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

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO

COLEGIO DE CIENCIA Y TECNOLOGÍA

Integración de las Redes Avanzadas en América: Canarie, I2 y Clara

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A :

DANIEL JAVIER SERRANO MARTÍNEZ

DIRECTOR DE TESIS

M. EN C. JOSÉ IGNACIO CASTILLO VELÁZQUEZ

Ciudad de México, Noviembre de 2017.

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©

Dedicatoria

Esta tesis primordialmente se la dedico a mis padres:

Leticia Martínez Aparicio

y

Sotico Serrano Mendez

Por todo su apoyo incondicional a lo largo de toda mi vida, los cuales nunca me han dejado caer y siempre motivandome a cumplir mis metas y aspiraciones

A mi hermana:

Lily Serrano Martínez

Por ser un modelo e inspiración a seguir para cumplir todos mis objetivos de la vida y el poder superme día a día

Al resto de mi familia:

Por creer en mí y brindarme siempre su apoyo para motivarme y nunca dejar de rendirme en todo lo que haga

Agradecimientos

Le agradezco rotundamente a mis padres por todo su tiempo, paciencia, afecto y tolerancia que me han tenido, con esto pude generar un producto como lo es este trabajo de tesis con el cual puedo cerrar un ciclo y comenzar uno mejor.

A mi asesor de tesis el **M. en C. José Ignacio Castillo Velázquez** le estoy sumamente agradezido por todo su valioso tiempo que me brindo a pesar de su apretada agenda, agradezco la atención y dedicación en todo el proceso de tesis en el que me ayudo a ver mis errores y virtudes. Le sumo la aceptación como uno de sus tesistas algo muy presiado para mí debido a la desdicha de no poder haber tomado alguna clase con él, pero me agradaron las grandes enseñanzas que me dio en toda esta travesia.

Agradezco a mis lectores:

El **Dr. Ricardo Marcelin** por aceptar la invitación y la disposición de su tiempo para la lectura y revisión de esta tesis asi como el ser parte del jurado de mi examen profesional, al **M. en C Joel Jazbek Buendia** le agradezco por haber sido uno de mis maestros de diferentes asignaturas del cual le aprendi muchas cosas, asi como ser parte de los lectores de este trabajo en el que tuvo el tiempo y la atención necesaria. Y al **Ing. Miguel Vargas** por haber aceptado ser parte de mis lectores el cual se tomo el tiempo y la dedicación para la lectura y revisión de esta tesis. Finalmente de manera general agradezco a todos los lectores por todos los consejos necesarios para esta obra.

Concluyo estos agradecimientos a mi casa de estudios, la **Universidad Autónoma de la Ciudad de México** por ofréceme un lugar para hacer y culminar mi carrera universitaria, asi como el haberme otorgado diferentes becas con las cuales pude salir adelante. Especialmente agradezco la beca de impresión y empastado que me otorgo la UACM para poder imprimir y empastar los libros de esta tesis y asi finalizar exitosamente mi Ingeniería.

Resumen

Después de la liberación del internet comercial en 1995, las Redes Avanzadas son aquellas en las cuales se realiza la investigación, educación y desarrollo tecnológico para potenciar el internet del futuro. Alrededor del mundo existen varias Redes Avanzadas pero la presente tesis se enfocará en las Redes Avanzadas del continente americano; por su importancia Canadá tiene a CANARIE, EEUU a Internet2 y la red CLARA integra a las Redes Avanzadas de Latinoamérica. Desde 2016 CANARIE cuenta con un Backbone de 26 nodos interconectados a 100 Gbps; Internet2 con un Backbone de 15 nodos (Advanced Layer 3 servicie) interconectados a 100 Gbps, mientras que CLARA con un Backbone de 13 nodos interconectados entre 1 y 10 Gbps.

La finalidad de la presente tesis es estudiar la arquitectura y funcionamiento del Backbone de cada una de las redes mencionadas, así como de la arquitectura y funcionamiento al integrar las tres Redes Avanzadas. Es por ello que se simula y emula el Backbone de cada una de las Redes Avanzadas, y aquella red resultante una vez que estas se integran en una sola red en toda América.

Se simuló la conectividad y la gestión de elementos de red, empleando los protocolos correspondientes. Los resultados obtenidos muestran que usar un simulador revela limitaciones en el software al querer compararle con la infraestructura real de una red avanzada pero constituye una muy buena primera aproximación.

Posteriormente se emuló la conectividad y la gestión empleando para ello los protocolos correspondientes. Los resultados obtenidos muestran que usar un emulador ofrece una mucho mejor segunda aproximación al querer compararla con la infraestructura real de una red avanzada.

La emulación consume aproximadamente 11 veces más recursos de los que consume la simulación. Sin embargo, la integración de las Redes Avanzadas reales no puede emularse en su totalidad, por lo que se requieren emuladores más poderosos que permita el empleo de routers de Backbone de alto desempeño y enlaces del orden de 100 Gbps.

Al final fue posible familiarizarse con la complejidad de las Redes Avanzadas y su infraestructura.

Abstract

After the release of the commercial Internet in 1995, advanced networks are the responsible for research, education, and technological development in order to potentialize the internet of future. Around the world there are several advanced networks, but this thesis will focus on advanced networks in the American Continent, because of it's importance: Canada has CANARIE, USA has INTERNET2 and the CLARA network integrates advanced networks in Latin America.

Since 2016 CANARIE has a backbone interconnecting 26 nodes, using 100 Gbps; Internet2 has backbone of 15 nodes (Advanced Layer 3 service), interconnected to 100 Gbps, while CLARA has a backbone of 13 interconnected nodes between 1 to 10 Gbps.

The purpose of this thesis is to study the architecture and operation of the Backbone of each one of the listed networks, as well as the architecture and operation to integrate the three advanced networks. For this reason, simulation, and emulation for the backbone of each one of the advanced networks and the resulting network as the resulting network from the integration of the three mentioned.

Connectivity and management of network elements were simulated, using the corresponding protocols. Simulation results show a number of simulator limitations when comparing to the real infrastructure of the faced advanced networks, but it shows a good first approximation.

On other hand, connectivity and management of network were emulated, using the corresponding protocols. Emulator results show offers a much better second approach to the real infrastructure of the advanced networks studied.

Emulation consumes a lot of resources, it is about 11 times more than it consumes the simulation. However actual advanced networks integration cannot be emulated in its entirely so, there is a need for more powerful emulators allowing the use of high-performance Backbone links in the order of 100 Gbps and router backbones closer to the nowadays infrastructure. At the end, it was possible to approach to the complexity of advanced networks and its infrastructure.

Contenido

Capítulo I

Introducción

"En la mayoría de los casos la ignorancia es algo superable. No sabemos porque no queremos saber"

Aldous Huxley

I.1 Introducción

El mundo de las telecomunicaciones que se viven en pleno siglo XXI están teniendo una revolución de avances tecnológicos en la que año con año crecen exponencialmente, donde los sistemas de comunicación, por mencionar, las redes de datos, implementan nuevas tecnologias, protocolos y estándares, gracias a toda una investigación y pruebas que se hacen antes de implementarlas y asi seguir en constante evolución. Internet siendo la gran red de redes la cual ha evolucionado de una forma enorme en los últimos 25 años, donde la gran mayoría de la población mundial se conecta fue un arduo trabajo de investigación y experimentación por varias décadas. Hoy en dia es común que la mayoría de la gente vea a internet como un servicio para enviar o recibir todo tipo de información, pero esta "internet comercial" conjunto de redes de datos, tenian como propósito apoyar la investigación, el desarrollo tecnológico y la educación, algo que poco a poco fue perdiendo.

Las redes que actualmente siguen con este propósito son llamadas *"Redes Avanzadas (RA)"*, las cuales tienen una gran invesión para actualizar su infraestructura y asi cumplir con la demanda de sus miembros. No cualquier centro educativo puede conectarse a este tipo de redes, ya que sólo pueden hacerlo las instituciones que necesiten una red confiable y altamente eficaz, donde, puedan enviar información delicada de cualquier índole como por ejemplo: alguna investigación que este de por medio. Lo que implica un monto monetario para poder hacer uso de este tipo de redes. Las RA ofrecen un backbone de gran ancho de banda con muy alta disponibilidad ya que son redes aisladas de la internet comercial, por lo que presentan un tráfico distinto y es poco probable que se pierdan algunos datos delicados.

En 2017 existen varias RA alrededor del mundo, las cuales conjuntamente forman una *"Segunda internet"*, donde se apoya a toda la comunidad científica para seguir experimentando con nuevos protocolos y desarrollos tecnológicos, los cuales posteriormente se estarán integrando al internet de la siguiente generación. Las RA no sólo son importantes para el desarrollo de nueva tecnología, sino que dentro de ellas se ejecutan las aplicaciones y proyectos que benefician a diferentes ramas de la ciencia como son; las ciencias médicas, biológicas, genómicas, astronómicas o físicas entre otras.

Para ver un mejor panorama de la importancia y beneficio de las RA a continuación se mencionan algunos de estos proyectos que están presentes en estas redes:

CANARIE:

- "Human brain Atlas" - proyecto dedicado a un modelo del cerebro humano en tres dimensiones, el cual ensambla 7000 rebanadas del cerebro con imágenes del nivel de 20 micrómetros (tamaño de algunas neuronas humanas) [1].
- "iReceptor" – plataforma de software de investigación que permite a los investigadores entender las condiciones de activar o suprimir genes del sistema inmunológico [2].
- "GenAp" - proyecto que permite a investigadores y médicos hacer el diagnóstico médico, tratamiento y evaluación de riesgos basados en composición genética [3].

Internet2

- "Leigh Orf" – proyecto dedicado a la simulación y visualización de tormentas y tornados en el cual se estudia los funcionamientos interno de las tormentas para entender su comportamiento [4].
- HIVE (High performance Integrated Virtual Environment – Entonrno virtual integrado de alto rendimiento) – infraestructura donde la comunidad médica pueden analizar datos biomédicos, datos clínicos, archivos de espectrometría de masas entre muchos más [5].
- RBHS (Rutgers Biomedical and Health Science) – Centro academico enfocado a la investigación y tratamiento del cancer, la neurociencia, la biotecnología avanzada y la medicina [6].
- "Research Wave Program" – programa el cual beneficia a investigadores de redes donde es posible poner a prueba los protocolos y algoritmos sobre bancos de pruebas experimentales antes de implementarlas en las infraestructuras de redes permanentes [7].

CLARA

- ChiVO – observatorio virtual chileno el cual es una plataforma astro-informática destinada a la administración y análisis de cantidades masivas de datos provenientes de distintos observatorios [8].
- "SPRACE (San Paulo Research and Analisys Center)" – proyecto que involucra varias investigaciones de ciencias físicas como la exploración de las propiedades del plasma "quark-gluon", la búsqueda de la materia oscura y fuertes resonancias en dibosons decadentes [9].

- OLE (Observatorio Latinoamericano de Eventos extraordinarios) - proyecto que ayuda a la gestión de riesgos de eventos ambientales extremos [10].

CLARA/Internet2

- Gran telescopio para rastreos sinópticos – proyecto internacional que beneficiará al campo de la astronomía el cual pretende funcionar en el 2022. [11]

Toda la información que se genera de diferentes proyectos, estudios o experimentos es muy delicada y valiosa por lo que se necesitan de redes 100% confiables, seguras y de alto rendimiento, además esa información se tiene que procesar en tiempo real debido que en su mayoría se generan grandes volúmenes de datos del órden de los Petabytes o Exabytes, contribuyendo al denominado "Big data". Este procesamiento de datos no es posible en la internet comercial ya que el tráfico que se presenta en ella es muy diferente, es por eso que se utiliza todo el conjunto de RA. En la actualidad existen numerosas RA las cuales conjuntamente se conectan entre sí para poder compartir todo tipo de información científica e incluso el poder compartir recursos de red que benefician a los miembros que pertenecen a estas RA.

Alrededor del mundo existen diferentes RA pertenecientes a cada país, por ello la presente tesis esta enfocada al estudio de las principales RA de América y la red resultante al interconectar a CANARIE (red avanzada de Canadá), Internet2 (red avanzada de EEUU) y la red CLARA (red avanzada de Latinoamérica).

I.2 Justificación

Debido a que las RA son importantes para la investigación, la educación e inovación tecnologíca, además de ser un tema poco explorado donde la información es muy escasa. Se hace una exploración de trabajo en el ramo y asi poder agregar valor al buscar un sistema que integra las 3 RA indicadas. El estudio de las RA es de sumo interés para el AdvNetLab en la UACM SLT, en el que se han generado como productos previos, trabajos relacionados con CUDI, CLARA y CANARIE como tesis y artículos arbitrados [12,13,14,15,16,17, 18].

I.3 Objetivo general

Estudiar la arquitectura de Backbone y funcionamiento de las RA: CANARIE, Internet2 y la red CLARA, para posteriormente realizar la integración de dichas redes.

I.4 Objetivos específicos

a. Técnicos

Realización de una simulación y una emulación de red como primera y segunda aproximación respectivamente, ya que, es imposible el acceso a equipos físicos que son utilizados en las RA.

Comprobar la conectividad de Backbone de la mencionada integración por medio de la implementación de protocolos de enrutamiento, así como la gestión del Backbone por medio de un protocolo de gestión.

Utilizar los programas *"Packet Tracer"* para la simulación y *"Graphical Network Simulator-3(GNS3)"* para la emulación, mismos que se pretenden esforzar para poder conocer los alcances y limitaciones de estos.

Adquirir las habilidades de ejecución sobre el emulador, ya que, es de suma importancia hacer una emulación de red antes de implementar alguna topología de red en el mundo real.

b. No técnicos

Adquirir las habilidades necesarias para el manejo de un proyecto, donde se involucra seguir una metodología de trabajo, misma que implica la planeación, ejecución y tiempos de entrega.

I.5 Estructura de la tesis

Esta tesis está constituida de 5 capítulos, dentro de los cuales el capítulo 1 está destinado a una breve descripción sobre la importancia de las RA y objetivos de esta tesis. El capítulo 2 está destinado a la revisión de las RA de América, comenzando por la red CANARIE, después Internet2 y finalmente la red CLARA, en el cual se menciona el surgimiento, objetivos y topologías de estas redes. El capítulo 3 está destinado a los protocolos que se pretenden implementar, dentro de este capítulo una primera parte estará destinada a los protocolos de enrutamiento, la cual plantea a detalle de 3 protocolos (RIP, OSPF y BGP) y una segunda parte estará destinada a los protocolos de gestión donde se plantea a detalle del protocolo SNMP y sus diferentes versiones.

El capítulo 4 está destinado a la metodología de la simulación y emulación de la integración de las RA de América, para abordar el diseño y configuración de toda la integración, así como de los protocolos de enrutamiento y de gestión.

El capítulo 5 está enfocado los resultados y conclusiones.

Capítulo II

Redes Avanzadas

"Solo podemos ver poco del futuro, pero lo suficiente para darnos cuenta de que hay mucho que hacer"

Alan Mathison Turing

II.1 Internet y Redes Avanzadas

ARPANET (Advanced Research Projects Agency NETwork) el predecesor de internet surgió en 1964 con las investigaciones y aportaciones de "*Paul Baran, Vinton Cerf, Donald Davis, Robert Kahn y Leonard Kleinrock*", fue la red pionera en usar la conmutación por paquetes, misma que conectaría a universidades y laboratorios de investigación. En 1969 sus primeros 4 nodos se conectaron a SRI (Stanford Research Institute), UCSB (University of California Santa Barbara) UCLA (University of California Los Angeles) y U.Utah (University of Utah) donde la comunicación se hizo por la red telefónica a 56 Kbps vía PSTN (Public Switching Telephonic Network). En este mismo año se utilizó el protocolo NCP (Network Control Protocol) para la comunicación de los nodos de ARPANET, que posteriormente se cambiaría por el modelo TCP/IP (1983) [19].

Para el año de 1981 contaba con 40 nodos, lo que conformaba una Internet no comercial. Cabe mencionar que dentro de ARPANET surgieron algunos de los protocolos que aún se siguen utilizando como TELNET (Telecommunication Network), FTP (File Transfer Protocol), así como del correo electrónico popularizado en 1972 y el desarrollo de ICMP (Internet Control Message Protocol). También se crearían los primeros protocolos de enrutamiento como: IGP (Interior Gateway Protocol), RIP (Routing Information Protocol), EGP (Exterior Gateway Protocol) y BGP (Border Gateway Protocol). Ajenamente, poco a poco fue creciendo el esfuerzo por desarrollar nuevas tecnologías, haciendo mención a Xerox al desarrollar la tecnología "Ethernet", bajo el estándar IEEE 802.3 siendo liberado en 1983. Otros desarrollos aparecieron en 1984 como DNS (Domain Name System) para poder organizar a los servidores en dominios (debido a que ya había demasiados), también se liberó el estándar ISO/OSI 7498 como un modelo de referencia básico para sistemas abiertos de redes de datos (modelo importante para el crecimiento gradual de protocolos y estándares) [19,20].

En 1981 a cargo de NSF (National Science Foundation) se crearía CSNET (Computer Science NETwork), proyecto que interconectaba los departamentos de informática de EEUU los cuales no tenían acceso a ARPANET, CSNET también comunicó a EEUU con las principales universidades y centros de investigación de Europa y Asia, posteriormente en 1983 ARPANET y CSNET se conectarían. Para 1985 nació la NSFNET (National Science Foundation NETwork) para comunicar a todas las universidades de EEUU para apoyarlas en sus proyectos de investigación. Su intención fue crear una red de redes académicas que se pudieran conectar a ARPANET. Posteriormente en 1990 ARPANET dejó de funcionar y cedió su lugar a NSFNET.

En 1991 nació CIX (Commercial Internet eXchange), proyecto donde se destinaría un poco del tráfico de NSFNET hacia el internet comercial que estaba surgiendo a cargo de los mismos proveedores de internet (ISP), pero aún así NSFNET hace un esfuerzo por privatizar las redes regionales. En abril de 1995 NSFNET se liberó definitivamente para ser usado como el internet comercial ya que la gran demanda de las redes que se querían conectar fue demasiada gracias a que el Backbone de NSFNET ofrecía 45 Mbps [19,21, 22].

En la figura 2.1 se muestra la transición de internet que paso de un proyecto de investigación a un servicio comercial donde creció en tamaño, complejidad y ancho de banda, así mismo se muestra el comienzo de Internet2 (red avanzada perteneciente U.S.A) que posteriormente se hablará de ella.

Figura 2.1 Espiral de desarrollo de internet (diagrama propio con base en [23])

Con esta liberación comercial se abrió la siguiente incógnita:

"*¿Están siendo satisfechas nuestras necesidades de investigación y educación por el internet de hoy en día (1996)?*" [24]

Es por este hecho que en Estados Unidos y otras partes del mundo empezaron a surgir diferentes proyectos dedicados a la creación de RA.

II.2 Redes Avanzadas

En 1996 con Internet ya no se podían fomentar nuevas capacidades de desarrollo de aplicaciones (servicios multimedia o iteracciones en tiempo real) asi como el poder hacer pruebas para nuevas tecnologías, y con ello aprovechar el potencial del internet en un futuro, entonces se inicio el desarrollo de las RA. El objetivo principal de las RA es crear una infraestructura enfocada a la investigación, educación y desarrollo tecnológico, la cual conecta a universidades y laboratorios de investigación a redes de alto rendimiento, debido a que el backbone empleado en estas redes ofrece un backbone de 2 a 10 veces mayores que el utilizado en un ISP, presentando un tráfico muy distinto al del internet comercial, así mismo las RA no buscan reemplazar ésta internet, sino potenciar el internet del futuro, debido a los avances y desarrollos que se hacen dentro de este tipo de redes.

Todos estos avances y aplicaciones que se desarrollan requieren una red con funcionalidades de alto nivel, como es gran ancho de banda, baja latencia, baja fluctuación de fase así comouna mayor seguridad, siendo estas características las que presentan las RA. Estas RA son importantes debido a que los miembros tienen ciertos beneficios, como el poder lograr una colaboración interactiva con otros miembros de diferente nacionalidad, así como el poder manejar instrumentación remota, tener acceso en tiempo real a diferentes recursos de red, almacenamiento de datos distribuidos, minería de datos, computación de alto rendimiento, virtualización dinámica de datos y realidad virtual compartida, entre muchos otros beneficios [25].

Las universidades y centros de investigación se han beneficiado de estas RA debido a que éstas ofrecen diferentes servicios para sus investigaciones, algunos de ellos son: XSEDE (eXtreme Science and Engineering Discovery Environment - Entorno de descubrimiento de ingeniería y ciencia extrema) sistema virtual que ocupan los científicos e investigadores para obtener datos y recursos informáticos de alta gama (como la utilización de supercomputadoras), y LAGO (Latin America Giant Observatory – Observatorio gigante Latinoamericano), observatorio extendido de astroparticulas, el cual consiste en una pequeña serie de detectores de partículas a nivel del suelo, que abarca desde México hasta la Antártida donde se puede estudiar la astronomía gamma, tiempo espacial, entre otros campos [25, 26, 27].

Las RA también benefician a simuladores o equipos que generan grandes volúmenes de datos, dicha información se tiene que enviar a diferentes centros de investigación en donde son

almacenados, posiblemente vía NAS (Network Area Storage), como son el caso de: NEES (Network for Earthquake Engineering Simulation - La Red de Simulación de Ingeniería Sísmica), BIRN (Biomedical Informatics Research Network - La Red de investigación en Informática Biomédica), LHC (Large Hadron Collider - El Gran Colisionador de Hadrones) y LIGO (the Laser Interferometer Gravitational wave Observatory - El Observatorio de ondas Gravitacionales del Interferómetro Láser)[25,28,29].

Algunos de los desarrollos tecnológicos que ofrecen las RA se encuentran: IPv6, QoS (Quality of Service), MPLS (Multiprotocol Label Switching), Multicast, H.323, videoconferencias en ultra HD, NDN (Named Data Networking), SDN (Sofware Defined Networking) y NFV (Network Funtion Virtualization) [23,24].

En la figura 2.2 se muestra la idea general de las RA así como los protocolos, servicios y proyectos que se han desarrollado dentro de estas redes.

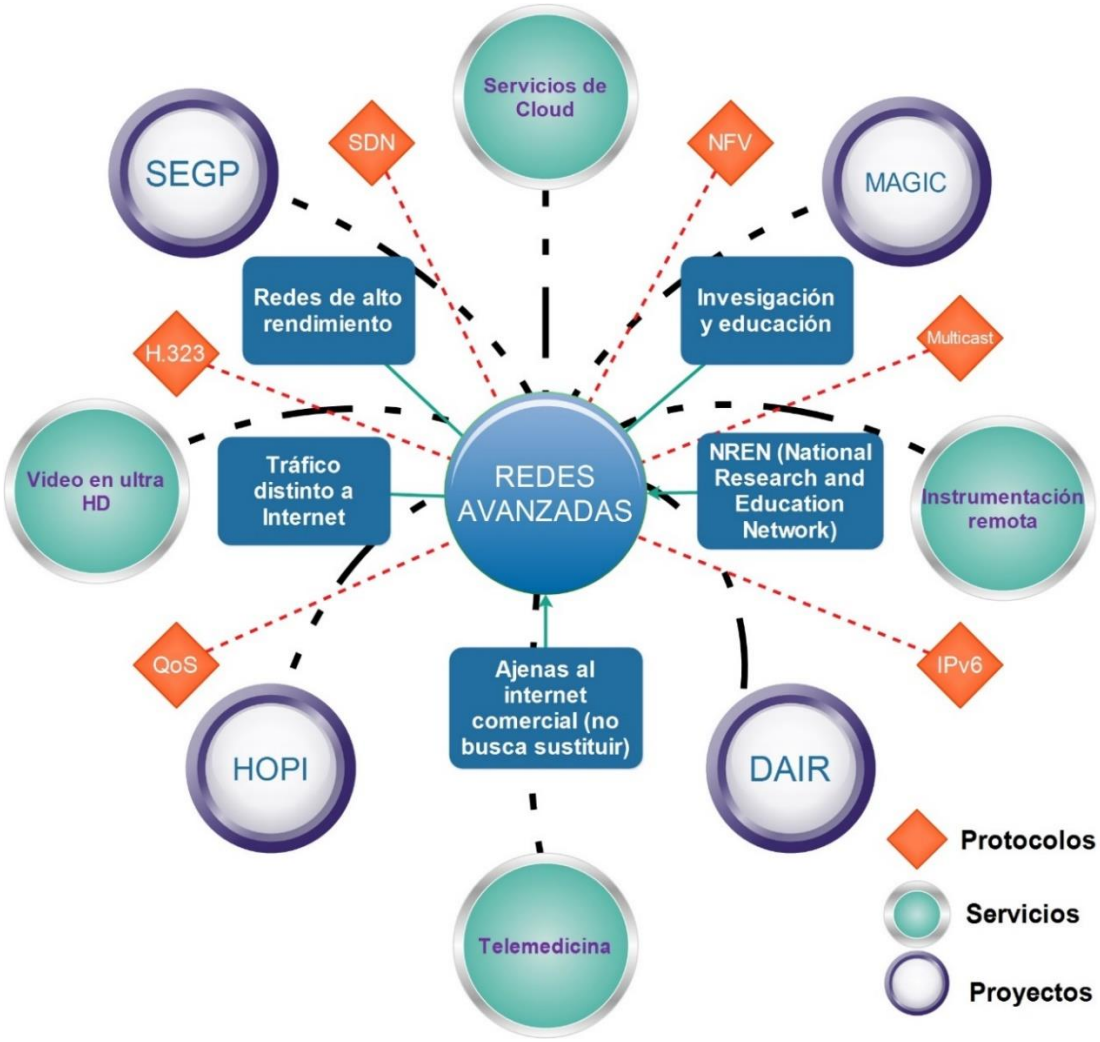


Figura 2.2 Idea general de RA.

La parte integradora de la mayoría de las RA es el GigaPoP (Gigabit Point of Presence), el cual es un punto de interconexión de tecnología avanzada de alta capacidad en donde los miembros conectados pueden intercambiar tráfico de servicios avanzados. En la figura 2.3 se muestra un diagrama que ejemplifica la conexión lógica de los GigaPoPs.

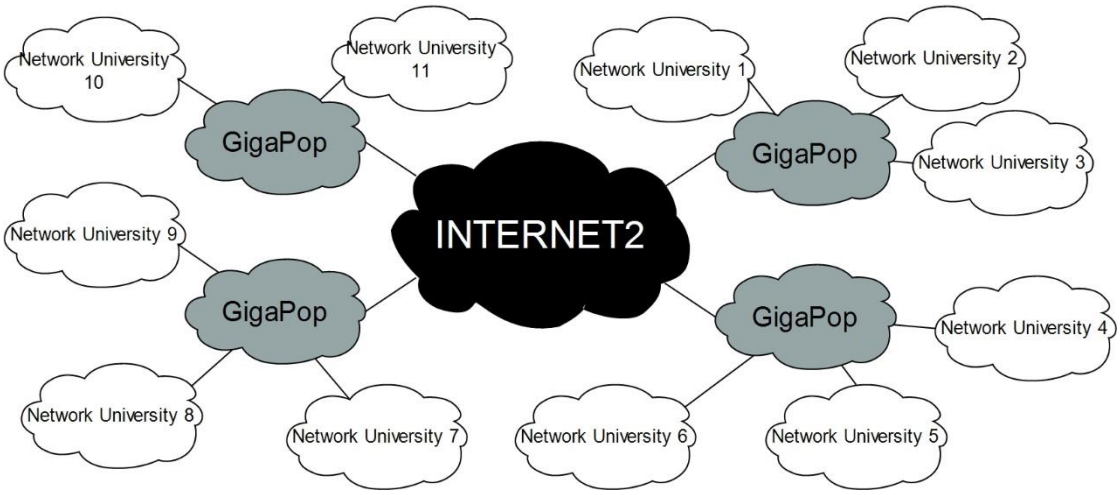


Figura 2.3 Conexión lógica entre Internet2 y GigaPoPs (diagrama propio con referencia de [30]

Estas conexiones pueden ser; Backbone a GigaPoP, GigaPoP a GigaPoP, GigaPoP a la red universitaria y de la red universitaria a host. Estos GigaPoPs se dividen en dos categorías:

1) Tipo 1 (Simple): Servicio dedicado sólo para miembros de la red avanzada, enruta el tráfico de dicha red a través de una o más conexiones con otros GigaPoPs, tiene poca necesidad de utilizar un enrutamiento interno complejo o firewalls.
2) Tipo 2 (Complejo): Servicio tanto a miembros de la red avanzada así como a otras redes a las que estos miembros necesitan comunicarse, tienen un conjunto variado de conexiones con otro GigaPoPs, por lo que necesitan políticas de enrutamiento (mecanismos para hacer un enrutamiento del tráfico correctamente) así como mecanismos de autorización para prevenir un uso no autorizado o impropio de la conectividad de la red avanzada [31,32 ,33].

A continuación se describen las RA correspondientes al continente Americano comenzando por la red CANARIE, despues Internet2 y por último la red CLARA. Posteriormente a estas 3 redes se describe las conexiones internacionales las cuales hacen posible la integración de estas 3 RA.

II.3 CANARIE

A mediados de la década de 1980 las universidades más grandes de Canadá comenzaron con los proyectos para instalar una red de alta velocidad, con el objetivo de establecer vínculos entre redes internas y redes externas como NSFNET. Es así como nació la red CA*net, misma que empezó a incursionar en el ámbito del internet comercial, debido a esto empezó a tener problemas con el tema de educación e investigación ya que esta red no les era suficiente para dichos fines. Influenciados por las ideas de EEUU de contar con una NREN (National Research and Education Network) se realizaron los acuerdos para desarrollar una red avanzada, pero a diferencia de EEUU no sólo fue para la educación e investigación sino también para la industria. En 1993 CANARIE (Canadian Network for the Advancement Research, Industry and Education) nació como un plan el cual fue patrocinado por algunos miembros de la industria, ciencia y tecnología de Canadá, se le dio el mandato para la creación de una red de alta velocidad para ser explotada en el ámbito de la educación, investigación, el desarrollo de nuevas tecnologías, servicios de aplicaciones de red y de telecomunicaciones [34,35].

Años más tarde CANARIE tendría un nuevo contrato con la industria (1999) para encabezar el desarrollo de aplicaciones de banda ancha en áreas clave, incluyendo el aprendizaje electrónico, el comercio electrónico y la telesalud, así mismo, administraría un programa de telecomunicaciones inalámbricas de investigación y desarrollo, donde se desarrollan nuevos productos y aplicaciones para el mercado inalámbrico. Esta red también trabaja con la autoridad de registro de internet de Canadá sobre las políticas, la tecnología y la organización para administrar el dominio "*ca"* de nivel superior de Canadá [34].

En 1998 se llegaron los acuerdos para la interconexión de CANARIE con Internet2, de modo que Internet22 sirvio de puente estratégico para las demás interconexiones hacia otras redes internacionales y en 1999 tendría los acuerdos con la red CUDI (red avanzada de México) para interconectarse y así mismo, después tener la conexión con la red CLARA.

En 2016 CANARIE es la red avanzada perteneciente a Canadá, es la responsable de la red troncal, así como de los servicios que presta a las redes regionales, misma que proporciona una cantidad de red de prueba para el uso de las comunidades de investigación de la industria canadiense, tecnologías de la información y de telecomunicaciones. CANARIE es considerado un centro de desarrollo de las tecnologías de las telecomunicaciones de la próxima generación y en consecuencia esta red está muy bien conectada a otras redes tanto formales como

informales. CANARIE tiene el financiamiento de la industria y del gobierno de Canadá, entre sus participantes se incluyen a universidades, organizaciones y centros de investigación. Algunos de los objetivos que tiene CANARIE son:

- Mejorar la red troncal de CA*net para ser usada en educación e investigación.
- Promover los servicios de CANARIE entre redes regionales.
- Establecer y experimentar una red de alta velocidad para uso del desarrollo y ensayo de tecnologías, aplicaciones, servicios aplicados en redes de próxima generación.
- Estimular el desarrollo de nuevas aplicaciones de red, software y servicios que puedan ser vendidos a nivel nacional como internacional.
- Apoyar la integración de nuevas tecnologías de red en la infraestructura de las redes operativas.
- Desarrollar, demostrar y aplicar tecnologías de última generación.
- Proporcionar una red de ultra alta velocidad para poder competir a nivel internacional dedicada a la investigación, innovación y educación.
- Ayudar a empresas e instituciones que operan en Canadá para avanzar en la innovación y la comercialización de productos y servicios para reforzar las capacidades tecnológicas de Canadá [36].

En el año 2016 CANARIE contaba con más de 200 miembros entre los cuales se encuentran Universidades, Corporaciones, Instituciones, entre otras, cuya misión es:

"CANARIE diseña y suministra la infraestructura digital, e impulsa su adopción para la investigación, la educación y la innovación" [37]

II.3.1 Topología de CANARIE

CA*net fue la red precursora de CANARIE, pero debido a que uno de los fines de CANARIE era apoyar la operación de CA*net, en el año en que entró en funcionamiento CANARIE actualizó la red para tener 10 Mbps. No fue hasta 1997 cuando se tendría otra actualización en la red teniendo como resultado a CA*net II con un ancho de banda de 155Mbps, en esta infraestructura se empezó a utilizar ATM (Asynchronous Transfer Mode) sobre SONET (Synchronous Optical Network), así como IP sobre ATM para las implementaciones de voz, video y transmisiones con QoS. Esta infraestructura ya soportaba IPv6, Multicast, VPNs y entrega de audio y video en tiempo real. Pero en 1998 se actualizó a CA*net III con la utilización

de DWDM que transmitía 32 longitudes de onda discretas de forma simultánea, esta red se asemejaba a la red Abilene de Internet2. Así mismo se tenían 10 GigaPoPs con los que se vincularon con las redes de investigación de cada región y con las redes los Estados unidos, Europa y Asia [38, 39].

En la figura 2.4 se muestra como estaba constituido el Backbone de CA*net de 1990 a 1997. Donde los nodos se encontraban en Vancouver, Edmonton, Regina, Winnipeg, Toronto, Quebec, Brunswik, Halifax, Charlottetow y St. John's [36].

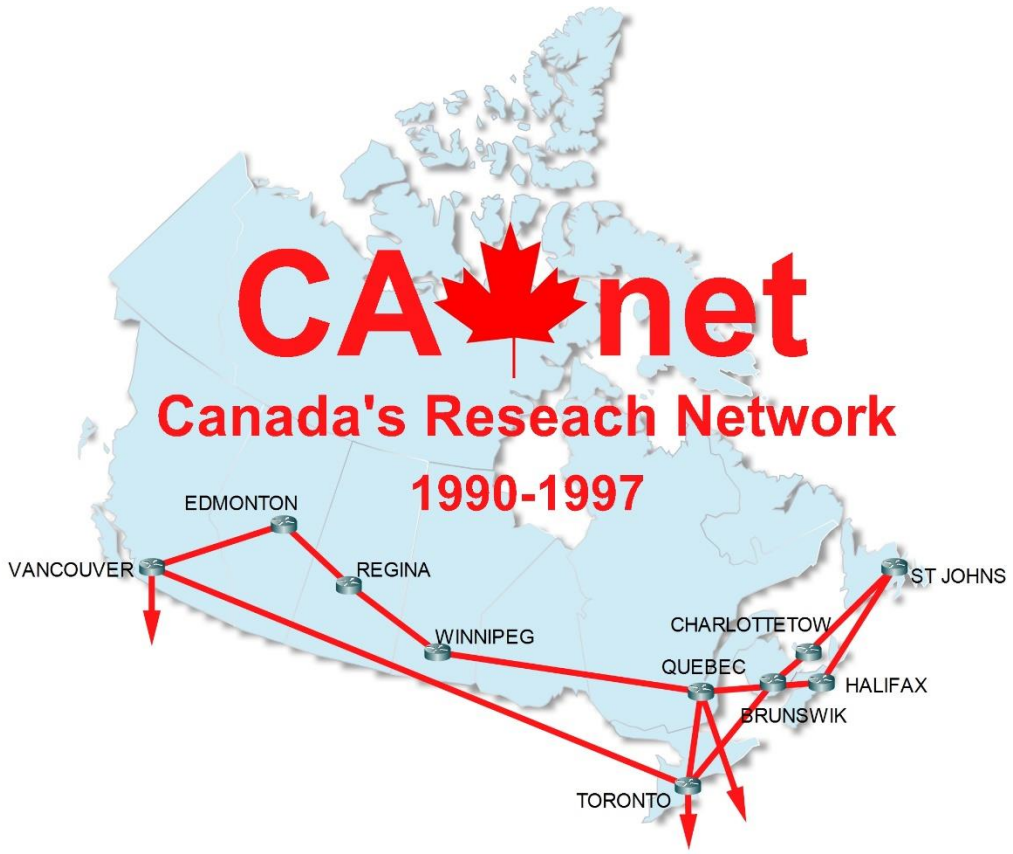


*Figura 2.4 Topología de Backbone de CA*net de 1997 con 10 nodos (diagrama propio con base en [32])*

Para 2003 se tendría a CA*net IV con una backbone de 40Gbps, pero en 2006 la visión de CANARIE fue completar una red de fibra óptica así que empezó a construir una infraestructura ROADM (Reconfigurable Optical Add-Drop Multiplexer) basada en DWDM infraestructura capaz de soportar 88 longitudes de onda de 100 Gbps. Para 2009 se implementaron los router Juniper MX-480, en 2016 se desconoce que router core ocupan pero se cree que son similares a los que están implementados en Internet2 (JuniperMX-960). En 2016 se tiene la red nacional CANARIE (podría decirse que es la versión CA*net V), esta red contaba con un backbone de 100 Gbps, la cual se extiende a más de 23,000 Km a través de Canadá desde el norte de Inuvik

hasta St. John's, NL. Esta red permite el desarrollo de herramientas de software de investigación, las cuales permiten a los investigadores acceder a los datos de investigación de manera más rápida y fácil, así mismo es una red que permite apoyar a los empresarios con su tecnología, ofrece servicios de cloud, para el desarrollo de productos por lo que se puede obtener una ventaja competitiva en el mercado [38,39].

Entre los principales servicios de red que ofrece CANARIE se tiene:

- Servicio IP para I&E: Servicio que ofrece una red core la cual soporta IPv4 e IPv6 para enrutamiento Unicast o Multicast, así mismo la red ofrece intercambio nacional e internacional dedicada a la investigación y educación. Esto lo logra gracias a los enlaces de 100 GE.
- Contenido de prestación de servicio: Proporciona a los usuarios institucionales acceso de alta velocidad a los principales proveedores de contenido como Amazon, Microsoft, Google, etc., debido a que se ha convertido un importante servicio de CANARIE, cabe decír que este servicio está separado lógicamente de la red dedicada a la investigación y educación.
- Servicio de conexión P2P: Servicio basado en el estándar Ethernet el cual puede hacer una conexión dedicada de 100 Gbps, con la que investigadores se pueden conectar a centros de cómputo de alto rendimiento o instalaciones de investigación [40].

En la tabla 2.1 se muestran los 2 principales aportes que maneja CANARIE, que son usados por parte de algunas compañias de Canada en donde hace que puedan tener cierta ventaja en el sector económico ya que con la ayuda de estos servicios pueden acelerar el desarrollo de algún producto o servicio.

Servicio de CANARIE	Aplicación
DAIR (Digital Accelerator for Innovation and Research) cloud	Medio Ambiente, Videojuegos, Seguridad informática, Educacion y Cuidados de la salud.
Research software	Tecnologías de la información y comunicación, Investigación biomédicas, Ciencias Físicas y Sociales, Astronomía, Psicología y Ciencias Cognitivas.

Tabla 2.1 Ejemplo de servicios ofrecidos por CANARIE [41]

En la figura 2.5 se muestra la topología de backbone de 2016 de CANARIE, esta topología esta compuesta principalemte de equipos Ciena (OME 6500) para servicios de capa 1 y 2, y Routers Juniper para servicios de capa 3. CANARIE que opera actualmente a 100 Gbps donde los "Router Core" están ubicados en Victoria,Vancouver, Edmonton, Front Simpson, Front Nelson, Whitehorse, Yellowknife, Kamloops, Kelowna, Saskatoon, Calgary, Regina, Winnipeg, Thundar Bay, Toronto, Windor, Ottawa, Montreal, Quebec, Rimouski, Fredericton, Moncton, Charlottetown, Halifax y STJohns[42,43].

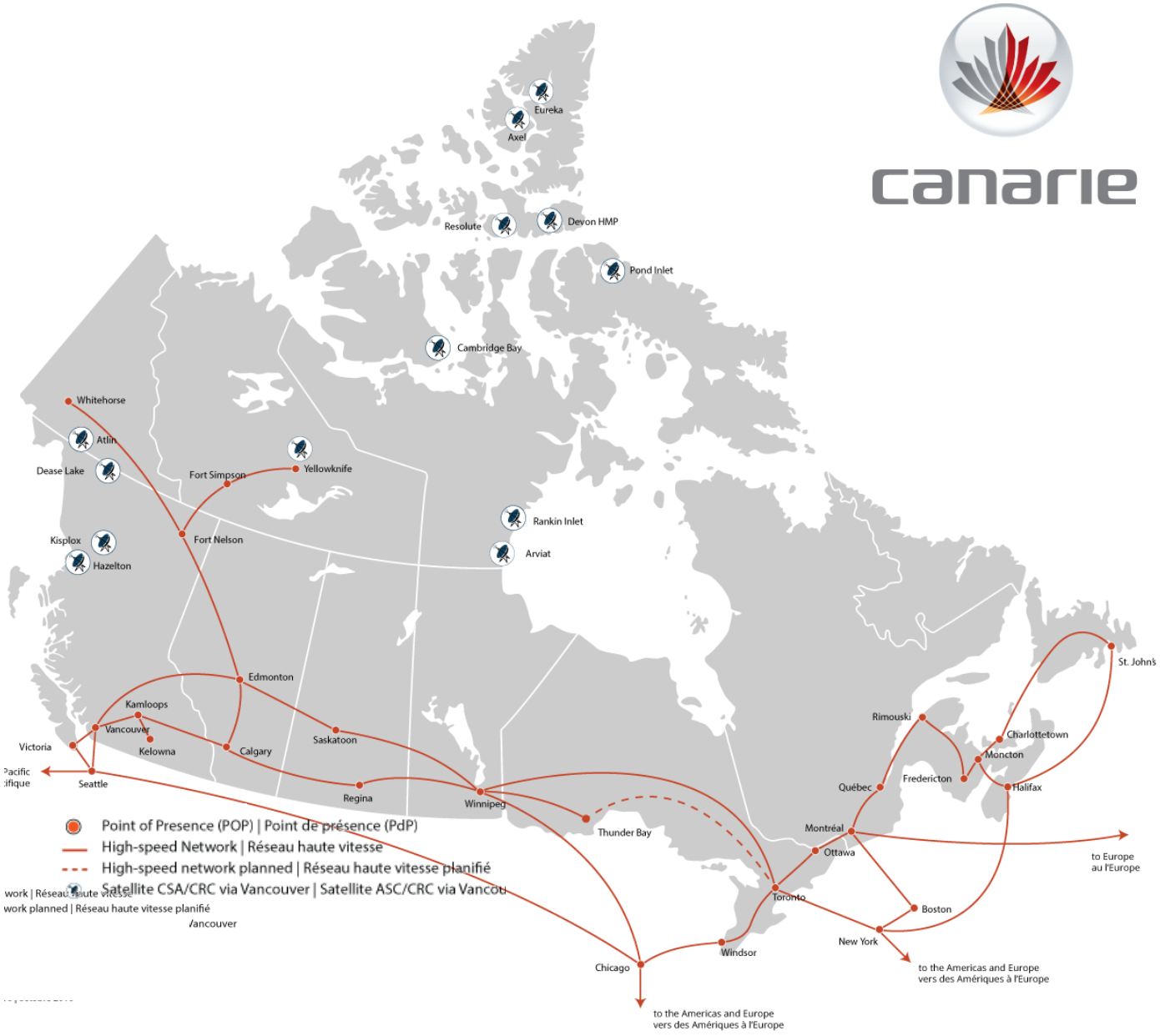


Figura 2.5 Topología de Backbone de CANARIE 2016 con 25 nodos [44]

A continuación se describe la red avanzada perteneciente Estados Unidos.

II.4 Internet2

A finales de 1996 en Estados Unidos nació la red avanzada llamada Internet2, esta red se estableció como un acuerdo entre universidades sin fines de lucro, cuyo propósito fue conectar diferentes universidades, haciendo de esta, una red para uso exclusivo de investigación y educación. Se creó a partir de una iniciativa llamada "NGI (Next Generation Internet – La Internet de la siguiente generación)". Siguiendo la iniciativa NGI se desprendería lo que se conocería como Internet2, cabe decir que Internet2 no es el resultado de esta iniciativa ya que se crearon otras redes nacionales con el mismo objetivo que pretendía NGI, por mencionar algunas de estas se tiene a "DREN" y "EsNet" [45, 46, 47,48].

La UCAID (University Corporation for Advanced Internet Development) inició el proyecto de Internet2 el cual pretendía conectar a sus miembros a una red libre del tráfico ocasionado con el internet comercial, Internet2 comenzó en 1996 con 34 miembros (soló universidades), y que hoy en día cuenta con más de 317 universidades más algunas corporaciones afiliadas, ha tenido un crecimiento tremendo transnacionalmente para uso en educación, así como de tecnología, la cual gracias a todos los avances e implementaciones que ha experiementado la red, ahora cuenta con capacidades muy altas de transmisión de datos por lo que también da lugar a las diferentes aplicaciones que han desarrollado, siendo algunos de estos: IPv6, Multicast, Videoconferencias IP en H.323, Video en ultra HD, Control remoto de instrumentos (telescopios, microscopios, etc.), hasta servicios de Cloud e implementaciones SDN y NFV. Así mismo Internet2 es una de las RA más sofisticadas y también la que mayor inversión ha tenido y ha estado involucrada en un gran número de proyectos y desarrollos como pueden ser; Middleware, SEGP (Sponsored Educational Group Participant), K20, HOPI (Hybrid Optical and Packet Infrastructure), RON (Regional Optical Network), DCN (Dynamic Circuit Network) entre muchas más [45, 46,48].

Esta red la operaba UCAID mediante su centro de operación de red (NOC) ubicado en la Universidad de Indiana, este NOC está dividido en 3 principales áreas [49]:

1) Administración: Se encarga de la gestión de las comunicaciones, gestión de la seguridad de la red, así como la coordinación general de la red.
2) Ingeniería: Se encarga de las pruebas hacia la red (asegurar el tráfico adecuado), así como de la recolección y análisis de datos.
3) Operaciones: Se encarga del monitoreo de la red 24x7, es un punto de contacto para la gestión de algún problema que ocurra en la red, aquí también se revisan los procesos de conexión de la red Abilene.

La misión actual de Internet2 es:

> *"Desarrollar e implementar aplicaciones y tecnologías de RA, lo que acelera la creación de internet del mañana" [50].*

II.4.1 Topología de Internet2

Internet2 es uno de los pilares importantes en cuestión de desarrollo, por lo que su infraestructura ha pasado por muchos cambios, donde a continuación se describen los más destacados. En un inicio Internet2 aún no contaba con su propio Backbone, por lo que sus miembros se podían conectar a la red vBNS (very high performace speed Backbone Network Service) que sirvió de Backbone inicial de Internet2. La red vBNS nació en 1995 gracias a "MCI telecommunications" y la "National Science Fundation" (NSF), la red se diseñó para las comunidades científicas y de investigación, donde ofreció un gran ancho de banda. Esta red permitía que las universidades (miembros de Internet2), tuvieran la posibilidad de conectarse a los dos centros de supercomputo de NSF. Es así que primeramente se interconectaron a la red vBNS, conectándose a través de OC-3 y OC-12 vía ATM y SONET logrando tener velocidades de 155 Mbps hasta 622 Mbps. Posteriormente se hicieron las negociaciones a cargo de UCAID, con otros socios para la construcción de la red Abilene que a lo largo de 1998 se diseñó y ensambló, donde la arquitectura core de Abilene se componía de la siguiente manera:

- Cisco 12008 GSR (Gigabit Switch Router)
- ICS Unix PC: IPPM and Network Mgmt.
- Cisco 3640 para el acceso remoto al NOC (Network Operation Center)
- 100BaseT para LAN y acceso "puerto de consola"
- Controlador de potencia remota de 48vDC

En el año de 1999 entró en operación la red Abilene la cual tenía la capacidad de fibra óptica por parte de Qwest (13,000 millas de fibra óptica), la tecnología SONET de Nortel y los Router (GSR 12008) de Cisco. De 1999 a 2003 esta red se conectaba con OC-48, los cuales conectaron 11 nodos (Core Router), estos estaban ubicados en Seattle, Denver, Sunnyvale (anteriormente este nodo estaba en Sacramento), Los Ángeles, Houston, Kansas, Atlanta, Indianápolis, Washington, New York y Chicago como se muestra en la figura 2.6. Así mismo se podía acceder a esta red por medio de OC-3 u OC- 12, utilizando POS (Packet Over SONET) o ATM (en este periodo el número de conexiones fue decreciendo), con esta arquitectura se lograba una velocidad de 2.5 Gbps [43,51].

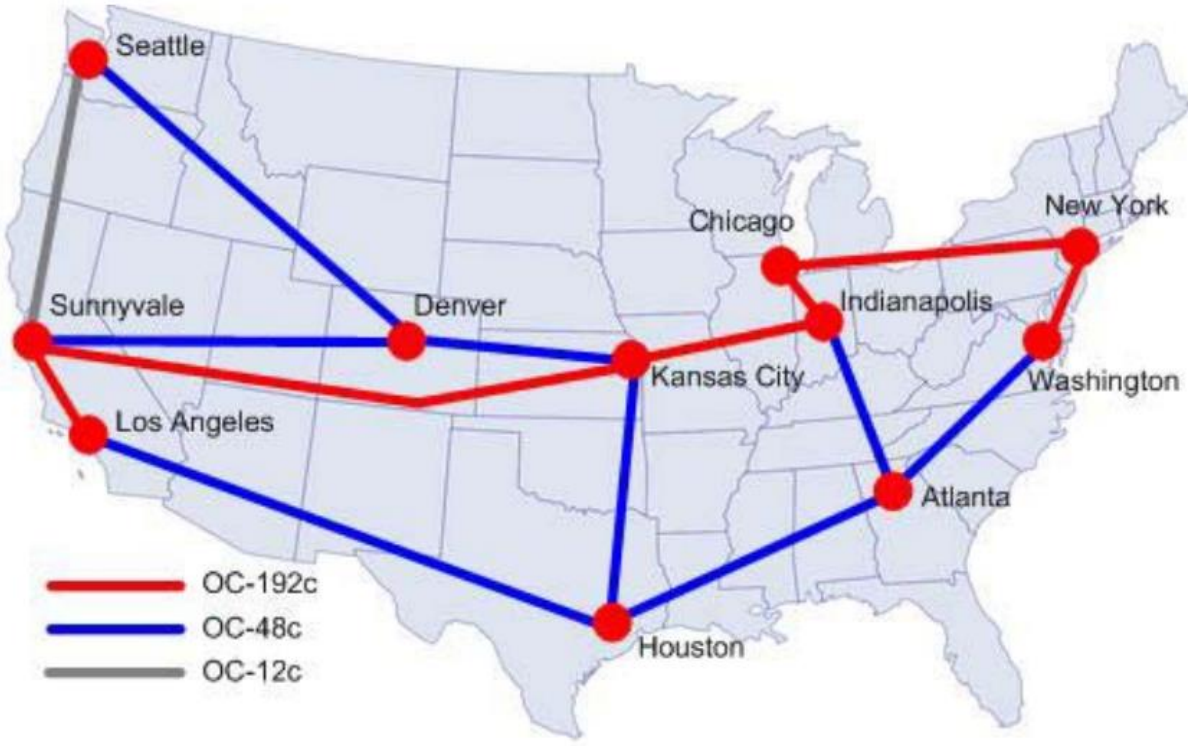


Figura 2.6 Backbone Abilene 2003 con 11 nodos [52]

A finales de 2007 fue cuando Level 3 Communications dio a conocer el nuevo backbone de Internet2 el cual sustituyó a la red Abilene lo cual se logró con el apoyo de Juniper Networks, Infinera, Ciena, entre otros. Esta nueva infraestructura contaba con 13,000 millas de fibra óptica [46,53].

La implementación física de este nuevo backbone se compuso de 3 redes robustas, lógicamente diferentes, pero relacionadas entre sí, las cuales son; Advanced IP Network, Virtual Circuit Network y Core Optical Network. Esta infraestructura completamente nueva se compuso principalmente de 9 nodos "IP Router (Router Core)" (advanced layer 3 service), 21 nodos "Optical Switching (Core Director)" de Ciena (advanced layer 2 service) y 27 nodos "Optical Core" proporcionados por Infinera (advanced layer 1 service). Los 9 nodos de los "Core Router" se ubicaron en Seattle, Los Ángeles, Salt Lake, Chicago, Atlanta, Houston, Kansas, New York y Washington, en donde se explotó más la tecnología DWDM, conectándose con enlaces 10 GbE (aunque aún se tenían algunos enlaces OC-192), así mismo se contaba con los Juniper T-640 que se re-utilizaron de Abilene pero se reemplazaron por los "Routers Juniper T-1600", logrando que esta nueva red tuviera un ancho de banda superior a los 10 Gbps suficientemente grande para las aplicaciones que se estaban desarrollando en Internet2 [54, 55, 56].

En 2014 se terminaron de cambiar todos los routers por los Juniper MX-960, y en 2016 contaba con 17 routers de este modelo, donde 15 de ellos se utilizaron para nodos "IP Router" (advanced layer 3 service) ubicados en Seattle, Sunnyvale, Los Angeles, Salt Lake, Kansas, Dallas, Houton, Atlanta, Chicago, Indianapolis, Washington, Ashburn, Cleveland y en New York (2 nodos), 39 nodos para "Optical Switching" (advanced layer 2 service) y 63 nodos para "Optical core" (advanced layer 1 service). La infraestructura de backbone de 2016 se muestra en la figura 2.7 la cual se tiene una velocidad de 100 Gbps tanto en capa 3 como en capa 2. Comparándola con la topología de 2013 hay aumento en los nodos de capa 3 (5 nodos más) y capa 2 (38 nodos más), así como un nodo menos en capa 1, así como el aumento de 15,717 millas de fibra oscura (fibra donde no pasan señales ópticas).

La red diseñada en 2007 tiene la facilidad de ser escalable en cuestión de infraestructura para cumplir con la demanda de la comunidad de Internet2, donde ha estado creciendo año con año. En 2016 se anunció la primera fase para la siguiente actualización, comenzando por el nodo de Seattle, cuyos objetivos son el de mejorar en los tipos y calidad de servicio de red avanzada y

el de apoyar más las necesidades de redes experimentales de la comunidad (explotación total de SDN) [57, 58].

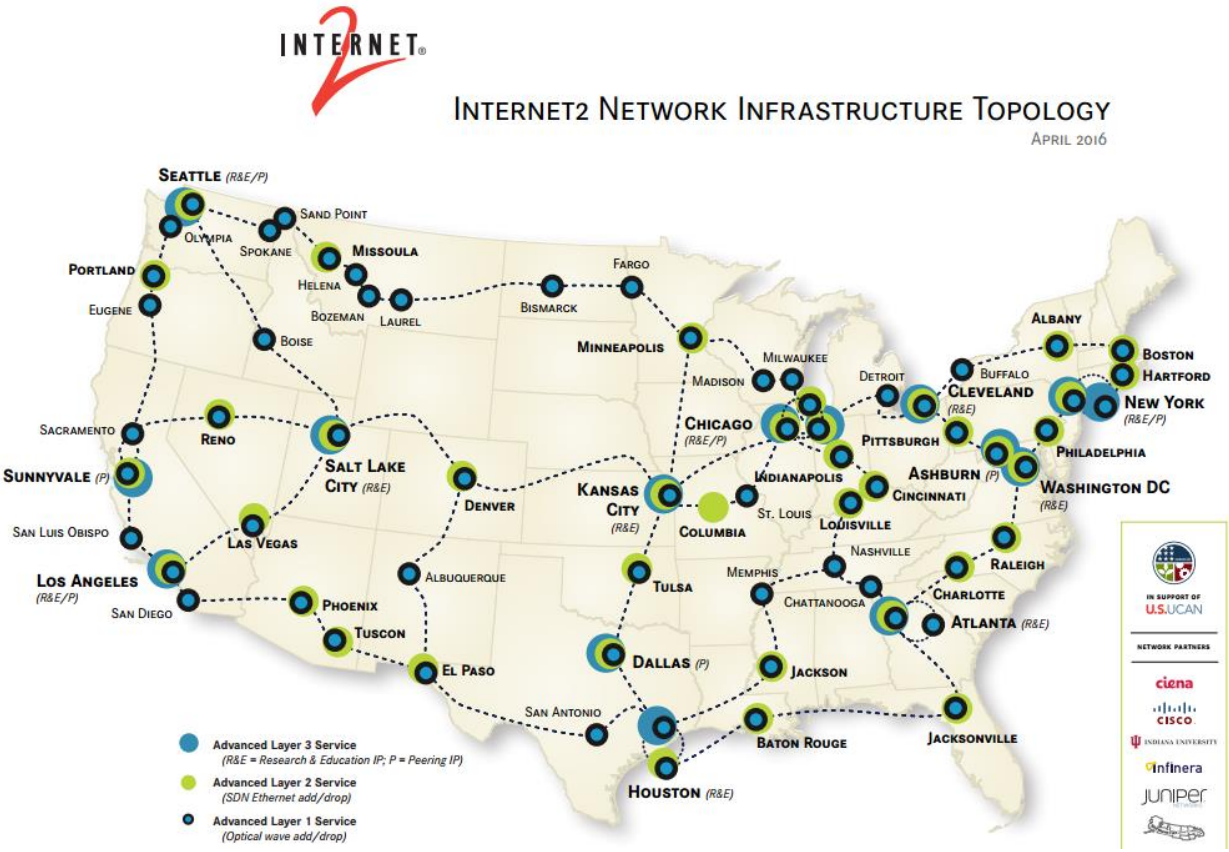


Figura 2.7 Backbone de Internet2 de 2016 [58]

En la siguiente sección se describe la red avanzada que agrupa a varios países de Latinoamerica, esta red es llamada CLARA.

II.5 Red CLARA

Ya que diferentes RA comenzaron a surgir a finales de la década de los 90, debido a las iniciativas de NREN, América Latina trabajo en un proyecto en donde se juntarian las principales NREN para ser conectadas con las RA de Europa, posteriormente también se tendría la conexión con Internet2 y otras RA. El organismo que llevo a cabo la coordinación de las principales NREN de América Latina es la red de Cooperación Latino Americana de Redes Avanzadas (CLARA). Otorgando a científicos, académicos e investigadores la infraestructura que les permita colaborar con la comunidad científica global.

En 2016 la misión de CLARA es:

"Fortalecer el desarrollo de la ciencia, educación, la cultura y la innovación en América Latina a través del uso innovador de RA" [59]

Esta red que conforma las principales RA de América Latina, año con año sigue haciendo un esfuerzo por interconectar a más países de América Latina con redes alrededor del mundo para poder contribuir a la educación, investigación y contribución de varios proyectos.

La red CLARA nació a finales del año 2003 pero fue establecida en 2004 gracias al proyecto ALICE (América Latina Interconectada con Europa), posteriormente la red mejoró sus capacidades debido al proyecto ALICE2 con lo cual conectó a la red GEANT2 desde Brasil mismo punto el cual conectó con EEUU por Miami. Actualmente los miembros que conforman la red CLARA son: Argentina, Brasil, Colombia, Chile, Ecuador, El Salvador, Guatemala, Perú y México.

Debido a que CLARA ha estado en constante evolución está optando por ofrecer servicios de conectividad (conectividad avanzada y pública), así mismo ha creado diferentes programas y proyectos para integrar diferentes comunidades científicas para un tema en específico como puede ser TICAL (Red de Directores de Tecnologías de Información y Comunicación de las Universidades Latinoamericanas), MAGIC (Middleware for collaborative Applications and Global virtual Communities) la cual integra cuatro comunidades globales de ciencia (e-salud, biodiversidad, medio ambiente e instrumentación remota) [60,61].

II.5.1 Topología de CLARA

Cuando el backbone de CLARA empezó a funcionar, este ofrecía 155 Mbps, ubicando sus "Core Router (Cisco 12400)" en México, Brasil, Argentina, Chile y Panamá como se muestra en la figura 2.8. Para el 2005 Cisco apoyo a las redes de Bolivia, Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua con "Routers 7206" para poder conectarse a CLARA. En años posteriores se actualizarían algunos enlaces para llegar a tener un poco más de 1 Gbps [62,63].

Figura 2.8 Topología del Backbone de CLARA de 2004 con 5 nodos [64]

El backbone de CLARA de 2016 está compuesto por 13 nodos, conectados a una topología punto a punto en donde cada nodo representa a un PoP (Point of Presence), doce de ellos ubicados en; México, Guatemala, El Salvador, Costa Rica, Panamá, Colombia, Venezuela, Perú, Ecuador, Chile, Brasil y Argentina mientras que el treceavo se encuentra en Miami. Esta red ofrece velocidades entre 1 y 10 Gbps en diferentes áreas de América Latina como se muestra en la figura 2.9.

Figura 2.9 Topología del Backbone de CLARA de 2016 con 13 nodos [64]

El 7 de julio de 2016 se activaron las 2 conexiones de 100 Gbps entre Miami y Sao Paulo (Brasil), esto financiado por: NSF (National Science Foundation), FAPESP (Fundación de Amparo a la investigación del Estado de Sao Paulo) y RNP (Red Nacional de Educación e Investigación), mismos que pretenden agregar 6 enlaces más para el 2017. Por lo que con estas capacidades estarían preparadas para la demanda que se está proyectando en los próximos 3 años. La red CLARA tiene como visión que para el año 2017 tengan asociados al 80% de América Latina [65].

A continuación se mencionan las conexiones internacionales que hacen posible la conectividad de las 3 RA que se describieron, asi como una breve descripción de las conexiones con otras RA de diferentes continentes.

II.6 Conexiones internacionales del Backbone de América

Hoy en día se han desarrollado diferentes RA en todo el mundo dedicadas a la investigación y educación llamadas REN (Research and Education Network), casi todos los continentes tienen un organismo el cual coordina ese tipo de redes. Es por ello que existen las llamadas "Multinational Networks" (redes multinacionales), siendo un conjunto de RA interconectadas, las cuales están conformadas por diferentes países, a su vez, cada país tiene interconectadas a diferentes universidades [66,67].

A continuación se mencionan algunas de estas redes multinacionales: para la gran parte de Europa se tiene a GEANT (Gigabit European Academic Network) (40 países conectados), para Latinoamérica está la red CLARA (13 países conectados), para parte de Asia y algunos países del pacífico se encuentra APAN (Asia Pacific Advanced Network, 42 países conectados), NorduNet conecta a los países nórdicos (5 países), se tiene a TEIN*CC (Trans-Eurasia Information Network *Cooperation Center, 20 países) red que conecta algunos países de Asia y Oceania, UbuntuNet (15 países) y WACREN (West And Central African Research And Education Network, 8 países) son las dos redes multinacionales las que interconectan gran parte de los países en África mismas forman la red "African connect 2"[68, 69].

Uno de los primeros puntos internacionales de América, siendo este de mucha importancia debido a que conecto a CANARIE con Internet2 y a su vez abrió paso a la conexión con las demás redes de Europa y Asia fue el GigaPop ubicado en Chicago (EEUU). A este punto se le denominó STARTAP (Science Technology And Research Transit Access Point) que por varios años fue utilizado por todas las NREN de distintos países para poder tener conexión entre estas RA. Así como fueron evolucionando las RA de América, también se fue dando esta misma evolución en los enlaces transatlánticos para poder conectar las RA de los diferentes continentes. En 2016 se tienen los suficientes enlaces transatlánticos de altas velocidades para poder interconectar todas estas RA, específicamente hablando del continente Americano con los demás continentes. A cargo de Pacific wave/TransPAC, se encarga de la interconexión con Asia, Oceanía y el pacífico, Atlantic Wave que en colaboración con AMPATH (America's PATH) da conexión a Latinoamérica y el Caribe, la iniciativa ANA (Advanced North Atlantic) y el proyecto ACE (America Connects to Europe) hacen la conexión con Europa, y StarLight que da conexión a la red avanzada de Canadá (CANARIE), Internet2, Europa y Asia [70,71, 72, 73, 74,75].

