 Recursos del sistema donde se emuló la topología de la red CLARA [72].

Al inicio del procedimiento de encendido de los dispositivos, el emulador saturó el consumo de la CPU al dispararse a un 100%, cuando se encendió el primer router, como se indica en la figura 15-17.

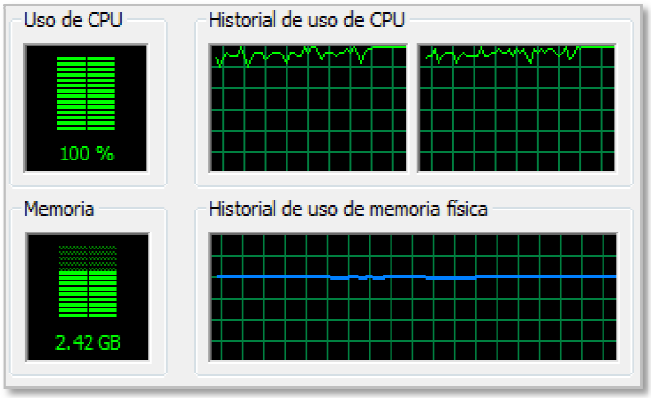


Figura 5-17 Consumo de memoria y del 100% del procesado al encender cada uno de los routers. Diagrama con base en [72].

El problema del consumo del 100% del procesador, se presentó en todos los routers al encenderlos, para poder solucionar este problema se ejecutó el parámetro IDLE-PC en cada router, para que el emulador GNS3 calculará el mejor valor y se le asignará al router, de este manera se reduce el consumo del procesador y la memoria del sistema en donde se está emulando la topología.

En la figura 5-18 se muestra el monitor de recursos del sistema operativo, en el cual se indica la reducción del procesador al 14%, también se indica un historial de la memoria y el procesador, en este último se puede ver que después de que el consumo del procesador llegó a valores muy altos como al 100% bajó para mantenerse en valores menores al 20% y la memoria también bajó a 2.83 GB.

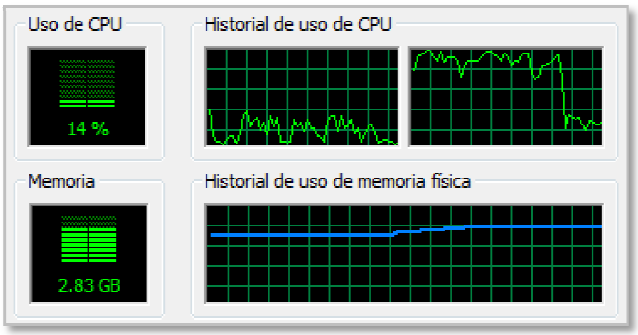


Figura 5-18 Reducción del consumo del procesador a 14% al calcular y asignar el parámetro de IDLE-PC. Diagrama con base en referencia [72].

En la figura 5-19 se indica el consumo del procesador y la memoria después de encender todos los dispositivos del backbone de la red CLARA y durante la emulación para la validación de los parámetros del protocolo OSPF y la validación de la transmisión de todos los enlaces de la topología de la red CLARA.

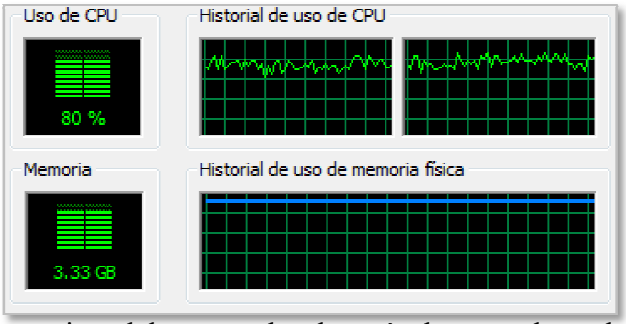


Figura 5-19 Consumo de memoria y del procesador después de encender todos los dispositivos y durante la emulación de toda la topología de red CLARA. Diagrama con base en referencia [72].

En la figura 5-20 se indica los valores del consumo de todos los dispositivos que se encendieron para emular el backbone de la red CLARA conforme se fueron encendiendo los dispositivos, el valor del consumo de procesador se fue incrementado hasta encender el último nodo. El primer dispositivo que se prendió fue la PC generando un consumo de procesador del 5% el segundo fue el R1Brasil generando un consumo de procesador del 15% hasta encender el ultimo nodo R10EEUU que generó el consumo total de la emulación de 81%.

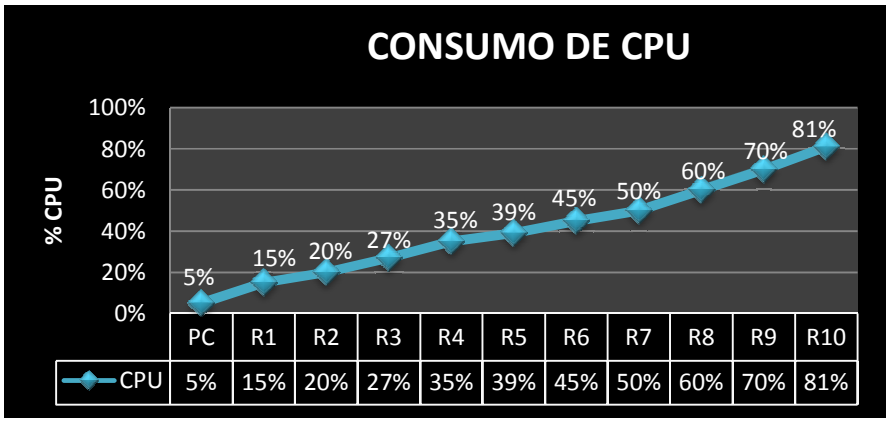


Figura 5-20 Consumo de CPU durante el encendido de los dispositivos de la emulación.

En la figura 5-21 se indica el consumo de la memoria de todos los dispositivos de la topología de la red, conforme se fueron prendiendo los dispositivos, se inició con la PC la cual genero un consumo de 2.54 GB, continuamos con el nodo R1Brasil generando un consumo de 2.74 hasta encender el ultimo nodo R10EE que genero el consumo total de la emulación de 3.33 GB.

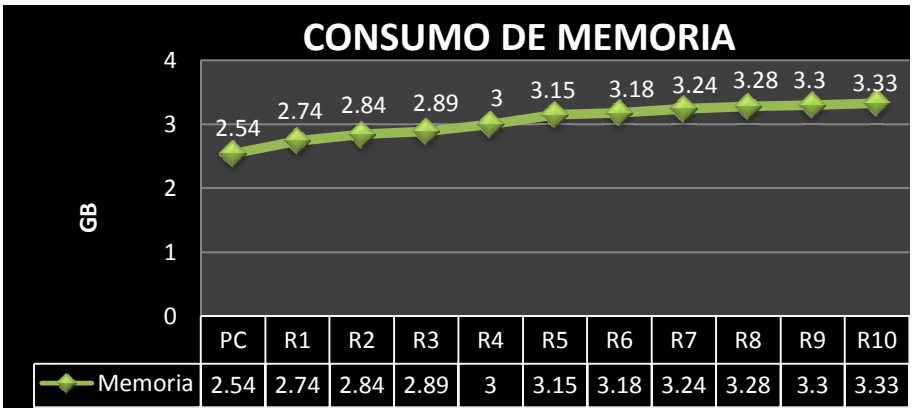


Figura 5-21 Consumo de memoria durante al encender cada uno de los dispositivos de la emulación.

CONCLUSIONES

Como resultado del análisis del backbone de la red avanzada CLARA y para finalizar el presente documento, se listan a continuación las diferentes conclusiones.

I. Con el conocimiento de la infraestructura de una red avanzada CLARA se puede realizar una a aproximación utilizando el simulador Packet Tracer, el cual no cuenta con routers de backbone como el router Cisco 7200, mismo que se utiliza en la infraestructura de la red CLARA; tampoco cuenta con enlaces de fibra óptica mayores a un 1 Gbps, para simular enlaces de 2.5 Gbps y 10 Gbps. En cuanto a los enlaces seriales no permite modificar la velocidad de transmisión, sólo el ancho de banda para calcular el costo de los enlaces para que se tuvieran valores aproximados en los equipos, interfaces y enlaces. Por tanto como una primera aproximación se simuló la topología de CLARA con routers genéricos que permitieran tener enlaces de fibra óptica a lo más de 1 Gbps y enlaces seriales con velocidades de 128 Kbps, con la selección de estos equipos se pudo simular el backbone de CLARA, para validar los parámetros del protocolo OSPF, la transmisión entre cada uno de los enlaces y los tiempos de respuesta de los mensajes enviados entre los routers. Debido a sus limitaciones que tiene para trabajar con equipos de backbone y en cuanto a los resultados que se obtienen al ejecutar los comandos, ya que este simulador no permite trabajar directamente con las IOS de los equipos, no se tiene una aproximación muy cercana a la infraestructura real de la red avanzada CLARA. Sin embargo como una aproximación, permite forzar al simulador.