Los puntos de interconexión internacional más importantes los tiene Internet2, junto a través de estos puntos que posee, CANARIE y la red CLARA también pueden conectarse con las redes internacionales, y así puedan hacer uso de los 100 GE, estos puntos de interconexión se encuentran en: Seattle, Sunnyvale, Los Ángeles, donde estos 3 puntos se conectan por medio de Pacificwave/TransPAC, Chicago (por Starlight), en Miami se encuentra la interconexión de AMPATH y a través de MANLAN (ManhattanLanding) ubicado en New York y WIX (Washington International Exchange) ubicado en Washington D.C, siendo estos dos últimos los que se conectan a ANA.

En 2016 las RA de CANARIE, Internet2 y CLARA tiene las siguientes interconexiones: CANARIE se conecta con Internet2 por medio de Seattle, Chicago y New York con enlaces de 100 Gbps y a su vez Internet2 se conecta con CANARIE por medio de Victoria,Vancouver, Winnipeg, Windor, Toronto y Halifax. Para la interconexión de CLARA con Internet2 lo hace atraves de Miami y El Paso con enlaces de 10 y 1 Gbps respectivamente, pero para conectarse a GEANT lo hace con el enlace dedicado de 5 Gbps que se ubica en San Paulo Brasil. CANARIE también se conecta con GEANT por medio de Chicago y Los Ángeles, y con Seattle conecta con las RA de Asia [72,76].

En la figura 2.10 se muestran las diferentes conexiones que tiene el continente Americano hacia las redes multinacionales más importantes, como se observa no existe una velocidad común en estas conexiones, pero en promedio la velocidad oscila entre los 10 Gbps y 100 Gbps, cabe mencionar que aún existen enlaces de backbone con bajas velocidades en los que aún se están trabajando como es el caso de África y Latinoamérica. Hay que destacar los enlaces transatlánticos que se están implementado con lo que se está logrando tener velocidades de 100 Gbps, ANA ha sido el proyecto más importante para llevar a cabo estos enlaces de mayor velocidad y sigue mejorando, en donde se espera en un tiempo corto tener a ANA-300 Gbps, en 2016 se contaba con ANA-200 Gbps debido a sus dos enlaces de 100 Gbps en anillo como se alcanza apreciar en la figura 2.10 [77, 78,79].

Es de suma importancia saber lo anterior debido que para lograr el objetivo de esta tesis se requiere previamente de conectar los backbone de las 3 redes de América; CANARIE, I2 y la red CLARA, para obtener una red backbone interconectada que cubra todo el continente Americano.

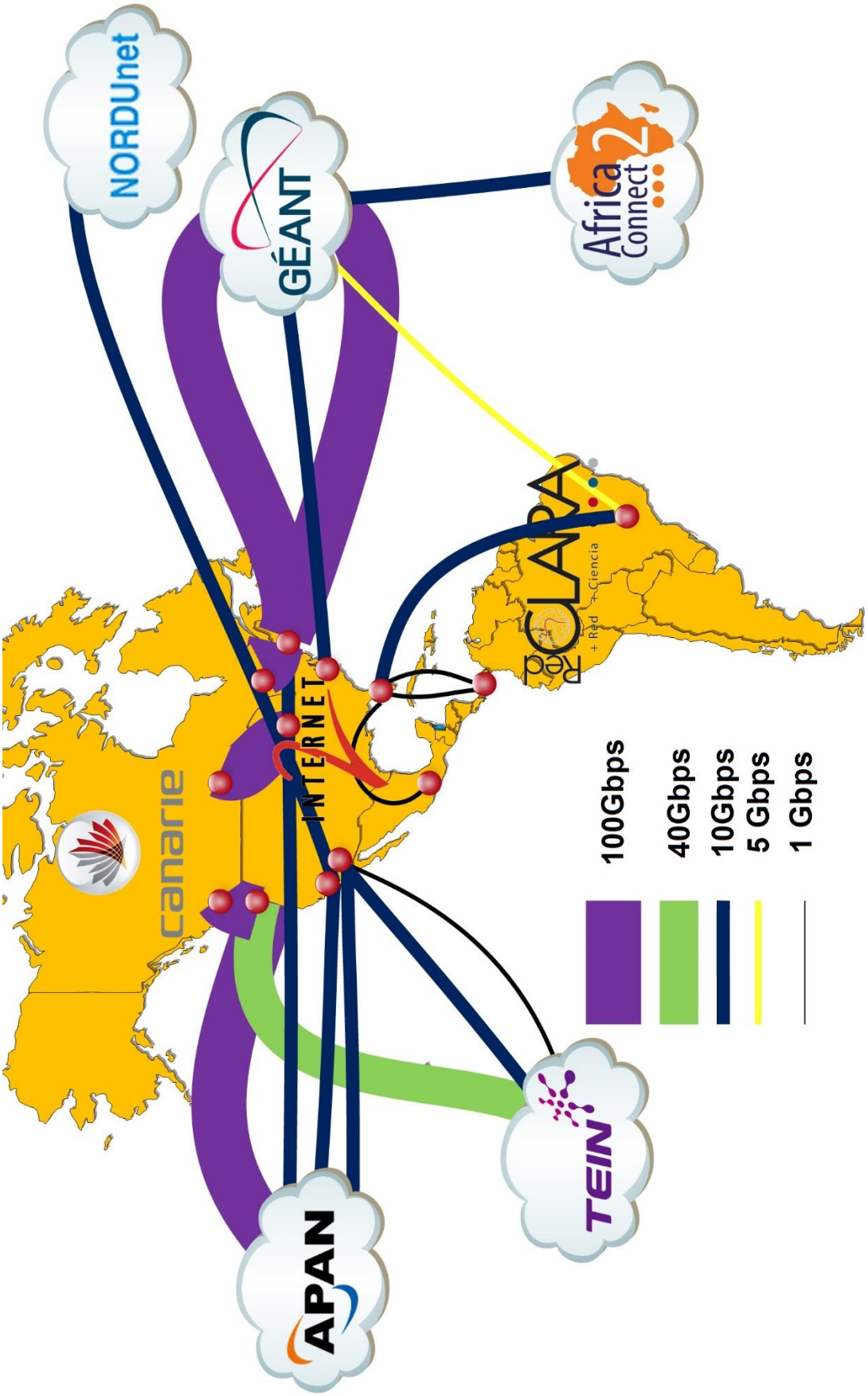


Figura 2.10 Conexiones internacionales de Backbone de CANARIE, Internet2 y CLARA de 2016 (Diagrama propio con base en [44,46, 80, 81, 82,83, 84])

Aquí termina el estudio y revisión de las RA que operan dentro del continente americano asi como las conexiones internacionales que hacen posible la conexión de estas tres RA. En el siguiente capitulo se hace la revisión de los protocolos de enrutamiento y de gestión, los cuales, son importantes para la parte metodológica de la simulacion y emulación.

Capítulo III

Protocolos de enrutamiento y de gestión

"En no mucho tiempo contaremos con unas líneas inteligentes y que estarán integradas totalmente con la Red"

Vinton Gray Cerf

III.1 Protocolos de enrutamiento

El enrutamiento es la función principal de cada Router, mismo que se puede definir como *"el acto de mover información a través de una interconexión desde su origen hasta su destino"* [85], debido a que se encarga de hacer la conexión de host a host, también asegura el envio de la tabla de enrutamiento, la cual refleja la topología de la red, todo este enrutamiento se da gracias a los protocolos de enrutamiento. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento donde estos completan las tablas de enrutamiento con la selección de las mejores rutas que el protocolo de enrutamiento debe seguir. Así mismo proporcionan al router la información que necesita acerca de la red utilizando métricas [85,86].

Una métrica es un estándar de medición o valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas, se utiliza para determinar que ruta es la adecuada cuando existen múltiples rutas hacia el mismo destino donde cada protocolo tiene su propia métrica, los tipos de métricas pueden ser [87, 88,89]:

- Conteo de saltos: cuenta la cantidad de routers que un paquete tiene que atravesar hasta llegar a su destino.
- Ancho de banda: selecciona la ruta con el mejor ancho de banda disponible
- Carga: considera el tráfico de un enlace determinado.
- Retardo: considera el tiempo en que tarda un paquete en atravesar una ruta.
- Confiabilidad: evalúa la probabilidad de fallas de enlace calculada a partir de las fallas ocurridas previamente en la interfaz o en el enlace.
- Costo: puede representar una métrica ya que es un valor que determina el IOS (Internetwork Operative System) o el administrador para indicar la preferencia de la mejor ruta.
- MTU (Maximum Transmisión Unit): referencia la longitud máxima de datos de la trama de nivel de enlace que puede ser aceptada por los enlaces de la ruta

Cada protocolo de enrutamiento está diseñado con un algoritmo de enrutamiento, siendo estos los que: inician, mantienen y llenan de información a las tablas de enrutamiento, está información sobre la ruta puede ser variada dependiendo del algoritmo que se utilice. Cabe decír que algunos algoritmos tienen uno o más de los siguientes objetivos dentro de su diseño [85]:

- Optimalidad: Capacidad del algoritmo para seleccionar la mejor ruta.

- Simplicidad y bajo costo operativo: La ejecución del algoritmo deber ser de manera eficiente, debe consumir un mínimo de recursos del CPU.
- Robustez y estabilidad: Los algoritmos deben afrontar las circunstancias inusuales o imprevistas ya sea fallos de hardware, condiciones de carga alta, o implementaciones incorrectas.
- Convergencia rápida y flexibilidad: Los algoritmos deben de distribuir los mensajes de actualizaciones de manera rápida en todos los routers ya que si no lo hacen se pueden crear bucles dentro de la red.

Los principales Algoritmos de enrutamiento son Bellman-Ford y Dijkstra:

- Bellman-Ford: Se le denomina un algoritmo interactivo debido a que todos los nodos intercambian información donde el proceso termina hasta que ningún nodo intercambie información, es asíncrono debido a que no todos los nodos operan síncronamente con otros nodos, este algoritmo distribuye información, esto es, cada nodo recibe información de los nodos conectados a él mismo, donde la información se vuelve a distribuir a los mismos vecinos después de efectuar el cálculo del algoritmo. Al final el camino más corto tendrá como costo la suma de todas las métricas de cada uno de los enlaces por los que ha pasado el algoritmo [89,90].
- Dijkstra: Es un algoritmo de cálculo de ruta basado en el estado del enlace, donde cada enlace está determinado por una métrica por lo que tendrá un valor numérico asociado (valor inversamente proporcional a la capacidad del enlace y proporcional a la carga), la ruta óptima será aquella que menor métrica calculada tenga. Este algoritmo calcula el camino de costo mínimo desde un nodo al resto de los nodos de la red, siendo un algoritmo iteractivo donde en la k-ésima interacción se conocen todos los caminos con el costo mínimo a k nodos distintos entre los k-caminos con el menor costo así como todos los nodos de destinos posibles [91, 92,93].

Por otro lado existen 2 tipos de enrutamiento:

- Enrutamiento estático: Este tipo de enrutamiento presenta tablas de enrutamiento asignadas por el administrador de red por lo que no se le considera la aplicación de algún algoritmo de enrutamiento, el enrutamiento estático no puede reaccionar a cambios en la red ya que no se consideran aptos para redes grandes (WAN y MAN), este tipo de enrutamiento se utilizan en redes donde su diseño es relativamente simple mismo que contiene tráfico de red

predecible. Aun así el enrutamiento estático pueden tener cierta ventaja la cual es tener una mayor seguridad de la red debido a su configuración manual así como el uso eficiente del equipo y del ancho de banda.

- Enrutamiento dinámico: Es el enrutamiento dominante donde se utilizan los protocolos de enrutamiento debido a que es un enrutamiento más "poderoso" y complejo, ya que se utiliza para el descubrimiento de red, así como la actualización y mantenimiento de las tablas de enrutamiento. Por lo mismo, este tipo de enrutamiento requiere menos sobrecarga administrativa, pero el costo de usar estos protocolos es dedicar parte de los recursos de un router para la operación del protocolo, incluyendo el tiempo de procesamiento del CPU y el ancho de banda del enlace de la red. La mejor ruta es elegida por un protocolo de enrutamiento en función al valor o la métrica que usa para determinar la distancia para llegar a esa red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta métrica [88,90, 91].

III.1.1 Clasificación de los protocolos de enrutamiento dinámico

A medida que fue evolucionando Internet, se fueron desarrollando diferentes algoritmos de enrutamiento, mismos que son aplicados en diferentes protocolos de enrutamiento dinámico que aún se siguen implementando. La evolución de estos protocolos de enrutamiento dinamico se fue dando durante un largo periodo de tiempo, en la figura 3.1 se muestra una línea del tiempo donde se aprecia la transición de los protocolos de enrutamiento con su respetivo año de lanzamiento y su RFC (Request For Comments) correspondiente al año en que se publicaron ya que en nuestros días tienen un RFC diferente debido a la actualizaciones y modificaciones que ha tenido la documentación del protocolo.

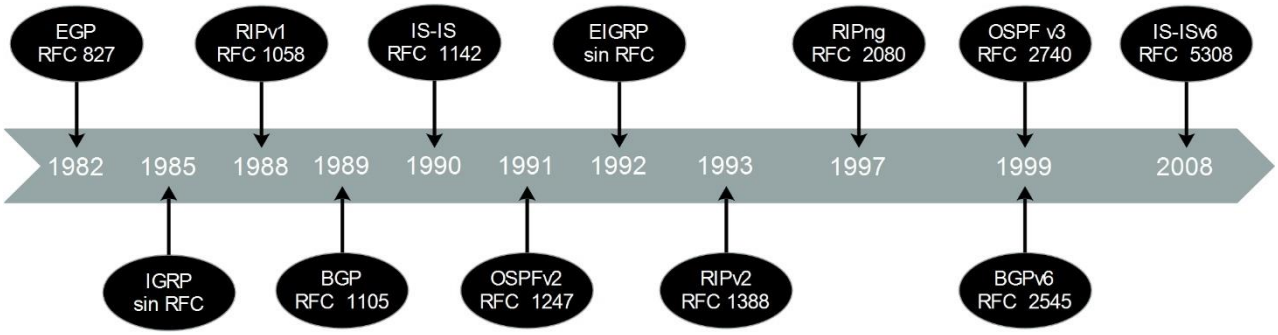


Figura 3.1 Línea del tiempo de los protocolos de enrutamiento (diagrama propio con base en [89])

Los protocolos de enrutamiento dinámico se dividen en dos grandes clases; "Interior Gateway Protocol (IGP)" y "Exterior Gateway Protocolo (EGP)", los protocolos del tipo IGP son usados dentro de un "Autonomous System (AS)" o intranets y para los protocolos de enrutamiento del tipo EGP funcionan con diferentes AS. Donde un AS es un conjunto de routers bajo una misma administración, como pueden ser los ISPs (Internet Servie Provider) y Backbone Netwoks. En la figura 3.2 se puede apreciar a grandes rasgos la clasificación de estos protocolos de enrutamiento dinámico [90].

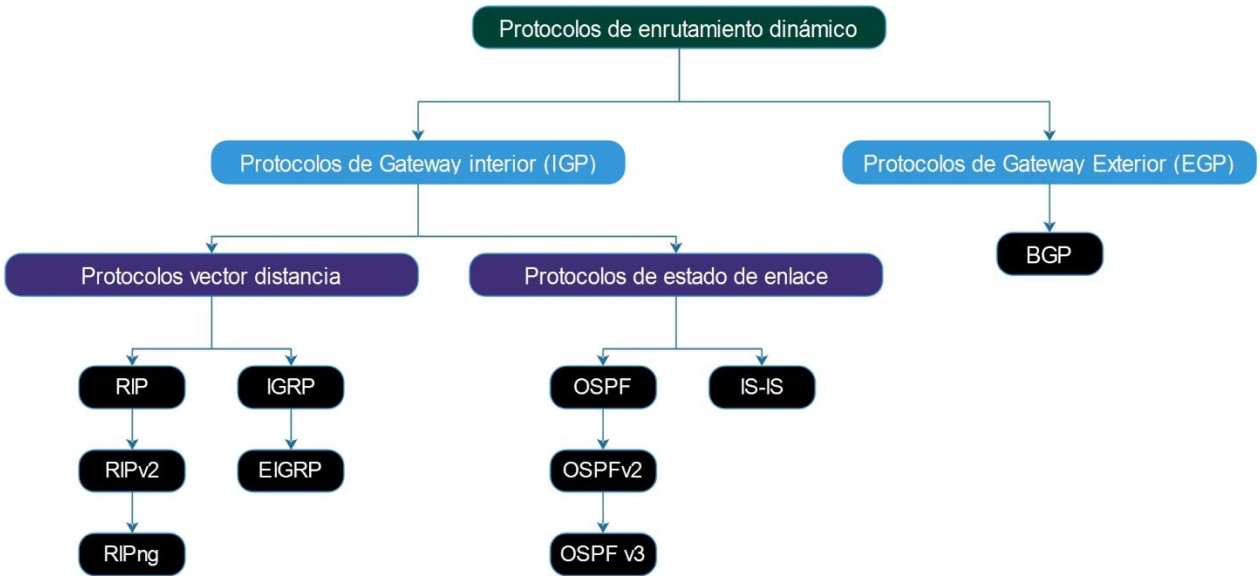


Figura 3.2 Clasificación general de los protocolo de enrutamiento dinámico. (Diagrama propio con referencia [90])

A continuación se describen la subdivisión de un IGP, siendo los protocolos vector distancia y estado de enlace:

- Protocolo vector distancia (ejemplo RIPv1, RIPv2): El protocolo vector distancia significa que las rutas son publicadas como vectores de distancia y dirección. La distancia se define en términos del conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida. Éste es un enrutamiento basado en los algoritmos Bellman-Ford, donde estos algoritmos pasan periódicamente información de sus tabla de enrutamiento a sus vecinos (routers), con esta información tiene que aprender acerca de las distancias que se tiene en la topología actual debido a que cada destinatario va agregando valor acerca de dicha distancia, por lo que se utilizan en pequeñas redes. El problema al que se enfrentan es al tiempo de convergencia entre los routers ya que durante este proceso la red puede ser vulnerable a un enrutamiento inconsistente mismo que puede llegar a crear un "loop" infinito de enrutamiento [86].

- Protocolo estado de enlace (ejemplo OSPF, IS-IS): Es un protocolo que puede usarse en redes de cualquier tamaño, siendo que puede crear una vista completa de la topología de la red al fluir la información de todos los demás routers, enviando información sólo cuando hay un cambio en la red. A este protocolo se le conoce como "Shortest Path First (SPF – Primera ruta más corta)", donde los protocolos mantienen una base de datos compleja de la topología de la red, desarrollan y mantienen un conocimiento completo de los router de la red así como la forma en que se conectan todos esos routers. Este intercambio se hace por medio de LSA (Link State Advertisement), por lo que todo router construye una base de datos topológica a partir de las LSAs recibidas [90,92].
- Protocolos Híbridos (ejemplo EIGRP, BGP): Se les denominan protocolos híbridos debido a que no sólo utilizan una única métrica para encontrar la mejor ruta, sino que pueden utilizar hasta 5 métricas distintas combinadas para poder decidir que ruta es la adecuada, en estos protocolos la convergencia se realiza más rápido en comparación de los demás protocolos.

Los punto críticos de los protocolos de enrutamiento son el tiempo de convergencia, siendo el tiempo en que los routers tardan en compartir información, calcular las mejores rutas y actualizar las tablas de enrutamiento, y también el cálculo de la ruta, el cual corresponde al tiempo de ejecución de un algoritmo de enrutamiento. Estos aspectos permiten la evaluación de los protocolos de enrutamiento. En la tabla 3.1 se aprecian los factores que influyen en estos puntos críticos [86,87].

Característica	Factores que influyen
Convergencia	• La distancia de un router desde el punto de cambio • El número de routers en la red que usan protocolos de enrutamiento dinámico • Ancho de banda y carga de tráfico con los enlaces de comunicación • Carga de un router • Protocolos de enrutamiento usados
Cálculo de ruta	• El protocolo calcula, almacena y tiene múltiples rutas para cada destino • Manera en que inician las actualizaciones de enrutamiento • La métrica o costo usado para calcular distancias

Tabla 3.1 factores de convergencia y cálculo de ruta.

Otro factor importante que los protocolos de enrutamiento tienen en cuenta es la distancia administrativa que está presente en cualquier tabla de enrutamiento. Esta distancia depende del

protocolo de enrutamiento que se emplea, en la tabla 3.2 se muestran las diferentes distancias administrativas que se manejan para cada protocolo [87].

Tipo de enrutamiento	Distancia administrativa
Conexión directa	0
Estática	1
EIGRP (resumen de ruta)	5
BGP (externo)	20
EIGRP (interno)	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1,RIPv2 y RIPng	120
EGP	140
EIGRP (externo)	170
BGP (interno)	200
Desconocido	255

Tabla 3.2 Distancia administrativa como métrica de los protocolos de enrutamiento.

A continuación se hace una revisión de RIP, OSPF y BGP, donde estos 2 últimos se utilizarán para la simulación y emulación. RIP se indica como el antecedente de los otros protocolos de enrutamiento.

III.1.2 RIP (Routing Information Protocol)

RIP fue uno de los primeros protocolos de enrutamiento que funcionó en un IGP, sus antecedentes se remontan al protocolo que usaba la Universidad de Berkeley llamado "*routed*", el cual operaba con el algoritmo Bellman-Ford, este mismo algoritmo se aplicó en el protocolo que usaban los sistemas de Xerox el cual denominaban *Protocolo de información de Gateway "GIP"* posteriormente lo llamaron RIP. Para 1988 RIP se lanzó como un estándar oficial en el RFC 1058, mismo que revolucionó el enrutamiento debido a que las tablas de enrutamiento y la actualización se hacían dinámicamente sin la intervención humana. Posteriormente se harían los cambios y mejoras para dar surgimiento a RIPv2 (1994), así como RIPng (1997) para poder ser utilizado con IPv6 [94,95].

III.1.2.1 RIPv1

Ripv1 es considerado como la primer versión antes de tener mejoras, tenía ciertas características las cuales se describen a continuación [95]:

- Protocolo vector distancia, el cual utiliza el algoritmo Bellman-Ford.
- Protocolo del tipo IGP.
- Utiliza como métrica el conteo de saltos para seleccionar la ruta adecuada, máximo 15 saltos si llegara a 16 la ruta es inalcanzable.
- Actualizaciones de mensajes cada 30 segundos.
- Tiempo de convergencia lento.
- Fácil implementación.
- Enrutamiento con clase (classfull)

El funcionamiento de RIP es simple, el router envía un paquete de actualización donde se encuentra una lista de toda las redes que conoce (dentro de esta lista incluye las redes que están directamente conectadas y las redes que ha aprendido de otros routers), la dirección de destino y la métrica asociada a cada destino. RIPv1 funciona con el protocolo UDP (User Datagram Protocol) a través del puerto 520, ya que todos los mensajes de RIP son encapsulados en un UDP con su respectivo campo de origen y destino.

Para la construcción de sus tablas de enrutamiento se tienen algunos factores; si en la actualización se encuentra con una ruta hacia otra red, esta ruta se añade, si hay una ruta conocida pero con mejor métrica esa ruta se utiliza. También elimina algunas rutas, lo puede hacer si la métrica de la ruta es mayor a 15 saltos. Además si un router no envía solicitudes durante 180 segundos los demás routers eliminarán la ruta hacia ese router. En la tabla 3.3 se muestran los temporizadores que utiliza RIP. Cuando un router descubre una nueva o mejor ruta desde la actualización se asume que el vecino del que recibió la actualización es el siguiente salto para la ruta, así el router le suma un salto a la métrica de entrada a la tabla de enrutamiento [94,96].

Temporizadores	Tiempo (segundos)	Descripción
Update	30	Tiempo de actualización
Invalid	180	Tiempo en que una ruta podría ser inválida
Hold down	180	Tiempo el cual suprime alguna ruta defectuosa
Flush	240	Tiempo en que se elimina la ruta inválida de la tabla de enrutamiento

Tabla 3.3 Temporizadores que emplea RIP [97]

En la figura 3.3 se muestra el formato de mensaje de RIP (el tamaño máximo del datagrama es de 512 Bytes), cada uno de los campos se explica a continuación:

Figura 3.3 Formato de mensaje de RIPv1 (diagrama propio con referencia [98])

- Comando: Este campo utiliza 1 si es un "Request message" (mensaje de solicitud): Mensaje que se usa para preguntar a sus vecinos para enviar actualizaciones. O utiliza 2 si es un "Response message" (mensaje de respuesta): Mensaje el cual lleva la actualización, con la información de sus tablas de enrutamiento y la métrica asociada a cada destino.
- Versión: Este campo identifica la versión de RIP que se usa; 1 para RIPv1 (posteriormente 2 para RIPv2).
- Identificador de dirección de familia: En este campo usa 2 para IP a menos que se realice la solicitud de una tabla de enrutamiento completa, cuyo caso se establecería un 0.
- Métrica: Campo que lleva el conteo de saltos (de 0 a 15). El router que realiza el envió aumenta la métrica a un salto antes de enviar un mensaje.
- Campos sin usar: Estos campos se reservaron para mejoras del protocolo su valor debe ser 0.
- Una de las problemáticas que tiene RIP es la creación de "loops" debido a la convergencia lenta que tiene, para poder corregír esta problemática se emplean "Split horizon"(horizonte

dividido) y "Poison reverse"(envenenado inverso); con "Split horizon" los routers no anuncian las rutas en el enlace del que se obtuvieron esas rutas y "Poison reverse" utiliza la idea de "Split horizon" pero añade una acción positiva a esa regla, de acuerdo con la cual un router debe anunciar una distancia infinita de ruta en el enlace [95,97].

III.1.2.2 RIPv2

RIPv2 (RFC 2453) no es un protocolo nuevo si no una extensión de RIPv1 (debido a las dificultades que presentaba) donde posee casi las mismas características que RIPv1, debido a las mejoras del protocolo las características adicionales a RIPv2 se describen a continuación [94, 95]:

- Agregación de máscara de subred (Classless,): posibilita la utilización de VLSM (Variable Length Subnet Mask) y CIDR (Classless Inter-Domain Routing).
- Dirección del siguiente salto incluidas en las actualizaciones de enrutamiento previniendo saltos innecesarios.
- Autenticación de actualización: Este podía reducir la posibilidad de aceptar actualizaciones erróneas de los sistemas mal configurados.
- Transmisión de actualizaciones a través de la dirección Multicast (utilizando la dirección 224.0.0.9 de la clase D): Se transmiten para reducir la carga en los sistemas que no eran capaces de procesar RIPv2 así como el tráfico global en la red.
- MIB para RIPv2: permite el seguimiento y control de la operación de RIP dentro del router
- Etiquetas de rutas externas, para saber si la ruta anunciada esta dentro o fuera del AS.

El funcionamiento de RIPv2 es similar a RIPv1 salvo que se utilizó de una mejor manera gracias a las características antes mencionadas. Así mismo en él se tiene una diferencia en su formato de mensaje, el cual no tuvo problema ya que RIPv1 contaba con varios campos vacíos. El mensaje de RIPv2 tuvo ligeras modificaciones en sus campos como se muestran en la figura 3.4 donde a continuación se explican sólo los campos agregados a dicho mensaje [98]:

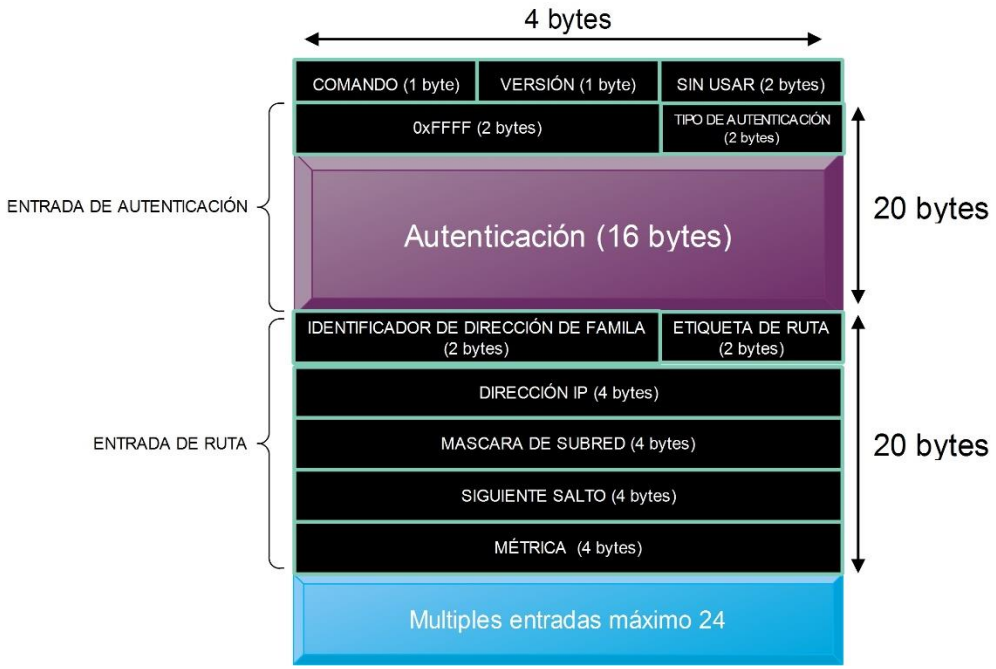


Figura 3.4 Formato de mensaje de RIPv2 con autenticación. (diagrama propio con base en [93])

- Etiqueta de ruta: Este campo se usa para diferenciar las rutas internas dentro de un dominio de enrutamiento RIP de rutas externas. Por lo que para rutas internas se coloca un 0 y para rutas externas se usa un número arbitrario o el número del sistema autónomo.
- Máscara de subred: Este campo permite el enrutamiento basado en la máscara de subred por lo que se puede utilizar VLSM.
- Siguiente salto: En este campo permite saber que salto se debe de realizar cuando tiene dos dominios de enrutamiento conectados.

Con RIPv2 se puede agregar una entrada de autenticación en el mensaje de RIPv2 donde se tienen los siguientes campos [95,99].

- Tipo de autenticación: Campo que se establece con un 2 para indicar que se trata de una simple contraseña de texto. Cisco aprovecha esta opción y ofrece la autenticación MD5 (Message Digest algorithm 5).
- 0xFFFF: Es similar al campo identificador de dirección de familia para autenticación. Se asigna todo el campo con “unos” en notación hexadecimal para identificar que es del tipo de autenticación.
- Autenticación: Campo que contiene la contraseña en 16 bytes. Debido a que la autenticación se considera como una entrada de ruta, el paquete de mensaje de RIPv2 sólo podrá admitir 24 entradas de ruta, cabe decir que si no se utiliza la autenticación se admitirían las 25 entradas de ruta

Existe una versión de RIP la cual funciona con direcciones IPv6 de acuerdo a las referencias [94] y [100], sin embargo queda fuera del alcance de esta obra.

III.1.3 OSPF (Open Shortest Path First)

En 1988 un grupo de trabajo se formó para el diseño de un protocolo basado en el algoritmo de la "primera ruta más corta (SPF)", debido a que RIP era incapaz de interconectar redes más grandes, por ello se creo un nuevo protocolo para solventar esta limitación, es así que en 1989 se dio a conocer en el RFC 1131 el cual presentó la primera versión de OSPF, solo fue un protocolo experimental por lo que nunca se implementó. Seria la segunda versión de OSPF la que se implementaría.

III.1.3.1 OSPFv2

En 1991 se desarrolló OSPFv2 y es la versión que actualmente se implementa en un IGP el cual está referenciado en el RFC 2328, a diferencia de RIP este protocolo lleva un registro de todas las posibles rutas utilizando métodos diferentes de RIP para evitar bucles de enrutamiento. A continuación se describen algunas características de OSPF [89,101]:

- Protocolo de estado de enlace: utiliza el algoritmo Dijkstra para calcular el camino más corto.
- Funciona con dirección IP sin clase lo que permite el soporte de VLSM y CIDR.
- Convergencia rápida, lo cual evita los bucles de paquetes.
- Alto uso del CPU del router, debido a que debe calcular más datos con el objetivo de reducir el tráfico de la red.
- Acepta autenticación para tener mayor seguridad.
- Su métrica es el costo, por lo que para ello utiliza el ancho de banda disponible.
- Utiliza direcciones Multicast para el envió de actualizaciones (224.0.0.5 y 224.0.0.6).
- Envía actualizaciones incrementales.
- Provee jerarquización de la red debido a que utiliza diferentes áreas.
- Todo el tráfico de OSPF se encapsula en paquetes IP mediante el puerto 89.
- El protocolo se activa por interfaz.

OSPF utiliza LSA (Link State Advertisement – Notificación del estado del enlace) que son los anuncios para listar todas las rutas posibles, en la tabla 3.4 se enlistan los tipos de LSA con los

que funciona OSPF. Las LSA del tipo 1 y 2 se envían dentro de todo un área y son empleadas por OSPF para elegir la ruta, las del tipo 3 y 4 pasan información entre áreas.

Tipo de LSA	Descripción
Tipo 1: "Router link LSA"	Cada uno de los routers genera LSA listando el costo hacia cada uno
Tipo 2: "Network link LSA"	Son las LSA enviadas por el router designado (DR) el cual contiene una lista de todos los routers con el que el DR forma adyacencias
Tipo 3: "Network summary link LSA"	Son las LSA generadas por los ABR para ser enviados entre áreas
Tipo 4: "AS external ASBR summary link LSA"	Son las LSAs para advertir a otros routers de como alcanzar al ASBR
Tipo 5: "External link LSA"	Son LSA originadas por un ASBR donde inundan todo el AS con información de rutas externas OSPF

Tabla 3.4 Tipos de LSA [93,101].

El protocolo OSPF trabaja dentro de un AS, pero para que OSPF pueda realizar su funcionamiento de una manera más fácil el AS se puede dividir en diferentes áreas manteniendo el dominio de OSPF, en esta segmentación de áreas, se encuentra un área 0 o de Backbone y las demás áreas se identifican por algún número asignado (área 1,2, 3,...etc.), un área de OSPF es una agrupación lógica de routers que están ejecutando OSPF y que comparten la misma información de la base de datos topológica, esta área es una subdivisión del domino de OSPF. El uso de múltiples áreas elimina la necesidad de comunicar todos los detalles a cada uno de los routers, también permite que los routers dentro de un área puedan mantener limitado la base de datos topológica, con estas pequeñas áreas contribuyen a tener un mejor rendimiento por lo que hará que los routers tengan menos desgaste del CPU y el poder tener un mejor rendimiento aun cuando la red este en proceso de escalabilidad.

En la figura 3.5 se muestra un esquema general del modelo jerárquico por áreas, asi como la descripción, función y nombre correspondiente para algunos routers [93, 101].

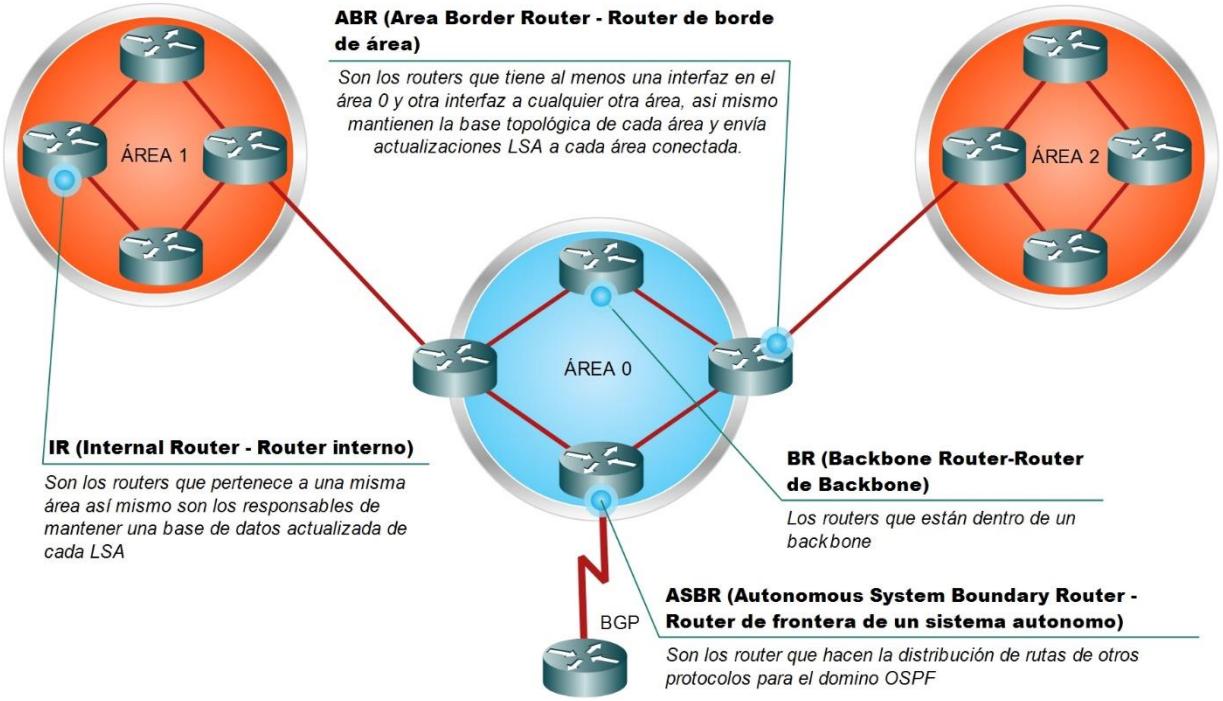


Figura 3.5 Áreas de funcionamiento de OSPF (diagrama propio con base en [93, 101])

El funcionamiento de OSPF en múltiples áreas funciona de la siguiente manera; los routers ABR generan propagaciones de LSA del tipo 3 y las envía al área de backbone, las adyacencias entre las áreas utilizan LSA del tipo 1 y 2 que pasan al área de backbone como LSA del tipo 3 y que a su vez inyectadas por otros ABR. Las rutas externas son recibidas por el ABR y enviadas al área local.

Cabe mencionar que existen otro tipo de áreas dependiendo de la utilización en la red. Estas áreas son; "Área estándar u ordinaria", en esta área todos los routers tiene conocimiento de todos los prefijos que hay en ella, así como la misma base de datos topológica, y la área "stub" donde esta área no acepta LSA de tipo 5, en lugar de inyectar LSA de tipo 5 el ABR crea una ruta por defecto que es enviada a los router internos para que la elijan como camino viable. Existen dos áreas más pero son propiedad de cisco ("totally stubby are" y "Not-So-Stubby-Area") [93, 102].

OSPF funciona con el anuncio de listas de sus conexiones, esto es, si un enlace se activa o se cae, se envían LSAs, que son compartidas por los vecinos (routes conectados entre si), así como la base topológica LSDB (Link State Database). Las LSAs se identifican con un número de secuencia para reconocer las más recientes en un rango de 0x8000 0001 a 0FFFF FFFF. Cuando los routers convergen tiene la misma LSDB, a partir de este momento el algoritmo Dijkstra sólo es capaz de determinar la mejor ruta hacia el destino. La tabla de la topología que tiene el router,

es la topología en la que se encuentra el router dentro de un área, esta tabla de topología y base de datos se actualizan por cada LSA que envía cada router dentro de la misma área.

Para que OSPF opere se ayuda de 3 tablas, tabla de vecinos, tabla de topologías y tabla de enrutamiento, así mismo de su respectiva métrica que es el costo, la cual se calcula a partir de la ecuación 1:

$$costo = \frac{10^8 bps}{Ancho\ de\ banda\ del\ enlace} \quad (1)$$

Si existen varios caminos para llegar al destino con el mismo costo, OSPF efectúa un balanceo de carga de 4 rutas diferentes. El valor del costo es de 16 bits por lo que el administrador lo puede configurar, algunos costos de interfaz con su respectivo cambio se muestran en la tabla 3.5:

Tipo de enlace	Ancho de banda	Costo por default	Cambio de ancho de banda con referencia a 100 Gbps
9.6 kbps	9.6 kbps	10, 416	10,416,666
56 kbps	56 kbps	1,785	1,785,714
64 kbps	64 kbps	1,562	1,562,500
T1	1.5 Mbps	64	66,666
E1	2.048 Mbps	48	48,828
T3	45 Mbps	2	2222
4 Mbps Token Ring	4 Mbps	25	2,5000
16 Mbps Token Ring	16 Mbps	6	6250
Ethernet	10 Mbps	10	10000
Fast Ethernet	100 Mbps	1	1000
Gigabit Ethernet	1 Gbps	1	100
10 Gigabit Ethernet	10 Gbps	1	10
100 Gigabit Ethernet	100 Gbps	1	1

Tabla 3.5 Costos que utiliza OSPF [89,101].

OSPF va descubriendo a todos sus vecinos y sus respectivos enlaces, esto lo hace a través de paquetes "hello" los cuales se envían con la dirección Multicast 224.0.0.5, una vez que los routers hayan intercambiado dichos paquetes comienzan a intercambiar información acerca de la red y una vez que esa información se tenga sincronizada los routers habrán formado adyacencias, por lo que han llegado a un estado "full". En la figura 3.6 se muestra la serie de estados por la que los routers pasan hasta llegar al estado "full".

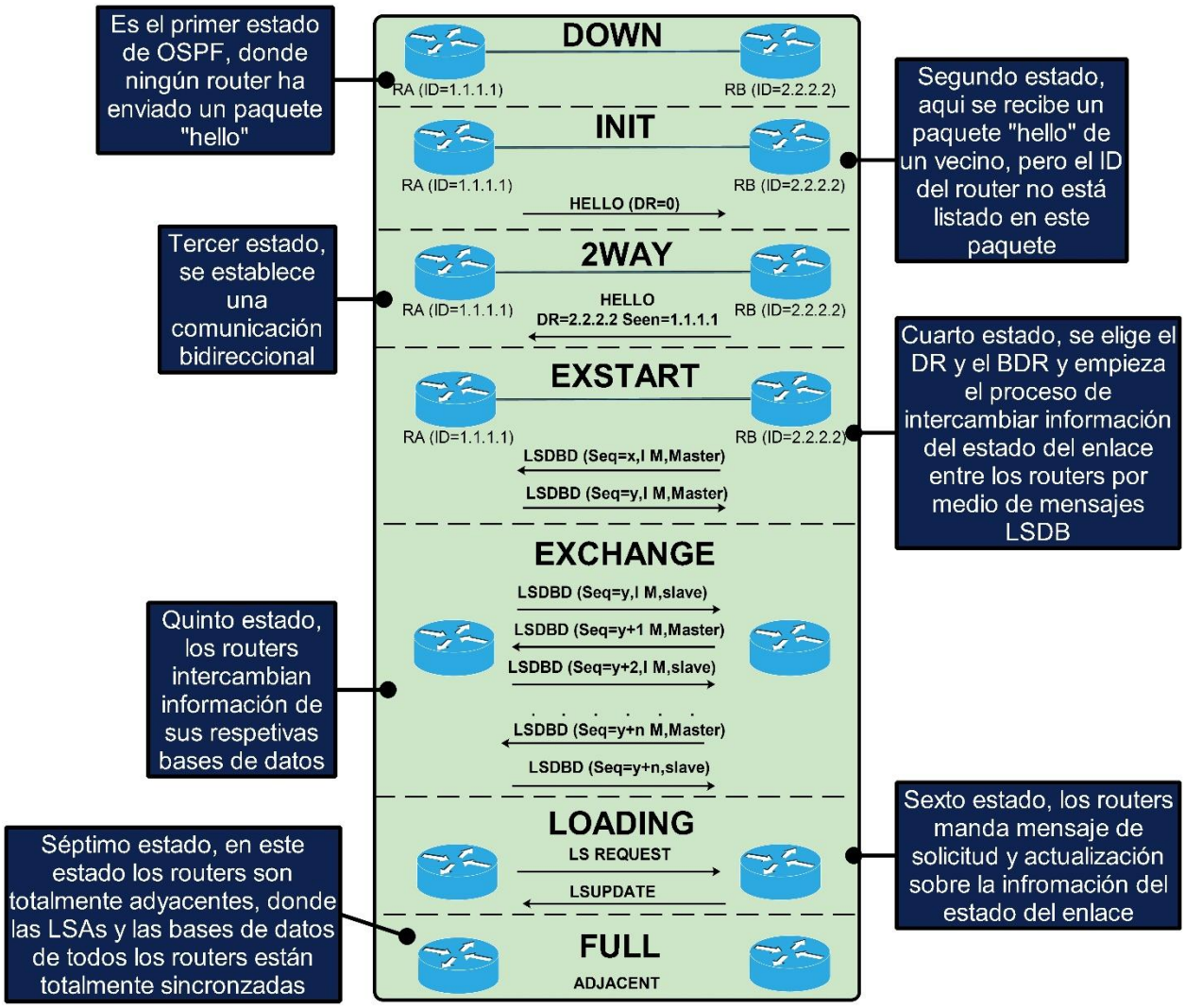


Figura 3.6 Estados de OSPF (diagrama propio basado en [93])

Cada router al momento de tener una lista de vecinos, se crea la base de datos topológica después se ejecuta el algoritmo Dijkstra y se obtiene la tabla de enrutamiento. En el estado "full" las tablas se mantienen actualizadas, en caso de que haya un cambio en la red se envían LSAs. Los mensajes se siguen enviando periódicamente para mantener las adyacencias, en el caso que no se reciban se dará por perdida dicha adyacencia.

Cuando varios routers están conectados a un segmento de red del tipo Broadcast, uno de esos routers tomará el control y mantendrá las adyacencias entre nodos, este router es llamado router designado (DR) y es elegido a través de la información que contienen los mensajes "hello" que se intercambian, para tener una redundancia también se elige un router designado de reserva (BDR), estos son elegidos dependiendo de la interfaz "loopback" o la prioridad que tengan (de 0 a 255, mientras más alto mayor prioridad). El objetivo de tener un DR es controlar el tráfico

en la red estableciendo adyacencias designadas para evitar adyacencias innecesarias, esto evita consumir gran ancho de banda, recursos de memoria y CPU de los routers.

El funcionamiento del DR es recibir actualizaciones y distribuirlas a todos los routers adyacentes a él, los routers notifican los cambios a través de la dirección Multicast 224.0.0.6 (llamada "All ID Address") a su vez el DR envía las LSA a los routers por la dirección Multicast 224.0.0.5 (llamada "All SPF Address"). En caso de que el DR elegido deje de enviar mensajes "hello" el BDR tomará el papel de DR [93, 101,102].

A continuación en la figura 3.7 se muestra el encabezado que siempre debe tener OSPF, en donde cada uno de los campos del encabezado se describe a continuación:

- Versión: Contiene la versión a utilizar, para IPv4 y la utilizada en la actualidad es la versión 2.
- Tipo: Dentro de este campo utiliza 5 diferentes tipos de paquete:
  - Tipo 1 - "Hello": su función es mantener y descubrir a los vecinos.
  - Tipo 2 - "Database Descriptor (DBD) o base de datos del estado del enlace": resume la base de datos de la topología de la red.
  - Tipo 3 - "Link State Request (LSR)": solicitud de paquetes LSA.
  - Tipo 4 - "Link State Update (LSU)": sirve para cargar o actualizar la base de datos del estado del enlace.
  - Tipo 5 - "Link State Acknowledgements (LSAck)": acuse de recibo de paquetes de actualización.

    Cabe decir que la descripción de la base de datos es la parte primaria de las LSA que tiene el router, la petición del enlace solicitan las LSA completas y las actualización del estado del enlace son la respuesta conteniendo las LSAs que se habían solicitado.

- Longitud del paquete: este campo incluye toda la longitud del paquete de OSPF incluyendo el encabezado.
- ID del router: este campo da a conocer el ID del router el cual origina los paquetes OSPF.
- ID del área: este campo identifica el área al que pertenece el router, el valor 0.0.0.0 está reservado para el área de backbone.

- Secuencia de verifación de identidad: es el cálculo de todo el paquete OSPF excluyendo al campo de autenticación.
- Tipo de autenticación: indica el tipo de autenticación entre ellas puede tener la opción de no autenticación, autenticación de texto plano y encriptación MD5 (Message Digest algorithm 5).
- Autenticación: son 64 bits de datos que pueden estar vacíos, contener texto plano o encriptación MD5 [93, 101,102].

Figura 3.7 Encabezado de OSPF con el contenido del Tipo 1 de paquete (diagrama propio con base en [93, 102])

La figura 3.7 viene añadido con el tipo 1 (hello) de mensaje el cual es de vital importancia ya que este ayuda a iniciar la negociación para despues establecer la base de datos topológica, así como adyacencia de todos los routers en el domnio de OSPF. A continuación se describen los campos de este paquete:

- Máscara de red: En este campo se encuentra la máscara de red asociada con la interfaz del router conectado a la red.
- Intervalo de “hello”: tiempo del intervalo entre las transmisiones hechas de “hello”.
- Opciones: este campo sirve para comunicar a otros routers sobre las capacidades opcionales de esos routers.

- Prioridad del router: Este campo se encarga de establecer el valor que podrá ser usado para la elección de router designado.
- Intervalo de muerte del router: En este campo se encuentra el tiempo antes de que un vecino se declara inválido.
- Router designado: En este campo identifica el router designado con su dirección IP en la red, el cual hace que se propague los paquetes de OSPF.
- Router designado de respaldo: Este campo contiene la dirección IP del router designado de respaldo en caso de que el enlace del router designado falle.
- Vecinos: En este campo se enlistan todos los vecinos con los que ha hecho adyacencia el router [93, 101,102].

Existen información adicional que acuerdo con los demás tipos de mensaje que se agrega al encabezado de OSPF, en la figura 3.8 se muestra el ejemplo los diferentes paquetes de acuerdo al "tipo de mensaje" que se adicionan al encabezado de OSPF.

Figura 3.8 Tipos de paquetes en el encabezado de OSPF (Diagrama propio con base en [93, 102])

Los paquetes de tipo 2 y 4 adicionan los paquetes tipo LSA, estos mensajes se muestran en la figura 3.9 donde se encuentra el encabezado que tiene cada LSA, así como el tipo de LSA (referenciados en la tabla 3.4), el cual se adiciona al encabezado del paquete LSA.

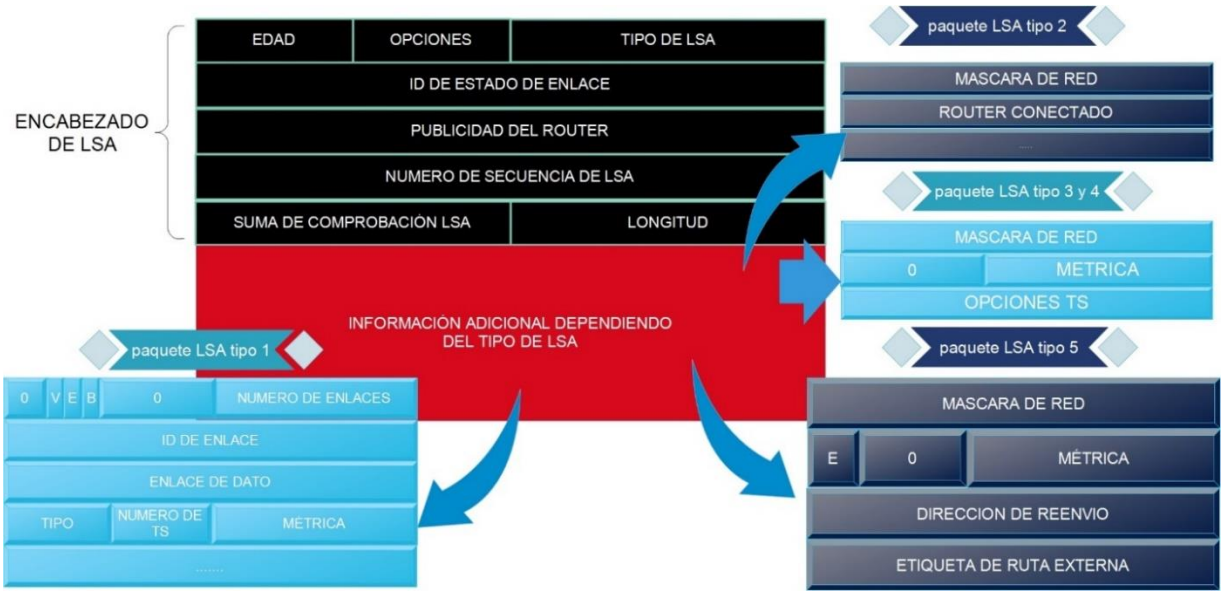


Figura 3.9 Paquete de LSA con diferente contenido dependiendo del tipo de LSA (Diagrama propio con base [93, 102])

A continuación se mencionan los campos correspondientes al encabezado del LSA:

- Edad: Este campo refleja el tiempo desde que se originó el LSA (por lo general se establece en un valor de 0).
- Opciones: Este campo se utiliza para identificar capacidades opcionales soportadas por OSPF.
- Tipo de LSA: Este campo indica el tipo de LSA, donde puede ser del tipo 1 al 5.
- ID del estado del enlace: Este campo identifica de manera exclusiva a un LSA.
- Publicidad del router: Este campo identifica el ID del router de la ruta originada.
- Numero de secuencia: Este campo se incrementa cada vez que un LSA es generado desde el router de origen.
- Suma de comprobación: Este campo comprueba la integridad del contenido completo de LSA exceptuando al campo edad.
- Longitud: Este campo refleja la longitud total de la entrada de LSA incluyendo la cabecera [75, 83].

III.1.4 BGP (Border Gateway Protocol)

BGP es un protocolo de enrutamiento que fue diseñado en 1989 (BGP-1) para ser escalable. Puede ser utilizado en grandes redes, referenciado en el RFC 4271 se encuentra BGP-4(2006), cuya versión es la que se utiliza actualmente. Es un protocolo de enrutamiento complejo cuyo propósito es conectar grandes redes (sistemas autónomos), por lo que este protocolo es usado en organizaciones multinacionales e Internet [101,103].

III.1.4.1 BGP-4

BGP es un protocolo del tipo EGP, algunas de sus caracteristicas se describen a continuación:

- Soporta VSLM y CIDR.
- Conecta grandes AS.
- Soporta enrutamiento entre dominios.
- Es un protocolo “path vector”.
- Es un protocolo robusto y escalable.
- BGP anuncia caminos para redes que están al final del camino.
- BGP describe el camino utilizando atributos.

BGP pretende que las redes permanezcan despejadas del tráfico innecesario el mayor tiempo posible por lo que manipula la ruta para dirigir todo ese tráfico, así mismo está diseñado para que las rutas sean estables y que no se estén advirtiendo e intercambiando constantemente. Debido a que es un protocolo complejo el cual puede tener cientos de miles de tablas de enrutamiento, BGP requiere determinadas políticas de enrutamiento complejas para hacer que los routers no se sobrecarguen. En la figura 3.10 se muestran las dos maneras de trabajo de BGP, cuando trabaja con sistemas autónomos se considera EBGP (External BGP) y al trabajar dentro de un AS para intercambiar ruta se considera IBGP (Interior BGP) [93].

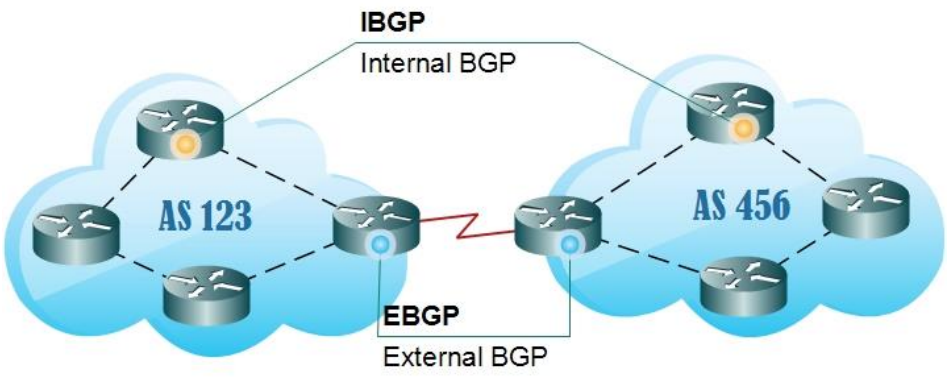


Figura 3.10 Modos de funcionamiento de BGP.

BGP funciona cuando asocia redes con sistemas autónomos de tal manera que otros routers envían tráfico hacia un destino a través de un AS, siendo un protocolo "path vector", las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando el tráfico y los bucles son evitados rechazando aquellas rutas que tiene el mismo número de sistema autónomo al cual están llegando. Un router que este ejecutando BGP puede recibir actualizaciones acerca de múltiples destinos de diferentes "peers" (vecinos de BGP) de diferentes AS, por lo que BGP sólo elegirá el mejor camino (path) para alcanzar un destino específico. Aun así, BGP no está diseñado para tener balanceo de carga cuando existen múltiples conexiones por lo que el "path" elegido esta asociado por las políticas establecidas y no por el ancho de banda [93,104].

La información del "path" de los AS es usada para construir un "grafo" libre de bucles e identificar las políticas de enrutamiento BGP, además especifica que un router pueda publicar las rutas que son usadas hacia un "peer" que está en otro AS. Algunas políticas no pueden ser soportadas por el paradigma de enrutamiento de salto por salto aunque puede soportar algunas políticas que se ajuste al paradigma de enrutamiento.

Para hacer posible este funcionamiento, BGP mantiene conexiones entre los "peers" utilizando el puerto TCP 179, una vez que se establece esta conexión los routers intercambian completamente sus tablas, después de hacer la conexión, los routers sólo envían cambios que haya en la red ya que las actualizaciones periódicas no son requeridas (cuando hay un cambio en la tabla de enrutamiento es detectado, los routers envían a los vecinos solo esas rutas que han cambiado). La tabla de BGP está separada de la tabla de enrutamiento del router. El router ofrece la mejor ruta de la tabla de BGP hacia la tabla de enrutamiento y puede ser configurado para compartir información entre las 2 tablas (tabla BGP y de enrutamiento).

Existen 4 tipos de mensajes que usa BGP para que la relación sea construida y posteriormente mantenida:

- "Open": Se utiliza para el establecimiento de una sesión BGP una vez que haya sido establecida la conexión TCP. Se suelen negociar ciertos parámetros que caracterizan a esa sesión.
- "Keepalive": Una vez que la sesión BGP está activa se envía periódicamente este mensaje para confirmar que el otro extremo sigue estando activo en la sesión BGP.
- "Update": Es un mensaje de actualización, mismo que se considera como un mensaje clave en las operaciones de BGP ya que contiene los anuncios de nuevos prefijos.

- "Notification": Se envía al cerrar una sesión BGP y esto sucede cuando ocurre algún error que requiera el cierre de la misma [93, 103, 104].

En la figura 3.11 se muestra la cabecera que se establece en todo paquete BGP, así mismo se muestran los diferentes complementos de acuerdo al tipo de mensaje elegido (open, keepalive, notification o update). Cabe mencionar que el tipo "keepalive" que no tiene datos por sí mismo, solo se envía con el número que identifica este tipo de mensaje para saber que la conexión sigue activa.

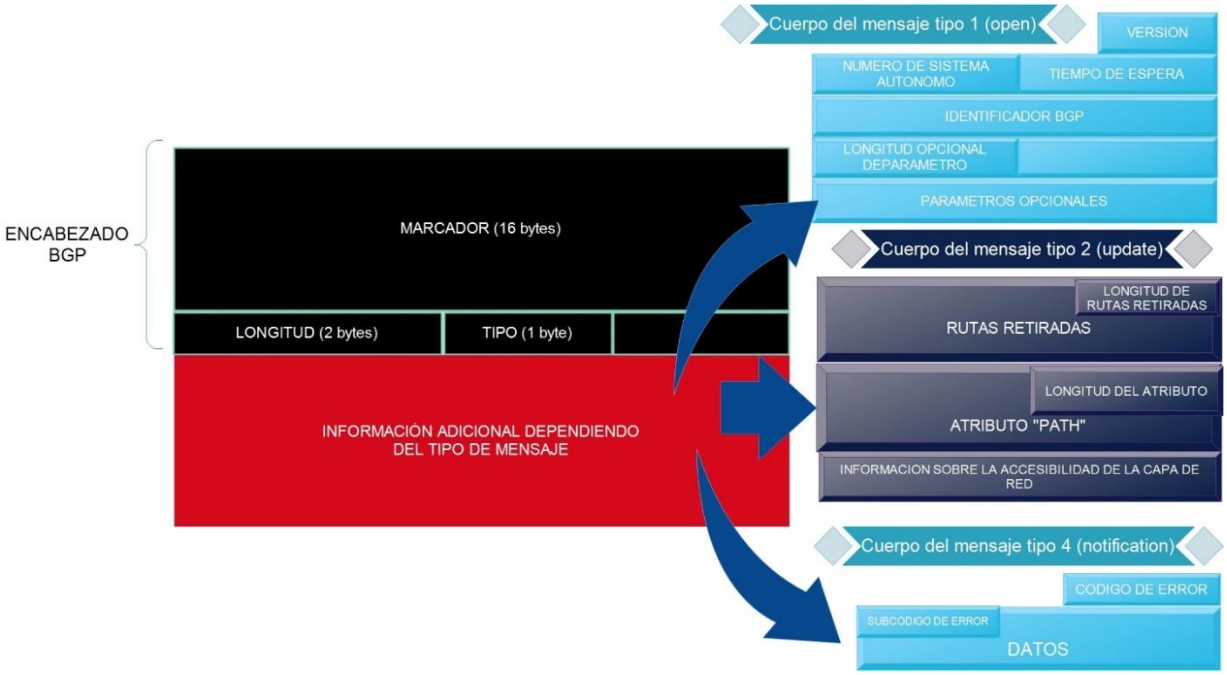


Figura 3.11 Encabezado BGP con los posibles mensajes de acuerdo al tipo seleccionado (diagrama propio con base en [93]).

Los campos del encabezado BGP se describen a continuación:

- Marcador: Se encarga principalmente de hacer la sincronización, aunque también se utiliza para la opción de seguridad.
- Longitud: Indica la longitud de todo el mensaje BGP incluyendo la cabecera.
- Tipo: Este campo asigna que tipo de mensaje se está enviando: 1 para mensajes "Open", 2 para "Update", 3 para "Notification" y 4 para "Keepalive" [103].

Después que se establece una conexión por el puerto TCP 179, el primer mensaje que se envía es un mensaje "open". Si este es aceptado, el mensaje "keepalive" confirma ese mensaje y lo envía por el lado que fue recibido. Cuando "open" es confirmado la conexión se establece y los mensajes "keepalive", "update" y "notification" pueden ser intercambiados. Los mensajes "keepalive" se envían para asegurar que la conexión entre los "peers" esté viva. Los mensajes

de “notification” se envían en respuesta a errores o condiciones especiales y los mensajes de “update” lleva información de un solo “path”, por lo que múltiples “path” tendrán que ser mantenidos usando múltiples mensajes “update”. Dentro del paquete de “update” se encuentran los atributos los cuales hacen referencia hacia el mejor “path” que se debe elegir.

Cuando los mensajes anteriores se encuentran en proceso de intercambio, los “peer” participantes en el proceso entran en diferentes estados, debido a que BGP actúa como una máquina de estados en un router. Entre los estados que se tiene entre los diferentes “peers” son:

- “Idle”: Durante este estado el router está buscando a los vecinos “peers”, técnicamente BGP espera una fase “start”. Este evento puede ser iniciado por un administrador o por el sistema BGP.
- “Connect”: En este estado BGP espera a que se complete la conexión del protocolo de transporte (TCP 179). Si la conexión es satisfactoria pasa al estado “open sent” en caso contrario pasa a un estado “active”.
- “Active”: Intenta establecer la conexión por medio de protocolo TCP 179, si lo logra pasa al estado “open sent”, cuando el temporizador de este estado expira BGP lo reinicia y vuelve al estado “connect”.
- “Open sent”: en este estado BGP espera los mensajes “open” del vecino, donde los mensajes son revisados para verificar que los datos sean correctos (versión BGP y sistema autónomo).
- “Open confirm”: En este estado espera a los mensajes “keepalive”, si recibe estos mensajes de su vecino entonces la sesión pasa al siguiente estado “established”.
- “Established”: Es el estado final y el necesario para que BGP comience a funcionar, en el se intercambian rutas por medio de mensajes “update” y se mantiene la sesión con los mensajes “keepalive” [101].

Este proceso de estados de BGP y los mensajes que se intercambian entre los diferentes estados se muestran en la figura 3.12.

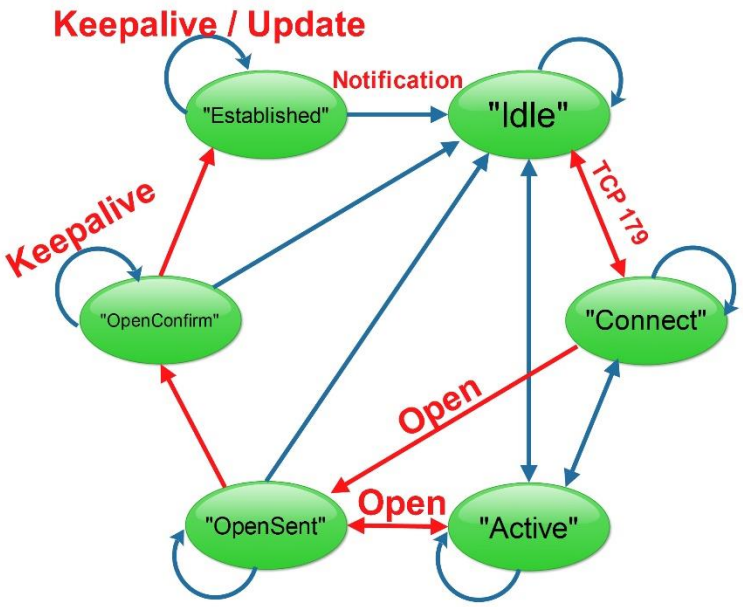


Figura 3.12 Estados de BGP (diagrama propio con base en [75])

BGP forma adyacencias enviando mensajes "keepalive", después de que se establece las adyacencias entre los "peers", estos intercambian sus mejores rutas, en donde cada router recolecta esas rutas desde cada "peer" con la cual establece satisfactoriamente una adyacencia y un lugar en la tabla BGP. Cada "path" aprendido es asociado con un atributo. La mejor ruta de cada red es seleccionada desde la tabla BGP usando los atributos en el proceso de selección de ruta y ofreciendo la mejor ruta. Cada peer o router compara las rutas ofrecidas hacia algún otro camino posible hacia esa red en la tabla de enrutamiento. La mejor ruta basada en la distancia administrativa es instalada en la tabla de enrutamiento [93, 104].

BGP usa muchos parámetros para calcular la mejor ruta, los cuales son llamados atributos, estos definen las políticas de enrutamiento y mantienen un entorno de enrutamiento estable. En la figura 3.13 se muestra la jerarquía completa de estos atributos que utiliza BGP, los cuales se dividen en dos grandes categorías:

1. "Well-known" que a su vez se dividen en "mandatory" (reconoce el atributo y debe aparecer en el mensaje "update") y "discretionary" (reconoce el atributo pero puede no incluirse en el mensaje "update").

2. "Optional" que se dividen en "transitive" (no puede admitir el atributo pero debe enviarlo a los "peers") y "non-transitive" (no soporta el atributo y no lo envía a los "peers")[93,103].

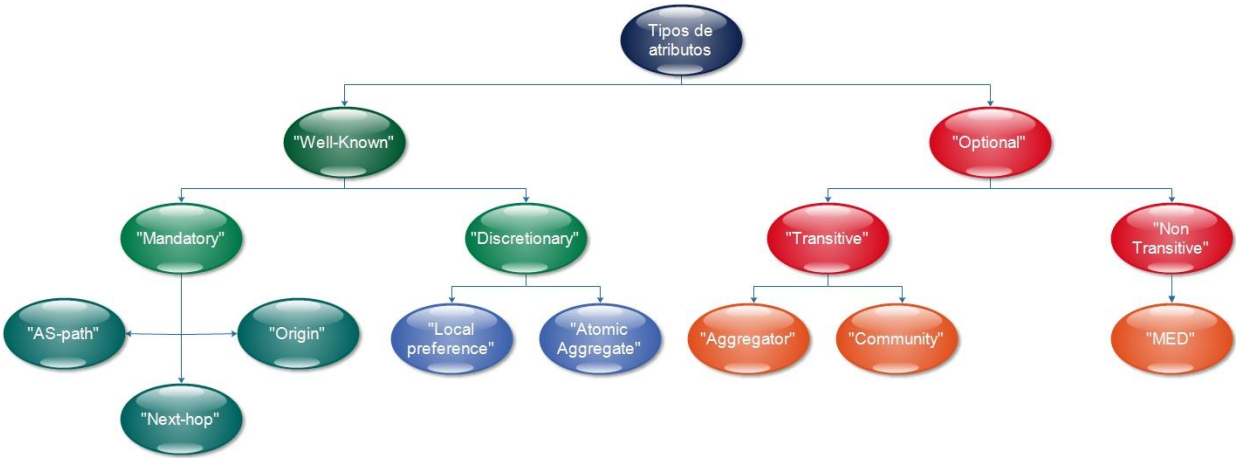


Figura 3.13 Jerarquía de atributos de BGP

Estos atributos se describen a continuación:

- "Local preference": Indica los routers dentro de un AS que son preferidos por el "path" para alcanzar prefijos externos, solo se envían dentro del IBGP por lo que no pasan a los EBGP.
- "Multi-Exit-Discriminator (MED)": Indica a vecinos externos el camino (path) preferido en un AS que usa para alcanzar prefijos. Es un modo dinámico para que un AS influya en otro AS para elegir el mejor camino "path" para alcanzar una ruta determinada.
- "Origin": Es el código de origen de la información preferido de un "path", en cual se prefiere primeramente un IGP y después un EGP.
- "AS_path": Este atributo enlista los AS que tienen que atravesar una ruta para alcanzar un destino con el número de AS que origino la ruta, asi mismo asegura que el camino esté libre de bucles.
- "Next hop": Este atributo indica el siguiente salto de la dirección IP que será usada para alcanzar un destino. No se usa en el proceso de selección de ruta.
- "Agregator": indica el ID y AS del router que lleva a cabo la sumarización. No se usa en el proceso de selección de ruta.
- "Atomic aggregate": Al generar una sumarización envía los AS de las rutas que componen dicha sumarizacion. No se usa en el proceso de selección de ruta.
- "Cluster ID": Identifica un cluster, router reflectors. No se usa en el proceso de selección de ruta.
- "Originator ID": Identifica el router reflector. No se usa en el proceso de selección de ruta.

- "Community": Es una forma de filtrar las rutas entrantes o salientes, por lo que permite a los routers etiquetar rutas con un indicador y a su vez que otros routers tomen decisiones basados en esa etiqueta. No se usa en el proceso de selección de ruta [93, 101, 103].

Dentro de los mensajes "update" se encuentra un apartado del datagrama llamado "atributo path" es donde se insertan los atributos antes mencionados, en la figura 3.14 se muestra el complemento el cual se integran dentro del mensaje "update".

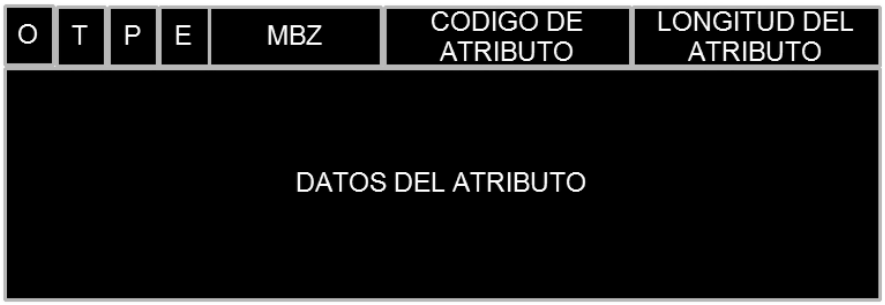


Figura 3.14 Datagrama del tipo de atributo (diagrama propio con base en [93]).

El proceso de decisión se divide en dos partes:

1) Selección de ruta: Es la responsable de seleccionar la rutas a varios prefijos IP, para lograrlo BGP mantiene dos bases de información de enrutamiento (RIB); 1 - "Adjacent RIB": Es la base de información que almacena información de enrutamiento a nivel AS, y 2 - "Loc-RIB": Es la base de información que almacena las rutas que se han determinado localmente.

2) Agregación y diseminación: Es la fase de la mejor ruta, se inicia después de complementar la política de importación y la fase de filtrado, a continuación se describe el proceso para determinar el mejor camino a un destino específico.

1. Si el prefijo IP no es deseado debido la política de importación (prefijos IP que no puede soportar) y el filtrado, se descarta la ruta.
2. Se prefiere la mejor ruta aplicando el grado más alto del "local preference" o la política local pre-configurada.
3. Si hay más de una ruta al destino del prefijo IP, se prefiere la mejor ruta que se origina localmente en el "BGP speaker" (redistribución desde un IGP).
4. Si todavía hay más de una ruta al prefijo de destino se prefiere la mejor ruta que tenga el número más pequeño de números de AS enumerados en el atributo "AS-path".

5. Si todavía hay más de una ruta al prefijo IP de destino se prefiere mejor la ruta que tenga el atributo "Origin" más bajo donde se prefiere un IGP que a un EGP.
6. Si todavía hay más de una ruta se prefiere la mejor ruta con el atributo "MED" más bajo.
7. Si todavía hay más de una ruta al prefijo de destino se prefiere la ruta recibida de un EBGP sobre IBGP. De ser elegido el camino EBGP se salta hasta el paso 9.
8. Si todavía hay más de una ruta al prefijo de destino se prefiere el camino a través de IGP con el menor costo "Next-hop" que se determina en función del valor de la métrica.
9. Se determina si se requiere instalar múltiples caminos en la tabla de enrutamiento para BGP Multipath.
10. Si todavía hay más de una ruta al prefijo de destino se prefiere la mejor ruta aprendida del vecino EBGP con el identificador más bajo, se prefiere el que fue recibido primero (el más antiguo), esto minimiza el "flapping" de rutas. Se omite este paso no si existe un "best path"
11. Si todavía hay más de una ruta al prefijo de destino se prefiere la mejor ruta eligiendo al vecino IBGP con el ID más bajo [93,101].

Después de terminar el proceso de selección de ruta, abre paso a la diseminación de rutas, en donde, las mejores rutas se almacenan en el "Local RIB", el cual implica la agregación de rutas junto con la aplicación de la política de exportación. Una capacidad crítica de BGP 4 es el manejo de agregación de rutas que es posible gracias a CIDR, donde se combinan bloques de direcciones de redes de dos o más AS a través de un "Supernetting" en un solo AS. Por lo que anunciará sólo el número del AS donde se realizó el "Supernetting". Para hacer esto posible se utilizan los atributos "Atomic aggregate" y "Aggregator", donde "Atomic aggregate" se adjunta a una ruta fuera del AS donde se realizó el "Supernetting" y con el atributo "Aggregator" identifica el "BGP speaker" que realiza esta agregación. [104].

BGP también funciona con prefijos IPv6, esta versión es MP-BGP pero queda fuera de los alcances de este trabajo [104,105].

Aquí termina la sección referente a los protocolos de enrutamiento, a continuación se hace la revisión del protocolo de gestion SNMP.

III.2 Protocolos de gestión

La gestión de red es una de las cuestiones importantes que está presente en grandes empresas o instituciones ya que con ello se logra gestionar todos esos dispositivos participes de la red como el de monitorear la parte de hardware así como de software, trayendo como consecuencia un mejor control y administración de todos los dispositivos.

Para hacer posible la gestión de red se utilizan los protocolos de gestión, estos empezaron aparecer a finales de la década de los 80 entre los que se tenía a CMISE/CMIP (Common Management Information Services Element/ Common Managment Information Protocol) por parte de OSI y a SNMP (Simple Network Managment Protocol), por parte de IETF (Internet Engineering Task Force), estos dos protocolos eran los más importantes para la gestión de red ya que se habían diseñado para ser independientes de productos y redes específicas de distintos vendedores. Sin embargo, SNMP encontró un amplio uso y aceptación, dado que se desarrolló rápidamente cuando se hizo más clara la idea de gestionar una red, por lo que SNMP hoy en día es el entorno de gestión de red más utilizado y desarrollado [106].

Después de tener una clara la idea de gestión de red se llegó a una definición más concreta, siendo esta la siguiente:

> *"La gestión de red incluye el despliegue, integración y coordinación del hardware, software y elementos humanos para supervisar, comprobar, sondear, configurar, analizar, evaluar y controlar la red y los recursos, de forma que se cumplan los requisitos de tiempo real, de rendimiento operacional y de calidad de servicio a un costo razonable."*
>
> Tuncay Saydam y Thomas Magedanz (Dic 1996) [106]

III.2.1 SNMP (Simple Network Management Protocol)

SNMP es un protocolo el cual funciona en la pila de protocolos del modelo TCP/IP, mismo que actúa en la capa de aplicación, lo que facilita el intercambio de información de gestión entre dispositivos de una red, permitiendo a los administradores de red supervisar el rendimiento de la red, buscar y resolver sus problemas, además del planear el crecimiento de la red.

III.2.1.1 SNMPv1

SNMPv1 fue un protocolo que nació en 1988 descrito en el RFC 1067 donde tuvo sus actualizaciones descritas en el RFC 1157, el cual junto con los RFC 1155 ,1212 y 1213 fueron piezas clave para definir SNMPv1. En la figura 3.15 se muestra los demás RFC fundamentales para el establecimiento de SNMP v1 [107,108, 109].

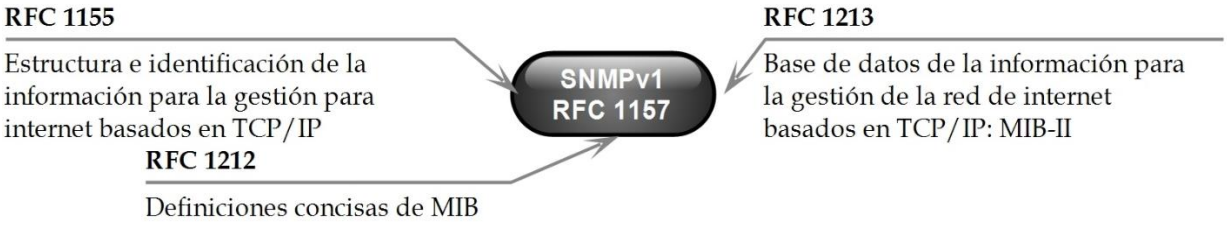


Figura 3.15 RFCs fundamentales para SNMv1

Así mismo algunos objetivos de SNMP como algunas de las variables que se pueden monitorear con dicho protocoló se muestran en la tabla 3.6.

Objetivos de SNMP	• **Monitorear el flujo del tráfico a través de los dispositivos** • **Detectar y notificar las fallas encontradas en los dispositivos de red.** • **Recolectar datos sobre el rendimiento de los dispositivos sobre largos periodos de tiempo e identificar tendencias** • **Configurar remotamente dispositivos de red** • **Acceso y control remoto de los dispositivos de red.** • **Mapear la disponibilidad la red** • **Rendimiento y Tasas de errores.** • **Monitorear y gestionar miles de sistemas en una red.**
Variables que SNMP puede medir	• Tráfico por unidad de tiempo • Carga de trabajo del CPU • Memoria utilizada y disponible • Tiempo de operación del equipo • Estado de sesión BGP • Tablas ARP • Tablas de reenvio

Tabla 3.6 Objetivos y variables de monitoreo de SNMP.

Una red administrada con SNMP consiste de 3 Componentes fundamentales:

1) Dispositivos administrados (Managed Devices): Estos dispositivos pueden ser routers, switches, firewalls, servidores, etc. Así un MD es un nodo de red que contiene un agente SNMP el cual reside en una red administrada. Los dispositivos administrados colectan y almacenan información y hacen que esta información esté disponible al NMS (Network Management System) utilizando SNMP.

   Los MD son supervisados y controlados utilizando 4 comandos SNMP básicos:

   a) "Read": Es utilizado por un NMS para supervisar los MD. El NMS examina diferentes variables que son mantenidas por los MD.
   b) "Write": Es utilizado por un NMS para controlar los MD. El NMS cambia los valores de las variables almacenadas dentro de los MD.
   c) "Trap": Es utilizado por los MD para reportar eventos de forma asíncrona a los NMS. Cuando cierto tipo de eventos ocurren, un MD envía un "trap" hacia el NMS.
   d) "Traversal options": Son utilizados por los NMS para determinar cuáles variables son soportadas por los MD y obtener secuencialmente información en una tabla de variables, tal como una tabla de enrutamiento.

2) Agentes SNMP: Un agente SNMP es un proceso residente en cualquier dispositivo gestionado, el cual recolecta información administrativa sobre su entorno local, almacena y recupera información como está definido en la MIB (Managment Information Base), así mismo indica cuándo se produce un evento al administrador. El agente reporta el estado de los elementos de redes que están siendo administrados bajo el control de los comandos de la entidad gestora (NMS).
3) Sistemas de gestión de red (NMS): Ejecuta aplicaciones que monitorean y controlan los MD. Los NMSs proporcionan la mayor parte de recursos de procesamiento y memoria requeridos para la gestión de la red. Uno o más NMSs deben existir en cualquier red administrada ya que estos recolectan información administrativa de los agentes SNMP de los dispositivos administrados y la almacenan de una manera más legible [106, 109,110].

En la figura 3.16 se muestra el funcionamiento de estos tres elementos:

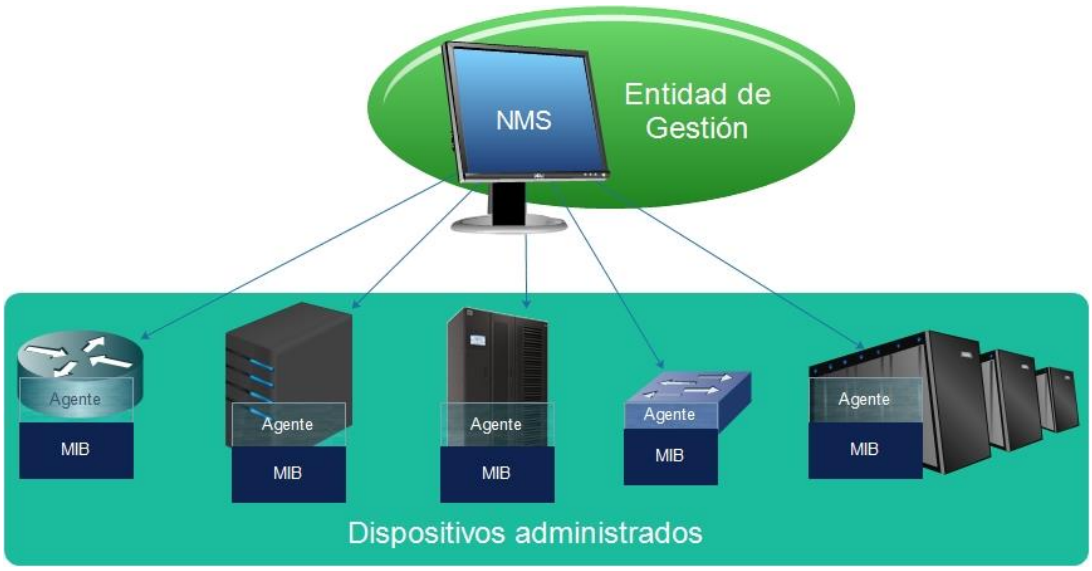


Figura 3.16 Componentes para la gestión con SNMP.

Otro elemento clave para SNMP son las MIB (Base de datos de la información para la gestión), las MIB son una base de datos compartida entre los agentes y el NMS que provee información sobre los elementos de red. Es una colección de información que está organizada jerárquicamente. Se puede tener acceso a las MIB utilizando SNMP, donde las MIB están compuestos de objetos administrados que son identificados por identificadores de objetos (OID) [107,108].

Un objeto administrado es cualquier número de características específicas de un dispositivo administrativo. Estos objetos están compuestos de una o más instancias de objeto, que son esencialmente variables. Dentro de estos existen dos tipos de objetos administrados:

- Escalares: estos definen una simple instancia de objeto.
- Tabulares: definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en las tablas MIB.

Por otro lado un OID identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles son asignados en algunas ocasiones por diferentes organizaciones. La estructura MIB se describe mediante el estándar ASN (Abstract Syntax Notation – Notación sintáctica abstracta). La MIB utiliza los OIDs, los objetos gestionados son identificados como una serie de números enteros separados por puntos, los cuales representan nodos en un árbol [109,110].

En la figura 3.17 se muestra una parte de todo el árbol jerárquico que puede tener integrado un MIB. Dentro de esta figura, en el apartado "private" se encuentra el otro objeto "enterprises", siendo este el que ofrecerá los objetos y especificaciones de cada vendedor (vendor), en este apartado un vendedor puede registrar sus únicos productos por lo que corresponderá a su única información de gestión.

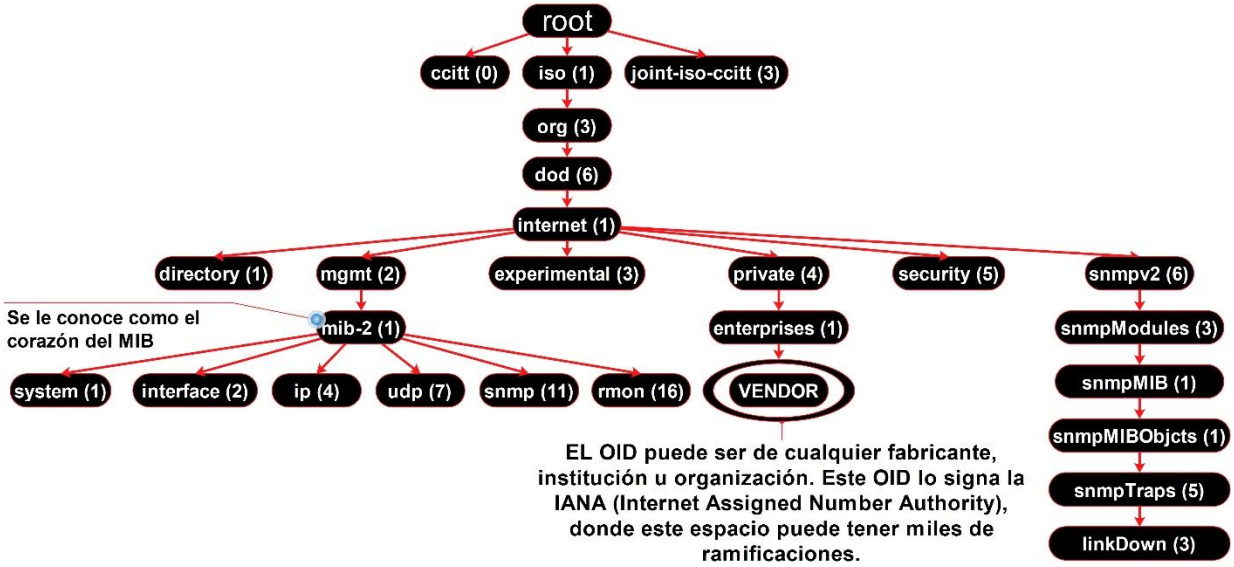


Figura 3.17 Árbol de internet (diagrama propio con base en [110])

SNMP define tablas estructuradas que utilizan para agrupar las instancias de un objeto tabular, estas tablas están compuestas de 1 o más filas. Las tablas están indexadas de manera que permitan al protocolo SNMP recuperar o alterar una fila entera. Así mismo SNMP es un protocoló de petición o solicitud/ repuesta donde el NMS emite una solicitud y los MD regresan una respuesta. Lo antes mencionado se realiza mediante las cuatro operaciones siguientes emitidas por el administrador, excepto la operación "trap" que es iniciado por un agente:

1) "Get-Request": Es utilizada por el NMS para recuperar el valor de una o más instancias de un objeto desde un agente. Si el agente responde a esta operación y no puede proporcionar valores para todas las instancias del objeto en una lista, este no proporcionara ningún valor.
2) "Get-Next-Request": es utilizada por el NMS para recuperar el valor de la siguiente instancia del objeto en una tabla o una lista dentro de un agente.
3) "Set-Request": Es usada por el NMS para colocar los valores de los objeto dentro de un agente.
4) "Get-Response": es utilizada para determinar si las solicitudes anteriormente mencionadas fueron procesadas correctamente por el agente.

5) "Trap": es utilizada por los agentes para informar asíncronamente al NMS sobre un evento importante (suceso de interrupción). La "Trap" se origina en el agente y se envía a la IP del NMS. Uno de los fallos que puede presentar es el no recibir un acuse de recibo por parte de NMS hacia el agente que envió la "Trap". Algunas de las situaciones donde puede reportar una "Trap" son [107,108,109,110]:
   - Una interfaz de red en el dispositivo (donde se está ejecutando el agente) ha tenido una caída
   - Una interfaz de red en el dispositivo (donde se está ejecutando el agente) se ha vuelto activar
   - Una llamada entrante a un rack de modem no pudo establecer una conexión a un modem
   - Alguna falla dentro de un Switch o Router

SNMP hace uso del protocolo de transporte UDP (User Datagran Protocol) para poder enviar datos entre los gestores y el agente, utiliza el puerto 161 para poder enviar y recibir solicitudes; y usa el puerto 162 para poder recibir "traps" de dispositivos administrados. En la figura 3.18 se muestra la función que SNMPv1 realiza con un gestor hacia un agente, donde se involucran las distintas operaciones de SNMPv1.

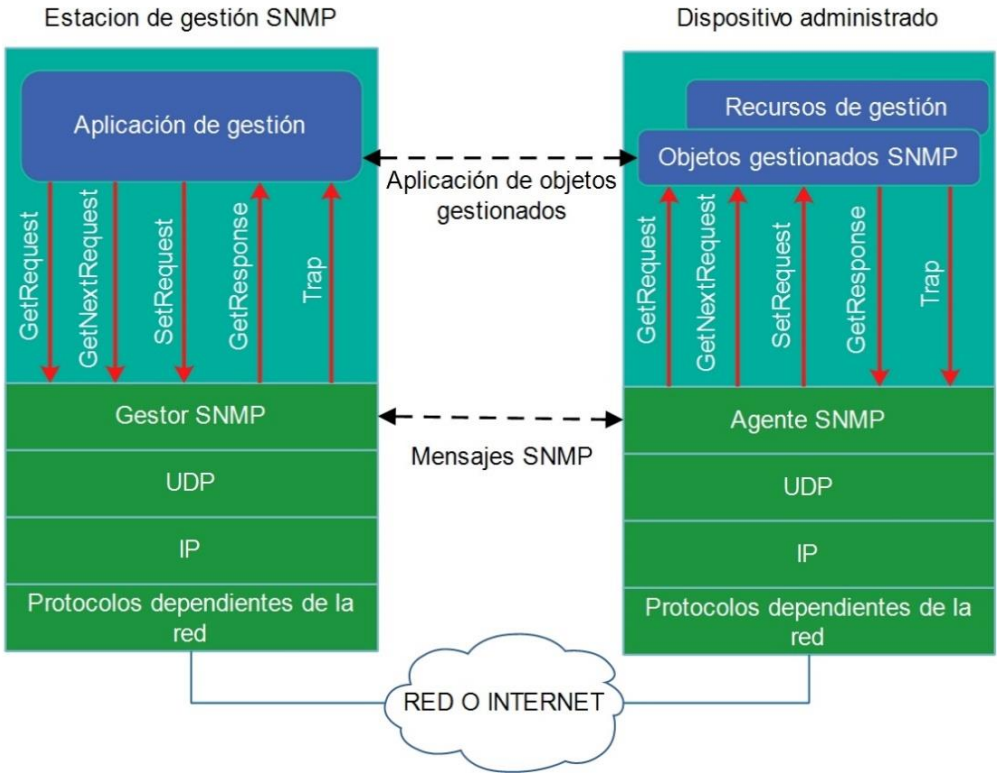


Figura 3.18 Rol de SNMPv1 (diagrama propio con base en [107])

En la figura 3.19 se muestra el formato del mensaje SNMPv1, donde los campos se describen a continuación:

- Versión: Este campo define la versión de SNMP en este caso sería la versión 1
- Comunidad: Este campo sirve como una forma débil de autenticación, ya que define el entorno de acceso para grupos de "NMS's". Existen tres nombres de comunidad:
    1) "Read only": Esto solo permitirá leer los datos pero no modificarlos
    2) "Read- write": permite leer y modificar los valores de los datos.
    3) "Trap": Permite recibir traps del agente

  Todas estas cadenas de comunidad se envían en texto plano, lo que hace una débil forma de seguridad pero aun asi se puede enviar una "trap" de autenticación cuando alguien intenta consultar un dispositivo con una cadena de comunidad incorrecta, asi estas traps de autenticación son útiles cuando un intruso intenta obtener acceso a la red.

- PDU SNMP: este campo contiene los formatos de las operaciones de SNMP

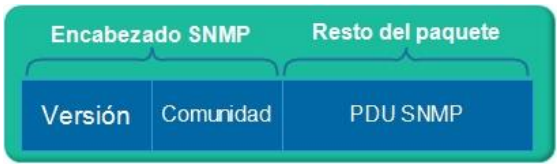


Figura 3.19 Mensaje SNMP

En las figura 3.20 se muestran el formato del PDU que se adicionan al mensaje de SNMP de acuerdo a las operaciones "get, get-next, set" y "response"

Tipo de PDU	ID de solicitud	0	0	Variable de enlaces

Figura 3.20 PDU para las operaciones "get, get-next, set"

En la figura 3.21 se muestra el PDU correspondiente a la operación "get-response"

Tipo de PDU	ID de solicitud	Estatus de error	Indice de error	Fijacion de variables

Figura 3.21 PDU para la operación "get-response"

Donde los campos se describen a continuación:

- Tipo de PDU: Especifica el tipo de PDU de transmisión; 0 para "get", 1 para "get-next", 2 para "set", 3 para "response" y 4 para "trap".
- ID de solicitud: Asocia las solicitudes y respuestas de SNMP. Se agrega un número que utiliza el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea.

- Estatus de error: Este campo indica uno de una serie de errores y los tipos de errores, solo lo usa la operación "response" de lo contrario el valor es 0.
- Índice de error: este campo asocia un error con una instancia de un objeto en particular, solo lo usa la operación "response" de lo contrario el valor es 0.
- Fijación de variable: actúa como campo de datos del PDU de SNMP, en el cual lleva toda una serie de nombres con sus valores correspondientes.

El formato de las "traps" se muestra en la figura 3.22:

Figura 3.22 PDU para la operación "trap"

Donde los campos se describen a continuación [107, 108, 109,110]:

- Empresa: indica el tipo de subsistema de gestión u objeto administrado que ha emitido el trap.
- Dirección de agente: proporciona la dirección del objeto administrado que genera el trap. Dirección IP del agente que ha emitido el trap.
- Tipo de trap genérica: de acuerdo a la tabla 3.7 se indica el tipo de trap genérica:

Nombre y código del trap	Descripción
"coldStart (0)"	Indica que el agente se ha iniciado o reiniciado
"warmStart (1)"	Indica que la configuración del agente ha cambiado
"linkDown (2)"	Indica que una interfaz está inactiva así mismo identifica la interfaz
"linkUp (3)"	Indica que una interfaz esta activa e identifica que interfaz.
"authenicationFailure (4)"	Indica que alguien ha querido consultar al agente con una contraseña incorrecta.
"egpNeighborLoss (5)"	Indica que un router utiliza EGP pero se encuentra inactivo
"enterpriseSpecific (6)"	Indica el "trap" de una empresa en especifico

Tabla 3.7 Traps genéricas

- Código de trap específico: es usada para "traps" privadas.
- Sello de tiempo: indica la cantidad de tiempo que ha transcurrido entre la última reinicializacion de la red o el agente y la generación del trap.

III.2.1.2 SNMPv2

Debido a que SNMPv1 fue la primera versión surgió la necesidad de cubrir algunas de las deficiencias que esta presentaba, lo que dio origen a SNMPv2 (1996 – RFC 1905), así mismo SNMPv2 también está constituido por varios RFC's (actualizados) como se muestra en la figura 3.23

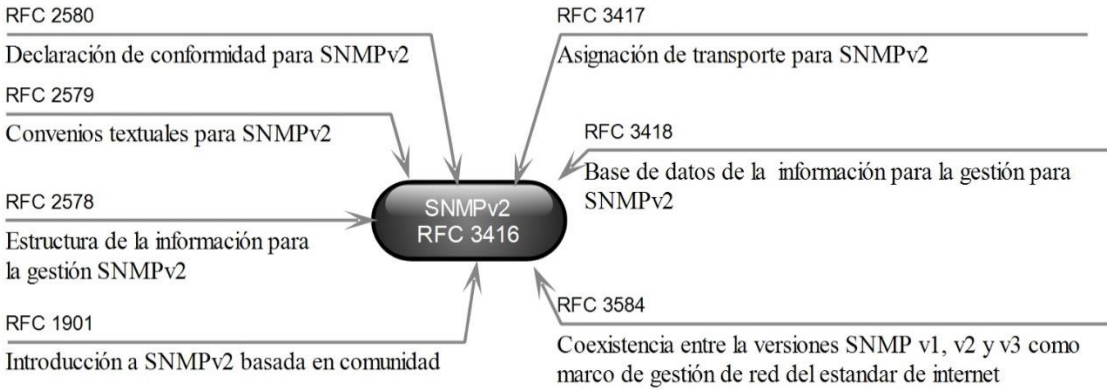


Figura 3.23 RFC's compuestos para SNMPv2.

A continuación, se describen algunas de las mejorías de SNMPv2 [107,109, 110,111]:

- Agrega y mejora algunas operaciones del protocolo: se agregan las operaciones "Get-bulk" e "Inform", así mismo se mejoran y se mantienen las operaciones que emplea SNMPv1 ("get, get-next, set y get- response"), dentro de estas mejoras hay cambios en estas operaciones.
- Mayor eficiencia en la trasferencia de la información.
- Agrega la comunicación gestor a gestor, permite que los sistemas operen tanto gestores así como agentes.
- Soporta una señalización extendida de errores y permite el uso de varios servicios de transporte.
- Dentro de una de las mejoras se encuentra en la estructura de la información para la gestión.
- Hubo agregación de funciones de seguridad, pero fueron cedidas a la versión 3 debido al poco rendimiento que presentaba SNMPv2.

El formato de los mensajes de SNMPv2 es igual al mostrado en la figura 3.19, donde se mantienen los mismos campos; solo que en el campo "versión" es donde se tiene la versión 2 y

el campo "comunidad" se mantiene la misma seguridad en texto plano solo que ahora está encriptada y el SNMP PDU que corresponderán a las operaciones que se realicen.

Debido a que los mensajes de error de SNMPv1 no eran muy robustos, se intentó solucionar este problema con SNMPv2 en donde se definen respuesta con errores adicionales que son válidos para las operaciones "get, set" y "get-bulk", siempre y cuando el agente y el NMS admita SNMPv2.

Entre las dos nuevas operaciones se tienen a "getbulk" e "inform" donde:

a) "Get-bulk": Esta operación llena un mensaje con la mayor cantidad de respuestas posibles. Es utilizada por el NMS para recuperar de manera eficiente grandes bloques de datos, tales como múltiples filas de una tabla. Para la operación "getbulk" en la figura 3.24 se muestra el PDU que se adiciona al paquete.

Figura 2.24 PDU para la operación "getbulk"

Los campos "tipo de PDU, ID de solicitud y variable de enlaces" se describieron anteriormente en SNMPv1, los campos "no repetidores" y "máximas repeticiones"se describen a continuación:

- "No repetidores": especifica el número de instancias de objetos en el campo asociado de variables que deben ser no más de una vez recuperadas desde el principio de la solicitud. Los no repetidores le dicen al comando "get-bulk" que los primeros N objetos pueden ser recuperados con una simple operación "get-next".
- "Máximas repeticiones": define el número máximo de veces que otras variables además de los especificados por el campo "no repetidores" deben ser recuperados. "Máximas repeticiones" le indica al comando "get-bulk" que intente hasta M operaciones "get-next" para recuperar los objetos restantes [106].

b) "Inform": Esta operación es utilizada por una entidad gestora para notificar a otra unidad gestora de cierta información MIB que es remota a la entidad receptora. Esta entidad devuelve con un PDU "response" que tiene el estatus "noError" para certificar la recepción del PDU de "Inform" [107,111].

Dentro del RFC de SNMPv2 se había agregado también la operación "report", sin embargo no tiene ninguna definición, solo se comenta que está destinada para que pueda ser definida tanto en sintaxis como semántica.

Los componentes, comandos, funciones y operaciones son similares a SNMPv1, pero a continuación se describen las mejoras a algunas operaciones, cabe mencionar que una de las características para mejorar la eficiencia de la trasferencia de datos es el llamado comando "Get no atómico", el cual consiste en devolver los resultados parciales o solo las variables que se puedan devolver, ya que con SNMPv1 dentro de una lista de variables, si el agente solo podía devolver un valor de una variable, el comando era rechazado completamente y el gestor debía volver a emitir dicho comando por lo que eso generaría mayor trasferencia de datos y como consecuencia se tendría mayor congestión en la red. Esta característica se agrega a las operaciones "get-request, get-next-request" y "set-request", a continuación se describe la mejora a las siguientes operaciones [107,110]:

- "Get-Next-Request": Sintaxis y significado igual que SNMPv1 salvo que la respuesta contiene en la lista de variables el identificador de objeto y el valor en caso de encontrar el objeto.
- "Set-Request": Una de las mejoras es la de cambiar el valor de un objeto administrado o para crear una nueva fila en una tabla. Los objetos que se definen en la MIB como "read-write" pueden ser alterados o creados utilizando esta operación, en donde es posible que un NMS establezca más de un objeto a la vez.
- Cambio sólo en el nombre de la operación "get.response", por sólo "response".
    - "Trap SNMPv2": Realiza la misma función que en SNMPv1 salvo que con un formato distinto.

En la figura 3.25 se aprecia el formato de PDU de la operación "Trap SNMPv2", donde ahora es similar al formato de las operaciones "get, get-next, set and inform"

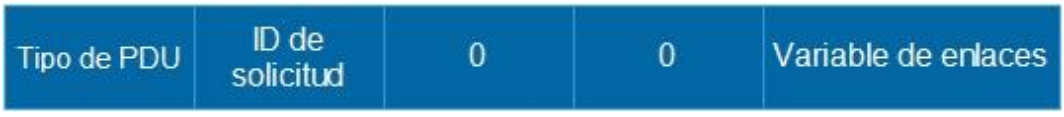


Figura 3.25 Formato PDU para las operaciones "get, get-next, set, inform, and trap snmpv2"

Este formato y sus campos son similares a SNMPv1 para las operaciones "get, get-next, set e inform" solo que con SNMPv2 dentro del campo tipo de PDU se agregan los siguientes valores mostrados en la tabla 3.8

Valor	Tipo PDU asociada
0	Get Request
1	Get-Next-Request
2	Get-Response
3	Set – Request
4	Trap – para snmpv2 se considera obsoleto
5	Get-Bulk-Request
6	Inform- Request
7	SNMPv2 Trap
8	SNMP Report

Tabla 3.8 Valores asociados al campo Tipo de PDU.

Para la operación "Trap SNMPv2" en comparación con la estructura del mensaje que se muestra en la figura 3.22 de SNMPv1, parte de esa información está contenida en el campo variables de enlace, así mismo este campo requiere de los 4 primeros campos para ser "sysUpTime"(indica el subsistema que genera la Trap) y "TrapOID" (parte del grupo de "trap" en la MIB de SNMPv2) con su valor respectivamente como se muestra en la figura 3.26, la información adicional variara de la implementación particular por el proveedor del producto [111,112].

Figura 3.26 información adicional dl PDU Trap SNMPv2

La operación de SNMPv2 sigue siendo igual a SNMPv1, en modo petición-respuesta, en donde una entidad gestora SNMPv2 envía una petición a un agente SNMPv2, el cual recibe la petición, realiza alguna acción, y envía una respuesta a la petición. Donde la petición es utilizada para consultar, obtener o modificar los valores de objetos MIB asociados con el dispositivo gestionado. Así mismo un agente puede enviar un mensaje no solicitado (trap) a una entidad gestora, donde estos mensajes notifican a la entidad gestora sobre algún evento que ha dado lugar a cambios en los valores de los objetos MIB.

A diferencia con SNMPv1, SNMPv2 ahora puede tener una comunicación con una entidad gestora hacia otra entidad gestora, así en grandes redes no solo una NMS es la encargada de toda la gestión, así se tiene a varios NMSs y poder comunicarse para dar información de los diferentes agentes a las otras estaciones gestoras. En la figura 3.27 se muestra un ejemplo del rol de SNMPv2 [106, 107,110].

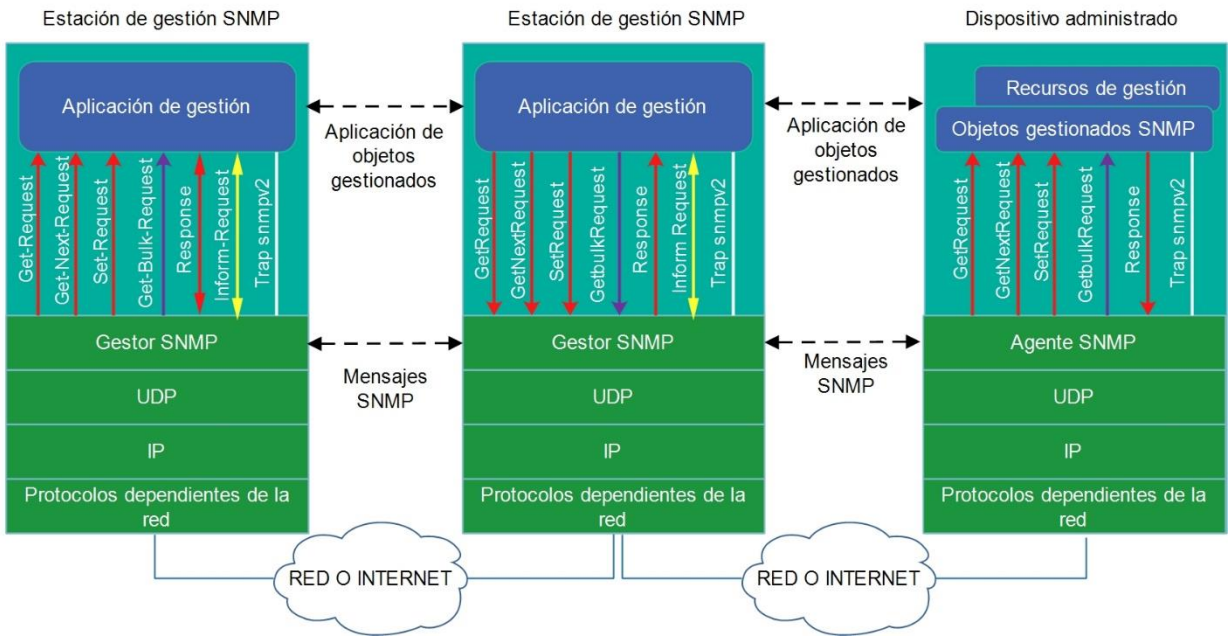


Figura 3.27 Rol de SNMPv2 (diagrama propio con base en [112])

III.2.1.3 SNMPv3

Esta versión de SNMP se desarrolló en 1999 debido a la falta de seguridad tanto SNMPv1 como en SNMPv2 donde en estas dos versiones solo contaban con una contraseña enviada en texto claro entre un gestor y un agente. Esto es un grave problema de seguridad debido a que si se intercepta la contraseña, esta puede ser utilizada por algún atacante para poder acceder a la información de los dispositivos de red lo que podría causar problemas en la infraestructura de la red ya que tendría control de todo dispositivo gestionado, dentro de este trabajo no se utilizará esta versión debido a que no todos los equipos de simulación lo soportan y esta fuera de los objetivos de este trabajo ya que esta versión esta dedicada más a caracteristicas de seguridad.

SNMPv3 es muy complejo debido a todas las funcionalidades adicionales que se involucran. Esta integrado por diferentes "RFCs" similares a sus antiguas versiones como se muestra en la figura 3.28.

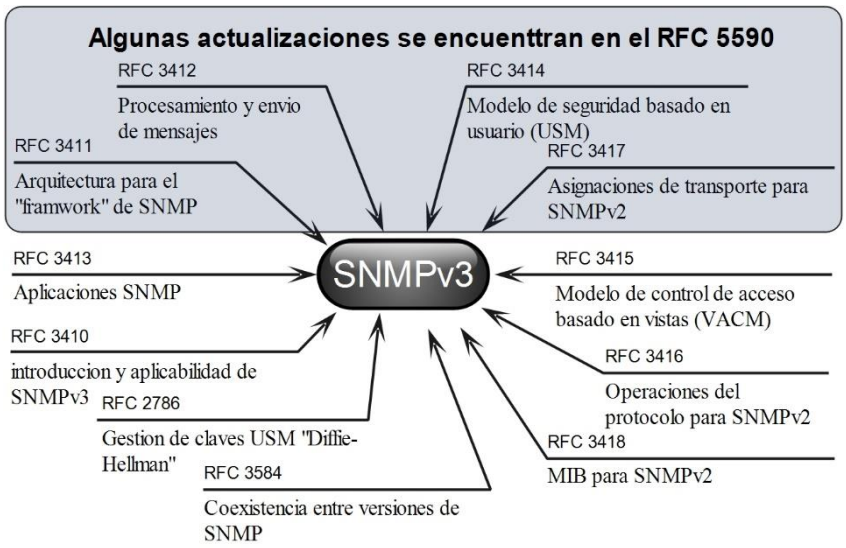


Figura 3.28 "RFCs" que conforman SNMPv3.

SNMPv3 sigue las mismas funciones que SNMPv1 y SNMPv2, a pesar que esta versión introduce nuevas convenciones, concepto y terminología esencialmente describen lo mismo, la gran diferencia se tiene en la agregación de seguridad; esto lo logra con la implementación, autenticación, privacidad, encriptación y control de acceso. En cuestión de la terminología SNMPv3 abandona la noción de gestor y agente por lo que son llamados entidades (entities), donde cada entidad consta de un motor (engine SNMP) y una o varias aplicaciones SNMP, estos conceptos son importantes porque definen una arquitectura en lugar de un simple conjunto de mensajes.

SNMPv3 sigue el modelo USM (User-based Security Model – Modelo de Seguridad Basado en Usuario), en donde se verifica que los mensajes SNMP que se reciben no hayan sido modificados durante la transmisión, así mismo verifica la identidad de los usuarios que interactúan con el sistema y cuida la privacidad de la información enviada y recibida. Para el control de acceso SNMP utiliza el modelo VACM (View Access Control Model – Modelo de control de acceso basado en vistas), el cual ofrece un conjunto de autentificación de acceso a las aplicaciones que pueden utilizarse, también posibilita el acceso al MIB y puede limitar las operaciones que los gestores pueden realizar sobre los agentes [112, 113,114].

El motor de SNMPv3 está compuesto de cuatro piezas con la implementacion de mecanismos de autenticación, privacidad y encriptación:

1. "Dispatcher": Su función es el de enviar y recibir mensajes, así mismo intenta determinar la versión de cada mensaje recibido (ya sea SNMPv1, v2 o v3), si la versión es

compatible, entrega el mensaje al "message processing subsystem". "Dispatcher" también envía mensajes SNMP a otras entidades.

2. "The message processing subsystem": Su función es preparar los mensajes que se van enviar y extrae los datos de los mensajes recibidos. Además puede tener varios módulos de procesamiento de mensajes (módulos para procesar peticiones SNMPv1, v2 o v3). Cabe mencionar que puede contener un módulo para otros modelos de procesamiento que aún no se han definido.
3. "The security subsystem": Su función es proporcionar servicios de autenticación y privacidad. SNMPv3 usa autenticación basada en el usuario, este tipo de autenticación utiliza los algoritmos MD5 (Message Digest 5) o SHA1 (Secure Hash Algorithm 1), con esto se autentican los usuarios sin enviar una contraseña de texto claro. El servicio de privacidad utiliza el algoritmo DES (Data Encryption Standard) para cifrar y descifrar mensajes SNMP.
4. "The Access control subsystem": Su función es controlar el acceso a los objetos MIB, puede controlar los objetos a los que un usuario puede acceder así como las operaciones que puede realizar con esos objetos [110, 113, 114].

Las operaciones que realiza SNMPv2, ahora el protocolo SNMPv3 la divide en una serie de aplicaciones que se muestran en la tabla 3.8.

Nombre de la aplicación	Descripción	¿Quién la genera?
""Command generator"	Genera las peticiones "get", "getnext" y "getbulk" y procesa las respuestas	Un NMS hacia una entidad de un MD
"Command responder"	Responde a las peticiones "get", "getnext" y "getbulk" y genera peticiones	Entidad de un MD
"Notification originator"	Genera "traps" y notificaciones	Entidad de un MD
"Notfication receiver"	Recibe los mensajes "traps" e "inform",	Un NMS
"Proxy forwarder"	Facilita el paso entre entidades.	

Tabla 2.8 Aplicaciones de SNMPv3.

En la figura 3.29 se muestra la entidad de SNMPv3 con su motor (engine) y las aplicaciones.

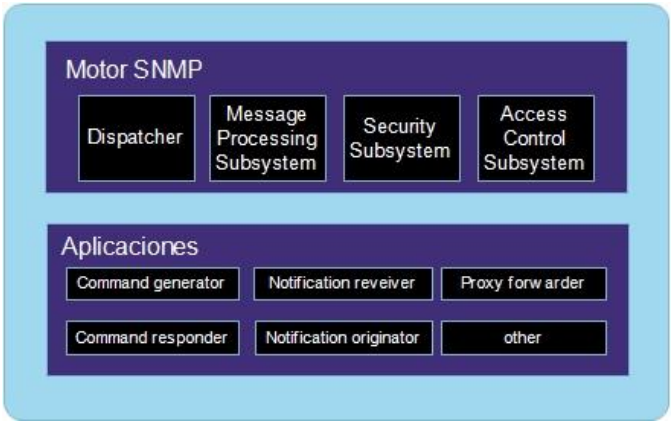


Figura 3.29 Entidad de SNMPv3 (Diagrama propio con base en [110])

Debido a que SNMPv3 es más complejo gracias a todas las implementaciones que efectúa, el tipo de mensajes que utiliza difiere mucho de SNMPv2, a continuación se describen los campos que contiene el mensaje SNMPv3 como se muestra en la figura 3.30.

- "Msg Version": Establece la versión del mensaje SNMP, en este caso es la versión 3.
- "MsgID": Se utiliza entre un gestor y un agente para coordinar los mensajes de solicitud y respuesta.
- "MsgMaxSize": Es el tamaño máximo de mensaje admitido por un remitente de un mensaje SNMP.
- "MsgFlags": Es un valor de 8 bits que especifica si se va a generar una PDU de informe, si se utiliza la privacidad y si se utiliza la autenticación.
- "MsgSecurityModel": Específica qué modelo de seguridad fue utilizado por el remitente del mensaje. Los valores son 1, 2 y 3 para SNMPv1, SNMPv2 y SNMPv3, respectivamente.

Los siguientes mensajes son generados por el modelo de seguridad USM:

- MsgAuthoritativeEngineID: Es el identificador del motor SNMP involucrado en el intercambio de mensajes. Puede ser la fuente de un "trap, response" o "report" ó el destino de un "get, getnext, getbulk" etc.
- MsgAuthoritativeEngineBoots: Representa la cantidad de veces que el motor se reinició a partir de la configuración inicial.
- MsgAuthoritativeEngineTime: Este campo se incrementa una vez por segundo, el destino del mensaje debe poder determinar este valor cada vez que se comunica.
- MsgUserName: Este campo contiene al usuario que puede estar autenticando y cifra el mensaje.

- MsgAuthenticationParameters: Este valor es nulo si no se utiliza ninguna autenticación. De lo contrario, el campo genera un código de autenticación de mensaje utilizando el algoritmo HMAC (Hashing Message Authentication Code - código de autenticación de mensaje basado en hash). Actualmente el RFC involucrado en SNMPv3 se especifica que MD5 y SHA deben ser utilizados.
- MsgPrivacyParameters: Este valor es nulo si no se utiliza encriptación. De lo contrario, este campo se utiliza para encriptar o desencriptar el mensaje con CBC-DES (Cipher Block Chaining mode of the Data Encryption Standard – modo de encadenamiento de bloques de cifrado del estándar de encriptación de datos).

El campo PDU es un PDU del protocolo SNMPv2 que junto con "contextEngineID" (Identifica de forma única una entidad SNMP) y "contextName" (identifica un contexto particular dentro de un motor SNMP) forman un "Scoped PDU", esta parte del mensaje puede estar en texto plano o encriptado [110,113].

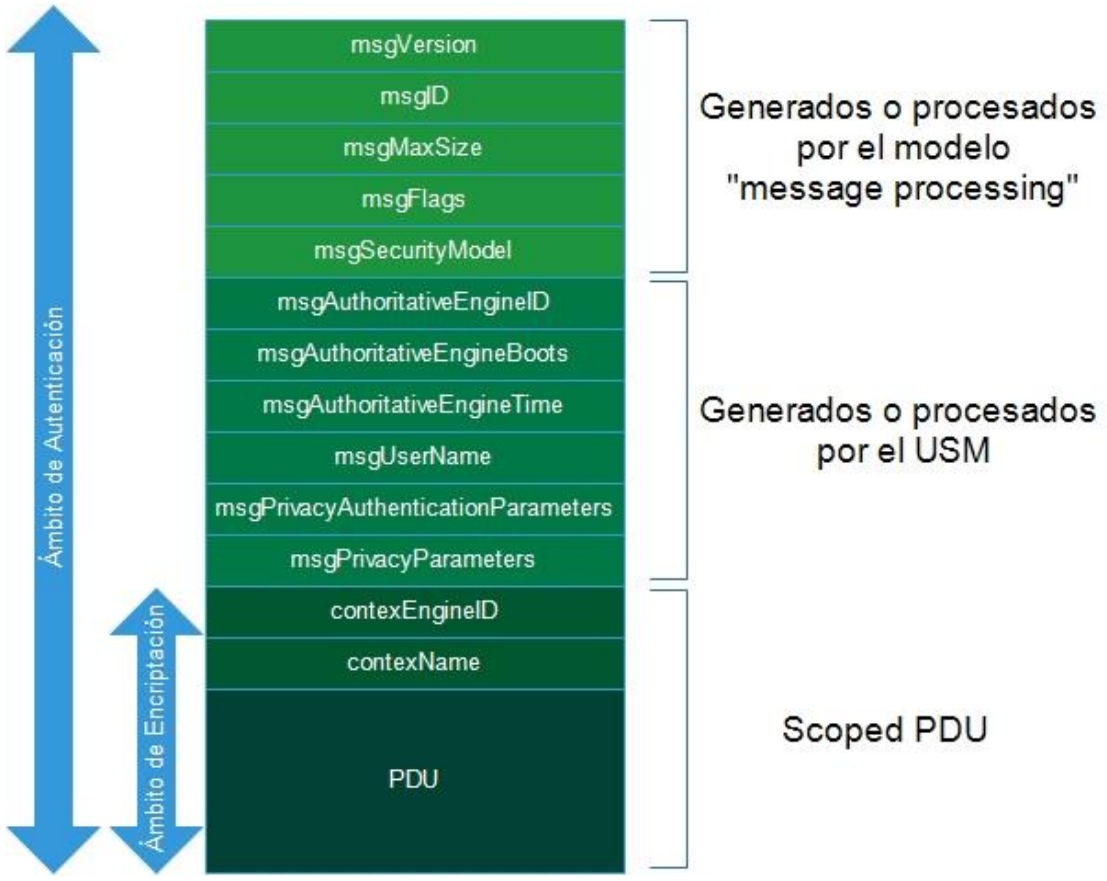


Figura 3.30 Formato de mensaje de SNMPv3 (Diagrama propio basado en [110])

Capítulo IV

Metodología para la simulación y emulación

"Podría parecer que hemos llegado a los límites alcanzables por la tecnología informática, aunque uno debe ser prudente con estas afirmaciones, pues tienden a sonar bastante tontas en cinco años"

John Von Neumann

IV.1 Simulación y emulación de la integración de las RA en América

La integración de las redes en América que se simuló y emuló está formada por las RA de: CANARIE, Internet2 y la red CLARA, se tomó la topología de backbone de cada red correspondiente al año 2016, cabe decir, que para la red de I2 se tomó sólo la "advanced layer 3 service". También se agregaron 5 routers para poder hacer la conectividad entre AS. El número total de routers implementados para el backbone fue de 58 routers de backbone, los cuales están distribuidos de la siguiente manera:

- Red CANARIE: 25 routers core
- Red Internet2: 15 routers core
- Red CLARA: 13 routers core

Los 5 routers faltantes son para la conectividad entre AS, los cuales están distribuidos de la siguiente manera:

- 3 routers (Pacific Wave, Startlight y MAN-LAN) están destinados para la conexión de CANARIE con Internet2 ubicados en Seattle, Chicago y New York
- 2 routers (El Paso y México) conectan a Internet2 con la red CLARA. Cabe mencionar que los routers de Atlanta y Miami también hacen la conectividad entre las RA mencionadas.

Además de estos 58 routers core se implementaron 15 routers de acceso, 5 routers por red avanzada, así el número total de routers es de 73 routers.

La asignación del número de AS de cada red está referido al ASN (Autonomous System Number) real de cada red, siendo estos: 6509 para CANARIE, 11537 para Internet2 y 27750 para CLARA. El ASN se obtuvo de la página *"Hurricane Electric Internet Service (www.he.net)",* dentro de esta misma página se obtuvieron también las direcciones IP que se implementaron en cada una de las redes.

Para la simulación se utilizó el programa "Packet Tracer v7.0.0.0306 (2016)", en el cual se agregaron los routers "Cisco 2811" para simular los routers core, ya que el simulador no cuenta con equipos core. Debido a la redundancia de algunos routers se agregaron 6 módulos "HWIC-2T" para las conexiones WAN. Para los routers de acceso se agregaron los routers "Cisco 1841", a estos routers se le conectaron los "switches 2960" donde se conectaron 5 laptops por cada red avanzada.

Para la emulación se utilizó el programa "Graphical Network Simulator-3 (GNS3 v1.5.3 -2017)" para el cual se ocuparon los routers "Cisco7200" con imagen IOS 7200 v15.1 (4)M4 para ser usados dentro del backbone; a ellos se le añadieron 6 módulos GbE (GigabitEthernet) y en algunos 1 módulo "FastEthernet" para la conexión con los routers de acceso. Los routers "Cisco 3620" con imagen IOS v12.3 (16) se ocuparon como routers de acceso donde sólo se añadieron 2 módulos FastEthernet, a estos routers se les conectaron los "Ethernet Switch" propios de GNS3. Se conectaron 5 host: 3 VPCS y 2 máquinas virtuales a cada red avanzada.

Para el enrutamiento dentro del AS de cada red avanzada se configuró el protocolo OSPFv2 y para el enrutamiento entre sistemas autónomos se configuró el protocolo BGPv4. Para la gestión de red se configuró el protocolo SNMPv2. Dentro de la simulación se encuentra un "MIB Browser" el cual viene integrado para poder analizar el protocolo SNMP, comparándolo con GNS3, este no tiene integrado un MIB Browser, así que se instalaron los programas "iReasoning MIB Browser" y "Power SNMP" dentro de una maquina virtual (VM) para poder hacer las pruebas de gestión. También se realizará una aproximación de cómo se ejecuta la gestión en un entorno real (similar a un NOC), para ello se ejecutara el software NPM (Network Performance Monitor) en un servidor, donde se comprobará como trabaja SNMP con NPM.

IV.2 Equipo necesario para simulación y emulación

El sistema donde se realizó la simulación, cumple con los requerimientos para soportarla debido a que en equipos similares se han hecho trabajos parecidos [15,16, 17], las características de este sistema son: Procesador Intel(R) Core (TM) i3-3120M CPU @ 2.50Ghz, Memoria RAM de 4GB, S.O. Windows 8.1 (64 bits) y 2 núcleos con 4 procesadores lógicos.

Debido a que las características del sistema donde se realizó la simulación no son suficientes para la realización de la emulación, esta se realizó en un sistema con recursos superiores a los óptimos de acuerdo a la referencia [115], el sistema es un "Super server" de SuperMicro el cual tiene las siguientes características: Procesador Intel Xeon (R) CPU E5-2620v2 @ 2.10Ghz, Memoria RAM de 32GB, S.O. Windows 8.1 (64 bits), 12 núcleos con 24 procesadores lógicos (con base en S.O), este sistema es un nodo del cluster "*xexelo*", ubicado en el B-404 de la UACM-SLT.

En la figura 4.1 se muestra como está constituida la integración de las RA de América, donde también se puede apreciar cómo está distribuido el backbone por todo el continente Americano y las correspondientes interfaces que conectan a todos los nodos del backbone.

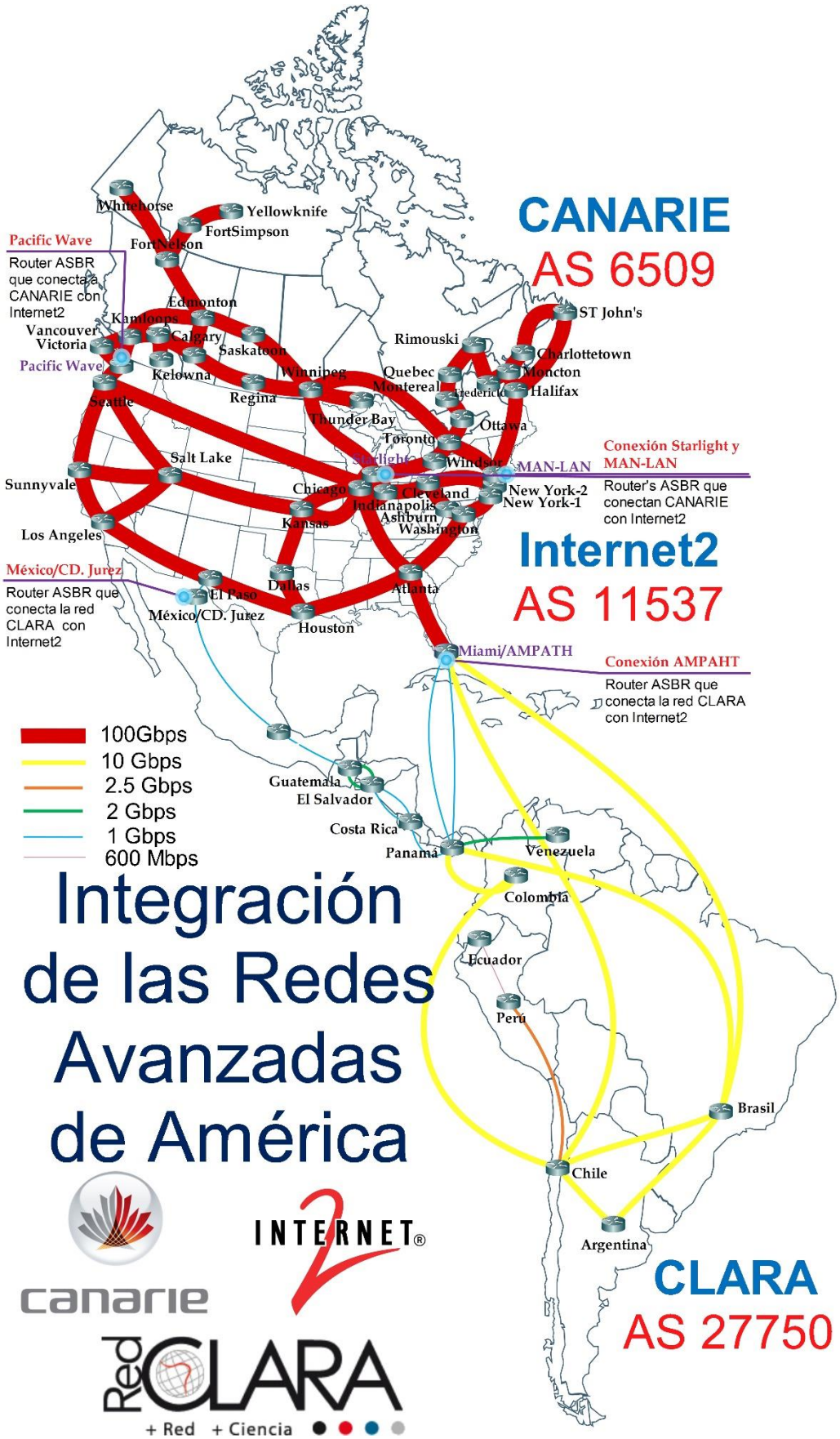


Figura 4.1 Integración de las Redes Avanzadas de América

IV.3 Tablas de direcciones IP

Esta sección describe las tablas de dirección IP que se utilizaron para cada red, en donde en cada porción de dirección IP se realizó VLSM para no desperdiciar muchas direcciones IP. En las tablas 4.1, 4.2 y 4.3 se encuentran las direcciones correspondiente a la red CANARIE, Internet2(cabe mencionar que también se listan las direcciones loopback utilizadas para el protocolo BGP) y la red CLARA, estas tablas están descritas de la siguiente manera: de izquierda a derecha se muestra el número de red correspondiente, la porción de red a la que pertenece, los nombres de los routers involucrados en ese segmento, la dirección IP asignada a cada router, la máscara de subred de cada dirección y en la última columna se encuentra en número de proceso de OSPF de cada red, así como el "wilcard" correspondiente.