II. Como segunda aproximación se utilizó el emulador GNS3 el cual permite simular interfaces de red y enlaces de fibra óptica a lo más de 1 Gbps. Para emular el backbone de la red CLARA se requieren enlaces de fibra óptica de 2.5 Gbps y hasta 10 Gbps. Pese a las citadas limitaciones del emulador GNS3 aquellos enlaces de 2.5 y 10 Gbps fueron sustituidos por enlaces de 1 Gbps como una aproximación bajo una configuración punto a punto. GNS3 cuenta con equipos de backbone como los routers Cisco 7200, que fueron

los que se utilizaron en todos los nodos de la topología y se trabaja directamente con los IOS de los equipos físicos, por lo que los valores que se obtuvieron al ejecutar los diferentes comandos para su configuración son similares a los que se ejecutan en un equipo real. Fue posible configurar los equipos del backbone de CLARA en GNS3 y tener comunicación, por lo que se obtuvo una aproximación muy cercana al backbone de la red CLARA

III. Con la configuración de broadcast de acceso múltiple en cada una de las interfaces de fibra óptica en todos los routers, se pudo configurar y activar OSPF sin problema a lo largo de toda la topología de la red. Se realizaron pruebas de tiempo de transmisión de los mensajes OSPF hello y los resultados que se obtuvieron coincidieron con los tiempos teóricos que se revisaron. Un punto importante que hay que resaltar de la emulación es que a pesar de que se configuró como una red de broadcast de acceso múltiple en las interfaces de red, la transmisión de la información se comportaba como un enlace punto a punto, debido a que la conexión entre los routers se realizó en un extremo con una interfaz DR en el otro con una interfaz Drother o BDR. Lo anterior permitió que sólo se enviara un mensaje OSPF o una sola interfaz y no a más de una como se comportan las configuraciones de redes broadcast de accesos múltiple.

IV. En cuanto a consumo de recursos al simular el backbone de la red CLARA en Packet Tracer sólo se requirió del 40% de procesador y de 1.99 GB de memoria, en la emulación con GNS3 se requirió de 80% del procesador y de 3.3GB de memoria. Como se puede ver el consumo de recursos es mayor en el emulador, así que para realizar la emulación del backbone de CLARA, se requiere de un equipo que tenga como mínimo una cantidad de memoria de 4 GB y un Procesador Dual Core a 2.2 Ghz.

V Los tiempos de respuesta que se registraron durante la ejecución del comando ping desde el nodo de Brasil hacia los nodos de México, Ecuador y El Salvador fueron mayores en la emulación, debido a factores

como el consumo de los recursos del equipo donde se hace la emulación. El trabajar directamente con la IOS y el uso de ancho de banda a través de todo el backbone, por el tráfico generado, es lo que retrasa el tiempo de respuesta en la emulación, ya que se trabaja muy cercano al backbone real de CLARA, a diferencia del simulador de Packet Tracer, en el cual, el uso de ancho de banda está determinado por un valor que no se puede modificar, por mucho tráfico que se genere en la simulación.

APÉNDICE A

ALGORITMOS DE ENRUTAMIENTO

Los algoritmos son una ciencia de la inteligencia. Una manifestación natural de la lógica de la inducción matemática. Una serie de propiedades y relaciones se convierten en un vínculo de recurrencia simple y complejidad ilimitada. Y para ver a través de la complejidad profunda se necesita inteligencia. [74].

A.1 Bellman-Ford (Vector de distancia)

El algoritmo de Bellman-Ford, calcula el camino más corto de un grafo dirigido ponderado, en el que el peso (valor numérico que se le a asigna a las aristas de un grafo) de una de las arista o lados puede ser negativo, fue desarrollado por Richard Bellman, Samuel End y Lester Ford, durante la ejecución de este algoritmo, se pueden presentar pesos, ya que es el resultado a la solución del problema del camino más corto, una de los principales problemas de este método para encontrar el camino más corto es que si se tiene en el grafo un ciclo de costo total negativo, entonces este grafo no tendrá solución por el algoritmo. Es importante mencionar que este algoritmo se utilizó en los dispositivos de la red ARPANET [44].

El algoritmo hace uso de la teoría de grafos, el cual es la representación grafica de una estructura de datos a través de aristas (lados), vértices (nodo), así como la asignación de valores a las aristas, estos pueden ser dirigidos, representados por flechas en sus aristas. Como se indica en la figura A-1 [45].

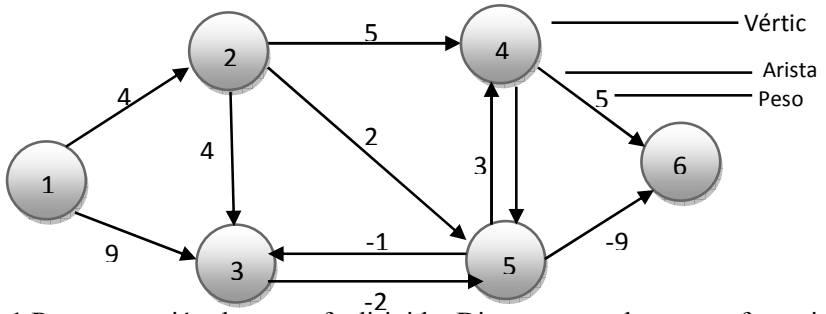


Figura A-1 Representación de un grafo dirigido. Diagrama con base en referencia [45]

En la tabla A-1 se listan las consideraciones para aplicar el Algoritmo Bellman Ford

Apropiado cuando existen distancias negativas
Su complejidad es mayor que la de Dijkstra
Si existen circuitos de longitud negativa, no hay solución
U_j^m Longitud del camino mínimo del nodo origen j usando m aristas
No puede fijarse ningún nodo como permanente hasta el final

Tabla A-1 consideraciones del algoritmo [45].

El algoritmo hace uso de expresiones matemáticas, para realizar el cálculo de la ruta más corta, realizando una serie de procedimiento hasta que se evalúen y se cumplan las condiciones, para que el algoritmo deje de realizar los cálculos y finalmente se tenga el camino más corto. Este procedimiento realiza los cálculos para que se obtenga los pesos menores y con ello determinar la ruta más corta [45].

Para describir el procedimiento que se lleva a cabo durante el cálculo de la ruta, vamos a utilizar el grafo de la figura A-2 [45].

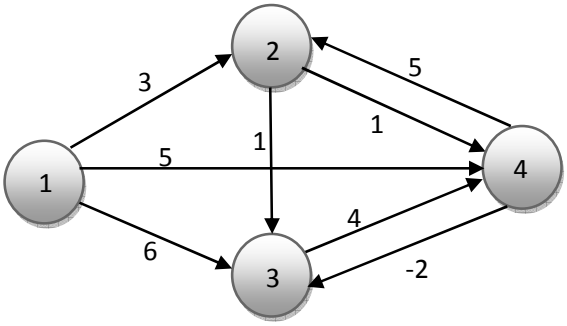


Figura A-2 Representación de un grafo dirigido ponderado. Diagrama con base en referencia [45].

Utilizaremos dos nodos genéricos, etiquetados como i nodo y el nodo j, en una red de n nodos. Ellos pueden estar conectados directamente como un enlace 1-4. Como se puede ver en la figura A-2, sí no consideramos la arista que va del vértice 1 a 4, veríamos que no estaría conectado directamente al nodo 4; en este caso, para encontrar la distancia entre estos dos nodos, tenemos que recurrir al uso de otros nodos y enlaces, por lo que se presentan dos notaciones importantes [45].

d_{ij} = Costo. Enlace entre los nodos i y j

U_{ij} = Costo mínimo de la ruta. Costo calculado del nodo i al nodo j

Sí se tiene un nodo que no se encuentra directamente conectado a un nodo j final, su peso entre este enlace sería infinito, este enlace se podría ver como el grafo del inciso a) de la figura A-3, ya que el nodo K

representa un nodo intermedio entre el nodo origen y el nodo final. Para obtener el valor del peso mínimo de la ruta de i a j se tendría que sumar los pesos del enlace U_{kj} y de $d_{kj,}$ sí se tienen Kn de nodos intermedios como se indica en el grafo del inciso a) de la figura A-3, se tendría que seleccionar la ruta con menor costo.

Sí el nodo 1 y 3 están conectados directamente con un costo de enlace 6 por lo tanto, podemos escribir d_{13}= 6. Por otra parte si no estuvieran directamente conectados, $d_{13} = \infty$, la diferencia de la notación $U_{ij,}$ es que esta representa la ruta de menor costo, si vamos del nodo 1 al 4 tendríamos d_{14}=5, esta ruta pasaría por el nodo 1 y el 4, mientras que la ruta más corta estaría representada por U_{14} =4, que pasaría por el nodo 1 y 2, para llegar al nodo 4. Como se puede ver, un camino de costo mínimo se puede conseguir entre dos nodos en una red, conectando directamente al nodo final o no, siempre y cuando uno de los nodos finales no esté completamente aislado del resto de la red [45].

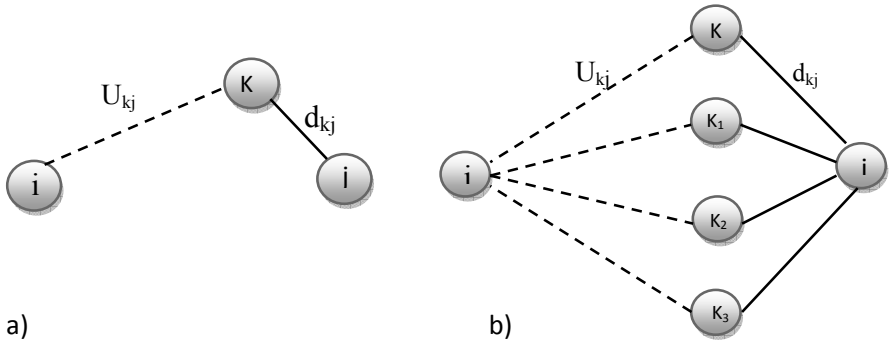


Figura A-3 Representación de un grafo con nodos intermedios. Diagrama con base en [45].