CANARIE 205.198.32.0/24					
Red	**Dirección de red**	**Routers asociados**	**Dirección ip**	**Máscara (para todas las direcciones)**	**Wilcard (ospf 50) mismo para todos**
1	205.189.32.0/32	Victoria	205.189.32.1	255.255.255.252	0.0.0.3
		Vancouver	205.189.32.2		
2	205.189.32.4/32	Vancouver	205.189.32.5		
		Kamloops	205.189.32.6		
3	205.189.32.8/32	Kamloops	205.189.32.9		
		Kelowna	205.189.32.10		
4	205.189.32.12/32	Kamloops	205.189.32.13		
		Calgary	205.189.32.14		
5	205.189.32.16/32	Calgary	205.189.32.17		
		Edmonton	205.189.32.18		
6	205.189.32.20/32	Edmonton	205.189.32.21		
		fortNelson	205.189.32.22		
7	205.189.32.24/32	fortNelson	205.189.32.25		
		Whitehorse	205.189.32.26		
8	205.189.32.28/32	Fortnelson	205.189.32.29		
		Fortsimpson	205.189.32.30		
9	205.189.32.32/32	Fortsimpson	205.189.32.33		
		Yellowknife	205.189.32.34		
10	205.189.32.36/32	Edmonton	205.189.32.37		
		Saskatoon	205.189.32.38		
11	205.189.32.40/32	Saskaton	205.189.32.41		
		Winnipeg	205.189.32.42		
12	205.189.32.44/32	Calgary	205.189.32.45		
		Regina	205.189.32.46		
13	205.189.32.48/32	Regina	205.189.32.49		
		Winnipeg	205.189.32.50		
14	205.189.32.52/32	Winnipeg	205.189.32.53		
		Thunder bay	205.189.32.54		
15	205.189.32.56/32	Winnipeg	205.189.32.57		
		Toronto	205.189.32.58		
16	205.189.32.60/32	Toronto	205.189.32.61		
		Windsor	205.189.32.62		
17	205.189.32.64/32	Toronto	205.189.32.65		
		Ottawa	205.189.32.66		
18	205.189.32.68/32	Ottawa	205.189.32.69		
		Montreal	205.189.32.70		
19	205.189.32.72/32	Montreal	205.189.32.73		
		Quebec	205.189.32.74		
20	205.189.32.76/32	Quebec	205.189.32.77		
		Rimouski	205.189.32.78		
21	205.189.32.80/32	Rimouski	205.189.32.81		
		Fredericton	205.189.32.82		
22	205.189.32.84/32	Fredericton	205.189.32.85		
		Moncton	205.189.32.86		
23	205.189.32.88/32	Moncton	205.189.32.89		
		Charlottetown	205.189.32.90		
24	205.189.32.92/32	Charlottetown	205.189.32.93		
		St johns	205.189.32.94		
25	205.189.32.96/32	St johns	205.189.32.97		
		Halifax	205.189.32.98		
26	205.189.32.100/32	Halifax	205.189.32.101		
		Moncton	205.189.32.102		
27	205.189.32.104/32	Vancouver	205.189.32.105		
		Edmonton	205.189.32.106		

Tabla 4.1 Direcciones para la red de CANARIE

Internet2 "Advanced Layer 3 Service" (198.71.45.0/24)					
Red	**Dirección de red**	**Routers asociados**	**Dirección IP**	**Máscara de red (misma para todos)**	**Wilcard (ospf 100) mismo para todos**
1	198.71.45.0/30	Seattle	198.71.45.1	255.255.255.252	0.0.0.3
		Sunnyvale	198.71.45.2		
2	198.71.45.4/30	Seattle	198.71.45.5		
		Salt lake	198.71.45.6		
3	198.71.45.8/30	Seattle	198.71.45.9		
		Indianápolis	198.71.45.10		
4	198.71.45.12/30	Sunnyvale	198.71.45.13		
		Salt lake	198.71.45.14		
5	198.71.45.16/30	Sunnyvale	198.71.45.17		
		Los ángeles	198.71.45.18		
6	198.71.45.20/30	Los ángeles	198.71.45.21		
		Salk lake	198.71.45.22		
7	198.71.45.24/30	Salt lake	198.71.45.25		
		Kansas	198.71.45.26		
8	198.71.45.28/30	Los Ángeles	198.71.45.29		
		El paso	198.71.45.30		
9	198.71.45.32/30	El paso	198.71.45.33		
		Houston	198.71.45.34		
10	198.71.45.36/30	Houston	198.71.45.37		
		Dallas	198.71.45.38		
11	198.71.45.40/30	Kansas	198.71.45.41		
		Dallas	198.71.45.42		
12	198.71.45.44/30	Kansas	198.71.45.45		
		Chicago	198.71.45.46		
13	198.71.45.48/30	Kansas	198.71.45.49		
		Chicago	198.71.45.50		
14	198.71.45.52/30	Houston	198.71.45.53		
		Atlanta	198.71.45.54		
15	198.71.45.56/30	Atlanta	198.71.45.57		
		Chicago	198.71.45.58		
16	198.71.45.60/30	Atlanta	198.71.45.61		
		Washington	198.71.45.62		
17	198.71.45.64/30	Washington	198.71.45.65		
		New york 1	198.71.45.66		
18	198.71.45.68/30	New york 1	198.71.45.69		
		Cleveland	198.71.45.70		
19	198.71.45.72/30	Cleveland	198.71.45.73		
		Ashburn	198.71.45.74		
20	198.71.45.76/30	Ashburn	198.71.45.77		
		Washington	198.71.45.78		
21	198.71.45.80/30	Cleveland	198.71.45.81		
		Indianápolis	198.71.45.82		
22	198.71.45.84/30	Chicago	198.71.45.85		
		Starlight	198.71.45.86		
23	198.71.45.88/30	New york 2	198.71.45.89		
		MAN-LAN	198.71.45.90		
24	198.71.45.92/30	Seattle	198.71.45.93		
		Pacific wave	198.71.45.94		
25	198.71.45.96/30	New york 1	198.71.45.97		
		New york 2	198.71.45.98		
26	198.71.45.100/30	Chicago	198.71.45.102		
		Indianápolis	198.71.45.103		
27	198.71.45.104/30	Chicago	198.71.45.105		
		Indianápolis	198.71.45.106		

Direcciones loopback para ser usadas BGP			
Router	**Dirección Loopback**	**Máscara**	**Router-ID**
Pacific Wave	1.1.1.1	255.255.255.255.255	11.11.11.11
MAN-LAN	2.2.2.2	255.255.255.255.255	22.22.22.22
Starlight	3.3.3.3	255.255.255.255.255	33.33.33.33
El Paso	4.4.4.4	255.255.255.255.255	44.44.44.44
Atlanta	5.5.5.5	255.255.255.255.255	55.55.55.55

Tabla 4.2 direcciones para la red Internet2

Red CLARA (200.0.204.0/22)					
Red	**Dirección de red**	**Routers asociados**	**Dirección ip**	**Mascara**	**Wilcard (ospf 200) mismo para todos**
1	200.0.204.0/32	CUDI	200.0.204.1	255.255.255.252	0.0.0.3
		Guatemala	200.0.204.2		
2	200.0.204.4/32	Guatemala	200.0.204.5		
		Salvador	200.0.204.6		
3	200.0.204.8/32	Salvador	200.0.204.9		
		Costa Rica	200.0.204.10		
4	200.0.204.12/32	Costa Rica	200.0.204.13		
		Panamá	200.0.204.14		
5	200.0.204.16/32	Panamá	200.0.204.17		
		Venezuela	200.0.204.18		
6	200.0.204.20/32	Panamá	200.0.204.21		
		Colombia	200.0.204.22		
7	200.0.204.24/32	Colombia	200.0.204.25		
		Chile	200.0.204.26		
8	200.0.204.28/32	Chile	200.0.204.29		
		Peru	200.0.204.30		
9	200.0.204.32/32	Peru	200.0.204.33		
		Ecuador	200.0.204.34		
10	200.0.204.36/32	Chile	200.0.204.37		
		Brasil	200.0.204.38		
11	200.0.204.40/32	Brasil	200.0.204.41		
		Argentina	200.0.204.42		
12	200.0.204.44/32	Argentina	200.0.204.45		
		Chile	200.0.204.46		
13	200.0.204.48/32	Chile	200.0.204.49		
		Miami	200.0.204.50		
14	200.0.204.52/32	Brasil	200.0.204.53		
		Miami	200.0.204.54		
15	200.0.204.56/32	Panamá	200.0.204.57		
		Brasil	200.0.204.58		
16	200.0.204.60/32	Panamá	200.0.204.61		
		Miami	200.0.204.62		
17	200.0.204.64/32	CUDI	200.0.204.65		
		México	200.0.204.66		

Tabla 4.3 Direcciones para la red CLARA

La tabla 4.4 corresponde a las direcciones IP que tendrán los routers para poder conectar un AS con otro AS, a diferencia de las tablas anteriores, aqui que se tiene agregada la sección de "sesión BGP" la cual corresponderá al ASN de cada red para establecer la sesión BGP en cada router para poder hacer el enrutamiento entre AS.

Conexiones externas					
Red	**Dirección de red**	**Routers asociados**	**Dirección ip**	**Máscara de red**	**Sesión bgp**
1	199.212.24.0/30	Victoria	199.212.24.1	255.255.255.252	6509
		Pacific wave	199.212.24.2		11537
2	199.212.24.4/30	Vancouver	199.212.24.5		6509
		Pacific wave	199.212.24.6		11537
3	199.212.24.8/30	Winnipeg	199.212.24.9		6509
		Starlight	199.212.24.10		11537
4	199.212.24.12/30	Windsor	199.212.24.13		6509
		Starlight	199.212.24.14		11537
5	199.212.24.16/30	Toronto	199.212.24.17		6509
		MAN-LAN	199.212.24.18		11537
6	199.212.24.20/30	Halifax	199.212.24.21		6509
		MAN-LAN	199.212.24.22		11537
7	198.32.154.0/30	El paso	198.32.154.1		11537
		México	198.32.154.2		27750
8	198.32.154.4/30	Miami	198.32.154.5		11537
		Atlanta	198.32.154.6		27750

Tabla 4.4 Direcciones para los nodos que conectan a los AS.

La tabla 4.5 corresponde a las redes que se conectarán al backbone de cada red, donde se tienen direcciones privadas de clase C, con su respectiva "wildcard" (ya que se sigue ocupando el protocolo OSPF en estas redes), su "Gateway", la dirección de red asociada entre el router de la red y el router de backbone al que se conectará y sus respectivas direcciones IP.

Conexión a CANARIE					
Dirección de red	**Wilcard de la dirección de red**	**Gateway**	**Red del Router asociado**	**Direcciones del router asociado**	**Dirección de router backbone**
192.168.1.0/24	0.0.0.255	192.168.1.1	192.168.10.0/30	192.168.10.1/30	192.168.10.2/30
				192.168.1.1/24	
192.168.2.0/24	0.0.0.255	192.168.2.1	192.168.10.4/30	192.168.10.5/30	192.168.10.6/30
				192.168.2.1/24	
192.168.3.0/24	0.0.0.255	192.168.3.1	192.168.10.8/30	192.168.10.9/30	192.168.10.10/30
				192.168.3.1/24	
192.168.4.0/24	0.0.0.255	192.168.4.1	192.168.10.12/30	192.168.10.13/30	192.168.10.14/30
				192.168.4.1/24	
Red de la unidad gestora					
192.168.100.128/25	0.0.0.127	192.168.100.129	192.168.100.0/25	192.168.100.1/25	192.168.100.2/25
				192.168.100.129	
Conexión a Internet2					
192.168.20.0/24	0.0.0.255	192.168.20.1	192.168.30.0/30	192.168.30.1/30	192.168.30.2/30
				192.168.20.1/24	
192.168.21.0/24	0.0.0.255	192.168.21.1	192.168.30.4/30	192.168.30.5/30	192.168.30.6/30
				192.168.21.1/24	
192.168.22.0/24	0.0.0.255	192.168.22.1	192.168.30.8/30	192.168.30.9/30	192.168.30.10/30
				192.168.22.1/24	
192.168.23.0/24	0.0.0.255	192.168.23.0	192.168.30.12/30	192.168.30.13/30	192.168.30.14/30
				192.168.23.1/24	
Red de la unidad gestora					
192.168.150.128/25	0.0.0.127	192.168.150.129	192.168.150.0/25	192.168.150.1/25	192.168.150.2/25
				192.168.150.129	
Conexión a la red CLARA					
192.168.40.0/24	0.0.0.255	192.168.40.1	192.168.50.0/30	192.168.50.1/30	192.168.50.2/30
				192.168.40.1/24	
192.168.41.0/24	0.0.0.255	192.168.41.1	192.168.50.4/30	192.168.50.5/30	192.168.50.6/30
				192.168.41.1/24	
192.168.42.0/24	0.0.0.255	192.168.42.1	192.168.50.8/30	192.168.50.9/30	192.168.50.10/30
				192.168.42.1/24	
192.168.43.0/24	0.0.0.255	192.168.43.1	192.168.50.12/30	192.168.50.13/30	192.168.50.14/30
				192.168.43.1/24	
Red de la unidad gestora					
192.168.200.128/25	0.0.0.127	192.168.200.129	192.168.200.0/25	192.168.200.1/25	192.168.200.2/25
				192.168.200.129	

Tabla 4.5 Direcciones de redes conectadas al Backbone

IV.4 OIDs para pruebas de gestión

De acuerdo con el árbol de internet se puede realizar la gestión de varios OIDs de un dispositivo, es por eso que en la tabla 4.6 se muestran sólo 10 objetos del árbol MIB correspondientes a la gestión de los routers, ya que analizar todos los OIDs esta fuera de los objetivos de este trabajo [116]. Estos objetos fueron seleccionados bajo ciertos criterios que a continuación se describen:

1) Se eligieron algunos objetos que se pudieran no solo gestionar, sino de igual manera el poder configurarlos, lo cual depende del "tipo" que sea objeto (read-only ó read-write).
2) Utilización de las operaciones de SNMPv2 (get,get-next, get-bulk y set), para objetos que demanden una o varias instancias.
3) Utilización de objeto pertenecientes a cada fabricante (de acuerdo con el árbol MIB es1.3.6.1.4.1.x, la x corresponde al número correspondiente a cada fabricante), en este caso "Cisco (1.3.6.1.4.1.9)" debido a que tanto en el simulador como en el emulador se están ocupando routers Cisco.
4) Objetos pertenecientes a los protocolos de enrutamiento OSPF y BGP.

OID	Nombre del OID	Tipo	Descripción del objeto
1.3.6.1.2.1.1.5.0	Name	Read-write	Nombre de router o switch
1.3.6.1.2.1.3.1.1.3	atNetAddres	Read-only	Objetos que describe la dirección IP de cada interfaz asociada.
1.3.6.1.2.1.2.2.1.2	ifDescription	Read-only	Describe el tipo de interfaz
1.3.6.1.1.2.1.2.2.1.7	ifAdminType	Read-write	Administración de interfaces del router
1.3.6.1.2.1.4.22.1.4	ipNetToMedia Types	Read-only	Tipo de mapeo usado en la interfaz
1.3.6.1.2.1.4.21.1.7	ipRouteNextHop	Read-write	Describe cual es el siguiente salto para llegar a una ruta
1.3.6.1.2.1.14.1.2.0	ospfAdminStat	Read-write	Describe el estado de OSPF (habilitado o inhabilitado)
1.3.6.1.2.1.14.10.1.1	ospfNbrip	Read-only	Direcciones IP de los vecinos OSPF
1.3.6.1.2..1.15.1	Bgp	Read-only	Aspectos generales de BGP
1.3.6.1.4.1.9.9.25.1.1.1.2	CiscoImageString	Read-only	Descripción sobre la imagen IOS del dispositivo

Tabla 4.6 Objetos de SNMP que se gestionarán

IV.5 Metodología para simulación

Teniendo tablas IP se procedió a configurar cada interfaz de cada router, posteriormente se realizó la configuración de OSPF pero debido a que son varios routers y en algunos de ellos tiene varias interfaces conectadas, primero se verificó si la conexión entre los routers de una misma red realizaba la comunicación de manera bidireccional, esto se comprobó aplicando el comando ping de un router a otro y de manera inversa. Una vez que el protocolo OSPF se ejecutó en cada uno de los routers de manera satisfactoria, se procedió a comprobar si la tabla de enrutamiento era correcta, ya que si no se hallaba una dirección de red, se tenía que verificar de nuevo la comunicación de los routers o verificar si el problema era con el protocolo debido a si una dirección fue mal asignada o la "wilcard" que se ocupa no era la que correspondía. Es importante tener bien la verificación de OSPF ya que si se procede a configurar el protocolo BGP en el router que está ejecutando OSPF, éste le enviará rutas inalcanzables o no podrá mandar rutas de red que existen, que no se encuentran en su tabla de enrutamiento.

Teniendo todo comprobado en cuanto al protocolo OSPF, se procedió a configurar el protocolo BGP sólo en los routers designados (Victoria, Vancouver, Winnipeg, Halifax, Pacific Wave, Startlight, MAN-LAN, Atlanta, Miami, El Paso y México), teniendo cuidado de la sesión implementada en los routers designados ya que BGP puede tener un único proceso a diferencia de OSPF que puede tener varios procesos. A continuación se explicará la configuración de interfaz, configuración de OSPF y configuración de BGP.

1. Configuración de interfaz

En el CLI (Command Line Interface) de cada router en modo privilegiado (escribiendo "enable"), se accede al modo global de configuración (escribiendo en el prompt "#configure terminal") y se procedió a realizar toda la configuración. En la figura 4.2 se muestra la configuración para la interfaz serial que se le hizo a cada uno de los routers de las tres RA que conforman la integración, así como a las redes conectadas al backbone final.

```
BRASIL(config)#int s0/3/0
BRASIL(config-if)#clock rate 64000
BRASIL(config-if)#ip add 200.0.204.58 255.255.255.252
BRASIL(config-if)#no shutdown
```

Figura 4.2 Configuración de interfaz serial en el router Brasil

2. Configuración de OSPF:

En la figura 4.3 se muestra la configuración del protocolo OSPF, el cual para cada red se le asignó un número de proceso diferente referido en las tablas IP, esta configuración también se realizó en las redes que se conectaron al backbone, la única diferencia se encuentra en la configuración del área, ya que para el backbone se asignó el área 0 y para las redes que se conectarían a este backbone se les asigno el área 1 y, si se agregaran más redes se asignaría otro número de área. Así mismo se debe tener cuidado al configurar un router con muchas interfaces conectadas ya que si se configura una dirección de red incorrecta, el protocolo tardará en alcanzar el estado "full" debido a que estará en constante búsqueda de la red. En esta misma figura se muestra como después de un lapso de tiempo el router llega a un estado "full" pasando por un estado "loading".

```
PANAMA(config-router)#net 200.0.204.56 0.0.0.3 area 0
PANAMA(config-router)#net 200.0.204.60 0.0.0.3 area 0
PANAMA(config-router)#
01:04:30: %OSPF-5-ADJCHG: Process 200, Nbr 200.0.204.18 on
Serial0/1/0 from LOADING to FULL, Loading Done

01:04:31: %OSPF-5-ADJCHG: Process 200, Nbr 200.0.204.25 on
Serial0/2/0 from LOADING to FULL, Loading Done
```

Figura 4.3 Configuración de protocolo OSPF en el router Panamá

3. Configuración de BGP

En la figura 4.4 se muestra la configuración del protocolo BGP, donde primero se inicia la sesión BGP de acuerdo al AS correspondiente, y después se configura el o los "peers" del AS que se quieren alcanzar. Ésta configuración correspondiente al modo EBGP, después de esto, los "peers" configurados hacen adyacencia con lo que llegan a un estado "established". Aquí los routers que ejecutan BGP llegan a un estado "established".

```
PACIFIC-WAVE(config)#router bgp 11537
PACIFIC-WAVE(config-router)#bgp router-id 10.10.10.10
PACIFIC-WAVE(config-router)#neighbor 199.212.24.1 remote-as 6509
PACIFIC-WAVE(config-router)#neighbor 199.212.24.5 remote-as 6509
PACIFIC-WAVE(config-router)#
```

Figura 4.4 Configuración del protocolo BGP en el router Pacific Wave

4. Configuración de redistribución de ruta

Una vez la sesión esta activa solo falta hacer una redistribución de rutas en donde el protocolo IGP le envia al protocolo EGP las rutas para alcanzar ciertas redes, en este caso se deben

configurar sólo los routers de borde de cada AS, haciendo redistribución tanto en OSPF como en BGP. Así BGP le anuncia a OSPF que rutas externas tiene para ciertas redes y a su vez OSPF le anuncia a BGP las rutas que tiene para las redes que él puede alcanzar dentro de un AS y con ello BGP podrá anunciar esas rutas a otro "peer" asociado a otro AS. En la figura 4.5 se muestra esta configuración y como es que la sesión BGP se ha establecido. Una vez hecho esto, las tablas de enrutamiento de OSPF, como de BGP se vuelven a cargar, hasta que todos los routers tienen la misma tabla de enrutamiento.

```
PACIFIC-WAVE(config-router)#redistribute ospf 100
PACIFIC-WAVE(config-router)#router ospf 100
PACIFIC-WAVE(config-router)#redistribute bgp 11537 subnet
PACIFIC-WAVE(config-router)#defa
PACIFIC-WAVE(config-router)#default-information originate
PACIFIC-WAVE(config-router)#%BGP-5-ADJCHANGE: neighbor
199.212.24.1 Up
%BGP-5-ADJCHANGE: neighbor 199.212.24.5 Up
```

Figura 4.5 Aplicación de redistribución de ruta en BGP y OSPF en el router Pacific Wave

5. Configuración de SNMP

Dentro de la simulación de la integración se configuró el protocolo SNMPv2, este protocolo se activó en cada router y switch de cada red, debido a que SNMP cuenta un campo de "comunidad" donde se almacena una contraseña para fines de seguridad del dispositivo e identificación de este en una topología red, se configuró la contraseña de cada router y switch de acuerdo al nombre de estos dispositivos, así sólo la unidad gestora correspondiente podrá utilizarla para poder acceder al dispositivo gestionado. En la figura 4.6 se muestra la configuración de SNMP en el router Quebec, esta misma configuración se puede hacer en los switches.

```
QUEBEC>en
QUEBEC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
QUEBEC(config)#snmp-server community quebec ro
%SNMP-5-WARMSTART: SNMP agent on host QUEBEC is undergoing a warm
start
QUEBEC(config)#snmp-server community quebec rw
QUEBEC(config)#
```

Figura 4.6 Configuración de SNMP en el router Quebec

En la figura 4.7 se muestra la topología del backbone que resulta de la integración de las tres RA en Packet tracer, una vez que se configuraron todas las interfaces y protocolos de enrutamiento.

Figura 4.7 Integración de las 3 RA en América en packet tracer

IV.6 Metodología para emulación

Para realizar la emulación se ocuparon las siguientes herramientas con las que cuenta GNS3:

- ✓ Dynamips: Emulador de imágenes IOS de routers Cisco, como ya se había mencionado se ocuparan las imágenes correspondientes a los router cisco 7200 y cisco 3620.
- ✓ Virtual box: Emulador de máquinas virtuales, donde se levantaron 6 máquinas en total, entre ellas con sistema operativo; Windows 8 (2 VM), Fedora 20 (2 VM), Ubuntu 16(1 VM), Centos 7 (VM) y un servidor (Windows server 2012). Para poder utilizar las máquinas virtuales GNS3 le asigna su propia NIC (Network Interface Card) a cada VM.
- ✓ Wireshark: Programa que se ocupa para el análisis de tráfico de paquetes que esta presente en una red.
- ✓ Putty: Cliente SSH (Secure Shell) y Telnet de licencia libre que permite la conexión remota a un dispositivo (en este caso sólo para los routers), con el podemos ingresar al CLI de cada router.
- ✓ VPCS: Emulación de PC propia de GNS3.

Similar a packet tracer, primero se configuraron las interfaces y después los protocolos de enrutamiento y el protocolo de gestión.

1. Configuración de interfaz

La configuración es similar a PT sólo difiere de configurar interfaces seriales a configurar interfaces GigaEthernet, donde se debe entrar al CLI por medio de putty. En la figura 4.8 se muestra esta configuración hecha en el router de Edmonton, que de igual manera se ocupó en todos los routers del backbone.

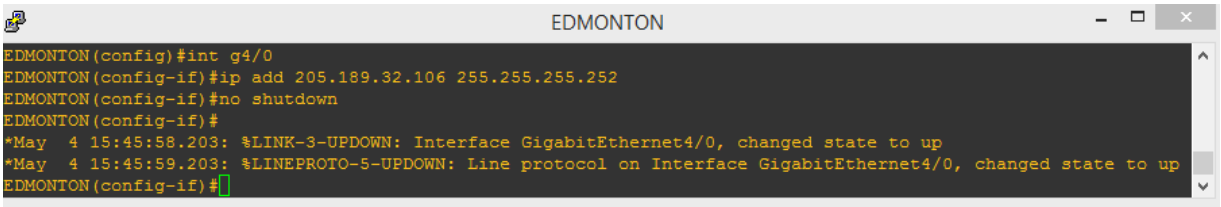


Figura 4.8 Configuración de interfaz GE en el router Edmonton

2. Configuración de OSPF

La configuración de OSPF es similar a PT como se muestra en la figura 4.9. En este ejemplo se muestra la configuración en el router Chicago debido a que éste presenta mayor redundancia y cómo es que se tiene que configurar todas las redes con las que el router está conectado.

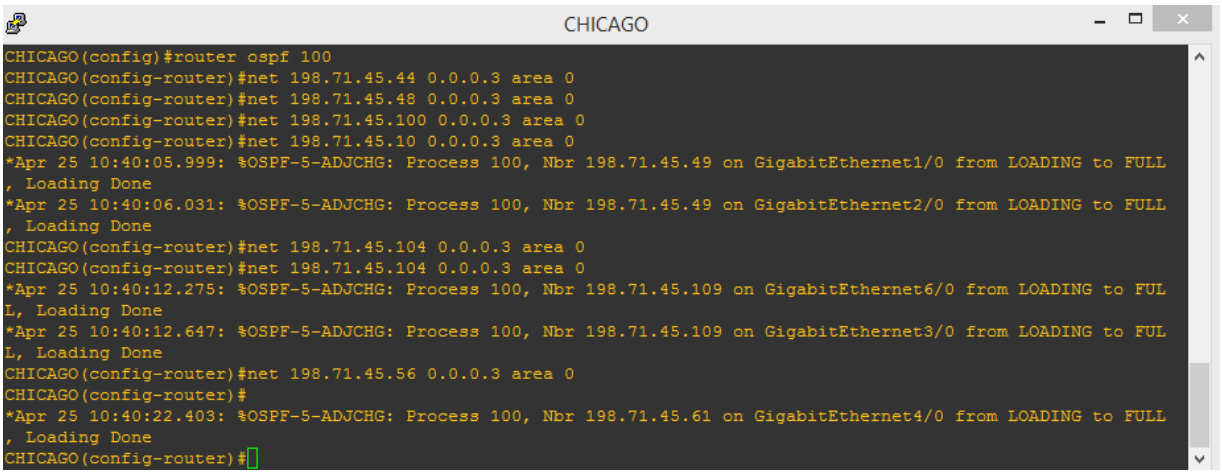


Figura 4.9 Configuración de OSPF en el router Chicago

3. Configuración de BGP y redistribución de ruta

La configuración es un poco similar a la de la simulación (tanto EBGP, como redistribución de ruta) salvo que GNS3 si permite la configuración de IBGP como se muestra en la figura 4.10. En esta imagen, se configuró en el router MAN-LAN la IP loopback para que pueda encontrar a su vecino dentro de un AS y así realizar una sesión IBGP para compartir actualizaciones con los respectivos "peers" de su mismo AS . Así mismo la utilización de direcciones loopback se tiene que activar ya que mediante estas direcciones se podrá establecer la sesión de vecindad dentro de un AS, así como el poder recibir actualizaciones de ruta que estos vecinos reciben de un AS distinto.

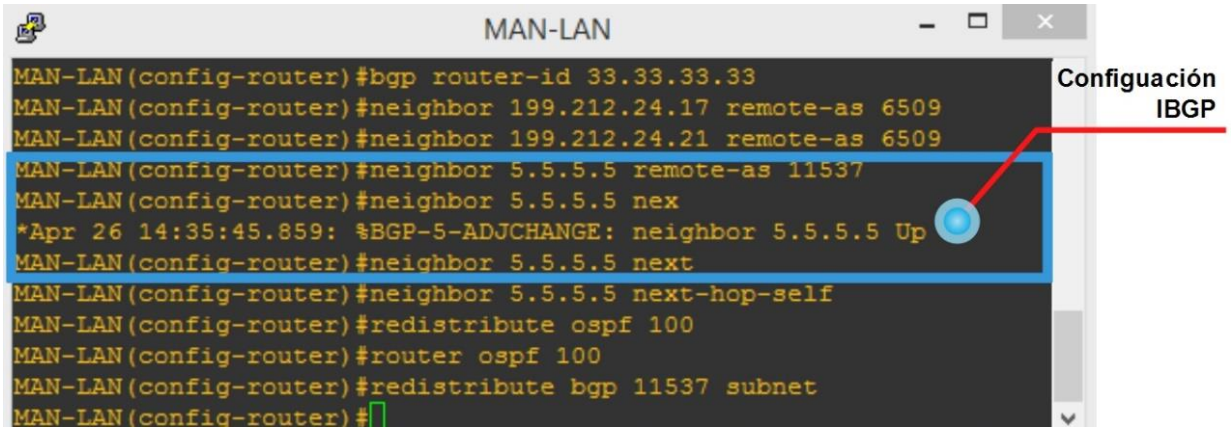


Figura 4.10 Configuración BGP incluyendo IBGP en el router MAN-LAN

4. Configuración de SNMP

Al igual que la simulación, la configuración es similar, pero la gran diferencia es que se pueden habilitar las "traps" en un router o switch. En la figura 4.11 se muestra esta configuración donde se configuró SNMPv2 en el router Vancouver. También se aprecia la configuración de la dirección IP de la unidad gestora.

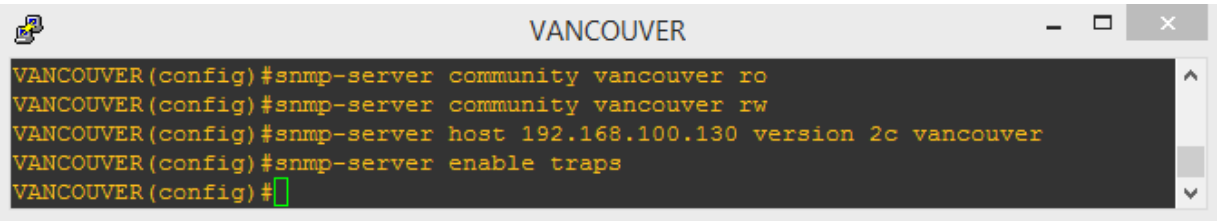


Figura 4.11 Configuración de SNMP en router Vancouver

5. Programas para comprobar el protocolo SNMP

Para el análisis de SNMP se instaló el programa "iReasoning MIB Browser" en la máquina virtual de windows, el cual desplegará una interfaz similar al MIB browser de Packet Tracer. En la figura 4.12 se muestra el despliegue del programa MIB Browser una vez instalado en la máquina virtual.

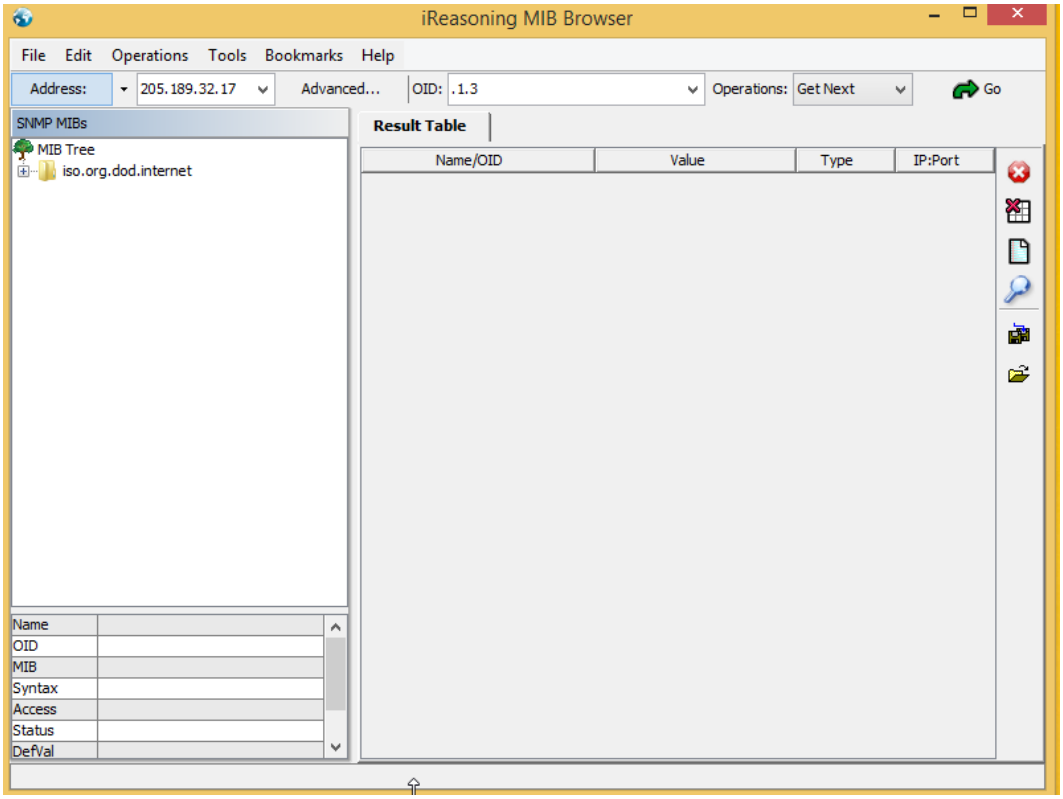


Figura 4.12 MIB browser ejecutado en la VM

También se instaló otro programa para comprobar SNMP, específicamente para la captura de "traps". La figura 4.13 muestra el programa "powerSNMP" instalado en la misma máquina virtual donde se instaló "MIB browser" el cual será de ayuda ya que con él se pueden recibir las "traps" que generan los routers gestionados.

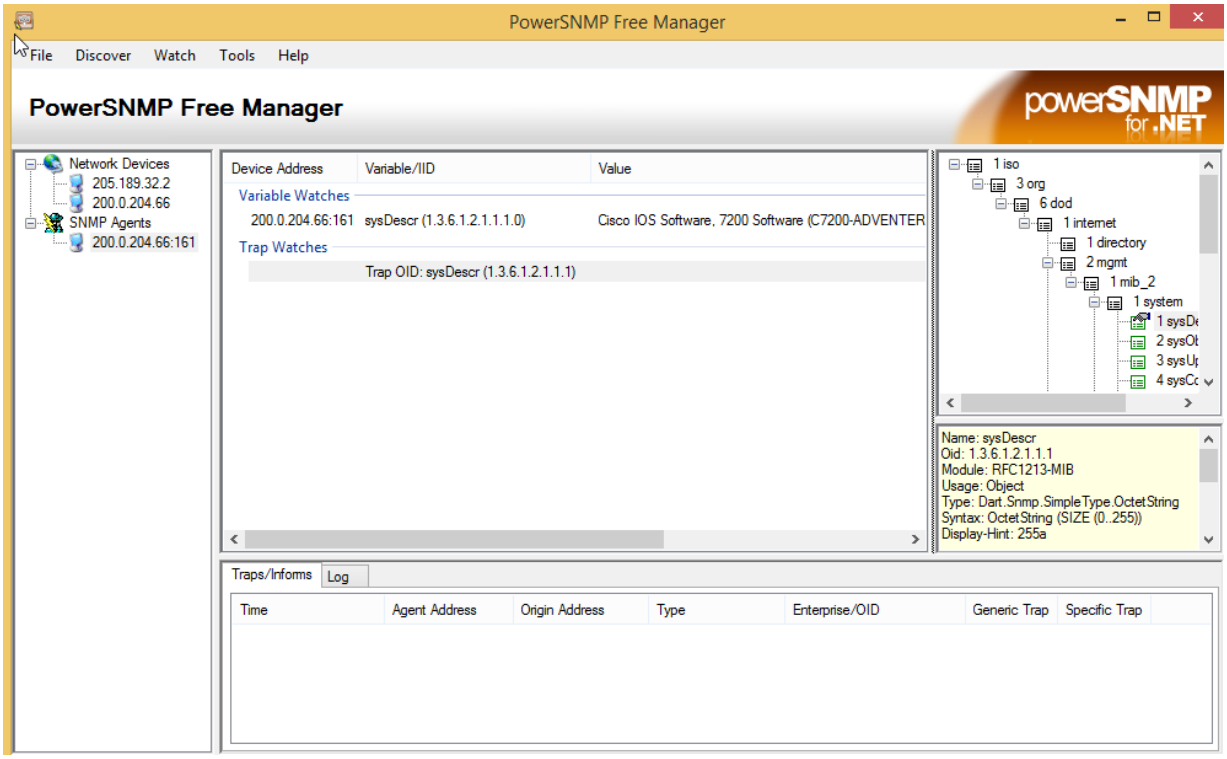


Figura 4.13 Power SNMP para la recolección de traps.

6. Servidor NPM como NMS de SNMP.

De acuerdo con los requerimientos de NPM, se levantó una VM donde se instaló el sistema "Windows server 2012" con las características óptimas para su instalación, una vez instalado se ejecutó el software NPM el cual se encarga de bajar los complementos necesarios para su ejecución. Una vez completado se accede a la página web que genero dicho programa, hecho esto se desplegará la interfaz de usuario (o gestor) como la que se muestra en la figura 4.14. Este servidor representa una aproximación a un NOC del mundo real donde se gestionarán todos lo routers del backbone de la integración.

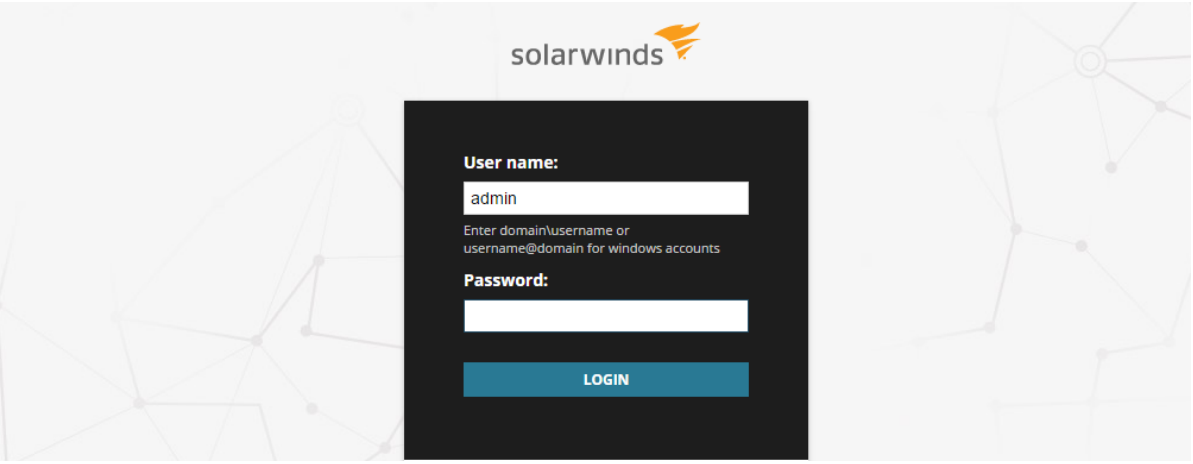


Figura 4.14 Interfaz de usuario para NPM

Una vez que se autentica el usuario se ingresa a una interfaz como la que se muestra en la figura 4.15, la cual despliega los elementos necesarios para descubrir la red que se requiere gestionar, esta parte no se realizó y se optó por añadir nodo por nodo para verificar la transferencia de OIDs de cada router.

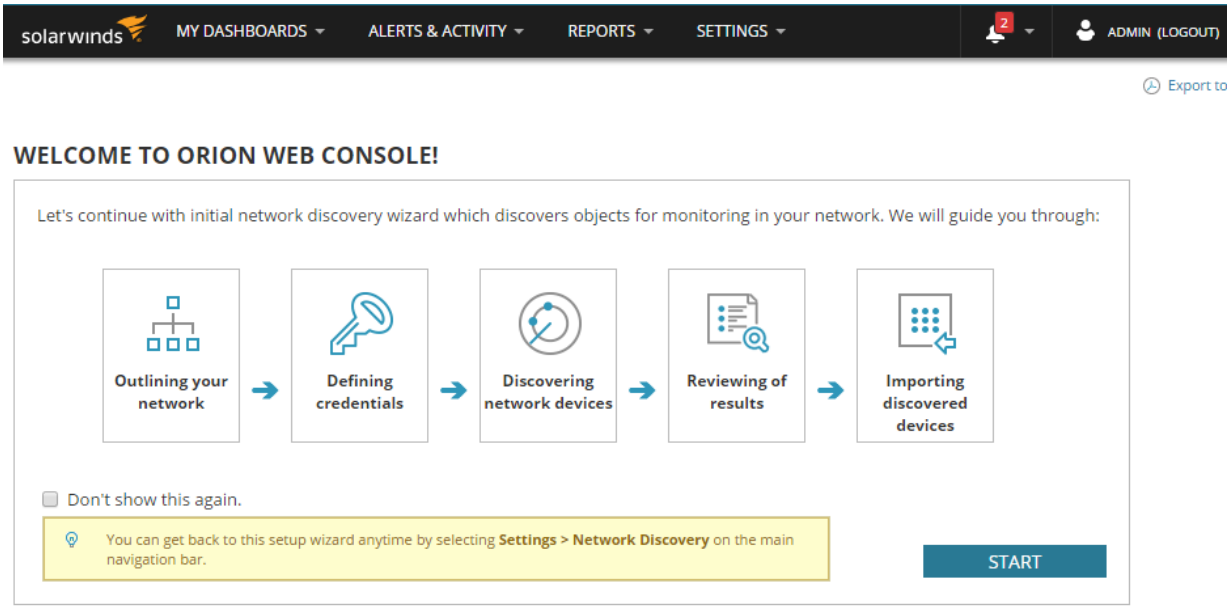


Figura 4.15 Interfaz NPM para el descubrimiento automático de la red.

En la figura 4.16 se muestra la distribución topológica del backbone integrado en GNS3 y la ubicación de las máquinas virtuales, éstas se identifican de acuerdo al símbolo del S.O utilizado en cada VM.

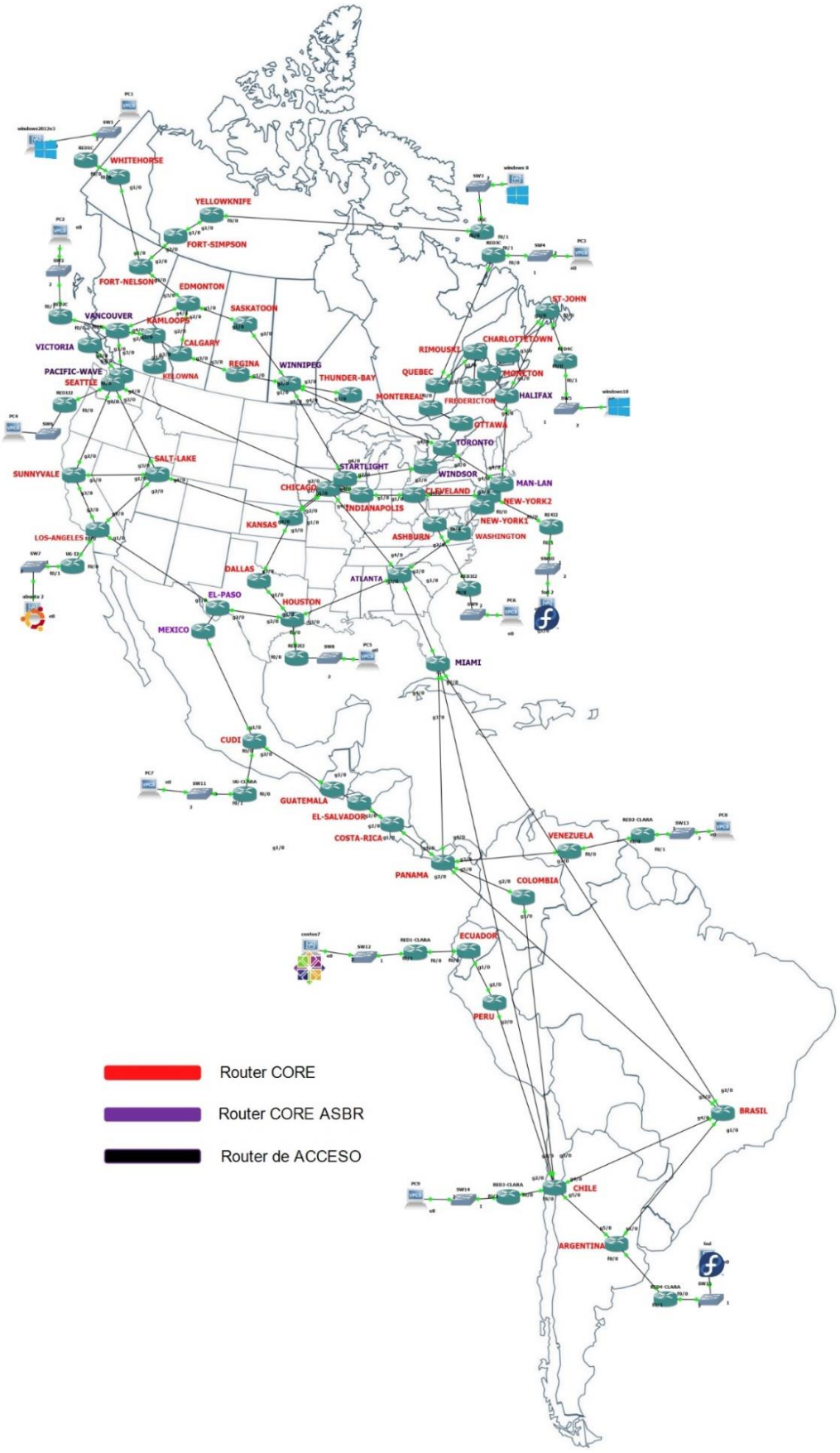


Figura 4.16 Topología de Backbone de la integración de las Redes Aavanzadas de América en GNS3

En la figura 4.17 se muestra cómo las VM están integradas a cada red avanzada, todas ellas están ejecutándose dentro del backbone y listas para ser usadas dentro de la integración, gracias a ellas se podrá comprobar la conectividad y la gestión de dispositivos con SNMP. De izquierda a derecha los sistemas operativos son: Windows server 2012, Windows8, windows10 (hosts para CANARIE), Ubuntu 16, Fedora 25 (hosts para Internet2), Centos7 y Fedora 25 (hosts para CLARA). Cabe decir que las aplicaciones que se ocuparán en la gestión sólo se están ejecutando en la máquina virtual Windows8 ubicada en elnodo Yellowknife.

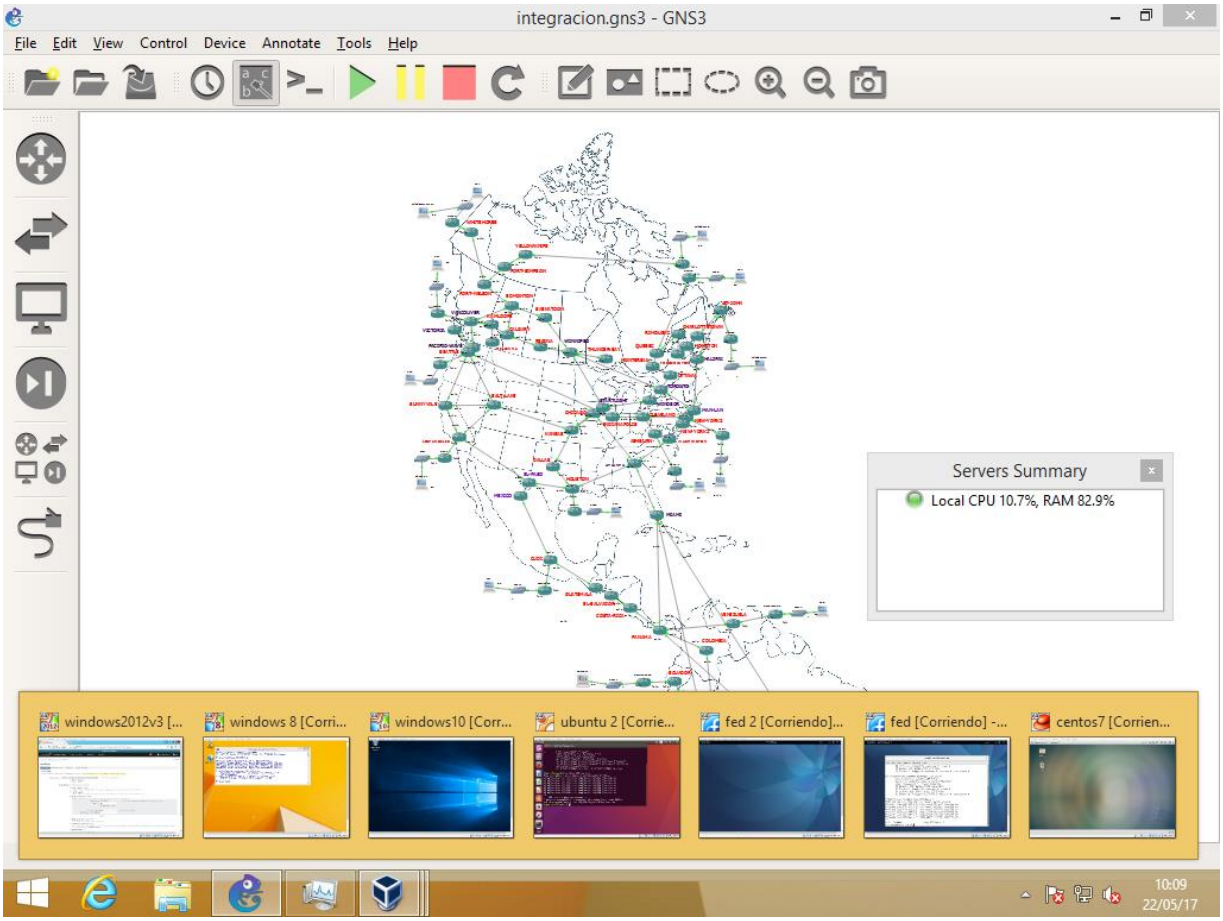


Figura 4.17 Integración de Backbone completa y funcionando en GNS3

Capítulo V

Resultados y discusiones

"En relación con la tecnología, no tenemos que preocuparnos solamente con que esta sea más eficiente y renovable, tenemos que invertir una tecnología creativa, que no solo lleva consigo un trabajo más creativo, sino que contribuya a mejorar el mundo natural al mismo tiempo que mejora el modo y la calidad de nuestras vidas."

Murray Bookchin.

V.1 Resultados de simulación

V.1.1 Resultados de los protocolos de enrutamiento

Una vez configurado OSPF en los 73 routers, cada uno alcanzó el estado “full”, asi que se procedió a comprobar la tabla de enrutamiento de cada router de cada red para corroborar si se encontraban todas las rutas en las tablas de enrutamiento. En algunas ocasiones puede existir una ruta hacia cierta red, pero el router no será capaz de alcanzarla, esto puede ser por una mala configuración del protocolo o comunicación entre los routers. Si se presenta este problema se tiene que comprobar toda la comunicación entre los routers hasta encontrar las rutas que interfieren con la comunicación. También se comprobaron las tablas de enrutamiento del protocolo BGP que están en los routers de frontera los cuales conectan a los 3 AS.

En la figura 5.1 se muestra la tabla de enrutamiento del router Pacific Wave perteneciente a Internet2, mismo que está ejecutando sólo el protocolo OSPF, se pueden apreciar las redes correspondientes al área 0 y las redes del área 1 (redes que estan conectadas al backbone), también se aprecia la interfaz y su dirección IP por la cual debe salir para alcanzar cierta red. Estas redes son las que el router puede alcanzar una vez ejecutado el algoritmo Dijkstra.

```
O IA 192.168.20.0/24 [110/66] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA 192.168.21.0/24 [110/194] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA 192.168.22.0/24 [110/322] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA 192.168.23.0/24 [110/450] via 198.71.45.93, 00:02:30, Serial0/0/0
     192.168.30.0/30 is subnetted, 4 subnets
O IA    192.168.30.0 [110/65] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA    192.168.30.4 [110/193] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA    192.168.30.8 [110/321] via 198.71.45.93, 00:02:30, Serial0/0/0
O IA    192.168.30.12 [110/449] via 198.71.45.93, 00:02:30, Serial0/0/0
     198.71.45.0/30 is subnetted, 26 subnets
O       198.71.45.0 [110/128] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.4 [110/128] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.8 [110/128] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.12 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.16 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.20 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.24 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.28 [110/256] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.32 [110/320] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.36 [110/320] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.40 [110/256] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.44 [110/256] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.48 [110/256] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.52 [110/320] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.56 [110/256] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.60 [110/320] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.64 [110/384] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.68 [110/512] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.72 [110/448] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.76 [110/384] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.88 [110/512] via 198.71.45.93, 00:02:51, Serial0/0/0
C       198.71.45.92 is directly connected, Serial0/0/0
O       198.71.45.96 [110/448] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.100 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.104 [110/192] via 198.71.45.93, 00:02:51, Serial0/0/0
O       198.71.45.108 [110/512] via 198.71.45.93, 00:02:51, Serial0/0/0
     199.212.24.0/30 is subnetted, 2 subnets
C       199.212.24.0 is directly connected, Serial0/0/1
C       199.212.24.4 is directly connected, Serial0/2/0

PACIFIC-WAVE>
```

Figura 5.1 Contenido de la tabla de enrutamiento del router Pacifc wave con 36 redes

En la figura 5.2 se muestra la tabla de enrutamiento del router Pacific Wave, en el cual se esta ejecutando tanto OSPF, como BGP; a diferencia de la figura 5.1 se pueden observar las rutas de las redes de CANARIE aprendidas mediante el protocolo BGP (este se identifica por la letra B).

```
Serial0/0/0
O       198.71.45.68 [110/256] via 198.71.45.93, 01:14:23,
Serial0/0/0
O       198.71.45.72 [110/256] via 198.71.45.93, 01:14:23,
Serial0/0/0
O       198.71.45.76 [110/320] via 198.71.45.93, 01:14:23,
Serial0/0/0
O       198.71.45.80 [110/192] via 198.71.45.93, 01:14:23,
Serial0/0/0
O       198.71.45.84 [110/192] via 198.71.45.93, 01:14:23,
Serial0/0/0
O       198.71.45.88 [110/320] via 198.71.45.93, 01:14:23,
Serial0/0/0
C       198.71.45.92 is directly connected, Serial0/0/0
     199.212.24.0/30 is subnetted, 2 subnets
C       199.212.24.0 is directly connected, Serial0/0/1
C       199.212.24.4 is directly connected, Serial0/2/0
     205.189.32.0/30 is subnetted, 26 subnets
B       205.189.32.0 [20/64] via 199.212.24.1, 01:14:51
B       205.189.32.4 [20/128] via 199.212.24.1, 01:14:51
B       205.189.32.8 [20/192] via 199.212.24.1, 01:14:51
B       205.189.32.12 [20/192] via 199.212.24.1, 01:14:51
B       205.189.32.16 [20/256] via 199.212.24.1, 01:14:51
B       205.189.32.20 [20/320] via 199.212.24.1, 01:14:51
B       205.189.32.24 [20/384] via 199.212.24.1, 01:14:51
B       205.189.32.28 [20/384] via 199.212.24.1, 01:14:51
B       205.189.32.32 [20/448] via 199.212.24.1, 01:14:51
B       205.189.32.36 [20/320] via 199.212.24.1, 01:14:51
B       205.189.32.40 [20/384] via 199.212.24.1, 01:14:51
B       205.189.32.44 [20/256] via 199.212.24.1, 01:14:51
B       205.189.32.48 [20/320] via 199.212.24.1, 01:14:51
B       205.189.32.52 [20/384] via 199.212.24.1, 01:14:51
B       205.189.32.56 [20/384] via 199.212.24.1, 01:14:51
B       205.189.32.60 [20/448] via 199.212.24.1, 01:14:51
B       205.189.32.64 [20/448] via 199.212.24.1, 01:14:51
```

Figura 5.2 Contenido de la tabla de enrutamiento del router Pacific wave

En el simulador sólo podemos ver en el CLI que OSPF y BGP llegan a la adyacencia alcanzando el estado “full” o “established” respectivamente, pero no se puede apreciar por todos los estados por los que pasan estos protocolos de enrutamiento, ya que el simulador no cuenta con un analizador de tráfico, En la figura 5.3 se aprecia una captura de inicio se sesión de BGP del router Startlight con Winnipeg para poder entablar la adyacencia, pero no se pueden apreciar si corresponde a un mensaje “open” o “update”, la misma limitación sucede con OSPF. El simulador no permite realizar un análisis más profundo de los estados de OSPF y BGP.

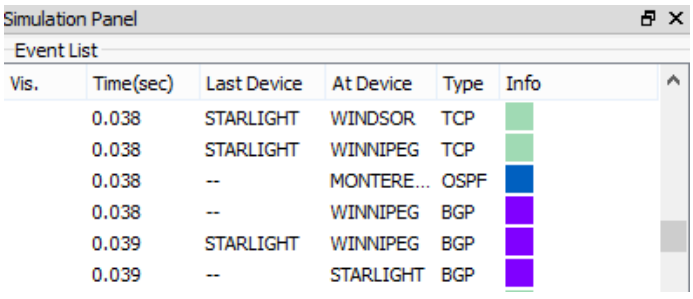


Figura 5.3 Inicio de Sesión de BGP en el router MAN-LAN

Continuando con el análisis de las tablas de enrutamiento, en la figura 5.4 se muestra el contenido de la tabla de enrutamiento del router Chicago perteneciente al backbone de Internet2, en la cual están contenidas las rutas para alcanzar a los AS (CANARIE y CLARA), a comparación de los routers de CLARA y CANARIE donde su tabla de enrutamiento no es tan grande debido a que no se puede ejecutar IBGP (Se explicará con detalle más adelante).

```
O E2 192.168.1.0/24 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                    [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2 192.168.3.0/24 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                    [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2 192.168.4.0/24 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                    [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
     192.168.10.0/30 is subnetted, 4 subnets
O E2    192.168.10.0 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    192.168.10.4 [110/20] via 198.71.45.105, 00:02:21, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:02:11, Serial0/2/0
O E2    192.168.10.8 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    192.168.10.12 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O IA 192.168.20.0/24 [110/130] via 198.71.45.105, 00:07:31, Serial0/0/0
O IA 192.168.21.0/24 [110/194] via 198.71.45.49, 00:07:31, Serial0/2/1
O IA 192.168.22.0/24 [110/130] via 198.71.45.57, 00:07:31, Serial0/2/0
O IA 192.168.23.0/24 [110/258] via 198.71.45.57, 00:07:31, Serial0/2/0
     192.168.30.0/30 is subnetted, 4 subnets
O IA    192.168.30.0 [110/129] via 198.71.45.105, 00:07:31, Serial0/0/0
O IA    192.168.30.4 [110/193] via 198.71.45.49, 00:07:31, Serial0/2/1
O IA    192.168.30.8 [110/129] via 198.71.45.57, 00:07:31, Serial0/2/0
O IA    192.168.30.12 [110/257] via 198.71.45.57, 00:07:31, Serial0/2/0
O E2 192.168.40.0/24 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2 192.168.41.0/24 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2 192.168.42.0/24 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2 192.168.43.0/24 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
     192.168.50.0/30 is subnetted, 4 subnets
O E2    192.168.50.0 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    192.168.50.4 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    192.168.50.8 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    192.168.50.12 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
     192.168.100.0/25 is subnetted, 2 subnets
O E2    192.168.100.0 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    192.168.100.128 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                        [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
     192.168.200.0/25 is subnetted, 2 subnets
O E2    192.168.200.0 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    192.168.200.128 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
     198.71.45.0/30 is subnetted, 26 subnets
O       198.71.45.0 [110/192] via 198.71.45.105, 00:07:59, Serial0/0/0
O       198.71.45.4 [110/192] via 198.71.45.49, 00:07:59, Serial0/2/1
                    [110/192] via 198.71.45.105, 00:07:59, Serial0/0/0
O       198.71.45.8 [110/128] via 198.71.45.105, 00:07:59, Serial0/0/0
O       198.71.45.12 [110/192] via 198.71.45.49, 00:07:59, Serial0/2/1
O       198.71.45.16 [110/256] via 198.71.45.49, 00:07:59, Serial0/2/1
                     [110/256] via 198.71.45.105, 00:07:59, Serial0/0/0
O       198.71.45.20 [110/192] via 198.71.45.49, 00:07:59, Serial0/2/1
O       198.71.45.24 [110/128] via 198.71.45.49, 00:07:59, Serial0/2/1
O       198.71.45.28 [110/256] via 198.71.45.57, 00:07:59, Serial0/2/0
                     [110/256] via 198.71.45.49, 00:07:59, Serial0/2/1
O       198.71.45.32 [110/192] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.36 [110/192] via 198.71.45.57, 00:07:59, Serial0/2/0
                     [110/192] via 198.71.45.49, 00:07:59, Serial0/2/1
O       198.71.45.40 [110/128] via 198.71.45.49, 00:07:59, Serial0/2/1
C       198.71.45.44 is directly connected, Serial0/0/1
C       198.71.45.48 is directly connected, Serial0/2/1
O       198.71.45.52 [110/128] via 198.71.45.57, 00:07:59, Serial0/2/0
C       198.71.45.56 is directly connected, Serial0/2/0
O       198.71.45.60 [110/128] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.64 [110/192] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.68 [110/320] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.72 [110/256] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.76 [110/192] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.88 [110/320] via 198.71.45.57, 00:07:59, Serial0/2/0
O       198.71.45.92 [110/192] via 198.71.45.105, 00:07:59, Serial0/0/0
O       198.71.45.96 [110/256] via 198.71.45.57, 00:07:59, Serial0/2/0
C       198.71.45.100 is directly connected, Serial0/3/1
C       198.71.45.104 is directly connected, Serial0/0/0
O       198.71.45.108 [110/320] via 198.71.45.57, 00:07:59, Serial0/2/0
     200.0.204.0/30 is subnetted, 17 subnets
O E2    200.0.204.0 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.4 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.8 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.12 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.16 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.16 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.20 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.24 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.28 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.32 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.36 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.40 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.44 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.48 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.52 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.56 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.60 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
O E2    200.0.204.64 [110/20] via 198.71.45.57, 00:05:24, Serial0/2/0
     205.189.32.0/30 is subnetted, 27 subnets
O E2    205.189.32.0 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.4 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.8 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                     [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.12 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.16 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.20 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.24 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.28 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.32 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.36 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.40 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.44 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.48 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.52 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.56 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.60 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.64 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.68 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.72 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.76 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.80 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.84 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.88 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.92 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.96 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                      [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.100 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                       [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
O E2    205.189.32.104 [110/20] via 198.71.45.105, 00:06:06, Serial0/0/0
                       [110/20] via 198.71.45.57, 00:05:38, Serial0/2/0
```

Figura 5.4 Contenido de la tabla de enrutamiento del router de Chicago perteneciente a I2 con 111 rutas

Dentro de la tabla de enrutamiento de la figura 5.4 se tiene todas las redes que puede alcanzar dentro del AS (Internet2) así como las redes que se encuentran en otro AS (CLARA y CANARIE) que aprendió por medio de BGP, todas estas redes descritas con su respectiva métrica de cómo alcanzarlas. Se puede apreciar la diferencia de estas rutas de acuerdo a cada término que a continuación se describe:

- C – Describe las redes que están conectadas directamente a ese router.
- O IA – Describe las redes que puede alcanzar, las cuales aprendió mediante OSPF a través de otra u otras áreas.
- O – Describe las redes que puede alcanzar, aprendidas mediante OSPF dentro de una misma área, en este caso dentro del área 0 o área de Backbone.
- O E2 – Describe las redes que puede alcanzar que aprendió mediante OSPF via BGP.