Las siguientes ecuaciones, conocidas como ecuaciones de Bellman-Ford, representan las operaciones y condiciones que se tienen que cumplir, para calcular la ruta más corta.

U_j^m=0 j=m

$$u_j^{m+1} = \forall \min\left\{u_j^m, \min_{k=j}\left\{u_k^m + d_{kj}\right\}\right\}$$

Se define el término con el mínimo costo en términos del número de aristas o arcos de la siguiente manera [45].

U_k^m Costo de la ruta de mínima desde el nodo k con m número de aristas

En la siguiente figura A-4 se indica la estructura del algoritmo, con las expresiones que se ejecuta en cada sentencia de la estructura, así como las condiciones que se evalúan para continuar iterando o para terminar la ejecución del algoritmo [45].

Paso 1 Inicialización

$u_1^1 = 0,\ u_j^1 = d_{1j},\ j = 2,\ldots,n.\ m = 1$

Paso 2 calculamos los caminos mínimos con m+1 aristas

Calcular, para cada $j = 2,\ldots,n,\ u_j^{m+1} = \min\left\{u_j^m, \min_{k=j}\left\{u_k^m + d_{kj}\right\}\right\}$

Si $u_j^{m+1} = u_j^m\ \forall j$ o $m+1 = n-1$ **Parar**

Si no hace m+1 **paso 2**

Figura A-4 Pasos del algoritmo Bellman-Ford [75].

En el siguiente ejemplo se muestra como itera el algoritmo, para cada uno de los nodos, calculando los costos para encontrar la ruta más corta, se tomo como referencia el grafo de la figura A-2, para este ejemplo. Siguiendo con los pasos del algoritmo primero se calculan los valores para el paso 1, en el cual se establece m=1, esto quiere decir que con una arista alcanzamos el nodo j. Realizando el cálculo, tenemos los siguientes valores de pesos: U_1^1 =0, U_2^1=3, U_3^1 =6, U_4^1 =5 m=1

Continuamos con el paso 2, ya que el algoritmo nos indica que después de realizar el cálculo del paso 1 se continua con el paso dos, se incrementa en 1 el valor de m, por lo que ahora se tiene que m=2, que es el número de aristas para alcanzar el nodo j, para la primera iteración de la expresión se calcula la ruta más próxima con dos aristas al nodo destino j=2 desde el nodo origen 1, dentro del cálculo se consideran los nodos

intermedios desde el origen hasta el nodo destino, los cuales se representan por k, se repite el cálculo hasta que j=4 como se indica.

$U_2^2 = \min\{ U_2^1, \min\{ U_2^1 + d_{32}, U_4^1 + d_{42} \}\} = \min \{3, 6 + \infty, 5 + 5\} = 3$

$U_3^2 = \min\{ U_3^1, \min\{ U_2^1 + d_{23}, U_4^1 + d_{43} \}\} = \min \{6, 3 + 1, 5 - 5\} = 3$

$U_4^2 = \min\{ U_4^1, \min\{ U_2^1 + d_{24}, U_3^1 + d_{34} \}\} = \min \{5, 3 + 1, 6 + 4\} = 3$

Como no se cumple la condición de $U_3^2 \neq U_3^1$ y m+1=2≠1, entonces incrementa 1 a m y se ejecuta nuevamente le paso 2, ahora se realizan los cálculos con m=3.

$U_2^3 = \min\{ U_2^2, \min\{ U_3^2 + d_{32}, U_4^2 + d_{42} \}\} = \min \{3, 3 + \infty, 4 + 5\} = 3$

$U_3^3 = \min\{ U_3^2, \min\{ U_2^2 + d_{23}, U_4^2 + d_{43} \}\} = \min \{6, 3 + 1, 4 - 2\} = 2$

$U_4^3 = \min\{ U_4^2, \min\{ U_2^2 + d_{24}, U_3^2 + d_{34} \}\} = \min \{4, 3 + 1, 3 + 4\} = 4$

Como m+1=9=n-1 se para el algoritmo y con los costos obtenidos se puede representar la ruta más corta del grafo como se indica en la figura A-5 [75].

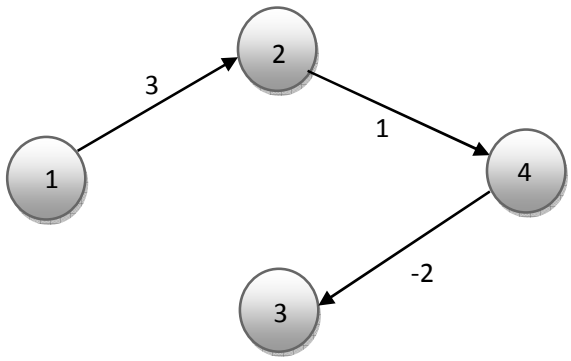


Figura A-5 Ruta más corta, calculada a partir de los cálculos del algoritmo Bellma-Ford. Diagrama con base en referencia [75].

En la tabla A-2 se indican los cálculos realizados para la obtención de la mejor ruta del grafo A-2.

m	U_{12}^m	Ruta	U_{13}^m	Ruta	U_{14}^m	Ruta
0	∞	-	∞	-	∞	-
1	1	1-2	∞	-	4	1-2-4
2	1	1-2	2	1-2-3	4	1-2-4
3	1	1-2	2	1-2-4-3	4	1-2-4
4	1	1-2	2	1-2-4-3	4	1-2-4

Tabla A-2 De los costos mínimos de nodo 1 a otros rutas [75].

A.2 Operación de Bellman-For en una red

En los diferentes dispositivos se realiza el cálculo de los costos de los enlaces a través del algoritmo, para terminar las rudas más cortas para cada router, hasta que convergen los cálculos en cada una de sus tablas de rutas, sí se presenta algún cambio en la topología de la red, el algoritmo realizará nuevamente las operaciones para calcular los costos de los enlaces y actualizar las rutas en cada tabla de ruteo.

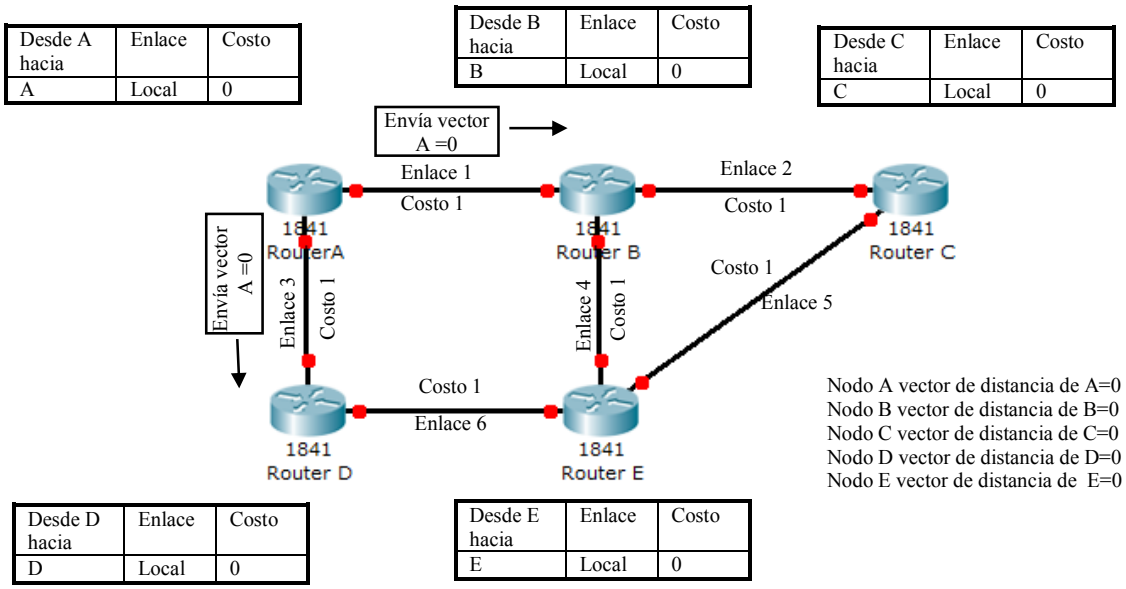


Figura A-6 Inicio del algoritmo Bellman-For en una red. Diagrama propio con base en referencia [76].

En el ejemplo que se presenta, inicialmente se establecen las tablas de rutas en cada uno de los routers en donde el costo de los enlaces que van del router origen al mismo router, se establece su enlace en local y su costo en 0, por ejemplo en el router A la tabla se inicializa en conste 0 ya que su primera ruta va hacia el mismo router A, así como para cada una de los routers de la red, cuando el router A envía el valor de sus rutas que tiene a cada uno de sus routers vecinos, los cuales son el B y el C, para que estos actualicen su tabla de ruteo, la información que envía el router A es el número de enlace y el costo de la ruta que están almacenados en su tabla, cuando el mensaje pasa por el router D, el router incrementa el número de costo de acuerdo al valor de costo que le corresponda al enlace por donde se recibió el mensaje, en el ejemplo cuando llega el mensaje enviado por el router A al router D, este incrementa a 1 el costo de la información que recibe, ya que se recibe el mensaje por el enlace 3 que tiene como sote 1, después de incrementar el valor el router agrega la nueva ruta a su tabla con el nuevo valor del costo, el mismo procedimiento se presenta al enviar la información de la ruta del router A ala B, como se indica en la figura A-6.