V.1.2 Resultados de conectividad

Una vez que se verificaron todas las tablas de enrutamiento se procedió a comprobar la conectividad de la integración, pero primeramente se comprobó la conectividad de cada red avanzada donde se mandaron paquetes ICMP con el comando “ping” dentro de un AS empezando por CANARIE, después Internet2 y por último la red CLARA. Posteriormente se mandaron los paquetes ICMP de un AS a otro AS para comprobar la integracion de las 3 RA. En la figura 5.5 se muestran los paquetes que se mandaron de la red CLARA a Internet2 y de la red CANARIE a Internet2 donde se aprecian las rutas que siguieron los paquetes para cada caso.

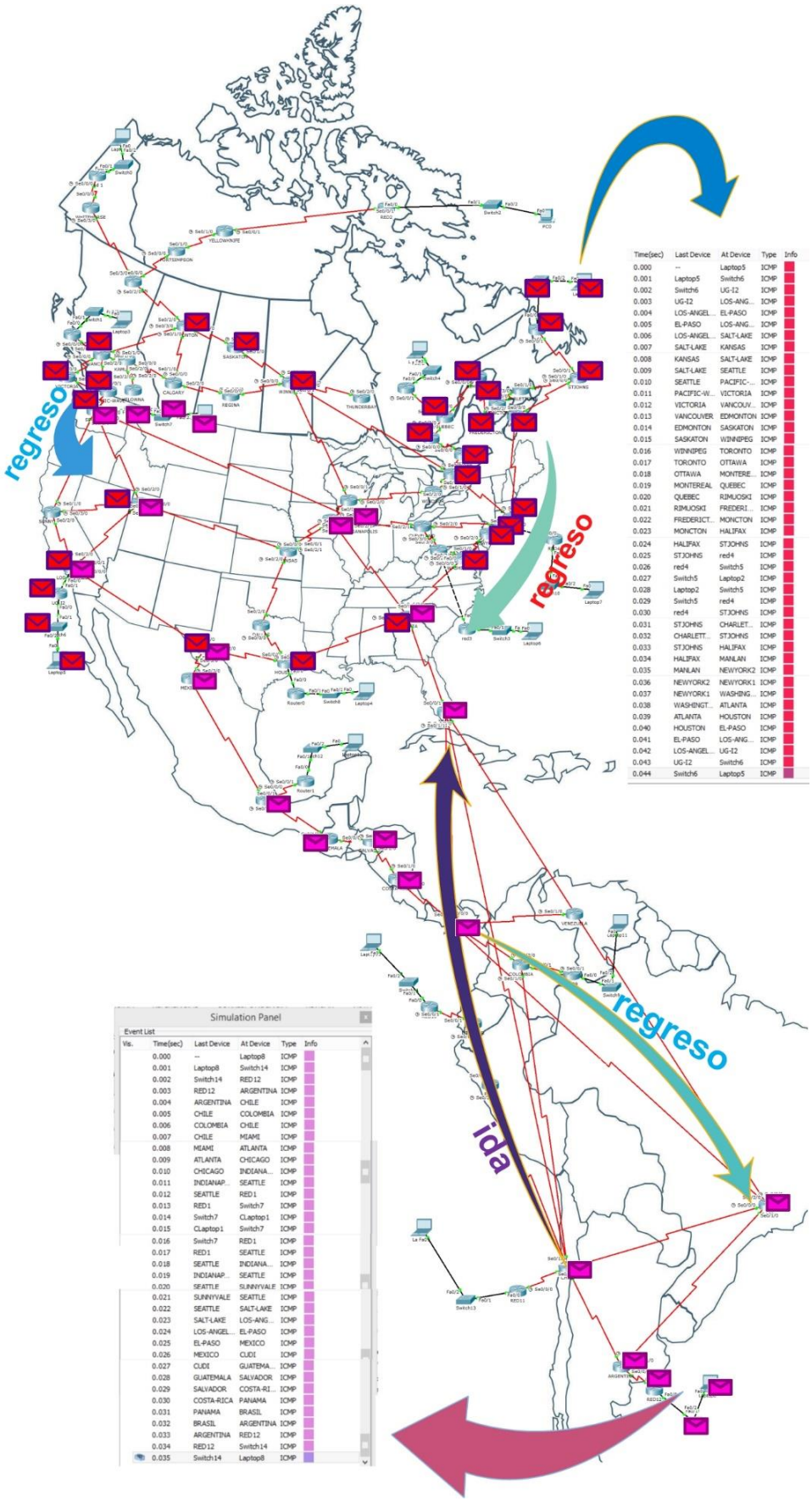


Figura 5.5 Verificación de conectividad entre sistemas autónomos en PT

En la tabla 5.1 se aprecia la diferencia entre el tiempo de envió de los mensajes ICMP (comando ping), recursos del sistema (CPU y Memoria RAM) que se emplearon en las diferentes redes, así como de la integración de las tres RA. Cabe decir que los resultados pueden variar (de 2 a 5 minutos), donde pueden ser mayor o menor tiempo de acuerdo a los mensajes que se vayan generando dentro del backbone de la simulación.

Packet tracer	Tiempo de envió de mensajes ICMP	Recursos del CPU	Recursos del memoria RAM
Red CANARIE			
Modo Simulación	21:30 min	25-27%	38% (1.5GB)
Modo Real	25 s	25-27%	38% (1.5GB)
Red Internet2			
Modo Simulación	15:30 min	25-27%	40% (1.6GB)
Modo Real	20 s.	25-27%	40% (1.6GB)
Red CLARA			
Modo Simulación	12:40 min	25-26%	38% (1.5GB)
Modo Real	17 s.	25-26%	38% (1.5GB)
Integración de las RA (de Internet2 a CANARIE)			
Modo Simulación	35:40 min	30-36%	60% (2.3GB)
Modo Real	1:31 min.	30-36%	60% (2.3GB)
Integración de las RA (de CLARA a Internet2)			
Modo Simulación	24:25 min	30-36%	59% (2.3GB)
Modo Real	1:17 min.	30-36%	59% (2.3GB)

Tabla 5.1 Evaluación de tiempos de envió del mensaje ICMP

Dentro de la tabla no aparece los mensajes ICMP de la red CLARA a CANARIE debido a una limitación de configuración que tiene "*packet tracer*". Para que la red CLARA tenga conectividad con la red CANARIE, los routers de borde (Peer BGP) de Internet2 que conectan a CANARIE y CLARA tiene que mandarse las rutas que apredieron de cada red avanzada, esta comunicación se hace através de IBGP. Mediante interfaces "loopback" pueden mandar información de un "peer" a otro"peer" sin necesidad de estar directamente conectados. Debido a las limitaciones del simulador, la configuración IBGP no es posible, en la figura 5.6 se muestra el mensaje que envia "packet tracer" al querer realizar la configuración de IBGP.

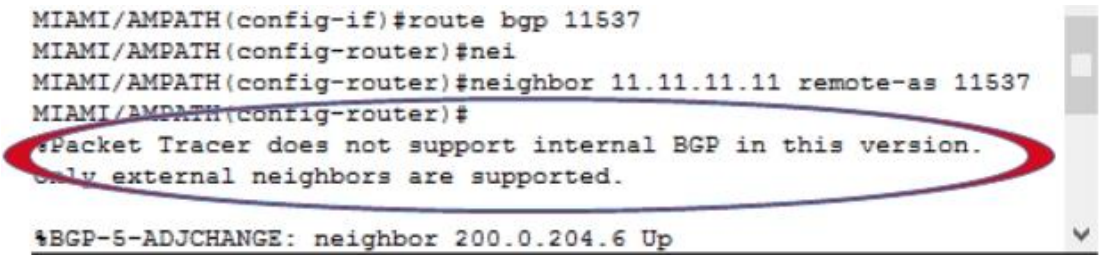


Figura 5.6 Mensaje de IBGP no soportable en PT

V.1.3 Resultados de prueba de gestión

Una vez hecha la configuración SNMP dentro de cada router, se comprobó si es posible gestionar los routers por medio de cualquier unidad gestora (pc), se hizo entrando al apartado "desktop" de la PC, una vez dentro se elige la opción "MIB Browser", después selecciona la opción llamada "advanced". Aqui se ingresa la dirección IP del dispositivo que se desee gestionar y la contraseña (cadena de comunidad) que se configuró en el dispositivo, también se elige la versión de SNMP a utilizar (en este caso se eligió la versión 2). Cabe decir que el simulador no diferencia entre la versión 2 o 3 debido a los pocos alcances que ofrece. En la figura 5.7 se muestra todo el proceso que se describió.

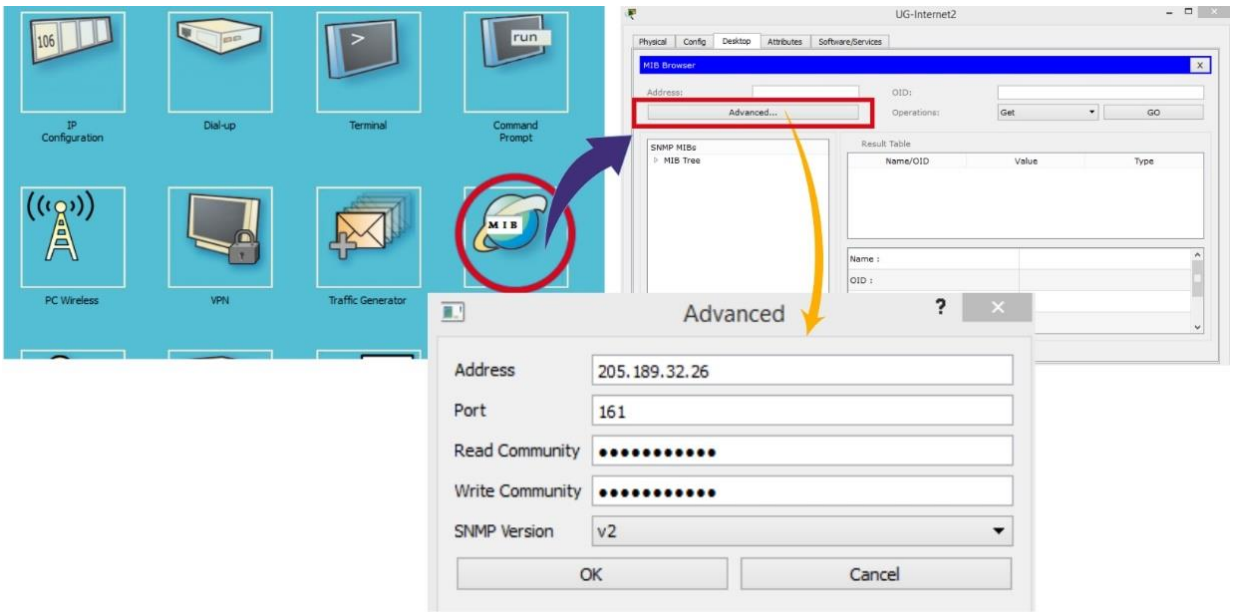


Figura 5.7 Inicio de sesión de gestión usando SNMPv2

Una vez teniendo la sesión lista se tendra una interfaz donde se podrá apreciar el árbol MIB como lo muestra la figura 5.8. Dentro de este árbol se puede elegir qué objeto del dispositivo se quiere gestionar. Una vez elegido el objeto, en la parte superior izquierda de la interfaz se encuentra un apartado para el OID (Object ID) y debajo de él se encuentran las operaciones SNMP que se pueden utilizar en packet tracer (sólo get, getbulk. y set).

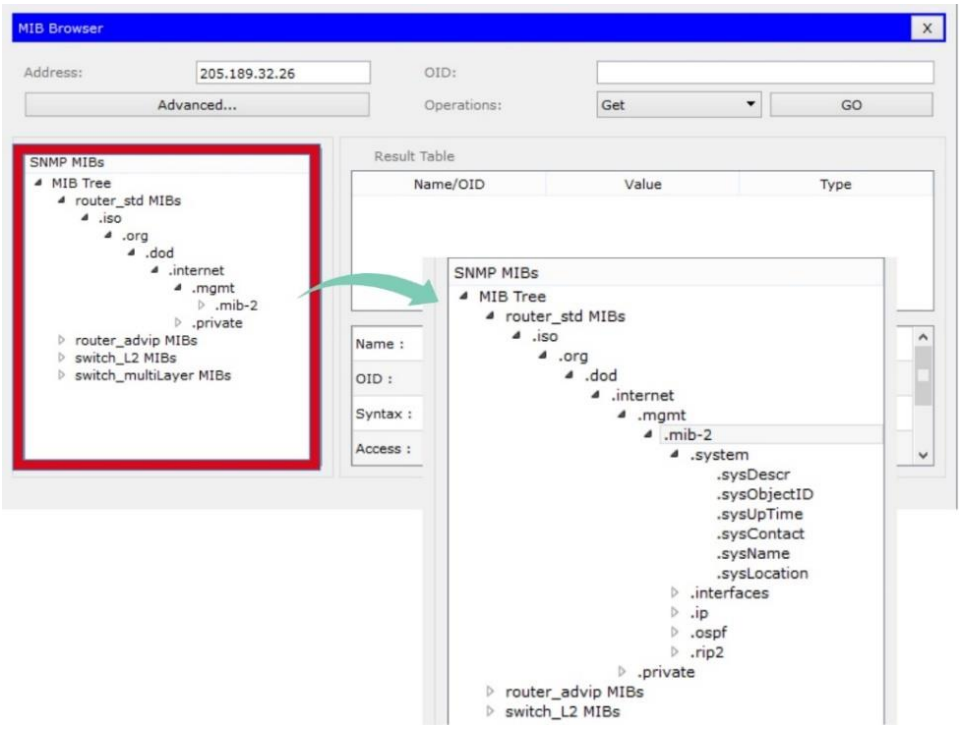


Figura 5.8 Árbol MIB en packet tracer

Las siguientes 6 figuras corresponden a los objetos gestionados de acuerdo con la tabla 4.6. Para esta demostración de prueba de gestión se ocupó el router Vancouver con la unidad gestora ubicada en Yellowknife. En la figura 5.9 se muestra el objeto "name", el cual despliega el nombre del router, en este caso se muestra el nombre "Vancouver".

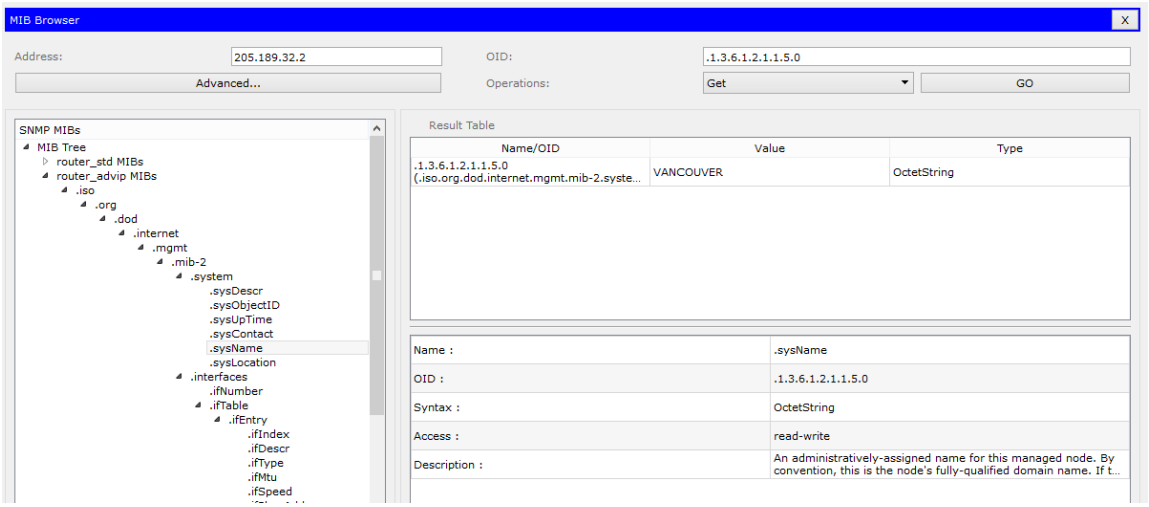


Figura 5.9 Gestión del Objeto "name"

En la figura 5.10 se muestra el objeto "ifDescription", el cual contiene el tipo de interfaz con el que está trabajando el router. En este ejemplo se muestran las interfaces seriales y "fastEhternet" del router Vancouver.

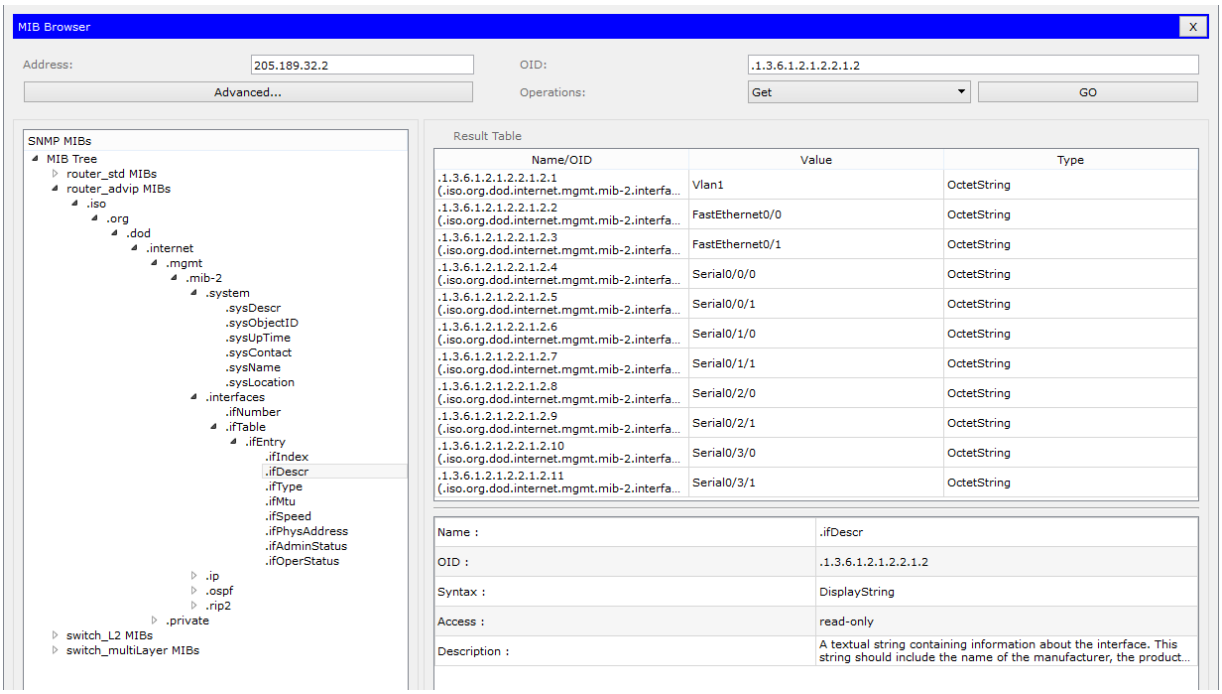


Figura 5.10 Gestión del objeto "ifDescription"

En la figura 5.11 se muestra el objeto "ifAdminStatus", el cual registra el estado de las interfaces, no muestra qué interfaces son, pero con el objeto anterior se puede saber que interfaz es la que está activa. En este ejemplo se muestran las interfaces activas (up) que corresponden a las interfaces seriales.

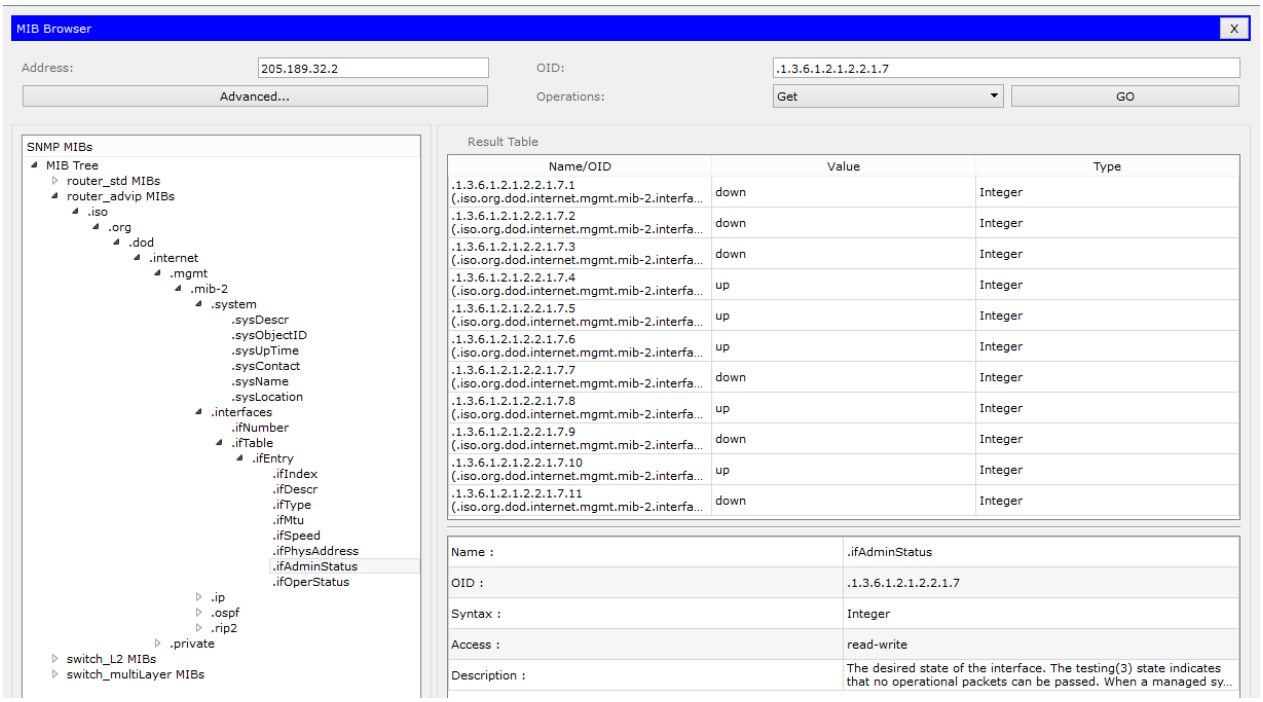


Figura 5.11 Gestión del objeto "ifAdminStatus"

En la figura 5.12 se muestra el objeto "ifNextHop", el cuál ayuda a saber cual es el siguiente salto que debe hacer el router dependiendo de la red que quiera alcanzar.

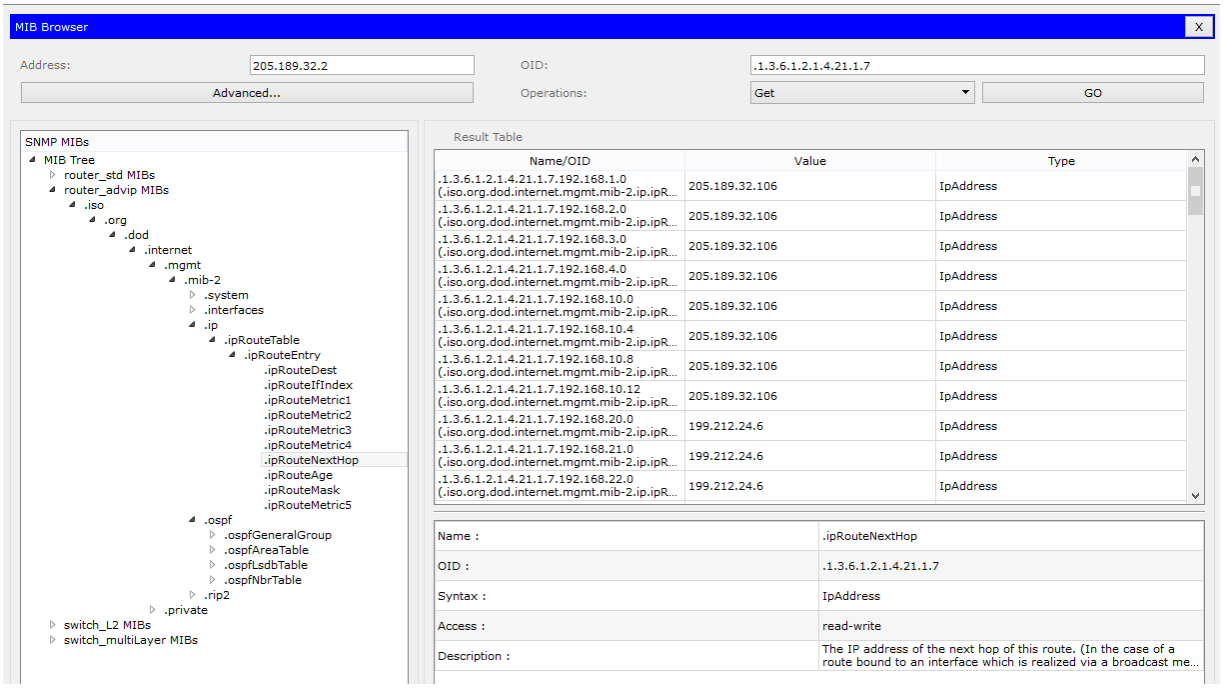


Figura 5.12 Gestión del objeto "ifNextHop"

En la figura 5.13 se muestra el objeto "ospfAdminStat", el cual despliega el estado en que se encuentra el protocolo OSPF. En este caso se tiene a OSPF como *"enabled"*.

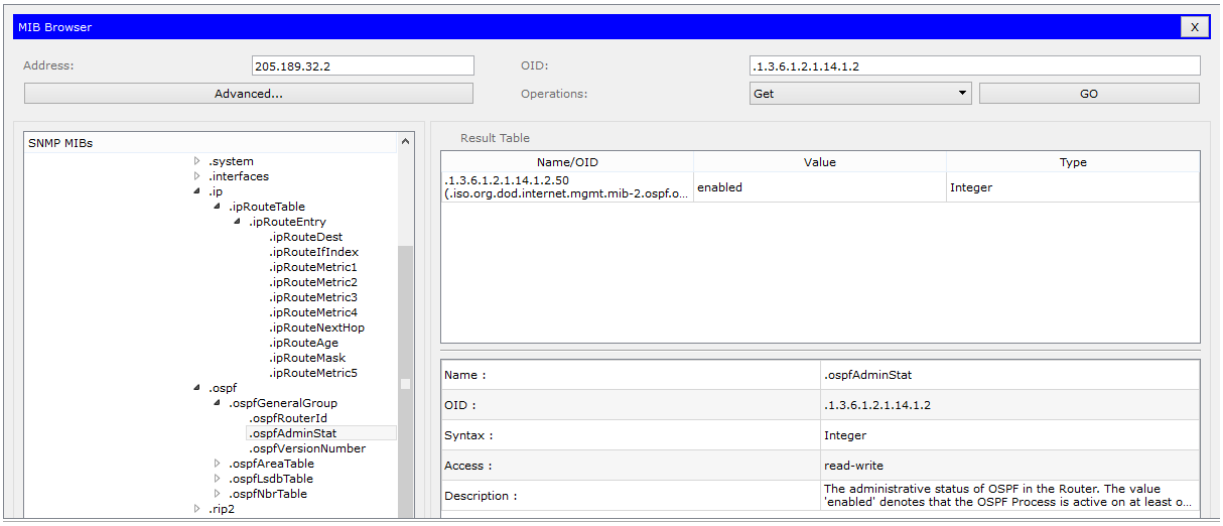


Figura 5.13 Gestion de objeto "ospfAdminStat"

En la figura 5.14 se muestra el objeto "ospfNbrIpAddr" el cual muestra las direcciones IP de los vecinos del router. En este caso se muestran las díreccíones IP de los vecinos que tiene el router Vancouver.

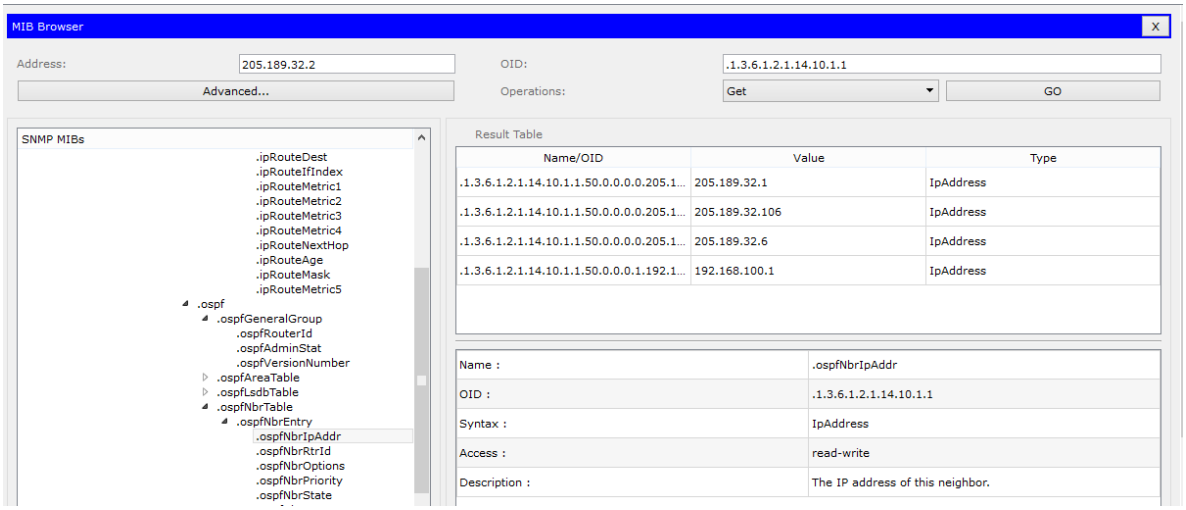


Figura 5.14 Gestión de objeto "ospfNbrIpAddr"

De acuerdo con la tabla 4.6 sólo se pudieron gestionar 6 de los 10 objetos, ya que los demás le es imposible al simulador acceder a ellos debido a sus limitaciones. Como resultado se logró la configuración de algunos objetos con la operación "set". Se configuró el nombre y la activación de las interfaces del router, donde éste no mostró algún aviso de cambio, sólo mostró el cambio del nombre al ingresar a él, asi como la verificación del estado de las interfaces. No hubo aviso cuando se configuró el objeto "ospfAdminStat", para ello se revisó la tabla de enrutamiento y OSPF estaba desactivado. La configuración del estado de OSPF es peligrosa ya que se notó que si se desactiva, este protocolo desaparece de la tabla de enrutamiento y se desactiva la adyacencia con sus vecinos ocasionando problemas de conectividad en el AS. En la tabla 5.2 se muestra el resumen de los objetos monitoreados y configurados con el protocolo SNMP.

Objeto	Monitoreado	Configurado
Name	✓	✓
atNetAddres	✗	✗
ifDescription	✓	✗
ifAdminType	✓	✓
ipNetToMedia Types	✗	✗
ipRouteNextHop	✓	✓
ospfAdminStat	✓	✓
ospfNbrip	✓	✗
Bgp	✗	✗
CiscoImageString	✗	✗

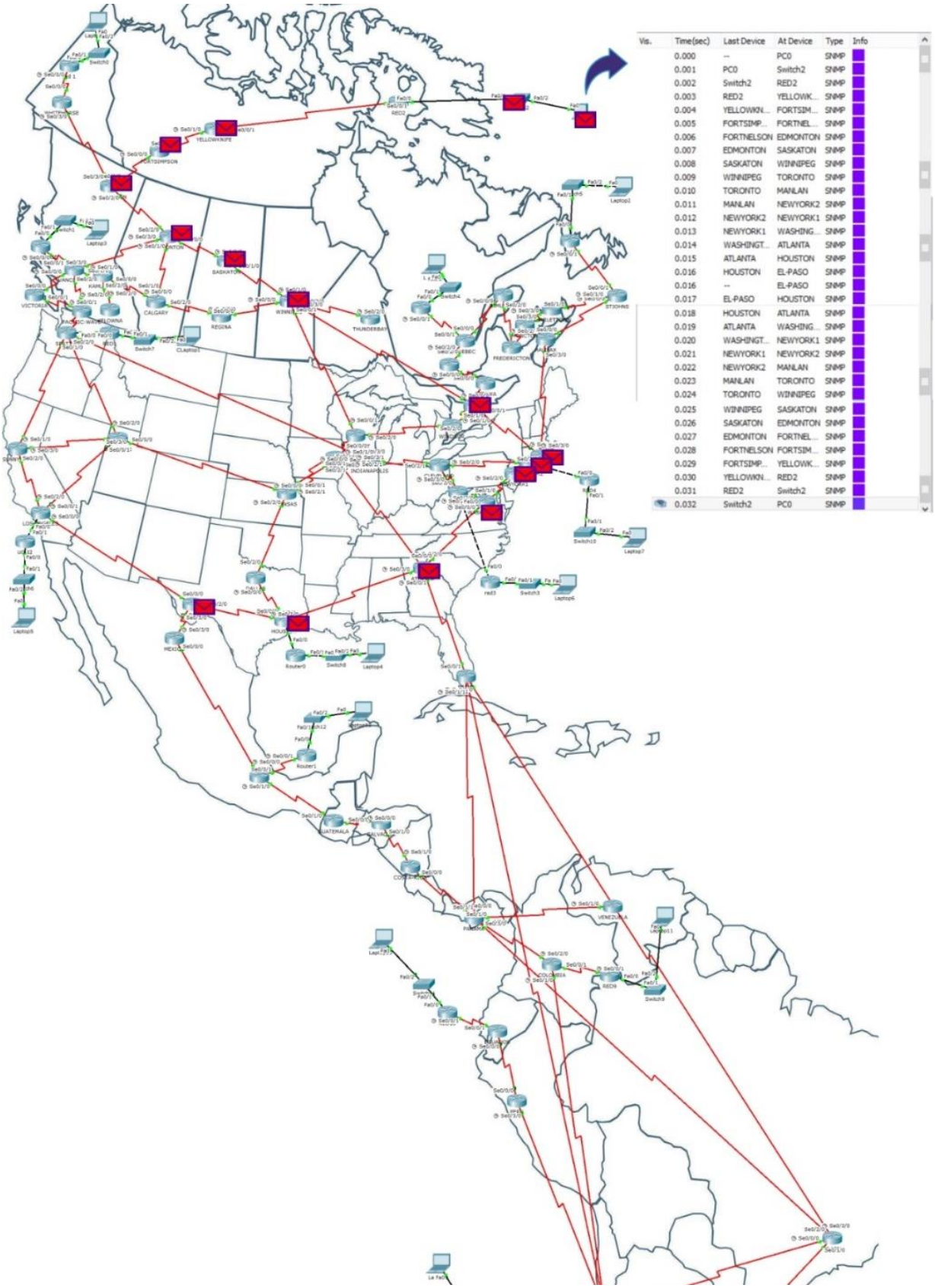
Tabla 5.2 Resumen de objetos monitoreados y configurados en PT

En la tabla 5.3 se muestran los resultados de tiempo en que un mensaje SNMP tarda en realizar la petición-respuesta, donde también se evaluan los recursos del sistema al ejecutar SNMP. Estos mensajes se enviaron dentro de las 3 RA y posteriormente se envió en la integración de estas 3 redes, los tiempos pueden variar dependiendo de que tan alejado se encuentre el dispositivo y la ruta que se elija para el envio del paquete.

Packet Tracer	Tiempo de envió del mensaje SNMP	Recursos del CPU	Recursos del memoria RAM
Red CANARIE			
Modo Simulación	1:50 min	25-27%	38% (1.5GB)
Modo Real	0.01 s	25-27%	38% (1.5GB)
Red Internet2			
Modo Simulación	1:41 min	25-27%	40% (1.6GB)
Modo Real	0.01s.	25-27%	40% (1.6GB)
Red CLARA			
Modo Simulación	2:10 min	25-26%	38% (1.5GB)
Modo Real	0.02s.	25-26%	38% (1.5GB)
Integración de las RA (de Internet2 a CANARIE)			
Modo Simulación	3:20 min	27-29%	45% (1.8GB)
Modo Real	0.02s.	27-29%	45% (1.8GB)
Integración de las RA (de Internet2 a CANARIE)			
Modo Simulación	2:57min	27-29%	45% (1.8GB)
Modo Real	0.02s	27-29%	45% (1.8GB)

Tabla 5.3 Evaluación de tiempos de envió del mensaje SNMP

Aunque la prueba de gestión se realizó dentro de CANARIE, en la figura 5.15 se muestra como se desplaza un paquete SNMP de CANARIE a Internet2, de la unidad gestora ubicada en Yellowknife al router El Paso. Se pudo apreciar que el simulador a veces presentaba dificultades al devolver objetos con instancias grandes, lo que provocaba que se generarán mensajes de error en la petición-respuesta.



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	SNMP	
	0.001	PC0	Switch2	SNMP	
	0.002	Switch2	RED2	SNMP	
	0.003	RED2	YELLOWK...	SNMP	
	0.004	YELLOWKN...	FORTSIM...	SNMP	
	0.005	FORTSIMP...	FORTNEL...	SNMP	
	0.006	FORTNELSON	EDMONTON	SNMP	
	0.007	EDMONTON	SASKATON	SNMP	
	0.008	SASKATON	WINNIPEG	SNMP	
	0.009	WINNIPEG	TORONTO	SNMP	
	0.010	TORONTO	MANLAN	SNMP	
	0.011	MANLAN	NEWYORK2	SNMP	
	0.012	NEWYORK2	NEWYORK1	SNMP	
	0.013	NEWYORK1	WASHING...	SNMP	
	0.014	WASHINGT...	ATLANTA	SNMP	
	0.015	ATLANTA	HOUSTON	SNMP	
	0.016	HOUSTON	EL-PASO	SNMP	
	0.016	--	EL-PASO	SNMP	
	0.017	EL-PASO	HOUSTON	SNMP	
	0.018	HOUSTON	ATLANTA	SNMP	
	0.019	ATLANTA	WASHING...	SNMP	
	0.020	WASHINGT...	NEWYORK1	SNMP	
	0.021	NEWYORK1	NEWYORK2	SNMP	
	0.022	NEWYORK2	MANLAN	SNMP	
	0.023	MANLAN	TORONTO	SNMP	
	0.024	TORONTO	WINNIPEG	SNMP	
	0.025	WINNIPEG	SASKATON	SNMP	
	0.026	SASKATON	EDMONTON	SNMP	
	0.027	EDMONTON	FORTNEL...	SNMP	
	0.028	FORTNELSON	FORTSIM...	SNMP	
	0.029	FORTSIMP...	YELLOWK...	SNMP	
	0.030	YELLOWKN...	RED2	SNMP	
	0.031	RED2	Switch2	SNMP	
	0.032	Switch2	PC0	SNMP	

Figura 5.15 Gestión via SNMP de I2 a CLARA

V.2 Resultados de emulación

V.2.1 Resultados de los protocolos de enrutamiento

A diferencia de la simulación que se realizó, gracias a Wireshark se pueden observar los paquetes que intercambian los routers vecinos antes de formar adyacencias (tanto OSPF como BGP), estos mensajes son los estados por los que pasa tanto OSPFv2 y BGP-4 hasta llegar a formar adyacencias. En la figura 5.16 se muestran los mensajes OSPF en el router de Chicago al formar adyacencia con Atlanta.

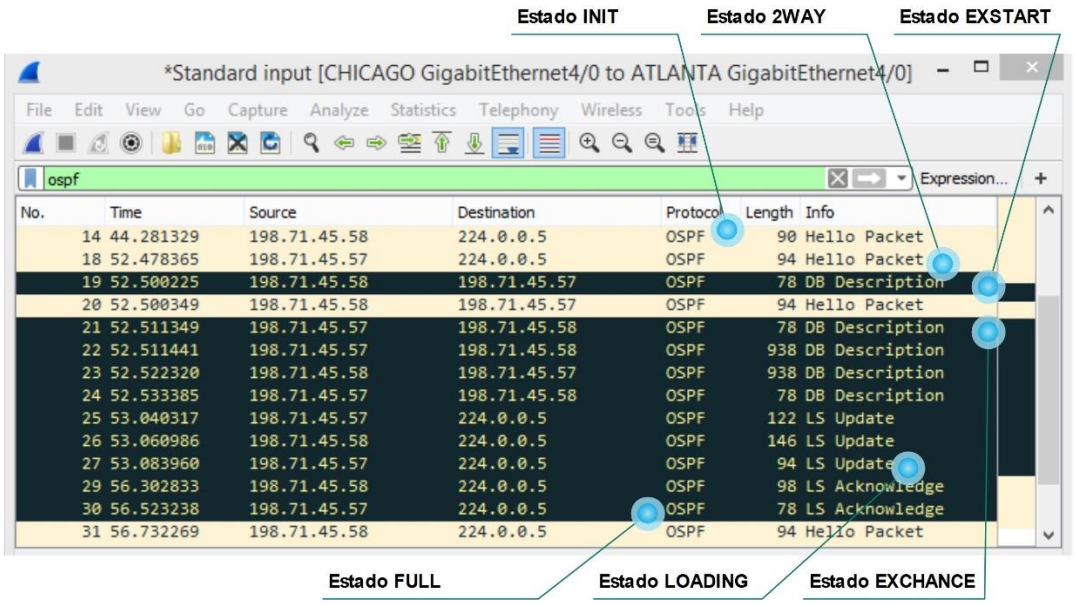


Figura 5.16 Paquetes OSPF para adyacencia del router Chicago con el router Atlanta

En la figura 5.17 se muestra los mensajes BGP que intercambia el router MAN-LAN ubicado en Internet2 al hacer adyacencia con el router Halifax ubicado en CANARIE.

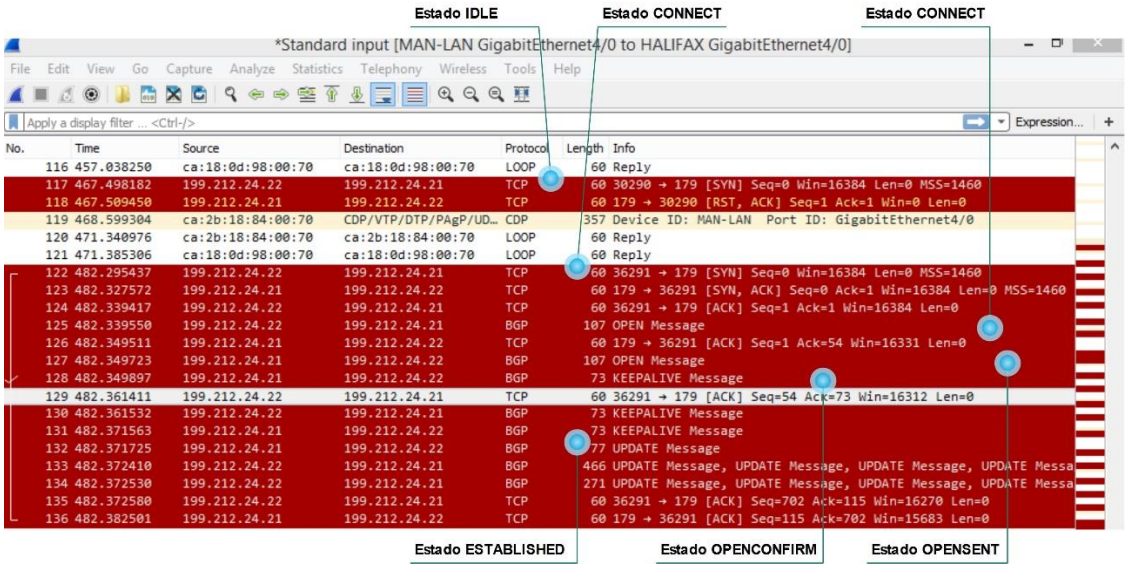


Figura 5.17 Paquetes BGP de acuerdo a los estados para formar adyacencia entre MANLAN y Halifax

Al igual que la simulación, en la emulación se comprobó la ejecución adecuada de los protocolos de enrutamiento, se comprobaron las tablas de enrutamiento de cada router para verificar si existen todas las rutas del AS al que pertenece el router. En las figura 5.18 se puede apreciar el despliegue de la tabla de enrutamiento del router de Chicago perteneciente a I2 donde sólo está ejecutando OSPF, como ya se había mencionado se hace para no tener fallas al ejecutar BGP.

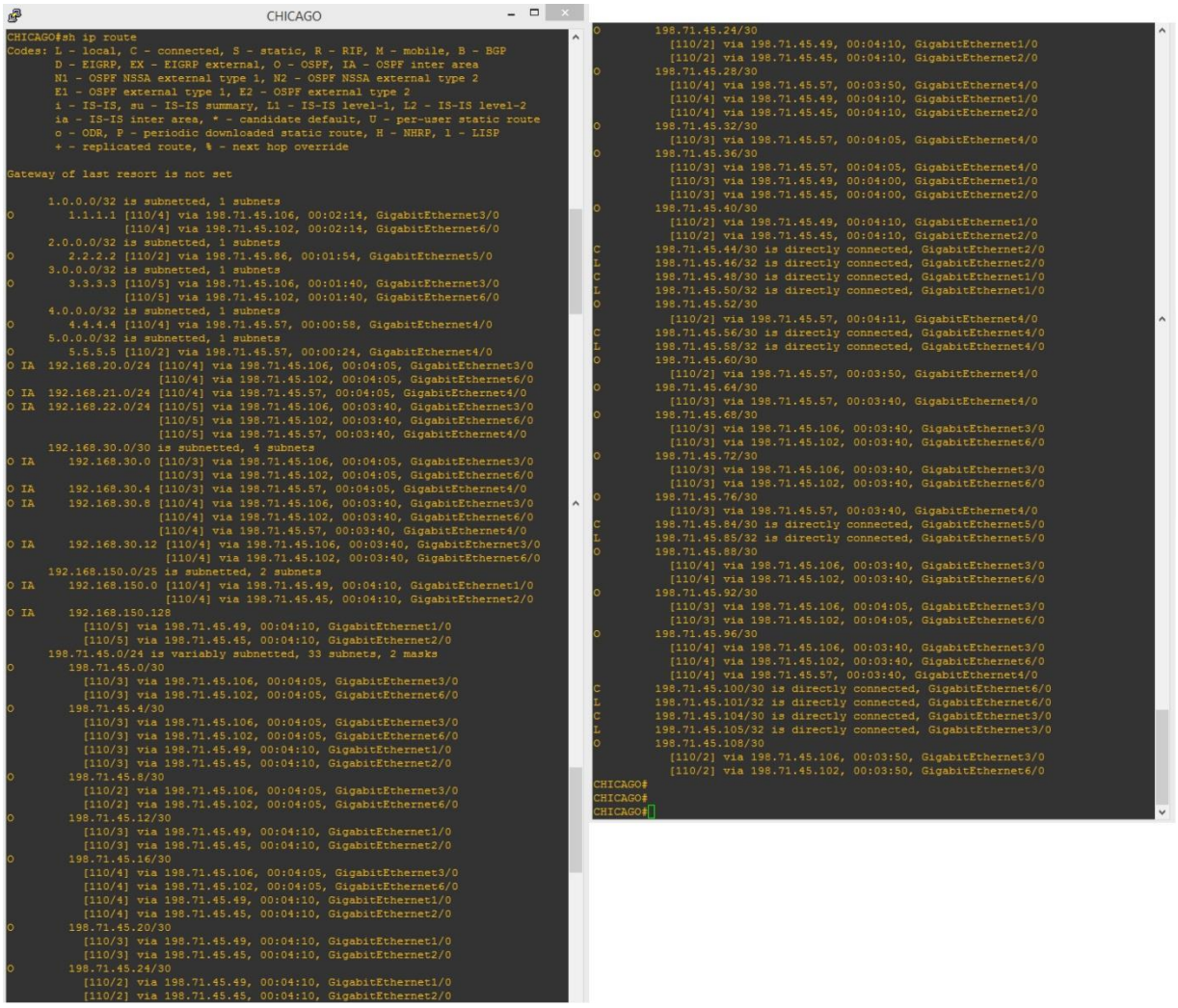


Figura 5.18 Despliegue de la tabla de enrutamiento del router Chicago sólo ejecutando OSPF (47 rutas)

Después de configurar BGP se comprobó la tabla de enrutamiento de todos los routers, donde deberían estar las rutas de las 3 RA, esto es posible en el emulador al permitir la configuración de IBGP. En la figura 5.4 se mostró la tabla de enrutamiento perteneciente al router Chicago donde este presentaba todas las rutas hacia las dos redes (CANARIE y CLARA), ahora se comprobó que cualquier router puede tener una tabla de enrutamiento similar para poder alcanzar cualquiera red de las 3 RA. En la figura 5.19 se muestra el contenido de la tabla de

enrutamiento de todas las rutas, similar al de la figura 5.4, pero ahora se muestra la tabla de enrutamiento del router de Panamá perteneciente a la red CLARA.

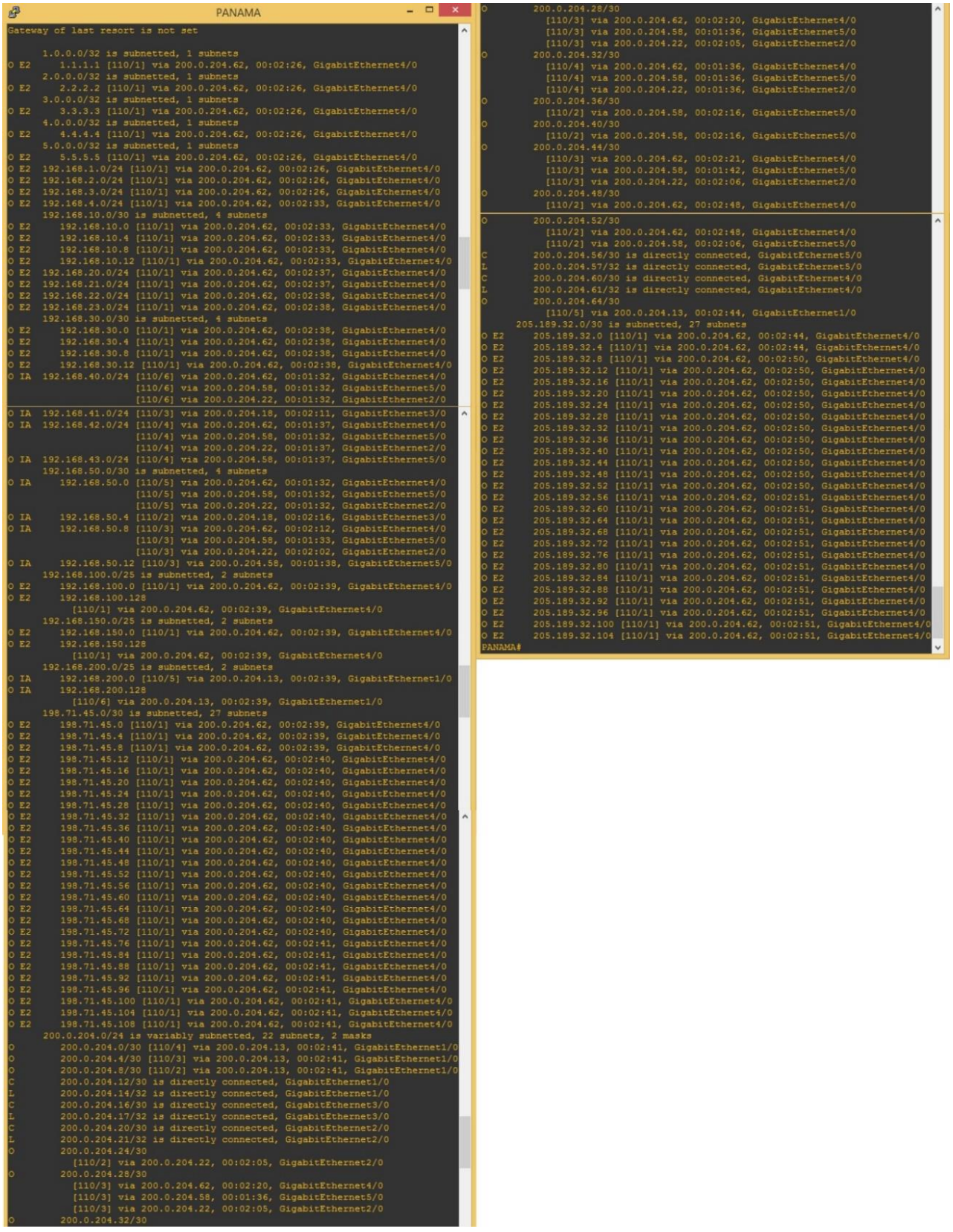


Figura 5.19 Contenido de la tabla de enrutamiento del router de Panamá con 111 rutas

V.2.2 Resultados de conectividad

Una vez que se comprobaron las tablas de enrutamiento de los routers se procedió a comprobar la conectividad de todo el backbone. Para comprobar la conectividad ejecutó el comando ping de la red conectada a Argentina a la red conectada a Yellowknife. En las figura 5.20 y 5.21 se muestran los mensajes ICMP que realizó cada VM.

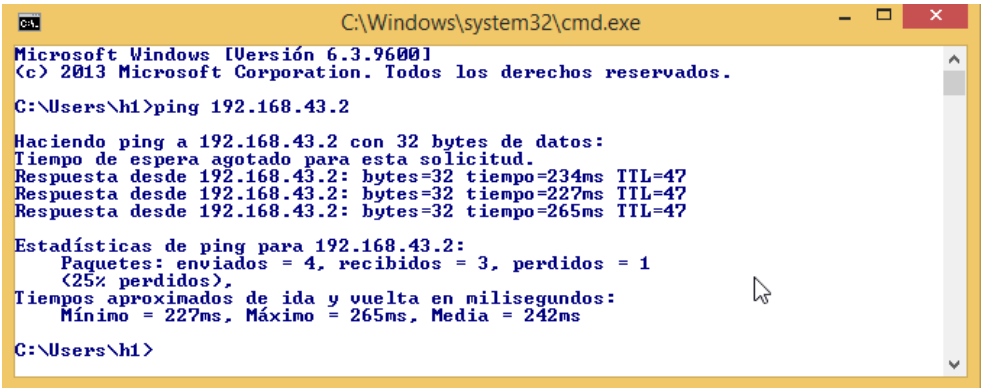


Figura 5.20 Ping de Yellowknife a Argentina

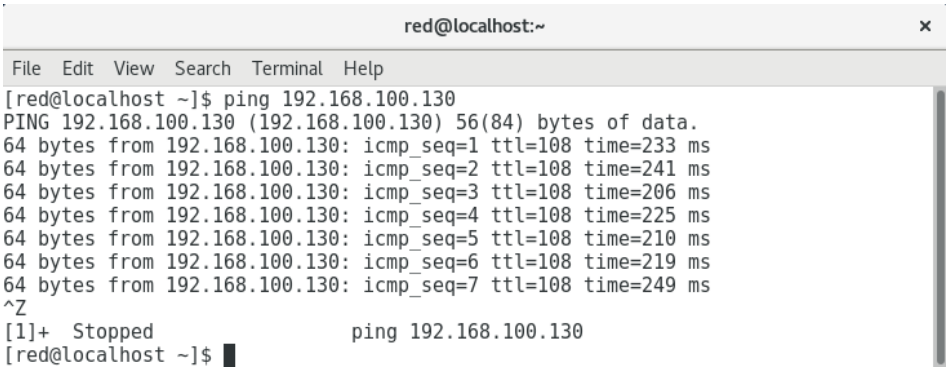


Figura 5.21 Ping de Argentina a Yellowknife

En la figura 5.22 se muestran la captura de los paquetes ICMP que se están intercambiando entre los hosts al realizar el comando ping.

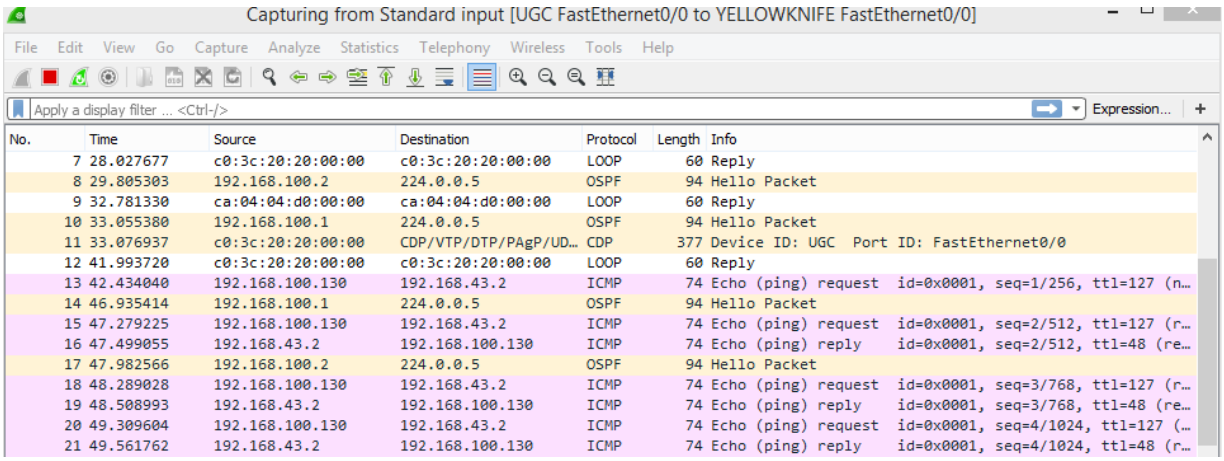


Figura 5.22 Captura de los paquetes ICMP al realizar ping

La diferencia entre el simulador con el emulador es que el emulador no cuenta con un modo de simulación en donde se puede apreciar como los routers mandan y procesan los paquetes que reciben de un origen a cierto destino, en el simulador también se puede apreciar como es la ruta entre los routers que sigue todo el paquete de su origen hasta su destino (automáticamente nos muestra el nombre del router por el que va pasando). Es por ello que para poder comprobar la ruta que va siguiendo el paquete hasta su destino se realizó un "traceroute" para poder ver la ruta que sigue el paquete. En la figura 5.23 se aprecia el "traceroute" de la ruta que sigue el paquete de la red conectada a Argentina hasta llegar a la red conectada a Yellowknife. Se puede apreciar que para alcanzar un host de la red CLARA al host de la red CANARIE (en este caso) se necesitaron 18 saltos. De acuerdo con las tablas IP 4.1, 4.2, 4.3, 4.4 y 4.5 la ruta que se sigue es la siguiente: Red4-CLARA, Argentina, Chile, Miami, Atlanta, Chicago, Indianápolis, Seattle, Pacific Wave, Vancouver, Kamloops, Calgary, Edmonton, Fort Nelson, Fort Simpson, Yellowknife, UG-C y el host windows8. Esto se tuvo que realizar para poder hacer una traza del paquete ya que GNS3 emula de forma real.

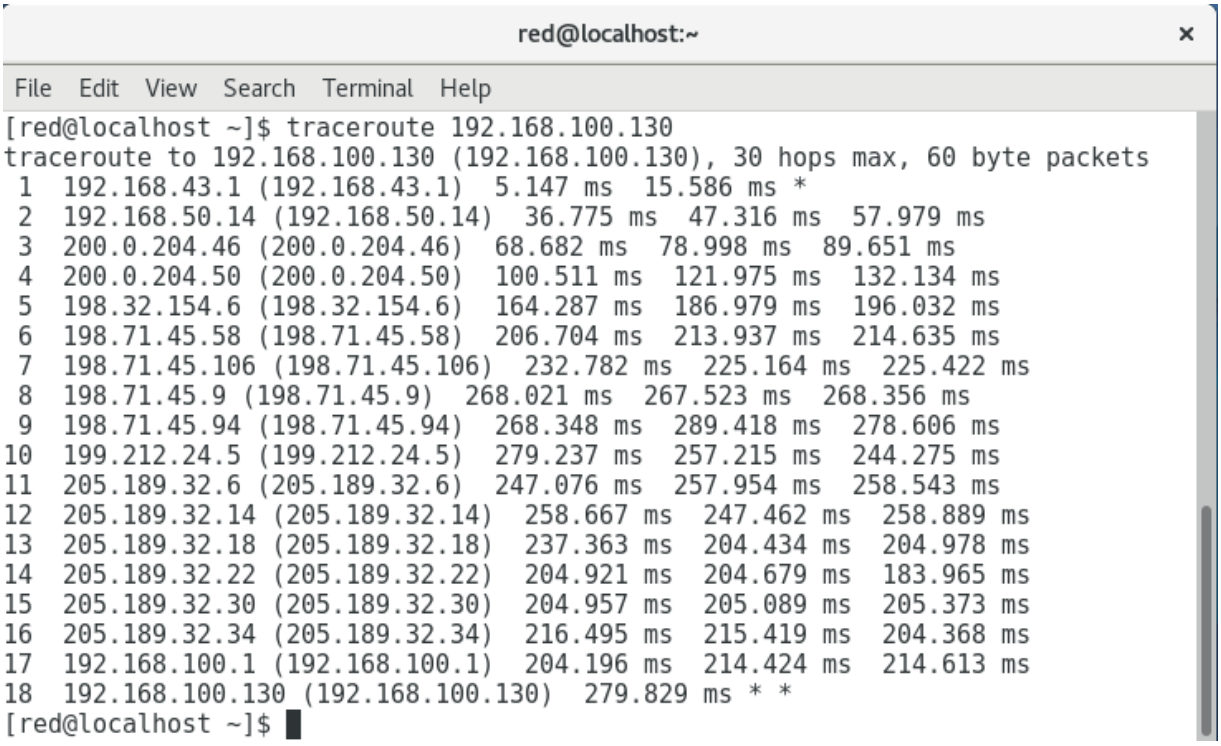
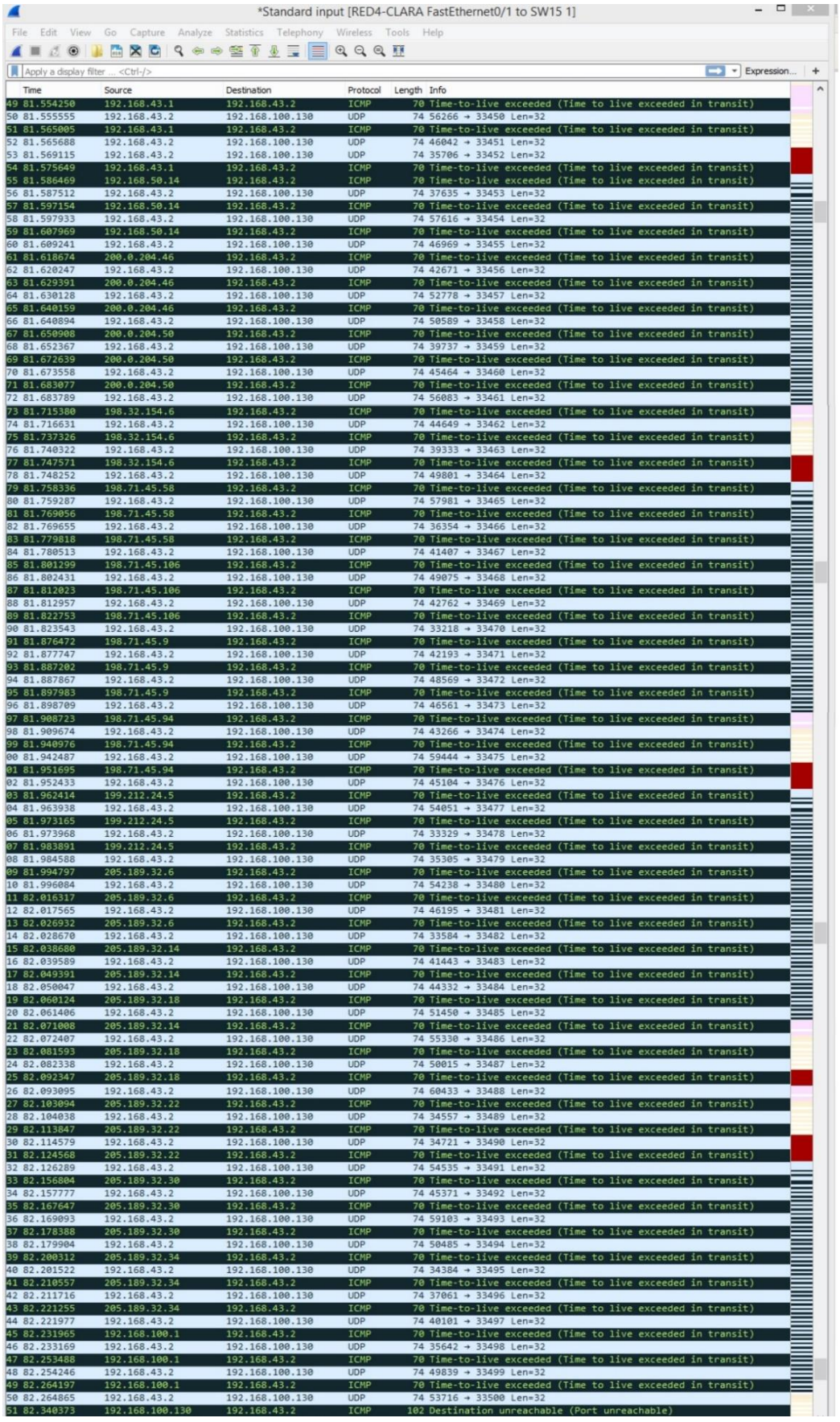


Figura 5.23 Traceroute de Argentina a Yellowknife

En la figura 5.24 se muestra cómo es que los routers le responden al host que generó el traceroute para poder trazar la ruta, estos paquetes ICMP fueron capturados por Wireshark.