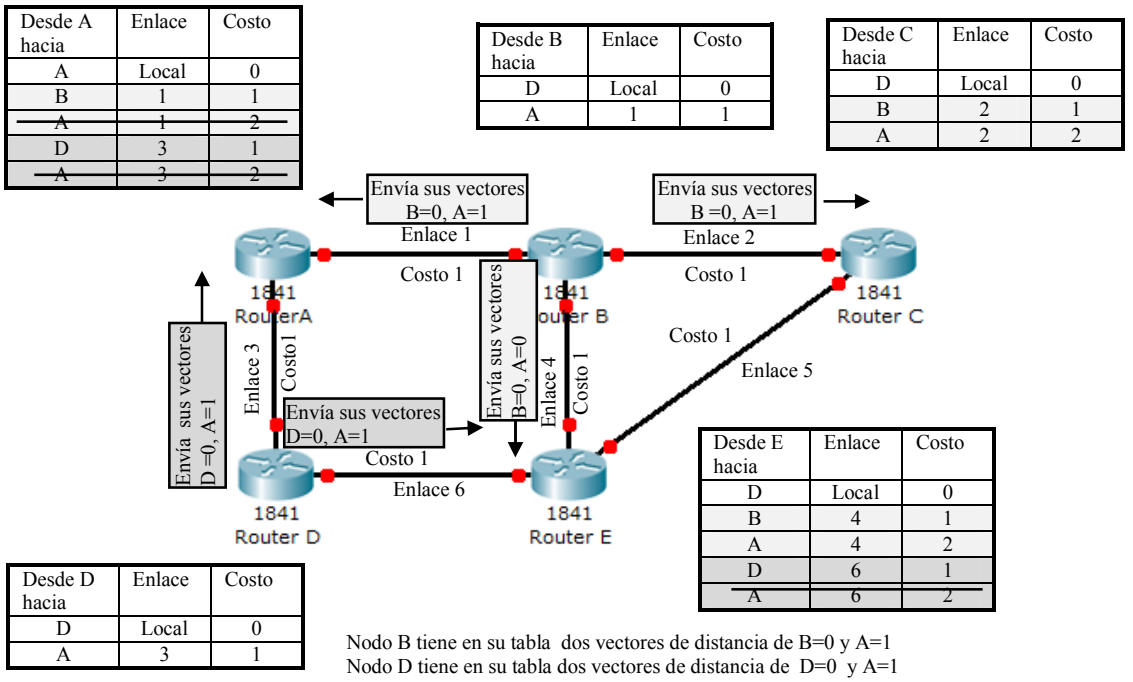
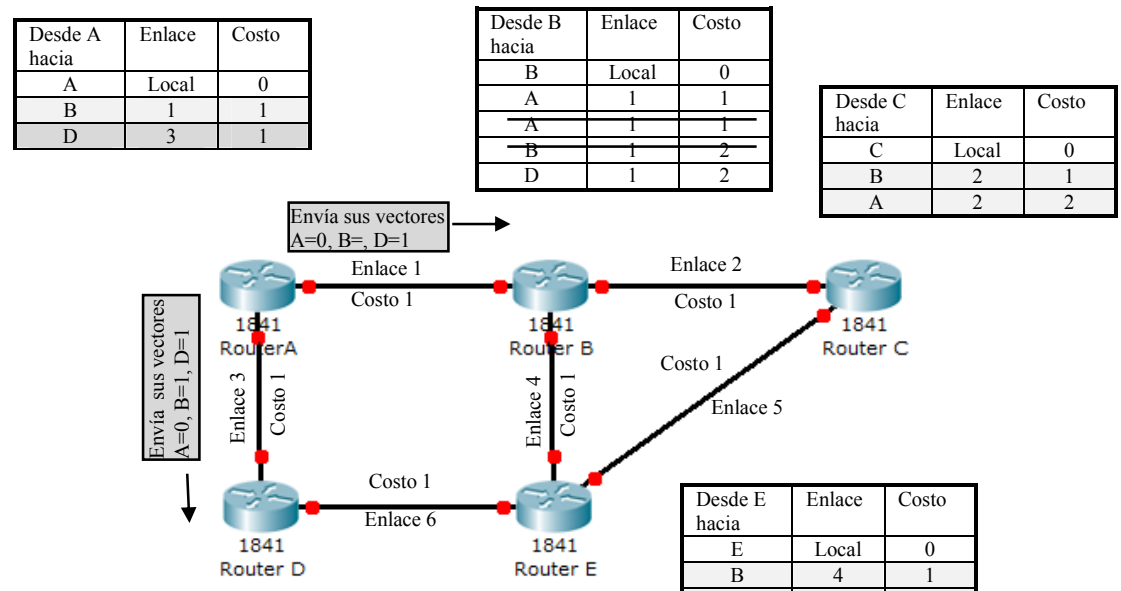


Figura A-7 Procedimiento de actualización de tablas de ruteo en la red. Diagrama propio con base en referencia [76].

Una vez que se actualizaron las tablas de los ruteo B y D, se envía información de su tabla de ruteo del router D al A y al E, así como del router B al A, C y E, como el Router D cuenta con información de 2 rutas la D y la A, esas se envían a el router A para que las agregue a su tabla, pero antes de actualizarla establece el costo de las rutas que envía el router D, por lo que ahora el costo de D será 1 y el enlace 3, para la ruta A sus costo será 2 y su enlace 3, ya que antes de agregarlos a su tabla el route incrementa el costo de a cuerdo al valor del enlace por donde recibe la información, al agregar las rutas probenintes de router D como de router B, se puede ver que se duplica la ruta A, como el algoritmo sólo calcula la ruta más próxima y esto se realiza con el valor de los costos menores, entonces el router de termina que ruta duplicda tiene el menor costo y esa es la que mantiene en su tabla, las demás las elimina, este mismo procedimiento se presenta en el router E, como se índice en la figura A-7



Desde A hacia	Enlace	Costo
A	Local	0
B	1	1
D	3	1

Desde B hacia	Enlace	Costo
B	Local	0
A	1	1
~~A~~	~~1~~	~~1~~
~~B~~	~~1~~	~~2~~
D	1	2

Desde C hacia	Enlace	Costo
C	Local	0
B	2	1
A	2	2

Desde E hacia	Enlace	Costo
E	Local	0
B	4	1
A	4	2
D	6	1

Desde D hacia	Enlace	Costo
D	Local	0
A	3	1
~~A~~	~~3~~	~~1~~
B	3	2
~~D~~	~~3~~	~~2~~

Nodo A tiene en su tabla tres vectores de distancia de A=0, B=1, y D=1
Nodo C tiene en su tabla tres vector es de distancia de C=0, B=1 y A=2
Nodo E tiene en sus tabla tres vectores de distancia de E=0, B=1, A=2 y =1

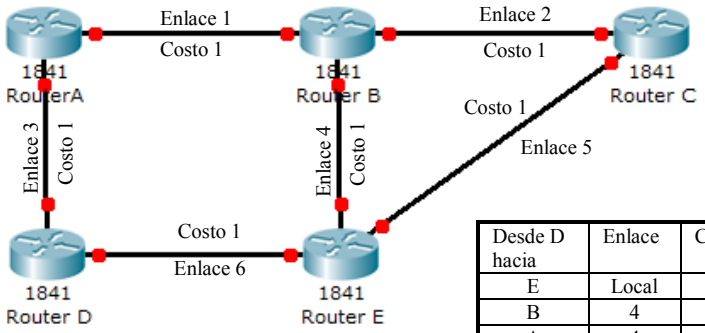
Figura A-8 Actualización de tablas de ruteo en la red. Diagrama propio con base en [76].

Después de hacer las a actualizaciones en las tablas, el router A envía información de las rutas que tiene, al router D y B, enviando dos rutas con sus enlaces y costos, cuando el router B recibe la información, este incrementa el número de costo con el valor que tiene asignado en enlace por donde recibe la actualización de las rutas, en este ejemplo la información la recibe por el enlace 1 con número de costo 1, después de recibir la información e incrementar el costo las agrega a su tabal de ruteo donde se puede ver que se duplica la ruta A y B, pero come se menciono anteriormente el router sólo deja en la tabla las rutas con menor cote cuando estas están duplicada en la tabla. Se marca con una raya las rutas duplicadas que el router eliminará como se indica en la figura A-8

DesdeA hacia	Enlace	Costo
A	Local	0
B	1	1
D	3	1
C	1	2
E	1	2

Desde B hacia	Enlace	Costo
B	Local	0
A	1	1
D	1	2
C	2	1
E	4	1

Desde C hacia	Enlace	Costo
C	Local	0
B	2	1
A	2	2
E	5	1
D	5	2



Desde D hacia	Enlace	Costo
E	Local	0
B	4	1
A	4	2
D	6	1
C	5	1

Desde D hacia	Enlace	Costo
D	Local	0
A	3	1
B	3	2
E	6	1
C	6	2

Figura A-9 Tablas de ruteo actualizadas con las rutas más cortas de la red. Diagrama propio con base en [76].

El proceso de actualización de las tablas se repite, hasta que converjan todas las rutas en todas las tablas de los router de la red, esto se refiere a que cada una de las tablas llegue a tener las rutas de cada uno de

los router con el menor costo, para que se puedan tener las rutas más cortas así cada router, ya que el algoritmo Bellman-Ford realiza el cálculo de las rutas con el costo más bajo y de estos cálculos se determina la ruta más corta. En el grafico A-9 se indica las tablas de ruteo con las rutas más cortas de cada router de la red.

A.3 Algoritmo Dijkstra

El algoritmo Dijktras, también conocido como SPF, que calcula el camino más corto en un grafo, ponderado fue desarrollado por el Físico Holandés Edar W. Dijkstra (1930-2002), quien fuera uno de los primeros en proponer la programación como una ciencia. Ganó el premio Turing Award de la Association for computing Machinery en 1972. Fue designado para presidir el Schlumberger Centennial en Ciencias de la Computación en la Universidad de Texas en Austin, en 1984. Fue un defensor incansable de la simplicidad y elegancia de las matemáticas, las cuales las utilizó como herramientas para solucionar problemas complicados de inteligencia. Se retiró como profesor emérito en 1999 .[48].

Este algoritmo sólo funciona con grafos que no tienen pesos negativos a diferencia del algoritmo Bellman-Ford, también hace uso de la teoría de grafos, para poder realizar el cálculo de los costos menores, basado en el estado de enlace de las aristas. Por lo tanto, una ruta vendrá determinada por la suma de todos los valores numéricos de las aristas por las que pase. Y la ruta optima, será aquella que menor valor numérico calculado tenga. Actualmente lo utiliza Google Maps para obtener la ruta más corta de un punto origen a uno destino. En la tabla A-3 se indican las consideraciones para aplicar el Algoritmo Dijkstra. [4].

Las distancias pueden ser también costos, tiempos, etc.
Si no existe vértice del nodo k al nodo j se asigna $d_{kj} = \infty$
En el caso de un grafo, se considera cada arista como un par de aristas de sentidos opuestos.
Todos los valores de las aristas tiene que ser positivos
El cada etapa se determinan 2 conjutos de nodos: P Formados pro nodos permanente y T por nodos transitorios.
Se denota pred(j) al nodo predecesor de j en el camino del origen a j

Tabal A-3 Consideraciones del algoritmo Dijkstra [75].

El algoritmo hace uso de expresiones matemáticas, para realizar el cálculo de la ruta más corta, realizando una serie de procedimiento hasta que se evalúen y se cumplan las condiciones, para que el algoritmo deje de realizar los cálculos y finalmente se tenga el camino más corto, al ir incrementado los valores numéricos de los vértices de menor peso. Este procedimiento calcula los pesos de cada una de las rutas, para determinar cuál camino tiene el menor peso e integrarlo a la ruta más corta. [76].

En la figura A-10 se indica el algoritmo, con las expresiones que se ejecuta en cada sentencia de la estructura, así como las condiciones que se evalúan para continuar iterando o para terminar la ejecución del algoritmo dependiendo de los valores obtenidos en cada iteración [75].

Sea 1 el nodo origen y $\mathcal{U}_j$ la longitud del camino mínimo del origen al nodo j
$\mathcal{U}_1 = 0$
$\mathcal{U}_j = \min_{k \neq j} \{ \mathcal{U}_j, \mathcal{U}_{jk} + d_{kj} \}$. J = 2,.., n

Paso 0 inicialización

$u_1 = 0, u_j = d_{1j}, j = 2,\ldots,n. P = \{1\}, T = \{2,\ldots,n\}, pred(j) = 1, j = 2,\ldots,n$

Paso 1 Hacer permanente el nodo con longitud mínima

Elegir K $\in T$ tal que $U_k = \min_{j \in T} \{U_j\}$. Hacer P = P U {K}, T= T-{K}

Si T = $\emptyset$ parar

Paso 2. Revisión de los nodos transitorios

Para cada J $\in T$ calcular $U_j = \min \{ U_j, U_{jk} + d_{kj} \}$.

Si se modifica U_j **hacer** *pred(j)* = K

Volver al paso 1

Figura A-10 Pasos del algoritmo Dijkstra [75].

Donde:
1 es el nodo origen
K Conjunto e nodos de la Red
P nodos permanentes
T nodos transitorios
d_{kj} distancia asociada a las aristas
U_j la longitud del camino mínimo del origen al nodo j
pred(j) nodo predecesor de j en el camino del origen a j

Para realizar el análisis de los procedimientos que realiza el algoritmo, para calcular las aristas de menor costo, vamos a realizar un ejemplo, describiendo cada uno de los pasos que se presentan en el algoritmo Dijkstra, utilizando un grafo ponderado con 6 nodos, como el que se indica en la figura A-11.

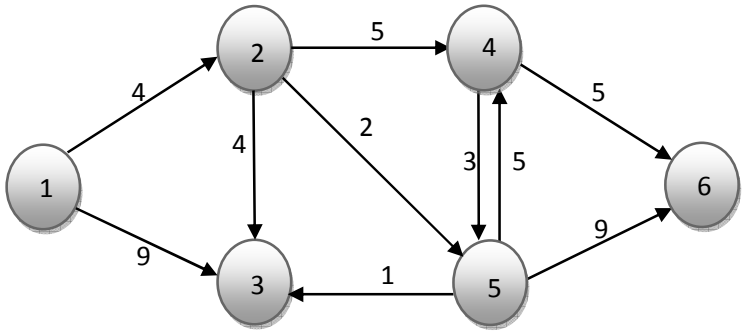


Figura A-11 Grafo dirigido y ponderado, para el algoritmo Dijsktra. Diagrama con base en [75].

Iniciando con el paso 0 del algoritmo, nuestro nodo inicial será 1, por lo que la distancia del nodo 1 al mismo nodo será 0, partimos del nodo 1 para calcular la distancia a los vértices a los que está conectado, como se indica en el grafo A-11, los cuales serán los vértice 2 y 3, los valores obtenidos son los siguientes: [74].

$U_1 = 0,\ U_2 = 4,\ U_3 = 9,\ U_4 = U_5 = U_6 = \infty$ P= $\{1\}$, T = $\{1,3,4,5,6\}$, *pred(j)*= 1, *j*=2,3,4,5,6

En el paso 1, se hace permanente el nodo con longitud mínima, se establece el valor de k con el valor de costo mínimo calculado entre las aristas que se encuentra conectadas del nodo 1 al 2 y del nodo 1 al 3, como la distancia mínima es del nodo 1 al 2 se establece K=2 y el valor de la distancia $U_2 = 4$, así también se identifican los nodos permanentes P y los nodos Transitorios T [75].

K= 2 $U_2 = 4$ P= $\{1,2\}$, T = $\{3,4,5,6\}$

Evaluamos la condición para saber si T = Ø, como no se cumple, porque aún tenemos nodos transitorios, pasamos al paso 2, para realizar los cálculos de las distancias mínimas entre los nodos vecinos del

nodo 2 al 3,4 y 5, al final de realizar el cálculo de la ruta para cada nodo se establece el valor del nodo predecesor *pred(j)* del origen al nodo destino j, para el ejemplo los predecesores de los nodos 3,4,5 será el nodo 2 y para el nodo 6 no tendrá predecesor, ya que su valor de distancia es ∞, como se indicó anteriormente si se calcula la distancia entre un nodo origen y nodo destino que no están directamente conectados su costo será infinito, como se indica en los siguientes cálculos [75].

$U_3 = \min\{ U_3, U_2 + d_{23} \} = \min \{9, 4 + 4\} = 8 \Rightarrow pred(3) = 2$

$U_4 = \min\{ U_4, U_2 + d_{24} \} = \min \{\infty, 4 + 5\} = 9 \Rightarrow pred(4) = 2$

$U_5 = \min\{ U_5, U_2 + d_{25} \} = \min \{\infty, 4 + 2\} = 6 \Rightarrow pred(5) = 2$

$U_6 = \min\{ U_6, U_2 + d_{26} \} = \min \{\infty, 4 + \infty\} = \infty$

Nos regresamos al paso 1 y ejecutamos los cálculos nuevamente, pero ahora con con K=5 y $U_5 = 6$, que se obtuvieron en el paso 2 al calcular las distancias menores entre dos nodos y modificando los nodos permanentes P y transitorios T, como se indica a continuación [75].

K= 5 $U_5 = 6$ P= $\{1,2,5\}$, T = $\{3,4,6\}$

Al final del paso 1 se evalúa nuevamente la condición T = Ø y como no se cumple continuamos en el paso dos, para realizar los cálculo de la distancia más corta con los valores obtenidos en el paso 1, en calculo de U_4, se obtiene 9 que es el mismo valor que se calculó anteriormente y el valor de su predecesor seria *pred(3)* = 5, pero como se pretende encontrar la ruta más corta con el costo mínimo, ya no se toma en cuenta el valor de 5 sino el que se calculó anteriormente y ya no se pone en el cálculo de las expresiones como se indica a continuación [75].