	Time	Source	Destination	Protocol	Length	Info
49	81.554250	192.168.43.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	81.555555	192.168.43.2	192.168.100.130	UDP	74	56266 → 33450 Len=32
51	81.565005	192.168.43.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
52	81.565688	192.168.43.2	192.168.100.130	UDP	74	46042 → 33451 Len=32
53	81.569115	192.168.43.2	192.168.100.130	UDP	74	35706 → 33452 Len=32
54	81.575649	192.168.43.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
55	81.586469	192.168.50.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	81.587512	192.168.43.2	192.168.100.130	UDP	74	37635 → 33453 Len=32
57	81.597154	192.168.50.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
58	81.597933	192.168.43.2	192.168.100.130	UDP	74	57616 → 33454 Len=32
59	81.607969	192.168.50.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
60	81.609241	192.168.43.2	192.168.100.130	UDP	74	46969 → 33455 Len=32
61	81.618674	200.0.204.46	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	81.620247	192.168.43.2	192.168.100.130	UDP	74	42671 → 33456 Len=32
63	81.629391	200.0.204.46	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
64	81.630128	192.168.43.2	192.168.100.130	UDP	74	52778 → 33457 Len=32
65	81.640159	200.0.204.46	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
66	81.640894	192.168.43.2	192.168.100.130	UDP	74	50589 → 33458 Len=32
67	81.650908	200.0.204.50	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
68	81.652367	192.168.43.2	192.168.100.130	UDP	74	39737 → 33459 Len=32
69	81.672639	200.0.204.50	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70	81.673558	192.168.43.2	192.168.100.130	UDP	74	45464 → 33460 Len=32
71	81.683077	200.0.204.50	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
72	81.683789	192.168.43.2	192.168.100.130	UDP	74	56083 → 33461 Len=32
73	81.715380	198.32.154.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
74	81.716631	192.168.43.2	192.168.100.130	UDP	74	44649 → 33462 Len=32
75	81.737326	198.32.154.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
76	81.740322	192.168.43.2	192.168.100.130	UDP	74	39333 → 33463 Len=32
77	81.747571	198.32.154.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
78	81.748252	192.168.43.2	192.168.100.130	UDP	74	49801 → 33464 Len=32
79	81.758336	198.71.45.58	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
80	81.759287	192.168.43.2	192.168.100.130	UDP	74	57981 → 33465 Len=32
81	81.769056	198.71.45.58	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
82	81.769655	192.168.43.2	192.168.100.130	UDP	74	36354 → 33466 Len=32
83	81.779818	198.71.45.58	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
84	81.780513	192.168.43.2	192.168.100.130	UDP	74	41407 → 33467 Len=32
85	81.801299	198.71.45.106	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	81.802431	192.168.43.2	192.168.100.130	UDP	74	49075 → 33468 Len=32
87	81.812023	198.71.45.106	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	81.812957	192.168.43.2	192.168.100.130	UDP	74	42762 → 33469 Len=32
89	81.822753	198.71.45.106	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
90	81.823543	192.168.43.2	192.168.100.130	UDP	74	33218 → 33470 Len=32
91	81.876472	198.71.45.9	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
92	81.877747	192.168.43.2	192.168.100.130	UDP	74	42193 → 33471 Len=32
93	81.887202	198.71.45.9	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	81.887867	192.168.43.2	192.168.100.130	UDP	74	48569 → 33472 Len=32
95	81.897983	198.71.45.9	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
96	81.898709	192.168.43.2	192.168.100.130	UDP	74	46561 → 33473 Len=32
97	81.908723	198.71.45.94	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
98	81.909674	192.168.43.2	192.168.100.130	UDP	74	43266 → 33474 Len=32
99	81.940976	198.71.45.94	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
00	81.942487	192.168.43.2	192.168.100.130	UDP	74	59444 → 33475 Len=32
01	81.951695	198.71.45.94	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
02	81.952433	192.168.43.2	192.168.100.130	UDP	74	45104 → 33476 Len=32
03	81.962414	199.212.24.5	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
04	81.963938	192.168.43.2	192.168.100.130	UDP	74	54051 → 33477 Len=32
05	81.973165	199.212.24.5	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
06	81.973968	192.168.43.2	192.168.100.130	UDP	74	33329 → 33478 Len=32
07	81.983891	199.212.24.5	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
08	81.984588	192.168.43.2	192.168.100.130	UDP	74	35305 → 33479 Len=32
09	81.994797	205.189.32.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	81.996084	192.168.43.2	192.168.100.130	UDP	74	54238 → 33480 Len=32
11	82.016317	205.189.32.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	82.017565	192.168.43.2	192.168.100.130	UDP	74	46195 → 33481 Len=32
13	82.026932	205.189.32.6	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	82.028670	192.168.43.2	192.168.100.130	UDP	74	33584 → 33482 Len=32
15	82.038680	205.189.32.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	82.039589	192.168.43.2	192.168.100.130	UDP	74	41443 → 33483 Len=32
17	82.049391	205.189.32.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	82.050047	192.168.43.2	192.168.100.130	UDP	74	44332 → 33484 Len=32
19	82.060124	205.189.32.18	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
20	82.061406	192.168.43.2	192.168.100.130	UDP	74	51450 → 33485 Len=32
21	82.071008	205.189.32.14	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
22	82.072407	192.168.43.2	192.168.100.130	UDP	74	55330 → 33486 Len=32
23	82.081593	205.189.32.18	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24	82.082338	192.168.43.2	192.168.100.130	UDP	74	50015 → 33487 Len=32
25	82.092347	205.189.32.18	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	82.093095	192.168.43.2	192.168.100.130	UDP	74	60433 → 33488 Len=32
27	82.103094	205.189.32.22	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	82.104038	192.168.43.2	192.168.100.130	UDP	74	34557 → 33489 Len=32
29	82.113847	205.189.32.22	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	82.114579	192.168.43.2	192.168.100.130	UDP	74	34721 → 33490 Len=32
31	82.124568	205.189.32.22	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	82.126289	192.168.43.2	192.168.100.130	UDP	74	54535 → 33491 Len=32
33	82.156804	205.189.32.30	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	82.157777	192.168.43.2	192.168.100.130	UDP	74	45371 → 33492 Len=32
35	82.167647	205.189.32.30	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
36	82.169093	192.168.43.2	192.168.100.130	UDP	74	59103 → 33493 Len=32
37	82.178388	205.189.32.30	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
38	82.179904	192.168.43.2	192.168.100.130	UDP	74	50485 → 33494 Len=32
39	82.200312	205.189.32.34	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	82.201522	192.168.43.2	192.168.100.130	UDP	74	34384 → 33495 Len=32
41	82.210557	205.189.32.34	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
42	82.211716	192.168.43.2	192.168.100.130	UDP	74	37061 → 33496 Len=32
43	82.221255	205.189.32.34	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	82.221977	192.168.43.2	192.168.100.130	UDP	74	40101 → 33497 Len=32
45	82.231965	192.168.100.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	82.233169	192.168.43.2	192.168.100.130	UDP	74	35642 → 33498 Len=32
47	82.253488	192.168.100.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
48	82.254246	192.168.43.2	192.168.100.130	UDP	74	49839 → 33499 Len=32
49	82.264197	192.168.100.1	192.168.43.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	82.264865	192.168.43.2	192.168.100.130	UDP	74	53716 → 33500 Len=32
51	82.340373	192.168.100.130	192.168.43.2	ICMP	102	Destination unreachable (Port unreachable)

Figura 5.24 Paquetes que se generan al ejecutar un tracertroute

En la figura 5.25 se muestra de una forma gráfica como es que el paquete ICMP viajá a través de los routers mencionados por todo el backbone de la integración. A comparación de la limitación del simulador en cuanto a conectividad, el emulador presenta conectividad en todo el backbone integrado.

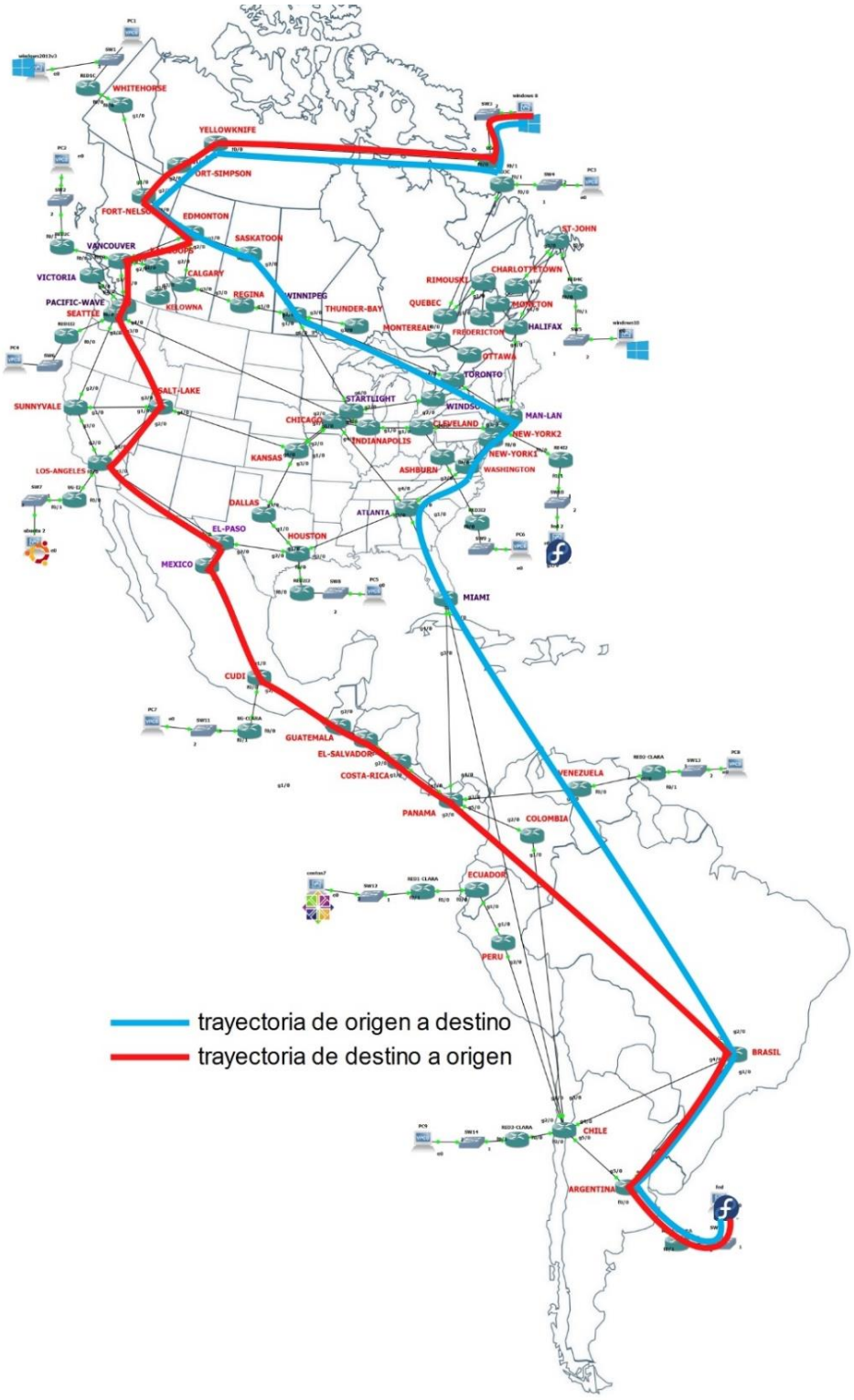


Figura 5.25 Trayectoria del mensaje ICMP de Argentina a Yellowknife

V.2.3 Resultados de prueba de gestión en emulación

Al igual que packet tracer, se configuró SNMP pero con la diferencia que se habilito el uso de las "traps", donde ahora el dispositivo puede mandar las "traps" por cualquier incidente o acción que pueda suceder en el dispositivo. En la figura 5.26 se muestra la conexión al dispositivo que se requiere gestionar, similar a la gestión en packet tracer, se ingresa la dirección IP y la contraseña del dispositivo y se elige la versión de SNMPv2 a utilizar, en este caso se está gestionando el router de Vancouver desde la unidad gestora ubicada en Yellowknife.

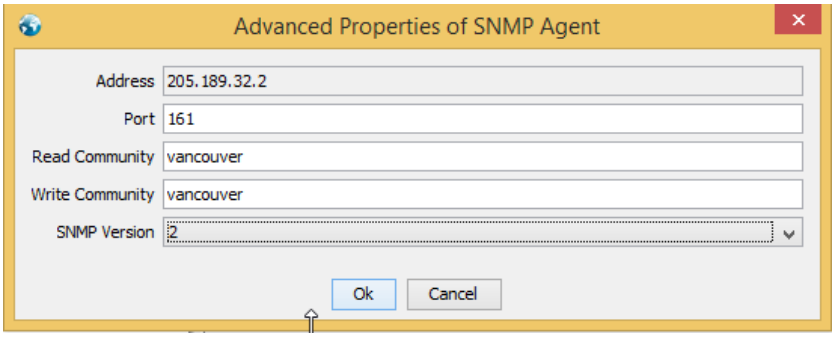


Figura 5.26 Conexión al router Vancouver via SNMPv2

La diferencia que se pudo notar es el poder utilizar la versión 3 de SNMP misma que en el simulador fue imposible ver, ya que en él no había diferencia entre la versión 2 con la 3. En la figura 5.27 se muestra cómo al utilizar la versión SNMPv3 (para este trabajo no se utilizó esta versión) el programa pide los campos de seguridad necesario para su utilización, esto es algo de lo que packet tracer carece.

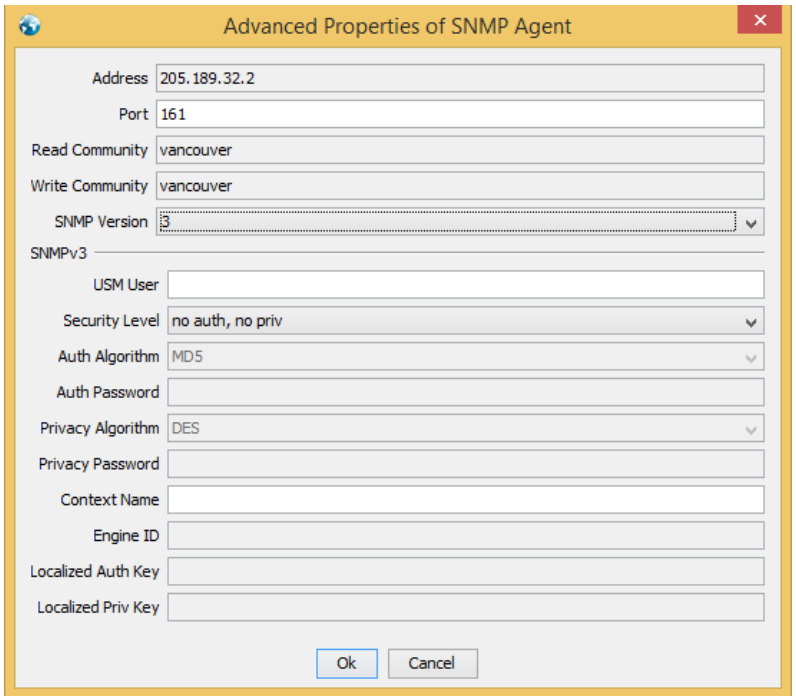


Figura 5.27 Campos necesarios para SNMPv3

En la figura 5.28 se muestra como se configuró el programa "Power SNMP" para poder comunicarse con el agente del router de Vancouver para poder recibir las traps. Se ingresó la dirección IP, la cadena de comunidad del router, version de SNMP asi como el puerto 162 para poder recibir las traps.

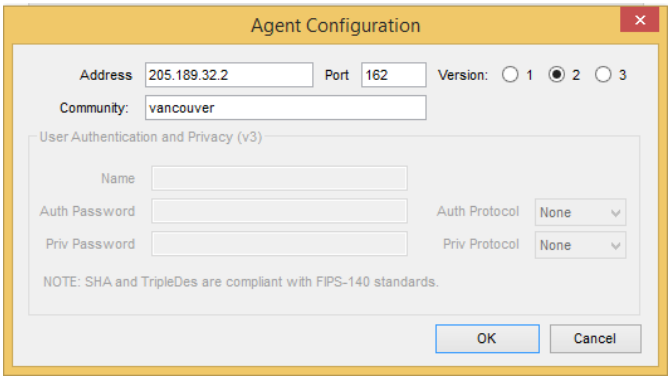


Figura 5.28 Configuración del agente del dispositivo para recolectar las "traps" con power SNMP

Otra de las cosas más notables es la gran cantidad de configuración que se puede realizar con SNMP en los routers que presentan una IOS real (en este caso del router cisco 7200), en comparación con el IOS que está presente en packet tracer. En la figura 5.29 se muestra el despliegue de todos los elemento de SNMP que se pueden configurar.

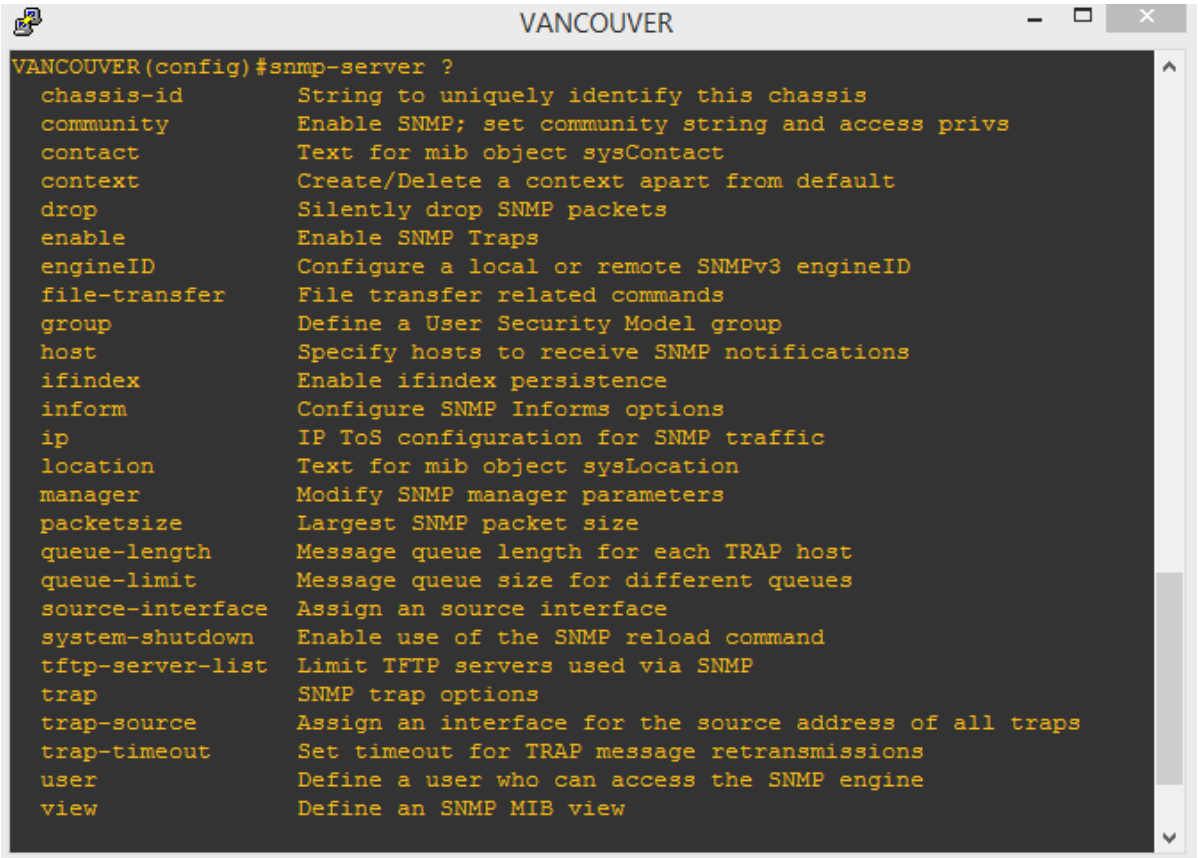


Figura 5.29 Elemento completos de SNMP que se pueden configurar en un router en GNS3

Además se cuentan con otras opciones de SNMP que se pueden configurar como lo muestra la figura 5.30 (todas estas opciones no se ocuparon sólo son para fines demostrativos sobre limitaciones entre simulador y emulador en cuestión del protocolo).

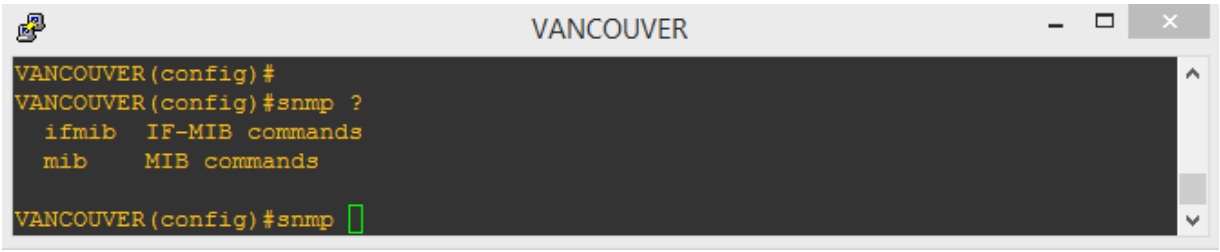


Figura 5.30 Otras opciones de configuración de SNMP en GNS3

Las 10 figuras siguientes muestran el resultado de gestionar los objetos seleccionados en la tabla 4.6. En la figura 5.31 se muestra la gestión del objeto "name" donde se despliega el nombre del router gestionado, en este caso el router Vancouver. También se muestra una breve descripción de los elementos de MIB browser, siendo un poco similar al MIB browser del simulador.

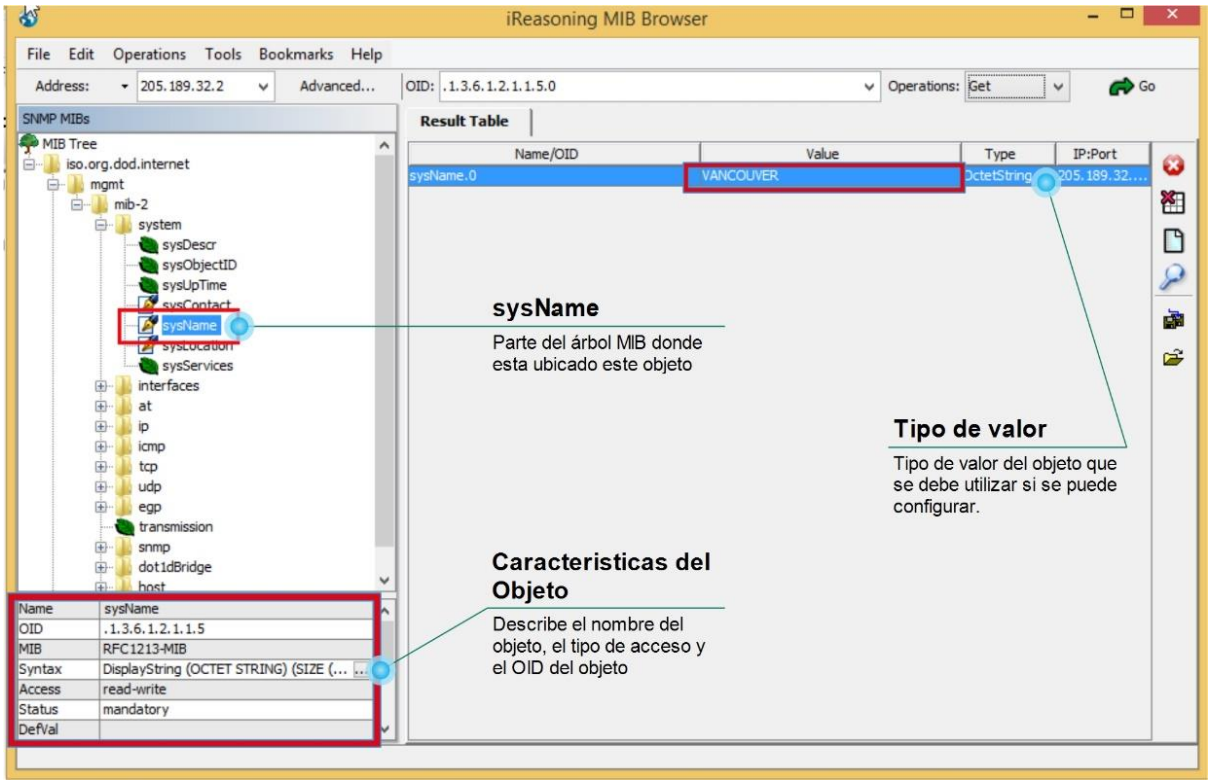


Figura 5.31 Gestión de objeto "Name" usando "Mib Browser" en GNS3

La figura 5.32 muestra el objeto "atNetAddr", donde se muestran las direcciones IP de las interfaces configuradas en el router Vancouver.

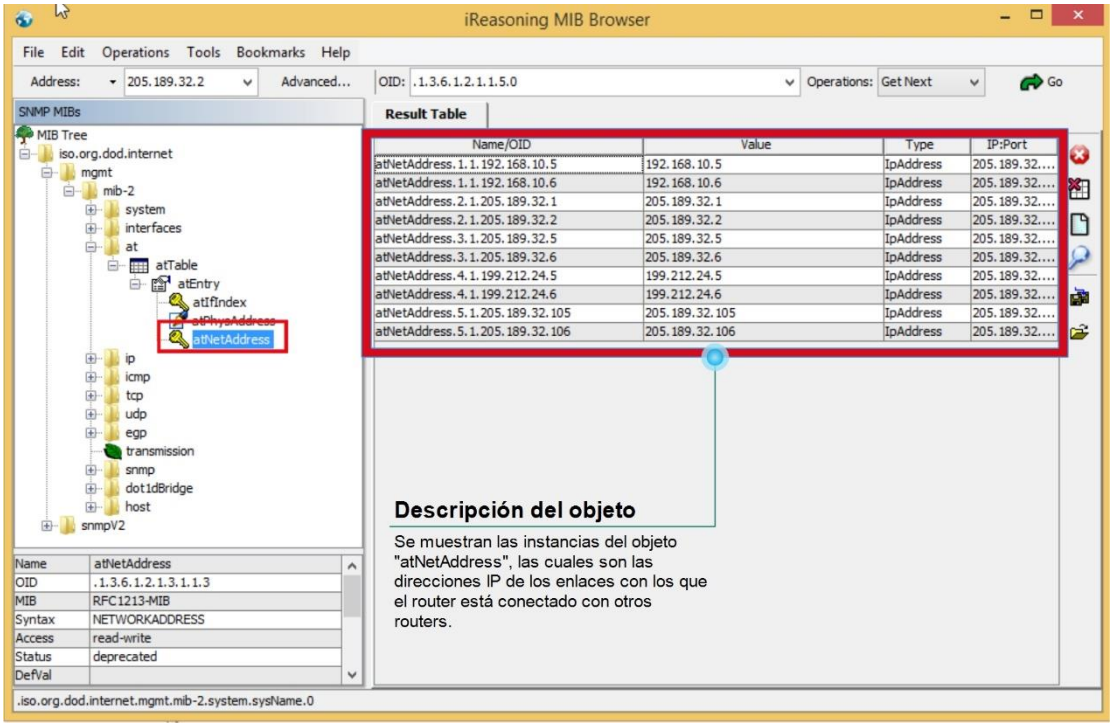


Figura 5.32 Gestión del objeto "atNetAddress" usando "Mib Browser" en GNS3

En la figura 5.33 se muestra el monitoreo del objeto "ifDescription", en comparación con el simulador el emulador muestra las interfaces GigabitEthernet. La figura 5.34 muestra el objeto "IfAdminStatus", donde se muestra el estatus de las interfaces GigabitEthernet.

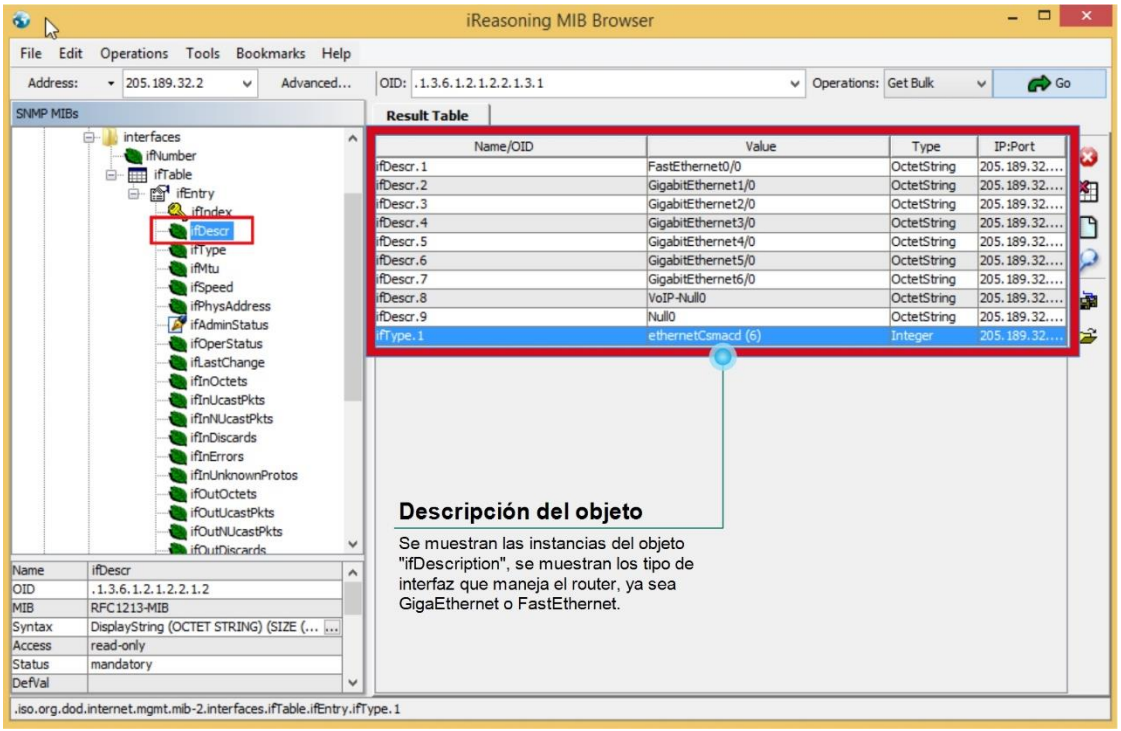


Figura 5.33 Gestión del objeto "ifDescription" usando "Mib Browser" en GNS3

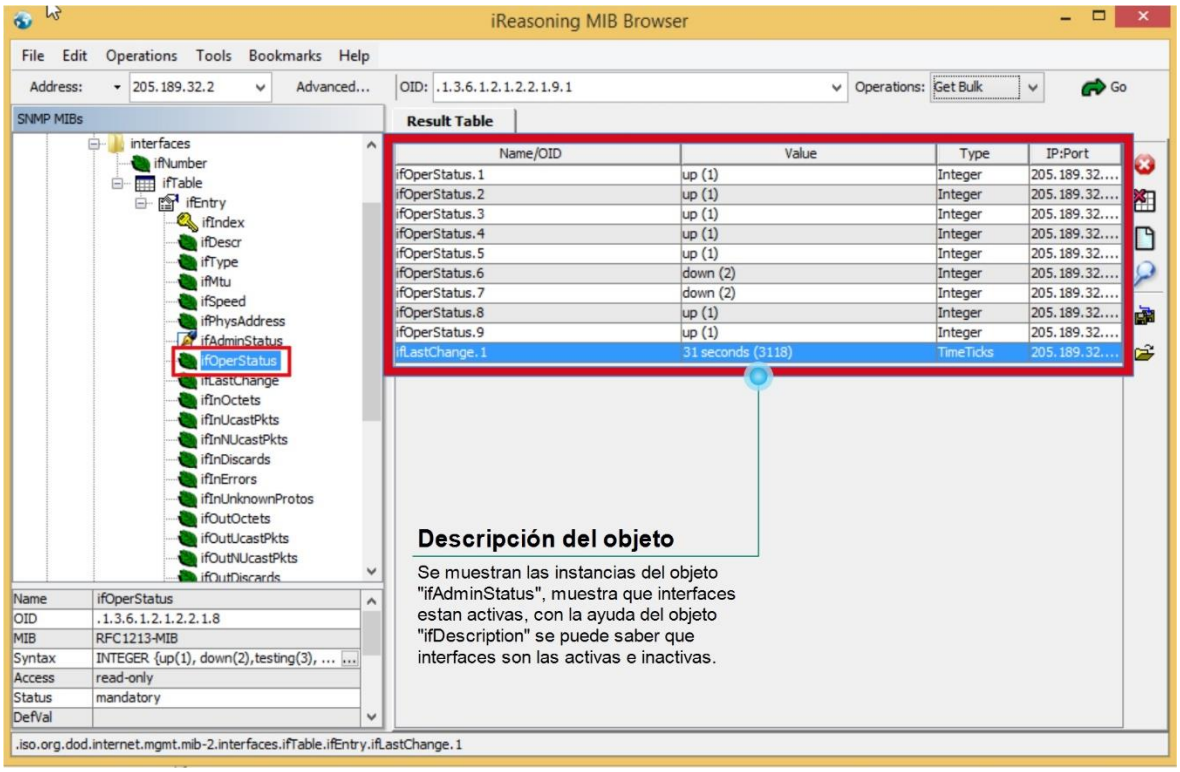


Figura 5.34 Gestión del objeto "ifAdminStatus" usando "Mib Browser" en GNS3

La figura 5.35 muestra el objeto "ipNetToMediaTypes", este objeto no se pudo obtener con el simulador, se muestra el tipo de mapeo de cada interfaz.

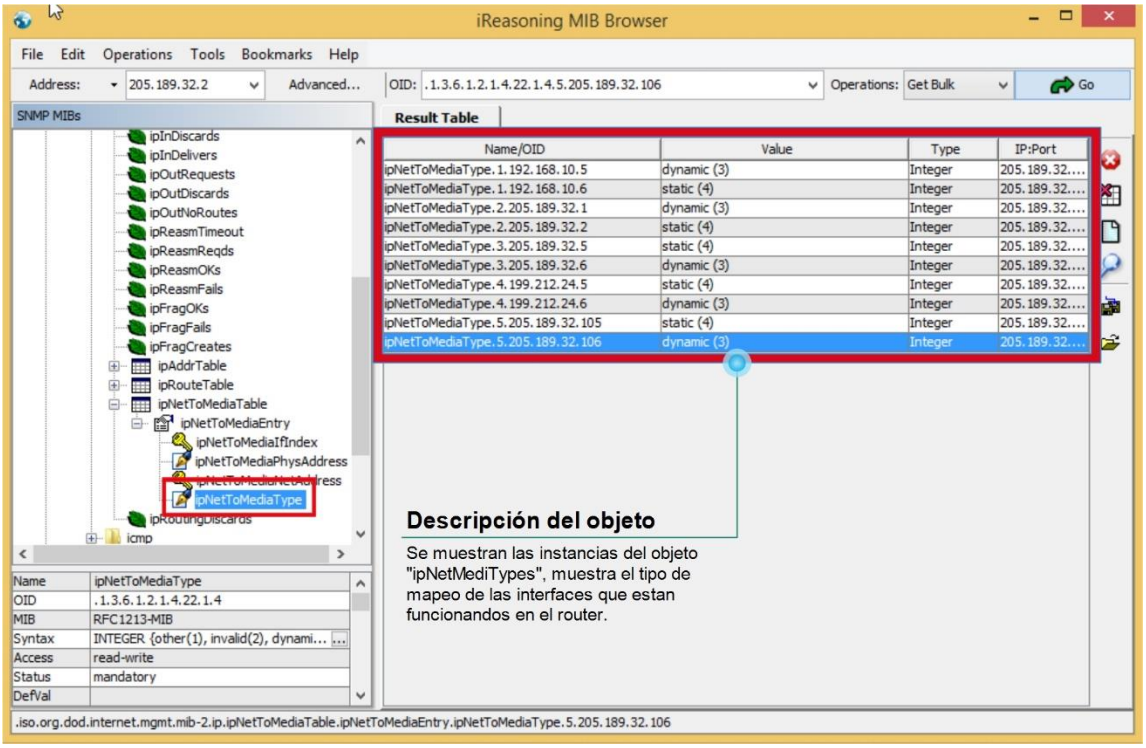


Figura 5.35 Gestión del objeto "ipNetMediaType" usando "Mib Browser" en GNS3

Para el monitoreo del objeto "ipRouteNextHop" el emulador no mostró datos disponibles, en la figura 5.36 se muestra el mensaje que arroja el programa. El simulador si mostró instancias de este objeto.

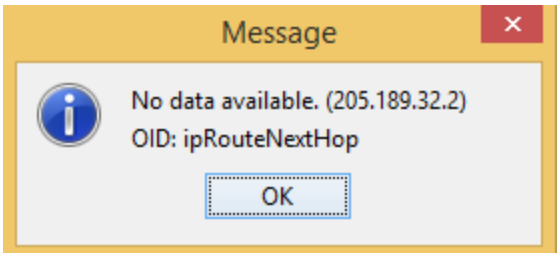


Figura 5.36 Datos no disponibles para el objeto ipRouteNextHop

En las 4 figuras siguientes el programa "MIB browser" ya no puede mostrar en qué parte del árbol MIB se encuentan esos objetos, a pesar de ello no se limita en poder encontrarlos ya que se puede teclear el OID con cual el agente responderá y el MIB browser, podrá mostrar esas instancias del objeto ingresado. En la figura 5.37 se muestra el objeto "ospfAdminStat" el cual muestra que el protocolo OSPF está activo, en este caso el número 1 indica "enable".

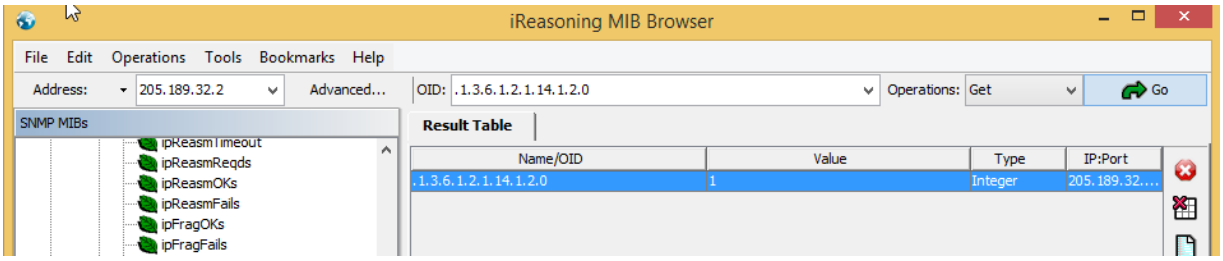


Figura 5.37 Gestión del objeto "ospfAdminStat" usando "Mib Browser" en GNS3

La figura 5.38 muestra el objeto "ospfNbrip", el cual muestra la direccio IP de los vecinos OSPF del router Vancouver.

Figura 5.38 Gestión del objeto "ospfNbrip" usando "Mib Browser" en GNS3

La figura 5.39 muestra las instancias correspondientes al objeto "bgp" donde se puede apreciar el ASN, direcciones IP de sus "peers", el ASN al que se está conectando, estado y sesión. La figura 5.40 muestra el objeto "cisco image", es importante porque nos da entender que se puede ingresar a los objetos MIB de un dispositivo de alguna compañía (Cisco en este caso).

Figura 5.39 Gestión del objeto "bgp" usando "Mib Browser" en GNS3

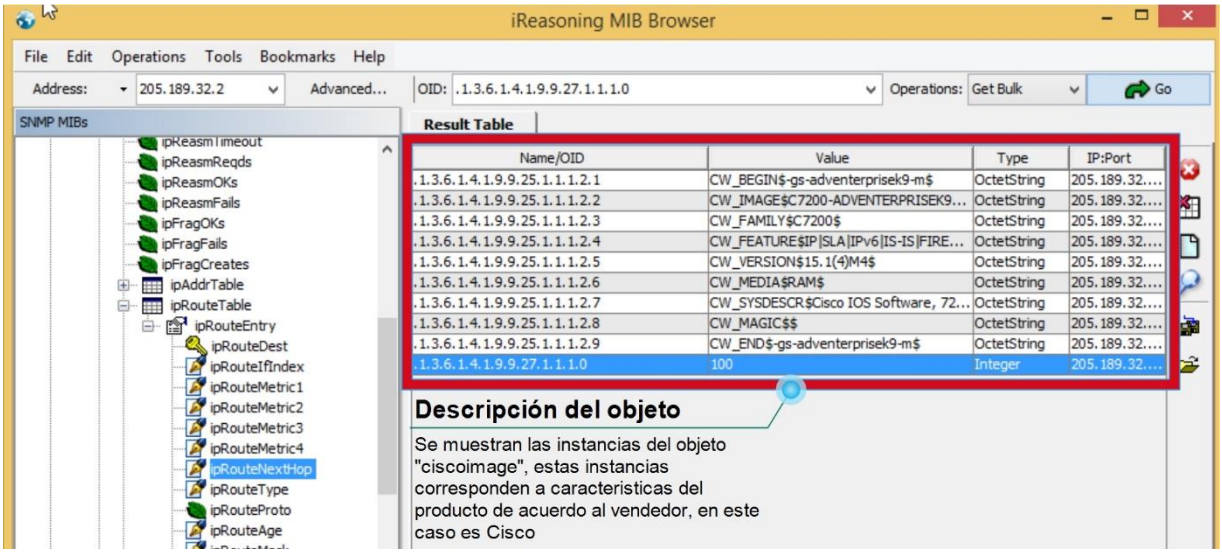


Figura 5.40 Gestión del objeto "ciscoimage" usando "Mib Browser" en GNS3

En la figura 5.41 se muestra la captura de los paquetes SNMP de petición y respuesta de los 10 objetos que se planearon (de acuerdo con la tabla 4.6), en los recuadros se aprecian los OIDs de algunos objetos que se gestionaron, asi como las operaciones que utilizó SNMP para devolver las instancias de los objetos, las operaciones dependen del número de instancias que contenga un objeto. Las operaciones que se pueden apreciar son "get, get-next, get- bulk y get-response".

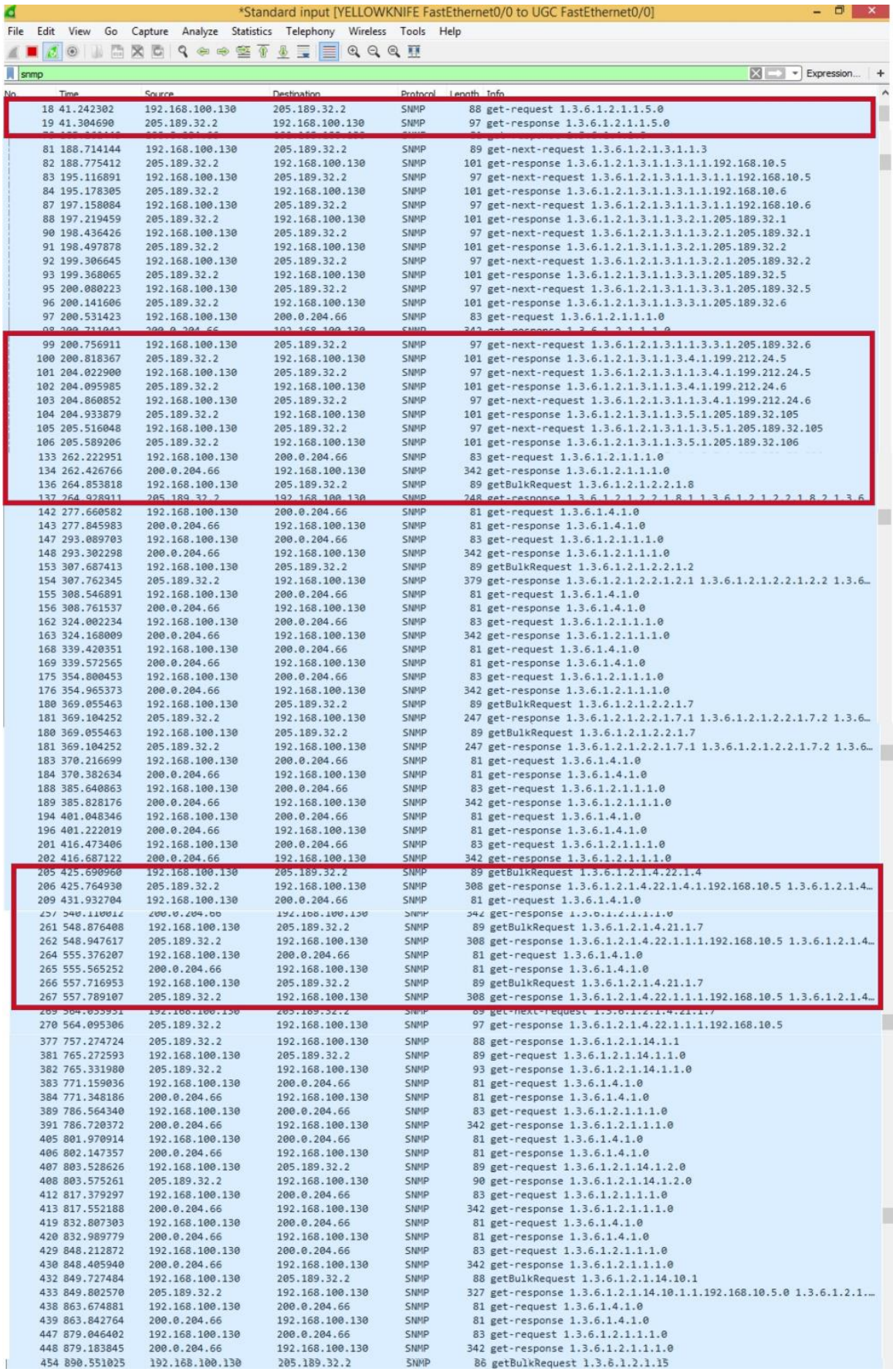


Figura 5.41 Captura de los paquetes SNMP de los objetos gestionados.

Las figuras 5.42 y 5.43 muestran la operación "set" que se utilizó con los objetos "name, ifadmintype", debido a que estos sólo se pudieron configurar, a pesar de que otros objetos son del tipo "read-write"el programa no dejó configurarlos.

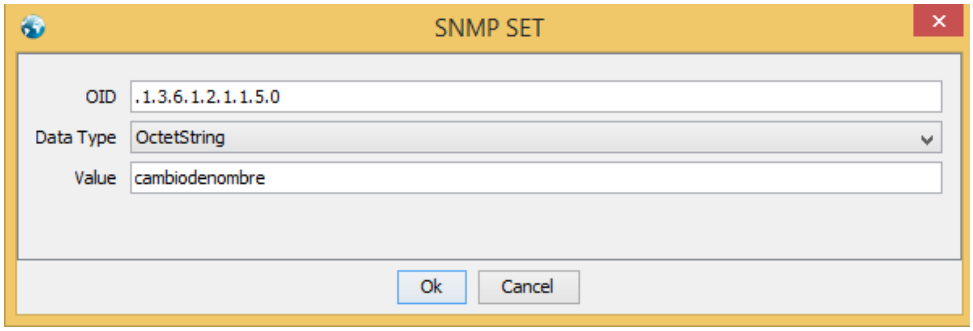


Figura 5.42 Operación "set" para el objeto "name"

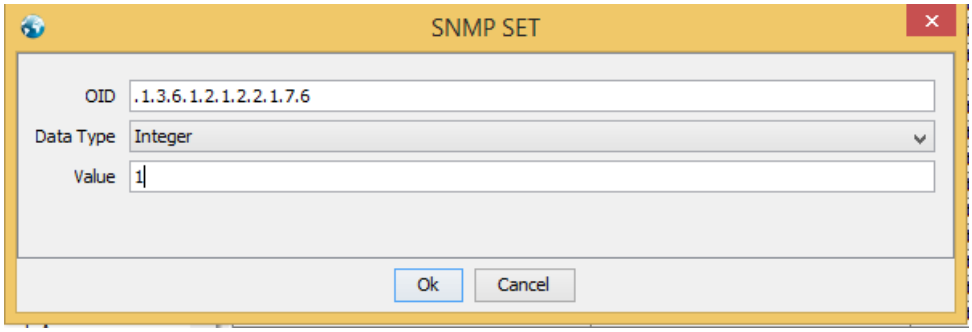


Figura 5.43 Operación "set" para el objeto "ifAdminStat"

Una vez hecho la operación *"set"* Mib browser envió un mensaje como se muestra en la figura 5.44, este mensaje es otra de las diferencias con el simulador ya que él no muestra mensaje alguno cuando se ejecuta la operación "set".

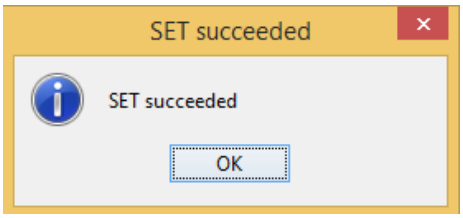


Figura 5.44 Mensaje de éxito en la operación set

Para los objetos "name" y "ifAdminStat" se pudo corroborar su configuración dentro del router, en la figura 5.45 se muestra cómo es que las interfaces GbitE 5/0 y GbitE 6/0 se activaron y desactivaron, en el recuadro se puede apreciar que estas acciones fueron hechas vía SNMP y la dirección IP de la unidad gestora. Cabe mencionar que para el cambio de nombre no arroja ningún aviso de configuración vía SNMP, sólo se hace el cambio y se ve reflejado cuando se ingresa al router.

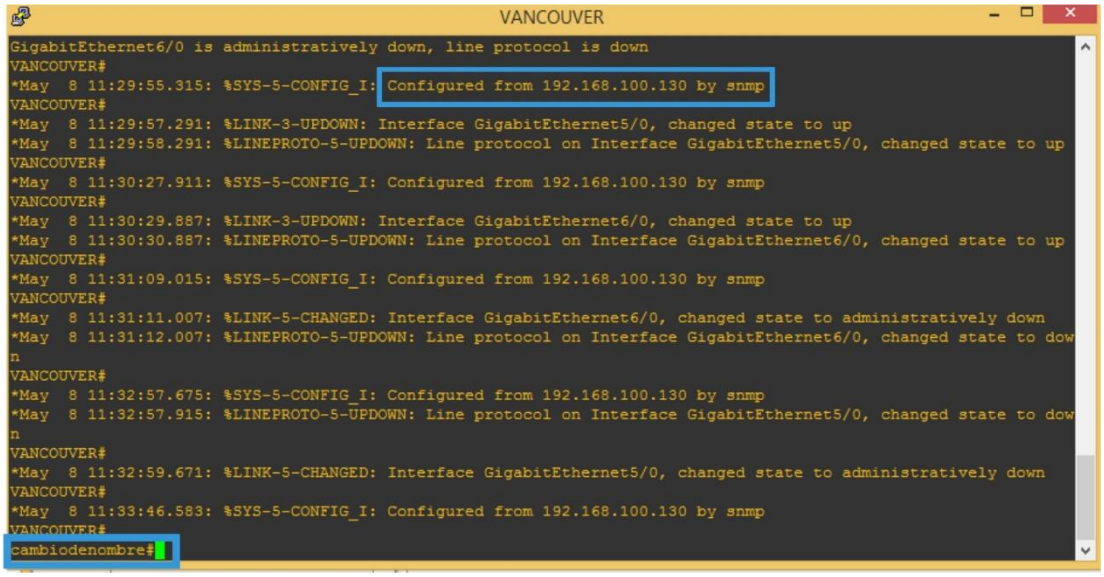


Figura 5.45 Resultado de la configuración de los objetos "name" y "ifAdminStat" en el router Vancover

El OID "ipNetofMediaTypes" de acuerdo al "MIB Browser" se puede configurar con 4 valores enteros diferentes, estos son; 1-other, 2-invalid, 3-dynamic y 4-static. De estos posibles cambios, MIB browser sólo permitió hacer el cambio con el número entero 2. En la figura 5.48 se muestra el resultado de manipular este objeto en donde se invalidaron 3 instancias del objeto. Si se compará con la figura 5.35 algunas instancias ya no se encuentran, al hacer esta manipulación en el router no da algún aviso de lo ocurrido sólo el programa MIB browser.

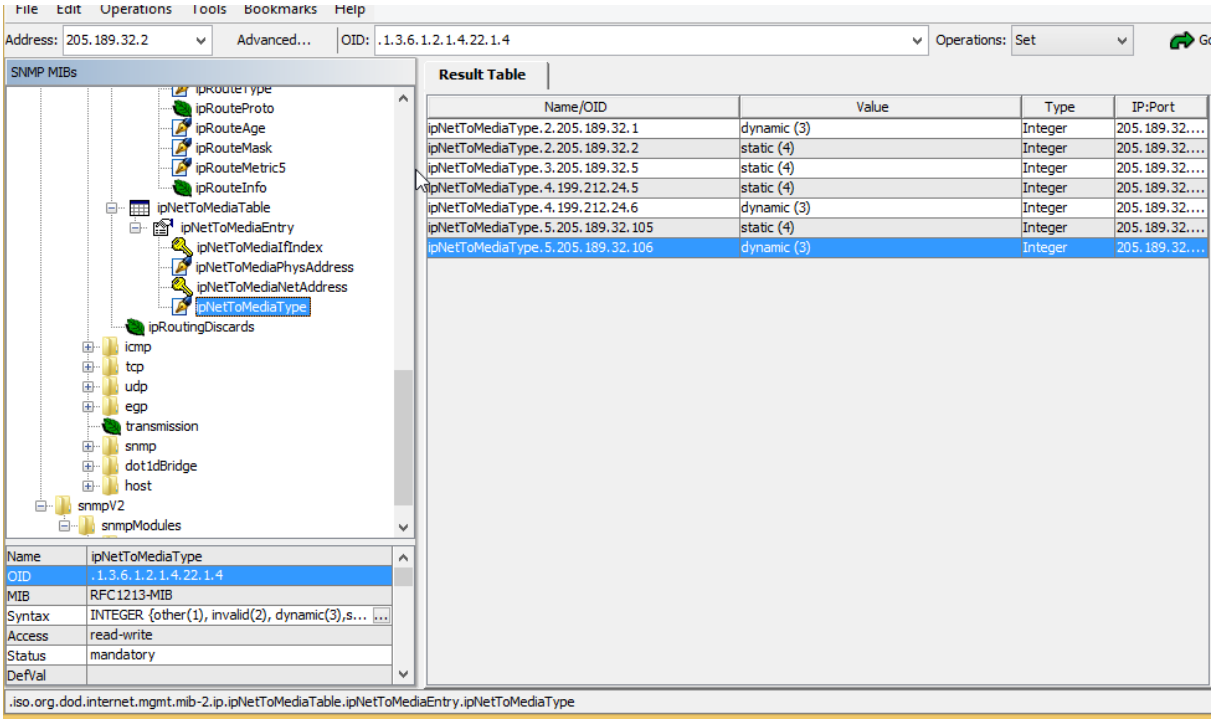


Figura 5.46 Configuración de instancia del objeto "ipNetofMediaTypes"

El OID "ospfAdminStat" se trató de configurar pero esto no fue posible, como puede verse con el mensaje de error que arrojaba como el que se muestra en la figura 5.47. En contraste, el simulador si dejo configurar este objeto.

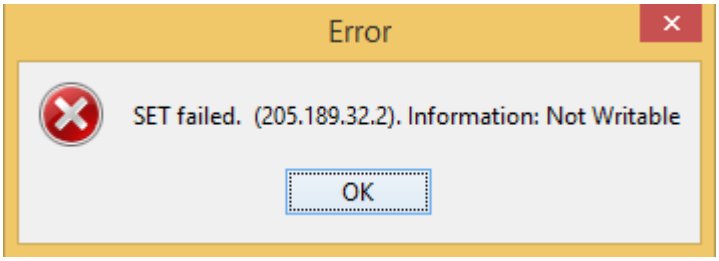


Figura 5.47 Mensaje de error al tratar de configurar el objeto "ospfAdminStat"

En la tabla 5.4 se muestra el resumen de los objetos que se pudieron monitorear y algunos que se pudieron configurar, a pesar de que se utilizó un software en una VM donde se creía que tendría más posibilidades de monitoreo y configuración, no se encontraron instancias de objeto como es el caso del objeto "ifNextHop", asi como la poca configuración de los objetos del tipo *"read-write"*.

Objeto	Monitoreado	Configurado
Name	✓	✓
atNetAddres	✓	✗
ifDescription	✓	✗
ifAdminType	✓	✓
ipNetofMediaTypes	✓	✓
ipRouteNextHop	✗	✗
ospfAdminStat	✓	✗
ospfNbrip	✓	✗
Bgp	✓	✗
CiscoImageString	✓	✗

Tabla 5.4 Resumen de objetos gestionados y manipulados en PT

En la figura 5.48 se muestra la captura de los mensajes correspondientes a la operación *"set"* y algunas traps snmpv2 que se envíaron debido al cambio que se hizo con los objetos configurados.

771	1575.629899	192.168.100.130	205.189.32.2	SNMP	91 set-request 1.3.6.1.2.1.2.2.1.7.7
772	1575.907112	205.189.32.2	192.168.100.130	SNMP	91 get-response 1.3.6.1.2.1.2.2.1.7.7
773	1576.270522	205.189.32.105	192.168.100.130	SNMP	179 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
774	1576.625034	205.189.32.105	192.168.100.130	SNMP	214 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.…
776	1578.912374	205.189.32.105	192.168.100.130	SNMP	209 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
777	1579.180808	205.189.32.105	192.168.100.130	SNMP	281 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
781	1589.735507	192.168.100.130	205.189.32.2	SNMP	89 getBulkRequest 1.3.6.1.2.1.2.2.1.7
782	1589.805650	205.189.32.2	192.168.100.130	SNMP	247 get-response 1.3.6.1.2.1.2.2.1.7.1 1.3.6.1.2.1.2.2.1.7.2 1.3.6…
794	1634.974477	192.168.100.130	205.189.32.2	SNMP	91 set-request 1.3.6.1.2.1.2.2.1.7.7
795	1635.162845	205.189.32.2	192.168.100.130	SNMP	91 get-response 1.3.6.1.2.1.2.2.1.7.7
796	1635.485148	205.189.32.105	192.168.100.130	SNMP	179 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
798	1638.342126	205.189.32.105	192.168.100.130	SNMP	209 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
800	1639.792105	205.189.32.105	192.168.100.130	SNMP	223 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.…
802	1643.945163	192.168.100.130	205.189.32.2	SNMP	91 set-request 1.3.6.1.2.1.2.2.1.7.8
803	1644.013176	205.189.32.2	192.168.100.130	SNMP	91 get-response 1.3.6.1.2.1.2.2.1.7.8
853	1790.210557	192.168.100.130	205.189.32.2	SNMP	91 set-request 1.3.6.1.2.1.2.2.1.7.6
854	1790.379281	205.189.32.2	192.168.100.130	SNMP	91 get-response 1.3.6.1.2.1.2.2.1.7.6
855	1790.734022	205.189.32.105	192.168.100.130	SNMP	179 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
856	1791.056148	205.189.32.105	192.168.100.130	SNMP	223 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.2.…
866	1816.625694	192.168.100.130	205.189.32.2	SNMP	88 get-request 1.3.6.1.2.1.1.5.0
867	1816.687938	205.189.32.2	192.168.100.130	SNMP	97 get-response 1.3.6.1.2.1.1.5.0
880	1859.126134	192.168.100.130	205.189.32.2	SNMP	102 set-request 1.3.6.1.2.1.1.5.0
881	1859.194275	205.189.32.2	192.168.100.130	SNMP	102 get-response 1.3.6.1.2.1.1.5.0
882	1859.559642	205.189.32.105	192.168.100.130	SNMP	179 snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.…
903	1939.589525	192.168.100.130	205.189.32.2	SNMP	89 get-request 1.3.6.1.2.1.3.1.1.3
904	1939.643068	205.189.32.2	192.168.100.130	SNMP	89 get-response 1.3.6.1.2.1.3.1.1.3

Figura 5.48 Captura de los mensajes SNMP de la operación "set" y "traps" generadas

Con el programa "power SNMP" se pudieron observar las "traps" que el agente está anunciando cuando ocurre alguna interrupción o suceso inesperado dentro del dispositivo. En la figura 5.49 se aprecian las traps que se generaron al hacer la configuración de los objetos antes mencionados, estas "traps" arrojan diferentes OIDs cuya significado se explicará más adelante.

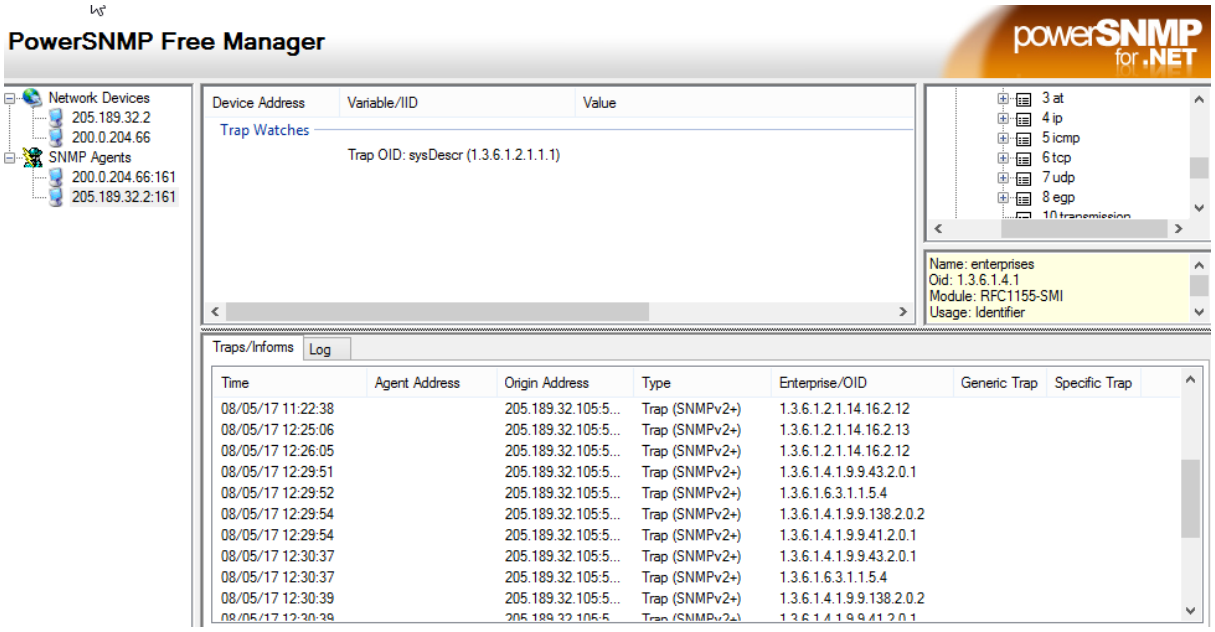


Figura 5.49 Captura de Traps generadas por interrupción o algún suceso

Para apreciar la ejecución de las "traps", se apagó casi todo el backbone de la integración y sólo se dejó el router Vancouver y algunos routers que conectan a la unidad gestora. En la imagen 5.50 se muestran las "traps" generadas por la acción antes mencionada.

Time	Agent Address	Origin Address	Type	Enterprise/OID
08/05/17 12:59:43		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.14.16.2.13
08/05/17 12:59:43		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.14.16.2.13
08/05/17 12:59:43		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.14.16.2.13
08/05/17 12:59:44		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.14.16.2.13
08/05/17 12:59:44		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.14.16.2.13
08/05/17 13:00:01		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.1
08/05/17 13:00:08		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.15.7.2
08/05/17 13:00:08		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.2
08/05/17 13:00:08		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.1
08/05/17 13:00:21		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.1
08/05/17 13:00:28		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.2.1.15.7.2
08/05/17 13:00:29		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.2
08/05/17 13:00:29		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.1
08/05/17 13:00:42		205.189.32.105:5...	Trap (SNMPv2+)	1.3.6.1.4.1.9.9.187.0.1
08/05/17 13:00:49		205.189.32.105:5	Trap (SNMPv2+)	1.3.6.1.2.1.15.7.2

Figura 5.50 Traps enviadas después de apagar el Backbone.