$U_3 = \min\{ U_3, U_5 + d_{53} \} = \min \{8, 6 + 1\} = 7 \Rightarrow pred(3) = 5$

$U_4 = \min\{ U_4, U_5 + d_{54} \} = \min \{9, 6 + 5\} = 9$

$U_6 = \min\{ U_6, U_5 + d_{56} \} = \min \{\infty, 6 + 2\} = 15 \Rightarrow pred(5) = 5$

Regresando al paso 1 con K=3 y con los siguientes valores

K= 3 $U_3 = 7$ P= $\{1,2,5,3\}$, T = $\{4,6\}$

Se evalúa la condición al final del paso 1, como no se cumple la condición T = Ø pasamos al paso 2, para realizar los cálculos de las rutas más cortas con las expresiones como se indica a continuación [70].

$U_4 = \min\{ U_4, U_3 + d_{34} \} = \min \{9, 7 + \infty\} = 9$

$U_6 = \min\{ U_6, U_3 + d_{36} \} = \min \{15, 7 + \infty\} = 15$

Se continua con los cálculos en el paso 1, con los siguientes valores

K= 4 $U_4 = 9$ P= $\{1,2,5,3,4\}$, T = $\{6\}$

Calculamos las distancias entre los nodos en el paso 2, ya que la condición T = Ø sigue sin cumplirse

$U_6 = \min\{ U_6, U_4 + d_{46} \} = \min \{15, 9 + 5\} = 14 \Rightarrow pred(6) = 4$

Después de estas operaciones finalmente se cumple la condición T = Ø en el paso 1, lo cual nos indica en los pasos del algoritmo que se detendrá la ejecución del algoritmo hasta que ya no se tengan nodos transitorios, ya que en cada iteración del algoritmo en el paso 1, uno de los nodos transitorio, pasa a formar parte de los nodos permanentes y este es el que tenga una distancia mínima, calculada en el paso 2 [75].

K= 6 $U_6 = 14$ P = V T = Ø

Para indicar la ruta más corta en el grafo, después de realizar los cálculos de los costos de cada una de las aristas, primero se obtiene la ruta menor calculada en el paso 0, para el ejemplo fue el valor de 4 que va de

nodo 1 a 2, después se toman los valores menores de las distancias calculadas en el paso 2, en cada iteración que se realiza para ese paso, en la primera iteración se obtuvieron los valores 8, 9 , 6 e infinito, por lo que el valor menor es 6 que corresponde al la ruta más corta del nodo origen 1 hasta en nodo destino 5 y su nodo predecesor es 2, en la siguiente iteración del paso 2 se obtuvieron los valores 7, 9 y 15, el valor menor corresponde a la ruta más corta que va del nodo origen 1 hasta el nodo 3 y como nos indica el nodo predecesor de la ruta en los cálculos realizados, la ruta será del nodo origen 1 hasta el nodo 3 pasando por el nodo 2 y el nodo predecesor 5. Finalmente se traza toda la ruta más corta en el grafo como se indica en la figura A-12 y en la tabla A-4 [75].

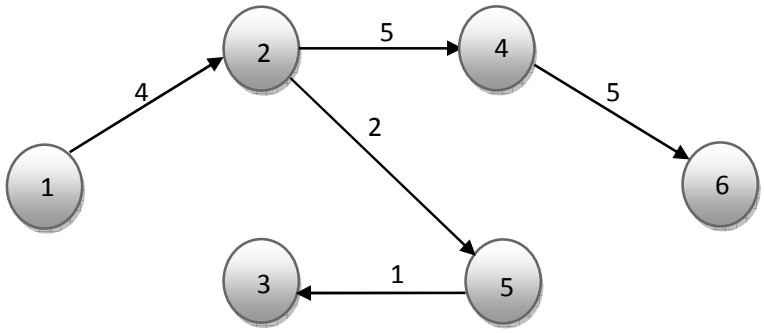


Figura A-12 Ruta más corta calculada con el algoritmo Dijsktra. Diagrama con base en [75].

Paso	N	*U*(2),P(2)	*U*(3),P(3)	*U*(4),P(4)	*U*(5),P(5)	*U*(6),P(6)
1	1	4,1	9,1	∞	∞	∞
2	1,2	-	8,1	9,2	6,2	15,5
3	1,2,5	-	7,5	9,2	-	15,5
4	1,2,5,3	-	-	9,2	-	14,4
5	1,2,5,3,4	-	-	-	-	14,4
6	1,2,5,3,4,6	-	-	-	-	14,4

Tabla A-4 Costo calculados de cada uno de las rutas [75].

A.4 Operación de Dijsktra en una red

En una red los routers envían un mensaje a sus router vecinos, para que estos los puedan identificar y se pueda obtener los datos de cada router vecinos en la red, que posteriormente serán utilizados por el algoritmo Dijkstra, para realizar el cálculo de los costos menores, para obtener la ruta más corta. Como se

puede ver en el gráfico, el nodo A envía un mensaje de descubrimiento a su nodo vecino C como se indica en la figura A-13 [75].

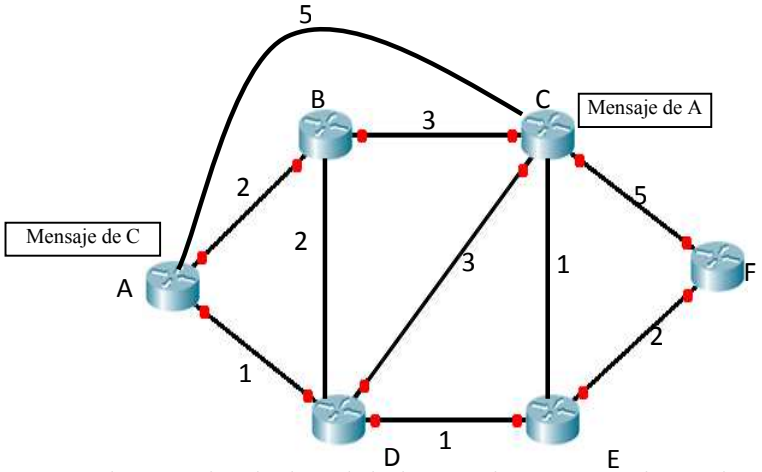


Figura A-13 Envío de mensajes de descubrimiento. Diagrama propio con base en referencia [75].

Posteriormente se crea una base de datos, la cual tendrá los costos de las rutas hacia cada uno de los router, que serán utilizados parara crear la ruta más corta, para cada uno de los dispositivos de la red como se muestra en la figura A-14 a continuación [75].

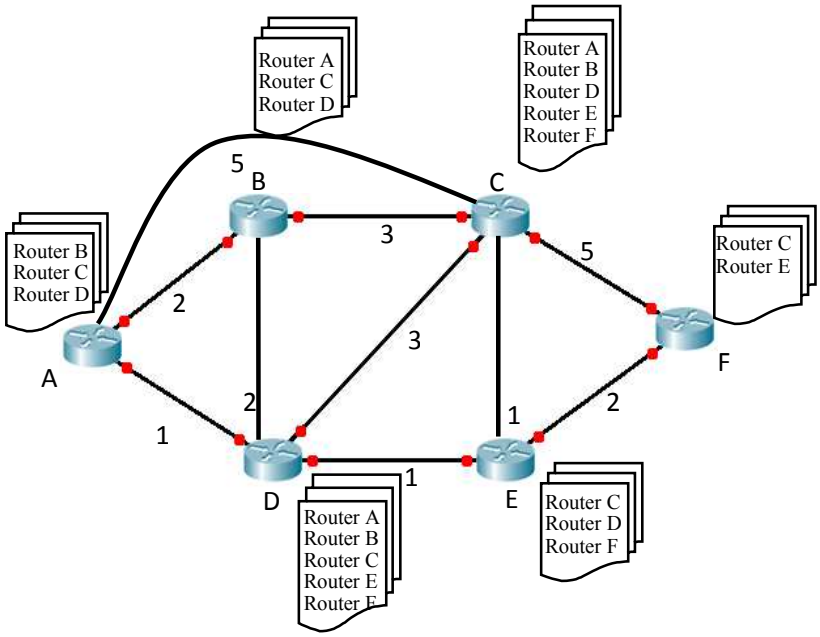


Figura A-14 Calculo de la base de datos de estados de enlace. Diagrama propio con base en [75].

Después cada router envía sus estados a sus routers vecinos, los cuales son enviados a través de mensajes, este proceso se realiza en cada uno de los roters de la red como se indica en el grafico A-15 [75].

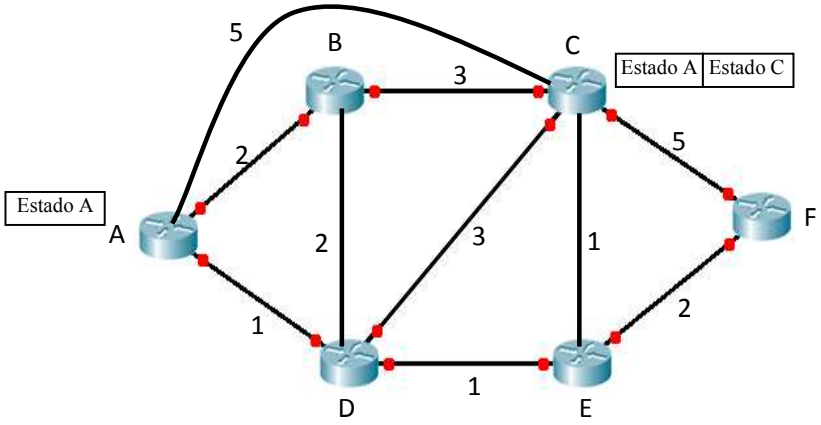


Figura A-15 Envío de mensajes de estado. Diagrama propio con base en referencia [75].