Para saber a qué corresponden estas "traps" se utilizó *"SNMP Object Navigator"* de la página de Cisco. En la tabla 5.5 se muestran los OIDs de las traps capturadas y su descripción.

OID trap	Descripción
1.3.6.1.2.1.14.16.2.12	Trap "OspfOrigninateLSA" describe que un nueva LSA se ha originado por ese router.
1.3.6.1.2.1.14.16.2.13	Trap "OspfMaxAgeLSA" significa que una de las LSA en la base de datos del estado del enlace del router ha llegado a un MAXage
1.3.6.1.4.1.9.9.43.2.0.1	Trap "CiscoConfigManEvent" notificación de un evento de gestión de la configuración como registrado en "ccmHistoruEventTable"
1.3.6.1.6.3.1.1.5.4	Trap "linkUp" significa que una entidad SNMP actúa en rol de agente donde detecto que el objeto "ifOperStatus" de uno de sus enlaces fue del estado "down" hacia otro estado.
1.3.6.1.4.1.9.9.138.2.0.2	Trap "ce AlarmCleared" es generada cuando una entidad física borra una alarma previamente confirmada.
1.3.6.1.4.1.9.9.187.0.1	Trap "cbgpFsmStateChange" se genera esta notificación para cada cambio de estado BGP.
1.3.6.1.4.1.9.9.187.0.2/1.3.6.1.2.1.15.7.2	Trap "cbgpBackwardTransition" se genera cuando BGP fsm se mueve desde un estado de numeración alto a uno más bajo.

Tabla 5.5 Muestra de las traps que envió el router de Vancouver

Después de gestionar los OIDs seleccionados se pudo comprobar en el router todos los mensajes SNMP y traps que se han enviado a la unidad gestora, en la figura 5.51 se muestra el resultado de esta comprobación por medio del comando "*show snmp*".

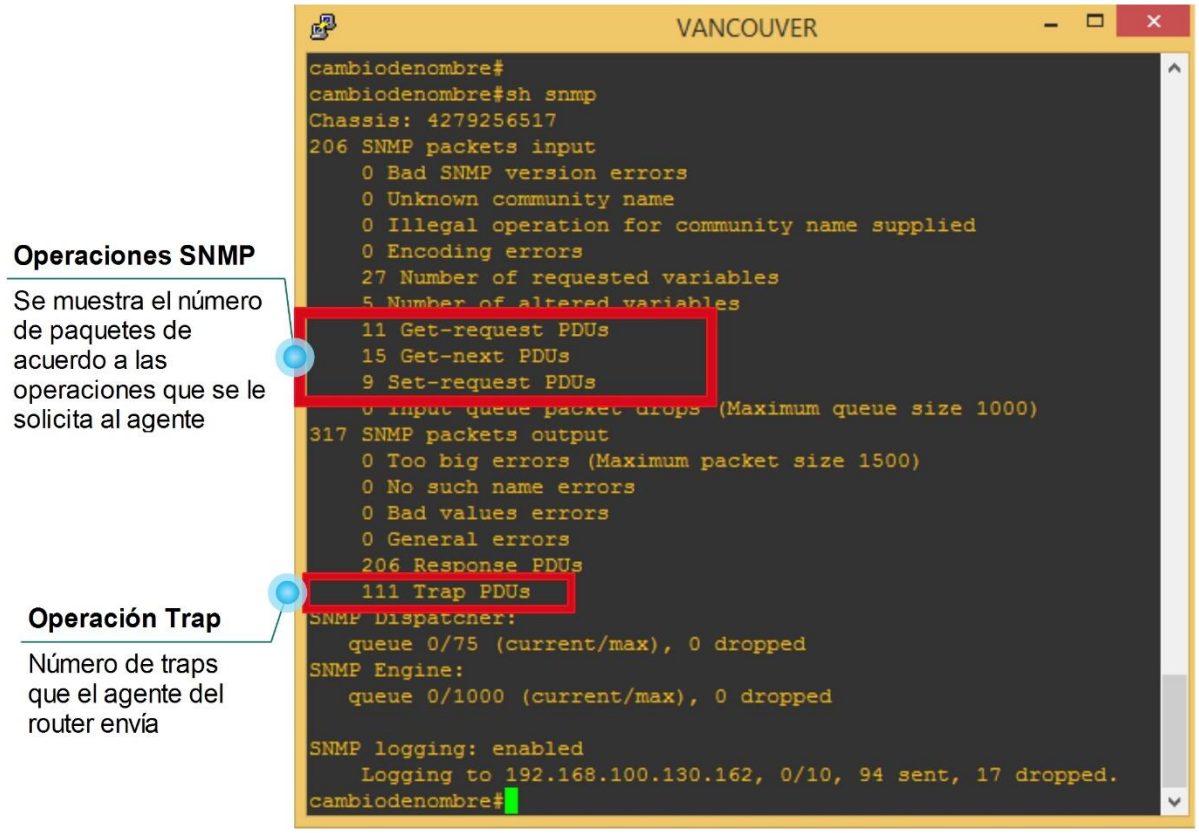


Figura 5.51 Paquetes SNMP que envía el router Vancouver

Como se puede apreciar el emulador ofrece una mejor aproximación de un entorno real para hacer la gestión de estos dispositivos, algo que el simulador esta por mucho limitado, en el emulador se pudo realizar la gestión de casi todos los objetos seleccionados, cabe decir para los objetos de OSPF, BGP y "enterprise" de cisco, el programa "MIB Browser" no proporcionaba el árbol MIB gráficamente pero no obstante se pudo ingresar el OID correspondiente donde el agente del dispositivo respondió y el programa sin problemas obtuvo las instancias de dichos objetos seleccionado. Se pensaba que el simulador podría ejecutar algo similar pero su árbol MIB está limitado tal como aparece en packet tracer. En la figura 5.52 se muestra la comparación de una parte del árbol MIB de emulador con el árbol MIB del simulador.

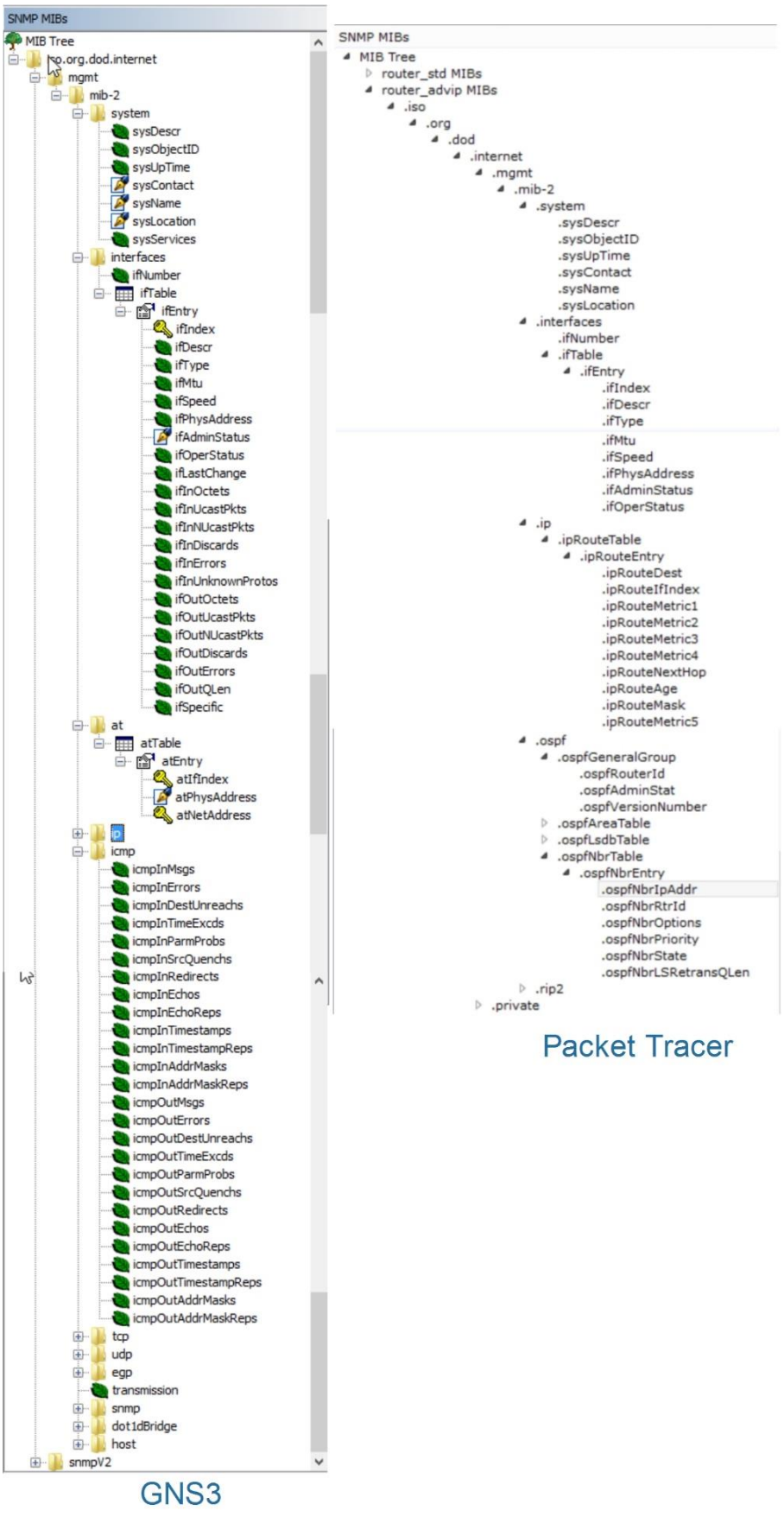


Figura 5.52 Comparación de los arboles MIB correspondientes al emulador y simulador

Desde la red CANARIE se pudieron gestionar los objetos seleccionados del router México, perteneciente a la red CLARA, en la figura 5.53 se muestra un resumen de los objetos gestionados de acuerdo con la tabla 4.6 donde el flujo de paquetes de varias instancias de objetos no tuvo problema, la petición- respuesta fue rápida, probando que la conectividad está funcionando adecuadamente en la integración de las 3 RA.

Name/OID	Value	Type	IP:Port
sysName.0	MEXICO	OctetString	200.0.204.66:161
atNetAddress.2.1.200.0.204.65	200.0.204.65	IpAddress	200.0.204.66:161
atNetAddress.2.1.200.0.204.66	200.0.204.66	IpAddress	200.0.204.66:161
atNetAddress.4.1.198.32.154.1	198.32.154.1	IpAddress	200.0.204.66:161
atNetAddress.4.1.198.32.154.2	198.32.154.2	IpAddress	200.0.204.66:161
ipForwarding.0	forwarding (1)	Integer	200.0.204.66:161
ipDefaultTTL.0	255	Integer	200.0.204.66:161
ipInReceives.0	739	Counter32	200.0.204.66:161
ipInHdrErrors.0	0	Counter32	200.0.204.66:161
ipInAddrErrors.0	0	Counter32	200.0.204.66:161
ipForwDatagrams.0	0	Counter32	200.0.204.66:161
ifOperStatus.1	down (2)	Integer	200.0.204.66:161
ifOperStatus.2	up (1)	Integer	200.0.204.66:161
ifOperStatus.3	down (2)	Integer	200.0.204.66:161
ifOperStatus.4	up (1)	Integer	200.0.204.66:161
ifOperStatus.5	down (2)	Integer	200.0.204.66:161
ifOperStatus.6	down (2)	Integer	200.0.204.66:161
ifOperStatus.7	down (2)	Integer	200.0.204.66:161
ifOperStatus.8	up (1)	Integer	200.0.204.66:161
ifOperStatus.9	up (1)	Integer	200.0.204.66:161
ifLastChange.1	30 seconds (3028)	TimeTicks	200.0.204.66:161
ipNetToMediaType.2.200.0.204.65	dynamic (3)	Integer	200.0.204.66:161
ipNetToMediaType.2.200.0.204.66	static (4)	Integer	200.0.204.66:161
ipNetToMediaType.4.198.32.154.1	dynamic (3)	Integer	200.0.204.66:161
ipNetToMediaType.4.198.32.154.2	static (4)	Integer	200.0.204.66:161
ifAdminStatus.1	up (1)	Integer	200.0.204.66:161
ifAdminStatus.2	up (1)	Integer	200.0.204.66:161
ifAdminStatus.3	down (2)	Integer	200.0.204.66:161
ifAdminStatus.4	up (1)	Integer	200.0.204.66:161
ifAdminStatus.5	down (2)	Integer	200.0.204.66:161
ifAdminStatus.6	down (2)	Integer	200.0.204.66:161
ifAdminStatus.7	down (2)	Integer	200.0.204.66:161
ifAdminStatus.8	up (1)	Integer	200.0.204.66:161
ifAdminStatus.9	up (1)	Integer	200.0.204.66:161
ifOperStatus.1	down (2)	Integer	200.0.204.66:161
ifDescr.1	FastEthernet0/0	OctetString	200.0.204.66:161
ifDescr.2	GigabitEthernet1/0	OctetString	200.0.204.66:161
ifDescr.3	GigabitEthernet2/0	OctetString	200.0.204.66:161
ifDescr.4	GigabitEthernet3/0	OctetString	200.0.204.66:161
ifDescr.5	GigabitEthernet4/0	OctetString	200.0.204.66:161
ifDescr.6	GigabitEthernet5/0	OctetString	200.0.204.66:161
ifDescr.7	GigabitEthernet6/0	OctetString	200.0.204.66:161
ifDescr.8	VoIP-Null0	OctetString	200.0.204.66:161
ifDescr.9	Null0	OctetString	200.0.204.66:161
ifType.1	ethernetCsmacd (6)	Integer	200.0.204.66:161
ipNetToMediaIfIndex.2.200.0.204.65	2	Integer	200.0.204.66:161
ipNetToMediaIfIndex.2.200.0.204.66	2	Integer	200.0.204.66:161
ipNetToMediaIfIndex.4.198.32.154.1	4	Integer	200.0.204.66:161
ipNetToMediaIfIndex.4.198.32.154.2	4	Integer	200.0.204.66:161
ipNetToMediaPhysAddress.2.200.0.204.65	CA-2D-1A-04-00-1C	OctetString	200.0.204.66:161
ipNetToMediaPhysAddress.2.200.0.204.66	CA-2C-18-DC-00-1C	OctetString	200.0.204.66:161
ipNetToMediaPhysAddress.4.198.32.154.1	CA-1D-13-48-00-54	OctetString	200.0.204.66:161
ipNetToMediaPhysAddress.4.198.32.154.2	CA-2C-18-DC-00-54	OctetString	200.0.204.66:161
ipNetToMediaNetAddress.2.200.0.204.65	200.0.204.65	IpAddress	200.0.204.66:161
ipNetToMediaNetAddress.2.200.0.204.66	200.0.204.66	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.14.1.2	No Such Instance	NoSuchInstance	200.0.204.66:161
.1.3.6.1.2.1.14.1.2.0	1	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.1.1.0	200.0.204.66	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.1.200.0.204.65.0	200.0.204.65	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.2.200.0.204.65.0	0	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.3.200.0.204.65.0	200.0.204.65	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.4.200.0.204.65.0	2	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.5.200.0.204.65.0	1	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.6.200.0.204.65.0	8	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.7.200.0.204.65.0	6	Counter32	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.8.200.0.204.65.0	0	Gauge	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.9.200.0.204.65.0	1	Integer	200.0.204.66:161
.1.3.6.1.2.1.14.10.1.10.200.0.204.65.0	1	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.1.0	0x10	OctetString	200.0.204.66:161
.1.3.6.1.2.1.15.2.0	27750	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.1.198.32.154.1	60.60.60.60	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.2.198.32.154.1	6	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.3.198.32.154.1	2	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.4.198.32.154.1	4	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.5.198.32.154.1	198.32.154.2	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.6.198.32.154.1	179	Integer	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.7.198.32.154.1	198.32.154.1	IpAddress	200.0.204.66:161
.1.3.6.1.2.1.15.3.1.8.198.32.154.1	28518	Integer	200.0.204.66:161

Figura 5.53 Gestion del router Mexico desde CANARIE

V.2.4 Resultados de gestión vía NPM

Para poder hacer una aproximación de un NOC, donde la gestión es con todos los equipos de la red integrada. Se ocupó el protocolo SNMP para descubrir los nodos de toda la integración, ya que NPM ocupa varios elementos para el descubrimiento de dispositivos o nodos. En la figura 5.54 se muestra como NPM descubre el router Victoria vía SNMP, donde se observa que es similar al programa "MIB Broswser". Pero se diferencia por que NPM puede hacer una prueba previa para comprobar si hay comunicación con el dispositivo.

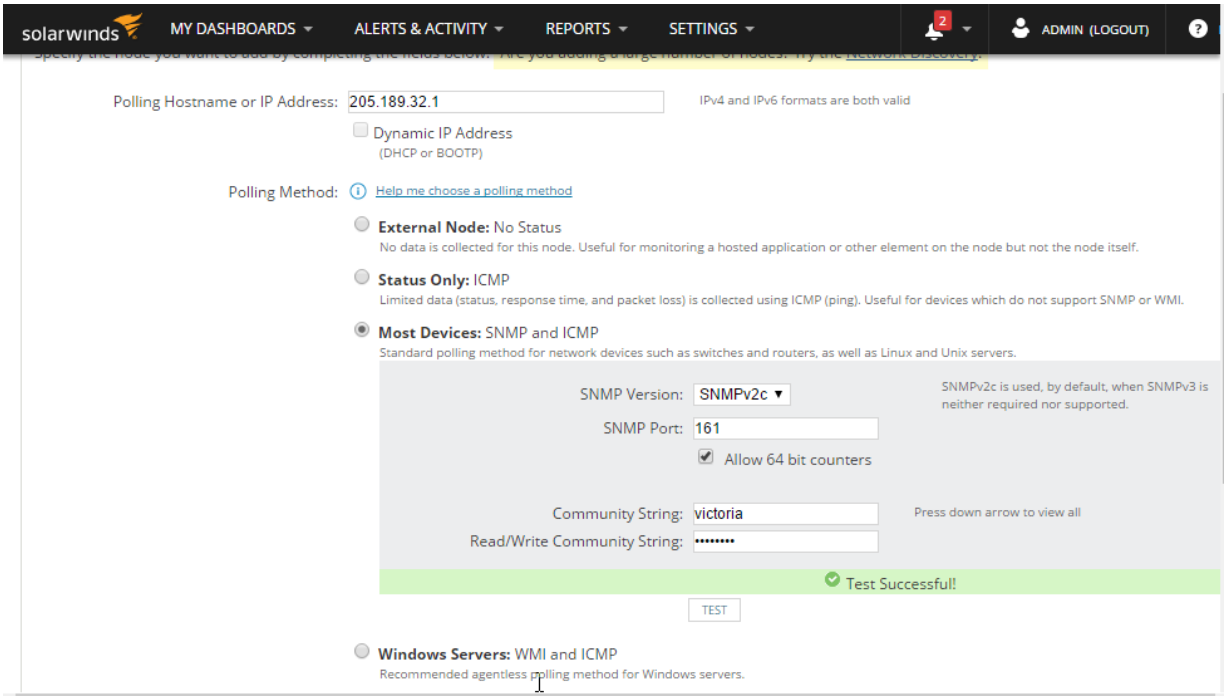


Figura 5.54 Descubrimiento de dispositivos vía SNMPv2

Debido a que NPM es más robusto en comparación con "MIB Browser", una vez que se encuentra el dispositivo se seleccionan los elementos que el programa puede monitorear, como se muestra en la figura 5.55. Se puede apreciar que se encuentran las interfaces, protocolos de enrutamiento (OSPF y BGP), CPU y memoria del router, aquí se pueden seleccionar qué elementos se requieren monitorear.

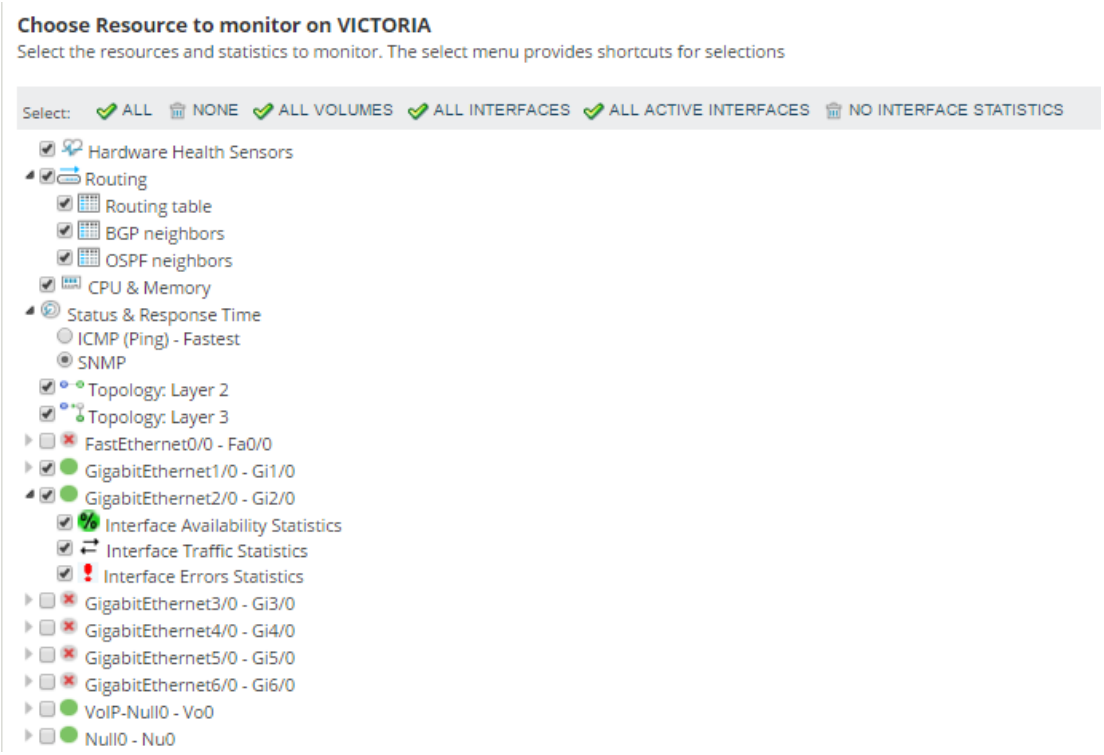


Figura 5.55 Elementos que puede monitorear NPM para el router Victoria

Para terminar de configurar el dispositivo se pueden seleccionar rangos de variables que se quieren monitorear para el CPU, memoria, pérdida de paquetes, etc. En la figura 5.56 se muestra esta configuración que se puede seleccionar en NPM.

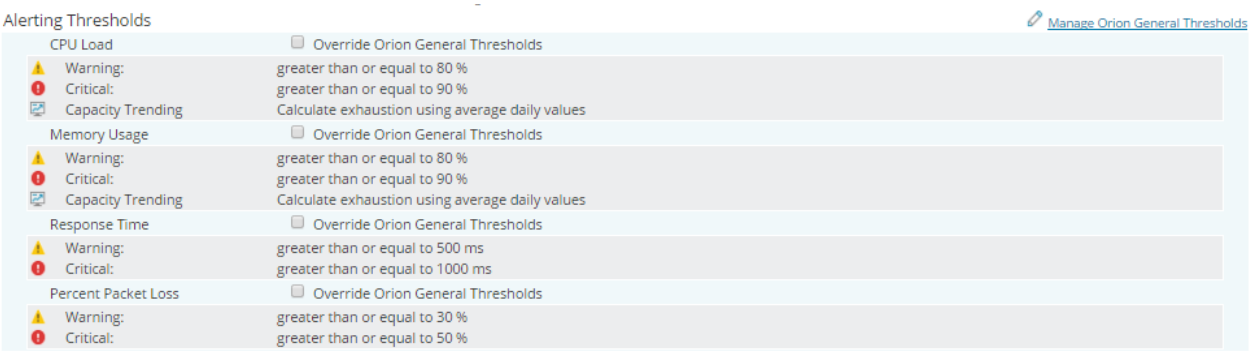


Figura 5.56 Elementos adicionales a monitorear que NPM ofrece para los routers

Todo el proceso anterior se realizó para gestionar los routers de backbone como los routers de acceso, en la figura 5.57 se muestran cómo están desplegados todos los routers dependiendo del modelo del router utilizado ya que NPM ofrece la posibilidad de gestionar varios modelos. Para este trabajo se muestra el número de router cisco 7200 y cisco 3620 que están empleados en el backbone de la integración de las RA de América.

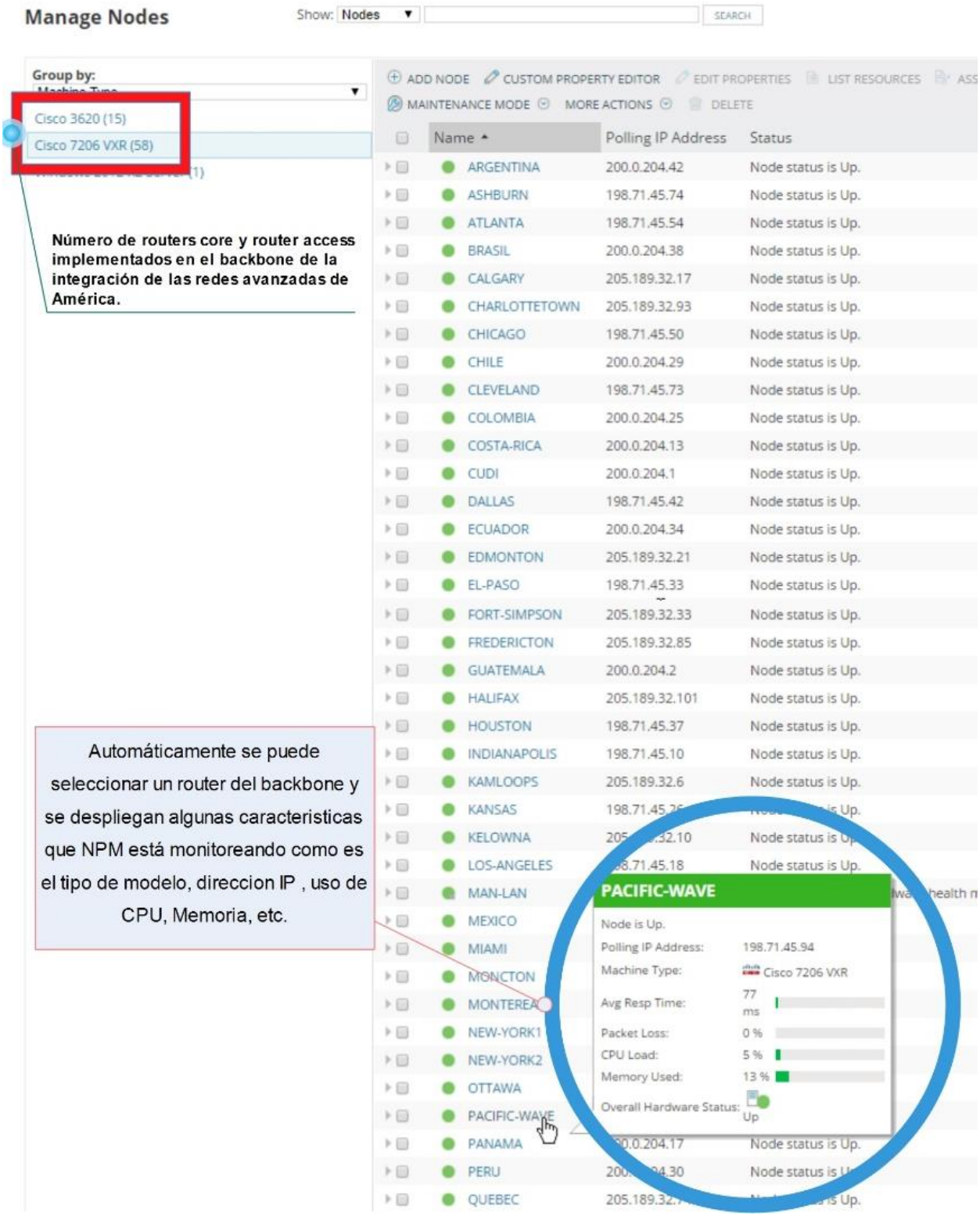


Figura 5.57 Monitoreo de todos los routers ocupados en la integración de las RA de América con NPM

Para fines demostrativos de como es el despliegue de todo el monitoreo, en la figura 5.58 se muestra los diferente elementos que NPM está monitoreando para el router Pacific Wave.

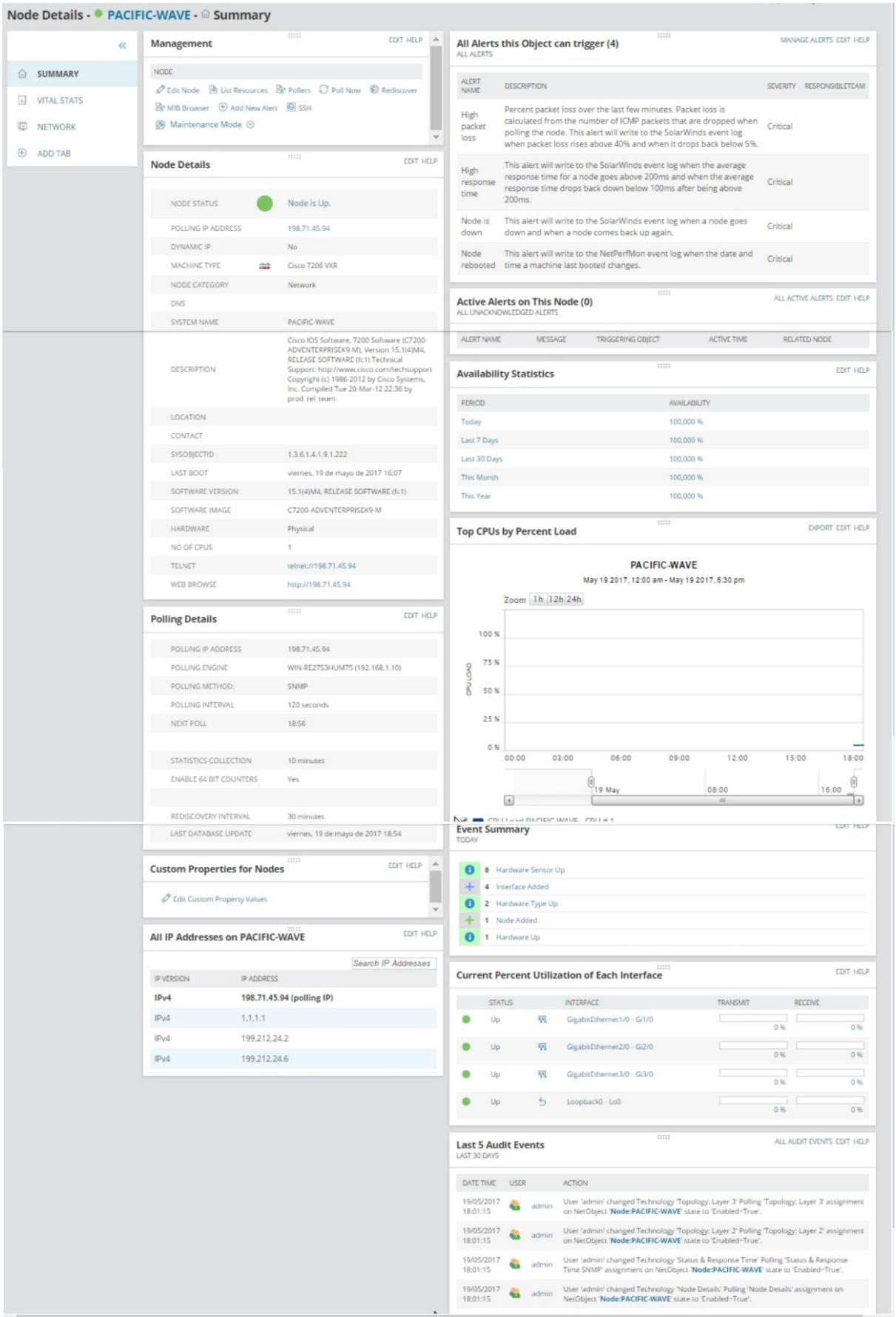


Figura 5.58 Capacidades de NPM para gestionar algunas características del router Pacific Wave

NPM ofrece muchas capacidades de monitoreo sobre dispositivos, en las figuras 5.59a y 5.59b se muestran otra colección de elementos que NPM es capaz de monitorear, ya sea de un solo router, o de todo el conjunto de routers. Entre estos elementos de gestión se encuentran: la tasa de uso de datos del enlace, el porcentaje de pérdidas de paquetes, el tipo de enlaces que utiliza el router, tipo de protocolos de enrutamiento que está ejecutando, uso de memoria, CPU y temperatura que presenta un router.

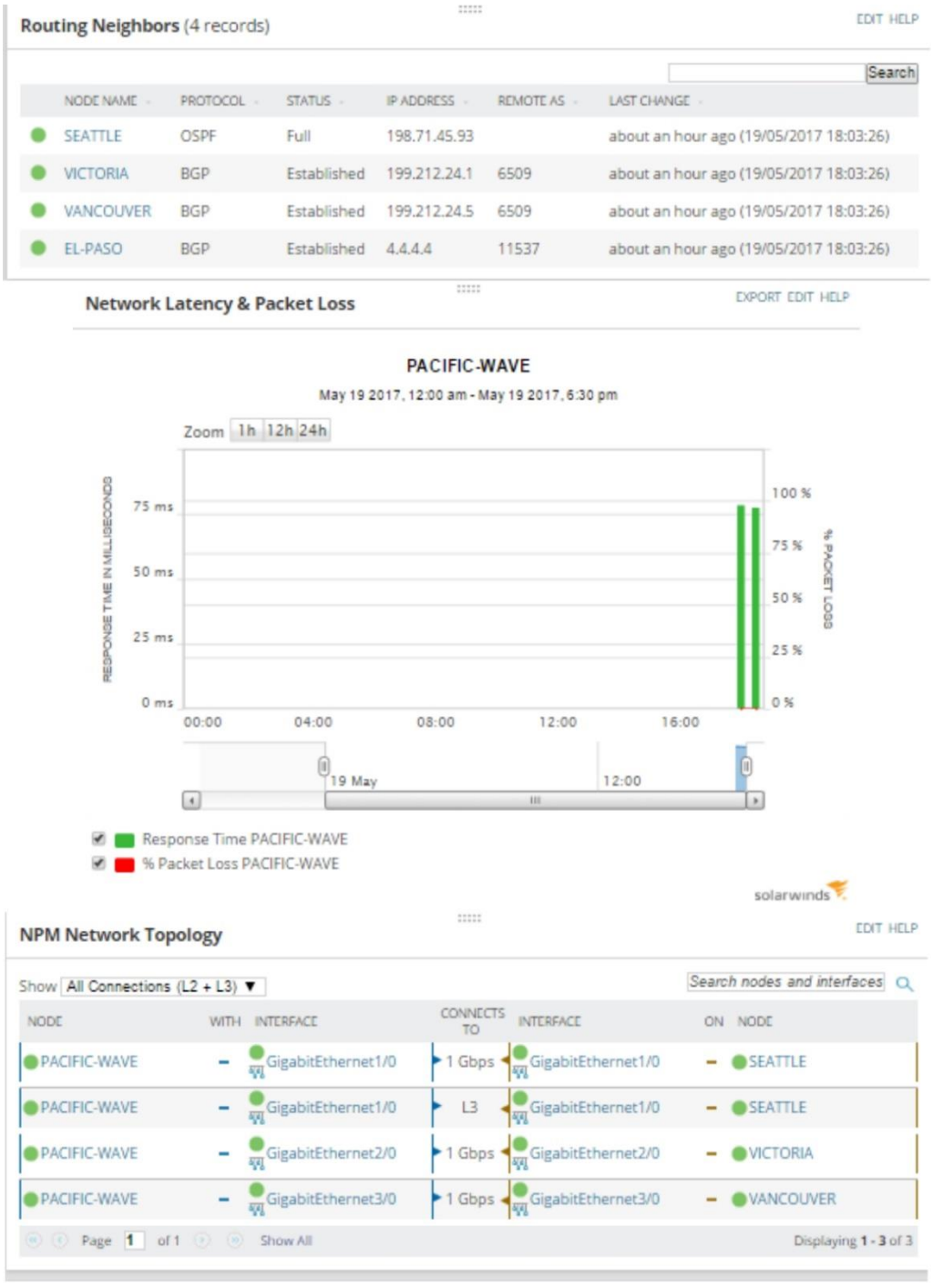


Figura 5.59a Elementos que se pueden monitorear en el router Pacfic Wave

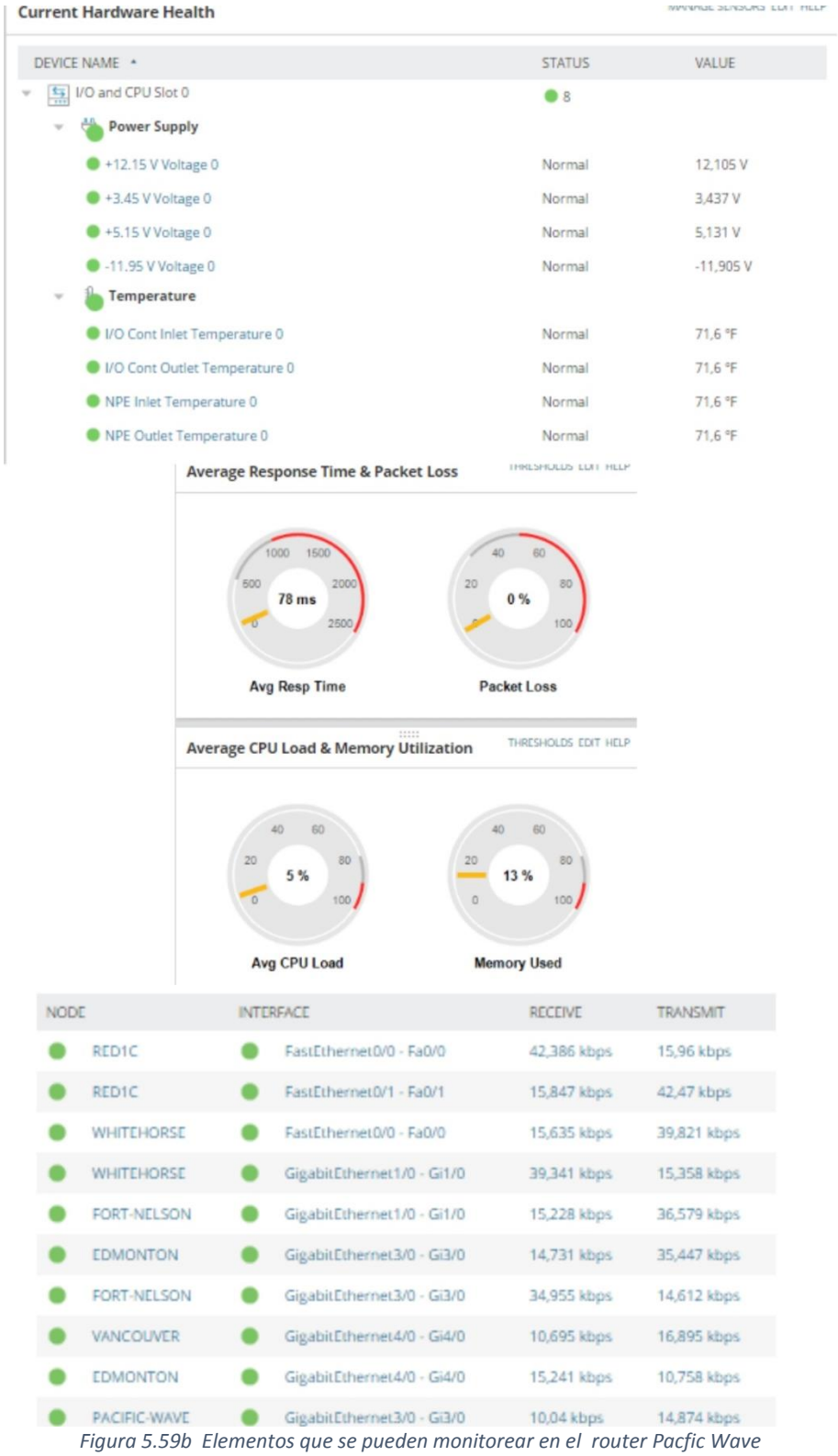
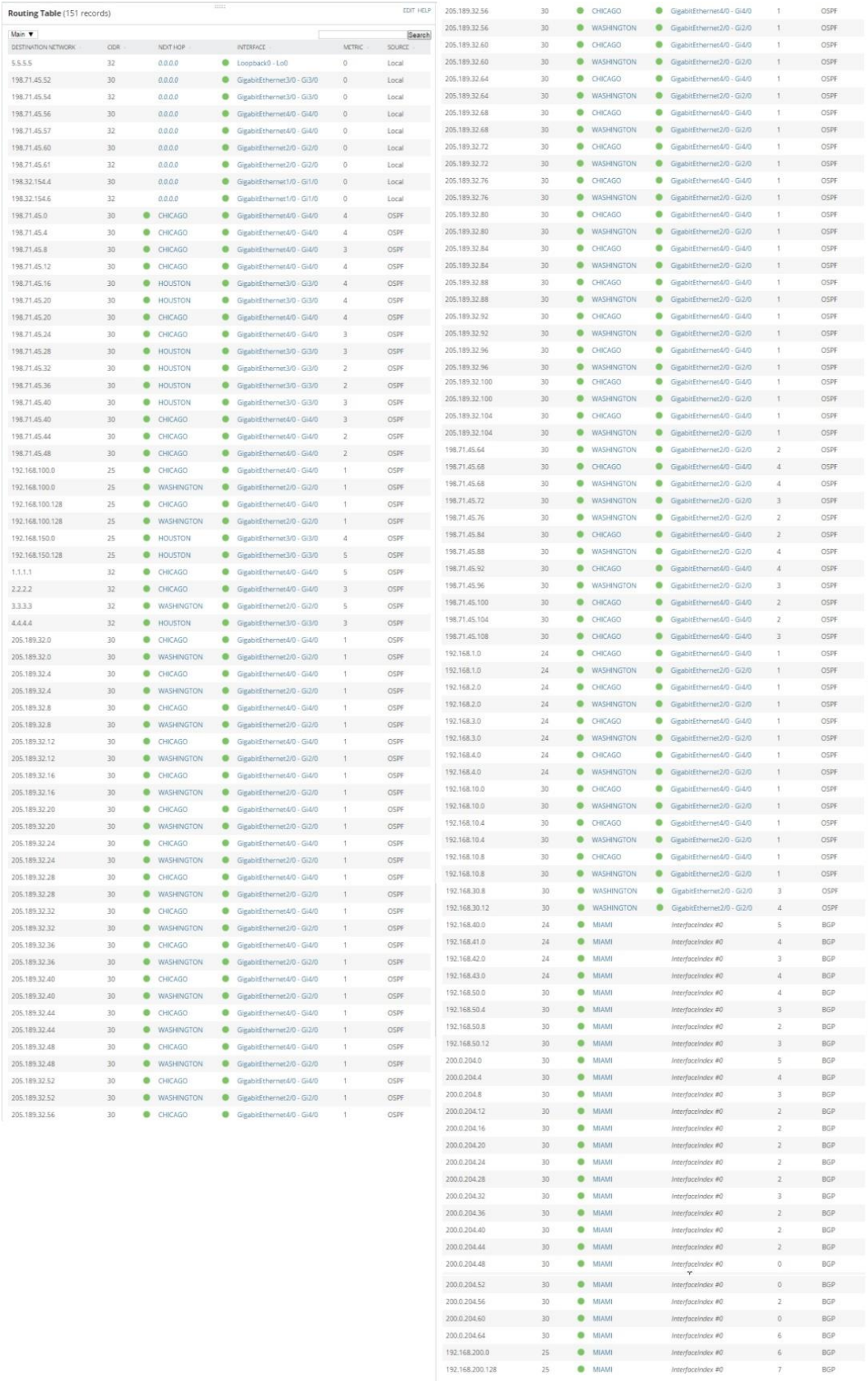


Figura 5.59b Elementos que se pueden monitorear en el router Pacfic Wave

Con NPM también se puede verificar de una manera más práctica la tabla de enrutamiento, donde presenta las redes que puede alcanzar, en este caso, el router de Atlanta. En la figura 5.60 se muestra la tabla de enrutamiento junto al protocolo de enrutamiento aprendido para cada red, su respectiva métrica y el salto que debe dar para alcanzar cierta red.



Routing Table (151 records)

EDIT HELP

Main ▼ Search

DESTINATION NETWORK	CIDR	NEXT HOP	INTERFACE	METRIC	SOURCE
5.5.5.5	32	0.0.0.0	Loopback0 - Lo0	0	Local
198.71.45.52	30	0.0.0.0	GigabitEthernet3/0 - Gi3/0	0	Local
198.71.45.54	32	0.0.0.0	GigabitEthernet3/0 - Gi3/0	0	Local
198.71.45.56	30	0.0.0.0	GigabitEthernet4/0 - Gi4/0	0	Local
198.71.45.57	32	0.0.0.0	GigabitEthernet4/0 - Gi4/0	0	Local
198.71.45.60	30	0.0.0.0	GigabitEthernet2/0 - Gi2/0	0	Local
198.71.45.61	32	0.0.0.0	GigabitEthernet2/0 - Gi2/0	0	Local
198.32.154.4	30	0.0.0.0	GigabitEthernet1/0 - Gi1/0	0	Local
198.32.154.6	32	0.0.0.0	GigabitEthernet1/0 - Gi1/0	0	Local
198.71.45.0	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.4	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.8	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	3	OSPF
198.71.45.12	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.16	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	4	OSPF
198.71.45.20	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	4	OSPF
198.71.45.20	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.24	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	3	OSPF
198.71.45.28	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	3	OSPF
198.71.45.32	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	2	OSPF
198.71.45.36	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	2	OSPF
198.71.45.40	30	HOUSTON	GigabitEthernet3/0 - Gi3/0	3	OSPF
198.71.45.40	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	3	OSPF
198.71.45.44	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	2	OSPF
198.71.45.48	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	2	OSPF
192.168.100.0	25	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.100.0	25	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.100.128	25	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.100.128	25	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.150.0	25	HOUSTON	GigabitEthernet3/0 - Gi3/0	4	OSPF
192.168.150.128	25	HOUSTON	GigabitEthernet3/0 - Gi3/0	5	OSPF
1.1.1.1	32	CHICAGO	GigabitEthernet4/0 - Gi4/0	5	OSPF
2.2.2.2	32	CHICAGO	GigabitEthernet4/0 - Gi4/0	3	OSPF
3.3.3.3	32	WASHINGTON	GigabitEthernet2/0 - Gi2/0	5	OSPF
4.4.4.4	32	HOUSTON	GigabitEthernet3/0 - Gi3/0	3	OSPF
205.189.32.0	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.0	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.4	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.4	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.8	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.8	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.12	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.12	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.16	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.16	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.20	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.20	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.24	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.24	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.28	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.28	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.32	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.32	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.36	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.36	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.40	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.40	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.44	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.44	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.48	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.48	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.52	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.52	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.56	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.56	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.60	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.60	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.64	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.64	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.68	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.68	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.72	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.72	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.76	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.76	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.80	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.80	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.84	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.84	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.88	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.88	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.92	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.92	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.96	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.96	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.100	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.100	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
205.189.32.104	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
205.189.32.104	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
198.71.45.64	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	2	OSPF
198.71.45.68	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.68	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	4	OSPF
198.71.45.72	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	3	OSPF
198.71.45.76	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	2	OSPF
198.71.45.84	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	2	OSPF
198.71.45.88	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	4	OSPF
198.71.45.92	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	4	OSPF
198.71.45.96	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	3	OSPF
198.71.45.100	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	2	OSPF
198.71.45.104	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	2	OSPF
198.71.45.108	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	3	OSPF
192.168.1.0	24	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.1.0	24	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.2.0	24	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.2.0	24	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.3.0	24	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.3.0	24	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.4.0	24	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.4.0	24	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.10.0	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.10.0	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.10.4	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.10.4	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.10.8	30	CHICAGO	GigabitEthernet4/0 - Gi4/0	1	OSPF
192.168.10.8	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	1	OSPF
192.168.30.8	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	3	OSPF
192.168.30.12	30	WASHINGTON	GigabitEthernet2/0 - Gi2/0	4	OSPF
192.168.40.0	24	MIAMI	Interfaceindex #0	5	BGP
192.168.41.0	24	MIAMI	Interfaceindex #0	4	BGP
192.168.42.0	24	MIAMI	Interfaceindex #0	3	BGP
192.168.43.0	24	MIAMI	Interfaceindex #0	4	BGP
192.168.50.0	30	MIAMI	Interfaceindex #0	4	BGP
192.168.50.4	30	MIAMI	Interfaceindex #0	3	BGP
192.168.50.8	30	MIAMI	Interfaceindex #0	2	BGP
192.168.50.12	30	MIAMI	Interfaceindex #0	3	BGP
200.0.204.0	30	MIAMI	Interfaceindex #0	5	BGP
200.0.204.4	30	MIAMI	Interfaceindex #0	4	BGP
200.0.204.8	30	MIAMI	Interfaceindex #0	3	BGP
200.0.204.12	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.16	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.20	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.24	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.28	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.32	30	MIAMI	Interfaceindex #0	3	BGP
200.0.204.36	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.40	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.44	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.48	30	MIAMI	Interfaceindex #0	0	BGP
200.0.204.52	30	MIAMI	Interfaceindex #0	0	BGP
200.0.204.56	30	MIAMI	Interfaceindex #0	2	BGP
200.0.204.60	30	MIAMI	Interfaceindex #0	0	BGP
200.0.204.64	30	MIAMI	Interfaceindex #0	6	BGP
192.168.200.0	25	MIAMI	Interfaceindex #0	6	BGP
192.168.200.128	25	MIAMI	Interfaceindex #0	7	BGP

Figura 5.60 Contenido de la tabla de enrutamiento del router de Atlanta en NPM.

En la figura 5.61 se puede ver el resultado de la ejecución de algunas "traps", donde NPM está interpretándolas como alarmas de perdida de paquetes o respuesta nula de algunos routers.

Figura 5.61 Alarmas que NPM interpreta de acuerdo a las traps enviaddas.

Para el descubrimiento y gestion de dispositivos se usó la versión 2 de SNMP, pero NPM también es capaz de ejecutar SNMPv3, en la figura 5.62 se muestra los campos requeridos por parte de NPM para poder utilizar SNMPv3 (esta versión no se utilizó ya que esta fuera de los objetivos de este trabajo).

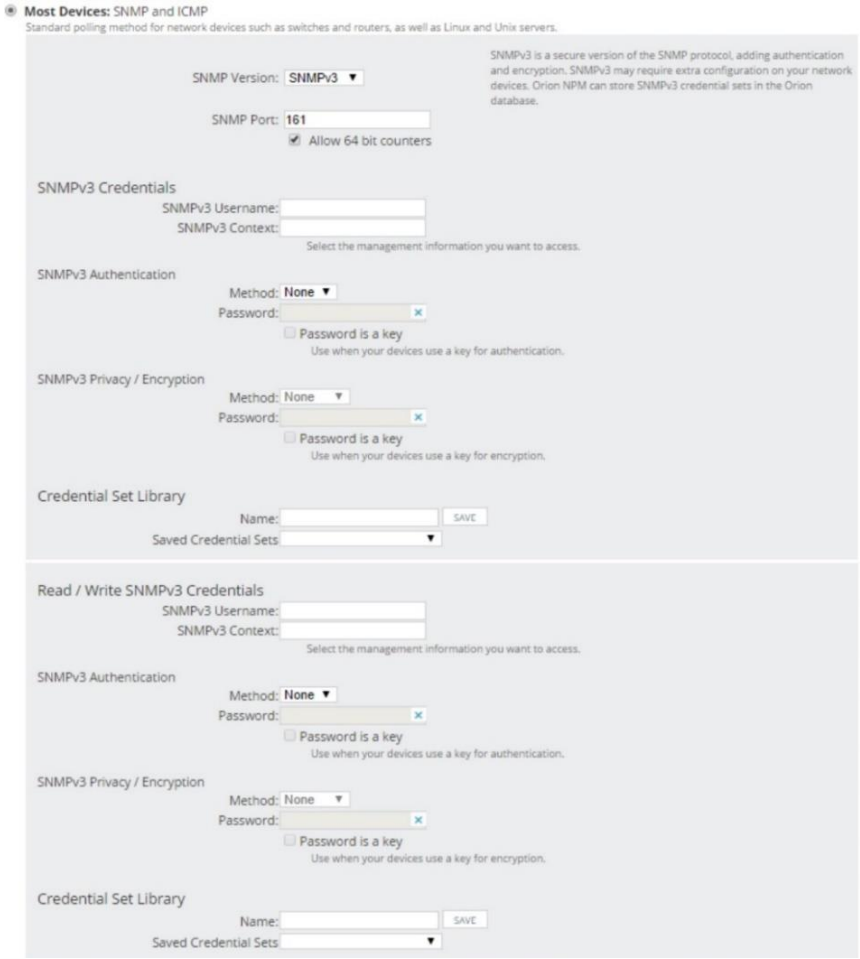


Figura 5.62 Campos para la configuración de SNMPv3 en NPM

Se verificó el tráfico respecto a los mensajes SNMP que está utilizando NPM, estos se pudieron capturar como se muestran en las figuras 5.63a y 5.63b, donde se observa de forma parcial el tráfico generado por un sólo router.

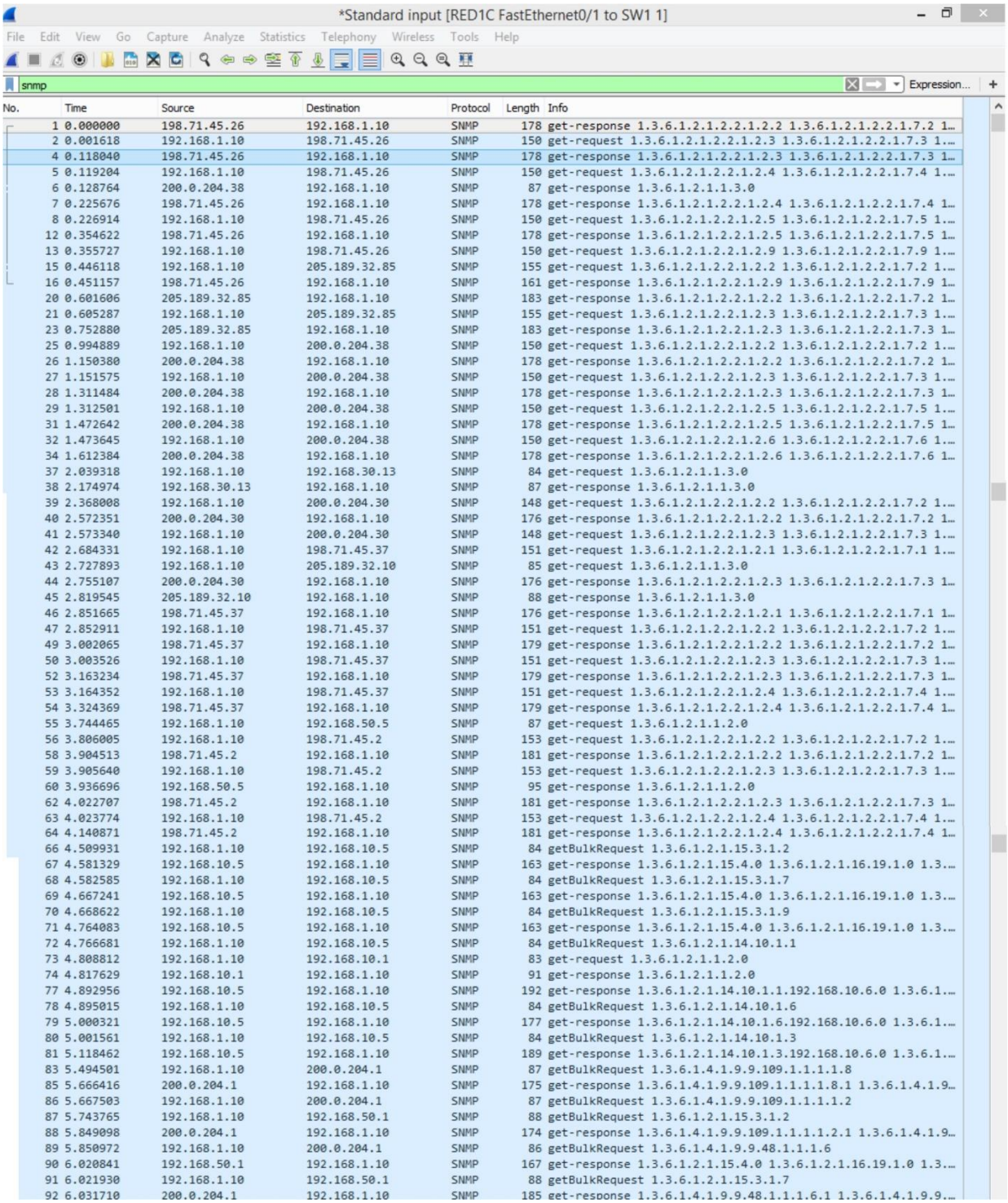


Figura 5.63a Mensajes SNMP que ocupa NPM

92	6.031710	200.0.204.1	192.168.1.10	SNMP	185 get-response 1.3.6.1.4.1.9.9.48.1.1.1.6.1 1.3.6.1.4.1.9.9.…
93	6.032750	192.168.1.10	200.0.204.1	SNMP	86 getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.5
94	6.056410	192.168.1.10	205.189.32.33	SNMP	94 getBulkRequest 1.3.6.1.4.1.9.9.109.1.1.1.1.8
95	6.117572	205.189.32.33	192.168.1.10	SNMP	182 get-response 1.3.6.1.4.1.9.9.109.1.1.1.1.8.1 1.3.6.1.4.1.9…
96	6.118712	192.168.1.10	205.189.32.33	SNMP	94 getBulkRequest 1.3.6.1.4.1.9.9.109.1.1.1.1.2
97	6.182014	205.189.32.33	192.168.1.10	SNMP	181 get-response 1.3.6.1.4.1.9.9.109.1.1.1.1.2.1 1.3.6.1.4.1.9…
98	6.183254	192.168.1.10	205.189.32.33	SNMP	93 getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.6
99	6.203539	200.0.204.1	192.168.1.10	SNMP	182 get-response 1.3.6.1.4.1.9.9.48.1.1.1.5.1 1.3.6.1.4.1.9.9.…
100	6.206679	192.168.1.10	200.0.204.1	SNMP	164 get-request 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0 …
101	6.246458	205.189.32.33	192.168.1.10	SNMP	192 get-response 1.3.6.1.4.1.9.9.48.1.1.1.6.1 1.3.6.1.4.1.9.9.…
102	6.247610	192.168.1.10	205.189.32.33	SNMP	93 getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.5
103	6.268585	192.168.50.1	192.168.1.10	SNMP	167 get-response 1.3.6.1.2.1.15.4.0 1.3.6.1.2.1.16.19.1.0 1.3.…
104	6.269924	192.168.1.10	192.168.50.1	SNMP	88 getBulkRequest 1.3.6.1.2.1.15.3.1.9
105	6.301143	205.189.32.33	192.168.1.10	SNMP	189 get-response 1.3.6.1.4.1.9.9.48.1.1.1.5.1 1.3.6.1.4.1.9.9.…
106	6.302888	192.168.1.10	205.189.32.33	SNMP	171 get-request 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0 …
107	6.321995	192.168.1.10	205.189.32.101	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1.…
110	6.365647	205.189.32.33	192.168.1.10	SNMP	178 get-response 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0…
111	6.376361	200.0.204.1	192.168.1.10	SNMP	170 get-response 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0…
112	6.505285	192.168.50.1	192.168.1.10	SNMP	167 get-response 1.3.6.1.2.1.15.4.0 1.3.6.1.2.1.16.19.1.0 1.3.…
113	6.506469	192.168.1.10	192.168.50.1	SNMP	88 getBulkRequest 1.3.6.1.2.1.14.10.1.1
114	6.516046	205.189.32.101	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1…
115	6.517453	192.168.1.10	205.189.32.101	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.4 1.3.6.1.2.1.2.2.1.7.4 1.…
116	6.720323	205.189.32.101	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.4 1.3.6.1.2.1.2.2.1.7.4 1…
117	6.722546	192.168.1.10	205.189.32.101	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.5 1.3.6.1.2.1.2.2.1.7.5 1.…
118	6.741792	192.168.50.1	192.168.1.10	SNMP	196 get-response 1.3.6.1.2.1.14.10.1.1.192.168.50.2.0 1.3.6.1.…
119	6.743690	192.168.1.10	192.168.50.1	SNMP	88 getBulkRequest 1.3.6.1.2.1.14.10.1.6
120	6.823059	192.168.1.10	198.71.45.54	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1.…
121	6.924273	205.189.32.101	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.5 1.3.6.1.2.1.2.2.1.7.5 1…
124	6.956557	198.71.45.54	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1…
125	6.957654	192.168.1.10	198.71.45.54	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.3 1.3.6.1.2.1.2.2.1.7.3 1.…
126	6.978053	192.168.50.1	192.168.1.10	SNMP	181 get-response 1.3.6.1.2.1.14.10.1.6.192.168.50.2.0 1.3.6.1.…
127	6.979156	192.168.1.10	192.168.50.1	SNMP	88 getBulkRequest 1.3.6.1.2.1.14.10.1.3
128	7.096187	198.71.45.54	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.3 1.3.6.1.2.1.2.2.1.7.3 1…
129	7.097840	192.168.1.10	198.71.45.54	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.4 1.3.6.1.2.1.2.2.1.7.4 1.…
132	7.212482	192.168.1.10	198.71.45.66	SNMP	91 getBulkRequest 1.3.6.1.4.1.9.9.109.1.1.1.1.8
133	7.225053	192.168.50.1	192.168.1.10	SNMP	193 get-response 1.3.6.1.2.1.14.10.1.3.192.168.50.2.0 1.3.6.1.…
134	7.235790	198.71.45.54	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.4 1.3.6.1.2.1.2.2.1.7.4 1…
135	7.236863	192.168.1.10	198.71.45.54	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.5 1.3.6.1.2.1.2.2.1.7.5 1.…
136	7.364749	198.71.45.66	192.168.1.10	SNMP	179 get-response 1.3.6.1.4.1.9.9.109.1.1.1.1.8.1 1.3.6.1.4.1.9…
137	7.365972	192.168.1.10	198.71.45.66	SNMP	91 getBulkRequest 1.3.6.1.4.1.9.9.109.1.1.1.1.2
138	7.375522	198.71.45.54	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.5 1.3.6.1.2.1.2.2.1.7.5 1…
139	7.376577	192.168.1.10	198.71.45.54	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.10 1.3.6.1.2.1.2.2.1.7.10 …
140	7.446806	192.168.1.10	198.71.45.6	SNMP	86 get-request 1.3.6.1.2.1.1.2.0
141	7.515110	198.71.45.54	192.168.1.10	SNMP	167 get-response 1.3.6.1.2.1.2.2.1.2.10 1.3.6.1.2.1.2.2.1.7.10…
142	7.525839	198.71.45.66	192.168.1.10	SNMP	178 get-response 1.3.6.1.4.1.9.9.109.1.1.1.1.2.1 1.3.6.1.4.1.9…
143	7.527465	192.168.1.10	198.71.45.66	SNMP	90 getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.6
144	7.547402	198.71.45.6	192.168.1.10	SNMP	95 get-response 1.3.6.1.2.1.1.2.0
146	7.650568	192.168.1.10	200.0.204.34	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.1 1.3.6.1.2.1.2.2.1.7.1 1.…
148	7.687039	198.71.45.66	192.168.1.10	SNMP	189 get-response 1.3.6.1.4.1.9.9.48.1.1.1.6.1 1.3.6.1.4.1.9.9.…
149	7.688228	192.168.1.10	198.71.45.66	SNMP	90 getBulkRequest 1.3.6.1.4.1.9.9.48.1.1.1.5
150	7.848180	198.71.45.66	192.168.1.10	SNMP	186 get-response 1.3.6.1.4.1.9.9.48.1.1.1.5.1 1.3.6.1.4.1.9.9.…
151	7.849569	192.168.1.10	198.71.45.66	SNMP	168 get-request 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0 …
152	7.858960	200.0.204.34	192.168.1.10	SNMP	176 get-response 1.3.6.1.2.1.2.2.1.2.1 1.3.6.1.2.1.2.2.1.7.1 1…
153	7.859934	192.168.1.10	200.0.204.34	SNMP	151 get-request 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1.…
156	7.987793	198.71.45.66	192.168.1.10	SNMP	175 get-response 1.3.6.1.4.1.9.2.1.35.0 1.3.6.1.4.1.9.2.1.67.0…
157	8.041489	200.0.204.34	192.168.1.10	SNMP	179 get-response 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1…
158	8.181643	192.168.1.10	200.0.204.2	SNMP	87 get-request 1.3.6.1.2.1.1.2.0
159	8.181746	192.168.1.10	205.189.32.66	SNMP	150 get-request 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1.…
160	8.299335	205.189.32.66	192.168.1.10	SNMP	178 get-response 1.3.6.1.2.1.2.2.1.2.2 1.3.6.1.2.1.2.2.1.7.2 1…
161	8.300473	192.168.1.10	205.189.32.66	SNMP	150 get-request 1.3.6.1.2.1.2.2.1.2.3 1.3.6.1.2.1.2.2.1.7.3 1.…
162	8.363824	200.0.204.2	192.168.1.10	SNMP	96 get-response 1.3.6.1.2.1.1.2.0
164	8.396050	205.189.32.66	192.168.1.10	SNMP	178 get-response 1.3.6.1.2.1.2.2.1.2.3 1.3.6.1.2.1.2.2.1.7.3 1…
166	8.524780	192.168.1.10	192.168.10.13	SNMP	83 get-request 1.3.6.1.2.1.1.3.0
169	8.696925	192.168.1.10	205.189.32.33	SNMP	89 get-request 1.3.6.1.2.1.1.3.0
170	8.750611	192.168.10.13	192.168.1.10	SNMP	86 get-response 1.3.6.1.2.1.1.3.0
171	8.760174	192.168.1.10	198.71.45.54	SNMP	85 get-request 1.3.6.1.2.1.1.3.0
172	8.761352	205.189.32.33	192.168.1.10	SNMP	92 get-response 1.3.6.1.2.1.1.3.0
173	8.868775	198.71.45.54	192.168.1.10	SNMP	88 get-response 1.3.6.1.2.1.1.3.0
174	8.869460	192.168.1.10	200.0.204.42	SNMP	153 get-request 1.3.6.1.2.1.2.2.1.2.1 1.3.6.1.2.1.2.2.1.7.1 1.…

Figura 5.63b Mensajes SNMP que ocupa NPM

Dentro de NPM se puede acceder al MIB de cada router, donde se obtuvo un árbol MIB mucho mayor que el que ofrecía el programa "MIB Browser", donde se probaron los objetos estipulados en la tabla 4.6, algo que no se pudo realizar fue la configuración de objetos, ya que NPM no es capaz de realizar dichas operaciones. En la figura 5.64 del lado izquierdo se muestra el árbol MIB que ofrece NPM y del lado derecho se muestra el despliegue de información respecto a un OID.

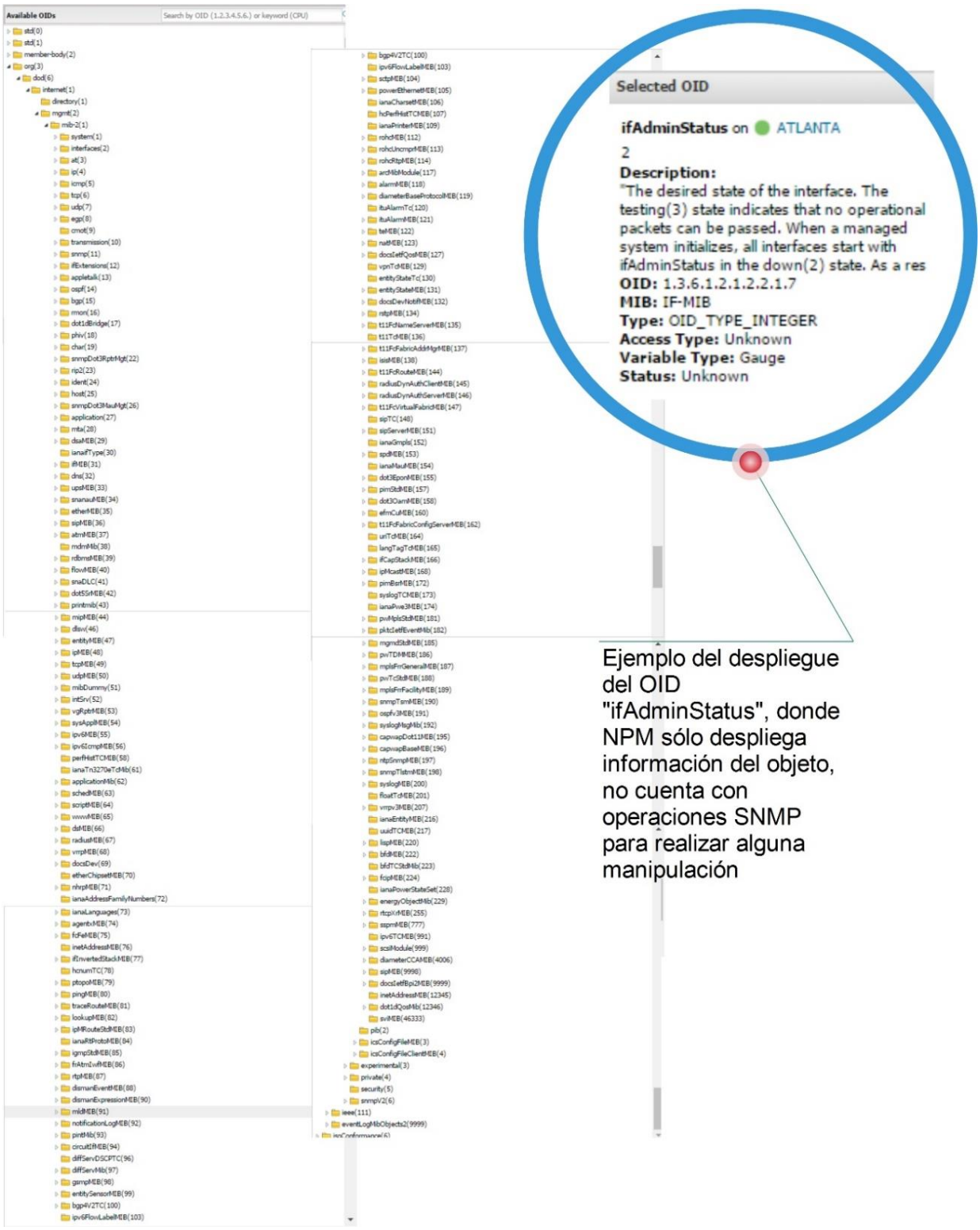


Figura 5.64 Árbol MIB de NPM.

NPM también es capaz de generar un mapa para estar monitoreando el tráfico y utilización de la red en cierta área geográfica, algo similar a lo que realiza un NOC .Ya que este trabajo está dedicado a la integración de las tres RA de América, se generó el mapa del continente

Americano con todo el backbone integrado. En la figura 5.65 se muestra el mapa de la integración de las RA generado por NPM y un ejemplo de como, al seleccionar un nodo de la red (por ejemplo el router Victoria), este desplegará detalles de conexión, donde se puede apreciar el tipo de interfaz usada, así como el porcentaje de tráfico que está pasando por ese enlace.

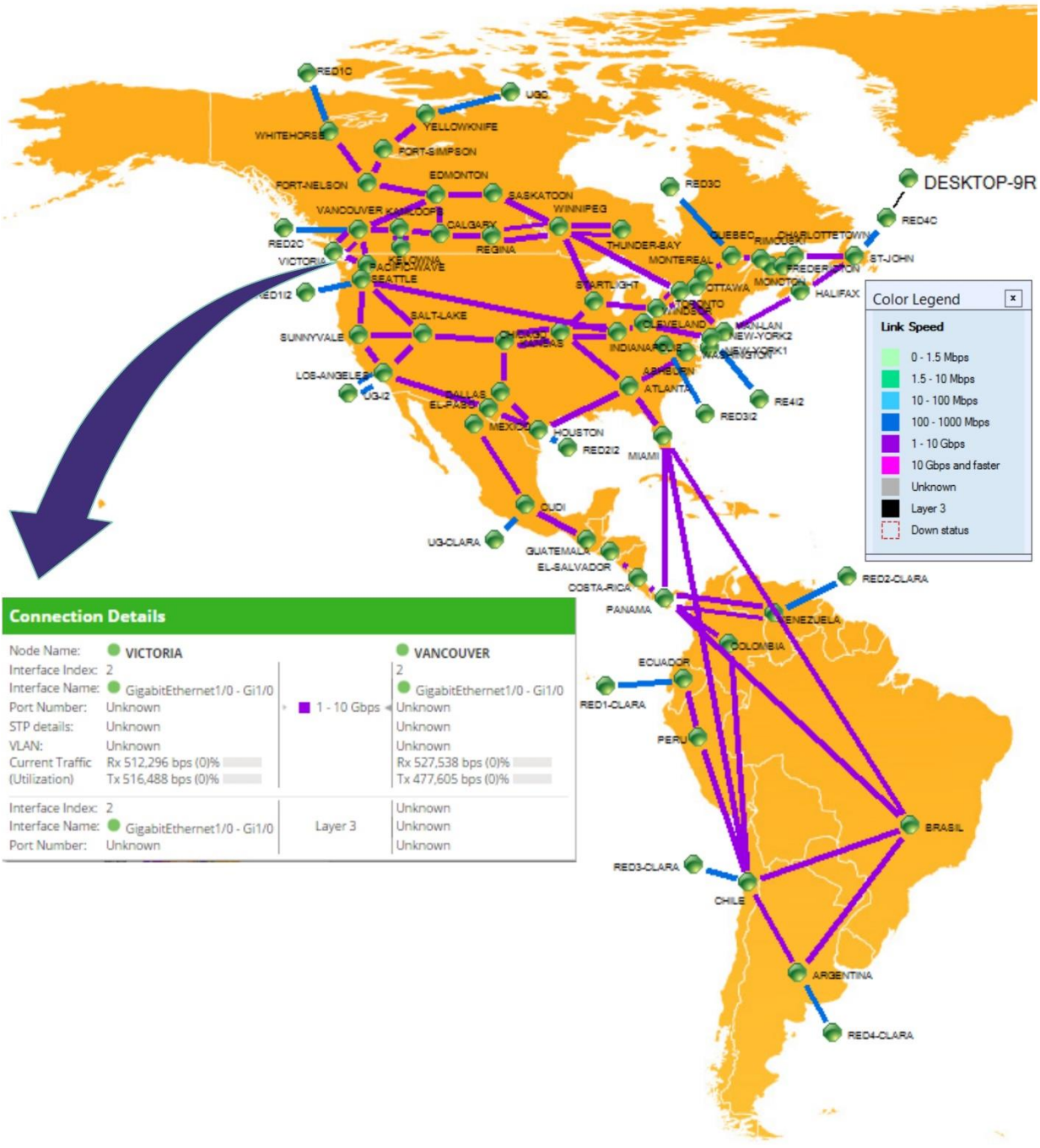


Figura 5.65 Monitoreo de la integración de las RA en NPM

V.2.5 Resultados del consumo de recursos de emulación

El consumo de recursos de GNS3 puede ser variado, esto depende de qué tan complejo es la emulación que se quiera realizar, en el caso particular de este trabajo se emularon 3 topologías y posteriormente la integración de estas, por lo cual en la tabla 5.6 se muestran los recursos que consumió cada red así como la integración de las RA, también se especifica el tiempo desde que se levanta la configuración de los routers y las VM hasta la estabilidad de la emulación.

Topología emulada	Recursos		Tiempo de estabilidad
	Uso de CPU	Memoria RAM (%)	
CANARIE	10 %	33% (10.6 GB)	5:40 min
Internet2	10 %	28% (8.6GB)	3:48 min
CLARA	8.9 %	27% (8.5GB)	3:30 min
Integración de las RA	29%	79% (25.4 GB)	36:46 min

Tabla 5.6 Tabla de recursos de utilizados por GNS3

En la figura 5.66 se muestra el total de recursos que se están consumiendo en la emulación de la integración de las RA de América la cual fue de 25.4 GB de memoria RAM, 11 veces más que la que requiere la simulación. Este consumo se debe a que la emulación toma parte de los recursos del equipo para que los dispositivos tengan una buena aproximación del mundo real, algo para lo que el simulador está muy limitado.

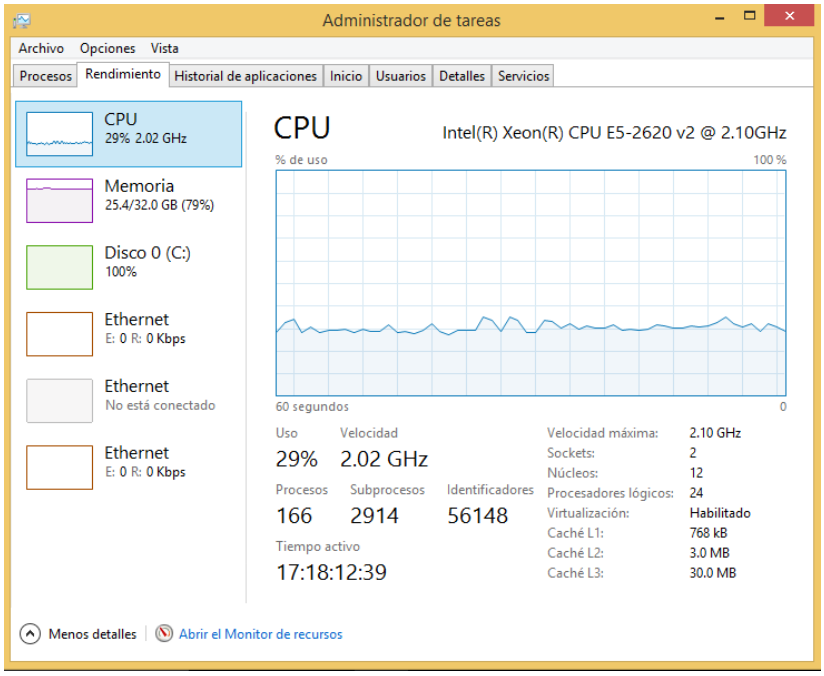


Figura 5.66 Recursos que consume el emulador

Es importante notar que el porcentaje del CPU es del 29%, esto debido a que se activaron todos los elementos de la integración por partes, ya que de lo contrario habría fallas de inicio y el CPU se hubiera disparado hasta el 100% y tardaría mucho tiempo en estabilizarse e inclusive podría correr el riesgo de no estabilizarse.

V.3 Conclusiones

De acuerdo con el estudio de las RA de América se encuentran los siguientes puntos a destacar:

- Las RA son importantes para grandes avances tecnológicos y científicos.
- Las RA de primer mundo (CANARIE e I2) están en constante evolución en su infraestructura, lo que permite contar con la tecnología de última generación proporcionada por la gran demanda de uso.
- No todas las instituciones son privilegiadas de poder conectarse a estas redes, ya que se conectan solo las instituciones o universidades que de verdad les es imprecindible tener conexión a una red de alto rendimiento, para la cual hay que pagar el servicio.

Conclusiones técnicas

Con base en análisis que se realizó sobre la integración de las RA en América a nivel simulación y emulación se presentan las siguientes conclusiones:

El simulador hace una buena aproximación de la topología de backbone pero esta muy limitado en varios aspectos en comparación con el emulador. El cual hace una buena segunda aproximación de la topología de backbone pero no puede emular fielmente las RA actuales, ya que, la mayoría de estas utilizan enlaces y routers de backbone de mayor capacidad.

A) Conectividad

La conectividad en el simulador y emulador en cada red fue satisfactoria donde el protocolo OSPF no tuvo ningún problema. El simulador realizó una conectividad parcial del backbone de la integración, debido a que no se pudo realizar la comunicación de la red CLARA a CANARIE o viceversa, esto porque el simulador no soporta el protocolo IBGP para poder comunicar los "peers" de un sistema autónomo. Por su parte, el emulador tuvo una conectividad completa del backbone de la red integrada, ya que el protocolo EBGP e IBGP funcionaron de manera correcta.

B) Gestión

- Se logró la gestión tanto en el simulador, como en el emulador de cada red avanzada, presentando algunas diferencias en cuantos a la gestión de OIDs y estabilidad del protocolo SNMP. En cuestión de la gestion del backbone integrado, el simulador tuvo fallas debido a la conectividad parcial, en cambio el emulador la ejecuto sin problema alguno.

a) SIMULADOR

- La implementación del protocolo SNMP en el simulador carece de comandos de configuración en los dispositivos (router y switch) y operaciones pertenecientes a SNMP. Por ejemplo, no se puede restringir el acceso a una unidad gestora por lo que otras entidades gestoras pueden acceder a los dispositivos sin ningún problema. Tampoco se pueden activar las "traps" en los dispositivos para prevenir alguna falla. Así mismo se tiene una deficiencia en sus versiones ya que packet tracer no diferencia principalmente entre la versión 2 y 3, siendo esta última enfocada a la seguridad misma que se ignora totalmente en el simulador.
- El simulador en algunas ocasiones llegó a tener mensajes de error al simular distintos paquetes de SNMP de un AS a otro, donde se concluye que pude ser causado por el esfuerzo del simulador al procesar los mensajes SNMP por todos los router en los que tiene que pasar de ida y vuelta. En la figura 5.67 se muestra este ejemplo de error por parte de "packet tracer".

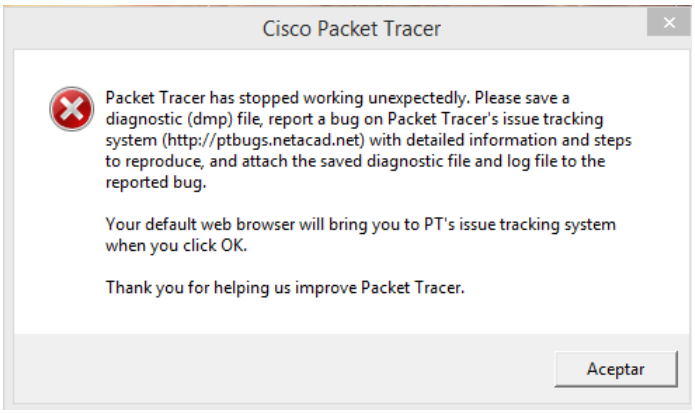


Figura 5.67 Mensaje de error

b) EMULADOR

- El emulador cuenta con funciones y operaciones completas de SNMP en v2 y v3.
- Las pruebas SNMP de gestión entre AS no tuvo ningún problema en el emulador, ya que al mover muchas instancias de objetos de un AS a otro AS no hubo pérdida, en contraste con en el simulador que presenta muchas limitaciones, como la perdida de instancias y fallas de entrega.
- No se pudo hacer toda una configuracion de objeto del router con SNMP, ya que algunos routers tienen que estar actualizados o incluso se deben cargar la MIB, pero esto sólo es posible con licencias de Cisco.

- La aproximación que se hizo de un NOC en el emulador sirvió para ver como esta presente el protocolo SNMP en la gestion de todos los dispositivos de red, y una vez mas se pudo comprobar la conectividad de todo el backbone de la integración al mover una gran cantidad de instancias de todos los "core routers", accediendo a más de 150 instancias por router. NPM no permitio configurar los dispositivos, ya que solo sirve para el monitoreo.

Limitaciones del simulador y emulador

Una de las limitaciones del simulador es el de no incluir routers de backbone, mismo que tampoco puede simular los enlaces de mayor capacidad con las que trabajan las RA.

Se forzó al simulador a que trabajara una cantidad grande de routers (73 routers en total), una de las problemáticas encontradas es que el simulador al abrir toda la integración, tanto la versión 7 y 6 de *packet tracer* tiene severas dificultades al levantar toda la configuración en todos los routers, ya que después de cierto tiempo (de 30 min a 1 h) estos empiezan a presentar fallas al bajar y subir interfaces a nivel protocolo de interfaz, lo que provocó que constantemente se estén enviando mensajes OSPF debido a esas fallas de interfaz.

Se quizo resolver este problema al realizar "troubleshooting", para lo cual primero se verificó a nivel protocolo de enrutamiento (se hizo un debug en OSPF y BGP) y después a nivel de interfaz donde se bajaron y levantaron las interfaces, asi como el cambio de estas. También se llegó a reinicializar los routers, pero el problema siguió. En conclusión el simulador "Packet Tracer" no soporta la activación de varios routers a la vez. En la figura 5.68 se puede apreciar este error extraido de un router después de pasar algunos minutos (10 min – 30 min).

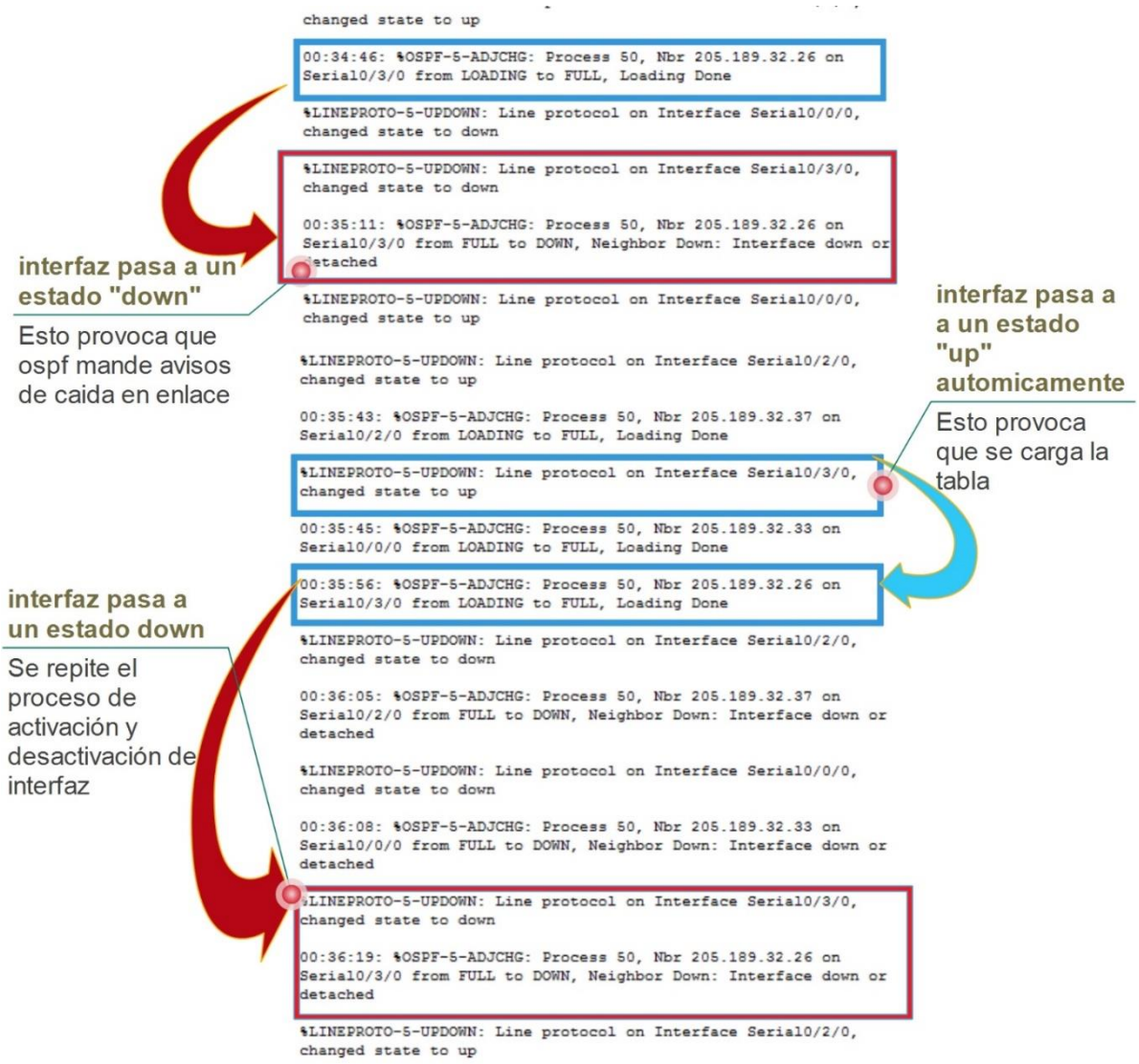


Figura 5.68 Error de carga en interfaz y tablas de enrutamiento

El emulador cuenta con equipo de backbone por lo que permite realizar redes más complejas donde se podría profundizar más en los protocolos OSPF y BGP, asi como la implementación de otros protocolos de enrutamiento.

El emulador permite crear redes más complejas que el simulador, y su funcionamiento, depende de los recursos del equipo en donde se requiera crear dicha emulación. Por ejemplo, como primer intento, se uso el mismo equipo que para la simulacion, pero se tuvieron las siguientes limitaciones:

- 13 routers cisco 7200 con versión 12, ya que, es una versión más ligera y utiliza menos recursos del equipo a comparación de la versión 15 que se utilizó
- 5 routers 2960 con version 12 y 5 VPCS.

La emulación con estos elementos consumió el 35% CPU y 82% RAM (3.28 GB), a pesar de ello GNS3 no podía emular otro core router C7200, sólo podía emular 1 router de acceso C2960.

Se optó por la implementación de VM debido a que las VPCS no soportan la gestión con SNMP, así como el resolver todo un "traceroute" de una dirección IP, de modo que sólo mostraban una ruta incompleta, las VPCS solo sirvieron para comprobar la conectividad mediante el comando ping.

Las VMs fueron una buena aproximación al conectarse al backbone, solo presentó un fallo, si se quiere analizar el tráfico con Wireshark en el enlace de host al Switch esto es imposible, solo se puede hacer el análisis del Switch al router, el problema es que se analizará todo el tráfico de todos los host conectados al Switch.

Otra limitacion de GNS3 son los enlaces que se pueden adicionar a un router C7200, para lo cual sólo se pueden agregar 7 enlaces GE, esto es un problema si un router tiene mucha conectividad con otros routers. Sin embargo se pueden agregar otros tipos de enlaces como FastEthernet y Seriales los cuales posibilitan más enlaces de este tipo. El problema que estos enlaces están alejados del estudio de RA.

Por último, para seguir estudiando las RA se necesita un emulador con mayores capacidades ó actualizar GNS3 con IOSs de routers de backbone superiores al C7200, asi como una mayor capacidad en los enlaces que se emulan, por lo menos se necesitan del orden de los 10 GbE.

Conclusiones no técnicas

El trabajo me ayudo adquirir conocimientos y habilidades en el manejo del emulador GNS3, lo cual hace que sea de utilidad al poder ejecutarlo en proyectos de redes de datos, donde se puede realizar una emulación de una red de datos antes de implementarla en el mundo real.

También adquiri la habilidad de seguir un metodologia de proyectos para estimar tiempos de planeacion y ejecución de tareas de algún proyecto.

Gracias a esta tesis dos trabajos relacionados con el tema de RA fueron enviados congresos arbritados los cuales fueron aceptados [18] y [128].

Apéndice A

Routers de Backbone para las RA

En este apéndice se describen algunos de los routers core acerca de los cuales se hicieron mención en esta tesis. En particular algunos de la marca Cisco y Juniper.

Los router core son la parte fundamental de las RA y algunos ISP, con estos se construye la infraestructura de red llamada Backbone para ofrecer diferentes servicios que son de suma importancia para las RA como el enrutamineto multiprotocolo, MPLS, VPN, QoS, L2TP. NetFlow, NAT, ACL, entre otros.

Estos routers core presentan un alto rendiemiento, arquitectura confiable y servicio de alta gama en comparación con los routers de acceso o distribución debido a que manejan y procesan demasiada informacion delicada.

Una de las características importantes de estos routers core es que no sólo cuentan con un solo sistema para procesar la información, sino que tiene la posibilidad de cambiar (inclusive integrar otro sistema) este sistema de procesamiento por otro (depende la compatibilidad) según sean las necesidades de la red. El sistema es llamado "processor route" para equipos Cisco o "routing engine" para equipos Juniper. Dichos sistemas se encargan de todos los procesos de los protocolos de enrutamiento, así como de los procesos de software que controlan las interfaces del router, los componentes del chasis, sistema de gestión y accesos de los usuarios del router [117].

En las siguientes 3 tablas se muestra una breve descripción de los routers core de Cisco y Juniper, posteriormente en la tabla A.4 se muestra una comparativa de algunas características, principalmente aquella máquina real que gestiona el enrutamiento integrado en los routers core antes mencionados.

Cisco 7200

Descripción

El Cisco 7200 presentó caracteristicas de modularidad y flexibilidad algo que los routers (1800,2800) de aquel entonces no presentaban. Tambien ofrecia una excepcional versatilidad en un formato compacto, adecuados para aplicaciones con conectividad GigaEthernet y POS (Packet Over SONET) ofreciendo procesamiento rápido de paquetes, de alrededor un poco mas de 2 millones de paquetes por segundo.

Así mismo, este modelo ofrece un extenso rango de interfaces para redes LAN o WAN, es adecuado para la agregacion WAN de alguna empresa o institución para ofrecer servicios de VoIP, seguridad y algunas otras aplicaciones IP debido a las caracteristicas excepcionales de enrutamenito que presenta, gracias a la incorporacion de un procesador potente.

Cisco GSR 12008	Descripción
	La serie GSR (Gigabit Switch Router) 12000 se basa en una arquitectura de enrutamiento distribuido de alta velocidad combinada con un sistema de conmutacion multigigabit. Este sistema hace las conexiones de tarjetas de líneas a una estructura centralizada, asi como las multiples transacciones de bus simultanea para ofrecer un enrutamiento de capa 3 a velocidades de Gigabit. Su arquitectura cumple con el ancho de banda, rendimiento, servicios y requisitos de fiabilidad de redes de Backbone. Ofrecen soporte de alta disponibilidad, conjunto básico y entidad de eje integrado con un rendimineto de 10 Gbps para uso de enrutamiento.

Tabla A. Router core Cisco 7200 y 12008 [118,119, 120]

Juniper MX-480	**Descripción**
	Los routers Juniper MX-480 y Mx-960 pertenecen a la familia "*MX series Universal Edge*" los cuales son routers de alto rendimiento, diseñados para proveer los requerimientos avanzados de *ethernet.* Ofrecen flexibilidad y fiabilidad para soportar servicios y aplicaciones avanzadas, están diseñados para proveer escalabilidad y alta densidad de puerto para enrutamiento y conmutación. Ofrecen características de enrutamiento mas complejas y avanzadas, segmentación de tráfico y virtualización con MPLS, Multicast con ultrabaja latencia, seguridad robusta e implementación QoS para la aceleración de entrega de aplicaciones y servicios. Estan diseñados para ofrecer rápido FRR (FastReRoute). Capaces de soportar servicios empresariales, móviles y residenciales gracias a una plataforma llamada "Universal Edge". El Router MX-480 está diseñado para data centers de medianas y grandes empresas por ofrecer una plataforma densa y altamente redundante. El Router MX-960 ofrece una plataforma de alta densidad para servicios de capa 3 y capa 2, alta gama de aplicaciones como VPLS para conectividad multipunto y soporte para MPLS VPN. Están enfocados para ser utilizados como routers core en los data centers por ser ideales para SCB (Switching Control Board) y RE (Routing Engine)
Juniper MX-960	
	

Tabla A.2 Routers Core Juniper MX 480 y 960 [122]

Juniper T-640	Descripción
	Los routers T-640 y T-1600 pertenecen a la famila “T series core routers”, la cual es una familia de routers core, ofreciendo características de funcionalidad, flexibilidad, requisitos de disponibilidad para un multiservicio core y la escala necesaria para las redes de gama alta y básica para satisfacer las necesidades de red actuales y futuras. Esta familia ofrece una solución multichasis llamada “TX Matriz y TX Matrix plus” para interconectar los routers core para aumentar su escala y capacidad por llevar un sistema único de 640 Gbps hasta un sistema de multichasis de hasta 22 Tbps. Esta familia ofrece una arquitectura para escalar hasta 64 Tbps y más allá del futuro donde pueden adaptarse a los cambiantes necesidades de servicios. Los router T-640 responden a la necesidad de enrutamiento de alto desempeño con la capacidad de enviar hasta 700 millones de paquetes por segundo. También admite interfaces de menor velocidad, ofreciendo mayor flexibilidad para combinar enrutamiento core de alta velocidad con agregacion de acceso dedicado en una sola plataforma. El T-1600 tiene la capacidad de enviar hasta 1.92 mil millones de paquetes por segundo. Las ranuras de 100 Gbps que ofrece el sistema ayuda a la compleja conmutación y reenvío de paquetes.
Juniper T-1600	
	

Tabla A.3 Routers Core Juniper T-640 y T-1600 [123]

Característica	Cisco 7200	Cisco GSR 12008	Juniper MX-480	Juniper MX-960	Juniper T 640	Juniper T 1600
Número de maquinas enrutamiento que se pueden cambiar.	4	2	8	8	5	5
Máquina real de enrutamiento	NPE-G2	GRP	RE-S-1300-2048	RE-S-2000-4096	RE-A-2000-4096 R	RE-DUO-C1800-8G
Microprocesador	Motorola Freescale 7448 @ 1.65 GHz	R5000 CPU @ 200 MHz	Pentium @ 1.3 GHz	Pentium @ 2 Ghz	Pentium @ 2 Ghz	Pentium @ 2 GHz
NVRAM	2 MB	2 MB	No disponible	No disponible	No disponible	No disponible
RAM	1 GB	512 MB	2 GB	4 GB	4 GB	4 GB
Flash	256 MB	512 MB	1 GB	1 GB	1 GB	1 GB
Interfaces	FDDI, ATM, Serial , POS, Token Ring, Ethernet, FastEthernet, GigaEthernet	ATM, POS/SDH, Ethernet, FastEthernet, GigaEthernet,	ATM IQ, SONET/SDH GigaEthernet, 10GigaEthernet, 40GigaEthernet, 100GgaEthernet	ATM IQ, SONET/SDH GigaEthernet, 10GigaEthernet, 40GigaEthernet, 100GigaEthernet	ATM IQ, SONET/SDH FastEthernet GigaEthernet, 10GigaEthernet, 40GigaEthernet	ATM IQ, SONET/SDH FastEhernet, GigaEthernet, 10GigaEthernet, 40GigaEthernet, 100GigaEthernet
IOS	Cisco IOS software release 12..2SB8/12.4(4)XD	Cisco IOS software release 12.0S/12.0ST	Junos 8.2 /Junos-WW	Junos 8.2 /Junos-WW	Junos 8.1 /Junos-WW	Junos 8.1/Junos-WW
Número de slots	4-6	8	8	11	8	8
Capacidades del sistema	2 Gbps	40 Gpbs	480 Gbps	480 Gbps	640 Gbps	1.6 Tbps

Tabla A.4 Tabla comparativa de caracteristicas de router's core [118, 120, 124, 125, 126, 127]

Lista de acrónimos

ARPANET (Advanced Research Project Agency Network – La red de la agencia de proyectos para la investigacion avanzada)

AS (Autonomous System –Sistema autónomo)

ATM (Asynchronous Transfer Mode – modo de transferencia asincrona)

BGP (Border Gateway Protocol – Protocolo de gateway de frontera)

CANARIE (CAnadian Network For The Advancement Research, Industry And Education - Red canadiense para el avance de la investigación, la industria y la educación.)

CLARA (Cooperación Latino Americana de Redes Avanzadas)

CPU (Central Processing Unit – Unidad de procesamieno central)

CSNET (Computer Science NETwork – Red de ciencias informaticas)

CUDI (Corporación Universitaria para el Desarrollo de Internet)

DWDM (Dense Wavelength Division Multiplexing – multiplexacion por division de longitud de onda densa)

EBGP (External BGP – BGP externo)

EGP (External Gateway Protocol – Protocolo de Gateway externo)

FTP (File Transfer Protocol – Protocolo de transferencia de archivo)

GigaPoP (Gigabit Point of Presence – Punto de presencia de un gigabit)

IBGP (Internal BGP – BGP interno)

ICMP (Internet Control Message Protocol – Protocolo de mensajes de control de internet)

IGP (Interior Gateway Protocol – Protocolo de gateway inerior)

IP (Internet Protocol – Protocolo de internet)

ISP (Internet Service Provider – Proveedor de servicios de internet)

LSA (Link State Advertisement – Anuncios del estado del enlace)

MIB (Management Information Base – Base de datos para la información)

NFV (Network Function Virtualitation – Virtualización de funciones de red)

NMS (Network Management System – Sistema de gestión de red)

NOC (network Operation Center – centro de operaciones de red)

NPM (Network Performance Monitor – Monitor de rendimiento de red)

NREN (National Research and Educationn Networks – Redes nacionales de investigación y educación)

NSFNET (National Science Fundation Network – red para la fundación nacional para la ciencia)

OID (Object IDentifier – Identificador de objeto)

OSPF (Open Shortest Path First – La primer ruta abierta mas corta)

PDU (Protocol Data Unit – Protocolo deunidad de datos)

POS (Packet Over Sonet- Paquetes sobre sonet)

PSTN (public switching telephonic network - Red telefónica publica conmutada)

RA (Redes avanzadas)

RFC (Request for Comments – Solicitud para comentarios)

RIP (Routng Information Protocol – protocolo de información de enrutamiento)

SDN (Software Defined Networking – Redes definidas por software)

SNMP (Simple Networtk Managment Protocol – Protocolo simple de gestion de red)

SONET (Synchronous Optical Network - Red optica sincrona)

TCP (Transport Control Protocol – Protocolo de control de transporte)

UDP (User Datagram Protocol – Protocolo de datagrama de usuario)

VLSM (Variable Length Subnet Mask – Máscara de subred de longitud variable)

VM (Virtual Machine – Máquina virtual)

Referencias

[1] CANARIE News, *Revolutionary human brain atlas created by Canadian-German team one of top 10 breakthrough technologies of 2014*, [en línea]; 30 april 2014 [consulta: 25 de mayo de 2017] Disponible: https://www.canarie.ca/revolutionary-human-brain-atlas-created-by-canadian-german-team-one-of-top-10-breakthrough-technologies-of-2014-2/

[2] Ireceptor, *About*, [en línea]; [consulta: 4 de julio de 2017] Disponible: http://ireceptor.irmacs.sfu.ca/about

[3] Genetics and Genomics Analysis Platform, *About*, [en línea]; 16 de mayo 2017 [consulta: 4 de julio de 2017] Disponible: https://genap.ca/public/home

[4] In the Field Stories, *Revealing the inner working of a tornado*, [en línea]; abril de 2017 [consulta: 4 julio de 2017] Disponible: https://www.inthefieldstories.net/revealing-the-inner-workings-of-a-tornado/

[5] School of medicine & Health Science, *institutions Connect to the Nation´s Fastest Research & Education Network to Benefit Health Researchers Nationwide*, [en línea]; 26 de febrero de 2014 [consulta: 4 julio de 2017] Disponible: https://smhs.gwu.edu/news/nih-and-george-washington-university-researchers-partner-accelerate-genomics-research-using

[6] Rutgers, *Information services & technologies*, [en línea]; 1 julio de 2013 [consulta: 4 julio de 2017] Disponible: http://ist.rbhs.rutgers.edu/research/hpc_resources.shtml#Internet2

[7] Internet2, *Research Wave Program*, [en línea]; [consulta: 4 julio de 2017] Disponible: https://www.Internet2.edu/research-solutions/research-support/research-wave-program/

[8] Red CLARA, *Inauguran chivo: el primer observatorio virtual*, [en línea]; 14 de mayo de 2015 [consulta: 4 julio de 2017] Disponible: https://redclara.net/index.php/noticias-y-eventos/noticias/destacados/3241-inauguran-chivo-el-primer-observatorio-virtual-chileno

[9] SPRACE, *The SPRACE project*, [en línea]; [consulta: 4 julio de 2017] Disponible: https://www.sprace.org.br/sprace-project

[10] Red CLARA, *OLE de como se emplean las e-tecnologías para la vigilancia y el pronostico de eventos medio ambientales en Latinoamérica*, [en línea]; 11 de marzo de 2011 [consulta: 4 julio de 2017] Disponible: https://www.redclara.net/index.php/noticias-y-eventos/noticias/destacados/1020-angel-g-munoz-s-ole2-de-como-se-emplean-las-e-tecnologias-para-la-vigilancia-y-el-pronostico-de-eventos-medioambientales-en-latinoamerica

[11] In the Field Stories, *Cientificos brasileños participan en un proyecto internacional de astronimia*, [en línea]; abril de 2017 [consulta: 4 julio de 2017] Disponible: https://www.inthefieldstories.net/es/cientificos-brasilenos-participan-en-un-proyecto-internacional-de-astronomia/

[12] Jose-Ignacio Castillo-Velázquez, Noe Galicia-Gutierrez, Juan-Arnulfo López-Ruiz, *"ingeniería inversa parcial y simulación de la infraestructura de una red de datos MAN",* ROC&C México 2013.

[13] Noé Galicia Gutiérrez (2015), *Emulación del BB de la red avanzada de Internet2 en México*, Tesis de Licenciatura, Universidad Autónoma de la Ciudad de México, Ciudad de México.

[14] Juan Arnulfo López Ruiz (2015), *Implementación de un modelo IPv4 Multicast*, Tesis de Licenciatura, Universidad Autónoma de la Ciudad de México, Ciudad de México.

[15] José Joaquín Sánchez Trejo (2015), *Emulación de la red Avanzada CLARA*, Tesis de Licenciatura, Universidad Autónoma de la Ciudad de México, Ciudad de México.

[16] J.I. Castillo and N. Galicia, *"Routing algorithms applied to an advanced academic network known as CUDI"*, IEEE Latin America Transactions, vol 14, no., pp 2974-2679, June 2016. doi:10.1109/TLA.2016.7555284.

[17] J.I. Castillo-Velazquez and J.J Sanchez-Trejo, *"Emulation for CLARA´s operation, the advanced network for Latin America",* 2016 IEEE ANDESCON, Arequipa, 2016, pp. 1-4. doi:10.1109/ANDESCON 2016.7836205.

[18] Jose-Ignacio Castillo-Velázquez, Daniel-Javier Serrano-Martínez, Augusto Morales, *"Emulation of Backbone´s connectivity and management for the advanced network in Latin America: 2016´s topology",* International Conference on Sensors Networks Smart and Emerging Technologies (SENSET 2017) Beirut, Lebanon, 2017. pp. 1-4 TBP.

[19] José Ignacio Castillo Velázquez, *Redes de datos: contexto y evolución*, Edit. SAMSARA, pp 52-60, 2016.

[20] Kathy Pretz, *The fathers of the internet*, [en línea]: 2014, [consulta:7 de septiembre de 2016] Disponible: http://theinstitute.ieee.org/technology-topics/consumer-electronics/the-fathers-of-the-internet

[21] R. Zakon, *Hobbes' Internet Timeline*, [en linea]; Noviembre de 1997 [consulta: 7 de septiembre de 2016] Disponible: http://www.rfc-base.org/txt/rfc-2235.txt

[22] Vinton G. Cerf, *Computer Networking: Global Infrastructure for the 21st Century*, [en linea]; 4 de noviembre de 2004, [consulta: 7 de septiembre de 2016] Disponible: http://courseweb.lt.unt.edu/gjones/fall2012/cecs5400/pdf/www.cs.washington.edu.pdf

[23] Internet2, *Internet2 Overview*, [en linea]; [consulta: 8 de septiembre de 2016] Disponible: https://www.Internet2.edu/presentations/LMP-Internet2-Brandeis.htm.ppt

[24] Internet2, *Internet2: A Tutorial part1*, [en linea]; [consulta: 8 de september de 2016] Disponible: https://www.Internet2.edu/presentations/SBRC99-1.ppt

[25] Bob Riddle, *Internet2 Overview*, [en linea]; 14 de febrero 2003, [consulta: 30 de Abril de 2017] Disponible: http://www.marquette.edu/ppts/Internet2/Ted-Hanss-20040305Marquette.ppt

[26] GITLER, Isidoro; KLAPP, Jaime. *High Performance Computer Applications: 6th International Conference, ISUM 2015*, Mexico City March 9-13, 2015, Revised Selected Papers. Springer, pp 25-32, 2016.

[27] XSEDE, *Overview*, [en linea]; 2017, [consulta: 30 de Abril de 2017] Disponible: https://www.xsede.org/overview

[28] Elizabeth Boten, Internet2 Congratulates LIGO Group on Recent Scientific Breakthrough, [en linea]; 17 de febrero 2016, [consulta: 30 de Abril de 2017] Disponible: http://www.Internet2.edu/news/detail/10207/

[29] Internet2, Case Studios, [en linea]; 2017, [consulta: 30 de Abril de 2017] Disponible: http://www.Internet2.edu/research-solutions/case-studies/

[30] Internet2, *Internet2 QBone: Building a Testbed for IP Differentiated Services*, [en línea]; california, E.U.A 1999 [consulta: 29 agosto 2019] Disponible: https://www.Internet2.edu/presentations/990623-INET99-BT/990623-INET99-BT.ppt

[31] Juha Eskelin, *Internet2*, [en linea]; 7 de mayo de 1998 [consulta: 28 de agosto de 2016] Disponible: http://www.tml.tkk.fi/Opinnot/Tik-110.551/1998/papers/07Internet2/

[32] Novatica, *Internet2 o la próxima generación de internet (parte segunda)*, [en linea]; agosto de 1997 [consulta: 28 agosto de 2016] Disponible: http://www.ati.es/novatica/1997/128/intdos-2.html

[33] Internet2, *Review of San Diego GigaPoP Meetings*, [en linea]; junio 1997 [consulta: 28 agosto 2016] Disponible: https://www.Internet2.edu/presentations/97-06-Denver-Giga-Tech/

[34] Leslie Regan Shade, *Computer Networking in Canada: from CA*net to CANARIE,* [en línea]; [consulta: 30 de septiembre de 2016] Disponible: http://www.cjc-online.ca/index.php/journal/article/view/794/700

[35] Howard C. Clark, *Formal Knowledge Networks*, [en linea]; 1998 Canada [consulta: 30 de septiembre de 2016] Disponible: https://www.iisd.org/pdf/fkn.pdf pag 60,61.

[36] CANARIE, *A Birthday for Canada's Internet,* [en linea]; 2015 [consulta: 1 octubre de 2016] Disponible: https://www.canarie.ca/a-birthday-for-canadas-internet/

[37] CANARIE, *About Us*, [en linea]; [consulta: 1 de octubre de 2016] Disponible: https://www.canarie.ca/about-us/

[38] CANARIE, *CANARIE – CA*net 3*, [en linea]; [consulta: 1 de octubre de 2016] Disponible: http://www.powershow.com/view1/e310b-ZDc1Z/CANARIE_CAnet_3_The_Customer_Empowered_Networking_Revolution_powerpoint_ppt_presentation

[39] CANARIE, *Network Infrastructure*, [en linea]; 2016 [consulta: 1 de octubre de 2016] Disponible: https://www.canarie.ca/network/infrastructure/

[40] Canadian ICFA, *Canadian Networks for Particle Physics Research*, [en linea]; 2015 [consulta: 1 de octubre de 2016] Disponible: http://hepnetcanada.ca/assets/themes/hepnet/documents/Canadian-ICFA-SCIC-Network-2014.pdf

[41]CANARIE, *CANARIE helps Canada Get There First*, [en linea]; 2016 [consulta: 2 de octubre de 2016] Disponible: https://www.canarie.ca/corporatereview/en/#?page=20

[42] CANARIE, *Canadian NREN Overview*, [en linea]; 2015 [consulta: 2 de octubre de 2016] Disponible: https://wiki.geant.org/download/attachments/47908767/20151109-CANARIE.pdf?version=1&modificationDate=1447153851340&api=v2

[43] CANARIE, *CANARIE Overview and Update*, [en linea]; 2009 [consulta: 2 de octubre de 2016] Disponible: https://www.Internet2.edu/presentations/fall09/20091005-itfr-bujold.pdf

[44] imagen tomada de CANARIE, *topology octuber2016*,[en linea]; 2016 [consulta 10 de octubre de 2016] Disponible https://www.canarie.ca/wp-content/uploads/CANARIENetworkMap_oct2016-web.png

[45] Internet2, http://www.Internet2.edu/, [Última visita: agosto de 2016]

[46] Internet2, *Timeline*, [en línea]; 2016 [consulta: agosto 2016] Disponible: http://www.Internet2.edu/about-us/Internet2-community-timeline/

[47] vBNS, *frequently asked,* [en linea]; [consulta: 28 agosto de 2016] Disponible: http://www.umass.edu/i2/vbns_faq.htm

[48] IEEE, *Internet2's Breakthroughs for Academic Research*, [en línea]; 2004 [consulta: julio 2016] Disponible: https://www.computer.org/csdl/mags/ds/2004/01/o1003.pdf

[49] Internet2, *Internet2: a tutorial part 2 of 4,* [en linea]; 1999 [consulta: 30 agosto de 2016] Disponible: https://www.**Internet2**.edu/presentations/SBRC99-**2**.ppt

[50] Internet2, *Internet2 101: Orientation and Overview,* [en linea]; 2005 [consulta: 29 de Agosto de 2016] Disponible: https://www.Internet2.edu/presentations/fall05/20050919-I2-I2.ppt

[51] CISCO, *The Internet2 Project,* [en línea]; [consulta: agosto 2016] Disponible: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-3/ipj-archive/article09186a00800c851d.html

[52] Imagen tomada de Internet2, *Abilene Update Session*, [en línea]; Washinton D.C., EEUU, 2003 [consulta: 15 de agosto 2016] Disponible: https://www.Internet2.edu/presentations/spring03/20030410-Abilene-Corbato.pdf

[53] IEEE, *Internet2 Network*, [en linea]; [consulta: julio 2016] Disponible: http://ewh.ieee.org/r6/san_francisco/comsoc/in2.htm

[54] Level3, *Internet2 and Level 3 Communications To Deploy Next Generation Nationwide Research Network,* [En línea]; 2006 [Consulta: julio 2016] Disponible: http://investors.level3.com/investor-relations/press-releases/press-release-details/2006/Internet2-and-Level-3-Communications-to-Deploy-Next-Generation-Nationwide-Research-Network/default.aspx

[55] Internet2, *News*, [en linea]; [consulta: agosto 2016] Disponible: http://www.Internet2.edu/news

[56] Imagen tomada de Internet2, *Internet2 Network Services & Operations Update*, [en línea]; 2008 [consulta: 15 de agosto 2016] Disponible: https://www.Internet2.edu/presentations/spring08/20080422-networkoperations-robb-vietzki.pdf

[57] Internet2, *About Intenet2: Accelerating research and education through community-developed technology* [en línea]; abril de 2014 [consulta: agosto 2016] Disponible: https://www.internet2.edu/media/medialibrary/2014/07/16/about-internet2-2014.pdf

[58] Imagen tomada de Internet2, *Internet2 Network Infrastructure Topology,* [en línea]; 2016, [consulta: agosto 2016] Disponible: http://www.Internet2.edu/media/medialibrary/2016/04/29/I2-Network-Infrastructure-Topology-All-201604.pdf

[59] RedCLARA, *Misión y Visión,* [en linea]; 2016 [consulta: 6 octubre de 2016] Disponble: *https://www.redclara.net/index.php/somos/mision-y-vision*

[60] RedCLARA, *Memoria Red CLARA 2015,* [en linea]; 2015 [consulta: 6 de octubre de 2016] Disponible: http://dspace.redclara.net/bitstream/10786/1017/1/RedCLARA_memoria_2015.pdf

[61] RedCLARA, DeCLARA Boletin Año 12, [en línea]; 2016 [consulta: 6 de octubre de 2016] Disponible: https://www.redclara.net/images/stories/DeCLARA/DeCLARA_es_47.pdf

[62] Cisco, *La tecnología de Cisco Systems potencia la red latinoamericana de investigación y educación, ALICE.* [en linea]; [consulta: 7 de octubre de 2016] Disponible: http://www.cisco.com/web/ES/about/press/press_home_s239.html

[63] RedCLARA, DeCLARA Boletin Año 1, [en línea]; 2005 [consulta: 7 de octubre de 2016] Disponible: http://dspace.redclara.net/bitstream/10786/615/1/DeCLARA_es_01.pdf

[64] Imagen tomada de CLARA, *Topoligia RedClara*,[en linea]; 2016 [consulta: 3 agosto 2016] Disponible: http://www.redclara.net/index.php/red-y-conectividad/topologia

[65] CLARA, http://www.redclara.net/ [Última visita; agosto 2016]

[66] Internet2, *Internet2's Global Programs: International Connectivity*,[En linea]; febrero 2016[consulta: 20 agosto de 2016] Disponible: https://www.nitrd.gov/nitrdgroups/images/a/ae/InternationalNetworkingI2Update.pdf

[67] West and Central African Research and Education Network (WACREN) http://wacren.net/en [ultima visita: 20 agosto de 2016]

[68] TEIN*CC, http://www.teincc.org/teincc/index.do [ultim visita: 20 agosto de 2016]

[69] Asia Pacific Advanced Network(APAN), *APAN Networks Maps*, [en linea]; 2016 [consulta: 24 agosto de 2016] Disponible: https://www.apan.net/images/apan-map-by-project-20130208.jpg

[70] Oregon State University, *Internet2: Basic Terms and Facts,* [en línea]; [consulta: Julio 2016] Disponible: http://web.engr.oregonstate.edu/~pancake/Internet2/Internet2.html

[71] CUDI, *Internet2 presentacion a la sociacion mexicana de la industria de tecnologías de la informacion,* [en linea]; 1999 [consulta: 29 de agosto de 2016] Disponible: http://www.cudi.mx/sites/default/files/CUDI/presentaciones/1999/1999_08_10_AMITI.PPT

[72] Internet2, *Global Services,* [en linea]; 2016 [consulta: 20 agosto de 2016] Disponible: http://www.Internet2.edu/products-services/advanced-networking/global-services/#service-overview

[73] CUDI, *Powered by Community,* [en linea]; 2016 [consulta: 21 agosto de 2016] Disponible: http://www.cudi.edu.mx/primavera_2016/presentaciones/internet_02.pdf

[74] AMPATH, *AMPATH Resourses,* [en linea]; 2016 [consulta 24 de agosto de 2016] Disponible: http://ampath.net/amlight.php

[75] Jennifer M. Schopf, *TransPAC4,* [en linea]; 2015 [consulta: 24 agosto 2016] Disponible: http://internationalnetworks.iu.edu/files/pdf/transpac_reports/TP4%20Y1Q2%20-%20Jan%2015%20-%20post.pdf#TransPAC Y1Q2

[76] TransPAC, *TransPAC: More than Just a Network,* [en línea]; 3 marzo de 2013 [consulta: 24 agosto de 2016] Disponible: http://archive.apan.net/meetings/apan39/Sessions/34/TP_for_APAN_March_2015.pdf

[77] Internet2, *Advanced North Atlantic 100 Gbit/s Ring for Research & Education Now Operational,* [en linea]; 2014 [consulta: 24 agosto de 2016] Disponible: http://www.Internet2.edu/news/detail/7477/

[78] Internet2, *NSF IRNC Program International Deployment and Experimental Efforts with SDN in 2013*,[en linea]; 2013 [consulta: 24 agosto de 2016] Disponible: https://www.Internet2.edu/media/cms_page_media/2014/1/17/IRNC_SDN_2013_whitepaper_final.pdf

[79] Tomoaki Nakamura ,*Update on SINET5 implementation for ICEPP (ATLAS) and KEK (Belle II),* [en linea]; 2013 [consulta: 24 agosto 2014] Disponible: https://indico.cern.ch/event/461511/contributions/1135235/attachments/1242599/1828298/2016-03-13_TNakamura.pdf

[80] GEANT, *Global Networking*,[en linea]; 2016 [consulta: 23 agosto de 2016] Disponible: http://www.geant.org/Resources/Documents/Global_Connectivity_map_04_june_2016.pdf

[81] Internet2, reachable Networks, [en linea]; 2013, Disponible https://www.Internet2.edu/media/medialibrary/2013/08/07/ReachableNetworks.pdf

[82] Networking and Indiana University, *Topology*, [en linea]; 2016 [consulta: 24 agosto de 2016] Disponible: http://internationalnetworks.iu.edu/initiatives/transpac/topology.html

[83] Pacific Wave, http://pacificwave.net/ [ultima vistia:24 de agosto de 2016]

[84] Canarie, *Canadian NREN Overview*, [en línea]; 9 de noviembre de 2015 [consulta: 25 de agosto de 2016] Disponible: https://wiki.geant.org/dosearchsite.action?queryString=CANARIE

[85] Press, Cisco. Internetworking Technologies Handbook. *Kapitel*, pp. 118-128, 2003, ISBN: 1-58705-119-2.

[86] Sportack, Mark A.; Fairweather, Julie. *IP routing fundamentals*. Cisco Press, pp. 128-146, 1999. ISBN: 1-57870-108-X.

[87] Peterson, Larry L.; Davie, Bruce S. *Computer networks: a systems approach*. Elsevier, pp, 240-250, 2012. ISBN: 978-0-12-385059-1.

[88] Malhotra, Ravi. *IP routing*. O'Reilly Media, Inc., pp, 1-9, 2002, ISBN: 0-596-00275-0,

[89]Cisco Modulo CCNA, *Exploración: Conceptos y protocolos de enrutamiento*, pp, 30-46, 110-133, 419-425.

[90] Kurose, James F., et al. *Redes de computadoras: un enfoque descendente*. Addison Wesley, pp, 292-308, 2010, ISBN: 84-7829-061-3.

[91] Pablo, Gil; Pomares, Jorge; Candelas, Francisco. *Redes y transmisión de datos*. Universidad de Alicante, pp, 174-177, 2010.

[92] Stallings, William, et al. *Redes de Computadoras*. pp, 321-325, 2000.

[93] Medhi, Deepankar. *Network routing: algorithms, protocols, and architectures*. Morgan Kaufmann, pp 30-40, 147-152, 166-191, 238-378, 2010, ISBN: 0-12-088588-3.

[94] Doyle, Jeff; Carroll, Jennifer. *Routing TCP/IP*, 2005, vol. 1, pp 202-252, 2006, ISBN: 1-68706-202-4.

[95] Sportack, Mark A.; Fairweather, Julie. *IP routing fundamentals*. Cisco Press, pp, 147-190, 1999, ISBN: 1-57870-108-X.

[96] Hunt, Craig. *TCP/IP network administration*. "O'Reilly Media, Inc.", pp 179-184, 2002. ISBN: 0596002971.

[97] Shamim, Faraz. *Troubleshooting IP routing protocols*. Cisco Press, pp 58-81, 2002, ISBN: 1-58705-019-6.

[98] Murhammer, Martin W., et al. *IP Network Design Guide*. IBM, pp 135-1380, 1999.

[99] Malkin G & Bay Networks. RFC 2453, *RIP version 2*, Nov. 1998, Network Working Group

[100] Malkin, G. & Minnear, R, RFC 2080, *RIPng for IPv6*, Jan. 1997, Network Working Group

[101] Ernesto, Ariganello; Sevilla, Barrietos. Redes Cisco CCNP a Fondo, Guía de estudio para profesionales. Alfaomega, pp 69-119, 201-225, 2010, ISBN: 978-607-7854-79-1.

[102] Tadimety, Phani Raj. *OSPF: A Networking Routing Protocol*. Apress, pp 37-105, 2015, ISBN: 978-1-4842-1411-4.

[103] REKHTER, Yakov; LI, Tony; HARES, Susan. RFC 4271, *A border gateway protocol 4 (BGP-4)*. Jan 2006, Network Working Group

[104] Teare, Diane; Vachon, Bob; Graziani, Rick, *Implementing Cisco IP routing (ROUTE) foundation learning guide: foundation learning for the ROUTE 300-301 exam*. Pearson Education, pp 423-506, 2010.

[105] Marques, Pedro R.; Dupont, Francis. RFC 2545, Use of BGP-4 multiprotocol extensions for IPv6 inter-domain routing. Mar. 1999, Network Working Group.

[106] Kurose, James F., et al. *Redes de computadoras: un enfoque descendente*. Addison Wesley, pp 659-679, 2010.

[107] Stallings, William, *SNMP and SNMPv2: the infrastructure for network management*; [en linea]; 1998 [consulta: 2 de diciembre de 2016] Disponible: http://www.cn.ryerson.ca/courses/8861/notes/Readings/SNMPv1v2.pdf

[108] Case, Jeffrey D., RFC 1157 *Simple network management protocol (SNMP)*. May 1990, Network Working Group.

[109] Case, Jeffrey, RFC 1905, *Protocol Operations for Version 2 of the Simple Network Managem ent Protocol SNMPv2*, Jan 1996, Network Working Group.

[110] Mauro, Douglas; Schmidt, Kevin, *Essential SNMP* ", O'Reilly Media, Inc.", pp 19-71, 73-78 , 2005, ISBN: 0-596-00840-6.

[111] Presuhn, Randy. RFC 3416, Version 2 of the protocol operations for the simple network management protocol (SNMP). Dec 2002, Network Working Group.

[112] Bahador Bakhshi, SNMPv2, [en linea], 2016, [consulta: 12 de enero de 2017] Disponible en http://ceit.aut.ac.ir/~bakhshis/NM/09-SNMPv2.pdf

[113] SNMP Research International Inc., *SNMPv3 White Paper*, [en línea]; [consulta: 8 de diciembre de 2016] Disponible: http://www.snmp.com/snmpv3/v3white.shtml

[114] Case, J RFC 3410. *Introduction and applicability statements for internet-standard management framework*. Dec 2002, Network Working Group.

[115] GNS3., *Software*, [en línea]; [consulta: 1 de mayo de 2017] Disponible: https://www.gns3.com/software

[116] José Ignacio Castillo Velázquez, *"El árbol de internet y estructura de la información de gestión de una red",* IEEE Latin America and the Caribbean Newsletter, pp. 15-17 , April 2009, Year 20, Number 62.

[117] Cisco, *Network Processing Engine and Network Services Engine Installation and Configuration*, [en línea]; [consulta: 22 de mayo de 2017] Disponible:

http://www.cisco.com/c/en/us/td/docs/routers/7200/install_and_upgrade/network_process_engine_install_config/npense.html

[118] Cisco, *Cisco 7200 VXR SeriesRouters Overview,* [en línea]; 2007 [consulta: 22 de mayo de 2017] Disponible: http://www.cisco.com/c/en/us/products/collateral/routers/7200-series-routers/product_data_sheet09186a008008872b.pdf

[119] Cisco, *Cisco 12000 series-Internet Routers,* [en línea]; 2002 [consulta: 23 de mayo de 2017] Disponible: http://www.dich.com.tw/Product/Router/Cisco/12000/12000.pdf

[120] Cisco, *Cisco 12008 Gigabit Swith Router Installation and Configuration Guide,* [en línea]; 2004 [consulta: 23 de mayo de 2017] Disponible: http://www.cisco.com/c/en/us/td/docs/routers/12000/12008/installation/guide/icg.pdf

[121] Juniper Networks, *MX960, MX480, MX240, MX104 and MX803D Universal Edge Routers,* [en línea]; may 2017 [consulta: 24 de mayo de 2017] Disponible: https://www.juniper.net/assets/jp/jp/local/pdf/datasheets/1000597-en.pdf

[122] Juniper Networks, *MX480 3D Universal Edge Routers Hardware Guide,* [en línea]; 30 de marzo de 2016 [consulta: 24 de mayo de 2017] Disponible: https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx480/

[123] Juniper Networks, *T Series Core Routers,* [en línea]; Oct 2014 [consulta: 25 de mayo de 2017] Disponible: http://www.juniper.net/us/en/local/pdf/datasheets/1000051-en.pdf

[124] Juniper Networks, *MX480 3D Universal Edge Routers Hardware Guide,* [en línea]; 30 de marzo de 2016 [consulta: 24 de mayo de 2017] Disponible: https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx480/

[125] Juniper Networks, *MX960 3D Universal Edge Routers Hardware Guide*, [en línea]; 2017 [consulta: 24 de mayo de 2017] Disponible: https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx960/index.pdf

[126] Juniper Networks, *T640 Core Router Hardware Guide,* [en línea]; 2015 [consulta: 25 de mayo de 2017] Disponible: http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/t-series/t640/index.pdf

[127] Juniper Networks, *T1600 Core Router Hardware Guide*, [en línea]; 2016 [consulta: 25 de mayo de 2017] Disponible: http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/t-series/t1600/index.pdf

[128] Jose-Ignacio Castillo-Velázquez, Daniel-Javier Serrano-Martínez, Augusto Morales, *"Emulation of Backbone´s connectivity and management for the layer 3 service of Internet2: 2016´s topology",* CONCAPAN XXXVII, Nicaragua, 2017. pp. 1-4 TBP.