A continuación los routers almacenan en su base de datos todos los estados de los routers, como se indica en la figura A-16. Esta base de datos es idéntica en toda la red. Al obtener la base de datos con todos los estados se ejecuta el algoritmo Disjktra en cada uno de los router, realizando los cálculos numéricos con las expresiones que se presentaron en el ejemplo anterior, para que se obtenga la ruta más corta [75].

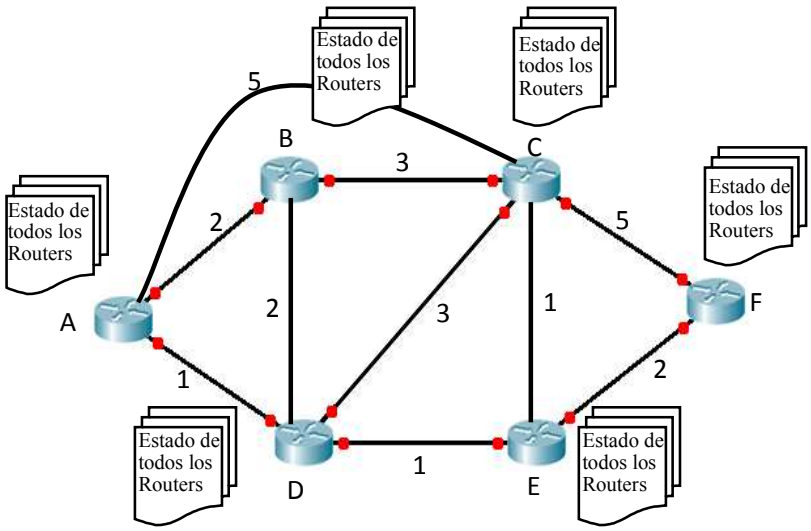


Figura A-16 Base de datos de los estados de enlaces. Diagrama propio con base en referencia [75].

REFERENCIAS

[1] Internet Society, *Brief History of the Internet*, [en línea];EEUU,2012[Consulta : 13 mar 2014] Disponible http://www.internetsociety.org/es/breve-historia-de-internet

[2] John L. Hennessy and David A. Patterson *Computer Archictecture; A Quantitative Approach*,California,EEUU,2003,3ra edition, ed. Morgan Kaufmann Publishers: 1-55860-724-2

[3] Internet2,*History of Excellence*, [en línea];EEUU,[Consulta: 13 Mar 2014] Disponible: http://www.internet2.edu/vision-initiatives/executive-insights/history-excellence/

[4] Red CLARA, *Memorias RedCLARA*, [en línea] [Consulta: 13 Mar 2014] Disponible: http://www.redclara.net/index.php?option=com_content&view=article&id=29&Itemid=321&lang=es

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

[6] José Ignacio Castillo Velázquez, *Internet y la WEB no son lo mismo: día internacional de internet 2011*, México D.F.,2011

[7] National Science Foundation,N,*NSF and the Birth of the Internet*, [en línea]; Virginia, EEUU, [Consulta: 13 Mar 2014] Disponible: http://www.nsf.gov/news/special_reports/nsf-net/home.jsp

[8] National Science Foundation , *NSF and the Birth of the Internet*, [en línea]; EEUU,[Consulta: 13 Mar 2014] Disponible: http://www.nsf.gov/news/special_reports/nsf-net/1990s.jsp

[9] The Internet Engineering Task Force, *Internet Protocol*, [en línea]; EEUU,1981 [Consulta:13 mar 2013] Disponible: http://www.ietf.org/rfc/rfc791.txt

[10] José Ignacio Castillo Velázquez, *Redes de Datos Contexoto y evolución*, México 2014, ed.SAMSARA. ISBN: 978-970-94-2915-2

[11] Computer History Museum, *Internet History*, [en línea]; EEUU,[Consulta: 13 Mar 2014] Disponible: http://www.computerhistory.org/internet_history/index.html

[12] National Science Foundation , *Backbone de NSFNET1995*, [en línea]; EEUU,[Consulta: 13 Mar 2014] Disponible: http://www.nsf.gov/news/special_reports/nsf-net/1990s.jsp

[13] Tadao Saito y Hiroshi Esaki, *Gigabit Network*, [en línea];Tokio,Japan,2003[Consulta : 13 mar 2014] Disponible:http://books.google.com.mx/books?id=3kEHWGKhumIC&pg=PA137&hl=es&source=gbs_selected_pages&cad=3#v=onepage&q&f=false

[14] Nathan Penner,*Internet2*,[en línea]; EEUU, [Consulta: 13 Mar 2014],Disponible: http://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/internet-2/overview.html

[15] Lee Perlis, *Internet2Overwiew*, [en línea]; EEUU [Consulta: 18 Abr 2014] Disponible: http://www.internet2.edu/presentations/ LMP-Internet2-Brandeis.htm.ppt

[16] Greg Wood, *Internet2 and Abilene Advanced Networking in Higher Education*, [en línea]; EEUU [Consulta: 18 Abr 2014] Disponible: http://www.internet2.edu/presentations/ Internet2-Vignette.ppt

[17] Networkcomouting, *Fore ASX*-100, [en línea]; EEUU [Consulta: 15 Abr 2014] Disponible: http://www.networkcomputing.com/909/909f136.html

[18] Paul, *Internet2: A Tutorial* ,[en línea]; EEUU [Consulta: 18 Abr 2014] Disponible: http://www.internet2.edu/presentations /SBRC99-1.pp

[19] Steve Corbató , *Internet2 Network of the Future,*[en línea]; EEUU [Consulta: 18 Abr 2014] Disponible: http://www.internet2.edu/presentations /200204-REUNA-Corbato.pp

[20] La Red de Investigación Educativa, *Abilene International Network Peers*, [en línea][Consulta: 13 mar 2014] Disponible: http://www.iered.org/miembros/ulises/presentaciones/2007-01-12_Presentacion-RENATA/Mapa_Internet2.gif

[21] Ana Preston, *Internet2: An overview*, [en línea]; EEUU [Consulta: 18 Abr 2014] Disponible: http://www.internet2.edu/presentations/20031203-PeruURP-AP.ppt

[22] Jordi Palet Martínez, *El Protocolo IPV6*, versión 4, España, 2004

[23] Internet2 , *Advanced Networking*, [en línea]; Washington, D. C, EEUU [Consulta: 13 mar 2014] Disponible: http://www.internet2.edu/products-services/advanced-networking/

[24] Internet2, *Advanced Layer-3-Service,* [en línea]; Washington, D. C, EEUU, 2013 [Consulta: 13 mar 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/09/07/IS-advanced-layer-3-service.pdf

[25] Internet2, *Advanced Layer-2-Service,* [en línea]; Washington, D. C, EEUU, 2013 [Consulta: 13 mar 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/09/07/IS-advanced-layer-2-service.pdf

[26] Internet2, *Advanced Layer-1-Service,* [en línea]; Washington, D. C, EEUU, 2013 [Consulta: 13 mar 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/09/07/IS-advanced-layer-1-service.pdf

[27] Internet2, Internet2 *Network Infrastructure Topology*, [en línea]; Washington, D. C, EEUU, 2013 [Consulta: 13 mar 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/07/31/Internet2-Network-Infrastructure-Topology.pdf

[28] Adriano Doniez, *Sobre Red CLARA,*[en línea]; 2007 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/index.php?option=com_content&view=article&id=3&Itemid=311&lang=es

[29] Red CLARA, *Memoria 2005,*[en línea]; 2006 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/Memorias/MemoriaCLARA2005.pdf

[30] DANTE, *About US*, [en línea]; 2014[Consulta: 18 Jul 2014] Disponible: http://www.dante.net/About_Us/Pages/Home.aspx

[31] Red CLARA, *Creating the first research andeducation network for Latin America,*[en línea]; 2004 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/541_Alice_Topology_map.pdf

[32] Red CLARA, *Memoria 2006,*[en línea]; 2007 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/Memorias/Memoria_CLARA_2006.pdf

[33] Red CLARA, *RedClara Topology 2006,*[en línea]; 2006 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/topology_RedCLARA_Dec_08_2006.pdf

[34] Red CLARA, *Memoria 2007,*[en línea]; 2008 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/Memorias/MemoriaCLARA2007.pdf

[35] Red CLARA, *Memoria anual 2008,*[en línea]; Uruguay,2009 [Consulta: 18 Abr 2014] Disponible: http://www.redclara.net/doc/Memorias/MemoriaCLARA2008.pdf

[36] Red CLARA, *RedClara Topology 2008,*[en línea]; 2008 [Consulta: 18 Abr 2014] Disponible: https://www.redclara.net/doc/topology_RedCLARA_June2008.pdf.

[37] Red CLARA, *Memoria anual 2009,*[en línea]; Uruguay,2010 [Consulta: 18 Abr 2014] Disponible: http://www.redclara.net/doc/Memorias/Memoria_RedCLARA_2010.pdf

[38] Red CLARA, *RedClara Topology 2011,*[en línea]; 2011 [Consulta: 18 Abr 2014] Disponible: .https://www.redclara.net/doc/topology_RedCLARA_300111.pdf

[39] Red CLARA, *Memoria anual 2012,*[en línea]; 2013 [Consulta: 18 Abr 2014] Disponible: http://www.redclara.net/doc/Memorias/RedCLARA_memoria_2012.pdf

[40] Red CLARA, *Especificaciones técnicas,*[en línea]; 2013 [Consulta: 18 Abr 2014] Disponible: http://www.redclara.net/index.php?option=com_content&view=article&id=52&Itemid=348&lang=es

[41] Red CLARA, *RedClara Topology 2013,*[en línea]; 2013 [Consulta: 20Abr 2014] Disponible: https://www.redclara.net/doc/topology_RedCLARA_June2013.pdf.

[42] Todd Lammle, *CCNA Cisco Certified Study Guide*; San Francisco,EEUU,2000,2da edition, ed. SYBEX Inc. Publishers: 0-7821-2647-2

[43] Cisco System*, Routing Basics,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://docwiki.cisco.com/wiki/Routing_Basics#Link-State_Versus_Distance_Vector

[44] Algoritmos*,Algoritmo Bellam-Ford,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://pradojah007.blogspot.mx/2010/11/algoritmo-bellman-ford.htm

[45] Deepankar Medhi, *Network Rouiting Algorithms, Protocols, and Architecture*; San Francisco CA, EEUU,2007,1ra edition, ed. Morgan Kaufmann. Publishers: 0-12-088588-3

[46] Richard Johnsonbaugh , *Matemáticas discretas* , ed. Pearson Educación, 2005 Publishers: 9702606373, 9789702606376

[47] Pablo Gil Vázquez, *Redes y transmisión de datos*; San Vicente del Raspeig, España,2010, ed. Universidad de Alicante. Publishers: 978-84-9717-125-0

[48] The Internet Engineering Task Force, *Routing Information Protocol*, [en línea]; EEUU,1988 [Consulta:30 junio 2014] Disponible: https://www.ietf.org/rfc/rfc1058.txt

[49] Eduardo Collado Cabeza, *Fundamentos de Routing,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://books.google.com.mx/books?id=zfaN9k840xsC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[50] Rick Graziani, Allan Johnson, *Routing Protocols and Concepts, CCNA Exploration Companion Guide*; Indianapolos EEUU 2008, ed. Cisco System Inc. ISBN 978-1-58-713-206-3

[51] The Internet Engineering Task Force, *Rip Versión 2*, [en línea]; EEUU,1998 [Consulta: 5 julio 2014] Disponible: http://tools.ietf.org/html/rfc2453#section-3.4

[52] Antonio Nogueira, Paulo Salvador, *A Practical Approach to Corporate Networks Engineering*, [en línea]; 2013 [Consulta: 5 Julio 2014] Disponible: http://books.google.com.mx/books?id=AWzisWQ2qlAC&pg=PA170&dq=RIPV2+and+RiPng&hl=es&sa=X&ei=sNA5VIuwGfO88QGa9YHIAQ&ved=0CEIQ6AEwBQ#v=onepage&q=RIPV2%20and%20RiPng&f=false

[53] The Internet Engineering Task Force, *RIPng for IPv6*, [en línea]; EEUU,1997 [Consulta:13 julio 2013] Disponible: http://www.ietf.org/rfc/rfc2080.txt

[54] IPV6 MX, *Cambios y Nuevas Características de RIPng* , [en línea]; [Consulta:13 julio 2014] Disponible: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6#

[55] Cisco System, Interior Gateway Routing Protoco,[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://docwiki.cisco.com/wiki/Routing_Basics#Link-State_Versus_Distance_Vector

[56] Francisco Valencia Arribas, *Manual Basico de Configuracion de Redes Cisco,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://books.google.com.mx/books?id=0gpdAgAAQBAJ&pg=PA80&dq=Manual+Basico+de+Configuracion+de+Redes+Cisco&hl=es&sa=X&ei=sQXjU6OsH8z4yQSD5oDwDw&ved=0CCUQ6wEwAA#v=onepage&q=Manual%20Basico%20de%20Configuracion%20de%20Redes%20Cisco&f=false

[57] Cisco System, CC-DA Self-Study: *CCDA Exam Certification Guide*, [en línea]; EEUU,2003 [Consulta:1 julio 2014] Disponible:http://books.google.com.mx/books?id=--l6gwwjyskC&printsec=frontcover&dq=CCDA+Exam+Certification+Guide&hl=es&sa=X&ei=9BXxU40egvrwAeOYgKgN&ved=0CCQQ6AEwAA#v=onepage&q=CCDA%20Exam%20Certification%20Guide&f=false

[58] Academia regional de Cisco, *CURRICULA CCN2*, [en línea] [Consulta: 29 Julio 2014] Disponible: http:// ocis.jimdo.com/ccna/ccna-2/

[59] Academia regional de Cisco, *Capitulo 9 EIGRP*, [en línea] [Consulta: 29 Julio 2014] Disponible: http:// ocis.jimdo.com/ccna/ccna-2/

[60] The Internet Engineering Task Force, *OSPF Version 2*, [en línea]; EEUU,1991 [Consulta:29 julio 2014] Disponible: http://tools.ietf.org/html/rfc1247

[61] Academia regional de Cisco, *Capitulo 11 OSPF*, [en línea] [Consulta: 29 Julio 2014] Disponible: http:// ocis.jimdo.com/ccna/ccna-2/

[62] Wendell Odom,*Official Cert Guide CCNA ICND2 640-816 Third Edition,*[en línea]; EEUU, 2011 [Consulta: 30 julio 2014] Disponible: http://books.google.com.mx/books?id=DtrF4N-giGsC&pg=PA401&dq=ospf+multiarea&hl=es-419&sa=X&ei=O_pOVNKLHcan8gH80IG4DA&ved=0CDEQ6AEwAw#v=onepage&q=ospf%20multiarea&f=false

[63] Allan Johnson ,*31 Days Before Your CCNA Routing and Switching Exam* ,[en línea]; EEUU, 2014 [Consulta: 2 Ago 2014] Disponible: http://books.google.com.mx/books?id=kURmAwAAQBAJ&pg=PA70&dq=ospf+multiarea&hl=es-419&sa=X&ei=gdBPVIGvFYfP8AGIhYDoCw&ved=0CFIQ6AEwBzgK#v=onepage&q=ospf%20multiarea&f=false

[64] Cisco Networking Academy ,*Scaling Network* ,[en línea]; EEUU, 2014 [Consulta: 2 Ago 2014] Disponible: http://books.google.com.mx/books?id=3ygKAwAAQBAJ&pg=PA330&dq=ospf+multiarea&hl=es-419&sa=X&ei=zPpPVMfsFO2n8QGZtYCQDw&ved=0CBoQ6AEwAA#v=onepage&q=ospf%20multiarea&f=false

[65] Cisco Networking Academy, *Configuring the Open Shortest Path First Protocol* ,[en línea]; EEUU, 2010 [Consulta: 2 Ago 2014] Disponible: http://www.sc.mahidol.ac.th/scsosd/Doc/km/Network/CCNP/en_ROUTE_v6_Ch03%28OSPF%29.pdf

[66] Juan Zambrano, *Material de estudio redes y Telecomunicaciones BGP,*[en línea];2014 [Consulta: 22 Agosto 2014] Disponible: http://www.teleccna.cl/bgp.html

[67] The Internet Engineering Task Force, *Aborder Gateway Protocol (BGP),* [en línea]; EEUU,1997 [Consulta:24 Agosto 2014] Disponible: http://tools.ietf.org/html/rfc1105

[68] Cisco System Networking Academy, *Simulador PAcket Tracer versión 5.3.0.0088* ,EEUU, 2010

[69] GNS3, *Domumentation*, [en línea]; 2013 [Consulta:27 Ago 2013] Disponible: https://community.gns3.com/community/support/documentation

[70] Julio Jornet Monteverde, *Estudio e implementación de la herramienta de simulación de redes GNS3*, [en línea]; España,2013 [Consulta:25 Ago 2013] Disponible: http://es.slideshare.net/jornetmonteverde/estudio-e-implementacin-de-la-herramienta-de-simulacin-de-redes-gns3?related=1

[71] Free Software Foundation, *GNS3 version 0.8.6* ,EEUU, 2012

[72] Windows Vista Home Premium Mircrosoft Corporation ,*Administrador de tareas Redndimiento,* EEUU, 2007

[73] Wireshark , *Network Protocol Analizer versión 1.10.2* ,EEUU, 2013

[74] Motherboard, *The Simple, Elegant Algorithm That Makes Google Maps Posssible* ,[en línea];2014 [Consulta: 29 junio 2014] Disponible: http://motherboard.vice.com/read/the-simple-elegant-algorithm-that-makes-google-maps-possible

[75] Universidad Pontifica de Madrid,*Teoía de Grafos y Optimización de Redes,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://www.iit.upcomillas.es/aramos/simio/transpa/t_nf_jf.pdf

[76] Universidad de Antioquia Área de Telemática, *Algoritmos de Enrutamiento Dinámico,*[en línea];2014 [Consulta: 30 junio 2014] Disponible: http://ingenieria.udea.edu.co/~aleal/ipt735/modulos/03_Enrutamiento_Dinamico.pdf

Agradezco a la UACM (Universidad Autónoma de la Ciudad de México), a través de la Coordinación de Servicios Estudiantiles por el apoyo económico otorgado, para la impresión y empastado del presente trabajo recepcional.